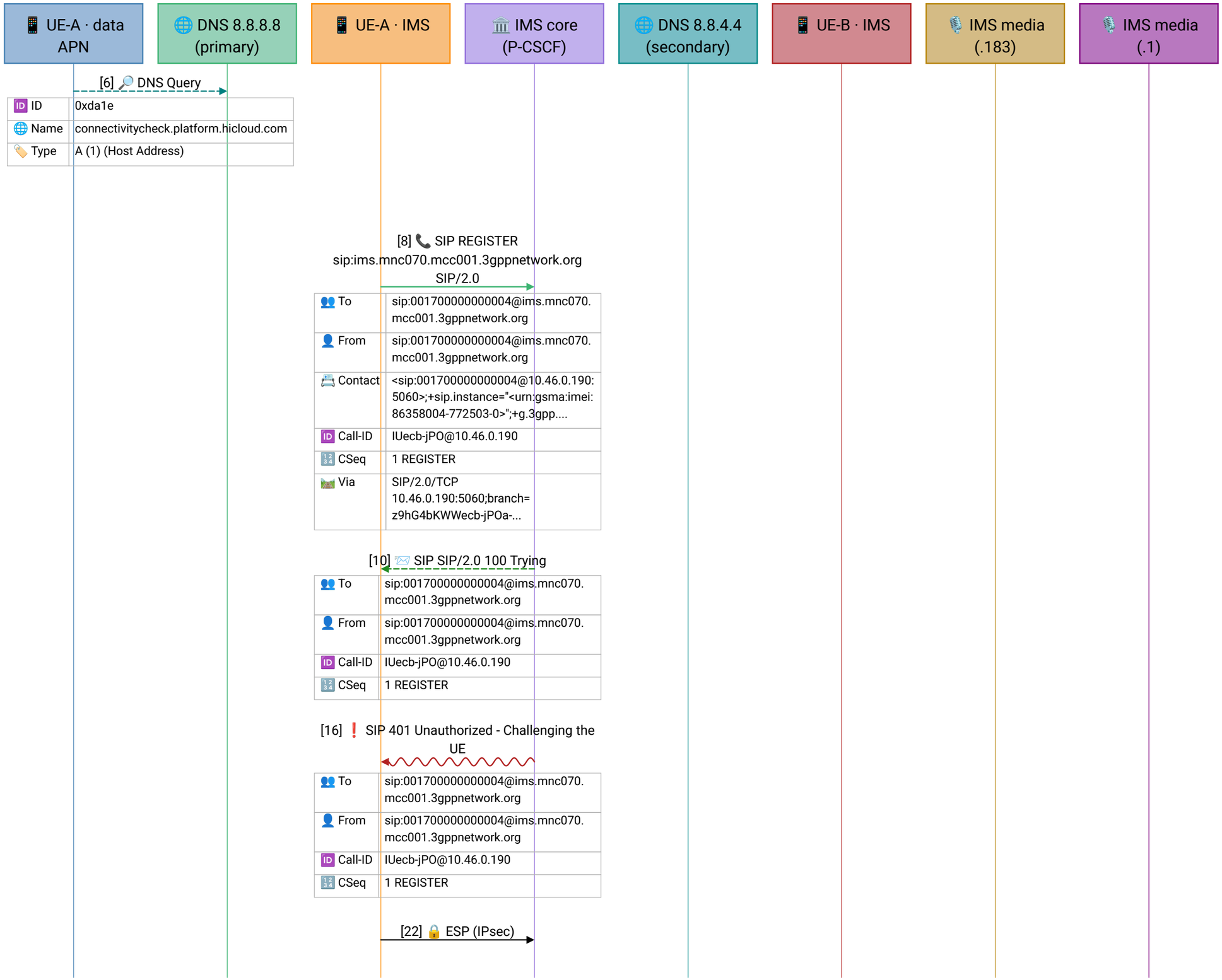


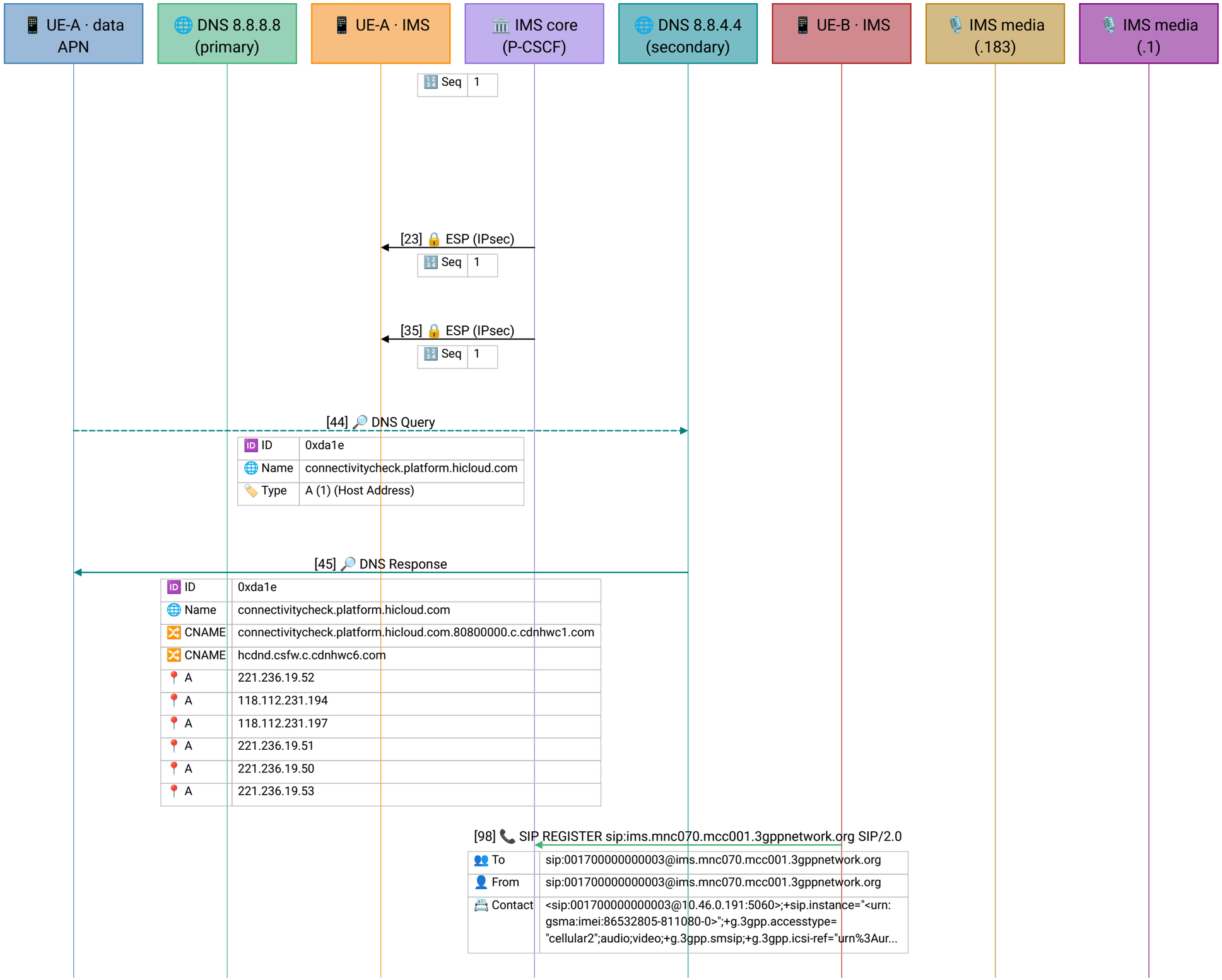
[Frame 6] Phase 1 -- Background DNS, and a resolver that never answers. The very first inner frame isn't voice at all – it is the handset's background app traffic. On its data APN (`10.45.0.181`) UE-A asks its primary resolver `8.8.8.8` to resolve `connectivitycheck.platform.hicloud.com` (a Huawei connectivity probe), transaction ID `0xda1e`. Keep an eye on this query: no answer ever comes back from `8.8.8.8`. The response arrives ~2 s later from a *different* server -- see frame 44.

[Frame 8] Phase 2 -- IMS registration begins, in the clear. Now the voice stack wakes up. On its IMS APN (`10.46.0.190`) UE-A sends a SIP REGISTER over TCP to the P-CSCF (`10.42.0.178`) for `sip:001700000000004@ims.mnc070.mcc001.3gppnetwork.org` – the home domain encodes the test PLMN (MCC 001 / MNC 070). The `Contact` advertises the MMTEL IMS communication service (`+g.3gpp.icsi-ref=...mmtel`) and an `audio` media feature tag: this device is registering to make voice calls. `CSeq: 1` with an empty `Authorization` digest (`nonce="", response=""`) marks this as the first, unauthenticated attempt.

[Frame 10] The P-CSCF acknowledges receipt with `100 Trying` -- it has the REGISTER and is working on it. No decision yet.

[Frame 16] The IMS-AKA challenge. The P-CSCF rejects the bare REGISTER with `401 Unauthorized` -- the status line literally reads *Challenging the UE*. Two headers make this an IMS registration rather than a plain SIP one: `WWW-Authenticate` carries `algorithm=AKAv1-MD5` with a nonce that packs the AKA RAND + AUTN (TS 33.203), and `Security-Server: ipsec-3gpp; ...; spi-s=4111; 6107; alg=hmac-md5-96; ealg=aes-cbc` hands the UE IPsec SA parameters to bring up. The UE will now compute the AKA response and re-REGISTER *inside* IPsec -- watch that `spi-s=4111` reappear in the next frame.

[Frame 22] Phase 3 -- The signalling goes dark (IPsec ESP). Right on cue, ~0.4 s after the 401, the first ESP packet flows



UE-A -> P-CSCF on SPI `0x0000100f` -- decimal `4111`, exactly the `spi-s` value the P-CSCF advertised in frame 16's `Security-Server` header. The security association is up. From here every SIP message -- the AKA-authenticated re-REGISTER, its `200 OK`, and crucially the `INVITE` and `200 OK` that set up the call -- rides *inside* these encrypted frames and is invisible to the capture. ESP shows only its SPI and sequence number; the payload is ciphered (aes-cbc).

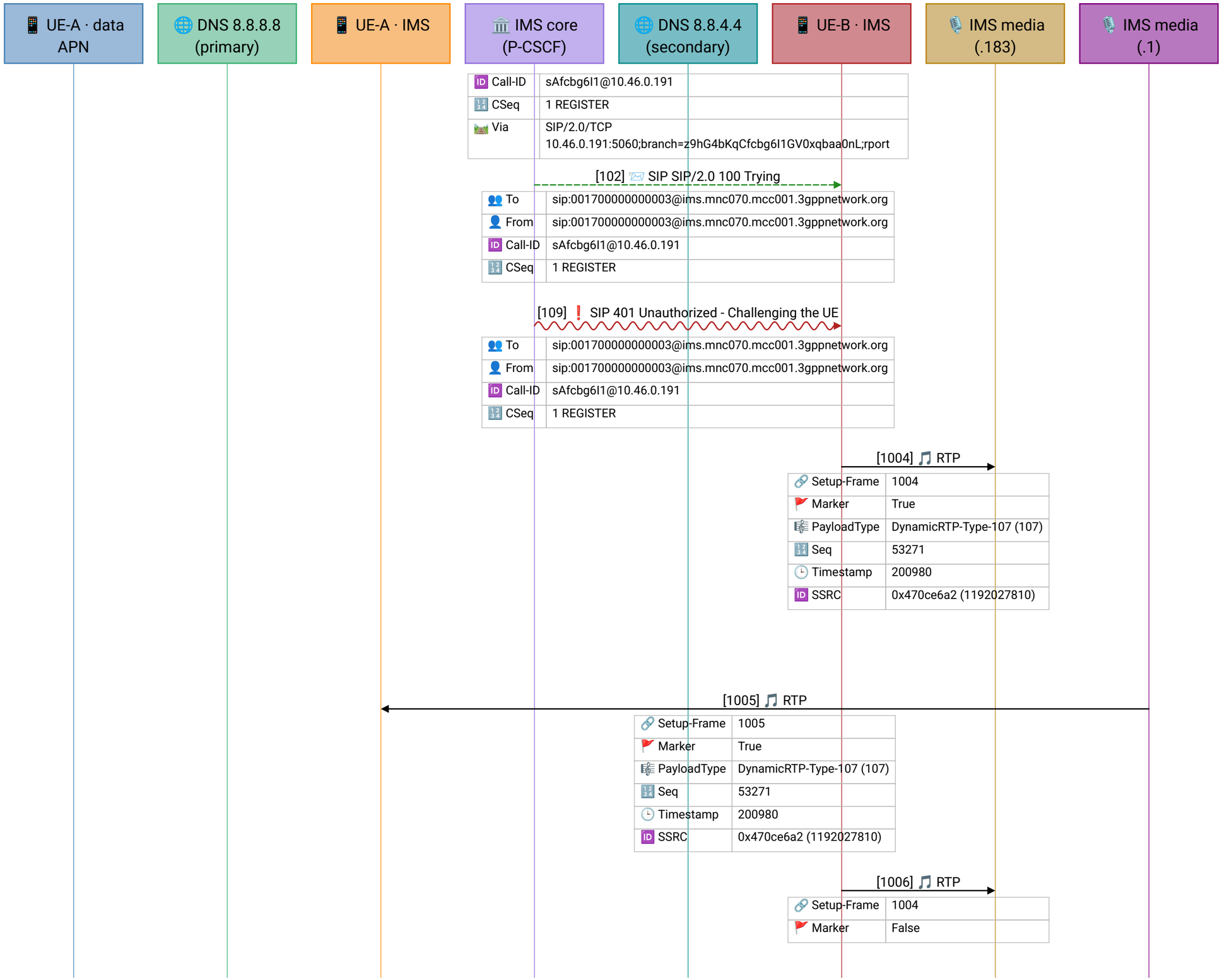
[Frame 23] The reverse-direction SA: P-CSCF -> UE-A ESP on a different SPI (`0x00ad2f75`), sequence 1. TS 33.203 establishes *two pairs* of SAs (protected client and server ports), so several SPIs appear here -- each end chooses the inbound SPI for its own direction.

[Frame 35] A third SPI (`0x0473f2ae`) appears on the P-CSCF -> UE leg -- the second SA pair coming into use. All of this protected traffic is the remainder of registration and, later, the call setup. There is a lot of it: 208 ESP frames across the full trace, and not one byte of it is readable.

[Frame 44] Phase 4 -- The DNS failover completes. Back to that unanswered query from frame 6. After ~1.95 s of silence from `8.8.8.8`, UE-A retransmits the *identical* request -- same transaction ID `0xda1e`, same name -- but this time to its secondary resolver `8.8.4.4`. This is classic resolver failover: the primary is silently unreachable on this testbed's egress, so every lookup eats a ~2 s timeout before trying the backup.

[Frame 45] `8.8.4.4` answers at once (transaction `0xda1e`), returning a CNAME chain into Huawei's CDN and six A records. The lookup succeeds -- just ~2.4 s later than it should have. The tell that this was failover and not packet loss: both query packets carry the *same* transaction ID, so they are one logical lookup, not two. A silent primary resolver is easy to miss, because every name still resolves -- only always two seconds slow.

[Frame 98] Phase 5 -- The second party registers. A second handset, UE-B (`10.46.0.191`, IMSI `...003`), runs the same IMS registration. Its `Contact` advertises `audio` *and* `video` feature tags -- a video-capable client -- though the service is still MMTEL telephony. Same procedure, same `CSeq: 1`, same empty digest: this is a two-party VoNR call, and we are watching both ends attach to IMS.



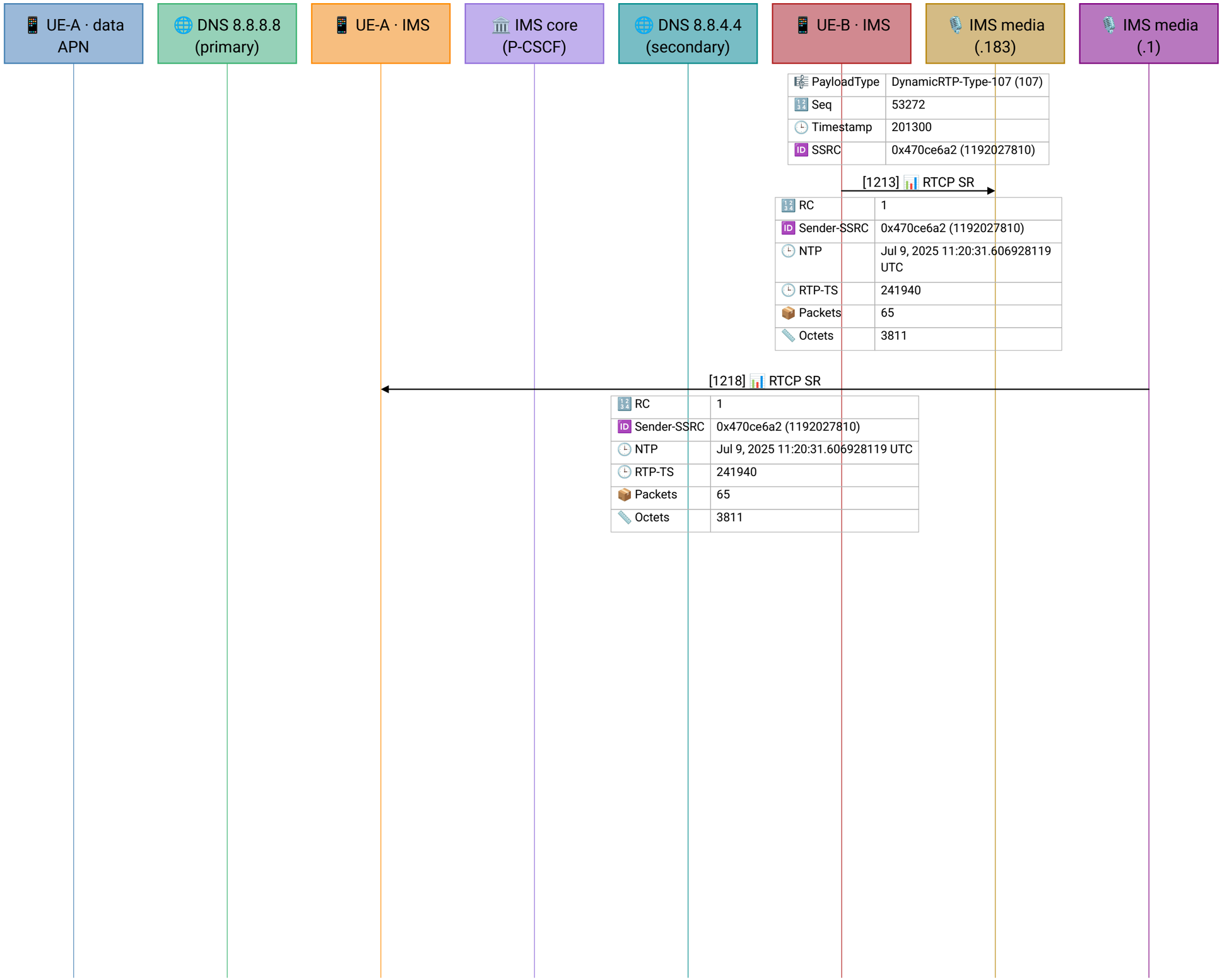
[Frame 102] `100 Trying` from the P-CSCF to UE-B -- its registration is in progress.

[Frame 109] UE-B gets its own `401 - Challenging the UE`, with its own AKA nonce and IPsec SA parameters. From here UE-B's signalling also disappears into ESP. Both parties are now authenticating and setting up the call entirely under IPsec.

[Frame 1004] Phase 6 -- Voice with no visible INVITE. ~11 s after registration, media appears -- and this is the headline of the whole capture. There was **no INVITE and no 200 OK in the clear,** yet here is RTP: a voice packet from UE-B toward the IMS media plane (`10.42.0.183`), dynamic payload type 107 (EVS or AMR-WB), SSRC `0x470ce6a2`, `Marker: True` flagging the first packet of a talkspurt. The call was negotiated entirely inside the ESP frames above -- TS 33.203 keeps all post-registration SIP under IPsec -- while the *media* is not IPsec-protected, so RTP is readable even though the INVITE that created it is not. If you are ever debugging a VoNR call and the INVITE seems to be missing, this is why. 1,670 RTP frames flow in total; only three are shown here.

[Frame 1005] The same RTP packet, one hop later: the IMS media plane relays it from `10.42.0.1` to UE-A (`10.46.0.190`). Note the identical SSRC, sequence (53271) and timestamp (200980) -- the media is *anchored* in the core, not sent UE-to-UE directly, so each packet appears twice (UE-B -> anchor, anchor -> UE-A). Anchored media is normal for IMS voice.

[Frame 1006] The stream continues: `Marker: False` now (mid-talkspurt), sequence advances to 53272, and the RTP timestamp jumps by 320 -- 20 ms of audio at a 16 kHz wideband clock, confirming a wideband voice codec. This 20 ms cadence is exactly the packetisation that rode, invisibly,



inside the F1-U DL User Data of the *outer* capture -- the two walkthroughs meet here.

[Frame 1213] Phase 7 -- RTCP quality reports. Every couple of seconds each endpoint emits an RTCP Sender Report on the paired control port. UE-B's SR (SSRC `0x470ce6a2`) reports 65 packets / 3,811 octets sent so far, with an NTP wall-clock stamp that lets the far end align this stream against others. RTCP is how the endpoints track loss and jitter without touching the media itself.

[Frame 1218] The same Sender Report, relayed through the media anchor (`10.42.0.1`) to UE-A -- identical packet/octet counts and NTP timestamp, mirroring the media anchoring seen on the RTP legs. This is the last frame of the walkthrough; the call runs on for another ~50 s in the full trace. Everything here -- DNS, registration, IPsec, voice -- was pulled out of a capture that Wireshark first showed as nothing but GTP.