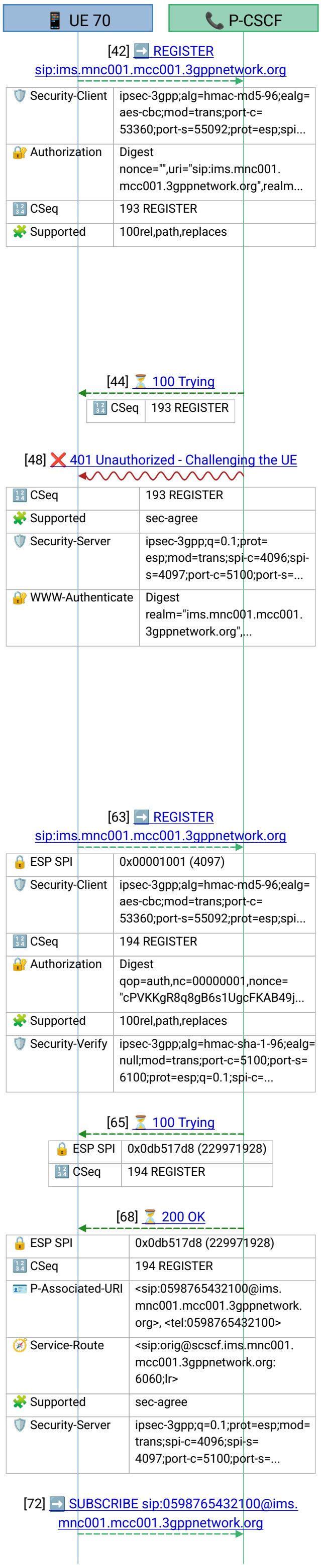


[Frame 42] Phase 1: register and agree on IPsec. UE 70, an iPhone (`User-Agent: iOS/14.4.2`), registers with IMS. No security exists yet, so this REGISTER travels in the clear, over TCP from port 49294 to the P-CSCF's port 5060. It is 1,609 bytes, sent in two TCP segments.

It names the subscriber by its private identity, `001011234567895@ims.mnc001.mcc001.3gppnetwork.org`, built from the IMSI. The `Authorization` header is a placeholder with an empty nonce and response: it only tells the network which identity to challenge.

`Require: sec-agree` asks for the RFC 3329 security agreement. `Security-Client` offers four IPsec suites: `hmac-md5-96` or `hmac-sha-1-96` integrity, each with `aes-cbc` or `null` encryption. Every offer carries the same ports and SPIs the UE has picked: protected client port 53360, protected server port 55092, `spi-c` 229971928 and `spi-s` 173156976.

[Frame 44] The P-CSCF acknowledges the REGISTER at once (`Server: TelcoSuite Proxy-CSCF`), 3 ms later. A 100 Trying only stops the sender from retransmitting; it is never forwarded.

[Frame 48] The IMS-AKA challenge. The S-CSCF (`Server: Kamailio S-CSCF`) rejects the first REGISTER, as the procedure intends, 25 ms after it was sent.

`WWW-Authenticate` uses `algorithm=AKAv1-MD5` (RFC 3310). Its nonce is base64 for 32 bytes: the 16-byte RAND and the 16-byte AUTN of an AKA challenge, the same challenge-response used for network attach. The SIM's ISIM or USIM application checks AUTN to authenticate the network, computes the response `RES`, and derives the keys `CK` and `IK`. Under TS 33.203 the S-CSCF passes the same keys to the P-CSCF inside this 401, and the P-CSCF removes them before forwarding it.

`Security-Server` is the P-CSCF's choice: `hmac-sha-1-96` with `ealg=null`, the fourth of the UE's offers. It adds the P-CSCF's own ports (client 5100, server 6100) and SPIs (`spi-c` 4096, `spi-s` 4097). With both halves known, each side can build four IPsec security associations (SAs), keyed with `IK`. Null encryption means SIP is integrity-protected but readable.

[Frame 63] The protected REGISTER. 335 ms after the 401, and after closing the first TCP connection, UE 70 sends REGISTER again. This time it goes inside ESP, from client port 53360 to the P-CSCF's server port 6100.

The ESP SPI is 4097, the `spi-s` the P-CSCF chose in frame 48. An SPI is always picked by the receiver, so it can find the right SA for each incoming packet.

`Authorization` now carries the answer: the same nonce, `qop=auth`, `nc=00000001`, and a digest `response` computed with RES as the password. `Security-Client` repeats the four offers unchanged. `Security-Verify` echoes the P-CSCF's `Security-Server` back. Both are checks against a man in the middle: had anyone edited the unprotected first exchange, the copies would not match.

[Frame 65] The P-CSCF's 100 Trying uses SPI 0x0db517d8 = 229971928, the `spi-c` UE 70 offered in frame 42. Responses come back on the TCP connection that carried the request, from port 6100 to 53360.

[Frame 68] Registered. The `200 OK` arrives 21 ms after the protected REGISTER. UE 70 is registered with IMS 2.25 s into the capture.

`P-Associated-URI` gives the public identities the UE may now use: `sip:0598765432100@ims.mnc001.mcc001.3gppnetwork.org` and `tel:0598765432100`. `Service-Route` names the S-CSCF (`orig@scscf...:6060`) that the UE must route its future requests through. `Security-Server` repeats the agreement.

[Frame 72] Phase 2: subscribe to its own registration state. UE 70 subscribes to the `reg` event package (RFC 3680) for its public identity, so the network can tell it if the registration

UE 70 | P-CSCF | Media relay | UE 71

ESP SPI	0x00001001 (4097)
Event	reg
CSeq	1 SUBSCRIBE
P-Preferred-Identity	sip:0598765432100@ims.mnc001.mcc001.3gppnetwork.org
Supported	100rel,path,replaces
Security-Verify	ipsec-3gpp;alg=hmac-sha-1-96;ealg=null;mod=trans;port-c=5100;port-s=6100;prot=esp;...

[74] 200 Subscription to REG saved

ESP SPI	0x0a522a70 (173156976)
CSeq	1 SUBSCRIBE

[78] NOTIFY sip:192.168.101.2:55092;alias=192.168.101.2~53360~1

ESP SPI	0x0a522a70 (173156976)
CSeq	4 NOTIFY
Event	reg
Subscription-State	active;expires=600000

[81] 200 OK

ESP SPI	0x00001000 (4096)
CSeq	4 NOTIFY
Supported	100rel,path,replaces

[821] INVITE tel:0698765432100;phone-context=ims.mnc001.mcc001.3gppnetwork.org

ESP SPI	0x00001001 (4097)
Supported	100-re-l,-...
CSeq	1 INVITE
P-Preferred-Identity	sip:0598765432100@ims.mnc001.mcc001.3gppnetwork.org
Security-Verify	ipsec-3gpp;alg=hmac-sha-1-96;ealg=null;mod=trans;port-c=5100;port-s=6100;prot=esp;...
SDP c	IN IP4 192.168.101.2
SDP m	audio 49120 RTP/AVP 116 99 97 105 100
Codec	116 EVS/16000
Codec	99 AMR-WB/16000
Codec	97 AMR/8000
Direction	inactive
QoS	des:qos mandatory local sendrecv
QoS	curr:qos local none
QoS	des:qos optional remote sendrecv
QoS	curr:qos remote none

[823] 100 Trying

ESP SPI	0x0db517d8 (229971928)
CSeq	1 INVITE

[827] INVITE sip:38523e65-de33-40ea-a65d-152b5632a32c@192.168.101.3:42027

ESP SPI	0xef2fb333 (4012880691)
Supported	100rel,path,precondition,replaces,timer
CSeq	1 INVITE
P-Asserted-Identity	<sip:0598765432100@ims.mnc001.mcc001.3gppnetwork.org>
SDP c	IN IP4 172.22.0.16
SDP m	audio 49000 RTP/AVP 116 99 97 105 100
QoS	des:qos mandatory local sendrecv

is ended or changed.

This request goes over UDP, still from port 53360 to 6100 under SPI 4097. It is 1,084 bytes. RFC 3261 sends a request over TCP when it is larger than 1,300 bytes (with no path MTU known), and UE 70 follows that rule throughout. The same frame carries a TCP FIN that closes the connection used for the protected REGISTER.

From here every request carries `Security-Verify`, and `P-Preferred-Identity` names the public identity the UE wants to appear as.

[Frame 74] The 200 OK to the SUBSCRIBE comes back over UDP, from the P-CSCF's client port 5100 to UE 70's server port 55092, under SPI 0x0a522a70 = 173156976, UE 70's `spi-s`. The request's `Via` names port 55092, and the response goes there.

[Frame 78] The S-CSCF's first `NOTIFY` (`Subscription-State: active`) carries a 1,173-byte `application/reginfo+xml` body listing both public identities as active. At 1,877 bytes it is too big for UDP, so the P-CSCF opens a TCP connection to UE 70's server port 55092 (SYN in frame 75) and sends it from port 5100. SPI 0x0a522a70 again: this is the SA into the UE's server port.

[Frame 81] UE 70 answers on the same TCP connection, from port 55092 to 5100, under SPI 4096, the P-CSCF's `spi-c`.

All four SAs are now in use. Into the P-CSCF: 53360 -> 6100 (SPI 4097) and 55092 -> 5100 (SPI 4096). Into UE 70: 6100 -> 53360 (SPI 229971928) and 5100 -> 55092 (SPI 173156976).

[Frame 821] Phase 3: the call. 21 s later, UE 70 calls `tel:0698765432100`, UE 71's number. The INVITE is 2,187 bytes, over a new TCP connection from 53360 to 6100 (SYN in frame 814). On the radio it took four RLC PDUs, frames 817-821.

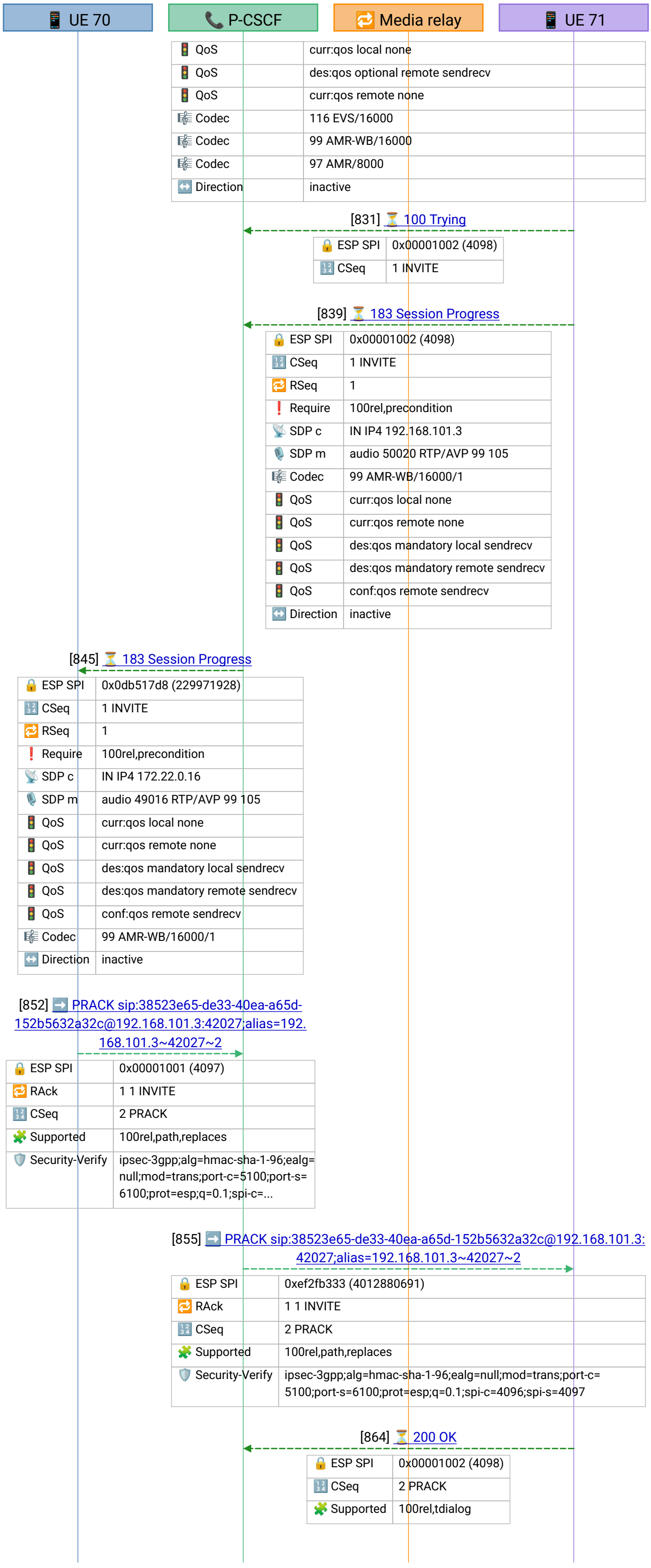
`Supported` lists `precondition` and `100rel`. The SDP offer, from `c=IN IP4 192.168.101.2` port 49120, lists EVS, AMR-WB and AMR (payload types 116, 99, 97), plus two telephone-event types.

The media is `a=inactive`, and the QoS precondition lines (RFC 3312) say why. UE 70 requires its own (local) resources in both directions (`des:qos mandatory local sendrecv`) and has none yet (`curr:qos local none`). The remote end's preconditions are `optional`, and its state is also `none`. Nothing may ring until the mandatory preconditions are met.

[Frame 823] The P-CSCF's 100 Trying, 1.7 ms after the INVITE. It is a hop-by-hop acknowledgment only.

[Frame 827] The same INVITE, 23 ms later, delivered to UE 71. In between it went through the IMS core: the `Via` headers show P-CSCF -> S-CSCF (172.22.0.20:6060) -> a node at 172.22.0.19:4060, most likely the I-CSCF that finds the callee's S-CSCF -> the same S-CSCF, now serving UE 71 -> the P-CSCF's port 5101. `Max-Forwards` has dropped from 70 to 65.

Three changes matter. The P-CSCF replaced `P-Preferred-Identity` with `P-Asserted-Identity`, which the network vouches for. The `Security-Verify` and `sec-agree` tags are gone. And the SDP now says `c=IN IP4 172.22.0.16` port 49000: the P-CSCF has rewritten the offer so UE 71 sends its media to a relay, not to UE 70.



The ESP SPI is 0xef2fb333, the `spi-s` UE 71 chose at its own registration, and the packet goes from port 5101 to UE 71's server port 42027.

[Frame 831] UE 71 acknowledges with its own 100 Trying, under SPI 4098: UE 71 has its own SA set with the P-CSCF (ports 5101 and 6101, SPIs 4098 and 4099).

[Frame 839] The answer: AMR-WB. 92 ms after the INVITE reached it, UE 71 (`User-Agent: xiaomi_Mi A2 Lite`) answers `183 Session Progress`. `Require: 100rel, precondition` and `RSeq: 1` make it a reliable provisional response (RFC 3262): UE 71 will retransmit it until a PRACK arrives.

The SDP keeps only `99 AMR-WB/16000/1` (plus telephone-event), at `c=IN IP4 192.168.101.3` port 50020. EVS and AMR are dropped.

The precondition lines move on. UE 71 upgrades the remote preconditions from optional to `mandatory`, and `conf:qos remote sendrecv` asks UE 70 to report when its resources are ready. Both ends are still `none`, so the media stays `inactive`.

This answer settles the codec and the ports. 8 ms later, in radio frame 844, the eNB sends UE 71 an RRC Connection Reconfiguration with its QCI 1 voice bearer.

[Frame 845] The 183 reaches UE 70, 129 ms after its INVITE. Its SDP has been rewritten the other way: `c=IN IP4 172.22.0.16` port 49016. Each phone now believes the other is at the relay, on a different port.

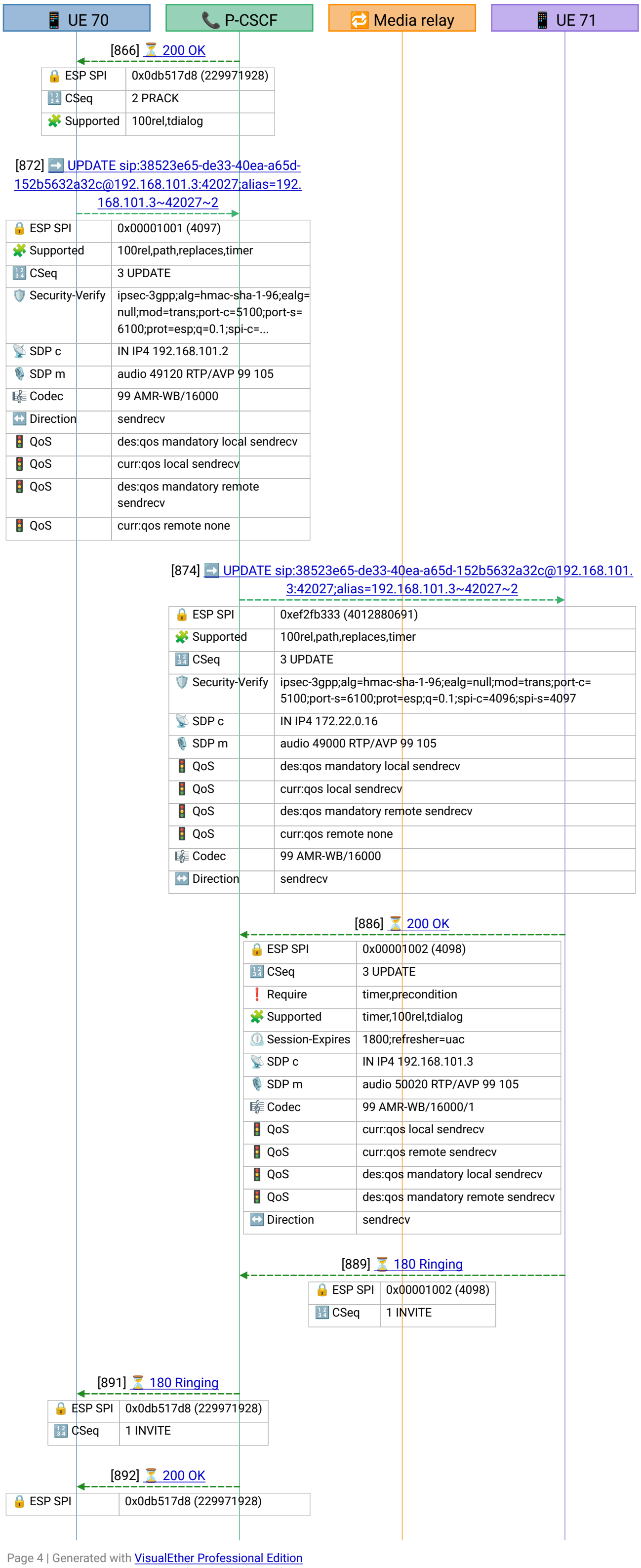
0.8 ms later, in radio frame 846, UE 70 receives its own QCI 1 bearer: EPS bearer 7 on DRB 3. It accepts it in frame 847.

[Frame 852] PRACK acknowledges the reliable 183: `RAck: 1 1 INVITE` names RSeq 1 of CSeq 1 INVITE. It is 1,528 bytes, so it goes over TCP, in three RLC PDUs. Like every request in this dialog it carries a `Route` set built from the `Record-Route` headers, so it follows the proxies that recorded themselves.

[Frame 855] The PRACK delivered to UE 71. It is an in-dialog request, so its `Via` path skips the node at 172.22.0.19: it goes P-CSCF -> S-CSCF -> P-CSCF only.

This time the P-CSCF leaves UE 70's `Security-Verify` and `Require: sec-agree` in. They mean nothing to UE 71, which ignores them. The same happens on the UPDATE, the ACK and the BYE.

[Frame 864] UE 71's 200 OK to the PRACK. It ends the PRACK transaction. The INVITE transaction is still open.



[Frame 866] The PRACK's 200 OK reaches UE 70.

[Frame 872] Preconditions: UE 70 is ready. UE 70's voice bearer has existed since frame 846, so it sends UPDATE (RFC 3311) with a new offer: `curr:qos local sendrecv`. The remote end is still `none`, as far as UE 70 knows.

The offer narrows the codecs to AMR-WB, changes the media from `inactive` to `sendrecv`, and adds `Require: precondition`. It also sets the RTCP bandwidth to zero (`b=RS:0`, `b=RR:0`, RFC 3556). UE 71's answer does the same, and the capture holds no RTCP at all.

[Frame 874] The UPDATE reaches UE 71, with c= rewritten to the relay's port 49000 as before.

[Frame 886] All preconditions met. UE 71's 200 OK to the UPDATE reports both ends ready: `curr:qos local sendrecv` and `curr:qos remote sendrecv`. Its own bearer has existed since radio frame 844.

It also adds a session timer (RFC 4028): `Session-Expires: 1800;refresher=uac`, so UE 70, the side that sent the request, must refresh the session before 1,800 s run out.

[Frame 889] Only now does UE 71 ring. The `180 Ringing` leaves 1.9 ms after the 200 OK to the UPDATE. This is the point of preconditions: the callee alerts its user only once a voice bearer exists at both ends.

The 180 has no `RSeq`, so it is not reliable and draws no PRACK.

[Frame 891] The 180 reaches UE 70, 360 ms after it dialed. It arrives 1.2 ms before the 200 OK to the UPDATE, the reverse of the order UE 71 sent them. They belong to different transactions, so the order doesn't matter.

[Frame 892] The UPDATE's 200 OK reaches UE 70, rewritten to the relay at port 49016. Both phones now agree: AMR-WB, `sendrecv`, every precondition met.

UE 70	P-CSCF	Media relay	UE 71

CSeq	3 UPDATE
Require	timer,precondition
Supported	timer,100rel,tdialog
Session-Expires	1800;refresher=uac
SDP c	IN IP4 172.22.0.16
SDP m	audio 49016 RTP/AVP 99 105
QoS	curr:qos local sendrecv
QoS	curr:qos remote sendrecv
QoS	des:qos mandatory local sendrecv
QoS	des:qos mandatory remote sendrecv
Codec	99 AMR-WB/16000/1
Direction	sendrecv

[973] 200 OK

ESP SPI	0x00001002 (4098)
CSeq	1 INVITE
Supported	timer,100rel,tdialog
Session-Expires	1800;refresher=uac
Require	timer

[Frame 973] Answered. UE 71's user picks up 1.64 s after the 180: `200 OK` to the INVITE. It carries no SDP; the offer/answer was finished by the 183 and the UPDATE. `Require: timer` repeats the session timer.

[976] 200 OK

ESP SPI	0x0db517d8 (229971928)
CSeq	1 INVITE
Supported	timer,100rel,tdialog
Session-Expires	1800;refresher=uac
Require	timer

[Frame 976] The 200 OK reaches UE 70, 2.0 s after the INVITE left it.

[981] ACK sip:38523e65-de33-40ea-a65d-152b5632a32c@192.168.101.3:42027;alias=192.168.101.3~42027~2

ESP SPI	0x00001001 (4097)
CSeq	1 ACK
Supported	100rel,path,replaces
Security-Verify	ipsec-3gpp;alg=hmac-sha-1-96;ealg=null;mod=trans;port-c=5100;port-s=6100;prot=esp;q=0.1;spi-c=...

[Frame 981] UE 70's ACK completes the three-way INVITE handshake, 32 ms after the 200 OK. ACK is its own request, with CSeq: 1 ACK, and it gets no response.

[983] ACK sip:38523e65-de33-40ea-a65d-152b5632a32c@192.168.101.3:42027;alias=192.168.101.3~42027~2

ESP SPI	0xef2fb333 (4012880691)
CSeq	1 ACK
Supported	100rel,path,replaces
Security-Verify	ipsec-3gpp;alg=hmac-sha-1-96;ealg=null;mod=trans;port-c=5100;port-s=6100;prot=esp;q=0.1;spi-c=4096;spi-s=4097

[Frame 983] The ACK reaches UE 71. The dialog is confirmed.

[985] RTP

UDP src port	49120
UDP dst port	49016
Marker	True
PT	AMR-WB (99)
Seq	1
SSRC	0x3dc765fd (1036477949)

[Frame 985] Phase 4: media through the relay. UE 70's first RTP packet, 31 ms after its ACK: AMR-WB (payload type 99), sequence 1, marker bit set for the start of a talk spurt. It goes from port 49120 to 172.22.0.16 port 49016, exactly where the rewritten 183 told it to send. It rides DRB 3, the voice bearer, not DRB 2.

[986] RTP

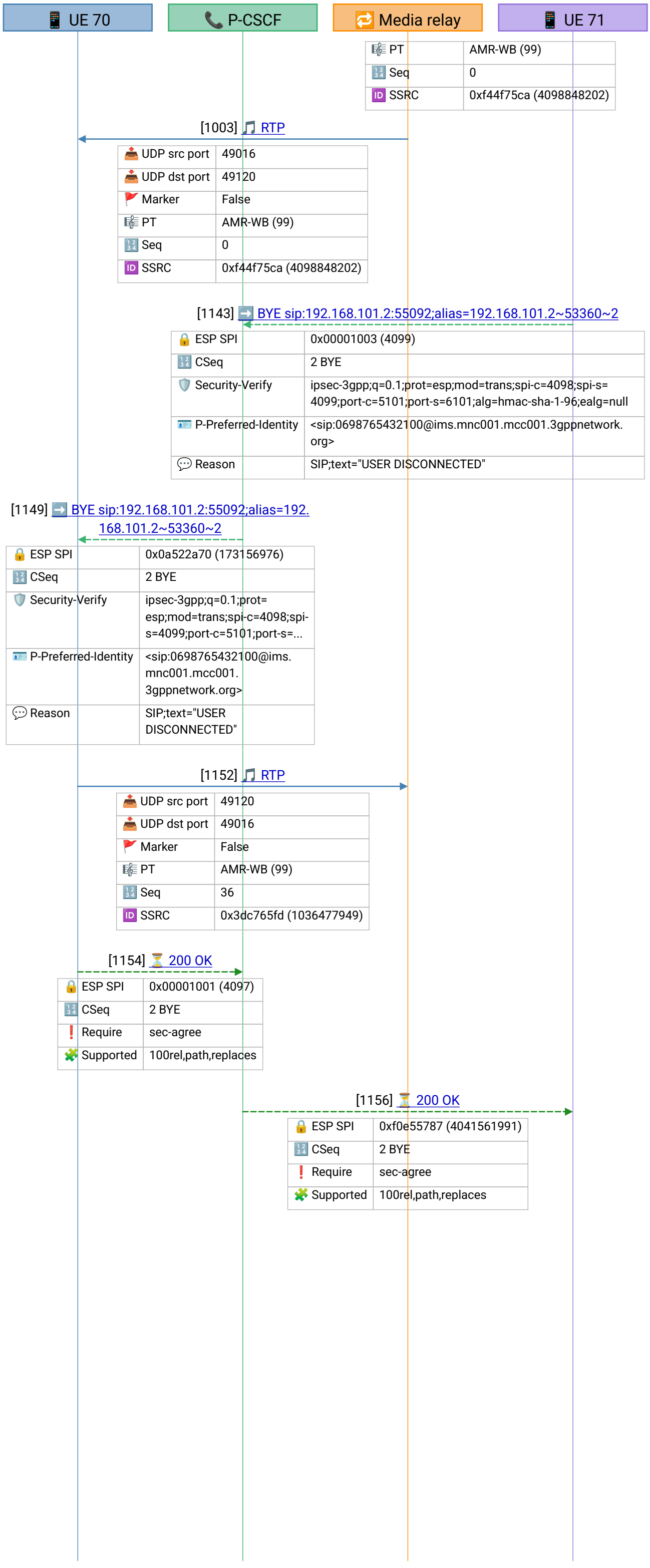
UDP src port	49000
UDP dst port	50020
Marker	True
PT	AMR-WB (99)
Seq	1
SSRC	0x3dc765fd (1036477949)

[Frame 986] 0.7 ms later the relay sends the same packet on to UE 71, from its port 49000 to UE 71's port 50020. The SSRC (0x3dc765fd) and sequence number are unchanged. Only the addresses and ports differ.

[1002] RTP

UDP src port	50020
UDP dst port	49000
Marker	False

[Frame 1002] UE 71's first RTP packet, sequence 0, from port 50020 to the relay's port 49000: the address in the rewritten INVITE. UE 71 doesn't set the marker bit on it.



[Frame 1003] The relay forwards it from port 49016 to UE 70's port 49120, 0.7 ms later. Each phone sends to and receives from the same relay port (symmetric RTP), and neither ever sees the other's address.

[Frame 1143] Phase 5: hang-up. 4.5 s after the 200 OK, UE 71 hangs up: BYE with `Reason: SIP;text="USER DISCONNECTED"`. It goes over TCP from UE 71's client port 42608 to the P-CSCF's server port 6101, under SPI 4099.

9.4 ms later, in radio frame 1146, the eNB is already removing UE 70's voice bearer, 20 ms before the BYE reaches UE 70.

[Frame 1149] The BYE reaches UE 70. It is 1,207 bytes, so the P-CSCF sends it over UDP, from its client port 5100 to UE 70's server port 55092, under SPI 0x0a522a70. UE 70's voice bearer was released in radio frame 1146 and UE 71's in frame 1147.

[Frame 1152] A voice packet after the bearer is gone. RTP sequence 36, a comfort-noise frame, still from port 49120 to the relay's port 49016. The BYE arrived 19 ms earlier, but UE 70's codec is still running. With DRB 3 removed, the packet no longer matches a voice packet filter and falls through to the IMS default bearer: it rides DRB 2, the SIP bearer.

[Frame 1154] UE 70's 200 OK to the BYE, 28 ms after the BYE arrived. It goes over UDP from UE 70's client port 53360 to the P-CSCF's server port 6100, under SPI 4097. That is the SA UE 70 uses for its own requests, not the reverse of the path the BYE came in on (the BYE's top `Via` names port 5100). The P-CSCF accepts it.

[Frame 1156] The 200 OK reaches UE 71, over its TCP connection from port 6101 to 42608, under SPI 0xf0e55787, UE 71's `spi-c`. Call 1 is over, 6.6 s after UE 70 dialed. Both phones stay registered for the five calls that follow.