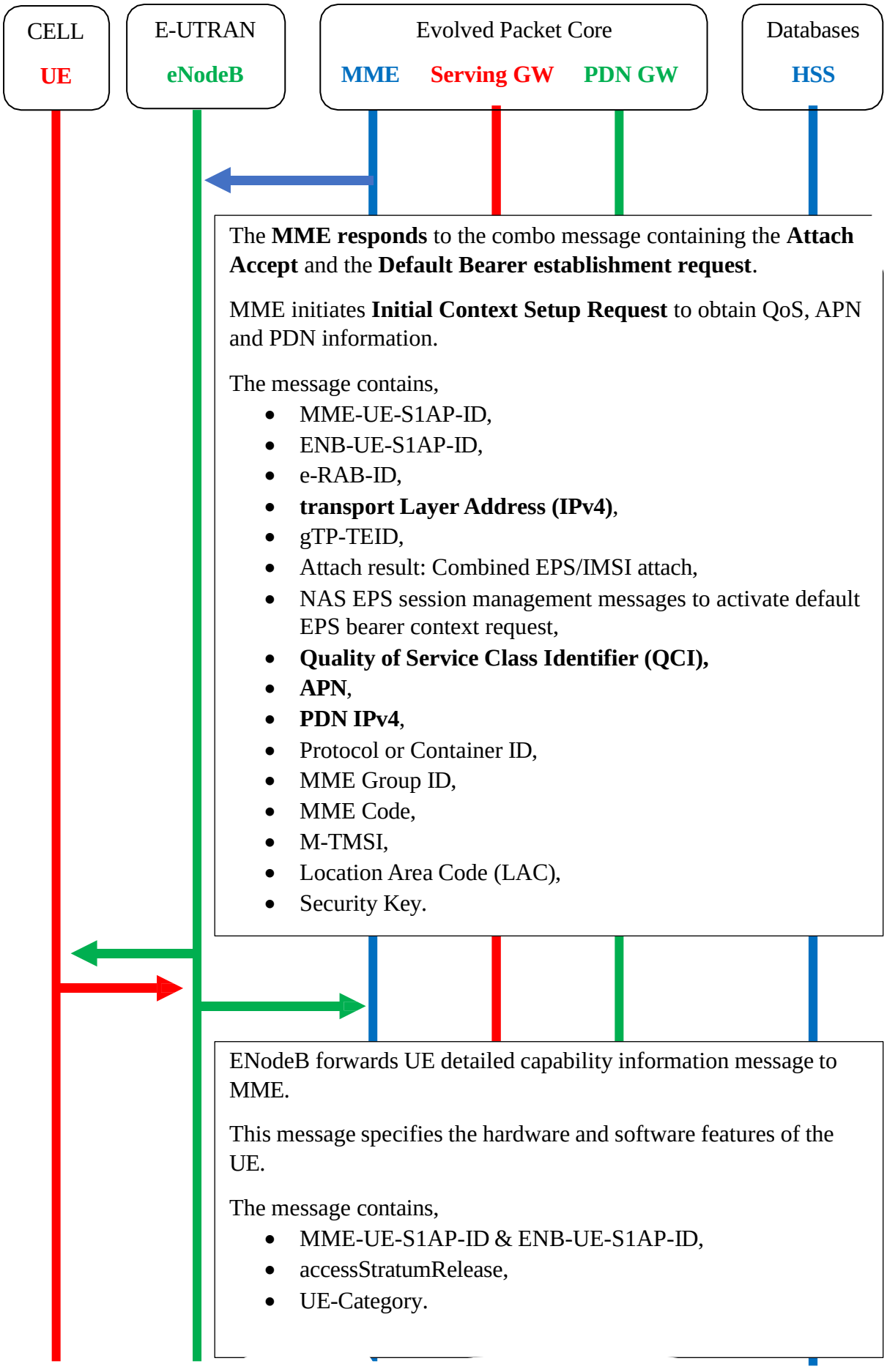


The **MME responds** to the combo message containing the **Attach Accept** and the **Default Bearer establishment request**.

MME initiates **Initial Context Setup Request** to obtain QoS, APN and PDN information.

The message contains,

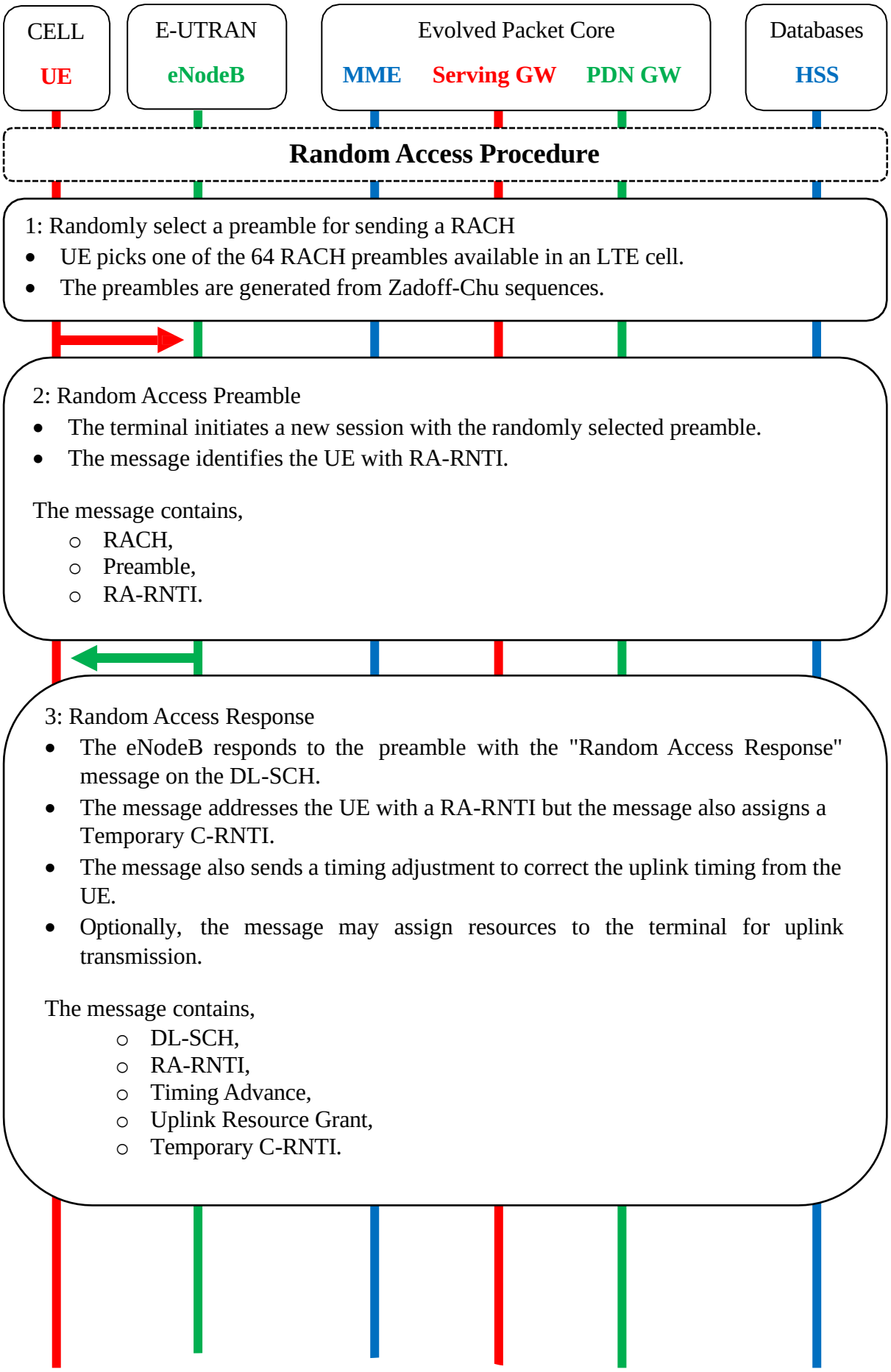
- MME-UE-S1AP-ID,
- ENB-UE-S1AP-ID,
- e-RAB-ID,
- **transport Layer Address (IPv4)**,
- gTP-TEID,
- Attach result: Combined EPS/IMSI attach,
- NAS EPS session management messages to activate default EPS bearer context request,
- **Quality of Service Class Identifier (QCI),**
- **APN**,
- **PDN IPv4**,
- Protocol or Container ID,
- MME Group ID,
- MME Code,
- M-TMSI,
- Location Area Code (LAC),
- Security Key.

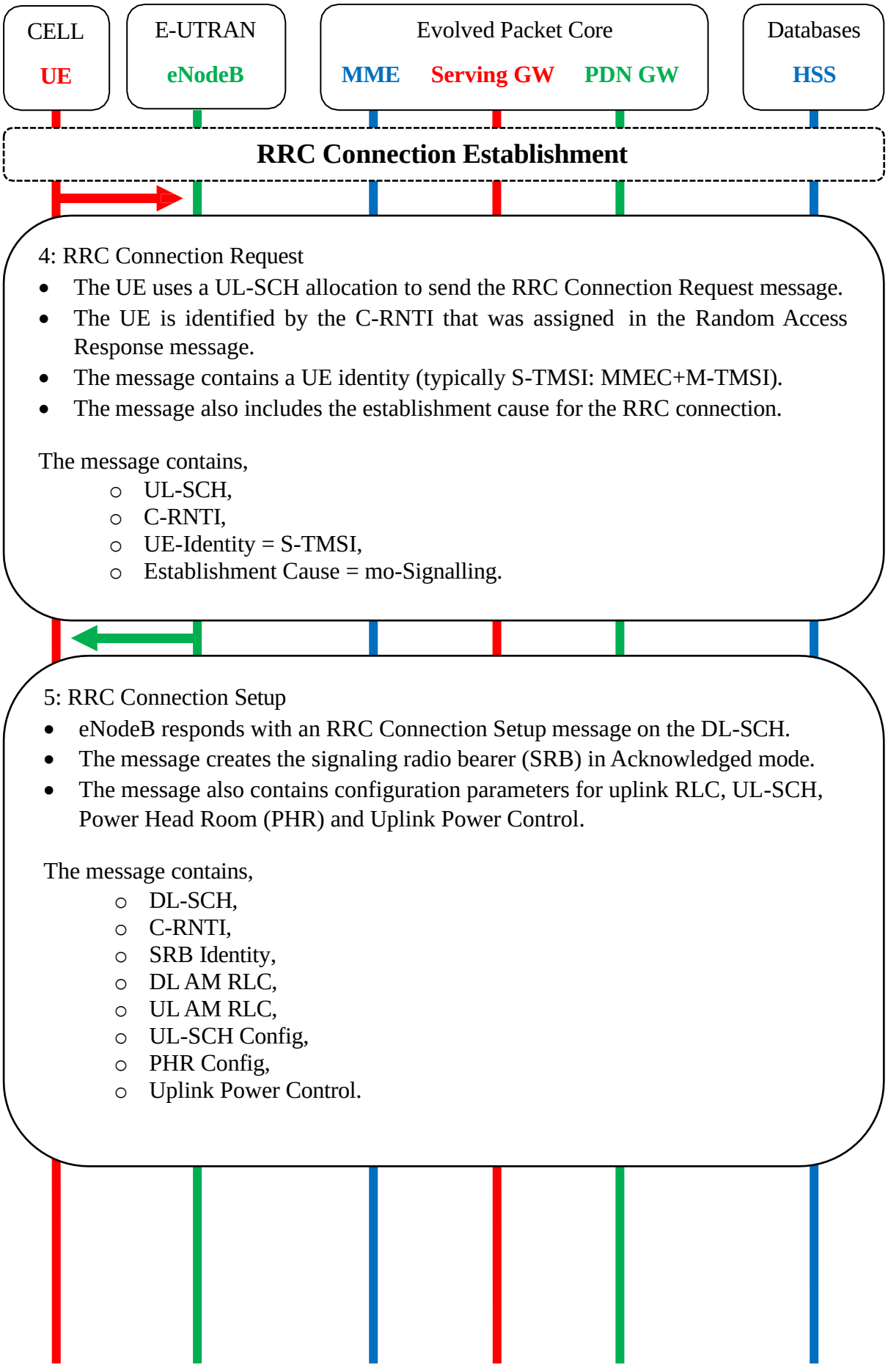
ENodeB forwards UE detailed capability information message to MME.

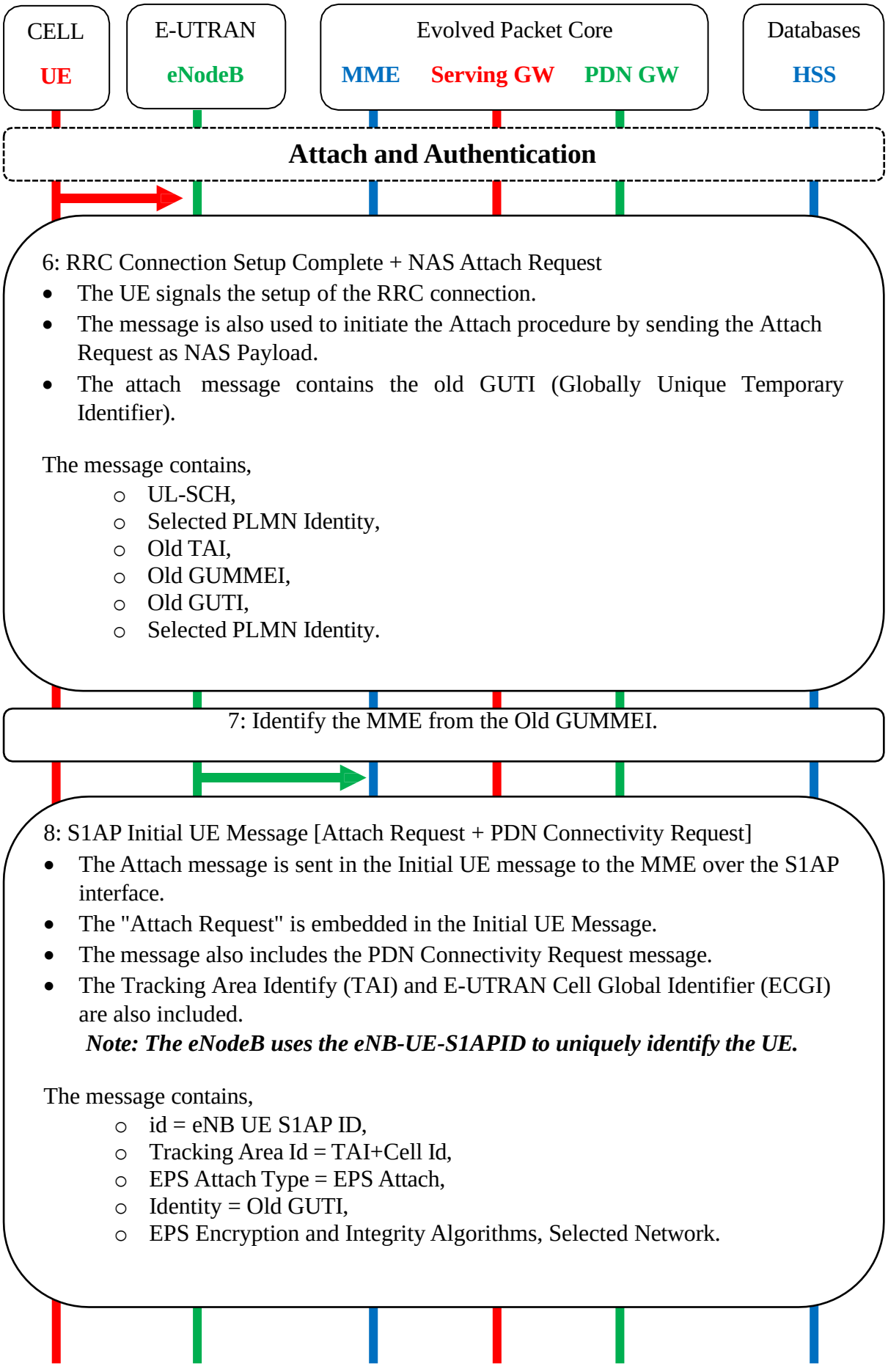
This message specifies the hardware and software features of the UE.

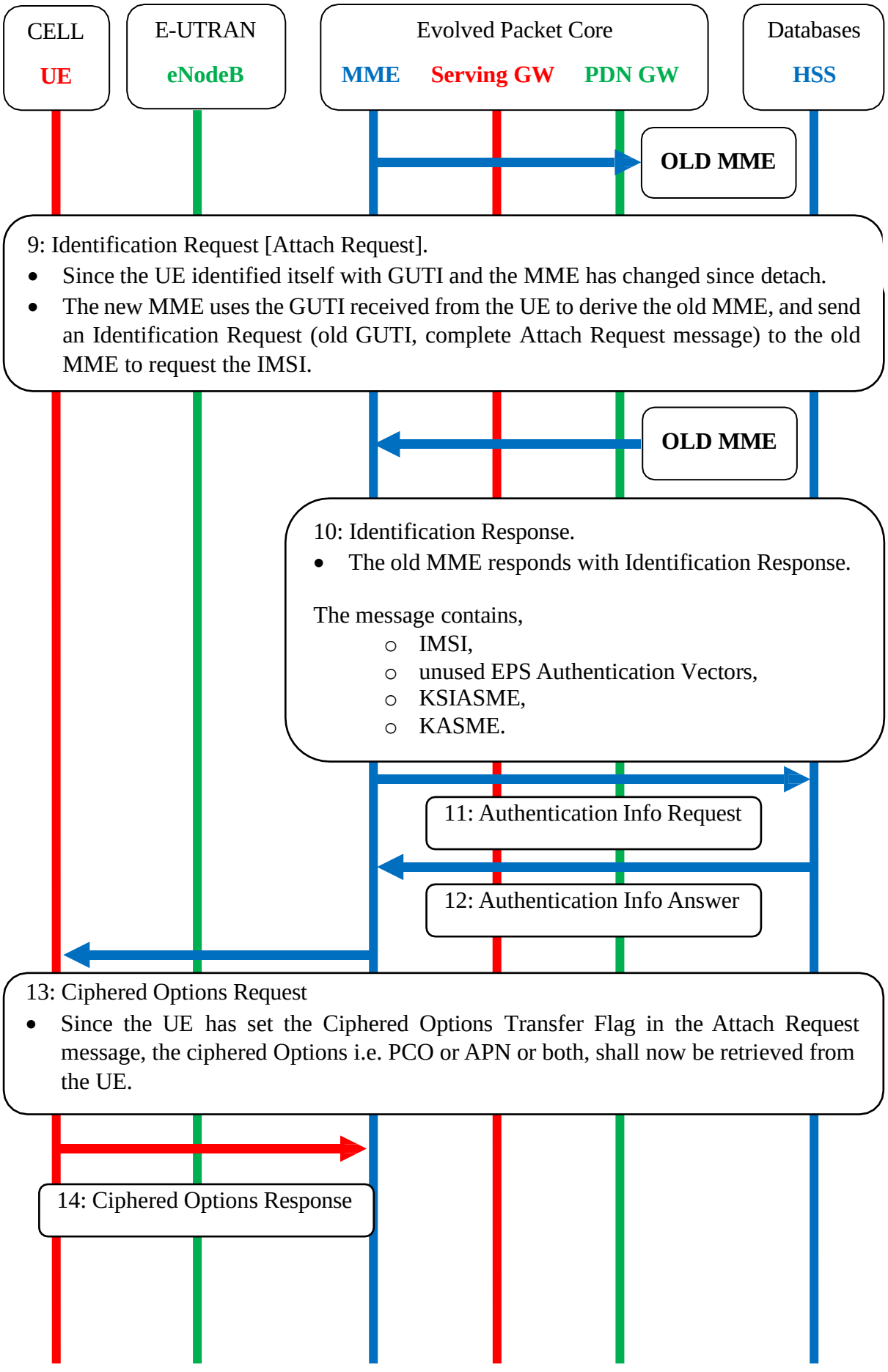
The message contains,

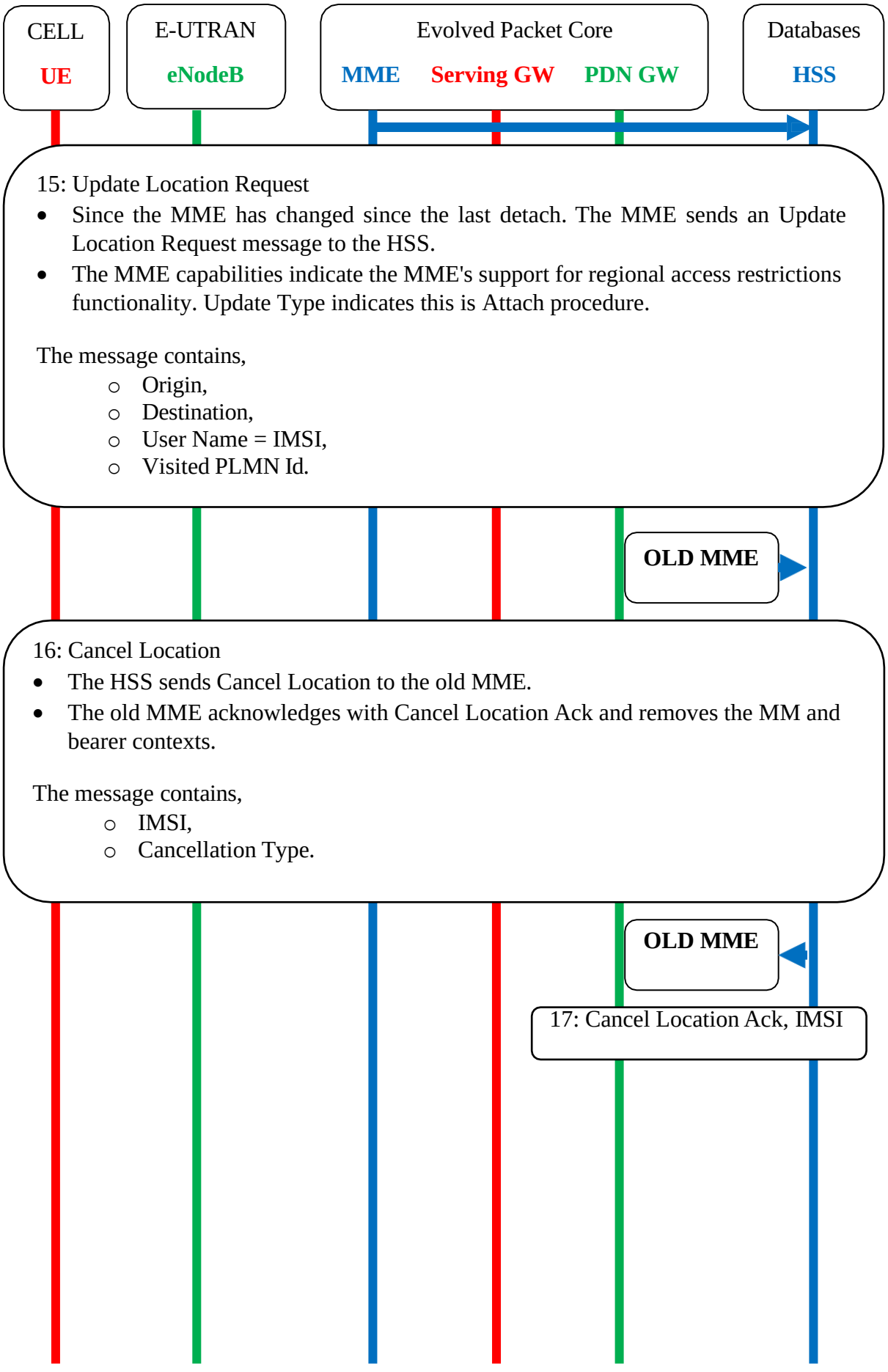
- MME-UE-S1AP-ID & ENB-UE-S1AP-ID,
- accessStratumRelease,
- UE-Category.

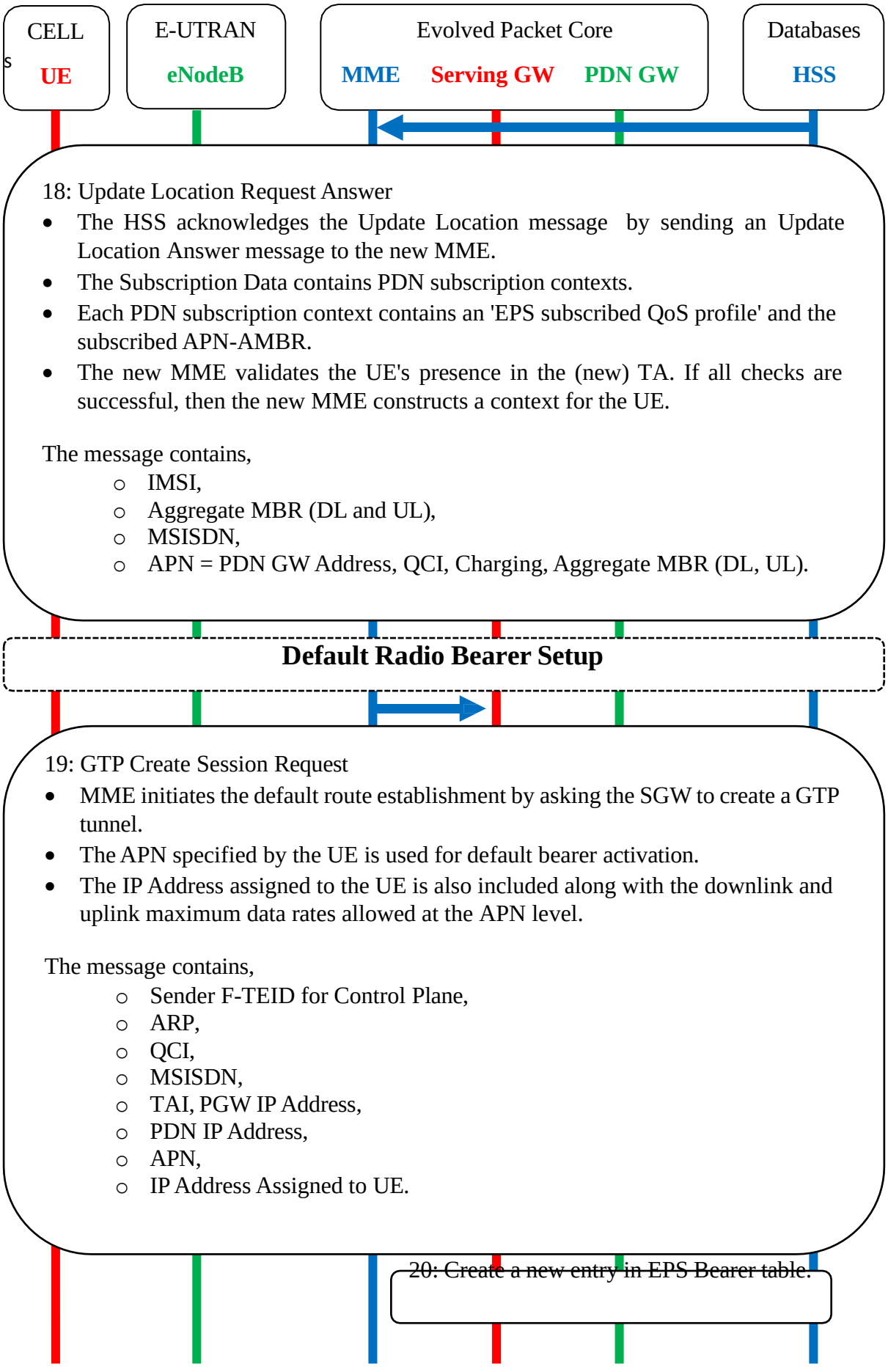

CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
Random Access Procedure
1: Randomly select a preamble for sending a RACH
UE picks one of the 64 RACH preambles available in an LTE cell.
The preambles are generated from Zadoff-Chu sequences.
2: Random Access Preamble
The terminal initiates a new session with the randomly selected preamble.
The message identifies the UE with RA-RNTI.
The message contains,
RACH,
Preamble,
RA-RNTI.
3: Random Access Response
The eNodeB responds to the preamble with the "Random Access Response" message on the DL-SCH.
The message addresses the UE with a RA-RNTI but the message also assigns a Temporary C-RNTI.
The message also sends a timing adjustment to correct the uplink timing from the UE.
Optionally, the message may assign resources to the terminal for uplink transmission.
The message contains,
DL-SCH,
RA-RNTI,
Timing Advance,
Uplink Resource Grant,
Temporary C-RNTI.

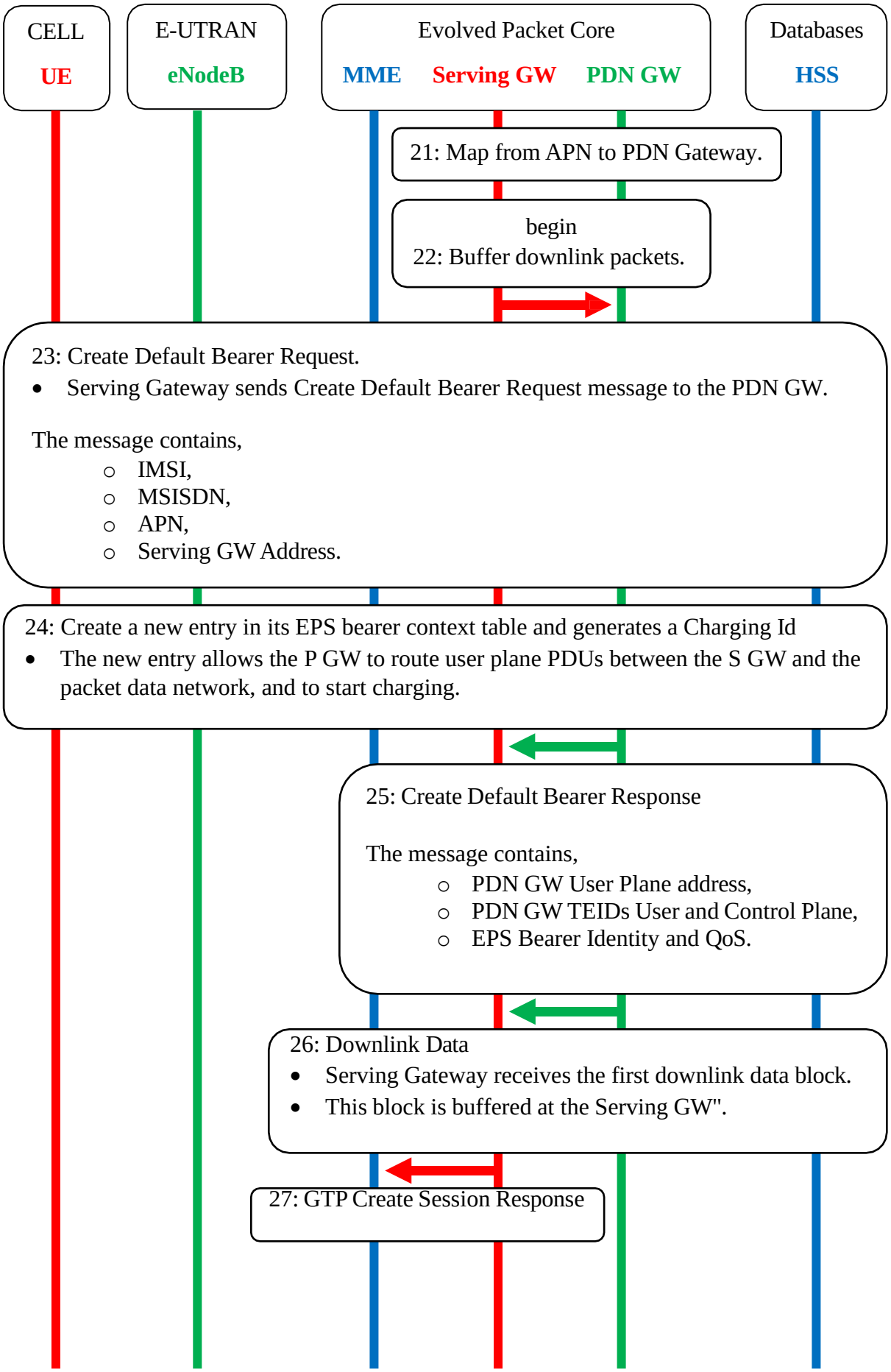

CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
RRC Connection Establishment
4: RRC Connection Request
The UE uses a UL-SCH allocation to send the RRC Connection Request message.
The UE is identified by the C-RNTI that was assigned in the Random Access Response message.
The message contains a UE identity (typically S-TMSI: MMEC+M-TMSI).
The message also includes the establishment cause for the RRC connection.
The message contains,
UL-SCH,
C-RNTI,
UE-Identity = S-TMSI,
Establishment Cause = mo-Signalling.
5: RRC Connection Setup
eNodeB responds with an RRC Connection Setup message on the DL-SCH.
The message creates the signaling radio bearer (SRB) in Acknowledged mode.
The message also contains configuration parameters for uplink RLC, UL-SCH, Power Head Room (PHR) and Uplink Power Control.
The message contains,
DL-SCH,
C-RNTI,
SRB Identity,
DL AM RLC,
UL AM RLC,
UL-SCH Config,
PHR Config,
Uplink Power Control.

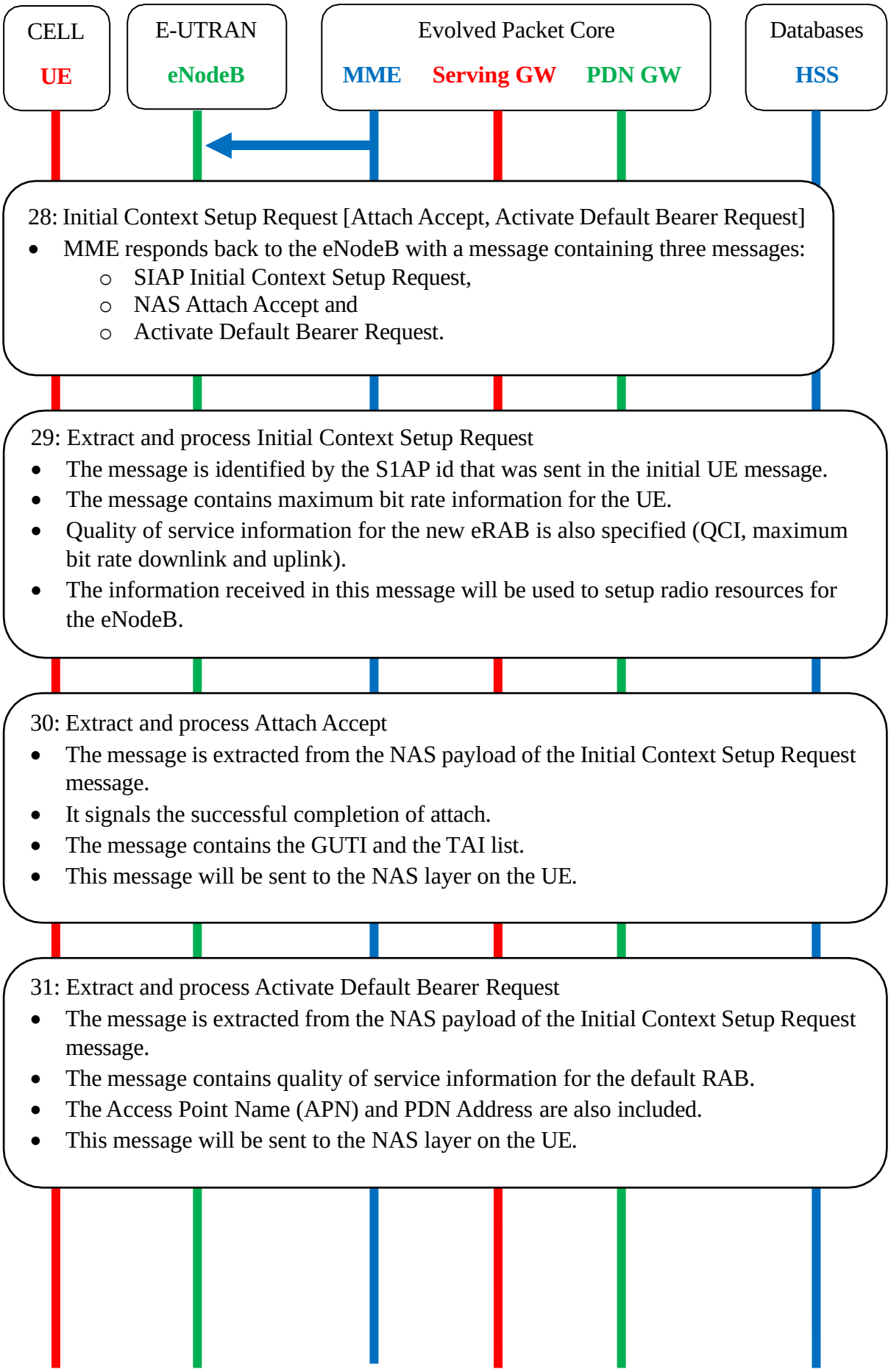

CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
Attach and Authentication
6: RRC Connection Setup Complete + NAS Attach Request
The UE signals the setup of the RRC connection.
The message is also used to initiate the Attach procedure by sending the Attach Request as NAS Payload.
The attach message contains the old GUTI (Globally Unique Temporary Identifier).
The message contains,
UL-SCH,
Selected PLMN Identity,
Old TAI,
Old GUMMEI,
Old GUTI,
Selected PLMN Identity.
7: Identify the MME from the Old GUMMEI.
8: S1AP Initial UE Message [Attach Request + PDN Connectivity Request]
The Attach message is sent in the Initial UE message to the MME over the S1AP interface.
The "Attach Request" is embedded in the Initial UE Message.
The message also includes the PDN Connectivity Request message.
The Tracking Area Identify (TAI) and E-UTRAN Cell Global Identifier (ECGI) are also included.
Note: The eNodeB uses the eNB-UE-S1APID to uniquely identify the UE.
The message contains,
id = eNB UE S1AP ID,
Tracking Area Id = TAI+Cell Id,
EPS Attach Type = EPS Attach,
Identity = Old GUTI,
EPS Encryption and Integrity Algorithms, Selected Network.

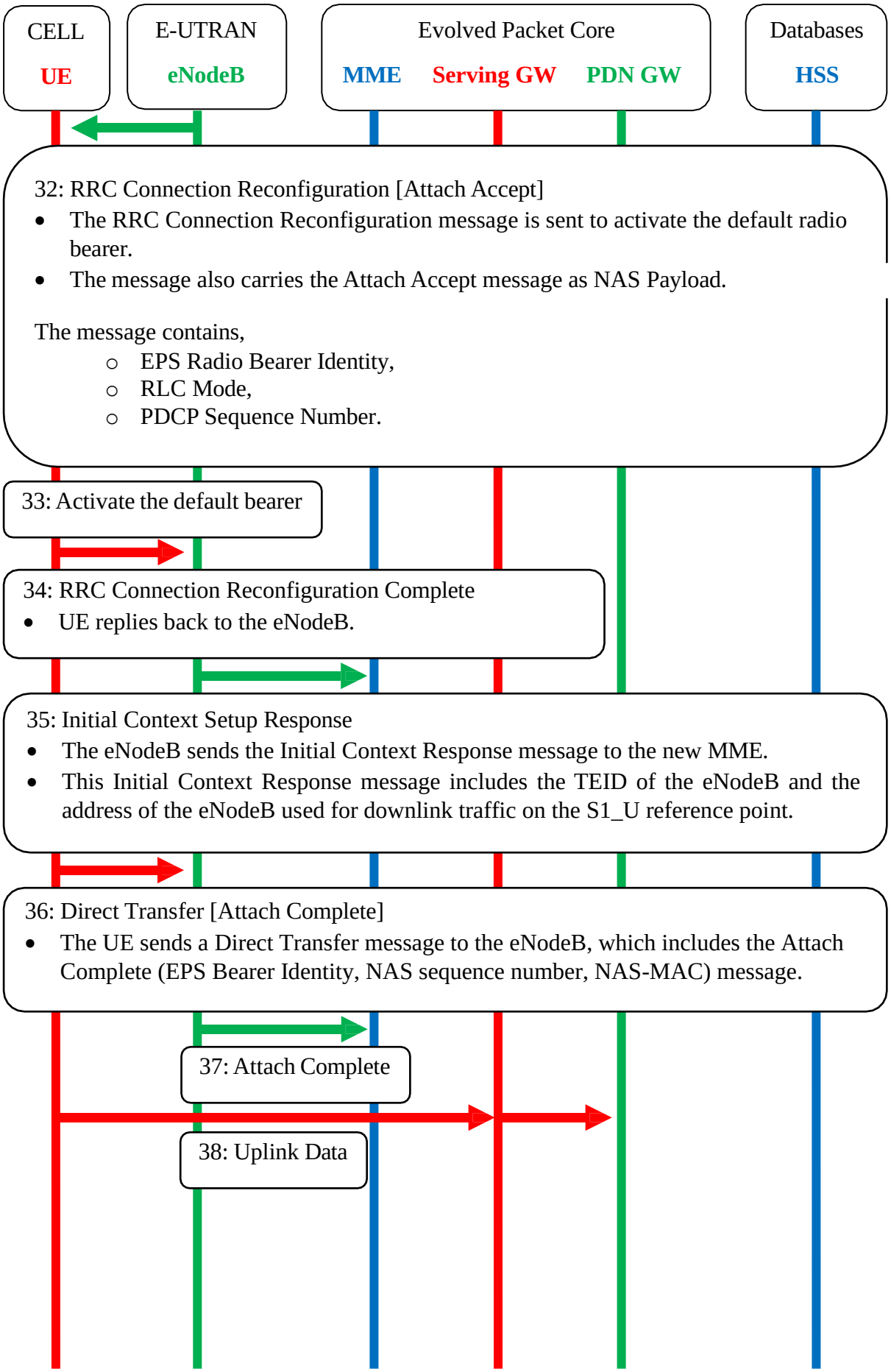

CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
OLD MME
9: Identification Request [Attach Request].
• Since the UE identified itself with GUTI and the MME has changed since detach.
• The new MME uses the GUTI received from the UE to derive the old MME, and send an Identification Request (old GUTI, complete Attach Request message) to the old MME to request the IMSI.
OLD MME
10: Identification Response.
• The old MME responds with Identification Response.
The message contains,
○ IMSI,
○ unused EPS Authentication Vectors,
○ KSIASME,
○ KASME.
11: Authentication Info Request
12: Authentication Info Answer
13: Ciphered Options Request
• Since the UE has set the Ciphered Options Transfer Flag in the Attach Request message, the ciphered Options i.e. PCO or APN or both, shall now be retrieved from the UE.
14: Ciphered Options Response

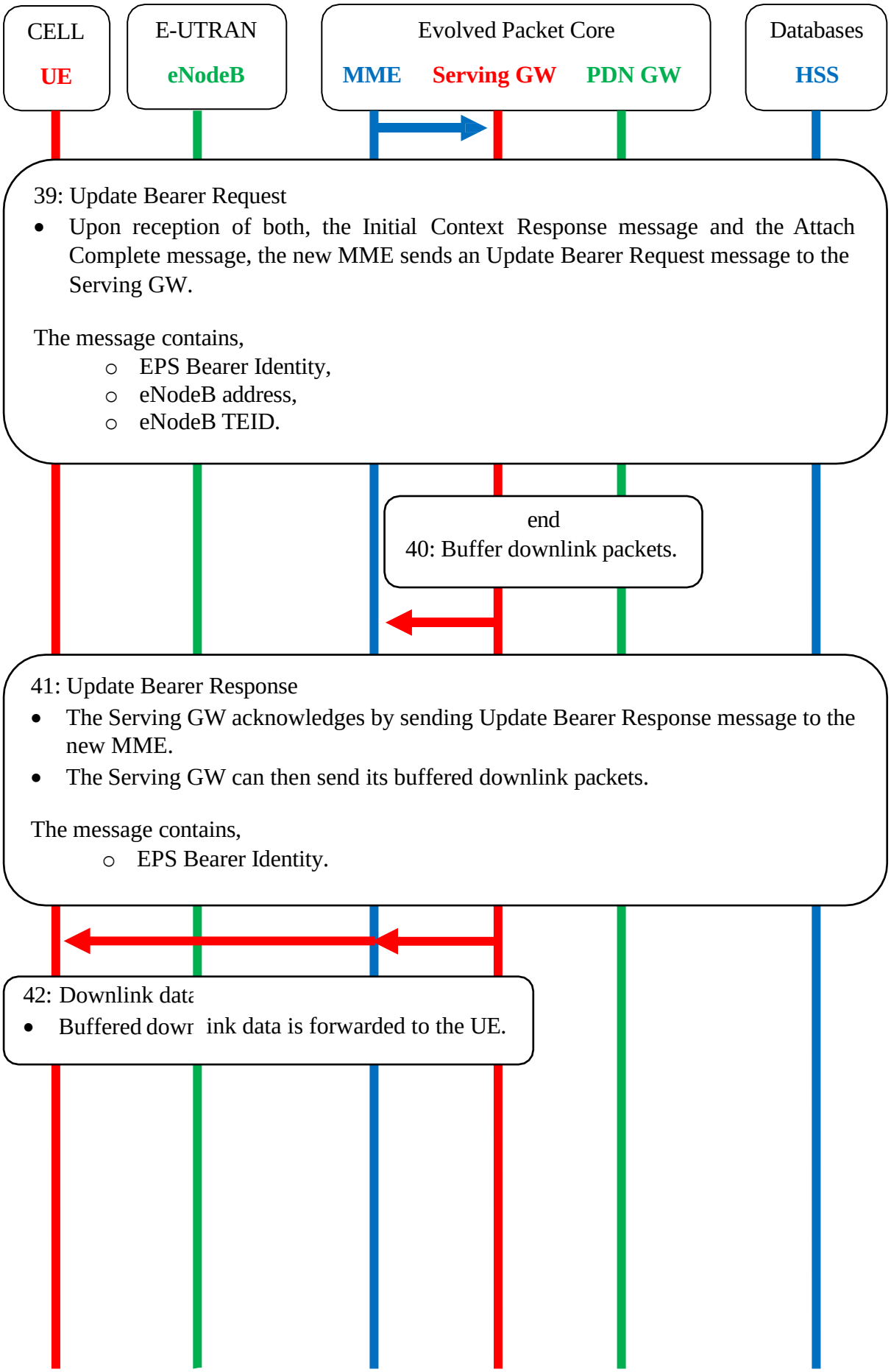

CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
15: Update Location Request
Since the MME has changed since the last detach. The MME sends an Update Location Request message to the HSS.
The MME capabilities indicate the MME's support for regional access restrictions functionality. Update Type indicates this is Attach procedure.
The message contains,
Origin,
Destination,
User Name = IMSI,
Visited PLMN Id.
OLD MME
16: Cancel Location
The HSS sends Cancel Location to the old MME.
The old MME acknowledges with Cancel Location Ack and removes the MM and bearer contexts.
The message contains,
IMSI,
Cancellation Type.
OLD MME
17: Cancel Location Ack, IMSI


CELL
s
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
18: Update Location Request Answer
• The HSS acknowledges the Update Location message by sending an Update Location Answer message to the new MME.
• The Subscription Data contains PDN subscription contexts.
• Each PDN subscription context contains an 'EPS subscribed QoS profile' and the subscribed APN-AMBR.
• The new MME validates the UE's presence in the (new) TA. If all checks are successful, then the new MME constructs a context for the UE.
The message contains,
○ IMSI,
○ Aggregate MBR (DL and UL),
○ MSISDN,
○ APN = PDN GW Address, QCI, Charging, Aggregate MBR (DL, UL).
Default Radio Bearer Setup
19: GTP Create Session Request
• MME initiates the default route establishment by asking the SGW to create a GTP tunnel.
• The APN specified by the UE is used for default bearer activation.
• The IP Address assigned to the UE is also included along with the downlink and uplink maximum data rates allowed at the APN level.
The message contains,
○ Sender F-TEID for Control Plane,
○ ARP,
○ QCI,
○ MSISDN,
○ TAI, PGW IP Address,
○ PDN IP Address,
○ APN,
○ IP Address Assigned to UE.
20: Create a new entry in EPS Bearer table.


CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
21: Map from APN to PDN Gateway.
begin
22: Buffer downlink packets.
23: Create Default Bearer Request.
Serving Gateway sends Create Default Bearer Request message to the PDN GW.
The message contains,
IMSI,
MSISDN,
APN,
Serving GW Address.
24: Create a new entry in its EPS bearer context table and generates a Charging Id
The new entry allows the P GW to route user plane PDUs between the S GW and the packet data network, and to start charging.
25: Create Default Bearer Response
The message contains,
PDN GW User Plane address,
PDN GW TEIDs User and Control Plane,
EPS Bearer Identity and QoS.
26: Downlink Data
Serving Gateway receives the first downlink data block.
This block is buffered at the Serving GW".
27: GTP Create Session Response


CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
28: Initial Context Setup Request [Attach Accept, Activate Default Bearer Request]
MME responds back to the eNodeB with a message containing three messages:
SIAP Initial Context Setup Request,
NAS Attach Accept and
Activate Default Bearer Request.
29: Extract and process Initial Context Setup Request
The message is identified by the S1AP id that was sent in the initial UE message.
The message contains maximum bit rate information for the UE.
Quality of service information for the new eRAB is also specified (QCI, maximum bit rate downlink and uplink).
The information received in this message will be used to setup radio resources for the eNodeB.
30: Extract and process Attach Accept
The message is extracted from the NAS payload of the Initial Context Setup Request message.
It signals the successful completion of attach.
The message contains the GUTI and the TAI list.
This message will be sent to the NAS layer on the UE.
31: Extract and process Activate Default Bearer Request
The message is extracted from the NAS payload of the Initial Context Setup Request message.
The message contains quality of service information for the default RAB.
The Access Point Name (APN) and PDN Address are also included.
This message will be sent to the NAS layer on the UE.


CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
32: RRC Connection Reconfiguration [Attach Accept]
The RRC Connection Reconfiguration message is sent to activate the default radio bearer.
The message also carries the Attach Accept message as NAS Payload.
The message contains,
EPS Radio Bearer Identity,
RLC Mode,
PDCP Sequence Number.
33: Activate the default bearer
34: RRC Connection Reconfiguration Complete
UE replies back to the eNodeB.
35: Initial Context Setup Response
The eNodeB sends the Initial Context Response message to the new MME.
This Initial Context Response message includes the TEID of the eNodeB and the address of the eNodeB used for downlink traffic on the S1_U reference point.
36: Direct Transfer [Attach Complete]
The UE sends a Direct Transfer message to the eNodeB, which includes the Attach Complete (EPS Bearer Identity, NAS sequence number, NAS-MAC) message.
37: Attach Complete
38: Uplink Data


CELL
UE
E-UTRAN
eNodeB
Evolved Packet Core
MME
Serving GW
PDN GW
Databases
HSS
39: Update Bearer Request
• Upon reception of both, the Initial Context Response message and the Attach Complete message, the new MME sends an Update Bearer Request message to the Serving GW.
The message contains,
○ EPS Bearer Identity,
○ eNodeB address,
○ eNodeB TEID.
end
40: Buffer downlink packets.
41: Update Bearer Response
• The Serving GW acknowledges by sending Update Bearer Response message to the new MME.
• The Serving GW can then send its buffered downlink packets.
The message contains,
○ EPS Bearer Identity.
42: Downlink data
• Buffered downlink data is forwarded to the UE.

IN LAB

Files Requirement:

- During Experiment 1, **.pcap** files were generated for CN and eNB in Step 8 and Step 14

Let's

- *Identify the communication protocols for message exchange between the entities.*
- *Analyze the communication information.*
- *Interpreting the sequence of messages.*

	eNB	MME	SPGWU	SPGWC	HSS
eNB		**192.168.1.2 (S1)**	**192.168.1.31:2522 (S1U)**		
MME	**192.168.1.2 (S1)**			**127.0.11.1 (S11)**	
SPGWC		**127.0.11.1 (S11)**	**127.0.12.1 (Sx)**		
SPGWU	**192.168.1.2:2522 (S1U)**			**127.0.12.2 (Sx)**	
HSS		**127.0.0.10 (S6A)**			
User Database					**172.17.0.2**

Table 1: IP configuration of 4G Evolved Packet Core entities.

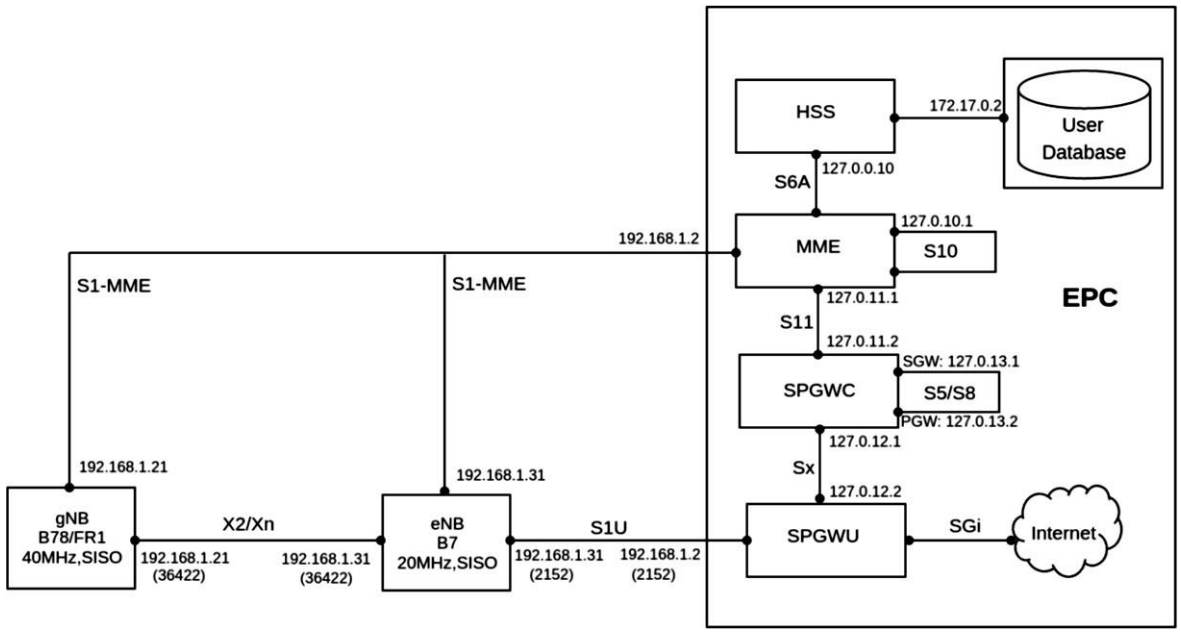
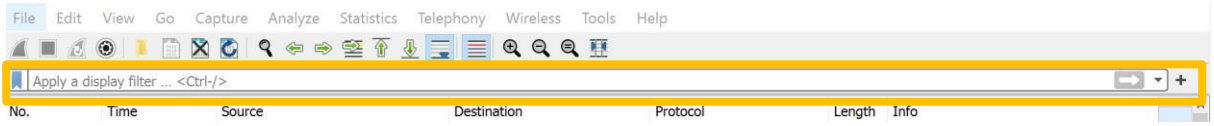


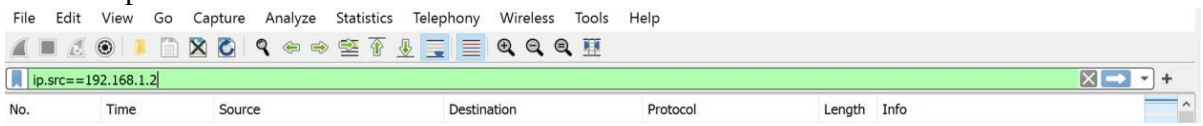
Figure 1: 4G Evolved Packet Core entities.

Step 1: Open the .pcap file (CN)

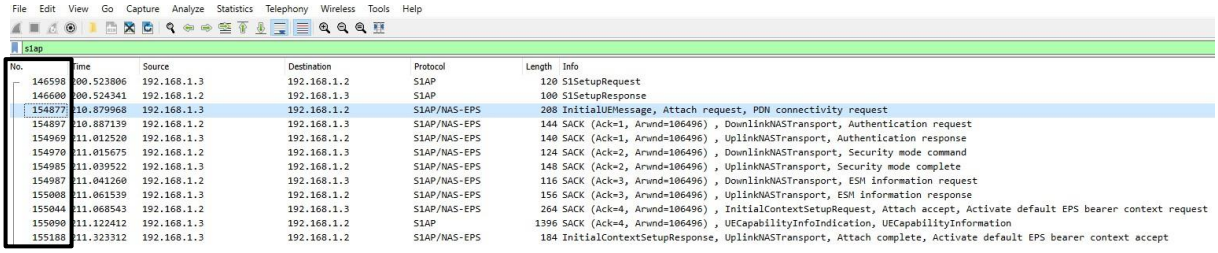
In the "Apply a display filter" enter ip.src==<ip address>



For example



Note: *We highly recommend recording the number sequence for exchange identification. It will be helpful to complete the Step 3, interference and analysis section.*



Step 2:

- **Identify the communication protocols for message exchange between the 4G Evolved Packet Core entities.**

5 2 MARK*

- **Analyze the communication information.**

5 1 MARK*

No.	Time	Source	Destination	protocol	Length	info
3569	355.63393	127.0.11.1	127.0.11.2	GTPv2	211	Create Session Request
3580	355.727128	127.0.11.1	127.0.11.2	GTPv2	91	Modify Bearer Request

No.	Time	Source	Destination	protocol	Length	info
3571	355.636004	127.0.12.1	127.0.12.2	PFCP	166	PFCP Session Establishment Request
3582	355.730809	127.0.12.1	127.0.12.2	PFCP	144	PFCP Session Modification Request

No.	Time	Source	Destination	protocol	Length	info
3570	355.635202	127.0.13.1	127.0.13.2	GTPV2	203	Create session request
3584	355.732341	127.0.13.1	127.0.13.2	GTPV2	78	Modify bearer request

No.	Time	Source	Destination	protocol	Length	info
3526	355.409666	127.0.0.1	127.0.0.10	DIAMETER	336	Authentication-Information Request
3537	355.412089	127.0.0.1	127.0.0.10	TCP	68	Acknowledgement

No.	Time	Source	Destination	protocol	Length	info
3529	355.410597	172.17.0.1	172.17.0.2	TCP	166	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=2855 Ack=2858 Win=64128 Len=98 TSval=815244505 TSecr=2220105601
3532	355.411777	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=2953 Ack=3050 Win=64128 Len=0 TSval=815244506 TSecr=2220132905
3533	355.411778	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3532#1] 35164 → 9042 [ACK] Seq=2953 Ack=3050 Win=64128 Len=0 TSval=815244506 TSecr=2220132905
3534	355.412013	172.17.0.1	172.17.0.2	CQL	199	v3 C->S Type QUERY
3535	355.412015	172.17.0.1	172.17.0.2	TCP	199	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=2953 Ack=3050 Win=64128 Len=131 TSval=815244506 TSecr=2220132905
3540	355.412384	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=3084 Ack=3063 Win=64128 Len=0 TSval=815244507 TSecr=2220132906
3541	355.412385	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3540#1] 35164 → 9042 [ACK] Seq=3084 Ack=3063 Win=64128 Len=0 TSval=815244507 TSecr=2220132906
3549	355.628145	172.17.0.1	172.17.0.2	CQL	589	v3 C->S Type QUERY
3550	355.628151	172.17.0.1	172.17.0.2	TCP	589	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=3084 Ack=3063 Win=64128 Len=521 TSval=815244722 TSecr=2220132906

3555	355.632586	172.17.0.1	172.17.0.2	CQL	155	v3 C->S Type QUERY
3556	355.632589	172.17.0.1	172.17.0.2	TCP	155	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=3605 Ack=4920 Win=64128 Len=87 TSval=815244727 TSecr=2220133125
3561	355.632952	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=3692 Ack=4991 Win=64128 Len=0 TSval=815244727 TSecr=2220133126
3562	355.632953	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3561#1] 35164 → 9042 [ACK] Seq=3692 Ack=4991 Win=64128 Len=0 TSval=815244727 TSecr=2220133126
3563	355.633034	172.17.0.1	172.17.0.2	CQL	280	v3 C->S Type QUERY
3564	355.633036	172.17.0.1	172.17.0.2	TCP	280	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=3692 Ack=4991 Win=64128 Len=212 TSval=815244727 TSecr=2220133126
3567	355.63389	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=3904 Ack=5004 Win=64128 Len=0 TSval=815244728 TSecr=2220133127
3568	355.633891	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3567#1] 35164 → 9042 [ACK] Seq=3904 Ack=5004 Win=64128 Len=0 TSval=815244728 TSecr=2220133127

Step 3: Establish the sequence of the information exchange from the above observation.

No.	Time	Source	Destination	protocol	Length	info
3525	355.406217	192.168.1.3	192.168.1.2	S1AP/NAS-EPS	212	InitialUEMessage, Attach request, PDN connectivity request
3526	355.409666	127.0.0.1	127.0.0.10	DIAMETER	336	cmd=3GPP-Authentication-Information Request(318) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=1379fdd8 e2e=0 |
3527	355.409695	127.0.0.10	127.0.0.1	TCP	68	3868 → 35546 [ACK] Seq=1285 Ack=1489 Win=65280 Len=0 TSval=554766239 TSecr=1145062469
3528	355.410594	172.17.0.1	172.17.0.2	CQL	166	v3 C->S Type QUERY
3529	355.410597	172.17.0.1	172.17.0.2	TCP	166	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=2855 Ack=2858 Win=64128 Len=98 TSval=815244505 TSecr=2220105601
3530	355.411767	172.17.0.2	172.17.0.1	CQL	260	v3 S->C Type RESULT[Malformed Packet]
3531	355.411767	172.17.0.2	172.17.0.1	TCP	260	[TCP Retransmission] 9042 → 35164 [PSH, ACK] Seq=2858 Ack=2953 Win=65024 Len=192 TSval=2220132905 TSecr=815244505
3532	355.411777	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=2953 Ack=3050 Win=64128 Len=0 TSval=815244506 TSecr=2220132905
3533	355.411778	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3532#1] 35164 → 9042 [ACK] Seq=2953 Ack=3050 Win=64128 Len=0 TSval=815244506 TSecr=2220132905
3534	355.412013	172.17.0.1	172.17.0.2	CQL	199	v3 C->S Type QUERY
3535	355.412015	172.17.0.1	172.17.0.2	TCP	199	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=2953 Ack=3050 Win=64128 Len=131 TSval=815244506 TSecr=2220132905
3536	355.412083	127.0.0.10	127.0.0.1	DIAMETER	356	Authentication-Information Answer(318) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=1379fdd8 e2e=0 |
3537	355.412089	127.0.0.1	127.0.0.10	TCP	68	35546 → 3868 [ACK] Seq=1489 Ack=1573 Win=65280 Len=0 TSval=1145062471 TSecr=554766241
3538	355.412374	172.17.0.2	172.17.0.1	CQL	81	v3 S->C Type RESULT

3539	355.412374	172.17.0.2	172.17.0.1	TCP	81	[TCP Retransmission] 9042 → 35164 [PSH, ACK] Seq=3050 Ack=3084 Win=64896 Len=13 TSval=2220132906 TSecr=815244506
3540	355.412384	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=3084 Ack=3063 Win=64128 Len=0 TSval=815244507 TSecr=2220132906
3541	355.412385	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3540#1] 35164 → 9042 [ACK] Seq=3084 Ack=3063 Win=64128 Len=0 TSval=815244507 TSecr=2220132906
3542	355.412658	192.168.1.2	192.168.1.3	S1AP/NAS-EPS	144	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request
3543	355.58629	192.168.1.3	192.168.1.2	S1AP/NAS-EPS	140	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response
3544	355.589372	192.168.1.2	192.168.1.3	S1AP/NAS-EPS	124	SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command
3545	355.606255	192.168.1.3	192.168.1.2	S1AP/NAS-EPS	148	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete
3546	355.607258	192.168.1.2	192.168.1.3	S1AP/NAS-EPS	116	SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, ESM information request
3547	355.626076	192.168.1.3	192.168.1.2	S1AP/NAS-EPS	156	SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, ESM information response
3548	355.627271	127.0.0.1	127.0.0.10	DIAMETER	324	cmd=3GPP-Update-Location Request(316) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=1379fdd9 e2e=0 |
3549	355.628145	172.17.0.1	172.17.0.2	CQL	589	v3 C->S Type QUERY
3550	355.628151	172.17.0.1	172.17.0.2	TCP	589	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=3084 Ack=3063 Win=64128 Len=521 TSval=815244722 TSecr=2220132906
3551	355.631869	172.17.0.2	172.17.0.1	CQL	1925	v3 S->C Type RESULT[Malformed Packet]
3552	355.631869	172.17.0.2	172.17.0.1	TCP	1925	[TCP Retransmission] 9042 → 35164 [PSH, ACK] Seq=3063 Ack=3605 Win=64384 Len=1857 TSval=2220133125 TSecr=815244722
3553	355.63194	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=3605 Ack=4920 Win=64000 Len=0 TSval=815244726 TSecr=2220133125
3554	355.631944	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3553#1] 35164 → 9042 [ACK] Seq=3605 Ack=4920 Win=64000 Len=0 TSval=815244726

						TSecr=2220133125
3555	355.632586	172.17.0.1	172.17.0.2	CQL	155	v3 C->S Type QUERY
3556	355.632589	172.17.0.1	172.17.0.2	TCP	155	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=3605 Ack=4920 Win=64128 Len=87 TSval=815244727 TSecr=2220133125
3557	355.632925	127.0.0.10	127.0.0.1	DIAMETER	1064	cmd=3GPP-Update-Location Answer(316) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=1379fdd9 e2e=0 |
3558	355.632932	127.0.0.1	127.0.0.10	TCP	68	35546 → 3868 [ACK] Seq=1745 Ack=2569 Win=64640 Len=0 TSval=1145062692 TSecr=554766462
3559	355.632943	172.17.0.2	172.17.0.1	CQL	139	v3 S->C Type RESULT
3560	355.632943	172.17.0.2	172.17.0.1	TCP	139	[TCP Retransmission] 9042 → 35164 [PSH, ACK] Seq=4920 Ack=3692 Win=64384 Len=71 TSval=2220133126 TSecr=815244727
3561	355.632952	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=3692 Ack=4991 Win=64128 Len=0 TSval=815244727 TSecr=2220133126
3562	355.632953	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3561#1] 35164 → 9042 [ACK] Seq=3692 Ack=4991 Win=64128 Len=0 TSval=815244727 TSecr=2220133126
3563	355.633034	172.17.0.1	172.17.0.2	CQL	280	v3 C->S Type QUERY
3564	355.633036	172.17.0.1	172.17.0.2	TCP	280	[TCP Retransmission] 35164 → 9042 [PSH, ACK] Seq=3692 Ack=4991 Win=64128 Len=212 TSval=815244727 TSecr=2220133126
3565	355.63387	172.17.0.2	172.17.0.1	CQL	81	v3 S->C Type RESULT
3566	355.63387	172.17.0.2	172.17.0.1	TCP	81	[TCP Retransmission] 9042 → 35164 [PSH, ACK] Seq=4991 Ack=3904 Win=64256 Len=13 TSval=2220133127 TSecr=815244727
3567	355.63389	172.17.0.1	172.17.0.2	TCP	68	35164 → 9042 [ACK] Seq=3904 Ack=5004 Win=64128 Len=0 TSval=815244728 TSecr=2220133127
3568	355.633891	172.17.0.1	172.17.0.2	TCP	68	[TCP Dup ACK 3567#1] 35164 → 9042 [ACK] Seq=3904 Ack=5004 Win=64128 Len=0 TSval=815244728 TSecr=2220133127
3569	355.63393	127.0.11.1	127.0.11.2	GTPv2	211	Create Session Request
3570	355.635202	127.0.13.1	127.0.13.2	GTPv2	203	Create Session Request
3571	355.63600	127.0.12.1	127.0.12.2	PFCP	166	PFCP Session Establishment

	4					Request
3572	355.636114	127.0.12.2	127.0.12.1	PFCP	114	PFCP Session Establishment Response
3573	355.636457	127.0.13.2	127.0.13.1	GTPv2	141	Create Session Response
3574	355.636778	127.0.11.2	127.0.11.1	GTPv2	141	Create Session Response
3575	355.637639	192.168.1.2	192.168.1.3	S1AP/NAS-EPS	264	SACK (Ack=4, Arwnd=106496) , InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request
3576	355.703018	192.168.1.3	192.168.1.2	SCTP	1516	SACK (Ack=4, Arwnd=106496) DATA (TSN=5) (Message Fragment)
3577	355.703019	192.168.1.3	192.168.1.2	S1AP	192	UECapabilityInfoIndication, UECapabilityInformation
3578	355.703102	192.168.1.2	192.168.1.3	SCTP	64	SACK (Ack=6, Arwnd=104935)
3579	355.72605	192.168.1.3	192.168.1.2	S1AP	104	InitialContextSetupResponse
3580	355.727128	127.0.11.1	127.0.11.2	GTPv2	91	Modify Bearer Request
3581	355.728623	127.0.13.1	127.0.13.2	GTPv2	78	Modify Bearer Request
3582	355.730809	127.0.12.1	127.0.12.2	PFCP	144	PFCP Session Modification Request
3583	355.731164	127.0.12.2	127.0.12.1	PFCP	75	PFCP Session Modification Response
3584	355.732341	127.0.13.2	127.0.13.1	GTPv2	90	Modify Bearer Response
3585	355.733718	127.0.11.2	127.0.11.1	GTPv2	90	Modify Bearer Response
3586	355.927993	192.168.1.2	192.168.1.3	SCTP	64	SACK (Ack=7, Arwnd=106496)
3587	355.928627	192.168.1.3	192.168.1.2	S1AP/NAS-EPS	128	UplinkNASTransport, Attach complete, Activate default EPS bearer context accept

Step 4: Calculate the total time taken to establish PDN connectivity.
Hint: APN and IP address allocation.

Ans:

The total time is the difference between the timestamps of the first message (**Attach Request**) and the last message (**Attach Complete**).
For example, based on the log from the experiment (from the provided lab steps):

1. **Attach Request** timestamp: 355.406217 seconds.
2. **Attach Complete** timestamp: 355.928627 seconds.

Total time calculation:
Total time=Attach Complete time−Attach Request time
Total time=355.928627 s−355.406217 s=0.52241
Thus, the total time taken to establish **PDN connectivity** is approximately **0.522 seconds**.