Mobile communication overview 2/2

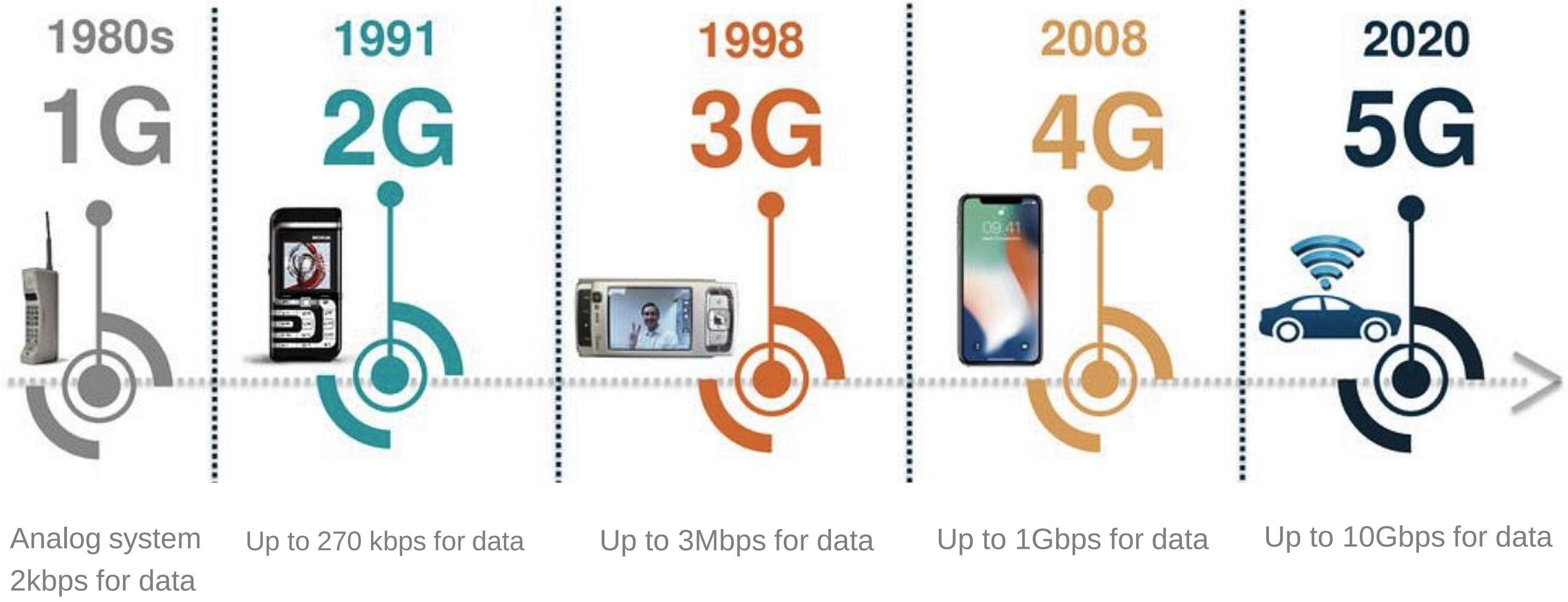
KIS FRI UNIZA

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

Mobile communication evolution to 5G (5th generation)

- 1G (NMT) – Analog system, poor voice quality & battery life, big phones, no security
- 2G (GSM) – Digital narrowband system, SMS, smaller phones, up to 270 kbps but often lower and bad quality
- 3G (UMTS) – Support both voice and video, data rates up to 3 Mbps
- 4G (LTE) – All IP transport, high data throughputs
- 5G (NR) – Cloud based and distributed architecture, network slicing (virtualization) used for various transport types and customer services, high data throughput

NMT	Nordic Mobile Telephone
GSM	Global System for Mobile
UMTS	Universal Mobile Telecommunication System
LTE	Long Term Evolution
NR	New Radio



https://slideplayer.com/slide/16305995/

3GPP
3rd Generation Partnership Project

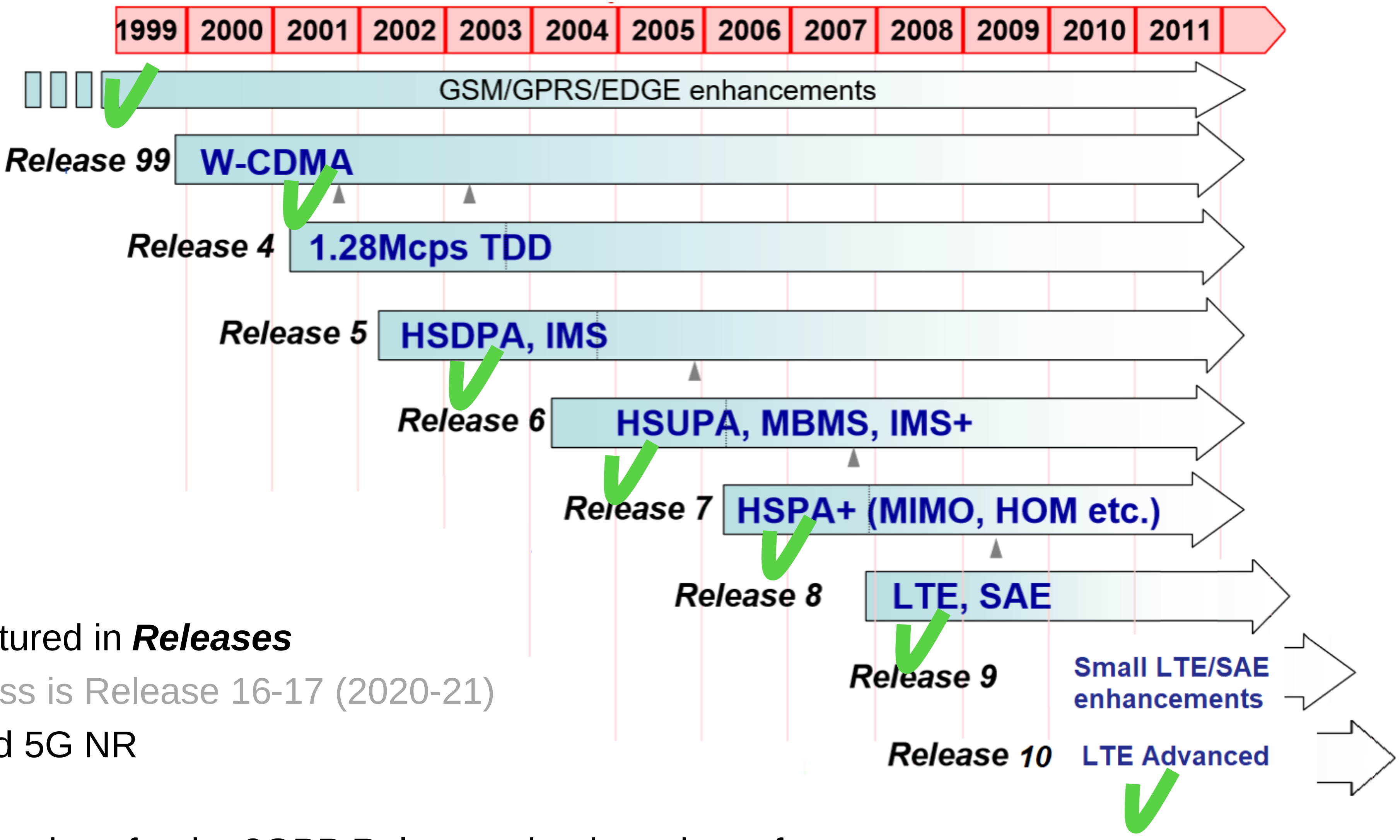
Understanding 3GPP

- 3GPP (3rd Generation Partnership Project) unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners”
- 3GPP was initially formed in December 1998 when the ETSI (European Telecommunications Standards Institute) partnered with other standard development organizations from around the world to develop new technologies for the third generation (3G) of cellular networks.
- 3GPP was heavily influenced at the start by existing 2G GSM standards
  - GSM is a standard developed by the ETSI to describe the protocols for second-generation (2G) digital cellular networks
- At the same time, another group in the United States formed the 3rd Generation Partnership Project 2 (3GPP2)
- The 3G technologies developed by 3GPP are called UMTS, whereas 3GPP2 technologies are called CDMA2000
- UMTS (Universal Mobile Telecommunications System) is a 3rd generation mobile cellular system for networks
- UMTS uses W-CDMA (Wideband Code Division Multiple Access) radio access technology
- HSPA (High Speed Packet Access) extends and improves the performance of initial 3G mobile telecommunication networks using the W-CDMA protocols

Understanding 3GPP

- In the mid-2000s, as it started to become clear that 3G networks would be overwhelmed by the need for faster Internet access, work begun on 4G standards. The requirements for 4G were not only faster peak data rates exceeding 100 Mbps, but it also required that 4G systems be built such that they are ideally suited for data-transmission, which equated to an all-IP packet-switched architecture.
- Three competing standards bodies worked on potential solutions for 4G at the same time
    1. **3GPP** standards organization worked on a system called **LTE** (Long Term Evolution)
    2. **3GPP2** started developing its own solution called the **UMB** (Ultra Mobile Broadband)
    3. **IEEE** started to develop a system called **WiMAX**
- In 2018, 3GPP published new standards, which includes what is described as "Phase 1" standardization for **5G NR** (New Radio)

Understanding 3GPP (UMTS, LTE and NR)



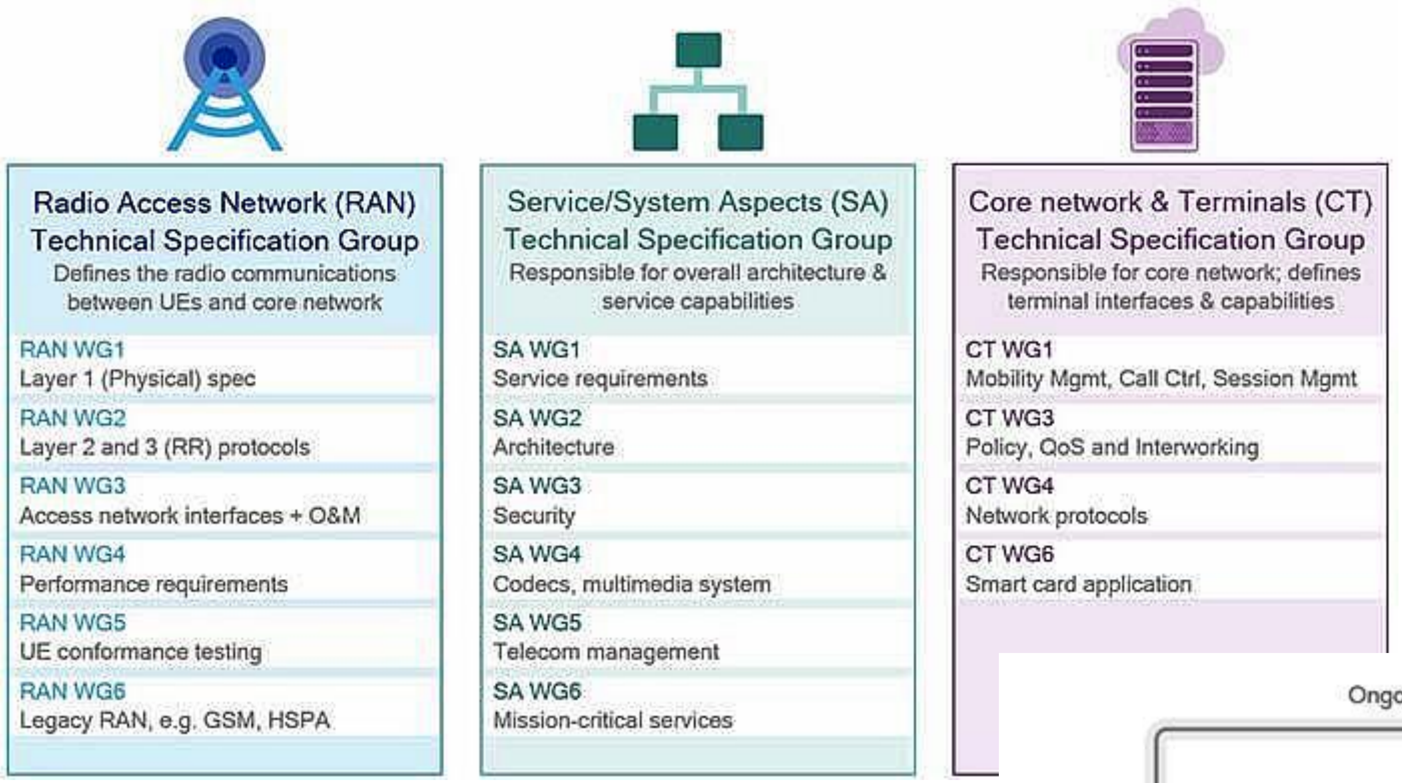
3GPP standards are structured in ***Releases***

Current Release in progress is Release 16-17 (2020-21)

Release 15 has introduced 5G NR

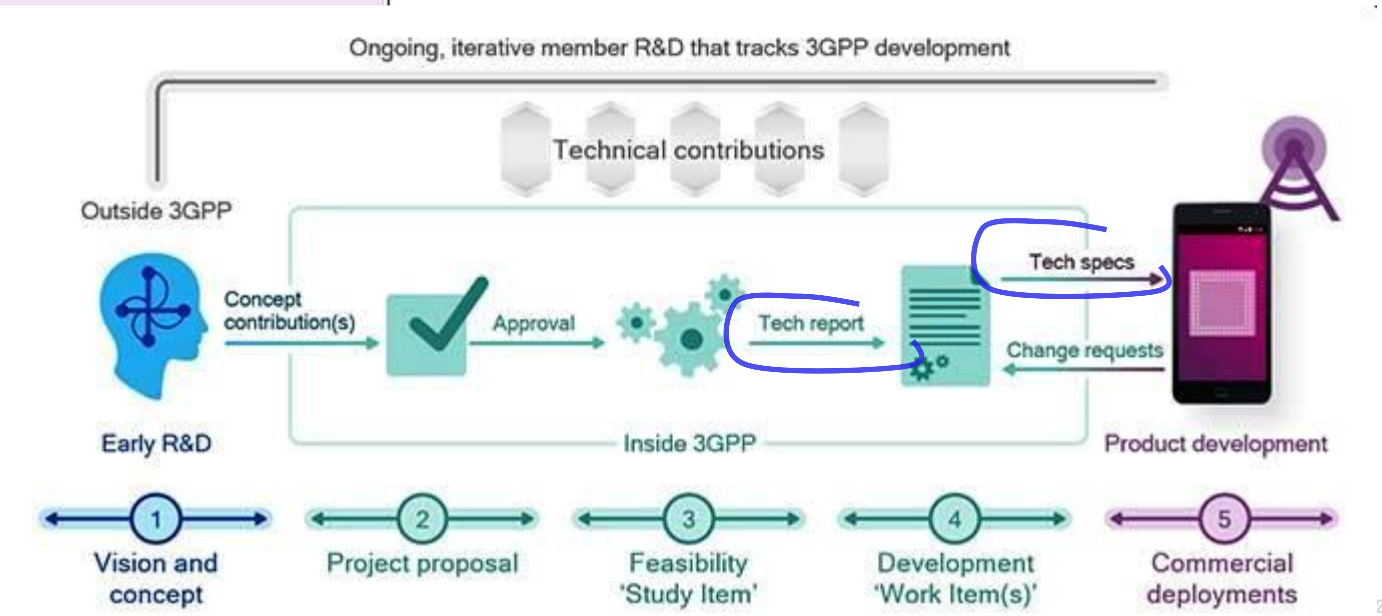
ETSI publishes the PDF versions for the 3GPP Releases that have been frozen

Understanding 3GPP



3GPP specification work is done in **Technical Specification Groups (TSGs)** and **Working Groups (WGs)**

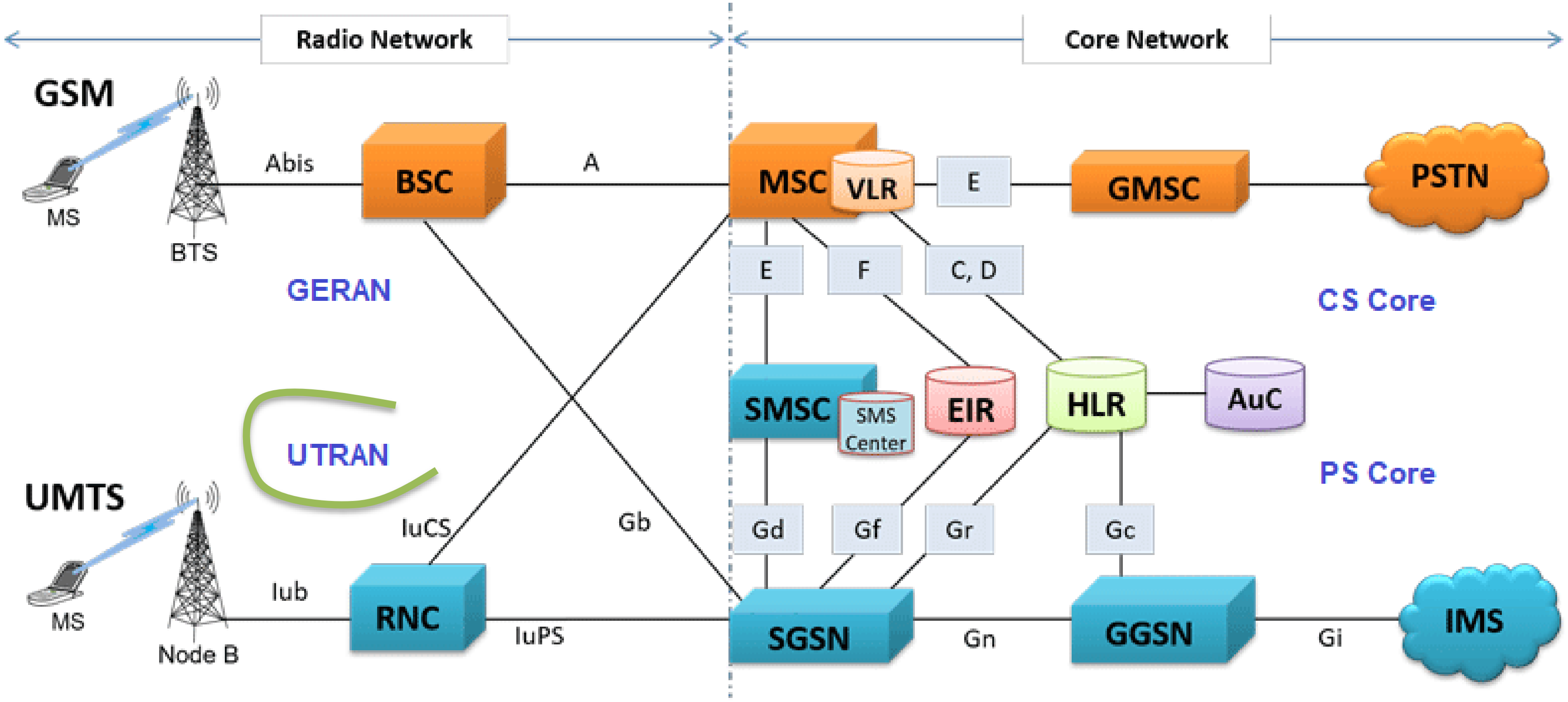
Technical Specification (TS) is an ultimate output of work completed in 3GPP
Over 1300 active 3GPP TSes



3G / UMTS
Universal Mobile Telecommunication System

3G UMTS

3G UMTS Architecture



GERAN - GSM/EDGE Radio Access Network
UTRAN - UMTS Terrestrial Radio Access Network
CS Core - Circuit Switched Core
PS Core - Packet Switched Core
RNC - Radio Network Controller
Node B - is an equivalent to the base transceiver station (BTS) in GSM

- Established during 2004 – 2005
- Higher bandwidth enables new applications (TV, Video, GPS, etc)
- High speeds up to 2Mbps
- More flexible as in principle can support CDMA, FDMA, TDMA access techniques

3G UMTS - Why W-CDMA? New bandwidth sharing technique

- **W-CDMA** - Wideband Code Division Multiple Access

- FDMA and TDMA are not efficient enough
  - TDMA wastes time resources
  - FDMA wastes frequency resource

- CDMA can exploit the whole bandwidth constantly, therefore selected for UMTS, different technologies
  - WCDMA typically deployed in Europe (3GPP)
  - CDMA2000 common in North America (3GPP2)

- UMTS W-CDMA uses 5 MHz (which also considers the guard bands on either sides)
  - Compared to narrowband CDMA (which uses a 200KHz-wide carrier), WCDMA system uses a 5MHz-wide carrier
  - The guard band in UMTS is 0.58 MHz or 580 KHz. Hence if we exclude the guard bands on both sides of the 5 MHz spectrum, we get an effective bandwidth of 3.84 MHz at least, which is used for transmission of the signals.

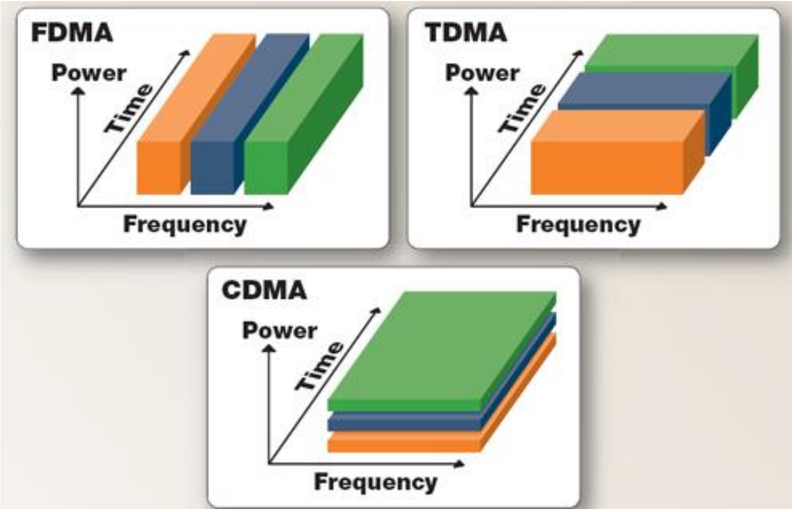
- R99/R4 defines QPSK modulation scheme (1 symbol = 2 bits)

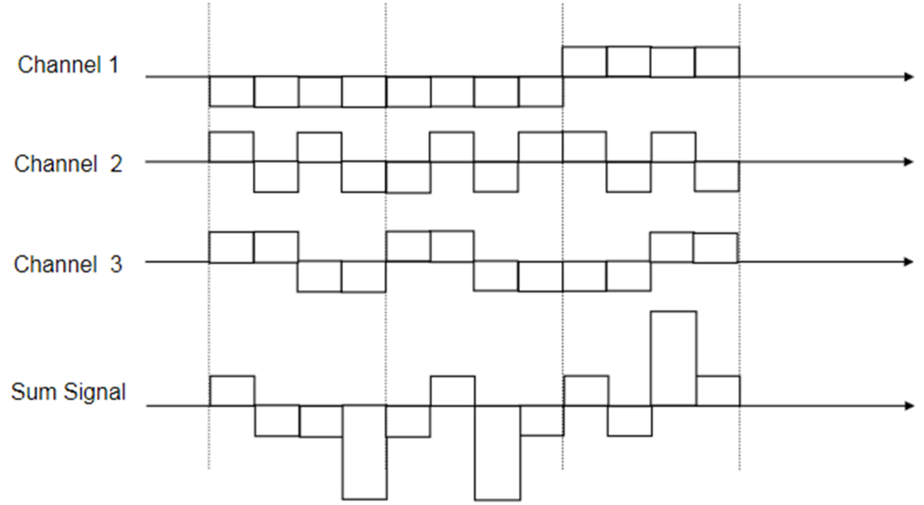
- Typical data rates of UMTS are:
  - 144 kbps for rural
  - 384 kbps for urban outdoor
  - 2048 kbps for indoor and low range outdoor

3G UMTS - CDMA principle

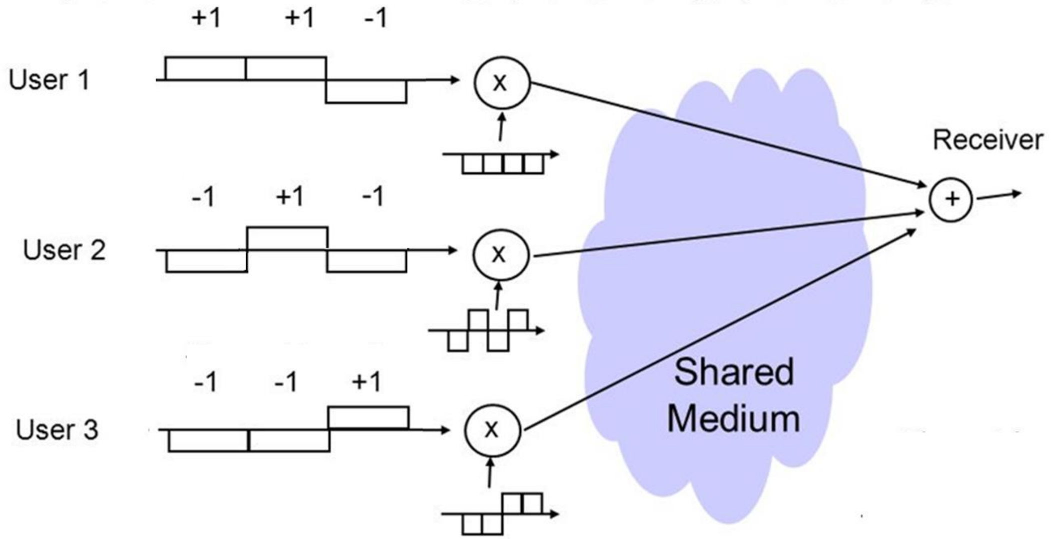
Channel 1: 110 -> +1+1-1 -> (-1,-1,-1,-1),(-1,-1,-1,-1),(+1,+1,+1,+1)
Channel 2: 010 -> -1+1-1 -> (+1,-1,+1,-1),(-1,+1,-1,+1),(+1,-1,+1,-1)
Channel 3: 001 -> -1-1+1 -> (+1,+1,-1,-1),(+1,+1,-1,-1),(-1,-1,+1,+1)
Sum Signal: (+1,-1,-1,-3),(-1,+1,-3,-1),(+1,-1,+3,+1)

Different (orthogonal) codes are used to separate different transmissions

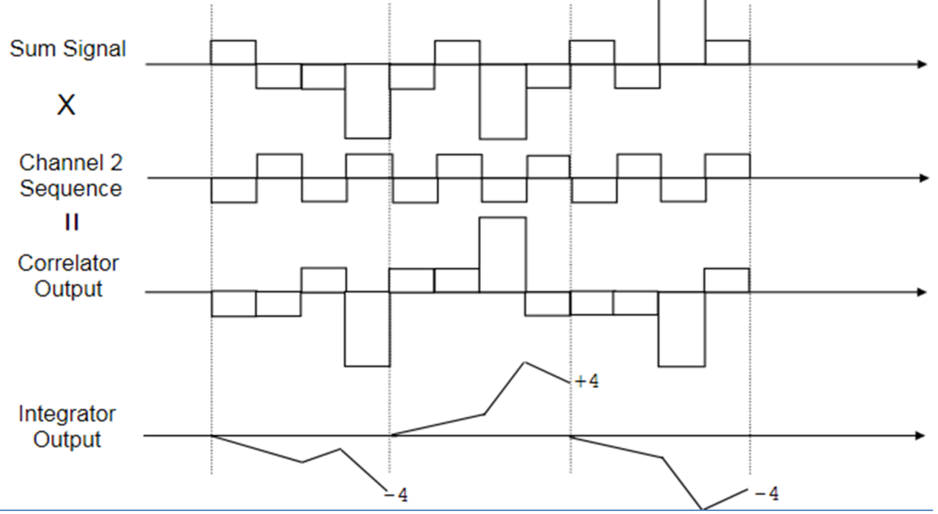




Users are synchronized & use different 4-bit orthogonal codes:
{-1,-1,-1,-1}, {-1, +1,-1,+1}, {-1,-1,+1,+1}, {-1,+1,+1,-1},



Sum Signal: (+1,-1,-1,-3),(-1,+1,-3,-1),(+1,-1,+3,+1)
Channel 2 Sequence: (-1,+1,-1,+1),(-1,+1,-1,+1),(-1,+1,-1,+1)
Correlator Output: (-1,-1,+1,-3),(+1,+1,+3,-1),(-1,-1,-3,+1)
Integrated Output: -4, +4, -4
Binary Output: 0, 1, 0

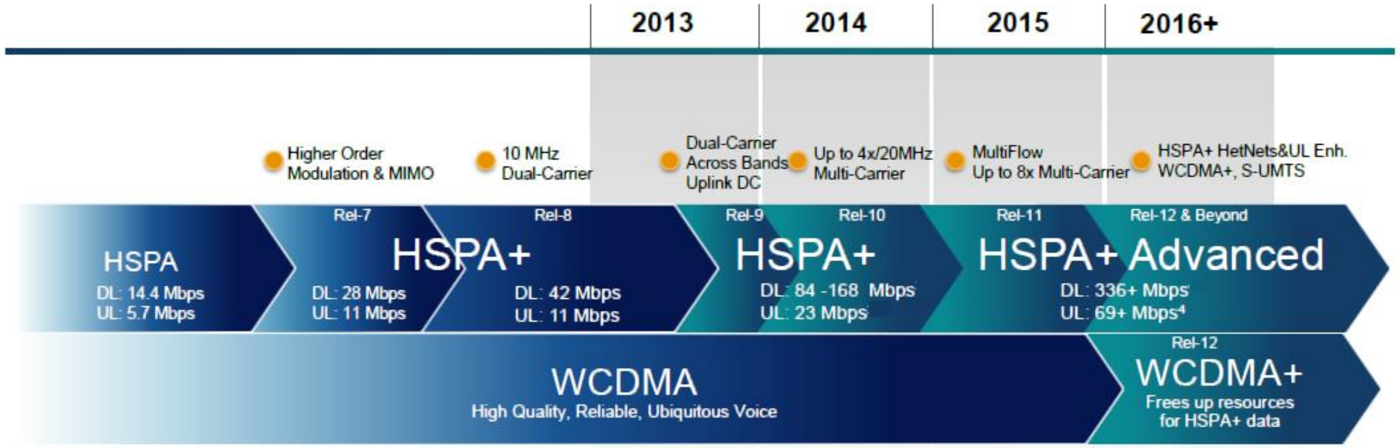


3G UMTS - HSPA

- **HSPA** (High Speed Packet Access) is an amalgamation of two mobile protocols, High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA)
- A further improved 3GPP standard, **HSPA+** (Evolved High Speed Packet Access)
  - released late in 2008 with subsequent worldwide adoption beginning in 2010.
  - the newer standard allows bit-rates to reach as high as 337 Mbit/s in the downlink and 34 Mbit/s in the uplink. However, these speeds are rarely achieved in practice.

- **MIMO** (Multiple-Input Multiple-Output) is a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time, multiple antennas are used at both sides. Operating at the same frequency, without requiring more spectrum. One transceiver is connected to a vertically-oriented part of the antenna and the other is connected to the horizontal (Vertical and horizontal polarization).
- What is the difference between **MIMO** and **Carrier Aggregation**?
  - MIMO combines signals and data streams from multiple antennas to improve signal quality and data rates, whereas **Carrier Aggregation** (CA) combines multiple frequency carriers (channels) to enhance the bandwidth and data rates.

# of codes	Modulation	Max data rate
5 codes	QPSK	1.8 Mbps
5 codes	16-QAM	3.6 Mbps
10 codes	16-QAM	7.2 Mbps
15 codes	16-QAM	10.1 Mbps
15 codes	16-QAM	14.4 Mbps



4G / LTE
Long Term Evolution

4G LTE

4G / LTE - summary

- Provides lower latency for subscriber's data
- Higher overall network throughput and increased data speeds for subscriber
  - ~ up to 100Mbps downlink (300Mbps downlink in 20Mhz x 4 MIMO x 64QAM), ~ 10msec latency
- Cost effectiveness
- New modulation types
  - OFDMA (Orthogonal Frequency Division Multiplexing Access) for downlink
  - SC-FDMA (Single Carrier Frequency Division Multiple Access) for uplink

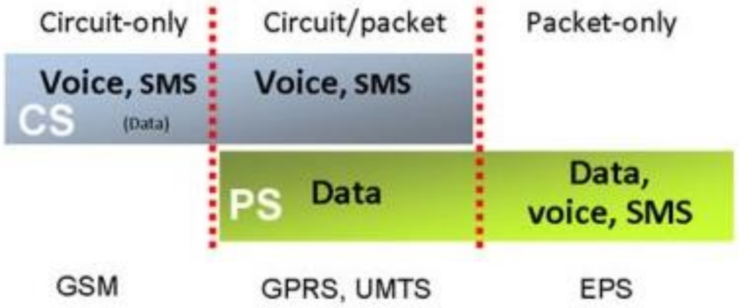
- The technology was standardized within the 3GPP as part of the 3GPP Release 8 (2008/2009)
- Mass deployment to begin around 2012
- Co-existence with older wireless technologies, call can be started in LTE and transferred into GSM, UMTS

- MIMO
- All IP architecture
- Spectrum flexibility 1.25MHz to 20 MHz
- TDD/FDD

- LTE Advanced, 3GPP Release 10
  - Improves capacity and coverage and provides large bandwidth up to 100Mhz of spectrum
  - Peak data rates up to 1Gbps

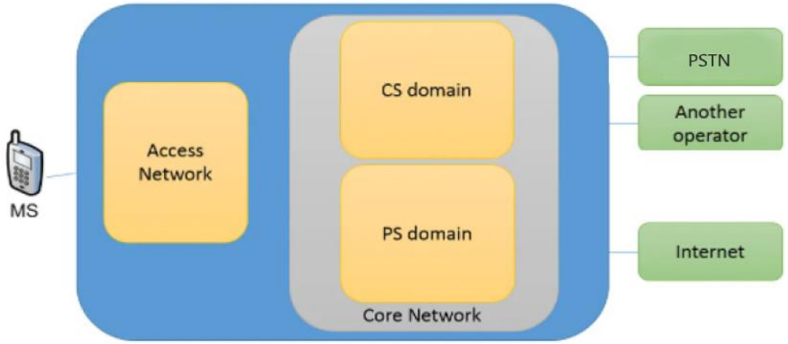
4G / LTE - architecture

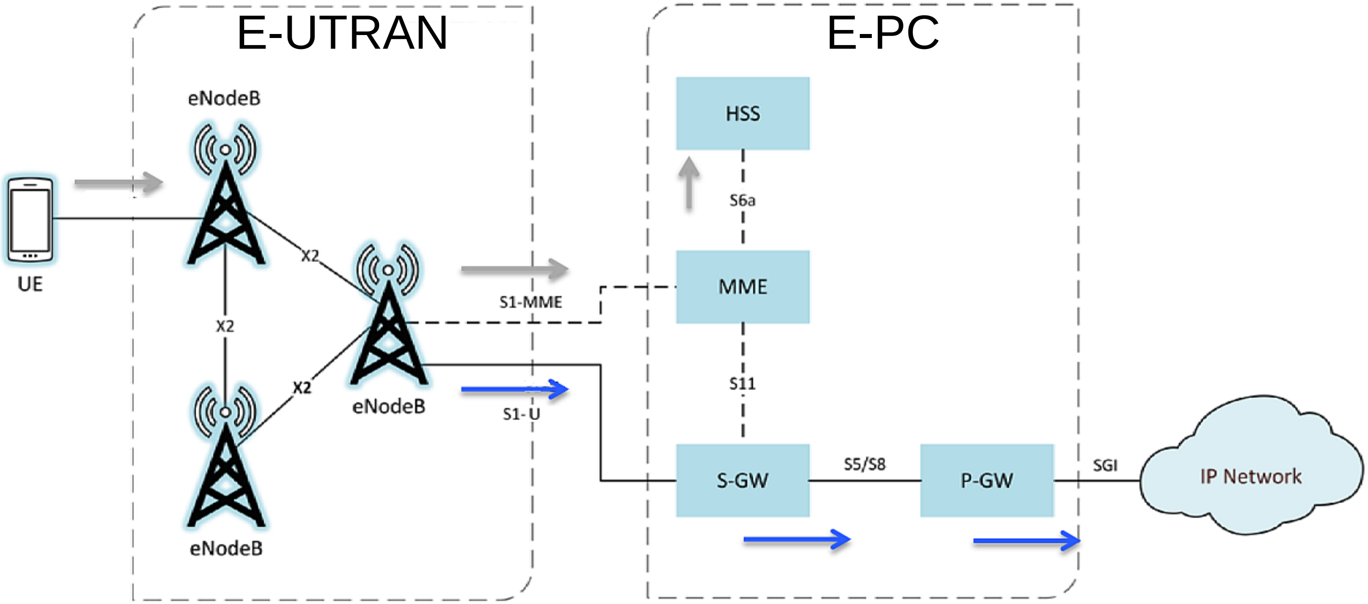
- Generally, mobile network consists of 2 parts:
  1. Radio access network (*GERAN in 2G, UTRAN in 3G, E-UTRAN in LTE*)
  2. Core network
     a. CS domain (Circuit Switched) – handles voice service
        - *MSC, HLR, VLR, etc.*
     b. PS domain (Packet Switched) – handles data
        - *SGSN & GGSN in 2G/3G; S/P-GW & HSS & MME & other in LTE*



- LTE network doesn't contain a CS domain. Even the voice calls are using PS domain
- EPS (Evolved Packet System) is composed of E-UTRAN and EPC which are commonly known as LTE and SAE (System Architecture Evolution) respectively

- E-UTRAN – Evolved UTRAN
- E-PC - Evolved Packet Core





4G / LTE – components and interfaces

- In mobile networks, every interface between two nodes, is having an interface name, that represents the protocol used in the communication between those nodes

eNodeB - Evolved Node B

MME - Mobility Management Entity

SGW – Serving Gateway

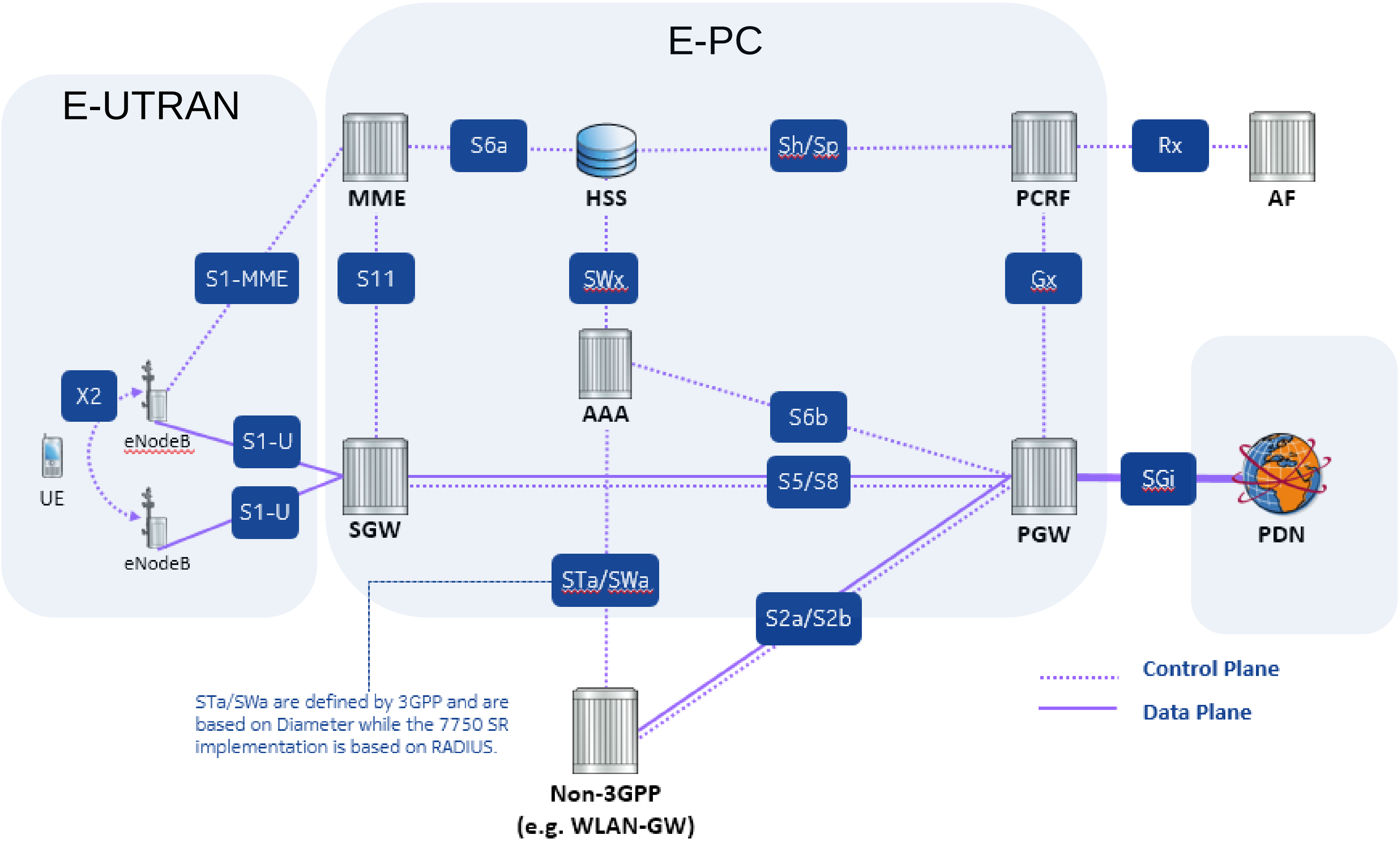
PGW – Packet Gateway

HSS – Home Susbscriber Server

PCRF – Policy and Charging Rules Function

AF – Application Function

AAA - Authentication, Authorization and Accounting

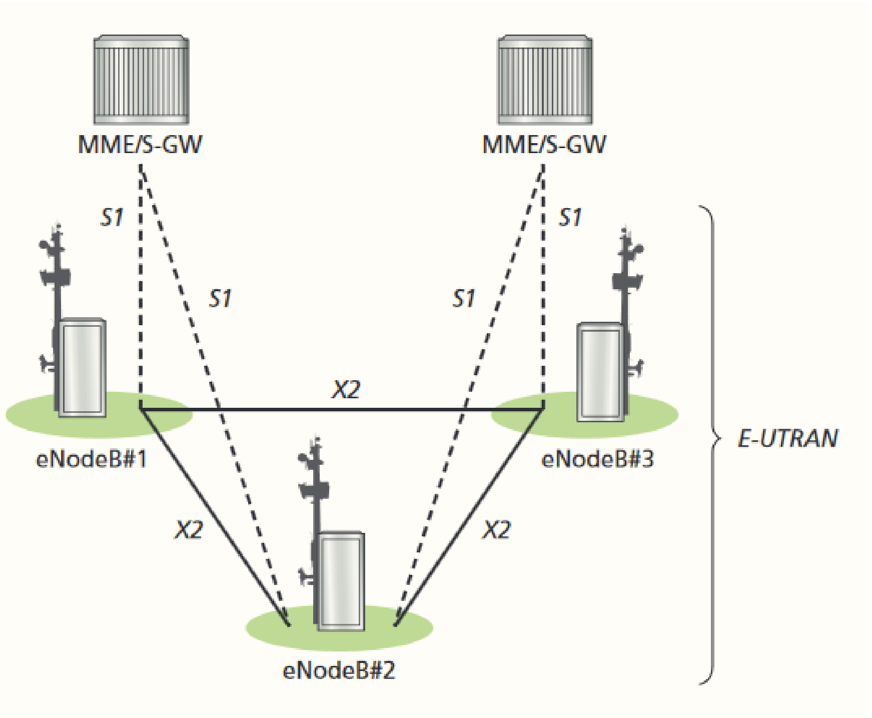


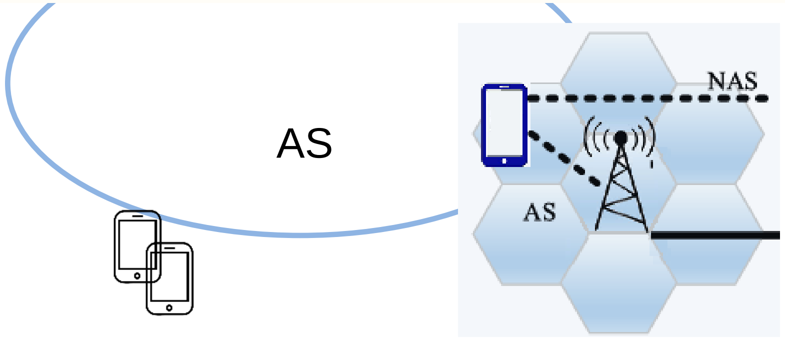
S6b interface between PGW->AAA, make sense when UE moves to non 3GPP networks like Wifi (over S2a/S2b)

E-UTRAN

- eNodeBs (base stations) are normally interconnected with each other by means of a logical interface known as X2 and to the E-PC by means of the logical S1 interface
  - more specifically, to the MME by means of the S1-MME interface and to the S-GW by means of the S1-U interface

- E-UTRAN domain is responsible for all radio-related functions
  - RRM - Radio resource management – This covers all functions related to the radio bearers, such as radio bearer control, radio admission control, radio mobility control, scheduling and dynamic allocation of resources to UEs in both uplink and downlink.
  - Header Compression – This helps to ensure efficient use of the radio interface by compressing the IP packet headers that could otherwise represent a significant overhead, especially for small packets such as VoIP
  - Security – All data sent over the radio interface is encrypted
  - Connectivity to the EPC – This consists of the signaling toward MME and the bearer path toward the S-GW.



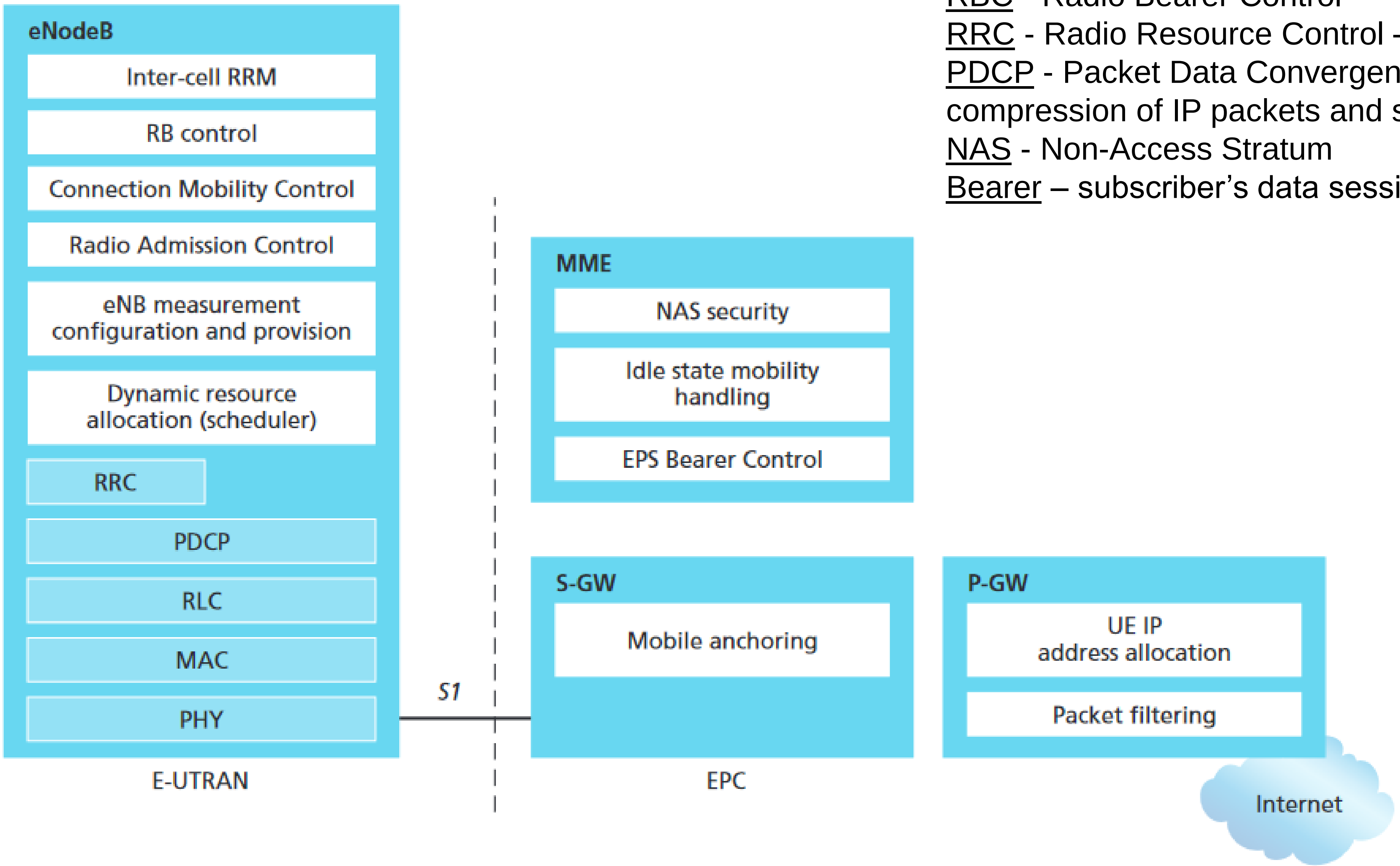


The protocols that run between the eNodeBs and the UE are known as the AS (Access Stratum) protocols.

E-PC

- S-GW - Serving Gateway - All user IP packets are transferred through the S-GW, which serves as the local mobility anchor for inter-eNodeB handover for the data bearers - when the UE moves between eNodeBs. It also retains the information about the bearers when the UE is in the idle state (known as EPS Connection Management) and temporarily buffers downlink data while the MME initiates paging of the UE to reestablish the bearers. Provides mobility between LTE and other types of networks, such as between 2G/3G and P-GW
- P-GW - PDN Gateway - Responsible for IP address allocation for the UE, as well as QoS enforcement and flow-based charging according to rules from the PCRF. It is responsible for the filtering of downlink user IP packets into the different QoS-based bearers
- PCRF - Policy Control and Charging Rules Function - Responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the PCEF (Policy Control Enforcement Function). The PCRF provides the QoS authorization (QoS class identifier [QCI] and bit rates), coops with charging function
- MME - Mobility Management Entity is the control node that processes the signaling between CN (Core network) and UE. The protocols running between the UE and the Core network (MME) are known as the NAS (Non-Access Stratum) protocols
- HSS - Home Subscriber Server contains users' SAE subscription data such as the EPS-subscribed QoS profile and any access restrictions for roaming. It also holds information about the PDNs to which the user can connect. This could be in the form of an APN (Access Point Name). In addition, the HSS holds dynamic information such as the identity of the MME to which the user is currently attached or registered.

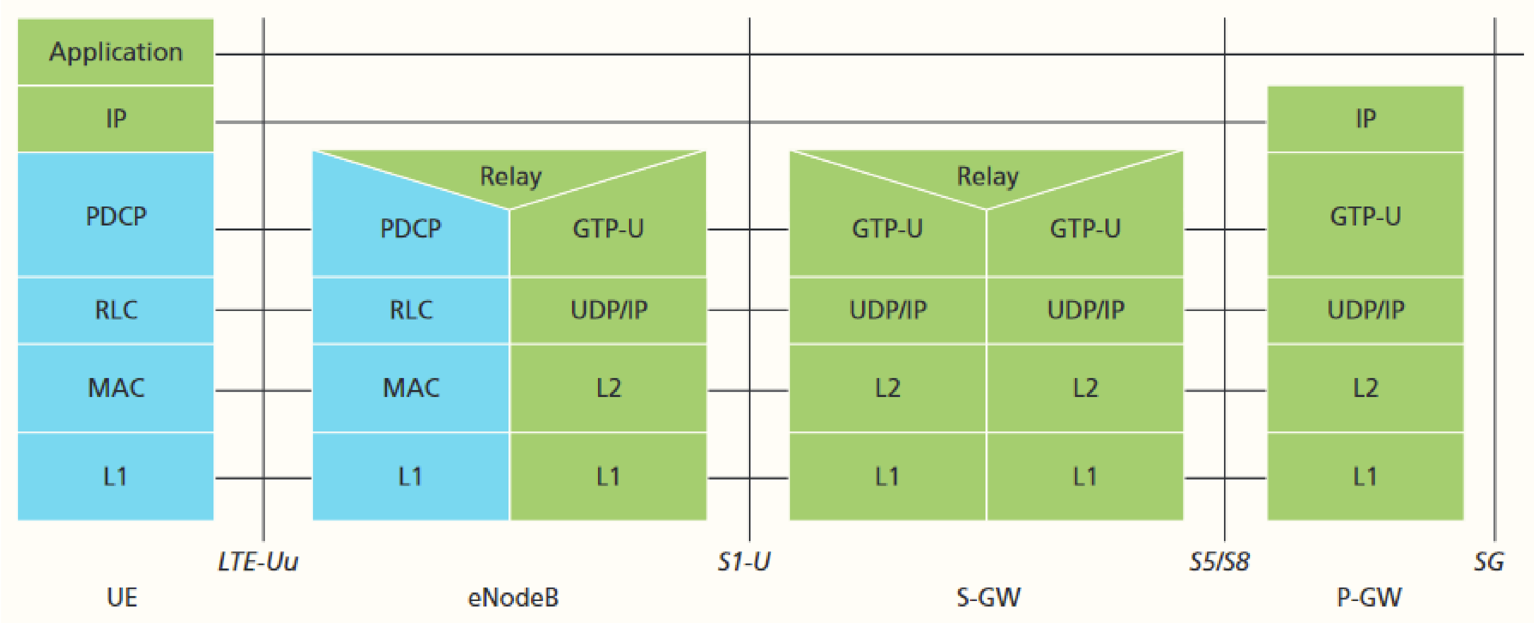
4G / LTE – Functional split



RRM - Radio resource management
RBC - Radio Bearer Control
RRC - Radio Resource Control – radio control functions
PDCP - Packet Data Convergence Protocol - header compression of IP packets and security functions
NAS - Non-Access Stratum
Bearer – subscriber's data session

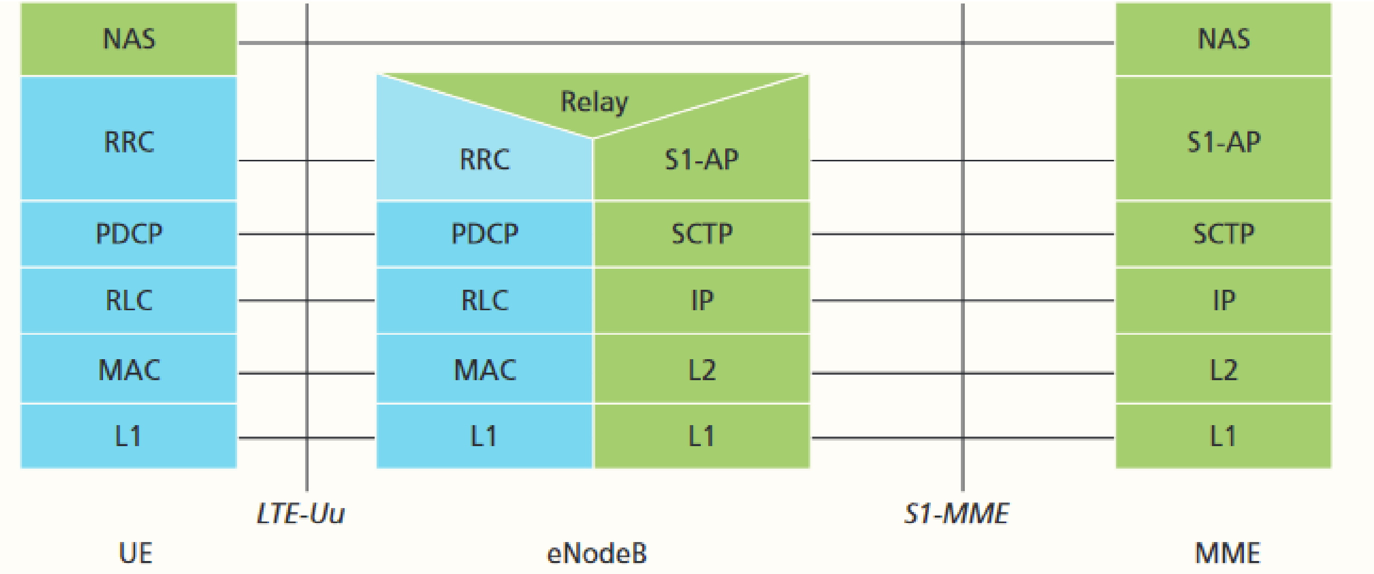
User plane

- IP packets for UE are encapsulated within EPC via 3GPP-specific tunneling protocol called GTP (GPRS Tunneling Protocol) is used over the CN interfaces, S1 and S5/S8 (in green)
- An EPS bearer is equivalent to a PDP Context (3G UMTS terminology). Is a logical (GTP) transport tunnel between the UE and the PGW, used for exchanging data When EPS bearer is established, a bearer context is created in all the nodes that handle the user data.
  - Two types – default and dedicated bearer
- The E-UTRAN user plane protocol stack is shown (in blue) consisting of the PDCP (Packet Data Convergence Protocol), RLC (Radio Link Control and MAC (Medium Access Control) sublayers that are terminated in the eNodeB on the network side.



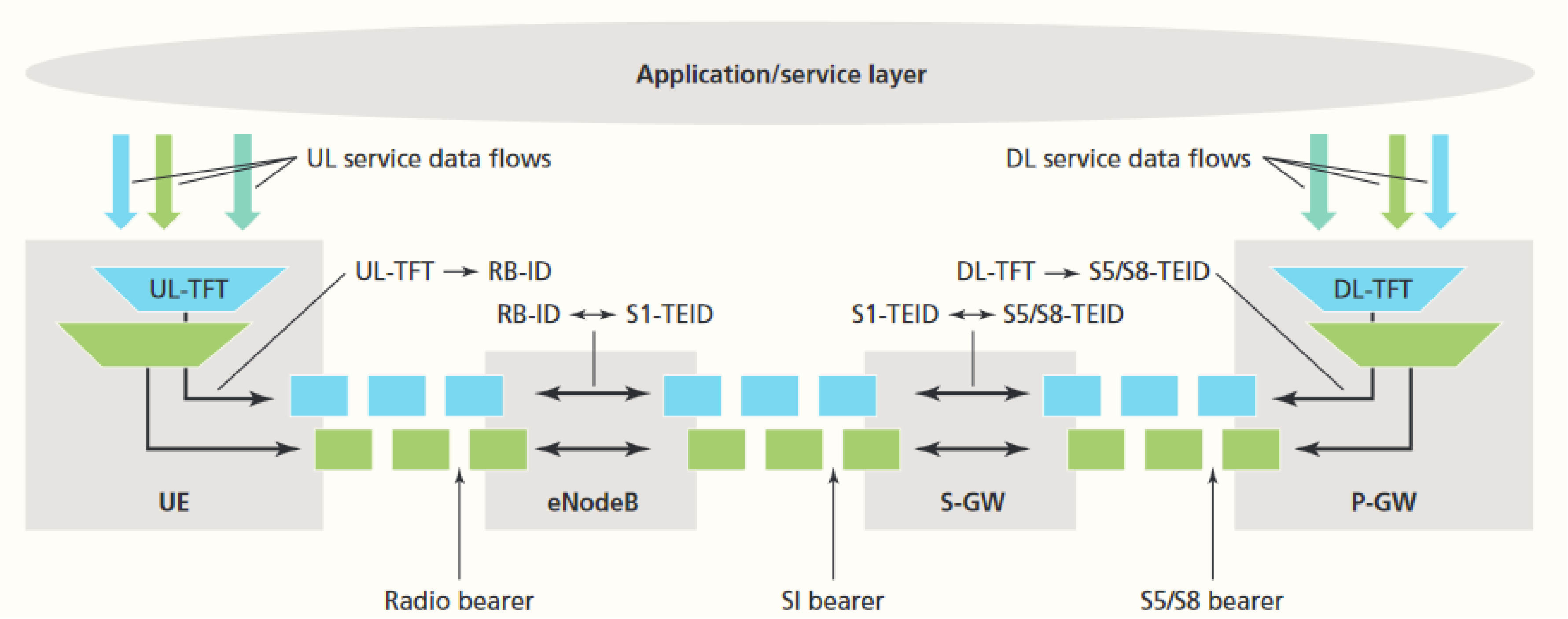
Control plane

- The blue region of the stack indicates the AS protocols. The lower layers perform the same functions as for the user plane with the exception that there is no header compression function for the control plane.
- RRC (Radio Resource Control) protocol is known as “layer 3” in the AS protocol stack. It is the main controlling function in the AS, being responsible for establishing the radio bearers
- RLC (Radio Link Control) is responsible for transfer of upper layer PDUs, error correction through ARQ (Automatic Repeat Request), segmentation and reassembly, duplicate detection
- MAC (Media Access Layer) layer is responsible for mapping between logical channels and transport channels
- Physical layer carries all information from the MAC transport channels over the air interface. Takes care of the link adaptation (AMC), power control, cell search



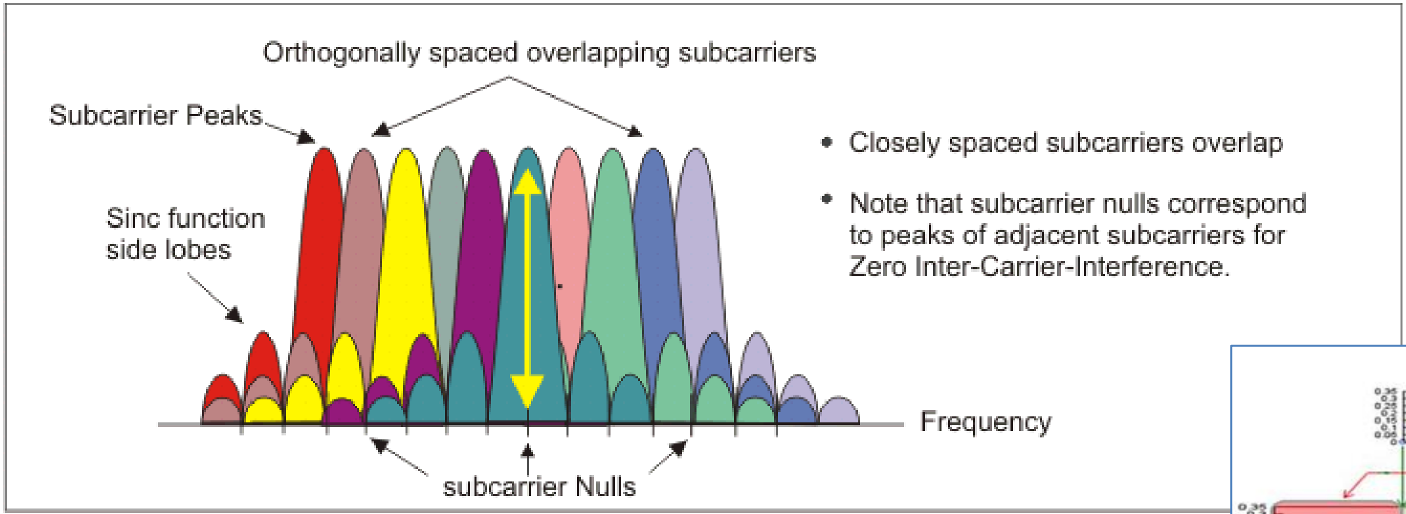
EPS bearer across different interfaces

- The EPS bearer is identified by the GTP tunnel ID across both interfaces, TEID (Tunnel Endpoint ID)
- TFT (Traffic Flow Template) - Packet filtering into different bearers (which can share the same IP address and APN) is based on TFT, based on IP, UDP/TCP port, UL (uplink), DL (downlink)
- Default bearer is established and “remains throughout the lifetime” of the PDN connection in order to provide the UE with always-on IP connectivity to the PDN (typically internet). The initial bearer-level QoS parameter values of the default bearer are assigned by the MME, based on subscription data retrieved from the HSS. The PCEF may change these values in interaction with the PCRF or according to local configuration. Another bearer type – dedicated bearer - used for VoIP traffic, for instance.

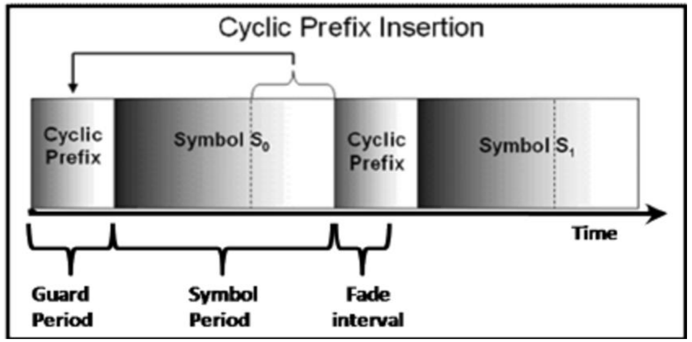


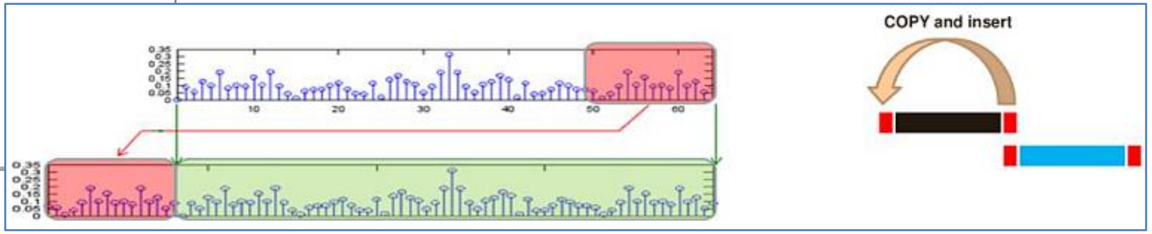
Radio physical interface – OFDMA & SC-FDMA modulation

- OFDM (Orthogonal Frequency Division Multiplexing) forms the basic signal format used within 4G LTE. OFDM is the basic format used and this is modified to provide the multiple access scheme: OFDMA in downlink direction
- SC-FDMA (Single Carrier Frequency Division Multiple Access) modulation scheme used in uplink direction - the benefit of a single carrier multiplexing of having a lower Peak-to-average Power Ratio
- Form of transmission that uses a large number of close spaced carriers that are modulated with low rate data. Normally these signals would be expected to interfere with each other, but by making the signals orthogonal to each other there is no mutual interference
- CP (Cyclic Prefix) refers to the prefixing of a symbol, with a repetition at the end of the symbol. It provides a guard interval to eliminate inter-symbol interference from the previous symbol.



OFDM Signal Frequency Spectra





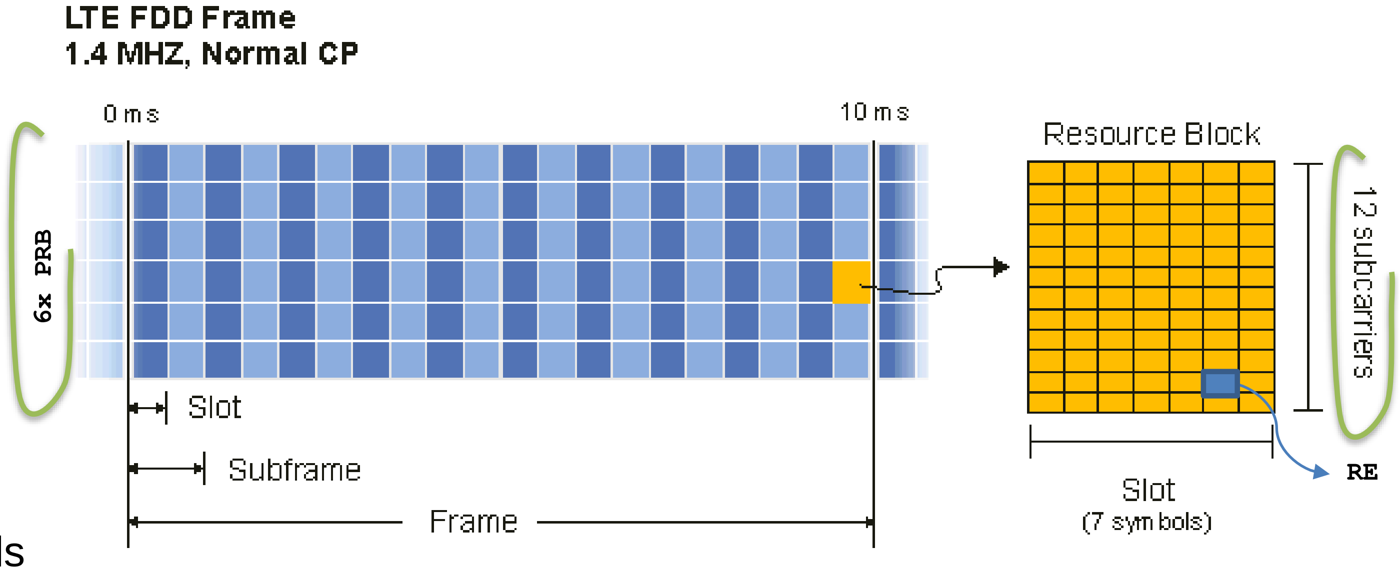
LTE frame structure

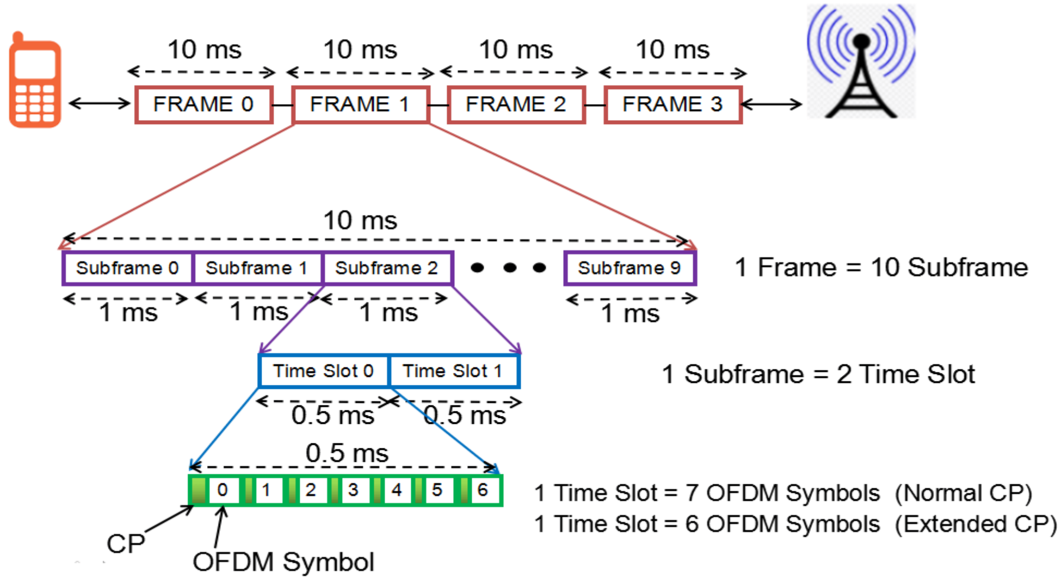
- OFDM symbol: 2048 samples + CP
- Timeslot: 0.5 msec, 6 or 7 OFDM symbols
- Sub-frame: 1 msec, 2 timeslots
- LTE radio frame: 10 msec, 10 sub-frames
- Subcarrier bandwidth: 15 kHz

- RE (Resource Element): a smallest unit in OFDMA system, used to carry user data, signals and control data, 1 subcarrier x 1 symbol
- RB or PRB (Physical Resource Block): the smallest unit of resources allocated to a user: 12*15kHz = 180kHz wide and 7 symbols length

- The bandwidths available defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz

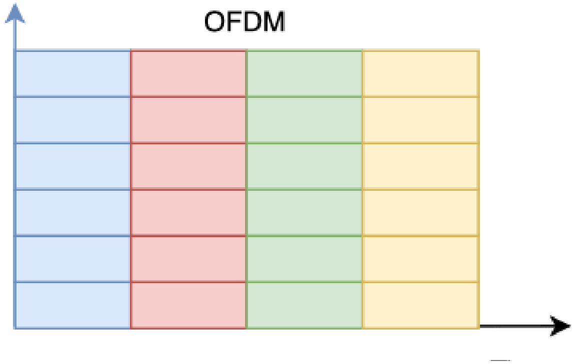
Bandwidth	Resource Blocks	Subcarriers (downlink)	Subcarriers (uplink)
1.4 MHz	6	73	72
3 MHz	15	181	180
5 MHz	25	301	300
10 MHz	50	601	600
15 MHz	75	901	900
20 MHz	100	1201	1200

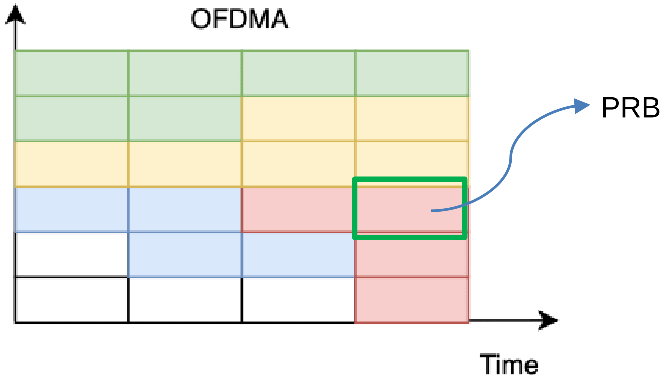


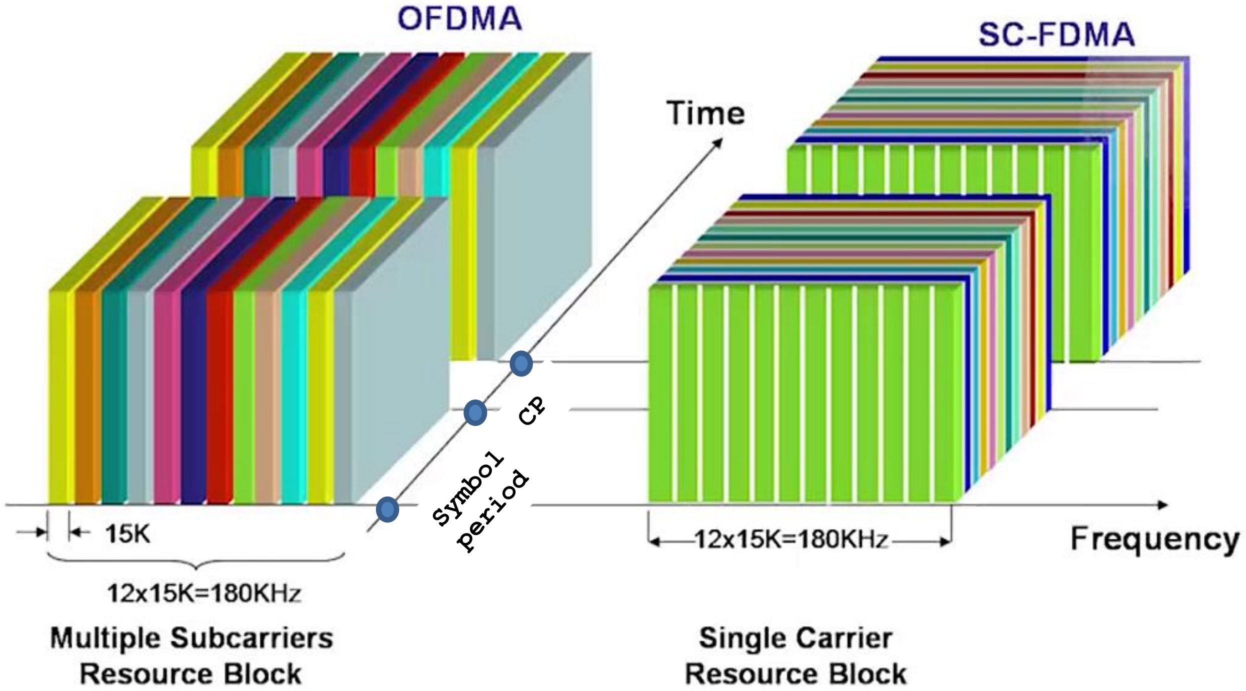


OFDM, OFDMA & SC-FDMA modulation

A. OFDM allocates users in time domain only
B. OFDMA allocates user in time and frequency domain
   - more flexible







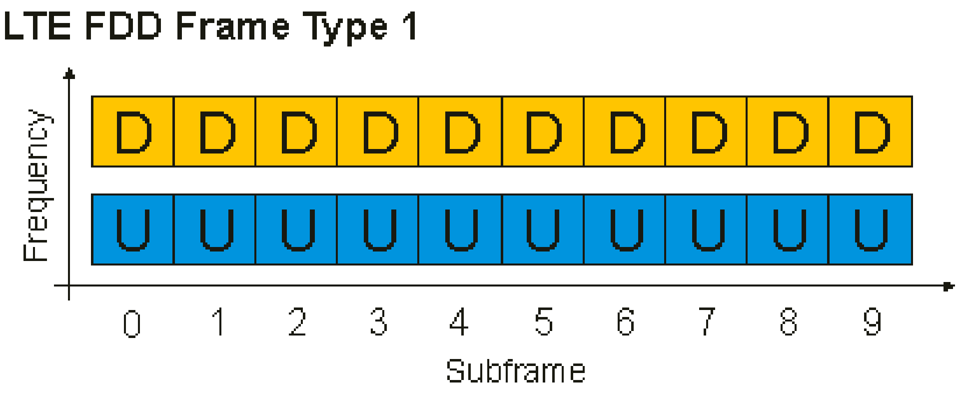
Data symbols occupies 15kHz for one OFDMA symbol period

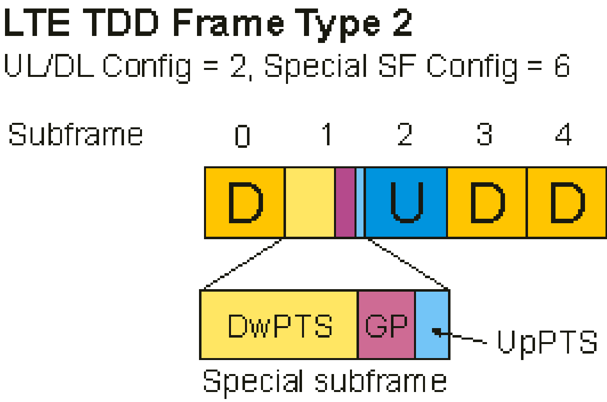
Data symbols occupies N*15kHz for 1/N SC-FDMA symbol period

FDD and TDD mode

- FDD and TDD transmission can occur in both directions simultaneously so that data can flow downlink (DL) and uplink (UL) at the same time. TDD systems use a single frequency band for both transmit and receive.

- In FDD (Frequency Division Duplex) mode, UL and DL frames are both 10ms long and are separated either in frequency or in time, For full-duplex FDD, uplink and downlink frames are separated by frequency and are transmitted continuously and synchronously.
- In TDD (Time Division Duplex) mode, the uplink and downlink subframes are transmitted on the same frequency and are multiplexed in the time domain. Special subframes are used for switching from downlink to uplink





LTE and LTE-Advanced UE categories & class definition

UE Category		Max. Data Rate		Min. Number of DL CCs	DL MIMO Layers	Highest Modulation	
		DL	UL			DL	UL
Rel 8	1	~ 10 Mbps	~ 5 Mbps	1	1	64 QAM	16 QAM
	2	~ 50 Mbps	~ 25 Mbps		2		
	3	~ 100 Mbps	~ 50 Mbps				
	4	~ 150 Mbps	~ 50 Mbps				
	5	~ 300 Mbps	~ 75 Mbps				64 QAM
Rel 10	6	~ 300 Mbps	~ 50 Mbps	1 or 2	2 or 4		16 QAM
	7	~ 300 Mbps	~ 100 Mbps				
	8	~ 3000 Mbps	~ 1500 Mbps	5	8		64 QAM
Rel 11	9	~ 450 Mbps	~ 50 Mbps	2 or 3	2 or 4		16 QAM
	10	~ 450 Mbps	~ 100 Mbps				
	11	~ 600 Mbps	~ 50 Mbps	2, 3 or 4		256 QAM	
	12	~ 600 Mbps	~ 100 Mbps				

Within the OFDM signal it is possible to choose between three types of modulation for the LTE signal:

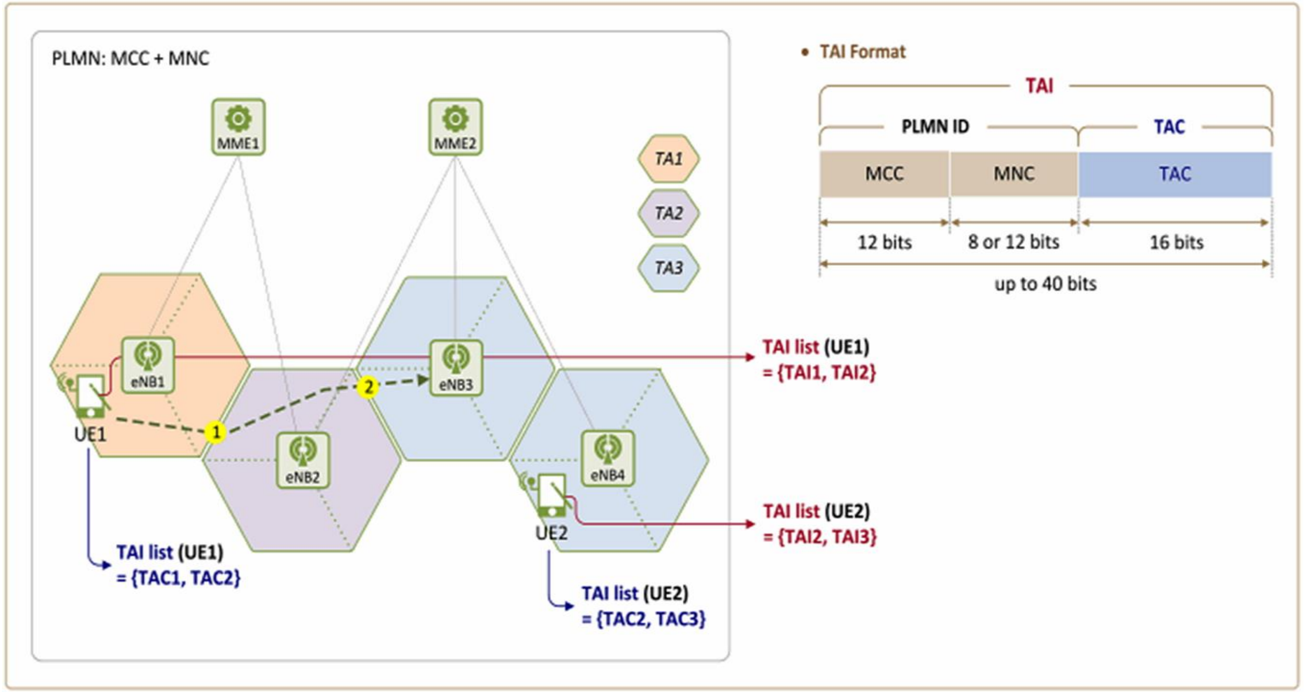
- QPSK (= 4QAM) 2 bits per symbol
- 16QAM 4 bits per symbol
- 64QAM 6 bits per symbol

- The OFDM signal used in LTE comprises a maximum of 2048 different sub-carriers having a spacing of 15 kHz. Although it is mandatory for the mobiles to have capability to be able to receive all 2048 sub-carriers, not all need to be transmitted by the base station which only needs to be able to support the transmission of 72 sub-carriers (6 PRBs or 1.4MHz bandwidth). In this way all mobiles will be able to talk to any base station.

- CA (Carrier Aggregation) is used in LTE-Advanced in order to increase the bandwidth (and bitrate), each aggregated carrier is referred to as a CC (Component Carrier)

LTE terminology

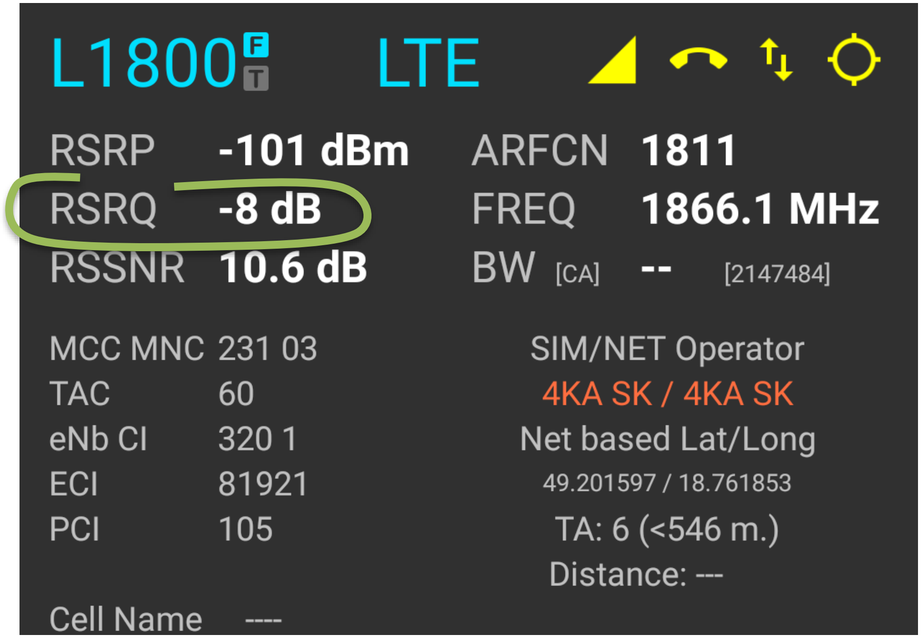
- While the UE is in idle state (i.e. while not communicating or in RRC-Idle state), its location is known by the LTE network at TA level (i.e. on a TA granularity), instead of Cell level. An operator defines a group of neighbor eNBs as a TA
- If there is data traffic heading to a UE in idle state (e.g. if someone sends a text message to a UE), the LTE network has to wake up the UE so that it can receive the data. Here, this "waking up" (called **Paging** or also Discontinuous Reception - **DRX**) is performed TA-wide.
- UE notifies, in idle state via Periodic TAU (TA Update), the LTE network (MME) of its current location by sending a TAU message (TAU Request message) every time it moves between TAs



- **TAC** Tracking Area Code
- **TAI** Tracking Area Identity = PLMN ID + TAC P-GW
- **TAI List** UE can move into the cells included in TAL list without Location Update (TA Update)
- **Local Cell ID (CI)** identify of the cell from an OAM perspective
- **ECI** E- UTRAN Cell ID - **eNodeB ID** (first 20 most significant bits) and the Local Cell ID (the last 8 bits) (2^8) * eNodeB-ID + Local-Cell-ID
- **PCI** Physical Cell Identity - has a range 0 - 503 and it is used to scramble the data to help the mobile separate information from the different transmitters. PCI will determine the primary and secondary sync signal sequence

LTE terminology

- 2G uses LAC (Location Area Code) – identifies area within PLMN, LTE uses **TAC** (Tracking Area Code)
- ARFCN (Absolute Radio Frequency Channel Number)
- **TA** (Timing Advance) in LTE - 78.125 m one way per unit (TA: 0, 1, 2… 1282)
- LTE uses **RSRP** (Reference Signal Receive Power) instead of RSSI (Received Signal Strength Indicator) in GSM
  - RSSI is th power of the signal
  - RSRP is the average power received from a single cell of a single **RE** (Resource Element) that carry cell specific Reference Signals (**RS**) over the entire bandwidth, so RSRP is only measured in the symbols carrying RS
  - RSRP does a better job of measuring signal power from a specific sector and RE while potentially excluding noise and interference from other sectors (RSSI)
  - RSRP measurements are used for cell selection, hand-overs
  - expressed in dBm
  - RSSI = wideband power = noise + serving cell power + interference power
  - RSSI = 12 * N_{PRB} * RSRP , N_{PRB} = number of PRBs [W]
  - defined from -140 dBm to – 44 dBm



- **RSRQ** (Reference Signal Received Quality) is defined as the ratio N_{PRB} × (RSRP / RSSI)
  - RSRQ is defined from -3dB to -19.5dB, -3dB to -15dB means good signal
- **RSSNR** (RS Signal to Noise Ratio)

LTE terminology

RSRP

RSRP	Signal strength	Description
>= -80 dBm	Excellent	Strong signal with maximum data speeds
-80 dBm to -90 dBm	Good	Strong signal with good data speeds
-90 dBm to -100 dBm	Fair to poor	Reliable data speeds may be attained, but marginal data with drop-outs is possible. When this value gets close to -100, performance will drop drastically

RSRQ

RSRQ	Signal quality	Description
>= -10 dB	Excellent	Strong signal with maximum data speeds
-10 dB to -15 dB	Good	Strong signal with good data speeds
-15 dB to -20 dB	Fair to poor	Reliable data speeds may be attained, but marginal data with drop-outs is possible. When this value gets close to -20, performance will drop drastically

- RSRQ is the key parameter, however if RSRP value (power of the signal on the receiver antenna) is too low, it can be close or bellow the sensitivity of the UE / receiver

AS - UE 1st time switched on

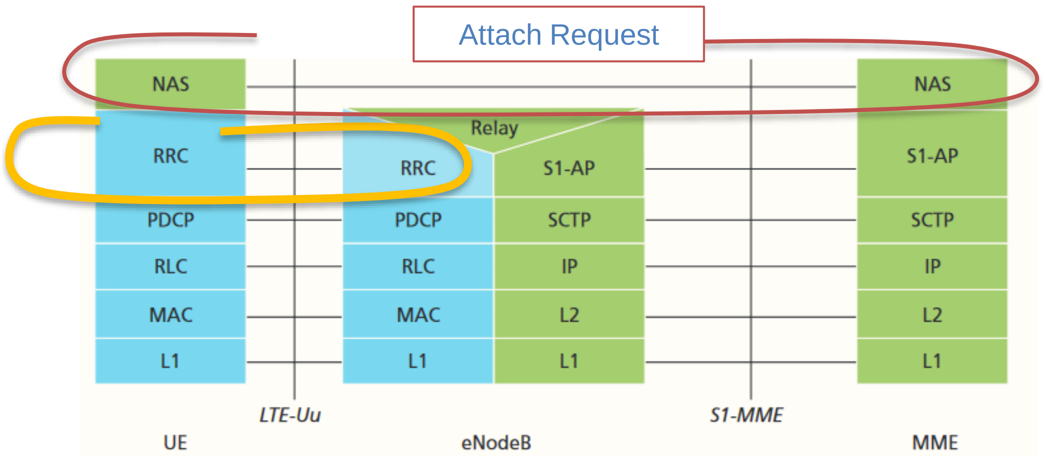
- Typically, LTE channels on adjacent cells will be on the same carrier (operating) frequency (in opposite with GSM). This does lead to interference between the cells, particularly at the cell edge, but it is manageable through adaptive coding and modulation
- Adjacent cells could use different frequencies (if operator has enough spectrum) but that means every hand-over is an inter-frequency hand-over – not desirable. PCI is used to determine the primary and secondary sync signal sequence

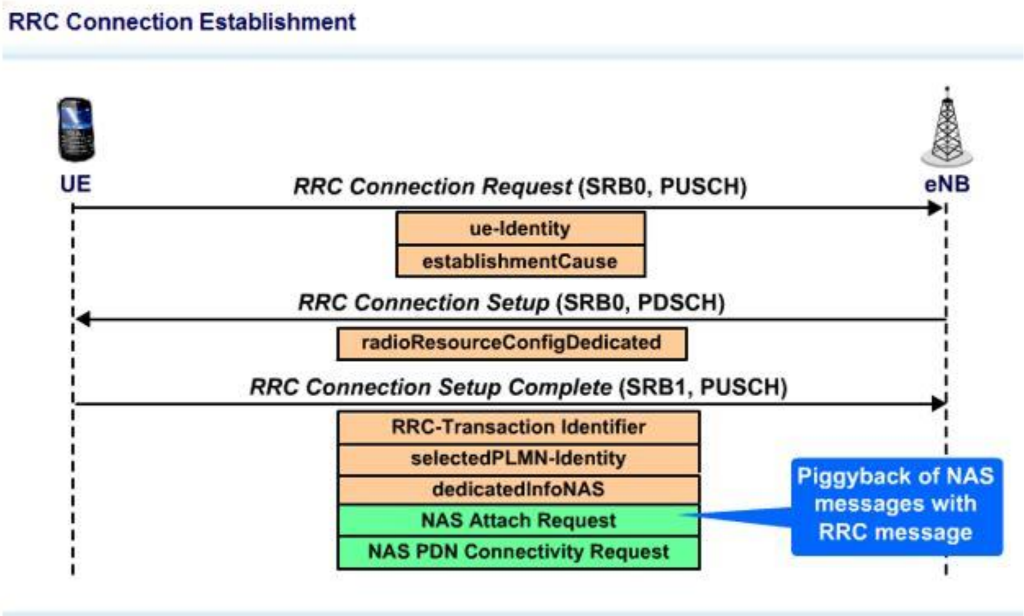
1. Scanning - phone scans all the available radio frequencies in the given LTE band/s, the strongest frequency with signal is chosen by using RSRP measurement
2. Downlink synchronization - UE needs to know PCI and frame timing, done by acquiring synchronization signals. PSS (Primary Synchronization signal) transmitted as the last OFDM symbol of 1st and 11th time slot.
3. Decoding Broadcast Information - bandwidth info via MIB (Master Information Block), first 4 OFDM symbols of second slot of first sub frame, transmitted every 40ms. Now UE knows how many PRBs (Phy Resource Blocks) are functional. UE reads also SIB1 (System Information Block) to decode eNodeB information (Cell ID, MCC, MNC, TAC, other SIB types mapping)
4. The Operator selection – PLMN ID comes from SIB. If selection fails (not allowed operator, test cell, etc.), the UE will have to find another LTE cell.
5. Uplink synchronization - UE undergoes a procedure called RACH (Random Access) to gain access of the resources to start transmission of uplink data – towards eNodeB. Control plane bidir frames can be now exchanged.

AS - UE 1st time switched on

6. RRC (Radio Resource Control) connection setup

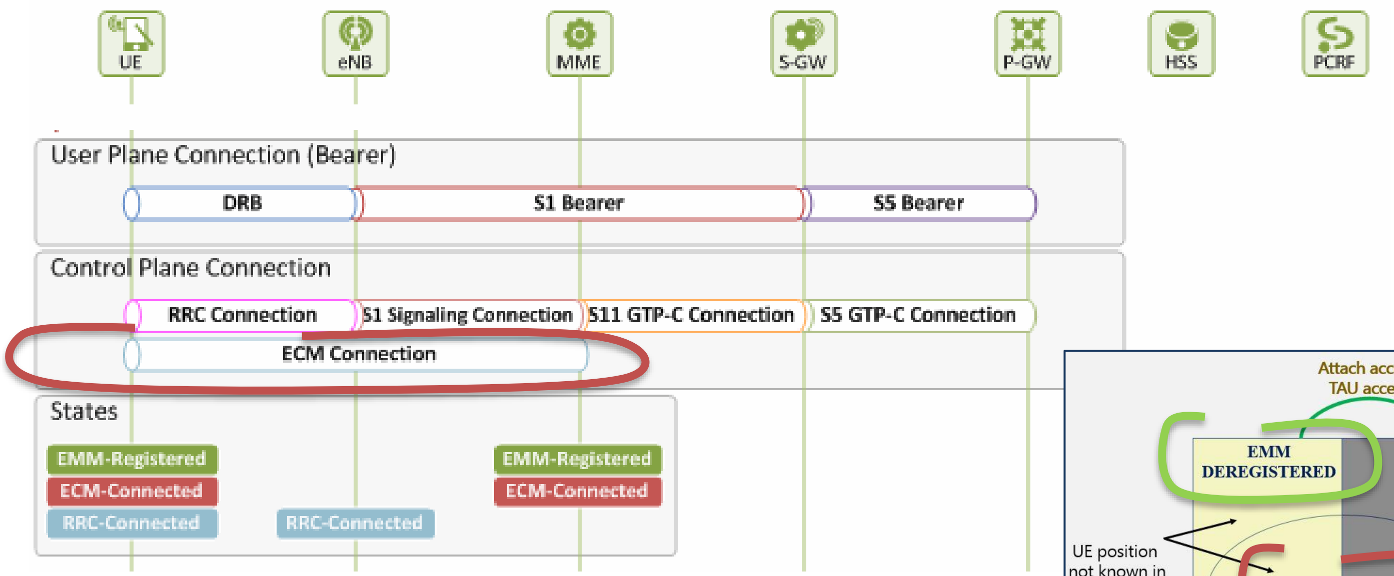
- **RRC Connection Request** - The UE will include in this message its UE identity, and the Establishment cause, for example; *Emergency*, *Mobile originated Signaling*, or *Mobile originated Data*
- **RRC Connection Setup –** confirmation from eNB side
- **RRC Connection Setup Complete** message to the eNB to confirm the successful 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 the MME.
  - Attach Request message includes EPS attach type, EPS mobile identity, UE network capability, ESM message container, Old P-TMSI signature, Additional GUTI, Last visited registered TAI, DRX parameter, Old location area identification, Additional update type, Voice domain preference and UE's usage setting etc…

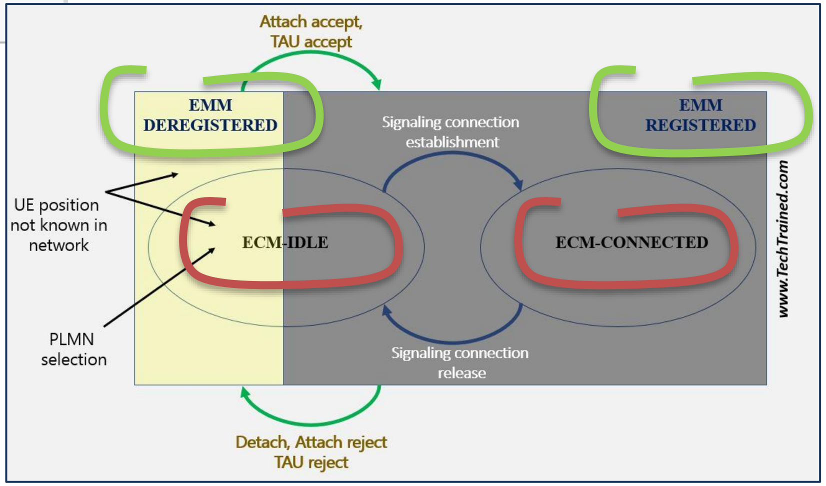


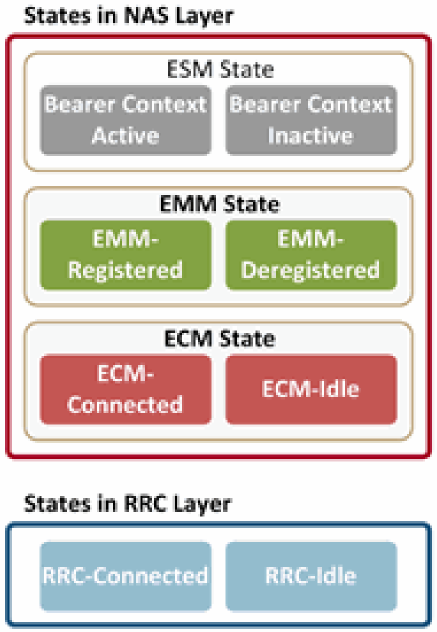


NAS - Mobility and Connection management

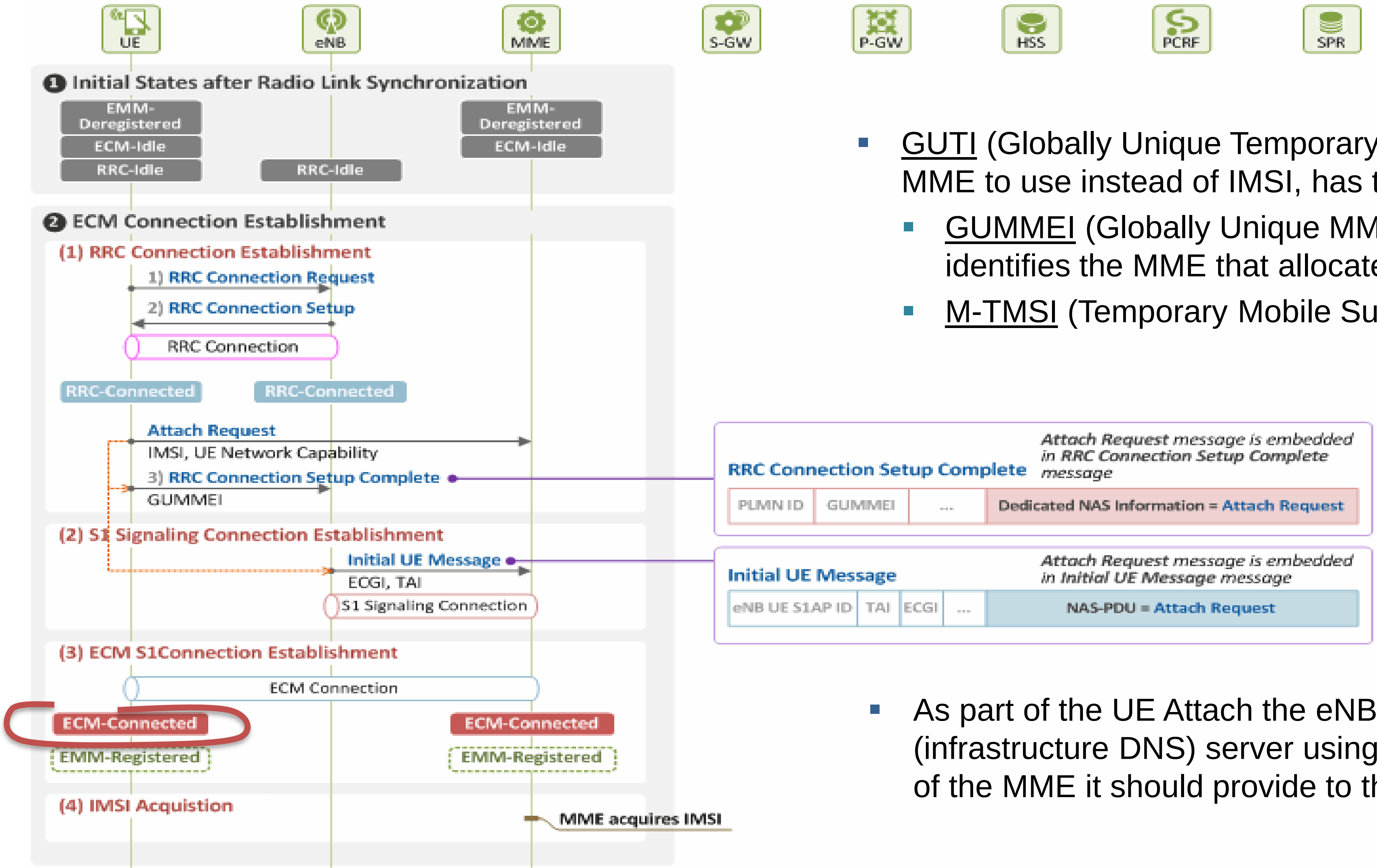
- ECM (EPS Connection Management) describes the signaling connectivity state between the UE and the EPC. It can be in 2 states: IDLE and CONNECTED
- EMM (EPS Mobility Management) states describe the Mobility Management states that result from the mobility management procedures like Attach / Detach, Paging and TAU (Tracking Area Update) procedures. It ensures if and where UE is reachable by the network and can receive the service.
  - UE can move from DEREGISTRED into REGISTERED state by completing *TAU* or after a successful handover or *Attach* procedure







1/5 Initial Attach with IMSI – Attach Request

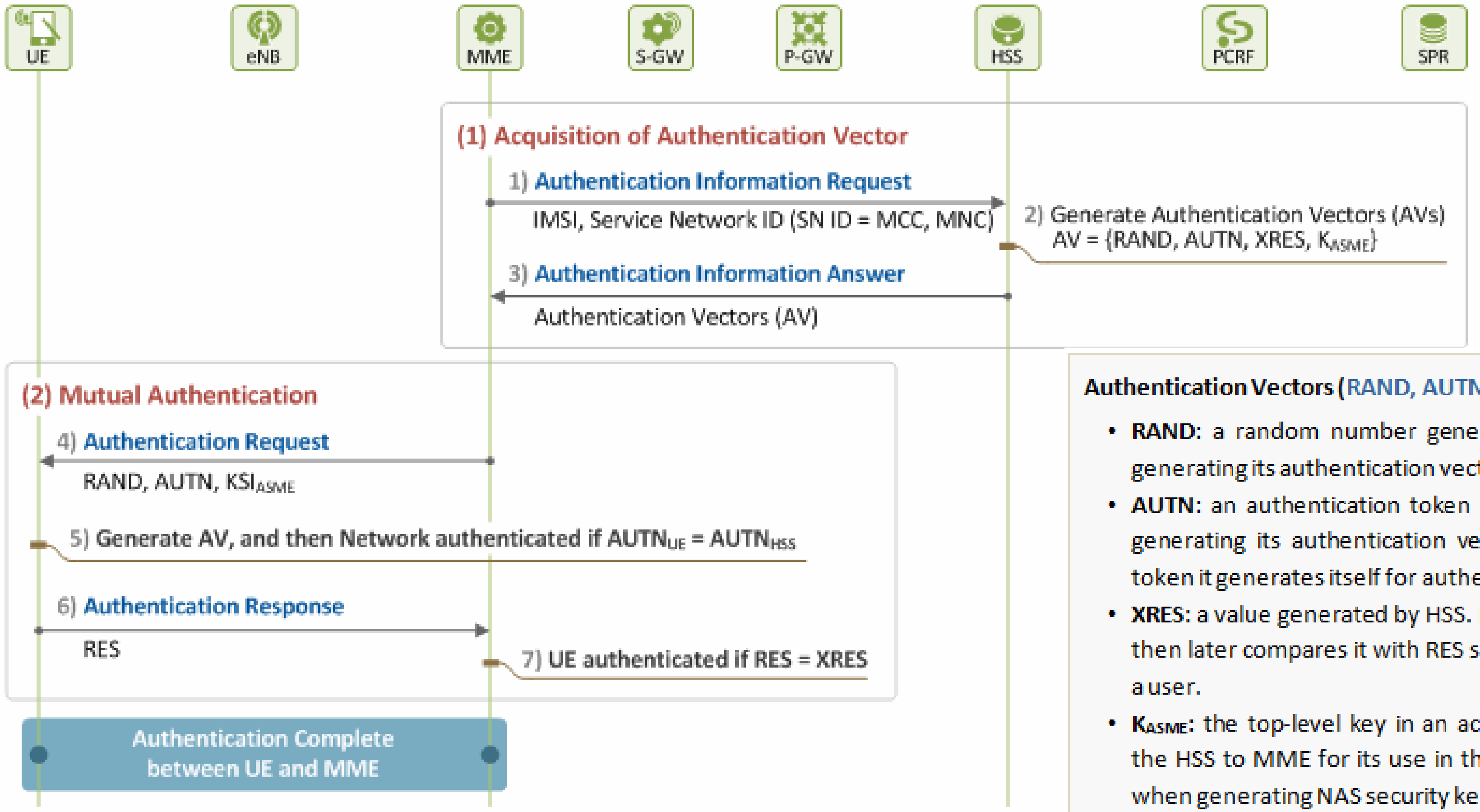


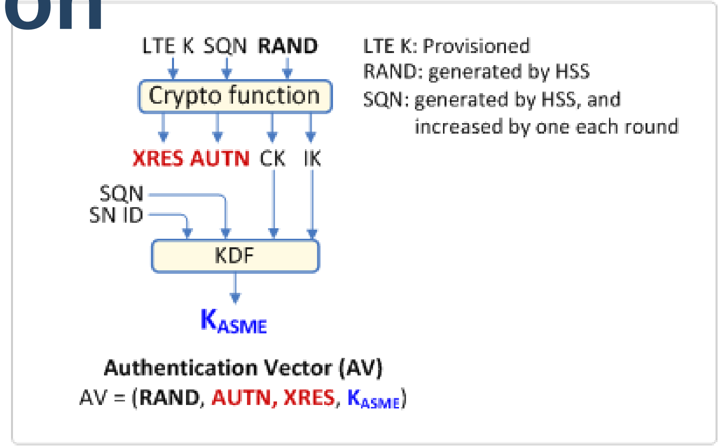
www.netmanias.com

- GUTI (Globally Unique Temporary Identity), allocated by MME to use instead of IMSI, has two main components:
  - GUMMEI (Globally Unique MME Identifier) that uniquely identifies the MME that allocated the GUTI
  - M-TMSI (Temporary Mobile Subscriber Identity)

- As part of the UE Attach the eNB will query the iDNS (infrastructure DNS) server using the TAI for the IP address of the MME it should provide to that UE

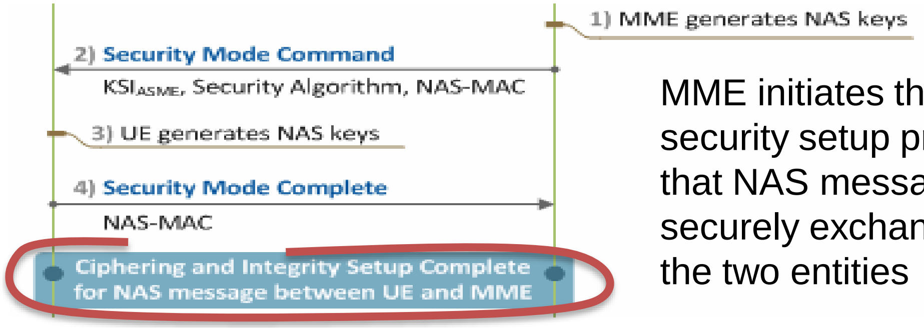
2/5 Initial Attach with IMSI – Authentication





Authentication Vectors (RAND, AUTN, XRES, K_{ASME})

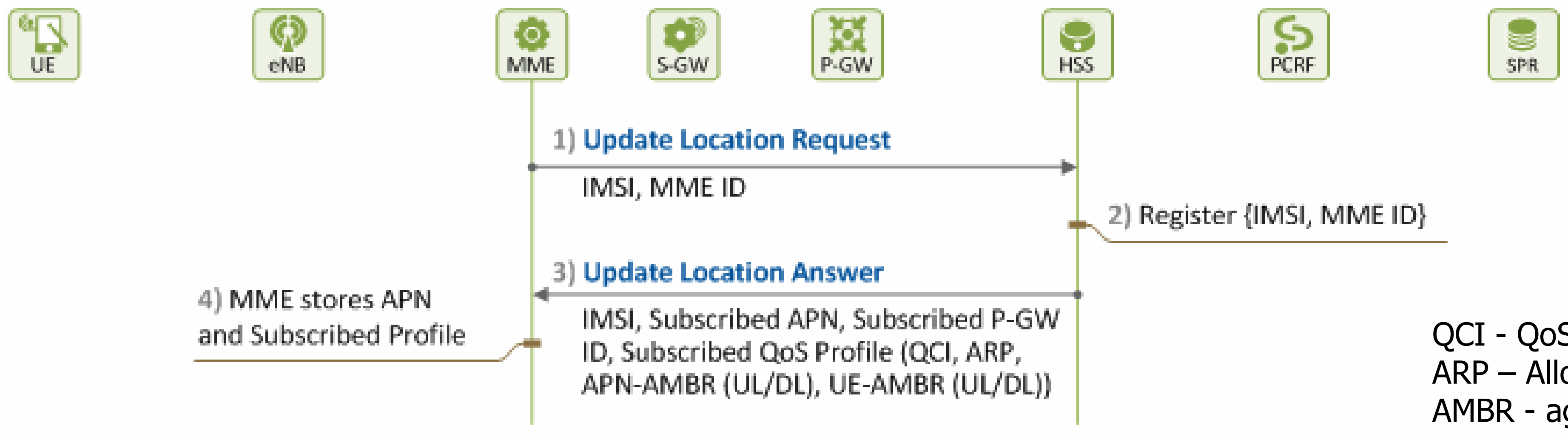
- **RAND**: a random number generated by HSS and delivered to UE. The UE uses it when generating its authentication vectors.
- **AUTN**: an authentication token generated by HSS and also delivered to UE. The UE, after generating its authentication vectors, compares the value of this token with that of the token it generates itself for authenticating a network.
- **XRES**: a value generated by HSS. MME keeps this value to itself without sending it to UE, and then later compares it with RES sent by the UE after network authentication to authenticate a user.
- **K_{ASME}**: the top-level key in an access network, generated by UE and HSS, and delivered by the HSS to MME for its use in the access network. It serves as a base key of MME and UE when generating NAS security keys.



MME initiates the NAS security setup procedure so that NAS messages can be securely exchanged between the two entities

KDF - Key Derivation Function, HMAC-SHA-256
KSI_{ASME} is an index for K_{ASME}

3/5 Initial Attach with IMSI – Location Update



QCI - QoS class identifier
ARP – Allocation retention policy
AMBR - aggregate maximum bit rate

- SGW/PGW and its internal (infrastructure) IPv4 address can be provided from HSS database or statically configured on MME
- However, during UE attach the MME can query the iDNS server to select the PDN-GW (Packet Data Network Gateway, PGW) where a requested (subscribed) PDN connectivity (APN) is located. Selection can be based on the information provided to the MME, when the UE attaches to the network.
- It is followed by the PGW selection (but could be also in opposite, SGW selection based on TAC first), the MME query the iDNS server to select an available SGW to serve the UE using the TAC, which in most cases is based on network topology and the location of the UE within the network, so that the best SGW is selected
- Within the EPC network the EPS nodes would access the iDNS servers via O&M interface (can be also Gn in 3G)

Infrastructure DNS – specific service resolving process

- FQDN (Fully Qualified Domain Name) - is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS)
  - DNS client performs a single or multiple look up operations in order to get IP address for a service and server
  - The home network domain for EPC will be in the form 'epc.mnc<mnc-val>.mcc<mcc-val>.3gppnetwork.org'

- NAPTR (Name Authority Pointer) DNS record- specifies lookup services for a wide variety of resources names, used to add particular services to a DNS entry, the output is service's FQDN (with exception of "a" knob)
  - It is common to use simplified S-NAPTR (Straightforward NAPTR) in EPC
  - apnComm.apn IN NAPTR 100 100 "s" "x-3gpp-pgw:x-s5-gtp" "" _nodes._pgw
  - apnName3.apn IN NAPTR 100 100 "a" "x-3gpp-pgw:x-s5-gtp" "" topon.s5-pgw.nodeName1
  - only "**S**", "**A**" or "" flags are allowed with S-NAPTR. "**S**" means next query is SRV, "**A**" means skip SRV and proceed with A record

- SRV (Service) DNS record - clients can ask for a specific service/protocol for a specific domain and gets back the names of any available servers, the output is server's FQDN
  - _nodes._pgw 1800 IN SRV 20 100 2123 topon.pgw.nodeName1
  - _nodes._pgw 1800 IN SRV 20 100 2123 topon.pgw.nodeName2

Round Robin Selection

- A records (or 'Address Records') returns an IPv4 address a specific domain name
  - topon.pgw.nodeName1 IN A 10.1.1.1
  - topon.pgw.nodeName2 IN A 10.2.2.2

Infrastructure DNS - example

;TAI S-NAPTR
;TA which exist within the North or South region
;North:
tac-lb01.tac-hb00.tac IN NAPTR 100 100 "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._north
tac-lb02.tac-hb00.tac IN NAPTR 100 100 "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._north
tac-lb03.tac-hb00.tac IN NAPTR 100 100 "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._north
;South:
tac-lb044.tac-hb00.tac IN NAPTR 100 100 "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._south
tac-lb045.tac-hb00.tac IN NAPTR 100 100 "s" "x-3gpp-sgw:x-s5-gtp" "" _sgw._south

;APN S-NAPTR
;APN's which exist only on one PGW use NAPTR "a" flag
;North:
apnName1.apn IN NAPTR 100 100 "a" "x-3gpp-pgw:x-s5-gtp" "" topon.s5-pgw.nodeName1.site1.north
apnName2.apn IN NAPTR 100 100 "a" "x-3gpp-pgw:x-s5-gtp" "" topon.s5-pgw.nodeName2.site2.north
;South:
apnName3.apn IN NAPTR 100 100 "a" "x-3gpp-pgw:x-s5-gtp" "" topon.s5-pgw.nodeName3.site3.south
apnName4.apn IN NAPTR 100 100 "a" "x-3gpp-pgw:x-s5-gtp" "" topon.s5-pgw.nodeName4.site4.south
;Common APN on all PGW's use NAPTR "s" flag
apnComm.apn IN NAPTR 100 100 "s" "x-3gpp-pgw:x-s5-gtp" "" _nodes._pgw

Direct mapping

"a" flag means skip SRV part

SRV Records for SGW
;North
_sgw._north 1800 IN SRV 20 100 2123 topon.s5-sgw.nodeName1.site1.north
_sgw._north 1800 IN SRV 20 100 2123 topon.s5-sgw.nodeName2.site2.north
;South
_sgw._south 1800 IN SRV 20 100 2123 topon.s5-sgw.nodeName3.site3.south
_sgw._south 1800 IN SRV 20 100 2123 topon.s5-sgw.nodeName4.site4.south

Round Robin Selection

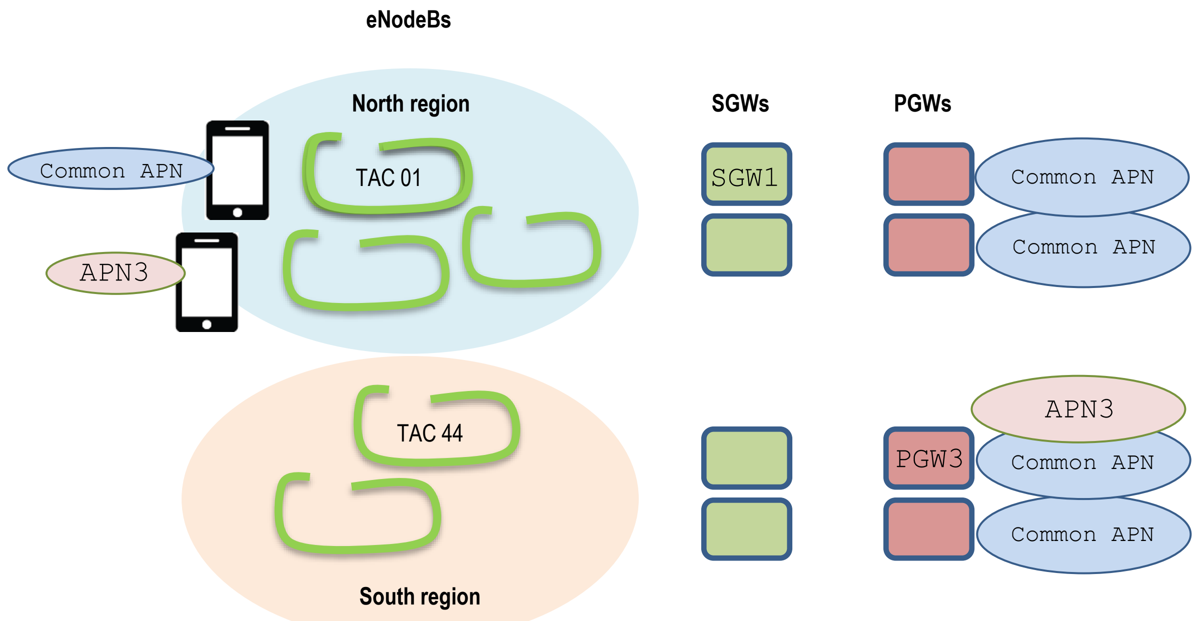
;SRV Records for PGW
;PGW, Equal weight for common apn's, TTL 1800. Port gtp-c v2 is 2123
_nodes._pgw 1800 IN SRV 20 100 2123 topon.s5-pgw.nodeName1.site1.north
_nodes._pgw 1800 IN SRV 20 100 2123 topon.s5-pgw.nodeName2.site2.north
_nodes._pgw 1800 IN SRV 20 100 2123 topon.s5-pgw.nodeName3.site3.south
_nodes._pgw 1800 IN SRV 20 100 2123 topon.s5-pgw.nodeName4.site4.south

Round Robin Selection

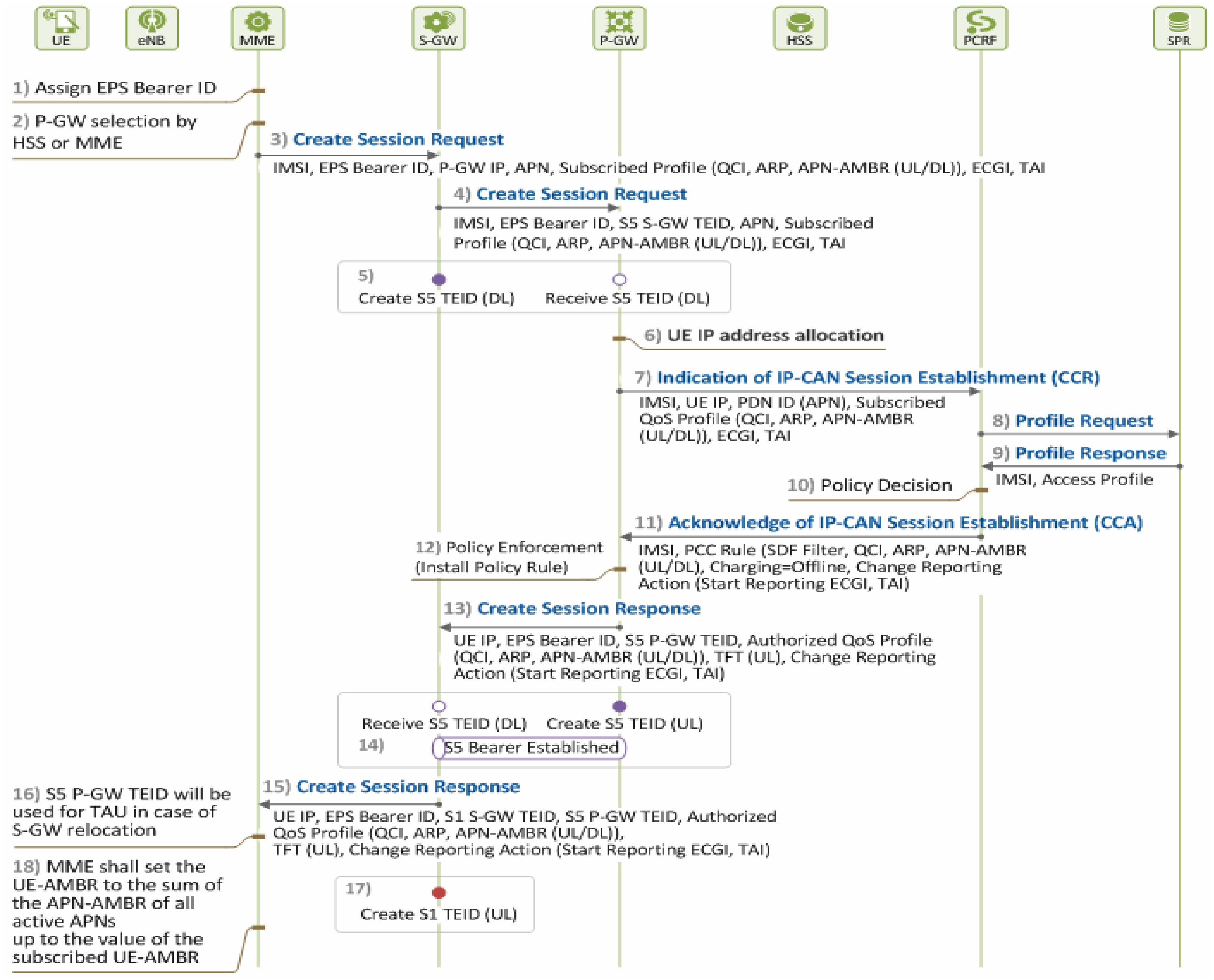
A records for SGW
;S11 addresses of SGWs that support GTP based S5 interfaces.
topon.s5-sgw.nodeName1.site1.north IN A 10.5.5.5
topon.s5-sgw.nodeName2.site2.north IN A 10.6.6.6
topon.s5-sgw.nodeName3.site3.south IN A 10.7.7.7
topon.s5-sgw.nodeName4.site4.south IN A 10.8.8.8

;A records for PGW
;S5 address of PGWs that support GTP based S5 interfaces.
topon.s5-pgw.nodeName1.site1.north IN A 10.1.1.1
topon.s5-pgw.nodeName2.site2.north IN A 10.2.2.2

topon.s5-pgw.nodeName3.site3.south IN A 10.3.3.3
topon.s5-pgw.nodeName4.site4.south IN A 10.4.4.4



4/5 Initial Attach with IMSI – default session/bearer setup



1. IP address allocation on PGW could be done via Diameter, Radius or from a local pool
2. IP-CAN (IP Connectivity Access Network) request – type of the connectivity for the subscriber (traffic attributes)
   - CCR Credit Control Request
   - CCA Credit Control Answer
3. PCRF provides PCC (Policy and Charging Control) rules
4. SPR (Subscription Profile Repository)
5. QCI (QoS Class Identifier) per single bearer, APN-AMBR (Aggregate Maximum Bitrate) per the same APN bearers, UE-AMBR per all bearers/single subscriber
6. ARP - Allocation and Retention Priority

Notes:

- UE-AMBR will be lowest of either pre-configured UE-AMBR via HSS or Sum of all APN-AMBRs for that subscriber.
- For LTE following protocols are used GTPv2-C & GTPv1-U

Wireshark – Create Session RESPONSE part 1

```
▷ Frame 4: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface 0
▷ Ethernet II, Src: Superlan_01:00:0a (00:00:01:01:00:0a), Dst: TimetraN_57:53:85 (00:03:fa:57:53:85)
▷ 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 1
▷ Internet Protocol Version 4, Src: 50.50.50.1, Dst: 10.207.5.2
▷ User Datagram Protocol, Src Port: 2123, Dst Port: 2123
◢ GPRS Tunneling Protocol V2
  ▷ Flags: 0x48
    Message Type: Create Session Response (33)
    Message Length: 173
    Tunnel Endpoint Identifier: 0x000f4240 (1000000)
    Sequence Number: 0x00000001 (1)
    Spare: 0
  ▷ Cause : Request accepted (16)
  ▷ Recovery (Restart Counter) : 1
  ▷ Protocol Configuration Options (PCO) :
  ▷ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S11/S4 SGW GTP-C interface, TEID/GRE Key: 0xfe100800, IPv4 50.50.50.1
  ▷ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 PGW GTP-C interface, TEID/GRE Key: 0xfe100800, IPv4 50.50.50.1
  ▷ APN Restriction : value 0
  ◢ PDN Address Allocation (PAA) :
      IE Type: PDN Address Allocation (PAA) (79)
      IE Length: 22
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
      .... .011 = PDN Type: IPv4/IPv6 (3)
      IPv6 Prefix Length: 64
      PDN Address and Prefix(IPv6): 20012001200100010000000000000000
      PDN Address and Prefix(IPv4): 180.0.0.1
```

Wireshark – Create Session RESPONSE part 2

```
◢ Aggregate Maximum Bit Rate (AMBR) :
    IE Type: Aggregate Maximum Bit Rate (AMBR) (72)
    IE Length: 8
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    AMBR Uplink (Aggregate Maximum Bit Rate for Uplink): 1234
    AMBR Downlink(Aggregate Maximum Bit Rate for Downlink): 4321
◢ Bearer Context : [Grouped IE]
    IE Type: Bearer Context (93)
    IE Length: 50
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
  ▷ EPS Bearer ID (EBI) : 5
  ▷ Cause : Request accepted (16)
  ▷ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S1-U SGW GTP-U interface, TEID/GRE Key: 0xfe100805, IPv4 50.50.50.1
  ◢ Bearer Level Quality of Service (Bearer QoS) :
      IE Type: Bearer Level Quality of Service (Bearer QoS) (80)
      IE Length: 22
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
      .0.. .... = PCI (Pre-emption Capability): Enabled
      ..00 01.. = PL (Priority Level): 1
      .... ...0 = PVI (Pre-emption Vulnerability): Enabled
      Label (QCI): 8
      Maximum Bit Rate For Uplink: 0
      Maximum Bit Rate For Downlink: 0
      Guaranteed Bit Rate For Uplink: 0
      Guaranteed Bit Rate For Downlink: 0
```

Offline charging, a user is charged for the network resources that he already used, the network reports the resource usage by the particular user by forwarding his CDR (Charging Data Record) to its billing domain.

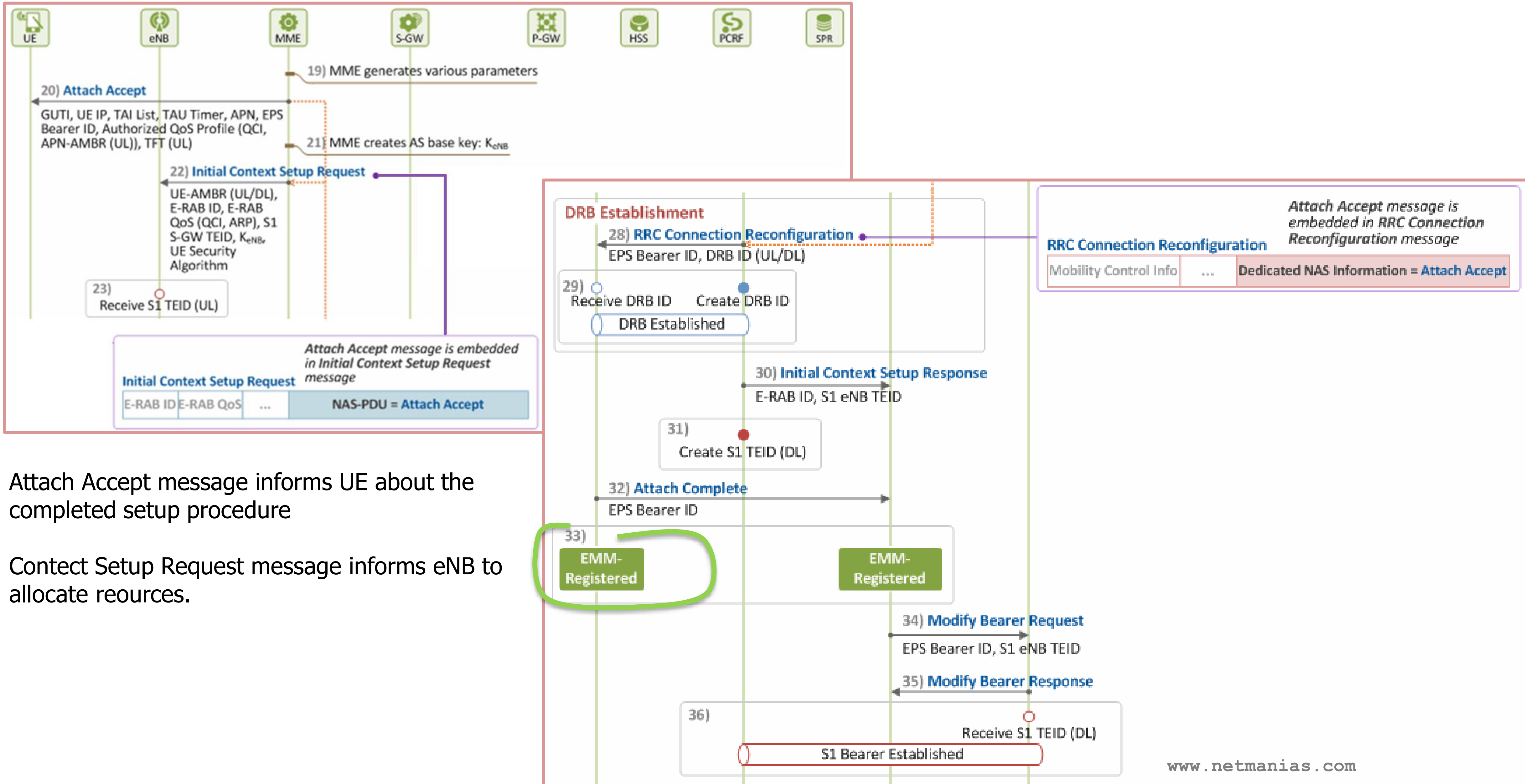
Online charging means real time monitoring

PCC - Policy and Charging Control

Default Bearer QoS	Policy Rule Name	SDF Template	SDF GBR	SDF MBR	SDF QCI/ARP	SDF Gating Status	SDF Charging
Default Bearer (APN: Internet) • QCI=9 • ARP=7 • APN-AMBR(UL)=Unlimited • APN-AMBR(DL)=Unlimited	• "Internet"	• UL: (UE IP, *,*,*,*) • DL: (*,UE IP, *,*,*)	-	• UL: Unlimited • DL: Unlimited	• QCI=9 • ARP=7	• Open (permit)	• Offline
Default Bearer (APN: IMS) • QCI=5 • ARP=6 • APN-AMBR(UL)=100Kbps • APN-AMBR(DL)=100Kbps	• "Voice-C"	• UL: (UE IP, *, SIP, *, UDP) • DL: (*, UE IP, SIP, *, UDP)	-	• UL: 100Kbps • DL: 100Kbps	• QCI=5 • ARP=6	• Open (permit)	• Offline
Dedicated Bearer (APN: IMS) • QCI=1 • ARP=7 • GBR/MBR(UL)=88Kbps • GBR/MBR(DL)=88Kbps	• "Voice-U"	• UL: (UE IP, *, RTP, *, UDP) • DL: (*, UE IP, RTP, *, UDP)	• UL: 88Kbps • DL: 88Kbps	• UL: 88Kbps • DL: 88Kbps	• QCI=1 • ARP=7	• Open (permit)	• Offline

PCRF determines a PCC rule for each SDF (Service Data Flow) based on the operator's policy (e.g. QoS policy, gate status, charging methods, etc.)

5/5 Initial Attach with IMSI – Attach Accept & Context Req



Attach Accept message informs UE about the completed setup procedure

Contect Setup Request message informs eNB to allocate reources.

Signaling states & Data bearer states

Case	State	UE	eNB	S-GW	P-GW	MME	HSS	PCRF	SPR
A	EMM-Deregistered + ECM-Idle + RRC-Idle	-	-	-	-	-	-	-	-
B	EMM-Deregistered + ECM-Idle + RRC-Idle	-	-	-	-	TAI of last TAU	MME	-	-
C	EMM-Registered + ECM-Connected + RRC-Connected	-	Cell/eNB	Cell/eNB	Cell/eNB	Cell/eNB	MME	Cell/eNB	-
D	EMM-Registered + ECM-Idle + RRC-Idle	-	-	TAI of last TAU	TAI of last TAU	TAI of last TAU	MME	TAI of last TAU	-

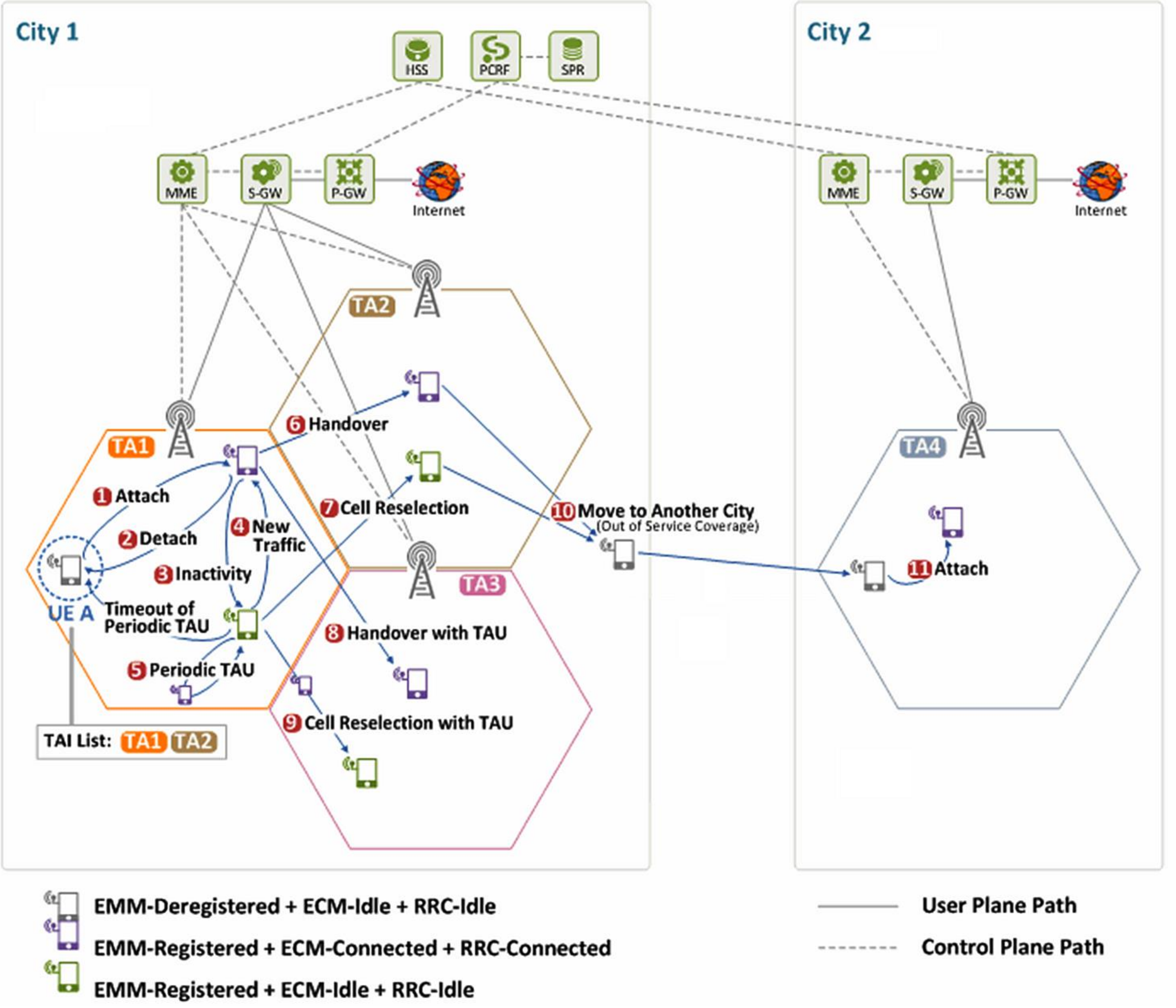
Case	State	UE	eNB	S-GW	P-GW	MME	HSS	PCRF	SPR
A	EMM-Deregistered + ECM-Idle + RRC-Idle	IMSI	-	-	-	-	IMSI	-	IMSI
B	EMM-Deregistered + ECM-Idle + RRC-Idle	IMSI, GUTI	-	-	-	IMSI, GUTI	IMSI	-	IMSI
C	EMM-Registered + ECM-Connected + RRC-Connected	IMSI, GUTI, UE IP addr, C-RNTI	C-RNTI, eNB/MME UE S1AP ID, Old/New eNB UE X2AP ID	IMSI	IMSI, UE IP addr	IMSI, GUTI, UE IP addr, eNB/MME UE S1AP ID	IMSI	IMSI, UE IP addr	IMSI
D	EMM-Registered + ECM-Idle + RRC-Idle	IMSI, GUTI, UE IP addr	-	IMSI	IMSI, UE IP addr	IMSI, GUTI, UE IP addr	IMSI	IMSI, UE IP addr	IMSI

- PLMN or Cell selection process ongoing
- MME may have Tracking AREA info last reported by UE
- Possible handover (X2, intra-eNB or S1 handover), TAU message sent by UE if TA change
- Possible cell re-selection, TAU message sent by UE when TA change, PAGING control, if no mobility then periodic TAU

To save battery life and resources of UE - it goes into IDLE mode after some time. eNB's inactivity timer expires (typical 10 sec) and eNB shuts down RRC connection. It does not release the default bearer (state D -> EMM registered) , it just release the air interface and S1 bearer (ECM / RRC idle). When required it can be re-connected.

PAGING - when a UE is attached to the network, but in idle state (state D), if there is user traffic to deliver, the network (MME->EMM) initiates PAGING message to wake up the UE, consequently transiting the UE’s state to state C. The paging is conducted (eNodeB notifies all TAs cells) based on the Tracking Area Identifier (TAI) information provided by the UE during its last TA update. UE sends Service Request

Handover examples



www.netmanias.com

1. Initial attach
2. Detach
3. Air/S1 release due to inactivity (~10sec) but still periodically listens to PAGING messages (wakes up each 1280 msec)
4. PAGING/Service request due to new traffic
5. UE is not moving, performs periodic TAU updates, active data or reestablishes ECM/RRC (54min)
6. Handover without TAU (TAI List), UE moves in “connected or data active” state
7. Cell reselection without TAU, UE moves in IDLE state
8. Handover with TAU (see 6)
9. Cell reselection with TAU (see 7)
10. No coverage, EMM deregistered
11. Initial attach

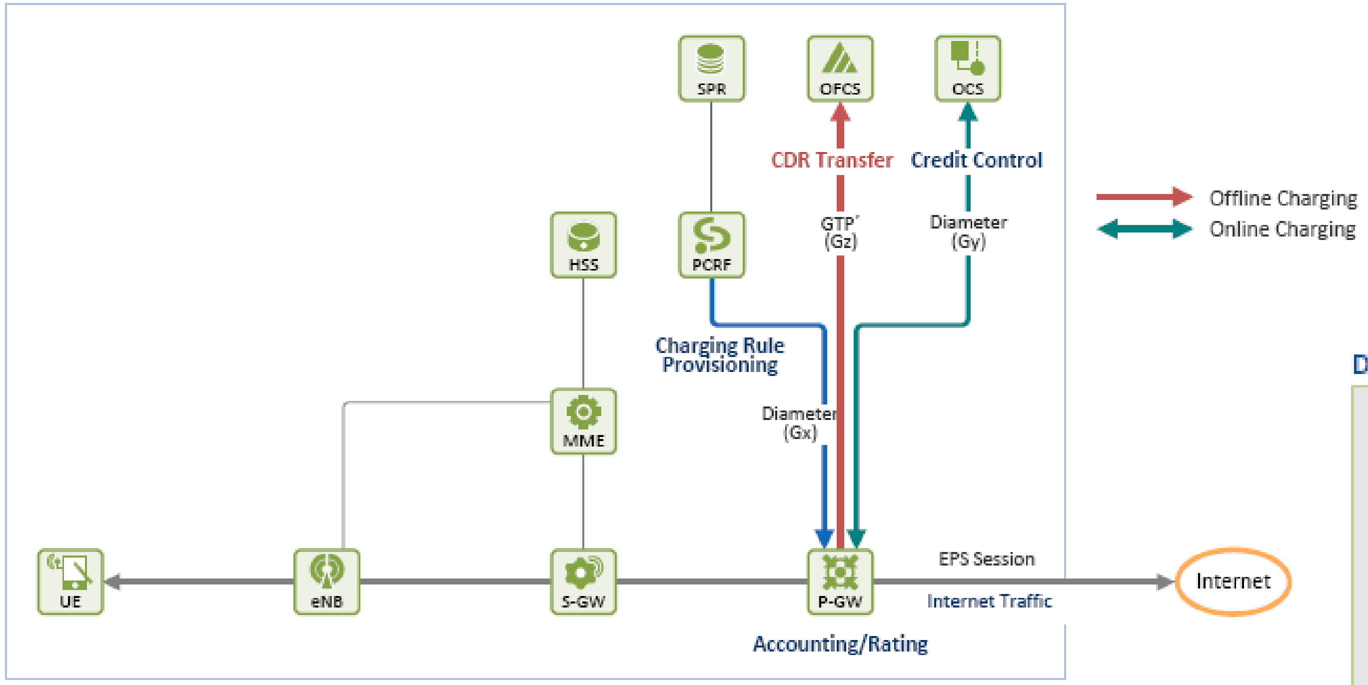
Intra-MME or Intra-S-GW Handover: Neither UE’s serving MME nor S-GW is changed after handover, also called X1 handover

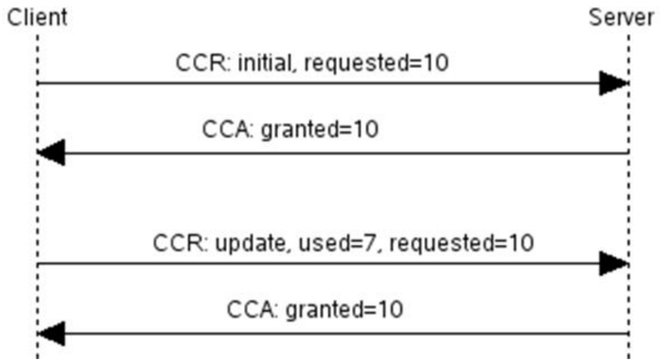
Inter-LTE Handover: UE’s serving MME and/or S-GW is changed

Inter-RAT Handover: Handover between networks that use different radio access technology

Offline and Online charging

- Offline charging, a user is charged for the network resources that he already used, the network reports the resource usage by the particular user by forwarding his CDR (Charging Data Record) generated by PGW to its billing domain via Gz interface.
- Online charging means real time monitoring. Uses Diameter protocol over Gy interface.
  - In online charging PGW requests and obtains a quota first, and then measures and reports the subscriber's usage by performing credit control with OCS (Online Charging System)





Data Record Transfer Request (CDR)

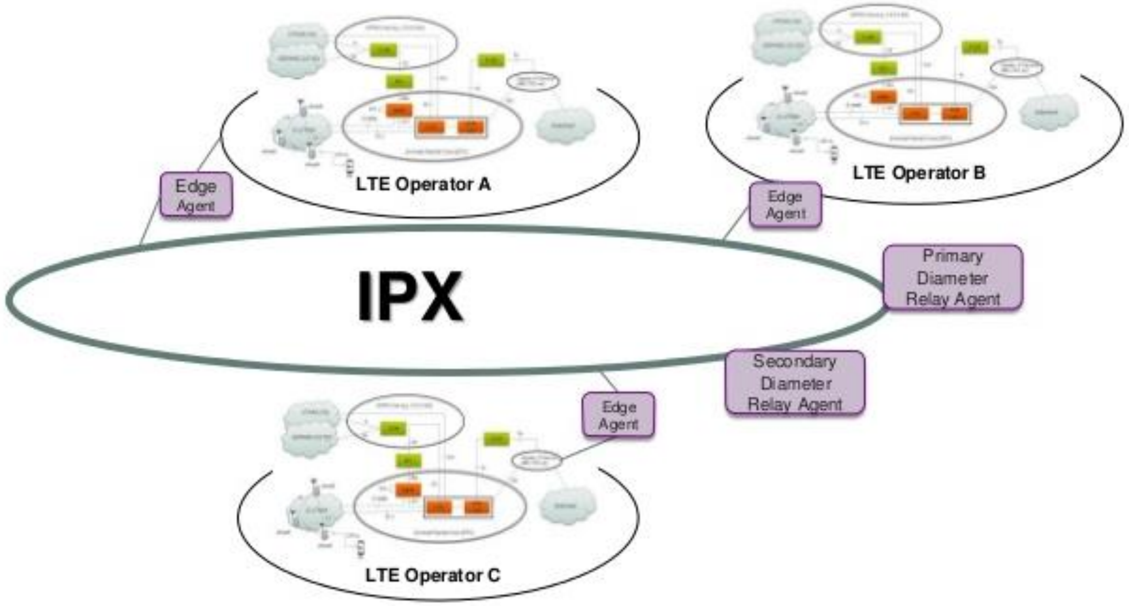
Subscription ID	IMSI
Serving Network ID	PLMN ID (MCC+MNC)
APN Network	Internet
Duration	1462 seconds
PDN Type	IPv4
Served PDN addr	10.25.200.1 (UE IP)
Start Time	18:01:53
End Time	18:47:31
User Location	ECGI, TAI

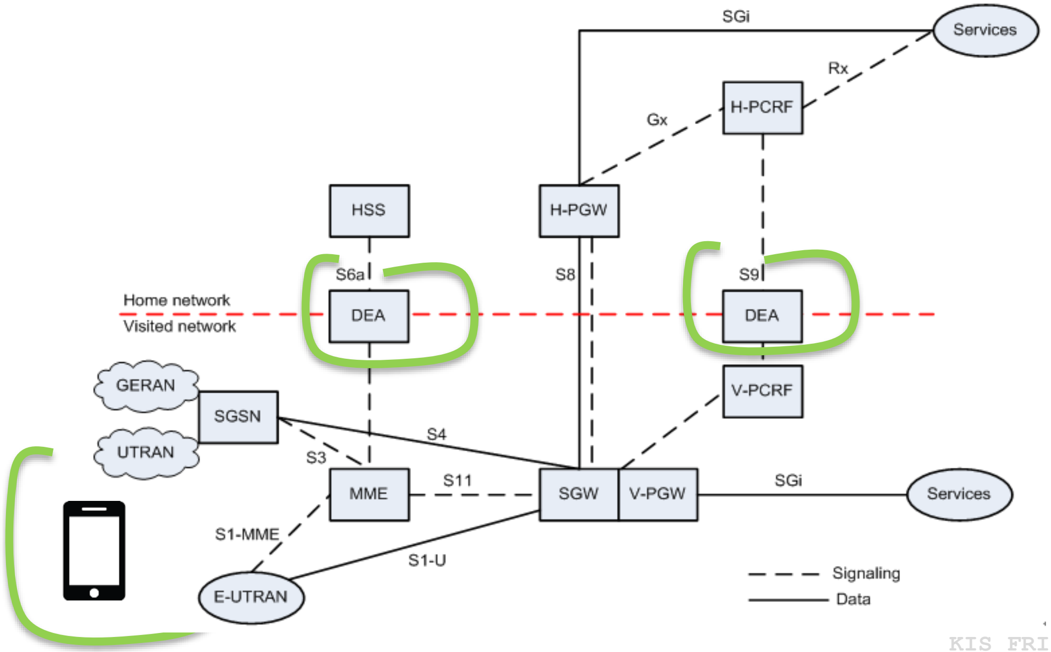
List of Service Data	
Rating Group	rgInternet
Time of First Usage	18:01:53
Time of Last Usage	18:47:31
Time Usage	1462 seconds
Data Volume (UL)	1.54MB
Data Volume (DL)	194.98MB
QoS Information	QCI, ARP, ...

CDR

LTE roaming

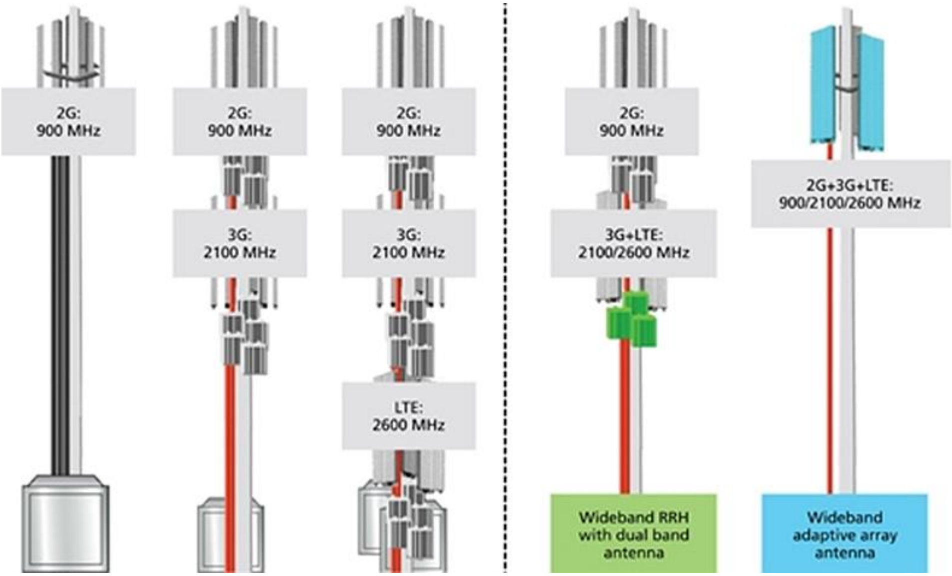
- Roaming - it lets subscribers access voice and data services when traveling outside of their home network thanks to roaming agreements between different operators
- LTE roaming via IPX (IP eXchange network)
- Home-routed roaming enables subscribers to access the internet network through the Home PGW (H-PGW)
- LocalBreakOut roaming enables subscribers to access the internet network through the Visited PGW (V-PGW). The Visited Policy and Charging Rules Function (V-PCRF) must obtain PCC policies of the home network from the Home PCRF (H-PCRF) over the S9 interface
- IPX connectivity via Diameter Edge Agents (DEA)

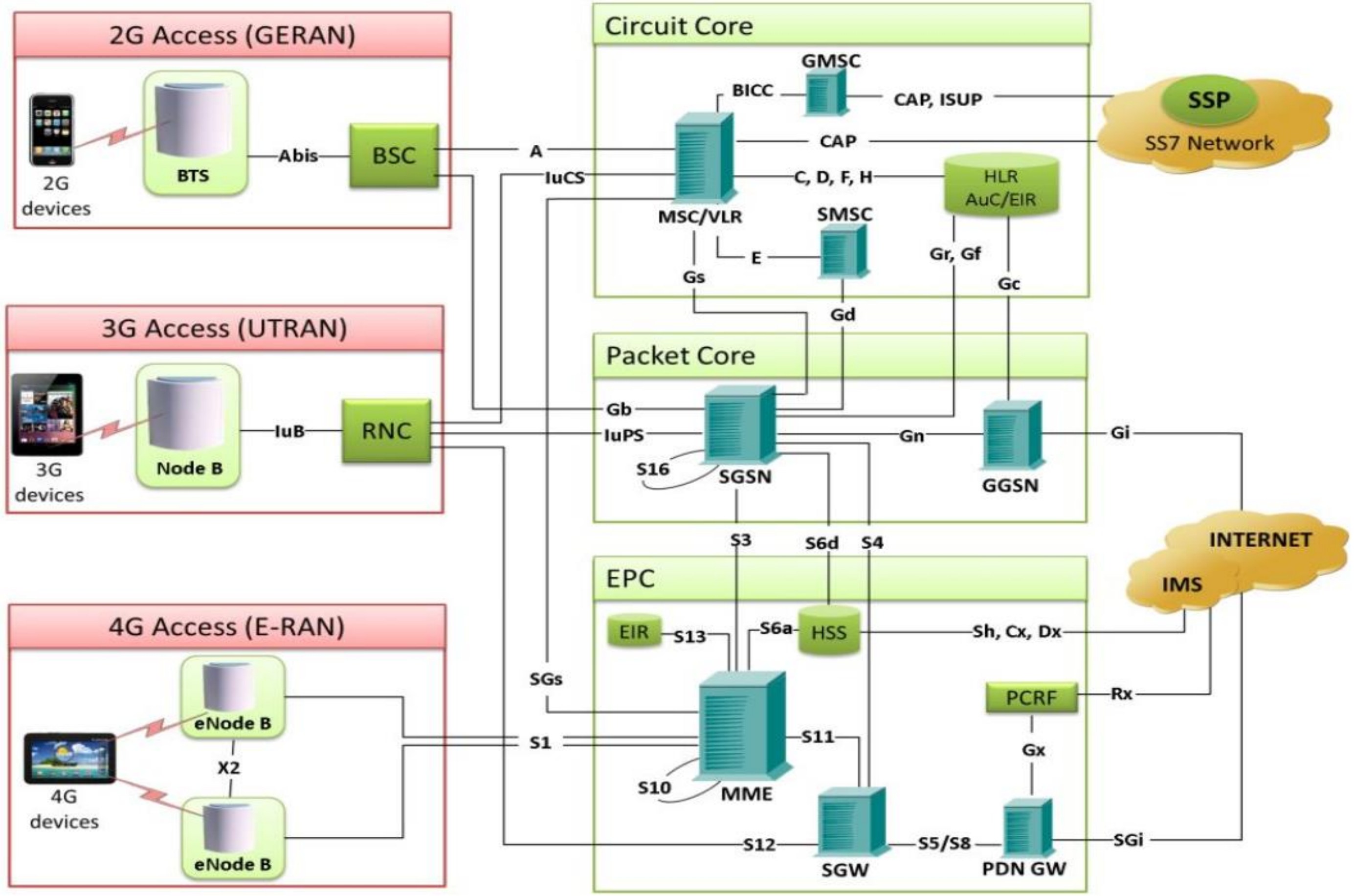




LTE co-existence with 2G / 3G, evolution to Single RAN

- Co-existence of different RATs (Radio Access Technology) and hand-over in between different RAT (so called inter-RAT handover in between 2G, 3G, LTE) of the same operator is necessary.
- Single Radio Access Network (SRAN) involves deploying GSM/UMTS/LTE functionality in a single base station unit (single HW), and hence reduces the operator's Total Cost of Ownership (TCO).





5G / NR
New Radio

5G NR

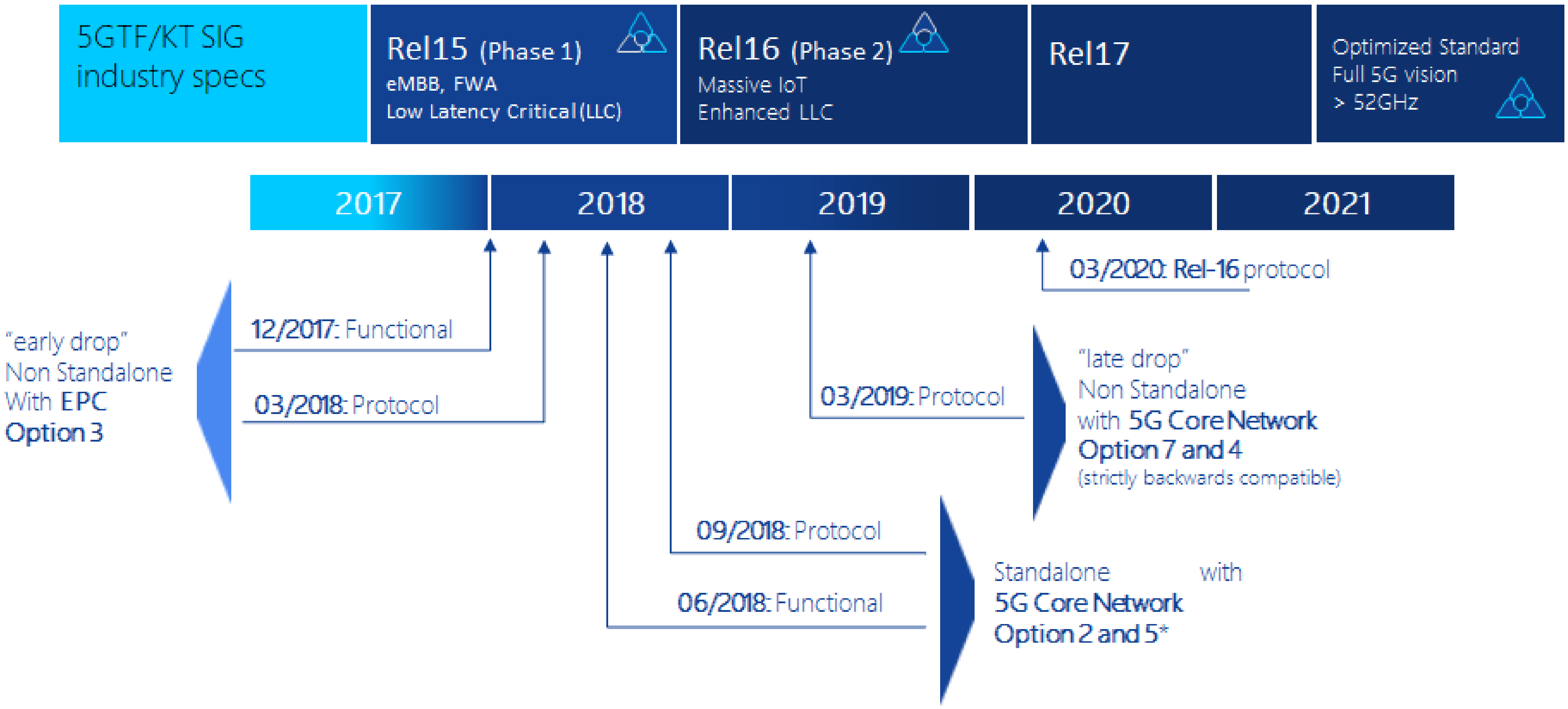
Frequency bands for 5G and 5G characteristics

- IMT-2020 (International Mobile Telecommunications) - common vision and requirements for 5G networks, issued by the ITU Radiocommunication Sector (ITU-R) in 2015
- 5G for Europe: An Action Plan, 2016
  - ✓ https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-588-EN-F1-1.PDF
- 3GPP R15, R16, R17
  - ✓ Release 15 (2018) – the first definition of NR (New Radio)
- Three key frequency bands for 5G in EU
  - ✓ 700 MHz, 3.4-3.8 GHz a 24.25-27.5 GHz
- Harmonization of frequency bands worldwide:
  - ✓ ITU, World Radio Conference 2019 (WRC-19), 3,400 delegates from around 165 Member States
  - ✓ Additional possible bands identified to enable standardized 5G (IMT-2020) deployments
  - ✓ 24.25-27.5 GHz, 37-43.5 GHz, 45.5-47 GHz, 47.2-48.2 and 66-71 GHz
- Frequency bands for 5G summary:
  - ✓ https://en.wikipedia.org/wiki/5G_NR_frequency_bands

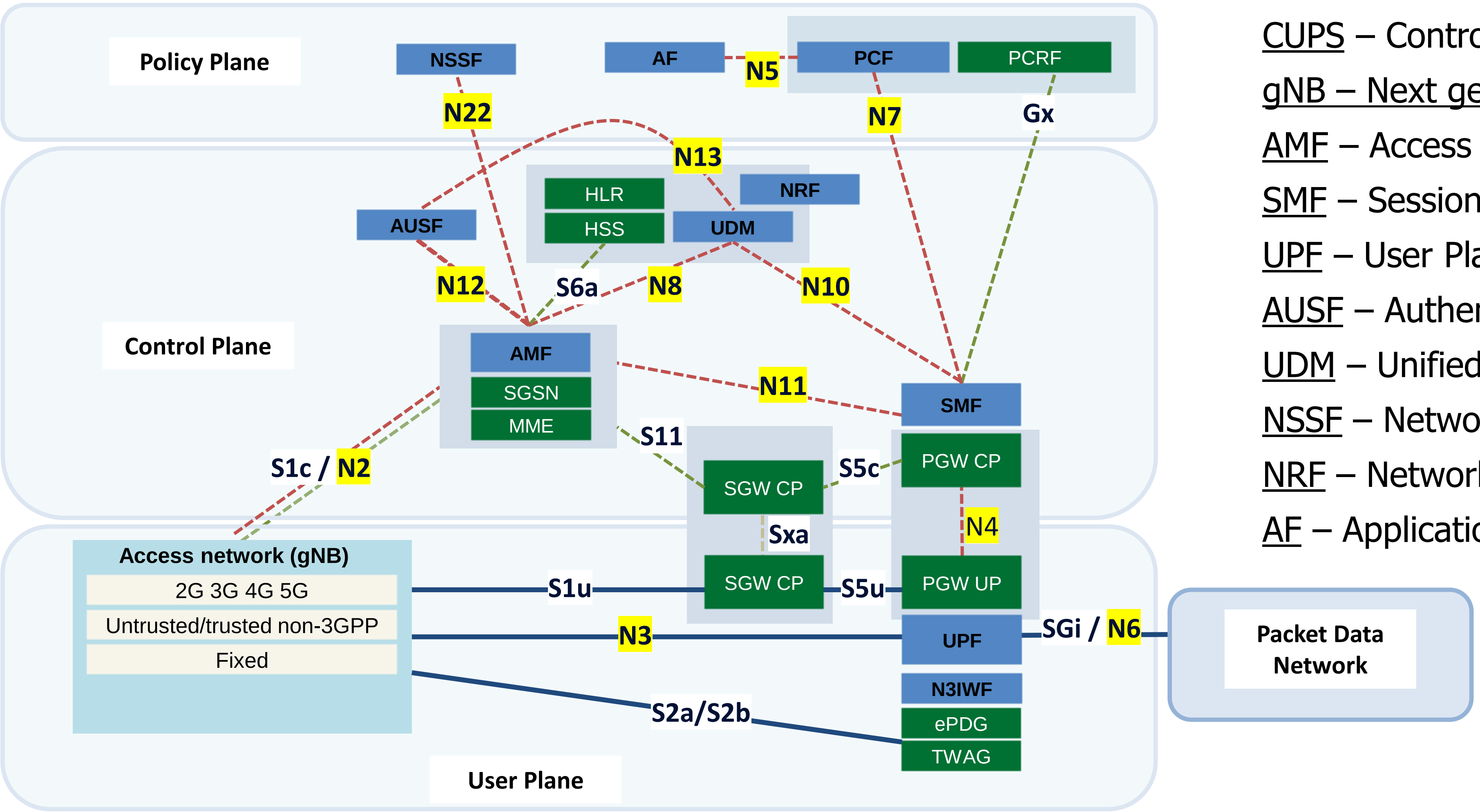
- 5G supports up to 1G speeds, allows new services with e2e KPIs

- Service-Based Architecture (SBA) - the control plane elements operate as VNFs (Virtualized Network Functions). Communication between VNFs is based on RESTful based API exchange, allowing a given VNF to offer “services” to other VNFs

3GPP Standardization



4G and 5G core functions with CUPS architecture



<u>CUPS</u> – Control and User Plane Separation

<u>gNB – Next generation NodeB</u>

<u>AMF</u> – Access and Mobility Function

<u>SMF</u> – Session Management Function

<u>UPF</u> – User Plane Function

<u>AUSF</u> – Authentication Server Function

<u>UDM</u> – Unified Data Management

<u>NSSF</u> – Network Slice Selection Function

<u>NRF</u> – Network Repository Function

<u>AF</u> – Application Function

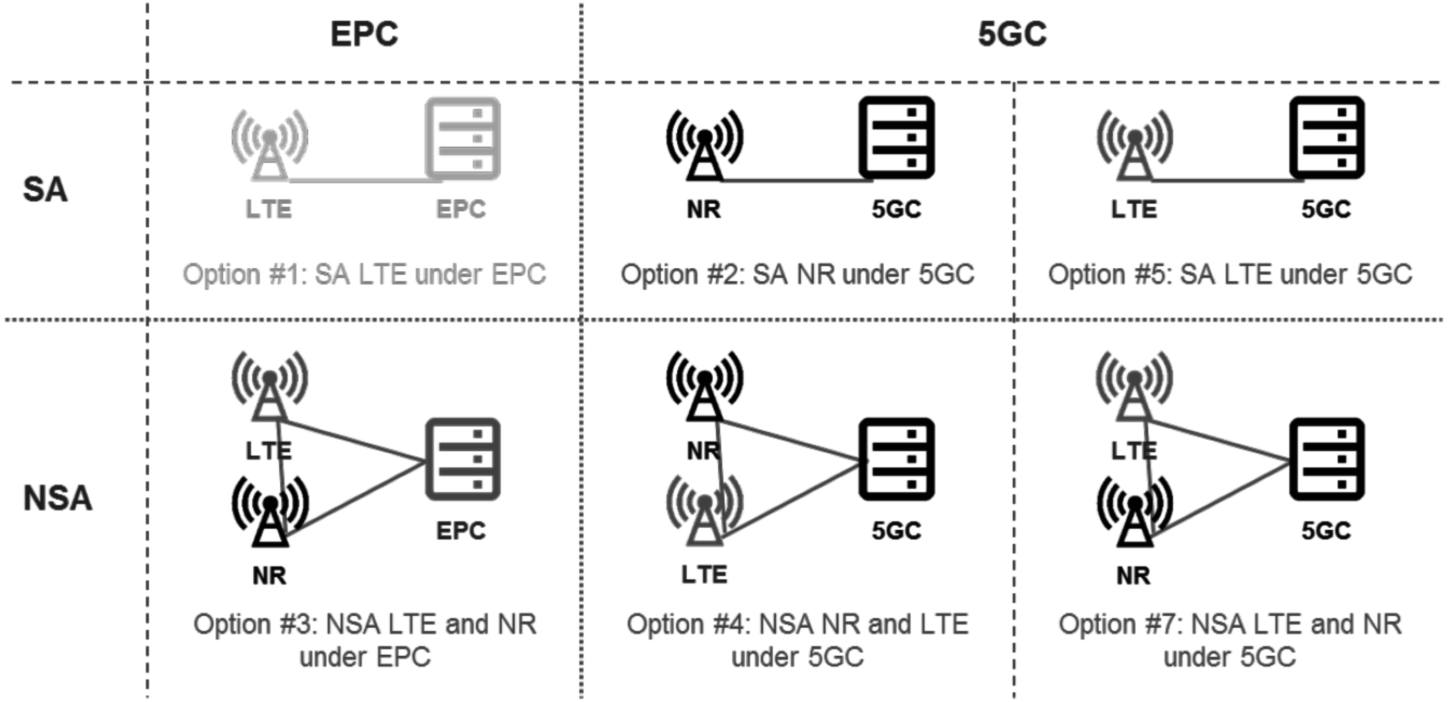
CUPS is essential to 5G networks because it allows operators to separate the evolved packet core (EPC) into a control plane that can sit in a centralized location and for the user plane to be placed closer to the application it is supporting. Also, it allows flexible scaling according to the signalling and traffic needs, control plane and data plane can be re-dimensioned in separate steps.

5G Network Functions

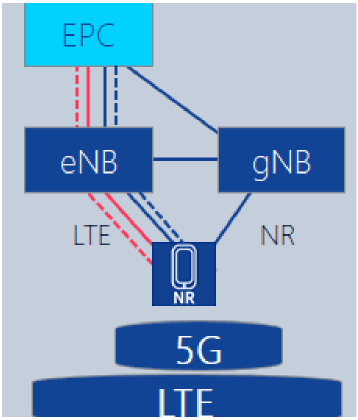
- AMF – Access and Mobility Function - Unique 5GC (5G Core) entity handling signaling, access control and mobility management
- SMF – Session Management Function - Unique 5GC entity handling session management for all access types, control plane for UPF
- UPF – User Plane Function - No SGW convergence point, no predefined roles (SGW-u, PGW-u), flexible entity embracing functions per need, use case or slice
- UDM – Unified Data Management – the database that stores subscription-related data
- AUSF – Authentication Server Function - receives authentication requests from the AMF and interacts with UDM to obtain information about UE and subscriber
- NSSF – Network Slice Selection Function - can be used by the AMF to assist with the selection of the Network Slice instances, NSSF may be used to allocate an appropriate AMF if the current AMF is not able to support all network slice instances for a given UE and the service requested
- NRF – Network Repository Function – allows 5G to nodes discover each other, maintains updated records/profiles of services provided by NFs (network functions)
- AF – Application Function - establishes the quality of service and potentially some charging aspects for a service, kind of controller for a specific application

Challenges in deploying a 5G network

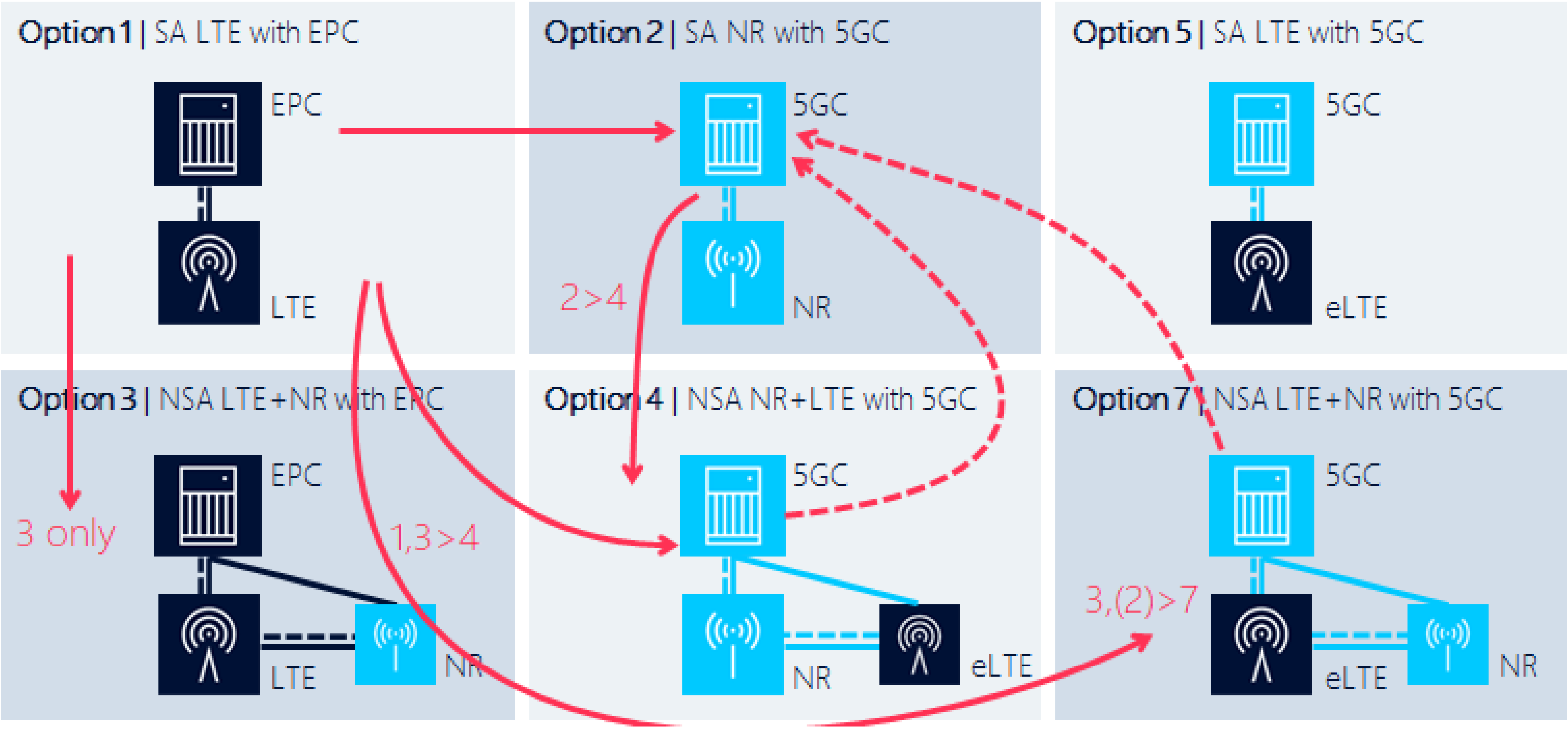
- In reality, subscribers may be slow to migrate since they have to invest in 5G-capable handsets
- Heavy investments into the new architecture, they may wait for 5G spectrum auctions, they may want to offer 5G services on 4G licensed spectrum
- 5G gives a flexibility in deployment scenarios, can be combined with 4G technology
  - Standalone (SA) option: uses only one radio access technology, either LTE radio or 5G NR. Both control and user planes go through the same RAN element
  - Non-Standalone (NSA): multiple radio access technologies are combined, control plane goes through what's called the master node whereas data plane is split across the master node and a secondary node



NSA Option 3x:
- LTE as a primary network, including all signaling
- eNB decides, which traffic can be moved to NR
- Secondary (NR) may split one or more of these bearers and forward to Master (LTE)



Network evolution – migration paths

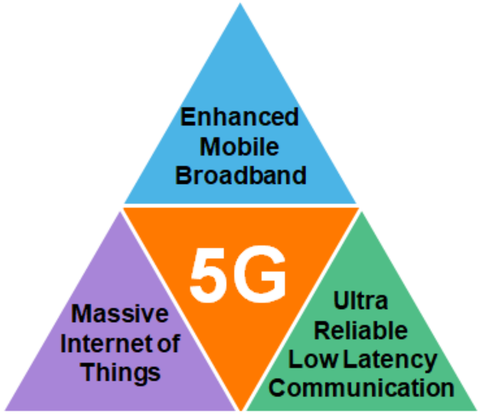


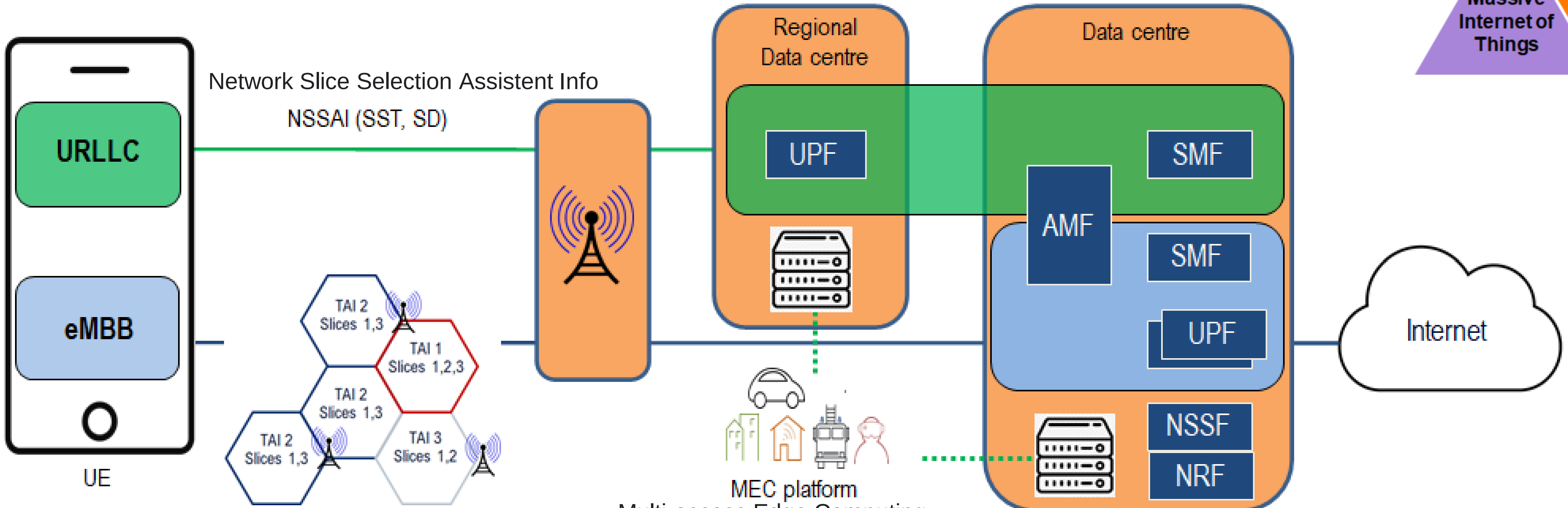
Nokia

End to End slicing for 5G

Network slicing - allows to virtualize the physical infrastructure and create multiple virtual networks for various services

eMBB (enhanced Mobile Brodband), URLLC (Ultra Reliable Low Latency Communication),
mIOT (mobile IOT), user defined slices
8 slices per UE
RAN & Transport – routing and prioritization per slice
Possibility to allocate dedicated resources per slice

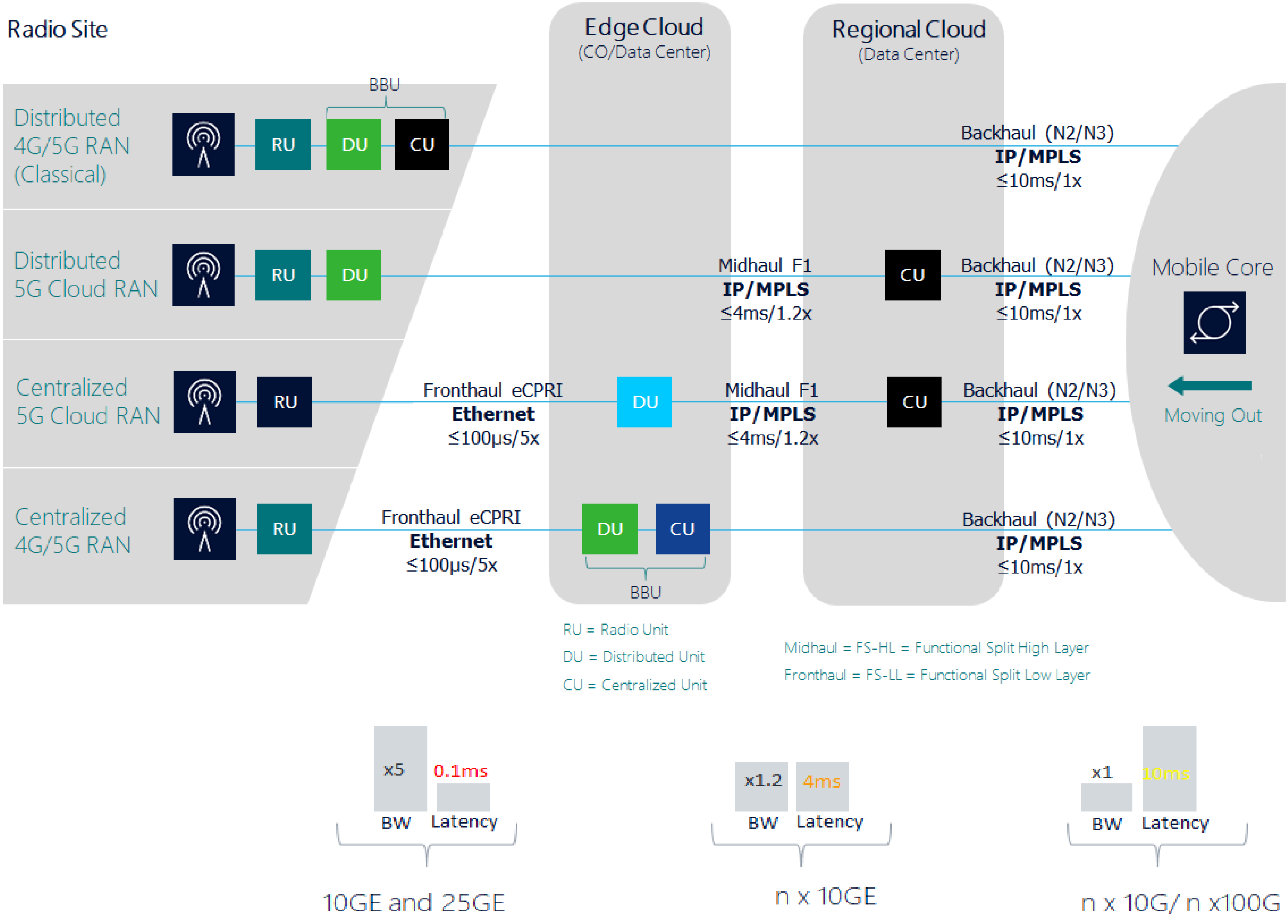


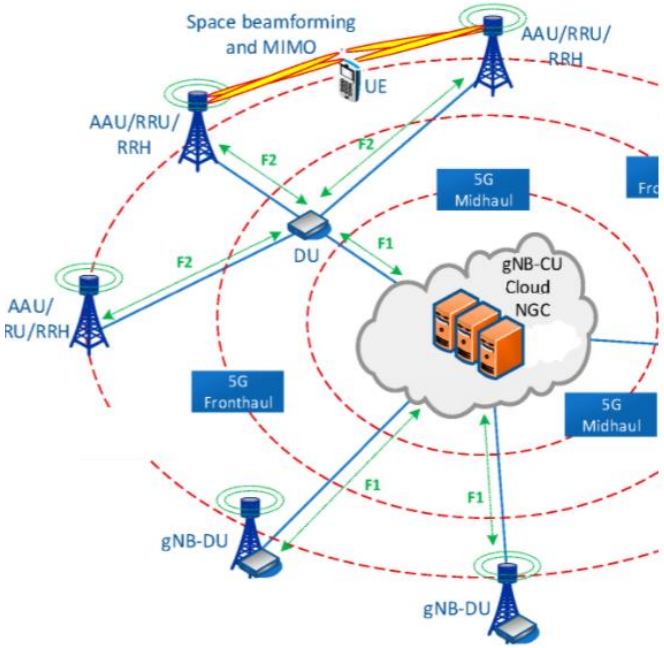


Use cases - different network requirements

	Use-Case				Delivered by Network Slice				
	Application Category	Examples	Cost Sensitivity	Deploy-ment	Throughput (bps)		Latency (RTT)		Reliability
					UL	DL	E2E Appl.	Network	
Consumers: • Mobile Broadband • Events • Entertainment • SoHo/Homes	Mobile Broadband	· Smartphones in dense urban · Corporate mobile office	Medium	mass	10-50M	100-300M	50-200ms	15-25ms	Medium - High
	Fixed Wireless Access	· 5G for residential homes · Wireless SOHO/VPN	High	targeted	100-200M	1-5G	150-200ms	1-20ms	High
	Event experience	· Immersive VR360 · AR gaming	Medium	targeted	1-5G	1-100M	5-50ms	1-5ms	Medium - High
	In -Vehicel Entertainment	· Private cars · Public transport	Medium	mass	1k-1M	5-100M	150-200ms	1-20ms	Medium-High
Industries: • Manufacturing • Seaports, Mining • Agriculture • Utilities • Smart Cities	Critical automation	· Collaborative robots/drones · Electrical grid tele-protection	Low	mass	1-10M	1M	5-50ms	1-5ms	High/Very High
	Tele-operation	· Video-based remote control · Video w/haptic remote cntrl	Medium	targeted	1-10M	1M	50-150ms	1-25ms	High/Very High
	Highly interactive AR	· Co-present Mixed Reality · 360° volumetric video AR/MR	Medium	targeted	1-100M	5-100M	50-100ms	1-10ms	Medium
	Mass sensor arrays	· Agriculture field sensors · Smart city sensors & meters	Very High	mass	1k-1M	1k-1M	1-2s	200-500ms	Medium-Low

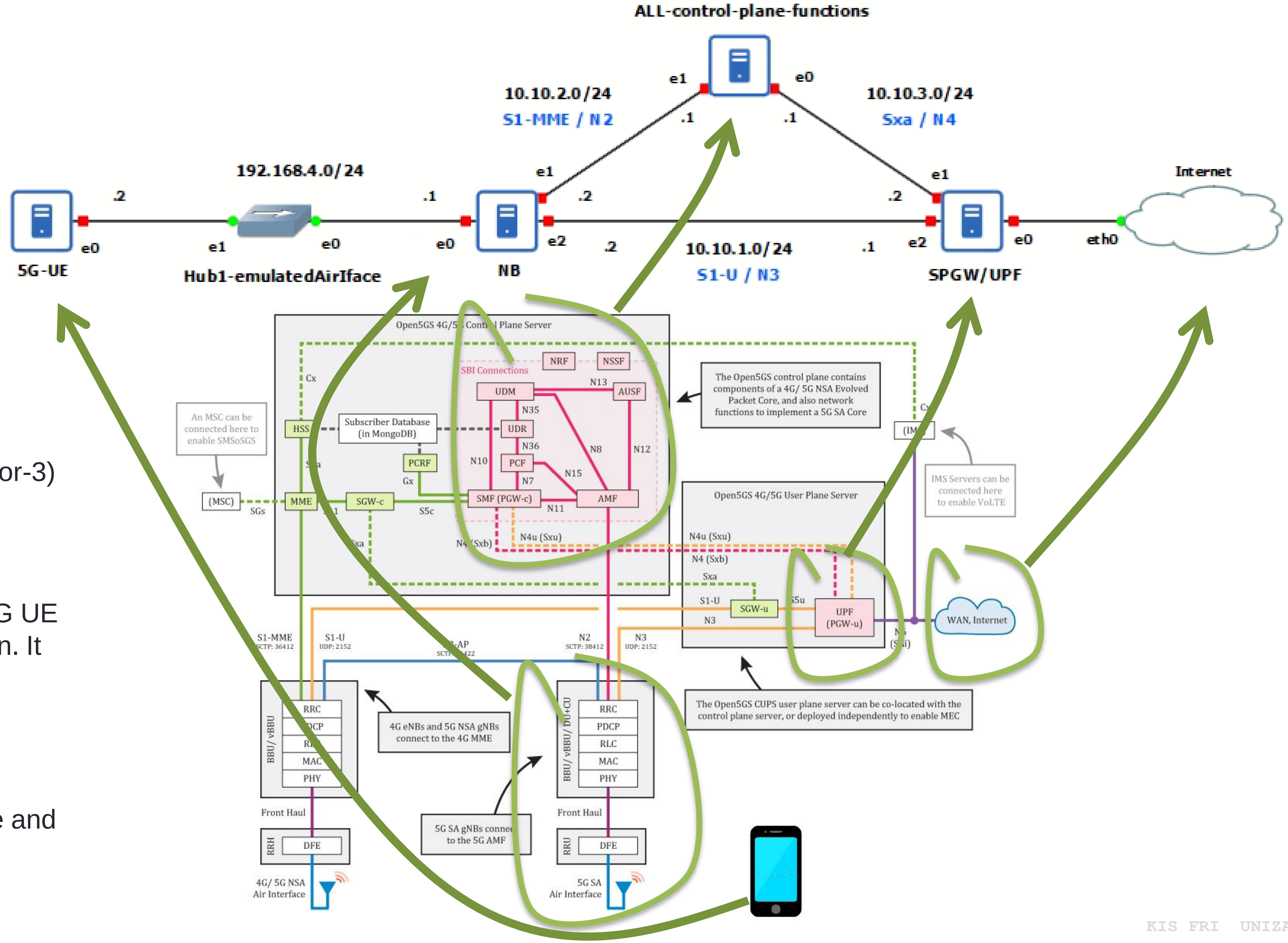
5G RAN Architecture Options





Virtualized NR/LTE infrastructure

Open Source based virtualized NR/LTE infrastructure



GNS3 (Graphical Network Simulator-3) software allows you to emulate complex network designs

UERANSIM is the open-source 5G UE and RAN (gNodeB) implementation. It can be considered as a 5G mobile phone and a base station

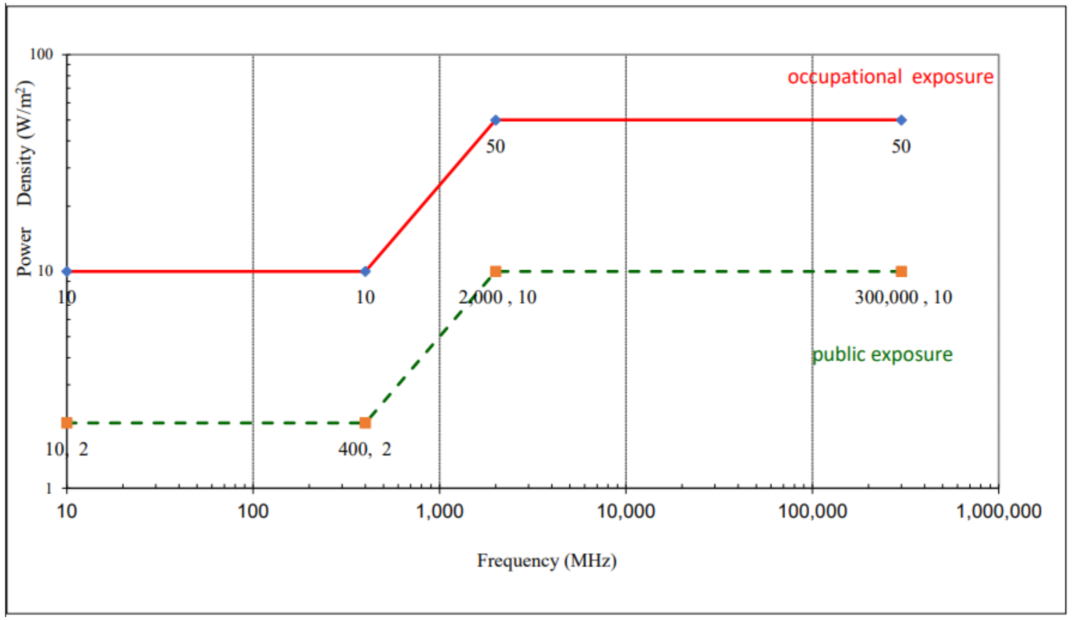
Open5GS is a C-language Open Source implementation of 5G Core and EPC

Exposure limits

Power-density exposure limits above 10MHz from 1998

- ICNIRP - International Commission for Non-Ionizing Radiation Protection, independent non-profit organization, provides scientific advice and guidance on the health and environmental effects of non-ionizing radiation (NIR) to protect people and the environment
- Assumption - electromagnetic radiation has only thermal effects
- Measurements are averaged over a 6 minute interval, not peak values
- The problem of high frequency modulated pulse signal

Frekvencia	900Mhz	1800 MHz	2100 MHz
	W/m2	W/m2	W/m2
EU	4.5	9	10
BE	-	-	-
Bulharsko	0.1	0.1	0.1
Cyprus	4.5	9	10
Česká Republika	4.5	9	10
Dánsko	-	-	-
Estónsko	4.5	9	10
Fínsko	4.5	9	10
Francúzsko	4.5	9	10
Grécko	2.7	5.4	6
Chorvátsko	0.72	1.4	1.7
Írsko	4.5	9	10
Litva	0.45	0.9	1
Lotyšsko	-	-	-
Luxembursko	4.5	9	10
Maďarsko	4.5	9	10
Malta	4.5	9	10
Nemecko	4.5	9	10
Holandsko	-	-	-
Poľsko	4.5	9	10
Portugalsko	4.5	9	10
Rakúsko	4.5	9	10
Rumunsko	4.5	9	10
Slovensko	4.5	9	10
Slovinsko	0.45	0.9	1
Španielsko	4.5	9	10
Švédsko	4.5	9	10
Taliansko	0.1	0.1	0.1
Veľká Británia	4.5	9	10



EU Council Recommendations (EU 1999/519 / EC) as a basis for national legislation

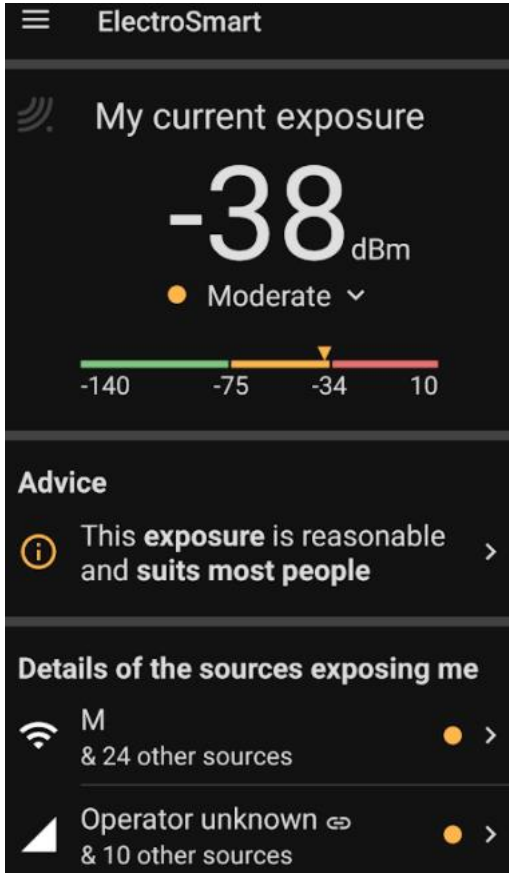
New proposed limits are at the range of 1-10 µW/m2, based on health risks

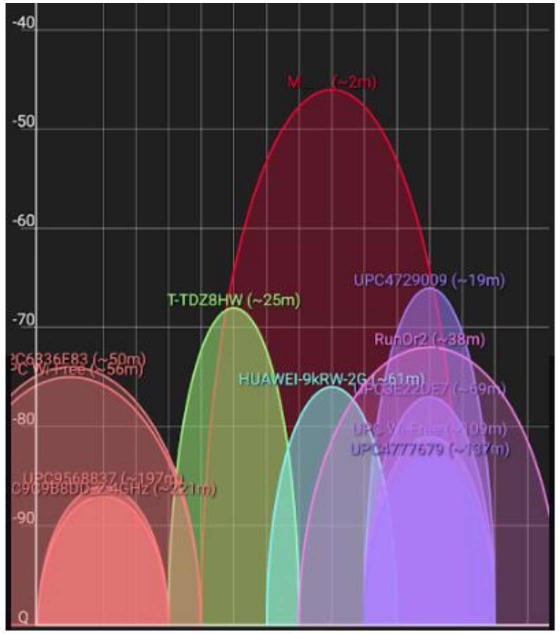
Exposure levels from sources and recommended biological limits

	(MHz)	Vyžiarený výkon	30 cm	1 m	5 m	20 m	300 m	5 km
Letecký radar	2700 - 2900	100 - 1000 kW					900k	3k
FM rádio	88 - 108	10 W - 100 kW					90k	300
DVB-T vysielač	470 - 790	10 W - 50 kW					45k	150
2G 3G 4G	700 - 3700	2 - 15 kW				400k - 3M	2k - 14k	6 - 50
Mikrovlnná rúra	2450	1 W	750k	75k	3k	200		
2G Mobilný telefón	900	2.5 mW - 2 W	2k - 1.6M	200 - 160k	8 - 6 300	0,5 - 400		
4G mobilný telefón	800/1700/2500	100 nW - 200 mW	0.1 - 160k	0.01 - 16k	0 - 630			
WiFi router / PC	2400	100 mW	80k	8k	320			
	5600				630			

1M µW	1000 mW	30 dBm
100k µW	100 mW	20 dBm
10k µW	10 mW	10 dBm
1k µW	1 mW	0 dBm
100 µW	0.1 mW	-10 dBm
10 µW	0.01 mW	-20 dBm
1 µW	0.001 mW	-30 dBm

EUROPAEM EMF 2016	Denná expozícia (µW/m²)	Nočná expozícia (µW/m²)
Analógový rozhlas (FM)	10 000	1 000
Komunikačný rádiový systém (TETRA)	1 000	100
Digitálna TV (DVB-T)	1 000	100
Základňová stanica GSM (2G)	100	10
Základňová stanica UMTS (3G)	100	10
Základňová stanica LTE (4G)	100	10
Bezdrôtový telefón, detská pestúnka (DECT)	100	10
GSM (2G) telefón / modem (8.33 Hz impulzy)	10	1
Digitálny rozhlas DAB+ (10.4 Hz impulzy)	10	1
Wi-Fi 2.4 / 5 GHz router (9.76 Hz impulzy)	10	1





Building biology evaluation guideline [µW/m²]

Smernica stavebnej biológie	Bez anomálie	Ľahká anomália	Silná anomália	Extrémna anomália
Intenzita pola E	< 0.006	0.006 - 0.06	0.06 - 0.6	> 0.6
Hustota radiačného toku S	< 0.1	0.1 - 10	10 - 1000	> 1000

Ďakujem za pozornosť.

roman dot kaloc at uniza dot sk

Vytvorené v rámci projektu KEGA 026TUKE-4/2021