Chapter 1

The EPS Network

COPYRIGHTED MATERIAL

1.1. Architecture

The 4th-generation mobile network EPS (Evolved Packet System) comprises a core network EPC (Evolved Packet Core) and an access network E-UTRAN (Evolved Universal Terrestrial Radio Access Network) (Figure 1.1).

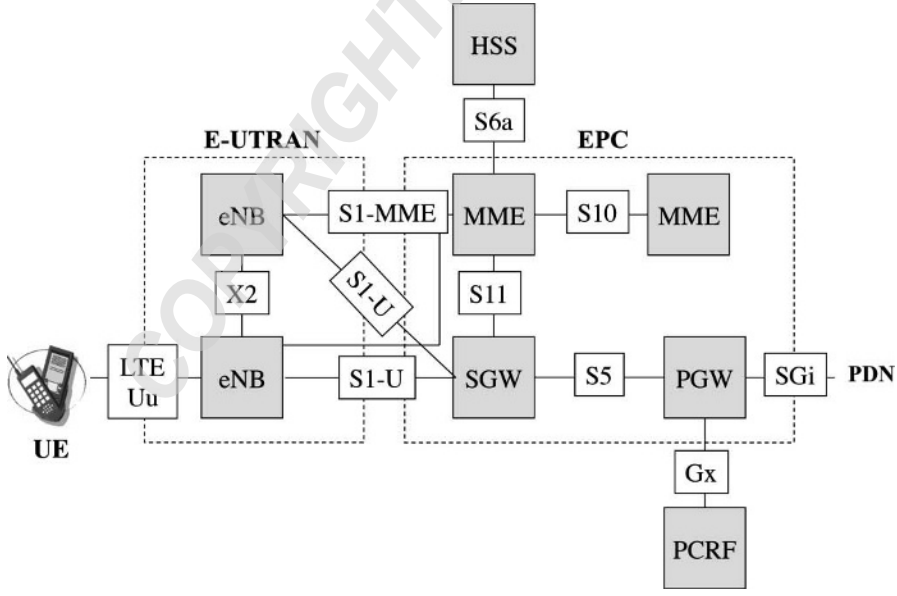


Figure 1.1. *Architecture of the EPS network*

The access network E-UTRAN takes care of connection of mobiles. The EPC core network interconnects the access network and provides the interface for the PDN (Packet Data Network). It ensures the attachment of mobiles to the network and the establishment of the bearers.

The term SAE (System Architecture Evolution) is used for the study of the evolution of the core network EPC.

The term LTE (Long Term Evolution) is attributed to the study of the evolution of the radioelectric interface Uu between the EPS and the mobile UE (User Equipment).

1.1.1. *Access network*

The access network E-UTRAN includes only one type of entity, the radioelectric station eNB (evolved Node B) to which the UE connects (Figure 1.1).

The eNB is responsible for managing radioelectric resources, the allocation of bearers to the mobile and the mobility of the UE.

The eNB transfers the traffic data from the mobile (or respectively the SGW (Serving Gateway) of the EPC) to the SGW (or respectively the mobile). When the eNB receives data from the UE or from the SGW, it examines the QCI (QoS Class Identifier) to implement the packet scheduling mechanism.

For outgoing data destined for the SGW, the eNB performs DSCP (DiffServ Code Point) marking of the IP (Internet Protocol) packets in relation with the QCI assigned to each packet.

The eNB compresses and encrypts the data traffic on the radioelectric interface.

The eNB encrypts and controls the integrity of the signaling data exchanged with the mobile.

The eNB selects the MME (Mobility Management Entity) in the EPC to which the mobile will be attached.

The eNB processes the paging request sent by the MME for broadcast into the cell. The cell is the area of the eNB's radioelectric coverage.

The eNB also broadcasts the data relating to the characteristics of the radioelectric interface into the cell, which the mobile uses to connect.

The eNB uses the measurements carried out by the mobile to make a decision on whether, or not, to trigger a handover and for scheduling the data packets exchanged with the mobile.

The eNB has the following interfaces (Figure 1.1):

– LTE-Uu with the mobile UE. This interface is used to connect the mobile to the eNB. It carries traffic from the mobile and the signaling exchanged between the mobile and the eNB. This signaling supports the signaling exchanged between the mobile and the MME of the EPC.

– X2 with the other eNBs. This interface is used for intra-E-UTRAN handover and for exchanging cell load information. It carries mobile traffic and the signaling exchanged between two eNBs.

– S1-MME with the MME of the EPC. This interface is used for activating the radioelectric bearer, for paging and for mobility management. It carries the signaling exchanged between the MME and the eNB. This signaling carries the signaling exchanged between the mobile and the MME.

– S1-U with the SGW of the EPC. This interface only carries the mobile traffic.

1.1.2. *Core network*

The EPC is made up of the MMEs only performing processing of the signaling from the EPS, and the SGW and PGW (PDN Gateway), which handle the transfer of the traffic data (Figure 1.1).

1.1.2.1. *The MME*

The MME is the control tower of the EPS. It grants mobiles access to the EPS and controls the establishment of bearers for transmission of the traffic data.

The MMEs belong to a pool. The load balancing of the MMEs is managed by the eNBs which need access to each of the MMEs in the same pool.

Each MME is identified by the parameters MMEGI (MME Group Identity) and MMEC (MME Code), which together make up the MMEI (MME Identity).

The MME is responsible for attachment and detachment of the mobile.

When an attachment is established, the MME retrieves the profile and authentication data for the mobile stored on the HSS (Home Subscriber Server), and authenticates the mobile. The HSS is a database which can be shared between the

different generations of mobile networks and the IMS (IP Multimedia Sub-system) network.

When an attachment is established, the MME registers the TAI (Tracking Area Identity) of the mobile and assigns the UE a GUTI (Globally Unique Temporary Identity).

The TAI comprises the following fields:

– MCC (Mobile Country Code);

– MNC (Mobile Network Code);

– TAC (Tracking Area Code).

The GUTI comprises the following fields:

– MCC;

– MNC;

– the MMEI of the MME to which the mobile is attached;

– the M-TMSI (MME – Temporary Mobile Subscriber Identity) assigned to the mobile by the MME.

The S-TMSI (Shortened-TMSI) is composed by combining the M-TMSI and the MMEC of the MME. The MME uses the S-TMSI for paging.

The MME manages a list of the TAIs allocated to mobiles, within which the mobile, in idle mode, can move without contacting the MME to update its tracking area.

When a mobile attaches, the MME selects the SGW and PGW to form the default bearer. The default bearer is formed when an attachment is established by the mobile (e.g. for the bearer of telephone signaling).

The MME also processes the mobile request for the establishment, modification and release of a dedicated bearer for the transmission of traffic data. The dedicated bearer is constructed on request from the mobile for a particular service (for instance, for voice data transmission).

For the construction of the bearer, the selection of the PGW is carried out on the basis of the APN (Access Point Name) communicated by the mobile or by the HSS in the subscriber's profile.

The MME also selects the target MME in the case of the handover of the mobile from one pool to another.

The MME provides the data required for legal interceptions, such as the state of the mobile (idle or connected), its TAI and the characteristics of the traffic.

The MME has the following interfaces (Figure 1.1):

– S1-MME with the eNB;

– S6a with the HSS. This interface carries the signaling in order to access the mobile data (authentication, service profile);

– S10 with the MME. This interface carries the signaling exchanged when the UE moves and necessitates a switch of MME;

– S11 with the SGW. This interface carries the signaling allowing the establishment of the bearer between the eNBs and the SGW.

1.1.2.2. *The SGW*

SGWs are also organized in pools. To balance the load of the SGWs, all the eNBs in an area must have access to all of the SGWs in the same pool.

The SGW transfers the incoming data from the PGW to the eNB and the outgoing data from the eNB to the PGW. When the SGW receives data from the eNBs or PGWs, it examines the QCI in order to implement the packet scheduling mechanism.

For the incoming and outgoing data, the SGW performs DSCP marking of the IP packets on the basis of their assigned QCI.

The SGW orders the traffic data when an inter E-UTRAN handover occurs.

The SGW is the anchor point for intra-system handover (within the 4G network), provided the mobile does not change pool. Otherwise, it is the PGW that performs this function.

The SGW is the anchor point for inter-system handover in PS mode, necessitating the transfer of traffic from the mobile to a 2G or 3G mobile network.

The SGW initiates notification to the MME for incoming data when the mobile is in idle mode. A mobile in idle mode remains attached to the MME. However, it is no longer connected to the eNB, so the bearers are released.

The SGW has the following interfaces (Figure 1.1):

– S11 with the MME;

– S5 with the PGW. This interface is used to establish a bearer between these two entities. It carries the signaling exchanged with the PGW and the mobile traffic;

– S1-U with the eNB.

1.1.2.3. *The PGW*

The PGW is the gateway router connecting the EPS to the PDN (i.e. the Internet network).

When the PGW receives data from the SGW or from the PDN, it uses the QCI to implement the packet-scheduling mechanism.

The PGW performs DSCP marking of the IP packets on the basis of their assigned QCI.

When an attachment is established, the PGW assigns a IPv4 or IPv6 address to the mobile.

The PGW is the anchor point for inter-SGW switch.

The PGW contains the PCEF (Policy and Charging Enforcement Function), which applies the rules relating to mobile traffic, packet filtering, charging and the QoS to be applied to the bearer being constructed. The PCRF (Policy Charging and Rules Function), outside of the EPS, tells the PCEF of the PGW which rules need to be applied.

The PGW generates data enabling charging entities to edit the charging records which are dealt with by the billing system.

The PGW diverts the traffic from the mobile in the case of legal interceptions.

The PGW has the following interfaces (Figure 1.1):

– S5 with the PGW;

– Gx with the PCRF. This interface carries the signaling enabling the PGW to receive the rules to be applied to the mobile traffic;

– SGi with the PDN. This interface carries the mobile traffic (IP packet).

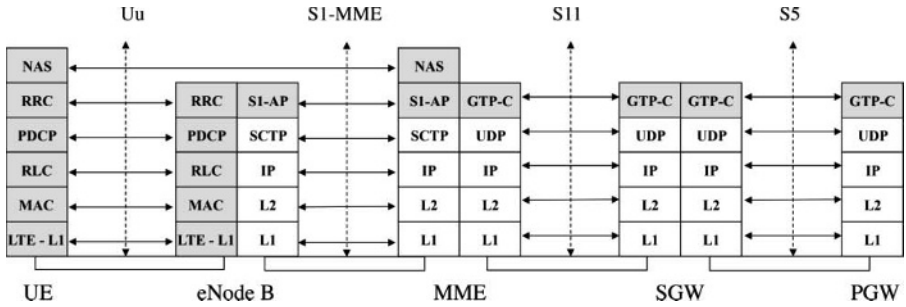
1.1.3. *Protocol architecture*

The LTE-Uu interface is the reference point between the mobile and the eNB for the signaling and traffic. RRC (Radio Resource Control) signaling is exchanged between the mobile and the eNB. The RRC protocol also deals with the transport of the NAS (Non Access Stratum) protocol exchanged between the mobile and the MME (Figure 1.2).

The S1-MME interface is the reference point between the MME and eNB for signaling using the S1-AP (Application Part) protocol. S1-AP also deals with the transport of the NAS protocol exchanged between the mobile and the MME (Figure 1.2).

The S11 interface is the reference point between the MME and SGW for signaling using the GTP-C [GPRS (General Packet Radio Service) Tunnel Protocol Control] protocol (Figure 1.2).

The S1-U interface is the reference point between the eNB and SGW for tunneling of the traffic (the IP packet) via the GTP-U (GPRS Tunnel Protocol User) protocol (Figure 1.3).

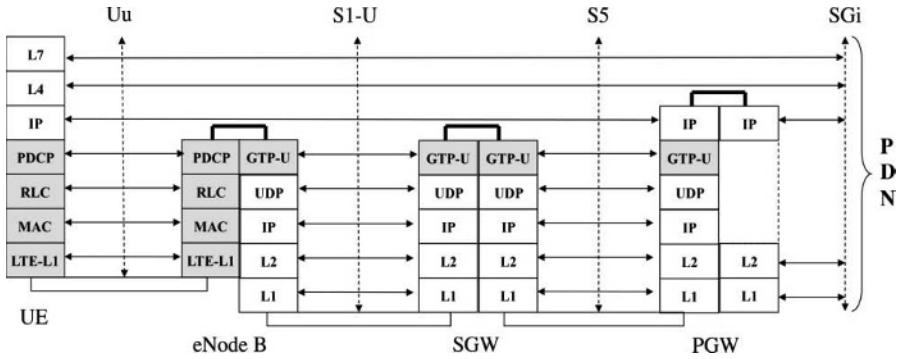


The shaded blocks are described in this book.
L2 (Layer 2): data link layer
L1 (Layer 1): physical layer

Figure 1.2. *Protocol architecture – the control plane*

The S5 interface is the reference point between the SGW and PGW for tunneling the traffic (the IP packet) via the GTP-U protocol (Figure 1.3) and for signaling via the GTP-C protocol (Figure 1.2).

The S10 interface is the reference point between the MMEs for signaling using GTP-C (Figure 1.1).



The shaded blocks are described in this book.
L7 (Layer 7): application layer
L4 (Layer 4): transport layer

Figure 1.3. *Protocol architecture – the traffic plane*

The SGi interface is the reference point between the PDW and the PDN (Figure 1.3).

The EPS transports mobile traffic (an IP packet) transparently to the PGW, which routes that packet. To perform this function, the network entities create bearers:

– the LTE-Uu Bearer (Radio Bearer). The eNB takes care of the construction of this bearer using RRC signaling exchanged with the mobile;

– the S1-U Bearer is identified by the TEID (Tunnel Endpoint Identifier), carried by the GTP-U protocol. The MME constructs this bearer using S1-AP signaling exchanged with the eNB and GTP-C exchanged with the SGW;

– the S5 Bearer is identified by the TEID carried by GTP-U. The SGW constructs this bearer using GTP-C signaling exchanged with the PGW. The identity of the PGW is communicated to the SGW by the MME.

To transfer the traffic data, the entities in the EPS network use a lookup table between the bearer IDs. In fact, the EPS constructs a virtual circuit (EPS Bearer) between the mobile and the PGW. Each EPS Bearer is attributed a QCI value.

The combination of the Radio Bearer and S1-U Bearer constitutes the E-RAB (EPS Radio Access Bearer).

Transport of the mobile traffic and the signaling between the entities in the EPS is taken care of by an IP network for which the entities in the EPS represent hosts.

At the LTE-Uu radioelectric interface, the signaling and the traffic from the mobile are borne by a data link layer and a physical layer.[1]

The data link layer is structured into three sub-layers:

– PDCP (Packet Data Convergence Protocol). This protocol takes care of the compression of the traffic data, the encryption of the traffic and signaling data, the control of the integrity of the signaling data and the scheduling of the traffic data when an intra-system handover occurs;

– RLC (Radio Link Control). This implements the retransmission mechanism in the case of error ARQ (Automatic Repeat reQuest), and concatenates or segments the PDCP data;

– MAC (Media Access Control). This protocol performs the multiplexing of the RLC data, implements the HARQ (Hybrid ARQ) mechanism in the case of error and schedules the downlink and uplink data.

The physical layer determines the characteristics of transmission over the LTE-Uu radioelectric interface (Table 1.1).

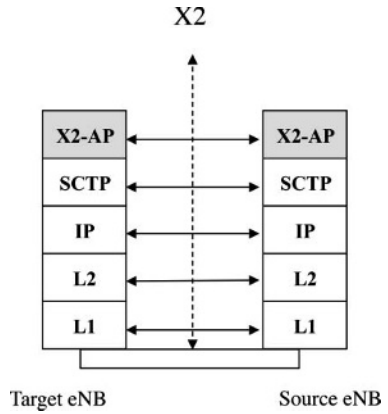
Frequency bandwidth	1.4 MHz, 3, 5, 10, 15, 20 MHz
Principle of duplex between both transmission directions	TDD or FDD
Modulation of sub-carriers	Downstream: QPSK, 16-QAM, 64-QAM Upstream: QPSK, 16-QAM, 64-QAM (for a particular category of mobile)
Principle of multiplexing of sub-carriers	Downstream: OFDM Upstream: DFTS-OFDM
Antenna system	MISO, MIMO
Maximum throughput	Downstream: 300 Mbit/s (Note 1) Upstream: 75 Mbit/s (Note 2)
Multiple access	Random attribution of resource blocks: 0.5 ms time and 180 kHz frequency

TDD: Time Division Duplex
FDD: Frequency Division Duplex
QPSK: Quadrature Phase-Shift Keying
QAM: Quadrature Amplitude Modulation
OFDM: Orthogonal Frequency-Division Multiplexing
DFTS: Discrete Fourier Transform Spread
MISO: Multiple Input Single Output
MIMO: Multiple Input Multiple Output
Note 1: the maximum throughput is obtained for a bandwidth of 20 MHz, 64-QAM modulation and a 4×4 MIMO antenna system.
Note 2: the maximum throughput is obtained for a bandwidth of 20 MHz and 64-QAM modulation.

Table 1.1. *Characteristics of the physical layer of the LTE-Uu interface*

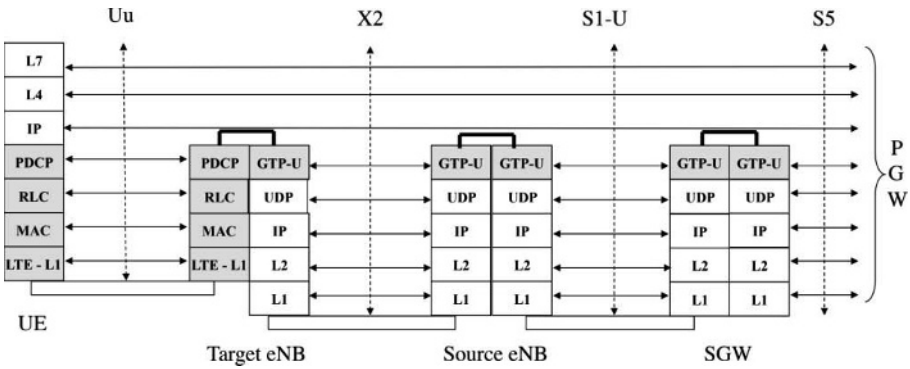
1 A detailed description of the data link layer and the physical layer is given in Chapter 2, on the LTE interface.

The X2 interface is the reference point between two eNBs for signaling using the X2-AP protocol (Figure 1.4) and for tunneling of the mobile traffic (the IP packet) via the GTP-U protocol, during a handover of the mobile (Figure 1.5).



The shaded blocks are described in this book.

Figure 1.4. *Protocol architecture over the X2 interface – the control plane*



The shaded blocks are described in this book.

Figure 1.5. *Protocol architecture – the traffic plane during handover based on the X2 interface*

The tunnel established between the two eNBs is unidirectional (source eNB to target eNB). It is used to transfer the data traffic received from the SGW to the target eNB. It is established temporarily, while the handover of the mobile takes place.

The S6a interface is the point of interface between the MME and HSS for signaling via the protocol DIAMETER, facilitating access to the mobile data (authentication, service profile) (Figure 1.1).

The Gx interface is the reference point between the PCRF and PGW for signaling via DIAMETER with regard to transfer of filtering-, QoS- and charging-rules (Figure 1.1).

1.2. Signaling protocols

1.2.1. *NAS protocol*

The NAS protocol is the signaling exchanged between the mobile and the MME. It is transported by the RRC protocol over the radioelectric interface LTE-Uu and by the S1-AP protocol over the S1-MME interface (Figure 1.2). It comprises the following two protocols:

– EMM (EPS Mobility Management). This takes care of controlling mobility and security;

– ESM (EPS Session Management). This controls the bearer establishment.

From the point of view of the MME, the mobile can be in one of two operational states: EMM-REGISTERED or EMM-DEREGISTERED.

In the EMM-DEREGISTERED state, the mobile's location is not known to the MME and, therefore, it cannot be contacted. The switch to the registered state takes place when the mobile attaches, which comprises the following four procedures:

– mutual authentication of the mobile and the MME;

– registration of the mobile's location with the MME;

– assignment of the GUTI to the mobile;

– establishment of the default bearer.

The switch to the deregistered state takes place when the mobile detaches or when the attachment of the mobile, the update of its location or the service request are rejected by the MME.

1.2.1.1. *EMM messages*

1.2.1.1.1. Attachment and detachment

The procedure of attachment is initiated by the mobile in the deregistered state, by sending the message EMM ATTACH REQUEST to the MME. This message contains the mobile GUTI or IMSI and its TAC. The mobile attaches the message ESM PDN CONNECTIVITY REQUEST to establish the default bearer.

Upon receiving this message, the MME begins the authentication and security procedures. If they are successfully completed, the MME responds with the message EMM ATTACH ACCEPT, containing a new GUTI, and the message ESM ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST, to establish the default bearer.

The mobile responds with the message EMM ATTACH COMPLETE containing the message ESM ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT, to acknowledge the previous message.

If the procedures are not successful, the MME responds with the message EMM ATTACH REJECT, containing the message ESM PDN CONNECTIVITY REJECT, which causes the mobile to detach.

Detachment may be initiated by the mobile or the MME by sending the message EMM DETACH REQUEST. The response EMM DETACH ACCEPT concludes the detachment procedure. The response is not transmitted by the MME if the detach request sent by the mobile indicates that it has been turned off. The detachment procedure implicitly causes the release of the active bearers.

1.2.1.1.2. Authentication

The procedure of mutual authentication is initiated by the MME by sending the message EMM AUTHENTICATION REQUEST, containing a random number RAND and the authentication code AUTN (Authentication Network).

The mobile uses the RAND received to locally compute its own authentication code RES (Result), and compares its AUTN to the one received from the MME.

If the MME is authenticated, the mobile responds with the message EMM AUTHENTICATION RESPONSE, containing the authentication code RES. Otherwise, it displays the message EMM AUTHENTICATION FAILURE.

The MME compares the RES value received from the mobile with that communicated by the HSS. If the two codes are the same, the mobile is

authenticated and the MME triggers security mode for NAS signaling. Otherwise, it responds with the message EMM AUTHENTICATION REJECT.

1.2.1.1.3. Security mode

When mutual authentication has been successful, the MME begins putting the NAS signaling in security mode by sending the message EMM SECURITY MODE COMMAND. The integrity of this message is protected.

If the check on the integrity of the EMM SECURITY MODE COMMAND is positive, the mobile responds with the message EMM SECURITY MODE COMPLETE. All subsequent NAS messages are encrypted and their integrity is checked.

If the check on the integrity of the EMM SECURITY MODE COMMAND is negative, the mobile responds with the message EMM SECURITY MODE REJECT.

1.2.1.1.4. Tracking area update

The procedure of tracking area update is periodically initiated so that the mobile can maintain its tracking area, or when the mobile has changed TAC. The mobile, in the registered state, sends the message EMM TRACKING AREA UPDATE REQUEST to the MME.

The MME responds either with the message EMM TRACKING AREA UPDATE ACCEPT if it accepts the update, or else with the message EMM TRACKING AREA UPDATE REJECT, indicating the cause of the rejection.

If the message EMM TRACKING AREA UPDATE ACCEPT attributes a new GUTI to the mobile, the mobile confirms receipt of this by sending the message EMM TRACKING AREA UPDATE COMPLETE.

1.2.1.1.5. Service request

The service request is initiated by the mobile, by sending the EMM SERVICE REQUEST when signaling or traffic data is waiting. The mobile is notified of awaiting data at the level of the network by way of the paging procedure. The service request is sent when the mobile is in idle mode, to re-establish the bearers on the LTE-Uu and S1-U interfaces.

The MME may reject the request, in which case it responds with the message EMM SERVICE REJECT. This response causes the passage of the mobile to the deregistered state.

1.2.1.2. *ESM messages*

The mobile sends the request to establish the default bearer when the mobile attaches to the MME. The dedicated bearer corresponds to a specific request by the mobile. The dedicated bearer is associated with a particular quality of service, corresponding to a particular QCI, which is different to that of the default bearer. The establishment request can be transmitted by the network or the mobile.

Table 1.2 recaps the ESM messages exchanged for the establishment, modification and release of the bearer.

Source	Message	Destination
Establishment of default bearer, initiated by the network		
MME	ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST	UE
UE	ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT or ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT	MME
Establishment of dedicated bearer, initiated by the network		
MME	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST	UE
UE	ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT or ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT	MME
Modification of dedicated bearer, initiated by the network		
MME	MODIFY EPS BEARER CONTEXT REQUEST	UE
UE	MODIFY EPS BEARER CONTEXT ACCEPT or MODIFY EPS BEARER CONTEXT REJECT	MME

Table 1.2. *Messages in the ESM protocol*

Release of dedicated bearer, initiated by the network		
MME	DEACTIVATE EPS BEARER CONTEXT REQUEST	UE
UE	DEACTIVATE EPS BEARER CONTEXT ACCEPT	MME
Release of default bearer, initiated by the mobile		
UE	PDN CONNECTIVITY REQUEST	MME
MME	ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST or PDN CONNECTIVITY REJECT	UE
Establishment or modification of dedicated bearer, initiated by the mobile		
UE	BEARER RESOURCE ALLOCATION REQUEST	MME
MME	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST or ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT or MODIFY EPS BEARER CONTEXT REQUEST	UE
Modification of dedicated bearer, initiated by the mobile		
UE	BEARER RESOURCE MODIFICATION REQUEST	MME
MME	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST or MODIFY EPS BEARER CONTEXT REQUEST or DEACTIVATE EPS BEARER CONTEXT REQUEST or BEARER RESOURCE MODIFICATION REJECT	UE
Release of default bearer, initiated by the mobile		
UE	PDN DISCONNECT REQUEST	MME
MME	DEACTIVATE EPS BEARER CONTEXT REQUEST or PDN DISCONNECT REJECT	UE

Table 1.2. *(Continued) Messages in the ESM protocol*

1.2.2. *RRC protocol*

The RRC protocol is the signaling exchanged between the mobile and the eNB over the LTE-Uu radioelectric interface (Figure 1.2). It performs the following functions:

– broadcast of system information relative to the characteristics of the radioelectric interface;

– control of the RRC connection. This procedure includes the procedures of paging, establishment, modification and release of the SRB (Signaling Radio Bearer) and the DRB (Data Radio Bearer). It also includes the activation of security mode, the procedure for which consists of putting mechanisms in place to encrypt the traffic and signaling flows, and to control the integrity of the signaling flows;

– control of handover. This procedure executes the changing of cell between two eNBs (intra-system handover) or between an eNB and an entity from a 2nd- or 3rd-generation mobile network (inter-system handover);

– measurement reporting. The eNB can trigger measurements carried out by the mobile, either periodically or on demand, to prepare for handover;

– transport of the NAS messages exchanged between the mobile and the MME.

From the point of view of the eNB, the mobile may be in one of two operational states: idle mode (RRC_IDLE) or connected mode (RRC_CONNECTED).

In idle mode, the mobile is not known to the eNB. It remains in this state until the RRC connection setup procedure is completed. The setup procedure is triggered by the mobile when it wishes to transmit traffic or signaling data. In that state, the mobile used the SRB0 bearer.

In connected mode, the mobile can transmit and receive signaling and traffic data. The mobile is attributed an identifier which is unique to the cell – the C-RNTI (Cell Radio Network Temporary Identity). In this state, the mobile uses either the SRB1 bearer for RRC messages with possible associated NAS messages, or the SRB2 bearer for RRC messages transporting solely NAS messages.

Table 1.3 recaps the type of SRB, the mode of RLC protocol and the channels used by the different RRC messages over the radioelectric interface.[2]

2 A detailed description of the data link layer and the physical layer is given in Chapter 2, on the LTE interface.

SRB	RLC mode	Logic channel	Transport channel	Physical channel
MasterInformationBlock				
None	TM	BCCH	BCH	PBCH
SystemInformationBlock				
None	TM	BCCH	DL-SCH	PDSCH
Paging				
None	TM	PCCH	PCH	PDSCH
RRCConnectionSetup *RRCConnectionReject* *RRCConnectionReestablishment* *RRCConnectionReestablishmentReject*				
SRB0	TM	CCCH	DL-SCH	PDSCH
RRCConnectionRequest *RRCConnectionReestablishmentRequest*				
SRB0	TM	CCCH	UL-SCH	PUSCH
RRCConnectionReconfiguration *RRCConnectionRelease* *SecurityModeCommand*				
SRB1	AM	DCCH	DL-SCH	PDSCH
DLInformationTransfer (1)				
SRB2	AM	DCCH	DL-SCH	PDSCH
RRCConnectionSetupComplete *SecurityModeComplete* *SecurityModeFailure* *RRCConnectionReconfigurationComplete* *RRCConnectionReestablishmentComplete* *MeasurementReport*				
SRB1	AM	DCCH	UL-SCH	PUSCH
ULInformationTransfer (2)				
SRB2	AM	DCCH	UL-SCH	PUSCH

(1): transport of NAS messages only, downstream
(2): transport of NAS messages only, upstream

Table 1.3. *Messages in the RRC protocol*

1.2.2.1. *Information concerning the radioelectric interface*

The information relating to the radioelectric interface is divided between the messages *MasterInformationBlock* (MIB) and *SystemInformationBlock* (SIB). These messages are transmitted periodically, and a change in these data is notified to the mobile by paging.

The MIB message contains the following data:

– the bandwidth of the radioelectric signal for the downstream direction (1.4 MHz, 3, 5, 10, 15, 20 MHz);

– the System Frame Number (SFN);

– the configuration of the physical channel PHICH of the radioelectric interface. The configuration of this physical channel is defined by the operator.

All *SystemInformationBlock* messages, with the exception of the message *SystemInformationBlockType1*, are mapped in a *SystemInformation* message. Each *SystemInformation* message contains *SystemInformationBlock* messages with the same periodicity. The message *SystemInformationBlockType2* must necessarily be mapped in the message *SystemInformation1*.

The message *SystemInformationBlockType1* contains the following data:

– the MCC and MNC of the mobile network;

– the TAC of the TAI;

– the cell identifier;

– the periodicity of the *SystemInformation* messages and the types of *SystemInformationBlock* messages that they contain.

Table 1.4 shows the data transported by the different types of *SystemInformationBlock* message.

SystemInformationBlockType2	Bandwidth in upstream direction Configuration of physical channels
SystemInformationBlockType3	Cell selection parameters
SystemInformationBlockType4	Neighboring EPS cells, same frequency
SystemInformationBlockType5	Neighboring EPS cells, different frequency
SystemInformationBlockType6	Neighboring UMTS cells
SystemInformationBlockType7	Neighboring GSM/GPRS cells
SystemInformationBlockType8	Neighboring CDMA 2000 cells
SystemInformationBlockType9	Identifier of the femtocell eNB
SystemInformationBlockType10 *SystemInformationBlockType11*	Tsunami and earthquake warning

Table 1.4. *SystemInformationBlock messages*

1.2.2.2. *Control of RRC connection*

The different procedures associated with the control of the RRC connection relate to paging, RRC connection setup, activation of security mode, RRC connection reconfiguration, RRC connection re-establishment and RRC connection release.

The message Paging is used by the eNB to alert one or more mobiles in the RRC_IDLE state. It also helps to inform the mobile in RRC_IDLE or RRC_CONNECTED state about a change in the system information or about a notification on the ETWS (Earthquake and Tsunami Warning System) transmitted in the messages *SystemInformationBlockType10* and *SystemInformation BlockType11*.

The message *RRCConnectionRequest* is used by the mobile to request the establishment of an RRC connection.

The message *RRCConnectionSetup* is used by the eNB to configure the SRB1 bearer.

The message *RRCConnectionSetupComplete* is used by the mobile to confirm the setup of the RRC connection. This message can also transport NAS messages.

The message *RRCConnectionReject* is used by the eNB to reject the RRC connection.

Upon receiving the context about the mobile from the MME, the eNB activates security mode for the RRC messages. The messages are only checked for integrity. The encryption of the RRC messages will be effective only if the procedure has been successful.

The message *SecurityModeCommand* is used by the eNB to command the activation of security mode on the radioelectric interface.

The message *SecurityModeComplete* is used by the mobile to confirm the activation of security mode.

The message *SecurityModeFailure* is used by the mobile to indicate that security mode was unable to be activated.

Having initiated the security mode activation procedure, the eNB begins the activation of the DRB. The RRC messages are encrypted and checked for integrity.

The message *RRCConnectionReconfiguration* is used by the eNB to command a modification of the RRC connection. This message may relate to the configuration

of the measurements, control of the mobility, configuration of the DRB, etc. This message can also transport NAS messages.

The message *RRCConnectionReconfigurationComplete* is used by the mobile to confirm the reconfiguration of the RRC connection.

The message *RRCConnectionReestablishmentRequest* is used by the mobile to request the re-establishment of the RRC connection.

The message *RRCConnectionReestablishment* is used by the eNB to re-establish the SRB1 bearer.

The message *RRCConnectionReestablishmentComplete* is used by the mobile to confirm the re-establishment of the RRC connection.

The message *RRCConnectionReestablishmentReject* is used by the eNB to indicate that the re-establishment of the RRC connection has been rejected.

The message *RRCConnectionRelease* is used by the eNB to release the RRC connection. The procedure can also be used to redirect the mobile to a different frequency band. In exceptional cases, the mobile can terminate the RRC connection without alerting the eNB.

1.2.2.3. *Measurement report*

The measurements carried out by the mobile must be in line with the configuration indicated in the message *RRCConnectionReconfiguration* transmitted by the eNB. The mobile sends the eNB the measurements in the RRC message *MeasurementReport*.

The configuration of the measurements defines which objects the mobile has to measure:

– the frequency received from the eNB (intra-frequency measurements);

– other frequencies on the EPS network (inter-frequency measurements);

– the frequencies delivered by other mobile networks.

The measurement configuration provides a list of reports containing the criteria giving rise to the sending of a report and the format of those reports. The criteria relate to the events which trigger the report. The format of the report specifies the parameters that need to be included, e.g. the RSRP (Reference Signal Received Power) or the RSRQ (Reference Signal Received Quality).

The measurement configuration determines the identifier of the measurements. Each identifier corresponds to a combination between an object and a report.

1.2.3. *S1-AP protocol*

The S1-AP protocol is the signaling exchanged between the eNB and MME over the S1-MME interface (Figure 1.2). It performs the following functions (Table 1.5):

– activation of the context of the mobile;

– establishment, modification and release of the E-RAB;

– handover management;

– paging. This procedure tells the eNB that the message needs to be broadcast in the cell;

– transport of the NAS signaling exchanged between the mobile and the MME;

– establishment of the S1-MME interface.

1.2.3.1. *Context management*

The context of the mobile has to be established at the level of the eNB and MME so as to transmit the mobile traffic and the NAS signaling. It includes the contexts relating to the default bearer, security, the capacities of the mobile and roaming restrictions. Context setup for the mobile begins with the message INITIAL CONTEXT SETUP REQUEST transmitted by the MME to the eNB. This message follows the reception of the message INITIAL UE MESSAGE.

The MME has to prepare the establishment of the default bearer before receiving the message INITIAL CONTEXT SETUP RESPONSE. This message might contain the cause of the failure to set up the context of the mobile, such as the lack of radioelectric resources.

If the eNB is unable to establish the context of the mobile, it responds with the message INITIAL CONTEXT SETUP FAILURE.

Release of the context of the mobile is done by way of the message UE CONTEXT RELEASE COMMAND transmitted by the MME to the eNB, for instance when the mobile changes cell. This message is acknowledged in return by the response UE CONTEXT RELEASE COMPLETE.

1.2.3.2. *Bearer management*

Establishment and modification of the dedicated bearer E-RAB are initiated by the MME by sending the messages E-RAB SETUP/MODIFY REQUEST. The eNB responds positively or negatively by sending the messages E-RAB SETUP/MODIFY RESPONSE.

Functions	Request	Response
Paging	PAGING	None
Context management	INITIAL CONTEXT SETUP REQUEST	INITIAL CONTEXT SETUP RESPONSE or INITIAL CONTEXT SETUP FAILURE
	UE CONTEXT RELEASE COMMAND	UE CONTEXT RELEASE COMPLETE
Bearer management	E-RAB SETUP/MODIFY REQUEST	E-RAB SETUP/MODIFY RESPONSE
	E-RAB RELEASE COMMAND	E-RAB RELEASE RESPONSE
	E-RAB RELEASE INDICATION	None
Mobility management	HANDOVER REQUIRED	HANDOVER COMMAND
	HANDOVER REQUEST	HANDOVER REQUEST ACKNOWLEDGE or HANDOVER FAILURE
	eNB STATUS TRANSFER	None
	MME STATUS TRANSFER	None
	HANDOVER NOTIFY	None
	PATH SWITCH REQUEST	PATH SWITCH ACKNOWLEDGE or PATH SWITCH FAILURE
S1-MME interface management	S1 SETUP REQUEST	S1 SETUP RESPONSE or S1 SETUP FAILURE
	ENB CONFIGURATION UPDATE	ENB CONFIGURATION UPDATE ACKNOWLEDGE or ENB CONFIGURATION UPDATE FAILURE
	MME CONFIGURATION UPDATE	MME CONFIGURATION UPDATE ACKNOWLEDGE or ENB CONFIGURATION UPDATE FAILURE
	OVERLOAD START	None
	OVERLOAD STOP	None
Transport of NAS signaling	INITIAL UE MESSAGE	None
	DOWNLINK NAS TRANSPORT	None
	UPLINK NAS TRANSPORT	None

Table 1.5. *Messages in the S1-AP protocol*

Release of the dedicated bearer is initiated by the MME by sending the message E-RAB RELEASE COMMAND, or by the eNB by sending an E-RAB RELEASE INDICATION. Upon receiving this message, the MME begins the procedure of release of the dedicated bearer.

1.2.3.3. *Mobility management*

The decision regarding handover based on the S1 interface is made by the source eNB. The phase of handover preparation begins with the sending of the message HANDOVER REQUIRED to the MME. When the reservation of resources by the target eNB is effective, the MME responds with the message HANDOVER COMMAND.

The MME asks the target eNB to reserve the radioelectric resources by way of the message HANDOVER REQUEST. If the operation is successful, the target eNB responds with the message HANDOVER REQUEST ACKNOWLEDGE. This message can contain the elements for construction of a GTP-U tunnel to transfer the received data from the source eNB to the target eNB so they can be transmitted to the mobile. If not, the target eNB responds with the message HANDOVER FAILURE.

The source eNB has to transfer the value of the field SN (Sequence Number) of the protocol PDCP to the target eNB in order to preserve, in the mobile reception, the continuity of the PDCP frame numbering. This operation is done by the transmission of the following messages:

– eNB STATUS TRANSFER from the source eNB to the MME;

– MME STATUS TRANSFER from the MME to the target eNB.

When the execution of the handover has been completed, the target eNB advises the MME of this by way of the message HANDOVER NOTIFY.

The message PATH SWITCH REQUEST is transmitted by the target eNB to the MME for the transfer of the extremity of the GTP-U tunnel corresponding to the source eNB to the target eNB. The MME responds with the message PATH SWITCH ACKNOWLEDGE if the response is positive or with PATH SWITCH FAILURE if not.

1.2.3.4. *S1-MME interface management*

The eNB is in charge of selecting the MME. The eNB therefore takes the initiative to activate the S1-MME interface by transmitting the message S1 SETUP REQUEST, indicating the list of TACs served. The response message from MME, S1 SETUP RESPONSE, contains information relating to the MME such as its

MMEC, the number of the pool to which it belongs and the MNC and MCC. The MME may respond negatively with the message S1 SETUP FAILURE.

Updates to the information about the eNB (or respectively MME) are transmitted by the message ENB CONFIGURATION UPDATE (or respectively MME CONFIGURATION UPDATE). These messages receive a positive response with the messages ENB/MME CONFIGURATION UPDATE ACKNOWLEDGE or a negative one with the messages ENB/MME CONFIGURATION UPDATE FAILURE.

The MME notifies the eNB of the beginning (or respectively the end) of a state of overload by the message OVERLOAD START (or respectively OVERLOAD STOP) so as to avoid being selected for the attachment of a new mobile.

1.2.4. *X2-AP protocol*

The X2-AP protocol is the signaling exchanged between two eNBs over the X2 interface (Figure 1.4). It performs the following functions (Table 1.6):

– mobility management. This function enables the source eNB to transfer the connection of a mobile to the target eNB;

– load management. This function is used by the eNBs to provide an indication of the load of the cells that they serve;

– X2 interface management. This function is used for the activation of the X2 interface, the reconfiguration and re-initialization of the X2 interface.

1.2.4.1. *Mobility management*

The function of mobility management contains the following elementary procedures:

– handover preparation;

– transfer of the state of the field SN of the PDCP protocol;

– deactivation of the context of the mobile;

– handover cancellation.

The procedure of handover preparation is initiated by the source eNB by transmission of the message HANDOVER REQUEST to the target eNB. The target eNB reserves the resources and responds with the message HANDOVER REQUEST ACKNOWLEDGE. This message contains the value of the TEID identifier used by the GTP-U protocol for the traffic transferred by the source eNB

to the target eNB. If the resources are unavailable, the target eNB sends back the message HANDOVER PREPARATION FAILURE.

Functions	Request	Response
Load management	LOAD INFORMATION	None
	RESOURCE STATUS REQUEST	RESOURCE STATUS RESPONSE or RESOURCE STATUS FAILURE
Load management	RESOURCE STATUS UPDATE	None
Mobility management	HANDOVER REQUEST	HANDOVER REQUEST ACKNOWLEDGE or HANDOVER PREPARATION FAILURE
	SN STATUS TRANSFER	None
	UE CONTEXT RELEASE	None
	HANDOVER CANCEL	None
X2 Interface management	X2 SETUP REQUEST	X2 SETUP RESPONSE or X2 SETUP FAILURE
	ENB CONFIGURATION UPDATE	ENB CONFIGURATION UPDATE ACKNOWLEDGE or ENB CONFIGURATION UPDATE FAILURE
	RESET REQUEST	RESET RESPONSE

Table 1.6. *Messages in the X2-AP protocol*

The procedure of transfer of the state of the field SN consists of transferring to the eNB the value of the SN (Sequence Number) of the PDCP protocol with the message SN STATUS TRANSFER. At the source eNB, this message stops the attribution of the SN of the PDCP protocol for the downstream direction.

The procedure for context release of the mobile is initiated by the target eNB by sending the message UE CONTEXT RELEASE to the source eNB. Upon receiving this message, the eNB eliminates the context of the mobile.

The procedure for cancelling the handover is initiated by the source eNB with the message HANDOVER CANCEL. This message causes the target eNB to release the resources on the radioelectric interface.

1.2.4.2. *Load management*

The function of load management includes the following elementary procedures:

– cell load indication;

– initialization of resource status reports;

– resource status reporting.

The procedure for indication of the load of the cell is initiated by either of the eNBs with the message LOAD INFORMATION. This message may contain the following elements of information:

– Interference Overload Indication. This information relates to the interference detected by the eNB, for the upstream direction. The eNB receiving this information has to decrease the level of interference transmitted by the mobile;

– High Interference Indication. This information relates to the interference detected by the eNB, for the upstream direction, indicating which bandwidths are affected. The eNB receiving this information needs to avoid using the said bandwidth, for the upstream direction, for the mobiles located on the periphery of the cell;

– Relative Narrowband Tx Power. This information relates to a decrease in the power transmitted by an eNB. The eNB receiving this information includes it in its traffic management mechanism.

The procedure for initialization of resource status reporting is initiated by either of the eNBs with the message RESOURCE STATUS REQUEST. The eNB receiving this message responds with the message RESOURCE STATUS RESPONSE, which may contain status information for the radioelectric resources, the S1 interface and the load of the eNB. The eNB may respond with RESOURCE STATUS FAILURE if the reports cannot be generated.

The resource status report is then transmitted periodically by the eNB by sending the message RESOURCE STATUS UPDATE.

1.2.4.3. *X2 interface management*

The X2 interface is set up with the intention of exchanging the configuration data necessary for both eNBs to function correctly. One of the eNBs initiates the procedure by indication of the cells served in a message X2 SETUP REQUEST to a

candidate eNB. The candidate eNB responds with the message X2 SETUP RESPONSE, also containing the list of cells served. The information communicated may also include the list of nearby cells and the number of antennas for each cell served. The eNB may refuse the establishment of the X2 interface by sending the message X2 SETUP FAILURE in response.

The X2 setup is followed by configuration updating of the eNB if the eNB's configuration changes. The configuration update is initiated by the message ENB CONFIGURATION UPDATE. The distant eNB may respond positively with the message CONFIGURATION UPDATE ACKNOWLEDGE or negatively with the message ENB CONFIGURATION UPDATE FAILURE.

The reset of the X2 interface is intended to align the resources of the eNBs in the case of an unexpected breakdown. The procedure is initiated by the message RESET REQUEST. The receiving eNB responds with the message RESET RESPONSE. The procedure does not affect the data exchanged during the X2 setup or the eNB configuration update.

1.2.5. *GTPv2-C protocol*

GTP tunnels are used between two entities. Such tunnels enable the traffic or signaling data to be compartmentalized. GTP-U traffic tunnels are constructed on the interfaces S1-U, S5 and X2. GTP-C signaling tunnels are created on the S5, S11 and S10 interfaces.

The tunnel is identified by the parameters TEID, the IP addresses and the UDP port numbers. The entity receiving the traffic or signaling data determines the value of the parameter TEID which the sending entity has to use.

The values of the parameter TEID of the GTP-U protocol are exchanged via the GTPv2-C, S1-AP and X2-AP protocols. This parameter is used for data flows belonging to the same QCI.

The TEID used for the signaling exchanged over the S5 interface is unique. The same parameter is used for all signaling messages relating to the activation of the various S5 bearers for the different mobiles.

The TEID used for the signaling exchanged over the S10 and S11 interfaces is unique for each mobile. The same parameter is used for all signaling messages relating to the establishment of the various S1-U bearers for the same mobile.

Table 1.7 recaps the messages making up the GTPv2-C protocol.

Type of messages	Request	Response
Mobility management	FORWARD RELOCATION REQUEST	FORWARD RELOCATION RESPONSE
	FORWARD RELOCATION NOTIFICATION	FORWARD RELOCATION ACKNOWLEDGE
	FORWARD ACCESS CONTEXT NOTIFICATION	FORWARD ACCESS CONTEXT ACKNOWLEDGE
	CONTEXT REQUEST	CONTEXT RESPONE
	CONTEXT ACKNOWLEDGE	
Bearer management	CREATE/DELETE SESSION REQUEST	CREATE/DELETE SESSION RESPONSE
	CREATE/MODIFY/DELETE BEARER REQUEST	CREATE/MODIFY/DELETE BEARER RESPONSE
	DOWNLINK DATA NOTIFICATION	DOWNLINK DATA NOTIFICATION ACKNOWLEDGE or DOWNLINK DATA NOTIFICATION FAILURE INDICATION
Bearer management	CREATE/DELETE INDIRECT DATA FORWARDING TUNNEL REQUEST	CREATE/DELETE INDIRECT DATA FORWARDING TUNNEL RESPONSE

Table 1.7. *Messages in the GTPv2-C protocol*

1.2.5.1. *Bearer management*

The signaling bearer unique to a mobile is created by the message CREATE SESSION REQUEST. It is reinforced by the use of a TEID. The message is transmitted:

– by the MME to the SGW, over the S11 interface;

– by the target SGW for the PGW over the S5 interface.

The request is transmitted when any of the following procedures are initiated:

– attachment of a mobile;

– traffic request from the mobile;

– updating of the TAC, leading to a switch of the SGW;

– cell handover, with switch of the SGW.

The SGW (or respectively PGW) responds to the MME (or respectively SGW) with the message CREATE SESSION RESPONSE.

The signaling bearer is deactivated by the exchange of the messages DELETE SESSION REQUEST/RESPONSE. The procedure is triggered when the mobile detaches, when the traffic is released, when the TAC changes, leading to a modification of the SGW, or when handover occurs, with a switch of the SGW.

Similarly, the traffic-dedicated bearer specific to a mobile is created, possibly modified and deleted by the exchange of the following messages:

– CREATE/MODIFY/DELETE BEARER REQUEST;

– CREATE/MODIFY/DELETE BEARER RESPONSE.

The message DOWNLINK DATA NOTIFICATION is sent by the SGW to the MME, over the S11 interface. The procedure follows the SGW's receipt of data from the PDW, with the mobile in ECM-IDLE mode. Upon receiving this message, the MME sends the paging message to the mobile.

The MME may respond with the message DOWNLINK DATA NOTIFICATION ACKNOWLEDGE, indicating whether or not the request is accepted, or DOWNLINK DATA NOTIFICATION FAILURE INDICATION if the mobile does not respond to the paging or if the mobile service request is rejected.

The messages CREATE INDIRECT DATA FORWARDING TUNNEL REQUEST/RESPONSE create a specific traffic bearer when cell handover occurs. This bearer channels the data traffic received by the source eNB to the SGW to then be re-transmitted to the mobile via the target eNB.

1.2.5.2. *Mobility management*

Mobility management messages are exchanged between the source and target MMEs, when the handover of the mobile imposes a switch of MME.

The source MME sends the target MME the message FORWARD RELOCATION REQUEST, containing the context of the mobile. The target MME responds with the message FORWARD RELOCATION RESPONSE when the resources needed for the handover have been reserved. The response contains the values of the TEIDs, which will enable the source SGW to redirect the traffic to the target SGW during handover. Upon receiving this message, the source MME sends the source eNB the command to initiate handover.

The source MME sends the target MME the message FORWARD ACCESS CONTEXT NOTIFICATION to furnish it with the elements of the context of the E-RAB bearer, such as the PDCP sequence number.

The target MME sends the source MME the message FORWARD RELOCATION NOTIFICATION to indicate that the handover procedure is complete.

The new MME sends the message CONTEXT REQUEST to the former one in the procedure of TAI updating, to retrieve information about the context of the mobile. The former MME provides this information in the message CONTEXT RESPONSE, which may contain a positive or negative response. The new entity acknowledges this previous message with the message CONTEXT ACKNOWLEDGE.

1.3. Procedures

1.3.1. *Attachment procedure*

The attachment procedure comprises the following stages:

– mutual authentication between the mobile and the MME;

– location of the mobile by the MME;

– establishment of a default bearer. If the telephone service is borne by the EPS network, a default bearer (QCI = 5) is created to transport the telephone signaling exchanged between the mobile and the IMS network;

– assignment of a temporary private identity (GUTI).

1.3.1.1. *Registration*

The registration procedure is described in Figure 1.6.

The procedure for the registration of the mobile with the MME is preceded by the procedure of connection of the mobile to the eNB.[3]

The registration procedure is triggered by the mobile when it sends the MME the messages EMM ATTACH REQUEST and ESM PDN CONNECTIVITY REQUEST containing its IMSI (International Mobile Subscriber Identity) or GUTI,

3 A description of the procedure for connection to the eNB is given in Chapter 2, on the LTE interface.

if known. The selection of the MME attributed to the mobile is performed by the eNB, which transfers the EMM and ESM messages.

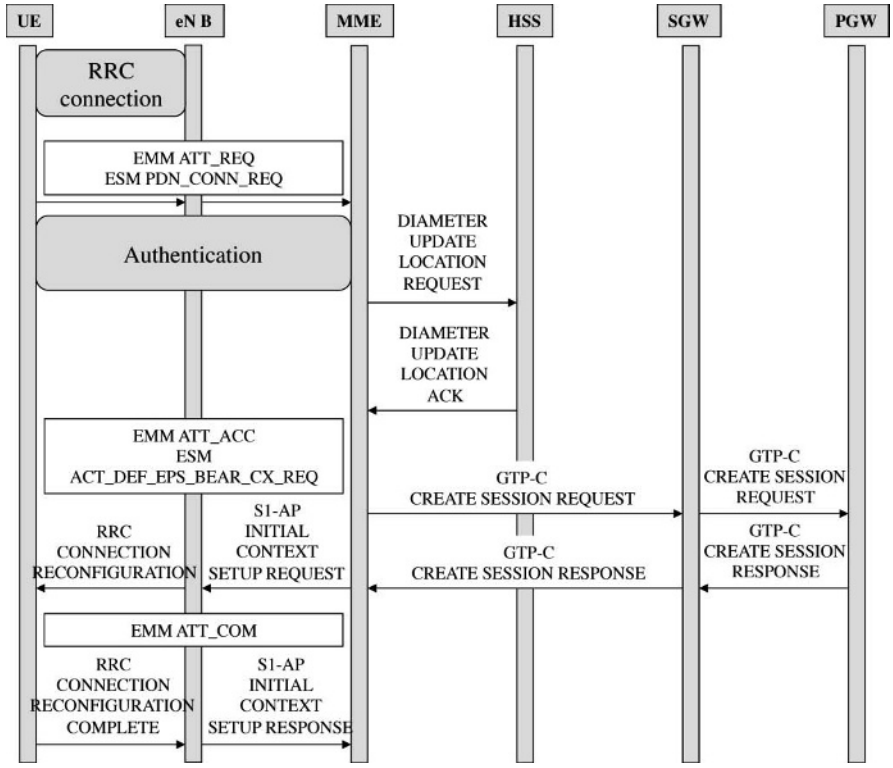


Figure 1.6. *Registration procedure*

The EMM and ESM messages are transmitted:

– by the message *RRCConnectionSetupComplete* over the LTE-Uu radioelectric interface;

– by the message S1-AP INITIAL UE MESSAGE over the S1-MME interface.

Following the procedure of mutual authentication, the MME updates the location of the mobile in the HSS database, via the message DIAMETER UPDATE LOCATION REQUEST.

In return, the HSS provides the MME with the profile of the mobile via the message DIAMETER UPDATE LOCATION ACK.

The default bearer is established by the following signaling exchanges:

– over the S11 and S5 interfaces, the messages GTP-C CREATE SESSION REQUEST and CREATE SESSION RESPONSE;

– over the S1-MME interface, the messages S1-AP INITIAL CONTEXT SETUP REQUEST and INITIAL CONTEXT SETUP RESPONSE;

– over the LTE-Uu radioelectric interface, the RRC messages *ConnectionReconfiguration* and *RRCConnectionReconfigurationComplete*.

The messages S1-AP INITIAL CONTEXT SETUP REQUEST and *RRCConnectionReconfiguration* transport the messages EMM ATTACH ACCEPT and ESM ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST.

The messages S1-AP INITIAL CONTEXT SETUP RESPONSE and *RRCConnectionReconfigurationComplete* transport the message EMM ATTACH COMPLETE.

1.3.1.2. *Authentication and security procedure*

The procedure for authentication and security activation is shown in Figure 1.7.

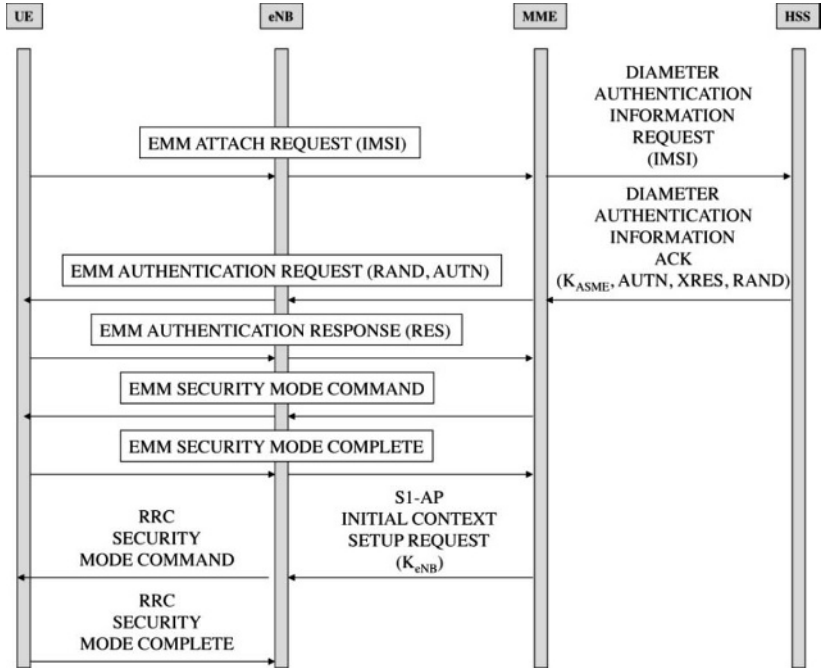


Figure 1.7. *Authentication and security mode procedure*

Upon receipt of the message EMM ATTACH REQUEST, an exchange of messages DIAMETER AUTHENTICATION INFORMATION REQUEST/ACK enables the MME to recover the following data from the HSS:

– a random number RAND;

– the authentication code XRES, computed on the basis of the RAND and the secret key Ki of the mobile;

– the network authentication AUTN;

– the key K_{ASME}, derived from the IK and CK keys, which themselves are derived from the Ki.

On the basis of the K_{ASME}, the MME derives the following keys:

– CK_{NAS}, used to encrypt the NAS messages;

– IK_{NAS}, used to verify the integrity of the NAS messages;

– Ke_{NB}, transferred to the eNB.

The MME sends the mobile the message EMM AUTHENTICATION REQUEST containing the RAND and the AUTN.

The mobile uses its secret Ki stored in the USIM (Universal Services Identity Module) on its UICC (Universal Integrated Circuit Card), and the RAND received, to locally compute its own authentication code RES and that of the network, which it compares to the AUTN value received. If the two values are identical, the network is authenticated.

The mobile also derives the keys CK_{NAS}, IK_{NAS} and Ke_{NB} from the Ki and the RAND received.

The mobile responds to the MME with the message EMM AUTHENTICATION RESPONSE, containing the authentication code RES. The MME compares the received values RES from the mobile and XRES from the HSS. If the values are identical, the mobile is authenticated.

The security mode for NAS signaling is activated by the exchange of the messages EMM SECURITY MODE COMMAND/COMPLETE.

The above EMM messages are transported:

– by the S1-AP messages DOWNLINK NAS TRANSPORT and RRC *DLInformationTransfer* for the downstream direction;

– by the messages RRC *ULInformationTransfer* and S1-AP UPLINK NAS TRANSPORT for the upstream direction.

The MME sends the eNB the key K_{eNB} in the message S1-AP INITIAL CONTEXT SETUP REQUEST.

Using the K_{eNB}, the eNB and mobile can derive the following keys:

– $CK_{eNB\text{-}RRC}$, used for the encryption of the RRC messages;

– $K_{eNB\text{-}RRC}$, used to check the integrity of the RRC messages;

– $CK_{eNB\text{-}UP}$, used to encrypt the data traffic.

Security mode for the LTE-Uu radioelectric interface is activated by the exchange of the RRC messages *SecurityModeCommand* and *SecurityMode Complete*.

1.3.2. *Location update*

The procedure of location updating is illustrated in Figure 1.8.

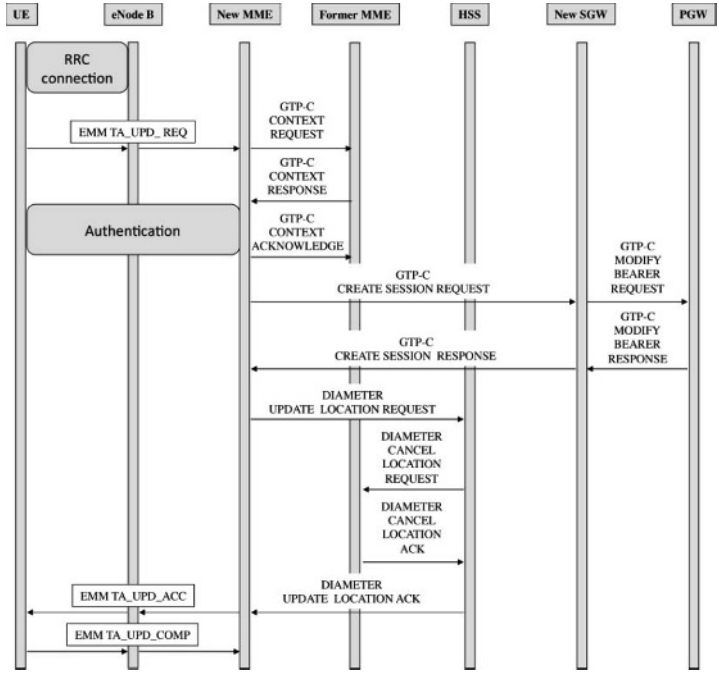


Figure 1.8. *Tracking area update procedure*

The procedure of registration of the mobile with the MME is preceded by the procedure of connection of the mobile to the eNB.

The mobile decides to update its location when it enters into a new TAI or when the hold-down timer has expired. The updating of the location includes the following operations:

– transfer of the context of the mobile from the former MME to the new one, if the new TAC belongs to a different pool;

– mutual authentication between the mobile and the new MME;

– updating of the bearer between the new SGW and the PGW;

– updating of the HSS with the identity of the new MME.

The mobile initiates the procedure of location update by sending the message EMM TRACKING AREA UPDATE REQUEST to the new MME.

The message EMM TRACKING AREA UPDATE REQUEST is transported:

– by the message *RRCConnectionSetupComplete* over the LTE-Uu radioelectric interface, between the mobile and the eNB;

– by the message S1-AP INITIAL UE MESSAGE over the S1-MME interface between the eNB and MME.

The new MME recovers the identity of the former one from the mobile GUTI, and contacts it, transmitting the message GTP-C CONTEXT REQUEST. The former MME sends back the context of the mobile in the message GTP-C CONTEXT RESPONSE.

The authentication procedure is performed between the mobile and the new MME, which then acknowledges transfer from the former MME by sending it the message GTP-C CONTEXT ACKNOWLEDGE.

The new MME creates a session with a new SGW by an exchange of signaling GTP-C CREATE SESSION REQUEST/RESPONSE. This message contains the IP address of the PGW, retrieved from the context of the mobile. The new SGW modifies the S5 bearer with the PGW by an exchange of signaling GTP-C MODIFY BEARER REQUEST/RESPONSE.

The new MME notifies the HSS of the updated location of the mobile by exchange of messages DIAMETER UPDATE LOCATION REQUEST/ACK.

For its part, the HSS cancels the data about the mobile in the former MME by exchanging the messages DIAMETER CANCEL LOCATION REQUEST/ACK. Upon receiving this message, the former MME deletes the context of the mobile. It performs the same operation on the SGW, deleting the session established by the exchange of the messages GTP-C DELETE SESSION REQUEST/RESPONSE.

The new entity can then respond to the mobile by sending the message EMM TRACKING AREA UPDATE ACCEPT containing a new GUTI. This message is acknowledged in return by the mobile with the message EMM TRACKING AREA UPDATE COMPLETE.

1.3.3. *Bearer activation*

The establishment of a dedicated bearer for voice data (QCI = 1) is coupled with the re-establishment of the default bearer attributed to the telephone signaling (QCI = 5).

The re-establishment of the default bearer is triggered by a service request. The procedure is initiated by the mobile in idle mode (with an outgoing call) or by the network (with an incoming call) to establish the DRB and S1 bearers.

1.3.3.1. *Re-establishment of the default bearer with an outgoing call*

The procedure for re-establishment of the default bearer in the case of an outgoing call is that shown in Figure 1.9.

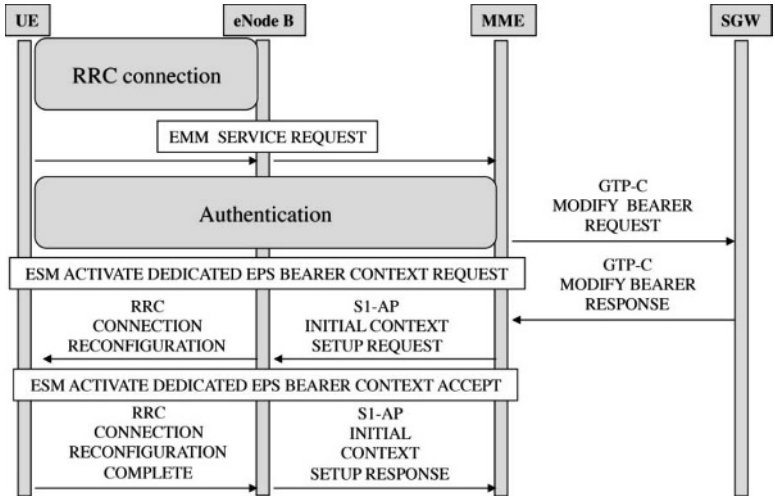


Figure 1.9. *Re-establishment of the default bearer with an outgoing call*

When making an outgoing call, the mobile initiates the service request procedure by activating the RRC connection and then sending a message EMM SERVICE REQUEST.

After authentication, the MME triggers the activation of the bearer on the S1-U interface by exchanging the messages GTP-C MODIFY BEARER REQUEST/RESPONSE with the SGW. The MME performs the same operation on the eNB, exchanging the messages S1-AP INITIAL CONTEXT SETUP REQUEST/RESPONSE. It should be noted that the S5 bearer remains active.

The eNB establishes the bearer on the radioelectric interface by exchange of the signaling *RRCReconfiguration* and *RRCReconfigurationComplete*.

1.3.3.2. *Re-establishment of the default bearer with an incoming call*

The procedure of re-establishment of the default bearer in the case of an incoming call is shown in Figure 1.10.

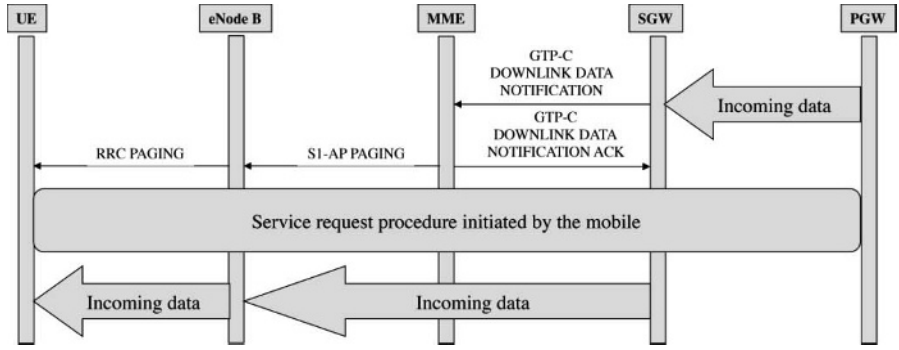


Figure 1.10. *Re-activation of the default bearer with an incoming call*

With an incoming call, because the S5 bearer is active, the SGW receives the telephone signaling data from the PGW, but the LTE-Uu and S1 bearers are inactive, as the mobile is in idle mode. The SGW generates the message GTP-C DOWNLINK DATA NOTIFICATION, sent to the MME.

The MME initiates the paging procedure by sending the eNB the message S1-AP PAGING, containing the S-TMSI (shortened temporary mobile subscriber) for the mobile.

The eNB transmits the RRC message *Paging* over the Uu interface. Upon receiving this message, the mobile initiates the service request procedure.

When the DRB and S1 bearers are established, the SGW transfers the stored incoming data to the eNB, which in turn sends them to the mobile.

1.3.3.3. *Establishment of the dedicated bearer*

The procedure for establishment of the dedicated bearer for voice data is shown in Figure 1.11.

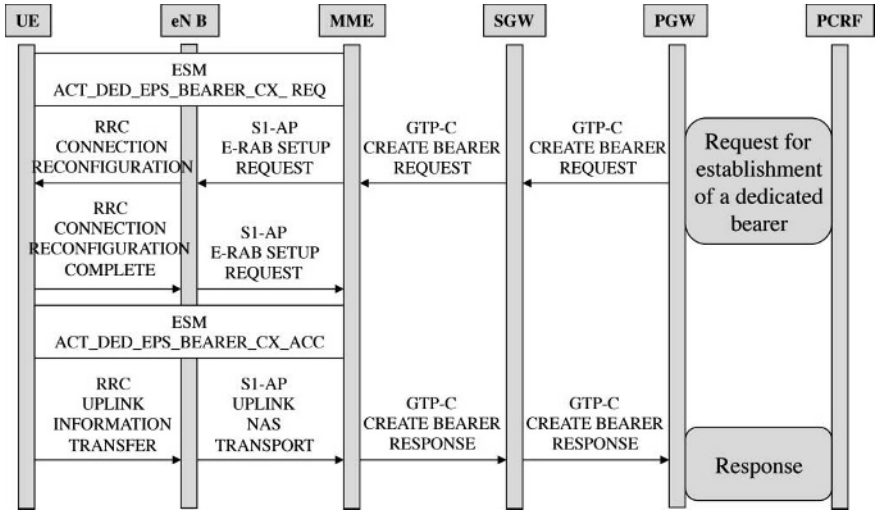


Figure 1.11. *Establishment of the dedicated bearer*

The establishment of the dedicated bearer is triggered by the IMS network, on the basis of the analysis of the telephone signaling exchanged between the terminals wishing to establish telephone communication.

The link between the IMS and EPS networks is ensured by the PCRF. This entity sends the PGW the characteristics of the voice-data dedicated bearer that needs to be activated. This dedicated bearer is coupled with the default bearer assigned to the telephone signaling, in the sense that the endings are identical for the two types of bearer.

The messages exchanged for the establishment of the dedicated bearer are as follows:

– for establishment of the S5 bearer, the GTP-C messages exchanged between the PGW and SGW (CREATE BEARER REQUEST/RESPONSE);

– for establishment of the S1 bearer, the GTP-C messages exchanged between the SGW and MME (CREATE BEARER REQUEST/RESPONSE) and the S1-AP messages exchanged between the MME and eNB (E-RAB SETUP REQUEST/RESPONSE);

– for establishment of the DRB, the RRC messages (*ConnectionReconfiguration* and *ConnectionReconfigurationComplete*) exchanged between the mobile and the eNB.

The establishment of the dedicated bearer is dependent upon the mobile's acceptance of it, in the wake of the exchange of ESM messages between the mobile and the MME:

– the request ESM ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST is sent by the MME;

– the response ESM ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT is sent back by the mobile.

1.3.4. *Handover procedure*

The procedure of handover takes place in two phases:

– the preparation phase, corresponding to the handover decision and to the reservation of the resources;

– the execution phase, corresponding to the handover itself, to the connection of the mobile to the target eNB and the release of the old resources.

1.3.4.1. *Handover based on the X2 interface*

This scenario refers to the activation of the X2 interface between two eNBs – the source and the target. Two procedures are possible, depending on whether or not the MME and SGW entities need to be relocated. The procedure without relocation is shown in Figure 1.12.

Upon receiving RRC messages *MeasurementReport*, the source eNB takes the decision to perform a cell handover and sends the target eNB the message X2-AP HANDOVER REQUEST.

On receiving the message X2-AP HANDOVER REQUEST ACK, the eNB triggers handover by sending the mobile the message *RRCConnection Reconfiguration*.

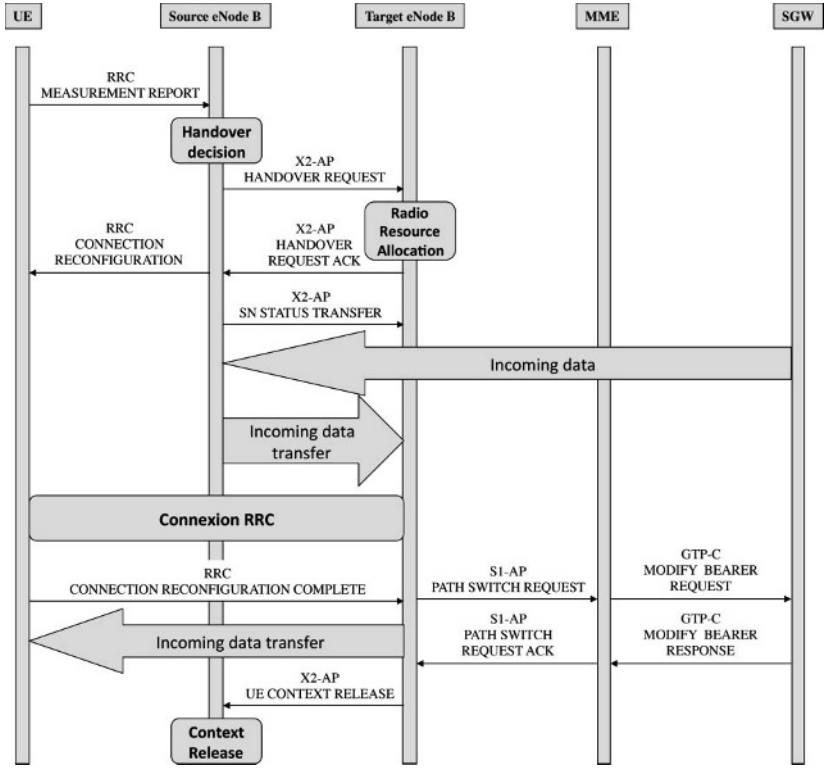


Figure 1.12. *Handover based on the X2 interface, without relocation*

The source eNB also sends the target eNB the PDCP sequence numbers in the message X2-AP SN STATUS TRANSFER, and then the incoming data which have not been acknowledged by the mobile. The target eNB will store these data until the mobile is able to receive them.

When the RRC connection is established between the mobile and the target eNB, the mobile sends a message *RRCConnectionReconfigurationComplete*, which triggers the transfer of the incoming data to the mobile and the modification of the S1-U bearer, by exchange of the following messages:

– S1-AP PATH SWITH REQUEST to the MME;

– GTP-C UPDATE BEARER REQUEST to the SGW.

When the S1-U bearer is available, the target eNB alerts the source eNB by the message X2-AP UE CONTEXT RELEASE so that it will release the context associated with the mobile.

1.3.4.2. *Handover based on the S1 interface, without relocation*

The procedure of handover based on the S1 interface occurs when the X2 interface is inactive. It may result in the relocation of the MME and SGW. The procedure without relocation is illustrated by Figure 1.13.

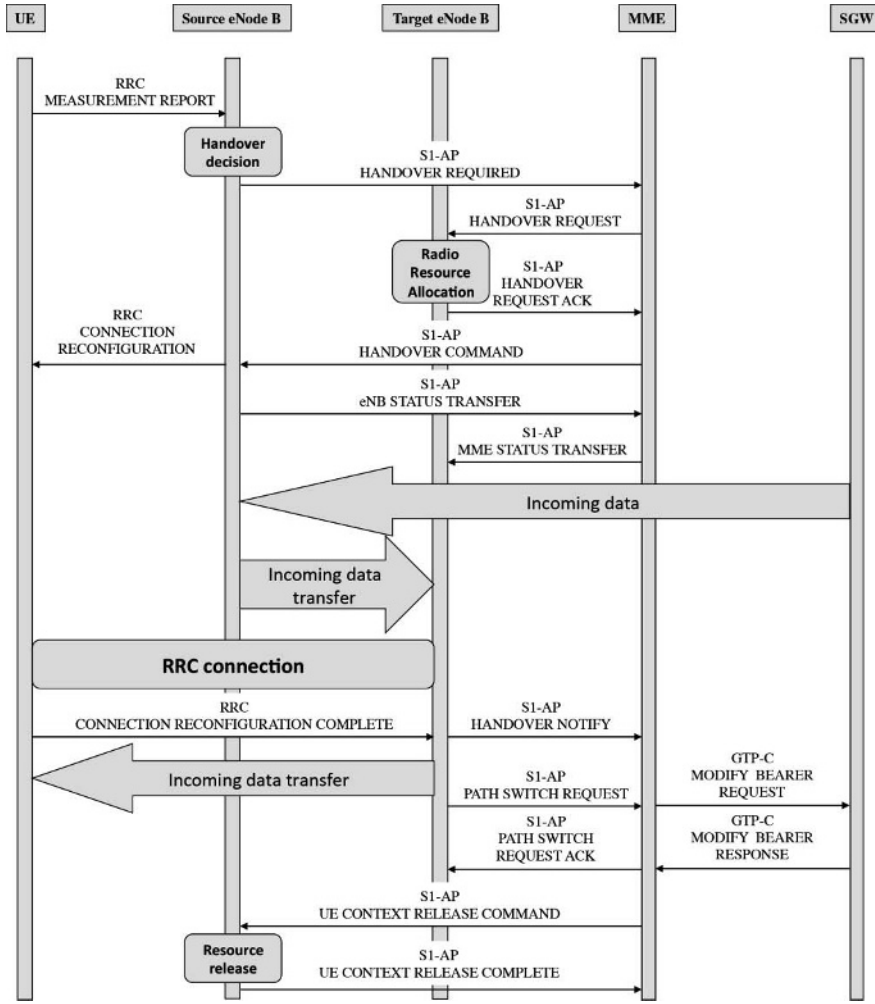


Figure 1.13. *Handover based on the S1 interface, without relocation*

The MME is no longer transparent to the handover mechanism, and plays the role of a signaling relay for the handover command between the source and target eNBs:

– upon receiving the message S1-AP HANDOVER REQUIRED from the source eNB, the MME generates and sends the message S1-AP HANDOVER REQUEST to the target eNB;

– upon receiving the message S1-AP HANDOVER REQUEST ACK from the target eNB, the MME sends the S1-AP HANDOVER COMMAND to the source eNB.

Similarly, the sequence number transfer takes place by way of the messages S1-AP ENB STATUS TRANSFER to the MME and S1-AP MME STATUS TRANSFER to the target eNB.

The modification of the S1-U bearer occurs by the same procedure as before.

The release of the context of the mobile at the source eNB is triggered by the MME, by sending the message S1-AP UE CONTEXT RELEASE COMMAND to the source eNB.

1.3.4.3. *Handover based on the S1 interface, with relocation*

The procedure of handover based on the S1 interface with relocation is illustrated in the following figures:

– Figure 1.14 for handover preparation;

– Figure 1.15 for handover execution;

– Figure 1.16 for context release.

The preparation phase begins with the message S1-AP HANDOVER REQUIRED, sent by the source eNB which has taken the handover decision. This information is relayed by the former MME to the new in the message GTP-C FORWARD RELOCATION REQUEST (Figure 1.14).

The information in the message S1-AP HANDOVER REQUEST ACK received by the new MME is relayed to the former one by the message GTP-C FORWARD RELOCATION RESPONSE (Figure 1.14).

The former and new MMEs create a specific tunnel between the former and new SGWs, by the messages CREATE INDIRECT DATA FORWARDING TUNNEL

REQUEST/RESPONSE. This tunnel is used to transfer the traffic data received by the source eNB (incoming data) to the target eNB during handover of the mobile (Figure 1.14).

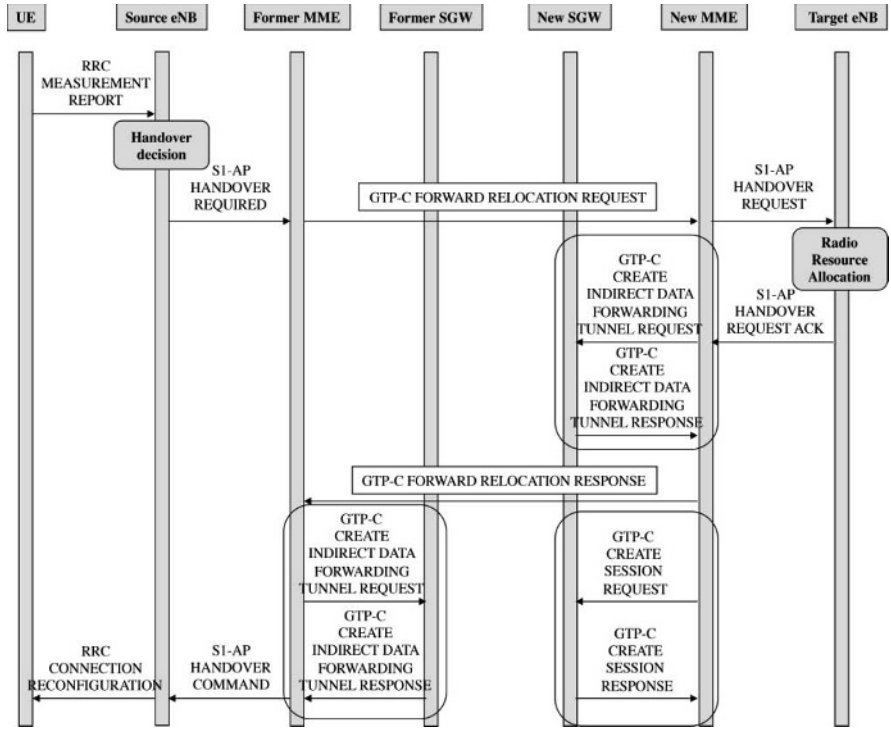


Figure 1.14. *Handover based on the S1 interface, with relocation – preparation*

The new MME creates a session with the new SGW to activate the S1-U bearer, by way of the messages GTP-C CREATE SESSION REQUEST/RESPONSE (Figure 1.14).

When the handover command has been sent to the mobile, the source eNB sends the message S1-AP eNB STATUS TRANSFER to the former MME. This information is relayed to the new MME by the message GTP-C FORWARD ACCESS CONTEXT NOTIFICATION, and then to the target eNB by the message S1-AP MME STATUS TRANSFER (Figure 1.15).

When the mobile is connected to the target eNB, the new eNB sends the message S1-AP HANDOVER NOTIFY to the new MME. This information is relayed to the

former MME by the message GTP-C FORWARD RELOCATION NOTIFICATION (Figure 1.15).

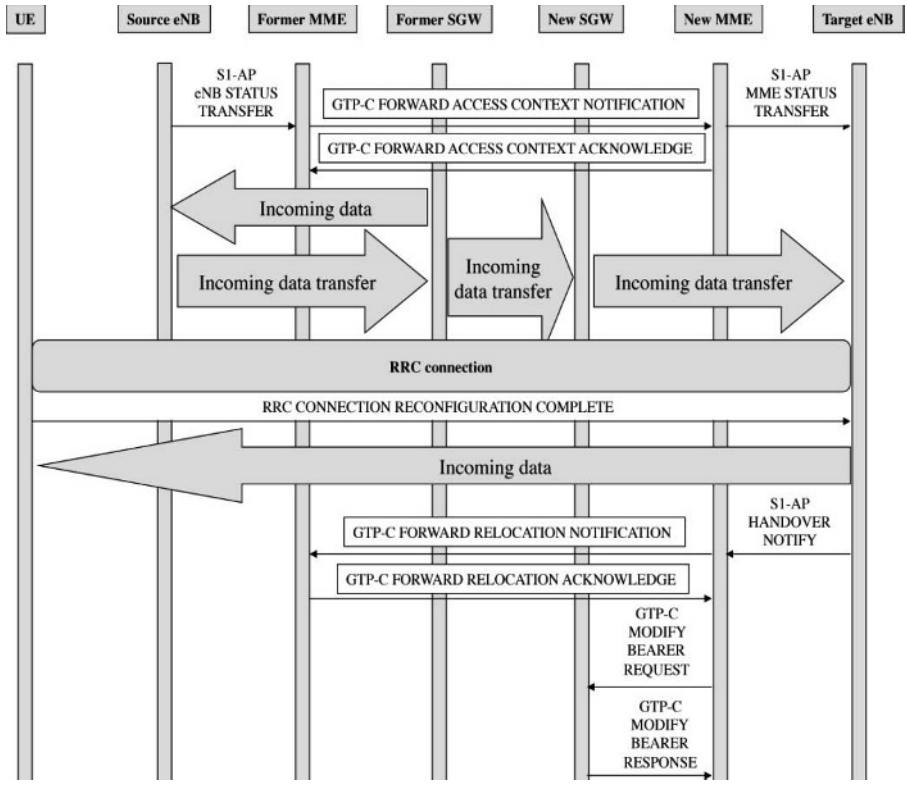


Figure 1.15. *Handover based on the S1 interface, with relocation – execution*

The last phase is the release of the following contexts and bearers:

– the context of the mobile in the source eNB, by the former MME's sending of the message S1-AP UE CONTEXT RELEASE (Figure 1.16);

– the S1-U bearer between the former SGW and the source eNB, by the exchange of the messages GTP-C DELETE SESSION REQUEST/RESPONSE between the former MME and former SGW (Figure 1.16);

– the specific tunnel created between the former and the new SGW, by the exchange of the messages DELETE INDIRECT DATA FORWARDING TUNNEL REQUEST/RESPONSE (Figure 1.16).

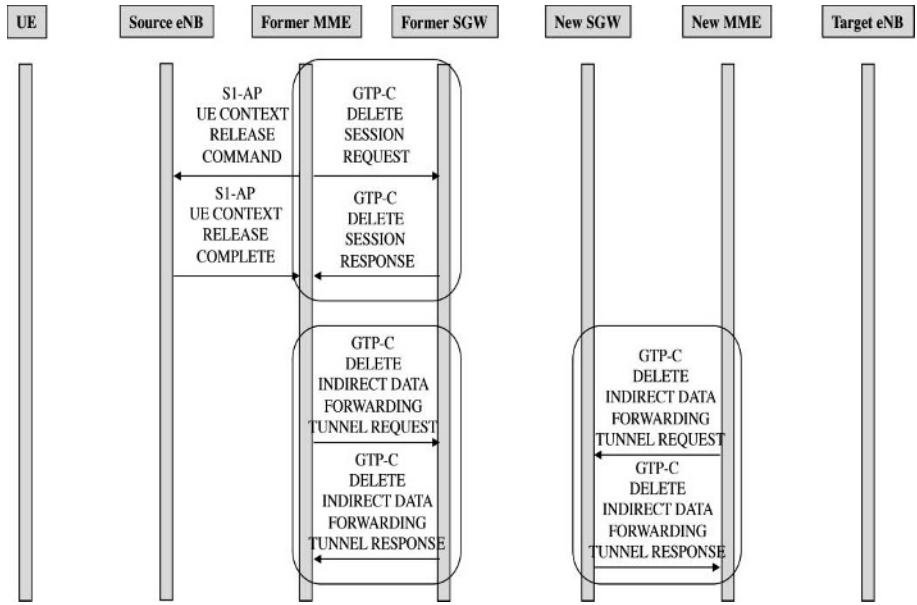


Figure 1.16. *Handover based on the S1 interface, with relocation – release*