LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

**LTE for Layman (part 3) - The Complete Picture!**

In this final part of "LTE for Layman" series, we conclude the learnings of first and second part to fully understand the underlying technology behind your LTE cell phone. In this entry, we try to establish complete picture of how your LTE enabled phone is able to upload #instagram selfie in seconds! Do go through the previous parts of this series, as most of the terminologies used in this text are explained beforehand. In case you are already knowledgeable in that, do read on for understanding the complete UE lifecycle, step by step, layman style!

**STEP 1: SCANNING**

When you switch on your brand new LTE enabled phone for the very first time, the first step (and this is true for all generations) is scanning. Your phone scans all the available radio frequencies in the given LTE band, also known as E-UTRA Absolute Radio Frequency Channel Number or (EARFCN). This is analogous to a simple Radio FM scan operation, which scans for all channels to check where the music is playing! For example, my Moto X play phone supports 800/900 /1800/2100/2600 MHz frequency. So when my phone is switched on for



**Messaging**

1 of 17 11/05/20, 12:50 am

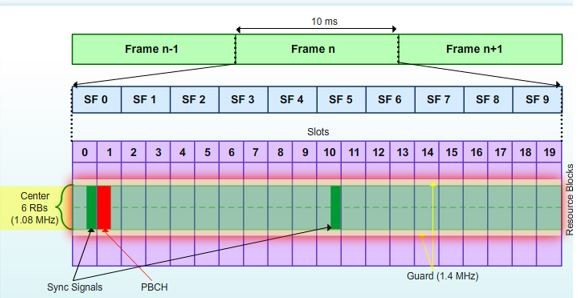
LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

the first time, it scans all these supported frequencies to see whether network is available. Suppose UE finds signals in all the band frequencies, which frequency does UE tune in? Frequency latching is decided on basis of something called **RSRP** or **Reference Signal** **Received Power**. This is a power measurement level of signal,analogous to which frequency is the strongest. The strongest RSRP emitting frequency is selected, and UE moves onto the next step.

**STEP 2: DOWNLINK SYNCHRONIZATION**

In this step, UE establishes cell level synchronization at the downlink level. This essentially means UE needs to know the physical cell id (PCI), and also the measurement units of signal, i.e slot and frame timings. This is done by acquiring Synchronization signals, which are always transmitted in center frequency of the acquired band (or center 62 sub carriers). There are two types of Synchronization signal:

 **Primary Synchronization signal (PSS)**: Determined using DC subcarrier or center frequency, this is always transmitted at last OFDM symbol of 1st and 11th time slot. Once UE has acquired PSS, it synchronizes on slot level basis, and knows the physical layer identity (0 – 2).

 **Secondary Synchronization signal (SSS)**: Sent at a slot just beforePSS, it is responsible for frame level synchronization. UE now knows the physical layer cell identity group (0 – 167).

Using both PSS and SSS, UE can calculate PCI or Physical Cell Identity by using a formula:

**PCI = 3\*(Physical layer cell identity group) + physical layer identity.**

If the formula or anything about synchronization seems a bit confusing, remember the basics of LTE measurement! The center frequency acts as a reference point for Y axis measurement. From there, moving a certain X axis of time slots helps UE acquire these signals to calculate the PCI and achieve complete synchronization of both X axis and Y axis.

**STEP 3: Decoding Broadcast Information**



**Messaging**

2 of 17 11/05/20, 12:50 am

LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

In this step, UE acquires key system information to establish complete downlink synchronization with the cell. There are two primary key information blocks that UE needs to know.

First key information that UE needs to know is the system bandwidth. This is acquired by something called **Master Information Block** (MIB). Having acquired the measurement units (slot and frame level synchronization), UE latches on the same center frequency and this time reads first 4 OFDM symbols of second slot of first sub frame. This is where MIB is transmitted on the physical broadcast channel. Since MIB is very crucial, it is transmitted every **40ms**, with the copies being transmitted every 10ms. This way, UE is ensured that it can create complete MIB even from the copies, and knows when a new MIB is transmitted (and the 40ms boundary). Upon decoding MIB, UE knows the following:

Rohan: MIB is in PBCH

 **System Bandwidth**: Determines how many resource blocks arefunctional for this cell, necessary for decoding any other physical channels.

 **PHICH information**: The size and duration of PHICH channel isgiven here, which is essential to diﬀerentiate between PCFICH and PDCCH channel (as all control channels share same region). PCFICH location is fixed and known, so by knowing PHICH location, UE can read the critical PDCCH region structure to get control level information for further decoding of broadcast information.

 **System Frame Number**: this is the clock of eNodeB. By knowingthe SFN, UE establishes complete synchronization with the eNodeB’s system timing.

After decoding MIB, UE has enough information to understand the control region structure of the downlink channel (or PDCCH). It’s from there that UE can know the information about second most critical information block called **System Information Blocks** (or SIBs). SIBs are of thirteen types! But luckily, only first two SIBs are essential for UE to decode complete eNodeB information. SIB 1 carries **Cell access** **related parameters and scheduling information** of other SIBs. Anew SIB 1 is transmitted every **80 ms** (every eight frames), but to add redundancy and to reduce acquisition time for the UE, it is repeated every other frame. SIB Type 1 also informs the UE of the expected schedule for the remaining SIBs which can be as often as every 8 frames

Rohan: SIB is in PDCCH

Rohan: Adding redundancy in communication systems

<https://www.quora.com/What-are-differences-between-source-coding-and-channel-coding>



**Messaging**

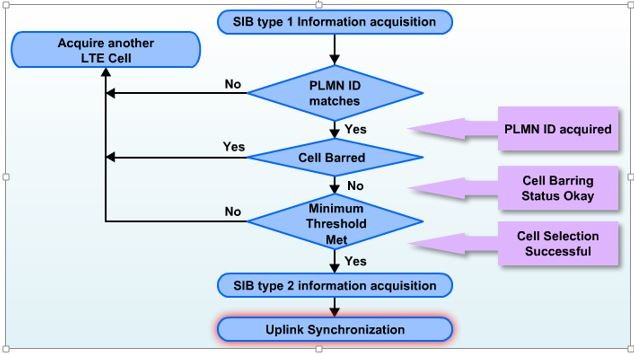
3 of 17 11/05/20, 12:50 am

LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

or as seldom as every 512 frames. For the remaining SIBs, the network operator will configure which ones are necessary.

**STEP 4: OPERATOR SELECTION**

For cell selection, the UE requires the **PLMN ID** (Public Land Mobile Network ID) of the network, cell barring status and minimum signal strength threshold from SIB type 1. The UE first checks the PLMN ID. PLMN ID is nothing but the operator id, and every operator is assigned one. It consists of two codes, a **Mobile Country Code** (MCC) and **Mobile Network Code** (MNC). Not going too much into theidentification schemes, but if analogy is drawn, think of PLMN ID as the legal ID card for your operators (eg: Airtel) to provide telecommunication services in a country. LTE cell supports a PLMN that the UE is allowed to use (naturally, your operator), and the UE will continue on to check the cell barred status. There are several reasons a cell on the air might be barred from commercial use. If for example, it is a test cell, we wouldn’t want the UE to continue on this cell. If the cell barring status is okay, the UE will check the minimum signal strength threshold to learn if it passes the signal strength criteria for the cell. Some UEs at or near the cell edge can be blocked from trying to access the cell using minimum signal strength threshold. Of course, if any of these criteria fail, the UE will have to find another LTE cell. Once cell selection is successful, the UE will read the information in SIB Type 2 to get the parameters it requires for beginning uplink synchronization.



**STEP 5: UPLINK SYNCHORNIZATION**

In this step, UE undergoes a procedure called “**RACH**” or Random Access to gain access of the resources to start transmission of uplink data. So far, UE has been only receiving messages without any capability to send its own messages. After RACH procedure is completed, UE gets into something called “**RRC Connected State**”, and gets dedicated bearers established to begin the transmission of #instagram selfie!

Let’s try to understand the RACH procedure in detail:

1.) **Message 1**: After reading SIB Type 2, the UE will know the format and location of the **PRACH**. This is the physical channel in which UEs are allowed to send their first transmission to the LTE network.

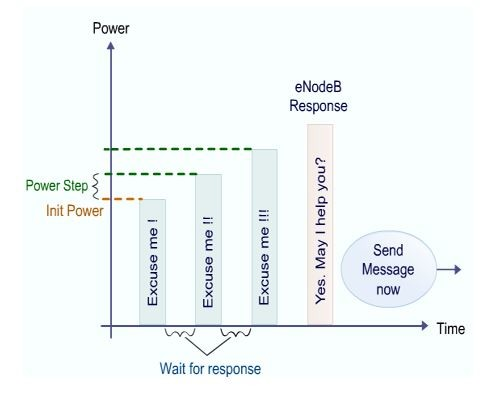
Rohan: First UP message is over RACH--PRACH

Each cell will also have a pool of **preambles** (short bit of message sequences)

which are unique from any neighboring cells. SIB Type 2 communicates to the UE the set of preambles (64 available in a cell) from which it will randomly choose for uplink synchronization. Now UE also needs to give its own identity to the network so that network can address it in next step. The identity which UE will use is called **RA-RNTI** (Random access radio network temporary identity). If UE does not receive any response from the network, it increases its power in fixed step and sends RACH preamble again.

Rohan: UE selects one RACH preamble from cells unique set of preambles. UE get this set from SIB2.

UE sends RA-RNTI + Unique RACH preamble on PRACH, in repeated process as shown below



2.) Message 2: eNodeB sends "Random Access Response" to UE on DL-SCH (Downlink shared channel) addressed to RA-RNTI. The message carries following information:

 **Temporary C-RNTI**: Now eNB gives another identity to UE which iscalled temporary C-RNTI (cell radio network temporary identity) for further communication

 **Timing Advance Value**: eNodeB also informs UE to change itstiming so it can compensate for the round trip delay caused by UE’s distance from the eNodeB

 **Uplink Grant Resource**: Network (eNodeB) will assign initialresource to UE so that it can use UL-SCH (Uplink shared channel).

Rohan: This down message on DL-SCH – PDSCH

Is this where it starts using SRB0

https://www.rfwireless-world.com/Tutorials/LTE-signaling-radio-bearers.html

RRC Conn Request Message uses SRB0 over CCCH—UL-SCH--PUSCH

Resource = Virtual pipe = bearer 0 allocated]

3.) **Message 3**: Using UL-SCH, UE sends "RRC connection request message" to eNodeB. UE is identified by temporary C-RNTI (assigned in the previous step by eNodeB). The message contains following:

Rohan: Second UP message is over UL-SCH -- PUSCH??

 **UE identity (TMSI or Random Value): TMSI** (Temporary MobileSubscriber Identity, used to protect privacy) is used if UE has previously connected to the same network (as Authentication Center allocates TMSI, and will have record of previous connections). With TMSI value, UE is identified in the core network. Random value is used if UE is connecting for the very first time to network. Why we need random value or TMSI? Because there is possibility that Temp-CRNTI has been assigned to more than one UEs in previous step, due to multiple requests coming at same time.

eNodeB). The message contains following:

Rohan: Second UP message is over UL-SCH -- PUSCH??

 **UE identity (TMSI or Random Value): TMSI** (Temporary MobileSubscriber Identity, used to protect privacy) is used if UE has previously connected to the same network (as Authentication Center allocates TMSI, and will have record

 **Connection establishment cause**: The shows the reason why UEneeds to connect to network.



**Messaging**

5 of 17 11/05/20, 12:50 am

LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

4.) **Message 4**: eNodeB responds with contention resolution message to UE whose message was successfully received in step 3. This message is address towards TMSI value or Random number (from previous steps) but contains the new C RNTI which will be used for the further communication.

The above example didn't consider any collision. Collision can occur because of following example scenario:

Let us assume two UEs send same RACH preamble at same time in step 1

Same Temp C-RNTI and up-link grant will be received by two UEs in step 2.

In step 3 eNodeB may be able to receive Msg3 from only one UE or none of them due to interference.

In step 4 the UE which does not receive Msg4 from eNodeB will back-oﬀ after expiration of RACH specific timers.

Possibility is also that none of them receive Msg4. The UE which receives msg4 will move to next step and decode RRC connection setup message.

Rohan:

Msg 1 and Msg 2 same, then Msg 3 random

But what about Msg 4, how does it clash, how is it used by UE????

Rohan: At this point UE is in RRC Connected State

**STEP 6: RRC Connection Setup**

 The first message from the UE is the **RRC Connection Request**. The UE will include in this message its UE identity, and the Establishment cause, for example; Emergency, Mobile originated Signaling, or Mobile originated Data.

Rohan: Is this message 3 in above step???

Rohan: Here we use SRB0 for RRC Conn Request

<https://www.rfwireless-world.com/Tutorials/LTEsignalling-radio-bearers.html>

RRC Conn Request Message uses SRB0 over CCCH--UL-SCH--PUSCH

About bearer: A bearer is a virtual pipe that is used to carry data from one

point to another

Default Bearer = normal one, non-GBR(Guaranteed Bit Rate)

Dedicated Bearer = carry specific traffic, linked with default Br, GBR/nonGBR

SRB = Signalling Radio Bearer

DRB = Data Radio Bearer

More bearer

<https://www.rfwireless-world.com/Tutorials/LTE-Bearer-types.html>

Among default bearers SRB0,1,2 all have fixed messages to carry as

defined in link above, above link

Each UE will have their own set of bearers

Bearer play important role in QoS

Bearer is above L1 layer concept, nothing to do with frequency

<https://www.sharetechnote.com/html/Handbook_LTE_SRB_Mapping.html>

 The eNB responds to the UE with the **RRC Connection Setup**. This message is used to establish SRB1 and the UE will now be identified by a C-RNTI which is assigned by the eNB. The details of SRB1 are provided to the UE by the eNB in this message.

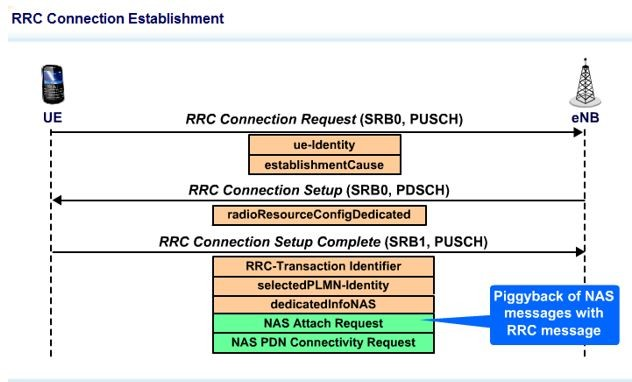
Rohan: Is this message 4 in above step???

 Finally, using the just-allocated SRB1, the UE now sends an **RRC** **Connection Setup Complete** message to the eNB to confirm thesuccessful completion of an RRC connection establishment. It includes the selected PLMN identity from the PLMN-Identity list provided in the SIB Type 1 and the first uplink NAS message containers. This includes the piggybacked **Attach Request** and **PDN** **Connectivity Request** messages to be transferred by the eNB to theMME.

Rohan: Here we use SRB1 for RRC Conn Setup Compelete

<https://www.rfwireless-world.com/Tutorials/LTEsignalling-radio-bearers.html> RRC Conn Request Message uses SRB1 over DCCH--UL-SCH--PUSCH  
SRB 2 also uses DCCH--UL-SCH--PUSCH channels

 On the successful completion of the RRC Connection establishment procedure, the UE is in the **RRC\_Connected** mode.



Rohan: Piggyback message, same happens in 5G N3GPP Reg Procedure. Reg Request goes in IKEv2 signaling instead of normal TCP message

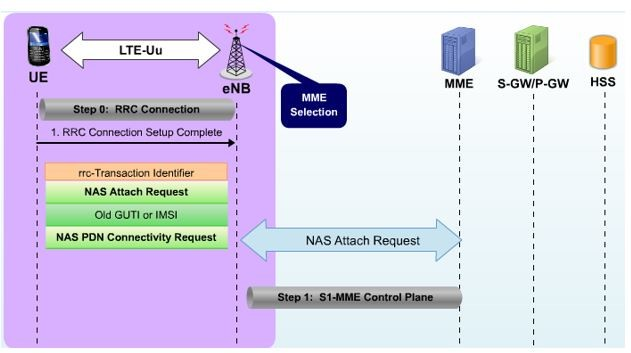
**STEP 7: Initial Attach**

The UE initiates the attach procedure with the completion of setting up the RRC connection. The NAS Attach Request is piggybacked to the RRC message. Also piggybacked on the RRC message is the NAS PDN Connectivity request which will also be passed to the MME for processing after the Attach.

Rohan: Check what is NAS PDN Connectivity request’s use => explained in step 9

The eNB, upon receiving the Attach Request will have to select an MME. MME selection can be based upon several network operator definable criteria including: MME loading, LTE network topology, and which MME last served the UE.

In the Attach Request, the UE will identify itself by sending its IMSI (International Mobile Subscriber Identity) or old GUTI (Globally Unique Temporary ID).



Rohan: Here we can see S1-AP connection is up, similar to NGAP connection up on successful NGSetup

Rohan:

In 5G, UE acquires Old GUTI from Reg Accept NAS message from previous AMF it registered to, lte mein b same hoga

So for first time usage IMSI is must, which is unsafe

About IMSI and GUTI https://www.netmanias.com/en/post/blog/5929/lte/lte-user-identifiers-imsi-and-guti

All initial attach cases <https://www.netmanias.com/en/?m=view&id=techdocs&no=10440>

IMSI Catchers <https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy>

5G uses SUCI instead of plain IMSI, tells why SUCI > IMSI

<https://blog.wirelessmoves.com/2018/04/the-5g-core-network-5gc-part-2-identifiers.html>  
Read 4G EPS-AKA tells why SUCI > GUTI

<https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication>

5G-Identifiers: <http://5gstuff.blogspot.com/2018/04/5g-identifiers-supi-pei-guti.html>

5G TS’es <https://blog.wirelessmoves.com/2017/09/5g-part-1.html>  
More about 5G https://blog.wirelessmoves.com/category/5g

In MME Selection: it says topology based selection, is it same as AMF Region ID used in 5G AMF Selection

**STEP 8.a: Authentication**

As part of processing the initial Attach, the MME will have to perform authentication of the subscriber. To initiate authentication, the MME will request authentication information from the HSS. The HSS will send an **authentication token** (AUTN), an **expected response** (XRES) and the **RAND** it used to generate the XRES to the MME. Now the MME has thenecessary information for completing authentication with the SIM card in the UE.

The MME sends an Authentication Request to the UE, including the RAND and the AUTN which it received from the HSS. The SIM card in the UE will process the request, using the RAND it received and its pre-shared secret key to generate authentication parameters. The SIM can use this to authenticate the requesting network prior to sending any response. If the network is authenticated, the UE will send an Authentication Response back to the MME, including the **Response** (RES). If the RES the UE sends matches the XRES the MME got from the HSS, then the subscriber is authenticated and we can proceed to the next step which is establishing security.

Rohan:

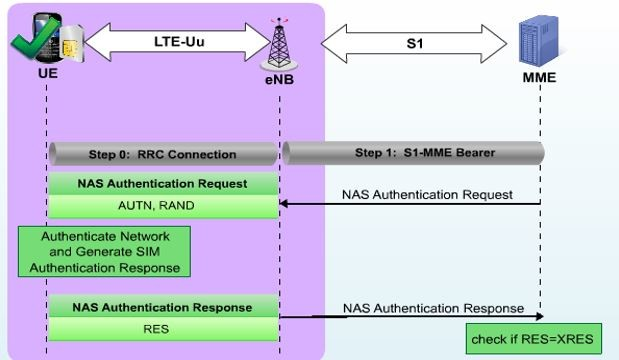
In detail https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication

Else check Cse teams AMF doc

In Non-3gpp, we have one more level of authentication, Wifi AP Auth using AAA Server   
https://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/

https://www.rfwireless-world.com/Terminology/Radius-protocol-vs-Diameter-protocol.html





7 of 17 11/05/20, 12:50 am

LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

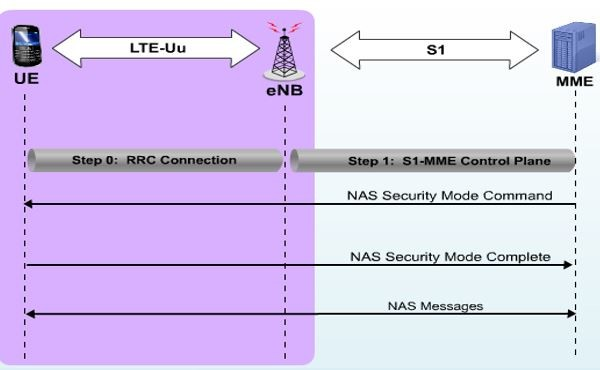
**STEP 8.b: Non Access Stratum Security:**

Now that the subscriber has been authenticated and is allowed to use the LTE network, the MME will initiate establishment of security between the UE and the MME, and between the UE and the eNB. The first step is to establish security for NAS signaling. The MME will first select the NAS integrity and encryption algorithm to be used. It will then convey this information to the UE in a **NAS Security Mode Command** message. This message is integrity protected (meaning no one can modify this message). The selection of integrity and encryption algorithms is based on a prioritized list configured at the MME and the security capabilities of the UE.

Rohan: Network sends security capabilities to UE

The UE makes a note of the selected encryption and integrity algorithms and validates the integrity of the received message. It then acknowledges the successful acceptance of the message by sending a **Security Mode Complete** message. This message is both integrityprotected and encrypted (meaning no one can read the message), and all future NAS signaling will be both integrity protected and encrypted.

The integrity procedure starts at the MME with the transmission of the NAS Security Mode Command and encryption at the MME starts after receiving the Security Mode Complete message. Integrity and encryption procedures start at the UE with the transmission of the NAS Security Mode Complete message.



**STEP 8.c: Access Stratum Security**

Once NAS security is established, the MME will let the eNB know to establish a context for the UE. This will cause the eNB to initiate establishment of Access Stratum (AS) security with the UE. In this case, it is the eNB selecting the RRC integrity and encryption algorithm to be used in addition to the user plane (UP) encryption algorithms for user traﬀic. The eNB will then convey this information to the UE in an **RRC** **Security Mode Command**. This message is integrity protected.

The UE makes a note of the selected encryption and integrity algorithms and validates the integrity of the received message. It then generates the keys required for these algorithms. UE acknowledges the successful acceptance of the message by sending an **RRC Security Mode Complete** message. This message is integrity protected. All subsequentRRC signaling will be integrity protected and both signaling and user traﬀic will be encrypted.

Rohan: Difference AS and NAS Security

ue<->mme ; ue<->enb

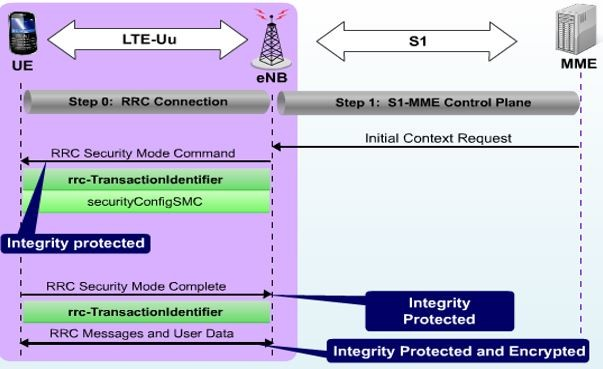
ue selects algo, enb selects algo

nas s/g integrity+encrypted; rrc s/g integrity+ecrypted and data encrpyted

ue matchs ue sec capabilities; ue generates keys

complete msg is int+encrypt; complete msg is int

AS Security trigger is Initial Context Setup message



**STEP 9: PDN Connectivity**

Now that the MME has completed authentication and security establishment (NAS and AS), the Attach is complete and the MME is managing the UE. In addition to the Attach Request, the UE also requested access to data services. Every UE in an LTE network will have at least one default connection established to a PDN.

Recall, that when the RRC connection was setup, the UE had piggybacked two NAS messages. The second of those messages, the **PDN Connectivity Request**, caused the MME to establish a defaultbearer for user traﬀic between the UE and a P-GW after authentication was completed.

Rohan: APN == DNN (APN is similar to dnn1.slice.net) and PDN = DN

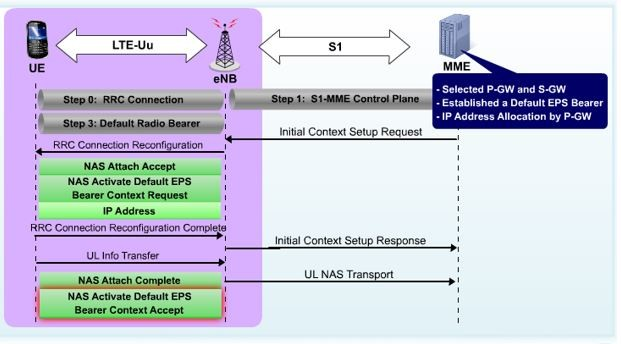
APN: Access Point Name, DNN: Data Network Name, PDN: Packet Data Network

The MME used a default APN, specific to that UE, which it received from the HSS subscriber database to determine to which PDN we are connecting and selected the appropriate P-GW for that PDN. Then the MME selected an S-GW and established the user traﬀic bearer in the EPC for the UE. The complete bearer path was not completed until security was established on the Access Stratum. As part of the bearer establishment in the EPC, the P-GW allocated an IP address for the UE. The IP address is delivered to the UE in the NAS Activate Default EPS Bearer Context Request message.

Rohan: Bearer setup details and IPv4 details in NAS reach at RAN through Initial context setup , bearer setup used at RAN then forwarded to UE along with IPv4 details is forwarded to UE..  
This is similar to 5G I nitial Context Setup which carries datapath info + NAS PDU carrying Ipv4 + .

Rohan: Below diagram shows RRC Reconfiguration carrying Attach Accept, Bearer Info, and IPv4

To acknowledge the completion of the Attach procedure and the establishment of the default EPS bearer, the UE sends 2 NAS messages to the MME: **Attach Complete** and **Activate Default EPS Bearer** **Context Accept**.



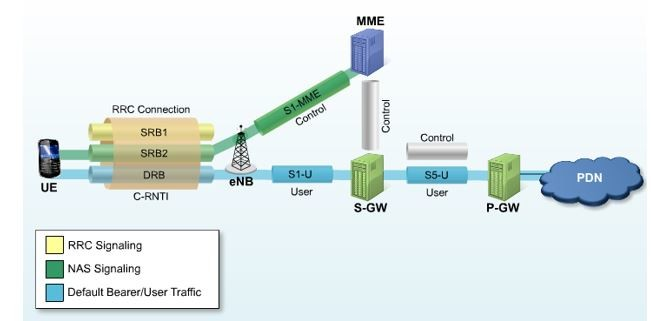
Once the IP address is allocated, end to end traﬀic starts flowing and your #instagram selfie finally finds its way into the Instagram servers over the internet! The end to end bearer connection looks something like this:



**Messaging**

9 of 17 11/05/20, 12:50 am

LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...



Now we know how an end to end LTE connection is established.

But what happens in maintaining that end to end connection, in both downlink and uplink direction? Let’s find out!

Rohan: Pts to discuss

* Traffic Handling in Downlink
* Traffic Handling in Uplink
* Idle
* Paging and Paging Request (Service Request)
* Handover

**Traffic Handling in Downlink**

In LTE, the coding and modulation schemes for downlink transmission are not fixed, instead, they are adapted to the air link conditions. **Channel Quality Indicator** (CQI) is a mechanism the UE can use tooﬀer feedback about these conditions to the eNB. So, we can say that *CQI is an indicator of downlink conditions as perceived by the UE*. It isimportant to note, that the derivation of CQI by the UE is not standardized, but rather proprietary to the manufacturer of the UE which can also include RS measurements and other information like Block Error Rate (BLER). When a UE reports a CQI value, it is making a statement to the eNB about the data rate it needs.

All UEs which are RRC\_Connected will monitor the reference signals embedded within the downlink transmissions. The measured quality of these signals helps the UE to determine the largest block size and modulation rate that it is capable of receiving. Using this information, the UE will encode a CQI index which is reported to the eNB using the Physical Uplink Control Channel (PUCCH) or, if uplink bandwidth has been allocated, it will include it on the Physical Uplink Shared Channel (PUSCH). It should be noted that depending upon the operator configuration, CQI reporting may be established as periodic or can be requested by the eNB as needed.



To sum up, following steps are followed to maintain traﬀic in downlink:

 CQI is transmitted using PUCCH.

 Downlink Scheduler uses CQI of each UE and recent allocation history. It makes a decision as to which set of UE gets downlink resource at this time.

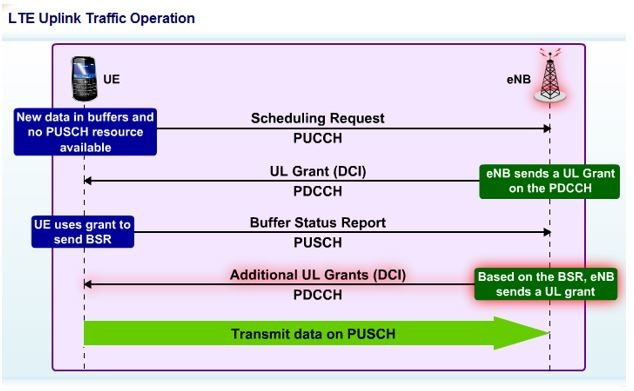
 eNodeB sends control information to ensure that the selected UE understand their allocation of resources. This is because many UE’s have given CQI.

Rohan: Is this the control information which tells which time slots and which RB belong to me? Does it also tell UE which slots to refer in each RB??

 At the end performs checksum of the packet and sends ACK/NACK back to eNodeB.

**Traffic Handling in Uplink**

When the UE has data to send, it must first let the eNB know that it has data, how much data, and what is the priority of data, so the eNB can properly prioritize and schedule uplink bandwidth. This process begins with the UE sending a **Scheduling Request**. The Scheduling Request is an uplink control element and it is like *raising a flag that lets the eNB* *know that the UE has data*.

In order to find out what data the UE has to send, the eNB will allocate just enough uplink resources for the UE to send a Buﬀer Status Report (BSR). The BSR will let the eNB know how much data the UE is buﬀering and the priorities of the data. Based on the BSR, the eNB will schedule the UE to send data in the uplink.

To sum up, following steps are followed to maintain traﬀic in uplink direction:

Rohan: Here communication takes place over PUCCH PDCCH to get PUSCH

 Each UE sends a scheduling request and buﬀer status report to inform the eNodeB of its current BW needs.

 The uplink scheduler then looks at all the requests, recent allocation history and allocates a resource to the UE

 UE performs data rate selection for uplink transmission.

 UE forms a data packet for transmission and transmit them on

PUSCH.UE also transmits control information on PUCCH.

 Then eNodeB sends either an ACK or NACK for the data.

|  |  |
| --- | --- |
|  | There are also certain additional operations that happens in LTE. We |
|  | would discuss three major ones here. The Idle Mode operation, in which |
|  | UE goes idling when no traﬀic is there to conserve power. Paging Mode, |
|  | in which an idle UE reestablishes its connections when a call comes |
|  | through. And finally Handover mode, in which a UE connects to a |
|  | diﬀerent eNodeB while travelling or when signal improves from diﬀerent |
|  | towers. |
|  |  |
| 11 of 17 |  |

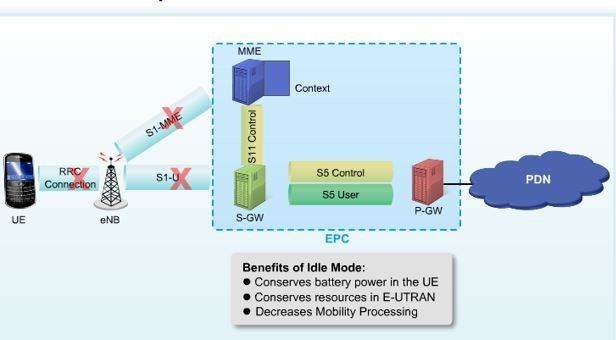
LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

**Idle Mode**

When the eNB detects that a UE has had no traﬀic for an operator defined period of time, usually referred to as an inactivity timer, the eNB can initiate procedures to place the UE in idle mode. In LTE, the UE is RRC\_Idle and from an EPS Mobility Management (EMM) perspective it is EMM-Registered and EMM-Idle. In this state, the UE no longer has any connectivity to the EPC, and all context relating to the UE is removed from the E-UTRAN.

There are several reasons for wanting to take advantage of idle capabilities defined for LTE. These include conserving UE battery, conserving eUTRAN resources, and decreasing processing related to mobility. For example, if an eNB manufacturer defines a maximum number of active users or RRC\_connected UEs in a cell, then leaving a UE connected when it isn’t transferring data could cause the blocking of new users who need to use the cell for access or handover.

When idle, the MME will maintain the context for the UE and continue to manage the UE. The bearers, at least all default bearers, which were established for the UE will also be maintained in the EPC.



Entering Idle mode is triggered by data inactivity. If no traﬀic is flowing for the UE, the eNB can initiate procedures to remove the RRC connection and to change the state to RRC\_Idle.

Rohan:

Trigger => No Activity

Once inactivity is detected, the eNB will send an **S1 UE Context** **Release Request** message to the MME. MME acting upon this requestwill send a **Release Access Bearers Request** message to the S-GW so that the S1-U bearers associated with the UE’s EPS bearers are released.

Rohan

Action => S1-U closed

The MME now tells the eNB to release its corresponding S1-U context with the **UE Context Release Command**. Over the LTE air interface, the eNB sends an **RRC Connection Release message** to the UE to tear down all traﬀic and signaling bearers on the air interface and the UE’s context in the eNB is removed.

Rohan

Action => radio bearer released

Action=> Ran context removed

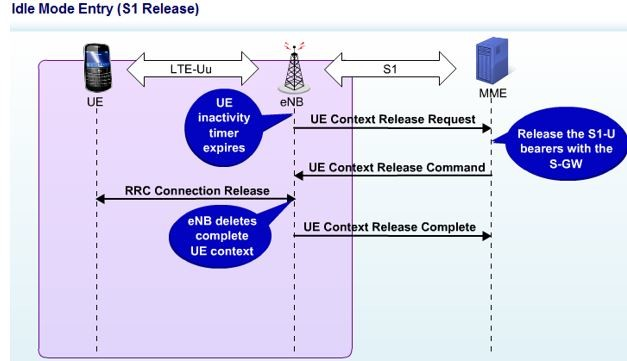
Finally, the eNB will let the MME know that the context has been released. At this point, the S1-AP signaling connection between the MME and the eNB for the UE is released.

Rohan: UE Context Release Complete

Rohan:

Action=>S1-MME Released

While idle, the MME will retain the UE's context, including the S-GW's S1-U configuration information.



In addition to cell reselection and TAU (Tracking Area Updates), the UE is required to periodically monitor the downlink of the selected cell for page messages.

Typically, page messages are initiated by the MME to locate an idle user when there is downstream traﬀic being buﬀered at the S-GW. To monitor for page messages, the UE must downlink synchronize and read SIBs in order to read downlink communications from the cell.

Rohan:

down sync -> read SIB -> get which channel?

Finally, the UE may need to exit idle mode, typically when there is new downstream traﬀic or new data in the UE’s buﬀers. The UE will uplink synchronize and establish an RRC connection. Then using NAS signaling with the MME, it will be able to reactivate current bearers.

Rohan:

up sync -> get which channel? -> RRC conn -> NAS signal

**Paging Operations**

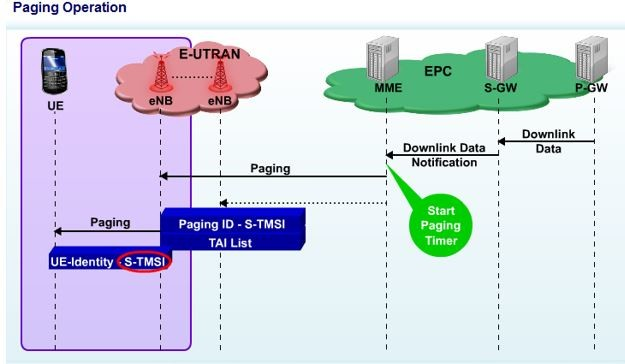
As mentioned earlier, if downlink data is received for a UE that is idle, the S-GW will buﬀer the data and request the MME to reestablish bearer connections with the UE. When the MME receives this downlink data notification from the S-GW, it will initiate paging of the cells in the tracking area to determine which cell the UE is in and as an indicator for the UE to reestablish connectivity. The eNBs in the tracking area will send paging . The UE’s S-TMSI will be included in the paging message so the UE will know if the page message is for it.

Rohan:

TMSI is part of GUTI shared with UE on completion of Registration. Reg Accept Msg mein GUTI value, UE ko milta h

Rohan:

What is UE’s listening interval, which specific channel are we talking abt??

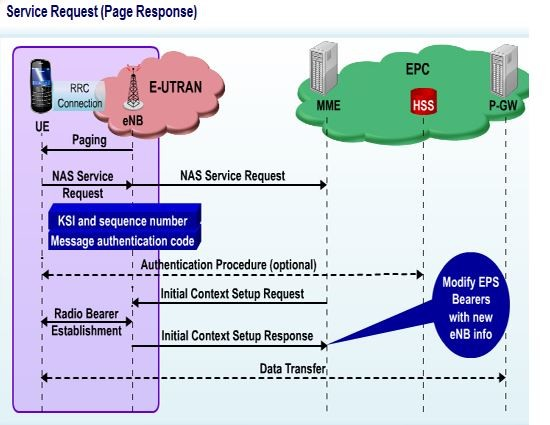
The MME will stop its timer for the paging procedure when a response is received from the UE; otherwise it will retransmit the page when the timer expires up to an operator configurable number of tries.

Rohan: How does MME knows S-TMSI and TAI List??? => MME and S-GW UE Context are still maintained. So on receiving data for idle UE MME looks up for associated idle UE’s S-TMSI and TAI List

When a UE receives a page message, it will uplink synchronize, establish an RRC connection, and send a NAS Service Request message to the MME. With this message the UE indicates that it is responding to a page and sends the necessary parameters, **Key Set Identifier** (KSI) and **NAS sequence number count**, to reestablish its security context. The **Message Authentication Code** (MAC) is used by the MME to make sure the sender is a valid UE.

The MME can optionally re-authenticate the UE at this time, or continue

with bearer setup. Once the bearers are reestablished, the LTE network

can begin sending the downlink data that has been buﬀered in the S-GW.

**Handover**

After an RRC connection is established, the serving eNB sends **RRC** **Connection Reconfiguration** messages to the UE informing it of thetypes of measurements to take and the types of events the eNB would like reported. This is commonly referred to as the measurement criteria. It is important to note that it is up to the eNB manufacturer to determine when to send the measurement criteria to the UE. In many cases it will be sent after authentication.

The UE then monitors the neighboring cells as it moves through the network. When any of the specified reporting criteria is met, the UE sends the results to the network in a **Measurement Report message**. If the Measurement Report indicates that a neighboring cell has met the handover criteria, the serving eNB can decide to initiate handover of the UE to the neighbor cell.

The measurement report includes the type of measurement, the identities of the neighbor cells meeting the criteria, and the measurement results. The eNB, based upon information received in the Measurement Report message will decide whether a handover is required.

In LTE the handover procedure goes through three distinct steps:-

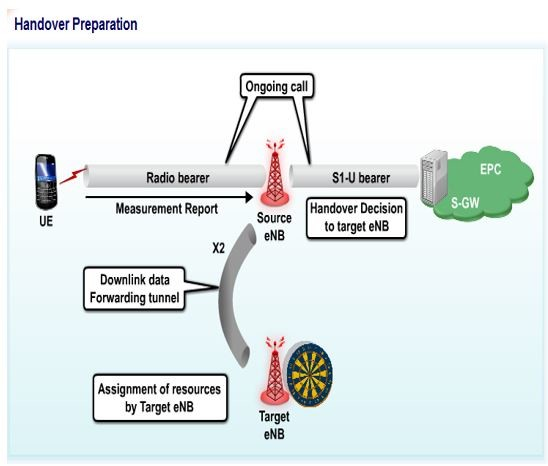
1.) **Handover preparation**: Using the X2 interface, the source eNB will collaborate with the target to determine if the target can accept the data sessions for the UE, and to establish a data forwarding tunnel for downlink data. The target will assign resources, like a new C-RNTI and a dedicated Preamble for uplink synchronization for the UE and report those resources back to the source.



**Messaging**

14 of 17 11/05/20, 12:50 am

LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

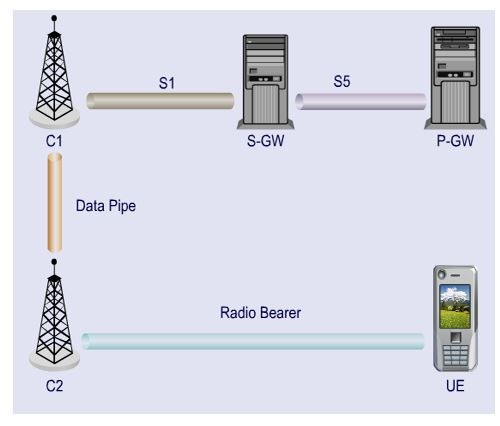


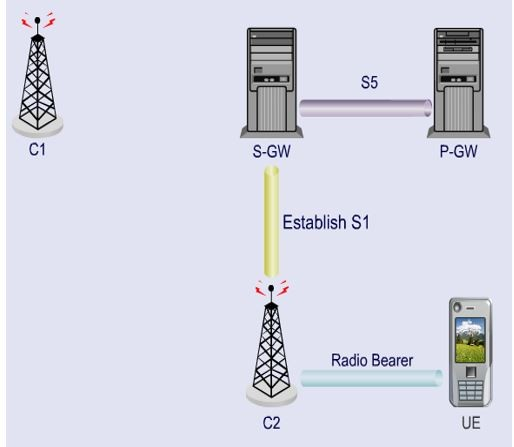
2.) **Handover execution**: The source eNB begins to forward any downlink packets to the target over the X2 data forwarding tunnel and tells the UE about the resources assigned by the target in an RRC Connection Reconfiguration message. Once the UE receives this message, it is no longer communicating with the serving cell, and will establish an RRC connection radio bearer with the target eNB. The UE performs a handover and now establishes an RRC connection with the target eNB. This establishes a radio bearer between the target eNB and the UE.

Rohan:

In this step, downlink traffic to target and UE informed about target for uplink traffic

As shown in diagram we have radio bearer with target eNB, but S1-U is still between old eNB and S-GW



3.) **Handover Completion**: The target eNB, working through the MME, establishes an S1-U bearer with the S-GW and maps it to the radio bearer. New packets arriving at the S-GW are now sent directly to the target eNB. At this point the old radio bearer and access bearer are released, and the data forwarding tunnel between the source and the target is removed, and any resources associated with the UE on the source eNB are de-allocated. CLEAN UP

**Conclusion:**

So this concludes the LTE for Layman series! Hope readers got the complete picture of everything related to LTE. We began with understanding the basic architecture, then moved on to understand the radio concepts and protocols layers. We concluded by understanding complete steps and message exchanges for establishing an end to end LTE connection. We also traversed through concepts such as Handover, Paging and Idle mode activities. Do give your feedback on improvement or suggestions for future topics!

So what will happen if you switch on your LTE enabled cell phone to like or share this article? 8 Simple steps for basic LTE connection

* Your UE will first scan the frequency bands supported to capture signals.
* It will then downlink synchronize by latching on the synchronization signals.
* Then, it will decode broadcast information to decode critical channel information.
* Using that, it will select the operator.
* Upon selecting the operator, UE will initiate RACH procedure to synchronize in uplink direction.
* Upon completion of uplink synchronization, UE will initiate ATTACH procedure with MME.
* Both AS and NAS security procedures are established, making every message integrity protected and encrypted.
* Finally, upon completion of security procedures, a default end to end bearer is created between UE and PDN. It’s using this bearer, that your command for “Like” would be finally transmitted and reflected back!

Add a comment…

**Surendra Singh** • 3rd+ 6mo 

NPO Engineer at Nokia

All the things are present in this notes.. Very nice. Never seen like you arranged step by step.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| · 1 Like |  | · 1 Reply | 6mo |  |
| **Aayush Shrut** • 2nd |  |  | | |
| Consultant at Deloitte |  |  | | |
| Thanks! |  |  |  | |
|  |  | 2y |  | |
|  |  |  |  |
| **Surbhi Agarwal** • 2nd |  |  | |
| Senior Engineer at Qualcomm |  |  | | |



Sir,

I have a doubt regarding the first process that is cell scanning.

How UE is able to measure RSRP ( through RS positions ) before doing cell synchronization process??

For RSRP measurement UE must know the RE(resource element) in which to search for the Reference signal corresponding to antenna port( in case of MIMO ), which is also according the PCI extracted from PSS…seeandmore



|  |  |  |  |
| --- | --- | --- | --- |
| · 2 Likes | · 2 Replies | 2y |  |
| **Aayush Shrut** • 2nd | |  |



Consultant at Deloitte



|  |  |  |  |
| --- | --- | --- | --- |
| Hi Surbhi, | **Messaging** |  |  |
|  |  |  |
|  | …see more |  |
|  |  |  |
|  |  |  |  |

16 of 17 11/05/20, 12:50 am

LTE for Layman (part 3) - The Complete Picture!... https://www.linkedin.com/pulse/lte-layman-part-...

RSRP (or narrowband RSSI) is simply a measurement of whatever energy/power it can measure. This measurement does not require any channel coding process. So at this step, UE does not need to know anything about the network. Its common process in any other radio device such as wifi



**Suraj Kumar** • 2nd 1mo 

Technology Manager (5G) at HARMAN International

Actually it is RSSI not RSRP

Whole energy will be measured without PCID calculations UEdoesnt have capability to understand CRS



**Messaging**

17 of 17 11/05/20, 12:50 am