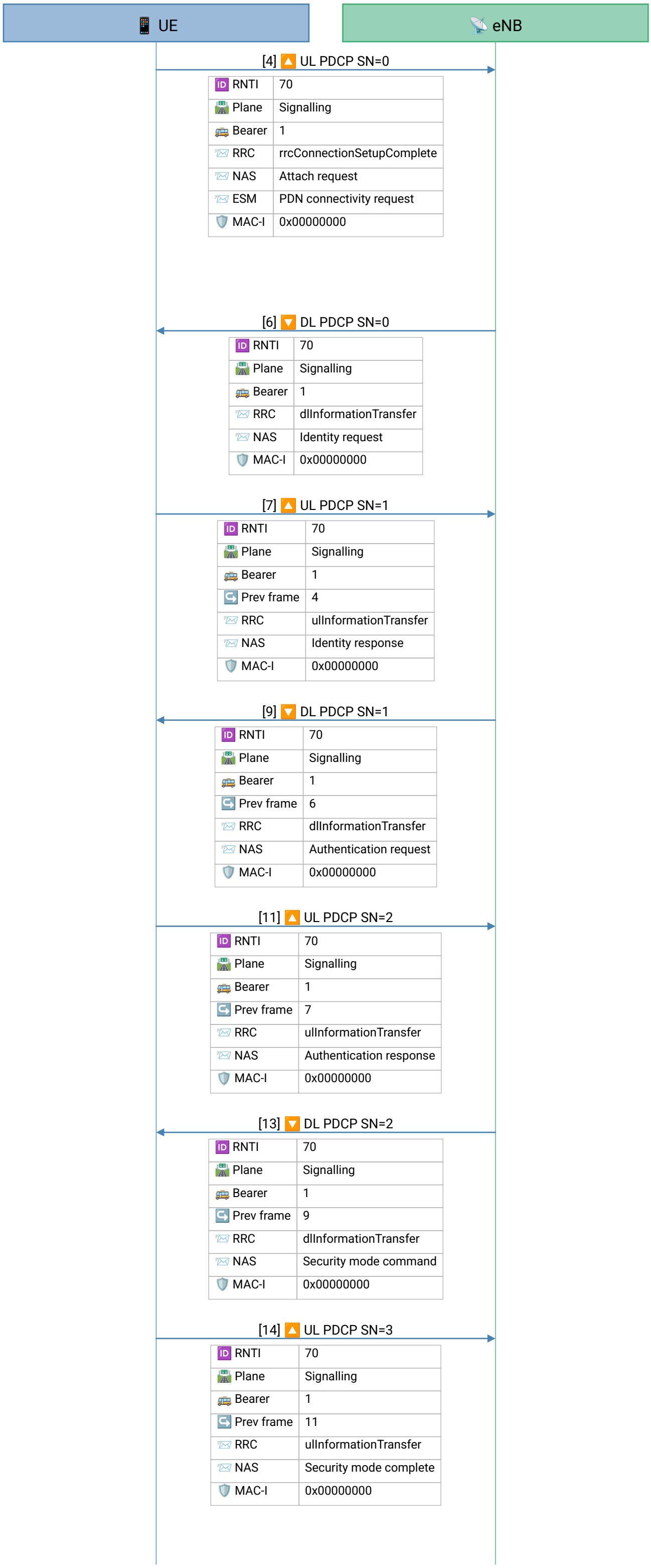
lte-pdcp-srb1.annotated



[Frame 4] SRB1's first PDCP PDU. RRC Connection Setup (frame 3) created SRB1, and with it one PDCP entity in the UE and one in the eNB. Each starts with sequence number 0 and HFN 0 (TS 36.323 §7.1).

This is uplink `SN=0`, carrying RRC Connection Setup Complete with the NAS Attach Request inside. The SRB header is one byte: three reserved bits and a 5-bit SN (TS 36.323 §6.2.2). The RRC message follows, then a 4-byte `MAC-I`.

The `MAC-I` is `0x00000000`. AS security isn't running yet, but an SRB PDU always has the field, padded with zeros until integrity protection starts (TS 36.323 §6.3.4). The NAS message inside is already signed by NAS: two security layers, independent of each other.

[Frame 6] The downlink entity starts its own count. `SN=0` again, 1.9 ms later, from the eNB's transmitting entity. It has nothing to do with frame 4's SN 0: each direction keeps its own counter.

The RRC message is a DL Information Transfer carrying the NAS Identity Request. `MAC-I` is zero.

[Frame 7] Uplink `SN=1`: the NAS Identity Response, inside an UL Information Transfer. "Prev frame 4" is Wireshark's link to the previous PDU on this entity in this direction, so the diagram can be read as two chains: uplink and downlink.

[Frame 9] Downlink `SN=1`: the NAS Authentication Request. `MAC-I` still zero.

[Frame 11] Uplink `SN=2`: the Authentication Response, 214 ms after the request while the SIM computes it. PDCP numbers whatever RRC hands it and doesn't care how long the gap was.

[Frame 13] NAS security, not radio security. Downlink `SN=2` carries the NAS Security Mode Command, which selects `EEA0` and `EIA2` for the link between the UE and the MME. It changes nothing at PDCP: the `MAC-I` stays zero. The radio link needs its own procedure, three frames later.

[Frame 14] Uplink `SN=3`: the NAS Security Mode Complete. It is the last uplink PDU with a zero `MAC-I`. From here every SRB1 PDU in both directions carries a real tag.

📱 UE | 📡 eNB

[16] 🔽 DL PDCP SN=3

🆔 RNTI	70
🛣️ Plane	Signalling
🚌 Bearer	1
🔁 Prev frame	13
✉️ RRC	securityModeCommand
🛡️ MAC-I	0x4efe0942
❌ MAC-I check	wrong (calc=00000000, got=4efe0942)

[Frame 16] AS Security Mode Command: integrity starts here. Downlink `SN=3`. The RRC command selects `eea0` (null ciphering) and `eia2` (AES-based integrity) for the radio link. The eNB protects the command itself with the new key `K_RRCint`, so its `MAC-I` is the first non-zero one on SRB1: `0x4efe0942` (TS 36.331 §5.3.4.3, TS 33.401 §7.2.4.5).

The command is not ciphered: ciphering starts only after it.

Wireshark flags the digest "wrong" because it applies the new settings only to PDUs after this one, so it expected zeros. It couldn't check the real value anyway: the capture has no keys.

[17] 🔼 UL PDCP SN=4

🆔 RNTI	70
🛣️ Plane	Signalling
🚌 Bearer	1
🔐 Sec	EEA0/EIA2
🔢 PDCP COUNT	4
🔁 Prev frame	14
✉️ RRC	securityModeComplete
🛡️ MAC-I	0xc1047431

[Frame 17] The first COUNT. Uplink `SN=4`, Security Mode Complete, 29 ms after the command. Integrity-protected (`MAC-I 0xc1047431`) and, by rule, still not ciphered (TS 36.331 §5.3.4.3).

From this PDU on, Wireshark prints the inputs EIA2 uses:

- `COUNT` 4: the 32-bit counter, the HFN (27 bits on an SRB) above the 5-bit SN. The HFN is 0, so COUNT equals SN.
- `BEARER` 0: the radio bearer identity minus 1, so 0 for SRB1.
- `DIRECTION` 0: uplink.
- Configuration frame 16: the command that set the algorithms.

128-EIA2 is AES-CMAC over the key, these three inputs, and the message (TS 33.401 Annex B.2). What it covers is the PDCP header plus the RRC message (TS 36.323 §5.7).

[19] 🔽 DL PDCP SN=4

🆔 RNTI	70
🛣️ Plane	Signalling
🚌 Bearer	1
🔐 Sec	EEA0/EIA2
🔢 PDCP COUNT	4
🔁 Prev frame	16
✉️ RRC	ueCapabilityEnquiry
🛡️ MAC-I	0xd8c5635b

[Frame 19] Ciphering is on, and changes nothing. Downlink `SN=4`, UE Capability Enquiry, `MAC-I 0xd8c5635b`. This is the first downlink PDU after the command, so it is ciphered, with EEA0. EEA0's keystream is all zeros, so the "ciphered" RRC message and `MAC-I` are byte for byte the plaintext. With EEA1 to EEA3, everything after the header byte would be unreadable without `K_RRCenc`.

[22] 🔼 UL PDCP SN=5

🆔 RNTI	70
🛣️ Plane	Signalling
🚌 Bearer	1
🔐 Sec	EEA0/EIA2
🔢 PDCP COUNT	5
🔁 Prev frame	17
✉️ RRC	ueCapabilityInformation
🛡️ MAC-I	0x4581ea09

[Frame 22] One SN for 2,017 bytes. Uplink `SN=5`: UE Capability Information. The PDCP PDU is 2,017 bytes, and RLC carried it in three segments, RLC SN 5 to 7 (frames 20 to 22). PDCP counts it once. How many pieces RLC needed is invisible from here.

[24] 🔽 DL PDCP SN=5

🆔 RNTI	70
🛣️ Plane	Signalling
🚌 Bearer	1
🔐 Sec	EEA0/EIA2
🔢 PDCP COUNT	5
🔁 Prev frame	19
✉️ RRC	rrcConnectionReconfiguration
✉️ NAS	Attach accept
✉️ ESM	Activate default EPS bearer context request
🛡️ MAC-I	0x1716ddce

[Frame 24] Downlink `SN=5`: the first RRC Connection Reconfiguration. It carries the NAS Attach Accept with the default bearer's activation request, and it adds SRB2 and DRB 1. SRB2 and DRB 1 get PDCP entities of their own, with their own counters starting at 0. This entity just continues.

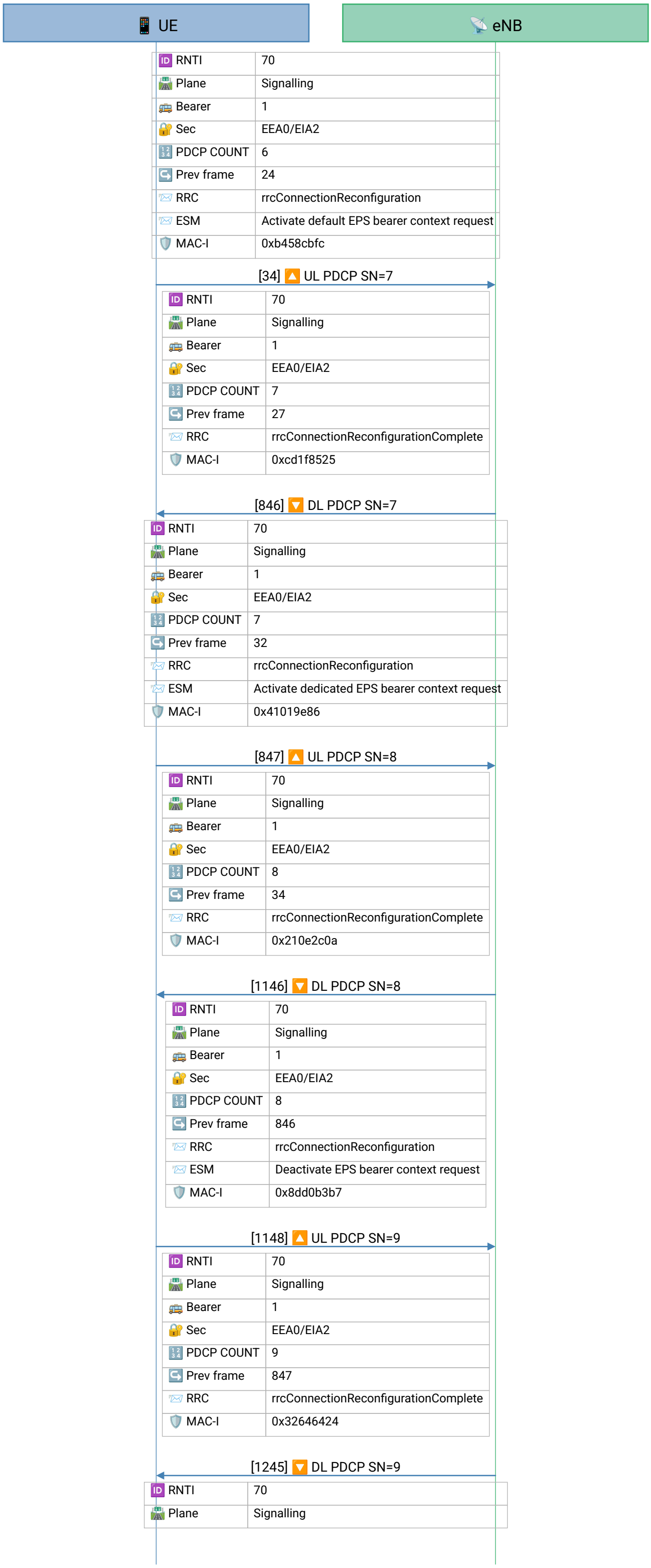
[27] 🔼 UL PDCP SN=6

🆔 RNTI	70
🛣️ Plane	Signalling
🚌 Bearer	1
🔐 Sec	EEA0/EIA2
🔢 PDCP COUNT	6
🔁 Prev frame	22
✉️ RRC	rrcConnectionReconfigurationComplete
🛡️ MAC-I	0xdc1bab6b

[Frame 27] Uplink `SN=6`: Reconfiguration Complete, `MAC-I 0xdc1bab6b`. The same transport block carries SRB2's first uplink PDU, SN 0, with the NAS Attach Complete. Two PDCP entities, two SN 0s in a row: SRB2's counter has nothing to do with this one. Only SRB1's PDU belongs on this diagram.

[32] 🔽 DL PDCP SN=6

[Frame 32] Downlink `SN=6`: the reconfiguration that adds DRB 2 for the IMS PDN, with the NAS default-bearer request



for EBI 6.

[Frame 34] The PDU bytes. Uplink `SN=7`, Reconfiguration Complete. The whole PDCP PDU is 7 bytes: `07` (header, SN 7), `10 00` (the RRC message), and `cd1f8525` (the `MAC-I`).

Compare frame 27: `06 10 00 dc1bab6b`. The same two RRC bytes, and a completely different tag, because COUNT changed. That is what makes a replayed message fail its integrity check.

[Frame 846] 23 seconds later, the count resumes. After frame 34, SRB1 is silent while IMS registration runs on DRB 2. The entity keeps its state: downlink continues at `SN=7`, COUNT 7.

This reconfiguration adds DRB 3, call 1's voice bearer (EBI 7, QCI 1), with PDCP 12-bit SN and `discardTimer` 100 ms. It creates the PDCP entity drawn on this page's second diagram, `lte-pdcp-voice-bearer`. The NAS Activate Dedicated EPS Bearer Context Request rides inside.

[Frame 847] Uplink `SN=8`: Reconfiguration Complete, 33 ms later. The same frame carries SRB2's uplink SN=3 (the NAS accept) and two DRB 2 PDUs, SN 28 and 29. Four PDCP PDUs from three entities in one MAC PDU, each counted on its own.

In the original capture, Wireshark gives this PDU no COUNT at all. See the page's re-tag section.

[Frame 1146] Call 1 ends. Downlink `SN=8`: the reconfiguration that releases DRB 3, with the NAS Deactivate EPS Bearer Context Request. Releasing the DRB deletes its PDCP entity and that entity's COUNTs. SRB1 is unaffected.

[Frame 1148] Uplink `SN=9`: Reconfiguration Complete, alone this time. 7 bytes again: `09 10 00 32646424`. The NAS accept follows on SRB2 in frame 1152.

[Frame 1245] Call 2. Downlink SN=9 adds DRB 4. From here each call adds one DRB and later removes it. Every add and every release costs this entity one downlink SN and one uplink SN.

lte-pdcp-srb1.annotated



Bearer	1
Sec	EEA0/EIA2
PDCP COUNT	9
Prev frame	1146
RRC	rrcConnectionReconfiguration
ESM	Activate dedicated EPS bearer context request
MAC-I	0x14cb44a8

[1248] UL PDCP SN=10

RNTI	70
Plane	Signalling
Bearer	1
Sec	EEA0/EIA2
PDCP COUNT	10
Prev frame	1148
RRC	rrcConnectionReconfigurationComplete
MAC-I	0xc9a80315

[Frame 1248] Uplink SN=10 : Reconfiguration Complete, MAC-I 0xc9a80315.

[1503] DL PDCP SN=10

RNTI	70
Plane	Signalling
Bearer	1
Sec	EEA0/EIA2
PDCP COUNT	10
Prev frame	1245
RRC	rrcConnectionReconfiguration
ESM	Deactivate EPS bearer context request
MAC-I	0x736cc50e

[Frame 1503] Downlink SN=10 : release of DRB 4.

[1504] UL PDCP SN=11

RNTI	70
Plane	Signalling
Bearer	1
Sec	EEA0/EIA2
PDCP COUNT	11
Prev frame	1248
RRC	rrcConnectionReconfigurationComplete
MAC-I	0x88fb3f65

[Frame 1504] Uplink SN=11 : Reconfiguration Complete.

[1599] DL PDCP SN=11

RNTI	70
Plane	Signalling
Bearer	1
Sec	EEA0/EIA2
PDCP COUNT	11
Prev frame	1503
RRC	rrcConnectionReconfiguration
ESM	Activate dedicated EPS bearer context request
MAC-I	0xed866da3

[Frame 1599] Call 3. Downlink SN=11 adds DRB 5.

[1603] UL PDCP SN=12

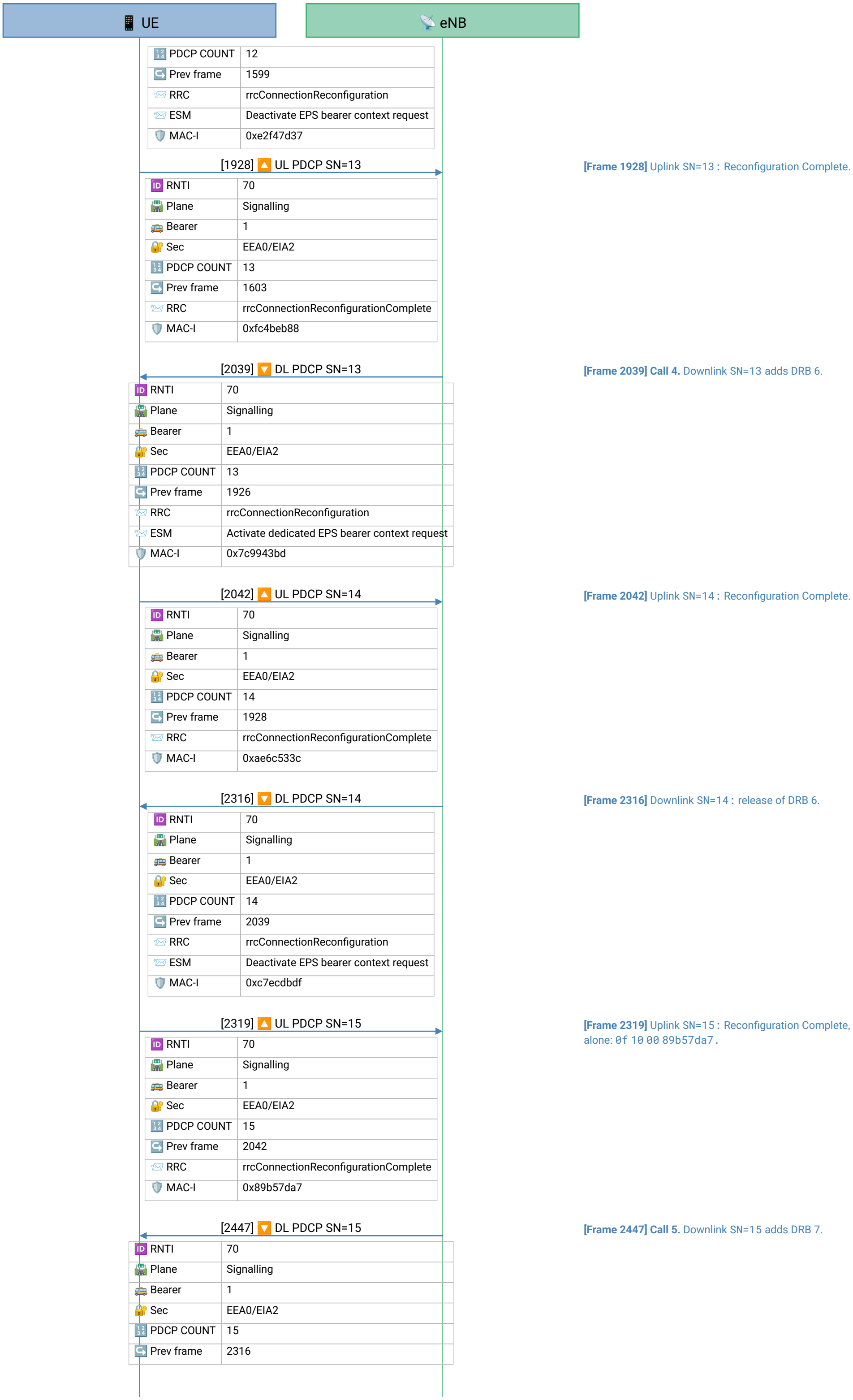
RNTI	70
Plane	Signalling
Bearer	1
Sec	EEA0/EIA2
PDCP COUNT	12
Prev frame	1504
RRC	rrcConnectionReconfigurationComplete
MAC-I	0x030deec6

[Frame 1603] Uplink SN=12 : Reconfiguration Complete.

[1926] DL PDCP SN=12

RNTI	70
Plane	Signalling
Bearer	1
Sec	EEA0/EIA2

[Frame 1926] Downlink SN=12 : release of DRB 5.



[Frame 1928] Uplink SN=13 : Reconfiguration Complete.

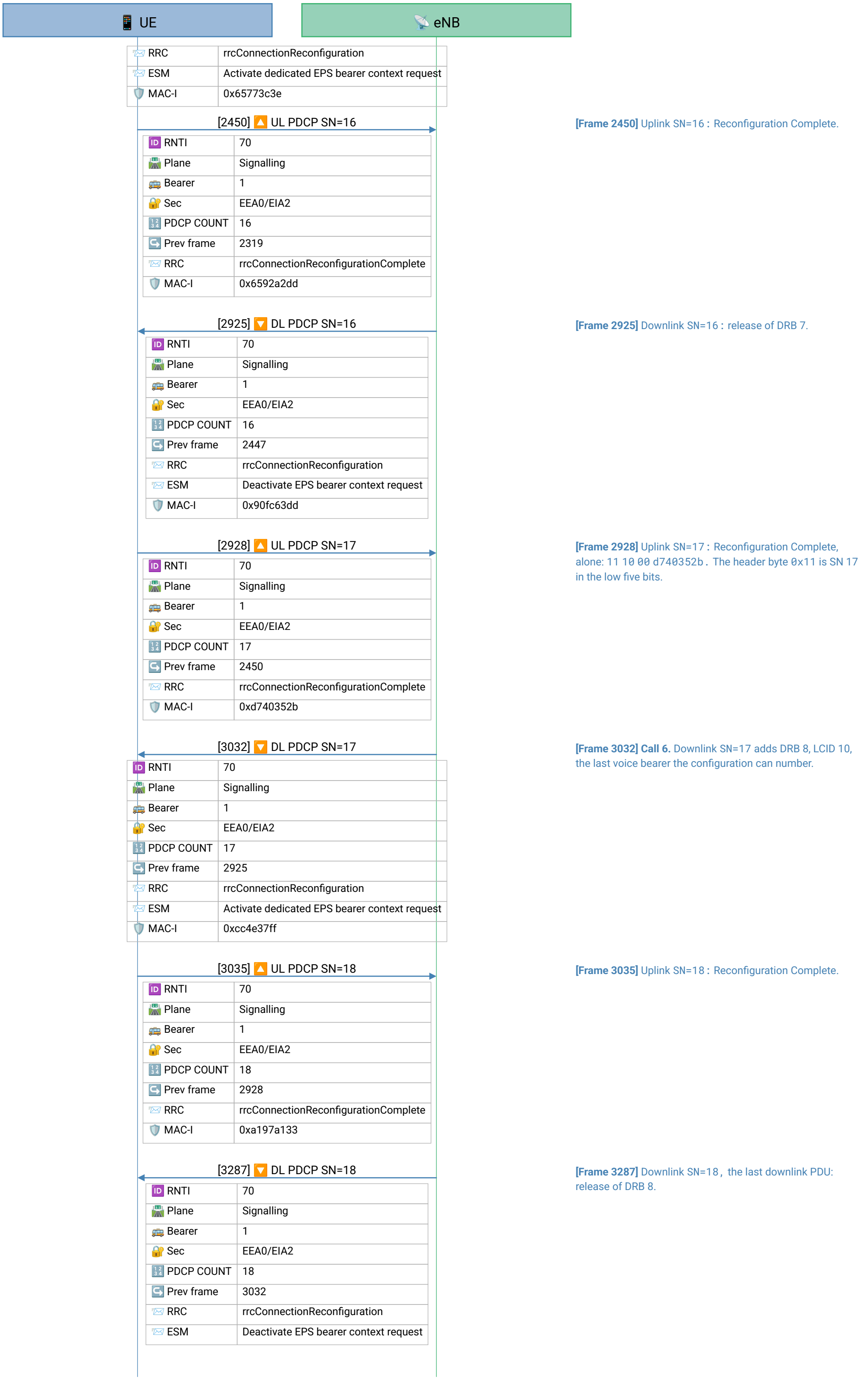
[Frame 2039] Call 4. Downlink SN=13 adds DRB 6.

[Frame 2042] Uplink SN=14 : Reconfiguration Complete.

[Frame 2316] Downlink SN=14 : release of DRB 6.

[Frame 2319] Uplink SN=15 : Reconfiguration Complete, alone: `0f 10 00 89b57da7`.

[Frame 2447] Call 5. Downlink SN=15 adds DRB 7.



[Frame 2450] Uplink SN=16 : Reconfiguration Complete.

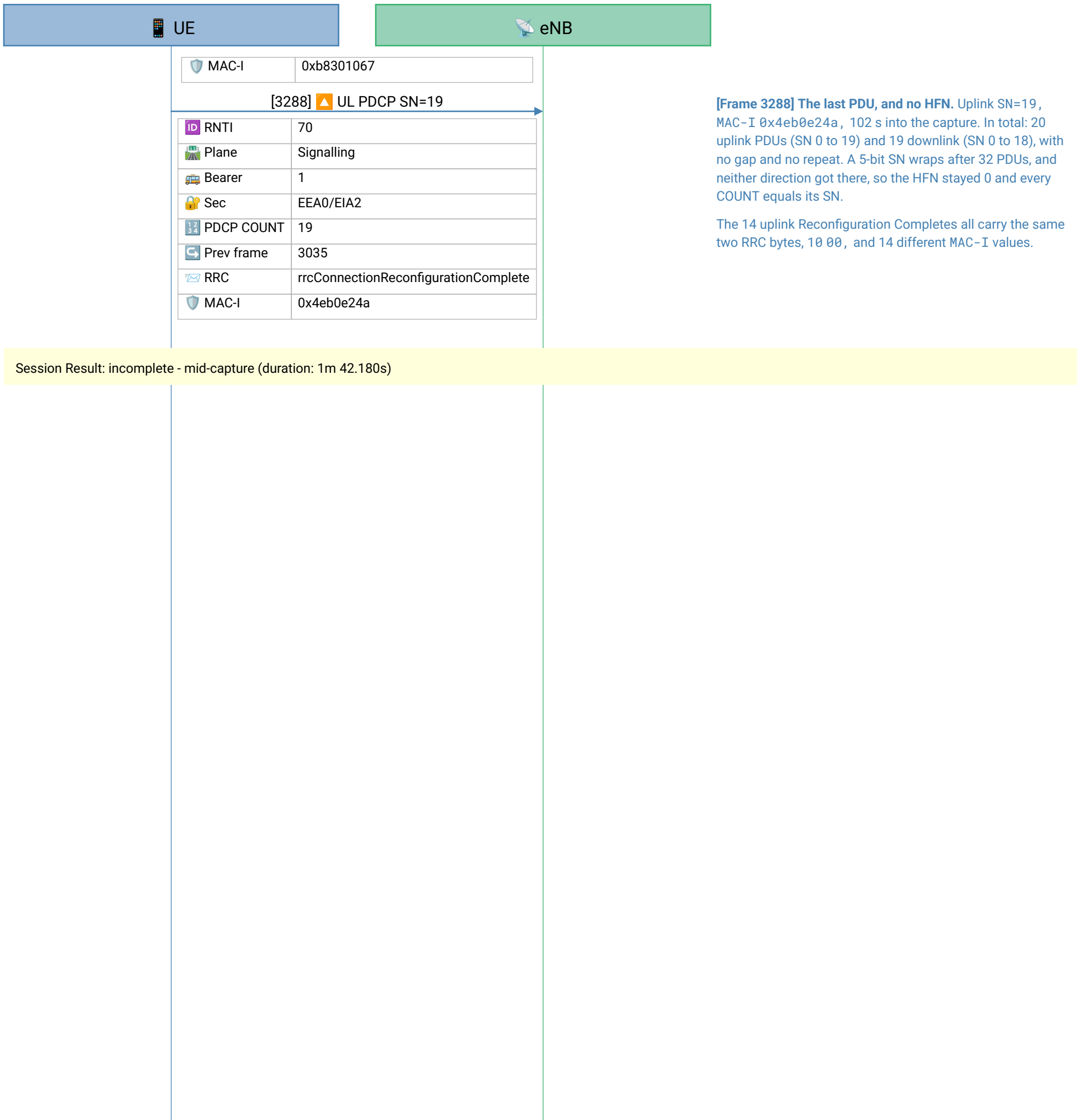
[Frame 2925] Downlink SN=16 : release of DRB 7.

[Frame 2928] Uplink SN=17 : Reconfiguration Complete, alone: `11 10 00 d740352b`. The header byte `0x11` is SN 17 in the low five bits.

[Frame 3032] Call 6. Downlink SN=17 adds DRB 8, LCID 10, the last voice bearer the configuration can number.

[Frame 3035] Uplink SN=18 : Reconfiguration Complete.

[Frame 3287] Downlink SN=18 , the last downlink PDU: release of DRB 8.



[Frame 3288] The last PDU, and no HFN. Uplink `SN=19`, `MAC-I 0x4eb0e24a`, 102 s into the capture. In total: 20 uplink PDUs (SN 0 to 19) and 19 downlink (SN 0 to 18), with no gap and no repeat. A 5-bit SN wraps after 32 PDUs, and neither direction got there, so the HFN stayed 0 and every COUNT equals its SN.

The 14 uplink Reconfiguration Completes all carry the same two RRC bytes, `10 00`, and 14 different `MAC-I` values.

Session Result: incomplete - mid-capture (duration: 1m 42.180s)