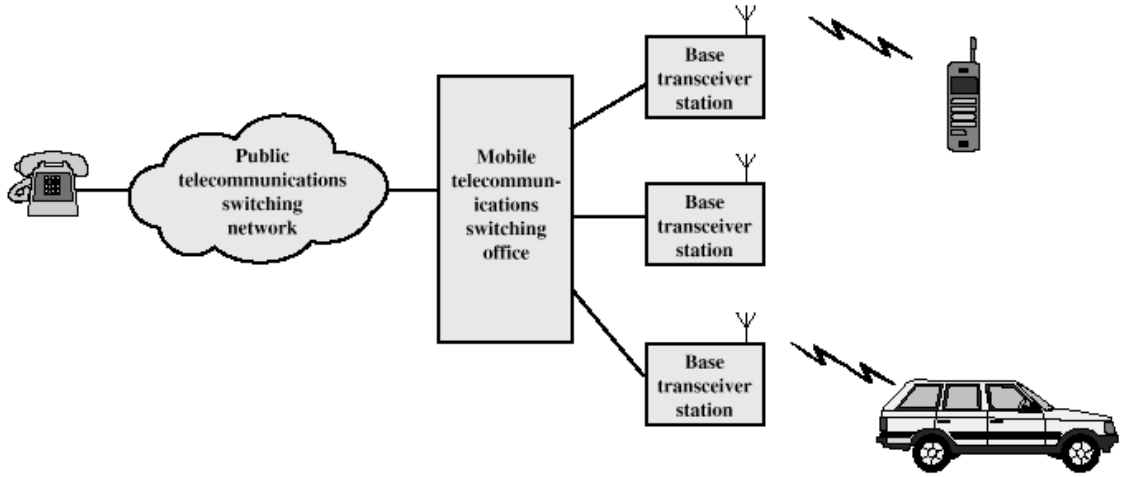
Cellular Networks

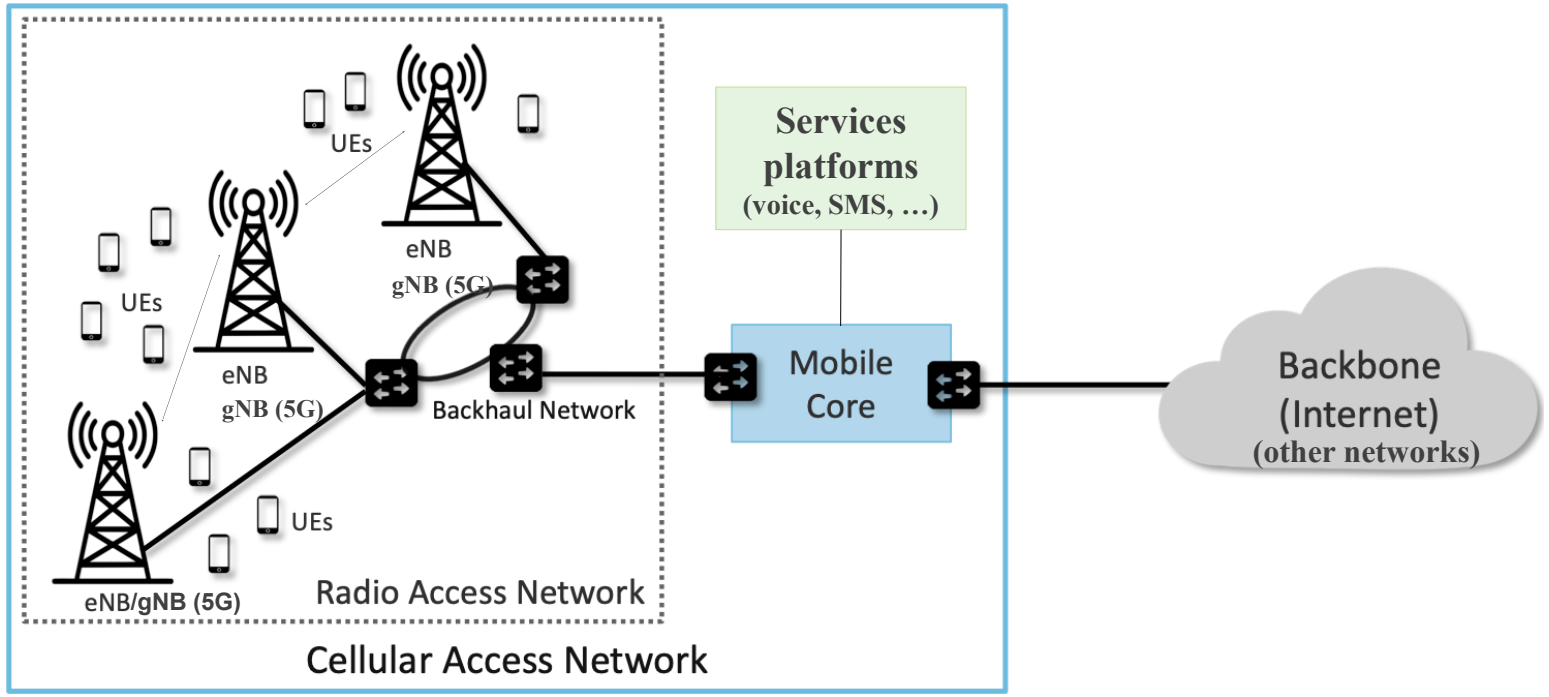
Mobile cellular networks
GSM to SAE (4G)

Wireless CELLULAR network

- **Single hop widespread wireless connectivity to the wired world**
  - **Covered area is divided into cells**
    - Mobile Terminals or User Equipment (MT/UE) is assigned and connected to a cell
  - **A Base Station (BS) is responsible for the MT/UE communication within its cell**
    - Communications: a voice call or a data session
  - **Continuous mobility support is paramount**
    - Handoff/handover (HO) operations occur when a MT/UE moves to a new base station, while busy on a call
  - **Highly supported by a fixed (wired) transport network**
- **Cell size:**
  - **Highly variable, depending on:**
    - Location (e.g. rural vs urban)
    - Expected number of users
    - Required bandwidth
    - Technology
    - Frequency band used
    - …



Generic cellular network architecture



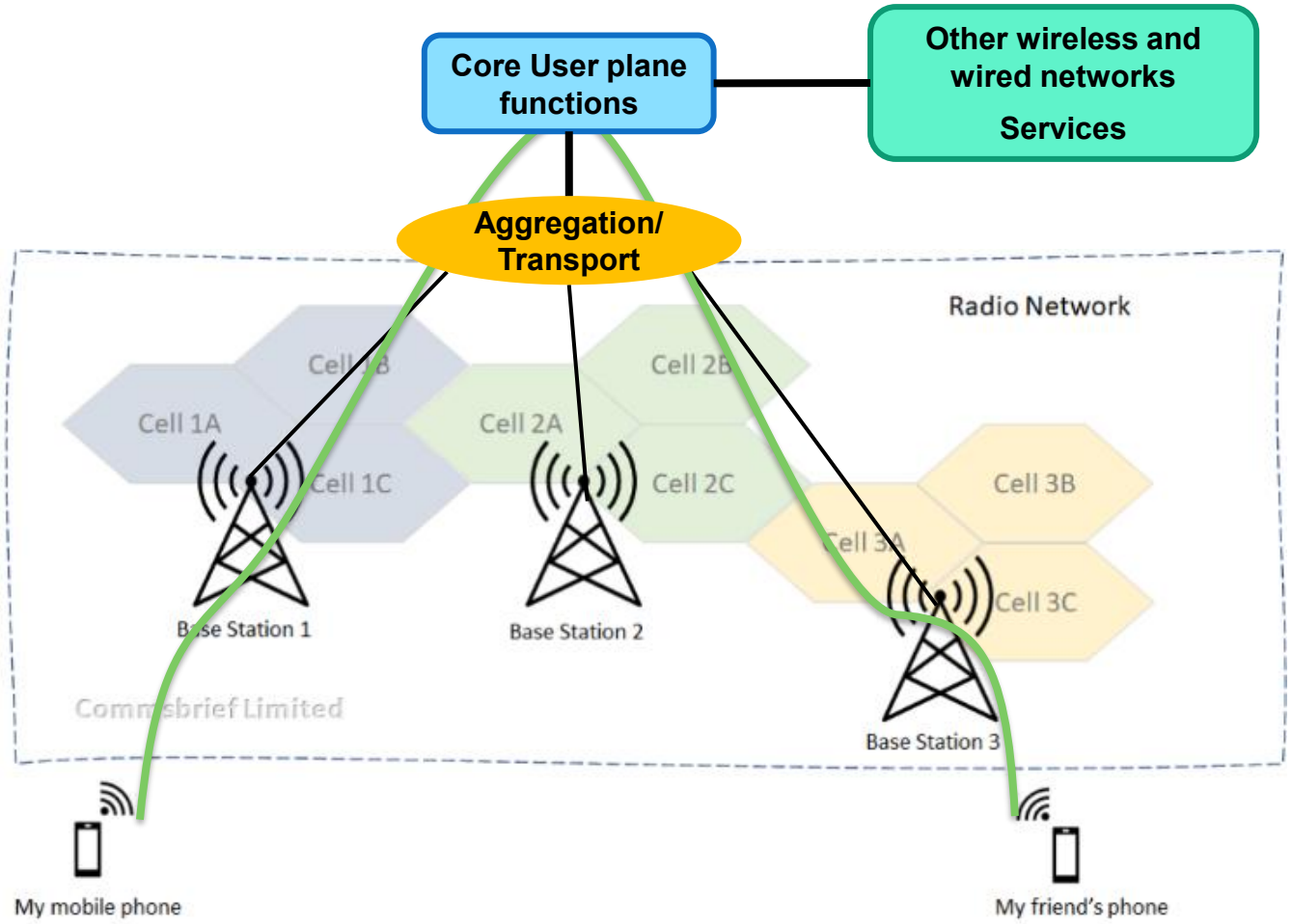
Only the communication between the MT/UE and eNB (4G)/gNB (5G) is radio based

'Mobile networks' are heavily supported on the fixed network (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



1.Your mobile phone connects to the nearest base station using wireless radio signals.

2.This base station forwards your communication request to the core network.

3.The core network then directs your request to the appropriate destination, either another base station for a different mobile user or e.g. the Internet for data services.

4.All these base stations are interconnected, creating a large web of coverage that allows your mobile device to stay connected as you move.

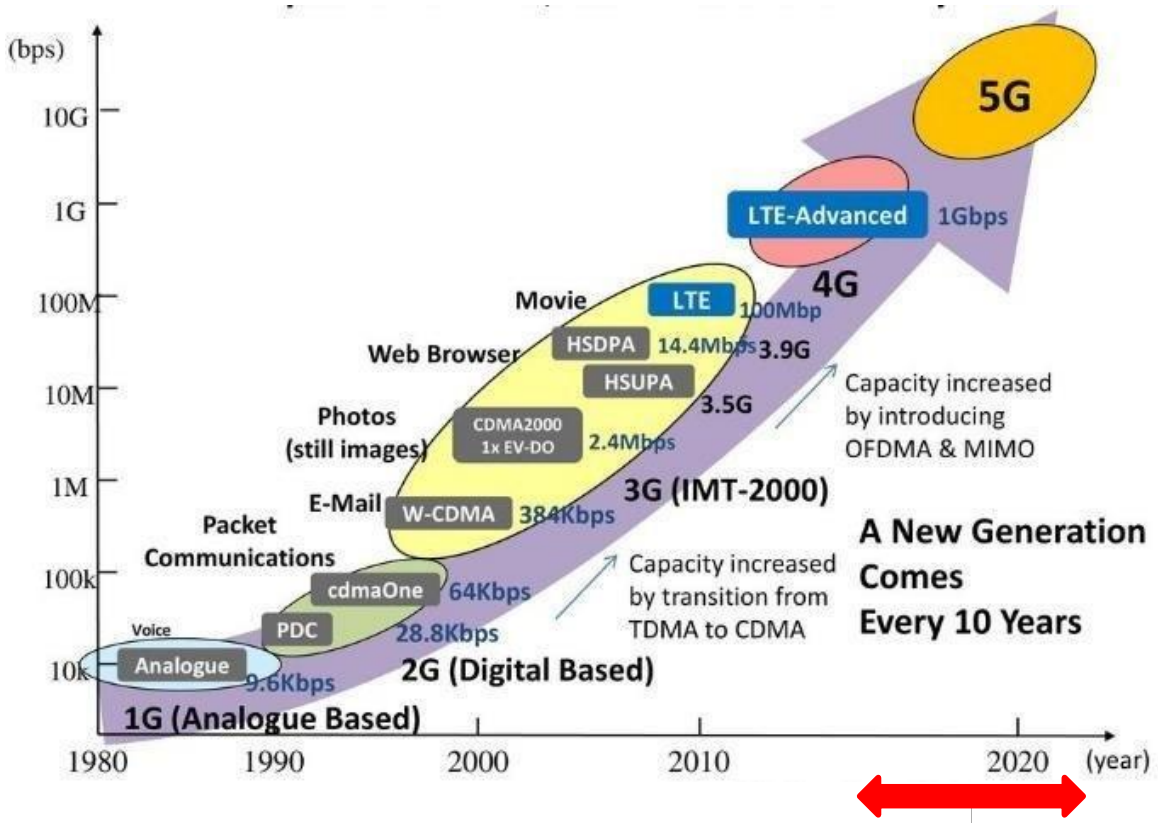
NO direct radio communication between mobiles

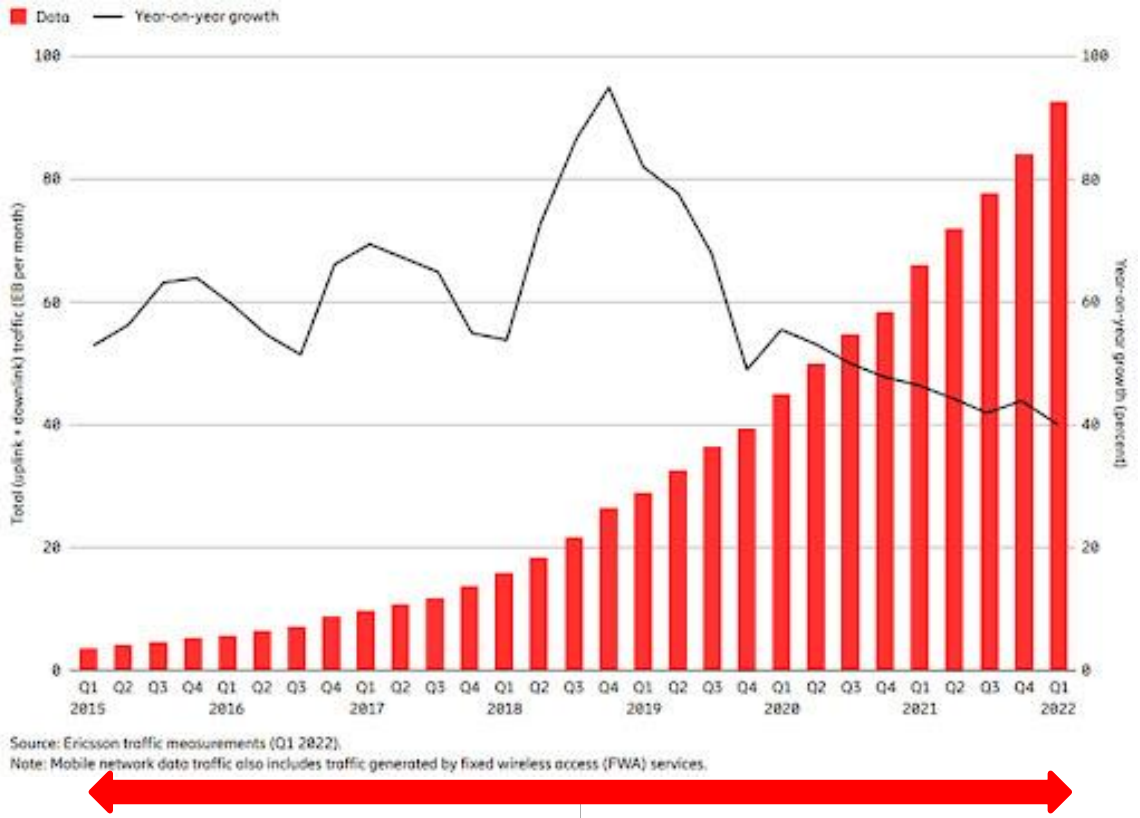
Technological waves (*Generations*)

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 < 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

Increasing spectral efficiency (more bits/Hz)

Technologies and usage evolution



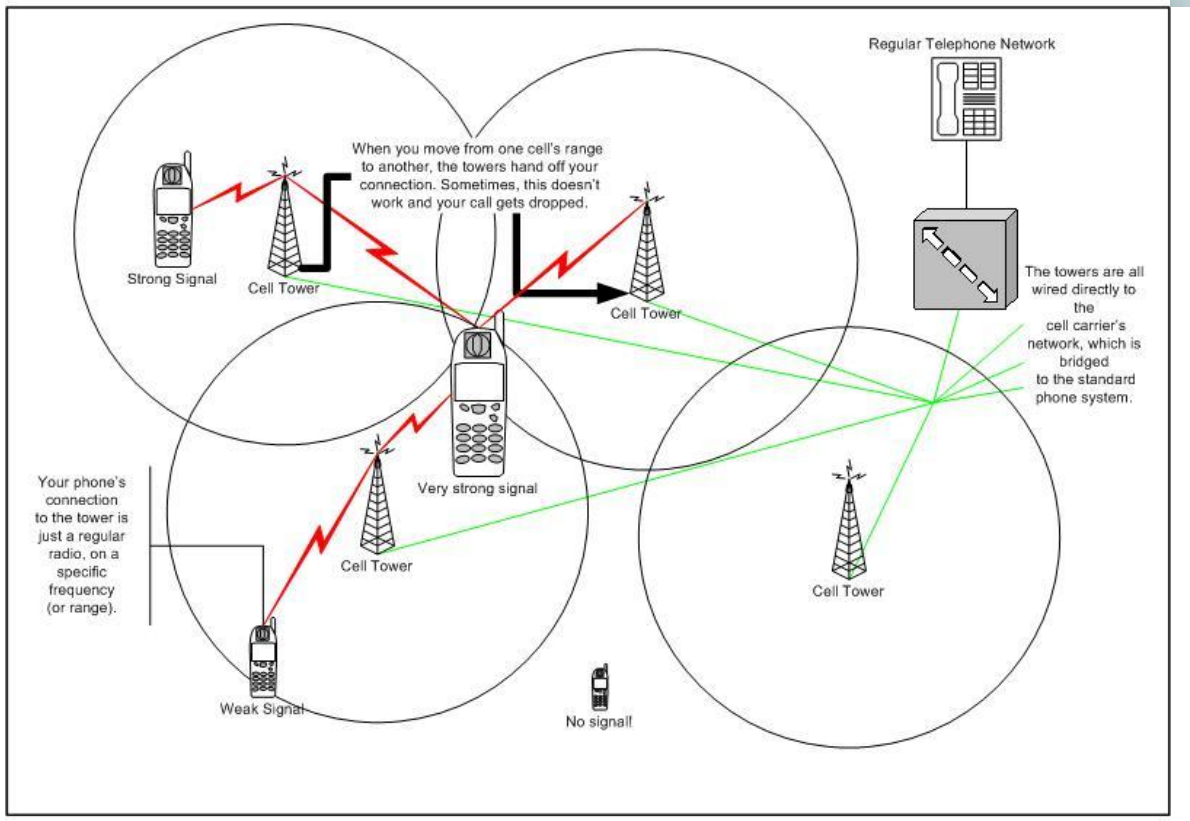


1G

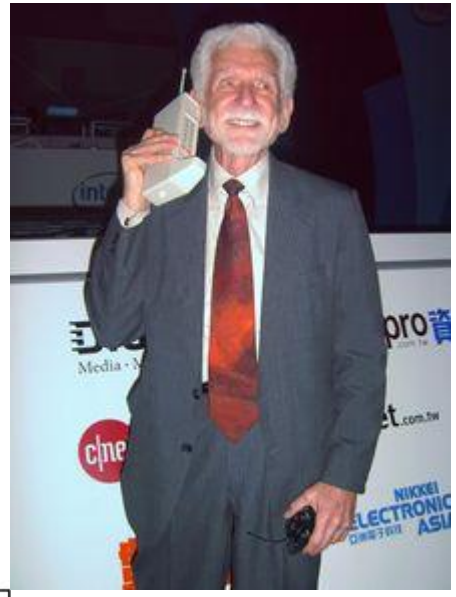
Mobile voice

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
  - Second-generation systems are digital
- Encryption
  - Provides encryption to prevent eavesdropping
- Error detection and correction
  - Results in clearer voice reception
- Channel access
  - Allow channels to be dynamically shared by a number of users

Basic Architecture

- **Defines a Mobile Terminal**
  MobileEquipment (ME) + SubscriberIdentityModule (SIM)
  (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)**

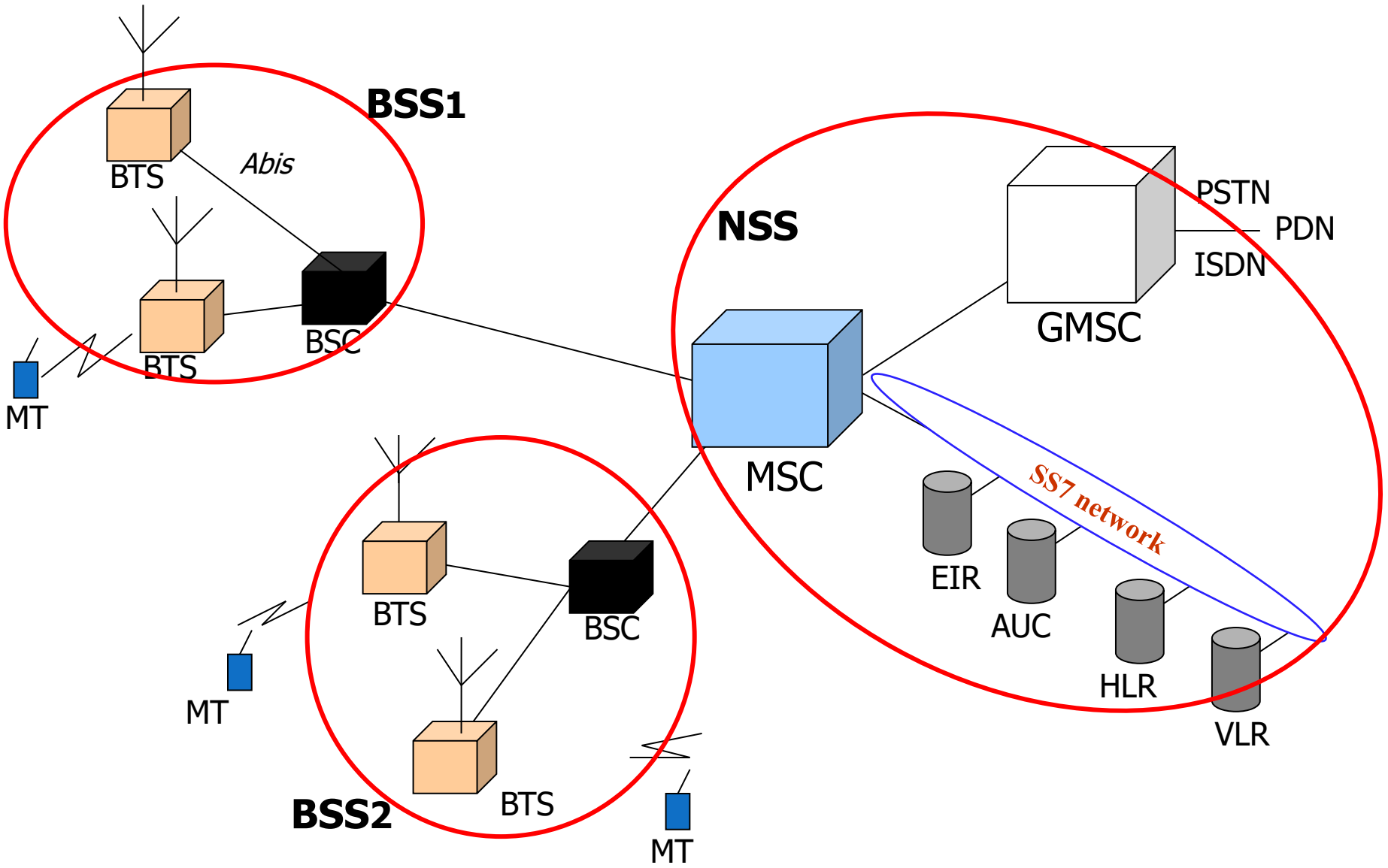
- **The Base Station Subsystem (BSS) is structured as Base Station Controllers (BSC) + Base Transceiver Station (BTS)**

- **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).**

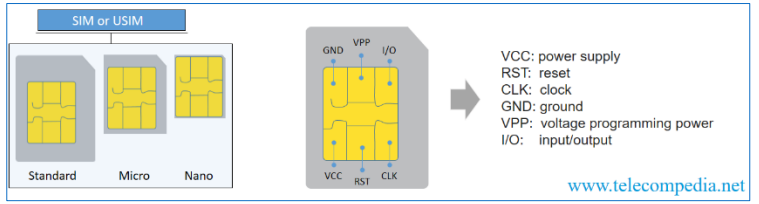
GSM Architecture



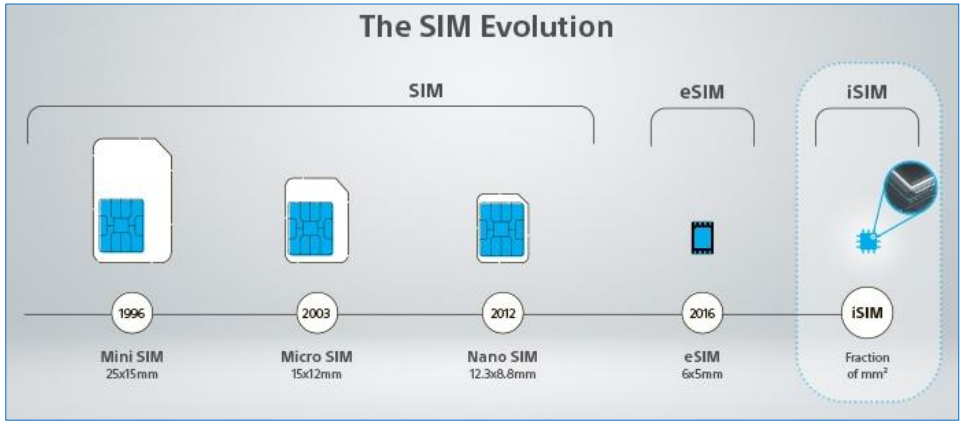
AuC: Authentication Centre
BSC: Base Station controller
BSS: Base Station Sub-system
BTS: Base Transceiver Station
EIR: Equipment Identity Register
GMSC: Gateway Mobile Switching Center
HLR: Home Location Register
ISDN: Integrated Services Digital Network
MSC: Mobile Switching Centre
MT: Mobile Terminal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

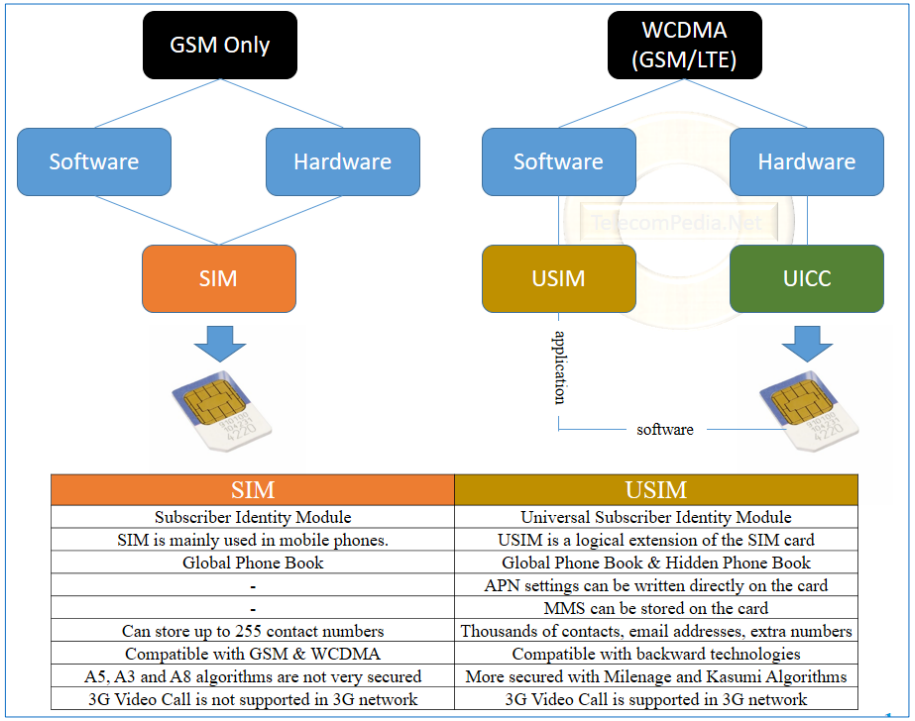
SIM: *Suscriber Identity Module*

- **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

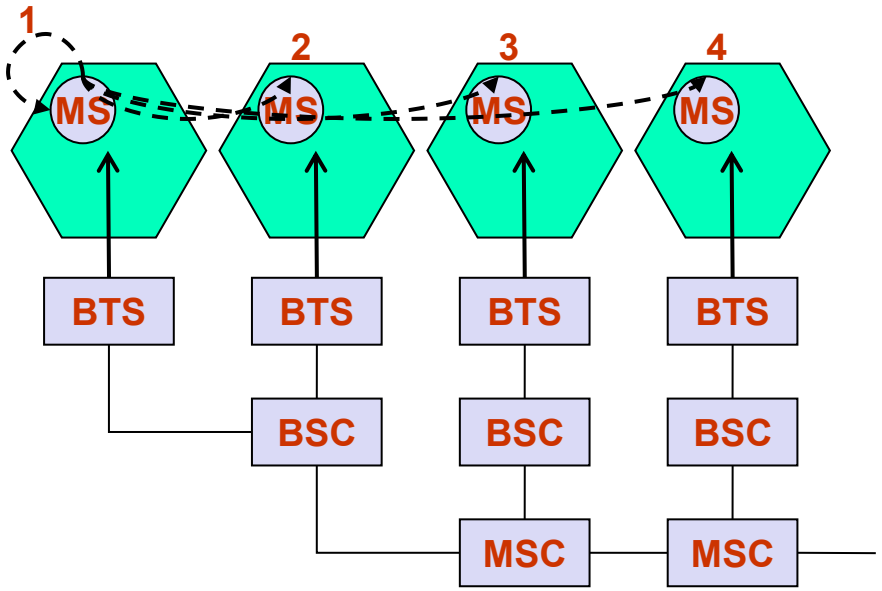
Types of handover (GSM)

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 (now 'X') 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)

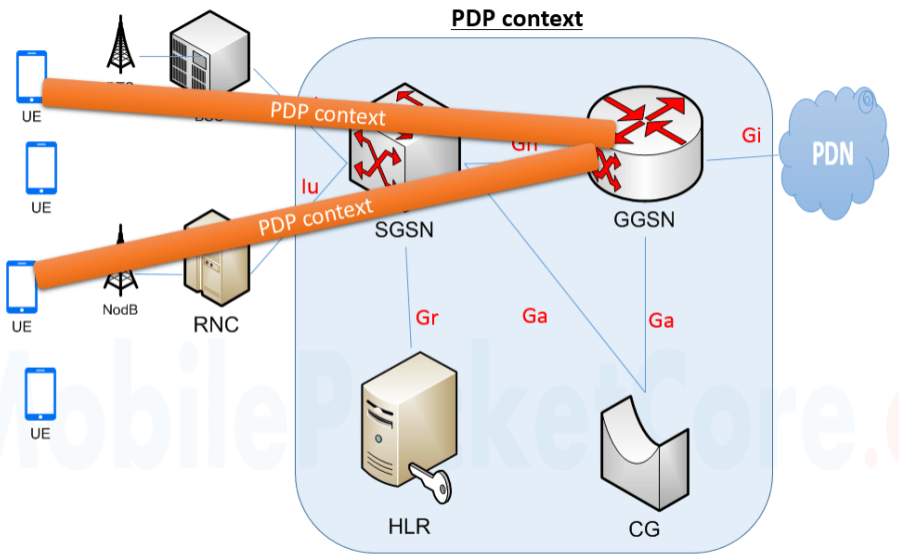
GPRS

- 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.)

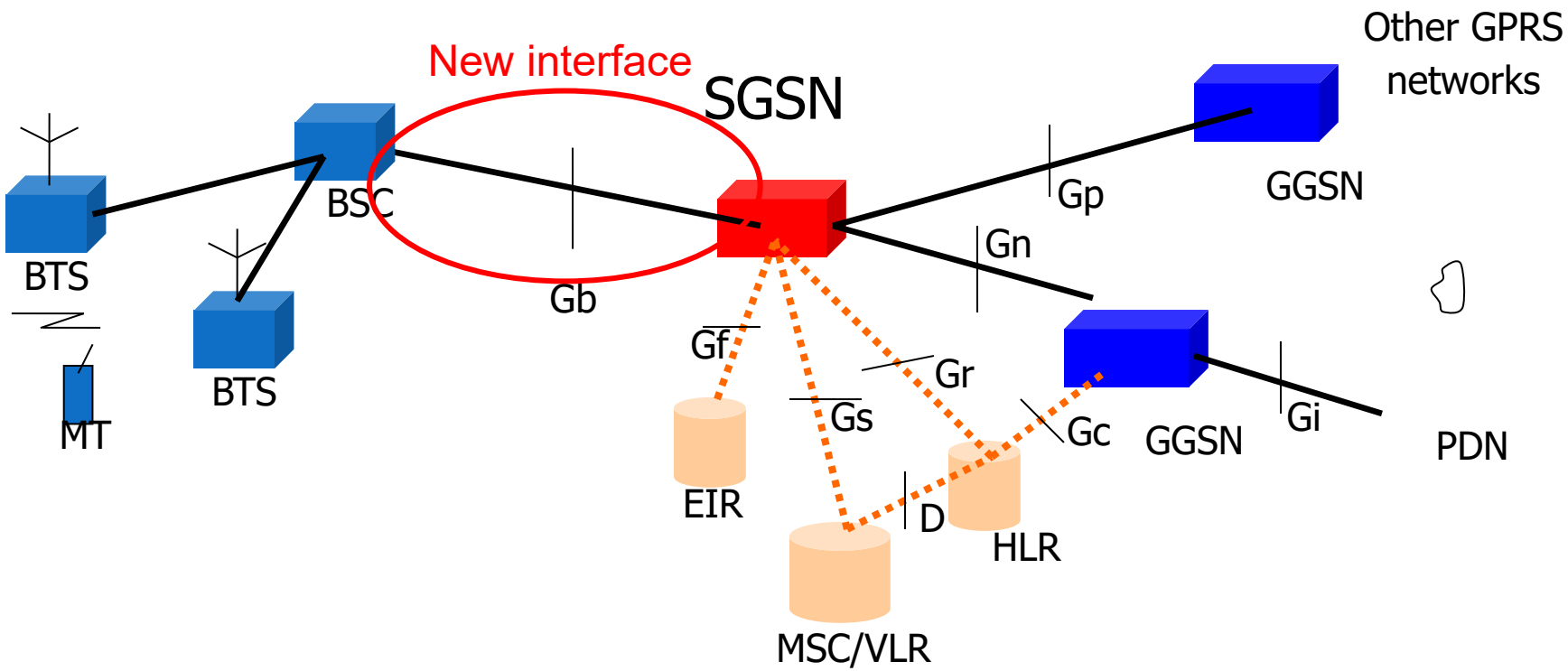
GPRS Architecture

- **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, by the establishment of a PDP Context**
- **Control plane**
  - **GTP (GPRS Tunneling Protocol): 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"**

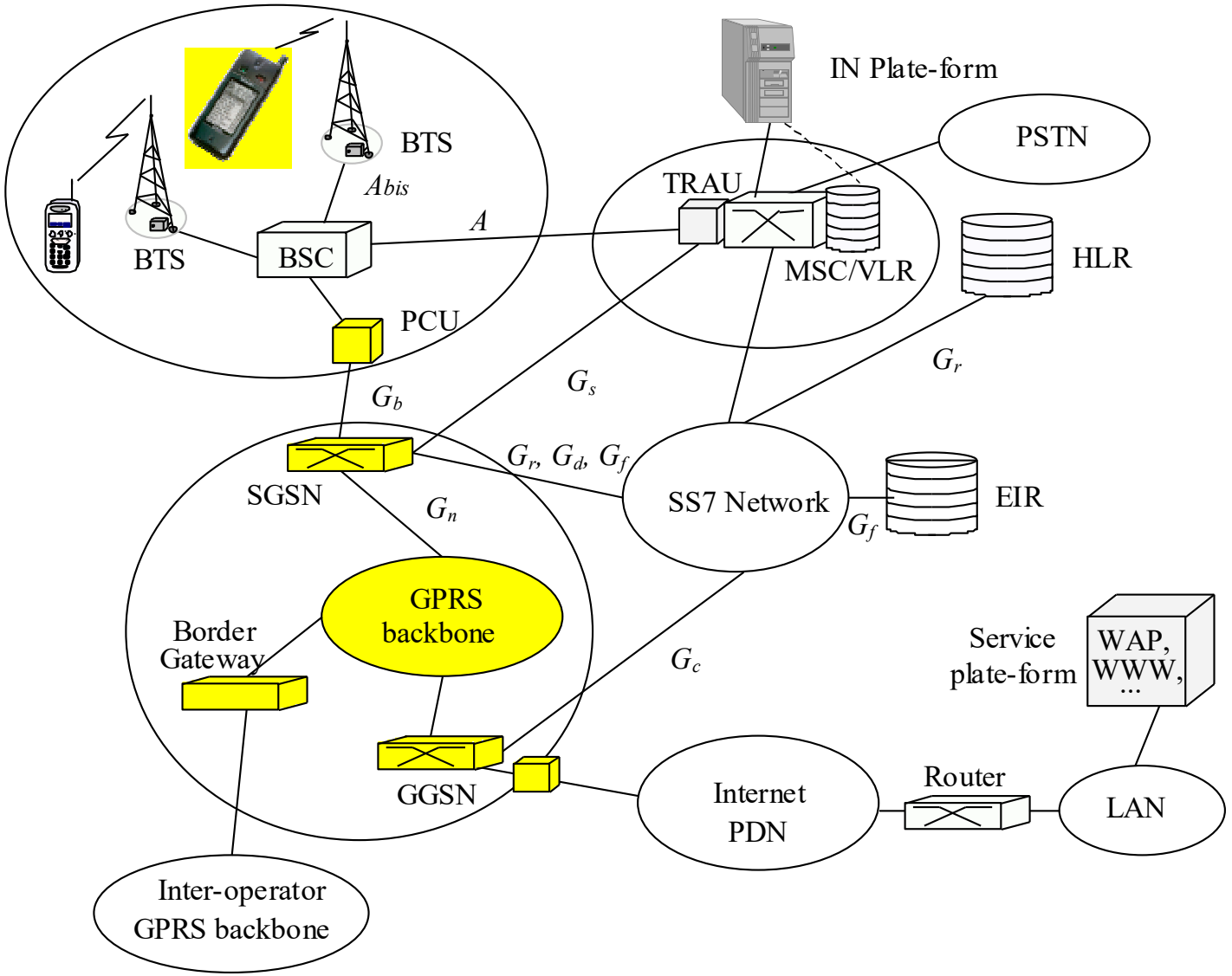


"A **PDP (Packet Data Protocol) Context** is a logical association between a MS (Mobile Station) and PDN (Public Data Network) running across a GPRS network. The context defines aspects such as Routing, QoS (Quality of Service), Security, Billing etc" (mpirical.com)

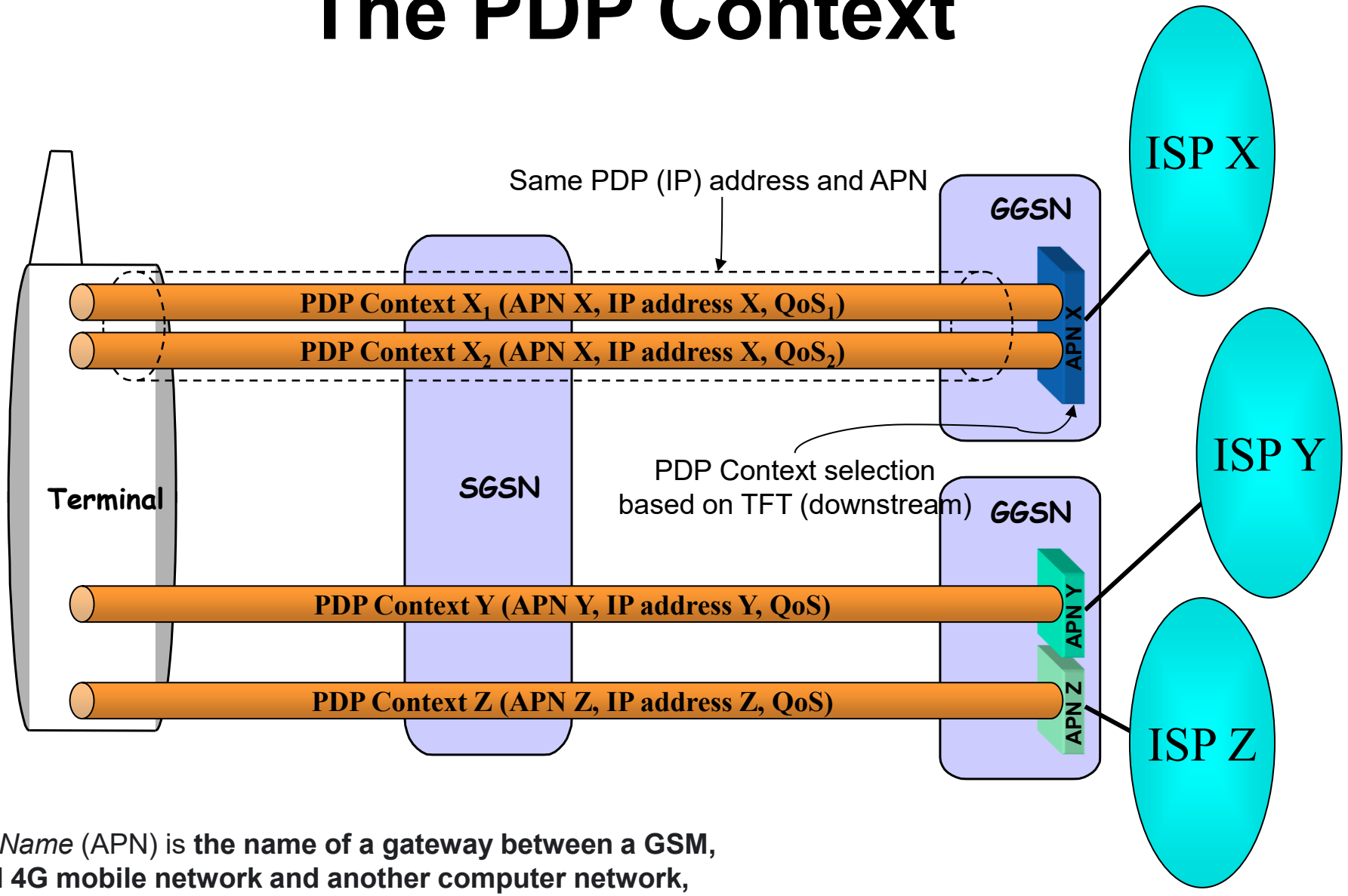
GPRS Architecture



GPRS introduction in a GSM network



The PDP Context



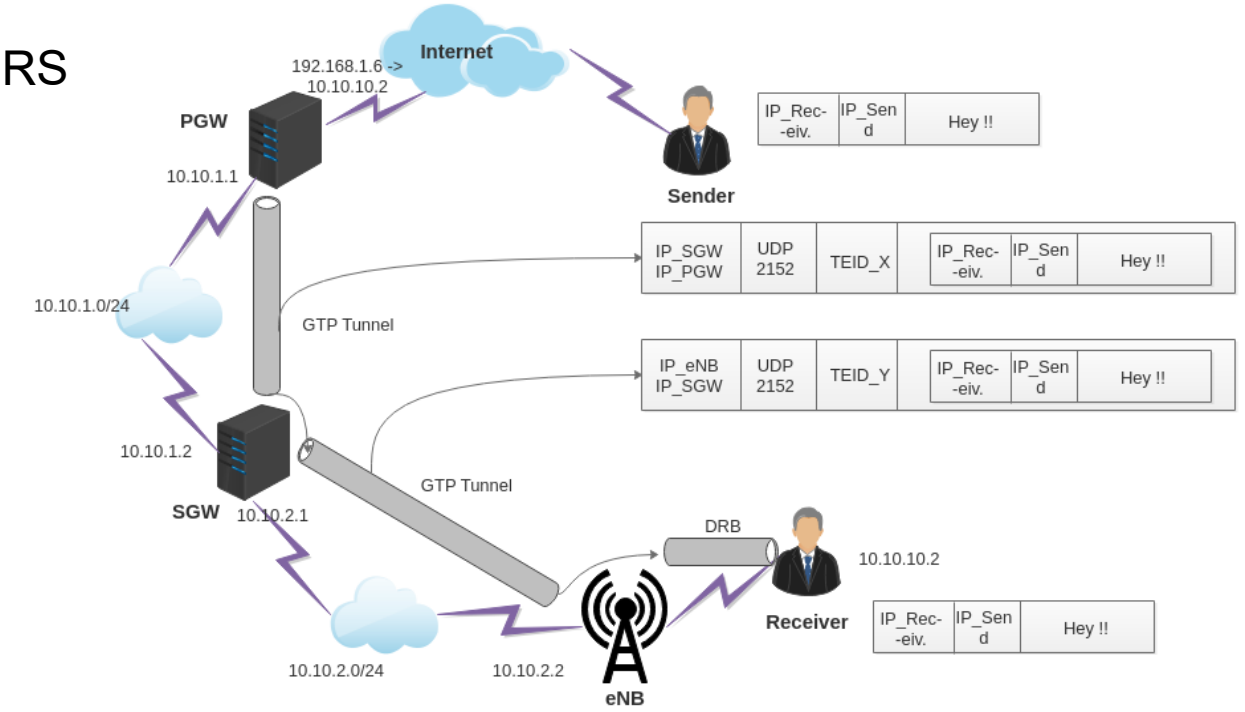
An *Access Point Name* (APN) is **the name of a gateway between a GSM, GPRS, 3G and 4G mobile network and another computer network, frequently the public Internet**.

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

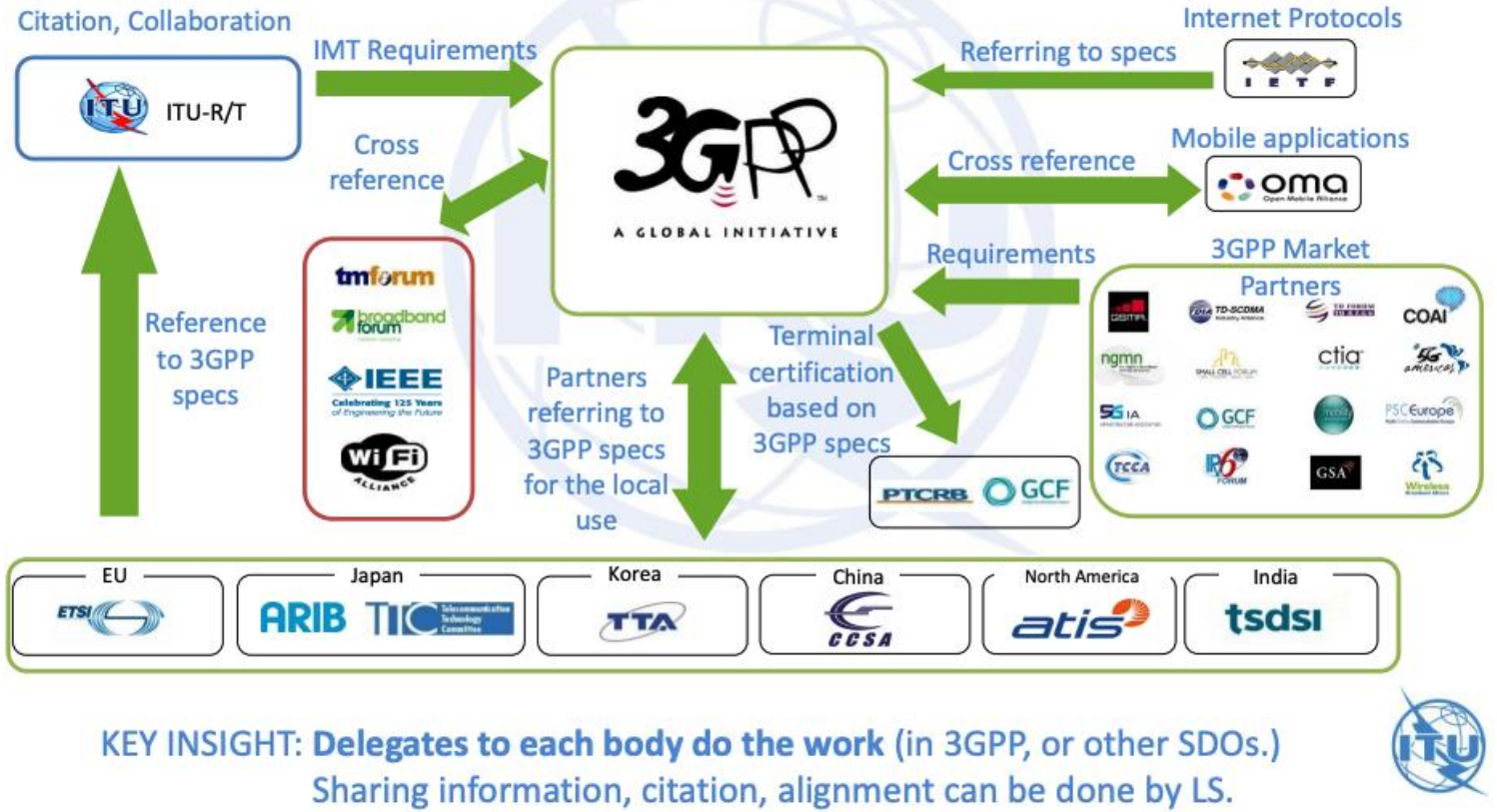
Universal Mobile Telecommunication System (UMTS)

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*

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

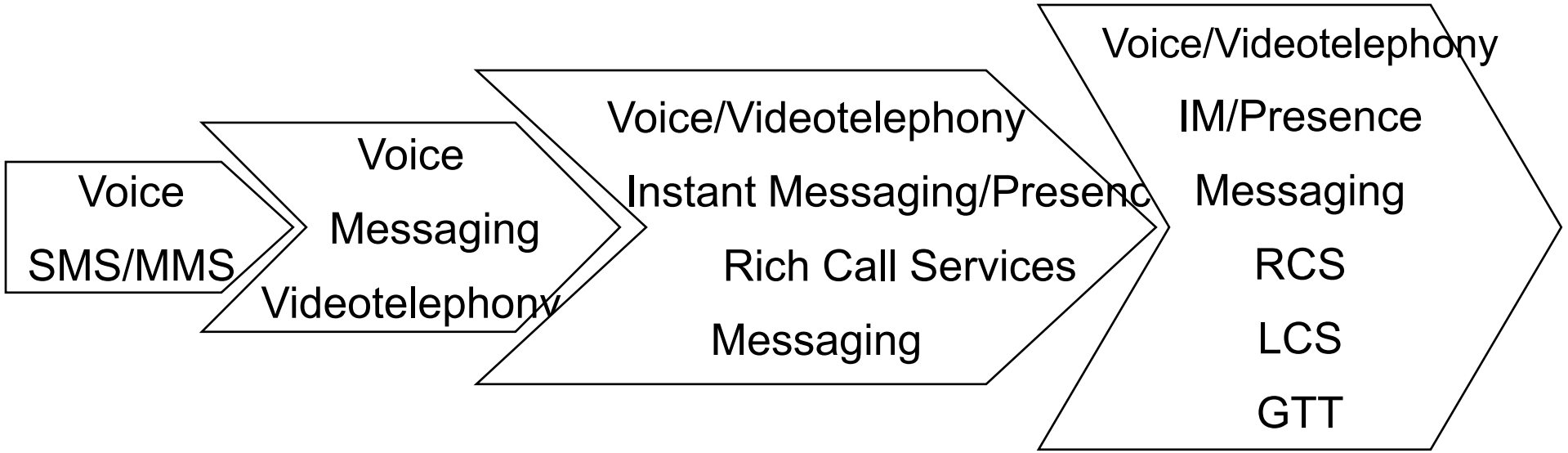
Max. 384 Kbps for global coverage (initially)

Max. 2Mbps for local coverage (initially)

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)



Advanced features (at the time)

Higher data rates compared to 2G technologies like GSM

Use of **Wideband Code Division Multiple Access (W-CDMA)** for more efficient use of the available spectrum

Improved voice quality through advanced codecs and error correction techniques

Simultaneous voice and data services, enabling activities like web browsing during a phone call.

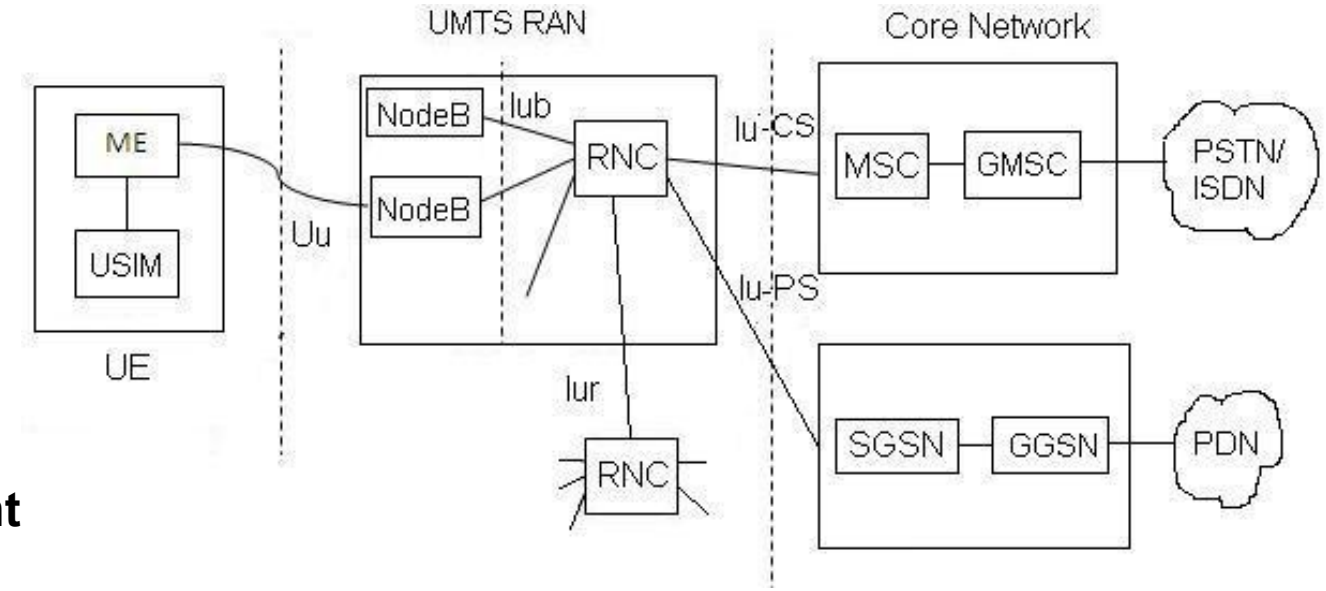
The architecture supports various applications, from basic voice calls to complex multimedia and data services, catering to both consumer and business needs.

The RNC (Radio Network Controller) in UTRAN can dynamically allocate resources based on user demand, optimizing network efficiency and ensuring quality of service (QoS).

UMTS includes robust security mechanisms, such as strong encryption and mutual authentication, protecting user data and privacy. Moreover, the architecture provides secure access to network services, reducing the risk of unauthorized use.

UMTS architecture

https://www.rfwireless-world.com/tutorials/umts-architecture-3g-network



UE: User Equipment

UMTS Terrestrial Radio Access Network (UTRAN):

- **NodeB** (Base Station): Handles the physical layer of communication with the UE, similar to the base station in GSM networks.
- **Radio Network Controller** (RNC): Manages radio resources and controls the NodeBs. It handles tasks such as handovers, power control, and connection management.

Core Network (CN):

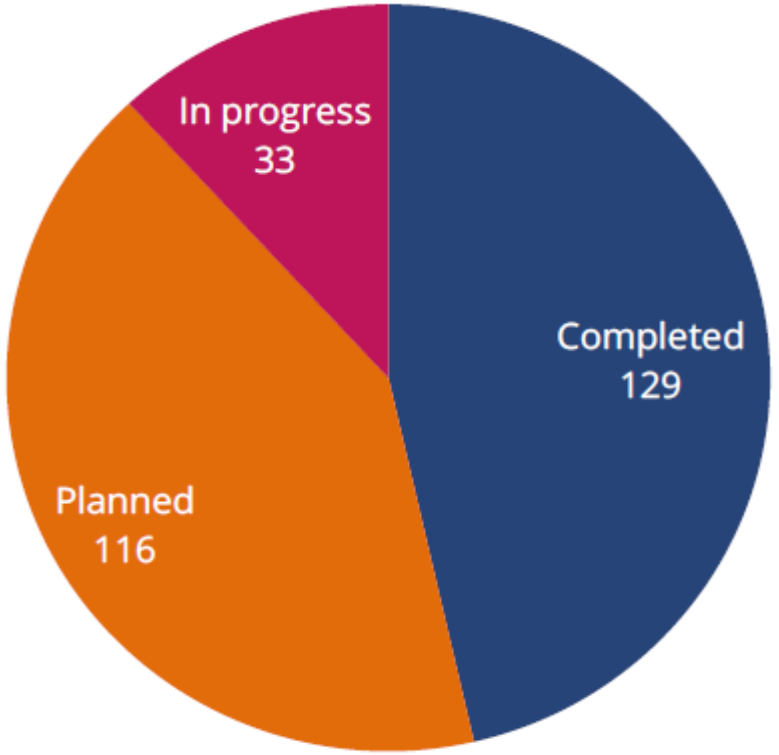
- **Circuit-Switched (CS) Domain**: Handles traditional voice calls. For CS operations, MSC and GMSC along with database modules such as VLR and HLR will be available.
- **Packet-Switched (PS) Domain**: Handles data services like internet access. For PS operations, SGSN and GGSN will serve the purpose.

2G and 3G switchoff

- **2G, 3G, 4G … 5G: too many domains to be addressed**
- **Free spectrum for newer technologies**

Enabled by:

- **Global 4G/5G coverage**
- **Migration of legacy services must be migrated: e.g. to VoLTE**

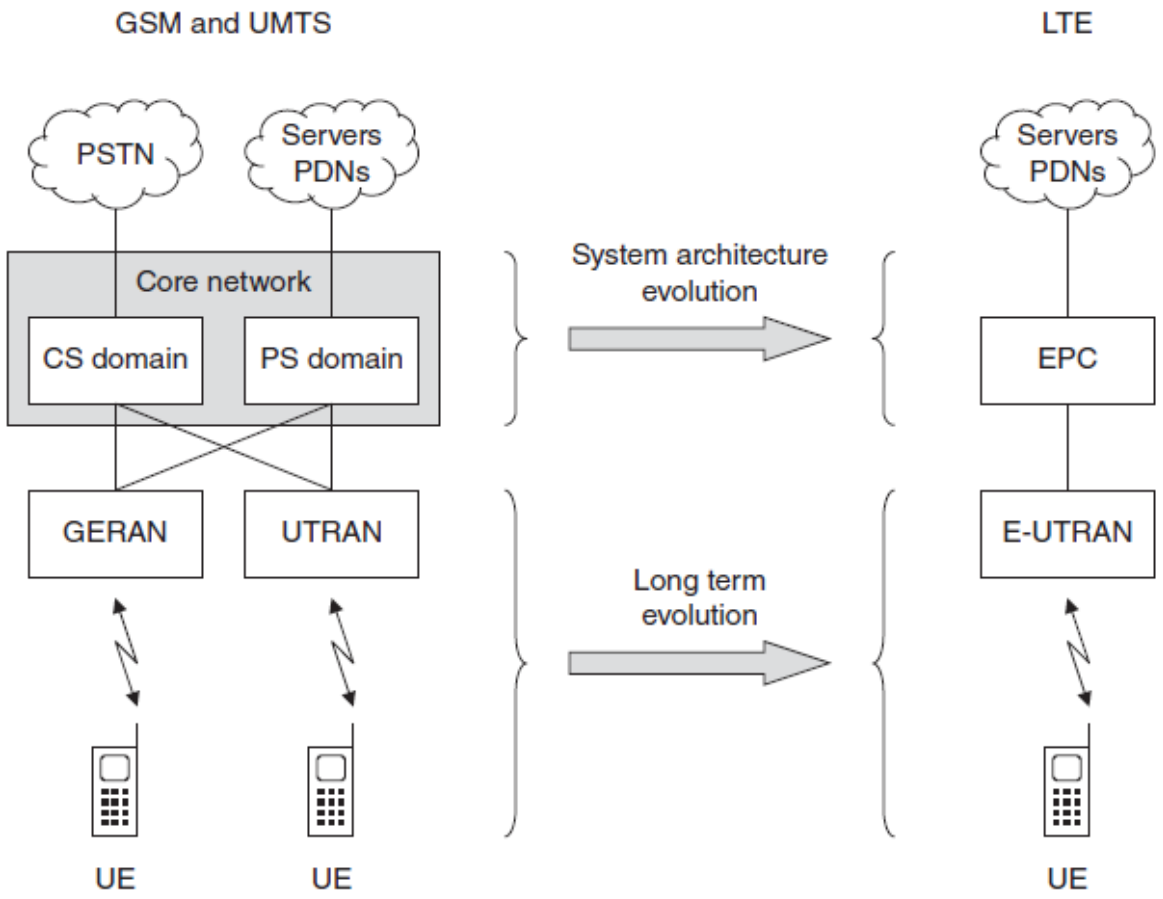


operators that have completed, planned or are in progress with 2G and 3G switch-offs to end of June 2025

4G

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

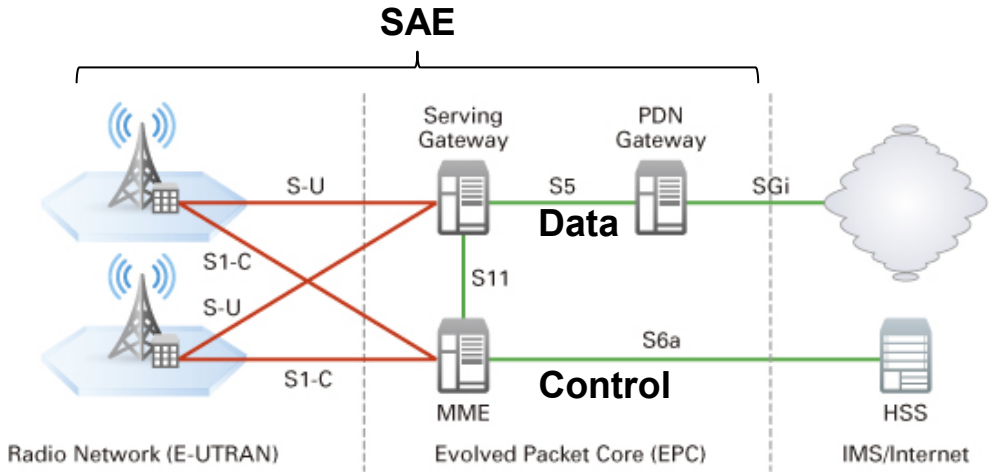
Network simplification



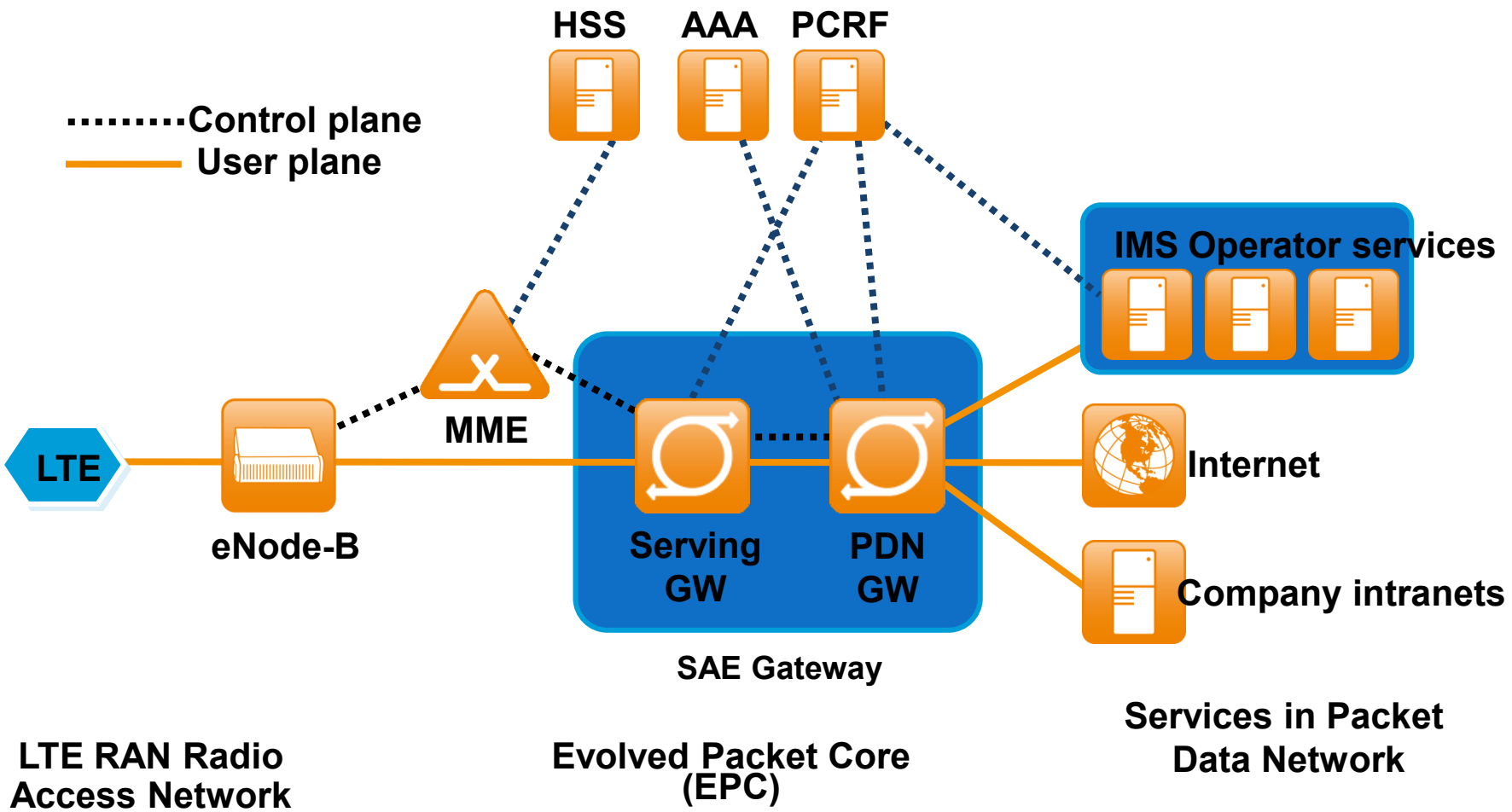
Feature	UMTS	LTE
IP version support	IPv4 and IPv6	IPv4 and IPv6
USIM version support	Release 99 USIM onwards	Release 99 USIM onwards
Transport mechanisms	Circuit & packet switching	Packet switching
CS domain components	MSC server, MGW	n/a
PS domain components	SGSN, GGSN	MME, S-GW, P-GW
IP connectivity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



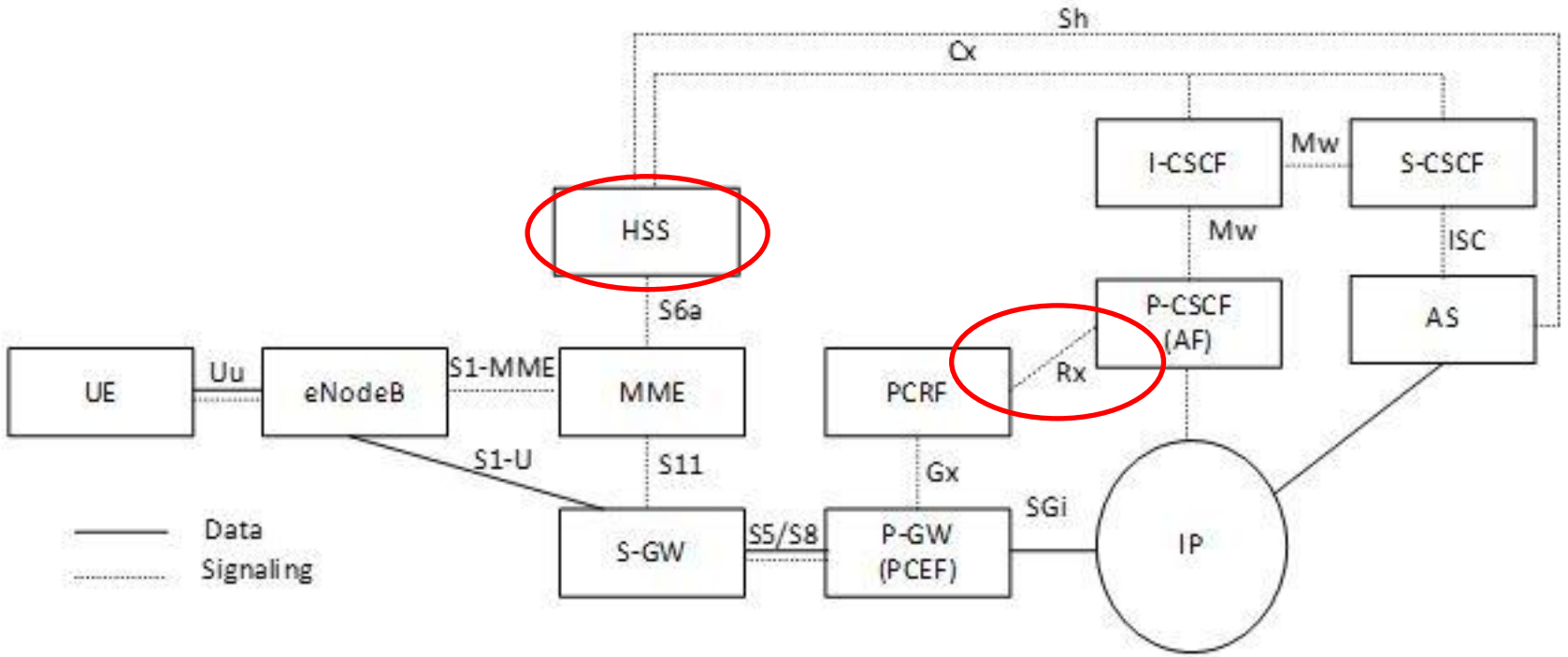
EPC architecture



- 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

VoLTE (Voice over LTE)

Exploits IMS () as the service platform, tightly integrated with the network (Rx interface)
Common HSS to host customer profile and data (connectivity and services)



https://ghbintellect.com/lte-ims-technology-white-paper/