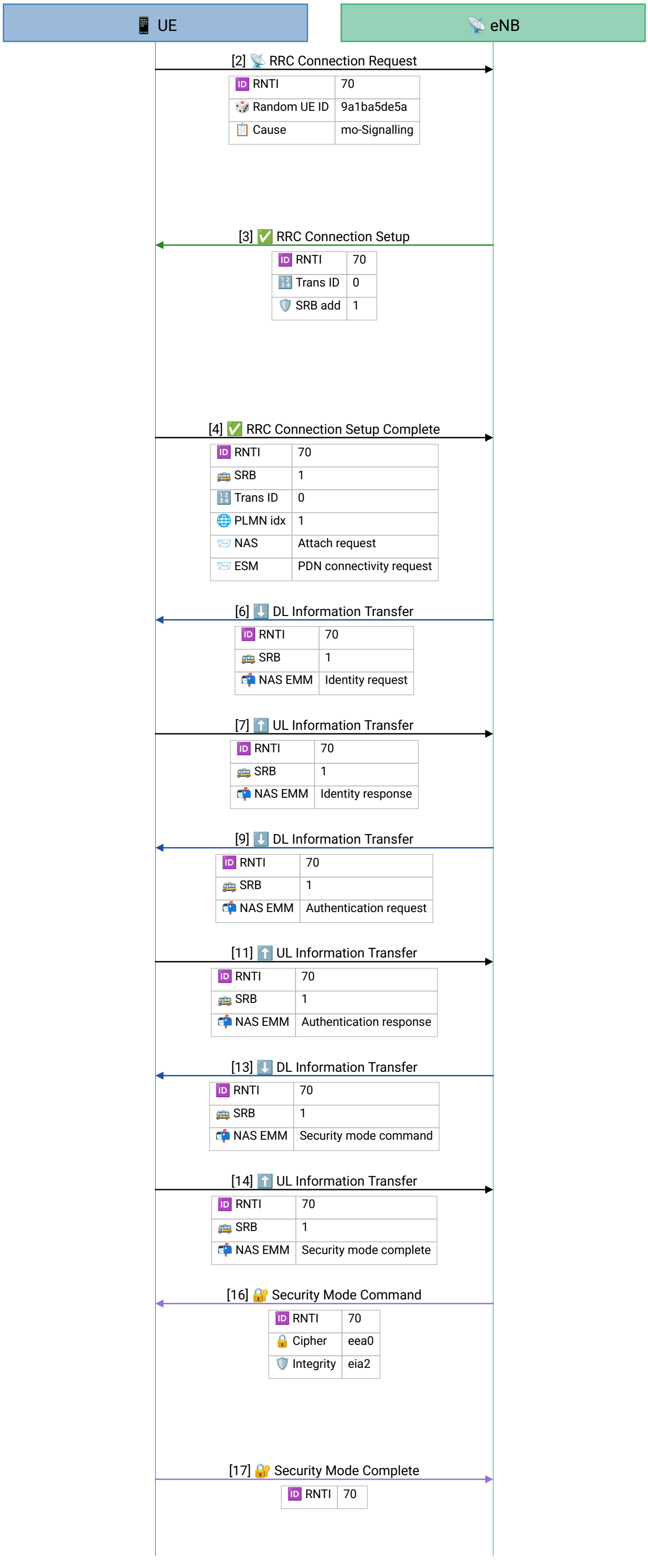
lte-rrc-connection.annotated



[Frame 2] Phase 1 - the connection opens. UE 70's first RRC message, on the common control channel (`UL-CCCH`, LCID 0, RLC transparent mode, no PDCP). This is Msg3 of random access. The UE has no identity the cell knows, so `ue-Identity` takes the `randomValue` branch: 40 random bits. A UE sends an `S-TMSI` instead only when NAS gives it one. `establishmentCause: mo-Signalling` says the UE wants to talk to the core network. There is no `rrc-TransactionIdentifier`: nothing has been asked yet. (TS 36.331 5.3.3)

[Frame 3] 2 ms later the eNB answers on `DL-CCCH`. The same MAC PDU carries a Contention Resolution control element that echoes Msg3's whole 6-byte CCCH message, so UE 70 knows it won random access. The RRC part installs SRB1 with the default RLC and logical channel configuration from TS 36.331 9.2.1.1 (`defaultValue`, so nothing is spelled out), plus `mac-MainConfig` (`maxHARQ-Tx` n4, BSR every 20 subframes, `timeAlignmentTimerDedicated` infinity) and the physical layer setup. On receipt the UE enters `RRC_CONNECTED`. It stays there for the rest of the capture.

[Frame 4] The first message on SRB1 (`UL-DCCH`, LCID 1, RLC AM SN 0, PDCP SN 0). From here on every RRC message travels on a Signaling Radio Bearer. `selectedPLMN-Identity`: 1 picks the first PLMN in the cell's SIB1 list. `dedicatedInfoNAS` carries the NAS `Attach Request` (combined EPS/IMSI attach, identifying itself by a GUTI from an earlier registration) with a PDN `Connectivity Request` inside it. RRC doesn't read it: to RRC it is a length and some bytes. The PDCP `MAC-I` is all zeros, because AS integrity isn't active yet.

[Frame 6] Phase 2 - RRC as a courier. The MME asks for the IMSI, so it couldn't use the GUTI. `DLInformationTransfer` exists only to carry NAS: its one payload field, `dedicatedInfoNAS`, holds an `Identity Request`. It rides SRB1 because SRB2 doesn't exist yet. (TS 36.331 5.6.1)

[Frame 7] `ULInformationTransfer` carries the `Identity Response` with IMSI 001011234567895. The UE answers within 38 ms.

[Frame 9] NAS `Authentication Request`: the MME's RAND and AUTN for EPS-AKA, carried through RRC unread.

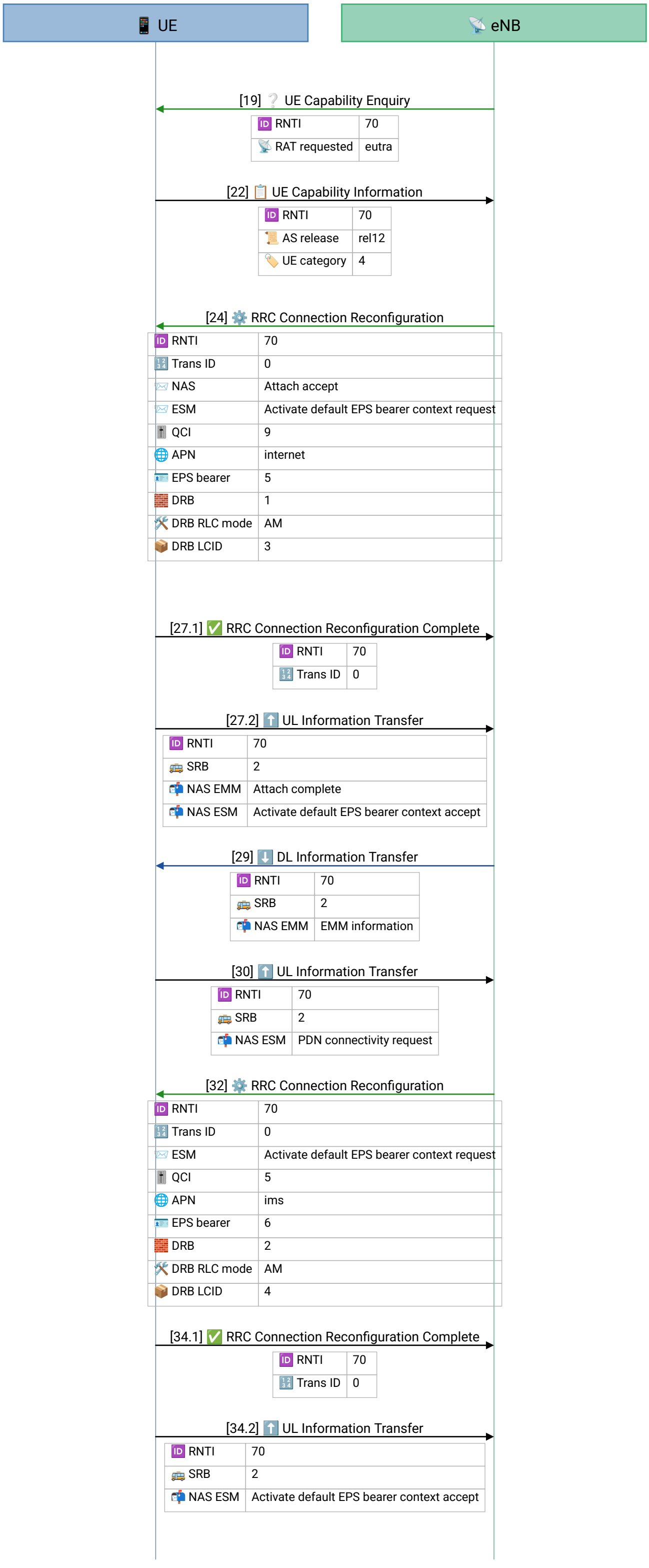
[Frame 11] NAS `Authentication Response` (RES). 214 ms after the request: the SIM computed the answer. RRC was idle the whole time.

[Frame 13] NAS `Security Mode Command`: the MME picks `EEA0` (null ciphering) and `EIA2` integrity for NAS. This is the core network's security, between the UE and the MME. It does not protect the radio link: that needs a second procedure, two frames on.

[Frame 14] NAS `Security Mode Complete`. Between this frame and the next, the MME sends the eNB `Initial Context Setup` over S1AP (0.7 ms before the next frame), with `K_eNB`, the key the eNB needs to start radio security.

[Frame 16] Phase 3 - AS security. RRC's own `SecurityModeCommand`, 10.7 ms after the NAS one. `cipheringAlgorithm: eea0`, `integrityProtAlgorithm: eia2`. Only the algorithm choice crosses the air, never a key: both sides derive the radio keys from `K_eNB`. The command itself is already integrity-protected: its PDCP `MAC-I` is 0x4efe0942, the first non-zero `MAC-I` on SRB1. Wireshark reports the digest "wrong" only because it has no keys to check it. (TS 36.331 5.3.4)

[Frame 17] `SecurityModeComplete` carries nothing but the transaction ID. The proof is in the PDCP layer: the message carries a valid `MAC-I` (0xc1047431), which the UE could compute only with the right keys. Ciphering would



start after this message, but `eea0` means the payloads stay readable.

[Frame 19] Phase 4 - capabilities. `UECapabilityEnquiry` with `ue-CapabilityRequest: eutra`. The eNB asks after security so that the answer is protected. (TS 36.331 5.6.3)

[Frame 22] `UECapabilityInformation`: `accessStratumRelease` rel12, UE category 4. The message is too big for one uplink grant, so RLC sent it in three segments, frames 20 to 22. The diagram shows it once, at the frame that completes it. The eNB forwards it to the MME in S1AP UE `Capability Info Indication`, so the next eNB doesn't have to ask again.

[Frame 24] Phase 5 - the attach reconfiguration. The first of 14 `RRCConnectionReconfiguration` messages on this connection. One message does four jobs:

- adds SRB2, with the default configuration of TS 36.331 9.2.1.2;
- adds DRB 1 for EPS bearer 5 on LCID 3, RLC AM, PDCP `discardTimer` 150 ms, logical channel priority 11, LCG 3;
- adds a `measConfig` with one measurement object (EARFCN 3150) but no report configuration or measurement ID, so the UE never sends a Measurement Report;
- carries the NAS `Attach Accept` and `Activate Default EPS Bearer Context Request` (APN `internet`, QCI 9) in `dedicatedInfoNASList`.

The UE applies the radio configuration and passes the NAS messages up. (TS 36.331 5.3.5, 5.3.10)

[Frame 27.1] `RRCConnectionReconfigurationComplete` on SRB1, 26 ms later. It echoes `rrc-TransactionIdentifier` 0, as does every response in this connection: the eNB runs one procedure at a time, so it never needs values 1 to 3.

[Frame 27.2] The first message on the new SRB2, in the same MAC PDU as the Complete: NAS `Attach Complete` with `Activate Default EPS Bearer Context Accept`. SRB2 carries NAS once it exists. It has lower priority than SRB1 (logical channel priority 3 against 1), so NAS traffic can't delay RRC's own messages. UE 70 is attached.

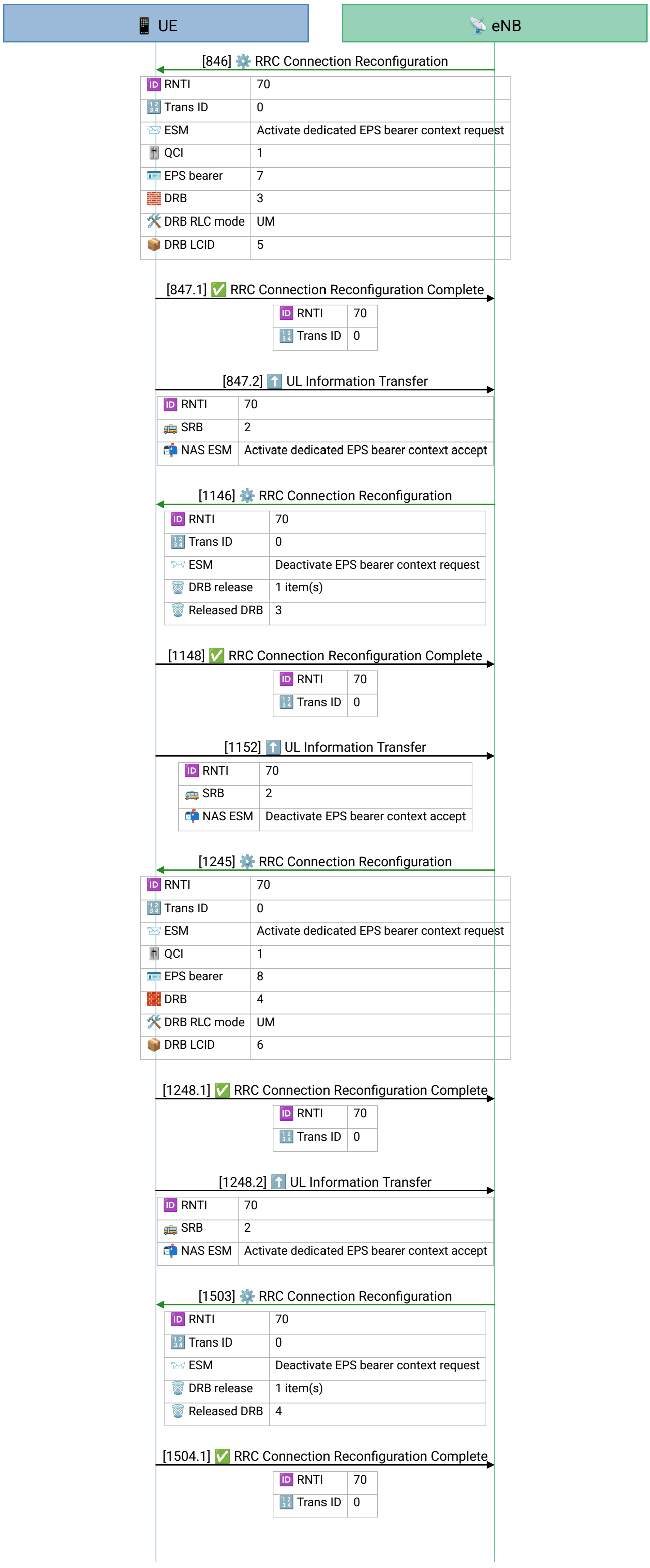
[Frame 29] The only `DLInformationTransfer` on SRB2 in the whole connection: NAS `EMM Information` (network name and time zone). Every later downlink NAS message rides inside a reconfiguration on SRB1 instead, because each one comes with a radio bearer change.

[Frame 30] Phase 6 - the IMS PDN. 0.2 s after attaching, the UE asks for a second PDN: NAS `PDN Connectivity Request` for the `ims` APN, on SRB2.

[Frame 32] Reconfiguration 2 adds DRB 2 for EPS bearer 6 (QCI 5, APN `ims`) on LCID 4, RLC AM. Its settings differ from DRB 1: `t-PollRetransmit` 80 ms, `pollPDU` 128, `pollByte` 125 kB, `maxRetxThreshold` 4, `t-StatusProhibit` 60 ms, PDCP `discardTimer` infinity, LCG 2. Only the radio bearer list changes: no SRB, no measurement or physical-layer fields. A reconfiguration carries only what changes.

[Frame 34.1] Reconfiguration Complete, 32 ms later.

[Frame 34.2] NAS `Activate Default EPS Bearer Context Accept` for bearer 6, on SRB2. UE 70 now has four radio bearers: SRB 1 and SRB 2 for signaling, DRB 1 and DRB 2 for data. It registers with IMS over DRB 2 next, and RRC stays silent for 23 s.



[Frame 846] Phase 7 - six calls, six new DRBs. Call 1: UE 70 dialed (the INVITE went up in frame 821). Reconfiguration 3 adds DRB 3 for EPS bearer 7 on LCID 5, and it is a voice bearer: RLC UM with a 10-bit SN, `t-Reordering` 50 ms, PDCP 12-bit SN, `discardTimer` 100 ms, logical channel priority 2 (above the data bearers' 11), LCG 1. The NAS `Activate Dedicated EPS Bearer Context Request` gives QCI 1 with an 80 kbit/s guaranteed bit rate, linked to bearer 6, the IMS PDN.

[Frame 847.1] Reconfiguration Complete, 33 ms later. The same MAC PDU also carries two ESP packets from UE 70 to the P-CSCF on DRB 2, which this RRC diagram doesn't show.

[Frame 847.2] NAS `Activate Dedicated EPS Bearer Context Accept` for bearer 7. The voice bearer exists; the RTP starts in frame 985.

[Frame 1146] Call 1 hangs up (UE 71 sent the BYE). Reconfiguration 4 carries `drb-ToReleaseList`: DRB 3 and NAS `Deactivate EPS Bearer Context Request` for bearer 7, ESM cause 36 (regular deactivation). Releasing a DRB removes its PDCP entity, RLC entity and logical channel together. DRB 3 lived 6.4 s. (TS 36.331 5.3.10.2)

[Frame 1148] Reconfiguration Complete, 20 ms later, alone in its MAC PDU this time.

[Frame 1152] NAS `Deactivate EPS Bearer Context Accept` on SRB2, in a later uplink transmission. Its MAC PDU also carries UE 70's next comfort-noise packet, now on DRB 2 because DRB 3 is gone.

[Frame 1245] Call 2, which UE 71 dialed. The voice bearer comes back with the next numbers, not the freed ones: DRB 4, LCID 6, EPS bearer 8. Every setting is the same as DRB 3's. LCID 5 has been free since frame 1146, and it is never used again.

[Frame 1248.1] Reconfiguration Complete, 26 ms later.

[Frame 1248.2] NAS `Activate Dedicated EPS Bearer Context Accept` for bearer 8.

[Frame 1503] Call 2 ends: release DRB 4 and deactivate bearer 8, ESM cause 36. DRB 4 lived 6.5 s.

[Frame 1504.1] Reconfiguration Complete, 32 ms later.

lte-rrc-connection.annotated

UE | eNB

[1504.2] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Deactivate EPS bearer context accept

[Frame 1504.2] NAS `Deactivate EPS Bearer Context Accept` for bearer 8, in the same MAC PDU this time.

[1599] RRC Connection Reconfiguration

RNTI	70
Trans ID	0
ESM	Activate dedicated EPS bearer context request
QCI	1
EPS bearer	9
DRB	5
DRB RLC mode	UM
DRB LCID	7

[Frame 1599] Call 3, dialed by UE 71: DRB 5, LCID 7, EPS bearer 9. The pattern holds on every voice bearer in the capture: DRB = EPS bearer - 4, and LCID = DRB + 2.

[1603.1] RRC Connection Reconfiguration Complete

RNTI	70
Trans ID	0

[Frame 1603.1] Reconfiguration Complete, 37 ms later.

[1603.2] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Activate dedicated EPS bearer context accept

[Frame 1603.2] NAS accept for bearer 9.

[1926] RRC Connection Reconfiguration

RNTI	70
Trans ID	0
ESM	Deactivate EPS bearer context request
DRB release	1 item(s)
Released DRB	5

[Frame 1926] Call 3 ends: release DRB 5, deactivate bearer 9. DRB 5 lived 6.7 s.

[1928.1] RRC Connection Reconfiguration Complete

RNTI	70
Trans ID	0

[Frame 1928.1] Reconfiguration Complete, 33 ms later.

[1928.2] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Deactivate EPS bearer context accept

[Frame 1928.2] NAS deactivate accept for bearer 9.

[2039] RRC Connection Reconfiguration

RNTI	70
Trans ID	0
ESM	Activate dedicated EPS bearer context request
QCI	1
EPS bearer	10
DRB	6
DRB RLC mode	UM
DRB LCID	8

[Frame 2039] Call 4, dialed by UE 70: DRB 6, LCID 8, EPS bearer 10.

[2042.1] RRC Connection Reconfiguration Complete

RNTI	70
Trans ID	0

[Frame 2042.1] Reconfiguration Complete, 38 ms later.

[2042.2] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Activate dedicated EPS bearer context accept

[Frame 2042.2] NAS accept for bearer 10.

[2316] RRC Connection Reconfiguration

RNTI	70
Trans ID	0
ESM	Deactivate EPS bearer context request
DRB release	1 item(s)

[Frame 2316] Call 4 ends: release DRB 6, deactivate bearer 10. DRB 6 lived 4.7 s.

UE | eNB

Released DRB	6

[2319] RRC Connection Reconfiguration Complete

RNTI	70
Trans ID	0

[Frame 2319] Reconfiguration Complete, 19 ms later, alone again.

[2323] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Deactivate EPS bearer context accept

[Frame 2323] NAS deactivate accept for bearer 10, 20 ms after the Complete.

[2447] RRC Connection Reconfiguration

RNTI	70
Trans ID	0
ESM	Activate dedicated EPS bearer context request
QCI	1
EPS bearer	11
DRB	7
DRB RLC mode	UM
DRB LCID	9

[Frame 2447] Call 5, dialed by UE 70: DRB 7, LCID 9, EPS bearer 11.

[2450.1] RRC Connection Reconfiguration Complete

RNTI	70
Trans ID	0

[Frame 2450.1] Reconfiguration Complete, 38 ms later.

[2450.2] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Activate dedicated EPS bearer context accept

[Frame 2450.2] NAS accept for bearer 11.

[2925] RRC Connection Reconfiguration

RNTI	70
Trans ID	0
ESM	Deactivate EPS bearer context request
DRB release	1 item(s)
Released DRB	7

[Frame 2925] Call 5 ends: release DRB 7, deactivate bearer 11. At 11.7 s, the longest call in the capture.

[2928] RRC Connection Reconfiguration Complete

RNTI	70
Trans ID	0

[Frame 2928] Reconfiguration Complete, 20 ms later.

[2932] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Deactivate EPS bearer context accept

[Frame 2932] NAS deactivate accept for bearer 11, 9 ms after the Complete.

[3032] RRC Connection Reconfiguration

RNTI	70
Trans ID	0
ESM	Activate dedicated EPS bearer context request
QCI	1
EPS bearer	12
DRB	8
DRB RLC mode	UM
DRB LCID	10

[Frame 3032] The last free LCID. Call 6, dialed by UE 71: DRB 8 on LCID 10, EPS bearer 12. TS 36.331 allows `logicalChannelIdentity` 3 to 10 for a DRB, so LCID 10 is the top of the range. UE 70 has only three DRBs at this moment (1, 2 and 8), and LCIDs 5 to 9 are all free, but the next bearer by this pattern would need LCID 11.

[3035.1] RRC Connection Reconfiguration Complete

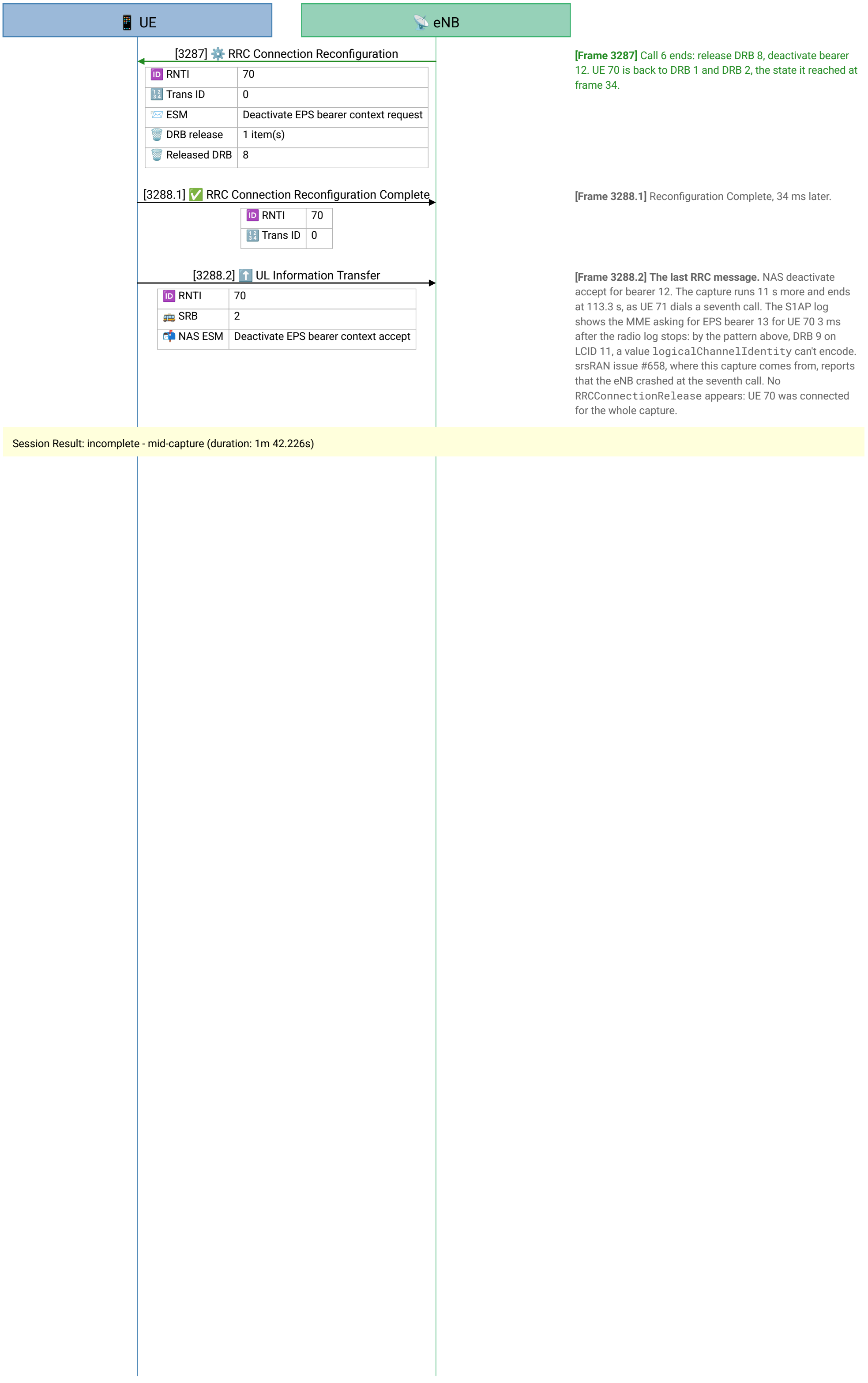
RNTI	70
Trans ID	0

[Frame 3035.1] Reconfiguration Complete, 36 ms later.

[3035.2] UL Information Transfer

RNTI	70
SRB	2
NAS ESM	Activate dedicated EPS bearer context accept

[Frame 3035.2] NAS accept for bearer 12.



[Frame 3287] Call 6 ends: release DRB 8, deactivate bearer 12. UE 70 is back to DRB 1 and DRB 2, the state it reached at frame 34.

[Frame 3288.1] Reconfiguration Complete, 34 ms later.

[Frame 3288.2] The last RRC message. NAS deactivate accept for bearer 12. The capture runs 11 s more and ends at 113.3 s, as UE 71 dials a seventh call. The S1AP log shows the MME asking for EPS bearer 13 for UE 70 3 ms after the radio log stops: by the pattern above, DRB 9 on LCID 11, a value `logicalChannelIdentity` can't encode. srsRAN issue #658, where this capture comes from, reports that the eNB crashed at the seventh call. No `RRCConnectionRelease` appears: UE 70 was connected for the whole capture.

Session Result: incomplete - mid-capture (duration: 1m 42.226s)