

# **Cellular Networks**

Mobile cellular networks

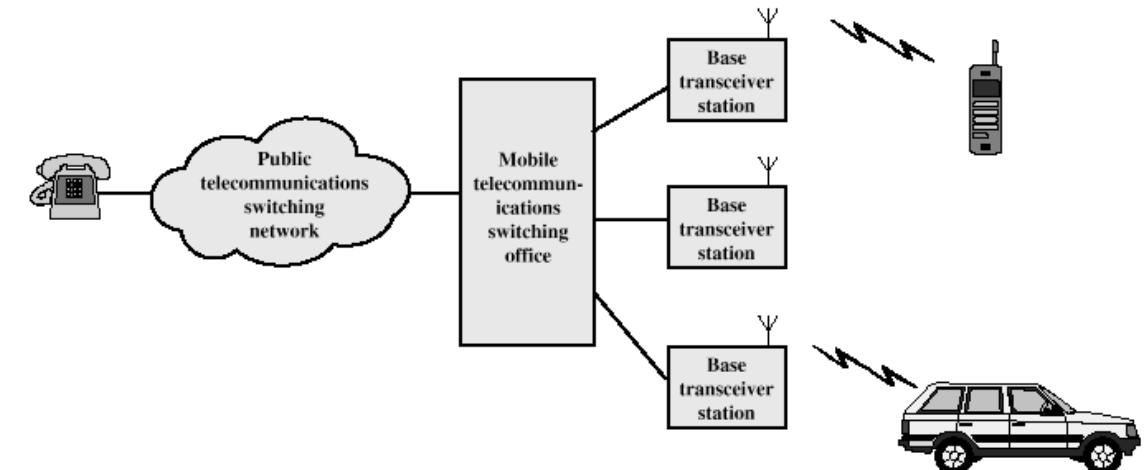
GSM to 5G

# Wireless CELLULAR network

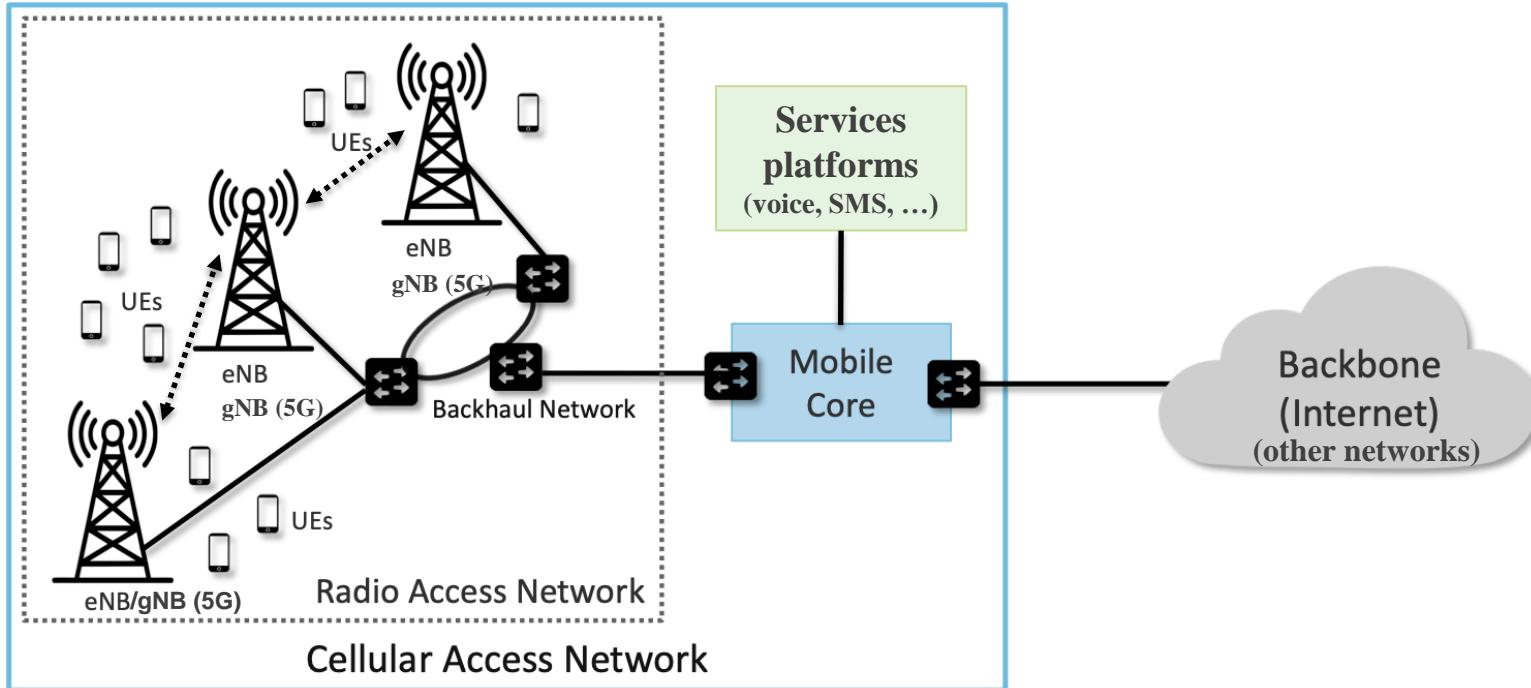
- Single hop widespread wireless connectivity to the wired world
  - Usually space divided into cells and Mobile Terminals (MTs) assigned to a cell
  - A Base Station (BS) is responsible for communicating with MTs in its cell
    - Communications: a voice call or a data session
  - Handoff/handover (HO) operations occur when a MT moves to a new base station, while busy on a call
  - Highly supported by a fixed (wired) transport network

- Cell size:

- Highly variable
- Technology and frequency dependent
- Varies with expected number of users



# Generic cellular network architecture



Only the UE to e/gNB interface is radio based

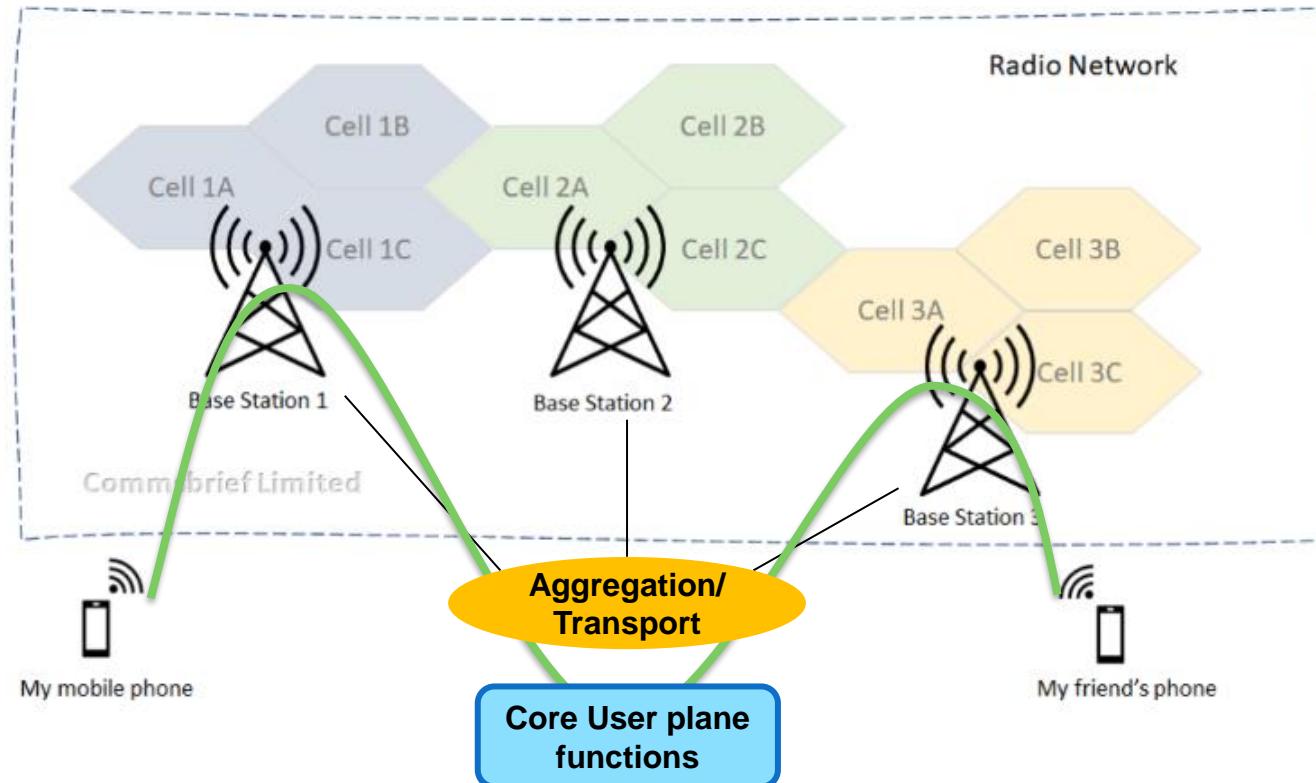
'Mobile networks' heavily supported on the fixed net (mostly fibber)

Service platforms are shared with the fixed access network (fibber and copper)

Reserved, dedicated, radio spectrum plays a central role in the success of PLMN (Public Land Mobile Networks)

# Cellular System Generic

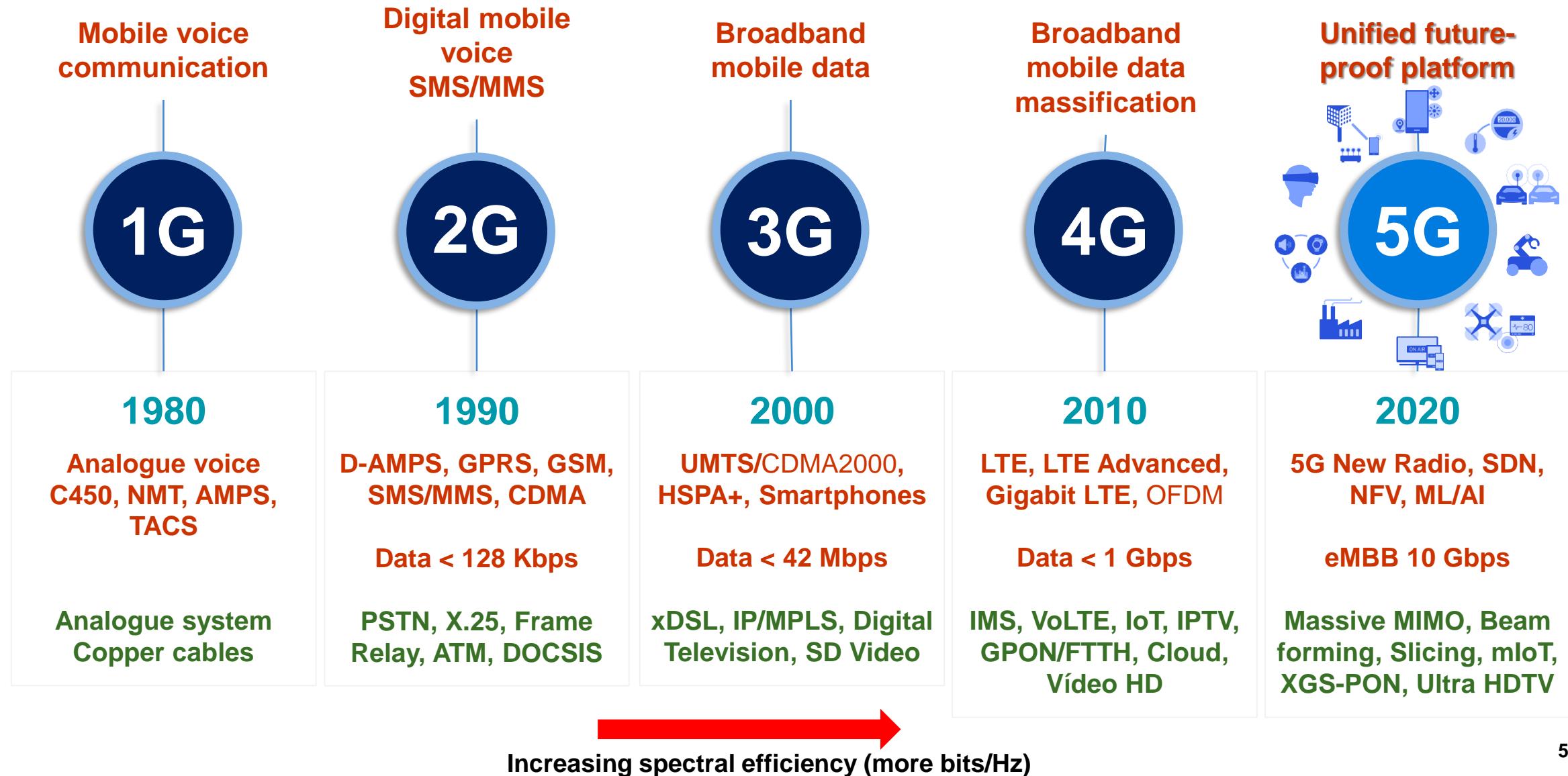
Garante que há sinal para todos os lados



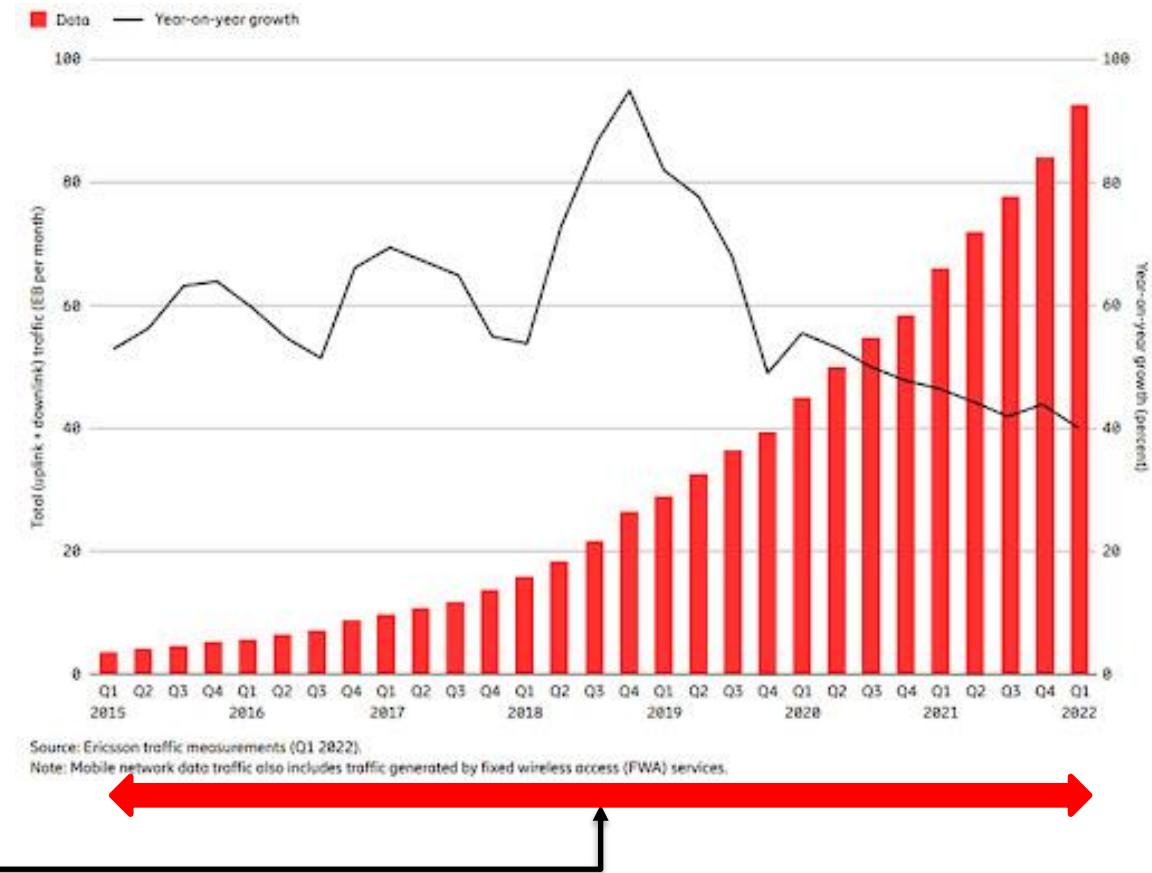
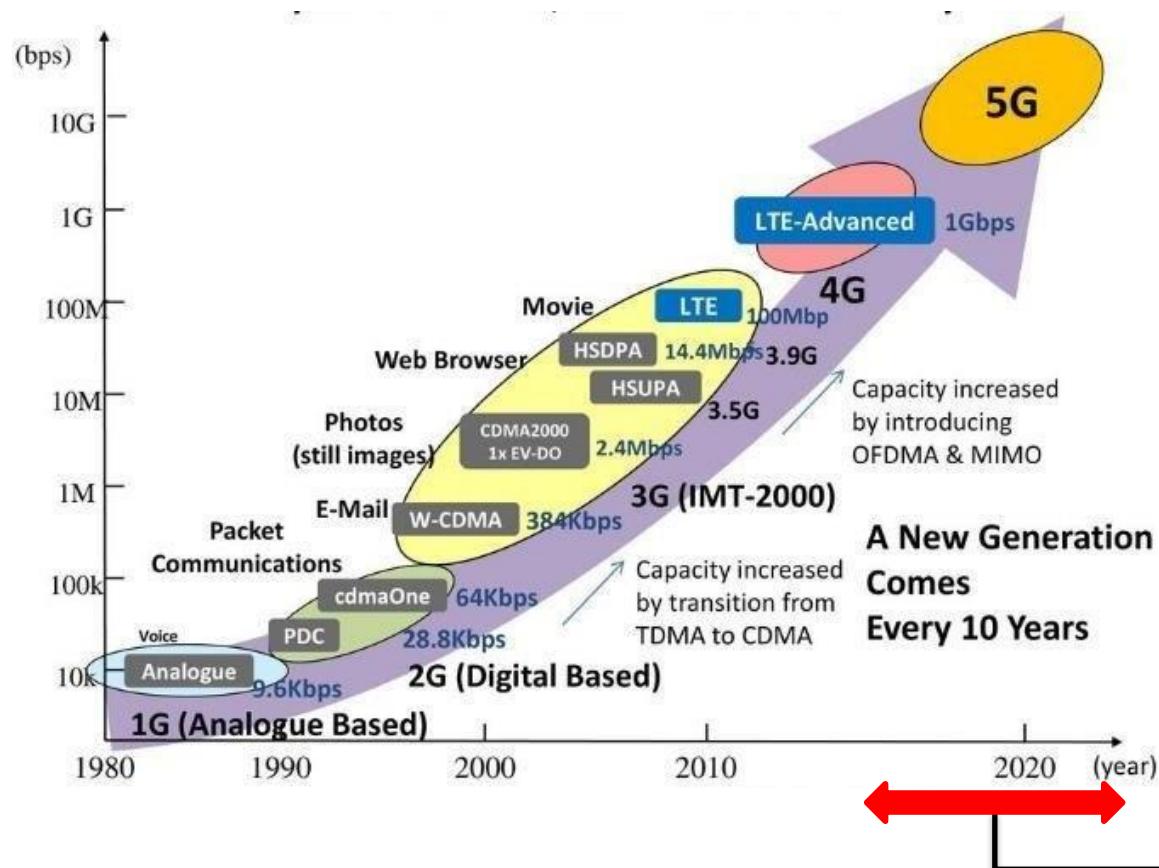
<https://commsbrief.com/what-are-cells-in-mobile-communications/>

# Technological waves (Generations)

Adaptado de: Qualcomm "What's in the future of 5G?"



# Technologies and usage evolution



# Wireless cellular network

In Telco terminology, a ***Public Land Mobile Network*** (**PLMN**) is a combination of wireless communication services offered by a specific operator in a specific country

A PLMN typically consists of several cellular technologies like **GSM/2G**, **UMTS/3G**, **LTE/4G** and **5G**, offered by a single operator within a given country, often referred to as a cellular network

A PLMN is identified by a globally unique **PLMN code**, which consists of a **MCC (Mobile Country Code)** and **MNC (Mobile Network Code)**

|                 |                    |   |
|-----------------|--------------------|---|
| <b>Portugal</b> | <b>MCC:</b><br>268 | <b>MNC:</b><br>Vodafone: 01<br>NOS: 03<br>MEO: 06 |
|-----------------|--------------------|---|

<https://mcc-mnc.com/>

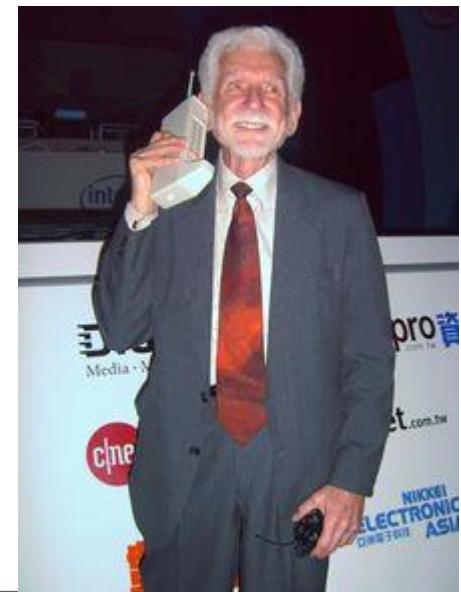
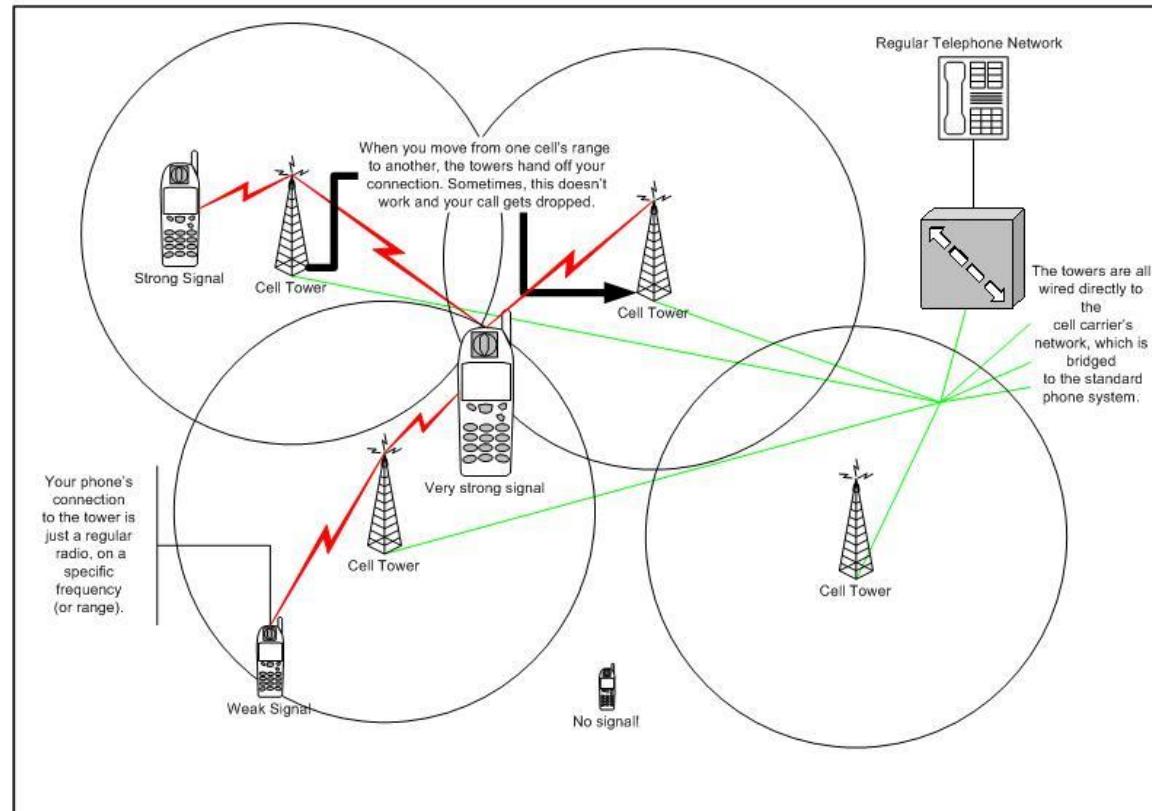
**1G**

**Mobile voice**

# First-Generation Analog

- Advanced Mobile Phone Service (AMPS)
  - In North America, two 25-MHz bands allocated to AMPS
    - One for transmission from base to mobile unit
    - One for transmission from mobile unit to base
  - Each band split in two to encourage competition
  - Frequency reuse exploited

<https://telephoneworld.org/cellular-phone-history/analog-cellular-amps-1g/>



**Martin Cooper**, American engineer who led the team that in 1972–73 built the first **mobile cell phone** and made the first cell phone call. He is widely regarded as the father of the cellular phone.

# 1G characterization

## Most popular 1G systems during 1980s

- Advanced Mobile Phone System (AMPS)
- Nordic Mobile Phone System (NMTS)
- Total Access Communication System (TACS)
- European Total Access Communication System (ETACS)

## Key features (technology) of 1G system

- Frequency 800 MHz and 900 MHz
- Bandwidth: 10 MHz (666 duplex channels with bandwidth of 30 KHz)
- Technology: Analogue switching
- Modulation: Frequency Modulation (FM)
- Mode of service: voice only
- Access technique: Frequency Division Multiple Access (FDMA)

## Disadvantages of 1G system

- Poor voice quality due to interference
- Poor battery life
- Large sized mobile phones (not convenient to carry)
- Less security (calls could be decoded using an FM demodulator)
- Limited number of users and cell coverage
- Roaming was not possible between similar systems

**2G**

**Global System for Mobile Communications  
(GSM)**

# 2<sup>nd</sup> Generation: GSM

- Defined by CEPT/ETSI
- Requirements in terms of:
  - Services      Portability, =PSTN
  - QoS            = PSTN
  - Security       Low cost cipher
  - RF Usage      Efficiency
  - Network       Numbering ITU-T, SS-7
  - Cost           Low

## Differences with the first Generation Systems

- Digital traffic channels
  - first-generation systems are almost purely analog; second-generation systems are digital
- Encryption
  - all second generation systems provide encryption to prevent eavesdropping
- Error detection and correction
  - second-generation digital traffic allows for detection and correction, giving clear voice reception
- Channel access
  - second-generation systems allow channels to be dynamically shared by a number of users

# Basic Architecture

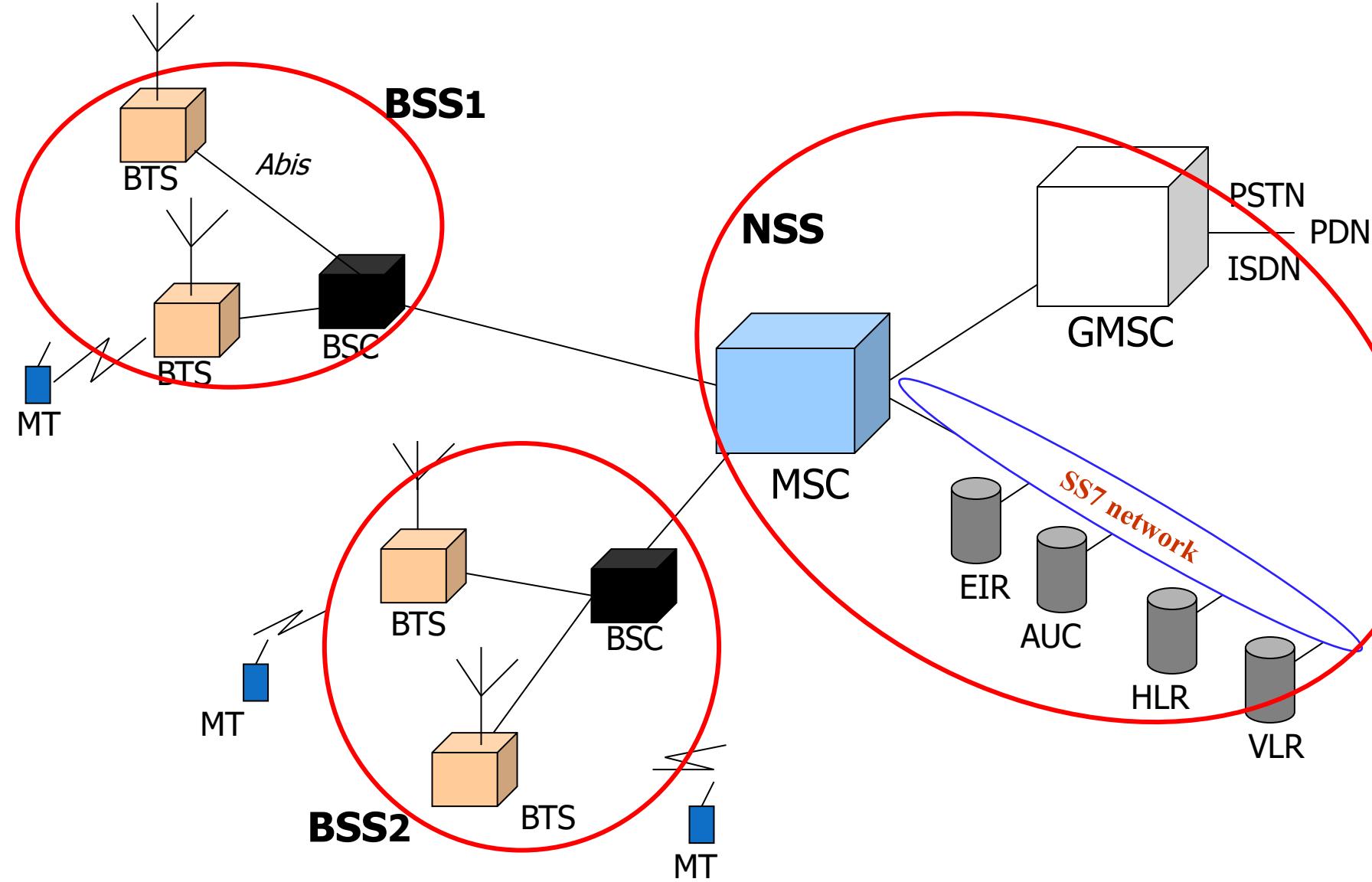
- Defines cells
- Defines a Mobile Terminal

Mobile Equipment + Subscriber Identity Module  
(etc...; e.g. International Mobile Station Equipment Identity (IMEI))
- Uses a Network Subsystem

MSC; HLR, VLR
- Uses a Radio Subsystem

BSS; BT<sub>ransceiver</sub>S, BSC<sub>ontroller</sub>
- Defines an Operation Support Subsystem (OSS)
- The Base Station Subsystem (BSS) is structured as **Base Station Controllers (BSC)** + **Base Transceiver Station (BTS )**
- BSCs are connected to the **Mobile Switching Center (MSC)** through physical lines
- MSCs are interconnected to each other
- There are MSCs connected to the public network (PSTN), the **Gateway Mobile Switching Center (GMSC)**.

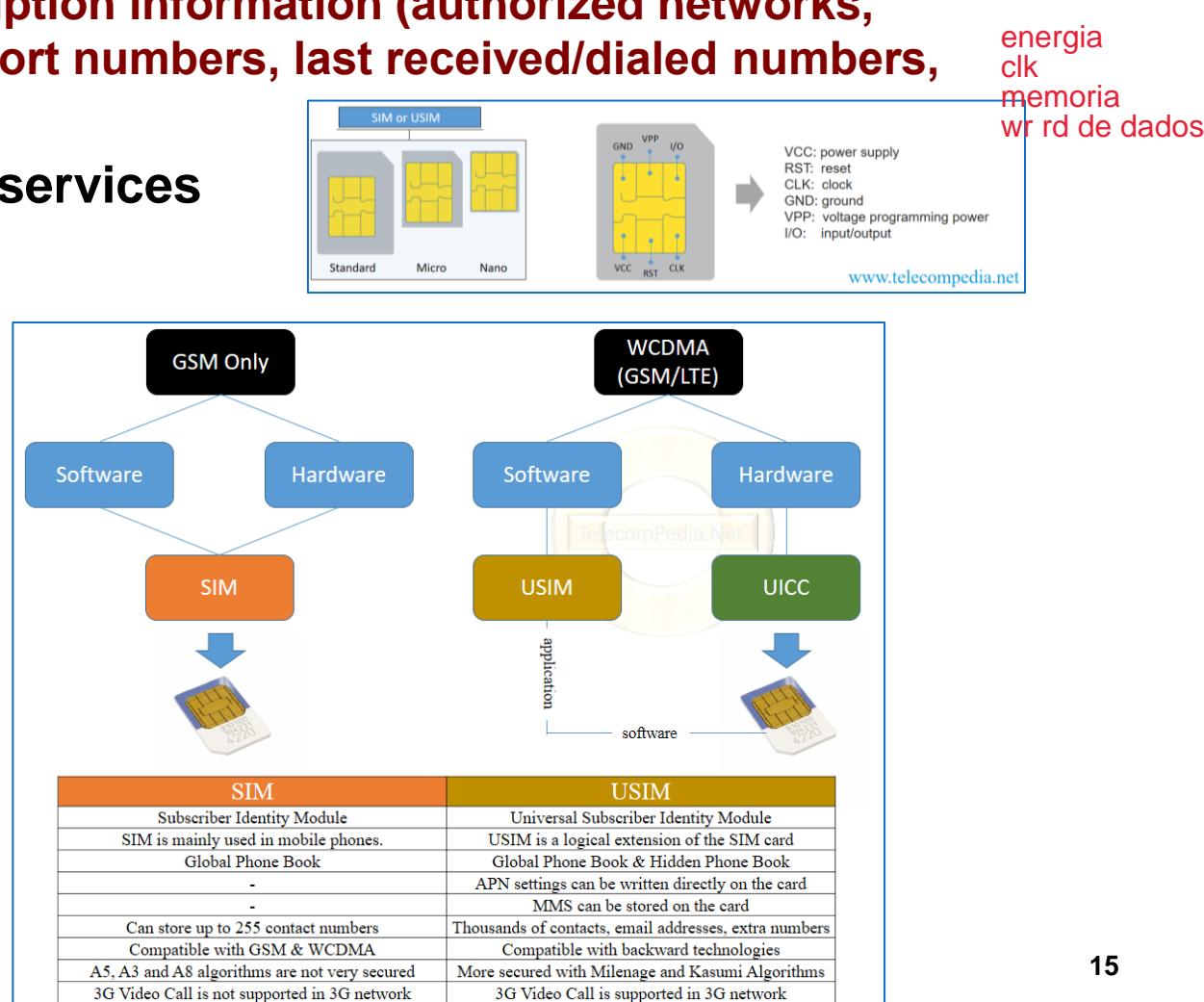
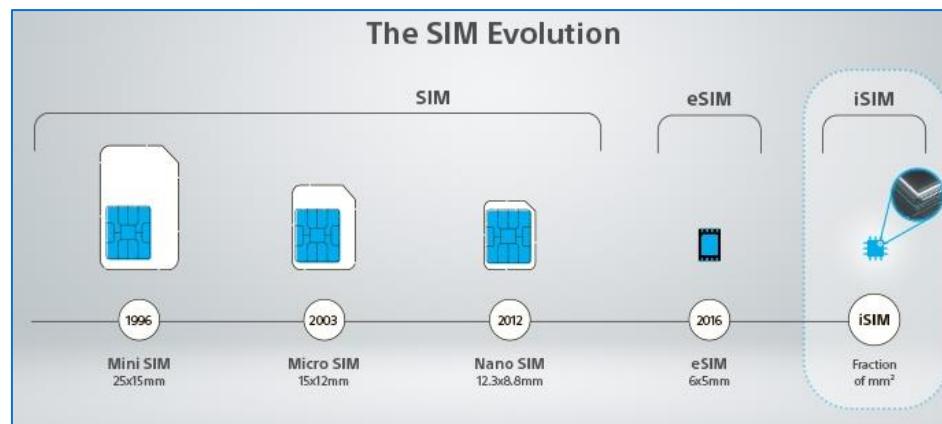
# GSM Architecture



AuC: Authentication Centre  
BSC: Base Station controller  
BSS: Base Station Sub-system  
BTS: Base Transceiver Station  
EIR: Equipment Identity Register  
GMSC: Gateway Mobile Switching Center  
HLR: Home Location Register  
ISDN: Integrated Services Digital Network  
MSC: Mobile Switching Centre  
MT: Mobile Terminal  
NSS: Network Switching Sub-system  
PDN: Packet Data Network  
PSTN: Public Switched Telephone Network  
SS7: Signaling System 7  
VLR: Visitor Location Register

# SIM: Subscriber Identity Module

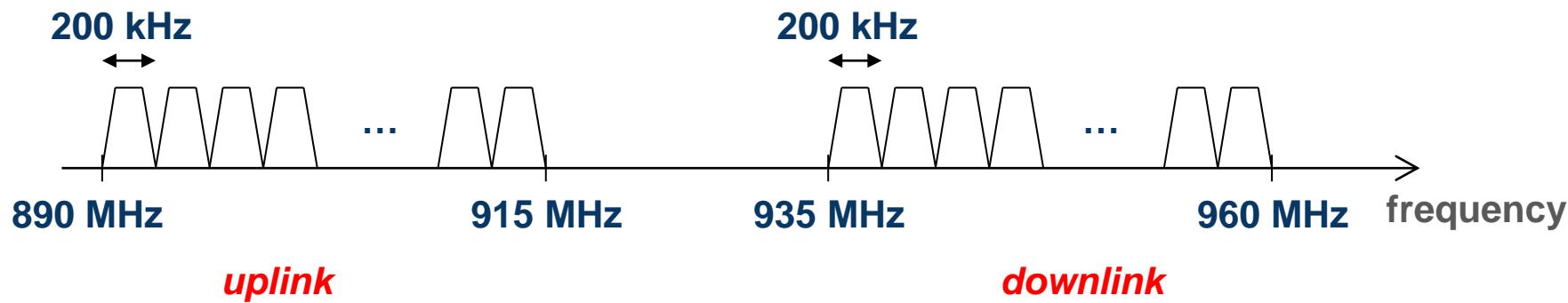
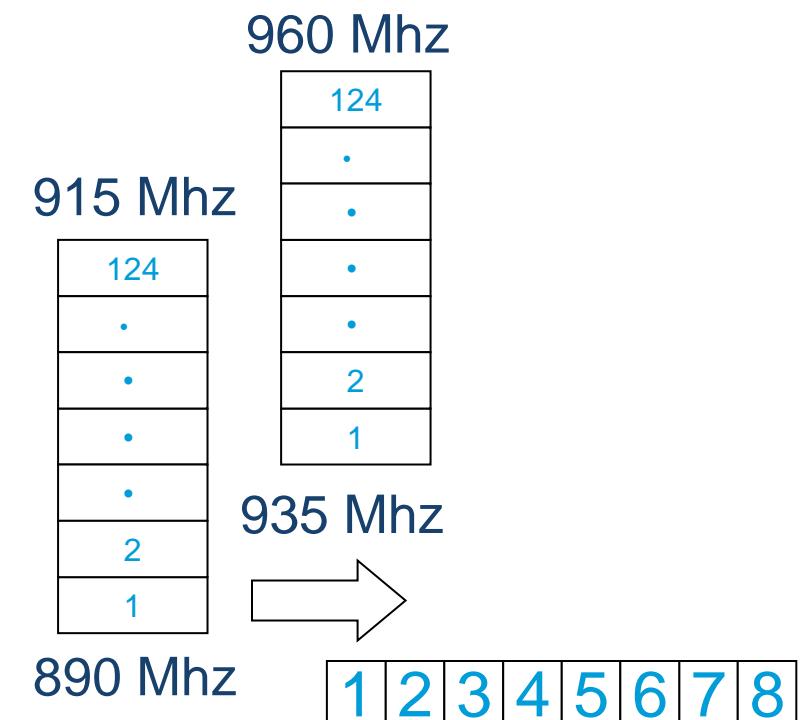
- Memory and microprocessor chip used in the mobile phones
- Informations:
  - subscriber identity, password (PIN), subscription information (authorized networks, call restrictions, ...), security algorithms, short numbers, last received/dialed numbers, last visited location area, ...
- SIM card + GSM terminal = access to GSM services
  - Hardware
- Evolution:
  - SIM (2G) → USIM (3G, software)
  - UICC (hardware)



# Air interface (Um) – channel allocation

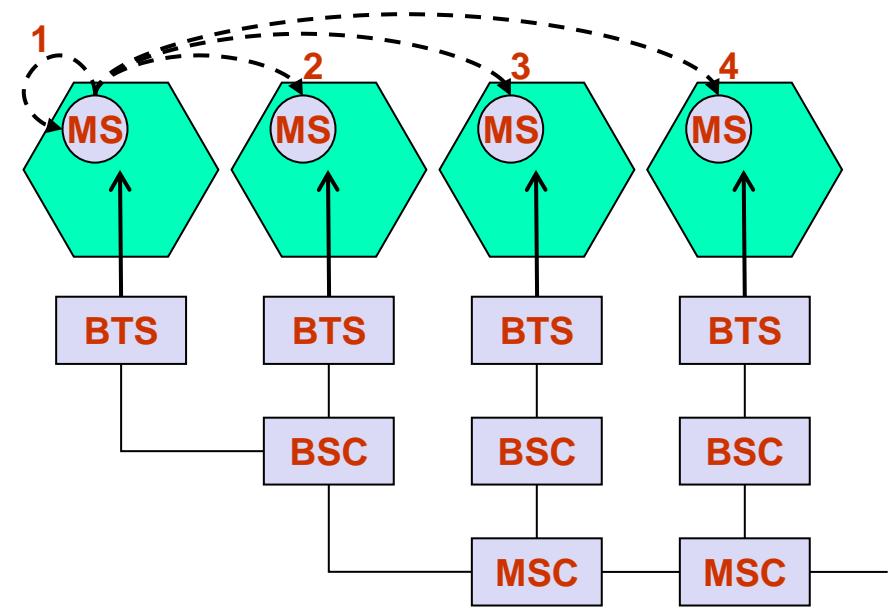
- **GSM uses:**

- **FDD (*Frequency Division Duplexing*) for duplexing**
- **TDMA (*Time Division Multiple Access*) with 8 time-slots for multiple access**
  - Three slots delay (up and down) → avoids simultaneous rx/tx
- **200 kHz frequency channels (124 in GSM 900) for each cell, 124 channels per band ( => maximum 8 users per channel)**



# Types of handover (GSM)

1. **Intra-cell**: from a channel to another within the same cell
2. **Inter-cell, Intra-BSC**: from a channel in one cell to a channel in another cell, both controlled by the same BSC
3. **Inter-BSC, Intra-MSC**: from a channel in one cell to a channel in another cell, controlled by different BSCs, under the same MSC control
4. **Inter-MSC**: from a channel in one cell to a channel in another cell connected to different MSCs



# Short Message Service - SMS

- Supports the transmission of messages up to 160<sup>1</sup> characters, between mobile terminals
- Messages are transmitted through the signalling channels
- Is used for a variety of applications:
  - text messages between users (very popular)
  - broadcast of information by the network operator (e.g. promotions)
  - broadcast of location-dependent information (e.g. local restaurants)
  - access to computing applications (e.g. home banking and e-mail)
  - configuration of mobile terminals over the air

<sup>1</sup> When using (7 bits/character); only 70 characters when using other codes (8 bits).

Twitter began as an SMS text-based service. This limited the original Tweet length to 140 characters (which was partly driven by the 160 character limit of SMS, with 20 characters reserved for commands and usernames). Over time as Twitter evolved, the maximum Tweet length grew to 280 characters - still short and brief, but enabling more expression.

**2.5G**

**General Packet Radio Service (GPRS)**

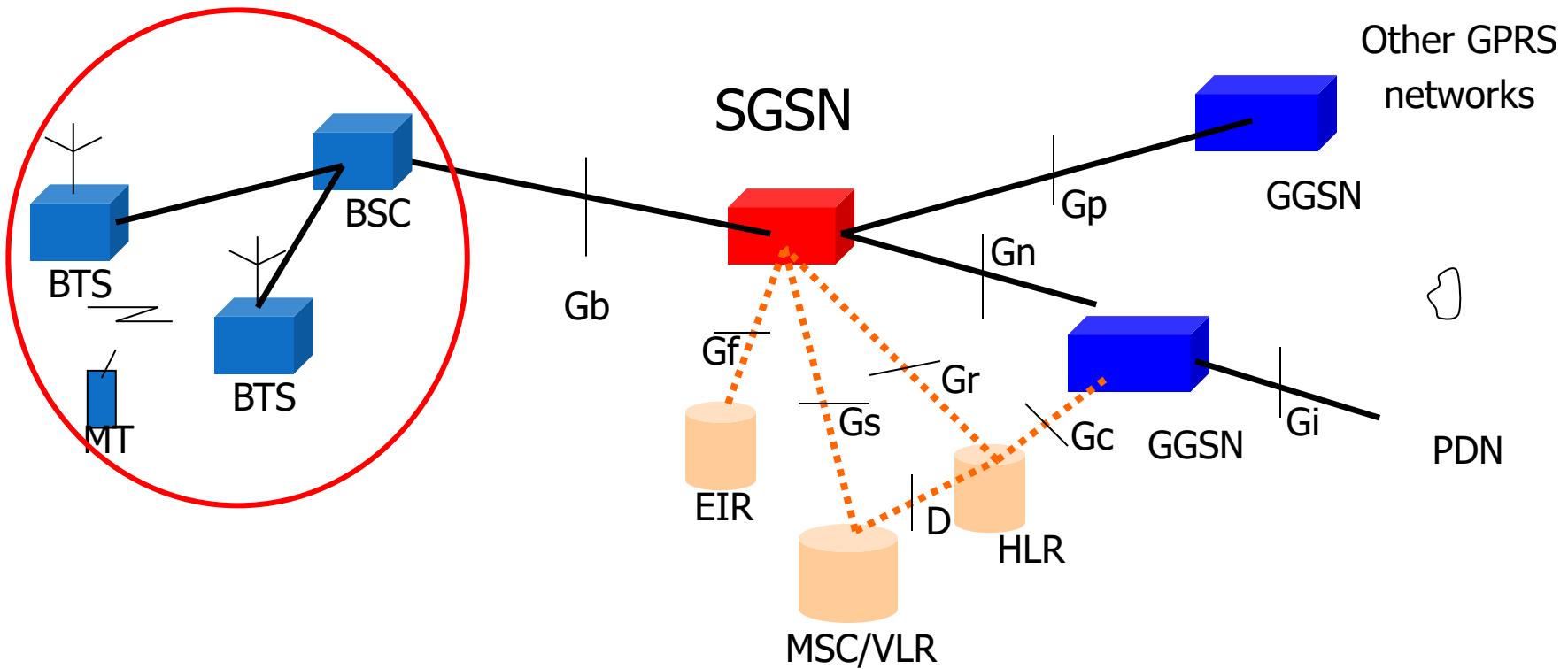
# GPRS

- GPRS: *General Packet Radio Service*
- Packet-oriented transport service, for data network connections (Internet)
  - Better transmission bit rates (max 150kbps)
  - Allows burst communications (“immediate”: connections in <1s)
  - New network applications
  - New billing mechanisms (user-oriented: by traffic, p.ex.)

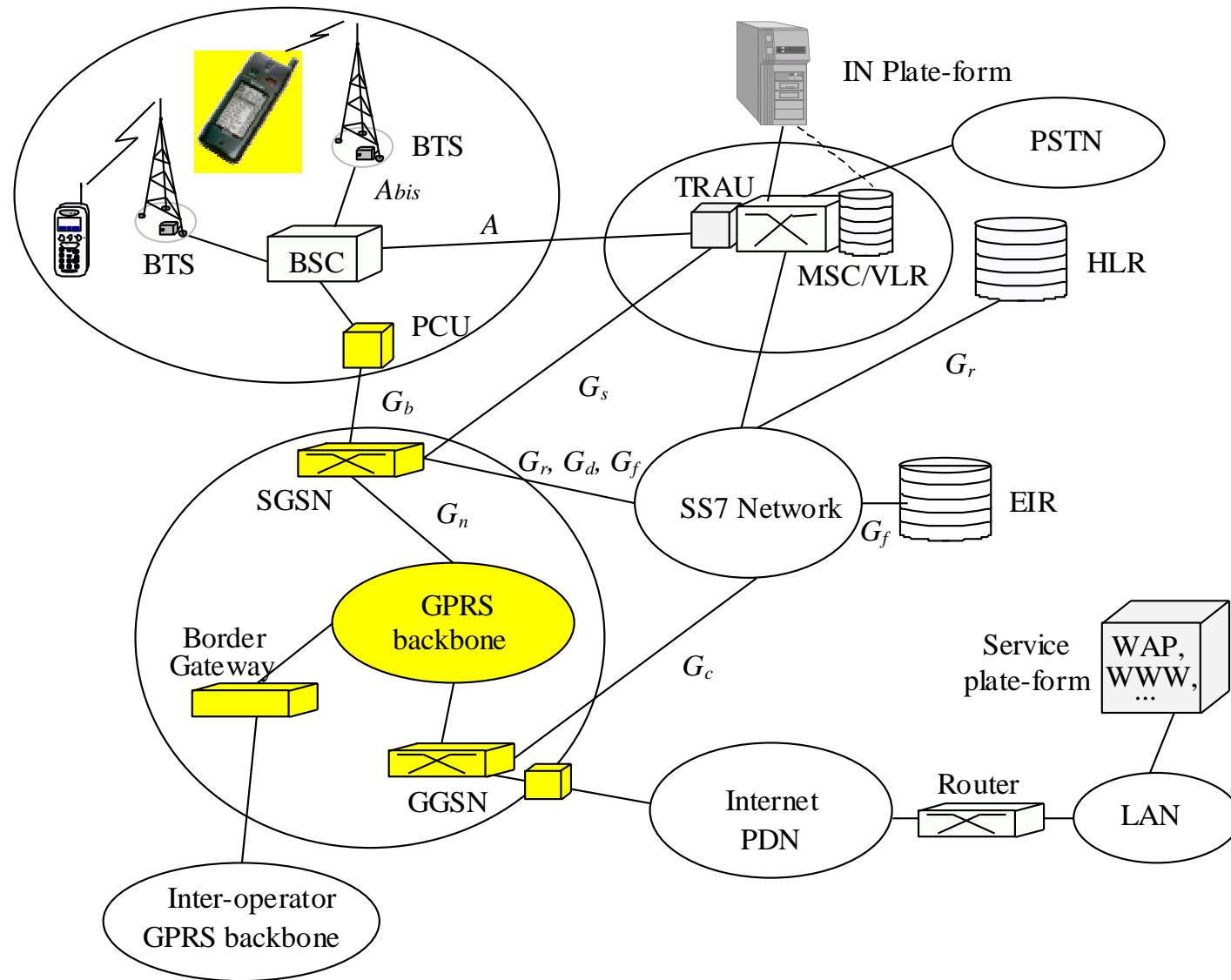
# GPRS Architecture

- New entities are defined
  - SGSN – serving GPRS support node
  - GGSN – gateway GPRS support node
  - Interfaces between entities GPRS, GSM, core and PSTN
- Transmission plane
  - Data packets are transmitted by a tunnel mechanism
- Control plane
  - GTP: a protocol for tunnel management (create, remove, etc..)
- Radio interface
  - Changed the logical channels and how they are managed
  - Remains the concept of “master-slave”

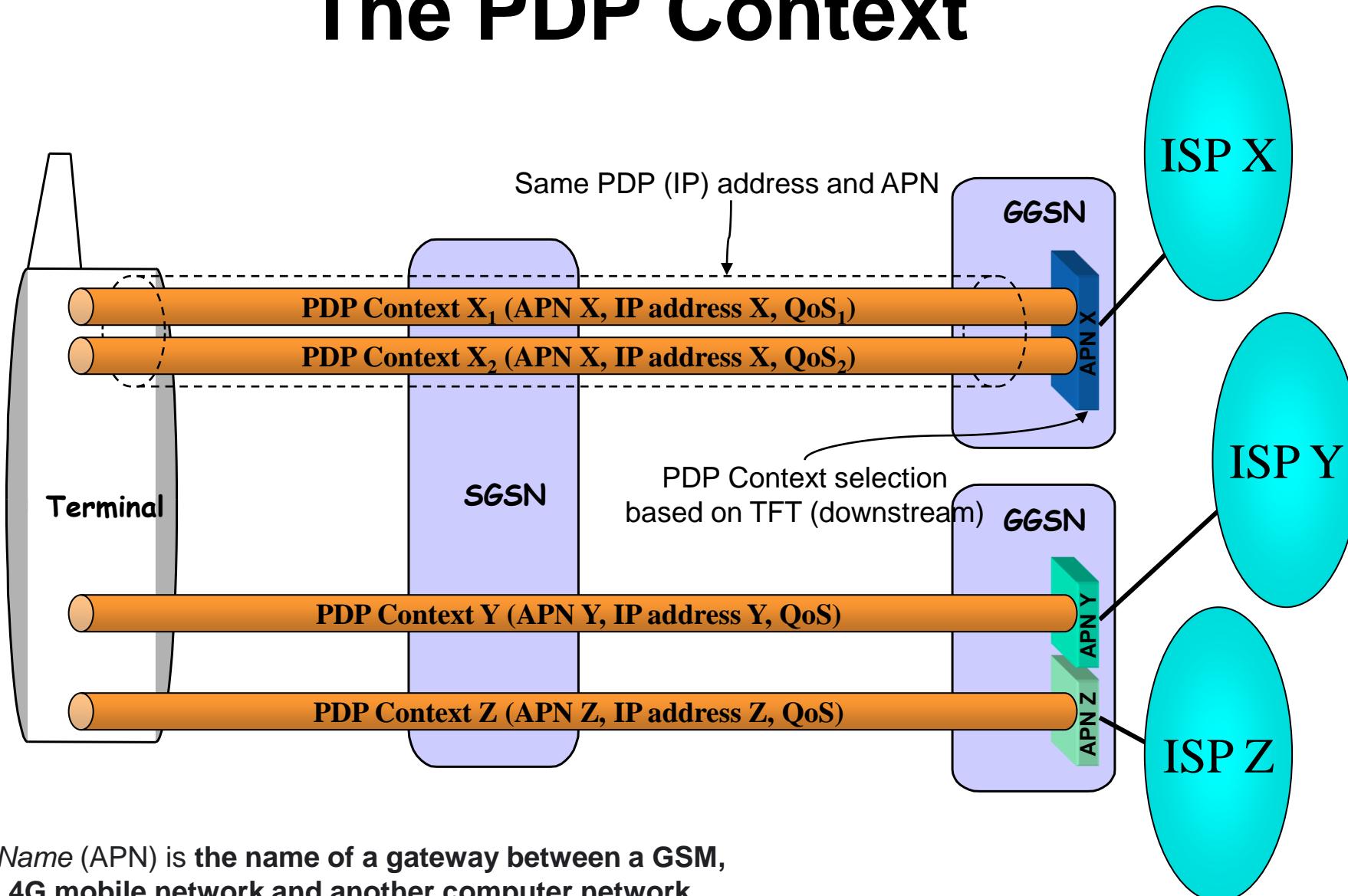
# GPRS Architecture



# GPRS introduction in a GSM network



# The PDP Context



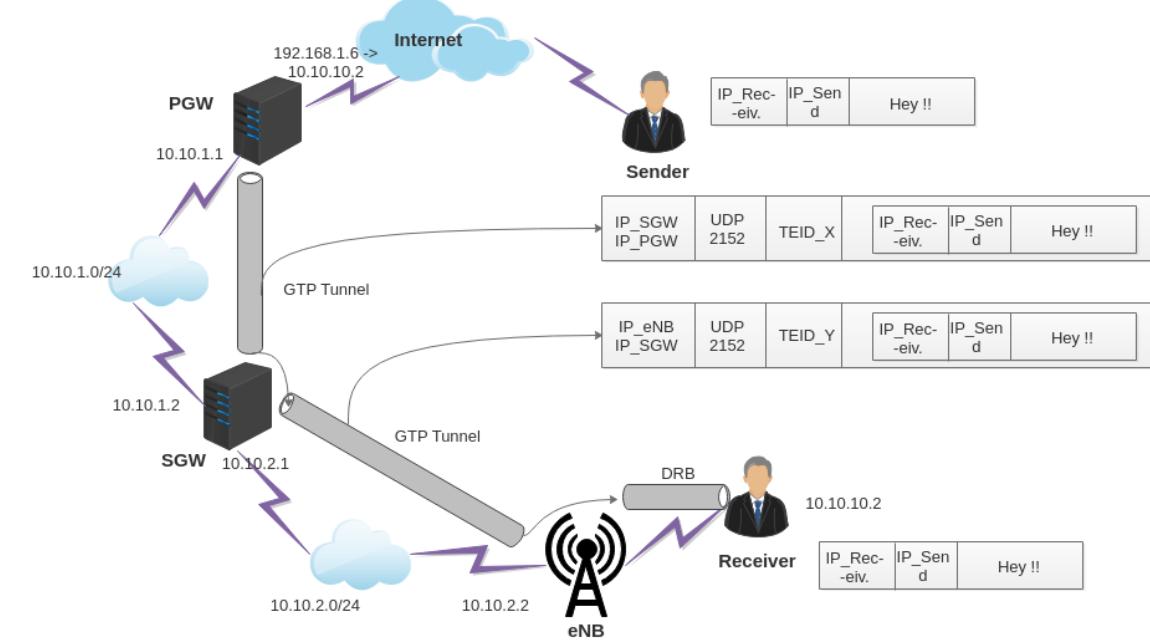
An Access Point Name (APN) is the name of a gateway between a GSM, GPRS, 3G and 4G mobile network and another computer network, frequently the public Internet.

Later called DNN in 5G

# GTP and PDP Context

- GTP
  - GPRS Tunneling Protocol is a simple tunneling protocol based on UDP/IP - used both in GSM/GPRS and UMTS.
  - Identified by a Tunnel Endpoint Identifier (TEID)
  - For every MS:
    - one GTP-C tunnel is established for signalling
    - Multiple GTP-U tunnels, one per PDP context (i.e. session), are established for user traffic.

- PDP Context
  - When an MS attaches to the Network:
    - SGSN creates a Mobility Management context with information about mobility and security for the MS.
    - At PDP Context Activation (PDP - Packet Data Protocol), both SGSN and GGSN create a PDP context, with information about the session (e.g. IP address, QoS, routing information , etc.)



**Note:** the figure is for 4G but the same principle applies, changing SGSN, GGSN and BSC by SGW, PGW and eNB

**3G**

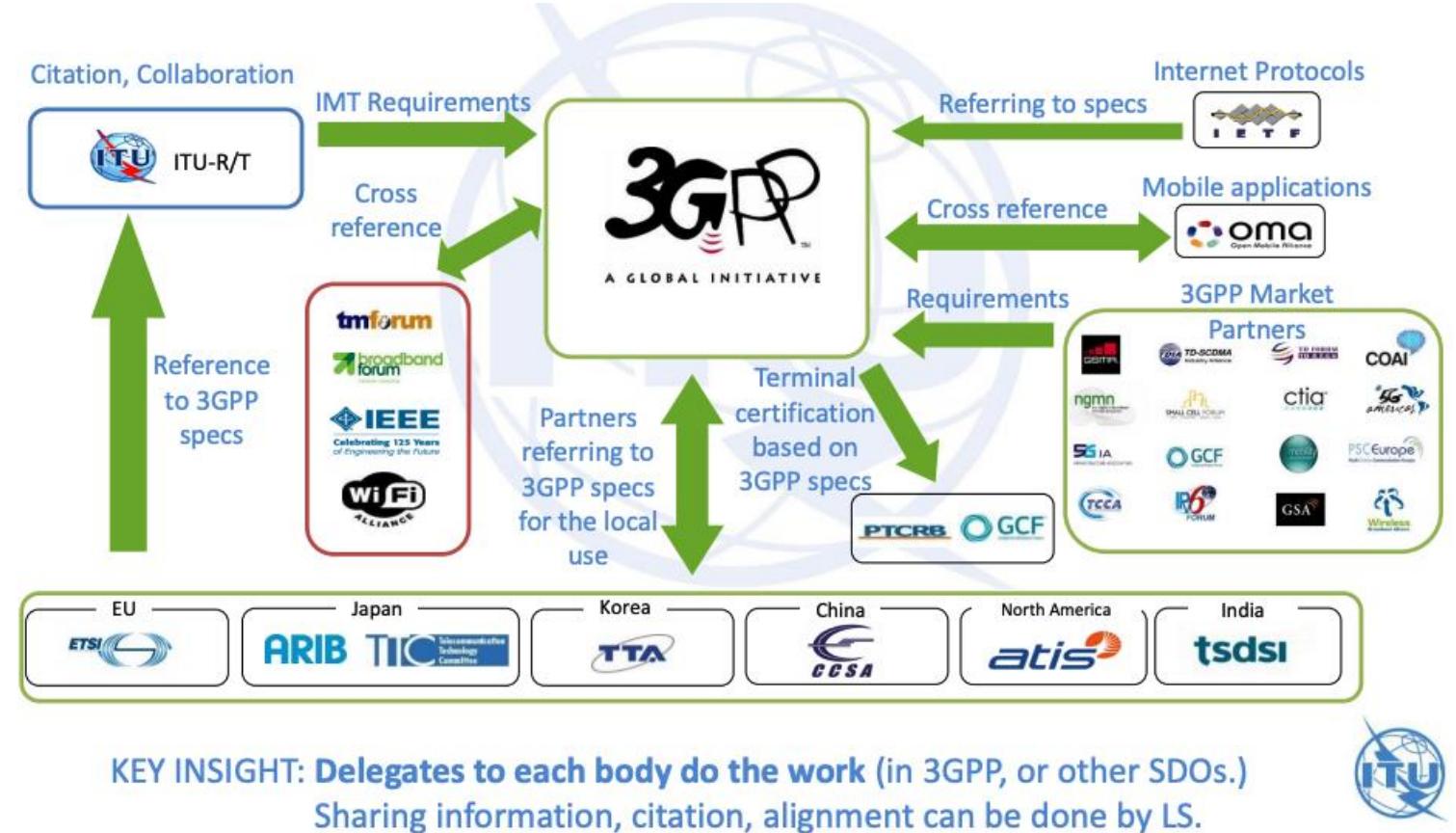
**Universal Mobile Telecommunication  
System**

# What is 3GPP?

3rd Generation Partnership Project - partnership of regional SDOs

"The original scope of 3GPP (1998) was to **produce Technical Specifications and Technical Reports for a 3G Mobile System** based on evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes).

The scope was subsequently amended to include the maintenance and development of the Technical Specifications and Technical Reports for evolved 3GPP technologies, **beyond 3G.**"

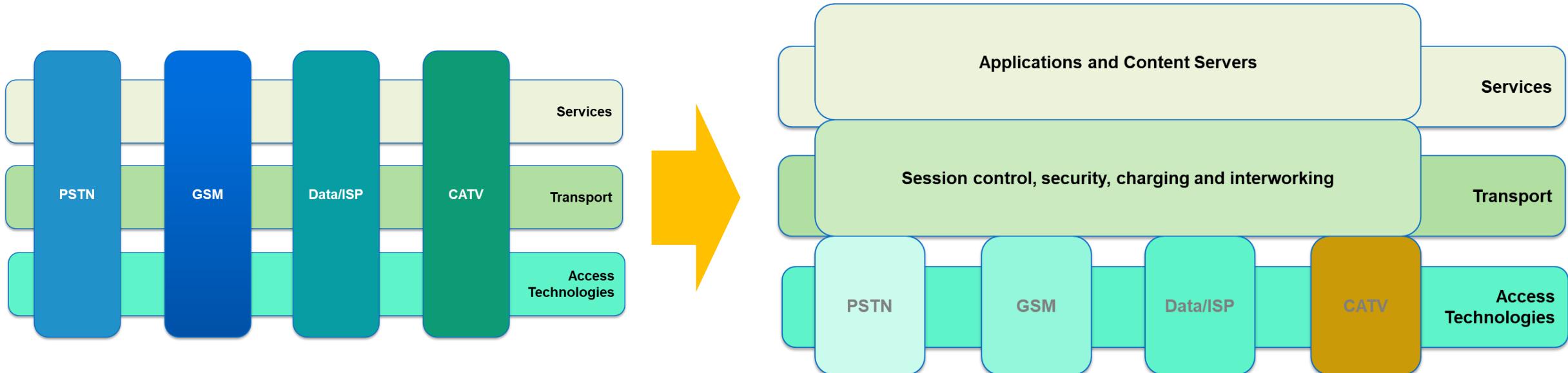


**SDOs take 3GPP specifications and transpose them to regional standards. Addresses:**

3G (IMT-2000) systems based on the evolved GSM core network and the Universal Terrestrial Radio Access (UTRA), in FDD and TDD modes; GSM, including GSM evolved radio access technologies (GPRS/EDGE/GERAN)

SDO: Standards Development Organization

# 3GPP/TISPAN Telecom Model



**Telecoms & Internet converged Services & Protocols for Advanced Networks**  
is a standardization body of ETSI, specializing in fixed networks and Internet convergence

# UMTS

- Universal Mobile Telecommunication System – 3G system
- Oriented towards generalized service diffusion, and future user trends: combines “cellular”, “wireless”, “Internet”, etc...
- “multimedia everywhere”
- Developed to have an evolutionary path from 2.5G systems; progressive evolution (GPRS-EDGE-UMTS)

## Specification

Flexible

Handles multiple multimedia flows in a single connection.

Support to packet transport

Flexible coding mechanisms (FDD/TDD WCDMA)

Variable transmission rates

Max. 384 Kbps for global coverage (initially)

Max. 2Mbps for local coverage (initially)

Any Device  
Any Access Technology  
Any Where

ALWAYS BEST CONNECTED

One Network, multiple access technologies

Common Session Control

Generic Application Servers

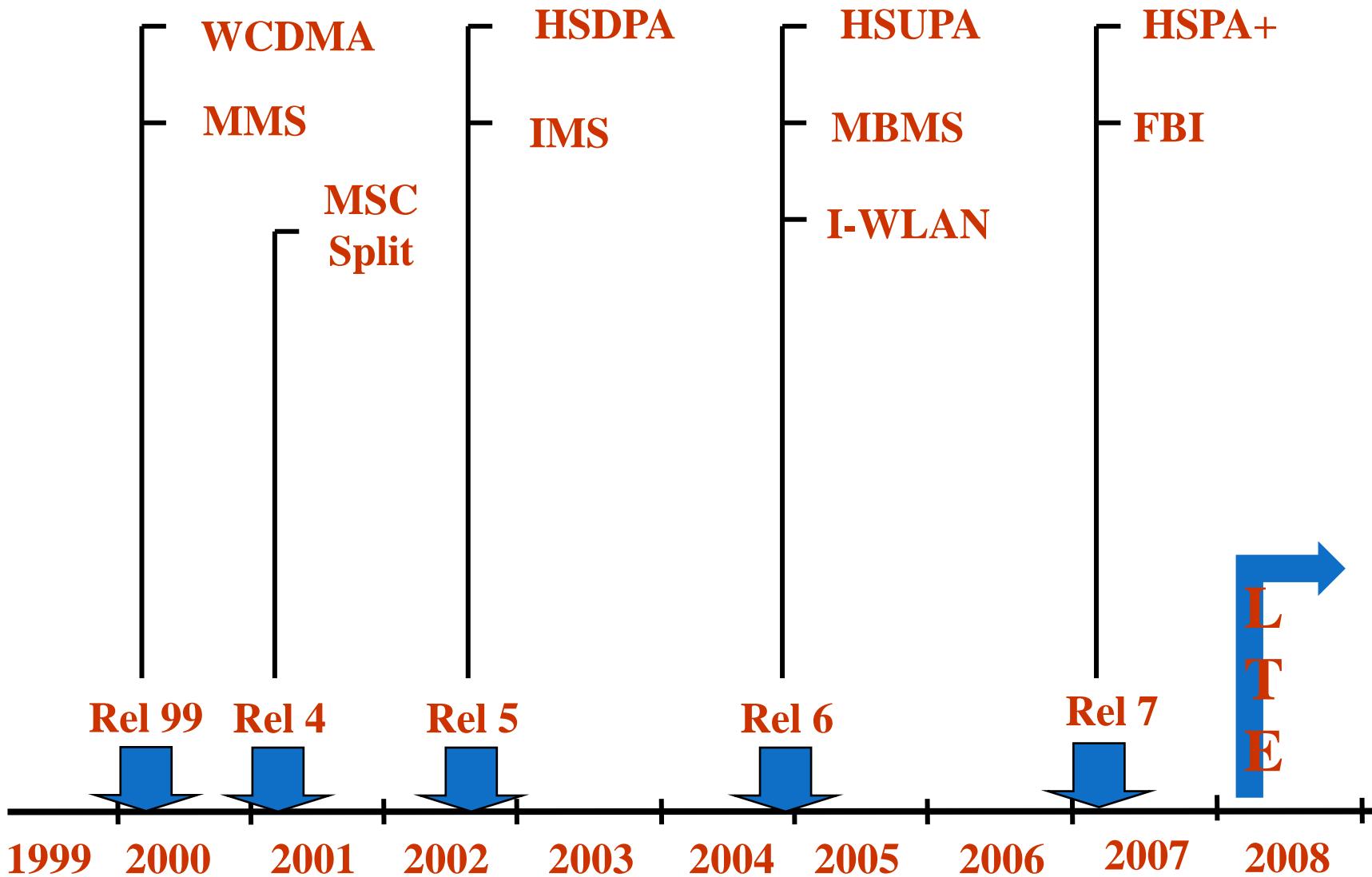
Single set of services that apply network wide

Consistent user experience

Operational efficiency

New services/applications

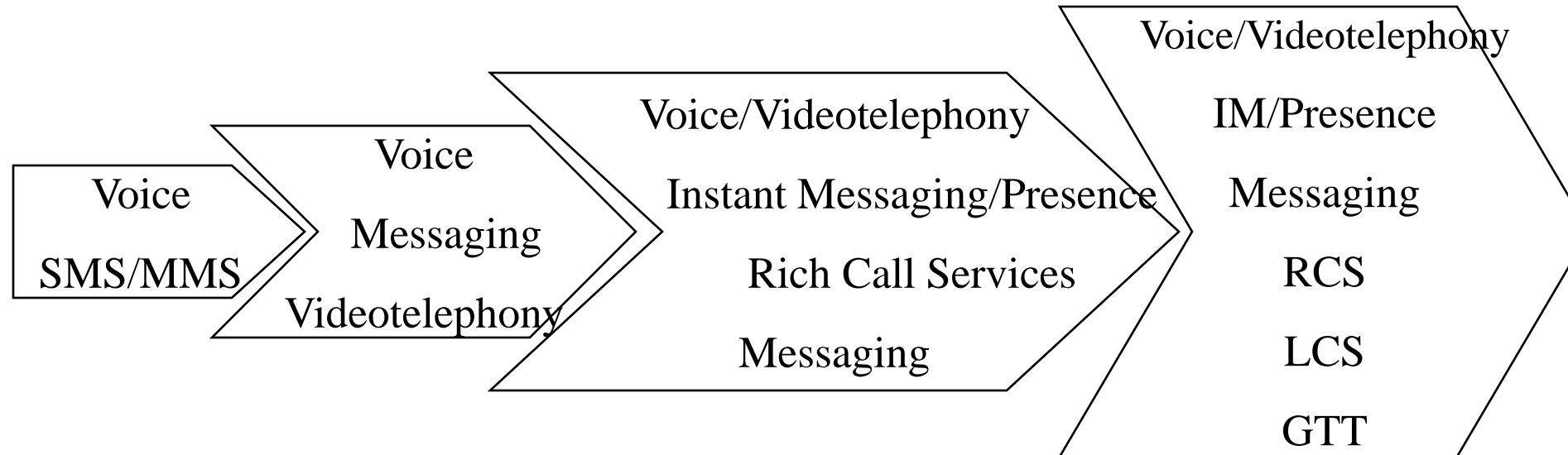
# UMTS evolution (3GPP Releases)



# Services evolution in UMTS R99/R4/R5/R6 networks

| Release | Services                                    |
|---------|---|
| R99     | MMS, streaming, LCS (cell), MExE, SAT, VHE, |
| R4      | TrFO, VHE, OSA, LCS in PS and CS,           |
| R5      | VoD, IMS, HSDPA, Wideband AMR, GTT          |
| R6      | MBMS, IMS phase 2                           |

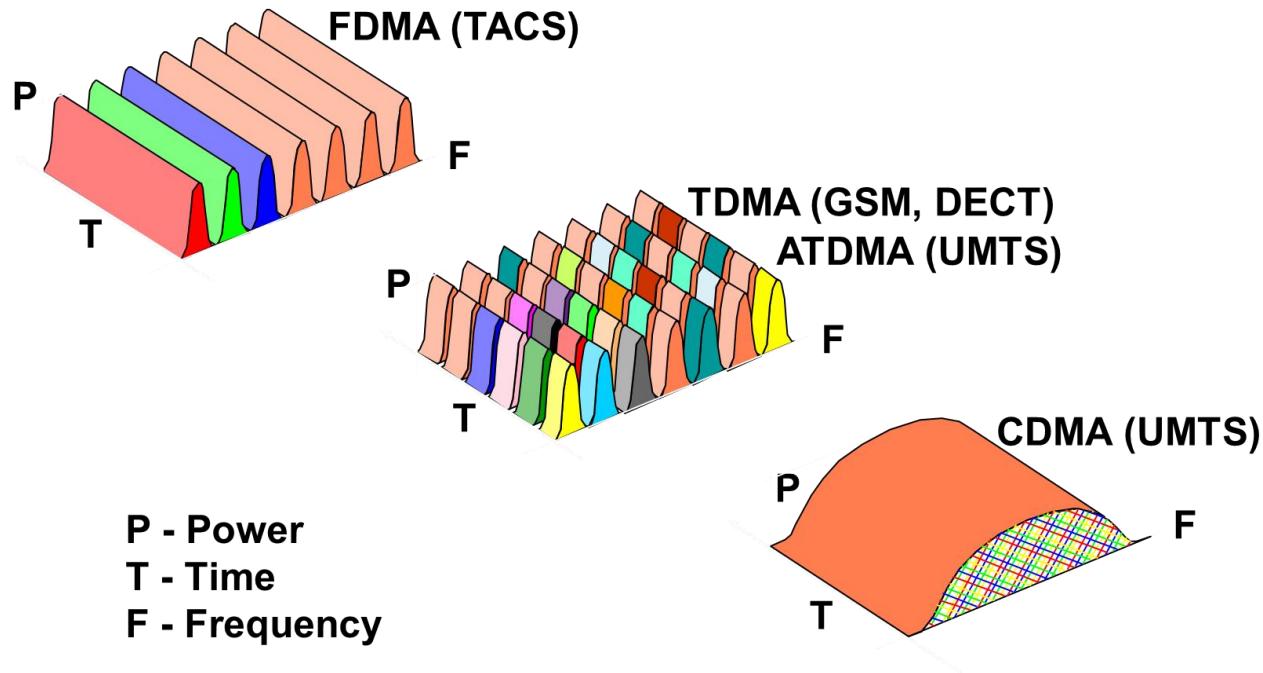
Evolution of the services (voice and interpersonal services)



# UMTS – air interface

- UTRA-FDD:
  - *uplink*: 1920 – 1980 MHz (60 MHz)
  - *downlink*: 2110 – 2170 MHz (60 MHz)
- UTRA-TDD:
  - 1900 – 1920 MHz (20 MHz)
  - 2010 – 2025 MHz (15 MHz)
- In Portugal:
  - 2x15 MHz for UTRA-FDD
  - 1x5 MHz for UTRA-TDD

# Multiplexing mechanisms



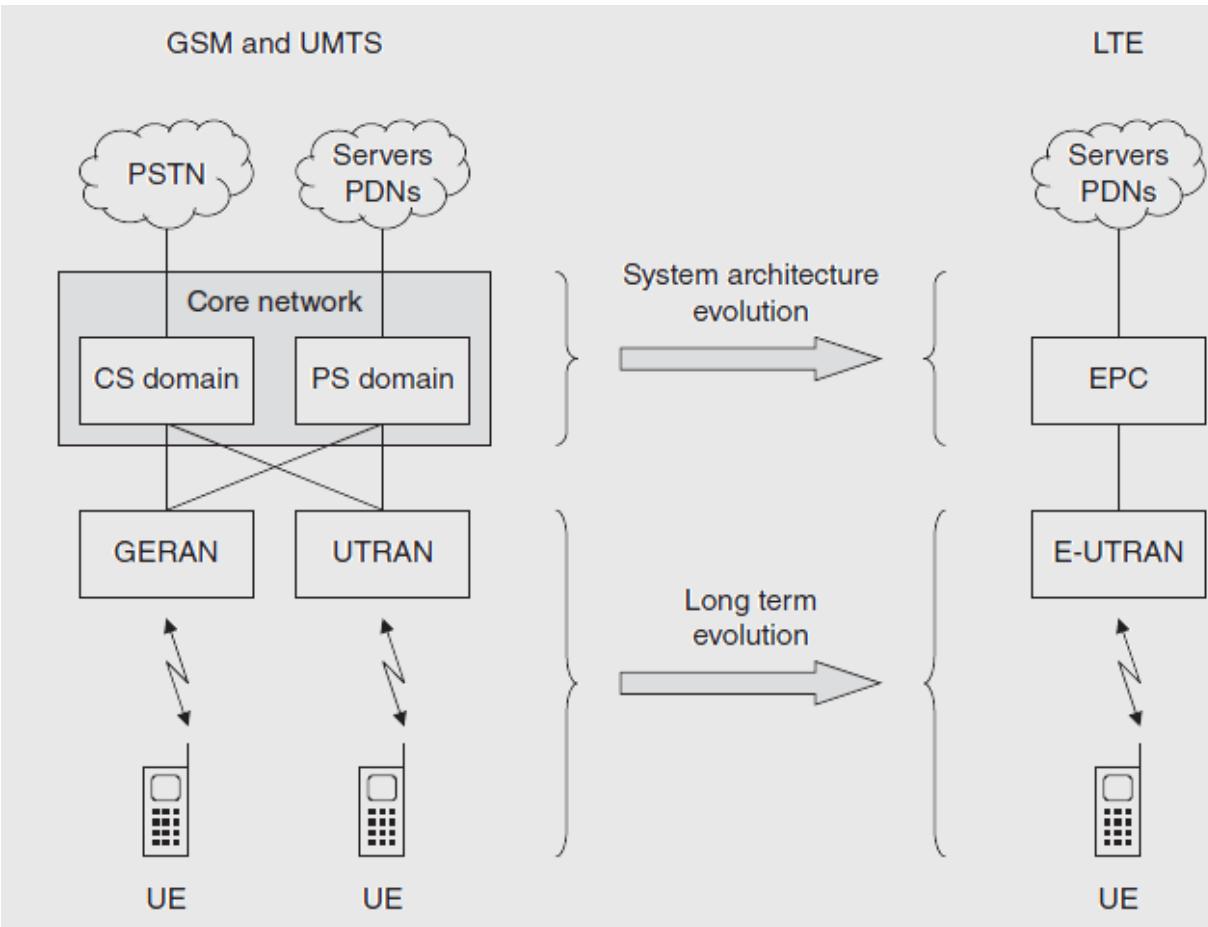
CDMA is a form of direct-sequence spread-spectrum technology that allows many users to occupy the same time and frequency allocations in a given band/space. CDMA assigns each user a unique spreading code to spread the baseband data before transmission, in order to help differentiate signals from various users in the same spectrum.

- Larger capacity and coverage, keeping compatibility with 2G
- Supports the flexibility required, with multiple parallel connections
- Efficient packet access

**4G**

**Long Term Evolution/Evolved Packet Core  
(LTE/EPC)**

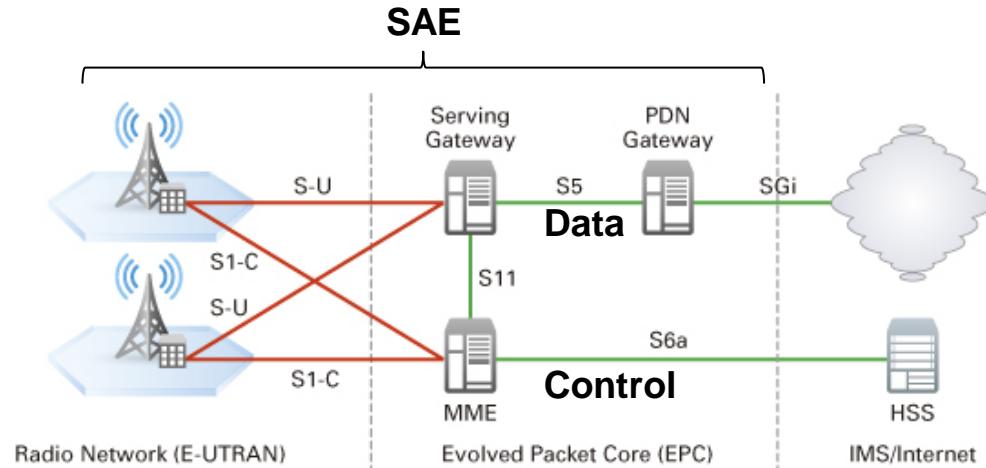
# Network simplification



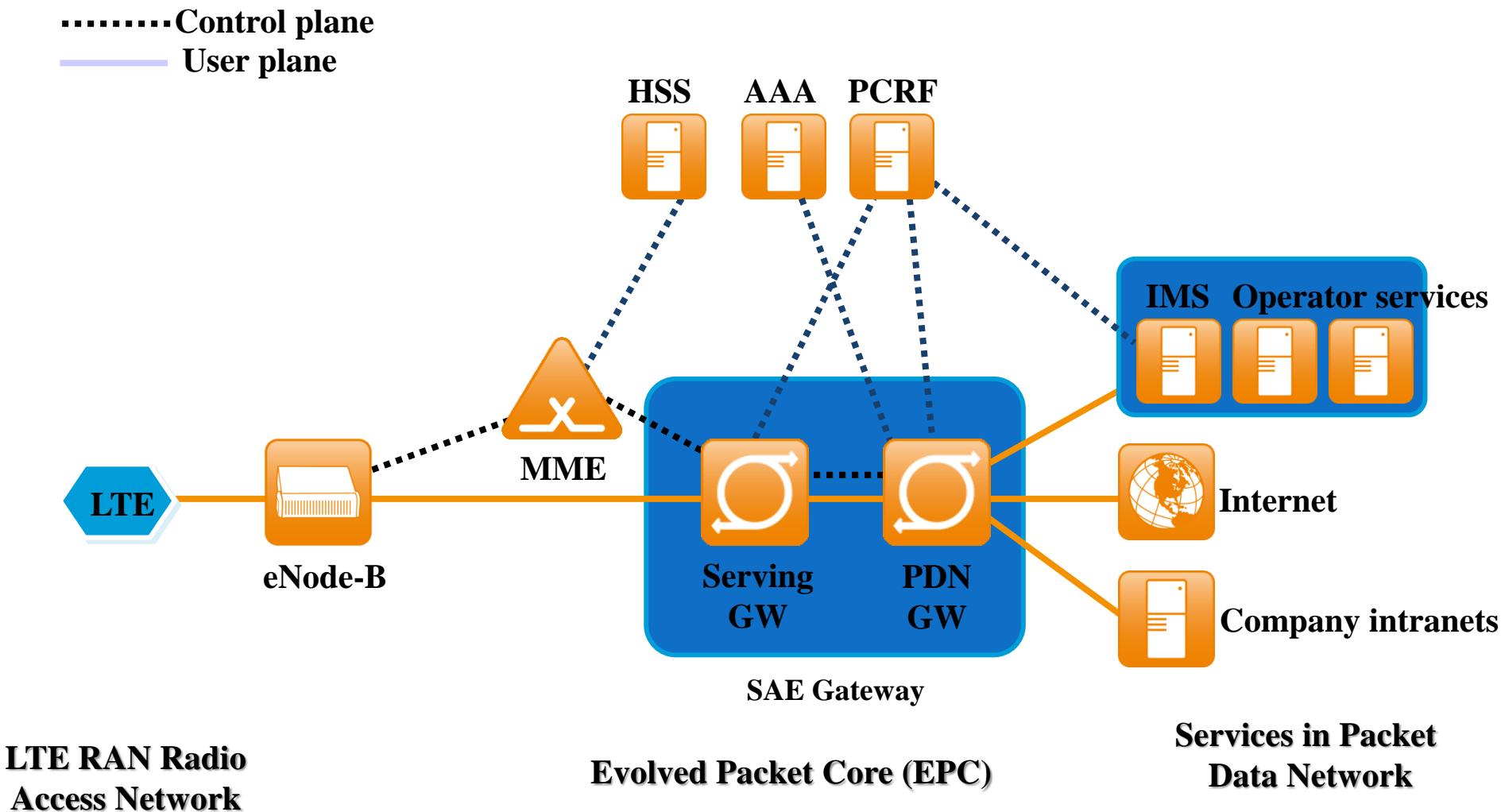
| Feature                    | UMTS                       | LTE                     |
|----------------------------|----------------------------|-------------------------|
| IP version support         | IPv4 and IPv6              | IPv4 and IPv6           |
| USIM version support       | Release 99 USIM onwards    | Release 99 USIM onwards |
| Transport mechanisms       | Circuit & packet switching | Packet switching        |
| CS domain components       | MSC server, MGW            | n/a                     |
| PS domain components       | SGSN, GGSN                 | MME, S-GW, P-GW         |
| IP connectivity            | After registration         | During registration     |
| Voice and SMS applications | Included                   | External                |

# 3GPP System Architecture Evolution (SAE) philosophy

- SAE focus is on:
  - enhancement of Packet Switched technology to cope with rapid growth in IP traffic
    - higher data rates
    - lower latency
    - packet optimised system
  - through
    - fully IP network
      - In addition to IMS services available in the current system, equivalent CS Services may be provided by IMS core since CS domain is not supported in LTE
    - simplified network architecture
      - Reduced number of nodes in the evolved packet core may be achieved compared to current architecture to provide connectivity to IMS
    - distributed control
      - Flexible accommodation and deployment of existing and new access technologies with mobility by a common IP-based network



# EPC architecture

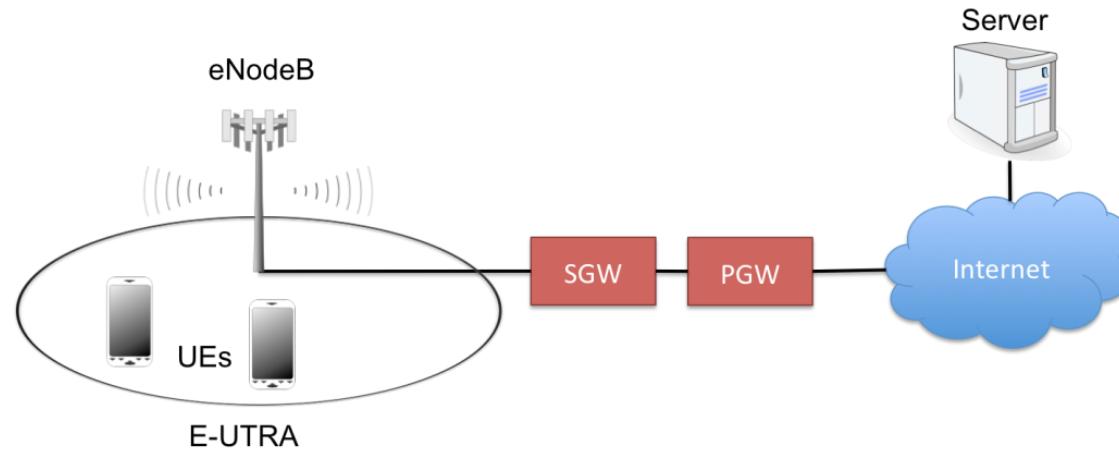


**LTE RAN Radio Access Network**

**Evolved Packet Core (EPC)**

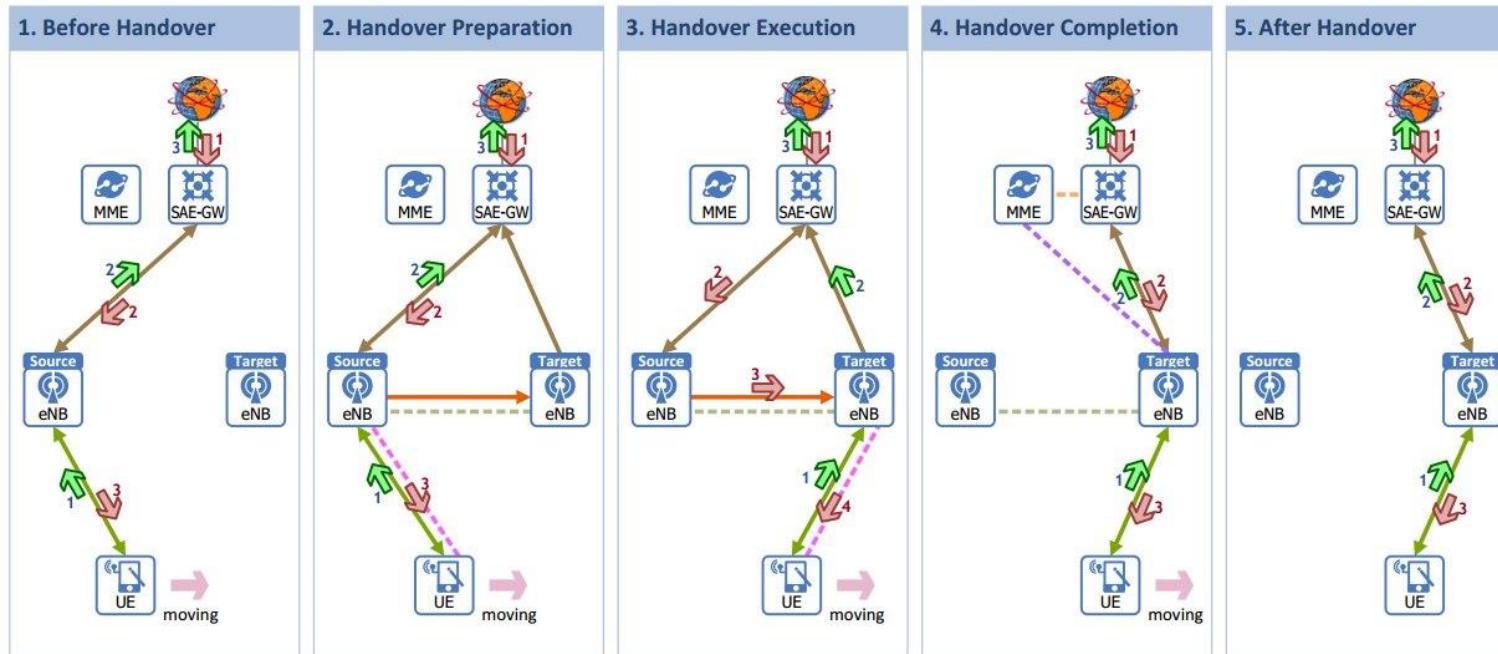
**Services in Packet Data Network**

# LTE Network



- **Packet Delivery Network Gateway (PGW)**
  - Connects LTE network to IP networks
- **Serving Gateway (SGW)**
  - Route packets to and from wireless access points
- **Enhanced Node B (eNodeB)**
  - Wireless access point
- **User Equipment (UE)**
  - End user devices

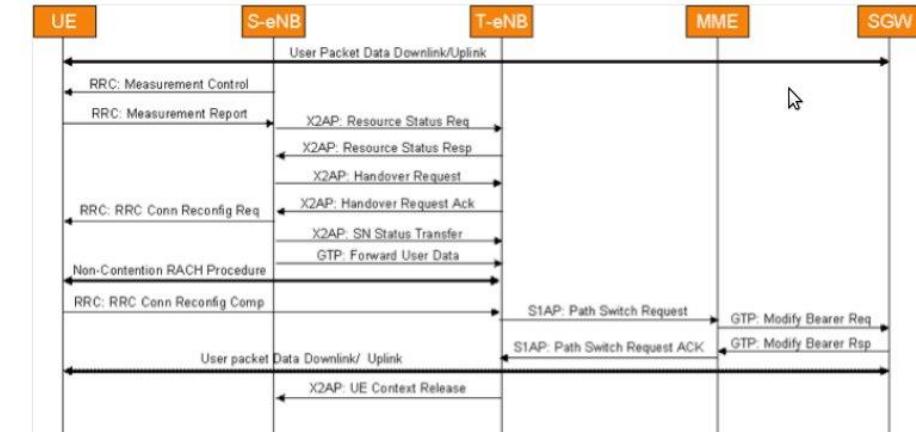
# Handover process in SAE



- Source eNB makes the HO decision
- Direct Tunnel Setup (X2 Transport Bearer between Source eNB and Target eNB)

- Detach from Source eNB
- Direct Packet Forwarding (DL traffic from Source eNB to Target eNB)

- Path Switch procedure between Target eNB and MME
- Release S1 Bearer of Source eNB
- Release X2 Transport Bearer for direct Packet Forwarding



DRB (Data Radio Bearer)  
S1 Bearer (GTP Tunnel)

X2 Bearer (GTP Tunnel)  
S11 (GTP-C) Signaling

S1 Signaling  
X2 Signaling

↑ UL Traffic  
↓ DL Traffic

# Long Term Evolution (LTE)

- Long Term Evolution (LTE) – Standard created by the 3rd Generation Partnership Project
  - Deployed globally
  - All packet switched network
  - High throughput and QoS considerations
  - Provides wireless retransmissions of lost data

| Technology            | 3G                | 4G              |
|-----------------------|-------------------|-----------------|
| Data Transfer Rate    | 3.1MB /sec        | 100MB/sec       |
| Internet services     | Broadband         | Ultra Broadband |
| Mobile -TV Resolution | Low               | High            |
| Bandwidth             | 5 - 20 MHz        | 100 +MHz        |
| Frequency             | 1.6- 2 GHZ        | 2 – 8 GHz       |
| Network Architecture  | Wide Area Network | Hybrid Network  |

# Radio evolution

## More flexible and resilient radio technology

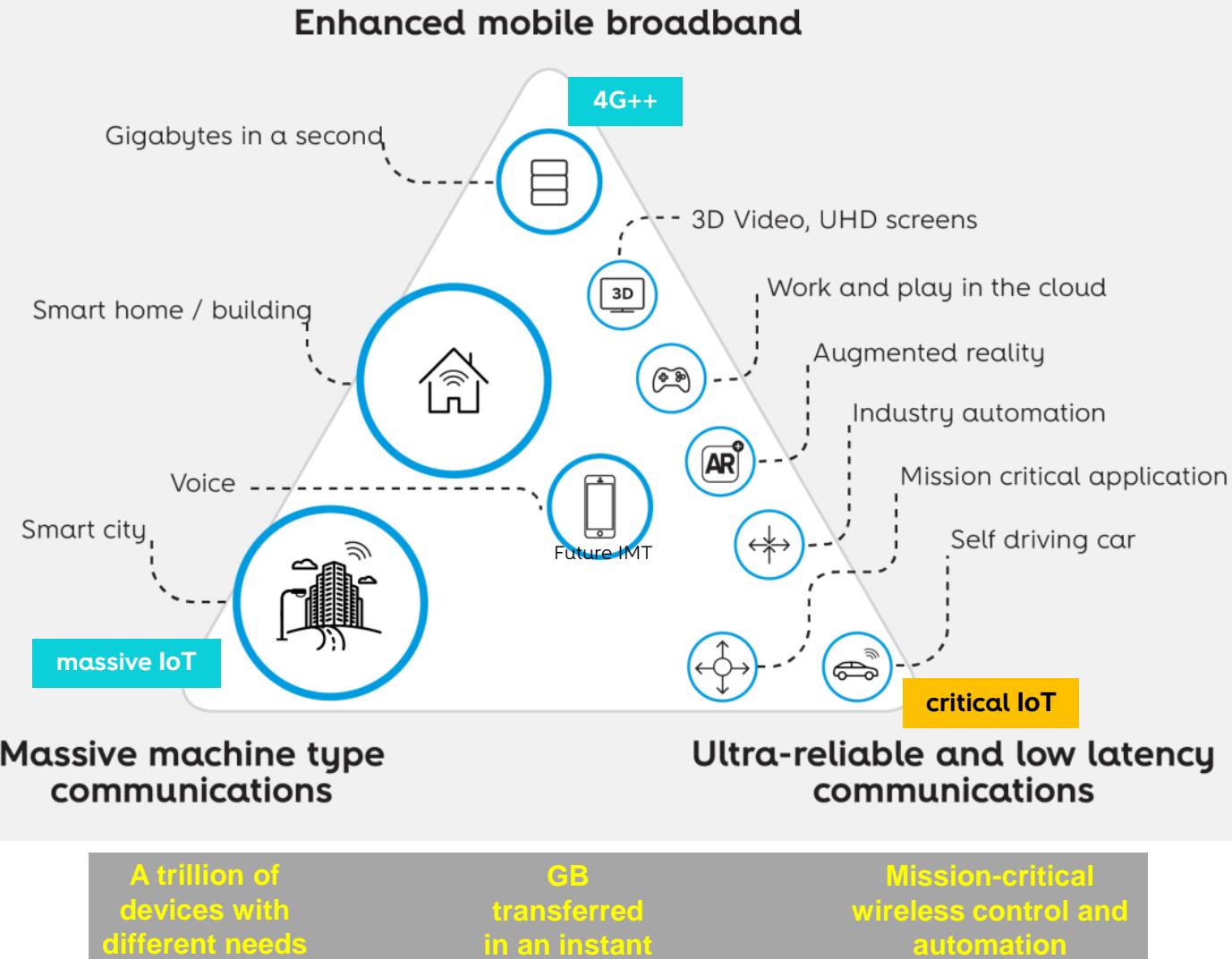
| Feature                         | WCDMA  | LTE                         |
|---------------------------------|--|-----------------------------|
| Multiple access scheme          | WCDMA  | OFDMA and SC-FDMA           |
| Frequency re-use                | 100%   | Flexible                    |
| Use of MIMO antennas            | From Release 7   | Yes                         |
| Bandwidth                       | 5 MHz  | 1.4, 3, 5, 10, 15 or 20 MHz |
| Frame duration                  | 10 ms  | 10 ms                       |
| Transmission time interval      | 2 or 10 ms   | 1 ms                        |
| Modes of operation              | FDD and TDD  | FDD and TDD                 |
| Uplink timing advance           | Not required   | Required                    |
| Transport channels              | Dedicated and shared                                   | Shared                      |
| Uplink power control            | Fast   | Slow                        |
| Radio access network components | Node B, RNC  | eNB                         |
| RRC protocol states             | CELL_DCH, CELL_FACH,<br>CELL_PCH, URA_PCH,<br>RRC_IDLE | RRC_CONNECTED,<br>RRC_IDLE  |
| Handovers                       | Soft and hard  | Hard                        |
| Neighbour lists                 | Always required  | Not required                |

# 5G

*"Enabling a seamlessly connected society in the 2020 timeframe and beyond that brings together people along with things, data, applications, transport systems and cities in a smart networked communications environment"*

ITU-R (*International Telecommunication Union*)

# 5G organization of ‘Usage Scenarios’



5G will power a **new generation of services and applications** in the areas of:

*Enhanced Mobile BroadBand (eMBB)*  
**Make it faster!**

*Massive Machine Type Communications (mMTC)*  
**Make it massive!**

*Ultra-Reliable, Low Latency Communications (URLCC)*  
**Make it trustable and responsive!**

All with a single, unified technology

...while driving down the cost per managed bit

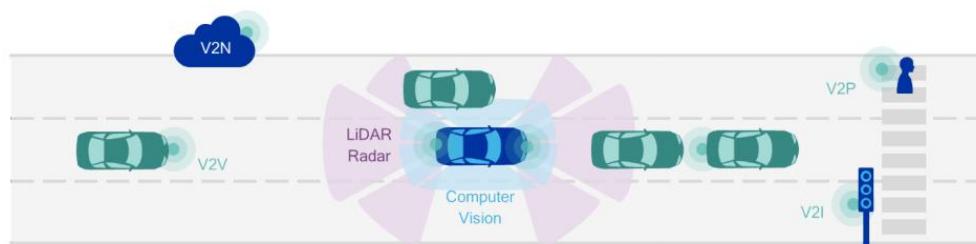
# Example of verticals: 5GAA (5G Automotive Association)

<http://5gaa.org/>

“Develop, test and promote communications solutions, initiate their standardization and accelerate their commercial availability and global market penetration to address society’s connected mobility and road safety needs with applications such as autonomous driving, ubiquitous access to services and integration into smart city and intelligent transportation”

## Vehicle to anything (V2x) communications:

- Vehicle to Vehicle (V2V)
- Vehicle to Network (V2N)
- Vehicle to Infrastructure (V2I)
- Vehicle to Pedestrian (V2P)



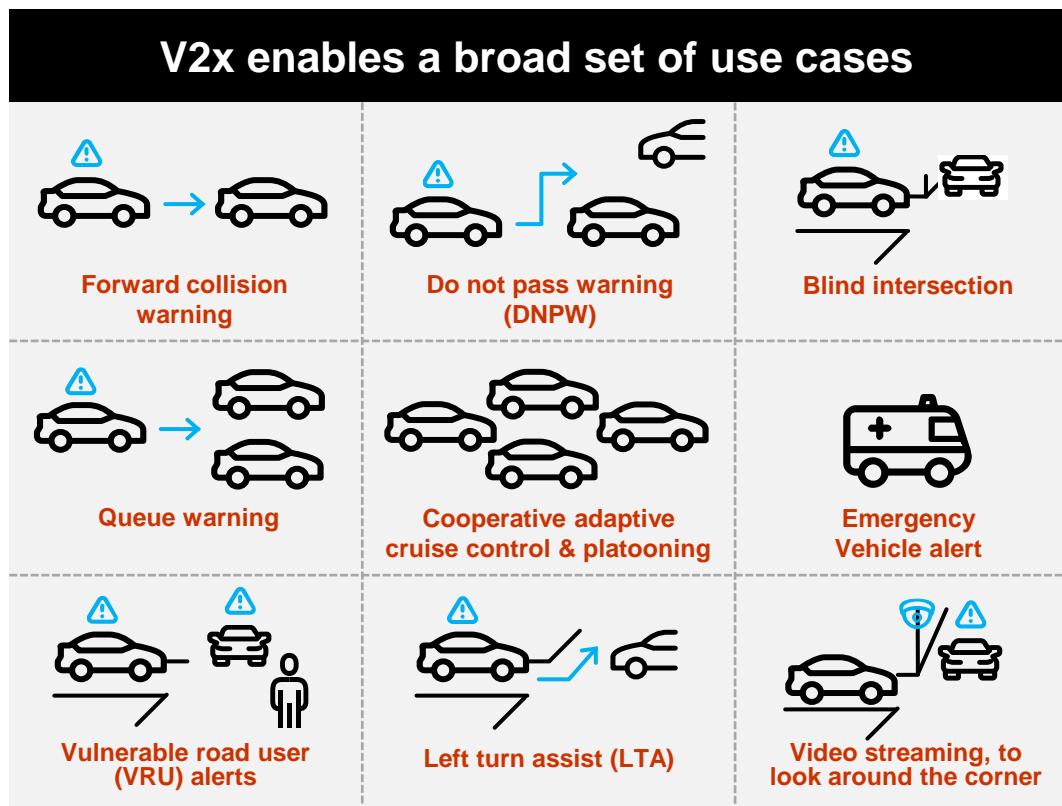
## MEMBERS



# V2x Use Cases

3GPP V2x evolutionary support

Adapted from Qualcomm



Enhanced  
V2x  
C-V2x 3GPP  
Rel 14

Basic V2x  
802.11p, DSRC,  
ETSI ITS

- V2v, V2p, V2i
- Safety
- EV

Advanced V2x  
C-V2x 3GPP Rel 15 and  
future Rel 16, etc

- Longer range
- Higher density
- Very high throughput
- Very high reliability
- Wideband ranging and positioning
- Very low latency

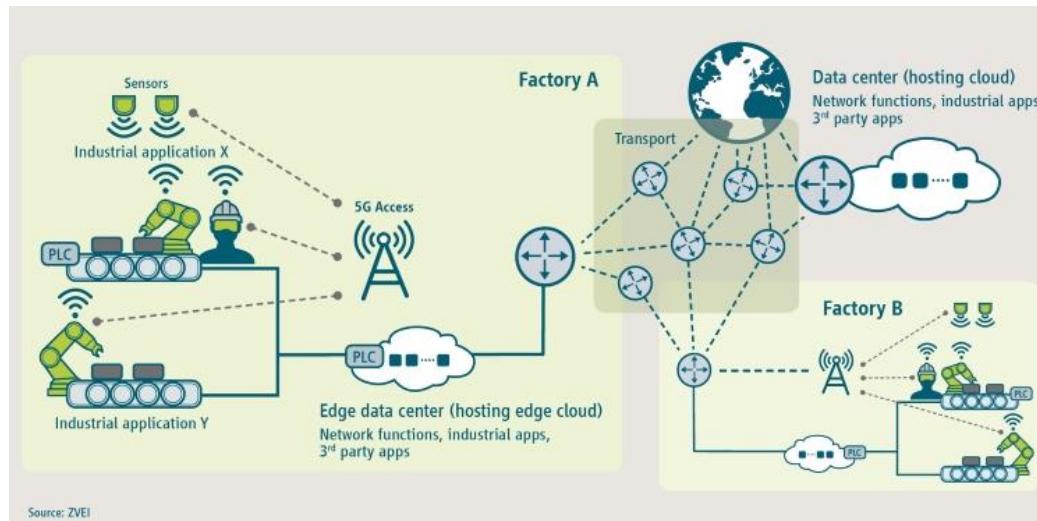
Source: 5G Americas Whitepaper, "Cellular V2x Communications towards 5G", Mar'18

| Communication scenario description  | Max end-to-end latency (ms) | Reliability (%) |
|---|-----------------------------|-----------------|
| Information exchange between a UE supporting V2X application and a V2X Application Server | 5                           | 99.999          |
| Cooperative driving for vehicle platooning  |                             |                 |
| Information exchange between a group of UEs supporting V2X application.                   | 10                          | 99.99           |
| Emergency trajectory alignment between UEs supporting V2X application.                    | 3                           | 99.999          |
| Sensor information sharing between UEs supporting V2X application                         | 3                           | 99.999          |

# Example of verticals: 5G-ACIA

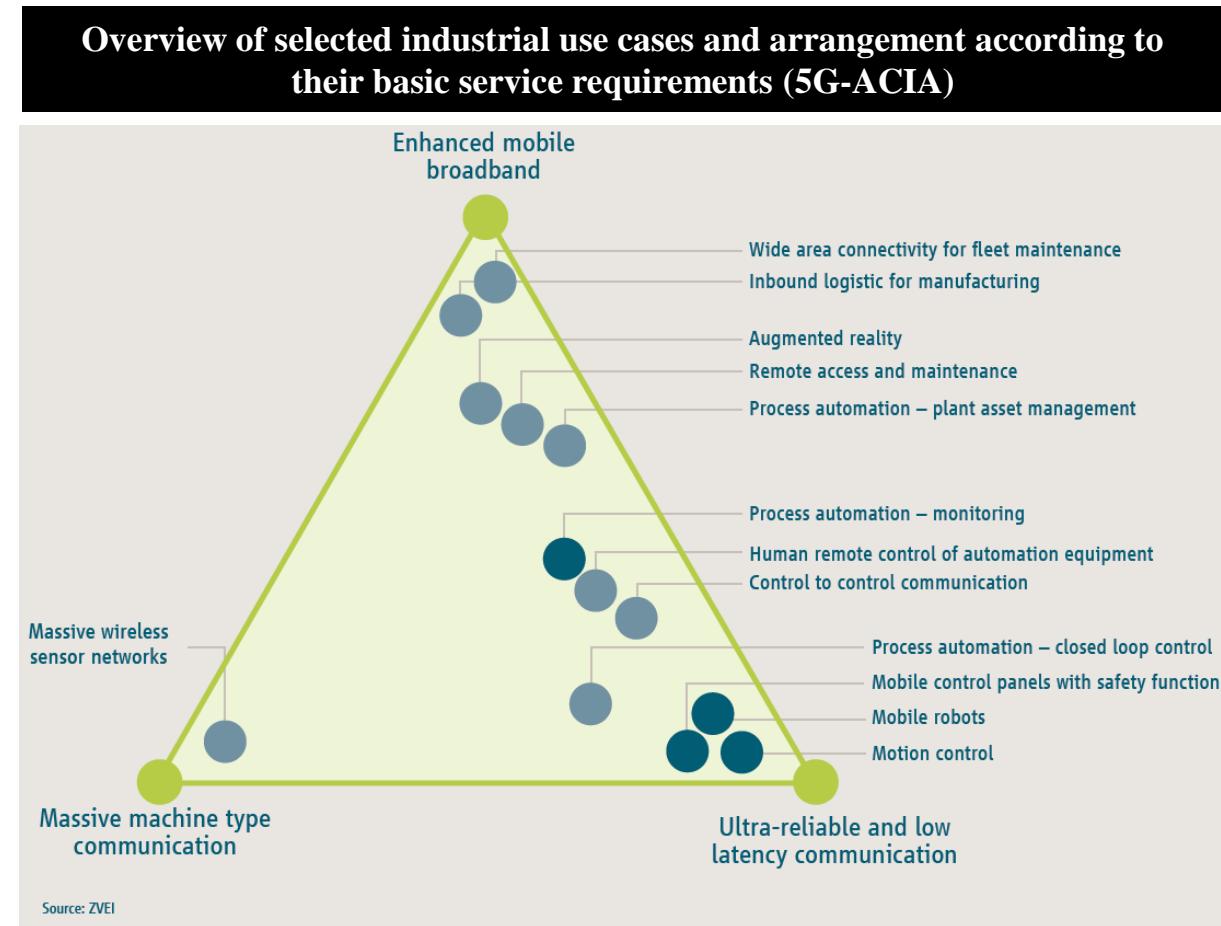
<https://www.5g-acia.org/>

“5G-ACIA ensures the best possible applicability of 5G technology and 5G networks for the manufacturing and process industries by addressing, discussing and evaluating relevant technical, regulatory and business aspects.”

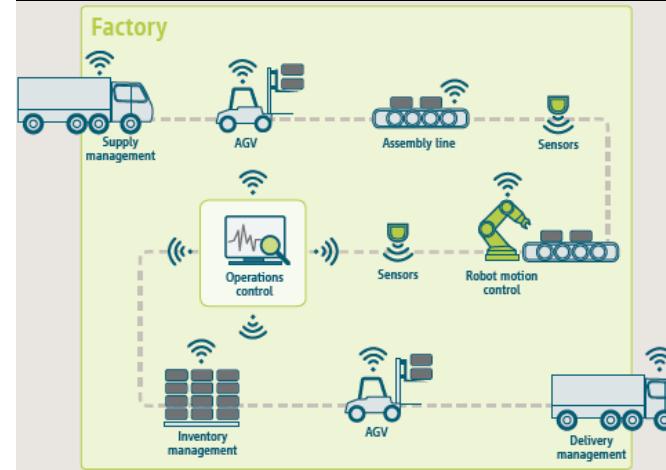


# Industry use cases

- 5G in the private domain



## Exemplary application areas of 5G in the factory of the future (5G-ACIA)



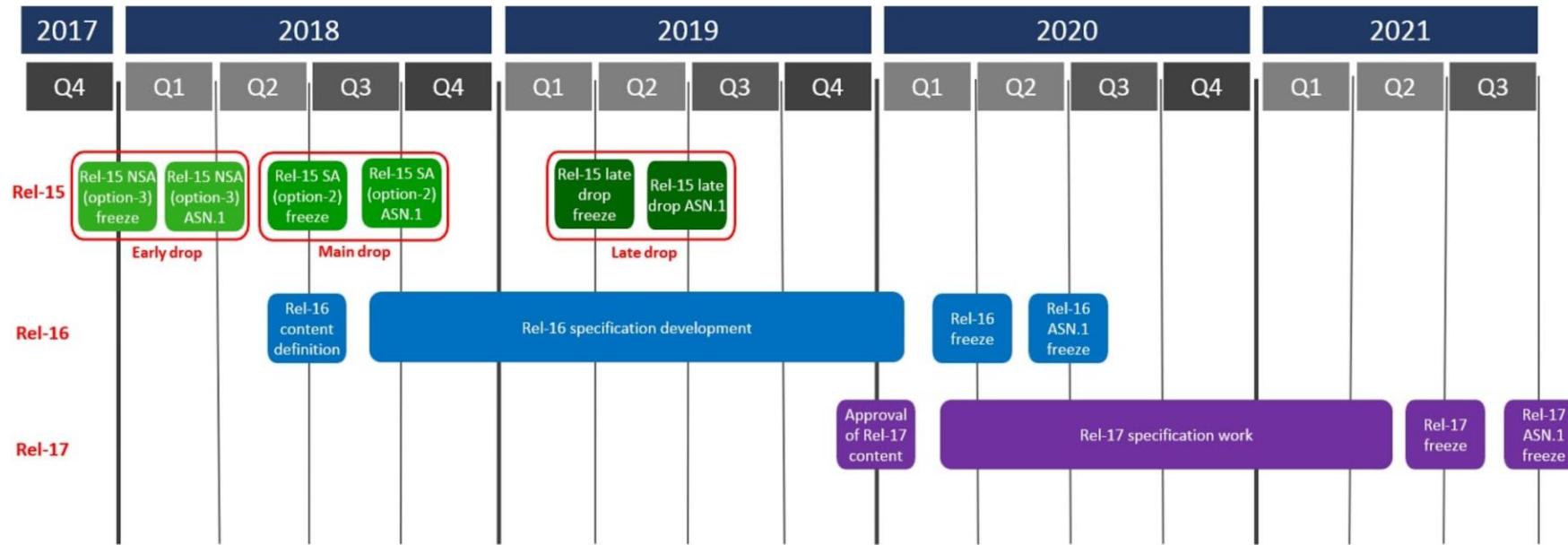
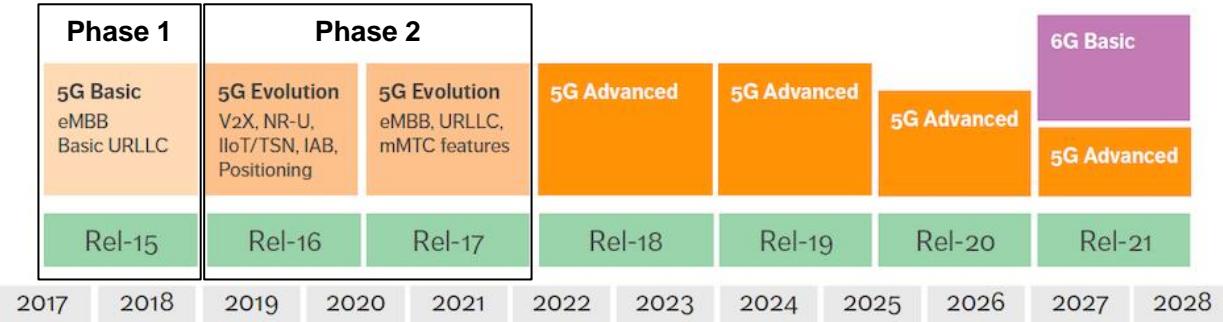
## Selected use cases requirements (5G-ACIA)

| Use case (high level)                       | Availability | Cycle time  | Typical payload size | # of devices                      | Typical service area |
|---|--------------|-------------|----------------------|-----------------------------------|----------------------|
| Motion control                              | >99.9999%    | < 2 ms      | 20 bytes             | >100                              | 100 m x 100 m x 30 m |
|   | >99.9999%    | < 0.5 ms    | 50 bytes             | ~20                               | 15 m x 15 m x 3 m    |
|   | >99.9999%    | < 1 ms      | 40 bytes             | ~50                               | 10 m x 5 m x 3 m     |
| Mobile robots                               | >99.9999%    | 1 ms        | 40-250 bytes         | 100                               | < 1 km <sup>2</sup>  |
|   | >99.9999%    | 10 – 100 ms | 15 – 150 kbytes      | 100                               | < 1 km <sup>2</sup>  |
| Mobile control panels with safety functions | >99.9999%    | 4-8 ms      | 40-250 bytes         | 4                                 | 10 m x 10 m          |
|   | >99.9999%    | 12 ms       | 40-250 bytes         | 2                                 | 40 m x 60 m          |
| Process automation (process monitoring)     | >99.99%      | > 50 ms     | Varies               | 10000 devices per km <sup>2</sup> |                      |

Service unavailability <31,5s / Year

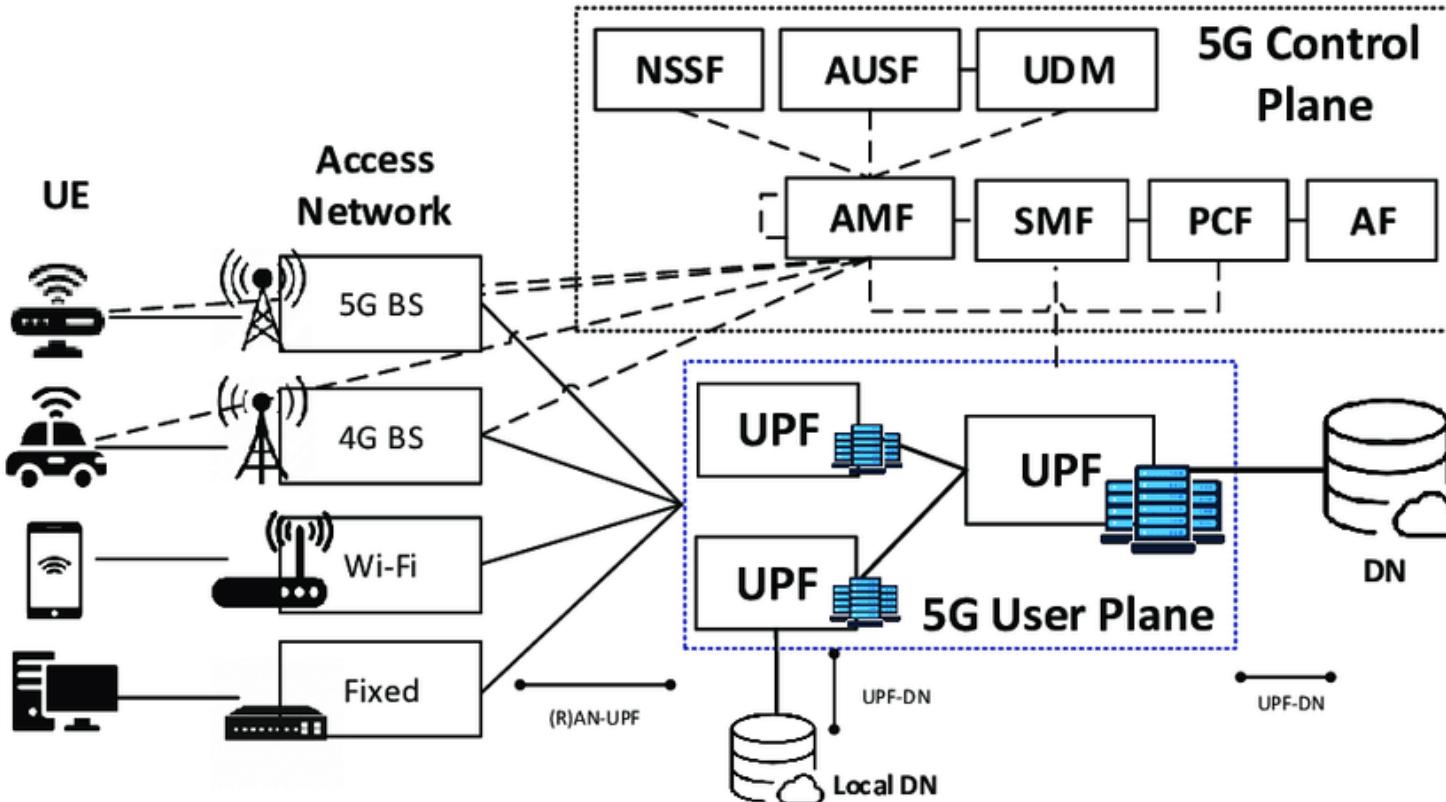
Cycle time shall be measured from command execution to feedback received ➔ 5G latency < half the cycle time

# 5G roadmap



Designed by 3G4G, based on roadmap from 3GPP, July 2019

# 5G System



## 5G System:

1. UEs
2. 5G RAN
3. 5G Core

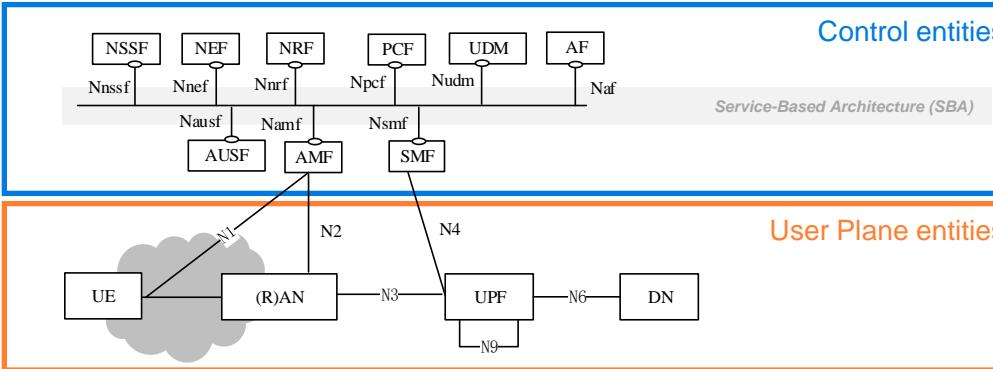
Control and user planes separation

Microservices (5G Core)

Multi-access

# 5G System arch. and functional modules (parcial)

3GPP TS 23.501 V0.3.1 (2017-03)

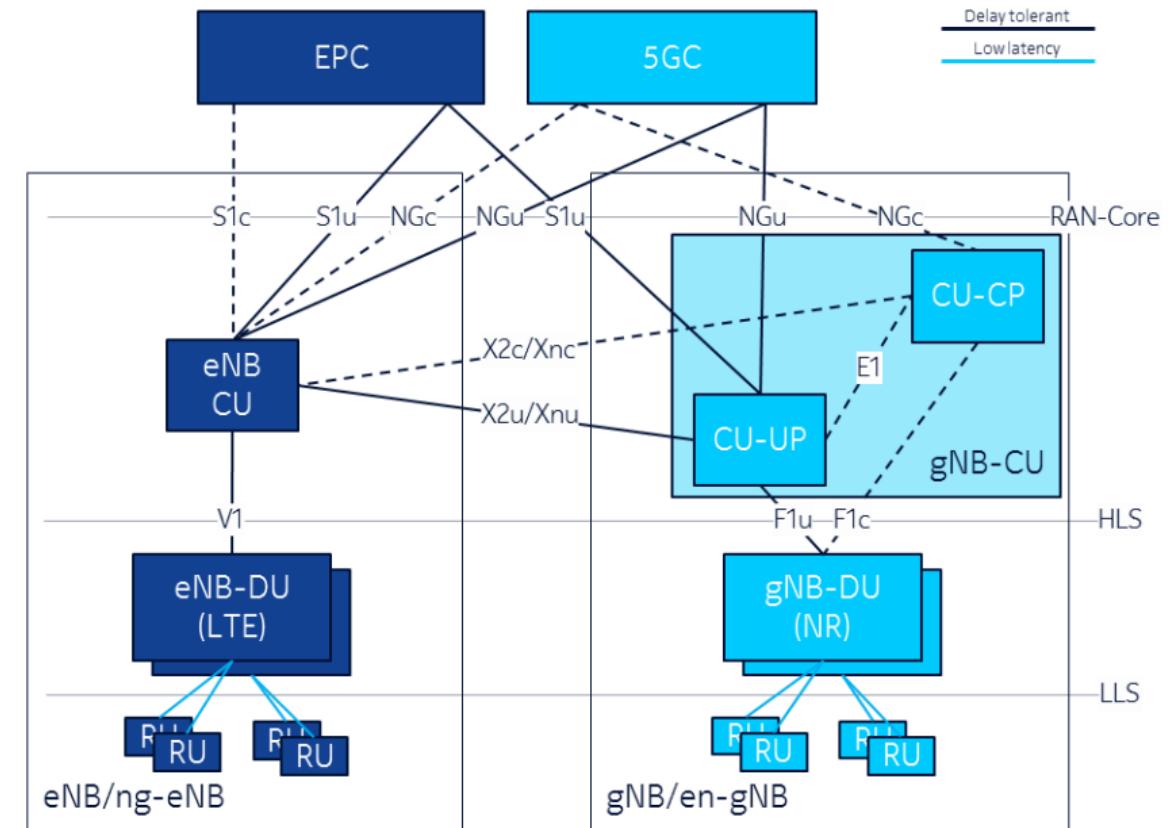
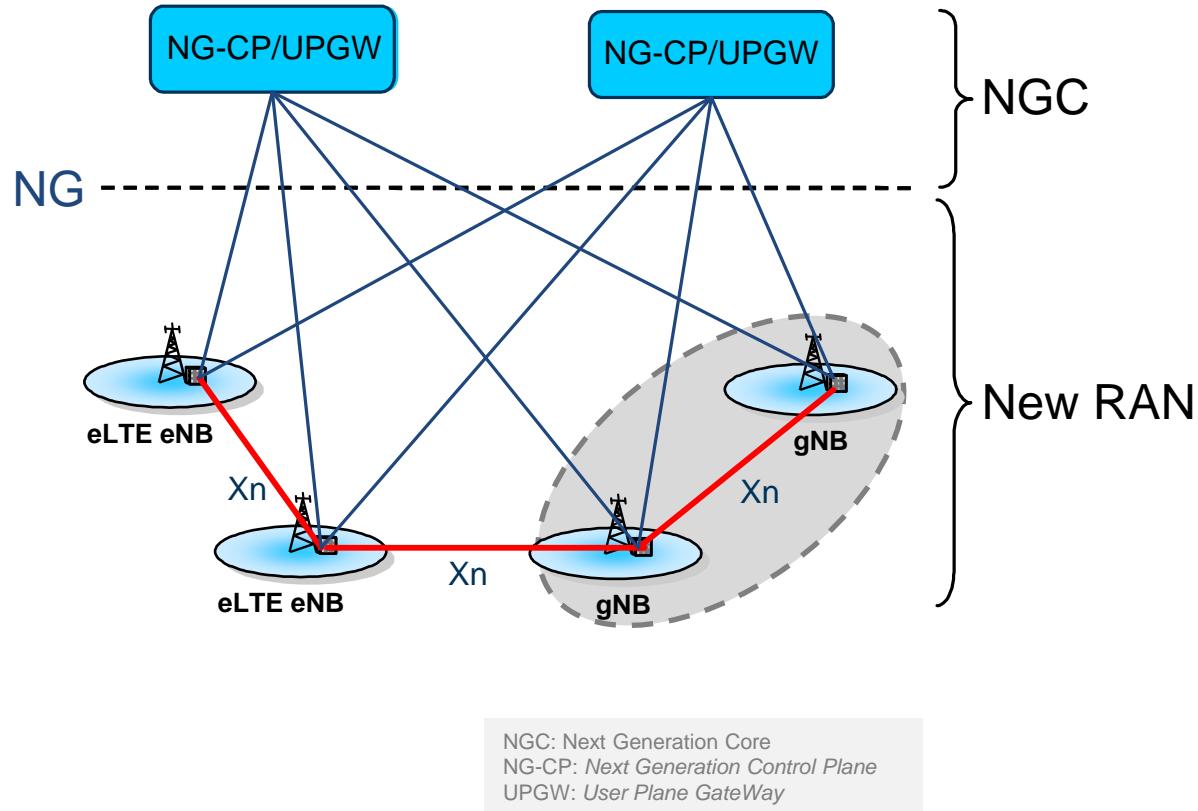


- Separate the User Plane (UP) functions from the Control Plane (CP) functions
- Modularize the function design, e.g. to enable flexible and efficient network slicing
- Define procedures (i.e. the set of interactions between network functions) as services
- Enable each Network Function to interact with other NF directly if required (direct interaction)
- Minimize dependencies between the Access Network (AN) and the Core Network (CN)
- Support a unified authentication framework
- Support "stateless" NFs, where the "compute" resource is decoupled from the "storage" resource
- Support capability exposure
- Support concurrent access to local and centralized services. To support low latency services and access to local data networks, UP functions can be deployed close to the Access Network

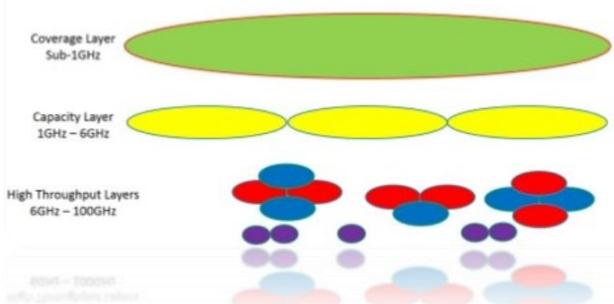
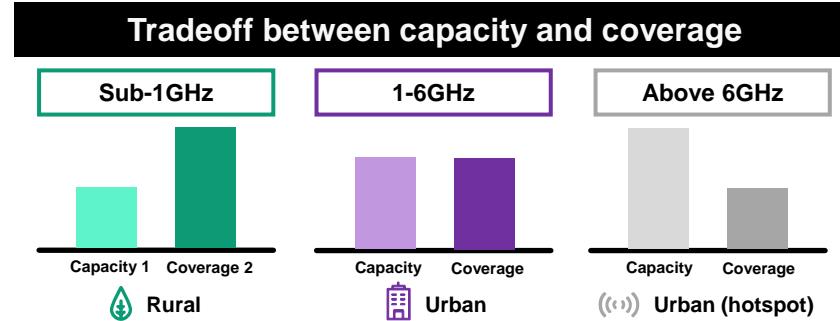
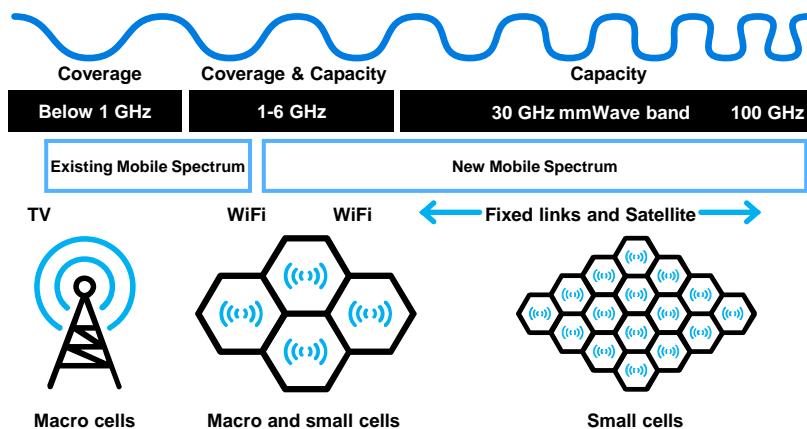
1. Network Slice Selection Function (NSSF)
2. Network Exposure Function (NEF)
3. NF Repository Function (NRF)
4. Policy Control Function (PCF)
5. Unified Data Management (UDM)
6. Application Function (AF)
7. Authentication Server Function (AUSF)
8. Access and Mobility Management Function (AMF)
9. Session Management Function (SMF)
10. Unified Data Repository (UDR)
11. Unstructured Data Storage Function (UDSF)
12. 5G-Equipment Identity Register (5G-EIR)
13. Security Edge Protection Proxy (SEPP)
14. Network Data Analytics Function (NWDAF)

1. User Equipment (UE)
2. (Radio) Access Network ((R)AN)
3. User Plane Function (UPF)
4. Data Network (DN)

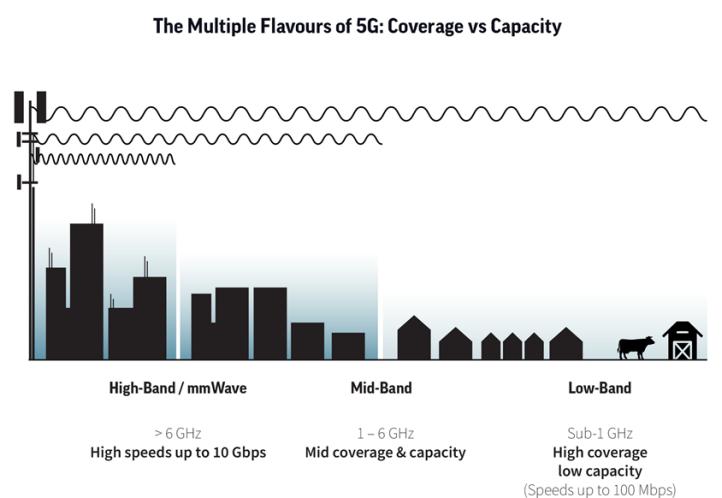
# 5G: a New Radio is required



# Larger spectrum usage to cover all applications



Universal coverage (10's of Mb/s) of reliable connectivity  
Urban coverage with dense small cells (1-3 Gb/s) e.g. mobile Gb/s society, smart cities, option for connected highways  
Hot spots coverage (up to 10 Gb/s) e.g. fixed wireless access, railway stations, sport events, smart factories,

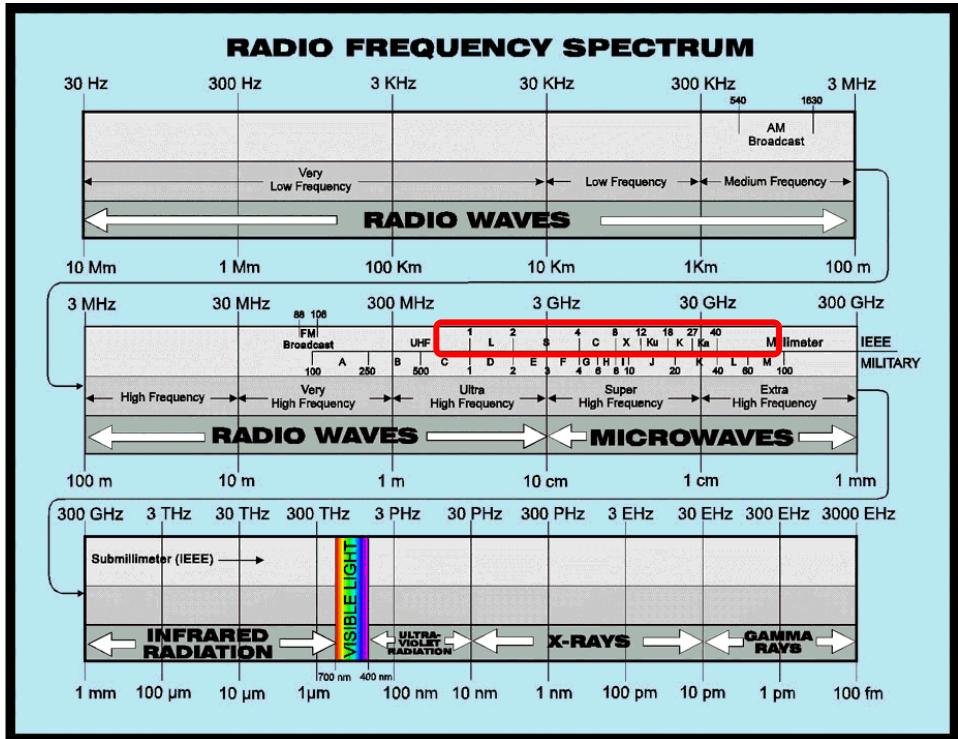


## 5G-NR to operate on a larger spectrum range

- Expanding to lower freqs. for coverage and penetration
- Expanding to higher freqs. for capacity and low latency

# 5G Spectrum

<http://donsnotes.com/tech/em-spectrum.html>



RADIO SPECTRUM POLICY GROUP, "STRATEGIC ROADMAP TOWARDS 5G FOR EUROPE"

"Opinion on spectrum related aspects for next-generation wireless systems (5G)", Nov/16

- <1GHz (e.g. 700MHz)
  - to "enable nationwide and indoor 5G coverage"< 1GHz
- 3400-3800 MHz GHz
  - >100MHz (400MHz) of continuous spectrum
  - to "put Europe at the forefront of the 5G deployment"> 1GHz  
< 6GHz
- 24.25-27.5 GHz
  - "pioneer band for earlier implementation in Europe"
- 31.8-33.4 GHz
  - "looks a promising band which could be made available"
- 40.5-43.5 GHz
  - "is a viable option for 5G in the longer term"> 6GHz

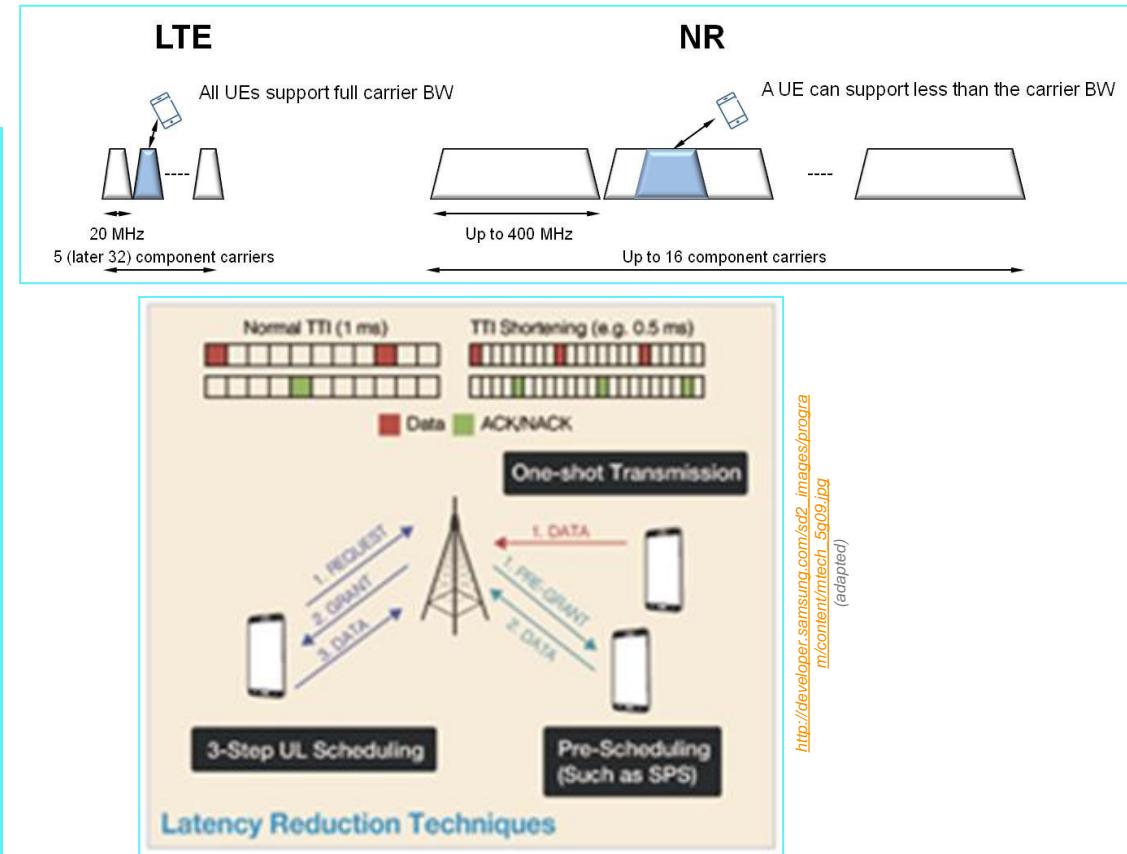
IMT frequencies usage between 24.25 and 86GHz will be analysed at the ITU-T WRC'19 (Nov/19)

| Quantidade de frequência adquirida |               |               |                |                |               |                |                |
|------------------------------------|---------------|---------------|----------------|----------------|---------------|----------------|----------------|
|                                    | Dense Air     | Dixarobil     | MEO            | NOS            | NOWO          | VODAFONE       | TOTAL          |
| 700 MHz                            | 0             | 0             | 10 MHz         | 20 MHz         | 0             | 20 MHz         | <b>50 MHz</b>  |
| 900 MHz                            | 0             | 10 MHz        | 4 MHz          | 4 MHz          |               |                | <b>18 MHz</b>  |
| 1800 MHz                           | 0             | 10 MHz        | 0              | 0              | 20 MHz        | 0              | <b>30 MHz</b>  |
| 2,1 GHz                            | 0             | 0             | 0              | 10 MHz         | 0             | 0              | <b>10 MHz</b>  |
| 2,6 GHz                            | 0             | 35 MHz        | 0              | 0              | 10 MHz        | 0              | <b>45 MHz</b>  |
| 3,6 GHz                            | 40 MHz        | 40 MHz        | 90 MHz         | 100 MHz        | 40 MHz        | 90 MHz         | <b>400 MHz</b> |
| <b>Total</b>                       | <b>40 MHz</b> | <b>95 MHz</b> | <b>104 MHz</b> | <b>134 MHz</b> | <b>70 MHz</b> | <b>110 MHz</b> | <b>553 MHz</b> |

**2021 PT Auction results**

# 5G-NR main characteristics

- Operation from low to very high bands: 0.4 – 100Ghz
  - Including standalone operation in unlicensed bands
- Up to 400 MHz component-carrier bandwidth (20 MHz for LTE)
  - Up to 100MHz in <6GHz
  - Up to 400MHz in >6GHz
- Up to 16 component carriers
- Set of different numerologies for optimal operation in different frequency ranges
- Native support for Low Latency
  - Shortened Transmission Time Interval (TTI)
- Native support for Ultra Reliability (Multiple diversity mechanisms)
- Flexible and modular RAN architecture: split fronthaul, split control-and user-plane
- Support for devices connecting directly, with no network (D2D, V2X)
- Native end-to-end support for Network Slicing
- New channel coding
  - LDPC for data channel, Polar coding for control channel



4G/LTE:

- Turbo codes for data channels
- TBCCs (Tail-Biting Convolutional Codes) for control channels

**LDPC (Low-Density Parity-Check):**

- Improved performance: block error rate (BLER) around or below  $10^{-5}$  for all code sizes and code rates
- Reduced decoding complexity and improved decoding latency (lower overall latency)
- Better area throughput efficiency and higher peak throughput

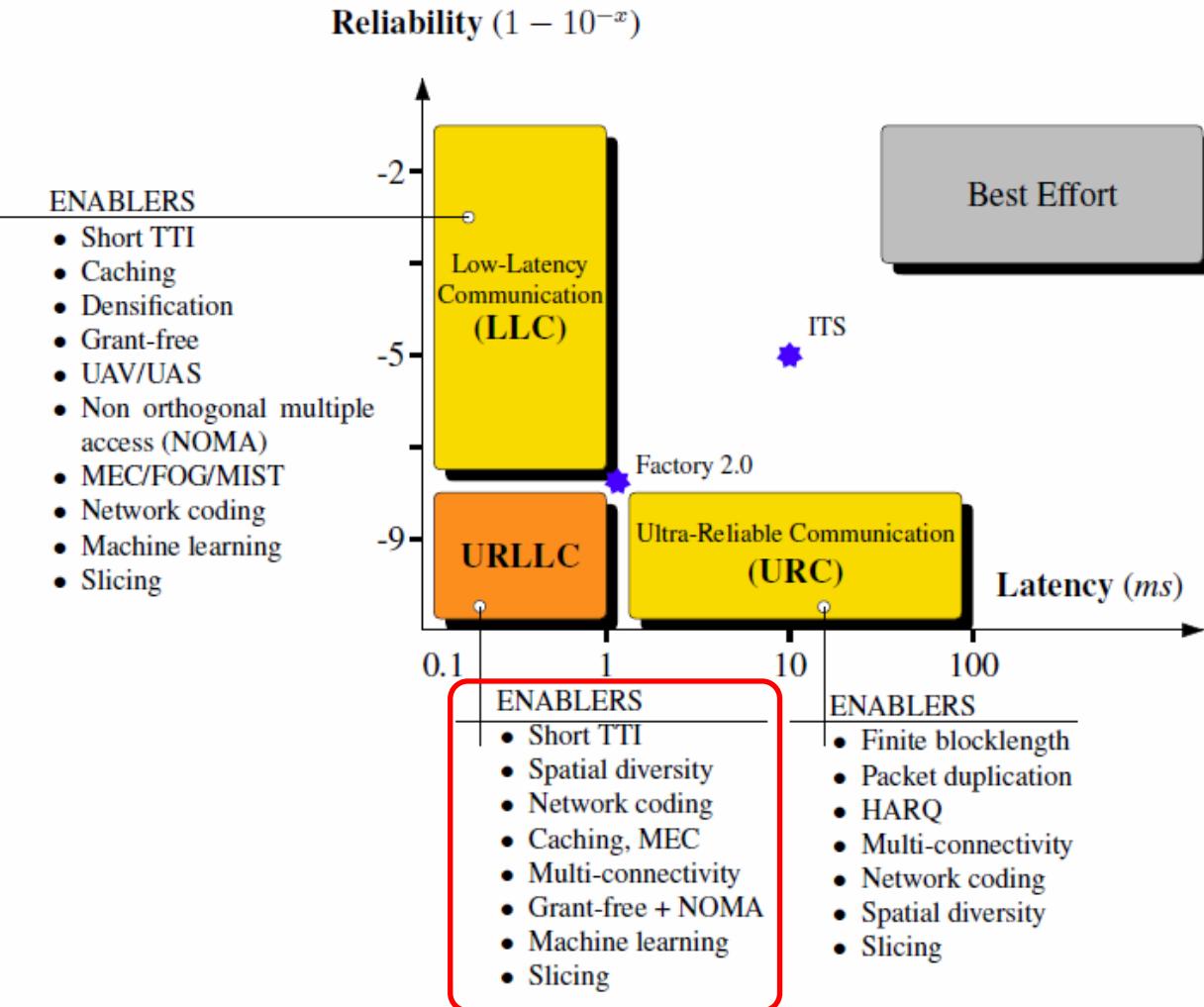
# URLLC: The Ultra Reliability versus Low Latency challenge

Answering two conflicting requirements:  
• **Low latency and ultra-high reliability**

Release 16 objective:

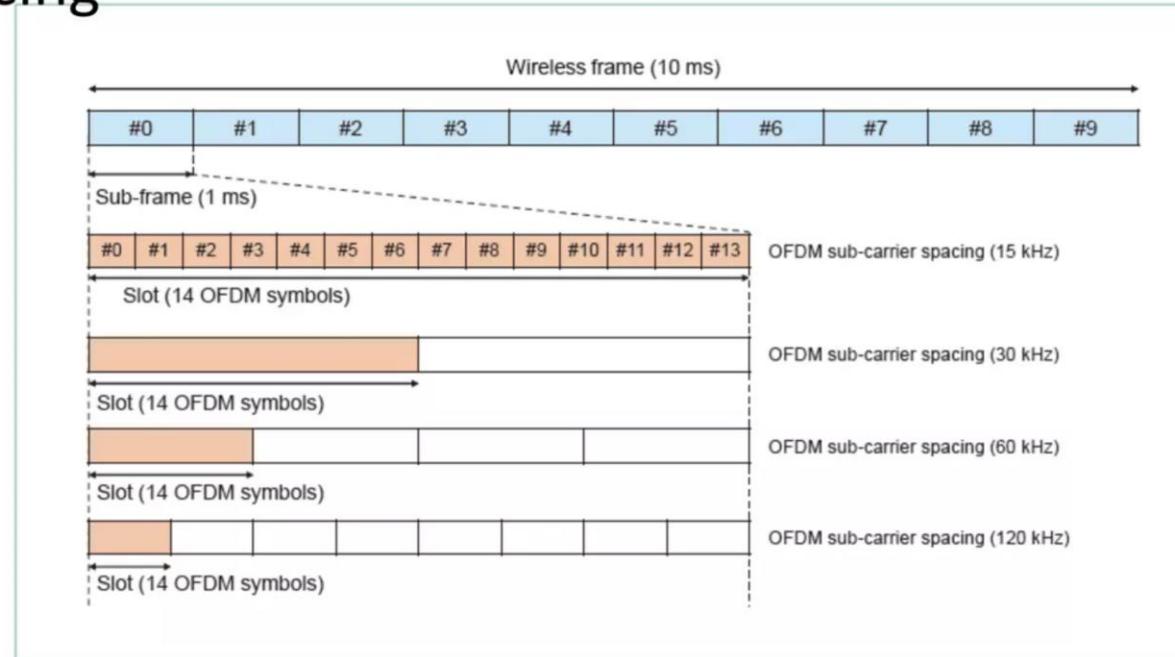
- **0.5-1ms one-way latency**
- **Reliability of up to 99.9999%**

Retransmissions (e.g. HARQ) and packet duplications in time (e.g. PDCP duplications) are useless, considering the low latency budget



# 5G NR Radio Frame

- The 5G NR Radio Frame is in units of 10ms
- Subframes are defined in units of 1ms
- Slots are defines as 14 OFDM Symbols and their time interval depends on sub-carrier spacing



| $\mu$ | $\Delta f = 2^\mu \cdot 15$ [kHz] | Cyclic prefix    |
|-------|-----------------------------------|------------------|
| 0     | 15                                | Normal           |
| 1     | 30                                | Normal           |
| 2     | 60                                | Normal, Extended |
| 3     | 120                               | Normal           |
| 4     | 240                               | Normal           |

Source: NTT Docomo

# 5G NR Logical ,Transport and Physical Channels Mapping

**Logical Channel Definition:** Medium Access Control (MAC) Layer of NR provides services to the Radio Link Control (RLC) Layer in the form of logical channels. A logical channel is defined by the type of information it carries and is generally differentiated as a control channel, used for transmission of control and configuration information or as a traffic channel used for the user data.

List of Logical Channels for NR:

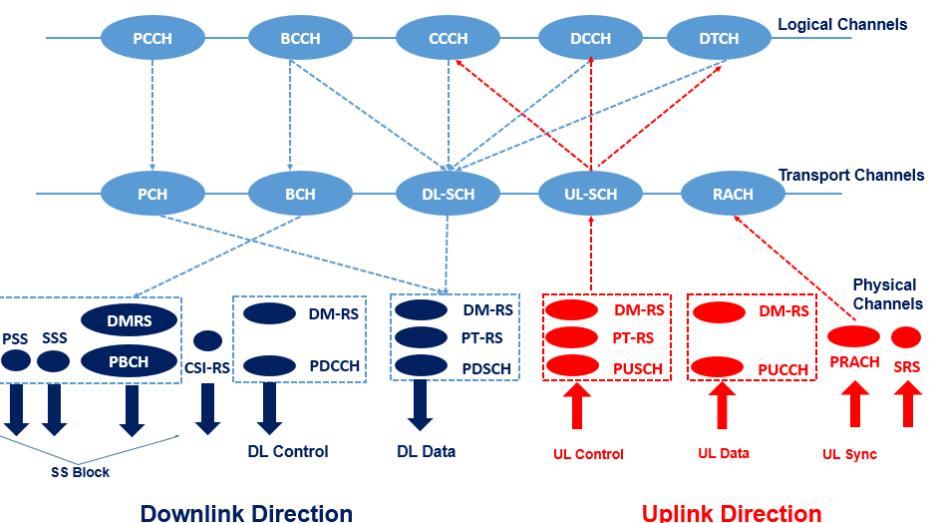
- **Broadcast Control Channel (BCCH):** It is used for transmitting system information from the network to UEs in a cell coverage.
- **Paging Control Channel (PCCH):** This is used to page the UEs whose location at cell level is not known to the network.
- **Common Control Channel (CCCH):** It is used for transmission of control information to UEs with respect to Random Access
- **Dedicated Control Channel (DCCH):** It is used for transmission of control information to/from a UE. This channel is used for individual configuration of UEs such as setting different parameters for different layers.
- **Dedicated Traffic Channel (DTCH):** It is used for transmission of user data to/from a UE. This is the logical channel type used for transmission of all unicast uplink and downlink user data.

**Transport Channel Definition:** A transport channel is defined by how and with what characteristics the information is transmitted over the radio interface. From the physical layer, the MAC layer uses services in the form of transport channels. Data on a transport channel are organized into transport blocks.

List of Transport Channels for NR:

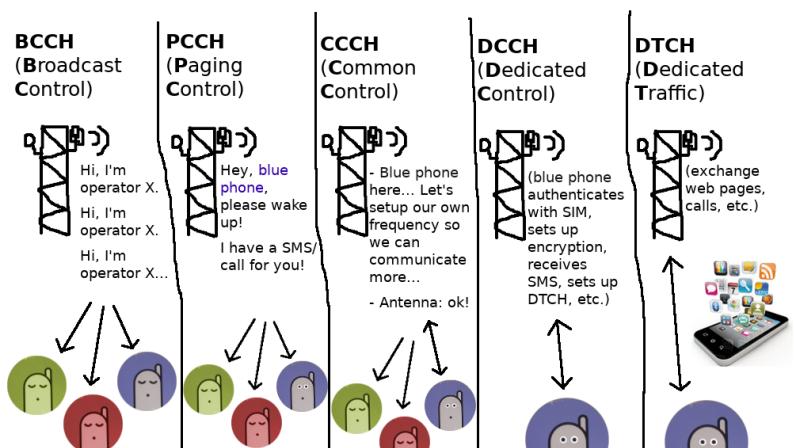
- **Broadcast Channel (BCH) :** It is used for transmitting the BCCH system information, more specifically Master Information Block (MIB). It has a fixed transport format, provided by the specifications.
- **Paging Channel (PCH):** This channel is used for transmission of paging information from the PCCH logical channel. The PCH supports discontinuous reception (DRX) to allow the device to save battery power by waking up to receive the PCH only at predefined time instants.
- **Downlink Shared Channel (DL-SCH) :** This is the main transport channel used for transmitting downlink data in NR. It supports key all NR features such as dynamic rate adaptation and channel aware scheduling, HARQ and spatial multiplexing. DL-SCH is also used for transmitting some parts of the BCCH system info which is not mapped to the BCH. Each device has a DL-SCH per cell it is connected to. In slots where system information is received there is one additional DL-SCH from the device perspective.
- **Uplink Shared Channel (UL-SCH):** This is the uplink counterpart to the DL-SCH that is, the uplink transport channel used for transmission of uplink data.
- **Random-Access Channel (RACH):** RACH is also a transport channel, although it does not carry transport blocks.

## Logical, Transport and Physical Channel Mapping



Downlink Direction

Uplink Direction

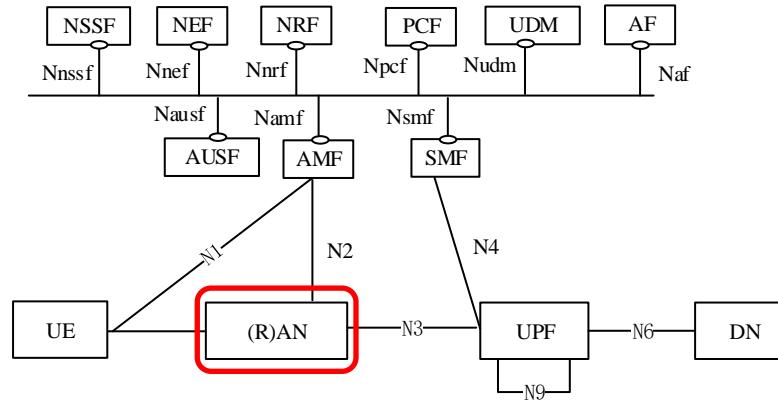


<https://labs.p1sec.com/2019/07/09/presenting-qcsuper-a-tool-for-capturing-your-2g-3g-4g-air-traffic-on-qualcomm-based-phones/>

# RAN

## Radio Access Network (RAN)

- Radio Resources Management (RRM)
- Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling)
- Selection of an AMF at UE attachment
- Routing of User Plane data towards UPF(s)
- Routing of Control Plane information towards AMF
- Connection setup and release
- Scheduling and transmission of paging messages and system broadcast information
- Measurement and measurement reporting configuration for mobility and scheduling
- Transport level packet marking in the uplink
- Session Management
- Support of Network Slicing
- QoS Flow management and mapping to data radio bearers



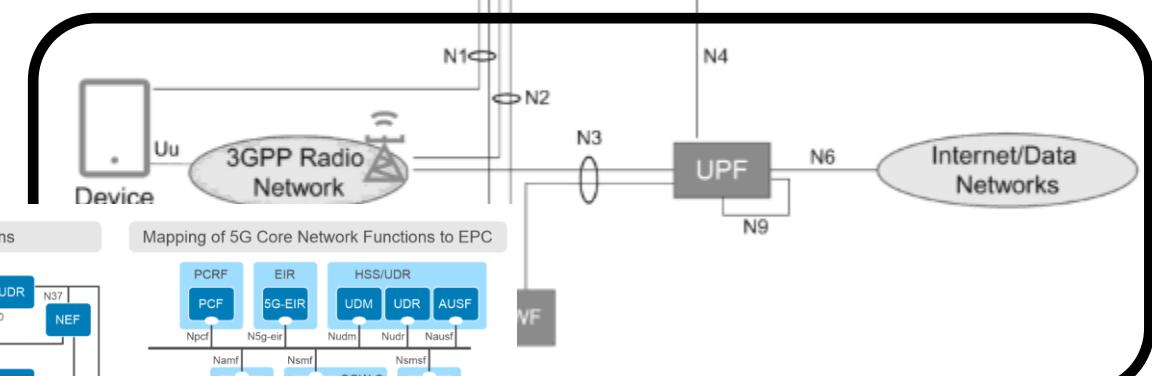
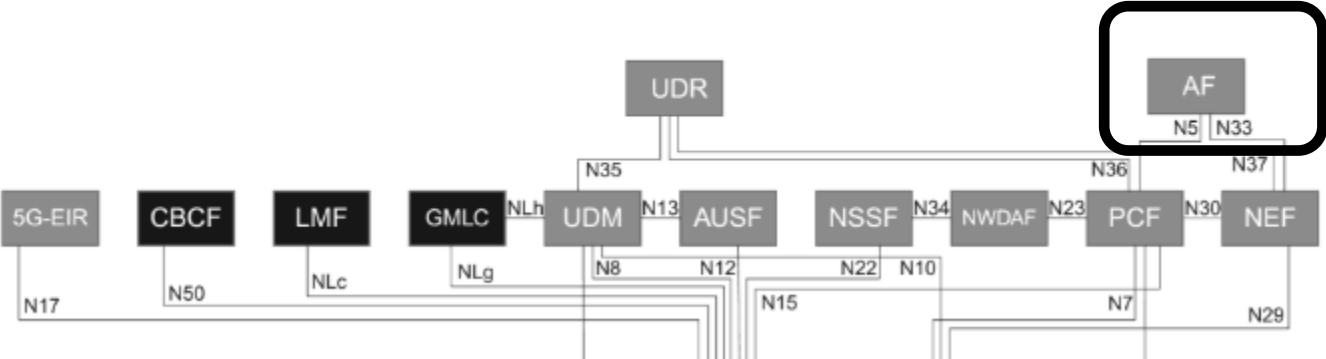
(3GPP TS 23.501)

# The 5G System architecture

- References points representation

- shows the interaction that exist between the NF services in the network
- functions described by point-to-point reference point (e.g. N11)
- between any two network functions (e.g. AMF and SMF)

AF: Application Function  
AUSF: Authentication Server Function  
AMF: Core Access and Mobility Management Function  
DN: Data Network  
LMF: Location Management Function  
NEF: Network Exposure Function  
NRF: Network Repository Function  
NSSF: Network Slice Selection Function  
PCF: Policy Control Function  
SMF: Session Management Function  
UDM: User Data Management  
UPF: User Plane Function



<https://infohub.delltechnologies.com/p/the-5g-core-network-demystified/>

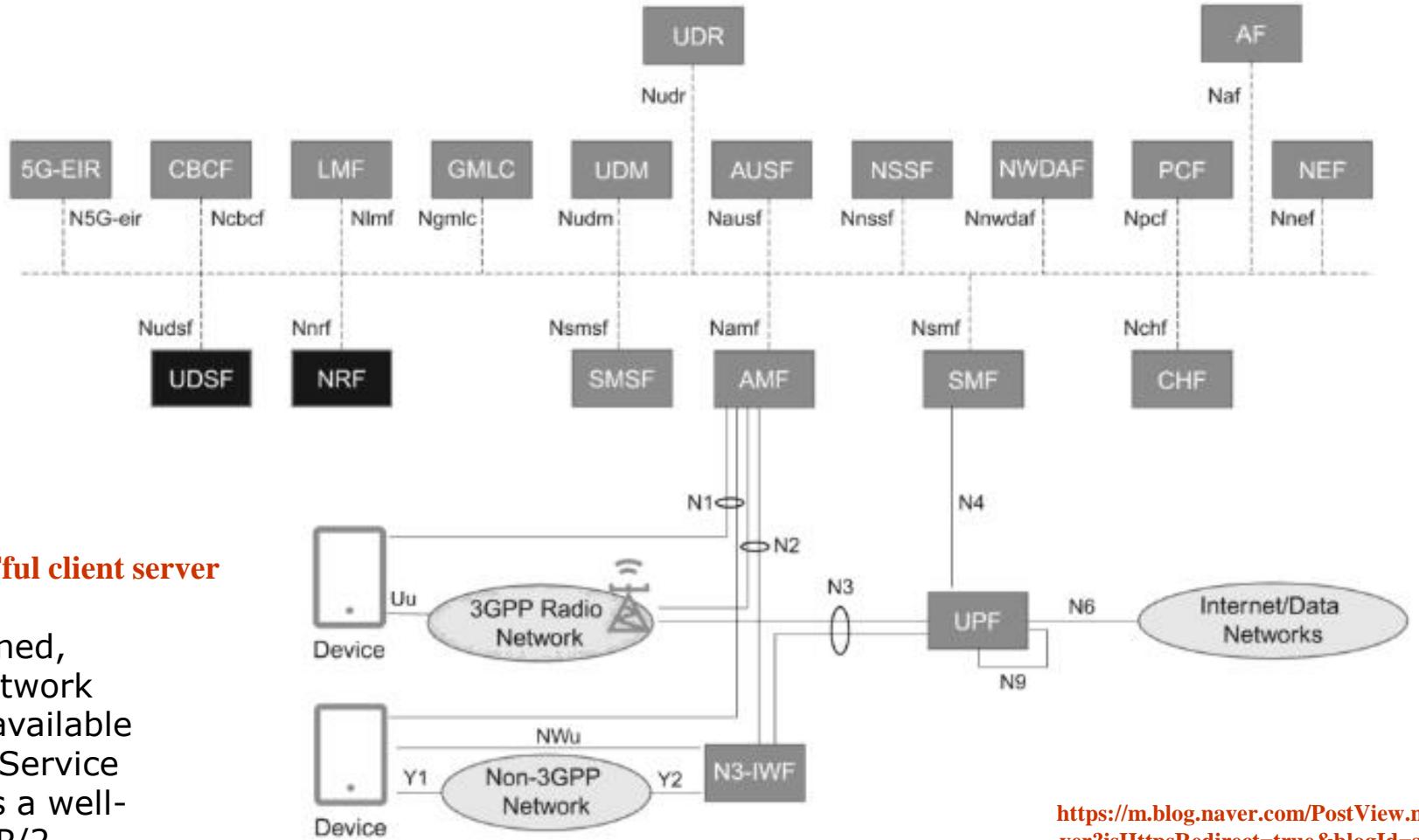
[https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=so\\_ng\\_sec&logNo=222025295180](https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=so_ng_sec&logNo=222025295180)

# The 5G System architecture

**Service based representation where network functions (e.g. AMF) within the control plane enables other authorized network functions to access their services**

NFs follow the web-based approach using RESTful client server communication

Network Functions are self-contained, independent and reusable. Each Network Function service exposes and makes available its functionality (services) through a Service Based Interface (SBI), which employs a well-defined REST interface using HTTP/2.



[https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=song\\_sec&logNo=222025295180](https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=song_sec&logNo=222025295180)

# AMF, SMF and PCF

## Access and Mobility Management Function (AMF)

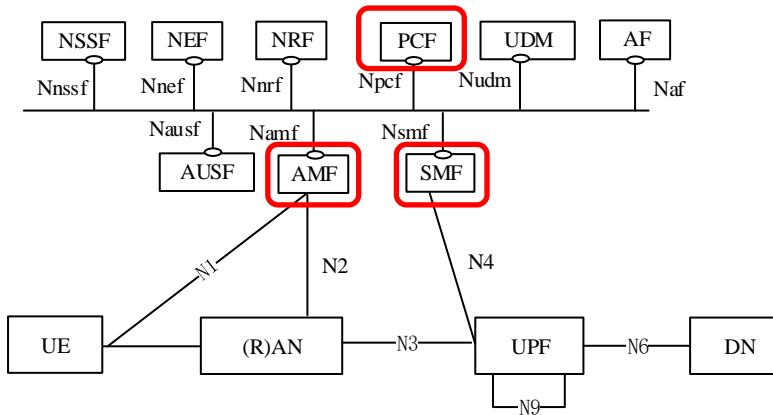
- Termination of NAS (Non-Access Stratum) signalling
- NAS ciphering & integrity protection
- Registration management
- Connection management
- Mobility management
- Access authentication and authorization
- Security context management

## Session Management Function (SMF)

- Session management (establishment, modification, release)
- UE IP address allocation & management
- UPF selection and configuration for QoS and traffic steering
- DHCP functions
- Lawful intercept functions
- Charging data collection and support of charging interfaces

## Policy Control Function (PCF)

- Supports unified policy framework to govern network behaviour
- Provides policy rules to Control Plane function(s) to enforce them
- Accesses subscription information relevant for policy decisions in a Unified Data Repository (UDR)



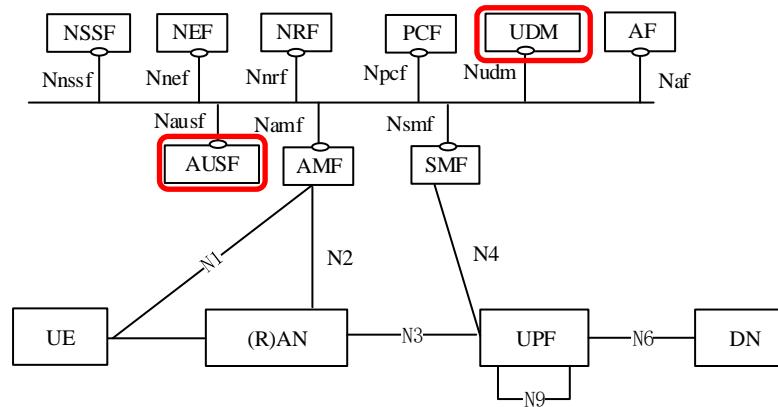
# AUSF and UDM

## Authentication Server Function (AUSF)

- Acts as an authentication server for 3GPP access and untrusted non-3GPP access

## Unified Data Management (UDM)

- Generation of 3GPP Authentication and Key Agreement (AKA) credentials
  - User Identification handling
  - Access authorization based on subscription data
  - Lawful Intercept functionality
  - Subscription management



# NEF, NRF and NSSF

## Network Slice Selection Function (NSSF)

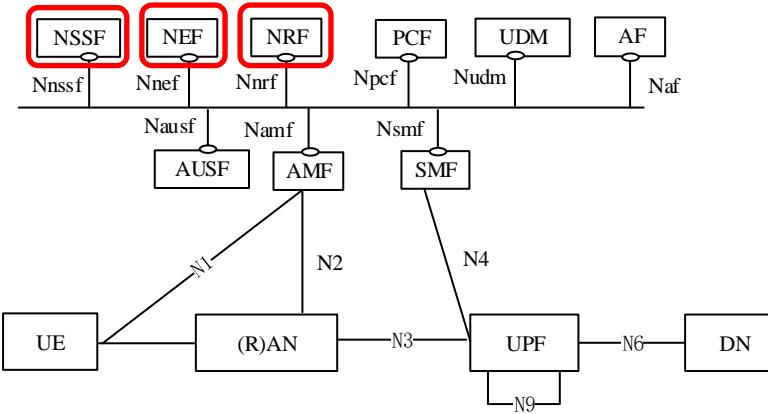
- Selecting of the Network Slice instances serving the UE
- Determining the Allowed NSSAI (*Network Slice Selection Assistance Information*)
- Determining the AMF set to be used to serve the UE

## Network Exposure function (NEF)

- Exposure of capabilities and events
- Secure provision of information from external application to 3GPP network
- Translation of internal/external information

## NF Repository function (NRF)

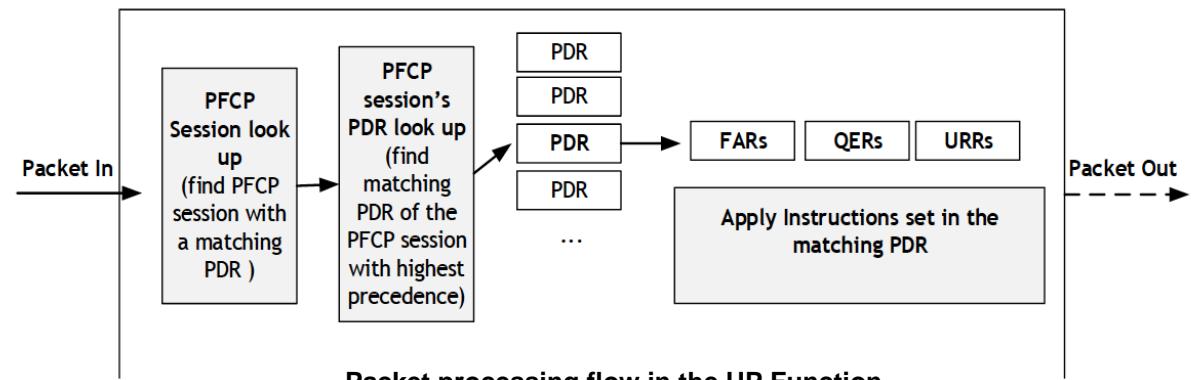
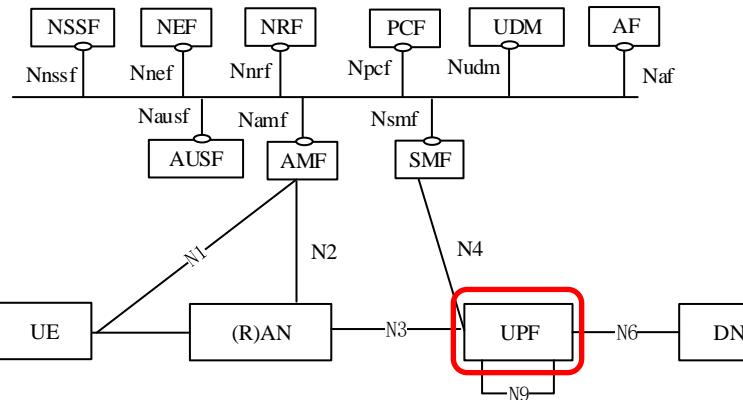
- Supports service discovery function
- Maintains the NF profile of available NF instances and their supported services



# UPF

## User Plane Function (UPF)

- Packet routing & forwarding
- Anchor point for Intra-/Inter-RAT mobility
- External PDU session point of interconnect to Data Network
- Packet inspection and User plane part of Policy rule enforcement
- Lawful intercept (UP collection)
- Traffic usage reporting
- Uplink classifier (ULCL) to support routing traffic flows to a data network
- QoS handling for user plane, e.g. packet filtering, gating, UL/DL rate enforcement
- Transport level packet marking in the uplink and downlink
- Downlink packet buffering and downlink data notification triggering



Sent from SMF to UPF in PFCP

- Packet Detection Rule (PDR):** This rule instructs the UPF how to detect incoming user data traffic (PDUs) and how to classify the traffic. The PDR contains Packet Detection Information (e.g., IP filters) used in the traffic detection and classification. There are separate PDRs for uplink and downlink.
- QoS Enforcement Rule (QER):** This rule contains information on how to enforce QoS, e.g., bit rate parameters.
- Usage Reporting Rule (URR):** This rule contains information on how the UPF shall measure (e.g., count) packets and bytes and report the usage to the SMF. The URR also contains information on events that shall be reported to SMF.
- Forwarding Action Rule (FAR):** This rule contains information for how a packet (PDU) shall be forwarded by the UPF, e.g., towards the Data Network in uplink or towards RAN in downlink.

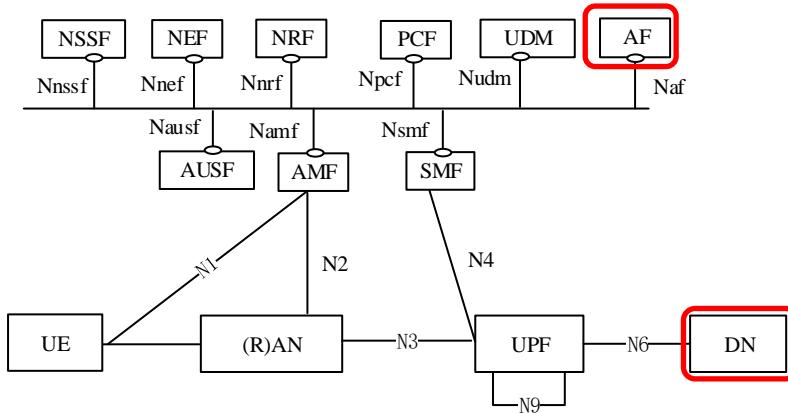
# AF and DN

## Application Function (AF)

- Application influence on traffic routing
- Accessing Network Exposure Function
- Interacting with the Policy framework for policy control

## Data Network (DN)

- Operator services
- Internet access
- 3rd party services
- **May be a Local Area Data Network (LADN):**
  - a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific **Data Network Name (DNN)**, and whose availability is provided to the UE.



# Data storage

## Unstructured Data Storage Function (UDSF) Unified Data Repository (UDR)

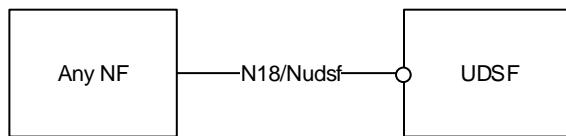


Figure 4.2.5-1: Data storage architecture for unstructured data from any NF (3GPP TS 23.501)

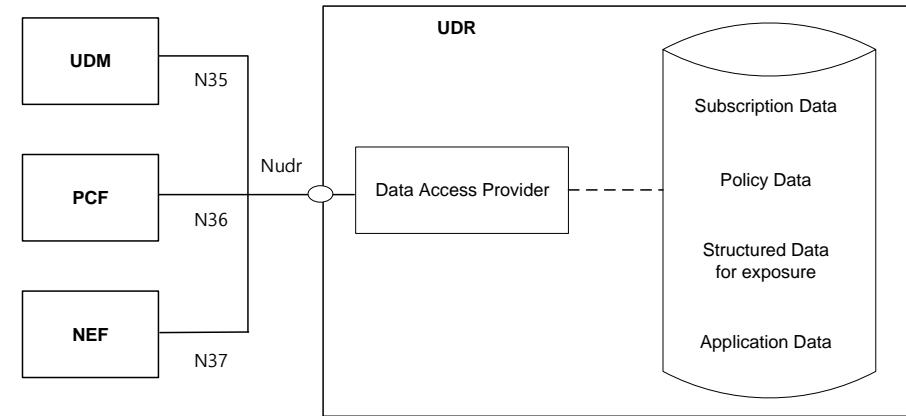
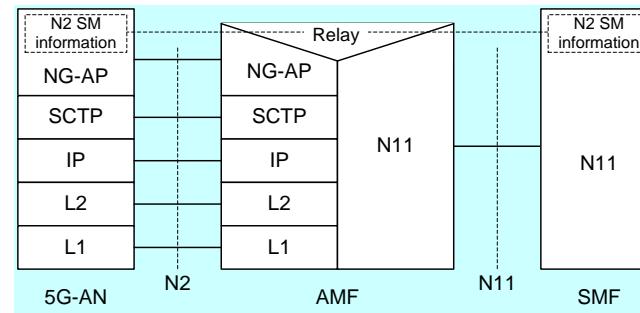
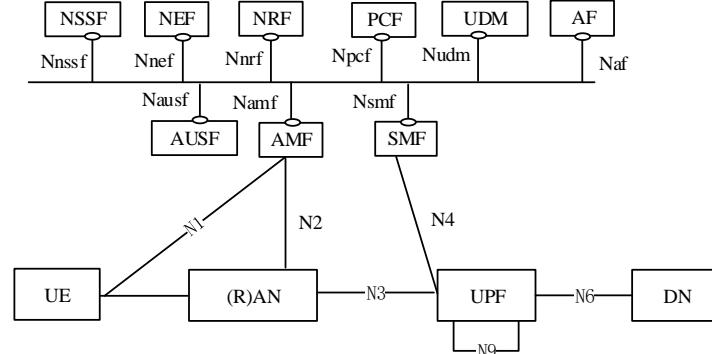
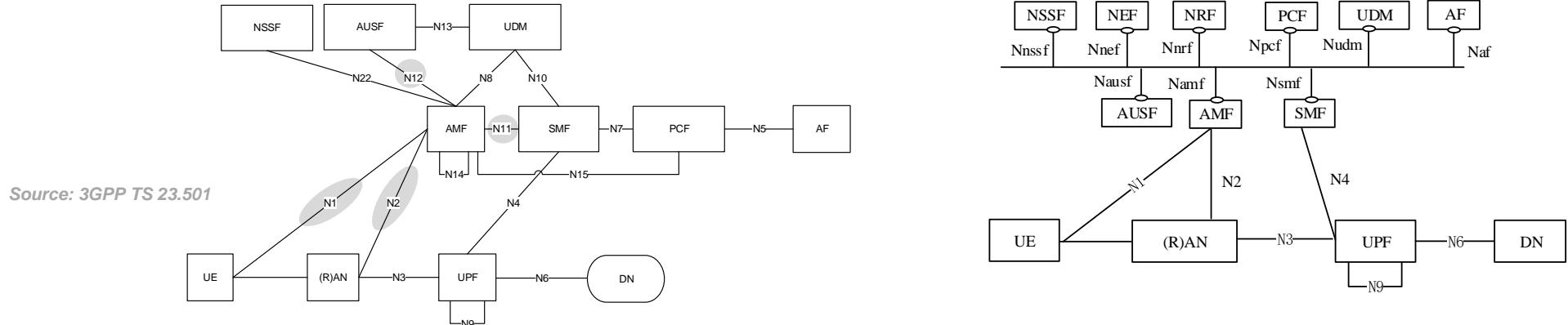
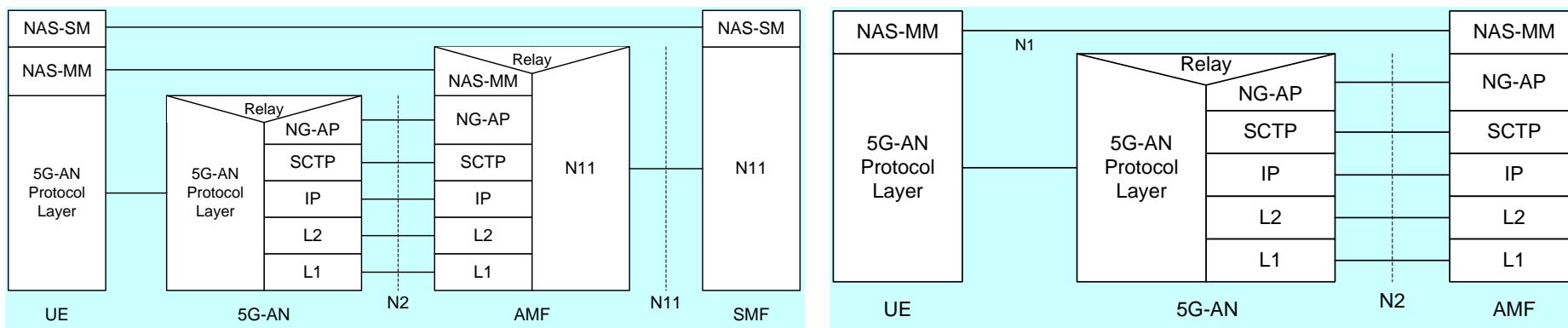


Figure 4.2.5-2: Data storage architecture (3GPP TS 23.501)

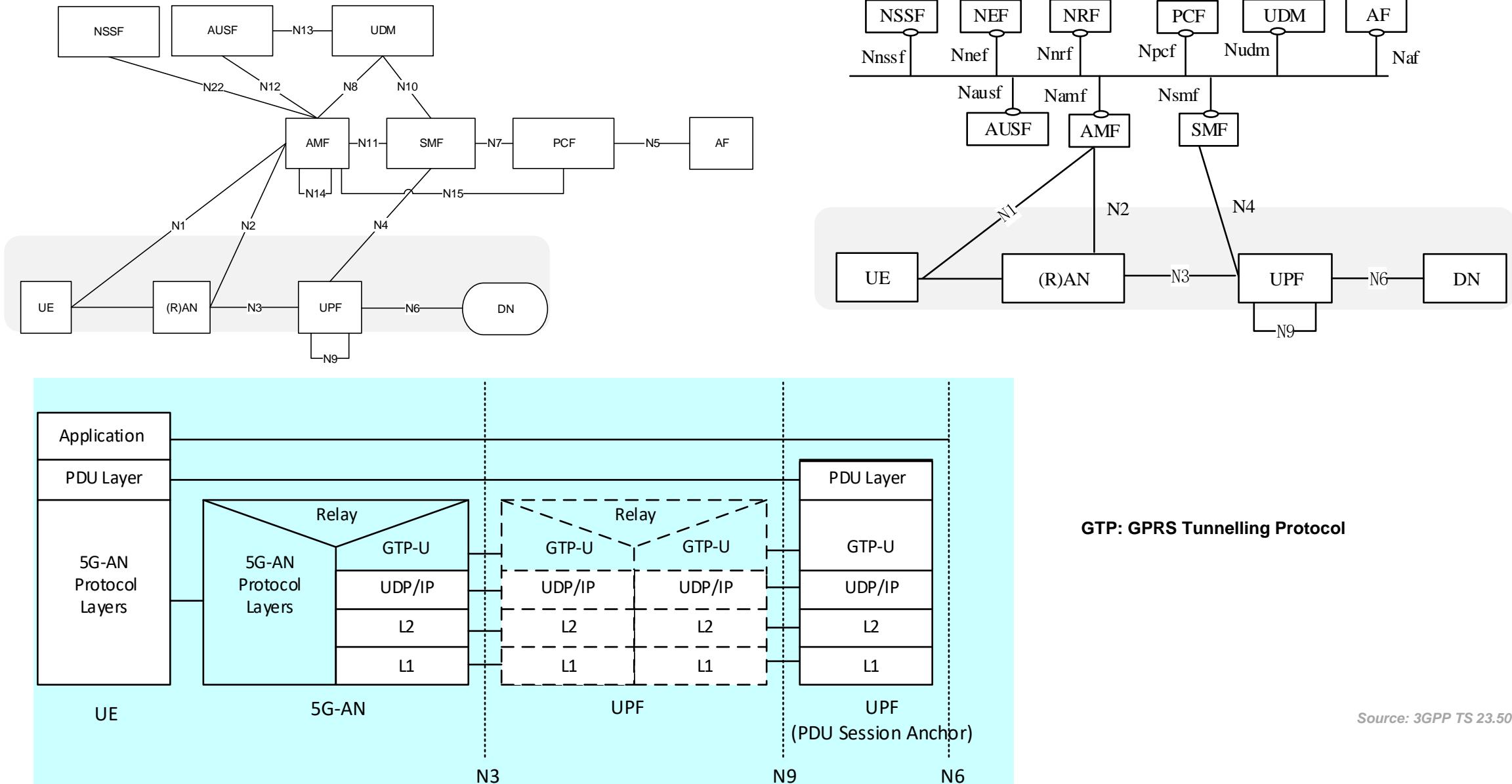
# Protocol stacks – control plane



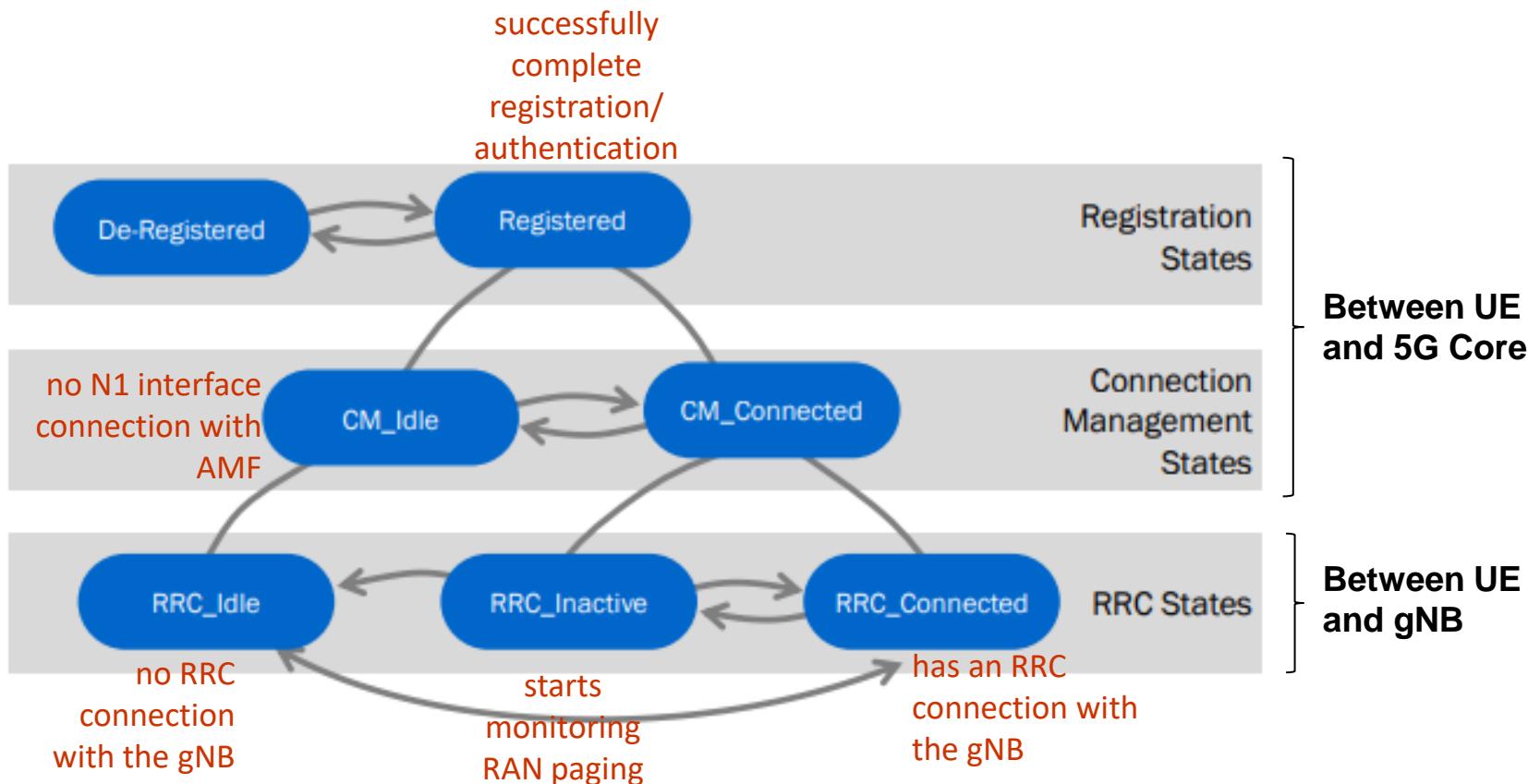
**SCTP:** Stream Control Transmission Protocol  
**PFCP:** Packet Forwarding Control Protocol  
**NG-AP:** NG Application Protocol  
**NAS-MM:** NAS Mobility Management  
**NAS-SM:** NAS Session Management  
**NAS:** Non-Access-Stratum



# Protocol stacks – user plane

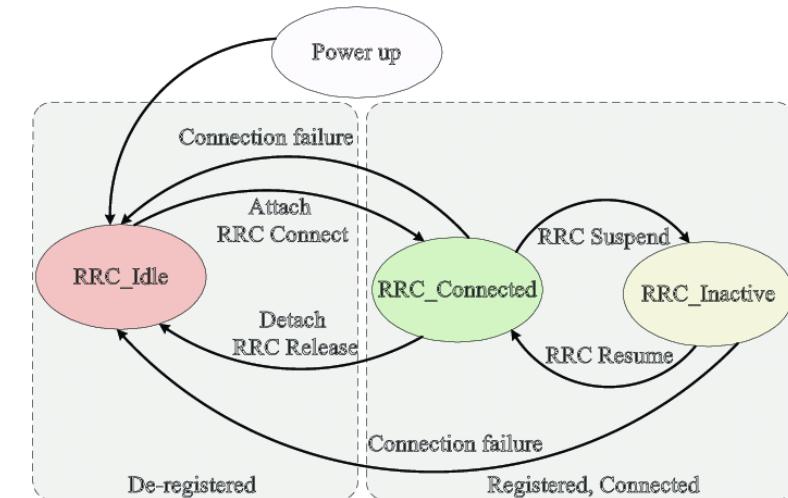


# UE states in 5G



Between UE and 5G Core

Between UE and gNB



[https://www.researchgate.net/figure/UE-state-machine-and-state-transitions-in-5G-78\\_fig3\\_350202251](https://www.researchgate.net/figure/UE-state-machine-and-state-transitions-in-5G-78_fig3_350202251)

# 5G Procedures

3GPP, TS 23.502, "Procedures for the 5G System (5GS)"

## 4 System procedures

- ▷ 4.1 General
- ▷ 4.2 Connection, Registration and Mobility Management procedures
- ▷ 4.3 Session Management procedures
- ▷ 4.4 SMF and UPF interactions
- ▷ 4.5 User Profile management procedures
- ▷ 4.6 Security procedures
- ▷ 4.7 ME Identity check procedure
- ▷ 4.8 RAN-CN interactions
- ▷ 4.9 Handover procedures
  - 4.10 NG-RAN Location reporting procedures
  - ▷ 4.11 System interworking procedures with EPC
  - ▷ 4.12 Procedures for Untrusted non-3GPP access
  - ▷ 4.12a Procedures for Trusted non-3GPP access
  - ▷ 4.12b Procedures for devices that do not support 5GC NAS over WLAN access
  - ▷ 4.13 Specific services
  - ▷ 4.14 Support for Dual Connectivity
  - ▷ 4.15 Network Exposure
  - ▷ 4.16 Procedures and flows for Policy Framework
  - ▷ 4.17 Network Function Service Framework Procedure
  - ▷ 4.18 Procedures for Management of PFDs
  - ▷ 4.19 Network Data Analytics
  - ▷ 4.20 UE Parameters Update via UDM Control Plane Procedure
    - 4.21 Secondary RAT Usage Data Reporting Procedure
  - ▷ 4.22 ATSSS Procedures
  - ▷ 4.23 Support of deployments topologies with specific SMF Service Areas
  - ▷ 4.24 Procedures for UPF Anchored Data Transport in Control Plane CloT 5GS Optimisation
  - ▷ 4.25 Procedures for NEF based Non-IP Data Delivery
  - ▷ 4.26 Network Function/NF Service Context Transfer Procedures
  - ▷ 4.27 Procedures for Enhanced Coverage Restriction Control via NEF

- **Connection, Registration and Mobility Management procedures**
- **Session Management**
  - **PDU Session Establishment**
  - **PDU Session Modification**
  - **PDU Session Release**
  - **Session continuity, service continuity and UP path management**
- **Handover procedures**
- **Procedures for Trusted/Untrusted non-3GPP access**

# 5G Security Parameters

- **Auth Method**
  - **5G-AKA or EAP-AKA'**
- **K: Long term 128 bit authentication key**
  - **Provisioned in the USIM (UE) and Operator (UDR)**
- **Operator Code Type:**
  - **OP: is an identifier assigned to a particular mobile network operator**
  - **OPc: Derived Operator Code, from OP value but unique for each USIM**
- **OP/OPc: Operator Code**
  - **Specific operator key parameters for Milenage and TUAK algorithms**
- **OPv: Operator Key**
  - **Value for OP or OPc**
- **SQN: Sequence Number**
  - **Used during the keys generation**
- **PLMN ID: MCC + MNC**
- **MSIN: Mobile Subscriber Identification Number**
- **SUPI: Subscription Permanent Identifier (not exchanged)**
  - **IMSI (PLMN ID+MSIN):**
  - **NAI**
- **SUCI: Subscriber Concealed Identifier**
  - **Identifier used during the authentication process, avoiding SUPI exchange**
- **GUTI: 5G Globally Unique Temporary Identity**
  - **Used in 5G as a means to keep the subscriber's IMSI confidential**

Free5GC subscriber creation example

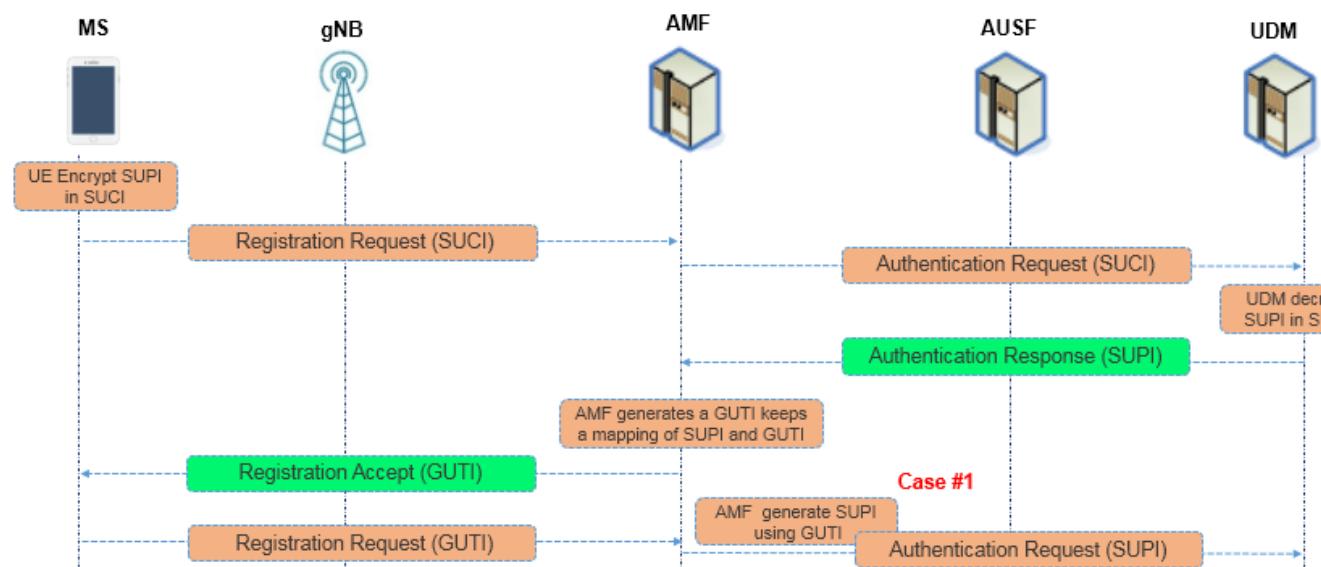
The screenshot shows a web-based interface for creating a new subscriber in the Free5GC system. The URL is 10.0.123.201:5000/#/subscriber. The main header has tabs for REALTIME STATUS, SUBSCRIBERS, and ANALYTICS. A sidebar on the right has a 'New Subscriber' button. The central 'New Subscriber' form contains the following fields:

- PLMN ID\***: 00101
- SUPI (IMSI)\***: 001010000000011
- Authentication Method\***: 5G\_AKA
- K\***: 8ba473f2f8fd09487cccbd7097c6862
- Operator Code Type\***: OPc
- Operator Code Value\***: 8e27b6af0e692e750f32667a3b14605d
- SQN\***: 16f3b3f70fc2
- S-NSSAI Configuration** section includes:
  - snssai**: snssai
  - SST\***: 1
  - SD\***: 010203
  - Default S-NSSAI
- DNN Configurations** section includes:
  - Data Network Name\***: internet
  - Uplink AMBR\***: 10 Mbps
  - Downlink AMBR\***: 20 Mbps
  - Default 5QI**: 9
- Flow Rules** section with three '+' buttons for adding new rules.

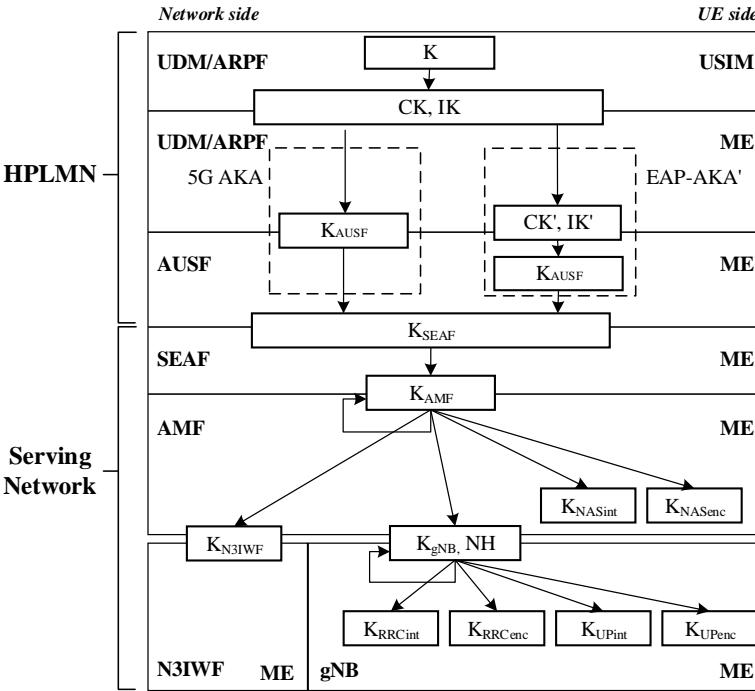
At the bottom right of the form is a **Submit** button.

# Authentication process

- Primary authentication:
  - Mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures
- Primary authentication offers two mechanisms:
  - (1) *5G Authentication and Key Agreement (5G AKA)*
  - (2) *Extensible Authentication Protocol AKA' (EAP-AKA')*

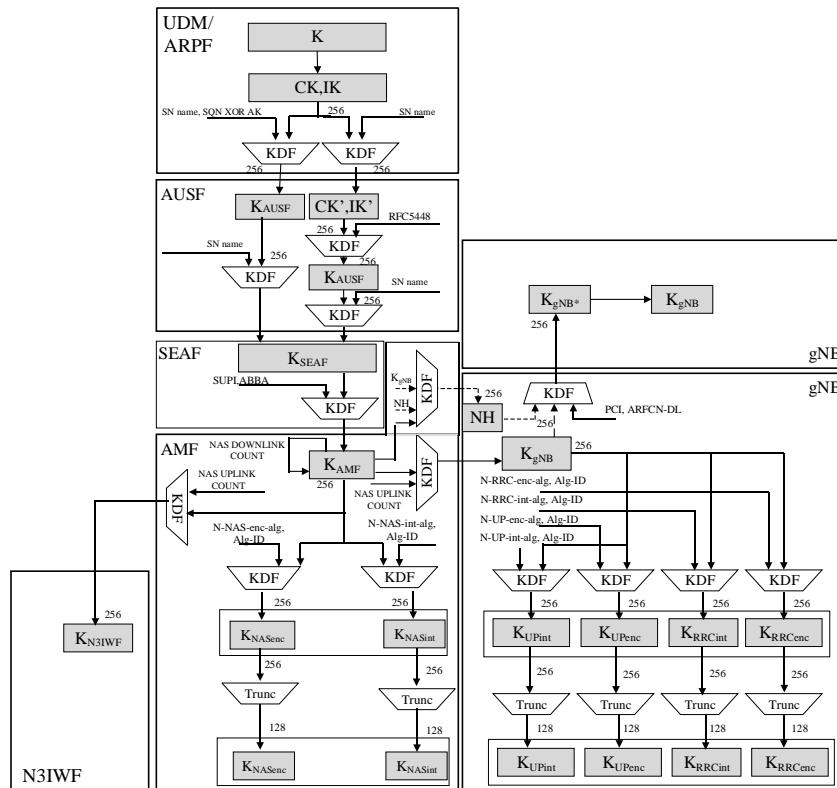


# Keys generation from K

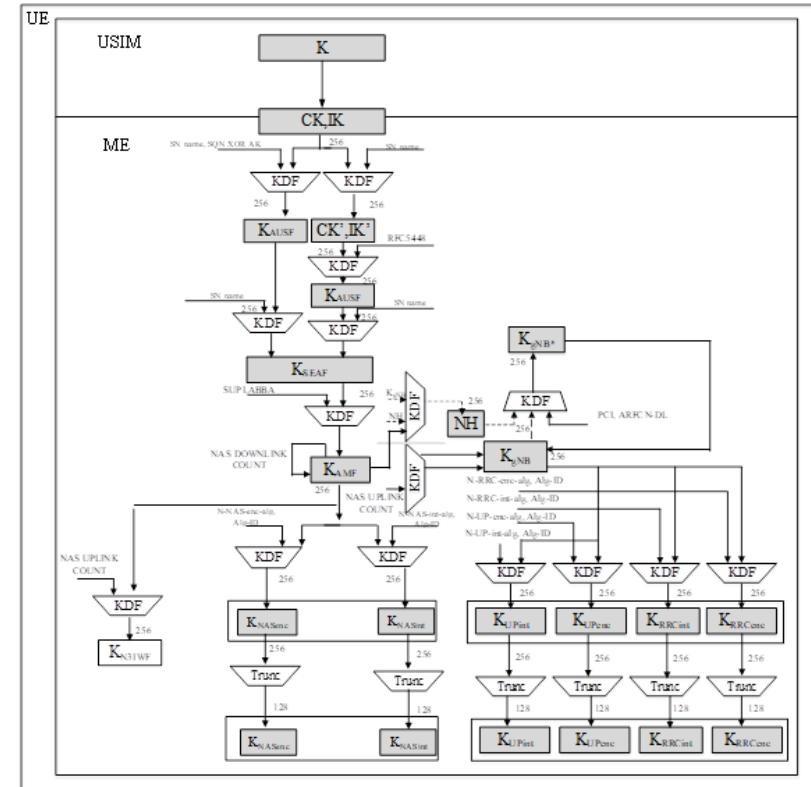


3GPP, TS 33.501, Figure 6.2.1-1: Key hierarchy generation in 5GS

CK: cipher key  
IK: integrity key

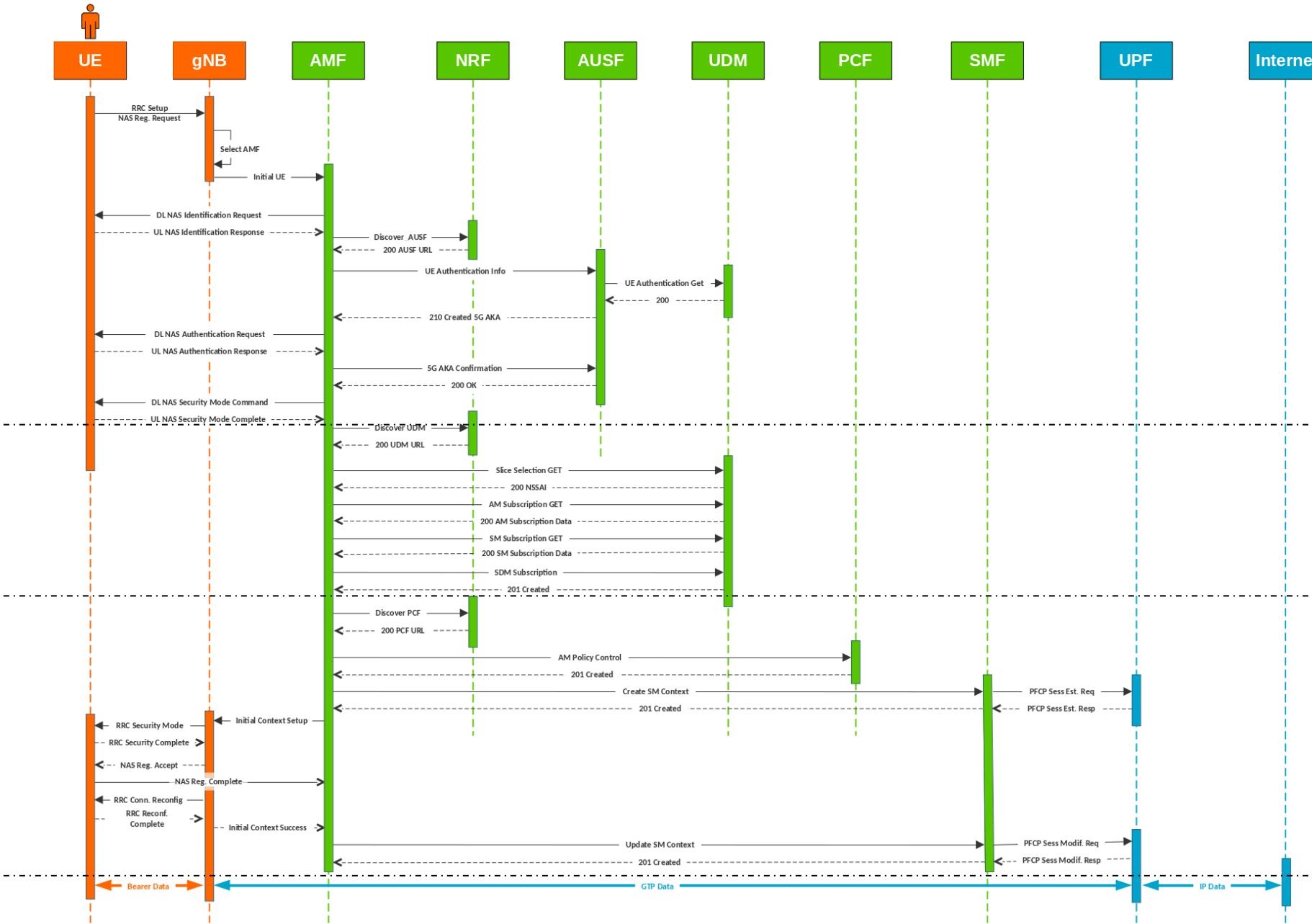


3GPP, TS 33.501, Figure 6.2.2-1:  
Key distribution and key derivation  
scheme for 5G for network nodes



3GPP, TS 33.501, Figure 6.2.2-2:  
Key distribution and key derivation  
scheme for 5G for the UE

## 5G Standalone Registration



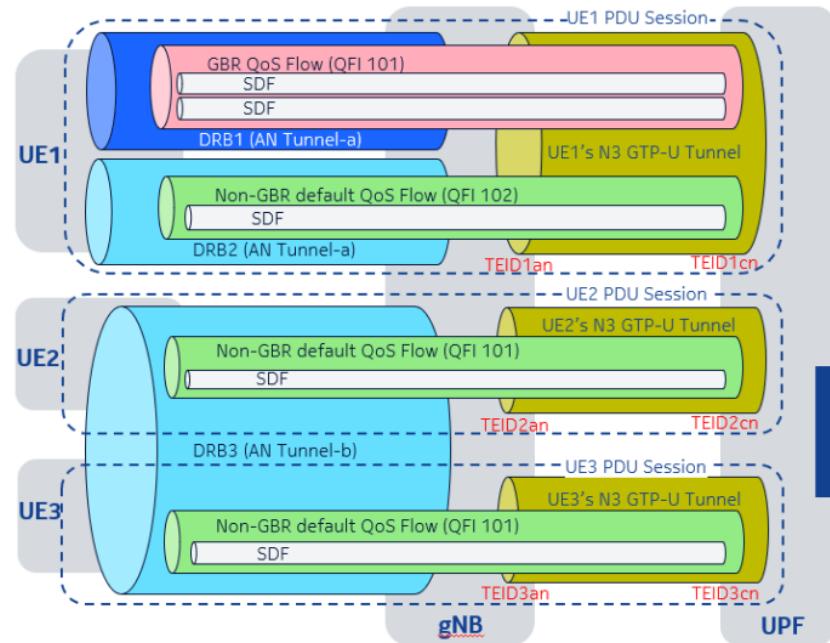
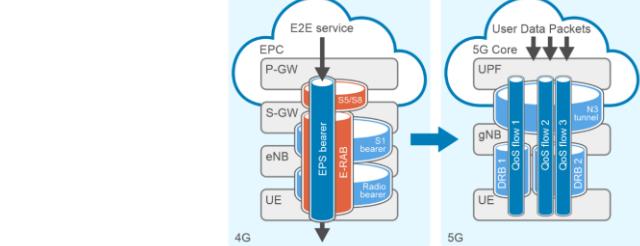
Registration

Slices selection

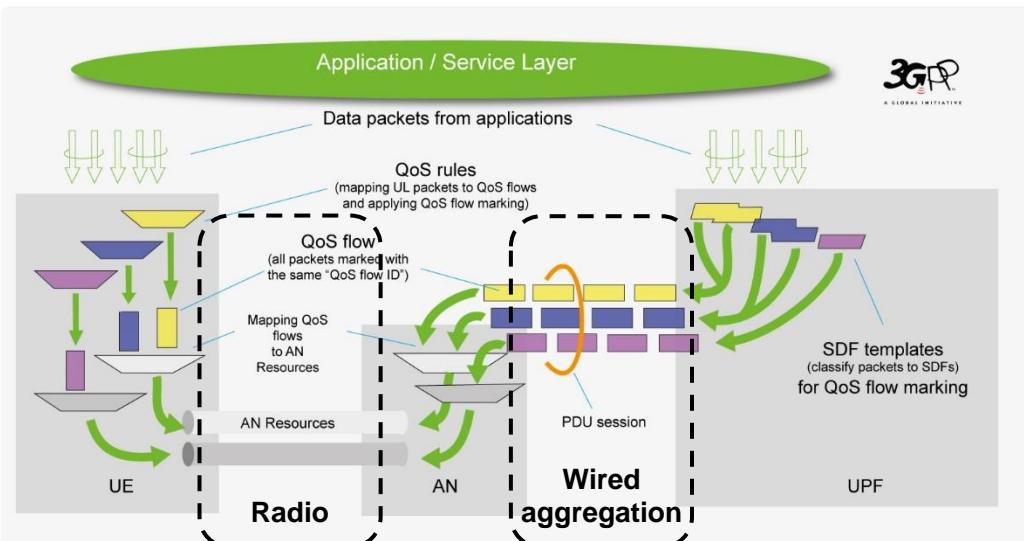
PDUs establishment

Data session

# QoS Model



- AN tunnel for a UE is identified by:
  - gNB's IP address
  - TEID<sub>an</sub>
- CN tunnel for a UE is identified by:
  - UPF's IP address
  - TEID<sub>cn</sub>
- A QoS Flow is mapped to a DRB based on QFI
- PDU Session, QFI, QoS Flow, N3 GTP\_U tunnel, TEID<sub>an</sub> and TEID<sub>cn</sub> are per UE



The QoS profile of a QoS flow contains QoS parameters:

For each QoS flow:

- A 5G QoS Identifier (5QI)
- An Allocation and Retention Priority (ARP)

In case of a GBR QoS flow only:

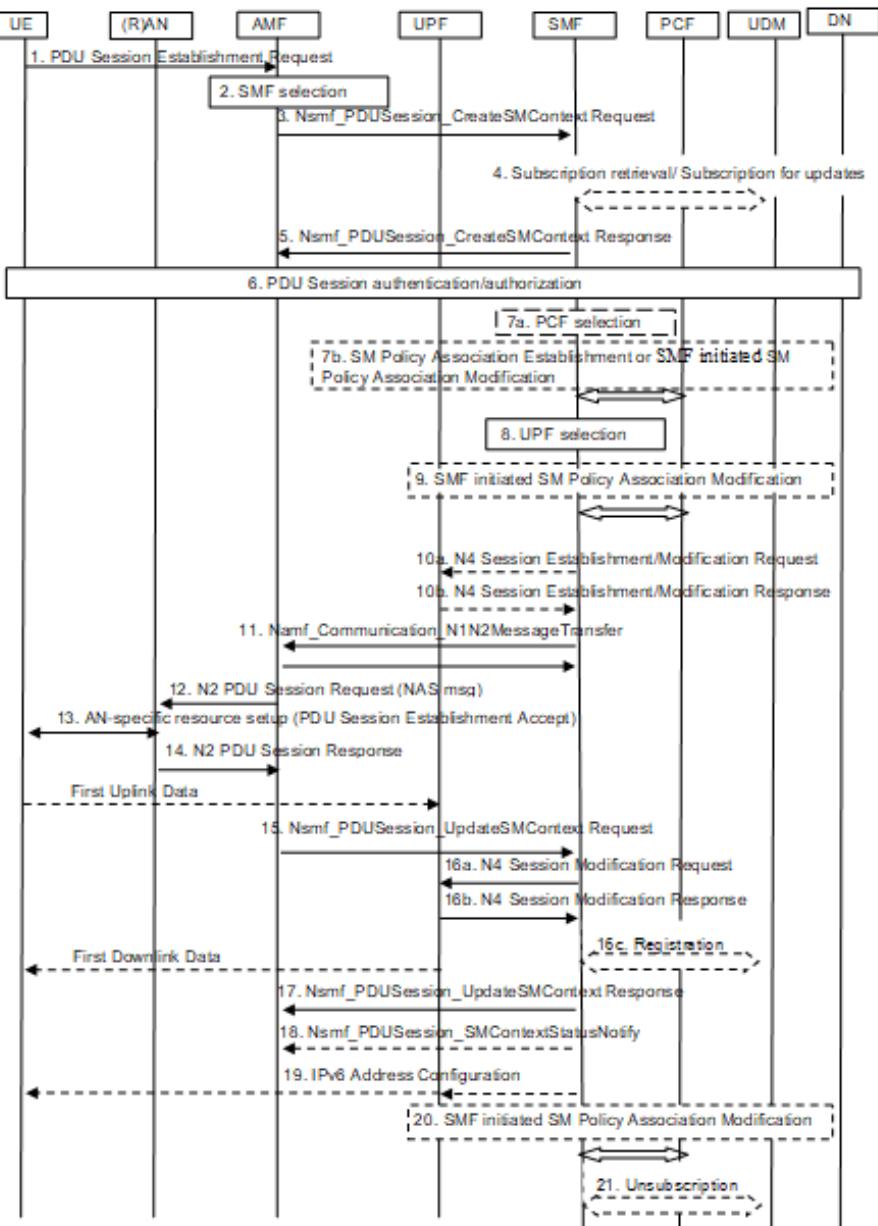
- Guaranteed Flow Bit Rate (GFBR) for both uplink and downlink
- Maximum Flow Bit Rate (MFBR) for both uplink and downlink
- Maximum Packet Loss Rate for both uplink and downlink

In case of Non-GBR QoS only

- Reflective QoS Attribute (RQA): the RQA, when included, indicates that some (not necessarily all) traffic carried on this QoS flow is subject to reflective quality of service (RQoS) at NAS.

## Standardized 5QI to QoS characteristics mapping

| 5QI Value | Resource Type | Priority Level | Packet Delay Budget | Packet Error Rate | Default Averaging Window | Example Services   |
|-----------|---------------|----------------|---------------------|-------------------|--------------------------|--|
| 1         | GBR           | 20             | 100 ms              | $10^{-2}$         | TBD                      | Conversational Voice   |
| 2         |               | 40             | 150 ms              | $10^{-3}$         | TBD                      | Conversational Video (Live Streaming)  |
| 3         |               | 30             | 50 ms               | $10^{-3}$         | TBD                      | Real Time Gaming, V2X messages   |
| 4         |               | 50             | 300 ms              | $10^{-6}$         | TBD                      | Non-Conversational Video (Buffered Streaming)  |
| 65        |               | 7              | 75 ms               | $10^{-2}$         | TBD                      | Mission Critical user plane Push To Talk voice (e.g., MCPTT)   |
| 66        |               | 20             | 100 ms              | $10^{-2}$         | TBD                      | Mission Critical user plane Push To Talk voice   |
| 75        |               | 25             | 50 ms               | $10^{-2}$         | TBD                      | V2X messages   |
| 5         |               | 10             | 100 ms              | $10^{-6}$         | N/A                      | IMS Signalling   |
| 6         |               | 60             | 300 ms              | $10^{-6}$         | N/A                      | Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) |
| 7         |               | 70             | 100 ms              | $10^{-3}$         | N/A                      | Voice, Video (Live Streaming) Interactive Gaming   |
| 8         | Non-GBR       | 80             | 300 ms              | $10^{-6}$         | N/A                      | Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) |
| 9         |               | 90             | 60 ms               | $10^{-6}$         | N/A                      | Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)  |
| 69        |               | 5              | 60 ms               | $10^{-6}$         | N/A                      | Mission Critical Data (e.g., example services are the same as QCI 6/8/9)                                       |
| 70        |               | 55             | 200 ms              | $10^{-6}$         | N/A                      | V2X messages   |
| 79        |               | 65             | 50 ms               | $10^{-2}$         | N/A                      | V2X messages   |



# QoS protocols' flows

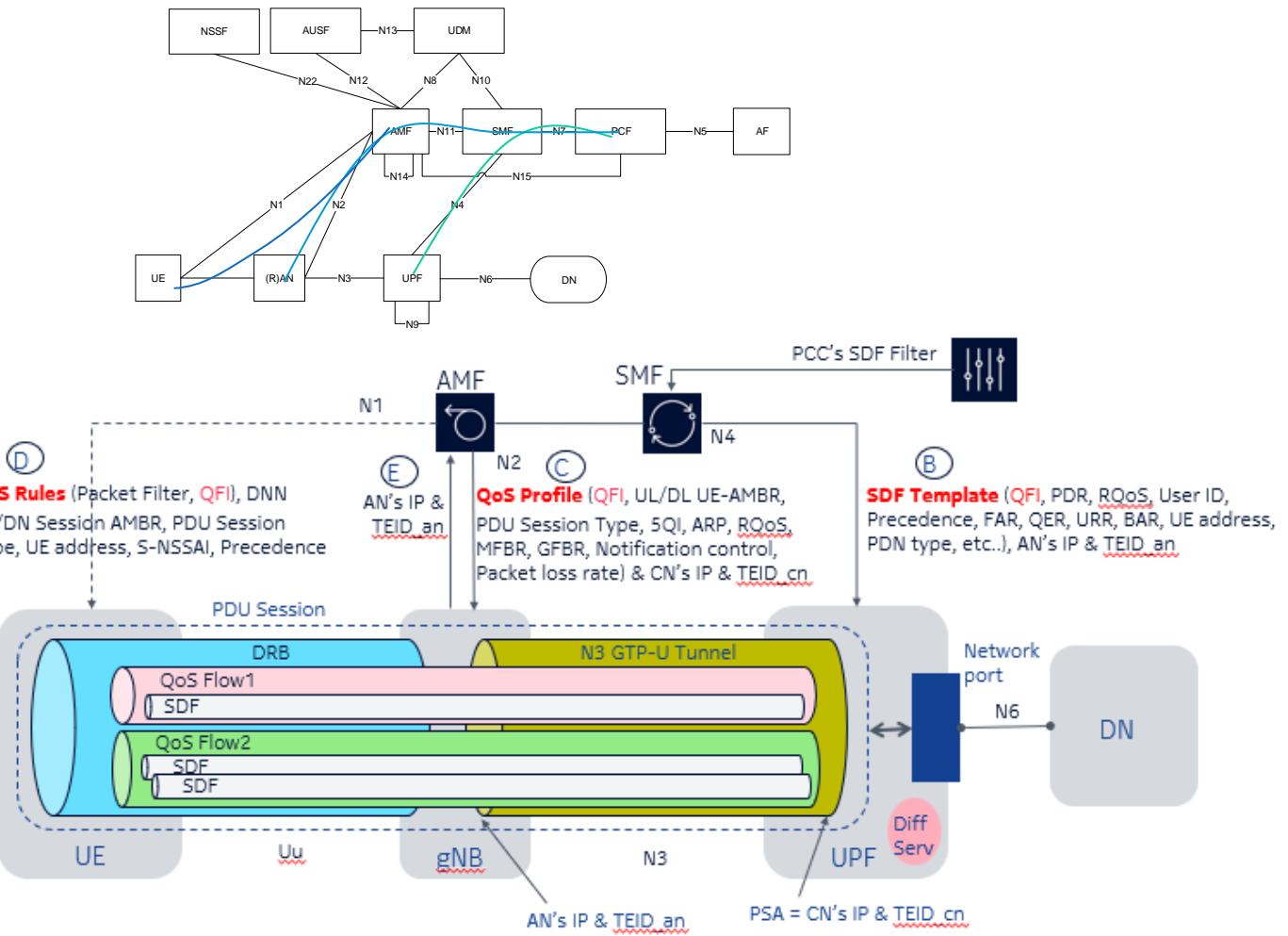
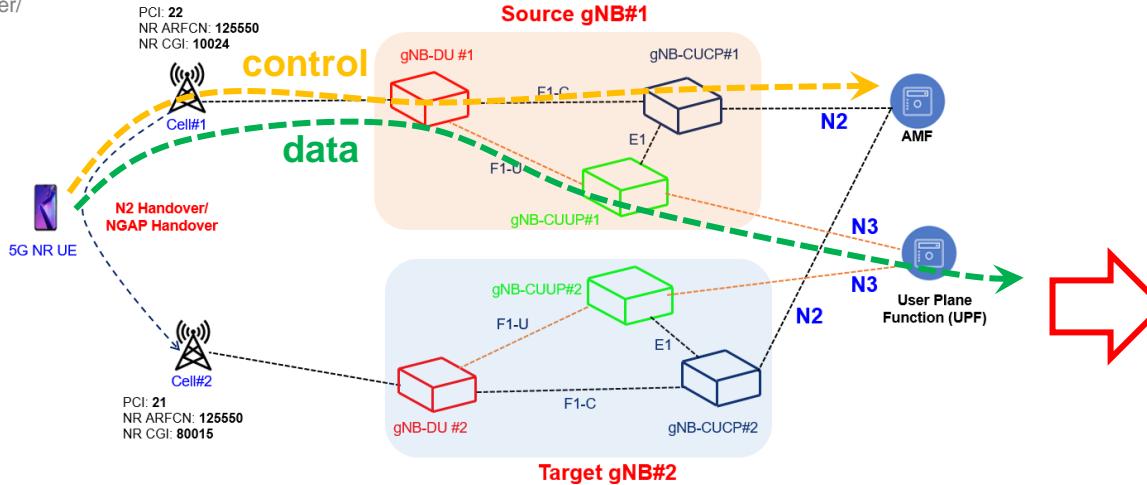


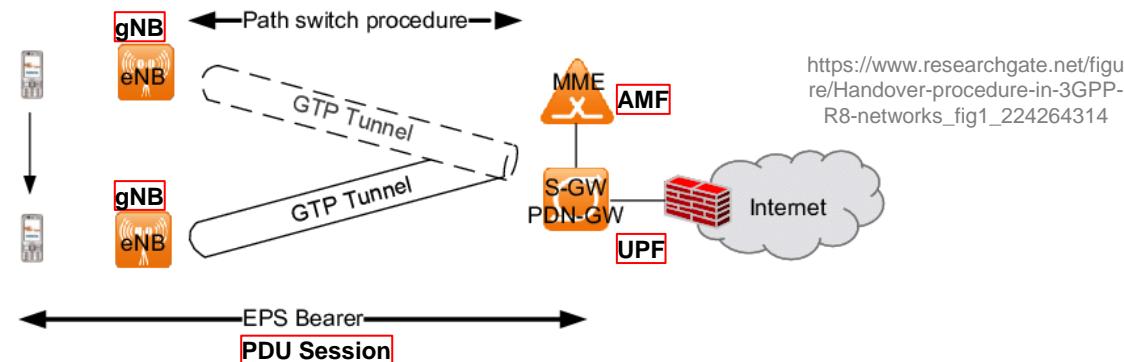
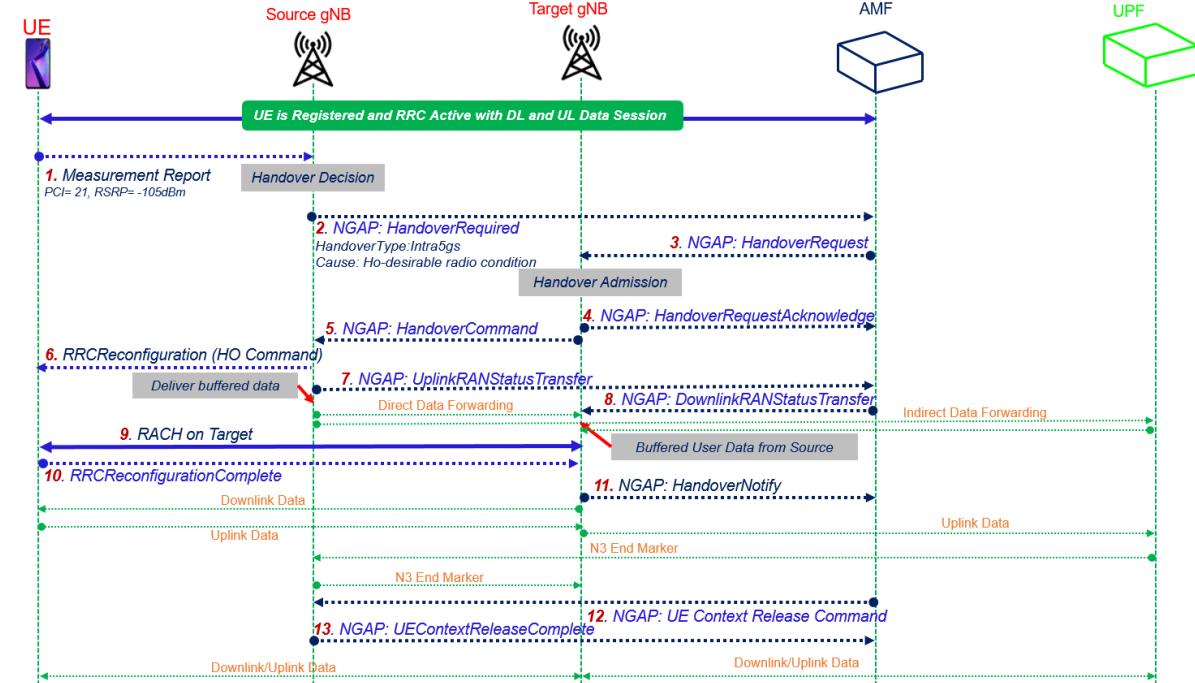
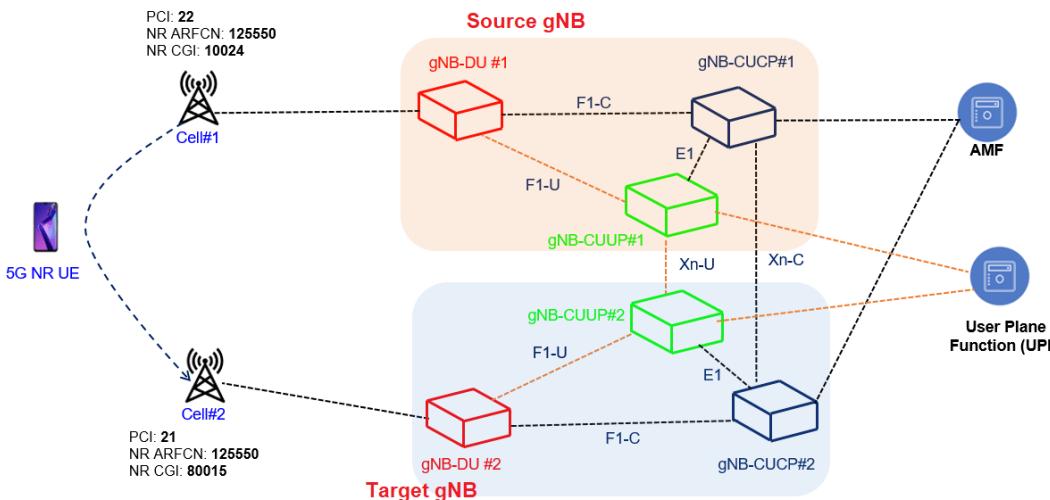
Figure 4.3.2.2.1-1: UE-requested PDU Session Establishment for non-roaming and roaming with local breakout

# Inter gNB mobility in 5G

<https://www.techplayon.com/5g-sa-inter-gnb-handover-n2-or-ngap-handover/>



<https://www.techplayon.com/5g-sa-inter-gnb-handover-xn-handover/>



[https://www.researchgate.net/figure/Handover-procedure-in-3GPP-R8-networks\\_fig1\\_224264314](https://www.researchgate.net/figure/Handover-procedure-in-3GPP-R8-networks_fig1_224264314)

# 5G Slicing

Network Slice definition (TR 23.799): *complete logical network (providing Telecommunication Services and Network Capabilities) including AN and CN.*

**Slicing enables the creation of distinct logical networks:**

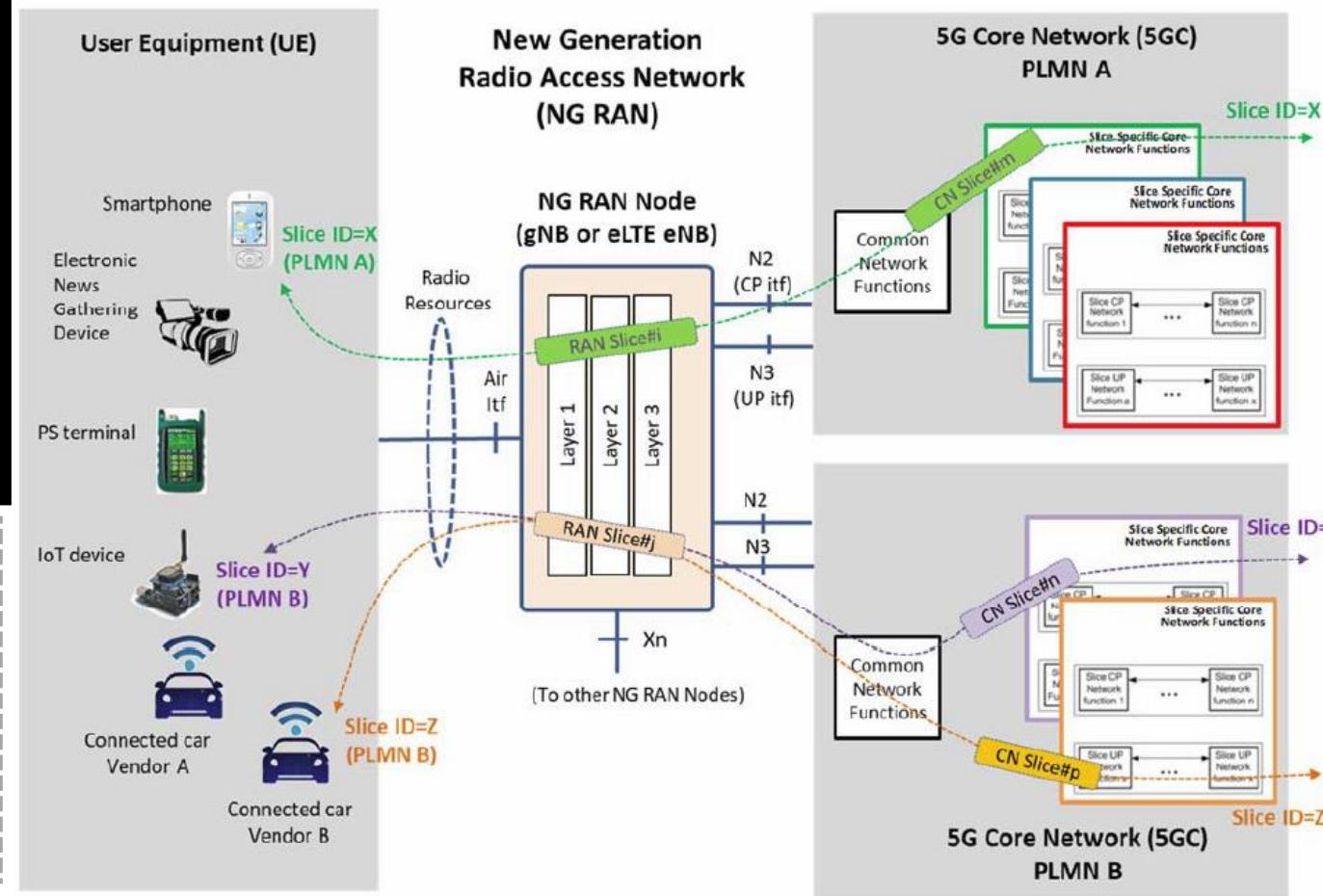
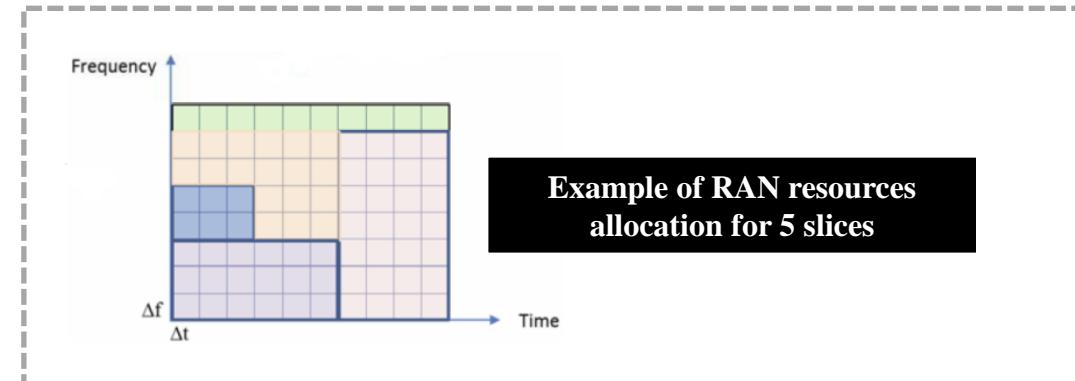
- Of the same type (different businesses)
- Providing differentiated behaviour (different services)

**5G supports end-to-end slicing (radio and core)**

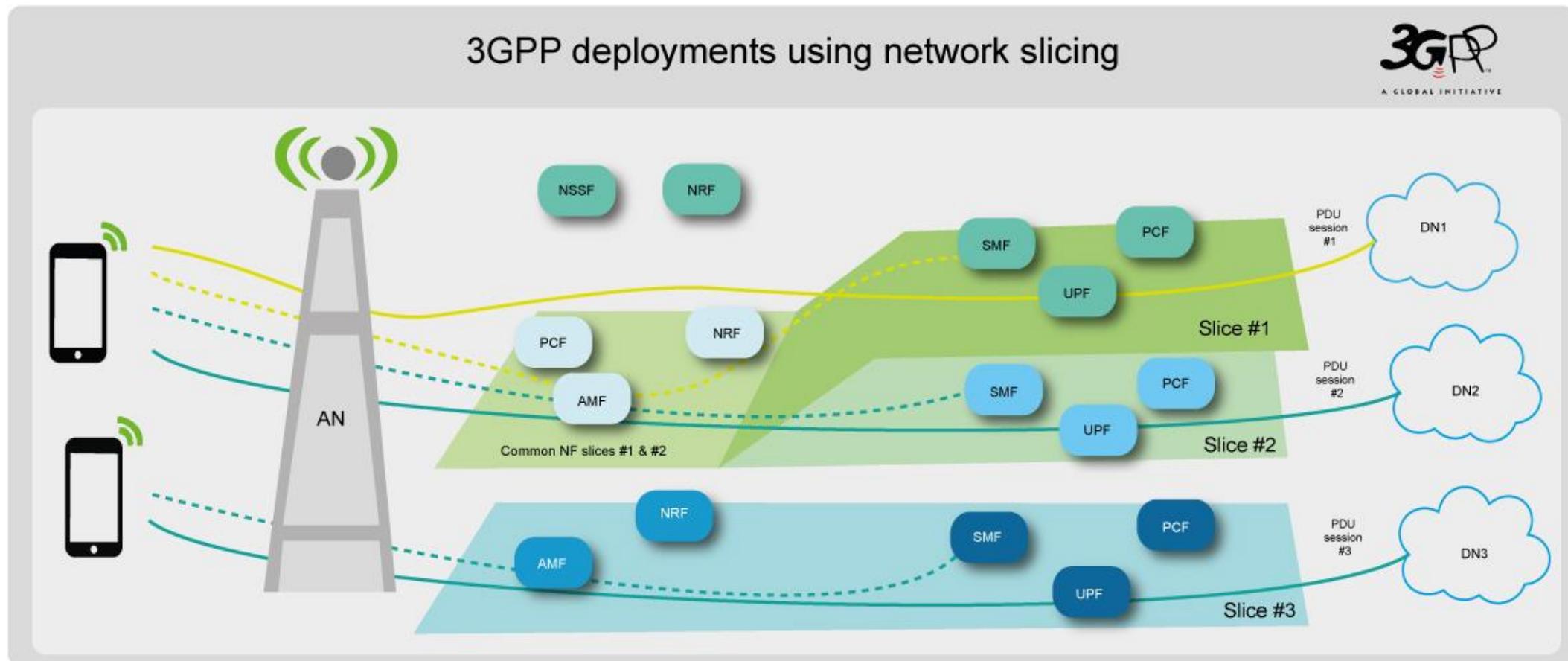
- Resources isolation between services
- Customized functions and/or capacities, according to SLA

**Each terminal (UE) may connect simultaneously to max 8 slices (no limit for the number of slices in the core)**

**Takes benefit of NVF for easy slices creation and management (LCM)**



# 5G Slicing

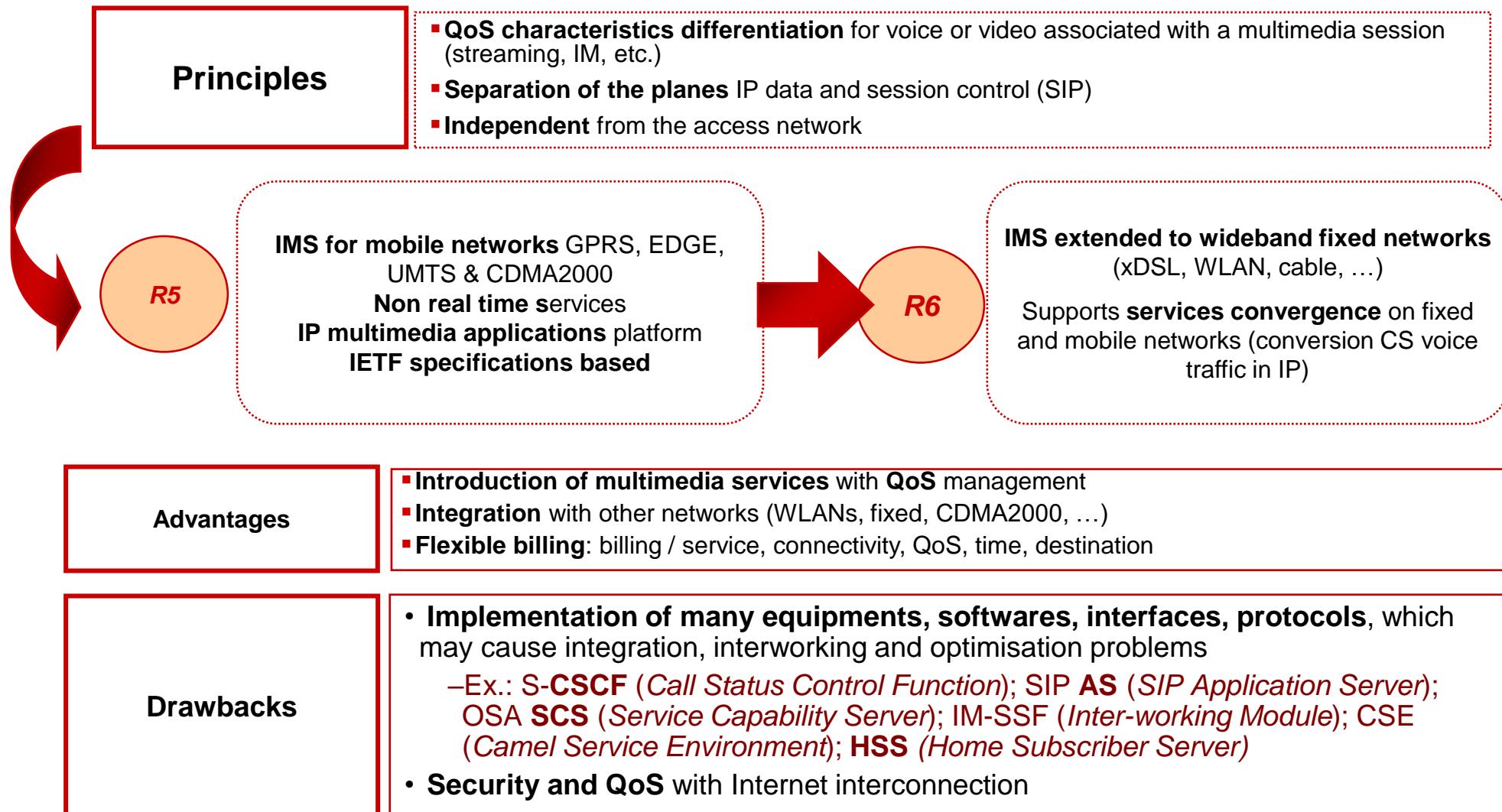


<https://www.3gpp.org/news-events/3gpp-news/sys-architecture>

**APN → DNN (Data Network Name)**

- <https://www.mpirical.com/blog/the-evolution-of-mobile-communication>
- <https://telecompendia.net/5g-core-network-overview/>
- <https://telecompendia.net/5g-nr-frequency-bands/>

# IMS - IP Multimedia Subsystem



# IMS – Key Architectural Principles

- **Border Functions**
  - Access and Network Border Security
  - QoS and Admission Control
  - Media and Signaling Adaptation
- **Core Functions**
  - Subscriber Management – Registration
  - Session Switching – Set-up and tear-down of session legs, Session state maintenance, Application Server invocation
  - Session Routing – Breakout to external networks
  - Centralized Provisioning – Subscriber and Routing data
- **Application Functions**
  - Access to legacy applications
  - Native SIP Applications
  - Service Brokering

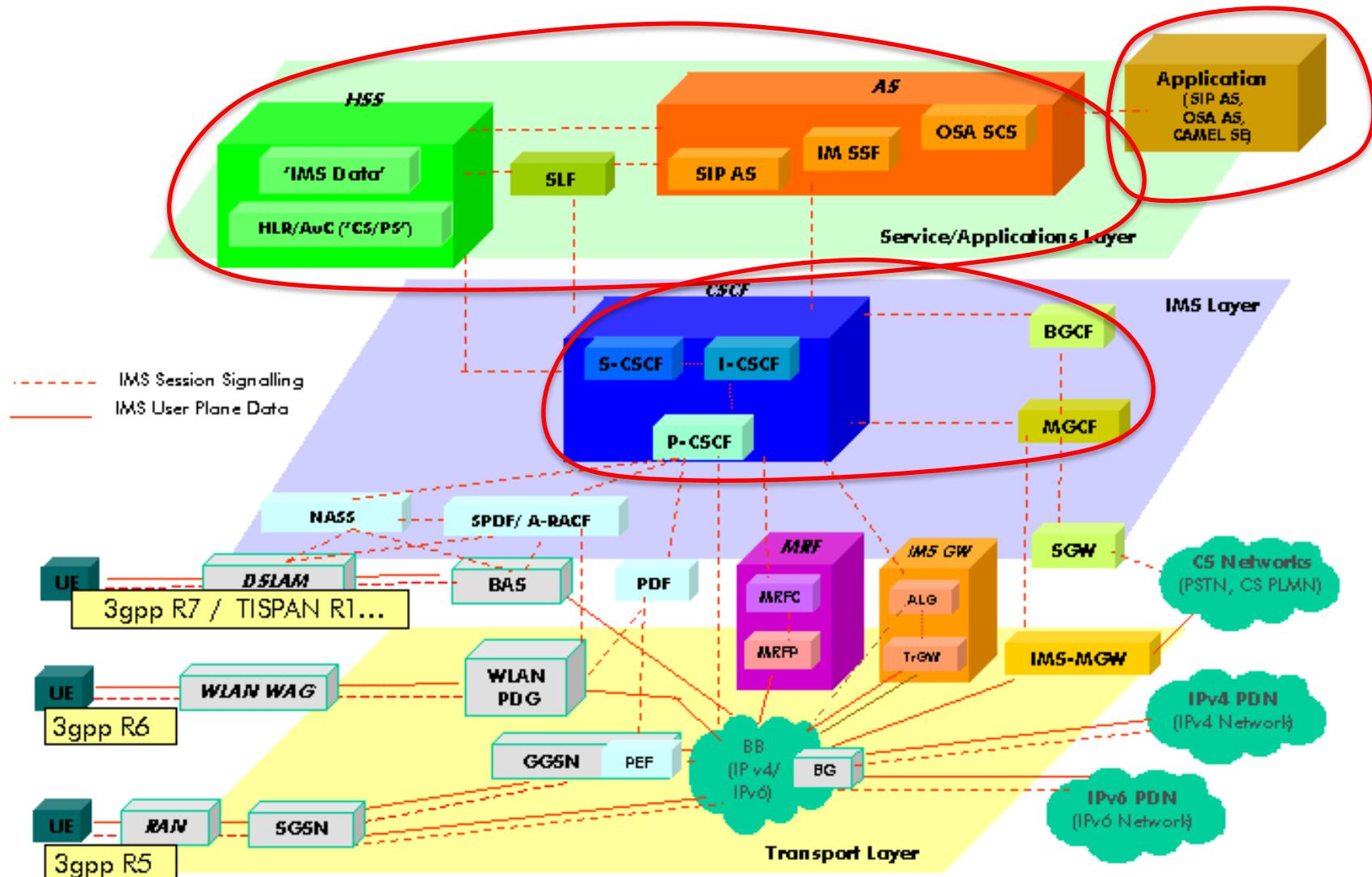
# SIP Protocol

- Defined in IETF RFC 3261
  - “... an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.”
- SIP is to the Internet what SS#7 is to telephony
- In IMS, SIP is extended to include extra functionality
  - E.g. 3GPP TS 23.228
- At the core of IMS there are several SIP proxies:
  - I-CSCF, S-CSCF, P-CSCF
  - The Call Session Control function (CSCF) is the heart of the IMS architecture
  - The main functions of the CSCF:
    - provide session control for terminals and applications using the IMS network
    - secure routing of the SIP messages,
    - subsequent monitoring of the SIP sessions and communicating with the policy architecture to support media authorization.
    - responsibility for interacting with the HSS.
- Serving - CSCF
  - Controls the user's SIP Session
  - very few per domain
  - Located in the home domain
  - Is a SIP registrar (and proxy)
- Proxy – CSCF
  - IMS contact point for the user's SIP signaling
  - Several in a domain
  - Located in the visited domain
  - Terminals must know this proxy (e.g. DHCP used)
  - Compresses and decompresses SIP messages
  - Secures SIP messages
  - Assures correctness of SIP messages
- Interrogating – CSCF
  - domain's contact point for inter-domain SIP signaling
  - one or more per domain
  - In case there are more than one S-CSCFs in the domain, locates which S-CSCF is serving a user

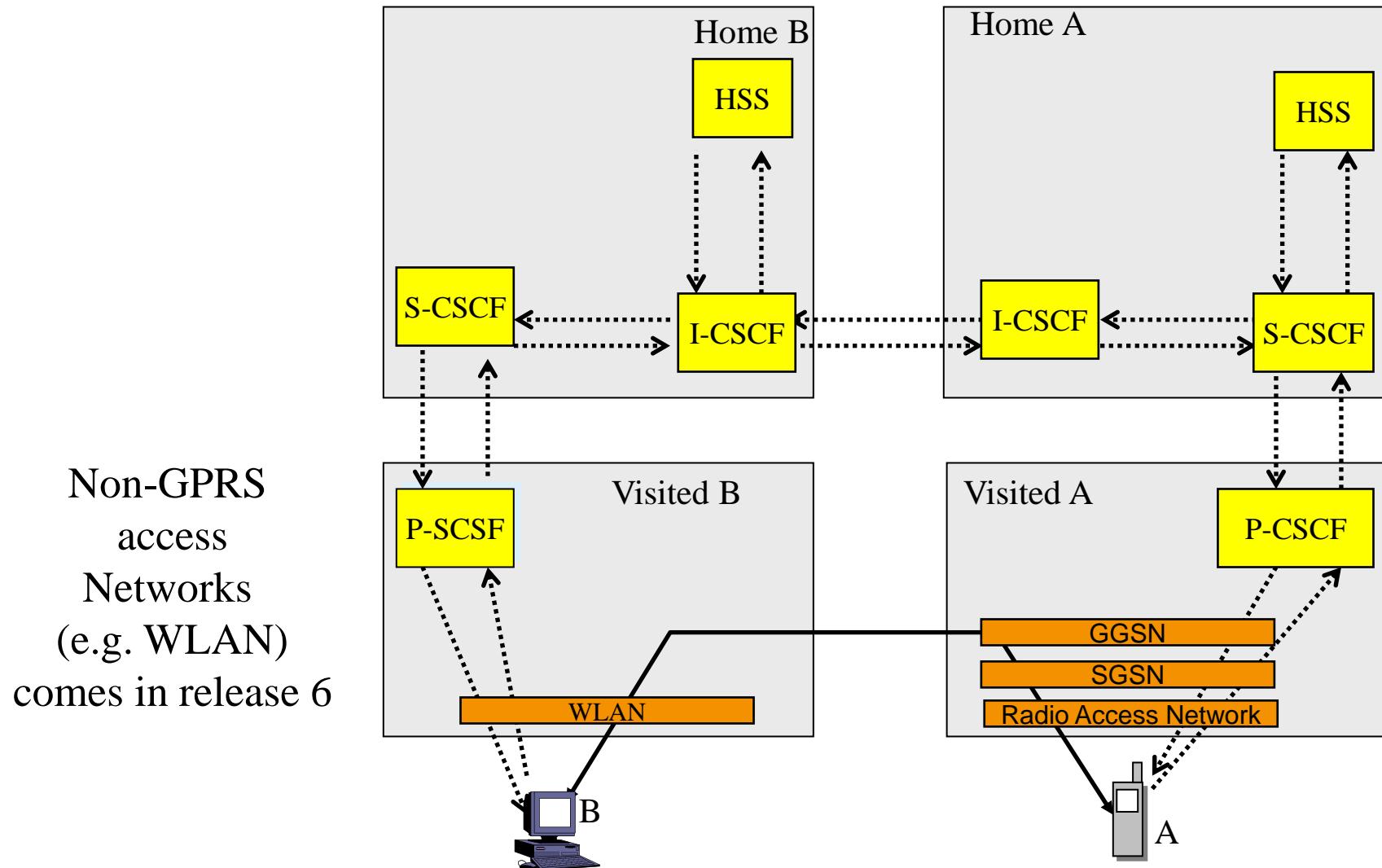
# **Services in IMS**

- **IMS is an advanced infrastructure enabling services. But the services are in the end points or peers (calls, etc.), not in the IMS**
- **Application Servers (AS) are the key part to endow IMS with services**
- **AS offered services enjoy all IMS advantages**
- **AS interact – using SIP - with the S-CSCF (which controls user's SIP session)**
- **AS can behave as another SIP proxy or as a SIP UA (terminal)**

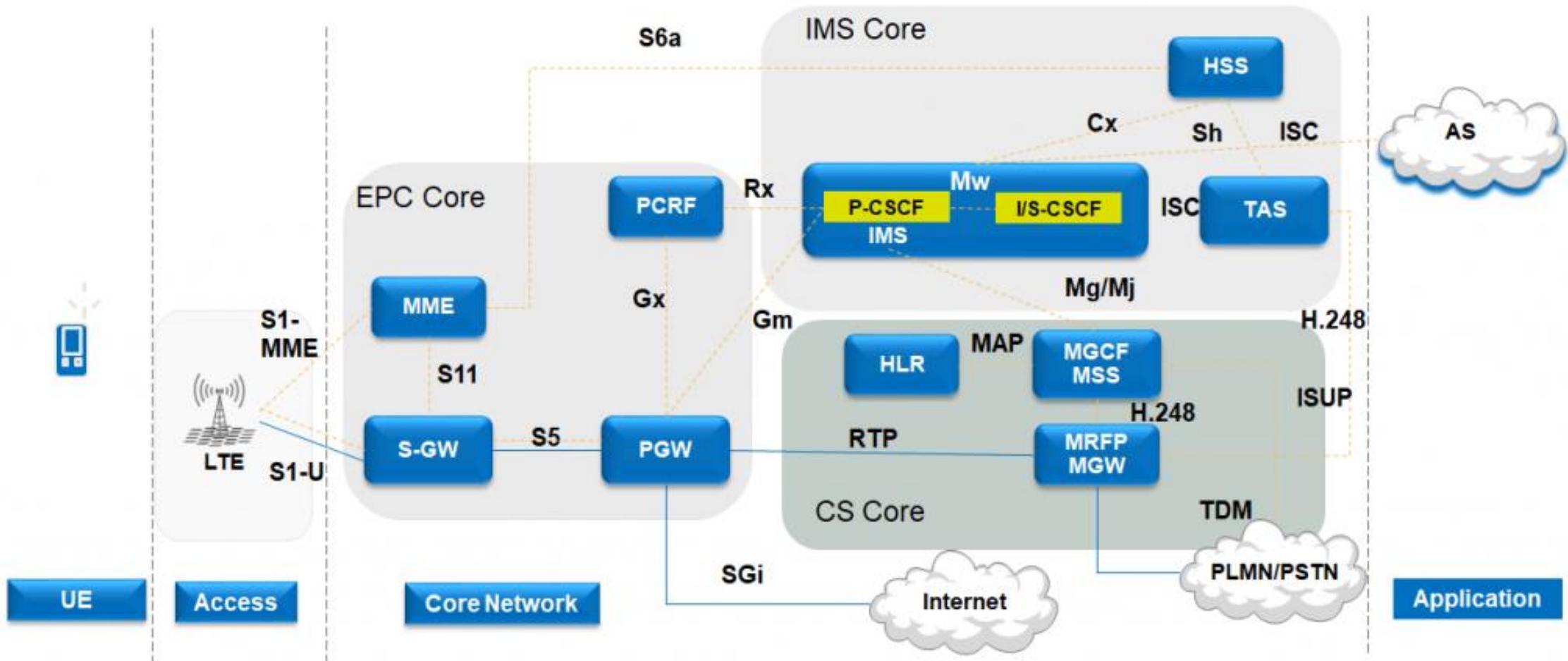
# Where is IMS ?



# UMTS IMS: basic call flow



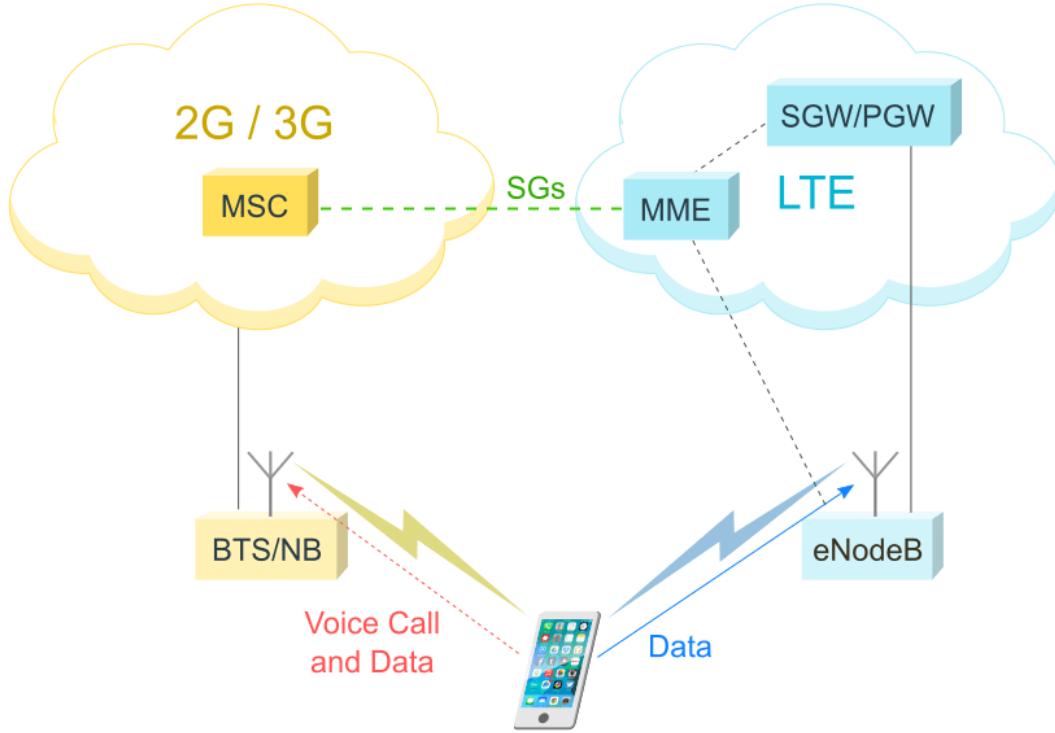
# VoLTE Network Architecture



<https://cafetele.com/volte-architecture/>

# Voice: CSFB or VoLTE

[https://yatebts.com/solutions\\_and\\_technology/csfb-to-volte-evolution/](https://yatebts.com/solutions_and_technology/csfb-to-volte-evolution/)



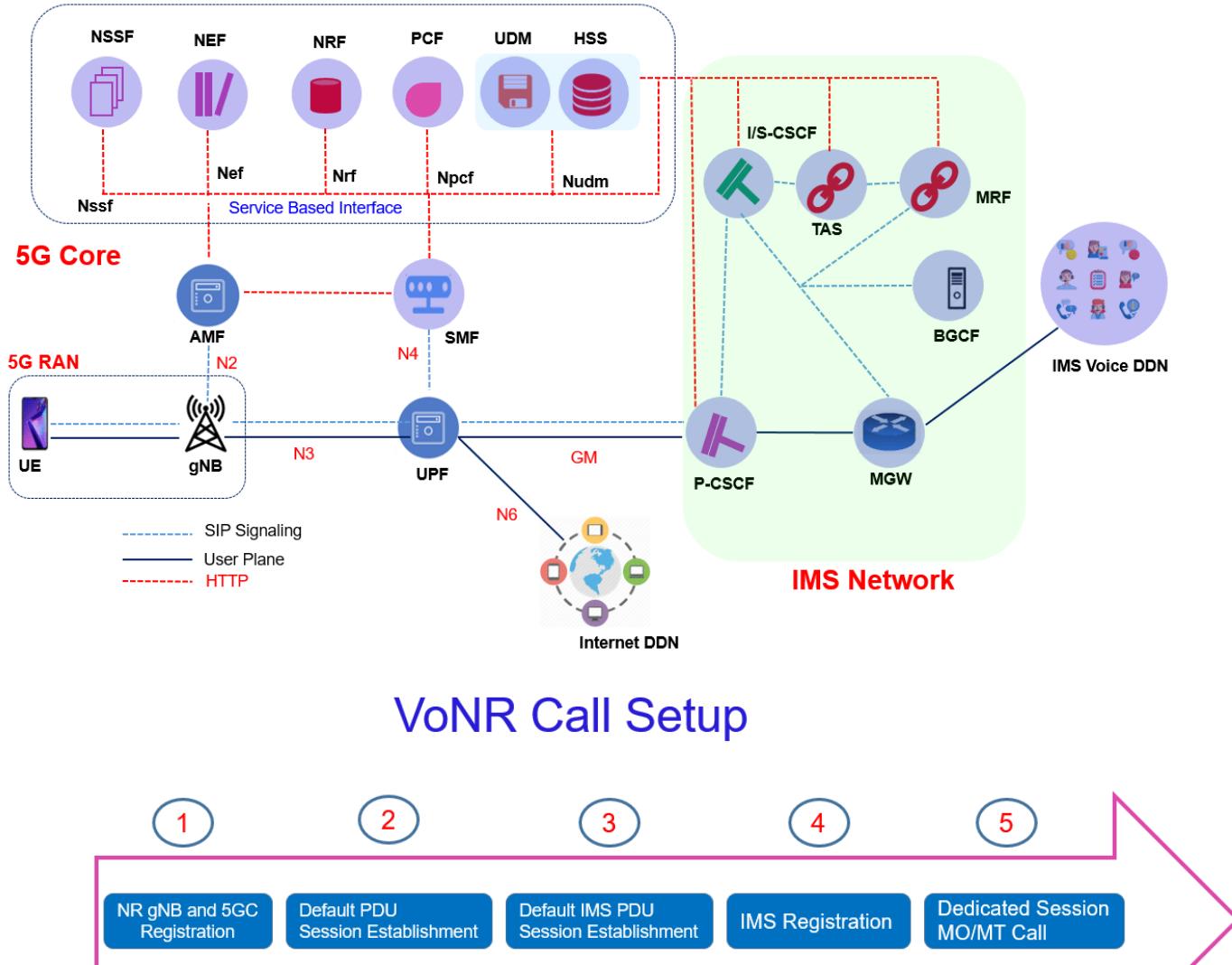
<https://www.mpirical.com/blog/delivering-5g-voice-services>

| Feature                   | CSFB                                       | VoLTE                                   |
|---------------------------|--|---|
| Easy of Deployment        | Challenging, but not as difficult as VoLTE | Numerous major challenges to overcome   |
| Economic Considerations   | Minor                                      | Major                                   |
| LTE Coverage Requirements | Low  | High                                    |
| Call Setup Time           | Approx. 3-7 secs                           | Approx. 2-4 secs                        |
| Voice Quality             | Acceptable                                 | HD Voice                                |
| Lifespan                  | 2G and 3G limited life                     | IMS forms basis for 5G voice and beyond |

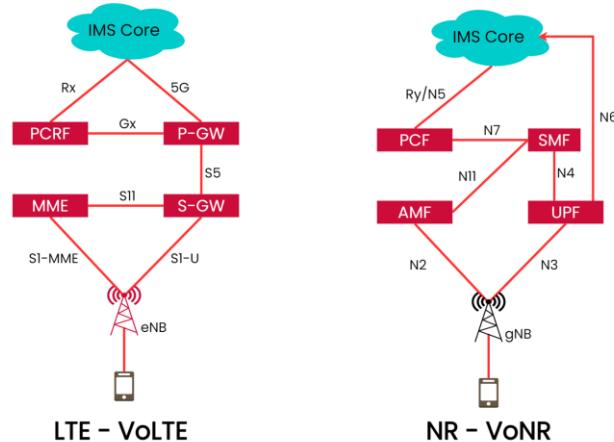
CSFB (Circuit Switch Fallback) is a technology that supports voice and SMS services in 4G networks using the 2G/3G systems.

VoLTE (Voice over LTE), on the other hand, means that a call is made through a 4G network (Making calls over IP).

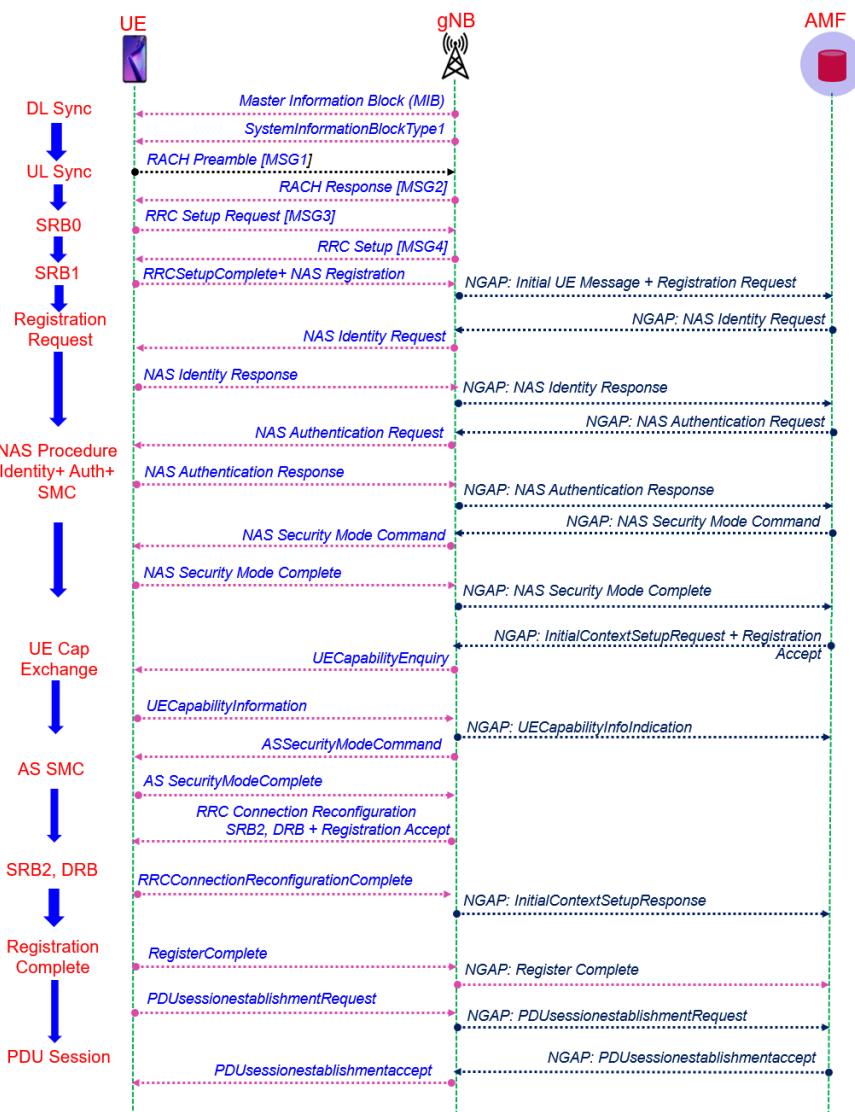
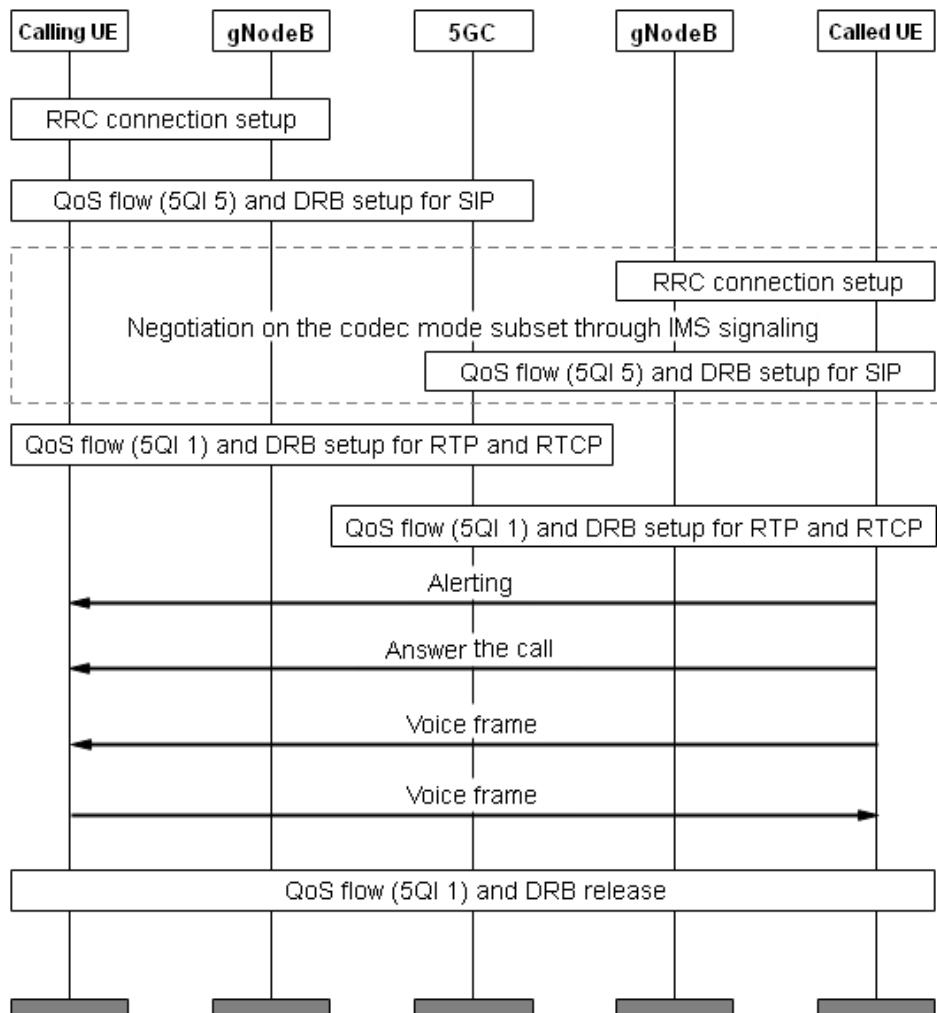
# Example: VoNR



- Main componentes: 5G RAN, 5G Core, IMS
- Establishement of specific PDU sessions
- QoS



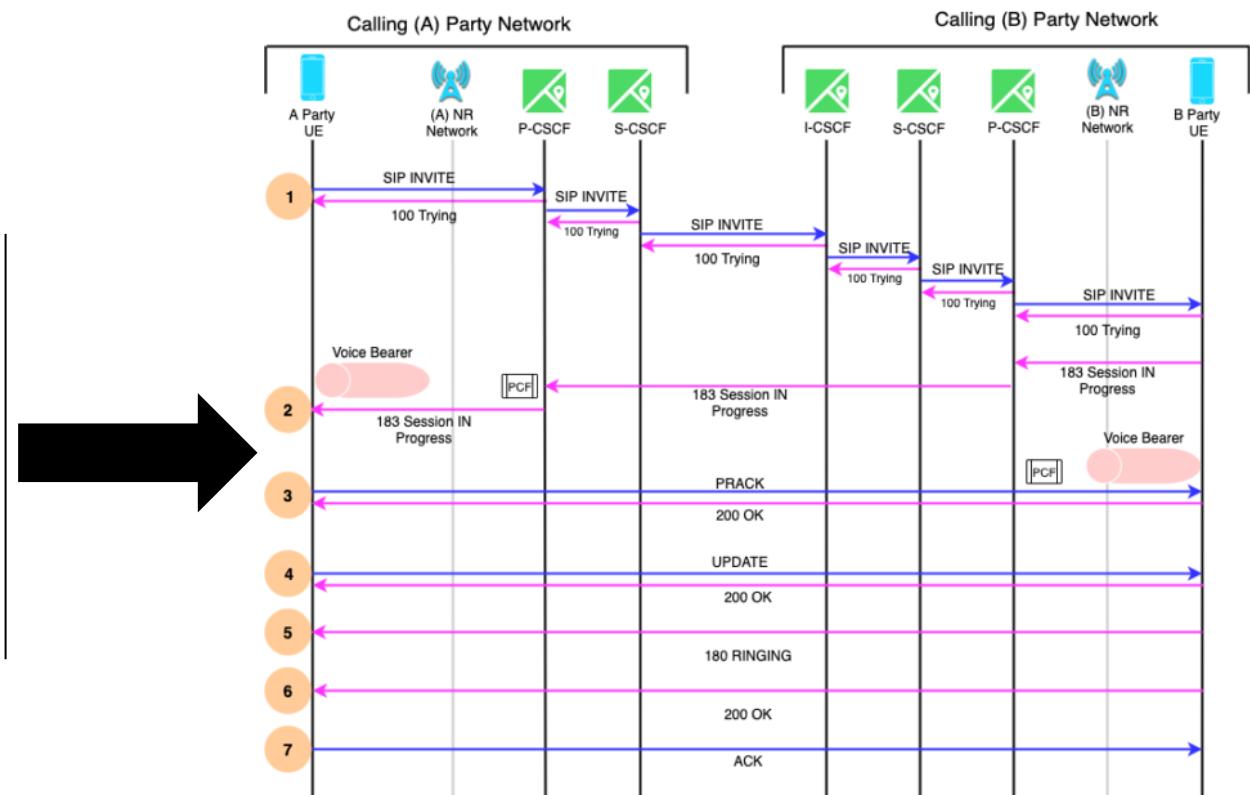
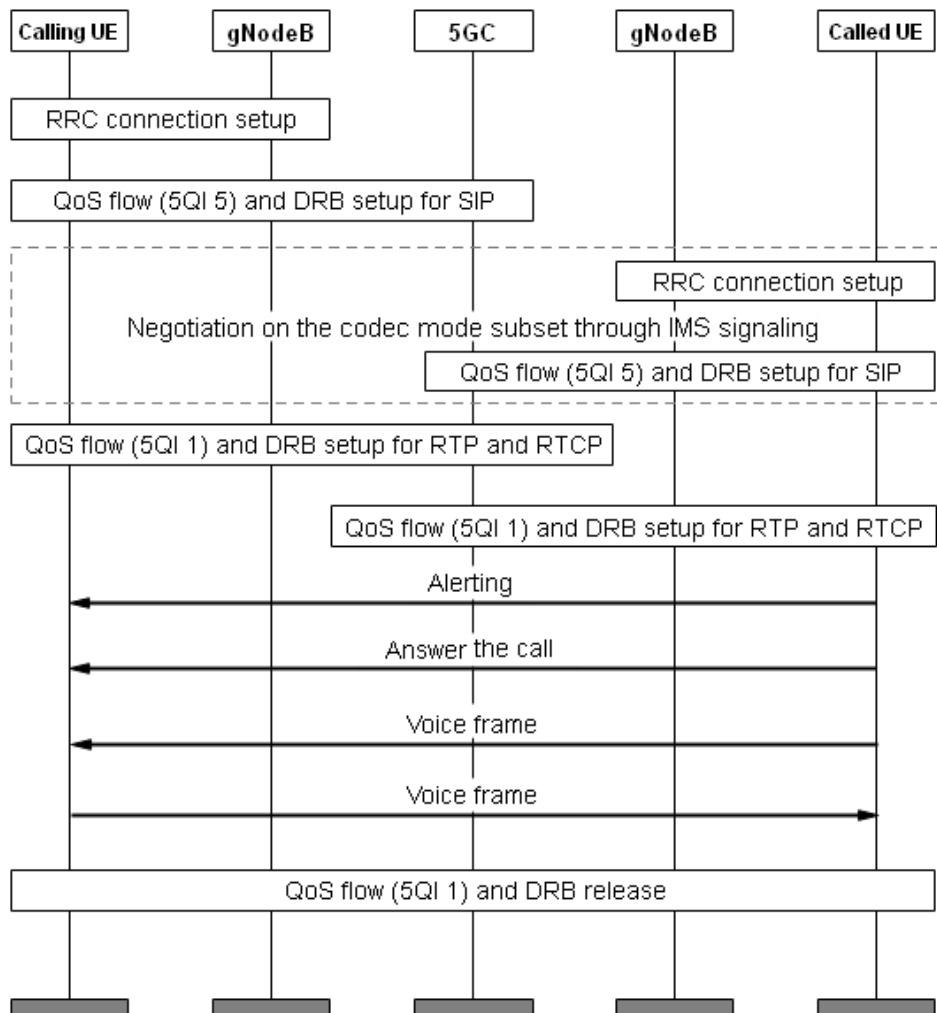
# VoNR Call Flow



<https://www.5gworldpro.com/blog/2021/05/30/voice-over-nr-call-flow/>

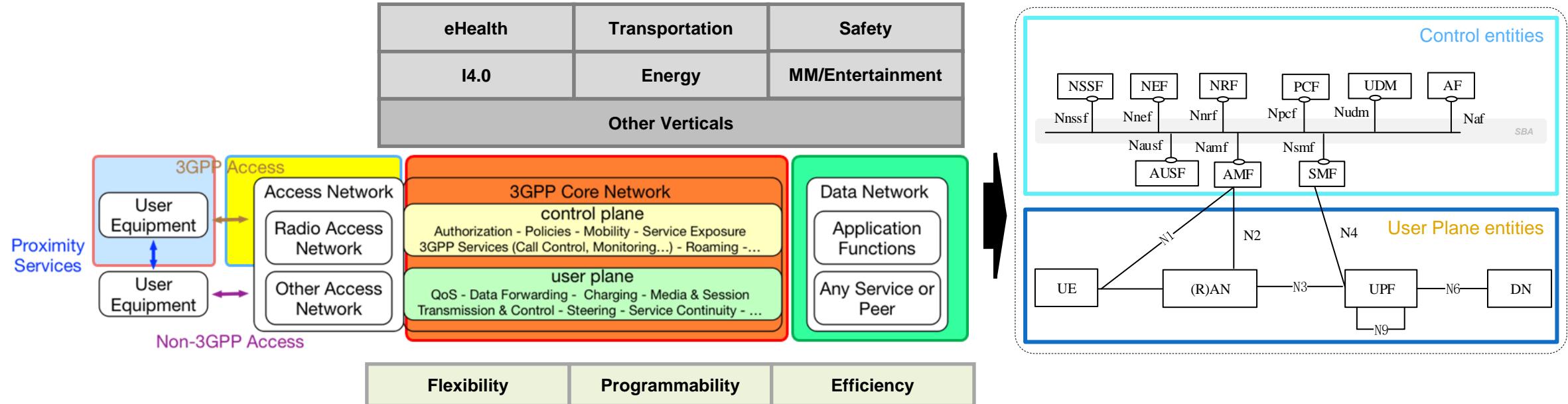
<https://www.techplayon.com/5g-nr-sa-registration-attach-call-flow/>

# VoNR Call Flow



<https://www.5gworldpro.com/blog/2021/05/30/voice-over-nr-call-flow/>

# 5G main building blocks



Based on a **new, unified, air interface** (*New Radio: NR - 5G-NR*) and a **new network architecture**, to connect everything

5G New Radio (NR) to “connect everything”:  
• A **unified air interface**

*You will be seeing 5G NR connectivity in your smartphones, cars, utility meters, wearables and much more* (Qualcomm)

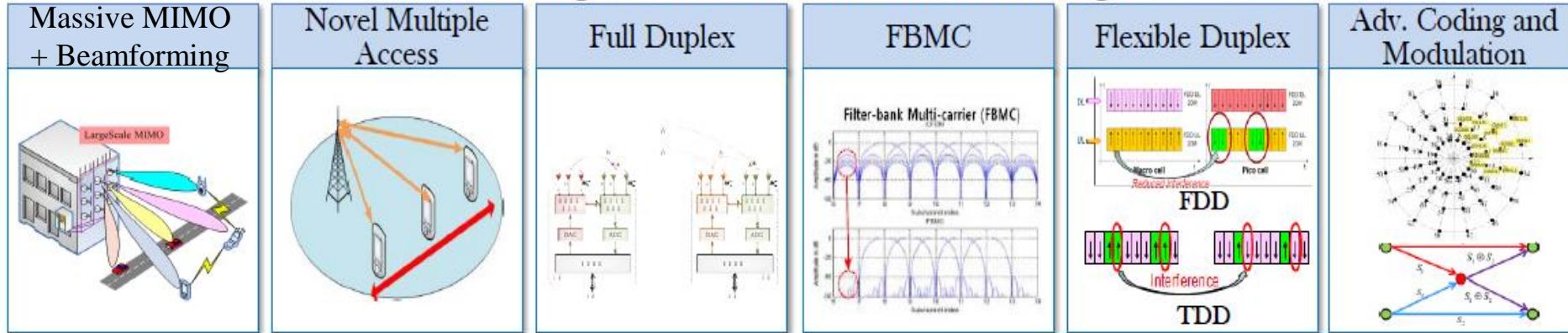
Able to **embrace all sort of wireless/wired accesses**, sharing a common core (5G Core Network – **5GC**)

5G new architecture to “interconnect everything”:  
• A **common core network**

*The new architecture shall support at least the new RAT(s), the Evolved E-UTRA, non-3GPP accesses and minimize access dependencies* (3GPP TR 23.799)

# Key Wireless Technology Directions

## Enabling wireless transmission technologies



## Key technical solutions

