REVIEW DRAFT - CISCO CONFIDENTIAL

Cisco Unified Communications Manager SIP Trunk Messaging Guide (Standard) Release 10.5(1)

First Published: May 14, 2014

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

CONTENTS

Preface

This document describes the implementation of the Session Initiation Protocol (SIP) for trunk side devices in Cisco Unified Communications Manager.

The preface covers these topics:

Audience

This document provides information for developers, vendors, and customers who are developing applications or products that integrate with Cisco Unified Communications Manager using SIP messaging.

Organization

This document consists of the following chapters.

Chapter	Description
Chapter 1, "SIP Standard Trunk Interface"	Provides an overview of SIP trunk messages and standards compliance.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.

Convention	Description
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in **boldface screen** font.
italic screen font	Arguments for which you supply values are in italic screen font.
–>	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

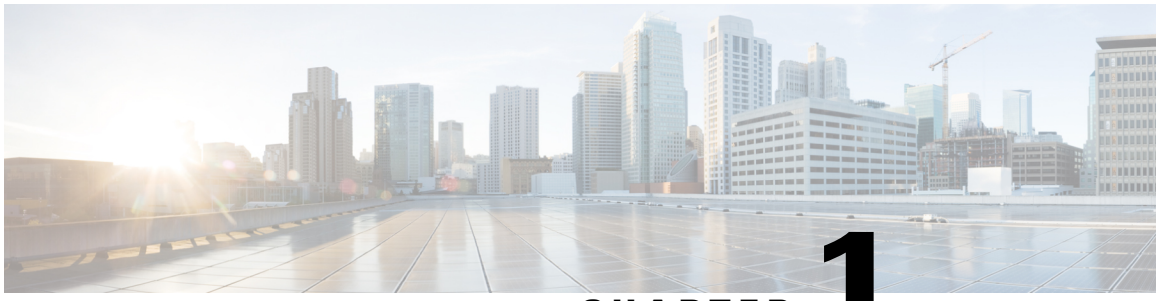
Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Tip Means the following information might help you solve a problem.

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco*

Product Documentation, also lists all new and revised Cisco technical documentation, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.



CHAPTER 1

SIP Standard Trunk Interface

This document describes the standard external interface for *Cisco Unified CM SIP* trunk device. It highlights the SIP primitives that are supported across the SIP trunk and also describes basic call flow scenarios that can be used as a guide for technical support.

This chapter includes the following sections:

New and Changed Information

This section describes new and changed SIP trunk messaging standard information for Cisco Unified Communications Manager and features supported in the previous releases. It contains the following sections:

Features Supported in Previous Releases

Cisco Unified Communications Manager Release 10.5(1)

Release 10.5(1) of Cisco Unified Communications Manager provides the following SIP trunk enhancements:

- SIP Best Effort Early Offer and SIP Early Offer, on page 91
- Cluster-wide SAN Certificate, on page 94

Cisco Unified Communications Manager Release 10.0(1)

The release 10.0(1) provides the following new SIP trunk interface enhancements:

- H.264 SVC Codecs, on page 83
- Confidential Access Level, on page 84
- iX Channel Support, on page 86
- Multiple Codecs in Answer SDP, on page 86
- Non-SRTP Call Block, on page 87
- Session Timer with UPDATE, on page 88
- SDP Transparency for Declarative Attributes, on page 88
- SIP BPA/488 Error Handling, on page 89
- Video On Hold, on page 90

Cisco Unified Communications Manager Release 9.x

The release 9.0(1) provides the following new SIP trunk interface enhancements:

- Outgoing Identity and Incoming CLI for SIP Calls, on page 79
- Conference Factory Support, on page 80
- URI Dialing, on page 81
- Anonymous Call Rejection for an Incoming and Outgoing SIP Trunk Call, on page 82

The release 9.1(1) does not provide any new or changed SIP trunk interface enhancements.

Cisco Unified Communications Manager Release 8.6(2)

The release 8.6(2) does not provide any new or changed SIP trunk interface enhancements.

Cisco Unified Communications Manager Release 8.6(1)

The release 8.6(1) provides the following new SIP trunk interface enhancements:

Backward Compatibility

The features that are introduced in this release do not impose any backward compatibility implications on previous versions of the SIP trunk.

Interface Compliance Summary

Cisco Unified CM SIP compliance on the SIP trunk depends on the portable SIP stack itself, which is based on the RFC 3261 standard.

The current stack supports the following items in RFC 3261:

- Can process UPDATE method.
- Support for generating branch and sent-by parameters in Via header used to identify transactions.
- Implementation of loose-routing based on lr parameter in Record-Route header.
- A UAS that receives a second INVITE before it sends the final response to a first INVITE with a lower Cseq sequence number on the same dialog must return a 500 (Server Internal Error) response to the

second INVITE and must include a Retry-After header field with a random value of between 0 and 10 seconds.

- If the non-2xx final response to a mid-call INVITE is a 481 (Call/Transaction Does Not Exist), or a 408 (Request Timeout), or no response at all is received for the re-INVITE (that is, a timeout is returned by the INVITE client transaction), the UAC will terminate the dialog.
- If the UAC receives a reliable provisional response with an answer, it may generate an additional offer in the PRACK. If the UAS receives a PRACK with an offer, it must place the answer in the 2xx to the PRACK.
- If a reliable provisional response is retransmitted for 32 seconds without reception of a corresponding PRACK, the UAS should reject the original request with a 5xx response.

Call Manager uses the portable SIP stack from IOS Gateway SunnyD project (EDCS-292452).

Table 1: SIP Trunk RFC Compliance, on page 4 identifies the RFC compliance for the SIP trunk.

Table 1: SIP Trunk RFC Compliance

RFC	Call Manager Supported	Comments
RFC2976 SIP INFO Method	Supported	Info method is used for video media channels; Picture Fast Update and Picture Freeze.
RFC2833 RTP Payload for DTMF Digits	Supported	
RFC2782 DNS SRV	Supported	
RFC3261 SIP: Session Initiation Protocol	Supported	
RFC3262 SIP Reliability of Provisional Responses	Supported	
RFC3264 Offer/Answer Model for SDP	Supported	
RFC3265 Specific Event Notification	Supported	Packages supported: KPML, Presence.
RFC3311 SIP UPDATE Method	Supported	
RFC3515 SIP REFER Method	Partially supported	SIP Trunk accepts inbound REFER's (in-dialog and out-of-dialog). In this release CCM only supports method = INVITE in the Refer-To header. CCM does not support multiple Refer requests within the same dialog.

RFC	Call Manager Supported	Comments
RFC3842 SIP MWI Package	Partially supported	SIP Trunk supports unsolicited NOTIFY events. It does not Subscribe for MWI events notification.
RFC3856 SIP PRESENCE Event Package	Supported	
RFC3859 Common Profile for Presence	Supported	
RFC3863 Presence Information Data Format	Supported	
RFC3891 SIP Replaces Header	Supported	INVITE w/Replaces and REFER w/Replaces.
RFC3903 SIP PUBLISH Method	Partially supported	SIP Trunk only supports outbound PUBLISH. Inbound PUBLISH is rejected with 405.
RFC4028 Session Timers in the SIP	Supported	For outgoing Invite's, the SIP Trunk indicates the support via Supported header. For incoming Invite's it accepts the Supported and Session-Expires headers.
RFC4480 RPID	Supported	RPID information is carried in the outbound messages if selected via SIP Trunk configuration.
Draft-ietf-sipping-kpml-07.txt	Supported	KPML Event Package (for OOB DTMF).
Draft-ietf-sip-privacy-05.txt	Supported	Remote Party ID (RPID) Header.
Draft-levy-sip-diversion-08.txt	Supported	Draft-levy-sip-diversion-08.txt.
RFC3323	Supported	A Privacy Mechanism for SIP.
RFC3324	Supported	Short Term Requirements for Network Asserted Identity.
RFC3325	Supported	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.
RFC4411	Supported	SIP Trunk supports extending Reason header for Preemption Events.

RFC	Call Manager Supported	Comments
RFC4412	Partially supported	SIP Trunk only supports outbound Resource-Priority header. A Resource-Priority header is added and will show up in "Require" header field when used.
RFC4040	Supported	A clear channel codec negotiation for SIP Trunk.
RFC4091	Supported	Alternative Network Address Types for advertising both IPv4 and IPv6 media in the SDP.
RFC4092	Supported	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP).
RFC3388	Partially supported	SIP Trunk only supports sections pertaining to grouping of M Lines for ANAT.
RFC3693	Partially supported	As part of Logical Partitioning feature, CUCM supports Geopriv Location Object specification described in this RFC.
RFC4119	Partially supported	Extension to RFC3693. CUCM supports PIDF-LO specification as described in RFC 4119.
draft-ietf-sip-location-conveyance-10	Partially supported	CUCM supports Location Conveyance specification described in this ietf draft.
RFC3312	Partially supported	End to End qos is supported but Segmented qos is not supported.
RFC4032	Partially supported	Extension to RFC3312, CUCM supports changing precondition strength based on target changes.
RFC4574	Partially supported	Compliant to RFC 4574 in the context of BFCP application.
RFC4583	Partially supported	Partially compliant as there are deviations from the floorctrl attribute.
draft-sandbakken-xcon-bfcp-upd-01	Supported	SDP format for BFCP. Cisco Unified CM only supports UDP/BFCP implementation based on IETF draft.

RFC	Call Manager Supported	Comments
RFC4796	Partially supported	Compliant to RFC 4796 in the context of BFCP application.
RFC 3455	Partially supported	Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).
Intrado GRISP v.3-8	Partially compliant	Cisco Emergency Responder can add Contact header additions to INVITE request with formatting as specified in draft-ietf-sip-gruu-12.
RFC 5079	Supported	Compliant with sending 433 Anonymity Disallowed response when caller's user portion in PAI/RPID/From is either marked private or not provided.
RFC 6337	Partially compliant	Supported as part of SIP Best Effort Early Offer changes.

This document identifies the SIP trunk compliance for SIP messages and headers, as described in Table 1-2 through Table 1-8.

Table 2: Compliance to SIP Requests

SIP Message	Cisco Unified CM Supported	Comments
INVITE	Yes	The system also supports re-INIVTE.
ACK	Yes	
OPTIONS	Yes	Supports basic OPTIONS ping fonctionality.
INFO	Yes	INFO method gets used for video support.
BYE	Yes	BYE can tunnel QSIG RELCOMP message.
CANCEL	Yes	CANCEL can tunnel QSIG RELCOMP message.
SUBSCRIBE	Yes	Supported events: kpml, presence

SIP Message	Cisco Unified CM Supported	Comments
NOTIFY	Yes	Supported events: kpml, presence In addition, Cisco Unified CM supports unsolicited NOTIFY for DTMF and MWI.
REFER	Yes	Cisco Unified CM SIP trunk supports inbound REFER only, both in dialog and out of dialog.
REGISTER	No	The system sends 405 Method Not Allowed for Cisco Unified CM SIP trunk.
PRACK	Yes	The system provides three options: • To send PRACK for Only 180 w/sdp, or • To disable PRACK entirely via CCM Service Parameter
UPDATE	Yes	Cisco Unified CM supports receiving and generating UPDATE.
PUBLISH	Yes	Cisco Unified CM supports only generating PUBLISH.

Table 3: Compliance to SIP Responses

SIP Message	Cisco Unified CM Supported	Comment
1xx Response	Yes	
100 Trying	Yes	
180 Ringing	Yes	The system supports early media.
181 Call Forward	No	Cisco Unified CM sends 181 Call forwarded response when the call forward feature is invoked.
182 Queued	No	Stack drops this message.
183 Progress	Yes	The system supports early media.
2xx Response	Yes	

SIP Message	Cisco Unified CM Supported	Comment
200 OK	Yes	
202 OK	Yes	For REFER
3xx Response	Yes	
300–302, 305, 380, 385	Yes	The system does not generate these messages, but contacts the new address in Contact header upon receiving.
4xx Response	Yes	Upon receiving, the system initiates a graceful call disconnect
401	Yes	Cisco Unified CM SIP trunk sends out 401 (Unauthorized) if authentication and authorization is enabled. Cisco Unified CM SIP trunk also responds to inbound 401 challenges.
403	Yes	Cisco Unified CM SIP trunk sends a 403 (Forbidden) message if a SIP method is on the Access Control List.
405	Yes	Cisco Unified CM SIP trunk sends a 405 message if the incoming SIP message is not supported.
407	Yes	Cisco Unified CM SIP trunk responds to inbound 407 (Proxy Authentication Required) message challenges.
412	Yes	Cisco Unified CM SIP trunk processes 412 response for PUBLISH.
415	Yes	Cisco Unified CM SIP Trunk sends out 415 (Unsupported Media Type) message when it does not support the media type received in incoming request's SDP.

SIP Message	Cisco Unified CM Supported	Comment
420	Yes	Cisco Unified CM SIP Trunk sends out 420 (Bad Extension) message when it receives sdp-anat tag in the Require/Supported header and it is not configured for ANAT.
424	Yes	Cisco Unified CM SIP Trunk sends out 424 (Bad Location Information) message when it receives INVITE requests carrying Location Conveyance info with errors against SIP compliance like: • Geolocation Headers indicate inclusion of PIDF-LO, but message body doesn't carry it. • Geolocation header has a cid header referring to a URI for which there is no corresponding Content-ID header with the same URI. • Geolocation header having URI other than cid header e.g SIP or SIPS URI for LbyR.
433	Yes	Cisco Unified Communications Manager SIP trunk sends 433 Anonymity Disallowed response to reject a call when it receives INVITE request where the user-portion in PAI, RPID or From header is either private or not provided.
5xx Response		Upon receiving, the system sends a new request if additional address is present. Otherwise, it initiates a graceful disconnect.

SIP Message	Cisco Unified CM Supported	Comment
580	Yes	CUCM get INVITE with precondition and its local RSVP layer sends reject because the bandwidth is not available, then CUCM responds with 580 Precondition Failed. Upon receiving the 580 response, CUCM will either continue the call with no RSVP involved or call fails based on local RSVP policy configuration.
6xx Response	Yes	The system does not generate this response; upon receiving, the system initiates a graceful disconnect.

Table 4: SIP Header Fields

SIP Header	Cisco Unified CM Supported	Comments
Accept	No	
Accept-Encoding	No	
Accept-Language	No	
Alert-Info	No	
Allow	Yes	
Authentication-Info	No	
Authorization	Yes	
Allow-Events	Yes	kpml, presence

SIP Header	Cisco Unified CM Supported	Comments
Call-Info	Yes	Call-Info is used to transmit the overall security level of the trunk call. For example: Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated Call-Info header is also used for figuring out the IP address of the originating device for SIP trunk identification, if it contains the tag, purpose=x-cisco-origIP. For example: Call-Info: <sip:172.18.200.127>; PURPOSE=x-cisco-origIP
Call-ID	Yes	
Contact	Yes	
Content-Disposition	Yes	Signal; handling=optional.
Content-Encoding	No	
Content-Language	No	
Content-Length	Yes	
Content-Type	Yes	Supported as: “sdp”, “kpml-request+xml”, “media_control+xml”, “text/plain”, “pidf+xml”, “simple-message-summary”, and “application/qsig”. The system only supports “multipart” for cases where both the SDP and QSIG content is to be tunneled.
CSeq	Yes	
Date	Yes	

SIP Header	Cisco Unified CM Supported	Comments
Diversion	Yes	The system uses this header for RDNIS information. If it is present, it is always the Original Called Party information. The receiving side of this header always assumes that it is the Original Called Party information if present. In case of chained-forwarding to a voice messing system, the system leaves the message to the Original Called Party.
Encryption	No	
Error-Info	No	
Expires	Yes	
Event	Yes	
From	Yes	Cisco Unified CM adds x-nearend, x-farend, x-refci, x-nearenddevice, x-farenddevice, x-farendaddr, and isfocus (for conference) parameters for Recording INVITEs. and UPDATEs.
Geolocation	Yes	Cisco Unified CM supports this header as part of Logical Partitioning feature
Geolocation-Error	Yes	Cisco Unified CM supports this header as part of Logical Partitioning feature. This is an informatory header which is sent in SIP response messages.
Hide	No	
In-Reply-To	No	
Max-Forwards	Yes	Cisco Unified CM sets to 70 for outgoing INVITE and does not increment/decrement it.
Min-Expires	Yes	

SIP Header	Cisco Unified CM Supported	Comments
MIME-Version	No	
Organization	No	
Priority	No	
Proxy-Authenticate	Yes	Cisco Unified CM SIP trunk supports receiving this header in 407 responses.
Proxy-Authorization	Yes	Cisco Unified CM SIP trunk supports sending new request with this header after receiving 407 responses.
Proxy-Require	No	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
RAck	Yes	
Record-Route	Yes	
Remote-Party-ID	Yes	The system uses this header for ID services including Connected Name and ID. This is a non-standard header from a draft specification.
Replaces	Yes	For INIVTE and REFER.
Require	Yes	
Response-Key	No	
Retry-After	Yes	The system sends it but ignores receiving it.
Resource-Priority	Yes	
Route	Yes	
RSeq	Yes	
Server	Yes	
SIP-If-Match	Yes	For PUBLISH

SIP Header	Cisco Unified CM Supported	Comments
SIP-Etag	Yes	For PUBLISH
Subject	No	
Supported	Yes	
Subscription-State	Yes	
Timestamp	Yes	
To	Yes	
Unsupported	Yes	
User-Agent	Yes	
Via	Yes	
Warning	Yes	
WWW-Authenticate	Yes	

Table 5: Supported Audio Media Types

Type	Encoding Name	Payload Type	Comments
G.711 u-law	PCMU	0	
GSM Full-rate	GSM	3	
G.723.1	G723	4	
G.711 A-law	PCMA	8	
G.722	G722	9	
G.728	G728	15	
G.729	G729	18	The system supports all combinations of annex A and B.
AAC	mpeg4-generic	Dynamically Assigned	Acceptable range is 96–127.
ILBC	iLBC	Dynamically Assigned	Acceptable range is 96–127.
RFC2833 DTMF	Telephony-event	Dynamically Assigned	Acceptable range is 96–127.

Type	Encoding Name	Payload Type	Comments
G.Clear	G.Clear	Dynamically Assigned	Acceptable range is 96–127. Cisco Unified CM default is 125.
iSAC	iSAC	Dynamically Assigned	Acceptable range is 96–127.
NoAudio (negociable in v1.50 MER)	NoAudio	Dynamically Assigned	Currently hard-coded to 126.
AAC-LD	MP4A-LATM	Dynamically Assigned	Acceptable range is 96-127.
G.722.1	G7221	Dynamically Assigned	Acceptable range is 96-127

Table 6: Supported Video Media Types

Types	Encoding Name	Payload Type
H.261	H261	31
H.263	H263	34
H.263+	H263-1998	Acceptable range is 96–127.
H.263++	H263-2000	Acceptable range is 96–127.
H.264	H264	Acceptable range is 96–127.

Table 7: Supported Application Media Type

Types	Encoding Name	Payload Type
H.224 FECC	H224	Acceptable range is 96–127

Table 8: Supported T38fax Payload Type

Types	Encoding Name	Payload Type
T38fax	Not applied	Not applied

SIP Message Fields

The SIP trunk supports SIP request and SIP response messages. The request messages include INVITE, ACK, OPTIONS, BYE, CANCEL, PRACK, SUBSCRIBE, UPDATE, and REFER methods. The response message consists of a status-line with various status codes (1xx, 2xx, 3xx, 4xx, 5xx and 6xx). The SIP trunk supports all mandatory fields from the SIP standard. See Table 9: INVITE Message Fields, on page 18 through Table 23: 6XX Message Fields, on page 46.

Request Messages

INVITE

Table 9: INVITE Message Fields

Field	Example	Notes
Request-Line	`INVITE sip:cdpn@destIP:destPort; phone-context=cisco.com; tgrp=ccdata;user=phone SIP/2.0`	destIP=resolved IP address of configured DestAddr under SIPTrunk; it also could be FQDN SRV instead of destIP. If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV. cgpn for outgoing INVITE, and cdpn for incoming INVITE. “phone-context=cisco.com; tgrp=ccdata;”= When MTP is not enabled and the G.Clear feature is enabled, these tags are added to the Request URI. Both of these values are user provisionable.
From	`From:"callerName"<sip:cgpn@CCM_IP_addr>; x-nearend; x-farend; x-refCI=CI_NUMBER; x-devicename=SEP_NAME`	callerName = caller display i.e.IP phone Cgpn = calling party number CCM_IP_addr = CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate Cisco Unified CM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. x-nearend = Recorded party is the near-end. x-farend = Recorded party is the far-end x-refCI = Cisco Unified CM call identifier for recorded party x-devicename = Device name of recorded party.

Field	Example	Notes
To	`To: "calledName" <sip:cdpn@destIP;user=phone>`	The system includes calledName if available. destIP=resolved IP address of configured DestAddr/DestV6Addr under SIPTrunk; it could also be FQDN SRV instead of destIP
Via	`Via:SIP/2.0 IP addr:Port;Branch=number`	IP addr = Cisco Unified CM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port = CCM Port Branch = Unique number
Call-ID	`Call-ID: number@CCM_IP_addr`	Cisco Unified CM generates the number internally.
Contact	`Contact: <sip:cgpn@CCM_IP_addr:localPort;user=phone>`	localPort = configured "Incoming port" of the indicated SIPTrunk
Cseq	`Cseq:number method`	Number = a traditional sequence number that is incremented for each new request within a dialog Method = INVITE
Max-Forwards	`Max-Forwards:number`	Number = Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop by sip proxy. CCM sets it 6 for outgoing INVITE.

Remote-Party-Id	IPv4 Example
	`Remote-Party-ID:"Alice Smith" <sip:9728135111@161.44.147.67;user=phone> ;party=calling;screen=no;privacy=off`
	IPv6 Example
	`Remote-Party-ID:"Alice Smith" <sip:9728135111@[2001:db8:1:101::12];user=phone>; party=calling;screen=no;privacy=off`
		Cisco Unified CM uses this SIP extension for more detailed description of Caller Identify and Privacy. It is also used to convey Connected Name and ID in a re-Invite message.

Field	Example	Notes

Diversion	IPv4 Example
	`Diversion: <sip:23222@172.18.193.123>;reason=no-answer`
	IPv6 Example
	`Diversion:<sip:23222@[2001:db8:1:101::12]>; reason=no-answer`
		Cisco Unified CM uses Diversion header to carry RDNIS. In this case, 23222 will be carried as the Original Called Party ID.

Call-Info	IPv4 Example
	`Call-Info: <sip:172.18.199.211>;purpose=x-cisco-origIP`
	IPv6 Example
	`Call-Info: <sip:[2001:db8:1:101::12]>;purpose=x-cisco-origIP`
		If this header is present in an incoming INVITE with the tag, purpose=x-cisco-origIP, and the trunk is configured to route the call based on the end device's IP Address, then this header will be used to route the call to the Trunk pointing to the IP Address in the Call-Info header.

P-Asserted-Identity	IPv4 Example
	`P-Asserted-Identity: "Alice" <sip:4762424@172.18.199.211>`
	IPv6 Example
	`P-Asserted-Identity: "Alice" <sip:4762424@[2001:db8:1:101::12]>`
	IPv6 Example
	`P-Preferred-Identity: "Alice" <sip: 4762424@[2001:db8:1:101::12]>`
		Cisco Unified CM uses this header to convey caller name/number information.
		In the re-Invite message, it is used to convey the connected name/number.
		Cisco Unified CM adds the PAI header if the SIP trunk is configured with Asserted-Type=PAI or Asserted-Type=Default and the call control in Cisco Unified CM provides the screening indication of UserProvided “VerifiedAndPassed” or NetworkProvided.
		PAI header values are displayed per the user configuration.

P-Preferred-Identity	IPv4 Example `P-Preferred-Identity: "Alice" <sip: 4762424@172.18.199.211>`	Cisco Unified CM uses this header to convey caller name/number information. In the re-Invite message, it is used to convey the connected name/number. Cisco Unified CM adds the PAI header if the SIP trunk is configured with Asserted-Type=PPI or Asserted-Type=Default and when the call control in Cisco Unified CM provides the screening indication of “Not Screened” or “VerifiedAndFailed” values. PPI header values are displayed as per the user configuration.

Field	Example	Notes
Resource-Priority	`Resource-Priority: DRSN.9`	If the MLPP feature is enabled, the Resource-Priority header is added to the initial INVITE.

Supported	`Supported: option-tag`
	Example:
	`Supported:`
	`100rel,timer,resource-priority,replaces`
		Cisco Unified CM adds Supported header in outgoing INVITE request when additional options like PRACK, Presence, Resource-Priority etc. are configured to indicate other side about Cisco Unified CM's capability.

Geolocation	`Geolocation:`
	`cid-url;inserted-by=hostport`
	Example:
	`Geolocation:`
	`<cid:4900@10.10.10.10>;inserted-by="10.10.10.10`
		SIP Trunk only supports sending and processing of cid-url in Geolocation header, though specification allows SIP, SIPS & pres URI's.

Content-Disposition	`Signal; handling=optional`	The system adds this header when QSIG tunneling is enabled.
SDP		If MTP is not enabled for the SIP trunk, SDP is not in the initial INVITE. If MTP is enabled, Cisco Unified CM always include telephone-event for RFC2833 DTMF in the SDP. This dynamic payload type is configurable under Cisco Unified CM Service Parameter with default value as 101. For a SIP Trunk in IPv4 only mode, the SDP will contain the IPv4 address of the MTP device For a SIP Trunk in IPv6 only mode, the SDP will contain the IPv6 address of the MTP device For a Dual Mode SIP Trunk, if ANAT is enabled then, the SDP will contain both the IPv4 address, and the IPv6 address using the ANAT format. If MTP is enabled and G.Clear feature is enabled, CCM sends G.Clear mode information in the SDP in the initial INVITE.

Field	Example	Notes
	IPv4 SDP v=0 o=CiscoSystemsCCM-SIP 2000 1000 IN IP4 10.89.79.203 s=SIP Call c=IN IP4 10.89.79.203 t=0 0 m=audio 32314 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000 a=ptime:20 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 m=audio 16604 RTP/AVP 125 a=rtpmap:125 CLEARMODE/8000 IPv6 SDP v=0 o=CiscoSystemsCCM-SIP 2000 1000 IN IP6 2001:db8:c18:1:21c:58ff:fe2a:23f8 s=SIP Call c=IN IP6 2001:db8:c18:1:21c:58ff:fe2a:23f3 t=0 0 m=audio 32314 RTP/AVP 0 101 a=rtpmap:0 PCMU/8000 a=ptime:20 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 ANAT SDP with both IPv4 and IPv6 addresses v=0 o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.199.129 s=SIP Call t=0 0 a=group:ANAT 1 2 m=audio 18484 RTP/AVP 0 101 c=IN IP6 2001:db8:c18:1:21c:58ff:fe2a:23f8 a=rtpmap:0 PCMU/8000 a=ptime:20 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a=mid:1 m=audio 18282 RTP/AVP 0 101 c=IN IP4 172.18.199.55 a=rtpmap:0 PCMU/8000 a=ptime:20 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a=mid:2	
QSIG Content	Binary body	QSIG content in SIP message is encoded as binary.

ACK

Table 10: ACK Message Fields

Field	Example	Notes
Request-Line	`ACK sip:cdpn@destIP:destPort;SIP/2.0`	destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV.
From	`From: "callerName" <sip:cgpn@CCM_IP_addr>`	callerName=caller display i.e. IP phone Cgpn = calling party number CCM_IP_addr=CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.
To	`To: "calledName"<sip:cdpn@destIP;user=phone>`	calledName is included if available destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	`Via:SIP/2.0 IP addr:Port;Branch=number`	IP addr=CCM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=CCM Port Branch=Unique number

Field	Example	Notes
Call-ID	`Call-ID: number@CCM IP addr`	Cisco Unified CM generates this number internally.
CSeq	`Cseq: number method`	Number=a traditional sequence number that is incremented for each new request within a dialog Method=ACK
Max-Forwards	`Max-Forwards:number`	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop.

BYE

Table 11: BYE Message Fields

Field	Example	Notes
Request-Line	`BYE sip:cdpn@destIP:destPort;SIP/2.0`	destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV.
From	`From: "callerName" <sip:cgpn@CCM_IP_addr>`	callerName=caller display i.e. IP phone Cgpn = calling party number CCM_IP_addr=CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.
To	`To: "calledName"<sip:cdpn@destIP;user=phone>`	calledName is included if available destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	`Via:SIP/2.0 IP addr:Port;Branch=number`	IP addr=Cisco Unified CM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate Cisco Unified CM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=CCM Port Branch=Unique number

Field	Example	Notes
Call-ID	`Call-ID: number@CCM IP addr`	Cisco Unified CM generates this number internally.
CSeq	`Cseq: number method`	Number=a traditional sequence number that is incremented for each new request within a dialog Method=BYE
Max-Forwards	`Max-Forwards:number`	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop.
Reason	`Reason: preemption;cause=<cause value>;text=<text string>`	Reason header is included when MLPP feature is enabled. Cause value and test string are defined as per RFC4411.
Content-Type	`Application/QSIG`	QSIG message REL COMP is tunneled in BYE only when QSIG tunneling is enabled.
Content-Disposition	`Signal;handling=optional`	Only when QSIG tunneling is enabled.

CANCEL

Table 12: CANCEL Message Fields

Field	Example	Notes
Request-Line	`CANCEL sip:cdpn@destIP:destPort;SIP/2.0`	destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV.
From	`From: "callerName" <sip:cgpn@CCM_IP_addr>`	callerName=caller display i.e. IP phone Cgpn = calling party number CCM_IP_addr=CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.
To	`To: "calledName"<sip:cdpn@destIP;user=phone>`	calledName is included if available destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	`Via:SIP/2.0 IP addr:Port;Branch=number`	IP addr=Cisco Unified CM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=Cisco Unified CM Port Branch=Unique number

Field	Example	Notes
Call-ID	`Call-ID: number@CCM IP addr`	Cisco Unified CM generates this number internally.
CSeq	`Cseq: number method`	Number=a traditional sequence number that is incremented for each new request within a dialog Method=CANCEL
Max-Forwards	`Max-Forwards:number`	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop.
Content-Type	`Application/QSIG`	QSIG message REL COMP is tunneled in BYE only when QSIG tunneling is enabled.
Content-Disposition	`Signal;handling=optional`	Only when QSIG tunneling is enabled.

PRACK

Table 13: PRACK Message Fields

Field	Example	Notes
Request-Line	Prack sip:cdpn@destIP:destPort;SIP/2.0	destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV.

Field	Example	Notes
From	From: "callerName" <sip:cgpn@CCM_IP_addr>	callerName=caller display i.e. IP phone Cgpn = calling party number CCM_IP_addr=CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.
To	To: "calledName"<sip:cdpn@destIP;user=phone>	calledName is included if available destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	Via:SIP/2.0 IP addr:Port;Branch=nu mber	IP addr=CCM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=CCM Port Branch=Unique number
Call-ID	Call-ID: number@CCM IP addr	Cisco Unified CM generates this number internally.
CSeq	Cseq:number PRACK	Number=a traditional sequence number that is incremented for each new request within a dialog Method=Method Name
Rack	Rack:number1 number2	Number1=value from the RSeq header in the provisional response that is being acknowledged Number2=The next number, and the method, are copied from the CSeq in the response that is being acknowledged.

UPDATE

Table 14: PRACK Message Fields

Field	Example	Notes
Request-Line	`UPDATE sip:cdpn@destIP:destPort;SIP/2.0`	destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV.
From	`From: "callerName" <sip:cgpn@CCM_IP_addr>`	callerName=caller display i.e. IP phone Cgpn = calling party number CCM_IP_addr=CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.
To	`To: "calledName"<sip:cdpn@destIP;user=phone>`	calledName is included if available destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	`Via:SIP/2.0 IP addr:Port;Branch=number`	IP addr=CCM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=CCM Port Branch=Unique number

Field	Example	Notes
Call-ID	`Call-ID: number@CCM IP addr`	Cisco Unified CM generates this number internally.
Contact	`Contact: <sip:cgpn@CCM_IP_addr:localPort;user=phone>`	localPort = configured "Incoming port" of the indicated SIPTrunk
Cseq	`Cseq:number method`	Number=a traditional sequence number that is incremented for each new request within a dialog Method=UPDATE
Max-Forwards	`Max-Forwards:number`	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop

Remote-Party-Id	`IPv4 Example`
	`Remote-Party-ID:"Alice Smith" <sip:9728135111@161.44.147.67;user=phone>; party=calling;screen=no;privacy=off`
	`IPv6 Example`
	`Remote-Party-ID:"Alice Smith" <sip:9728135111@[2001:db8:1:101::12];user=phone>; party=calling;screen=no;privacy=off`
		Cisco Unified CM uses this SIP extension for more detailed description of Caller Identify and Privacy. It is also used to convey Connected Name & ID in a re-Invite message.

P-Asserted-Identity	`IPv4 Example`
	`P-Asserted-Identity: "Alice" <sip:4762424@172.18.199.211>`
	`IPv6 Example`
	`P-Asserted-Identity: "Alice" <sip:4762424@[2001:db8:1:101::12]>`
		Cisco Unified CM uses this header for conveying the Connected Name/Number.
		Cisco Unified CM adds the PAI header, if SIP Trunk is configured with Asserted-Type=PAI or Asserted-Type=Default and when the call control in Cisco Unified CM provides the screening indication of UserProvided "VerifiedAndPassed" or NetworkProvided.
		Table 1-14 UPDATE Message Fields (continued)
		Field Example Notes

P-Preferred-Identity	`IPv4 Example`
	`P-Preferred-Identity: "Alice" <sip: 4762424@172.18.199.211>`
	`IPv6 Example`
	`P-Preferred-Identity: "Alice" <sip: 4762424@[2001:db8:1:101::12]>`	

Field	Example	Notes
		Cisco Unified CM uses this header for conveying the Connected Name/Number. Cisco Unified CM adds the PPI header, if SIP Trunk is configured with Asserted-Type=PPI or Asserted-Type=Default and when the call control in Cisco Unified CM provides the screening indication of "Not Screened" or "VerifiedAndFailed" values. PPI header values are displayed as per the user configuration.
Resource-Priority	`Resource-Priority: DRSN.9`	If the MLPP feature is enabled, Resource-Priority header is added to the UPDATE message.

Geolocation	`Geolocation: cid-url;inserted-by=hostport`
	Example:
	`Geolocation: <cid:4900@10.10.10.10>;inserted-by="10.10.10.10`
		SIP Trunk only supports sending and processing of cid-url in Geolocation header, though specification allows SIP, SIPS & pres URI's.

SUBSCRIBE

Table 15: SUBSCRIBE Message Fields

Field	Example	Notes
Request-Line	SUBSCRIBE sip:subscribee@destIP:destPort SIP/2.0	destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV.

Field	Example	Notes
From	From: "callerName" <sip:cgpn@CCM_IP_addr>	callerName=caller display i.e. IP phone Cgpn = calling party number CCM_IP_addr=CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.
To	To: "calledName"<sip:cdpn@destIP>	calledName is included if available destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	Via:SIP/2.0 IP addr:Port;Branch=nu mber	IP addr=CCM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=CCM Port Branch=Unique number
Call-ID	Call-ID: number@CCM IP addr	Cisco Unified CM generates this number internally.
Contact	Contact: <sip:cgpn@CCM_IP_addr:localPort;user=phone>	localPort = configured "Incoming port" of the indicated SIPTrunk
Cseq	Cseq:number method	Number=a traditional sequence number that is incremented for each new request within a dialog Method=SUBSCRIBE
Expires	Expires: number	Number = The duration of the subscription, in seconds.

Field	Example	Notes
Max-Forwards	Max-Forwards:number	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop by sip proxy.
Event:	kpml, presence	The Event Type that the Subscribe if for. Unified CM supports kpml and presence event packages.
Content-Type:	application/kpml-request+xml or message/sipfrag;version=2.0	Unified CM SIP Trunk supports message/sipfrag;version=2.0, application/kpml-request+xml and application/pidf+xml

NOTIFY

Table 16: NOTIFY Message Fields

Field	Example	Notes
Request-Line	NOTIFY sip:subscriber@destIP:destPort SIP/2.0	destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV;
From	From: "callerName" <sip:cgpn@CCM_IP_addr>	callerName=caller display i.e. IP phone Cgpn = calling party number CCM_IP_addr=CCM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.

Field	Example	Notes
To	To: "calledName"<sip:cdpn@destIP>	calledName is included if available destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP. If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	Via:SIP/2.0 IP addr:Port;Branch=nu mber	IP addr=CCM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate CCM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=CCM Port Branch=Unique number
Call-ID	Call-ID: number@CCM IP addr	Number is generated internally by Cisco Unified CM.
Contact	Contact: <sip:cgpn@CCM_IP_addr:localPort>	localPort = configured "Incoming port" of the indicated SIPTrunk
Cseq	Cseq:number method	Number=a traditional sequence number that is incremented for each new request within a dialog Method=NOTIFY
Subscription-State:	Subscription-State:state-value; expires=number	State-value=active|pending|terminated Expires= authoritative subscription duration.
Max-Forwards	Max-Forwards:number	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop by SIP proxy.
Event	kpml, presence	The Event Type that the Subscribe if for. Cisco Unified CM supports kpml and presence event packages.

Field	Example	Notes
Content-Type:	application/kpml-request+xml or message/sipfrag;version=2.0	Cisco Unified CM SIP Trunk supports message/sipfrag;version=2.0, application/kpml-request+xml and application/pidf+xml

PUBLISH

Table 17: PUBLISH Message Fields

Field	Example	Notes
Request-Line	PUBLISH sip:user@destIP:destPort SIP/2.0	user=end user name associated with a line appearance; destIP = resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV;
From	From: <sip:user@CCM_IP_addr>	user=end user name associated with a line appearance; CCM_IP_addr=Cisco Unified CM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate Cisco Unified CM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets.
To	To: <sip:user@destIP>	user=end user name associated with a line appearance; destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.

Field	Example	Notes
Via	Via:SIP/2.0 IP addr:Port;Branch=nu mber	IP addr=Cisco Unified CM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate Cisco Unified CM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=Cisco Unified CM Port Branch=Unique number
Call-ID	Call-ID: number@CCM IP addr	Cisco Unified CM generates the number internally.
Cseq	Cseq:number method	Number=a traditional sequence number that is incremented for each new request within a dialog Method=PUBLISH
Max-Forwards	Max-Forwards:number	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop by sip proxy.
Event	presence	Cisco Unified CM supports presence event for PUBLISH.
Expires	Expires: number	number=suggested expiration time for PUBLISH in seconds. Default is 3600.
Content-Type:	application/pidf+xml	

OPTIONS

Table 18: OPTIONS Message Fields

Field	Example	Notes
Request-Line	OPTIONS sip:destIP:destPort SIP/2.0	destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk, it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets. destPort=configured destPort or resolved port from DNS SRV;
From	From: <sip:CCM_IP_addr>;tag=number	CCM_IP_addr=Cisco Unified CM IP address (Depending on if this is a IPv4 or an IPv6 call, the appropriate Cisco Unified CM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Tag=unique number
To	To: <sip:destIP>	destIP=resolved IP address of configured DestAddr/DestAddrIPv6 under SIPTrunk; it could also be FQDN SRV instead of destIP; If the address is an IPv6 address then it will be specified within [ ] square brackets.
Via	Via:SIP/2.0/Transport_type IP addr:Port;Branch=number	Transport_type=TCP or UDP. IP addr=Cisco Unified CM IP (Depending on if this is a IPv4 or an IPv6 call, the appropriate Cisco Unified CM IP Address will be used) If the address is an IPv6 address then it will be specified within [ ] square brackets. Port=Cisco Unified CM Port Branch=Unique number
Call-ID	Call-ID: number@CCM IP addr	Cisco Unified CM generates the number internally..

Field	Example	Notes
Cseq	Cseq:number method	Number=a traditional sequence number that is incremented for each new request within a dialog Method=OPTIONS
Max-Forwards	Max-Forwards:0	Number= Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop by sip proxy.

Response Messages

18x

Table 19: 18X Message Fields

Field	Example	Notes
Remote-Party-Id	IPv4 Example Remote-Party-ID:"Bob Jones" <sip:9728135111@161.44.147.67; user=phone>; party=called;screen=no;privacy=off IPv6 Example Remote-Party-ID:"Bob Jones" <sip:9728135111@[2001:db8:1:101::12]; user=phone>; party=called;screen=no;privacy=off	Cisco Unified CM uses this SIP extension to convey Connected Name and ID information.
P-Asserted-Identity	IPv4 Example P-Asserted-Identity: "Alice" <sip:4762424@172.18.199.211> IPv6 Example P-Asserted-Identity: "Alice" <sip:4762424@[2001:db8:1:101::12]>	Cisco Unified CM uses this header for conveying the Alerting Name/Number. Cisco Unified CM adds the PAI header, if SIP Trunk is configured with Asserted-Type=PAI or Asserted-Type=Default and when the call control in Cisco Unified CM provides the screening indication of UserProvided "VerifiedAndPassed" or NetworkProvided. PAI header values are displayed as per the user configuration.
P-Preferred-Identity	IPv4 Example P-Preferred-Identity:"Alice" <sip: 4762424@172.18.199.211> IPv6 Example P-Preferred-Identity:"Alice" <sip: 4762424@[2001:db8:1:101::12]>	Cisco Unified CM uses this header for conveying the Alerting Name/Number. Cisco Unified CM adds the PPI header, if SIP Trunk is configured with Asserted-Type=PPI or Asserted-Type=Default and when the call control in Cisco Unified CM provides the screening indication of "Not Screened" or "VerifiedAndFailed" values. PPI header values are displayed as per the user configuration.
Content-Disposition	Signal;handling=optional	Added only when QSIG tunneling is enabled.
SDP		

Field	Example	Notes

	`m=audio 30844 RTP/AVP 0 101`
	`a=rtpmap:0 pcmu/8000`
	`a=rtpmap:101 telephone-event/8000`
	`a=fmtp:101 0-11`
		If a call resulted in early media setup (that is, a SIP to MGCP PRI call), Cisco Unified CM includes SDP answer in 183 message.

QSIG	`Binary content`	If QSIG tunneling is enabled on the SIP tunk, then 183 message will have tunneled PROGRESS, ALERT, or DISCONNECT/RELEASE/COMPLETE message. Cisco Unified CM always tunnels PROGRESS only. Other messages are tunneled when interworking with the IOS SIP gateway.

2xx

Table 20: 2XX Message Fields

Field	Example	Notes
Remote-Party-Id	IPv4 Example Remote-Party-ID:"Bob Jones" <sip:9728135111@161.44.147.67;user=phone>; party=called;screen=no;privacy=off IPv6 Example Remote-Party-ID:"Bob Jones" <sip:9728135111@[2001:db8:1:101::12];user=phone>; party=called;screen=no;privacy=off	Cisco Unified CM uses this SIP extension to convey Connected Name and ID information.
P-Asserted-Identity	IPv4 Example P-Asserted-Identity:"Alice" <sip:4762424@172.18.199.211> IPv6 Example P-Asserted-Identity:"Alice" <sip:4762424@[2001:db8:1:101::12]>	Cisco Unified CM uses this header for conveying the Connected Name/Number. Cisco Unified CM adds the PAI header, if SIP Trunk is configured with Asserted-Type=PAI or Asserted-Type=Default and when the call control in Cisco Unified CM provides the screening indication of UserProvided "VerifiedAndPassed" or NetworkProvided. PAI header values are displayed as per the user configuration.
P-Preferred-Identity	IPv4 Example P-Preferred-Identity:"Alice" <sip: 4762424@172.18.199.211> IPv6 Example P-Preferred-Identity:"Alice" <sip: 4762424@[2001:db8:1:101::12]>	Cisco Unified CM uses this header for conveying the Connected Name/Number. Cisco Unified CM adds the PPI header, if SIP Trunk is configured with Asserted-Type=PPI or Asserted-Type=Default and when the call control in Cisco Unified CM provides the screening indication of "Not Screened" or "VerifiedAndFailed" values. PPI header values are displayed as per the user configuration.
Content-Disposition	Signal;handling=optional	Added only when QSIG tunneling is enabled.
QSIG	Binary content	If QSIG tunneling is enabled on the SIP tunk, then 200 OK response will have tunneled CONNECT.

3xx

3xx responses give information about the new user location or about alternative services that might be able to satisfy the call.

Field	Example	Notes
Status Code	`SIP/2.0 302 Moved Temporarily`	The requesting client SHOULD retry the request at the new address(es) given by the Contact header field.

From	`IPv4 Example`
	`From:<sip: 1101@10.89.79.20 3>;tag=16777234`
	
	`IPv6 Example`
	
	`From:<sip: 1101@[2001:db8:1:101::12]>;tag=16777234`
		10.89.79.203 is CCM IPv4 address
		2001:db8:1:101::12 is CCM IPv6 Address
		16777234 is the Call Id

To	`IPv4 Example`
	
	`To:<sip:30000@10.89.73.75>; tag=0002fd06e9300108228d58c1 -614f99be`
	
	`IPv6 Example`
	
	`To: <sip:30000@ [2001:db8:1:2::12]>; tag=0002fd06e9300108228d58c1-614f99be`
		3000 is the Calling Party Number

Via	`IPv4 Example`
	
	`Via: SIP/2.0/TCP 10.89.79.20 3:5060;received=10.89.79.203 ;branch=z9hG4bKfe8d27ec`
	
	`IPv6 Example`
	
	`Via: SIP/2.0/TCP [2001:db8:1:101::12]:5060; branch=z9hG4bKfe8d27ec`
		10.89.79.203=CCM IPv4 Address
		2001:db8:1:101::12 is CCM IPv6 Address
		5060=CCM Port
		Branch=Unique number

Contact	`IPv4 Example`
	`Contact: <sip:30000@10.8.69.115:5060>`
	`IPv6 Example`
	`Contact: <sip:30000@[2001:db8:1:101::12]:5060>`
		localPort = configured "Incoming port" of the indicated SIPTrunk

4xx

4xx responses represent definite failure responses from a particular server.

Table 21: 4XX Message Fields

Field	Example	Notes
Status Code	SIP/2.0 487 Request Cancelled	The request was terminated by a BYE or CANCEL request.

Field	Example	Notes
From	IPv4 Example From: <sip: 1101@10.89.79.203>;tag=16777234 IPv6 Example From: <sip: 1101@[2001:db8:1:101::12]>;tag=16777234	10.89.79.203 is CCM IPv4 address 2001:db8:1:101::12 is CCM IPv6 Address 16777234 is the Call Id
To	IPv4 Example To: <sip:30000@10.89.73.75>; tag=0002fd06e9300108228d58c1-614f99be IPv6 Example To: <sip:30000@ [2001:db8:1:2::12]>; tag=0002fd06e9300108228d58c1-614f99be	3000 is the Calling Party Number.
Via	IPv4 Example Via: SIP/2.0/TCP 10.89.79.203:5060; received=10.89.79.203;branch=z9hG4bKfe8d27ec IPv6 Example Via: SIP/2.0/TCP [2001:db8:1:101::12]:5060; branch=z9hG4bKfe8d27ec	10.89.79.203=CCM IPv4 Address 2001:db8:1:101::12 is CCM IPv6 Address 5060=CCM Port Branch=Unique number
Contact	IPv4 Example Contact: <sip:30000@10.8.69.115:5060> IPv6 Example Contact: <sip:30000@[2001:db8:1:101::12]:5060>	localPort = configured "Incoming port" of the indicated SIPTrunk
Content-Disposition	Signal;handling=optional	Added only when QSIG tunneling is enabled.
QSIG	Binary content	If QSIG tunneling is enabled on the SIP tunk, then 4xx response will have tunneled RELEASE/REL COMP.

5xx

The server encountered an unexpected condition that prevented it from fulfilling the request.

Table 22: 5XX Message Fields

Field	Example	Notes
Status Code	SIP/2.0 501 Not Implemented	This is the appropriate response when a UAS does not recognize the request method
From	IPv4 Example From: <sip: 1101@10.89.79.203>;tag=16777234 IPv6 Example From: <sip: 1101@[2001:db8:1:101::12]>;tag=16777234	10.89.79.203 is CCM IPv4 address 2001:db8:1:101::12 is CCM IPv6 Address 16777234 is the Call Id

Field	Example	Notes
To	IPv4 Example To: <sip:30000@10.89.73.75>; tag=0002fd06e9300108228d58c1-614f99be IPv6 Example To: <sip:30000@ [2001:db8:1:2::12]>; tag=0002fd06e9300108228d58c1-614f99be	3000 is the Calling Party Number
Via	IPv4 Example Via: SIP/2.0/TCP 10.89.79.203:5060; received=10.89.79.203;branch=z9hG4bKfe8d27ec IPv6 Example Via: SIP/2.0/TCP [2001:db8:1:101::12]:5060; branch=z9hG4bKfe8d27ec	10.89.79.203=CCM IPv4 Address 2001:db8:1:101::12 is CCM IPv6 Address 5060=CCM Port Branch=Unique number
Contact	IPv4 Example Contact: <sip:30000@10.8.69.115:5060> IPv6 Example Contact: <sip:30000@[2001:db8:1:101::12]:5060>	localPort = configured "Incoming port" of the indicated SIPTrunk
Content-Disposition	Signal;handling=optional	Added only when QSIG tunneling is enabled.
QSIG	Binary content	If QSIG tunneling is enabled on the SIP tunk, then 5xx response will have tunneled RELEASE/REL COMP.

6xx

6xx indicates that the callee end system was contacted successfully but the callee is busy and does not want to take the call at this time.

Table 23: 6XX Message Fields

Field	Example	Notes
Status Code	SIP/2.0 600 Busy Everywhere	The callee end system was contacted successfully, but the callee is busy and does not want to take the call at this time.
From	IPv4 Example From: <sip: 1101@10.89.79.203>;tag=16777234 IPv6 Example From: <sip: 1101@[2001:db8:1:101::12]>; tag=16777234	10.89.79.203 is CCM IPv4 address 2001:db8:1:101::12 is CCM IPv6 Address 16777234 is the Call Id
To	IPv4 Example To: <sip:30000@10.89.73.75>; tag=0002fd06e9300108228d58c1-614f99be IPv6 Example To: <sip:30000@ [2001:db8:1:2::12]>; tag=0002fd06e9300108228d58c1-614f99be	3000 is the Calling Party Number

Field	Example	Notes
Via	IPv4 Example Via: SIP/2.0/TCP 10.89.79.203:5060; received=10.89.79.203;branch=z9hG4bKfe8d27ec IPv6 Example Via: SIP/2.0/TCP [2001:db8:1:101::12]:5060; branch=z9hG4bKfe8d27ec	10.89.79.203=CCM IPv4 Address 2001:db8:1:101::12 is CCM IPv6 Address 5060=CCM Port Branch=Unique number
Contact	IPv4 Example Contact: <sip:30000@10.8.69.115:5060> IPv6 Example Contact: <sip:30000@[2001:db8:1:101::12]:5060>	localPort=configured “Incoming port” of the indicated SIPTrunk

Message Timers

The following timers are service parameters that are configurable in Cisco Unified CM Administration. Cisco Unified CM maintains the following configuration data for the SIP timers.

Table 24: Message Timers

Timer	Value(Default/range)	Definition
trying	500 ms/100–1000 ms	The time to wait for a 100 response to an INVITE request.
connect	500 ms / 100–1000 ms	The time to wait for a 200 response to an ACK request.
disconnect	500 ms / 100–1000 ms	The time to wait for a 200 response to a BYE request.
expires	3 min/ 1–5 min	Limits the time duration for which an INVITE is valid.
rel1xx	500 ms / 100–1000 ms	The time that Cisco Unified CM should wait before retransmitting the reliable 1xx responses.
prack	500 ms / 100–1000 ms	The time that Cisco Unified CM should wait before retransmitting the PRACK request.
notify	500 ms / 100–1000 ms	The time that Cisco Unified CM should wait before retransmitting the Notify message.
publish	500 ms / 100–1000 ms	The time that Cisco Unified CM should wait before retransmitting the Publish message.

Timer	Value(Default/range)	Definition
options	500 ms / 100–1000 ms	The time that Cisco Unified CM should wait before retransmitting the Options message.

Message Retry Counts

All the following retry counts are service parameters that are configurable in Cisco Unified CM Administration. Cisco Unified CM maintains the following configuration data for the SIP retries. In case of TCP transportation type, the timers will still pop as usual; however, in the event of timeout, Stack does not retransmit; it will instead rely on TCP itself to do the retry.

Table 25: Message Retry Counts

Counter	Default Value	Suggested Range	Definition
Invite retry count	5	1 – 10	Number of INVITE retries
Response retry count	6	1 – 10	Number of RESPONSE retries
Bye retry count	10	1 – 10	Number of BYE retries
Cancel retry count	10	1 – 10	Number of CANCEL retries
PRACK retry count	6	1 – 10	Number of PRACK retries
Rel1xx retry count	10	1 – 10	Number of Reliable 1xx response retries
Notify retry count	6	1 – 10	Number of NOTIFY retries
Publish retry count	6	1 – 10	Number of PUBLISH retries
Options retry count	6	1 – 10	Number of OPTIONS retries

SIP Status Code To Q.850 Cause Code Mapping

Table 26: SIP Status Code to Q.850 Cause Code Mapping, on page 49 lists the SIP Status Codes and maps them to the Q.850 Release Cause Codes.

Table 26: SIP Status Code to Q.850 Cause Code Mapping

SIP Status Code	Q.850 Cause Code	Q.850 Release Cause Description	Scenarios when generated by Cisco Unified CM (due to internal errors)
404 Not Found 485 Ambiguous 604 Does not exist anywhere	1 Unallocated (unassigned) number	Indicates that the destination requested by the calling user cannot be reached because the number is unassigned.	The number is not in the routing table, or it has no path across the ISDN network.
486 Busy here 491 Request pending 493 Undecipherable 600 Busy everywhere	17 User busy	Indicates that the called party cannot accept another call because the user busy condition has been encountered. Either the called user or the network can generate this cause value. In the case of a user-determined user busy, be aware that the user equipment is compatible with the call.	User is already using the telephone.
480 Temporarily unavailable	18 No user responding	Used when the called party does not respond to a call establishment message with either an alerting or connect indication within the time allotted. The number that is being dialed has an active D-channel, but the far end chooses not to answer.	The user does not answer the telephone.

SIP Status Code	Q.850 Cause Code	Q.850 Release Cause Description	Scenarios when generated by Cisco Unified CM (due to internal errors)
401 Unauthorized 402 Payment Required 403 Forbidden 407 Proxy Authentication Required 600 Decline	21 Call rejected	Indicates that the equipment sending this cause code does not want to accept this call, although it could accept the call because the equipment sending the cause is neither busy nor incompatible. The network might also generate this code to indicate that the call was cleared because of a supplementary service constraint. The diagnostic field might contain additional information about the supplementary service and reason for rejection.	A subscriber has a service constraint that does not accept this call.
410 Gone	22 Number changed	Returned to a calling party when the called number that is indicated by the calling party is no longer assigned. This diagnostic field might optionally contain the new called party number.	A subscriber changed their number.
482 Loop detected 483 Too many hoops	25 Exchange routing error	Indicates that the destination indicated by the user cannot be reached because an intermediate exchange released the call due to reaching a limit in executing the hop counter procedure.	The network is overloaded.
484 Address incomplete	28 Invalid number format	Indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.	The caller calls out by using a network type number (enterprise) rather instead of Unknown or National.

SIP Status Code	Q.850 Cause Code	Q.850 Release Cause Description	Scenarios when generated by Cisco Unified CM (due to internal errors)
487 Request terminated 488 Not acceptable here 606 Not acceptable	31 Normal unspecified	Reports a normal event only when no other cause in the normal class applies.	Normal operation
502 Bad gateway	38 Network out of order	Indicates that the network is not functioning correctly and that the condition is likely to last for an extended time .	Network failure
400 Bad Request 481 Call leg does not exist 500 Server internal error 503 Service Unavailable	41 Temporary failure	Indicates that the network is not functioning correctly and that the condition is likely to be resolved quickly.	Network failure
405 Method not allowed	63 Service or option not available, unspecified	Reports a service or option as a not available event only when no other cause in the service or option not available class applies.	Service not available
406 Not acceptable 415 Unsupported media type 501 Not implemented	79 Service or option not implemented, unspecified	Reports a service or option as a not implemented event only when no other cause in the service or option not implemented class applies.	Service not implemented
408 Request timeout 504 Server timeout	102 Recovery on timer expiry	Indicates that the expiration of a timer in association with error handling procedures initiated the procedure.	• No H.323 call proceeding • No H.323 alerting or connect message received from the terminating gateway • Invite expires timer reached maximum number of retries that are allowed.

SIP Status Code	Q.850 Cause Code	Q.850 Release Cause Description	Scenarios when generated by Cisco Unified CM (due to internal errors)
411 Length required 413 Request entity too long 414 Request URI too long 416 Unsupported URI scheme 420 Bad extension 421 Extension required 423 Interval too brief 505 SIP version not supported 513 Message too large	127 Internal error, unspecified	CC_CAUSE_INTERWORKING Indicates that interworking occurred with a network that does not provide causes for actions that it takes. The precise cause cannot be ascertained.	Failed to send message to Public Switched Telephone Network (PSTN).

SIP Trunk Supported Features

This section provides details with respect to overall flow and handling of basic SIP trunk features. This includes, but is not limited to, the following features:

- Identification Services
- Basic Call
- Simple Hold/Resume
- Transfer
- Enhanced Click-to-Dial
- Conference
- Call Forwarding
- Message Waiting Indication
- Endpoint 302 Redirect
- Park and Retrieve
- Video
- T38 Fax
- Presence (Busy Lamp Field)
- Out-of-band DTMF using KPML
- SIP Over TLS Connection

- Call Preservation
- Outbound PUBLISH
- Click-to-Call
- Monitoring and Recording
- SIP Trunk Device Identification
- Click-to-conference
- G.729 with MTP
- PAI/PPI
- SRTP
- G.Clear
- MLPP
- V.150.1
- SIP T38 Fax Interoperability with Microsoft Exchange
- MMoH
- Location based CAC
- IPv6
- Calling Party Number Transformations
- Logical Partitioning
- Early Offer G.Clear
- SRTP over non-secure SIP Trunks
- End to End Preconditions
- Connected Party Number Transformation
- Secure Monitoring and Recording
- End to end call tracing
- Q.735 MLPP over SIP Trunk
- SIP OPTIONS Ping
- Static Call Routing
- SIP Header Enhancements for Recordings
- Third Party HD video support
- Early Offer Support for SIP Trunk
- QSIG Tunneling over SIP
- SIP Refer Transparency for CVP
- BFCP support

- Cisco Telepresence MCU integration as Unicast Audio / Video mixer
- VCS integration
- Cisco Unified CM Video - SIP Video Encryption
- Cisco Unified CM G.722.1 codec support
- Cisco Unified CM AAC-LD MP4A-LATM codec support on SIP
- Cisco Unified CM V.150.1 MER

Identification Services

This section describes the SIP Identification Services in Cisco Unified CM. These services include Line Identification Services and Name Identification Services. Line Identification Services include Calling Line and Connected Line Presentation/Restriction. Name Identification Services include Calling Name and Connected Name Presentation/Restriction.

The following sections describe the options that Cisco Unified CM 6.1 and later provide for communication of identity and presentation information. The selection of these options is controllable through a SIP trunk configuration. You can use either or both options. If you select both, Asserted-Identity takes precedence over RPID.

- Using Remote-Party-ID Header, on page 54
- Using P-Asserted-Identity/P-Preferred-Identity and Privacy Header, on page 56

Using Remote-Party-ID Header

Cisco Unified CM provides flexible configuration options to provide these services on a call-by-call basis or statically preconfigured for each SIP trunk. This section does not describe those configuration options; it only provides the details on how Cisco Unified CM conveys these ID services in SIP by using the Remote-Party-ID header. Table 27: Support Levels for Various Parameters, on page 54 captures the support levels for the various parameters:

Table 27: Support Levels for Various Parameters

Parameter	Values	Notes
party	calling called	Ignored if received by Cisco Unified CM. Set to called for outgoing INVITE or UPDATE from Cisco Unified CM. Set to calling for outgoing responses from Cisco Unified CM.
id-type	subscriber user term	Ignored if received by Cisco Unified CM. Set to subscriber for outgoing requests and responses.

Parameter	Values	Notes
privacy	full name uri off	Supported if received by Cisco Unified CM. Cisco Unified CM also supports sending all values in either INVITE or UPDATE requests and responses for the same.
screen	no yes	Ignored if received by Cisco Unified CM. Cisco Unified CM always sends yes when generating an Remote-Party-ID header.

The following sections provide additional details:

- Calling Line and Name Identification Presentation, on page 55
- Calling Line and Name Identification Restriction, on page 55
- Connected Line and Name Identification Presentation, on page 56
- Connected Line and Name Identification Restriction, on page 56

Cisco Unified CM uses SIP “From” and “Remote-Party-ID” headers to provide ID services as described in the following sections.

Calling Line and Name Identification Presentation

Calling Line and Name Identification presentation services provide the connected party in a call with the name and number of the calling party. By default, the SIP trunk is configured to allow the name and number to be presented in the SIP header.

You can also configure a number or name restriction on the SIP trunk. You may choose to present the name in the SIP header, while configuring a restriction on the number, or vice versa.

Calling Line and Name Identification Restriction

The following items provide examples of calling line and name identification restrictions:

- Name—When name is restricted, the display field (calling Name) in “From” header is set to a configurable string (that is, “Anonymous”). The display field in the “Remote-Party-ID” header still includes the actual name but the privacy field is set to “name”. For example:
  From: “Anonymous” <sip:9728135001@localhost> Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>; party=calling;screen=yes;privacy=name
- Number—When number is restricted, the calling Line is left out in the “From” header; however, it is still included in the “Remote-Party-ID” header with privacy=uri. For example:
  From: “Bob Jones” <sip: 9728135001@localhost> Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>; party=calling;screen=yes;privacy=uri

- Both Name and Number—When both name and number are restricted, the same principle applies with privacy=full:
  From: “Anonymous” <sip: 9728135001@localhost> Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>; party=calling;screen=yes;privacy=full
- None—When both name and number are allowed, the following example applies:
  From: “Bob Jones” <sip: 9728135001@localhost> Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>; party=calling;screen=yes;privacy=off

Connected Line and Name Identification Presentation

The Connected Number (Line) and Name Identification supplementary service provides the calling user with the called (connected) user number and/or name.

Cisco Unified CM uses the “Remote-Party-ID” headers in 18x, 200 and re-INVITE or UPDATE messages to convey connected information. The “party” field of the “Remote-Party-ID” header is set to “called” (instead of “calling” for calling ID services).

Connected Line and Name Identification Restriction

Similar to Calling ID services, customers have option to restrict connected number and name independently.

- Name—When name is restricted, the connected name still gets included with privacy=name For example:
  Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>;
  party=called;screen=yes;privacy=name
- Number Restrict only—When number is restricted, the connected number still gets included with privacy=uri. For example:
  Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>;
  party=called;screen=yes;privacy=uri
- Both Name and Number Restrict—When both name and number are restricted, both get included with privacy=full. For example:
  Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>;
  party=called;screen=yes;privacy=full
- None—Both name and number are allowed.
  For example, if Cisco Unified CM receives an INVITE that is destined to extension 9728135001, Cisco Unified CM includes the called party name in 18x and 200 messages as follows:
  Remote-Party-ID: “Bob Jones”<9728135001@localhost; user=phone>;
  party=called;screen=yes;privacy=off

Using P-Asserted-Identity/P-Preferred-Identity and Privacy Header

Cisco Unified CM provides a flexible configuration options to provide these services based on a static configuration for each SIP Trunk. This section provides an overview of these configuration options and of how Cisco Unified CM conveys ID services in SIP protocol using the P-Asserted-Identity/P-Preferred-Identity and Privacy headers.

Table 28: Values for Various Parameters, on page 57 shows information about the Cisco Unified CM SIP trunk use and relevance of the various values for a “Privacy” header.

Table 28: Values for Various Parameters

Value	Notes
Header doesn't exist	The absence of Privacy header in an INVITE, UPDATE, 180, 183 or 200 message means that the presentation is allowed for name and number. In case of initial INVITE, the presentation information applies to calling party information. In the case of reINVITE, UPDATE, 180, 183, or 200 it applies to connected party information.
id	For outgoing INVITE: Used for specifying presentation restriction for Calling Party name/number. For outgoing re-INVITE, UPDATE, 180, 183, or 200: Used for specifying presentation restriction for Connected Party name/number. For incoming INVITE, UPDATE, 180, 183, or 200: Interpreted as presentation restriction for Connected Party name/number.
header	If present in an incoming SIP request (INVITE or UPDATE), interpreted as presentation restriction for Connected Party name/number. If present in an incoming SIP response, ignored (interpreted as presentation allowed).
user	If present in an coming SIP request (INVITE or UPDATE), interpreted as presentation restriction for Connected Party name/number. If present in an incoming SIP response, ignored (interpreted as presentation allowed).
none	For outgoing INVITE: Used for specifying presentation allowed for Calling Party name/number. For outgoing re-INVITE, UPDATE, 180, 183, or 200: Used for specifying presentation allowed for Connected Party name/number. For incoming INVITE, UPDATE, 180, 183, or 200: Interpreted as presentation allowed for Connected Party's name/number.

Value	Notes
critical	For outgoing INVITE/UPDATE, implies that privacy services requested for this message are critical and therefore, if these privacy services cannot be provided by the network, this request should be rejected. Additionally, the request should carry a Proxy-Require header containing the new option-tag “privacy.” Per rfc3323, the “critical” value is not set in outgoing responses. For incoming SIP messages (requests or Responses), Cisco Unified CM performs no specific handling for “critical” other than syntax verification.

Table 29: P-Asserted-Identity/P-Preferred-Identity Headers, on page 58 provides information about P-Asserted-Identity/P-Preferred-Identity.

Table 29: P-Asserted-Identity/P-Preferred-Identity Headers

Headers with value formats	Notes
P-Asserted-Identity: “name” SIPURI, tel:+DN	Comma separated headers. One SIP URI and one tel URI.
P-Asserted-Identity: “name” SIPSURI, tel:+DN	Comma separated headers. One SIPS URI and one tel URI.
P-Asserted-Identity: “name” SIPURI P-Asserted-Identity: tel:+DN	Multiple PAI headers.

The P-Asserted-Identity/P-Preferred-Identity headers are validated for syntactical correctness. If the format is not expected as per rfc3325, a “400 Bad Request” response is sent to the UAC and the request is dropped.

The format of P-Preferred-Identity header the same as that of P-Asserted-Identity header, so this section does not explicitly cover P-Preferred-Identity.

The identity information is communicated by using P-Asserted-Identity or P-Preferred-Identity headers. The presentation information is communicated by using Privacy header.

Various pages in Cisco Unified CM Administration (such as the route pattern and the translation pattern configuration pages) allow the configuration of calling number or name restrictions. The SIP trunk screen provides configuration options for the type of Identity (either Asserted or RPID). For Asserted-Identity, there is no option for allowing or restricting name/number separately (as RFC 3323 & RFC 3325 does not provide separate option for this configuration). Therefore, the SIP Privacy option applies to name and number (calling and connected). When SIP Privacy selection box set to Default, the presentation information that is received

from the upper layer (call control) is used by the SIP trunk for setting the presentation of name/number in outgoing SIP request and response messages.

The following sections provide additional details:

- Calling Line and Name Identification Presentation, on page 55
- Connected Line and Name Identification Presentation, on page 56

Outbound PUBLISH

Cisco Unified CM uses the PUBLISH method as the preferred mechanism to send IP phone presence information over a SIP trunk.. The main reason for using the PUBLISH method is the performance improvement over the SUBSCRIBE/NOTIFY mechanism used in previous releases.

- Cisco Unified CM sends presence information for the phones that it manages over a SIP trunk.
- Release 5.x uses the SUBSCRIBE/NOTIFY framework for the presence communication over a SIP trunk; Release 6.0(1) uses the SIP PUBLISH method for presence communication.
- Presence status in Release 5.x (SUB/NOT) applies on a per-directory-number basis. Presence status in Release 6.0(1) (PUBLISH) applies on a per-line-appearance basis.
- Line appearance maps to one directory number on a specific phone device. Thus, if two phones share the same directory number 1000, two line appearances exist: (phone1, 1000) and (phone2, 1000)
- The PUBLISH message has user association.
- The PUBLISH mechanism works with multiple partitions.
- Only two status possibilities exist for Busy/Idle in PUBLISH: “Busy” or “Idle.” (Release 5.x also supports “Available.”)
- DND Status gets published if it is turned on.
- Mobility support improves because the mobile number is in the PUBLISH message.
- Performance improvement: by using the SUBSCRIBE/NOTIFY framework, a refresh requires four messages with the PIDF body. Using the PUBLISH mechanism, a refresh requires two messages without the PIDF body.
- Release 6.0(1) includes a set of BAT tools to facilitate the upgrade from Release 5.x.

G.729 With MTP

In Cisco Unified CM 7.0, the SIP trunk allows early-offer calls (calls with pre-allocated MTP) to be initiated with low bandwidth codecs such as G.729. In previous releases, the SIP trunk supports only G711.a/ulaw with pre-allocated MTP. This feature is required for endpoints that do not support delayed media calls and that do not want to use the high bandwidth G.711 codec. This feature is turned off by default.

Software MTP on Cisco Unified CM does not support the G.729 codec. Therefore, this feature requires an external MTP/Xcoder device that supports the G29 coded to be configured.

G.729 has four variants. However, because there is no difference from the signaling perspective between G.729 and G.729a and between G.729b and G.729ab, the configuration menu for the preferred originating codec provides only show two options.

The two variants are not compatible with each other on the IOS MTP devices. Interworking with each other requires the presence of a transcoder that supports G.729 (annexb=no) to G.729 (annexb=yes) transcoding.

Cisco Unified CM treats an incoming call with G.729 with annexb=yes as an indication of all the 4 G.729 codec variants.

If MTP required is configured. The initial INVITE only contains an offer, if the trunk is able to reserve MTP/Xcoder resource. Otherwise the call is initiated as a Delayed Media call.

If the terminating side does not support the codec that is offered, the call is torn down and not tried as a delayed media call.

T38 Fax is supported with G.729 codec. However, the call will not switch back to an audio call after the fax transmission completes. This functionality is consistent with T38 Fax support with other codecs.

Mid-call codec switching from the UAS is supported if there is an Xcoder/MTP device that supports both the original codec and the new codec that is offered.

MLPP

The Multilevel Precedence and Preemption (MLPP) feature implementation is based on RFC4411 (Reason Header for Preemption Events) and RFC4412 (Resource Priority for SIP). MLPP supplementary services over SIP trunk are:

- Precedence Call Waiting
- Call Hold
- Call Transfer
- Call Forwarding
- Three-way Calling
- Call Pickup
- Hunt List

Resource Priority Header Overview

- Resource priority (RP) headers can be used in the following SIP messages: INVITE, UPDATE, REFER (in-dialogue only)
- Messages that contain RP header must mark message with the resource priority required tag: Require: resource-priority
- RP headers use either of the following formats:
  - Resource-Priority:<network-domain>.<priority-value>
  - Resource-Priority:<network-domain>-<precedence-domain>.<priority-value>
- RP Header precedence domain originates from the MLPP domain of the call. AMLPP domain of 000000 may or may not be present as it is the default MLPP domain and optional.

Preemption Reason Header Overview

Preemption reason headers are included in SIP messages that terminate existing dialogues.

The following text shows the format of the preemption reason header:
Reason: preemption;cause=<cause value>;text=<text string>

The following cause values are defined by RFC4411.

1 UA Preemption
2 Reserved Resources Preempted
3 Generic Preemption
4 Non-IP Preemption
5 Network Preemption

V.150.1 MOIP

ITU V.150.1 specifies the transport of modem communications, including modem relay and voice band data, over IP networks. For the SIP, this information is transmitted in the SDP by using the media capability sequence that is specified by RFC3407. The following example shows an SDP with MOIP data:

```
v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.152.50
s=SIP Call
c=IN IP4 172.18.154.236
t=0 0
m=audio 4000 RTP/AVP 0 8 18 118
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:8 PCMA/8000
a=ptime:20
a=rtpmap:18 G729/8000
a=ptime:20
a=rtpmap:118 v150fw/8000
a=sqn:0
a=cdsc: 1 audio udpsprt 120
a=cpar: a=sprtmap:120 v150mr/8000
a=sendonly
```

In this example, the dynamic payload type 118 is mapped to v150 modem relay using sprt channel 120. The MOIP SDP information is internally generated based on device type and is not configurable. The following values are always used and systems that need to interconnect must use these values:

- SPRT channel: 120
- Modem relay payload type: 118
- Voice band data payload type: 100

Note There is no Cisco Unified CM configuration to enable this feature or change the information that is signaled. When a V.150.1 capable device is registered with Cisco Unified CM, the V.150.1 capabilities are automatically signaled in the SDP when communicating over a SIP trunk.

SIP T.38 Interoperability with Microsoft Exchange

The feature provides Cisco Unified CM with an alternate way to signal the call party switching over to T.38 in SIP.

Cisco Unified CM and gateways use a consistent way to initiate T.38 over audio calls in H.323, SIP, MGCP. The current way of representation in protocol signaling indicates to switch the existing audio channel to an image channel for a T.38 facsimile, and the existing ports are normally reused. The signal also implies that the audio transmission is be terminated before establishing image channels for a facsimile.

Some third-party products such as Microsoft Exchange Server prefer switching an established audio call to T.38 by explicitly indicating that the existing voice channel is terminated/not wanted and another new channel is needed to transmit T.38 facsimile. Both ways of representation for T.38 fax relay in SIP conform to the standards suggested by ITU T.38 and RFC3264. However, Cisco Unified CM does not handle the Microsoft negotiation method so that the call fails to switch over to fax.

Cisco Unified CM continues to behave the same so that when an audio call is established and a call party sends out T.38 call request, Cisco Unified CM terminates the existing audio channels and re-establishes an image channel for facsimile. Therefore, the existing functionality/mechanisms for T.38 will not be changed. The change supports incoming SIP signal that is supported by Microsoft and provides a configurable option in Cisco Unified CM to initiate fax request in the new signaling context.

Cisco Unified CM accepts the context of SIP signaling suggested by Microsoft to switch an audio call to a T.38 facsimile. Specifically, the SIP mid-call INVITE signal specifies that the current audio channel will be terminated by setting the audio port number as 0. In the same signal, another SIP media line syntax will be included to indicate detailed capability of T.38 and its receiving channel. Cisco Unified CM interprets this message as request of T.38 request.

If a SIP INVITE signal indicates active audio and image channels, it is continuously treated as an audio call request and Cisco Unified CM ignores the fax capability. Cisco Unified CM does not support Audio + Image call.

However, the limitation does not affect MS interoperability request as MS also intends to terminate audio session before establishing image channel for T.38.

Besides accepting multiple m=line (audio+image line) syntax in SIP signal to switch a call to T.38, Microsoft provides a configurable parameter in the SIP profile to initiate outgoing SIP signal in multiple m=line with audio port as 0 to negotiate T.38 calls. This parameter is offered to the SIP trunk only. Therefore, when an Exchange server (a server from another vendor) has been registered as SIP trunk in Microsoft and the parameter is checked, the server receives SIP T.38 in multiple m=lines.

This interoperability support is in Cisco Unified CM only and Cisco Unified CM should continue to interact with Cisco SIP gateways with a signal image m=line for a T.38 request. Therefore, the configurable parameter should not be checked to any SIP trunk that is associated with Cisco gateways.

Although the new parameter can be checked in a SIP profile that is associated with a SIP ICT, you should avoid doing so as it does not offer any benefit for the call.

This interoperability support for MS Exchange should not change any existing behavior of T.38 calls in any VoIP protocols. In addition, this support should not affect any VoIP protocol interoperability. But the current T.38 limitations stated will remain.

Multicast MOH Over H.323/SIP Trunk

Currently, multicast MoH does not work fully as expected over SIP ICT trunk. Due to this, extra bandwidth used for each unicast MoH over the same ICT is wasted. This feature is to make multicast MoH work completely over SIP and H.323 ICT.

If the holding side is configured to use MMoH, multicast address is sent in SIP SDP message. If the other side supports MMoH, only then will it work. The new service parameter "Send Multicast MOH in H.245 OLC Message" does not apply for SIP ICT. MMoH works on tandem SIP/SIP and H.323/H.323 cases but not for SIP/H.323 interop scenarios.

IPv6

Cisco Unified CM has been enhanced to operate in both IPv4 only mode, or Dual Mode, i.e. IPv4_IPv6 mode. If IPv6 is enabled on Cisco Unified CM, then it behaves in Dual Mode, otherwise it behaves in IPv4 only mode.

SIP Trunk was one of the components on Cisco Unified CM that added support for IPv6. SIP Trunk via configuration can behave in IPv4 only mode, IPv6 only mode, or Dual Mode IPv4_IPv6.

The mode a trunk behaves is configured under the Common Device Configuration via setting the IP Addressing Mode. The default mode for a SIP Trunk is Dual Mode.

The IP Addressing Mode has three settings

- IPv4 only – The SIP Trunk uses the Cisco Unified CM IPv4 server address as its source address for SIP signaling and either, an MTP's, or Phone's IPv4 address for media.
- IPv6 only – The SIP Trunk uses the Cisco Unified CM IPv6 server address as its source address for SIP signaling and either, an MTP's, or Phone's IPv6 address for media.
- IPv4 and IPv6 – The SIP Trunk uses either the Cisco Unified CM IPv4 server address, or the Cisco Unified CM server IPv6 address as its source address for signaling and either, an MTP's IPv4 and/or IPv6 address, or the Phone's IPv4 and/or IPv6 address for media. If the trunk is configured in Dual Mode, then Cisco Unified CM will listen for SIP Traffic on both the IPv4 and IPv6 Interface.

For an IPv4 only trunk, the destination address will be populated with the remote peer's IPv4 address.

For an IPv6 only trunk, the destination IPv6 address field will be populated with the remote peer's IPv6 address.

For a dual mode trunk, both the Destination Address and the Destination v6 address fields are populated. If for some reason only one of the fields is populated, then the trunk will behave in only that mode. For a dual mode SIP Trunk, with both IP Addresses configured on the SIP Trunk device page, the enterprise parameter IP addressing mode Preference Control will dictate whether to use IPv4 or the IPv6 address for signaling.

For an IPv6 call, all the SIP URI's will use the following IPv6 address format (address enclosed in [ ] square brackets) as defined by RFC 3261

```
SIP-URI = "sip:" [ userinfo ] hostport
uri-parameters [ headers ]hostport
hostport = host [ ":" port ]
host = hostname / IPv4address / IPv6reference
IPv6reference = "[" IPv6address "]"
```

Example:

```
INVITE sip:25421@[2001:db8:1:2::12]:5083 SIP/2.0
```

Support for Alternative Network Address Types (ANAT) Over SIP Trunk

Cisco Unified CM supports ANAT over dual mode (IPv4_IPv6) SIP Trunks. ANAT allows for SIP devices to send both IPv4 and IPv6 addresses in the SDP body of a SIP Offer, and to return in the SDP body of the SIP Answer a preferred IP address (IPv4 or IPv6) with which to establish a media connection. ANAT is only supported over dual mode SIP Trunk and must be supported by both ends of the SIP Trunk.

Example ANAT Offer SDP

```
v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.199.129
s=SIP Call
t=0 0
a=group:ANAT 1 2
m=audio 18484 RTP/AVP 0 101
c=IN IP6 2001:db8:c18:1:21c:58ff:fe2a:23f8
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=mid:1
m=audio 18282 RTP/AVP 0 101
c=IN IP4 172.18.199.55
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=mid:2
```

ANAT is enabled by checking the "Enable ANAT" checkbox on the SIP Profile associated with the SIP Trunk. ANAT can be used with both Early Offer and Delayed Offer calls. ANAT should only be enabled on SIP Trunks with an IP Addressing Mode setting of IPv4 and IPv6.

The use of ANAT on a Dual Mode SIP Trunk is indicated in the header of the SIP Invite

- The field "Require: sdp-anat" is used by Cisco Unified CM SIP Trunks using Early Offer.
- The field "Supported: sdp-anat" is used by Cisco Unified CM SIP Trunks using Delayed Offer.
- The "require" sdp-anat value indicates to the far end of the SIP Trunk connection that an ANAT based response "must" be supported.
- The "supported" sdp-anat value indicates to the far end of the SIP Trunk connection that that an ANAT based response "should" be supported.

If ANAT is enabled it should be configured on both ends of the SIP Trunk, (If "require: sdp-anat" is sent in the SIP Invite and the receiving SIP Trunk does not support ANAT all calls will be rejected).

Inbound SIP Trunk Call Rules

- If IPv6 is not enabled on Cisco Unified CM and a call comes into Cisco Unified CM on IPv6 signaling, call is dropped with no response being sent to caller. The reason for this is that when IPv6 is disabled, Cisco Unified CM does not have any ports listening for IPv6 connections. The caller hears dead air.
- If IPv6 is enabled on Cisco Unified CM and a call comes into Cisco Unified CM with invalid mode, the call is rejected with an error being sent from Cisco Unified CM to caller.

  For example, in case IPv6_only trunk receives a call w/v4 signaling in INVITE, Cisco Unified CM sends a 503 response for that INVITE request. The caller hears fast busy tone.

Outgoing SIP Trunk Call Rules

- If IP addressing mode for SIP Trunk is set to IPv4_only and no IPv4 address is specified on the SIP Trunk configuration page, no call can be made from that sip trunk. Same is true for IPv6_only.
- If IP addressing mode for SIP Trunk is set to IPv6_only, IPv6 is chosen for signaling to send out INVITE. Same is true for IPv4_only.
- If IP addressing mode for SIP Trunk is IPv4_v6, signaling mode is chosen based on 'IP addressing mode preference for Signaling' and specified IP address on trunk configuration page. If preferred IP is not configured on trunk page then whatever is configured on SIP trunk is chosen.
- If IP addressing mode of SIP Trunk is set to IPv4_only and MTP Required is checked, IPv4 media is sent out in SDP if MTP is allocated. If no MTP is available, INVITE without SDP is sent.
- If IP addressing mode of SIP Trunk is set to IPv6_only and MTP Required is checked, IPv6 media is sent out in SDP If dual stack MTP is allocated. If no IPv4\IPv6 MTP is available, INVITE without SDP is sent.
- If IP addressing mode of SIP Trunk is set to IPv4_v6, and MTP Required is checked, a dual stack MTP is allocated if media preference is IPv6; Otherwise IPv4 MTP is allocated. If no MTP is available, the call is tried as a delayed media call.
- If IP addressing mode of SIP Trunk is set to IPv4_v6, and MTP Required is checked and a dual stack is allocated, SIP Trunk decides whether to send both IPv4 and IPv6 SDP or only IPv4 or only IPv6 SDP based on "ANAT Configuration" parameter.
- If ANAT is enabled both IPv4 and IPv6 SDP is sent with ANAT parameters set. Peer device can select one and that one is used for media for that call.
- If ANAT is disabled, SDP sent is based on media preference configured under Enterprise parameters.

Calling Party Number Transformations

The current design in Cisco Unified CM for globalizing on ingress and localizing on egress leaves very few holes that remain to be addressed.

The current design allows for prefixing digits to inbound calls based on ISDN number type. There is no way to manipulate the digits other than prefixing or stripping a fixed number of digits.

A problem that has come up in some of the early Alpha testing is that service providers are not consistently delivering numbering plan information correctly, leading to incorrect number manipulation because the calls are presented as unknown when they should be coming in as national or international. Unknown calls need to be transformed conditionally based on the digits presented and the current prefix/strip field does not offer a way to modify digits conditionally.

Also, SIP only has unknown numbering type, making it almost impossible to prefix anything that will apply to all the different numbers that may come in. This will be problematic for customers subscribing to SIP trunking services. Some of this problem can possibly be addressed if there is an SBC in the picture or the call is going to a SIP gateway by doing the manipulation on the SBC/Gateway, but the capabilities of the SBCs are questionable.

As part of this feature the prefix digits field is modified to allow stripping as well with a special notation (prefix:strip digits). However this is not very user friendly for an administrator.

To address these limitations, the following enhancements are being made:

- For all the current Incoming Calling Party Settings configuration sections on Gateway and Trunk configuration pages as well as Device Pool and Service Parameters, adding an option to configure Number of Digits to Strip in addition to the already available Prefix fields. This would replace the colon (:) notation that was added in Cisco Unified CM 7.0.
- Add the ability to configure a Transformation CSS on each of the above mentioned configuration pages as well. There will be a transformation CSS for each calling party number type to allow the ability to conditionally transform the calling party number based on number type.

For Globalization with this feature, three operations are possible to the Incoming Calling Party Number

- Strip - valid entries 0-24
- Prefix - maximum length is 16 digits
- Incoming Calling Party Transformation CSS which uses Calling Party Transformation patterns

It is recommended to use Strip & Prefix together as per the customer requirements. If conditional modifications are required then instead CSS can be used. There are not many cases where all 3 should be used together.

If all three are configured then the order in which these are applied are:

1. Strip
2. Prefix
3. CSS match and transformations applied

After the above feature changes, administrator is able to configure Prefix and Strip Digits at different levels and there was no sync at device, device pool and service parameter levels. In Cisco Unified CM 7.0, this issue was non-existant, as both the Prefix and Strip Digits, were configure in the Prefix field, using (Prefix: Strip digits) notation.

In addition to this, the Strip Digits and Transformation CSS field, by default had the NULL and <None> configuration.

In initial feature implementation, it was assumed that these default configuration for both Strip Digits and CGPN Transformation CSS, indicates that the call processing will use the values configured at the next level (Device Pool). Whereas, the Prefix field has the "Default" option, which implies that the call processing will use Prefix Digits, at the next level setting (Device Pool/Service Parameter).

So, ideally there's no way to indicate the call processing that, the user does not want to apply Strip Digits and CGPN Transformation CSS. Call processing will always go to the next level (Device Pool) and if nothing is configured at the next level, then no Strip Digits and CGPN Transformation CSS, will be applied.

Extra changes for this feature addressed these limitations in Cisco Unified CM 7.1(2) by:

- Adding "Use Device Pool Calling Party Transformation CSS" checkbox, associated with Incoming Calling Party Transformation CSS for National, International, Subscriber and Unknown number types.
- Database shouldn't allow Strip Digits to be configured, when the Prefix field is set to "Default".

Connected Party Number Transformation

The Cisco Unified CM's 6.0 & 7.0 releases added transformations support for the calling party and called party numbers by introducing the concept of "Calling Party Transformation Pattern" and "Called Party

Transformation Pattern". Depending upon UCM deployments, routing requirements, number presentation requirements & CDR requirements, these existing transformations allow the calling/called numbers to be transformed to globalized, localized etc formats.

For the incoming SIP Trunk calls on UCM, in the backwards direction signaling for ringing or connect messages, the UCM communicates the display number information of target destination's Directory Number or Route Pattern number. Currently, if required there is no provision on UCM for transforming the number, which is sent in backward direction of signaling.

- In IME (ViPR) UCM deployments, the requirement is for terminating cluster to communicate E164 number of the called or connected party in IME SIP Trunk communication. The internal numbers of the called enterprise may not be useful for communication across the enterprise.
- In Tandem/Leaf UCM cluster solutions which use Softswitch for PSTN Trunking, the requirement is for UCM to communicate DID number of the called or connected party in SIP Trunk communication. This is required for billing purpose etc.

To address these requirements, the proposal is to support mechanism to transform connected party number by performing transformations on the called/connected number before sending the display number in identity headers (PAI or RemotePartyId) of SIP messages on SIP Trunk.

This feature is going be useful for Cisco Unified CM deployments involving SIP Trunk and needing capability to communicate transformed number in identity headers of 180 Ringing, 200 OK and mid-call UPDATE/reINVITE messages. This would allow the calling endpoint in other Cisco Unified CM cluster, Voice Gateway or 3rd Party [IP]PBX to be able to display the alerting or connected number in format such as DID or E164 number.

For connected party transformations support, the SIP Trunk (all Service Types) is enhanced by adding following configurations:-

1. On SIP Trunk device configuration pages:-
   --Inbound Calls---------- --Connected Party Settings---------- -Connected Party Transformation CSS [DropDown] - [] Use Device Pool Connected Party Transformation CSS
2. On Device Pool configuration pages, new configuration for:-
   --Call Routing Information---------- --Connected Party Settings---------- - Connected Party Transformation CSS [DropDown]

Q.735 MLPP Over SIP Trunk

The Cisco Unified CM currently provides MLPP capability over the SIP Trunk for DSN/DRSN namespaces as defined by RFC4412; however it is geared to DoD requirements. The German Army uses MLPP based on I.255.3/Q.735.3 and Q.955.3. With this feature we will support the registered namespace Q735. As done for DSN/DSRN, UCM will continue using the "Resource-Priority" header as specified in RFC4412 to signal the call precedence using the values defined in the RFC. This has been covered in MLPP, page 1-46 of this document.

Call preemption will continue to be signaled using the preemption values for the SIP Reason header as specified by RFC4411 and as covered in MLPP, page 1-46. No changes are made in this area.

SIP OPTIONS Ping

Currently SIP trunk doesn't track the status of its remote destination peers. SIP trunk always sends (or tries to send) SIP request to the remote destination peer. If the remote destination peer is actually unavailable, the

call will not get dropped or failed over to another destination until the timeout happens. By default, it takes one minute to get a timeout. Users get nothing but silence during the time.

With the OPTIONS Ping feature, the Cisco Unified CM periodically sends SIP OPTIONS to every remote destination peer to detect its availability. If the remote destination peer is unavailable (no response or it responds "408 Request Timeout" or "503 Service Unavailable"), the Cisco Unified CM will mark this peer as unavailable. If the remote destination peer is available (any other responses other than "503" or "408"), Cisco Unified CM will mark this peer as available. The Cisco Unified CM will send a new INVITE only to the "available" remote destination peers.

Only a SIP trunk with a default type, "type None(default)", supports this feature. If FQDN or SRV is configured as a remote destination peer, Cisco Unified CM will send OPTIONS to all resolved IP addresses. The FQDN/SRV remote destination peer is marked as available if one or more of its resolved IP addresses are available. The FQDN/SRV remote destination peer is marked as unavailable if ALL of its resolved IP addresses are unavailable. The FQDN/SRV remote destination peer is marked as unavailable if DNS lookup failed.

Static Call Routing

One SIP trunk can have up to 16 destination addresses. The stack will randomly select one address to send out the SIP message. Also, the Cisco Unified CM will be able to handle the inbound messages from all those configured addresses.

Note The SIP OPTIONS Ping feature is an exception which is sent to all destination addresses.

SIP Header Enhancements for Recording

This feature enhances the From header in the SIP INVITE and UPDATE for recording. Now, the Cisco Unified CM sends both agent (nearend) and customer (farend) call information to the recorder. New data includes the farend refci, devicename, and address. This is more scalable since the recorder no longer requires a CTI connection to get the farend call information.

Third Party HD Video Support

The Cisco Unified CM mainly supports H.264 negotiation with Profile, Level and all the optional parameters specified in the H241 and RFC3984 specifications. The support of these parameters for SCCP protocol is limited to a small subset of these. However, Cisco Unified CM does not currently take notice of the signaled packetization modes from H323 endpoints. Also, RFC3984 is undergoing a revision and the current draft of RFC3984 bis-08 has added additional optional parameters and updated the semantics of the offer/answer negotiation, taking these parameters into account.

The additional parameters are:

- max-smbps
- sprop-level-parameter-sets
- use-level-src-parameter-sets
- in-band-parameter-sets

- sar-understood
- sar-supported
- max-recv-level
- level-asymmetry-allowed

The Cisco Unified CM does not currently support rtcp-fb attributes in SDP. Cisco Telepresence endpoints are being enhanced to use a new proprietary mux attribute in the SDP and Cisco Unified CM should allow this to be passed through in the offer and answer SDPs.

As a part of this feature enhancement we have added the support of the above mentioned 8 H264 attributes, rtcp-fb and the Cisco proprietary x-cisco-mux parameter.

The following is an example of Third Party HD video support:

```
m=video 20310 RTP/AVP 99
        c=IN IP4 10.13.5.196
        b=TIAS:1000000
        a=rtpmap:99 H264/90000
        a=fmtp:99 profile-level-id=42801E;
        max-recv-level=B00E;
        max-mbps=2000;
        max-br=1550;
        max-cpb=15;max-fs=512;
        max-smbps=1000;
        max-dpb=64;
        sprop-parameter-sets=Z0IACpZTBYmI,aMljiA==;
        max-rcmd-nalu-size=1024;
        sar-supported=16;
        sar-understood=124;
        packetization-mode=1
        a=rtcp-fb: 99 nack pli
```

These are no changes in any call flow, it would just have a few additional attributes in the SDP message as mentioned above.

QSIG Tunneling Over SIP

This feature adds support for tunneling QSIG messages in SIP on the trunk side. You can enable the feature by configuring tunneling on the sip trunk configuration page.

This feature makes SIP trunk on par with H323 ICT. Cisco Unified CM supports QSIG features like Call Transfer, Call Diversion, Call Completion, Path replacement, ID Services, and Message Waiting Indicator. One of the ways by which these features can be delivered between Cisco Unified CM clusters connected with SIP Intercluster trunk is by tunneling the QSIG content in SIP messages.

Table 30: QSIG and SIP Message Correspondence, on page 69 shows mapping of QSIG messages and the corresponding SIP messages.

Table 30: QSIG and SIP Message Correspondence

QSIG message	SIP Message
SETUP	INVITE
ALERTING	180 Ringing
PROGRESS	183 Session Progress

QSIG message	SIP Message
CONNECT	200 OK (INVITE)
CALL PROCEEDING	Not Tunneled
DISCONNECT	INFO
RELEASE	INFO
REL COMP	BYE
FACILITY	INFO

Secure Icon Enhancement over SIP Trunk

This enhancement provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, irrespective of the signaling transport.

A new drop-down list, Consider Traffic on this Trunk Secure, has been added to the Trunk Configuration window for SIP trunks. The drop-down list can be configured only when the sRTP Allowed check box is checked, and contains the following options:

- When using both sRTP and TLS
- When using only sRTP

When a user configures a SIP trunk to be secure when using both sRTP and TLS, the secure lock icon displays on the phone only if both sRTP and TLS are selected as the negotiated media and transport.

When a user configures a SIP trunk to be secure when using only sRTP, the SIP Trunk device layer does not take the device security mode into account, which would achieve H.323 parity. The secure lock icon displays on the phone if sRTP media is negotiated, irrespective of whether TCP, UDP, or TLS are negotiated as the transport protocol.

Overall call security must still depend on the SIP trunk and other parties in the call. Incoming call-Info header (over the SIP trunk) can still influence the overall secure status of the call.

Security Icon Support and BFCP

Secure media is supported for Audio, Video (main), and Video (presentation). Security is not supported for the BFCP media line. Cisco Unified CM 8.6 introduces Cisco CallManager service parameter, **Ignore BFCP Application Stream Encryption Status When Designating Call Security Status**, which indicates whether Cisco Unified CM considers the secure status of BFCP application stream when determining whether a call is designated secure. When this parameter is set to "True" (default value), calls utilizing a non-secured BFCP application stream will be treated as secure, provided that the remaining media streams in the call are secured.

Support for Image Attribute in SDP

This feature adds support for the SDP attribute, image attribute. Image attribute is a video media-level attribute to specify different image properties, such as the supported image size for sending and receiving video stream. For early offer, delayed offer, or split/join scenarios, Cisco Unified CM's answer will contain image attribute only if both party offer image attributes for the negotiated video payload. If both payload-specific (for example, imageattr:97) and all-payload (for example, imageattr:*) image attributes are offered in the same SDP for the negotiated codec, payload-specific image attribute is chosen. For early offer to early offer or mid-call reINVITES, image attribute transparently passes through to the second call leg. Same rules apply when MTP is part of the calling path.

Support for Initial INVITE Request-URI Parameter Passthrough

Request URI header parameters received in an initial INVITE are automatically relayed (transparently passed-through) in the corresponding outbound initial INVITE associated with the call.

Support for Blind Transfer Refer Parameter Passthrough

During a blind transfer operation, if any header parameters are included in the Refer-To header of the blind transfer REFER, those header parameters are automatically relayed in the corresponding outbound initial INVITE's requri header associated with the call.

Support for Contact Header Parameter Passthrough

Contact header parameters embedded in any of the below SIP messages received by Cisco Unified CM are automatically relayed (transparently passed-through) in subsequent applicable outgoing messages to the other endpoint involved in the two party call:

- INVITE (initial)
- 180 Ringing
- 183 Session Progress
- 200 for INVITE/reINVITE/UPDATE
- Mid-Call reINVITE
- UPDATE

The only exception to the above is with respect to the ";video" parameter. Cisco Unified CM will only relay this parameter if it believes the call to have negotiated the video.

MAX-FPS Attribute Support for H264 Codec

Max-fps is another H.264 optional parameter, and it is treated as a declarative parameter. This parameter will be passed transparently from one side to the other. This is the same behavior as all other H.264 optional parameters we supported in 8.5.

Sample SDP:

```
b=TIAS:128000
        a=rtpmap:97 H264/90000
        a=fmtp:97
        profile-level-id=42800D;max-mbps=40500;max-fs=1344;max-cpb=37;max-br=925;
        max-smbps=40500;max-fps=5440
        a=rtpmap:98 H264/90000
        a=fmtp:98
        profile-level-id=42800D;packetization-mode=1;max-mbps=40500;max-fs=1344;
        max-cpb=37;max-br=925;max-smbps=40500;max-fps=5440
```

AMR/AMR-WB Codec Support

GSM mobile uses the AMR or AMR-WB codecs for voice call. Generally, when a mobile user calls another mobile phone, the call would be established using the AMR codec end-to-end without requiring a transcoder. With the HEC solution, all HEC mobile calls are now routed via Cisco Unified CM first. However, UCM does not support AMR/AMR-WB codecs. Cisco Unified CM would ignore any codecs it does not understand. So for a HEC mobile call another mobile thru Cisco Unified CM, it would select the G711 codec instead of AMR. As a result, a transcoder is needed in the mobile network to convert from AMR to G711 and back out to AMR.

The AMR/AMR-WB codec support would eliminate the need for a transcoder for mobile to mobile calls in a HEC deployment.

Sample SDP Content of an offer with AMR & AMR-WB codec:

```
v=0
o=user1 53655765 2353687637 IN IP4 10.77.21.34
s=-
c=IN IP4 10.77.21.34
t=0 0
m=audio 49194 RTP/AVP 97 98 99
a=rtpmap:97 AMR/8000
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2; mode-change-neighbor=1
a=maxptime:20
a=rtpmap:98 AMR/8000
a=fmtp:98 mode-set=0,2,5,7; mode-change-period=2; mode-change-neighbor=1
a=maxptime:30
a=rtpmap:99 AMR-WB/16000/2
a=fmtp:99 mode-change-period=2; mode-change-neighbor=1
a=sendrecv
```

BFCP Support

The purpose of the Binary Floor Control Protocol (BFCP) is to enable presentation sharing between BFCP capable endpoints. BFCP support in Cisco Unified CM 8.6 strictly applies to SIP devices. Both SIP Trunk and SIP Line interfaces are fully supported. BFCP is supported on Early Offer (EO) and Delayed Offer (DO) SIP trunks. BFCP capabilities on a SIP Trunk or SIP Line can be turned on or off via SIP Profile Configuration. Cisco Unified CM's main task is to negotiate BFCP between endpoints via SIP SDP. Cisco Unified CM never terminates the BFCP protocol. BFCP protocol exchanges are between endpoints only.

In a normal call scenario with successful BFCP negotiation, the following media are negotiated via the SIP Protocol:

- Audio.
- Video (main).
- Video (presentation).
- BFCP Application Line

Audio is the audio stream.

Video (main) is the standard video stream (i.e. person to person).

Video (presentation) is the video from a presentation source such as a laptop connected to a BFCP capable phone.

BFCP Application Line is the control channel and is the media line used to perform the majority of the BFCP negotiation.

Note Cisco Unified CM and the BFCP capable SIP Phones negotiate the actual media via the SIP Protocol. However, in the BFCP call, all four media types travel from SIP Phone to SIP Phone.

In order for successful BFCP Presentation Sharing during a call, all SIP Interfaces for the call must have BFCP enabled. BFCP feature activation for a particular SIP Line or SIP Trunk interface is controlled by the **Allow Presentation Sharing using BFCP** checkbox within the SIP Profile. It is very important to note that BFCP Presentation sharing is disabled by default in the SIP Profile.

If the **Allow Presentation Sharing using BFCP** checkbox is unchecked (i.e. reject BFCP), then:

- Cisco Unified CM will not send an offer to the line or trunk endpoint containing the BFCP application media line or Presentation video line.
    - Note - a second video line is allowed if it isn't in the context of BFCP. This is for future use when non-BFCP applications utilize multiple video lines. Cisco Unified CM will know it's not in the context of BFCP if the BFCP Application line isn't present.
- Offers received by Cisco Unified CM with BFCP and Presentation Media Line will have those media lines rejected via media port if the media line set to zero.

As long as this checkbox is checked, Cisco Unified CM does not reject BFCP capabilities for that particular interface. However, BFCP must be enabled on all SIP interfaces in the call path for BFCP Presentation to work.

The new BFCP control line is an SDP Application line with the below example markings:
m=application 5070 UDP/BFCP *

UDP/BFCP indicates that the application being negotiated is BFCP using the UDP protocol. TCP/BFCP is not supported by Cisco Unified CM.

The following sections provide additional information:

- Secure Icon Enhancement over SIP Trunk, on page 70
- MTP, TRP, Transcoder and RSVP Agents, on page 74

Security Icon Support and BFCP

Secure media is supported for Audio, Video (main), and Video (presentation). Security is not supported for the BFCP media line. Cisco Unified CM 8.6 introduces Cisco CallManager service parameter, **Ignore BFCP Application Stream Encryption Status When Designating Call Security Status**, which indicates whether Cisco Unified CM considers the secure status of BFCP application stream when determining whether a call is designated secure. When this parameter is set to "True" (default value), calls utilizing a non-secured BFCP application stream will be treated as secure, provided that the remaining media streams in the call are secured.

MTP, TRP, Transcoder and RSVP Agents

In CUCM 8.6, when any of the following devices are inserted in any part of the BFCP call path, BFCP presentation sharing will not function:

- Media Termination Point (MTP)
- Trusted Relay Point (TRP)
- RSVP Agent
- Transcoder

If any of these devices are present in a BFCP call, the BFCP application media line will be zeroed as well as the secondary video line.

CUCM G.722.1 Codec Support

G.722.1 provides high quality, wideband audio codec at moderate bit rates of 24 or 32 kb/s. G.722.1 is supported for calls between two SIP devices or between two H.323 devices, and calls between SIP and H.323 devices.

Cisco Unified CM supports the following call scenarios:

- Calls between SIP devices with audio codec G.722.1 (Symmetric Dynamic Payload Number).
- Calls between SIP devices with audio codec G.722.1 (Asymmetric Dynamic Payload Number).MTP pass-through calls with audio codec G.722.1.
- MTP pass-through calls with audio codec G.722.1.
- E2E RSVP calls with audio codec G.722.1.
- Local RSVP calls with audio codec G.722.1.
- Calls across SIP trunk (configured as DO or EO) with audio codec G.722.1.
- Calls between SIP and H.323 devices with G.722.1 codec Dynamic Payload Number mismatching.

Note G.722.1Annex C is not supported.

Sample SDP Content of an offer with G.722.1 code:

```
m=audio 2366 RTP/AVP 100 101 9 8 0
        b=TIAS:32000
        a=rtpmap:100 G7221/16000
        a=fmtp:100 bitrate=32000
        a=rtpmap:101 G7221/16000
        a=fmtp:101 bitrate=24000
        a=rtpmap:9 G722/8000
        a=rtpmap:8 PCMA/8000
        a=rtpmap:0 PCMU/8000
        a=sendrecv
```

CUCM AAC-LD MP4A-LATM Codec Support on SIP

AAC-LD stands for Advanced Audio Coding-Low Delay, which is a super-wideband audio codec that provides superior sound quality for voice and music. This codec provides equal or improved sound quality over older codecs, even when using relatively lower bit rates.

There are 2 different RTP payload formats for this codec:

- **mpeg4-generic** (RFC 3640), used for MPEG-4 audio, video, and systems, has been supported for SIP in CUCM since version 6.0. Cisco TelePresence uses this variant.
- **MP4A-LATM** (RFC 3016). used for MPEG-4 audio, is supported for SIP starting from 8.5(1). Tandberg and most third parties use this variant.

Cisco Unified CM supports MP4A-LATM of the following bit rates: 128 kbps, 64 kbps, 56 kbps, 32 kbps, 24 kbps.

Cisco Unified CM supports the following call scenarios using the MP4A-LATM codec:

- Calls between SIP devices with audio codec MP4A-LATM (Symmetric Dynamic Payload Number).
- Calls between SIP devices with audio codec G.722.1 (Asymmetric Dynamic Payload number).
- MTP pass-through calls (including E2E RSVP and Local RSVP calls) with audio codec MP4A-LATM.
- Calls across SIP trunk (configured as DO or EO) with audio codec MP4A-LATM.

Note CUCM supports AAC-LD MP4A-LATM codec for SIP only.

The following is a sample SDP with MP4A-LATM codec parameters:

```
m=audio 2358 RTP/AVP 100 101 102 103 104 105 9 8 0
        b=TIAS:64000
        a=rtpmap:100 MP4A-LATM/90000
        a=fmtp:100 profile-level-id=25;object=23;bitrate=128000
        a=rtpmap:101 MP4A-LATM/90000
        a=fmtp:101 profile-level-id=24;object=23;bitrate=64000
        a=rtpmap:102 MP4A-LATM/90000
        a=fmtp:102 profile-level-id=24;object=23;bitrate=56000
        a=rtpmap:103 MP4A-LATM/90000
        a=fmtp:103 profile-level-id=24;object=23;bitrate=48000
        a=rtpmap:104 G7221/16000
        a=fmtp:104 bitrate=32000
        a=rtpmap:105 G7221/16000
        a=fmtp:105 bitrate=24000
        a=rtpmap:9 G722/8000
        a=rtpmap:8 PCMA/8000
        a=rtpmap:0 PCMU/8000
        a=sendrecv
```

SIP REFER Transparency

In earlier SME release, the way SME (or Cisco Unified CM) handles an incoming feature transfer request (via SIP Refer request) that is received on an active call leg is by acting on the transfer request and initiaing a new call to the transferred leg. (i.e SME/Cisco Unified CM processes the incoming SIP Refer request and processes the Refer-To header information and creates a brand new call to the number given in the Refer-To header.) Due to this behaviour, SME will always be involved in the call arc even if the endpoints are not geographically present near SME.

This SIP Refer Transparancy feature causes SME to transparently pass the transfer request across the call arc, instead of processing it locally, thereby allowing the local SME to be dropped completely from the triggered call being originated from the transferring party.

This behavior does not apply to transfer requests generated by line-side devices.

This feature applies only to SIP REFER requests received with the following characteristics

- in a SIP tandem trunk deployment. i.e both sides of call arc must be a SIPTrunk. One of the call leg cannot be a line or non-SIP signaling protocol.
- the REFER request is received within an existing dialog. Specifically, a 'blind' transfer feature invocation where the transfer-to party is 1st contacted by transferee.
- does not contain a Replaces tag, which has relevance only within the local user-agent (in this case SME/CUCM).
- the peer endpoint has advertised support for receiving REFER requests in the Allow: header received during call setup in either the INVITE request, or the 200 OK response to INVITE.
- Finally, a provided LUA script (refer-passthrough ua script) must be provisioned on the trunk on which the REFER request is received.

When SME/Cisco Unified CM receives an in-dialog incoming REFER (with no Replaces tag) and this feature is invoked by hitting the LUA script, and above said conditions are met, you will notice that SME/Cisco Unified CM will forward the incoming REFER message to the other side of the call arc. Any NOTIFY messages that are sent by the endpoint (in response to the forwarded REFER message indicated the progress of this transfer) will be forwarded by SME/Cisco Unified CM to the originating side (that initially sent the REFER request).

CUCM Video - SIP Video Encryption

Cisco Unified CM supports the following SIP Video Encryption features:

1. Support of new Crypto Suites and Session Parameters in the SDP
   a. Crypto suites - AES_CM_128_HMAC_SHA1_32,AES_CM_128_HMAC_SHA1_80, F8_128_HMAC_SHA1_80
   b. Crypto session parameters:
      a. Negotiated parameters - UNENCRYPTED_SRTP, UNENCRYPTED_SRTCP, UNAUTHENTICATED_SRTP
      b. Declarative parameters - KDR, FEC_ORDER, FEC_KEY, WSH
2. For SIP to Non-SIP calls, support AES_CM_128_HMAC_SHA1_32 only and no session parameters.
3. CUCM shall not support crypto lines with UNENCRYPTED_SRTP. Hence crypto lines containing UNENCRYPTED_SRTP (session negotiated parameter), will be removed from the offer before the crypto matching is done.
4. New Crypto Policy is supported for Audio, Video (main and 2nd) and FECC Lines. It is not supported for BFCP and T.38 fax lines.
5. For MTP pass thru and RSVP scenarios 2nd Video M Line and BFCP crypto is not supported.
6. Cisco Unified CM supports only first encryption key in the crypto line.
7. Added support for preferential selection of encryption algorithms for SIP to SIP calls

a Both Crypto Suite and Session parameters should match.

b Select the crypto algorithm based on lower sum of matched crypto positional indexes from the offered Crypto lines from both endpoints.

c Prefer 80 bit encryption algorithm in case of multiple matches with the same sum.

Sample SDP

```
v=0
o=tandberg 77 1 IN IP4 10.29.6.85
s=-
c=IN IP4 10.29.6.85
m=audio 16888 RTP/SAVP 100 101 102 9 18 11 8 0 103
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:g4bG4IwinJEgmkefTeR0rnueTcFF7UAQfhoSqCHd|2^48
UNENCRYPTED_SRTCP
a=sendrecv
m=video 16890 RTP/SAVP 97 98 99 34 31
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:2iYWKcuIrKp+IDyd1yQg3Le0J1SF7wPF5aCxl/uA|2^48
UNENCRYPTED_SRTCP
a=sendrecv
a=content:main
m=application 5070 UDP/BFCP *
a=floorctrl:c-s
m=video 16892 RTP/SAVP 97 98 99 34 31
b=TIAS:1152000
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:kGQ0bpXhtnH6Uwz48LUwZSXnOiata5pbYw+fsTpP|2^48
UNENCRYPTED_SRTCP
a=sendrecv
m=application 16894 RTP/SAVP 104
a=rtpmap:104 H224/4800
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:n+95fbtBmH+FzgZekfNbhRih2Ky9NQ4fiaP10xOe|2^48
UNENCRYPTED_SRTCP
a=sendrecv
Current Encryption Selection Policy in CUCM -
Offer from A:
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline :.............
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline :.............
Offer from B
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline :.............
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:.............
```

Result - CUCM will not consider any Algorithm other than AES_CM_128_HMAC_SHA1_32 inline for crypto line match. Therefore Cisco Unified CM picks the first crypto line match which is highlighted in green.

```
New Encryption Selection policy in CUCM -
Offer from A:
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:............. UNENCRYPTED_SRTCP
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.............
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.............
Offer from B:
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.............
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:............. FEC_ORDER=FEC_SRTP
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:............. UNENCRYPTED_SRTCP
```

In this example, there are two matches. When there is more than one match, the following rule shall be applied in selecting the crypto pair:

- Both Crypto Suite and Session parameters should match.
- Select the crypto algorithm based on lower sum of matched crypto indexes.
- Prefer 80 bit encryption algorithm in case of multiple matches with the same sum.

Result - second match has a lower sum value so Cisco Unified CM picks that match. The selected crypto lines shall be responded in the respective answer SDP.

```
1.crypto-lineIndex =1 (A) and crypto-lineIndex=3(B) ? sum of crypto line index values = 4
       2.crypto-lineIndex=2 (A) and crypto-lineIndex=1(B) ? sum of crypto line Index values
 = 3
```

V.150.1 MER

Modem relay as implemented according to standard SCIP-215/216 is referred to as V150 MER modem relay, MER is short for "Minimal Essential Requirements". SCIP is developed to provide end to end encrypted voice and data communication between terminals operating on heterogeneous networks.

V.150.1 MER enables the use of non-secure Modem over IP (MOIP) via modem-relay and audio passthrough as well as Fax over IP (FOIP) via T.38 v3. Note that although we say this is non-secure many cases may involve the endpoints themselves setting up their own encryption, such as with STEs. This implementation replaces legacy Griphus/Semper Fi V.150 and is backwards compatable with it.

Sample SDP content:

```
v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.154.43
s=SIP Call
c=IN IP4 172.18.155.77
t=0 0
m=audio 4000 RTP/AVP 0 8 18 101 100 118 126
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:8 PCMA/8000
a=ptime:20
a=rtpmap:18 G729/8000
a=ptime:20
a=sendonly
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15,32-35
a=rtpmap:100 X-NSE/8000 Optional Line: Indicates legacy VBD support
a=rtpmap:118 v150fw/8000
a=rtpmap:126 NoAudio/8000 Optional Line: Will be omitted in responses w/ negotiated audio
a=sprtparm:190 200 132 220 50 8 Optional Line: Various SPRT Window sizes and max payloads
a=sqn:0
a=cdsc: 1 audio RTP/AVP 0 8 18 101 100 118 126
a=cdsc: 8 audio udpsprt 120
a=cpar: a=sprtmap:120 v150mr/8000
a=cpar: a=fmtp:120 mr=1;mg=0;CDSCselect=1;jmdelay=no;Versn=1.1;mrmods=1-5,7-8,10
a=vndpar:2 9 2 15 Optional Line: Keeps track of legacy capabilities
```

T.38 support is signalled as normal except with an a=cdsc line rather than an m line. Event 4 also needs to be listed on the fmtp line associated with the v150fw payload type.

```
...(abridged)...
a=rtpmap:118 v150fw/8000
a=fmtp:118 1,3-4
a=rtpmap:126 NoAudio/8000
a=sqn:0
a=cdsc: 1 audio RTP/AVP 0 8 18 101 118 126
a=cdsc: 7 audio udpsprt 120
a=cpar: a=sprtmap:120 v150mr/8000
a=cpar: a=fmtp:120 mr=1;mg=0;CDSCselect=1;jmdelay=no;Versn=1.1;mrmods=1,3
a=cdsc: 8 image udptl t38
a=cpar: a=T38FaxVersion:3
a=cpar: a=T38MaxBitRate:33600
a=cpar: a=T38FaxFillBitRemoval:0
a=cpar: a=T38FaxTranscodingMMR:0
a=cpar: a=T38FaxTranscodingJBIG:0
a=cpar: a=T38FaxRateManagement:transferredTCF
a=cpar: a=T38FaxUdpEC:t38UDPRedundancy
a=cpar: a=T38FaxMaxBuffer:200
a=cpar: a=T38FaxMaxDatagram:320
```

User-Agent/Server Header and Identity Header Hostname Pass-Through

In prior releases, the User-Agent header added by Cisco Unified CM to outgoing SIP requests specified Cisco Unified CM and the software release (e.g., Cisco-CUCM8.5). In no case was a SIP Server header included in outgoing responses.

There are 3 new configuration settings available within the SIP Profile to control the pass-through of the User-Agent and Server SIP headers. These are under the configuration:**User-Agent and Server header information**

- **Send Unified CM Version Information as User-Agent -**This option maintains the currect behavior of Cisco Unified CM to provide the current release as the User-Agent in requests and not provide any Server header in responses.
- **Pass Through Received Information as Contact Header parameter**- This option is intended only for intercluster SIP trunks, and passes the information through as a parameter to the Contact parameter.
- **Pass Through Received Information as User-Agent Header**- This configuration option is intended to be enabled on all trunks pointing to 3rd party equipment, where it is useful to pass-through the User-Agent and Server headers of the peer device.

The SIP identity headers (From:, Remote-Party-ID:, and P-Asserted-Identity:) provide the identity of the party generating the messages. Because existing Cisco Unified CM behavior is geared toward the use of numeric user parts (for example, telephone numbers), the incoming hostname info provided in the incoming SIP message was suppressed, and replaced with the IP address of the local Cisco Unified CM when those messages were delivered to the endpoints or sent out a SIP trunk. However, some devices are geared toward the use of full SIP URIs. It thus became useful to provide the full SIP URL (user@host) that was received in the incoming SIP messages. This allows these endpoints to acquire the full username and host of the other party, and enable their native capability of making calls directly to those SIP URLs rather than relying on that information being provisioned by the Cisco Unified CM.

On the SIP Profile configuration page, the **Use Fully Qualified Domain Name in SIP Requests** checkbox was added. When disabled (the default), the previous behavior of Cisco Unified CM is maintained: only the user part of the identity header is passed through, the hostpart is replaced with the Cisco Unified CM IP address. When enabled, the hostname received by the Cisco Unified CM in the incoming SIP message will be passed through, and will appear in the outgoing messages.

Outgoing Identity and Incoming CLI for SIP Calls

This feature provides the ability to enhance the identity selection, presentation and restriction on SIP interfaces. These capabilities will be offered via additional configuration fields used for presentation (Identity headers and From headers) on SIP Trunk as well as on SIP profiles for controlling corresponding SIP phones.

In such Service Provider's network, there are two sets of identities maintained by the SP network, network provided identity (trusted) and user provided identity (non trusted). In terms of SIP calls, the Identity headers, including P-Asserted-Identity (PAI), P-Preferred-Identity (PPI), and Remote-Party-ID (RPID) should carry network provided identity, while the From header carries user/caller provided identity.

Traditionally, Cisco Unified CM only provides a single set of identity for outgoing calls into the Service Provider's network. Therefore, the identities in Identity headers and From header are exactly the same and there is no differentiation between network provided identity and user provided identity. Typically, the Cisco Unified CM administrator configures each user device with a Directory Number (DN) and a display name.

An outgoing call from this DN will carry its directory number and display name in both Identity headers and From header. Since Release 9.0(1), Cisco Unified CM allows configuring a URI instead of a DN.

The Cisco Unified CM administrator can also configure another identity on a SIP trunk. This identity, sometimes termed as switchboard idenity, is used to hide each individual caller's identity. It can be configured on the Caller Information section of a SIP Trunk for outbound calls. The configuration includes two fields, Caller ID DN and Caller Name. For example, all calls originating from a SIP Trunk carry the same identify, Caller Name with "Cisco Systems" and "(800) 555-1234" for the Caller ID DN. However, the caller's original directory number and display name will be overwritten when such configurations are enabled.

With this new feature, however, Cisco Unified CM provides configurations where the administrator can enable both sets of identifications, switchboard identity and original caller identity, for each SIP trunk or SIP device. Switchboard identity will be carried in the From header and original caller identity will be carried in the Identity headers.

For the incoming calls from Service Provider's network, Cisco Unified CM provides configurations to accept network provided identity carried in Identity headers or user provided identity carried in From header. Cisco Unified CM maintains only a single set of identities per call.

Outgoing Call With Both Switchboard Identity and Original Caller Identity

For calls originated from Cisco Unified CM devices, the Identity headers are set to the LINE ID of the respective device (original caller identity) and the From header can be set to either the same as the Identity header or switchboard information.

In this example, a new INVITE carrying both network provided identity, "Cisco Support" and "4761000" and user provided identity, "Alice" and "4762124".

```
INVITE sip:bob@biloxi.com SIP/2.0
        To: Bob <sip:bob@biloxi.com>
        From: Cisco Support <sip:4761000@cisco.com>;tag=1928301774
        P-Asserted-Identify: Alice <sip:47611234@cisco.com>
        Remote-Party-ID: Alice <sip: 47611234@cisco.com>;party=calling; screen=yes;
privacy=off
        Contact: <sip: 47611000@cisco.com>
```

As you can see, the Identity headers (P-Asserted-Identify and Remote-Party-ID) carries original caller identity (Alice's real number and name) and From header carries switchboard identity. Please note Contact header matches From header as mandated by the requirement.

Conference Factory Support

Conference Factory support follows the call flow from Figure 5.3.4.13-30 of the Department of Defense Unified Capabilities Requirements 2008. For more information about UCR 2008, seehttp://www.disa.mil/_large_files/DOD_UCR_2008_Change_3.pdf.This feature allows AS-SIP lines to establish conference package subscriptions with a Conference Server connected via SIP trunk. You must enable the trunk for AS-SIP in its SIP Profile. The primary change is to support outbound conference package subscriptions, and to switch Contact header changes (userinfo and isfocus) through the call arc during re-INVITE and NOTIFY.

This call flow derives from RFC-4579 section 5.3, and includes conference-aware event processing as specified in RFC-4575. The call flow works as follows.

1 A conference server is deployed which controls one or more conference resources and supports the Conference Factory flow.

2 The conference initiator calls the conference server using INVITE(Conference Factory URI) to begin a conference. The AS-SIP-EI conference factory URI looks like <confFactoryDigitString>@<UCMaddress>. The UCM routes the request via normal DA dialplan routing using confFactoryDigitString.
3 After connect, the conference server prompts the user (via non-SIP means like IVR) for information, and then reserves a conferencing resource represented by a conference URI of the form <conference-ID>@<conference-server-address>;isfocus. The conference ID is a digit string capable of navigating the dialplans of the UCM's, so that later a SUBSCRIBE addressed to this URI can arrive back to the conference server (see later below).
4 The conference server sends a re-INVITE (on the same dialog) and changes the Contact header to the conference URI of the resource that was just reserved. The userinfo and "isfocus" parts are switched by each UCM to the EI (the host part will change to <UCMaddress> as it transits each UCM, per pre-Kirra behavior).
5 When the AS-SIP EI sees the isfocus, it sends SUBSCRIBE(conf-URI) to the conference server (via the UCM) in order to receive conference events. Conf-URI is <confIDDigitString>@<UCMaddress>. Each UCM in the call path routes the request using the userinfo field, via the normal DA dialplan. The SUBSCRIBE arrives at the conference server. The conference server and UCM respond locally with 200 responses to the SUBSCRIBE requests.
6 The conference server sends an initial NOTIFY with an XML body containing a list of all conference participants, and a Contact header containing the isfocus parameter. Initially there are none.
7 The conference server prompts (via non-SIP means such as IVR) the initiator to enter additional info to add more conferees, the initiator feeds the server digits, and the server then calls these conferees. The INVITEs from the server contain a Contact header with the conference URI pointing to the common conference resource. The switching/translation of this Contact to the EI, and the subsequent SUBSCRIBE/NOTIFY exchange, are as previously described for the conference initiator.
8 Once all attendees are added, the conference initiator adds himself to the conference (again via non-SIP means such as IVR).
9 Subsequently the conference initiator may add/drop conferees. Any change in attendee status is reported by the server to the conferees using NOTIFY within the individual subscriptions.

URI Dialing

The URI dialing feature allows the Cisco Unified CM to route a URI, such as bob@cisco.com. URI dialing has the following requirements:

- Endpoints still require a DN
- Optionally, a DN can have 0-n alphanumeric URIs associated with it.
- An alphanumeric URI must be unique within a partition and can be in a separate partition from the associated DN.
- A device can be dialed using its DN or associated alphanumeric URI.
- UCM will "blend" the two pieces of information together and pass it through the call arc. This will be done for both called and calling parties. (Connected party information)
- At the edge, delivery policy will dictate whether to pass the DN or the URI across the SIP signaling.

Outbound Changes

From a signaling point of view, the SIP trunk can deliver identity of DN or URI across the SIP signaling. This is configurable on the SIP trunk page.

Inbound Changes

Due to dial-able characters 0-9, A-D,*,+ spanning both the numeric and alpha-numeric sets, there needs to be a way to disambiguate when an incoming dial string is arbitrary. For example, is the user portion of **sip:1234@10.10.10.1** a number or an alphanumeric dial string? At the ingress edge, there is logic to disambiguate in order to lookup the dial string in the right dial tree. By default, dial strings that consist of characters 0-9, *, and + exclusively are considered numeric DNs, all others are alpha-numeric URIs.

Anonymous Call Rejection for an Incoming and Outgoing SIP Trunk Call

This feature allows the administrator to block calls from anonymous callers coming into the cluster over a SIP trunk. If the caller's DN is either not present or caller's DN is private - then the call is treated as a call from an anonymous caller. If the caller's name is private but caller's DN is provided and not restricted, then the call is not treated as a call from an anonymous caller.

Anonymous calls in SIP are identified based on the criteria described in RFC 5079. Based on RFC 5079, calls are identified to be anonymous when incoming initial INVITE has -

- From or PAI/PPI header with display-name "Anonymous"
- From header host-portion = anonymous.invalid
- Privacy: id or Privacy: user or Privacy: header [associated with PAI/PPI]
- Remote-Party-ID header has a display-name "Anonymous"
- Remote-Party-ID header has privacy=uri/name/full

If the incoming anonymous call arrives from a sip device like a phone or trunk, Cisco Unified CM will reject the call with a SIP response 433 Anonymity Disallowed. The 433 response will also carry a Reason header with Q.850 cause value 21 (call rejected).

For other protocols, calling leg gets rejected with Q.850 cause = 21 (call rejected).

The following is an example of an INVITE and 433 response:

```
INVITE sip:1008@10.81.54.134:5060 SIP/2.0^M
Via: SIP/2.0/TCP 10.81.54.224:5060;branch=z9hG4bKbbf1e969eb^M
From: "Anonymous"
<sip:anonymous@anonymous.invalid>;tag=19583~078d0a52-bf48-420d-b77b-7737bebdf89b-28868768^M
To: <sip:1008@10.81.54.134>^M
Date: Fri, 06 Jul 2012 14:34:45 GMT^M
Call-ID: b9c4f600-ff61f785-b5d-e036510a@10.81.54.224^M
Supported: timer,resource-priority,replaces^M
Min-SE: 1800^M
User-Agent: Cisco-CUCM9.0^M
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY^M
CSeq: 101 INVITE^M
Expires: 180^M
Allow-Events: presence, kpml^M
Cisco-Guid: 3116692992-0000065536-0000000002-3761656074^M
Session-Expires: 1800^M
P-Asserted-Identity: "Conn6003" <sip:6003@10.81.54.224>
Privacy: id
```

```
Remote-Party-ID: "Conn6003" <sip:6003@10.81.54.224>;party=calling;screen=yes;privacy=uri
.....
SIP/2.0 433 Anonymity Disallowed
Via: SIP/2.0/TCP 10.81.54.224:5060;branch=z9hG4bKbbf1e969eb
From: "Anonymous"
<sip:anonymous@anonymous.invalid>;tag=19583~078d0a52-bf48-420d-b77b-7737bebdf89b-28868768
To: <sip:1008@10.81.54.134>;tag=4581~91cf308a-25ef-4abc-b972-0b276e0bf42d-30891801
Date: Fri, 06 Jul 2012 14:34:45 GMT
Call-ID: b9c4f600-ff61f785-b5d-e036510a@10.81.54.224
CSeq: 101 INVITE
Allow-Events: presence
Reason: Q.850; cause=21
Content-Length: 0^M
```

The Cisco Unified CM SIP trunk can also be configured to block any outgoing call which has either no caller information or with private caller information. In this case, the SIP trunk layer will reject the call setup request from call control with Q.850 cause value 21.

H.264 SVC Codecs

Unified Communications Manager supports H.264 negotiation with Profile, Level and the optional parameters specified in the H241 and RFC 3984 specifications. The support of these parameters for SCCP protocol is limited to a subset. However, Unified Communications Manager does not currently take notice of the signaled packetization modes from H323 endpoints. Further, the RFC3984 is undergoing a revision and the current draft of RFC3984 bis-08 has added additional optional parameters and updated the semantics of the offer/answer negotiation, taking these parameters into account.

The additional parameters are as follows:

- max-smbps
- sprop-level-parameter-sets
- use-level-src-parameter-sets
- in-band-parameter-sets
- sar-understood
- sar-supported max-recv-level
- level-asymmetry-allowed

Unified Communications Manager does not currently support rtcp-fb attributes in SDP. Cisco Telepresence endpoints are being enhanced to use a new proprietary mux attribute in the SDP and Unified Communications Manager allows this to be passed through in the offer and answer SDPs.

As a part of this feature enhancement is the support of the preceding eight H264 attributes, rtcp-fb and the Cisco proprietary x-cisco-mux parameter.

The following is a sample SDP message with the above parameters:

```
m=video 20310 RTP/AVP 99
c=IN IP4 10.13.5.196
b=TIAS:1000000
a=X-Cisco-mux: cisco partner
a=rtpmap:99 H264/90000
a=fmtp:99 profile-level-id=42801E;
max-recv-level=B00E;
max-mbps=2000;
max-br=1550;
max-cpb=15;max-fs=512;
max-smbps=1000;
max-dpb=64;
```

```
sprop-parameter-sets=Z0IACpZTBYmI,aMljiA==;
max-rcmd-nalu-size=1024;
sar-supported=16;
sar-understood=124;
packetization-mode=1
```

Apart from a few additional parameters in the SDP message, no call flows are changed.

Confidential Access Level

Confidential Access Level (CAL) controls which calls can be completed, based on how the feature is configured, and persistently displays information on the phone that provides additional information about the call.

Configuration

A CAL value is a numeric value within the range of 0 to 99. In a CAL-enabled system, every device, line, and trunk, has a configured CAL value:

- A numeric value that is assigned to an entity:
  - Device (IP phone)
  - Trunk (PRI, SIP)
  - Line
- Allowable range: 0 to 99
- Each numeric value has an associated textual value

The CAL modes are as follows:

- Fixed
  - Emphasizes CAL level over call completion
  - Calculation occurs at each hop
  - Incoming CAL is resolved against outgoing CAL
  - Resolved CAL must match the CAL of whichever party is in Fixed mode (one party or both parties to the call)
- Variable
  - Emphasizes call completion over CAL level
  - Calculation occurs at each hop
  - Incoming CAL is resolved against outgoing CAL
  - The numeric value may change as the call moves through the voice network (As long as it resolves to a value, call is allowed to proceed to next hop)

The following information describes how CAL works:

- CAL is assigned to devices, lines, and trunks

- While building the outgoing call leg, the incoming CAL and outgoing CAL are plugged into the CAL table
  - Incoming CAL on the Y-axis
  - Outgoing CAL on the X-axis
  - The intersection of X and Y is the Resolved CAL value
- Call routing can continue if the following conditions are met:
  - X and Y resolve to a numeric value in the table
  - The resolved value meets the minimum required CAL value of both parties

SIP Phones (9971,9951 and 8961 models) support the CAL feature.

Confidential Access Level (CAL) Enforcement is the enterprise parameter to enable or disable CAL.

Confidential-Access-Level SIP Header

The following is the SIP header syntax that is used to negotiate CAL between AS-SIP enabled Call Agents:

```
Confidential-Access-Level = “Confidential-Access-Level” HCOLON local-access-level SEMI
reflected-access-level [SEMI access-display]
local-access-level = (access-level SEMI access-mode)
reflected-access-level = (“ref” EQUAL access-level SEMI reflected-mode)
access-level = (1*2DIGIT ; 0 to 99)
access-mode = (“mode” EQUAL mode-param)
reflected-mode = (“rmode” EQUAL mode-param)
mode-param = (fixed / variable)
access-display = (1*16display-text)
display-text = (ALPHA/SP/”/”/”-”)
```

Example

- CAL in initial INVITE:

  Confidential-Access-Level: 4;mode=variable;ref=0;rmode=fixed;PENDING
- CAL in 200 OK to INVITE:

  Confidential-Access-Level: 4;mode=variable;ref=4,rmode=variable;EXTERNAL

418 Incompatible CAL Message

If an AS-SIP signaling appliance (LSC or SS) in the signaling path between parties receives an initial INVITE with a CAL header that the AS-SIP signaling appliance cannot successfully resolve against the locally configured value of the next hop routing domain (CAL Header Processing), then the AS-SIP signaling appliance responds with a 418 Incompatible CAL.

The 418 response contain a CAL header in which the local-accesslevel is set to the classification level and mode that is supported by the AS-SIP signaling appliance that is responding with the 418 and the reflected-access-level is set to the last successfully resolved value in the request path.

CAL causes Additional Headers to be included in INVITE messages. Some SIP entities may not support it. There are parameters to control the inclusion on CAL header using SIP profile. The parameter Confidential Access Level Headers in SIP profile takes three values, Disabled, Preferred, and Required.

These three options would do the following:

- Disabled does not send any CAL headers.
- Preferred includes the CAL header in INVITE message and put the "confidential-access-level" tag in a Supported header.
- Required includes the CAL header in INVITE message and put the "confidential-access-level" tag in Require and Proxy-Require headers.

CAL header is populated in INVITE,180 Ringing,200 OK and UPDATE messages .

iX Channel Support

IX provides a simple, reliable and secure channel over which multiple application layer protocols can be multiplexed. The transport that is used for IX channel is UDP. To provide a reliable channel, IX utilizes UDT over UDP. IX channel can be negotiated and set up using the Session Description Protocol (SDP) and the Offer/Answer model. IX channel extends SDP to support new attribute mapping the protocols to be multiplexed.

IX support strictly applies to SIP devices. Both SIP Trunk and SIP Line interfaces are fully supported. Both SIP Trunk and SIP Line interfaces are fully supported. IX is supported on Early Offer (EO) and Delayed Offer (DO) SIP trunks.

The following is a sample IX application mline in SDP:

```
m=application 12345 UDP/UDT/IX *
 b=as:64
 a=ixmap:1 XCCP
 a=ixmap:2 MSCP
 a=connection:new
 a=setup:actpass
```

Both sides of a call have to support IX for IX to be negotiated and work. Unified Communications Manager does not terminate the IX protocol.

In order for IX to work, all SIP Interfaces for the call must have IX enabled or support IX. IX feature activation for a particular SIP Trunk interface is controlled by Allow iX Application Media checkbox within the SIP Profile.

Note IX is disabled by default in the SIP Profile.

If IX cannot be negotiated (for example, one side does not support IX), IX application is rejected and the port number is set to 0.

```
m=application 0 UDP/UDT/IX *  < ---- Inactive channel
a=setup:actpass
a=ixmap:0 ping
a=ixmap:2 xccp
a=ixmap:3 rmultisitectrl
```

Multiple Codecs in Answer SDP

When a call is routed through Unified Communications Manager, Unified Communications Manager takes the role of selecting a single audio and video codec for the call based on the CAC policy and the codec preference configured in Unified Communications Manager. Therefore, the endpoint can only communicate with the codec specified by Unified Communications Manager. This logic applies to audio and video codecs.

However, there are endpoints that can support receiving more than one codec within a media channel. Simulcast is one of the applications that can transmit more than one encoded data within an established channel. In order to support such usage, Multiple Codec in Answer SDP supports this function that Unified Communications Manager will not narrow down to a single codec during negotiation when both parties are capable of handling more than one codec in the SIP answer message. Instead, Unified Communications Manager will send a common set of codecs in the SIP answer message, provided that the codec offered by the endpoints does not exceed the inter-region bandwidth policies. This feature applies only to endpoints that indicate the support of Multiple Codec in Answer and they have to be homogenous SIP protocol calls. The rest of the call scenarios will remain to be single codec negotiation as Unified Communications Manager does in the present day.

When Unified Communications Manager allows multiple codecs to be negotiated, the endpoint can decide which codecs will be transmitted and prepared to receive any codec being offered. The endpoint may choose to transmit more than one media codec, depending on the application. Unified Communications Manager will not know what codec has been transmitted inside the RTP channels by the call devices.

Unified Communications Manager recognizes the SIP endpoint supporting multiple codecs in answer in the following ways:

- **SIP contact header URI**

  The endpoint can specify "**+multiple-codecs-in-ans**" in the Contact header line of SIP message to indicate the support multiple codecs negotiation. It is noted that Unified Communications Manager recognizes the tag in the incoming SIP "offer" message only, not in the "answer" message.

  Contact:<sip:84626@172.27.31.84:5060;transport=tcp>;video;audio**;+multiple-codecs-in-ans**>

- **SIP trunk configuration**

  A configuration check box **Allow multiple codecs in answer SDP** was introduced in the SIP profile for trunk type device. Any SIP endpoints behind a trunk that have this checkbox enabled can handle multiple codecs in the SIP answer message. Unified Communications Manager will still consider SIP endpoints that support multiple codecs in the answer SDP if the incoming offer message contains the contact header URI indicated above, even though this configuration check box is unchecked.

- **Multiple Codecs Specified in SIP answer Signals**

  When Unified Communications Manager offers a SIP endpoint with SDP and the endpoint responds with multiple codecs in answer signals, Unified Communications Manager identifies that the endpoint is capable of negotiating multiple codec in the answer. This applies to both SIP trunks and SIP line devices, regardless of whether they have hinted the support of multiple codec negotiation by any means discussed above. This operation occurs in the media layer.

Non-SRTP Call Block

For the Non-SRTP Call Block feature, all the SIP endpoints (both line and trunk) will not allow any non-secure call to establish if the service parameter Block Unencrypted Calls is set to true. All the non-secure calls will be blocked based on this service parameter.

For an inbound SIP trunk, if the preceding service parameter is set to true and no secure audio capabilities are present in its sdp (if any), then the call will be blocked and will not proceed further.

For an outbound SIP trunk, if the preceding service parameter is set to true and the SRTP Allowed check box is not checked (if the SIP trunk is non-secure), then the call will be blocked and will not be proceed further.

Session Timer with UPDATE

This feature adds the Session Refresh MethodRequired field to the trunk specific configuration section of the SIP profile. The allowed values are Invite and Update, with the default being Invite. This value specifies which SIP method should be used when the Unified Communications Manager originates a SIP request as the refresher of a SIP session.

Previously, Unified Communications Manager always sent a SIP INVITE request, and this existing capability will be retained when the configuration is Invite. Note that sending a mid-call INVITE request requires that an offer SDP be specified in the request. This means that the far end must send an answer SDP in the INVITE response.

If the configuration is Update, then the Unified Communications Manager will instead send a SIP UPDATE request, if support for the UPDATE method is specified by the far end of the SIP session in either the Supported or Require headers. When sending the UPDATE request, the Unified Communications Manager will not include an SDP. This method simplifies the session refresh since no SDP offer or answer exchange is required.

Note If the UPDATE method is not supported by the far end of the SIP session (the UPDATE method is not included in either the Supported or Required headers), the Unified Communications Manager will continue to use the INVITE method for session refresh.

The administrator will provide the capability to configure in the trunk specific configuration of the SIP profile whether Unified Communications Manager should send INVITE or UPDATE for session refresh when Unified Communications Manager is the refresher. The new parameter is Session Refresh Method.

SDP Transparency for Declarative Attributes

This feature allows the administrator to specify declarative SDP attributes that are not natively supported by Unified Communications Manager to be passed from the ingress call leg to the egress call leg. The administrator also has the option of configuring all unrecognized attributes to the egress leg. If the Unified Communications Manager is not configured to pass all unrecognized attributes transparently and it receives attributes that are not explicitly identified by the administrator to send to the egress leg, then Unified Communications Manager will drop the attribute from the outgoing SDP similar to previous versions of Unified Communications Manager.

Note For the purposes of identifying which attributes are passed to the egress leg, comparisons are both case sensitive and white space is considered.

The administrator may identify attributes that will be sent to the egress leg in multiple ways. In addition to passing all unrecognized attributes, the administrator has the option to specify all property attributes with a particular name, all value attributes with a particular name, or all value attributes with a specific name and specific value. The administrator performs configuration at the SIP Profile level by associating an SDP Transparency Profile that specifies which attributes are passed transparently or picking the pre-configured SDP Transparency Profile named “Pass all unknown SDP attributes” to indicate all unrecognized declarative attributes must be passed to the egress leg. The configuration for this feature on the SIP Profile applies all registered SIP endpoints and SIP trunks using that SIP Profile.

Note A reset of all devices using this SIP Profile is needed for any changes to take effect.

There are exceptions, however, for when the feature will take effect. The feature does not apply to the following situations:

- One or more of the following apply on the egress leg:
  - One or more Media Termination Points (MTPs) that does not support pass through has been allocated
  - One or more Trusted Relay Points (TRPs) that does not support pass through has been allocated
  - The use of the RSVP feature
  - The use of a transcoder
  - "Media Termination Point Required" is selected
  - The ingress call leg is using Delayed Offer while the egress call leg is using Early Offer
  - The media line has been rejected (the port is set to 0). Note that in this situation, it may be possible to see certain attributes in the media line. Any attribute on a rejected media line should be ignored and solutions must not rely on this feature to send attributes on rejected media lines. Doing so is strictly not supported.
  - Either call leg uses any protocol other than SIP

This feature supports the passing of attributes that follow the grammar prescribed in RFC 4566. Any attribute that deviates from this grammar is not guaranteed to pass correctly. However, the best effort is made to pass the attribute in these situations.

SIP BPA/488 Error Handling

The purpose of this feature is to include a warning header “370 Insufficient Bandwidth” in the 488 Error messages for the following scenarios:

- If the Unified Communications Manager receives an inbound precedence call request (for example, with precedence level PRIORITY or above) over the IP network for a served endpoint and the Unified Communications Manager has insufficient bandwidth-related resources (for example, due to call count threshold) to handle the call request, and if there are insufficient existing calls or call requests of lower precedence where their removal would provide the necessary resources to support the pending call request, then the Unified Communications Manager must reply with a 488 (Not Acceptable Here) response code and must include a Warning header with warning code 370 (Insufficient Bandwidth). The BPA blocked precedence announcement is played or displayed to the user through the calling IP EI.
- For an outgoing call when Unified Communications Manager receives an outbound precedence call request from a served IP endpoint and there are insufficient resources to support the outbound precedence call request (for example, bandwidth restriction), the Unified Communications Manager must compare the precedence level of the new precedence call request with the precedence levels of the existing calls or call requests to determine whether sufficient resources of lesser precedence can be preempted to accommodate the new precedence call request. This comparison can occur only for calls and call requests that have the same value for the precedence-domain subfield in the namespace of the Resource-Priority header field.

Configuration

No configuration changes exist for this feature.

Changes

Included the Warning header to the 488 Not Acceptable Media error messages in the above mentioned situations. The Warning header format is as follows:

Warning: 371 <Host IP> "Insufficient Bandwidth"

Sample Message

```
SIP/2.0 488 Not Acceptable Media
Via: SIP/2.0/TCP 10.77.46.84:5064;branch=z9hG4bKd47639f069
From: <sip:7654@10.77.46.84>;tag=1657~c86d348c-200d-4847-ba87-837e294a0ef2-23831059
To: <sip:4444@10.77.46.93>;tag=1014~785d648c-40a2-4556-b74c-cd3d2402bb56-23829943
Date: Tue, 09 Jul 2013 16:50:09 GMT
Call-ID: 9c10fc00-1dc13f41-60-542e4d0a@10.77.46.84
CSeq: 101 INVITE
Allow-Events: presence
Server: Cisco-CUCM10.0
Warning: 370 10.77.46.93 "Insufficient Bandwidth"
Remote-Party-ID: <sip:4444@10.77.46.93;user=phone>;party=x-cisco-original-called;privacy=off
Content-Length: 0
```

Video On Hold

The Video On Hold feature let you watch a specific video after initial consultation with the agent at the contact center. In this case, the agent will select a video stream that is played to the customer while the customer is on hold.

This feature can be deployed in contact centers and within an enterprise if the deployment requires a generic video on hold capability.

Unified Communications Manager Release 10.0(1) has a Video on Hold Server configuration that allows a media content server to be provisioned under the existing Media Resources menu. The media content server is a device that can stream audio and video content when directed by Unified Communications Manager.

This feature is similar to the existing music on hold capability in Unified Communications Manager but differs in certain key aspects as listed below:

- The media content server is an external device that can store and stream audio and video content under Unified Communications Manager control.
- The media content server is controlled by Unified Communications Manager using SIP as the signal protocol.
- The media content server is capable of providing hi-definition video content at 1080p, 720p and lower resolutions such as 480p and 360p.

The media content server configuration and allocation for a particular session follows the Media Resource Group and Media Resource Group List constructs in Unified Communications Manager.

The following performance measures are supported for this feature:

- VideoOnHoldResourceActive
- VideoOnHoldOutOfResources

SIP Best Effort Early Offer and SIP Early Offer

As of release 10.5(1), the SIP Best Effort Early Offer feature has been added as an enhancement to the SIP Early Offer feature, which was available as of release 8.6(1). SIP Best Effort Early Offer and SIP Early Offer are supported by Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition. The feature improves interoperability between Cisco Unified Communications Manager and third party SIP PBXes during initial call setup and reduces the issues associated with the use of MTPs.

A new drop-down list, Early Offer support for voice and video calls, has been added to the SIP Profile configuration window. This drop-down list replaces the Enable Early Offer check box from previous releases. The drop-down list provides the following options:

Disabled (Default Value)

When Disabled is configured on the trunk, Cisco Unified Communications Manager sends a Delayed Offer SIP INVITE that does not include SDP. This is the default setting.

Best Effort (no MTP inserted)

When Best Effort is configured on the trunk, SIP Best Effort Early Offer is invoked. For any call that originates from a Cisco Unified Communications Manager endpoint, if the caller media information is known, Cisco Unified Communications Manager includes an SDP offer in the initial INVITE. The SDP includes the caller's IP address, ports, and media capabilities. However, if the caller media information is unknown, the SIP INVITE is sent as Delayed Offer.

Mandatory (insert MTP if needed)

When Mandatory is configured on the trunk, SIP Early Offer is invoked for any call that originates from a Cisco Unified Communications Manager endpoint, whether the caller media information is known or unknown. If the caller media information is known, Cisco Unified Communications Manager includes an offer SDP in the initial INVITE with the caller media information making up the SDP portion. If the caller media information is unknown, Cisco Unified Communications Manager inserts an MTP and uses the MTP information for the SDP portion of the Early Offer INVITE.

MTP Required Overrides Best Effort Early Offer

If the Media Termination Point Required check box in the Trunk Configuration window is checked, this configuration overrides whatever setting is selected for the Early Offer support for voice and video calls drop-down list. In this case, an MTP gets inserted in the SDP and the SIP INVITE gets sent as SIP Early Offer with audio only codecs.

When Endpoint's Media Capabilities and Media Port Is Available

Cisco Unified Communications Manager gets the media capabilities and port information of the calling device for the following cases:

- Outgoing call initiated from a SIP phone registered with Cisco Unified CM.
- Outgoing call initiated from a 69xx series, 7984 series (7941 or higher), 796x series (7961 or higher), and 797x series SCCP phone (SCCP v20) registered with Cisco Unified CM
- When incoming INVITE with offer SDP is received on a SIP trunk

- Incoming fast start call on a H323 trunk
- Incoming call from MGCP GW

For either 'Best Effort' and 'Mandatory' options, Cisco Unified Communications Manager passes the media capabilities of the calling device to the SIP trunk. For the outbound SIP INVITE, Cisco Unified Communications Manager inserts the media capabilities, ip address, and port of the endpoint in the SDP offer.

For the endpoint media capabilities Cisco Unified Communicaitons Manager applies audio codec priority rules based on the region-pair of the calling device and outgoing SIP trunk. As a result, the available codecs in the SDP poriton may have equal or less codecs than the calling device's actual capabilities. For example, calling device SIP phone offers codec G.711, G.729, L16 and G.722 in the INVITE to the Cisco Unified Communications Manager. The region-pair settings applicable for the calling phone and the SIP trunk may require L16 to be filtered.

However, if a dynamic MTP is required for a reason such as a DTMF mismatch, Ipv4-IPv6 interworking, TRP requirement, or a transcoder, the call is presented as early offer with the MTP details inserted into the SDP portion.

When Endpoint Media Capabilities And/Or Port Information is Not Available

Cisco Unified Communications Manager may not have the media capabilities and/or media port of the calling device for the following cases:

- call initiated from an older version of SCCP phone
- call initiated from a Cisco Unified CM controlled slow start H.323 or SCCP gateway
- delayed-offer call coming on a SIP trunk
- slow start call coming on a H.323 trunk

If SIP Best Effort Early Offer is configured by selecting Best Effort from the Early Offer for Voice and Video calls drop-down list, and the endpoint media capabilities are not known, the following occurs:

- By default, Cisco Unified Communications Manager presents the SIP INVITE as delayed offer without an MTP.
- If an MTP gets allocated for a reason such as TRP, or a DTMF mismatch, Cisco Unified Communications Manager presents the call as delayed offer and the MTP gets allocated after the 200 OK.
- If the Media Termination Point Required check box in the SIP Trunk configuration window is checked, the MTP configuration overrides the Best Effort Early Offer configuration and the call is presented as SIP early offer with audio only codecs.

If SIP Early Offer is configured by selecting Mandatory from the Early Offer for Voice and Video calls drop-down list, and the endpoint media capabilities are not known, Cisco Unified Communications Manager uses an MTP in the Early Offer SIP INVITE. In this case, the following occurs:

- Cisco Unified Communications Manager allocates an MTP in order to generate a send-recv offer with a valid media port and IP address. The MTP gets allocated from the media resources associated with the endpoint rather than from the SIP trunk side media resources. This will avoid issues with the media path when the MTP is allocated on the SIP trunk side.
- If the media capabilities of the endpoint are available (for example, for SCCP phone or MGCP gateway initiated calls), Cisco Unified Communications Manager creates a superset of the endpoint and MTP

codec capabilities and applies the codec filtering and priorities based on the applicable region-pair settings. In this case, it is expected that the MTP supports the getPort capability and also supports codec pass-through.

- If the MTP does not support codec passthrough, then only the codec supported by MTP shall be offered, subject to codec preference and filtering rules applicable for the MTP and SIP trunk region.
- If the media capabilities of the caller are not available, the media capabilities of the MTP are modified with the codec filtering and priorities based on the region-pair settings, to create the codec list for the outbound SDP. With this change, the Cisco Unified CM advertises multiple codecs when MTP is allocated.
- For slow start H323, Cisco Unified CM advertises the superset of codecs since the codec needs to be re-negotiated after the media cut-thru. Having a superset of codecs can avoid possible call failures due to a codec mismatch.
- If the MTP allocated does not support pass thru, the Cisco Unified CM can only advertise MTP's codecs. The IP address and port in the offer SDP is that of the MTP.
- If the MTP resource is not available, the call might be sent as a delayed offer call or might be rejected based on the SIP service parameter - Fail call over SIP trunk if MTP Allocation Fails.

Server Initiated Call From Cisco Unified Communications Manager

Cisco Unified Communications Manager may initiate a call on behalf of the IP phones. This can happen if the user wants to move the call from an IP Phone to their cell phone. Other scenarios include using the recording feature on sip trunk, OOD REFER initiated click to call, or click to conference.

If Mandatory is selected for the Early Offer support for Voice and Video Calls, Cisco Unified Communications Manager will have to allocate an MTP port to provide a valid IP port and address for the outbound SDP for server initiated calls. This port will be used until the call is answered and then will be replaced with the caller's media information using a re-INVITE. Since the duration of the MTP usage is small, the same MTP port can be reused for multiple server initiated calls.

If the MTP resource is not available, the call might be sent as a delayed offer call or it might be rejected based on the SIP service parameter Fail call over SIP trunk if MTP Allocation Fails.

If 'Best Effort' is selected for the Early Offer support for Voice and Video calls then the call is presented as delayed offer. Cisco Unified Communicaitons Manager does not allocate an MTP, unless an MTP is configured, or due to reasons such as DTMF mismatch, TRP, or IPv4–IPv6 conversion.

Send Send-Receive SDP in Mid-Call INVITE for Mid-Call Feature

This is a configuration added in the **Trunk Specific Configuration** section of the SIP Profile configuration page. If this configuration is enabled, the SIP trunk will not send **a=inactive**, **a=sendonly**, or **a=recvonly** in the outgoing SDP of a midcall INVITE or UPDATE. This usually happens when the media is being disconnected for call hold/resume or for a feature invocation like transfer or conference.

You should enable this configuration only if either SIP Best Effort Early Offer or SIP Early Offer are also enabled.

For MOH or TOH insertion when configuration is enabled, the SIP trunk will directly send a sendrcv SDP to the remote-peer directing the media to the MOH or Annunciator source. If the local MOH or Annunicator for TOH is not available, the Cisco Unified Communications Manager SIP trunk will send an inactive SDP to break the media stream.

During the media resumption phase, SIP trunk will directly send a delayed-offer mid-call INVITE to resume the media path.

Cluster-wide SAN Certificate

In release 10.5(1), Cisco Unified Communications Manager supports a single cluster-wide SAN certificate. With this feature, Cisco Unified Communications Manager now checks for both Subject Name and Subject Alternate Names in the incoming SAN certificates to identify the cluster and the peer.

In the previous releases of Cisco Unified Communications Manger, before establishing a TLS connection, Cisco Unified Communications Manager checked the X.509 subject name that is configured in Cisco Unified Communications Manager against the certificate X.509 Subject Name.

With this feature enhancement, all servers in the cluster can share the same certificate. As a result, the certificate X.509 Subject Name, which can be customized, is shared by all servers in the cluster and cannot be used by itself to identify an individual server or application. To provide a means of identifying an individual server, the Subject Alternate Name field in the certificate is now used to confirm the server identity.

In Cisco Unified Communications Manager, you can simultaneously enter both the Subject Name and the Subject Alternate Name, separated by a comma ,in the X.509 Subject Name field of the SIP Trunk Security Profile. Prior to establishing a TLS connection, Cisco Unified Communications Manager confirms the cluster and server identity by checking the certificate Subject Name and the Subject Alternate Name against the same values configured in Cisco Unified Communications Manager.

Troubleshooting

Table 31: Troubleshooting SIP Trunk Configuration, on page 95 highlights some of the common problems that might be encountered when you are configuring a SIP trunk.

Table 31: Troubleshooting SIP Trunk Configuration

Symptom	Possible Cause	Recommended Action
Cannot receive or make calls through a SIP trunk.	The SIP trunks are not initialized because the Cisco Unified CM process is not part of a Cisco Unified CM Group.	Associate the Cisco Unified CM to a Cisco Unified CM Group. 1 In Cisco Unified CM Administration, choose**System** > **Cisco Unified CM Group**. 2 Click**Find**and choose a group name (such as Default). 3 Make sure that the Cisco Unified CM appears under the "Selected Cisco Unified CMs" section. The following example SDL logs illustrate how a SIP trunk fails initialization because the Cisco Unified CM node is not a member of a Cisco Unified CM Group: `|SIPD(1,100,76,1)|SIPInit(1,100,73,1)|| NumOfCurrentInstances:1000000561|2005/07/2012:54:17.598| 001|SdlSig|Start|start|SIPD(1,100,76,1)|SIPD(1,100,76,1)| (1,100,76,1).1-(*:*) |[R:HP-HP:0,NP:0,LP:0,VLP:0,LZP:0DBP:0]000000562| 2005/07/2012:54:17.598|001|SdlSig|DbSIPTspReq|initializing| Db(1,100,160,1)|SIPD(1,100,76,1)|(1,100,76,1).1-(*:*)| [NP-PQ:0] 000000563|2005/07/2012:54:17.620|001|SdlSig|DbSIPTspRes tsp_discovery|SIPD(1,100,76,1)|Db(1,100,160,1)| (1,100,76,1).1-(*:*) |[R:NP-HP:0,NP:0,LP:0,VLP:0,LZP:0DBP:0] 000000564|2005/07/2012:54:17.621|001|SdlSig| DbSimpleDeviceServerReq|initializing|Db(1,100,160,1)| SIPD(1,100,76,1)|(1,100,76,1).1-(*:*)|[NP-PQ:0] 000000565|2005/07/2012:54:17.636|001|SdlSig| DbSimpleDeviceServerRes|device_server_discovery| SIPD(1,100,76,1)|Db(1,100,160,1)|(1,100,76,1).1-(*:*) |[R:NP-HP:0,NP:0,LP:0,VLP:0,LZP:0DBP:0] 000000566|2005/07/2012:54:17.636|001|Stopping|| SIPD(1,100,76,1)|SIPD(1,100,76,1)||NumOfCurrentInstances:1 000000567|2005/07/2012:54:17.637|001|Stopped|| SIPD(1,100,76,1)|SIPD(1,100,76,1)|| NumOfCurrentInstances:0 000000568|2005/07/2012:54:17.637|001|SdlSig|DeviceStop`
The UAS may reject all outbound calls associated with a SIP trunk with a 4xx response, or signaling may go through, but no audio path gets detected.	Unusual third-party SIP UA might not support delayed media INVITE.	The SIP trunk default configuration results in sending INVITE (without SDP). This definition prevents the use of an MTP resource. Cisco recommends that you leave the "MTP Required" checkbox on the SIP trunk configuration page unchecked; however, if third-party devices do not support delayed media INVITE requests, you can check this box. You must reset the SIP trunk for the change to take effect

Symptom	Possible Cause	Recommended Action

DTMF digits do not get sent to the remote SIP device such as a Unity Voice Messaging server.	This could represent an interoperability issue.
	The SIP trunk supports RFC2833 and Out-of-Band methods when sending DTMF tones across the network.
	• Most SIP devices support RFC2833.
	• The supported OOB methods are KPML and Unsolicited Notify. KPML is not widely used in the marketplace at this time. Currently, the only known products supporting KPML are the Cisco TNP phones, Cisco Unified CM, and Cisco IOS Gateway (12.4 and later). Unsolicited Notify is a Cisco proprietary method that is used only on Cisco IOS Gateways (12.2 and later?). Unity does not support either one at this time but might support KPML in the future. If you are connecting Unity to Cisco Unified CM via SCCP, OOB is assumed.
		Check whether an MTP resource is allocated for the call:
		• If both parties have at least one common DTMF method, an MTP is *not* required.
		• If one party only supports the Out-of-Band method, but the other party only supports RFC2833, an MTP is required.
		For RFC23833 DTMF events, verify that the media stream (via Sniffer) contains packets with the DTMF Payload Type value. For OOB, incoming or outgoing NOTIFY messages get captured in the Cisco Unified CM trace file.
		The following example shows Subscribing for DTMF-KPML:
		`SUBSCRIBE sip:172.18.199.61:5060 SIP/2.0`
		`Via: SIP/2.0/UDP 172.18.199.62:5060;branch=z9hG4bK1BD`
		`From: <sip:3601@172.18.199.62>;tag=169AEB4-93D`
		`To: "sccp_3000" <sip:3000@172.18.199.61>; tag=520767e3-a20b-488e-9ca2-3b1506ab9e94-24577005`
		`Call-ID: 47b5f280-2de1b302-3fc-3dc712ac@172.18.199.61`
		`CSeq: 101 SUBSCRIBE`
		`Max-Forwards: 70`
		`Date: Wed, 20 Jul 2005 20:24:36 GMT`
		`User-Agent: Cisco-SIPGateway/IOS-12.x`
		`Event: kpml`
		`Expires: 7200`
		`Contact: <sip:3601@172.18.199.62:5060>`
		`Content-Type: application/kpml-request+xml`
		`Content-Length: 327`
		`<?xml version="1.0" encoding="UTF-8"?><kpml-request xmlns="urn:ietf:params:xml:ns:kpml-request“ xmlns:xsi="http://www.w3.org/2001 /XMLSchema-instance" xsi:schemaLocation="urn:ietf:params:xml:ns:kpml-request kpml-request.xsd" version="1.0"><pattern persist="persist"><regex tag="dtmf">`
		`x*#ABCD]</regex></pattern></kpml-request>`
		`SIP/2.0 200 OK`
		`Via: SIP/2.0/UDP 172.18.199.62:5060;branch=z9hG4bK1BD`
		`From: <sip:3601@172.18.199.62>;tag=169AEB4-93D`
		`To: "sccp_3000" <sip:3000@172.18.199.61>; tag=520767e3-a20b-488e-9ca2-3b1506ab9e94-24577005`
		`Call-ID: 47b5f280-2de1b302-3fc-3dc712ac@172.18.199.61`
		`CSeq: 101 SUBSCRIBE`
		`Content-Length: 0`
		`Contact: <sip:172.18.199.61:5060>`
		`Expires: 3600`

Symptom	Possible Cause	Recommended Action

DTMF digits do not get sent to the remote SIP device
(continued)
		The following example shows an outbound KPML NOTIFY message:
		`NOTIFY sip:3010@172.18.199.92:5060 SIP/2.0`
		`Via: SIP/2.0/UDP 172.18.199.61:5060;branch=z9hG4bK48b28f9b`
		`From: <sip:3010@172.18.199.61>; tag=520767e3-a20b-488e-9ca2-3b1506ab9e94-26499709`
		`To: <sip:3501@172.18.199.92>;tag=1A60AE98-324`
		`Call-ID: 4724DD80-FC6211D9-8190EC13-60F39CA2@172.18.199.92`
		`CSeq: 103 NOTIFY`
		`Max-Forwards: 70`
		`Date: Mon, 25 Jul 2005 16:45:29 GMT`
		`User-Agent: Cisco-CCM5.0`
		`Event: kpml`
		`Subscription-State: active;expires=3600`
		`Contact: <sip:172.18.199.61:5060>`
		`Content-Type: application/kpml-response+xml`
		`Content-Length: 177`
		`<?xml version="1.0" encoding="UTF-8" standalone="no" ?>`
		`<kpml-response code="200" digits="1" forced_flush="false" suppressed="false" tag="dtmf" text="Success" version="1.0"/>`
		The following example shows negotiating Unsolicited NOTIFY request:
		`INVITE sip:3501@172.18.199.92:5060 SIP/2.0`
		`Call-Info: <sip:172.18.199.61:5060>; method="NOTIFY;Event=telephone-event;Duration=500"`
		`Response:`
		`SIP/2.0 200 OK`
		`Call-Info: <sip:172.18.199.92:5060>; method="NOTIFY;Event=telephone-event;Duration=500"`
		The following example shows an outbound Unsolicited NOTIFY message:
		`07/26/2005 14:15:18.658 CCM|`
		`Outgoing UDP SIP message to 172.18.199.92:[57475]:`
		`NOTIFY sip:172.18.199.92:57475 SIP/2.0`
		`Via: SIP/2.0/UDP 172.18.199.61:5060;branch=z9hG4bK66516ae9`
		`From: "sccp_3010" <sip:3010@172.18.199.61>; tag=520767e3-a20b-488e-9ca2-3b1506ab9e94-26499723`
		`To: <sip:3501@172.18.199.92>;tag=1FD98A34-1DC0`
		`Call-ID: 314ae380-2e617dac-325-3dc712ac@172.18.199.61`
		`CSeq: 102 NOTIFY`
		`Max-Forwards: 70`
		`Date: Tue, 26 Jul 2005 18:15:18 GMT`
		`User-Agent: Cisco-CCM5.0`
		`Event: telephone-event;rate=1000`
		`Subscription-State: active;expires=-1281397684`
		`Contact: <sip:172.18.199.61:5060>`
		`Content-Type: audio/telephone-event`
		`Content-Length: 4`

Symptom	Possible Cause	Recommended Action

UAS responds to an INVITE request with a 401 (Unauthorized) message.	Authentication or Authorization is failing	If authentication or authorization are not needed, make sure the appropriate check boxes on the SIP Trunk Security Profile window are unchecked.
		or
		Configure the application user on Cisco Unified CM with proper authorization.
		Configure the UAC to match credentials on Cisco Unified CM.
		`INVITE sip:5000@172.18.193.222 SIP/2.0`
		`Via: SIP/2.0/UDP 172.18.194.208:5060;branch=z9hG4bK5ba60c17`
		`From: "4900" <sip:4900@172.18.193.222>; tag=000f24c6a16f000d171bb590-611445d9`
		`To: <sip:5000@172.18.193.222>`
		`Call-ID: 000f24c6-a16f000c-245cb98c-57a622e0@172.18.194.208`
		`.....`
		`SIP/2.0 401 Unauthorized`
		`From: "4900" <sip:4900@172.18.193.222>; tag=000f24c6a16f000d171bb590-611445d9`
		`To: <sip:5000@172.18.193.222>;tag=466540560`
		`Call-ID: 000f24c6-a16f000c-245cb98c-57a622e0@172.18.194.208`
		`CSeq: 101 INVITE`
		`WWW-Authenticate: DIGEST realm="siptrunk4l", nonce="YoK5FiEuXpeIlp52EnUWFLIU1m24t5gV", algorithm=MD5`
		`Content-Length: 0`
		`.....`

UAS responds to a SIP request with a 403 (Forbidden) message.	**In the System** > **Security Profile** > **SIP Security** Profile window, and per the default settings, the following features require authorization:
	• Presence Subscription
	• OOD REFER
	• Unsolicited NOTIFY
	• INVITE and REFER w/ Replaces header
		If authentication or authorization are not needed, make sure the appropriate check boxes on the SIP Trunk Security Profile window are unchecked.
		or
		Configure the application user on Cisco Unified CM with proper authorization.
		Configure the UAC to match credentials on Cisco Unified CM.
		`INVITE sip:5000@172.18.193.222:5060 SIP/2.0`
		`Via: SIP/2.0/UDP 172.18.195.83:5060`
		`From: sipp <sip:sipp@172.18.195.83:5060>;tag=1`
		`To: sut <sip:5000@172.18.193.222:5060>`
		`Call-ID: 1-21473@172.18.195.83`
		`Cseq: 1 INVITE`
		`Replaces: 425928@bobster.example.org;to-tag=7743; from-tag=6472`
		`.....`
		`SIP/2.0 403 Forbidden`
		`Via: SIP/2.0/UDP 172.18.195.83:5060`
		`From: sipp <sip:sipp@172.18.195.83:5060>;tag=1`
		`To: sut <sip:5000@172.18.193.222:5060>;tag=673966968`
		`Date: Tue, 5 Jul 2005 18:25:02 GMT`
		`Call-ID: 1-21473@172.18.195.83`
		`CSeq: 1 INVITE`
		`Content-Length: 0`

Symptom	Possible Cause	Recommended Action
UAS responds to a SIP request with a 404 Not Found message.	Digit analysis failed to find the device or a route for the called number.	This could happen for many reasons. If the phone with the dialed number is not registered, or if the host in the request does not match the Cisco Unified CM host or IP address and there is no SIP route pattern to route this number or DN, Digit Analysis will fail.
Potential problems with forking exist. Downstream SIP endpoints do not receive ACK to responses.	Not actually a problem. The SIP trunk does not support downstream forking for delayed media INVITE (w/o SDP).	If downstream forking support is required, the SIP trunk must use an MTP. Make sure the "MTP Required" check box is checked on the SIP trunk configuration window.
TLS connection for SIP trunk fails with "HandleSSLError - TLS protocol error…" in SDI log (ccmtrace).	TLS SIP trunk peer X509 certificate has not been imported into the local Cisco Unified CM trust store or is the incorrect version.	Ensure that the peer X509 certificate is version 3 and has been properly imported into the local Cisco Unified CM trust store.
TLS connection for SIP trunk fails with a 'ConnectionFailure' alarm on the TLS SIP trunk.	X509 Certificate validation failed for the TLS SIP trunk peer.	Possible problems include X509 Subject Name mismatch or cipher string mismatch. Check the SDL log for more detailed logs under 'validTLSConnection' log. Reason code 1 – Got X509 certificate for neither Authenticate or Encrypted trunk. (Should not happen.) Reason code 2 – X509 Subject Common Name (CN=) mismatch with the trunk security profile settings. Reason code 3 – TLS cipher string mismatch. (The trunk security profile 'Device Security Mode' settings determine this.)
TLS connection from CSPS to Cisco Unified CM via SIP fails with '416 Unsupported URI Scheme' or fails following a '301 Redirect' message.	Cisco Unified CM does not support SIPS URI handling, and CSPS will not complete a TLS connection without SIPS URI support.	Do not use SIP TLS connections between CSPS and Cisco Unified CM.

Symptom	Possible Cause	Recommended Action
No Diversion header exists in the outgoing INVITE message when the call is forwarded	The SIP trunk configuration option "Redirecting Diversion Header Delivery - outbound" does not get checked.	Make sure that the "Redirecting Diversion Header Delivery - outbound" is checked.
Although an end user is associated with primary extension and phone, no PUBLISH comes out.	The preceding configuration applies for SUB/NOT based presence. It does not get used for PUBLISH.	Associate the user to the line appearance in the phone number configuration window.
Although an end user is associated to a line appearance, no PUBLISH comes out.	PUBLISH will not get sent for the line appearance if its associated user does not have a Cisco Unified Presence license.	Assign a Cisco Unified Presence license to that user.
Application Server for click2call wants to get the call status until the call terminates, but the final NOTIFY was sent when the call is connected.	Cisco Unified CM's default behavior is to terminate the implicit subscriptions after a call connects.	Ensure the Refer-To header has a "x-cisco-monitor-call" tag.
REFER (method=BYE) does not terminate the call in a multinode Cisco Unified CM cluster.	Refer Manager cannot find the dialog to terminate.	Make sure REFER(method=BYE) comes into the same node as the node that receives REFER(method=INVITE), for the same call.

Symptom	Possible Cause	Recommended Action
Troubleshooting Calling Party Number Transformations feature	Troubleshooting Calling Party Number Transformations feature	There are a few detailed level SDI trace line that will help us find the number Prefixed and the number of digits striped, and the CSS applied. Example Stripping/Prefixing Digits, CSS: 12/17/2008 00:43:18.826 CCM|//SIP/SIPCdpc(0,0,0)/ci=0/ccbId=0/scbId=0/globalize: Performing stripAndPrependDigits --- Prefix data = +1, Strip Data = 1|<CLID::StandAloneCluster><NID::rtp-galaxy><LVL::Detailed><MASK::20000> 12/17/2008 00:43:18.826 CCM|SPROC :: stripAndPrependDigits- The number 4089023019 is prepended with prefix +1, updated number=+14089023019| <CLID::StandAloneCluster> <NID::rtp-galaxy><LVL::Detailed><MASK::ffffff> 12/17/2008 00:43:18.826 CCM|//SIP/SIPCdpc(0,0,0)/ci=0/ccbId=0/scbId=0/globalize: CallingNumber after stripAndPrependDigits +14089023019 12/17/2008 00:58:54.923 CCM|//SIP/SIPCdpc(0,0,0)/ci=0/ccbId=0/scbId=0/globalize: Using Calling CSS 57803b7e-1bcc-b0d7-da08-f023c78dd179| <CLID::StandAloneCluster><NID::rtp-galaxy><LVL::Detailed><MASK::20000>
Calls using SRTP over non secure trunk don't behave correctly.	Cisco Unified CM down grades to RTP (i.e. AVP)	Check if endpoint on the far end of the trunk indicates support for SAVP in the SDP.
Calls using SRTP over non secure trunk don't behave correctly.	Cisco Unified CM down grades to RTP (i.e. AVP)	Check if other call leg (e.g. perhaps a line side endpoint) on Cisco Unified CM supports SRTP.
Calls using SRTP over non secure trunk don't behave correctly.	Cisco Unified CM down grades to RTP (i.e. AVP)	Check if Cisco Unified CM had to insert an MTP (e.g. due to codec mismatch for example).
Calls using SRTP over non secure trunk don't behave correctly.	Cisco Unified CM disconnects call during setup.	Check if endpoint on the other side of the trunk indicates support for X-cisco-srtp-fallback but the call requires RTP for other reasons (see problems above).

Symptom	Possible Cause	Recommended Action
G.Clear calls not working for SIP line/trunk to MGCP GW T1/E1 PRI	Call drops due to media mismatch.	Check if G.Clear codec was offered by SIP leg.
G.Clear calls not working for SIP line/trunk to MGCP GW T1/E1 PRI	Call drops due to media mismatch.	Check if "Enable G.Clear" checkbox is checked on the MGCP PRI.
G.Clear calls not working for SIP line/trunk to MGCP GW T1/E1 PRI	Call rejected by PSTN/PBX with incompatible destination (88).	Check if ISDN setup from MGCP GW to PBX/PSTN has bearer cap set to 0x8890.
G.Clear calls not working for SIP line to SIP line/trunk	INVITE without G.Clear SDP going out.	Check if G.Clear codec was offered by SIP leg.
G.Clear calls not working for SIP line to SIP line/trunk	INVITE without G.Clear SDP going out	Check if SIP Profile for both the legs have "Enable Early Offer for G.Clear" enabled.
G.Clear calls not working for SIP line to SIP line/trunk	G.Clear call rejected with 488 Incompatible Media	Check if the terminating device supports G.Clear codec / data calls. Cisco IP Phones do not support G.Clear codec.

Symptom	Possible Cause	Recommended Action
Logical Partitioning feature not working	Logical Partitioning feature not working	• Check if Enterprise Param "Enable Logical Partitioning" is True. • Check that the device is associated with a valid Geolocation at device or device pool level. • Check that the device is associated with a valid Geolocation filter, having selection of some of the Geolocation fields, at device or device pool level. • When Enterprise Param "Logical Partitioning Default Policy" is DENY, check if ALLOW LP policies between GeolocationPolicy of a Gateway & VoIP site configured. • Make sure case is correct for fields of the LP GeolocationPolicy records and match with that configured for Geolocation records. • There is no LP Policy check for VoIP to VoIP device call or feature with only VoIP participants. • The Cisco Unified CM Admin will allow configuring policies between Interior:geolocpolicyX to Interior:geolocpolicyY but it will not be used during LP checks. • Hierarchy is important for fields of Geolocation 1 Say searching for policy between Border:IN:KA and Interior:IN:KA 2 The following possible policies will match in order • The possible policies that lack some of the fields in hierarchy, such as following will not match: ◦ Border:KA ◦ Interior:KA ◦ Border:BLR ◦ Interior:BLR ◦ Border:KA:BLR ◦ Interior:KA:BLR ◦ Note: Country=IN is missing

Symptom	Possible Cause	Recommended Action
IPv6 calls not working	IPv6_only phones are not able to register with Cisco Unified CM	• Verify that IPv6 has been enabled on the Cisco Unified CM server using platform CLI. • Verify that "Enable IPv6" enterprise parameter is set to True. • Verify Server IPv6 Name has been configured with either the hostname or the IPv6 address. If configured for hostname, verify that phone has been configured with a DNS address to resolve hostname to an IPv6 address. • Verify that Cisco Unified CM host only has 1 non link-local IPv6 address. • If the phone will get an IPv6 address via RA, verify that "Allow Auto Configuration for Phone" enterprise parameter is set to ON. • Verify Cisco Unified CM and Cisco TFTP services are running.
IPv6 calls not working	Incoming calls on V6_only SIP Trunk are not answered	• Verify that IPv6 has been enabled on the Cisco Unified CM server using CLI. • Verify that "Enable IPv6" enterprise parameter is set to True. • Verify that the INVITE does not contains IPv4 signaling.
IPv6 calls not working	Outgoing calls on V6_only SIP Trunk are not answered	• Verify that IPv6 has been enabled on the Cisco Unified CM server using CLI. • Verify that "Enable IPv6" enterprise parameter is set to True. • Verify that an IPv6 address is configured on the SIP Trunk configuration page.
IPv6 calls not working	Calls between two endpoint fail	Verify the addressing modes of the endpoints. If one is configured for IPv4_only and the other is configured for IPv6_only, ensure that a dual stack MTP is available to do the media translation.

Symptom	Possible Cause	Recommended Action
IPv6 call no MOH is heard	No MOH is heard	• Verify the addressing modes of the endpoint to which MOH is played. If the addressing mode is IPv6_only and MOH is configured for unicast, ensure that a dual stack MTP is available. • If MOH is configured for multicast, the expected behavior is that no MOH will be heard on the IPv6_only phones.
Fax works but no midcall INVITE with T.38 SDP is seen.	T38fax configuration issue.	T.38 fax relay is not being used for fax transmission. • For SIP and H.323 gateways, verify that the T.38 fax is enabled under VOIP dial-peer. • For MGCP gateway, verify fxr-package is enabled. Verify that "mgcp fax t38 inhibit" is not enabled.
Fax call fails as the initial INVITE transaction is rejected with 580 or 488.	T38fax configuration issue.	Check the locations page on both clusters and verify that the qos is enabled between the SIP trunk and endpoint. Verify that the media resources like MTP(enabled for RSVP) are configured on the endpoint's media resource group. Verify that the devices are registered with CUCM.
Initial INVITE is rejected with 420 Bad extension	End to end RSVP is not configured correctly.	If the unsupported: preconditions is seen in 420, verify that the SIP trunk is configured for E2E RSVP and PRACK is enabled on the cluster that is rejecting the call attempt.
Mid call INVITE with T.38 SDP is rejected with 488.	T38fax problem	Verify that the endpoint supports fax i.e. not an IP Phone. Verify that the endpoint is configured to support fax. See the CLI commands for the gateways.
After tandem/remote transfer, the final call is no longer E2E RSVP call.	End to end RSVP is not configured correctly.	In the transferring node, make sure the RSVP policy is activated for locations the inbound and outbound SIP Trunks assigned to.
When the call is put on hold, no E2E RSVP between the MOH server and held party	End to end RSVP is not configured correctly.	In the holding cluster, make sure the MOH's device pool has MRGL that has the RSVP agents assigned. Also make sure RSVP policy is activated for locations the MOH server and SIP Trunks assigned to.

Symptom	Possible Cause	Recommended Action
When the device in campus (Hub_none location) is making a call, no E2E RSVP.	End to end RSVP is not configured correctly.	Make sure RSVP policy is activated between Hub_none location and location that the SIP Trunk assigned to.
When the conference call is invoked, no E2E RSVP between the Conference Bridge and remote conference participants.	End to end RSVP is not configured correctly.	In the Conference invoked cluster, make sure the Conference Bridge's device pool has MRGL that has the RSVP agents assigned. Also make sure RSVP policy is activated for locations the Conference Bridge and SIP Trunks assigned to.
When a call is blind transferred to a remote system, no E2E RSVP between the Announciator and calling phone.	End to end RSVP is not configured correctly.	In the Transferring cluster, make sure the Announciator's device pool has MRGL that has the RSVP agents assigned. Also make sure RSVP policy is activated for locations the Announciator and SIP Trunks assigned to.
The original call between agent and customer is non secure. However, the non secure supervisor received reorder when trying to monitor the agent	Agent security is not configured correctly.	Check the secure capability of the agent. If the agent is encrypted, this scenario works as designed. The supervisor needs to meet or exceed the agent's secure capability in order for the monitoring call to be successful.
When conference is started during secure monitoring, the secure icon display is incorrect	Hardware problem	Check if using hardware conference bridge or default (SW) conference bridge. SW conference bridge does not support security.

Symptom	Possible Cause	Recommended Action
While using 7970/71 phones, if auto recording is enabled on these, we are unable to start a conference call	Codec negotiation problem	7970/71 phones offer/negotiate G.722 codec by default unless it is disabled. During recording, the codec is locked to be the same as the original call between the customer and agent. If using SW conference bridge with limited codec support, a transcoder maybe needed to complete the conference call. As alternative options, G.722 codec can be disabled on the agent phone or HW conference bridge which supports G.722 codec can be used.
The agent is secure and the recorder is secure. Auto recording is enabled on the agent. However, the CUCM does not send invite to the recorder	Network topology issue.	The SIP Trunk connected to the recorder needs to be secure as well for CUCM to send INVITE to the recorder. No MTP should be inserted on the SIP Trunk between agent and recorder (since MTP does not support security).
The agent is authenticated. Recording does not start on this agent	Configuration issue.	CUCM does not support recording on authenticated phones.
The farend call info is missing the remote address/directory number	This could be due to feature interaction such as Call Park/Call Retrieve	
No remote farend call information update	Configuration Issue	Use a SIP Trunk, H323 Trunk, PRI DMS100, PRI DMS250, or PRI ISO Qsig T1 between the two clusters.
The b-number is missing for a remote conference	Configuration Issue	Use a SIP Trunk between the clusters and enable 'Deliver Conference Bridge Identifier' on the remote SIP Trunk's SIP Profile.
“isfocus” is missing for a remote conference	Configuration Issue	Use a SIP Trunk or H323 trunk between the two clusters.

Symptom	Possible Cause	Recommended Action
OPTIONS message is not sent out	TCP is used and cannot create socket	If TCP is used and socket cannot be created you won't see OPTIONS going out. However you should still see the alarm in RTMT or logs.
	By default the OPTIONS is sent out every 60 or 120 seconds and you didn't wait long enough	Make sure you wait enough time or you can shorten the timer value in the SIP Profile.
	SIP trunk is not default type	Only the default type SIP trunk supports this feature. IME, SAF and EMCC SIP trunks do not. You must use a default type SIP trunk.
OPTIONS message is sent to a destination I didn't configure	If FQDN or SRV is configured as SIP trunk's destination OPTIONS is sent to ALL resolved IP addresses	Not a real issue, you can configure the IP address as the destination.
Configured SIP trunk between two UCM. One side sent OPTIONS but the other side responded with "503 Service Unavailable"	Receiving side Cisco Unified CM didn't recognize the sending side Cisco Unified CM	On the receiving side Cisco Unified CM, configure a SIP trunk that points back to the sending side Cisco Unified CM. Make sure the destination address, port number and transport type match.
Initial outgoing INVITE for Early Offer SIP trunk call does not have SDP	Early Offer configuration is disabled	Verify that the associated SIP Profile has "Enable Early Offer for voice and video calls" enabled.
	SIP Trunk is in Ipv6 only mode or dual mode with media preference as Ipv6	Verify that the SIP trunk is not in Ipv6 only mode or dual-mode trunk with ANAT or media preference set to Ipv6.
	Calling device is an Ipv6 only device	Verify that the Calling device is not an Ipv6 only device.
	Calling device is a pre-SCCP v20 device or H323 device and no MTP is available that supports GetPort capability	If initiating calls from a pre SCCP v20 device or H323 Slowstart device or delayed offer incoming call, verify that the MTP allocation is taking place. Ensure that the caller or SIP trunk MRGL has an MTP available. Verify that the MTP firmware supports getPort capability. If the MTP image does not support getPort capability, upgrade to a newer image with the fix for CSCtb19331 (IOS release: 15.1(2)T).

Symptom	Possible Cause	Recommended Action
Outgoing call for Early Offer SIP trunk fails. No INVITE is sent out	Calling device is a pre-SCCP v20 device or H323 device	If initiating calls from a pre SCCP v20 device or H323 slowstart device or delayed offer incoming trunk, verify that the MTP allocation is taking place. Ensureo that MTP supports SCCP v20. If MTP allocation fails, check the configuration for "Fail Call Over SIP trunk if MTP Allocation Fails" and set it to FALSE.
	No MTP is available that supports GetPort capability	If the MTP allocation fails, reconfigure to have an MTP in MRGL associated with SIP trunk or default pool.
	The "Fail Call Over SIP trunk if MTP Allocation Fails" configuration is set to FALSE	If the MTP image does not support getPort, upgrade to newer image with the fix for CSCtb19331 (IOS release: 15.1(2)T).
Outgoing call for Early Offer SIP trunk always has SDP with one codec and MTP's IP & Port.	The "MTP Required" configuration is enabled.	Verify that "MTP Required" is not selected on the SIP Trunk page. If "MTP Required" is not selected on the SIP trunk page, check if a media resource is being allocated. Media resource can get allocated for local RSVP, TRP enabled on trunk, Early offer, DTMF mismatch or Codec mismatch.
	MTP is getting allocated and is not configured for media passthru	Verify that the media resource is configured for pass-through codec.
Caller's QSIG/SIP Call is disconnected	On a static SIP trunk, if the originating side trunk is QSIG tunneling enabled but the terminating side trunk is not, then the call will be disconnected when originating cluster does not get first provisional response with QSIG content	On the terminating side SIP trunk, enable QSIG tunneling if possible. If the terminating cluster is based on pre-8.5 version, then disable QSIG tunneling on originating side trunk.
Cisco Telepresence MCU status shows unregistered on CUCM	Most likely a configuration issue	• Verify that the MCU address is correct • Verify that the SIP port incoming, and outgoing match what is configured on the MCU • Verify that the MCU is online and alive. • Verify that the MCU is configured for SIP. • Verify the UCM traces, and see the results for the OPTIONS ping to the MCU.

Symptom	Possible Cause	Recommended Action
MCU shows registered but can not make conference calls using that MCU	Most likely a configuration issue	Verify that the MCU http information is configured correctly, and match what is configured on the UCM, mainly: **1** Admin user name **2** Admin password **3** HTTP port **4** Verify in the UCM traces that http create Requests are being sent to the MCU, and that the MCU is sending an HTTP response back. **5** Verify that the MCU http information is configured correctly with the port reservation setting enabled.
It is not possible to add a 4th participant to the MCU Ad-Hoc conference	Most likely not enough ports available	Verify that the MCU has enough ports. Verify in the UCM traces that the HTTP modify Request is sent and that the MCU sends a Response back to UCM
V.150.1 (MER or Legacy) capabilities are lost over SIP trunk	Most likely a configuration issue	Ensure that appropriate V.150.1 SDP Filtering options are set for the trunk. Filtering options are set via the trunks associated SIP Trunk Security Profile and the "SIP V.150 Outbound Offer SDP filtering" service parameter.
MP4A-LATM codec is not selected for the call, even though both EPs supports the codec and the Region configuration limits the codec bit rate to that of MP4A-LATM	The EPs does not have matching MP4A-LATM codec parameters, even though both are MP4A-LATM-capable For example: Tandberg MXP1700 vs. Tandberg E20	For MP4A-LATM codec to be selected, not only the two End must both support the codec, they must also match on the following MP4A-LATM-specific parameters: • clock rate • profile-level-id • object • bitrate

Symptom	Possible Cause	Recommended Action
G.722.1codec is not selected for the call, even though both EPs supports the codec and the Region configuration limits audio maximum bandwidth as 32K or 24 K	Verify that both ends provide clock rate,	Cisco Unified CM only supports the G.722.1 codec with a clock rate of 16000. Both ends must provide the same clock rate.
One way audio	Verify the SDL trace.	Ensure that the dynamic Payload number is propagated between endpoints correctly if both ends are SIP devices. If a call has SIP and H.323 devices, the SIP device must honor H.323 side's dynamic PT number; this negotiation via reInvite is issued by Cisco Unified CM and sent to the SIP side. The SIP device must send back the same dynamic PT number via 200 OK. Ensure that reInvite has a=x-cisco-symm-pt.
Presentation sharing via BFCP does not work or Cisco Unified CM rejects theBFCP stream	Configuration issue or endpoint issue	There are several scenarios in which CUCM rejects the BFCP and Presentation stream. Here are a few common scenarios: • The “Allow Presentation Sharing using BFCP” SIP Profile checkbox on the SIP Trunk or SIP Line is not enabled. • One Party offers BFCP and the other Party does not offer BFCP • SIP endpoint to non-SIP endpoint. • Both sides offer BFCP but the floor control attributes within BFCP application line are in conflict. • Unsupported BFCP transport type is offered (e.g. "TCP/BFCP") • MTP, TRP, Transcoder, or RSVP Agent is inserted in the call.