LTE-EPC WORKSHOP

LTE/EPC TECHNOLOGY ESSENTIALS

Fast Track

Hussien Mahmoud- PS Core/EPC Consultant

LTE Workshop

Introduction

This Workshop is a fast track Course to cover the basic architecture and functionalities of the LTE-EPC from the Packet Core Perspective. The course is a little bit advanced and the target Audience is requested to have a basic PS Foundations and Mobility Knowledge as a prerequisite. The course will cover the LTE-EPC Architecture, Call flows, Mobility and session management in addition to introductory slides for the EPS Security and LTE-DNS.

Author Information

Hussien Mahmoud
PS Core/ EPC Consultant
Packet Core Networks
Linkedin: https://eg.linkedin.com/in/hussienmahmoud

LTE Workshop

- **LTE/EPC Technology Essentials**
  - **LTE/EPC Overview.**
  - **LTE/EPC Network Architecture.**
  - **LTE/EPC Mobility and Session Management.**
  - **LTE/EPC Security and Authentication.**
  - **DNS Functionalities in LTE.**

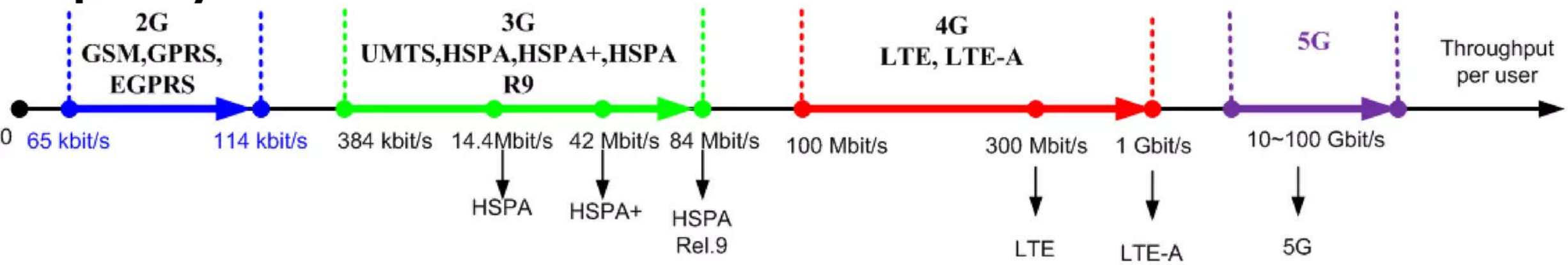
LTE/EPC Overview

Module One

Hussien Mahmoud- PS Core/EPC Consultant

LTE/EPC Overview

Adapt the user requirements for **high speed data** and **efficient quality.**



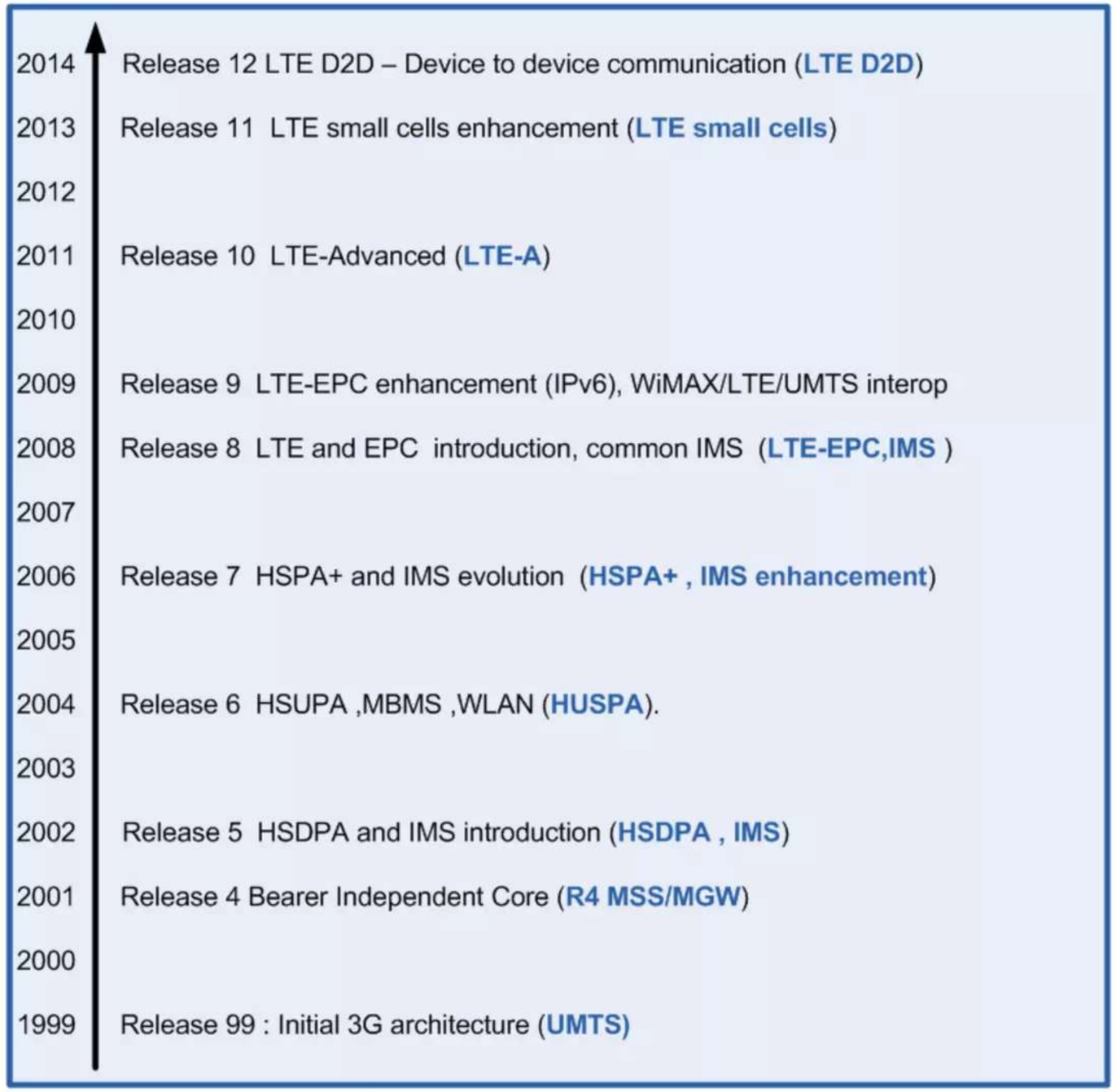
•**2G GPRS Mobile Technology** was the first step to provide data services over the mobile networks.

•**3G Technolog**y provides a higher data rates support with better integrity.

•**LTE** has the biggest challenges to overcome over the later technologies

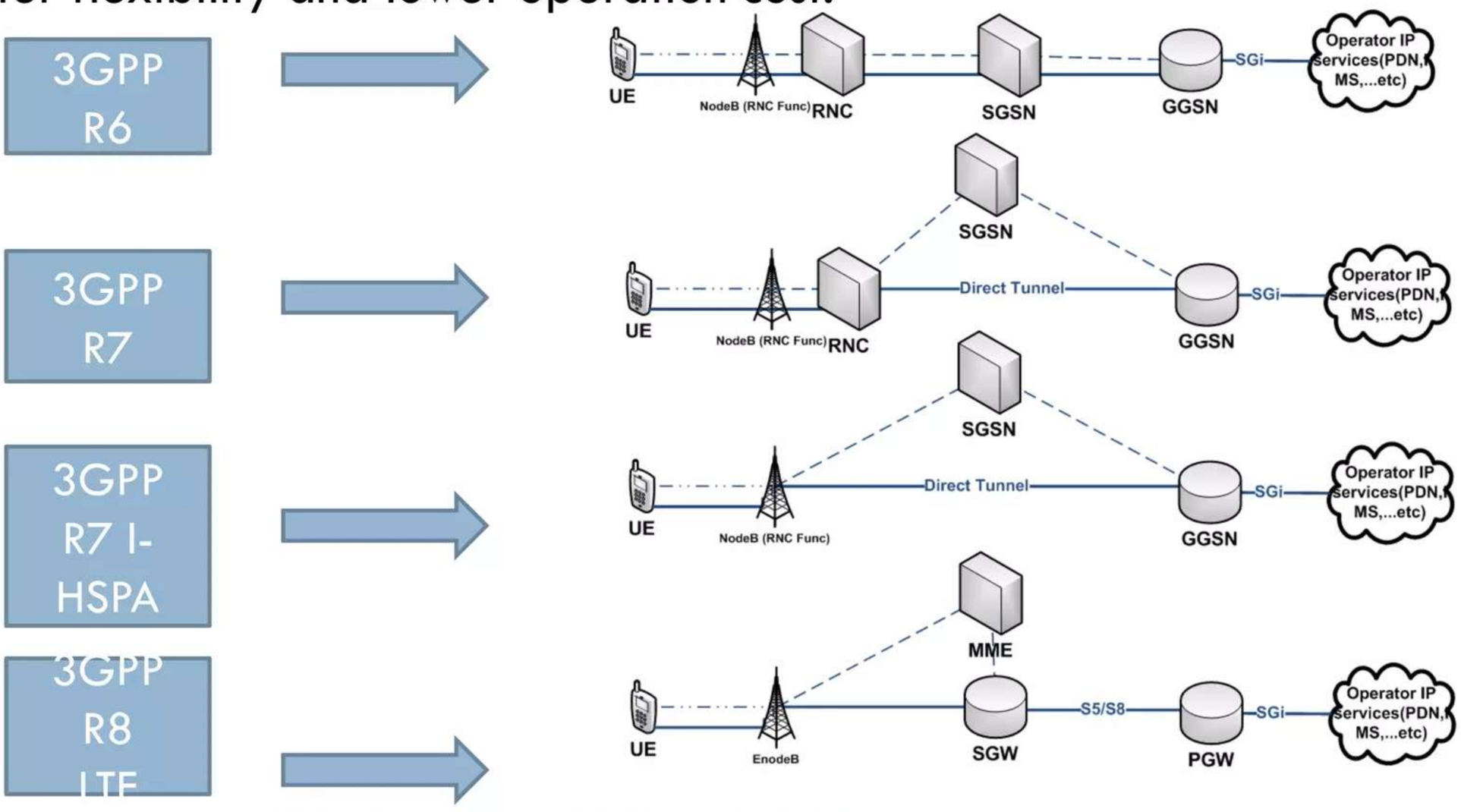
LTE/EPC Overview

- LTE is compatible with the current 2G/3G Network as it is counted as the next step of 3G HSPA Network.
- LTE have been developed by the same standard group of 2G/3G (3gpp).
- **Release 13 ,** IOT and M2M integration and customization of RAN plus Major enhancement for LTE features (SRVCC, power reduction).
- **Release 14 ,** Introduction of 5G Networks "Next Generation".



LTE/EPC Overview.

- **Flat Architecture:** 2 nodes based IP interface architecture.
- Flat network architecture are characterized by fewer network elements, **lower latency**, greater flexibility and lower operation cost.



LTE/EPC Network Architecture

Module Two

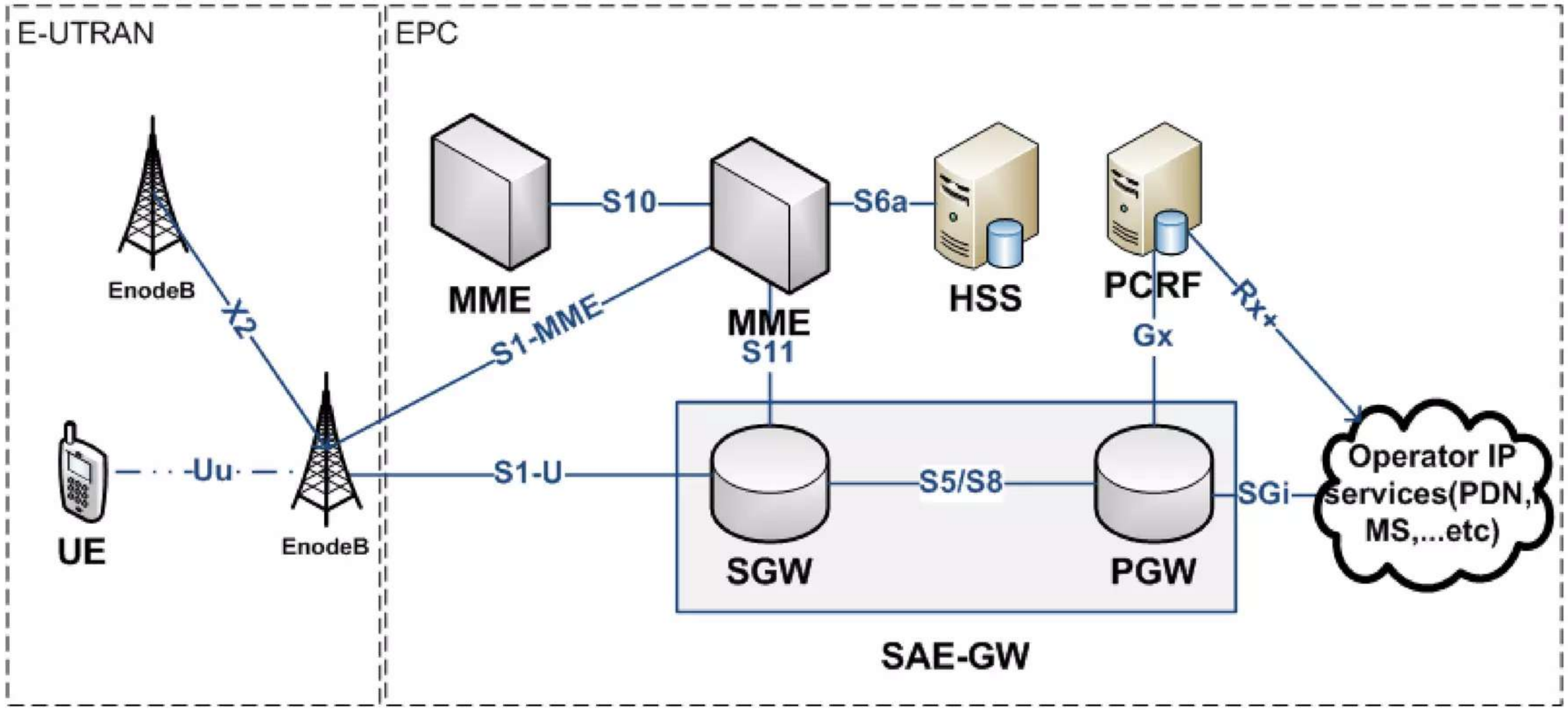
Hussien Mahmoud- PS Core/EPC Consultant

LTE/EPC Network architecture

Introduction

The LTE Network consists of mainly two parts

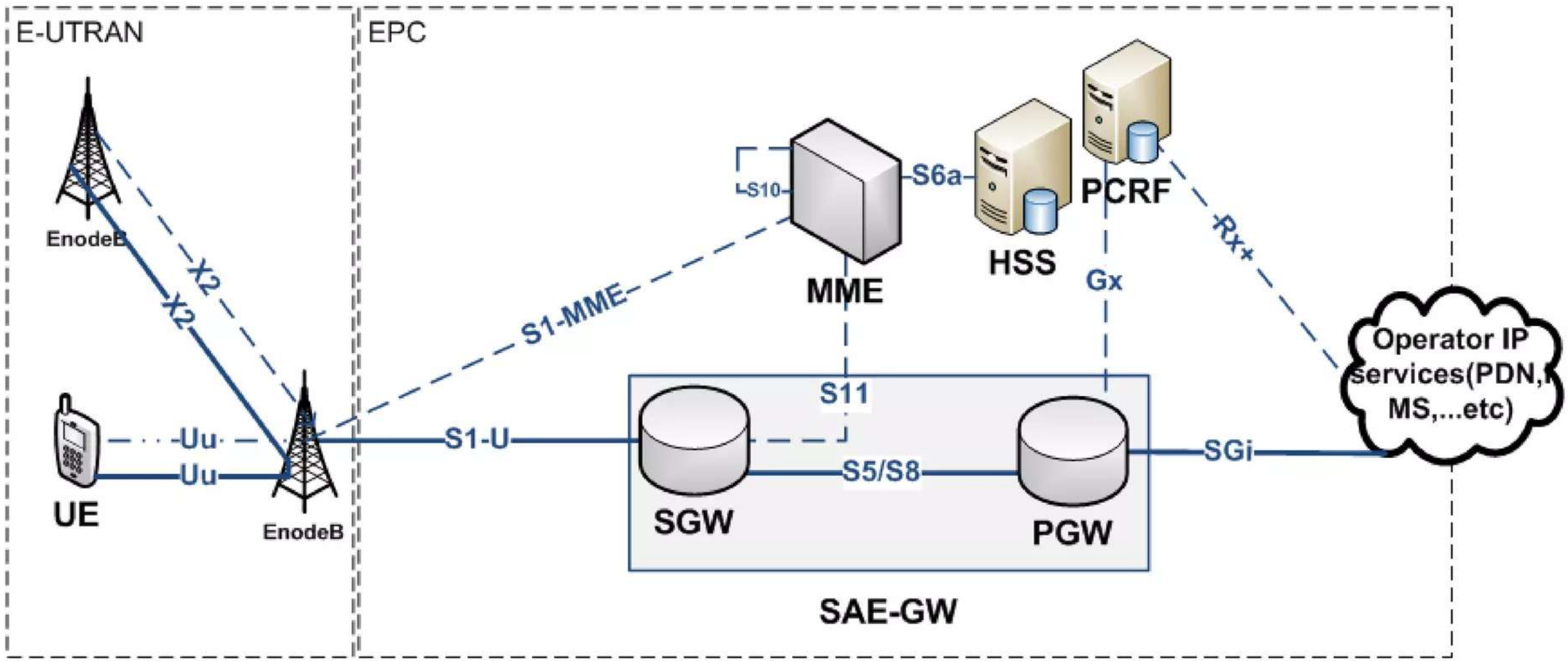
- **The Enhanced UTRAN** part which is composed of only EnodeB.
- **The EPC part** which includes the main components of the LTE Technology such as : MME , SGW ,PGW ,HSS and PCRF.



LTE/EPC Network architecture

Introduction

The LTE-EPC interfaces is divided in to interfaces that serves user plane, and interfaces that serves control plane in addition to hybrid interfaces that serves both user/control plane.



LTE/EPC Network architecture

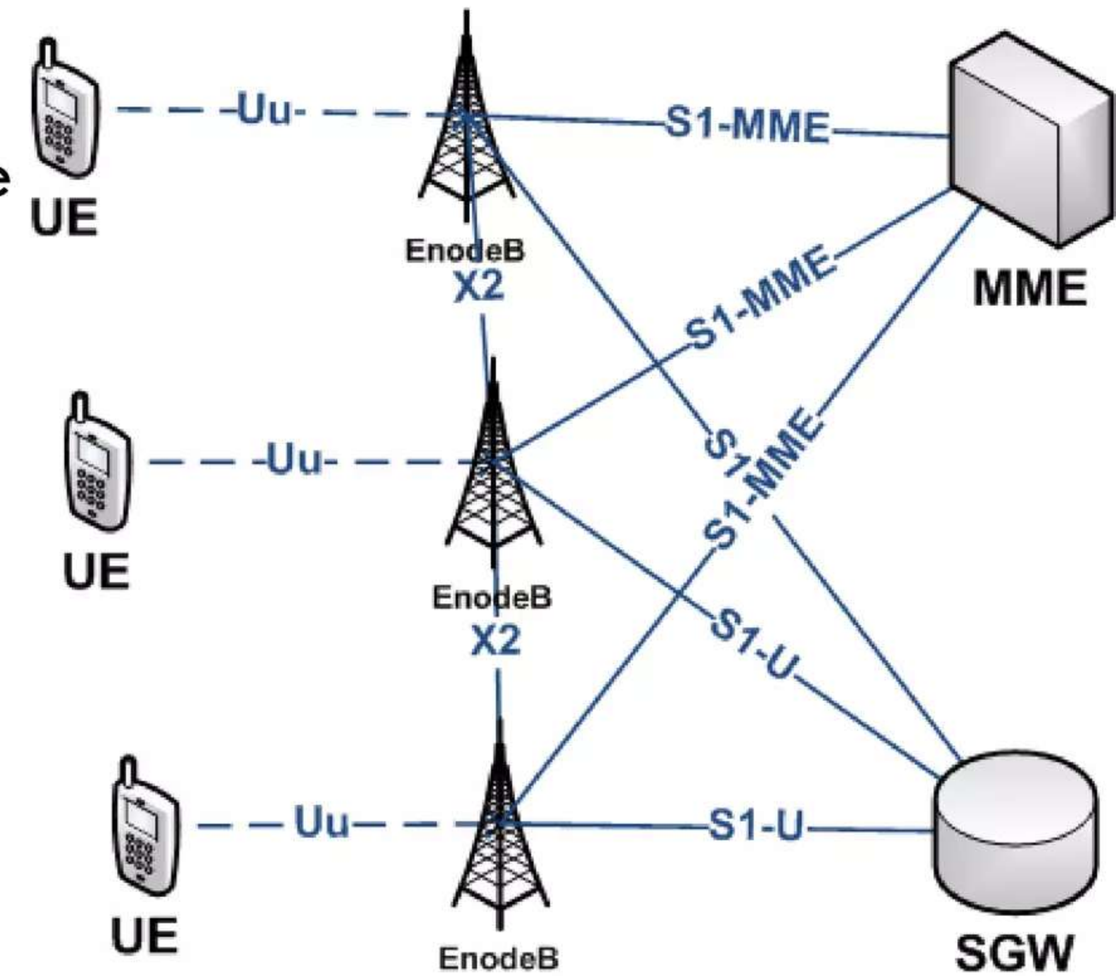
EnodeB

- The EnodeB provides the **Radio physical layer** and **Radio resource management** of the formal NodeB.

- Through the new Added **X2 interface** , the EnodeB can do a call handover **without the EPC involvement.**

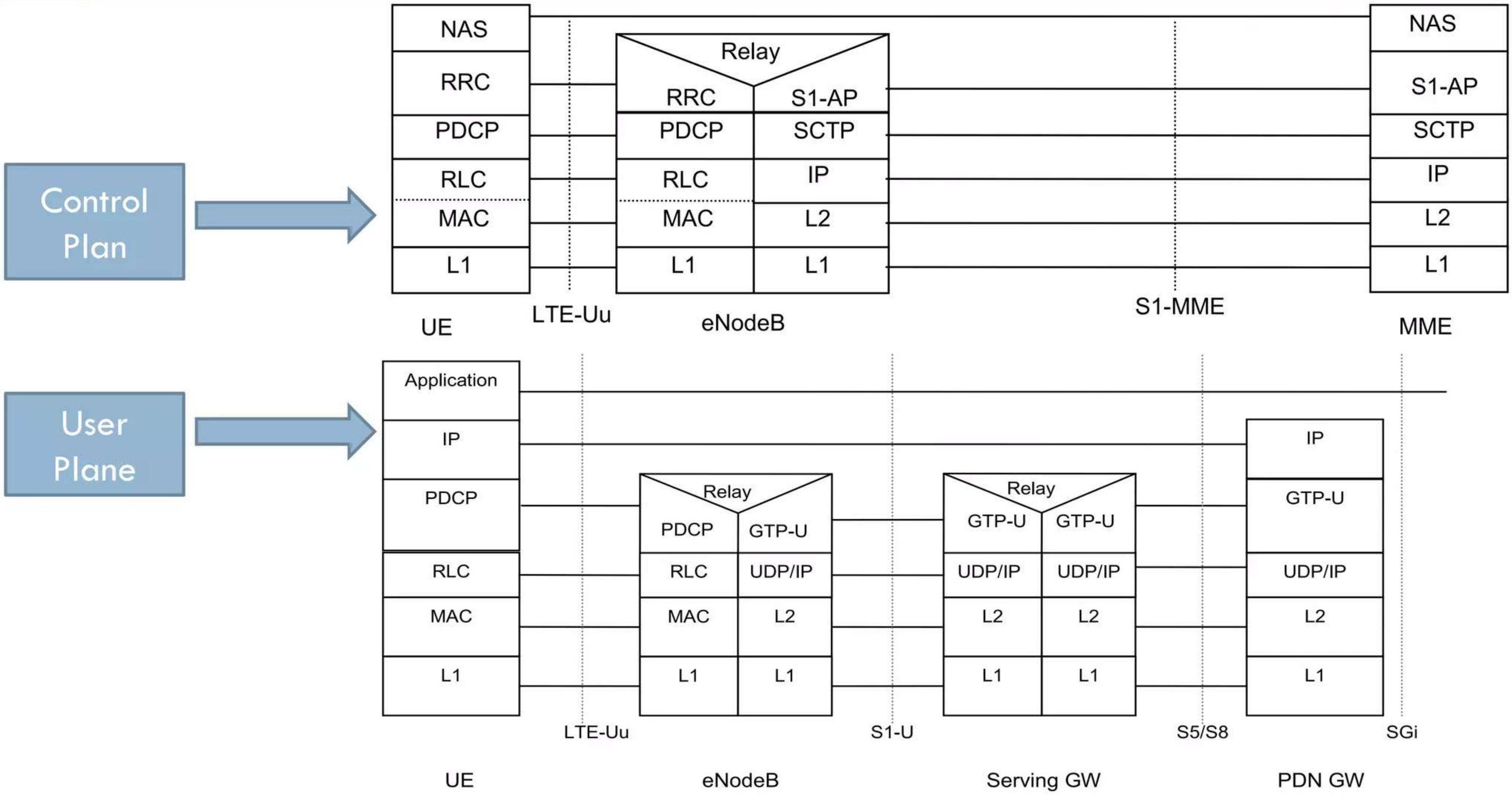
- Enode B provides the **user date routing** through the **SAE-GW.**

- Provide the **MME Selection** Algorithm.



LTE/EPC Network architecture

EnodeB: Protocol Stack

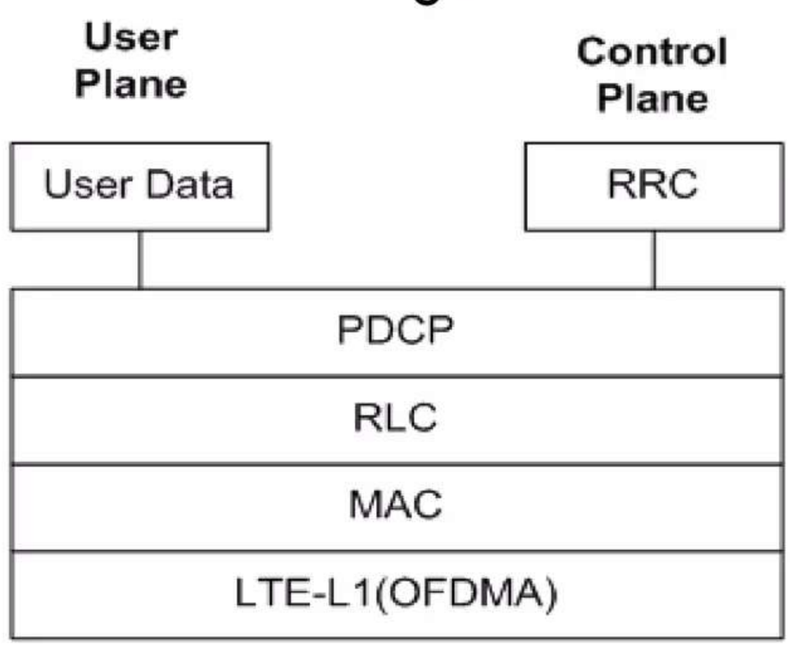


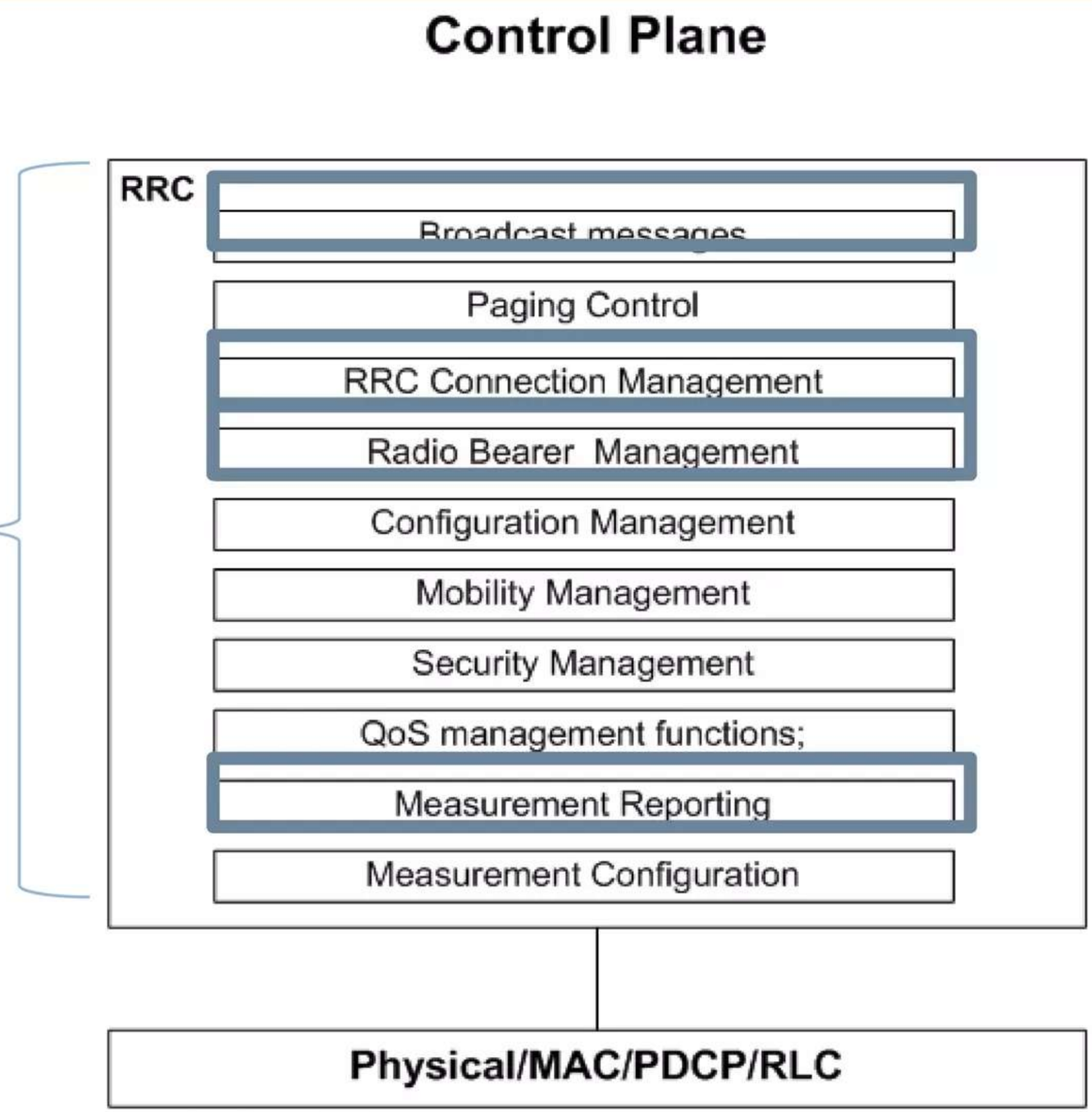
LTE/EPC Network architecture

EnodeB: Protocol Stack-Control Plane

- The EnodeB Protocol stack is divided into Control plane and User plane.

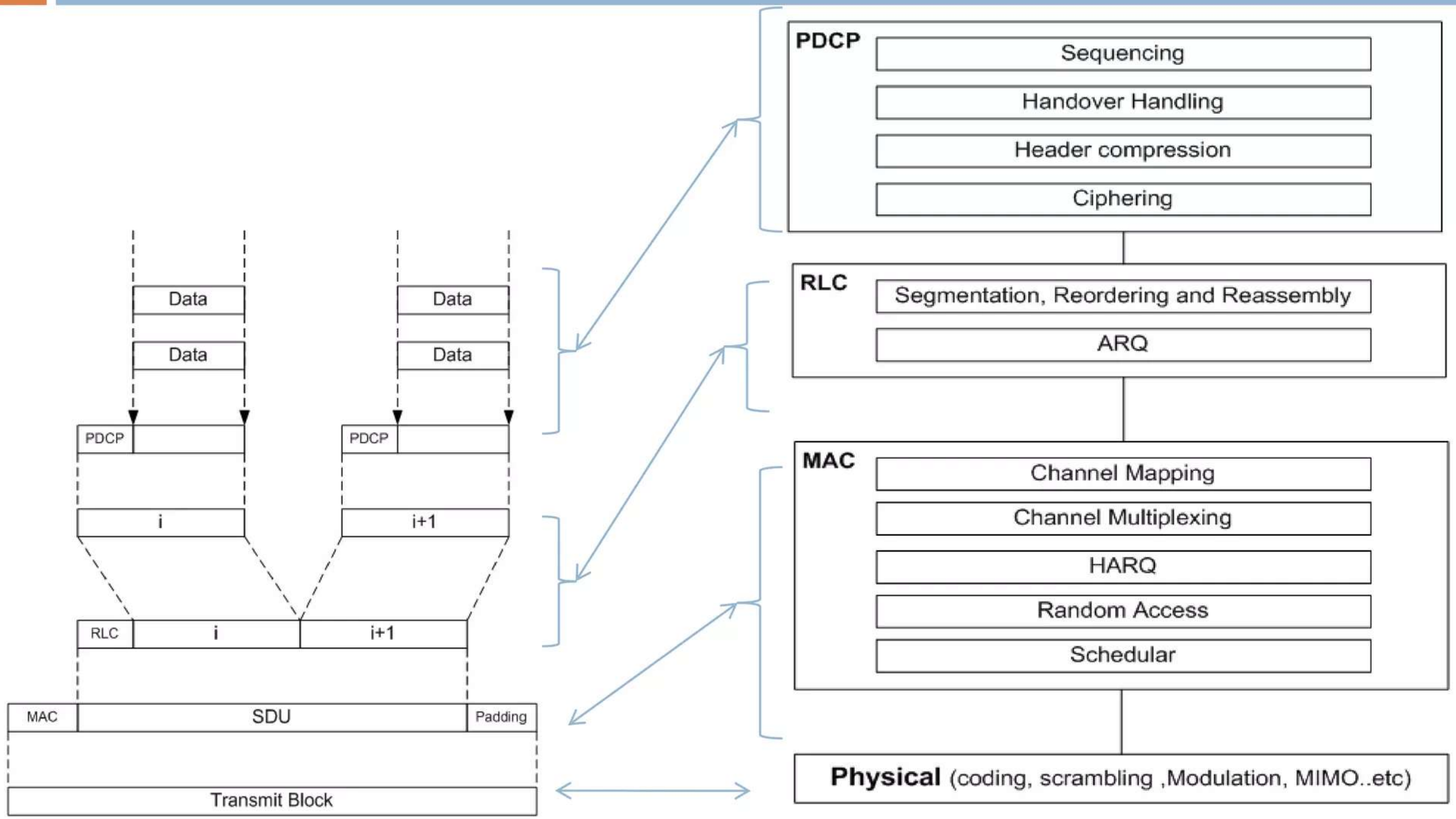
- The RRC is the main layer on the Control plane which includes all the radio resource management functions.





LTE/EPC Network architecture

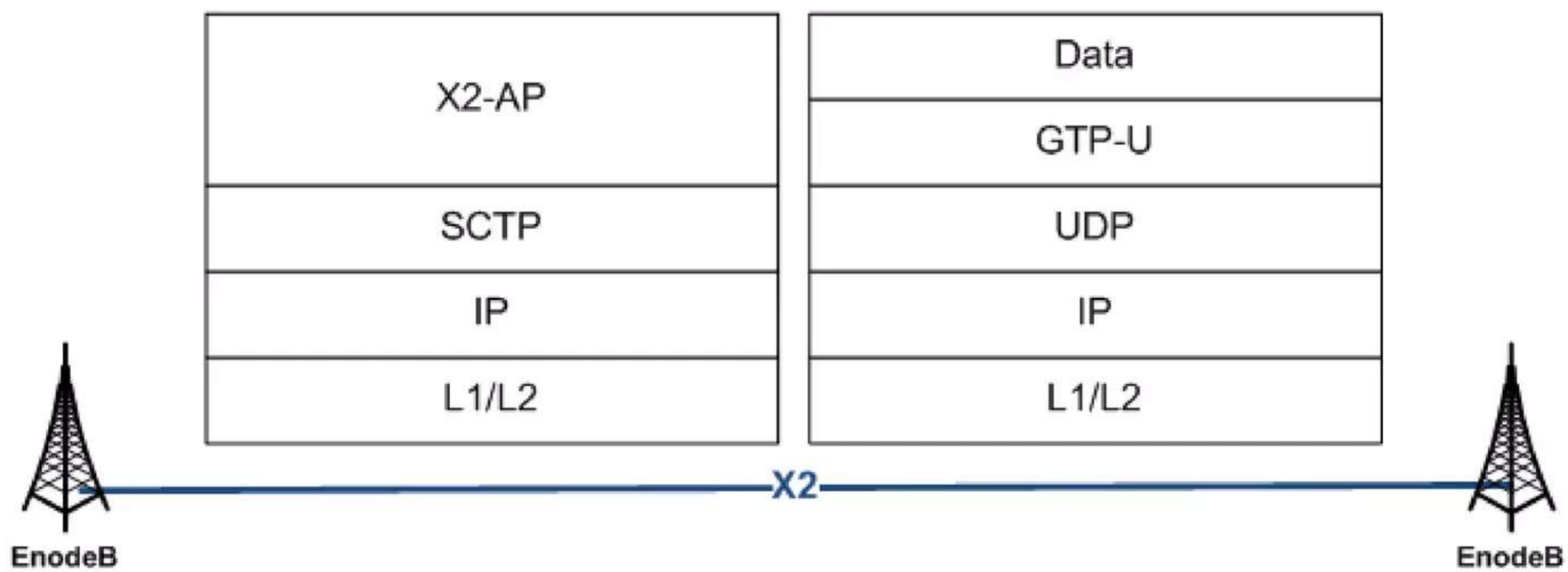
EnodeB: Protocol Stack-User Plane



LTE/EPC Network architecture

EnodeB: X2 Interface

- The X2 interface main function is to provide an E-UTRAN handover without the involvement of the Core network .
- The control plan is **based on SCTP** and User plane is **based on UDP.**
- The handover **Data is buffered within the EnodeB** and tunneled through a GTP interface to the Enode B.



LTE/EPC Network architecture

EnodeB: X2 Interface

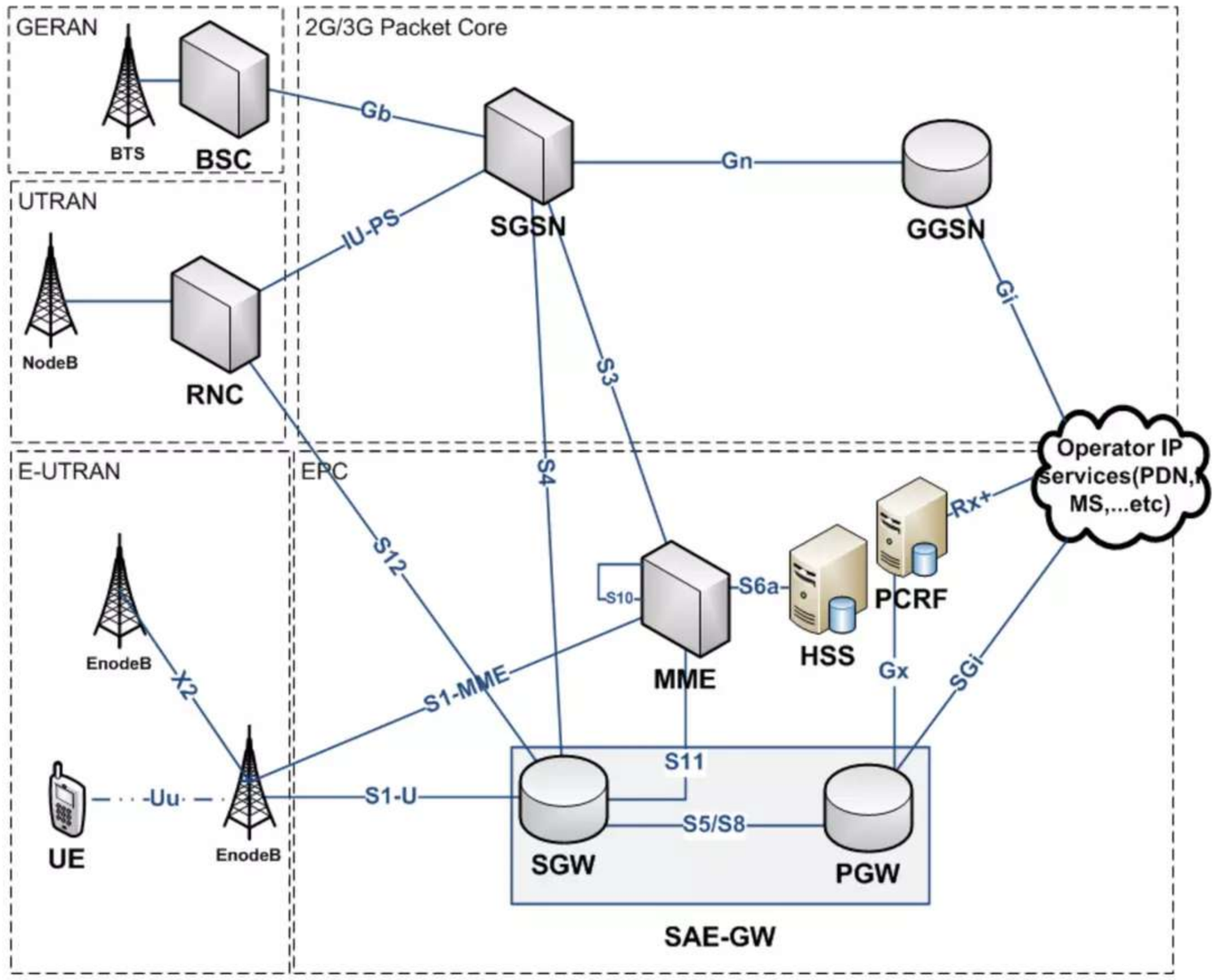
- The control plane is handled by the **X2-AP layer.**

```
◢ EUTRAN X2 Application Protocol (X2AP)
  ◢ X2AP-PDU: initiatingMessage (0)
    ◢ initiatingMessage
        procedureCode: id-handoverPreparation (0)
        criticality: reject (0)
      ◢ value
        ◢ HandoverRequest
          ◢ protocolIEs: 6 items
            ▷ Item 0: id-Old-eNB-UE-X2AP-ID
            ▷ Item 1: id-Cause
            ▷ Item 2: id-TargetCell-ID
            ▷ Item 3: id-GUMMEI-ID
            ▷ Item 4: id-UE-ContextInformation
            ▷ Item 5: id-UE-HistoryInformation
```

LTE/EPC Network architecture

Mobility Management Entity

- The MME is the main **signaling Node** across the LTE Network, the MME only handles the Signaling and doesn't include any user plane processing.



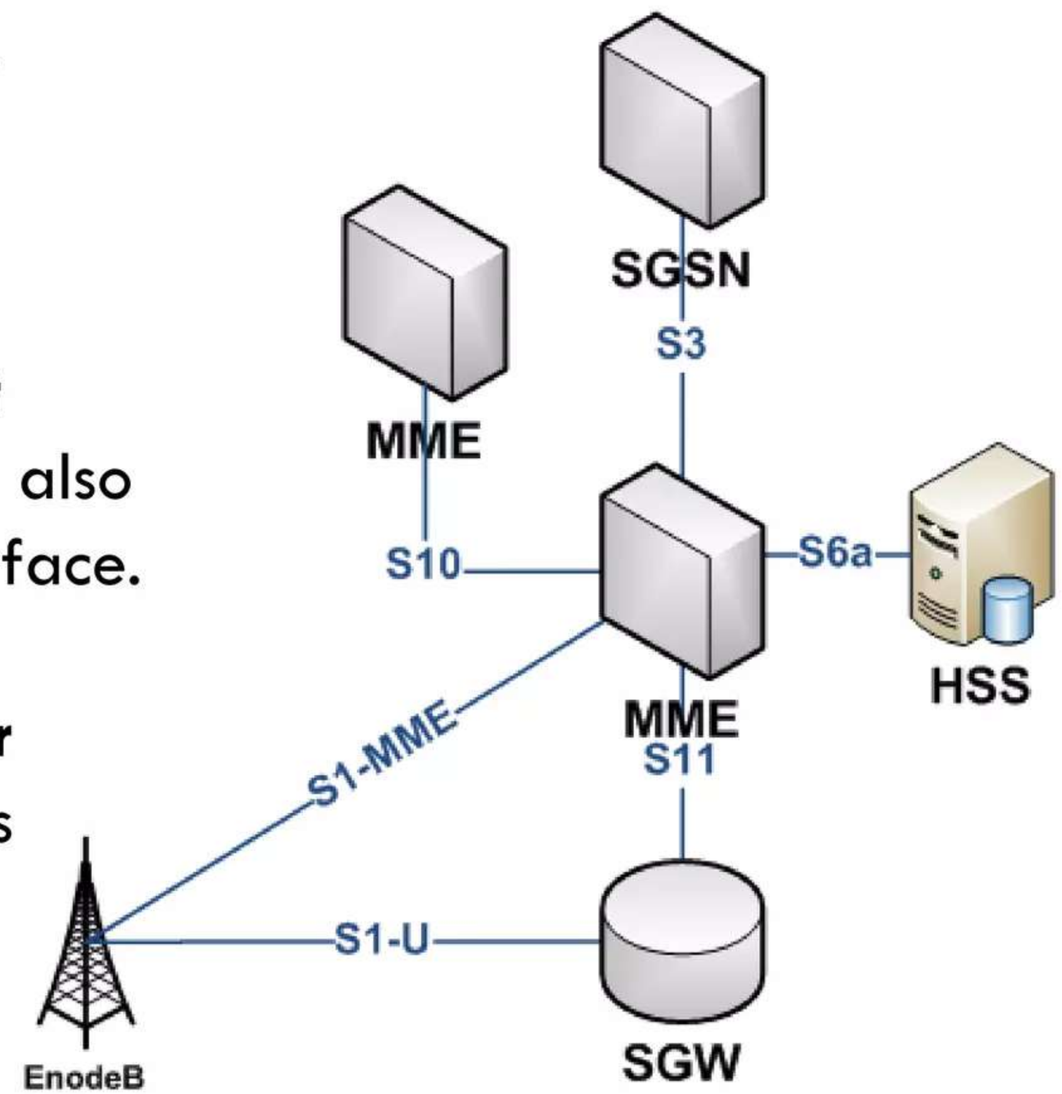
LTE/EPC Network architecture

Mobility Management Entity

- The MME provides a **Session management function** through Attach/Detach procedures , Bearer Management Across EPC (setup/release)…etc

- The MME provides a **Mobility management function** through Tracking Area Updates and also MME tracking area update through S10 interface.

- the MME is connected to **the HSS subscriber management** through the S6a interface , thus provide a **user authentication.**

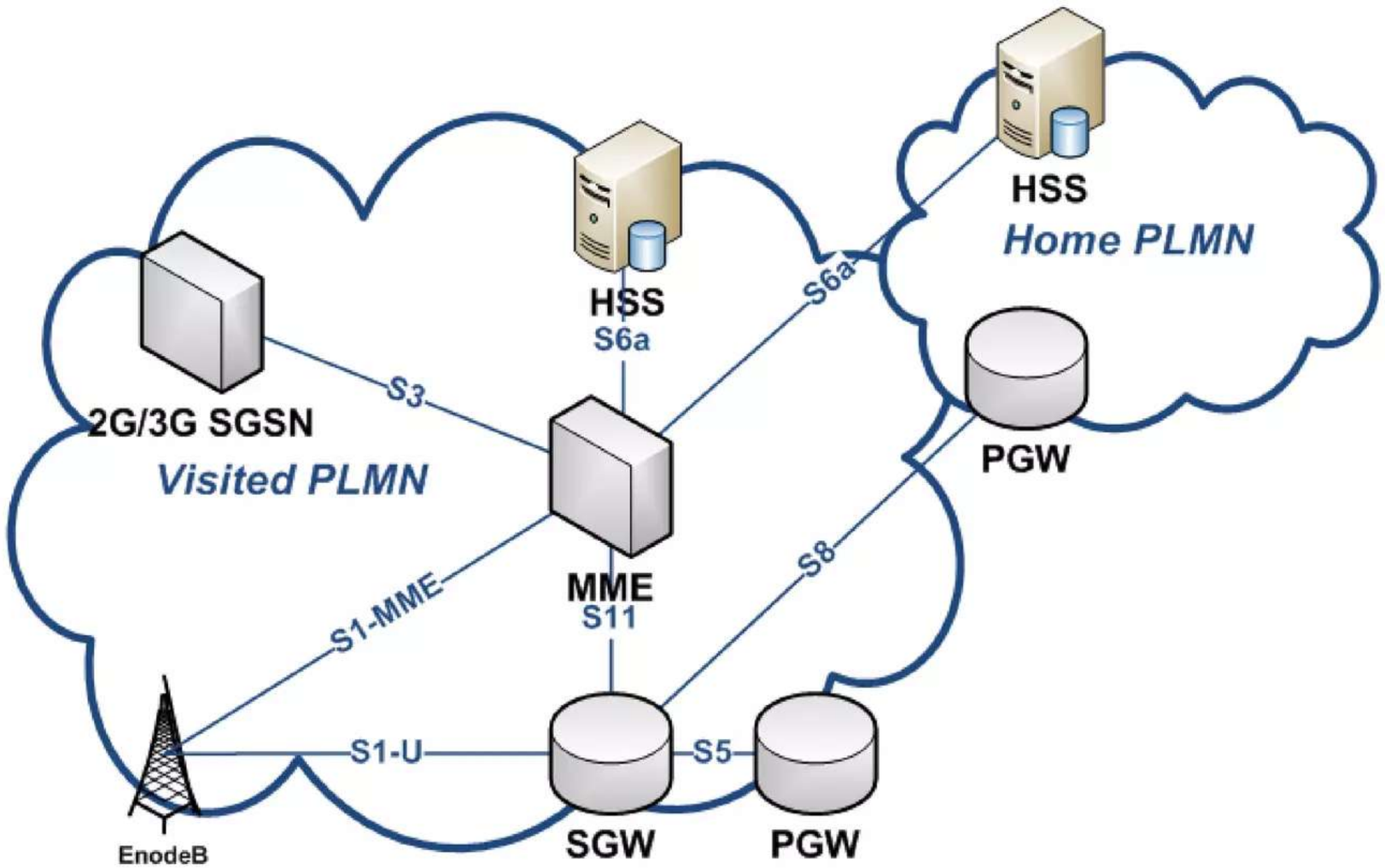


LTE/EPC Network architecture

Mobility Management Entity

•The MME Provides the main **Roaming** Architecture for inbound roamers flow.

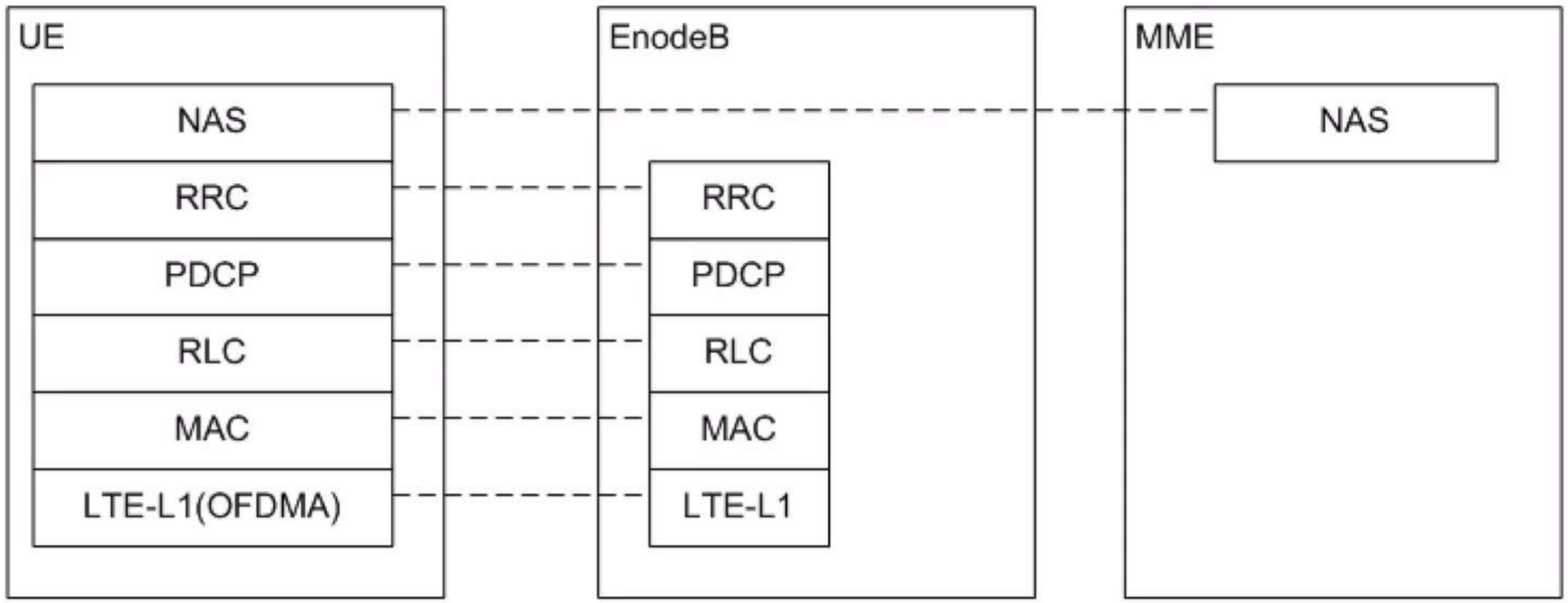
•.the MME provides an **integration point** with the **2G/3G Core SGSN** through the S3 interface which facilitate a better user mobility



LTE/EPC Network architecture

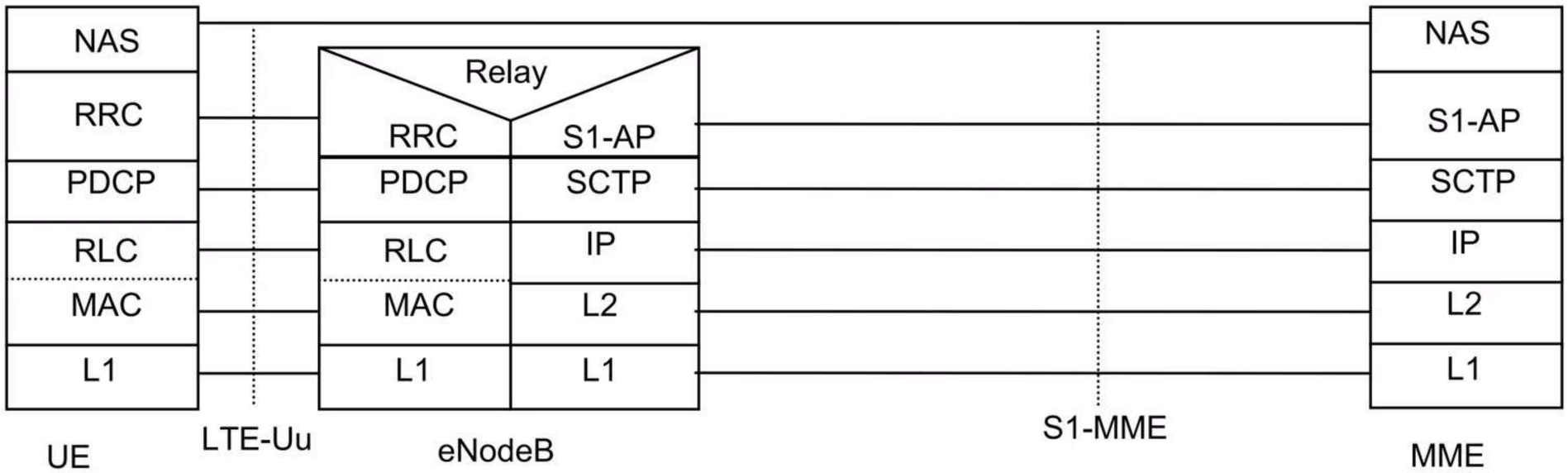
Mobility Management Entity: Protocol Stack

- The MME mobility and session management functionalities is implemented on the NAS layer.
- The non-access stratum (NAS) is highest protocol of the control plane between UE and MME at the radio interface.



LTE/EPC Network architecture

Mobility Management Entity: Protocol Stack

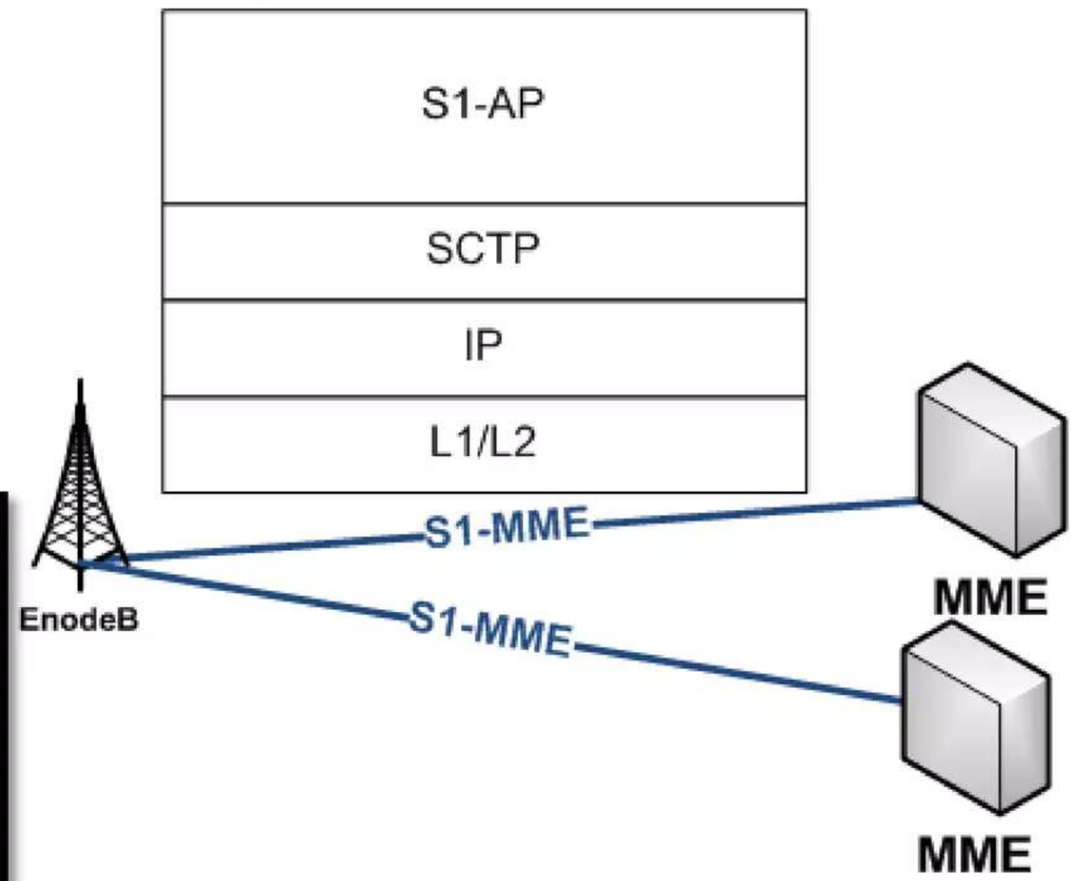


1	2013-05-06 10:3…	10.	.10	10	2	S1AP	110	id-S1Setup, S1SetupRequest
2	2013-05-06 10:3…	10.	.2	10	10	S1AP	102	id-S1Setup, S1SetupResponse
3	2013-05-06 11:0…	10.	.10	10	2	S1AP/NAS-EPS	238	id-initialUEMessage, Attach request, PDN connectivity request
4	2013-05-06 11:0…	10.	.2	10	10	S1AP/NAS-EPS	138	SACK id-downlinkNASTransport, Authentication request
5	2013-05-06 11:0…	10.	.10	10	2	S1AP/NAS-EPS	138	SACK id-uplinkNASTransport, Authentication response
6	2013-05-06 11:0…	10.	.2	10	10	S1AP/NAS-EPS	122	SACK id-downlinkNASTransport, Security mode command
7	2013-05-06 11:0…	10.	.10	10	2	S1AP/NAS-EPS	146	SACK id-uplinkNASTransport, Security mode complete

LTE/EPC Network architecture

Mobility Management Entity: S1-AP interface

- Provide a Control interface to the Enode B's.
- All signaling messages mobility and session management will flow through this interface.
- No traffic .
- The control plans is based on SCTP.
- S1-AP is the application protocol .
- Multiple S1-MME is supported




```
S1 Application Protocol
  S1AP-PDU: initiatingMessage (0)
    initiatingMessage
        procedureCode: id-S1Setup (17)
        criticality: ignore (1)
      value
        S1SetupRequest
          protocolIEs: 5 items
            Item 0: id-Global-ENB-ID
            Item 1: id-eNBname
            Item 2: id-SupportedTAs
            Item 3: id-DefaultPagingDRX
            Item 4: id-CSG-IdList
```

LTE/EPC Network architecture

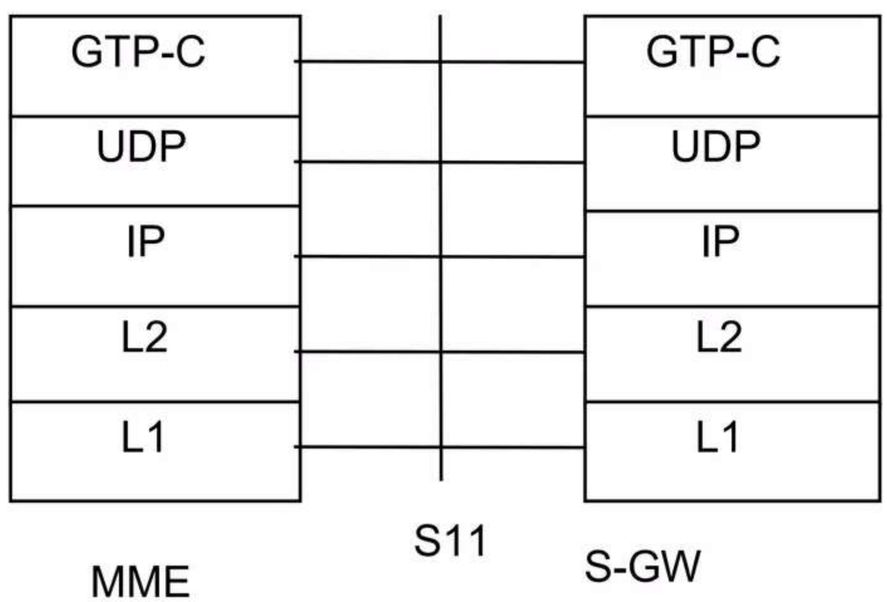
Mobility Management Entity: S1-AP interface

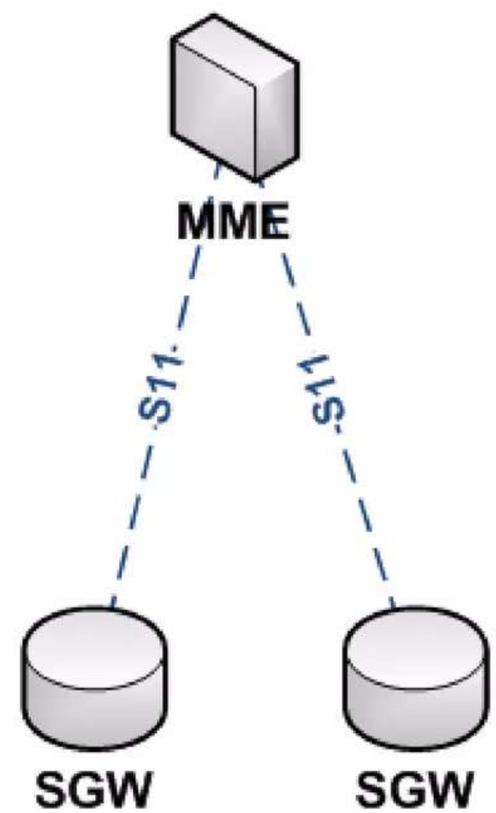
```
▲ S1AP-PDU: initiatingMessage (0)
  ▲ initiatingMessage
      procedureCode: id-initialUEMessage (12)
      criticality: ignore (1)
    ▲ value
      ▲ InitialUEMessage
        ▲ protocolIEs: 5 items
          ▷ Item 0: id-eNB-UE-S1AP-ID
          ▲ Item 1: id-NAS-PDU
            ▲ ProtocolIE-Field
                id: id-NAS-PDU (26)
                criticality: reject (0)
              ▲ value
                  NAS-PDU: [redacted]
                ▲ Non-Access-Stratum (NAS)PDU
                    0000 .... = Security header type: Plain NAS message, not security protected (0)
                    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
                    NAS EPS Mobility Management Message Type: Attach request (0x41)
                    0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
                    .111 .... = NAS key set identifier: No key is available (7)
                    .... 0... = Spare bit(s): 0x00
                    .... .001 = EPS attach type: EPS attach (1)
                  ▷ EPS mobile identity
                  ▷ UE network capability
                  ▷ ESM message container
                  ▷ DRX Parameter
                  ▷ MS Network Capability
          ▷ Item 2: id-TAI
          ▷ Item 3: id-EUTRAN-CGI
          ▷ Item 4: id-RRC-Establishment-Cause
```

LTE/EPC Network architecture

Mobility Management Entity: S11 Interface

- Provides a control interface between the MME and SAE GW.
- No traffic Only control plane.
- Multiple S11 connectivity to several SAE GW.
- The MME controls the user plane data through this interface.

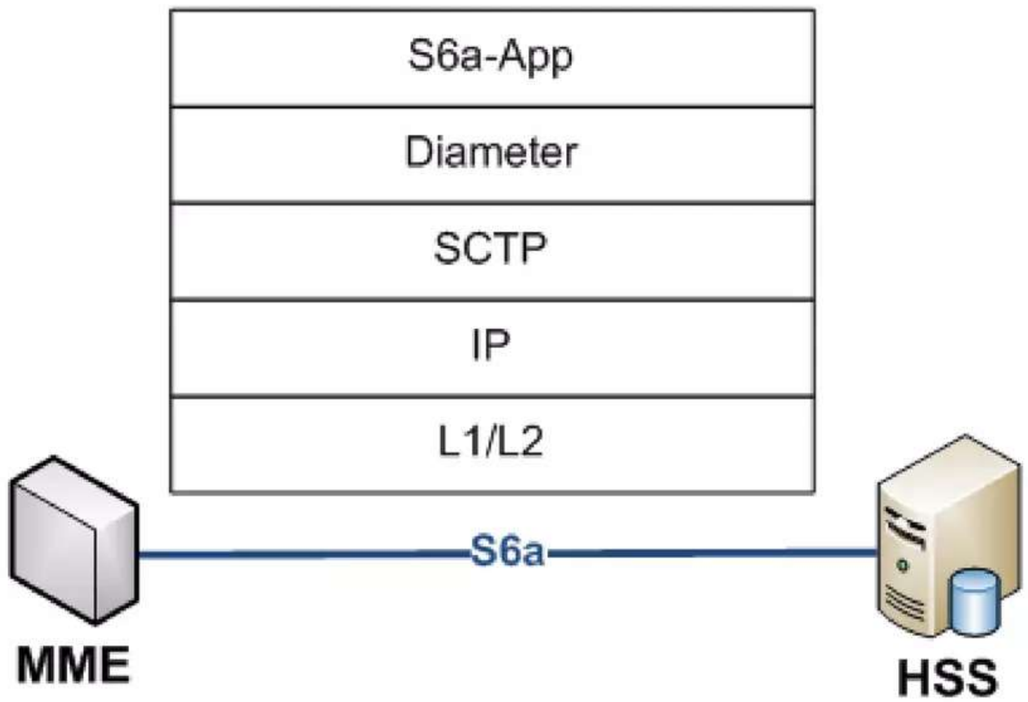




LTE/EPC Network architecture

Mobility Management Entity: S6a Interface

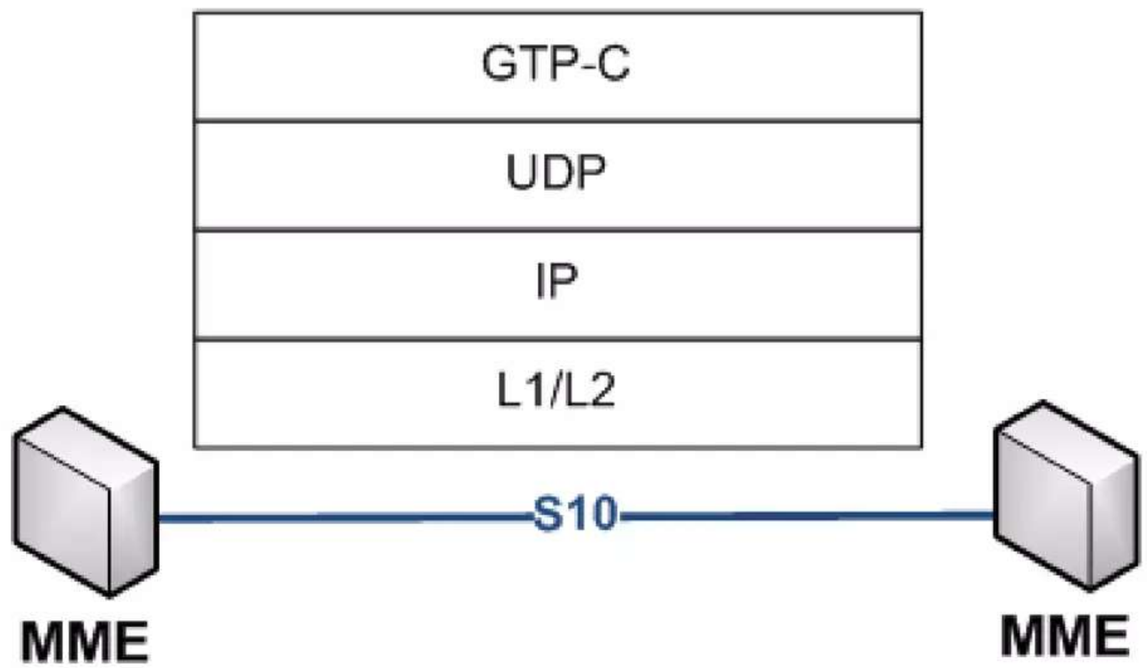
- The main functionality is to provide access to the HSS which is a subscriber management node.
- The connection is purely control plane
- The connection is based on SCTP and is using a Diameter protocol instead of the old SS7 application.
- The HSS Stores the subscriber data information (User ISD , Auth. Vectors , user apn profiles , QoS, TAI)



LTE/EPC Network architecture

Mobility Management Entity: S10 Interface

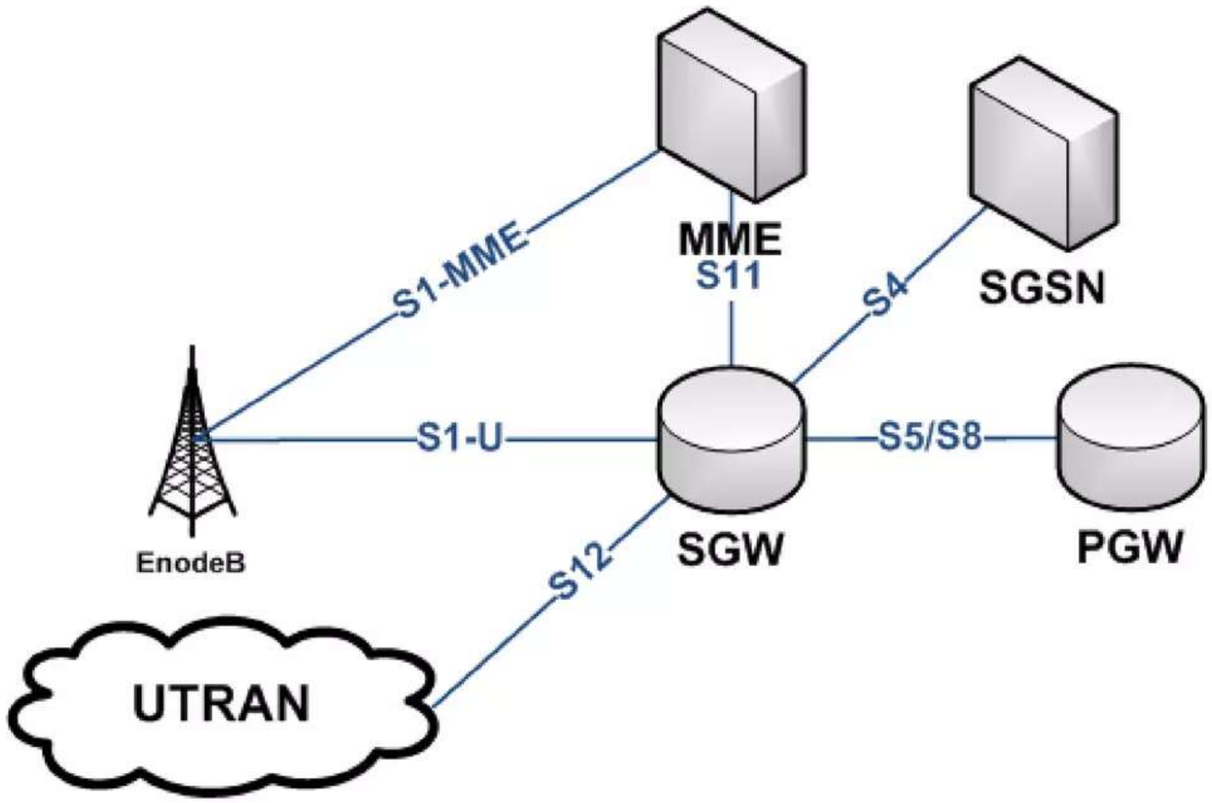
- The main functionality is to connect the MME with the neighbor MME for Different purposes.
- The interface supports only control plane.
- Inter MME Handover , subscriber IMSI retrieval , subscriber contexts.



LTE/EPC Network architecture

Serving SAE Gateway

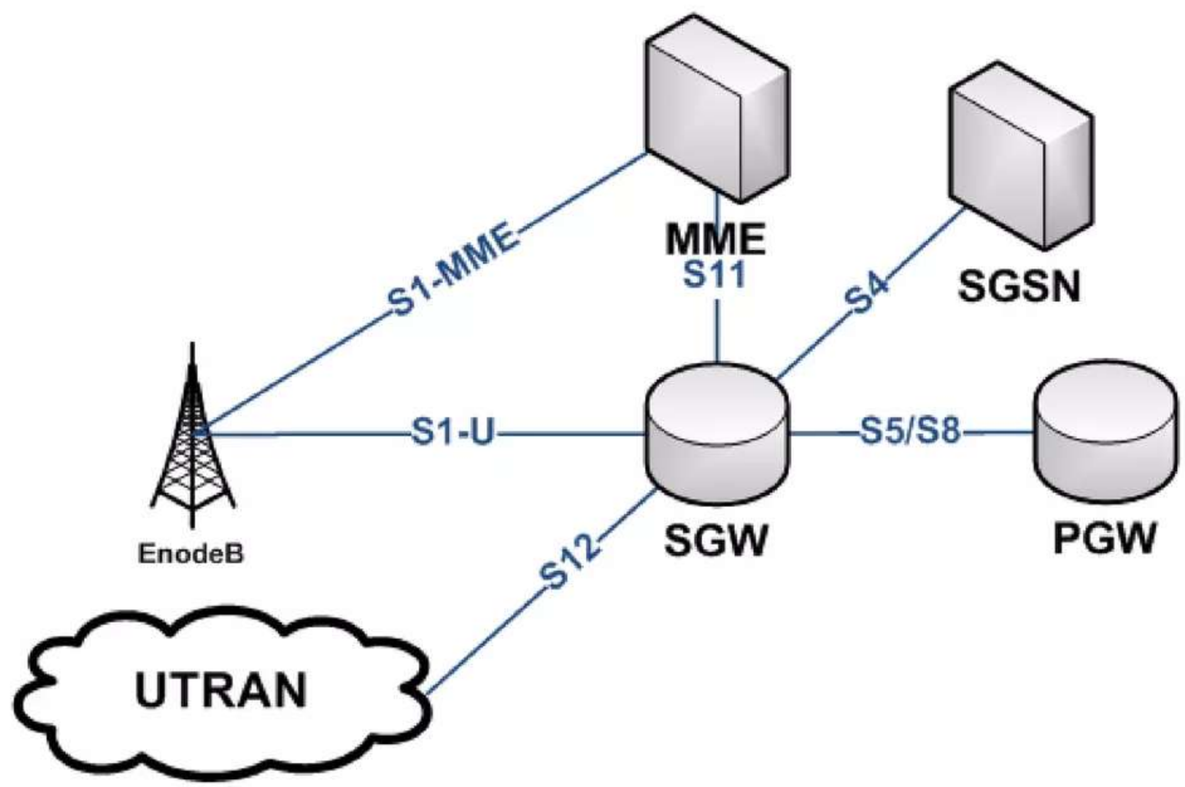
- The SAE acts as a user plane anchor where it manages the user data path through the S1-U and S5/S8 interface by forwarding the packets and buffering the data packets incase the idle mode.
- The SAE is controlled by one or more MME through the S11 interface.
- Multiple EnodeB's is connected via the SGW , where the SGW acts as a packet anchor for data handover.
- Setup and release the SAE bearer.
- Lawful interception.



LTE/EPC Network architecture

Serving SAE Gateway

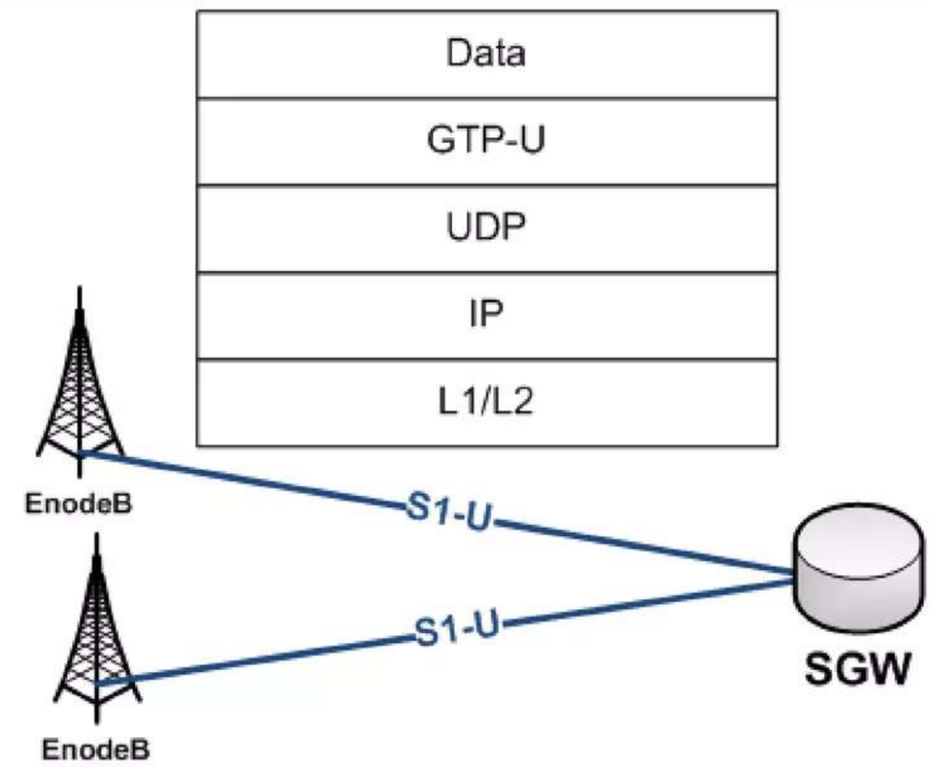
- Mobility anchoring for inter-3GPP mobility (S4 Interface).
- ECM-IDLE mode downlink packet buffering and notifying for MME.
- Packet routing and forwarding.
- Uplink and Downlink Transport Level Marking.
- Accounting for inter-operator charging.



LTE/EPC Network architecture

Serving SAE Gateway: S1-U Interface

- Provide user plane interface to the Enode B's.
- All user traffic are forwarded using this interface
- The user plan is based on GTP tunnels.
- Multiple S1-U connectivity is supported is supported



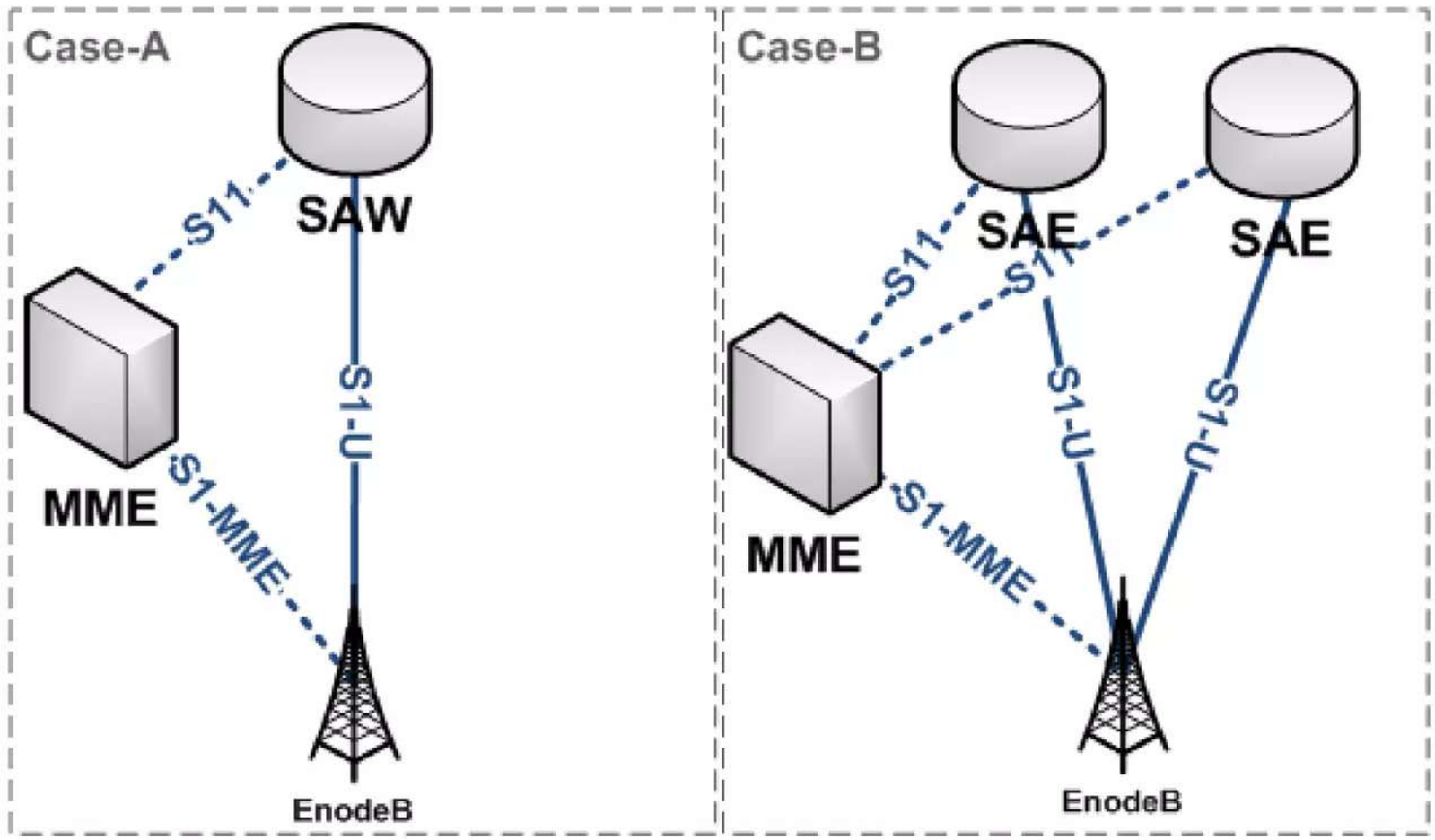

```
▷ User Datagram Protocol, Src Port: 2152 (2152), Dst Port: 2152 (2152)
◢ GPRS Tunneling Protocol
  ▷ Flags: 0x30
    Message Type: T-PDU (0xff)
    Length: 594
    TEID: 0x02000000
    T-PDU Data: 45000252000040004011223 80aff01010a00006413e213c4...
▷ Internet Protocol Version 4, Src: 1[redacted] Dst: [redacted]
▷ User Datagram Protocol, Src Port: 5090 (5090), Dst Port: 5060 (5060)
▷ Session Initiation Protocol (REGISTER)
```

LTE/EPC Network architecture

S1-U/S11 Connectivity

Case-A the basic connectivity model for the LTE-EPC data plane where the Enode is connected to one MME and one SAE GW.

Case-B the Enode B is connected to only one MME and multiple SAE-GW controlled by the same MME.

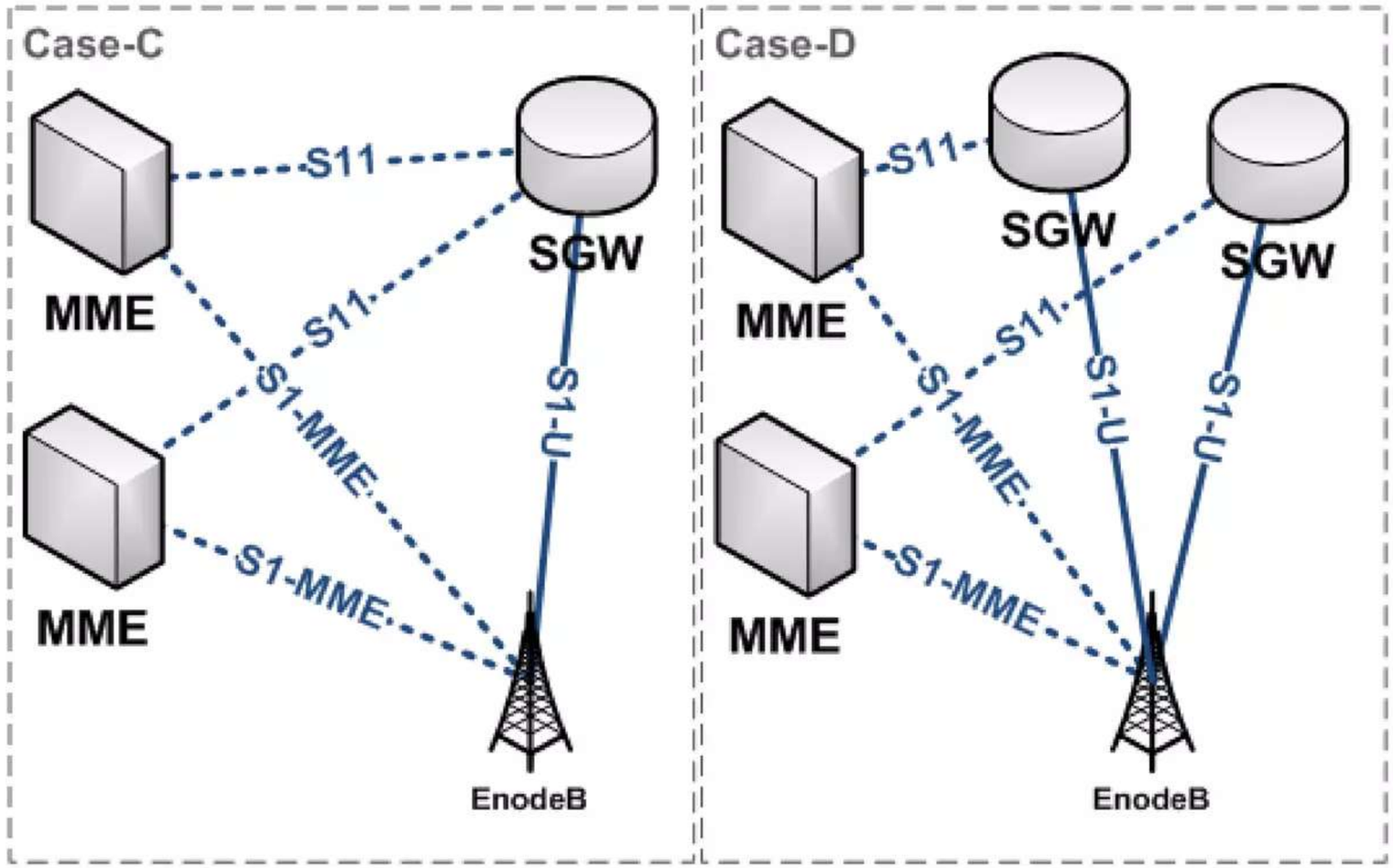


LTE/EPC Network architecture

S1-U/S11 Connectivity

Case-C the Enode B is connected to multiple MME's and only connected to one SAE-GW.

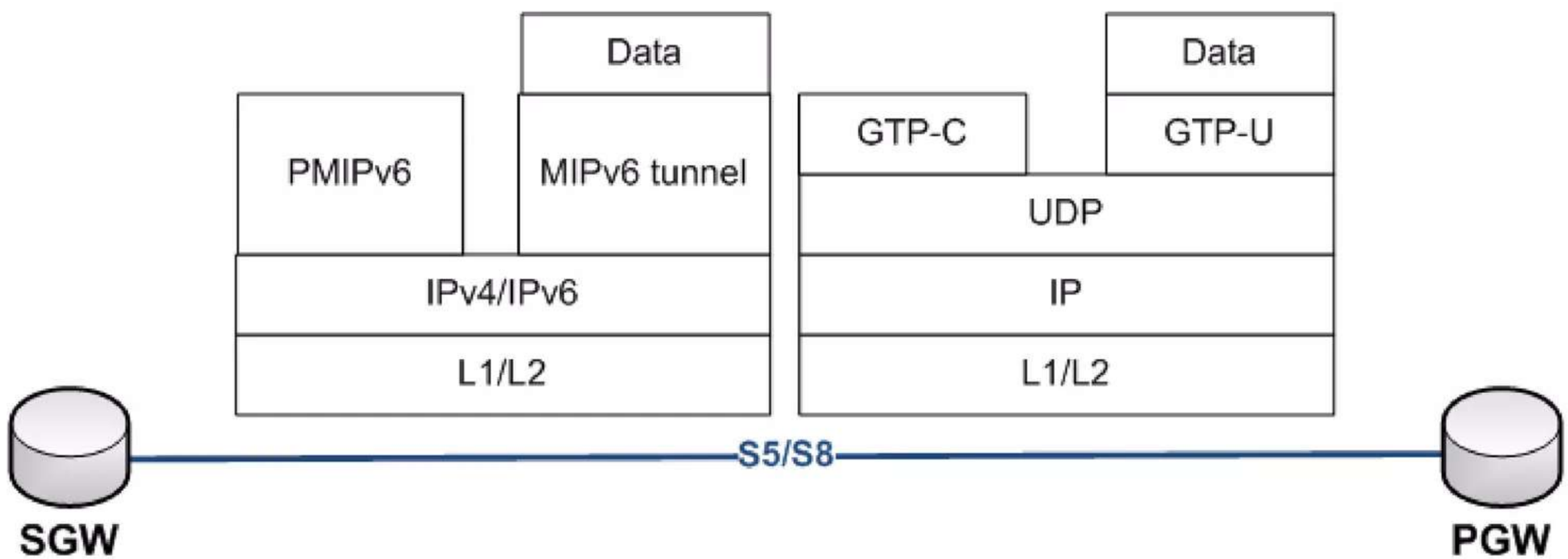
Case-D the Enode B is connected to multiple MME's and multiple SAE-GW.



LTE/EPC Network architecture

Serving SAE Gateway: S5/S8 Interface

- The main functionality is to forward traffic between S –GW and P-GW.
- S5 is standardized for local network and S8 is standardized for roaming
- A control and user plane is under two different protocol stacks GTP and PMIP.

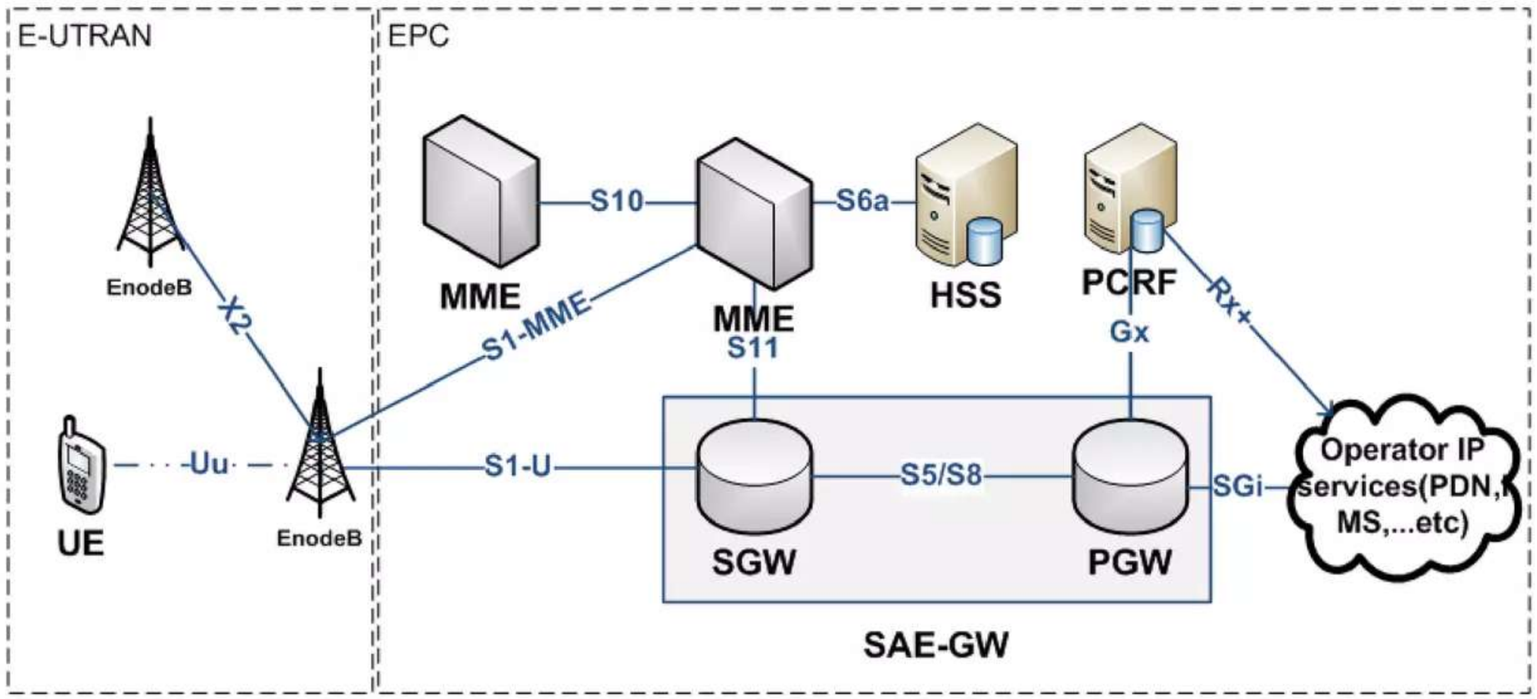


LTE/EPC Network architecture

PDN SAE Gateway

PDN Gateway (PGW) – Functions

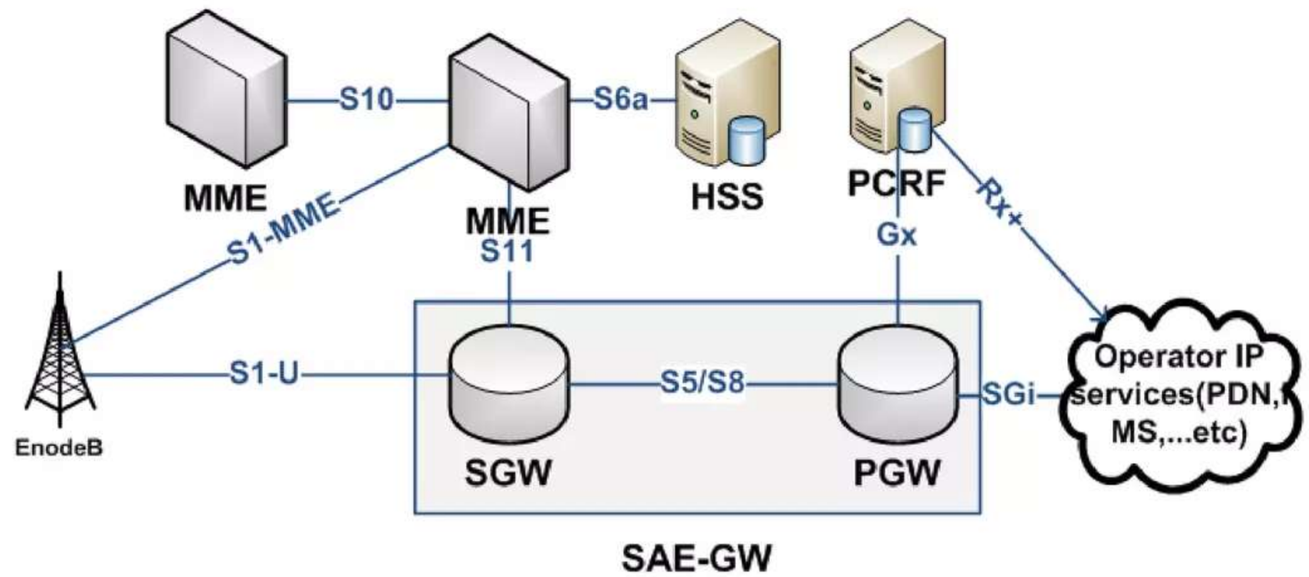
- UE IP address allocation.
- Per-user based packet filtering .
- Transport level packet marking in the uplink and downlink.
- Accounting for inter-operator charging.
- UL and DL service level gating control.
- Policy & Charging enforcement.

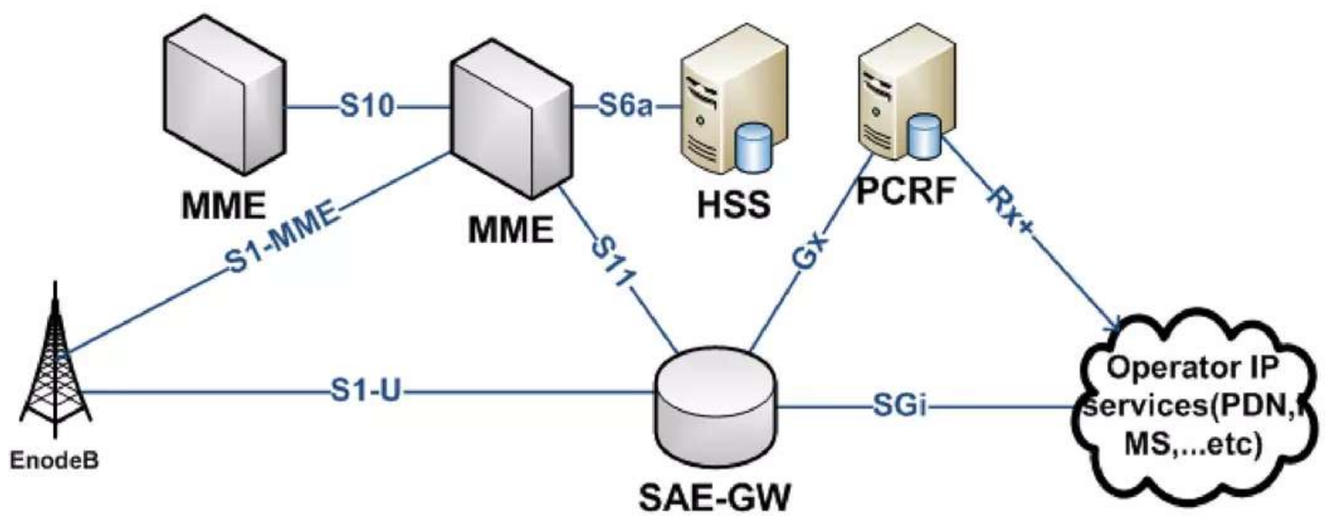


LTE/EPC Network architecture

Combined SAE-Gateway

- The S-GW and P-GW may be integrated into one node to act as an SAE-GW

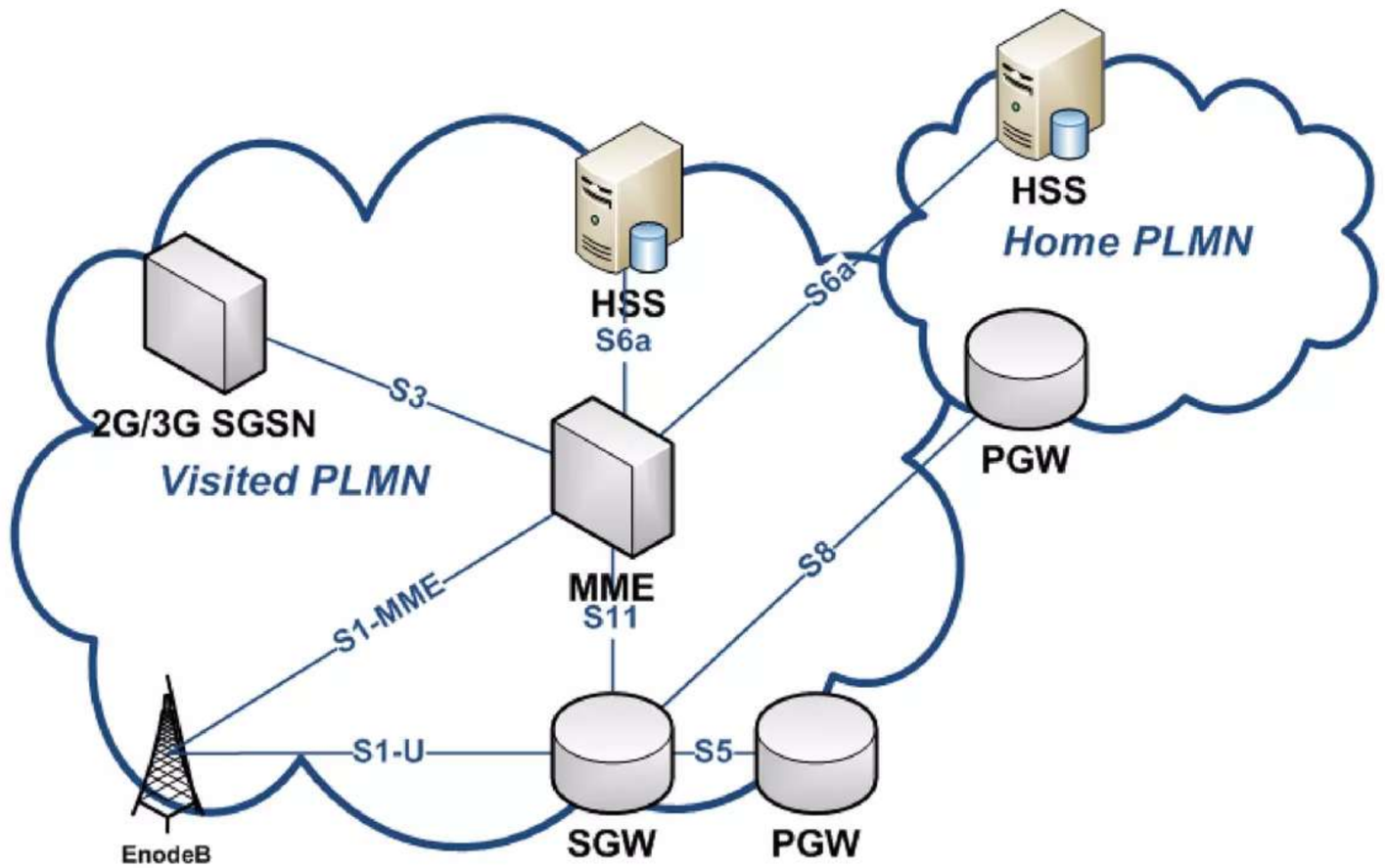




LTE/EPC Network architecture

Home Subscriber Server

- Provides the subscriber Data Management and mobility information (User Number ,location, profile , QoS…etc.)
- The HSS includes also the functionality of the AUC.
- Connects to the SAE or S-GW via the S6a interface for roaming and local Networks.

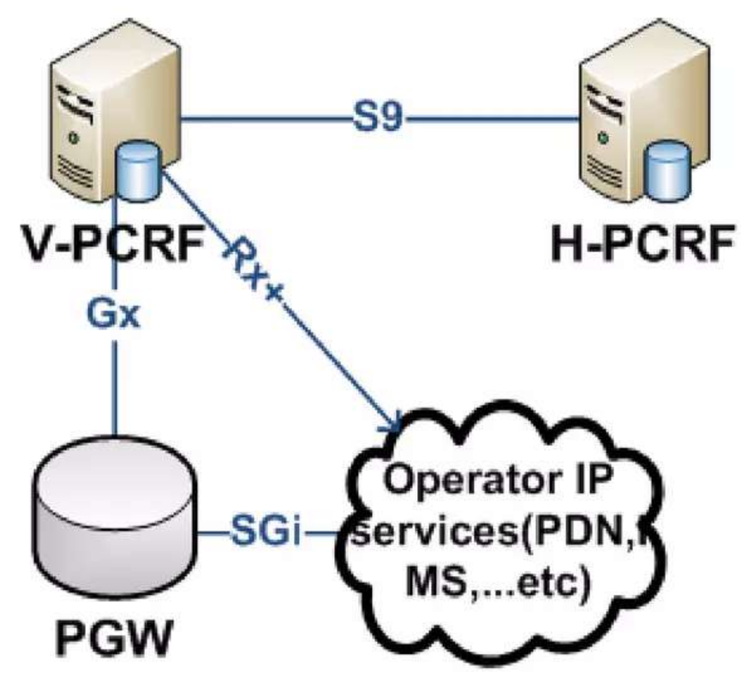


LTE/EPC Network architecture

Policy and Charging Rule Function

- The PCRF controls the main policies assigned per subscriber.
- Provide a QoS Negotiation and management through the Gx interface which may include a modification or change in the SAE Bearer.
- Provide a Data Network interface through the Rx+

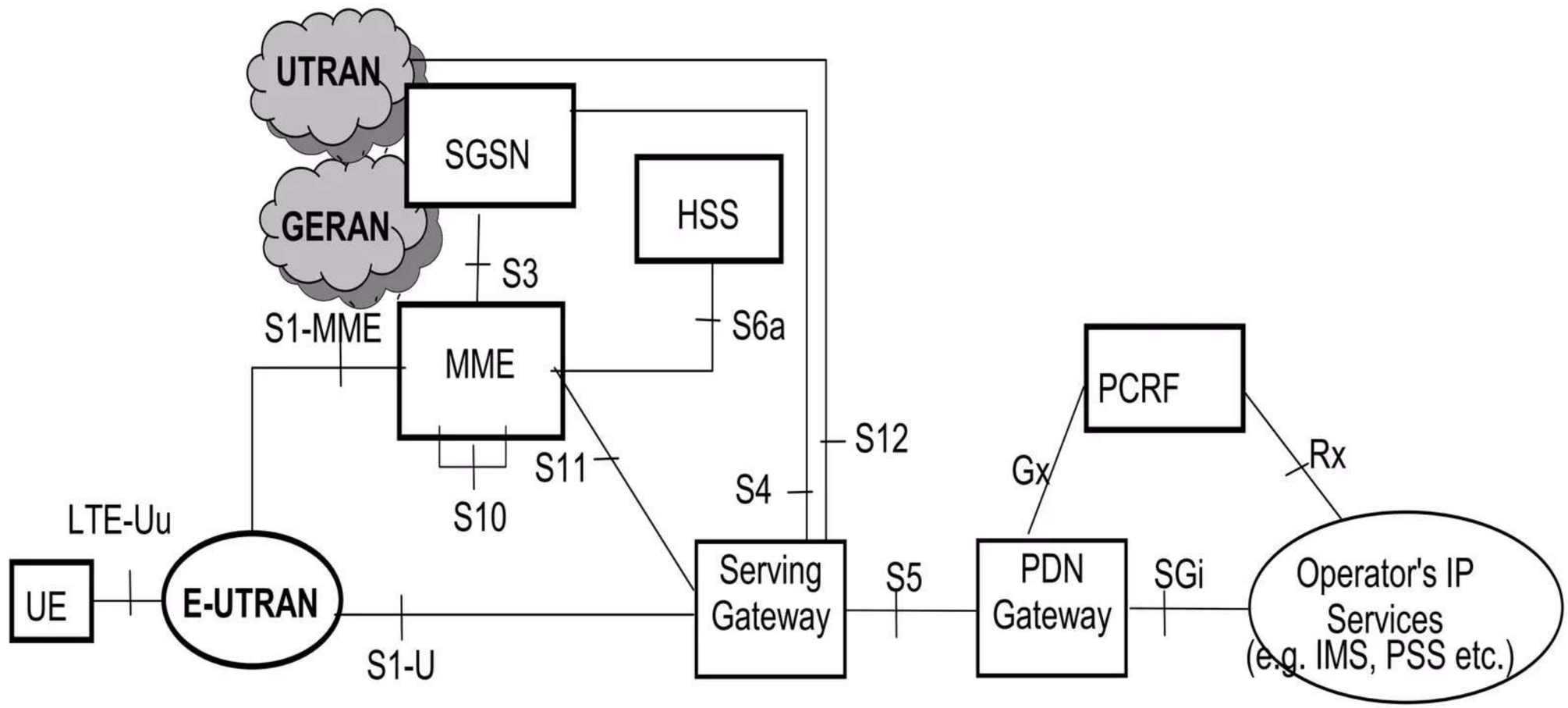
- An extra interface is provided between local and roaming PCRF the interface is defined in the 3GPP by S9.



LTE/EPC Network architecture

Roaming/Non-Roaming Architecture

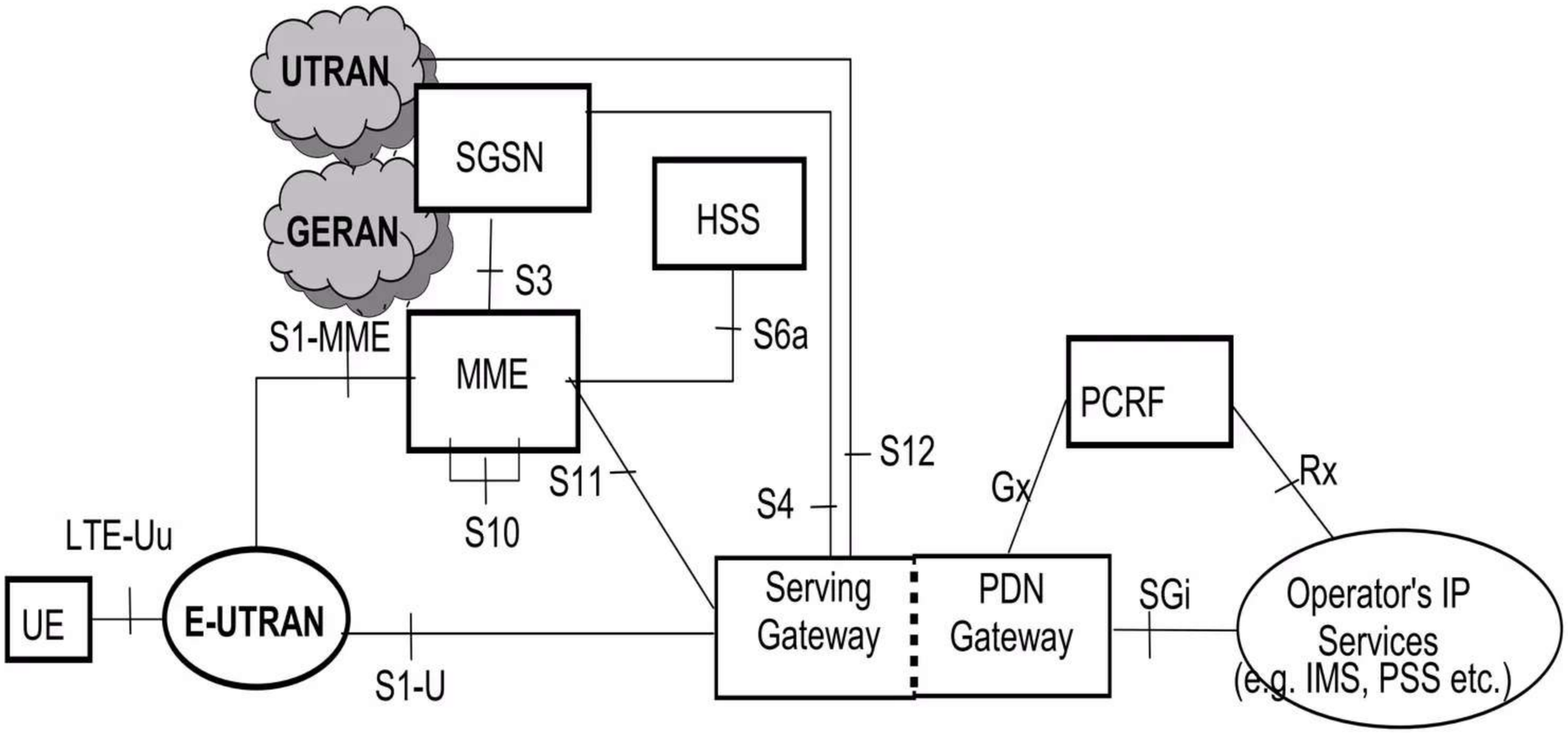
Non-roaming architecture



LTE/EPC Network architecture

Roaming/Non-Roaming Architecture

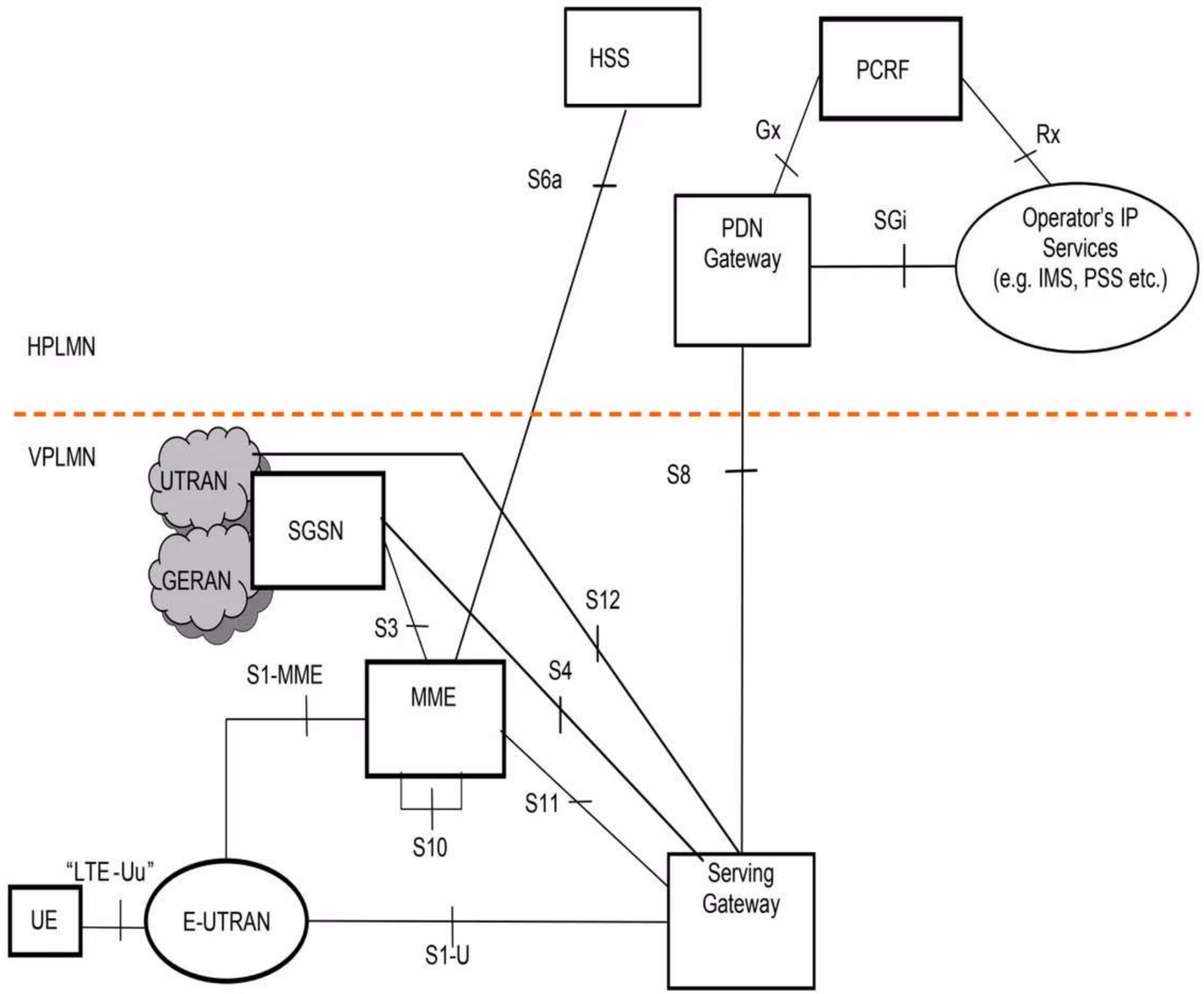
Non-roaming architecture for 3GPP accesses. Single gateway configuration option



LTE/EPC Network architecture

Roaming/Non-Roaming Architecture

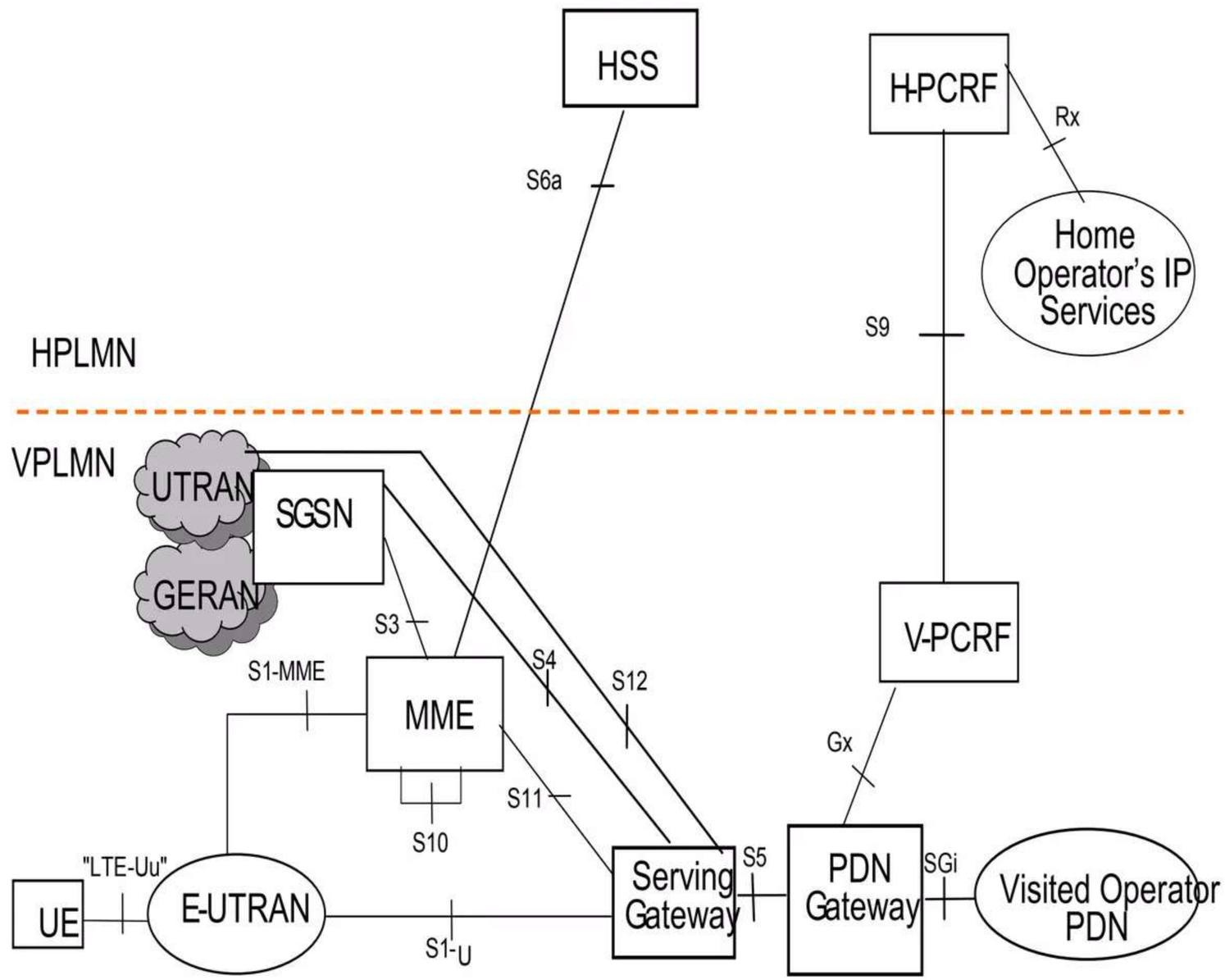
Roaming architecture for 3GPP accesses. Home routed traffic



LTE/EPC Network architecture

Roaming/Non-Roaming Architecture

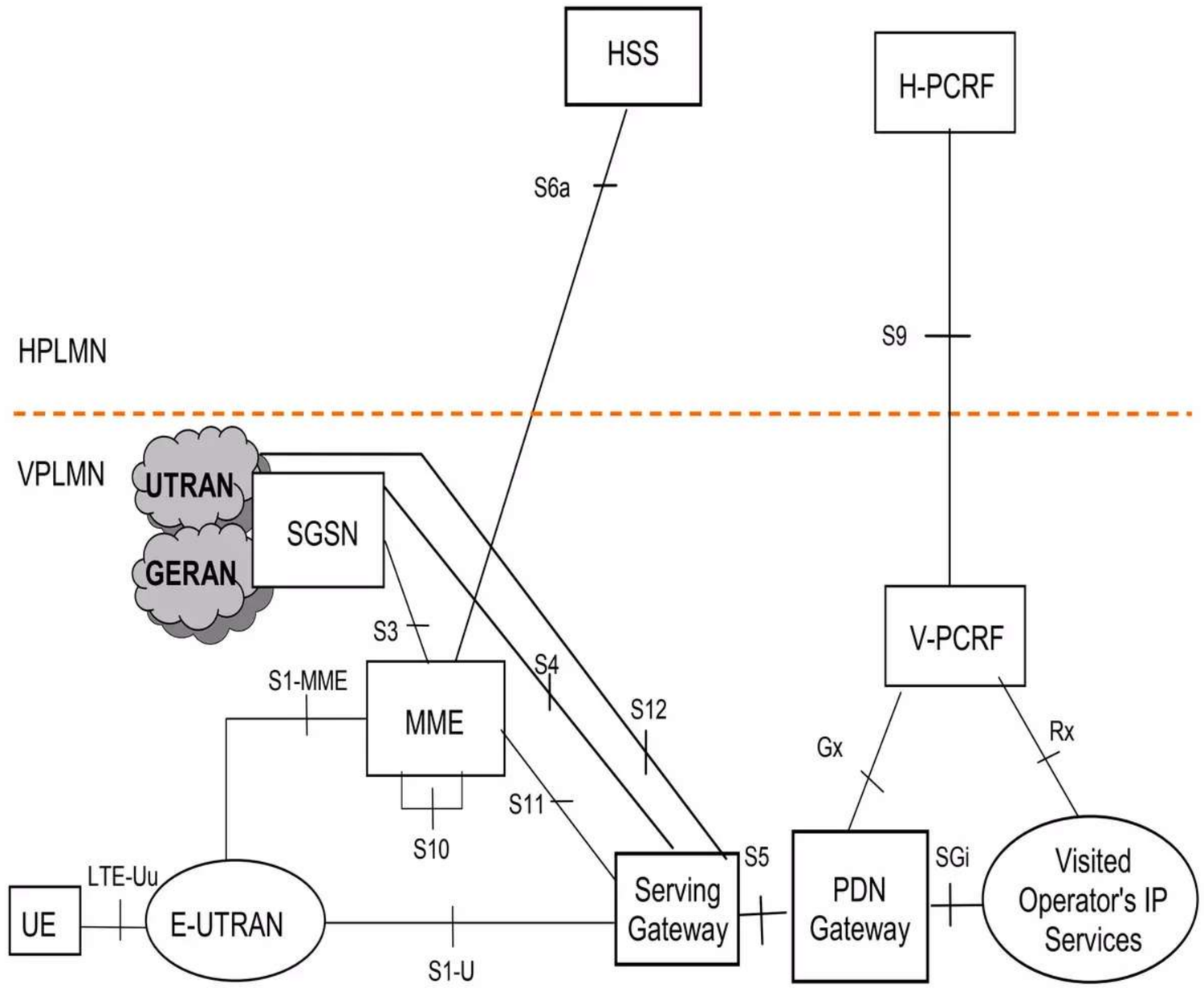
Roaming architecture for local breakout, with home operator's application functions only



LTE/EPC Network architecture

Roaming/Non-Roaming Architecture

Roaming architecture for local breakout, with visited operator's application functions only



LTE/EPC Mobility And Session Management

Module Three

Hussien Mahmoud- PS Core/EPC Consultant

Agenda

- **Mobility and Session Management states**
- UE and Network identifications
- LTE/EPC Bearer Types and QoS
- LTE/EPC Attach Procedure
- LTE/EPC Detach Procedure
- LTE/EPC Bearer Activation Procedure
- LTE/EPC Service Request Procedures
- Tracking Area Update
- LTE/EPC Handover

MM and SM States

Introduction

Analogue between 2G/3G network and LTE networks

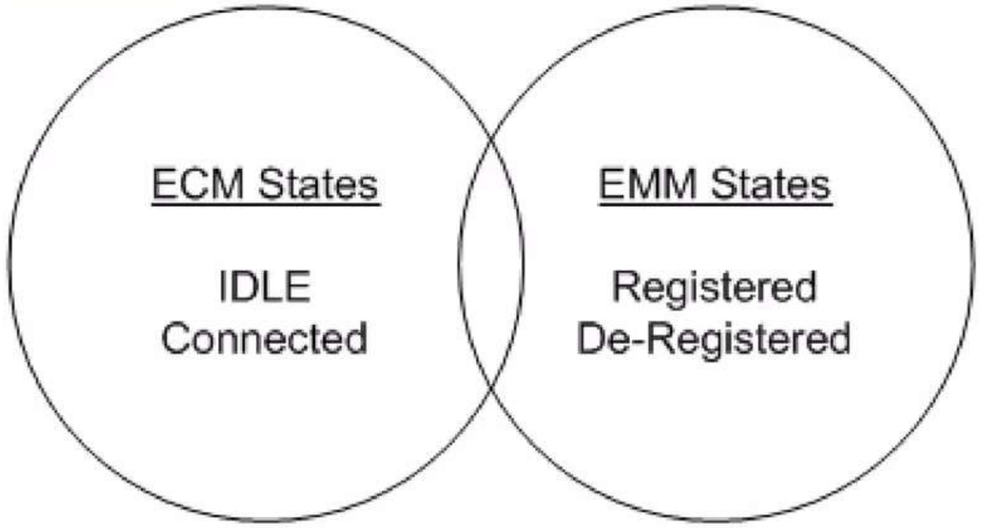
	3G	LTE
Concept	GPRS attached	EMM Registered
	PDP Context	EPC Bearer
	RAB	Radio Bearer+S1 Bearer
	3G	**LTE**
Process	GPRS attach	Attach+Default Bearer
	Primary PDP Context	Default Bearer Activation
	Secondary PDP Context	Dedicated Bearer Activation
	Routing Area Update	Tracking Area Update
	RAB assignment (primary)	Initial Content Setup
	RAB assignment (secondary)	Bearer Setup request

MM and SM States

Introduction

- MM and SM in LTE is serving the same purpose as in the previous 2G/3G networks.
- In LTE we have two states defined for each UE
  - **EPS Mobility Management States (EMM).**
  - **EPS Session Management States (ESM).**

- ESM purpose is to keep track of **the session assignment and data handling**
- EMM purpose is to keep track of **the user location** and to keep the wireless mobility to a high accuracy level.



MM and SM States

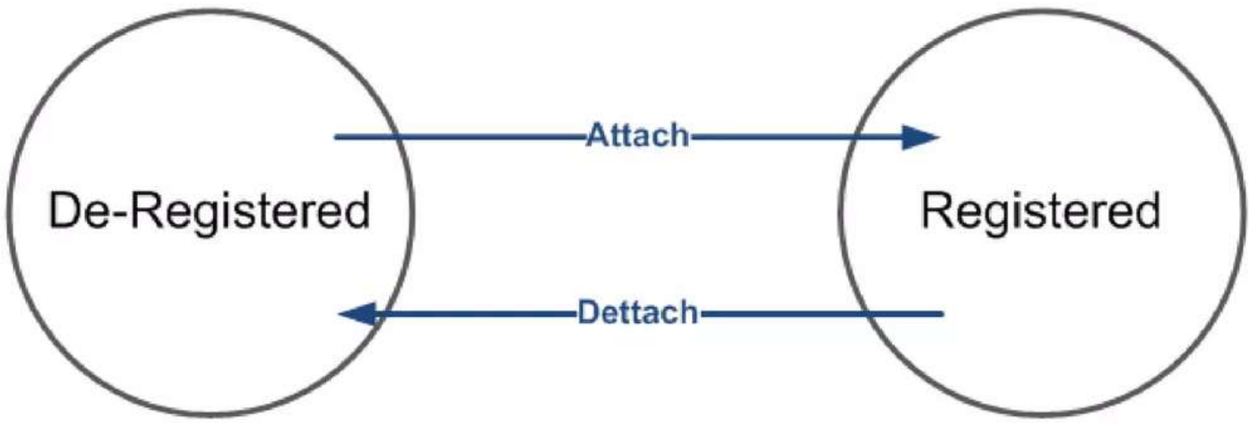
Introduction: EMM States

EMM De-registered

- The MME **doesn't have any information about the UE locat**ion at any level.
- The MME may hold an **old information** about the UE context.
- Attach or TAU would change the status to a Registered EMM state.

EMM Registered

- The MME hold the location information of the UE.
- The **Tracking Area is the min. Location information.**
- The UE would perform all the related EMM procedure such as the TRAU.
- The UE can also request to send data or receive data.



MM and SM States

Introduction: ECM States

ECM IDLE

- There **is no context for the UE** in the UTRAN
- There is **no signaling associated between the UTRAN and EPC**
- The Location is known up to the level of **the Tracking area**
- **Tracking area Updates**

ECM Connected

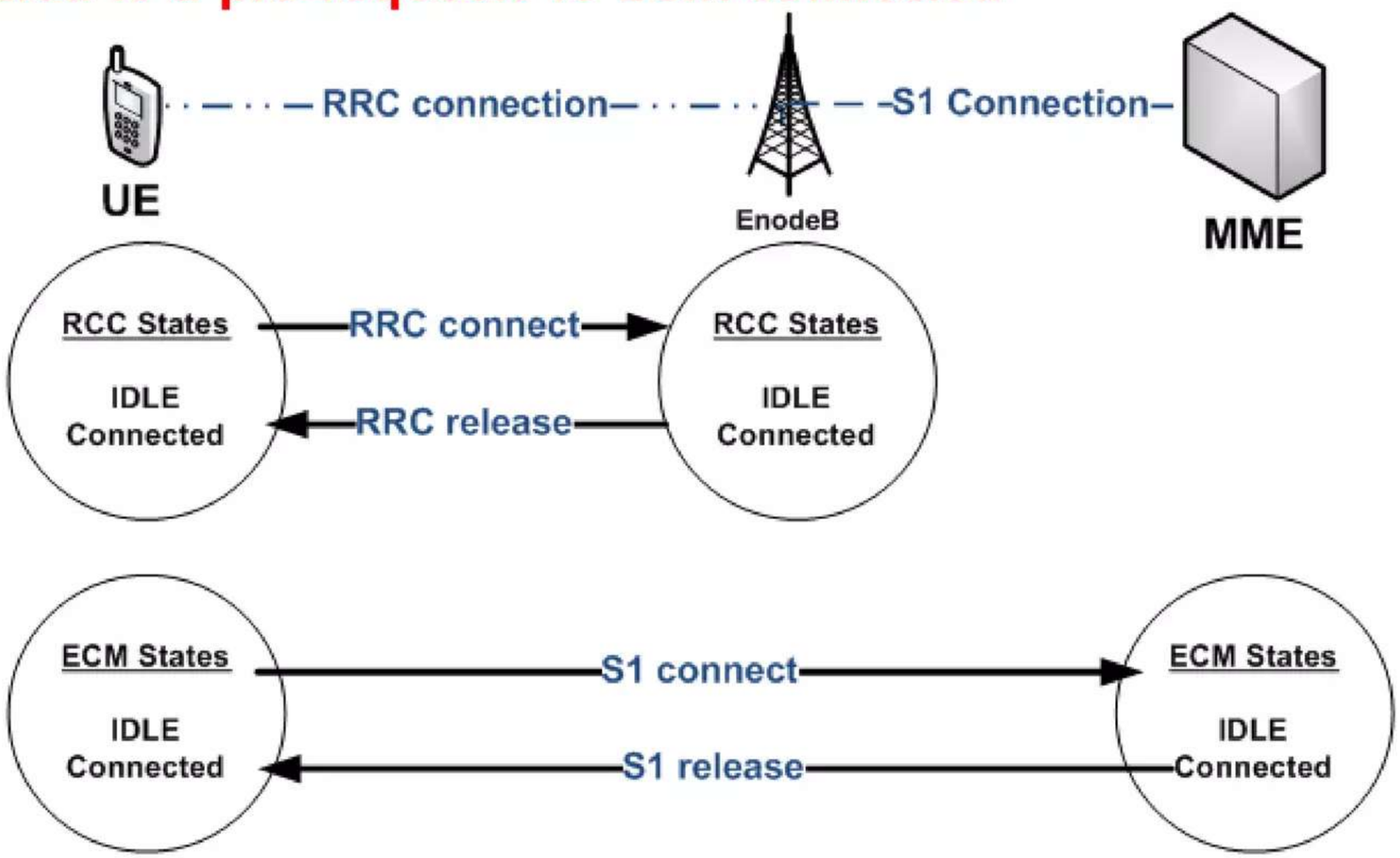
- There is a **valid context for the UE**
- There is a signaling associated in the UTRAN (RRC) and signaling associated in the EPC level (S1 bearer)
- The location is known up to to the **accuracy of cells**
- Cell handover

ECM Connected= RRC Connected + S1 Connection

MM and SM States

Introduction: ECM States

- The UE has two states RRC status and ECM status.
- The E-UTRAN has only RRC status.
- The MME has only ECM status
- **RRC connected is a pre-requests to ECM connected**



MM and SM States

Introduction: RRC States

RRC IDLE

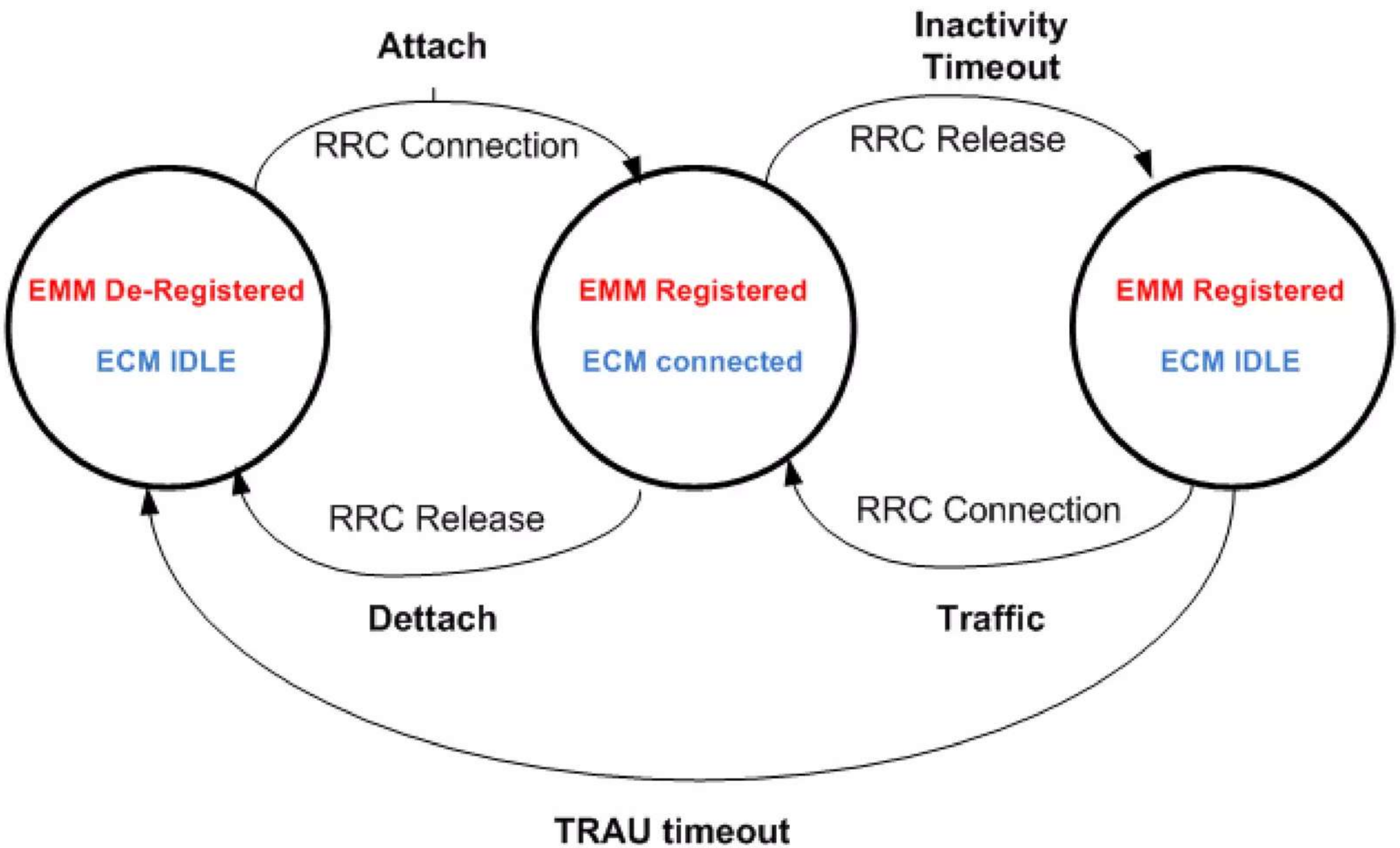
- There is no RRC context stored in the EnodeB
- There is no signaling associated between the EnodeB and UE
- Cell selection and reselection
- **UE is ready for paging**
- UE receives system information

RRC Connected

- There is an RRC context stored in the EnodeB
- There is a signaling associated between the EnodeB and UE
- Cell handover
- **UE can transmit and receive data**
- UE reports neighbor cell measurement

MM and SM States

State Diagram



Agenda

- Mobility and Session Management states
- **UE and Network identifications**
- LTE/EPC Bearer Types and QoS
- LTE/EPC Attach Procedure
- LTE/EPC Detach Procedure
- LTE/EPC Bearer Activation Procedure
- LTE/EPC Service Request Procedures
- Tracking Area Update
- LTE/EPC Handover

UE And Networks Identifiers

Introduction

In LTE we have four main identifications:

IMSI:

International Mobile Subscriber Identity ,used to identify the UE globally each SIM card has a unique IMSI which identifies the user profile **within the Mobile Network**

S-TMSI:

SAE Temporary Mobile Subscriber Identity ,used to identify the UE **temporarily within the Mobile Network**

C-RNTI:

Cell Radio Network Temporary Identity, used to temporarily identify the User **within the Radio Access.**

S1-AP UE ID:

S1 Application Protocol User Equipment Identity, identifies **the S1 control signaling within the Core part.**

UE And Networks Identifiers

IMSI

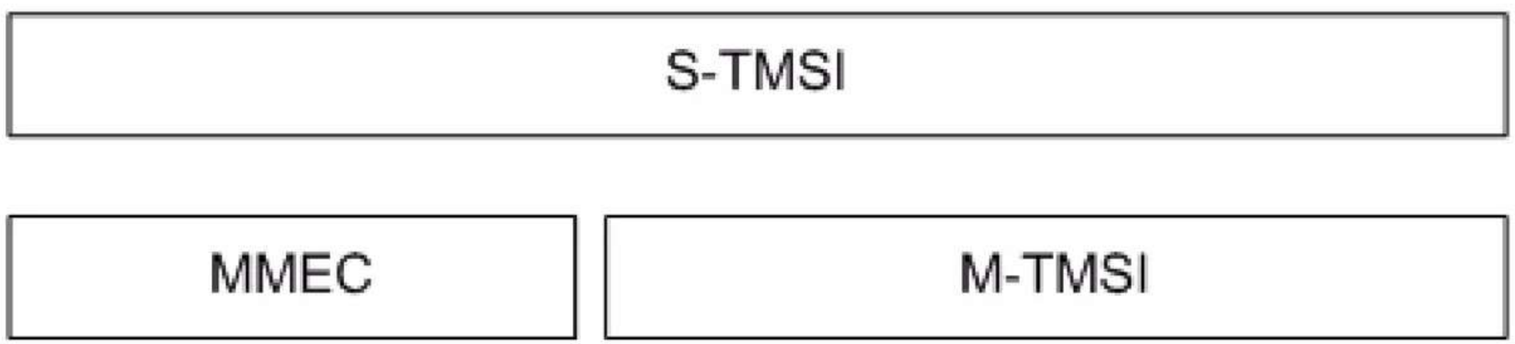
- Uniquely identifies the UE globally within the Mobile Network
- IMSI is the same for 2G/3G/4G Network
- IMSI is composed of MCC+MNC+MSIN:
  - MCC: mobile country code
  - MNC: mobile network code
  - MSIN: mobile subscriber identification number
- MME identifies the UE using the IMSI

MCC	MNC	MSIN
3 digits	2 digits	10 digits

UE And Networks Identifiers

S-TMSI

- S stands for SAE , SAE Temporary Mobile Subscriber Identity
- S-TMSI is allocated temporarily by the MME
- S-TMSI is used instead of the IMSI for security reasons
- MME ID identifies the MME incase multiple MME connectivity
- S-TMSI is associated with the IMSI within the MME
- S-TMSI is a 32 Bit size
- Used for paging and Service Request



UE And Networks Identifiers

C-RNTI

- Cell Radio Network Temporary Identity
- C-RNTI is assigned by the enodeB when the RRC is connected
- Temporary identification used for radio resource management
- The RNTI is signaled in the MAC layer
- The C-RNTI is a 16-bit numeric value.

UE And Networks Identifiers

S1-AP

- S1-AP identifies the Signaling messages transferred between the MME and EnodeB.
- Each of The Enode B and MME assigns a separate S1-AP ID

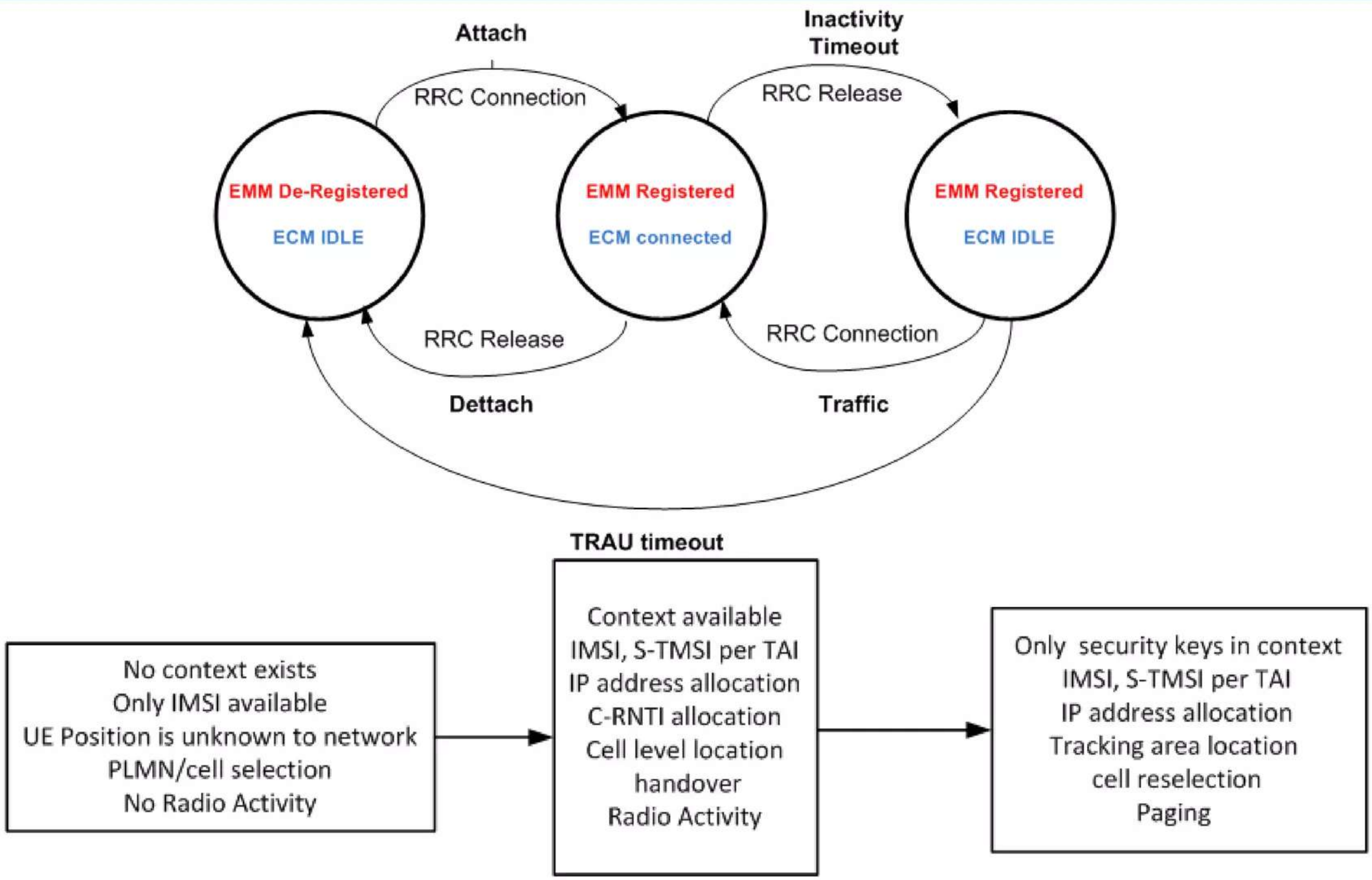
  eNB S1-AP UE ID

  MME S1-AP IE ID
- This two ID's is to control the messages between MME and Enode B on the S1 interface.

```
◢ S1AP-PDU: initiatingMessage (0)
  ◢ initiatingMessage
      procedureCode: id-initialUEMessage (12)
      criticality: ignore (1)
    ◢ value
      ◢ InitialUEMessage
        ◢ protocolIEs: 5 items
          ◢ Item 0: id-eNB-UE-S1AP-ID
            ◢ ProtocolIE-Field
                id: id-eNB-UE-S1AP-ID (8)
                criticality: reject (0)
              ◢ value
                  ENB-UE-S1AP-ID: 264
```

UE And Networks Identifiers

State Diagram



UE And Networks Identifiers

GUTI

- Globally Unique Temporary Identity (GUTI)
  - the GUTI is allocated to the UE by the MME
  - The purpose of the GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the Evolved Packet System (EPS).
  - It can be used by the network and the UE to establish the UE's identity during signalling between them in the EPS.

```
◢ Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Attach request (0x41)
    0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
    .111 .... = NAS key set identifier: No key is available (7)
    .... 0... = Spare bit(s): 0x00
    .... .001 = EPS attach type: EPS attach (1)
  ▷ EPS mobile identity
  ▷ UE network capability
  ▷ ESM message container
  ▷ Tracking area identity - Last visited registered TAI
```

```
◢ EPS mobile identity
    Length: 11
    .... 0... = odd/even indic: 0
    .... .110 = Type of identity: GUTI (6)
    Mobile Country Code (MCC): [redacted]
    Mobile Network Code (MNC): [redacted]
    MME Group ID: 33333
    MME Code: 1
    M-TMSI: 0xe0000009
```

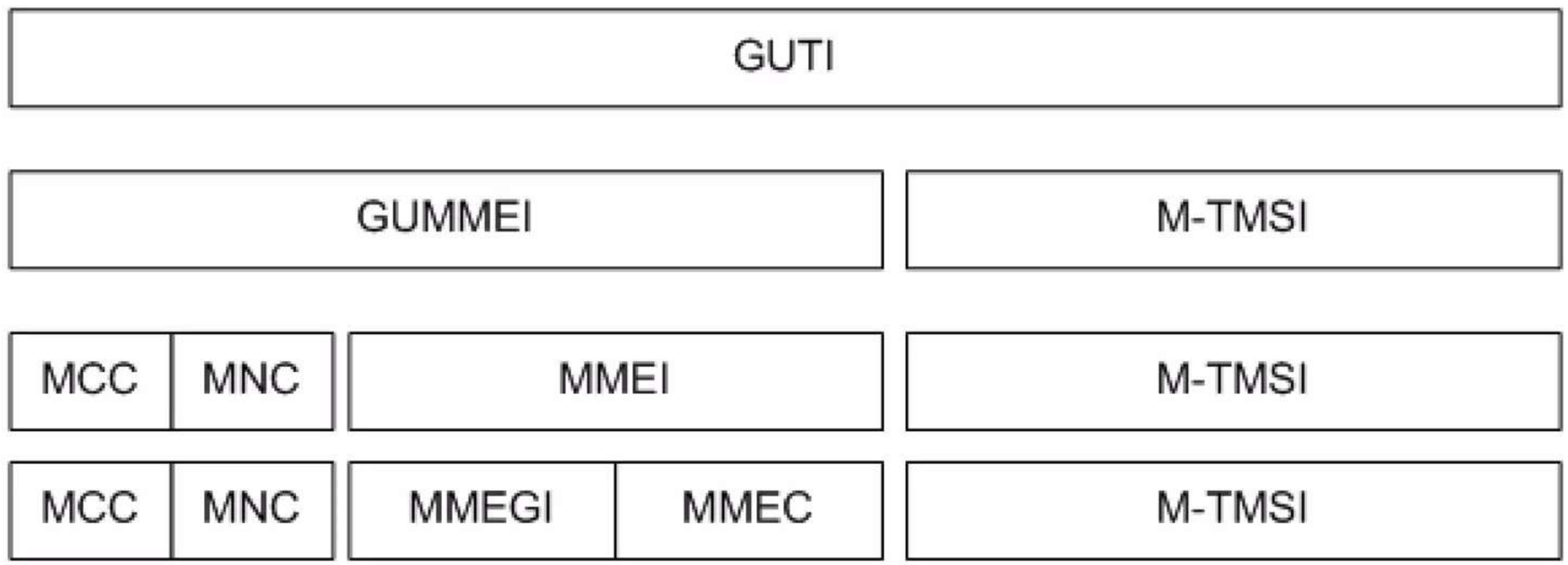
UE And Networks Identifiers

GUTI

The GUTI has two main components:

-one that uniquely identifies the MME which allocated the GUTI.

-one that uniquely identifies the UE within the MME that allocated the GUTI.



UE And Networks Identifiers

ECGI

E-UTRAN Cell Global Identifier (ECGI)

An Identifier used to identify cells globally. The ECGI is constructed from the PLMN identity the cell belongs to and the Cell Identity (CI) of the cell.

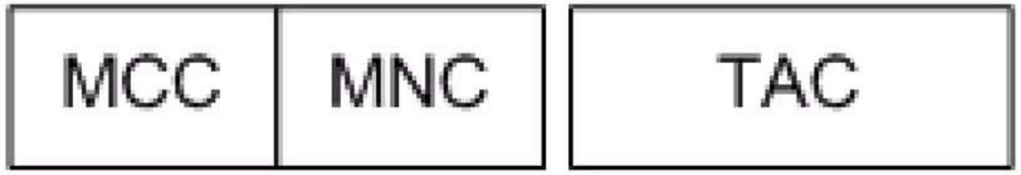
```
Item 3: id-EUTRAN-CGI
  ProtocolIE-Field
      id: id-EUTRAN-CGI
      criticality: ignore (1)
    value
      EUTRAN-CGI
          pLMNidentity:
          Mobile Country Code (MCC)
          Mobile Network Code (MNC)
          cell-ID:        [bit length 28, 4 LSB pad bits, 0000 0000  0001 1010  0111 0000  0001 .... decimal value 108289]
```

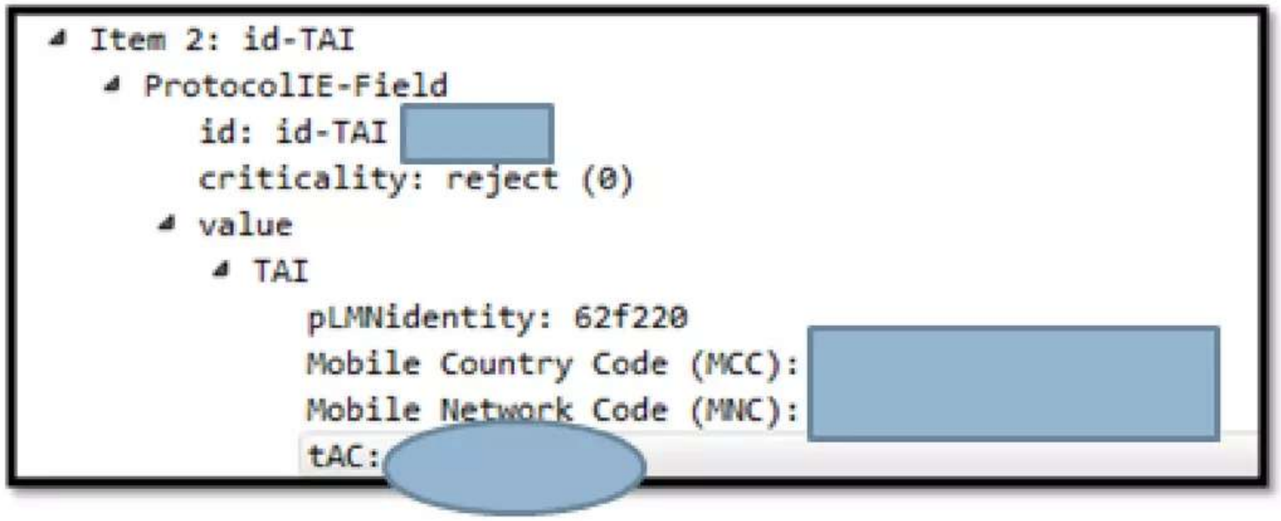
UE And Networks Identifiers

TAI

Tracking Area Identity (TAI)

The Identifier is used to identify tracking areas. The TAI is constructed from the PLMN identity the tracking area belongs to and the TAC (Tracking Area Code) of the Tracking Area.





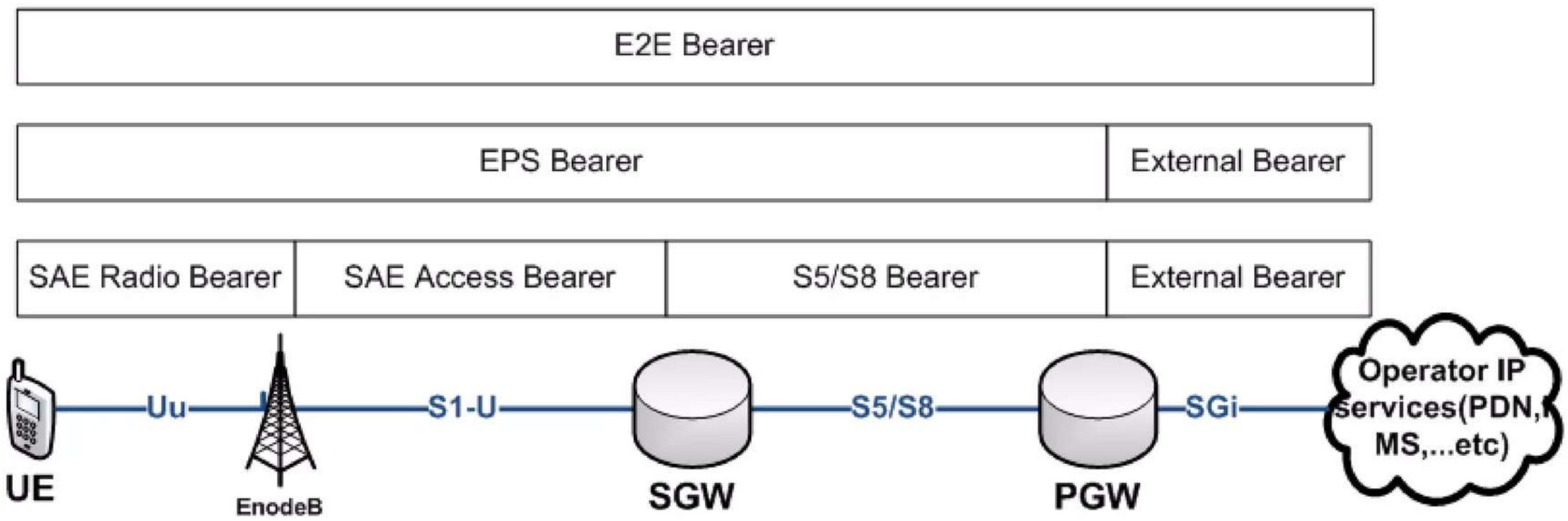
Agenda

- Mobility and Session Management states
- UE and Network identifications
- **LTE/EPC Bearer Types and QoS**
- LTE/EPC Attach Procedure
- LTE/EPC Detach Procedure
- LTE/EPC Bearer Activation Procedure
- LTE/EPC Service Request Procedures
- Tracking Area Update
- LTE/EPC Handover

LTE/EPC Bearer Types and QoS

E2E Bearer

- Bearers identifies the User plane across the LTE/EPC network (E2E Bearer)
- Each user is identified by a certain Bearer and QoS assigned
- Bearers (Radio bearers , SAE Access Bearer , S5/S8 bearer)
- The SAE Bearer is associated with QoS



LTE/EPC Bearer Types and QoS

E2E Bearer

Radio bearers

The first bearer Between UE and eNB.

The Radio bearers is mapped to the air interface physical resources.

SAE Access Bearer

The second bearer Between eNB and SAE GW.

Implemented using GTP tunnel version 1

MME exchange signaling with EnodeB to create Bearer.

S5/S8 bearer

The third bearer Between the P-GW to S-GW.

This is usually a GTP or MIP tunnel between S –GW and P-GW.

External bearer

The fourth bearer Between the P-GW to the application layer.

LTE/EPC Bearer Types and QoS

E2E Bearer

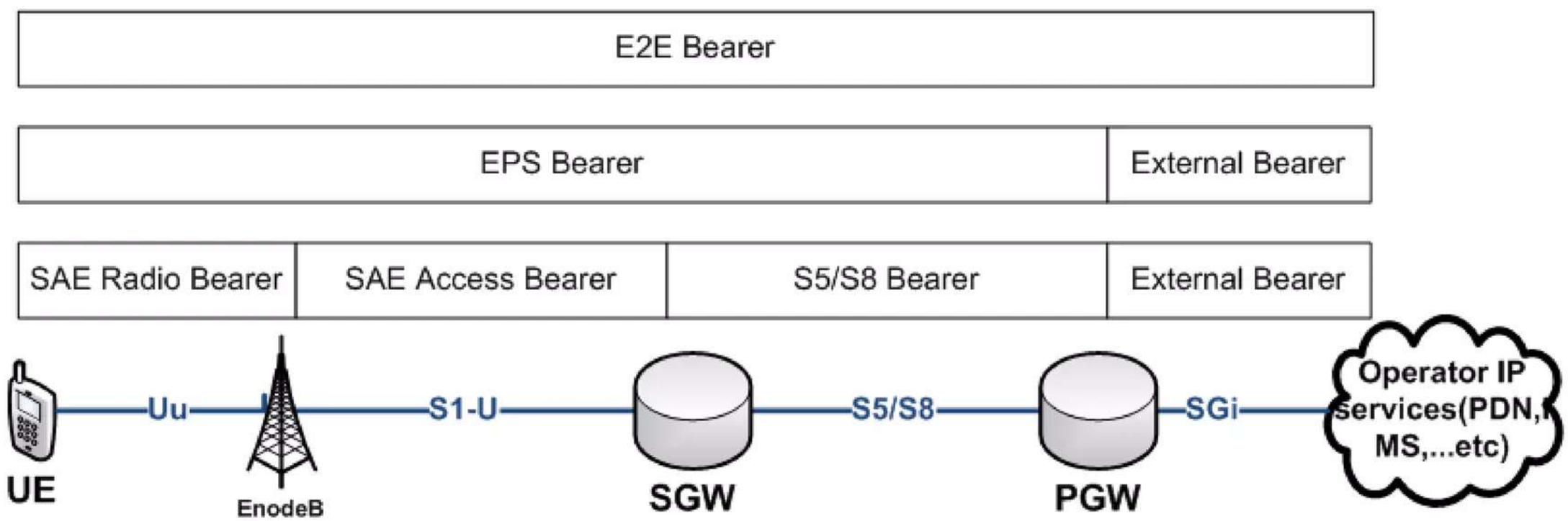
Every Service on LTE requires a certain QoS and certain level of efficiency i.e. priority , delay , jitter…etc.

Application services could be (browsing, downloading , streaming ,voice….etc)

Each traffic flow inside the LTE network would achieve a certain QoS based on the service request.

All data transmitted/received within a bearer, must have the same QoS assigned to that Bearer.

A UE could have multiple services with multiple bearers assigned



LTE/EPC Bearer Types and QoS

Bearer Definition

1-Default Bearer

Allocated during the Initial attach of the system

Non-GBR (Non Guaranteed Bit Rate) is allocated

2-Dedicated Bearer

Allocated on demand by external Services

GBR is allocated (Guaranteed Bit Rate)

GBR bearers is always reserve a dedicated resources ,This is required for services with low delay and jitter (Voice).

GBR bearer will usually also limit the resources for some services based on the assigned bandwidth.

MBR: the maximum bit rate assigned for GBR Bearers.

AMBR: the total maximum bit rate (MBR) for all non-GBR bearers .

LTE/EPC Bearer Types and QoS

Bearer QoS

Traffic Flow Template (TFT)

The TFT is a kind of a filter that specifies each bearer with the associated traffic which data traffic to which bearer.

The filter is applied on Uplink and downlink traffic with a certain criteria (IP address , port, protocol ,…etc).

Traffic flow template is always associated with dedicated bearer and while default bearer may or may not have TFT.

QoS Class Identifier (QCI)

An integer number assigned to each bearer to identify the QoS category assigned to it.

These labels can be transferred to IP header tags on S1-U,S5/S8 to implement IP QoS.

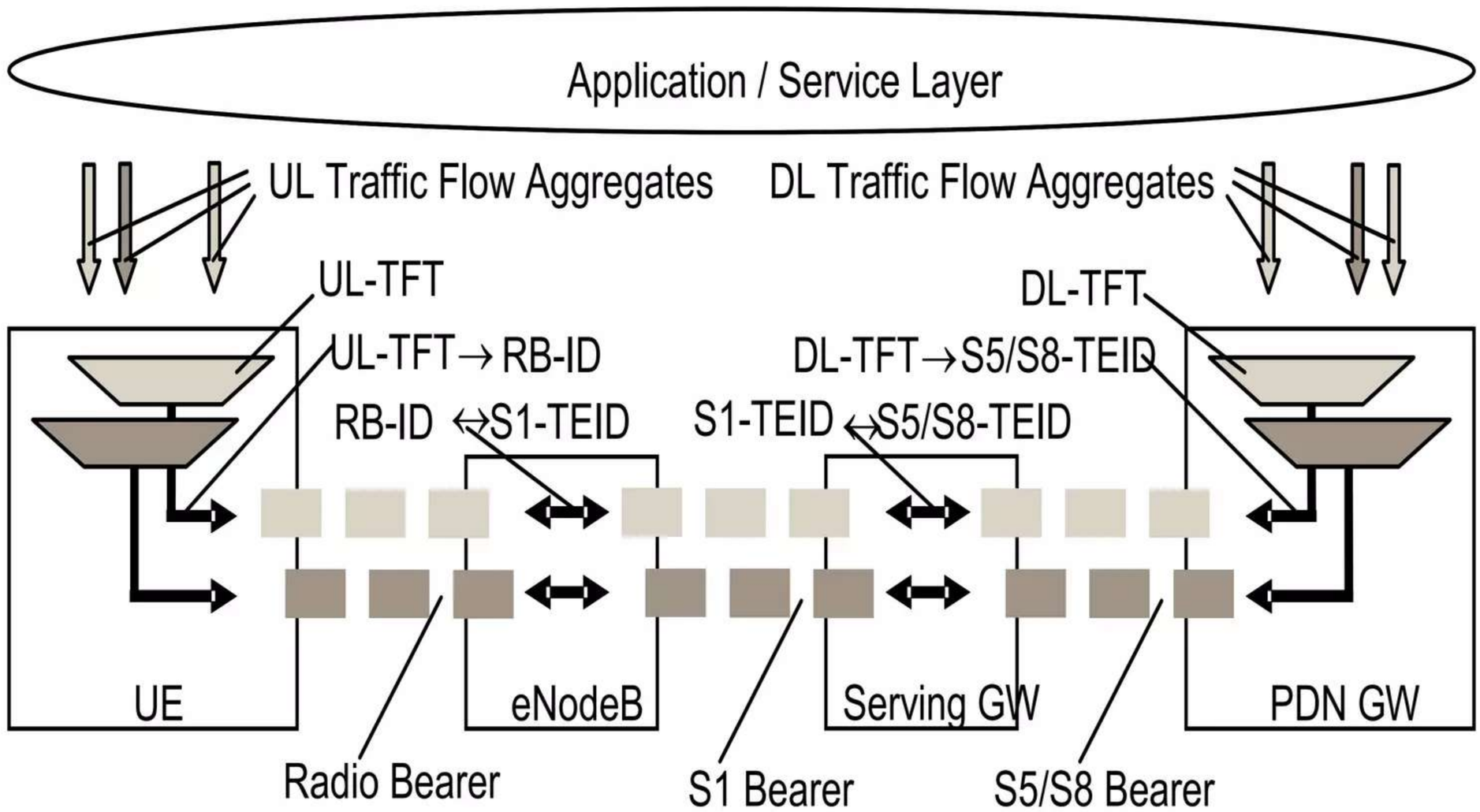
Allocation/Retention Priority (ARP)

This parameter identifies the Resource allocation priority during the SAE bearer setup.

LTE/EPC Bearer Types and QoS

Bearer QoS

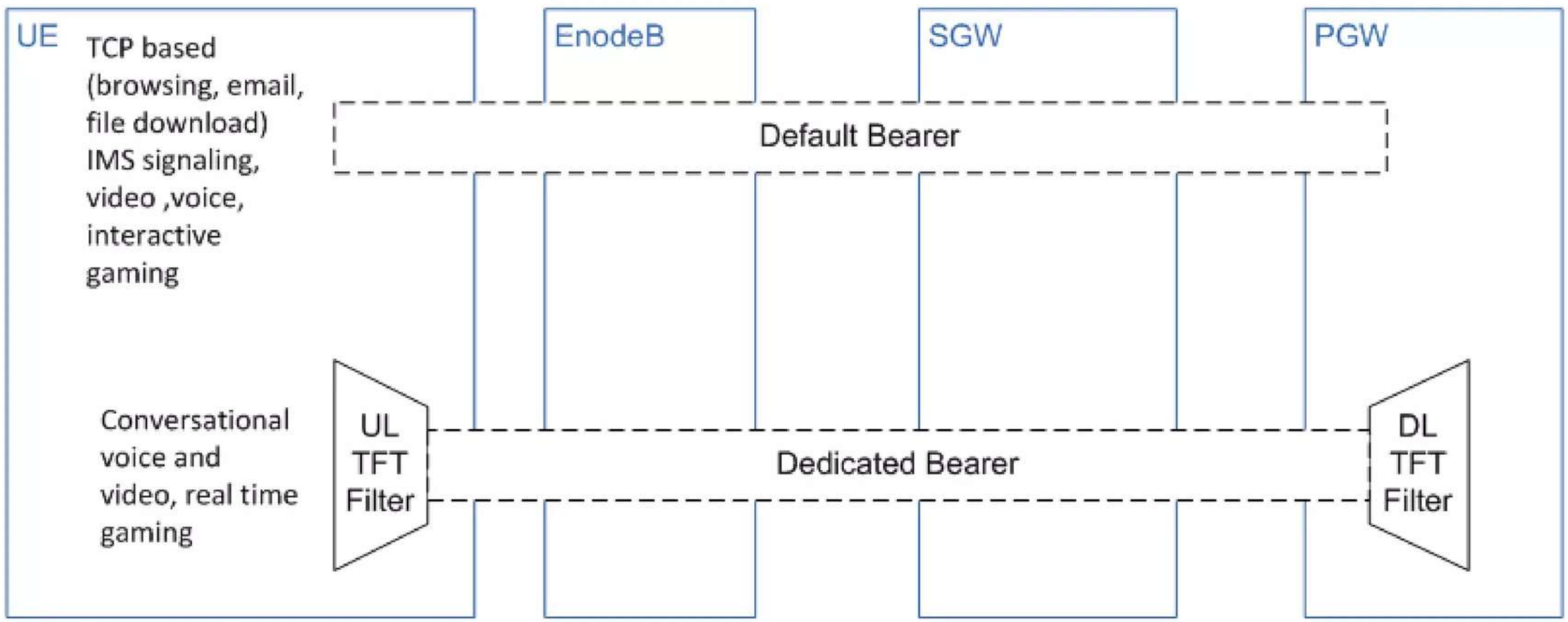
The EPS bearer with GTP-based S5/S8



LTE/EPC Bearer Types and QoS

Bearer QoS

Each SAE bearer Quality of service would include QCI, ARP ,MBR,GB, TFT and AMBR.



L-EBI: It stands for Linked EPS bearer ID

L-EBI tells Dedicated bearer which default bearer it is attached to

LTE/EPC Bearer Types and QoS

Bearer QoS

NAS PDU, Activate Dedicated Bearer Request (E-RAB Request)

```
Non-Access-Stratum (NAS)PDU
  0010 .... = Security header type: Integrity protected and ciphered (2)
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
  Message authentication code: 0x70510843
  Sequence number: 3
  0110 .... = EPS bearer identity: EPS bearer identity value 6 (6)
  .... 0010 = Protocol discriminator: EPS session management messages (0x02)
  Procedure transaction identity: 0
  NAS EPS session management messages: Activate dedicated EPS bearer context reques
  0000 .... = Spare half octet: 0
  .... 0101 = Linked EPS bearer identity: EPS bearer identity value 5 (5)
⊟ EPS quality of service
    Length: 5
    Quality of Service Class Identifier (QCI): QCI 1 (1)
    Maximum bit rate for uplink: 8640 kbps
    Maximum bit rate for downlink: 8640 kbps
    Guaranteed bit rate for uplink: 0 kbps
    Guaranteed bit rate for downlink: 0 kbps
⊟ Traffic Flow Template
    Length: 18
    001. .... = TFT operation code: Create new TFT (1)
    ...0 .... = E bit: Parameters list is not included
    .... 0001 = Number of packet filters: 1
  ⊟ Packet filter 0
⊟ Linked TI - Transaction identifier
⊟ Quality Of Service - Negotiated QoS
⊟ LLC Service Access Point Identifier - Negotiated LLC SAPI
⊟ Radio Priority
⊟ Packet Flow Identifier - Best Effort
⊟ Protocol Configuration Options
    Element ID: 0x27
    Length: 20
    [Link direction: Network to MS (1)]
    1... .... = Extension: True
    Configuration Protocol: PPP for use with IP PDP type or IP PDN type (0)
  ⊟ Protocol or Container ID: Internet Protocol Control Protocol (0x8021)
```

```
⊟ Packet filter 0
    00.. .... = Spare bit(s): 0
    ..11 .... = Packet filter direction: Bidirectional (3)
    .... 0110 = Packet filter identifier: 7 (6)
    Packet evaluation precedence: 0x0a (10)
    Packet filter length: 0x0e (14)
  ⊟ Packet filter component type identifier: Protocol identifier/Next header type (48)
      Protocol/header: UDP (0x11)
  ⊟ Packet filter component type identifier: IPv4 remote address type (16)
      IPv4 address [redacted]
      IPv4 address mask: 255.255.255.255 (255.255.255.255)
  ⊟ Packet filter component type identifier: Single local port type (64)
      Port [redacted]
```

LTE/EPC Bearer Types

Bearer QoS

–QoS Class Identifier(QCI)

•Value for scheduling and Identifies a particular service or class of services

–Allocation and Retention Priority(ARP)

•Used to accept/modify/drop bearers in case of resource limitation

–Guaranteed Bit Rate(GBR)

•Only for GBR-bearers

- **Maximum Bit Rate (MBR).**

The **MBR** limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function).

LTE/EPC Bearer Types and QoS

Bearer QoS

Table 6.1.7: Standardized QCI characteristics

QCI	Resource Type	Priority	Packet Delay Budget (NOTE 1)	Packet Error Loss Rate (NOTE 2)	Example Services
1 (NOTE 3)	GBR	2	100 ms	10^{-2}	Conversational Voice
2 (NOTE 3)		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3 (NOTE 3)		3	50 ms	10^{-3}	Real Time Gaming
4 (NOTE 3)		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
5 (NOTE 3)	Non-GBR	1	100 ms	10^{-6}	IMS Signalling
6 (NOTE 4)		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7 (NOTE 3)		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8 (NOTE 5)		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9 (NOTE 6)		9			

LTE/EPC Bearer Types and QoS

Bearer QoS

- The **ARP** shall contain information about the priority level (scalar), the pre-emption capability (flag) and the pre-emption vulnerability (flag).
- The pre-emption capability information of the ARP defines whether a bearer with a lower ARP priority level should be dropped to free up the required resources.
- The pre-emption vulnerability information of the ARP defines whether a bearer is applicable for such dropping by a pre-emption capable bearer with a higher ARP priority value.

Your request is accepted, and because you have a higher priority you can pre-empt

Agenda

- Mobility and Session Management states
- UE and Network identifications
- LTE/EPC Bearer Types and QoS
- **LTE/EPC Attach Procedure**
- LTE/EPC Detach Procedure
- LTE/EPC Bearer Activation Procedure
- LTE/EPC Service Request Procedures
- Tracking Area Update
- LTE/EPC Handover

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

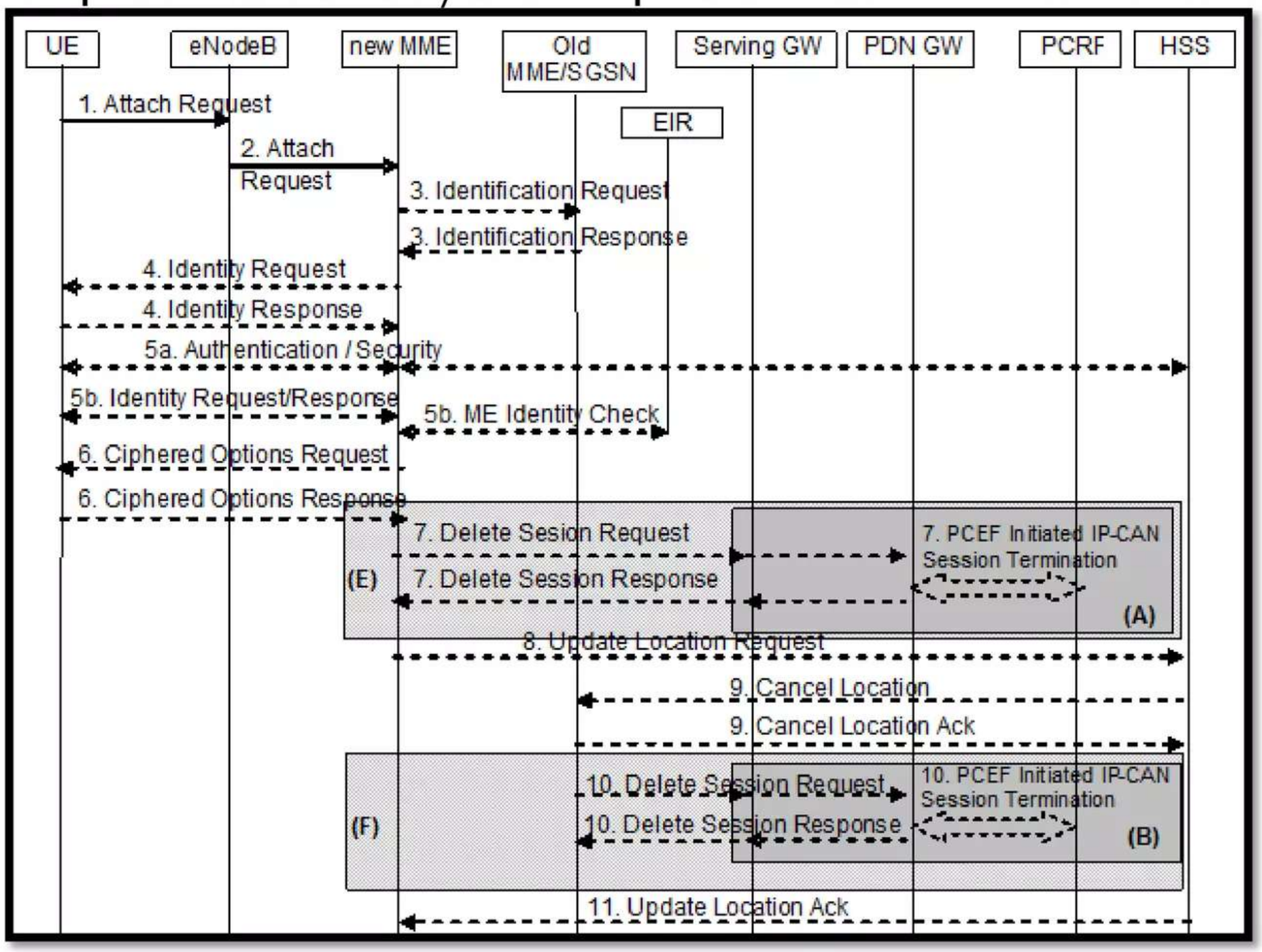
The attach procedure in LTE/SAE is quite similar to the GPRS attach in 2G/3G

1. The UE sends the *ATTACH REQUEST* message (NAS) including **old S-TMSI, old TAI** and information about the allocated PDN (IP) addresses.
2. The eNB selects an available MME and forwards the message to it.
3. The first task of the MME is to identify and authenticate the subscriber. **Thus it contacts the old MME (identified via S-TMSI/TAI)** with *IDENTIFICATION REQUEST* (GTP-C).
4. **Authentication vectors** for the subscriber. (Flowchart shows direct contact with HSS). The authentication mechanism is the same as in 3G.
5. the new MME can begin to update the HSS and download the subscription data from there
6. During this process the HSS will also force the old MME to clear the stored data about the subscriber using the Diameter operation *CANCEL LOCATION*.

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

The attach procedure in LTE/SAE is quite similar to the GPRS attach in 2G/3G



LTE/EPC Bearer Types

LTE/EPC Attach Procedure

The attach procedure in LTE/SAE is quite similar to the GPRS attach in 2G/3G

1. Based on the subscription data the new MME must decide whether a **default bearer has to be created or not.**
2. The default access point name (default APN) assists the MME in selection of an appropriate SAE GW. To this serving gateway the ***CREATE DEFAULT BEARER REQUEST*** message (GTP-C) is sent to.
3. The SAE GW will now create the S5/S8 tunnel. This is done with the same message, but sent to the PDN GW.
4. When the EPC resources for the default bearer are prepared, the new MME can give the ***ATTACH ACCEPT*** message to eNB.
5. The S1-AP message which will contain this one will hold the tunnel **endpoint identifier allocated by the SAE GW for S1 interface.**

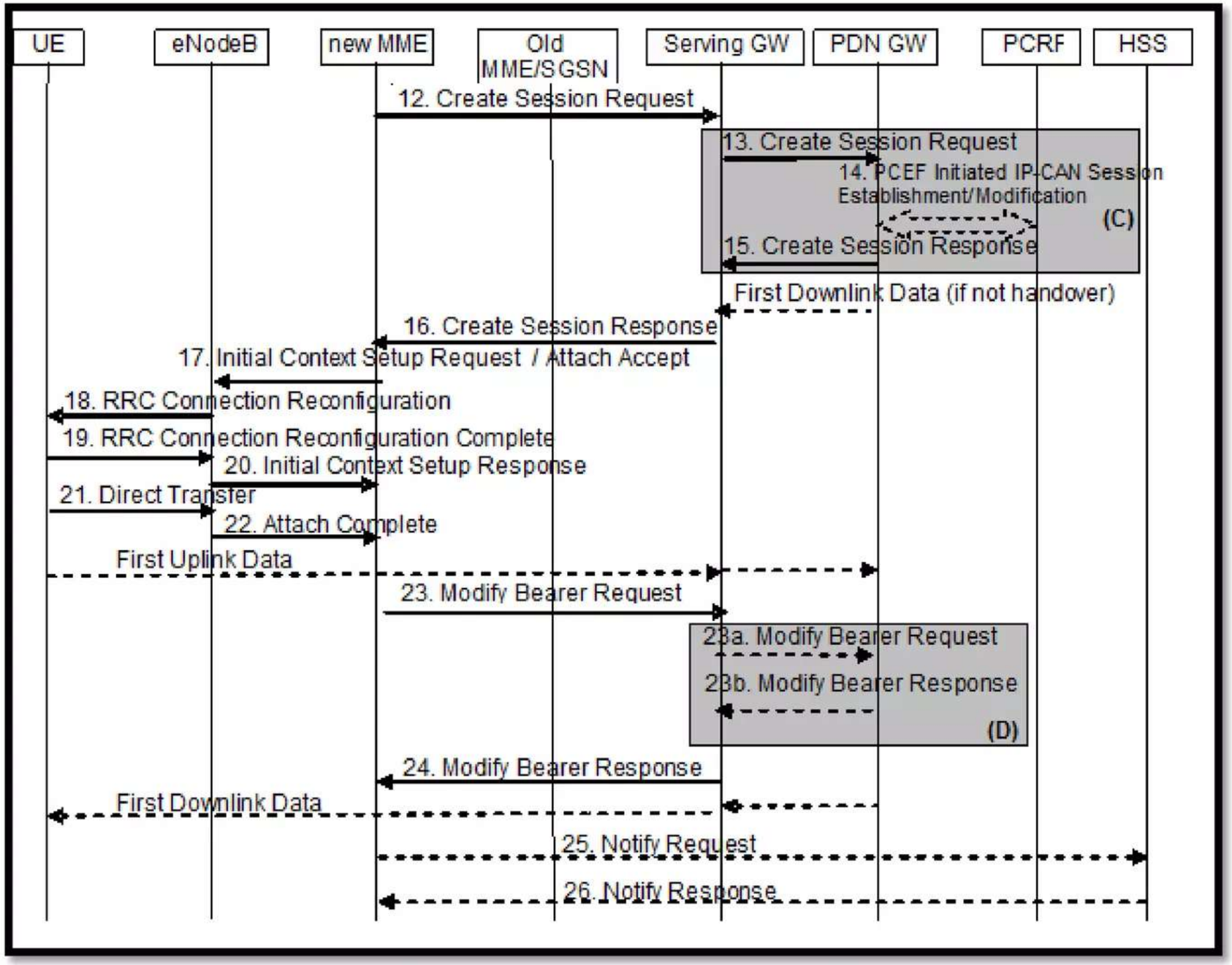
LTE/EPC Bearer Types

LTE/EPC Attach Procedure

7. The eNB creates **the radio bearer for the default SAE bearer** and returns *ATTACH COMPLETE* to the MME.
8. The S1-AP message this one is in will hold the **TEID allocated by the eNB** for S1 interface.
9. **Via an *UPDATE BEARER* procedure the MME will give this parameter to the SAE GW.**
10. Now the default SAE bearer is complete and the UE is in state EMM_REGISTERED and ECM_CONNECTED.

LTE/EPC Bearer Types

LTE/EPC Attach Procedure



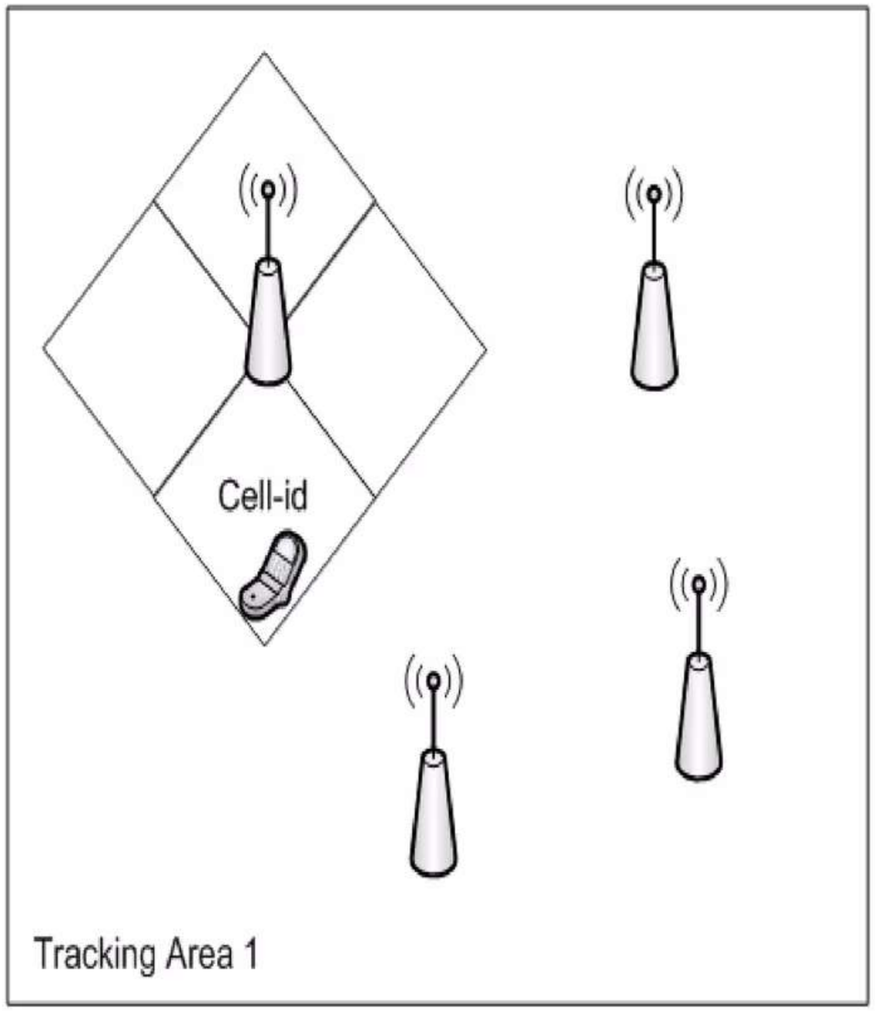
LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Initial Attach Request, **Initial UE message**

RRC establishment with cause (**mo-signaling**)

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-initialUEMessage (12)
      criticality: ignore (1)
    ⊟ value
      ⊟ InitialUEMessage
        ⊟ protocolIEs: 5 items
          ⊞ Item 0: id-eNB-UE-S1AP-ID
          ⊞ Item 1: id-NAS-PDU
          ⊞ Item 2: id-TAI
          ⊞ Item 3: id-EUTRAN-CGI
          ⊟ Item 4: id-RRC-Establishment-Cause
            ⊟ ProtocolIE-Field
                id: id-RRC-Establishment-Cause (134)
                criticality: ignore (1)
              ⊟ value
                RRC-Establishment-Cause: mo-Signalling (3)
```



Identities in the First attach message:

- eNB-UE-S1AP-ID
- TAI (MNC,MCC,TAC)
- EUTRAN-CGI (PLMN id, MCC, MNC, Cell-id)

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Initial Attach Request, the NAS PDU (**EPS attach request**)

```
⊟ Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Attach request (0x41)
    0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
    .111 .... = NAS key set identifier: No key is available (7)
    .... 0... = Spare bit(s): 0x00
    .... .001 = EPS attach type: EPS attach (1)
  ⊞ EPS mobile identity
  ⊞ UE network capability
  ⊞ ESM message container
  ⊞ DRX Parameter
  ⊞ MS Network Capability
```

Identities of the NAS PDU:

- EPS Mobility identity (IMSI)

Capabilities:

- UE Network Capability (integrity algorithm supported, EEA,EIA,UEA,UCS,UIA, etc)
- MS Network Capability (SRVCC,I SR, inter-RAT HO, Encryption Algorithm GEA,LCS, etc)
- DRX Parameters (Timers, Cycle Length, etc.)
- ESM Container (EPS Session Management)

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Initial Attach Request, ESM Container (**EPS Session Management**),PDN Connectivity Request

```
⊟ ESM message container
    Length: 101
  ⊟ ESM message container contents: 0201d011d1275e80c223230101002310eca390003edbf917...
      0000 .... = EPS bearer identity: No EPS bearer identity assigned (0)
      .... 0010 = Protocol discriminator: EPS session management messages (0x02)
      Procedure transaction identity: 1
      NAS EPS session management messages: PDN connectivity request (0xd0)
      0001 .... = PDN type: IPv4 (1)
      .... 0001 = Request type: initial request (1)
    ⊟ ESM information transfer flag
      1101 .... = Element ID: 0xd-
      .... 000. = Spare bit(s): 0x00
      .... ...1 = EIT (ESM information transfer): Security protected ESM information transfer required
  ⊟ Protocol Configuration Options
      Element ID: 0x27
      Length: 94
      [Link direction: MS to network (0)]
      1... .... = Extension: True
      Configuration Protocol: PPP for use with IP PDP type or IP PDN type (0)
    ⊞ Protocol or Container ID: Challenge Handshake Authentication Protocol (0xc223)
    ⊞ Protocol or Container ID: Challenge Handshake Authentication Protocol (0xc223)
    ⊞ Protocol or Container ID: Internet Protocol Control Protocol (0x8021)
```

Protocol Configuration Options:

- DNS IP's
- Authentication Challenges

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Initial Attach Request, ESM Container (**EPS Session Management**),PDN Connectivity Request

Security ESM information transfer required → for security Reasons (No APN information)

```
◢ ESM message container contents: 0201d011d1275e80c223230101002310eca390003edbf917...
    0000 .... = EPS bearer identity: No EPS bearer identity assigned (0)
    .... 0010 = Protocol discriminator: EPS session management messages (0x02)
    Procedure transaction identity: 1
    NAS EPS session management messages: PDN connectivity request (0xd0)
    0001 .... = PDN type: IPv4 (1)
    .... 0001 = Request type: initial request (1)
  ◢ ESM information transfer flag
      1101 .... = Element ID: 0xd-
      .... 000. = Spare bit(s): 0x00
      .... ...1 = EIT (ESM information transfer): Security protected ESM information transfer required
```

Will be communicated after Authentication: ESM information Request/ Reply

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Authentication request from the MME to the UE

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-downlinkNASTransport (11)
      criticality: ignore (1)
    ⊟ value
      ⊟ DownlinkNASTransport
        ⊟ protocolIEs: 3 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
```

```
⊟ Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Authentication request (0x52)
    0000 .... = Spare half octet: 0
    .... 0... = Type of security context flag (TSC): Native security context (for KSIasme)
    .... .000 = NAS key set identifier:  (0) ASME
  ⊟ Authentication Parameter RAND - EPS challenge
      RAND value: [redacted]
  ⊟ Authentication Parameter AUTN (UMTS and EPS authentication challenge) - EPS challenge
      Length: 16
    ⊟ AUTN v[redacted]
        SQN [redacted]
        AMF: [redacted]
        MAC: [redacted]
```

Identities in the AIR:

- eNB-UE-S1AP-ID
- MME-UE-S1AP-ID

Authentication Parameters:

- RAND
- SQN
- AMF
- MAC

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Authentication Reply from the UE to the MME

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-uplinkNASTransport (13)
      criticality: ignore (1)
    ⊟ value
      ⊟ UplinkNASTransport
        ⊟ protocolIEs: 5 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
          ⊞ Item 3: id-EUTRAN-CGI
          ⊞ Item 4: id-TAI
```

```
NAS-PDU: 075308ae97e0016aa10f13
⊟ Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Authentication response (0x53)
  ⊟ Authentication response parameter
      Length: 8
      RES: [redacted]
```

Identities in the AIR :

- eNB-UE-S1AP-ID
- MME-UE-S1AP-ID
- TAI (MNC,MCC,TAC)
- EUTRAN-CGI (PLMN id, MCC, MNC, Cell-id)

Authentication Parameters:

- RES

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Security Mode Command from the MME to the UE

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-downlinkNASTransport (11)
      criticality: ignore (1)
    ⊟ value
      ⊟ DownlinkNASTransport
        ⊟ protocolIEs: 3 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
```

```
⊟ Non-Access-Stratum (NAS)PDU
    0011 .... = Security header type: Integrity protected with new EPS security context (3)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0x673cbd6b
    Sequence number: 0
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Security mode command (0x5d)
  ⊞ NAS security algorithms - Selected NAS security algorithms
    0000 .... = Spare half octet: 0
    .... 0... = Type of security context flag (TSC): Native security context (for KSIasme)
    .... .000 = NAS key set identifier:  (0) ASME
  ⊞ UE security capability - Replayed UE security capabilities
  ⊞ IMEISV request
```

NAS Selected Security Algorithm:

- Integrity Algorithm (ex. 128-EIA1)
- Ciphering Algorithm (ex. EEA0)

UE Security Capability

IMEISV Request

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Security Mode Complete from the UE to the MME

Identities :

- eNB-UE-S1AP-ID
- MME-UE-S1AP-ID
- TAI (MNC,MCC,TAC)
- EUTRAN-CGI (PLMN id, MCC, MNC, Cell-id)

IMEISV Sent with Security mode complete confirmation

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-uplinkNASTransport (13)
      criticality: ignore (1)
    ⊟ value
      ⊟ UplinkNASTransport
        ⊟ protocolIEs: 5 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
          ⊞ Item 3: id-EUTRAN-CGI
          ⊞ Item 4: id-TAI
```

```
⊟ Non-Access-Stratum (NAS)PDU
    0100 .... = Security header type: Integrity protected and ciphered with new EPS security context (4)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0xc5197989
    Sequence number: 0
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Security mode complete (0x5e)
  ⊞ Mobile identity - IMEISV - IMEISV [redacted]
```

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

ESM Information Request/ ESM Information Reply

NAS ESM information :

- APN information

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-downlinkNASTransport (11)
      criticality: ignore (1)
    ⊟ value
      ⊟ DownlinkNASTransport
        ⊟ protocolIEs: 3 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
```

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-uplinkNASTransport (13)
      criticality: ignore (1)
    ⊟ value
      ⊟ UplinkNASTransport
        ⊟ protocolIEs: 5 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
          ⊞ Item 3: id-EUTRAN-CGI
          ⊞ Item 4: id-TAI
```

```
⊟ Non-Access-Stratum (NAS)PDU
    0010 .... = Security header type: Integrity protected and ciphered (
    .... 0111 = Protocol discriminator: EPS mobility management messages
    Message authentication code: 0x70fc0048
    Sequence number: 1
    0000 .... = EPS bearer identity: No EPS bearer identity assigned (0)
    .... 0010 = Protocol discriminator: EPS session management messages
    Procedure transaction identity: 1
    NAS EPS session management messages: ESM information request (0xd9)
```

```
⊟ Non-Access-Stratum (NAS)PDU
    0010 .... = Security header type: Integrity protected and ciphered (2)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0x3b6685b9
    Sequence number: 1
    0000 .... = EPS bearer identity: No EPS bearer identity assigned (0)
    .... 0010 = Protocol discriminator: EPS session management messages (0x02)
    Procedure transaction identity: 1
    NAS EPS session management messages: ESM information response (0xda)
  ⊟ Access Point Name
      Element ID: 0x28
      Length: 23
      APN: [redacted]
  ⊞ Protocol Configuration Options
```

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-InitialContextSetup (9)
      criticality: reject (0)
    ⊟ value
      ⊟ InitialContextSetupRequest
        ⊟ protocolIEs: 6 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-uEaggregateMaximumBitrate
          ⊞ Item 3: id-E-RABToBeSetupListCtxtSUReq
          ⊞ Item 4: id-UESecurityCapabilities
          ⊞ Item 5: id-SecurityKey
```

```
⊟ Item 2: id-uEaggregateMaximumBitrate
  ⊟ ProtocolIE-Field
      id: id-uEaggregateMaximumBitrate (66)
      criticality: reject (0)
    ⊟ value
      ⊟ UEAggregateMaximumBitrate
          uEaggregateMaximumBitRateDL: 5000000
          uEaggregateMaximumBitRateUL: 3000000
```

```
⊟ Item 4: id-UESecurityCapabilities
  ⊟ ProtocolIE-Field
      id: id-UESecurityCapabilities (107)
      criticality: reject (0)
    ⊟ value
      ⊟ UESecurityCapabilities
          ..0. .... Extension Present Bit: False
          encryptionAlgorithms: 0000 [bit length 16, 0000 0000  0000 0000 decimal value 0]
          ...0 .... Extension Present Bit: False
          integrityProtectionAlgorithms: c000 [bit length 16, 1100 0000  0000 0000 decimal value 49152]
⊟ Item 5: id-SecurityKey
  ⊟ ProtocolIE-Field
      id: id-SecurityKey (73)
      criticality: reject (0)
    ⊟ value
        SecurityKey: [redacted] [bit length 256]
```

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

```
⊟ Item 3: id-E-RABToBeSetupListCtxtSUReq
  ⊟ ProtocolIE-Field
      id: id-E-RABToBeSetupListCtxtSUReq (24)
      criticality: reject (0)
    ⊟ value
      ⊟ E-RABToBeSetupListCtxtSUReq: 1 item
        ⊟ Item 0: id-E-RABToBeSetupItemCtxtSUReq
          ⊟ ProtocolIE-SingleContainer
              id: id-E-RABToBeSetupItemCtxtSUReq (52)
              criticality: reject (0)
            ⊟ value
              ⊟ E-RABToBeSetupItemCtxtSUReq
                e-RAB-ID: 5
                ⊞ e-RABlevelQoSParameters
                0... .... Extension Present Bit: False
                ⊞ transportLayerAddress: 0a01010c [bit length 32, 0000 1010  0000 0001  0000 0001  0000 1100 decimal value 167837964]
                gTP-TEID: 02000000
                nAS-PDU: [redacted]
                ⊞ Non-Access-Stratum (NAS)PDU
```

The Attach accept message include the e-RAB setup RAB Setup Context id's:

- e-RAB-ID
- GTP-TEID

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

```
⊟ Item 3: id-E-RABToBeSetupListCtxtSUReq
  ⊟ ProtocolIE-Field
      id: id-E-RABToBeSetupListCtxtSUReq (24)
      criticality: reject (0)
    ⊟ value
      ⊟ E-RABToBeSetupListCtxtSUReq: 1 item
        ⊟ Item 0: id-E-RABToBeSetupItemCtxtSUReq
          ⊟ ProtocolIE-SingleContainer
              id: id-E-RABToBeSetupItemCtxtSUReq (52)
              criticality: reject (0)
            ⊟ value
              ⊟ E-RABToBeSetupItemCtxtSUReq
                  e-RAB-ID: 5
                ⊞ e-RABlevelQoSParameters
                  0... .... Extension Present Bit: False
                ⊞ transportLayerAddress: 0a01010c [bit length 32, 0000 1010  0000 0001  0000 0001  0000 1100 decimal value 167837964]
                  gTP-TEID: 02000000
                  nAS-PDU: [redacted]
                ⊞ Non-Access-Stratum (NAS)PDU
```

The Attach accept message include the e-RAB setup

RAB Setup Context id's:

- e-RAB-ID
- GTP-TEID

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

```
⊟ Non-Access-Stratum (NAS)PDU
    0010 .... = Security header type: Integrity protected and ciphered (2)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0xee842d22
    Sequence number: 2
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Attach accept (0x42)
    0000 .... = Spare half octet: 0
    .... 0... = Spare bit(s): 0x00
    .... .001 = Attach result: EPS only (1)
  ⊞ GPRS Timer - T3412 value
  ⊞ Tracking area identity list - TAI list
  ⊞ ESM message container
  ⊞ EPS mobile identity - GUTI
```

RAB Setup Contains the NAS PDU

- GPRS Timers
- TAI list
- GUTI (MCC, MNC ,MME Group-id, MME Code, M-TMSI)

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

ESM Message Container

- QoS (QCI 5 for default)
- APN name
- IP assigned
- LLC
- QoS
- AMBR
- Packet Flow filter
- PCO

```
⊟ ESM message container
    Length: 90
  ⊟ ESM message container contents: 5201c10105170361706e0373697005766f696365046e6734...
      0101 .... = EPS bearer identity: EPS bearer identity value 5 (5)
      .... 0010 = Protocol discriminator: EPS session management messages (0x02)
      Procedure transaction identity: 1
      NAS EPS session management messages: Activate default EPS bearer context request (0xc1)
    ⊟ EPS quality of service
        Length: 1
        Quality of Service Class Identifier (QCI): QCI 5 (5)
    ⊟ Access Point Name
        Length: 23
        APN: [redacted]
    ⊟ PDN address
        Length: 5
        0000 0... = Spare bit(s): 0x00
        PDN type: IPv4 (1)
        PDN IPv4: [redacted]
    ⊞ Linked TI - Transaction identifier
    ⊞ Quality Of Service - Negotiated QoS
    ⊞ LLC Service Access Point Identifier - Negotiated LLC SAPI
    ⊞ Radio Priority
    ⊞ Packet Flow Identifier - Best Effort
    ⊞ APN aggregate maximum bit rate
    ⊞ Protocol Configuration Options
⊞ EPS mobile identity - GUTI
```

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

Attach accept

- GTP-TEID
- E-RAB ID

```
S1AP-PDU: successfulOutcome (1)
⊟ successfulOutcome
    procedureCode: id-InitialContextSetup (9)
    criticality: reject (0)
  ⊟ value
    ⊟ InitialContextSetupResponse
      ⊟ protocolIEs: 3 items
        ⊞ Item 0: id-MME-UE-S1AP-ID
        ⊞ Item 1: id-eNB-UE-S1AP-ID
        ⊟ Item 2: id-E-RABSetupListCtxtSURes
          ⊟ ProtocolIE-Field
              id: id-E-RABSetupListCtxtSURes (51)
              criticality: ignore (1)
            ⊟ value
              ⊟ E-RABSetupListCtxtSURes: 1 item
                ⊟ Item 0: id-E-RABSetupItemCtxtSURes
                  ⊟ ProtocolIE-SingleContainer
                      id: id-E-RABSetupItemCtxtSURes (50)
                      criticality: ignore (1)
                    ⊟ value
                      ⊟ E-RABSetupItemCtxtSURes
                          e-RAB-ID: 5
                          .... ...0 Extension Present Bit: False
                        ⊟ transportLayerAddress: 0a01020b [bit length 32, 0000
                            transportLayerAddress(IPv4): [redacted]
                          gTP-TEID: 02000000
```

LTE/EPC Bearer Types

LTE/EPC Attach Procedure

- **Attach Complete**
- **Default Bearer Context Accept**

```
⊞ Item 0: id-MME-UE-S1AP-ID
⊞ Item 1: id-eNB-UE-S1AP-ID
⊟ Item 2: id-NAS-PDU
  ⊟ ProtocolIE-Field
      id: id-NAS-PDU (26)
      criticality: reject (0)
    ⊟ value
        NAS-PDU: 2728e2796b02074300195201c227148080211003000010 81...
      ⊟ Non-Access-Stratum (NAS)PDU
          0010 .... = Security header type: Integrity protected and ciphered (2)
          .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
          Message authentication code: 0x28e2796b
          Sequence number: 2
          0000 .... = Security header type: Plain NAS message, not security protected (0)
          .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
          NAS EPS Mobility Management Message Type: Attach complete (0x43)
        ⊟ ESM message container
            Length: 25
          ⊟ ESM message container contents: 5201c227148080211003000010810600000000830600000 0...
              0101 .... = EPS bearer identity: EPS bearer identity value 5 (5)
              .... 0010 = Protocol discriminator: EPS session management messages (0x02)
              Procedure transaction identity: 1
              NAS EPS session management messages: Activate default EPS bearer context accept (0xc2)
            ⊟ Protocol Configuration Options
                Element ID: 0x27
                Length: 20
                [Link direction: MS to network (0)]
                1... .... = Extension: True
                Configuration Protocol: PPP for use with IP PDP type or IP PDN type (0)
              ⊞ Protocol or Container ID: Internet Protocol Control Protocol (0x8021)
⊞ Item 3: id-EUTRAN-CGI
⊞ Item 4: id-TAI
```

Agenda

- Mobility and Session Management states
- UE and Network identifications
- LTE/EPC Bearer Types and QoS
- LTE/EPC Attach Procedure
- **LTE/EPC Detach Procedure**
- LTE/EPC Bearer Activation Procedure
- LTE/EPC Service Request Procedures
- Tracking Area Update
- LTE/EPC Handover

Detach Procedures

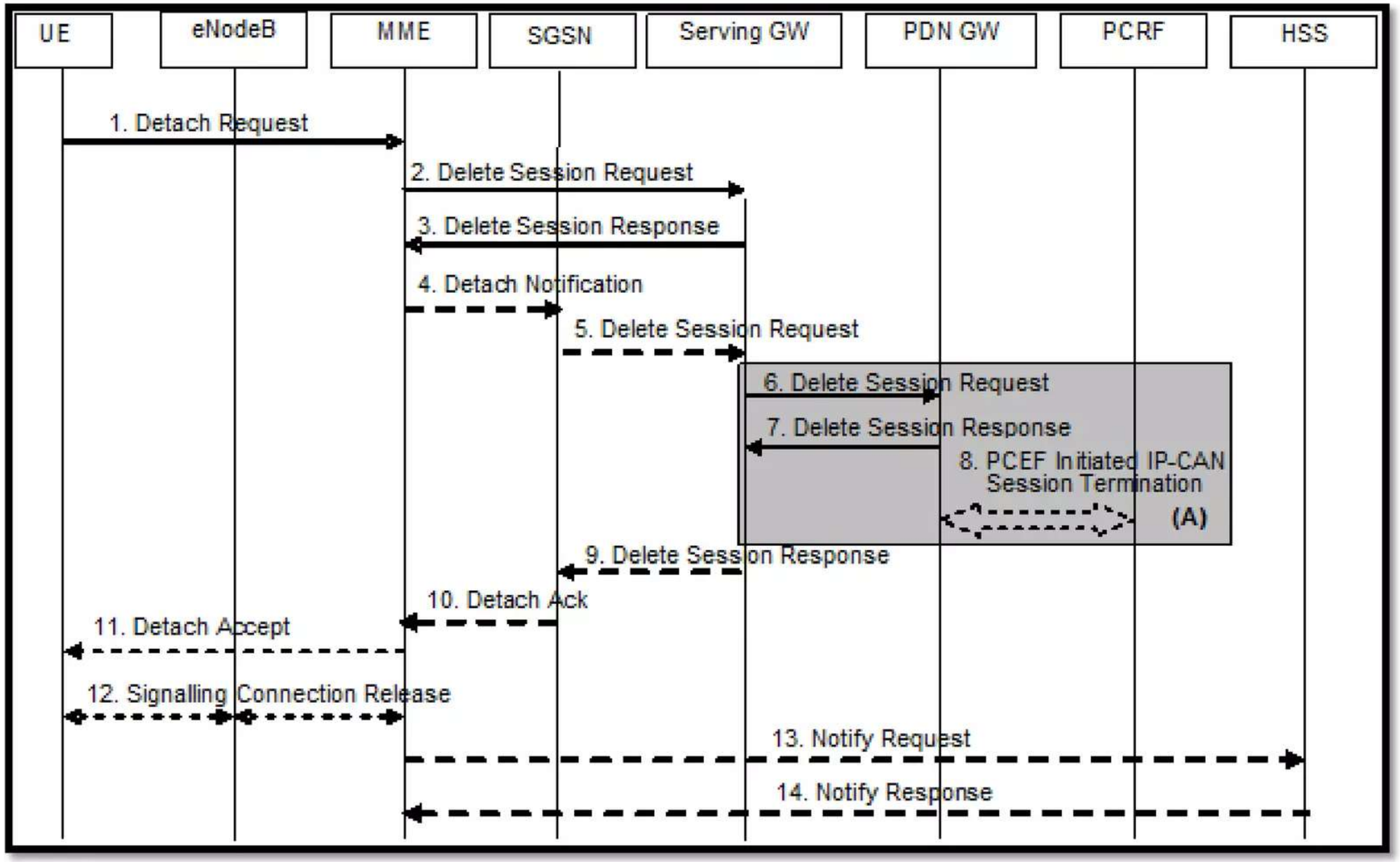
UE Initiated Detach

- The transition to **EMM_DEREGISTERED state** is achieved by the NAS detach procedure.
- The procedure consists of:
  - ***DETACH REQUEST / DETACH ACCEPT*** procedure between UE and MME.
  - the ***DELETE BEARER*** procedure between MME and SAE GW and PDN GW.
  - ***S1 RELEASE*** procedure between MME and eNB deletes all radio resources.

- Detach Procedures Can be triggered by three Parties:
  1. UE
  2. MME
  3. HSS

Detach Procedures

UE Initiated Detach



Detach Procedures

UE Initiated Detach

UE NAS Detach Request

```
◢ protocolIEs: 5 items
  ▷ Item 0: id-MME-UE-S1AP-ID
  ▷ Item 1: id-eNB-UE-S1AP-ID
  ◢ Item 2: id-NAS-PDU
    ◢ ProtocolIE-Field
        id: id-NAS-PDU (26)
        criticality: reject (0)
      ◢ value
          NAS-PDU:
        ◢ Non-Access-Stratum (NAS)PDU
            0010 .... = Security header type: Integrity protected and ciphered (2)
            .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
            Message authentication code: 0x54209443
            Sequence number: 6
            0000 .... = Security header type: Plain NAS message, not security protected (0)
            .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
            NAS EPS Mobility Management Message Type: Detach request (0x45)
            Uplink
            0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
            .000 .... = NAS key set identifier:  (0)
            .... 0... = Switch off: Normal detach (0)
            .... .001 = Detach Type: EPS detach (1)
          ▷ EPS mobile identity
  ▷ Item 3: id-EUTRAN-CGI
  ▷ Item 4: id-TAI
```

Detach Procedures

UE Initiated Detach

Signaling Connection Release (Context Release)

```
S1 Application Protocol
  S1AP-PDU: initiatingMessage (0)
    initiatingMessage
      procedureCode: id-UEContextRelease (23)
      criticality: reject (0)
      value
        UEContextReleaseCommand
          protocolIEs: 2 items
            Item 0: id-UE-S1AP-IDs
              ProtocolIE-Field
                id: id-UE-S1AP-IDs (99)
                criticality: reject (0)
                value
                  UE-S1AP-IDs: uE-S1AP-ID-pair (0)
                    uE-S1AP-ID-pair
                      mME-UE-S1AP-ID: 0
                      eNB-UE-S1AP-ID: 10
            Item 1: id-Cause
              ProtocolIE-Field
                id: id-Cause (2)
                criticality: ignore (1)
                value
                  Cause: nas (2)
                    nas: detach (2)
```

Detach Procedures

MME Initiated Detach

The transition to **EMM_DEREGISTERED** state is achieved by the NAS detach procedure.
The procedure consists :

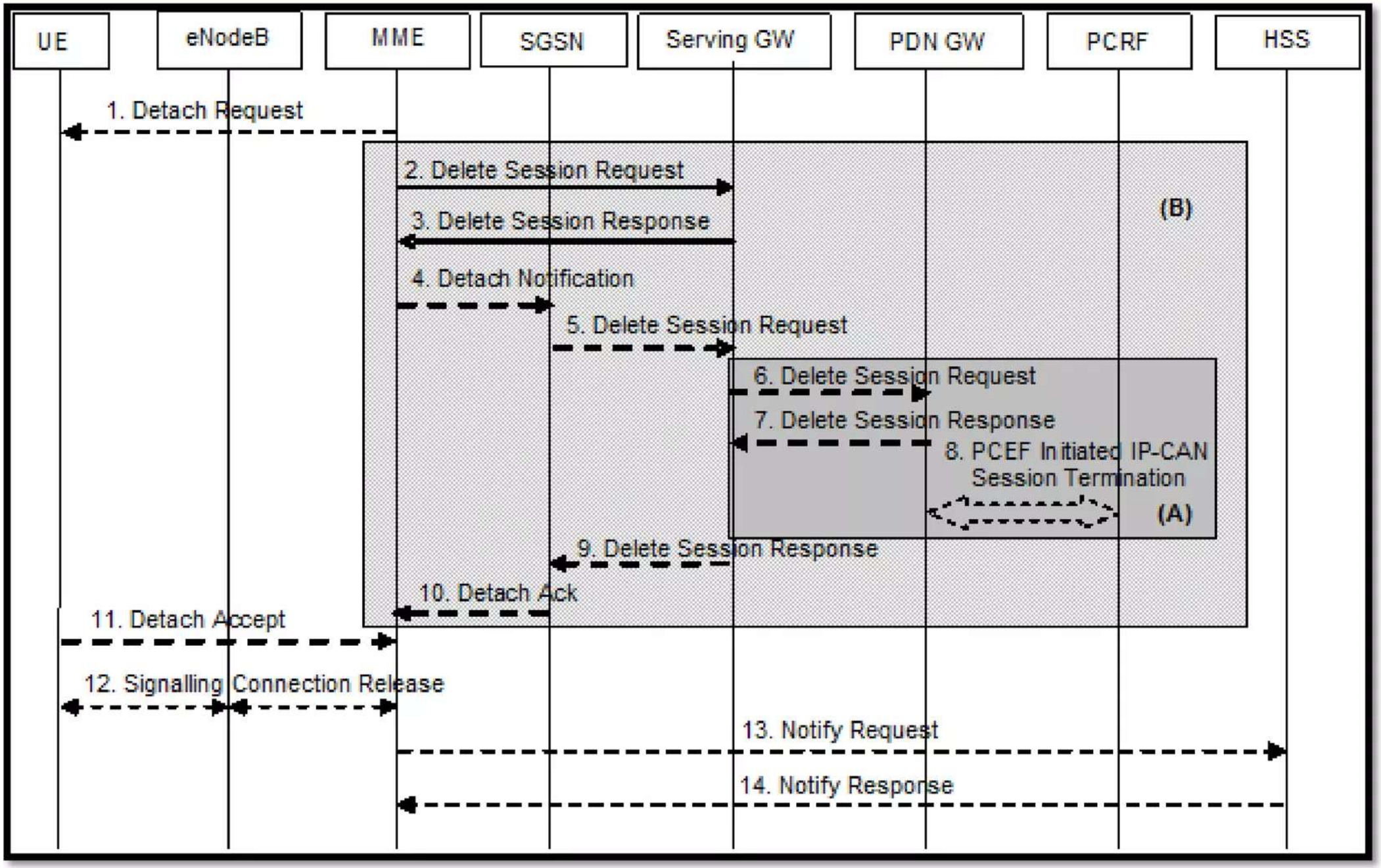
1. ***DETACH REQUEST / DETACH ACCEPT*** procedure between UE and MME

2. ***DELETE BEARER*** procedure between MME and SAE GW and PDN GW.

3. ***S1 RELEASE*** procedure between MME and eNB deletes all radio resources.

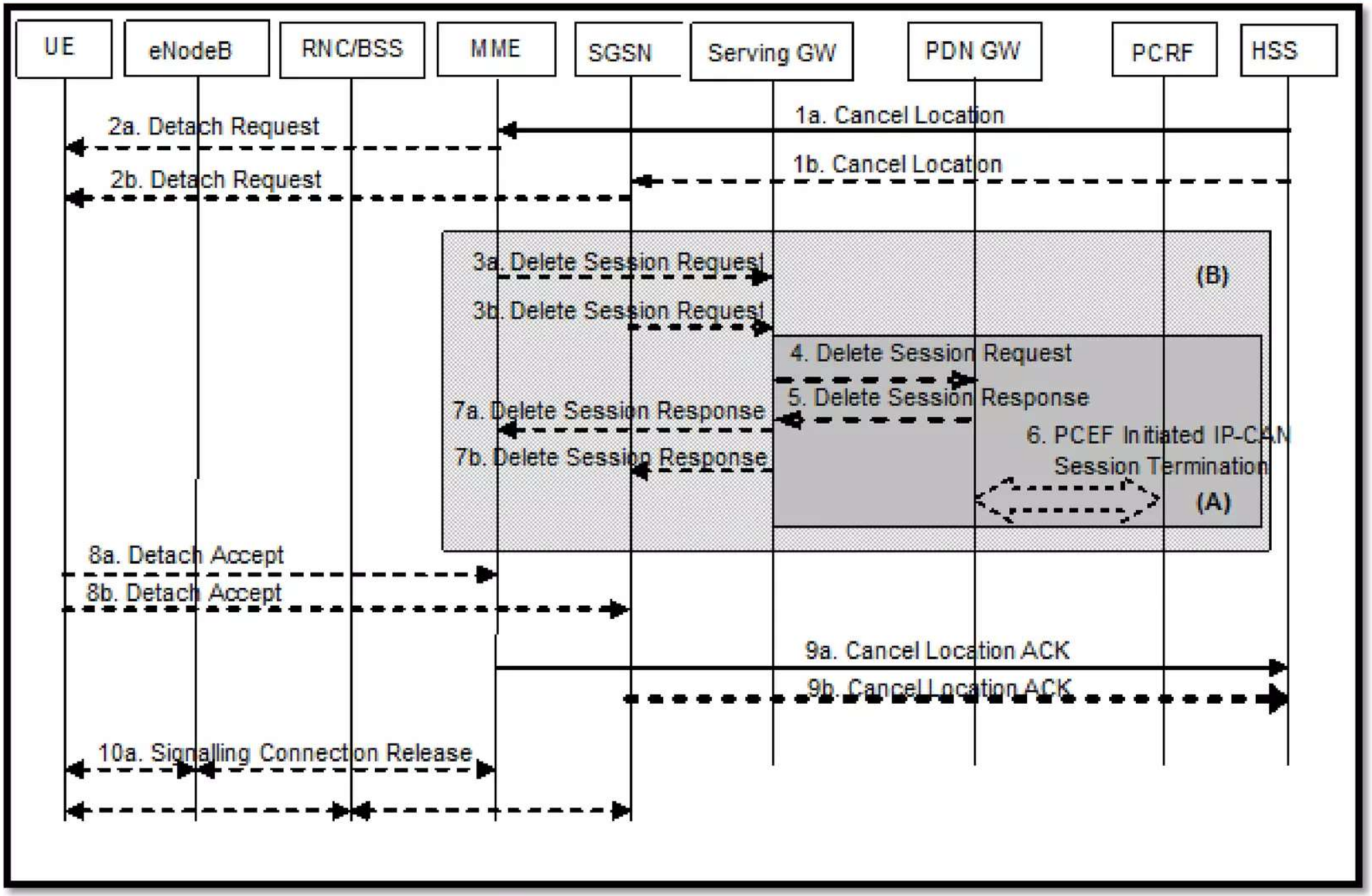
Detach Procedures

MME Initiated Detach



Detach Procedures

HSS Initiated Detach



Agenda

- Mobility and Session Management states
- UE and Network identifications
- LTE/EPC Bearer Types and QoS
- LTE/EPC Attach Procedure
- LTE/EPC Detach Procedure
- **LTE/EPC Bearer Activation Procedure**
- LTE/EPC Service Request Procedures
- Tracking Area Update
- LTE/EPC Handover

LTE/EPC Bearer Activation

Dedicated Bearer Activation

1. The external data network triggers the request **for a new IP connectivity bearer (SAE bearer) via the PCRF connected** to the PDN gateway that owns the default SAE bearer of this user. This is sent in form of a policy and charging control (PCC) decision from PCRF to PDN GW.

2. The PDN GW first of all uses ***GTP-C CREATE DEDICATED BEARER REQUEST*** to setup the tunnel between **PDN GW and SAE GW.**

3. The **SAE GW allocates the resources for the S5/S8 tunnel** and forwards an associated request to the **MME for the S1 tunnel.**

4. If the UE is currently ECM_IDLE it must be paged. Thus the MME sends *PAGING* messages of S1-AP protocol to all eNB that own cell's of the UE's current tracking area (or tracking areas).

LTE/EPC Bearer Activation

Dedicated Bearer Activation

5. If the UE receives such a paging it will respond with the ***SERVICE REQUEST*** procedure. in the following the default SAE bearer will be re-established.

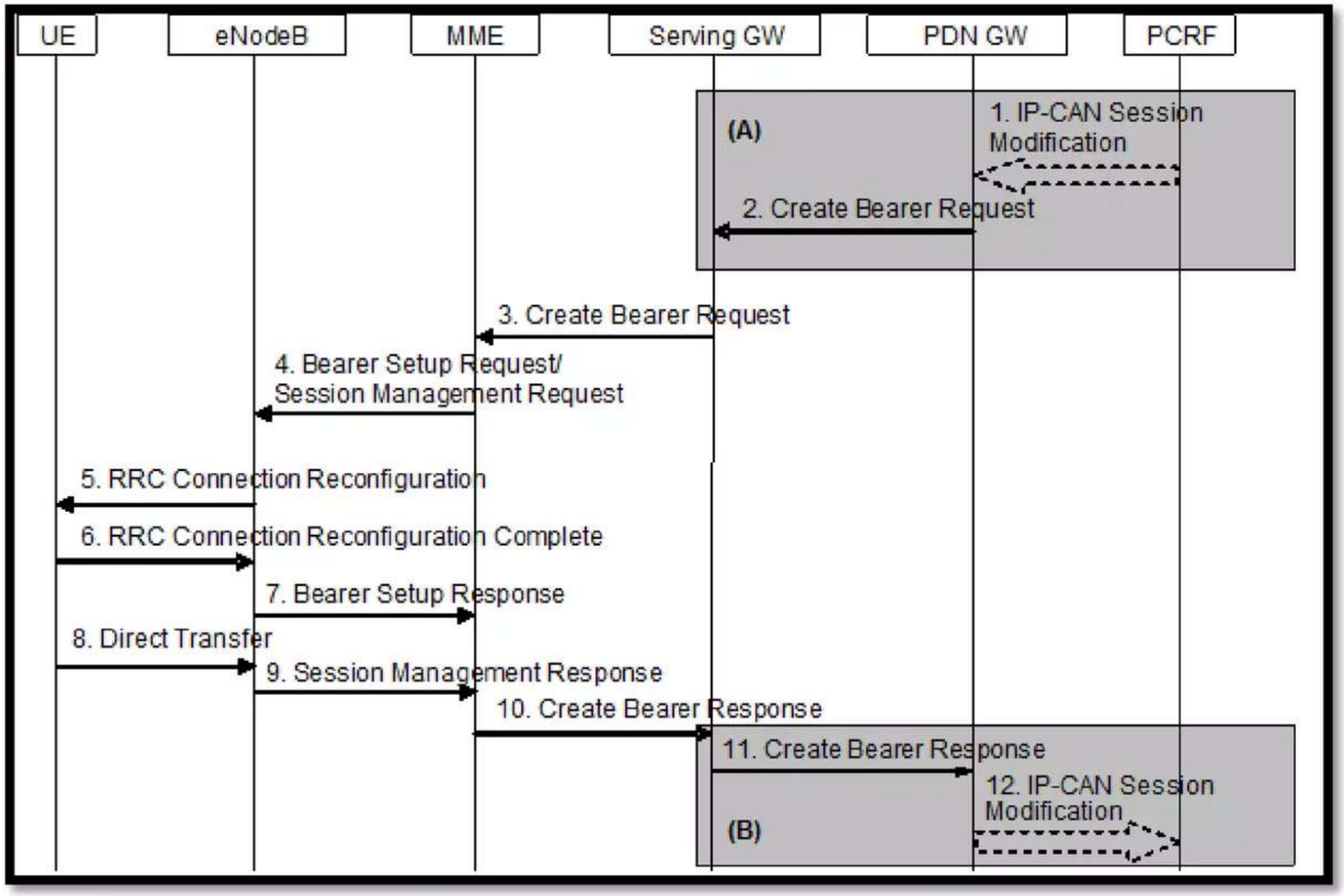
6. If the default bearer is up and the UE is in state ECM_Connected the radio bearer and S1 tunnel for the new SAE bearer can be created. Thus the MME sends to the eNB the S1-AP message ***BEARER SETUP REQUEST***. It contains the TEID from SAE GW for the new S1 tunnel. This message also triggers the setup of the new radio bearers.

7. The **response messages** now run from **UE to eNB** to **MME to SAE GW** to **PDN GW to PCRF.** With this the new SAE bearer is ready for use.

LTE/EPC Bearer Activation

Dedicated Bearer Activation

The default SAE bearer is created when the UE is attached to the Network. Any other bearers is activated via a dedicated bearer procedure ,Dedicated bearers can be triggered by the external data network and user.



LTE/EPC Bearer Activation

Dedicated Bearer Activation

Activate Dedicated EPS Service

Activate Dedicated Bearer Request is Sent from the MME to the UE, with the E-RAB Setup

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-E-RABSetup (5)
      criticality: reject (0)
    ⊟ value
      ⊟ E-RABSetupRequest
        ⊟ protocolIEs: 4 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊟ Item 2: id-uEaggregateMaximumBitrate
            ⊟ ProtocolIE-Field
                id: id-uEaggregateMaximumBitrate (66)
                criticality: reject (0)
              ⊟ value
                ⊟ UEAggregateMaximumBitrate
                    uEaggregateMaximumBitRateDL: 5598
                    uEaggregateMaximumBitRateUL: 5599
          ⊞ Item 3: id-E-RABToBeSetupListBearerSUReq
```

```
⊟ Item 3: id-E-RABToBeSetupListBearerSUReq
  ⊟ ProtocolIE-Field
      id: id-E-RABToBeSetupListBearerSUReq (16)
      criticality: reject (0)
    ⊟ value
      ⊟ E-RABToBeSetupListBearerSUReq: 1 item
        ⊟ Item 0: id-E-RABToBeSetupItemBearerSUReq
          ⊟ ProtocolIE-SingleContainer
              id: id-E-RABToBeSetupItemBearerSUReq (17)
              criticality: reject (0)
            ⊟ value
              ⊟ E-RABToBeSetupItemBearerSUReq
                  e-RAB-ID: 6
                ⊞ e-RABlevelQoSParameters
                  0... .... Extension Present Bit: False
                ⊞ transportLayerAddress: 0a01010c [bit length 32, 0000 1010  0000
                  gTP-TEID: 03000000
                  nAS-PDU:
                ⊞ Non-Access-Stratum (NAS)PDU
```

LTE/EPC Bearer Activation

Dedicated Bearer Activation

NAS PDU, Activate Dedicated Bearer Request (E-RAB Request)

```
Non-Access-Stratum (NAS)PDU
  0010 .... = Security header type: Integrity protected and ciphered (2)
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
  Message authentication code: 0x70510843
  Sequence number: 3
  0110 .... = EPS bearer identity: EPS bearer identity value 6 (6)
  .... 0010 = Protocol discriminator: EPS session management messages (0x02)
  Procedure transaction identity: 0
  NAS EPS session management messages: Activate dedicated EPS bearer context reques
  0000 .... = Spare half octet: 0
  .... 0101 = Linked EPS bearer identity: EPS bearer identity value 5 (5)
⊟ EPS quality of service
    Length: 5
    Quality of Service Class Identifier (QCI): QCI 1 (1)
    Maximum bit rate for uplink: 8640 kbps
    Maximum bit rate for downlink: 8640 kbps
    Guaranteed bit rate for uplink: 0 kbps
    Guaranteed bit rate for downlink: 0 kbps
⊟ Traffic Flow Template
    Length: 18
    001. .... = TFT operation code: Create new TFT (1)
    ...0 .... = E bit: Parameters list is not included
    .... 0001 = Number of packet filters: 1
  ⊞ Packet filter 0
⊞ Linked TI - Transaction identifier
⊞ Quality Of Service - Negotiated QoS
⊞ LLC Service Access Point Identifier - Negotiated LLC SAPI
⊞ Radio Priority
⊞ Packet Flow Identifier - Best Effort
⊟ Protocol Configuration Options
    Element ID: 0x27
    Length: 20
    [Link direction: Network to MS (1)]
    1... .... = Extension: True
    Configuration Protocol: PPP for use with IP PDP type or IP PDN type (0)
  ⊞ Protocol or Container ID: Internet Protocol Control Protocol (0x8021)
```

```
⊟ Packet filter 0
    00.. .... = Spare bit(s): 0
    ..11 .... = Packet filter direction: Bidirectional (3)
    .... 0110 = Packet filter identifier: 7 (6)
    Packet evaluation precedence: 0x0a (10)
    Packet filter length: 0x0e (14)
  ⊟ Packet filter component type identifier: Protocol identifier/Next header type (48)
      Protocol/header: UDP (0x11)
  ⊟ Packet filter component type identifier: IPv4 remote address type (16)
      IPv4 address [redacted]
      IPv4 address mask: 255.255.255.255 (255.255.255.255)
  ⊟ Packet filter component type identifier: Single local port type (64)
      Port: [redacted]
```

LTE/EPC Bearer Activation

Dedicated Bearer Activation

E-RAB Setup Response

```
⊟ protocolIEs: 3 items
  ⊞ Item 0: id-MME-UE-S1AP-ID
  ⊞ Item 1: id-eNB-UE-S1AP-ID
  ⊟ Item 2: id-E-RABSetupListBearerSURes
    ⊟ ProtocolIE-Field
        id: id-E-RABSetupListBearerSURes (28)
        criticality: ignore (1)
      ⊟ value
        ⊟ E-RABSetupListBearerSURes: 1 item
          ⊟ Item 0: id-E-RABSetupItemBearerSURes
            ⊟ ProtocolIE-SingleContainer
                id: id-E-RABSetupItemBearerSURes (39)
                criticality: ignore (1)
              ⊟ value
                ⊟ E-RABSetupItemBearerSURes
                    e-RAB-ID: 6
                    .... ...0 Extension Present Bit: False
                  ⊟ transportLayerAddress: 0a01020b [bit length 32, 0000
                      transportLayerAddress(IPv4):
                    gTP-TEID: 03000000
```

E-RAB Response identities:

- GTP-TEID
- E-RAB ID

LTE/EPC Bearer Activation

Dedicated Bearer Activation

```
⊟ UplinkNASTransport
  ⊟ protocolIEs: 5 items
    ⊞ Item 0: id-MME-UE-S1AP-ID
    ⊞ Item 1: id-eNB-UE-S1AP-ID
    ⊟ Item 2: id-NAS-PDU
      ⊟ ProtocolIE-Field
          id: id-NAS-PDU (26)
          criticality: reject (0)
        ⊟ value
            NAS-PDU: 27fbf7cacc036200c627148080211003000010810 6ac1100...
          ⊟ Non-Access-Stratum (NAS)PDU
              0010 .... = Security header type: Integrity protected and ciphered (2)
              .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
              Message authentication code: 0xfbf7cacc
              Sequence number: 3
              0110 .... = EPS bearer identity: EPS bearer identity value 6 (6)
              .... 0010 = Protocol discriminator: EPS session management messages (0x02)
              Procedure transaction identity: 0
              NAS EPS session management messages: Activate dedicated EPS bearer context accept (0xc6)
            ⊞ Protocol Configuration Options
    ⊞ Item 3: id-EUTRAN-CGI
    ⊞ Item 4: id-TAI
```

Agenda

- Mobility and Session Management states
- UE and Network identifications
- LTE/EPC Bearer Types and QoS
- LTE/EPC Attach Procedure
- LTE/EPC Detach Procedure
- LTE/EPC Bearer Activation Procedure
- **LTE/EPC Service Request Procedures**
- Tracking Area Update
- LTE/EPC Handover

LTE/EPC Service Request

Introduction

The purpose of this procedure is to transfer the EMM mode **from EMM-IDLE** to **EMM-CONNECTED mode**, and establish the radio and S1 bearers when user data or signaling is to be sent.

The Service Request Procedure is used in the following conditions

- UE in EMM-IDLE and has a pending User data or signalling to be sent.
- UE is EMM-IDLE and receives a "PS" paging request.
- CS Fallback Scenarios (Extended Service Request)

The Service reuest is divided to two types:

1. UE Initiated Service Request
2. MME Initiated Service Request

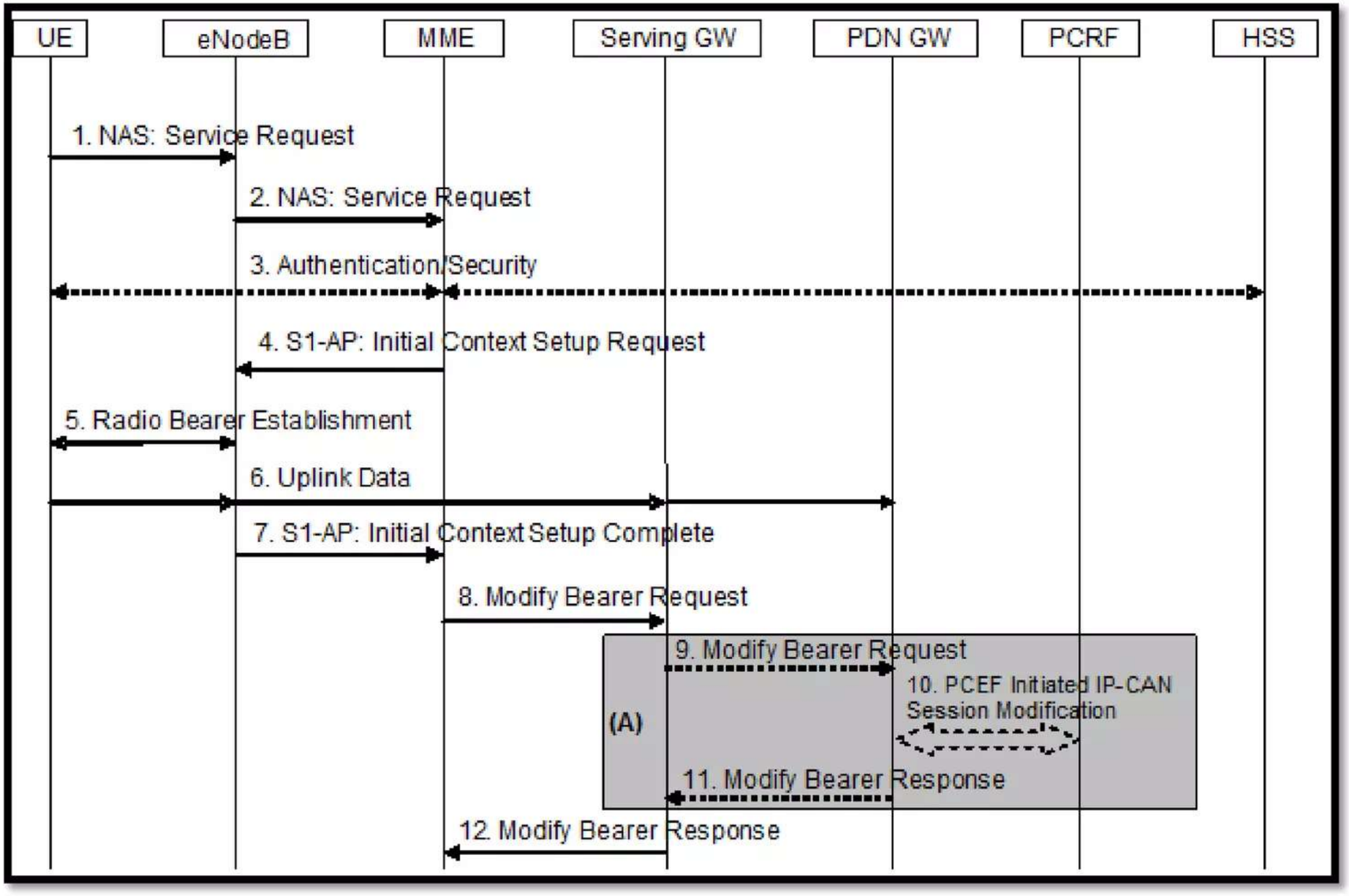
LTE/EPC Service Request

UE Initiated Service Request

1. The UE sends the NAS message ***SERVICE REQUEST* uplink** via eNB to the MME. If there are multiple MME connected to the eNB it is the task of the eNB to select the **right MME** (the one the UE is registered with) from **S-TMSI and TAI**.
2. The MME can now start authentication if required.
3. the MME start to re-establish the radio bearer and S1 tunnels for the active SAE bearers of the UE.
4. MME sends the S1-AP message ***INITIAL CONTEXT SETUP REQUEST*** to the eNB. This message contains the **still active tunnel endpoint identifiers from SAE GW** and request the eNB to create new radio bearers.
5. eNB returns ***INITIAL CONTEXT SETUP RESPONSE*** in which it indicates **its own tunnel endpoint identifiers** for S1 interface.
6. These TEIDs of the eNB are now forwarded to the SAE GW with GTP-C ***UPDATE BEARER REQUEST***. This completes the transition of the UE to LTE_ACTIVE.

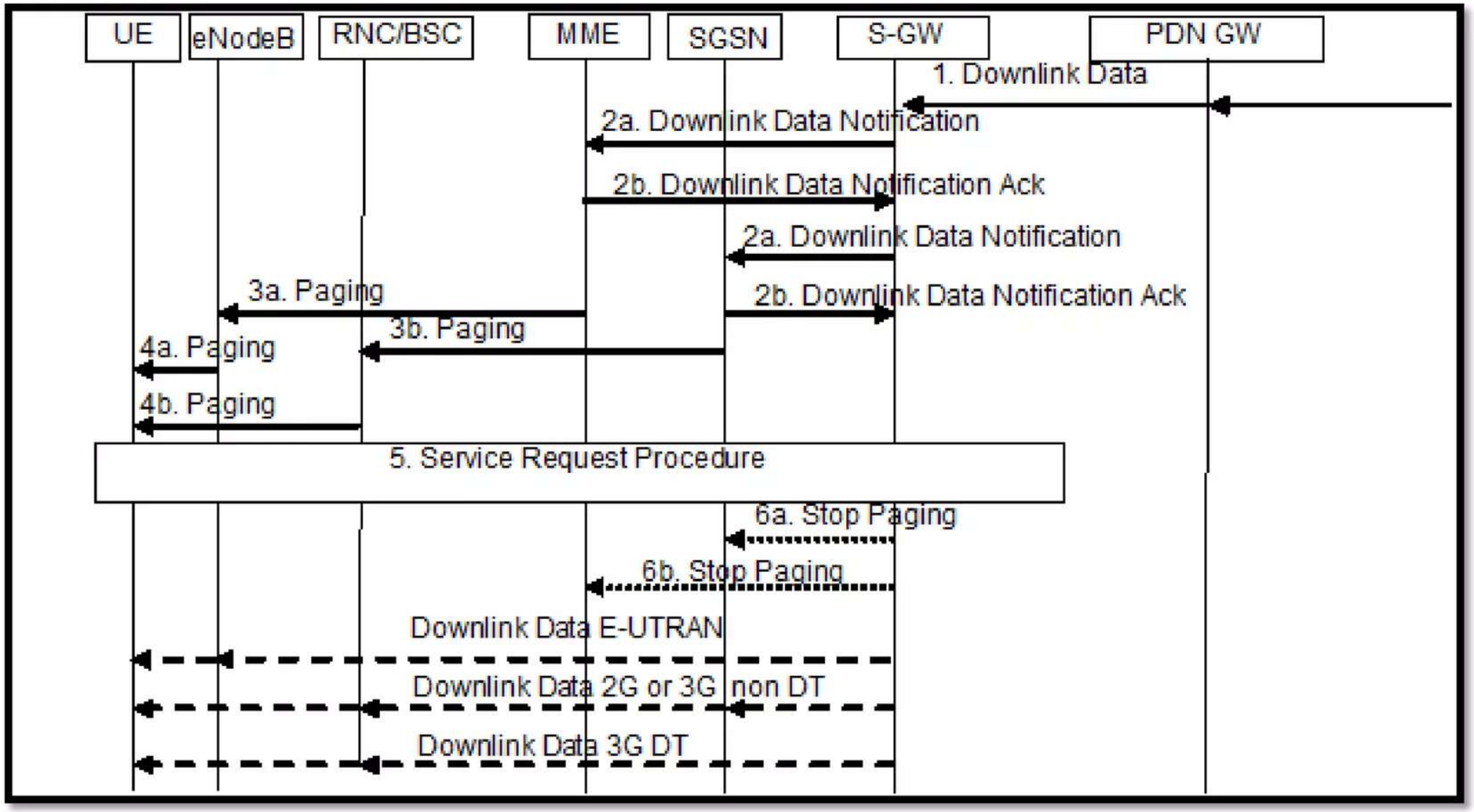
LTE/EPC Service Request

UE Initiated Service Request



LTE/EPC Service Request

MME Initiated Service Request



LTE/EPC Service Request

MME Initiated Service Request

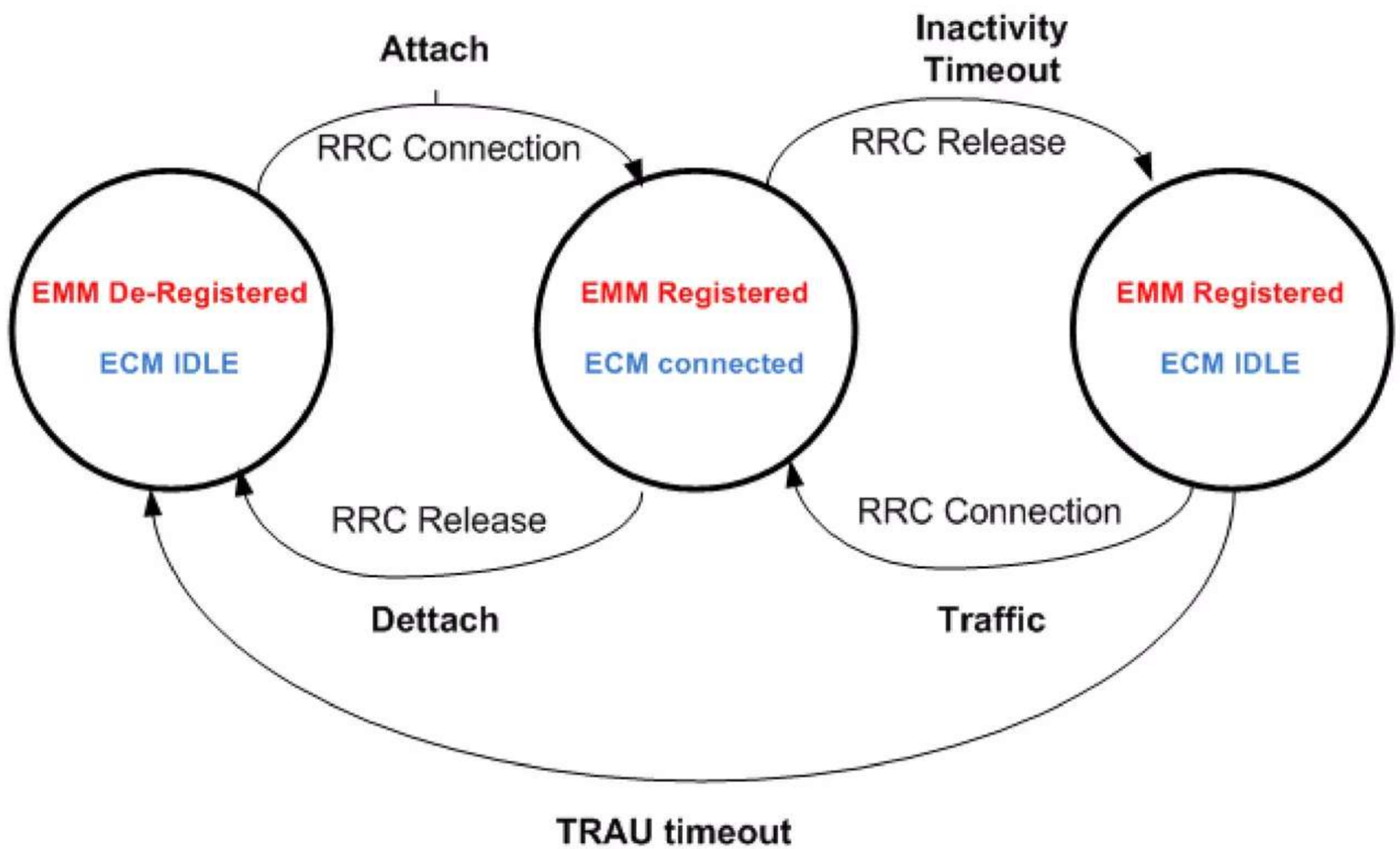
Extended Service Request used in CS Fallback Scenarios

```
⊟ Non-Access-Stratum (NAS)PDU
    0001 .... = Security header type: Integrity protected (1)
    .... 0111 = Protocol discriminator: EPS mobility management messages (7)
    Message authentication code: 0x59904bf4
    Sequence number: 7
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (7)
    NAS EPS Mobility Management Message Type: Extended service request (0x4c)
    0... .... = Type of security context flag (TSC): Native security context (for KSIasme) (0)
    .000 .... = NAS key set identifier:  (0)
    .... 0000 = Service type: Mobile originating CS fallback or 1xCS fallback (0)
  ⊟ Mobile identity - M-TMSI - TMSI/P-TMSI [redacted]
      Length: 5
      0000 .... = Unused
      .... 0... = Odd/even indication: Even number of identity digits
      .... .100 = Mobile Identity Type: TMSI/P-TMSI (4)
      TMSI/P-TMSI: [redacted]
```

LTE/EPC Bearer Activation

S1 Release

If the UE spends too much time in inactivity time , either the enodeB or the MME should free the resources through what is called S1 release



LTE/EPC Bearer Activation

S1 Release

1. The eNB send the message ***S1 RELEASE REQUEST* (S1-AP)** to the MME to request the release of all EUTRAN resources for a UE.

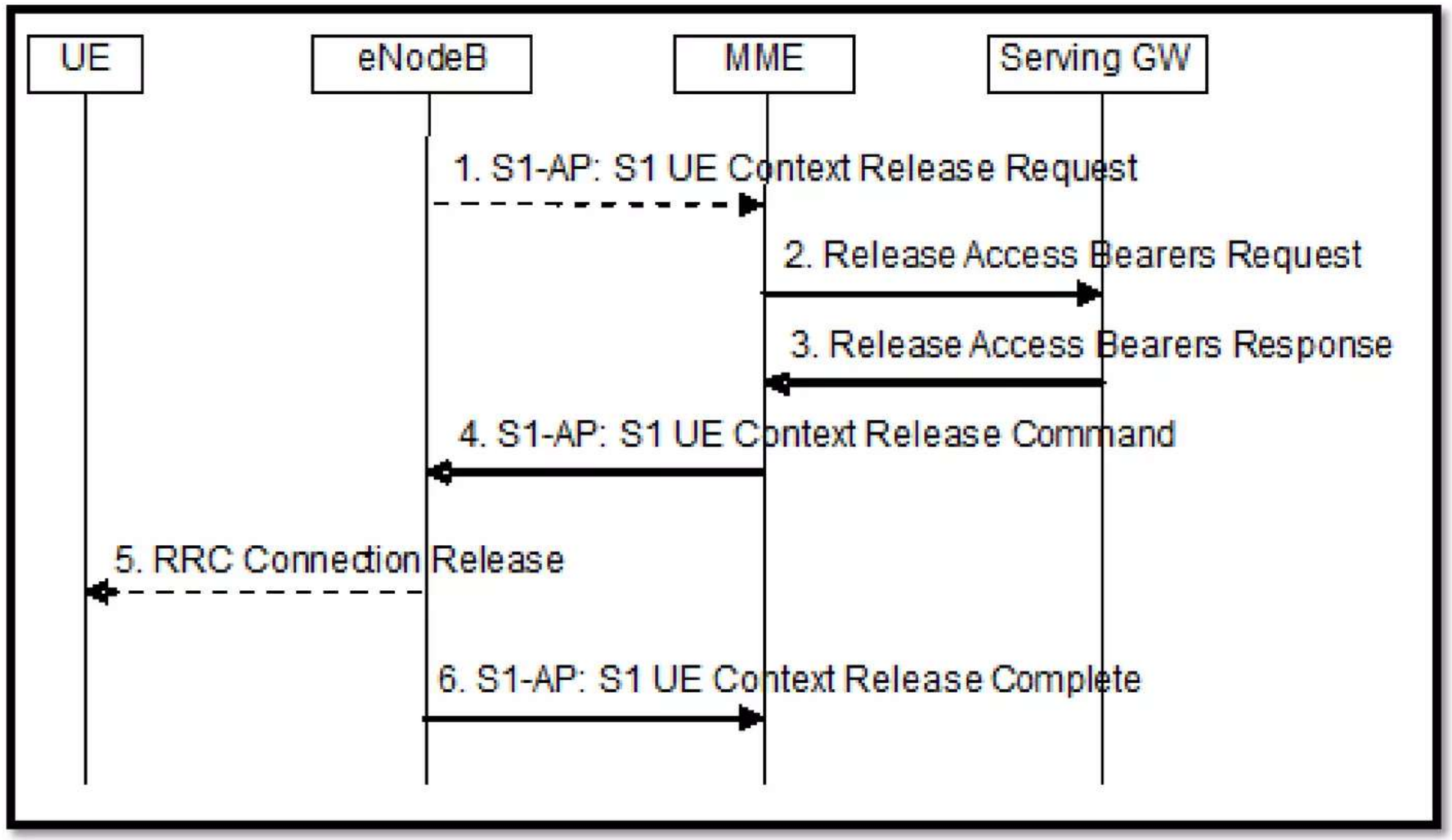
2. When the MME gets a trigger to release the UE from EUTRAN, it will release the S1 tunnels allocated for the SAE bearers of the UE. This is done by sending an ***UPDATE BEARER REQUEST*** message (GTP-C) to the SAE GW.

3. In parallel to the previous step the MME will send the **S1-AP message *S1 RELEASE COMMAND*** to the eNB. It will trigger the release of the UE on the air interface with message *RRC CONNECTION RELEASE* (RRC).

4. This will bring the UE to **RRC_IDLE state** and with that also to **LTE_IDLE** state. The UE acknowledges with ***RRC CONNECTION RELEASE ACK***.

LTE/EPC Bearer Activation

S1 Release



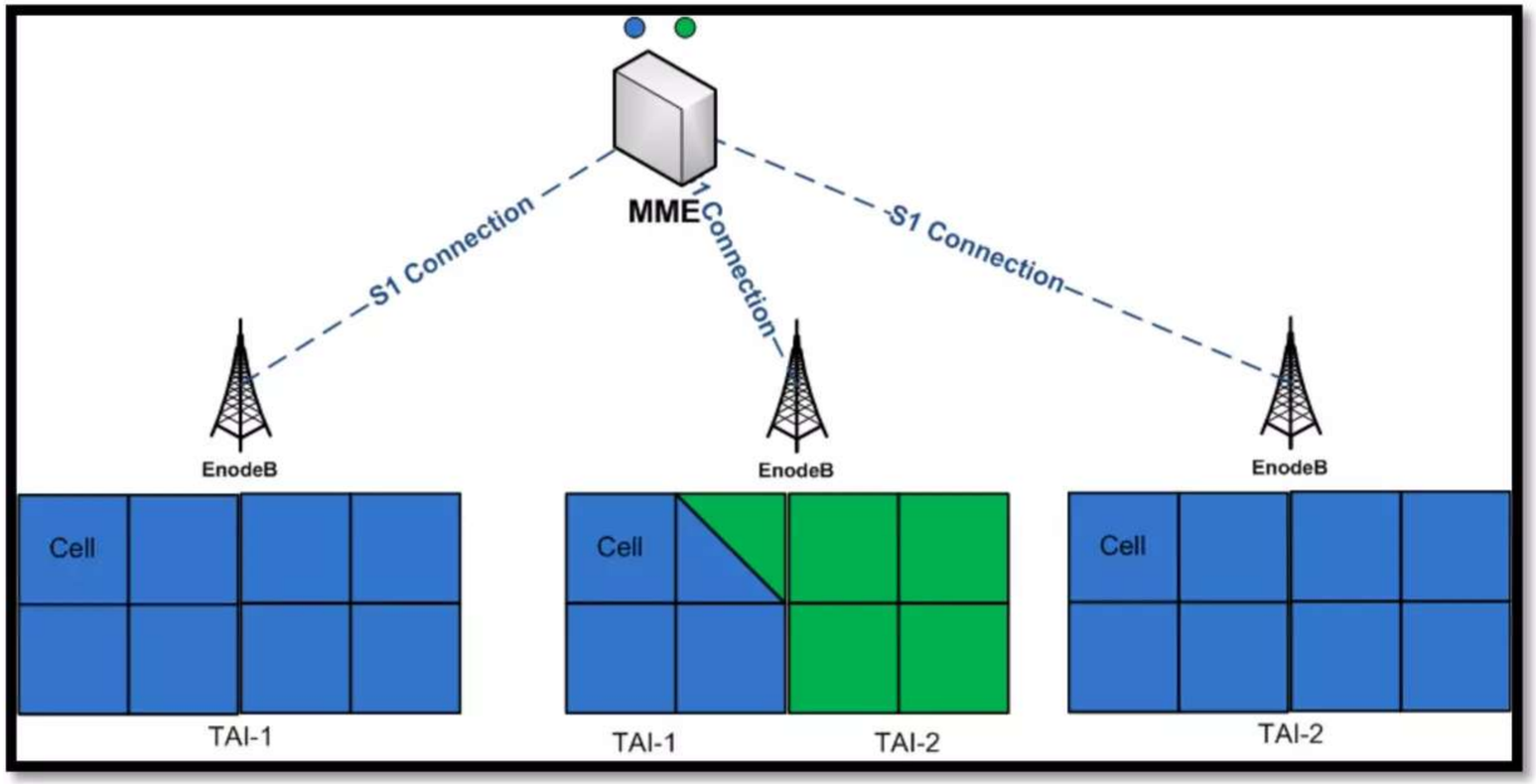
Agenda

- Mobility and Session Management states
- UE and Network identifications
- LTE/EPC Bearer Types and QoS
- LTE/EPC Attach Procedure
- LTE/EPC Detach Procedure
- LTE/EPC Bearer Activation Procedure
- LTE/EPC Service Request Procedures
- **Tracking Area Update**
- LTE/EPC Handover

Tracking Area Update

Introduction

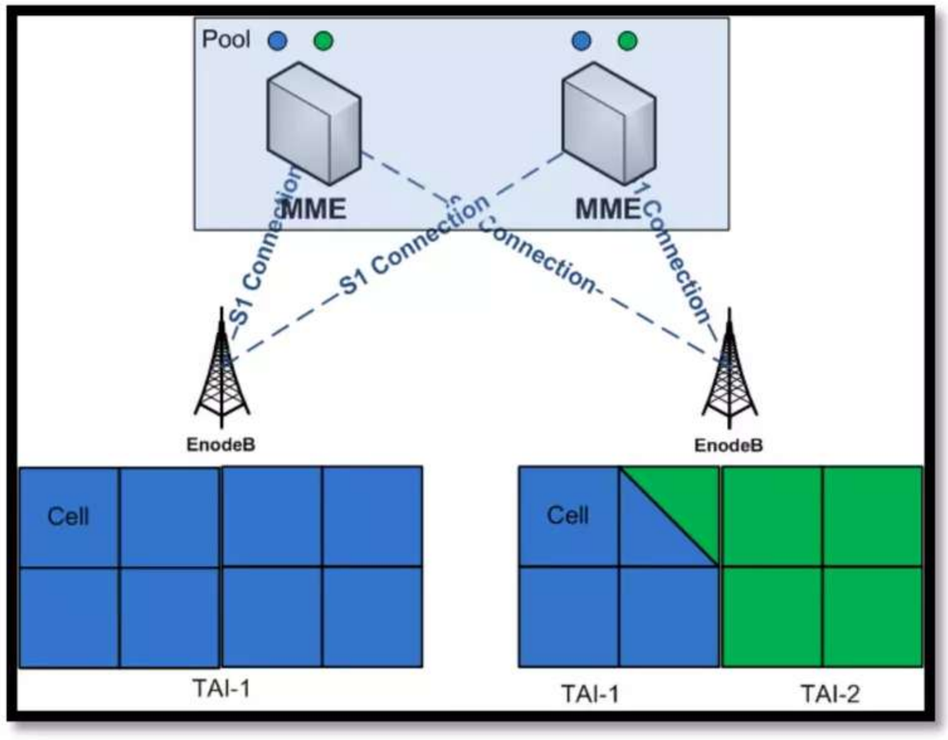
- Tracking area is the counterpart of the routing area in the 2G / 3G system as a reference of paging during MT call.
- TAI is composed of a group of cells.
- Tracking Area Identity is composed of MCC (Mobile Country Code) plus MNC (Mobile Network Code) plus TAC (Tracking Area Code).

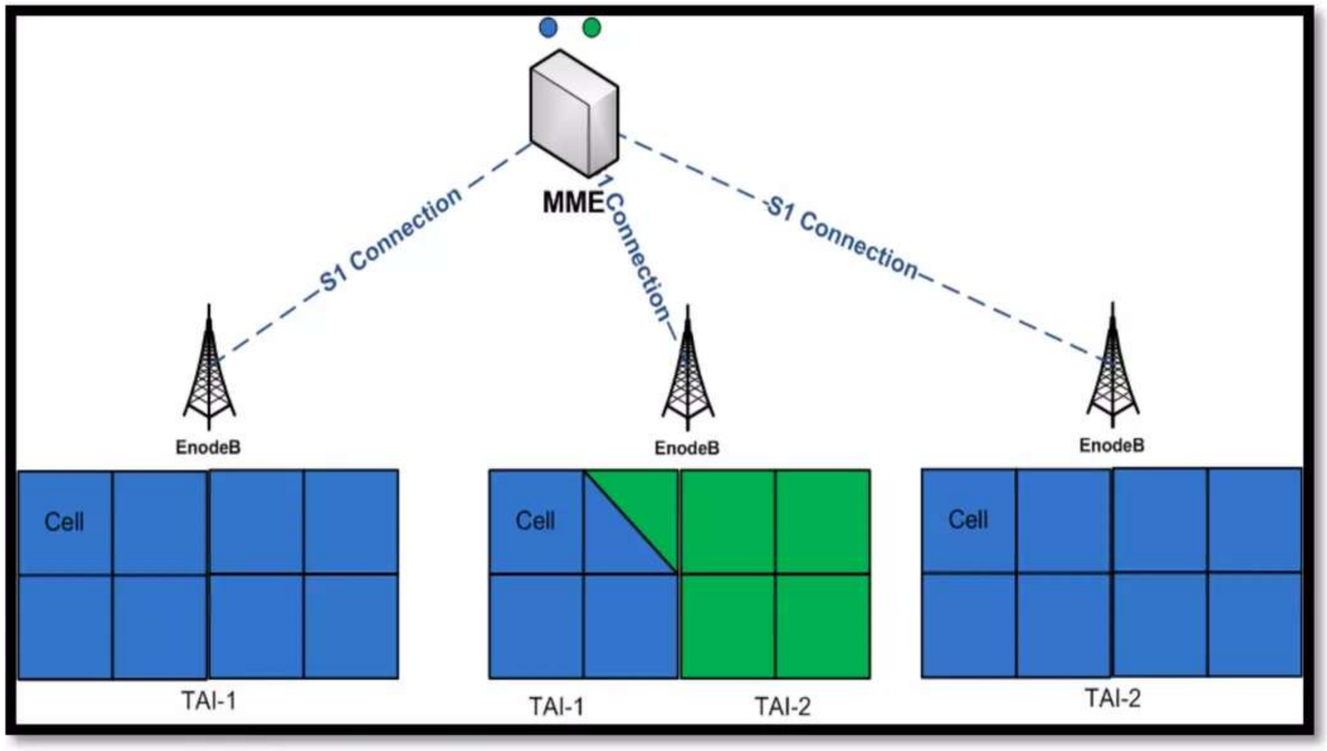


Tracking Area Update

Introduction

- A cell may co-exist in two TAI meaning a TAI may overlap.
- A UE reports several TAI on the same time as an advantage to reduce multiple RAI change.
- **Multi Tracking Area Registration :** UE only triggers TAU when moving to a cell belonging to a TA not in the TA list for that UE.
- **MME Pooling:** several MME handle the same tracking area.





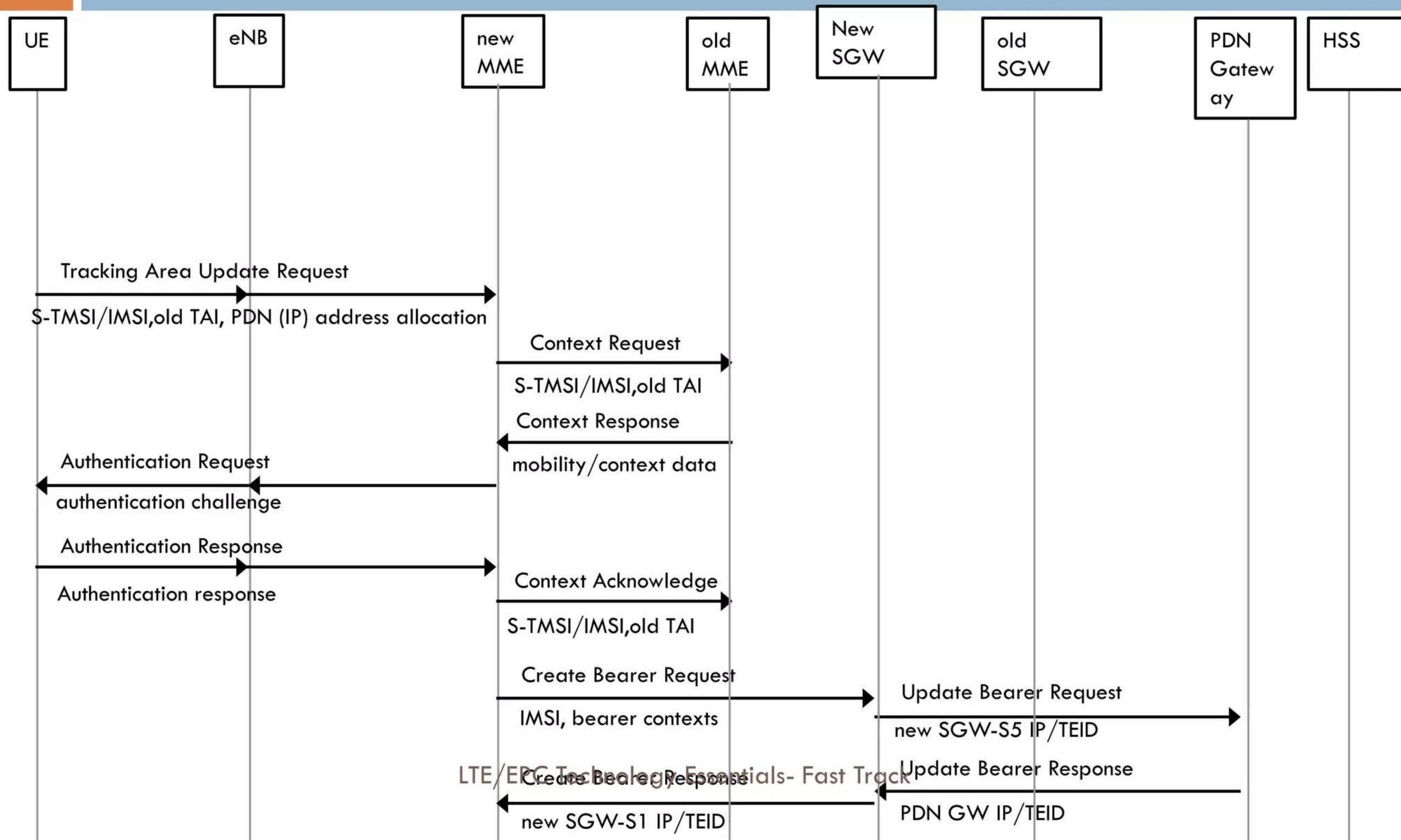
Tracking Area Update

Procedure

1. The UE sends ***TRACKING AREA UPDATE REQUEST*** with its current **S-TMSI and old TAI** to the eNB. This one has to forward the message to a MME. If the old MME cannot be selected, then a new MME must be chosen by the eNB.
2. The new MME must first of all get the identity (IMSI) of the subscriber and authenticate him/her. Therefore the new MME contacts the old one via **GTP-C *CONTEXT REQUEST***.
3. The ***CONTEXT RESPONSE*** contains **IMSI, authentication vectors**, but also all information about the currently **active SAE bearers of this user.**
4. After a successful authentication **the new MME** informs the old one, that it is ready to take control over the UE.
5. **The old MME** will now start a timer and **wait for the cancellation** of the subscriber record.
6. In parallel to the previous step the new MME **sends GTP-C *CREATE BEARER REQUEST*** to the SAE GW it has selected.
7. The message will trigger the setup of new S1 tunnels and trigger an update towards PDN GW. This will change the traffic path from PDN GW to new SAE GW to new eNB.

Tracking Area Update

Procedure



LTE/EPC Technology Essentials- Fast Track

Tracking Area Update

Procedure

```
◢ Non-Access-Stratum (NAS)PDU
    0010 .... = Security header type: Integrity protected and ciphered (2)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0xcb5940ab
    Sequence number: 4
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Tracking area update request (0x48)
    0... .... = Type of security context flag (TSC): Native security context (for KSIasme)
    .000 .... = NAS key set identifier:  (0) ASME
    .... 1... = Active flag: Bearer establishment requested
    .... .000 = EPS update type value: TA updating (0)
  ▷ EPS mobile identity - Old GUTI
  ◢ Tracking area identity - Last visited registered TAI
      Element ID: 0x52
      Mobile Country Code (MCC):
      Mobile Network Code (MNC):
      Tracking area code(TAC):
  ◢ EPS bearer context status
      Element ID: 0x57
      Length: 2
      0... .... = EBI(7): BEARER CONTEXT-INACTIVE
      .1.. .... = EBI(6): BEARER CONTEXT-ACTIVE
      ..1. .... = EBI(5): BEARER CONTEXT-ACTIVE
      ...0 .... = EBI(4) spare: False
      .... 0... = EBI(3) spare: False
      .... .0.. = EBI(2) spare: False
      .... ..0. = EBI(1) spare: False
      .... ...0 = EBI(0) spare: False
      0... .... = EBI(15): BEARER CONTEXT-INACTIVE
      .0.. .... = EBI(14): BEARER CONTEXT-INACTIVE
      ..0. .... = EBI(13): BEARER CONTEXT-INACTIVE
```

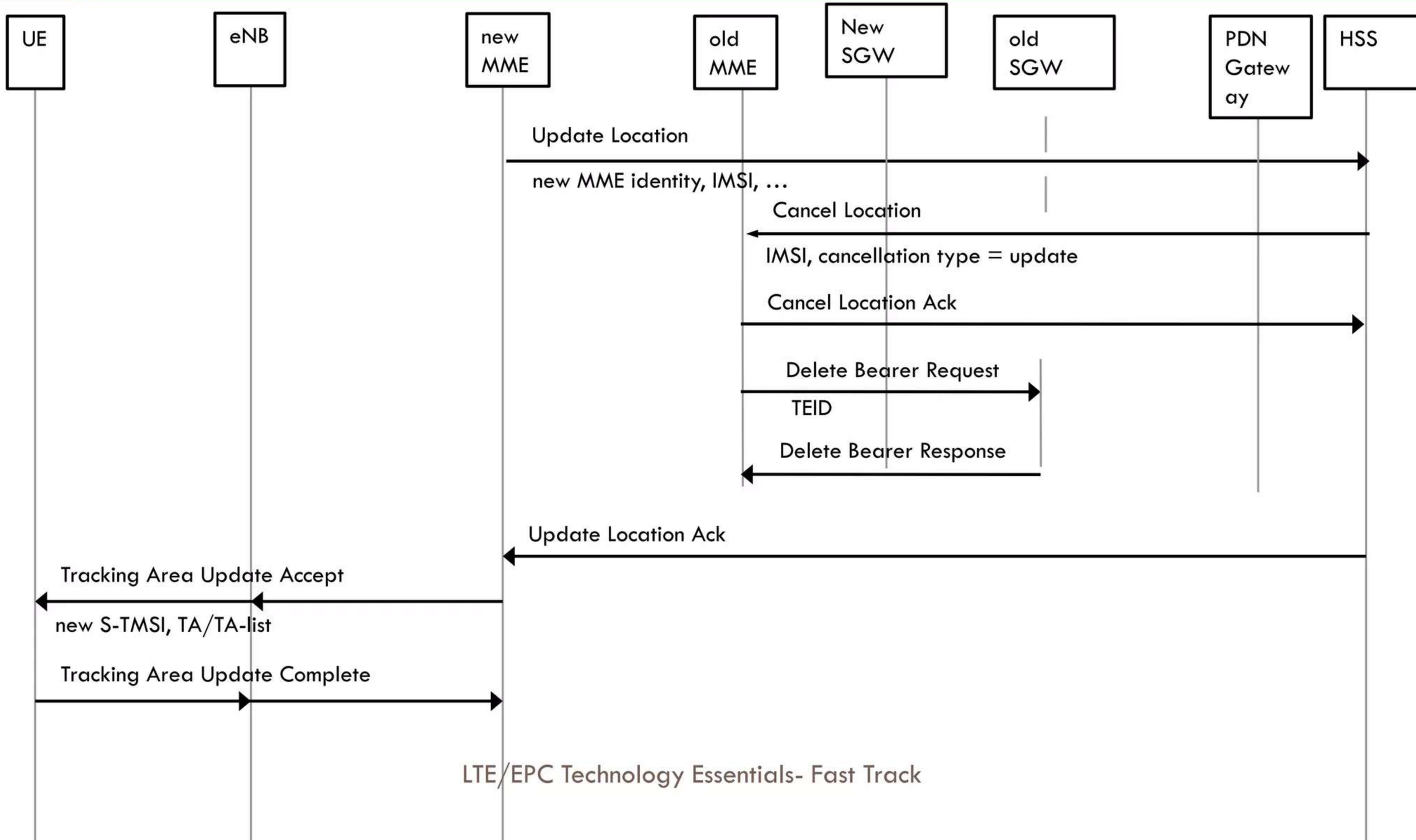
Tracking Area Update

Procedure

8. Also simultaneously with the previous steps the **MME will update the HSS.**
9. During this the HSS will cancel the subscriber record in the old MME. The **old MME will of course also delete the old tunnels** in the old SAE GW.
10. At the end the UE gets a NAS message ***TRACKING AREA UPDATE ACCEPT***. In it a new S-TMSI and new tracking area (or tracking area list) can be contained.
11. The UE has to acknowledge with ***TRACKING AREA UPDATE COMPLETE***.

Tracking Area Update

Procedure



Agenda

- Mobility and Session Management states
- UE and Network identifications
- LTE/EPC Bearer Types and QoS
- LTE/EPC Attach Procedure
- LTE/EPC Detach Procedure
- LTE/EPC Bearer Activation Procedure
- LTE/EPC Service Request Procedures
- Tracking Area Update
- **LTE/EPC Handover**

LTE/EPC Handover

Introduction

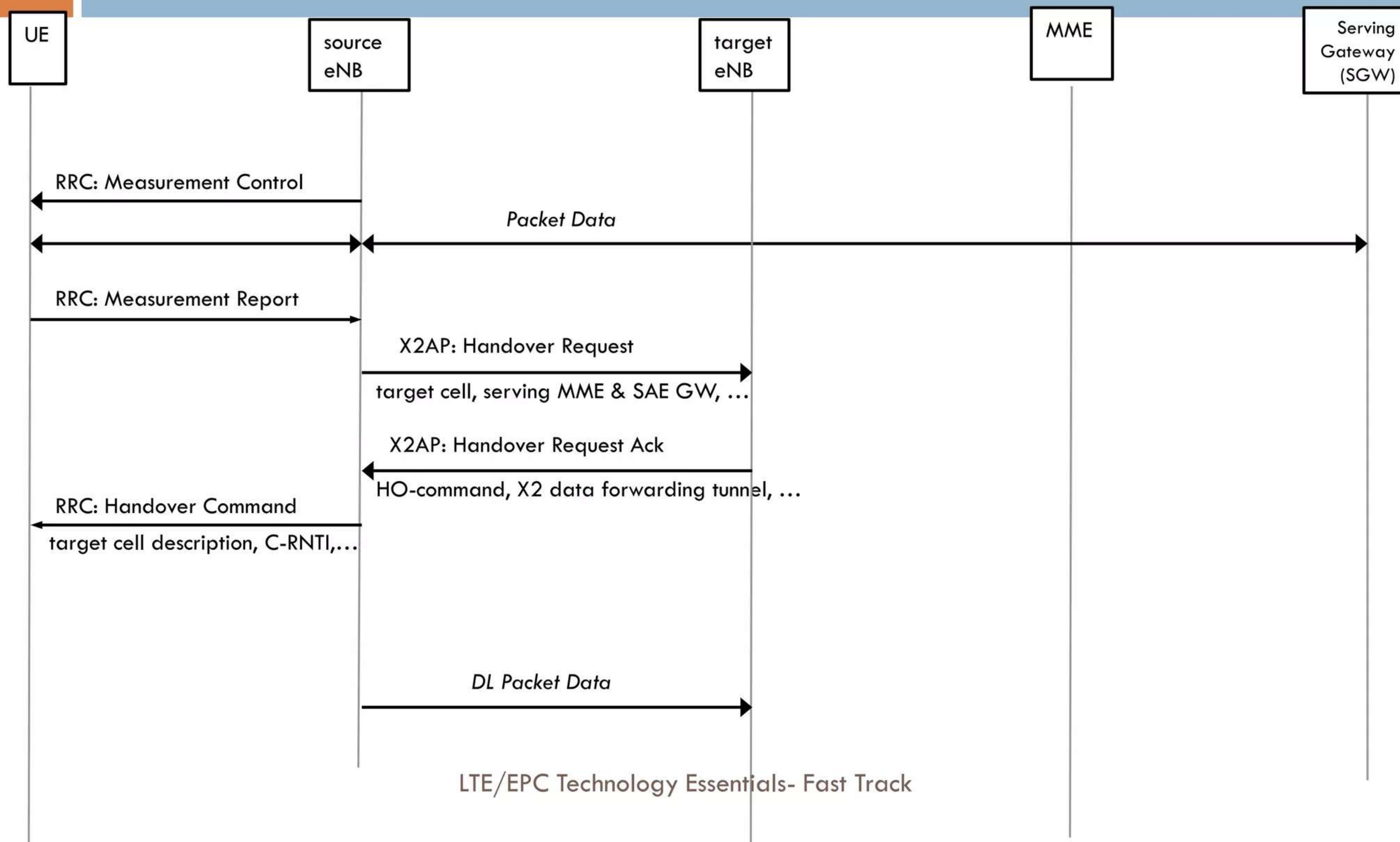
- UE is in **ECM_Connected** state.
- UE sends measurements and reports to the eNB to assist in the handover decision.
- Downlink Packets are forwarded from the source cell to the target cell.
- Target cell is selected by the network, not by the UE.
- Handover control in E-UTRAN (not in packet core), Only once the handover is successful, the packet core is involved.

Intra LTE/SAE Network Handover Types:

1. Intra eNB handover.
2. Inter eNB handover with X2 interface and without CN node relocation.
3.-Inter eNB handover without X2 Interface.

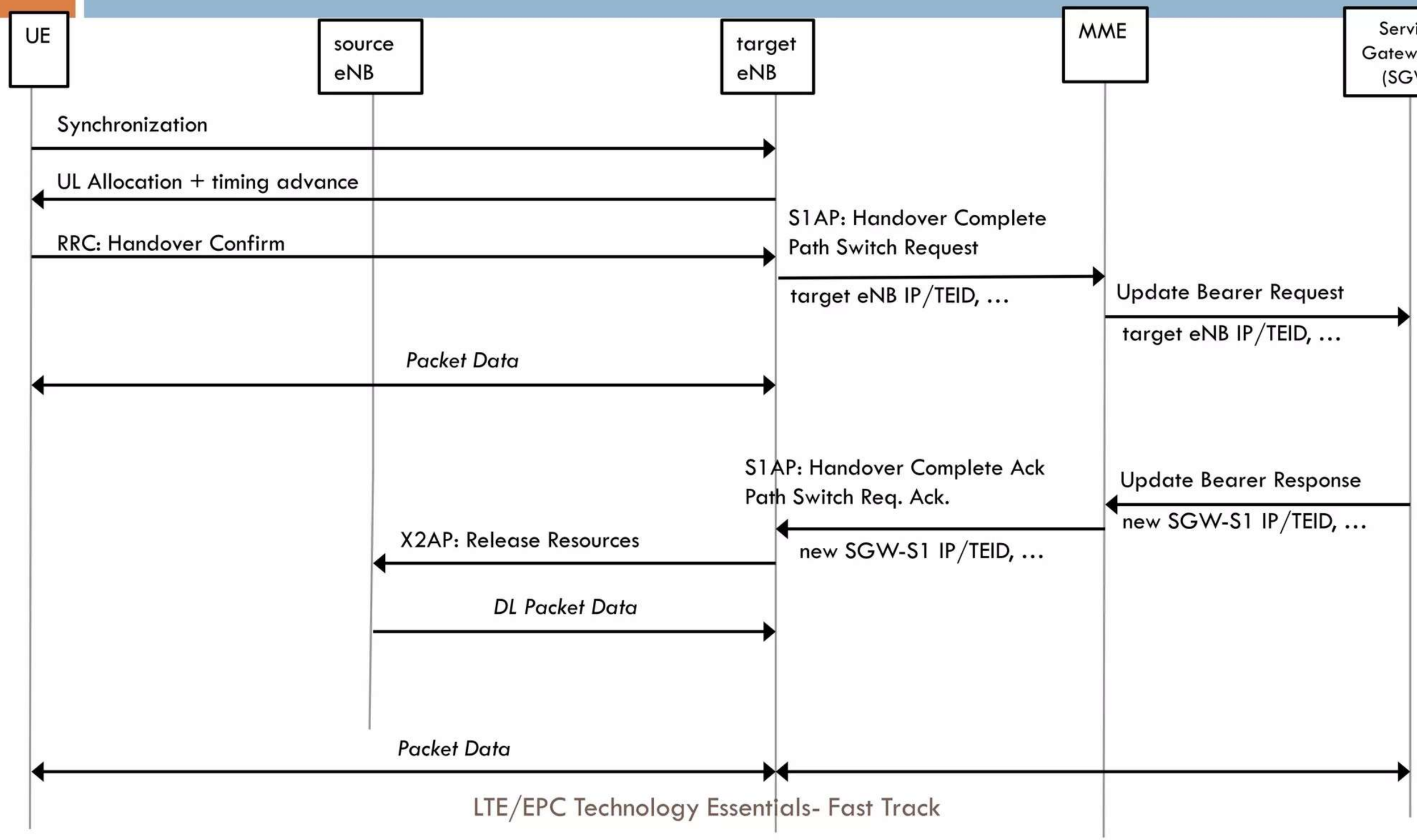
LTE/EPC Handover

X2 Based Handover



LTE/EPC Handover

X2 Based Handover



LTE/EPC Handover

X2 Based Handover

X2-based Handover – Handover Request

```
⊟ HandoverRequest
    <0... .... Extension Bit: False>
    <Sequence-Of Length: 6>
  ⊟ protocolIEs: 6 items
    ⊞ Item 0: id-Old-eNB-UE-X2AP-ID
    ⊞ Item 1: id-Cause
    ⊞ Item 2: id-TargetCell-ID
    ⊞ Item 3: id-GUMMEI-ID
    ⊞ Item 4: id-UE-ContextInformation
    ⊞ Item 5: id-UE-HistoryInfor
```

```
⊟ Item 4: id-UE-ContextInformation
  ⊟ ProtocolIE-Field
      id: id-UE-ContextInformation (14)
      <Enumerated Index: 0>
      criticality: reject (0)
      <Open Type Length: 65>
    ⊟ value
      ⊟ UE-ContextInformation
          <0... .... Extension Bit: False>
          <.0.. .... Optional Field Bit: False (subscriberProfileIDforRFP is NOT present)>
          <..0. .... Optional Field Bit: False (handoverRestrictionList is NOT present)>
          <...0 .... Optional Field Bit: False (locationReportingInformation is NOT present)>
          <.... 0... Optional Field Bit: False (iE-Extensions is NOT present)>
          mME-UE-S1AP-ID: 1
        ⊞ uESecurityCapabilities
        ⊞ aS-SecurityInformation
        ⊞ uEaggregateMaximumBitRate
          <Sequence-Of Length: 1>
        ⊞ e-RABs-ToBeSetup-List: 1 item
          <Octet String Length: 2>
          rRC-Context:
        ⊞ HandoverPreparationInformation
```

LTE/EPC Security And Authentication

Module Four

Hussien Mahmoud- PS Core/EPC Consultant

EPS Security And Authentication

EPS AKA

- EPS AKA: EPS Authentication and Key Agreement
- EPS AKA shall be based on USIM and **extensions to UMTS AKA**
- Access to E-UTRAN with **2G SIM shall not be granted,** R99 USIM will be accepted.
- UMTS AKA achieves **mutual authentication** between the **user** and the **network (MME,HSS)** by demonstrating knowledge of a pre-shared secret key *K*
- K is only known by the USIM and the AuC in the user's HSS.
- EPS AKA shall produce keys that are the basis of:
    1. C-plane Protection.
    2. U-plane protection.

EPS Security And Authentication

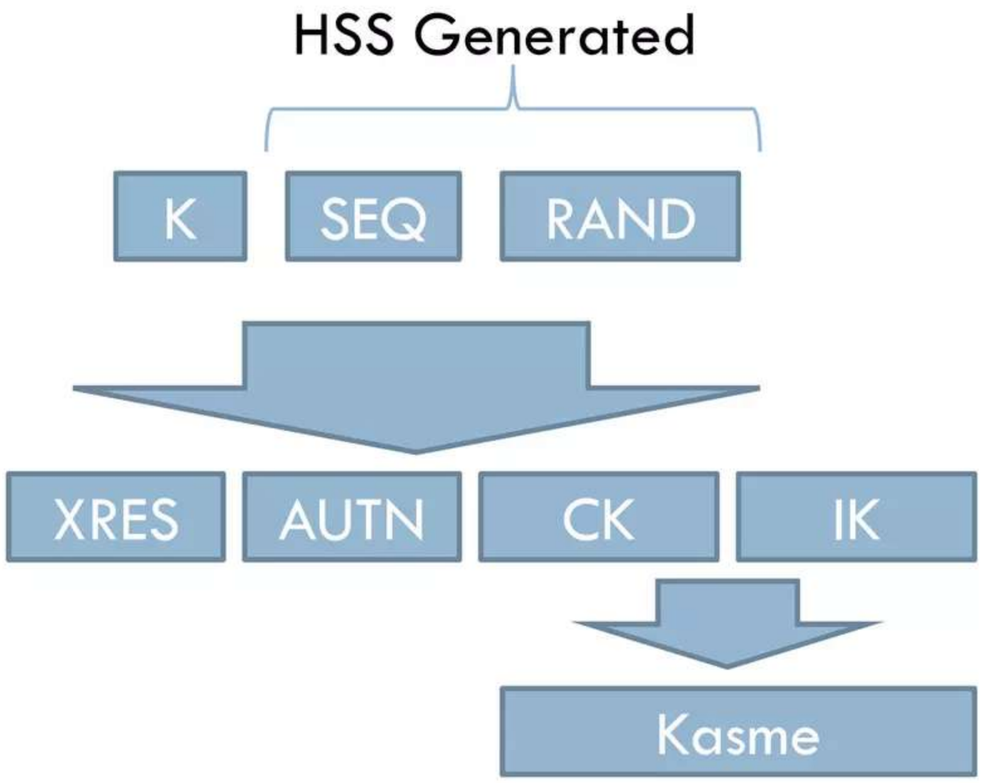
EPS Authentication Procedures

1. HSS replies with Authentication Vector (RAND, AUTN, Kasme, XRES).

2. MME sends UE (RAND, AUTN, Kasme).

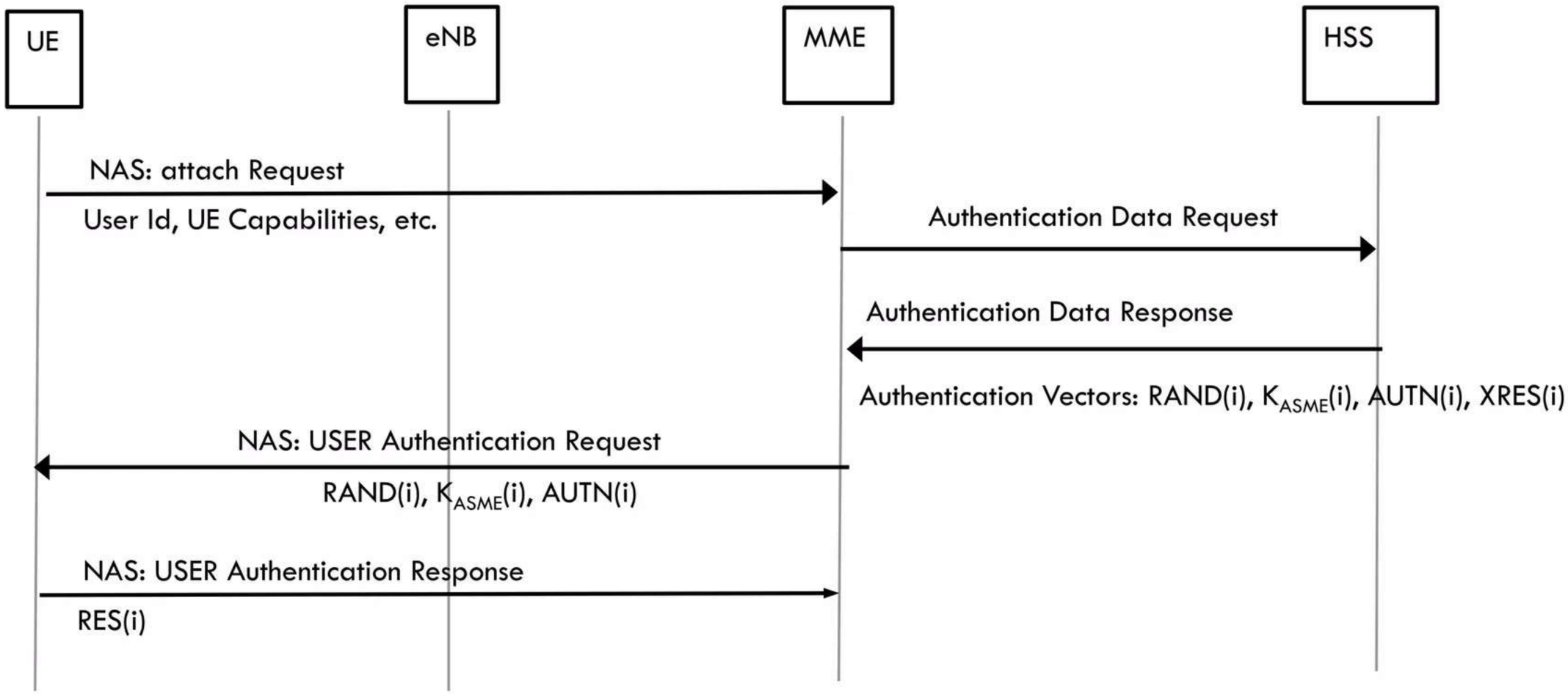
3. UE uses AKA algorithm to calculate (RES,AUTNue)

4. UE Compares AUTN,AUTNue→ **HSS Authenticated**
5. MME Compares RES,XRES →**UE Authenticated**



EPS Security And Authentication

EPS Authentication Procedures



EPS Security And Authentication

EPS Authentication Procedures

Authentication request from the MME to the UE

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-downlinkNASTransport (11)
      criticality: ignore (1)
    ⊟ value
      ⊟ DownlinkNASTransport
        ⊟ protocolIEs: 3 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
```

```
⊟ Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Authentication request (0x52)
    0000 .... = Spare half octet: 0
    .... 0... = Type of security context flag (TSC): Native security context (for KSIasme)
    .... .000 = NAS key set identifier:  (0) ASME
  ⊟ Authentication Parameter RAND - EPS challenge
      RAND value:
  ⊟ Authentication Parameter AUTN (UMTS and EPS authentication challenge) - EPS challenge
      Length: 16
    ⊟ AUTN value:
        SQN
        AMF
        MAC
```

Identities in the AIR:

- eNB-UE-S1AP-ID
- MME-UE-S1AP-ID

Authentication Parameters:

- RAND
- SQN
- AMF
- MAC

EPS Security And Authentication

EPS Security

Authentication Reply from the UE to the MME

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-uplinkNASTransport (13)
      criticality: ignore (1)
    ⊟ value
      ⊟ UplinkNASTransport
        ⊟ protocolIEs: 5 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
          ⊞ Item 3: id-EUTRAN-CGI
          ⊞ Item 4: id-TAI
```

```
  NAS-PDU: 075308ae97e0016aa10f13
⊟ Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Authentication response (0x53)
  ⊟ Authentication response parameter
      Length: 8
      RES: [redacted]
```

Identities in the AIR :

- eNB-UE-S1AP-ID
- MME-UE-S1AP-ID
- TAI (MNC,MCC,TAC)
- EUTRAN-CGI (PLMN id, MCC, MNC, Cell-id)

Authentication Parameters:

- RES

EPS Security And Authentication

EPS Security

```
◢ UE security capability - Replayed UE security capabilities
    Length: 5
    1... .... = EEA0: Supported
    .0.. .... = 128-EEA1: Not Supported
    ..0. .... = 128-EEA2: Not Supported
    ...0 .... = 128-EEA3: Not Supported
    .... 0... = EEA4: Not Supported
    .... .0.. = EEA5: Not Supported
    .... ..0. = EEA6: Not Supported
    .... ...0 = EEA7: Not Supported
    0... .... = EIA0: Not Supported
    .1.. .... = 128-EIA1: Supported
    ..1. .... = 128-EIA2: Supported
    ...0 .... = 128-EIA3: Not Supported
    .... 0... = EIA4: Not Supported
    .... .0.. = EIA5: Not Supported
    .... ..0. = EIA6: Not Supported
    .... ...0 = EIA7: Not Supported
    1... .... = UEA0: Supported
    .1.. .... = UEA1: Supported
    ..1. .... = UEA2: Supported
    ...0 .... = UEA3: Not Supported
    .... 0... = UEA4: Not Supported
    .... .0.. = UEA5: Not Supported
    .... ..0. = UEA6: Not Supported
    .... ...0 = UEA7: Not Supported
    0... .... = Spare bit(s): 0x00
    .1.. .... = UMTS integrity algorithm UIA1: Supported
    ..1. .... = UMTS integrity algorithm UIA2: Supported
```

EPS Security And Authentication

EPS Security

Security Mode Command from the MME to the UE

```
⊟ S1AP-PDU: initiatingMessage (0)
  ⊟ initiatingMessage
      procedureCode: id-downlinkNASTransport (11)
      criticality: ignore (1)
    ⊟ value
      ⊟ DownlinkNASTransport
        ⊟ protocolIEs: 3 items
          ⊞ Item 0: id-MME-UE-S1AP-ID
          ⊞ Item 1: id-eNB-UE-S1AP-ID
          ⊞ Item 2: id-NAS-PDU
```

```
⊟ Non-Access-Stratum (NAS)PDU
    0011 .... = Security header type: Integrity protected with new EPS security context (3)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0x673cbd6b
    Sequence number: 0
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Security mode command (0x5d)
  ⊞ NAS security algorithms - Selected NAS security algorithms
    0000 .... = Spare half octet: 0
    .... 0... = Type of security context flag (TSC): Native security context (for KSIasme)
    .... .000 = NAS key set identifier:  (0) ASME
  ⊞ UE security capability - Replayed UE security capabilities
  ⊞ IMEISV request
```

NAS Selected Security Algorithm:

- Integrity Algorithm (ex. 128-EIA1)
- Ciphering Algorithm (ex. EEA0)

UE Security Capability

IMEISV Request

EPS Security And Authentication

EPS Security

•**EPS Authentication,** Mutual Authentication between UE,MME and HSS.
Base Key: K
Derived Keys: Kasme

•**Core network (NAS) signaling,** integrity and confidentiality protection terminate in MME.
Base Key: Kasme
Derived Keys: Knas(int), Knas(enc)

•**Radio network (RRC) signaling,** integrity and confidentiality protection terminate in eNodeB.
Base Key: KeNB
Derived Keys: Krrc(int), Krrc(enc)

•**For User plane protection,** to protect the traffic between UE and EnodeB Encryption terminates in eNodeB
Base Key: KeNB
Derived Keys: Krrc(int), Krrc(enc)

DNS Functionalities in LTE

Module Five

Hussien Mahmoud- PS Core/EPC Consultant

DNS Functionalities in LTE

Introduction

A records

•A stands for IPv4 records lookup.

•Map Host names to IP's.

AAA Records

•AAAA stands for IPv6 record lookup.

•Map Host names to IP's.

```
◢ Domain Name System (response)
    [Request In: 3]
    [Time: 0.001164000 seconds]
    Transaction ID: 0x6e57
  ▷ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 1
  ◢ Queries
    ◢ topon.s5-pgw.saegw1.site1.epc.mn[redacted].mc[redacted].3gppnetwork.org: type AAAA, class IN
        Name: topon.s5-pgw.saegw1.site1.epc.mnc[redacted].mcc[redacted].3gppnetwork.org
        [Name Length: 59]
        [Label Count: 9]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
```

DNS Functionalities in LTE

Introduction

Name Authority Pointer (NAPTR)

•Resource records specify lookup services

•NAPTR will produce a new domain label or URI

•S-NAPTR: Straightforward NAPTR is used to add particular services to a DNS entry.

•The S-NAPTR also simplifies the use of NAPTR by limiting the NAPTR flags only to "a", "s" and ""

NAPTR Reply

•the next lookup is an SRV records (**The "S" Flag**).

•the next lookup is A, AAAA records. i.e. IP record (**The "A" Flag**).

•more NAPTR RR lookups are to be performed (**empty flag " "**).

DNS Functionalities in LTE

Introduction

```
▷ User Datagram Protocol, Src Port: 57833 (57833), Dst Port: 53 (53)
◢ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x671e
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ◢ Queries
    ◢ lte.lab.apn.epc.mnc[redacted].mcc[redacted].3gppnetwork.org: type NAPTR, class IN
        Name: lte.lab.apn.epc.mnc[redacted].mcc[redacted].3gppnetwork.org
        [Name Length: 45]
        [Label Count: 8]
        Type: NAPTR (Naming Authority Pointer) (35)
        Class: IN (0x0001)
  ▷ Additional records
```

DNS Functionalities in LTE

Introduction

```
◢ Domain Name System (query)
    [Response In: 6]
    Transaction ID: 0x6d92
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ◢ Queries
    ◢ tac-lb0a.tac-hb00.tac.epc.mnc[redacted].mcc[redacted].3gppnetwork.org: type NAPTR, class IN
        Name: tac-lb0a.tac-hb00.tac.epc.mnc[redacted].mcc[redacted].3gppnetwork.org
        [Name Length: 55]
        [Label Count: 8]
        Type: NAPTR (Naming Authority Pointer) (35)
        Class: IN (0x0001)
  ▷ Additional records
```

DNS Functionalities in LTE

Introduction

DNS Server Selection SRV

Allows DNS administrators to use pool of servers for a single domain, to move services from host to host, and to designate some hosts as primary servers for a service from a pool of hosts.

For the flag "s" case the topologically aware naming restriction applies to the targets in the SRV record, and not the NAPTR record replacement target.

Entry

topon.nodes.sgw.be.epc IN SRV 1 100 2123 test-SGW.sgw.be.epc.mnc99.mcc999.3gppnetwork.org.

DNS Functionalities in LTE

Introduction

```
◢ Queries
  ▷ tac-lb0a.tac-hb00.tac.epc.mn[redacted].mc[redacted].3gppnetwork.org: type NAPTR, class IN
◢ Answers
  ◢ tac-lb0a.tac-hb00.tac.epc.mn[redacted].mc[redacted].3gppnetwork.org: type NAPTR, class IN, order 100, preference 100, flags s
      Name: tac-lb0a.tac-hb00.tac.epc.mn[redacted].mc[redacted].3gppnetwork.org
      Type: NAPTR (Naming Authority Pointer) (35)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 74
      Order: 100
      Preference: 100
      Flags Length: 1
      Flags: s
      Service Length: 19
      Service: x-3gpp-sgw:x-s5-gtp
      Regex Length: 0
      Regex:
      [Replacement Length: 47]
      Replacement: _nodes._sgw.epc.mn[redacted].mc[redacted].3gppnetwork.org
```

DNS Functionalities in LTE

Introduction

<"topon" | "topoff"> . <single-label-interface-name> . <canonical-node-name>

•Where the first label is "topon" or "topoff" to indicate whether or not collocated and topologically close node selection shall be preferred,

•"single-label-interface-name" is a single label used to name a specific interface on a node (e.g. Eth-0, S8, vip, board3)

•"canonical-node-name" is a the canonical name of a specific node. When comparing host name FQDNs to find out whether the nodes are actually the same, the first two labels of the host name FQDN shall be ignored.

DNS Functionalities in LTE

SGW Selection

SGW FQDN=
tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Service Parameters =
x-3gpp-sgw:x-s5-gtp

•Topological matching with "topon" shall have higher importance in ordering which DNS records are used than the S-NAPTR ordering

DNS Functionalities in LTE

SGW Selection

```
◢ Additional records
  ◢ topon.s5-sgw.saegw1.site1.epc.mnc[redacted].mcc[redacted].3gppnetwork.org: type A, class IN, addr 192.1[redacted]
      Name: topon.s5-sgw.saegw1.site1.epc.mnc[redacted].mcc[redacted].3gppnetwork.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 4
      Address: 192.1[redacted] (192.1[redacted])
  ◢ topon.s11-sgw.saegw1.site1.epc.mnc[redacted].mcc[redacted].3gppnetwork.org: type A, class IN, addr 192.1[redacted]
      Name: topon.s11-sgw.saegw1.site1.epc.mnc[redacted].mcc[redacted].3gppnetwork.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 4
      Address: 192.1[redacted] (192.1[redacted])
```

DNS Functionalities in LTE

PGW Selection

- PGW selection is performed by the MME/SGSN at initial attach or PDN connection establishment.
- *Query is done based on APN.*
- *No Topology logic included.*

PGW FQDN=

<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Service Parameters =

x-3gpp-pgw:x-s5-gtp

DNS Functionalities in LTE

Service Parameters

PGW

- **Discovering a PGW for a 3GPP Access - S8/Gp roaming case** → "x-3gpp-pgw:x-s8-gtp", "x-3gpp-pgw:x-s8-pmip", "x-3gpp-ggsn:x-gp", etc.
- **Discovering a PGW for a 3GPP Access - S5/Gn intra-operator existing PDN** → "x-3gpp-pgw:x-s5-gtp", "x-3gpp-pgw:x-s5-pmip", "x-3gpp-ggsn:x-gn"
- **Discovering a PGW for a non-3GPP Access – S2a/S2b initial attach for roaming and non-roaming** →"x-3gpp-pgw:x-s2a-pmip", "x-3gpp-pgw:x-s2b-pmip", "x-3gpp-pgw:x-s2a-mipv4"
- **Discovering a PGW for a non-3GPP Access – S2a/S2b initial attach and chained S2a/S2b with GTP or PMIPv6 based S8** → "x-3gpp-pgw:x-s2a-pmip", "x-3gpp-pgw:x-s2b-pmip"

DNS Functionalities in LTE

Service Parameters

SGW

- **SGW Selection during TAU with SGW change - 3GPP roaming case** →"x-3gpp-sgw:x-s8-gtp" or "x-3gpp-sgw:x-s8-pmip"
- **SGW Selection during TAU with SGW change - non-roaming case** → "x-3gpp-sgw:x-s5-gtp" and/or "x-3gpp-sgw:x-s5-pmip"

DNS Functionalities in LTE

Service Parameters

Various

- **Services of a PGW from PGW node name** → "x-3gpp-pgw:x-s5-pmip" , "x-3gpp-pgw:x-s8-pmip" , "x-3gpp-pgw:x-s5-gtp" , "x-3gpp-pgw:x-s8-gtp", etc.
- **Services of a MME from MME node name** → " x-3gpp-mme:x-s10 ", "x-3gpp-mme:x-s11", etc.
- **Services of an SGSN from a P-TMSI** → "x-3gpp-sgsn:x-gn", "x-3gpp-sgsn:x-gp", "x-3gpp-sgsn:x-s3", "x-3gpp-sgsn:x-s4" , etc.

Thanks

Hussien Mahmoud- PS Core/EPC Consultant