System Architecture Evolution

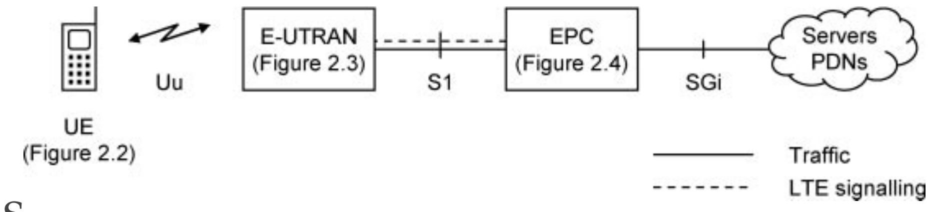
Contents

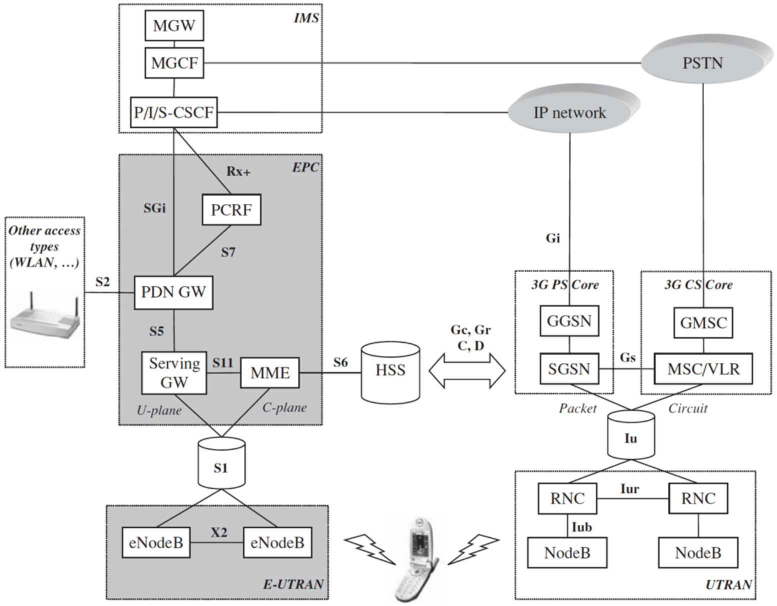
2.1 Architecture of LTE

- 2.1.1 High Level Architecture
- 2.1.2 User Equipment
- 2.1.3 Evolved UMTS Terrestrial Radio Access Network
- 2.1.4 Evolved Packet Core
- 2.1.5 Roaming Architecture
- 2.1.6 Network Areas
- 2.1.7 Numbering, Addressing and Identification

2.1.1 High Level Architecture

- Figure 2.1: the high-level architecture of Evolved Packet System (EPS) with three main components
  - ✓ User Equipment (UE)
  - ✓ Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)
  - ✓ Evolved Packet Core (EPC)
- EPC communicates with Packet Data Networks (PDN) in the outside world such as Internet, private corporate networks or IMS
- Interfaces between different parts of the system are denoted *Uu*, *S1* and *SGi*





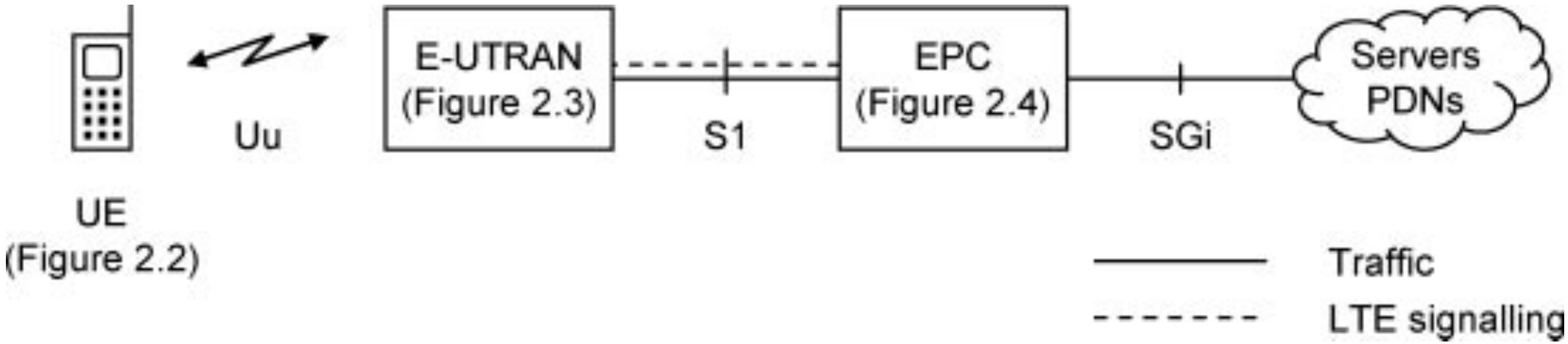


Figure 2.1 High level architecture of LTE.

2.1.2 User Equipment

- Figure 2.2
  - ✓ The internal architecture of UE
  - ✓ Identical to the one used by UMTS and GSM

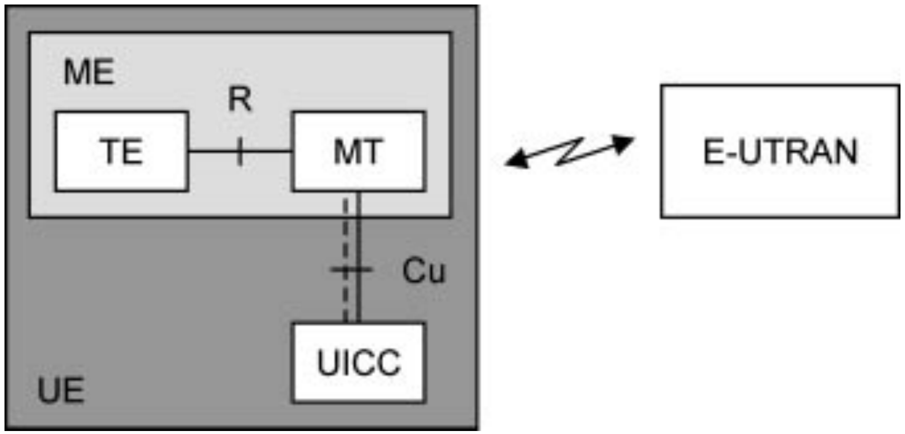
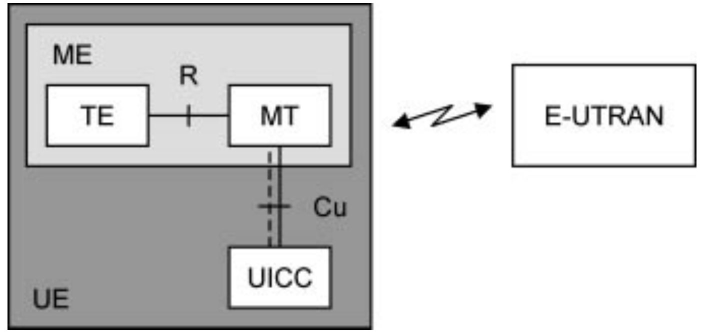


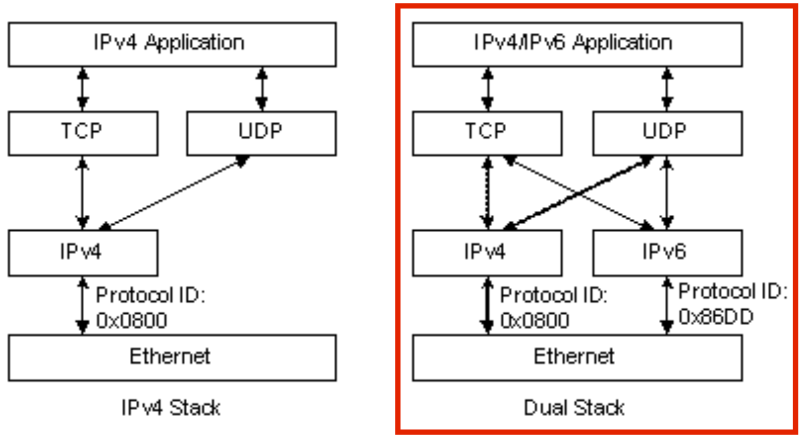
Figure 2.2 Internal architecture of the UE.

- Mobile equipment has two components
  - ✓ Mobile Termination (MT)
    - Handles all <u>communication</u> functions
  - ✓ Terminal Equipment (TE)
    - Terminates the <u>data streams</u>
  - ✓ Example
    - MT: a <u>plug-in LTE card</u> for a laptop
    - TE: the <u>laptop</u> itself



- Universal Integrated Circuit Card (UICC)
  - ✓ A smart card, known as SIM card
- Universal Subscriber Identity Module (USIM)
  - ✓ Stores user-specific data
    - User's phone number
    - Home network identity
  - ✓ Carries out various security-related calculations
    - Using the secure keys that the smart card stores
- LTE USIM
  - ✓ LTE supports USIM from Release 99 or later
  - ✓ LTE does not support the Subscriber Identity Module (SIM) used by earlier releases of GSM

- IPv4 & IPv6
  - ✓ LTE supports mobiles that are using
    - IP version 4 (IPv4)
    - IP version 6 (IPv6)
    - Dual stack IPv4/IPv6



- Dual stack IPv4/IPv6
  - ✓ The most direct approach to making IPv6 nodes compatible with IPv4 nodes by maintaining a complete IPv4 stack
  - ✓ A network node that supports both IPv4 and IPv6 is called a dual stack node
  - ✓ A dual stack node configured with an IPv4 address and an IPv6 address can have both IPv4 and IPv6 packets transmitted
- For an upper layer application supporting both IPv4 and IPv6, either TCP or UDP can be selected at the transport layer, while IPv6 stack is preferred at the network layer

- A mobile receives one IP address for every packet data network (PDN) that it is communicating with, for example
  - One for Internet
  - One for any private corporate network
- The mobile can receive an IPv4 address as well as an IPv6 address, if the mobile and network both support the two versions of the protocol

- Mobiles can have a wide variety of radio capabilities, e.g.
  - ✓ Max data rate that they can handle
  - ✓ Different types of radio access technology that they support
  - ✓ The carrier frequencies on which they can transmit and receive
- Mobiles pass these capabilities to the radio access network by means of signaling messages, so that E-UTRAN knows how to control them correctly
- Table 2.1, UE category
  - ✓ Mainly covers the max data rate with which the mobile can transmit and receive
  - ✓ Also covers some technical issues that are listed in the last three columns of the table

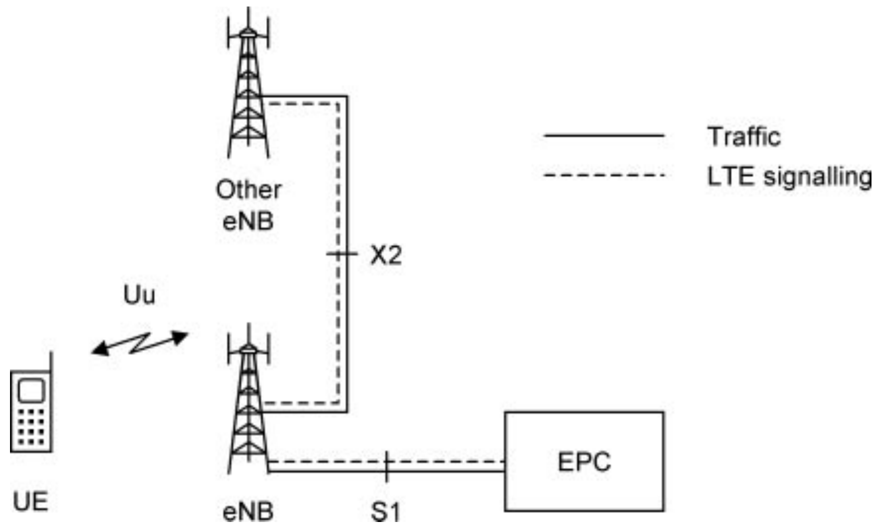
UE category	Release	Maximum # DL bits per ms	Maximum # UL bits per ms	Maximum # DL layers	Maximum # UL layers	Support of UL 64-QAM?
1	R8	10 296	5 160	1	1	No
2	R8	51 024	25 456	2	1	No
3	R8	102 048	51 024	2	1	No
4	R8	150 752	51 024	2	1	No
5	R8	299 552	75 376	4	1	Yes
6	R10	301 504	51 024	4	1	No
7	R10	301 504	102 048	4	2	No
8	R10	2 998 560	1 497 760	8	4	Yes

UE category	Release	Maximum # DL bits per ms	Maximum # UL bits per ms	Maximum # DL layers	Maximum # UL layers	Support of UL 64-QAM?
1	R8	10 296	5 160	1	1	No
2	R8	51 024	25 456	2	1	No
3	R8	102 048	51 024	2	1	No
4	R8	150 752	51 024	2	1	No
5	R8	299 552	75 376	4	1	Yes
6	R10	301 504	51 024	4	1	No
7	R10	301 504	102 048	4	2	No
8	R10	2 998 560	1 497 760	8	4	Yes

Table 2.1 UE categories.

2.1.3 Evolved UMTS Terrestrial Radio Access Network

- Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)
  - ✓ Handles the <u>radio communications</u> between mobile and EPC
  - ✓ Just has one component, evolved Node B (eNB)



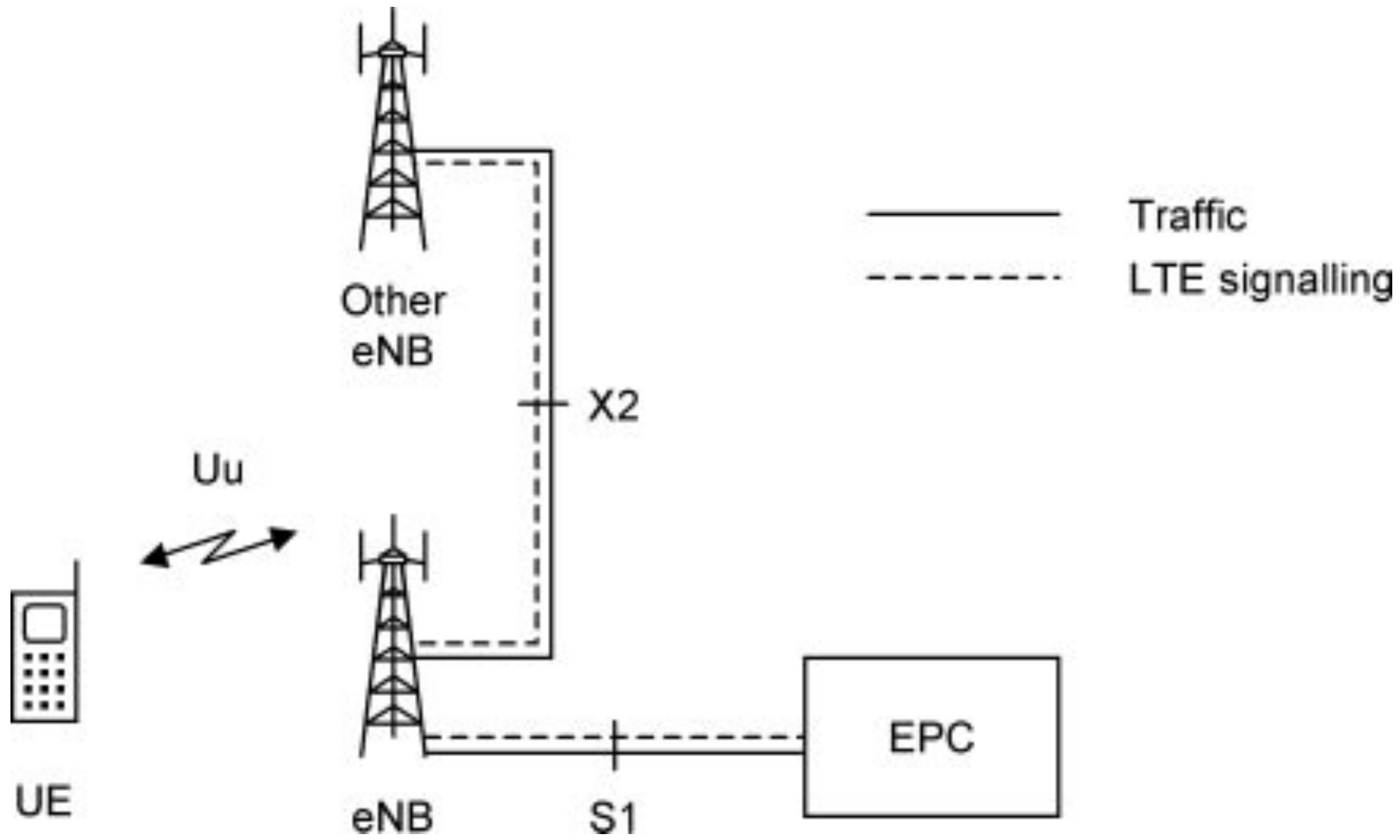
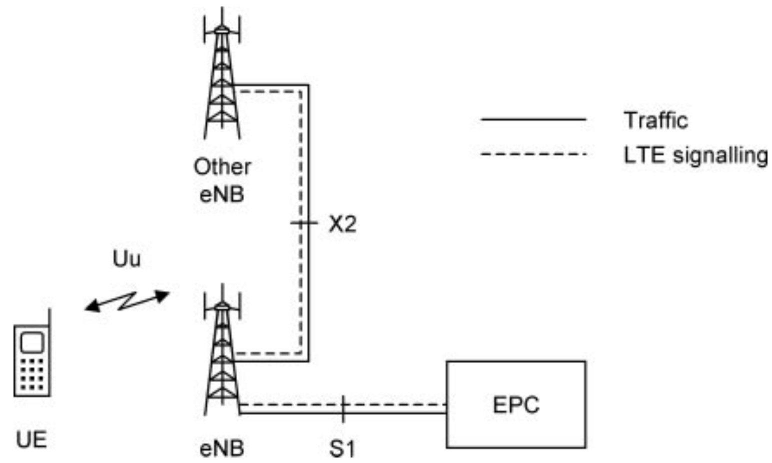


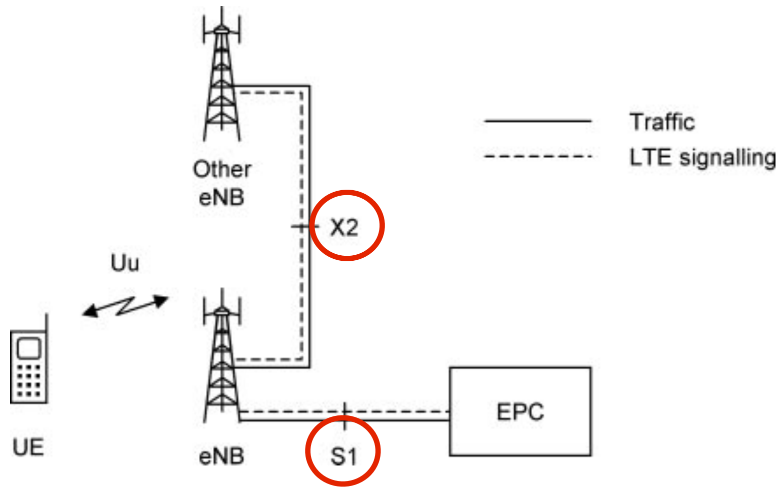
Figure 2.3 Architecture of the evolved UMTS terrestrial radio access network.

- eNB
  - ✓ A base station that controls the mobiles in one or more cells
  - ✓ A mobile communicates with just one base station and one cell at a time, so there is no equivalent of the soft handover state from UMTS
  - ✓ The base station that is communicating with a mobile is known as its serving eNB



- eNB has two main functions
  - ✓ eNB sends radio transmissions to all its mobiles on the downlink and receives transmissions from them on the uplink, using the analogue and digital signal processing functions of the LTE air interface
  - ✓ eNB controls the low-level operation of all its mobiles, by sending them signaling messages such as handover commands that relate to those radio transmissions
- eNB combines the earlier functions of Node B and Radio Network Controller (RNC), to reduce the latency that arises when the mobile exchanges information with the network

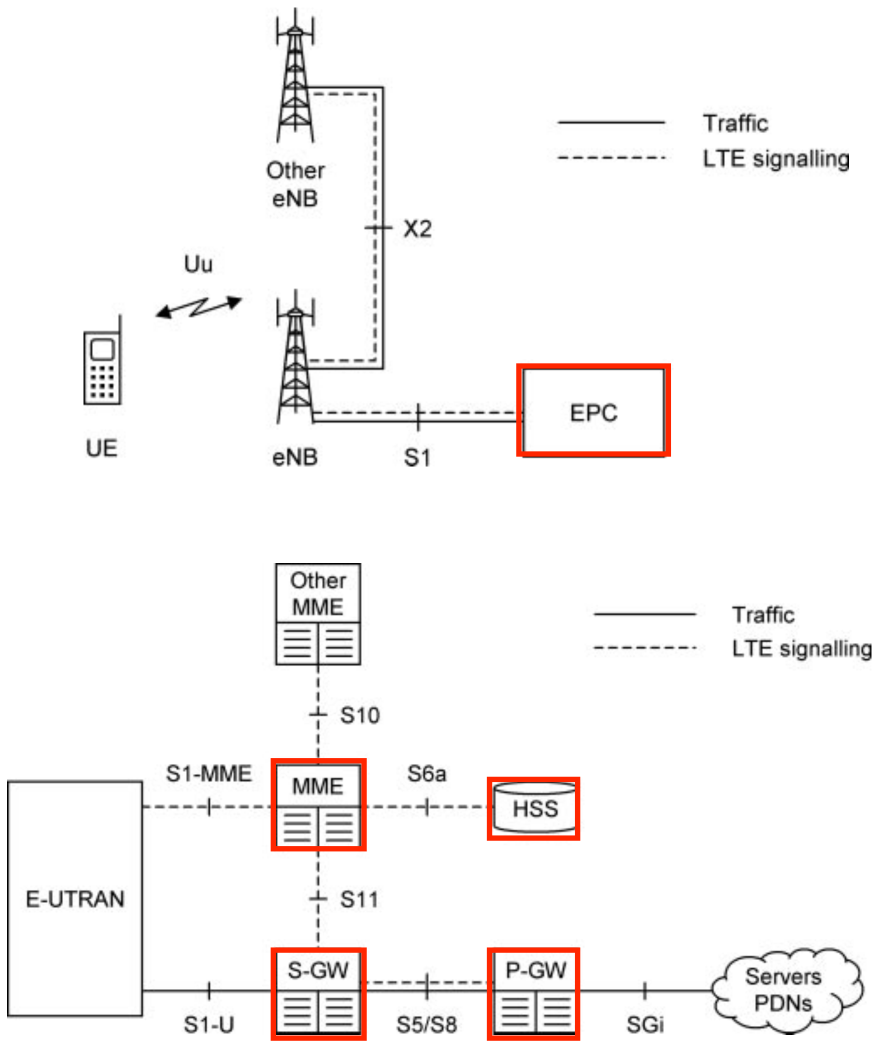
- eNB interfaces
  - ✓ eNB is connected to EPC by *S1* interface
  - ✓ eNB is connected to nearby eNB by *X2* interface
    - Mainly used for signaling and packet forwarding during handover
    - *X2* interface is optional
      - *S1* interface can also handle all the functions of *X2*, though indirectly and more slowly



- Home eNB (HeNB)
  - ✓ A base station to provide femtocell coverage within the home
  - ✓ Belongs to a Closed Subscriber Group (CSG) and can only be accessed by mobiles with a USIM that also belongs to the CSG
  - ✓ HeNB can be connected
    - Directly to the EPC in the same way as any other base station, or
    - By way of an intermediate device known as a home eNB gateway that collects the information from several HeNBs
  - ✓ Only control one cell, and do not support X2 interface until Release 10

2.1.4 Evolved Packet Core

- Main components of EPC
  - ✓ Home Subscriber Server (HSS)
  - ✓ Packet Data Network (PDN) Gateway (P-GW)
  - ✓ Serving Gateway (S-GW)
  - ✓ Mobility Management Entity (MME)
- Home Subscriber Server (HSS)
  - ✓ A central database that contains information about all the network operator's subscribers
  - ✓ The components of LTE carried forward from UMTS and GSM



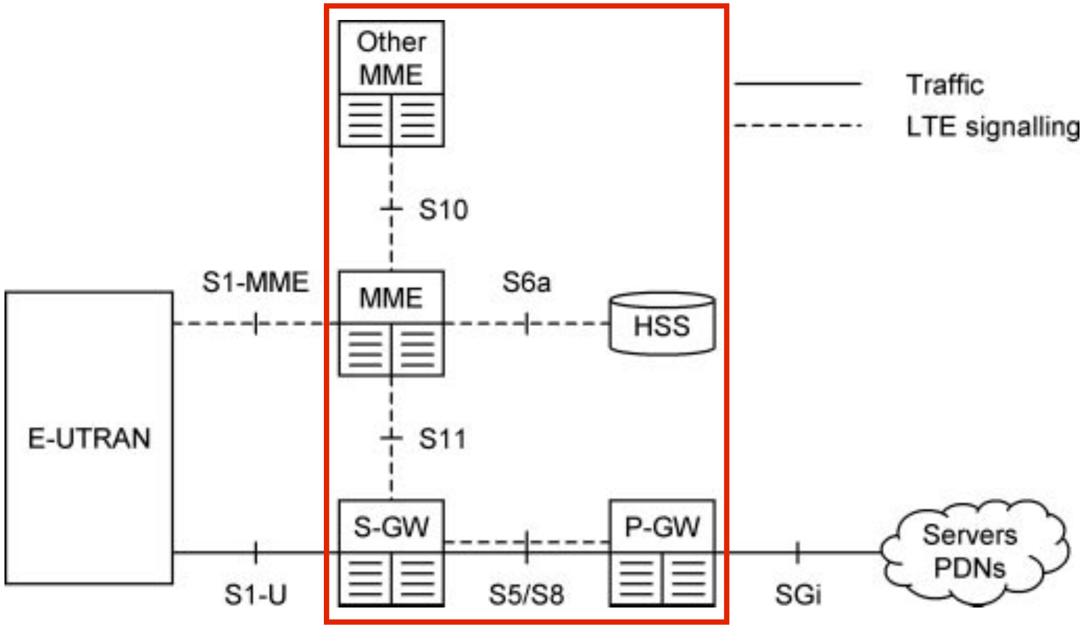
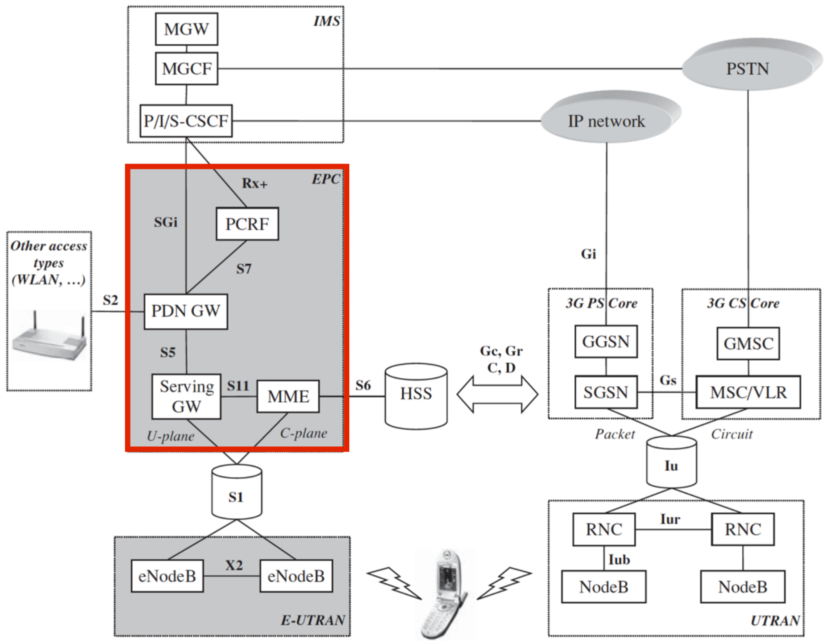
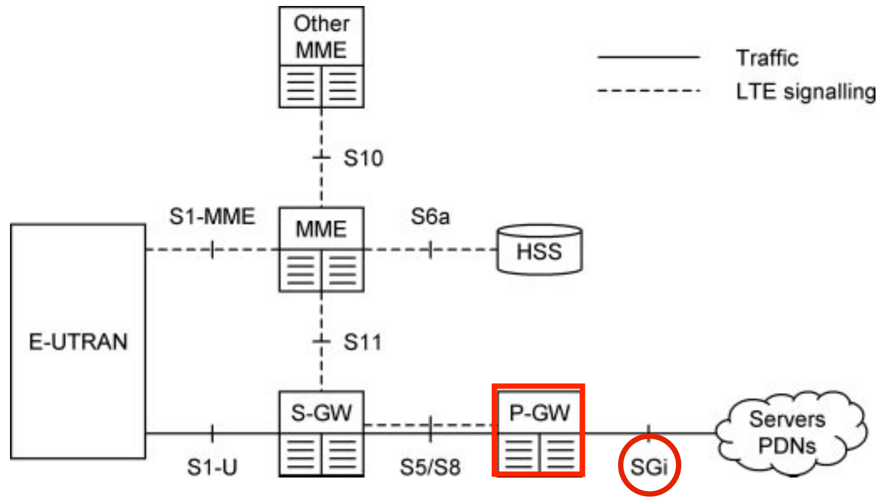
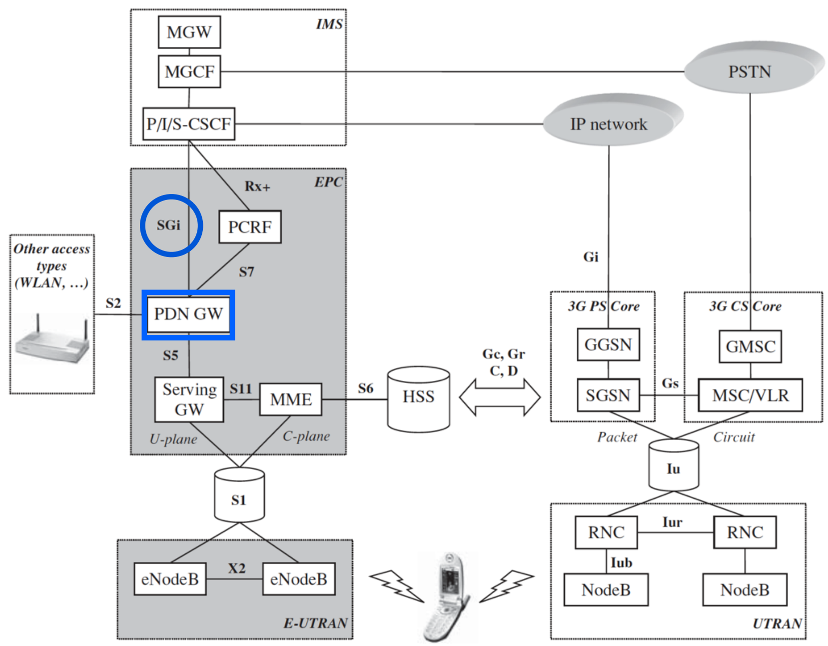


Figure 2.4 Main components of the EPC.

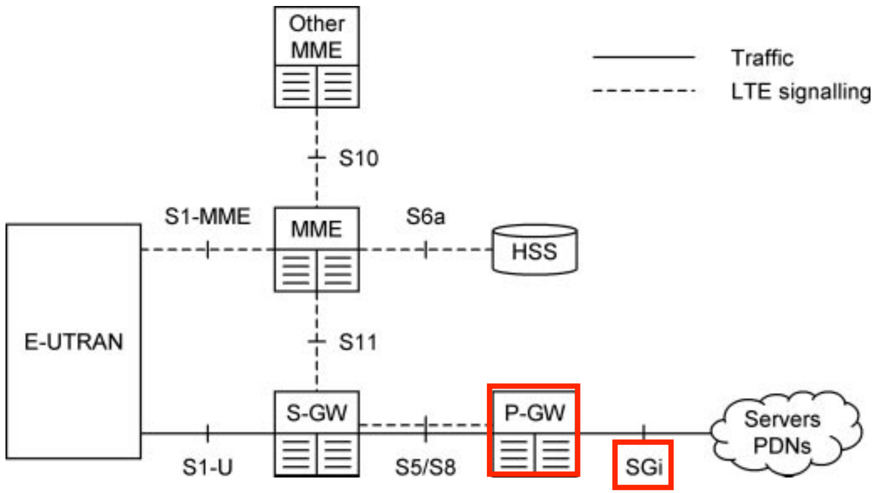


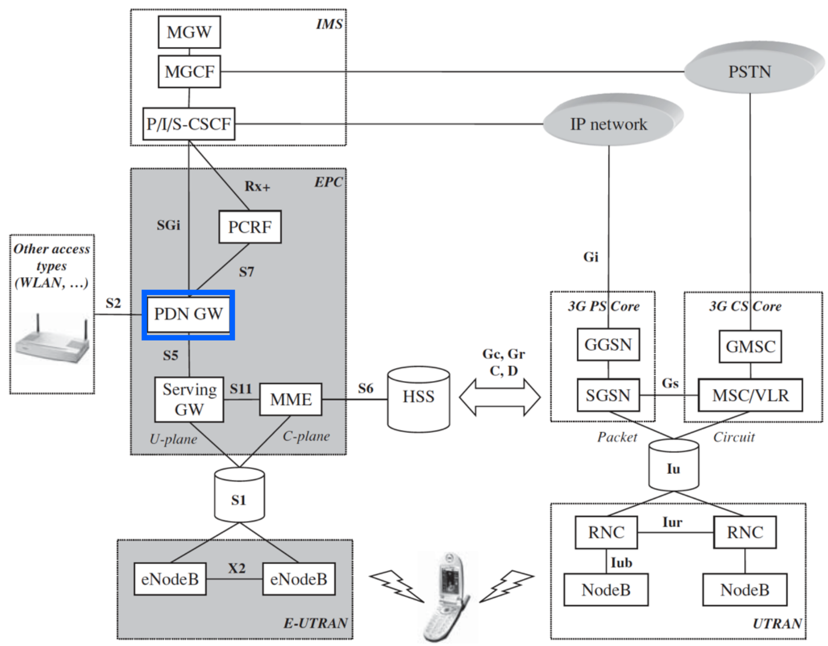
- Packet Data Network (PDN) Gateway (P-GW)
  - ✓ EPC's point of contact with outside world
  - ✓ Through the *SGi* interface, each P-GW exchanges data with one or more external devices or PDNs, such as network operator's servers, Internet or IMS
  - ✓ Each packet data network (PDN) is identified by an Access Point Name (APN)
  - ✓ A network operator typically uses a handful of different APNs, e.g., one for its own server and one for Internet



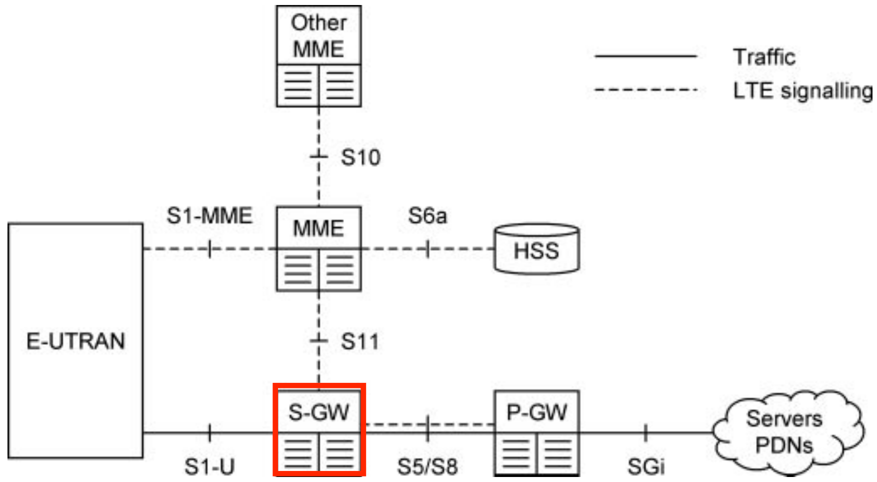


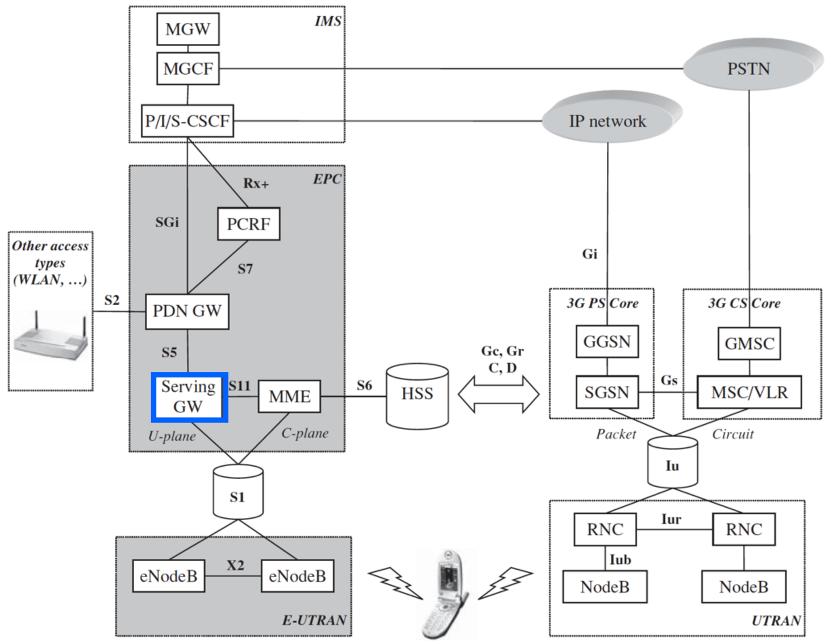
- Mobile-PGW assignment
  - ✓ Each mobile is assigned to a default P-GW when it first switches on, to give it always-on connectivity to a default PDN such as Internet
  - ✓ Later on, a mobile may be assigned to one or more additional P-GW, if it wishes to connect to additional PDNs such as private corporate networks



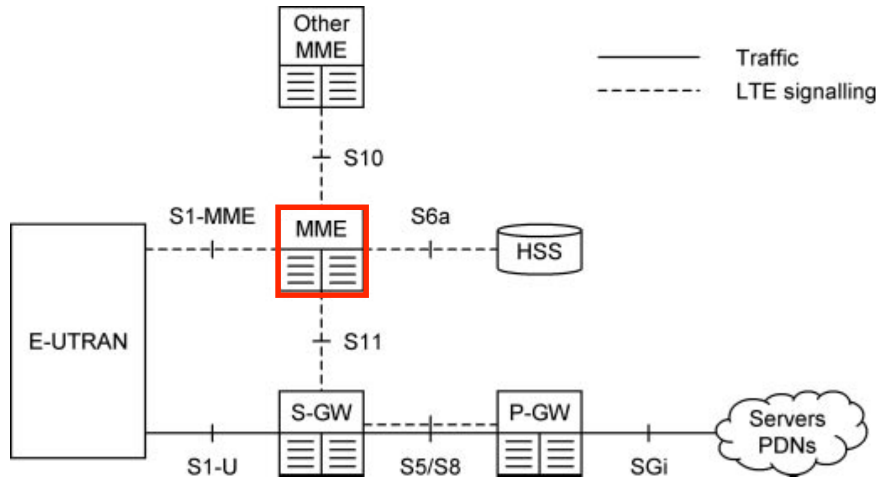


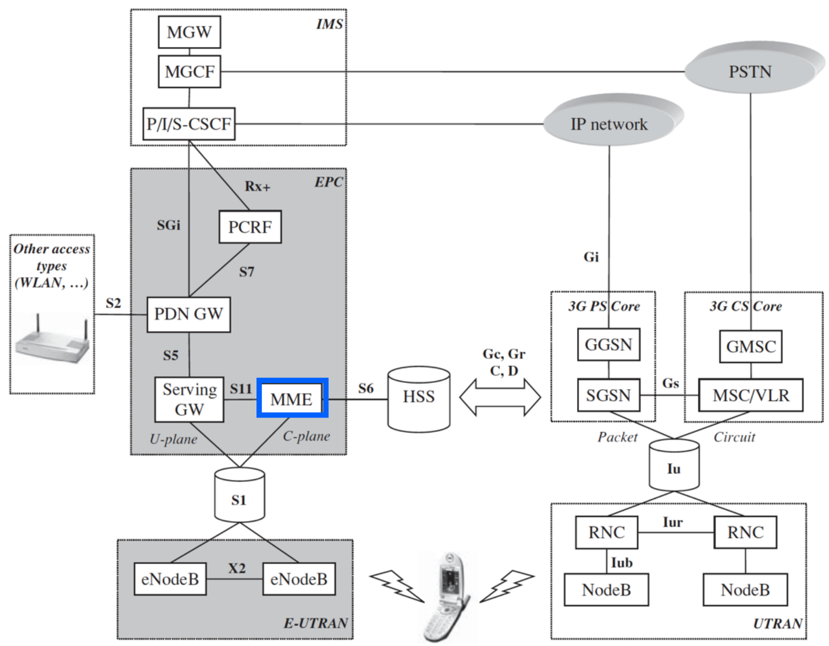
- Serving Gateway (S-GW)
  - ✓ Acts as a router, and forwards data between eNB and P-GW
  - ✓ A typical network might contain a handful of S-GW
    - Each of which looks after the mobiles in a certain geographical region
- Each mobile is assigned to a single S-GW
  - ✓ But the S-GW can be changed if the mobile moves sufficiently far



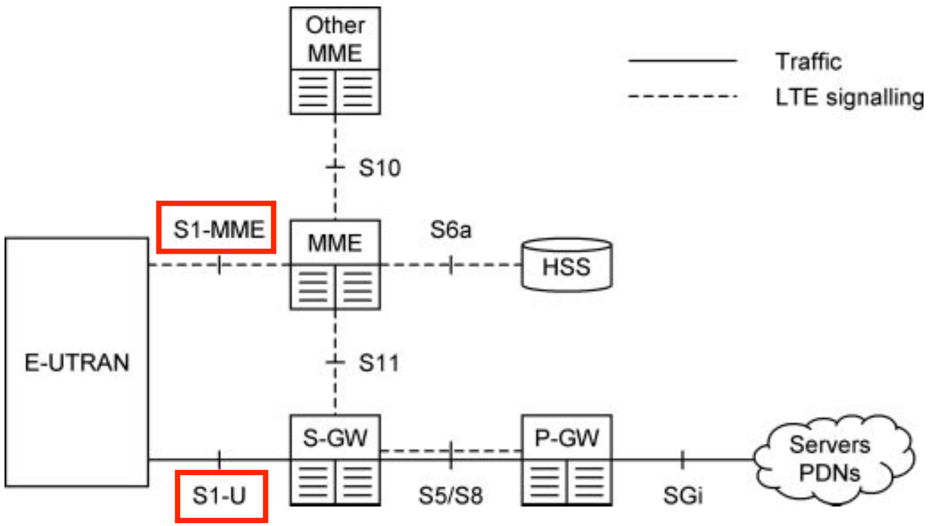


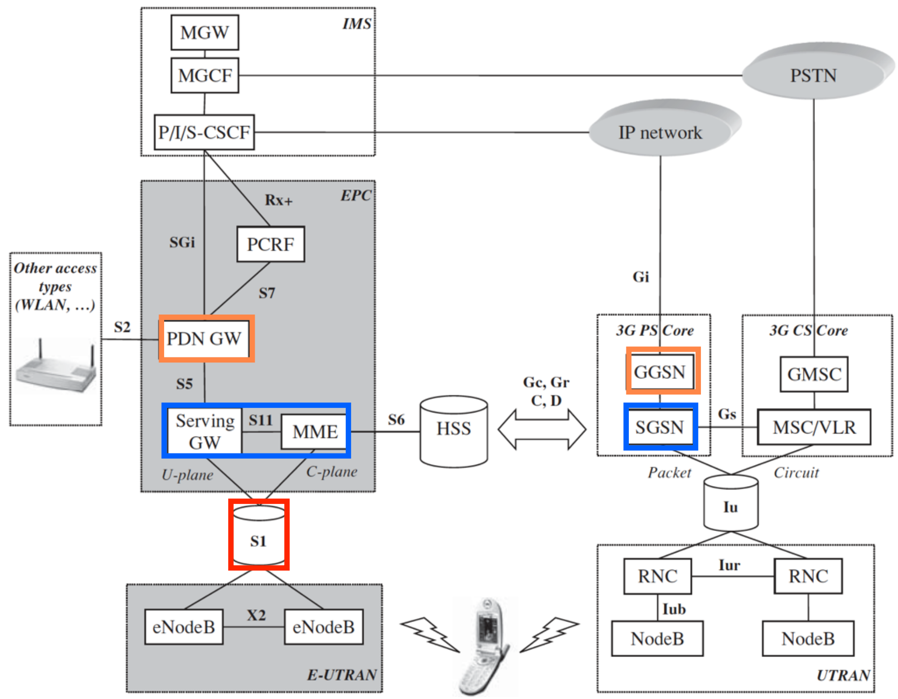
- Mobility Management Entity (MME)
  - ✓ Controls the high-level operation of the mobile, by sending it signaling messages about issues such as security and the management of data streams that are unrelated to radio communications
  - ✓ A typical network might contain a handful of MMEs
    - Each of which looks after a certain geographical region
  - ✓ Each mobile is assigned to a single MME
    - Which is known as its serving MME
    - That can be changed if the mobile moves sufficiently far





- Comparison with UMTS and GSM
  - ✓ P-GW has the same role as the gateway GPRS support node (GGSN)
  - ✓ S-GW and MME handle the data routing and signaling functions of the serving GPRS support node (SGSN)
  - ✓ Splitting SGSN in two makes it easier for an operator to scale the network in response to an increased load
    - Add more S-GWs as the traffic increases
    - Add more MMEs to handle an increase in the number of mobiles
    - S1 interface has two components
      - *S1-U* interface carries traffic for S-GW
      - *S1-MME* interface carries signaling messages for MME

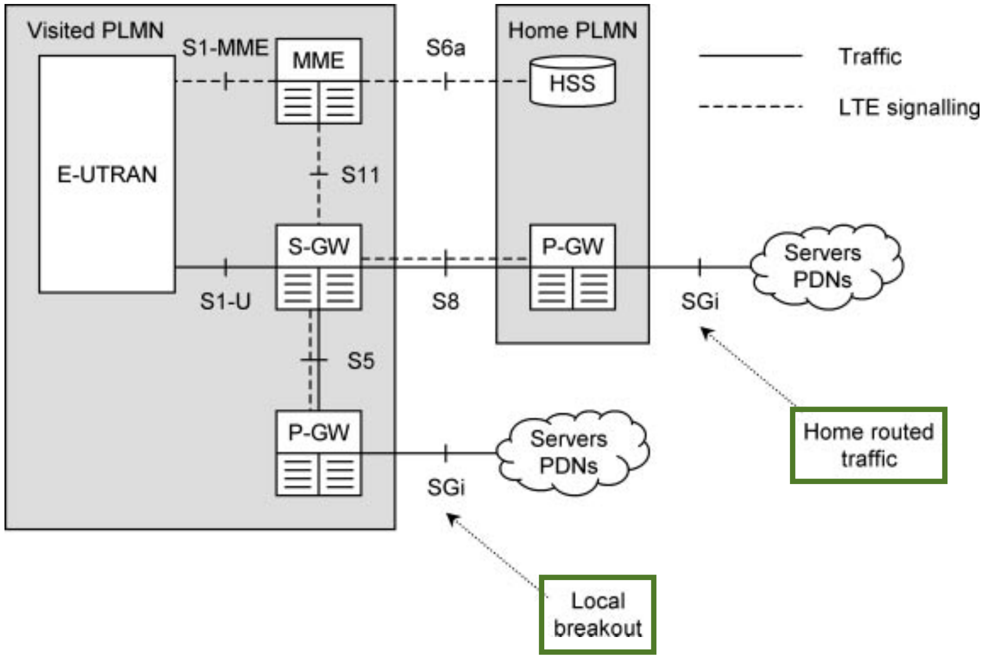




- EPC has some other components (not shown in Figure 2.4)
  - ✓ Cell Broadcast Centre (CBC)
    - Previously used by UMTS for Cell Broadcast Service (CBS)
    - In LTE, the equipment is re-used for a service known as Earthquake and Tsunami Warning System (ETWS)
  - ✓ Equipment Identity Register (EIR)
    - Also inherited from UMTS, and lists the details of lost or stolen mobiles

2.1.5 Roaming Architecture

- Roaming allows users to <u>move outside</u> their network operators' coverage area by using the resources from <u>two different networks</u>
- Relies on the existence of a <u>roaming agreement</u>, which defines how the operators will <u>share</u> the resulting <u>revenue</u>



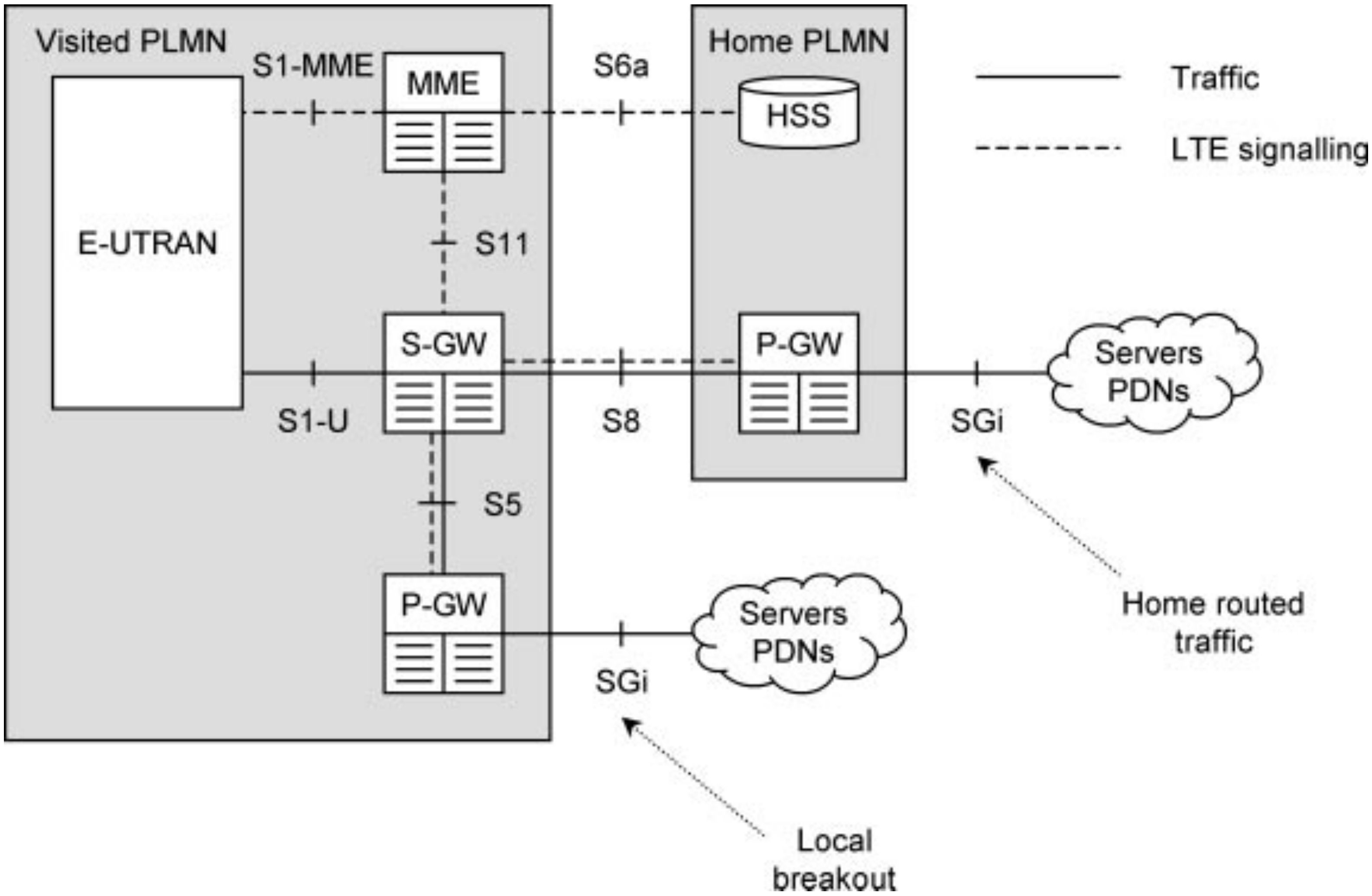
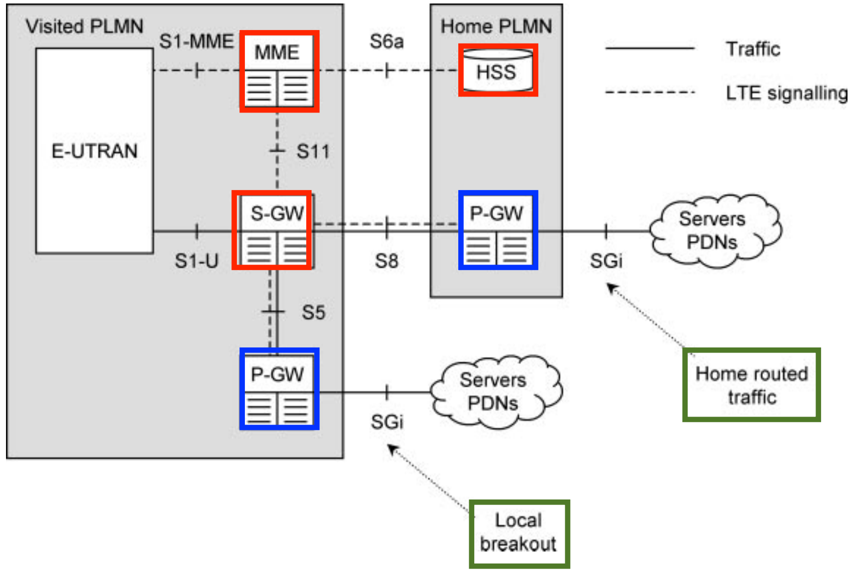
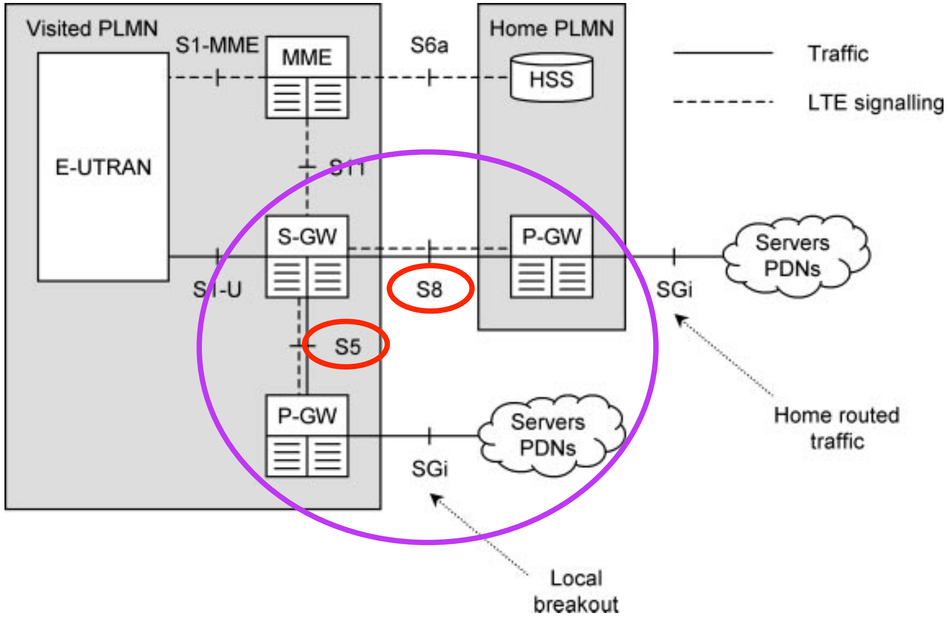


Figure 2.5 Architecture of LTE for a roaming mobile.

- If a user is roaming
  - ✓ Home Subscriber Server (HSS) is always in the home network
  - ✓ The mobile, E-UTRAN, MME and S-GW are always in the visited network
- P-GW can be in two places
  - ✓ Home routed traffic
    - P-GW lies in the home network, through which all the user's traffic is all routed
    - Allows the home network operator to
      - See all the traffic
      - Charge the user for it directly
    - Can be inefficient if the user is traveling overseas, particularly during a voice call with another user nearby
  - ✓ Local breakout
    - P-GW is located in the visited network



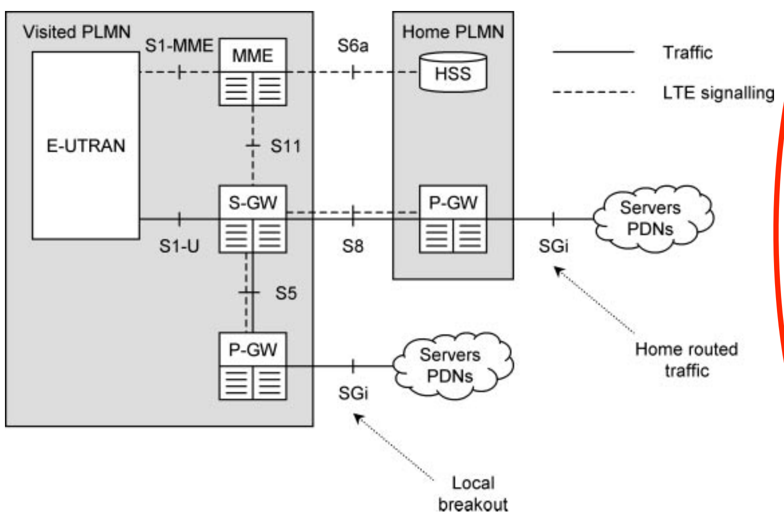
- The interface between S-GW and P-GWs is <u>*S5/S8*</u>
  - ✓ *S5*: if two devices are in the <u>same network</u>
  - ✓ *S8*: if two devices are in <u>different networks</u>

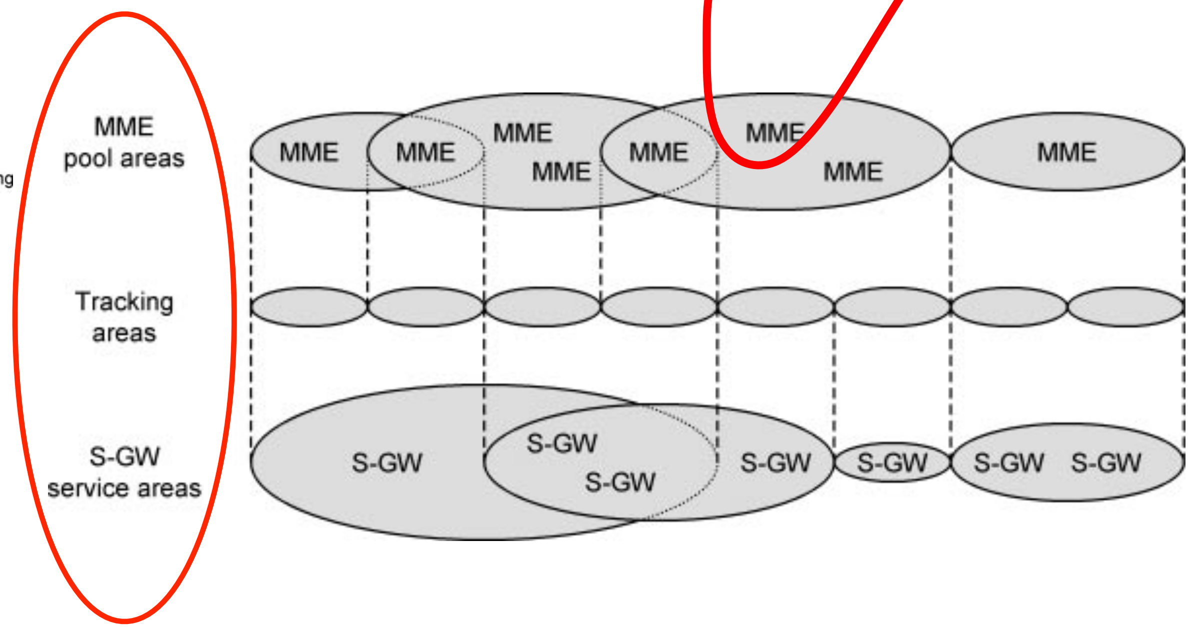


- For mobiles that are <u>not roaming</u>
  - ✓ S-GW and P-GWs can be integrated into a <u>single device</u>, so that the S5/S8 interface vanishes altogether

2.1.6 Network Areas

- EPC is divided into three different types of geographical area
  - ✓ MME pool area
  - ✓ S-GW service area
  - ✓ Tracking area





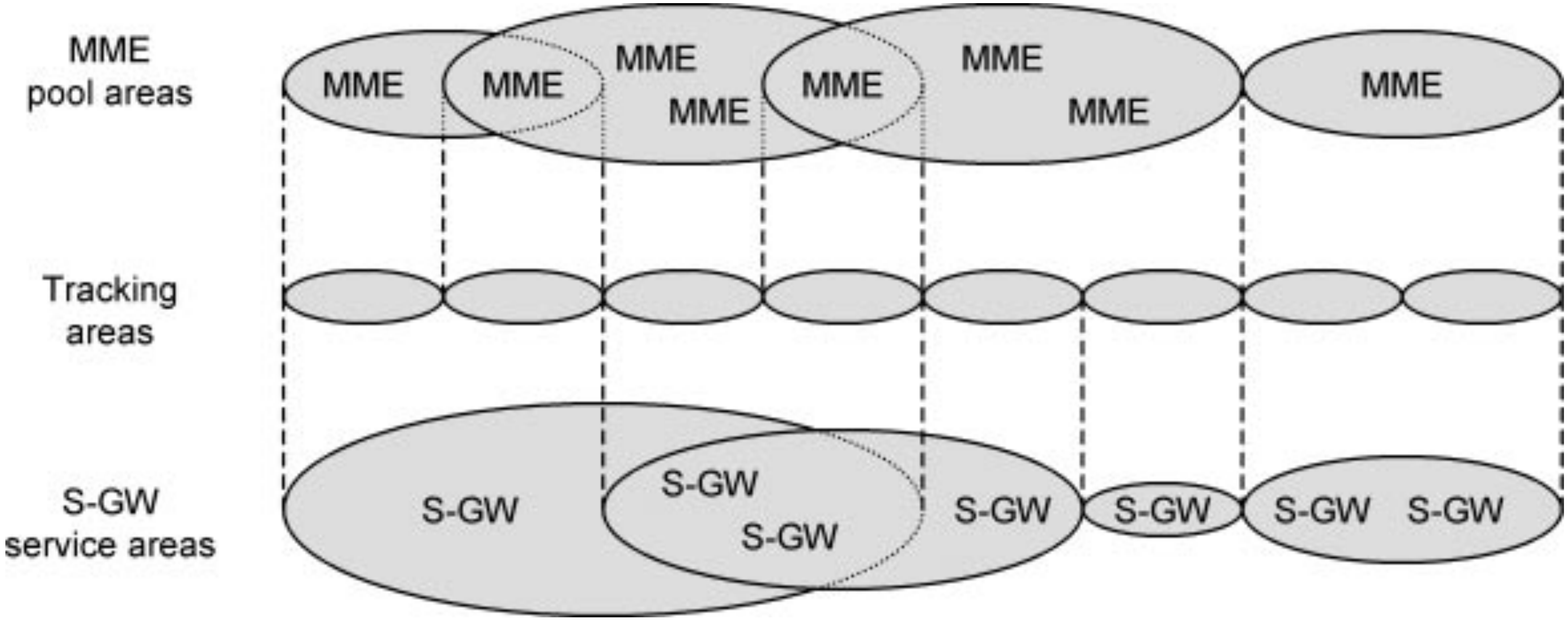
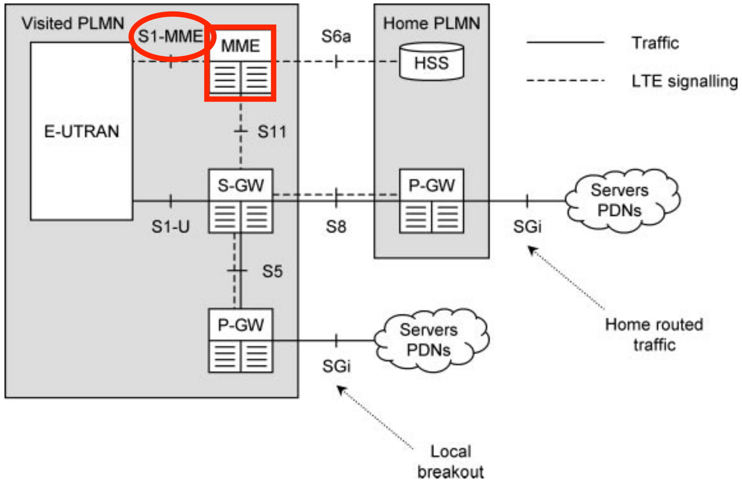
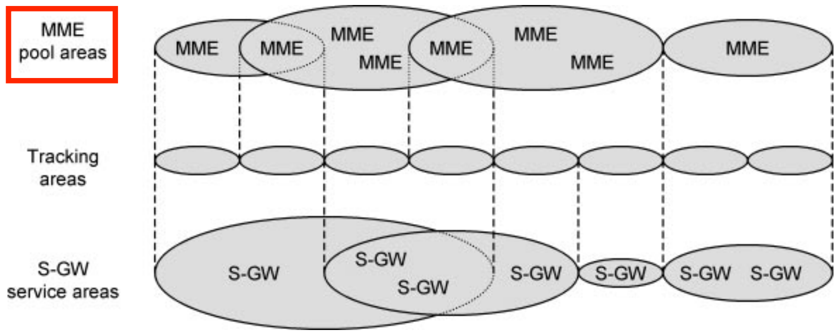


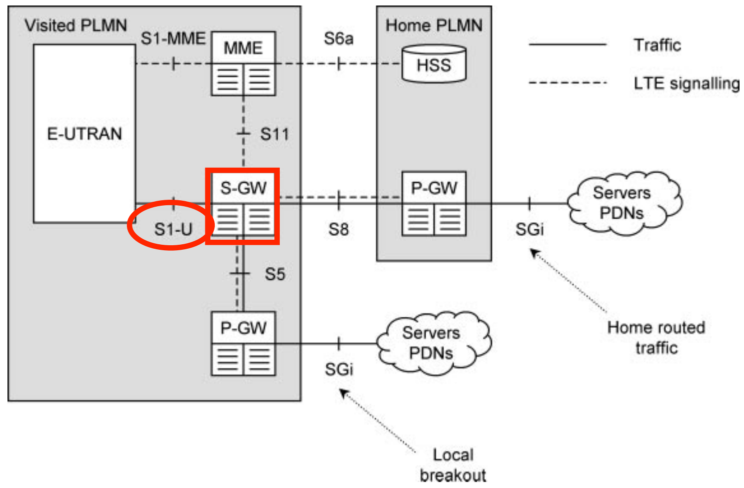
Figure 2.6 Relationship between tracking areas, MME pool areas and S-GW service areas.

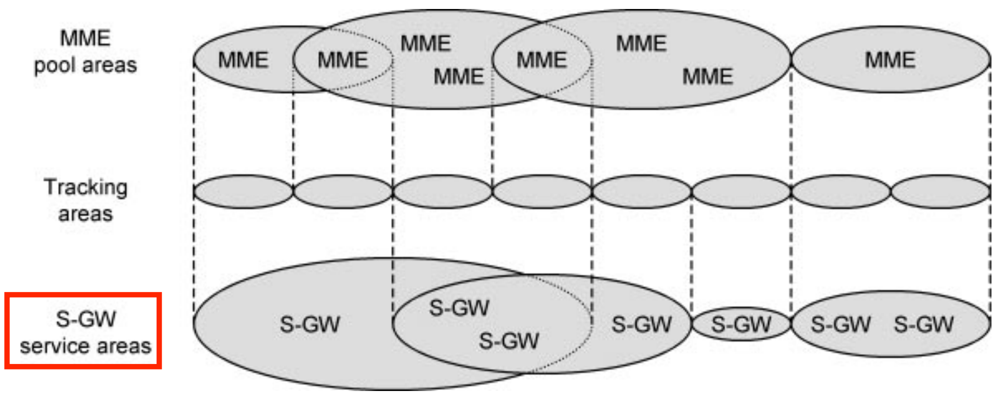
- MME pool area
  - An area through which the mobile can move without a change of serving MME
  - Every pool area is controlled by one or more MMEs
    - Every BS is connected to all the MMEs in a pool area by means of *S1-MME* interface
  - Pool areas can also overlap
  - A network operator might configure a pool area to cover a large region of the network such as a major city and might add MMEs to the pool as the signaling load in that city increases



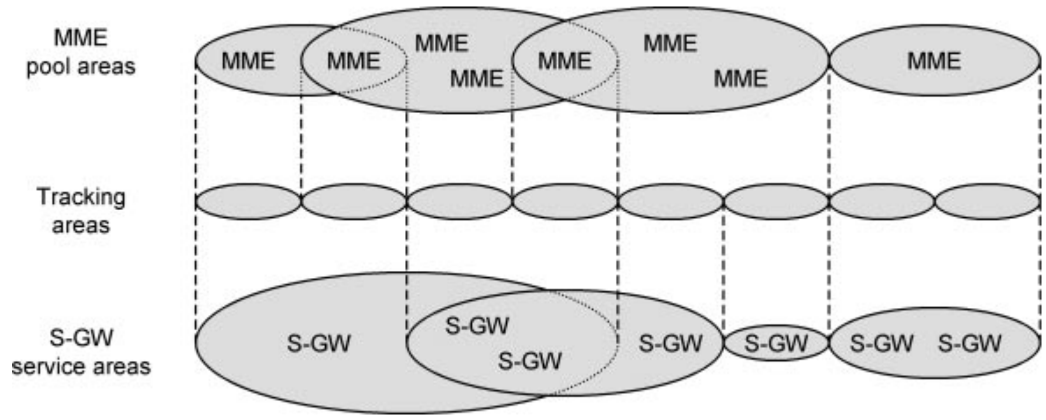


- S-GW service area
  - ✓ An area served by one or more S-GWs, through which the mobile can move without a change of S-GW
  - ✓ Every BS is connected to all the S-GWs in a service area by means of *S1-U* interface





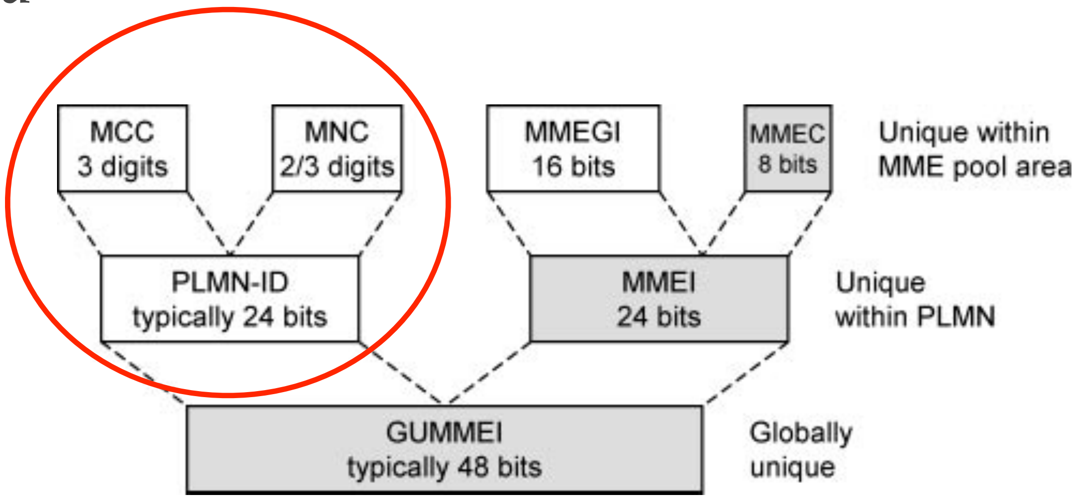
- Tracking areas
  - ✓ MME pool areas and S-GW service areas are both made from smaller, non-overlapping units known as tracking areas (TAs)



  - ✓ TAs
    - Used to track the locations of mobiles that are on standby
    - Similar to the location areas (LA) and routing areas (RA) from UMTS and GSM

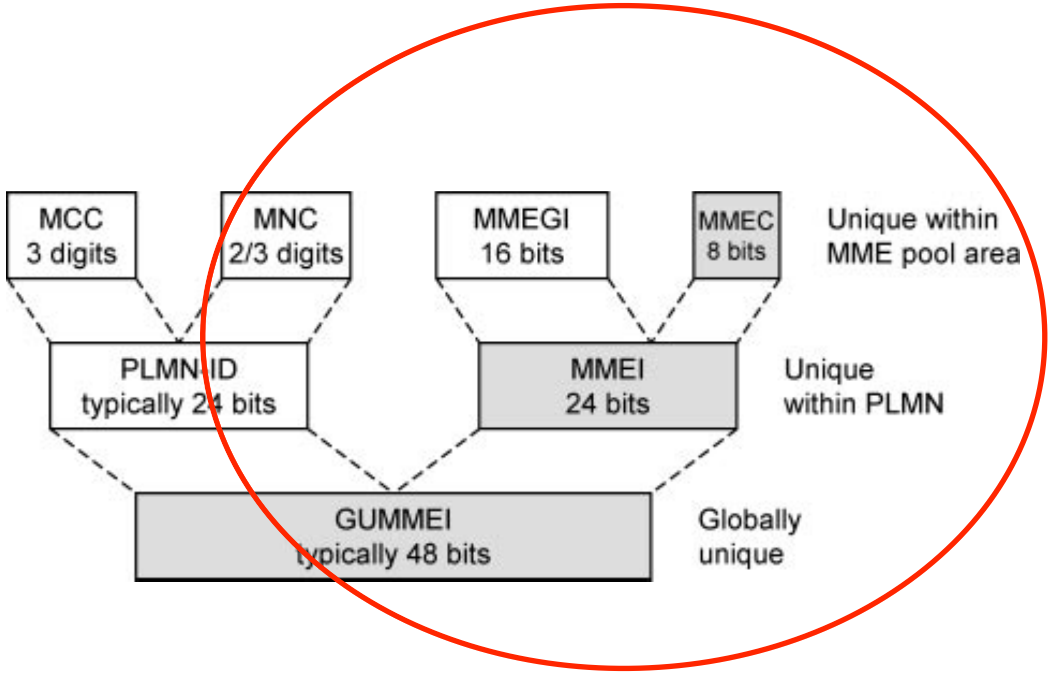
2.1.7 Numbering, Addressing and Identification

- Each <u>network</u> is associated with a Public Land Mobile Network IDentity (PLMN-ID)
  - ✓ A three digit <u>Mobile Country Code</u> (MCC)
  - ✓ A two or three digit <u>Mobile Network Code</u> (MNC)
  - ✓ Example
    - UK MCC is 234
    - Vodafone's UK network uses a MNC of 15



Identities used by MME

- MME has three main identities
  - ✓ 8 bit MME Code (MMEC) uniquely identifies the MME within all the pool areas that it belongs to
  - ✓ By combining this with a 16 bit MME Group Identity (MMEGI), we arrive at a 24 bit MME Identifier (MMEI), which uniquely identifies the MME within a particular network
  - ✓ By bringing in the network identity, we arrive at the Globally Unique MME Identifier (GUMMEI), which identifies an MME anywhere in the world



Identities used by MME

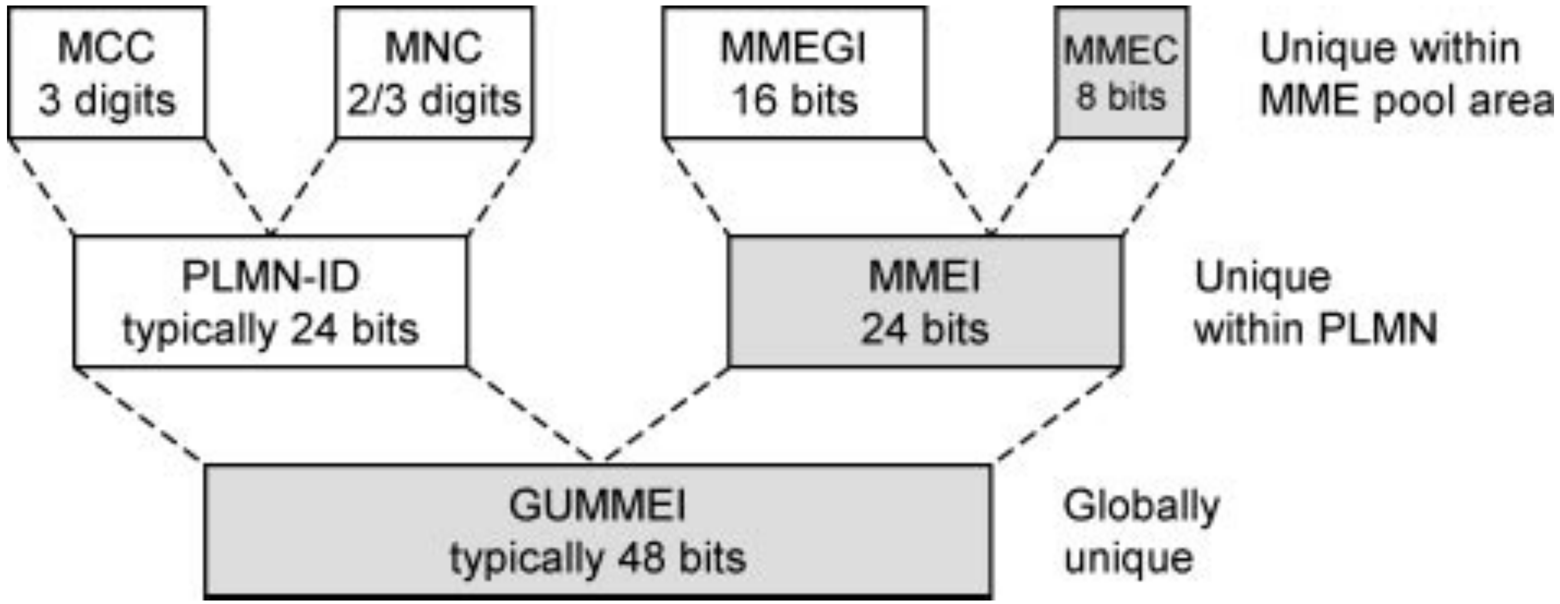
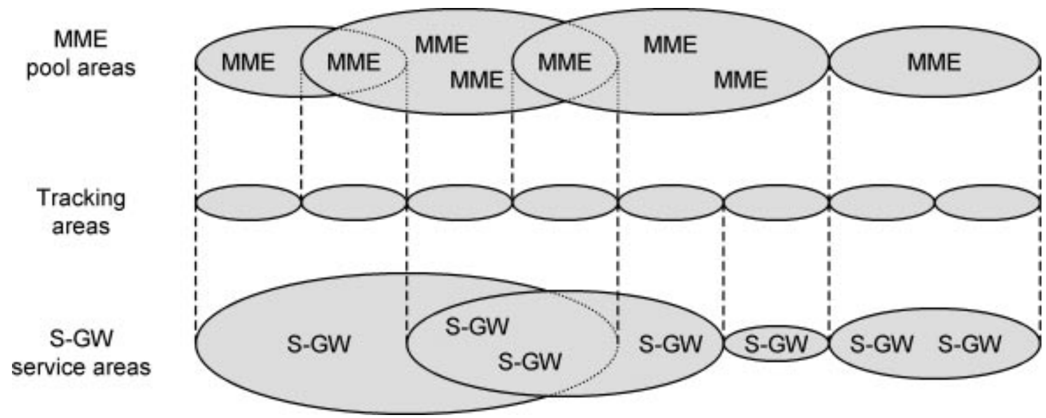


Figure 2.7 Identities used by MME.

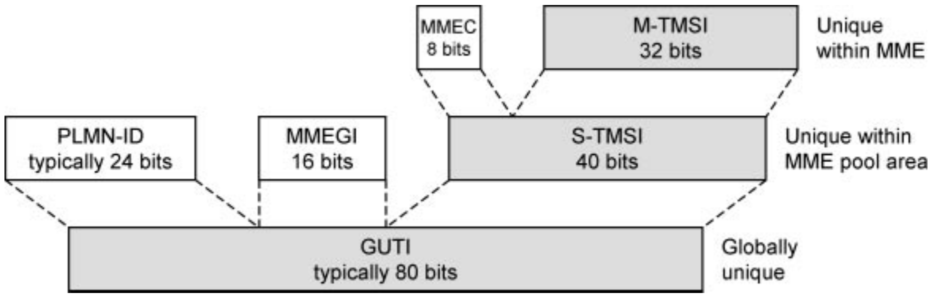
- Each tracking area has two main identities
  - ✓ 16 bit Tracking Area Code (TAC) identifies a tracking area within a particular network
  - ✓ Combining this with the network identity gives the globally unique Tracking Area Identity (TAI)



- Cells have three types of identity
  - ✓ 28 bit E-UTRAN Cell Identity (ECI) identifies a cell within a particular network
  - ✓ E-UTRAN Cell Global Identifier (ECGI) identifies a cell anywhere in the world
  - ✓ Physical cell identity
    - A number from 0 to 503 that distinguishes a cell from its immediate neighbors

- A mobile is also associated with several different identities
  - ✓ International Mobile Equipment Identity (IMEI)
    - A unique identity for the mobile equipment
  - ✓ International Mobile Subscriber Identity (IMSI)
    - A unique identity for the UICC and the USIM

- IMSI
  - ✓ One of the quantities that an intruder needs to clone a mobile
  - ✓ We avoid transmitting it across the air interface wherever possible
- Serving MME
  - ✓ Identifies each mobile using temporary identities, which it updates at regular intervals
- Three types of temporary identity
  - ✓ 32 bit M Temporary Mobile Subscriber Identity (M-TMSI) identifies a mobile to its serving MME
  - ✓ Add the 8 bit MME code results in the 40 bit S Temporary Mobile Subscriber Identity (S-TMSI), which identifies the mobile within an MME pool area
  - ✓ Add the MME group identity and the PLMN identity results in Globally Unique Temporary Identity (GUTI)



Temporary identities used by the mobile

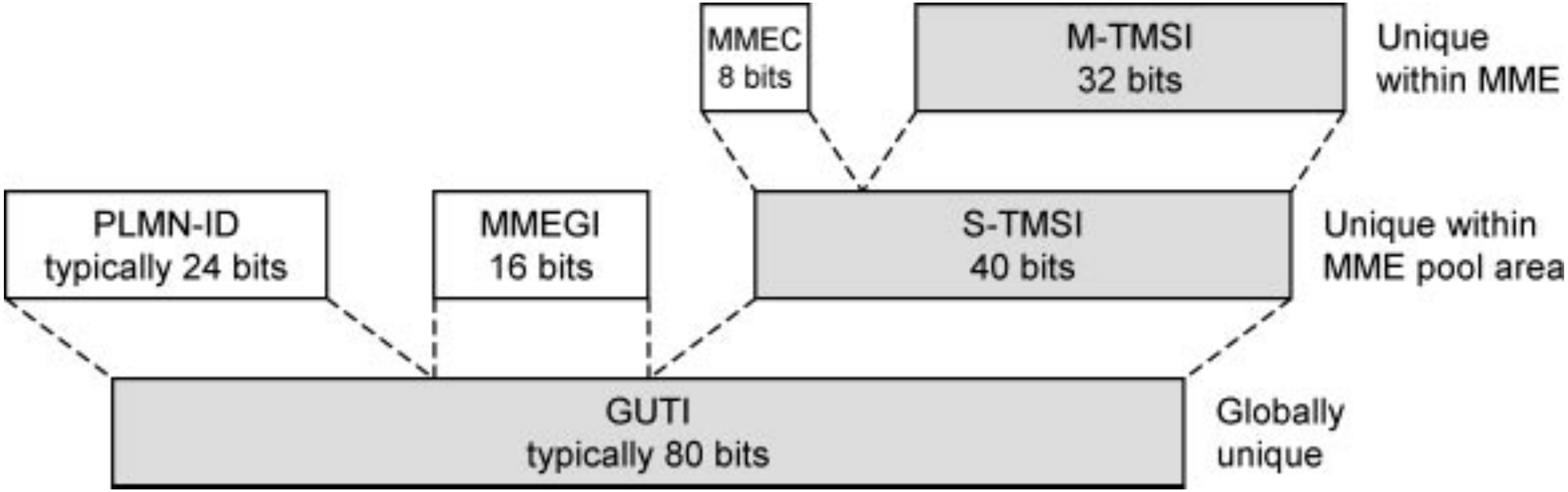


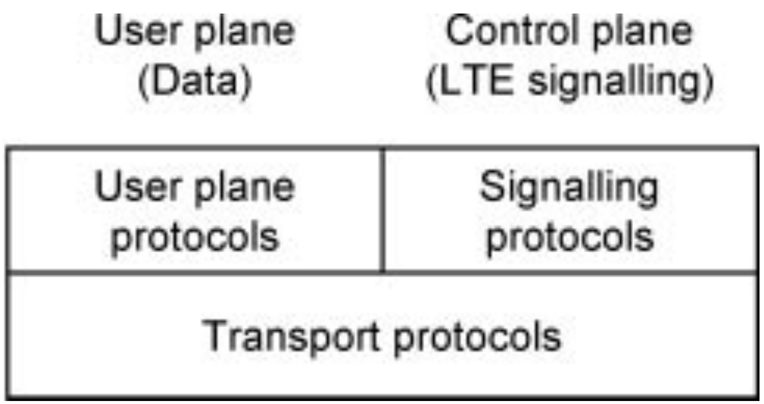
Figure 2.8 Temporary identities used by the mobile.

2.2 Communication Protocols

- 2.2.1 Protocol Model
- 2.2.2 Air Interface Transport Protocols
- 2.2.3 Fixed Network Transport Protocols
- 2.2.4 User Plane Protocols
- 2.2.5 Signaling Protocols

2.2.1 Protocol Model

- The high-level structure of protocol stacks
- The protocol stack has two planes
  - ✓ Protocols in the user plane handle data that are of interest to the users
  - ✓ Protocols in the control plane handle signaling messages that are only of interest to the network elements themselves



High level protocol architecture of LTE

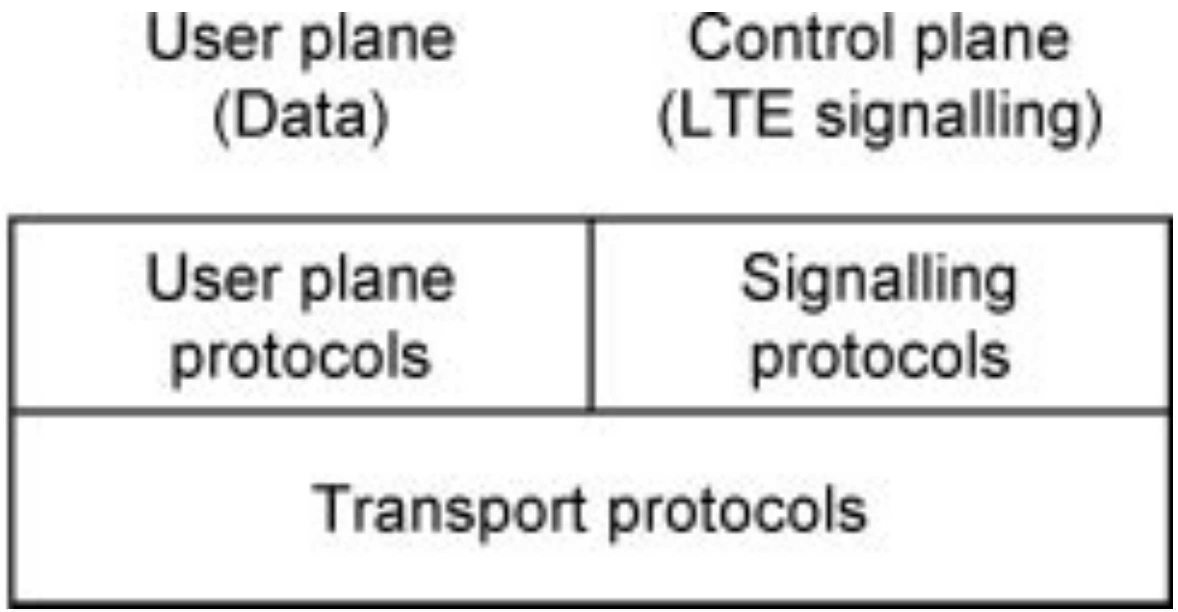
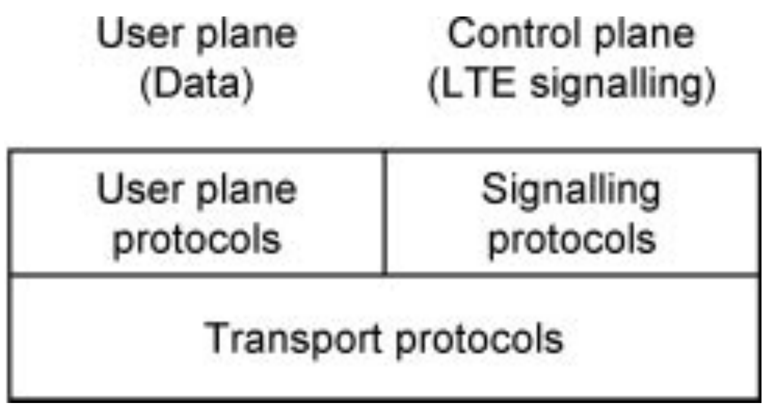


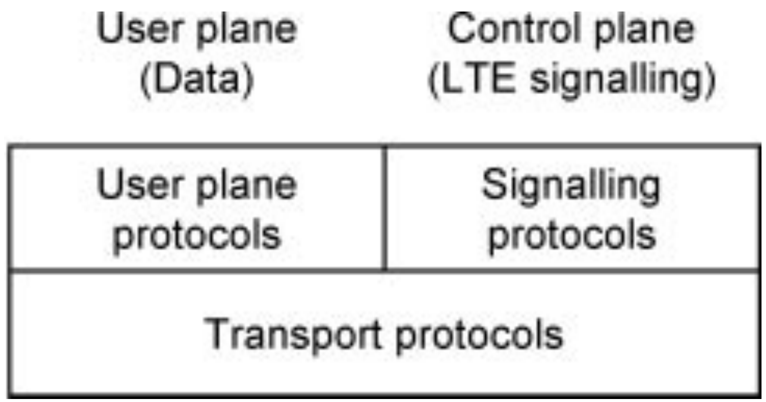
Figure 2.9 High level protocol architecture of LTE.

- The protocol stack also has two main layers
  - ✓ Upper layer
    - Manipulates information in a way that is specific to LTE
    - In the E-UTRAN, known as radio network layer
  - ✓ Lower layer
    - Transports information from one point to another
    - In the E-UTRAN, known as transport network layer



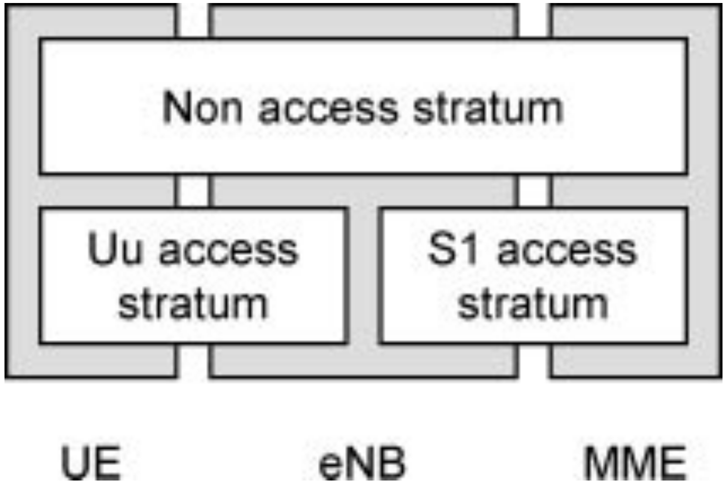
High level protocol architecture of LTE

- There are then three types of protocol
  - ✓ Signaling protocols
    - Define a language by which two devices can exchange signaling messages with each other
  - ✓ User plane protocols
    - Manipulate the data in the user plane, most often to help route the data within the network
  - ✓ Underlying transport protocols
    - Transfer data and signaling messages from one point to another

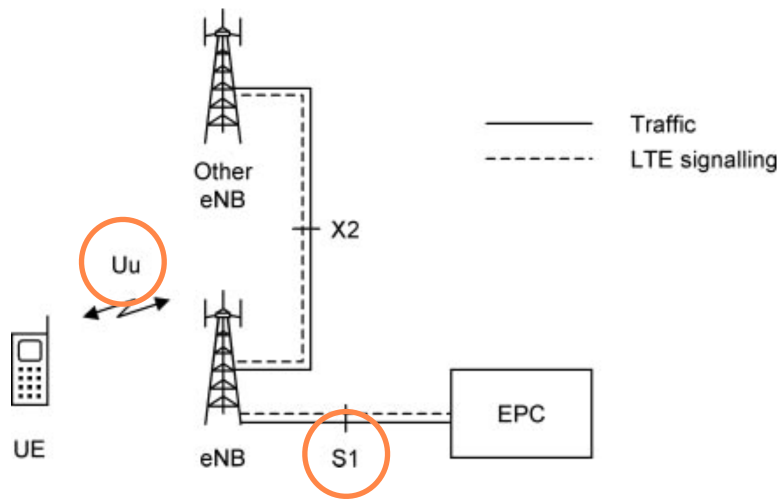


High level protocol architecture of LTE

- On the air interface, there is an extra level of complexity as shown in Figure 2.10
- MME controls the high-level behavior of mobile by sending it signaling messages
  - ✓ However, no direct path between MME and mobile
  - ✓ The air interface is divided into
    - Access Stratum (AS)
    - Non Access Stratum (NAS)
- High-level signaling messages lie in NAS and are transported using AS protocols of *S1* and *Uu* interfaces



The access stratum and non access stratum on the air interface



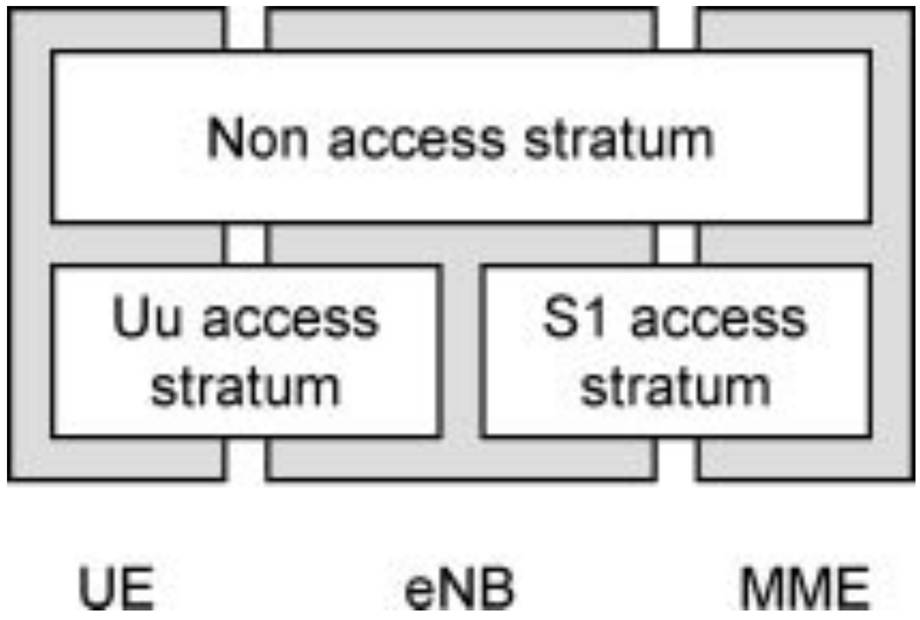
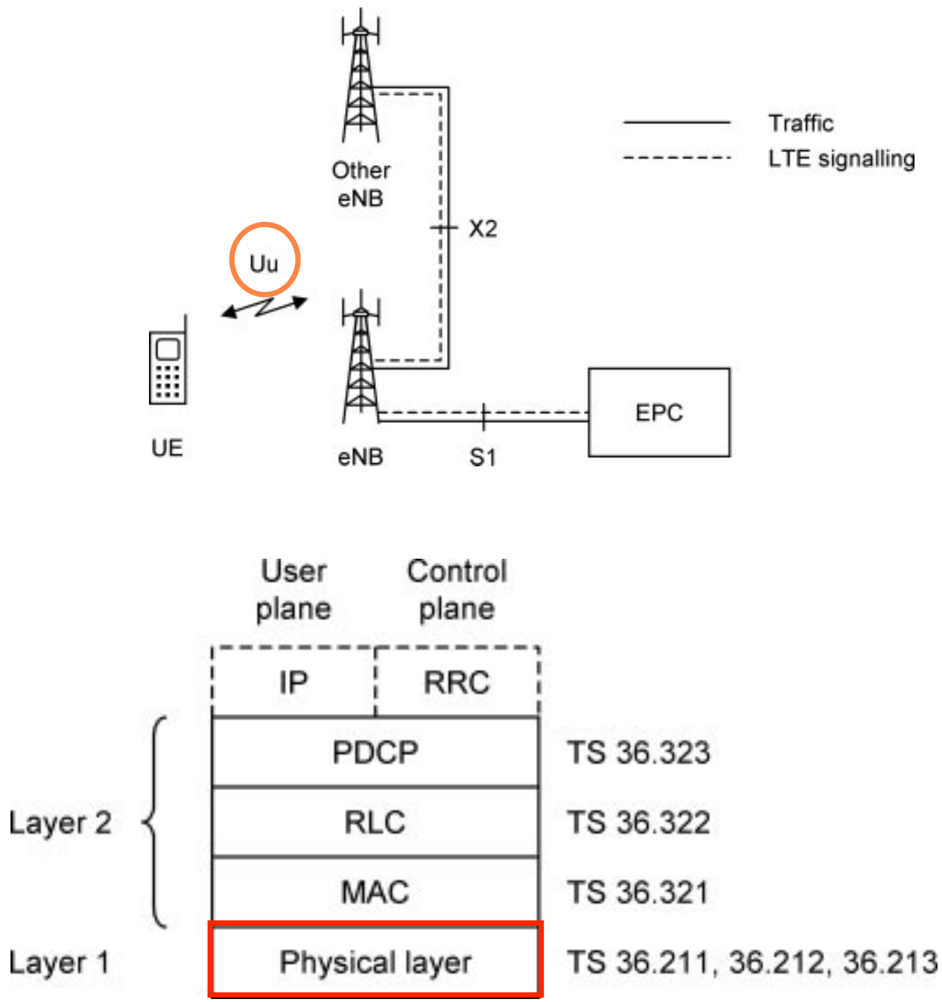


Figure 2.10 Relationship between the access stratum and non access stratum on the air interface.

2.2.2 Air Interface Transport Protocols

- The air interface, *Uu*, lies between mobile and BS
- Figure 2.11 shows the air interface's transport protocols
- Starting at the bottom, the air interface physical layer contains the digital and analogue signal processing functions that the mobile and BS use to send and receive information



Transport protocols used on the air interface

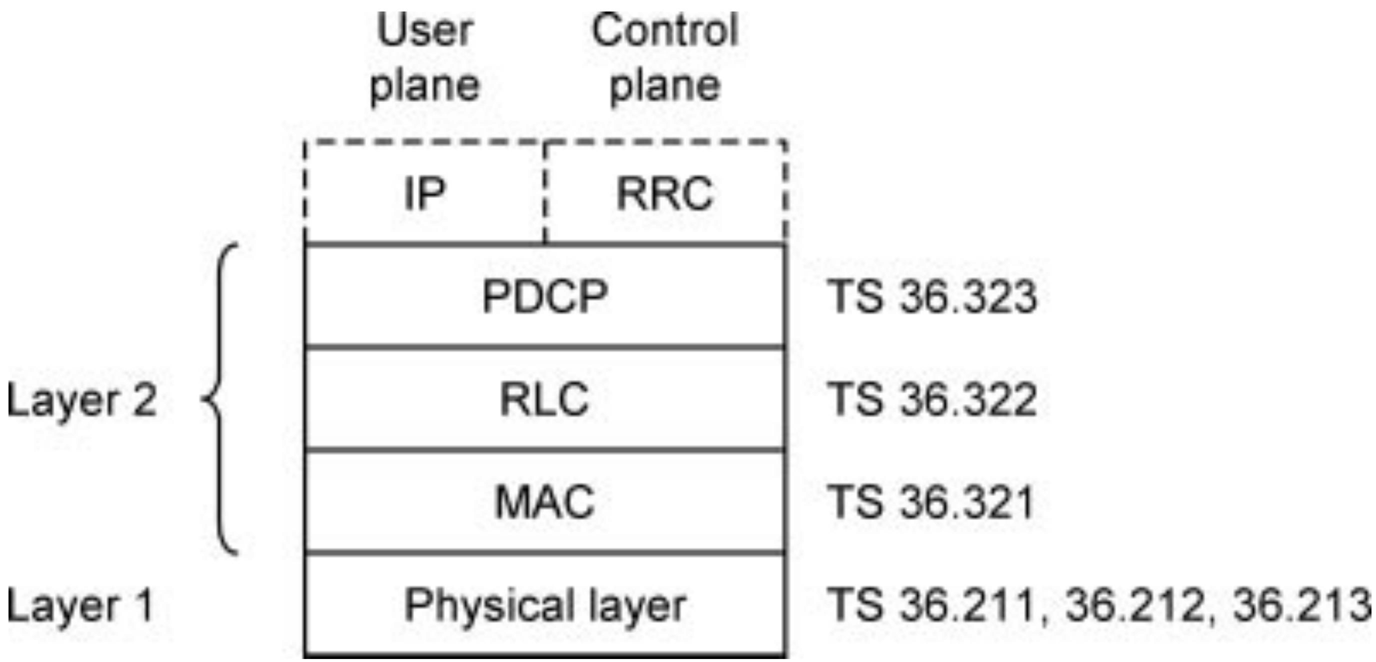
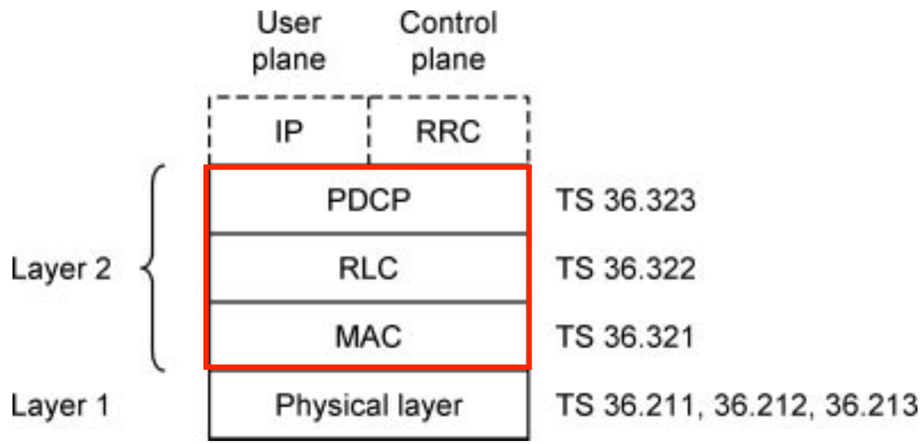


Figure 2.11 Transport protocols used on the air interface.

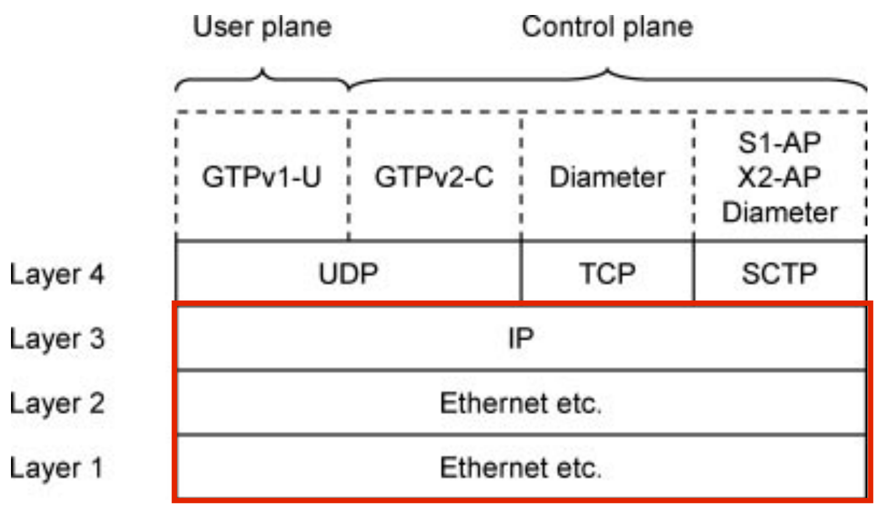
- The next three protocols make up data link layer, the layer 2 of OSI model
  - ✓ Packet Data Convergence Protocol (PDCP)
    - Carries out higher-level transport functions that are related to header compression and security
  - ✓ Radio Link Control (RLC) protocol
    - Maintains the data link between the two devices, for example by ensuring reliable delivery for data streams that need to arrive correctly
  - ✓ Medium Access Control (MAC) protocol
    - Carries out low-level control of the physical layer, particularly by scheduling data transmissions between mobile and BS



Transport protocols used on the air interface

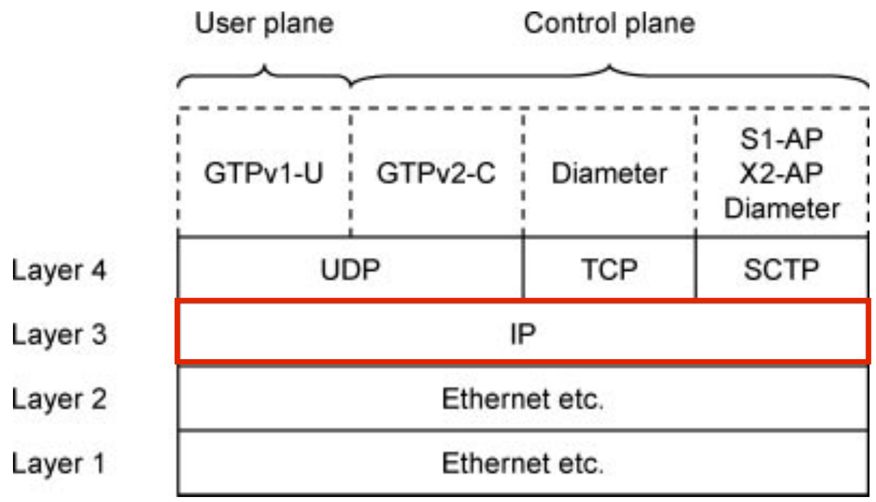
2.2.3 Fixed Network Transport Protocols

- Each interface in the fixed network uses standard IETF transport protocols shown in Figure 2.12
- These interfaces use protocols from layers 1 to 4 of the usual OSI model
- The transport network can use any suitable protocols for layers 1 and 2, such as Ethernet
- Every network element is then associated with an IP address, and the fixed network uses the Internet Protocol (IP) to route information from one element to another across underlying transport network



Transport protocols used by the fixed network

- LTE supports both IPv4 and IPv6 for this task
- In the EPC, support of IPv4 is mandatory and support of IPv6 is recommended
- The radio access network can use either or both of the two protocols



Transport protocols used by the fixed network

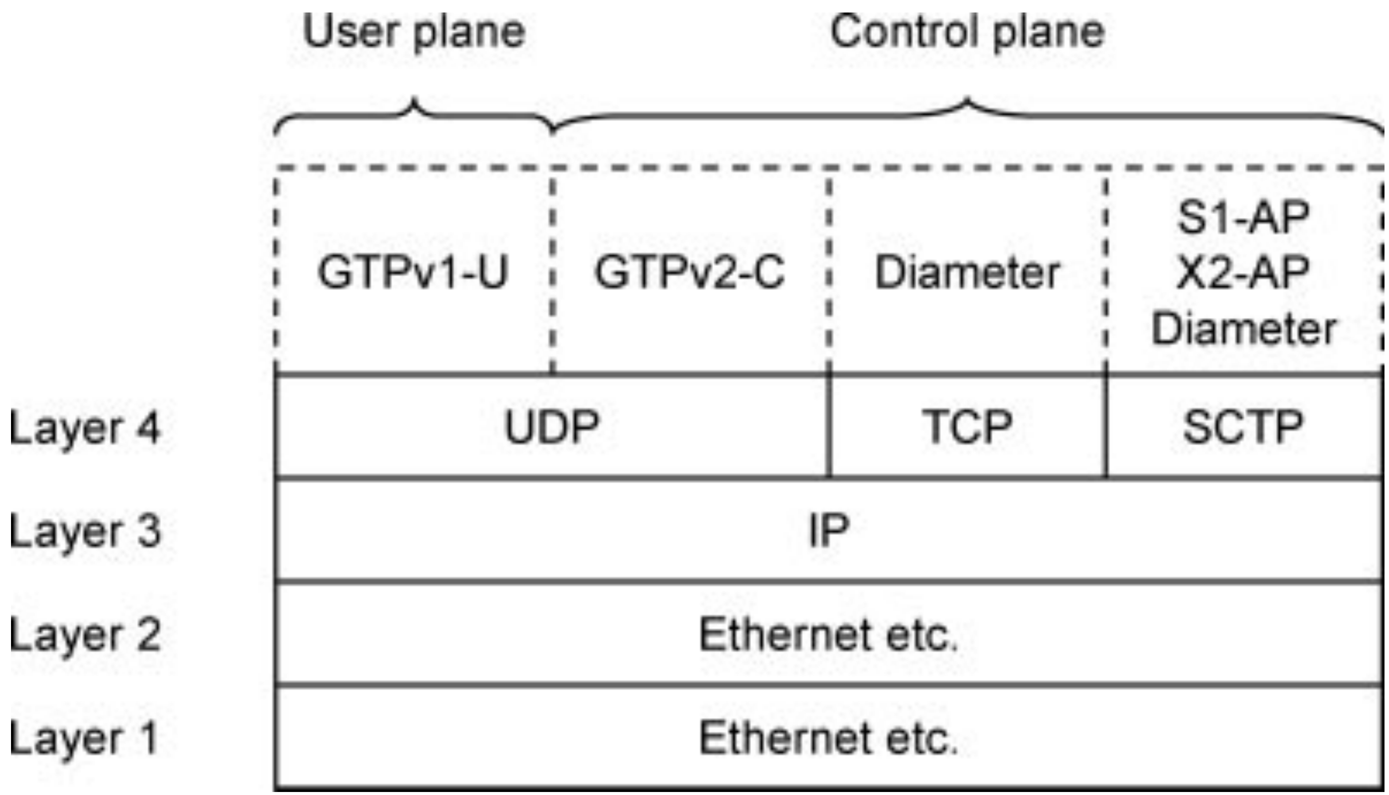
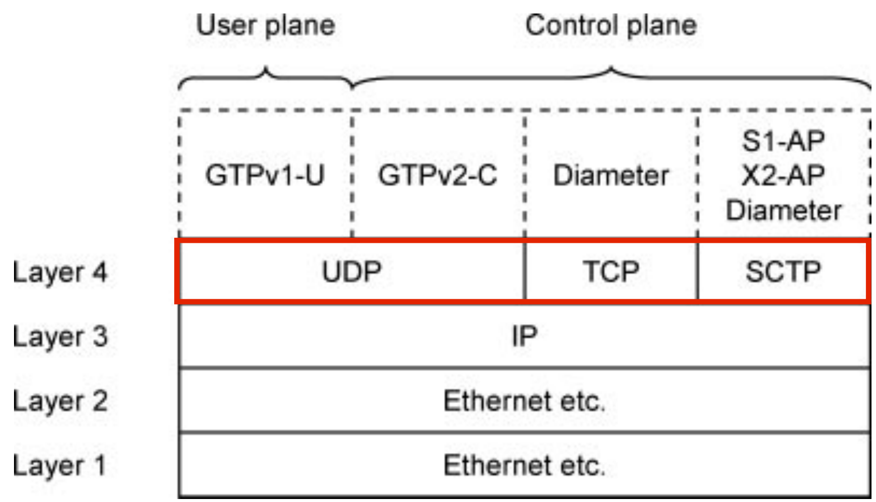
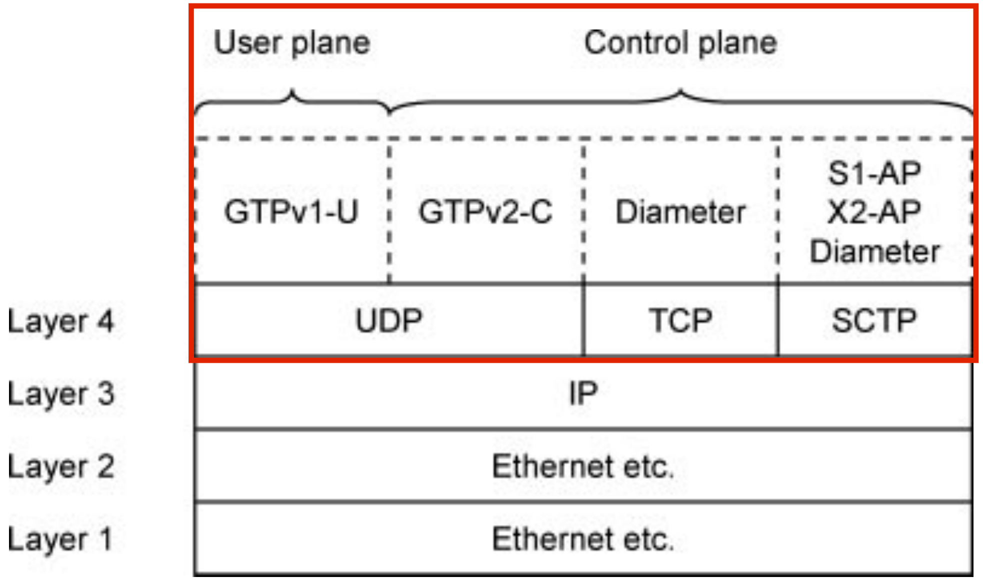


Figure 2.12 Transport protocols used by the fixed network.

- Above IP, there is a transport layer protocol across the interface between each individual pair of network elements
- Three transport protocols are used
  - ✓ User Datagram Protocol (UDP)
    - Just sends data packets from one network element to another
  - ✓ Transmission Control Protocol (TCP)
    - Re-transmits packets if they arrive incorrectly
  - ✓ Stream Control Transmission Protocol (SCTP)
    - Based on TCP, but includes extra features that make it more suitable for the delivery of signaling messages

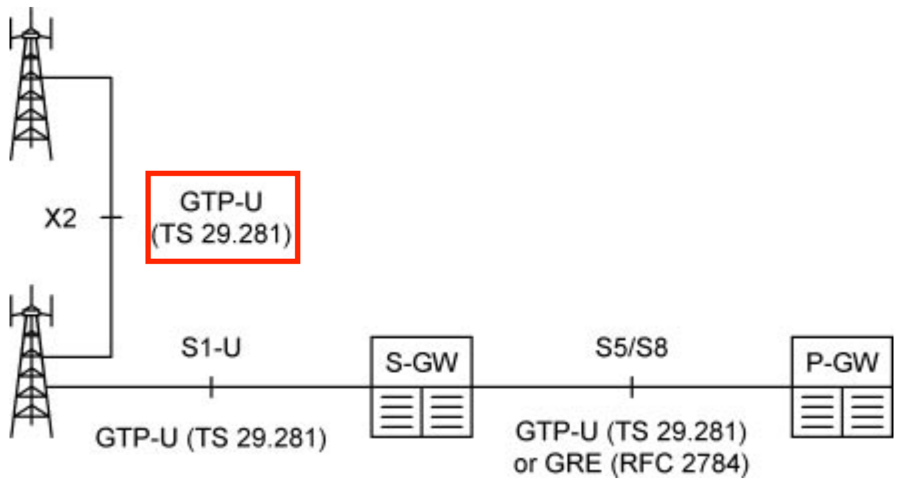


- User plane
  - ✓ Always uses UDP as its transport protocol, to avoid delaying the data
- Control plane
  - ✓ Its choice depends on the overlying signaling protocol



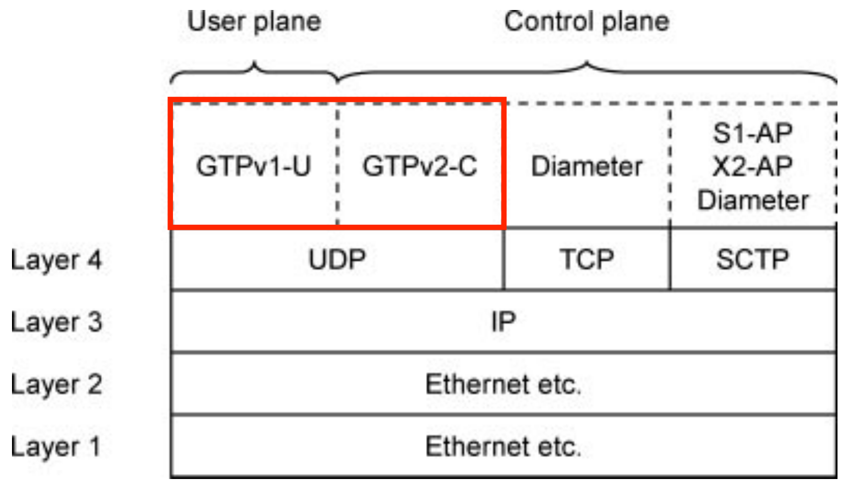
2.2.4 User Plane Protocols

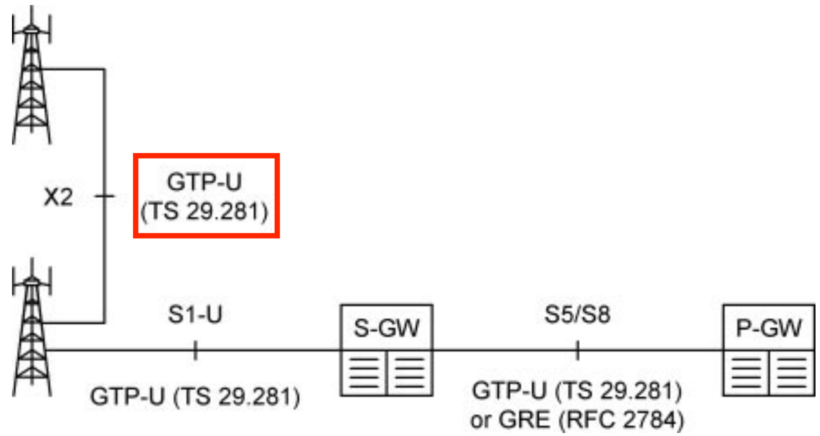
- LTE user plane contains mechanisms to
  - ✓ Forward data correctly between mobile and P-GW
  - ✓ Respond quickly to changes in the mobile's location
- These mechanisms are implemented by user plane protocols shown in Figure 2.13



User plane protocols used by LTE

- Most of the user plane interfaces use a 3GPP protocol known as GPRS Tunneling Protocol User part (GTP-U)
- GTPv1-U
  - ✓ LTE uses version 1 of the protocol along with the 2G and 3G packet switched domains from Release 99
- GTPv0-U
  - ✓ Earlier 2G networks used version 0





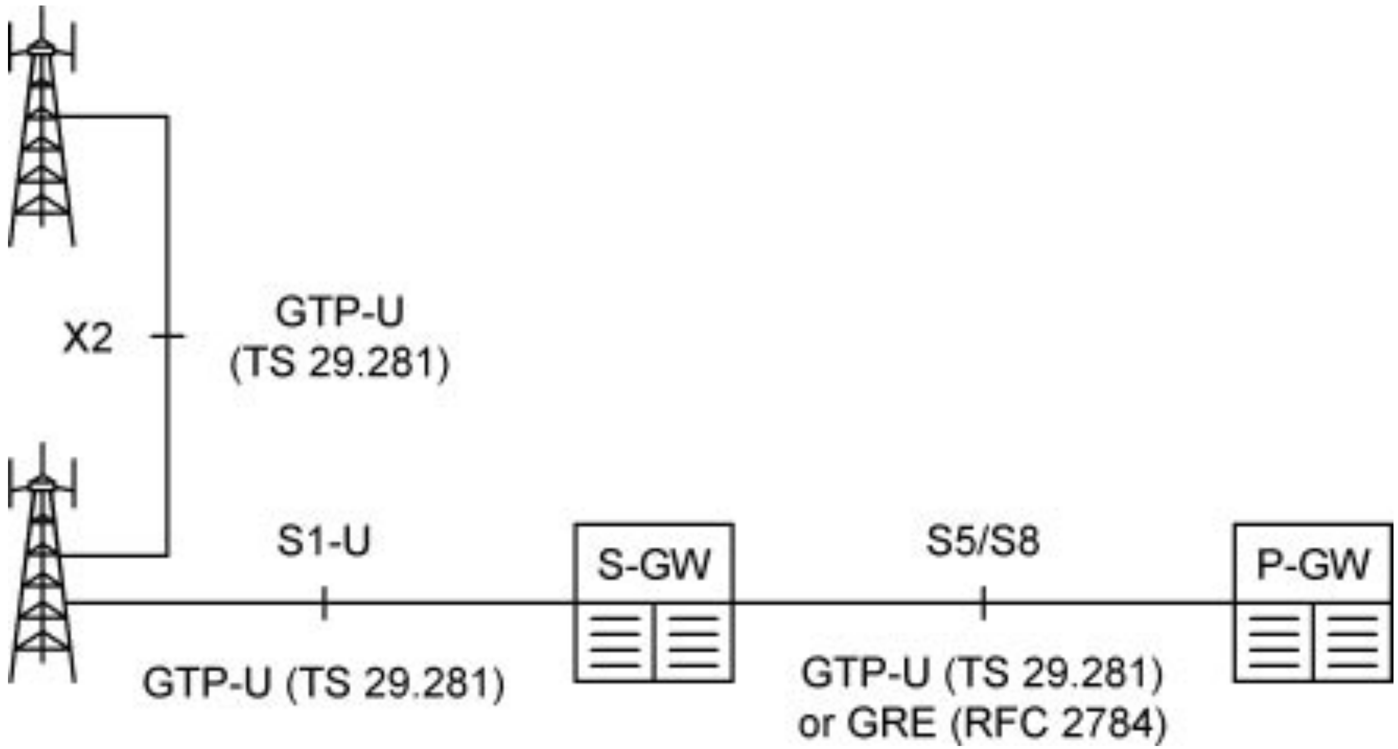
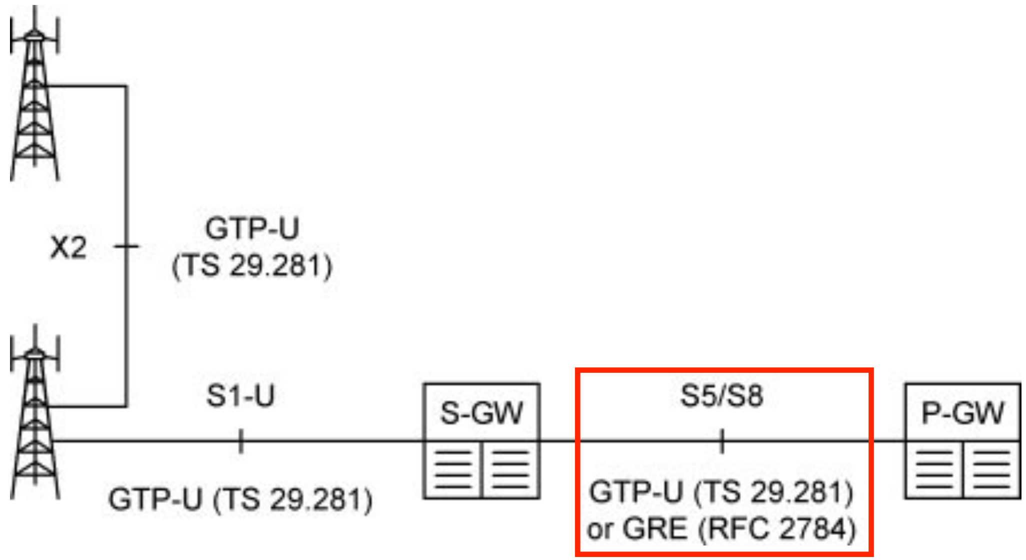


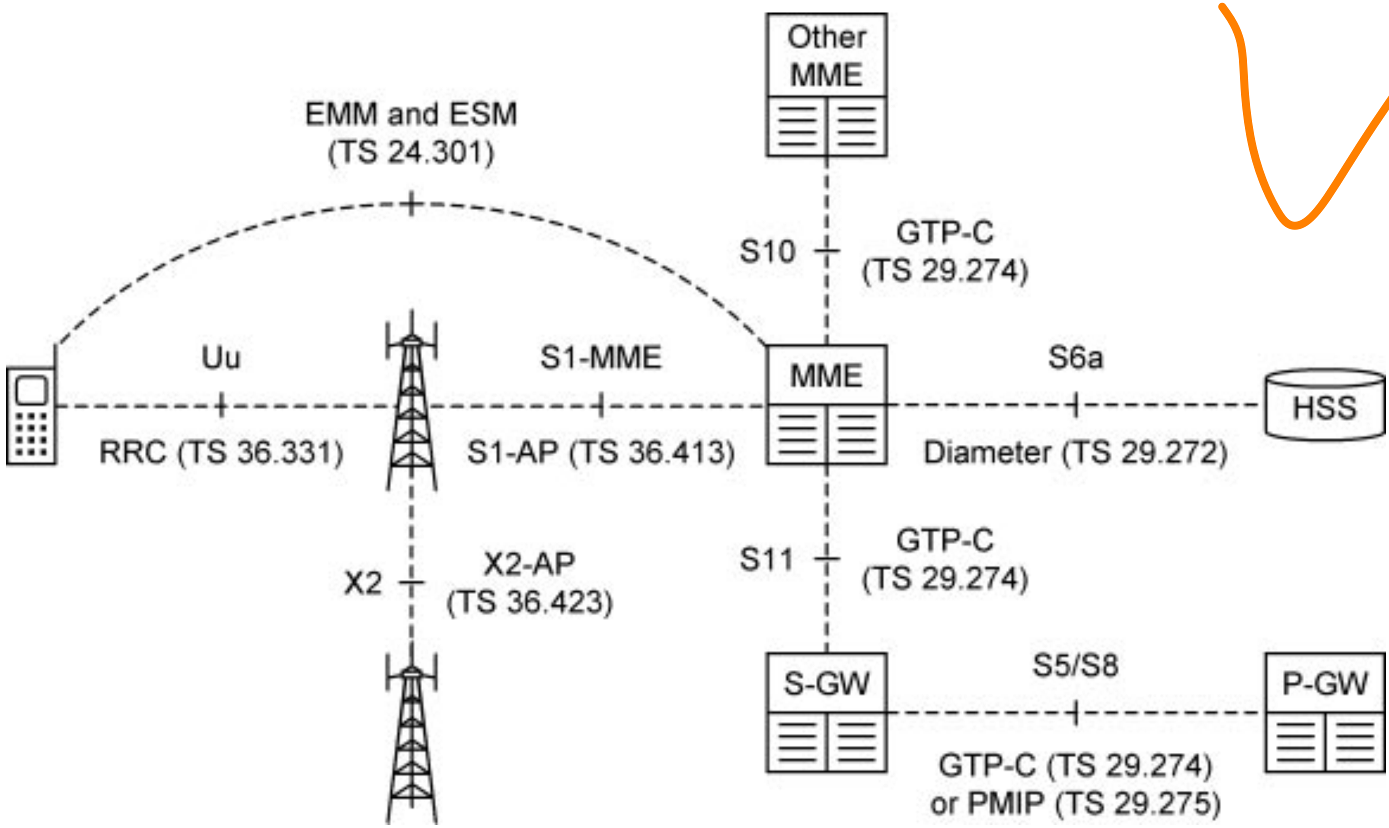
Figure 2.13 User plane protocols used by LTE.

- Between S-GW and P-GW, the S5/S8 user plane has an alternative implementation, known as Generic Routing Encapsulation (GRE)
- GTP-U and GRE forward packets from one network element to another using a technique known as tunneling



2.2.5 Signaling Protocols

- LTE uses a large number of signaling protocols (Figure 2.14)



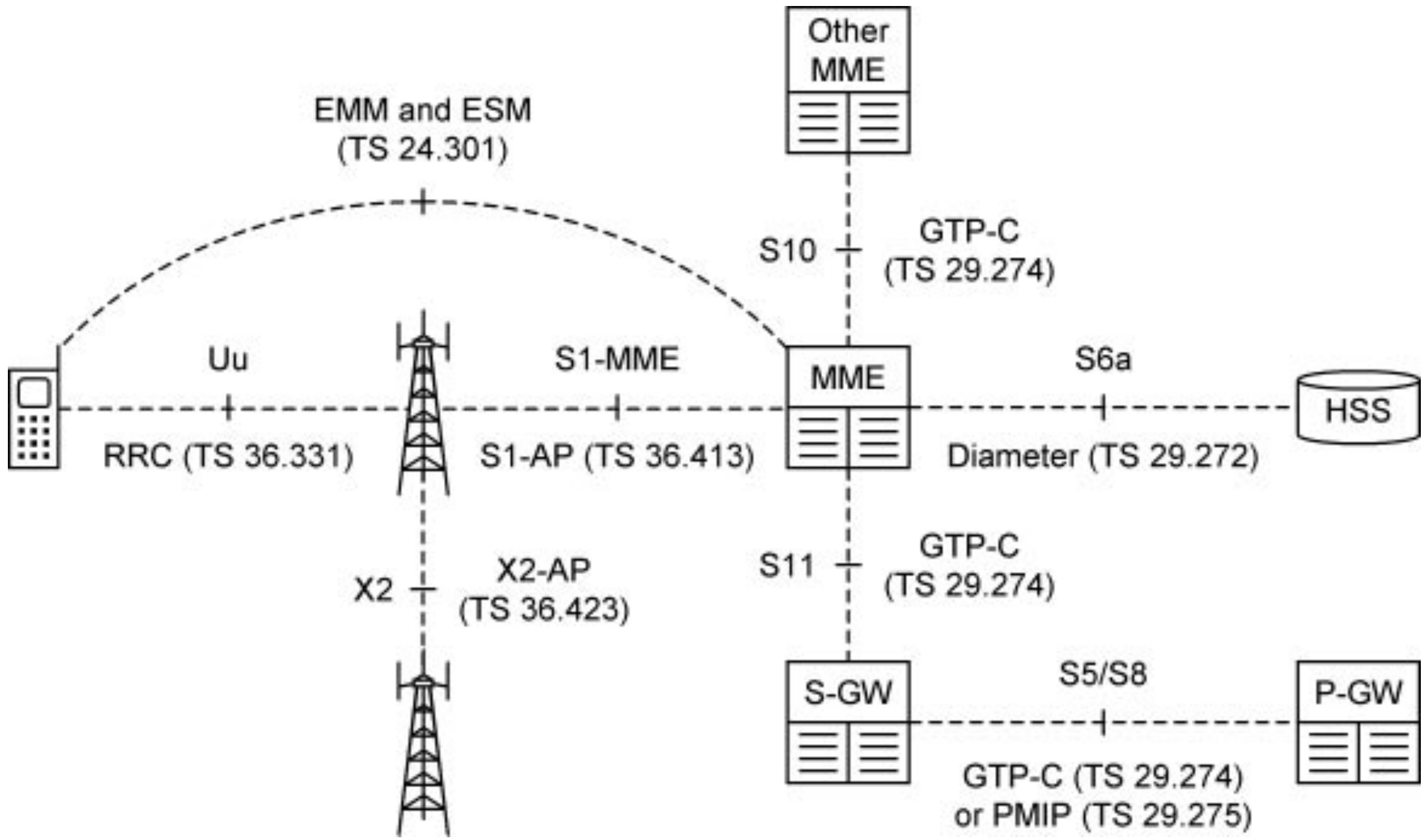
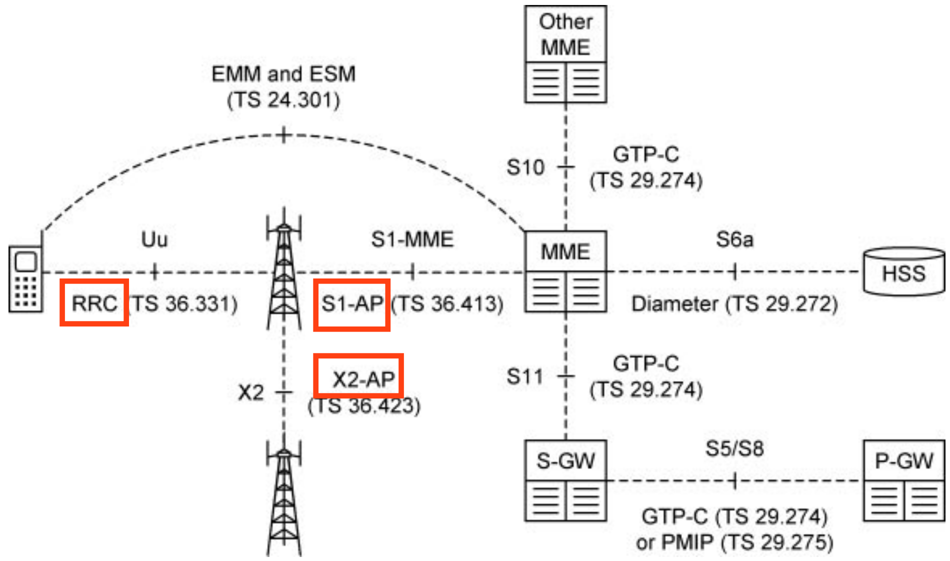
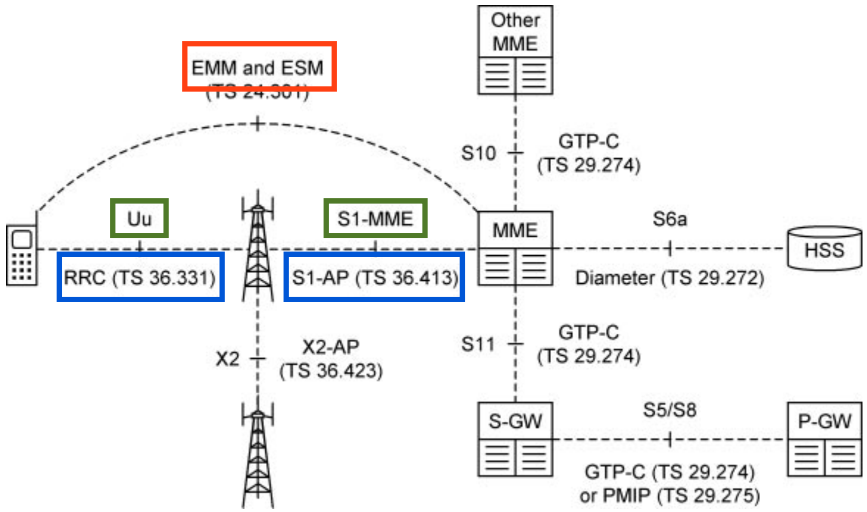


Figure 2.14 Signaling protocols used by LTE.

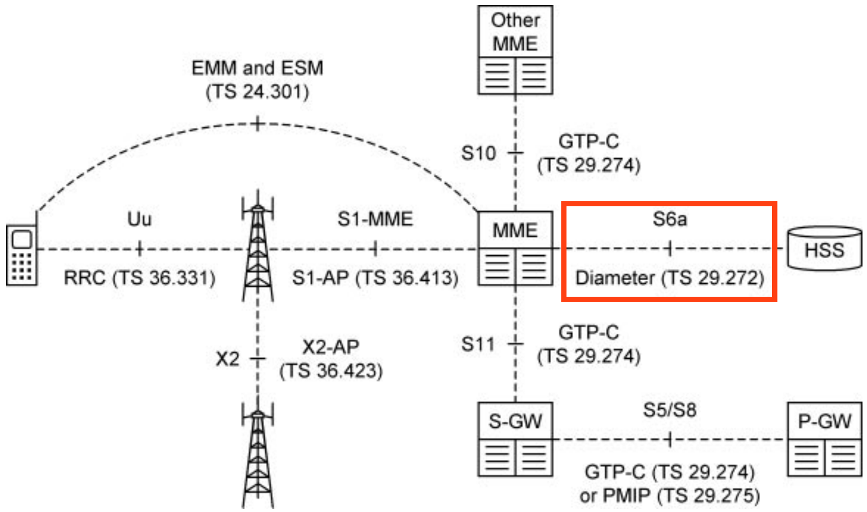
- Radio Resource Control (RRC) protocol
  - ✓ BS controls a mobile's radio communications
- S1 Application Protocol (S1-AP)
  - ✓ MME controls BSs
- X2 application protocol (X2-AP)
  - ✓ Communication between two BSs



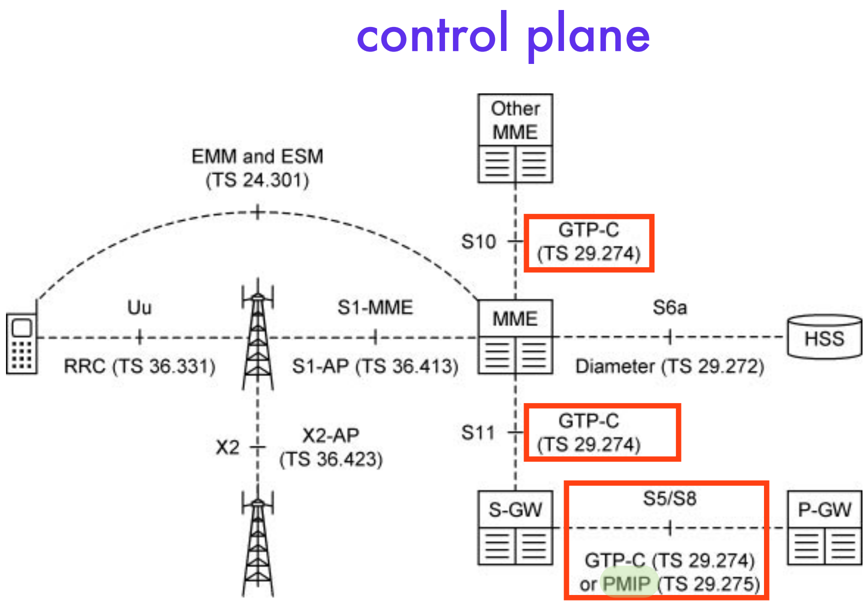
- MME controls a mobile's high-level behavior using
  - ✓ EPS Session Management (ESM)
    - Controls the data streams through which a mobile communicates with the outside world
  - ✓ EPS Mobility Management (EMM)
    - Handles internal bookkeeping within EPC
- The network transports EMM and ESM messages by
  - ✓ Embedding them into lower-level RRC and S1-AP messages and then
  - ✓ Using the transport mechanisms of the *Uu* and *S1* interfaces

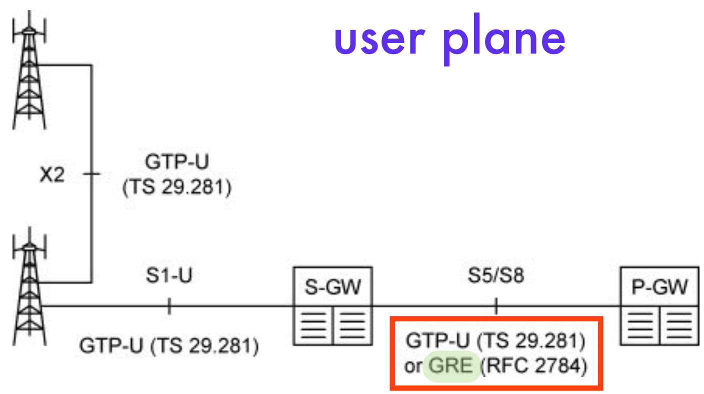


- Inside the EPC, HSS and MME communicate using a protocol based on Diameter
- Basic Diameter protocol
  - ✓ A standard IETF protocol for authentication, authorization and accounting
  - ✓ Based on an older protocol known as Remote Authentication Dial In User Service (RADIUS)
  - ✓ Can be enhanced for use in specific applications: the implementation of Diameter on the *S6a* interface

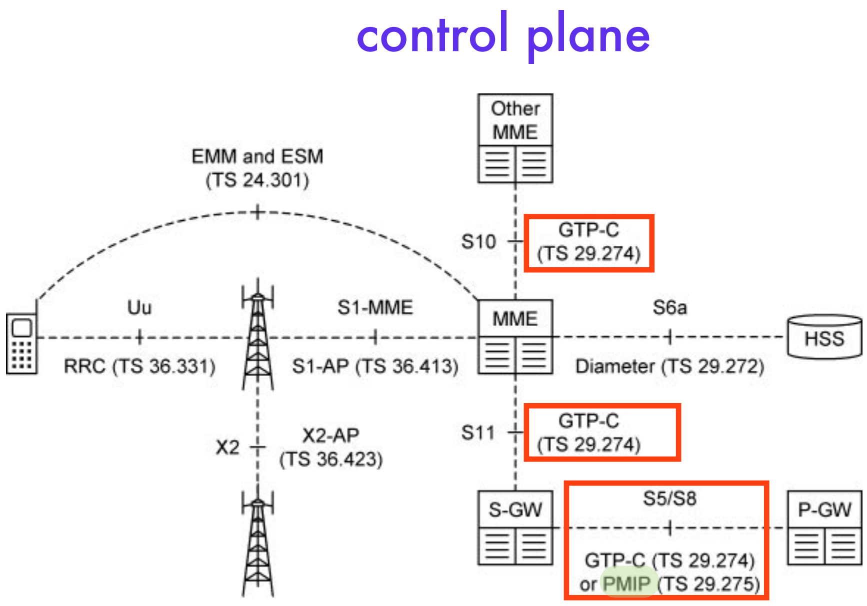


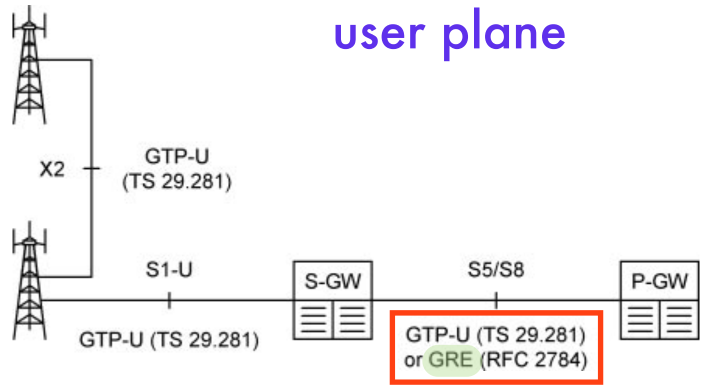
- Most of the other EPC interfaces use a 3GPP protocol known as GPRS Tunneling Protocol Control part (GTP-C)
  - ✓ LTE uses version 2 of the protocol, GTPv2-C
- If the *S5/S8* user plane is using GRE, then its control plane uses a signaling protocol known as Proxy Mobile IPv6 (PMIPv6)
  - ✓ PMIPv6 is a standard IETF protocol for the management of packet forwarding, in support of mobile devices such as laptops





- Operators of legacy 3GPP networks
  - ✓ Prefer GTP-U and GTP-C, for consistency with their previous systems and with other signaling interfaces in the EPC
- Operators of non 3GPP networks
  - ✓ Prefer GRE and PMIP, which are standard IETF protocols, and which are also used for inter-operation between LTE and non 3GPP technologies



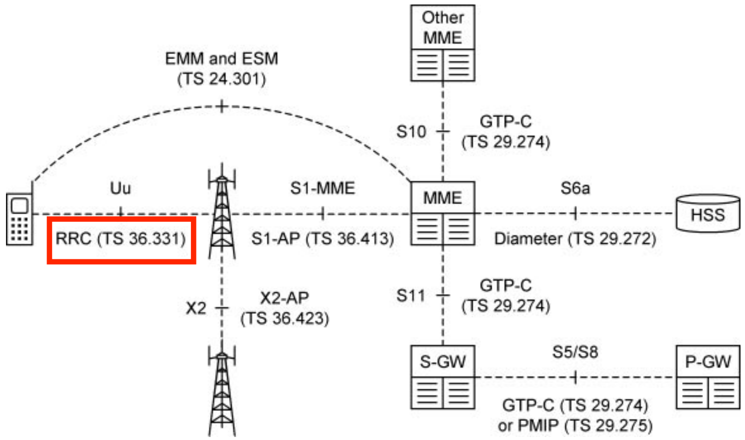


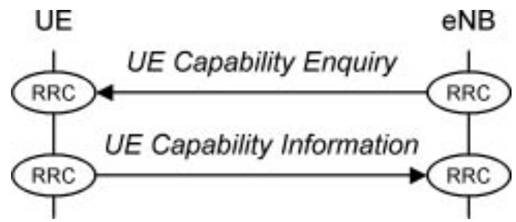
2.3 Example Information Flows

- 2.3.1 Access Stratum Signaling
- 2.3.2 Non Access Stratum Signaling
- 2.3.3 Data Transport

2.3.1 Access Stratum Signaling

- Consider an exchange of RRC signaling messages between mobile and BS
- Figure 2.15 is the message sequence for an RRC procedure known as UE Capability Transfer
- The serving eNB wishes to find out the mobile's radio access capabilities
  - ✓ The max data rate it can handle
  - ✓ The specification release that it conforms to
- RRC protocol composes a message called UE Capability Enquiry, and sends it to the mobile
- The mobile responds with an RRC message called UE Capability Information, in which it lists the capabilities required





UE capability transfer procedure

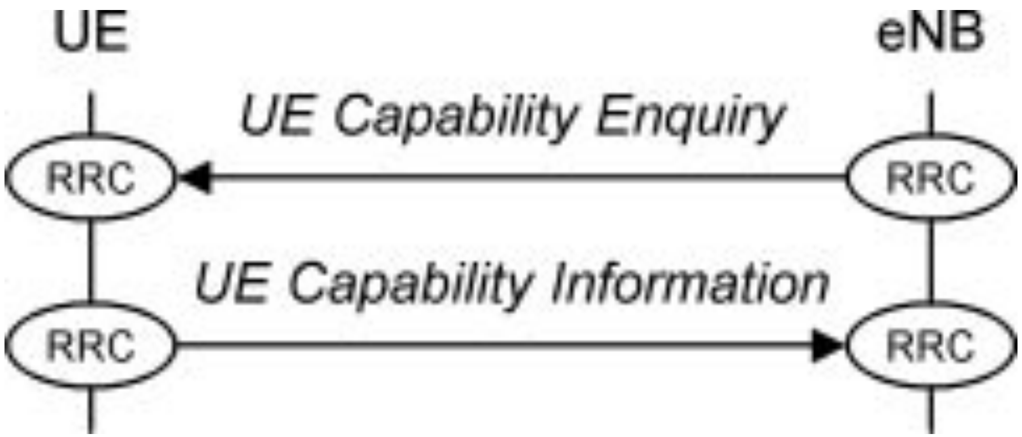
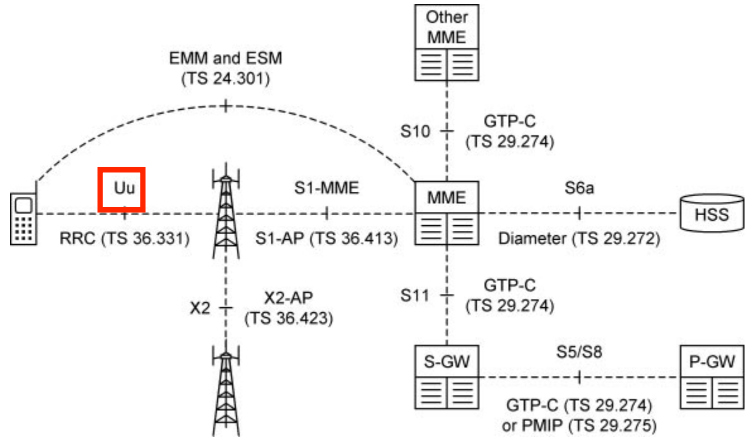
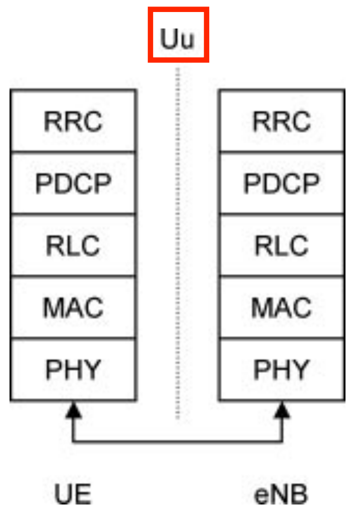


Figure 2.15 UE capability transfer procedure.

- The corresponding protocol stacks of RRC signaling messages exchange between mobile and BS are shown in Figure 2.16
  - ✓ BS
    - Composes its capability enquiry using RRC protocol
    - Processes it using PDCP, RLC and MAC
    - Transmits it using the air interface physical layer
  - ✓ Mobile
    - Receives the BS's transmission
    - Processes the information by passing it through the same sequence of protocols in reverse
    - Reads the enclosed message
    - Composes its reply





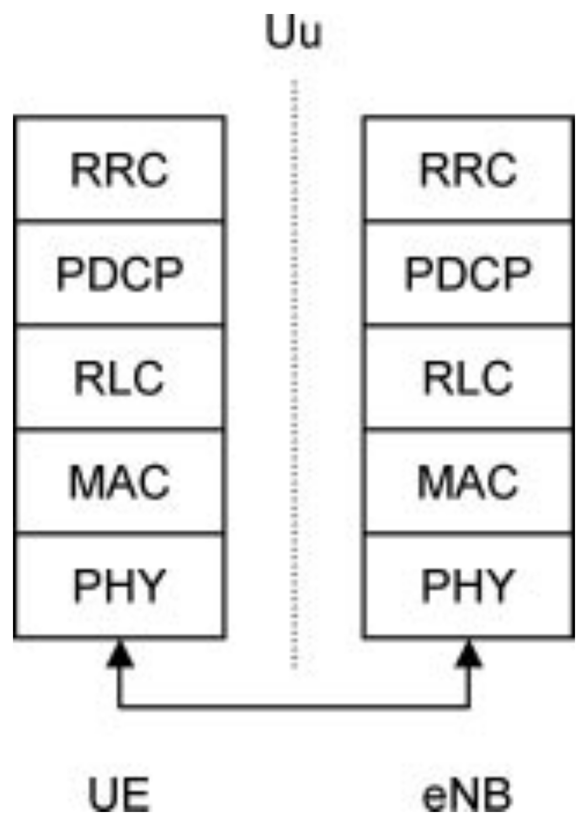
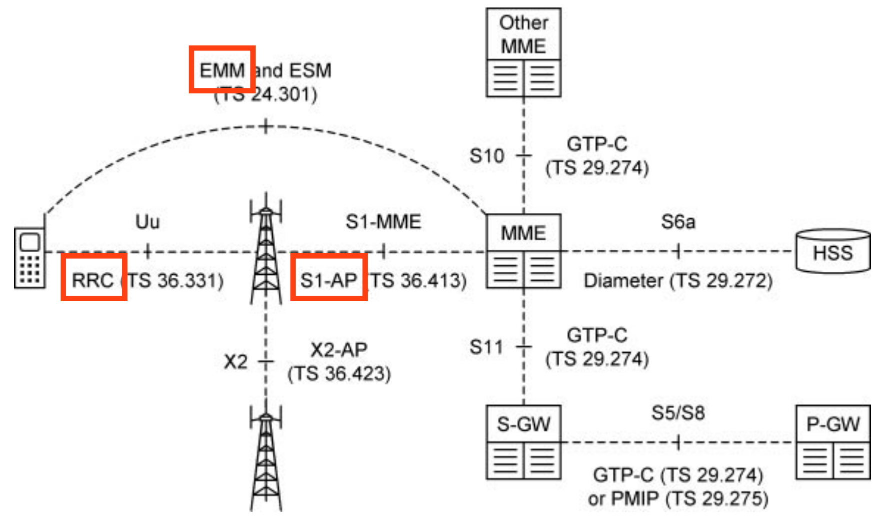
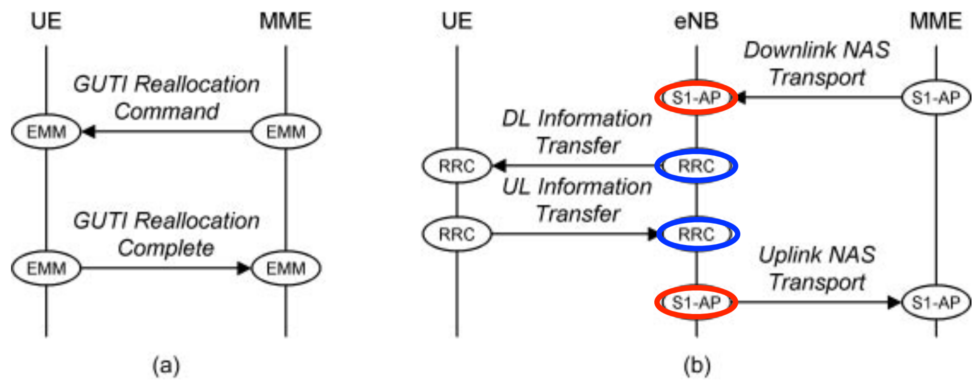


Figure 2.16 Protocol stacks used to exchange RRC signaling messages between mobile and BS.

2.3.2 Non Access Stratum Signaling

- Figure 2.17(a) shows the message sequence for an EMM procedure known as a GUTI (Globally Unique Temporary Identity) reallocation
- Using an EMM GUTI Reallocation Command, the MME can give the mobile a new GUTI
- In response, the mobile sends the MME an acknowledgement using an EMM GUTI Reallocation Complete
- LTE transports these messages by embedding them into S1-AP and RRC messages, as shown in Figure 2.17(b)
  - ✓ S1-AP messages are known as Uplink NAS Transport and Downlink NAS Transport
  - ✓ RRC messages are known as UL Information Transfer and DL Information Transfer





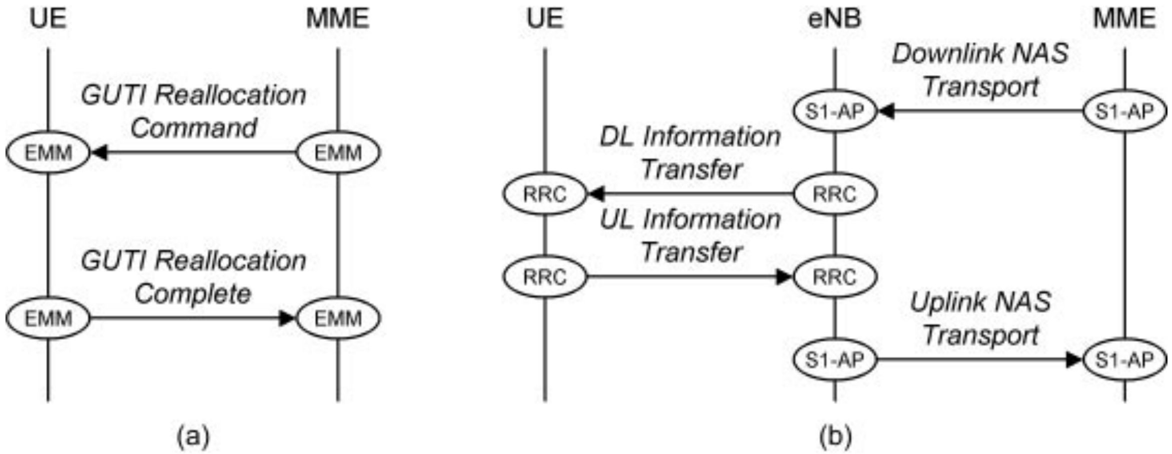
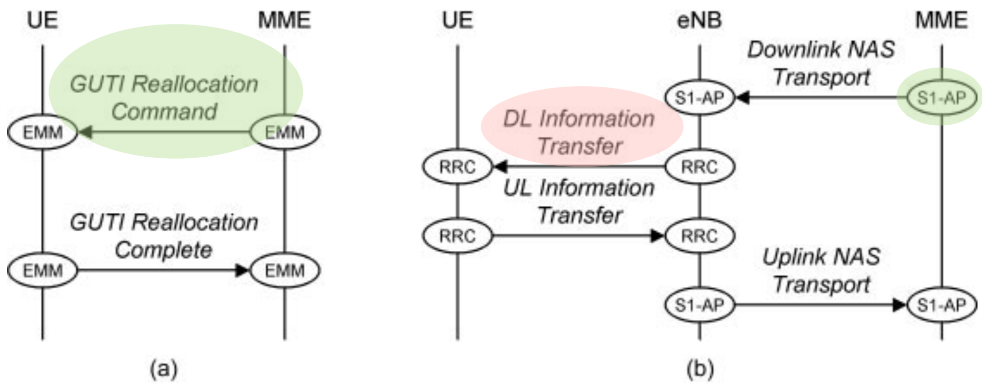
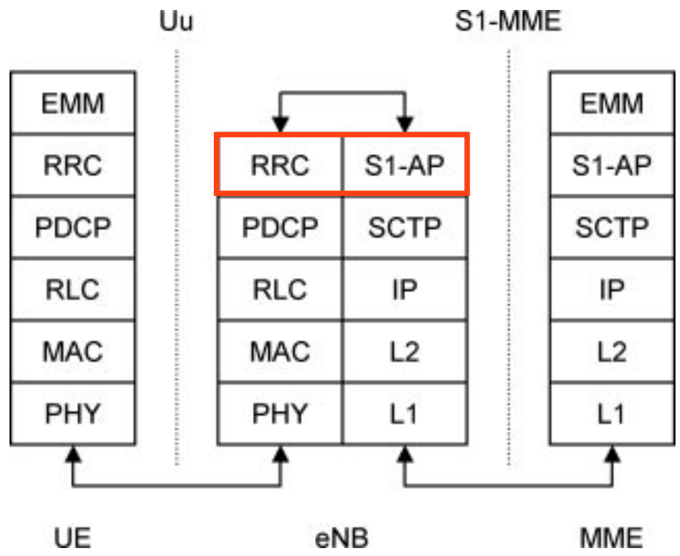


Figure 2.17 GUTI reallocation procedure.
(a) Non access stratum messages.
(b) Message transport using access stratum.

- Figure 2.18 shows the protocol stacks for this message sequence
  - ✓ MME
    - Writes the GUTI Reallocation Command using its EMM protocol
    - Embeds it in the S1-AP Downlink
  - ✓ NAS
    - Transport message and sends it to the BS using the transport mechanisms of the S1 interface
  - ✓ BS
    - Unwraps EMM message
    - Embeds it into an RRC DL Information Transfer
    - Sends it to the mobile using the air interface protocols
  - ✓ Mobile
    - Reads the message
    - Updates its GUTI
    - Sends an acknowledgement using the same protocol stacks in reverse





Protocol stacks used to exchange non access stratum signaling messages between mobile and MME

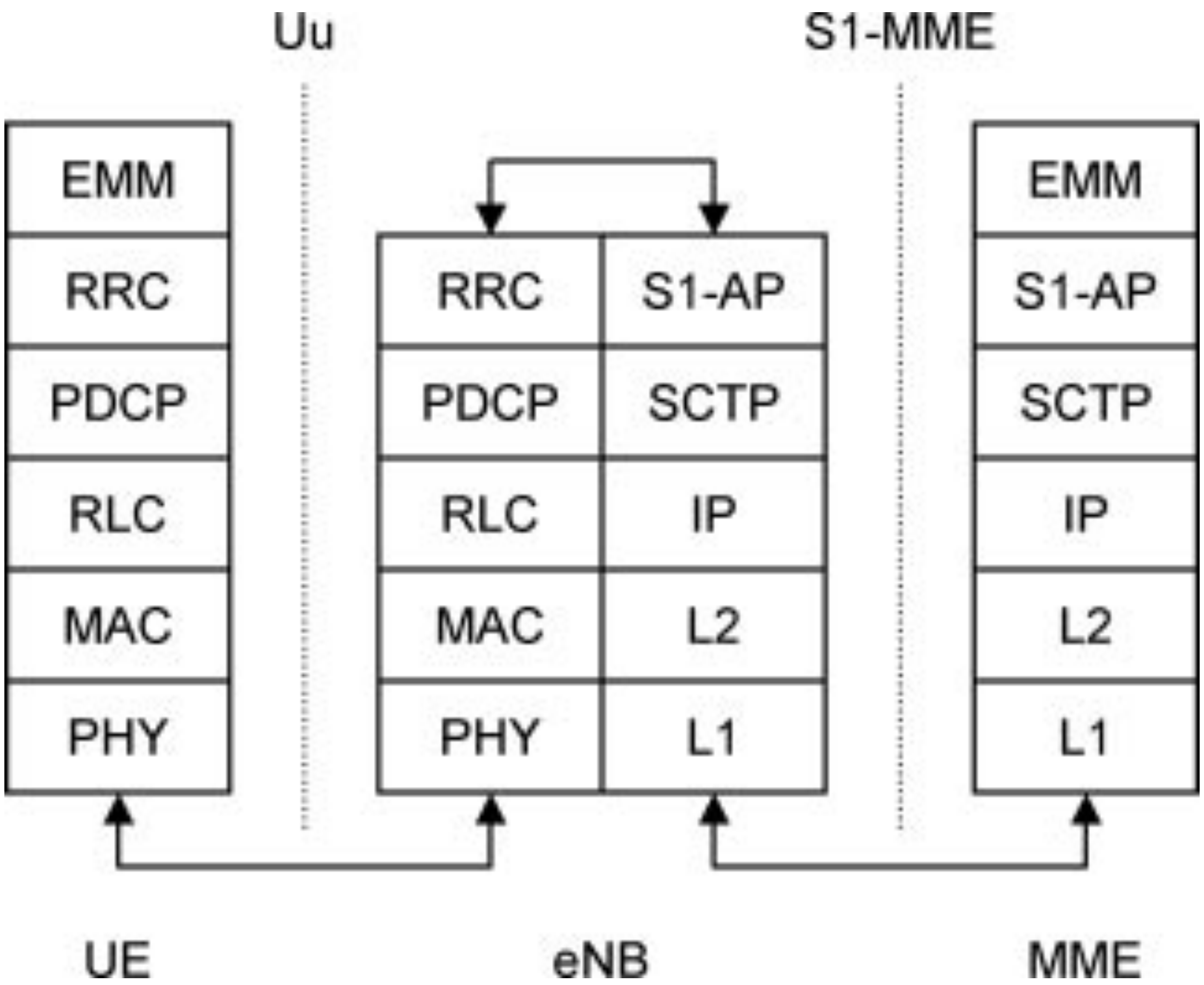
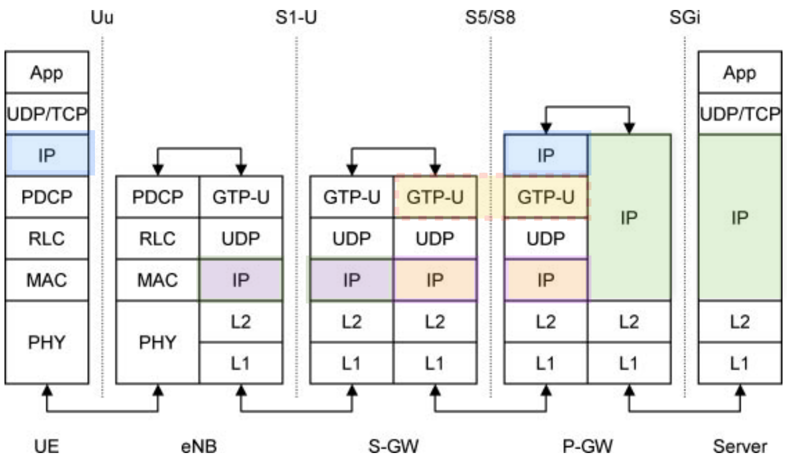


Figure 2.18 Protocol stacks used to exchange non access stratum signaling messages between mobile and MME.

2.3.3 Data Transport

- Figure 2.19 shows the protocol stacks that are used to exchange data between the mobile and a server in the outside world
- Assumed that the *S5/S8* interface is based on GTP rather than PMIP
- Consider the downlink path, from server to mobile
- [Server → P-GW] The mobile's IP address lies in the address space of the PDN gateway (P-GW), so the Internet routes each of the mobile's data packets towards that device
- [P-GW → S-GW] Using the tunneling mechanisms, the P-GW identifies the S-GW that is looking after the mobile, wraps the incoming packet up inside a second IP packet and sends that packet to the serving gateway's IP address
- [S-GW → eNB] In turn, the S-GW unwraps the incoming packet, and repeats the process on the *S1* interface towards the base station
- [eNB → mobile] Finally, the BS uses the transport mechanisms of the air interface to deliver the packet to the mobile



Protocol stacks used to exchange data between mobile and an external server, when using an S5/S8 interface based on GTP

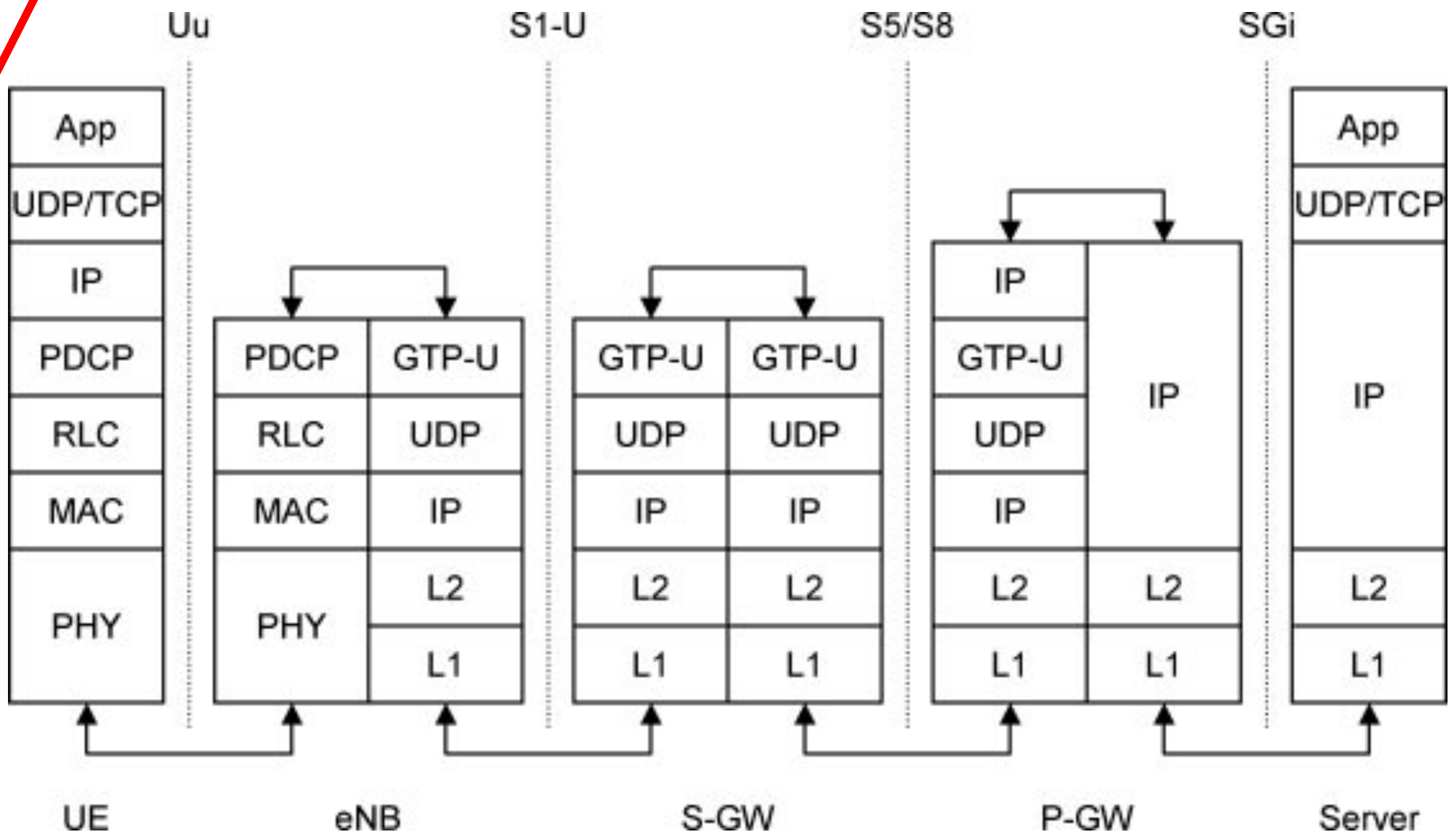


Figure 2.19 Protocol stacks used to exchange data between mobile and an external server, when using an S5/S8 interface based on GTP.

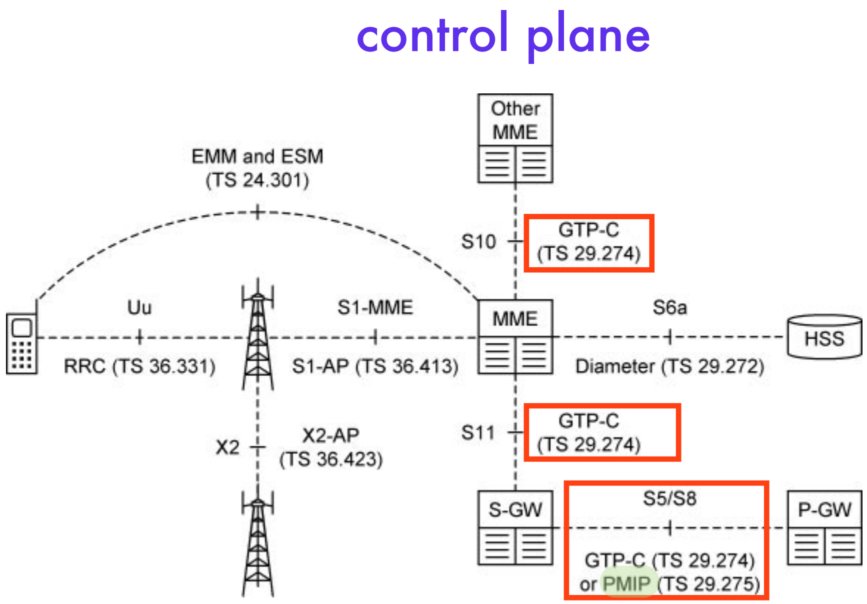
2.4 Bearer Management

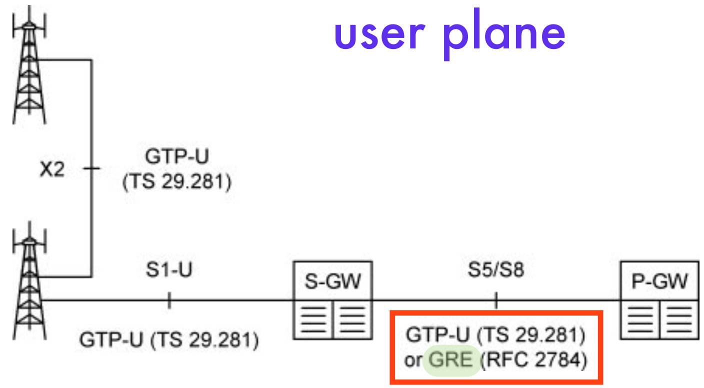
- 2.4.1 EPS Bearer
- 2.4.2 Tunneling Using GTP
- 2.4.3 Tunneling Using GRE and PMIP
- 2.4.4 Signaling Radio Bearers

2.4.1 EPS Bearer

- Bearer
  - ✓ A bearer channel is a digital signal that carries call content i.e. one that does not carry signaling
  - ✓ In the common-channel signaling scheme for telecommunications, signaling is sent out-of-band, while all other traffic rides bearer channels
- At a high level, LTE transports data from one part of the system to another using bearers
- The implementation of bearers depends on whether the S5/S8 interface is based on GTP or PMIP
- We start by describing what happens when using GTP, and cover the differences in the case of PMIP later on

- EPS (Evolved Packet System) bearer
  - ✓ Best thought of as a bi-directional data pipe, which
    - Transfers information between mobile and P-GW with a specific Quality of Service (QoS)
  - ✓ QoS
    - Defines how the data will be transferred
    - Parameters: data rate, error rate and delay
  - ✓ GTP-U and GTP-C protocols include mechanisms to
    - Set up, modify and tear down EPS bearers
    - Specify and implement their QoS





- The information carried by an EPS bearer comprises one or more service data flows
- Each service data flow comprises one or more packet flows, such as audio and video streams which make up that service
- LTE gives the same QoS to all the packet flows within a particular EPS bearer

- EPS bearers can be classified in two ways
  - ✓ 1st classification (GBR bearer & Non GBR bearer)
    - GBR bearer
      - GBR: Guaranteed Bit Rate
      - A long term average data rate that the mobile can expect to receive
      - Suitable for real-time services such as voice
    - Non GBR bearer
      - Receives no such guarantees
      - Suitable for non real-time services such as web browsing

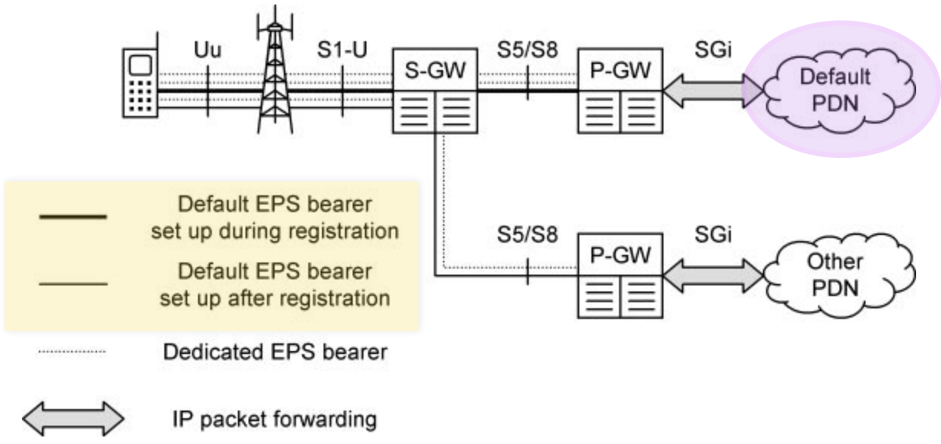
✓ 2nd classification (default bearer & dedicated bearer)

- Default bearer

  - The EPC sets up one EPS bearer, known as a default bearer, whenever a mobile connects to a PDN

  - A default bearer is always a non GBR bearer

  - As shown in Figure 2.20, a mobile receives one default bearer as soon as it registers with the EPC, to provide it with always-on connectivity to a default PDN such as Internet

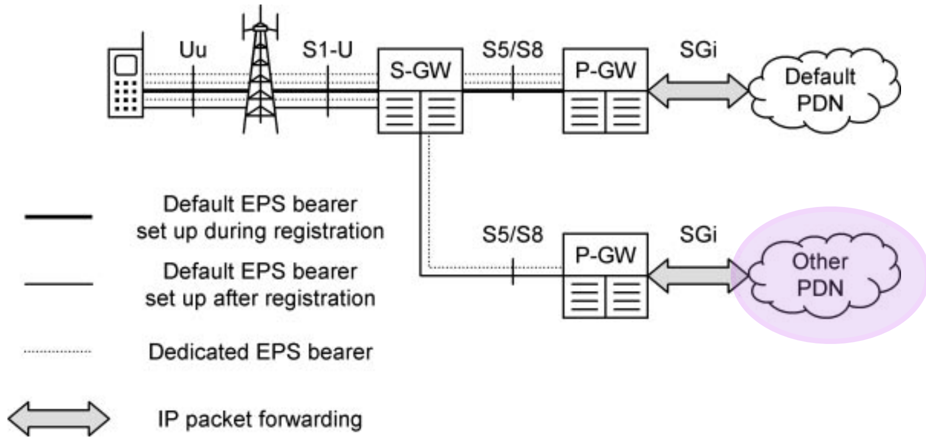


Default and dedicated EPS bearers, when using an S5/S8 interface based on GTP

- At the same time, the mobile receives an IP address for it to use when communicating with that network, or possibly an IPv4 address and an IPv6 address

- Later on, the mobile can establish connections with other packet data networks (PDN), for example private company networks

- If it does so, then it receives an additional default bearer for every network that it connects to, together with an additional IP address



Default and dedicated EPS bearers, when using an S5/S8 interface based on GTP

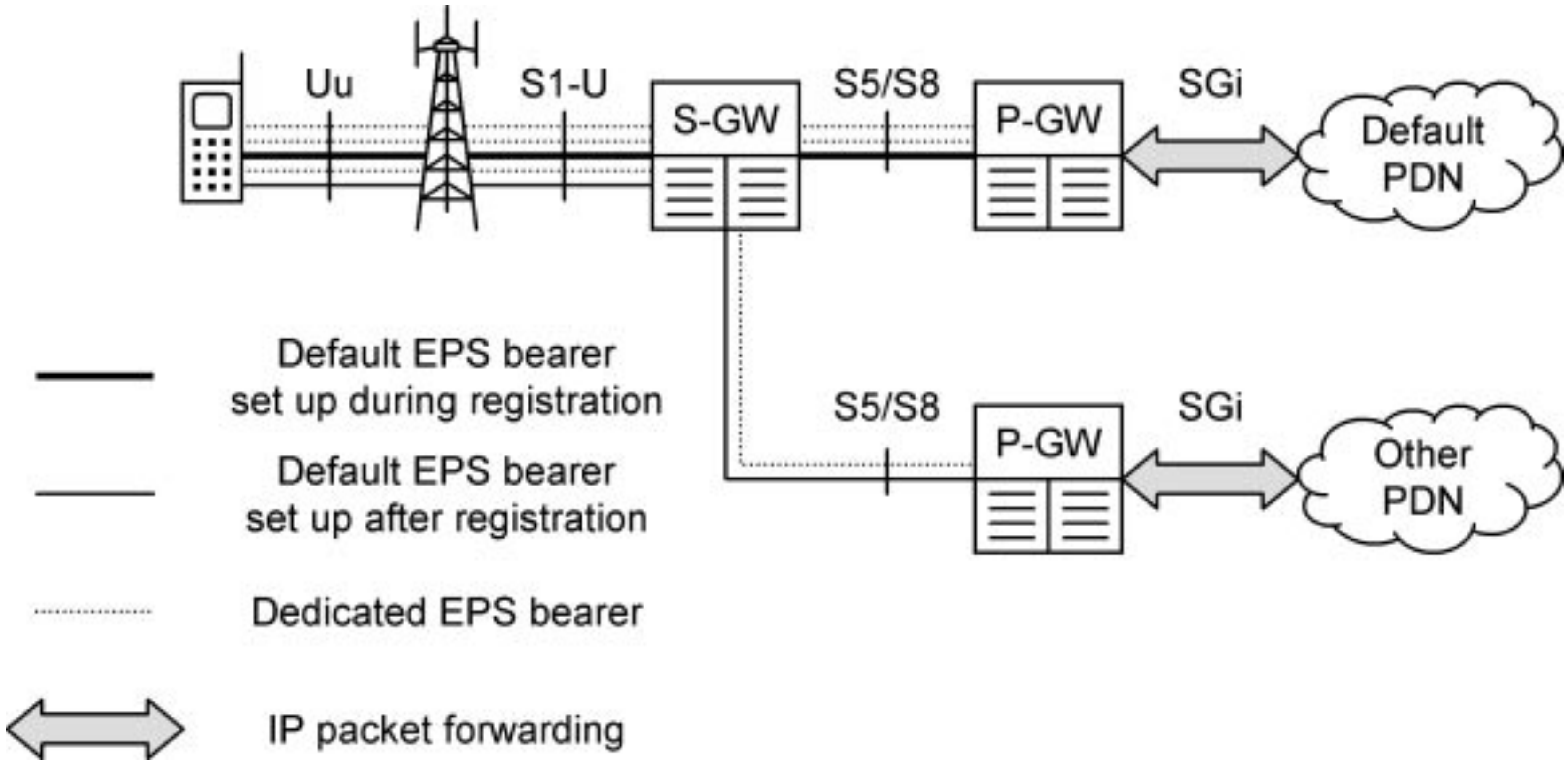


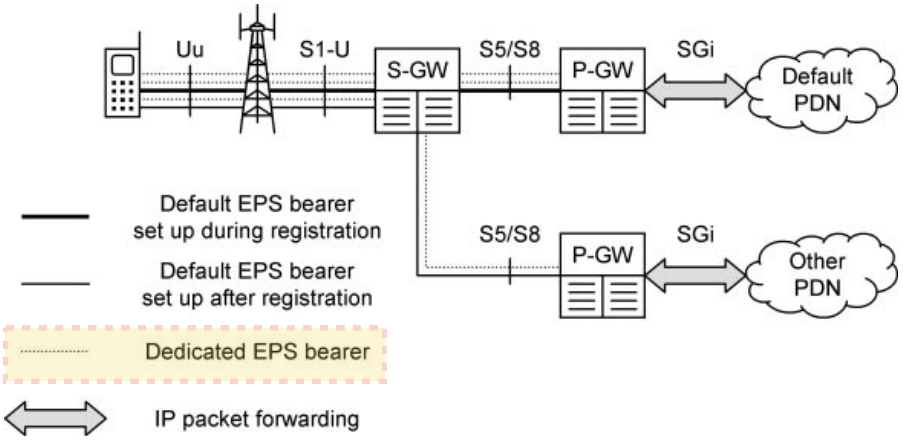
Figure 2.20 Default and dedicated EPS bearers, when using an S5/S8 interface based on GTP.

Dedicated bearer

- After connecting to a PDN and establishing a default bearer, a mobile can also receive one or more dedicated bearers that connect it to the same network

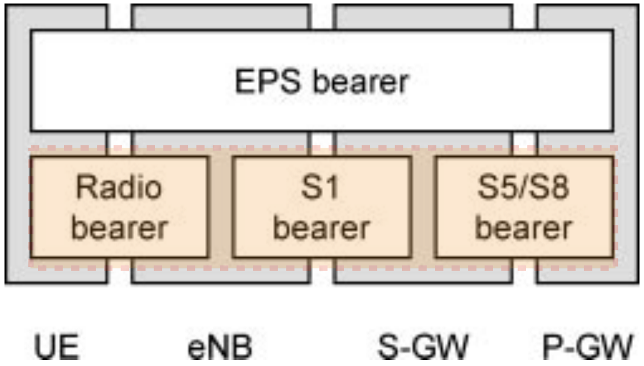
- This does NOT lead to the allocation of any new IP addresses: instead, each dedicated bearer shares an IP address with its parent default bearer

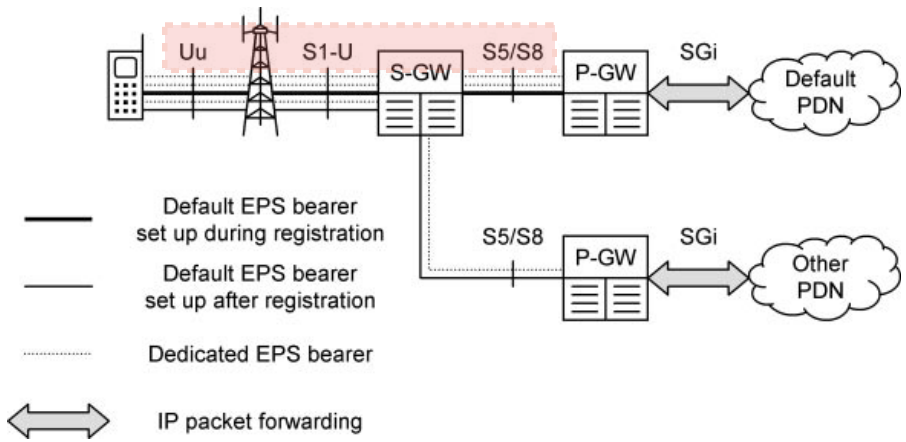
- A dedicated bearer typically has a better QoS than the default bearer can provide and in particular can have a guaranteed bit rate (GBR)



Default and dedicated EPS bearers, when using an S5/S8 interface based on GTP

- EPS bearer is broken down into three lower level bearers
  - ✓ Radio bearer (*Uu*)
  - ✓ *S1* bearer
  - ✓ *S5/S8* bearer
- Each of these is also associated with a set of QoS parameters, and receives a share of the EPS bearer's error rate and delay





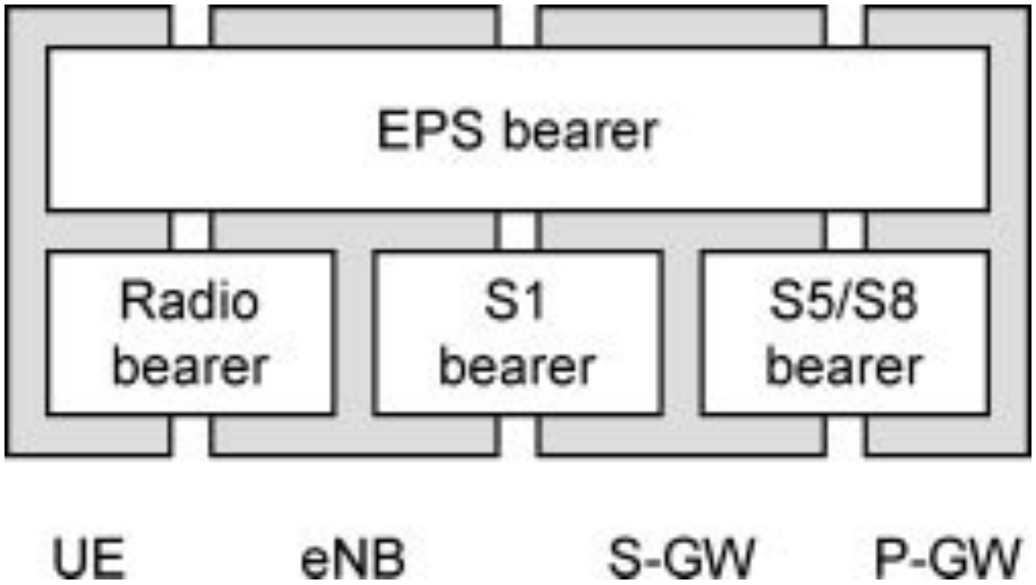
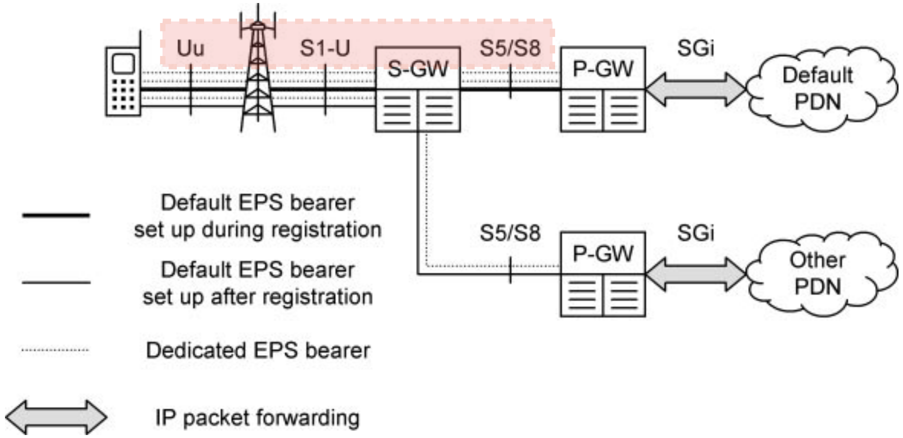


Figure 2.21 Bearer architecture of LTE, when using an S5/S8 interface based on GTP.

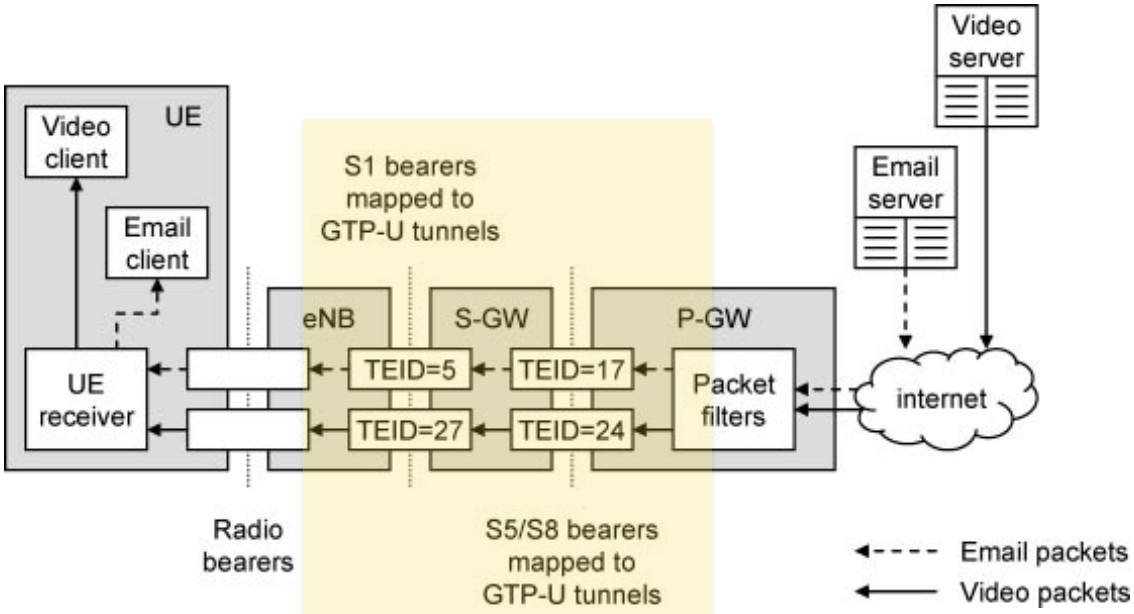
- Radio bearer
  - ✓ Implemented by a suitable configuration of air interface protocols



- *S1* and *S5/S8* bearers
  - ✓ Implemented using GTP-U tunnels
- Evolved Radio Access Bearer (E-RAB)
  - ✓ The combination of radio bearer and *S1* bearer

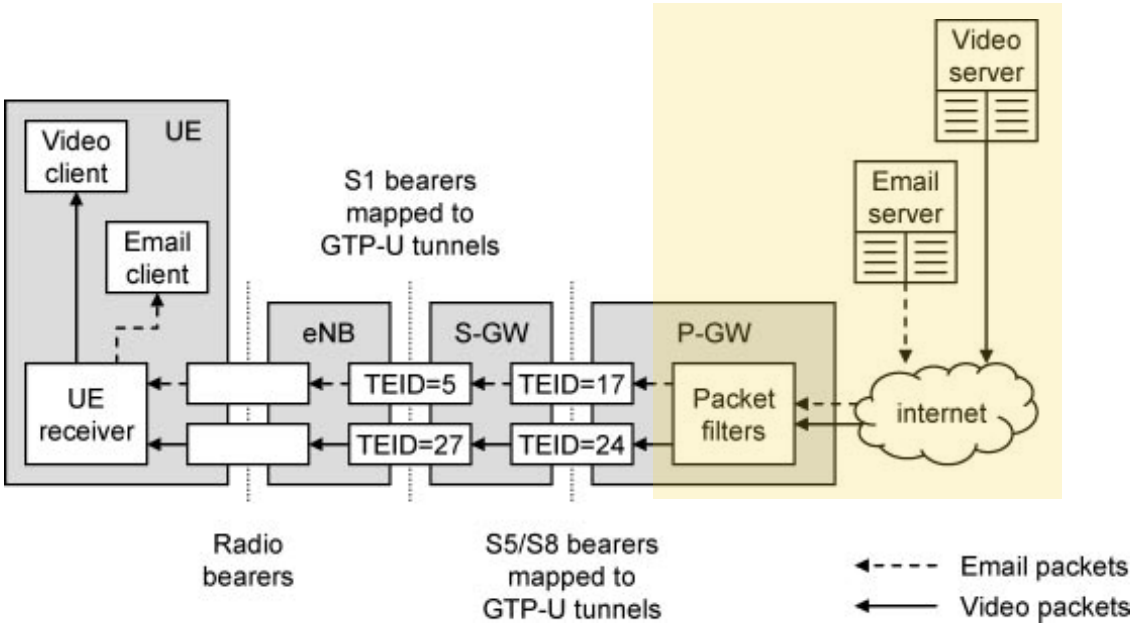
2.4.2 Tunneling Using GTP

- GTP-U protocol carries out a mapping between S1 and S5/S8 bearers and the fixed network's transport protocols, by associating each bearer with a bi-directional GTP-U tunnel
- Each tunnel is associated with two Tunnel Endpoint IDentifiers (TEIDs), one for uplink and one for downlink
- These identifiers are set up using GTP-C signaling messages, and are stored by the network elements at both ends of the tunnel



- GTP-C : GPRS Tunneling Protocol Control part
- GTP-U : GPRS Tunneling Protocol User part

- To illustrate how the tunnels are used, let us consider the flow of data packets on the downlink
  - ✓ In Figure 2.22, a mobile has two EPS bearers, which are carrying video and email packets that require different QoS
  - ✓ These packets arrive at the P-GW using the normal transport mechanisms of the Internet



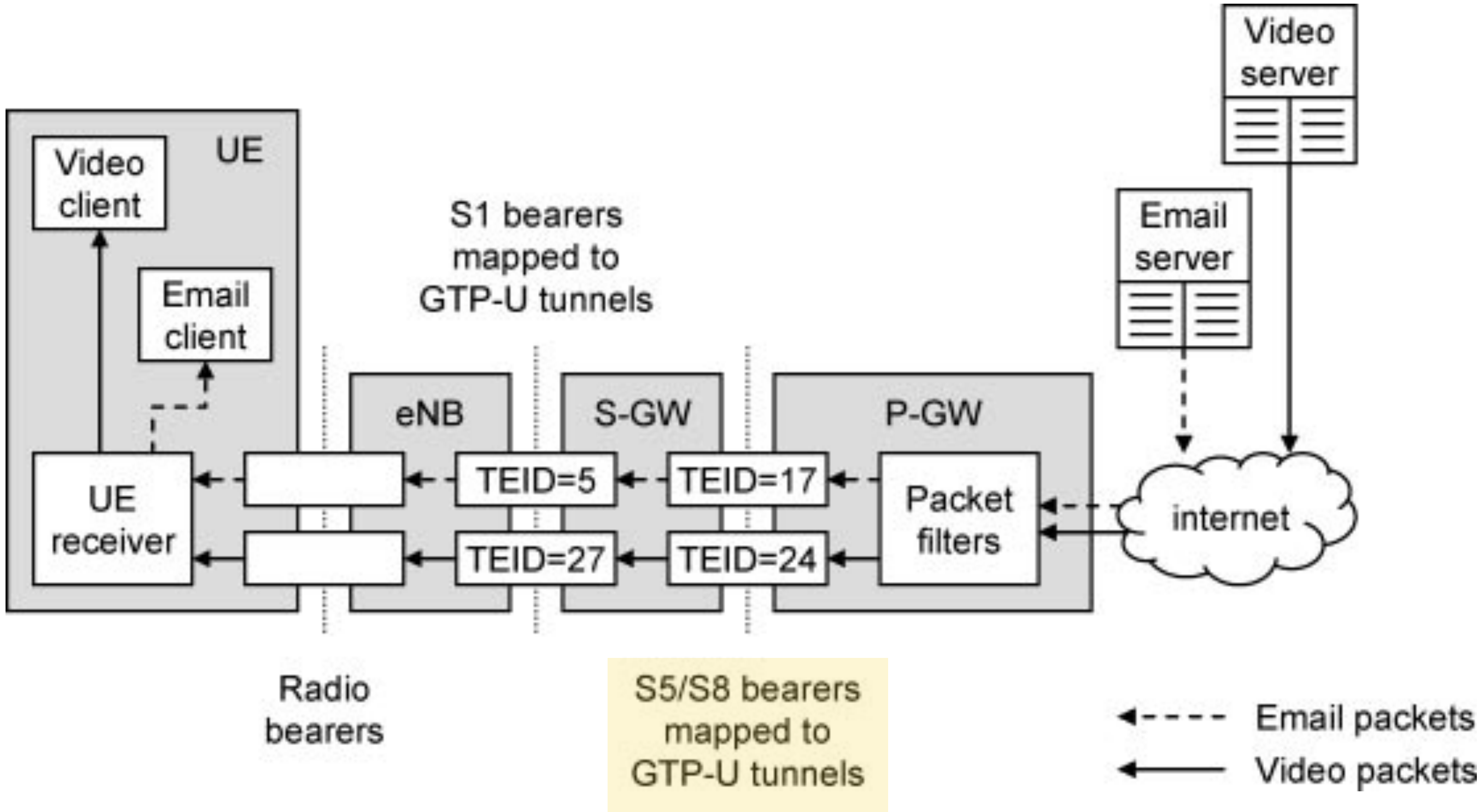
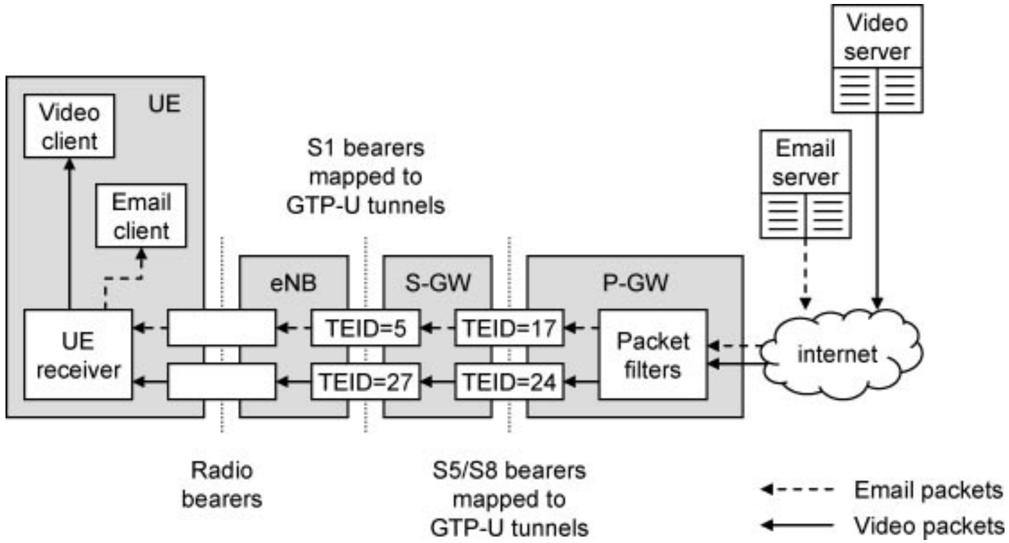


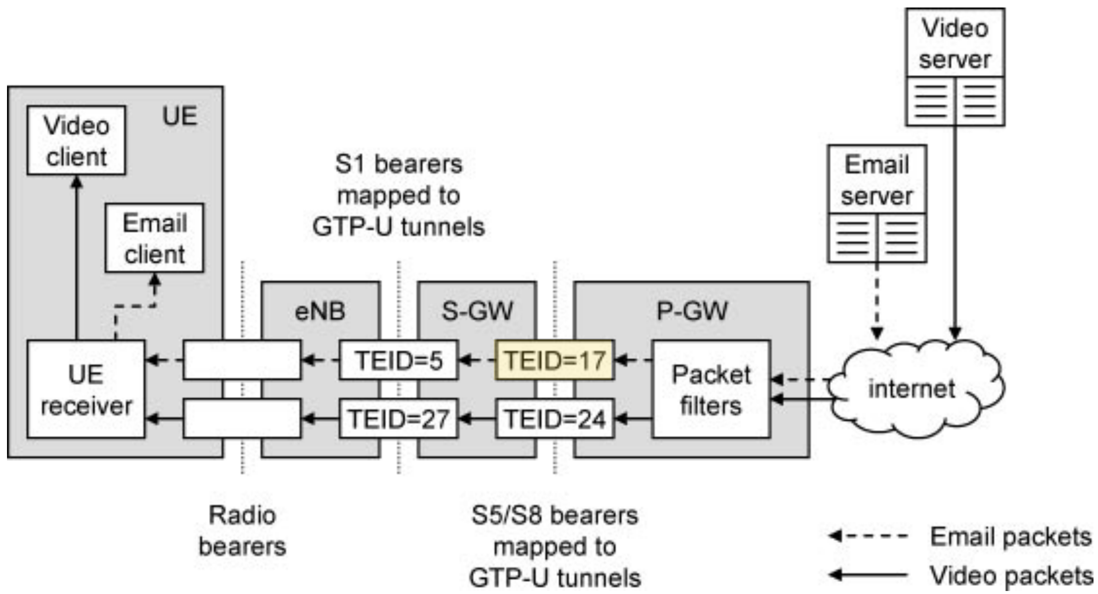
Figure 2.22 Implementation of tunneling in the downlink, when using an S5/S8 interface based on GTP.

- The P-GW now has to assign each incoming packet to the correct EPS bearer
  - ✓ Each EPS bearer is associated with a Traffic Flow Template (TFT)
  - ✓ This comprises a set of packet filters, one for each of the packet flows that make up the bearer
  - ✓ Each packet filter contains information
    - IP addresses of the source and destination devices
    - UDP or TCP port numbers of the source and destination applications

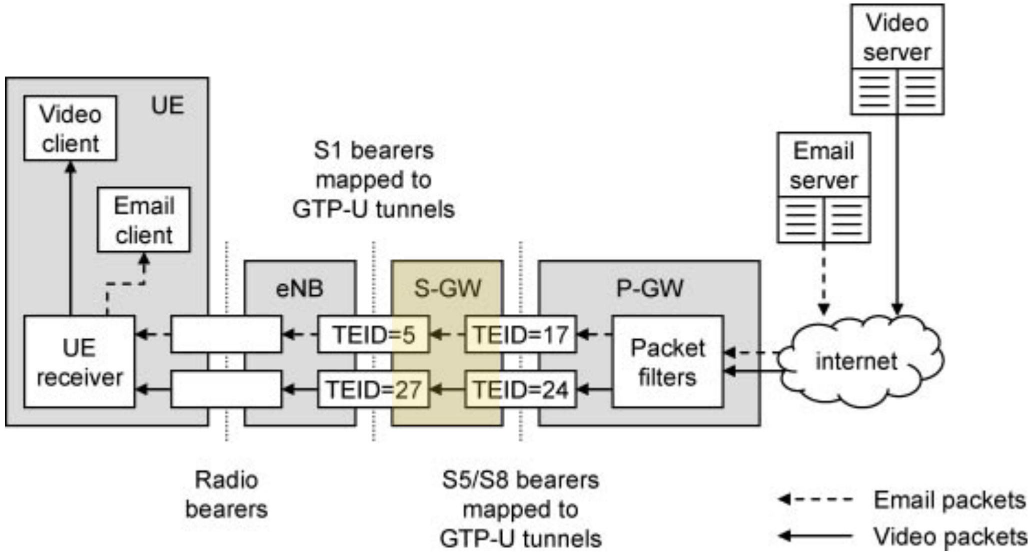


- ✓ P-GW assign every packet to the correct bearer by <u>inspecting</u> every <u>incoming packet</u> and <u>comparing</u> it with all the <u>packet filters</u> that have been installed

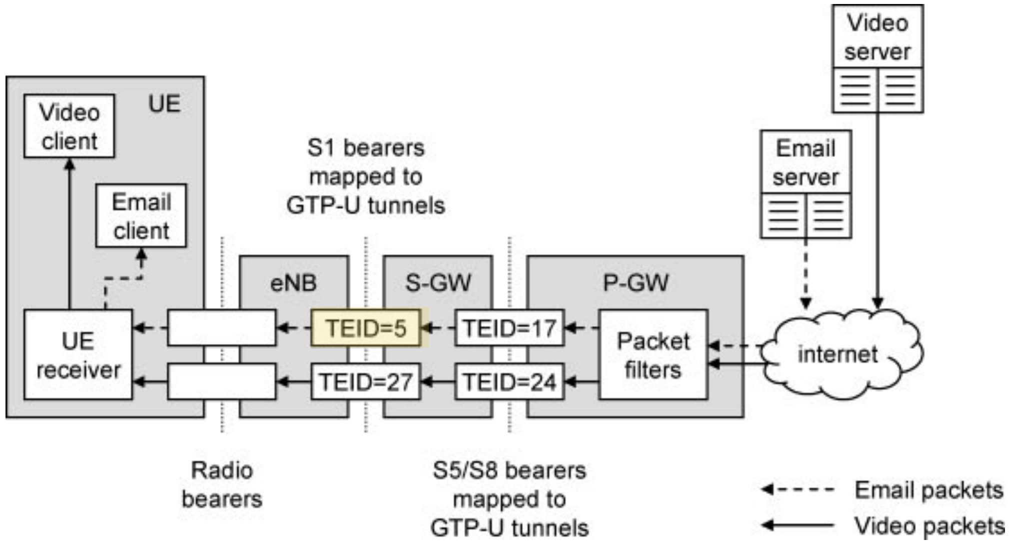
- ✓ P-GW now looks up the corresponding <u>GTP-U tunnel</u> and adds a <u>GTP-U header</u> that contains the <u>downlink TEID</u> (17 for email packets)



- It also looks up the mobile's <u>S-GW</u> and adds an <u>IP header</u> that contains the <u>S-GW's IP address</u>
- It can then forward the packet to the S-GW
- When the packet arrives, the S-GW opens the GTP-U header and reads its TEID



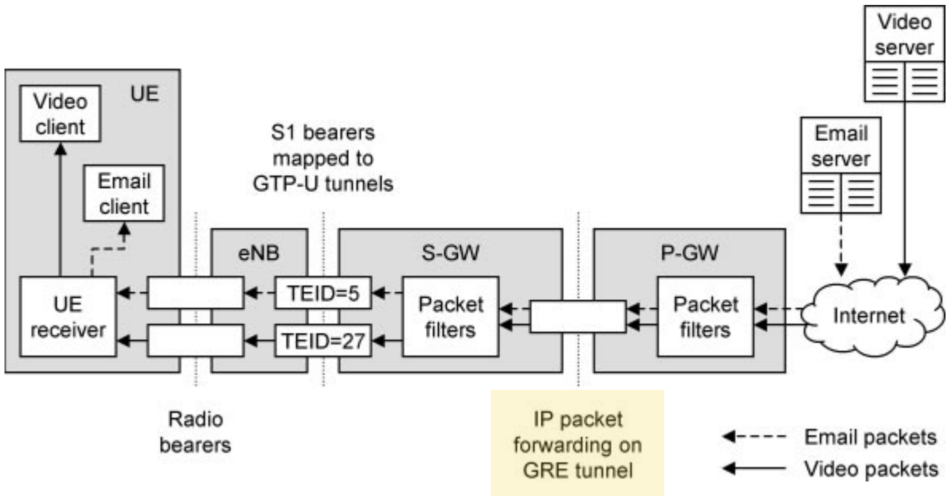
- ✓ It uses this information to identify the corresponding EPS bearer, and to look up the destination BS and the next TEID (5 for email in this example)
- ✓ It then forwards the packet to the BS
- ✓ The BS transmits the packet to the mobile
- ✓ A similar process happens in reverse on the uplink



2.4.3 Tunneling Using GRE and PMIP

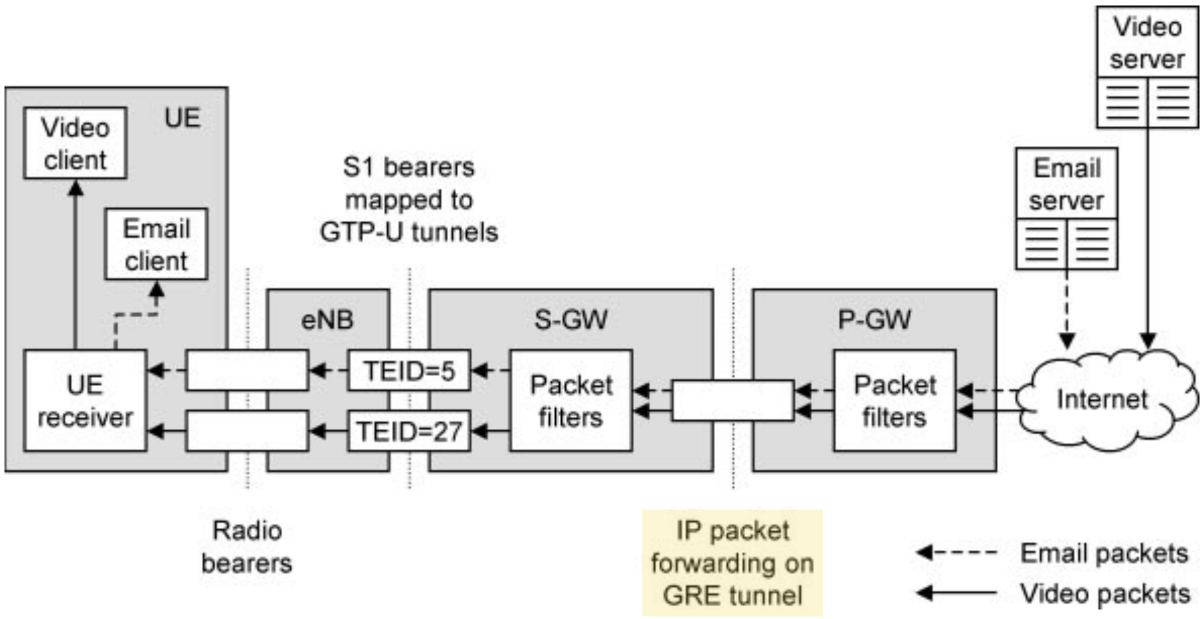
- The GRE protocol also uses tunnels, each of which is identified using a 32 bit key field in the GRE packet header

- Unlike GTP-C, PMIP does not include any mechanism to specify the QoS of a data stream



- GRE : Generic Routing Encapsulation
- PMIP : Proxy Mobile IPv6

- On the *S5/S8* interface, a mobile only has one GRE tunnel (Figure 2.23)
  - ✓ This handles all the data packets that the mobile is transmitting or receiving, without any QoS guarantees
  - ✓ P-GW still contains a set of packet filters, which it uses to direct incoming packets to the correct GRE tunnel, and hence to the correct mobile
  - ✓ The S-GW now contains packet filters as well, to handle one-to-many mapping from GRE tunnels to EPS bearers



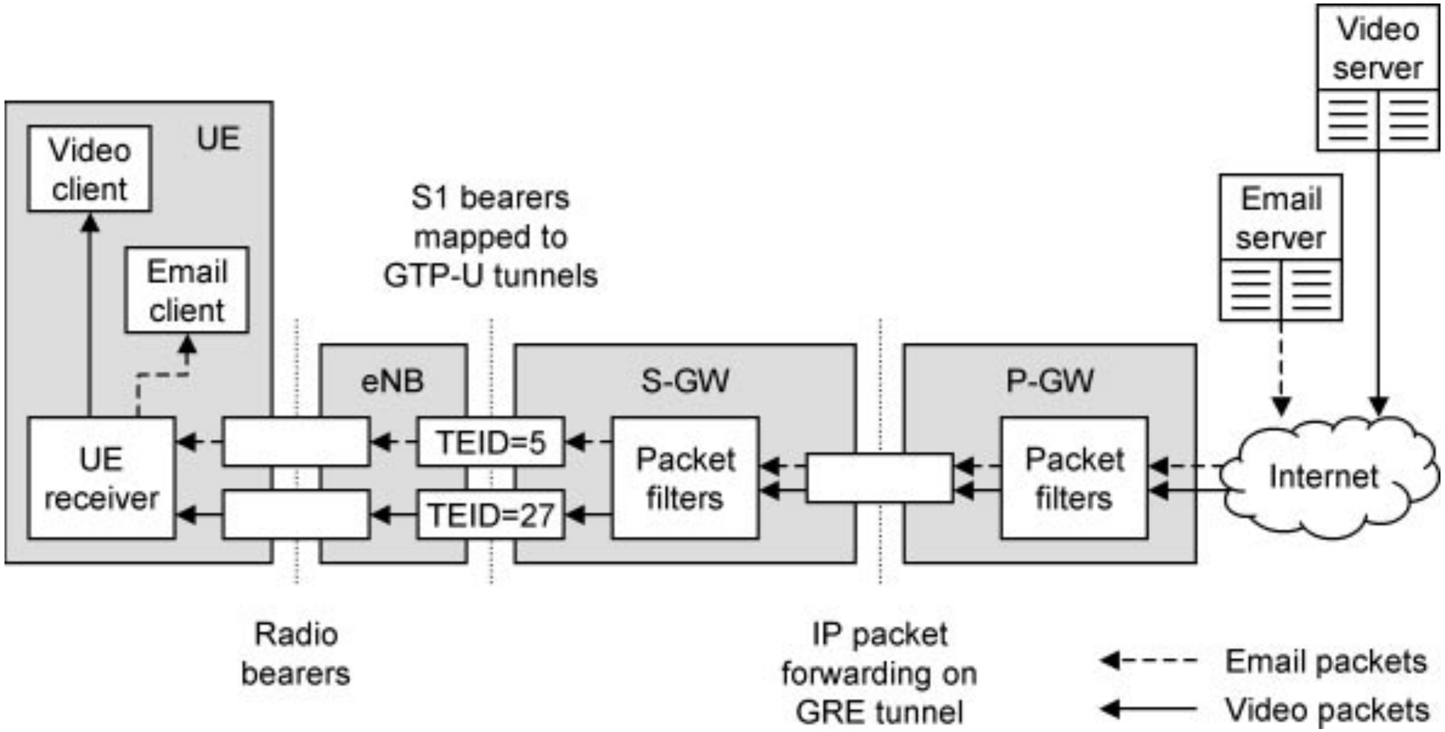


Figure 2.23 Implementation of tunneling in the downlink, when using an S5/S8 interface based on PMIP.

2.4.4 Signaling Radio Bearers

- LTE uses three special radio bearers, known as Signaling Radio Bearers (SRBs), to carry signaling messages between mobile and BS (Table 2.2)
- Each of the signaling radio bearers is associated with a specific configuration of the air interface protocols, so that the mobile and BS can agree on how the signaling messages should be transmitted and received

Signalling radio bearer	Configured by	Used by
SRB 0	System information	RRC messages before establishment of SRB 1
SRB 1	RRC message on SRB 0	Subsequent RRC messages
		NAS messages before establishment of SRB 2
SRB 2	RRC message on SRB 1	Subsequent NAS messages

Table 2.2 Signaling radio bearers

- SRB0
  - ✓ Only used for a few RRC signaling messages, which the mobile and BS use to establish communications in a procedure known as RRC connection establishment
  - ✓ Its configuration is defined in special RRC messages known as system information messages, which the BS broadcasts across the whole of the cell to tell the mobiles about how the cell is configured

Signalling radio bearer	Configured by	Used by
SRB 0	System information	RRC messages before establishment of SRB 1
SRB 1	RRC message on SRB 0	Subsequent RRC messages NAS messages before establishment of SRB 2
SRB 2	RRC message on SRB 1	Subsequent NAS messages

- SRB1
  - ✓ Configured using signaling messages that are exchanged on SRB0, at the time when a mobile establishes communications with the radio access network
  - ✓ Used for all subsequent RRC messages, and also transports a few EMM and ESM messages that are exchanged prior to the establishment of SRB2
- SRB2
  - ✓ Configured using signaling messages that are exchanged on SRB1, at the time when the mobile establishes communications with EPC
  - ✓ Used to transport all the remaining EMM and ESM messages

Signalling radio bearer	Configured by	Used by
SRB 0	System information	RRC messages before establishment of SRB 1
SRB 1	RRC message on SRB 0	Subsequent RRC messages NAS messages before establishment of SRB 2
SRB 2	RRC message on SRB 1	Subsequent NAS messages

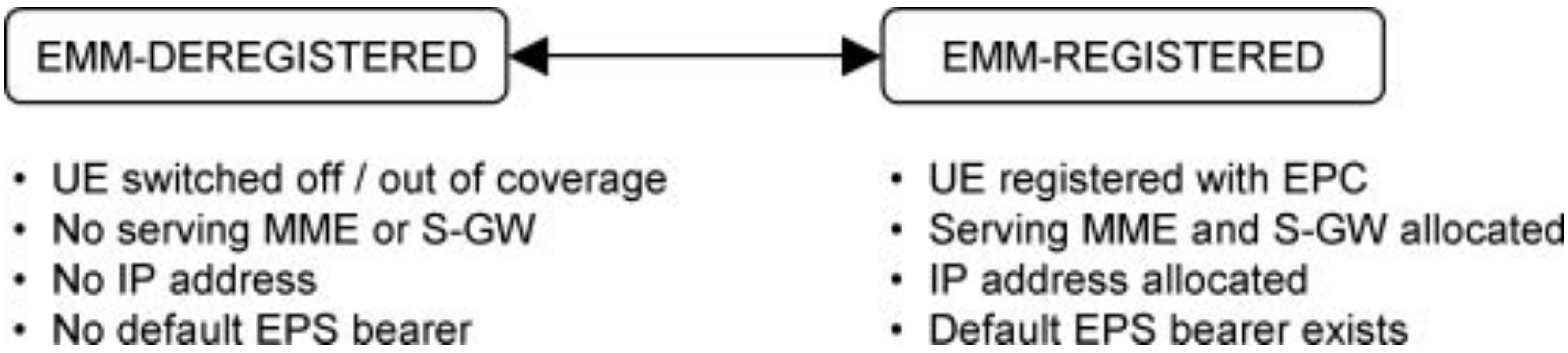
2.5 State Diagrams

- 2.5.1 EPS Mobility Management
- 2.5.2 EPS Connection Management
- 2.5.3 Radio Resource Control

- A mobile's behavior is defined using three state diagrams, which describe whether the mobile is registered with the EPC and whether it is active or idle
  - ✓ EPS Mobility Management (EMM) state diagram
  - ✓ EPS Connection management (ECM) state diagram
  - ✓ Radio Resource Control (RRC) state diagram

2.5.1 EPS Mobility Management

- EPS Mobility Management (EMM) state diagram
  - ✓ States are managed by EMM protocol in the mobile and the MME, and is shown in Figure 2.24



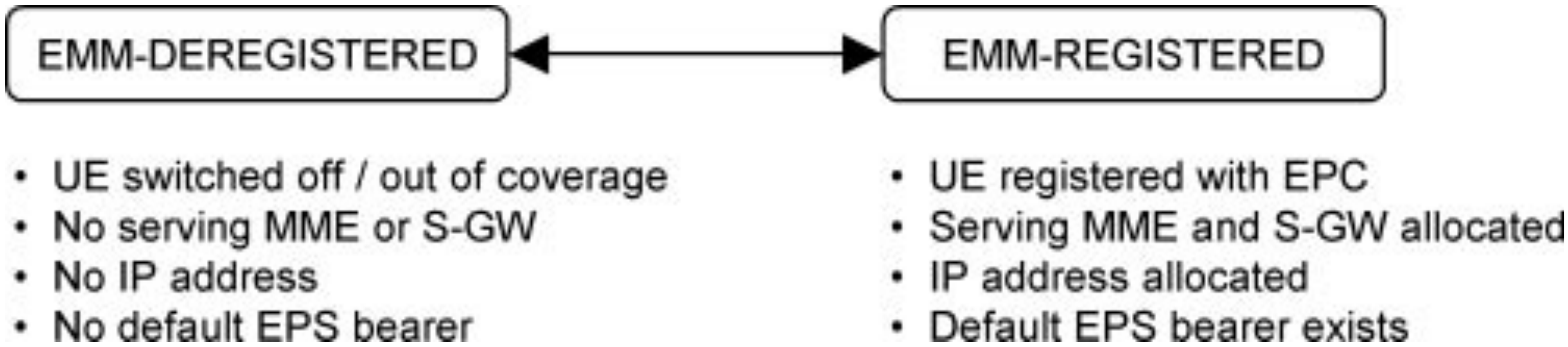
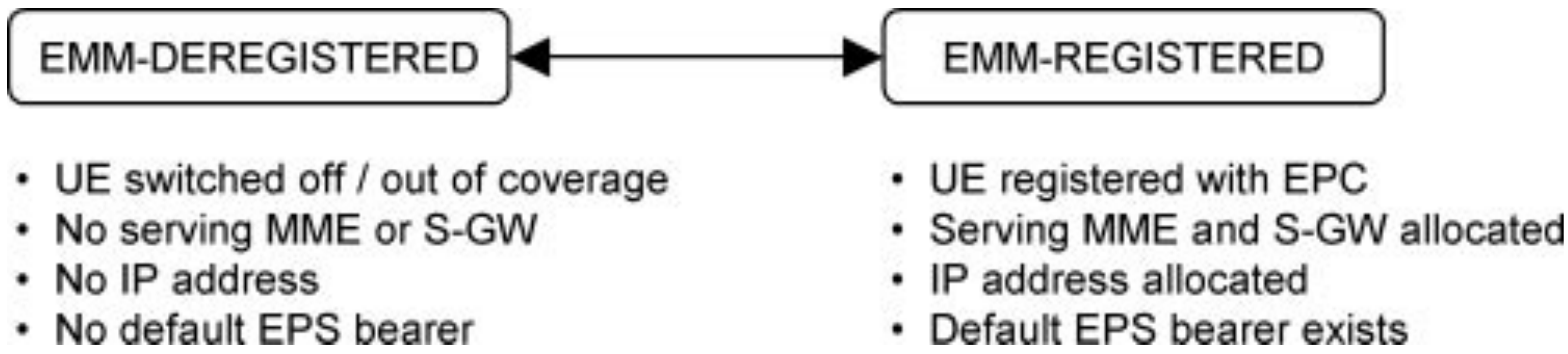


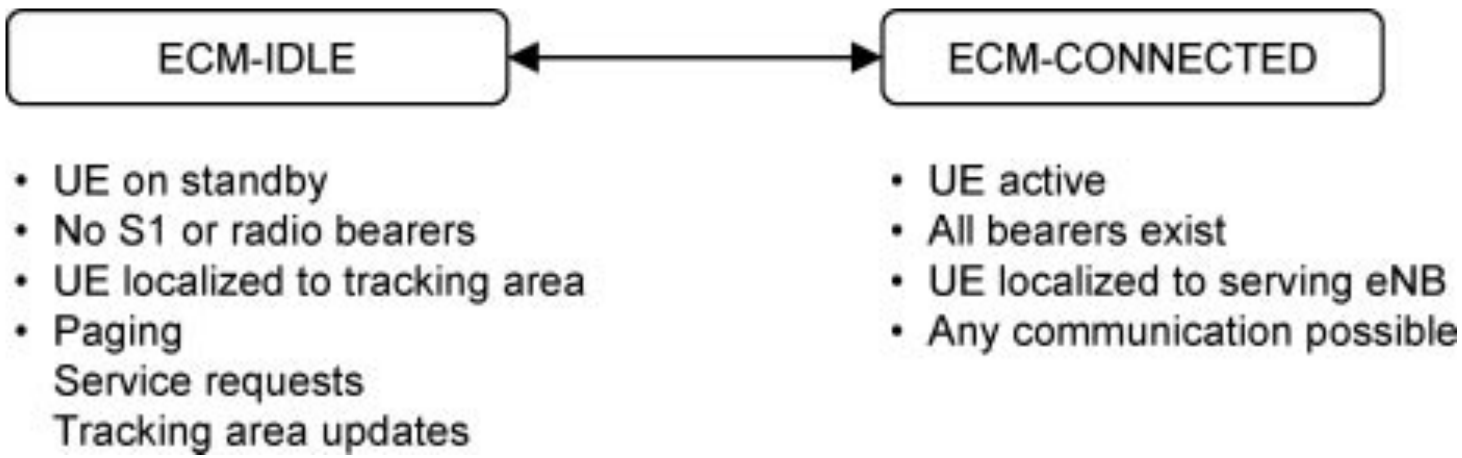
Figure 2.24 EPS mobility management (EMM) state diagram.

- The mobile's EMM state depends on whether it is registered with EPC
  - ✓ EMM-REGISTERED state
    - The mobile is switched on, and is registered with a serving MME and a S-GW
    - The mobile has an IP address and a default EPS bearer, which gives it always-on connectivity with a default PDN
  - ✓ EMM-DEREGISTERED state
    - The mobile is switched off or out of coverage and has none of these attributes

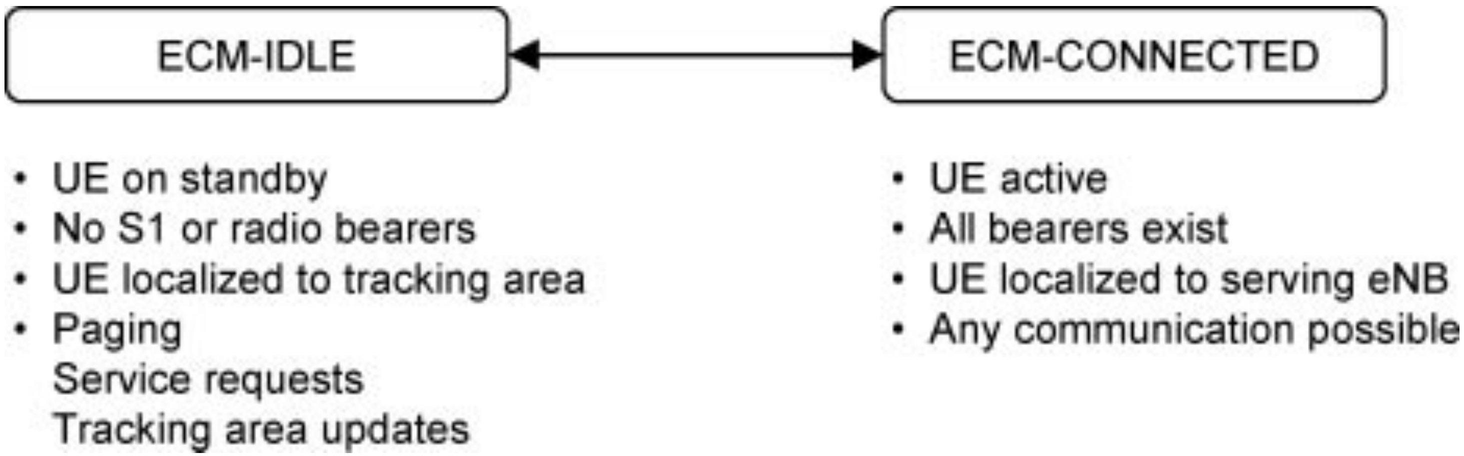


2.5.2 EPS Connection Management

- EPS Connection Management (ECM) state diagram (Figure 2.25)
  - ✓ States are managed by EMM protocol
  - ✓ Each state has two names
    - TS 23.401 calls them ECM-CONNECTED and ECM-IDLE (here use this name)
    - TS 24.301 calls them EMM-CONNECTED and EMM-IDLE



- The mobile's ECM state depends on whether it is active or standby, from the viewpoint of non access stratum protocols and EPC
  - ✓ An active mobile is in ECM-CONNECTED state
    - All the data bearers and signaling radio bearers are in place
    - Mobile can freely exchange signaling messages with MME through a logical connection that is known as a signaling connection
    - Mobile can freely exchange data with S-GW



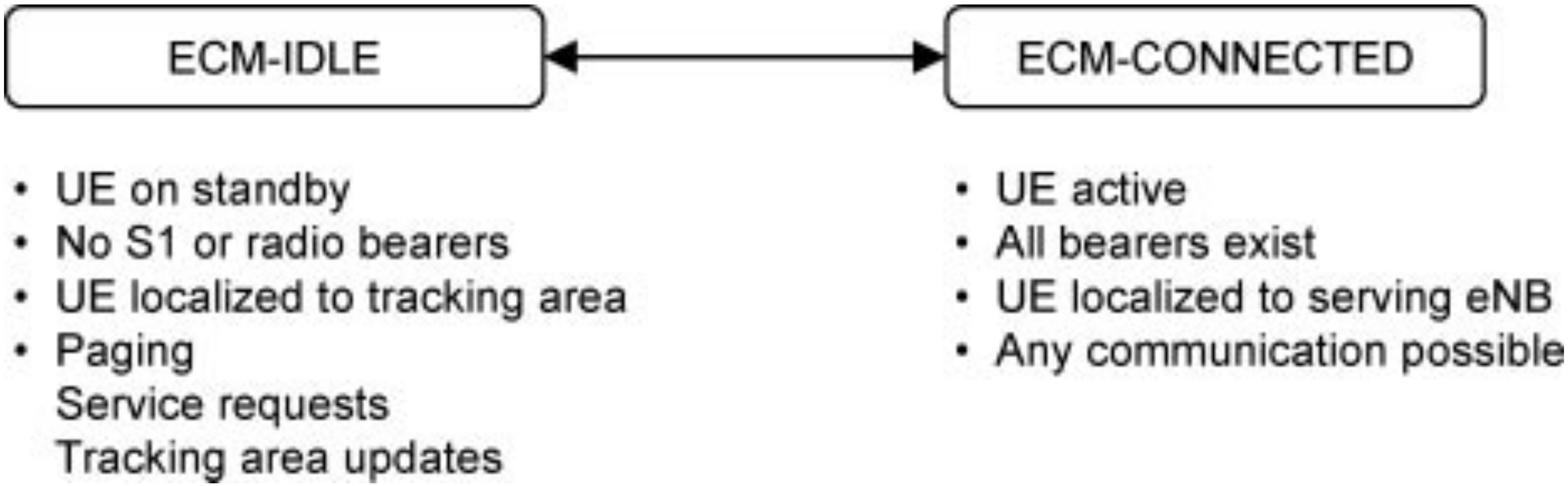
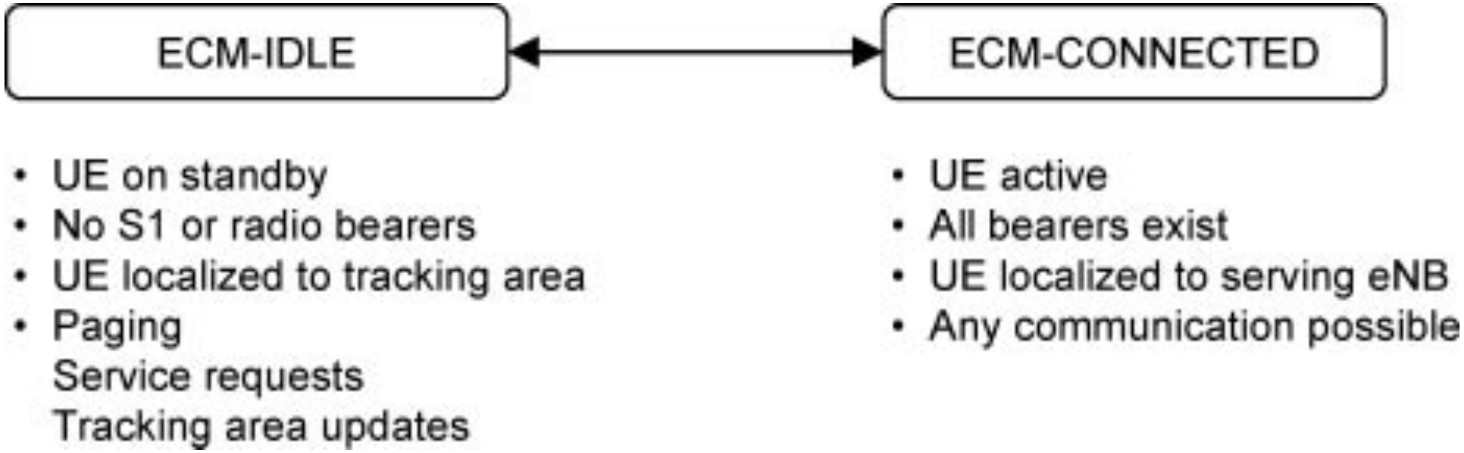
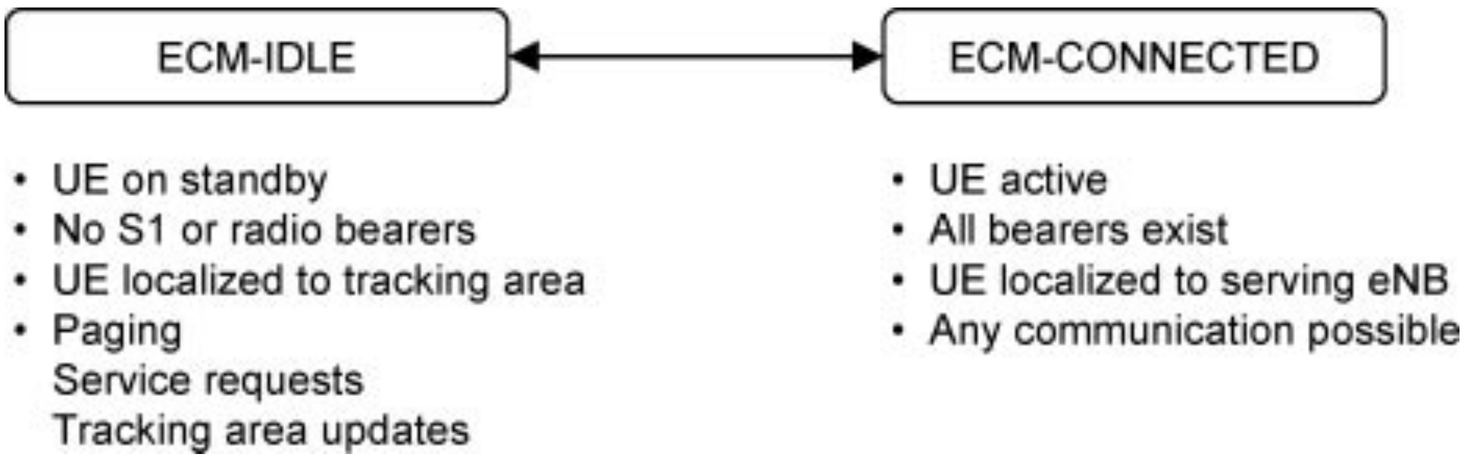


Figure 2.25 EPS connection management (ECM) state diagram.

- ✓ When on standby, a mobile is in ECM-IDLE state
  - Inappropriate to keep all the bearers in place
  - To avoid the resulting signaling overhead, the network tears down a mobile's *S1* bearers and radio bearers whenever the mobile enters ECM-IDLE
  - The mobile can then freely move from one cell to another, without the need to re-route the bearers every time



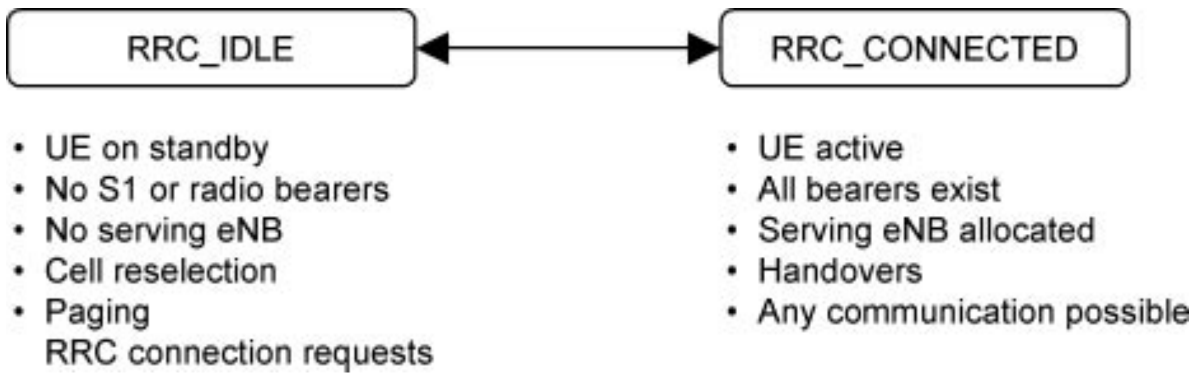
- MME does not know exactly where an idle mobile is located; instead, it just knows which tracking area the mobile is in
- This allows the mobile to move from one cell to another without notifying the MME; instead, it only does so if it crosses a tracking area boundary
- The MME can also register a mobile in more than one tracking area and can tell the mobile to send a notification only if it moves outside those tracking areas



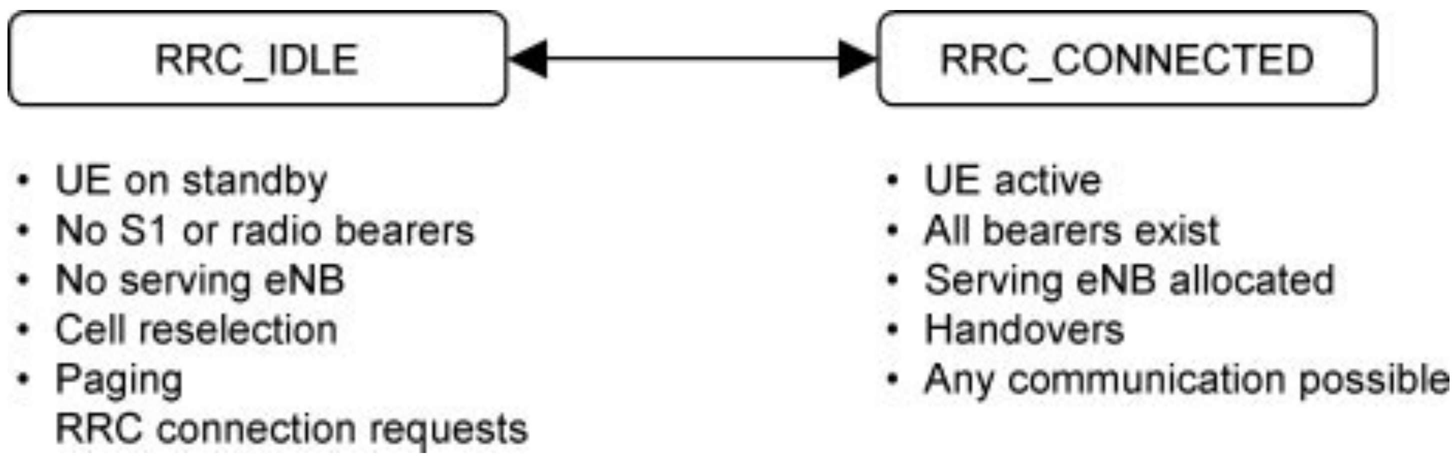
- If the MME wishes to contact an idle mobile, then it can do so by sending an *S1-AP* Paging message to all the BSs in the mobile's tracking area(s)
  - The BSs react by transmitting an RRC Paging message
- If the mobile wishes to contact the network or reply to a paging message, then it sends the MME an EMM message called a Service Request and the MME reacts by moving the mobile into ECM-CONNECTED
- Finally, the mobile can send an EMM Tracking Area Update Request to the MME, if it notices that it has moved into a tracking area in which it is not currently registered

2.5.3 Radio Resource Control

- Radio Resource Control (RRC) state diagram (Figure 2.26)
  - ✓ States are managed by RRC protocol in the mobile and the serving eNB
  - ✓ The mobile's RRC state depends on whether it is active or idle, from the viewpoint of access stratum protocols and the E-UTRAN



- ✓ An active mobile is in RRC_CONNECTED state
  - The mobile is assigned to a serving eNB, and can freely communicate with it using signaling messages on SRB 1



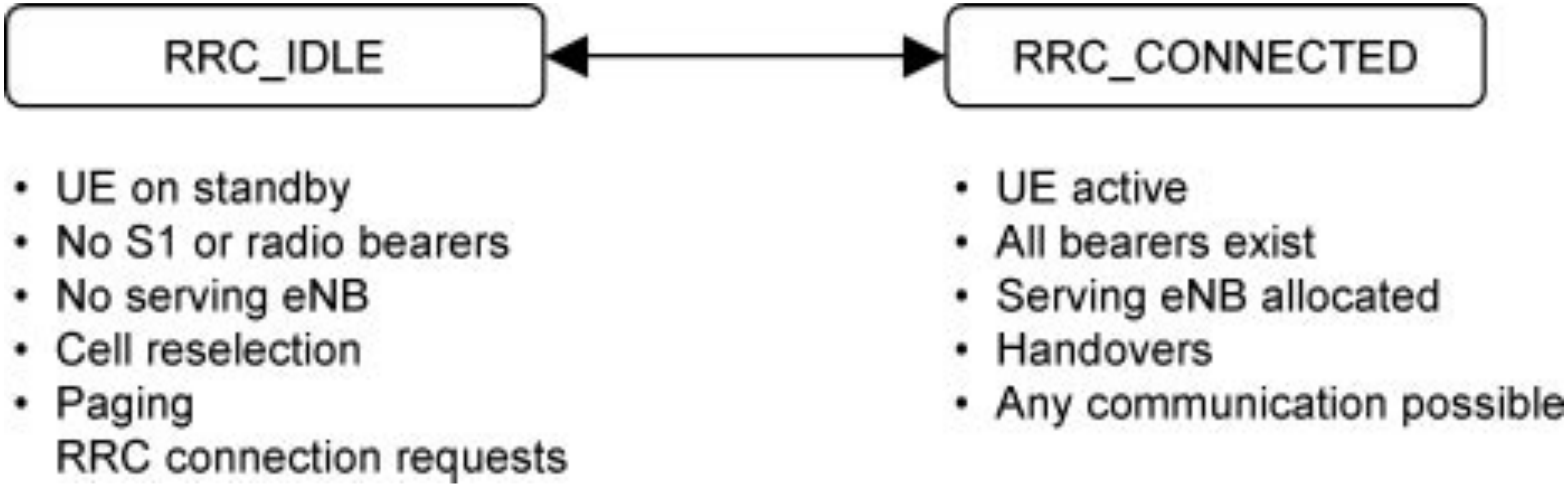
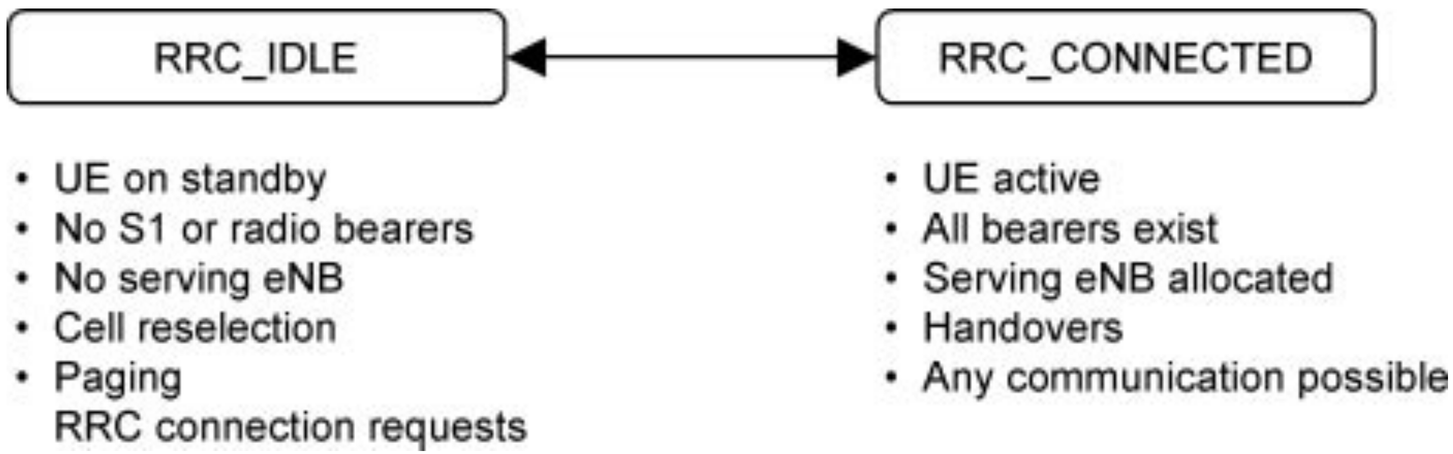


Figure 2.26 Radio resource control (RRC) state diagram.

✓ When on standby, a mobile is in RRC_IDLE

- SRB 1 is torn down, and there is no serving eNB assigned
- If the radio access network wishes to contact the mobile, typically because it has received a paging request from EPC, then it can do so using an RRC paging message
- If the mobile wishes to contact the radio access network or reply to a paging message, then it can do so by initiating the RRC connection establishment procedure
- In turn, the BS reacts by moving the mobile into RRC_CONNECTED



- The two RRC states handle moving devices in different ways
  - ✓ A mobile in RRC_ CONNECTED state
    - Can be transmitting and receiving at a high data rate
    - It is important for the radio access network to control which cell the mobile is communicating with
    - It does this using handover, in which the network switches the mobile's communication path from one cell to another
    - If the old and new cells are controlled by different BSs, then the network also re-routes the mobile's S1-U and S1-MME interfaces, so that they run directly between the new BS and the EPC
    - In addition, the network will
      - change the mobile's S-GW and S5/S8 interface(s) if it moves into a new S-GW service area
      - change the mobile's serving MME if it moves into a new MME pool area

- A mobile in RRC_IDLE state
  - Main motivation is to reduce signaling
  - The mobile decides which cell it will listen to, using cell reselection
  - The radio access network remains completely unaware of its location, while the EPC is only informed if a tracking area update is required
  - The tracking area update may lead to a change of S-GW or serving MME
- The ECM and RRC state diagrams are always used together
  - An active mobile is always in ECM-CONNECTED and RRC_CONNECTED
  - A mobile on standby is always in ECM-IDLE and RRC_IDLE

2.6 Spectrum Allocation

- The 3GPP specifications allow mobiles and BSs to use a large number of frequency bands
- Table 2.3 lists the bands that support Frequency Division Duplex (FDD) mode
- Table 2.4 lists the bands that support Time Division Duplex (TDD)
- The tables also show the first release in which each band was introduced
- Most of the bands are also supported by other systems such as UMTS and GSM

Band	Release	Uplink band (MHz)	Downlink band (MHz)	Main regions	Notes
1	R99	1920–1980	2110–2170	Europe, Asia, Africa	WCDMA
2	R99	1850–1910	1930–1990	Americas	GSM 1900, CDMA
3	R5	1710–1785	1805–1880	Europe, Asia, Africa	GSM 1800
4	R6	1710–1755	2110–2155	Americas	
5	R6	824–849	869–894	Americas	GSM 850, CDMA
6	–	–	–	–	Not used by LTE
7	R7	2500–2570	2620–2690	Europe	
8	R7	880–915	925–960	Europe, Asia, Africa	GSM 900
9	R7	1749.9–1784.9	1844.9–1879.9	Japan	
10	R7	1710–1770	2110–2170	Americas	
11	R8	1427.9–1447.9	1475.9–1495.9	Japan	
12	R8	699–716	729–746	USA	Digital dividend
13	R8	777–787	746–756	USA	Digital dividend
14	R8	788–798	758–768	USA	Digital dividend
15	–	–	–	–	Not used by 3GPP
16	–	–	–	–	Not used by 3GPP
17	R8	704–716	734–746	USA	Digital dividend
18	R9	815–830	860–875	Japan	
19	R9	830–845	875–890	Japan	
20	R9	832–862	791–821	Europe	Digital dividend
21	R9	1447.9–1462.9	1495.9–1510.9	Japan	
22	R10	3410–3490	3510–3590	Europe	
23	R10	2000–2020	2180–2200	North America	
24	R10	1626.5–1660.5	1525–1559	North America	
25	R10	1850–1915	1930–1995	Americas	

Table 2.3 FDD frequency bands. Reproduced by permission of ETSI

Band	Release	Frequency band (MHz)	Main regions
33	R99	1900–1920	Europe, Asia
34	R99	2010–2025	Europe, Asia
35	R99	1850–1910	Americas
36	R99	1930–1990	Americas
37	R99	1910–1930	Americas
38	R7	2570–2620	Europe
39	R8	1880–1920	China
40	R8	2300–2400	China
41	R10	2496–2690	USA
42	R10	3400–3600	Europe
43	R10	3600–3800	Europe

Table 2.4 TDD frequency bands. Reproduced by permission of ETSI

- Some of these frequency bands are being newly released for use by mobile telecommunications.
    - ✓ In 2008, the US Federal Communications Commission (FCC) auctioned frequencies around 700MHz (FDD bands 12, 13, 14 and 17) that had previously been used for analogue television broadcasting
    - ✓ In Europe, similar auctions have been taking place for frequencies around 800 and 2600MHz (FDD bands 7 and 20, and TDD band 38)
- Network operators can also re-allocate frequencies that they have previously used for other mobile communication systems, as their users migrate to LTE
    - ✓ FDD bands 1, 3 and 8 in Europe (originally used by WCDMA, GSM 1800 and GSM 900 respectively)
    - ✓ FDD bands 2, 4 and 5 in the USA
- The result is that LTE is likely to be deployed in a large number of frequency bands, with different bands used by different regions, countries and network operators