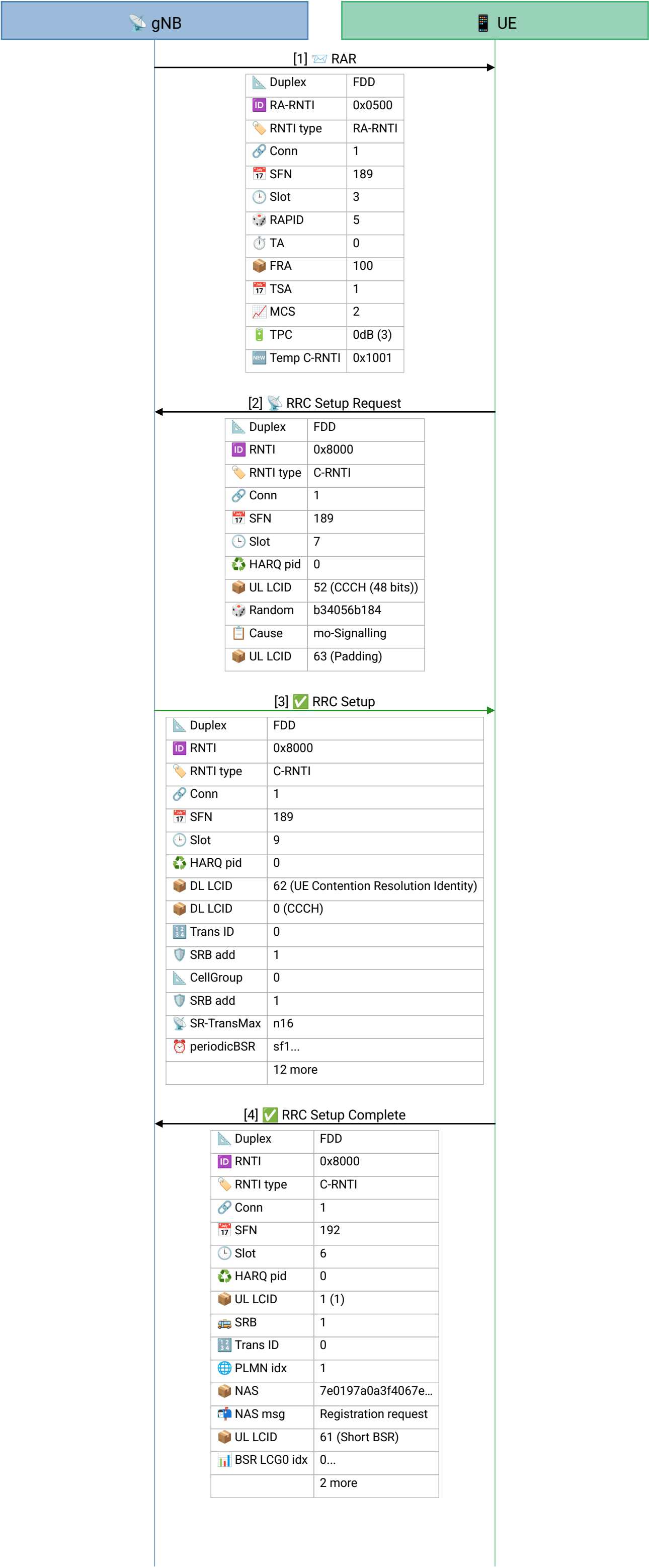
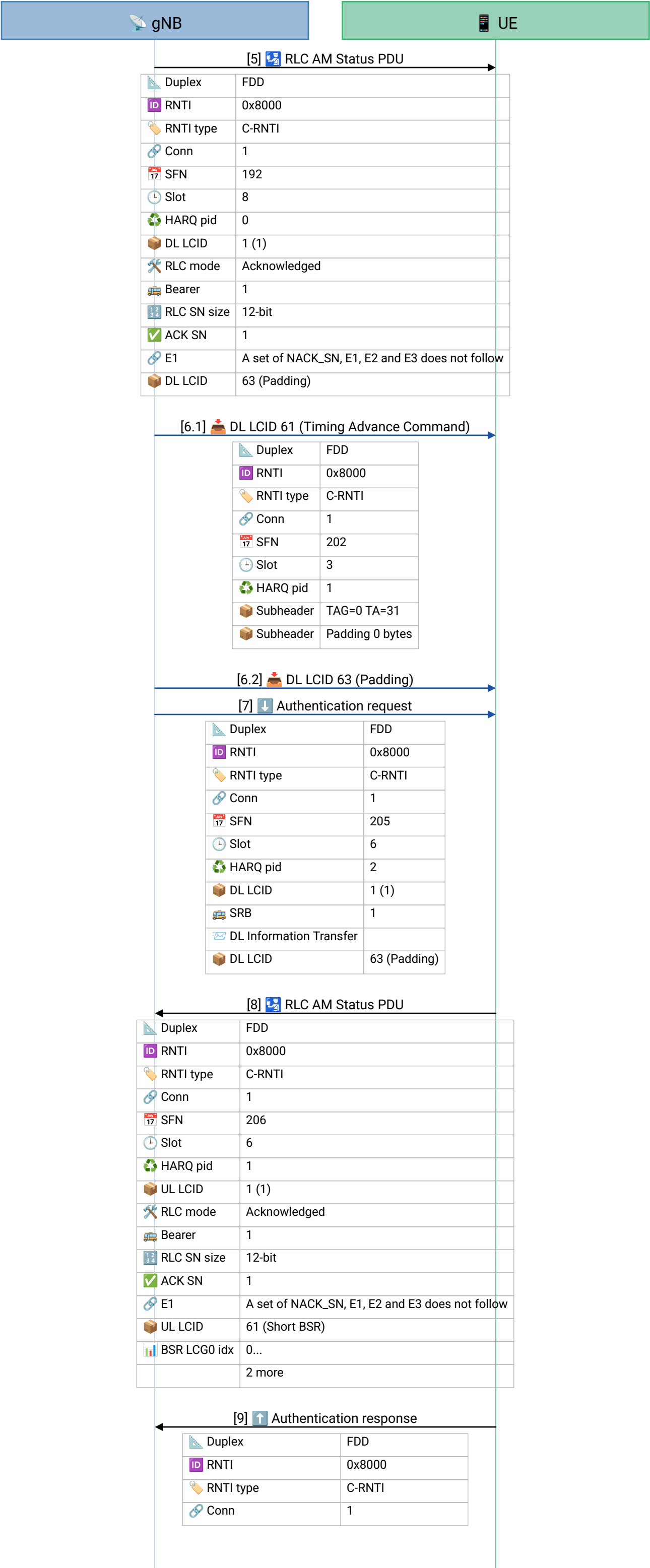
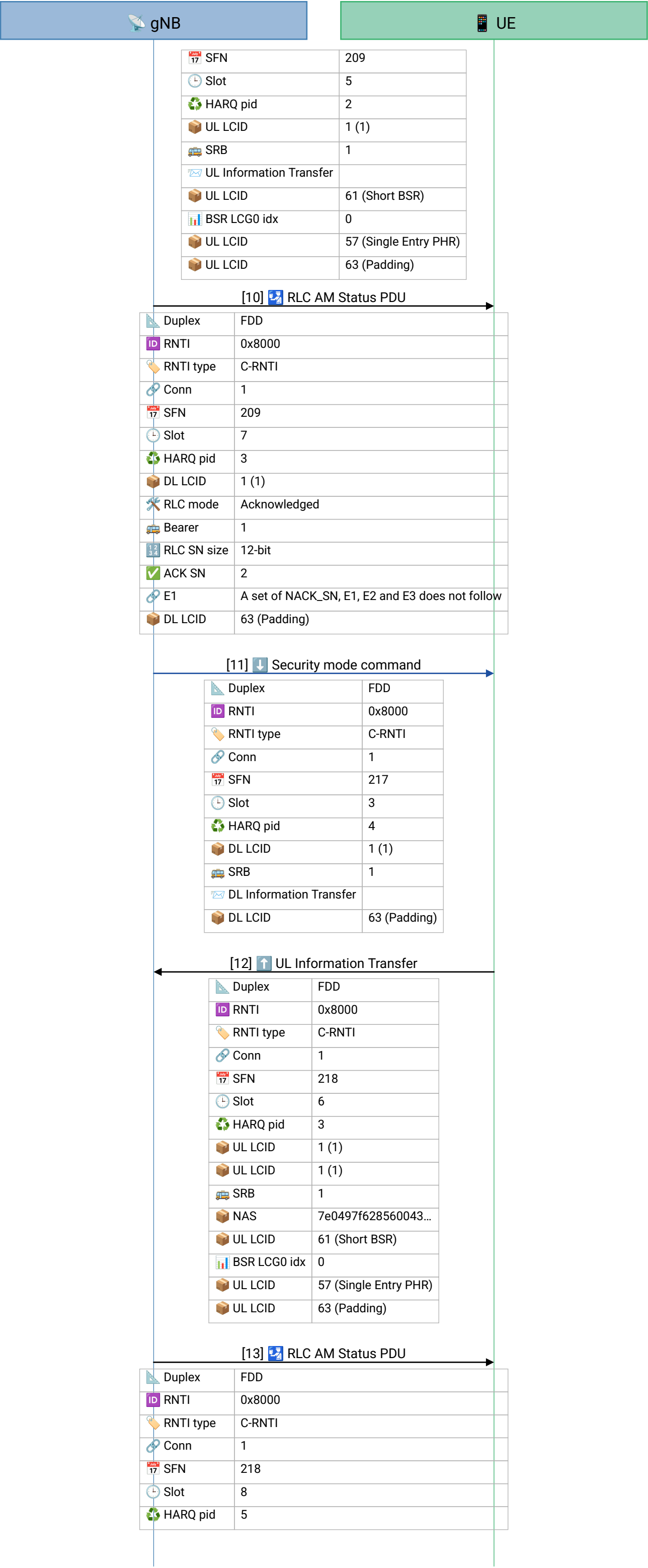






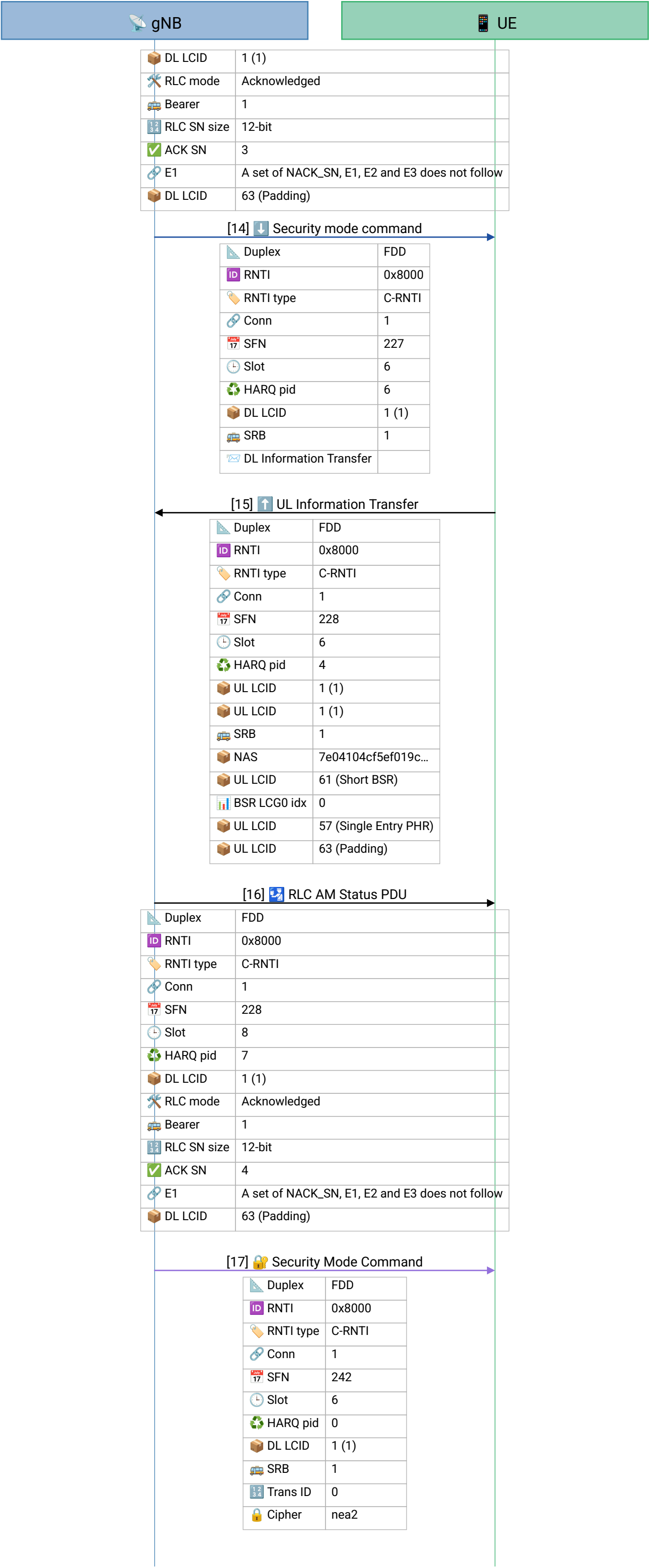


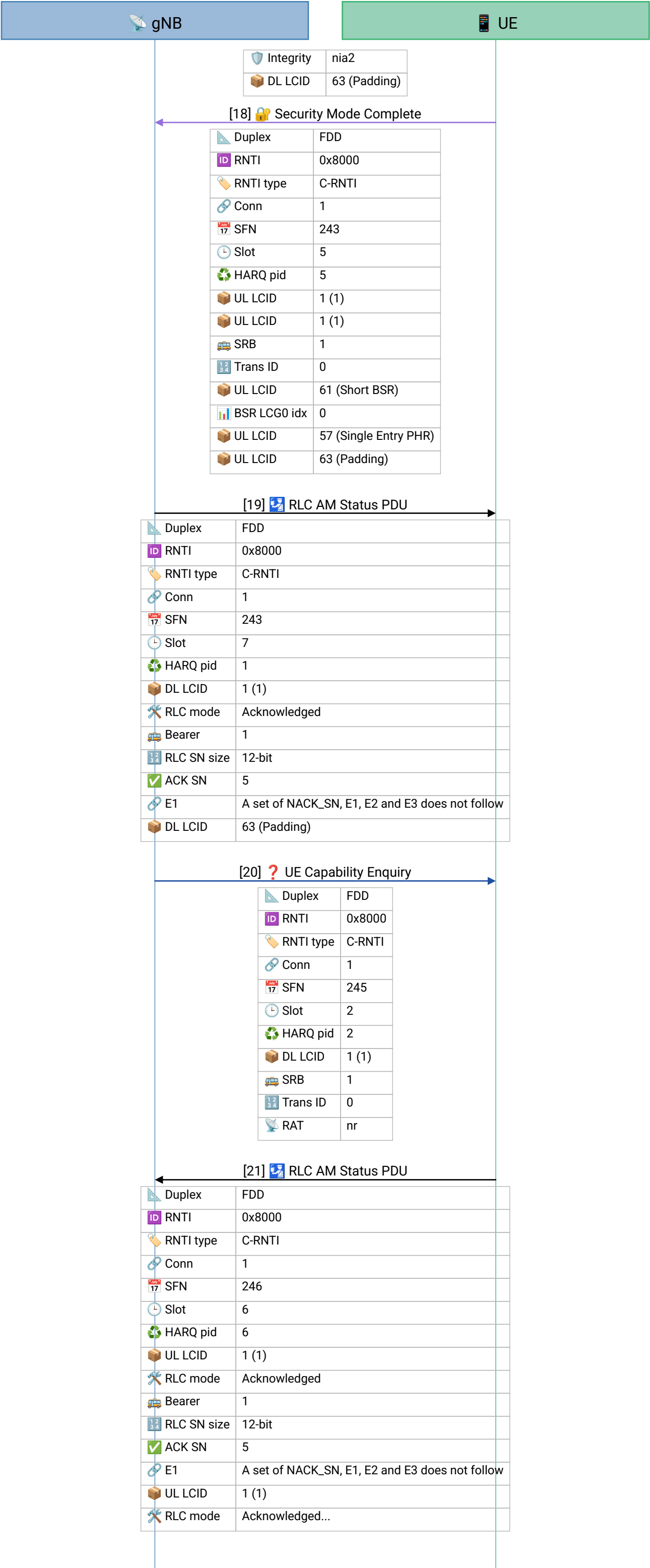
**[Frame 10]** RLC-AM Status PDU, ACK\_SN = 2 – the gNB has now taken the Authentication response.

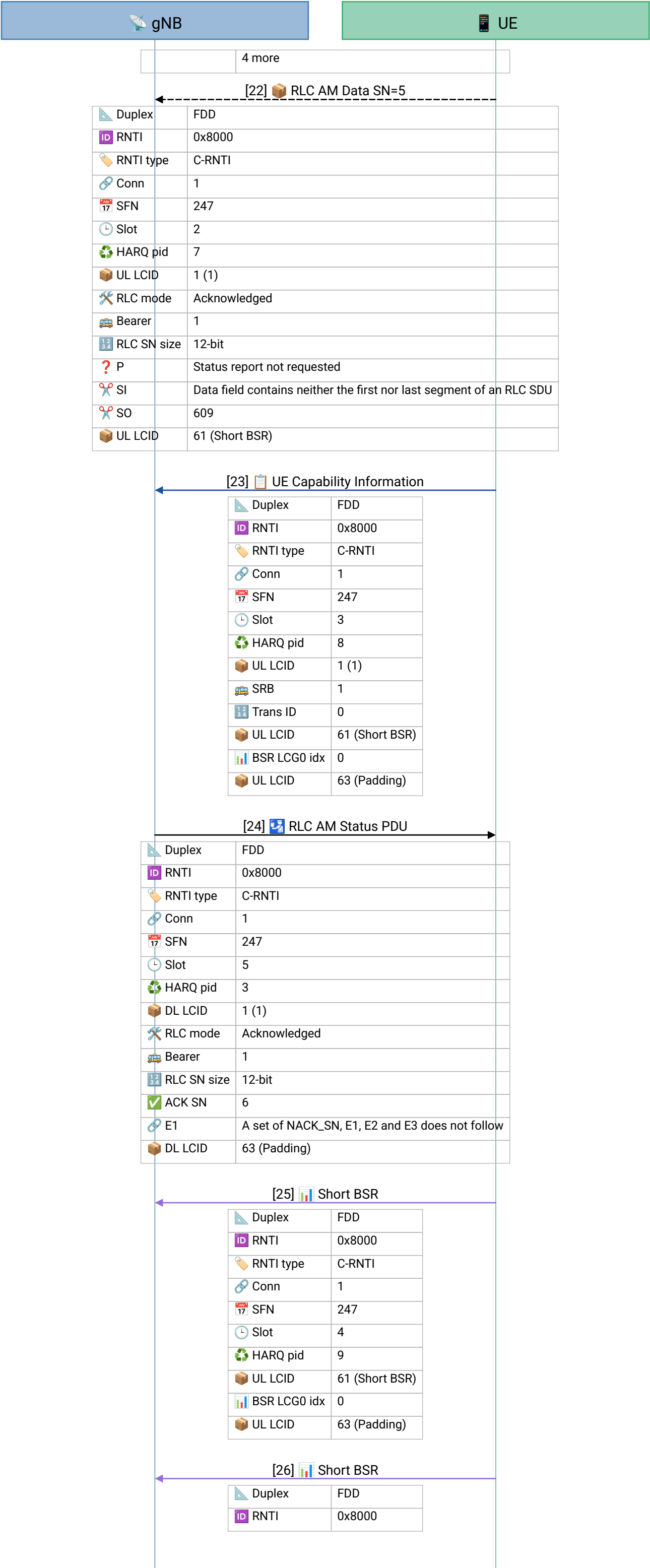
**[Frame 11] Phase 2 – NAS (core-network) security.** NAS Security mode command from the AMF (security-header type 3, "integrity protected with a new 5G NAS security context"). This activates *NAS-layer* ciphering and integrity – a security context that is entirely separate from the radio-layer one the gNB will set up later. Keep that separation in mind: it is the reason parts of this trace stay unreadable even after we apply the radio keys.

**[Frame 12]** NAS Security mode complete from the UE (security-header type 4, "integrity protected and ciphered with a new NAS context"). This is the first *NAS-ciphered* message in the capture. Its body is encrypted with the NAS keys — which we do **not** have — so the inner message type is opaque here.

**[Frame 13]** RLC-AM Status PDU on SRB1, ACK\_SN = 3.







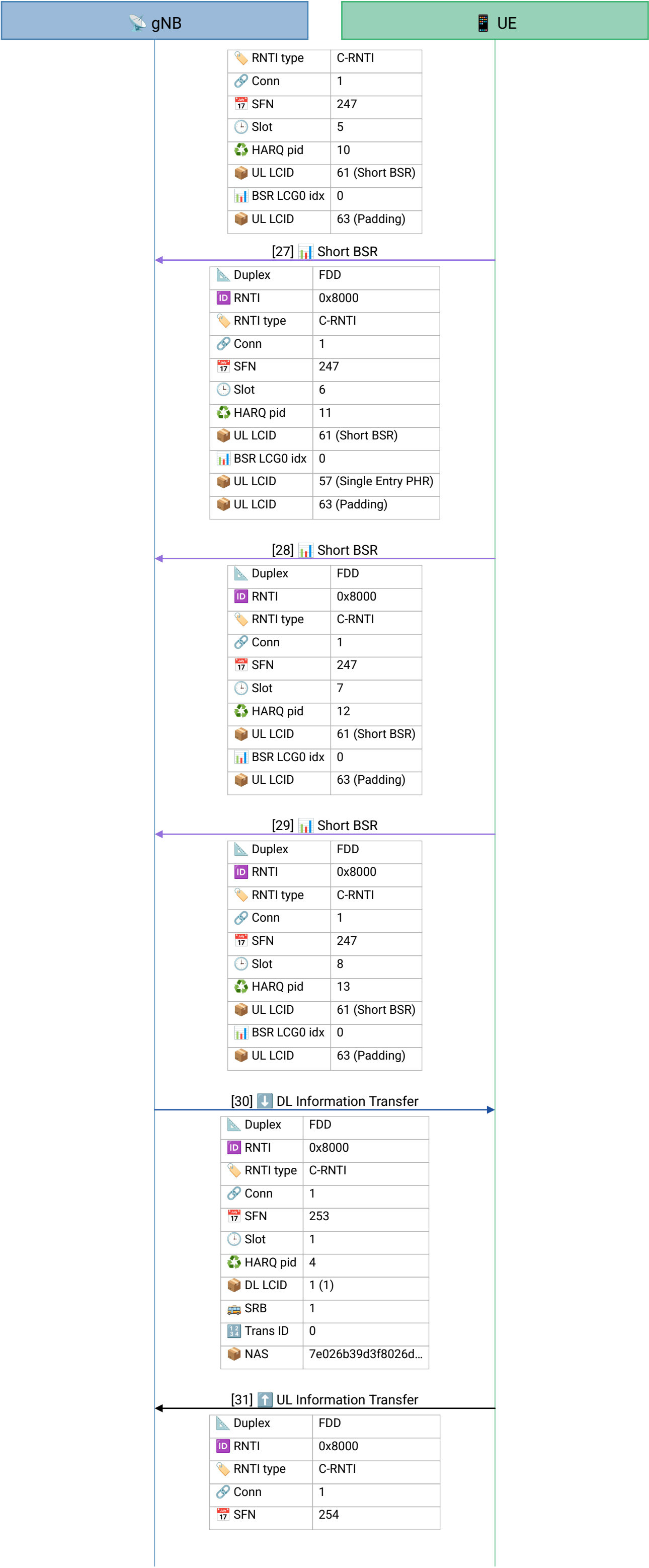
**[Frame 22]** RLC-AM Data PDU on SRB1 ( SN 5 ) , a non-first/non-last segment ( SO = 609 ) of the segmented UE Capability Information. RLC-AM splits a large SDU and reassembles it at the receiver using the Segment Offset.

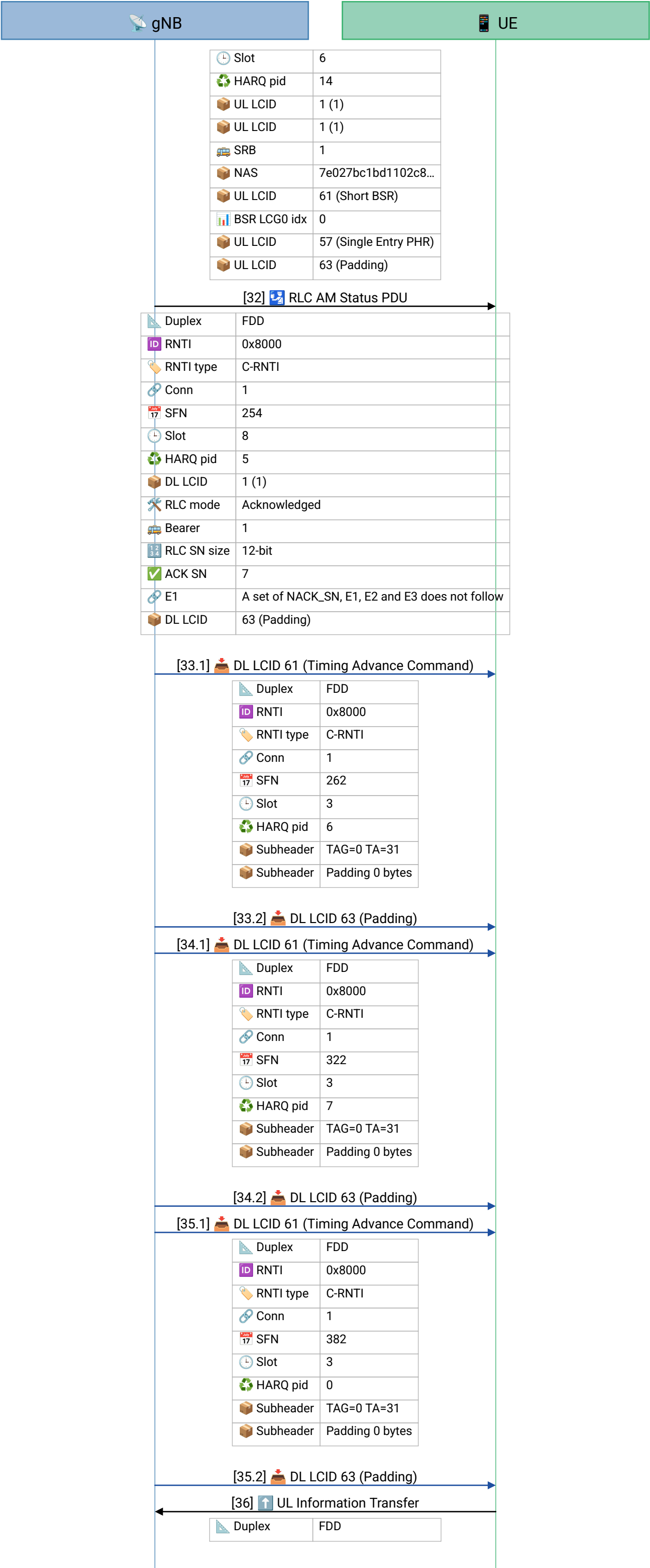
**[Frame 23] UE Capability Information.** The UE returns its capability set. Among the R16 features it advertises is `LoggedMeasurements-r16: supported` – the UE can perform logged Minimization-of-Drive-Tests measurements. (Only the *capability* appears; the network never configures an actual MDT logging session in this trace.)

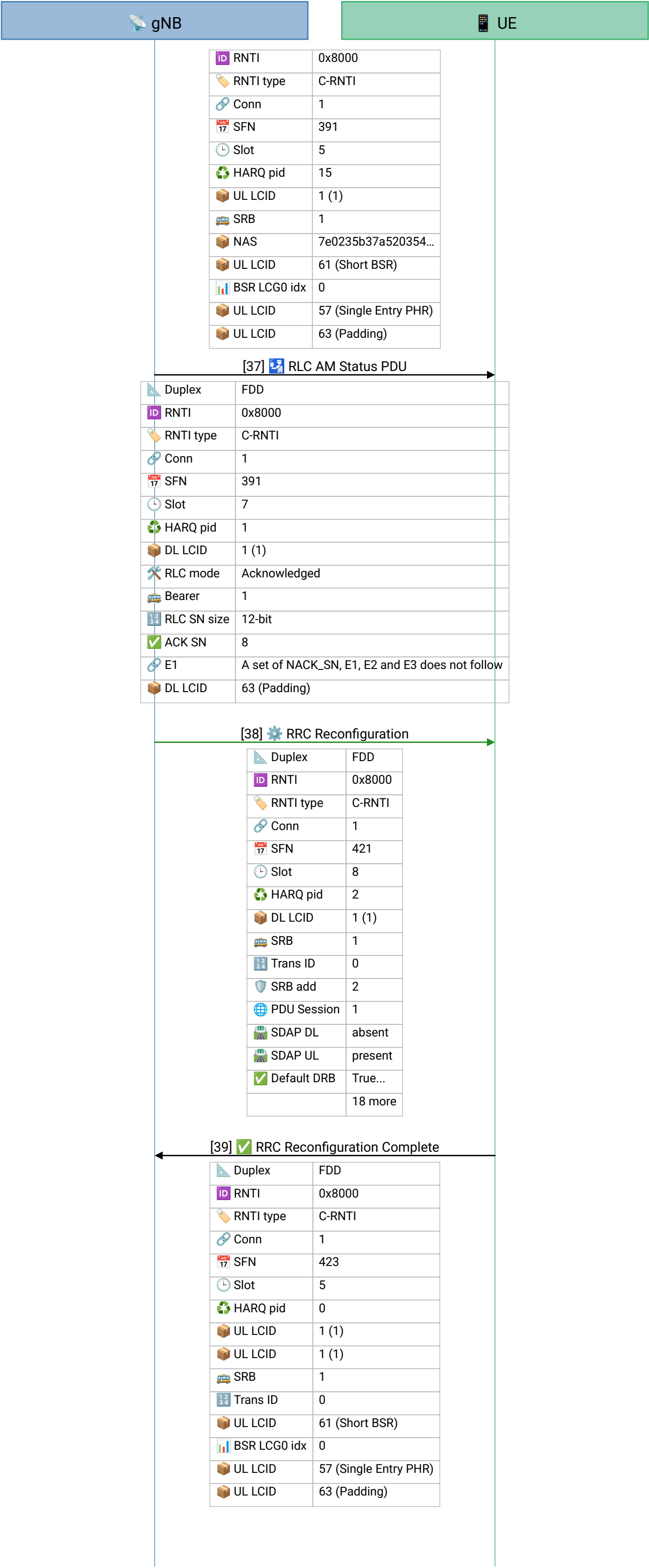
**[Frame 24]** RLC-AM Status PDU, ACK\_SN = 6 – the gNB has reassembled the capability report.

**[Frame 25]** Short Buffer Status Report: the UE tells the scheduler how much uplink data is queued for one Logical Channel Group. Index 0 here means the buffer has effectively drained.

**[Frame 26]** Short BSR – buffer-status housekeeping as the UE's uplink queue empties.





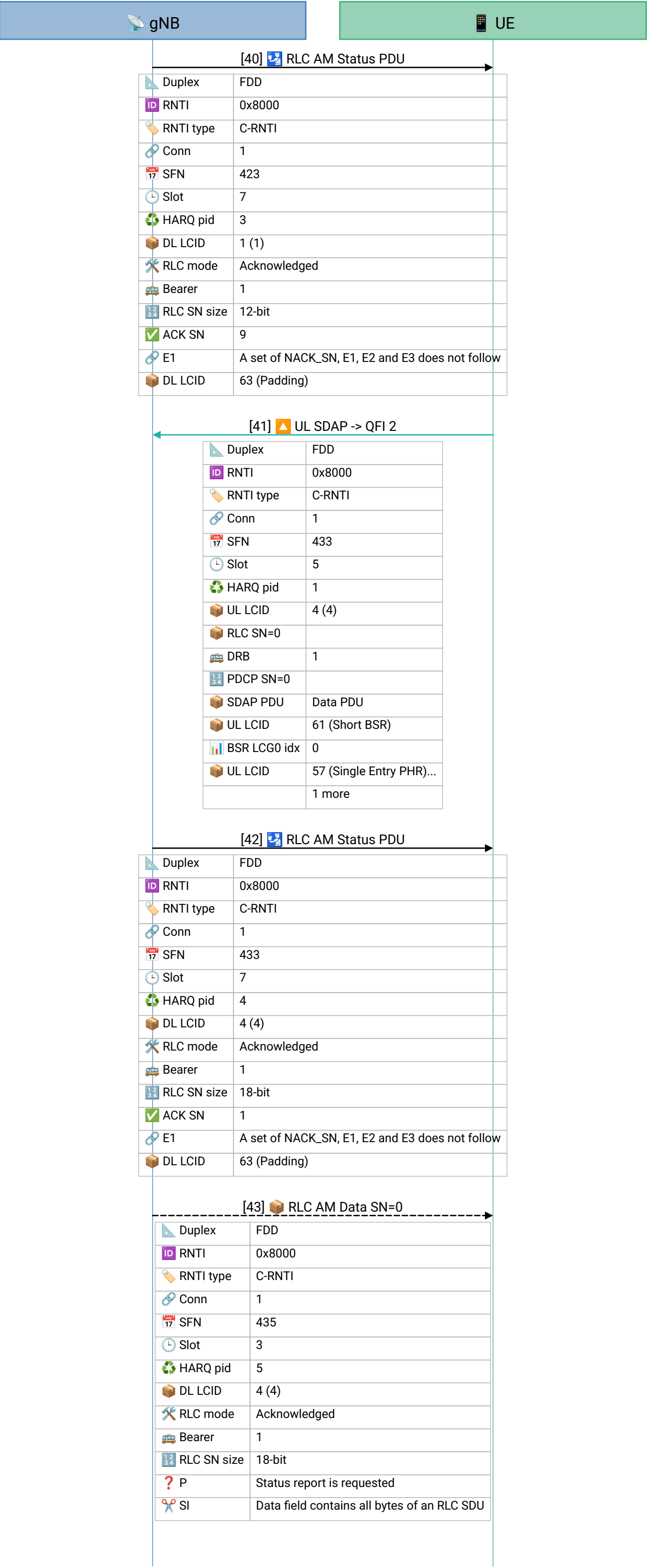


encryption.

**[Frame 37]** RLC-AM Status PDU on SRB1, ACK\_SN = 8.

**[Frame 38] Phase 5 – building the data radio bearer.** RRC Reconfiguration, the pivotal control frame. It adds SRB2 and a data radio bearer DRB 1 on LCID 4, and maps a PDU session's QoS flow onto it: sdap-Config with the SDAP downlink header **absent** and the uplink header **present**, default DRB, QFI 2. PDCP uses an 18-bit sequence number in both directions, ROHC off; RLC-AM is configured with t-PollRetransmit = 80 ms, pollPDU = 32768, pollByte = 750 kB. It also carries a piggybacked NAS message – but that NAS PDU is type 2 (NAS-ciphered), so its contents stay opaque even though the RRC around it is now readable.

**[Frame 39]** RRC Reconfiguration Complete. The UE has applied the new bearer configuration; DRB 1 is live and user data can now flow.

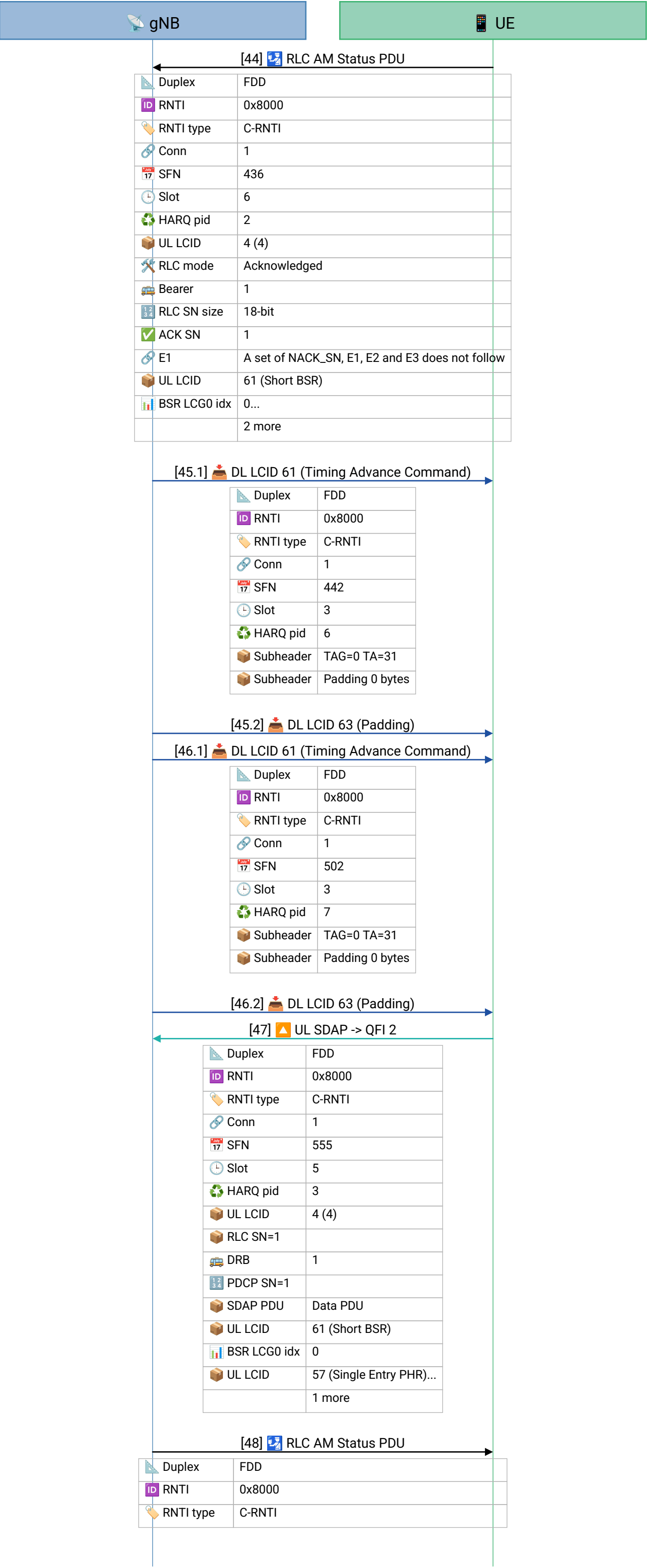


**[Frame 40]** RLC-AM Status PDU on SRB1, ACK\_SN = 9 – acknowledging the reconfiguration exchange.

**[Frame 41] Phase 6 – user-plane data on the DRB.** The first uplink SDAP Data PDU on DRB 1 . The one-byte SDAP header (TS 37.324) carries the QFI = 2 the UE stamped on its IP packet, so the network knows which QoS flow this belongs to. This – and everything below the SDAP header – only becomes visible because the AS keys deciphered PDCP; without them this is an opaque ciphertext blob. Underneath sits IPv6 (here the start of IPv6 setup); the deeper look at what the user plane actually carries is the subject of the companion decryption article.

**[Frame 42]** RLC-AM Status PDU on the DRB ( ACK\_SN = 1 , 18-bit SN) – the data bearer has its own ARQ, distinct from SRB1 's.

**[Frame 43]** Downlink RLC-AM Data PDU on DRB 1 ( SN 0 ), a complete SDU, with the Poll bit set to demand an immediate Status PDU back.



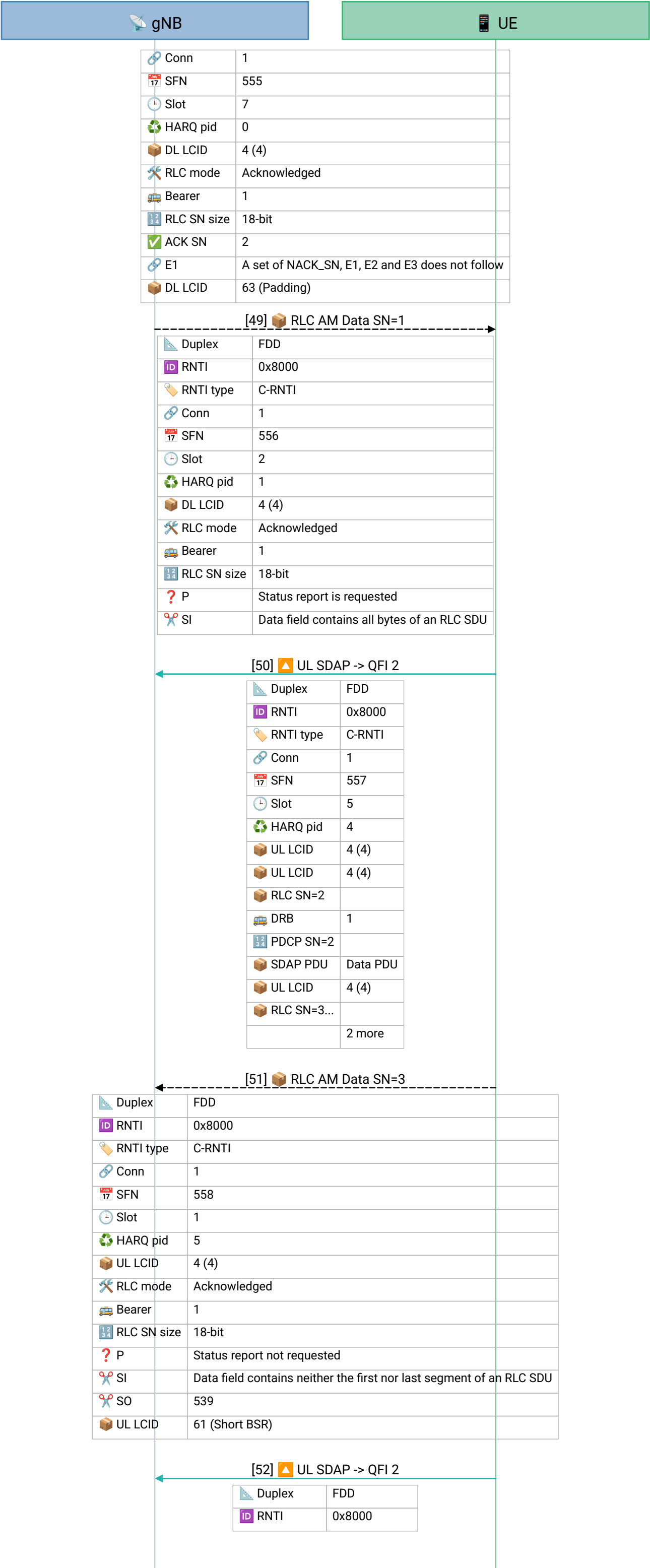
**[Frame 44]** RLC-AM Status PDU (uplink), ACK\_SN = 1 on the DRB – the UE confirms the downlink data.

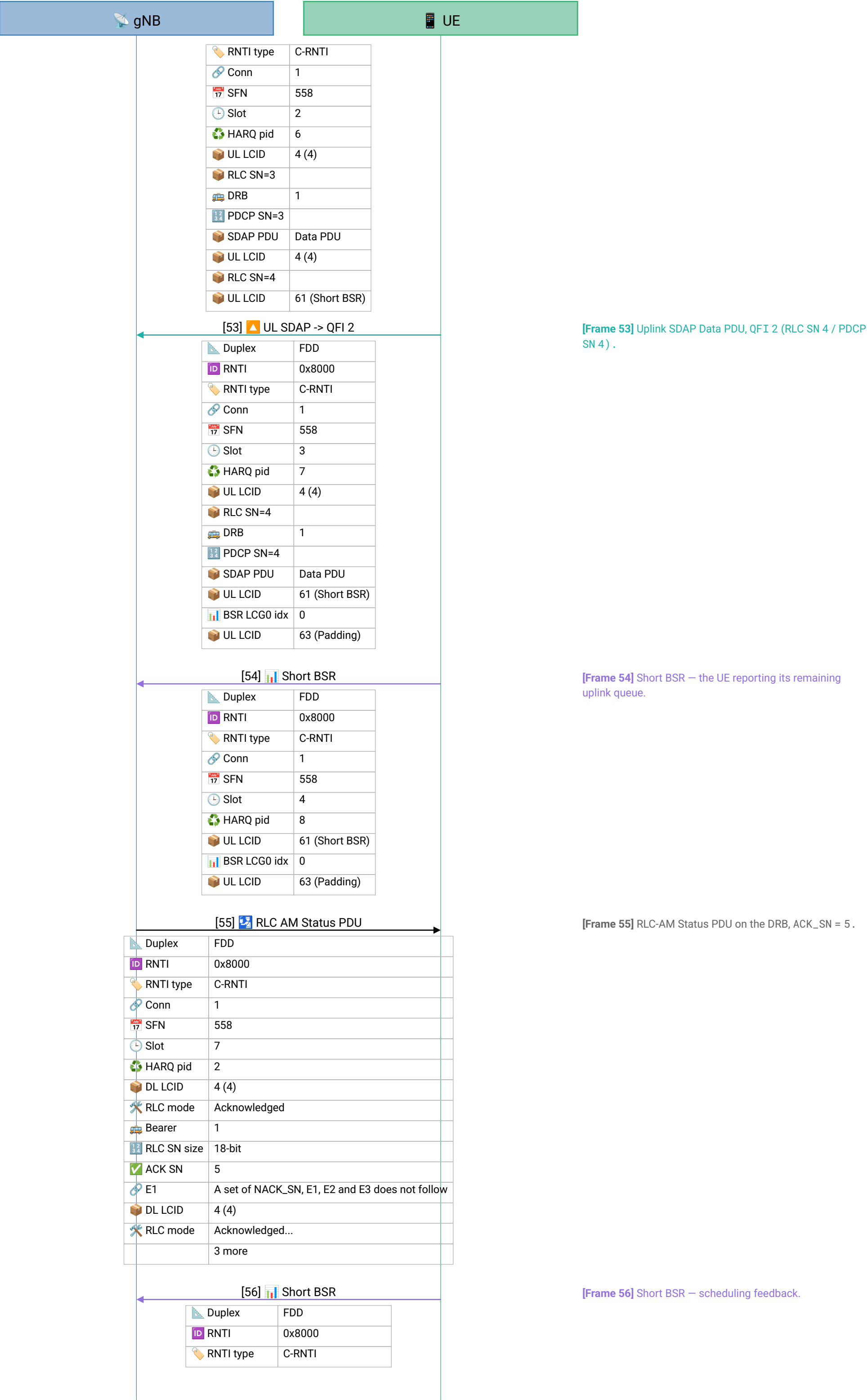
**[Frame 45.1]** MAC Timing Advance Command – link upkeep between data bursts.

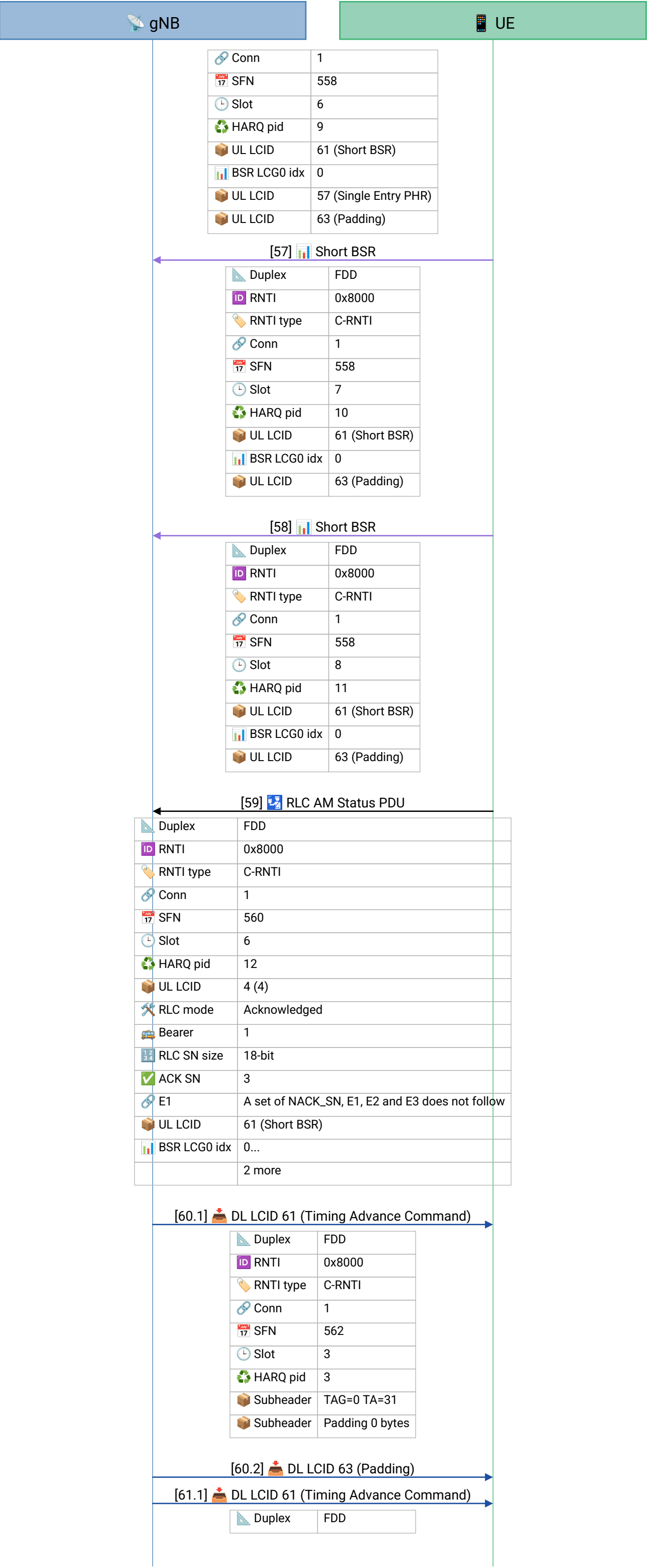
**[Frame 46.1]** MAC Timing Advance Command – link upkeep.

**[Frame 47]** Uplink SDAP Data PDU on DRB 1, QFI 2 (RLC SN 1, PDCP SN 1) . User-plane traffic continues on the deciphered bearer.

**[Frame 48]** RLC-AM Status PDU on the DRB, ACK\_SN = 2 .







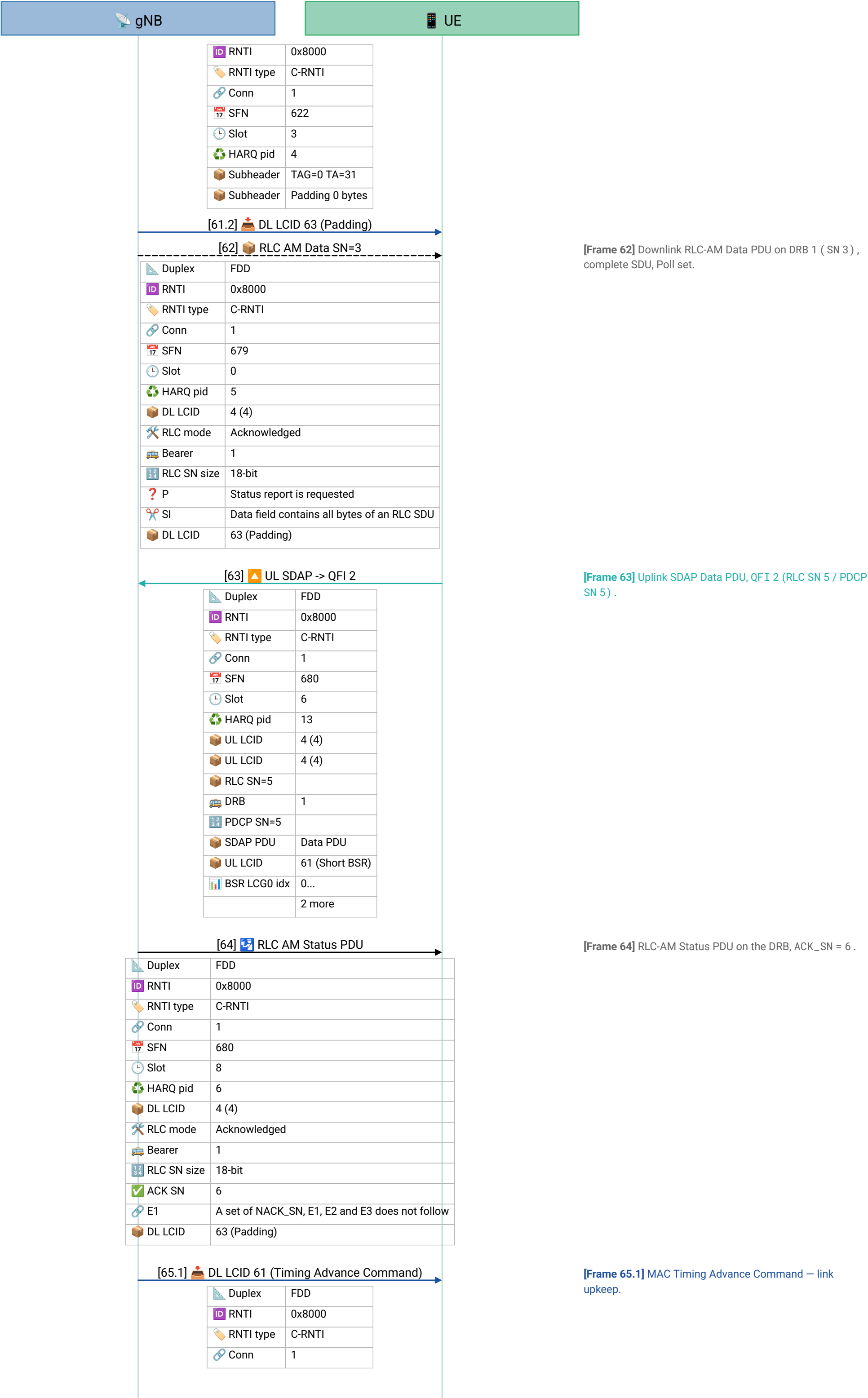
**[Frame 57]** Short BSR – scheduling feedback.

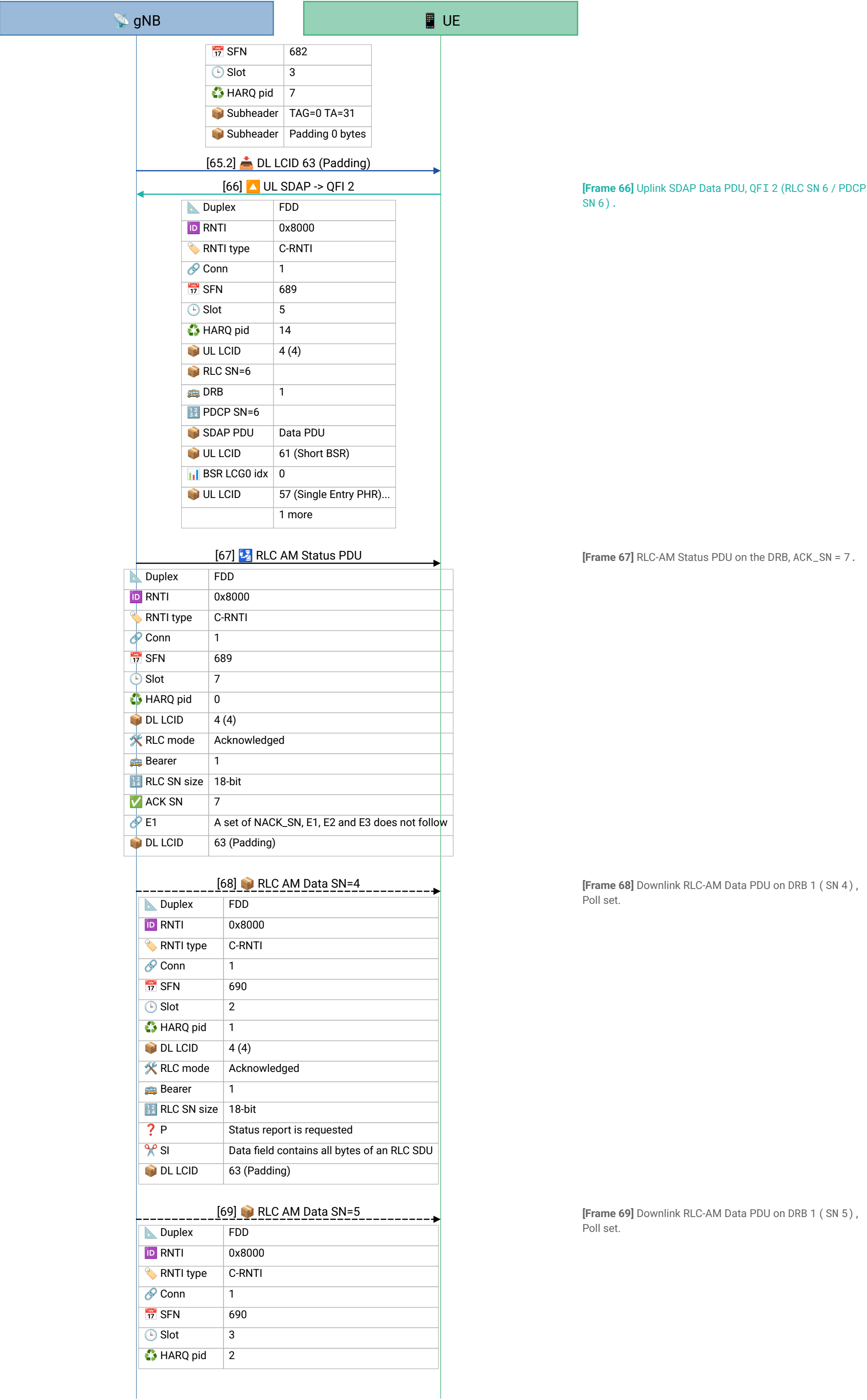
**[Frame 58]** Short BSR – scheduling feedback.

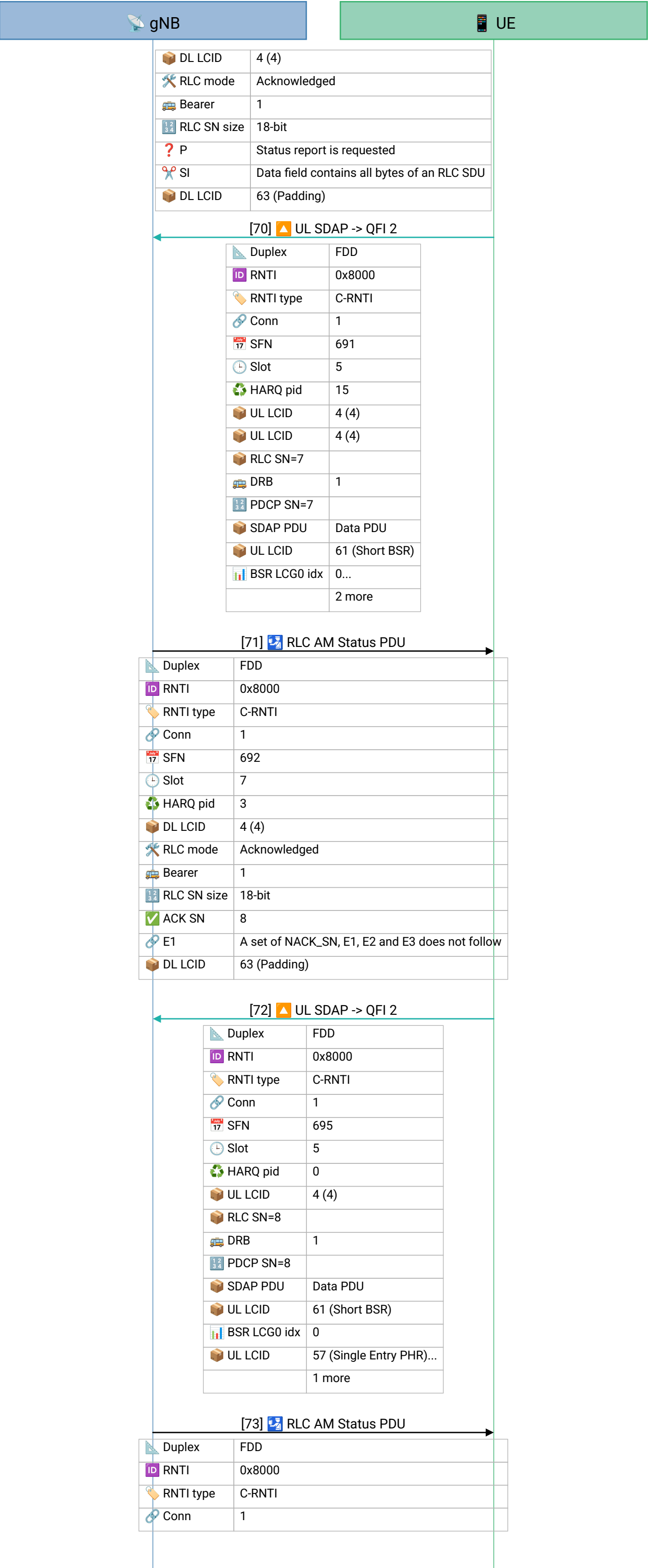
**[Frame 59]** RLC-AM Status PDU (uplink) on the DRB, ACK\_SN = 3.

**[Frame 60.1]** MAC Timing Advance Command – link  
upkeep.

**[Frame 61.1]** MAC Timing Advance Command – link upkeep during a ~0.6 s data lull.





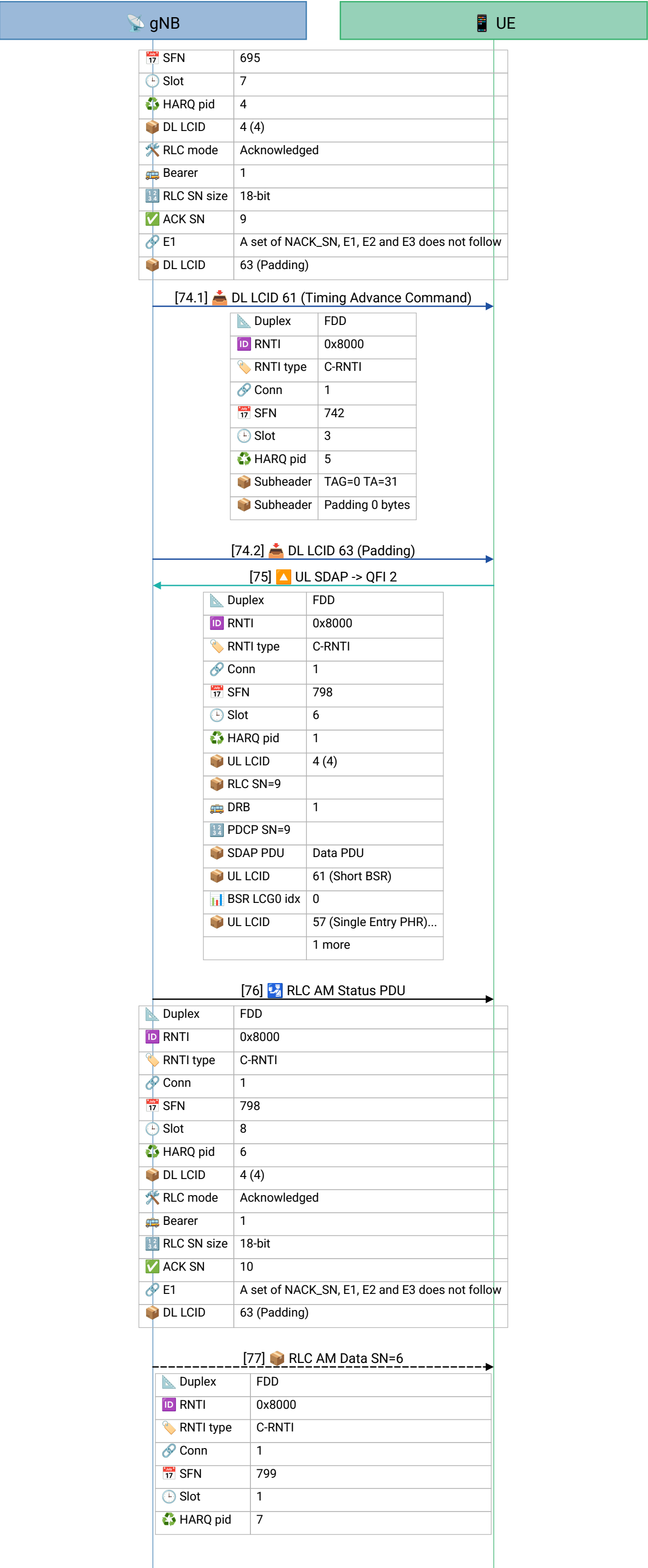


**[Frame 70]** Uplink SDAP Data PDU, QFI 2 (RLC SN 7 / PDCP SN 7) .

**[Frame 71]** RLC-AM Status PDU on the DRB, ACK\_SN = 8 .

**[Frame 72]** Uplink SDAP Data PDU, QFI 2 (RLC SN 8 / PDCP SN 8) . (Work-item-19757 flags this frame for a payload-length warning in the dissector — a decode nit, not a signaling problem.)

**[Frame 73]** RLC-AM Status PDU on the DRB, ACK\_SN = 9 .



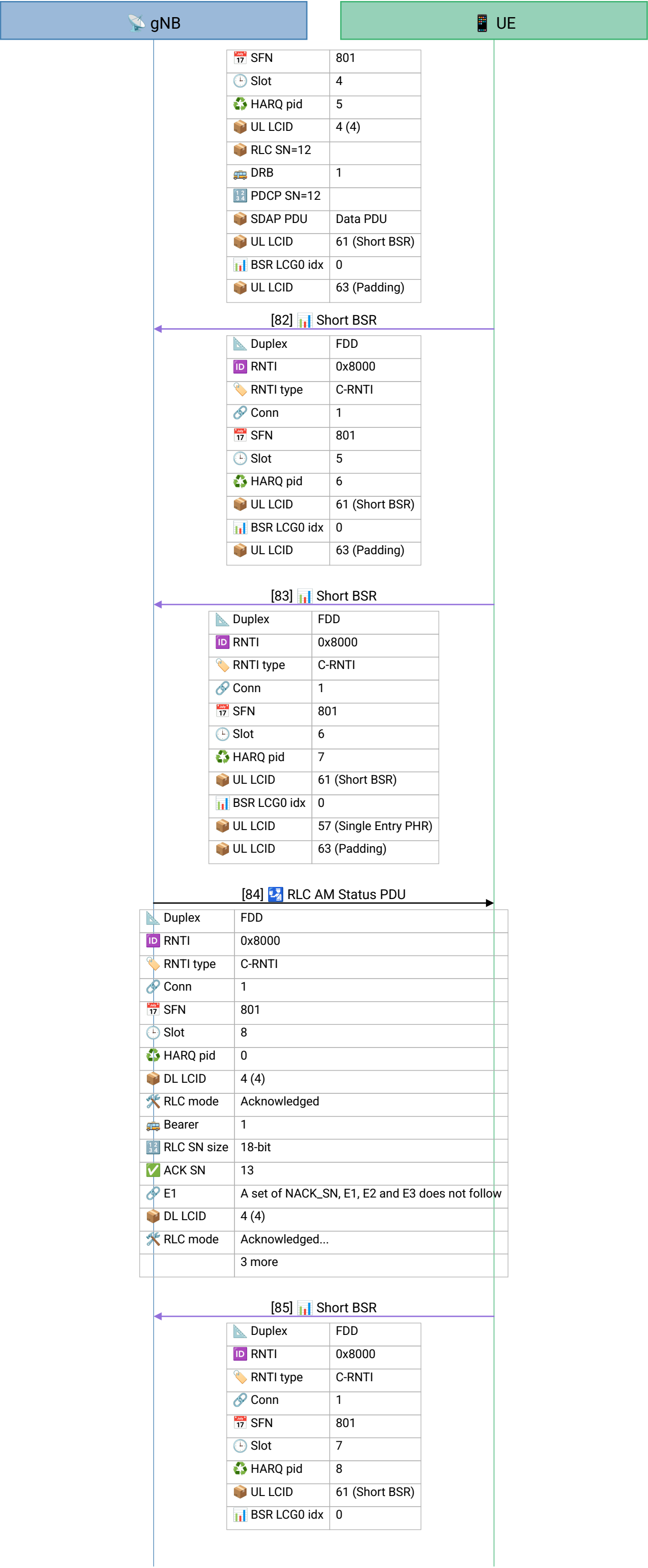
**[Frame 74.1]** MAC Timing Advance Command – link upkeep.

**[Frame 75]** Uplink SDAP Data PDU, QFI 2 (RLC SN 9 / PDCP SN 9) .

**[Frame 76]** RLC-AM Status PDU on the DRB, ACK\_SN = 10 .

**[Frame 77]** Downlink RLC-AM Data PDU on DRB 1 ( SN 6 ) ,  
Poll set.



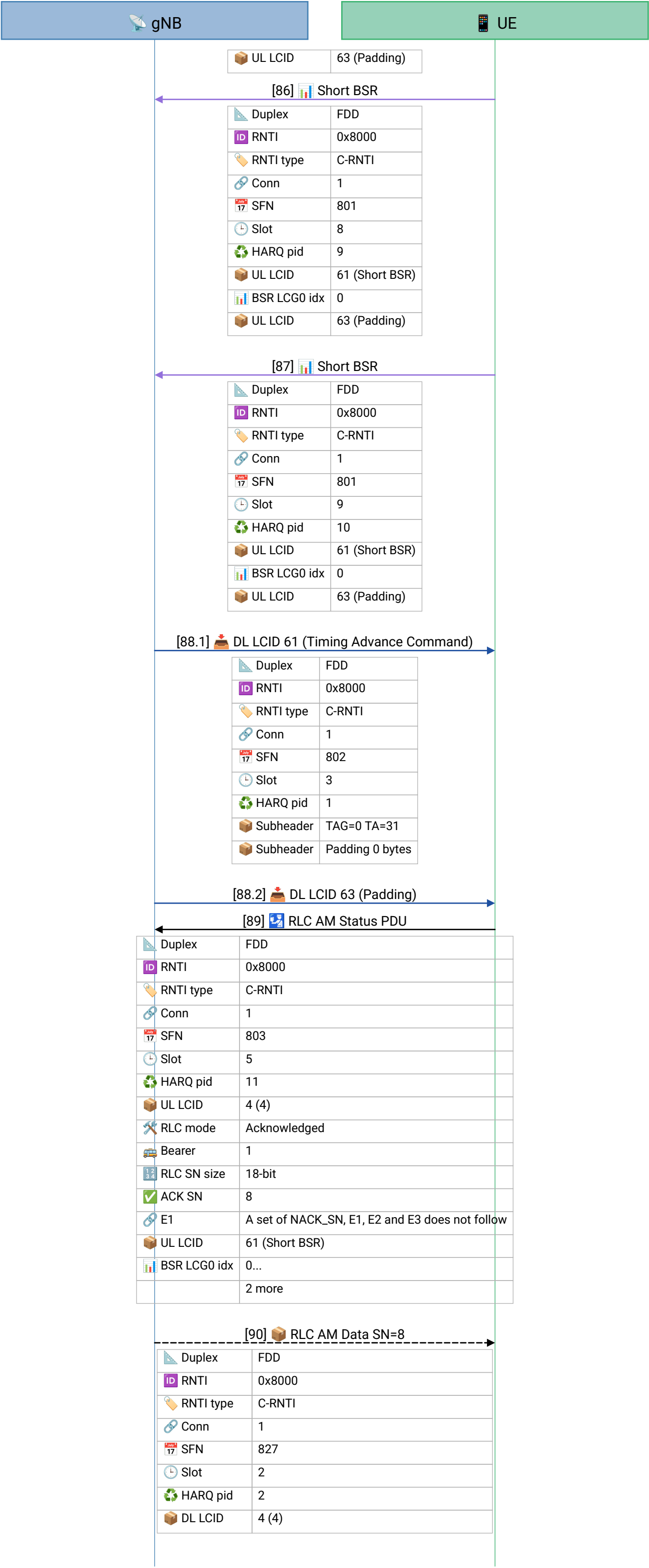


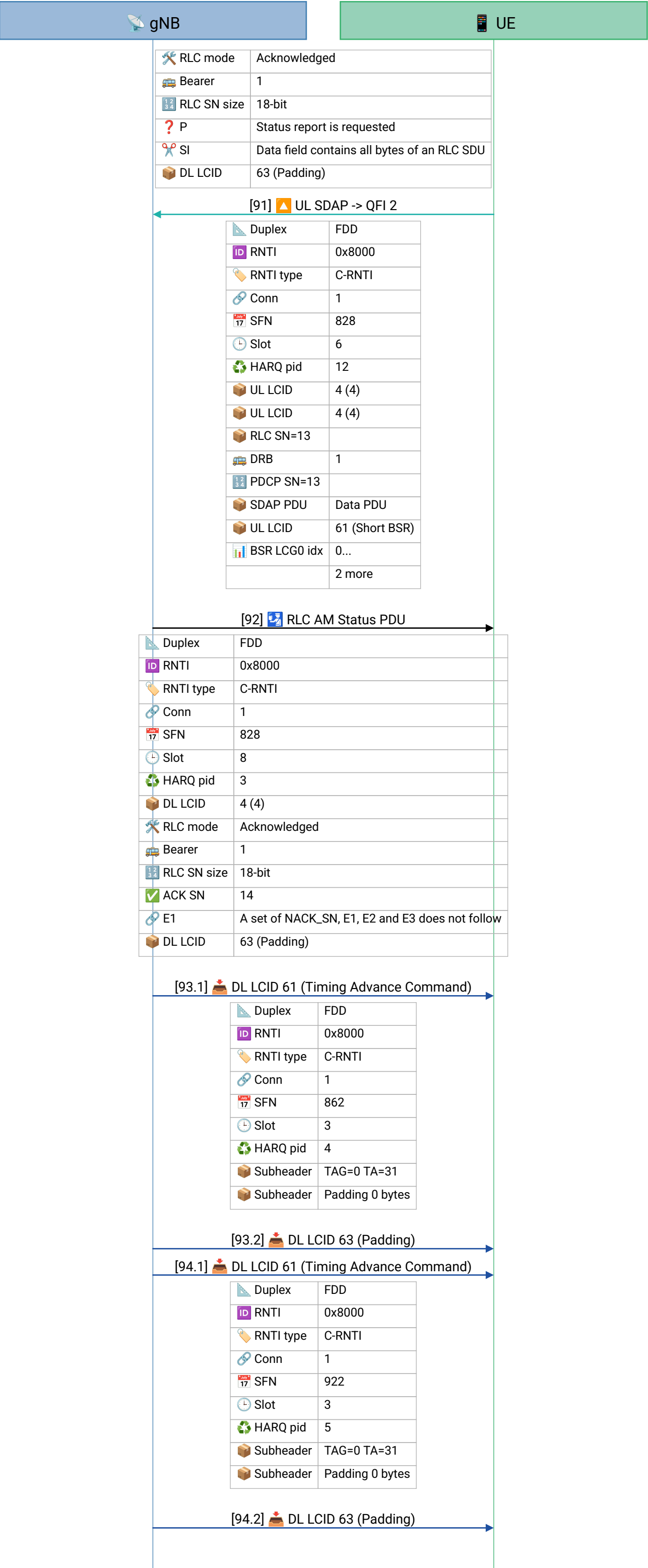
**[Frame 82]** Short BSR – scheduling feedback.

**[Frame 83]** Short BSR – scheduling feedback.

**[Frame 84]** RLC-AM Status PDU on the DRB, ACK\_SN = 13 .

**[Frame 85]** Short BSR – scheduling feedback.



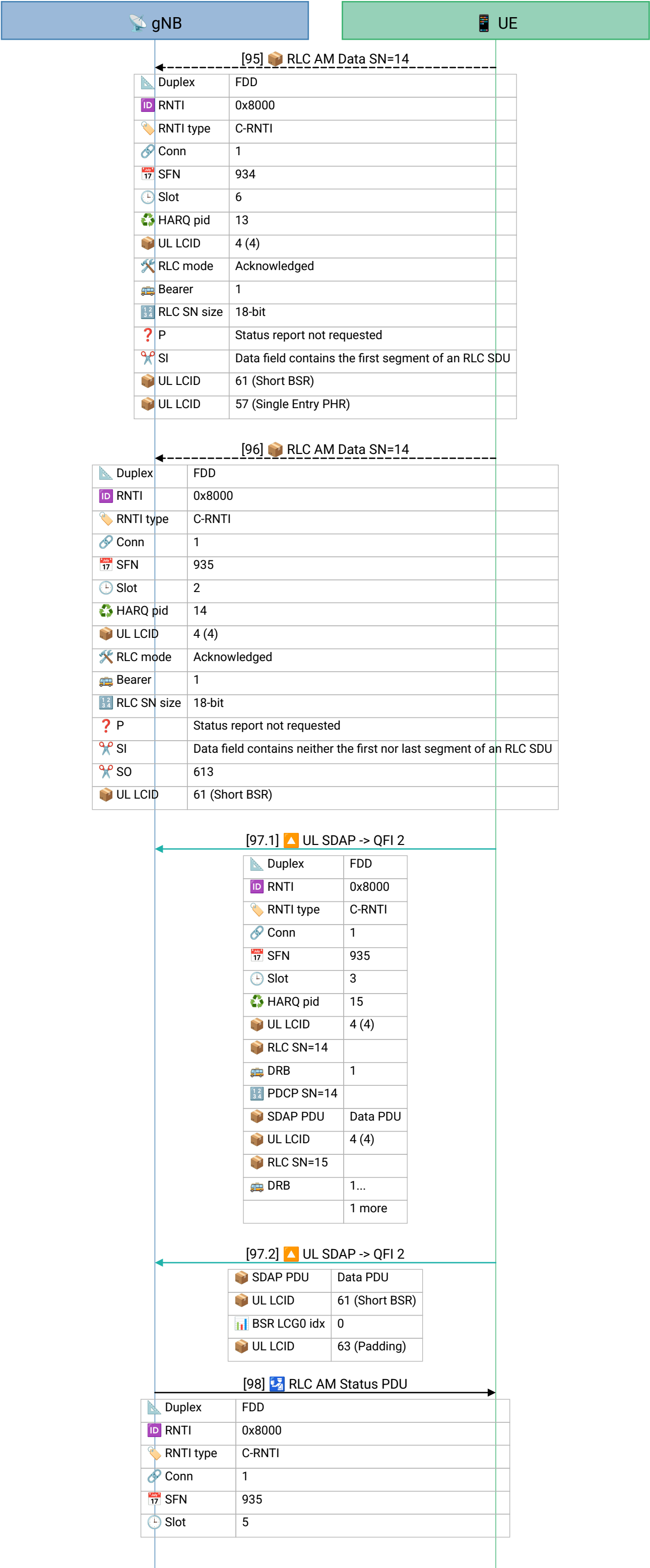


**[Frame 91]** Uplink SDAP Data PDU, QFI 2 (RLC SN 13 / PDCP SN 13) .

**[Frame 92]** RLC-AM Status PDU on the DRB, ACK\_SN = 14 .

**[Frame 93.1]** MAC Timing Advance Command – link upkeep.

**[Frame 94.1]** MAC Timing Advance Command – link upkeep.





|                                                                                               |                                                 |  |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------|--|
|  HARQ pid    | 6                                               |  |
|  DL LCID     | 4 (4)                                           |  |
|  RLC mode    | Acknowledged                                    |  |
|  Bearer      | 1                                               |  |
|  RLC SN size | 18-bit                                          |  |
|  ACK SN      | 16                                              |  |
|  E1          | A set of NACK_SN, E1, E2 and E3 does not follow |  |
|  DL LCID     | 63 (Padding)                                    |  |

[99]  Short BSR

|                                                                                                |                |
|------------------------------------------------------------------------------------------------|----------------|
|  Duplex       | FDD            |
|  RNTI         | 0x8000         |
|  RNTI type    | C-RNTI         |
|  Conn         | 1              |
|  SFN          | 935            |
|  Slot         | 4              |
|  HARQ pid     | 0              |
|  UL LCID      | 61 (Short BSR) |
|  BSR LCG0 idx | 0              |
|  UL LCID     | 63 (Padding)   |

[Frame 99] Short BSR – scheduling feedback.

[100]  Short BSR

|                                                                                                  |                |
|--------------------------------------------------------------------------------------------------|----------------|
|  Duplex       | FDD            |
|  RNTI         | 0x8000         |
|  RNTI type    | C-RNTI         |
|  Conn         | 1              |
|  SFN          | 935            |
|  Slot         | 5              |
|  HARQ pid     | 1              |
|  UL LCID      | 61 (Short BSR) |
|  BSR LCG0 idx | 0              |
|  UL LCID      | 63 (Padding)   |

[Frame 100] Short BSR – scheduling feedback.

[101]  Short BSR

|                                                                                                  |                       |
|--------------------------------------------------------------------------------------------------|-----------------------|
|  Duplex       | FDD                   |
|  RNTI         | 0x8000                |
|  RNTI type    | C-RNTI                |
|  Conn         | 1                     |
|  SFN          | 935                   |
|  Slot         | 6                     |
|  HARQ pid     | 2                     |
|  UL LCID      | 61 (Short BSR)        |
|  BSR LCG0 idx | 0                     |
|  UL LCID      | 57 (Single Entry PHR) |
|  UL LCID      | 63 (Padding)          |

[Frame 101] Short BSR – scheduling feedback.

[102]  RLC AM Data SN=9

|                                                                                                 |                                             |
|-------------------------------------------------------------------------------------------------|---------------------------------------------|
|  Duplex      | FDD                                         |
|  RNTI        | 0x8000                                      |
|  RNTI type   | C-RNTI                                      |
|  Conn        | 1                                           |
|  SFN         | 935                                         |
|  Slot        | 8                                           |
|  HARQ pid    | 7                                           |
|  DL LCID     | 4 (4)                                       |
|  RLC mode    | Acknowledged                                |
|  Bearer      | 1                                           |
|  RLC SN size | 18-bit                                      |
|  P           | Status report is requested                  |
|  SI          | Data field contains all bytes of an RLC SDU |

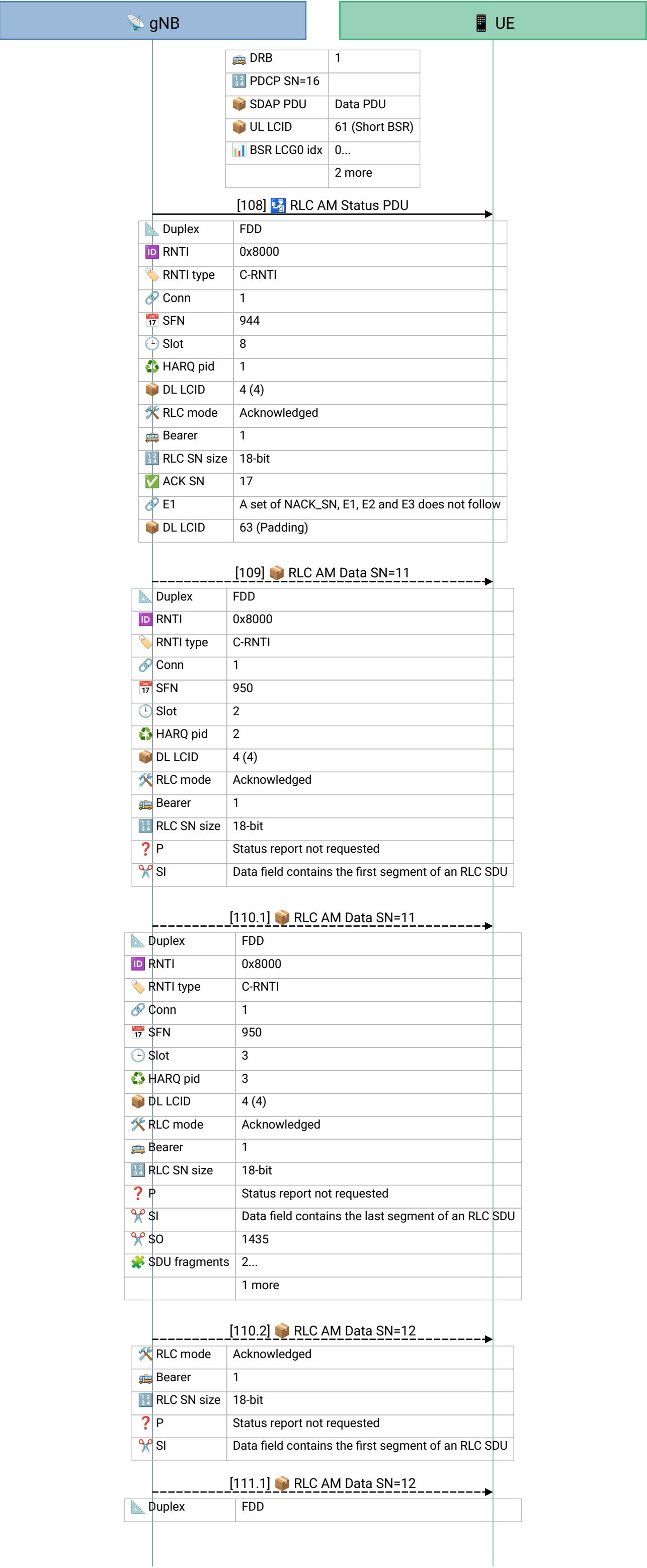
[Frame 102] Downlink RLC-AM Data PDU on DRB 1 ( SN 9 ) , complete SDU, Poll set.

[103]  Short BSR

|                                                                                               |        |
|-----------------------------------------------------------------------------------------------|--------|
|  Duplex    | FDD    |
|  RNTI      | 0x8000 |
|  RNTI type | C-RNTI |

[Frame 103] Short BSR – scheduling feedback.



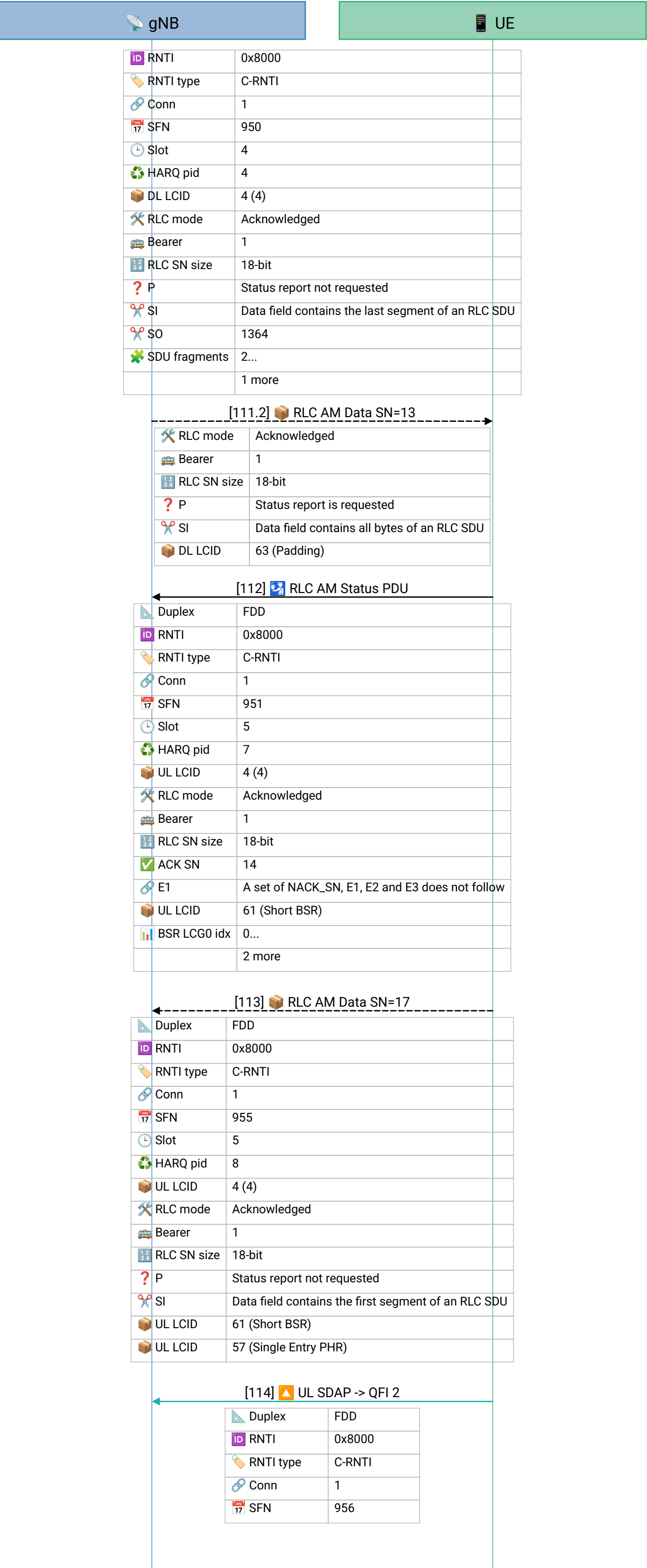


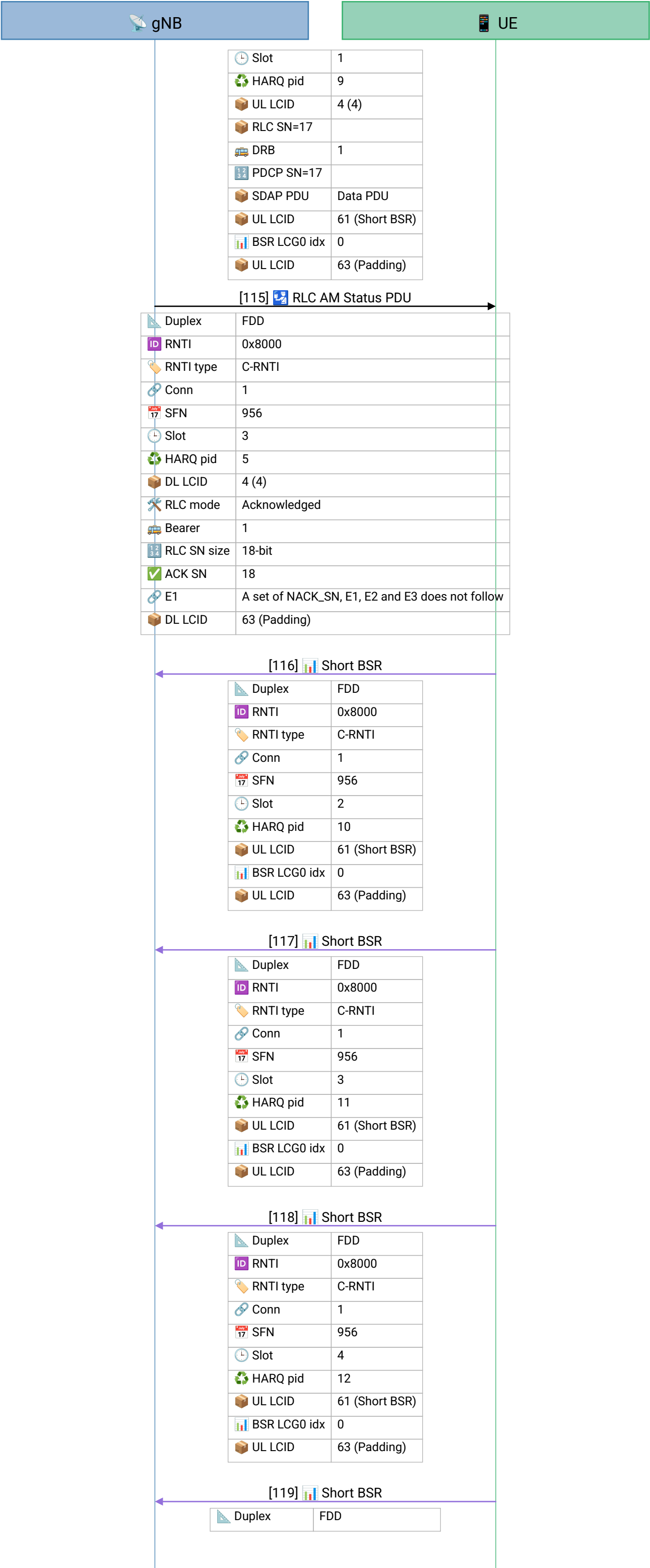
**[Frame 108]** RLC-AM Status PDU on the DRB, ACK\_SN = 17.

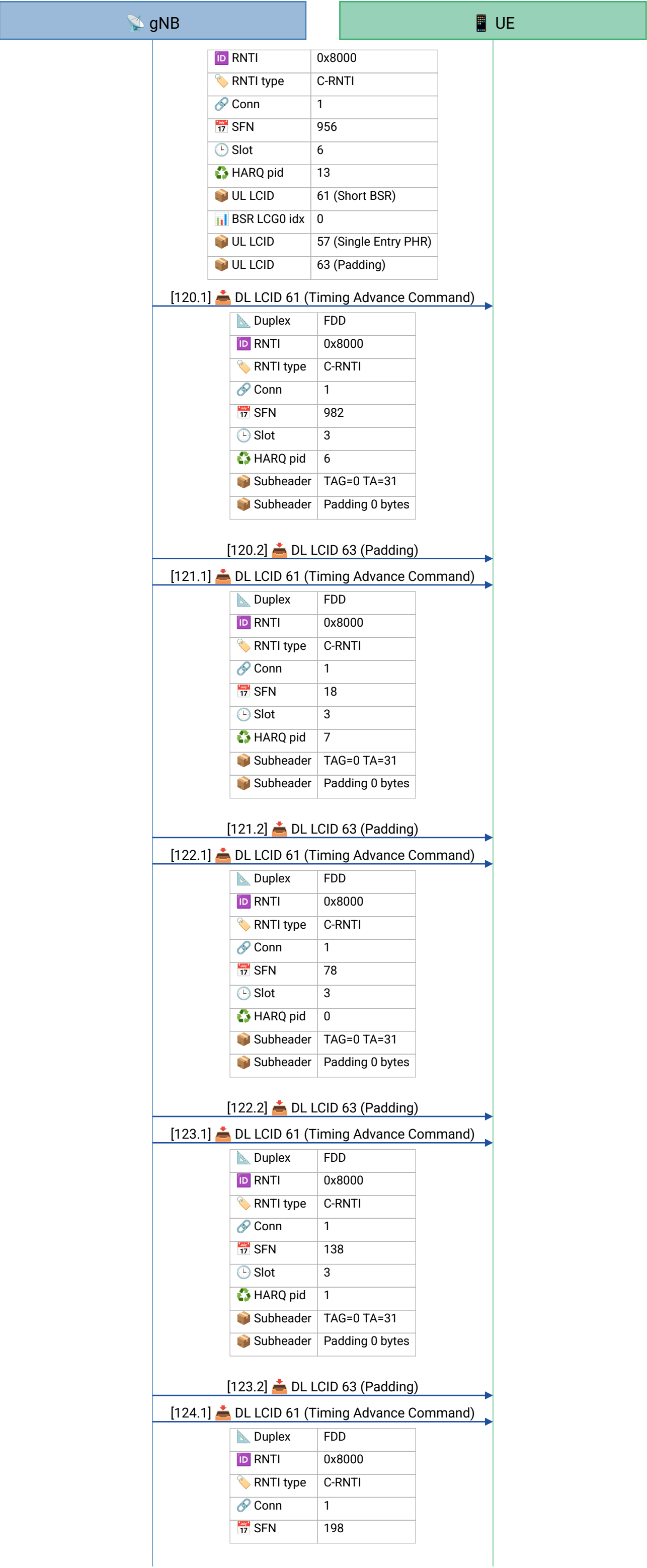
**[Frame 109]** Downlink RLC-AM Data PDU on DRB 1 ( SN 11 ), first segment of a larger SDU.

**[Frame 110.1]** Downlink RLC-AM Data PDU on DRB 1 : the last segment of SN 11 ( S0 = 1435, reassembled from 2 fragments) plus the first segment of SN 12 – two SDUs' fragments multiplexed into one transport block.

**[Frame 111.1]** Downlink RLC-AM Data PDU on DRB 1 : the last segment of SN 12 ( SO = 1364, 2 fragments) plus a complete SN 13 , Poll set.







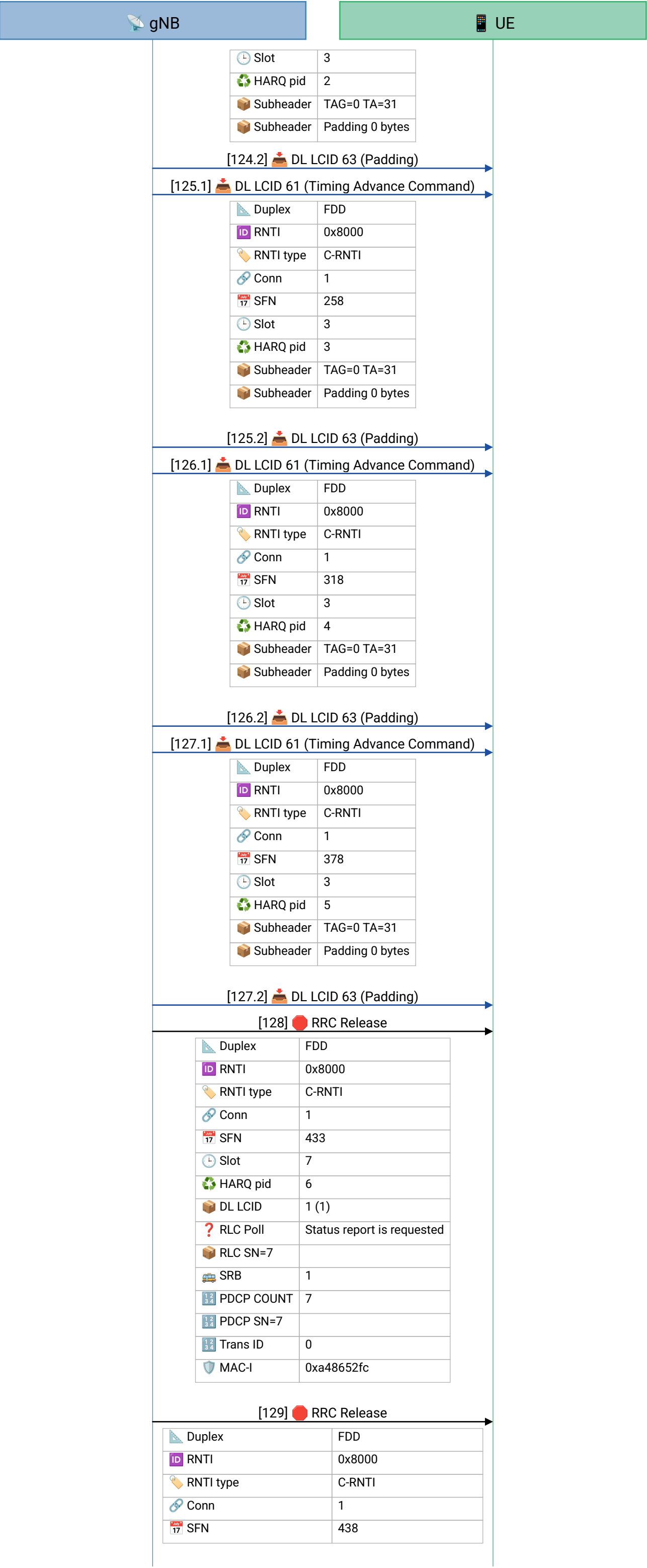
**[Frame 120.1]** MAC Timing Advance Command – link upkeep. Note the System Frame Number wraps (1023 -> 0) around here; the SFN is a 10-bit counter, so this is normal roll-over, not a gap.

**[Frame 121.1]** MAC Timing Advance Command – link upkeep.

**[Frame 122.1]** MAC Timing Advance Command – link upkeep.

**[Frame 123.1]** MAC Timing Advance Command – link upkeep.

**[Frame 124.1]** MAC Timing Advance Command – link upkeep.



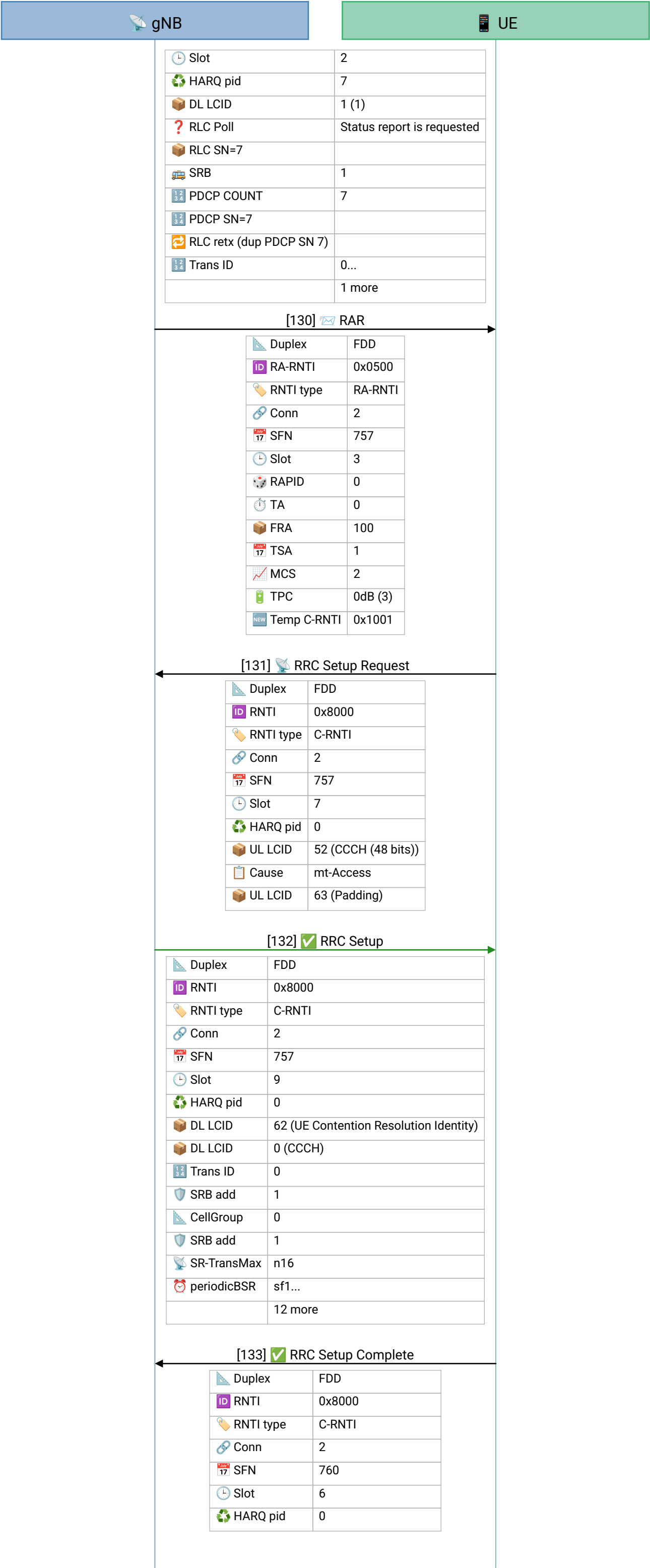
**[Frame 125.1]** MAC Timing Advance Command – link upkeep.

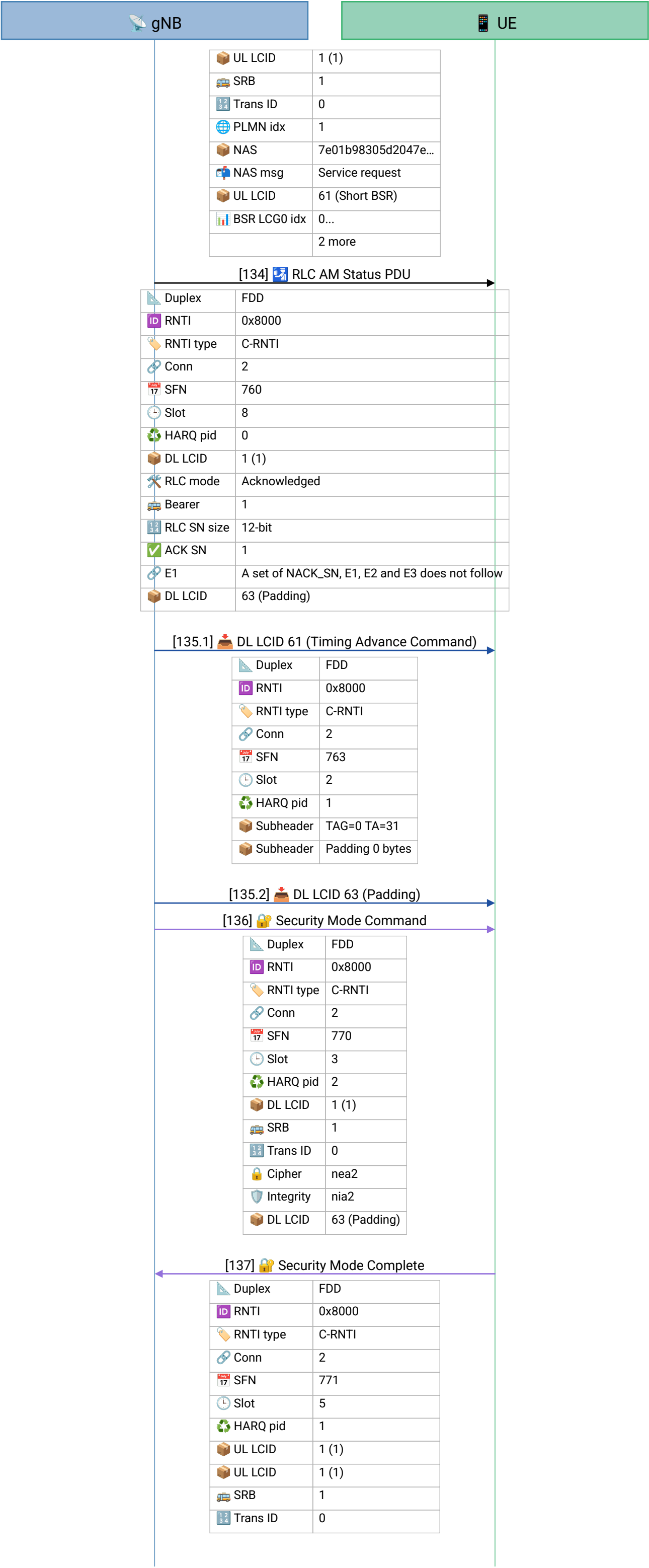
**[Frame 126.1]** MAC Timing Advance Command – link upkeep.

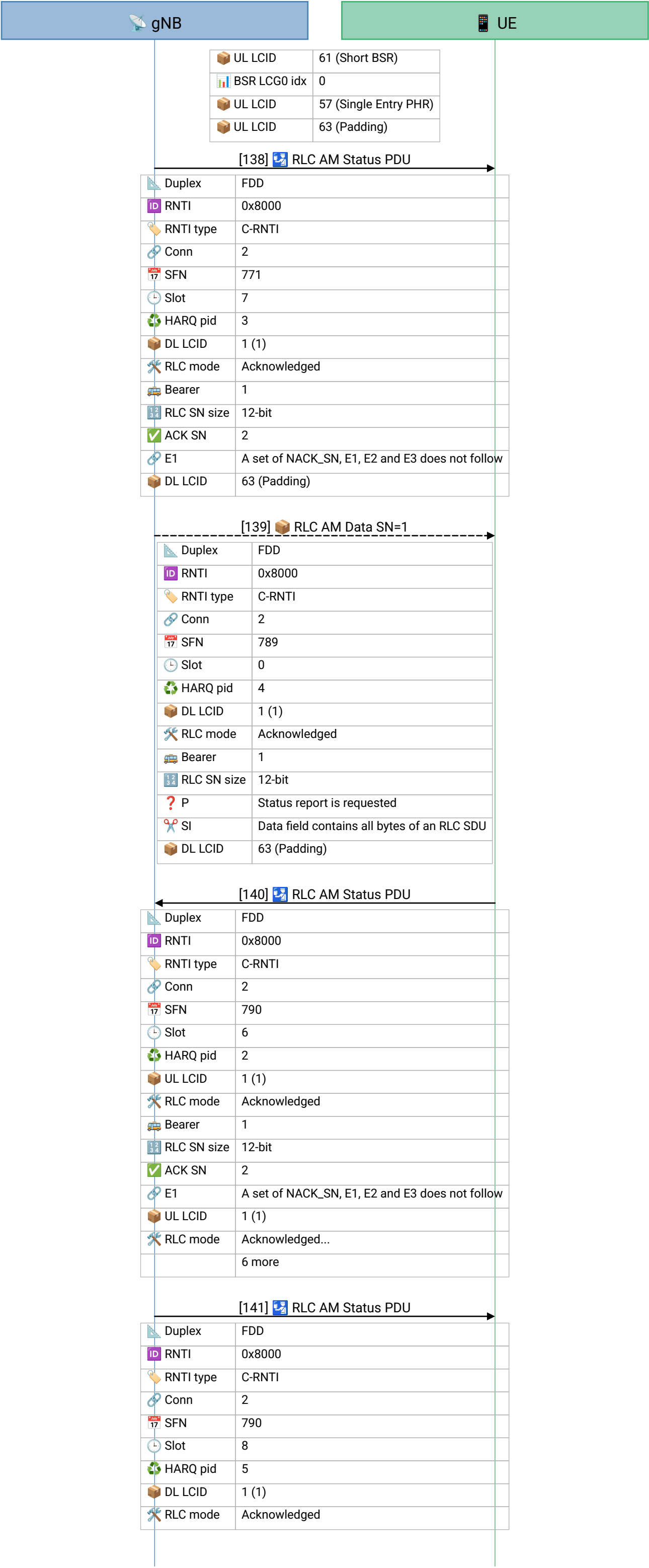
**[Frame 127.1]** MAC Timing Advance Command – the last of the periodic upkeep before the connection is torn down.

**[Frame 128] Phase 7 – releasing the connection.** RRC Release on SRB1 (PDCP SN 7, COUNT 7, integrity tag MAC-I = 0xa48652fc), with the RLC Poll bit set so the gNB expects a Status PDU confirming delivery. There is no suspendConfig, so the UE is sent to RRC\_IDLE (a full release, not the suspended RRC\_INACTIVE state).

**[Frame 129]** The **same** RRC Release again – byte-identical (PDCP SN 7, MAC-I 0xa48652fc), flagged as a duplicate. The UE did not acknowledge the first copy in time, so **Retransmit** fired and RLC re-sent it. One retransmission here – a far cry from a storm; the identical SN and MAC-I are the tell that it is one message resent, not a new command.





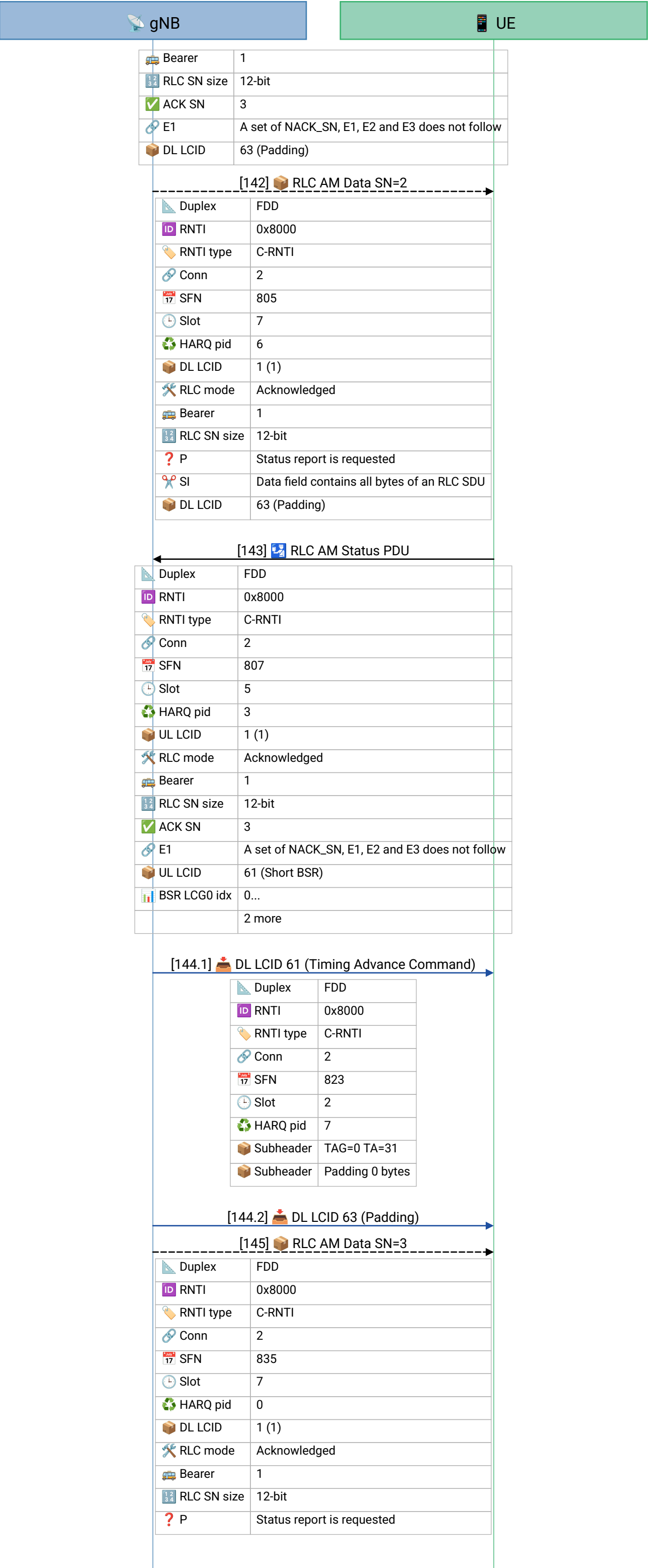


**[Frame 138]** RLC-AM Status PDU on SRB1, ACK\_SN = 2 (connection 2).

**[Frame 139]** Downlink RLC-AM Data PDU on SRB1 ( SN 1 ) , complete SDU, Poll set – post-security signaling on connection 2.

**[Frame 140]** RLC-AM Status PDU (uplink), ACK\_SN = 2, with a second AM segment beginning.

**[Frame 141]** RLC-AM Status PDU on SRB1, ACK\_SN = 3.

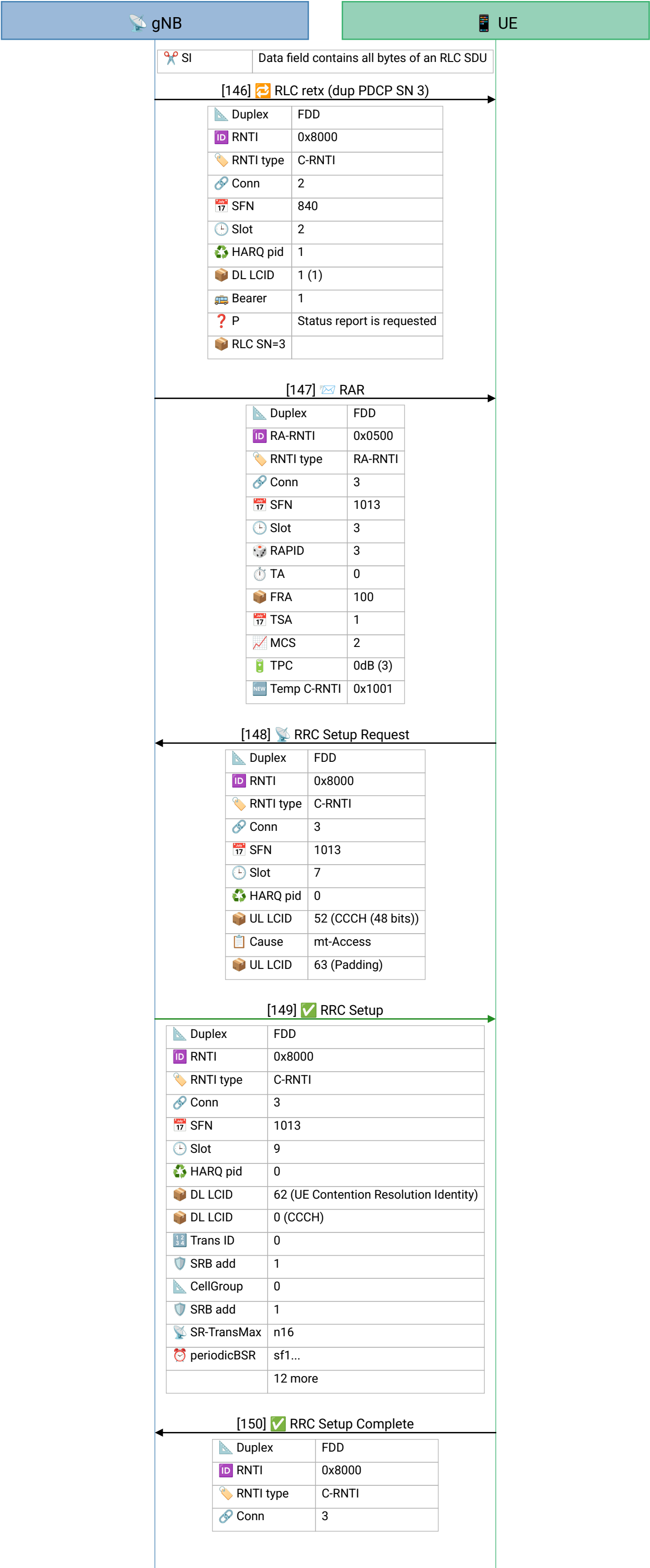


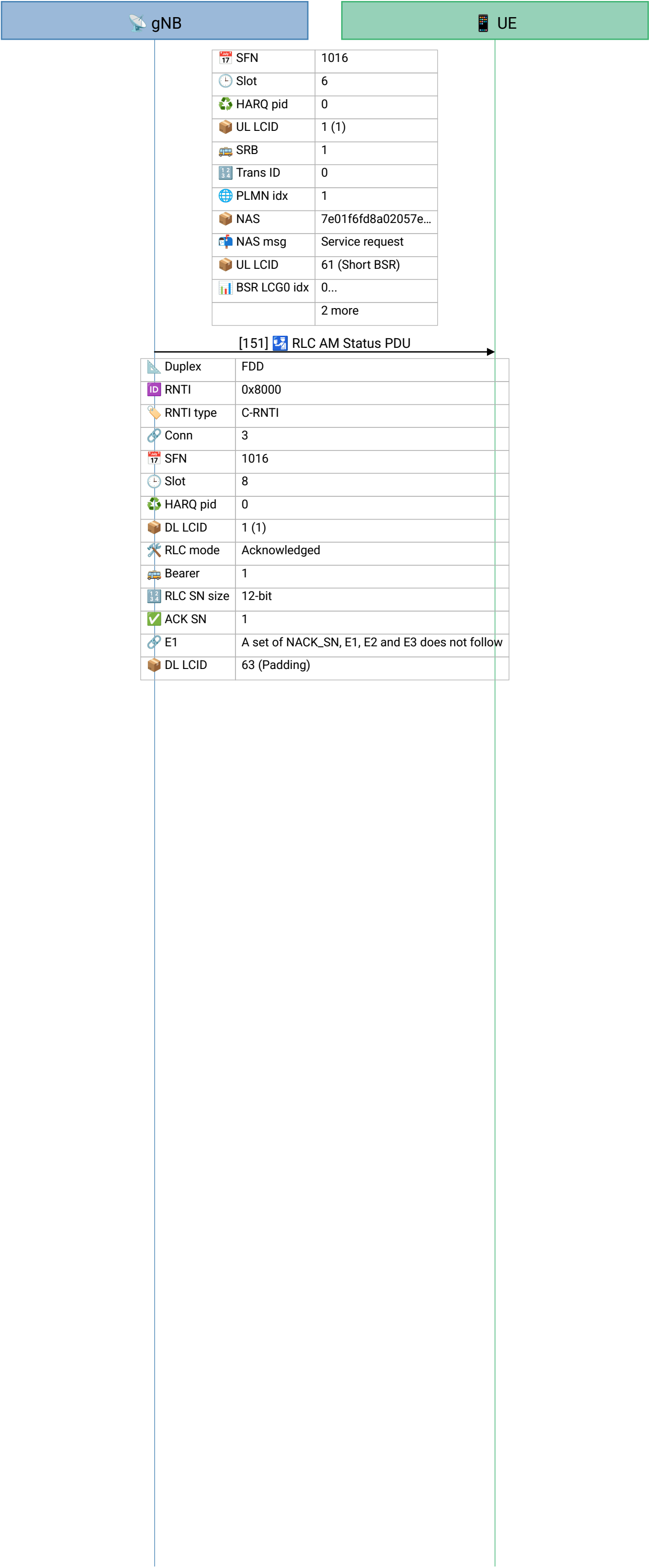
**[Frame 142]** Downlink RLC-AM Data PDU on SRB1 ( SN 2 ) , complete SDU, Poll set.

**[Frame 143]** RLC-AM Status PDU (uplink) on SRB1, ACK\_S = 3.

**[Frame 144.1]** MAC Timing Advance Command – link upkeep.

**[Frame 145]** Downlink RLC-AM Data PDU on SRB1 ( SN 3 ) , complete SDU, Poll set.





**[Frame 151]** RLC-AM Status PDU on SRB1 , ACK\_SN = 1 (connection 3) — and the capture ends here, mid-setup, before AS security is re-established for this third connection.