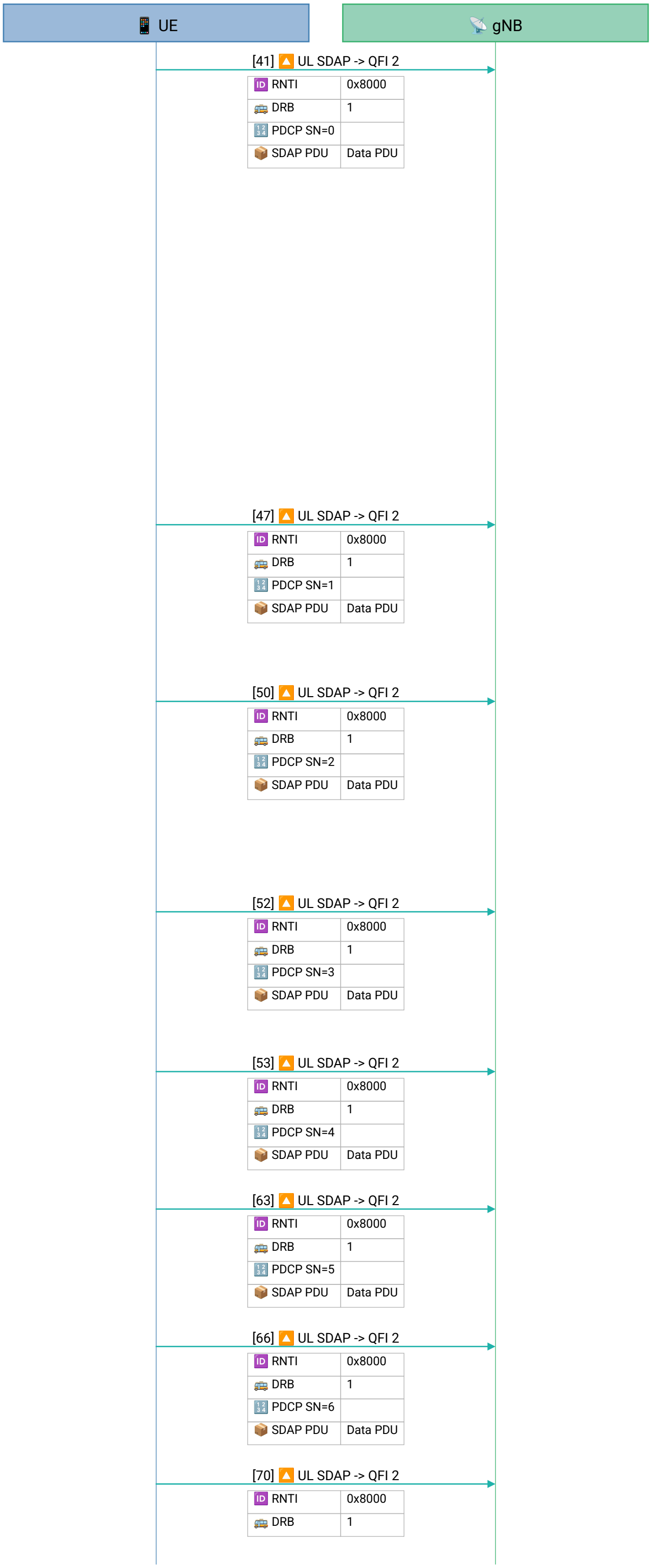
sdap-nr-qos-flows.annotated



[Frame 41] The first SDAP PDU of the capture, and the whole layer in one byte. The bearer this rides on did not exist until a moment ago. Frame 38's RRC Reconfiguration added `drb-Identity: 1` with an `sdap-Config` reading `pdu-Session: 1`, `sdap-HeaderUL: present (0)`, `sdap-HeaderDL: absent (1)`, `defaultDRB: True`, and a `mappedQoS-FlowsToAdd: 1 item` holding `QFI: 2`. Everything on this diagram is that configuration being obeyed.

Unwrap this transmission from the bottom and the SDAP header falls out of the bytes. MAC-NR carries a 55-byte SDU on `LCID: 4`. RLC-NR reads it as DRB 1, AM, uplink, `SN=0`, poll set, 52 bytes of data beginning `800000827dbd4542`. Split that: `80 00 00` is the three-byte PDCP header for an 18-bit sequence number (`PDU Type: Data PDU, Seq Num: 0`), and the very next byte, `82`, is the entire SDAP header — `1000 0010`, which Wireshark expands as `PDU Type: Data PDU, Reserved: 0x0, QFI: 2`. Note where the ciphertext starts. This bearer runs NEA2 (AES), yet the 82 sits in the clear and Wireshark's `Deciphered Data` for the same PDU begins `6000000000083aff` — an IP header, not the SDAP byte. TS 38.323 §5.8 excludes the SDAP header from ciphering precisely so a receiver can classify a packet before it decrypts it. Everything above the SDAP header on this diagram is Decrypting a 5G NR radio capture 's subject; SDAP stops at the QFI.

[Frame 47] The second PDU, 1219.994 ms later, and the QFI has not moved. RLC `SN=1`, 84 bytes, data `80000182be762cf9` — the same 82 in the same position, one byte past a PDCP header whose sequence number has advanced to 1. One QoS flow was mapped onto this bearer and only one is in use, so the QFI is a constant for the whole session. That is not SDAP being redundant: the header still has to be sent, because once several flows share one DRB the receiver has no other way to tell which flow a packet belongs to.

[Frame 50] Three RLC PDUs in one transport block, and exactly one SDAP PDU. MAC packs a 3-byte status PDU, a whole 64-byte data PDU (`SN=2`) and the first 539 bytes of SN=3 into one uplink grant. Only SN=2 completes here, so only one PDCP SDU is delivered upward and only one SDAP header is dissected — `QFI: 2`, from PDCP `SN=2`. Look at the bytes of the other one anyway: SN=3 starts `800003 82`, so its SDAP header is already on the wire in this frame. It is simply not *deliverable* yet. SDAP sees a packet only after RLC has reassembled it and PDCP has deciphered it, which is why this diagram has 18 arrows where RLC's uplink on this bearer has 27 data PDUs.

[Frame 52] Reassembly completes, and the SDAP PDU appears where the last segment landed. The first RLC PDU here is SN=3 at `SO=1153`, the third and final segment of an SDU that began in frame 50 and continued through frame 51. That completes PDCP `SN=3`, and its SDAP header reads `QFI: 2`. The frame's second RLC PDU opens the next SDU — `SN=4`, `800004 82` — 498 bytes of it. Two different SDUs in flight in one transmission, and the SDAP layer above cannot tell: it is handed whole packets or nothing.

[Frame 53] Sixteen bytes finish the burst. RLC SN=4 at `SO=498` contributes its last 16 bytes and sets the poll bit, PDCP SN=4 comes together, and the SDAP header on it is `QFI: 2` like every one before it. Four PDUs delivered since frame 47, at 19.999 ms, 6.995 ms and 0.996 ms apart — the uplink is running as fast as the scheduler will grant, and then it stops.

[Frame 63] A new burst, 1222.999 ms after the last one. RLC `SN=5`, 64 bytes whole, `800005 82`, PDCP `SN=5`, `QFI: 2`. The gap is the application's cadence, not SDAP's: the layer has no timers, no keepalives and no state of its own to maintain. When there is nothing to map, SDAP emits nothing.

[Frame 66] PDCP `SN=6`, `QFI: 2`. A 64-byte RLC SDU, 88.996 ms after the last. Same one-byte header, same flow, same bearer. The monotony is the point — this is what a correctly configured single-flow DRB looks like, and all the interesting variation is in the layers below.

[Frame 70] PDCP `SN=7`, `QFI: 2`. Another 64-byte SDU, piggybacked behind an RLC status PDU in the same grant. The status report belongs to RLC's own bookkeeping and never reaches SDAP; only the data PDU carries a QFI.

[Frame 72] PDCP SN=8, QFI: 2 — and the packet gets bigger, 108 bytes of RLC data rather than 64. The SDAP header does not care and does not change: one byte, `82`, whatever the payload turns out to be. What that payload turns into from here is Decrypting a 5G NR radio capture 's territory.

[Frame 75] Third burst, 1030.999 ms on. RLC `SN=9`, 108 bytes, `800009 82`, PDCP `SN=9`, `QFI: 2`. Ten SDAP PDUs so far — this is the tenth message of the session — and ten identical headers.

[Frame 78] One of only two frames in the session carrying three RLC PDUs, and again one SDAP PDU out of it. The transport block holds an RLC status PDU, `SN=10` whole at 88 bytes, and the first 515 bytes of `SN=11`. Frame 50 was the other; every remaining uplink transmission on this bearer carries one RLC PDU or two. PDCP `SN=10` is the only SDU that completes here, so the only SDAP header dissected is its `QFI: 2`. Note what does *not* vary. Every one of the session's 27 uplink transmissions is 691 bytes on the wire, so no frame here is a bigger grant than any other — only a more fully packed one.

[Frame 80] PDCP SN=11 completes at SO=1129, 6.993 ms after frame 78. Three RLC transmissions — frames 78, 79 and 80 — for one SDAP PDU carrying one QFI. Segmentation is invisible from up here, and so is the number of transmissions it cost. In the same frame SN=12 starts with `80000c 82`.

[Frame 81] PDCP SN=12, QFI: 2. SN=12 finishes at `SO=450` with 538 bytes and the poll bit, 0.997 ms after frame 80. Second burst in a row that ends with a segmented SDU completing on the last frame of the run.

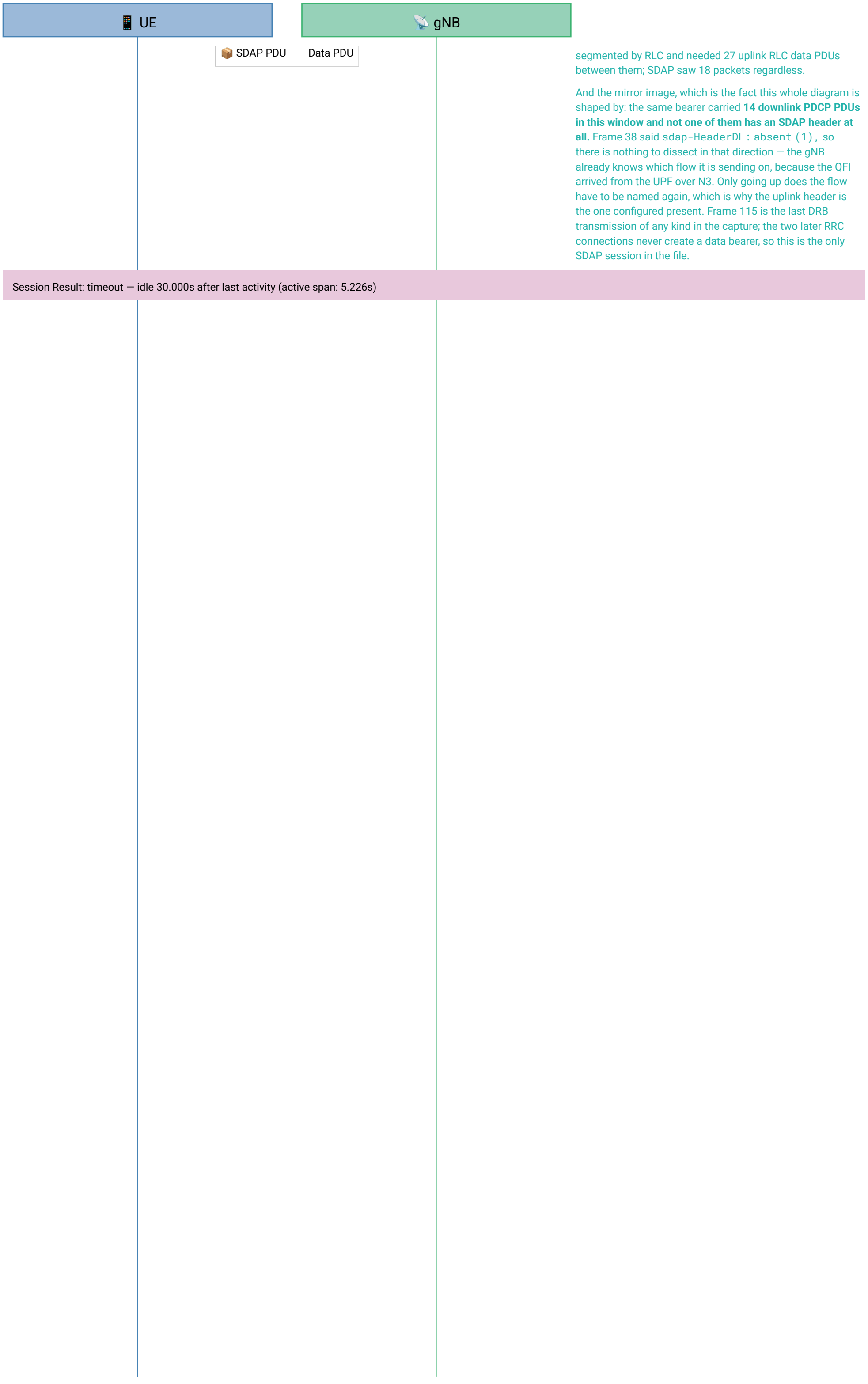
[Frame 91] PDCP SN=13, QFI: 2, 272.008 ms later — an 88-byte SDU, whole, behind a status PDU. This is the fourteenth message of the session: fourteen uplink SDAP PDUs, fourteen `QFI: 2` headers, and the `D/C` bit has read `Data` PDU on every one. There is no SDAP Control PDU anywhere in this capture, and there is no reason for one: the only SDAP Control PDU the spec defines is the end-marker a UE sends after a QoS flow is remapped to a different DRB (TS 37.324), and nothing here is ever remapped.

[Frame 97.1] Two SDAP PDUs in one frame — this is the first. The frame's opening RLC PDU is `SN=14` at `SO=1227`, the last 61 bytes of a three-segment SDU that started back in frame 95. That completes PDCP `SN=14`, and its SDAP header reads `QFI: 2`. Because two PDCP PDUs finish inside this single transmission, the diagram splits the frame into two arrows. They are genuinely independent packets: two sequence numbers, two SDAP headers, one radio transmission.

[Frame 97.2] The second SDAP PDU of frame 97. RLC `SN=15` rides whole in the same transport block, 332 bytes, poll set, data beginning `80000f82` — PDCP `Seq Num: 15`, then the familiar `82`. `QFI: 2` again. Two packets of the same QoS flow, mapped onto the same DRB, delivered in the same slot: exactly the case SDAP's per-packet header exists to keep unambiguous.

[Frame 107] PDCP SN=16, QFI: 2, 93.002 ms after frame 97. An 88-byte SDU behind a status PDU, data `800010 82`. Seventeen down, one to go.

[Frame 114] The last SDAP PDU on the bearer, 5225.955 ms after the first. RLC SN=17 completes at SO=613 with 371 bytes and the poll bit; PDCP SN=17 is delivered; the SDAP header reads `QFI: 2`. The session's totals: **18 SDAP PDUs across 17 frames, every one uplink, every one a Data PDU, every one carrying `QFI: 2`** — the single QoS flow that frame 38 mapped onto DRB 1. Six of those 18 SDUs were


📱 UE
📡 gNB
📦 SDAP PDU
Data PDU
segmented by RLC and needed 27 uplink RLC data PDUs between them; SDAP saw 18 packets regardless.
And the mirror image, which is the fact this whole diagram is shaped by: the same bearer carried **14 downlink PDCP PDUs in this window and not one of them has an SDAP header at all.** Frame 38 said `sdap-HeaderDL: absent (1)`, so there is nothing to dissect in that direction — the gNB already knows which flow it is sending on, because the QFI arrived from the UPF over N3. Only going up does the flow have to be named again, which is why the uplink header is the one configured present. Frame 115 is the last DRB transmission of any kind in the capture; the two later RRC connections never create a data bearer, so this is the only SDAP session in the file.
Session Result: timeout — idle 30.000s after last activity (active span: 5.226s)