SIP Line Messaging Guide (Standard Edition) for Cisco Unified Communications Manager, Release 11.5(1)

First Published: 2016-10-25

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

CHAPTER 1

SIP Standard Line Interface

This chapter describes the external interface for Cisco Unified CM SIP line-side devices. It highlights SIP primitives that are supported on the line-side interface and describes call flow scenarios that can be used as a guide for technical support and future development.

This document describes the Cisco Unified CM SIP line interface from an external interface point of view.

This chapter includes these sections:

New and Changed Information

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

- Cisco Unified Communications Manager, Release 11.5(1), on page 1

Cisco Unified Communications Manager, Release 11.5(1)

With this release, Cisco Unified Communications Manager introduces the following features for SIP lines:

- iX Channel Encryption, on page 50
- X-ULPFECUC Codec Support for Audio, on page 51

Features Supported in Previous Releases

- Cisco Unified Communications Manger, Release 11.0(1), on page 2

- Cisco Unified Communications Manager Release 10.5(2) , on page 2
- Cisco Unified Communications Manager Release 10.0(1), on page 2
- Cisco Unified Communications Manager Release 9.x, on page 3
- Cisco Unified Communications Manager Release 8.6(1), on page 3

Cisco Unified Communications Manger, Release 11.0(1)

With Release 11.0(1), Cisco Unified Communications Manager now supports the following features for SIP lines:

- ECDSA TLS Cipher Support, on page 48
- Opus Codec Support, on page 49
- Referred-By Header Support, on page 49
- Session ID Header Support, on page 50

Cisco Unified Communications Manager Release 10.5(2)

Release 10.5(2) provides the following enhancements for SIP lines:

- AES 256 GCM Support for SRTP and TLS, on page 48

Cisco Unified Communications Manager Release 10.0(1)

Cisco Unified Communications Manager Release 10.0(1) provides the following new SIP line interface enhancements:

- Cisco Unified Communications Manager Version in User-Agent and Server Headers, on page 42
- Confidential Access Level, on page 46
- Configurable NonPreemptable Numbers, on page 44
- CTI Video, on page 43
- isFocus Support, on page 44
- iX Channel Support, on page 44
- Multilevel Precedence and Preemption Using Resource Priority, on page 38
- Multiple Codecs in Answer, on page 45
- Non-SRTP Call Block, on page 45
- SDP Transparency for Declarative Attributes, on page 41
- SIP BPA/488 Error Handling, on page 45

Cisco Unified Communications Manager Release 9.x

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

- Added SIP REGISTER method for BFCP, on page 37
- Added application/conference-info+xml to Supported Content Types, on page 17 table.
- Multilevel Precedence and Preemption Using Resource Priority, on page 38
- Outgoing Identity and Incoming CLI for SIP Calls, on page 38
- URI Dialing, on page 39
- Anonymous Call Rejection for a Directory Number, on page 40

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

Cisco Unified Communications Manager Release 8.6(1)

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

- BFCP, on page 37

Note This section describes the new features and call flows added to Unified CM 8.6(1). It is recommended that you view the complete list of existing SIP basic call flows from SIP Line Messaging Guide (Standard) for Release 8.0(1)from: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

Definitions/Glossary

Acronym/Word	Definition
AOR	Address of Record
BLF	Busy Lamp Field
Cseq	Call Sequence Number
CPN	Calling Party Normalization
CSS	Calling Search Space
CTI	Computer Telephony Integration
DND	Do Not Disturb
DNS	Domain Name Server

Acronym/Word	Definition
DTMF	Dual-Tone Multifrequency
FECC	Far-End Camera Control
FMTP	Format-Specific Parameters
FQDN	Fully Qualified Domain Name
KPML	Key Pad Markup Language
MLPP	Multilevel Precedence and Preemption
MTP	Media Termination Point
MWI	Message Waiting Indication
OOB	Out Of Band
OOD	Out of Dialog
PRACK	Provisional Response ACKnowledgment
RDNIS	Redirected Dialed Number Information Service
RPID	Remote Party ID
RTT	Retransmission Time
SDP	Session Description Protocol
SIP	Session Initiated Protocol
SIS	SIP line Interface Specification
TLS	Transport Layer Security
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier
URN	Uniform Resource Name
VM	Voice Mail

Standard Interface Compliance Summary

This section provides details about Cisco Unified CM SIP line interface standards compliance. The Standard Feature Scenarios, on page 26 provides a feature implementation-oriented view of how the system works relative to the SIP line-side implementation.

Refer to the following tables for SIP line interface compliance:

- Table 1: Applicable Standards and Drafts - Standard Interface, on page 5 identifies the applicable standards and drafts.
- Table 2: Compliance to SIP Requests, on page 5 and Table 3: Compliance to SIP Responses, on page 6 provide SIP line-side compliance for SIP messages.
- Table 4: Standard SIP Header Fields, on page 8 provides SIP line-side compliance for standard SIP headers.

Table 1: Applicable Standards and Drafts - Standard Interface

Id	Notes
RFC 3261	SIP
RFC 3262	PRACK
RFC 3264	SDP offer/answer
RFC 3311	UPDATE
RFC 3515	REFER
RFC 3842	MWI Package
RFC 3891	Replaces Header
RFC 3892	Referred-by Mechanism
draft-levy-sip-diversion-08.txt	Diversion Header
draft-ietf-sip-privacy-04.txt	Remote-Party-Id Header

Table 2: Compliance to SIP Requests

SIP Message	Cisco Unified CM Supported	Comments
INVITE	Yes	The system also supports re-INVITE for outbound calls.
ACK	Yes	—

SIP Message	Cisco Unified CM Supported	Comments
OPTIONS	Yes	Cisco Unified CM will respond to it if received. Cisco Unified CM does not send OPTIONS request.
INFO	Yes	INFO method is used for video support.
BYE	Yes	—
CANCEL	Yes	—
SUBSCRIBE	No	Refer to Supported Event Packages section.
NOTIFY	Yes	Refer to Supported Event Packages section.
REFER	Yes	The system supports inbound REFER as it applies to transfer. Cisco Unified CM line side does not generate outbound REFER for transfer. It will support re-INVITE for outbound calls.
REGISTER	Yes	—
PRACK	Yes	You can configure support for PRACK.
UPDATE	Yes	Cisco Unified CM supports receiving and generating UPDATE.
PUBLISH	No	Refer to Advanced Call Flow section.

Table 3: Compliance to SIP Responses

SIP Message	Cisco Unified CM Supported	Comments
1xx Response	Yes	—
100 Trying	Yes	—
180 Ringing	Yes	Early media is supported.

SIP Message	Cisco Unified CM Supported	Comments
181 Call Forward	No	Cisco Unified CM ignores this message.
182 Queued	Yes	Cisco Unified CM ignores this message.
183 Progress	Yes	Early media is supported.
2xx Response	Yes	—
200 OK	Yes	—
202 OK	Yes	Message applies for REFER.
3xx Response	Yes	—
300–302, 305, 380, 385	Yes	This message does not generate. The system contacts the new address in the Contact header upon receiving.
4xx Response	Yes	Upon receiving, the system initiates a graceful call disconnect.
401	Yes	Cisco Unified CM SIP sends out message 401 (Unauthorized) if authentication and authorization are enabled. Cisco Unified CM SIP also responds to inbound 401 challenges.
403	Yes	Cisco Unified CM SIP sends out message 403 (Forbidden) if a SIP method is not on the Access Control List. 403 can also get returned if the system does not support a method in a particular state.
407	Yes	Cisco Unified CM SIP responds to inbound 407 (Proxy Authentication Required) challenges.

SIP Message	Cisco Unified CM Supported	Comments
412	Yes	Cisco Unified CM SIP sends out 412 if a PUBLISH refresh or PUBLISH remove request is received with an unknown entity tag.
423	Yes	Cisco Unified CM SIP 423 if an expired header is received with an expires time lower than the acceptable minimum.
5xx Response	Yes	Upon receiving this message, the system sends a new request if an additional address is present. Otherwise, the system initiates a graceful disconnect.
6xx Response	Yes	This message does not get generated. Upon receiving this message, the system initiates a graceful disconnect.

Table 4: Standard SIP Header Fields

SIP Headers	Cisco Unified CM Supported	Comments
Accept	Yes	—
Accept-Encoding	No	—
Accept-Language	No	—
Alert-Info	Yes	Cisco Unified CM sends Alert-Info to indicate internal versus external call.
Allow	Yes	—
Authentication-Info	No	—
Authorization	Yes	—
Call-ID	Yes	—
Call-Info	Yes	—

SIP Headers	Cisco Unified CM Supported	Comments
Contact	Yes	—
Content-Disposition	No	Cisco Unified CM will ignore this header if it gets received. Cisco Unified CM does not generate this header.
Content-Encoding	No	—
Content Language	No	—
Content-Length	Yes	—
Content-Type	Yes	See Supported Content Types.
CSeq	Yes	—
Date	Yes	—
Error-Info	No	—
Expires	Yes	—
From	Yes	—
In-Reply-To	No	—
Max-Forwards	Yes	Cisco Unified CM sets to 70 for outgoing INVITE and does not increment/decrement it.
MIME-Version	Yes	This header gets used with REFER.
Min-Expires	Yes	—
Organization	No	—
Priority	No	—
Proxy-Authenticate	Yes	Cisco Unified CM SIP supports receiving this header in 407 responses.

SIP Headers	Cisco Unified CM Supported	Comments
Proxy-Authorization	Yes	Cisco Unified CM SIP supports sending new request with this header after it receives 407 responses.
Proxy-Require	No	—
Record-Route	Yes	—
Reply-To	No	—
Require	Yes	—
Retry-After	Yes	Send it but ignore receiving it.
Route	Yes	—
Server	Yes	—
Subject	No	—
Supported	Yes	—
Timestamp	Yes	—
To	Yes	—
Unsupported	Yes	—
User-Agent	Yes	—
Via	Yes	—
Warning	Yes	—
WWW-Authenticate	Yes	—

Proprietary and Nonstandard SIP Headers and Identification Services

Table 5: Proprietary or Nonstandard SIP Header Fields, on page 11 lists the proprietary and nonstandard header fields for the standard SIP line-side interface. Refer to the topic Remote-Party-ID Header, on page 11 for additional information.

Table 5: Proprietary or Nonstandard SIP Header Fields

SIP Headers	Cisco Unified CM Supported	Comments
Diversion	Yes	Used for RDNIS information. If it is present, it always presents the Original Called Party info. The receiving side of this header always assumes it is the Original Called Party info if present. In case of chained-forwarding to a VM, the message will get left to the Original Called Party.
Remote-Party-ID	Yes	Used for ID services including Connected Name & ID. This nonstandard, non-proprietary header gets included in the Standard Feature Scenarios anyway.

Remote-Party-ID Header

This section describes the SIP Identification Services in the Cisco Unified CM for the SIP line, including Line and Name Identification Services. Line Identification Services include Calling Line and Connected Line Directory Number. Name identification Services include Calling Line Name, Alerting Line Name, and Connected Line Name.

The Remote-Party-ID header provides ID services header as specified in draft-ietf-sip-privacy-03.txt.

The Cisco Unified CM provides flexible configuration options for the endpoint to provide both Alerting Line Name and/or the Connected Line Name. This section does not describe those configuration options; it only provides the details on how Cisco Unified CM sends and receives these ID services to and from the SIP endpoint. The Remote-Party-ID header contains a display name with an address specification followed by optional parameters. The display carries the name while the user part of the address carries the number.

Cisco Unified CM 8.0(1) enables the Cisco Unified CM to route the localized and globalized forms of a calling number to the receiving endpoint,which is known as Calling Party Normalization (CPN). For example, when receiving a local call outside an enterprise in North America, it is desirable to display the familiar seven-digit calling number to the endpoint user (for example, 232-5757). To return a call to a local number outside the enterprise, the endpoint user typically dials an access code (for example, 9) to indicate dialing of an external directory number (92325757). This form of the calling number is referred to as the global or globalized number. The localized form of the calling number is presented in the SIP Remote-Party-ID header as the user part of the address. The globalized form of the calling number is presented as an optional SIP URI parameter.

Note Although the Remote-Party-ID header is nonstandard, many vendors implement it, and it gets included in most Cisco SIP products. Therefore, the standard section of this document includes it, even though it is effectively proprietary. The use of this header is not negotiated. Recipients should ignore it if it is not understood.

Table 6: Identification Parameters Support, on page 12 describes the support levels for identification parameters. Subsequent sections cover the following topics:

- Calling Line and Name Identification Presentation, on page 13
- Calling Line and Name Identification Restriction, on page 13
- Connected Line and Name Identification Presentation, on page 13
- Connected Line and Name Identification Restriction, on page 14

Table 6: Identification Parameters Support

Parameter	Values	Notes
x-cisco-callback-number	various	Ignored if received by Cisco Unified CM. Set to the globalized form of the calling (callback) number. The globalized from of a number is the form that, when dialed by the endpoint, is successfully routed to the desired destination with no editing by the user.
party	calling called	Ignored if Cisco Unified CM receives it. 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 Cisco Unified CM receives it. Set to subscriber for outgoing requests and responses.
privacy	full name uri off	Supported if Cisco Unified CM receives it. Cisco Unified CM will also support sending all values in either INVITE or UPDATE requests and responses for the same.
screen	no yes	Ignored if Cisco Unified CM receives it. Cisco Unified CM always sends yes when generating a Remote-Party-ID header.

Calling Line and Name Identification Presentation

The system includes the Calling Line (Number) and Name in both the From header and optionally the Remote-Party-ID headers in the initial INVITE message from the endpoint. For example, an incoming INVITE from an endpoint with directory number, 69005, and a Caller ID, “sip line,” for an outbound call will have the following Remote-Party-ID and From headers:

```
Remote-Party-ID: "sip line"
<sip:69005@10.10.10.2>;party=calling;id-type=subscriber;privacy=off;screen=yes
From: "sip line" <sip:69005@10.10.10.2>;tag=1234
```

Calling Line and Name Identification Restriction

The system conveys the SIP Line (Number) and Name restrictions by using the privacy parameter. If neither is restricted, privacy gets specified as off. The details that follow provide other values of privacy (name, uri, and full) with their impact on the various values in the From and Remote-Party-ID headers:

name

Name Restrict only—When name is restricted, the display field (Calling Name) in “From” header gets set to “Anonymous.” The display field in the “Remote-Party-ID” header still includes the actual name, but the privacy field gets set to “name.” For example:

```
Remote-Party-ID: "Anonymous"
<sip:69005@10.10.10.2>;party=calling;id-type=subscriber;privacy=name;screen=yes
From: "Anonymous" <sip:69005@10.10.10.2>;tag=1234
```

uri

Number Restrict only—When number is restricted, the system sets the calling Line to “Anonymous” out in the “From” header; however, it still gets included in the “Remote-Party-ID” header with privacy=uri. For example:

```
Remote-Party-ID: "sip line"
<sip:69005@10.10.10.2>;party=calling;id-type=subscriber;privacy=uri;screen=yes
From: "sip line" <sip:Anonymous@10.10.10.2>;tag=1234
```

full

Both Name and Number Restrict—When both name and number are restricted, the same principle applies with privacy=full. For example:

```
Remote-Party-ID: "sip line"
<sip:69005@10.10.10.2>;party=calling;id-type=subscriber;privacy=full;screen=yes
From: "Anonymous" <sip:Anonymous@10.10.10.2>;tag=1234
```

Connected Line and Name Identification Presentation

Connected Line/Name Identification is a supplementary service that provides the called or connected party number and name.

Cisco Unified CM uses the Remote-Party-ID header in 18x, 200, re-INVITE, and UPDATE messages to convey the connected name and number information. In this example, an endpoint placed a call to 9728135001. Cisco Unified CM determined that this number is for “Bob Jones” and sent that back to the originator in a 180 or 183 message.

```
Remote-Party-ID: "Bob Jones" <sip:
```

9728135001@10.10.10.2>;party=called;screen=yes;privacy=off

Connected Line and Name Identification Restriction

Similar to Calling ID services, the RPID can restrict the connected number and/or the name independently.

name

Name Restrict only—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=no;privacy=name

uri

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=no;privacy=uri

full

Both Name and Number Restrict—When both name and number are restricted, both information parameters get included with privacy=full. For example:

Remote-Party-ID: "Bob Jones"<9728135001@localhost; user=phone>;
party=called;screen=no;privacy=full

CPN Number Presentation

Calling Party Normalization is a supplementary service which provides the calling number in a localized (normalized) and globalized format. Both forms of the calling number may appear in any of the SIP request or response messages where the Remote-Party-ID is present. The localized form of the calling number is presented as the user part of the SIP URI. The globalized form is presented as an optional SIP URI parameter. For example:

Remote-Party-ID: "sip line"
<sip:2325757@10.10.10.2;x-cisco-callback-number=99192325757>;party=calling;id-type=subscriber;privacy=off;screen=yes
Because this is an optional URI parameter, endpoints that do not support the x-cisco-callback-number parameter should ignore it.

Supported Media Types

Refer to the following tables for supported media types at the SIP line interface:

- For supported audio media types, see Table 7: Supported Audio Media Types, on page 15.
- For supported video media types, see Table 8: Supported Video Media Types, on page 15.
- For supported application media types, see Table 9: Supported Application Media Types, on page 16
- For supported T38fax media types, see Table 10: Supported T38fax Payload Types, on page 16

Table 7: Supported Audio Media Types

Type	Encoding Name	Payload Type	Comments
G.711 µ-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	Supports all combinations of annex A and B.
RFC2833 DTMF	Telephony-event	Dynamically assigned	Acceptable range is 96 through 127.
G.Clear	CLEARMODE	Dynamically assigned	Typically 125 for all Cisco products. Cisco Unified CM supports other encoding names such as X-CCD, CCD, G.nX64 as well.

Table 8: 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.
H.264 SVC	H264-SVC	Acceptable range is 96-127
X-H.264 UC	X-H264UC	Acceptable range is 96-127
X-ULPFECUC	X-ULPFECUC	Acceptable range is 96-127
H.265	H265	Acceptable range is 96-127

Table 9: Supported Application Media Types

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

Table 10: Supported T38fax Payload Types

Types	Encoding Name	Payload Type
T38fax	Not applied	Not applied

Supported Event Packages

Table 11: Supported Event Packages, on page 16 provides supported event packages at the SIP line interface.

Table 11: Supported Event Packages

Event Package	Supported	Subscription or Unsolicited	Comments
message-summary	Yes	Unsolicited	Used for Message Waiting Indication notifications.
kpml	Yes	Subscription	Used for digit collection and DTMF relay.
dialog	Yes	Subscription	Used for hook status (offhook and onhook only). Used for shared line remote state notifications.
presence	Yes	Subscription	Used for BLF speed dials. Used for DND status. Used for missed, placed, and received calls as well as other directory services. Used for BLF alert indicator.

Event Package	Supported	Subscription or Unsolicited	Comments
refer	Yes	Subscription	Used to carry sipfrag responses during call transfer. Used to carry remotecc responses.
service-control	Yes	Unsolicited	Used to send service control notifications to the endpoint.

Supported Content Types

Table 12: Supported Content Types, on page 17 provides supported content types at the SIP line interface.

Table 12: Supported Content Types

Content Type	Comments
text/plain	See message-summary package.
message/sipfrag;version=2.0	See refer package as used for transfer.
application/pidf+xml	See presence package.
application/dialog-info+xml	See dialog package.
application/kpml-request+xml	See kpml package.
application/kpml-response+xml	See kpml package.
application/x-cisco-remotecc-request+xml	See refer package and remotecc.
application/x-cisco-remotecc-response+xml	See refer package and remotecc.
application/x-cisco-remotecc-cm+xml	See refer package and remotecc.
application/x-cisco-servicecontrol	See service-control package.
application/x-cisco-alarm+xml	See Phone Alarm System.
multipart/mixed	See refer package and remotecc.
application/conference-info+xml	Used only by Third-Party AS-SIP Endpoints for the conference factory method of conferencing.

SIP Message Fields

Cisco Unified CM SIP line supports request messages and response messages. The request messages include INVITE, ACK, OPTIONS, BYE, CANCEL, PRACK, and UPDATE methods. The response message comprises the status line with various status codes (1xx, 2xx, 3xx, 4xx, 5xx and 6xx). SIP line supports all mandatory fields in the SIP standard interface.

Request Messages

The following sections provide individual summaries for some types of SIP requests. These sections examine the dialog-initiating requests. You can deduce the values that midcall transactions use from these requests.

The SIP Request messages detailed in this section include:

- INVITE, on page 18
- ACK, on page 20

INVITE

Table 13: INVITE Message Fields, on page 18 provides the fields of INVITE SIP Request message.

Table 13: INVITE Message Fields

Message Lines	Variable	Incoming (to Cisco Unified CM)	Outgoing (from Cisco Unified CM)
INVITE sip:userpart@destIP:destPort SIP/2.0	userpart	Called Party Number	Calling Party Number
	destIP	Cisco Unified CM IP address or FQDN	Endpoint IP address
	destPort	Cisco Unified CM SIP port	Endpoint SIP port
Via: SIP/2.0/UPD ip:port;Branch=number	ip	Endpoint IP address	Cisco Unified CM IP address
	port	Endpoint SIP port	Cisco Unified CM SIP port
	number	Endpoint branch number	Cisco Unified CM branch number

Message Lines	Variable	Incoming (to Cisco Unified CM)	Outgoing (from Cisco Unified CM)
From: "display" <sip:userpart@ip>;tag=from-tag	display[1]	Calling Party Name	Calling Party Name
	userpart	Calling Party Number	Calling Party Number
	ip	Cisco Unified CM IP address or FQDN	Cisco Unified CM IP address
	from-tag	Endpoint local tag	Cisco Unified CM local tag
To: <sip:userpart@destIP>	userpart	Called Party Number	Called Party Number
	destIP	Cisco Unified CM IP address or FQDN	Endpoint IP address
Remote-Party-ID: "display" <sip:userpart@ip>;params	display	Calling Party Name	Calling Party Name
	userpart	Calling Party Number	Calling Party Number
	ip	Endpoint IP address	Cisco Unified CM IP address
	params	Varies per Endpoint	Varies per Cisco Unified CM configuration
Call-ID: string	string	Endpoint-generated string	Cisco Unified CM generated string
Contact: <sip:userpart@ip:port >	userpart	Calling Party Number	Calling Party Number
	ip	Endpoint IP address	Cisco Unified CM IP address
	port	Endpoint port	Cisco Unified CM port
Cseq: number method	number	sequence number	Sequence number
	method	SIP method	SIP method
Max-Forwards: number	number	Max forwards	Max forwards

Message Lines	Variable	Incoming (to Cisco Unified CM)	Outgoing (from Cisco Unified CM)
SDP [sdp]	sdp	Endpoint SDP	Cisco Unified CM typically uses delayed media.

1. Any display field in any SIP header can be encoded as ASCII or Unicode.

ACK

The ACK message values will reflect the values that were established by the INVITE/18x/200 message sequence.

Note The ACK may contain SDP and Remote-Party-ID headers.

Response Messages

Note The order of the outgoing and incoming columns is switched in the following table compared to the preceding table for the INVITE messages. This way, the columns align according to dialog across these tables; in other words, an incoming INVITE to Cisco Unified CM results in an outgoing 180 message.

The SIP Response messages that are detailed in this section include

- 180 Ringing, on page 20
- 183 Session Progress, on page 22
- 2xx, on page 22

180 Ringing

Table 14: 180 Ringing Message Fields, on page 20 provides the fields of 180 Ringing SIP Response message.

Table 14: 180 Ringing Message Fields

Message Lines	Variable	Outgoing (from Cisco Unified CM)	Incoming (to Cisco Unified CM)
SIP/2.0 180 Ringing			

Message Lines	Variable	Outgoing (from Cisco Unified CM)	Incoming (to Cisco Unified CM)
Via: SIP/2.0/UPD ip:port;Branch=number	ip	Endpoint IP address	Cisco Unified CM IP address
	port	Endpoint SIP port	Cisco Unified CM SIP port
	number	Endpoint branch number	Cisco Unified CM branch number
From: "display"<sip:userpart@ip>;tag=from-tag	display	Calling Party Name	Calling Party Name
	userpart	Calling Party Number	Calling Party Number
	ip	Cisco Unified CM IP address or FQDN	Cisco Unified CM IP address
	from-tag	Endpoint local tag	Cisco Unified CM local tag
To: <sip:userpart@destIP>;tag=to-tag	userpart	Called Party Number	Called Party Number
	destIP	Cisco Unified CM IP address or FQDN	Endpoint IP address
	to-tag	Cisco Unified CM local tag	Endpoint local tag
Remote-Party-ID: “display” <sip:userpart@ip>;params	display	Called Party Name	Called Party Name
	userpart	Called Party Number	Called Party Number
	ip	Cisco Unified CM IP address	Endpoint IP address
	params	Varies per Cisco Unified CM processing	Varies per endpoint processing

Message Lines	Variable	Outgoing (from Cisco Unified CM)	Incoming (to Cisco Unified CM)
Call-ID: string	string	Endpoint-generated string from the initial INVITE	Cisco Unified CM-generated string from the initial INVITE
Contact:<sip:userpart@ip:port >	userpart	Called Party Number	Called Party Number
	ip	Cisco Unified CM IP address	Endpoint IP address
	port	Cisco Unified CM port	Endpoint port
Cseq: number INVITE	number	Sequence number from initial INVITE	Sequence number from initial INVITE
SDP [sdp]	sdp	Cisco Unified CM SDP	Endpoint SDP

183 Session Progress

The 183 message establishes early media. Cisco Unified CM will include SDP in a 183 message that is sent to an endpoint. The Remote-Party-ID header may have changed as well. Otherwise, a 183 carries the same values as a 180.

2xx

Note Most 2XX values match the 180 message; 200 carries SDP. Also, the Remote-Party-ID may have changed after a 18x message was sent.

Table 15: 2XX Message Fields, on page 22 provides the fields of 2xx SIP Response message.

Table 15: 2XX Message Fields

Message Lines	Variable	Outgoing (from Cisco Unified CM)	Incoming (to Cisco Unified CM)
SIP/2.0 200 OK			

Message Lines	Variable	Outgoing (from Cisco Unified CM)	Incoming (to Cisco Unified CM)
Via: SIP/2.0/UPD ip:port;Branch=number	ip	Endpoint IP address	Cisco Unified CM IP address
	port	Endpoint SIP port	Cisco Unified CM SIP port
	number	Endpoint branch number	Cisco Unified CM branch number
From: "display"<sip:userpart@ip>;tag=from-tag	display	Calling Party Name	Calling Party Name
	userpart	Calling Party Number	Calling Party Number
	ip	Cisco Unified CM IP address or FQDN	Cisco Unified CM IP address
	from-tag	Endpoint local tag	Cisco Unified CM local tag
To: <sip:userpart@destIP>;tag=to-tag	userpart	Called Party Number	Called Party Number
	destIP	Cisco Unified CM IP address or FQDN	Endpoint IP address
	to-tag	Cisco Unified CM local tag	Endpoint local tag
Remote-Party-ID: “display” <sip:userpart@ip>;params	display	Called Party Name	Called Party Name
	userpart	Called Party Number	Called Party Number
	ip	Cisco Unified CM IP address	Endpoint IP address
	params	Varies per Cisco Unified CM processing	Varies per endpoint processing

Message Lines	Variable	Outgoing (from Cisco Unified CM)	Incoming (to Cisco Unified CM)
Call-ID: string	string	Endpoint-generated string from the initial INVITE	Cisco Unified CM-generated string from the initial INVITE
Contact:<sip:userpart@ip:port >	userpart	Called Party Number	Called Party Number
	ip	Cisco Unified CM IP address	Endpoint IP address
	port	Cisco Unified CM port	Endpoint port
Cseq: number INVITE	number	Sequence number from initial INVITE	Sequence number from initial INVITE
SDP [sdp]	sdp	Cisco Unified CM SDP	Endpoint SDP

Message Timers

The following timers are service parameters that are configurable in Cisco Unified Communications Manager Administration.

The following table provides the configuration data for the SIP timers that Cisco Unified Communications Manager maintains.

Table 16: Message Timers

Message	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

Message	Value (Default/Range)	Definition
rel1xx	500 ms / 100–1000 ms	The time that Cisco Unified CM should wait before retransmitting the reliable 1xx responses
prack	500 ms /1 00–1000 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	2147483647	Cisco Unified CM does not manage a timer for aging out published event state data it receives from endpoints. Cisco Unified CM requires endpoints to specify an expires time of 2147483647 when publishing event state data to Cisco Unified CM.

Message Retry Counts

All the following retry counts are service parameters that are configurable in Cisco Unified Communications Manager Administration. In case of TCP transportation type, the timers will still pop as usual. In the event of timeout, however, the stack will not retransmit; it will rely instead on TCP itself to do the retry.

Table 17: Message Retry Counts, on page 25 provides the configuration data for the SIP retries that Cisco Unified Communications Manager maintains.

Table 17: 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

Counter	Default Value	Suggested Range	Definition
Rel1xx retry count	10	1-10	Number of Reliable 1xx response retries
Notify retry count	6	1-10	Number of NOTIFY retries

Standard Feature Scenarios

This section provides details with respect to overall flow and handling of standard SIP features on the Cisco Unified CM line-side interface. This includes, but is not limited to, the following features:

- Registration, on page 26
- Basic Call, on page 28
- Simple Hold and Resume, on page 28
- Transfer, on page 28
- Three-Way Calling, on page 30
- Call Forwarding, on page 31
- Message Waiting Indication, on page 32
- Endpoint Returns 302 Redirect, on page 32
- Endpoint Returns 486 Busy, on page 32
- Announcements for Certain Call Setup Failures, on page 33
- INFO Packages, on page 33
- G.Clear Calls, on page 36
- BFCP, on page 37

Registration

Cisco Unified CM supports standard RFC3261 registration from any compliant SIP phone. Because Cisco Unified CM is a B2BUA, however, it must be able to uniquely identify the registering device to match that device with a configuration entry in the database. Furthermore, Cisco Unified CM must be able to identify the originating device (and line) for all other SIP requests that it receives (INVITE, REFER, SUBSCRIBE, and so on) to authorize, filter, and route the message. Because standard SIP does not provide a consistent and unambiguous mechanism for identifying the originating device, for standard registration, Cisco Unified CM relies on the HTTP digest user ID to identify the sending device.

Knowledge of the sending device and line allows Cisco Unified CM to apply various routing, authorization, and filtering logic to incoming registrations, subscriptions, and invites.

The system supports TCP and UDP transports for Standard registration, but not TLS.

Source Device ID for RFC3261-Compliant Phones

Cisco Unified CM must uniquely identify the device sending the REGISTER message to apply authentication, routing, and filtering. The Contact IP address is not suitable because it can change dynamically if DHCP is used. Instead, Cisco Unified CM uses the HTTP digest user ID. Each device that is configured in Cisco Unified CM requires a unique digest user ID. When the device sends the REGISTER, Cisco Unified CM will immediately respond with a 401 challenge to get the Authentication header. The system uses the user ID from the authentication header to find the configuration entry in the database. If the third-party phone is not configured with the correct user ID, or the user ID is not associated with the device in the Cisco Unified CM database, Cisco Unified CM will respond with a 404 Not Found.

MultiLine Registration

Multiple lines can register with Cisco Unified CM if each line has a unique directory number. The directory number must appear in the To and From header of the REGISTER, and it must be numeric.

REGISTER Refresh (Keepalive)

Cisco Unified CM uses REGISTER refreshes as keepalive messages to ensure the phone is still alive and connected. When the phone first registers with Cisco Unified CM, the 200OK response will include an Expires header with the configured keepalive interval. The phone must send a REGISTER refresh within this interval with the same Call ID, Contact IP address, and Contact port number. If Cisco Unified CM fails to receive a keepalive message within the configured interval (default 120 seconds), it will unregister the phone internally, so no calls can originate from or terminate to the phone.

Device Binding

After the device has been identified by the digest user ID, the system creates a binding within Cisco Unified CM between that device ID and the transport address. This binding gets created because Cisco Unified CM must identify the sending device for all subsequent requests from the phone (INVITE, REFER, SUBSCRIBE, and so on), and these requests do not contain the device ID. However, these requests do contain source transport information, so the binding gets created between the device ID and the transport information. The transport information that is used differs for UDP and TCP.

For UDP, the system creates the binding between the device ID and the IP address and port number in the Contact header. After the first REGISTER message is sent, all subsequent requests must use the same IP address and port number in the Contact header. If it changes, a 5xx error response gets returned because Cisco Unified CM cannot route the message.

For TCP, the system uses a combination of Contact binding and TCP connection binding. When a device registers over a TCP connection, Cisco Unified CM cannot determine whether the TCP connection will be transient (a new connection gets used for each transaction) or persistent. Therefore, Cisco Unified CM initially binds the device ID to the Contact IP address and port number. After several transactions get sent over the same TCP connection, the system considers it as proved-in and marks it as persistent. At this point, a binding gets created between the device ID and the TCP connection.

Multiple Bindings for the Same AOR

Cisco Unified CM includes a minor deviation from RFC3261 for the case of multiple registration bindings for a single address of record. Under the Cisco Unified CM architecture, if three devices are configured to have a shared line at 321-1000, each will register a contact in the form of 3211000@ip:port for that line. Each device will have its own unique IP address and thus have a unique contact for that line. RFC3261 states that, upon registration, all known contact bindings shall be returned to the registering entity in the 200OK response. Cisco Unified CM will only return the contact binding of the registering device during each registration; it will not enumerate other bindings that it knows about for a given AOR during registration. A registering endpoint should not rely on the binding list that is returned in the 200OK response as an exhaustive list for all bindings that are associated with the AOR. In addition, an endpoint cannot modify bindings for another device through Cisco Unified CM; it can only refresh or delete its own binding.

Contact: *

Cisco Unified CM deviates from RFC3261 in that it does not support the Contact: * format. This format is often used to unregister all contacts currently associated with an AOR. However Cisco Unified CM requires that the Contact header in each REGISTER message must contain the SIP URI identifying the device, and the unregister message (REGISTER with Expires: 0) must contain the same Contact header as the original REGISTER message.

This restriction occurs because Cisco Unified CM must be able to identify the source device for each incoming SIP message, and it uses the Contact header for that purpose. Cisco Unified CM cannot use the AOR in the To header because the shared line feature allows multiple different source devices to have the same AOR; thus, it is not unique to a specific device.

Basic Call

Cisco Unified CM follows the procedures that are described in RFC 3261, 3262, and 3264 to establish and clear down basic SIP calls. Often, on the outgoing side, Cisco Unified CM will send out INVITE without SDP. This allows Cisco Unified CM to discover the capabilities of both sides and provide media services in between if necessary (for example, transcoding).

Simple Hold and Resume

Cisco Unified CM SIP line side supports simple media hold as per RFC 2543 (a.k.a. c = 0) or as per RFCs 3261 and 3264 (a = sendonly or a = inactive).

Transfer

SIP line-side Transfer uses the REFER message, and REFER with an embedded Replaces header, as per RFC 3515.

The following three participants exist for call transfer:

- **Transferee—**The person who is being transferred.
- **Transferor—**The person who is transferring the call.

- Transfer Target (Target)—The person who is receiving the transfer.

Cisco Unified CM supports three types of transfer:

- Attended (also known as Consultative)
- Early Attended
- Blind

Attended Transfer

With attended transfer, the transferor places the transferee on hold and calls the target. After conversing with the target, the transferor completes the transfer and drops out of the call. The transferee automatically gets taken off hold and connected to the target.

Attended transfer involves two somewhat independent dialogs at the transferor device up until the time the device sends a REFER with embedded replaces header. When this message is received, Cisco Unified CM knows that the calls are associated.

Because Cisco Unified CM is a B2BUA, a REFER with embedded replaces does not trigger an INVITE with replaces from the transferee to the transfer target. The dialogs between Cisco Unified CM and each phone stay independent. Instead, Cisco Unified CM reINVITEs (and UPDATEs) the transferee and transfer target to connect them together. During this process, the transferor will receive sipfrag NOTIFY messages. After the connection is complete, both dialogs between Cisco Unified CM and transferor get BYE'd.

The following more detailed view shows what happens when the REFER is received:

1. Split transferor and transferee call:
    - reINVITE to disconnect media.
2. Split transferor and transfer target call:
    - reINVITE to disconnect media.
3. Join transferee and transfer target call legs:
    a. reINVITE to connect media.
    b. UPDATE display name and number via Remote-Party-ID header.
4. Clear transferor dialogs.

Early Attended Transfer

With early attended transfer, the transferor places the original call on hold and calls the target. Upon receiving a ringback tone, the transferor transfers the call to the target and drops out of both calls. The transferee receives a ringback while the target phone is alerting. When the target answers, the system establishes a connection between transferee and target.

The transferor call flow, which uses a REFER with embedded replaces header, is based on the existing implementation of this feature on the SIP phones and gateways. The problem with this implementation in a peer-to-peer environment is the failure to support parallel forking to multiple targets. Version 04 of the replaces draft specifically precludes a UAS from accepting a replaces header that was not initiated by that UA. The receiving UAS must to return a 481 message in that situation. Instead, the existing implementation honors the request and replaces the early dialog. That causes it to send a 487 message back to the transferor.

Early attended transfer involves two somewhat independent dialogs at the transferor device up until the time the device sends a REFER with embedded replaces header. When this message is received, Cisco Unified CM registers that the calls are associated. Because Cisco Unified CM is a B2BUA, a REFER with replaces header does not trigger an INVITE with replaces from the transferee to the transfer target. The dialogs between Cisco Unified CM and each phone stay independent. Instead, Cisco Unified CM reINVITEs (and UPDATEs) the transferee and transfer target to connect them together. During this process, the transferor will receive sipfrag NOTIFY messages. After the connection is complete, both dialogs between Cisco Unified CM and transferor get BYE'd.

The following more detailed view shows what happens when the REFER is received:

1. Split transferor and transferee call:
    - reINVITE to disconnect media.
2. Split transferor and transfer target call:
    - reINVITE sent to transferor to disconnect media.
3. Join transferee and transfer target call legs
    1. reINVITE to connect media.
    2. UPDATE display name and number via Remote-Party-ID header.
    3. Clear transferor dialogs.

The transferee will not receive a ringback although the target is alerting.

Blind Transfer

With blind transfer, the transferor places the original call on hold and dials the target. The transferor then uses SIP REFER to redirect the transferee to the target. No call gets made to the target prior to transfer. The timing for when the transferor drops out of the call depends on the transferor implementation of the feature, but, most likely, the drop occurs when the transferor is notified that the redirect operation was accepted and has begun.

The REFER does not contain an embedded replaces as it does for attended and early attended transfer.

Three-Way Calling

Many SIP phones support local mixing by the endpoint. For example, the existing SIP implementation on the Cisco Unified IP Phone 7960/40 supports it. It will continue to work for Cisco Unified CM line-side SIP endpoints. To support local mixing on the phone, Cisco Unified CM must allow the endpoint to have multiple active calls. Cisco Unified CM will allow this for SIP endpoints. From the Cisco Unified CM perspective, a locally mixed three-way call (or an n-way call) just looks like individual active calls. Cisco Unified CM does not perceive local mixing. Cisco Unified CM conference-related features like Conference List and Remove Last Party do not apply.

In a SIP environment, the endpoint that is hosting a three-way call can drop out and arrange to have the remaining two parties connected together. With SIP, the system accomplishes this by using REFER with embedded replaces. Prior to this action, two calls with four dialogs exist:

1. A.1 to B call:
   1. A.1 to Cisco Unified CM dialog.
   2. Cisco Unified CM to B dialog.
2. A.2 to C call:
   1. A.2 to Cisco Unified CM dialog.
   2. Cisco Unified CM to C dialog.

Phone A can drop out of the call by sending an in-dialog REFER on dialog A.1 with an embedded replaces header that specifies dialog A.2. Cisco Unified CM will invoke its attended transfer feature, which results in the remaining parties being connected together. Refer to the Attended Transfer, on page 29 for details regarding the operation of that feature.

Call Forwarding

Call Forwarding occurs when a call does not get answered by the original called party but, instead, gets presented to one or more subsequent forwarded parties. Cisco Unified CM supports three types of forwarding:

- Call Forward All (also known as Call Forward Unconditional)
- Call Forward No Answer
- Call Forward Busy

In only in the call forward no answer case does the call actually get presented to the original called party. Cisco Unified CM detects call forward all and call forward busy prior to sending an INVITE to the called party, so forwarding bypasses that party. Call forward no answer will get detected via a timer in Cisco Unified CM, so Cisco Unified CM will initiate the canceling of the call to the original called party.

Older Cisco phones that use SIP or third-party SIP phones may elect to implement forward all and forward busy locally on the phone, in which case they will need to use 302 (see Endpoint Returns 302 Redirect, on page 32) and 486 (see Endpoint Returns 486 Busy, on page 32 response codes, respectively, to the INVITE.

Cisco Unified CM informs the calling party that their call has been forwarded via “Remote-Party-ID:” headers in updated 180 messages. The type of forwarding does not get communicated to the calling party.

For example:

Remote-Party-ID: "Line 1030 Name"
<sip:1030@172.18.203.78>;party=called;id-type=subscriber;privacy=off;screen=yes
Cisco Unified CM indicates forwarding to the called (or current forwarded-to) party by using “Diversion:” headers in subsequent INVITEs. Cisco Unified CM will report, at most, two diversion headers. The first will indicate the last forwarding party, and the second will indicate the original called party. In a single-hop forwarding case, the system uses only a single diversion header because the original called party and last forwarding parties are the same. In a three-or-more-hop case, the intermediate parties do not get communicated to the current forwarded-to party. For example

Diversion: "Line 1020 Name"
<sip:1020@172.18.203.99>;reason=no-answer;privacy=off;screen=yes
Diversion: "Line 2020 Name"
<sip:2020@172.18.203.99>;reason=unconditional;privacy=off;screen=yes

Diversion: "Line 3020 Name"
<sip:3020@172.18.203.99>;reason=user-busy;privacy=off;screen=yes
The phone may activate Call Forward All via a softkey.

Message Waiting Indication

The system triggers activation of the Message Waiting Indication (MWI) on the phone via an unsolicited NOTIFY from Cisco Unified CM. The NOTIFY will have an event type of "message-summary" and a message body with content type of "application/simple-message-summary" and a body that contains either "Messages-Waiting: yes" to instruct the phone to turn on its MWI or "Messages-Waiting: no" to instruct the phone to turn off its MWI.

This MWI Notify will get sent whenever that Cisco Unified CM detects that the phone MWI status should change. This could occur if a message is left for that subscriber on a connected voice messaging server and that voice messaging server informs Cisco Unified CM or if all messages are cleared. Additionally, this NOTIFY that contains the current MWI state always gets sent during registration of a line, so phones with flash memory have the latest MWI state that is known to Cisco Unified CM.

Endpoint Returns 302 Redirect

Because not all SIP phones will support the enhanced call forward all activation behavior to synchronize the call forward all state between the phone and Cisco Unified CM, some phones may allow the user to configure a call forward number on the phone locally and then return a 302 message to an INVITE instead.

The 302 message must contain a "Contact:" header that indicates the party to which the call should be forwarded. A phone that sends a 302 should also include a "Diversion:" header that includes its own name and number as well as the reason for forwarding.

When Cisco Unified CM receives a 302 message from a phone, the system presents the call to the next party that is indicated in the contact header of that 302 with the diversion header from the 302 that is listed first (assuming the next party is also a SIP device). If that next party also forwards, the diversion header that is sent in the first 302 may get passed along to subsequent forwarded-to parties if the phone that is sending the 302 was the original called party.

Endpoint Returns 486 Busy

You can configure all lines on a Cisco Unified CM with a "busy trigger." After the number of active calls to that line reaches the busy trigger, Cisco Unified CM will prevent further calls from being presented to that phone by initiating a call forward busy without sending another INVITE to the phone.

However, due to misconfiguration or the potential for calls of which Cisco Unified CM is not aware to exist on the phone (for example, a phone in a dialing state that has not yet sent an INVITE), the phone may need to manage its own busy trigger and autonomously throttle calls. Phones accomplish this by sending a 486 response code to an INVITE.

Although Cisco Unified CM may have Call Forward Busy behavior configured for a line (for example, forward to DN or forward to a voice-messaging system), that behavior does not get exercised when a 486 message is received from the phone. Instead, the 486 message will be passed back to the original called party.

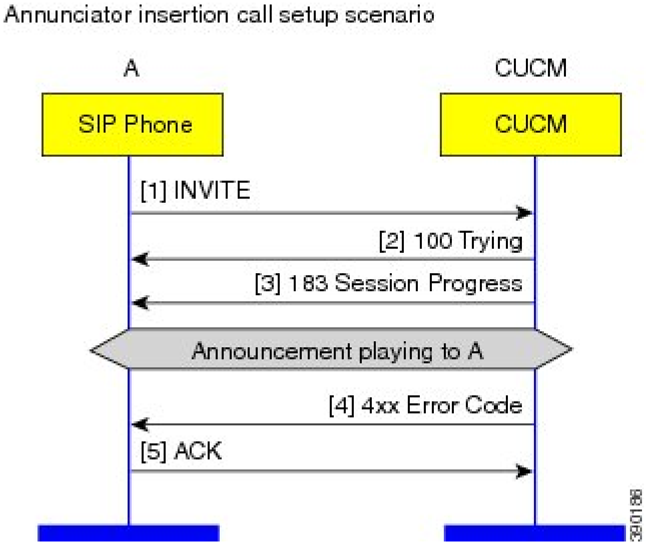
Announcements for Certain Call Setup Failures

When Party A calls Party B, there are circumstances in which the call cannot complete and an announcement as to the reason for the call failure is played to party A. A simple example is when party A misdials the B's number and the misdialed number does not exist. This results in a vacant code error.

In this same scenario if Party A were a SCCP phone, then party A would be connected to an annunciator and would receive an announcement similar to "`Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording.`" Once the announcement is completed, the Party A would hear the re-order tone if they were still offhook. Previous to Cisco Unified CM 8.0 if Party A were SIP, they would immediately hear re-order locally on the phone as a result of the 4xx SIP error message and not hear the announcement- Cisco Unified CM 8.0, SIP phones now have parity for error scenarios where an announcement is performed (for example, vacant code).

The call flow for these announcements utilizes standard SIP. A sample of the flow is shown below. In this scenario, announcement is played and the 4xx/5xx error code is sent as before. The SIP 183 contains SDP.

Figure 1: Annunciator Insertion Call Setup Scenario



Error scenarios that may result in announcements during call setup include vacant code and certain call setup failures that result from MLPP.

INFO Packages

During the life of an INVITE dialog, INFO packages allow SIP UA's to exchange negotiated content without managing and correlating a subscription. The INFO package negotiation occurs during initial call setup and is remembered throughout the life of the INVITE dialog. This is independent of the number of times the endpoint is subject to some feature interaction such as transfer or conference.

Unified Communication Manager supports the conference package. The negotiation works according to the rules spelled out in the following draft:

draft-ietf-sip-info-events-01.txt.

INFO Conference Package Negotiation

Unified Communication Manager is a B2BUA. As such, each endpoint has their own specific INVITE dialog with Unified Communication Manager, when a call is established. Due to feature invocations, Unified Communication Manager can move the media around, while maintaining the original INVITE dialog. For example, if A transfers B to C, B and C just get reINVITEs and UPDATEs to redirect their media towards each other and to update the connected party information. The original dialogs established between B and Unified Communication Manager and C and Unified Communication Manager prior to the transfer remain intact.

The conference INFO package negotiation occurs during initial call setup and is remembered throughout the life of the INVITE dialog. This is independent of the number of times the endpoint is subject to some feature interaction such as transfer or conference. The actual conference package XML is borrowed from the following RFC:

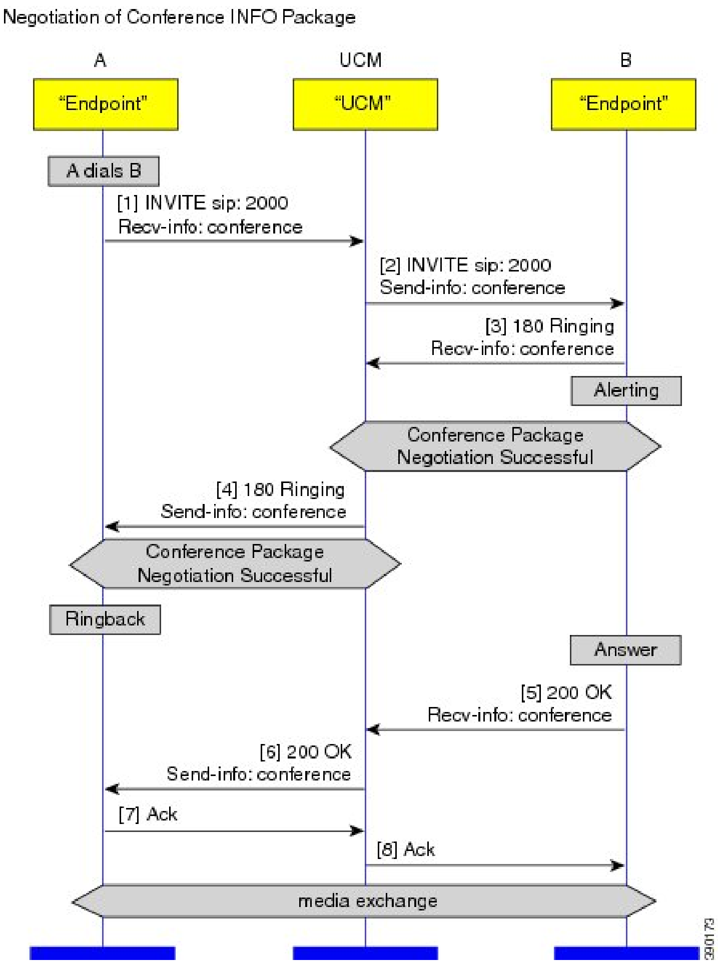
RFC-4575, A Session Initiation Protocol (SIP) Event Package for Conference State

RFC defines the package in the context of the SUBSCRIBE/NOTIFY framework. The same XML schema can be used in the INFO event package framework.

The negotiation within the context of Unified Communication Manager works the following way:

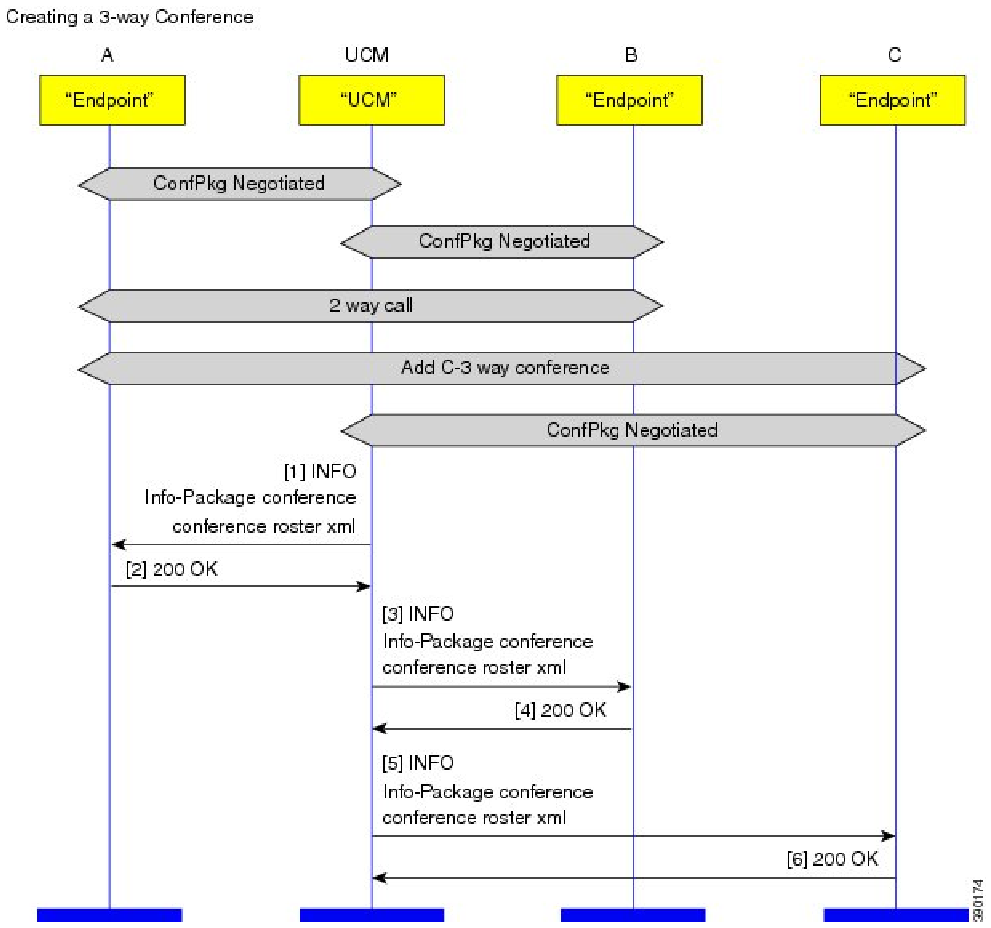
When A calls B, this is two distinct dialogs since Unified Communication Manager is a B2BUA. In this example, A is the initiator of the dialog between A and Unified Communication Manager. On the other hand, Unified Communication Manager is the initiator of the dialog between Unified Communication Manager and B. The negotiation works based on who initiates the dialog and who is the sender versus receiver of the data. In our example, A and B are receivers and Unified Communication Manager is the sender of conference roster updates. Figure 2: Negotiation of Conference INFO Package, on page 35 shows how Send-Info and Recv-Info headers are used in this example to negotiate usage of INFO conference package. If an endpoint doesn't include the header, Recv-Info: conference, then Unified Communication Manager will not send INFO messages with the conference package if the call is later connected to a conference.

Figure 2: Negotiation of Conference INFO Package



Having negotiated use of the INFO conference package, the endpoint must be ready to receive conference INFO at any time during the life of the dialog. It may find itself in and out of conferences throughout the life of the dialog. End of the conference does not guarantee that the endpoint will not receive more conference updates. The call could transit from 3 way to 2 way and back to 3 way. Figure 3: Creating 3-way Conference, on page 36 depicts creation of a 3 way conference:

Figure 3: Creating 3-way Conference



G.Clear Calls

Cisco Unified CM supports voice and video calls. It also establishes a media session between two registered SIP endpoints using the G.Clear codec. A G.Clear media session uses RTP to establish a 64kbps transparent data channel between two devices. This allows data streams generated by ISDN terminals to be transparently being carried via an IP network Please refer to RFC 4040 for details.

Cisco Unified CM supports the following:

1. G.Clear codec (RFC 4040) handling in SIP signaling and codec negotiation.
2. Including SDP in the outgoing INVITE from Cisco Unified CM for G.Clear calls without requiring an MTP.

Example SDP for G.Clear Call

SIP endpoints capable of initiating a G.Clear calls sends the indication by using the G.Clear codec in the m=audio line of the INVITE SDP.

Note Only third party SIP devices are capable of initiating a G.Clear call with Cisco Unified Communication Manager.

Example SDP having a G.Clear codec:

```
v=0
o=XYZ 317625 317625 IN IP4 172.18.199.61
s=XYZ
c=IN IP4 172.18.199.61
t=0 0
m=audio 30002 RTP/AVP 125
a=rtpmap:125 CLEARMODE/8000
a=ptime:20
```

Cisco Unified CM also support other rtpmap attributes in addition to the CLEARMODE. It can identify X-CCD, CCD and G.nX64 rtpmap attributes as G.Clear codec in incoming SDPs. Cisco Unified CM supports sending one of these values - CLEARMODE, X-CCD, CCD and G.nX64 in rtpmap attribute of the outgoing SDP. This is based on Cisco Unified CM configuration. For example, Cisco Unified CM need to be configured to send this attribute line for a G.Clear codec in outgoing SDPL:

```
a=rtpmap:125 X-CCD/8000
```

Early Offer Support for G.Clear Calls

Cisco Unified CM shall route the call based on called number in the INVITE request-uri to another SIP endpoint or over SIP trunk. Cisco Unified CM shall include the offer SDP in the outgoing INVITE for G.Clear calls, which is configurable. The SDP included in outgoing INVITE is received from the incoming SIP call leg. Therefore Cisco Unified CM supports, sending offer SDP in outgoing INVITE without requiring an MTP, only for G.Clear calls. Cisco Unified CM Voice calls will still require “MTP Required” checkbox to be enabled in order to include SDP for voice calls.

BFCP

The 8.6(1) release of Cisco Unified CM adds support for negotiation of the Binary Floor Control Protocol (BFCP) between SIP Line and SIP Trunk devices participating in calls that include a presentation sharing session. Presentation sharing is the ability to send a second video stream such as a PowerPoint slide presentation in addition to the main video stream. BFCP enables this functionality.

A sample use case scenario consists of two users in a video call via their Cisco EX90 phones. Each user has the video output of their laptop computer connected to their respective EX90 via HDMI or DVI. During the call, user A on his EX90 decides to share his laptop video with user B. User A presses the "Present" button on the EX90. The EX90s and Cisco Unified CM would utilize SIP and BFCP protocols to enable User B to see User A's main video along with the User A's laptop video.

BFCP is an SDP-only feature and does not entail any signaling related changes.

BFCP is enabled by default for all Cisco TelePresence endpoints.

As of release 9.0(1), other Cisco endpoints that support BFCP can enable the feature in Cisco Unified Communications Manager by advertising BFCP capability to Cisco Unified Communications Manager in the SIP REGISTER message as follows:

```
<optionsind>
<bfcp></bfcp>
</optionsind>
```

Third party endpoints that register to Cisco Unified Communications Manager can enable the feature in the Phone Configuration window of Cisco Unified CM Administration.

Multilevel Precedence and Preemption Using Resource Priority

Cisco Unified CM supports Multilevel Precedence and Preemption (MLPP) for both Cisco and third-party endpoints, based on the configured device type. Cisco Unified CM only supports MLPP for certain models. The Resource Priority header communicates precedence information between the Cisco Unified CM and endpoint. The Cisco Unified CM implementation of Resource Priority is compliant with DISA Unified Capabilities Requirements, which go beyond the RFC 4412 standards, particularly with regard to the treatment of the namespace. While RFC 4412 gives no special significance to the presence of a dash in the namespace, the UCR reserves the dash for tokenizing a namespace into network domain and precedence domain. The Cisco Unified CM allows the use of the dash in the namespace and determines whether it is simply a part of the namespace or a token delimiter based on whether it is configured as part of the network domain on Cisco Unified CM.

The preemption function of MLPP is handled by the endpoint, not by the Cisco Unified CM. The Cisco Unified CM will override the normal busy trigger when MLPP is enabled to present a precedence call to the endpoint.

Configurable NonPreemptable Numbers

Configurable NonPreemptable numbers affect the preemption behavior of the SIP endpoints. If the feature is enabled at the service parameter level, and the SIP endpoint had more than one call on the phone, then the Cisco Unified Communications Manager will not present the subsequent incoming call to the SIP phone as the phone does not implement NonPreemptable numbers feature. Hence in order to prevent the phone from preempting a NonPreemptable number, Cisco Unified Communications Manager rejects the incoming call to the phone which is higher than the busy trigger. For example, if the busy trigger is 2, then the Cisco Unified Communications Manager will reject the 3rd call.

Outgoing Identity and Incoming CLI for SIP Calls

The Outgoing Identity and Incoming CLI for SIP calls feature provides the ability to enhance the identity selection, presentation and restriction on SIP Interfaces. These capabilities are offered via additional configuration fields you can use for presentation (Identity headers and From headers) on SIP Trunk as well as on SIP profiles for controlling corresponding SIP phones.

There are two sets of identities: network provided identity (trusted) and user provided identity (untrusted). In terms of SIP calls, Identity headers including P-Asserted-Identity (PAI), P-Preferred-Identity (PPI) and Remote-Party-ID (RPID) should carry network proven identity while From header carries user/caller provided identity.

Previously, Cisco Unified CM only provides a single set of identity for outgoing calls. 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, administrators configure 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.

The administrator can also configure another identity on a SIP trunk. You can use this identity, sometimes termed as switchboard, to hide each individual caller's identity. You can configure it 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 you enable such configurations.

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. Switchboard identity will be carried in From header and original caller identity will be carried in Identity headers. You can enable this configuration for each SIP Trunk or SIP device.

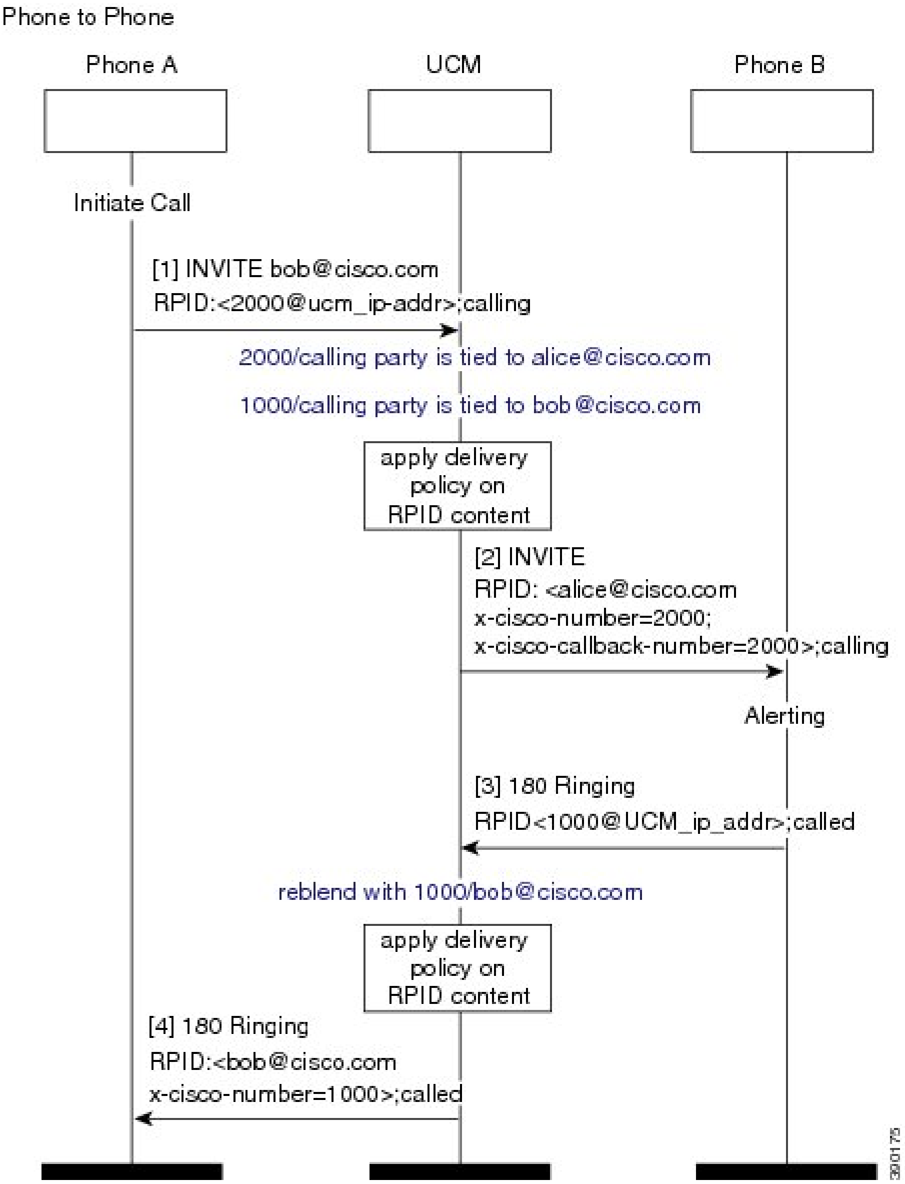
For incoming calls, Cisco Unified CM provides configurations to accept network provided identity carried in Identity headers or user provided identity carried in From header. Cisco Unified CM maintains only a single set of identities per call.

URI Dialing

The URI Dialing feature gives Cisco Unified CM the ability to route an alphanumeric URI, such as bob@cisco.com, and allows the delivery of both URI and DN in indentity headers for endpoints that supports both.

The following use case shows a URI intra-cluster call and presumes that blended delivery is enabled and the phones can consume.

1. Phone A dials bob@cisco.com. UCM discovers blended info, for calling and called parties 1000/bob@cisco.com, 2000/alice@cisco.com
2. UCM extends INVITE to Phone B. Since phone B is configured to consume blended identity info, the RPID contains blended.
3. Phone extends Alerting, RPID from phone is ignored. UCM will re-blend with 1000/bob@cisco.com
4. UCM extends 180 Ringing to phone A. Since phone A is configured to consume blended identity info, the RPID contains blended.


Phone to Phone
Phone A
UCM
Phone B
Initiate Call
[1] INVITE bob@cisco.com
RPID:<2000@ucm_ip-addr>;calling
2000/calling party is tied to alice@cisco.com
1000/calling party is tied to bob@cisco.com
apply delivery policy on RPID content
[2] INVITE
RPID: <alice@cisco.com
x-cisco-number=2000;
x-cisco-callback-number=2000>;calling
Alerting
[3] 180 Ringing
RPID<1000@UCM_ip_addr>;called
reblend with 1000/bob@cisco.com
apply delivery policy on RPID content
[4] 180 Ringing
RPID:<bob@cisco.com
x-cisco-number=1000>;called
390175

Anonymous Call Rejection for a Directory Number

The Anonymous Call Rejection for a Directory Number feature allows the administrator to block anonymous calls for a particular Directory Number. This feature enables the administrator to have a granular control on allowing or disallowing anonymous callers from reaching a particular Directory Number.

If the caller's DN is either not present or caller's DN is private and will not be displayed to the called party - then the call is 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 such as a phone or trunk, Cisco Unified CM rejects the call with SIP response 433 Anonymity Disallowed. The 433 response will also carry a Reason header with Q.850 cause value 21 (call rejected).

The following example shows a SIP 433 response sent to the anonymous caller.

```
SIP/2.0 433 Anonymity Disallowed
Via: SIP/2.0/TLS 172.18.199.91:50486;branch=z9hG4bK3584db90
From: "Connected6005" <sip:6005@10.81.54.224>;tag=f0257279babd003850ae8c99-11653498
To: <sip:*@10.81.54.224>;tag=32638~078d0a52-bf48-420d-b77b-7737bebdf89b-18845479
Date: Mon, 11 Jun 2012 16:39:40 GMT
Call-ID: f0257279-babd0004-0c6a0894-727311e0@172.18.199.91
CSeq: 101 INVITE
Allow-Events: presence
Reason: Q.850; cause=21
Content-Length: 0
```

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

SDP Transparency for Declarative Attributes

This feature allows the administrator to specify declarative SDP attributes that are not natively supported 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 Cisco 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 the Cisco Unified Communications Manager will drop the attribute from the outgoing SDP similar to previous releases of Cisco Unified Communications Manager.

Note that 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 is allowed to identify attributes that will be sent to the egress leg in multiple ways. In addition to passing all unrecognized attributes, he or she has the option to choose 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 configuration is done at the level of the SIP Profile by associating an SDP Transparency Profile specifying which attributes should be passed transparently or picking the pre-configured SDP Transparency Profile named "Pass all unknown SDP attributes" to indicate all unrecognized declarative attributes need to 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 that a reset of all devices using this SIP Profile is needed for any changes to take affect.

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, best effort is made to pass the attribute in these situations.

Cisco Unified Communications Manager Version in User-Agent and Server Headers

This feature adds a new field to the common section of the SIP profile called "Version in User Agent and Server Header". There are 5 possible values and each specifies a portion of the installed build version that will be used as the value of these headers in SIP requests.

Previously, Cisco Unified Communications Manager always used a value representing the major and minor version (for example "Cisco-CUCM9.0") as the User-Agent value in outgoing SIP requests. The Server header was not previously sent in SIP responses, except as part of the feature for passthrough of User-Agent and Server headers.

When the passthrough feature is not in use (for example if the value of the SIP profile parameter "User-Agent and Server header information" is "Send Unified CM Version Information as User-Agent Header"), this feature will populate the User-Agent and Server headers as specified in the following table, given an example build version of "10.0.1.98000-19".

Value specified for SIP profile parameter "Version in User Agent and Server Header"	Example string value in the User-Agent and Server header
Major and Minor	Cisco-CUCM10.0
Major	Cisco-CUCM10
Major, Minor And Revision	Cisco-CUCM10.0.1
Full Build	Cisco-CUCM10.0.1.98000-19
None	Header will be omitted

The value “Major and Minor” matches the current behavior and is the default value.

CTI Video

You can advertise video capabilities of SIP endpoints to CTI applications after successful registration. When the video capability of the endpoints are known, CTI applications can take into account the video capability of the calling and called endpoint during call routing. Cisco Unified Communications Manager will also notify the CTI application with the setup and tear-down of video streams during a call session.

To support this feature, SIP video endpoints are required to report additional feature tags to indicate video capabilities in the SIP REGISTER message. When the endpoint refreshes its registration, it must continue to include these feature tags - to keep these capabilities active in Cisco Unified Communications Manager and CTI application. Absence of these tags in a subsequent registration implies this capability is no longer available.

The following table indicates the fields that endpoints should send in the Contact header of a SIP REGISTER message.

Capability	SIP REGISTER Contact Header Parameter Name	Comment
Video capable	video	**Defined in RFC 3840.** If "video" parameter is present in Contact header, it indicates the device is video capable. Absence of this parameter indicates that the video is not enabled on the device or device is not video capable.
Number of screen	x-cisco-multiple-screen=<n> where <n> is number of screens.	I f this parameter is not present , Cisco Unified Communications Manager will report unknown.
Tele-presence Interoperability	x-cisco-tip	Presence indicates support for Telepresence Interoperability Protocol (TIP). Absence of this tag implies device does not support TIP.

Examples of Contact in SIP REGISTER -

Contact: <sip:1234@10.1.1.1>;…;video	Device is video capable. TIP is not supported. Number of screen is reported as unknown.
Contact: <sip:1234@10.1.1.1>;…;video;x-cisco-multiple-screen=3;x-cisco-tip	Device is video and TIP capable. Device supports three screens.

The system will also monitor the SDP exchange involved in offer-answer with the video endpoints. When a video stream is established, Cisco Unified Communications Manager will inform CTI applications about the stream such as IP address, port, codec, content-type (main/presentation) and maximum bit rate of the video stream. Similarly, when the video stream is broken down, Cisco Unified Communications Manager will indicate that to the CTI application. This will allow CTI applications to monitor the active video streams for a particular call.

iX Channel Support

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

IX support strictly applies to SIP devices. Both SIP Trunk and SIP Line interfaces are fully supported.

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
```

IX is not yet a public standard or draft. It’s currently supported by Cisco devices. Both sides of a call have to support IX for IX to be negotiated and work. Cisco 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 capable Cisco endpoints indicate IX capability during registration, using a new optionsInd tag, <ix>, in the REGISTER message. If UCM is also iX capable, it will add the <ix> tag in optionsInd in the 200OK response message

If IX cannot be negotiated, ex one side doesn’t 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
```

isFocus Support

With the help of new implementation, any line device which is capable of local mixing should send an 'isfocus' parameter in the Contact header so the MOH will be suppressed when one of the participants puts the call on hold during a conference.

Configurable NonPreemptable Numbers

In Release 10.0 the new feature, Configurable NonPreemptable Numbers is introduced which affects the preemption behavior of the SIP endpoints. If the feature is enabled at the service parameter level, and the SIP endpoint had more than one call on the phone, then the Unified Communications Manager does not present the subsequent incoming call to the SIP phone as the phone does not implement NonPreemptable numbers feature. In order to prevent the phone from preempting a NonPreemptable number, Unified Communications Manager rejects the incoming call to the phone which is higher than the busy trigger. For example, if the busy trigger is 2, then Unified Communications Manager rejects the 3rd call.

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 (due to call count threshold) to handle the call request, and if there are insufficient existing calls (and/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), and BPA blocked precedence announcement to be played and/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 and/or call requests to determine whether there are sufficient resources of lesser precedence that can be preempted to accommodate the new precedence call request. This comparison can only occur for calls and call requests having the same value for the precedence-domain subfield in the namespace of the Resource-Priority header field.

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
```

Non-SRTP Call Block

All the SIP endpoints (both line and trunk) should not allow any non-secure call to establish if the service parameter "Block Unencrypted Calls" is set to true. Therefore, for any originating/terminating SIP Line device, if the above service parameter is set to true and the device is non-secure, then the call is blocked and is not allowed to proceed further.

Multiple Codecs in Answer

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 codec.

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, Unified Communications Manager 10.0 release has introduced Multiple Codec in Answer SDP to support 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 common set of codecs in the SIP answer message provided the codec offered by the endpoints does not exceed the inter-region bandwidth policies. This feature only applies to endpoints that indicate the support of Multiple Codec in Answer and they have to be homogenous SIP protocol call. The rest of the call scenarios will remain to be single codec negotiation as Unified Communications Manager does today.

When Unified Communications Manager allows multiple codec to be negotiated, the endpoint can decide which codec to be transmitted and be 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 which codec has been transmitted inside the RTP channels by the call devices

CUCM recognizes the SIP endpoint supporting multiple codecs in answer in several 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 of 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>
- **Multiple Codecs Specified in SIP answer Signals**: When Unified Communications Manager offers an SIP endpoint with SDP and the endpoint respond with multiple codecs in answer signals, Unified Communications Manager will consider the endpoint is capable of negotiating multiple codec in the answer. This applies to both sip trunk and sip line device regardless if they have hinted the support of multiple codec negotiation by any means discussed above. This operation is performed in media layer.

Confidential Access Level

Confidential Access Level (CAL) is a Department of Defence feature. Confidential Access Level controls which calls can be completed and persistently displays information on the phone that conveys additional information about the call.

SIP Phones 9971, 9951 and 8961 support the Confidential Access Level feature.

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

Confidential Access Level has two modes:

- Fixed mode:
  - Emphasizes the CAL level over call completion
  - The calculation is done at each hop: an incoming CAL is resolved against outgoing CAL
  - The resolved CAL must match CAL of whichever party is in Fixed mode, which could be one, or both parties of the call.
- Variable mode:
  - Emphasizes call completion over CAL level

- ◦ The calculation is done at each hop: an 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, the call is allowed to proceed to next hop.

The Enterprise Parameter to enable or disable the Confidential Access Level feature is 'Confidential Access Level (CAL) Enforcement'.

Confidential-Access-Level SIP Header is a new SIP header used to negotiate CAL between AS-SIP enabled Call Agents.

Syntax:

```
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/”/”/”-”)
```

The Enterprise Parameter displays the display-text present in CAL header and Enterprise Parameter does not generate the CAL header in any message.

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:

When an AS-SIP signaling appliance (i.e., 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 respond with a 418 Incompatible CAL.

CAL causes Additional Headers to be included in INVITE messages.Some SIP entities may not support it. So 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 options would do the following:

- Disabled: would not send any CAL headers
- Preferred: would include the CAL header in INVITE message and put the "confidential-access-level" tag in a Supported header
- Required: would include 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.

AES 256 GCM Support for SRTP and TLS

With release 10.5(2), AES 256 Galois/Counter Mode crypto cipher suite support has been added for both SRTP and TLS.

AES 256 GCM Support for SRTP

Cisco Unified Communications Manager now supports the following SRTP crypto cipher suites:

- AEAD_AES_256_GCM (32-byte key)
- AEAD_AES_128_GCM (16-byte key)

When a SIP line advertises one of the two GCM crypto cipher suites, Cisco Unified Communications Manager can negotiate these ciphers based on the cipher preference set by the SIP Line endpoint and the existing cipher negotiation rules. Cisco Unified Communications Manger gives preference to the GCM cipher over a SHA1 cipher, due to higher security, in the event there is a tie.

In addition, a new enterprise parameter, **SRTP Ciphers**, has been added to determine which crypto cipher suites Cisco Unified Communications Manager allows endpoints to use for SRTP. By default, Cisco Unified Communications Manager allows all ciphers, including AES 256 GCM and AES 128 GCM, to be used. However, you can reconfigure the **SRTP Ciphers** enterprise parameter so that Cisco Unified Communications Manager accepts only an AES 128 SHA cipher and rejects attempts to use either the AES 256 GCM or AES 128 GCM cipher.

Following is the sample crypto attribute line that gets appended for each media line in the SDP message:

```
a=crypto:1 AEAD_AES_256_GCM
inline:iZLP7bds308s27xmZZ7fMwycIO2FRhnnk/Br1Q/d1zYNd30YIIF9FkGUn3c=
a=crypto:2 AEAD_AES_128_GCM inline:sExqh5iE+ILVuHiQVTuKoDrHCFVWjdv9EXnMcQ==
```

AES 256 GCM Support for TLS 1.2

Cisco Unified Communications Manager now supports the following TLS 1.2 crypto cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Cisco Unified Communications Manager uses either of the above ciphers to negotiate when a SIP line endpoint handshakes a secure TLS 1.2 connection. If the peer doesn't support TLS1.2 or the GCM ciphers, the connection can fall back to TLS 1.0 with TLS_RSA_WITH_AES_128_CBC_SHA.

In addition, a new enterprise parameter, **TLS Ciphers**, has been added in order to configure whether the AES 256 cipher is preferred or the AES 128 cipher (TLS_RSA_WITH_AES_128_CBC_SHA). By default, the enterprise parameter is set so that Cisco Unified Communications Manager uses the AES 256 cipher if the cipher is supported by the peers. However, you can also set the enterprise parameter so that Cisco Unified Communications Manager uses the AES 128 cipher only.

ECDSA TLS Cipher Support

Cisco Unified Communications Manager supports the following ciphers for SIP connections that use TLS:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

You can configure Cisco Unified Communications Manager to use these ciphers via the **TLS Ciphers** enterprise parameter. The default configuration for this enterprise parameter supports the two new ciphers as well as the following existing ciphers:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_CBC_SHA

Opus Codec Support

Cisco Unified Communications Manager supports the Opus interactive speech and audio codec. Opus can scale from low bitrate narrowband speech at 6 kbt/second, up to high quality stereo music at 510 kbit/s.

Opus is designed to handle a wide range of applications including VoIP, in-game chat, and even live music. The codec is royalty free. The algorithms and source code are openly documented and available.

Opus supports several clock rates. The SDP advertises only the highest clock rate, 48000Hz. The actual clock rate of the corresponding media is signaled inside the payload.

SDP Example 1

```
m=audio 54312 RTP/AVP 100
a=rtpmap:100 opus/48000/2
```

SDP Example 2

```
m=audio 54312 RTP/AVP 99
a=rtpmap:99 opus/48000/2
a=fmtp:99 maxplaybackrate=16000; sprop-maxcapturerate=16000;
maxaveragebitrate=20000; stereo=1; useinbandfec=1; usedtx=0
```

Referred-By Header Support

Cisco Unified Communications Manager transparently passes the Referred-By header, which is present in an incoming REFER message that a SIP endpoint sends, to the outbound initial INVITE (triggered by the REFER).

When a SIP endpoint wants to blind transfer to a different endpoint, the SIP endpoint sends the REFER message to Cisco Unified Communications Manager with the Refer-To header and Referred-By headers populated. If Cisco Unified Communications Manager has to generate a brand new call to the Refer-To target, then Cisco Unified Communications Manager includes the Referred-By header in the outbound initial INVITE to the Refer-To target. If additional redirect features such as call forwarding are configured, the Referred-By header does not get included in any SIP INVITES that are communicated as a result of the supplementary feature.

If the Refer-To destination endpoint does not understand the Referred-By header, it can respond with a 429 Provide Referrer Identity response. Cisco Unified Communications Manager passes this error response back to endpoint that initiated the REFER, and clears the call.

Session ID Header Support

Cisco Unified Communications Manager supports passing the SIP Session-ID headers through to all call legs. When Cisco Unified Communications Manager receives an inbound SIP INVITE message from a SIP endpoint, and the Session ID header is included, Cisco Unified Communications Manager passes the header through to the other call leg and includes it in the outbound INVITE dialog message that gets sent to the other endpoint.

If the SIP endpoint does not provide the Session-ID header, Cisco Unified Communications Manager generates the header on behalf of the endpoint after the first inbound SIP message that is received.

iX Channel Encryption

Encryption support with DTLS is now added to the iX Channel for application media. This update ensures privacy for information transmitted using iX Channel. When iX Channel encryption is used in video conferences, this update ensures that the privacy of transmitted information, such as the identities of meeting participants is protected.

There are two types of SDP offers for iX Channel encryption:

- Best Effort Encryption—The SDP offer is for an encrypted iX Channel, but will fall back to a non-encrypted iX Channel if the SIP peers do not support it. This approach may be used if encryption is not mandatory in the solution. For example, encryption is usually mandatory within the cloud, but not within a single enterprise.
- Forced Encryption—The SDP offer is for an encrypted iX Channcel only. This offer will be rejected if the SIP peers do not support iX Channel encryption. This approach may be used in deployments where encryption is mandatory between endpoints.

SDP Body for Encrypted iX Channel

For Best Effort offers, the SDP portion looks like:

```
m=application 12345 UDP/UDT/IX *
b=as:64
a=ixmap:1 XCCP
a=ixmap:2 MSCP
a=connection:new
a=setup:actpass
a=fingerprint: SHA-1 4A:AD:BA:XX:W7:82:18:3B:54:92:12:SA:3E:5D:99:6B:19:E5:75:R9
```

For Forced Encryption offers, the SDP portion looks like:

```
m=application 12345 UDP/DTLS/UDT/IX *
b=as:64
a=ixmap:1 XCCP
a=ixmap:2 MSCP
a=connection:new
a=setup:actpass
a=fingerprint: SHA-1 4A:AD:BA:XX:W7:82:18:3B:54:92:12:SA:3E:5D:99:6B:19:E5:75:R9
```

For Best Effort encryption, the m line transport protocol is UDP/UDT/IX. For forced encryption, the m line transport protocol is UDP/DTLS/UDT/IX.

The setup attribute indicates which endpoint should initiate the DTLS/UDT connection. If the fingerprint attribute is present, the setup attribute must also be present at either the m line level or session level.

The fingerprint attribute is the user's DTLS authorization certificate and must be present at the m line level or session level. For forced encryption, the fingerprint is mandatory.

X-ULPFECUC Codec Support for Audio

X-ULPFECUC is a Forward Error Correction (FEC) codec based on Reed Solomon error correction or similar algorithms. X_ULPFECUC works by creating K additional packets based on encoded input data for every N media packets which enables the receiving entity to recover (N-K) errored packets. This ensures media stream resiliency and can help deliver higher audio quality.

Although the recommended payload type for FEC Codec is 123, it can negotiate using other dynamic payload types. Clock rate is transparently passed from one leg to other, along with FMTP parameters.

As FEC Codec is a non-primary codec, an SDP containing only FEC Codec (or FEC + any non primary codecs like RFC2833) in audio mLine is rejected with a 488 message.

The SDP offer looks like:

```
m=audio 47352 RTP/AVP 114 18 123 18 101
a=sendrecv
a=rtpmap:114 opus/48000/2
a=rtpmap:123 X-ULPFECUC/8000
a=fmtp:123 multi_ssrc=0;max_esel=20;m=2;max_n=20
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```