# Cellular Networks

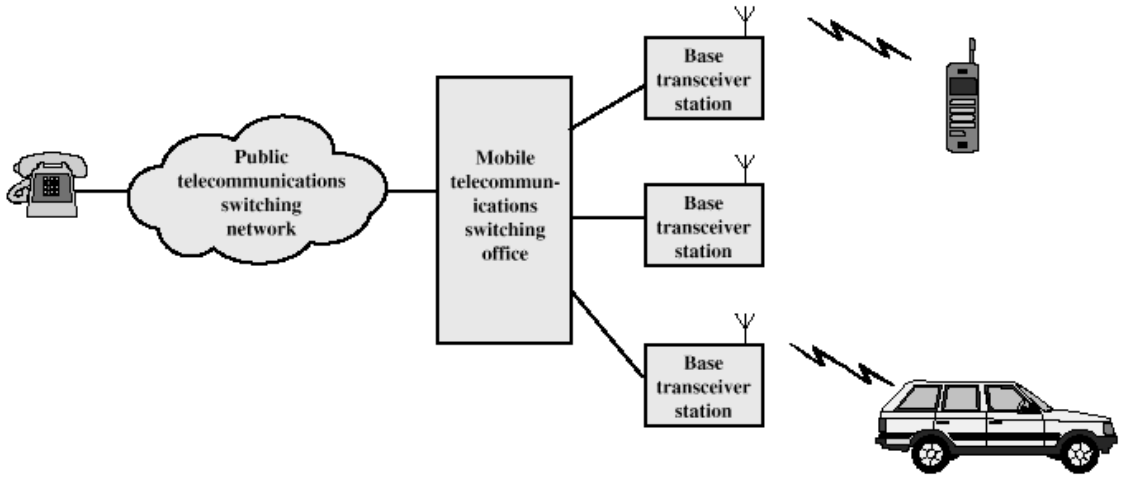
Mobile cellular networks

GSM to 5G

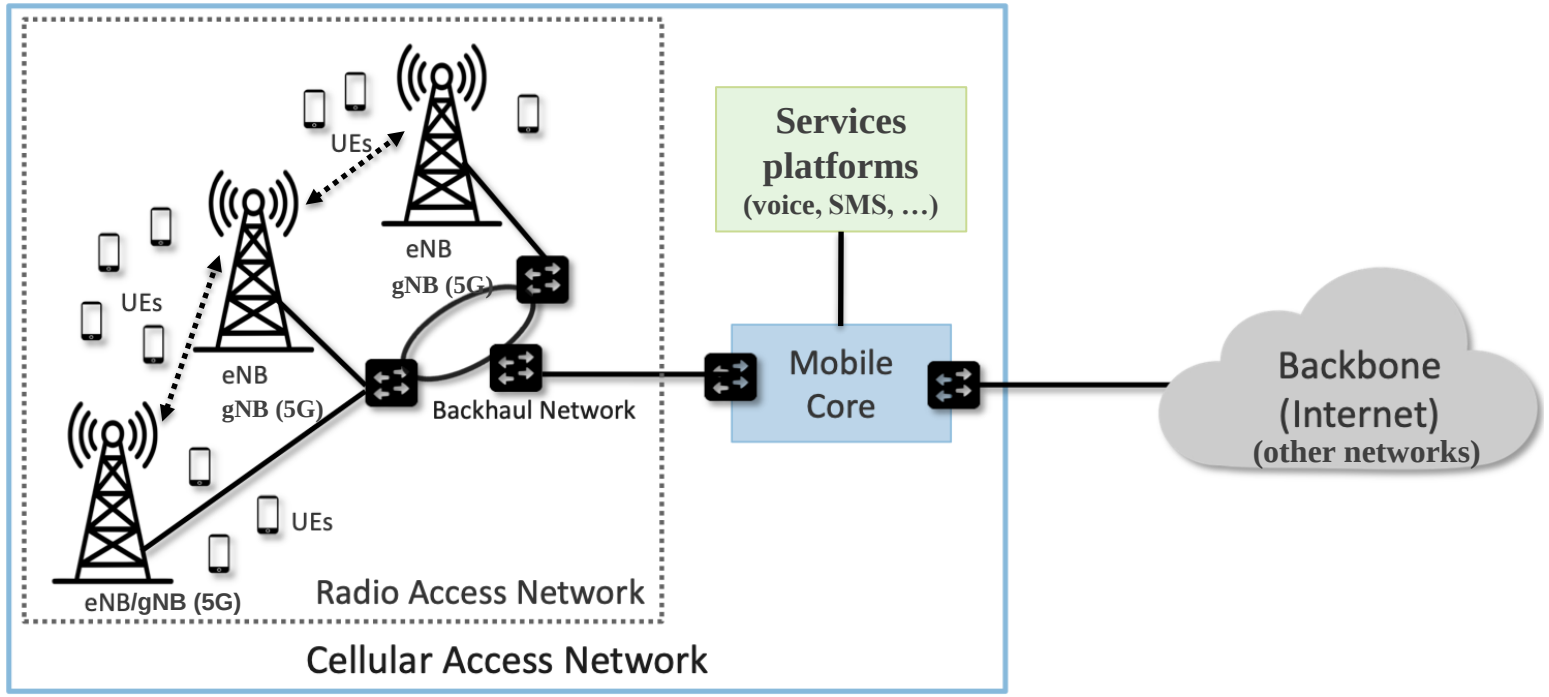
# Wireless CELLULAR network

- **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



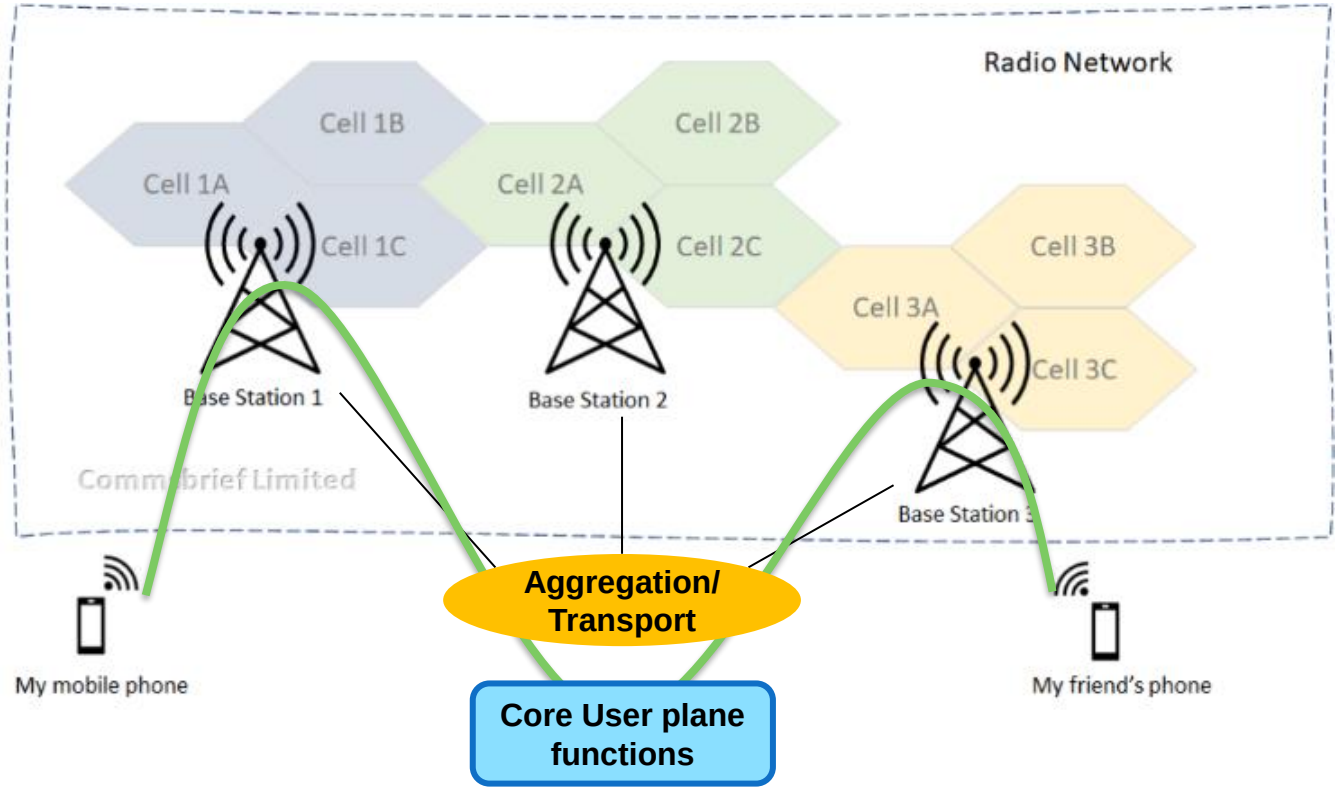

**Only the UE to e/gNB interface is radio based**

**‘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




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

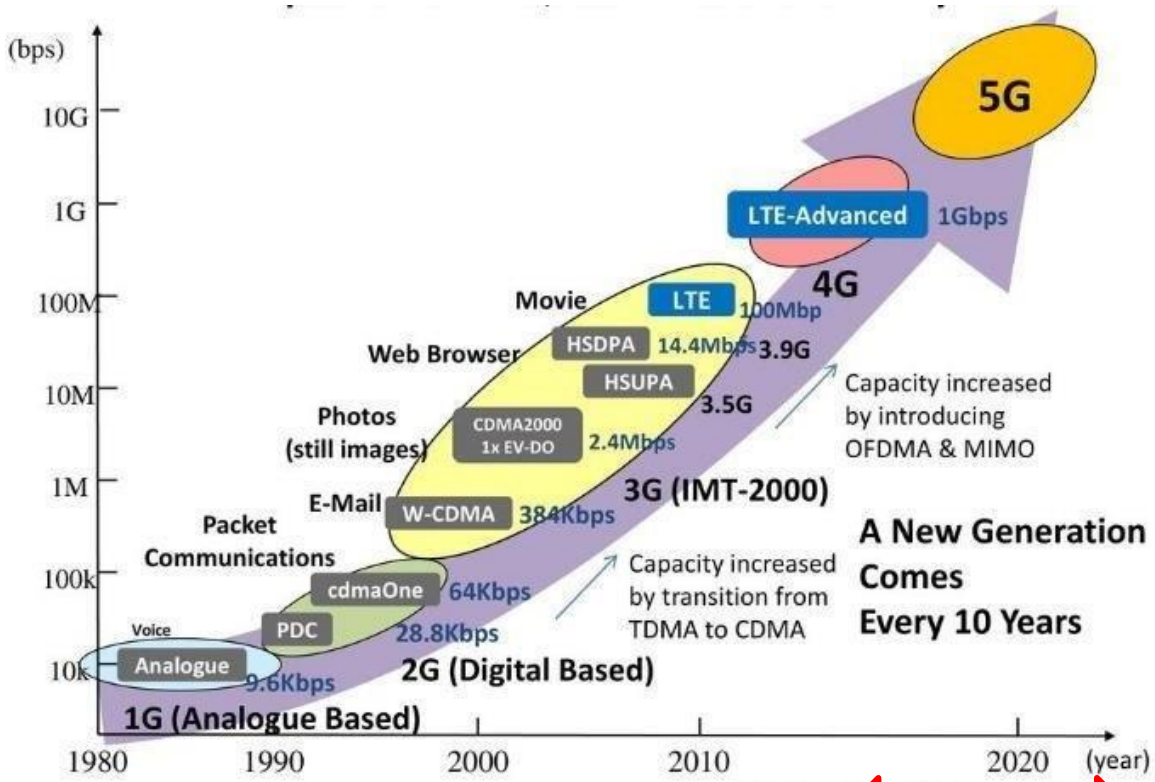
# Technological waves (*Generations*)

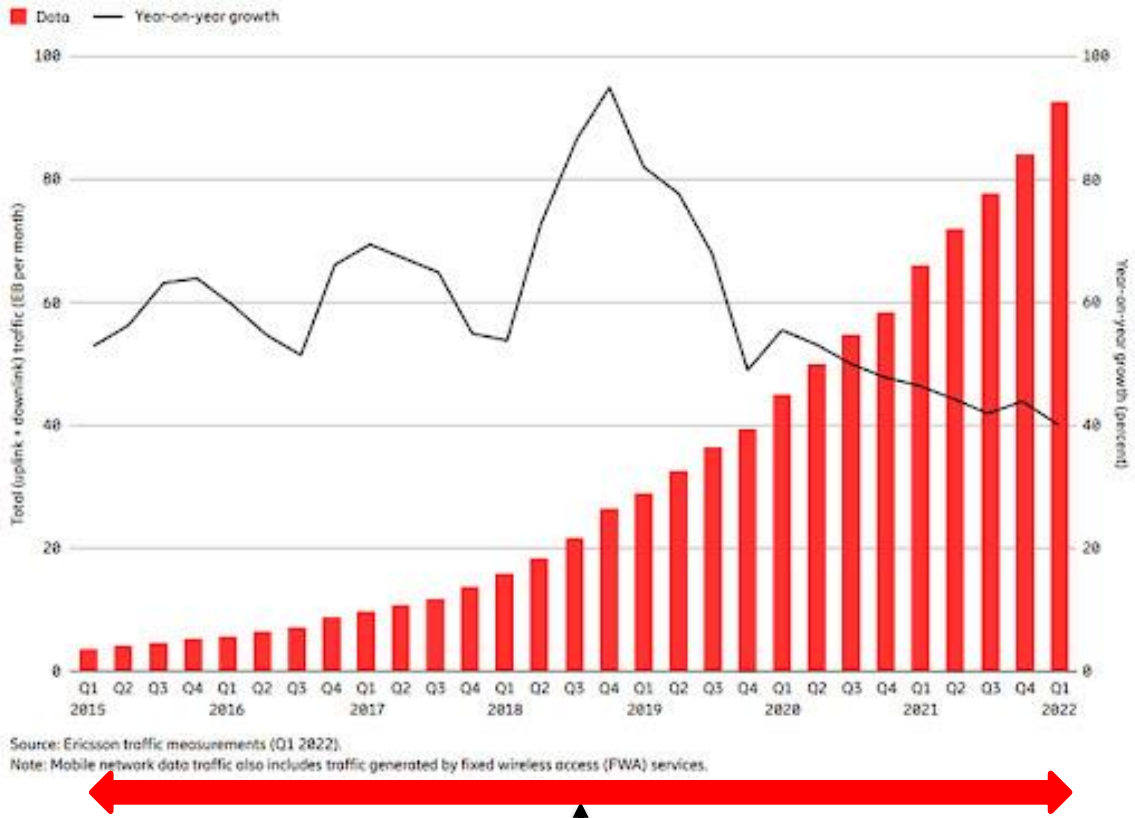
| 1G | 2G | 3G | 4G | 5G |
|---|---|---|---|---|
| Mobile voice communication | Digital mobile voice SMS/MMS | Broadband mobile data | Broadband mobile data massification | Unified future-proof platform |
| 1980 | 1990 | 2000 | 2010 | 2020 |
| Analogue voice C450, NMT, AMPS, TACS | D-AMPS, GPRS, GSM, SMS/MMS, CDMA | UMTS/CDMA2000, HSPA+, Smartphones | LTE, LTE Advanced, Gigabit LTE, OFDM | 5G New Radio, SDN, NFV, ML/AI |
| Data < 128 Kbps | Data < 128 Kbps | Data < 42 Mbps | Data < 1 Gbps | eMBB 10 Gbps |
| Analogue system Copper cables | PSTN, X.25, Frame Relay, ATM, DOCSIS | xDSL, IP/MPLS, Digital Television, SD Video | IMS, VoLTE, IoT, IPTV, GPON/FTTH, Cloud, Vídeo HD | Massive MIMO, Beam forming, Slicing, mIoT, XGS-PON, Ultra HDTV |

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

Increasing spectral efficiency (more bits/Hz)

# 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

wikipedia

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)**

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

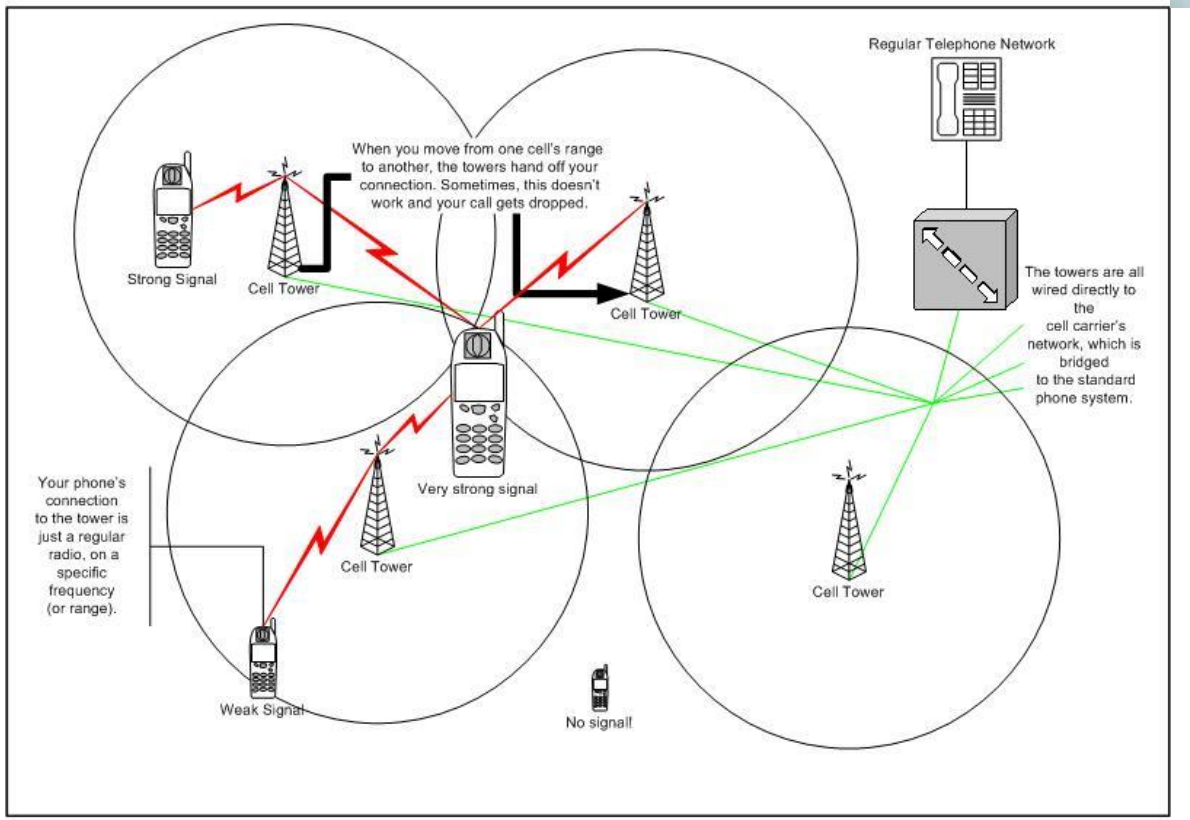
**https://mcc-mnc.com/**

# 1G

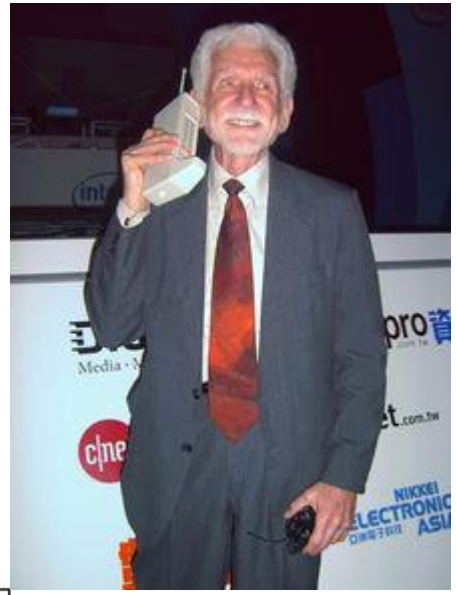
## Mobile voice

# 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

https://www.rfpage.com/evolution-of-wireless-technologies-1g-to-5g-in-mobile-communication/

# 2G

## Global System for Mobile Communications (GSM)

# 2nd 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**

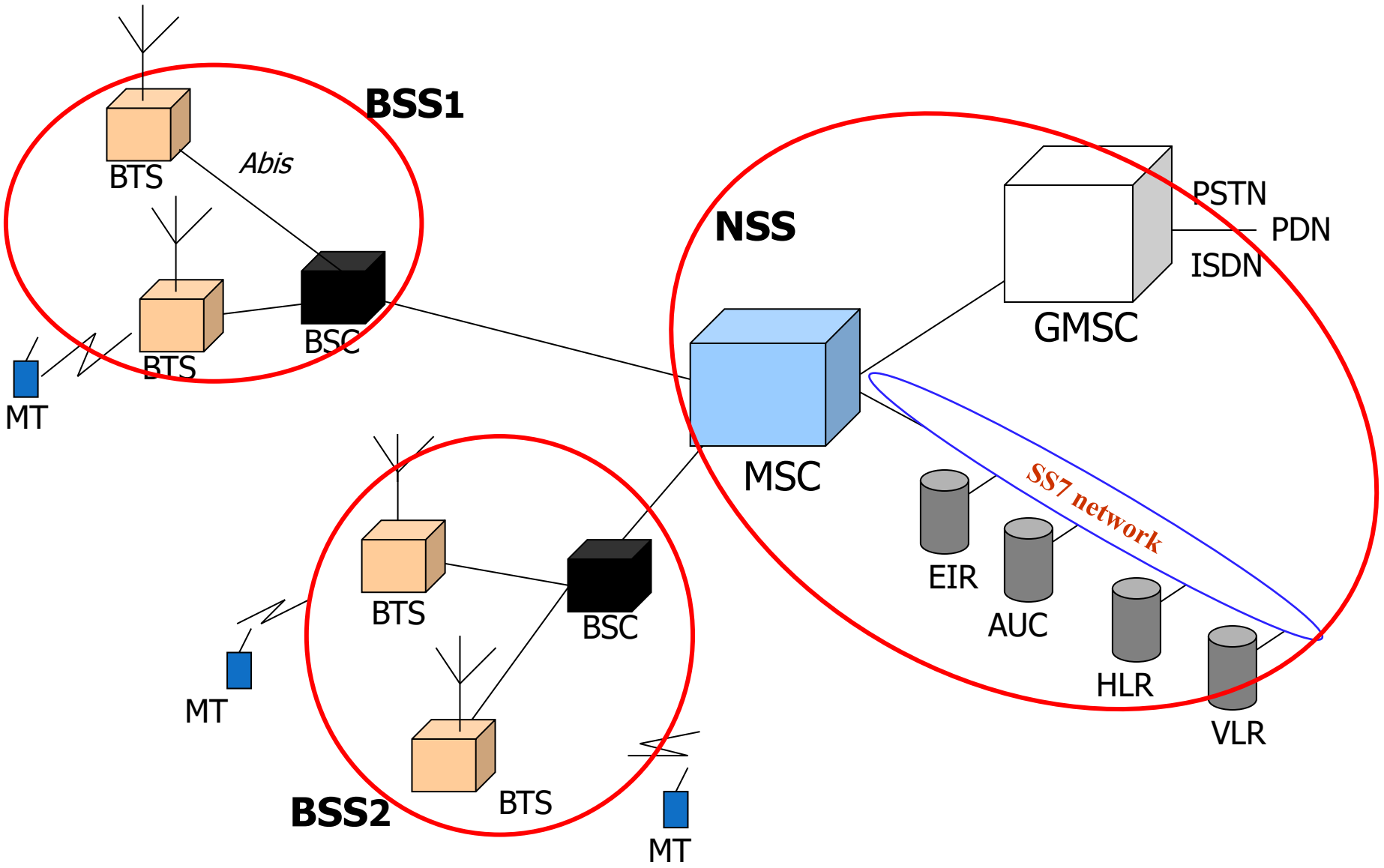
  **MobileEquipment+ SubscriberIdentityModule**
  (etc…; e.g. International Mobile Station Equipment Identity (IMEI))
- **Uses a Network Subsystem**

  **MSC; HLR, VLR**
- **Uses a Radio Subsystem**

  **BSS; BTransceiverS, BSController**
- **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).**

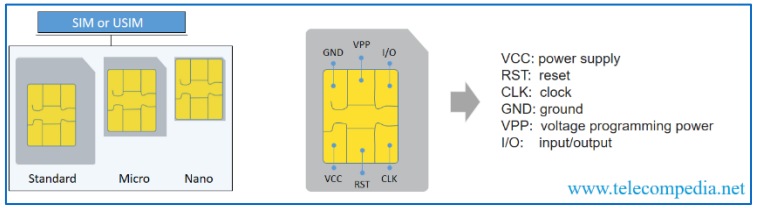
# GSM Architecture



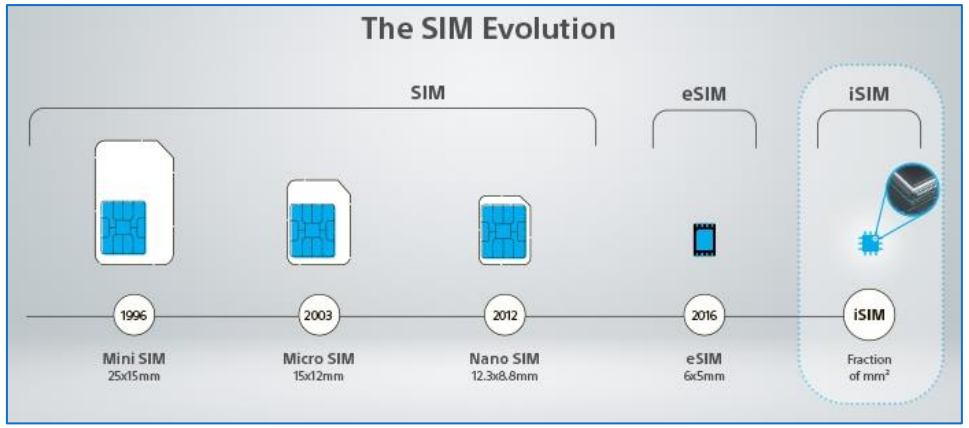

AuC: Authentication Centre
BSC: Base Station controller
BSS: Base Station Sub-system
BTS: Base Transceiver Station
EIR: Equipment Identity Register
GMSC: Gateway Mobile Switching Center
HLR: Home Location Register
ISDN: Integrated Services Digital Network
MSC: Mobile Switching Centre
MT: Mobile Terminal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

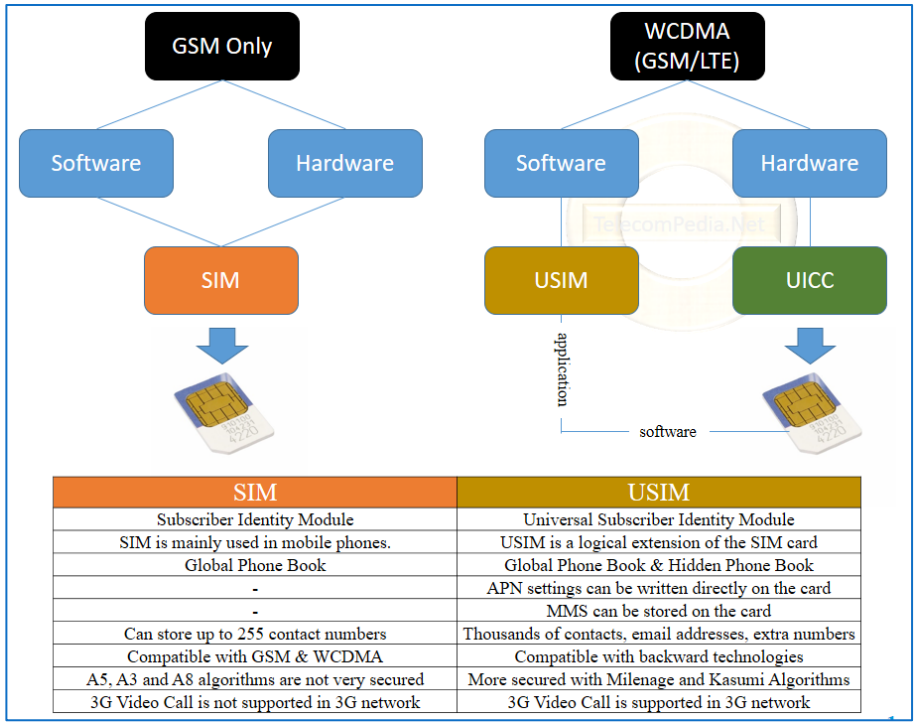
# SIM: *Suscriber Identity Module*

- **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)**

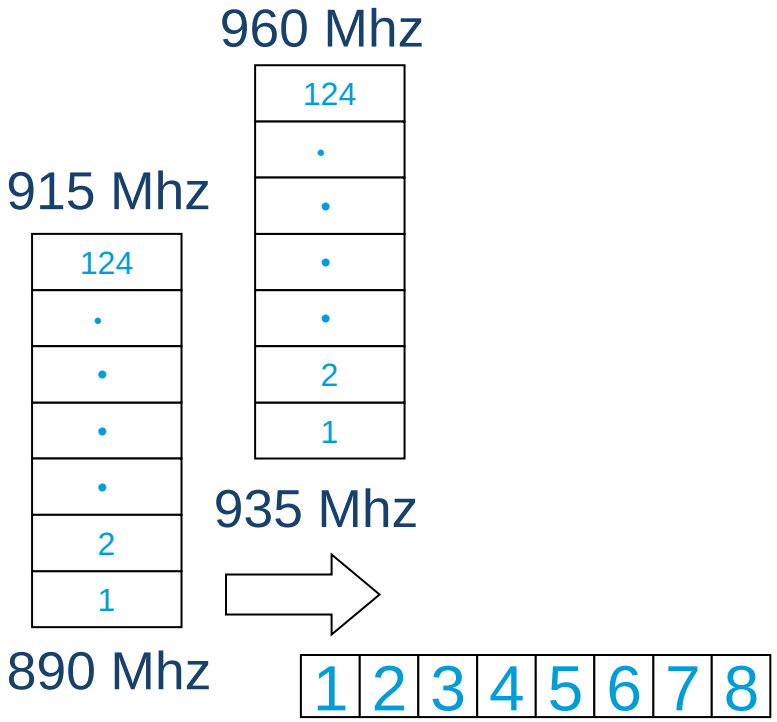


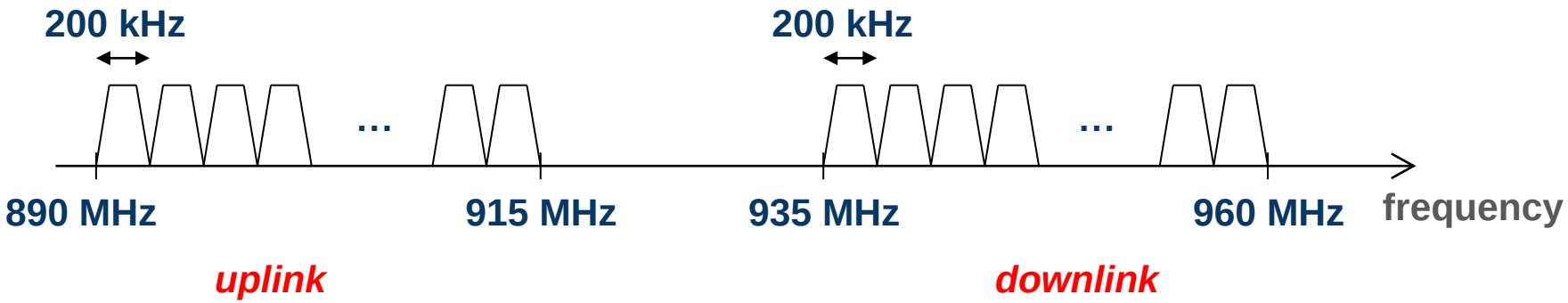




| SIM | USIM |
|---|---|
| Subscriber Identity Module | Universal Subscriber Identity Module |
| SIM is mainly used in mobile phones. | USIM is a logical extension of the SIM card |
| Global Phone Book | Global Phone Book & Hidden Phone Book |
| - | APN settings can be written directly on the card |
| - | MMS can be stored on the card |
| Can store up to 255 contact numbers | Thousands of contacts, email addresses, extra numbers |
| Compatible with GSM & WCDMA | Compatible with backward technologies |
| A5, A3 and A8 algorithms are not very secured | More secured with Milenage and Kasumi Algorithms |
| 3G Video Call is not supported in 3G network | 3G Video Call is supported in 3G network |

# Air interface (Um) – channel allocation

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



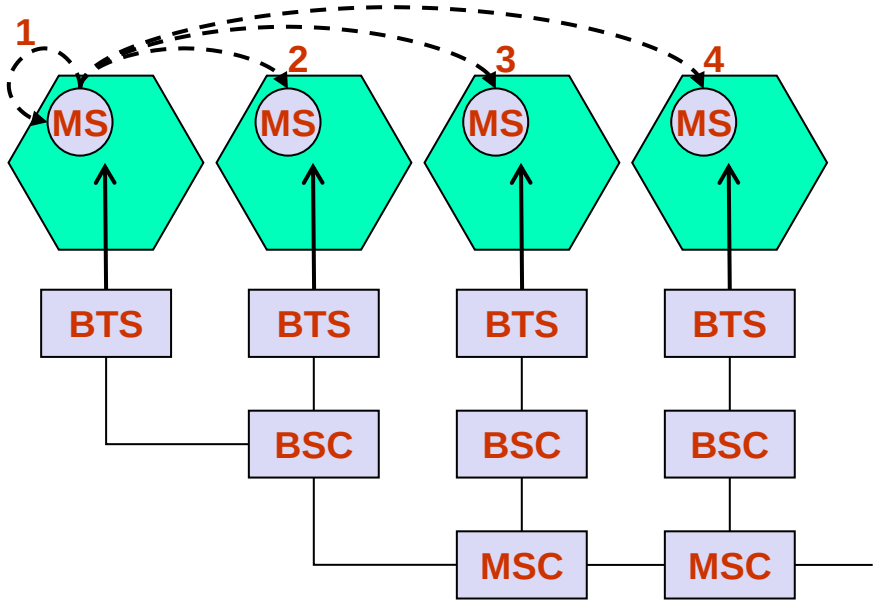
# Types of handover (GSM)

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[1] 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**

**1 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.

https://developer.twitter.com/en/docs/counting-characters

# 2.5G

## General Packet Radio Service (GPRS)

# GPRS

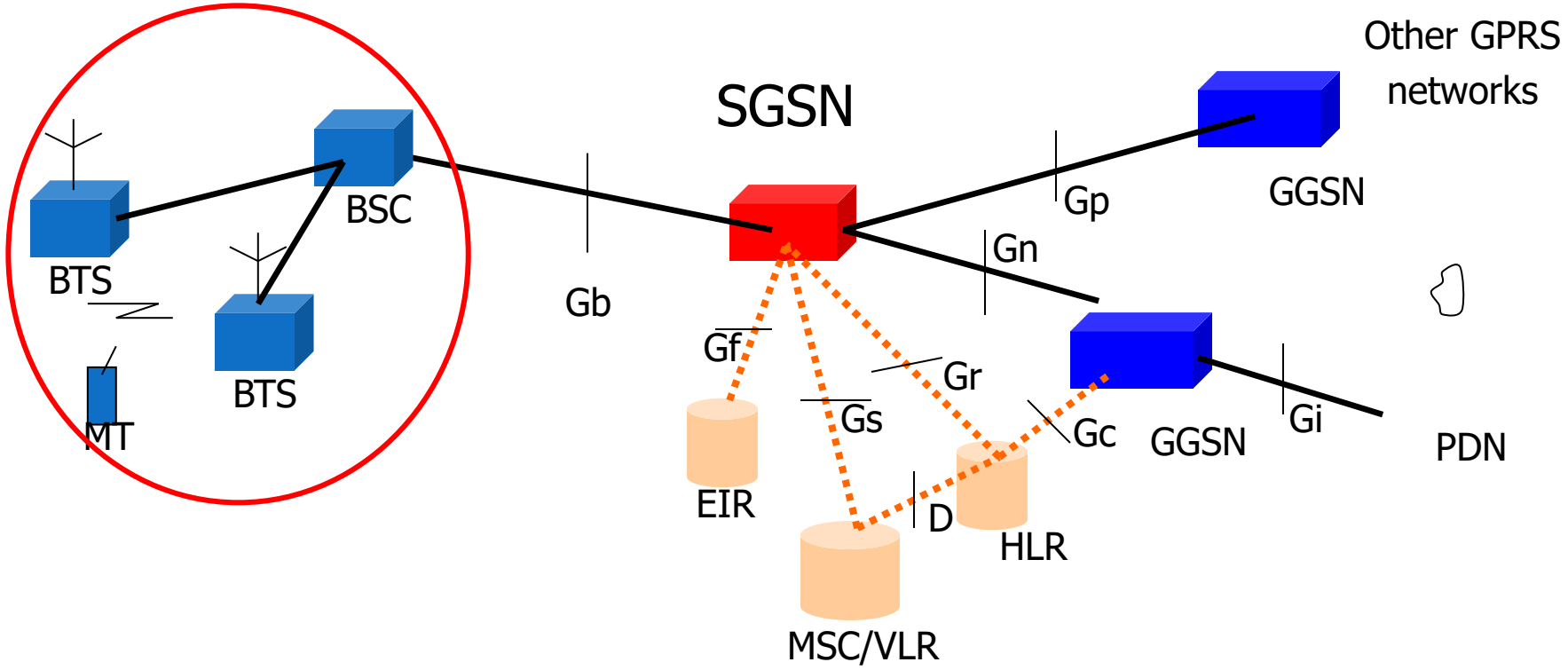
- **GPRS: *General Packet Radio Service***

- **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.)**

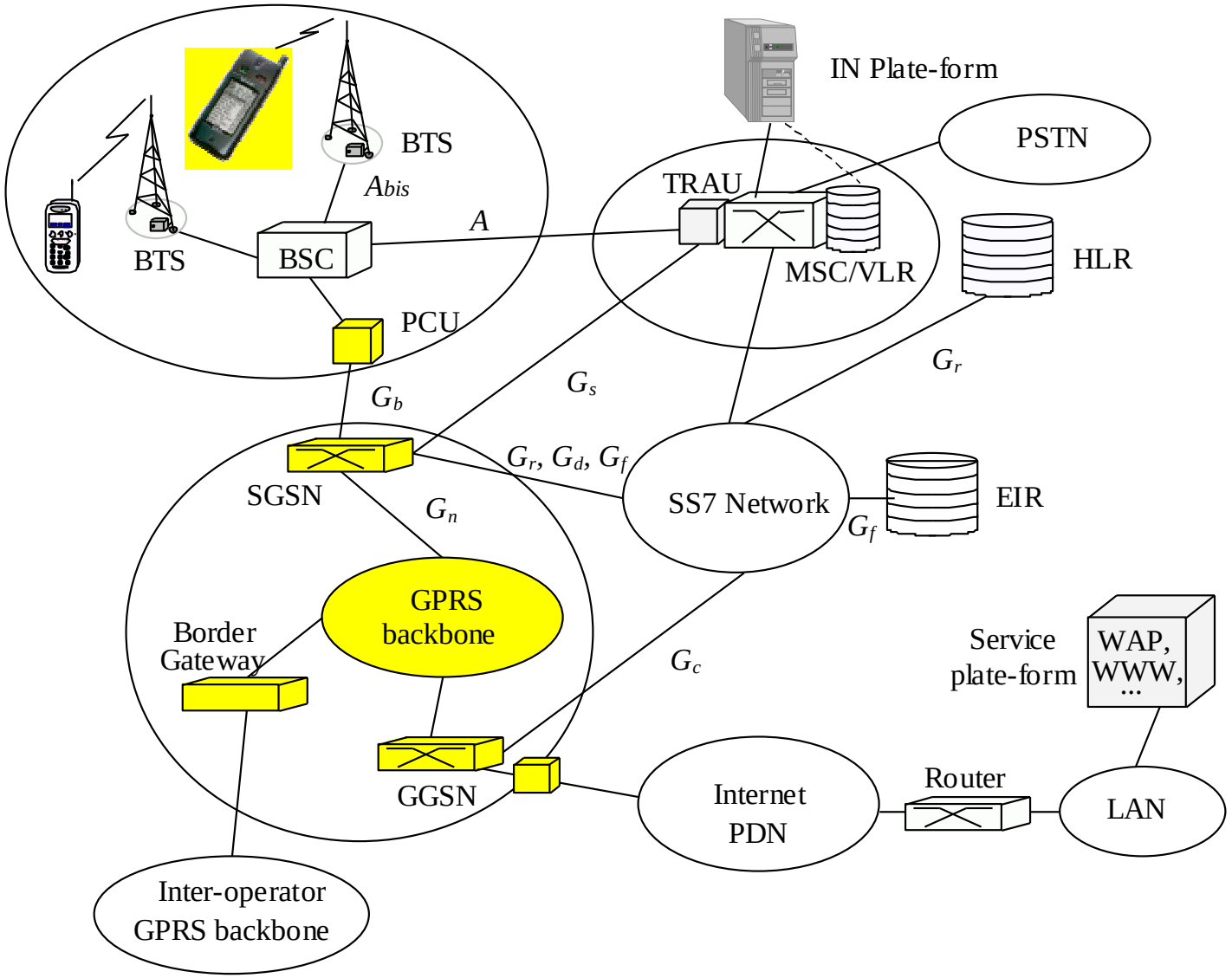
# GPRS Architecture

- 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”

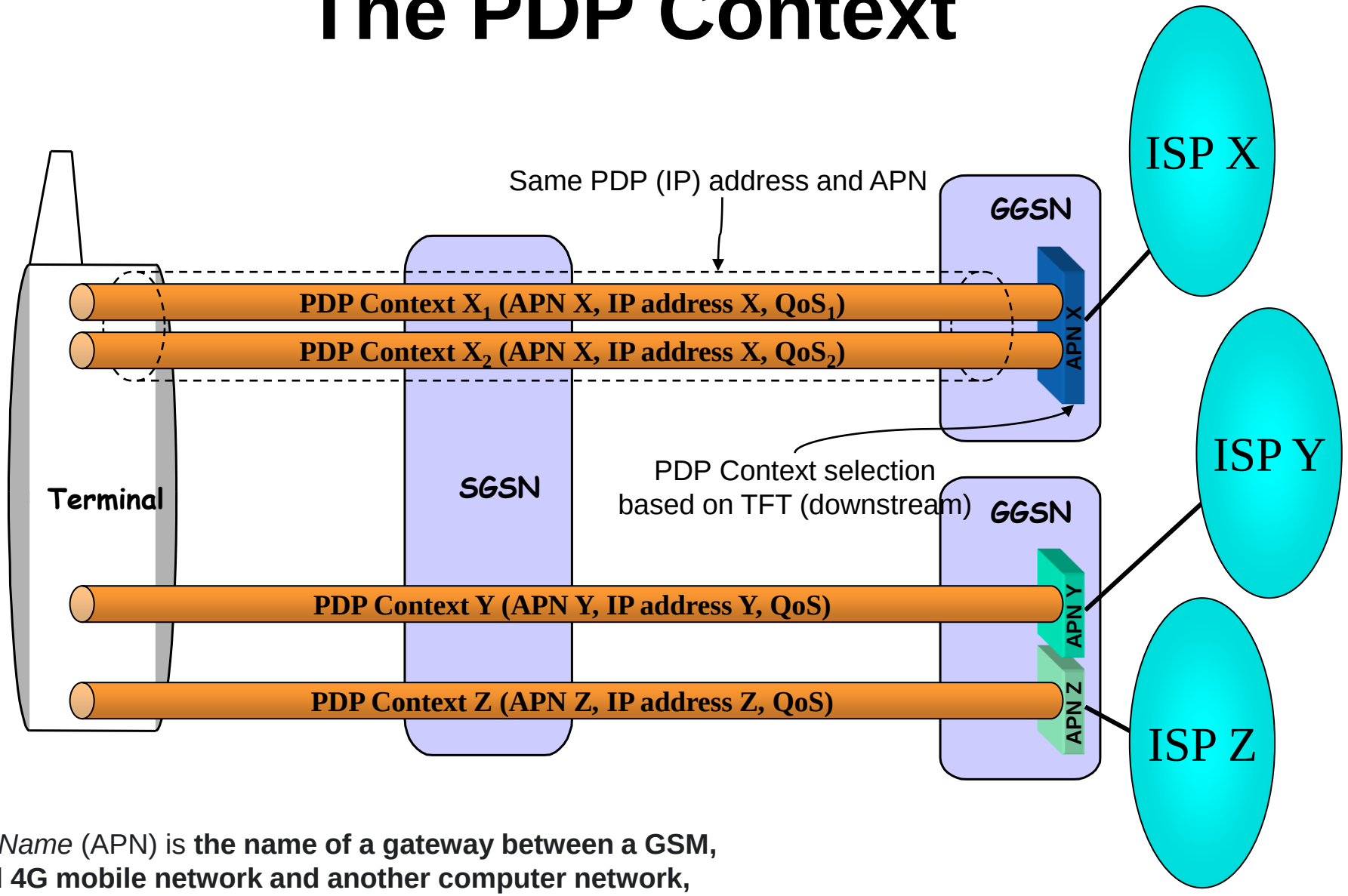
# GPRS Architecture



# GPRS introduction in a GSM network



# The PDP Context



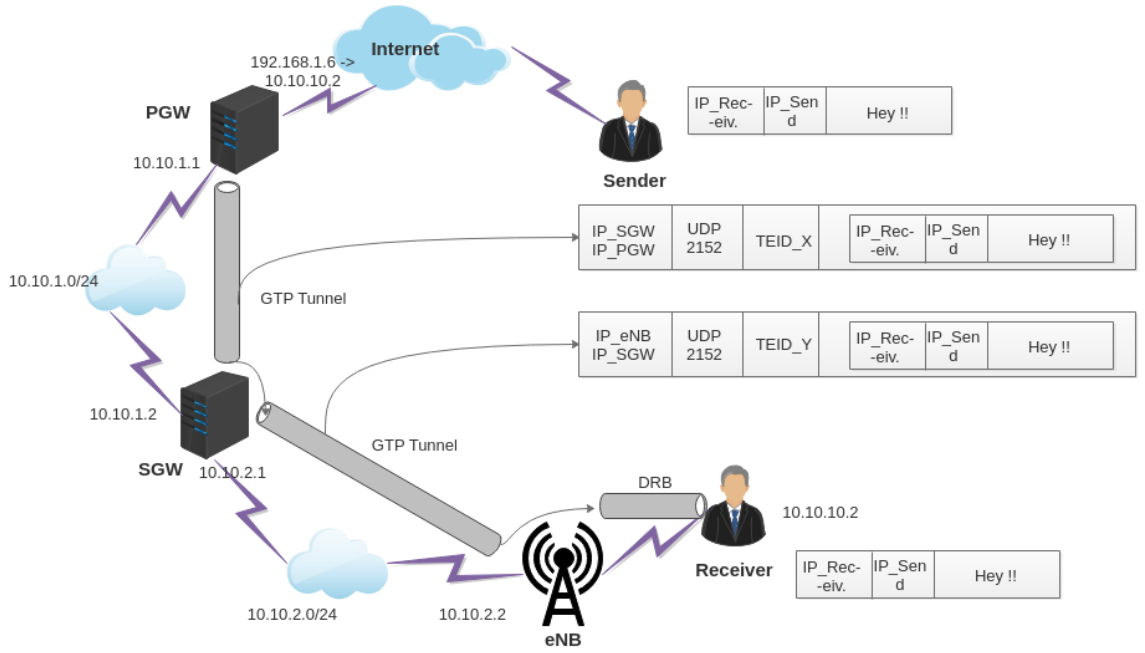

An *Access Point Name* (APN) is **the name of a gateway between a GSM, GPRS, 3G and 4G mobile network and another computer network, frequently the public Internet**.

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

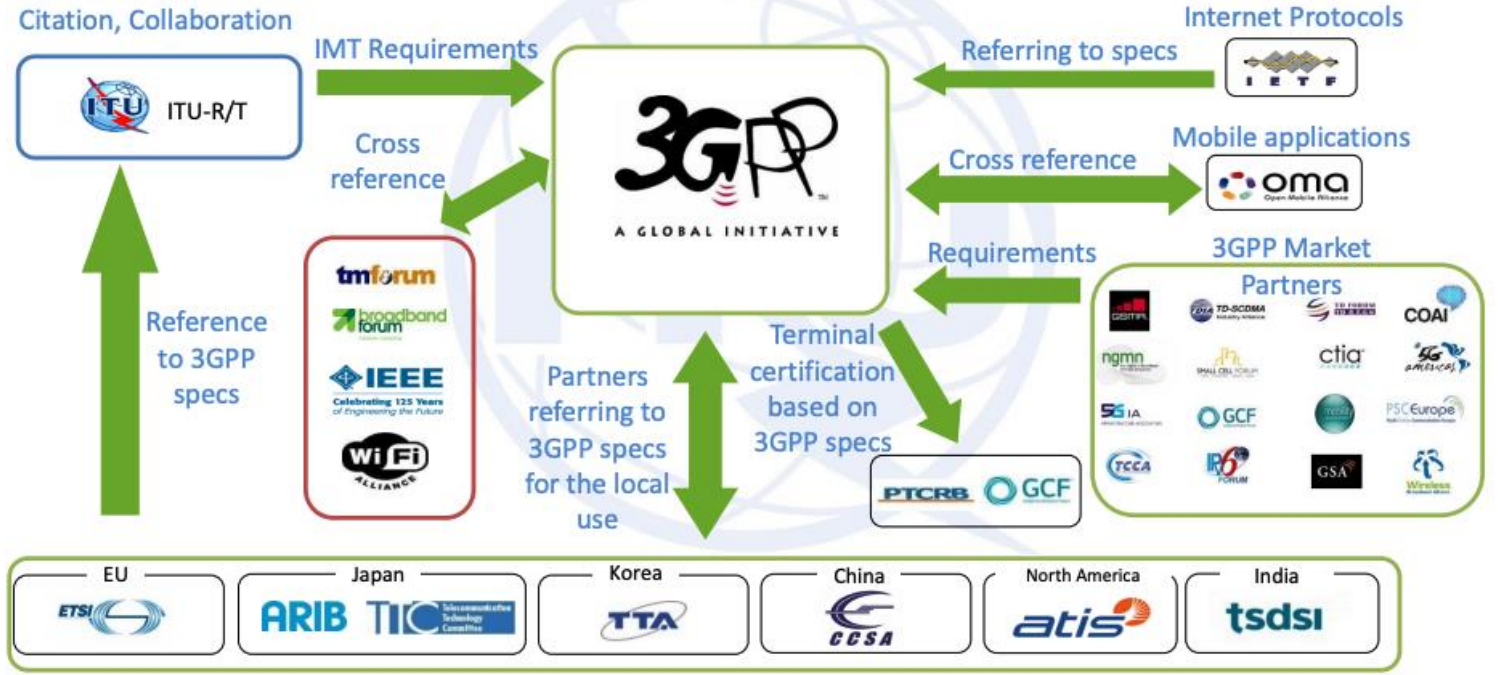
## Universal Mobile Telecommunication System

# 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**."



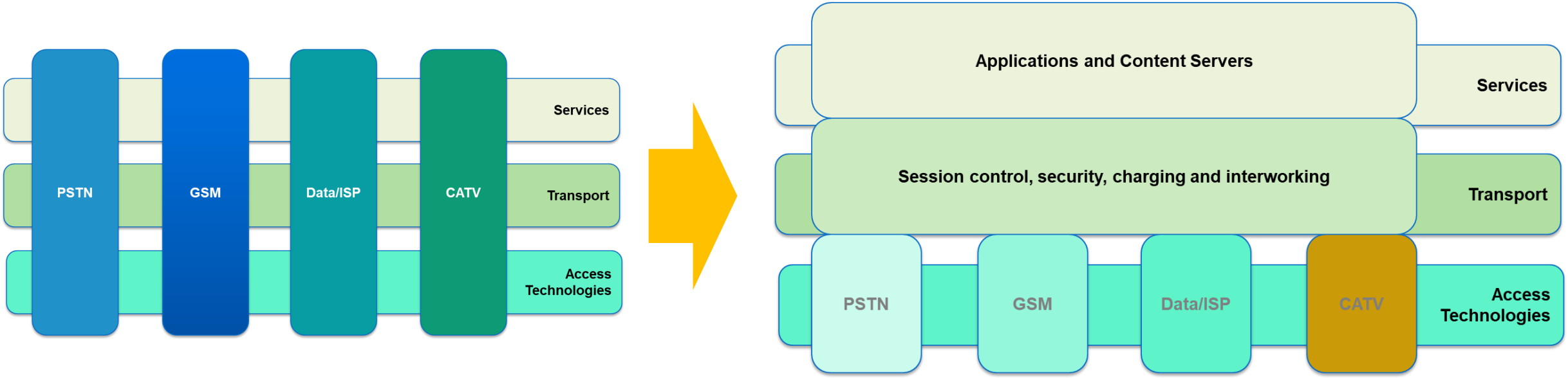

KEY INSIGHT: **Delegates to each body do the work** (in 3GPP, or other SDOs.)
Sharing information, citation, alignment can be done by LS.

**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

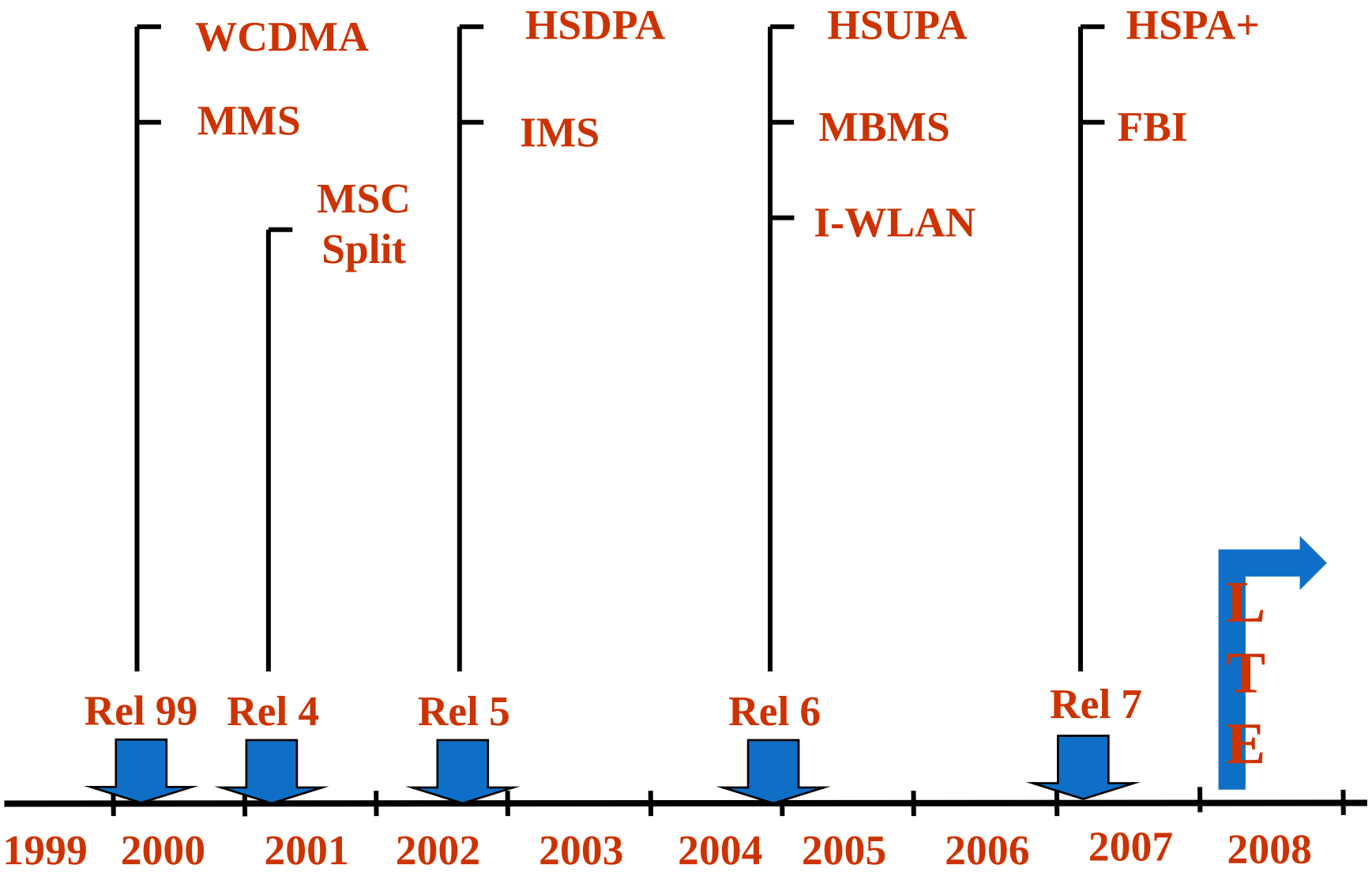
Max. 384 Kbps for global coverage (initially)

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**

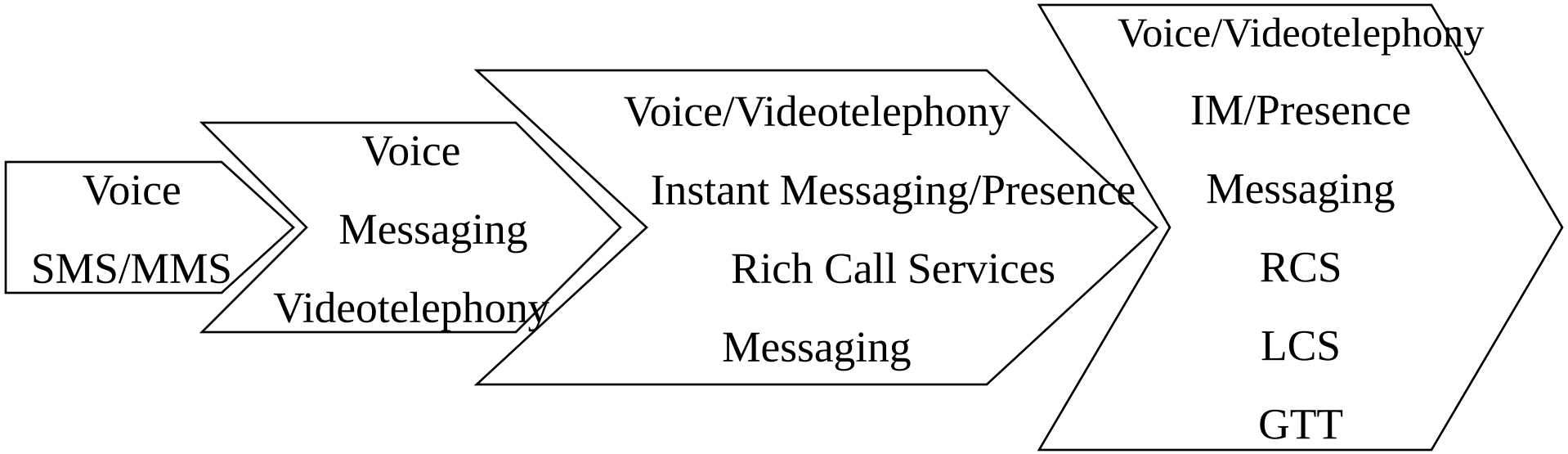
# UMTS evolution (3GPP Releases)



# 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)

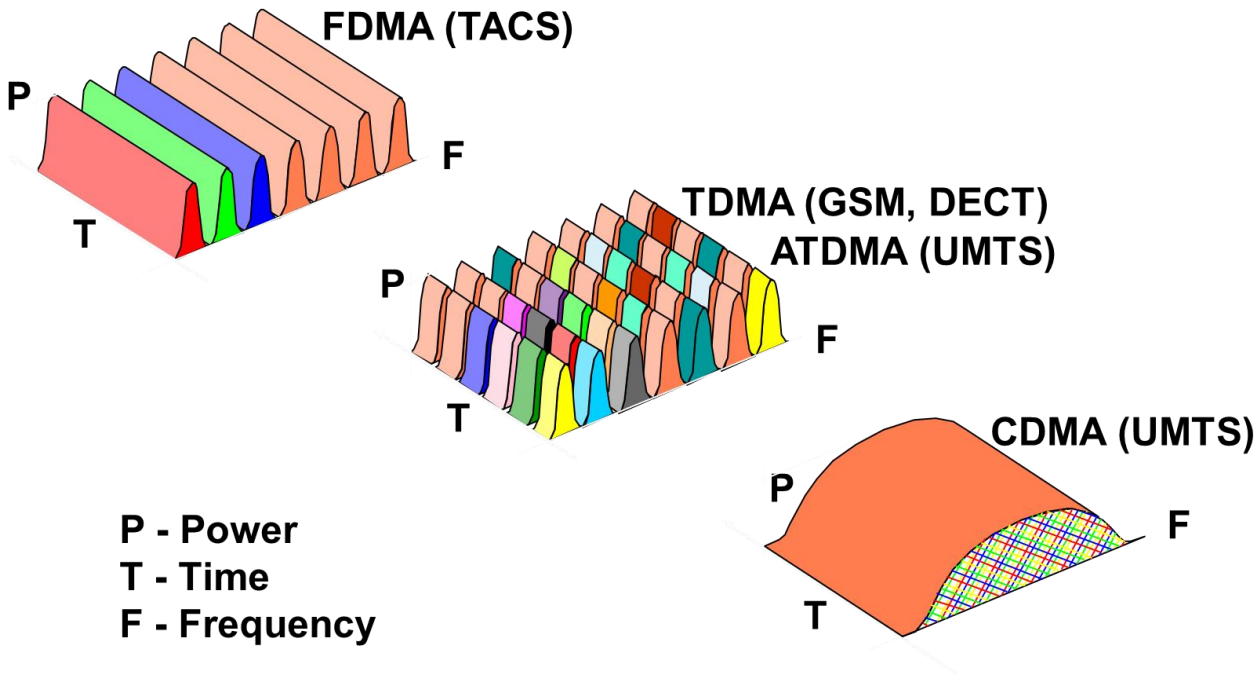


# UMTS – air interface

- **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



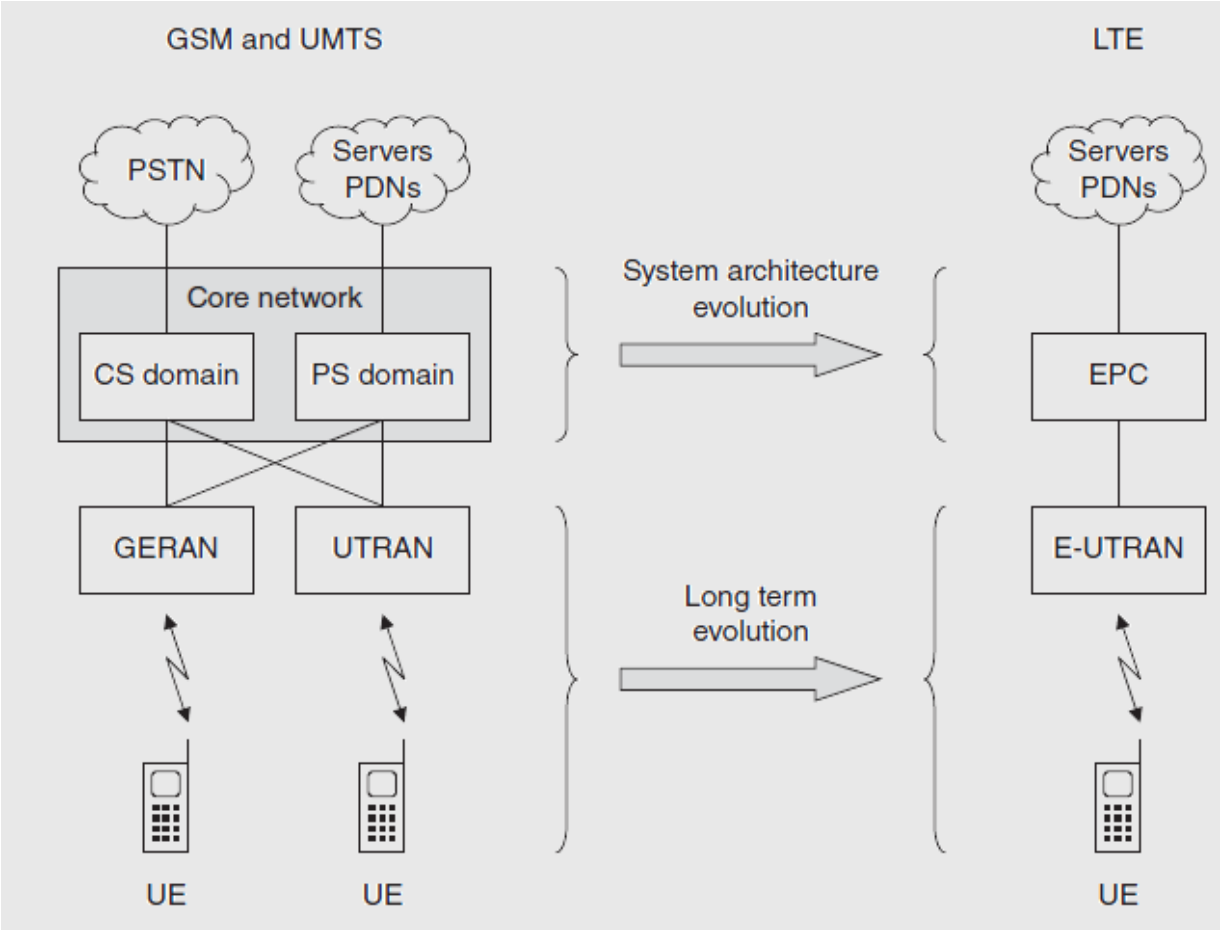

**CDMA is a form of direct-sequence spread-spectrum technology that allows many users to occupy the same time and frequency allocations in a given band/space. CDMA assigns each user a unique spreading code to spread the baseband data before transmission, in order to help differentiate signals from various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

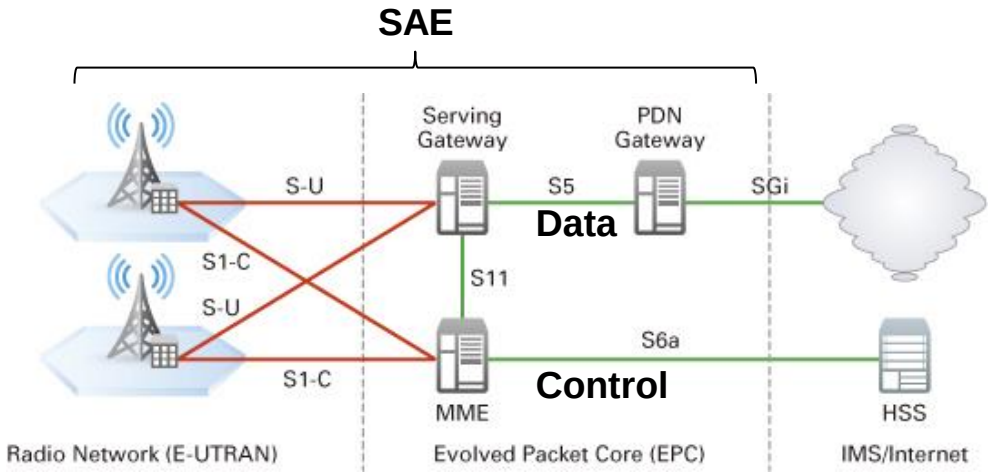
# Network simplification



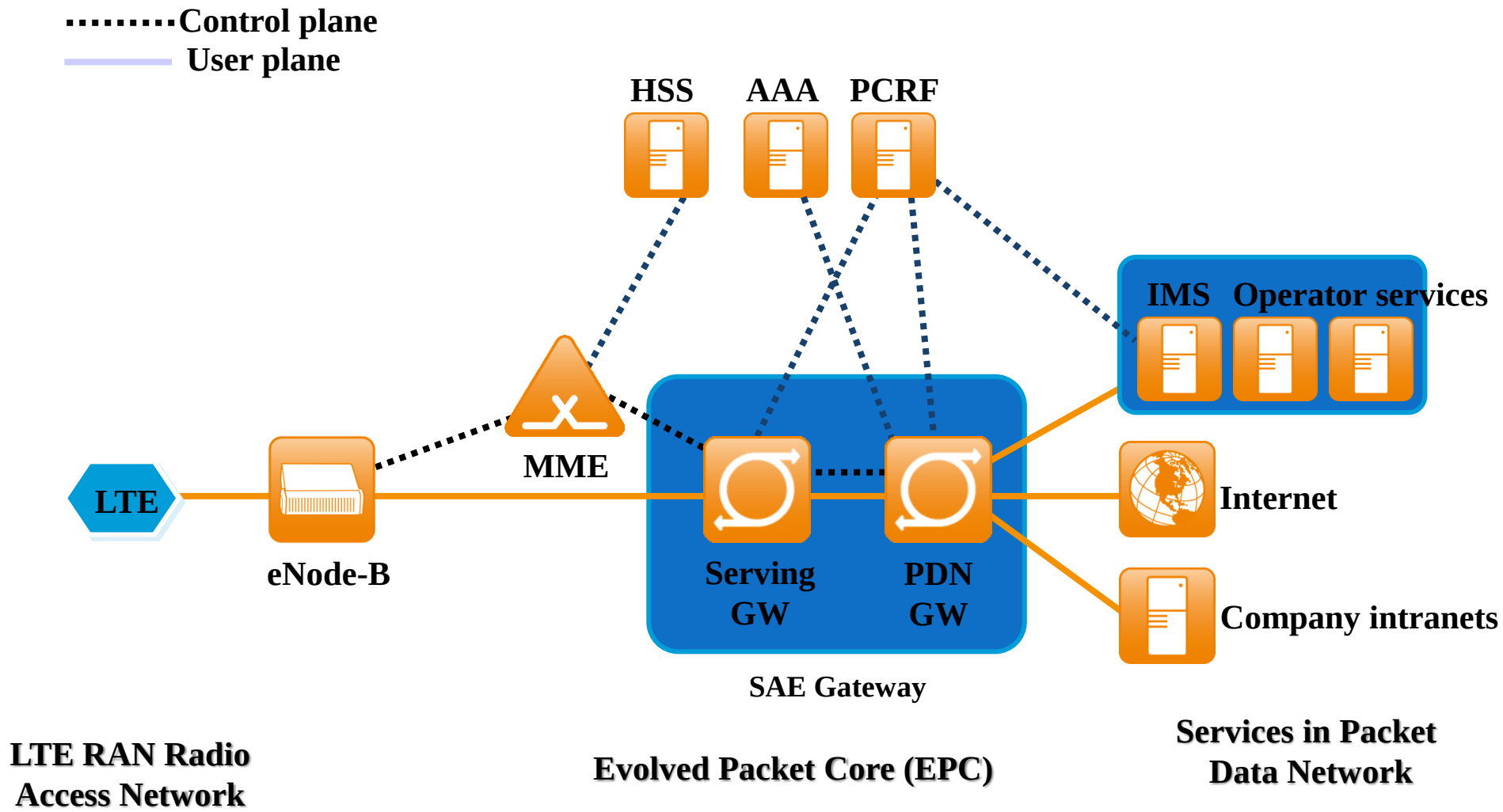

| Feature | UMTS | LTE |
|---|---|---|
| IP version support | IPv4 and IPv6 | IPv4 and IPv6 |
| USIM version support | Release 99 USIM onwards | Release 99 USIM onwards |
| Transport mechanisms | Circuit & packet switching | Packet switching |
| CS domain components | MSC server, MGW | n/a |
| PS domain 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

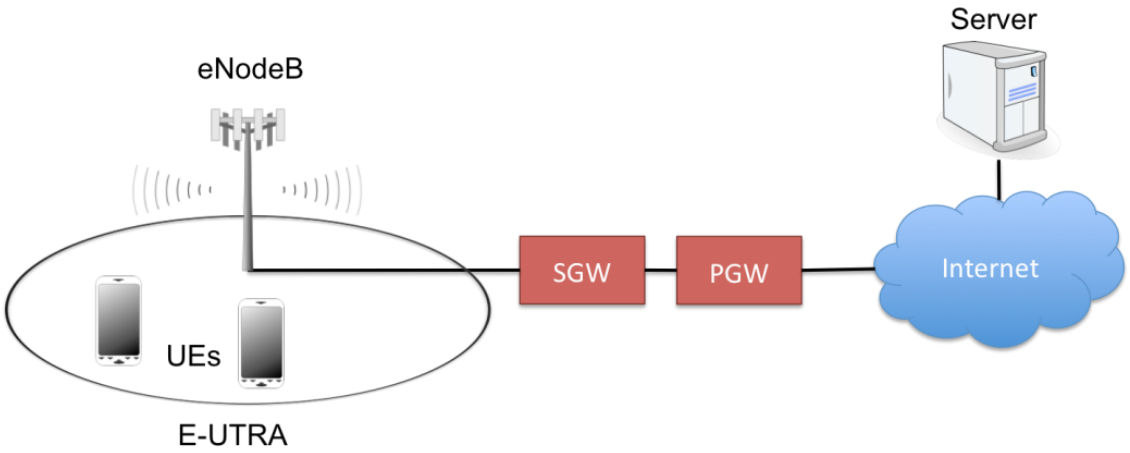
- **SAE focus is on:**
  - **enhancement of Packet Switched technology to cope with rapid growth in IP traffic**
    - higher data rates
    - lower latency
    - packet optimised system
  - **through**
    - fully IP network
      - In addition to IMS services available in the current system, equivalent 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

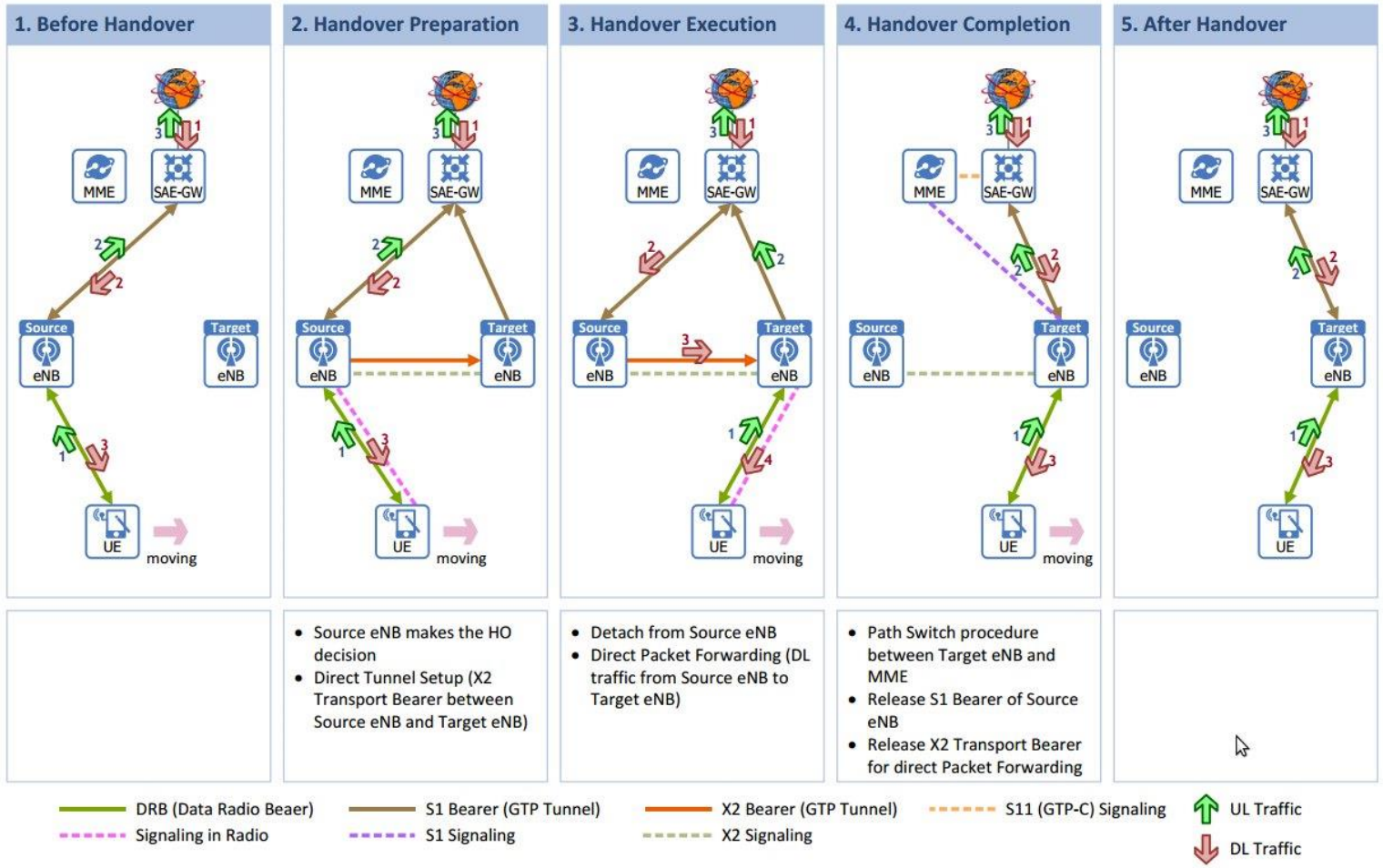


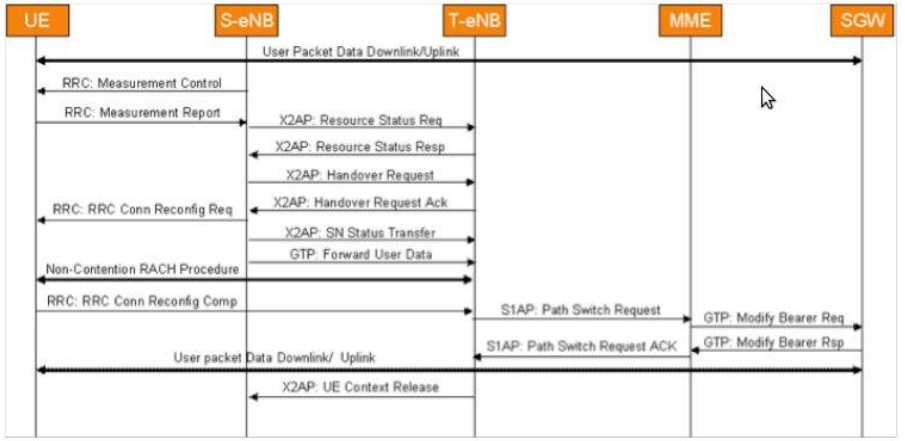
# LTE Network




- **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




https://www.3glteinfo.com/intra-lte-handover-using-x2-interface/

# 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, CELL_PCH, URA_PCH, RRC_IDLE | RRC_CONNECTED, 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*)