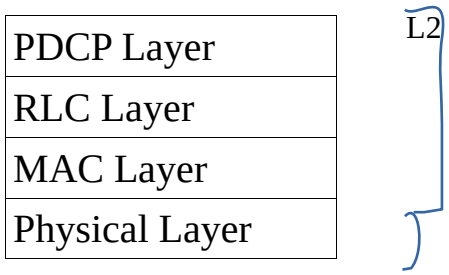
> LTE Lyaers



1. PDCP (Packet Data Compression Protocol) Layer

> Sequence Numbering Procedure

PDCP add Sequence number on each incomming packets to manage on reciever side such as

> Is the data gatting delivered in order

> Is there any duplicate packet

> combine multiple chunk of data block into an original big chunk data.

> Header Compression Procedure Using ROHC (Robust Header compression) method

> Only on User Plane packets not control Plane Packets

> we can also disable header compression in user plane as well

> Integrity Protection Process

> Applies only on Control Plane not User plane Packets

> we can also disable Integrity process in control plane as well

> Ciphering Process

> Applies on both user plane and Control plane

> we can disable this process

> PDCP Header is added and getting out fron PDCP

2. RLC (Radio Link Layer) Layer

> Three types of RLC modes

1. TM (Transparant Mode)

> packets goes through this without any modification

> Add or Remove any header to the input data

> Does not spilt the input data into multiple segments

> Does not combine the multiple input data into a single big chunk.

> only **buffering** being done only for small time or till next packet came

ex. Broadcasting SIB and MIB ect.

2. UM (Unacknowledgement)

> Does not require any respone (ACK/NACK) from reciever

> Buffering

> Assign sequence number

> Segmentation

> Concatenation

> Reordering

> Add/Remove RLC Header

Ex. UDP, live streaming

3. AM (Acknowledgement Mode)

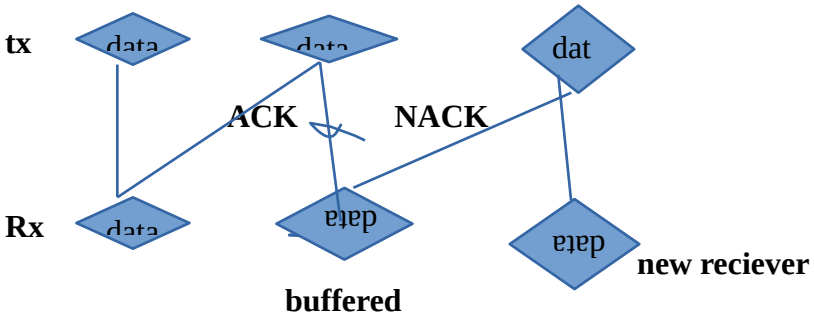
> Require respone (ACK/NACK) from reciever.

> Creates two copies of packets, one transmit to MAC layer and another copy to retransmession buffer. If does not recieve response, it sends packets in the retransmission buffer.

> Error correction by ARQ

3 MAC (Medium Access Control)Layer

> HARQ = ARQ + FEC/ Soft Combination



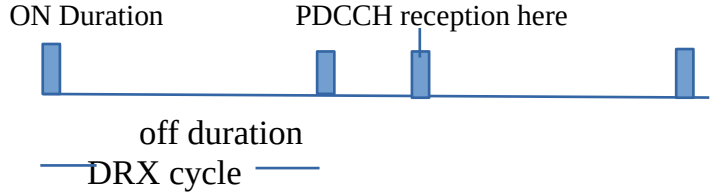
buffered + new recieved = Data2

> Multiplexing/Demultiplexing

> Controller

DRX (Discontinuous Reception/Transmission)

> DRX is a Machanism in which UE gets into sleep mode for a certain period of time and wake up for another period of time



DRX cycle = on duration + off Duration

> Scheduling/Priortization

> Initiate RACH

4. Physical Layer

> Error Detection

> FEC Encoding and Decoding

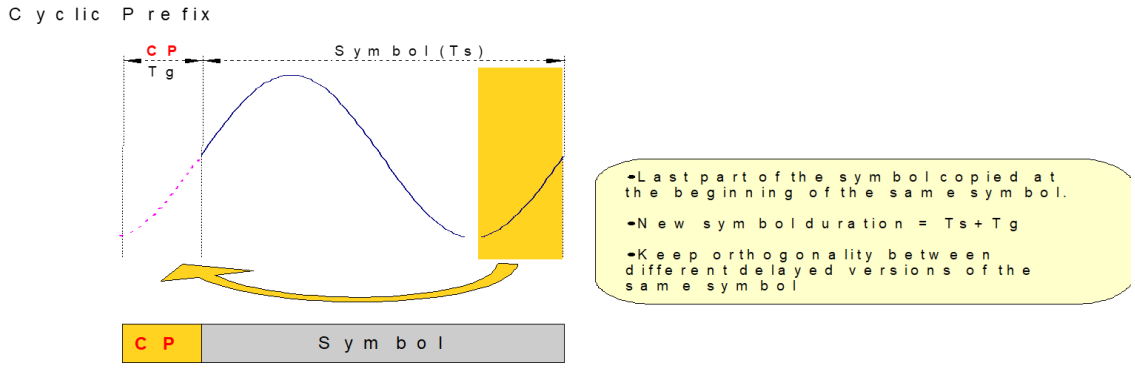
> Rate Matching

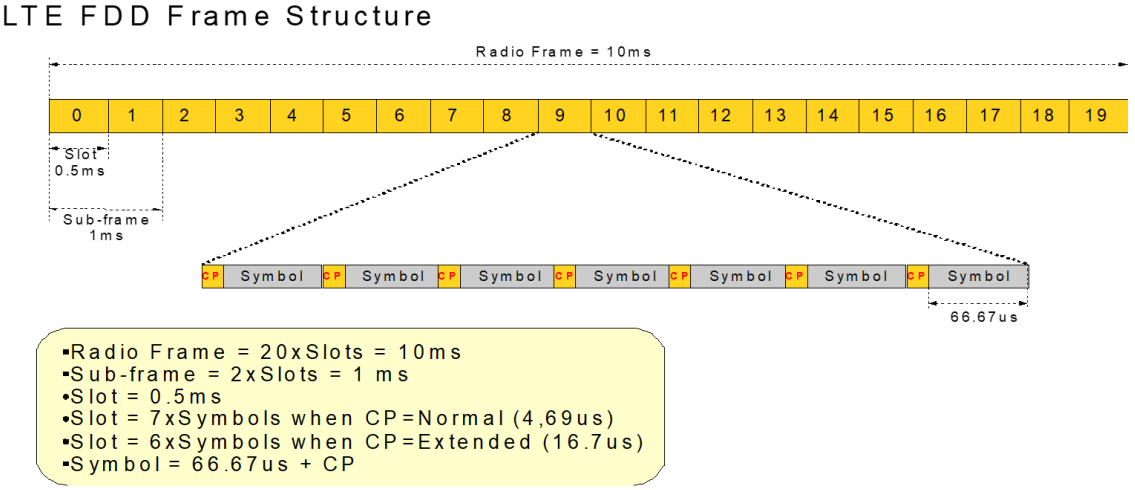
> Power Weighting

> Modulation and Demodulation

. OFDMA (orthogonal to each other and space between sub-carriers is equal to bandwidth)Downling direction

Bandwidth 1.4, 3, 5, 10, 15, 20 Khz (Space between sub-carriers) on 15 Kh -> Symbol duration = 1/15KHz = 66.67uS



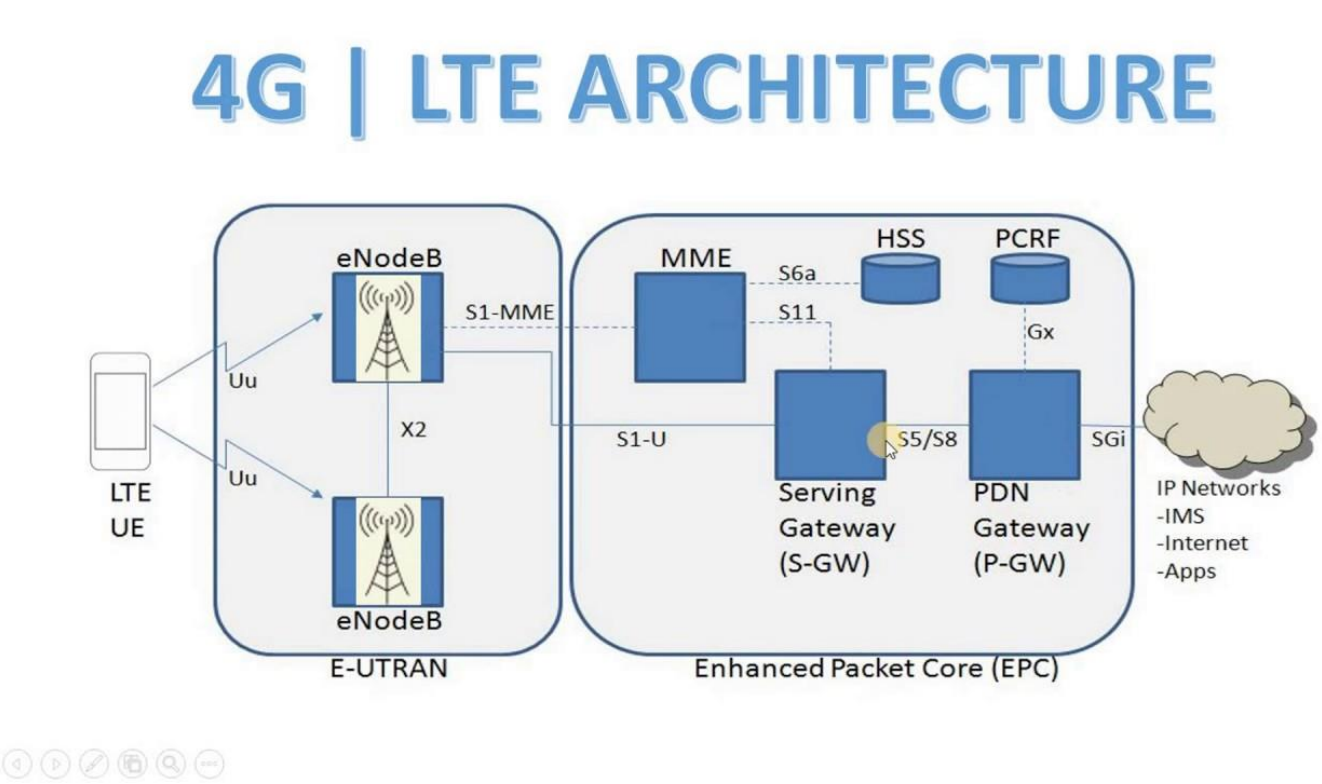


. SC-OFDMA Upling Direction
Difference
OFDMA uses more sub-carriers for same symbol
SC-OFDMA uses one sub-carriers for same symbol

> **Maping of Physical Layer**

LTE Architecture.

The CN (called EPC in SAE) is responsible for the overall control of the UE and establishment of the bearers. The main logical nodes of the EPC are:
• PDN Gateway (P-GW);
• Serving Gateway (S-GW);
• Mobility Management Entity (MME).



• **PCRF.** It is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF) which resides in the P-GW. The PCRF provides the QoS authorization (QoS class identifier and bitrates) that decides how a certain data flow will be treated in the PCEF and ensures that this is in accordance with the user's subscription profile.

• **Home Location Register (HLR).** The HLR contains users' SAE subscription data such as the EPS-subscribed QoS profile and any access restrictions for roaming (see Section 2.2.3). It also holds information about the PDNs to which the user can connect. In addition the HLR holds dynamic information such as the identity of the MME to which the user is currently attached or registered. The HLR may also integrate the Authentication Centre (AuC) which generates the vectors for authentication and security keys.

• **P-GW.** The P-GW is responsible for IP address allocation for the UE, as well as QoS enforcement and flow-based charging according to rules from the PCRF. The P-GW is responsible for the filtering of downlink user IP packets into the different QoS based bearers. The P-GW performs QoS enforcement for Guaranteed Bit Rate (GBR) bearers. It also serves as the mobility anchor for inter-working with non-3GPP technologies such as CDMA2000 and WiMAX networks.

• **S-GW.** All user IP packets are transferred through the S-GW, which serves as the local mobility anchor for the data bearers when the UE moves between eNodeBs. It also retains the information about the bearers when the UE is in idle state and temporarily buffers downlink data while the MME initiates paging of the UE to re-establish the bearers.

In addition, the S-GW performs some administrative functions in the visited network such as collecting information for charging (e.g. the volume of data sent to or received from the user), and legal interception. It also serves as the mobility anchor for inter-working with other 3GPP technologies such as GPRS and UMTS.

MME. The MME is the control node which processes the signalling between the UE and the CN. The protocols running between the UE and the CN are known as the Non-Access Stratum (NAS) protocols.
The main functions supported by the MME are classified as:
Functions related to bearer management. This includes the establishment, maintenance and release of the bearers, and is handled by the session management layer in the NAS protocol.
Functions related to connection management. This includes the establishment of the connection and security between the network and UE, and is handled by the connection or mobility management layer in the NAS protocol layer.

UE Attach Procedure

There are two types of connections.
> ECM Connection :- This one is used for signaling purpose.
> EMM Connection :- This one is used for transfering IP packets.

ECM connection
This is a combination of rrc connection (UE to Enodeb) and s1 signaling (Enodeb to mme).

RACH procedure and RRC Connection etablishment

Random Access Procedure in LTE

Background

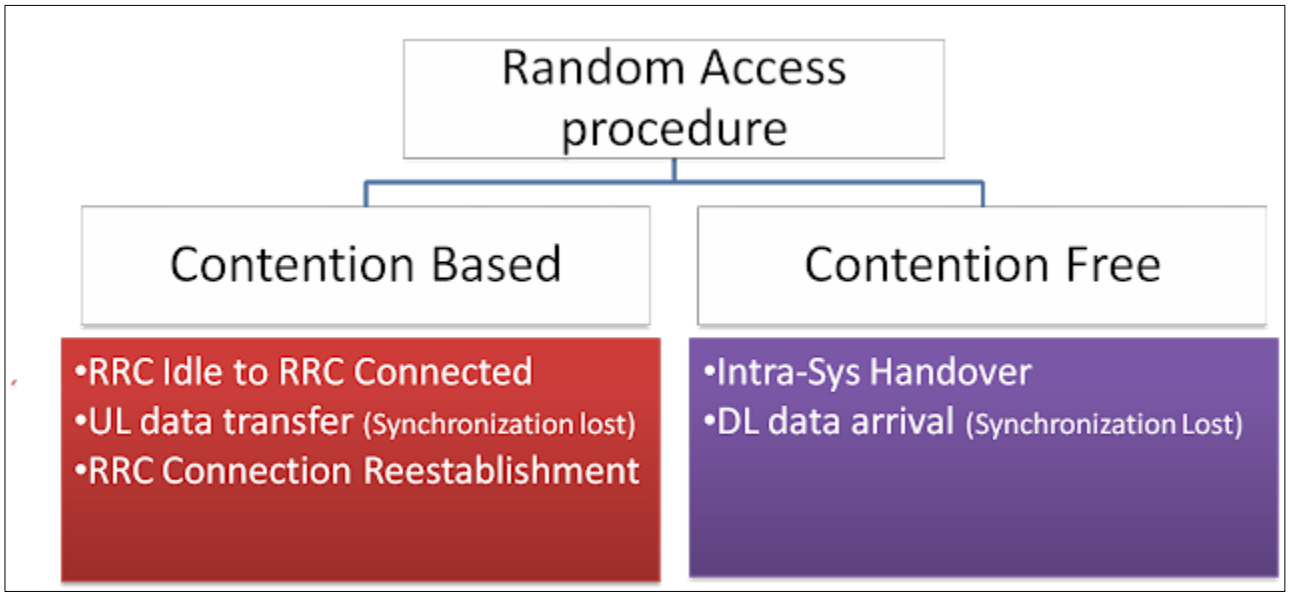
When you switch on smartphone for the very first time, it will start searching for the network. There is a possibility that there are many networks or to put in other words , there are many frequencies from different operators available in the air to which UE (user equipment) can connect. Therefore, UE needs to synchronize to each frequency and check whether this is frequency from the right operator to which it wants to connect to. UE does this by going through very initial synchronisation process.
Once synchronized UE reads the master information block and System information blocks to check whether this is the right PLMN. Lets assume that it finds that PLMN value to be correct and so UE will proceed with reading System information block 1 and System information block 2. The next step is known as Random Access Procedure in which the network for the first time knows that some UE is trying to get access.

At this stage, UE does not have any resource or channel available to inform network about its desire to connect to it so it will send its request over the shared medium. Now there are two possibilities at this stage, either there are many other UEs in the same area (same cell) sending same request in which there is also a possibility of collision among the requests coming from various other UEs. Such random access procedure is called contention based Random access procedure. In second scenario, network can inform UE to use some unique identity to prevent its request from colliding with requests coming from other UEs. The second scenario is called contention free or non contention based random access procedure.

RACH preambles

The concept of RACH preamble though a little confusing is important in understanding the random access procedure.

When UE sends the very first message of random access procedure to some network, it basically sends specific pattern or signature which is called RACH preambles. The preamble value differentiate requests coming from different UEs. But if two UEs uses same RACH preambles at same time then there can be collision. There are totally 64 such patterns or signature available to the UE for the very first message of random access procedure and UE will decide any one of them randomly for contention-based random access procedure but for non-contention based procedure, actually network will inform UE about which one to use



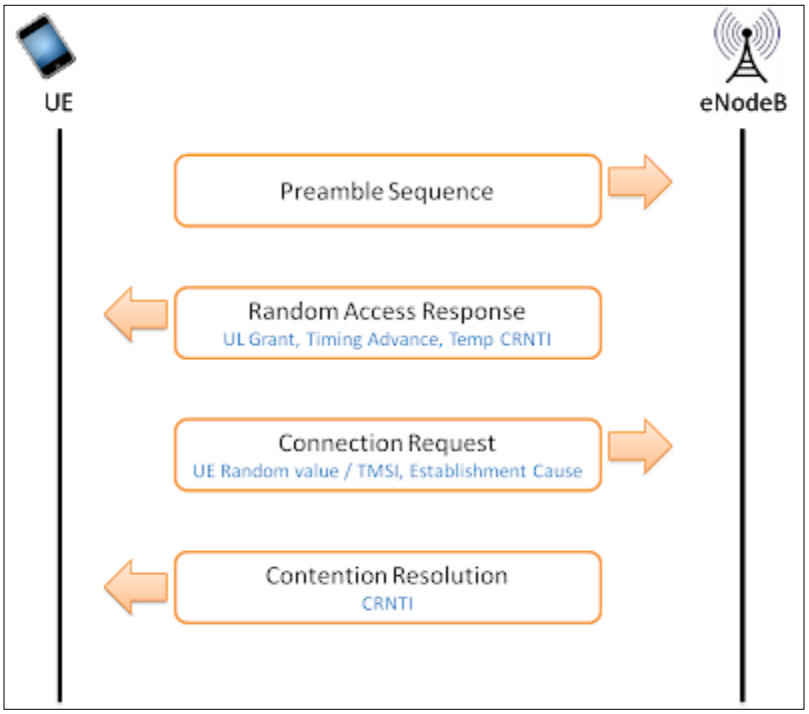
In case, when UE goes from idle state to RRC connected state, there is no way for network to inform

UE about which preamble out of 64 values should be used. Therefor UE has no choice but to use one of the preambles randomly which also result in possibility of collision if the same preamble is being used by another UE, provided the requests comes at same time (same frame)

In another scenario if UE has to take handover to another eNB, in this case actually the UE can be informed about which preamble it can use, since UE is already in connected state

Steps of Random access procedure

Random access procedure consist of four steps explained below (Only contention based procedure is shown below)



Step 1: Msg1

- UE selects one of the 64 available RACH preambles
- Now UE also needs to give its own identity to the network so that network can address it in next step. The identity which UE will use is called RA-RNTI (Random access radio network temporary identity). Basically its not some value sent by UE but interestingly RA RNTI is determined from the time slot number in which the preamble is sent
- If UE does not receive any response from the network, it increases its power in fixed step and sends RACH preamble again

Step 2: Msg2

- eNodeB sends "Random Access Response" to UE on DL-SCH (Downlink shared channel) addressed to RA-RNTI calculated from the timeslot in which preamable was sent, as explained in step 1 (about RA-RNTI calculation)
- The message carries following information
- Temporary C-RNTI: Now eNB gives another identity to UE which is called temporary C-RNTI (cell radio network temporary identity) for further communication
- Timing Advance Value: eNodeB also informs UE to change its timing so it can compensate for the round trip delay caused by UE distance from the eNodeB
- Uplink Grant Resource: Network (eNodeB) will assign initial resource to UE so that it can use UL-SCH (Uplink shared channel)

Step 3: Msg3

- Using UL-SCH, UE sends "RRC connection request message" to eNodeB
- UE is identified by temporary C-RNTI (assigned in the previous step by eNodeB)
- The message contains following
- UE identity (TMSI or Random Value)
- TMSI is used if UE has previously connected to the same network. With TMSI value, UE is identified in the core network
- Random value is used if UE is connecting for the very first time to network. Why we need random value or TMSI? Because there is possibility that Temp-CRNTI has been assigned to more than one UEs in previous step, due to multiple requests coming at same time (Collision scenario explained later)
- Connection establishment cause: The shows the reason why UE needs to connect to network

Step 4: Msg4

- eNodeB responds with contention resolution message to UE whose message was successfully received in step 3. This message is address towards TMSI value or Random number (from previous steps) but contains the new C RNTI which will be used for the further communication

Collision Scenario

The above example didn't consider any collision. Collision can occur because of following example scenario

- Lets assume two UEs send same RACH preamble at same time in step 1
- Same Temp C-RNTI and up-link grant will be received by two UEs in step 2
- In step 3 eNodeB may be able to receive Msg3 from only one UE or none of them due to interference.
- In step 4 the UE which does not receive Msg4 from eNodeB will back-off after expiration of RACH specific timers. Possibility is also that none of them receive Msg4
- UE which receive msg4 will move to next step and decode RRC connection setup message

RRC Connection Setup

The RRC connection setup message contain configuration details for SRB1 so that later messages can be transferred via SRB1. Remember the SRB2 is always configured after the security activation.

RRC Connection setup message include default configuration for SRB1 but can also include configuration information for PUSCH, PUCCH, PDSCH physical channels, CQI Reports, Sounding reference signal, antenna configuration and scheduling requests.

RRC Connection Setup Complete

After receiving the RRC Connection setup message, UE complete the three way handshake procedure by sending 'RRC Connection setup complete' message and moves to RRC Connected mode.

the Attach Request message[1] that was delivered to the NAS layer is sent to the eNB when delivering the RRC Connection Setup Complete message, as embedded in the Dedicated NAS Information field (DedicatedInfoNAS) of the RRC Connection Setup Complete message.

The message contains following information

- *selectedPLMN-Identity*: This is equal to 1 if UE selects the first PLMN from the *plmn-identityList* included in SIB1 or 2 if the second PLMN is selected in case UE belongs to more than one PLMN
- *dedicatedInfoNAS*: This IE is used to transfer UE specified NAS layer information between network and UE.

(2) S1 Signaling Connection Establishment

Control messages between the eNB and the MME are sent over S1-MME interface as embedded in S1AP messages. S1AP messages are delivered through S1 signaling connections dedicatedly established for each user. The S1 signaling connections are

defined by an ID pair (eNB UE S1AP ID, MME UE S1AP ID) allocated by the eNB and the MME for identifying UEs.
In Figure 2, an Attach Request message, the first NAS message, arrives at the eNB before S1 signaling connection is established. The eNB then allocates an eNB UE S1AP ID for establishment of S1 signaling connection, and sends the MME an Attach Request message, as embedded in an Initial UE Message. The Attach Request message is delivered as embedded in the NAS-PDU field of the Initial UE Message. The Initial UE Message consists of the following information elements:

Initial UE Message (eNB UE S1AP ID, NAS-PDU, TAI, ECGI, RRC Establishment Cause)

- **eNB UE S1AP ID:** ID identifying UEs in an eNB over S1-MME interface (Uplink)
- **NAS-PDU:** a NAS message (**Attach Request**)
- **TAI:** shows the TA a UE is located in
- **ECGI:** shows the cell a UE is located in
- **RRC Establishment Cause = mo-Signaling:** indicates the signaling was generated by a UE

When the MME receives the Initial UE Message from the eNB over S1-MME, it allocates an MME S1AP UE ID for the UE. Now with this newly allocated ID and the previously allocated eNB UE S1AP ID, S1 signaling connection between the two entities are established. The MME UE S1AP ID is used later when the MME identifies UEs over S1-MME interface (Downlink).

(3) ECM S1 Connection Establishment

Through Steps (1) and (2) above, the ECM connection between the NAS layers of the UE and the MME is established. Then, the UE transits to EMM-Registered[2], ECM-Connected and RRC-Connected state.

(4) IMSI Acquisition

The NAS layer of the MME acquires the IMSI of the UE from the Attach Request message sent from the NAS layer of the UE, and finds out the UE's security capability by learning what security algorithms the UE can use from the UE's network capability information.

After collecting the UE's IMSI and security capability information from the Attach Request (IMSI, UE Network Capability) message received from the UE, the MME performs the authentication and NAS security Setup procedures for secured delivery of NAS messages, by using the collected information, and in accordance with the EPS-AKA (Evolved Packet System-Authentication and Key Agreement). The two procedures - authentication and NAS security setup - are described in Sections 2.2 and 2.3, respectively. As they are already explained in details in our LTE Security documents [3][4], they will be discussed briefly here in this document.

Authentication

3.1 Authentication Request by UE

1 [UE → MME] Request by UE for Network Registration

When a UE attempts to access the network for initial attach, it delivers Attach Request (IMSI, UE Network Capability, KSI_{ASME}=7) message to an MME. And this triggers EPS AKA procedure. The following information elements are included in the Attach Request message:

- IMSI: International Mobile Subscriber Identity, a unique identifier associated with the user
- UE Network Capability: security algorithms available to UE
- KSI_{ASME}=7: indicates UE has no authentication key

UE network capability informs the MME of what kinds of capability the UE has related to EPS, and indicates which NAS and AS security algorithms, i.e., EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA) are supported by the UE. Each of them has a value of 1 bit that is presented as on (supported) or off (not supported) (e.g. EEA0=on, EEA1=on, EEA2=off, …, EIA1=on, EIA2=on, …). Table 1 lists some of UE network capability information, specifically ciphering and integrity protection algorithms defined in [3].

3.2 Authentication Data Exchange between MME and HSS

2 [MME → HSS] Request by MME for Authentication Data

The MME recognizing the UE has no K_{ASME} available initiates LTE authentication procedure to get new authentication data by sending an Authentication Information Request (IMSI, SN ID, n, Network Type) message to the HSS. Message parameters used for this purpose are as follows:

- IMSI: a unique identifier associated with the user
- SN ID (Serving Network ID): refers to the network accessed by the user. Consists of PLMN ID (MCC+MNC).
- n (number of Authentication Vectors): No. of authentication vectors that MME requests
- Network Type: type of the network accessed by UE (E-UTRAN herein)

Upon receipt of the Authentication Information Request message from the MME, the HSS generates RAND and SQN, and creates XRES, AUTN, CK and IK using EPS AKA algorithm with LTE key (K), SQN and RAND. Thereafter, using CK, IK, SQN and SN ID, it derives a top-level key (K_{ASME}) of the access network, from Key Derivation Function (KDF), to be delivered to the MME. KDF is a one-way has function. Since SN ID is required when deriving K_{ASME}, K_{ASME} is derived again if the serving network is changed. After K_{ASME} is derived, the HSS forms authentication vectors AV_i=($RAND_i$, $AUTN_i$, $XRES_i$, K_{ASMEi}), i=0..n.

3 [MME ← HSS] Response by HSS to the Authentication Data Request

THe HSS forms as many AVs as requested by the MME and then delivers an Authentication Information Answer (AVs) message to the MME.

3.3 Mutual Authentication by UE and MME

The MME stores the AVs received from the HSS, and selects one of them to use in LTE authentication of the UE. In Figure 3, the MME selected ith AV (AV_i). K_{ASME} is a base key of MME and serves as a top-level key in the access network. It stays within EPC only and is not delivered to the UE through E-UTRAN, which is not secure. The MME allocates KSI_{ASME}, an index for K_{ASME}, and delivers it instead of K_{ASME} to the UE so that the UE and the MME can use it as a substitute for K_{ASME} (in Fig. 3, KSI_{ASME}=1).

4 [UE ← MME] Request by MME for User Authentication

The MME keeps K_{ASMEi} and $XRES_i$ in AV_i but delivers KSI_{ASMEi}, in substitution for K_{ASMEi}, $RAND_i$ and $AUTN_i$ as included in the Authentication Request (KSI_{ASMEi}, $RAND_i$, $AUTN_i$) message to the UE. $XRES_i$ is used later in 5 when authenticating the user.

The UE, upon receiving the Authentication Request message from the MME, delivers $RAND_i$ and $AUTN_i$ to USIM. USIM, using the same EPS AKA algorithm that the HSS used, derives RES, $AUTN_{UE}$, CK and IK with the stored LTE key (K) and $RAND_i$ and SQN generated from the HSS[5]. The UE then compares $AUTN_{UE}$ generated using EPS AKA algorithm and AUTN received from MME ($AUTN_i$ in Fig. 3) to authenticate the LTE network (the serving network).

5 [UE → MME] Response by UE to User Authentication

Once the UE completes the network authentication, it delivers an Authentication Response (RES) including RES generated using EPS AKA algorithm to MME. If the network authentication using AUTN fails in 4, UE sends an Authentication Failure (CAUSE) message that contains a CAUSE field stating reasons for such failure.

When the MME receives the Authentication Response message from the UE, it compares RES generated by the UE and $XRES_i$ of the AV received from the HSS to authenticate the user.

USIM delivers CK and IK to the UE after its network authentication is completed. The UE derives K_{ASME} using Key Derivation Function (KDF) with CK, IK, SQN and SN ID and stores it using KSI_{ASME} received from the MME as its index. Thereafter, KSI_{ASME} is used instead of K_{ASME} during the NAS security setup between the UE and the MME.

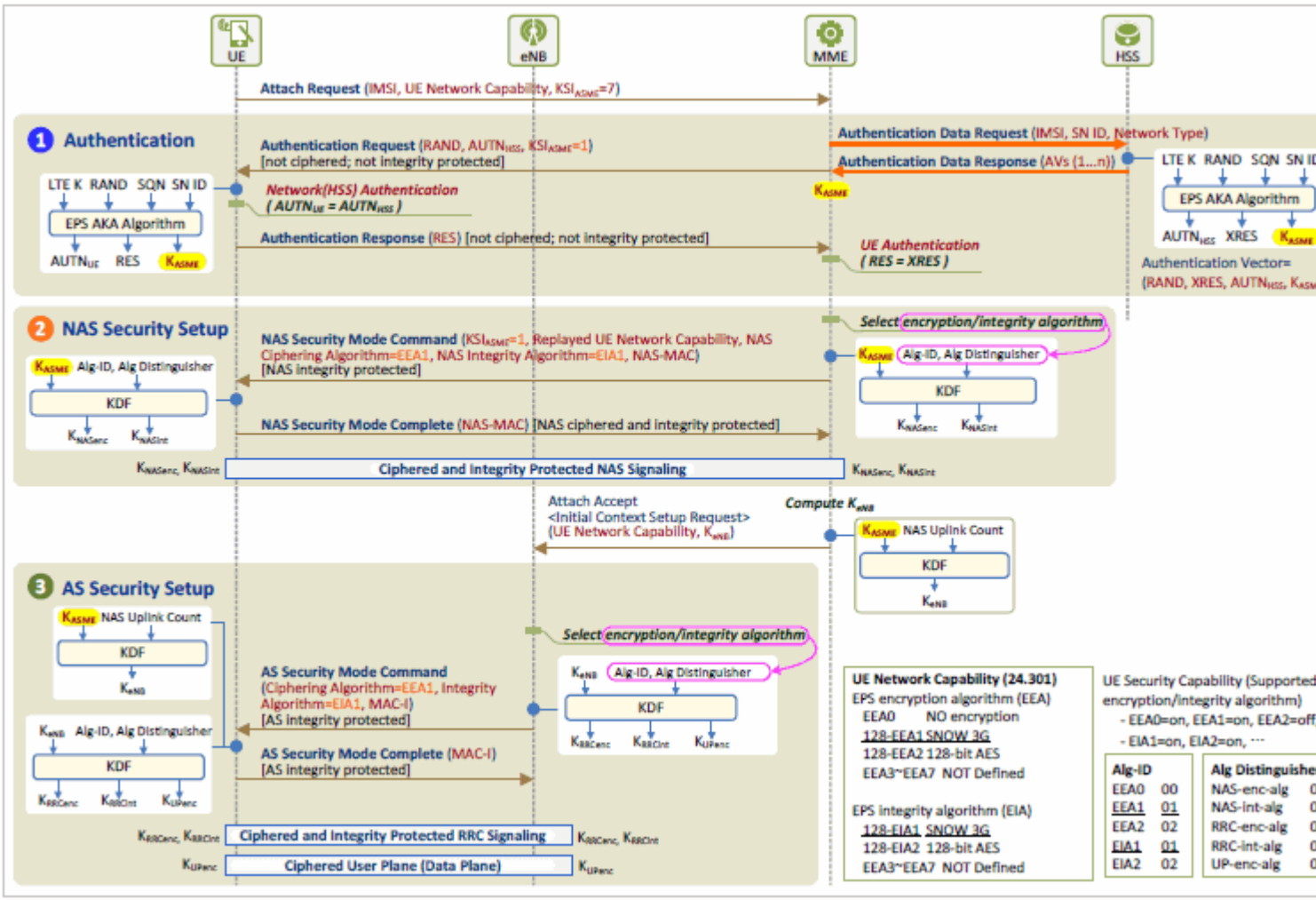
LTE Security Concept

2 NAS Security: performs integrity protection/verification and ciphering (encryption/decryption) of NAS signaling between a UE and an MME.

3 AS Security

- performs integrity protection/verification and ciphering of RRC signaling between a UE and an eNB.

- performs ciphering of user traffic between a UE and an eNB.



2 NAS Security

Once the UE and MME have authenticated each other and the same key K_{ASME} is shared, NAS security setup procedure begins. In this procedure, NAS security keys to be used when delivering NAS signaling messages are derived from K_{ASME} for secure delivery of these messages. This procedure consists of a round trip of NAS signaling messages (Security Mode Command and Security Mode Complete message), and begins when the MME delivers a Security Mode Command message to the UE.

First, the MME selects NAS security algorithms (Alg-ID: Algorithm ID) and uses them to create an integrity key (K_{NASint}) and a ciphering key (K_{NASenc}) from K_{ASME}. Then, it applies K_{NASint} to the Security Mode Command message to generate an NAS message authentication code (NAS-MAC, Message Authentication Code for NAS for Integrity). The MME then delivers the Security Mode Command message including the selected NAS security algorithms and the NAS-MAC to the

UE. As the UE does not know the selected encryption algorithm yet, this message is integrity protected only but not ciphered.

Upon receiving the Security Mode Command message, the UE verifies the integrity thereof by using the NAS integrity algorithm selected by the MME and uses NAS integrity/ciphering algorithm to generate NAS security keys (K_{NASint} and K_{NASenc}) from K_{ASME}. Then it ciphers the Security Command Complete message with K_{NASenc} and generates a message authentication code, NAS-MAC with K_{NASint} to the ciphered message. Now it forwards the ciphered and integrity protected message to the MME with the NAS-MAC included.

Once the MME successfully verifies the integrity of the received Security Mode Complete message and has them decrypted using the NAS security keys (K_{NASint} and K_{NASenc}), the NAS security setup procedure is completed.

Once the NAS security is set up, NAS signaling messages between the UE and the MME are ciphered and integrity protected by the NAS security keys and then securely delivered over radio links.

3 AS Security

After NAS security setup is finished, AS security setup procedure between a UE and an eNB begins. In this procedure, AS security keys to be used when delivering RRC signaling messages and IP packets are derived from K_{eNB} for secure delivery of these data. This procedure consists of a round trip of RRC signaling messages (Security Mode Command and Security Mode Complete message), and begins when an eNB delivers Security Mode Command message to the UE.

First, the MME calculates K_{eNB} from K_{ASME} and delivers it to the eNB, which uses it to perform the AS security setup procedure. The eNB selects AS security algorithms (Alg-ID: Algorithm ID) and uses them to create an integrity key (K_{RRCint}) and a ciphering key (K_{RRCenc}), from $K_{eNB.}$ to be used for RRC signaling messages, and a ciphering key (K_{UPenc}) to be used in the user plane. Then, it applies K_{RRCint} to the Security Mode Command message to generate a message authentication code (MAC-I, Message Authentication Code for Integrity). The eNB now delivers the Security Mode Command message including the selected AS security algorithms and the MAC-I to the UE.

Upon receiving the Security Mode Command message from the eNB, the UE verifies the integrity thereof by using the AS integrity algorithm selected by the eNB and uses AS integrity/ciphering algorithm to generate AS security keys (K_{RRCint}, K_{RRCenc} and K_{UPenc}). Then it generates a message authentication code, MAC-I, with the RRC integrity key to the Security Command Complete message, and then forwards the message including the MAC-I to the eNB.

When the eNB successfully verifies the integrity of the received Security Mode Complete message by using the AS integrity key, the AS security setup procedure is completed.

After the AS security is set up, RRC signaling messages between the UE and the eNB are ciphered and integrity protected by the AS security keys, and user IP packets are encrypted and then securely delivered over radio links.

2.4 Location Update

Once the procedures for authentication and NAS security setup are completed, now the MME has to register the subscriber in the network, and find out what services the subscriber can use. To this end, the MME notifies the HSS the subscriber is registered in the network and located in its TAs, and then downloads information about the subscriber from the HSS. All these are done through the location update procedure, and by using Diameter protocol over the S6a interface between the MME and the HSS. The call flows during this procedure are as in Figure 6.

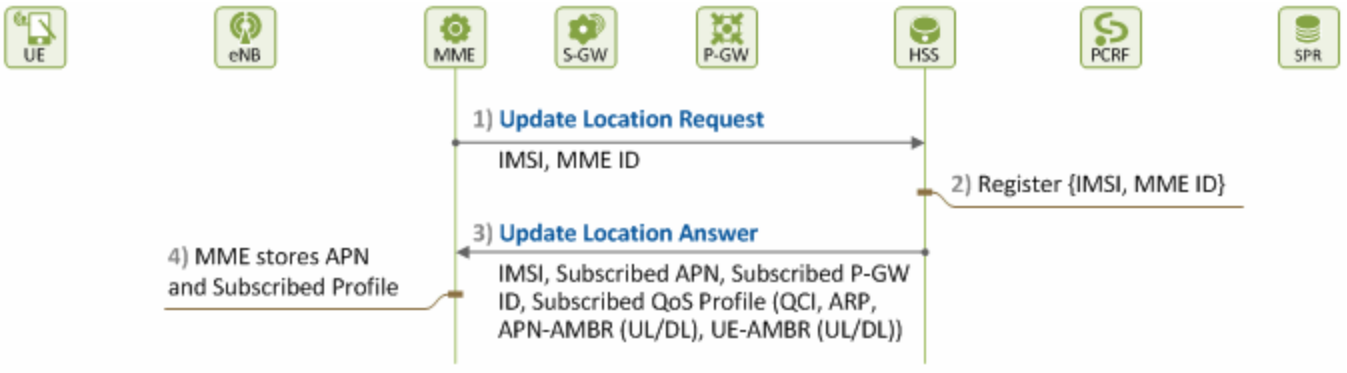


Figure 6. Procedure for Location Update

1) [MME → HSS] Notifying UE Location

The MME sends an Update Location Request (IMSI, MME ID) message to the HSS in order to notify of the UE's registration and obtain the subscription information of the UE.

2) [HSS] UE Location Update

The HSS registers the MME ID to indicate in which MME the UE is located in.

3) [MME ← HSS] Delivering User Subscription Information

The HSS sends the MME subscription information of the subscriber as included in an Update Location Answer message, so that the MME can create an EPS session and a default EPS bearer for the subscriber. The subscription information included in the Update Location Answer message is as follows:

Update Location Answer (IMSI, Subscribed APN, Subscribed P-GW ID, Subscribed QoS Profile)

- **Subscribed APN:** APN that a user is subscribing to (e.g. Internet service)
- **Subscribed P-GW ID:** an ID for P-GW through which a user can access the Subscribed APN
- **Subscribed QoS Profile[5] (UE-AMBR(UL/DL), QCI, ARP, APN-AMBR(UL/DL))**
  - **UE-AMBR (UL/DL):** the aggregate bandwidth of all non-GBR bearers that a UE can have Determined by MME and controlled by eNB.
  - **QCI, ARP, APN-AMBR (UL/DL):** QoS applied to the Subscribed APN

4) [MME] Storing Subscription Information

The MME receives the Update Location Answer message from the HSS, and stores the subscription information from the message.

From the downloaded subscription information, the MME can check what services the user is subscribing to, and to which APN and with what QoS level the resources are to be allocated.

ESM Information Request Procedure

●□□□□□□□The ESM information request procedure is used by the network to retrieve ESM information, i.e. protocol configuration options, APN, or both from the UE during the attach procedure if the UE has indicated (in the *PDN CONNECTIVITY REQUEST*) that it has ESM information that needs to be sentsecurity protected.

●□□□□□□□The purpose of this procedure is to provide privacy for the ESM information if ciphering is enabled in the network.

●□□□□□□□The network initiates the ESM information request procedure by sending a*ESM INFORMATION REQUEST* message to the UE and starts the timer T3489.

●□□□□□□□This message shall be sent only after the security context has been setup, and if the ESM information transfer flag has been set in the *PDN CONNECTIVITY REQUEST* message.

●□□□□□□□The MME shall set the EPS bearer identity of the *ESM INFORMATION REQUEST*message to the value "*no EPS bearer identity assigned*" and include the PTI from the associated *PDN CONNECTIVITY REQUEST* message.

●□□□□□□□After receiving the *ESM INFORMATION REQUEST* message, the UE shall send an *ESM INFORMATION RESPONSE* message to the network.

●□□□□□□□The UE shall include all the protocol configuration options that need to be transferred security protected, and APN if required, to the network in the *ESM INFORMATION RESPONSE (see the example below)*message.

●□□□□□□□The UE shall set the EPS bearer identity of the *ESM INFORMATION RESPONSE*message to the value "no EPS bearer identity assigned" and include the PTI from the *ESM INFORMATION REQUEST* message

2.5 EPS Session Establishment

The MME, based on the subscription information, establishes an EPS session and a default EPS bearer for the user. By doing so, the MME allocates the network/radio resources for providing each user with satisfying QoS they are subscribing to. Figure 7 and Figure 8 illustrate procedures for establishing an EPS session and a default EPS bearer, respectively.

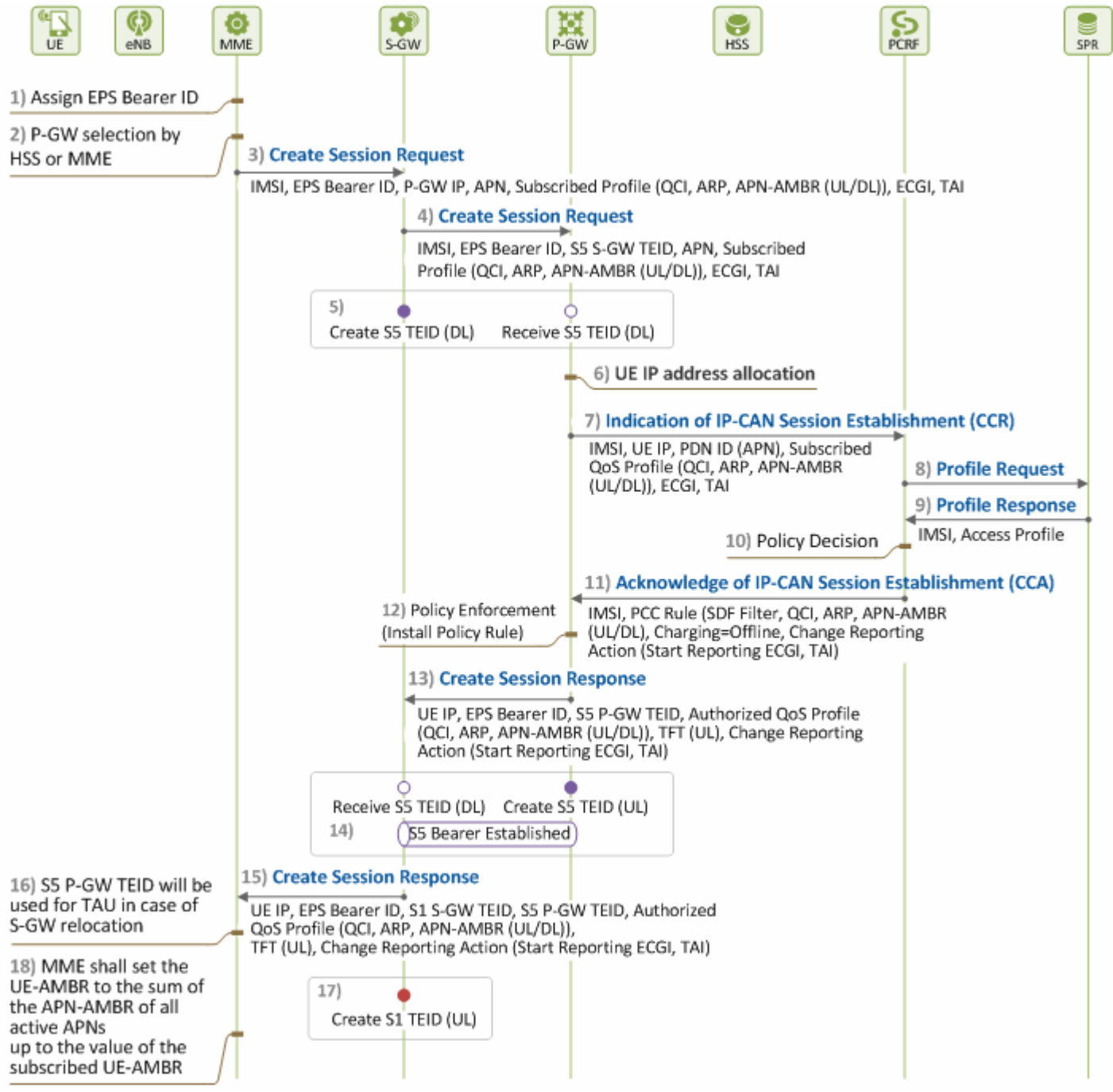


Figure 7. Procedure for EPS Session Establishment (1)

1) [MME] Assigning EPS Bearer ID

The MME selects a value from 5~15, and allocates it as an EPS Bearer ID (EBI) in order to establish a default EPS bearer for the newly attached user.

2) [MME] Selecting P-GW

The MME checks the APN received from the HSS, and decides to which P-GW to connect to access the APN. This decision can be made based on the subscription information received from the HSS (specifically, P-GW ID). Or if there is no such information, the MME queries the DNS server for APN FQDN (e.g. internet.apn.epc.mnc05.mcc450.3gppnetwork.org), and selects one from the returned P-GW IP address list in accordance with its P-GW selection policies[6]. At this time, it also chooses which S-GW to go through to get the selected P-GW.

◇ 3) ~ 4) Request for EPS Session Creation

The MME requests creation of an EPS session and a default EPS bearer by sending a Create Session Request message to the P-GW selected in Step 2) above. Here, the MME includes the subscription information it received from the HSS in the message, so that the P-GW can use it when requesting PCRF for EPS session creation. At this time, UE-AMBR is not included as it is to be determined by the MME.

3) [MME → S-GW] Request for EPS Session Creation

The MME and the S-GW communicate over S11 interface in the control plane using GTP protocol (GTP-C)[7]. The MME sends the S-GW selected in Step 2) a Create Session Request message, with the following parameters:

Create Session Request (IMSI, EPS Bearer ID, P-GW IP, APN, Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL)), ECGI, TAI)

- **IMSI:** a fixed subscriber ID
- **EPS Bearer ID:** a default EPS bearer ID assigned by MME
- **P-GW IP:** an IP address of the P-GW that MME selected for EPS Session/Bearer creation
- **APN:** APN that a user is subscribing to
- **Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL)):** QoS information to be applied when establishing an EPS default bearer
- **ECGI:** a cell in which UE is located
- **TAI:** a TA in which UE is located

4) [S-GW → P-GW] Request for EPS Session Creation

The S-GW and the P-GW communicate over S5 interface in the user and control planes using GTP protocol (UP: GTP-U, CP: GTP-C). The S-GW allocates a downlink S5 TEID (S5 S-GW TEID) to establish S5 GTP to the P-GW indicated in the received Create Session Request message. Then, it sends the ID along with other parameters, as included in the Create Session Request message, to the P-GW.

Create Session Request (IMSI, EPS Bearer ID, S5 S-GW TEID, APN, Subscribed Profile (QCI, ARP, APN- AMBR (UL/DL)), ECGI, TAI)

5) [S5 Bearer: Downlink]

Once Step 4) is completed, the downlink S5 GTP-U tunnel is created, allowing the P-GW to send downlink traffic to the S-GW. In Figures 7 and 8, the entity that allocates and sends a GTP tunnel TEID is marked as "fill" (●), and the one that receives it is marked as "empty" (○).

6) [P-GW] Allocating User IP Address

The P-GW, upon receiving the Create Session Request message, realizes the user is attempting to access the network again with IMSI. So, it allocates an IP address to the UE so that the UE can use it when using APN.

7) [P-GW → PCRF] Notifying of EPS Session Setup

The P-GW and the PCRF communicate over Gx interface using Diameter protocol. When creating an EPS session for a user, resources allocation and QoS control for the user must be determined based on the services that the user is subscribing to. It is PCRF that is in charge of controlling policies concerning all the users who accessed to the network. So, the P-GW provides the PCRF with subscription information about the user, and obtains the PCRF's authorization for resources allocation in accordance with the network operator's policies. From the UE's subscription information received from the MME, the P-GW gathers information required for the PCRF's decision-making on the operator's policies, and sends it to the PCRF through a CCR (CC-Request) message. An example of the message is as follows:

CCR (IMSI, UE IP, PDN ID (APN), Subscribed QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), ECGI, TAI)

- **IMSI:** a fixed subscriber ID
- **UE IP:** an IP address to be used by a user when using services in PDN
- **PDN ID:** APN to be used by a user
- **Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL)):** QoS information to be applied when establishing an EPS default bearer
- **ECGI:** a cell in which UE is located
- **TAI:** a TA in which UE is located

8) [PCRF → SPR] Requesting Access Profiles

The PCRF requests the SPR for the user's access profile to determine PCC policies for the user.

9) [PCRF ← SPR] Returning Access Profiles

The SPR returns an access profile for the user. The profile may include information such as SDF Filter, QCI, ARP, APN-AMBR (UL/DL), Charging Method (e.g. Offline), Changing Reporting Action (e.g. Start Reporting ECGI, TAI), etc.

10) [PCRF] Determining Policies

The PCRF determines PCC policies for the EPS session to be established based on the user access profile.

11) [P-GW ← PCRF] Acknowledging EPS Session Establishment

The PCRF delivers the PCC policies determined in Step 10) to the P-GW, as included in a CCA (CC-Answer) message. An example of the message is as follows:

> **CCA (IMSI, PCC Rule (SDF Filter, QCI, ARP, APN-AMBR (UL/DL), Charging=Offline, Change Reporting Action (Start Reporting ECGI, TAI))**

12) [P-GW] Policy Enforcement

The P-GW applies the PCC policies received from the PCRF. As the PCC policies are applied to each SDF, the P-GW sets up mapping between SDFs and the EPS bearer, and prepares a QoS profile to be applied to the default EPS bearer (see our technical document, "LTE QoS: SDF and EPS Bearer QoS"[5] for more information).

◇ 13) ~ 15) EPS Session Creation Response

The P-GW informs the MME of the QoS information applied to the established EPS sessions and default EPS bearer, by sending it in a Create Session Response message. The PCRF may decide to keep the value the MME received from the HSS, or select a new value.

13) [S-GW ← P-GW] EPS Session Creation Response

The P-GW allocates an uplink S5 TEID (S5 P-GW TEID) for establishing S5 GTP to the S-GW. It then includes the S5 P-GW TEID and the QoS profile to be applied to the default EPS bearer (S5 bearer) in the Create Session Response message, and sends it to the S-GW as a response to the Create Session Request message received in Step 4).

> **Create Session Response (UE IP, EPS Bearer ID, S5 P-GW TEID, Authorized QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), TFT (UL), Change Reporting Action (Start Reporting ECGI, TAI))**

14) [S5 Bearer: Uplink] S5 Bearer Established

Completing Step 13) establishes the uplink S5 GTP-U tunnel, allowing the S-GW to exchange uplink/downlink traffic with the P-GW.

15) [MME ← S-GW] EPS Session Creation Response

When receiving the Create Session Response message from the P-GW, the S-GW keeps the uplink S5 TEID (S5 P-GW TEID) to be used for uplink traffic, and allocates an uplink S1 TEID (S1 S-GW TEID) of S1 GTP tunnel to be used for S1 bearer. After processing the message, the S-GW adds the newly allocated S1 S-GW TEID to the processed message, and sends it to the MME as a response to the Create Session Request message it received in Step 3).

16) [MME] Why MME Keeps S5 P-GW TEID?

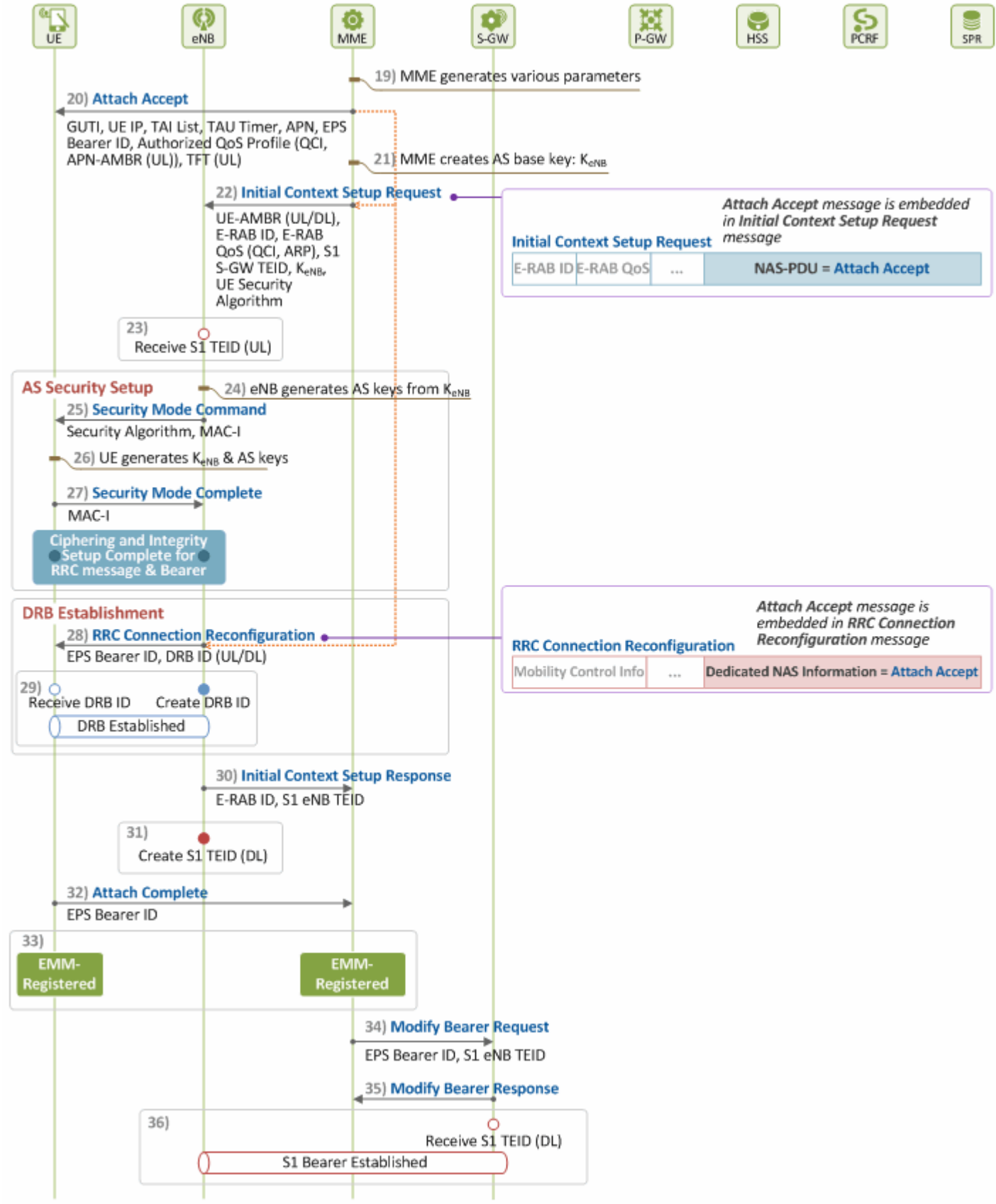
Once attached to a network, if a UE performs a TAU or handover, its S-GW may be changed. For this reason, the MME informs the UE's new S-GW of the uplink S5 TEID so that the new S-GW can deliver uplink traffic to the P-GW.

17) [S1 Bearer: Uplink]

Completing Step 15) establishes the uplink S1 GTP-U tunnel. However, since the eNB does not have this value (S1 S-GW TEID) yet, it cannot deliver uplink traffic to the S-GW at this time.

18) [MME] Calculating UE-AMBR

Now, the MME returns an Attach Accept message to the UE as a response to the Attach Request message, and prepares for E-RAB setup (i.e. for allocating resources to radio link and S1 bearer) by controlling the eNB. For this, the MME calculates the UE-AMBR value to send to the eNB. The MME has already received the UE-AMBR value, as included in subscription information, from the HSS in Section 2.4 above. However, it can adjust the value to the extent not exceeding the total APN-AMBR of each APN, and allocates it instead


UE
eNB
MME
S-GW
P-GW
HSS
PCRF
SPR
19) MME generates various parameters
20) Attach Accept
GUTI, UE IP, TAI List, TAU Timer, APN, EPS Bearer ID, Authorized QoS Profile (QCI, APN-AMBR (UL)), TFT (UL)
21) MME creates AS base key: K_eNB
22) Initial Context Setup Request
UE-AMBR (UL/DL), E-RAB ID, E-RAB QoS (QCI, ARP), S1 S-GW TEID, K_eNB, UE Security Algorithm
Attach Accept message is embedded in Initial Context Setup Request message
Initial Context Setup Request
E-RAB ID
E-RAB QoS
...
NAS-PDU = Attach Accept
23)
Receive S1 TEID (UL)
AS Security Setup
24) eNB generates AS keys from K_eNB
25) Security Mode Command
Security Algorithm, MAC-I
26) UE generates K_eNB & AS keys
27) Security Mode Complete
MAC-I
Ciphering and Integrity Setup Complete for RRC message & Bearer
DRB Establishment
28) RRC Connection Reconfiguration
EPS Bearer ID, DRB ID (UL/DL)
Attach Accept message is embedded in RRC Connection Reconfiguration message
RRC Connection Reconfiguration
Mobility Control Info
...
Dedicated NAS Information = Attach Accept
29)
Receive DRB ID
Create DRB ID
DRB Established
30) Initial Context Setup Response
E-RAB ID, S1 eNB TEID
31)
Create S1 TEID (DL)
32) Attach Complete
EPS Bearer ID
33)
EMM-Registered
EMM-Registered
34) Modify Bearer Request
EPS Bearer ID, S1 eNB TEID
35) Modify Bearer Response
36)
Receive S1 TEID (DL)
S1 Bearer Established

19) Determining Information needed for E-RAB and NAS Signaling

By receiving the Create Session Response message from the P-GW, the MME learns resources have been approved and allocated to the user. Then, it becomes in charge of E-RAB (DRB+S1 bearer) setup, and controls the eNB and the S-GW. To this end, it determines the resources required for E-RAB setup and the information needed for NAS signaling (Attach Accept) as follows:

- Allocating a GUTI that the UE can use instead of the IMSI
- Determining parameters related to controlling TAU (TAI list allocation, TAU Timer value)
- Determining UE-AMBR for the eNB's use
- Allocating an E-RAB ID

20) [UE ← MME] Attach Accept

The MME includes information, such as the UE IP address allocated by the P-GW, the GUTI, TAI list, EPS Bearer ID, UE-AMBR values allocated by itself, and QoS parameters received from the S-GW, in the Attach Accept message[8], and sends it to the UE as a response to the Attach Request message received in Section 2.1.

This message is delivered as included in the Initial Context Setup Request message through the S1 signaling connection, and then in the RRC Connection Reconfiguration message through the RRC connection.

21) [MME] Creating K_{eNB}

The MME creates K_{eNB}, the AS security base key, from K_{ASME}. This is to ensure the eNB can generate AS security keys to be used for secured communication between the eNB and the UE over radio link (i.e. for AS security setup).

22) [eNB ← MME] Requesting E-RAB Setup

The MME sends an Initial Context Setup Request message so that the eNB can establish S1 bearer with the S-GW, and DRB with the UE. The Initial Context Setup Request message consists of the following information elements:

Initial Context Setup Request (UE-AMBR (UL/DL), E-RAB ID, E-RAB QoS (QCI, ARP), S1 S-GW TEID, K_{eNB}, , UE Security Algorithm, NAS-PDU)

- **UE-AMBR(UL/DL):** QoS parameter that can only be controlled by eNB (because a user uses the same eNB no matter what APN the user is using)
- **E-RAB ID:** allocated by MME, and used by eNB as an EPS bearer ID
- **E-RAB QoS:** determined by MME based on the EPS bearer QoS received from P-GW
- **S1 S-GW TEID:** uplink S1 TEID value received from S-GW
- **K_{eNB}:** generated by MME from K_{ASME}, and used by eNB for derivation of AS security keys
- **UE Security Algorithm:** included in the **Attach Request** message received from UE, and used by eNB along with K_{eNB} for AS security setup.
- **NAS-PDU:** NAS message (**Attach Accept**)

23) [S1 Bearer: Uplink]

Once Step 22) is completed, and the S1 S-GW TEID is obtained, the eNB can deliver uplink traffic to the S-GW.

When the eNB receives the MME's Initial Context Setup Request message that requests E-RAB setup, it sets up DRB by sending an Attach Accept message to the UE. Then, it completes S1 bearer setup by including a downlink S1 TEID in the Initial Context Setup Response message, and sending the message as a response to the Initial Context Setup Request message to the MME, so that the MME can forward it to the S-GW.

◇ 24) ~ 27) AS Security Setup

Upon receiving the MME's Initial Context Setup Request message, the eNB attempts to communicate with the UE to set up DRB. To ensure secured communication over the radio link, the eNB performs the procedure for AS security setup before sending messages to the UE (see our technical document, "LTE Security II: NAS and AS Security" [3] for more information).

24) [eNB] Generating AS Security Keys

The eNB generates AS security keys from K_{eNB} received from the MME for safe delivery of RRC messages and user traffic to/from the UE. The eNB selects ciphering and integrity algorithms for RRC messages from the security algorithms that the MME forwarded for the UE, and ciphering algorithms for user traffic. Next, from K_{eNB}, it derives K_{RRCint}/K_{RRCenc}, RRC integrity/ciphering keys, and K_{UPenc}, a key for ciphering user traffic.

25) [UE ← eNB] Helping UE to Generate AS Security Keys

The eNB helps the UE to generate AS security keys (K_{RRCint}, K_{RRCenc} and K_{UPenc}) by informing the UE of the AS security algorithms it selected (i.e. control plane RRC integrity/ciphering algorithm and user plane ciphering algorithm) through a Security Mode Command (AS Security Algorithm, MAC-I) message. The eNB sends this RRC message with its integrity-protected (by including MAC-I).

26) [UE] Generating AS Security Keys

Upon receiving the Security Mode Command message from the eNB, the UE generates AS security keys using the AS security algorithm that the eNB selected, and performs integrity check on the Security Mode Command message.

27) [UE → eNB] AS Keys Generation Complete

Once the integrity check on the Security Mode Command message is completed, AS security keys are successfully set up and ready to work between the UE and the eNB. The UE then indicates to the eNB that AS security keys are generated by sending a Security Mode Complete (MAC-I) message. The UE sends the message with its integrity-protected by using the RRC integrity key.

As the AS security setup over the radio link is ended, RRC messages exchanged over the radio link thereafter are sent as encrypted and integrity-protected, and user traffic is delivered as encrypted. Now, the eNB begins DRB establishment.

◇ 28) ~ 29) DRB Establishment

28) [UE ← eNB] Reconfiguring RRC Connection

The eNB allocates uplink/downlink DRB IDs, and configures DRB QoS parameters from E-RAB QoS in order to establish DRB, an EPS bearer over the radio link. Thereafter, it sends a RRC Connection Reconfiguration message to the UE through the secured RRC connection. The RRC connection was already established when the UE sent the Attach Request message. However, it must be reconfigured now that the UE needs to configure parameters according to the resources allocated by the network as a result of permission to access the network. The RRC layer of the UE allocates radio resources based on the configuration parameters gathered from the RRC Connection Reconfiguration message. Next, it extracts an Attach Accept message from the RRC Connection Reconfiguration message, and sends it to the NAS layer.

When the NAS layer of the UE receives the message, it obtains the UE IP address and GUTI from the message, and uses them for future communication.

29) [DRB Establishment: Uplink and Downlink] DRB Establishment Complete

Once Step 28) is completed, and the UE can deliver uplink/downlink traffic from/to the eNB.

30) [eNB → S-GW] E-RAB Setup Response

The eNB allocates a downlink S1 TEID (S1 eNB TEID) for S1 bearer. Then it includes the allocated ID in an Initial Context Setup Response message, and sends it to the MME as a response to the Initial Context Setup Request message received in Step 22), so that the MME can forwards it to the S-GW.

31) [eNB] Allocating a Downlink TEID for S1 Bearer

Once Step 29) is completed, a downlink TEID is allocated by the eNB to S1 bearer, establishing the downlink S1 GTP-U tunnel. However, since the S-GW does not know about the establishment yet, it cannot delivery downlink traffic to the eNB at this time.

32) [UE → MME] Sending Attach Complete Message

The UE sends an Attach Complete message[9] to the MME, as a response to the message in Step 20). The Attach Complete message is delivered through an UL Information Transfer message over the RRC connection, and then through an Uplink NAS Transport message over the S1 signaling connection.

33) [UE][MME] EMM State

Now the UE and the MME stay in EMM-Registered state. If an Attach Reject message is sent from the MME to the UE in Step 20), the UE must release the ECM/RRC connection and transit to EMM-Deregistered state.

34) [MME → S-GW] Requesting S1 Bearer Modification

The MME forwards the downlink S1 TEID (S1 eNB TEID) received from the eNB to the S-GW through a Modify Bearer Request message.

35) [MME ← S-GW] Responding to S1 Bearer Modification Request

The S-GW sends the MME a Modify Bearer Response as a response to the Modify Bearer Request message. Now, the S-GW is ready to deliver downlink S1 traffic.

36) [S1 Bearer: Downlink] S1 Bearer Setup Complete

Step 35) completes the setup procedure for S1 bearer. With the establishment of S1 bearer, the eNB and the S-GW can exchange traffic with each other. Now, the default EPS bearer from the UE all the way to the P-GW is finally established, allowing uplink/downlink EPS bearer communication between the UE and the P-GW.

2. Cases of Detach

A user uses LTE services after generating an EPS session and default EPS bearer through the initial attach procedures. In some cases, he may detach from the network once done using the services. In other cases, he may be detached by the network while still using services through the network, and becomes unable to stay connected to the network any more.

Once a user is detached from the network, all the network/radio resources allocated to the EPS session and bearer established for the user are released. This release will delete the user's MM context and EPS bearer that have been set to the EPS entities (UE and network nodes). At this time, the EMM state transits from Registered to De-Registered. If the user is properly detached, GUTI, a NAS-level user ID, and the security context that he used to access the network are kept valid in the UE and the MME, so that he can use the same in his next access to the network. Detach can be triggered by UE or a network. Network-triggered detach is caused by either MME or HSS. Detach can be categorized as one of the following cases depending on where detach triggering is detected:

1) Detach Case 1: UE-initiated Detach
UE can initiate detach:

- if UE is turned off
- if a USIM card is removed from UE
- if UE is attempting to use a non-EPS service (e.g. CS fallback, SMS, etc.)

2) Detach Case 2: MME-initiated Detach
MME-initiated detach can be further divided into explicit detach and implicit detach. In case of explicit detach, MME notifies UE of its intent to detach in advance by sending a Detach Request message, and informs the UE whether it has to attach the network again or not after detach. In case of implicit detach, however, the MME initiates detach procedures without notification (i.e. without sending a Detach Request message) because the UE is not capable of communicating with the MME. MME can initiate:

i) Explicit Detach

- for an operator's O&M (Operation & Maintenance) purposes
- if re-authentication fails
- if it cannot provide the resources allocated to a user

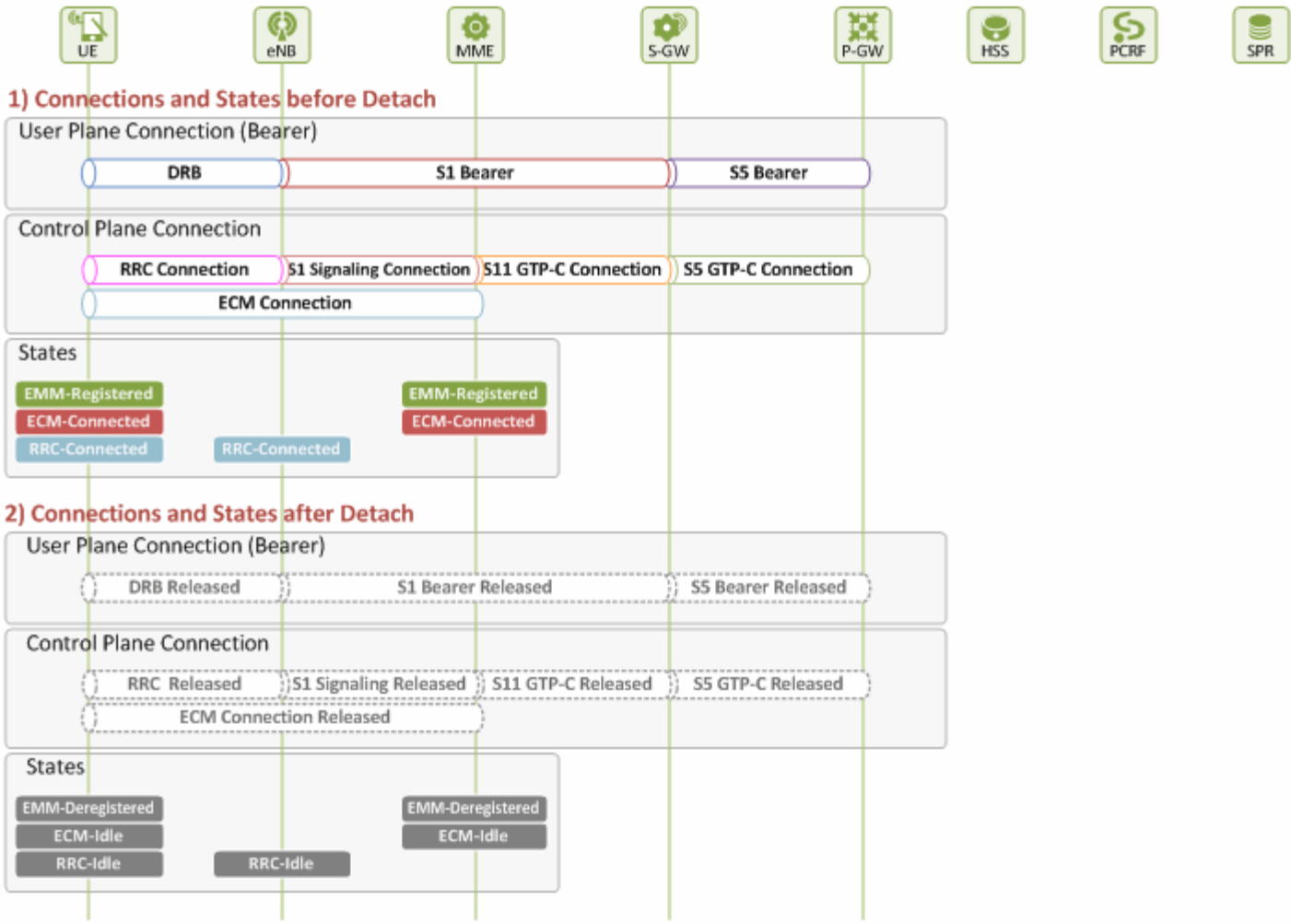
ii) Implicit Detach

- if it is not able to communicate with a user because of poor radio link quality (e.g. radio link failure)

3) Detach Case 3: HSS-initiated Detach
HSS can initiate detach:

- if the user profile provisioned in HSS is changed, and thus the one saved in MME also has to be changed
- if an operator is trying to restrict access by an illegal UE (e.g. a stolen device) to its network

The next three chapters (III, IV and V) describe different detach procedures required in the three detach cases mentioned above. In all three cases, it is assumed a user is in EMM-Registered, ECM-Connected and RRC-Connected state before detach, and services are provided through the default EPS bearer only. Figure 1 illustrates what connections are established, and in what state UE and MME are in user/control planes before and after detach. Before detach, a default EPS bearer and its related control connections are established, and the user is in EMM-Registered, ECM-Connected and RRC-Connected. Then, after detach, the default EPS bearer and all the signaling connections are released, and the user enters EMM-Deregistered, ECM-Idle and RRC-Idle state.



UE-initiated Detach

Figure 2 shows how user-initiated detach is performed. The detach procedure for this type of detach begins when detach triggering is detected at UE (see Chapter II), and thus the UE sends a Detach Request message. The procedure ends when the UE receives a Detach Accept message from MME, unless the UE is turned off by the user.

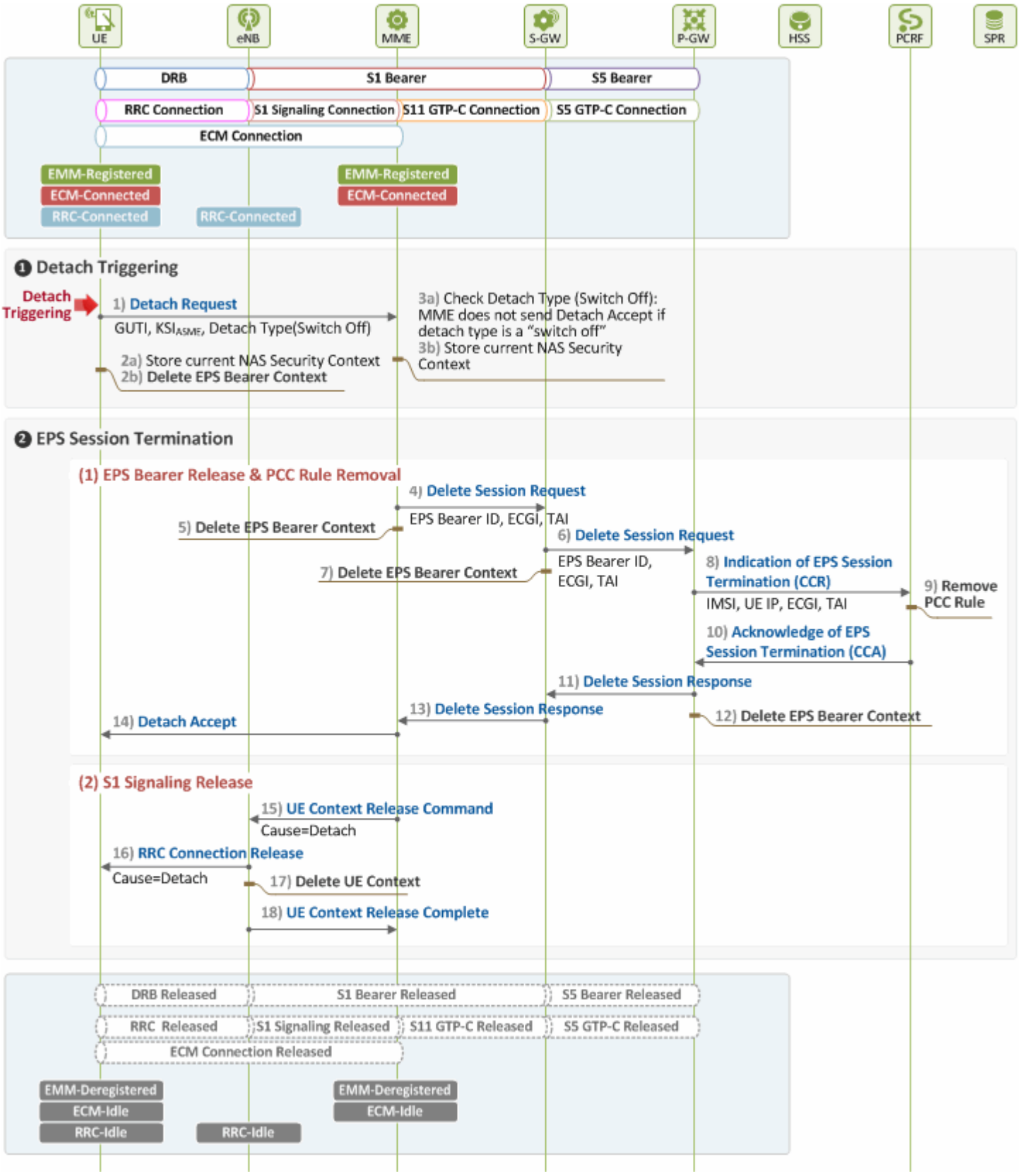


Figure 2. Procedure for UE-initiated Detach

❶ Detach Triggering by UE

When detach triggering is detected at UE, and thus the UE and MME become aware of it, the two entities will begin the following procedures:

1) [UE → MME] Detach Request

The UE requests the MME for detach by sending a Detach Request message to the MME. Interpretation of the Detach Request message parameters varies depending on which direction the message is delivered. If it is from UE to MME, the message parameters will be as follows:

Detach Request (GUTI, KSI_{ASME}, Detach Type(Switch Off))

- **GUTI**: User ID assigned by MME at the time of network attach
- **KSI_{ASME}**: KSI value that is being used by UE
- **Detach Type**: Indicates a detach type
  - **Switch Off**: Indicates whether the case is normal detach (0) or switch off (1)
  - **Type of Detach**: EPS detach

2) [UE] Handling Security and Bearer Contexts

After sending the Detach Request message, the UE stores its current NAS security context, GUTI and TA information, and then deletes its EPS bearer context.

3) [MME] Noticing Detach Intent and Handling Security Context

After receiving the Detach Request message from the UE, the MME becomes aware of the UE's intent to detach. It then stores the user's current NAS security context, and checks the type of the intended detach, i.e. whether it is a case of normal detach, or a turned off device. By doing this, the MME finds out whether it has to send a Detach Accept message or not.

❷ EPS Session Termination

Once the MME perceived UE-initiated detach and stored the user's current NAS security context, it requests for termination of the activated EPS session. This request triggers PCEF (P-GW)-initiated EPS termination, releasing all the network/radio resources allocated to the user, as to be described below.

(1) EPS Bearer Release and PCC Rule Removal

4) [MME → S-GW] Requesting EPS Session Release

The MME and the S-GW communicate with each other over S11 interface using GTP protocol (GTP-C). The MME begins procedures for deleting the user's EPS session and default EPS bearer by sending the S-GW a Delete Session Request message. At this time, the default EPS bearer ID and UE location information (ECGI, TAI) are delivered.

5) [MME] Deleting EPS Bearer Context

The MME deletes the user's EPS bearer context after sending the Delete Session Request message.

6) [S-GW → P-GW] Requesting EPS Session Release

The S-GW and the P-GW communicate with each other over S5 interface using GTP protocol (UP: GTP-U, CP: GTP-C). The S-GW forwards the Delete Session Request message received from the MME to the P-GW.

7) [S-GW] Deleting EPS Bearer Context

The S-GW deletes the user's EPS bearer context after sending the Delete Session Request message.

8) [P-GW → PCRF] Notifying of EPS Session Termination

The P-GW and the PCRF communicate with each other over Gx interface using Diameter protocol. The P-GW sends PCRF a CCR (CC-Request) message to notify the user has finished using services through the network. This way it has the EPS session termination procedures (PCEF-initiated EPS Session Termination) initiated.

9) [PCRF] Deleting RCC Rule

The PCRF deletes the user's PCC rule once it receives the CCR message from the P-GW.

10) [P-GW ← PCRF] Acknowledging EPS Session Termination

The PCRF acknowledges the user's PCC rule has been deleted by sending a CCA (CC-Answer) message to the P-GW.

11) [S-GW ← P-GW] Responding to EPS Session Release Request

When the P-GW receives the CCA message from the PCRF, it sends the S-GW a Delete Session Response message as a response to the message sent in Step 6) above.

12) [P-GW] Deleting EPS Bearer Context

The P-GW deletes the user's EPS bearer context after sending the Delete Session Response message.

13) [MME ← S-GW] Responding to EPS Session Release Request

When the S-GW receives the Delete Session Response message from the P-GW, it sends the MME a Delete Session Response message as a response to the message sent in Step 4) above.

14) [UE ← MME] Acknowledging Detach

Upon receipt of the Delete Session Response message, the MME recognizes the user's resource release has been approved by the PCRF. So, it sends the UE a Detach Accept message as a response to the request sent in Step 1). A Detach Accept message is sent only when the UE's detach request was made due to a cause other than a switched off device (i.e. when Switch Off=0 in the Detach Request). If

detach was requested because of a device's switch off, no Detach Accept message is sent by MME.

(2) S1 Signaling Connection Release

After sending the Detach Accept message to the UE, the MME and the eNB release any resources left for the user (S1 signaling connection, RRC connection and UE Context left in the eNB) as they do not serve the UE any more.

15) [eNB ← MME] Acknowledging S1 Signaling Connection Release

The MME sends a UE Context Release Command message to the eNB to release the S1 signaling connection.

16) [UE ← eNB] RRC Connection Release

The eNB sends an RRC Connection Release message to the UE to release any RRC connection left unleased.

17) [eNB] Deleting UE Context

The eNB deletes all the information related to the UE.

18) [eNB → MME] RRC Connection Release Complete

Finally, the eNB sends the MME a UE Context Release Complete message as a response to the request sent in Step 15).

MME-initiated Detach

Figure 3 displays how MME-initiated explicit detach is performed. The detach procedure for this type of detach begins when detach triggering is detected at MME, and thus the MME sends a Detach Request message to the UE. The procedure ends when the resources previously allocated to the UE's EPS session are released.

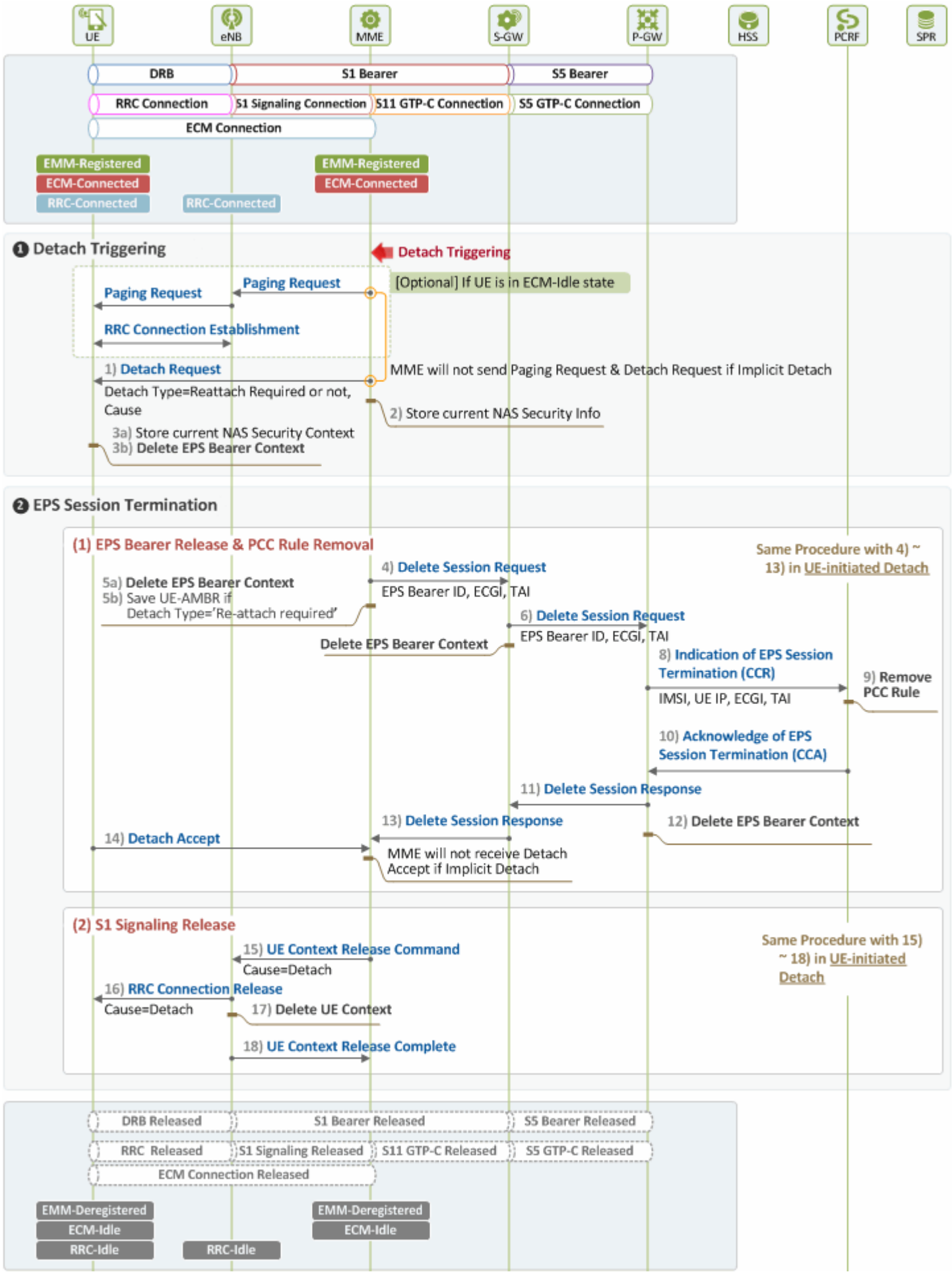

UE
eNB
MME
S-GW
P-GW
HSS
PCRF
SPR
DRB
S1 Bearer
S5 Bearer
RRC Connection
S1 Signaling Connection
S11 GTP-C Connection
S5 GTP-C Connection
ECM Connection
EMM-Registered
ECM-Connected
RRC-Connected
EMM-Registered
ECM-Connected
RRC-Connected
❶ Detach Triggering
Detach Triggering
[Optional] If UE is in ECM-Idle state
Paging Request
Paging Request
Paging Request
RRC Connection Establishment
1) Detach Request
Detach Type=Reattach Required or not,
Cause
MME will not send Paging Request & Detach Request if Implicit Detach
2) Store current NAS Security Info
3a) Store current NAS Security Context
3b) Delete EPS Bearer Context
❷ EPS Session Termination
(1) EPS Bearer Release & PCC Rule Removal
Same Procedure with 4) ~ 13) in UE-initiated Detach
4) Delete Session Request
EPS Bearer ID, ECGI, TAI
5a) Delete EPS Bearer Context
5b) Save UE-AMBR if
Detach Type='Re-attach required'
6) Delete Session Request
EPS Bearer ID, ECGI, TAI
Delete EPS Bearer Context
8) Indication of EPS Session Termination (CCR)
IMSI, UE IP, ECGI, TAI
9) Remove PCC Rule
10) Acknowledge of EPS Session Termination (CCA)
11) Delete Session Response
13) Delete Session Response
12) Delete EPS Bearer Context
14) Detach Accept
MME will not receive Detach Accept if Implicit Detach
(2) S1 Signaling Release
Same Procedure with 15) ~ 18) in UE-initiated Detach
15) UE Context Release Command
Cause=Detach
16) RRC Connection Release
Cause=Detach
17) Delete UE Context
18) UE Context Release Complete
DRB Released
S1 Bearer Released
S5 Bearer Released
RRC Released
S1 Signaling Released
S11 GTP-C Released
S5 GTP-C Released
ECM Connection Released
EMM-Deregistered
ECM-Idle
RRC-Idle
EMM-Deregistered
ECM-Idle
RRC-Idle

Figure 3. Procedure for MME-initiated Detach

❶ Detach Triggering by MME

Below is a description of the procedures to be performed after MME detects detach triggering, and before the EPS session termination procedure is carried out. If the user is in Idle state at this time, the MME performs paging to establish S1 signaling connection (Detailed paging procedures will be explored in our technical document "EMM Procedure 4. Service Request due to New Traffic", and hence will not be discussed here).

1) [UE ← MME] Detach Request

As it is explicit detach, the MME sends a Detach Request message to request the UE for detach. Message parameters are as follows in case a detach request is sent by MME to UE:

Detach Request (Detach Type(Re-attach required or not), Cause)

- **Detach Type:** indicates whether UE is required to be re-attached or not after detach
  - 001: Re-attach required
  - 010: Re-attach not required
- **Cause:** indicates why detach is caused

In case of implicit detach, however, MME does not send a Detach Request message to UE.

2) [MME] Handling Security Context

After sending the Detach Request message to the UE, the MME stores the current NAS security context in use before deleting the EPS session. Next time the UE re-attaches, the MME can use the stored context again and skip the authentication and NAS security setup procedures for the user.

3) [UE] Noticing Detach Intent and Handling Security and Bearer Contexts

After receiving the Detach Request message from the MME, the UE becomes aware of the MME's intent to detach. It checks the type of the intended detach to see whether or not re-attach is required after detach. Then it stores the current NAS security context and deletes the EPS bearer context.

❷ EPS Session Termination

Once the MME stored the NAS security context upon perceiving detach triggering, it requests the P-GW for termination of the user's EPS session. This request triggers PCEF (P-GW)-initiated EPS termination, releasing all the network/radio resources allocated to the user, as to be described below.

(1) EPS Bearer Release and PCC Rule Removal

Through Steps 4) ~ 13), the MME requests for termination of the user's EPS session, the PCRF deletes PCC rule upon the request, and S5 bearer resources are released, as in Steps

4) ~ 13) in Chapter III. In case of a detach type that requires re-attach, the MME can save the current UE-AMBR value in Step 5) so that the UE can establish an EPS bearer faster next time it re-attaches.

4) [UE → MME] Acknowledging Detach

After storing the NAS security context and deleting the EPS bearer context upon receipt of the Detach Request message from the MME in Step 1), the UE sends the a Detach Accept message as a response to the request in Step 1). In case of implicit detach, Steps 1), 14) and 16) are skipped.

(2) S1 Signaling Connection Release

In this phase, the MME releases any unreleased resources (S1 signaling connection, RRC connection and UE context left in the eNB) after receiving the Detach Accept message from the UE and the Delete Session Response message from the S-GW. Steps in this phase are the same as Steps 15) ~ 18) in Chapter III, except that in case the detach type is set as "re-attach required", UE re-attaches the network after RRC connection is released.

HSS-initiated Detach

Figure 4 provides an illustration of how HSS initiates detach after detecting detach triggering.

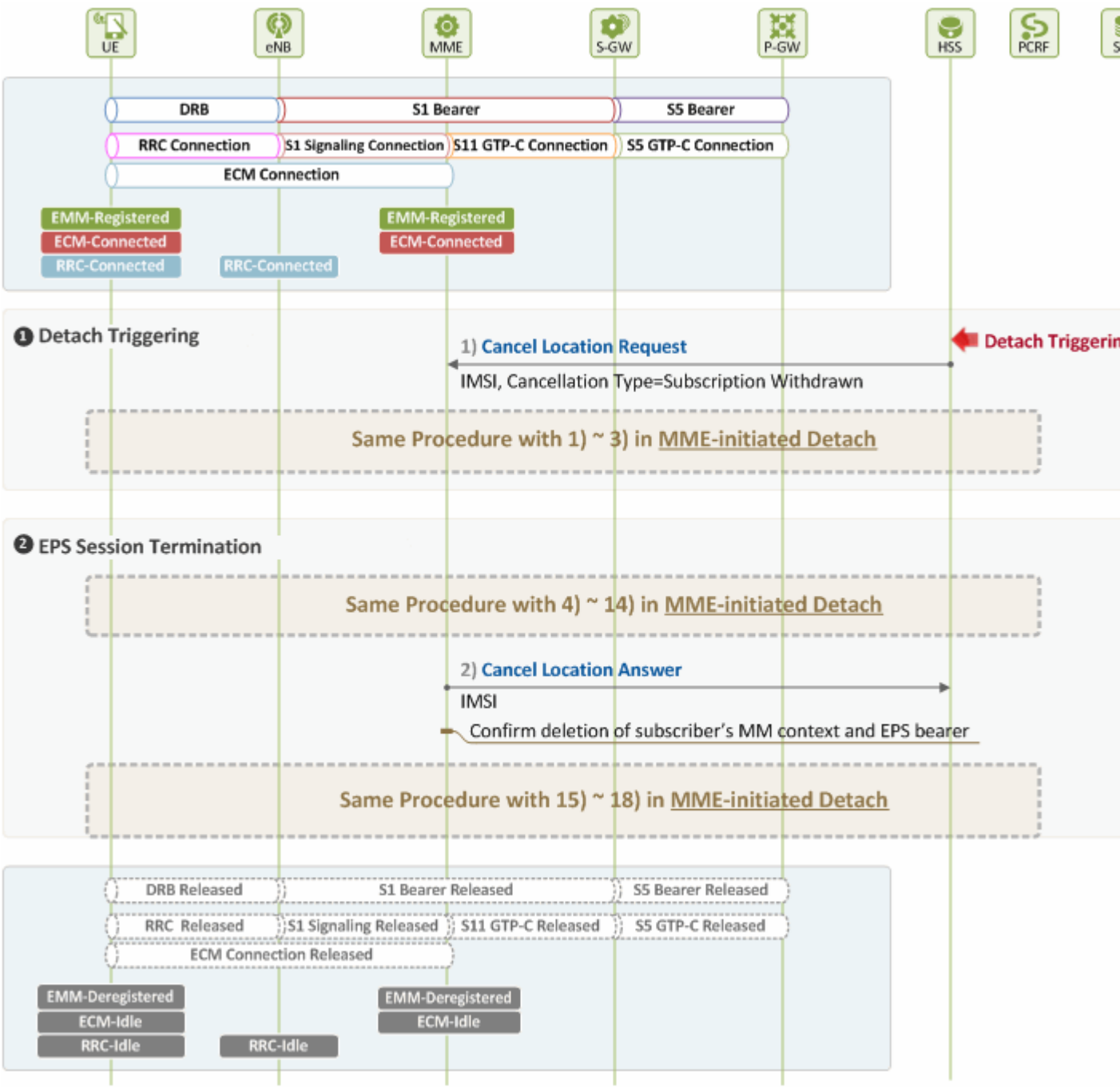


Figure 4. Procedure for HSS-initiated Detach

❶ Detach Triggering by HSS

When detach is triggered at HSS due to subscriber withdrawal, the HSS attempts to delete the user's MM context and EPS bearer immediately.

1) [MME ← HSS] Detach Request

The HSS and the MME communicate with each other over S6a interface using Diameter protocol. The HSS requests the MME for detach of the user by sending a Cancel Location Request (CLR) message with the following parameters:

Cancel Location Request (IMSI, Cancellation Type)

- **IMSI:** ID of the user to be detached (i.e. the user whose MM Context and EPS bearer are to be deleted)
- **Cancellation Type**[1] = **Subscription Withdrawn:** indicates the reason for detach

❷ EPS Session Termination

Upon receipt of the Cancel Location Request (CLR) message from the HSS, the MME releases all the resources previously allocated to the user. Steps for such procedure are the same as in MME-initiated detach (Figure 3) described in Chapter III, except that an additional action is required by the MME in Step 2). The MME needs to send the HSS a Cancel Location Answer message as a response to the request made in Step 1).

2) [MME → HSS] Responding to Detach Request

After receiving the Detach Accept message from the UE, and the Delete Session Response message from the S-GW, the MME sends a Cancel Location Answer message to the HSS as a response to the Cancel Location Request message sent in Step 1).

S1 Release due to User Inactivity

S1 release may be triggered by either eNB or MME. eNB-triggered release can be caused by:

- user inactivity
- repeated RRC signaling integrity check failure
- release due to UE generated signaling connection release
- unspecified failure
- O&M intervention

MME-triggered release can be caused by:

- authentication failure
- detach
- disallowed CSG cell

In addition, S1 release can be triggered by the two for other reasons, such as control processing overload, not enough user plane processing resources available, etc.

Figure 1 shows the connections established in user and control planes, and the UE and MME states in the planes, before and after S1 release. Before the release, an EPS bearer and signaling connection are established to support traffic transmission between a user and the network (UE through P-GW). The EPS bearer consists of a DRB, S1 bearer and S5 bearer, while the signaling connection consists of an ECM (RRC + S1 signaling connections), S11 and S5 connections. The UE and MME are in EMM-Registered and ECM-Connected state, while the UE and eNB are in RRC-Connected state.

However, after S1 release, the DRB and downlink S1 bearer are released in the user plane, and the ECM connection (RRC + S1 signaling connections) is lost in the control plane, releasing E-UTRAN resources. It should be noted that at this time only the resources for the downlink S1 bearer are released, and those for the uplink are kept in the network.
The S1 release is different from the one in detach events described in our previous document. In the event of detach, all the resources allocated to a UE by the network are released, and thus the UE transits to EMM-Deregistered state. However, in the event of S1 release, only those allocated by the radio access network (E-UTRAN or eNB) are released, and ones allocated by EPC are kept unreleased. So, the UE remains in EMM-Registered state, transiting to ECM-Idle state. Then later when there is uplink/downlink user traffic, ECM connection and DRB/S1 bearer (downlink) setup is performed, switching the UE state into ECM-Connected, and delivers the traffic.

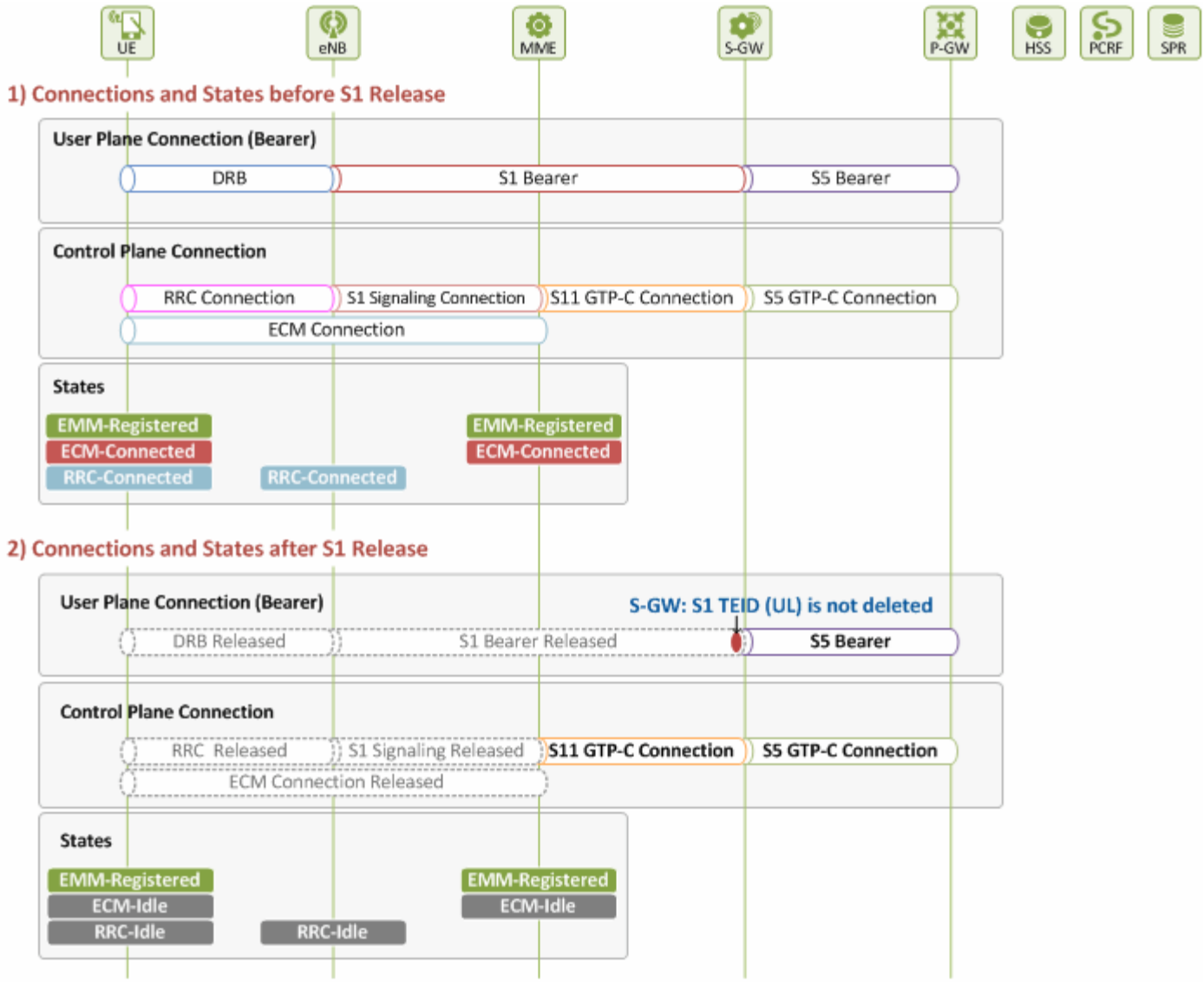


Figure 1. Connections and States before/after S1 Release

Figure 2 displays the procedures for S1 release triggered by eNB upon detection of user inactivity (Note: Procedures will still be the same even when S1 release is triggered by a cause other than user inactivity). In case S1 release is triggered by MME, Step 1) in Figure 2 will be skipped.

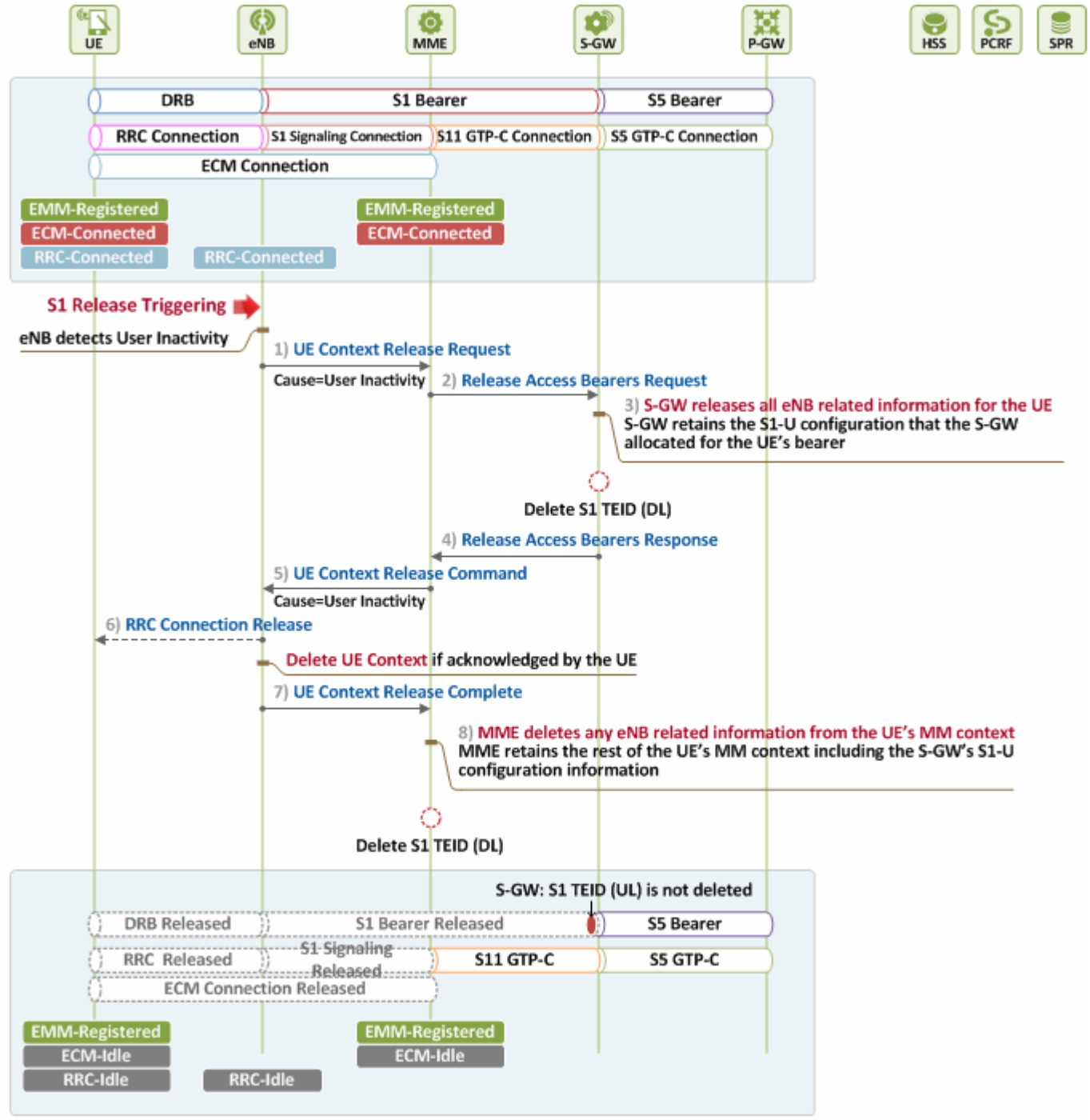


Figure 2. Procedures for S1 Release (eNB-initiated)

1) [eNB → MME] Requesting UE Context Release

The eNB, upon detecting user inactivity, sends the MME a UE Context Release Request message, along with the cause for release, to release the UE context.

2) [MME → S-GW] Requesting S1 Bearer Release

The MME requests the S-GW for release of resources associated with the eNB, a downlink endpoint of the S1 bearer, by sending the S-GW a Release Access Bearers Request message. This way, it informs the S-GW that no downlink traffic can be delivered to the UE.

3) [S-GW] Downlink S1 Bearer Release

The S-GW releases all the downlink S1 bearer resources associated with the UE (eNB related resources, including downlink S1 TEID allocated by eNB, etc.), but keeps the uplink S1 bearer resources (S-GW related resources, including uplink S1 TEID allocated by itself, etc.) unreleased. So, when uplink packets arrive, the eNB can obtain the uplink S1 TEID from the MME, and deliver the packets through the S1 bearer without delay.

4) [MME ← S-GW] Responding to S1 Bearer Release Request

The S-GW acknowledges that the downlink S1 bearer resources have been released by sending the MME a Release Access Bearers Response message. After that, if downlink packets destined to the UE arrive, the S-GW buffers them, and delivers them only after the downlink S1 bearer is re-established. The detailed procedures will be explored in the subsequent document, "EMM Procedure 4. Service Request".

5) [eNB ← MME] UE Context Release Command

The MME sends the eNB a UE Context Release Command message to release the UE context stored at the eNB.

6) [UE ← eNB] RRC Connection Release

The eNB, upon receiving the command from the MME, deletes all the UE contexts it had. If RRC connection has not been released yet, the eNB sends the UE a RRC Connection Release message to release it. By doing so, the eNB releases all the radio resources and bearers allocated to the UE, and deletes the UE contexts.

7) [eNB → MME] UE Context Release Complete

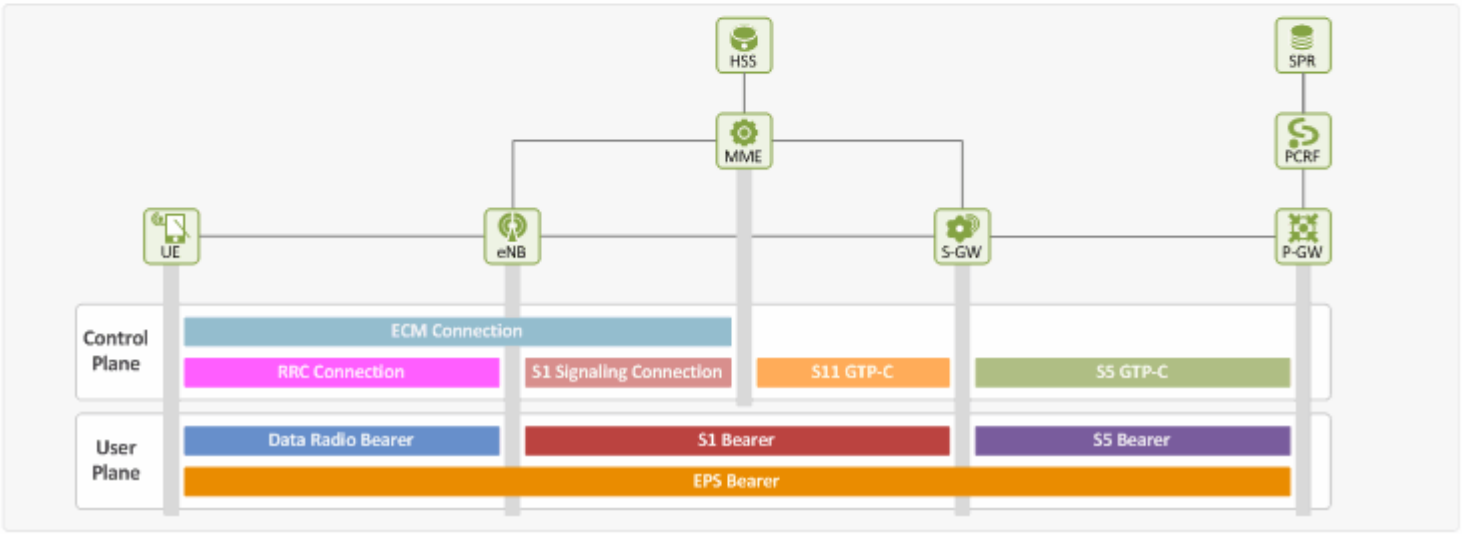
The eNB sends the MME a UE Context Release Complete message as a response to the request sent in Step 5). The MME then confirms all the UE contexts have been deleted.

8) [MME] S1 Release

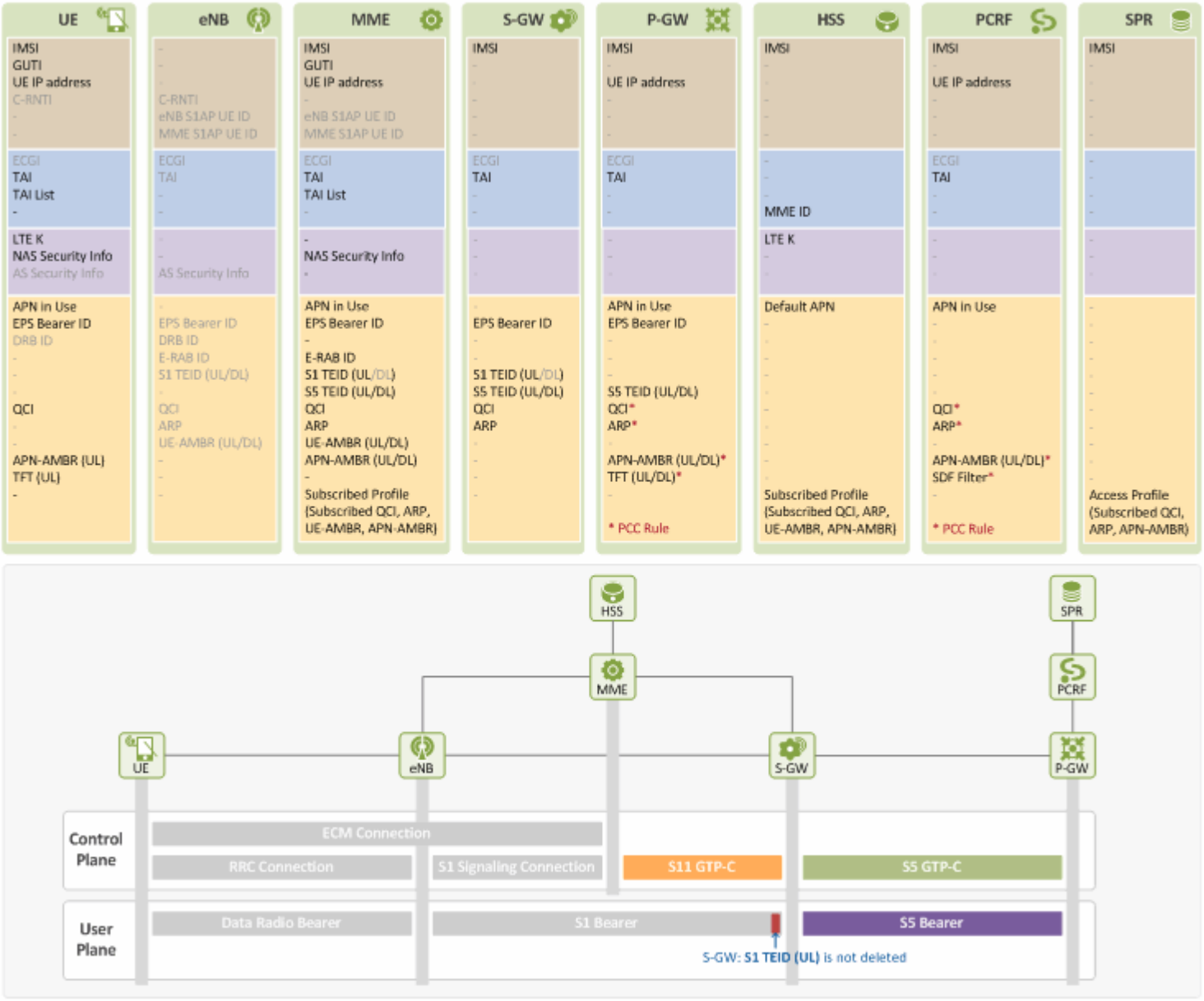
The MME deletes all the eNB related information, except for uplink S1 bearer information, in the UE contexts. But it keeps other information not related to the eNB.

Before S1 Release

UE	eNB	MME	S-GW	P-GW	HSS	PCRF	SPR
IMSI GUTI UE IP address C-RNTI - -	- - - C-RNTI eNB S1AP UE ID MME S1AP UE ID	IMSI GUTI UE IP address - eNB S1AP UE ID MME S1AP UE ID	IMSI - - - - -	IMSI - UE IP address - - -	IMSI - - - - -	IMSI - UE IP address - - -	IMSI - - - - -
ECGI TAI TAI List -	ECGI TAI - -	ECGI TAI TAI List -	ECGI TAI - -	ECGI TAI - -	- - - MME ID	ECGI TAI - -	- - - -
LTE K NAS Security Info AS Security Info	- - AS Security Info	- NAS Security Info -	- - -	- - -	LTE K - -	- - -	- - -
APN in Use EPS Bearer ID DRB ID - - - QCI - - APN-AMBR (UL) TFT (UL) -	- EPS Bearer ID DRB ID E-RAB ID S1 TEID (UL/DL) - QCI ARP UE-AMBR (UL/DL) - - -	APN in Use EPS Bearer ID - E-RAB ID S1 TEID (UL/DL) S5 TEID (UL/DL) QCI ARP UE-AMBR (UL/DL) APN-AMBR (UL/DL) - Subscribed Profile (Subscribed QCI, ARP, UE-AMBR, APN-AMBR)	- EPS Bearer ID - - S1 TEID (UL/DL) S5 TEID (UL/DL) QCI ARP - - - -	APN in Use EPS Bearer ID - - - S5 TEID (UL/DL) QCI* ARP* - APN-AMBR (UL/DL)* TFT (UL/DL)* - * PCC Rule	Default APN - - - - - - - - - - Subscribed Profile (Subscribed QCI, ARP, UE-AMBR, APN-AMBR)	APN in Use - - - - - QCI* ARP* - APN-AMBR (UL/DL)* SDF Filter* - * PCC Rule	- - - - - - - - - - - Access Profile (Subscribed QCI, ARP, APN-AMBR)



After S1 Release



Information deleted at UE:

- C-RNTI: identifies UEs in a cell that UE has connected to
- ECGI: information on the cell that UE is connected to
- DRB ID: ID for EPS bearer over radio link (DRB). Allocated to UE by eNB.
- AS Security Info: AS security context between UE and eNB (to be used for integrity protection/ciphering of RRC messages, and for ciphering of user packets)

Information deleted at eNB:

- All information

Information deleted at MME:

- S1AP UE ID: UE IDs information used in S1 signaling connection (eNB S1AP UE ID and MME S1AP UE ID)

- ECGI: information on the cell that UE is connected to
- S1 TEID (DL): TEID information to be used in downlink S1 bearer

Information deleted at S-GW:

- ECGI: information on the cell that UE is connected to
- S1 TEID (DL): TEID information to be used in downlink S1 bear

Important Terms to Know

There are two types of EPS bearers: default and dedicated. In the LTE network, the EPS bearer QoS is controlled using the following LTE QoS parameters:

- ▶ Resource Type: GBR or Non-GBR
- ▶ QoS Parameters
- QCI
- ARP
- GBR
- MBR
- APN-AMBR
- UE-AMBR

Every EPS bearer must have QI and ARP defined. The QCI is particularly important because it serves as reference in determining QoS level for each EPS bearer. In case of bandwidth (bit rate), GBR and MBR are defined only in GBR type EPS bearers, whereas AMBR (APN-AMBR and UE-AMBR) is defined only in Non-GBR type EPS bearers.

Below, we will explain the LTE QoS parameters one by one.

Resource Type = GBR (Guaranteed Bit Rate)

For an EPS bearer, having a GBR resource type means the bandwidth of the bearer is guaranteed. Obviously, a GBR type EPS bearer has a "guaranteed bit rate" associated (GBR will be further explained below) as one of its QoS parameters. Only a dedicated EPS bearer can be a GBR type bearer and no default EPS bearer can be GBR type. The QCI of a GBR type EPS bearer can range from 1 to 4.

Resource Type = Non-GBR

For an EPS bearer, having a non-GBR resource type means that the bearer is a best effort type bearer and its bandwidth is not guaranteed. A default EPS bearer is always a Non-GBR bearer, whereas a dedicated EPS bearer can be either GBR or non-GBR. The QCI of a non-GBR type EPS bearer can range from 5 to 9.

QCI (QoS Class Identifier)

QCI, in an integer from 1 to 9, indicates nine different QoS performance characteristics of each IP packet. QCI values are standardized to reference specific QoS characteristics, and each QCI

contains standardized performance characteristics (values), such as resource type (GBR or non-GBR), priority (1~9), Packet Delay Budget (allowed packet delay shown in values ranging from 50 ms to 300 ms), Packet Error Loss Rate (allowed packet loss shown in values from 10-2 to 10-6. For more specific values, search on Google for "3GPP TS 23.203" and see Table 6.1.7 in the document. For example, QCI 1 and 9 are defined as follows:

QCI = 1
: Resource Type = GBR, Priority = 2, Packet Delay Budget = 100ms, Packet Error Loss Rate = 10-2 , Example Service = Voice
QCI = 9
: Resource Type = Non-GBR, Priority = 9, Packet Delay Budget = 300ms, Packet Error Loss Rate = 10-6, Example Service = Internet

QoS to be guaranteed for an EPS bearer or SDF varies depending on the QCI values specified. QCI, though a single integer, represents node-specific parameters that give the details of how an LTE node handles packet forwarding (e.g. scheduling weights, admission thresholds, queue thresholds, link layer protocol configuration, etc). Network operators have their LTE nodes pre-configured to handle packet forwarding according to the QCI value.

By pre-defining the performance characteristics of each QCI value and having them standardized, the network operators can ensure the same minimum level QoS required by the LTE standards is provided to different services/applications used in an LTE network consisting of various nodes from multi-vendors.

QCI values seem to be mostly used by eNBs in controlling the priority of packets delivered over radio links. That's because practically it is not easy for S-GW or P-GW, in a wired link, to process packets and also forward them based on the QCI characteristics all at the same time (As you may know, a Cisco or Juniper router would not care about delay or error loss rate when it processes QoS of packets. It would merely decide which packet to send first through scheduling (WFQ, DWRR, SPQ, etc.) based on the priority of the packets (802.1p/DSCP/MPLS EXP)).

ARP (Allocation and Retention Priority)

When a new EPS bearer is needed in an LTE network with insufficient resources, an LTE entity (e.g. P-GW, S-GW or eNB) decides, based on ARP (an integer ranging from 1 to 15, with 1 being the highest level of priority), whether to:

- remove the existing EPS bearer and create a new one (e.g. removing an EPS bearer with low priority ARP to create one with high priority ARP); or
- refuse to create a new one.

So, the ARP is considered only when deciding whether to create a new EPS bearer or not. Once a new bearer is created and packets are delivered through it, the ARP does not affect the priority of the delivered packet, and thus the network node/entity forwards the packets regardless of their ARP values.
One of the most representative examples of using the ARP is an emergency VoIP call. So, an existing EPS bearer can be removed if a new one is required for a emergency 119 (911 in US, 112 in EC, etc) VoIP call.

GBR (UL/DL)

This parameter is used for a GBR type bearer, and indicates the bandwidth (bit rate) to be guaranteed by the LTE network. It is not applied to a non-GBR bearer with no guaranteed bandwidth (UL is for uplink traffic and DL is for downlink traffic).

MBR (UL/DL)

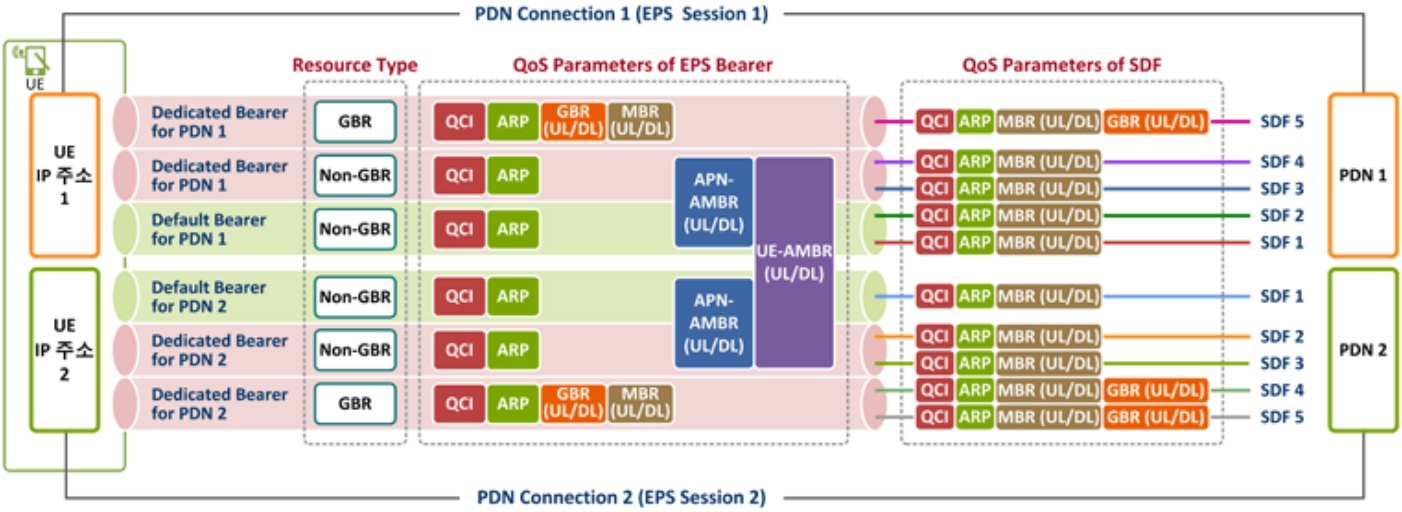
MBR is used for a GBR type bearer, and indicates the maximum bit rate allowed in the LTE network. Any packets arriving at the bearer after the specified MBR is exceeded will be discarded.

APN-AMBR (UL/DL)

As you read the foregoing paragraph, you may wonder why a non-GBR type bearer does not have a "bandwidth limit"? In case of non-GBR bearers, it is the total bandwidth of all the non-GBR EPS bearers in a PDN that is limited, not the individual bandwidth of each bearer. And this restriction is controlled by APN-AMBR (UL/DL). As seen in the figure above, there are two non-GBR EPS bearers, and their maximum bandwidths are specified by the APN-AMBR (UL/DL). This parameter is applied at UE (for UL traffic only) and P-GW (for both DL and UL traffic).

UE-AMBR (UL/DL)

In the figure above, APN-AMBR and UE-AMBR look the same. But, please take a look at the one below.
A UE can be connected to more than one PDN (e.g. PDN 1 for Internet, PDN 2 for VoIP using IMS, etc.) and it has one unique IP address for each of its all PDN connections. Here, UE-AMBR (UL/DL) indicates the maximum bandwidth allowed for all the non-GBR EPS bearers associated to the UE no matter how many PDN connections the UE has. Other PDNs are connected through other P-GWs, this parameter is applied by eNBs only.



2. EPS Session and EPS Bearer: Overview

Before we discuss IDs relating EPS sessions and EPS bearers, an overview of what the EPS sessions and EPS bearers are and what they are like and a description of the relationship among the IDs will be given.

Figure 1 shows the EPS sessions and EPS bearers of a user, with their IDs shown underneath.

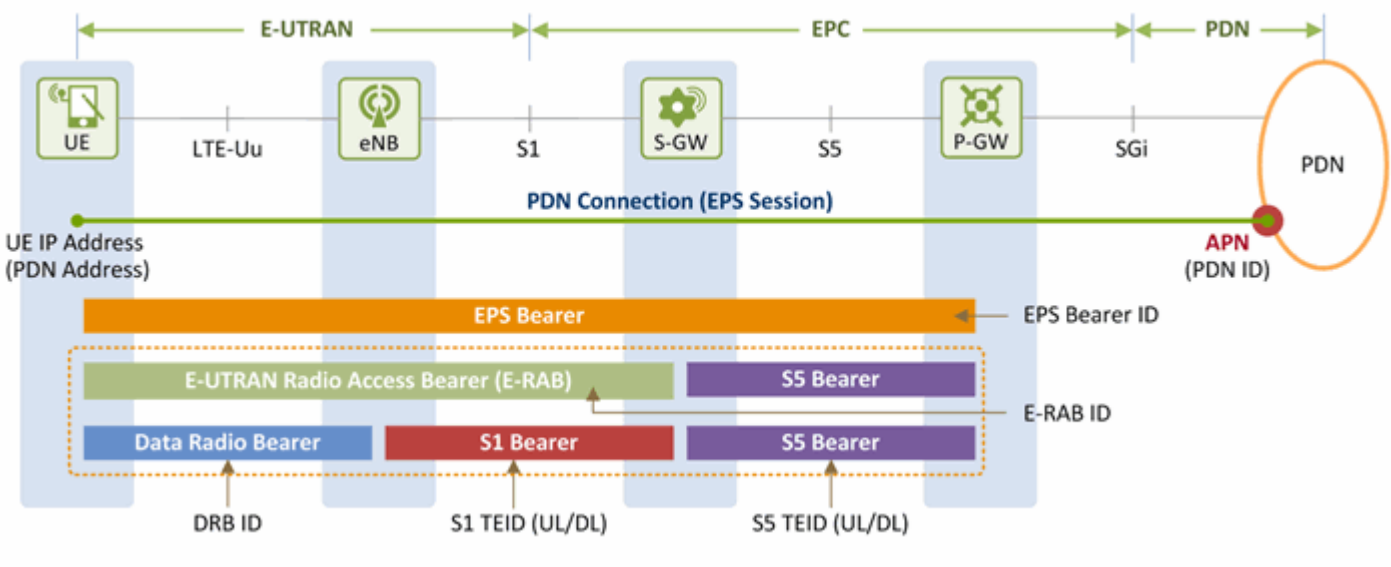


Figure 1. Overview of Session/Bearer IDs

2.1 EPS Session

IP connection between a UE and a PDN is called PDN connection or EPS session. Each PDN connection (or EPS session) is represented by an IP address of the UE and a PDN ID (in other words, Access Point Name (APN)). It has more than one EPS bearer to deliver user traffic (IP packets), and applies the service quality (QoS) policy obtained from a PCRF to the EPS bearers. The minimum fundamental bearer that an EPS session has for a PDN is called a default EPS bearer.

Having an EPS session established means i) a PDN through which a user is to use services has been selected (by the user's input or based on the subscription information provisioned by an HSS), ii) an IP address to be used in the PDN has been assigned to the user, iii) policy rules to be applied to the user IP packets (QoS and charging rules) have been selected, and iv) a default EPS bearer for delivering IP packets over the LTE network has been established. Through this EPS session established, IP packets can be exchanged between the user and the PDN according to the rules set by the operator.
Management and operation of sessions, including PCRF, will be explained in other document, and a PDN ID (APN) will be discussed as an ID relating to the EPS session in this document.

2.2 EPS Bearer

An EPS session is in charge of delivering and handling flows of the IP packets that are labeled with UE IP addresses and travel between a UE and a PDN (UE – P-GW – PDN). On the other hand, an EPS bearer is a pipe through which IP packets are delivered over the LTE network, i.e., between a UE and a P-GW (UE – eNB – S-GW - P-GW). A UE can have multiple EPS bearers concurrently. So, different EPS bearers are identified by their EPS bearer ID, which is allocated by an MME.
As seen in Figure 1, an EPS bearer actually is a concatenation of the following three bearers (DRB, S1 bearer and S5 bearer):

- [UE] - [eNB]: Data Radio Bearer (DRB)

  EPS bearer established over LTE-Uu interface. User traffic (IP packet) is delivered through a DRB. Different DRBs are identified by their DRB ID, which is allocated by an eNB.
- [eNB] - [S-GW]: S1 bearer

  EPS bearer established over S1-U interface. User traffic is delivered through a GTP tunnel. Different S1 bearers are identified by their tunnel endpoint identifier (TEID), which is allocated by the endpoints (eNB and S-GW) of the GTP tunnel.
- [S-GW] - [P-GW]: S5 bearer

  EPS bearer established over S5 interface. User traffic is delivered through a GTP tunnel. Different S5 bearers are identified by their tunnel endpoint identifier (TEID), which is allocated by the endpoints (S-GW and P-GW) of the GTP tunnel.

E-RAB is a bearer that has two endpoints of a UE and an S-GW, and consists of a DRB and an S1 bearer. Technically, E-RAB is a concatenation of a DRB and an S1 bearer, and connects from a UE to an S-GW (UE – eNB – S-GW). Different E-RABs are identified by their E-RAB ID, which is allocated by an MME. DRB IDs and E-RAB IDs are mapped with EPS bearer IDs on 1:1 basis.

2.3 Types of EPS Bearers

Before we go ahead and describe EPS bearer-related IDs, we will look at different types of EPS bearers and how they work. Figure 2 shows two different types of EPS bearers: default and dedicated. Each PDN must have one default EPS bearer, but may have none to many dedicated EPS bearers.

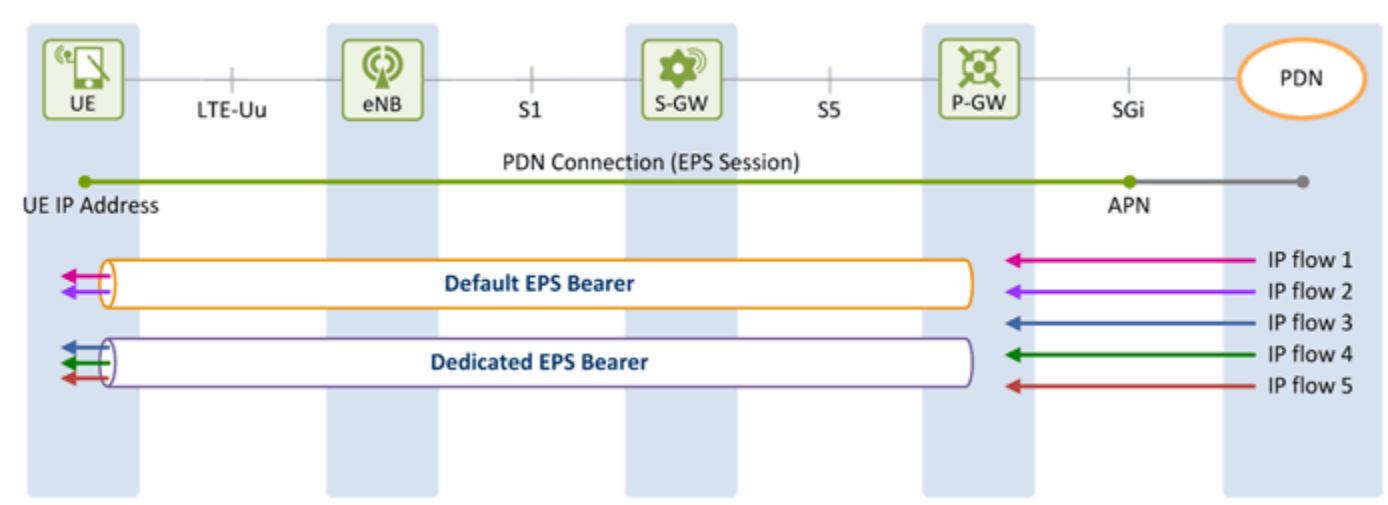


Figure 2. EPS Bearer Types

The LTE network is an all-IP network, and provides its users with always-on IP connectivity. This means, once a UE connects to a PDN using the IP address assigned at its initial attach to the network, the IP connection remains connected after a default EPS bearer is established over the LTE network and until the UE detaches from the LTE network (i.e., the PDN connection is terminated). Even when there is no user traffic to send, the default EPS bearer always stays activated and ready for possible incoming user traffic.

Additional EPS bearer can be established if the default EPS bearer itself is not sufficient enough to obtain QoS (see LTE QoS document). The additional EPS bearer established is called a dedicated EPS bearer and multiple dedicated bearers can be created if required by the user or the network. When there is no user traffic, these dedicated EPS bearers can be removed, whereas the default one is never removed and keeps the user staying connected to the network unless the user detaches from the network. Dedicated EPS bearers are linked to a default EPS bearer. The linked bearers are represented by a Linked EPS Bearer Identity (LBI), indicating they are all associated with the same default EPS bearer.

IP traffic from or to a UE is delivered through an EPS bearer appropriately depending on QoS class over the LTE network. Uplink IP traffic is mapped from a UE up to the EPS bearer while downlink IP traffic is mapped from a P-GW down to the EPS bearer.

As discussed in Sections 2.2 and 2.3, IDs relating to EPS bearers, such as EPS bearer ID, E-RAB ID, DRB, TEID, and LBI are described in this document. The following Chapter III will further explain about these EPS session/bearer IDs.