



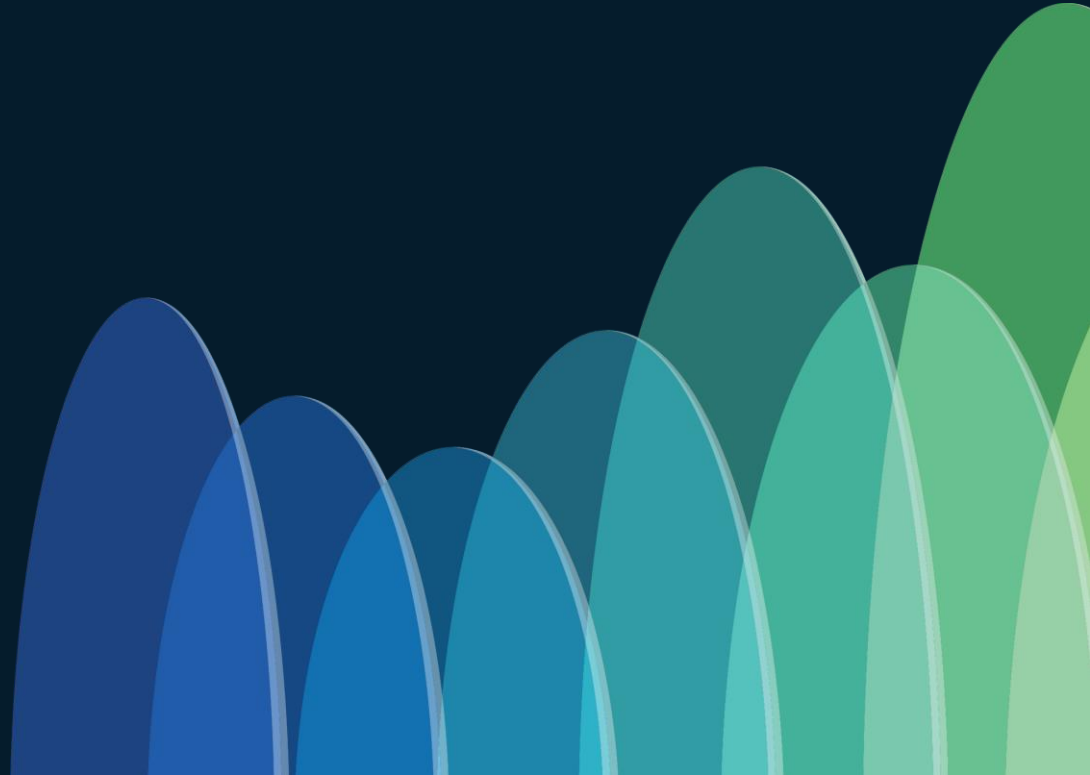
Troubleshooting the Session Initiation Protocol (SIP)

Paul Giralt - Distinguished Engineer
pgiralt@cisco.com
BRKCOL-2143

Agenda

- Session Initiation Protocol (SIP) Overview
 - User Agents
 - Requests and Responses
 - Headers
 - Session Description Protocol
 - Offer / Answer Model
 - DTMF Relay
 - SIP Session ID
 - ICE Overview
- Troubleshooting Tools
- Troubleshooting Methodology & Case Studies
- Additional Resources

SIP Protocol Overview



What is SIP?

- Signaling protocol used to establish, manage, and terminate sessions over an IP network
- Core protocol defined in RFC 3261
- Relies heavily on RFC 3262, RFC 3263, RFC 3264, and RFC 3265
- Extended in many, many other RFCs
- ASCII-based messages

User Agents

- **User Agent Clients** (UAC) send **requests** to **User Agent Servers** (UAS)
- **User Agent Servers** send **responses** to the **requests**
- Nearly all SIP devices are **both a UAC and a UAS** (they both initiate and accept requests)
- Call Control devices can be a Proxy, a Back-to-Back User Agent (B2BUA), or sometimes both



SIP Request Methods defined in RFC 3261

- **INVITE** – A user or service is being invited to participate in a multimedia session (e.g., set up a new call)
- **ACK** – Confirms that a client has received a final response to an INVITE request
- **BYE** – Terminates an existing session
- **CANCEL** – Cancels pending requests; does not terminate sessions that have been accepted
- **OPTIONS** – Queries the capabilities of servers (Also used as a keepalive)
- **REGISTER** – Registers the user agent with the registrar server of a domain

Additional SIP Request Methods

- **PRACK** (RFC 3262) – to acknowledge a provisional response
- **SUBSCRIBE** (RFC 3265) – to tell a remote node to look for a certain event
- **NOTIFY** (RFC 3265) – to respond when that certain event occurs
- **UPDATE** (RFC 3311) – to update parameters of a session set-up
- **REFER** (RFC 3515) – to “refer” one UA to communicate with another UA
- **INFO** (RFC 2976) – to send more information within an established dialog
- **PUBLISH** (RFC 3903) – to push UA state information to a compositor/presence server

SIP INVITE Method

INVITE sip:918008001180@12013670.us10.bcld.webex.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.107:62580;branch=z9hG4bK86686aef70059660;alias;rport
Max-Forwards: 70
To: sip:918008001180@12013670.us10.bcld.webex.com
From: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bcld.webex.com;tag=660dba695714ad08e
CSeq: 2121402554 INVITE
Call-ID: d16f2f19634f0e84532da13c4ed4f741
Contact: <sip:c4628b59bp_GDWYMXEZAXNN_1@192.168.1.107:8933;transport=tls>
accept: application/sdp
accept-contact: *
allow-events: hold, talk, mute, unmute
p-preferred-identity: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bcld.webex.com
recv-info: x-broadworks-client-session-info
session-id: 0f4c9bcc0120500080005cf6dad3c2e0;remote=00000000000000000000000000000000
User-Agent: bc-uc teams (sparkmac/45.3.0.31637 (15.3.0) (en-US) (Native Desktop) (Purple))
Supported: timer, replaces, 100rel
Session-Expires: 3600;refresher=uac
Allow: INVITE, BYE, ACK, PRACK, CANCEL, OPTIONS, NOTIFY, INFO, UPDATE
Content-Type: application/sdp
Content-Length: 1394

SIP INVITE Method

INVITE sip:918008001180@12013670.us10.bclid.webex.com SIP/2.0

Via: SIP/2.0/TLS 192.168.1.107:62580;branch=z9hG4bK86686aef70059660;alias;rport

Max-Forwards: 70

To: sip:918008001180@12013670.us10.bclid.webex.com

From: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bclid.webex.com;tag=660dba695714ad08e

CSeq: 2121402554 INVITE

Call-ID: 632da13c4ed4f741

Contact: GDWYMXEZAXNN_1@192.168.1.107:8933;transport=tls>

accept: application/sdp

accept-contact: *

allow-events: hold, talk, mute, unmute

p-preferred-identity: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bclid.webex.com

recv-info: x-broadworks-client-session-info

session-id: 0f4c9bcc0120500080005cf6dad3c2e0;remote=00000000000000000000000000000000

User-Agent: bc-uc teams (sparkmac/45.3.0.31637 (15.3.0) (en-US) (Native Desktop) (Purple))

Supported: timer, replaces, 100rel

Session-Expires: 3600;refresher=uac

Allow: INVITE, BYE, ACK, PRACK, CANCEL, OPTIONS, NOTIFY, INFO, UPDATE

Content-Type: application/sdp

Content-Length: 1394

Request URI

SIP Version

SIP Method

SIP Headers

INVITE sip:918008001180@12013670.us10.bclld.webex.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.107:62580;branch=z9hG4bK86686aef70059660;alias;rport
Max-Forwards: 70
To: sip:918008001180@12013670.us10.bclld.webex.com
From: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bclld.webex.com;tag=660dba695714ad08e
CSeq: 2121402554 INVITE
Call-ID: d16f2f19634f0e84532da13c4ed4f741
Contact: <sip:c4628b59bp_GDWYMXEZAXNN_1@192.168.1.107:8933;transport=tls>
accept: application/sdp
accept-contact: *
allow-events: hold, talk, mute, unmute
p-preferred-identity: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bclld.webex.com
recv-info: x-broadworks-client-session-info
session-id: 0f4c9bcc0120500080005cf6dad3c2e0;remote=00000000000000000000000000000000
User-Agent: bc-uc teams (sparkmac/45.3.0.31637 (15.3.0) (en-US) (Native Desktop) (Purple))
Supported: timer, replaces, 100rel
Session-Expires: 3600;refresher=uac
Allow: INVITE, BYE, ACK, PRACK, CANCEL, OPTIONS, NOTIFY, INFO, UPDATE
Content-Type: application/sdp
Content-Length: 1394

SIP Mandatory Headers – RFC 3261 Section 20

- Where column:
 - R: header field may only appear in requests;
 - r: header field may only appear in responses;
 - 2xx, 4xx, etc.: A numerical value or range indicates response codes with which the header field can be used;
 - c: header field is copied from the request to the response.
- Requirements:
 - c: Conditional; requirements on the header field depend on the context of the message.
 - m: The header field is mandatory.
 - m*: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field.
 - o: The header field is optional.
 - t: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field. If a stream-based protocol (such as TCP) is used as a transport, then the header field MUST be sent.
 - *: The header field is required if the message body is not empty. See Sections [20.14](#), [20.15](#) and [7.4](#) for details.

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Accept	R		-	o	-	o	m*	o
Accept	2xx		-	-	-	o	m*	o
Accept	415		-	c	-	c	c	c
Accept-Encoding	R		-	o	-	o	o	o
Accept-Encoding	2xx		-	-	-	o	m*	o
Accept-Encoding	415		-	c	-	c	c	c
Accept-Language	R		-	o	-	o	o	o
Accept-Language	2xx		-	-	-	o	m*	o
Accept-Language	415		-	c	-	c	c	c
Alert-Info	R	ar	-	-	-	o	-	-
Alert-Info	180	ar	-	-	-	o	-	-
Allow	R		-	o	-	o	o	o
Allow	2xx		-	o	-	m*	m*	o
Allow	r		-	o	-	o	o	o
Allow	405		-	m	-	m	m	m
Authentication-Info	2xx		-	o	-	o	o	o
Authorization	R		o	o	o	o	o	o
Call-ID	c	r	m	m	m	m	m	m
Call-Info		ar	-	-	-	o	o	o
Contact	R		o	-	-	m	o	o
Contact	1xx		-	-	-	o	-	-
Contact	2xx		-	-	-	m	o	o
Contact	3xx	d	-	o	-	o	o	o
Contact	485		-	o	-	o	o	o
Content-Disposition			o	o	-	o	o	o
Content-Encoding			o	o	-	o	o	o
Content-Language			o	o	-	o	o	o
Content-Length		ar	t	t	t	t	t	t
Content-Type			*	*	-	*	*	*
CSeq	c	r	m	m	m	m	m	m

SIP Response

SIP/2.0 200 OK

Free-text Reason

Response Code

Via: SIP/2.0/TLS 192.168.1.107:62580; branch=z9hG4bK3b6fa283d026c87f;alias;rport
Max-Forwards: 70
To: sip:918008001180@10.21.0.192.us10.bclld.webex.com;tag=994605466-1738354282585
From: sip:c462e2axnn_1@12013670.us10.bclld.webex.com;tag=660dba695...
CSeq: 2121402555 INVITE
Call-ID: d16f2f19634f0e84532da13c4ed4f741
Contact: <sip:23.89.40.102:8934;transport=tls>
accept: application/media_control+xml,application/sdp
call-info: <sip:10.21.0.192>;appearance-index=1
content-disposition: session;handling=required
recv-info: x-cisco-mute-status,x-broadworks-client-session-info
session-id: 0b0ad62f609f590d801ad0948a1a88d3;remote=0f4c9bcc0120500080005cf6dad3c2e0
x-broadworks-correlation-info: 720a4e4e-0e4e-4d80-9299-bcf8a362c914
Privacy: none
P-Asserted-Identity: <sip:+18008001180@10.21.0.192;user=phone>
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Content-Type: application/sdp
Content-Length: 629

SIP Response

SIP/2.0 200 OK

Via: SIP/2.0/TLS 192.168.1.107:62580; branch=z9hG4bK3b6fa283d026c87f;alias;rport

Max-Forwards: 70

To: sip:918008001180@12013670.us10.bcld.webex.com;tag=994605466-1738354282585

From: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bcld.webex.com;tag=660dba695...

CSeq: 2121402555 INVITE

Call-ID: d16f2f19634f0e84532da13c4ed4f741

Contact: <sip:23.89.40.102:8934;transport=tls>

accept: application/media_control+xml,application/sdp

call-info: <sip:10.21.0.192>;appearance-index=1

content-disposition: session;handling=required

recv-info: x-cisco-mute-status,x-broadworks-client-session-info

session-id: 0b0ad62f609f590d801ad0948a1a88d3;remote=0f4c9bcc0120500080005cf6dad3c2e0

x-broadworks-correlation-info: 720a4e4e-0e4e-4d80-9299-bcf8a362c914

Privacy: none

P-Asserted-Identity: <sip:+18008001180@10.21.0.192;user=phone>

Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE

Content-Type: application/sdp

Content-Length: 629

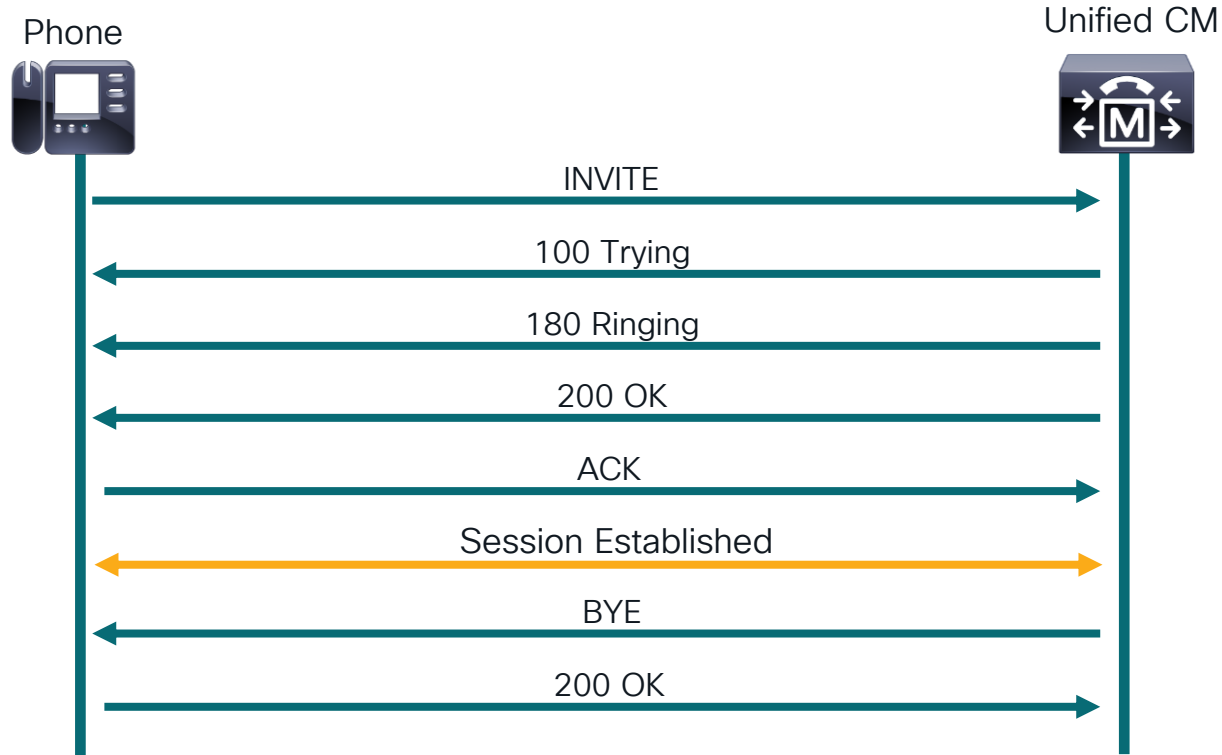
SIP Responses

Response Code	Description	Example
1XX	Informational – Request Received and Continuing to Process Request	100 Trying 180 Ringing 183 Session Progress
2XX	Success – Action was successfully received, understood, and accepted	200 OK 202 Acceptable
3XX	Redirection – Another SIP Element needs to be contacted to complete the request	300 Multiple Choices 302 Moved Temporarily
4XX	Client Error – The server cannot fulfill the request based on the information contained in the request. Could indicate malformed data or a request the server cannot process based on the data in the request.	401 Unauthorized 404 Not Found 406 Not Acceptable 486 Busy Here 488 Not Acceptable Here
5XX	Server Error – Server failed to fulfill an apparently valid request	500 Internal Server Error 503 Service Unavailable
6XX	Global Failure – Request is invalid at any server. Usually like 4XX errors but indicate no server can process the request.	600 Busy Everywhere 603 Decline 604 Does Not Exist Anywhere

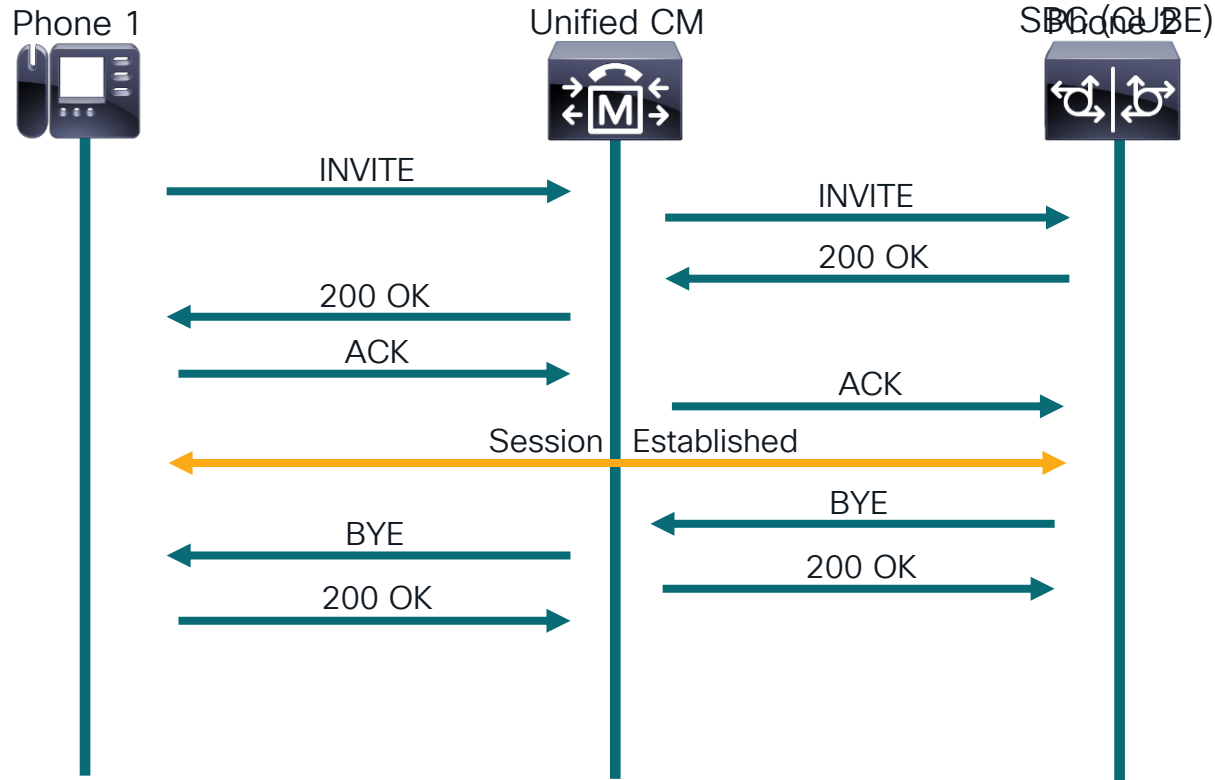
SIP Transactions and Dialogs

- **Transactions:** A request and any related responses to that request. Ensures reliable transmission of a request
- **Dialog:** All transactions related to a session
 - INVITE starts a dialog and BYE or CANCEL ends it
 - SUBSCRIBE can start a dialog and all NOTIFY are part of the dialog
 - Uniquely identified by Call-ID + To tag + From tag
- Not all Transactions are part of a Dialog (e.g., REGISTER, OPTIONS, out-of-dialog REFER)

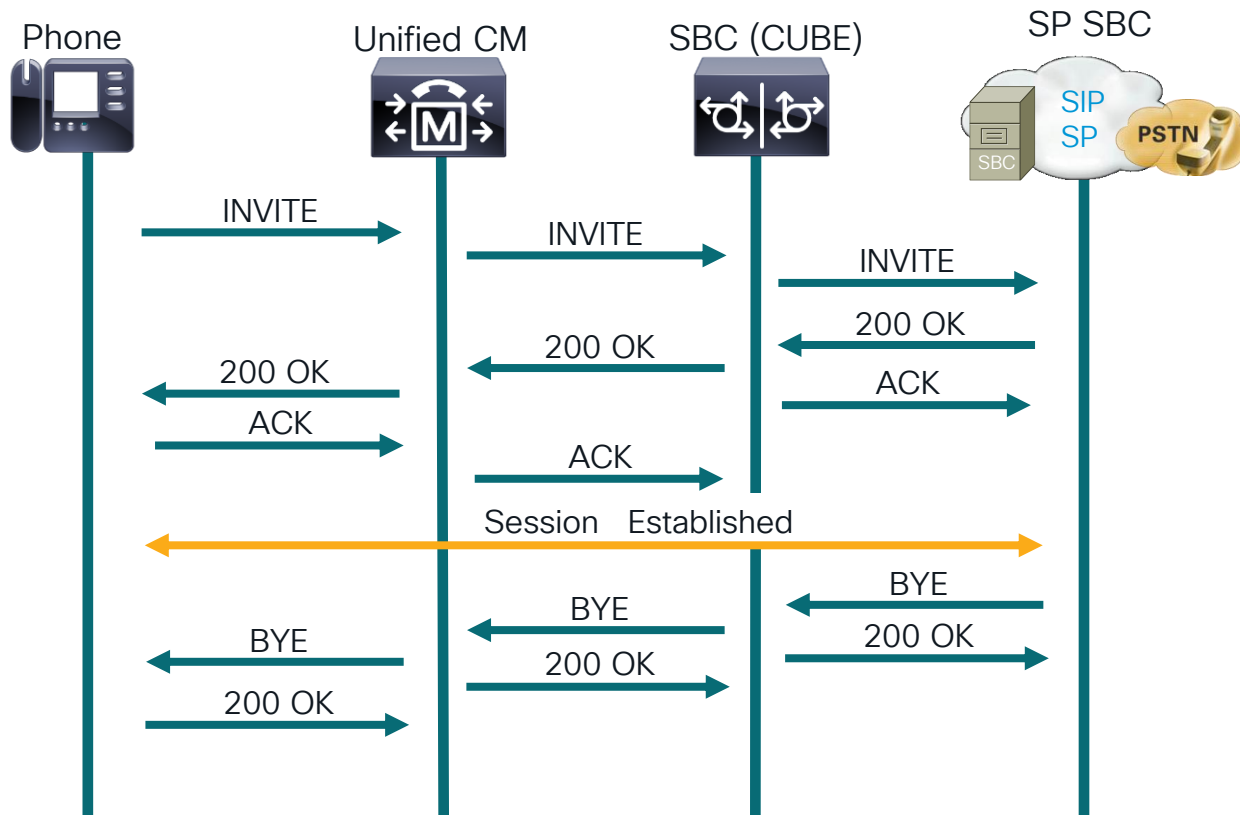
Basic SIP Call Setup



Basic SIP Call Setup with B2BUA (Unified CM)



Basic SIP Call Setup with Unified CM and CUBE



Media Negotiation

- SIP leverages the Session Description Protocol (SDP) (RFC 4566/3266/2327) to communicate media information.
- SIP uses the offer/answer model described in RFC 3264 to negotiate media using SDP

```
v=0
o=xmserver 3782060655 3782060656 IN IP4 172.31.175.196
s=xmserver
c=IN IP4 172.31.175.196
b=AS:80
t=0 0
m=audio 19436 RTP/AVP 0 101
b=AS:80
a=sendrecv
a=rtcp-mux
a=ssrc:3806853901 cname:77YAVdIFx9N7
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```



```
v=0
o=CiscoSystemsSIP-GW-UserAgent 636 1650 IN IP4 10.81.225.210
s=SIP Call
c=IN IP4 10.81.225.210
t=0 0
m=audio 24106 RTP/AVP 0 101
c=IN IP4 10.81.225.210
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
```

Offer/Answer Model (RFC 3264)

- One endpoint sends an offer SDP containing all the capabilities the endpoint wishes to negotiate.
- SDP contains m lines for each media stream being negotiated (i.e. audio, video, content channel, etc...)
- Receiving endpoint sends an answer SDP that contains the same or a subset of capabilities received in the offer.
- Per RFC 3264, “For each "m=" line in the offer, there MUST be a corresponding "m=" line in the answer. The answer MUST contain exactly the same number of "m=" lines as the offer.”

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```

Session Description Protocol (SDP) – Offer

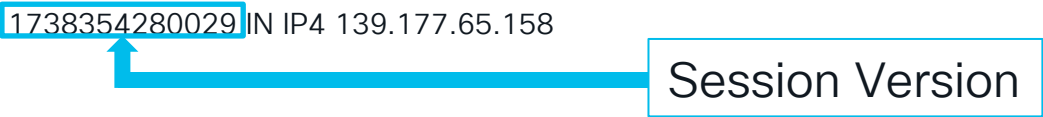
```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpqMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.218 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.218 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 305944921738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```



Session Version

Session Description Protocol (SDP) – Offer

v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158

c=IN IP4 139.177.65.158

Connection Data

t=0 0

a=cisco-mari:v1

a=cisco-mari-rate

a=cisco-mari-rtx:v0

a=cisco-mari-hybrid-resilience:v0

m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112

a=sendrecv

a=rtpmap:99 opus/48000/2

a=rtpmap:105 xcodec/48000

a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1

a=rtpmap:9 G722/8000

a=rtpmap:0 PCMU/8000

a=rtpmap:8 PCMA/8000

a=rtpmap:18 G729/8000

a=fmtp:18 annexb=no

a=rtpmap:102 iLBC/8000

a=fmtp:102 mode=30

a=rtpmap:101 telephone-event/8000

a=rtpmap:111 x-ulpfecuc/8000

a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0

a=rtpmap:112 mari-rtx/90000

a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180

Session Description Protocol (SDP) – Offer

v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0

a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0

Media Adaptation and Resilience

m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_src=1;FEC_ORDER=FEC_SRTTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTTP;rtx-time=180

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```



Audio m-line

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:0 PCMA/8000
a=rtpmap:0 PCMA/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```

Audio m-line

UDP Port

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcode/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
```

Audio m-line

Transport Protocol: AVP=RTP, SAVP=SRTP

```
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_src=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-version=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_src=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```

Audio m-line

RTP Payload Types / Codecs

Session Description Protocol (SDP) – Offer

```
v=0
o=BroadWorks 30594492 1738354280029 IN IP4 139.177.65.158
c=IN IP4 139.177.65.158
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 30024 RTP/SAVP 99 105 9 0 8 18 102 101 111 112
```

Media Attributes



```
a=sendrecv
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:102 iLBC/8000
a=fmtp:102 mode=30
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
```

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

RTP Header
Extensions

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

RTP Control Protocol
Extended Reports (RFC 3611)

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com
a=extmap:9/sendrecv http://www.webrtc.org
a=rtcp-xr:rcvr-rtt=all voip-metrics
```

Interactive Connectivity Establishment (ICE)

```
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com
a=extmap:9/sendrecv http://www.webrtc.org
a=rtcp-xr:rcvr-rtt=all voip-metrics
```

Interactive Connectivity Establishment (ICE)

```
a=ice-ufrag:Xo3F
a=ice-pwd:8gUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1671727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1671727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:5 158 30024 typ relay
a=candidate:5 158 30025 typ relay
```

Username / Password

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com
a=extmap:9/sendrecv http://www.webrtc.org
a=rtcp-xr:rcvr-rtt=all voip-metrics
```

Interactive Connectivity Establishment (ICE)

```
a=ice-ufrag:Xo3F
a=ice-pwd:8gUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
```

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
```

```
a=sendrecv
```

```
a=rtpmap:109 H264/90000
```

```
a=fmtp:109 profile-level-id=ICE Candidates=0
```

```
a=rtcp-fb:109 ccm fir
```

```
a=rtcp-fb:109 nack pli
```

```
a=rtcp-fb:109 nack
```

```
a=ice-ufrag:f1mh
```

```
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
```

```
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
```

```
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```



Encryption Key

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AFS_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

Video m-line

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```



Bandwidth

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```



Direction Attribute

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtptime:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

H.264 Attributes

Session Description Protocol (SDP) – Offer

a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packetization-mode=0
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host

RTCP Feedback (RFC 4585)

Session Description Protocol (SDP) – Offer

```
a=extmap:4/sendrecv http://protocols.cisco.com/timestamp#100us
a=extmap:9/sendrecv http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=ice-ufrag:Xo3F
a=ice-pwd:8qUtOBXZvcs43hpgMc0dkPtCVQpnZA57
a=candidate:1 1 UDP 2113935615 192.168.1.107 8560 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8561 typ host
a=candidate:3 1 UDP 1677727999 136.56.9.219 8560 typ srflx raddr 192.168.1.107 rport 8560
a=candidate:3 2 UDP 1677727998 136.56.9.219 25567 typ srflx raddr 192.168.1.107 rport 8561
a=candidate:mse 1 UDP 16777215 139.177.65.158 30024 typ relay
a=candidate:mse 2 UDP 16777214 139.177.65.158 30025 typ relay
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
m=video 8600 RTP/SAVP 109 111 112
b=AS:2500
a=sendrecv
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f; packet
a=rtcp-fb:109 ccm fir
a=rtcp-fb:109 nack pli
a=rtcp-fb:109 nack
a=ice-ufrag:f1mh
a=ice-pwd:urqVaa2MTz5gKx0W0rk+Xad8X/nq41Qp
a=candidate:1 1 UDP 2113935615 192.168.1.107 8600 typ host
a=candidate:1 2 UDP 2113935614 192.168.1.107 8601 typ host
```

Interactive Connectivity Establishment (ICE)



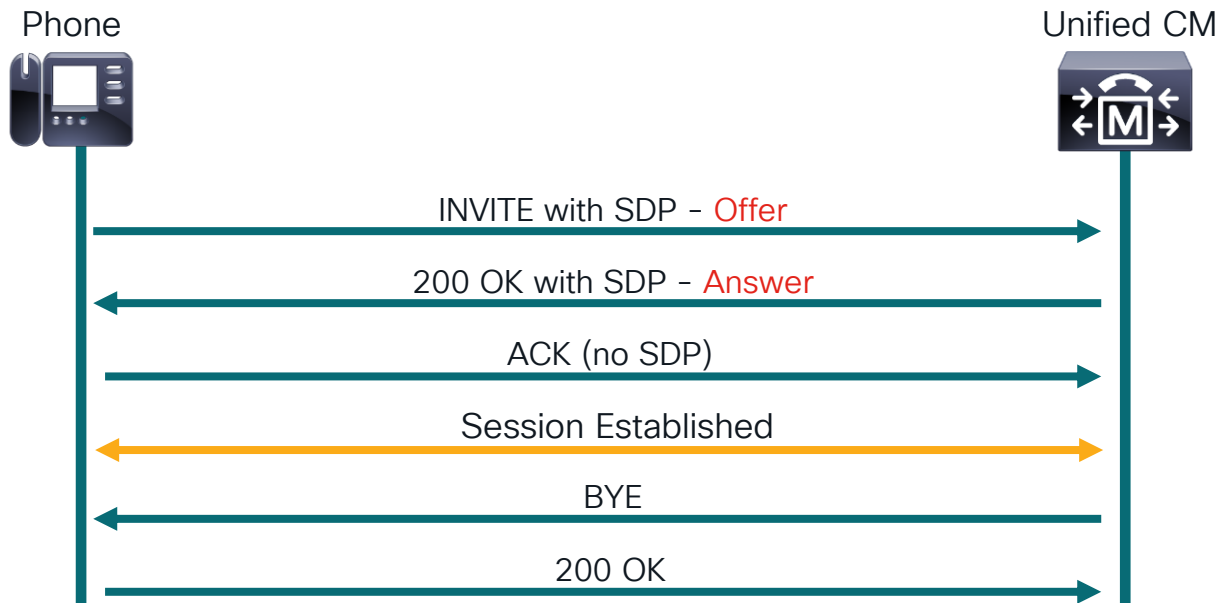
Session Description Protocol (SDP) – Answer

```
v=0
o=Broadworks 30594835 1738354282717 IN IP4 23.89.40.99
s=-
c=IN IP4 23.89.40.99
t=0 0
a=ice-lite
m=audio 28870 RTP/SAVP 0 101
c=IN IP4 23.89.40.99
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=candidate:1 1 UDP 2130706431 64.102.250.134 11550 typ host
a=candidate:1 2 UDP 2130706430 64.102.250.134 11551 typ host
a=ice-ufrag:QxSQ
a=ice-pwd:weO9wS0bmQ6N36wqAgmnhH
a=crypto:*****dKDj
a=candidate:mse 1 UDP 16777215 23.89.40.99 28870 typ relay
a=candidate:mse 2 UDP 16777214 23.89.40.99 28871 typ relay
m=video 0 RTP/SAVP 109
```

Media Negotiation – Early Offer and Delayed Offer

- Initiator of the call can send SDP offer in the INVITE – this is called an Early Offer (EO)
- Receiving endpoint can send the SDP offer in a response if the INVITE did not contain an offer – this is called a Delayed Offer (DO)
- For Early Offer, the answer is sent in a response (usually 200 OK).
- For Delayed Offer, the answer is typically sent in the ACK.

Early Offer



Delayed Offer



Early Media

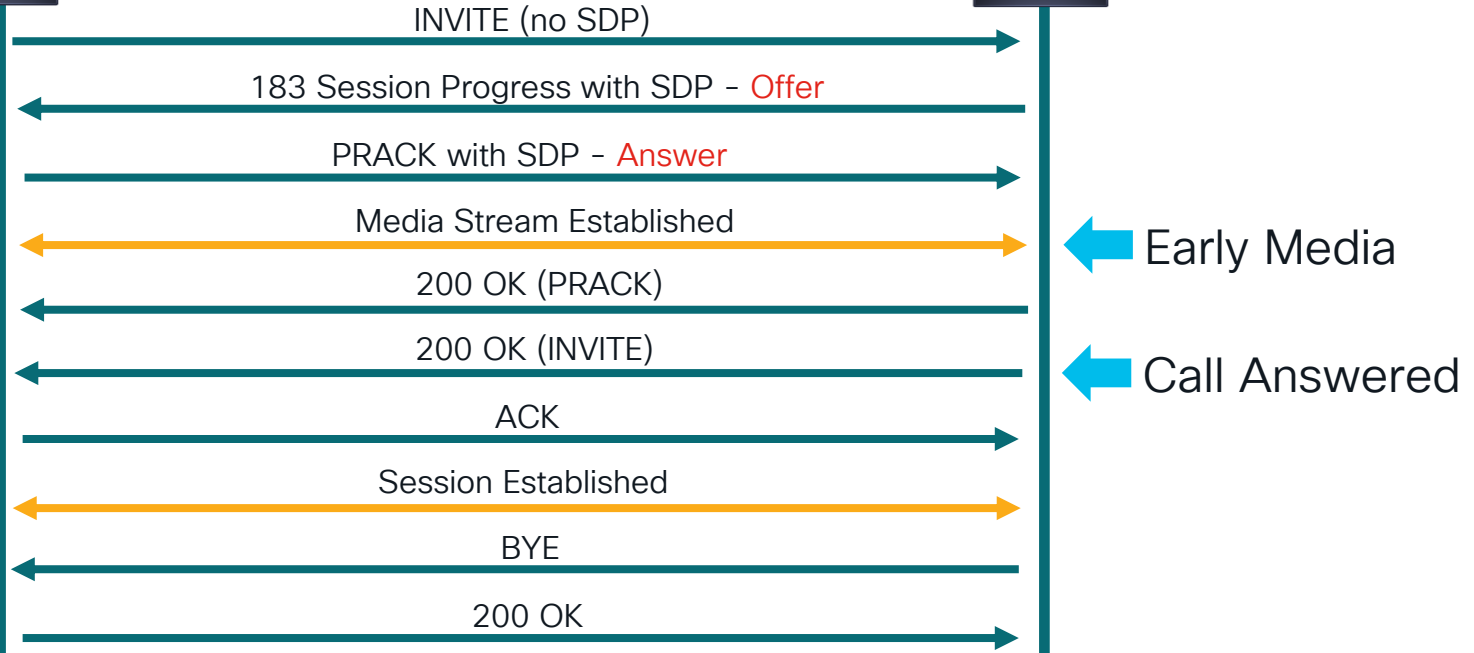
- Delayed Offer calls do not set up media until the 200 OK (call is answered)
- If media is required prior to the call being connected, SIP has provisions for Early Media
- With Early Media on a Delayed Offer call, the offer comes from the terminating side in a provisional response (e.g. 183 Session Progress)
- Originating side sends SDP Answer in a PRACK message (defined in RFC 3262)

Early Media

Unified CM



CUBE

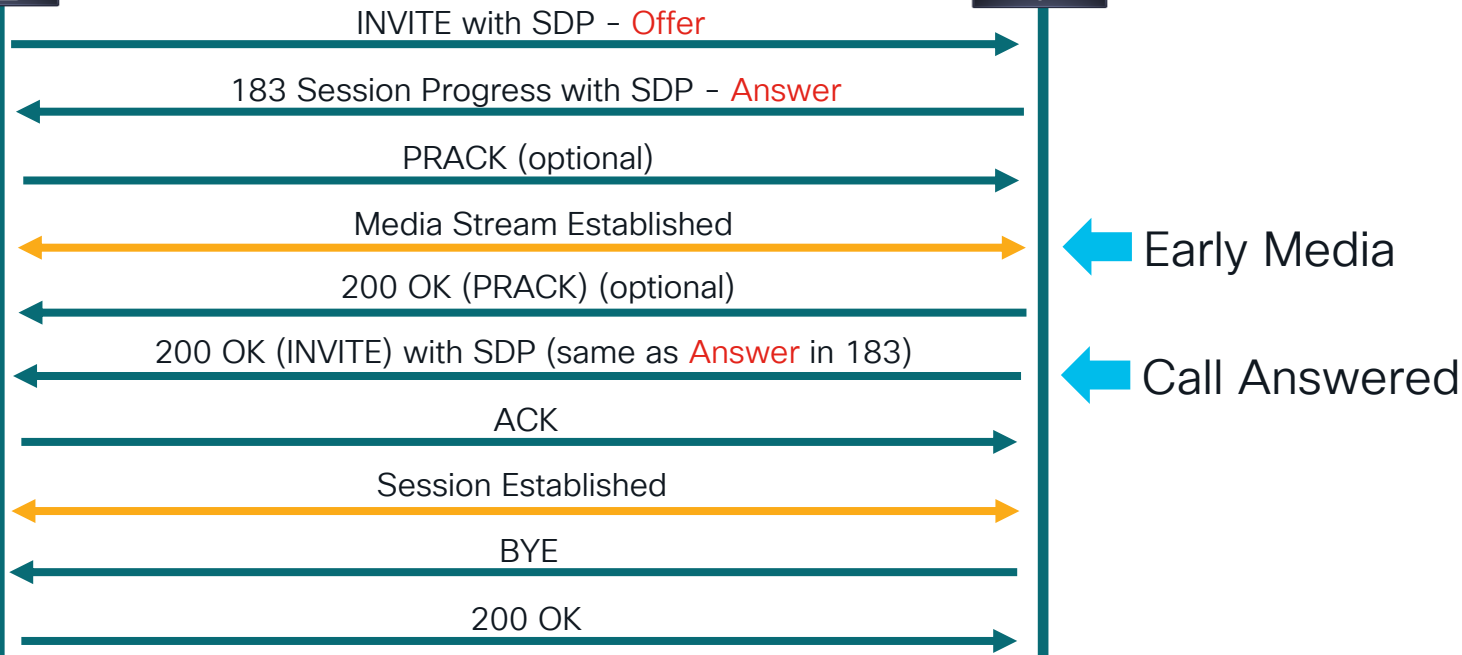


Early Media w/ Early Offer

Unified CM



CUBE



Media Re-negotiation

Re-INVITE

- Either UA involved in a call can re-INVITE an existing dialog to re-negotiate parameters for the call.
- Cannot re-INVITE until any previous INVITE messages have received a final response.
- UPDATE method can also be used to re-negotiate prior to a final response.

Media Re-negotiation

Re-INVITE w/ sendonly directly

Presence of “tag” in “To” header indicates re-INVITE



```
INVITE sip:23.89.40.102:8934;transport=tls SIP/2.0
Via: SIP/2.0/TLS 192.168.1.107:56281;branch=z9hG4bK955ab044eb0373d4;alias;rport
Max-Forwards: 70
To: sip:+18008001180@12013670.us10.bcld.webex.com;tag=1185912546-1738465877213
From: sip:c4628b59bp_GDWYMXEZAXNN_1@12013670.us10.bcld.webex.com;tag=b13de0ff609ca8acd6a451fc9353ef7d
CSeq: 1770842046 INVITE
Call-ID: 58e5733eab46f997f01185e5f3662785
Contact: <sip:c4628b59bp_GDWYMXEZAXNN_1@192.168.1.107:8933;transport=tls>
allow-events: hold, talk, mute, unmute
authorization: *****
recv-info: x-broadworks-client-session-info
session-id: ce9bff85012050008000ac5e0b4f6183;remote=168cd19500cd5eed887cb044ce573c81
User-Agent: bc-uc teams (sparkmac/45.3.0.31637 (15.3.0) (en-US) (Native Desktop) (Purple))
Supported: timer, replaces, 100rel
Content-Type: application/sdp
Session-Expires: 3600;refresher=uac
Allow: INVITE, BYE, ACK, PRACK, CANCEL, OPTIONS, NOTIFY, INFO, UPDATE
Content-Length: 1466
```

Media Re-negotiation

Re-INVITE w/ sendonly directly

```
v=0
s=-
c=IN IP4 136.56.9.218
t=0 0
a=cisco-mari:v1
a=cisco-mari-rate
a=cisco-mari-rtx:v0
a=cisco-mari-hybrid-resilience:v0
m=audio 34039 RTP/SAVP 111 112 99 105 9 0 8 18 102 101
a=rtpmap:111 x-ulpfecuc/8000
a=fmtp:111 max_esel=1400;max_n=255;m=8;multi_ssrc=1;FEC_ORDER=FEC_SRTP;non_seq=1;feedback=0
a=rtpmap:112 mari-rtx/90000
a=fmtp:112 RTX_ORDER=RTX_SRTP;rtx-time=180
a=rtcp-xr:rcvr-rtt=all voip-metrics
a=sendonly
a=rtpmap:99 opus/48000/2
a=rtpmap:105 xcodec/48000
a=fmtp:105 performance=HP;encode-versions=1;decode-versions=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
```

Media Re-negotiation

Re-INVITE - stop media then re-negotiate

INVITE sip:db40e44-0dfe-45f1-bd7f-e652098ca344@10.116.101.41:49833;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.106.59:5061;branch=z9hG4bK901f9c72c19221
From: "Paul Giralt" <sip:89915644@172.18.106.59>;tag=15462272~0d0d25d7-4931-4a07-83c6-b82e2c213ca7-45545776
To: <sip:89915644@172.18.106.59>;tag=0022bdd6843100702aae8e5b-4be253be
Date: Wed, 11 Jan 2025 03:08:51 GMT
Call-ID: 8c045780-f0c1fd34-8d838f-3b6a12ac@172.18.106.59
Supported: timer,resource-priority,replaces
Min-SE: 1800
User-Agent: Cisco-CUCM15.0
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
CSeq: 104 INVITE
Max-Forwards: 70
Expires: 180
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Authenticated; orientation= from; gci= 2-231448; call-instance= 2
Remote-Party-ID: "Paul Giralt" <sip:89915644@172.18.106.59>;party=calling;screen=yes;privacy=off
Contact: <sip:89915644@172.18.106.59:5061;transport=tls>
Content-Type: application/sdp
Content-Length: 489

Media Re-negotiation

Re-INVITE - stop media then re-negotiate

```
v=0
o=CiscoSystemsCCM-SIP 15462272 2 IN IP4 172.18.106.59
s=SIP Call
c=IN IP4 0.0.0.0
t=0 0
m=audio 19594 RTP/SAVP 9 101
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=inactive
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
m=video 19444 RTP/AVP 126
b=TIAS:1000000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801E;packetization-mode=1;level-asymmetry-allowed=1
a=inactive
a=mid:227796888
```

Media Re-negotiation

Re-INVITE – Delayed Offer to Re-establish Media Stream

INVITE sip:db40e44-0dfe-45f1-bd7f-e652098ca344@10.116.101.41:49833;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.106.59:5061;branch=z9hG4bK901fac34c0fb1b
From: "Paul Giral" <sip:89915644@172.18.106.59>;tag=15462272~0d0d25d7-4931-4a07-83c6-b82e2c213ca7-45545776
To: <sip:89915644@172.18.106.59>;**tag=0022bdd6843100702aae8e5b-4be253be**
Date: Wed, 11 Jan 2025 03:08:52 GMT
Call-ID: 8c045780-f0c1fd34-8d838f-3b6a12ac@172.18.106.59
Supported: timer,resource-priority,replaces
Min-SE: 1800
User-Agent: Cisco-CUCM15.0
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
CSeq: 106 INVITE
Max-Forwards: 70
Expires: 180
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= from; gci= 2-231448; call-instance= 2
Remote-Party-ID: "Paul Giral" <sip:89915644@172.18.106.59>;party=calling;screen=yes;privacy=off
Contact: <sip:89915644@172.18.106.59:5061;transport=tls>
Content-Length: 0

Media Re-negotiation

Re-INVITE – Offer in 200 OK

SIP/2.0 200 OK

Via: SIP/2.0/TLS 172.18.106.59:5061;branch=z9hG4bK901fac34c0fb1b

From: "Paul Giralte" <sip:89915644@172.18.106.59>;tag=15462272~0d0d25d7-4931-4a07-83c6-b82e2c213ca7-45545776

To: <sip:89915644@172.18.106.59>;tag=0022bdd6843100702aae8e5b-4be253be

Call-ID: 8c045780-f0c1fd34-8d838f-3b6a12ac@172.18.106.59

Date: Wed, 11 Jan 2025 03:08:52 GMT

CSeq: 106 INVITE

Server: Cisco-8865/12.0.1

Contact: <sip:db40e44-0dfe-45f1-bd7f-e652098ca344@10.116.101.41:49833;transport=tls>

Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO

Remote-Party-ID: "Paul Giralte" <sip:89915644@172.18.106.59>;party=called;id-type=subscriber;privacy=off;screen=yes

Supported: replaces,join,sdp-anat,norefersub,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-config,X-cisco-sis-5.2.0,X-cisco-xsi-8.5.1

Allow-Events: kpml,dialog

Recv-Info: conference

Recv-Info: x-cisco-conference

Content-Length: 788

Content-Type: application/sdp

Content-Disposition: session;handling=optional

Media Re-negotiation

Re-INVITE – Offer in 200 OK

v=0
o=Cisco-SIPUA 26259 2 IN IP4 10.116.101.41
s=SIP Call
t=0 0
m=audio 32518 RTP/SAVP 0 8 18 102 9 116 124 101
c=IN IP4 10.116.101.41
a=crypto:XX
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:102 L16/16000
a=rtpmap:9 G722/8000
a=rtpmap:116 iLBC/8000
a=rtpmap:124 ISAC/16000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
m=video 17614 RTP/AVP 126 97
c=IN IP4 10.116.101.41
b=TIAS:2500000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801F;packetization-mode=1;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801F;packetization-mode=0;level-asymmetry-allowed=1
a=sendrecv

Media Re-negotiation

Re-INVITE – Answer in ACK

ACK sip:db40e44-0dfe-45f1-bd7f-e652098ca344@10.116.101.41:49833;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.106.59:5061;branch=z9hG4bK901fb064465a06
From: "Paul Giralt" <sip:89915644@172.18.106.59>;tag=15462272~0d0d25d7-4931-4a07-83c6-b82e2c213ca7-45545776
To: <sip:89915644@172.18.106.59>;tag=0022bdd6843100702aae8e5b-4be253be
Date: Wed, 11 Jan 2025 03:08:52 GMT
Call-ID: 8c045780-f0c1fd34-8d838f-3b6a12ac@172.18.106.59
Max-Forwards: 70
CSeq: 106 ACK
Allow-Events: presence
Content-Type: application/sdp
Content-Length: 446

Media Re-negotiation

Re-INVITE – Answer in ACK – Decline Video Support

```
v=0
o=CiscoSystemsCCM-SIP 15462272 3 IN IP4 172.18.106.59
s=SIP Call
t=0 0
m=audio 4000 RTP/SAVP 0
c=IN IP4 172.18.106.58
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
a=rtpmap:0 PCMU/8000
a=ptime:20
a=sendonly
m=video 0 RTP/AVP 126
c=IN IP4 10.116.101.50
b=TIAS:1000000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801E;packetization-mode=1;level-asymmetry-allowed=1
a=mid:227796888
```

DTMF Relay

- 3 Methods for passing DTMF digits over a SIP network:
 - RFC 4733 (a.k.a. RFC 2833)
 - SIP NOTIFY
 - SIP Keypad Markup Language (KPML)

DTMF Relay

RFC 4733 / RFC 2833

- Digits are passed in the RTP stream with a unique payload type
- Capability is negotiated in SDP like any other codec

Offer

```
m=audio 30414 RTP/AVP 0 8 116 18 100 101
c=IN IP4 172.18.106.231
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 iLBC/8000
a=fmtp:116 mode=20
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:100 X-NSE/800
a=fmtp:100 192-194
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

Answer

```
m=audio 17236 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

DTMF Relay

SIP NOTIFY

- Passes DTMF information in a SIP NOTIFY message telephone-event Event
- Negotiated in Call-Info header

```
INVITE sip:+19195553333@172.18.106.231:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.106.59:5060;branch=z9hG4bK9843c455840434
From: "Paul Giralto" <sip:9195551234@172.18.106.59>;tag=14902469~0d0d25d7-4931-4a07-83c6
To: <sip:+19195553333@172.18.106.231>
Date: Mon, 13 May 2024 14:48:00 GMT
Call-ID: 1a189580-1901fd20-962c99-3b6a12ac@172.18.106.59
... snip ...
Allow-Events: telephone-event
Call-Info: <sip:172.18.106.59:5060>;method="NOTIFY;Event=telephone-event;Duration=500"
Call-Info: <urn:x-cisco-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
... snip ...
Max-Forwards: 69
Content-Length: 0
```

DTMF Relay

SIP NOTIFY

SIP/2.0 200 OK

Via: SIP/2.0/UDP 172.18.106.59:5060;branch=z9hG4bK9843c455840434

From: "Paul Giralt" <sip:9195551234@172.18.106.59>;tag=14902469~0d0d25d7-4931-4a07-83c6

To: <sip:+19195553333@172.18.106.231>;tag=4363A830-17FC

Call-ID: 1a189580-1901fd20-962c99-3b6a12ac@172.18.106.59

... snip ...

Allow-Events: telephone-event

Call-Info: <sip:172.18.106.231:5060>;method="NOTIFY;Event=telephone-event;Duration=500"

... snip ...

Content-Length: 601

DTMF Relay

SIP NOTIFY

- Digits passed in payload of a NOTIFY message

NOTIFY sip:172.18.106.231:5060 SIP/2.0

Via: SIP/2.0/UDP 172.18.106.59:5060;branch=z9hG4bK98443140152a0a

From: "Paul Giralt" <sip:9195551234@172.18.106.59>;tag=14902469~0d0d25d7-4931-4a07-83c6

To: <sip:+19195553333@172.18.106.231>;tag=4363A830-17FC

Call-ID: 1a189580-1901fd20-962c99-3b6a12ac@172.18.106.59

CSeq: 104 NOTIFY

Max-Forwards: 70

Date: Mon, 13 May 2024 14:48

User-Agent: Cisco-CUCM15.0

Event: telephone-event

Subscription-State: active

Contact: <sip:172.18.106.59:5060>

P-Asserted-Identity: "Paul Giralt" <sip:9195551234@172.18.106.59>

Content-Type: audio/telephone-event

Content-Length: 4

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7		
event								E	R	unused								duration															

.d

DTMF Relay

SIP KPML

- Passes DTMF information in a SIP NOTIFY message kpml Event
- Capability advertised in Allow-Events – uses SUBSCRIBE message to subscribe

```
INVITE sip:+19195554444@172.18.106.231:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.106.59:5060;branch=z9hG4bK986efd6c4e51e4
From: "Paul Giralto" <sip:9195551234@172.18.106.59>;tag=14918970~0d0d25d7-4931-4a07-83c6
To: <sip:+19195554444@172.18.106.231>
Date: Mon, 13 May 2024 15:05:24 GMT
Call-ID: 885e5780-19110134-96567f-3b6a12ac@172.18.106.59
User-Agent: Cisco-CUCM15.0
... snip ...
Allow-Events: presence, kpml
... snip ...
Session-Expires: 18000
Max-Forwards: 69
Content-Length: 0
```

DTMF Relay

SIP KPML

SIP/2.0 200 OK

Via: SIP/2.0/UDP 172.18.106.59:5060;branch=z9hG4bK986efd6c4e51e4

From: "Paul Giralto" <sip:9195551234@172.18.106.59>;tag=14918970~0d0d25d7-4931-4a07-83c6

To: <sip:+19195554444@172.18.106.231>;tag=437394E8-2E1

Date: Mon, 13 May 2017 15:05:26 GMT

Call-ID: 885e5780-19110134-96567f-3b6a12ac@172.18.106.59

CSeq: 101 INVITE

Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO

~~Allow-Events:~~ kpml, telephone-event

Remote-Party-ID: <sip:9196247285@172.18.106.231>;party=called;screen=no;privacy=off

Contact: <sip:+19196247285@172.18.106.231:5060>

Supported: replaces

Server: Cisco-SIPGateway/IOS-15.6.2.T

Require: timer

Session-Expires: 18000;refresher=uac

Content-Type: multipart/mixed;boundary=uniqueBoundary

Mime-Version: 1.0

Content-Length: 600

DTMF Relay

SIP KPML

Subscribe to KPML

SUBSCRIBE sip:9195554444@172.18.106.59:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.106.231:5060;branch=z9hG4bKBAE27139E
From: <sip:+19195551234@172.18.106.231>;tag=437394E8-2E1
To: "Paul Giralt" <sip:9195554444@172.18.106.59>;tag=14918970~0d0d25d7-4931-4a07-83c6
Call-ID: 885e5780-19110134-96567f-3b6a12ac@172.18.106.59
CSeq: 101 SUBSCRIBE
Max-Forwards: 70
User-Agent: Cisco-SIPGateway/IOS-15.6.2.T
Event: kpml
Expires: 7200
Contact: <sip:172.18.106.231:5060>
Content-Type: application/kpml-request+xml
Content-Length: 327

```
<?xml version="1.0" encoding="UTF-8"?><kpml-request xmlns="urn:ietf:params:xml:ns:kpml-request"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:ietf:params:xml:ns:kpml-
request kpml-request.xsd" version="1.0"><pattern persist="persist"><regex
tag="dtmf">[x*#ABCD]</regex></pattern></kpml-request>
```

DTMF Relay

SIP KPML

Send a Digit

NOTIFY sip:172.18.106.231:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.106.59:5060;branch=z9hG4bK986f73662cca3b
From: "Paul Giralt" <sip:9195554444@172.18.106.59>;tag=14918970~0d0d25d7-4931-4a07-83c6
To: <sip:+19195551234@172.18.106.231>;tag=437394E8-2E1
Call-ID: 885e5780-19110134-96567f-3b6a12ac@172.18.106.59
CSeq: 104 NOTIFY
Max-Forwards: 70
User-Agent: Cisco-CUCM12.0
Event: kpml
Subscription-State: active;expires=7197
Contact: <sip:9195554444@172.18.106.59:5060>
Content-Type: application/kpml-response+xml
Content-Length: 336

```
<?xml version="1.0" encoding="UTF-8" ?>  
<kpml-response xmlns="urn:ietf:params:xml:ns:kpml-response"  
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  xsi:schemaLocation="urn:ietf:params:xml:ns:kpml-response kpml-response.xsd" code="200" digits="1"  
  forced_flush="false" suppressed="false" tag="dtmf" text="Success" version="1.0"/>
```

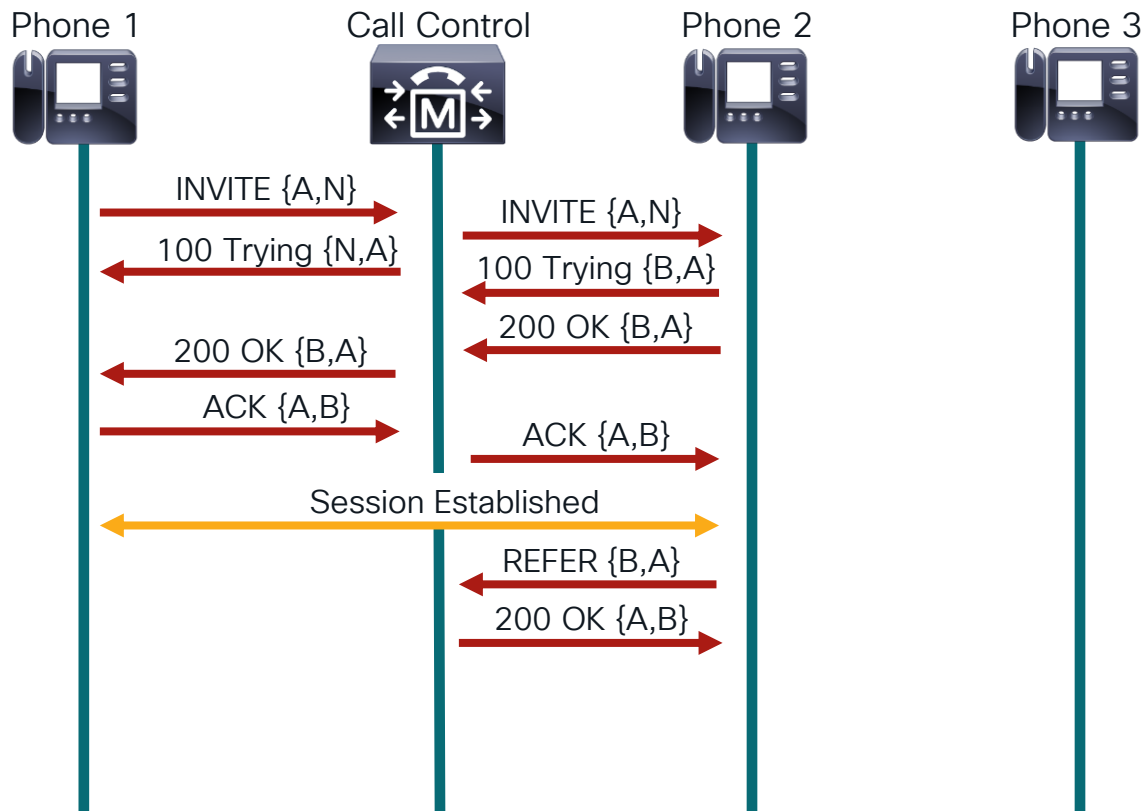
SIP Session-ID (RFC 7989)

- Session-ID Header carries an end-to-end session identifier
- Allows you to track a call as it traverses through various SIP systems

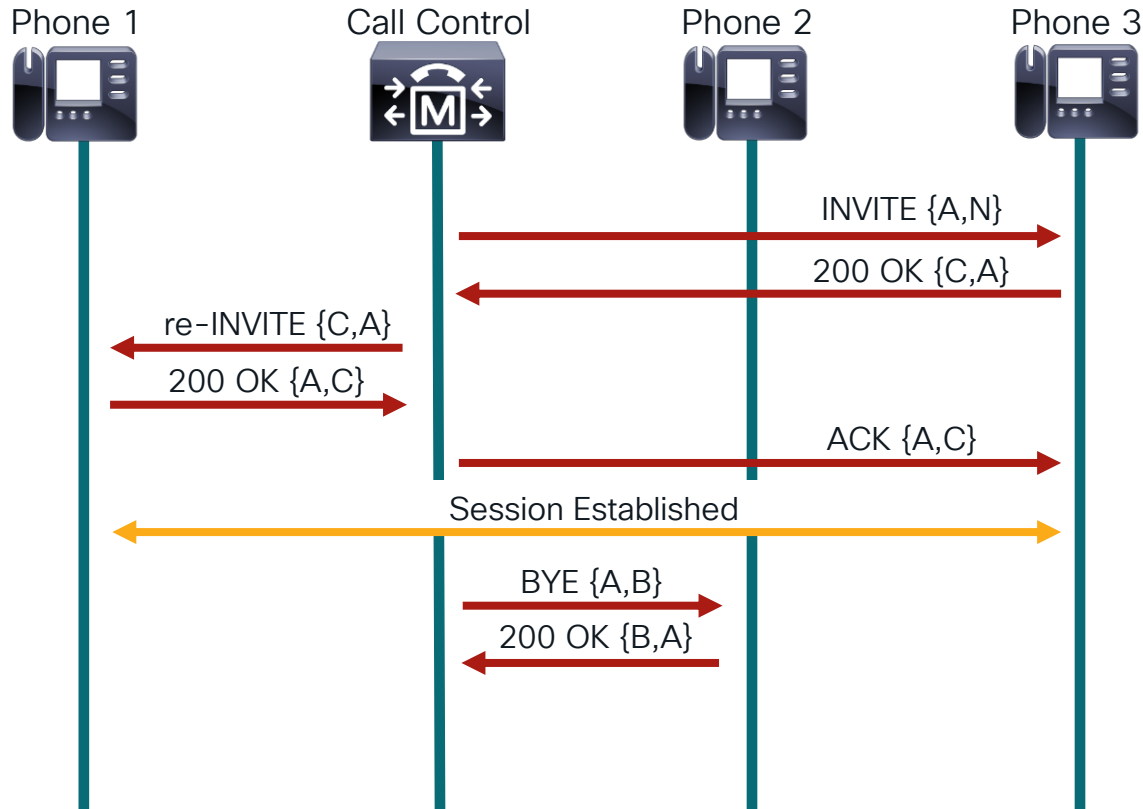
Session-ID: 65596d4800105000a00074a02fc0d796 remote=747a0ead00105000a00074a02fc0cf3b
Local UUIDRemote UUID

- Each UUID represents an endpoint in the session
- Session Identifier represented as {A,B} referring to {local,remote} UUIDs
- {A,B} is equivalent to {B,A}
- Initial INVITE starts with the null (all zero) remote UUID represented as {A,N}

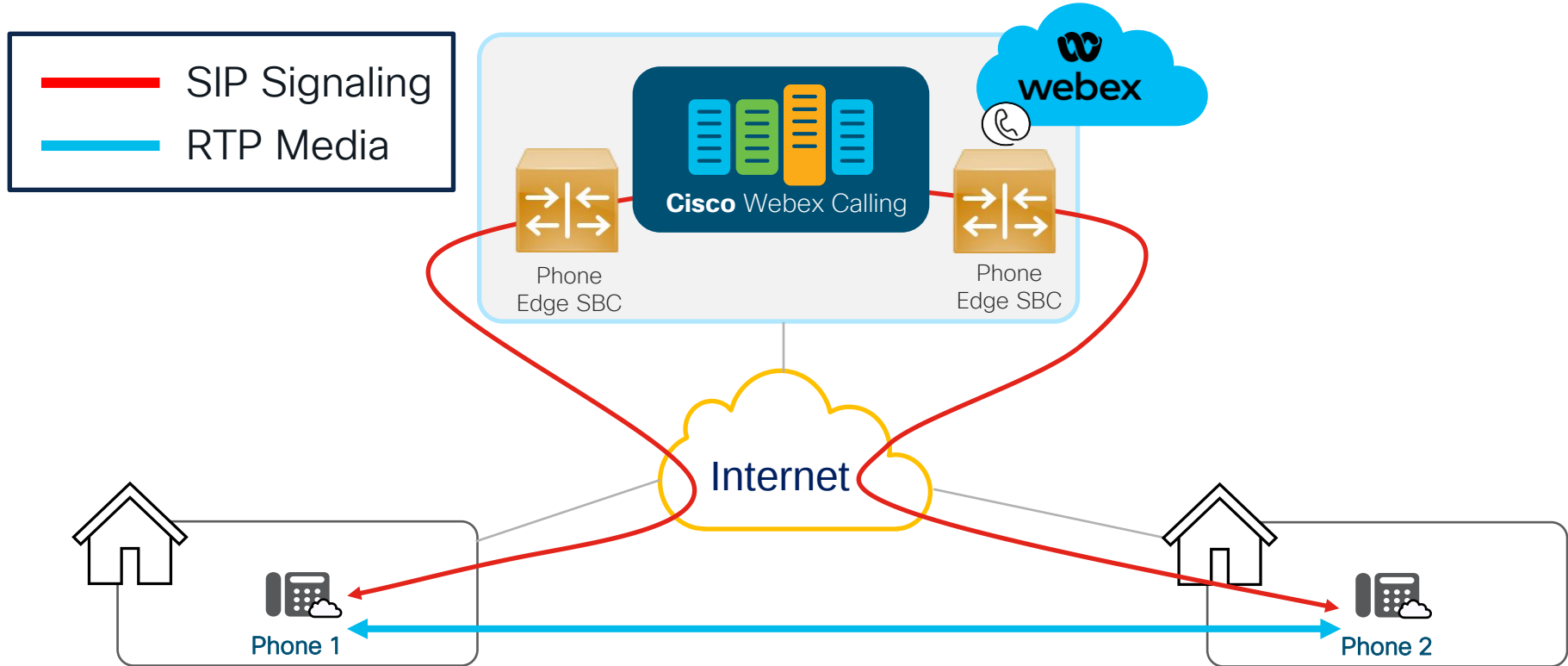
SIP Call with Session-ID Headers



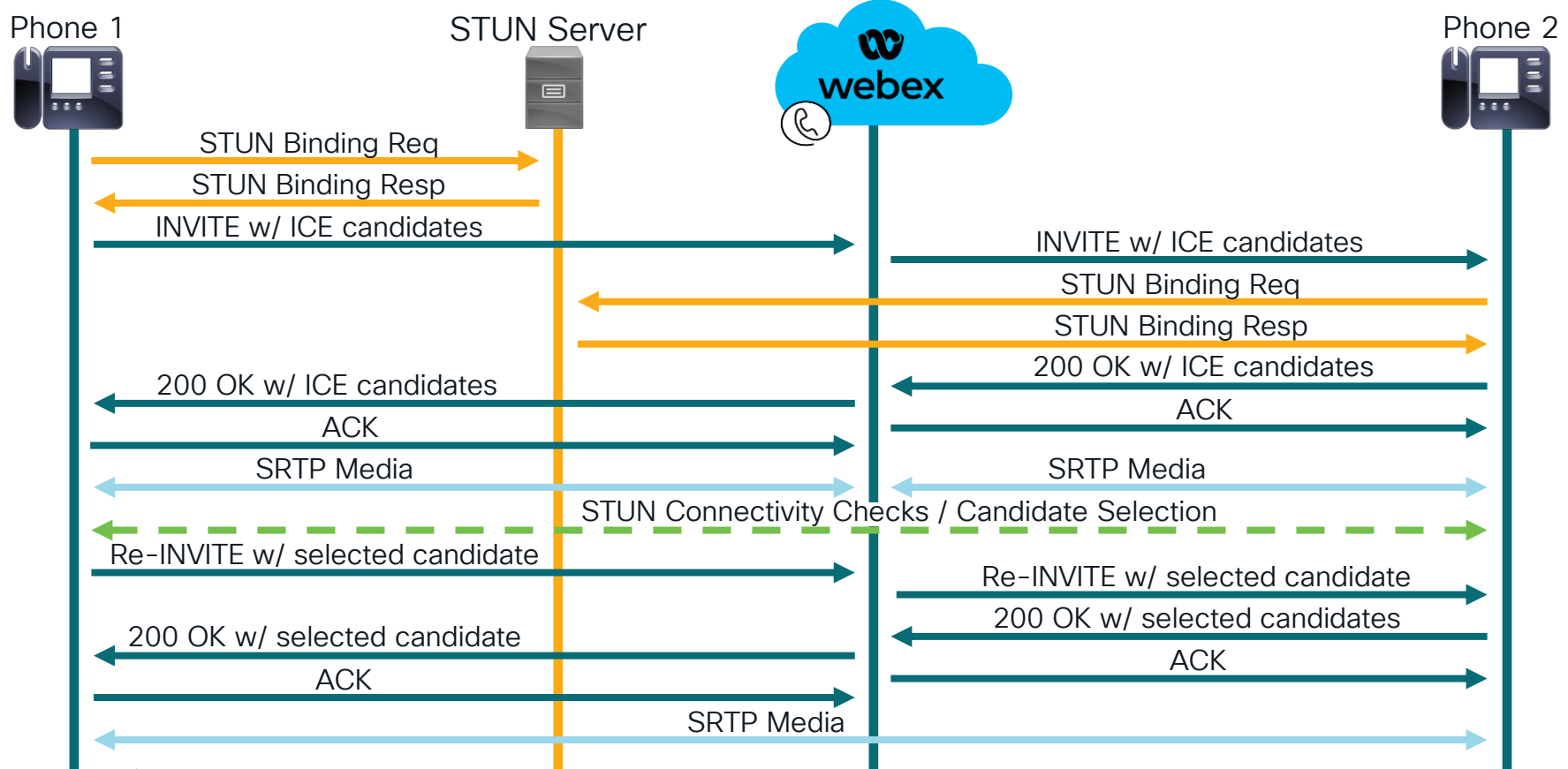
SIP Call with Session-ID Headers



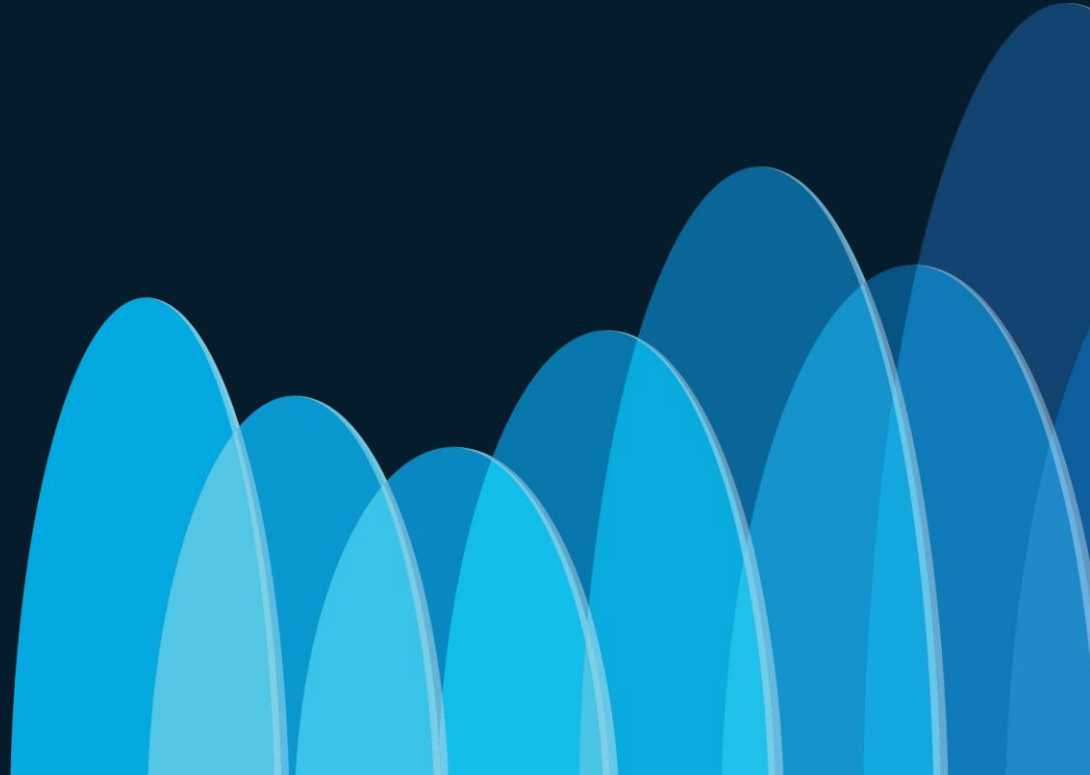
Interactive Connectivity Establishment (ICE)



Call Setup with ICE



Troubleshooting Tools



Collaboration Solutions Analyzer

cway.cisco.com/csa

The screenshot displays the Cisco TAC Tool interface for the Collaboration Solutions Analyzer. The left pane shows a list of events, and the right pane shows a detailed SIP call log.

Tools Catalog / Cisco TAC Tool

Back to top Available files Diagnostic signatures System information Log overview

Device

- [20:21:33.249] cucm1b Outgoing SIP TCP 180 Ringing response for CSeq:1000003ee1-00005df3@10.0.251.126
- [20:21:33.255] cucm1b Incoming SIP TCP 200 OK response for CSeq:101 INVITE
- [20:21:33.257] cucm1b RouteListCdrC stopped hunting for Route List
- [20:21:33.257] cucm1b Remote party with CI 34411856 answered the call and

Media

- [20:21:33.258] cucm1b MediaConnect Request for CI (34411855, 34411856) i
- [20:21:33.259] cucm1b SIPInterface sending offer with audio caps ('OPUS' 'G729' 'G729AnnexA' 'H264_FEC'), video caps ('H264' 'H264_FEC') and app c
- [20:21:33.262] cucm1b Media is established on 'SIP Trunk' with CI 34411855
- [20:21:33.264] cucm1b Media is established on 'SIP Trunk' with CI 34411856
- [20:21:33.266] cucm1b Outgoing SIP TCP ACK request with CSeq:101 ACK

Detail

10.0.251.126

CUCM 10.0.130.82

10.0.130.51

20:21:32.761 200 OK

20:21:33.079 Invite

+ SDP ver.: 0

20:21:33.080 100 Trying

20:21:33.087 Invite

20:21:33.090 100 Trying

20:21:33.248 180 Ringing

20:21:33.249 180 Ringing

20:21:33.255 200 OK

+ SDP ver.: 0

20:21:33.266 Ack

+ SDP ver.: 1

20:21:33.267 200 OK

cisco *Live!*

Connected UC Troubleshooting in Control Hub

Troubleshooting > Connected UC

The image displays two screenshots of the Cisco Webex Control Hub Troubleshooting interface, specifically the 'Connected UC' section.

Left Screenshot: Ladder diagram

- Call leg info:** Ladder diagram, Signalling, Digit analysis.
- Global Call Id:** 5049705.
- Call leg info:** Cisco-SIPGateway... 64.102.247.94, Cisco-CUCM15.0 172.18.106.59.
- Events:**
 - 03:11:14.808: INVITE (101 INVITE) SDP v:1204
 - 03:11:14.809: 100 TRYING (101 INVITE)
 - 03:11:14.814: (No event)
 - 03:11:14.815: (No event)
 - 03:11:14.816: (No event)
 - 03:11:14.819: (No event)
 - 03:11:14.827: (No event)
 - 03:11:17.105: (No event)
 - 03:11:17.113: (No event)
- Session Status:** 181 SESSION IN PROGRESS (101 INVITE)

Right Screenshot: Message

- Global Call Id:** 5049705.
- Call leg info:** Ladder diagram, Signalling, Digit analysis.
- Global Call Id:** 5049705.
- Message body:**

```
INVITE sip:18008001180@172.18.106.59 SIP/2.0
Via: SIP/2.0/TCP 64.102.247.94:5060;branch=z9hG4bK7878D80
Remote-Party-ID: "Paul Giral" <sip:19199940111@64.102.247.94>;party=calling;screen=yes;privacy=off
From: "Paul Giral" <sip:19199940111@64.102.247.94>;tag=6F5A36DF-149F
To: <sip:18008001180@172.18.106.59>
Date: Sun, 02 Feb 2025 03:11:14 GMT
Call-ID: 324EEC3E-E04A11EF-B419AD6F-8A7E25D7@64.102.247.94
Supported: 100rel, timer, resource-priority, replaces
Mn-SE: 1800
Cisco-Guid: 0843763019-3762950639-3021188463-2323523031
User-Agent: Cisco-SIPGateway/IOS-17.12.2
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1738465874
Contact: <sip:19199940111@64.102.247.94:5060;transport=udp>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 68
Session-ID: ce9b9f85012050008000ac5e0b4f6183;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 448
v=0
o=CiscoSystemsSIP-GW-UserAgent 6564 1204 IN IP4 64.102.247.94
s=SIP Call
c=IN IP4 64.102.247.94
t=0 0
m=audio 11598 RTP/AVP 99 0 8 101
c=IN IP4 64.102.247.94
a=rtpmap:99 opus/48000/2
a=ftmp:99
```

Download from [translatorx.org](https://www.translatorx.org)

Cisco Collaboration Trace Translator

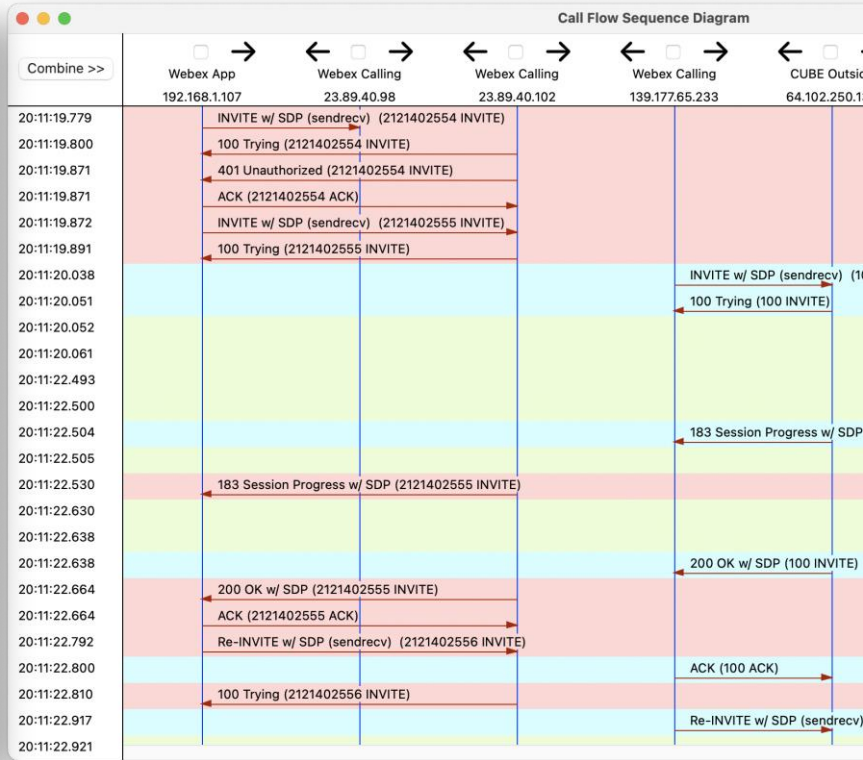
☒ Filters Enabled

3 Filters Configured

Timestamp	Node/Interface	Remote Device	Direction	Protocol	Message Name	TCP Handle/From Tag	Call Ref / ID
01/31/2025 20:11:19.779	192.168.1.107	23.89.40.98	Out	SIP	INVITE	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.779	192.168.1.107	23.89.40.98	Out	SIP	INVITE	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.800	192.168.1.107	23.89.40.102	In	SIP	100 Trying	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.800	192.168.1.107	23.89.40.102	In	SIP	100 Trying	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.871	192.168.1.107	23.89.40.102	In	SIP	401 Unauthorized	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.871	192.168.1.107	23.89.40.102	Out	SIP	ACK	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.871	192.168.1.107	23.89.40.102	In	SIP	401 Unauthorized	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.871	192.168.1.107	23.89.40.102	Out	SIP	ACK	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.872	192.168.1.107	23.89.40.102	Out	SIP	INVITE	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.872	192.168.1.107	23.89.40.102	Out	SIP	INVITE	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.891	192.168.1.107	23.89.40.102	In	SIP	100 Trying	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:19.891	192.168.1.107	23.89.40.102	In	SIP	100 Trying	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:20.038	64.102.250.134	139.177.65.233	In	SIP	INVITE	1086480704-17383542800...	SS620120033301025-8304...
01/31/2025 20:11:20.051	64.102.250.134	139.177.65.233	Out	SIP	100 Trying	1086480704-17383542800...	SS620120033301025-8304...
01/31/2025 20:11:20.051	64.102.250.134	172.18.106.59	Out	SIP	INVITE	68B369E1-1A4B	5EA76BE2-DF4611EF-BFAA...
01/31/2025 20:11:20.061	64.102.247.94	172.18.106.59	In	SIP	100 Trying	68B369E1-1A4B	5EA76BE2-DF4611EF-BFAA...
01/31/2025 20:11:22.493	64.102.247.94	172.18.106.59	In	SIP	183 Session Progress	68B369E1-1A4B	5EA76BE2-DF4611EF-BFAA...
01/31/2025 20:11:22.500	64.102.247.94	172.18.106.59	Out	SIP	PRACK	68B369E1-1A4B	5EA76BE2-DF4611EF-BFAA...
01/31/2025 20:11:22.504	64.102.250.134	139.177.65.233	Out	SIP	183 Session Progress	1086480704-17383542800...	SS620120033301025-8304...
01/31/2025 20:11:22.505	64.102.247.94	172.18.106.59	Out	SIP	200 OK	68B369E1-1A4B	5EA76BE2-DF4611EF-BFAA...
01/31/2025 20:11:22.530	192.168.1.107	23.89.40.102	In	SIP	183 Session Progress	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:22.530	192.168.1.107	23.89.40.102	In	SIP	183 Session Progress	660dba695714ad08efa374...	d16f219634f0e84532da13c...
01/31/2025 20:11:22.630	64.102.247.94	172.18.106.59	In	SIP	200 OK	68B369E1-1A4B	5EA76BE2-DF4611EF-BFAA...
01/31/2025 20:11:22.638	64.102.247.94	172.18.106.59	Out	SIP	ACK	68B369E1-1A4B	5EA76BE2-DF4611EF-BFAA...
01/31/2025 20:11:22.638	64.102.250.134	139.177.65.233	Out	SIP	200 OK	1086480704-17383542800...	SS620120033301025-8304...

INVITE sip:91800801180812013670.us10.bcld.webex.com SIP/2.0

Via: SIP/2.0/TLS 192.168.1.107;cs=80;branch=s9bdc48f866ee617



Wireshark

cvp1.pcap

Filter: sip

No.	Time	Timestamp	Source	Destination	Protocol	Length	Info
48	20.994069	14:29:27.528037	172.18.106.86	161.44.248.92	SIP	1130	Request: INVITE sip:89295994@161.44.248.92:5060;transport=...
49	20.996497	14:29:27.530465	161.44.248.92	172.18.106.86	SIP	580	Status: 100 Trying
52	21.006751	14:29:27.540719	161.44.248.92	172.18.106.86	SIP	1003	Request: INVITE sip:8003200119@172.18.106.86:5060;transport=...
53	21.030568	14:29:27.564536	172.18.106.86	161.44.248.92	SIP	368	Status: 100 Trying
54	21.075842	14:29:27.609810	172.18.106.86	161.44.248.92	SIP/SDP	1146	Status: 200 OK
55	21.077323	14:29:27.611291	161.44.248.92	172.18.106.86	SIP/SDP	1349	Status: 200 OK
58	21.296759	14:29:27.830727	172.18.106.86	161.44.248.92	SIP/SDP	866	Request: ACK sip:161.44.248.92:5060;transport=tcp
59	21.335569	14:29:27.869537	161.44.248.92	172.18.106.86	SIP/SDP	777	Request: ACK sip:8003200119@161.44.248.21:5060
197	26.639364	14:29:33.173332	161.44.248.92	172.18.106.86	SIP	999	Request: INVITE sip:91919191@172.18.106.86:5060;transport=...
200	26.640884	14:29:33.174852	161.44.248.92	172.18.106.86	SIP	524	Request: BYE sip:8003200119@161.44.248.21:5060
217	26.663060	14:29:33.197028	172.18.106.86	161.44.248.92	SIP	366	Status: 100 Trying
218	26.669918	14:29:33.203886	172.18.106.86	161.44.248.92	SIP	391	Status: 404 Not Found
219	26.670455	14:29:33.204423	161.44.248.92	172.18.106.86	SIP	419	Request: ACK sip:91919191@172.18.106.86:5060;transport=ud...
220	26.675194	14:29:33.209162	172.18.106.86	161.44.248.92	SIP	633	Request: BYE sip:89363903@161.44.248.92:5060;transport=ud...

Frame 52: 1003 bytes on wire (8024 bits), 1003 bytes captured (8024 bits)

- Ethernet II, Src: Vmware_b0:1e:9f (00:50:56:b0:1e:9f), Dst: CiscoInc_98:c0:00 (00:50:3e:98:c0:00)
- Internet Protocol Version 4, Src: 161.44.248.92, Dst: 172.18.106.86
- User Datagram Protocol, Src Port: 34806 (34806), Dst Port: 5060 (5060)
- Session Initiation Protocol (INVITE)
 - Request-Line: INVITE sip:8003200119@172.18.106.86:5060;transport=udp SIP/2.0
 - Message Header
 - Via: SIP/2.0/UDP 161.44.248.92:5060;branch=z9hG4bKYjrw2d3BA5raZsR4YS2T0w~143
 - Max-Forwards: 68
 - To: <sip:8003200119@172.18.106.86:5060;transport=udp>
 - From: "Lab Telephone" <sip:89363903@161.44.248.92:5060>;tag=ds4f52e2ed
 - Call-ID: 121397216753839@161.44.248.92

```

0000 00 50 3e 98 c0 00 00 50 56 b0 1e 9f 08 00 45 60 .P>...P V....E`
0010 03 dd 7b 39 00 00 00 11 0b 85 a1 2c f8 5c ac 12 ..{9.... ,... \..
0020 6a 56 87 f6 13 c4 03 c9 c7 55 49 4e 56 49 54 45 jV.....UINVITE
0030 20 73 69 70 3a 38 30 30 33 32 30 30 31 31 39 40 sip:800 3200119@
0040 31 37 32 2e 31 38 2e 31 30 36 2e 38 36 3a 35 30 172.18.1 06.86:50
0050 36 30 3b 74 72 61 6e 73 70 6f 72 74 3d 75 64 70 60;trans port=udp
0060 20 53 49 50 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 SIP/2.0 ..Via: S
0070 49 50 2f 32 2e 30 2f 55 44 50 20 31 36 31 2e 34 IP/2.0/U DP 161.4
  
```

Packets: 338 · Displayed: 56 (16.6%) · Load time: 0:0.8 Profile: Default

SIP Troubleshooting Methodology & Case Studies



Common SIP Problem Domains

- Call Establishment Failure
- Call Drop
- Mid-call feature failure
- Media-related issues (which may be due to signaling failures)
 - Audio cut-through delay
 - No audio / one-way audio
 - Media optimization issues
- Identity (name, number) Presentation Issues

Finding the Problematic Call(s)

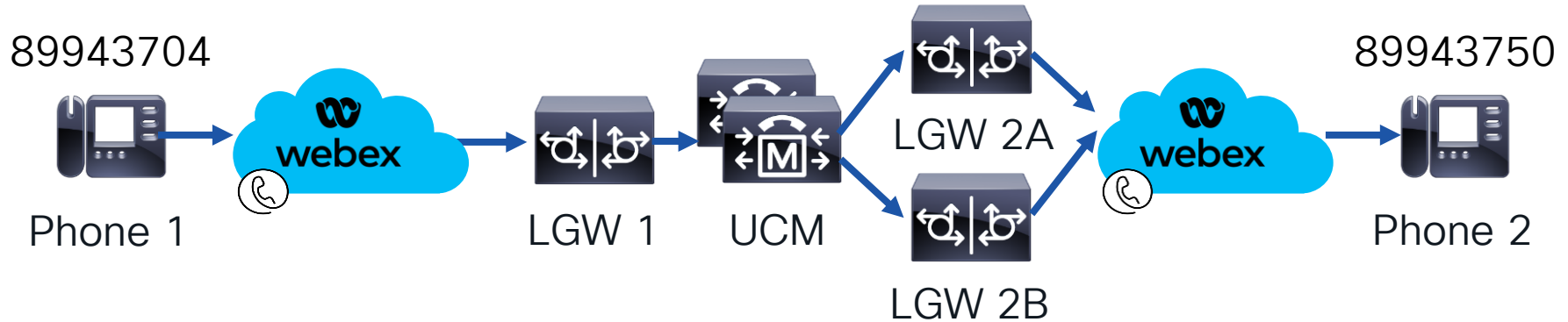
- Search by calling / called number
 - “INVITE sip:<number>”
 - Search on calling number or domain to find in From or PAI/PPI headers
- Search for calls with “bad” disconnect reasons
- Search for a timeframe when problem occurred
- Start a live log tail while reproducing the issue
- Search Call Detail Records
 - Search for calls based on number or disconnect reason
 - Find SIP Session ID, Call ID, Correlation ID and use to search SIP signaling

Call Establishment Failure

- Is the calling / called device registered?
- Does called / calling number match dial plan entries?
- Are calls blocked due to dial plan restrictions?
- Network related issue?
- TLS Handshake issues?
- Authentication issues?
- “Double Calls”

Call Establishment Failure

Calling from Phone 1 to Phone 2 Fails



Call Establishment Failure Demo

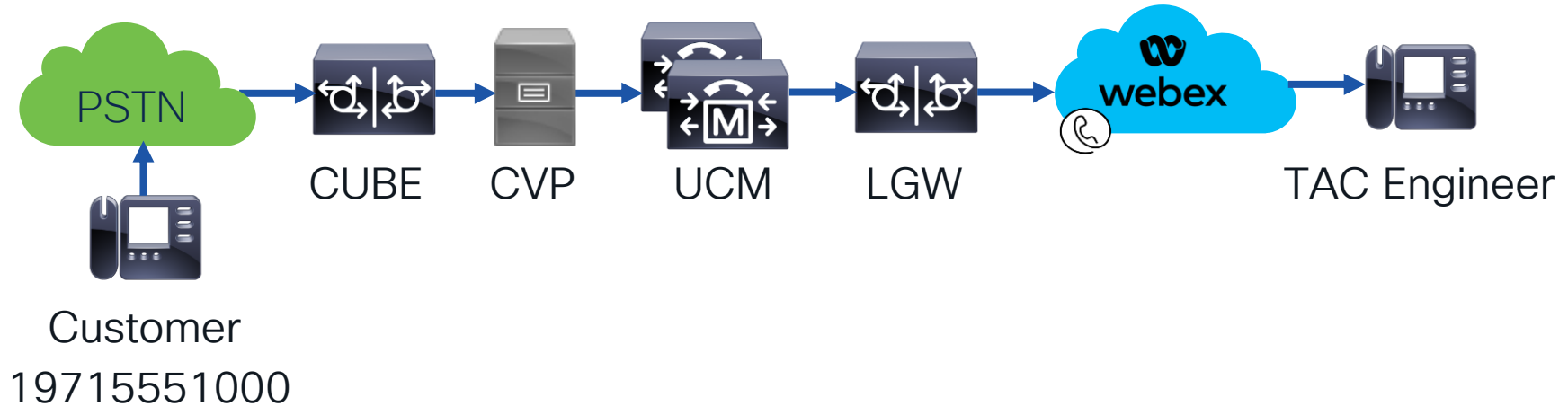


Call Drop

- When did the call drop happen?
- Which side dropped the call?
- Any Reason headers or other indications as to why?
- Any network issues at the time when the drop occurred?

Call Drop

TAC reports intermittent call drops



Call Drop Demo



Mid-Call Feature Failure

- Which side dropped the call?
- Is it reproducible?
- Where in the process of invoking the feature did it fail?

Media Related Issues

- Which IP addresses were negotiated for media?
- Did the call use Early Offer or Delayed Offer? Early Media?
- Was ICE attempted? Did it succeed?
- How long did it take to exchange the media?
- Does media issue start after a mid-call feature invocation?
- Check media direction attributes – stuck in inactive?
- If using SRTP, check for ROC issues

Identity Presentation Issues

- What do Identity Headers say at different points in the call?
 - From
 - P-Asserted-Identity (PAI)
 - P-Preferred-Identity (PPI)
- What transformations might be applied to calling / called name / number?
- Check for translations / transformations along the call path
- Pay attention to forward / transfer scenarios

Caller ID for Calls from Webex Calling to Trunks

TN and/or extension configured?			“Caller ID Format for Calls from and to On-premises”	
			+E.164	ESN
TN	Extension	<u>PAI</u>	<u>From</u>	<u>From</u>
Yes	Yes	TN, +E.164	TN, +E.164	Location prefix + extension
Yes	No	TN, +E.164	TN, +E.164	According to user caller ID configuration, +E.164
No	Yes	Location main number, +E.164	According to user caller ID configuration, +E.164	Location prefix + extension
No	No	No calls allowed without either TN or extension configured		

Identity Presentation Issues

Caller ID	External caller ID phone number	☒ Direct line: +19199943712, Ext 43712 ☐ Location number: +19199943700 ☐ Other number from organization
	Additional external caller ID phone numbers	When checked, these numbers are available for this user to select as external caller ID ☐ Direct line: +19199943712, Ext 43712 ☒ Location number: +19199943700 ☒ Custom number from organization +19199943702
	External caller ID name	☒ Direct line: Joni Sherman ☐ Location external caller ID name: RTP ☐ Other external caller ID name
	Caller ID first name	Joni
	Caller ID last name	Sherman
	Block caller ID for received calls	☒ Block this user's identity when receiving a call.
	Connected Line Identity Privacy for Redirected Calls	Users can choose to keep the identity of the person they are forwarding calls to private. They can either choose to do this only for external calls or for all calls. Terminating identity

Additional SIP Training and Case Studies



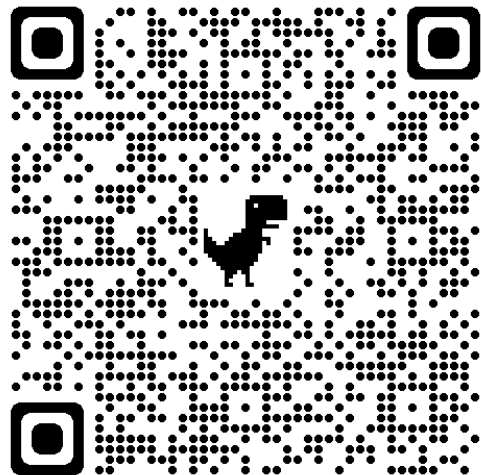
 On-Demand Library Featured Sessions Learning Maps Upcoming Events

On-Demand Library

Explore a free collection of on-demand sessions from our global Cisco Live events.

Here are the topics covered in each chapter:

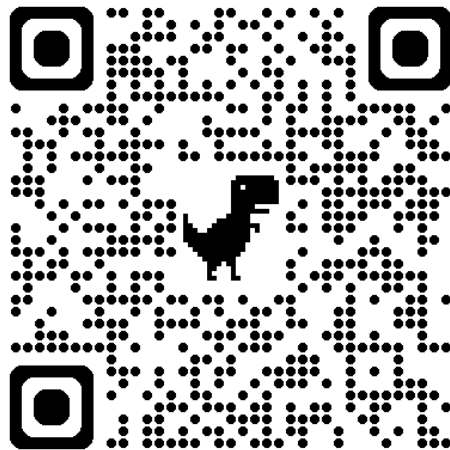
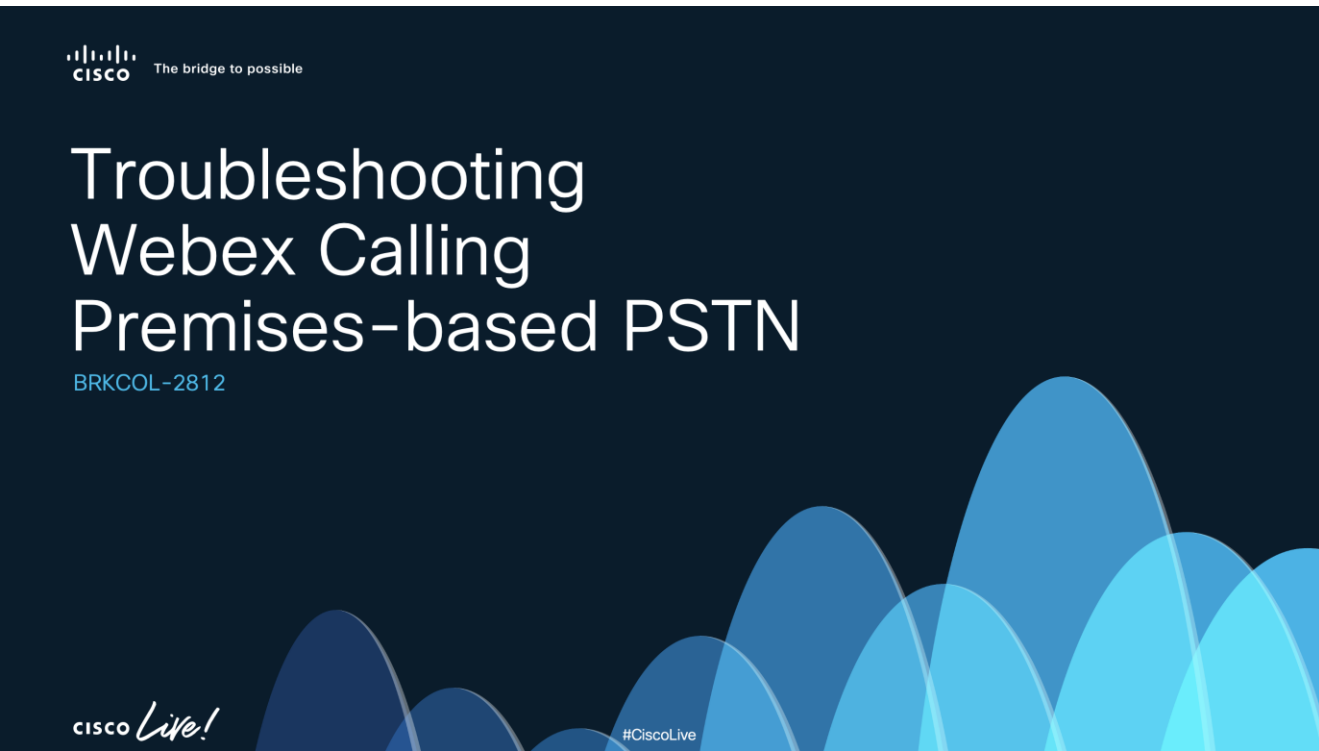
- **Chapter 1 - Introduction:** A brief introduction and overview of the agenda.
- **Chapter 2 - SIP Protocol Overview:** An overview of the SIP protocol. Examination of requests, responses, response codes, media establishment, early offer / delayed offer / early media, and DTMF relay.
- **Chapter 3 - Troubleshooting Tools:** An examination of the various troubleshooting tools available to help diagnose issues with SIP sessions.
- **Chapter 4 - Trace Configuration:** A quick overview of enabling and extracting SIP signaling from Unified CM, Expressway, and CUBE.
- **Chapter 5 - Case Studies - Part 1:** Detailed walk-through of two real-world case studies and examination of the SIP signaling as well as root cause determination.
- **Chapter 6 - Case Studies - Part 2:** Additional case studies with focus on live-demonstration of the troubleshooting tools and how they can be used to troubleshoot a problem.



Make sure you log in after
going to the above site

<https://www.ciscolive.com/on-demand/on-demand-library.html?#/session/16360601780640017Giu>

Additional SIP Training and Case Studies



Make sure you log in after going to the above site

<https://www.ciscolive.com/on-demand/on-demand-library.html?#/session/1717269041261001tKS9>

Reference Materials

- Reference Slides at the end of the PDF for this presentation include trace configuration and download details for:
 - UCM
 - Expressway
 - CUBE
 - Webex App
 - PhoneOS / MPP Phones
 - RoomOS Devices

Conclusion

- Session Initiation Protocol (SIP) Overview
 - User Agents
 - Requests and Responses
 - Headers
 - Session Description Protocol
 - Offer / Answer Model
 - DTMF Relay
 - SIP Session ID
 - ICE Overview
- Troubleshooting Tools
- Troubleshooting Methodology & Case Studies
- Additional Resources

Webex App

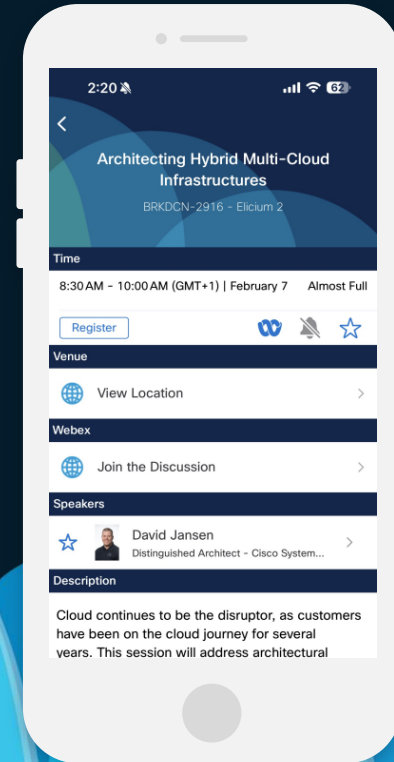
Questions?

Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events mobile app
- 2 Click “Join the Discussion”
- 3 Install the Webex app or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: pgiralt@cisco.com on Webex

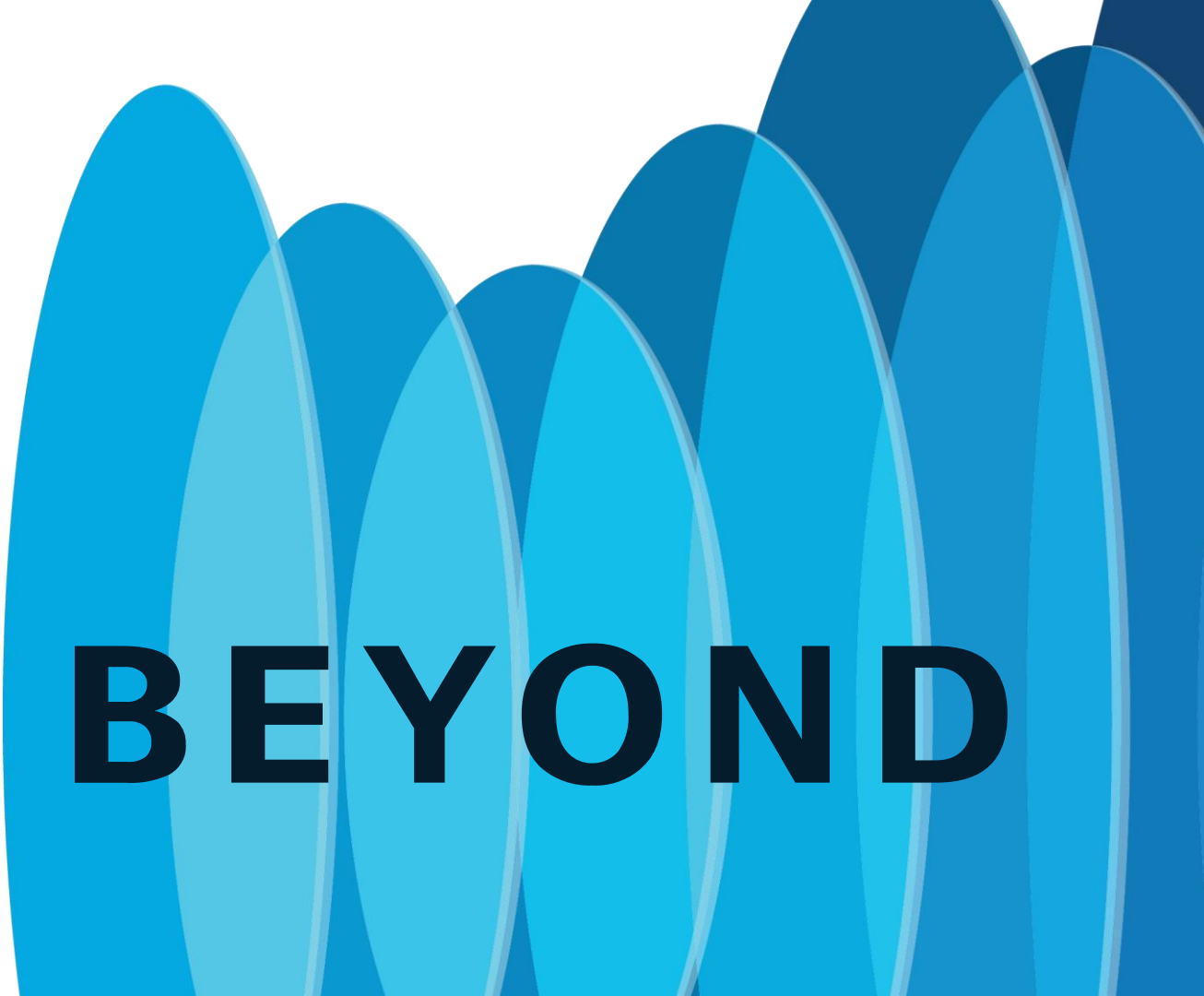


Thank you



CISCO *Live!*

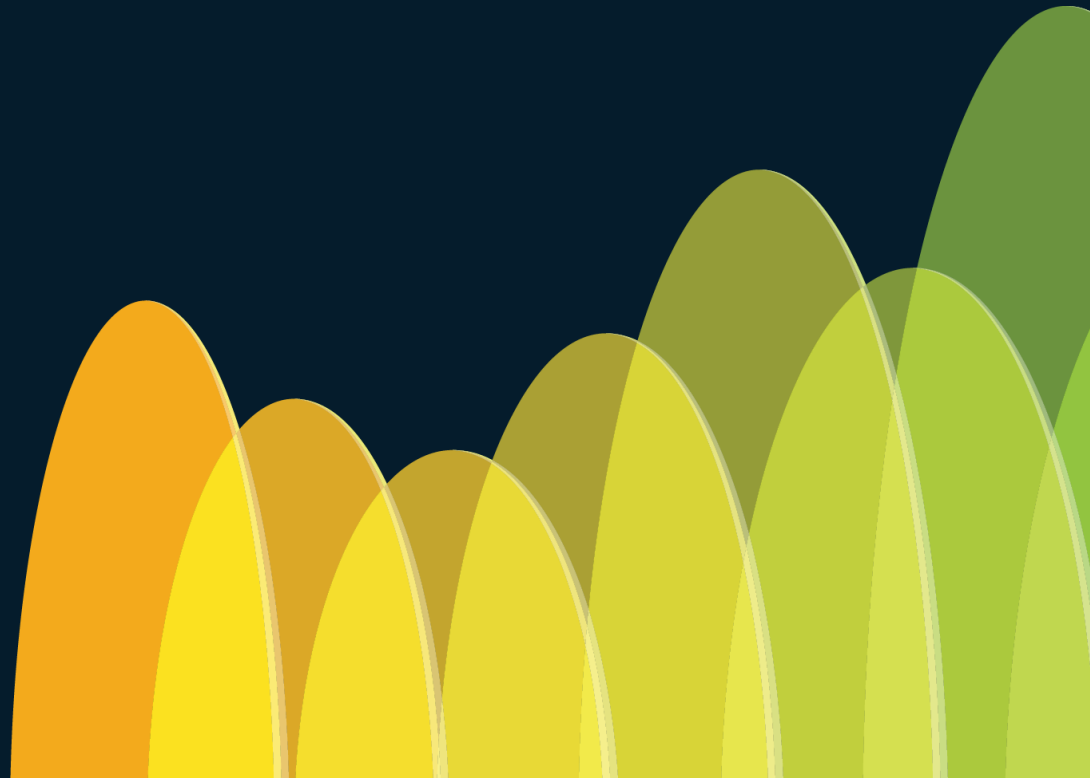
GO BEYOND

The background of the slide features a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are arranged in a way that creates a sense of depth and movement, resembling a stylized horizon or a series of waves. The overall composition is clean and modern, with the text elements clearly legible against the white background.

Reference Slides



Unified CM Trace Configuration



Unified CM Trace Configuration

- SIP messaging in Unified CM is written to the SDL trace file when appropriate trace levels are set
- Configured from **Cisco Unified Serviceability > Trace > Configuration** or by using Analysis Manager
- Unified CM 9.0 and later **fresh install** and later default to detailed tracing – no need to configure traces.

Unified CM Trace Configuration

The screenshot shows the Cisco Unified Serviceability interface for configuring traces. The page has a header with the Cisco logo and the text "Cisco Unified Serviceability For Cisco Unified Communications Solutions". Below the header is a navigation bar with links: Alarm, Trace, Tools, Snmp, CallHome, and Help. The main section is titled "Trace Configuration" and includes "Save" and "Set Default" buttons. The "Status" section shows "Ready". The "Select Server, Service Group and Service" section contains three dropdown menus: "Server*" (vnt-cm1a.cisco.com--CUCM Voice/Video), "Service Group*" (CM Services), and "Service*" (Cisco CallManager (Active)). Each dropdown has a "Go" button. Annotations with callout boxes point to these elements: "Select the Server" points to the Server dropdown, "Select Service Group" points to the Service Group dropdown, and "Select the Service on Which Trace Needs to Be Enabled" points to the Service dropdown. There is also an "Apply to All Nodes" checkbox and a "Trace On" checkbox (which is checked). The "Trace Filter Settings" section is partially visible at the bottom.

Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Alarm ▾ Trace ▾ Tools ▾ Snmp ▾ CallHome ▾ Help ▾

Trace Configuration

Save Set Default

Status:

Ready

Select Server, Service Group and Service

Server* vnt-cm1a.cisco.com--CUCM Voice/Video **Select the Server**

Service Group* CM Services **Select Service Group**

Service* Cisco CallManager (Active) **Select the Service on Which Trace Needs to Be Enabled**

☐ Apply to All Nodes

☒ Trace On

Trace Filter Settings

Unified CM Trace Configuration

Trace ConfigurationRelated Links: [SDL Configuration](#) [Go](#)

 Save  Set Default

1. Press Set Default

Status:
 Ready

Select Server, Service Group and Service
Server*
Service Group*
Service*
☒ Apply to All Nodes

Updates All Servers in this cluster with these settings

☒ Trace On

Trace Filter Settings
Debug Trace Level
☒ Enable H245 Message Trace ☒ Enable CDR Trace

2. Set to Detailed

Unified CM Trace Configuration

Trace Filter Settings

Debug Trace Level Detailed

- | | |
|--|--|
| ☒ Enable H245 Message Trace | ☒ Enable CDR Trace |
| ☒ Enable DT-24+/DE-30+ Trace | ☒ Enable Analog Trunk Trace |
| ☒ Enable PRI Trace | ☒ Enable All Phone Device Trace |
| ☒ Enable ISDN Translation Trace | ☒ Enable MTP Trace |
| ☒ Enable H225 & Gatekeeper Trace | ☒ Enable All GateWay Trace |
| ☒ Enable Miscellaneous Trace | ☒ Enable Forward & Miscellaneous Trace |
| ☒ Enable Conference Bridge Trace | ☒ Enable MGCP Trace |
| ☒ Enable Music On Hold Trace | ☒ Enable Media Resource Manager Trace |
| ☒ Enable CM Real-Time Information Server Trace | ☒ Enable SIP Call Processing Trace |
| ☒ Enable SIP Stack Trace | ☒ Enable SCCP Keep Alive Trace |
| ☒ Enable Annunciator Trace | ☒ Enable SpeedDial Trace |
| ☒ Enable SoftKey Trace | ☐ Enable SIP Keep Alive (REGISTER Refresh) Trace |
| ☐ Enable Route or Hunt List Trace | ☐ Enable IVR Trace |

Trace Collection

Various Ways to Collect Trace Files

- RTMT Collect Files ← Recommended
- RTMT Analysis Manager
- RTMT Remote Browse
- RTMT Query Wizard
- OS CLI (file get or file tail)
 - file tail activelog cm/trace/ccm/sdl recent

Gathering a Packet Capture from Unified CM

Use the Platform CLI command 'utils network capture'

```
admin:utils network capture ? (or utils network capture-rotate)
```

Syntax:

```
utils network capture [options]
```

```
options optional page, numeric, file fname, count num, size bytes, src addr,  
dest addr, port num, host protocol addr
```

```
admin:utils network capture file capturefile count 100000 size ALL host ip  
10.1.1.1
```

Executing command with options:

size=ALL	count=100000	interface=eth0
src=	dest=	port=
ip=10.1.1.1		

```
admin:file list activelog platform/cli
```

```
capturefile.cap
```

```
dir count = 0, file count = 1
```

```
admin:file get activelog platform/cli/capturefile.cap
```

Please wait while the system is gathering files info ...done.

Sub-directories were not traversed.

Number of files affected: 1

Total size in Bytes: 24

Total size in Kbytes: 0.0234375

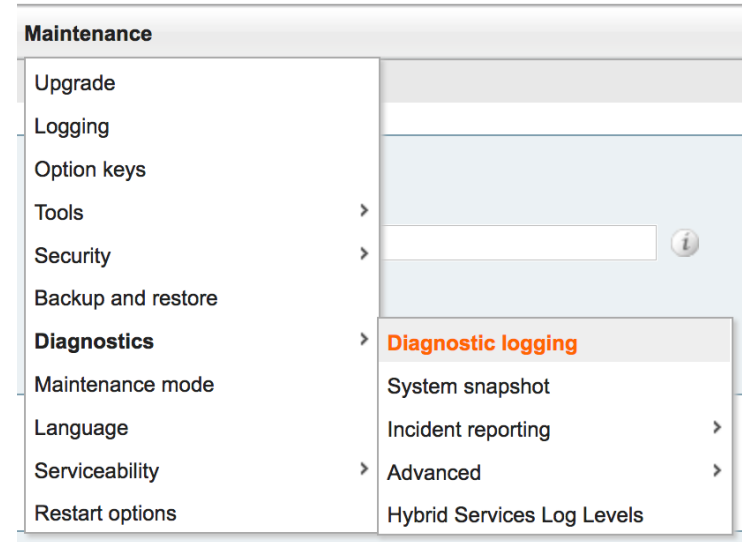
Would you like to proceed [y/n]? y

Expressway Trace Configuration



Expressway Trace Configuration

- Expressway-C / Expressway-E can log SIP messages to a diagnostic log file.
- To enable, navigate to **Maintenance > Diagnostics > Diagnostic logging**



Expressway Trace Configuration

Logging status

Started logging at

Tuesday 29th of January 2019 07:12:21 AM (US/Eastern) logging started by admin@10.82.178.191

Stopped logging at

Tuesday 29th of Ja

Marker

Add marker

Take tcpdump while logging

☒

Select this if you want to get a Wireshark capture

i

Start new log **Stop logging** **Collect log**

Log collection status

No log currently available

Click Start new log

Confirm

Any existing diagnostic log file or tcpdump will be overwritten.

OK **Cancel**

Click OK to Confirm

Expressway Trace Configuration



Success: Logging has started

Logging status

Status In progress

Started logging at Tuesday 29th of January 2019 07:12:21 AM (US/Eastern) logging started by admin@10.82.178.191

Stopped logging at

Marker

Take tcpdump while logging ☒

Log collection status

No log currently available for download.

Click Stop logging after reproducing your problem

Expressway Trace Configuration



Success: Logging has been stopped and saved

Logging status

Started logging at

Tuesday 29th of January 2019 07:12:21 AM (US/Eastern) logging started by admin@10.82.178.191

Stopped logging at

Tuesday 29th of January 2019 07:14:10 AM (US/Eastern)

Marker



Add marker

Take tcpdump while logging



Start new log

Stop logging

Collect log

Log collection status

No log currently available for download.

Click to Collect the log and
tcpdump (for Wireshark)

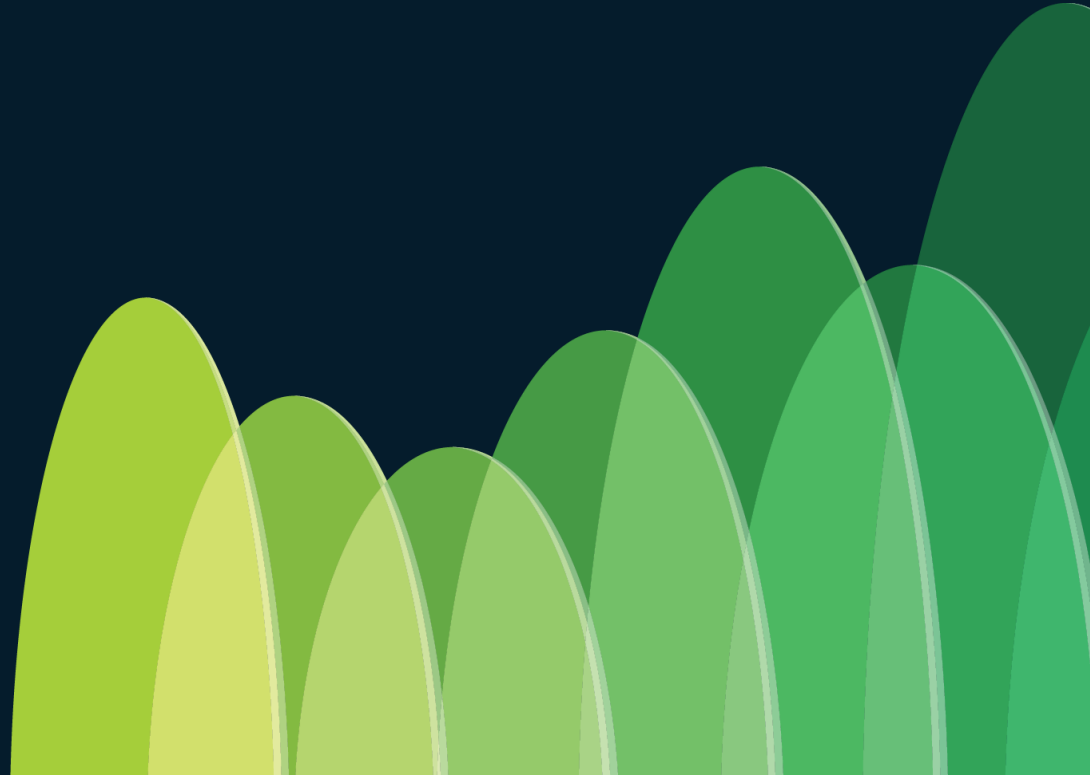
Expressway Trace Configuration

Log collection status

Download log

Click to Download the log and
tcpdump (for Wireshark)

Cisco Unified Border Element (CUBE) Trace Configuration



CUBE Debugging

- When debugging in IOS, configure logging buffered to a fairly large value (based on available memory)
- Disable logging to the console with command 'no logging console'
- Enable timestamps for debugs
- Make sure router has NTP enabled

```
service timestamps debug datetime msec localtime  
service timestamps log datetime msec localtime
```

```
logging buffered 10000000 debugging  
no logging console
```

```
clock timezone EST -5 0  
clock summer-time EDT recurring
```

```
ntp server 10.14.1.1
```

CUBE Debugging

Various SIP debugs available

CUBE#**debug ccsip ?**

all	Enable all SIP debugging traces
calls	Enable CCSIP SPI calls debugging trace
dhcp	Enable SIP-DHCP debugging trace
error	Enable SIP error debugging trace
events	Enable SIP events debugging trace
function	Enable SIP function debugging trace
info	Enable SIP info debugging trace
media	Enable SIP media debugging trace
messages	Enable CCSIP SPI messages debugging trace
non-call	Enable Non-Call-Context trace (OPTIONS, SUBSCRIBE etc)
preauth	Enable SIP preauth debugging traces
states	Enable CCSIP SPI states debugging trace
translate	Enable SIP translation debugging trace
transport	Enable SIP transport debugging traces
verbose	Enable verbose mode

CUBE VOIP Trace Feature

```
voice service voip  
trace
```

- Logs debugs for **all SIP calls automatically**
- VOIP Trace is enabled **by default** from IOS-XE 17.4.1, 17.3.2
- VOIP Trace captures:
 - SIP messages for SIP Trunk to Trunk calls
 - Events and API calls from SIP layer to other layers in CUBE
 - SIP Errors
 - Call Control (unified communication call flows processed by CUBE)
 - FSM (Finite State Machines) states and events
 - Dial peer matched
 - RTP ports allocated
- Will not log REGISTER, OPTIONS, SUBSCRIBE/NOTIFY, INFO

VOIP Trace – show commands

CUBE#**show voip trace ?**

all Display all VoIP Traces
call-id Filter traces based on Internal Call Id
correlator Filter traces based on FPI Correlator
cover-buffers Display the summary of all cover buffers
session-id Filter traces based on SIP Session ID
sip-call-id Filter traces based on SIP Call Id
statistics Display statistics for VoIP Trace

CUBE#**sh voip trace all**

Displaying 11858 cover buffers

This may severely impact system performance.

Continue? [yes/no] no



Don't do this

VOIP Trace – Cover Buffer – Search-Key

CUBE# show voip trace cover-buffers

----- Cover Buffer -----

Search-key = +19195552653:+19195550050:44669
Timestamp = Mar 17 00:16:28.136
Buffer-Id = 12
CallID = 44669
Peer-CallID = 44670
Correlator = 1
Called-Number = +19195550050
Calling-Number = +19195552653
SIP CallID = BW001626946170324-1056393246@152.188.44.31
SIP Session ID = 4b8cf36c00105000a000ac7e8ab697e8
GUID = 6E12C492AEA1
Tenant = 0
Cause-code = normal call clearing (16)

----- Cover Buffer -----

Search-key = +19195552653:+19195550050:44670
Timestamp = Mar 17 00:16:28.138
Buffer-Id = 13
CallID = 44670
Peer-CallID = 44669
Correlator = 1
Called-Number = +19195550050
Calling-Number = +19195552653
SIP CallID = 6E1360BA-E32A11EE-AEA7B1B7-8E2179A6@64.102.247.82
SIP Session ID = e59da4baa9f45d60979613901ad09af2
GUID = 6E12C492AEA1
Tenant = 0
Cause-code = normal call clearing (16)

- Each call leg is assigned a “search key”
- Search key is a combination of
Calling number, Called number and call-id

Inbound Call Leg Search-key:

+19195552653 : +19195550050 : 44669

Outbound Call Leg Search-key:

+19195552653 : +19195550050 : 44670

VOIP Trace

- To find a call, search for calling or called number
show voip trace cover-buffer | section <calling or called number>
- To view debugs for the call
show voip trace call-id <call-id>

VOIP Trace – Tip!

alias exec **fc** show voip trace cover-buffer | section
alias exec **sc** show voip trace call-id

- To find a call by calling / called number:

CUBE#**fc 9195552653**



- To show the call details based on call-id:

CUBE#**sc 44669**



CUBE# **fc 9195552653**

----- Cover Buffer -----

Search-key = +19195552653:+19195550050:44669

Timestamp = Mar 17 00:16:28.136

Buffer-Id = 12

CallID = 44669

Peer-CallID = 44670

Correlator = 1

Called-Number = +19195550050

Calling-Number = +19195552653

SIP CallID = BW001626946170324-1056393246@152

SIP Session ID = 4b8cf36c00105000a000ac7e8ab697e8

GUID = 6E12C492AEA1

Tenant = 0

Cause-code = normal call clearing (16)



CUBE – IOS-XE Embedded Traffic Capture

Export Packet Data in PCAP Format

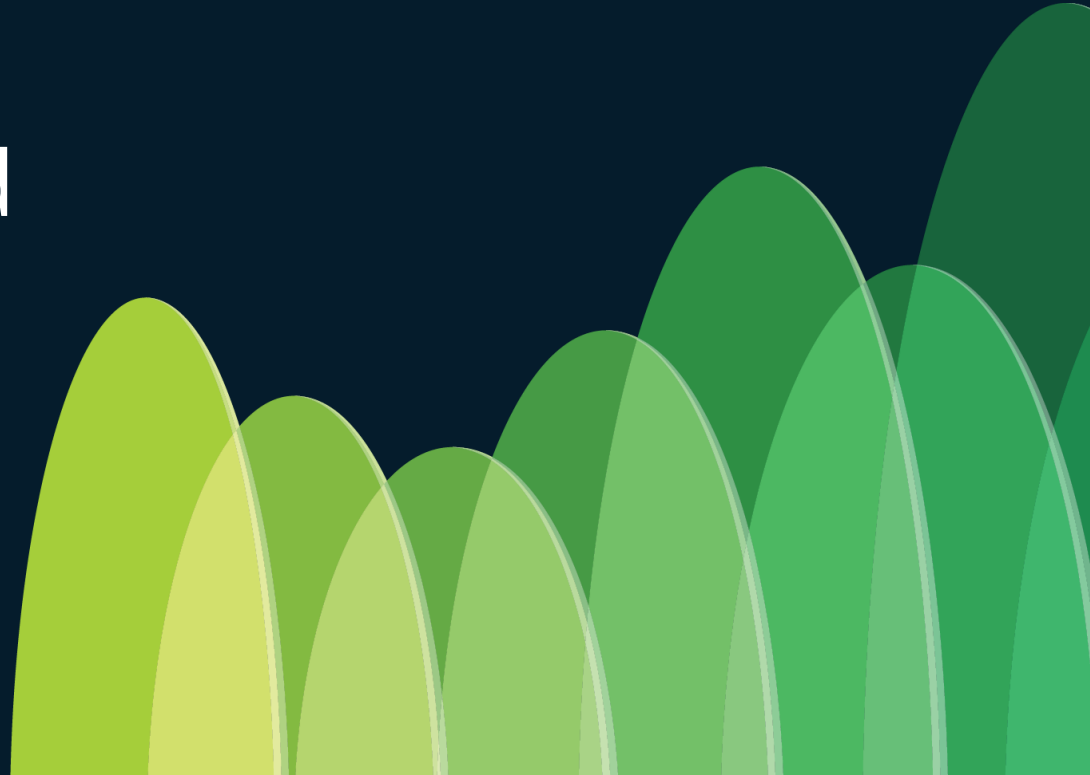
- IP Traffic Export feature allows export of packets on an interface
- Configuration (From Enable mode, not Config mode):

```
monitor capture capture-name access-list access-list-name  
monitor capture capture-name limit duration seconds  
monitor capture capture-name interface interface-name both  
monitor capture capture-name buffer circular size bytes
```

- Usage:

```
monitor capture capture-name start  
monitor capture capture-name export file-location/file-name  
monitor capture capture-name stop
```

IP Phone, Webex App, and RoomOS / Device Logging

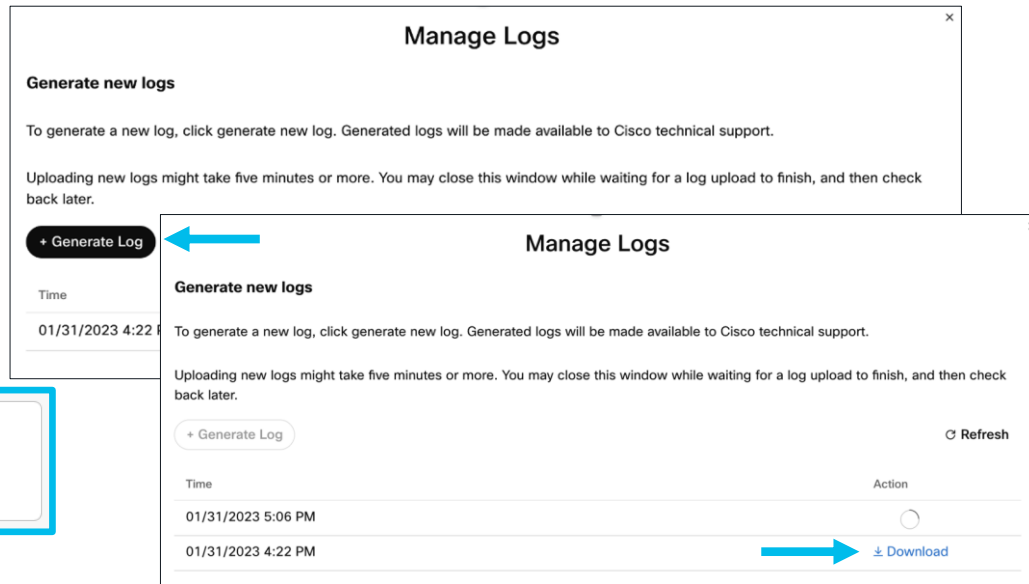
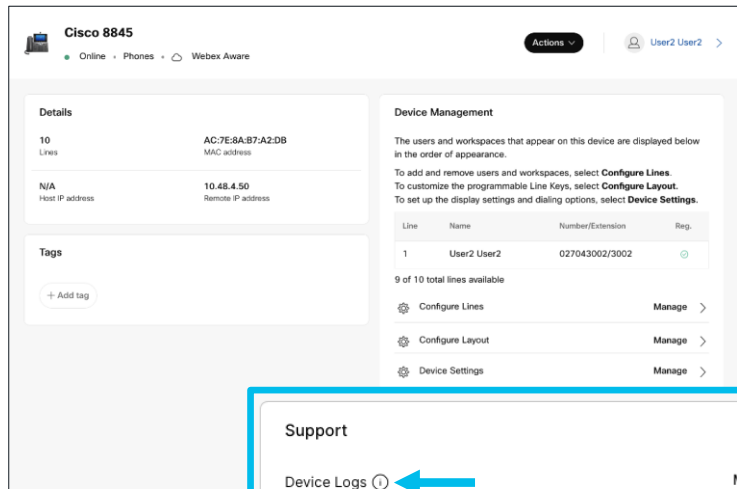


Collecting Logs from IP Phones

Problem Report Tool (PRT)

Method 1 - Generate and Collect *Obfuscated* Problem Report (PRT) from Control Hub

- Devices > Select Device > Device Logs
- From **Manage Logs** you can **Generate** and **Download** PRT logs



Collecting Logs from IP Phones

Problem Report Tool (PRT)

Method 2 – Generate *Obfuscated* Problem Report (PRT) from **Phone menu**

- Settings > Status > Report Problem > Problem description > Submit
- Uploaded PRT can be downloaded from Webex Control Hub



Report problem

Date of problem

Time of problem

Problem description

Submit

Problem description

1 Phone disconnect or reboot

2 Network connection failure

3 Phone registration failure

4 Failed to place a call

5 Cannot answer a call

Select Cancel

Collecting Logs from IP Phones

Problem Report Tool (PRT)

Method 3 – Generate and Collect PRT from Phone web menu

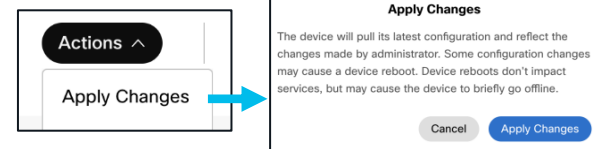
- o Enable MPP **Web Access** (User) & **Logging Level**

For 7800/8800 Cisco Phones

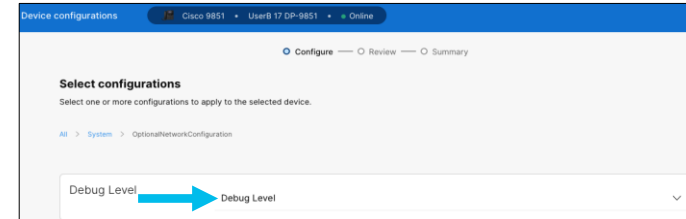
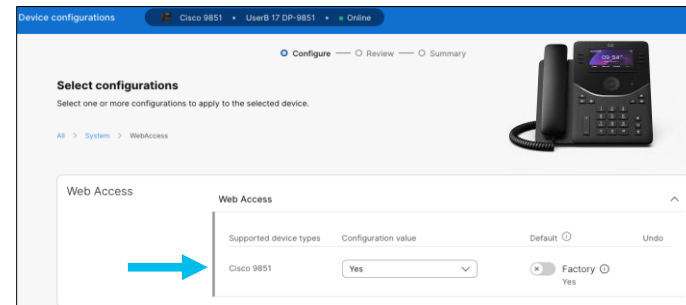
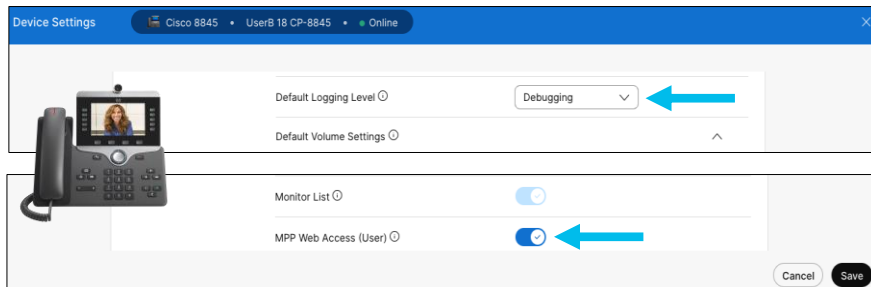
- Devices > Select Device > Device Settings
- Locations > Select Location > Calling > Device Settings
- Calling > Service Settings > Configure Default Device Settings

For 9800 Cisco Desk Phones

- Devices > Select Device > All configurations
- Devices > Template > Create template



Always Apply Changes



cisco Live!

Collecting Logs from IP Phones

Problem Report Tool (PRT)

Method 3 – Generate and Collect from Phone web menu

- Navigate to **Info** tab then **Debug Info** tab
- Click **Generate PRT & Submit**
- Download PRT

The screenshot shows the Cisco IP Phone web interface. The top navigation bar has tabs: Info, Voice, Call History, and Personal Directory. The 'Info' tab is selected. Below it, there are sub-tabs: Status, Debug Info, Download Status, and Network Statistics. The 'Debug Info' sub-tab is selected. The main content area is divided into two sections: 'Console Logs' and 'Problem Reports'. The 'Console Logs' section displays eight debug messages, each with a link to a messages file (e.g., messages, messages.0, messages.1). The 'Problem Reports' section has a 'Report Problem:' label followed by a 'Generate PRT' button and a 'Prt File:' label followed by a link to 'prt-log.tar.gz'. A blue arrow points from the 'Generate PRT' button to the right, and another blue arrow points from the 'prt-log.tar.gz' link to the bottom right.

The 'Report Problem' dialog box is shown. It contains the following fields: 'Date of problem:' with a date picker set to 01/28/2023, 'Time of problem:' with a time picker set to 02:20:56 PM, and 'Problem description:' with a dropdown menu set to 'Other'. There are 'Cancel' and 'Submit' buttons at the bottom.

The 'Problem Report Status' dialog box is shown. It contains the text: 'Your data has been uploaded successfully. File: prt-log.tar.gz'. There is an 'OK' button at the bottom.

Click link to download [prt.log.tar.gz](#)

Collecting Logs from IP Phones

Problem Report Tool (PRT)

✓  prt-4b43cc26-0a2f-4b3c-937b-5ffb2e8d9abc	
 cfg.xml	 Phone Configuration File
 description-20240508-142222.log	 PRT Timestamp, Firmware and Phone Description
 logcat-20240508-192226.log	 Latest Messages log
 lyra_config.xml	 Device Settings (<i>9800 Phones only</i>)
 messages.tar.gz	 Latest Messages log (same as logcat)
 net.cfg	 Phone Network Information
 show-output-20240508-142222.log	 CPU, Sockets, WLAN, etc.
 status.xml	 Phone Info and Stats
 usrlog_kernel_cur_boot.log	 Kernel Information Current boot
 usrlog_kernel_prev_boot.log	 Kernel Information Previous boot
 webex_service_status.json	 Cloud Awareness and Features Status
 wxc_internal_param.cfg	 Webex User Information
 archive.tar.gz	 Historical Messages Logs
 backtraces.tar.gz	 Crash Log / OS Logging
>  cert	 Certificates

Collecting Packet Capture from IP Phones

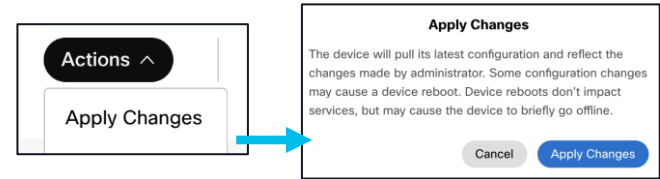
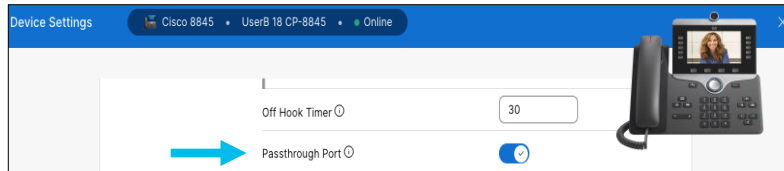
Enable PC Passthrough Port from Control Hub

For Cisco Phones

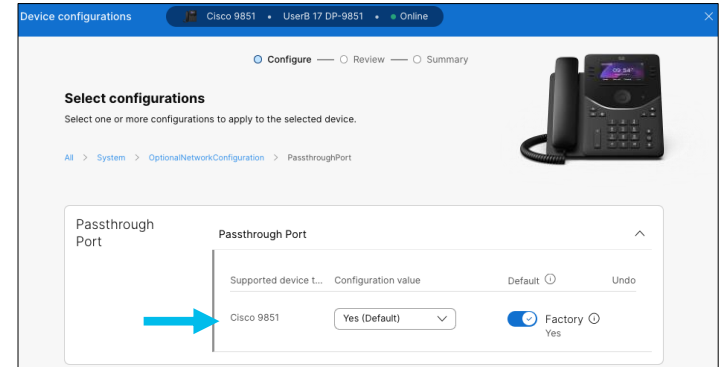
- Devices > Select Device > Device Settings

For new 9800 Cisco Desk Phones

- Devices > Select Device > All configurations



Always Apply Changes



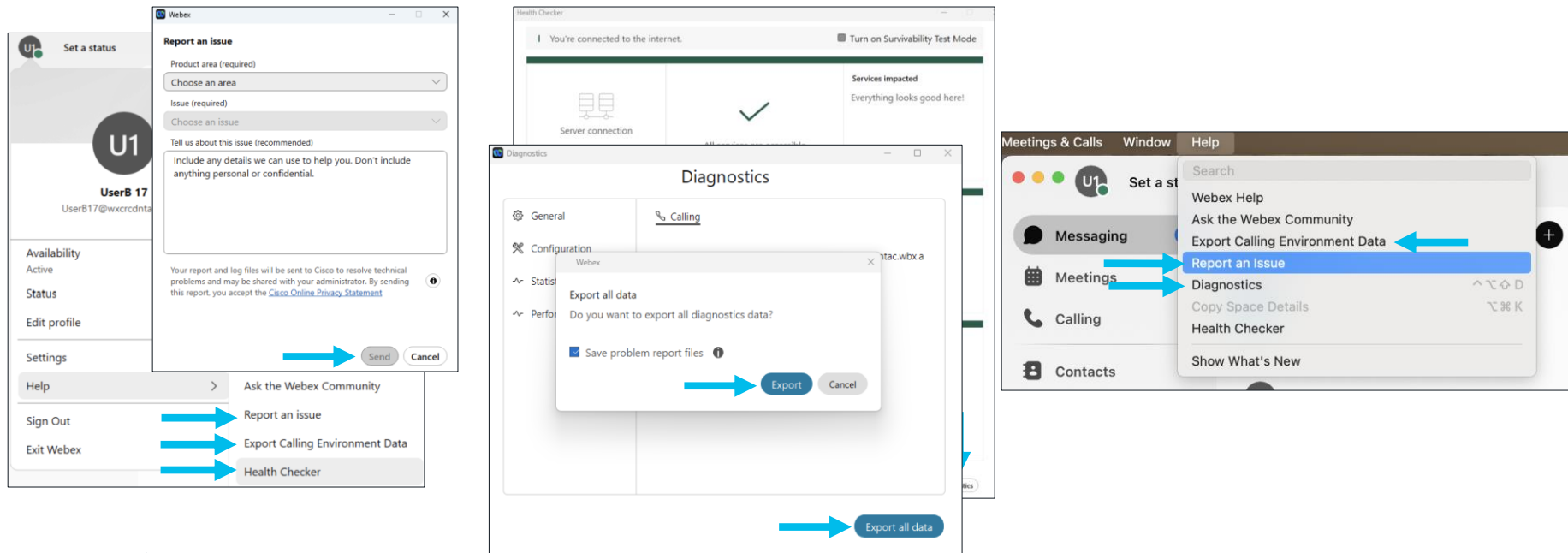
Collecting Logs from Webex App

Location of log files for Webex Application

1. Windows: %USERPROFILE%\AppData\Local\CiscoSpark
2. MacOS: ~/Library/Logs/SparkMacDesktop

Method 1 – Generate and Collect *Obfuscated* logs from Webex App

- Navigate to Help > Report an Issue & Calling Environment
- Help > Health Checker > Diagnostics > Export all data (Includes Calling Environment)



Collecting Logs from Webex App

Method 2 – Generate and Collect *Obfuscated* logs from Control Hub

- Navigate to **Troubleshooting** > **Logs** > search for **UserB17@wxcrcdntac.wbx.ai**
- **Calling Environment Data** needs to be downloaded from the App

The screenshot shows the Webex Control Hub interface. On the left, the 'Troubleshooting' menu item is highlighted. In the main area, the 'Logs' tab is selected. A search bar contains the text 'UserB17@wxcrcdntac.wbx.ai'. Below the search bar, the date range is set to 'Apr 12, 2024' to 'Apr 19, 2024', and the time zone is '(GMT -05:00) America/Chicago'. A table displays two log entries for 'UserB17@...'. A 'Collect logs' button is visible in the top right corner of the table. A dialog box titled 'Collect logs?' is open on the right, providing instructions on how to collect logs and a 'Collect' button.

Collect logs?

You're collecting **UserB17@wxcrcdntac.wbx.ai**'s latest client logs.

Please check back in few hours to see if the logs were uploaded. If not please try again or ask user to send logs from the webex client.

This user must have an active internet connection while running their Webex app. Collecting logs take extra time and bandwidth, and can impact this user's Webex connection.

Date	User logs	Email Address	Call start time	Feedback ID	Correlation ID	Locus ID	User agent	Metadata
Apr 19, 2024 3:28:35 PM	Download	UserB17@...	-	9aa8d262-...	-	-	sparkmac/...	View
Apr 19, 2024 3:25:56 PM	Download	UserB17@...	-	e6b6409d...	-	-	sparkmac/...	View

Calling Environment Data

From current_log.txt

```
REGISTER sip:98027369.us10.bcl.d.webex.com SIP/2.0
Via: SIP/2.0/TLS {!9f15ed7865f56151!};55486;branch=z9hG4bKf7bcd2fb8a625947;alias;rport
Max-Forwards: 70
To: sip:{!78a08c89abe884c3!}@{!3f29207b5c1fdb70!}
From:
sip:{!78a08c89abe884c3!}@{!3f29207b5c1fdb70!};tag=0399a3bdc7fb55d1ebdd4d59984bec77
CSeq: 340389365 REGISTER
```

"78a08c89abe884c3": "asaweeusz8_G80CS6Z7XSBL",

Calling-environment-data.dat

```
"3f29207b5c1fdb70": "98027369.us10.bcl.d.webex.com",
"3fad57e49b2ca43a" : "<sip:asaweeusz8_G80CS6Z7XSBL@192.168.50.248:8933;transport=tls>;q=1.0",
"78a08c89abe884c3" : "asaweeusz8_G80CS6Z7XSBL",
"834484e4a0608d8a" : "UserB 17",
"9f15ed7865f56151" : "192.168.50.248",
"a281b427a997a4eb" : "asaweeusz8_G80CS6Z7XSBL@98027369.us10.bcl.d.webex.com",
```

Collecting Logs from Webex App

✓  27be7fee-edb2-4cc9-8cc2-c0344a6b7667	
>  accessories	 Accessories Log Folder
>  attachments	
>  bwc	 Webex Calling Log Folder
>  callLogs	
 current_log.txt	 General Webex App Logs
>  logArchive	
>  media	 Media Engine Log Folder
>  meetings	 Meetings Log Folder
>  mercury	
>  restarter	
>  uclgin	 UCM Log Folder
 HelperLog.log	
 StartupLog.log	
 FinderLog.log	
 last_run_current_log.txt	 Previous Current Log
 last_run_current_log_header.txt	
 last_run_current_log1.txt	

Collecting Logs from Room Devices

Method 1 – Generate *Obfuscated* Logs from Control Hub

- Devices > Select Device > Device Logs
- From Manage Logs you can **Generate** and **Download** the logs

The screenshot shows the Cisco Desk Mini interface. The top bar includes the Cisco logo, 'Cisco Desk Mini', status 'Online - Rooms & Desks', an 'Actions' dropdown, and a user profile 'UserC 21'. The main content area is divided into 'Overview' and 'History' tabs. Under 'Overview', there are sections for 'Details' (Wired network connectivity, IP address 192.168.50.41, MAC address 4C:42:1E:CC:1B:D1, Serial number FOC2701NT1J, UserC21@wxcrdntac-sbx.calls.webex.com, SIP address userc_21_desk_mini@wxcrdntac-sbx.rooms.webex.com, 6021 Lines), 'Issues & Information' (Everything is looking fine), 'Configurations' (All configurations, Configuration templates, Digital signage, Navigator persistent web app), 'Software' (Cisco Platform, Stable Channel, RoomOS April 2024 Release, RoomOS 11.15.1.6 Version), and 'Alerts' (New). A 'Support' modal is open, showing 'Device Logs' (with a blue arrow pointing to it), 'Local Device Controls', and 'Cisco Support'. The 'Device Logs' section has a 'Manage' link.

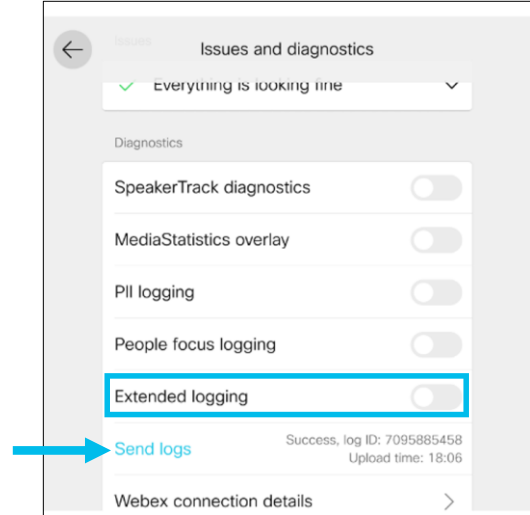
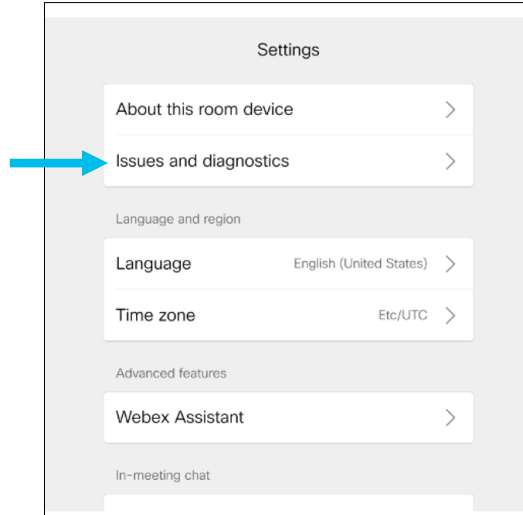
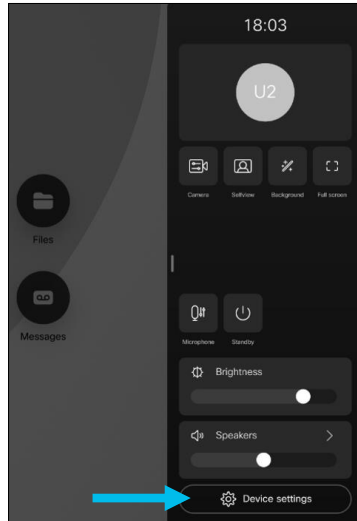
The screenshot shows the 'Manage Logs' interface. It has a title 'Manage Logs' and a section 'Generate new logs'. Below this, there is a paragraph explaining that logs generated by the Cisco Webex Cloud are also made available to the Cisco technical support organization. Another paragraph states that uploading new logs might take five minutes or more. There is a '+ Generate Log' button (with a blue arrow pointing to it) and a dropdown menu set to 'All Logs' with a 'Refresh' button. Below this is a table of logs:

Time	Type	Feedback ID	Action
04/29/2024 1:06 PM	Full Log	7095885458	Download
04/29/2024 12:54 PM	Full Log	356cdfd-a873-b5de-9083-2c8a89726612	Download (with a blue arrow pointing to it)
04/29/2024 12:33 PM	Full Log	71f49106-4f49-c1fd-3402-3c965261798e	Download
04/29/2024 12:31 PM	Full Log	3375e50b-21ea-8ef0-adf0-bd04e53e843a	Download

Collecting Logs from Room Devices

Method 2 – Generate *Obfuscated* Logs from Device Menu

- Swipe right to left > Device Settings
- Issues and diagnostics send logs
- Optional: Extended Logging (Verbose Logs)



Collecting Logs from Room Devices

Method 3 – Generate and Collect Device Logs from Device web menu

- Device > Local Device Controls > Proceed
- Issues and Diagnostics > System Logs > System logs / Extended Logging

