Faculty Orientation Program

on

BE (E&TC) Revised Syllabus_2019 Course

Mobile Computing

Unit 2: Mobile Telecommunication System

under the aegis of

Board of Studies E&TC, SPPU, Pune.

[30/01/2023 to 01/02/2023]

By – Prof. R R Itkarkar

AISSMS COE Pune

Introduction to Cellular Systems, GSM architecture, Protocols, Connection Establishment, Frequency Allocation, Routing, Mobility Management, Security, GPRS and UMTS: Architecture, Handover, Security.

Introduction to 5G: Introduction, 5G network architecture, Applications, 5G enable technologies, Recent trends in Telecommunication Industries

CO2: Analyse next generation Mobile Communication System.

Unit- II Mobile Telecommunication System	
Contents	Text Book & Page no
Introduction to Cellular Systems,	R1 (2.8, ch-4 pg no 93-100)
GSM architecture,	R1-(pg no100-110 (4.1.2 & 4.1.3)
Protocols,	R1- (pg 110 - 113 (4.1.4)
Connection Establishment, Mobility Management	R1 (pg 113-117 (4.1.5)
Frequency Allocation, Routing, ,	R1 Pg 72,73,75
Security,	R1 pg 120-122) (4.1.7)
GPRS and UMTS: Architecture, Handover, Security	R1 pg 124- 128 (4.1.8.2) pg 142, 143

Introduction to Cellular Systems

Cellular systems for mobile communications

- Each transmitter, typically called a base station
  - Cell Shape, Cell Radius, clustering, Frequency Reuse, channel allocation(Fixed and Dynamic)
  - Interference, Cell splitting, Cell sectoring etc.

Advantages of cellular systems with small cells

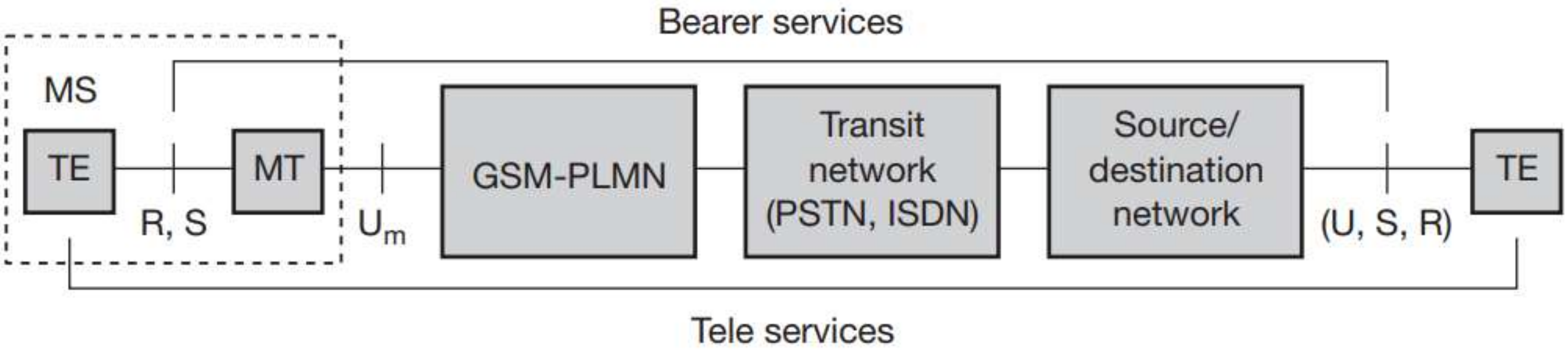
- **Higher capacity**: Due to use FDM-TDM which allows frequency reuse capacity increases
- **Less transmission power**
- **Local interference only-** Due to small cells, mobile stations and base stations only have to deal with ‘local’ interference.
- **Robustness**:Cellular systems are decentralized and so, more robust against the failure of single components. If one antenna fails, this only influences communication within a small area

Small cells also have some disadvantages:

- **Infrastructure needed**: Cellular systems need a complex infrastructure to connect all base stations. This includes many antennas, switches for call forwarding, location registers to find a mobile station etc, which makes the whole system quite expensive.
- **Handover needed**: Depending on the cell size and the speed of movement, handover happen quite often.
- **Frequency planning**: To avoid interference between transmitters using the same frequencies, frequencies have to be distributed carefully. Interference should be avoided, with limited number of frequencies hence frequency planning essential.

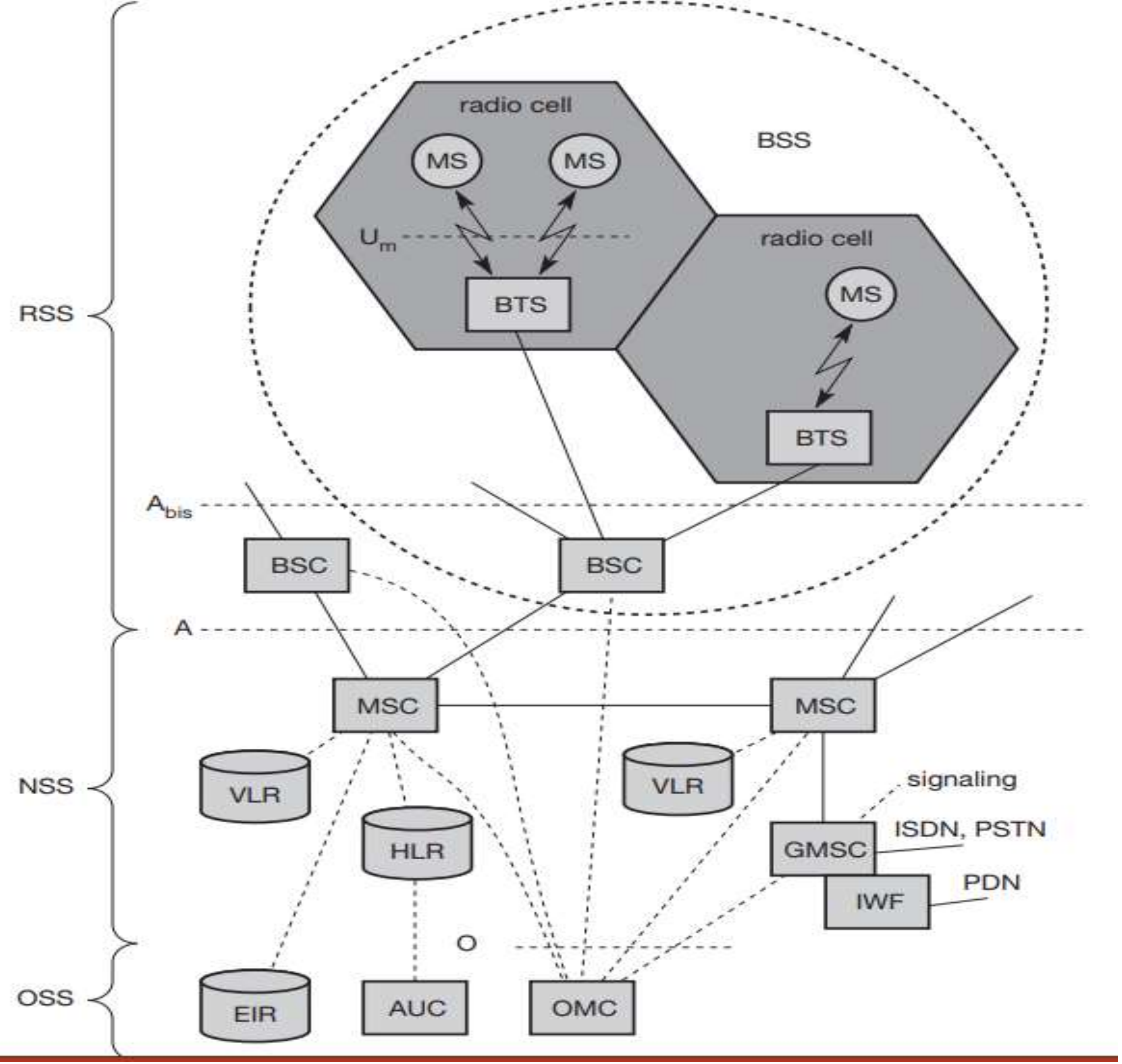
GSM (Global system for Mobile communication)

- GSM is the most successful digital mobile telecommunication system in the world today.
- GSM permits the integration of different voice and data services and the interworking with existing networks.
- Services make a network interesting for customers. GSM has defined three different categories of services: bearer, tele, and supplementary services



- **Bearer services** permit transparent and non-transparent, synchronous or asynchronous data transmission.
- Data transmission is full-duplex, synchronous with data rates of 1.2, 2.4, 4.8, and 9.6 kbit/s or full-duplex, asynchronous from 300 to 9,600 bit/s

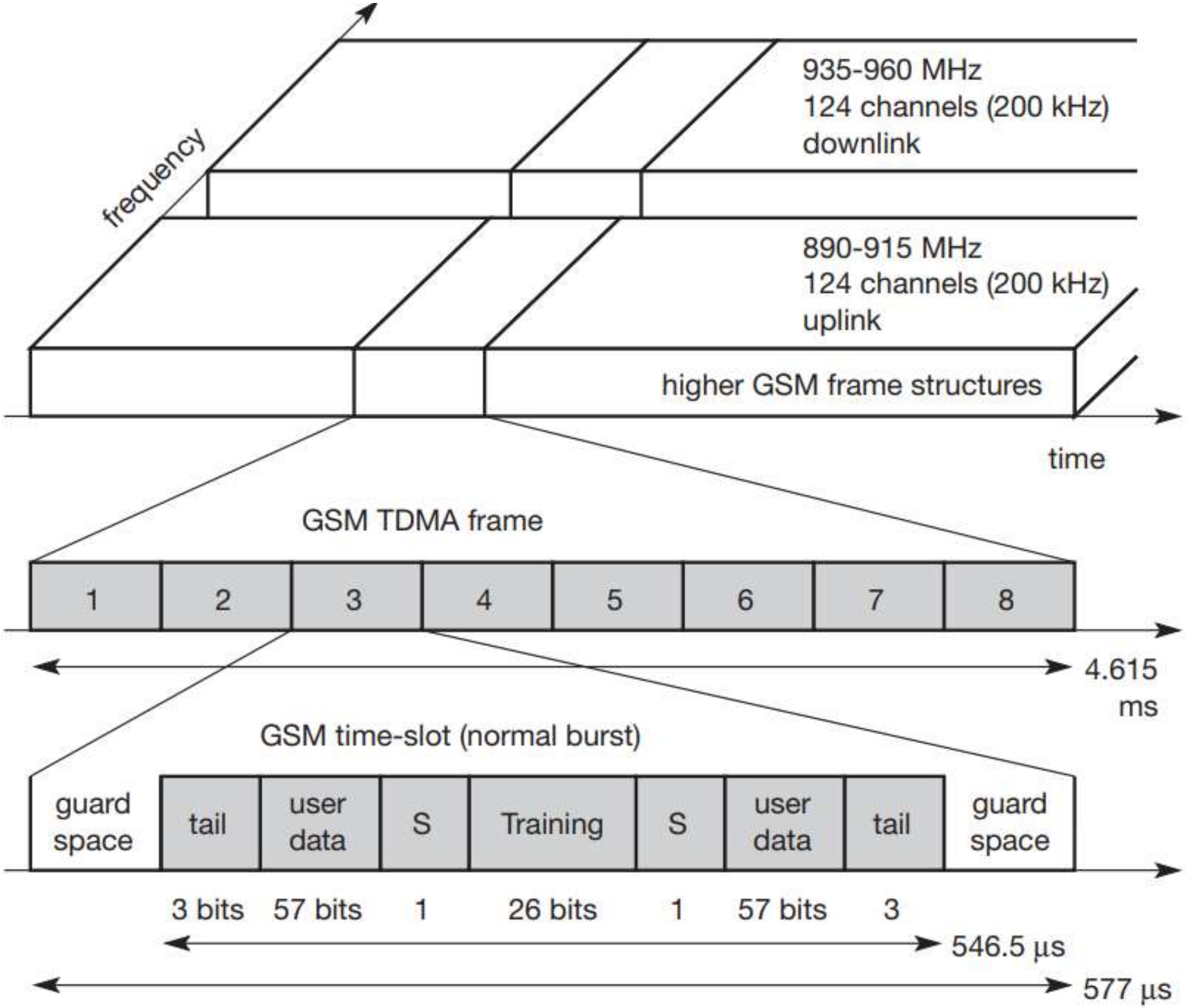
- **Tele services** GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN .
- Another service offered by GSM is the **emergency number**. This service is mandatory for all providers and free of charge.
- A useful service for very simple message transfer is **the short message service** (SMS), which offers transmission of messages of up to 160 characters. Sending and receiving of SMS is possible during data or voice transmission.
- GSM providers can offer **supplementary services.** Typical services are user identification, call redirection, or forwarding of ongoing calls.



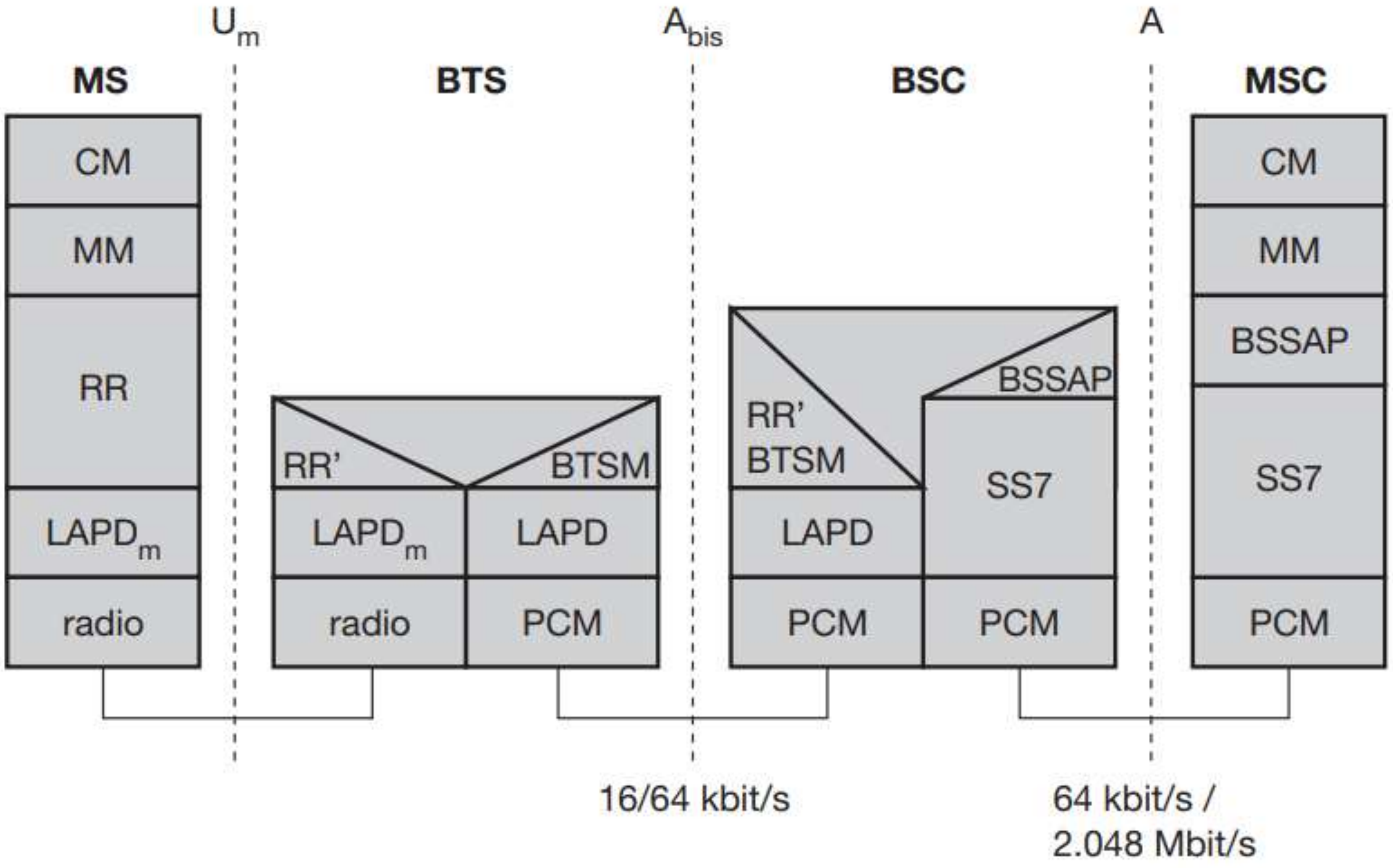
GSM Architecture

A GSM system consists of three subsystems, the radio sub system (RSS), the network and switching subsystem (NSS), and the operation subsystem (OSS).

GSM TDMA frame, slots, and bursts



GSM Protocols



- The physical layer at Um uses GMSK for digital modulation and performs encryption/decryption of data, i.e., encryption is not performed end-to-end, but only between MS and BSS over the air interface.
- Synchronization also includes the correction of the individual path delay between an MS and the BTS. All MSs within a cell use the same BTS and thus must be synchronized to this BTS.
- the BTS sends the current RTT(round trip times) to the MS, which then adjusts its access time so that all bursts reach the BTS within their limits.
- An MS close to the BTS has a very short RTT, whereas an MS 35 km away already exhibits an RTT of around 0.23 ms.
- The main tasks of the physical layer comprise channel coding and error detection/correction(different forward error correction (FEC))

- As voice was assumed to be the main service in GSM, the physical layer also contains special functions, such as **voice activity detection** (VAD), which transmits voice data only when there is a voice signal.
- Signaling between entities in a GSM network requires higher layers**, LAPDm,** as the name already implies, has been derived from **link access procedure** for the D-channel (LAPD) .
- LAPDm offers reliable data transfer over connections, re-sequencing of data frames, and flow control.
- The lowest sublayer is the **radio resource management (RR),** The main tasks of RR are setup, maintenance, and release of radio channels.
- **Mobility management** (MM) contains functions for registration, authentication, identification, location updating, and the provision of a temporary mobile subscriber identity (TMSI) that replaces the international mobile subscriber identity (IMSI) and which hides the real identity of an MS user over the air interface.

- The **call management (CM**) layer contains three entities: call control (CC), short message service (SMS), and supplementary service (SS).
- Additional protocols are used at the Abis and A interfaces
- Signaling system No. 7 (SS7) is used for signaling between an MSC and a BSC. This protocol also transfers all management information between MSCs, HLR, VLRs, AuC, EIR, and OMC. An MSC can also control a BSS via a BSS application part (BSSAP).

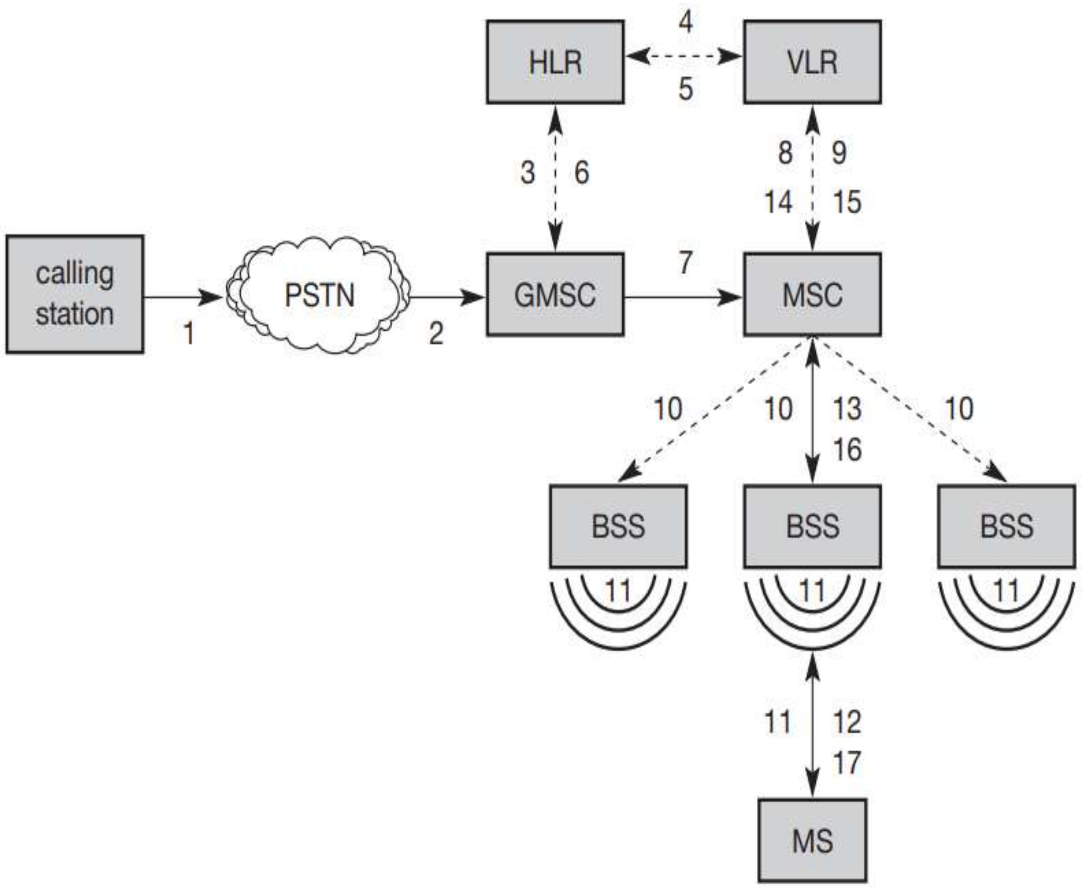
Mobility Management and Connection Established (Localization and Calling)

- One fundamental feature of the GSM system is the automatic, worldwide localization of users.
- The system always knows where a user currently is, and the same phone number is valid worldwide.
- To provide this service, GSM performs periodic location updates.
- The HLR always contains information about the current location, and the VLR currently responsible for the MS informs the HLR about location changes.
- As soon as an MS moves into the range of a new VLR (a new location area), the HLR sends all user data needed to the new VLR.
- Changing VLRs with uninterrupted availability of all services is also called roaming.

To locate an MS and to address the MS, several numbers are needed:

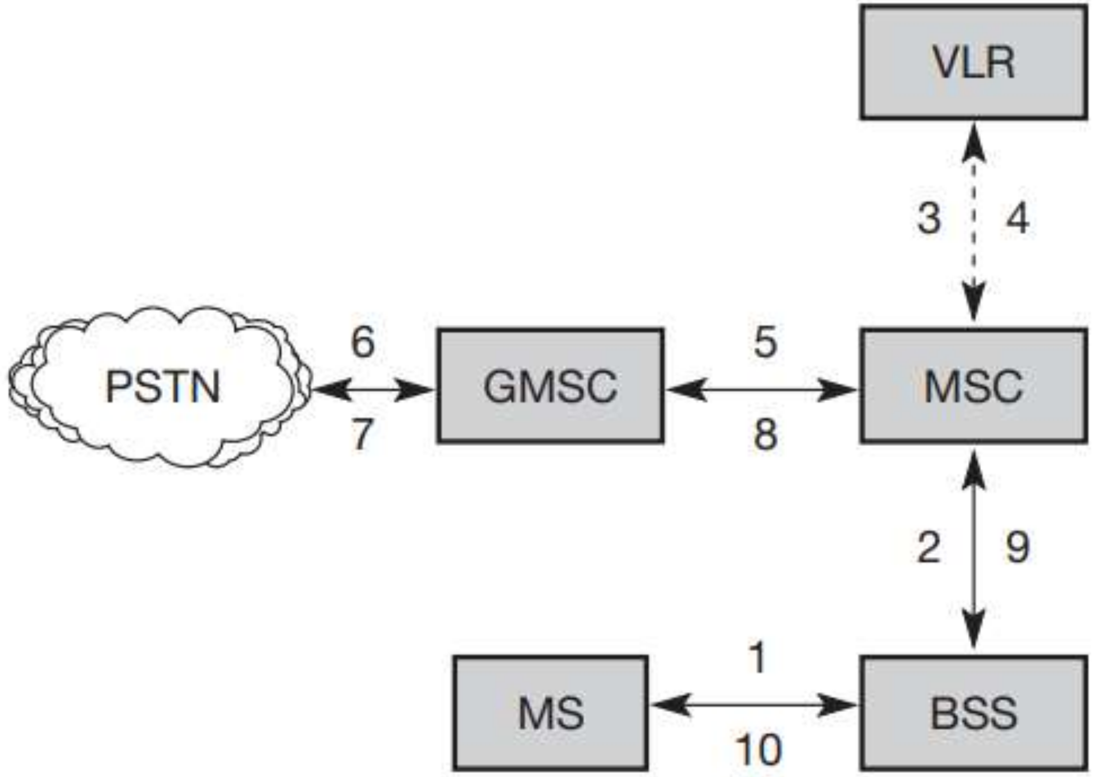
- **Mobile station international ISDN number (MSISDN):** This number consists of the country code, the national destination code (NDC), the address of the network provider, and the subscriber number (SN).
- **International mobile subscriber identity (IMSI):** IMSI consists of a mobile country code (MCC), the mobile network code (MNC) (i.e., the code of the network provider), and finally the mobile subscriber identification number (MSIN)
- **Temporary mobile subscriber identity (TMSI):** TMSI is selected by the current VLR and is only valid temporarily and within the location area of the VLR.
- **Mobile station roaming number (MSRN):** MSRN contains the current visitor country code (VCC), the visitor national destination code (VNDC), the identification of the current MSC together with the subscriber number. The MSRN helps the HLR to find a subscriber for an incoming call.
- **All these numbers are needed to find a subscriber and to maintain the connection with a mobile station**

Connection Established



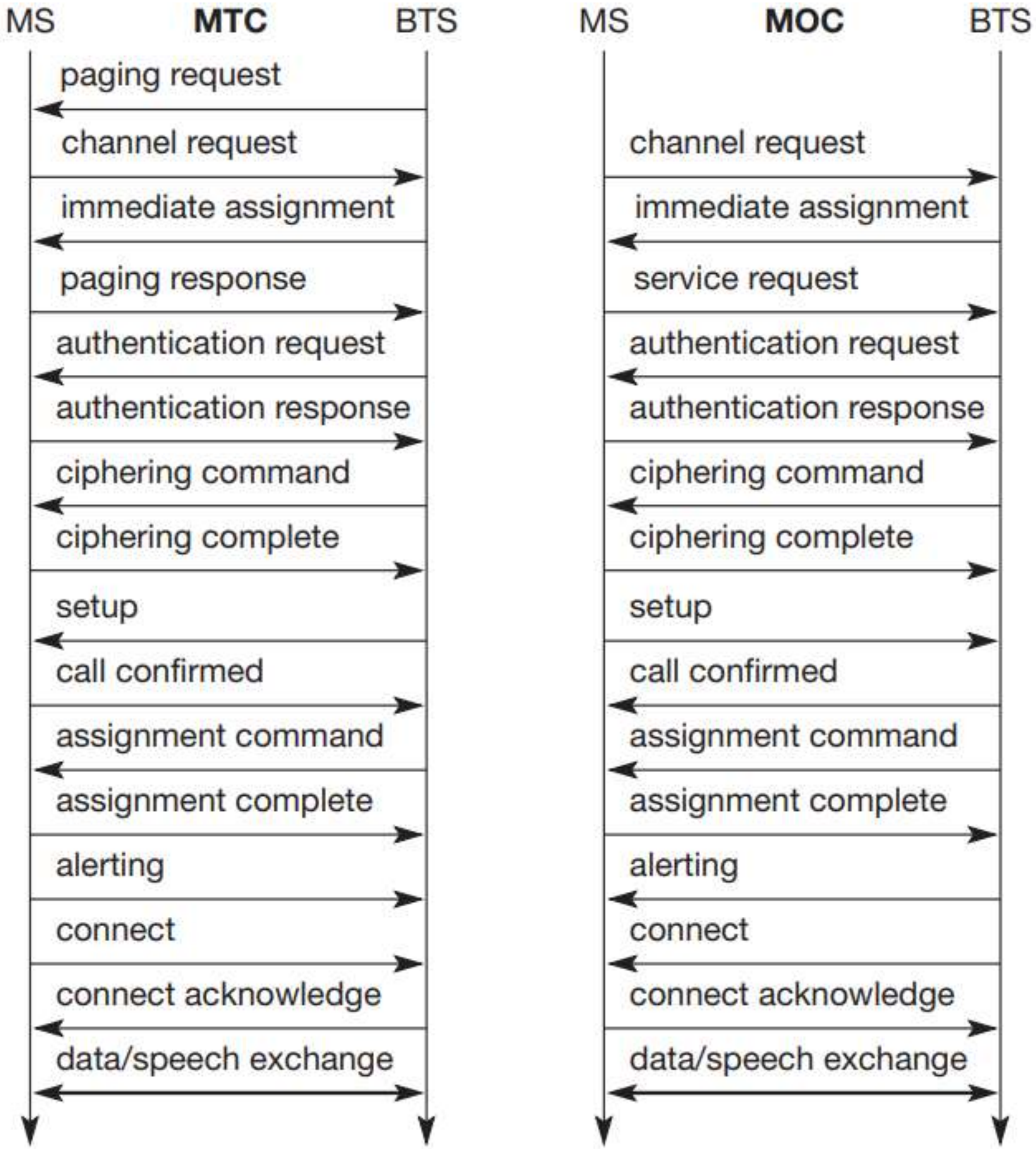
Mobile terminated call (MTC)

1. user dials the phone number of a GSM subscriber
2. GSM network forwards the call setup to the Gateway MSC
3. The GMSC identifies the HLR, and signals the call setup to the HLR
4. The HLR checks for existence of number, and requests an MSRN from the current VLR
5. After receiving the MSRN,
6. the HLR can determine the MSC responsible for the MS and forwards this information to the GMSC .
7. The GMSC can now forward the call setup request to the MSC indicated
8. MSC requests the current status of the MS from the VLR
9. If the MS is available, the MSC initiates paging in all cells
10. BTSs of all BSSs transmit this paging signal to the MS
11. . If the MS answers, the VLR has to perform security checks
12. The VLR then signals to the MSC to set up a connection to the MS



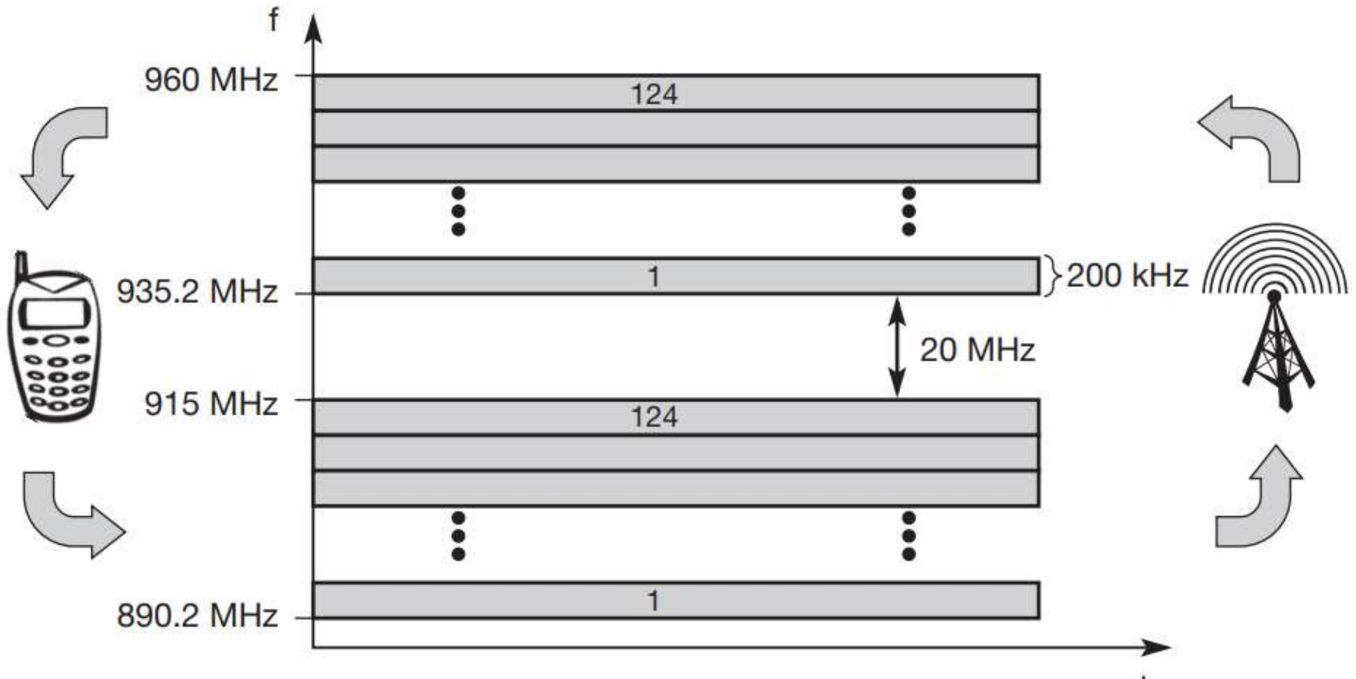
Mobile originated call (MOC)

The MS transmits a request for a new connection (1),
the BSS forwards this request to the MSC (2).
The MSC then checks if this user is allowed to set up a call with the requested service (3 and 4) and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network


MS
MTC
BTS
paging request
channel request
immediate assignment
paging response
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange
MS
MOC
BTS
channel request
immediate assignment
service request
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange

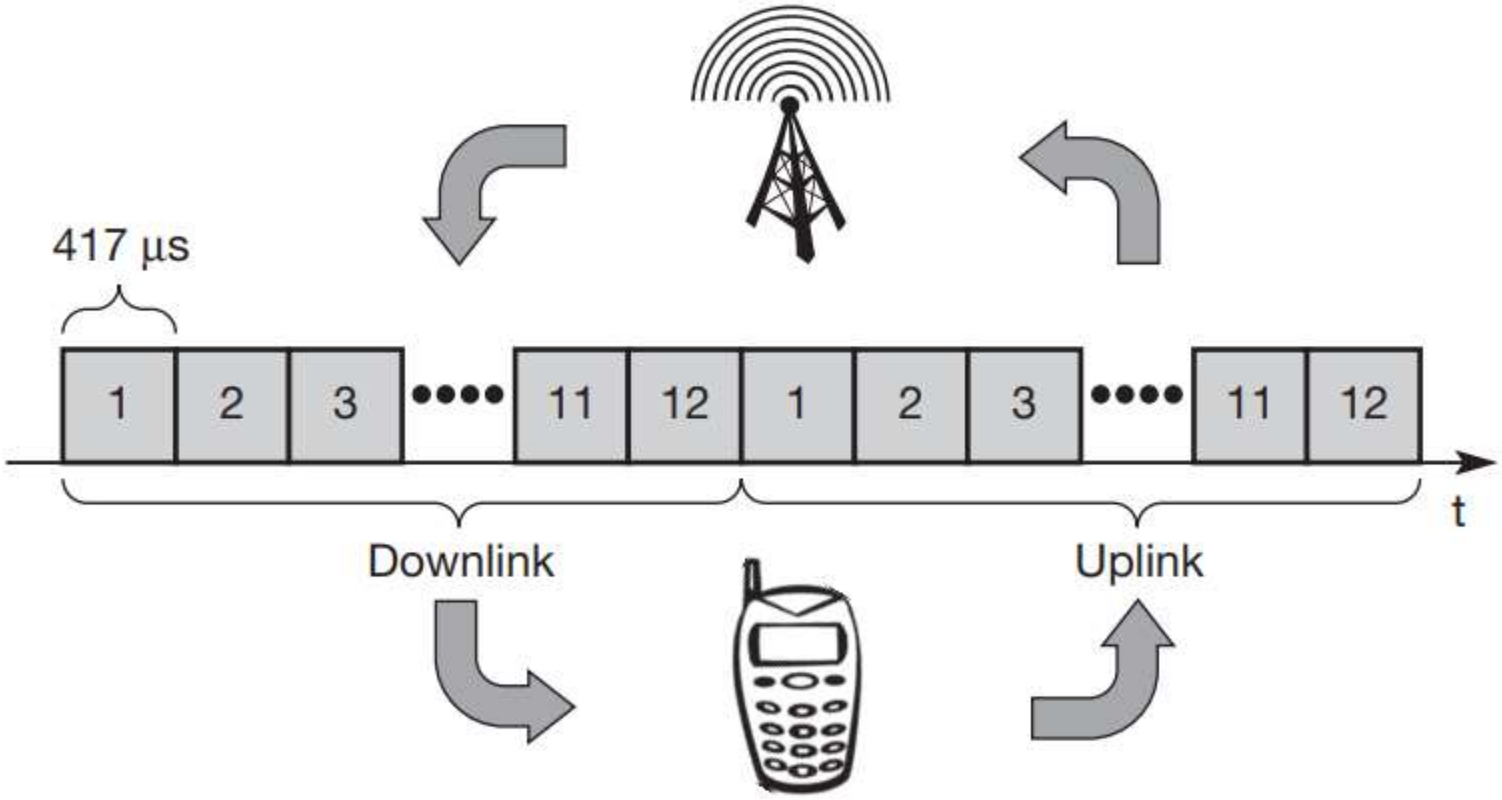
Frequency Allocation

- The ITU-R holds, the World Radio Conference (WRC), to periodically discuss and decide frequency allocations for all three regions.
- The Allocation can either be **fixed** (as for radio stations or the general planning and regulation of frequencies) or **dynamic** (i.e., demand driven). Duplexing is used for simultaneous transmission between MS and BS.
- The two frequencies are also known as **uplink,** i.e., from mobile station to base station or from ground control to satellite, and as **downlink**, i.e., from base station to mobile station or from satellite to ground control.
- Example FDM and FDD, in a mobile phone network based on the GSM standard for 900 MHz .



- The basic frequency allocation scheme for GSM is fixed and regulated by national authorities.
- All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz.
- Up- and downlink have a fixed relation. If the uplink frequency is fu = 890 MHz + n·0.2 MHz, the downlink frequency is fd = fu + 45 MHz, i.e., fd = 935 MHz + n·0.2 MHz for a certain channel n.
- Each channel (uplink and downlink) has a bandwidth of 200kHz.

- Compared to FDMA, time division multiple access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication



The base station uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink. Uplink and downlink are separated in time.

GSM frequency bands

GSM band	*f* (MHz)	Uplink (MHz) (mobile to base)	Downlink (MHz) (base to mobile)	Channel numbers	Equivalent LTE band	Regional deployments
T-GSM-380[a]	380	380.2 – 389.8	390.2 – 399.8	dynamic	None	None
T-GSM-410[a]	410	410.2 – 419.8	420.2 – 429.8	dynamic	87/88	None
GSM-450	450	450.6 – 457.6	460.6 – 467.6	259–293	31/72/73	None
GSM-480	480	479.0 – 486.0	489.0 – 496.0	306–340	None	None
GSM-710	710	698.2 – 716.2	728.2 – 746.2	dynamic	12	None
GSM-750	750	777.2 – 792.2	747.2 – 762.2	438–511	None	None
T-GSM-810[a]	810	806.2 – 821.2	851.2 – 866.2	dynamic	27	None
GSM-850	850	824.2 – 848.8	869.2 – 893.8	128–251	5	CALA,[b] NAR[c]
P-GSM-900[d]	*900*	*890.0 – 915.0*	*935.0 – 960.0*	*1–124*	*8 (subset)*	None *deprecated*
E-GSM-900[e]	900	880.0 – 915.0	925.0 – 960.0	0–124, 975–1023	8	APAC,[f] EMEA[g]
R-GSM-900[h]	900	876.0 – 915.0	921.0 – 960.0	0–124, 955–1023	?	APAC,[f] EMEA[g] *used for GSM-R*
T-GSM-900[a]	900	870.4 – 876.0	915.4 – 921.0	dynamic	None	None
DCS-1800[i]	1800	1710.2 – 1784.8	1805.2 – 1879.8	512–885	3	APAC,[f] EMEA[g]
PCS-1900[j]	1900	1850.2 – 1909.8	1930.2 – 1989.8	512–810	2	CALA,[b] NAR[c]

a. ^ [a] [b] [c] [d] T-GSM is Trunking-GSM.

b. ^ [a] [b] CALA: Canada, US, Caribbean, and Latin America

c. ^ [a] [b] NAR: North American Region

d. ^ P-GSM is the standard or primary GSM-900 band

e. ^ E-GSM is the extended GSM-900 band: a superset of the standard GSM-900 band.

f. ^ [a] [b] [c] APAC: Asia-Pacific

g. ^ [a] [b] [c] EMEA: Europe, the Middle East and Africa

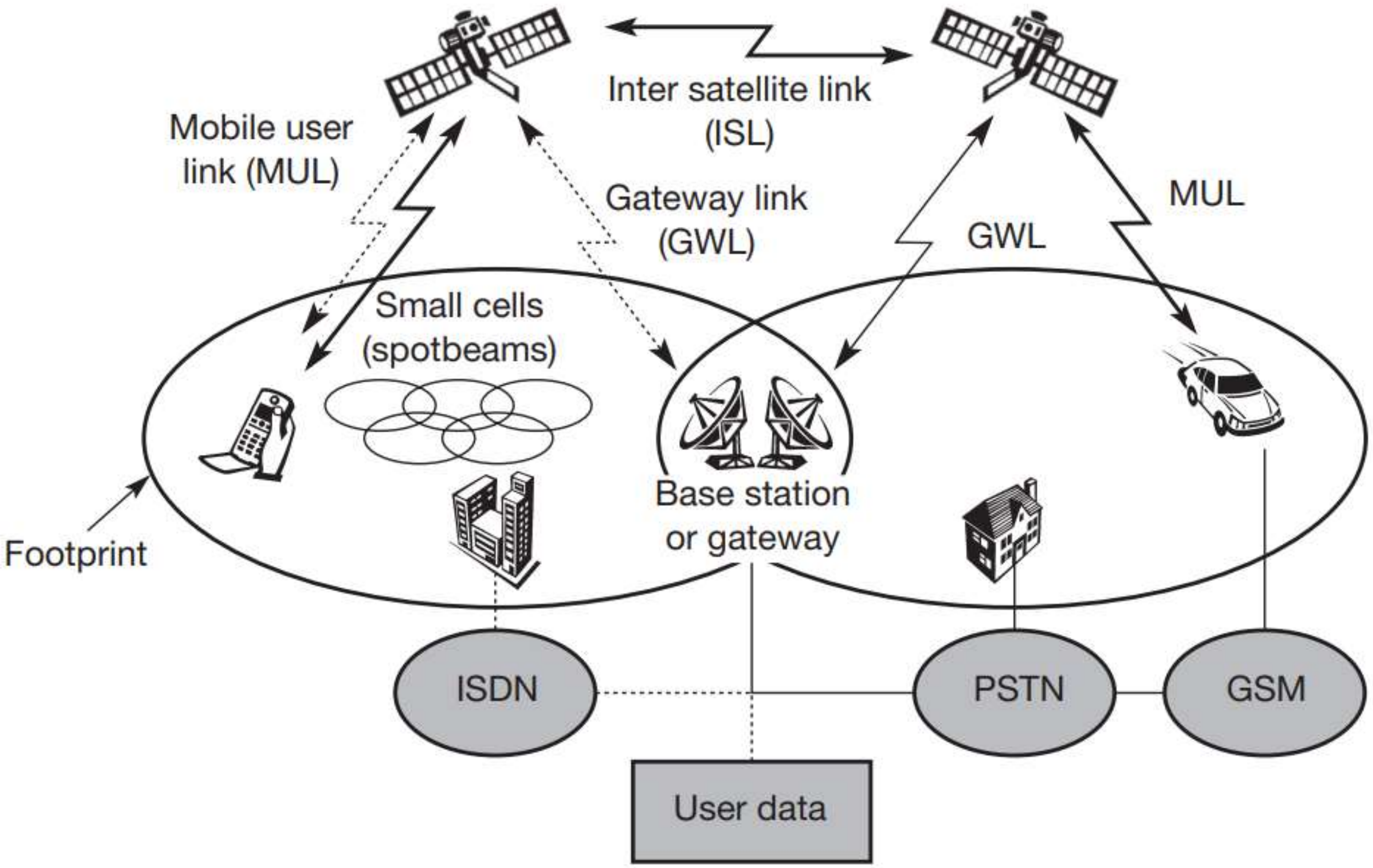
h. ^ R-GSM, or GSM-R, is the Railways GSM-900 band, which also includes the standard and extended GSM-900 bands.

i. ^ DCS: Digital Cellular System

j. ^ PCS: Personal Communications Service

Routing

A satellite system together with gateways and fixed terrestrial networks shown in Figure has to route data transmissions from one user to another as any other network does.



- Routing in the fixed segment (on earth) is achieved as usuak
- While two different solutions exist for the satellite network in space.
    - If satellites offer ISLs(inter satellite link), traffic can be routed between the satellites.
    - If not, all traffic is relayed to earth, routed there, and relayed back to a satellite.
    - ➢ So, Latency matters in the 2nd case, as routing takes requires 2 uplink and 2 downlinks.
    - ➢ Depending on the orbit and the speed of routing in the satellite network compared to the terrestrial network, the solution with ISLs offer lower latency.
    - ➢ The drawbacks of ISLs are higher system complexity due to additional antennas and routing hardware and software for the satellites.

Security

- GSM offers several security services using confidential information stored in the AuC and in the individual SIM.
- The SIM stores personal, secret data and is protected with a PIN against unauthorized use.

The security services offered by GSM are explained below:

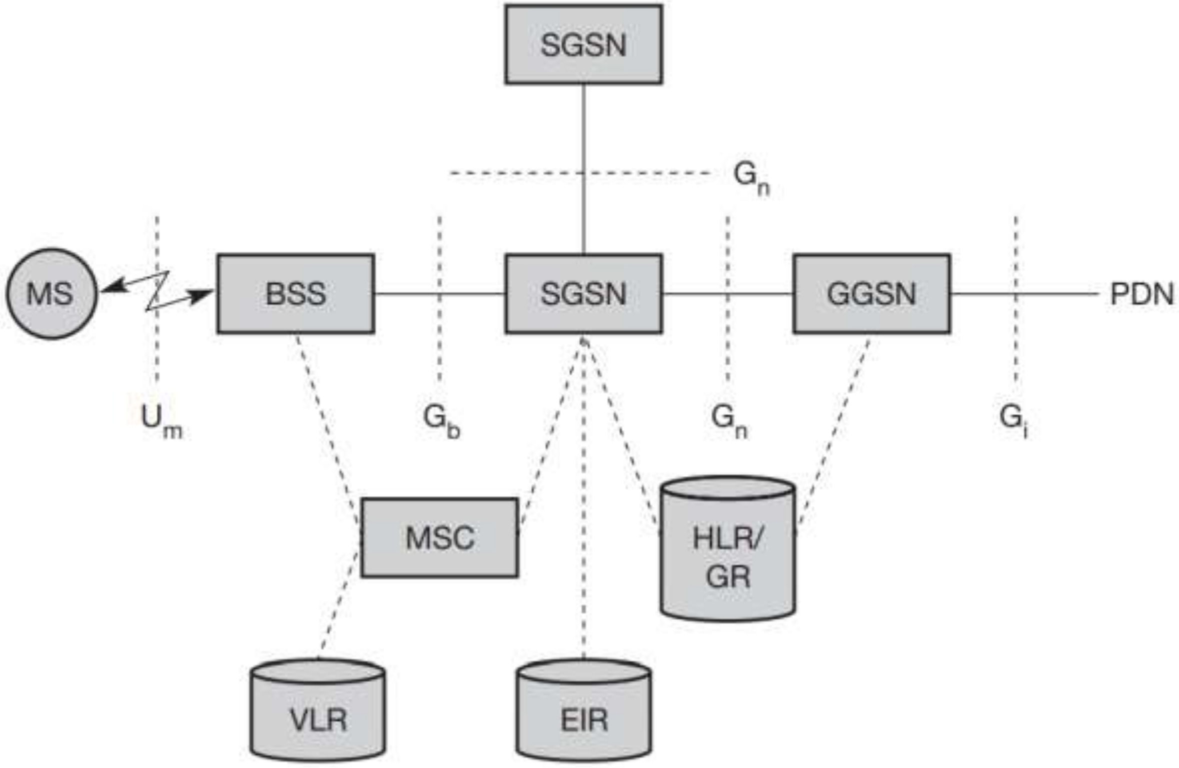
- **Access control and authentication**: The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber authentication
- **Confidentiality:** All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signaling.
- **Anonymity (Being Anonymous):** To provide user anonymity, all data is encrypted before transmission, and user identifiers are not used over the air.
- Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

Three algorithms have been specified to provide security services in GSM.

- Algorithm A3 is used for authentication,
- A5 for encryption, and
- A8 for the generation of a cipher key.

GPRS -general packet radio service

- GPRS is used for video calling, Email accessing, multimedia messaging etc
- The next step toward more flexible and powerful data transmission avoids the problems of HSCSD by being fully packet-oriented.
- The general packet radio service (GPRS) provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission of small volumes



The GPRS architecture introduces two new network elements, which are called GPRS support nodes (GSN) and are in fact routers. All GSNs are integrated into the standard GSM architecture.

- The gateway GPRS support node (GGSN) is the interworking unit between the GPRS network and external packet data networks (PDN).
- This node contains routing information for GPRS users, performs address conversion
- The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via an IP-based GPRS backbone network (Gn interface).
- serving GPRS support node (SGSN) which supports the MS via the Gb interface.

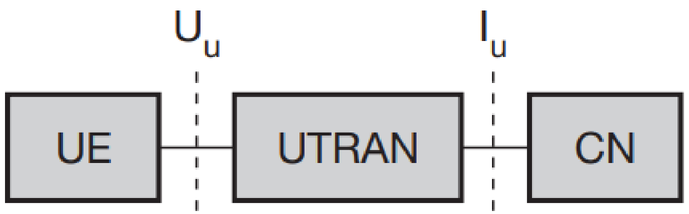
Packet data is transmitted from a PDN, via the GGSN and SGSN directly to the BSS and finally to the MS. The MSC, which is responsible for data transport in the traditional circuit-switched GSM, is only used for signaling in the GPRS scenario.

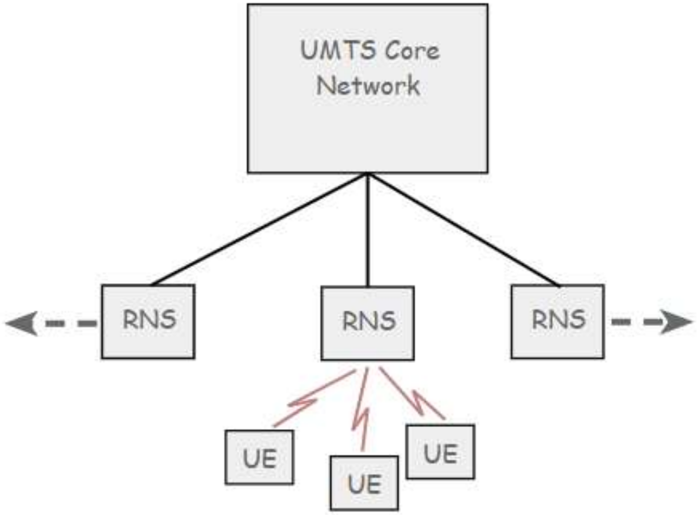
Universal Mobile Telecommunications System (UMTS)- is a broadband, packet-based, 3G mobile cellular system based upon GSM standards.

Features

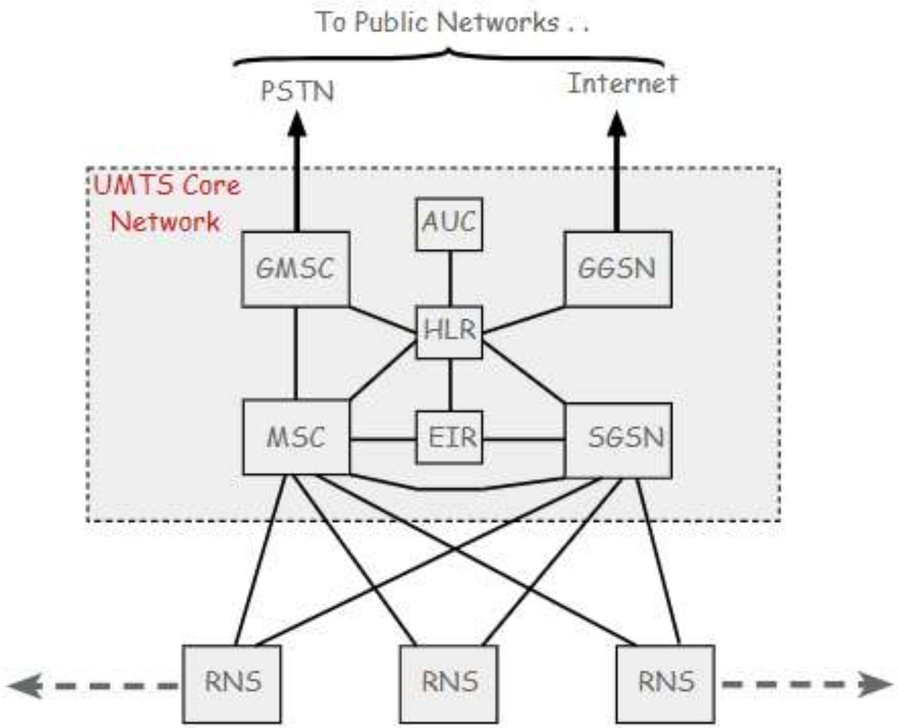
- •UMTS is a component of IMT-2000 standard of the International Telecommunications Union (ITU), developed by 3GPP.
- •It uses wideband code division multiple access (W-CDMA) air interface.
- •It provides transmission of text, digitized voice, video and multimedia.
- •It provides high bandwidth to mobile operators.
- •It gives a high data rate of 2Mbps. For High-Speed Downlink Packet Access (HSDPA) handsets, the data-rate is as high as 7.2 Mbps in the downlink connection.
- •It is also known as Freedom of Mobile Multimedia Access (FOMA).

UMTS system architecture





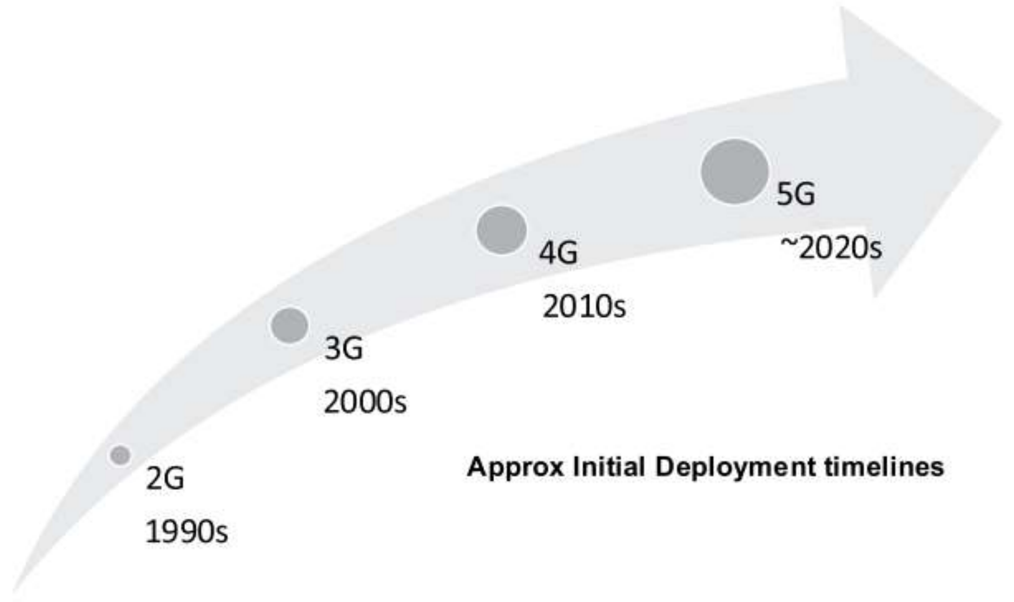
The main UMTS network blocks



UMTS Network Architecture Overview

Introduction, 5G network architecture, Applications, 5G enable technologies, Recent trends in Telecommunication Industries.

- The **1G analog system** are no longer operational, which only provided voice services and had no support for data.
- The **2G digital systems** are currently operational and support voice and limited data services.
- **The 3G system**s support voice, low speed data, and enable a number of data services.
- **The 4G systems** enable mobile broadband in the true sense, targeting 100 Mbps or higher on the move.



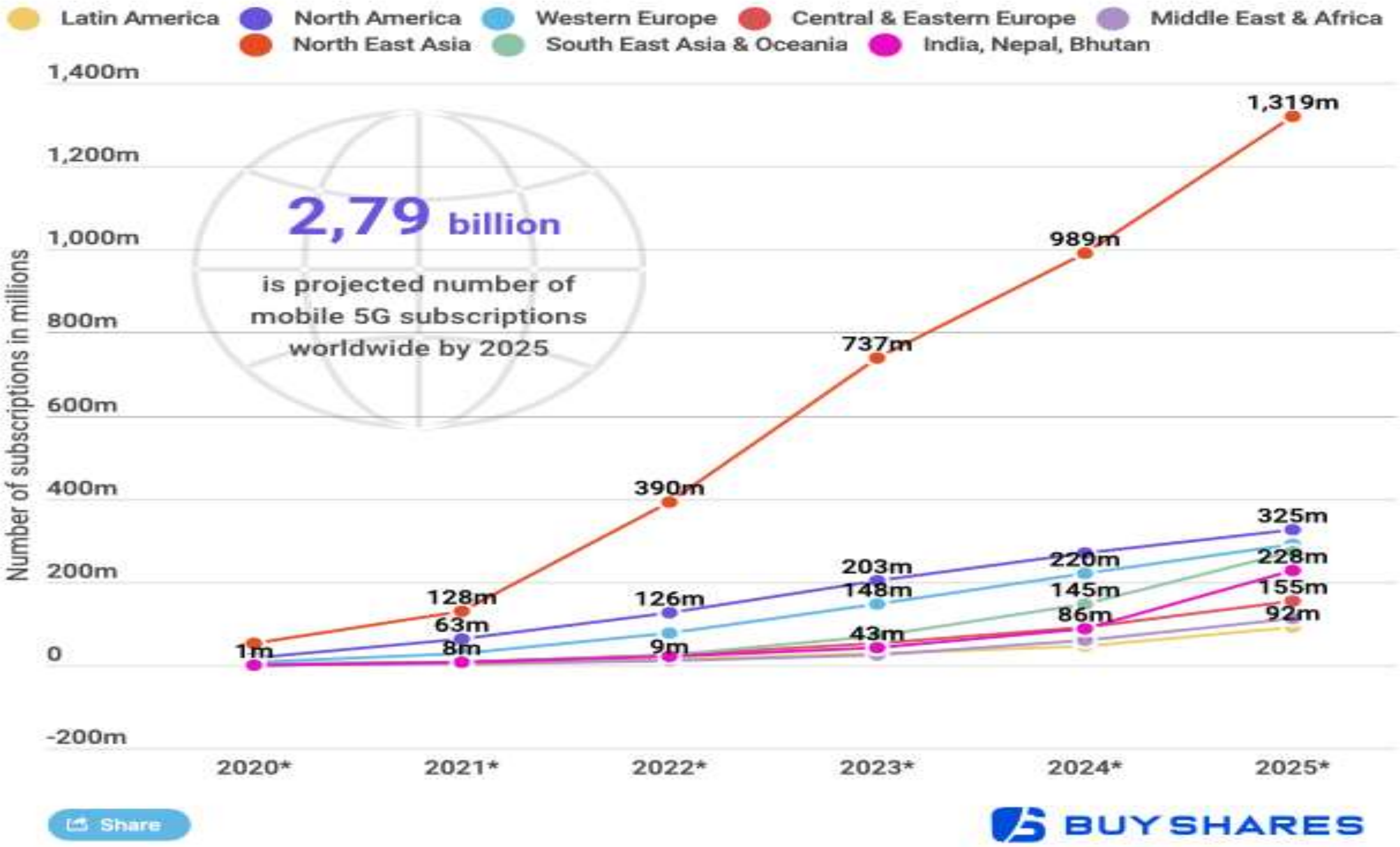
Mobile telecom evolution.

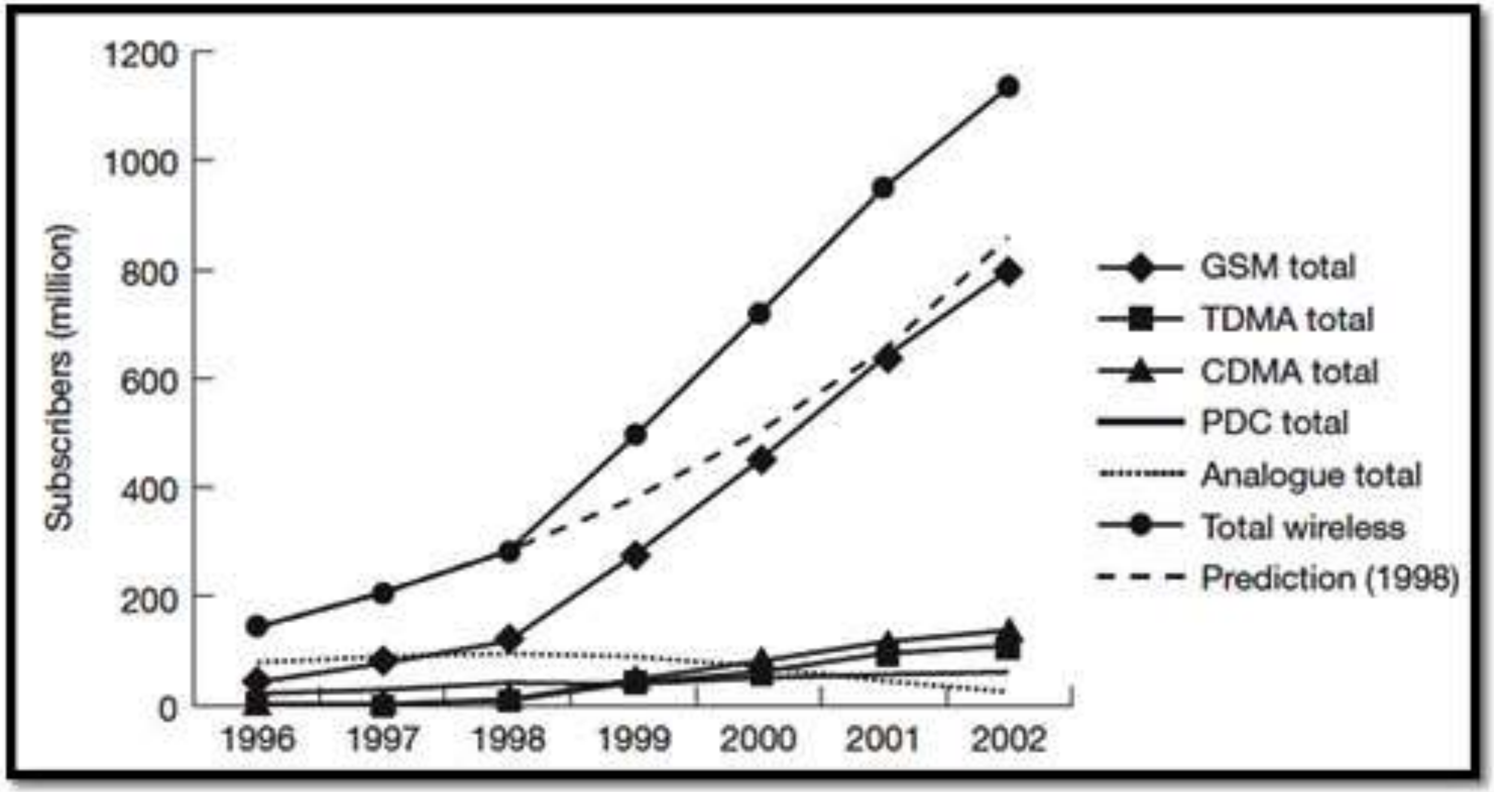
Channel access methods (physical layer).

Forecast number of mobile 5G subscriptions worldwide

by region from 2019 to 2025 (in millions); worldwide

Source: Ericsson.com





The main focus is always on data service, so the evolution of GSM offering higher data rates and packet-oriented data transfer.

Development of different generations of mobile telecommunication systems

Table 1: COMPARISON OF ALL GENERATIONS OF MOBILE TECHNOLOGIES

Technology ⇨ **Feature** ⇩	**1G**	**2G**	**3G**	**4G**	**5G**
Start/ Deployment	1970 – 1980	1990 – 2004	2004-2010	Now	Soon (probably 2020)
Data Bandwidth	2kbps	64kbps	2Mbps	1 Gbps	Higher than 1Gbps
Technology	Analog Cellular Technology	Digital Cellular Technology	CDMA 2000 (1xRTT, EVDO) UMTS, EDGE	Wi-Max LTE Wi-Fi	WWWW(coming soon)
Service	Mobile Telephony (Voice)	Digital voice, SMS, Higher capacity packetized data	Integrated high quality audio, video and data	Dynamic Information access, Wearable devices	Dynamic Information access, Wearable devices with AI Capabilities
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, Packet	Packet	All Packet	All Packet
Core Network	PSTN	PSTN	Packet N/W	Internet	Internet

- Fourth Generation (4G): The main difference between 3G and 4G is the data rate. The key technologies that have made 4G possible are **MIMO (Multiple Input Multiple Output) and OFDM (Orthogonal Frequency Division Multiplexing).**
- The most important 4G standards are WiMAX and LTE. While 4G LTE is a major improvement over 3G speeds.
- 4G LTE are: Supports interactive multimedia, voice, video. High speed, high capacity and low cost per bit (Speeds of up to 20 Mbps or more.) Global and scalable mobile networks. Ad hoc and multi-hop networks.
- **5G systems** are expected to provide an enhanced mobile broadband targeting peak data rate of 20 Gbps, extend 4G's Internet of Things capability, and enable mission-critical applications that require ultra-high reliability and low latency.

Fundamental Concepts in 5G

- **Air-Interface**
- The air-interface defines the method for transmitting/receiving information over the air between mobiles and base stations.
- The air interfaces of 2G, 3G, and 4G were all designed while keeping certain Key Performance Indicators like mean opinion score for voice,dropped/blocked call rates, data throughput, etc.
- However, the emerging trends of IoTs, M2M (Machine to Machine), V2X (Vehicle-to-everything), and so on are all demanding to go beyond such a specific approach.
- **Channel Capacity**: Communicating messages from one location to another requires some form of pathway or medium. Cellular communications use radio waves to carry information over the air from the user to the base station and vice versa. $C = B\log_2\left(1+\frac{S}{N}\right)$

- **Channel Access Methods**: A channel access method is based on multiplexing allowing sharing of a communication channel between users/devices.
- OFDMA, which is used in 4G standards, is a form of FDMA.
- OFDM achieves high spectral efficiency by using orthogonal subcarriers.
- Orthogonality allows subcarriers' spectra to overlap, which in turn, enables transmission of more data than FDMA over the same fixed bandwidth

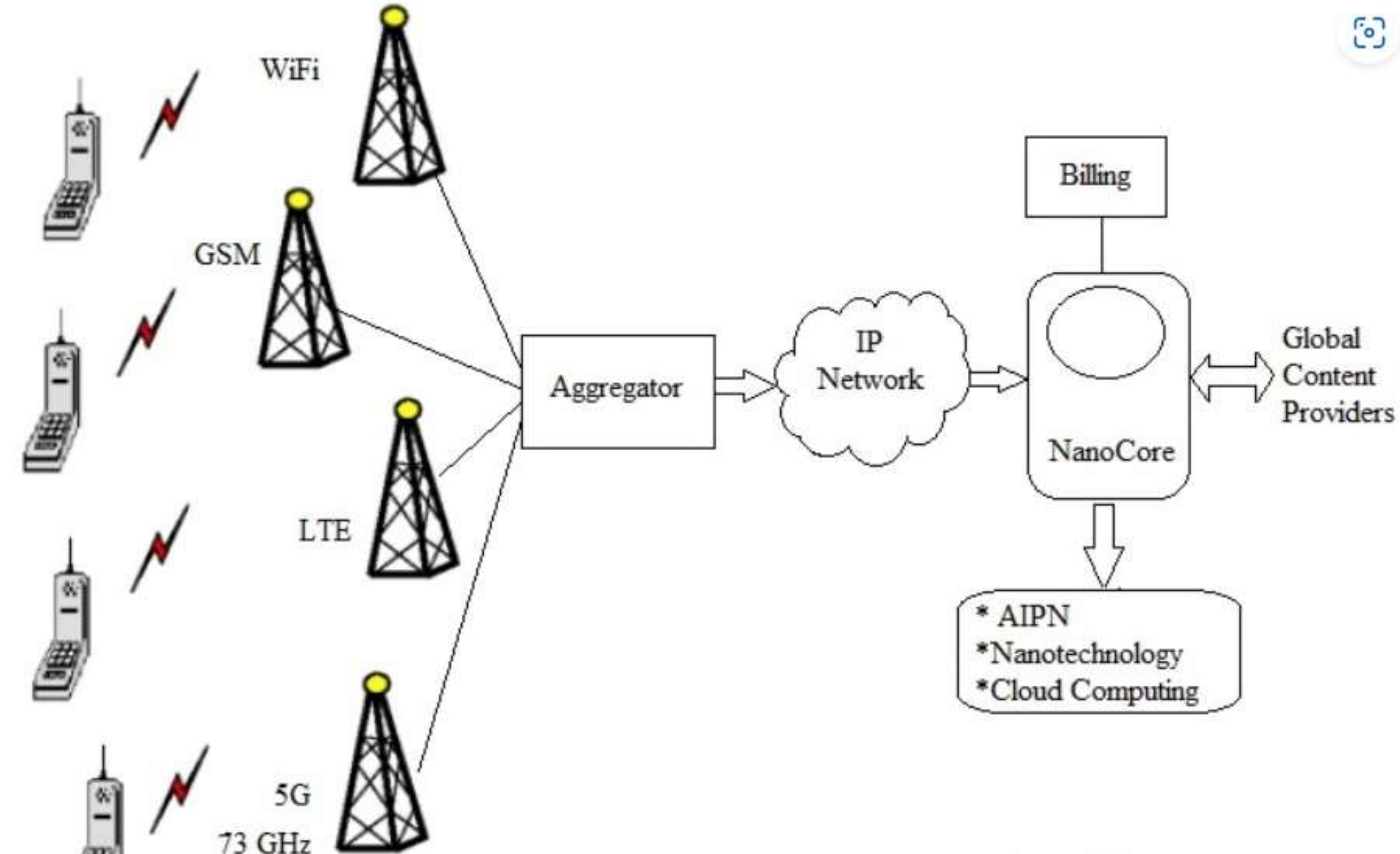
OFDM does have drawbacks such as

- The spectrum is not localized and requires a guard band.
- The subcarrier spacing and symbol duration are fixed and transmission is synchronous giving a large overhead for time alignment.

- **Spectral Efficiency:T**he spectral efficiency refers to the information rate that can be transmitted over a given bandwidth which depends on the multiple access method.

- The other factors may include the type of modulation used, error correction methods, frequency reuse factor, the number of users served, radio capability, and the percentage of time a service is active.
- OFDM offers a Better spectral efficiency in 5G.
- To improve spectral efficiency, a nonorthogonal scheme, namely NOMA (Non-Orthogonal Multiple Access), has been considered for 5G.

5G network architecture



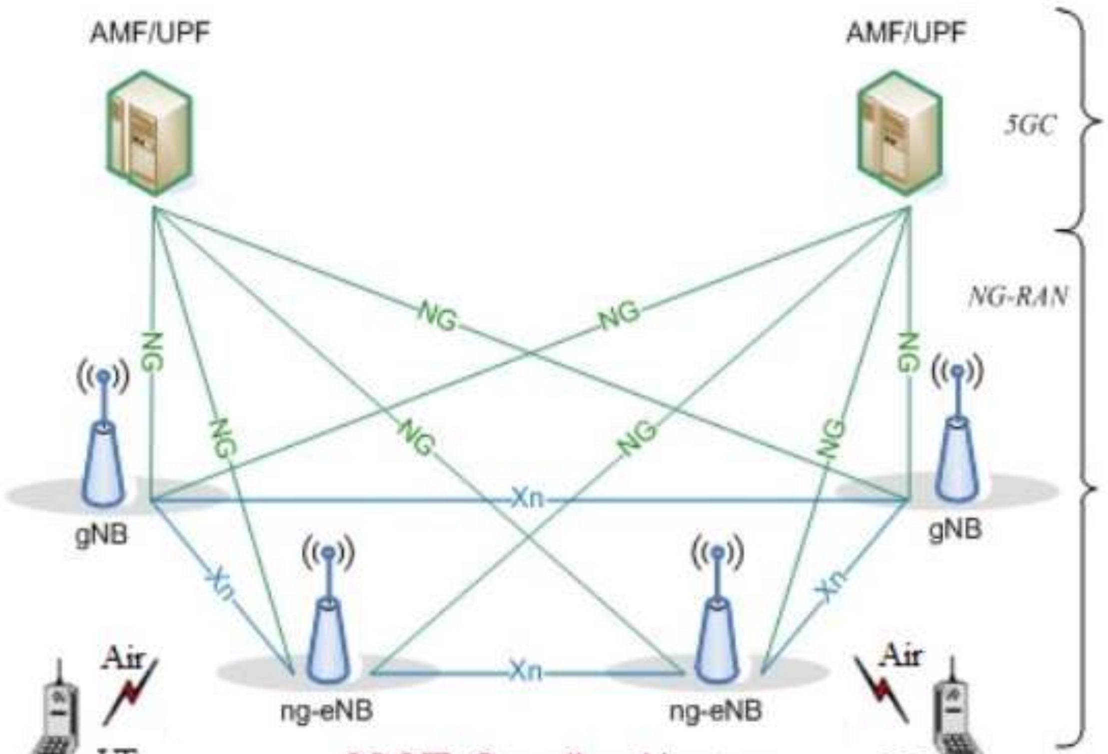
5G Network Architecture

The 5G architecture consists of all RANs(Radio Access Networks) , aggregator, IP network, nanocore etc. network elements. 5G NR (New Radio) architecture as per 3GPP(3rd Generation Partnership Project) document published in dec. 2017

- 5G network uses flat IP concept so that different RANs (Radio Access Networks) can use the same single Nanocore for communication.

- The concept of nanocore is the mutual combination of three technologies
  - Nanotechnology
  - Cloud Computing
  - All IP Platform
- RANs supported by 5G architecture are GSM, GPRS/EDGE, UMTS, LTE, LTE-advanced, WiMAX, WiFi, CDMA2000, EV-DO, CDMA One, IS-95 etc.
- This architecture reduces number of network elements in data path and hence reduces cost to greater extent. It also minimizes latency.
- 5G aggregator aggregates all the RAN traffics and route it to gateway.
- 5G aggregator is located at BSC/RNC(Base Station Controller/Radio Network Controller) place.

5G architecture as per 5G NR(New Radio) standard

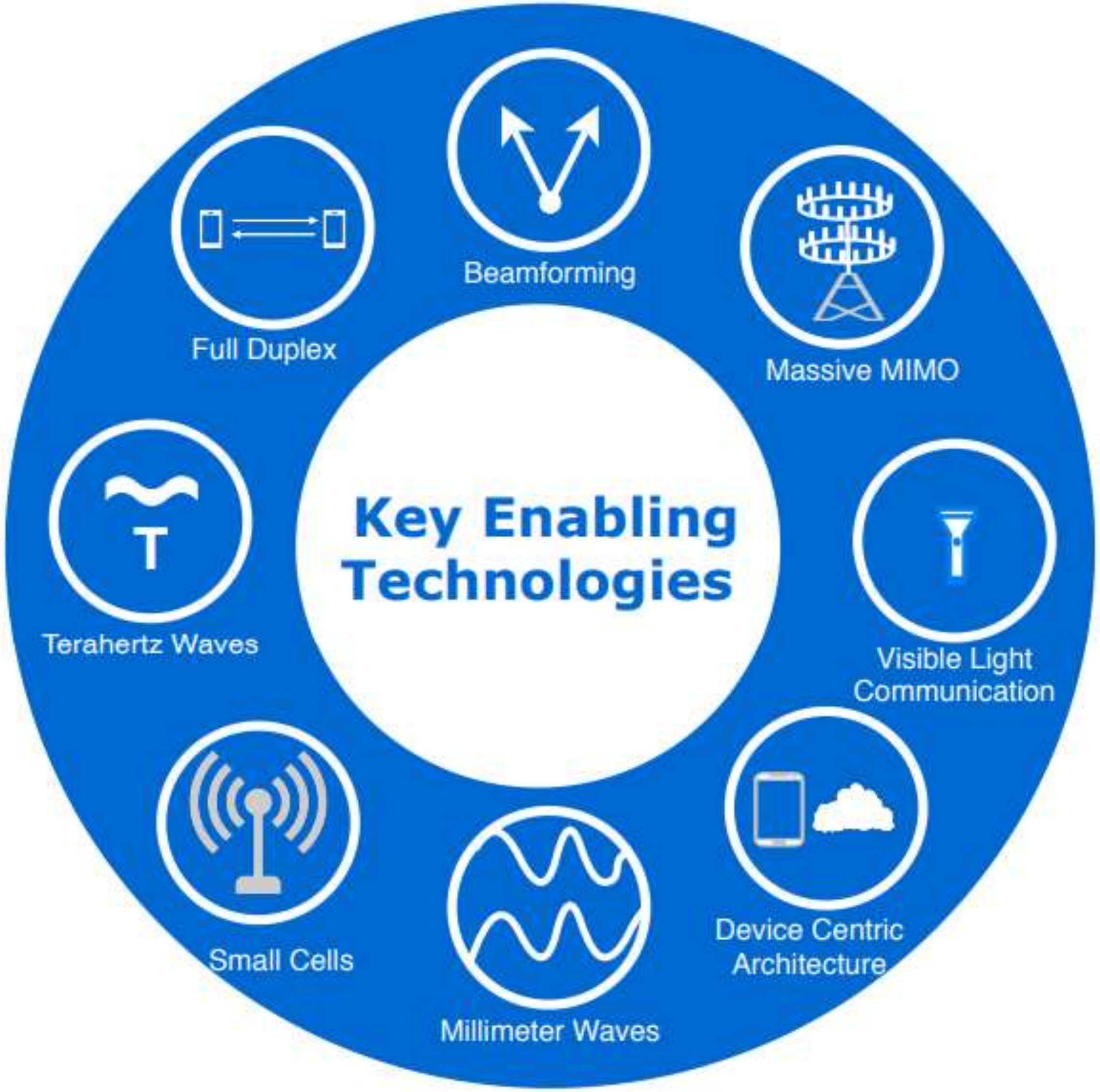


5G NR Overall architecture

- The gNB (Next Generation Node B.)(or ng-eNB) is responsible for all radio-related functions in one or several cells, for example radio resource management, admission control, connection establishment, routing
- AMF stands for Access and Mobility Management Function and UPF stands for User Plane Function.
- The main functions and responsibilities of AMF are: Registration Management. Reachability Management. Connection Management

- 5G smartphones interact with 5G-RAN over Uu radio interface.
- 5G RAN interacts with 5GC (5G Core Network).
- Customers that are connected to a type of 5G network, which is only shown on iPhones or Android phones with 5G support, are referred to as 5G UC (ultra capacity)
- If you are a T-Mobile customer, a new “5G UC” icon will appear in your iPhone status bar if this new network appears

Key Enabling Technologies for 5G



Millimeter waves are frequency between 30 GHz to 300 GHz, and it is called millimeter waves because its length varies from 1 to 10 mm compared to the radio waves that are used in the current mobile communication system, which measure tens of centimeters in length.
Millimeter waves can provide bandwidth ten times more than that of the entire 4G cellular band. These high-frequency waves are used in some satellite application.

Small Cells or Heterogeneous Networks Small cells are low power tiny base stations that can be placed within every 100 m distance to cover small geographical areas. These low power base stations prevent the signal from dropping in crowded areas.

Beamforming Beamforming is the ability of the base station to adapt the radiation pattern of the antenna . Beamforming helps the base station to find a suitable route to deliver data to the user, and it also reduces interference with nearby users along the route

Top 10 Telecom Industry Trends

1. Internet of Things
2. Connectivity Solutions
3. 5G & Network Infrastructure
4. Artificial Intelligence
5. High Resolution Content
6. Cybersecurity
7. Cloud Computing
8. Communication Models
9. Software Defined Networks
10. Edge Computing