NETMANIAS
www.netmanias.com

NMC CONSULTING GROUP
www.nmcgroups.com

# EMM Procedure 6. Handover without TAU

## Part 3. S1 Handover

**Table of Contents**



This document will describe the procedure for S1 handovers 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 handovers on S1 protocol will be discussed, followed by detailed procedures of S1 handover. We will learn how EPC (MME) intervenes in preparation of a handover between eNBs, and how DL packets are forwarded through an indirect tunnel that passes S-GW 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 information elements in EPS entities are different before and after the S1 handover procedure.

**April 8, 2014**

**(Initial Released: July 31, 2012)**

www.netmanias.com

**NMC Consulting Group (tech@netmanias.com)**

## 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 | |
| **18** | | **LTE EMM Procedure 6. Handover without TAU - Part 3. S1 Handover** | **O** |
| 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 |
| GUMMEI | Globally Unique MME Identifier |
| 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 |
| S-GW | Serving Gateway |
| SN | Sequence Number |
| TA | Tracking Area |
| TAC | Tracking Area Code |
| TAU | Tracking Area Update |
| TEID | Tunnel Endpoint IDentifier |
| UE | User Equipment |
| UMTS | Universal Mobile Telecommunication System |
| UL | Uplink |

# I. Introduction

In the previous document, "EMM Case 6. Handover without TAU – Part 2. Overview of X2 Handover" [1], we have discussed the procedures related to an X2 handover that is performed solely by two eNBs. This document will focus on procedures for an S1 handover performed between two eNBs with intervention of EPC. As in X2 handovers discussed previously, we will assume both source and target eNBs are connected to the same MME/S-GW (intra-LTE environment), 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 S1 handover, and Chapter III provides detailed procedures of S1 handover. Finally, Chapter IV will summarize how information elements in EPS entities are different before and after the handover.

# II. Concept of S1 Handover

## 2.1 S1 Protocol Stacks

S1 handovers are performed between a source eNB and a target eNB through the S1 interface, which connects eNB and EPC. eNB communicates with MME through S1AP signaling in the control plane, and communicates with S-GW through GTP tunnel in the user plane. Figure 1 shows the protocol stacks over the S1 interface in control and user planes.

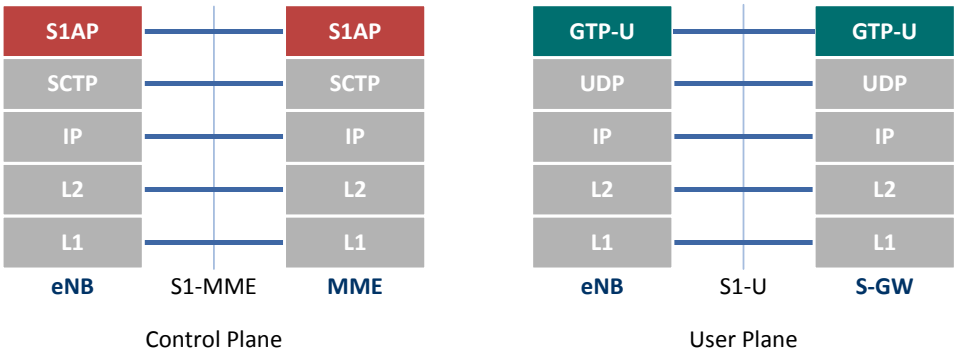



**Figure 1. Protocol Stacks over S1 Interface**

When a new eNB is installed, an "S1 Setup" procedure is performed between the eNB and MME(s). The eNB provides the MME(s) with eNB configuration information by sending an **S1 Setup Request** (eNB ID, eNB Name, TAC) message. Then, each MME returns an **S1 Setup Response** (GUMMEI, MME Name, Relative MME Capacity) message to the eNB so that it can update its configuration information. Here, Relative MME Capacity parameter is used in load balancing among MMEs in an MME. Its value, marked in weight factor, shows each MME's relative capacity to handle UE connection. eNBs connected to more than one MME use this value when selecting a MME to establish a new UE connection with.

UE connections between eNB and EPC are as follows: In the control plane, each user's signaling between eNB and MME is provided through S1 Application Protocol (S1AP) signaling connection[1], and identified by {eNB UE

[1] It is also referred to as "S1 signaling connection" in short.

S1AP ID, MME UE S1AP ID}. In the user plane, each user's S1 bearer between eNB and S-GW is provided through GTP (GPRS Tunneling Protocol) tunnel, and identified by {DL S1 TEID (S1 eNB TEID), UL S1 TEID (S1 S-GW TEID)}.

### 2.2 S1AP Procedures and Messages Relating to Handover

Tables 1 and 2 in 3GPP TS 36.413 S1AP show the elementary procedures of S1AP, which include both non-UE and UE related procedures. This document is about handover, and hence only discusses UE related procedures, particularly those related to the handover procedures to be explained in Chapter III. Table 1 lists the elementary S1AP procedures related to S1 handover, and their associated S1AP messages.

**Table 1. S1 Messages for Handover related S1AP Elementary Procedures [2]**

| Elementary Procedure | Initiating Message | Response Message | |
|---|---|---|---|
| | | Successful | Unsuccessful |
| Handover Preparation | **Handover Required** | **Handover Command** | **Handover Preparation Failure** |
| Handover Resource Allocation | **Handover Request** | **Handover Request Acknowledge** | **Handover Failure** |
| Handover Cancellation | **Handover Cancel** | **Handover Cancel Acknowledge** | - |
| UE Context Release | **UE Context Release Command** | **UE Context Release Complete** | - |
| SN Status Transfer | **eNB Status Transfer MME Status Transfer** | - | - |
| Handover Notification | **Handover Notify** | - | - |

Among the S1AP messages listed the table above, those to be used in Chapter III (those used in successful handovers) are briefly explained below.

- **Handover Required** message: This message is used during the handover preparation phase. It is sent by the source eNB to MME, and includes information about the target eNB and the radio resources at the source cell.
- **Handover Request** message: This message is used during the handover preparation phase. It is sent by MME to the target eNB, and includes the user's UE context.
- **Handover Request Acknowledge** message: This message is used during the handover preparation phase. It is sent by the target eNB to MME when the resource allocation for the UE is successfully completed at the target eNB. The target eNB allocates DL S1 TEID for S1 bearer to be used after the handover, and DL S1 TEID for S1 bearer (indirect tunnel) to be used for DL packet delivery during the handover, and then forwards them as included in the message.
- **Handover Command** message: This message is used during the handover preparation phase, and is sent by MME to the source eNB. It includes the information required when the UE accesses the target eNB (e.g. Target C-RNTI, Target eNB AS Security algorithm, DRB ID, etc.), and UL S1 TEID for S1 bearer (indirect tunnel) to be used by S-GW for DL packet delivery during the handover.
- **eNB Status Transfer** message: This message is used during the handover execution phase, and is sent by the source eNB to MME. It indicates from which packet the target eNB should receive or send.
- **MME Status Transfer** message: This message is used during the handover execution phase, and is

sent by MME to the target eNB. It indicates from which packet the target eNB should receive or send.

- **Handover Notify** message: This message is used during the handover completion phase, and is sent by the target eNB to MME. It indicates that the UE has completed the handover to the target eNB.
- **UE Context Release Command** message: This message is used during the handover completion phase, and is sent by MME to the source eNB to request release of the UE context.
- **UE Context Release Complete** message: This message is used during the handover completion phase, and is sent by the source eNB to MME to inform that the UE context has been released.

### 2.3 S1 Handover Procedure at a Glance

As seen in the previous document [3], an S1 handover procedure consists of preparation, execution and completion phases. Before we go further into detail, we will briefly preview the S1 handover procedure.

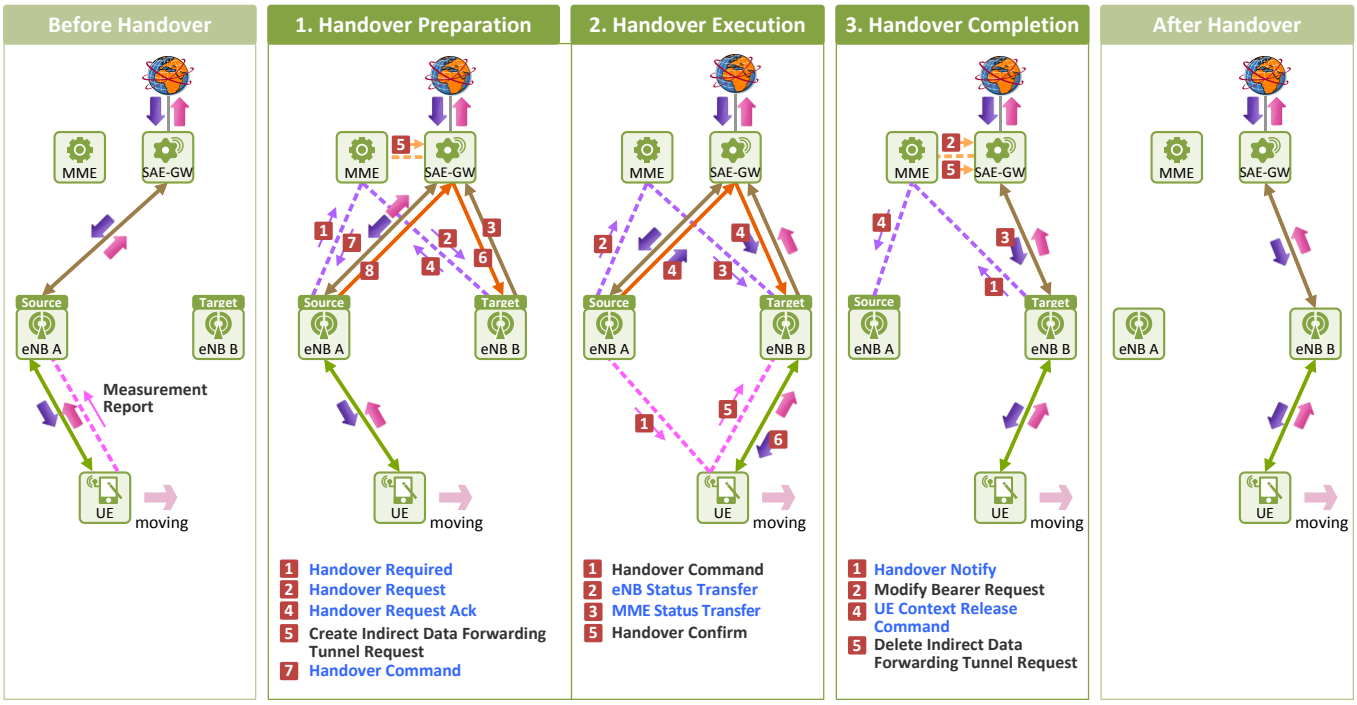



**Figure 2. Simplified Procedure of S1 Handover**

Figure 2 above illustrates at a glance the procedures required before, during (preparation, execution and completion phases) and after S1 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.

### Before S1 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 connected to. When the UE detects a measurement event, it sends a **Measurement Report** message to eNB A.

### S1 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. Next, it, realizing a handover to the target eNB through the X2 connection is not possible, decides to perform a S1 handover instead, and prepares to perform one through MME. Both eNBs communicate with the MME through S1AP signaling. At this time, the target eNB allocates radio resource in advance to ensure the same services currently provided by the source eNB are also available at the target eNB. The MME also provides the source eNB with the information required for the UE to access the target cell.

In the meantime, the target eNB and S-GW allocate resources needed to create an indirect tunnel through which DL packets arriving at the source eNB are forwarded to the S-GW and finally to the target eNB while a handover is being performed, as follows:

- The source eNB sends the information about the target eNB, as included in a **Handover Required** message, to the MME (1).
- The MME then sends a **Handover Request** message that includes AS security information required for the target eNB to create the AS security base key along with the UE Context to the target eNB (2).
- **Target eNB**
  - establishes an UL S1 bearer through which to forward UL packets after the handover by using the S1 S-GW TEID obtained from the MME, and allocates S1 target eNB TEID for a DL S1 bearer (3).
  - allocates S1 target eNB TEID for the tunnel connecting the S-GW and the target eNB (this tunnel is a part of the indirect tunnel[2] connecting all the way from the source eNB, S-GW and the target eNB) to be used for forwarding DL packets while the UE attempts to access (i.e. perform a handover to) the target eNB.
  - configures a **Handover Command** message that includes information needed for the UE to access the target cell (e.g. Target C-RNTI, Target DRB ID, etc.).
  - and sends the information to the MME by including it in a **Handover Request Ack** message (4).
- The MME, upon receiving the message, includes the S1 target eNB TEID that the target eNB has allocated for the indirect tunnel in a **Create Indirect Data Forwarding Tunnel Request** message, and sends the message to the S-GW (5).

[2] It is called an "indirect tunnel" because the source eNB sends the DL packets not directly to the target eNB, but through the S-GW.

- **S-GW**
  - Creates an indirect tunnel connecting the target eNB (6).
  - allocates S1 S-GW TEID for the tunnel connecting the source eNB and the S-GW (this tunnel is a part of the indirect tunnel connecting all the way from the source eNB, S-GW and the target eNB), and sends it to the MME through a **Create Indirect Data Forwarding Tunnel Response** message.
- The MME includes i) the S1 S-GW TEID that the S-GW has allocated for the indirect tunnel, and ii) the information required for the UE to access the target cell, in a **Handover Command** message, and sends the message to the source eNB (7).
- Then, the source eNB creates an indirect tunnel connecting to the S-GW (8).

Through Steps 8 and 6, the entire indirect tunnel connecting all the three entities, the source eNB, S-GW and target eNB, is created.

### S1 Handover Execution

Now the two eNBs are ready to perform a handover, it is time to command the UE to perform one.

- **Source eNB**
  - commands the UE to perform a handover to the target cell by sending a **Handover Command** message that includes all the information needed for the UE's access to the target cell (1).
  - informs the MME about from which UL/DL packet it should receive/send from/to the UE by sending an **eNB Status Transfer** message (2).
  - sends the DL packets received from the S-GW on to the target eNB through the indirect tunnel connected to the target eNB via the S-GW (4).
- The MME informs the target eNB about from which UL/DL packet it should send/receive to/from the UE by sending an **MME Status Transfer** message (3).
- The UE disconnects from the source eNB, and connects to the target eNB (5).
- Once the UE is successfully accessed to the target eNB, it becomes immediately capable of sending or receiving packets (6).

### S1 Handover Completion

As the MME already knew that the UE was about to perform a handover, the target eNB, unlike in X2 handover, does not request the MME for path modification. Instead, the target eNB sends the MME a **Handover Notify** message to indicate the UE has completed the handover once the UE is connected to the target eNB.

- As soon as the UE is connected, the target eNB sends the MME a **Handover Notify** message to inform about the completed handover (1).
- Then, the MME requests the S-GW for S1 bearer modification (2). The S-GW modifies the DL S1 bearer path to connect to the target eNB, as requested (3).
- The S-GW changes the bearer path as follows:
  - It stops DL packet delivery by sending an End Marker (EM) packet through the DL S1 bearer connected to the source eNB.

    - Then it creates a DL S1 bearer that connects to the target eNB, and resumes DL packet delivery to the target eNB.
- The target eNB sends DL packets to the UE as follows:
    - It sends DL packets arriving through the indirect tunnel to the UE until an EM packet arrives.
    - Once an EM packet arrives, it sends the UE the ones arriving through the new path.
- The MME:
    - requests the source eNB to release S1 resources related to the source eNB and the UE Context it has by sending an **UE Context Release Command** message (4).
    - request the S-GW to release resources associated with the indirect tunnel by sending a **Delete Indirect Data Forwarding Tunnel Request** message (5).

#### After S1 Handover

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

### 2.4 UE State and Connection Information Before and After S1 Handover

Figure 3 illustrates the connection establishments in the user/control planes, and the UE and MME states before, during and after the S1 handover.

- **Before S1 Handover**

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

- **During S1 Handover**

  Even during the handover phase, the UE's state on the NAS layer remains unchanged. Both the source and target eNBs are connected to the MME through the S1 signaling connection established over the S1-MME interface. They are also connected to the S-GW through the indirect tunnel created over the S1-U interface for DL packet forwarding. 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 S1 Handover**

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

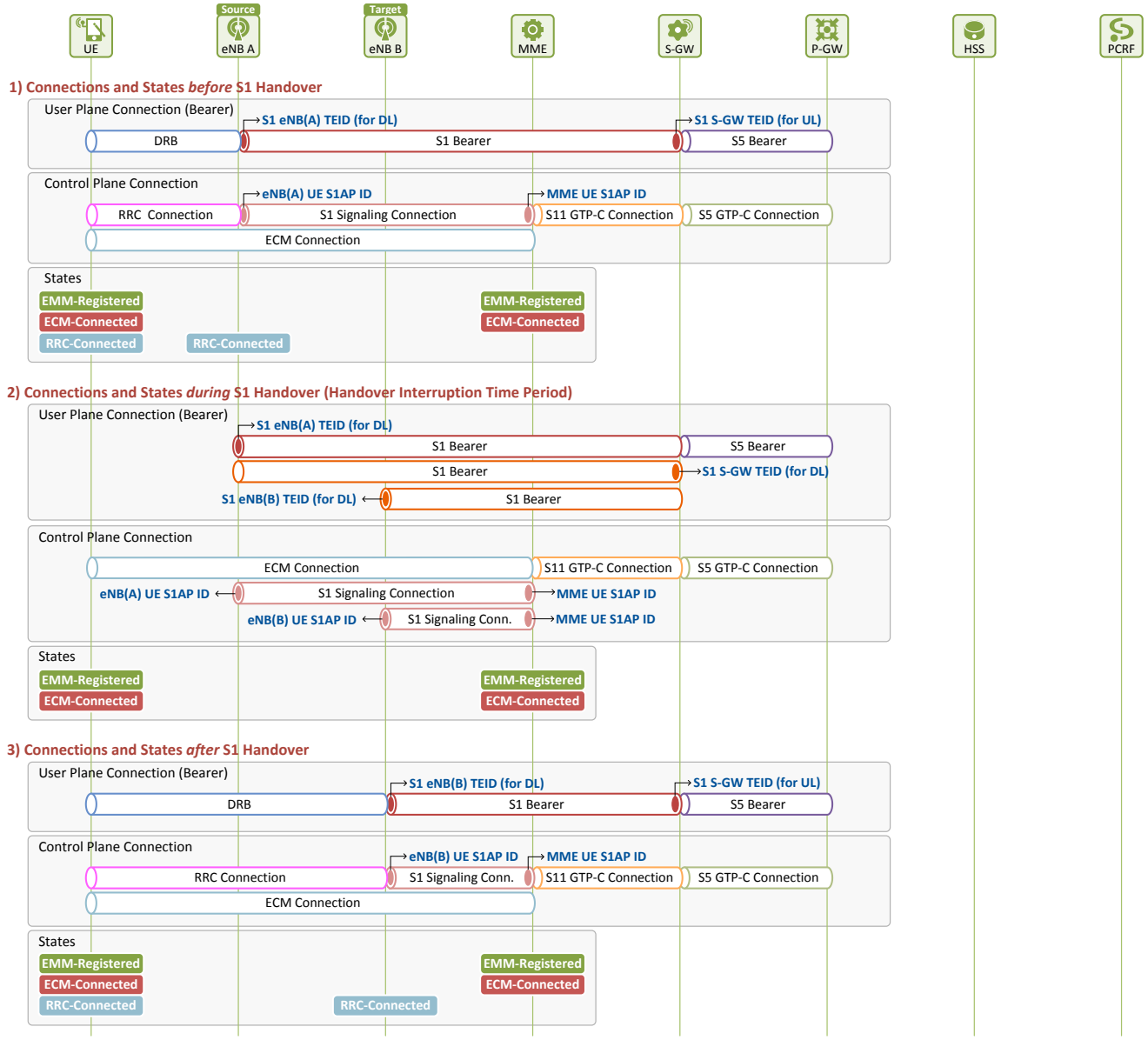



**Figure 3. Connections and States before/after S1 Handover**

## III. Procedure of S1 Handover

Now we will look into the detailed S1 handover procedures.[3] Figure 4 illustrates the EPS bearer and signaling connections prior to the S1 handover, and the detailed procedures of the S1 handover preparation phase.

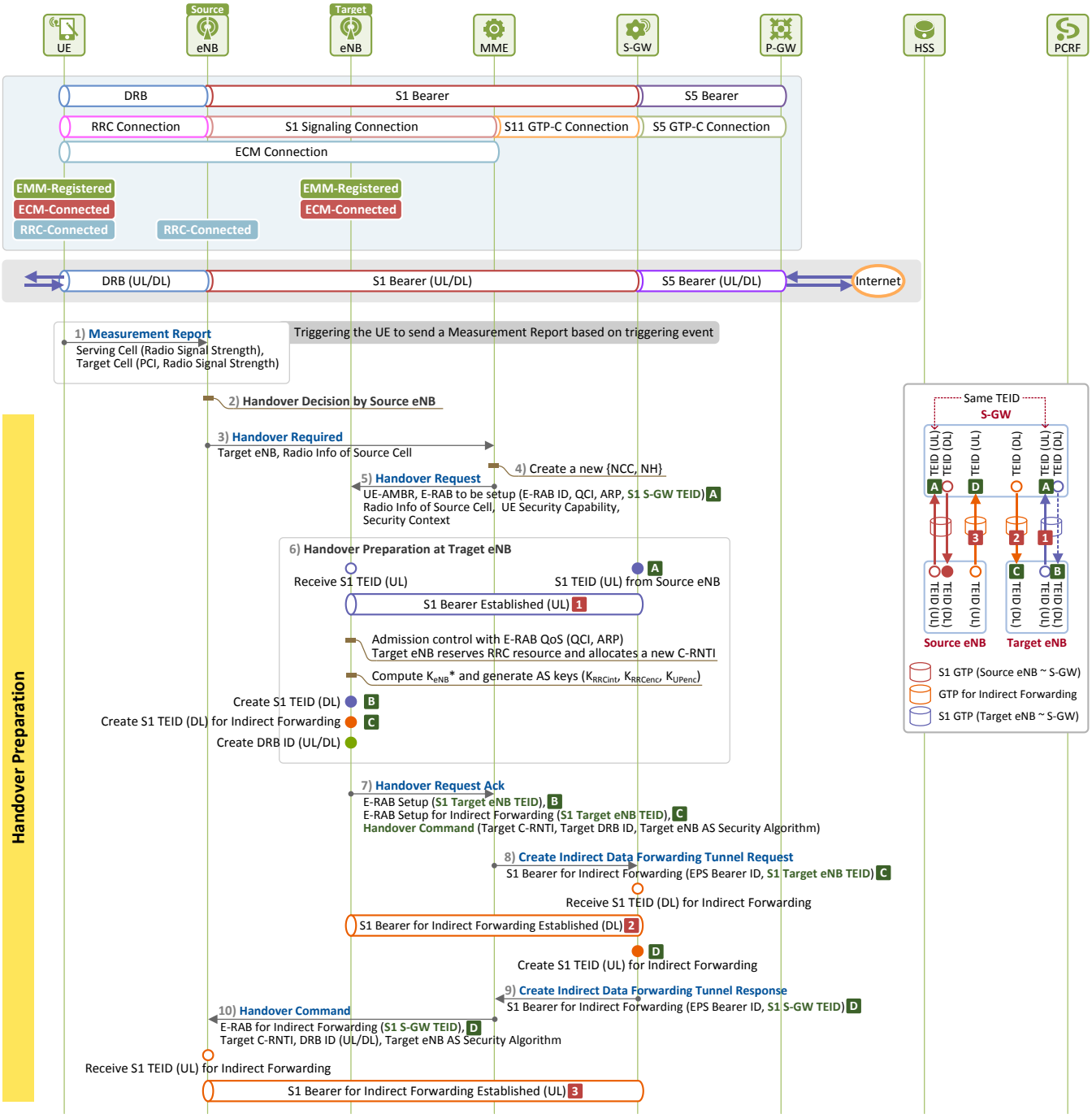



**Figure 4. S1 Handover - Handover Preparation Phase**

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

■ **Before Handover**

**1) [UE → eNB] Measurement Report**

As a measurement event is triggered,[4] 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. Becoming aware that no X2 connection is available for a handover between two eNBs, the source eNB decides to perform an S1 handover.

**3) [Source eNB → MME] Requesting a Handover**

The source eNB sends a **Handover Required** message to the MME, requesting a handover to the target eNB. The information included in the message is as follows:

**Handover Required (Handover Type, Target eNB ID, Source to Target Transparent Container)**

- **Handover Type**: indicates the type of a handover initiated. "IntraLTE" in this example
- **Target eNB ID:** includes Target Global eNB ID and Selected TAI information
- **Source to Target Transparent Container**: is used when forwarding the radio-related information of the source cell to the target cell transparently through EPC (MME)

**4) [MME] Deriving Security Context to Forward to the Target eNB**

The MME derives the Security Context {NCC, NH} so that the target eNB can derive the AS security base key[5]. NCC increases by 1 starting from the initial NCC value ($NCC_0$=0), and NH is derived from the initial NH value ($NH_0$) and $K_{ASME}$.

- $NCC_1 = NCC_0 + 1 = 1$
- $NH_1 = KDF(NH_0, K_{ASME})$

**5) [Target eNB ← MME] Requesting the Target eNB for a Handover**

The MME sends a **Handover Request** message to the target eNB, requesting a handover on behalf of the source eNB. The information included in the message is as follows:

**Handover Request (UE-AMBR, E-RAB to be setup (E-RAB ID, QCI, ARP, S1 S-GW TEID), Source to Target Transparent Container, UE Security Capability, Security Context)**

- **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.
- **E-RAB to be setup:** UE's E-RAB information stored at Source eNB. Includes E-RAB ID, QoS parameters, UL S1 bearer information[A]
- **Source to Target Transparent Container**: is used when forwarding the radio-related information of the source cell (e.g. UE radio access capability, RRC configuration Info, etc.) to the target cell transparently through EPC (MME).

[4] See our "LTE EMM Procedure 6. Handover without TAU – Part 1. Overview of Handover" document [3] and 3GPP TS 36.331 [4] for more information about measurement events.

[5] See our "LTE Security II" document [5] for more information about AS security.

- **UE Security Capability**: security algorithms supported by UE (encryption and integrity algorithm)
- **Security Context:** includes {NCC, NH} to be used when Target eNB derives the AS Security base key, $K_{eNB}^*$.

### 6) [Target eNB] Preparing S1 handover

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

(i) **New S1 bearer resource allocation**: 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[A]) stored at the source eNB. Then it allocates S1 Target eNB TEID[B] to prepare a DL S1 bearer to be used after the handover.

(ii) **Indirect tunnel resource allocation**: While the UE is performing a handover (i.e. after it disconnects from the source eNB, until it connects to the target eNB), there should be an indirect tunnel for rerouting DL packets arriving at the source eNB to the target eNB via the S-GW. For this, the target eNB allocates S1 Target eNB TEID[C] so that the S-GW can establish an indirect tunnel connecting to the target eNB.

(iii) **Allocation of resource to be used by UE over radio link**: 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) **$K_{eNB}^*$ derivation**: It derives $K_{eNB}$* by using the security context information (NCC1, NH1)[6] it received from the MME for handover, and then obtains AS security keys ($K_{RRCint}$, $K_{RRCenc}$, $K_{Upenc}$). Shortly after, when the UE connects to the target eNB, the two can communicate with each other securely over the radio link by using these key values. Figure 5 shows how $K_{eNB}$* is derived. We can see that $K_{eNB}$* is derived from $NH_1$, the target cell's Physical Cell ID (PCI) and frequency (E-UTRA Absolute Radio Frequency Channel Number-Downlink (EARFCN-DL)).

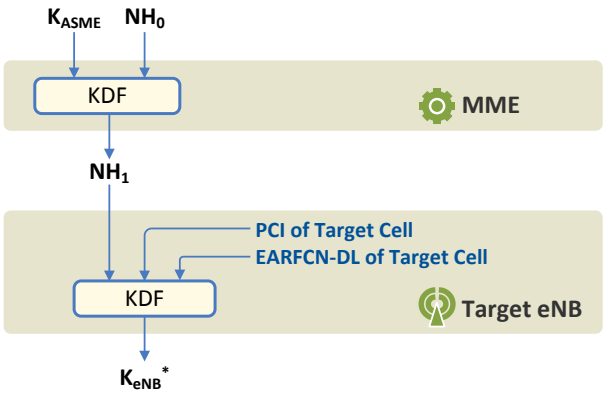



**Figure 5. Derivation of $K_{eNB}^*$ (S1 Handover case)**

[6] Security is out of the scope of this document, and hence will not be discussed in details here.

### 7) [Target eNB → MME] Notifying the MME of Preparation Completion

The target eNB sends the MME all the information about the resources prepared in Step 6), as included in a **Handover Request Ack**[7] message. The information in the message is as follows

**Handover Request Ack (E-RAB Admitted(E-RAB ID, S1 Target eNB TEID, DL S1 Target eNB TEID), Handover Command (Target C-RNTI, Target DRB ID, AS Security Algorithm of Target eNB))**

- **E-RAB Admitted**[8]:
  - **E-RAB ID**: E-RAB ID allocated by the target eNB
  - **S1 Target eNB TEID**: DL S1 TEID[B] that the target eNB allocated to S-GW for establishment of S1 bearer connecting to itself.
  - **DL S1 Target eNB TEID**: DL S1 TEID[C] that the target eNB allocated for establishment of an indirect tunnel for handover through which to deliver DL packets.
- **Handover Command**: Transparent Container, delivered by the target eNB to the source eNB, that contains the radio information of the target cell 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.

### 8) [MME → S-GW] Requesting for Creation of S1 Bearer for DL Packet Delivery

The MME sends the S-GW a **Create Indirect Data Forwarding Tunnel Request** message, requesting creation of an indirect tunnel for delivering DL packets while the UE is performing a handover. This message includes GTP TEID (S1 Target eNB TEID[C]) that the target eNB has allocated for the tunnel.

### 9) [MME ← S-GW] Notifying that S1 Bearer is Created for DL Packet Delivery

The S-GW, upon receiving the **Create Indirect Data Forwarding Tunnel Request** message, creates an indirect tunnel connecting to the target eNB. It then allocates S1 S-GW TEID[D], forwards it through the **Create Indirect Data Forwarding Tunnel Response** message to the MME so that the source eNB can create an indirect tunnel connecting to the S-GW.

### 10) [Source eNB ← MME] Notifying of the Completed Handover

The MME sends the source eNB a **Handover Command** message that includes i) the S1 S-GW TEID[D] received from the S-GW in Step 9), and ii) the **Handover Command** information received from the target eNB in Step 7).

The source eNB learns from the **Handover Command** message that the target eNB and EPC are ready for UE handover.

---

[7] 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.

[8] 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 S1 handover execution phase.

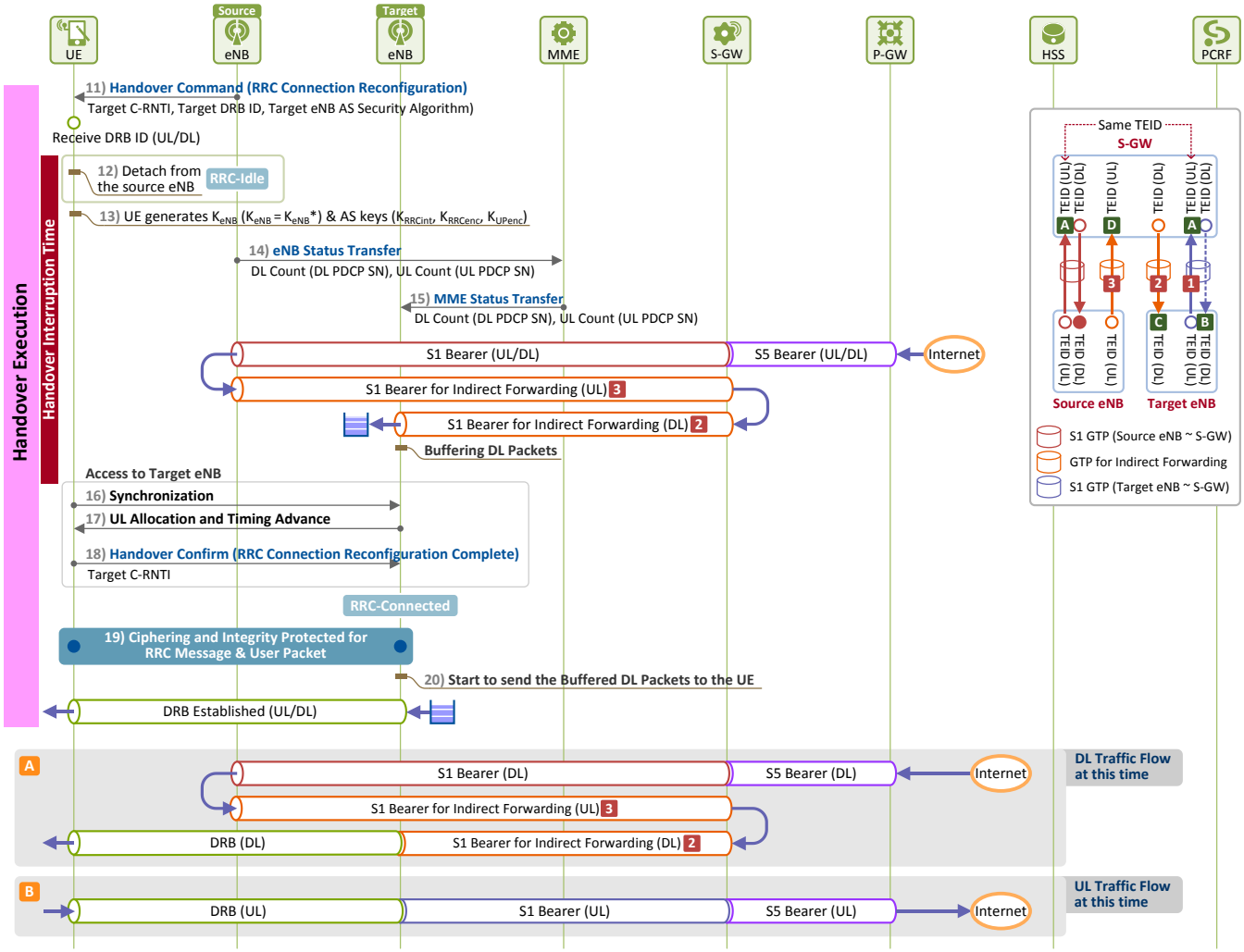



**Figure 6. S1 Handover - Handover Execution Phase**

### 11) [UE ← Source eNB] Commanding UE to Perform a Handover

Once the source eNB becomes ready for a handover, it commands the UE to perform a handover by sending a **Handover Command** message. The **Handover Command** message is delivered to the UE, as included in an **RRC Connection Reconfiguration** message.

### 12) [UE] Executing a Handover

Once the UE obtains, from the received **Handover Command** message, C-RNTI and DRB ID to be used at the target cell, and detaches from the source eNB. Now, all packet exchanges between the UE and the source eNB are stopped, and the handover interruption time[9] begins.

### 13) [UE] AS Security Setup

The UE derives AS security keys to be used over the radio link of the target eNB. First it derives $K_{eNB}$*, the

[9] See our "LTE EMM Procedure 6. Handover without TAU. Part 1 - Overview of Handover" document[3] for more information about the handover interruption time.

AS base key, (the relevant key derivation functions are as seen in Figure 5), then it derives AS security keys ($K_{RRCint}$, $K_{RRCenc}$, $K_{UPenc}$) by using the AS security algorithms that the target eNB selected.

### 14) ~ 15) [Source eNB → MME, MME → target eNB] Notifying the No. of the Packet to Send/Receive

The source eNB sends an **eNB Status Transfer** message that includes DL Count and UL Count to the MME, which then forwards the same information through an **MME Status Transfer** message to the target eNB. This was the target eNB knows from which packet it should send to (or receive from) the UE. 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:

**eNB 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 **eNB Status Transfer** message, the source eNB begins to forward DL packets arriving from S-GW to the target eNB through the indirect tunnel established over the S1 interface. The target eNB buffers the packets and waits for completion of the UE's access.

### 16) ~ 18) [UE, Target eNB] UE가 UE's Access to the Target eNB

16) 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. 17) The target eNB sends the UE the timing alignment information and UL Grant. 18) 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 is ended.

### 19) [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.

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

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

> **S5 bearer** (P-GW to S-GW) → **S1 bearer** (S-GW to source eNB) → **S1 bearer** (source eNB to S-GW) → **S1 bearer** (S-GW to target eNB) → **DRB** (target eNB to UE)

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 the S-GW through the following path (See **[B]** in Figure 6):

> **DRB** (UE to target eNB) → **S1 bearer** (target eNB to S-GW) → **S5 bearer** (S-GW to P-GW)

## ■ Handover Completion

Figure 7 illustrates the procedure for S1 handover completion phase.

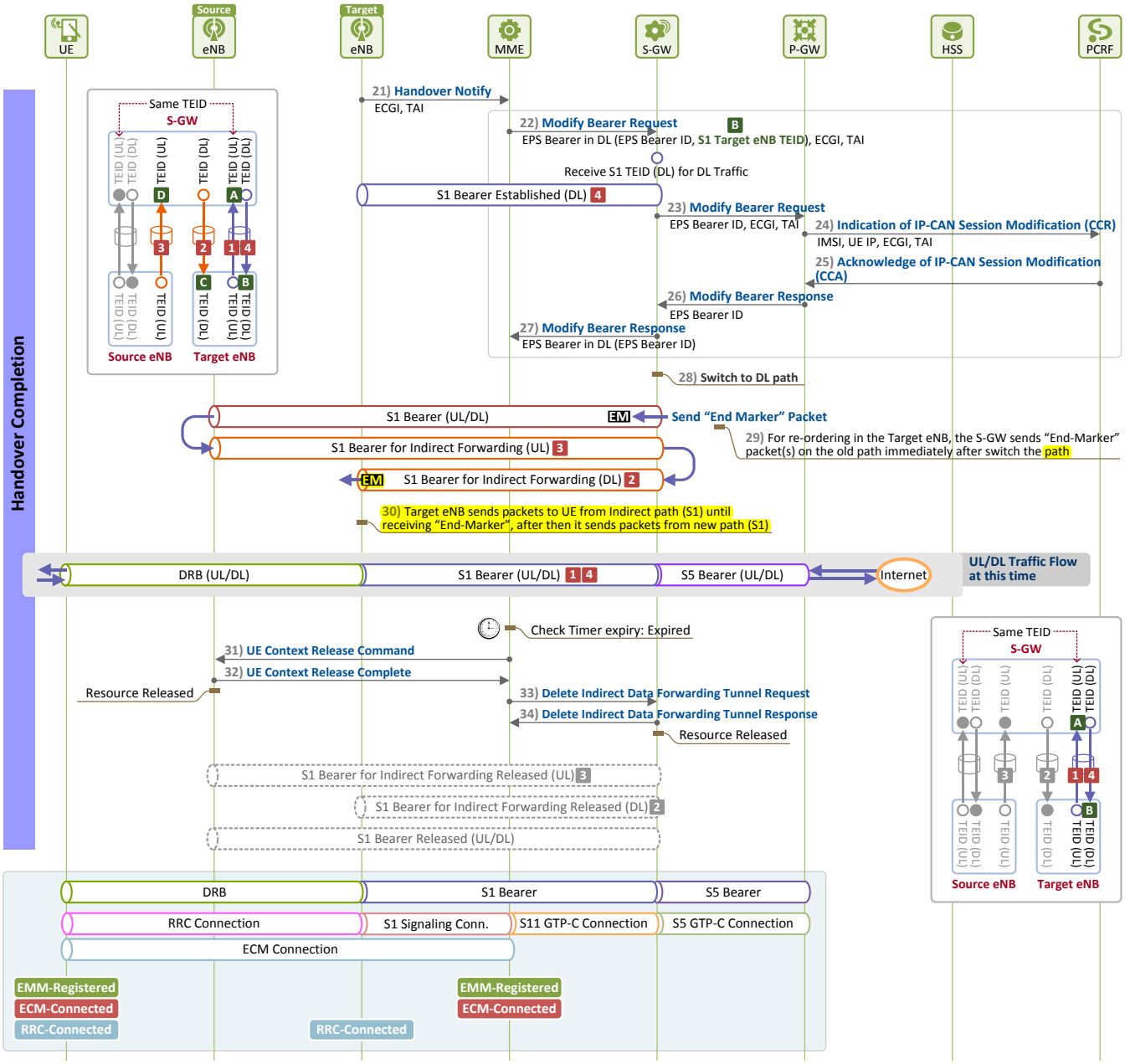



**Figure 7. S1 Handover - Handover Completion Phase**

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

Once the UE is accessed, the target eNB notifies EPC (MME) that the UE has successfully finished the S1 handover by sending a **Handover Notify** message that includes its ECGI and TAI.

### 22) ~ 27) Modifying the EPS Bearer

The MME forwards the S1 Target eNB TEID[B] that was allocated by the target eNB to the S-GW by sending a **Modify Bearer Request** message. This way it requests the S-GW to modify the bearer path. 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. 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.

**28) ~ 29) [S-GW] Modifying the EPS Bearer (S1 Bearer) Path**

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.

**30) [Target eNB] Packet Re-ordering**

Now the target eNB receives DL packets forwarded from the source eNB through the indirect tunnel AND those sent from the S-GW through the newly modified path. So, it should be able to deliver them to the UE in the correct order. First, the target eNB forwards the DL packets received through the indirect tunnel to the UE. Then when EM arrives, it knows that the packet was the last one from this path, and thereafter it sends the DL packets received from the new path to the UE.

**31) ~ 32) [Source eNB ←→ MME] Releasing the UE Context and S1 Resources Stored at the Source eNB**

The MME informs the source eNB that it may release the resources (S1 bearer and indirect tunnel) it has kept over the S1 interface and the UE Context by sending an **UE Context Release Command** message.

The source eNB then releases the UE Context and S1 resources, and informs the MME of such release by sending an **UE Context Release Complete** message.

**33) ~ 34) [MME ←→ S-GW] Releasing the Indirect Tunnel**

The MME sends the S-GW a **Delete Indirect Data Forwarding Tunnel Request** message, requesting for release of the indirect tunnel.

Upon the request, the S-GW releases the indirect tunnel, and informs the MME of such release by sending a **Delete Indirect Data Forwarding Tunnel Response** message.

## IV. EPS Entity Information: Before/After S1 Handover

As, in an intra-LTE environment, the information elements stored at EPS entities before and after S1 handover are the same as in X2 handover, see our previous document [1] for the details (For EPS entities information, see below).

- Information on handover-related AS Security context may vary depending on the types of handover, e.g. X2 or S1. Handover security is however out of the scope of this document, and hence was not presented here in details.
- Information elements stored at EPS entities during the handover procedure are pretty similar but can be different depending on the types of handover. Those generated during handover and then deleted were not presented.

## V. Closing

We have so far discussed the S1 handover procedure performed in an intra-LTE environment where neither MME nor S-GW is changed after the procedure. Unlike X2 handover, in S1 handover, EPC already knows about UE's handover even before an actual handover is performed. Thus, EPC is involved in the handover procedure from the handover preparation phase. It performs a handover in cooperation with the source eNB and target eNB, and forwards DL packets arriving at the source eNB during the handover interruption time to the target eNB through the indirect tunnel that passes the S-GW, preventing packet loss.

In EMM Case 6, we have discussed LTE handovers in an intra-LTE environment through the three companion documents. In the subsequent document, we will explain the cell reselection procedure required when a UE which has camped on a cell moves and camps on another cell while staying in Idle (as defined as EMM Cases 7 and 9 [6]).

## References

[1] Netmanias Technical Document, "LTE EMM Procedure 6 – Part 2. X2 Handover", March 2014, http://www.netmanias.com/en/?m=view&id=techdocs&no=6257

[2] 3GPP TS 36.413, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)"

[3] Netmanias Technical Document, "LTE EMM Procedure 6 – Part 1. Overview of LTE Handover", March 2014, http://www.netmanias.com/en/?m=view&id=techdocs&no=6224

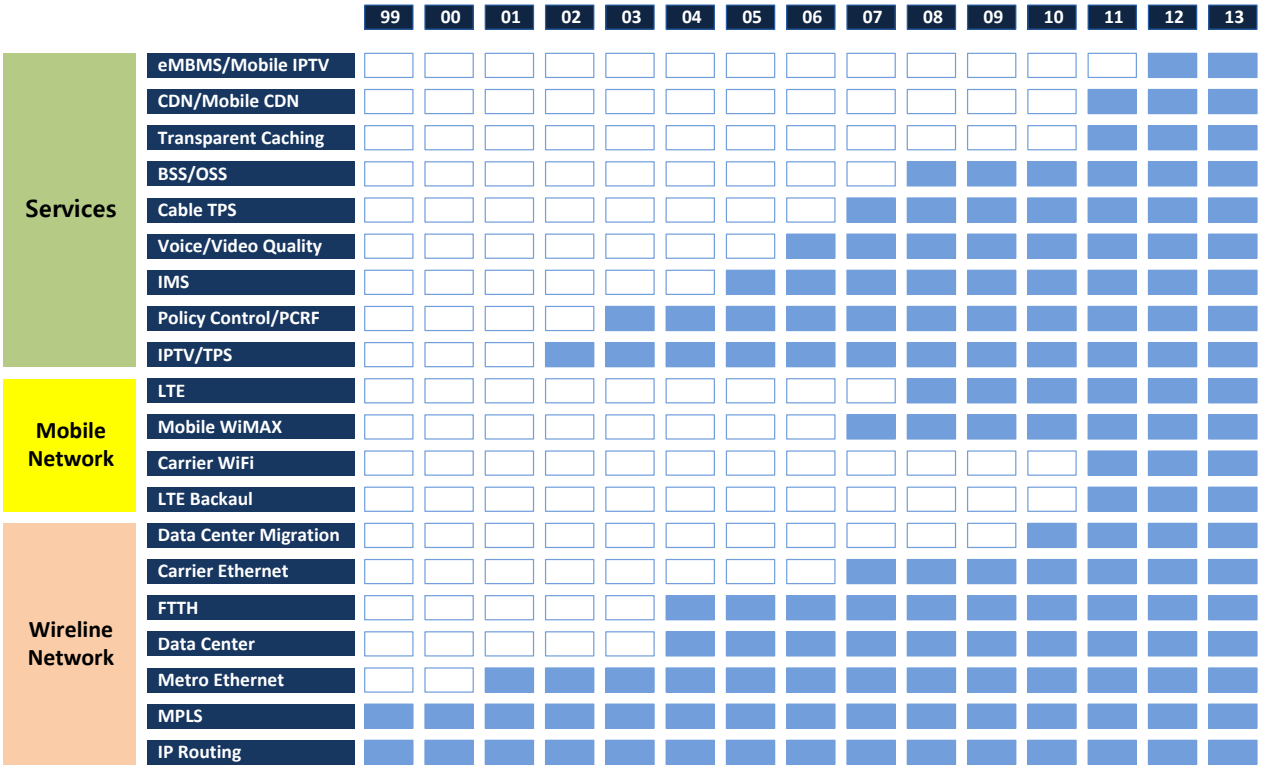
[4] 3GPP TS 36.331, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification"

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

[6] Netmanias Technical Document, "Eleven EMM Cases in an EMM Scenario", October 2013, http://www.netmanias.com/en/?m=view&id=techdocs&no=6002

[7] 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.**