NETMANIAS
www.netmanias.com

NMC CONSULTING GROUP
www.nmcgroups.com

LTE Identification I: UE and ME Identifiers

Table of Contents

The LTE Security technical document consists of three companion documents (LTE Identification I, II and III). As the first document for LTE Identification, this document (Part I, LTE Identification I) classifies LTE identifications into different groups, and describes two of these groups, i.e., User Equipment Identifiers (UE IDs) and Mobile Equipment identifiers (ME IDs). First, UE IDs such as IMSI, GUTI, S-TMSI, IP address and C-RNTI are explained and then UE IDs identified over the S1-MME and X2 interfaces are discussed. Then, ME IDs such as IMEI and IMEISV are explained. Finally features of UE and ME IDs are briefly summarized.

August 20, 2013
(Initial Released: January 19, 2011)

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**	**O**
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	
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

APN	Access Point Name
CD	Check Digit
C-RNTI	Cell Radio Network Temporary Identifier
DNS	Domain Name Server
DRB	Data Radio Bearer
ECGI	E-UTRAN Cell Global Identifier
ECI	E-UTRAN Cell Identifier
eNB	Evolved Node B
EPC	Evolved Packet Core
E-RAB	E-UTRAN Radio Access Bearer
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GUMMEI	Globally Unique MME Identifier
GUTI	Globally Unique Temporary Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
LBI	Linked EPS Bearer Identity
MCC	Mobile Country Code
MME	Mobility Management Entity
MMEC	MME Code
MMEGI	MME Group Identifier
MNC	Mobile Network Code
MSIN	Mobile Subscriber Identification Number
M-TMSI	MME Temporary Mobile Subscriber Identity
NE	Network Equipment
OCS	Online Charging System
OFCS	Offline Charging System
PCRF	Policy and Charging Rule Function
PDN	Packet Data Network
P-GW	PDN Gateway
PLMN	Public Land Mobile Network
S1AP	S1 Application Protocol
S-GW	Serving Gateway
SPR	Subscriber Profile Repository
SRN	Serial Number
S-TMSI	SAE Temporary Mobile Subscriber Identity
TAC	Type Allocation Code
TAC	Tracking Area Code
TAI	Tracking Area Identity
TEID	Tunnel Endpoint IDentifier
TIN	Temporary Identifier used in Next update
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
USIM	UMTS Subscriber Identity Module
X2AP	X2 Application Protocol

I. Introduction

In LTE network, different IDs are used to identify each entity depending on their relationship with other IDs just like different names and titles are used to refer to a person - a name (e.g. James), or a title at work (e.g. Manager James, James from Netmanias, James from Google, etc.) or at home (e.g. son, dad, uncle, etc.) - in human network. Understanding these IDs as well as the EPS entities defined in [1] is essential to understand LTE technologies.

We have previously discussed the LTE network architecture, our first topic in LTE area. Now we will cover LTE identification, our second topic in the area, in a series of three companion documents. This document is the first of the series and will focus on user equipment (UE) IDs. The second and third documents will specifically cover network equipment (NE) IDs and EPS sessions/bearers, respectively.

This document is organized as follows. In Chapter II, LTE identification is classified into different groups, and in Chapter III and Chapter IV, UE IDs and ME IDs are described respectively based on the classification. In Chapter V, the overall features of the UE and ME IDs are briefly summarized.

II. Classification of LTE Identification

Figure 1 shows, using the LTE network reference model [1], IDs defined and used in some entities and interfaces. Features of these LTE IDs will be explained in terms of their creation time, attribute type (permanent/temporary) and ranges within which they are uniquely identified.

Creation Time: Creation time of an LTE ID can be one of the following:

- When commissioned upon equipment installation
- When provisioned by the operator before or during service operation
- When created on-demand as a user accesses to the network or uses services

LTE IDs commissioned or provisioned are presented with the blue boxes on the corresponding EPS entities in Figure 1[1].

Type: An LTE ID can have an attribute type, either a permanent value that stays fixed once set, or a temporary one that changes whenever activated. The ones allocated by being commissioned or provisioned have permanent values while others allocated on-demand as a user accesses to the network or uses services have temporary values.

Range (within which IDs are uniquely identified): Each LTE ID is uniquely identified across the world, operator networks, entities or channels.

[1] If SON (Self-Organizing Network) technology is applied, ECGI and TAI/TAI lists may be auto-configured without being provisioned.

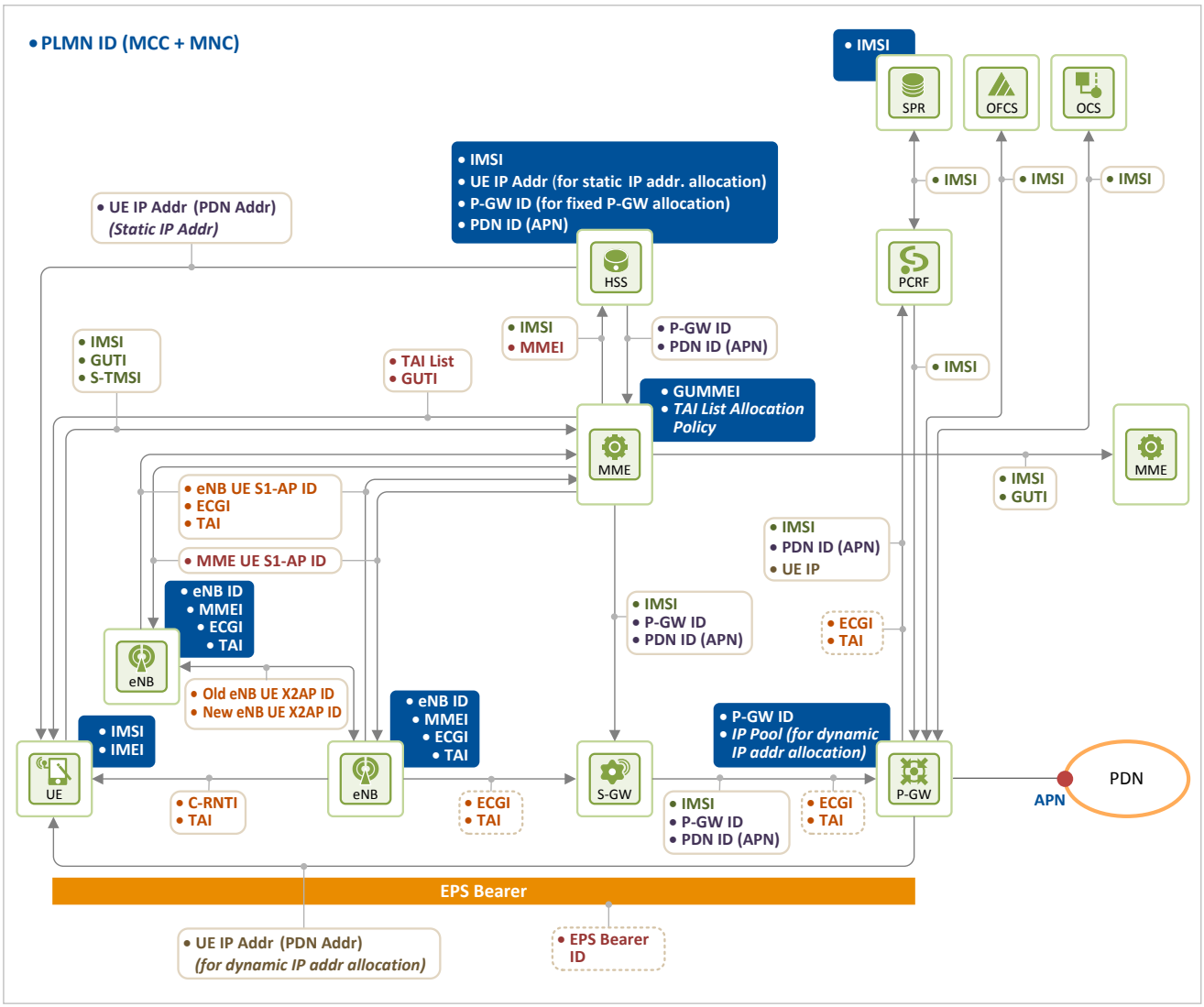


Figure 1. LTE identification

Figure 1 shows different IDs used depending on where LTE identification is actually being performed, i.e., layers, interfaces or geographical areas. For the convenience of description, the IDs shown in Figure 1 are grouped as seen in Table 1.

First, IDs for the EPS entities are grouped into UE IDs, ME IDs and NE IDs. The EPS entities are classified into UEs and NEs. MEs, one of the UE components, are separated from UEs and classified as a separate group. NEs are the network entities operated by an LTE operator such as MMEs, eNBs and P-GWs. IDs, such as IMSI, GUTI, S-TMSI, IP address, C-RNTI, UE S1AP ID and UE X2AP ID that identify a user, belong to the UE ID group. IDs such IMEI and IMEISV that identify a device belongs to the ME ID group.

And IDs, such as GUMMEI and MMEI for MMEs, Global eNB ID and eNB ID for eNBs, ECGI and ECI for cells, and P-GW ID for P-GWs, belong to the NE ID group. Location IDs, such as TAI and TAC, identify the area where a user is located.

Finally, session/bearer IDs, such as PDN ID(or APN), EPS bearer ID, E-RAB ID, DRB ID, TEID and LBI, are related to user traffic delivery, and identify EPS sessions (PDN connections) and EPS bearers.

This document, the first document in the LTE Identification series, describes LTE IDs for UE and ME shown in gray in Table 1. The second document will explain LTE NE IDs and location IDs which identify location of UEs,

and the third document will discuss IDs for EPS session/bearer.

Table 1. Classification of LTE identification

ID group	LTE ID	Related document
UE ID	IMSI, GUTI, S-TMSI, IP address (PDN address), C-RNTI, eNB UE S1AP ID, MME UE S1AP ID, Old UE X2AP ID, UE X2AP ID	LTE Identification I
ME ID	IMEI	
NE ID	GUMMEI, MMEI, Global eNB ID, eNB ID, ECGI, ECI, P-GW ID	LTE Identification II
Location ID	TAI, TAC	
Session/Bearer ID	PDN ID(APN), EPS Bearer ID, E-RAB ID, DRB ID, TEID, LBI	LTE Identification III

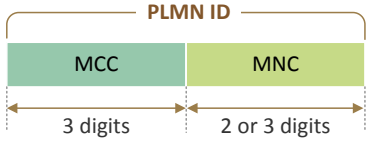
III. Identifiers for User Equipment (UE IDs)

LTE networks are all IP networks. Because of such nature, UEs in an LTE network share radio and network resources. EPS entities of the LTE network allocate a UE ID to each UE to identify it. Because the UEs share resources in various layers and interfaces, various UE IDs are required.
The most essential ID in a mobile communication network is the Public Land Mobile Network (PLMN) ID which identifies the operator of a particular network. So, we will begin the description of UE IDs with the PLMN ID.

3.1 PLMN ID indicating the network that a user has subscribed to

PLMNs are constituted and operated by operators[2] for the purpose of providing mobile communication services to the public. A PLMN ID is used globally to identify the mobile communication network that a user has subscribed to. It consists of an MCC (Mobile Country Code) and an MNC (Mobile Network Code) as shown in Figure 2. The three-digit MCC identifies the country where the mobile network in use is located. And each country may have one or more PLMN IDs as needed. The MCC allocation is administered by the ITU-T and defined in ITU-T E.212 [3]. For example, Korea has the MCC value of 450. An MNC identifies the operator of a mobile communication network and is allocated by each country. For example, there are three mobile operators in Korea: SK Telecom, KT and LG U+, and their MNCs are shown in Figure 2.

- **PLMN ID Format**



MCC: Mobile Country Code
MNC: Mobile Network Code

- **Example: South Korea – KR**

MCC	MNC	Brand Name	Mobile Network Operator
450	02	KT	KT
450	04	KT	KT
450	05	SKT	SK Telecom
450	06	LG U+	LG Telecom
450	08	Olleh	KT

Figure 2. PLMN ID format and an example

[2] An operator means an administration or a recognized private operating agency (RPOA) as defined in TS 23.002.

3.2 IMSI: Permanent ID allocated to a mobile subscriber

International Mobile Subscriber Identity (IMSI) is a unique number identifying a mobile subscriber globally. Figure 3 shows an allocation process of an IMSI and the format of the IMSI. An IMSI is composed of a PLMN ID that indicates the network the user subscribes to and a Mobile Subscriber Identification Number (MSIN) that is assigned by the operator. The IMSI can have a maximum length of 15-digits. The MSIN identifies a mobile subscriber within a PLMN.

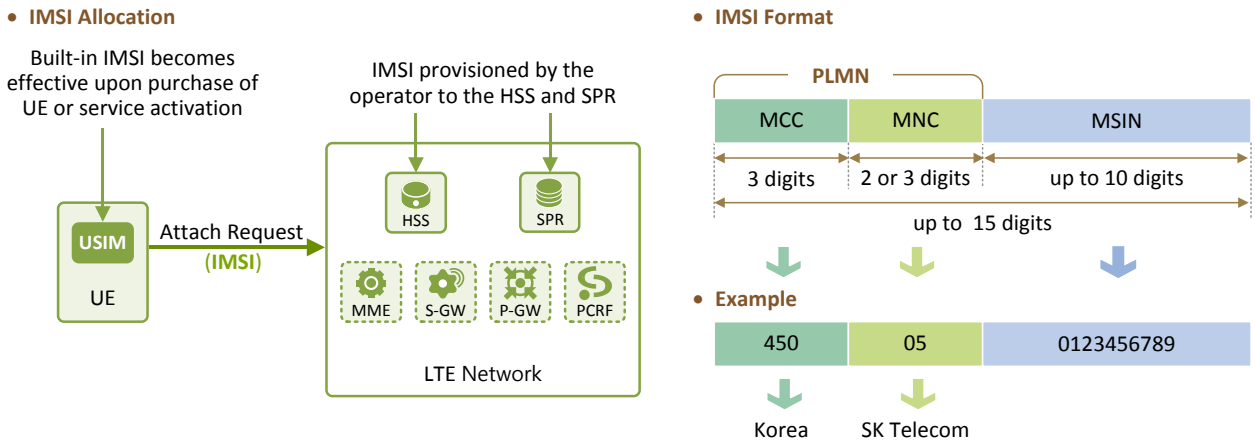


Figure 3. IMSI allocation and format

When a user purchases a USIM (only USIM or USIM with a phone) and subscribes to a mobile network, a built-in unique number called International Mobile Subscriber Identity (IMSI) becomes effective and associated with the user. The IMSI is stored in the USIM inside the phone, and the subscription information with the IMSI is provisioned to a Home Subscriber Server (HSS) and Subscriber Profile Repository (SPR) by the operator[3]. After being provisioned, the IMSI is sent by the UE to the mobile network when the UE attaches to the LTE network[4]. After receiving the IMSI from the UE, an MME begins establishment of a default EPS bearer, the basic transport path in the LTE network, by (i) identifying the home network of the subscriber based on the IMSI received from UE, (ii) selecting an HSS holding the subscription information of the subscriber and (iii) downloading the information from the HSS (For more information about establishment of default EPS bearers, see the technical document, “Initial Attach document”).

The IMSI installed in the USIM, HSS and SPR is a permanent value not to be removed. On the other hand, the IMSI stored in the MME, S-GW, P-GW and PCRF while establishing a default EPS bearer during a UE’s initial attach process is a temporary value to be removed when the default EPS bearer is terminated.

3.3 IDs Used at MME: GUTI, S-TMSI and M-TMSI

An IMSI is a permanent and unique ID that identifies a mobile subscriber. There might be security problems if it is frequently exposed over the radio link. For security enhancement, a Globally Unique Temporary Identifier (GUTI) is allocated to a UE by an MME when the UE attaches to the Network, and used instead of the IMSI to

[3] Unless otherwise specified, an operator means an LTE operator in this document.

[4] A UE begins initial attach to a LTE network by sending Attach Request message including an IMSI to an MME.

identify the UE. Figure 4 shows the allocation process and format of a GUTI.

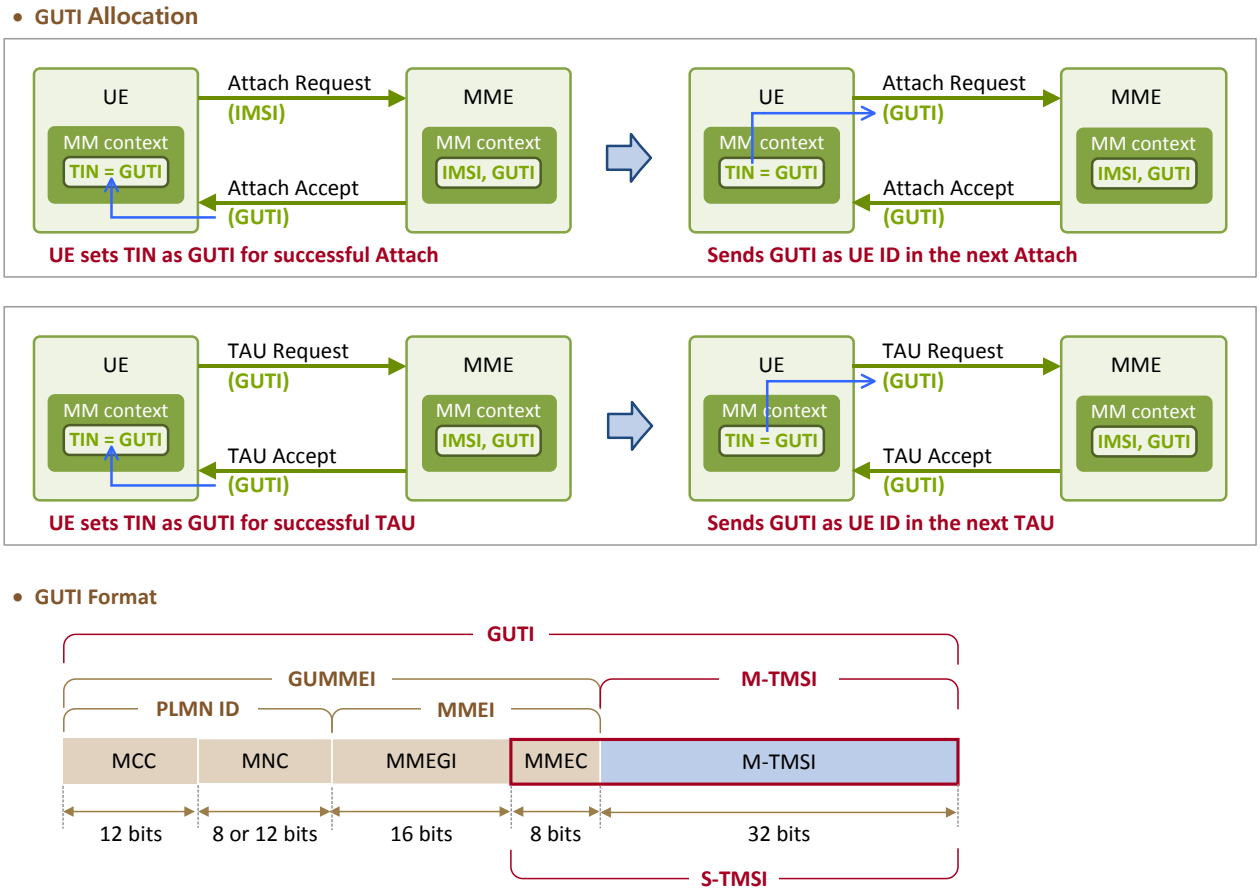


Figure 4. GUTI allocation and format

GUTI allocation: When a UE attaches to a LTE Network for the first time, it uses its IMSI to request access to the network and obtains a GUTI allocated by the network (i.e. MME). The UE thereafter uses the GUTI, instead of IMSI, when it attaches again to the network. Whether the UE uses IMSI or GUTI as its ID when reattaching to the network depends on which value is being set as Temporary Identifier used in Next update (TIN).

Once the initial attach process or the tracking area update (TAU)[5] procedure of the UE is performed successfully, the MME allocates and sends a GUTI to the UE[6], which then sets the GUTI as its TIN. The GUTI is used thereafter instead of the IMSI when the UE attaches to the network or requests TAU update.

GUTI format: An LTE operator can have one or more than one MME groups consisting of multiple MMEs. An MME Identifier (MMEI in Figure 4), therefore, is made up of an MME Group Identifier (MMEGI) that represents an MME group and an MME Code (MMEC) that represents an MME within the MME group. A Globally Unique MME Identifier (GUMMEI) is created by adding a PLMN ID to the MME ID. Each MME allocates an MME Temporary Mobile Subscriber Identity (M-TMSI), the unique value in the MME, to each registered subscriber to preserve the subscriber's confidentiality.

[5] A UE begins TAU (tracking area update) by sending **TAU Request** message to an MME.

[6] An MME delivers a GUTI to an UE through **Attach Accept** message when the UE initially attaches, and through **TAU Accept** message when TAU is updated.

A GUTI, composed of a GUMMEI and an M-TMSI, is a globally unique value and is used instead of an IMSI to identify a UE. Unlike an IMSI that has a fixed value, it has a temporary value that is allocated by an MME whenever a UE is registered to the LTE network. So the GUTI can still be kept secure even when frequently exposed over the radio link. An S-TMSI consisting of an MMEC and an M-TMSI is used to uniquely identify a UE within an MME group. It is shorter than a GUTI and thus it helps to improve transmission efficiency on radio links if used in an operator's network that does not have more than one MME groups.

3.4 IP Address: ID Necessary to Connect to a PDN

An IP address, also called as a "PDN address" is allocated by an LTE network to a UE in order for the UE to connect to a PDN (i.e. an IP network) when the UE initially attaches to the LTE network. Because a UE can be connected to more than one PDN through an LTE network depending on the services, the LTE network allocates each UE a different IP address per each PDN the UE is connected to (e.g. two IP addresses for a UE with two connected PDNs, three IP addresses for one with three PDNs, and so on.). These IP addresses (PDN addresses) are used to identify the UE from/to which an IP packet is sent when the IP packet is forwarded from an LTE network to a PDN, or received from a PDN.

An IP address is allocated to an UE either permanently or dynamically for the UE to connect to the PDN. These two types of allocation are called static IP address allocation and dynamic IP address allocation, respectively. (For more information, see the technical document, "IP Address Allocation").
In case of static IP address allocation, an operator allocates a permanent IP address to a UE at the time of subscription, and provisions the UE's IP address to an HSS (as shown in Figure 1). That way, the UE is assigned the same IP address every time it initially attaches to the PDN regardless of the time and location of such attach. In case of dynamic IP address allocation, a P-GW has an IP pool (as shown in Figure 1) and dynamically assigns an available IP address from the pool every time a UE performs initial attach to an LTE network. Therefore, a different IP address is assigned to a UE upon each initial attach of the UE to the network.

Figure 5 shows an example of dynamic IP address allocation. It provides a brief illustration of the procedure during which the P-GW dynamically allocates a temporary IP address when a default EPS bearer is established during the initial attach process (See "Initial Attach" document for detailed procedure of default EPS bearer establishment) and the procedure during which the UE uses the Internet service after allocating an dynamic IP address during the initial attach process (See [1] for the Internet traffic flow).

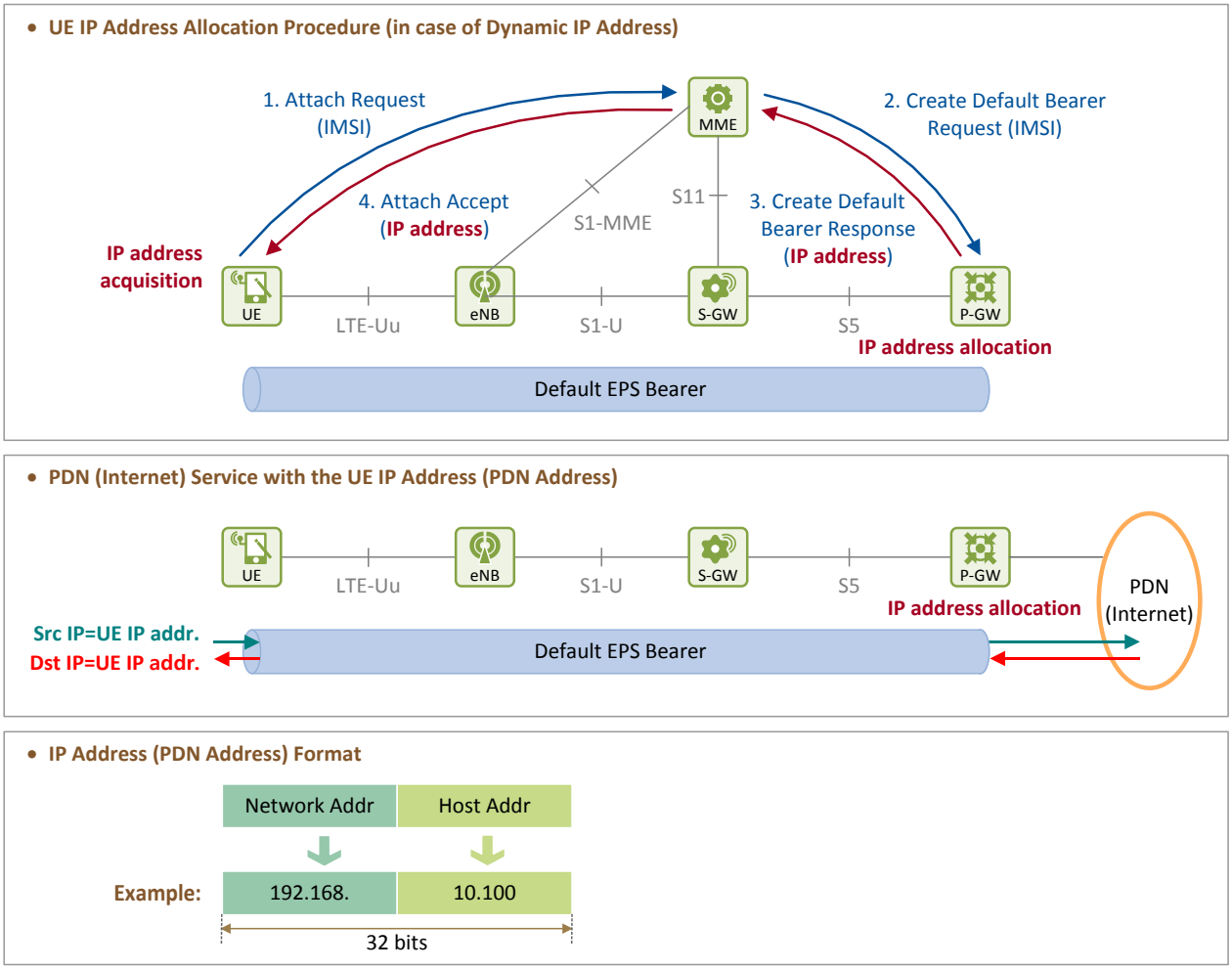


Figure 5. IP address allocation and format

3.5 C-RNTI: ID required to distinguish UEs within a Cell

Cell Radio Network Temporary Identifier (C-RNTI) is allocated to a UE by an eNB through a random access procedure in a cell controlled by the eNB and is effective only within the [serving] cell. UEs in the cell are uniquely identified by their C-RNTI. A new C-RNTI is allocated when the UE leaves the current cell and moves to a new cell through a random access procedure. Figure 6 shows how a C-RNTI is allocated and to which layer the C-RNTI is applied to.

An eNB is responsible for allocating radio resources to UEs on uplink and downlink. It notifies which UE can use the radio resources in the next Transmission Time Interval (TTI)[7] by broadcasting a C-RNTI on Physical Downlink Control Channel (PDCCH). If a UE finds its C-RNTI on the PDCCH in the cell it accessed, the UE then realizes it can use the radio resources in the next uplink or downlink TTI.

[7] TTI is the duration of an independent decodable transmission on radio links. TTI, also called "sub-frame", is a unit that constitutes a radio frame. Each TTI has a length of one ms (e.g. a 10 ms radio frame consists of 10 one ms TTIs (or sub-frames)).

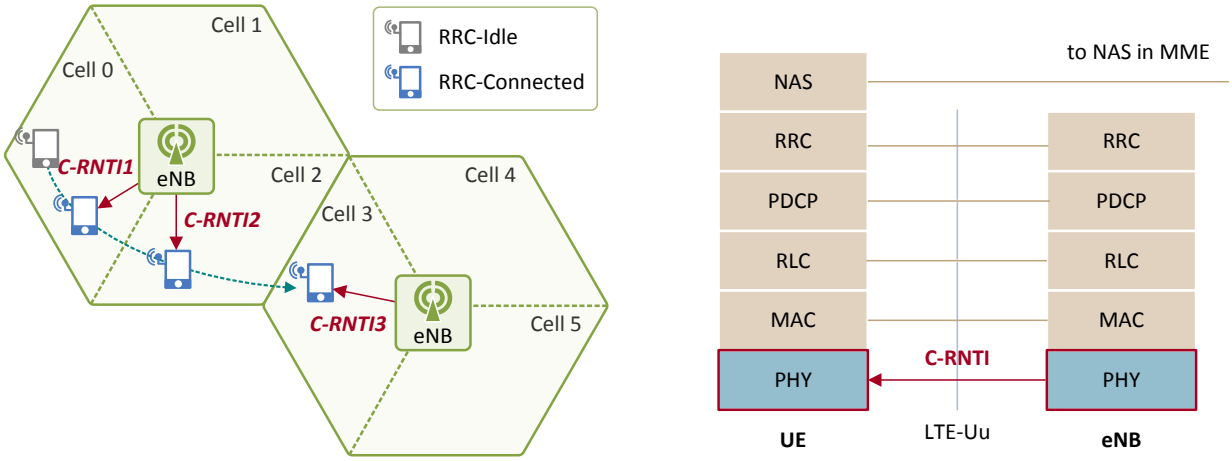


Figure 6. C-RNTI allocation

3.6 Paired UE S1AP IDs needed to distinguish UEs over the S1-MME Interface

S1AP layer handles the control messages between an eNB and an MME over an S1-MME interface. Many UEs stay connected to an eNB at the same time. And the eNB uses the same S1 link for all the S1AP control messages it exchanges with an MME with respect to the UEs. So, in order to tell which S1AP message is for which UE, an eNB allocates an ID (eNB UE S1AP ID) to each UE when it sends the first S1AP message for a UE to an MME. Likewise, one MME exchanges S1AP messages with many eNBs (e.g. more than hundreds) and through many S1 links concurrently. Again, in order to tell which S1AP message is for which UE in which eNB, the MME allocates an ID (MME UE S1AP ID) to each UE when it sends the first message for a UE to an eNB.

After this very first round trip of S1AP message, all the user control messages (S1AP messages) exchanged over the S1-MME interface are delivered with a pair of UE S1AP IDs (eNB UE S1AP ID, MME UE S1AP ID) in order that the eNB and the MME can tell which S1AP message is for which UE. Then, with the paired IDs, the MME can find out which UE in which eNB the received S1AP message is for, and the eNB can also tell which UE the received S1AP message is for. Figure 7 shows the process of UE S1AP ID allocation and the S1AP layer where the UE S1AP ID is applied.

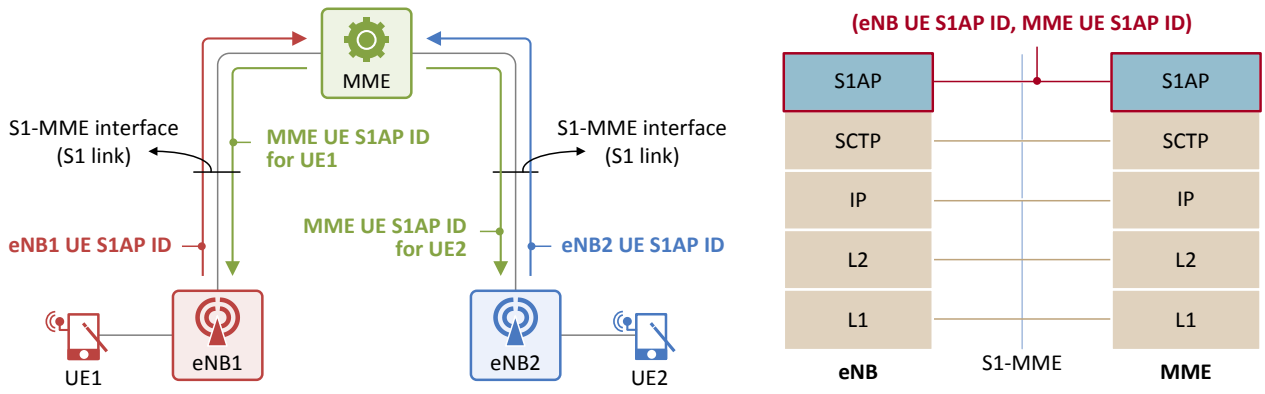


Figure 7. UE S1AP ID allocation and S1AP layer

3.7 Paired UE X2AP IDs needed to distinguish UEs over the X2 Interface

X2AP layer handles the control messages (X2AP messages) between two neighbor eNBs over an X2 interface. During each handover of UEs between two neighbor eNBs, the X2AP messages from the UEs are delivered to the peer eNB using the same X2 link. The first time an eNB (source eNB or target eNB) sends a X2AP message to a peer eNB, the eNB assigns an ID to each UE and sends the message with the ID in order to show for which UE the X2AP message is. A source eNB allocates an Old eNB UE X2AP ID to its first message (Handover Request message) to a target eNB, which also allocates a New eNB UE X2AP ID to its first response message (Handover Request Acknowledge message) to the source eNB.

After this very first round trip, all the handover-related X2AP messages over the X2 interface are exchanged with a pair of IDs (Old eNB UE X2AP ID, New eNB UE X2AP ID) in order that the source eNB and the target eNB can tell which X2AP messages are for which UE. Figure 8 shows the process of UE X2AP ID allocation and the X2AP layer where the UE X2AP ID is applied.

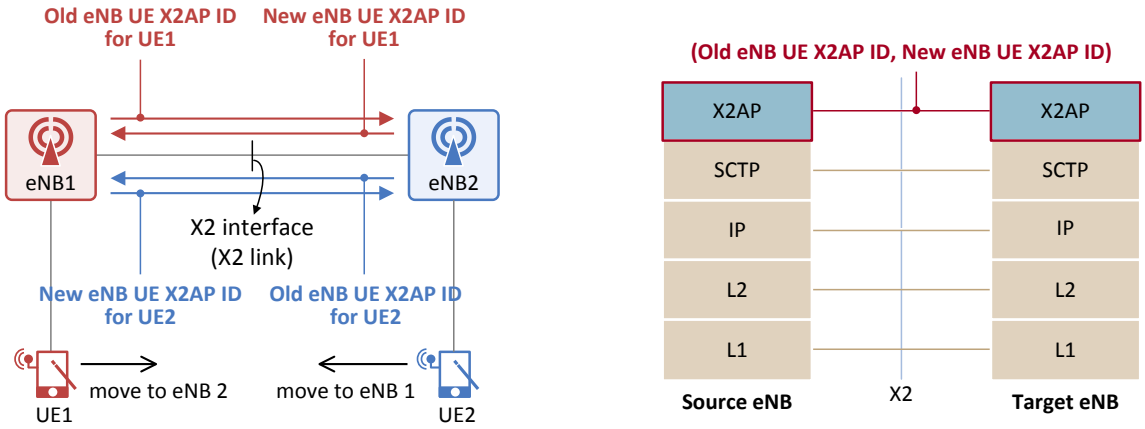


Figure 8. UE X2AP ID allocation and X2AP layer

IV. Identifiers for Mobile Equipment (ME IDs)

Chapter IV describes IDs of Mobile Equipment (ME). The relationship between UEs and MEs is described first before ME IDs are discussed. A UE consists of an ME and a UMTS Subscriber identity Module (USIM), and an ME can further be divided into Terminal Equipment (TE) and a Mobile Terminal (MT). An MT is where radio access protocols work (e.g. USB dongle) while TE is where the MT control functions work. Figure 9 shows a couple of combinations of such functional groups as examples. The MT and the TE are integrated in a mobile phone, but separated in a note PC.

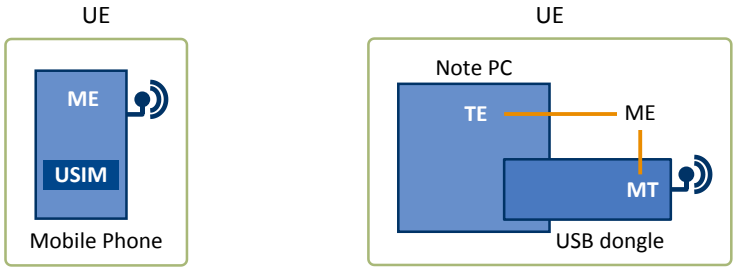


Figure 9. Relationship between UE and ME

4.1 IMEI and IMEISV: IDs permanently owned by an ME

International Mobile Equipment Identity (IMEI) is a unique number allocated to each mobile equipment (ME). An IMEI is given when an ME is being manufactured, and contains information about the manufacturer, model, and serial number of the ME. Figure 10 illustrates the format of an IMEI and an example of an IMEI usage. The IMEI is composed of a Type Allocation Code (TAC), a Serial Number (SNR) and a Check Digit (CD). And an IMEI/SV is composed of a TAC, an SNR and a Software Version Number (SVN).

A TAC is made up of a Reporting Body Identifier (RBID) that indicates a reporting body (See GSMA "IMEI Allocation and Approval Guidelines" [4] for the RBID list and codes), and an ME Type ID that represents the manufacturer's name and the model identifier. Serial numbers are assigned by the manufacturer. In the example used in Figure 10, the RBID of "35" indicates the ME was approved by British Approvals Board for Telecommunications (BABT), and the ME Type ID of "643205" shows the ME is a smartphone manufactured by Samsung.

An operator has a DB[8] storing IMEI information, and thus can deny any access attempted by an ME reported stolen or lost using the DB.

- **IMEI, IMEI/SV Format**

- IMEI:

- IMEI/SV:

	Format	Description [4]
TAC*	NN	**Reporting Body ID**
	XXXXYY	**ME Type ID** defined by Reporting Body
SNR	ZZZZZZ	**Serial No**, Allocated by Reporting Body but assigned per ME by the manufacturer
CD	A	**Check Digit**, defined as a function of all other IMEI digits
SVN	SS	**Software Version Number**, 00 – 98. 99 is reserved for future use.

* TAC: Type Allocation Code

- **Example**

IMEI: 356432053951377			
TAC	35643205		
	RBID	35	BABT**
	ME Type ID	643205	Samsung SHV-E330S
SNR	395137		
CD	7		

Device Information	
Brand	Samsung
Model	SHV-E330S
Manufacturer	Samsung Korea
Device type	Phone
Additional Info.	E330S Galaxy S4 LTE-A

** BABT: British Approvals Board for Telecommunications

Figure 10. IMEI format and an example applied

[8] A DB containing IMEI information is called EIR (Equipment Identity Register).

V. Closing

We have discussed LTE identification before we move on to LTE technology. In this document, we have first explained UE and ME IDs, and then classified and summarized these IDs in terms of their range (within which IDs are uniquely identified), allocators and attribute type as shown in Table 2. Other IDs shown in Table 1 will be described in the companion documents that follow, LTE Identification II and III.

Table 2. LTE Identifiers: UE and ME

ID group	LTE Identifier	Range (uniquely identified within)	Allocator	Type of value
UE ID	IMSI	Global	Operator	Permanent
	GUTI	Global	MME	Temporary
	S-TMSI	MME Group	MME	Temporary
	IP address (PDN address)	Global (public IP addr)	Operator (static IP addr)	Permanent
		PLMN (private IP addr)	P-GW (dynamic IP addr)	Temporary
	C-RNTI	Cell	eNB	Temporary
	eNB UE S1AP ID	eNB	eNB	Temporary
	MME UE S1AP ID	MME	MME	Temporary
	Old UE X2AP ID	eNB	Source eNB	Temporary
	New UE X2AP ID	eNB	Target eNB	Temporary
ME ID	IMEI	Global	Manufacturer	Permanent

References

[1] Netmanias Technology Document, “LTE Network Architecture: Basic”, July 2013, http://www.netmanias.com/en/?m=view&id=techdocs&no=5904

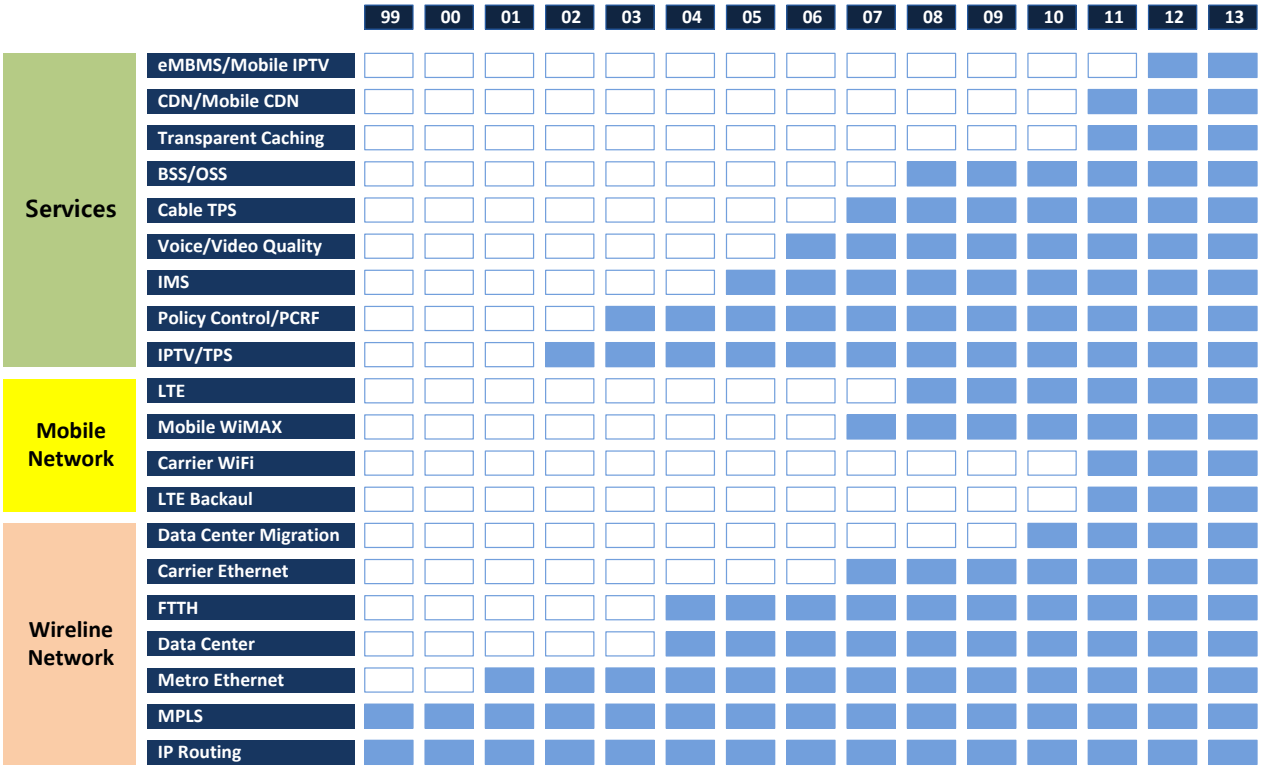
[2] 3GPP TS 23.003, “Numbering, addressing and identification”.

[3] ITU-T E.212, “The international identification plan for public networks and subscriptions”.

[4] GSMA TS.06, “IMEI Allocation and Approval Guidelines”.

[5] 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.