Evolved Packet Core (EPC) – 4G

Course Goals

By the end of this course you will have a deep understanding about the following topics in LTE

- Introduction
  - Motivation for LTE (4G)
  - How is LTE different from other technologies ?
  - Evolution in LTE.
- Network Architecture – Introduction
  - E-UTRAN Architecture
  - EPC Architecture
  - LTE Architecture Summary
- Identifiers in LTE – (IMSI, GUTI, TAC, APN, MNC, MCC)
- Interfaces in LTE EPC
- LTE Protocol Stack
- LTE QoS
  - Bearers in LTE
  - Traffic Flow Templates

Course Goals Contd.

By the end of this course you will have a deep understanding about the following topics in LTE

- EPC Core Elements – Deep Dive
  - MME
  - HSS
  - SGW
  - PGW
  - PCRF
- Security in LTE
  - Authentication
  - Encryption
  - Integrity
  - Wireshark Logs from real network – Analysis and call/message flow
- LTE UE Attach Call flow
  - Review message flow.
  - Wireshark logs from real network – Analysis
- LTE Roaming
  - Review of 3GPP and GSMA based architectures

Further Your Learning with These courses

After Completing this course if you want to further your learning of 4G you can check out the course below (referral Code Included) -

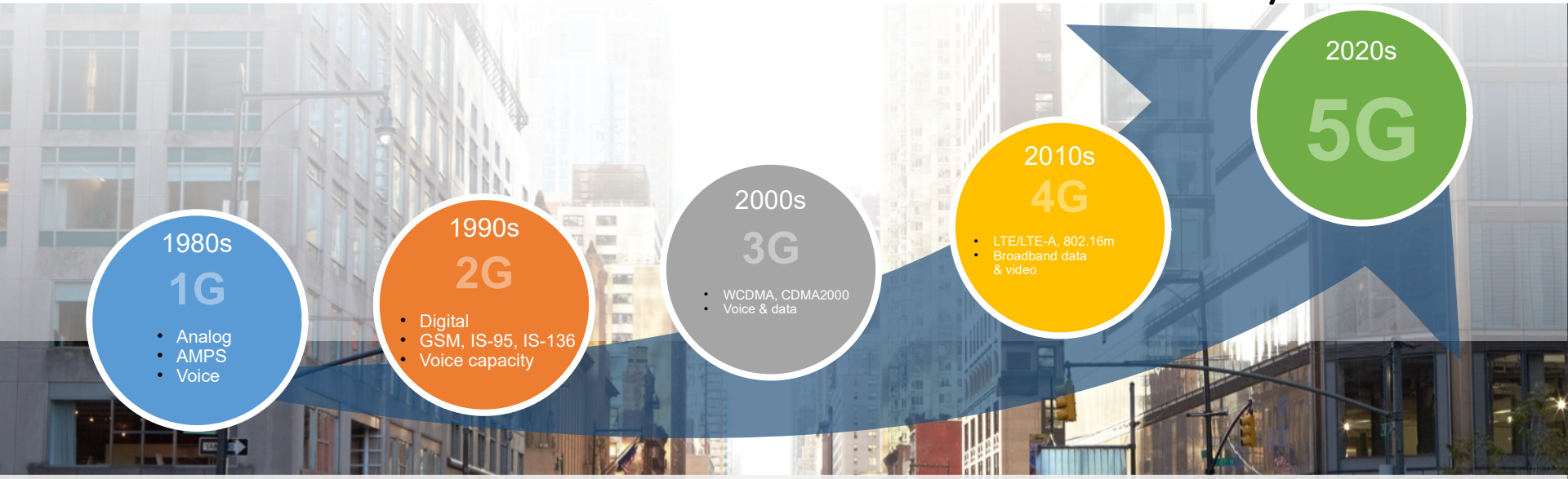
https://www.udemy.com/course/4g-lte-epc-advanced-troubleshooting-using-wireshark/?referralCode=2BA5F6FDE6C76FC74EA5

For becoming an expert on 5G I also recommend checking out this course (referral Code Included) -

https://www.udemy.com/course/5g-core-architectures-concepts-and-call-flows/?referralCode=399C46706125617AA682

Introduction:
Motivation for 4G LTE

Time For The Next Generation of Mobility?



Market Disruptors
- Open Source Software
- Hyper Connectivity
- Internet of Everything

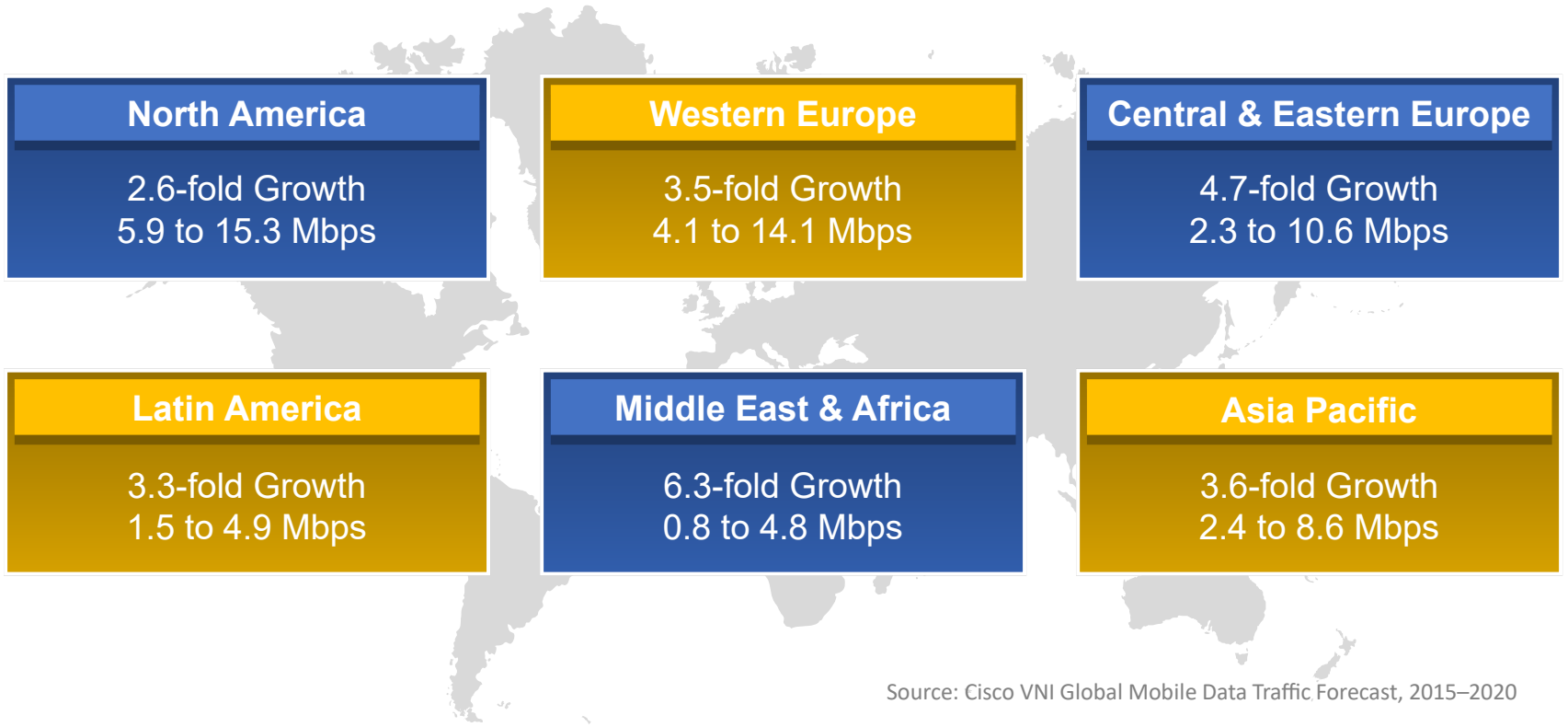
Business Models
- Consumption based
- Agile & On Demand
- Software Innovations

Technology Landscape
- Virtualization
- Cloud Workloads
- Programmability

Source: Cisco

Global Mobile Speed Growth

Average Mobile Speed Will More Than Triple from
2.0 Mbps (2015) to 6.5 Mbps (2020)



Source: Cisco VNI Global Mobile Data Traffic Forecast, 2015–2020

Comparison of Wireless technologies

Generation	1G	2G	3G	4G	5G
Deployment	1970-84	1980-89	1990-2002	2000-18	2018-2020+
Throughput	2Kbps	14-64 Kbps	2 Mbps	200 Mbps	1Gbps+
Services	Analog Voice	Digital Voice SMS,MMS	Integrated HD Video and data	High Speed Data, Voice over LTE (VoLTE)	Ultra-low Latency, massive IoT,V2V
Underlying Technology std.	AMPS,TACS	D-AMPS,CDMA (IS-95)	CDMA2000, EVDO,W-CDMA,HSPA+	LTE, VoLTE, LTE Advanced, LTE Advanced Pro	5G-NR

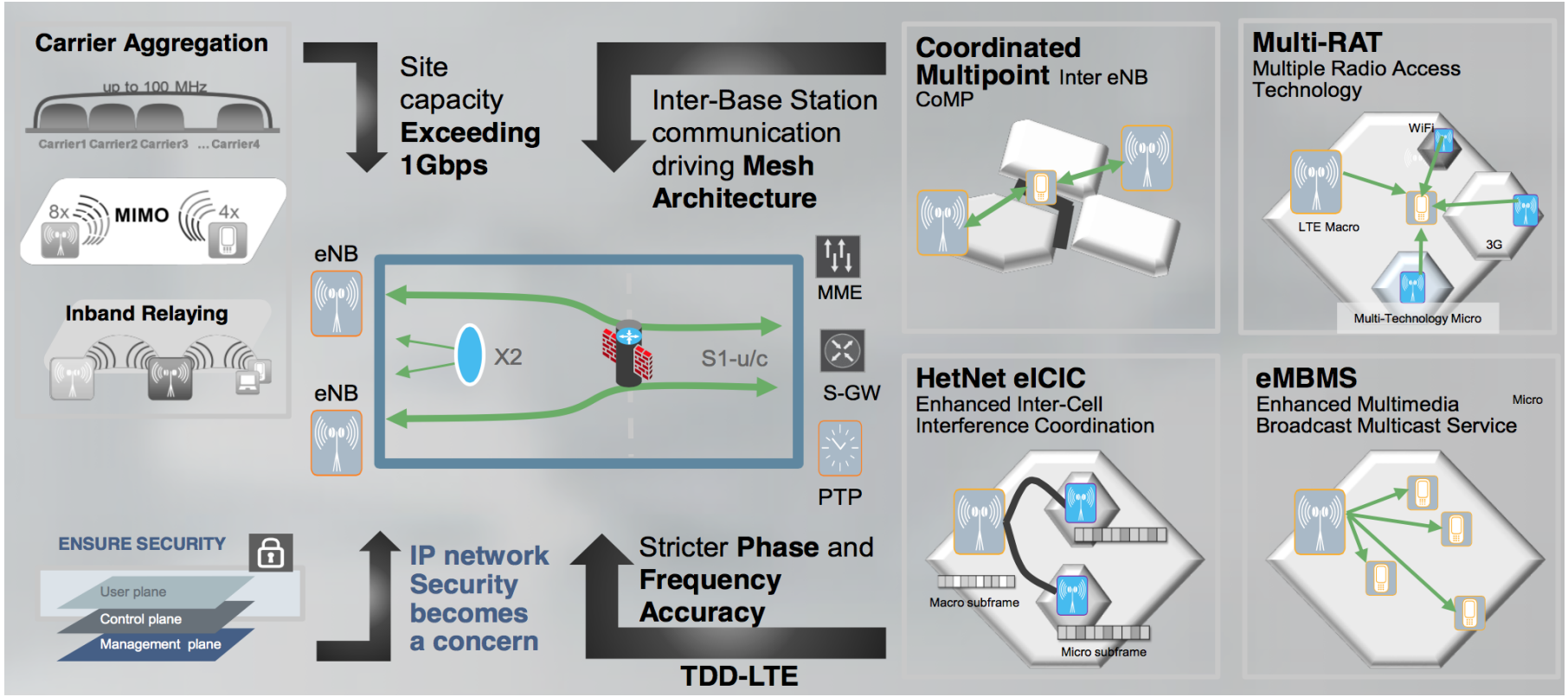
Introduction:
How is LTE different from the previous technologies ?

How is LTE different ?

LTE benefits (Compared to 3G) include :

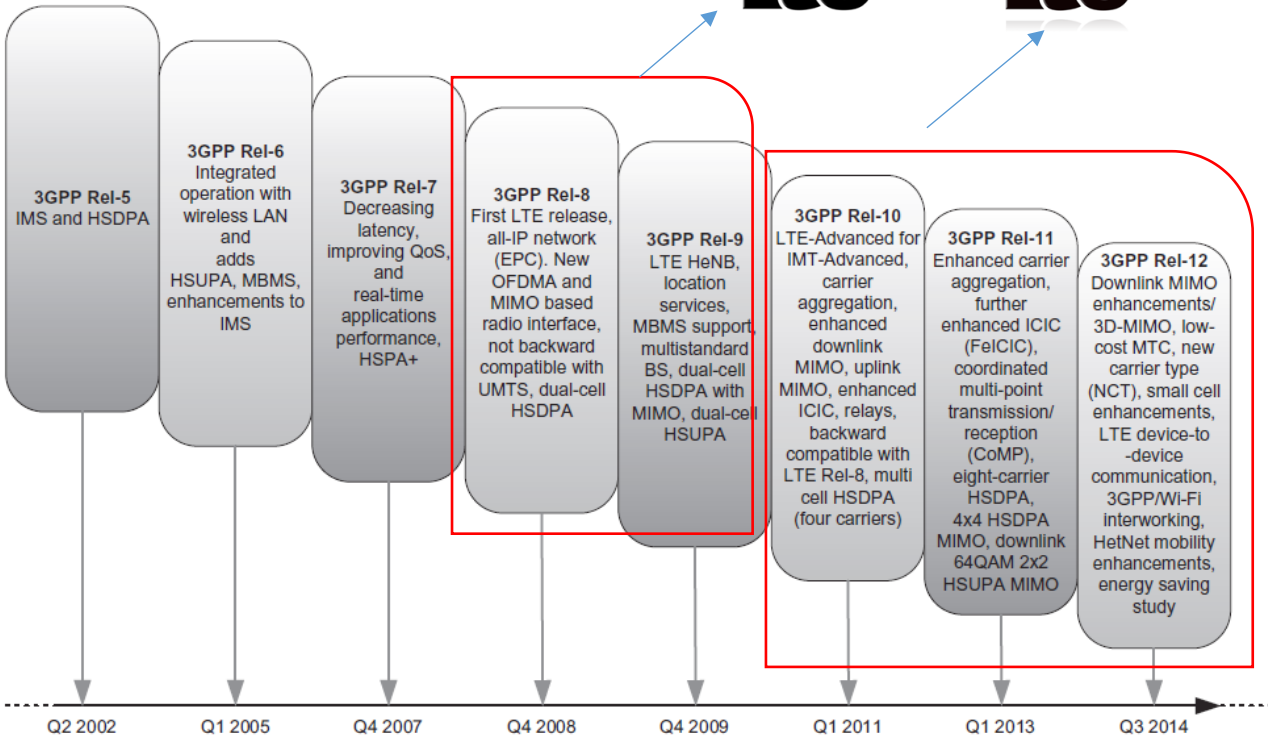
- High Data rates
- Reduced Latency for user applications.
- Improved end-user throughputs for applications such as a Voice and Video
- Flexibility of radio frequency deployment since LTE can be deployed in various bandwidth configurations (1.4, 3, 5, 10, 15, 20 MHz)
- Multiple Input Multiple Output (MIMO)
- Flat all-IP network with fewer network elements which leads to lower latency.
- Offers a TDD solution (LTE-TDD) in addition to FDD (LTE-FDD)

4G, LTE and LTE-A Drivers



Introduction: Evolution in LTE

Evolution in LTE

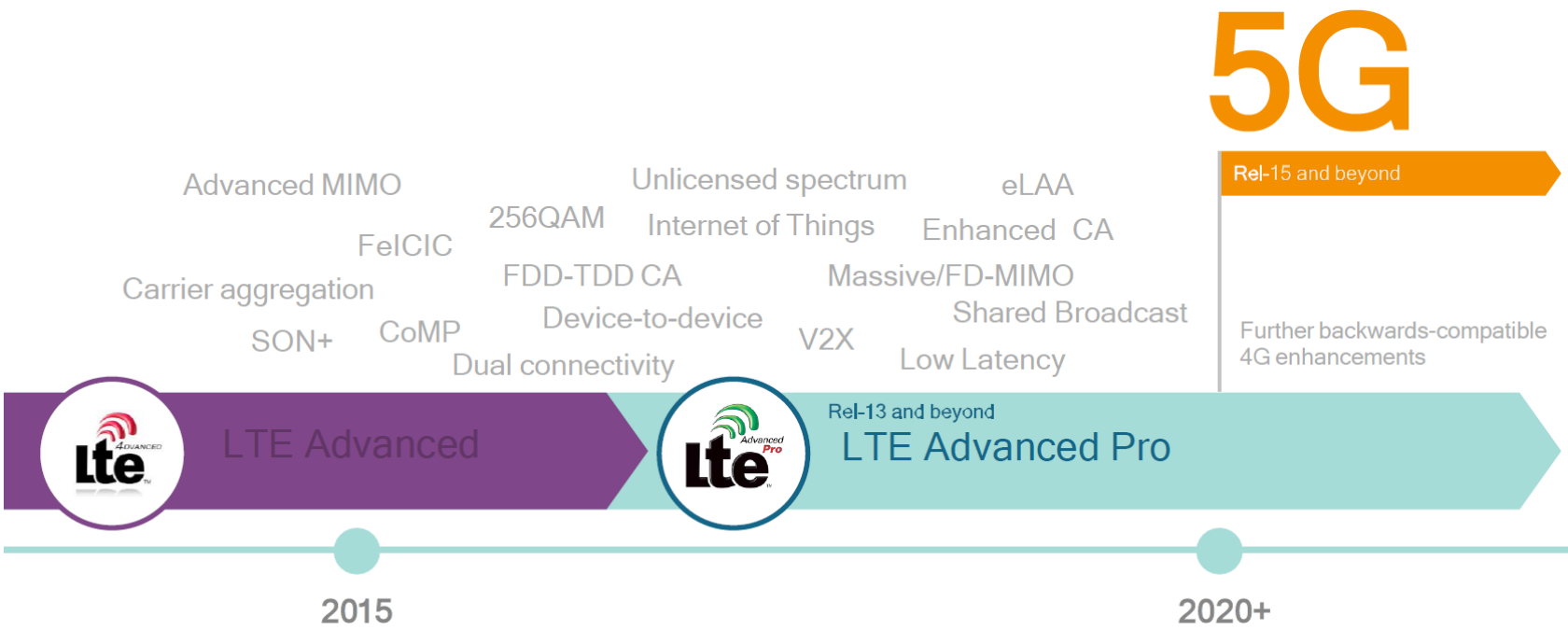


3GPP Rel. 13,14

*Source – 3GPP

Progress LTE capabilities towards 5G

In parallel driving 4G and 5G to their fullest potential



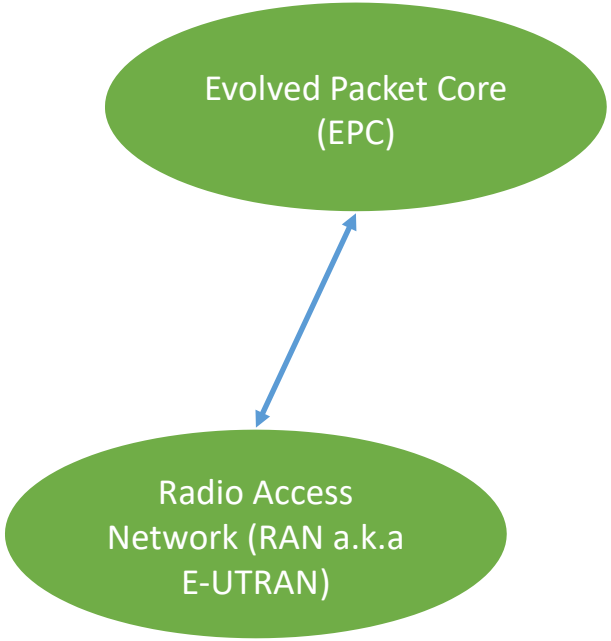
*Source – Qualcomm

Network Architecture – Introduction:

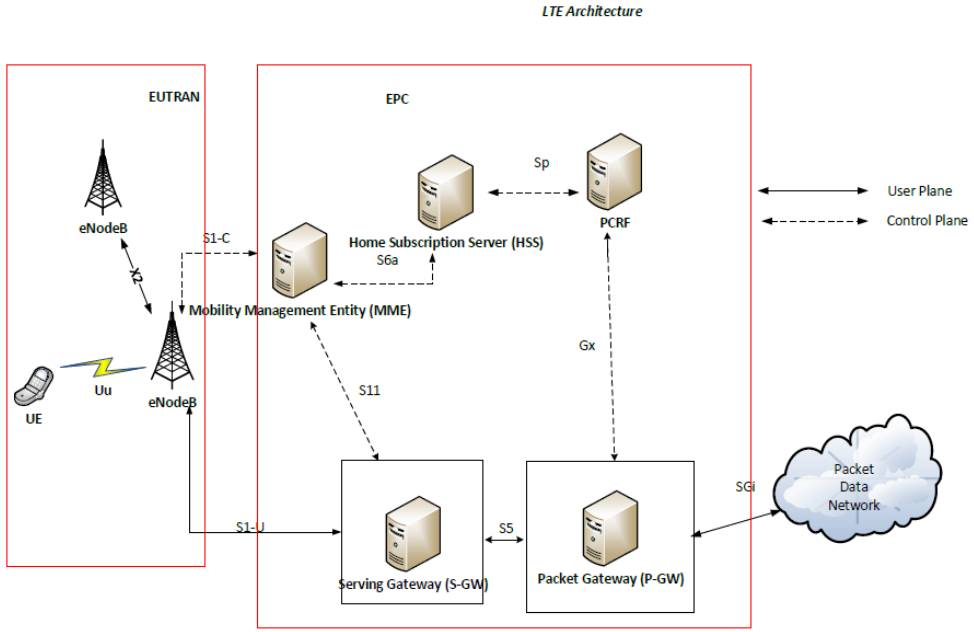
Network Architecture in LTE:

LTE architecture is composed of 2 parts –

- Radio Access Network: Evolved UTRA Network (E-UTRAN)
- Core Network Architecture : Evolved Packet Core (EPC)



Network Architecture in LTE contd:



eNodeB Functions:

- Radio Resource management, radio bearer control, radio admission control, connection mobility control, uplink/downlink scheduling
- IP header compression and ciphering of the User data stream.
- MME selection
- Paging
- CMAS

MME Functions:

- Non-Access Stratum (NAS) signaling (attachment, bearer setup/deletion)
- NAS signaling security
- Signaling for mobility between 3GPP access networks
- Idle mode user tracking
- Tracking Area list mgmt.
- PDN gateway, S-GW selection
- Roaming – S6a interface to HSS
- Authentication

Serving Gateway Functions:

- Local mobility anchor for inter-eNodeB handover.
- EUTRAN downlink packet buffering-while idle UE is being paged.
- Lawful intercept
- Packet routing and forwarding
- Transport level packet marking (UL/DL)
- Accounting for inter-operator charging.
- Accounting per UE

Home Subscriber Server:

- Storage of Sub Data (Auth keys, QoS profile, APN profile etc.).
- Address of currently serving MME, TA

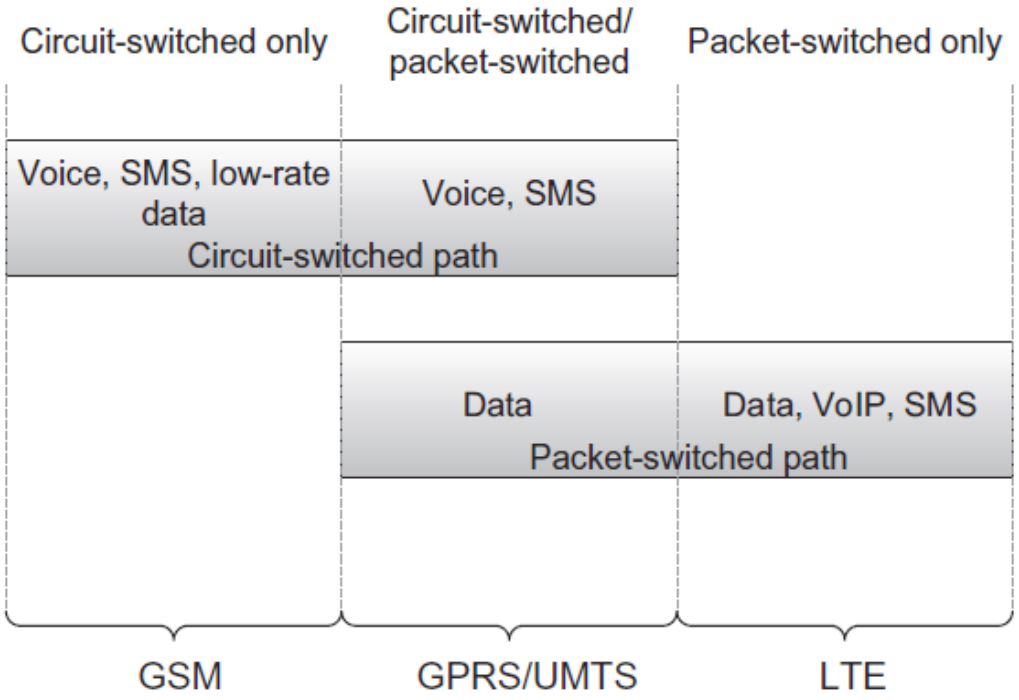
PDN Gateway:

- Lawful Intercept
- IP address allocation
- Transport level marking for DL
- Downlink rate enforcement based on AMBR (Aggregate Maximum Bit Rate)
- Accounting per UE

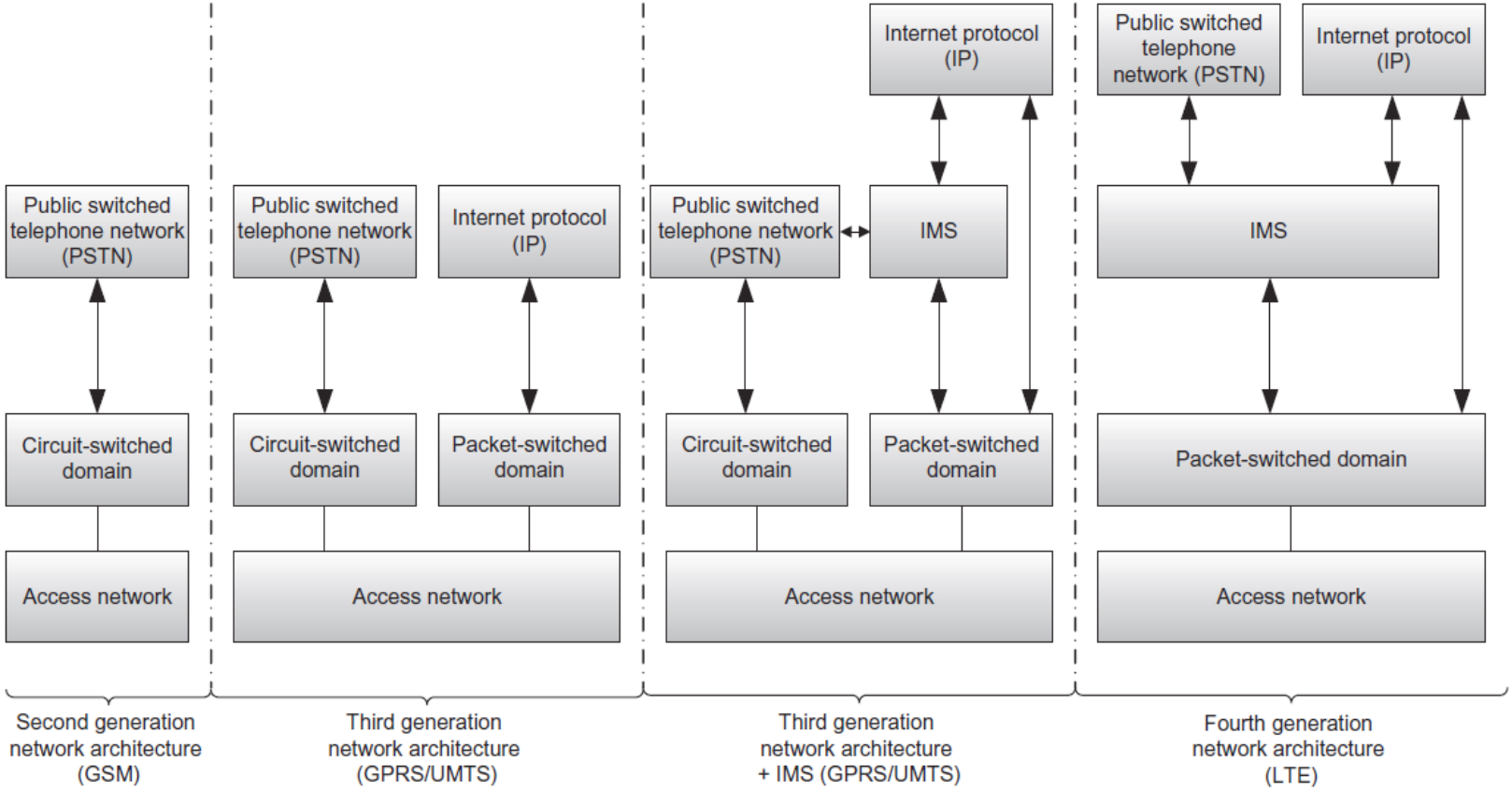
Policy Charging and Rate Function (PCRF):

- Interfaces with Proxy – Call session control function.
- Interfaces with PDN – GW to convey policy decisions and profiles.
- Decides how services will be treated in PDN GW according to User policy.

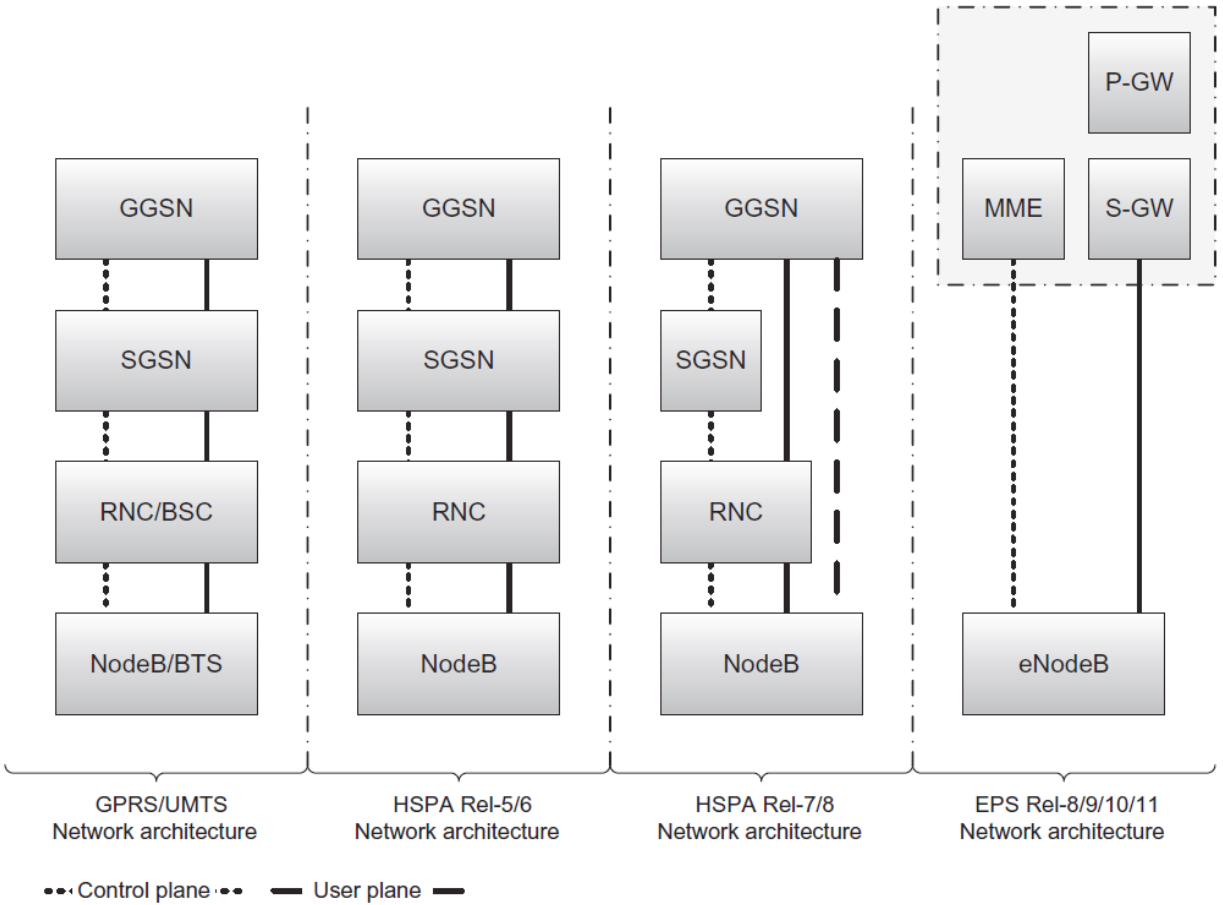
Evolution of Network Services



Evolution of network architecture through cellular generations.



Evolution of 3GPP Architecture.



Network Architecture – Introduction:

E-UTRAN- Evolved UTRA Network

Network Architecture in LTE contd.

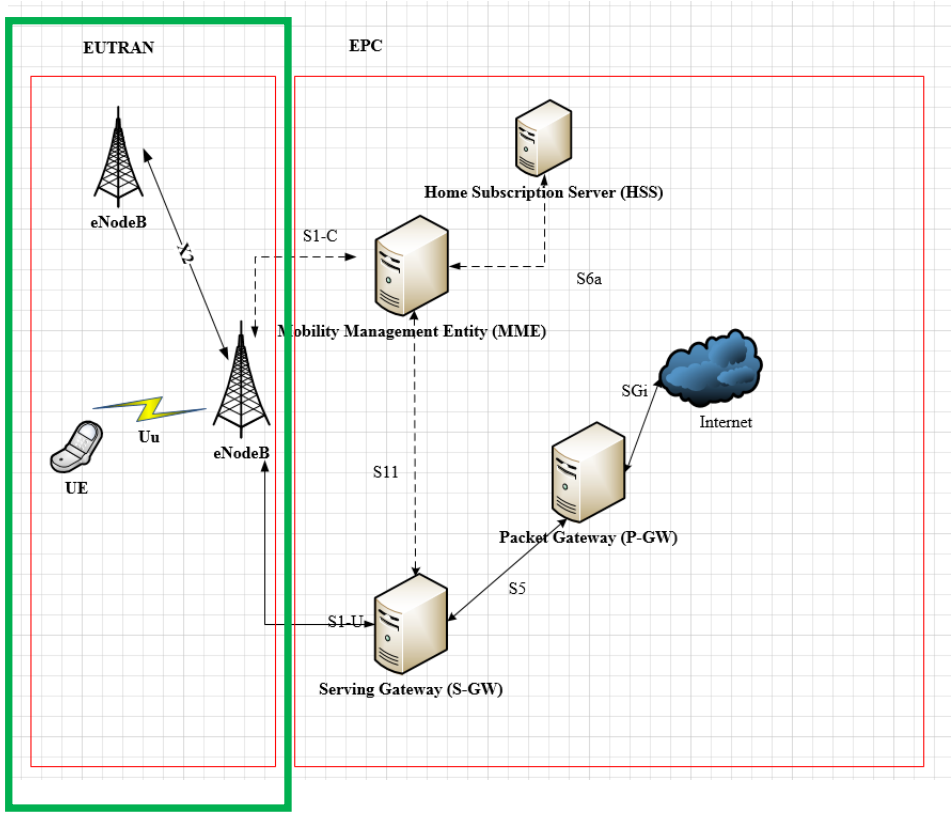
EUTRAN:

Evolved NodeB (eNodeB)

Unlike 3G there is no central controller for unicast data traffic. EUTRAN is referred to as a distributed architecture.

eNodeBs are connected to the MME via the S1-C/S1-MME interface.

eNodeBs can be connected to each other logically over X2 interface.

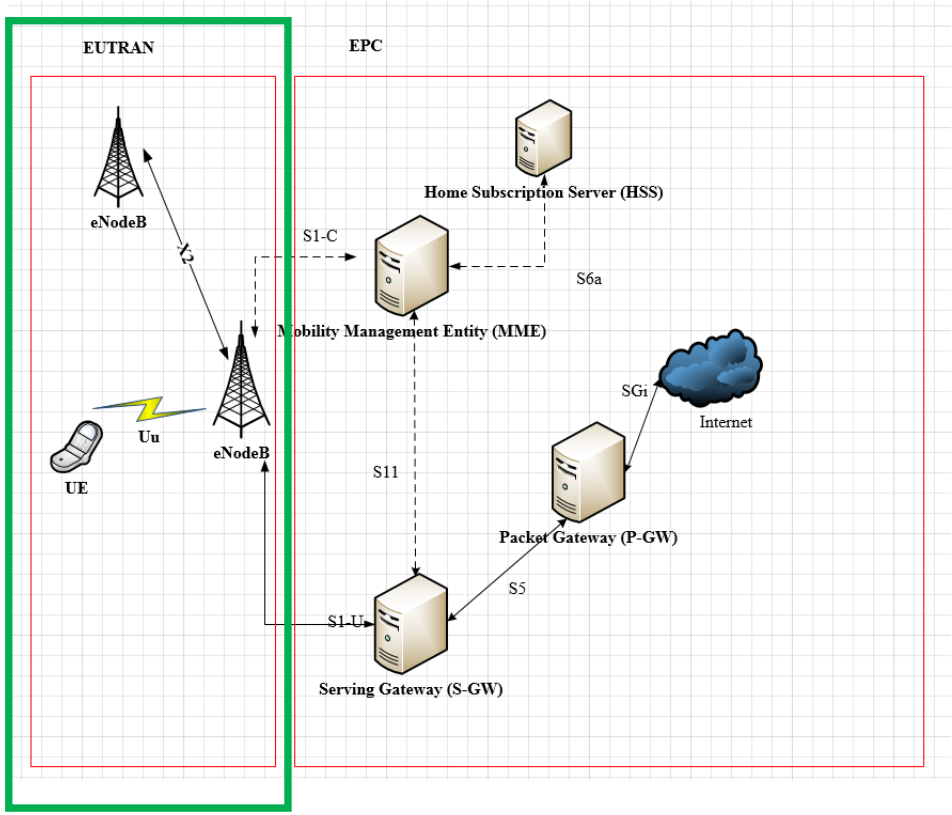


Network Architecture in LTE contd.

EUTRAN:

Evolved NodeB (eNodeB) Functions -

- Radio Resource management
- Synchronization and Interference control
- MME Selection among MME Pool
- Routing of User Plane data from/to S-GW
- Encryption/Integrity protection of user data
- IP Header Compression



Network Architecture in LTE contd.

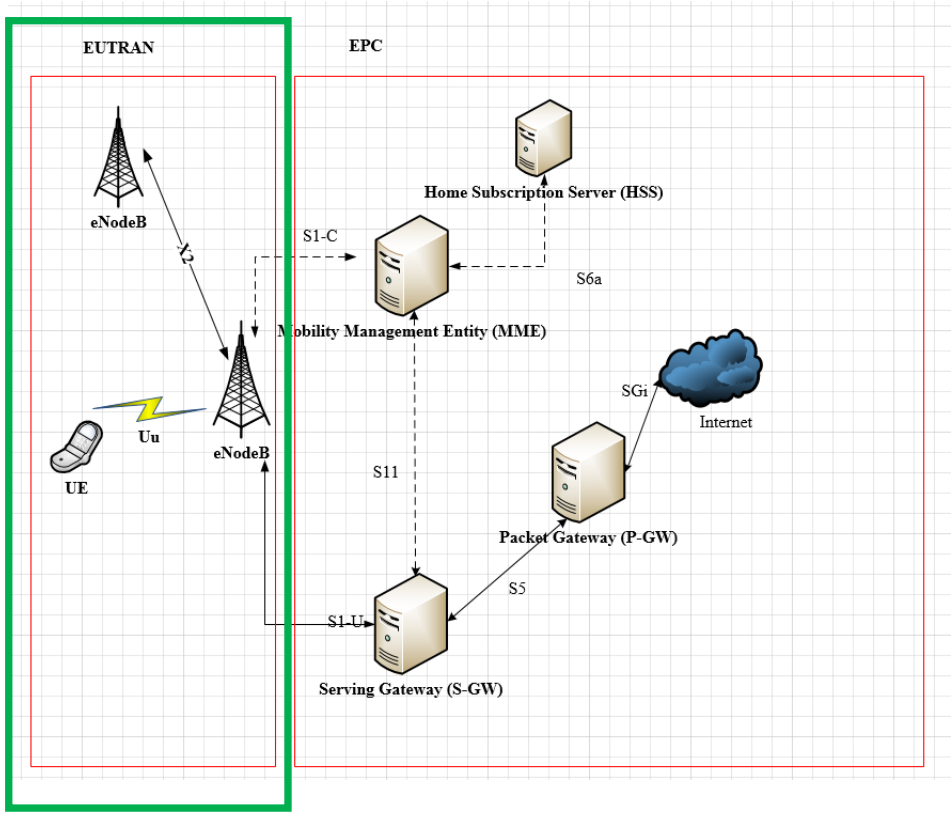
EUTRAN:

User Equipment (UE)

Represents the mobile/fixed device used to connect to the network.

Specifications specified by 3GPP

3GPP has defined various categories in accordance to capabilities. \\Below are some categories as defined by 3GPP



HEADLINE DATA RATES FOR LTE CATEGORIES								
	LTE UE CATEGORY							
LINK	1	2	3	4	5	6	7	8
Downlink	10	50	100	150	300	300	300	1200
Uplink	5	25	50	50	75	50	150	600

UE Categories

Network Architecture in LTE contd.

EUTRAN:

User Equipment (UE)

Each Category is has a given set of capabilities.

RAN keeps track of each of the connected UE's capabilities in order to optimize experience.

IoT – example

LTE CATEGORY 0 PERFORMANCE SUMMARY	
PARAMETER	LTE CAT 0 PERFORMANCE
Peak downlink rate	1 Mbps
Peak uplink rate	1 Mbps
Max number of downlink spatial layers	1
Number of UE RF chains	1
Duplex mode	Half duplex
UE receive bandwidth	20 MHz
Maximum UE transmit power	23 dBm

UL AND DL PARAMETERS FOR LTE UE CATEGORIES 1 - 5					
	LTE CATEGORY				
PARAMETER	LTE CAT 1	LTE CAT 2	LTE CAT 3	LTE CAT 4	LTE CAT 5
Max number of DL-SCH transport block bits received in a TTI	10 296	51 024	102 048	150 752	302 752
Max number of bits of a DL-SCH block received in a TTI	10 296	51 024	75 376	75 376	151 376
Total number of soft channel bits	250 368	1 237 248	1 237 248	1 827 072	3 667 200
Maximum number of supported layers for spatial multiplexing in DL	1	2	2	2	4
Max number of bits of an UL-SCH transport block received in a TTI	5 160	25 456	51 024	51 024	75 376
Support for 64-QAM in UL	No	No	No	No	Yes

UL AND DL PARAMETERS FOR LTE UE CATEGORIES 6, 7, 8					
	LTE CATEGORY				
PARAMETER	LTE CAT 6	LTE CAT 7	LTE CAT 8		
Max number of DL-SCH transport block bits received in a TTI	299 552	299 552	1 200 000		
Max number of bits of a DL-SCH block received in a TTI	TBD	TBD	TBD		
Total number of soft channel bits	3 667 200	TBD	TBD		
Maximum number of supported layers for spatial multiplexing in DL					
Max number of bits of an UL-SCH transport block received in a TTI	TBD	TBD	TBD		
Support for 64-QAM in UL	No	Yes, up to RAN 4	Yes		

UE Categories

Network Architecture – Introduction:

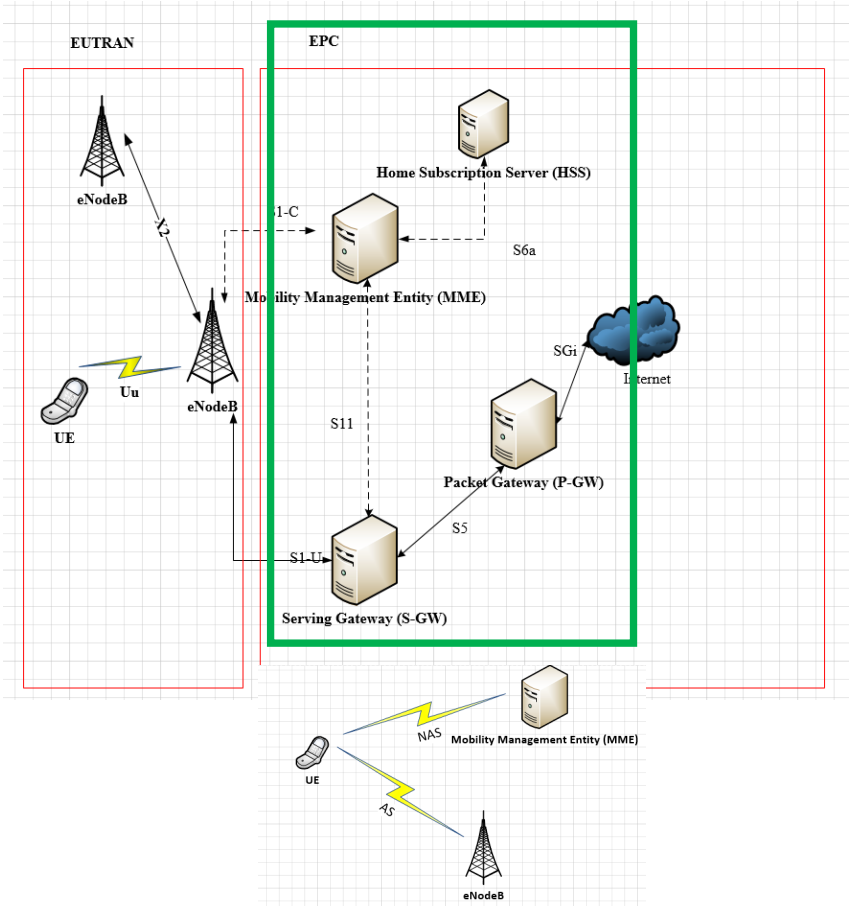
EPC – Evolved Packet Core

Network Architecture in LTE contd.

EPC:

Mobility Management Entity (MME)

- NAS (non-access stratum) signaling and its security
- Tracking Areas List management
- PDN GW and SGW selection.
- Roaming and Authentication
- EPS bearer management
- Signaling for mobility management between 3GPP RANs



Network Architecture in LTE contd.

EPC Contd.:

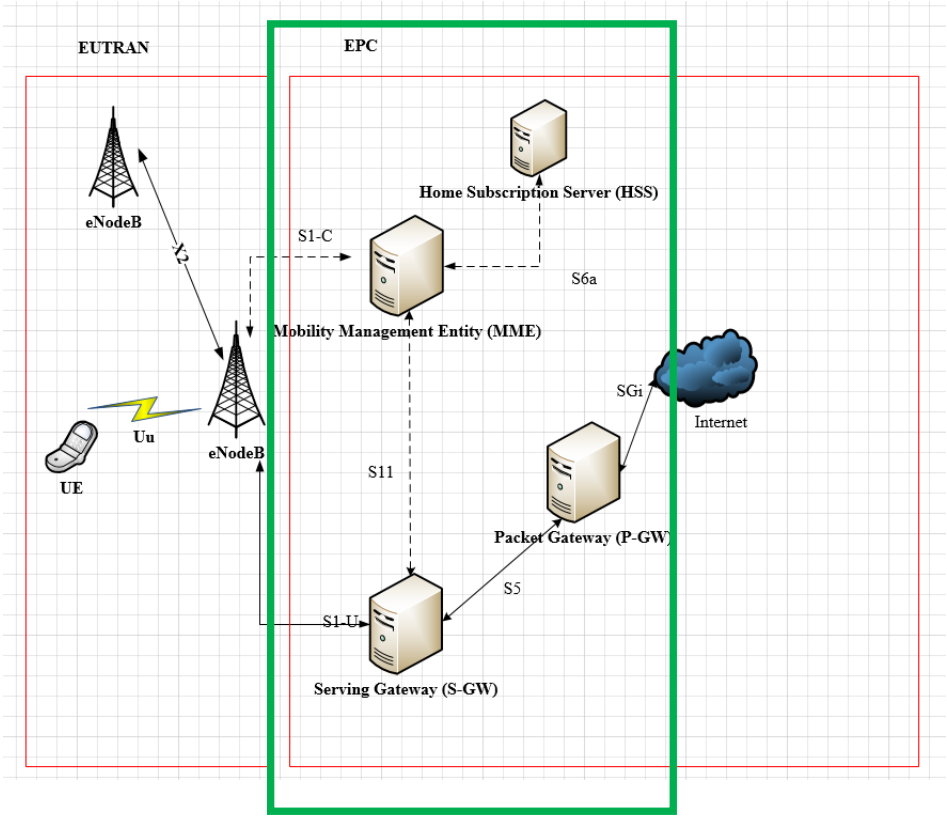
Home Subscription Server (HSS)

User Authentication

Subscription/Profile management –

Roaming

Speed/throughput limits

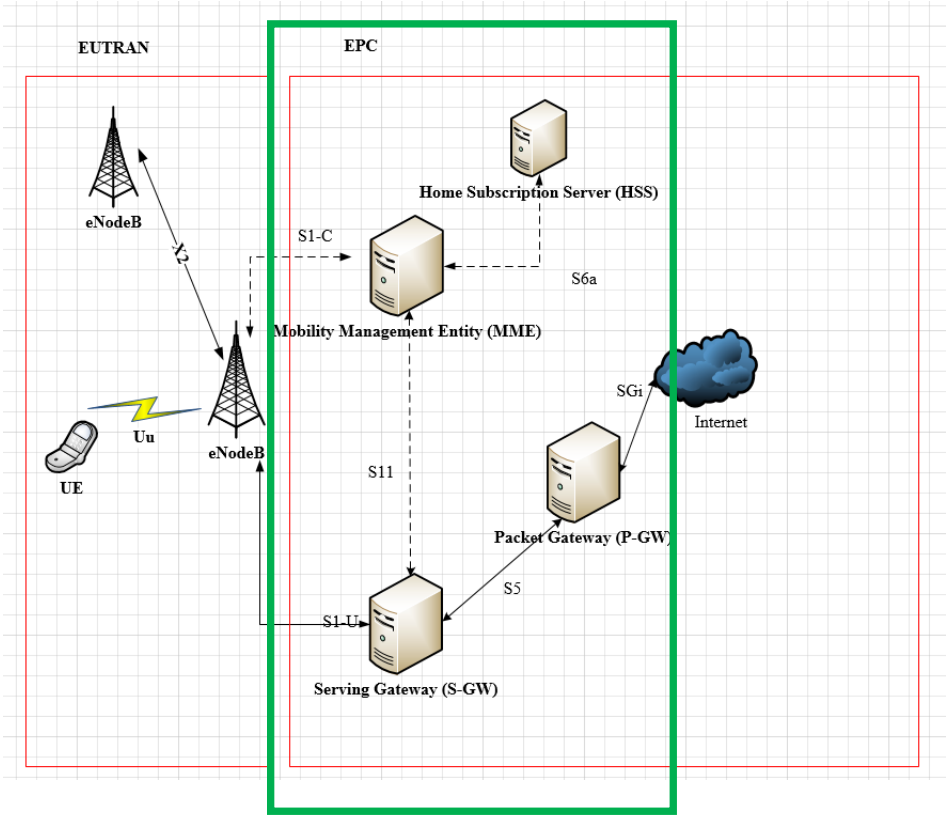


Network Architecture in LTE contd.

EPC Contd.:

Serving Gateway (S-GW)

- Packet routing and forwarding
- EUTRAN Idle mode DL packet buffering
- EUTRAN and inter-3GPP mobility anchoring
- UL and DL charging per UE, PDN and QCI



Network Architecture in LTE contd.

EPC Contd:

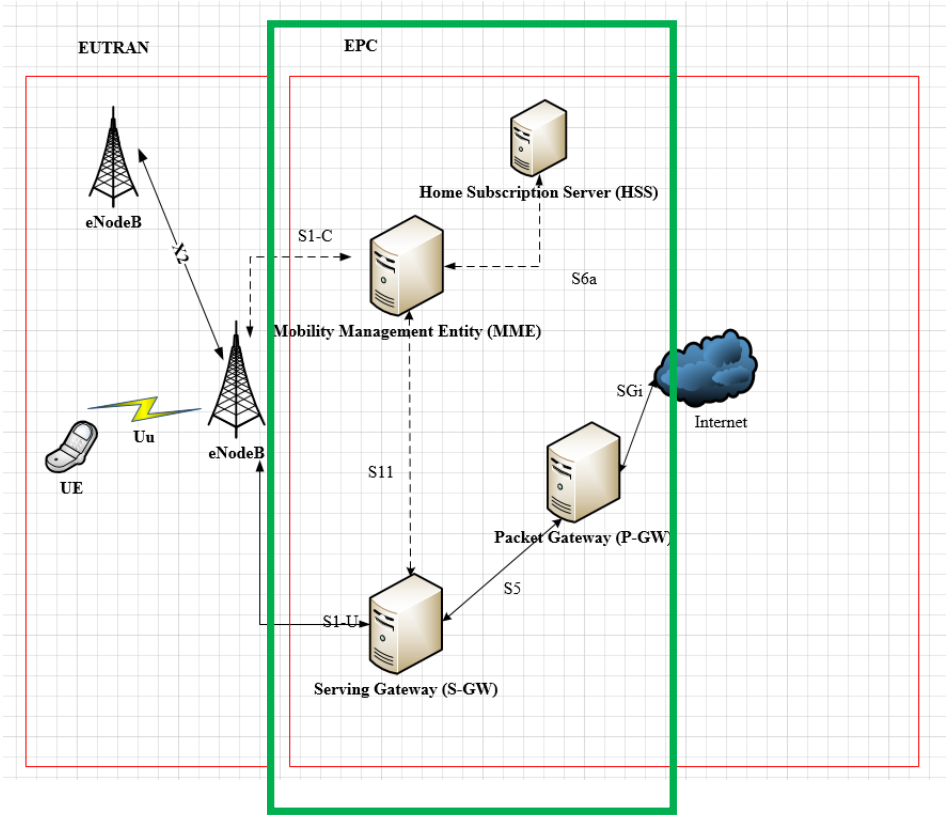
Packet Data Network Gateway (P-GW)

IP Address allocation

Packet filtering and Policy enforcement

Transport Level QoS mapping and marking.

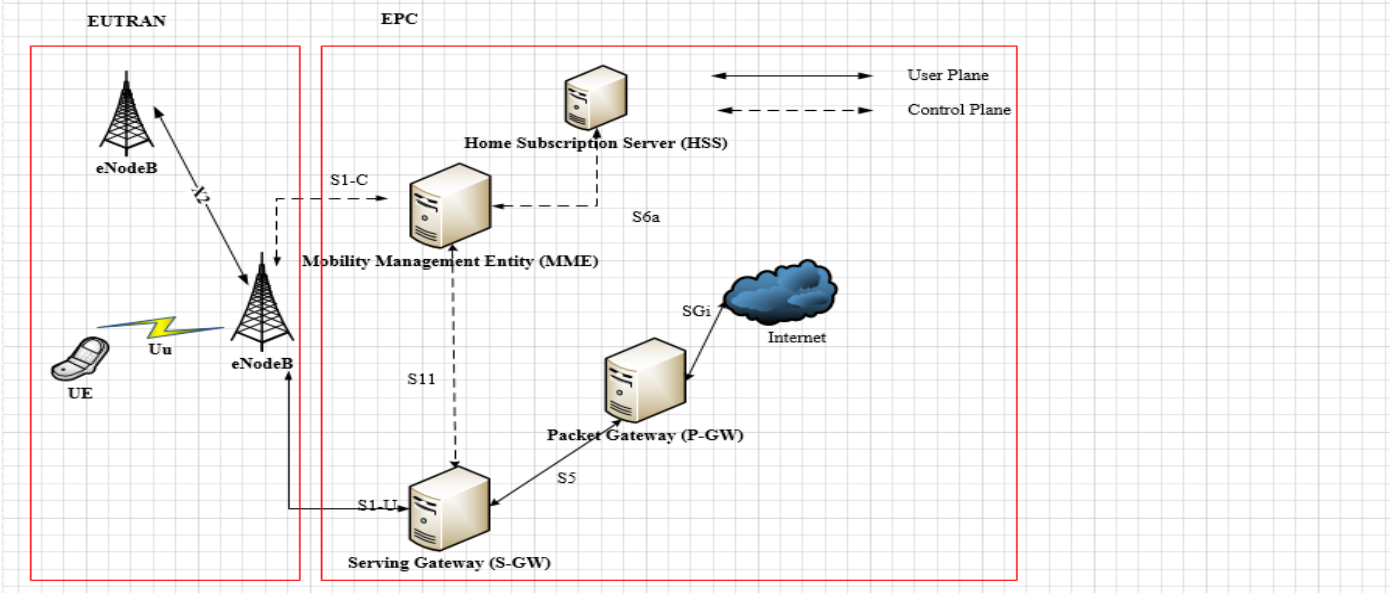
User Info anchoring for 3GPP and non-3GPP handovers.



Network Architecture – Introduction:

LTE-Architecture- Summary

Network Architecture in LTE contd:



eNodeB Functions:

- Radio Resource management, radio bearer control, radio admission control, connection mobility control, uplink/ downlink scheduling
- IP header compression and ciphering of the User data stream.
- MME selection
- Paging
- CMAS

MME Functions:

- Non-Access Stratum (NAS) signaling (attachment, bearer setup/deletion)
- NAS signaling security
- Signaling for mobility between 3GPP access networks
- Idle mode user tracking
- Tracking Area list mgmt.
- PDN gateway, S-GW selection
- Roaming – S6a interface to HSS
- Authentication

Serving Gateway Functions:

- Local mobility anchor for inter-eNodeB handover.
- EUTRAN downlink packet buffering-while idle UE is being paged.
- Lawful intercept
- Packet routing and forwarding
- Transport level packet marking (UL/DL)
- Accounting for inter-operator charging.
- Accounting per UE

Home Subscriber Server:

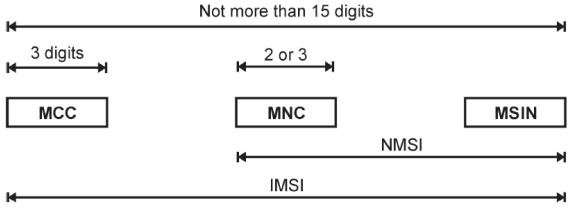
- Storage of Sub Data (Auth keys, QoS profile, APN profile etc.).
- Address of currently serving MME, TA

PDN Gateway:

- Lawful Intercept
- IP address allocation
- Transport level marking for DL
- Downlink rate enforcement based on AMBR (Aggregate Maximum Bit Rate)
- Accounting per UE

Identifiers in LTE- EPC

IMSI



• International Mobile Subscriber Identity

The IMSI allows unambiguous identification of a particular SIM or USIM card. The IMSI is composed of three parts -

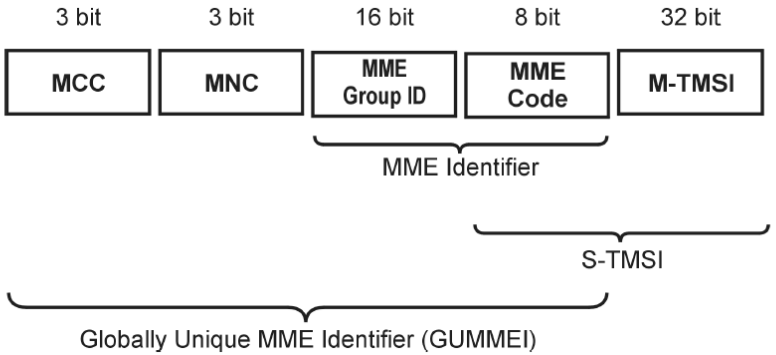
• The **Mobile Country Code (MCC),** consisting of three digits. The MCC uniquely identifies the country of domicile of the mobile subscriber. MCC values are administrated and allocated by an international numbering plan.

• The **Mobile Network Code (MNC),** consisting of two or three digits for GSM/UMTS applications. The MNC identifies the home PLMN of the mobile subscriber. The length of the MNC (two or three digits) depends on the value of the MCC. A mixture of two- and three-digit MNC codes within a single MCC area is not recommended and is beyond the scope of this specification.

• The **Mobile Subscriber Identification Number (MSIN),** identifying the mobile subscriber within a PLMN. As a rule the first two or three digits of the MSIN reveal the identity of the Home Location Register (HLR) or HSS that is used for Signaling Connection Control Part (SCCP) Global Title translation procedures when roaming subscribers register in foreign networks

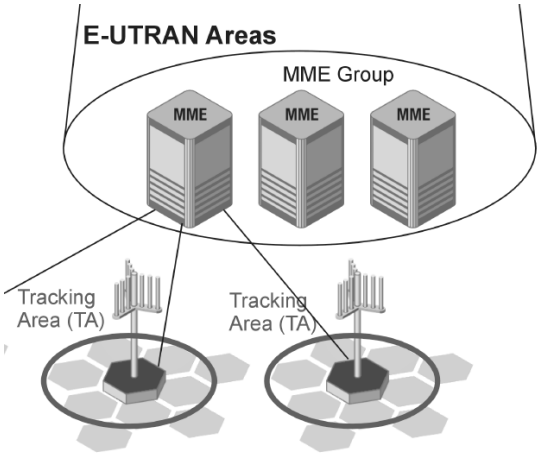
GUTI

- Globally Unique Temporary Identifier.
- The GUTI is assigned only by the MME during initial attach of a UE to the E-UTRAN
- The purpose of GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the E-UTRAN. It also allows identification of the MME and network to which the UE attaches. The GUTI can be used by the network to identify each UE unambiguously during signaling connections.
- The GUTI has two main components: the Globally Unique Mobility Management Entity Identifier (GUMMEI) that uniquely identifies the MME which allocated the GUTI; and the M-TMSI that uniquely identifies the UE within the MME that allocated the GUTI. The GUMMEI is constructed from the MCC, MNC, and Mobility Management Entity Identifier (MMEI).
- The MMEI should be constructed from a Mobility Management Entity Group ID (MMEGI) and a MMEC.



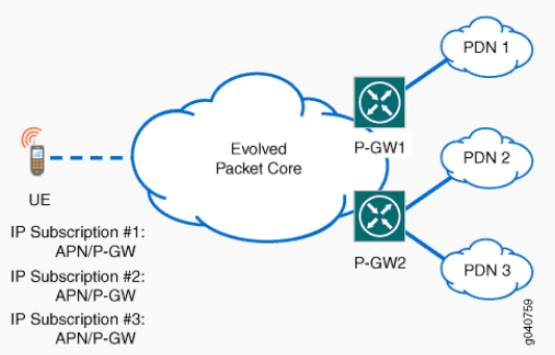
Tracking Area

- The Tracking Area Identity (TAI) is the identity used to identify tracking areas. The TAI is constructed from the MCC, MNC, and TAC (Tracking Area Code).
- A Tracking Area (TA) includes one or several E-UTRAN cells.
- Tracking Areas are used for Paging Idle mode Subscribers.
- UE informs MME every time it changes its TA via the TAU (tracking area Update) procedure, or at expiration of a timer (T3412).



Access Point Name (APN)

- APN represents a PDN (packet data network).
- UE during attach presents an APN to the network as part of attach. There also exist provisions in LTE where the NW can provide UE an APN as part of attach.
- APNs often look like Internet domain names and have two parts:
    - Network identifier—This defines the PDN the user connects to through a P-GW. This part of the APN is mandatory. It can be as simple as internet or have a more complicated structure such as juniper.net.
    - Operator identifier—This defines the operator whose PDN the user connects to through a P-GW. This part of the APN is optional and is often omitted. If present, it consists of the operator's Mobile Country Code (MCC) and Mobile Network Code (MNC). A more complex APN would be something like internet.mnc012.mcc345.gprs or, more realistically, Web.omnitel.it.



Interfaces in LTE Network

Interfaces in LTE

- What is an interface ?

Interface represents a channel on which 2 network entities exchange information.

- Why do we need interfaces ?

Interfaces are needed in LTE to deliver information (signaling or user data) for a subscriber or network element.

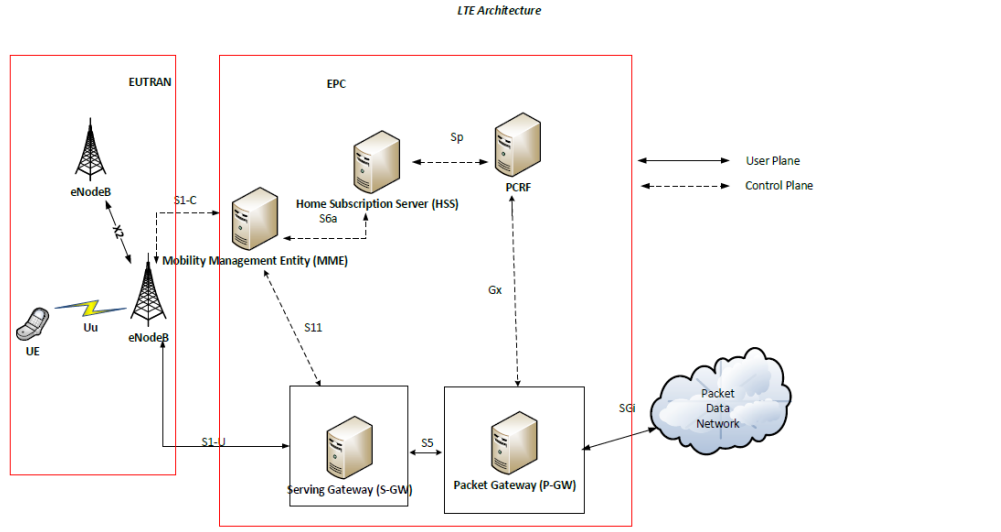
- Who defines these interfaces ?

The various network interfaces are defined by 3GPP. All network vendors or manufacturers are required to comply to these standards.

- Do these interfaces remain static ?

No. Depending on new capabilities and requirements 3GPP continues to make changes to the interface standards. However in most cases they are backward compatible.

Interfaces in LTE contd:



eNodeB Functions:
- Radio Resource management, radio bearer control, radio admission control, connection mobility control, uplink/downlink scheduling
- IP header compression and ciphering of the User data stream.
- MME selection
- Paging
- CMAS

MME Functions:
- Non-Access Stratum (NAS) signaling (attachment, bearer setup/deletion)
- NAS signaling security
- Signaling for mobility between 3GPP access networks
- Idle mode user tracking
- Tracking Area list mgmt.
- PDN gateway, S-GW selection
- Roaming – S6a interface to HSS
- Authentication

Serving Gateway Functions:
- Local mobility anchor for inter-eNodeB handover.
- EUTRAN downlink packet buffering-while idle UE is being paged.
- Lawful intercept
- Packet routing and forwarding
- Transport level packet marking (UL/DL)
- Accounting for inter-operator charging.
- Accounting per UE

Home Subscriber Server:
- Storage of Sub Data (Auth keys, QoS profile, APN profile etc.).
- Address of currently serving MME, TA

PDN Gateway:
- Lawful Intercept
- IP address allocation
- Transport level marking for DL
- Downlink rate enforcement based on AMBR (Aggregate Maximum Bit Rate)
- Accounting per UE

Policy Charging and Rate Function (PCRF):
- Interfaces with Proxy – Call session control function.
- Interfaces with PDN – GW to convey policy decisions and profiles.
- Decides how services will be treated in PDN GW according to User policy.

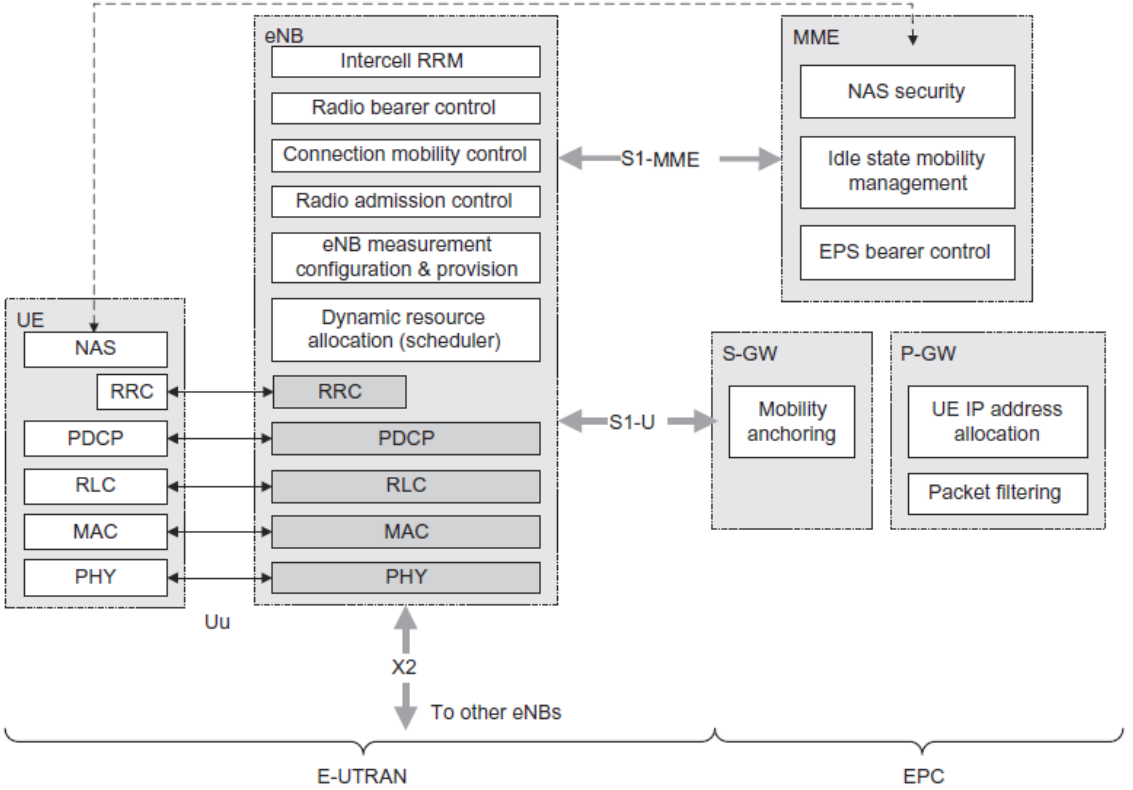
3GPP References:

- EUTRAN
  TS 36.401,36.300,23.002
- S1 Interface
  TS 36.41x series, TS 29.274, 24.301
- X2 Interface
  TS 36.42x series
- MME functions and interfaces
  TS 23.401, 23.402, 23.002
- S10/S11
  TS 29.274
- S6a
  TS 29.272
- SGW and PGW functions
  TS 23.401, 23.402, 23.002
- S5/S8 interface
  TS 29.274, 29.275
- SGi Interface
  TS 29.061

http://www.3gpp.org/specifications/specifications

LTE-Protocol Stack

Protocol Stack in LTE:

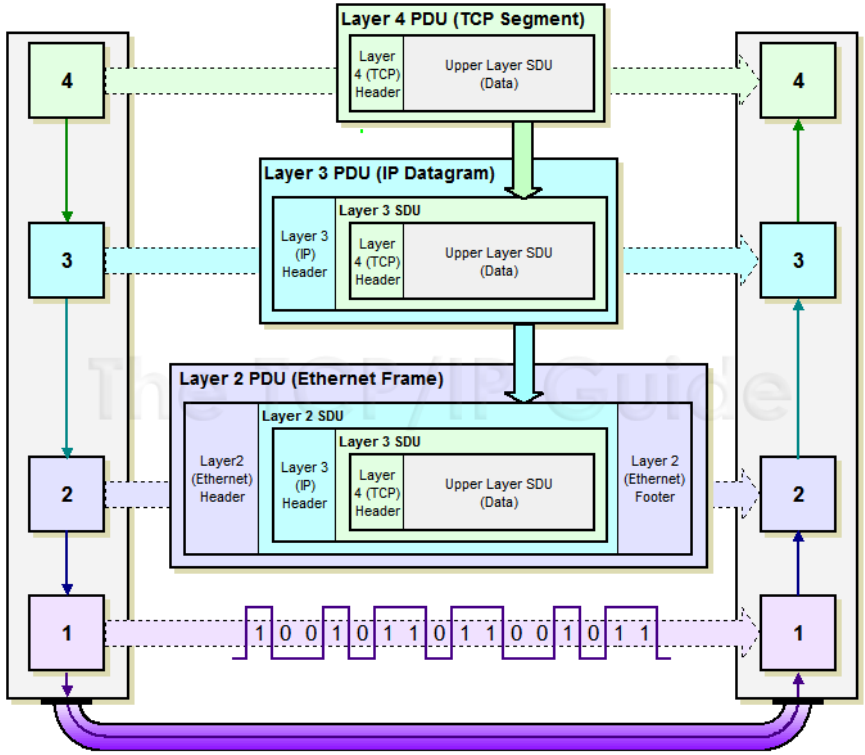


Protocol Stack in LTE:

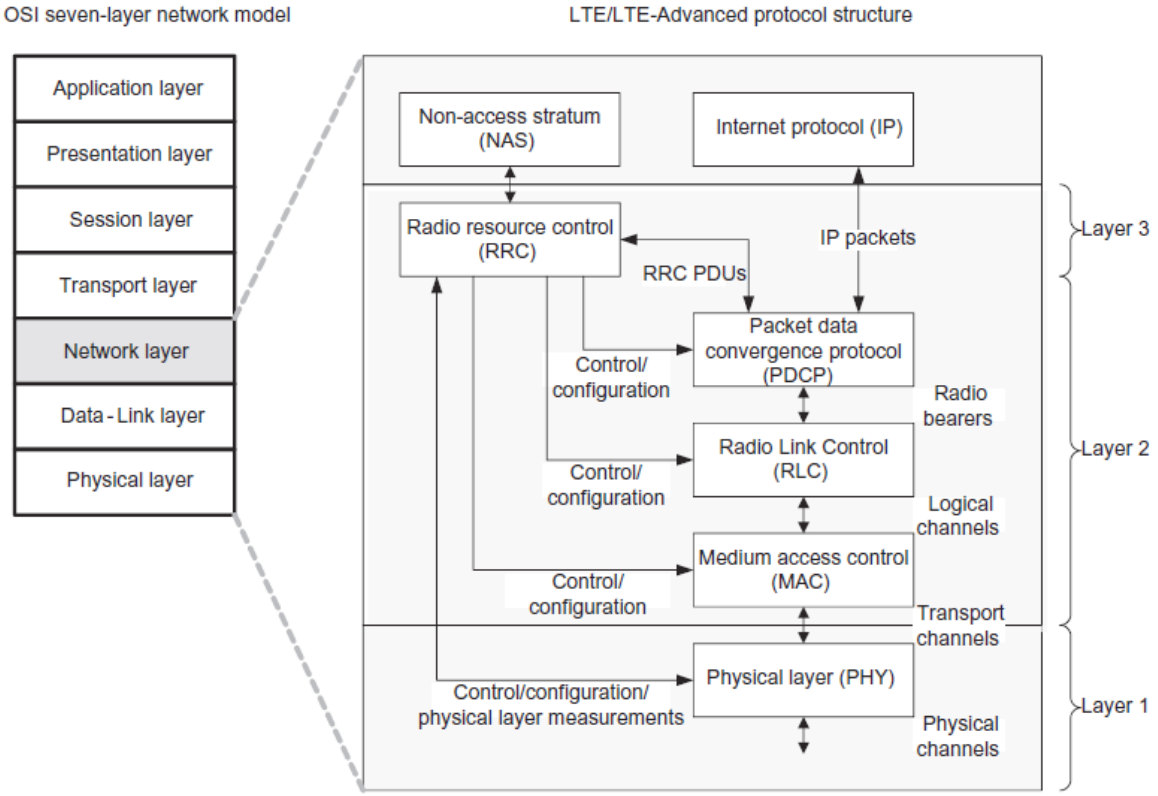
- Protocol Data Units (PDU)
- Service Data Unit (SDU)

On the transmit side packets are transferred from layer N to layer N-1.

At a given layer N-1 data received from the layer N is treated as SDU. Layer N adds header information to SDU. The new packet is then referred to as PDU.



Protocol Stack in LTE:

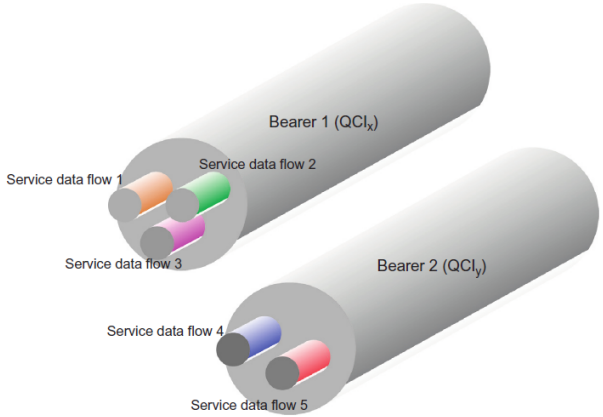


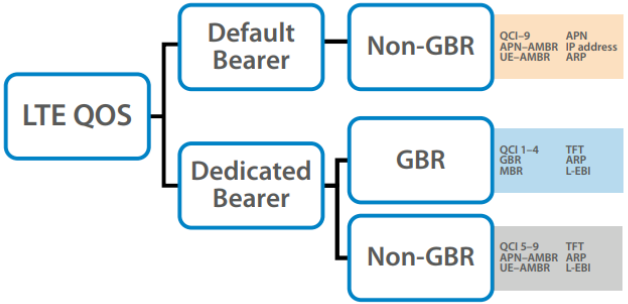
QoS in LTE:

Bearers in LTE

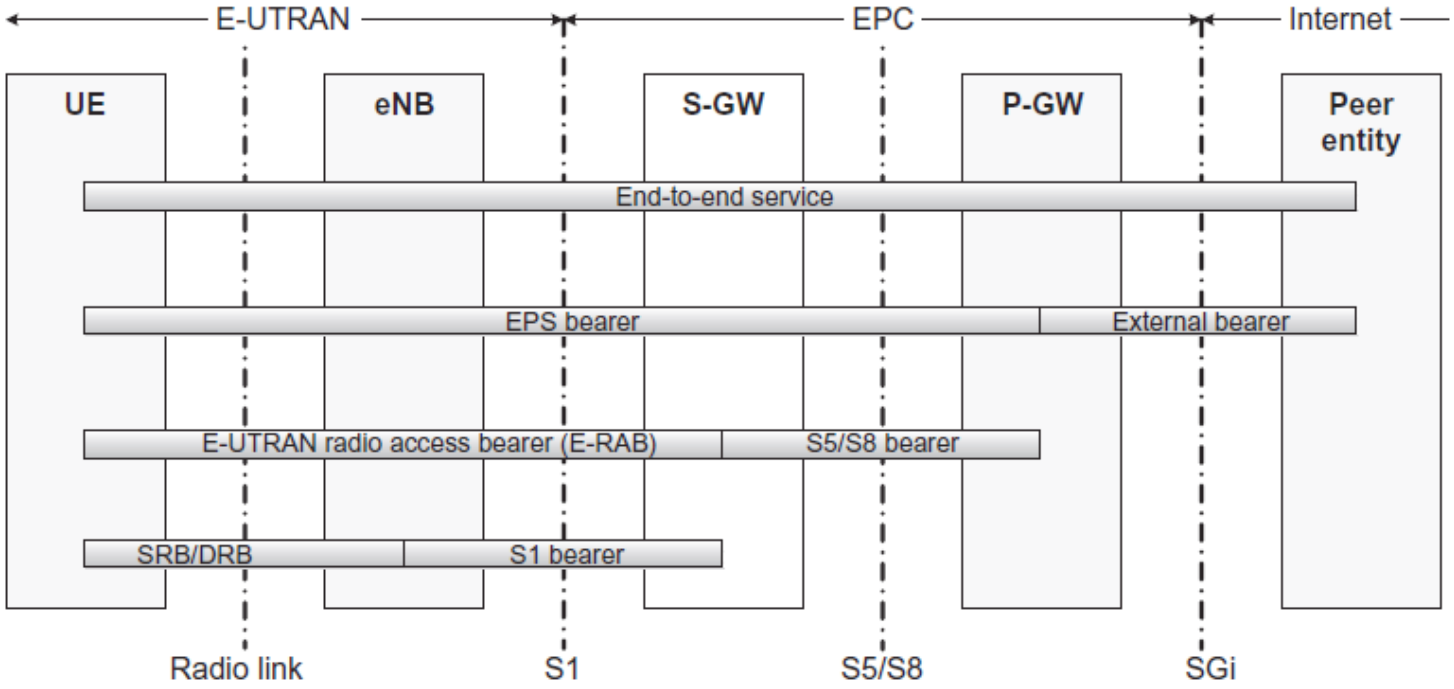
Bearers in LTE

- In LTE data-plane traffic is carried via virtual connections known as service data flows (SDF). The SDFs are carried over bearers that are virtual connections. Each bearer has a QoS requirement.





Bearers in LTE

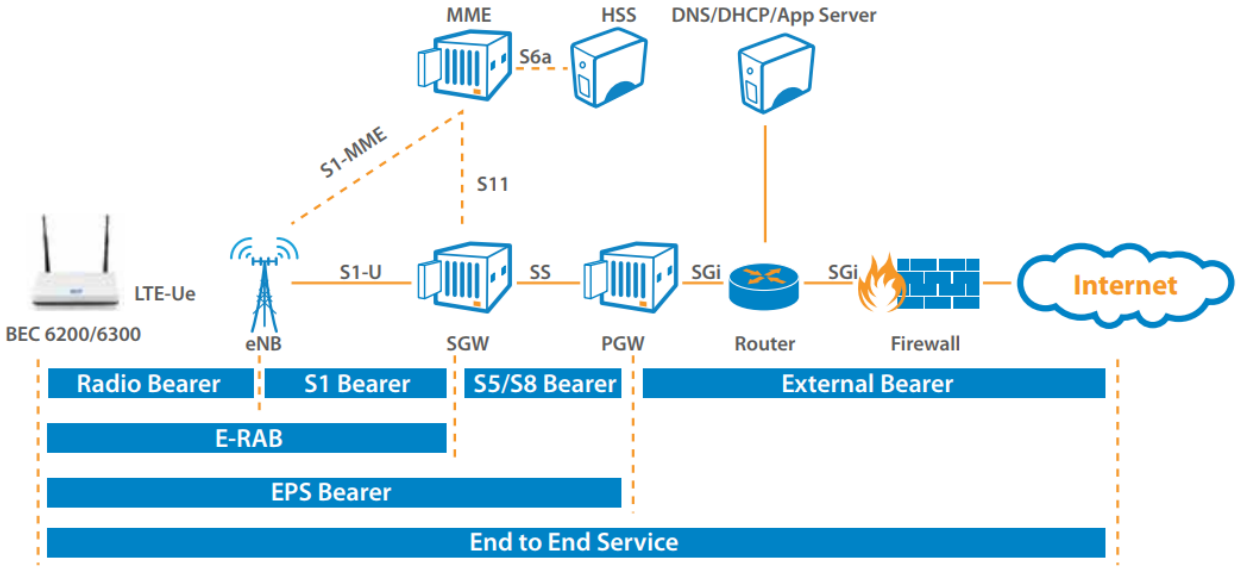


Each Bearer can have specific QoS requirements.

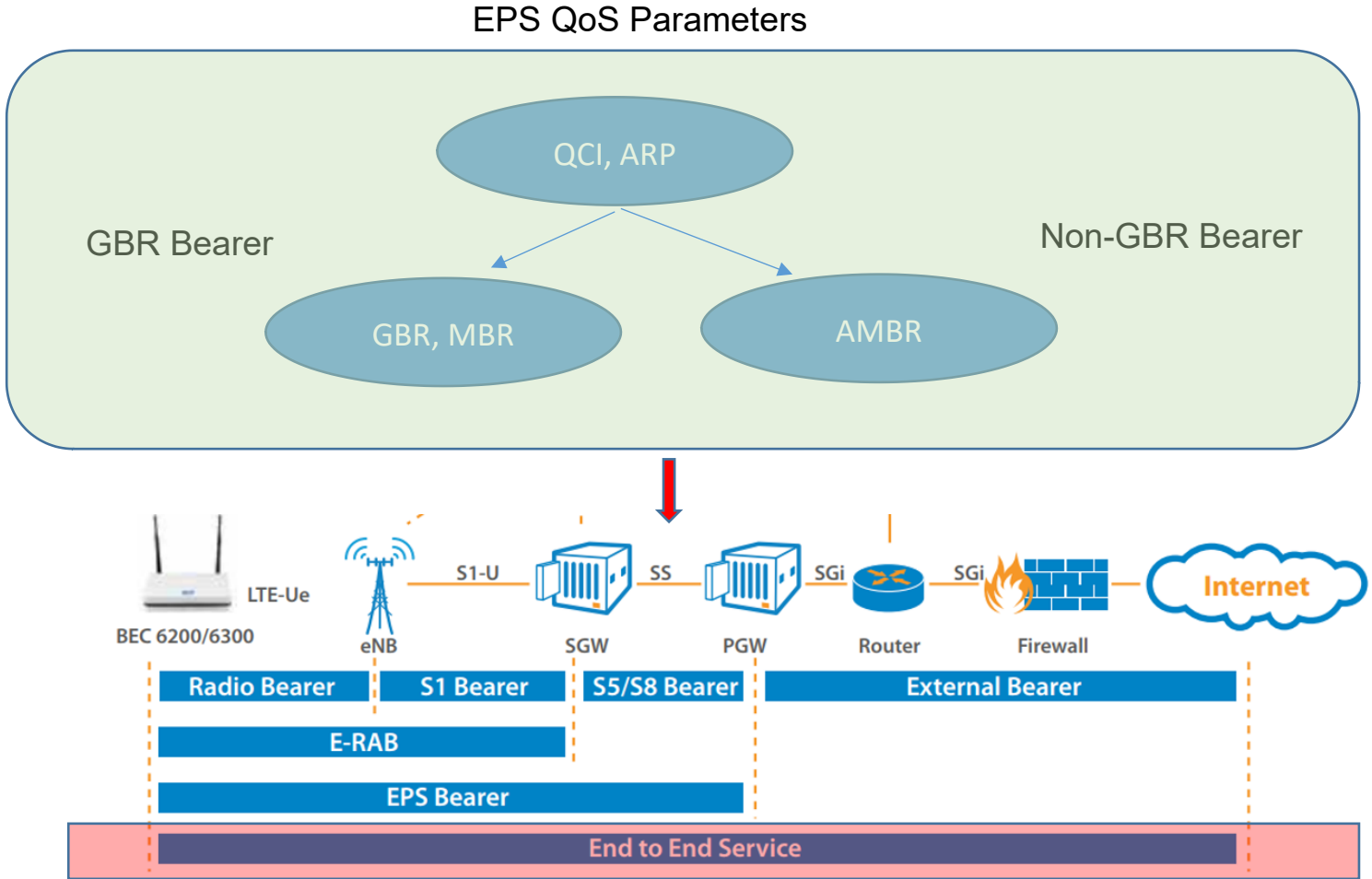
Bearers in LTE

QCI	Bearer Type	Priority	Packet Delay	Packet Loss	Example
1	GBR	2	100 ms	10	VOIP Call
2		4	150 ms	10	Video Call
3		3	50 ms		Online Gaming (Real Time)
4		5	300 ms	10	Video Streaming
5	Non-GBR	1	100 ms		IMS Signaling
6		6	300 ms		Video, TCP based services e.g. email, chat, ftp etc.
7		7	100 ms	10	Voice, Video, Interactive gaming
8		8	300 ms	10	Video, TCP based services e.g. email, chat, ftp etc.
9		9			

Bearers in LTE



Bearers in LTE

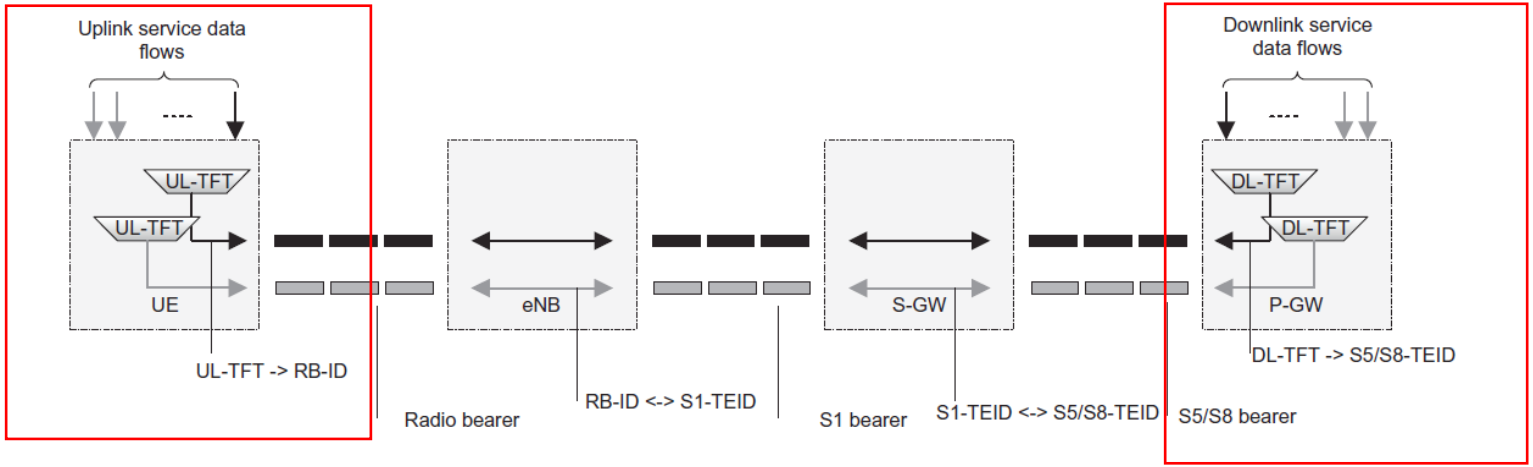


QoS in LTE:

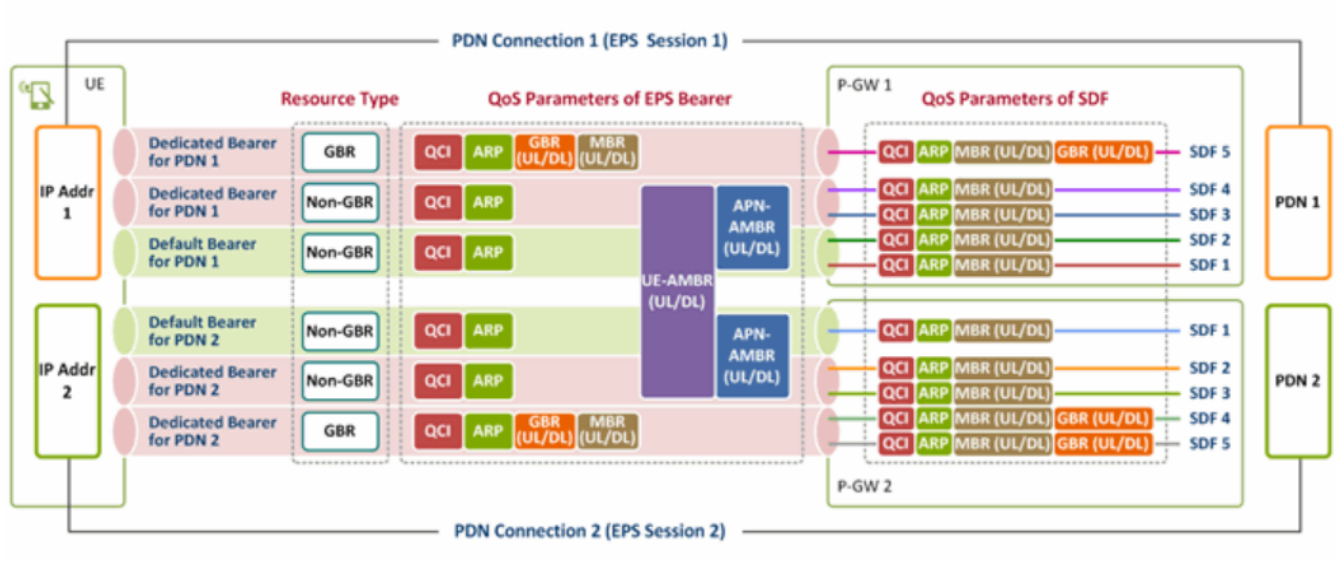
TFTs in LTE

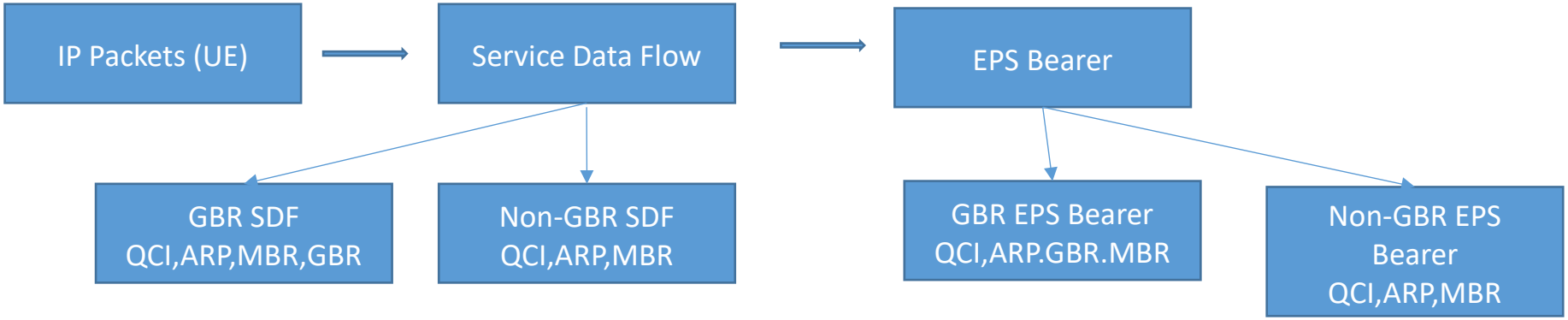
Traffic Flow Templates (TFT)

- IP Packets belong to different service data flows
- TFTs defines how IP packets are mapped to EPS Bearers.
- TFTs are applied at 2 places in the network –
  - Uplink – at the UE
  - Downlink – at the PGW



Traffic Flow Templates (TFT)





Summary of QoS parameters in LTE

Terms	Description
QCI	• Indicates different QoS performance characteristics. • Standardized QoS characteristics values are defined as QCI=1 ~ 9 (See 3GPP TS 23.203 [3] table 6.1.7). • QoS characteristics represented by QCI value: resource type (GBR or non-GBR), priority (1~9), packet delay budget (50ms ~ 300ms), and packet error loss rate (10^{-2} ~ 10^{-6}) • Controls packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.) at network nodes (eNB, S-GW and P-GW). • Pre-configured in operators' network node (e.g. eNB)
ARP	• ARP parameters: Priority Level, Pre-emption Capability and Pre-emption Vulnerability - Priority Level (1~15): defines relative importance of a resource request, with 1 being the highest. - Pre-emption Capability (yes or no): defines whether a SDF can get resources already assigned to another SDF/bearer with a lower priority level. - Pre-emption Vulnerability (yes or no): defines whether a SDF can lose the resources already assigned to it in order to establish a SDF/bearer with a higher priority level. • Used for controlling call admission. Indicates a priority value used to decide whether to refuse to activate a new SDF/EPS bearer or remove the existing SDF/EPS bearer when a new SDF/EPS bearer needs to be activated or fixed in a network with limited resources. • Considered only when deciding whether to activate a new SDF/bearer or not. Once successfully established, ARP has no impact on packet forwarding treatment.
GBR (UL/DL)	• Applied to a GBR SDF/bearer. Indicates a minimum bandwidth (bit rate) to be guaranteed for the SDF/bearer.
MBR(UL/DL)	• Applied to a GBR/Non-GBR SDF and GBR bearer. Indicates a maximum bandwidth (bit rate) allowed for the SDF/bearer. • Any traffic in excess of the specified MBR is discarded through rate policing.
APN-AMBR(UL/DL)	• Defined per PDN. Indicates a maximum bandwidth (bit rate) allowed for all the non-GBR bearers associated with a PDN connected to a UE. • Applied only to the aggregated bandwidth of non-GBR bearers.
UE-AMBR(UL/DL)	• Defined per UE. Indicates a maximum bandwidth (bit rate) allowed for all the non-GBR bearers associated with a UE. • Applied only to the aggregated bandwidth of non-GBR bearers. • Subscription information provide by an HSS ($UE\text{-}AMBR_{HSS}$). Still, can be modified by an MME with the APN-AMBR of all PDNs within a UE to the extent permitted (within a range of values provided by the HSS, $UE\text{-}AMBR_{HSS}$). (UE-AMBR = $\sum$ APN-AMBR(s) for all PDNs)

Terms	Description
GBR SDF/Bearer	• Dedicated network resources are assigned to these types of SDFs/bearers for guaranteed GBR. • The network always reserves the bandwidth specified as GBR for GBR SDFs/bearers even when there is no traffic.
Non-GBR SDF/Bearer	• Dedicated network resources are not assigned to these types of SDFs/bearers. • Traffic is delivered on a best-effort basis depending of the degree of congestion in the network.

EPC Core Elements – Deep Dive

MME

Mobility Management Entity (MME):

- Responsible for NAS connection with the UE. All NAS messages are exchanged between the UE and MME to trigger further procedures in the Core network if necessary.
- NAS security – Integrity and Encryption
- Paging for Idle mode UEs.
- SGW and PGW selection
- Perform management of S1 based and inter-RAT handovers.
- Sets up, modifies and releases default and dedicated bearers for UEs

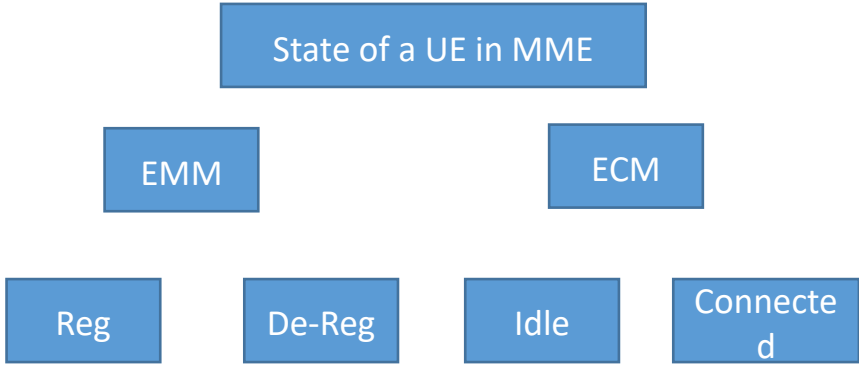
Mobility Management Entity (MME):

- Managing and storing UE contexts
- Generating temporary UE Identifiers
- S1-MME is the standard reference point between the enodeb and MME.
    - S1-MME has 2 components – S1-C (enb <-> MME) and S1-U (enb <-> SGW)
    - SCTP is used for reliable transport of messages on the S1-C.

Mobility Management Entity (MME):

States in MME-

- The **EPS Mobility Management (EMM)** states describe the Mobility Management.
- The **EPS Connection Management (ECM**) states describe the signaling connectivity between the UE and the EPC.



Definition of main **EPS Mobility Management** states

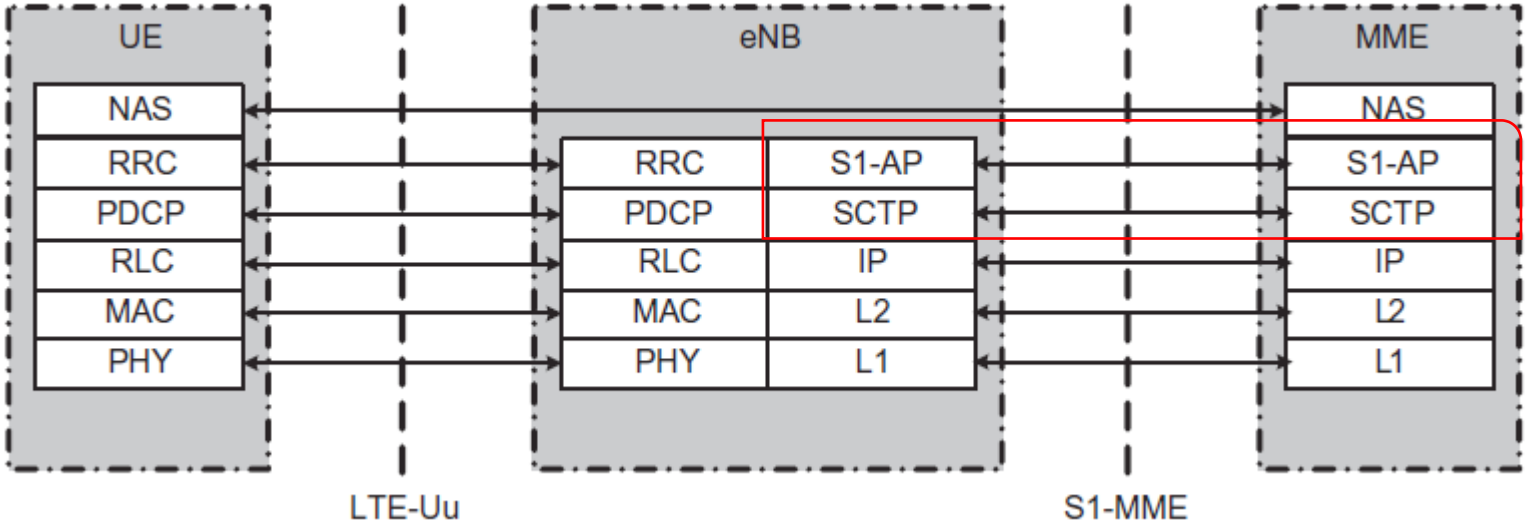
- EMM-DEREGISTERED

– The UE is not reachable by a MME.
– UE context can still be stored in the UE and MME

- EMM-REGISTERED

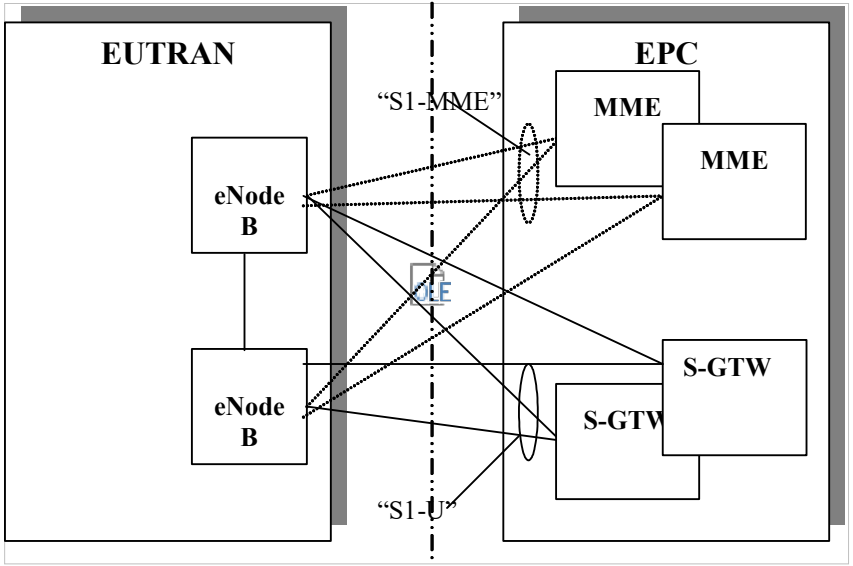
– UE enters to EMM-Registered with Attach or Tracking Area Update procedure.
– The UE location is known an accuracy of the tracking area list.
– UE has at least one active PDN connection;
– After Detach procedure the state is changed to EMM-DEREGISTERED

Mobility Management Entity (MME):



SCTP (Stream control transmission protocol) is a tunneling protocol used between eNodeB and MME. S1-AP uses SCTP.

Mobility Management Entity (MME):



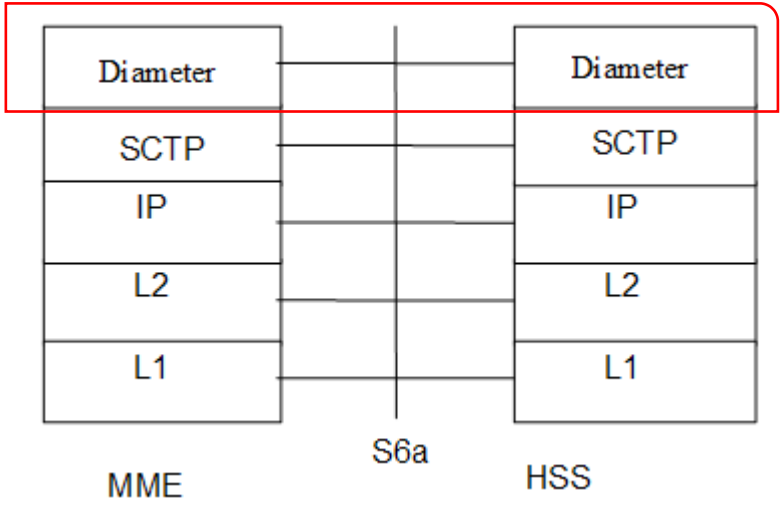
One to Many relationship

HSS

Home Subscriber Server (HSS):

HSS is responsible for the following functions in EPC –

- Master database that stores subscription related information to support call control and session management entities
- Storehouse for subscription profiles and user Identities
- Involved in User authentication
- Works with MME to authenticate user



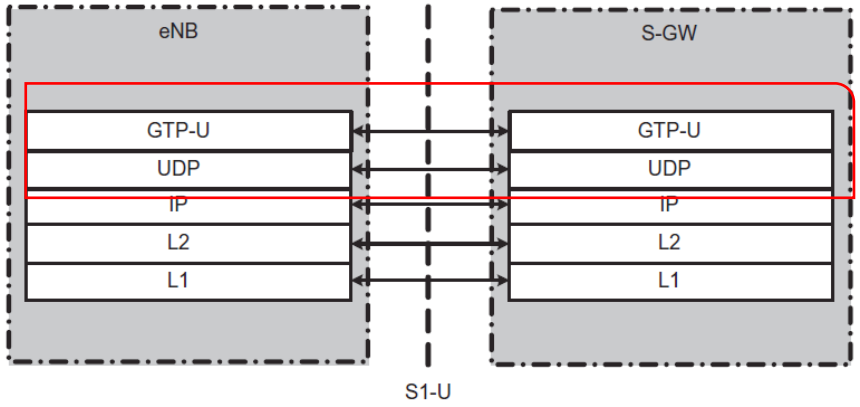
Serving Gateway (S-GW)

Serving Gateway (S-GW):

SGW is responsible for the following functions in EPC –

- Terminates interface to the EUTRAN. A particular LTE subscriber will be connected to one SGW
- In case of an inter-enodeb Handover, the S-GW acts as a mobility anchor of the connection and remains the same while the path fir the transport of signaling and user plane will be switched onto the S1 interface.
- Mobility anchoring of the S-GW is also defined for inter-3GPP mobility, Here the S-GW acts as the terminating point of the S4 interface and routes traffic between the 2G/3G SGSN and the P-GW of the EPC.
- If the UE is in idle mode the S-GW will buffer packets until the UE is paged and the bearers are setup.
- Provides interface for lawful intercept.
- S-GW is responsible for marking packets based on QoS. It marks packets with appropriate DSCP values.

Serving Gateway (S-GW):



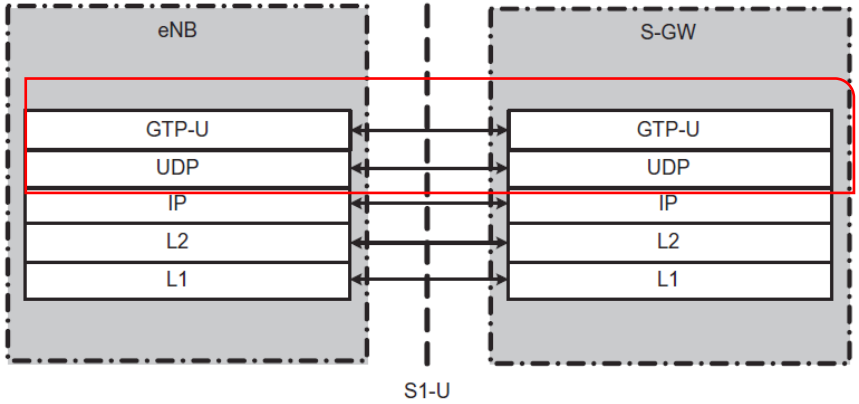
GTP-U is used on top of UDP/IP to carry the user plane PDUs between the enodeb and SGW

Packet Gateway (P-GW)

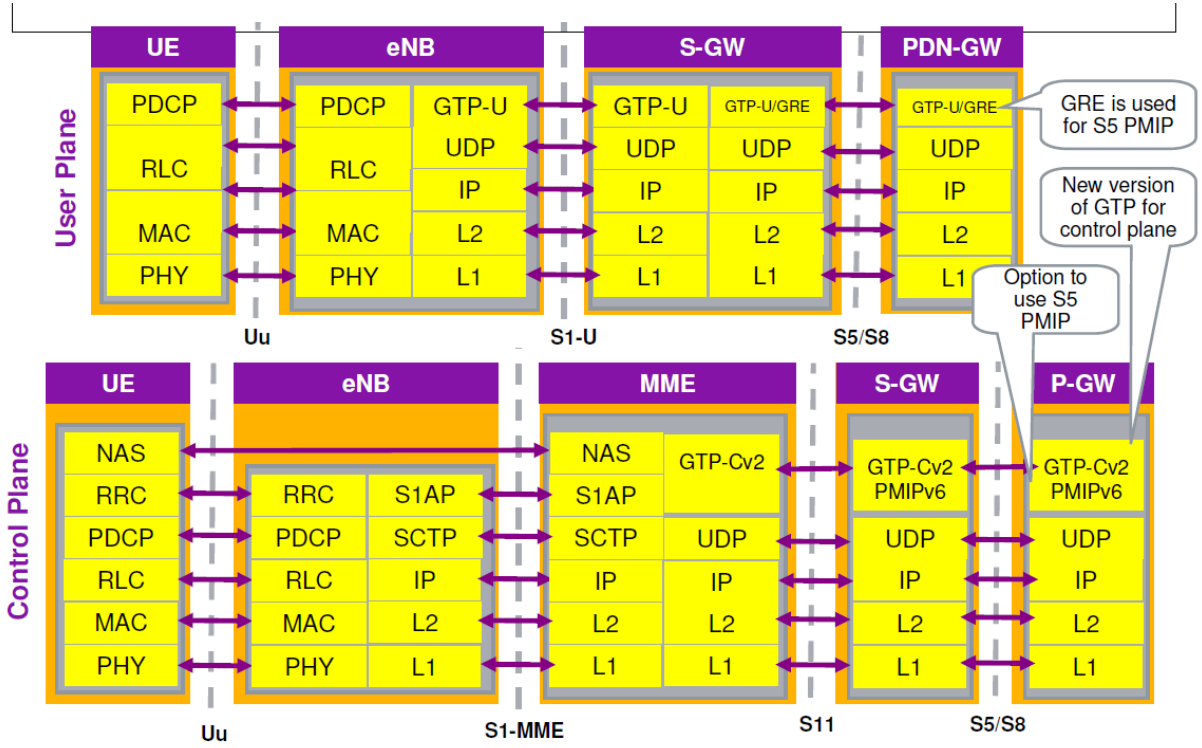
Packet Gateway (P-GW):

PGW is responsible for the following functions in EPC –

- Acts as router for the UE traffic
- Allocates IP address to the UE/bearer
- Performs DSCP/QoS marking for UE packets
- P-GW can be connected to a PCRF (Policy control and charging function via the Gx interface. PCRF provides subscriber level QoS parameters.



Protocols for Control and User Plane



LTE Security

LTE Security – key Pillars

Valid Subscriber/Valid Network	No man-in-the middle attacks	Privacy!
Authentication	**Integrity**	**Encryption**
• The LTE Network verifies the UE's identity by challenging the UT use the keys and report a result. • The network checks the result against the expected result	• Signaling message receiver verifies that the received message is exactly the message that the transmitter sent • This is done using an integrity checksum • Guards against "man in the middle" attacks where the senders messages and intercepted by a hacker and a modified message is relayed to the receiver	• The sender encrypts the data with a secret key that is only known to the receiver • Only the receiver is able to decode the message • Guards against hackers listening in on the data

- To understand how the overall LTE security concept works, it is crucial to understand the hierarchy of LTE security keys first. This LTE security key hierarchy, shown in Figure below, includes the following keys: KeNB, KNASint, KNASenc, KUPenc, KRRCint, and KRRCenc:

- K = This is the master Key and is stored in the SIM and the HSS/AuC

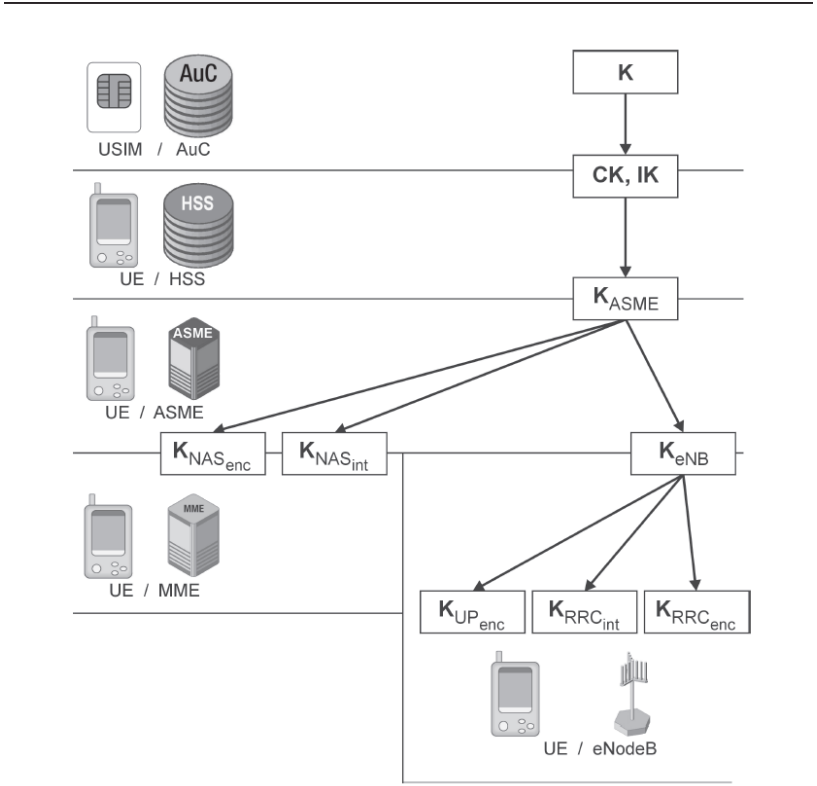
- All Keys are derived from K Key.

- K Key is never transmitted

- K Key is used to derive the Cipher Key CK and Integrity Key IK.

- With CK and IK, the HSS and UE are able to derive the KASme.

- With KASme, the MME is able to derive the NAS and AS keys.



KeNB is a key derived by the UE and MME from KASME or by the UE and target eNB from KeNB* during eNB handover.KeNB should only be used for the derivation of keys for RRC traffic and the derivation of keys for UP (User Plane) traffic, or to derive a transition key KeNB* during an eNB handover.

Keys for NAS traffic:

• **KNASint** is a key which should only be used for the protection of NAS traffic with a particular integrity algorithm. This key is derived by the UE and MME from KASME, as well as an identifier for the integrity algorithm.

• **KNASenc** is a key which should only be used for the protection of NAS traffic with a particular encryption algorithm. This key is derived by the UE and MME from KASME, as well as an identifier for the encryption algorithm.

Keys for UP traffic:

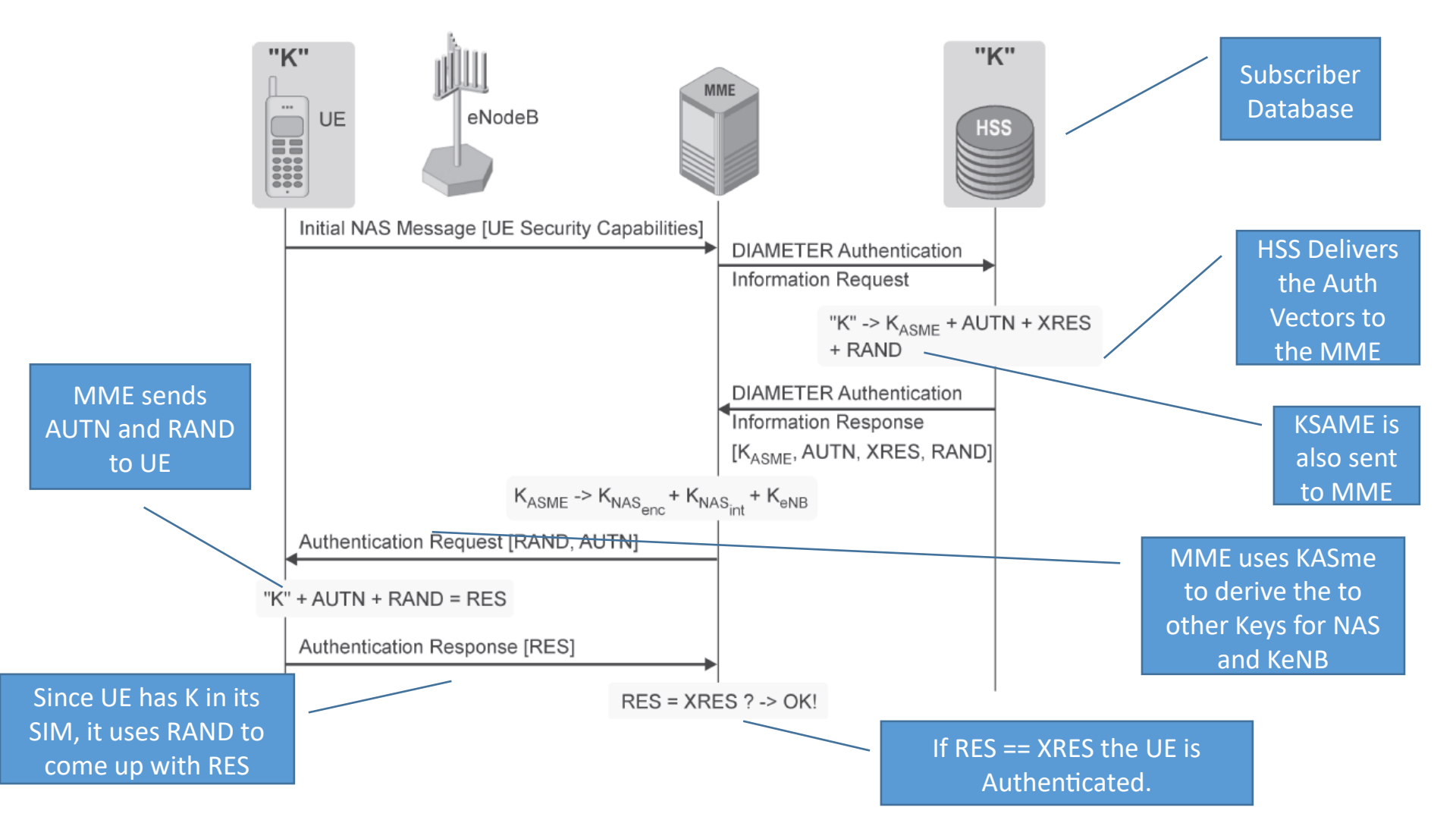
• **KUPenc** is a key which should only be used for the protection of UP traffic with a particular encryption algorithm. This key is derived by the UE and eNB from KeNB, as well as an identifier for the encryption algorithm.

Keys for RRC traffic:

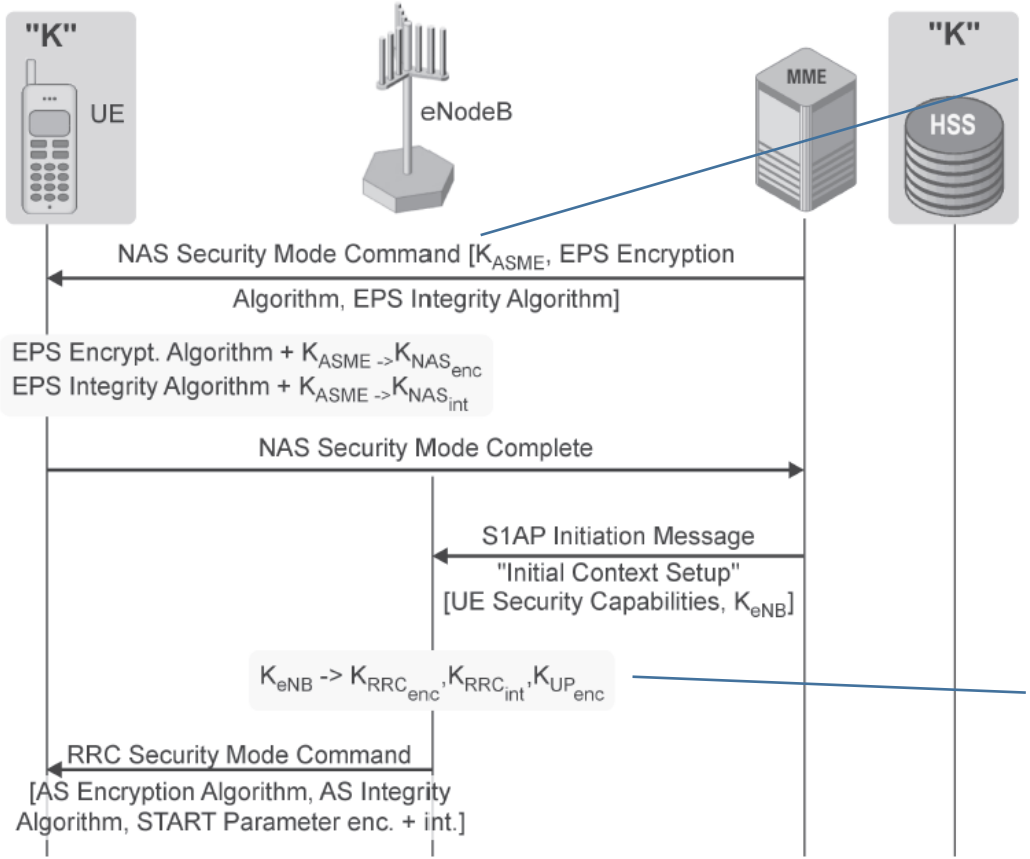
- KRRCint is a key which should only be used for the protection of RRC traffic with a particular integrity algorithm.KRRCint is derived by the UE and eNB from KeNB, as well as an identifier for the integrity algorithm.
- KRRCenc is a key which should only be used for the protection of RRC traffic with a particular encryption algorithm.KRRCenc is derived by the UE and eNB from KeNB as well as an identifier for the encryption algorithm.

** Keys in LTE/EPC is a pretty vast topic. Refer to 3GPP TS 33.401 for more details.*

LTE Security – Big picture

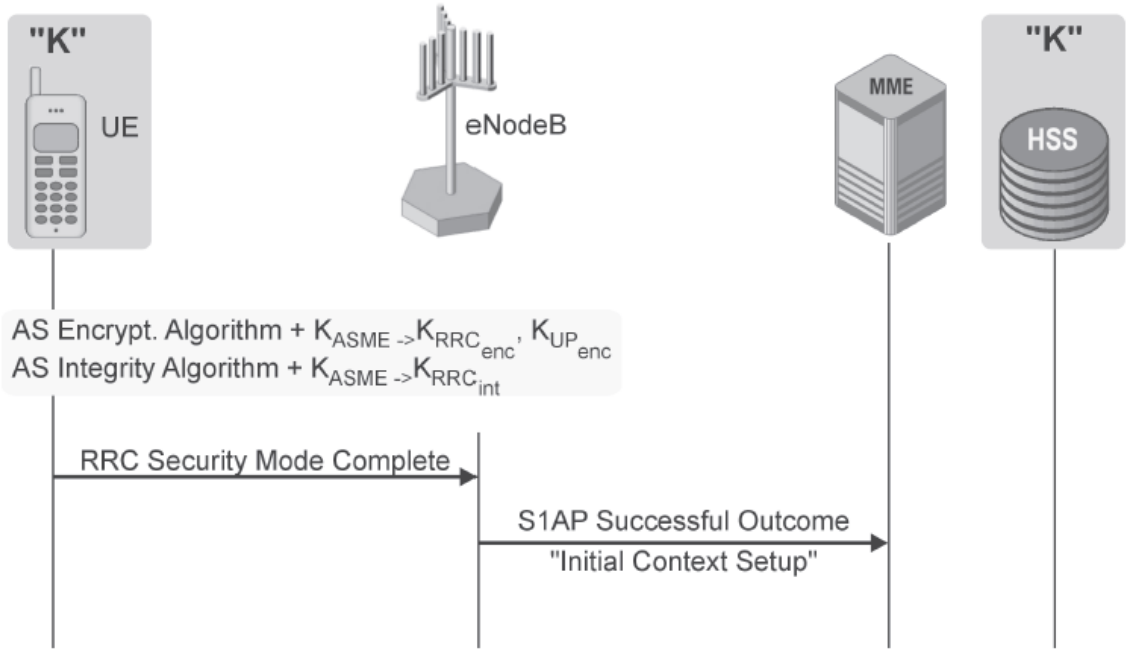

"K"
UE
eNodeB
MME
"K"
HSS
Subscriber Database
Initial NAS Message [UE Security Capabilities]
DIAMETER Authentication Information Request
"K" -> K_{ASME} + AUTN + XRES + RAND
HSS Delivers the Auth Vectors to the MME
MME sends AUTN and RAND to UE
DIAMETER Authentication Information Response [K_{ASME}, AUTN, XRES, RAND]
KSAME is also sent to MME
K_{ASME} -> $K_{NAS_{enc}}$ + $K_{NAS_{int}}$ + K_{eNB}
Authentication Request [RAND, AUTN]
MME uses KASme to derive the to other Keys for NAS and KeNB
"K" + AUTN + RAND = RES
Authentication Response [RES]
Since UE has K in its SIM, it uses RAND to come up with RES
RES = XRES ? -> OK!
If RES == XRES the UE is Authenticated.

UE uses the previous informati on and derives the NAS Keys



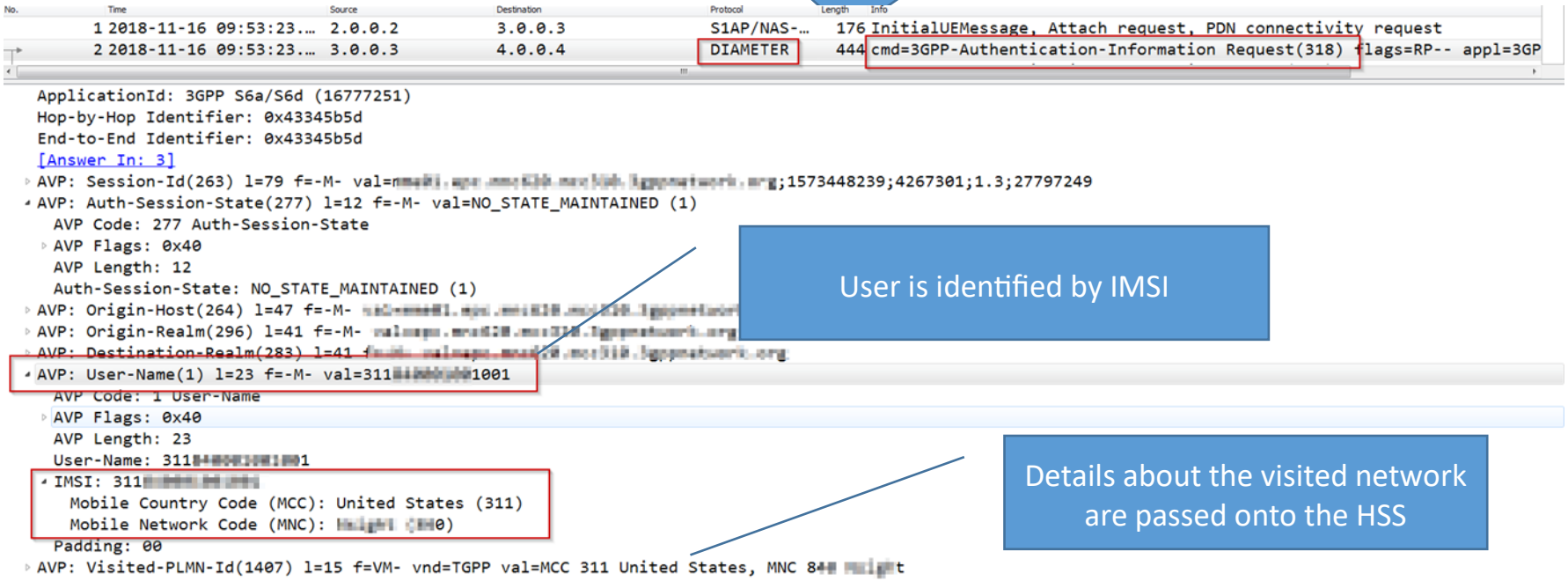
Upon Auth Succ the MME sends a security mode command to UE with all the information re to Enc and Int algos

MME sends enb the KeNB. eNB derives the RRC and UP enc Keys


"K"
UE
eNodeB
MME
"K"
HSS
AS Encrypt. Algorithm + K_{ASME} -> $K_{RRC_{enc}}$, $K_{UP_{enc}}$
AS Integrity Algorithm + K_{ASME} -> $K_{RRC_{int}}$
RRC Security Mode Complete
S1AP Successful Outcome
"Initial Context Setup"

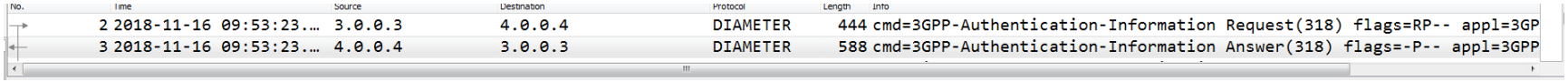
LTE Security – Real Logs

Authentication Information Request. Sent my MME -> HSS
On S6a using Diameter protocol



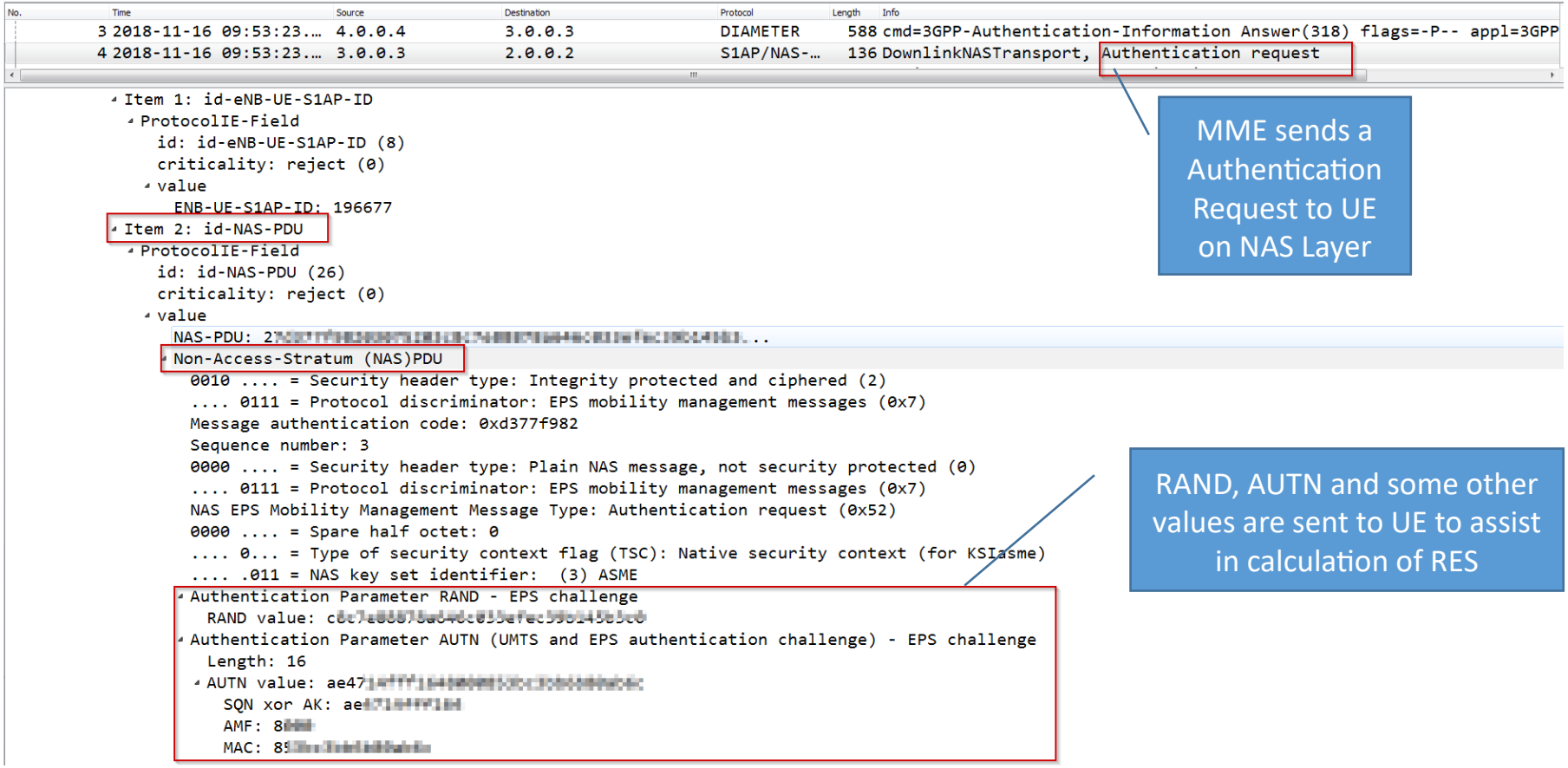
User is identified by IMSI

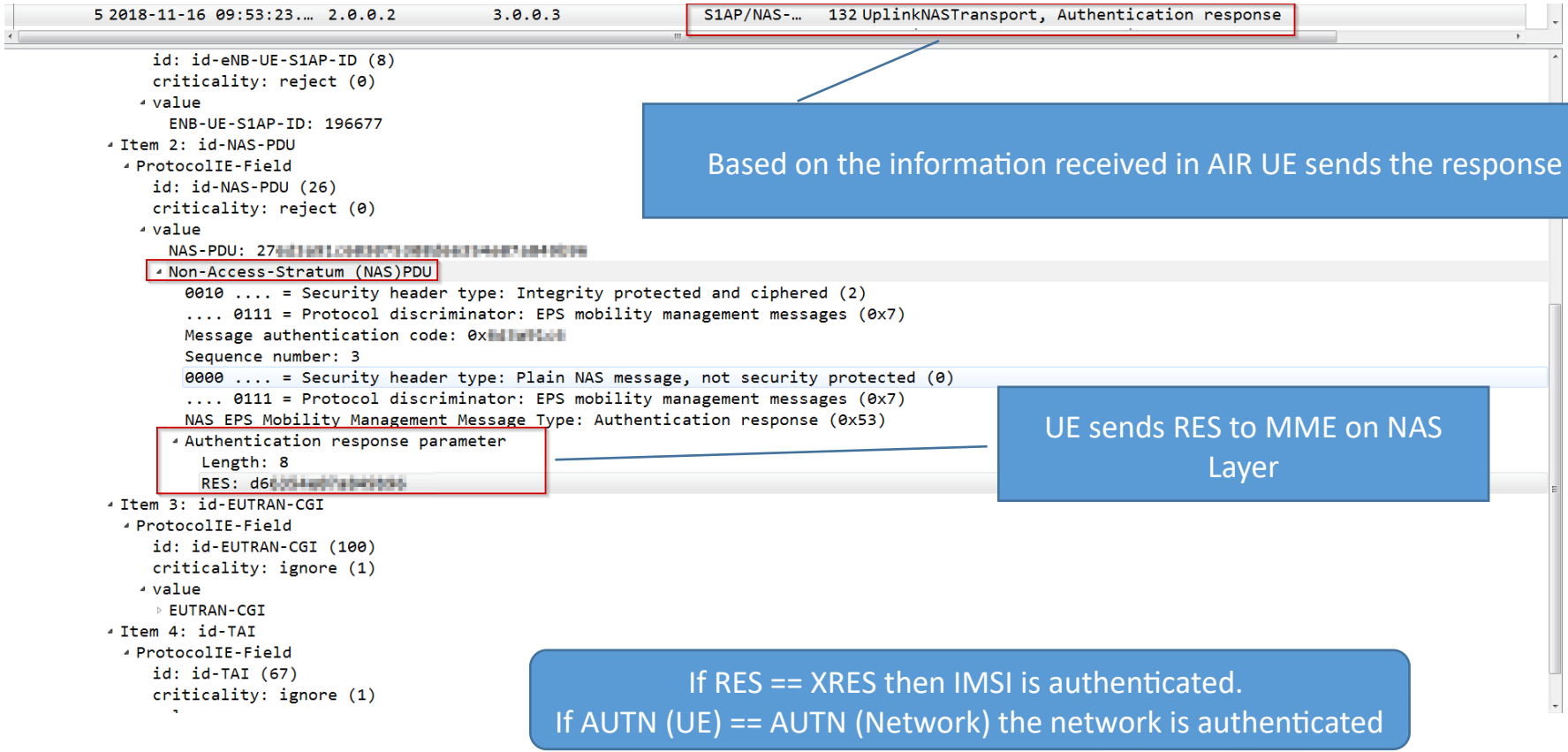
Details about the visited network are passed onto the HSS

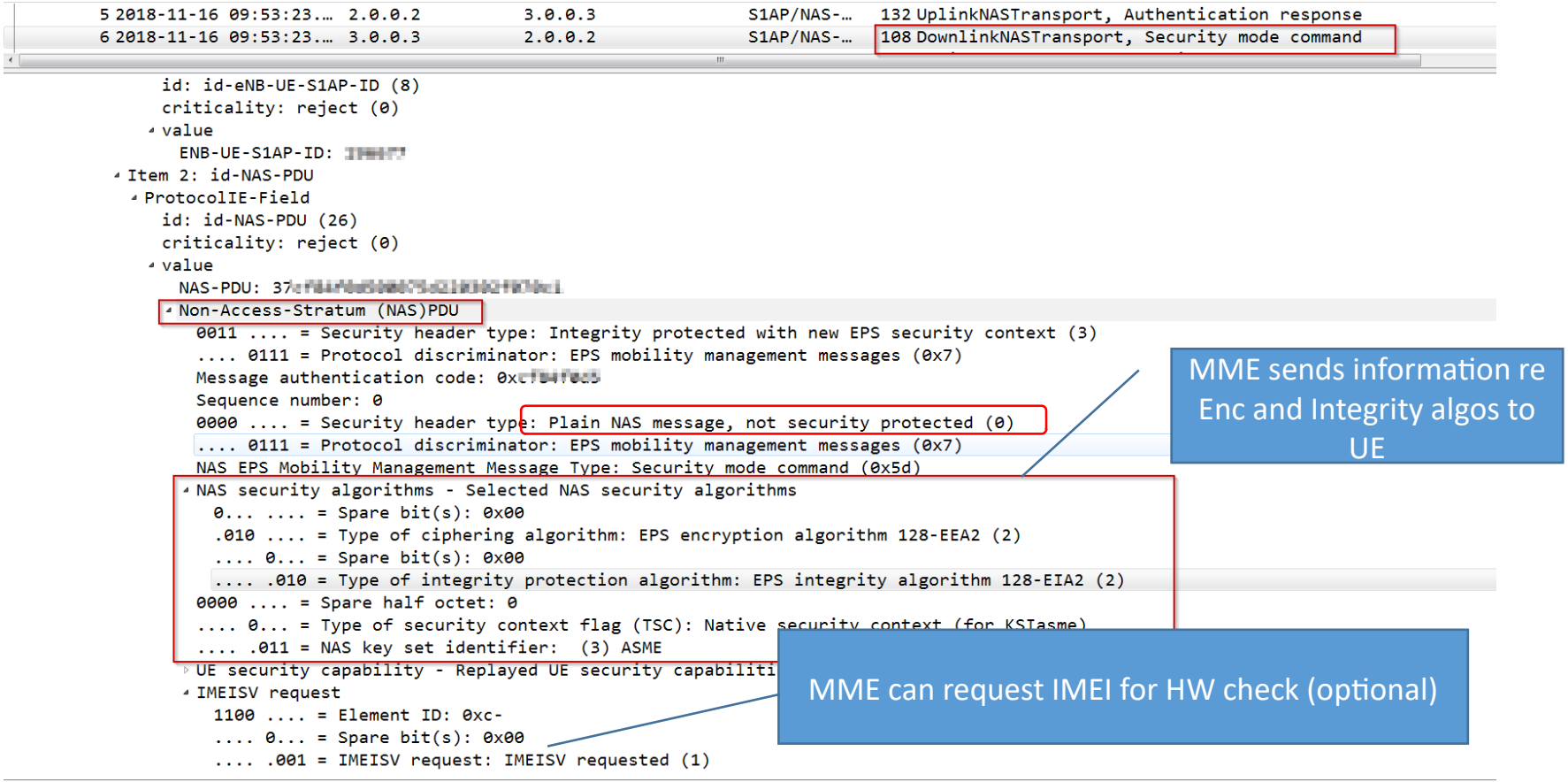


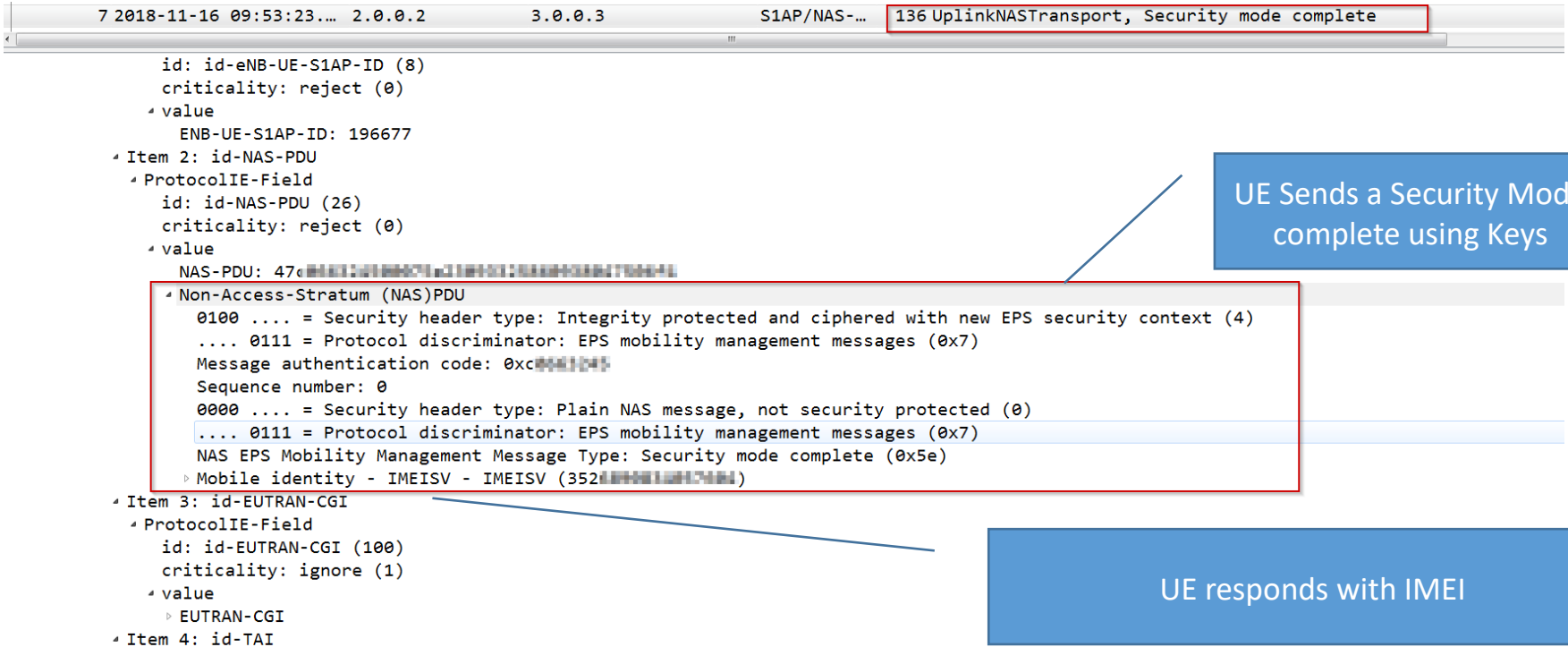

```
        AVP Code: 1419 Item-Number
      ◢ AVP Flags: 0xc0
          1... .... = Vendor-Specific: Set
          .1.. .... = Mandatory: Set
          ..0. .... = Protected: Not set
          ...0 .... = Reserved: Not set
          .... 0... = Reserved: Not set
          .... .0.. = Reserved: Not set
          .... ..0. = Reserved: Not set
          .... ...0 = Reserved: Not set
        AVP Length: 16
        AVP Vendor Id: 3GPP (10415)
        Item-Number: 1
      ▷ AVP: RAND(1447) l=28 f=VM- vnd=TGPP val=c8
      ▷ AVP: XRES(1448) l=20 f=VM- vnd=TGPP val=d6
      ▷ AVP: AUTN(1449) l=28 f=VM- vnd=TGPP val=ae
      ▷ AVP: KASME(1450) l=44 f=VM- vnd=TGPP val=6
    ◢ AVP: E-UTRAN-Vector(1414) l=148 f=VM- vnd=TGPP
        AVP Code: 1414 E-UTRAN-Vector
      ◢ AVP Flags: 0xc0
          1... .... = Vendor-Specific: Set
          .1.. .... = Mandatory: Set
          ..0. .... = Protected: Not set
          ...0 .... = Reserved: Not set
          .... 0... = Reserved: Not set
          .... .0.. = Reserved: Not set
          .... ..0. = Reserved: Not set
          .... ...0 = Reserved: Not set
        AVP Length: 148
        AVP Vendor Id: 3GPP (10415)
      ▷ E-UTRAN-Vector: 00
```

Authentication Vectors are delivered to MME from HSS over S6a (Diameter) interface


No. Time Source Destination Protocol Length Info
3 2018-11-16 09:53:23.… 4.0.0.4 3.0.0.3 DIAMETER 588 cmd=3GPP-Authentication-Information Answer(318) flags=-P-- appl=3GPP
4 2018-11-16 09:53:23.… 3.0.0.3 2.0.0.2 S1AP/NAS-… 136 DownlinkNASTransport, Authentication request
Item 1: id-eNB-UE-S1AP-ID
ProtocolIE-Field
id: id-eNB-UE-S1AP-ID (8)
criticality: reject (0)
value
ENB-UE-S1AP-ID: 196677
Item 2: id-NAS-PDU
ProtocolIE-Field
id: id-NAS-PDU (26)
criticality: reject (0)
value
NAS-PDU: 2
Non-Access-Stratum (NAS)PDU
0010 .... = Security header type: Integrity protected and ciphered (2)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
Message authentication code: 0xd377f982
Sequence number: 3
0000 .... = Security header type: Plain NAS message, not security protected (0)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
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)
.... .011 = NAS key set identifier: (3) ASME
Authentication Parameter RAND - EPS challenge
RAND value:
Authentication Parameter AUTN (UMTS and EPS authentication challenge) - EPS challenge
Length: 16
AUTN value:
SQN xor AK:
AMF:
MAC:
MME sends a Authentication Request to UE on NAS Layer
RAND, AUTN and some other values are sent to UE to assist in calculation of RES

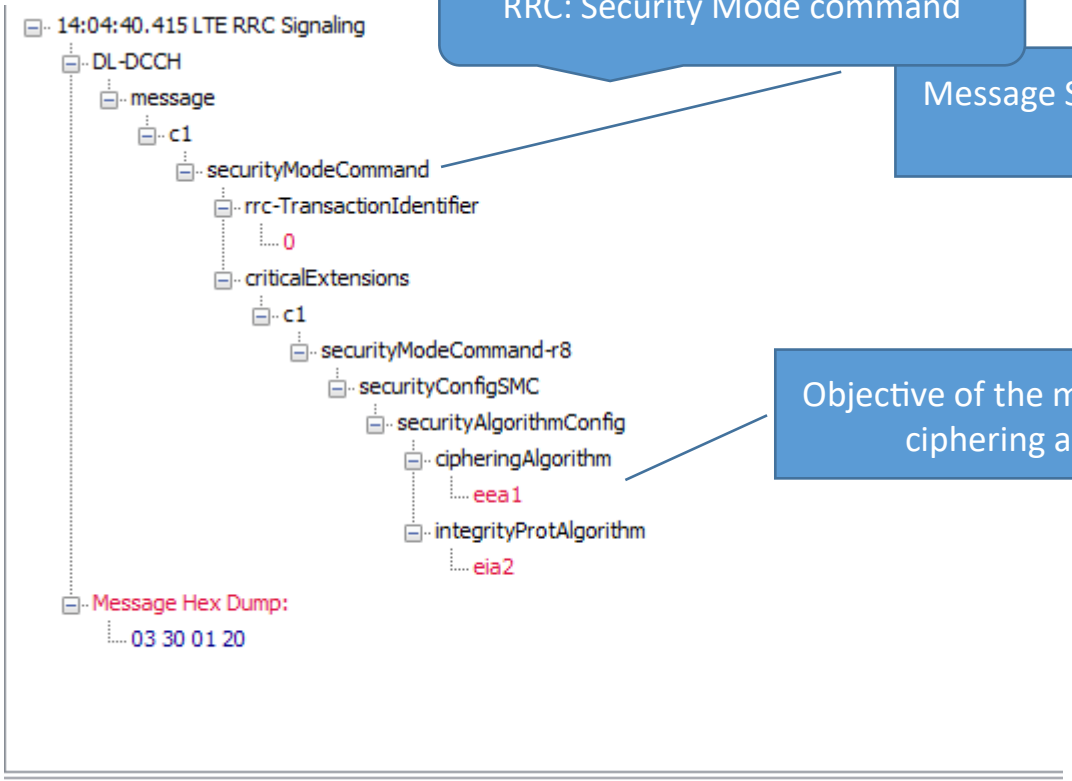

5 2018-11-16 09:53:23.… 2.0.0.2 3.0.0.3 S1AP/NAS-… 132 UplinkNASTransport, Authentication response
id: id-eNB-UE-S1AP-ID (8)
criticality: reject (0)
value
ENB-UE-S1AP-ID: 196677
Item 2: id-NAS-PDU
ProtocolIE-Field
id: id-NAS-PDU (26)
criticality: reject (0)
value
NAS-PDU: 27
Non-Access-Stratum (NAS)PDU
0010 .... = Security header type: Integrity protected and ciphered (2)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
Message authentication code: 0x
Sequence number: 3
0000 .... = Security header type: Plain NAS message, not security protected (0)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
NAS EPS Mobility Management Message Type: Authentication response (0x53)
Authentication response parameter
Length: 8
RES: d6
Item 3: id-EUTRAN-CGI
ProtocolIE-Field
id: id-EUTRAN-CGI (100)
criticality: ignore (1)
value
EUTRAN-CGI
Item 4: id-TAI
ProtocolIE-Field
id: id-TAI (67)
criticality: ignore (1)
Based on the information received in AIR UE sends the response
UE sends RES to MME on NAS Layer
If RES == XRES then IMSI is authenticated.
If AUTN (UE) == AUTN (Network) the network is authenticated


5 2018-11-16 09:53:23.… 2.0.0.2 3.0.0.3 S1AP/NAS-… 132 UplinkNASTransport, Authentication response
6 2018-11-16 09:53:23.… 3.0.0.3 2.0.0.2 S1AP/NAS-… 108 DownlinkNASTransport, Security mode command
id: id-eNB-UE-S1AP-ID (8)
criticality: reject (0)
value
ENB-UE-S1AP-ID:
Item 2: id-NAS-PDU
ProtocolIE-Field
id: id-NAS-PDU (26)
criticality: reject (0)
value
NAS-PDU: 37
Non-Access-Stratum (NAS)PDU
0011 .... = Security header type: Integrity protected with new EPS security context (3)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
Message authentication code: 0x
Sequence number: 0
0000 .... = Security header type: Plain NAS message, not security protected (0)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
NAS EPS Mobility Management Message Type: Security mode command (0x5d)
NAS security algorithms - Selected NAS security algorithms
0... .... = Spare bit(s): 0x00
.010 .... = Type of ciphering algorithm: EPS encryption algorithm 128-EEA2 (2)
.... 0... = Spare bit(s): 0x00
.... .010 = Type of integrity protection algorithm: EPS integrity algorithm 128-EIA2 (2)
0000 .... = Spare half octet: 0
.... 0... = Type of security context flag (TSC): Native security context (for KSIasme)
.... .011 = NAS key set identifier: (3) ASME
UE security capability - Replayed UE security capabiliti
IMEISV request
1100 .... = Element ID: 0xc-
.... 0... = Spare bit(s): 0x00
.... .001 = IMEISV request: IMEISV requested (1)
MME sends information re Enc and Integrity algos to UE
MME can request IMEI for HW check (optional)


7 2018-11-16 09:53:23.… 2.0.0.2 3.0.0.3 S1AP/NAS-… 136 UplinkNASTransport, Security mode complete
id: id-eNB-UE-S1AP-ID (8)
criticality: reject (0)
value
ENB-UE-S1AP-ID: 196677
Item 2: id-NAS-PDU
ProtocolIE-Field
id: id-NAS-PDU (26)
criticality: reject (0)
value
NAS-PDU: 47
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 (0x7)
Message authentication code: 0xc
Sequence number: 0
0000 .... = Security header type: Plain NAS message, not security protected (0)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
NAS EPS Mobility Management Message Type: Security mode complete (0x5e)
Mobile identity - IMEISV - IMEISV (352
Item 3: id-EUTRAN-CGI
ProtocolIE-Field
id: id-EUTRAN-CGI (100)
criticality: ignore (1)
value
EUTRAN-CGI
Item 4: id-TAI
ProtocolIE-Field
id: id-TAI (67)
criticality: ignore (1)
value
TAI
UE Sends a Security Mode complete using Keys
UE responds with IMEI

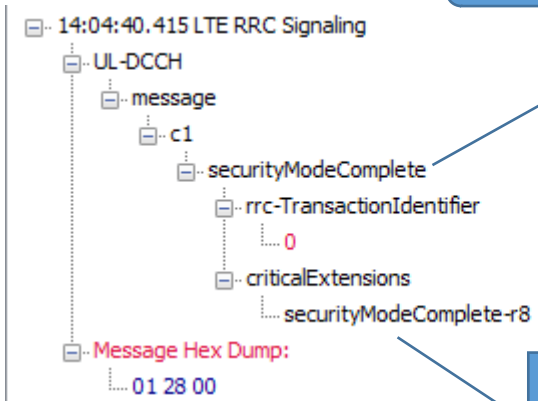
RRC: Security Mode command

Message Sent from eNB -> UE over RRC Layer.



Objective of the message is to tell UE about the ciphering and integrity algorithms

RRC: Security Mode command Complete.

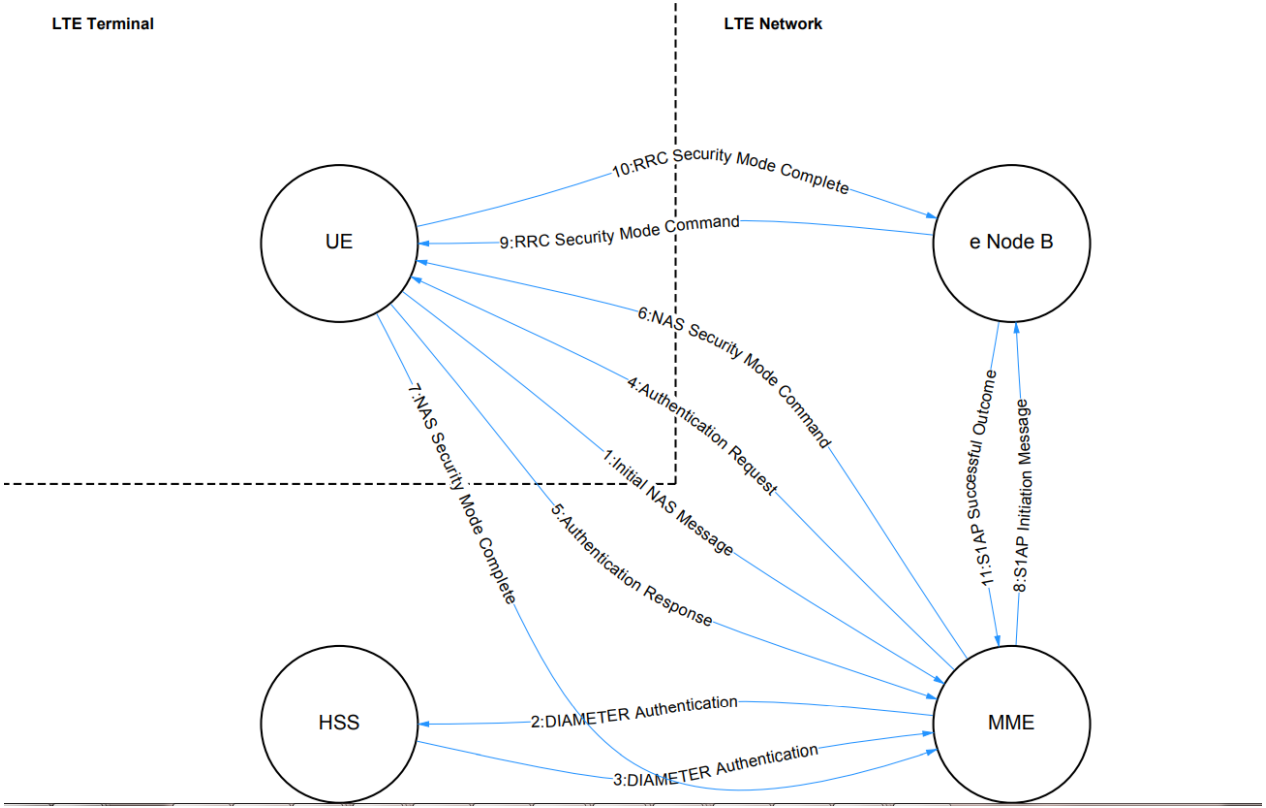


Message Sent from UE -> eNB over RRC Layer.

Objective of the message is to tell eNB that Ciphering and Integrity Algos. have been negotiated and are in use.

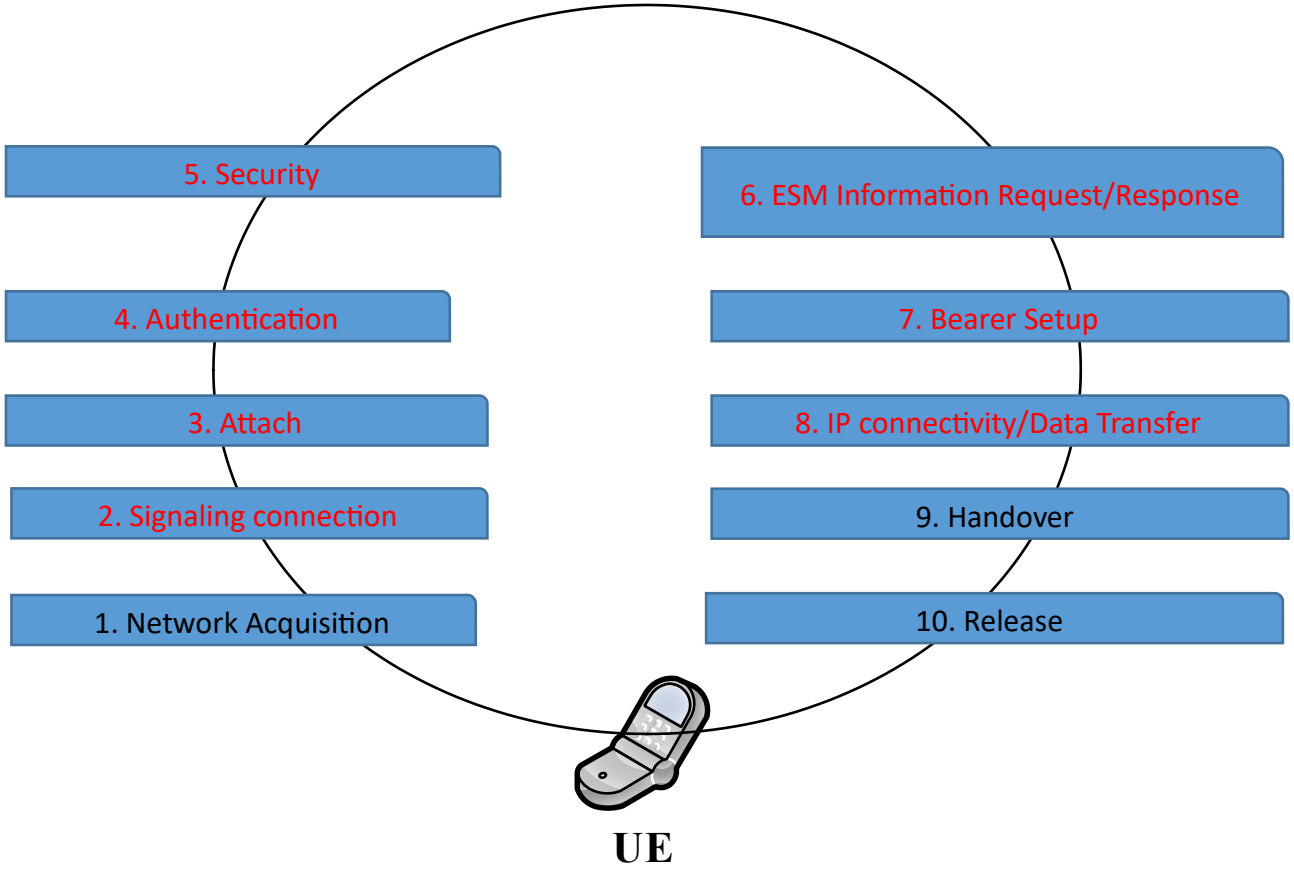
All the following RRC signaling will be protected using the algorithms as negotiated during this process.

Mind Map – Showing LTE Authentication/Security

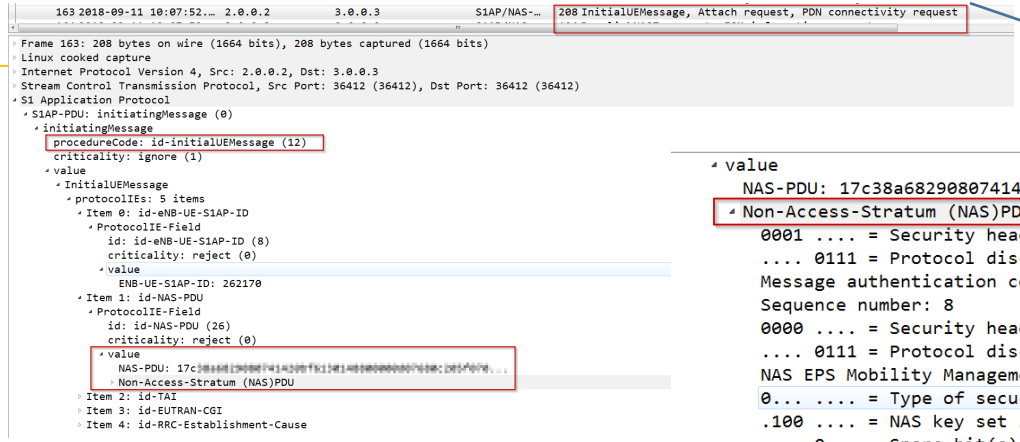


LTE Attach Call Flow

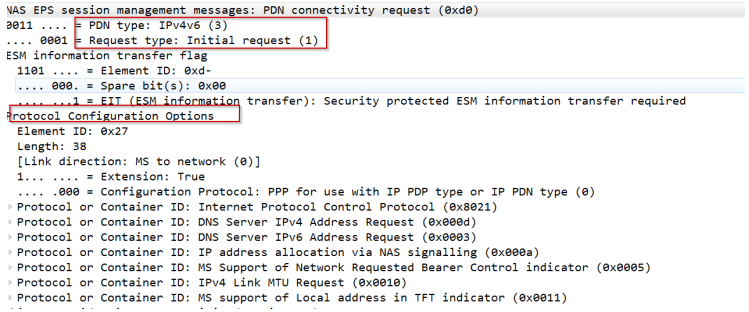
Life Cycle of a UE

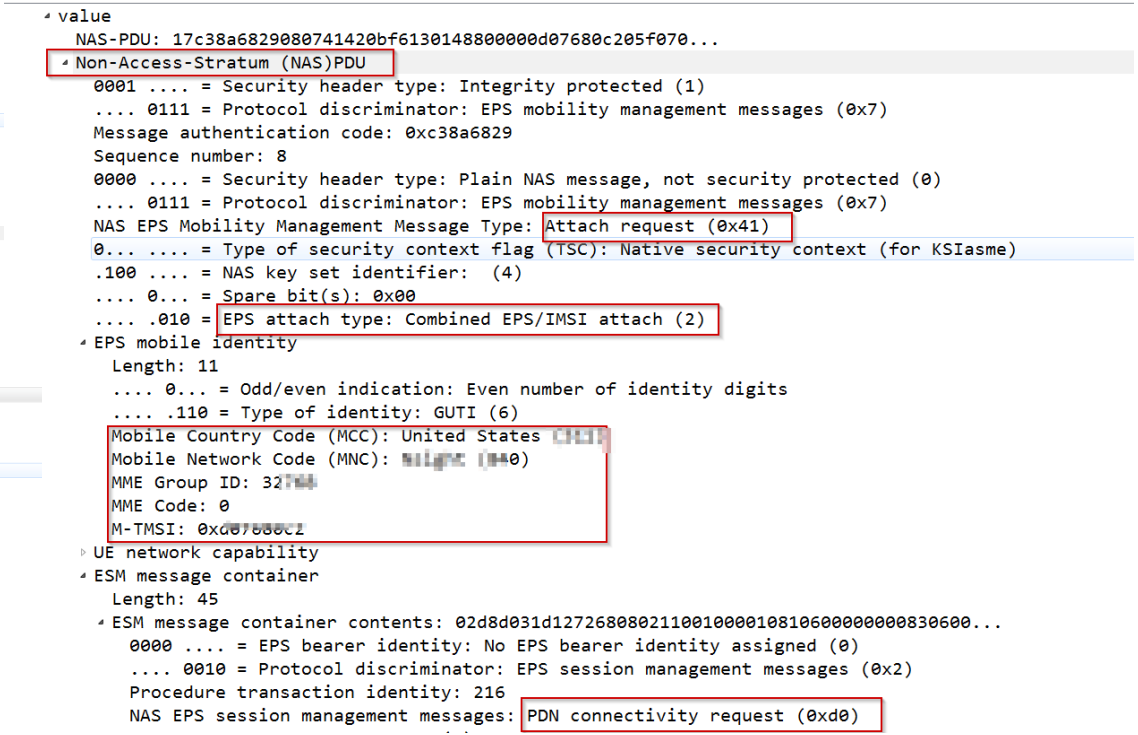


LTE Attach – Complete Picture

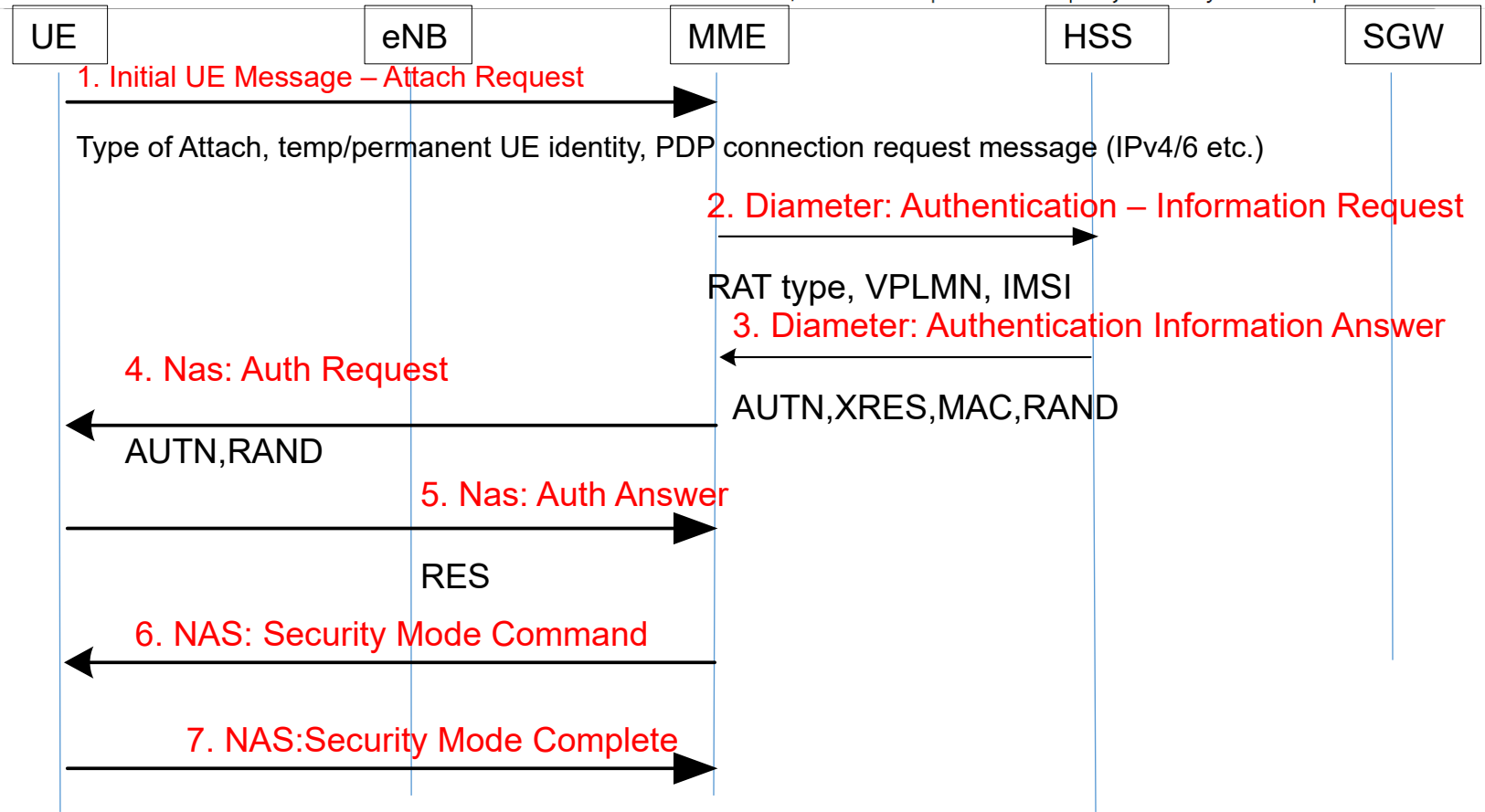


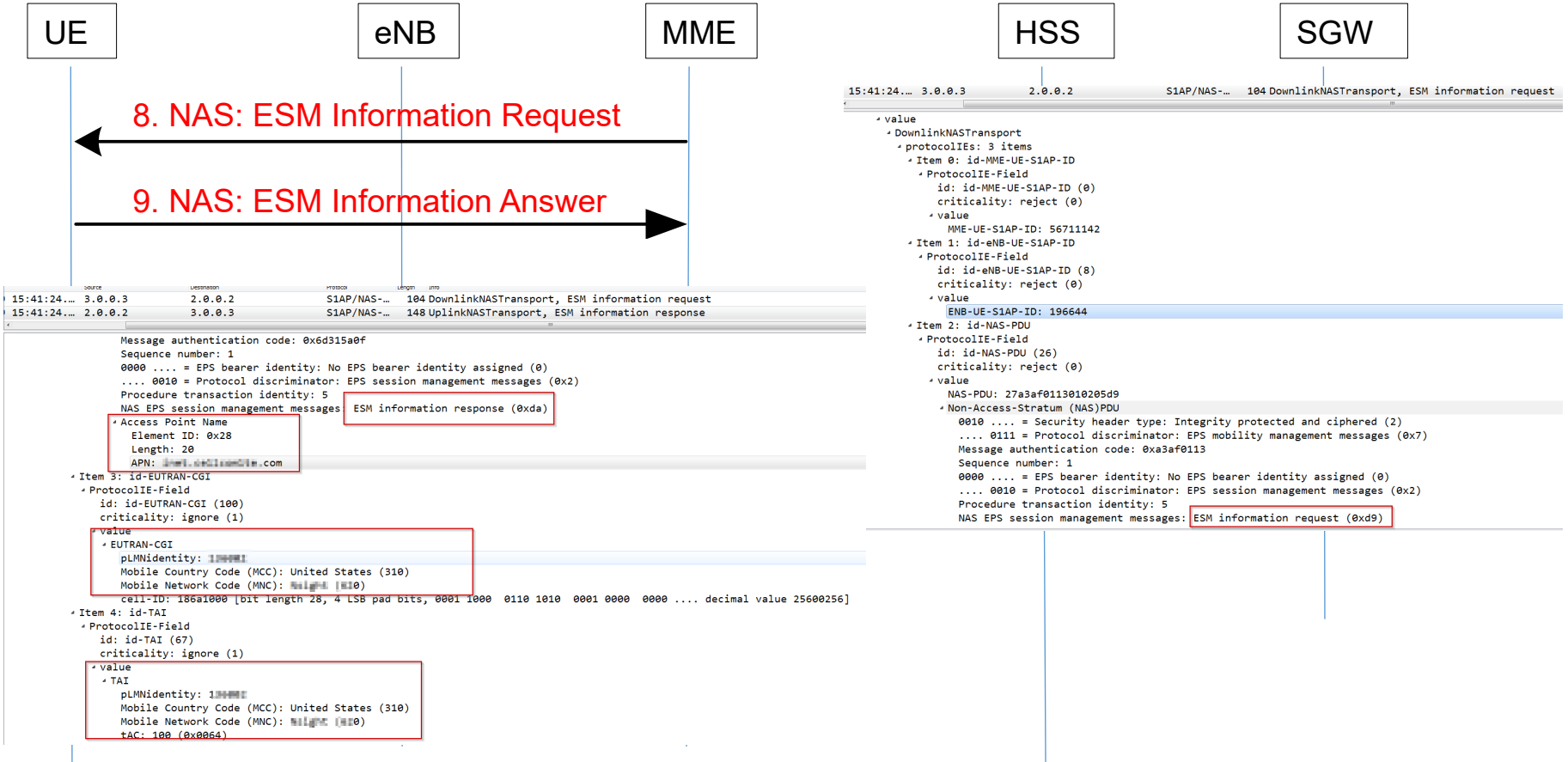
1. Initial UE Message (Attach Request)

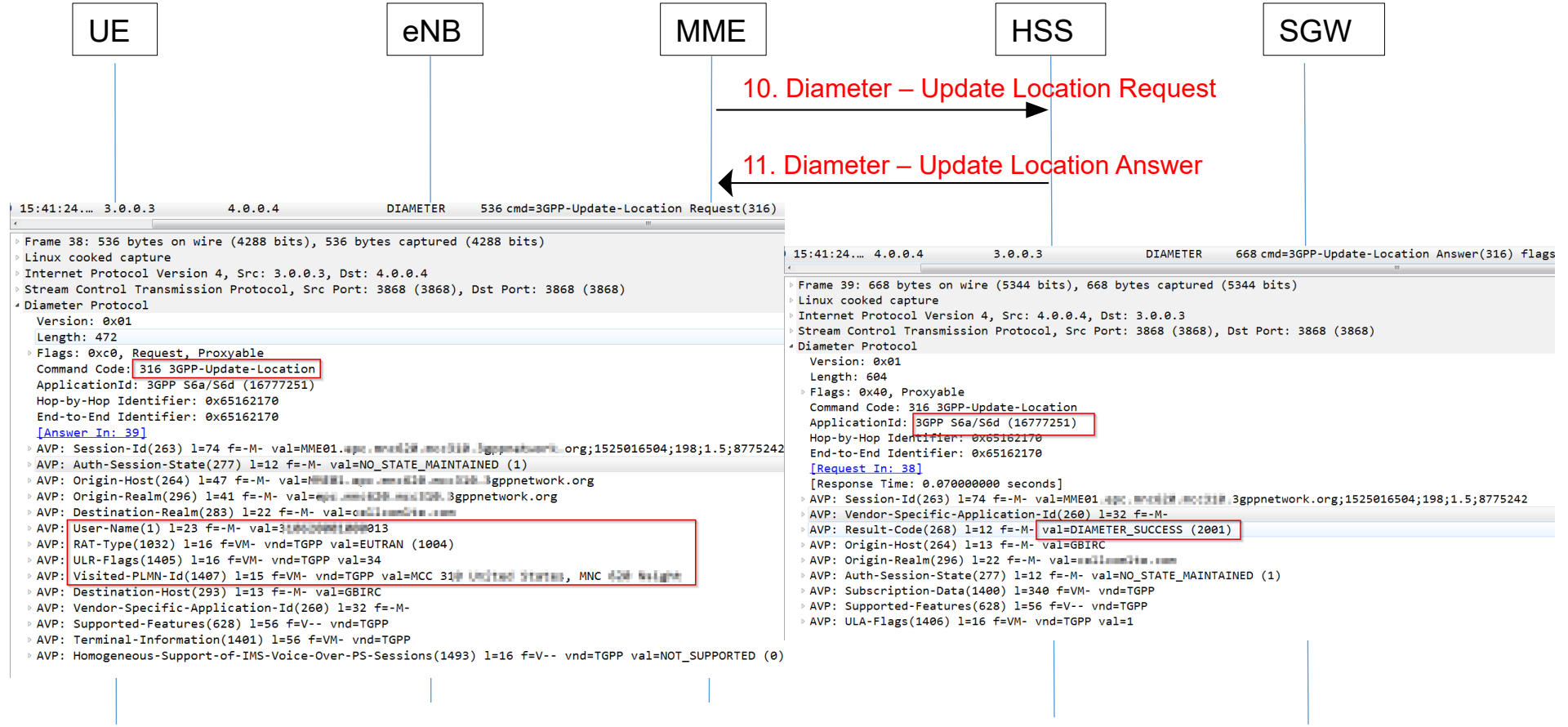


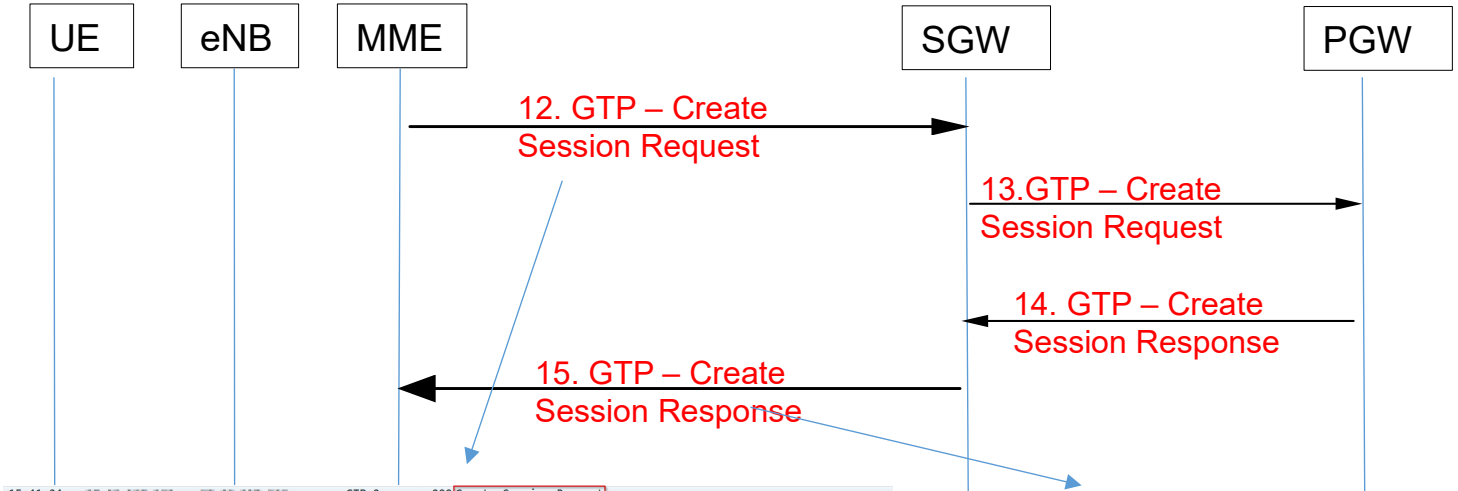


1	2018-11-16 09:53:23.…	2.0.0.2	3.0.0.3	S1AP/NAS-…	176	InitialUEMessage, Attach request, PDN connectivity request
2	2018-11-16 09:53:23.…	3.0.0.3	4.0.0.4	DIAMETER	444	cmd=3GPP-Authentication-Information Request(318) flags=RP-- appl=3GP
3	2018-11-16 09:53:23.…	4.0.0.4	3.0.0.3	DIAMETER	588	cmd=3GPP-Authentication-Information Answer(318) flags=-P-- appl=3GPP
4	2018-11-16 09:53:23.…	3.0.0.3	2.0.0.2	S1AP/NAS-…	136	DownlinkNASTransport, Authentication request
5	2018-11-16 09:53:23.…	2.0.0.2	3.0.0.3	S1AP/NAS-…	132	UplinkNASTransport, Authentication response
6	2018-11-16 09:53:23.…	3.0.0.3	2.0.0.2	S1AP/NAS-…	108	DownlinkNASTransport, Security mode command
7	2018-11-16 09:53:23.…	2.0.0.2	3.0.0.3	S1AP/NAS-…	136	UplinkNASTransport, Security mode complete




UE
eNB
MME
HSS
SGW
8. NAS: ESM Information Request
9. NAS: ESM Information Answer
15:41:24.… 3.0.0.3 2.0.0.2 S1AP/NAS-… 104 DownlinkNASTransport, ESM information request
15:41:24.… 2.0.0.2 3.0.0.3 S1AP/NAS-… 148 UplinkNASTransport, ESM information response
Message authentication code: 0x6d315a0f
Sequence number: 1
0000 .... = EPS bearer identity: No EPS bearer identity assigned (0)
.... 0010 = Protocol discriminator: EPS session management messages (0x2)
Procedure transaction identity: 5
NAS EPS session management messages: ESM information response (0xda)
Access Point Name
Element ID: 0x28
Length: 20
APN:
Item 3: id-EUTRAN-CGI
ProtocolIE-Field
id: id-EUTRAN-CGI (100)
criticality: ignore (1)
value
EUTRAN-CGI
pLMNidentity:
Mobile Country Code (MCC): United States (310)
Mobile Network Code (MNC):
cell-ID: 186a1000 [bit length 28, 4 LSB pad bits, 0001 1000 0110 1010 0001 0000 0000 .... decimal value 25600256]
Item 4: id-TAI
ProtocolIE-Field
id: id-TAI (67)
criticality: ignore (1)
value
TAI
pLMNidentity:
Mobile Country Code (MCC): United States (310)
Mobile Network Code (MNC):
tAC: 100 (0x0064)
15:41:24.… 3.0.0.3 2.0.0.2 S1AP/NAS-… 104 DownlinkNASTransport, ESM information request
value
DownlinkNASTransport
protocolIEs: 3 items
Item 0: id-MME-UE-S1AP-ID
ProtocolIE-Field
id: id-MME-UE-S1AP-ID (0)
criticality: reject (0)
value
MME-UE-S1AP-ID: 56711142
Item 1: id-eNB-UE-S1AP-ID
ProtocolIE-Field
id: id-eNB-UE-S1AP-ID (8)
criticality: reject (0)
value
ENB-UE-S1AP-ID: 196644
Item 2: id-NAS-PDU
ProtocolIE-Field
id: id-NAS-PDU (26)
criticality: reject (0)
value
NAS-PDU: 27a3af0113010205d9
Non-Access-Stratum (NAS)PDU
0010 .... = Security header type: Integrity protected and ciphered (2)
.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
Message authentication code: 0xa3af0113
Sequence number: 1
0000 .... = EPS bearer identity: No EPS bearer identity assigned (0)
.... 0010 = Protocol discriminator: EPS session management messages (0x2)
Procedure transaction identity: 5
NAS EPS session management messages: ESM information request (0xd9)


UE
eNB
MME
HSS
SGW
10. Diameter – Update Location Request
11. Diameter – Update Location Answer
15:41:24.… 3.0.0.3 4.0.0.4 DIAMETER 536 cmd=3GPP-Update-Location Request(316)
Frame 38: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 3.0.0.3, Dst: 4.0.0.4
Stream Control Transmission Protocol, Src Port: 3868 (3868), Dst Port: 3868 (3868)
Diameter Protocol
Version: 0x01
Length: 472
Flags: 0xc0, Request, Proxyable
Command Code: 316 3GPP-Update-Location
ApplicationId: 3GPP S6a/S6d (16777251)
Hop-by-Hop Identifier: 0x65162170
End-to-End Identifier: 0x65162170
[Answer In: 39]
AVP: Session-Id(263) l=74 f=-M- val=MME01.
org;1525016504;198;1.5;8775242
AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
AVP: Origin-Host(264) l=47 f=-M- val=
3gppnetwork.org
AVP: Origin-Realm(296) l=41 f=-M- val=
3gppnetwork.org
AVP: Destination-Realm(283) l=22 f=-M- val=
AVP: User-Name(1) l=23 f=-M- val=
013
AVP: RAT-Type(1032) l=16 f=VM- vnd=TGPP val=EUTRAN (1004)
AVP: ULR-Flags(1405) l=16 f=VM- vnd=TGPP val=34
AVP: Visited-PLMN-Id(1407) l=15 f=VM- vnd=TGPP val=MCC 31
, MNC
AVP: Destination-Host(293) l=13 f=-M- val=GBIRC
AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
AVP: Supported-Features(628) l=56 f=V-- vnd=TGPP
AVP: Terminal-Information(1401) l=56 f=VM- vnd=TGPP
AVP: Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions(1493) l=16 f=V-- vnd=TGPP val=NOT_SUPPORTED (0)
15:41:24.… 4.0.0.4 3.0.0.3 DIAMETER 668 cmd=3GPP-Update-Location Answer(316) flags
Frame 39: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 4.0.0.4, Dst: 3.0.0.3
Stream Control Transmission Protocol, Src Port: 3868 (3868), Dst Port: 3868 (3868)
Diameter Protocol
Version: 0x01
Length: 604
Flags: 0x40, Proxyable
Command Code: 316 3GPP-Update-Location
ApplicationId: 3GPP S6a/S6d (16777251)
Hop-by-Hop Identifier: 0x65162170
End-to-End Identifier: 0x65162170
[Request In: 38]
[Response Time: 0.070000000 seconds]
AVP: Session-Id(263) l=74 f=-M- val=MME01.
3gppnetwork.org;1525016504;198;1.5;8775242
AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
AVP: Result-Code(268) l=12 f=-M- val=DIAMETER_SUCCESS (2001)
AVP: Origin-Host(264) l=13 f=-M- val=GBIRC
AVP: Origin-Realm(296) l=22 f=-M- val=
AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
AVP: Subscription-Data(1400) l=340 f=VM- vnd=TGPP
AVP: Supported-Features(628) l=56 f=V-- vnd=TGPP
AVP: ULA-Flags(1406) l=16 f=VM- vnd=TGPP val=1




```
15:41:24.…                          GTPv2      299 Create Session Request
Frame 40: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits)
Linux cooked capture
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
User Datagram Protocol, Src Port: 33968, Dst Port: 2123
GPRS Tunneling Protocol V2
  Flags: 0x48
  Message Type: Create Session Request (32)
  Message Length: 251
  Tunnel Endpoint Identifier: 0x00000000 (0)
  Sequence Number: 0x00001908 (6408)
  Spare: 0
  International Mobile Subscriber Identity (IMSI) : 31[redacted]13
  MSISDN : 9[redacted]83
  Mobile Equipment Identity (MEI) : 01[redacted]15
  User Location Info (ULI) : TAI ECGI
  Serving Network : MCC 31[redacted] United States, MNC [redacted] Sprint
  RAT Type : EUTRAN (6)
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S11 MME GTP-C interface, TEID/GRE Key: 0x09500078, IPv4 [redacted]
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 PGW GTP-C interface, TEID/GRE Key: 0x00000000, IPv4 [redacted]
  Access Point Name (APN) : inet.[redacted].gprs
  Selection Mode : MS or network provided APN, subscribed verified
  PDN Type : IPv4
  PDN Address Allocation (PAA) :
  APN Restriction : value 0
  Aggregate Maximum Bit Rate (AMBR) :
  Protocol Configuration Options (PCO) :
  Bearer Context : [Grouped IE]
  Recovery (Restart Counter) : 170
  UE Time Zone :
```

```
15:41:25.…                          GTPv2      202 Create Session Response
Frame 41: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits)
Linux cooked capture
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
User Datagram Protocol, Src Port: 2123, Dst Port: 33968
GPRS Tunneling Protocol V2
  Flags: 0x48
  Message Type: Create Session Response (33)
  Message Length: 154
  Tunnel Endpoint Identifier: 0x09500078 (156237944)
  Sequence Number: 0x00001908 (6408)
  Spare: 0
  Cause : Request accepted (16)
  Bearer Context : [Grouped IE]
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S11/S4 SGW GTP-C interface, TEID/GRE Key: 0xb5f00d60, IPv4 [redacted]
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 PGW GTP-C interface, TEID/GRE Key: 0x7a8d1d30, IPv4 [redacted]
  PDN Address Allocation (PAA) :
  APN Restriction : value 0
  Aggregate Maximum Bit Rate (AMBR) :
  Protocol Configuration Options (PCO) :
  Recovery (Restart Counter) : 8
  [Response To: 40]
  [Response Time: 0.081000000 seconds]
```

UE | eNB | MME | HSS | SGW

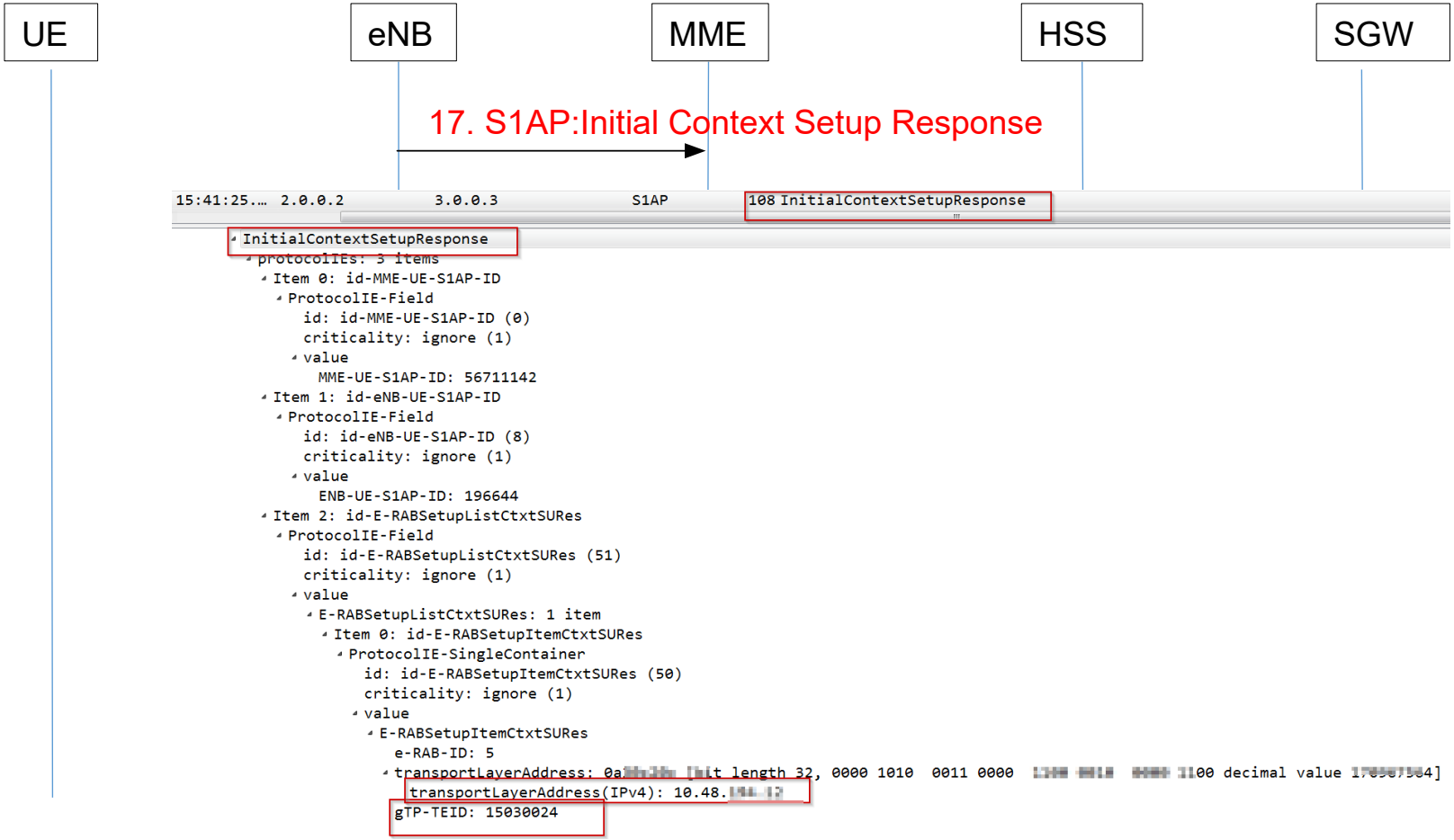
16. S1AP:Initial Context Setup Request

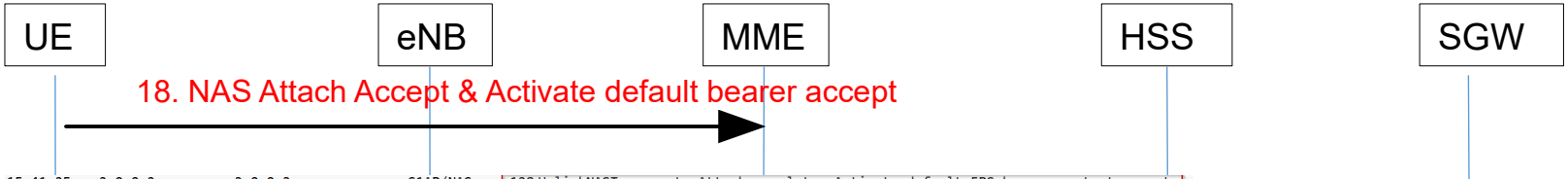
```
15:41:25.…  3.0.0.3   2.0.0.2   S1AP/NAS-…  356 InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request …
```

```
initiatingMessage
  procedureCode: id-InitialContextSetup (9)
  criticality: reject (0)
  value
    InitialContextSetupRequest
      protocolIEs: 8 items
        Item 0: id-MME-UE-S1AP-ID
          ProtocolIE-Field
            id: id-MME-UE-S1AP-ID (0)
            criticality: reject (0)
            value
              MME-UE-S1AP-ID: 56711142
        Item 1: id-eNB-UE-S1AP-ID
          ProtocolIE-Field
            id: id-eNB-UE-S1AP-ID (8)
            criticality: reject (0)
            value
              ENB-UE-S1AP-ID: 196644
        Item 2: id-uEaggregateMaximumBitrate
          ProtocolIE-Field
            id: id-uEaggregateMaximumBitrate (66)
            criticality: reject (0)
            value
              UEAggregateMaximumBitrate
                uEaggregateMaximumBitRateDL: 5000bits/s
                uEaggregateMaximumBitRateUL: 500bits/s
        Item 4: id-UESecurityCapabilities
          ProtocolIE-Field
            id: id-UESecurityCapabilities (107)
            criticality: reject (0)
            value
              UESecurityCapabilities
                encryptionAlgorithms: c000 [bit length 16, 1100 0000  0000 0000 decimal value 49152]
                  1... .... .... .... = 128-EEA1: Supported
                  .1.. .... .... .... = 128-EEA2: Supported
                  ..0. .... .... .... = 128-EEA3: Not supported
                  ...0 0000 0000 0000 = Reserved: 0x0000
                integrityProtectionAlgorithms: c000 [bit length 16, 1100 0000  0000 0000 decimal value 49152]
                  1... .... .... .... = 128-EIA1: Supported
                  .1.. .... .... .... = 128-EIA2: Supported
                  ..0. .... .... .... = 128-EIA3: Not supported
                  ...0 0000 0000 0000 = Reserved: 0x0000
        Item 5: id-SecurityKey
          ProtocolIE-Field
            id: id-SecurityKey (73)
            criticality: reject (0)
            value
              SecurityKey: [illegible]6... [bit length 256]
```

```
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
                  qCI: 9
                  allocationRetentionPriority
                transportLayerAddress: 0a2b7712 [bit length 32, 0000 1010  0010 1011  0111 0111  0001 0010 decimal value 170620690]
                gTP-TEID: b5f00072
                nAS-PDU: 274eba[illegible]
```

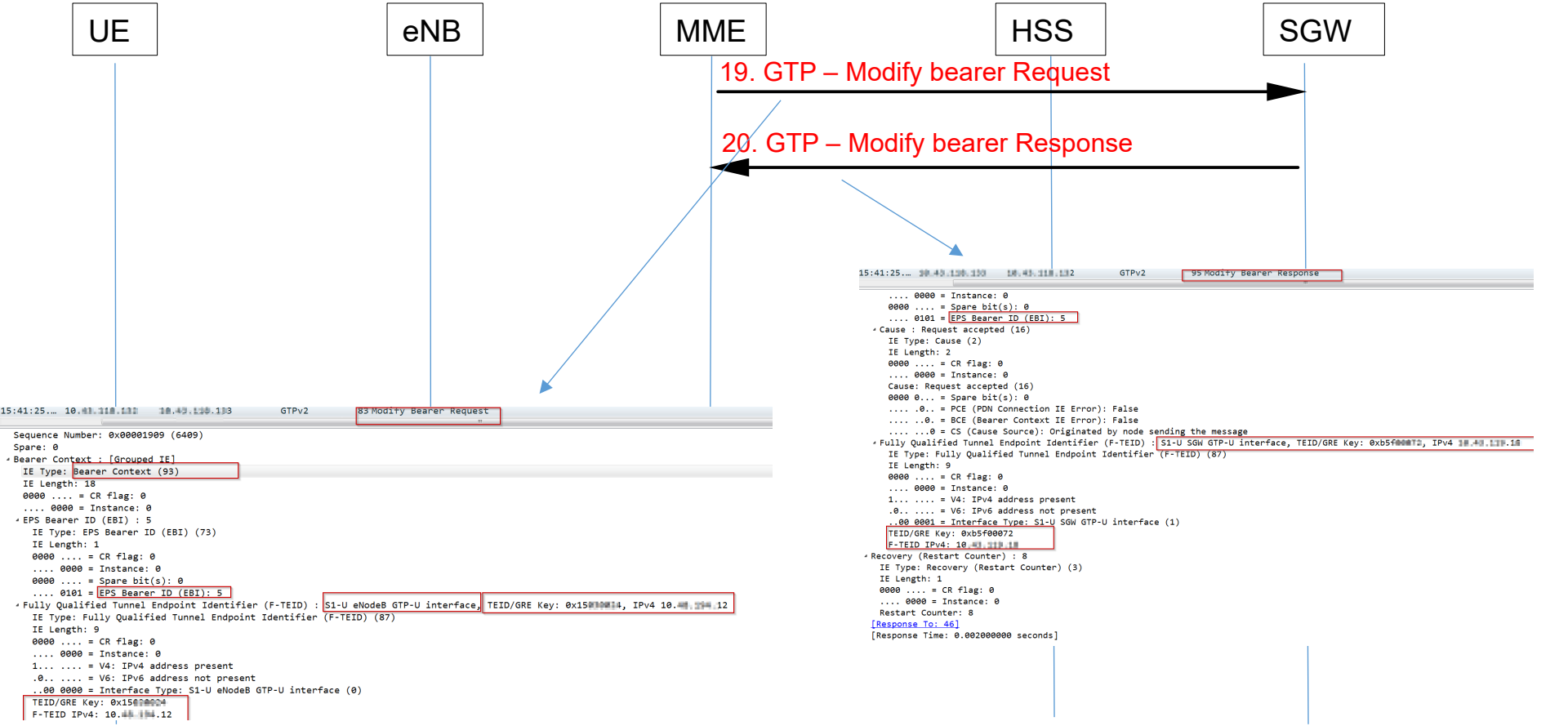
```
Non-Access-Stratum (NAS)PDU
  0010 .... = Security header type: Integrity protected and ciphered (2)
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
  Message authentication code: 0x4eba2668
  Sequence number: 2
  0000 .... = Security header type: Plain NAS message, not security protected (0)
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
  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
  EMM cause
  EPS network feature support
```


UE
eNB
MME
HSS
SGW
17. S1AP:Initial Context Setup Response
15:41:25.… 2.0.0.2 3.0.0.3 S1AP 108 InitialContextSetupResponse
InitialContextSetupResponse
protocolIEs: 3 items
Item 0: id-MME-UE-S1AP-ID
ProtocolIE-Field
id: id-MME-UE-S1AP-ID (0)
criticality: ignore (1)
value
MME-UE-S1AP-ID: 56711142
Item 1: id-eNB-UE-S1AP-ID
ProtocolIE-Field
id: id-eNB-UE-S1AP-ID (8)
criticality: ignore (1)
value
ENB-UE-S1AP-ID: 196644
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
transportLayerAddress: 0a
transportLayerAddress(IPv4): 10.48.
gTP-TEID: 15030024

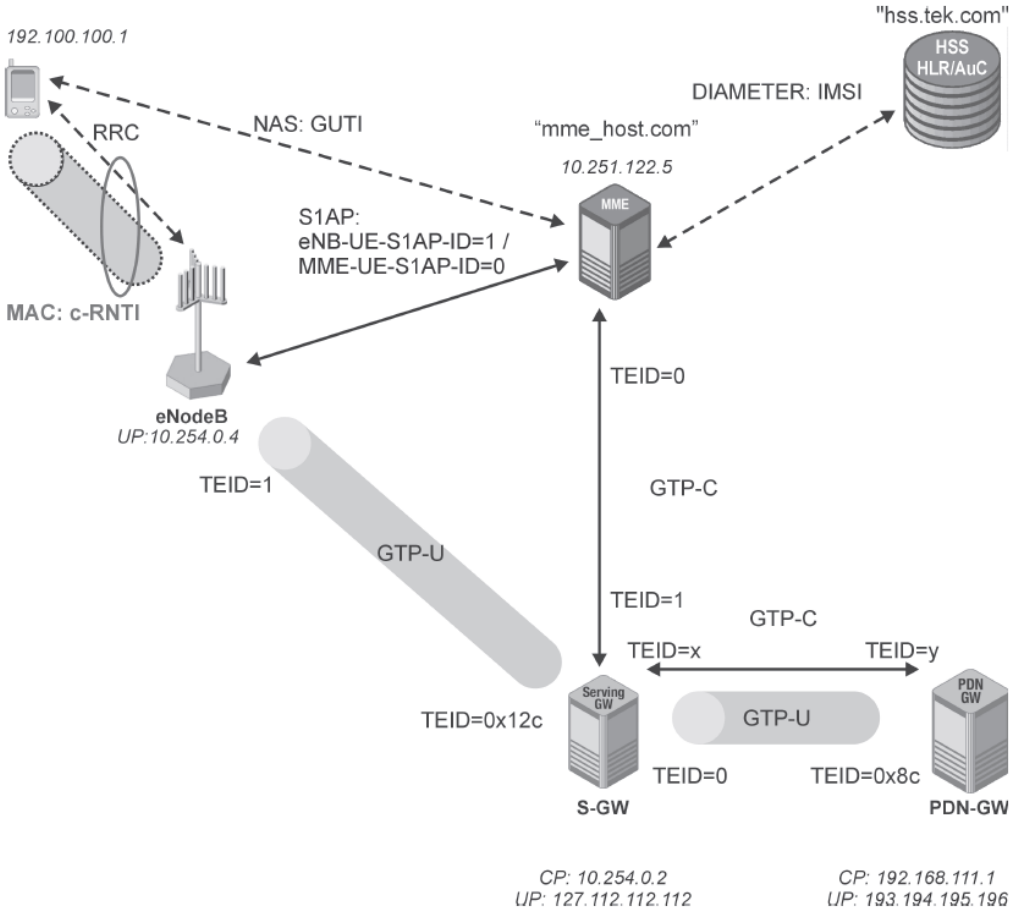



```
15:41:25.…  2.0.0.2          3.0.0.3          S1AP/NAS-…  128 UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
Frame 45: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 2.0.0.2, Dst: 3.0.0.3
Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
S1 Application Protocol
 S1AP-PDU: initiatingMessage (0)
  initiatingMessage
    procedureCode: id-uplinkNASTransport (13)
    criticality: ignore (1)
   value
    UplinkNASTransport
     protocolIEs: 5 items
      Item 0: id-MME-UE-S1AP-ID
       ProtocolIE-Field
          id: id-MME-UE-S1AP-ID (0)
          criticality: reject (0)
         value
           MME-UE-S1AP-ID: 56711142
      Item 1: id-eNB-UE-S1AP-ID
       ProtocolIE-Field
          id: id-eNB-UE-S1AP-ID (8)
          criticality: reject (0)
         value
           ENB-UE-S1AP-ID: 196644
```

```
    Non-Access-Stratum (NAS)PDU
       0010 .... = Security header type: Integrity protected and ciphered (2)
       .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
      Message authentication code: [illegible]79f
      Sequence number: 2
      0000 .... = Security header type: Plain NAS message, not security protected (0)
      .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
      NAS EPS Mobility Management Message Type: Attach complete (0x43)
     ESM message container
       Length: 3
      ESM message container contents: 5200c2
         0101 .... = EPS bearer identity: EPS bearer identity value 5 (5)
         .... 0010 = Protocol discriminator: EPS session management messages (0x2)
         Procedure transaction identity: 0
         NAS EPS session management messages: Activate default EPS bearer context accept (0xc2)
Item 3: id-EUTRAN-CGI
 ProtocolIE-Field
    id: id-EUTRAN-CGI (1[illegible])
    criticality: ignore (1)
   value
    EUTRAN-CGI
       pLMNidentity: [illegible]2
       Mobile Country Code (MCC): United [illegible]0)
       Mobile Network Code (MNC): [illegible]0)
       cell-ID: 18[illegible] [bit length 28, 4 LSB pad bits, 0001 1000  0110 1010  0001 0000  0000 .... decimal value [illegible]6]
Item 4: id-TAI
 ProtocolIE-Field
    id: id-TAI (67)
    criticality: ignore (1)
   value
    TAI
       pLMNidentity: 1[illegible]02
```


UE
eNB
MME
HSS
SGW
19. GTP – Modify bearer Request
20. GTP – Modify bearer Response
15:41:25.… 10.41.118.131 10.43.130.193 GTPv2 83 Modify Bearer Request
Sequence Number: 0x00001909 (6409)
Spare: 0
Bearer Context : [Grouped IE]
IE Type: Bearer Context (93)
IE Length: 18
0000 .... = CR flag: 0
.... 0000 = Instance: 0
EPS Bearer ID (EBI) : 5
IE Type: EPS Bearer ID (EBI) (73)
IE Length: 1
0000 .... = CR flag: 0
.... 0000 = Instance: 0
0000 .... = Spare bit(s): 0
.... 0101 = EPS Bearer ID (EBI): 5
Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S1-U eNodeB GTP-U interface, TEID/GRE Key: 0x15
IE Type: Fully Qualified Tunnel Endpoint Identifier (F-TEID) (87)
IE Length: 9
0000 .... = CR flag: 0
.... 0000 = Instance: 0
1... .... = V4: IPv4 address present
.0.. .... = V6: IPv6 address not present
..00 0000 = Interface Type: S1-U eNodeB GTP-U interface (0)
TEID/GRE Key: 0x15
F-TEID IPv4: 10.
15:41:25.… GTPv2 95 Modify Bearer Response
.... 0000 = Instance: 0
0000 .... = Spare bit(s): 0
.... 0101 = EPS Bearer ID (EBI): 5
Cause : Request accepted (16)
IE Type: Cause (2)
IE Length: 2
0000 .... = CR flag: 0
.... 0000 = Instance: 0
Cause: Request accepted (16)
0000 0... = Spare bit(s): 0
.... .0.. = PCE (PDN Connection IE Error): False
.... ..0. = BCE (Bearer Context IE Error): False
....0 = CS (Cause Source): Originated by node sending the message
Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S1-U SGW GTP-U interface, TEID/GRE Key: 0xb5f
IE Type: Fully Qualified Tunnel Endpoint Identifier (F-TEID) (87)
IE Length: 9
0000 .... = CR flag: 0
.... 0000 = Instance: 0
1... .... = V4: IPv4 address present
.0.. .... = V6: IPv6 address not present
..00 0001 = Interface Type: S1-U SGW GTP-U interface (1)
TEID/GRE Key: 0xb5f00072
F-TEID IPv4: 10.
Recovery (Restart Counter) : 8
IE Type: Recovery (Restart Counter) (3)
IE Length: 1
0000 .... = CR flag: 0
.... 0000 = Instance: 0
Restart Counter: 8
[Response To: 46]
[Response Time: 0.002000000 seconds]

Signaling and user plane connection after successful attach



LTE Roaming Architecture

LTE Roaming

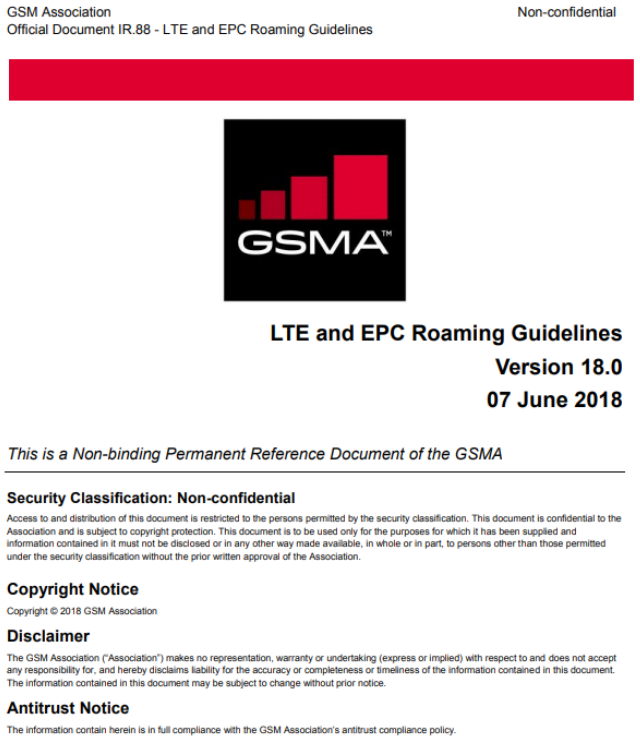
Roaming is an important functionality, where operators share their networks with each other's subscribers. Typically roaming happens between operators serving different areas, such as different countries, since this does not cause conflicts in the competition between the operators,
and the combined larger service area benefits them as well as the subscribers.

The words *home* and *visited* are used as prefixes to many other architectural terms to describe where the subscriber originates from and where it roams to respectively.

3GPP SAE specifications define which interfaces can be used between operators, and what additional considerations are needed if an operator boundary is crossed. In addition to the connectivity
between the networks, roaming requires that the operators agree on many things at the service level, e.g. what services are available, how they are realized, and how accounting and charging is handled. This agreement is called the *Roaming Agreement*, and it can be made directly between the operators, or through a broker. The 3GPP specifications do not cover these
items, and operators using 3GPP technologies discuss roaming related general questions in a private forum called the GSM Association, which has published recommendations to cover these additional requirements.

LTE Roaming

https://www.gsma.com/newsroom/wp-content/uploads//IR.88-v18.0.pdf



GSM Association
Official Document IR.88 - LTE and EPC Roaming Guidelines

Non-confidential

GSMA

LTE and EPC Roaming Guidelines
Version 18.0
07 June 2018

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2018 GSM Association

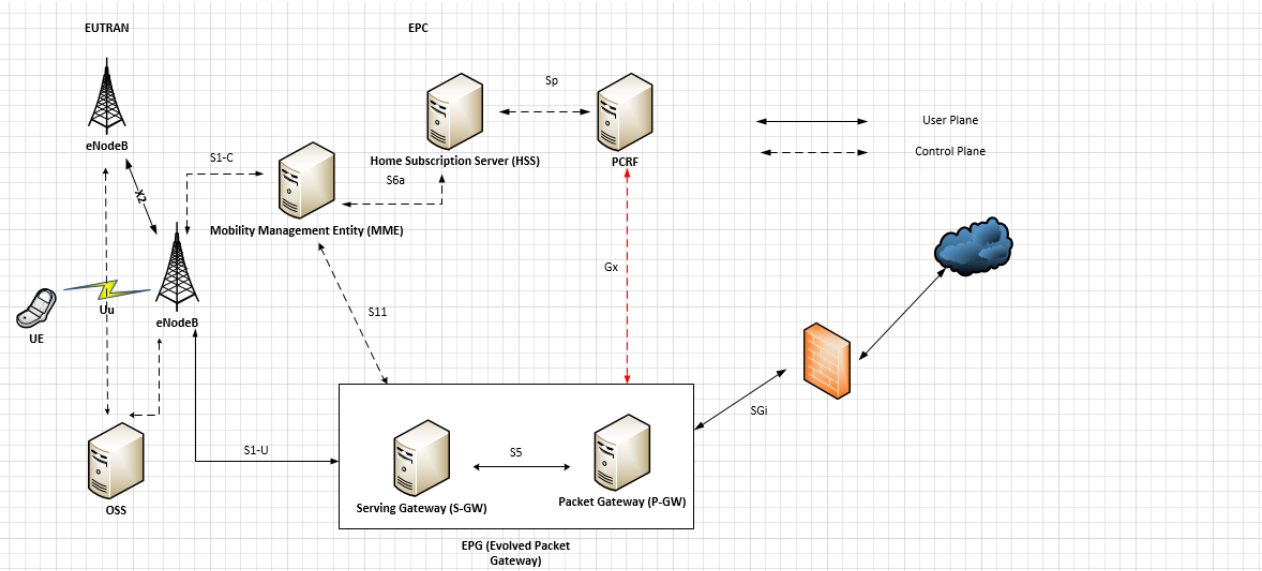
Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

LTE Roaming



eNodeB Functions:

- Radio Resource management, radio bearer control, radio admission control, connection mobility control, uplink/ downlink scheduling
- IP header compression and ciphering of the User data stream.
- MME selection
- Paging
- CMAS

MME Functions:

- Non-Access Stratum (NAS) signaling (attachment, bearer setup/deletion)
- NAS signaling security
- Signaling for mobility between 3GPP access networks
- Idle mode user tracking
- Tracking Area list mgmt.
- PDN gateway, S-GW selection
- Roaming – S6a interface to HSS
- Authentication

Serving Gateway Functions:

- Local mobility anchor for inter-eNodeB handover.
- EUTRAN downlink packet buffering-while idle UE is being paged.
- Lawful intercept
- Packet routing and forwarding
- Transport level packet marking (UL/DL)
- Accounting for inter-operator charging.
- Accounting per UE

Home Subscriber Server:

- Storage of Sub Data (Auth keys, QoS profile, APN profile etc.).
- Address of currently serving MME, TA

PDN Gateway:

- Lawful Intercept
- IP address allocation
- Transport level marking for DL
- Downlink rate enforcement based on AMBR (Aggregate Maximum Bit Rate)
- Accounting per UE

Policy Charging and Rate Function (PCRF):

- Interfaces with Proxy – Call session control function.
- Interfaces with PDN – GW to convey policy decisions.
- Decides how services will be treated in PDN GW according to User policy.

LTE Roaming

Home Routed

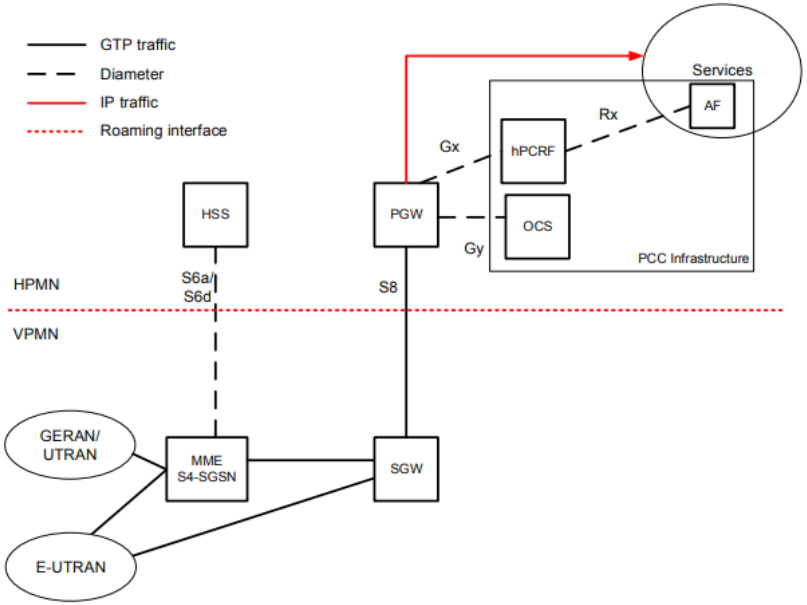


Figure 29: PCC Architecture with Home Routed architecture

LTE Roaming

Local breakout

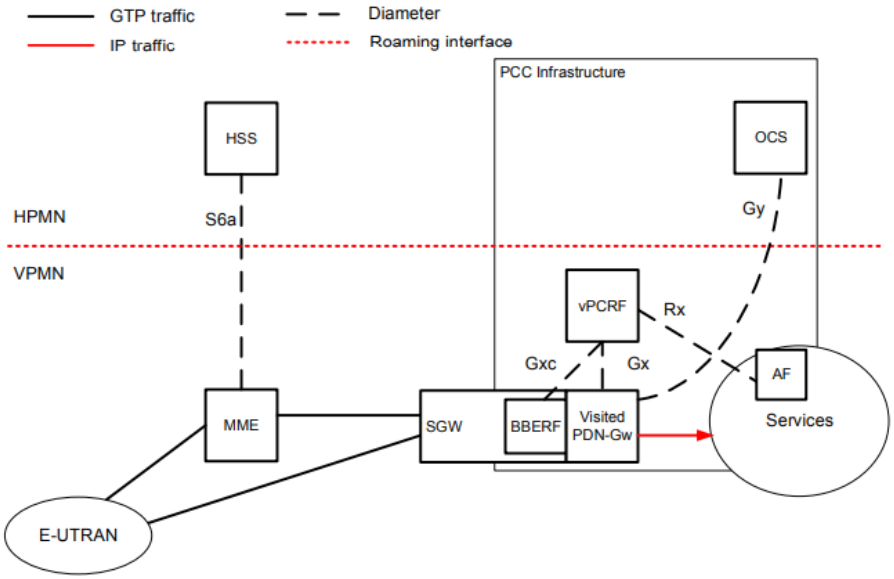
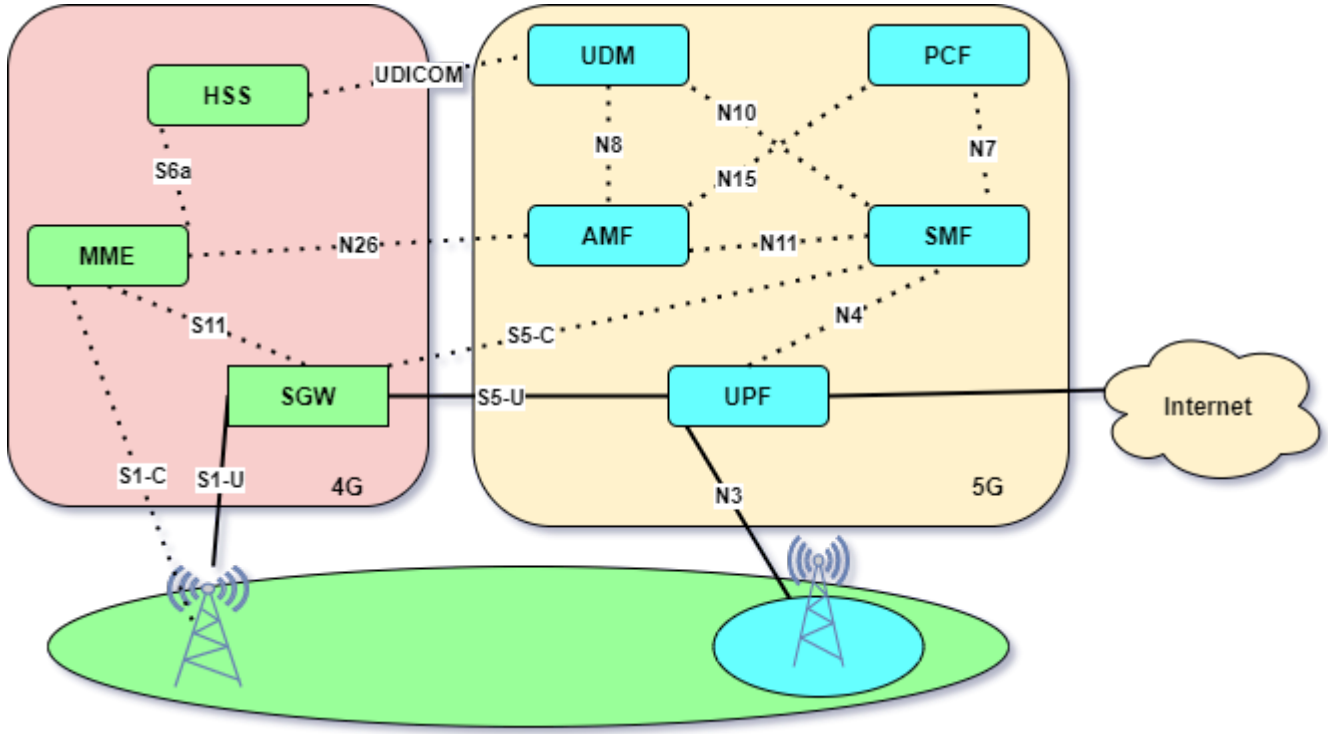


Figure 30: PCC Architecture with Local Break Out architecture

Interworking between 5G and 4G Core

4G - 5G Interworking



4G - 5G Interworking

- To ensure successful interworking with appropriate EPS functionality, only one PGW-C + SMF is allocated per APN to the UE, and this is enforced by the HSS+UDM. HSS+UDM sends the PGW-C + SMF FQDN per APN to the MME.
- As discussed before when the UE has been registered in one system and moves to the other, the UE has no native UE ID for the target system. Therefore UE maps the temp ID of the source system to the target system. 4G GUTI <-> 5G-GUTI
- When moving from 5GS -> EPS, UE includes GUMMEI in RRC as a native GUMMEI. In addition UE states that 4G -GUTI has been mapped from 5G-GUTI
- When moving from EPS -> 5G, UE includes GUAMI in RRC as a native GUAMI. Also it mentions 5G-GUTI has been mapped from 4G-GUTI.

Further Your Learning with These courses

After Completing this course if you want to further your learning of 4G you can check out the course below (referral Code Included) -

https://www.udemy.com/course/4g-lte-epc-advanced-troubleshooting-using-wireshark/?referralCode=2BA5F6FDE6C76FC74EA5

For becoming an expert on 5G I also recommend checking out this course (referral Code Included) -

https://www.udemy.com/course/5g-core-architectures-concepts-and-call-flows/?referralCode=399C46706125617AA682