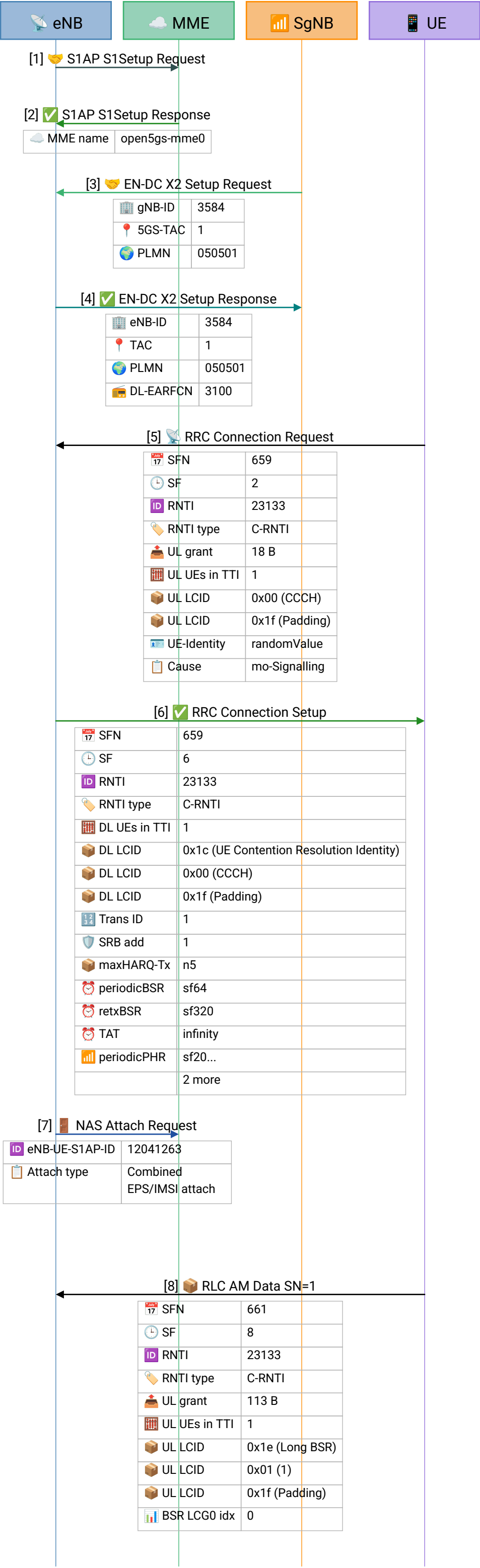
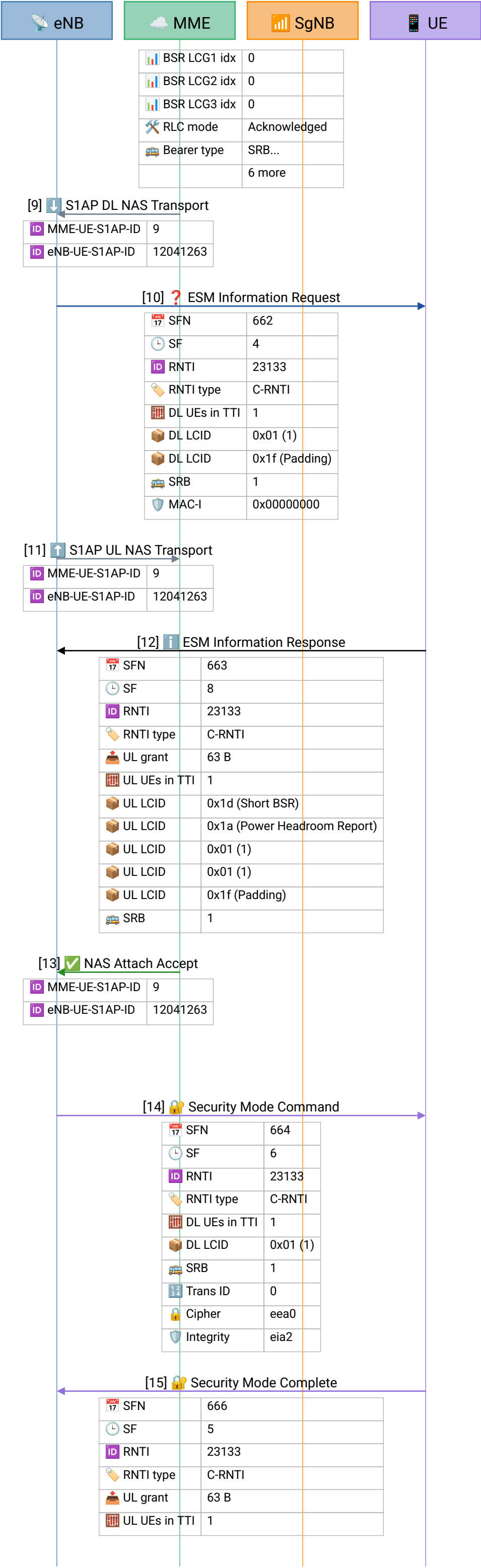






[Frame 9] S1AP DownlinkNASTransport (procedure 11): the MME tunnels a NAS ESM Information Request down to the eNB. The network is asking the UE to supply the APN and protocol configuration options for the PDN connection.

[Frame 10] Radio leg of that ESM Information Request — a downlink PDCP PDU on SRB1. Note the MAC-I is 0x00000000 : AS security is not active yet, so this PDU is neither ciphered nor integrity-protected. Compare with frame 16, the first PDU after security activation.

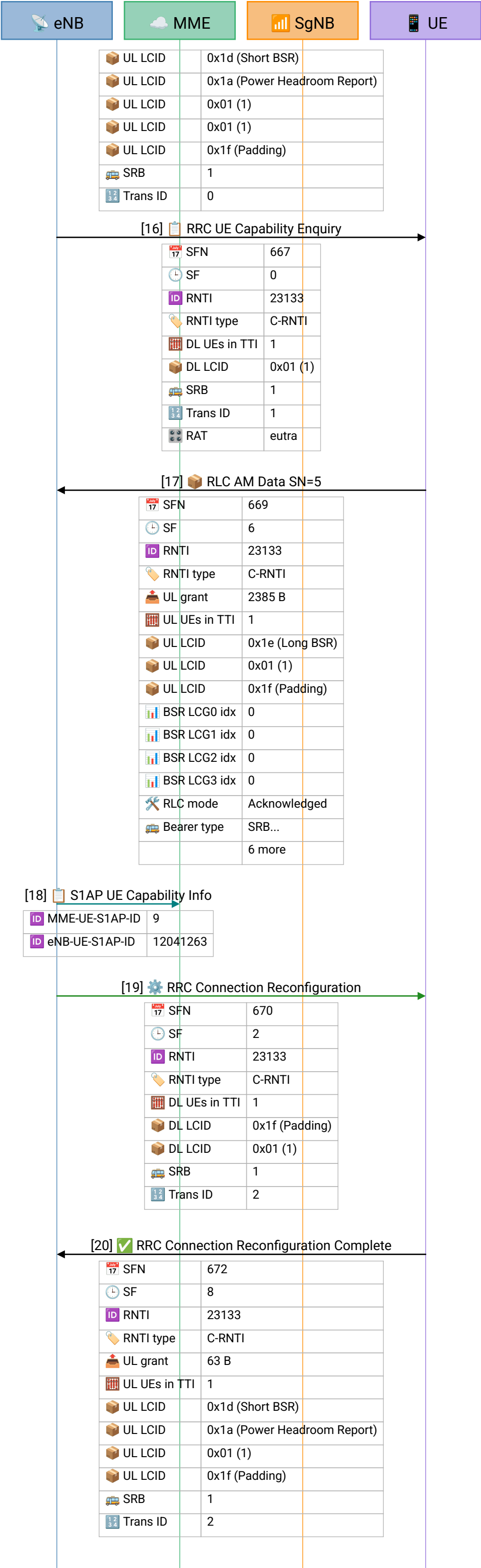
[Frame 11] S1AP UplinkNASTransport (procedure 13): the eNB tunnels the UE's NAS ESM Information Response up to the MME, carrying the APN and PCO the network asked for. Mirror of frame 9.

[Frame 12] The radio leg of the ESM Information Response — the UE returns the APN and protocol configuration options inside an RRC UL Information Transfer, the over-the-air twin of the S1AP UplinkNASTransport in frame 11. The frame also carries an RLC AM Status PDU (ARQ): the UE acknowledges the downlink up to ACK_SN=1 with no NACKs, and piggybacks a Short BSR and a Power Headroom Report as MAC control elements.

[Frame 13] The pivotal S1 message. S1AP InitialContextSetupRequest (procedure 9). The MME delivers, in one shot: the NAS Attach Accept + Activate Default EPS Bearer Context Request, the default bearer E-RAB 5 (QCI 9), the K_eNB security key the eNB will use to activate AS security, and the UE security capabilities. Crucially it includes the UE's NRUESecurityCapabilities (NEA1/2/3) — the network now knows this UE can do NR security, which is what makes the later EN-DC leg possible. The Attach Accept in the same message closes the loop the DCNR bit opened in frame 7: it marks dual connectivity with NR Not restricted, the core's explicit go-ahead for this UE to use a 5G secondary RAT.

[Frame 14] AS security activation. RRC Security Mode Command. The eNB turns on Access Stratum security keyed from K_eNB: ciphering EEA0 (null, a lab choice) and integrity EIA2 (TS 36.331, TS 33.401). From the UE's acknowledgement onward every SRB/DRB PDCP PDU is integrity-protected.

[Frame 15] RRC Security Mode Complete. The UE confirms AS security is active. This is the boundary: subsequent PDCP PDUs carry a real MAC-I and (with a non-null cipher) ciphered payload.



[Frame 16] First downlink PDCP PDU *after* security activation – the security context now shows EEA0/EIA2 and the MAC-I is a real value 0x76596de5 (PDCP COUNT 2), not the 0x00000000 seen in frame 10. That contrast is AS security taking effect on the wire. This first secured PDU is the RRC UE Capability Enquiry (transaction 1), requesting RAT-Type : eutra – the LTE capabilities. The UE answers in frames 17-18, and those E-UTRA capabilities already carry its supported NR bands (supportedBandListNR) . The EN-DC-specific enquiry for eutra-nr / nr follows separately in frame 21.

[Frame 17] A large uplink RLC AM segment: a 2331-byte SDU granted 2385 bytes in one TTI. This is the UE Capability Information travelling over the air – big because it enumerates every supported band, band combination and feature. The eNB forwards it on S1 in the next frame.

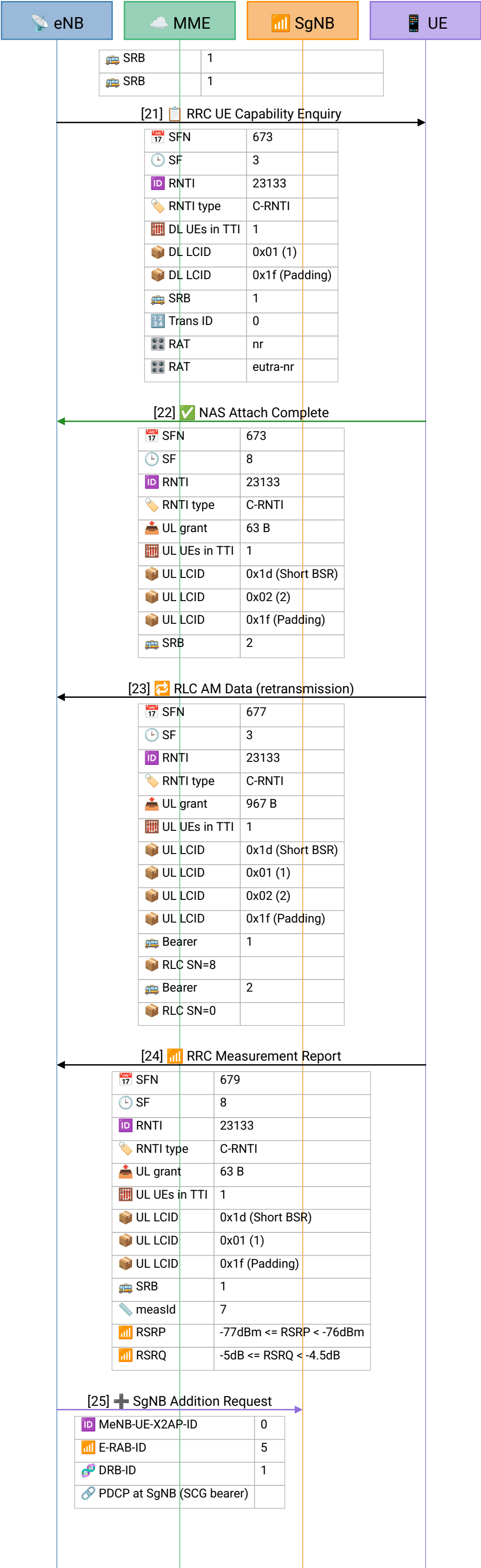
[Frame 18] S1AP UECapabilityInfoIndication (procedure 22). The eNB relays the UE's RAT capabilities – including its NR bands (n78) and EN-DC band combinations – up to the MME for storage. The eNB keeps its own copy to drive measurement configuration and SgNB Addition.

[Frame 19] The reconfiguration that arms the whole flow. RRC Connection Reconfiguration carrying three things at once: the piggybacked NAS Attach Accept; the radio bearers (SRB2 plus DRB1 for EPS bearer 5); and the full measConfig . That measConfig defines two measurement objects – E-UTRA at EARFCN 3100 and **NR n78 at NR-ARFCN 640000 (~3600 MHz)** – and seven measIds:

measId	Object	Report config	Purpose
1	E-UTRA 3100	periodic (RSRP+RSRQ)	serving-cell heartbeat
2	E-UTRA 3100	event A1	serving above threshold
3-6	E-UTRA 3100	events A2/A3/A4/A5	intra-LTE mobility (unused here)
7	NR n78	event B1-NR	detect an NR cell -> trigger EN-DC

measId 7 is the one to watch: its B1-NR threshold is set to the RSRP floor, so it fires as soon as the UE sees any NR cell.

[Frame 20] RRC Connection Reconfiguration Complete – the UE has applied the bearers, security and measurement config from frame 19; SRB2 and DRB1 are now usable. (This same uplink frame also bundles the first two measurement reports, measId 1 and measId 2 – both LTE-only; the diagram renders the completion.)



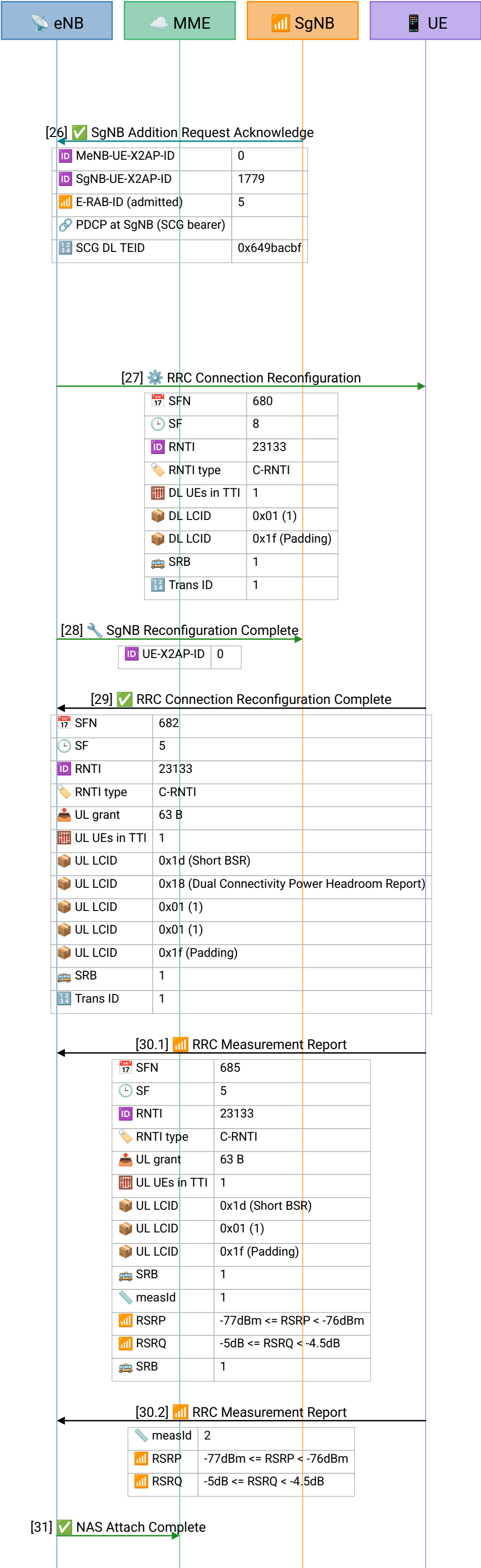
[Frame 21] A second RRC UE Capability Enquiry (transaction 0), and the EN-DC-relevant one: where frame 16 asked for eutra, this requests RAT-Type: eutra-nr and nr – the NR and MR-DC capabilities proper. Secured on SRB1 (EEA0/EIA2) . Its response is not in this capture.

[Frame 22] First uplink traffic on SRB2 (bearer 2), now that frame 19 created it. It carries the NAS Attach Complete + Activate Default EPS Bearer Context Accept – the UE confirming both the attach and the default bearer. NAS moves to SRB2 once it exists.

[Frame 23] RLC retransmission / continuation of that SRB2 uplink (RLC SN=8 and SN=0 segments in one grant). RLC-AM stitching the Attach Complete delivery back together after a poll.

[Frame 24] The 5G trigger. This is the first measurement report carrying NR. Event B1-NR (measId 7) has fired: alongside the LTE PCell result the UE reports a detected NR neighbour – PCI 0, SS-RSRP in the -91 to -90 dBm bucket, SS-RSRQ around -11 dB – inside measResultNeighCellListNR . Crossing the B1 threshold is exactly what tells the eNB "this UE can see 5G", and it reacts immediately in the next frame. Only the measId-7 sub-reports ever carry 5G measurements; measId 1 and 2 are LTE-only.

[Frame 25] Phase 4 – SgNB Addition (adding the 5G leg). X2AP SgNB Addition Request (procedure id-sgNBAdditionPreparation). The master eNB, which owns the UE, asks the secondary gNB to allocate NR radio resources for E-RAB 5 / DRB 1. It hands over the S-KgNB security key (derived from K_eNB), the UE's NR security capabilities, and the en-DC-ResourceConfiguration . The UE-association is one-sided so far: the request carries only the MeNB-UE-X2AP-ID – the gNB mints its own ID in the Acknowledge. Watch the bearer shape: resource-configuration here is sgNBPDCCPpresent , so PDCP is placed at the gNB – an SgNB-terminated (SCG) bearer, not the MCG-anchored split bearer (PDCP kept at the MeNB) shown in the companion X2AP walkthrough. Because the bearer



now terminates at the gNB, the request also carries the S-GW's uplink S1-U endpoint (`s1-UL-GTPTunnelEndpoint, 0x00000010`), so the gNB can send this bearer's uplink straight to the core. The `MeNBtoSgNBContainer` carries the LTE-side RRC context as a `CG-ConfigInfo`.

[Frame 26] X2AP SgNB Addition Request Acknowledge — a successful outcome of the same procedure. Where the Request was the eNB's ask, this is the gNB's admit, and two things complete here:

- **The UE-association becomes a pair.** The gNB mints its own SgNB-UE-X2AP-ID (1779) to sit beside the MeNB-UE-X2AP-ID — the two IDs both nodes now use for every later X2AP message about this UE.
- **The user-plane endpoint is set.** The gNB returns its downlink GTP-TEID for the SCG leg, 0x649bacbf — where the serving gateway's downlink data for E-RAB 5 must now be sent. Frame 31's E-RAB Modification hands exactly this TEID to the MME.

The `SgNBtoMeNBContainer` carries the NR `RRCReconfiguration` as an RRC `CG-Config` — the reply container, distinct from the `CG-ConfigInfo` the eNB sent outbound in frame 25. The eNB forwards it to the UE in frame 27; the EN-DC secondary cell group is now prepared.

[Frame 27] RRC Connection Reconfiguration, this time carrying the SCG. The eNB forwards the gNB's NR config to the UE: `nr-SecondaryCellGroupConfig` (band n78, p-NR-FR1 20 dBm, SSB and CSI reporting) plus `nr-RadioBearerConfig1`. It also releases LTE DRB 1 (`drb-ToReleaseList`) — the bearer the attach had set up for EPS bearer 5 in frame 19 — and re-adds that bearer on the SCG, so the default bearer's radio leg and its PDCP migrate from the eNB to the gNB. This is the message that actually tells the UE to add the 5G secondary cell.

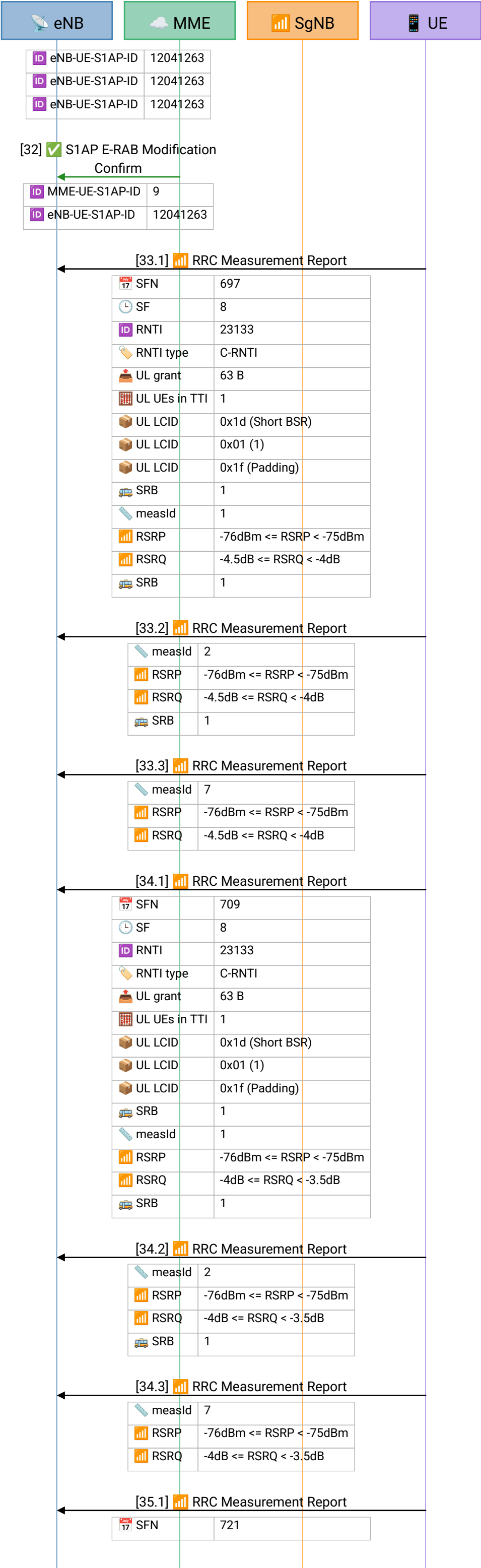
[Frame 28] X2AP SgNB Reconfiguration Complete. The eNB tells the gNB the UE is applying the SCG configuration, so the gNB can consider the secondary cell group active (TS 36.423).

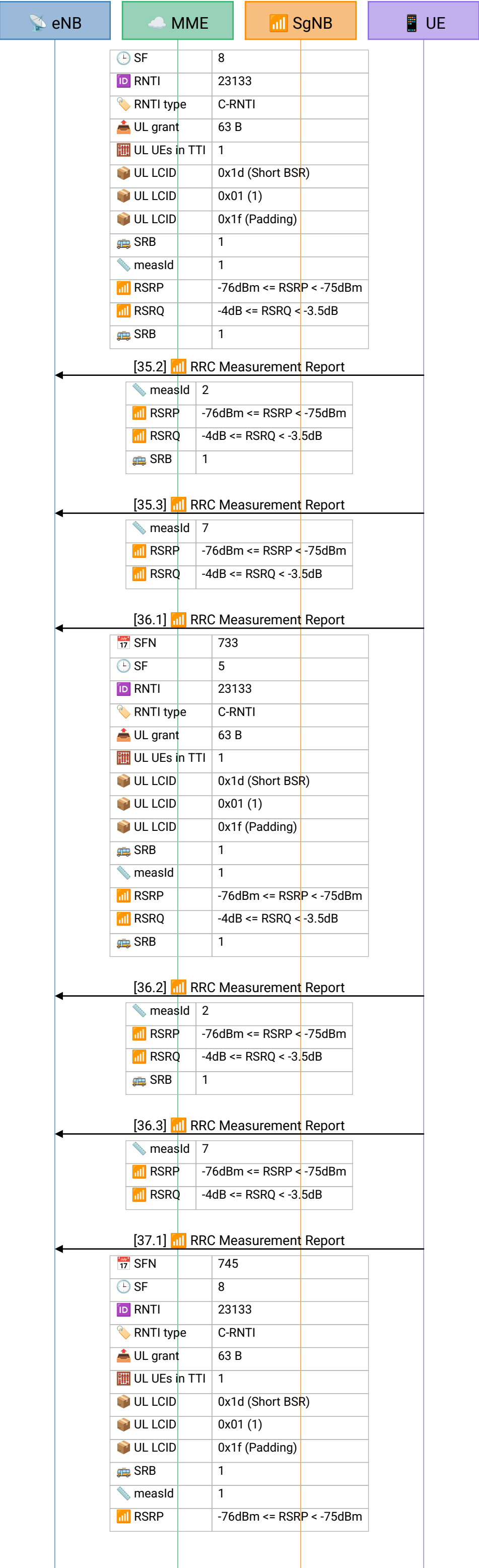
[Frame 29] RRC Connection Reconfiguration Complete — and this uplink message embeds the NR `RRCReconfigurationComplete` (the SCG-complete) inside the LTE completion. Note the MAC now carries a Dual Connectivity Power Headroom Report (LCID 0x18): concrete on-air evidence that the UE is now operating two cell groups. EN-DC is established.

[Frame 30.1] Periodic measurement reports resume: measId 1 (the RSRP+RSRQ heartbeat on the LTE serving cell). RSRP sits in the -77 to -76 dBm bucket. This sub carries no NR — it is an E-UTRA-only object.

[Frame 30.2] measId 2 — the event-A1 report (serving cell above its RSRP threshold). Also E-UTRA-only; no 5G measurement here.

[Frame 31] Phase 5 — user-plane rehoming. This S1AP frame bundles three PDUs: `InitialContextSetupResponse`, the uplink NAS Attach Complete, and — the





[Frame 35.2] measId 2 (event A1), LTE serving. No NR.

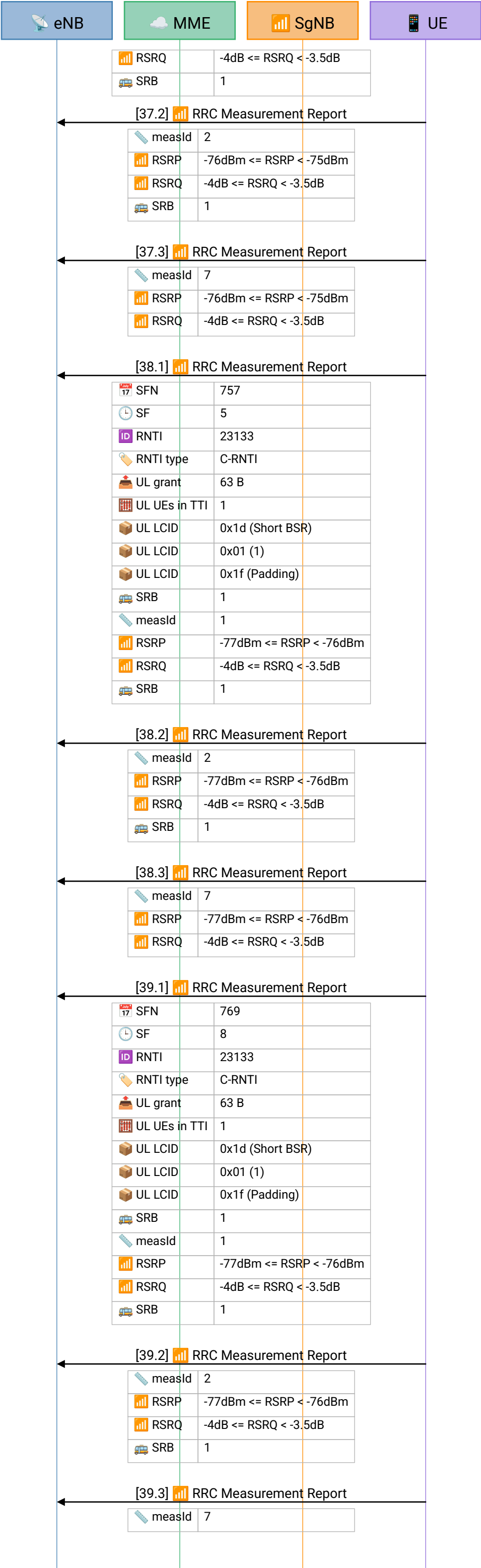
[Frame 35.3] measId 7 (event B1-NR) – the 5G-carrying sub-report (NR PCI 0).

[Frame 36.1] Periodic bundle, sub 1 – measId 1 LTE serving heartbeat. E-UTRA-only.

[Frame 36.2] measId 2 (event A1), LTE serving. No NR.

[Frame 36.3] measId 7 (event B1-NR) – the 5G-carrying sub-report (NR PCI 0).

[Frame 37.1] Periodic bundle, sub 1 – measId 1 LTE serving heartbeat. E-UTRA-only.



[Frame 37.2] measId 2 (event A1), LTE serving. No NR.

[Frame 37.3] measId 7 (event B1-NR) – the 5G-carrying sub-report (NR PCI 0).

[Frame 38.1] Periodic bundle, sub 1 – measId 1 LTE serving heartbeat. RSRP easing back toward the -77 to -76 dBm bucket. E-UTRA-only.

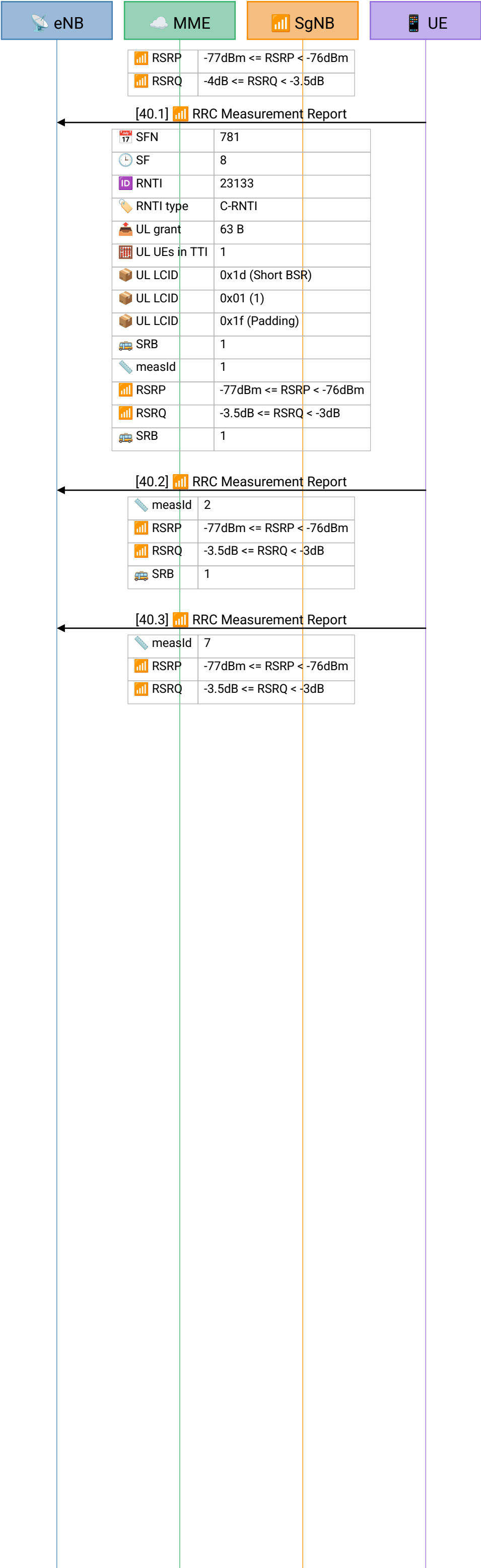
[Frame 38.2] measId 2 (event A1), LTE serving. No NR.

[Frame 38.3] measId 7 (event B1-NR) – the 5G-carrying sub-report (NR PCI 0).

[Frame 39.1] Periodic bundle, sub 1 – measId 1 LTE serving heartbeat. E-UTRA-only.

[Frame 39.2] measId 2 (event A1), LTE serving. No NR.

[Frame 39.3] measId 7 (event B1-NR) – the 5G-carrying sub-report (NR PCI 0).



[Frame 40.1] Periodic bundle, sub 1 — measId 1 LTE serving heartbeat; the capture ends here with EN-DC established and both legs being monitored. E-UTRA-only.

[Frame 40.2] measId 2 (event A1), LTE serving. No NR.

[Frame 40.3] measId 7 (event B1-NR) — the final 5G-carrying sub-report of the trace (NR PCI 0), confirming the 5G neighbour is still present as the capture closes.