Cisco Unified CM Trunks

Revised: November 19, 2013; OL-30952-01

A trunk is a communications channel on Cisco Unified Communications Manager (Unified CM) that enables Unified CM to connect to other servers. Using one or more trunks, Unified CM can receive or place voice, video, and encrypted calls, exchange real-time event information, and communicate in other ways with call control servers and other external servers.

Trunks are an integral and crucial part of a Cisco Collaboration System deployment, hence it is important to understand the types of trunks available, their capabilities, and design and deployment considerations such as resiliency, capacity, load balancing, and so forth.

There are two basic types of trunks that can be configured in Unified CM:

- SIP and H.323 trunks, both of which can be used for external communications
- Intercluster trunks (ICTs)

While H.323 trunks are still supported, SIP trunks are the recommended trunk type for Unified Communication deployments because SIP trunks provide additional features and functionality not available with H.323 trunks. This chapter provides a comparative overview of the capabilities of H.323 and SIP trunks, but the focus of this chapter is on SIP trunks, their operation, and features for Unified Communications deployments. For detailed information on H.323 trunk capabilities and operation, refer to the *Cisco Unified CM Trunks* chapter of the *Cisco Collaboration 9.x SRND*, available at

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/collab09/trunks.html

For more details on the applications of Unified CM trunks, refer to their respective sections in the following chapters of this document:

- Collaboration Deployment Models, page 10-1
- Media Resources, page 7-1
- Call Admission Control, page 13-1
- Cisco IM and Presence, page 20-1

What's New in This Chapter

Note This chapter has been revised significantly for the current release of this document. Cisco recommends that you read this entire chapter before attempting to deploy trunks in your Collaboration and Unified Communications System.

Table 6-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

*Table 6-1   New or Changed Information Since the Previous Release of This Document*

New or Revised Topic	Described in:	Revision Date
MTP-Less SIP Early Offer	MTP-Less Early Offer, page 6-21	November 19, 2013
H.323 trunk information has been removed from this chapter, and the chapter has been rewritten to focus on SIP trunks and their operation and features.	For information on H.3213 trunks, refer to the *Cisco Unified CM Trunks* chapter of the *Cisco Collaboration 9.x SRND*, available at http://www.cisco.com/go/ucsrnd	November 19, 2013

Unified CM Trunks Solution Architecture

Cisco Unified CM uses the mechanism of IP trunks to exchange call-related information with other components of a Unified Communications solution. Given their importance in this respect, it is important to develop the system architecture of the IP trunks with proper regard to the protocol, feature and service expectations, performance requirements, and so forth.

Figure 6-1 illustrates the role of IP trunks in system connectivity. The illustration does not show all possible connections from the Unified CM cluster.

Figure 6-1   IP Trunks Provide Connections to Unified CM
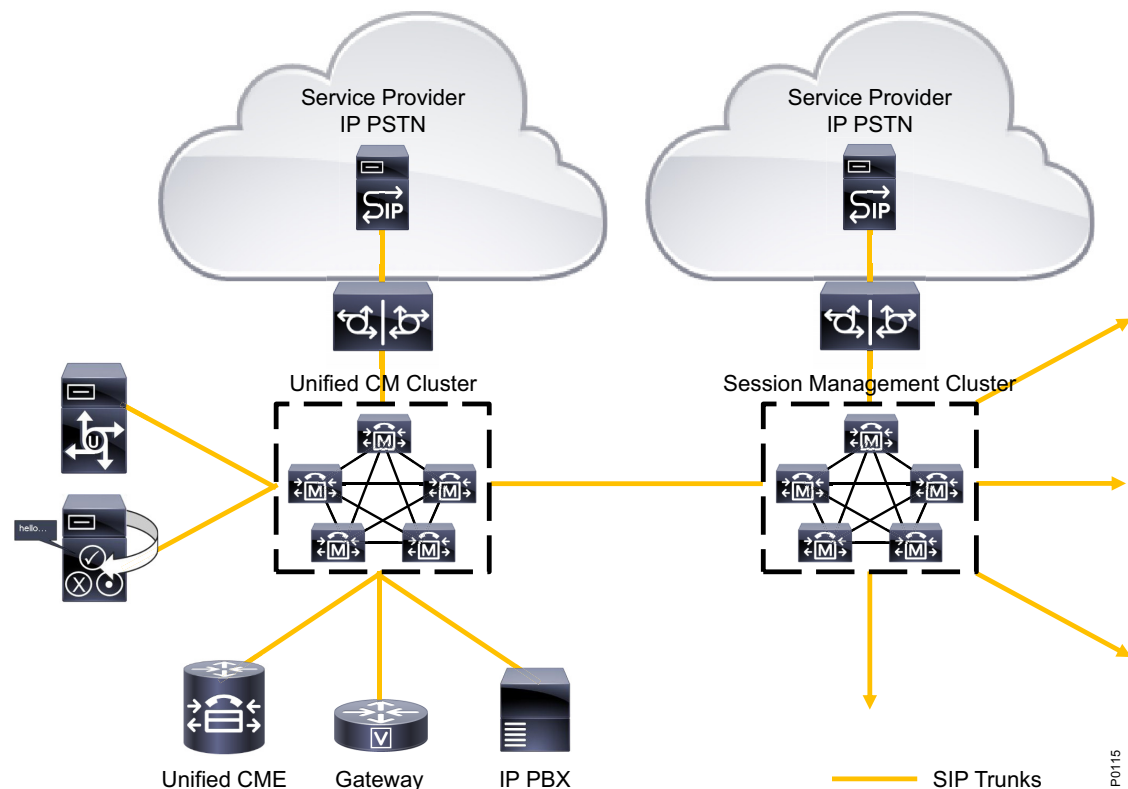
Calls are directed toward trunks as defined by the dial plan, using the route pattern construct. A route pattern can use a trunk either directly or through a route list. The route list, if used, consists of one or more route groups, each of which contains one or more trunks. An individual trunk within a route group may be configured to be selected in either a top-down or circular fashion. For outgoing calls, Unified CM selects one of the trunks associated in this fashion with the route pattern. Before it accepts an incoming call, Unified CM verifies whether a trunk is defined to the remote address from which the call is received.

A Comparison of SIP and H.323 Trunks

Cisco Unified CM trunk connections support both SIP and H.323. The decision to use SIP or H.323 is driven by the unique feature(s) offered by each protocol. Over the past several releases, as SIP has grown in popularity among both Unified Communications vendors and customers, the features and functionality supported by SIP trunks have grown to the point where SIP trunks offer a richer set of features than H.323 trunks, making SIP trunks the recommended choice for Unified Communications deployments. Today, most customers are migrating away from H.323 trunks and gatekeeper-based Unified Communications deployments to those that use SIP trunks only, with Cisco Unified Communications Manager Session Manager Edition as the trunk and dial plan aggregation platform.

As can be seen in Table 6-2, while SIP and H.323 trunks share many of the same features for trunk connections between Cisco devices, SIP trunks support several features that are not supported by H.323 trunks. For trunk connections to other vendors' products and to service provider networks, SIP is the most commonly deployed protocol today and is growing in usage as Unified Communications products and networks using protocols such as H.323 migrate to SIP.

Table 6-2 compares some of the features offered over SIP and H.323 trunks between Unified CM clusters.

Table 6-2   Comparison of SIP and H.323 Features on Cisco Unified CM Trunks

Feature	SIP	H.323
Calling Line (Number) Identification Presentation	Yes	Yes
Calling Line (Number) Identification Restriction	Yes	Yes
Calling Name Identification Presentation	Yes	Yes
Calling Name Identification Restriction	Yes	Yes
Connected Line (Number) Identification Presentation	Yes	Yes
Connected Line (Number) Identification Restriction	Yes	Yes
Connected Name Identification Presentation	Yes	Yes
Connected Name Identification Restriction	Yes	Yes
Alerting Name	Yes	*No*
Call Transfer (Blind/Attended)	Yes/Yes	Yes/Yes
Call Forward All	Yes	Yes
Call Forward Busy	Yes	Yes
Call Forward No Reply	Yes	Yes
QSIG Call Completion to Busy Subscriber	Yes	Yes

Table 6-2   Comparison of SIP and H.323 Features on Cisco Unified CM Trunks (continued)

Feature	SIP	H.323
QSIG Call Completion No Reply	Yes	Yes
QSIG Path Replacement	Yes	Yes
Subscribe/Notify, Publish - Presence	Yes	*No*
Message Waiting Indication (MWI: lamp ON, lamp OFF)	Yes	*No*
Call Hold/Resume	Yes	Yes
Music On Hold (unicast and multicast)	Yes	Yes
DTMF-relay	RFC 2833, KPML (OOB), Unsolicited Notify (OOB)	H.245 Out Of Band (OOB)[1]
SIP Early Offer	Yes - MTP may be required	N/A
SIP Delayed Offer	Yes	N/A
H.323 Fast Start	N/A	Yes - MTP always required for Outbound Fast Start - Voice Calls Only supported
Accept Audio Codec Preference in Received Offer	Yes	*No*
Codecs with MTP for SIP Early Offer/ H323 Fast Start	All codecs supported when **Early Offer support for voice and video calls (insert MTP if needed)** is checked G.711, G.729 when **MTP Required** is checked	G.711, G.723, G.729 only
Video	Yes	Yes
Video codecs	H.261, H.263, H.263+, H.264 AVC	H.261, H.263, H.263+, H.264 AVC
Video Presentation sharing (BFCP)	Yes	*No*
Multi-Level Precedence and Preemption (MLPP)	Yes	Yes
T.38 Fax	Yes	Yes
Signalling Authentication	Digest, TLS	*No*
Signalling Encryption	TLS	*No*
Media Encryption (audio)	SRTP	SRTP
RSVP-based QoS and call admission control	Yes	*No*
Support for + character	Yes	*No*
Incoming Called Party Transformations	Yes	Yes
Incoming Calling Party Transformations	Yes	Yes

Table 6-2   Comparison of SIP and H.323 Features on Cisco Unified CM Trunks (continued)

Feature	SIP	H.323
Connected Party Transformation	Yes	Yes
Outbound Calling Party Transformations	Yes	Yes
Outbound Called Party Transformations	Yes	Yes
Outbound Calling/Called Party Number Type Setting	SIP does not support Number Type	Unified CM, Unknown, National, International, Subscriber
Outbound Called/Called Party Numbering Plan Setting	SIP does not support Number Plan	Unified CM, ISDN, National Standard, Private, Unknown
Trunk destination - State detection mechanism	OPTIONS Ping	*Per call attempt*
IPv6, Dual Stack, ANAT	Yes	*No*
Protocol modification scripts for interoperability	Yes	*No*
Run on All Unified CM Nodes	Yes	Yes
Up to 16 Destination Addresses	Yes	Yes
URI based calls	Yes	No
Geo Location support	Yes	Yes

1. H.323 trunks support signalling of RFC 2833 for certain connection types.

SIP Trunks Overview

SIP trunks provide connectivity to other SIP devices such as gateways, Cisco Unified CM Session Management Edition, SIP proxies, Unified Communications applications, and other Unified CM clusters. Today, SIP is arguably the most commonly chosen protocol when connecting to service providers and Unified Communications applications. Cisco Unified CM provides the following SIP trunk and call routing features:

- Runs on all Unified CM nodes
- Up to 16 destination IP addresses per trunk
- SIP OPTIONS ping keep-alives
- SIP Early Offer support for voice and video calls (insert MTP if needed)
- Audio codec preference (and Accept Audio Codec Preference in Received Offer)
- SIP trunk normalization and transparency scripts for interoperability
- SIP REFER transparency
- H.264 Video with Desktop Presentation (Binary Flow Control Protocol (BFCP)) and Far End Camera Control (FECC)

The SIP trunk features available in the current release of Unified CM make SIP the preferred choice for new and existing trunk connections. The QSIG over SIP feature provides parity with H.323 intercluster trunks and can also be used to provide QSIG over SIP trunk connections to Cisco IOS gateways (and on to QSIG-based TDM PBXs). The ability to run on all Unified CM nodes and to handle up to 16 destination IP addresses improves outbound call distribution from Unified CM clusters and reduces the number of SIP trunks required between clusters and devices. SIP OPTIONS ping provides dynamic

reachability detection for SIP trunk destinations, rather than per-call reachability determination. SIP Early Offer support for voice and video calls (insert MTP if needed) can reduce or eliminate the need to use MTPs and allows voice, video, and encrypted calls to be made over SIP Early Offer trunks.

SIP trunk normalization and transparency using Lua scripts improve native Unified CM interoperability with third-party unified communications systems. Normalization allows inbound and outbound SIP messages and SDP information to be modified on a per-SIP-trunk basis. Transparency allows Unified CM to pass SIP headers, parameters, and content bodies from one SIP trunk call leg to another, even if Unified CM does not understand or support the parts of the message that are being passed through.

These features are discussed in detail later in this section.

For the complete list of new enhancements for SIP trunks, refer to the Cisco Unified Communications Manager product release notes available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

Session Initiation Protocol (SIP) Operation

This section explains how Unified CM SIP trunks operate and describes several key SIP trunk features that should be taken into account when designing and deploying Unified CM SIP trunks.

SIP Offer/Answer Model

Cisco Unified CM uses the SIP Offer/Answer model for establishing SIP sessions, as defined in RFC 3264. In this context, an Offer is contained in the Session Description Protocol (SDP) fields sent in the body of a SIP message. The Offer typically defines the media characteristics supported by the device (media streams, codecs, directional media attributes, IP address, and ports to use). The device receiving the Offer sends an Answer in the SDP fields of its SIP response, with its corresponding matching media streams, codec, directional media attributes, and the IP address and port number on which it wants to receive the media streams. Once the Offer and Answer have been exchanged, two-way media can be established between the calling and called endpoints. Unified CM uses this Offer/Answer model to establish SIP sessions as defined in the key SIP standard, RFC 3261.

RFC 3261 defines two ways that SDP messages can be sent in the Offer and Answer. These two methods are commonly known as Delayed Offer and Early Offer, and support for both methods by User Agent Client/Servers is required by specification RFC 3261. In the simplest terms, an initial SIP Invite sent with SDP in the message body defines an Early Offer, whereas an initial SIP Invite without SDP in the message body defines a Delayed Offer.

Delayed Offer and Early Offer are the two options available to all standards-based SIP switches for media capabilities exchange. Most vendors have a preference for either Delayed Offer or Early Offer, each of which has its own set of benefits and limitations.

Unified CM SIP trunks support both SIP Delayed Offer and SIP Early Offer. By default, SIP trunks are configured as Delayed Offer and support voice, video and encrypted calls. For Early Offer calls, Unified CM inserts a media termination point (MTP) if the media characteristics of the calling device cannot be determined (for example, for an inbound Delayed Offer call forwarded over an Early Offer SIP trunk). Unified CM Early Offer trunk configuration is discussed in detail later in this chapter.

SIP Delayed Offer

In a Delayed Offer, the session initiator (calling device) does not send its capabilities in the initial Invite but waits for the called device to send its capabilities first (for example, the list of codecs supported by the called device, thus allowing the calling device to choose the codec to be used for the session). Figure 6-2 shows an example of a SIP Delayed Offer.

Figure 6-2   *SIP Delayed Offer*
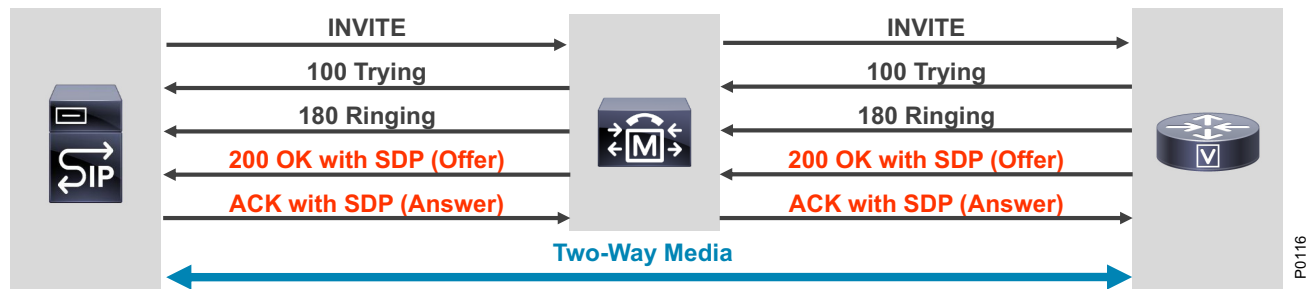
SIP Early Offer

In an Early Offer, the session initiator (calling device) sends its capabilities (for example, codecs supported, IP address, and UDP port number for RTP) in the SDP body contained in the initial Invite (thus allowing the called device to choose the codec for the session). Early Offer is often preferred by third-party unified communications vendors, and it is almost always used by service providers. Service providers use a feature of Early Offer that allows one-way media to be established to the calling device on receipt of the SDP Offer in the initial INVITE. This one-way media feature is used to play announcements to the caller (for example, Unknown Number) before call charges commence. (Call charges typically commence after two-way media is established and the final acknowledgment (ACK) for the transaction is received.)

Note   SIP-based Cisco Unified IP Phones send Early Offer. (See Figure 6-3.)

Figure 6-3   *SIP Early Offer*
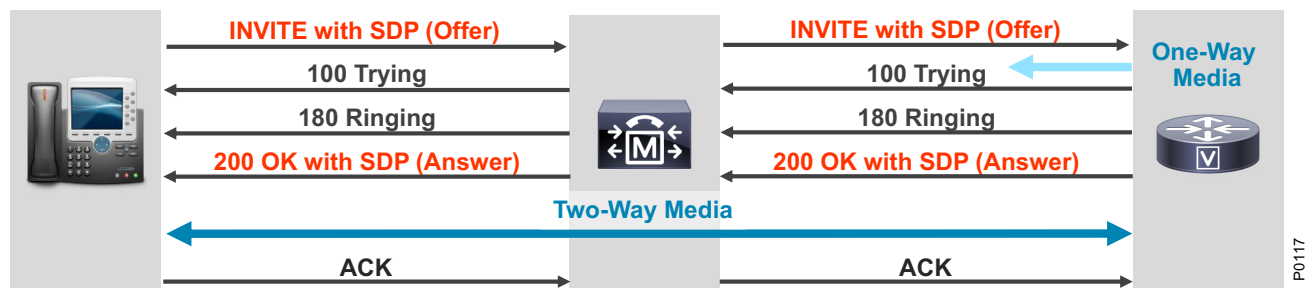
Provisional Reliable Acknowledgement (PRACK)

SIP defines two types of responses to SIP Requests: Final Responses and Provisional Responses.

Final Responses (for example, 2XX, 3XX, and 4XX Responses) convey the result of a processed Request (such as an INVITE) and are sent reliably (which means they are acknowledged).

Provisional Responses (all 1XX Responses) provide information on the progress of the request, but they are not sent reliably, so the sender of a provisional response does not know that it has been received. For this reason SDP information is not sent in unreliable 1XX responses.

Provisional Reliable Acknowledgment (PRACK) is an extension to the SIP protocol that allows 1XX responses to be sent reliably. PRACK is useful because it provides reliability of 1XX responses for interoperability scenarios with the PSTN, and it can also be used to reduce the number of SIP messages that need to be exchanged before setting up two-way media. (See Figure 6-4 and Figure 6-5.)

PRACK can be used over SIP trunks using Early Offer or Delayed Offer, and it is often called *Early Media*. PRACK is supported by the majority of Cisco Collaboration products and is a generally recommended feature.

Figure 6-4   ***SIP Early Offer with Early Media (PRACK)***
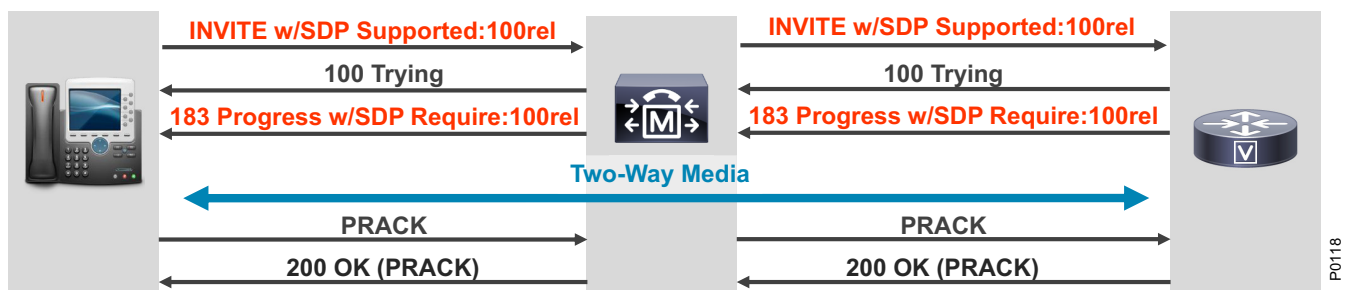
Figure 6-5   ***SIP Delayed Offer with Early Media (PRACK)***
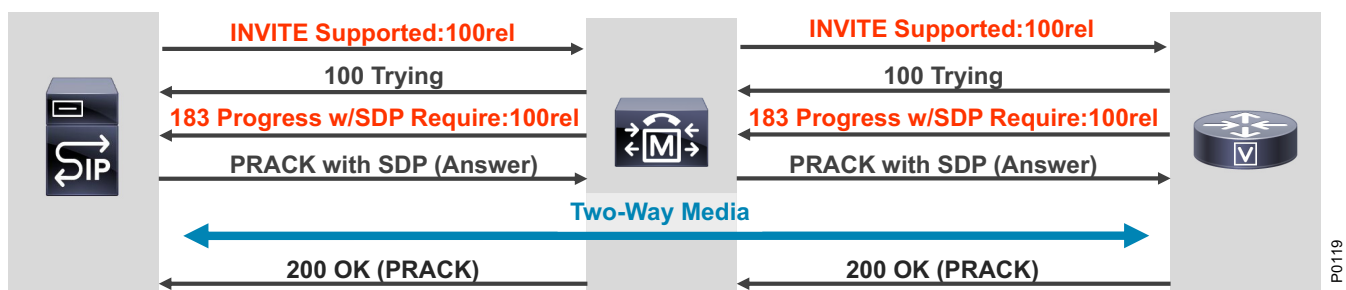
Note   100 Trying Responses indicate that Unified CM has received the INVITE. 180 Ringing and 183 Session in Progress Responses indicate that the user is being alerted of the call and are used to send information about the called user in SIP header messages and, if PRACK is used, in SDP messages.

Session Description Protocol (SDP) and Media Negotiation

SDP is the companion protocol of SIP. Defined in RFC 4566, SDP is used to describe media characteristics and to negotiate the media type, format, and associated parameters for a multimedia session between endpoints. These media characteristics are described by a series of one-line fields in a SDP message.

Session Description Protocol (SDP) and Voice Calls

The example in Table 6-3, Table 6-4, and Figure 6-6 illustrates an SDP Offer and Answer for a voice call.

Table 6-3   Voice Call – SDP Offer

SDP Message Field	Description
v=0	SDP version (currently version 0)
o=CiscoCCM-SIP 2000 1 IN IP4 10.10.199.250	Origin (contains Unified CM IP address)
s=SIP Call	Session name
c=IN IP4 10.10.199.130	Connection data (endpoint IP address)
t=0 0	Timing (0 0 = permanent session)
m=audio 16444 RTP/AVP 0 8 18 101	Media description – UDP port, RTP payload type for offered codecs (in preference order), and DTMF
a=rtpmap:0 PCMU/8000	G.711 mu-law codec
a=ptime:20	Packetization (sampling) interval (ms)
a=rtpmap:8 PCMA/8000	G.711 a-law codec
a=ptime:20	Packetization (sampling) interval (ms)
a=rtpmap:18 G729/8000	G.729 codec
a=ptime:20	Packetization (sampling) interval (ms)
a=sendrecv	Media direction
a=rtpmap:101 telephone-event/8000	RFC 2833 in-band DTMF
a=fmtp:101 0-15	DTMF characters supported

The corresponding SDP Answer describes the media characteristics of the endpoint that receives the Offer and the voice codec selected by the endpoint for two-way voice media (see Table 6-4).
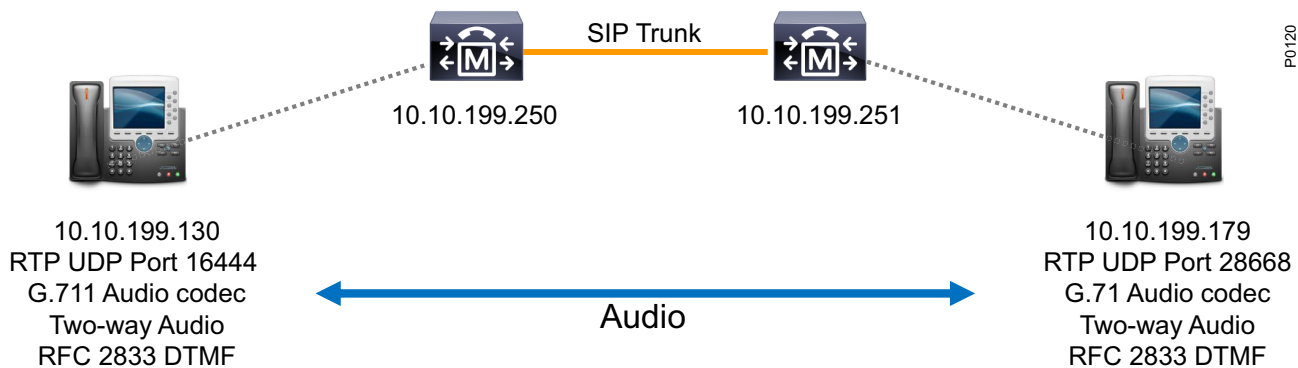
Table 6-4   Voice Call – SDP Answer

SDP Message Field	Description
v=0	SDP version (currently version 0)
o=CiscoCCM-SIP 2000 1 IN IP4 10.10.199.251	Origin (contains Unified CM IP address)
s=SIP Call	Session name
c=IN IP4 10.10.199.179	Connection data (endpoint IP address)
t=0 0	Timing (0 0 = permanent session)
m=audio 28668 RTP/AVP 0 101	Media description – UDP port, RTP payload type for the selected codec, and DTMF
a=rtpmap: 0 PCMU/8000	G.711 mu-law codec
a=ptime:20	Packetization (sampling) interval (ms)
a=sendrecv	Media direction
a=rtpmap:101 telephone-event/8000	RFC 2833 in-band DTMF
a=fmtp:101 0-15	DTMF characters supported

Figure 6-6   Negotiated Voice Call

SIP Trunk

10.10.199.250   10.10.199.251

10.10.199.130
RTP UDP Port 16444
G.711 Audio codec
Two-way Audio
RFC 2833 DTMF

Audio

10.10.199.179
RTP UDP Port 28668
G.71 Audio codec
Two-way Audio
RFC 2833 DTMF

Session Description Protocol (SDP) and Video Calls

For voice calls, symmetric media flows with a common voice codec are negotiated by the endpoints. For video media flows, it is commonly desirable for the send and receive media capabilities to be asymmetric. The requirement for asymmetry stems from a number of use cases such as broadband services where the upload and download speeds are different (often by an order of magnitude). In addition, video encoding is more CPU intensive than decoding video, and video endpoints can typically decode at higher resolution than they can encode. Because of these requirements, the video codec capabilities sent in an SDP Offer and Answer should be considered as the receive capabilities of the respective endpoints and are commonly asymmetric.

Table 6-5 shows the SDP Offer for a voice and video call.

Table 6-5   Voice and Video Call – SDP Offer

SDP Message Field	Description
v=0	SDP version (currently version 0)
o=CiscoCCM-SIP 161095 1 IN IP4 10.10.199.250	Origin (contains Unified CM IP address)
s=SIP Call	Session name
t=0 0	Timing (0 0 = permanent session)
m=audio 16444 RTP/AVP 0 8 18 101	Audio media – Port number and audio codecs listed by payload type in preference order and DTMF payload type
c=IN IP4 10.10.199.130	Connection data (endpoint IP address)
….	Attributes of multiple audio codecs and DTMF
m=video 16446 RTP/AVP 98 99	Media description – UDP port and RTP payload type for offered video codecs (in preference order)
c=IN IP4 10.10.199.130	Endpoint IP address
a=rtpmap:98 H264/90000	H.264 video codec
a=fmtp:98 profile-level-id=428016;packetization-mode=1;max-mbps=245000;max-fs=9000;max-cpb=200;max-br=5000;max-rcmd-nalu-size=3456000;max-smbps=245000;max-fps=6000	H.264 codec media attributes
a=rtpmap:99 H263-1998/90000	H.263 video codec
a=fmtp:99 QCIF=1;CIF=1;CIF4=1;CUSTOM=352,240,1	H.263 codec media attributes
a=rtcp-fb:* nack pli	RTCP for packet loss indication
a=rtcp-fb:* ccm tmmbr	RTCP for video rate adaptation

Notice that the H.264 and H.263 codecs offered in this SDP message contain a range of additional parameters that describe the receive capabilities of the endpoint. As shown in Table 6-6 for the negotiated H.264 codec in the SDP Answer, these parameters do not need to be symmetrical.

Table 6-6   Voice and Video Call – SDP Answer

SDP Message Field	Description
v=0	SDP version (currently version 0)
o=CiscoCCM-SIP 112480 1 IN IP4 10.10.199.251	Origin (contains Unified CM IP address)
s=SIP Call	Session name
t=0 0	Timing (0 0 = permanent session)
m=audio 28668 RTP/AVP 0 101	Audio media – Port number, selected audio codec, and DTMF payload type
c=IN IP4 10.10.199.179	Connection data (endpoint IP address)
….	Attributes of selected G.711 audio codec and DTMF

Table 6-6   Voice and Video Call – SDP Answer (continued)

SDP Message Field	Description
m=video 28670 RTP/AVP 98	H.264 codec selected for video
c=IN IP4 10.10.199.179	Endpoint IP address
a=rtpmap:98 H264/90000	H.264 codec details
a=fmtp:98 profile-level-id=428016;packetization-mode=1;max-mbps=108000;max-fs=3600;max-cpb=200;max-br=5000;max-rcmd-nalu-size=1382400;max-smbps=108000;max-fps=6000	Media attributes of the selected H.264 codec. Profile-level-id and packetization mode must be symmetric for the negotiated call; other attributes need not be symmetric and represent the receive capabilities of the endpoint.
a=rtcp-fb:* nack pli	RTCP for packet loss indication
a=rtcp-fb:* ccm tmmbr	RTCP for video rate adaptation

The Profile Level ID and Packetization Mode must be symmetrical for the negotiated video call. The Profile Level ID describes a minimum subset of H.264 features, resolution, frame rate, and bit rate supported by the endpoint. The Packetization Mode describes how video samples can be encapsulated and sent in RTP packets. The media attributes, which follow the Profile Level ID and Packetization Mode, need not be symmetrical and indeed are not all symmetrical for the negotiated video call shown in Table 6-6 and Figure 6-7.

Figure 6-7   Negotiated Voice and Video Call
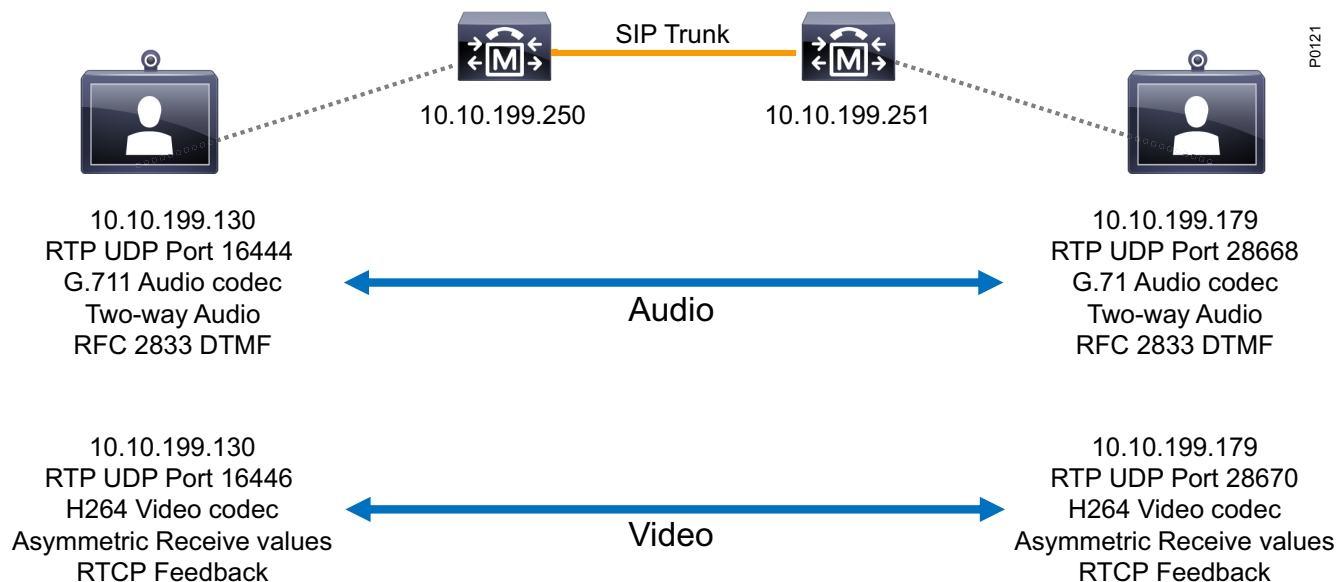
Video Desktop Sharing and Binary Floor Control Protocol (BFCP)

For video desktop and presentation sharing, the endpoints negotiate an additional RTP video channel to transmit the shared content (presentation slides, for example) and a UDP channel for BFCP, which manages shared access to resources within the video or conference call. (See Figure 6-8.) BFCP is described in RFC 4582 and RFC 4583.

Far End Camera Control (FECC)

Far End Camera Control allows a user to select a video source and to control camera actions such as pan, tilt, zoom and focus. Endpoints using FECC negotiate an additional RTP channel for camera control. (See Figure 6-8.) FECC is described in H.281, H.224, and RFC 4573.

Figure 6-8   ***Audio and Video Call with Presentation Sharing and Far End Camera Control***

SIP Trunk

10.10.199.250   10.10.199.251

10.10.199.130   10.10.199.179

Audio RTP UDP Port 16444 G711 Audio codec RFC 2833 DTMF	Audio	Audio RTP UDP Port 28668 G711 Audio codec RFC 2833 DTMF
Video RTP UDP Port 16446 H.264 Video codec	Main Video	Video RTP UDP Port 28670 H.264 Video codec
Video RTP UDP Port 16448 H.264 Video codec	Slide Video	Video RTP UDP Port 28672 H.264 Video codec
BFCP UDP Port 5070	Binary Floor Control	BFCP UDP Port 5070
FECC UDP Port 16450 RTP Payload Type 107	Far End Camera Control	FECC UDP Port 28674 RTP Payload Type 107

P0122

Unified CM SIP Trunk Features and Operation

This section explains how Unified CM SIP trunks operate and describes several key SIP trunk features that should be taken into account when designing and deploying Unified CM SIP trunks.

Run on All Unified CM Nodes

Cisco Unified CM provides a configuration option for allowing SIP trunk calls to be made or received on any call processing subscriber node in the cluster.

SIP Trunks – Run on All Nodes and the Route Local Rule

When the **Run on all Active Unified CM Nodes** option is checked on a SIP trunk, Unified CM creates an instance of the SIP trunk daemon on every call processing subscriber within the cluster, thus allowing a SIP trunk call to be made or received on any call processing subscriber. (Prior to this feature, up to three nodes could be selected per trunk by using Unified CM Groups.) With **Run on all Active Unified CM Nodes** enabled, outbound SIP trunk calls originate from the same node on which the inbound call (for example, from a phone or trunk) is received (based on the Route Local rule). The **Run on all Active Unified CM Nodes** feature overrides the trunk's Unified CM Group configuration.

For SIP trunks, the Route Local rule operates as follows:

For outbound SIP trunk calls, when a call from a registered phone or inbound trunk arrives at a Unified CM node, Unified CM checks to see if an instance of the selected outbound trunk exists on the same node where the inbound call arrived. If so, Unified CM uses this node to establish the outbound trunk call.

Enabling **Run on all Active Unified CM Nodes** on SIP trunks is highly recommended because this feature allows outbound calls to originate from, and be received on, any call processing node within the cluster. **Run on all Active Unified CM Nodes** can also eliminate calls from being set up between call processing nodes within the same cluster before being established over the outbound SIP trunk.

As with all Unified CM SIP trunks, the SIP daemons associated with the trunk will accept inbound calls only from end systems with IP addresses that are defined in the trunk's destination address fields. When multiple SIP trunks to the same destination(s) are using the same call processing nodes, a unique incoming and destination port number must be defined per trunk to allow each trunk to be identified uniquely.

Route Lists – Run on All Nodes and the Route Local Rule

Although this is not specifically a SIP trunk feature, running route lists on all nodes provides benefits for trunks in route lists and route groups. Running route lists on all nodes improves outbound call distribution by using the Route Local rule to avoid unnecessary intra-cluster call setup traffic.

For route lists, the Route Local rule operates as follows:

For outbound calls that use route lists (and associated route groups and trunks), when a call from a registered phone or inbound trunk arrives at the node with the route list instance, Unified CM checks to see if an instance of the selected outbound trunk exists on the same node as the route list. If so, Unified CM uses this node to establish the outbound trunk call.

If both the route list and the trunk have **Run on all Active Unified CM Nodes** enabled, outbound call distribution will be determined by the node on which the inbound call arrives. If the selected outbound trunk uses Unified CM Groups instead of running on all nodes, Unified CM applies the Route Local rule

if an instance of the selected outbound trunk exists on the same node on which the inbound call arrived. If an instance of the trunk does not exist on this node, then Unified CM forwards the call (within the cluster) to a node where the trunk is active.

If the route list does not have **Run on all Active Unified CM Nodes** enabled, an instance of the route list will be active on one node within the cluster (the primary node of the route list's Unified CM Group). If the selected outbound trunk is also active on the primary node of the route list's Unified CM Group, the Route Local rule will apply, resulting in sub-optimal outbound call distribution because all outbound trunk calls will originate from this node.

Cisco strongly recommends enabling **Run on all Active Unified CM Nodes** on all route lists and SIP trunks.

Up to 16 SIP Trunk Destination IP Addresses

SIP trunks can be configured with up to 16 destination IP addresses, 16 fully qualified domain names, or a single DNS SRV entry. Support for additional destination IP addresses reduces the need to create multiple trunks associated with route lists and route groups for call distribution between two Unified Communications systems, thus simplifying Unified CM trunk design. This feature can be used in conjunction with the **Run on all Active Unified CM Nodes** feature. (See Figure 6-9 and Figure 6-10.) Bear in mind, however, that the SIP daemons associated with a Unified CM SIP trunk will accept inbound calls only from end systems with IP addresses that are defined in the trunk's destination address fields. Use a single SIP trunk with one or more destination addresses to connect a Unified CM cluster to one other unified communications system. If trunk fail-over is required, create an additional trunk to the fail-over unified communications system and use route lists and route groups to order trunk selection. Unified CM randomly distributes outbound calls over the configured SIP trunk destination addresses.

Figure 6-9   SIP Trunks with Run on All Unified CM Nodes and Multiple Destination Addresses
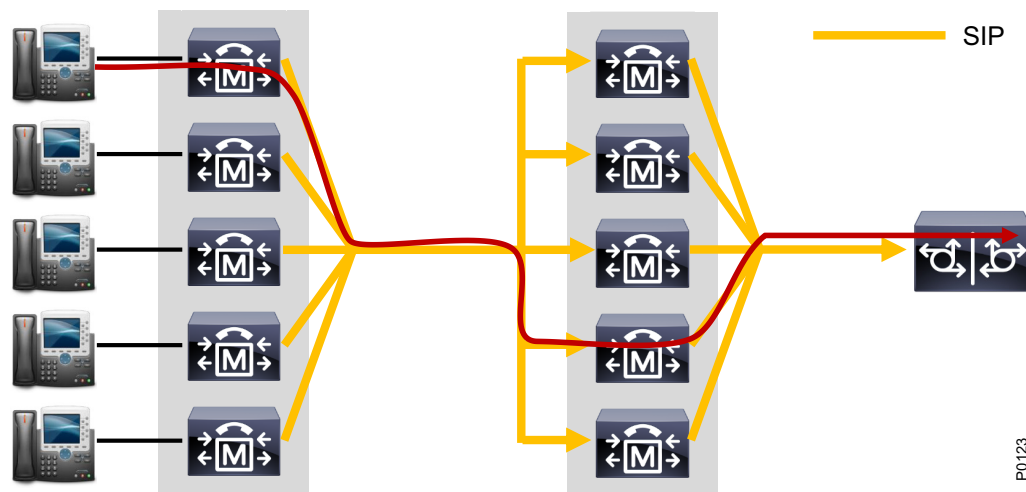
Figure 6-10   SIP Trunks and Route Lists with Run on All Unified CM Nodes Enabled

Trunk A

Trunk B

SIP

Route List instance

P0124
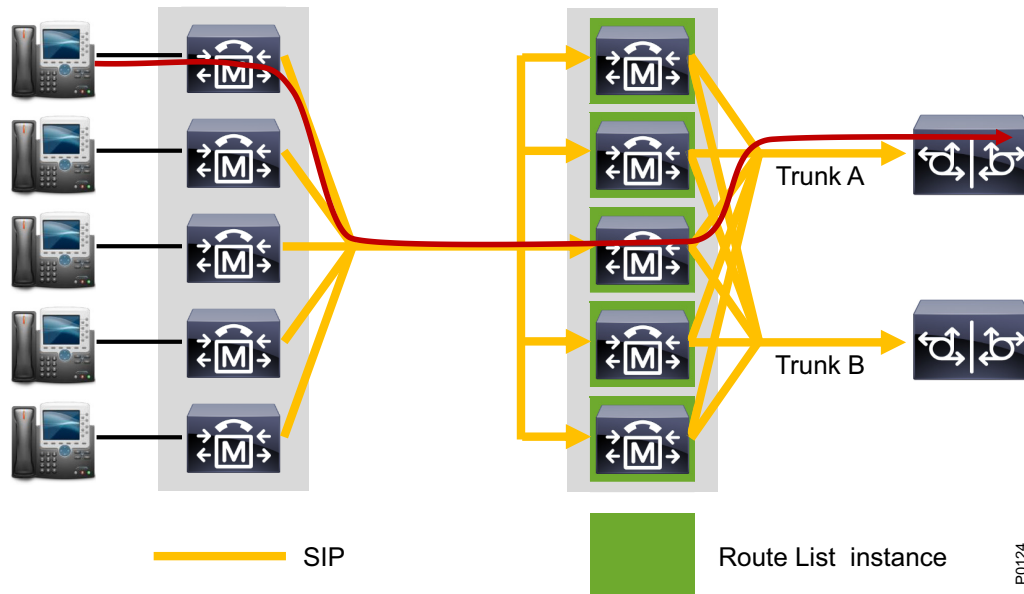
SIP Trunks Using DNS

Using a DNS SRV entry as the destination of a SIP trunk might be preferable to defining multiple destination IP addresses in certain situations such as the following:

- SRV host prioritization is required
- SRV host weighting is required
- More than 16 destination IP addresses are required
- DNS SRV resolution is a requirement of the destination Unified Communications system

Note   If the configuration option **Destination Address is an SRV** is selected, only a single SRV entry can be added as the trunk destination. (For example, Destination Address = cluster1.cisco.com. Port = 0.)

Figure 6-11 shows the call flow for a SIP trunk using DNS SRV to resolve the addresses to a destination Unified CM cluster. However, this destination could also be a third-party unified communications system.

Figure 6-11   *Call Flow for Intercluster SIP Trunk Using DNS SRV*
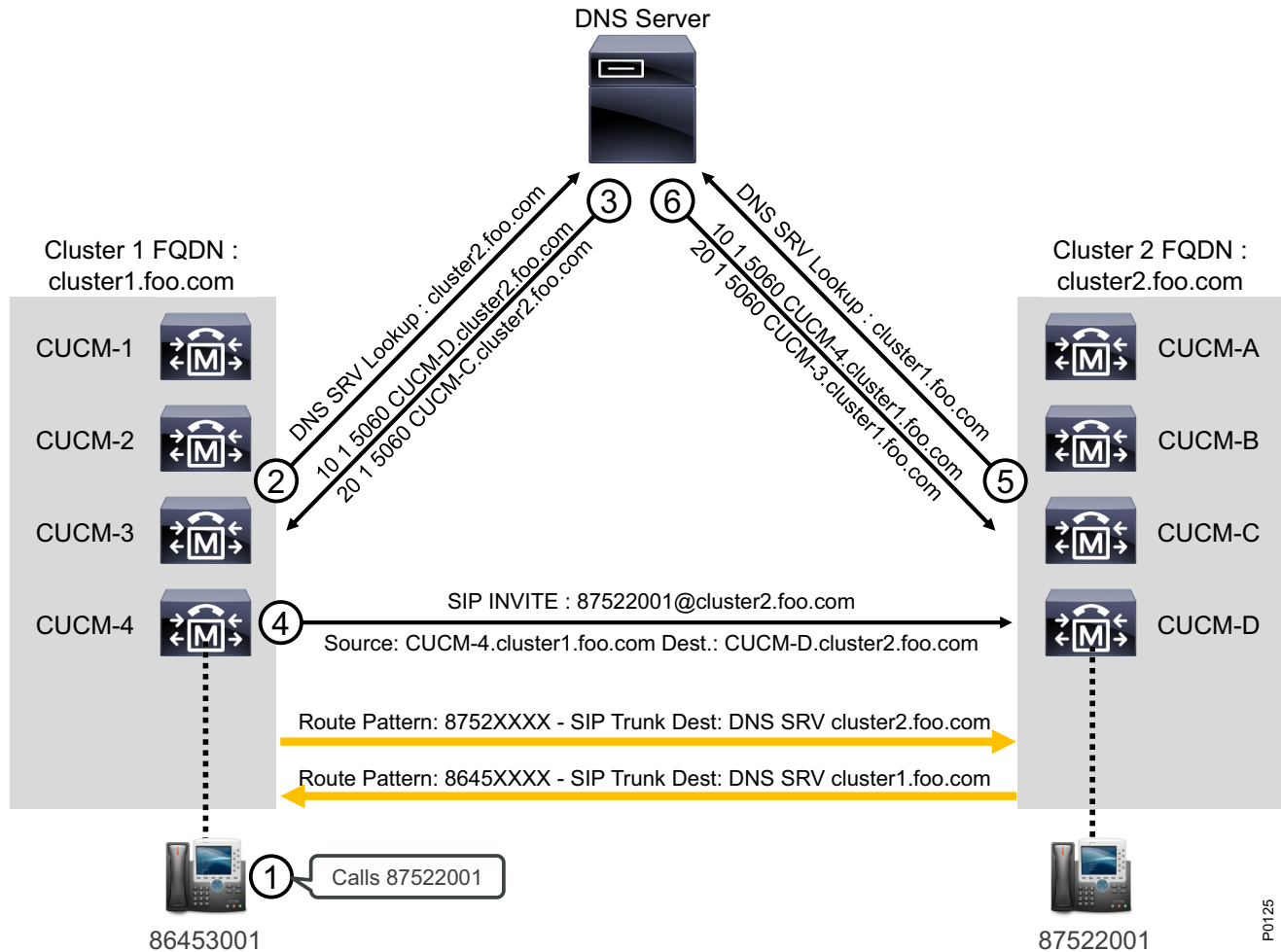
Figure 6-11 illustrates the following steps in the call flow:

1. The IP phone in Cluster 1 calls 87522001.

2. The call matches a route pattern of 8752XXXX that is pointing to the SIP trunk with DNS SRV of cluster2.foo.com. CUCM-4 in Cluster 1 is the node handling this call because the phone and the SIP trunk are both registered to it. CUCM-4 sends a DNS SRV lookup for cluster2.foo.com.

3. The DNS server replies with two records: CUCM-D.cluster2.foo.com and CUCM-C.cluster2.foo.com. Because CUCM-D.cluster2.foo.com has a higher priority, the call is attempted to this Unified CM. Before sending the SIP Invite, another DNS lookup is done for CUCM-D.cluster2.foo.com.

4. CUCM-4 sends a SIP Invite to 87522001@cluster2.foo.com, with destination address set to the IP address of CUCM-D.

5. Unified CM interprets this call as a local call because the host portion of the uniform resource identifier (URI) matches the Cluster FQDN enterprise parameter. Cluster 2 does not have any SIP trunk configured with a destination of CUCM-4, so it does a DNS SRV lookup for all domains configured under the SIP trunks with DNS SRV. In this case, the example shows a single trunk with a DNS SRV destination of cluster1.foo.com.

6. The DNS server returns two entries, and one of them matches the source IP address of the Invite. The cluster accepts the call and extends it to extension 87522001.

Note   The DNS A Look-up is not shown in this call flow.

SIP OPTIONS Ping

The SIP OPTIONS Ping feature can be enabled on the SIP Profile associated with a SIP trunk to dynamically track the state of the trunk's destination(s). When this feature is enabled, each node running the trunk's SIP daemon will periodically send an OPTIONS Request to each of the trunk's destination IP addresses to determine its reachability and will send calls only to reachable nodes. A destination address is considered to be "out of service" if it fails to respond to an OPTIONS Request, if it sends a Service Unavailable (503) response or Request Timeout (408) response, or if a TCP connection cannot be established. The overall trunk state is considered to be "in service" when at least one node receives a response (other than a 408 or 503) from a least one destination address. SIP trunk nodes can send OPTIONS Requests to the trunk's configured destination IP addresses or to the resolved IP addresses of the trunk's DNS SRV entry. Enabling SIP OPTIONS Ping is recommended for all SIP trunks because it allows Unified CM to track trunk state dynamically rather than determining trunk destination state on a per-node, per-call, and time-out basis.

Unified CM SIP Trunks – Delayed Offer and Early Offer

This section provides guidance on the use of Delayed Offer and Early Offer with SIP trunks.

Unified CM SIP Delayed Offer

The default configuration for Unified CM SIP trunks is to use Delayed Offer (SIP INVITE without SDP). Unlike Early Offer, Delayed Offer trunks do not need to use media termination points (MTPs) to create the SDP Offer. In certain cases (discussed below) MTPs can limit the media types supported for a call to voice only; therefore, if support for voice, video, and encrypted calls is desired, Delayed Offer should be used.

Unified CM SIP Early Offer

Two configurable options are available to enable Early Offer for Unified CM SIP trunks:

*   Media Termination Point Required
*   Early Offer support for voice and video calls (insert MTP if needed)

Early Offer Using Media Termination Point Required

Enabling the **Media Termination Point Required** option on the SIP trunk assigns an MTP from the trunk's media resources group (MRG) to every inbound and outbound call. (See Figure 6-12.) This statically assigned MTP supports either the G.711 or G.729 codec only, thus limiting media to voice calls only, using the selected codec type. Enabling Early Offer using **Media Termination Point Required** has been superseded by **Early Offer support for voice and video calls (insert MTP if needed)**. Early Offer using **Media Termination Point Required** can be useful in cases where voice media for inbound and outbound calls needs to be anchored to a single IP address (that of the MTP).

Figure 6-12   SIP Early Offer with Media Termination Point Required
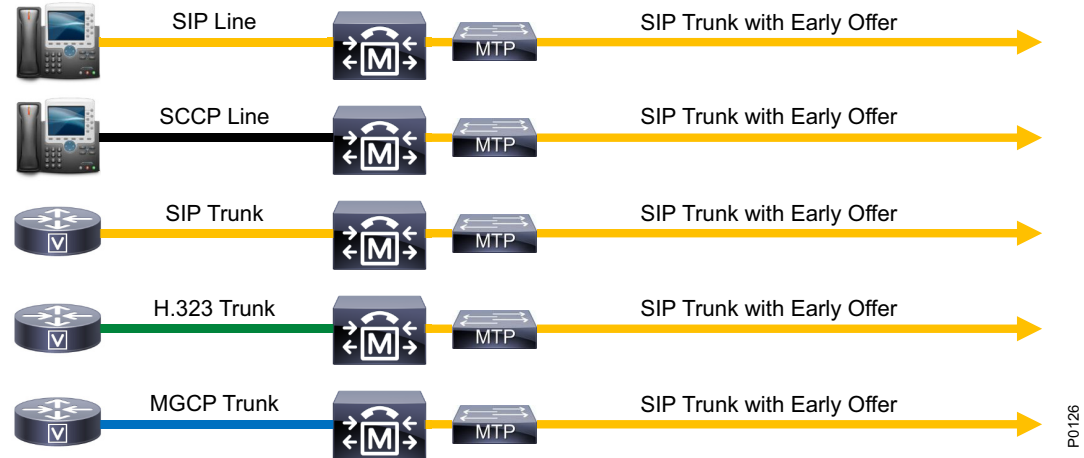
Early Offer Using Early Offer support for voice and video calls (insert MTP if needed)

Enabling **Early Offer support for voice and video calls (insert MTP if needed)** on the SIP Profile associated with the SIP trunk inserts an MTP only if the calling device cannot provide Unified CM with the media characteristics required to create the Early Offer. In general, **Early Offer support for voice and video calls (insert MTP if needed)** is recommended over **Media Termination Point Required** because this configuration option reduces MTP usage and can support voice, video, and encrypted calls. (see Figure 6-13).

For outbound calls over a SIP trunk configured as Early Offer support for voice and video calls (insert MTP if needed), Unified CM inserts an MTP to create an SDP Offer in the following cases only:

- An inbound call to Unified CM is received over a Delayed Offer SIP trunk
- An inbound call to Unified CM is received over an H.323 Slow Start trunk
- An inbound call is received from an older SCCP-based IP phone registered to Unified CM

As a general rule, Early Offer calls of this type that use MTPs support voice only, but they are not limited to a single voice codec (as they are with Early Offer using MTP Required). These calls support only audio in the initial call setup but can be escalated mid-call to support video and SRTP if the call media is renegotiated (for example, after hold or resume).

Note   MTP resources are not required for incoming INVITE messages, whether or not they contain an initial Offer SDP.

Figure 6-13   *Early Offer Support for Voice and Video Calls*

Unified CM does not need to insert an MTP to create an outbound Early Offer call over a SIP trunk if the inbound call to Unified CM is received by any of the following means:

- On a SIP trunk using Early Offer

- On an H.323 trunk using Fast Start

- On an MGCP trunk

- From a SIP-based IP phone registered to Unified CM

- From newer SCCP-based Cisco Unified IP Phone models registered to Unified CM

For the above devices, Unified CM uses the media capabilities of the endpoint and applies the codec filtering rules based on the region-pair of the calling device and outgoing SIP trunk to create the offer SDP for the outbound SIP trunk call. In most cases, the offer SDP will have the IP address and port number of the endpoint initiating the call. This is assuming that Unified CM does not have to insert an MTP for other reasons such as a DTMF mismatch, TRP requirements, or a transcoder requirement when there is no common codec between the regions of the calling device and the SIP trunk.

When **Early Offer support for voice and video calls (insert MTP if needed)** is configured on a trunk's SIP Profile, calls from older SCCP-based phones, SIP Delayed Offer trunks, and H.323 Slow Start trunks will cause Unified CM to allocate an MTP. The MTP is used to generate an offer SDP with a valid media port and IP address. The MTP will be allocated from the media resources associated with the calling

device rather than from the outbound SIP trunk's media resources. (This prevents the media path from being hair-pinned via the outbound SIP trunk's MTP). If the MTP cannot be allocated from the calling device's media resource group list (MRGL), then the MTP allocation is attempted from the SIP trunk's MRGL.

For calls from older SCCP phones registered to Unified CM, some of the media capabilities of the calling device (for example, supported voice codecs, video codecs, and encryption keys if supported) are available for media exchange through the Session Description Protocol (SDP). Unified CM will create a superset of the endpoint and MTP codec capabilities and apply the codec filtering based on the applicable region-pair settings. The outbound Offer SDP will use the MTP's IP address and port number and can support voice, video, and encrypted media. Note that a Cisco IOS-based MTP should be used and configured to support the pass-through codec.

Note   Older SCCP-based IP phones such as the Cisco Unified IP Phone 7902, 7905, 7910, 7912, 7920, 7935, 7940, and 7960 require the use of an MTP when they make calls over a SIP trunk with the **Early Offer for voice and video (insert MTP if needed)** feature enabled. If you have a significant number of these phone types deployed in a cluster, consider deploying Delayed Offer trunks instead of Early Offer trunks. If Early Offer trunks are used, provision MTP resources in the cluster equivalent to the number of busy hour calls over those SIP trunks that use the **Early Offer for voice and video (insert MTP if needed)** feature.

When Unified CM receives an inbound call on an H.323 Slow Start or SIP Delayed Offer trunk, the media capabilities of the calling device are not available when the call is initiated. In this case, Unified CM must insert an MTP and will use its IP address and UDP port number to advertise all supported audio codecs (after region pair filtering) in the Offer SDP of the initial INVITE sent over the outbound SIP trunk. When the Answer SDP is received on the SIP trunk, if it contains a codec that is supported by the calling endpoint, then no additional offer-answer transaction is needed. In case of codec mismatch, Unified CM can either insert a transcoder to address the mismatch or send a Re-INVITE or UPDATE to trigger media negotiation. Calls from H.323 Slow Start or SIP Delayed Offer trunks support only audio in the initial call setup, but they can be escalated mid-call to support video and SRTP if the call media is renegotiated (for example, after Hold or Resume).

MTP-Less Early Offer

MTP-Less Early Offer is a special case configuration for Unified CM Session Manager Edition (SME) SIP trunks. For SME deployments using SIP trunks only, MTP-Less Early Offer allows you to deploy an SME cluster that is media transparent (no media resources are required in the SME cluster) because all media negotiation takes place in the leaf Unified Communications systems, which insert media resources (MTPs, transcoders, and so forth) as required. (See Figure 6-14.)

MTP-Less Early Offer takes advantage the Unified CM SIP service parameter **Fail Call Over SIP Trunk if MTP Allocation Fails**. The default setting for this service parameter is **False**, thus allowing an inbound Delayed Offer call to proceed over the outbound SIP trunk (configured for Early Offer) as a Delayed Offer call if no MTP resources are available.

Figure 6-14   *MTP-Less Early Offer – SME Media Transparency*
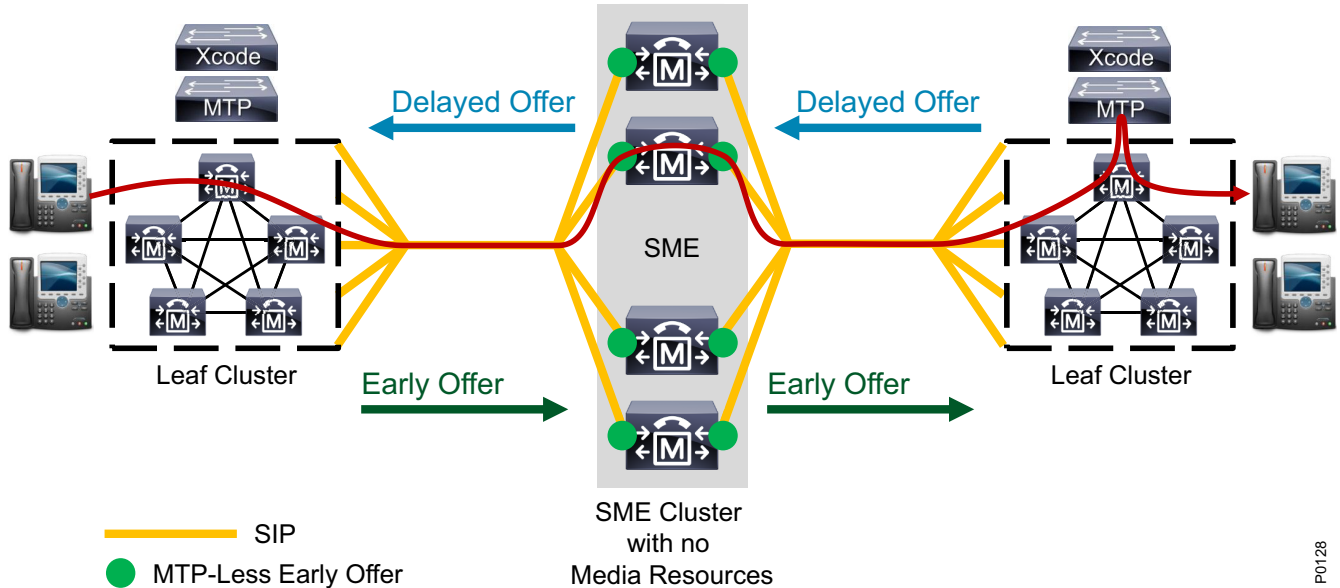
To configure a media-transparent SME cluster:

- Use only SIP trunks on the SME cluster.

- Enable all trunks with **Early Offer support for voice and video calls (insert MTP if needed)**.

- Disable the IPVMS service on all SME nodes. This disables Unified CM media termination points, conferencing, music on hold, and annunciator resources.

- Do not associate any Cisco IOS media resources with the SME cluster.

- Configure SIP trunk DTMF settings to **No Preference** (the default setting).

- Enable **Accept Audio Codec Preference in Received Offer** on all SME SIP trunks.

Media Termination Points

MTPs are used by Unified CM for the following purposes:

o To deliver a SIP Early Offer over SIP trunks

o To address DTMF transport mismatches

o To act as an RSVP agent

o To act as a Trusted Relay Point (TRP)

o To provide conversion between IPv4 and IPv6 for RTP streams

MTPs are available in three forms:

- Software MTPs in Cisco IOS gateways — Available with any Cisco IOS T-train software release and scaling up to 5,000 sessions (calls) on the Cisco Aggregation Services Routers (ASR) 1000 Series with Route Processor RP2.

- Hardware MTPs in Cisco IOS gateways — Available with any Cisco IOS T-train software release, hardware MTPs use on-board DSP resources and scale calls according to the number of DSPs supported on the Cisco router platform.

- Cisco Unified CM software MTPs using the Cisco IP Voice Media Streaming Application on a Unified CM subscriber node

Cisco IOS MTPs are recommended over Unified CM MTPs because Cisco IOS MTPs provide additional scalability and greater functionality, such as support for additional codec types, multiple media streams, and the pass-through codec. (For details, see the section on Media Termination Point (MTP), page 7-8.)

The following example configuration is for a Cisco IOS software MTP:

```
!
sccp local Vlan5
sccp ccm 10.10.5.1 identifier 5 version 8.6.2
! Communications Manager IP address (10.10.5.1)
sccp
!
sccp ccm group 5
 bind interface Vlan5
 associate ccm 5 priority 1
 associate profile 5 register MTP000E83783C50
! MTP name (MTP000E83783C50) ... must match the Unified CM MTP name.
!
dspfarm profile 5 mtp
 description software MTP
 codec g711ulaw
 codec pass-through
 maximum sessions software 500
 associate application SCCP
```

DTMF Transport over SIP Trunks

There are several methods of transporting DTMF information between SIP endpoints. In general terms, these methods can be classified as out-of-band and in-band signalling. In-band DTMF transport methods send either raw or signalled DTMF tones within the RTP stream, and they need to be handled and interpreted by the endpoints that generate and/or receive them. Out-of-band signalling methods transport DTMF tones outside of the RTP path, either directly to and from the endpoints or through a call agent such as Cisco Unified CM, which interprets and/or forwards these tones as required.

Out-of-band (OOB) SIP DTMF signalling methods include Unsolicited Notify (UN), Information (INFO), and Key Press Mark-up Language (KPML). KPML (RFC 4730) is the OOB signalling method preferred by Cisco and is supported by Cisco Unified CM, Cisco IOS platforms (Release 12.4 and later), and most models of Cisco Unified IP Phones. INFO is not supported by Unified CM.

In-band DTMF transport methods send DTMF tones as either raw tones in the RTP media stream or as signalled tones in the RTP payload using RFC 2833. Among SIP product vendors, RFC 2833 has become the predominant method of sending and receiving DTMF tones and is supported by the majority of Cisco voice products.

Because in-band signalling methods send DTMF tones in the RTP media stream, the SIP endpoints in a session must either support the transport method used (for example, RFC 2833) or provide a method of intercepting this in-band signalling and converting it. If the two endpoints are using a back-to-back user agent (B2BUA) server for the call control (for example, Cisco Unified CM) and the endpoints negotiate different DTMF methods between each device and call control box, then the call agent determines how to handle the DTMF differences, either through MTP insertion or by OOB methods. With Unified CM, a DTMF transport mismatch (for example, in-band to out-of-band DTMF) is resolved by inserting a media termination point (MTP), which terminates the RTP stream with in-band DTMF signalling (RFC 2833), extracts the DTMF tones from the RTP stream, and forwards these tones out-of-band to Unified CM, where they are then forwarded to the endpoint supporting out-of-band signalling. For DTMF mismatches, the inserted MTP is always in the media path between the two endpoints. In-band DTMF packets are identified by their RTP Payload type, extracted by Unified CM, and converted to out-of-band DTMF, while RTP media packets pass transparently through the MTP.

In-band DTMF tones can also be transported as raw (audible) tones in the RTP media stream. This transport method is not widely supported by Cisco products and, in general, is not recommended as an end-to-end DTMF transport mechanism. In-band audio DTMF tones can generally be reproduced reliably only when using G.711 a-law or mu-law codecs, and they are not suitable for use with low-bandwidth codecs. In cases where in-band audio is the only available DTMF transport mechanism, the Cisco Unified Border Element can be used to translate the in-band audio DTMF signalling into RFC 2833 signalling.

Three DTMF options are available on Unified CM SIP trunks:

- DTMF Signalling Method: No Preference

  In this mode, Unified CM attempts to minimize the usage of MTP resources by selecting the most appropriate DTMF signalling method for the call.

  If both endpoints support RFC 2833 in-band DTMF, then no MTP is required.

  If both devices support any out-of-band DTMF mechanism, then Unified CM uses KPML or Unsolicited Notify over the SIP trunk.

  The only case where an MTP is required is when one of the endpoints supports only out-of-band DTMF and the other supports only RFC 2833 in-band DTMF.

  The majority of Cisco Collaboration System endpoints support both in-band and out-of-band DTMF.

- DTMF Signalling Method: RFC 2833

  By placing a restriction on the DTMF signalling method across the trunk, Unified CM is forced to allocate an MTP if any one or both of the endpoints do not support RFC 2833 in-band DTMF. In this configuration, the only time an MTP will not be allocated is when both endpoints support RFC 2833 in-band DTMF.

- DTMF Signalling Method: OOB and RFC 2833

  In this mode, the SIP trunk signals both out-of-band (OOB) DTMF (KPML or Unsolicited Notify) and RFC 2833 in-band DTMF across the trunk, and it is the most intensive MTP usage mode. The only cases where MTP resources will not be required is when both endpoints support both RFC 2833 in-band DTMF and out-of-band DTMF.

Cisco recommends configuring the DTMF Signalling Method to **No Preference** on Unified CM SIP trunks. This setting allows Unified CM to make an optimal decision for DTMF and to minimize MTP allocation.
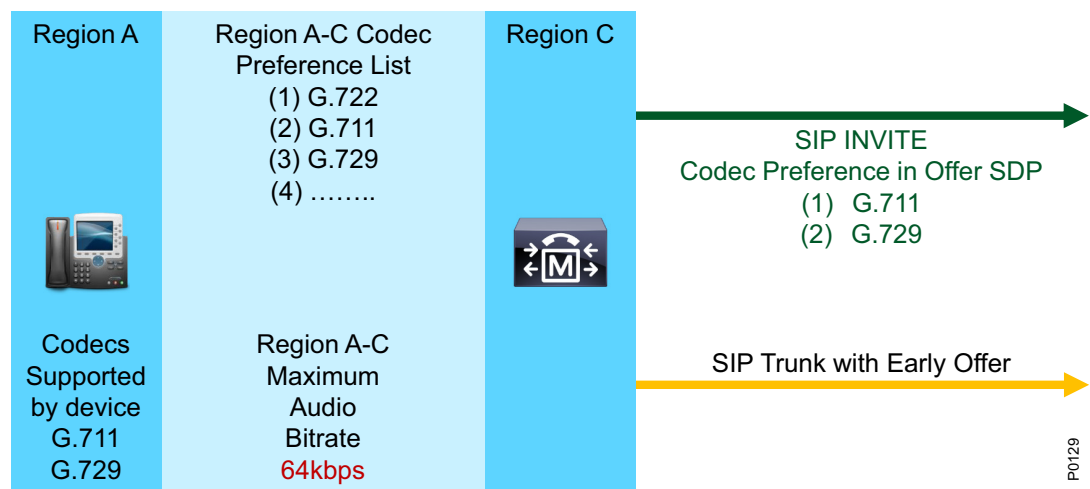
Codec Selection over SIP Trunks

Before media can be established between communicating entities, both the entities must agree on the codec(s) that they want to use. This codec (or codecs, if both audio and video are involved) is derived from the intersection of codecs supported by communicating entities involved and the configured policy in Unified CM, configured by *region* settings.

The region settings in Unified CM provide for configurable audio codec preference lists. In addition to the default Lossy and Low Loss audio codec preference lists that can be selected via a region's Link Loss Type, multiple custom audio codec preference lists can also be created. Audio codec preference lists can be used for codec selection for calls within a region and between regions. The Maximum Audio Bit Rate is still applied for calls within a region and between regions; but rather that using the highest audio quality codec (as in earlier Unified CM releases) based on the maximum bit rate setting, the codec selection is made based on the codec order in the audio codec preference list and the codecs that the endpoints support. (See Figure 6-15 and Figure 6-16.)

An Audio Codec Preference List is a list of all the codec types supported by Unified CM. The preference order of this list of codecs can be modified and saved as a custom preference list. (Note that codecs cannot be removed from the Audio Codec Preference List). The list of codecs used for codec negotiation during call setup is the subset of codecs supported by the device and those in the codec preference list, limited by the maximum audio bit rate for the region or region pair.

Figure 6-15 and Figure 6-16 show examples of how codecs are selected for codec negotiation during call setup.

Figure 6-15   *Codec Selection with Maximum Audio Codec Bit Rate of 64 kbps*

Figure 6-16   Codec Selection with Maximum Audio Codec Bit Rate of 48 kbps
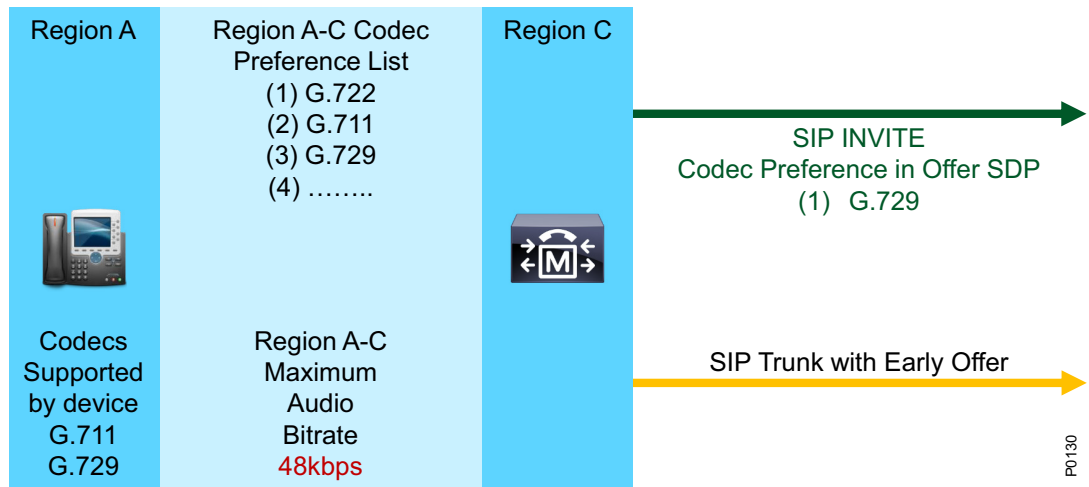
For calls between two Unified CM clusters over SIP intercluster trunks, audio codec preference lists allow the codec to be selected for a call based upon the codec preferences of the calling and called devices. By grouping devices in each cluster into regions based on their codec preferences, a single intercluster trunk can be used to support multiple calls, with each call type using its preferred codec. (See Figure 6-17.)

Figure 6-17   Audio Codec Preference Lists for Voice and Fax Calls Between Two Unified CM Clusters
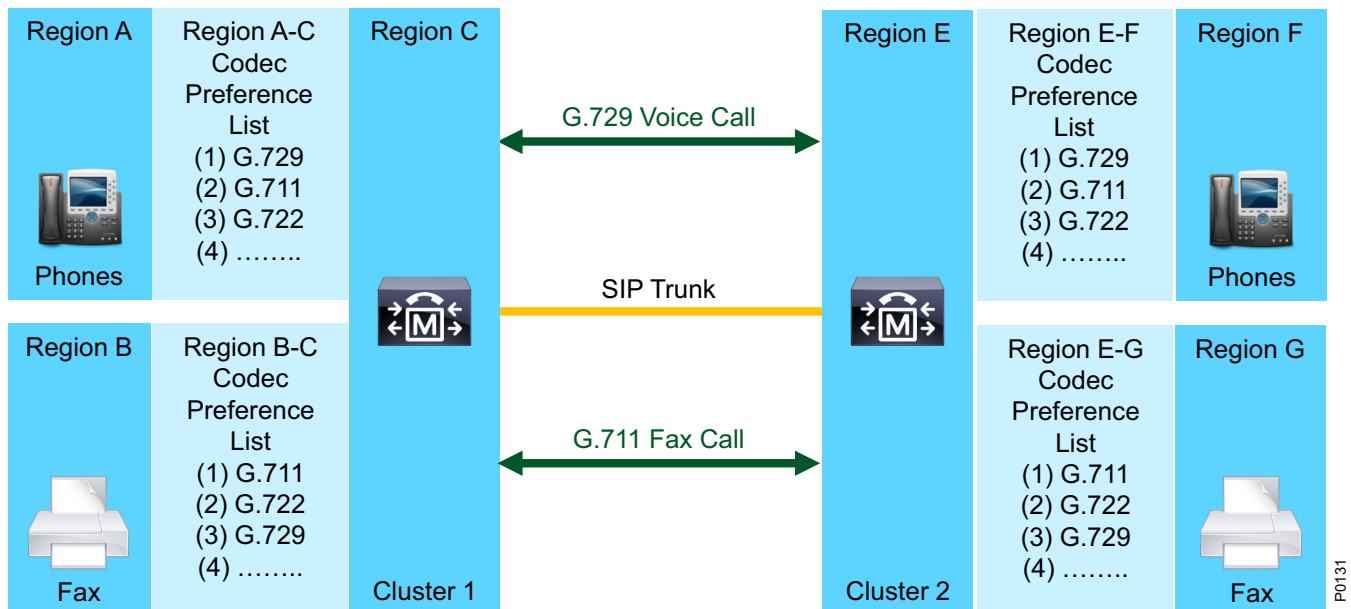
> **Note** Configure equivalent inter-region audio codec preference lists for each device type in each cluster to ensure that a common codec is selected for each device type, irrespective of call direction or trunk configuration. If the audio codec preference lists in each cluster are not equivalent, the codecs used per call can vary based on call direction and trunk configuration. (Ordinarily, the codec preference order is not honoured by the cluster receiving the codec preference list.)

> **Note** Do not use SIP trunks configured for Early Offer with **MTP Required** enabled if codec preference is required. This trunk configuration inserts an MTP for inbound and outbound calls, which is limited to a single audio codec only, thereby overriding codec preference and selection.

Accept Audio Codec Preferences in Received Offer

In deployments where calls can pass through more than one Unified CM cluster (for example, SME deployments), the inter-region audio codec preference list of the intermediary Unified CM (SME) cluster can override the preferred codec selection between the calling and called devices. To ensure that the endpoints' codec preferences are honoured as calls pass through SME, enable the SIP Profile feature **Accept Audio Codec Preferences in Received Offer** on all SME SIP trunks. (See Figure 6-18.)

Figure 6-18   ***SME Deployment Using "Accept Audio Codec Preferences in Received Offer" on SIP Trunks***
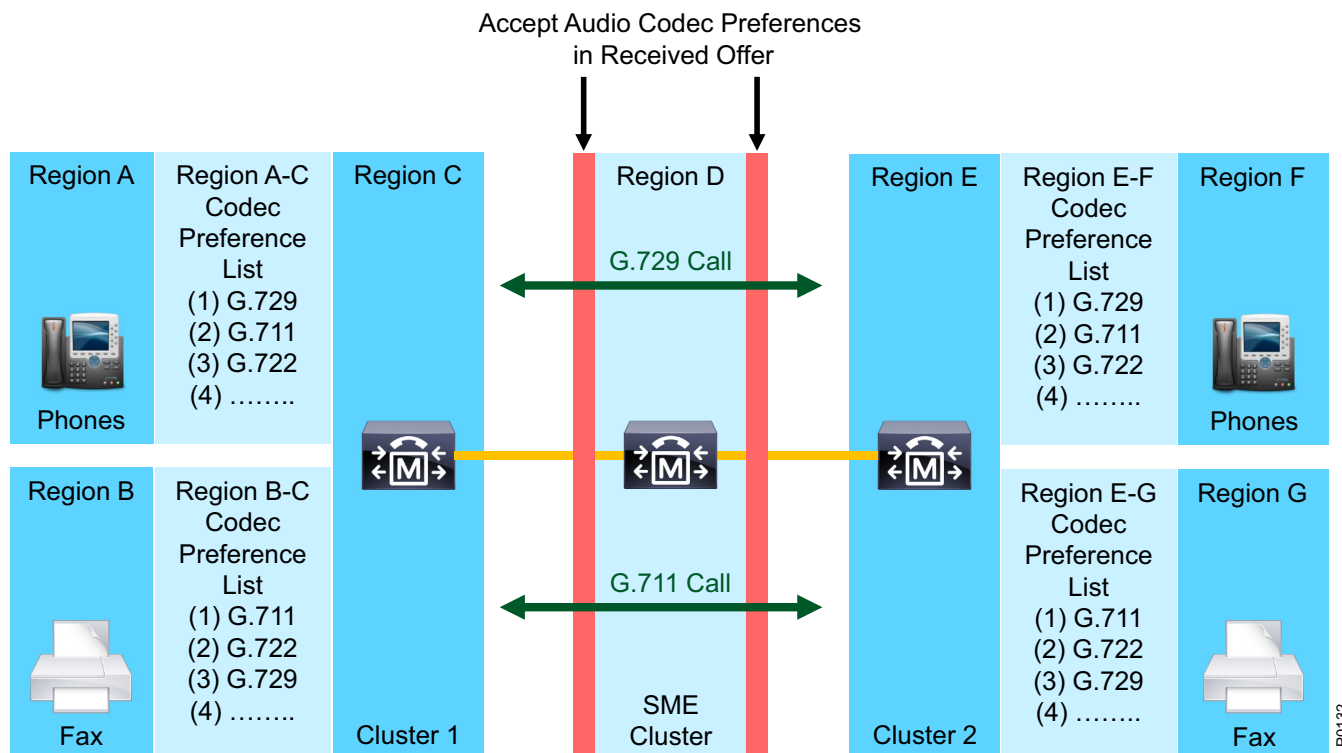
Note   The **Accept Audio Codec Preferences in Received Offer** feature is available only on SIP trunks (a SIP Profile feature). This feature does not offer consistent results if used in an SME deployment where the SME cluster uses a combination of SIP, H.323, and/or MGCP trunks. Therefore, the **Accept Audio Codec Preferences in Received Offe**r feature should be used when the SME cluster is deployed using only SIP trunks.


Cisco Unified CM and Cisco Unified Border Element SIP Trunk Codec Preference

Unified CM audio codec preference lists can be used in Unified Communications deployments with Cisco Unified Border Element to simplify configuration of SIP trunks between Unified CM and Unified Border Element. For example, instead of using dedicated SIP trunks to the Unified Border Element for voice and fax calls, a single Unified CM SIP trunk can be used where the codec preference for each device type is honored as calls pass through the Unified Border Element.

In Figure 6-19 the Voice Class Codec Preference lists defined on Cisco Unified Border Element's inbound and outbound dial peers do not change the preference of the listed codecs in the received Offer. Cisco Unified Border Element does codec filtering on the received Offer, both on the inbound and outbound dial-peer, and passes across the common codecs in the same preference order as received in the inbound Offer to the peer leg.

If codecs, in addition to those received in an Offer, are defined in the voice class codec list, then these codecs will be appended to those received in the ordered list and sent out in the outbound Offer.

Thus, a single inbound and outbound dial-peer can be configured on Cisco Unified Border Element for all device types. Cisco recommends using the same voice class codec preference list for both the inbound and outbound dial-peer, with that list containing the codecs that you want to negotiate with the service provider. As mentioned above, the order of the codecs will be dictated first by the order received in the inbound Offer and then by the order defined in the voice class codec preference list.

Figure 6-19   ***Cisco Unified CM and Cisco Unified Border Element SIP Trunk Codec Preference***
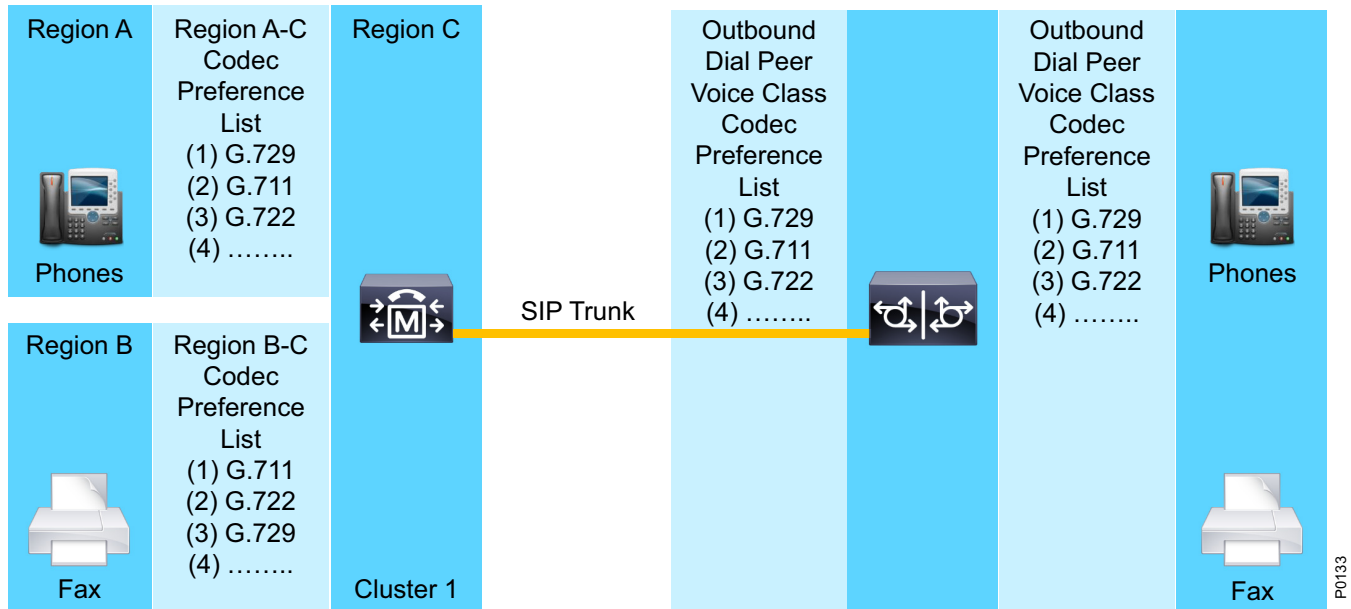
SIP Trunk Transport Protocols

SIP trunks can use TCP, TLS (which runs over TCP), or UDP as a message transport protocol. Unified CM provides a native interworking function for SIP trunks using different transport protocols. TCP is recommended within Cisco Collaboration Systems networks because it is a reliable and connection-orientated protocol with the capability to fragment and re-assemble large SIP messages. UDP is not connection-orientated or reliable (message delivery is not guaranteed), and it relies on the SIP Invite Retry count and SIP Trying timers to detect and respond to far-end device failures. Cisco recommends using SIP OPTIONS Ping to dynamically track the state of each destination IP address on each SIP trunk and the collective state of the trunk as a whole.

For more information on SIP trunk timer tuning, refer to the configuration example and technical notes at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a008082d76a.shtml

Note   Although TCP is the recommended transport protocol within a Cisco Collaboration Systems network, most service providers prefer to use UDP because it has a lower processing overhead than TCP. Cisco Unified Border Element can be used to provide TCP-based SIP trunk connections to the Cisco Collaboration Systems network and UDP-based SIP trunk connections to service provider networks.

Secure SIP Trunks

Securing SIP trunks involves two processes:

- Configuring the trunk to encrypt media (see Media Encryption, page 6-30)
- Configuring the trunk to encrypt signalling (see Signalling Encryption, page 6-30)

Media Encryption

Media encryption can be configured on SIP trunks by checking the trunk's **SRTP allowed** check box. It is important to understand that enabling **SRTP allowed** causes the media for calls to be encrypted, but the trunk signalling will not be encrypted and therefore the session keys used to establish the secure media stream will be sent unencrypted. It is therefore important that you ensure that signalling between Unified CM and its destination SIP trunk device is also encrypted so that keys and other security-related information do not get exposed during call negotiations.

Signalling Encryption

SIP trunks use TLS for signalling encryption. TLS is configured on the SIP Security Profile associated with the SIP trunk, and it uses X.509 certificate exchanges to authenticate trunk devices and to enable signalling encryption.

Certificates can be either of the following:

- Imported to each Unified CM node from every device that wishes to establish a TLS connection to that node's SIP trunk daemon
- Signed by a Certificate Authority (CA), in which case there is no need to import the certificates of the remote devices; only the CA certificate needs to be imported

Unified CM provides a bulk certificate import and export facility. However, for SIP trunks using **Run on all Active Unified CM Nodes** and up to 16 destination addresses, using a Certificate Authority provides a centralized and less administratively burdensome approach to setting up signalling encryption on SIP trunks.

For more information on TLS for SIP trunks, refer to the latest version of the *Cisco Unified Communications Manager Security Guide*, available at

> http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

For information on certificate authorities, refer to the Certificate Authority (CA) information in the latest version of the *Cisco Unified Communications Operating System Administration Guide*, available at

> http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

If the system can establish a secure media or signalling path and if the end devices support SRTP, the system uses an SRTP connection. If the system cannot establish a secure media or signalling path, or if at least one device does not support SRTP, the system uses an RTP connection. SRTP-to-RTP fall-back (and vice versa) may occur for transfers from a secure device to a non-secure device or for conferencing, transcoding, music on hold, and so on.

For SRTP-configured devices, Unified CM classifies a call as encrypted if the **SRTP Allowed** check box is checked for the device and if the SRTP capabilities for the devices are successfully negotiated for the call. If these criteria are not met, Unified CM classifies the call as non-secure. If the device is connected to a phone that can display security icons, the phone displays the lock icon when the call is encrypted.

> **Note** MTPs that are statically assigned to a SIP trunk by means of the **MTP Required** checkbox do not support SRTP because they do not support the pass-through codec.

To ensure that SRTP is supported for all calls, configure the SIP trunk for Delayed Offer.

Where **Early Offer support for voice and video calls (insert MTP if needed)** is configured for devices that support encryption, all calls that do not need to use MTPs can support SRTP. When an MTP is inserted into the call path, this dynamically inserted MTP supports the pass-through codec, and encrypted calls are supported in the following cases:

- If the calling device is an older SCCP-based phone registered to Unified CM, SRTP can be negotiated in the initial call setup.

- If the call arrives inbound to Unified CM on a Delayed Offer SIP trunk or an H.323 Slow Start trunk, SRTP will not be negotiated in the initial call setup because no security keys are available, but the call can be escalated mid-call to support SRTP if the call media is renegotiated (for example, after hold or resume).

If Unified CM dynamically inserts an MTP for reasons other than Early Offer, such as for a Trusted Relay Point or as an RSVP agent, then SRTP will be supported with an MTP that supports the pass-through codec (Cisco IOS MTPs).

> **Note** In-band to out-of-band DTMF conversion using MTPs does not function for SRTP encrypted media streams because the MTP is unable to decrypt the DTMF packets.

User Identity and SIP Trunks

A calling user's name and number can be sent over Unified CM SIP trunks in the following SIP message headers:

Message Header	Examples
From:	From: "Jim Bob" <sip:1000@10.10.199.250>
	From: "Anonymous" <sip:localhost>
To:	To: "Nick Cave" <sip:2000@10.10.100.251>
P-Asserted-Identity:	P-Asserted-Identity: "Jim Bob" <sip:1000@10.10.199.250>
Remote-Party-ID:	Remote-Party-ID: "Jim Bob" <sip:1000@10.10.199.250>

The From and To message headers sent in SIP Requests and Responses indicate the direction of the call. (The From header represents the calling user and the To header represents the called user.) The From and To headers remain the same in all SIP Requests and Responses for the call.

SIP allows the From header to be made anonymous so that the calling user information is not presented to the called user.

The P-Asserted-Identity and Remote-Party-ID headers (if present) always contain the user's identity. The user information contained in SIP messages with these identity headers is directional, so that the headers contain the calling user's identity in an Initial INVITE and the called user's identity in Responses. The P-Asserted-Identity and Remote-Party-ID headers can be used to trace the identity of an anonymous call.

By default, both the P-Asserted-Identity and Remote-Party-ID headers are sent over Unified CM SIP trunks, but they can be disabled. The usage of P-Asserted-Identity and Remote-Party-ID headers will depend upon the device that the Unified CM SIP trunk is connected to. P-Asserted-Identity is a more recent standard and more commonly used than Remote-Party-ID. The P-Asserted-Identity standard (RFC 3325) is considered to be more secure than Remote-Party-ID because it supports authentication between untrusted SIP Realms. For SIP trunk connections to untrusted networks, configure Unified CM to send a P-Preferred-Identity header instead of a P-Asserted-Identity header. Unified CM will respond to a Digest authentication challenge for the sent the P-Preferred-Identity header.

Caller ID Presentation and Restriction

As discussed above the calling user's name and number can be anonymized in the From header in SIP messages sent over a SIP trunk. Calling name and number presentation and restriction can be enabled in three ways:

- By configuring calling name and calling number presentation or restriction in a translation pattern associated with the calling device

- By configuring calling name and calling number presentation or restriction on the Unified CM trunk

- By configuring the P-Asserted-Identity related, SIP Privacy value on the Unified CM SIP trunk

These caller ID presentation and restriction configuration options operate in the following precedence order (highest precedence first):

1. SIP Privacy value

2. Trunk configuration

3. Device configuration

Called and Calling Party Number Normalization and SIP Trunks

As calls traverse the edge between the public PTSN or IP PTSN and the private enterprise network, the called and calling party numbers sent in call setup messages should ideally be normalized to a globally routable international format such as +E.164. How and where these numbers are normalized depends upon the type of PSTN network to which your enterprise is connected:

ISDN and Q.931 PSTN Networks

Calls within ISDN and Q.931 PSTN networks provide additional information in the Number Type fields of call setup messages to classify called and calling numbers. Number-types can be one of four types: Unknown, Subscriber, National, or International. For calls from the PSTN to the enterprise network, the number-type parameter can be used by the enterprise to globalize the calling number to its +E.164 value by prefixing it with the appropriate digits. Using a globalized PSTN calling number within the enterprise allows calls to be returned to the PSTN caller with little or no additional digit manipulation. Depending on the number format sent by the service provider, the enterprise called number might also have to be modified to match that of the enterprise dial plan. Cisco recommends deploying a +E.164 dial plan within the enterprise.

For more details and examples on how these number-types are used and dial plan recommendations, refer to the chapter on .

SIP-Based IP PSTN Networks

Calls from SIP-based IP PSTN networks do not include number type information in SIP messages. In this case, the IP PSTN service provider should present the PSTN calling number using a globally routable international representation (for example, a +E.164 number). Depending on the number format sent by the service provider, the enterprise called number might have to be modified to match that of the enterprise dial plan. Cisco recommends deploying a +E.164 dial plan within the enterprise.

If the service provider sends the PSTN calling number in +E.164 format and the called number in a format that matches that used by the enterprise dial plan (+E.164 recommended), then little or no changes need to be made to these numbers within the enterprise.

The inability of SIP to transport the number type implies that the normalization of the calling number must be performed before the call is presented to Unified CM's call routing process. One place where the transformation can be performed is on the ingress SIP gateway. The following example configuration shows the translation rules that can be defined on a Cisco IOS gateway to accomplish this transformation:

```
voice translation-rule 1
 rule 1 // /+4940/ type subscriber subscriber
 rule 2 // /+49/ type national national
 rule 3 // /+/ type international international
...
voice translation-profile 1
 translate calling 1
...
dial-peer voice 300 voip
 translation-profile outgoing 1
 destination-pattern .T
 session protocol sipv2
 session target ipv4:9.6.3.12
...
```

When configured as in the example above, a Cisco IOS gateway using SIP to communicate with Unified CM will send calling party information digits normalized to the E.164 format, including the + sign. The Unified CM configuration will receive all calls from this gateway with a numbering type of "unknown" and will not need to add any prefixes.

For more details on configuring translation rules, refer to the *Voice Translation Rules* document, available at

http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml

Unified CM can set the calling party number of outgoing calls to the normalized global format. The number-type in outgoing calls from the SIP trunk will be "unknown," and the Cisco IOS gateway should change it to International if no stripping is done, or perform a combination of stripping and numbering type change if required by the connected service provider.

Reasons for Using Only SIP Trunks in Cisco Collaboration Systems Deployments

For Cisco Collaboration Systems networks consisting of one or more Unified CM clusters, Unified Communications applications, Session Border Controllers, and gateways, using SIP as the sole interconnecting trunk protocol allows you to build a simplified Collaboration Systems network with a rich set of common features.

When compared to other trunk protocols, SIP trunks today support a number of unique features, such as:

- SIP OPTIONS Ping which tracks the overall operational status of the trunk and the state of each trunk's destination nodes.

- Codec Preference Lists and the ability to accept the codec preferences received in an SDP Offer.

- Support for H.264 video with BFCP-based presentation sharing and Far End Camera Control.

- SIP message normalization and transparency, which provides powerful script-based functionality for SIP trunks that can be used to transparently forward and/or modify SIP messages and message body (SDP) contents as they traverse Unified CM. Normalization and transparency scripts are designed to address SIP interoperability issues, allowing Unified CM to interoperate with SIP-based third-party PBXs, applications, and IP PSTN services.

- Support for IPv4 only, IPv6 only, or Dual Stack (IPv4 and IPv6) ANAT-enabled SIP trunks.

Design and Configuration Recommendations for Using SIP Trunks

When designing and deploying a SIP-based Cisco Collaboration Systems network, Cisco recommends that you use the following SIP trunk features:

Run on All Unified CM Nodes

This feature is supported on SIP trunks and route lists, and it greatly simplifies call routing from and through Unified CM and SME clusters. Cisco highly recommends enabling the **Run on all Unified CM nodes** feature on all SIP trunks and route lists. Call routing is simplified through a combination of the **Run on all Unified CM nodes** and the Route Local features, whereby phone calls over SIP trunks will always originate from the Unified CM node where the phone is registered. Likewise for trunk to trunk calls, the outbound SIP trunk call will always originate from the Unified CM node on which the inbound Trunk call arrived. Enabling **Run on all Unified CM nodes** on all SIP trunks and route lists eliminates the need to set up calls between call processing nodes within the cluster, which can be useful when clustering over the WAN is deployed within a Unified CM or SME cluster.

Up to 16 SIP Trunk Destination IP Addresses

SIP trunks can be configured with up to 16 destination IP addresses, 16 fully qualified domain names, or a single DNS SRV entry. Support for additional destination IP addresses reduces the need to create multiple trunks associated with route lists and route groups for call distribution between two Unified Communications systems, thus simplifying Unified CM trunk design. When IP addresses are used as destinations on a SIP trunk, Unified CM randomly distributes calls across all defined destination IP addresses.

SIP OPTIONS Ping

Enable the SIP OPTIONS Ping feature on the SIP Profile associated with a SIP trunk to dynamically track the state of each the trunk's destinations and the overall state of the trunk.

PRACK

PRACK provides reliability of 1XX responses for interoperability scenarios with the PSTN, and it can also be used to reduce the number of SIP messages that need to be exchanged before setting up two-way media. Enable PRACK through the **SIP Rel1XX Options** parameter on the SIP Profile associated with the trunk.

SIP Trunk DTMF Signalling Method – No Preference

Using **DTMF Signalling Method: No Preference** is recommended on SIP trunks because in this mode Unified CM attempts to minimize the usage of MTP resources by selecting the most appropriate DTMF signalling method (in-band or out-of-band) for the call.

Session Management Edition SIP Trunks – MTP-Less Early Offer

For SME clusters using SIP trunks only, MTP-Less Early Offer allows you to deploy an SME cluster that is media transparent. No media resources are required in the SME cluster because media negotiation takes place in the leaf UC systems, which insert media resources (MTPs, transcoders, and so forth) as required.

To deploy a media-transparent SME cluster:

- Use only SIP trunks on the SME cluster.

- Enable all trunks with **Early Offer support for voice and video calls (insert MTP if needed)**.

- Disable the IPVMS service on all SME nodes. This disables Unified CM media termination points, conferencing, music on hold, and annunciator resources.

- Do not associate any Cisco IOS media resources with the SME cluster.

- Configure SIP trunk DTMF settings to **No Preference** (the default setting)

- Enable **Accept Audio Codec Preference in Received Offer** on all SME SIP trunks.

Unified CM SIP Trunks – Delayed Offer or Early Offer

The decision to use SIP Delayed Offer or Early Offer in Unified CM clusters largely depends on the number of older SCCP-based phones that are registered to the Unified CM cluster.

If the majority of the phones registered to your cluster are newer SCCP or SIP phones, you can use either Delayed Offer or Early Offer, although Early Offer is generally preferred because IP PSTN service providers and some Unified Communications applications will accept only Early Offer SIP trunk calls.

Older SCCP-based IP phones such as the Cisco Unified IP Phone 7902, 7905, 7910, 7912, 7920, 7935, 7940, and 7960 require the use of an MTP when they make calls over a SIP trunk with the **Early Offer support for voice and video (insert MTP if needed)** feature enabled. If you have a large number of these older SCCP-based phones registered in your cluster, a significant number of MTPs will be required if Early Offer is used. In this case, using Delayed Offer is recommended so that no MTPs are needed to generate the SDP Offer or Answer.

In Unified Communications deployments, Early Offer is typically always required by IP PSTN service providers and also by certain other Unified Communications applications. Cisco Unified Border Element provides a SIP Delayed Offer to Early Offer feature for voice calls, which converts inbound Delayed Offer voice calls to outbound Early Offer voice calls, thus allowing Unified CM and SME to use Delayed Offer trunks rather than Early Offer SIP trunks and MTPs. For Unified Communications applications that accept only SIP Early Offer, if the peak call volume is low and a dedicated SIP trunk from Unified CM to the application is used, it might be more economical to use MTPs in conjunction with the **Early Offer support for voice and video (insert MTP if needed)** feature instead of Cisco Unified Border Element.

Unified CM Session Management Edition

Cisco Unified Communications Manager Session Management Edition (Unified CM SME) is the recommended trunk and dial plan aggregation platform in multi-site distributed call processing deployments. SME is essentially a Unified CM cluster with trunk interfaces only and no IP endpoints. It enables aggregation of multiple unified communications systems, referred to as leaf systems. (See Figure 6-20.)

SIP trunks are highly recommended for SME and Leaf Unified Communications systems because SIP offers additional features and functionality not available in H.323 and MGCP trunks. As discussed later in this section, there are certain trunk features that are exclusive to SME designs that use SIP trunks only. If your Unified Communications network must support H.323 or MGCP trunk connections to gateways or other Unified Communications applications, to preserve the SIP-only trunk features in your SME cluster, connect these H.323 and/or MGCP trunks to leaf Unified Communications systems instead of SME.

Cisco Unified CM Session Management Edition (SME) supports the following call types:

- Voice calls
- Video calls
- Encrypted calls
- Fax calls

Unified CM Session Management Edition may also be used to connect to the PSTN and third-party unified communications systems such as PBXs and centralized unified communications applications.

Figure 6-20   Multisite Distributed Call Processing Deployment with Unified CM Session Management Edition
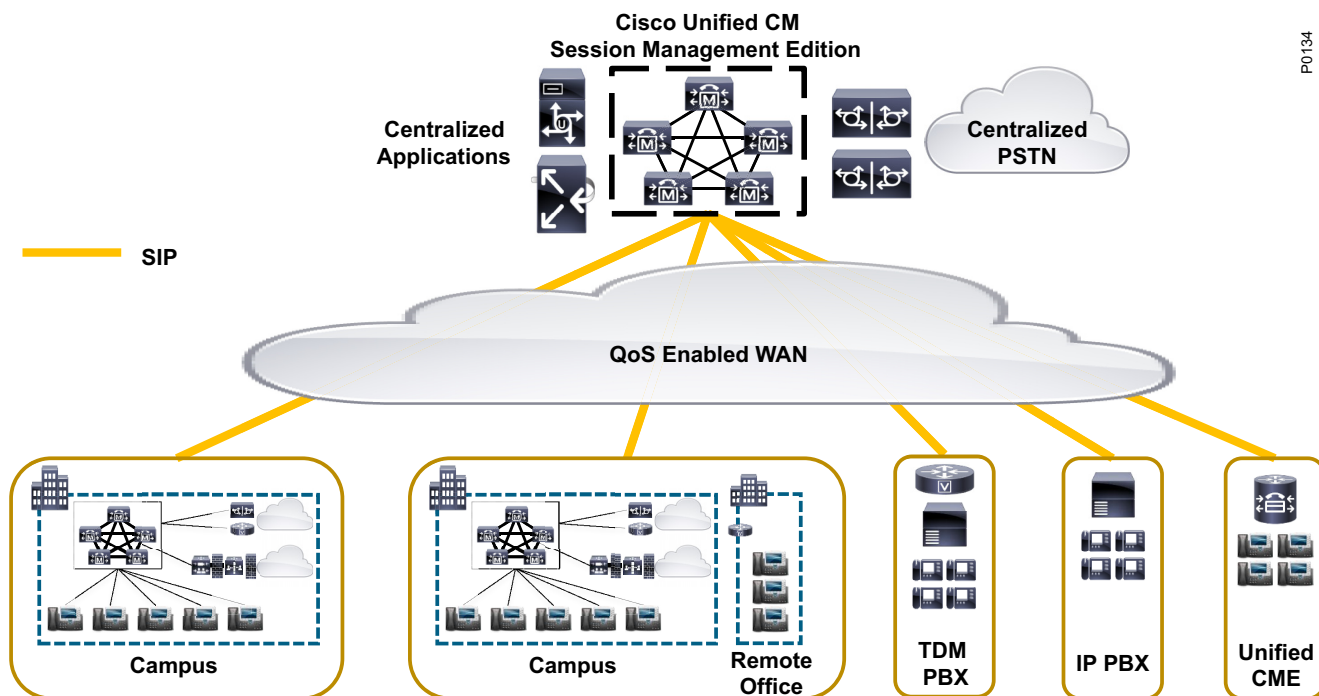
When to Deploy Unified CM Session Management Edition

Cisco recommends deploying Unified CM Session Management Edition if you want to do any of the following:

- Create and manage a centralized dial plan

  Rather than configuring each unified communications system with a separate dial plan and trunks to connect to all the other unified communications systems, Unified CM Session Management Edition allows you to configure the leaf unified communications systems with a simplified dial plan and trunk(s) pointing to the SME cluster. Unified CM Session Management Edition holds the centralized dial plan and corresponding reachability information about all the other unified communications systems.

  > ✎
  >
  > **Note**   Running ILS GDPR on SME and Unified CM leaf clusters further simplifies dial plan administration because individual directory numbers, E.164 numbers corresponding to DNs, route patterns (for internal and external number ranges), and URIs can be distributed using the ILS service. This approach simplifies dial plan administration by reducing the required number of route patterns to one SIP route pattern per call control system (Unified CM cluster, for example), instead of a route pattern for each unique number range. For more information on ILS and GDPR, see Intercluster Lookup Service (ILS) and Global Dial Plan Replication (GDPR), page 10-29.

- Provide centralized PSTN access

  Unified CM Session Management Edition can be used to aggregate PSTN access to one (or more) centralized PSTN trunks. Centralized PSTN access is commonly combined with the reduction or elimination of branch-based PSTN circuits.

- Centralize applications

  The deployment of Unified CM Session Management Edition enables commonly used applications such as conferencing or voice mail to connect directly to the SME cluster, thus reducing the overhead of managing multiple trunks to leaf systems.

- Aggregate PBXs for migration to a Unified Communications system

  Unified CM Session Management Edition can provide an aggregation point for multiple PBXs as part of the migration from legacy PBXs to a Cisco Unified Communications System. If ILS GDPR is deployed, the number ranges and/or URIs supported by each third party system can also be imported into ILS GDPR and reached by means of a SIP route pattern and corresponding SIP trunk.

Differences Between Unified CM Session Management Edition and Standard Unified CM Clusters

The Unified CM Session Management Edition software is exactly the same as Unified CM. However, Unified CM software has been enhanced to satisfy the requirements of this new deployment model. Unified CM Session Management Edition is designed to support a large number of trunk-to-trunk connections, and as such it is subject to the following design considerations:

Capacity and Sizing

It is important to size the Unified CM Session Management cluster correctly based on the expected BHCA traffic load between leaf Unified Communications systems (for example, between Unified CM clusters and PBXs), to and from any centralized PSTN connections, and to any centralized applications. Determine the average BHCA and call holding time for users of your Unified Communications system, and share this information with your Cisco account Systems Engineer (SE) or Cisco Partner to size your Unified CM Session Management Edition cluster correctly. For more information on SME sizing, see the chapter on Collaboration Solutions Design and Deployment Sizing Considerations, page 27-1.

SME Trunks

Although SME supports SIP, H.323, and MGCP trunks, Cisco highly recommends SIP as the trunk protocol of choice for SME and Unified CM leaf clusters running Cisco Unified Communications System Release 8.5 and later versions.

Using only SIP trunks in the SME cluster allows you deploy a "media transparent" cluster where media resources (when required) are inserted by the end or leaf Unified Communications system and never by SME. Using only SIP trunks also allows you use extended round-trip times (RTTs) between SME nodes when clustering over the WAN.

SME SIP trunks should be configured as **MTP-less Early Offer** trunks. Leaf Unified CM clusters can be configured as SIP Delayed Offer or SIP **Early Offer for Voice and Video (insert MTP if needed)**.

SME Transparency for Media Negotiation

When a media resource such as an MTP or transcoder is needed to allow a call to proceed successfully, these resources should be allocated by the leaf Unified Communications systems. If SME trunk media resources are deployed and used for a call traversing the SME cluster, the media path call will hairpin through the SME media resource. By using SIP trunks only and **MTP-less Early Offer**, an SME cluster can be deployed without media resources. If or when media resources are required, they can be provided by the leaf Unified Communications system.

Clustering over the WAN with SME CoW+

With Cisco Unified CM 9.1 and later releases, SME deployments support round-trip times (RTTs) of up to 500 ms between SME cluster nodes. (See Figure 6-21.) This extended RTT applies only to SME clusters (80 ms is the maximum RTT for standard Unified CM cluster designs) and is subject to the following design restrictions:

- SME deployments with extended clustering over the WAN (CoW+) round-trip times are supported with SIP trunks only. All SIP trunks must be configured as **MTP-less Early Offer** and must use the **Run on all Unified CM Nodes** feature so that calls are not routed between nodes within the SME cluster. H.323, MGCP, and SCCP protocols are not supported for SME deployments with extended clustering over the WAN round-trip times.

- No endpoints or CTI devices are configured or registered to the SME cluster.

- No media resources such as MTPs, trusted relay points (TRPs), RSVP agents, or transcoders are configured or registered to the SME cluster. (To disable media resources hosted on Unified CM nodes, deactivate the IPVMS service on each node within the cluster.)

- A minimum of 1.544 Mbps (T1) bandwidth is required for Intra-Cluster Communication Signalling (ICCS) traffic between sites.

- In addition to the bandwidth required for Intra-Cluster Communication Signalling (ICCS) traffic, a minimum of 1.544 Mbps (T1) bandwidth is required for database and other inter-server traffic between the publisher node and every remote subscriber node.

Note   As with all SME designs, your SME design must be reviewed and approved by the Cisco SME Team prior to deployment.

The upgrade process for an SME cluster consists of two key parts:

- Version switch-over — The call processing node is rebooted and initialized with the new software version (this takes approximately 45 minutes per server).

- Database replication — The subscriber's database is synchronized with that of the publisher node.

The time taken to complete this database replication phase depends on the number of subscribers nodes in the cluster and the RTT between the publisher and subscriber nodes. The database replication process has a minimal impact of the subscriber's call processing capability and typically can be run as a background process during normal SME cluster operation. Avoid making changes to the SME cluster configuration during the database replication phase because this increases the time it takes to complete the replication.

For SME clusters deployed with extended RTTs, before upgrading the cluster, run the following administrator-level CLI command on the publisher node:

utils dbreplication setprocess 40

This command improves replication setup performance and reduce database replication times.

Figure 6-21   *Unified CM Session Management Edition – Clustering over the WAN with Extended Round Trip Times*
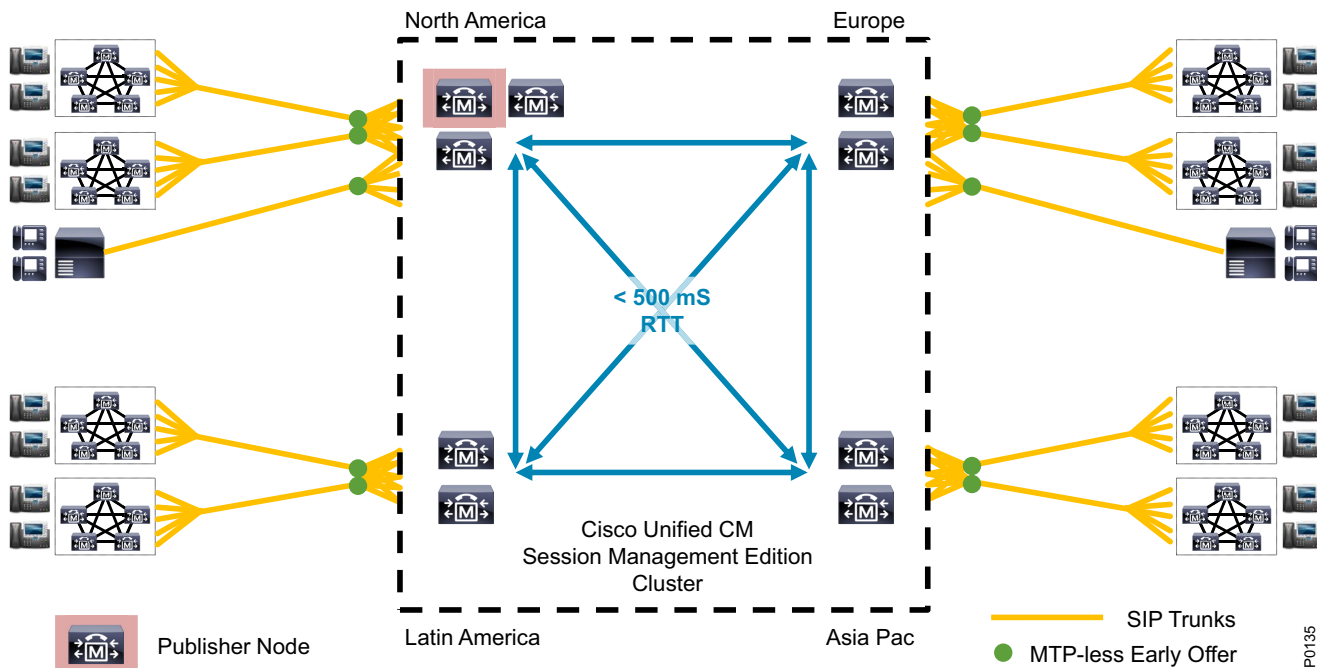
Unified CM Versions

Using the latest Cisco Collaboration Systems Release and SIP trunks across all Unified CM leaf clusters and the SME cluster enables your deployment to benefit from common cross-cluster features such as codec preference lists, ILS, GDPR, and Enhanced Locations call admission control (CAC). If you do not wish to upgrade to the latest Unified CM version on all clusters, the lowest recommended version is Cisco Unified CM 8.5 using SIP trunks because this version includes features that improve and simplify call routing through Unified CM and Session Management Edition clusters.

Summary of SIP Trunk Recommendations for Multi-Cluster SME Deployments

This section provides a summary of the SIP trunk recommendations and operation for multi- cluster deployments with Unified CM Session Management Edition.
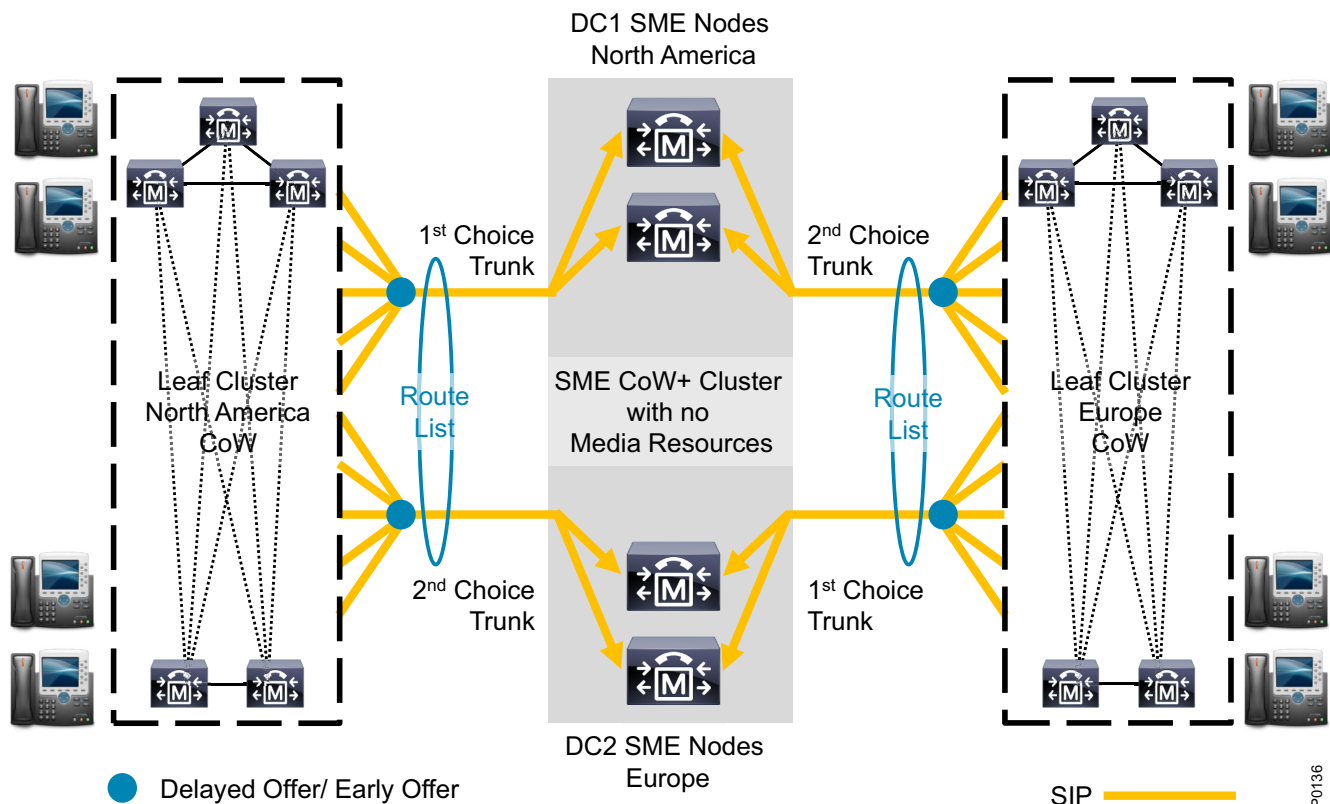
For Unified CM Leaf Clusters:

- Configure one SIP trunk to each set of SME nodes in each regional data center. For example, if there are four regional SME data centers, create four SIP trunks in each leaf cluster (see Figure 6-22). This allows calls from all SME nodes to be received and accepted by the leaf clusters. Enable **Run on all Unified CM nodes** on all of these trunks.

- Place two or more of these leaf cluster SIP trunks into a route list and route groups for path redundancy to the SME CoW+ cluster.

- SIP trunks may use either SIP Early Offer or SIP Delayed Offer.

- Enable the IPVMS service on all leaf cluster nodes. Activate conferencing, music on hold, and annunciator resources as required. (Deactivating IPVMS-based MTPs is recommended.)

- As required, configure and associate Cisco IOS media resources (MTPs, conferencing, and transcoding) with the leaf cluster.
- Configure SIP trunk DTMF settings to **No Preference** (the default setting).
- Enable SIP Options Ping and PRACK.
- If required, configure and apply codec preference lists.

Figure 6-22   Recommended Trunk Configuration for CoW Leaf Cluster Trunks

For Session Management Edition Clusters:

- Use only SIP trunks on the SME cluster.
- Configure one SIP trunk from the SME cluster to each leaf cluster (see Figure 6-23). Enable **Run on all Unified CM nodes** on these trunks, and configure trunk destinations to every call processing node in the leaf clusters.
- Enable all trunks with **Early Offer support for voice and video calls (insert MTP if needed)**.
- Disable the IPVMS service on all SME nodes. This disables Unified CM media termination points, conferencing, music on hold, and annunciator resources.
- Do not associate any Cisco IOS media resources with the SME cluster.
- Configure SIP trunk DTMF settings to **No Preference** (the default setting).
- Enable **Accept Audio Codec Preference in Received Offer** on all SME SIP trunks.
- Enable SIP Options Ping and PRACK.

Figure 6-23   Recommended Trunk Configuration for CoW+ SME Cluster Trunks
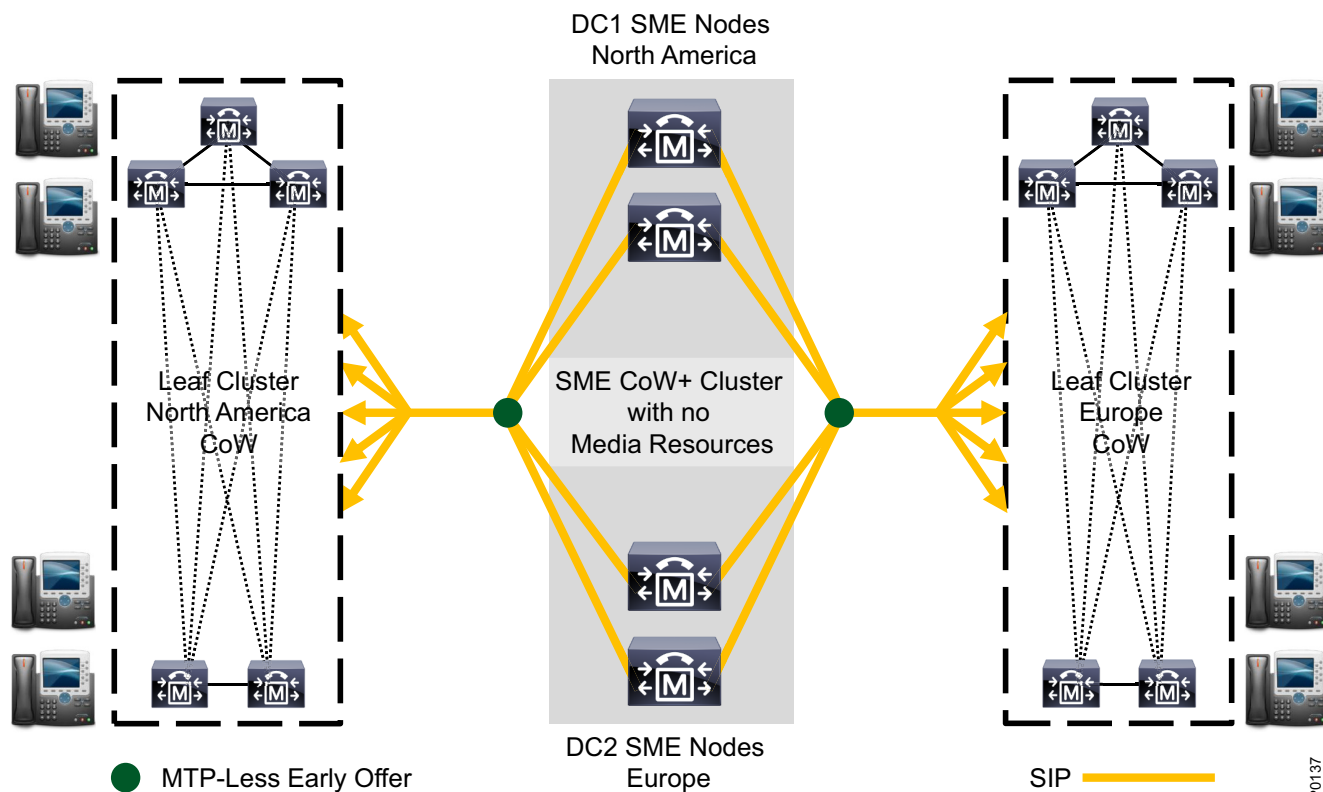

For Call Routing Through Leaf and SME Clusters:

The outbound leaf cluster will originate a SIP trunk call from the same node that the calling device is registered to (using the Route Local rule). The leaf cluster will randomly select a destination address from the SIP trunk route list. (For the example in Figure 6-24, the first-choice trunk is selected.)

Outbound calls from the SME cluster will originate from the same node that the inbound call arrived on (using the Route Local rule). With **Run on all Unified CM nodes** enabled on all SME trunks, calls will never be set up between call processing nodes within the SME cluster. The SME cluster will randomly select a destination address on the SIP trunk pointing toward the destination leaf cluster.

For inbound SIP trunk calls to the destination leaf cluster, calls may be extended from the call processing node on which the inbound call arrived, to the node where the called device is registered.

Media resources, if needed, will be inserted by the leaf clusters. If the calling leaf cluster SIP trunk uses Delayed Offer, the media decision will be made by this cluster, which will insert media resources (MTPs and/or transcoders) as required. If the calling leaf cluster SIP trunk uses Early Offer, the media decision will be made by the destination leaf cluster, which will insert media resources (MTPs and/or transcoders) as required.

Figure 6-24   *Recommended Trunk Configuration for Call Routing Through Leaf and SME Clusters*
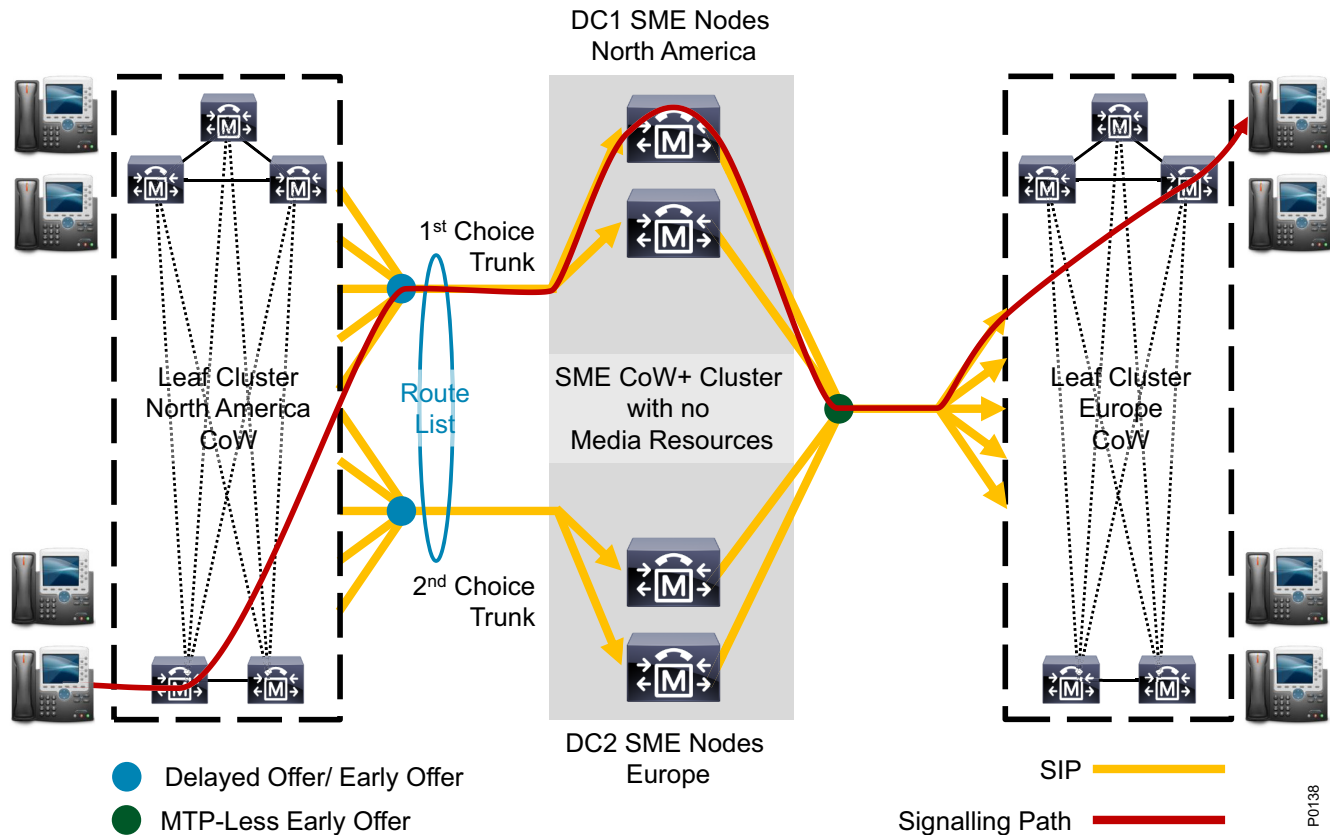
Minor Features of Unified CM SIP Trunks

This section describes the function and usage of several minor features available on Unified CM SIP trunks.

Send sendrecv in Mid-Call INVITE

This feature is used to address interoperability issues with third-party products. When Unified CM places a call hold over a SIP trunk, it sends a mid-call INVITE with audio direction media attribute a=inactive in the SDP body to disconnect the media connection. On call resumption, Unified CM sends a Delayed Offer INVITE (without SDP) to the held device to obtain its media characteristics through an SDP Offer. According to RFC 3261 (section 14.2), the held device should construct the Offer as if it were making a new call; that is, with a list of all supported codecs and a=sendrecv. Some third-party products respond with only the last used codec and media direction attributes, with the result that the call always remains in the inactive state and media cannot be resumed. When **Send "sendrecv" in mid call INVITE** is enabled, this feature inserts an MTP into the media path between the calling and calling devices, allowing the media connection to be disconnected between the Unified CM device and the MTP, while establishing and maintaining media between the MTP and the held device with a=sendrecv. On call resumption, the MTP is removed from the media path. This feature addresses the mid-call Delayed Offer INVITE issue for audio direction, but it cannot resolve the issue of a device responding with its

last used codec rather than the full list of all supported codecs. This issue can be problematic in cases where a codec change is required on re-establishment of media, such as placing a G.729 call on hold and connecting it to a music on hold source where G711 is preferred.

Require SDP Inactive in Mid-Call Media Exchange

SIP allows mid-call updates to codecs and connection information, such as IP addresses and UDP port numbers, without disconnecting the media connection. Some third-party devices cannot accept media changes using this method, and they require the media path to be closed gracefully and reopened to make media changes. If this feature is enabled, during mid-call codec or connection updates Cisco Unified CM sends an INVITE a=inactive SDP message to the endpoint to break the media exchange.

Note   For SIP trunks enabled for Early Offer, this parameter will be overridden by the **Send send-receive SDP in mid-call INVITE** parameter.

Disable Early Media on 180

By default, Cisco Unified CM signals the registered calling phone to play local ringback if SDP is not received in a 180 Ringing or 183 Session Progress Response.

If SDP is included in the 180 or 183 Response, instead of playing ringback locally, Cisco Unified CM connects media, and the calling phone plays whatever the called device is sending in its media stream (such as ringback or busy signal).

If ringback is not received, the device to which you are connecting might be including SDP in the 180 response, but it is not sending any media before the 200 OK response. In this case, check this check box to play local ringback on the calling phone and connect the media upon receipt of the 200 OK response

Redirect by Application

When enabled, the Redirect by Application feature allows Unified CM to:

- Apply a specific calling search space to redirected contacts that are received in the 3xx response.
- Apply digit analysis to the redirected contacts to make sure that the call gets routed correctly.
- Prevent a DOS attack by limiting the number of redirection (recursive redirection) requests
- Allow other features to be invoked while the redirection is taking place.

If the Redirect by Application check box is unchecked, outbound SIP trunk calls can be redirected to a restricted phone number (such as an international number) because redirection is handled and routed at the SIP stack level without intervention of Unified CM digit analysis and class of service.

Re-Route Incoming Request to New Trunk Based on

Inbound SIP trunk calls to Unified CM will be accepted only if the source IP address and port number of the calling device match the destination IP address and port number of a configured SIP trunk. Once the call has been accepted, it can then optionally be re-routed to another Unified CM SIP trunk based on information contained within the received SIP message header.

By default, calls are never re-routed after being matched to a SIP trunk based on IP address and port number.

Optionally, incoming Requests can be re-routed to a new trunk based on the received:

- Contact header

    The call is re-routed to another SIP trunk based on the IP address and port number received in the contact header. This feature is typically used to re-route calls from a SIP Proxy to a Unified CM SIP trunk assigned to a specific end user or system.

- Call-Info Header with purpose=x-cisco-origIP

    This option is used to match inbound calls from Cisco Unified Customer Voice Portal (CVP) to a specific trunk based on the IP address and port number contained in the Call-Info header parameter purpose=x-cisco-origIP. This feature is typically used to map calls from Unified CVP to Unified CM trunks for call admission control.

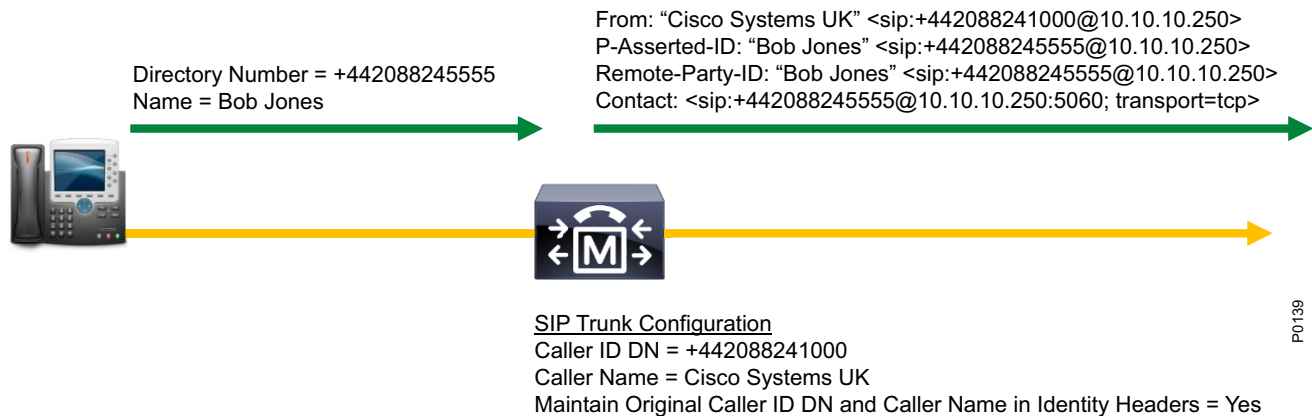**Overwriting Caller ID Number and Name in Outbound Trunk Calls**

This feature can be useful if, for example, you wish to send a company switchboard number and company name instead of the caller's number and name in the SIP messages of calls sent over the SIP trunk. (See Figure 6-25.)This feature can be applied at the device level (for branch offices using a centralized SIP trunk) or at the trunk level.

At the device level, use the Caller ID DN and Caller Name fields of the Incoming Requests FROM URI Setting section on the SIP Profile associated with the device.

At the trunk level, use the Caller ID DN and Caller Name fields of the Outbound Calls - Caller Information section of the trunk configuration page.

By default the Caller ID DN and Caller Name sent in the From header, Contact header, and P-Asserted-Identity and Remote-Party-ID headers are modified in outbound SIP trunk calls. If you wish to keep the original Caller ID in the P-Asserted-Identity and Remote-Party-ID headers, check the **Maintain Original Caller ID DN and Caller Name in Identity Headers** check box on the trunk configuration page. Checking this check box allows the originator of the call to be traced.

Figure 6-25 *Overwriting Caller ID Number and Caller Name on Outbound SIP Trunk Calls*

From: "Cisco Systems UK" <sip:+442088241000@10.10.10.250>
P-Asserted-ID: "Bob Jones" <sip:+442088245555@10.10.10.250>
Remote-Party-ID: "Bob Jones" <sip:+442088245555@10.10.10.250>
Contact: <sip:+442088245555@10.10.10.250:5060; transport=tcp>

Directory Number = +442088245555
Name = Bob Jones

SIP Trunk Configuration
Caller ID DN = +442088241000
Caller Name = Cisco Systems UK
Maintain Original Caller ID DN and Caller Name in Identity Headers = Yes

SIP Trunk Message Normalization and Transparency

Normalization and transparency provide powerful script-based functionality for SIP trunks that can be used transparently to forward and/or modify SIP messages and message body (SDP) contents as they traverse Unified CM. Normalization and transparency scripts are designed to address SIP interoperability issues, allowing Unified CM to interoperate with SIP-based third-party PBXs, applications, and IP PSTN services.

SIP Trunk Normalization

Normalization allows incoming and outgoing SIP messages to be modified on their way through Unified CM. For example, Unified CM supports the Diversion header for carrying redirecting number information. Some SIP devices connected to Unified CM use the History-Info header for this purpose. An inbound normalization script can be used to transform the History-Info headers into Diversion headers so that Unified CM recognizes the redirecting information. Likewise, an outbound normalization script can be used to transform Diversion headers into History-Info headers so that the external SIP device will recognize the redirecting information.

The normalization script is associated with a SIP trunk or a SIP line. The scripts manifest themselves as a set of message handlers that operate on inbound and outbound SIP messages. For normalization, the script manipulates almost every aspect of a SIP message, including:

- The request URI
- The response code and phrase
- SIP headers
- SIP parameters
- Content bodies
- SDP

Normalization applies to all calls that traverse a SIP trunk with an associated script, regardless of what protocol is being used for the other endpoint involved in the call. For example, a SIP trunk normalization script can operate on a call from a SIP line device to a SIP trunk, from an SCCP device to a SIP trunk, from MGCP trunk to SIP trunk, from H.323 trunk to SIP trunk, and so forth. (See Figure 6-26.)

Figure 6-26   *SIP Trunk Normalization*
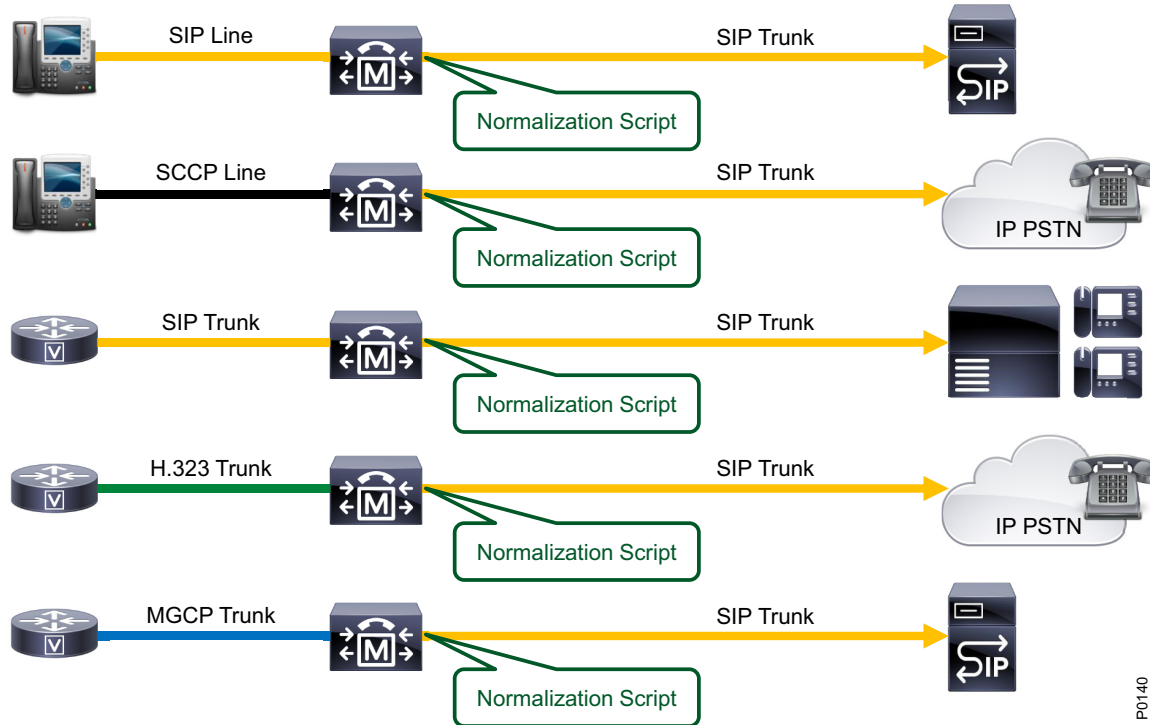
SIP Trunk Transparency

Transparency allows Unified CM to pass SIP headers, parameters, and message body contents from one SIP trunk call leg to another, even if Unified CM does not understand or support the parts of the message that are being passed through. Transparency (or transparent pass-through) is applicable only for SIP-to-SIP calls through Unified CM. (See Figure 6-27.)

The transparency script is associated with a SIP trunk or a SIP line. The scripts manifest themselves as a set of message handlers that operate on inbound and outbound SIP messages. For transparency, the script passes through almost any information in a SIP message, including:

- SIP headers
- SIP parameters
- Content bodies

Figure 6-27   *SIP Trunk Transparency*
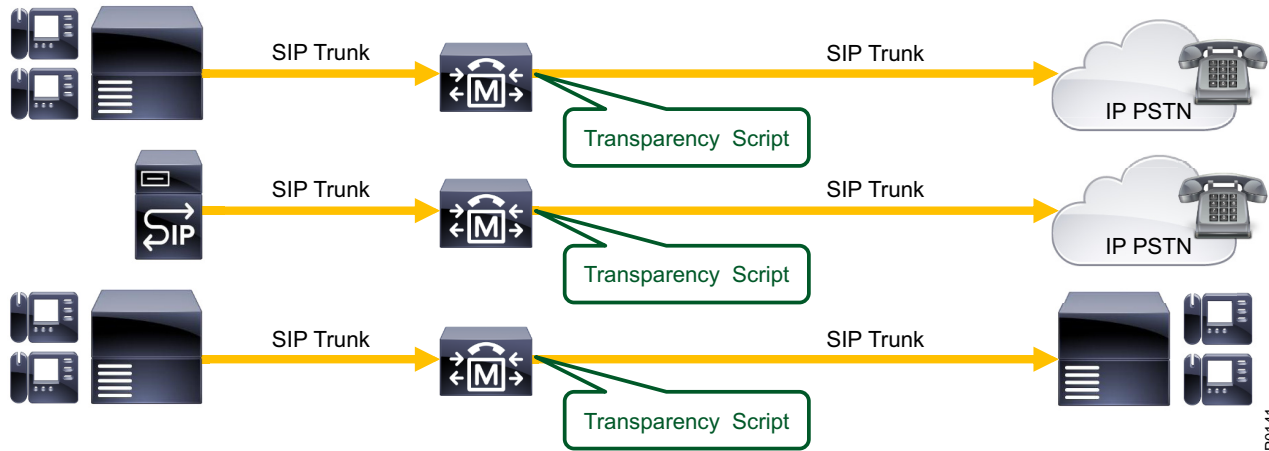
Normalization and transparency scripts use Lua, a powerful, fast and lightweight, embeddable scripting language to modify SIP messages and SDP body content on SIP trunks. (For more information on Lua, refer to the documentation available at http://lua-users.org/wiki/LuaOrgGuide.)

For more information on SIP trunk normalization and transparency scripts, refer to the latest version of the *Developer Guide for SIP Transparency and Normalization*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

The developer guide describes the scripting environment and APIs used to manipulate and pass through SIP message information.

For more information on script management, refer to the latest version of the *Cisco Unified Communications Manager Administration Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Pre-Loaded Unified CM Normalization and Transparency Scripts

A number of normalization and transparency scripts are pre-loaded into Unified CM, and the following scripts are a representative sample of them:

- Refer-passthrough script — This script allows Unified CM to be removed from the call signalling path when a blind transfer (using an in-dialog REFER) is invoked between two SIP trunks.

- ContactHeader script — This script removes the audio and video attributes from the contact header in an inbound Delayed Offer mid-call re-invite.

- HCS-PCV-PAI-passthrough script — This script is used for integration with IP Multimedia Subsystem (IMS) networks, and it passes through or adds the P-Charging-Vector header in INVITE, UPDATE, and 200 OK messages.

- Diversion-Counter script — This script provides the capability to adjust the diversion counter for various Call Forward scenarios.

- VCS-interop script — This script provides interoperability for endpoints registered to the Cisco TelePresence Video Communication Server (VCS).

IP PSTN and IP Trunks to Service Provider Networks

Service providers are increasing their offerings of non-TDM PSTN connections to enterprise customers. Apart from the key benefit of the cost savings from deploying non-TDM interfaces, these IP-based PSTN connections can also offer additional voice features compared to traditional PSTN interfaces.

SIP services dominate today's available offerings, and although earlier H.323 services were available in select geographies, they are being phased out. This is mainly due to the increasing popularity of SIP as the protocol of choice by unified communications vendors and within the enterprise.

When connecting to a service provider's IP PSTN network, Cisco strongly recommends the use of the Cisco Unified Border Element as an enterprise edge Session Border Controller to provide a controlled demarcation and security point between your enterprise and the service provider's network.

Cisco Unified Border Element

Cisco Unified Border Element is a Session Border Controller that provides the following features and services:

- Address and port translations (privacy and Level 7 topology hiding)
- Conversion from SIP Delayed Offer to Early Offer
- Protocol interworking (H.323 and SIP) and normalization
- Media interworking (DTMF, fax, transcoding, transrating, volume and gain control)
- Call admission control (based on total calls, CPU, memory, call arrival spike detection, or maximum calls per destination)
- Security (including RTP to SRTP interworking, SIP malformed packet detection, non-dialog RTP packet drops, SIP listening port configuration, digest authentication, simultaneous call limits, call rate limits, toll fraud protection, and a number of signalling and media encryption options)
- PPI/PAI/Privacy and RPID – Identity Header Interworking with service providers
- QoS and bandwidth management (QoS marking using ToS, DSCP, and bandwidth enforcement using RSVP and codec filtering)
- Simultaneous connectivity to SIP trunks from multiple service providers
- High availability with in-box or box-to-box failover options (platform dependant)
- URI routing use GDPR route-strings to match dial peers
- Domain-based routing
- Multicast music on hold to unicast music on hold
- Voice and video media forking
- Enterprise Phone Proxy – VPN-Less IP Phone registration to Unified CM through Cisco Unified Border Element
- Billing statistics and CDR collection

The Cisco Unified Border Element is a licensed Cisco IOS application available on a wide range of Cisco router and gateway platforms. Depending on your choice of hardware platform, the Cisco Unified Border Element can provide session scalability from 4 to 16,000 concurrent voice calls with in-box or box-to-box failover options.

For more information on the Cisco Unified Border Element, refer to the documentation at

http://www.cisco.com/go/cube

IP-PSTN Trunk Connection Models

Trunks may be connected to IP PSTN service providers in several different ways, depending on the desired architecture. The two most common architectures for this connectivity are centralized trunks and distributed trunks.

Centralized trunks connect the enterprise network to the service provider through one logical connection (although there may be more than one physical connection for redundancy) by means of a Session Border Controller (SBC) such as the Cisco Unified Border Element. (See Figure 6-28.) All calls to and from the IP PSTN use this set of trunks. For all sites remote from the centralized IP PSTN connection, the media and signalling for PSTN calls must traverse the enterprise IP WAN.

Figure 6-28   Centralized or Aggregated SIP Trunk Model
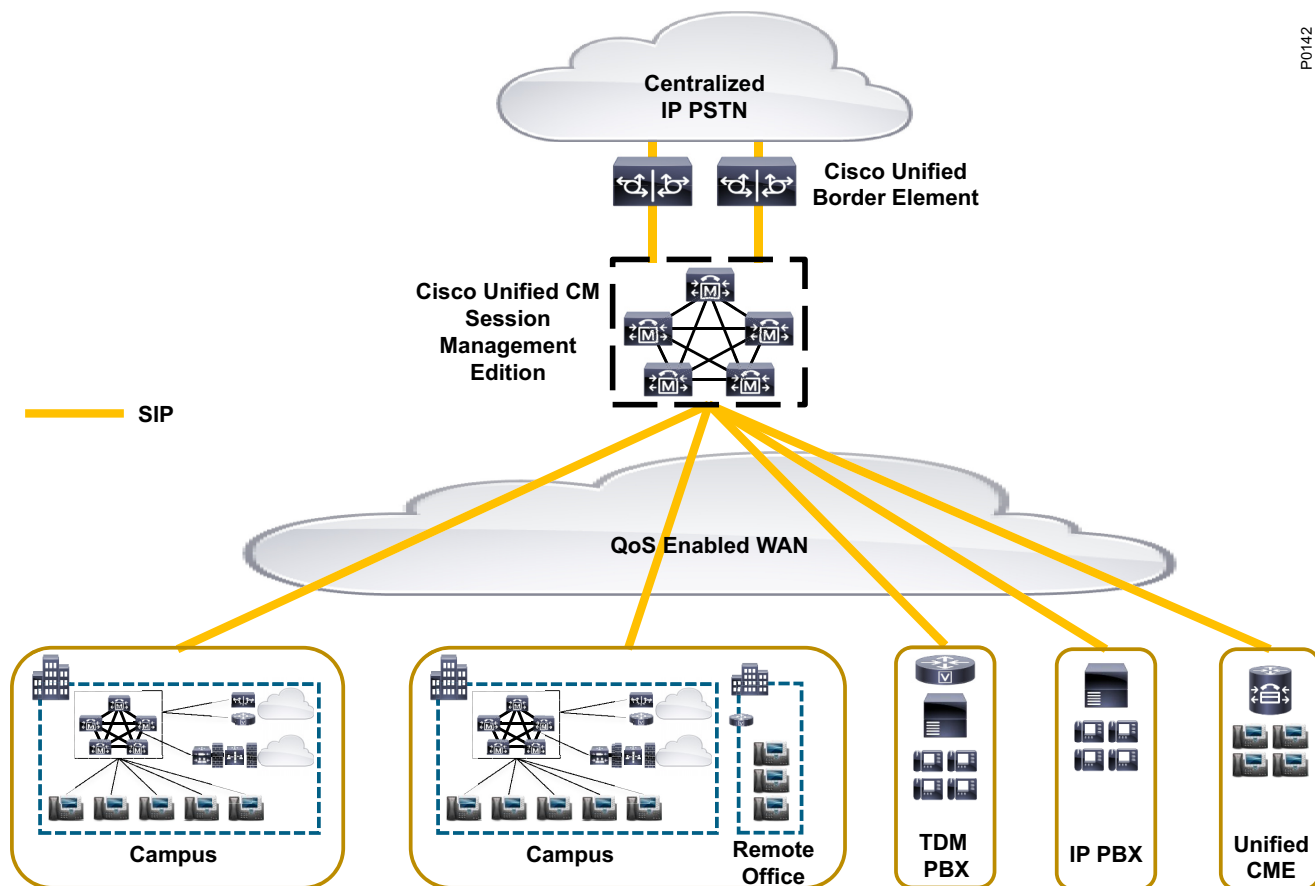
Distributed trunks connect to the service provider through several geographically distributed logical connections. (See Figure 6-29.) Each branch of an enterprise may have its own local trunk to the service provider. With distributed trunks in each branch site, media no longer needs to traverse the enterprise WAN, but flows to the service provider interface through a local SBC.

Figure 6-29   ***Distributed SIP Trunk Model***
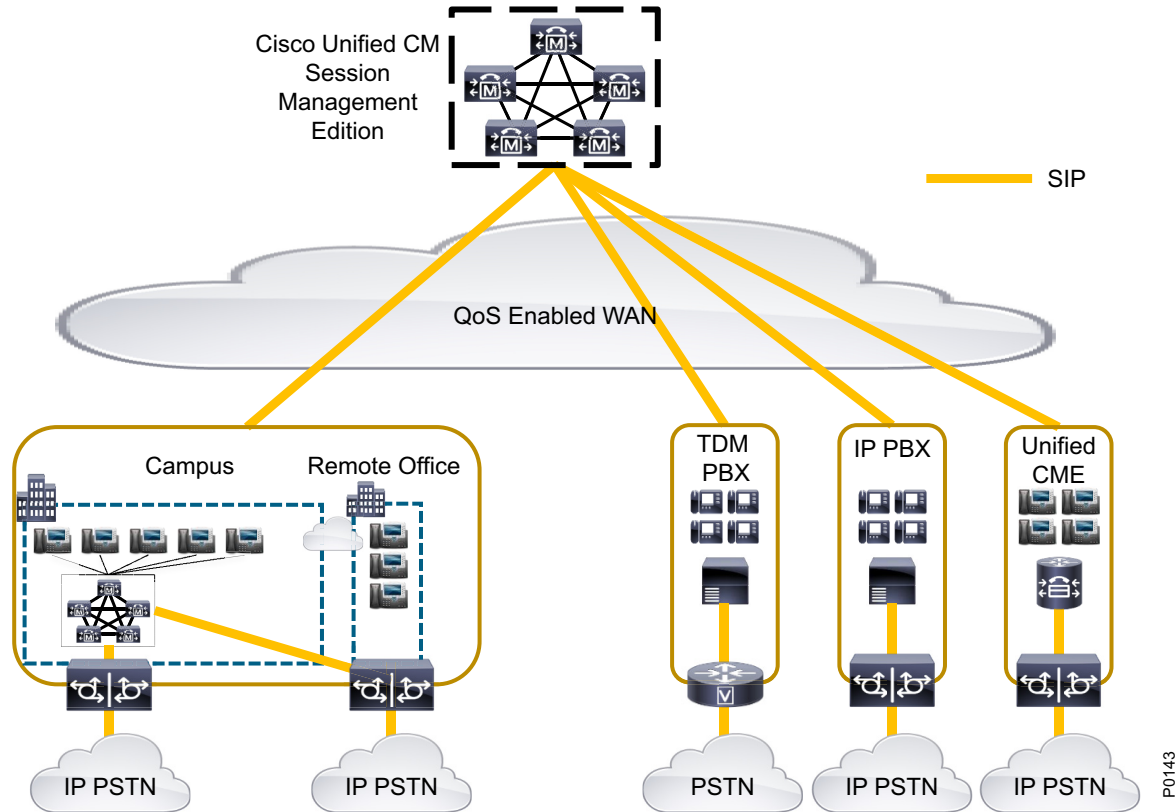
Each connectivity model has its own advantages and disadvantages. Centralized trunks are generally easier to deploy in terms of both physical equipment and configuration complexity, but media and signalling must traverse the enterprise to reach the PSTN, therefore requiring high availability in the enterprise WAN. Distributed trunks have the advantage of local hand-off of media and better number portability from local providers. As illustrated in Figure 6-30, a hybrid connectivity model that groups some of the branches together for connectivity, or that provides trunks from each Unified CM cluster of a multi-cluster deployment, captures the advantages of both forms of deployment models.

Figure 6-30   *Hybrid SIP Trunk Model with Regional Aggregation*
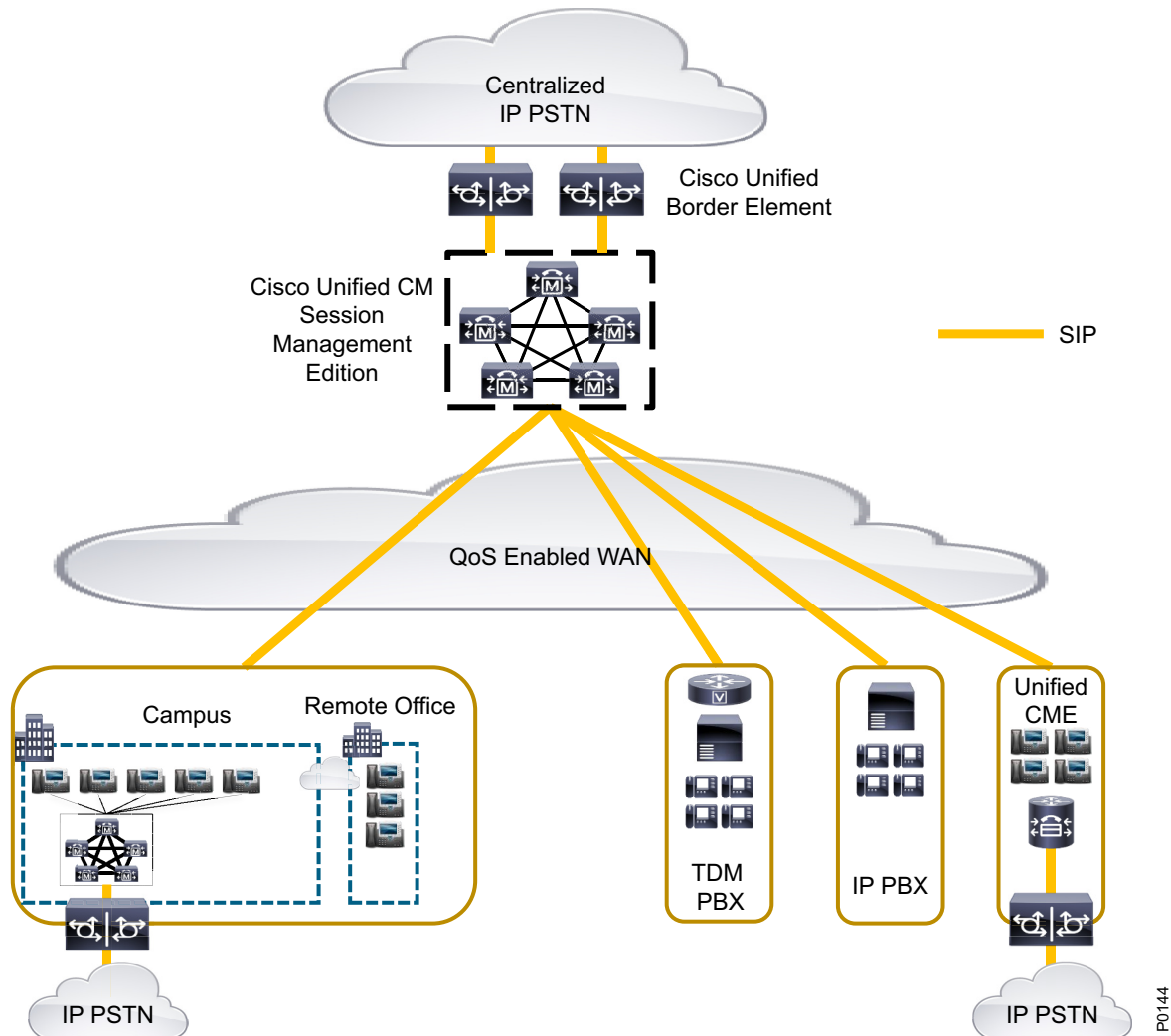
IP PSTN Trunks and Emergency Services

IP trunks might be unable to deliver emergency 911 calls or, like centralized PSTN trunks, might be unable to deliver such calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location. Customers must investigate carefully the capabilities of the IP trunk service provider to deliver emergency 911 calls and caller locations to the appropriate PSAP. Cisco Emergency Responder may be used to provide the location-specific calling party number to the IP trunk service provider for emergency 911 calls.

Centralized IP or PSTN trunks might also temporarily become unavailable for emergency 911 calls from remote locations due to WAN congestion or failure. For this reason, remote locations should always have local gateways to the PSTN that are capable of delivering emergency 911 calls. For more information, see the chapter on Emergency Services, page 15-1.