NETMANIAS
www.netmanias.com

NMC
CONSULTING GROUP
www.nmcgroups.com

EMM Procedure 6. Handover without TAU

Part 2. X2 Handover

Table of Contents

I. Introduction

II. Concept of X2 Handover

III. Procedure of X2 Handover

IV. EPS Entity Information: Before/After X2 Handover

V. Closing

This document will describe the procedure for X2 handover performed in an intra-LTE environment, as defined as EMM Case 6 in our technical document, "Eleven EMM Cases in an EMM Scenario". First, features related to handover on X2 protocol will be discussed, followed by detailed procedures of X2 handover. We will learn how a handover between eNBs is prepared and performed without EPC intervention, and how DL packets are forwarded through a direct tunnel between two eNBs during the handover interruption time for seamless service provision. We will also look into how EPC gets involved in switching the EPS bearer path after a handover. Finally, we will examine how the information elements in EPS entities are different before and after the X2 handover procedure.

March 21, 2014

(Initial Released: July 05, 2012)

www.netmanias.com

NMC Consulting Group (tech@netmanias.com)

About NMC Consulting Group

NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.

Netmanias LTE Technical Documents

Visit http://www.netmanias.com to view and download more technical documents.

Index	Topic	Document Title	Document presented here
1	Network Architecture	LTE Network Architecture: Basic	
2	Identification	LTE Identification I: UE and ME Identifiers	
3		LTE Identification II: NE and Location Identifiers	
4		LTE Identification III: EPS Session/Bearer Identifiers	
5	Security	LTE Security I: LTE Security Concept and LTE Authentication	
6		LTE Security II: NAS and AS Security	
7	QoS	LTE QoS: SDF and EPS Bearer QoS	
8	EMM	LTE EMM and ECM States	
9		Eleven EMM Cases in an EMM Scenario	
10		LTE EMM Procedure 1. Initial Attach - Part 1. Cases of Initial Attach	
11		LTE EMM Procedure 1. Initial Attach - Part 2. Call Flow of Initial Attach	
12		LTE EMM Procedure 2. Detach	
13		LTE EMM Procedure 3. S1 Release	
14		LTE EMM Procedure 4. Service Request	
15		LTE EMM Procedure 5. Periodic TAU	
16		LTE EMM Procedure 6. Handover without TAU - Part 1. Overview of LTE Handover	
17		**LTE EMM Procedure 6. Handover without TAU - Part 2. X2 Handover**	**O**
18		LTE EMM Procedure 6. Handover without TAU - Part 3. S1 Handover	
19		LTE EMM Procedure 7. Cell Reselection without TAU	
20		LTE EMM Procedure 8 & 9. Handover and Cell Reselection with TAU	
21		LTE EMM Procedure 10 & 11. Move to Another City and Attach	
22	PCC	LTE Policy and Charging Control (PCC)	
23	Charging	LTE Charging I: Offline	
24		LTE Charging II: Online (TBD)	
25	IP Address Allocation	LTE IP Address Allocation Schemes I: Basic	
26		LTE IP Address Allocation Schemes II: A Case for Two Cities	

Abbreviations

AMBR	Aggregated Maximum Bit Rate
ARP	Allocation and Retention Priority
AS	Access Stratum
ASME	Access Security Management Entity
C-RNTI	Cell Radio Network Temporary Identifier
DL	Downlink
DRB	Data Radio Bearer
EARFCN	E-UTRA Absolute Radio Frequency Channel Number
ECGI	E-UTRAN Cell Global Identifier
EMM	EPS Mobility Management
eNB	Evolved Node B
EPS	Evolved Packet System
E-RAB	E-UTRAN Radio Access Bearer
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GTP	GPRS Tunneling Protocol
HFN	Hyper Frame Number
HSS	Home Subscriber Server
LTE	Long Term Evolution
MME	Mobility Management Entity
NAS	Non Access Stratum
NCC	Next hop Chaining Counter
NH	Next Hop
PCI	Physical Cell ID
PDCP	Packet Data Convergence Protocol
P-GW	Packet Data Network Gateway
QCI	QoS Class identifier
RRC	Radio Resource Control
S1AP	S1 Application Protocol
SCTP	Stream Control Transmission Protocol
S-GW	Serving Gateway
SN	Sequence Number
SON	Self-Organizing Networks
TA	Tracking Area
TAI	Tracking Area Identity
TAU	Tracking Area Update
TEID	Tunnel Endpoint IDentifier
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UL	Uplink
X2AP	X2 Application Protocol

I. Introduction

In the previous document, "EMM Case 6. Handover without TAU – Part 1. Overview of LTE Handover" [1], we have discussed the procedures related to LTE handover, and learned that LTE handover is a "UE-assisted/network-controlled" process that is reported by UE, and determined by eNB. This document will focus on procedures for X2 handover that is performed through the x2 interface in an intra-LTE environment. So, we will assume both source and target eNBs are connected to the same MME/S-GW, and are located in a TA that IS in the Tracking Area Identifier (TAI) list for the associated UE.

Chapter II describes the concept of X2 handover, and Chapter III provides detailed procedures of X2 handover. Finally, Chapter IV will summarize how information elements in EPS entities are different before and after the X2 handover.

II. Concept of X2 Handover

2.1 X2 Protocol Stacks

X2 handover is performed between a source eNB and a target eNB through the X2 interface. In an LTE network, these two eNBs can directly communicate with each other via the X2 interface, which differentiates the network from its precedents (2G and 3G). In a 2G or 3G network, the only way an eNB could learn of the status of its neighboring eNB was through control by packet core nodes. However, now LTE networks allow eNBs to directly exchange status information with each other via the X2 interface, and to independently perform handovers without any intervention by EPC nodes. Figure 1 shows the protocol stacks over the X2 interface in control and user planes.

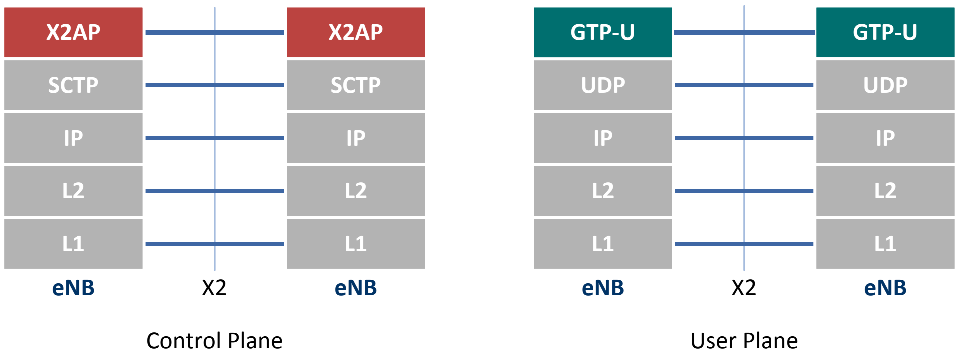


Figure 1. Protocol Stacks over X2 Interface

In the control plane, two eNBs provide multiple users with X2 Application Protocol (X2AP) signaling through a single Stream Control Transmission Protocol (SCTP) connection. In the X2AP layer, users are identified by eNB UE X2AP ID (Old eNB UE X2AP ID, New eNB UE X2AP ID)[1]. In the data plane, the two eNBs are connected through a GPRS Tunneling Protocol (GTP) tunnel, as in S1/S5 bearer. A unique GTP tunnel is generated for each user[2], and each tunnel is identified by its allocated Tunnel Endpoint Identifiers (TEIDs).

[1] Old eNB UE X2AP ID is allocated by a source eNB while New eNB UE X2AP ID is allocated by a target eNB.
[2] In case of a user with more than one bearer, this tunnel is generated for each bearer. However, this document discusses only the cases where each user has only one bearer.

2.2 X2AP Functions

Table 1 lists the functions that are performed through X2AP signaling, and the elementary procedures related to each function [2]. As seen below, X2AP signaling information can be roughly classified into two kinds, the one related to load/interference (i.e. Load Management function in the table) and the one related to handover (i.e. Mobility Management, Mobility Parameter Management, Mobility Robustness Optimization functions in the table).

Table 1. X2AP Functions and Elementary Procedures [2]

Function	Elementary Procedure(s)
Mobility Management	Handover Preparation SN Status Transfer UE Context Release Handover Cancel
Load Management	Load Indication Resource Status Reporting Initiation Resource Status Reporting
Reporting of General Error Situations	Error Indication
Resetting the X2	Reset
Setting up the X2	X2 Setup
eNB Configuration Update	eNB Configuration Update Cell Activation
Mobility Parameters Management	Mobility Settings Change
Mobility Robustness Optimization	Radio Link Failure Indication Handover Report
Energy Saving	eNB Configuration Update Cell Activation

Compared to 2G/3G networks, broadband networks like LTE have less cell coverage but a lot more base stations to cover. Thus, conventional ways of configuring and managing networks used in 2G/3G networks are not efficient any more. To address this issue, now in LTE networks, X2AP protocol is defined, providing Self-Organizing Networks (SON) functionality. This allows an eNB to connect to its neighbor eNB(s), collect their status information, and use the collected information to automatically configure and optimize its parameters.[3] Among the X2AP functions listed in Table 1, those related to SON are as follows:

- **Load Management**: enhances the interception performance among cells by exchanging load and interference information between two eNBs
- **eNB Configuration Update**: performs automatic eNB configuration
- **Mobility Parameters Management**: negotiates on handover triggering setting information among peer eNBs and uses the information for handover optimization
- **Mobility Robustness Optimization**: provides information on a handover failure event
- **Energy Saving**: help eNBs to consume less energy by exchanging information on cell activation/deactivation

[3] SON functionality is out of the scope of this document. This document will focus on the elementary procedures of handover, and will not discuss Mobility Parameter Management and Mobility Robustness Optimization functions that are more related to handover parameter optimization.

2.3 X2 Messages Relating to Mobility Management Function

Table 2 shows messages used particularly in the Mobility Management function - among all the X2 functions listed in Table 1 above - relating to handovers to be discussed in Chapter III below [2]. We can see a response message from a target eNB is required during the handover preparation procedure.

- **Handover Request** message: This message is used during the handover preparation phase. It is delivered by a source eNB to a target eNB, and includes a user's UE context.
- **Handover Request Acknowledge** message: This message is used during the handover preparation phase. It is delivered by the target eNB to the source eNB if resource allocation is successfully completed by the target eNB.
- **Handover Preparation Failure** message: This message is used during the handover preparation phase. It is delivered by the target eNB to the source eNB if resource allocation at the target eNB fails.
- **SN Status Transfer** message: This message is used during the handover execution phase. The source eNB delivers it to the target eNB to indicate from which packet it should receive or send.
- **UE Context Release** message: This message is used during the handover completion phase. The target eNB sends it to the source eNB, to request release of the UE context.
- **Handover Cancel** message[4]: This message is used during the handover preparation phase. The source eNB sends it to the target eNB when it needs to cancel a handover in preparation.

Table 2. X2 Messages for Mobility Management Function [2]

Procedure	Initiating Message	Response Message	
		Successful	Unsuccessful
Handover Preparation	**Handover Request**	**Handover Request Acknowledge**	**Handover Preparation Failure**
SN Status Transfer	**SN Status Transfer**	-	-
UE Context Release	**UE Context Release**	-	-
Handover Cancel	**Handover Cancel**	-	-

2.4 X2 Handover Procedure at a Glance

As seen in the previous document [1], an X2 handover procedure consists of preparation, execution and completion phases. Before we go further into detail, we will briefly preview the X2 handover procedure. Figure 2 illustrates at a glance the procedures required before, during (preparation, execution and completion phases) and after X2 handover. For convenience's sake, S-GW and P-GW are marked as SAE-GW, and source and target eNBs are marked as SeNB and TeNB, respectively.

[4] Chapter III covers successful X2 handovers only, and hence Handover Cancel messages are not discussed.

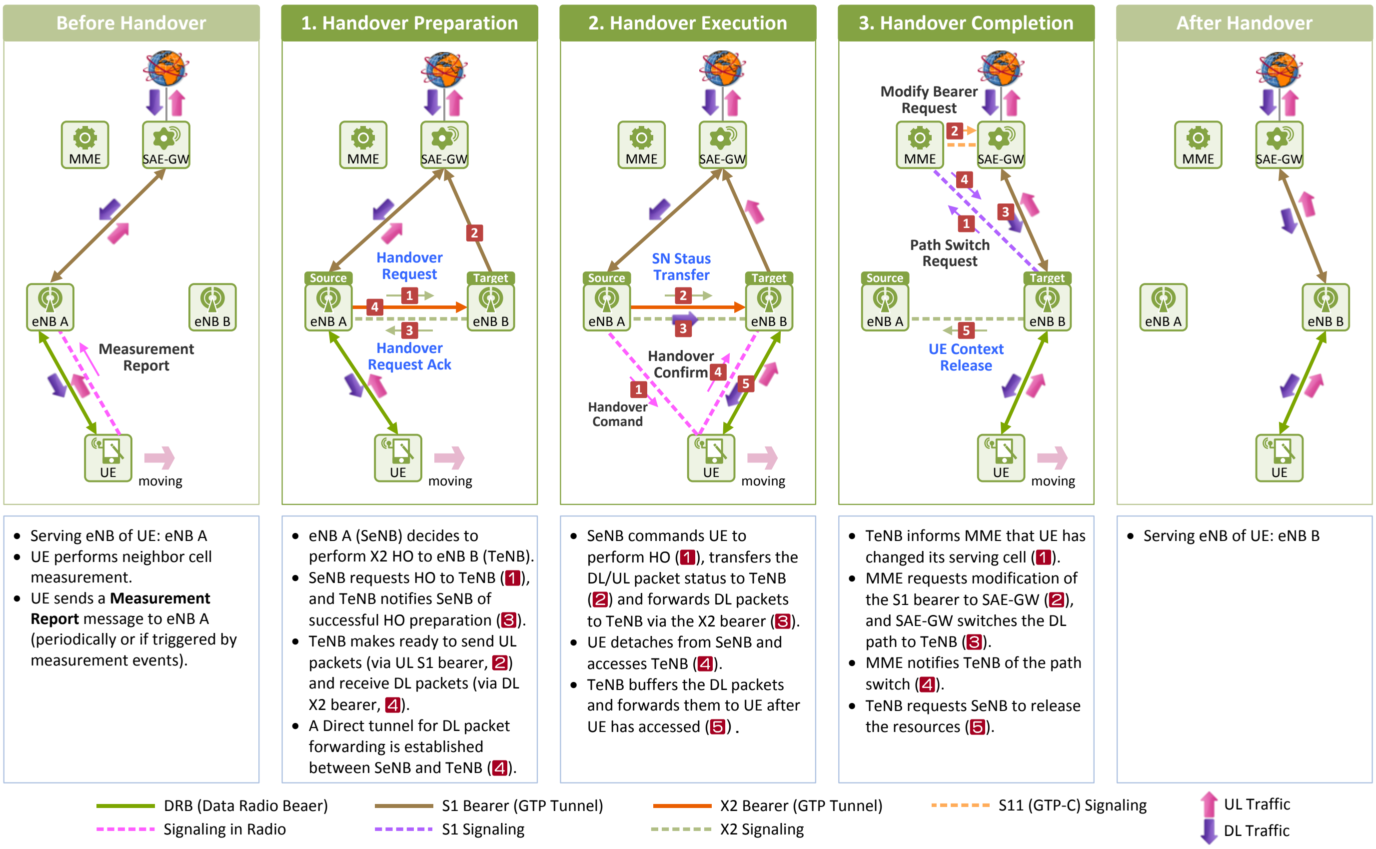


Figure 2. Simplified Procedure of X2 Handover

Before X2 Handover

In the figure above, the UE is being served through eNB A (a serving cell in eNB A, to be more exact) that it has accessed to. When the UE detects a measurement event, it sends a **Measurement Report** message to eNB A.

X2 Handover Preparation

The source eNB (i.e. eNB A in the figure) chooses a target eNB (i.e. eNB B in the figure) to handover to, based on the neighbor cell list information it has kept and the information on the signal strength of the neighbor cells included in the **Measurement Report** message.[5] Next, it prepares an X2 handover with the target eNB through X2 signaling. In the meantime, the target eNB allocates resources in advance so that the same services currently available to the user at the source eNB are readily available at the target eNB as well. Also, to ensure a fast handover, the target eNB sends all the information needed for the user to connect to the target cell (e.g. C-RNTI) to the source eNB, which then forward the same to the UE, initiating the handover execution phase. The target eNB allocates resources as follows:

- When the source eNB sends the target eNB a **Handover Request** message that includes the user's UE context (1),
- The target eNB:
  - obtains S1 bearer information (S1 S-GW TEID) to establish an UL S1 bearer through which to transport UL packets (2).
  - allocates TEID for the X2 transport bearer (GTP-U tunnel) through which to receive DL packets

5 Source eNB may select cell(s) other than the one(s) reported by UE, as its target eNB. Cases of selecting more than one target eNB are beyond the scope of this document, and hence this document concerns a case of selecting only one target eNB.

while UE attempts to access the target eNB.
  - allocates DRB resources and C-RNTI to be used by UE in the target cell.
  - sends a **Handover Request Ack** message to the source eNB (3).
- Upon receiving the message, the source eNB establishes an X2 transport bearer through which to send DL packets (4).

X2 Handover Execution

Once handover preparation between the two eNBs is completed, it is time to have the UE perform a handover.

- The source eNB:
  - instructs the UE to perform a handover to the target cell by sending it a **Handover Command** message that includes all the information needed to access the target cell (1).
  - informs from which UL/DL packet the target eNB should receive or send when communicating with the UE by sending the target eNB an **SN Status Transfe**r message (2).
  - forwards the DL packets received from S-GW to the target eNB through the X2 transport bearer established between itself and the target eNB (3).
- The UE detaches from the source eNB and accesses to the target eNB (4).
- The target eNB becomes capable of sending and receiving packets once the UE has successfully accessed (5).

X2 Handover Completion

As seen so far, all the procedures performed during the handover execution phase (i.e. after the source eNB decided to perform a handover, and until the UE finally was connected to the target eNB) were just between the two eNBs, and no information about the handover was reported to EPC (MME). Now that the handover is completed, the target eNB informs EPC as follows:

- Once the UE has accessed, the target eNB informs EPC and sends a **Path Switch Request** message to MME so that the EPS bearer path can be modified accordingly (1).
- When receiving the message, the MME becomes aware of the UE's new serving cell. Then, it requests S-GW for S1 bearer modification (2).
- Upon the request, the S-GW establishes a DL S1 bearer (S1 Target eNB TEID) that connects to the target eNB. Then it stops sending DL packets to the source eNB, and begins to send them to the target eNB through the newly established DL bearer (3).
- The MME informs the target eNB that the DL S1 bearer path has been modified (4).
- The target eNB sends the source eNB a **UE Context Release** message, allowing the source eNB to release the UE context (5).

After X2 Handover

The UE is now being served through eNB B (the serving cell at eNB B, to be more exact) that it has accessed.

2.5 UE State and Connection Information Before and After X2 Handover

Figure 3 illustrates the connection establishments in the user/control planes, and the UE and MME states before, during and after the X2 handover.

- **Before X2 Handover**

  The UE stays in **EMM-Registered** and **ECM/RRC-Connected** and keeps all the resources allocated by E-UTRAN and EPC.

- **During X2 Handover**

  Even during the handover phase, the UE's state in the NAS layer remains unchanged, and an X2 bearer[6] and X2 signaling connection are established over the X2 interface. In Figure 3, Step 2) shows the connections and states while the handover is interrupted during the handover execution phase. During this period, no radio link connection is active, but the UE still remains Connected.

- **After X2 Handover**

  The UE remains in **EMM-Registered** and **ECM/RRC-Connected** states. The E-RAB (DRB + S1 bearer) path is switched to access to a new eNB in the user plane while a new RRC connection and S1 signaling connection (eNB(B) S1AP UE ID) are established in the control plane.

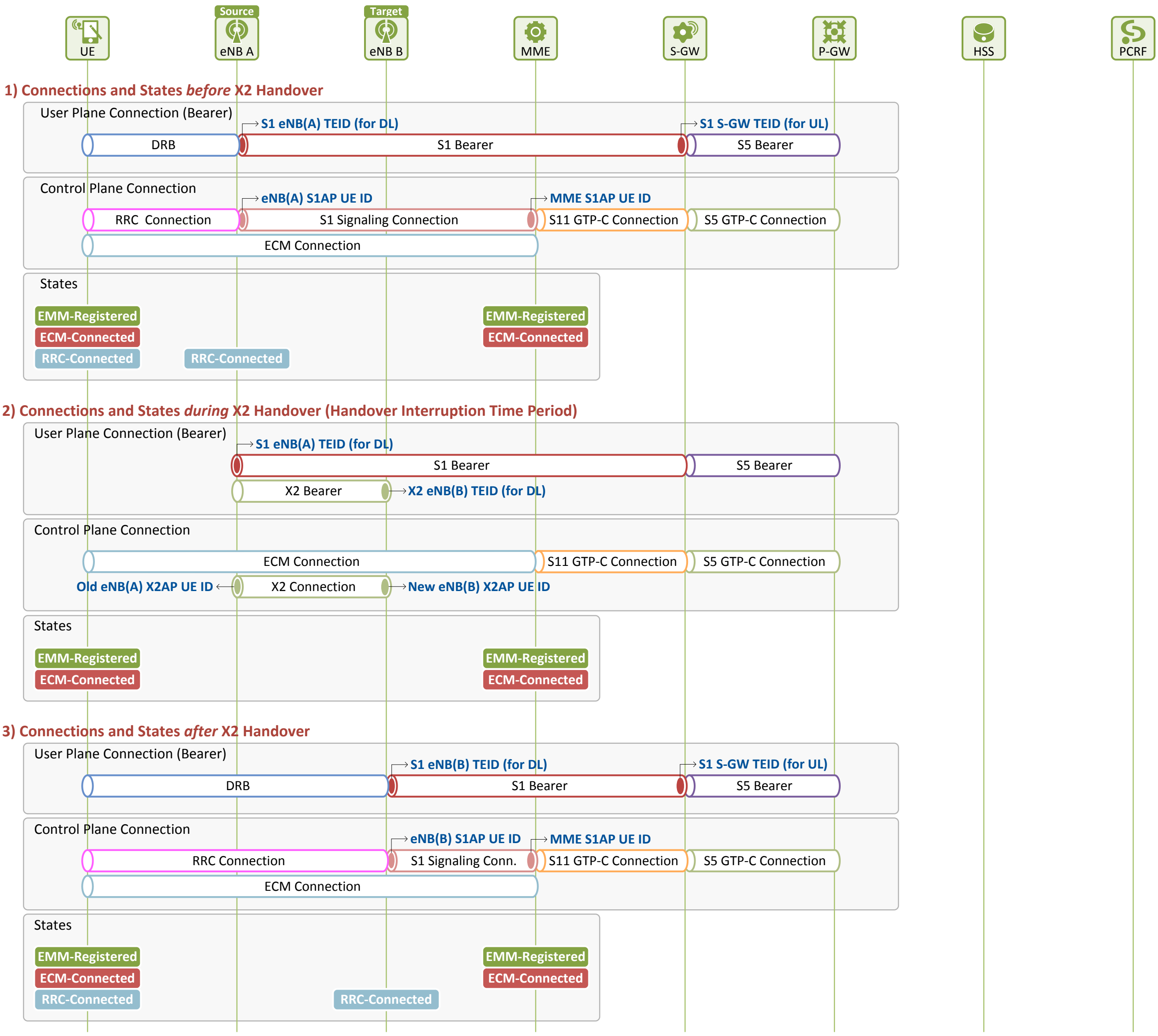


Figure 3. Connections and States before/after X2 Handover

6 If UE has more than one EPS bearer, more than one X2 bearer can be established. This document however discusses only cases where just one EPS bearer is established.

III. Procedure of X2 Handover

Now we will look into the detailed X2 handover procedures.[7] Figure 4 illustrates the EPS bearer and signaling connections prior to the X2 handover, and the detailed procedures of the X2 handover preparation phase.

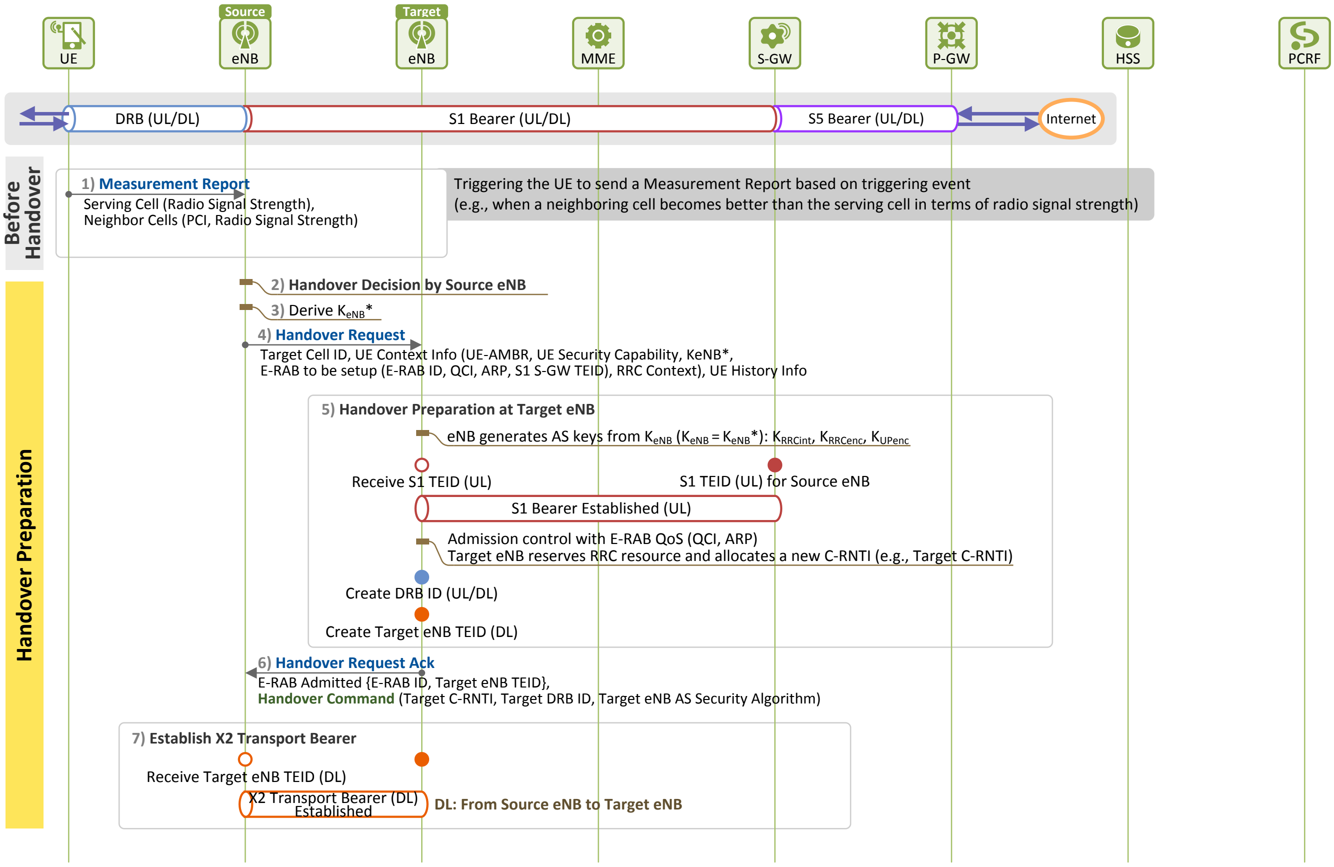


Figure 4. X2 Handover - Handover Preparation Phase

■ Before Handover

1) [UE → eNB] Measurement Report

As a measurement event is triggered,[8] the UE measures the signal strength of neighbor cells, and sends a **Measurement Report** message to its associated eNB (serving cell).

■ Handover Preparation

2) [Source eNB] Handover Decision

The source eNB selects a target eNB based on the information included in the **Measurement Report** message sent by the UE, and the neighbor cell list information it has kept. In actual handovers, there can be more than one target eNB candidate, or a neighbor cell other than the one(s) reported by UE may be selected as a target cell. However, we will assume that only one eNB where the cell included in the **Measurement Report** message belongs is selected as a target eNB in this document.

---

[7] We assume the UE's serving cell and the target cell are located in different eNBs for the purposes of this chapter.

[8] See our "LTE EMM Procedure 6. Handover without TAU - Part 1. Overview of Handover" document [1] and 3GPP TS 36.331 [3] for more information about measurement events.

3) [Source eNB] Deriving the AS Security Base Key (KeNB*) to be Used by the Target eNB

When a handover takes place, the serving eNB of a UE is switched. During this switch, RRC signaling messages and user packets still have to be delivered seamlessly and securely. Over the radio link, it is AS security keys that ensure secured delivery of such data. AS security keys are derived from K_{eNB}, the AS security base key[9]. K_{eNB} is derived from K_{ASME} by MME after user authentication, and sent to eNB[10]. However, because X2 handover is performed between two eNBs without any intervention by EPC (MME), the target eNB cannot obtain K_{eNB}^* (K_{eNB} to be used by the target eNB) from MME. So, the source eNB derives it and sends to the target eNB.

For this reason, once the source eNB decides to perform a handover, it derives K_{eNB}^* first, as seen in Figure 5. We can see that K_{eNB}^* is derived from K_{eNB} (the AS security base key of the source eNB), and the target cell's Physical Cell ID (PCI) and frequency (E-UTRA Absolute Radio Frequency Channel Number-Downlink (EARFCN-DL)).

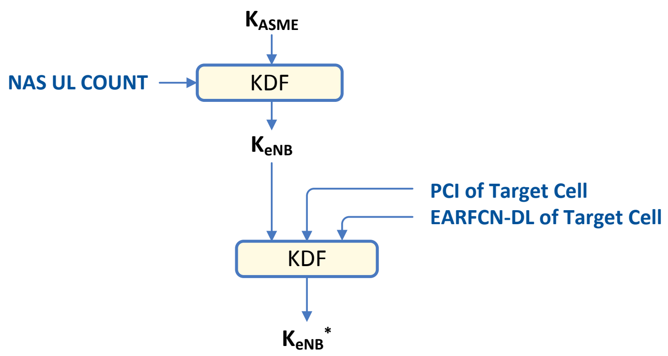


Figure 5. Derivation of K_{eNB}^* (for the 1st Handover)

4) [Source eNB → Target eNB] Requesting X2 Handover

The source eNB requests a handover by sending a **Handover Request** message to the target eNB. Through this message, it delivers the UE context information it has stored, and the UE history which shows the cells that the UE has connected to prior to the last handover to the target cell. The information included in the message is as follows:

Handover Request (Target Cell ID, UE Context Info(UE-AMBR, UE Security Capability, K_{eNB}^*, E-RAB to be setup (E-RAB ID, QCI, ARP, S1 S-GW TEID), RRC Context), UE History Info)

- **Target Cell ID**: the target cell's ECGI
- **UE Context Info**: UE context stored at the source eNB
  - **UE-AMBR**: provided by HSS, but can be modified by MME. This value can be set for eNB, and used to control the aggregated MBR value of non-GBR bearers.
  - **UE Security Capability**: security algorithms supported by UE (encryption and integrity algorithm)
  - **K_{eNB}^***: AS security base key generated by the source eNB for the target eNB's use, i.e. **K_{eNB}** to be used by the target eNB
  - **E-RAB to be setup:** UE's E-RAB information stored at the source eNB
- **UE History Info:** information about the cells that UE has accessed while staying Active, including each cell's ECGI, type and the duration of UE's stay in the cell.

[9] See our "LTE Security II" document [4] for more information about AS security.
[10] See our "LTE Security I" document [5] for more information about LTE user authentication.

5) [Target eNB] Preparing X2 Handover

Upon receiving the **Handover Request** message, the target eNB begins handover preparation to ensure seamless service provision for the UE.

(i) First, it derives AS security keys (K_{RRCint}, K_{RRCenc}, K_{UPenc}) from $K_{eNB}{}^{*}$ it received from the source eNB. Using these keys, the target eNB can communicate securely with the UE over the radio link when the UE accesses.

(ii) Next, the target eNB, based on the E-RAB to be setup information, checks if the same QoS provided by the source eNB is available at the target eNB as well. If available, it establishes an UL S1 bearer connecting to S-GW, by using the UL S1 bearer information (S1 S-GW TEID) stored at the source eNB.

(iii) Then, based on the E-RAB QoS information, the target eNB reserves RRC resources to be used by the UE over the radio link (e.g. DRB ID allocation, etc.), and allocates C-RNTI.

(iv) While the UE is performing a handover (i.e. after it disconnects from the source eNB, until it connects to the target eNB), DL packets arriving at the source eNB need to be forwarded to the target eNB. For this, the target eNB allocates X2 Target eNB TEID (DL TEID of X2 GTP tunnel) so that the source eNB can establish an X2 transport bearer (GTP tunnel).

6) [Source eNB ← Target eNB] Notifying the Source eNB of Preparation Completion

The target eNB sends the source eNB all the information about the resources prepared in Step 5), as included in a **Handover Request Ack**[11] message. The included information is as follows:

Handover Request Ack (E-RAB Admitted (E-RAB ID, Target eNB TEID), Handover Command (Target C-RNTI, Target DRB ID, AS Security Algorithm of Target eNB))

- **E-RAB Admitted**[12]: includes i) E-RAB ID allocated by the target eNB, and ii) TEID information of X2 transport bearer through which E-RAB packets are to be forwarded to the target eNB.
- **Handover Command**: Transparent Container, delivered by the target eNB to the source eNB, that contains information that UE needs to access the target eNB
  - **Target C-RNTI**: C-RNTI allocated by the target cell to identify UE
  - **Target DRB ID**: ID of DRB that the target eNB set to deliver user packets over the radio link
  - **AS Security Algorithm of Target eNB**: AS Security algorithm supported by the target eNB

7) [Source eNB] Establishing X2 Transport Bearer for DL Packets Delivery

Upon receipt of the **Handover Request Ack** message, the source eNB knows the target eNB can serve the UE. Then, using the X2 Target eNB TEID, it begins to establish an X2 transport bearer so that DL packets can be forwarded to the target eNB during the handover execution phase.

[11] The full name of the message defined in the standards is "Handover Request Acknowledge". However, it is referred to as "Handover Request Ack" for short in this document.

[12] Should be E-RAB Admitted List, if Target eNB has more than one E-RAB established. However, this document assumes there is only one E-RAB established.

■ Handover Execution

Figure 6 shows the procedure for X2 handover execution phase.

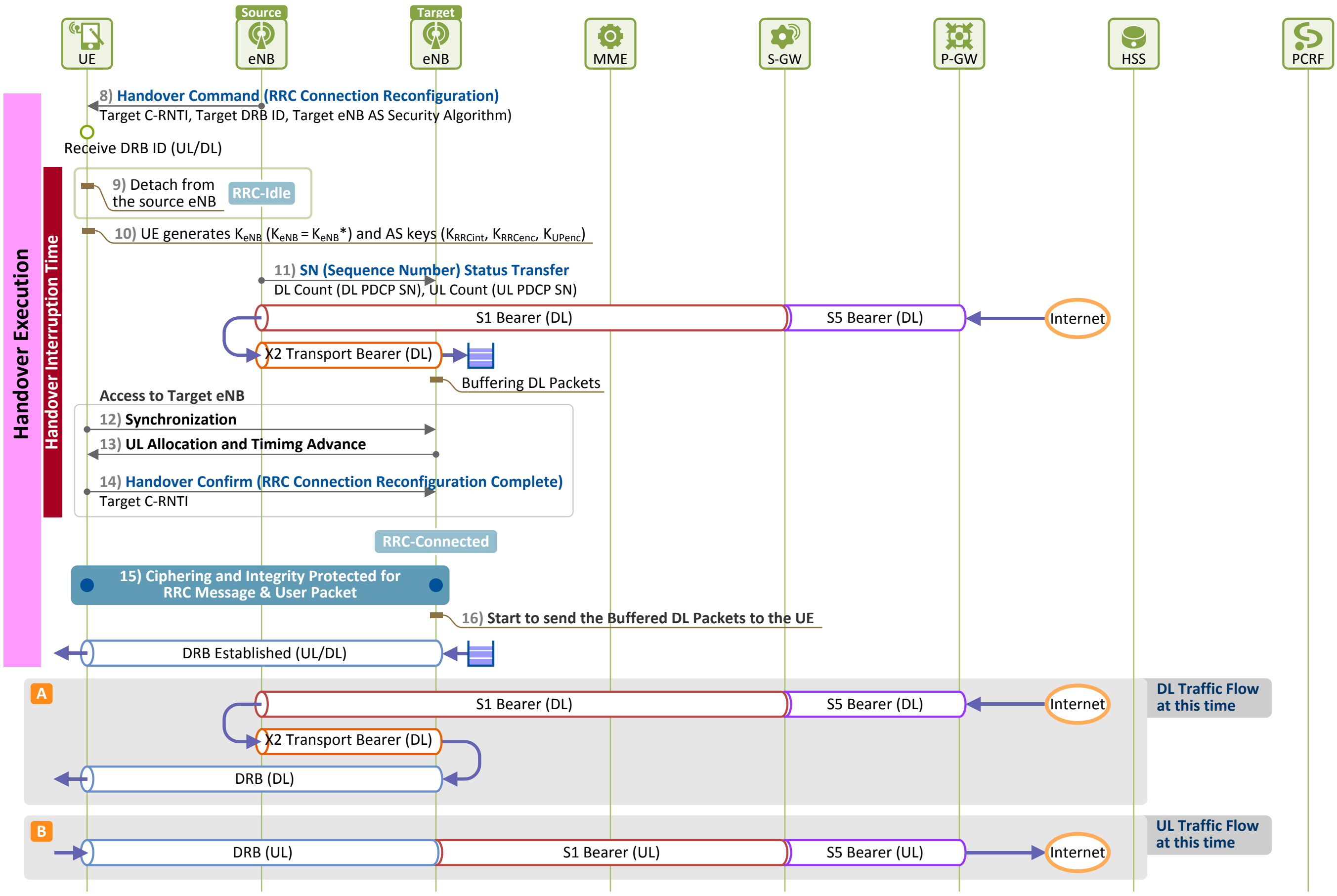


Figure 6. X2 Handover - Handover Execution Phase

8) [UE ← Source eNB] Commanding a Handover

Once the source eNB completes the handover preparation with the target eNB, it orders the UE to perform a handover by sending a **Handover Command** message.

9) [UE] Executing a Handover

The UE, from the received **Handover Command** message, obtains C-RNTI and DRB ID to be used at the target cell, and detaches from the source eNB. Now, all packet delivery between the UE and the source eNB is stopped, and the handover interruption time[13] period begins.

10) [UE] AS Security Setup

The UE derives AS security keys to be used over the radio link of the target eNB. First it derives K_{eNB}* (AS base key for the target eNB) from the source eNB's K_{eNB}, the target cell's PCI and frequency (the relevant key derivation functions are as seen in Figure 5). Next, it derives AS security keys for the target eNB (K_{RRCint}, K_{RRCenc}, K_{UPenc}) by using the AS security algorithms that the target eNB selected.

13 See our "LTE EMM Procedure 6. Handover without TAU – Part 1. Overview of Handover" document [1] for more information about the handover interruption time.

11) [Source eNB → Target eNB] Notifying the No. of the Packet to Send/Receive

The source eNB informs the target eNB from which packet it should send to (or receive from) the UE by sending a **SN Status Transfer** message that includes DL Count and UL Count. Here, the count values are PDCP PDU Counts, and each Count is a 32-bit value consisting of Hyper Frame Number (HFN) and PDCP Sequence Number (SN). The information included in the message is as follows:

SN Status Transfer (DL Count, UL Count)

- **DL Count**: Count of the first packet to send to the UE
- **UL Count**: Count of the first packet to receive from the UE

After sending the **SN Status Transfer** message to the target eNB, the source eNB begins to forward DL packets arriving from S-GW to the target eNB through the X2 transport bearer (GTP tunnel) established over the X2 interface. The target eNB buffers the packets and waits for completion of the UE's access.

12) ~ 14) [UE, Target eNB] UE's Access to the Target eNB

12) The UE detects the synchronization signal from the target eNB to perform synchronization to the target eNB. Once synchronized, the UE initiates non-contention based random access. **13)** The target eNB sends the UE the timing alignment information (timing advance) and UL Grant. **14)** The UE sends the target eNB a **Handover Confirm** message as included in the **RRC Connection Reconfiguration Complete** message. Now, the UE can send/receive packets to/from the target eNB, and the handover interruption time period is ended.

15) [UE - Target eNB] Secure Communication over the Radio Link

All RRC signaling messages and user packets sent over the radio link between the UE and the target eNB are now securely delivered using the AS security keys. RRC signaling messages are integrity protected and encrypted while user packets are encrypted before being sent.

16) [Target eNB] Resuming DL Packet Delivery to the UE

As the UE is successfully connected to the target eNB, the target eNB starts to send the buffered DL packets to the UE through the following path (See [A] in Figure 6):

S5 bearer → S1 bearer (@source eNB) → X2 bearer → DRB (@target eNB)

In case packets are sent by the UE, the target eNB checks if the UL packets are received in the correct order, and then forwards them to S-GW through the following path (See [B] in Figure 6):

DRB (@target eNB) → S1 bearer (@target eNB) → S5 bearer

■ Handover Completion

Figure 7 illustrates the procedure for X2 handover completion phase.

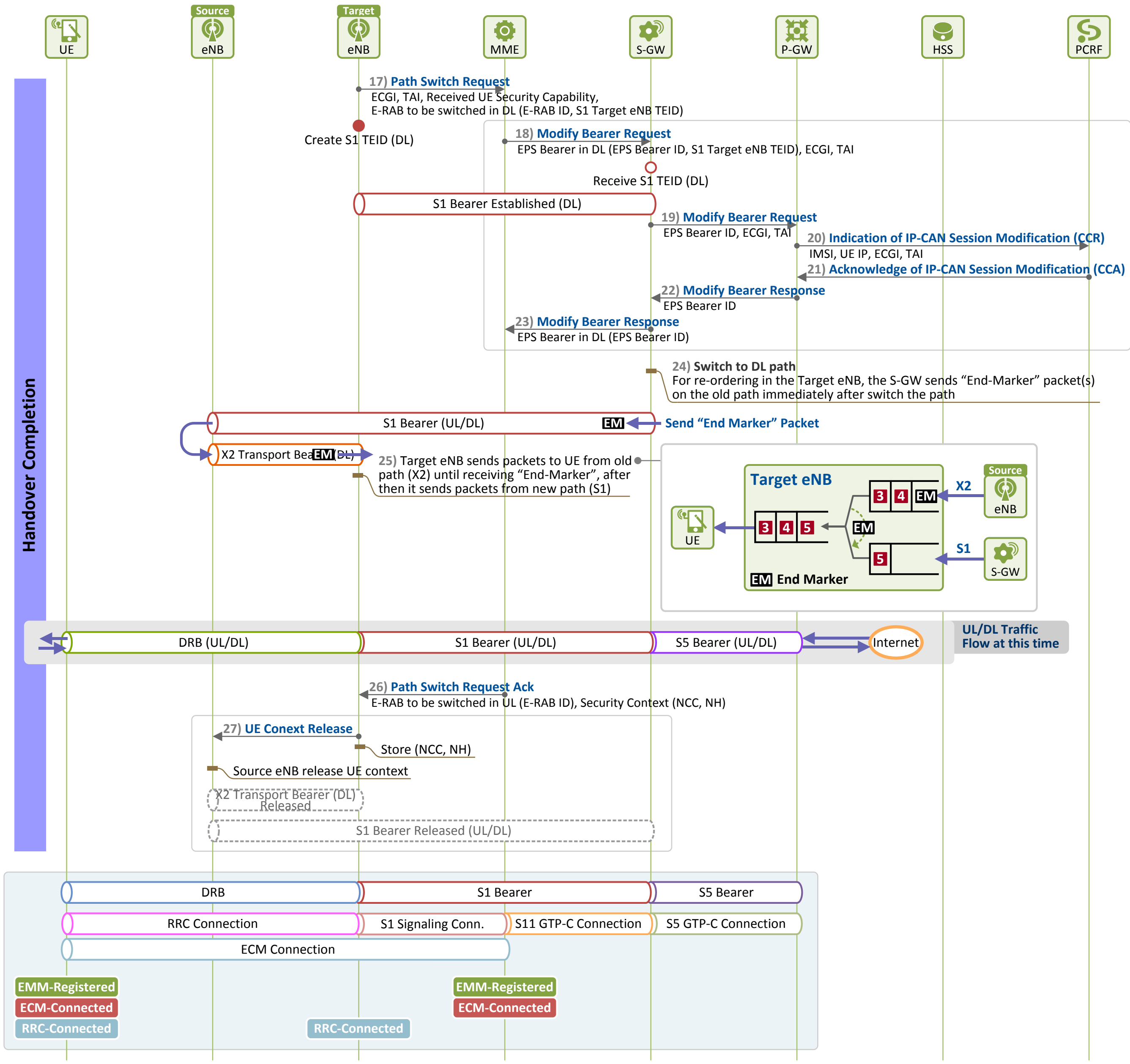


Figure 7. X2 Handover - Handover Completion Phase

17) [Target eNB → MME] Requesting the EPS Bearer (S1 Bearer) Path Switch

The target eNB notifies EPC (MME) that the UE's serving cell is switched by sending a **Path Switch Request** message, and requests for switch of EPS bearer path.

18) ~ 23) Modifying the EPS Bearer

The MME forwards the S1 Target eNB TEID that was allocated by the target eNB to the S-GW by sending a **Modify Bearer Request** message. This way it informs the S-GW that the DL S1 bearer has been switched, and asks to switch the bearer path accordingly. Then the S-GW establishes a DL S1 bearer connecting to the target eNB, as requested. Some S-GWs, according to the options set during UE's initial attach, are required to report if the UE's serving cell is changed while an EPS session is created. In such case, the S-GW sends a **Modify Bearer Request** message to P-GW, having the P-GW report to PCRF, according to the EPS session modification procedure, that the UE's serving cell has been changed.

24) [S-GW] Modifying the EPS Bearer Path and Sending EM Packets

Now that the DL S1 bearer path is modified, the S-GW switches the DL packet delivery path into the DL S1 bearer that is connected to the target eNB. For this, first it sends End Marker (EM) to indicate the last packet to the DL S1 bearer connected to the source eNB. Then, it sends DL packets to the target eNB through the modified DL S1 bearer.

25) [Target eNB] Packet Re-ordering

Now the target eNB receives DL packets forwarded from the source eNB through the X2 transport bearer AND those sent by the S-GW that has the modified downlink S1 bearer. So, it should be able to deliver them to the UE in the correct order. First, the target eNB forwards the DL packets received from the X2 transport bearer to the UE. Then when EM arrives, it knows that the packet was the last one from the X2 transport bearer, and thereafter it sends the DL packets received from the S1 Bearer to the UE.

26) [Target eNB ← MME] Notifying the Modified Bearer Path

The MME notifies the target eNB that the S-GW has switched the EPS bearer (S1 bearer) path, by sending a **Path Switch Request Ack** message. Then, it forwards the security context required for handover {NH Chaining Count (NCC), Next Hop (NH)} so that the target eNB can use in UE's next handover to another cell.[14]

27) [Source eNB ← Target eNB] Notifying to Release UE Context

The target eNB keeps {NCC, NH}, and sends the source eNB a **UE Context Release** message, informing the UE context may be released now that the UE's bearer path has been switched.

[14] Security is beyond the scope of this document, and hence details about security will not be discussed here.

IV. EPS Entity Information: Before/After X2 Handover

This chapter will describe how information elements in the EPS entities are different before and after the X2 handover. All the information elements are categorized into UE ID, UE Location, Security, and EPS Session/Bearer information.

4.1 Before X2 Handover

Before X2 handover, UE stays in **EMM-Registered** and **ECM/RRC-Connected** state. Therefore, all the information elements stored after the initial attach in the EMM Case 1, or the service request in the EMM Case 4, remain the same in the EPS entities until an X2 handover procedure is performed. That is, all of the resources allocated by E-UTRAN and EPC, and the UE context information are stored in the EPS entities. Figure 8 lists the information elements stored in each EPS entity before an X2 handover procedure.

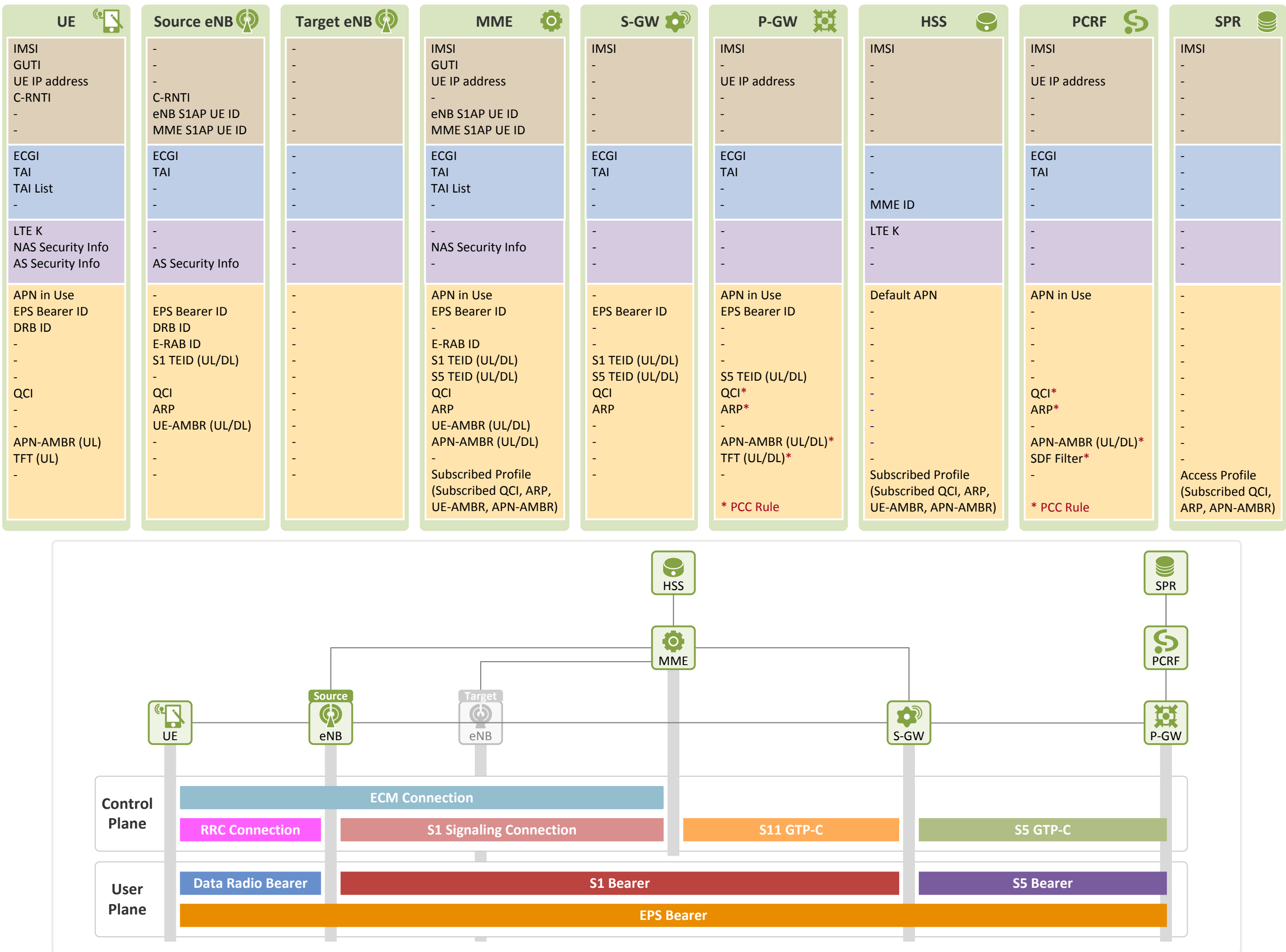


Figure 8. Information in EPS entity before X2 Handover

4.2 After X2 Handover

After X2 handover, UE still remains in **EMM-Registered** and **ECM/RRC-Connected** state. The types of information elements stored in each EPS entity remain unchanged, but UE location information is modified. The E-UTRAN resources and UE context are all released at the source eNB, but set for the target eNB. Figure 9 lists the information elements stored in each EPS entity after an X2 handover procedure (in case the target eNB supports the QoS supported by the source eNB, and reporting to PCRF is required according to the PCC policies when UE's serving cell is changed). In the figure, information elements that are changed after the handover are marked in blue.

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

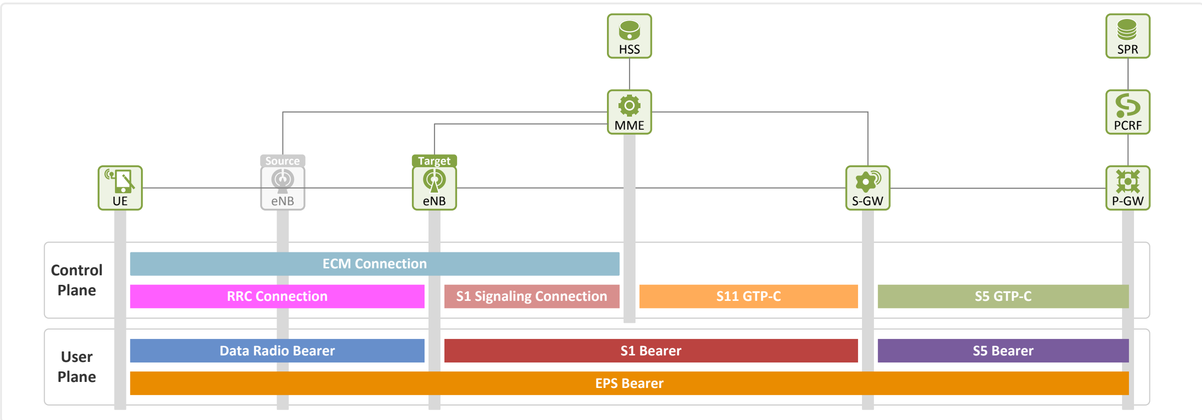


Figure 9. Information in EPS entity after X2 Handover

V. Closing

We have so far discussed the X2 handover procedure performed in an intra-LTE environment where neither MME nor S-GW is changed after the procedure. X2 handovers are performed by source and target eNBs without EPC's intervention. We also learned that DL packets are forwarded through the X2 transport bearer during the handover interruption time, to prevent packet loss. In the third document, we will explain the detailed S1 handover procedure in an intra-LTE handover, and the difference between S1 and X2 handovers.

References

[1] Netmanias Technical Document, "LTE EMM Procedure 6. Handover without TAU – Part 1. Overview of Handover", March 2014, http://www.netmanias.com/en/?m=view&id=techdocs&no=6224

[2] 3GPP TS 36.423, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 application protocol (X2AP)"

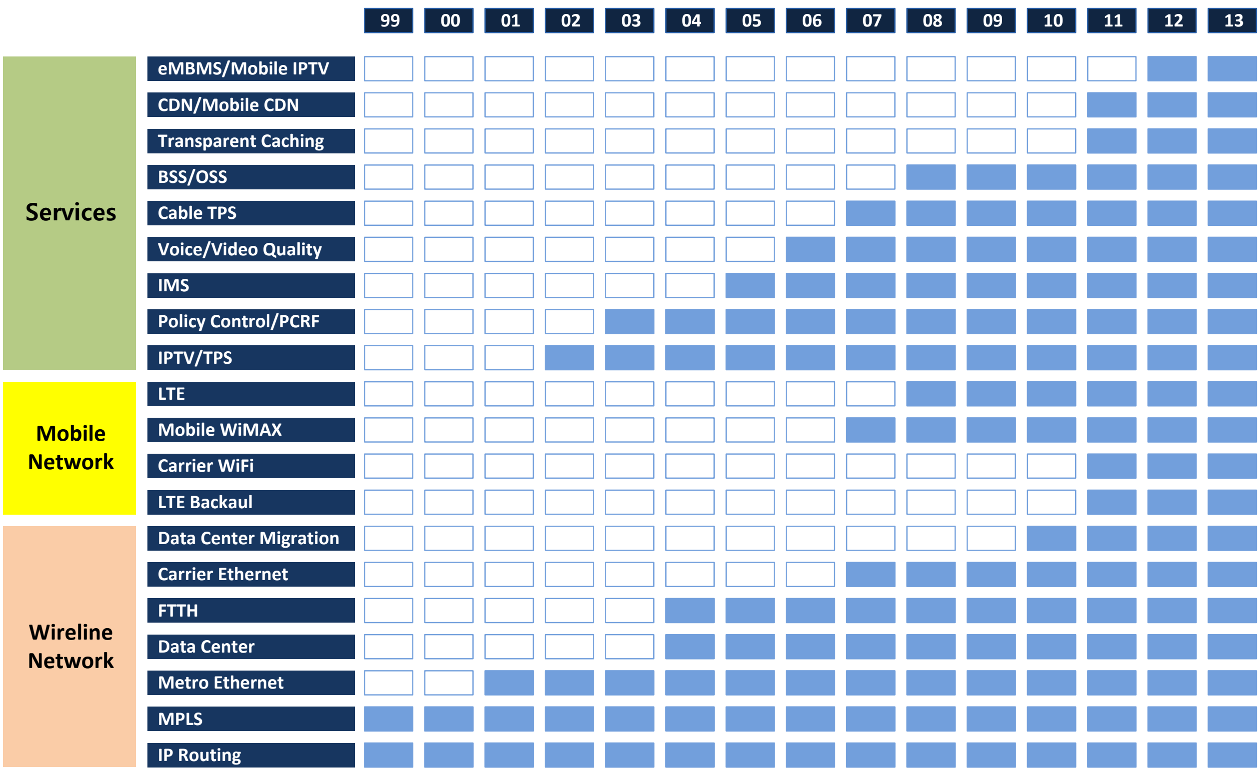
[3] 3GPP TS 36.331, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification"

[4] Netmanias Technical Document, "LTE Security II: NAS and AS Security", August 2013, http://www.netmanias.com/en/?m=view&id=techdocs&no=5903

[5] Netmanias Technical Document, "LTE Security I: LTE Security Concept and LTE Authentication", July 2013, http://www.netmanias.com/en/?m=view&id=techdocs&no=5902

[6] NMC Consulting Group Confidential Internal Report, "E2E LTE Network Design", August 2010

Netmanias Research and Consulting Scope



Visit http://www.netmanias.com to view and download more technical documents.

About NMC Consulting Group

NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.