Mobile communication overview 1/2

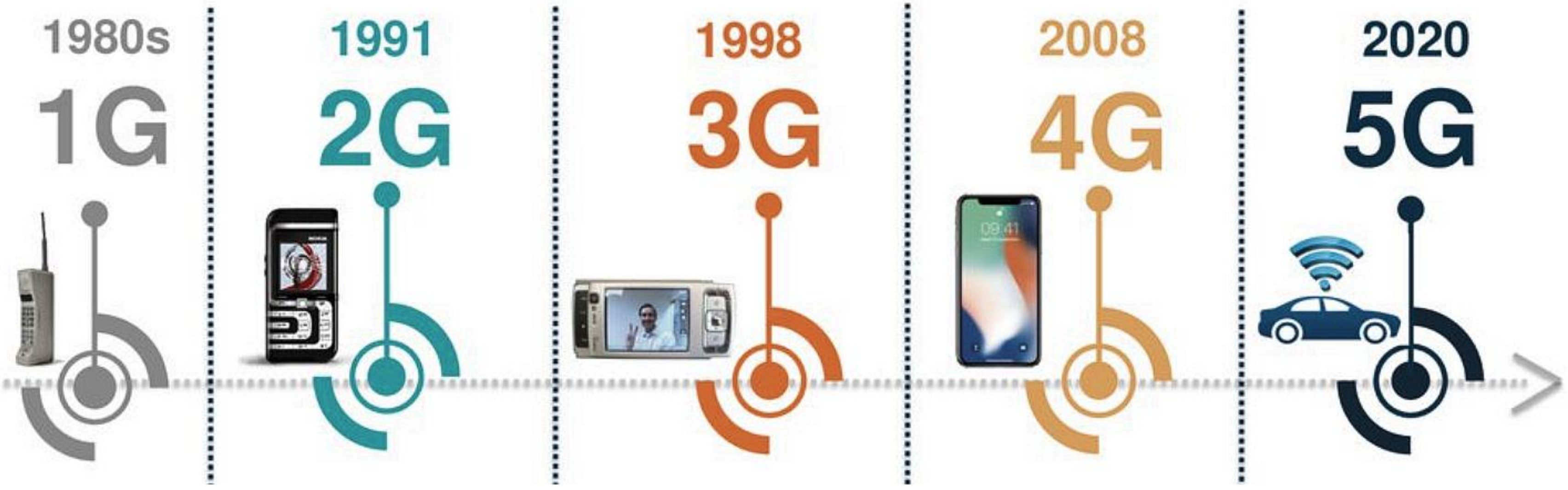
KIS FRI UNIZA

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

Mobile communication evolution to 5G (5^{th} generation)

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

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

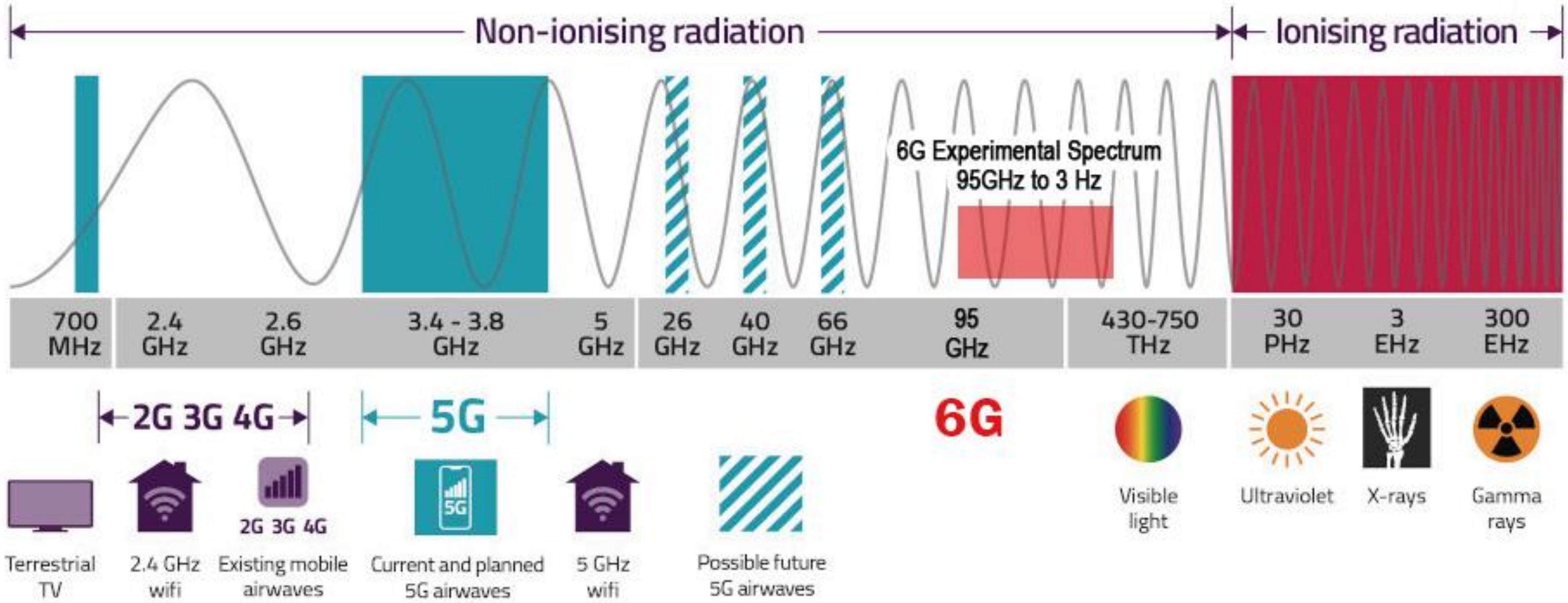


Analog system 2kbps for data | Up to 270 kbps for data | Up to 3Mbps for data | Up to 1Gbps for data | Up to 10Gbps for data

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

Electromagnetic spectrum overview

- Unlicensed spectrum 2.4Ghz and 5Ghz for Wi-Fi technology
- 450 MHz used by former NMT (1G) mobile communication
- 800 MHz to 2600 MHz spectrum for current 2G, 3G and 4G (LTE) mobile communication
- Sub-6 GHz frequency bands for 5G are 700 MHz, 3400-3800 MHz
- Planned future use of higher 5G bands: 24.25 GHz - 52.6 GHz (24.25 - 27.5 GHz in EU)
- Future 6G communication planned at 95 GHz

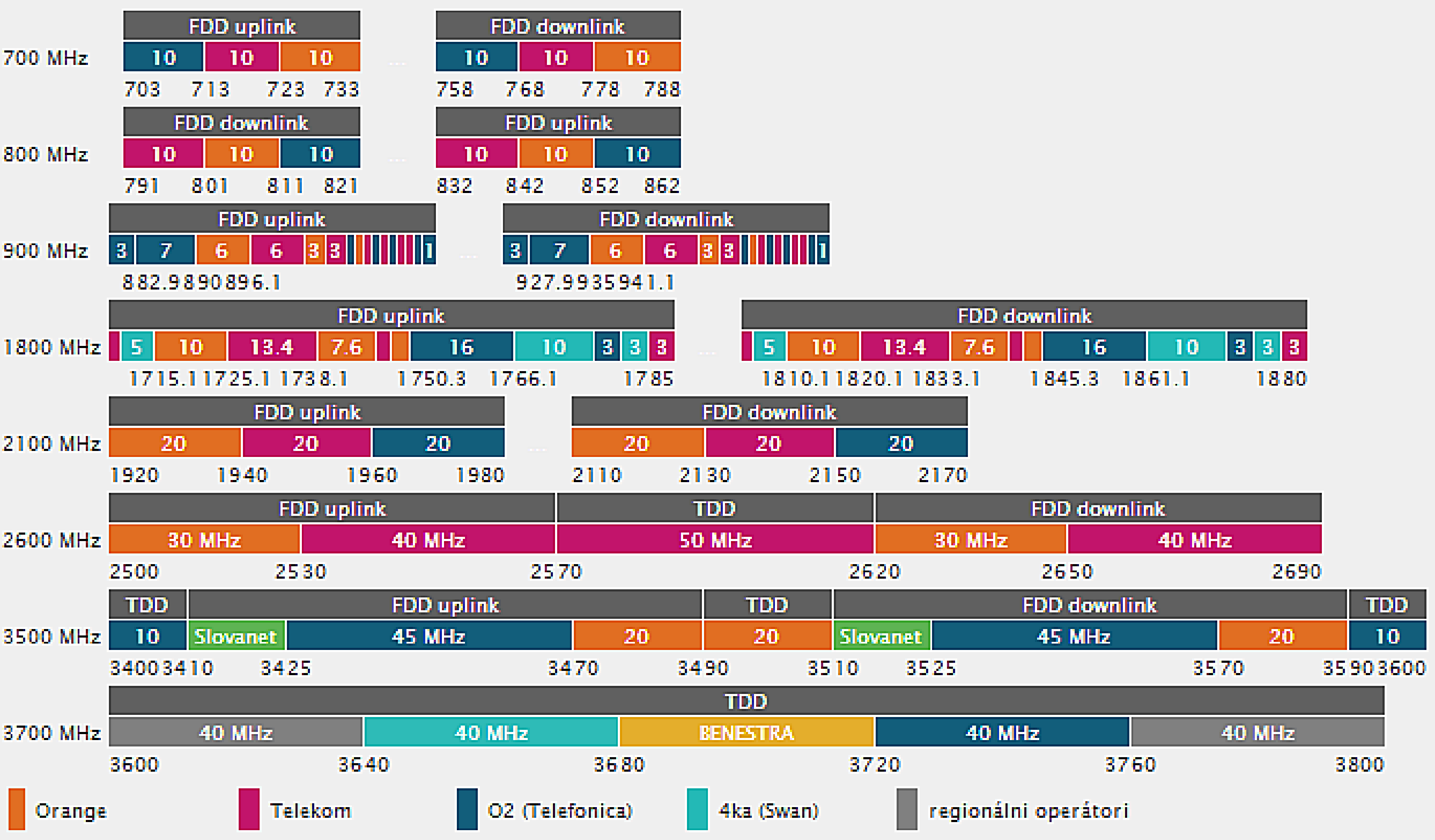


https://www.miwv.com/

Overview of band auctions & other milestones in SK

- 1991 – 450 MHz for NMT (ČSFR)
- 1996 – 900 and 1800 MHz for GSM, EuroTel (T-Mobile) and Globtel (Orange)
- 2002 – 2100 MHz
- 2006 – additional frequencies in 900 MHz, 1800 MHZ and 2100 MHz bands
- 2012 – Plan to free up 800MHz bands
- 2013 – 800, 1800 and 2600 MHz bands, including O2 and SWAN
- 2015 – 3500 MHz (3400 – 3600 MHz)
- 2016 – EU countries agreed on freeing up 700 MHz band for mobile communication (used for TV broadcasting, digital terrestrial TV broadcasting moved to 470 – 694 MHz)
- 2017 – 3700 MHz (3600 – 3800 MHz)
- 2020 – 700 MHz, 900 MHz and 1800 MHz, bands for 5G

Current (2020 - 2021) utilization of frequency bands

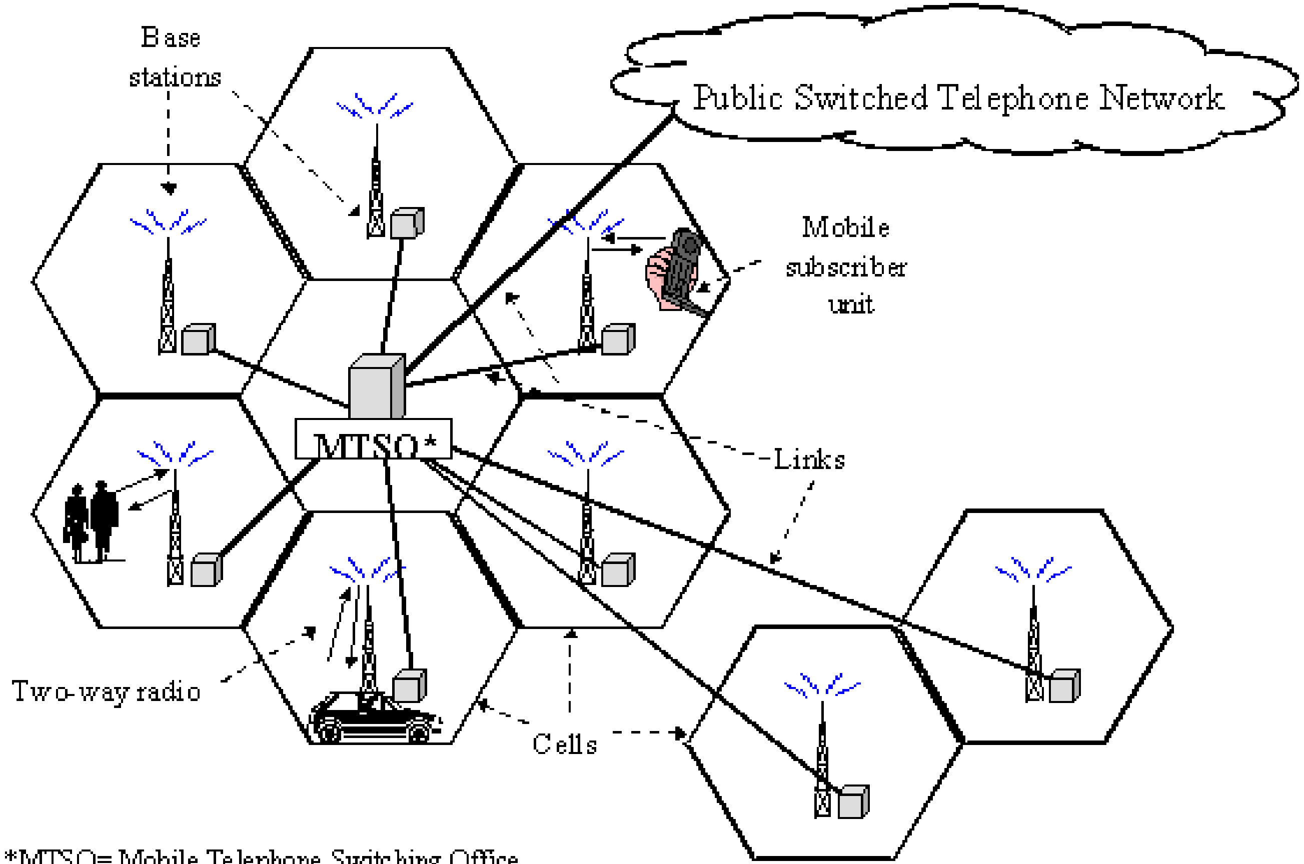


https://elektrosmog-info.voxo.eu/

- 2022 – 1800 MHz frequency band re-farming, each of 4 operators will receive a 20 MHz block of frequencies on the three agreed parts of SK and in one part 15 MHz

Mobile communication principle

- Mobility - cellular technology allows the “hand-off” of subscribers from one cell to another as they travel around
- A system constantly tracks mobile subscribers within a cell, and when a user reaches the border of a cell, the system automatically hands-off the call and the call is assigned with a new channel in a different cell

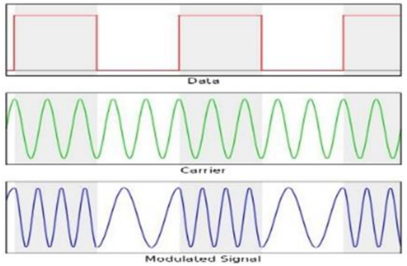


*MTSO= Mobile Telephone Switching Office

1G NMT
Nordic Mobile Telephone

1G - 1st generation of analog mobile communication

- NMT (Nordic Mobile Telephone)
  - NMT450 and NMT900, driven by Nordic PTT, E///, Mobira(Nokia)
  - Free standard ready in 1977
  - 1st network in 1981 in Sweden and Norway
  - Analog voice channel, FM modulation, FDMA multiple access, 25kHz
  - No SIM, phone number in EPROM (misused by cloning the number)
  - Digital control channel, FSK (Freq shift keying) modulation for signalling
  - NMT signalling transfer speed 1,200 bps
  - NMT also supported a simple but robust integrated data transfer mode (text messages)



FSK

- AMPS (Advanced Mobile Phone System)
  - Common effort between Bell Labs (Nokia Bell Labs today) and Motorola
  - Introduced in 1983 in North America

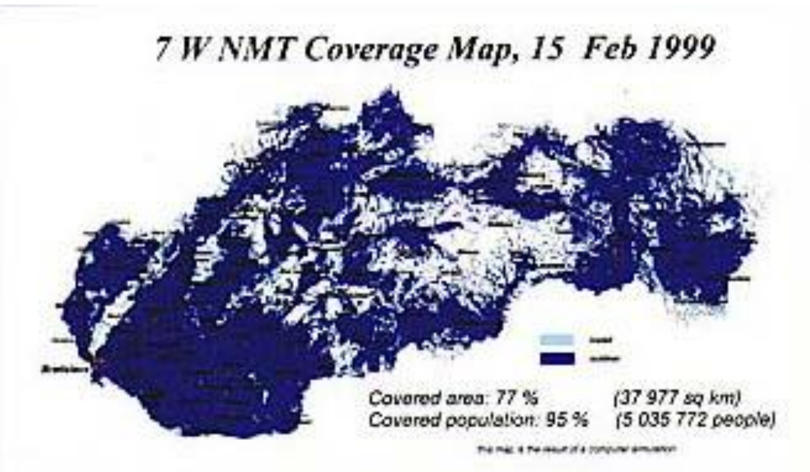
- NTT (Nippon Telegraph and Telephone)
- TACS (Total Access Communications System) in UK
- Other

One of the 1st mobile phones released in 80's. It took 10 hours to charge, lasted for 30 minutes of talk-time, stored 30 numbers and cost $4,000 at the time

1G / NMT in our region

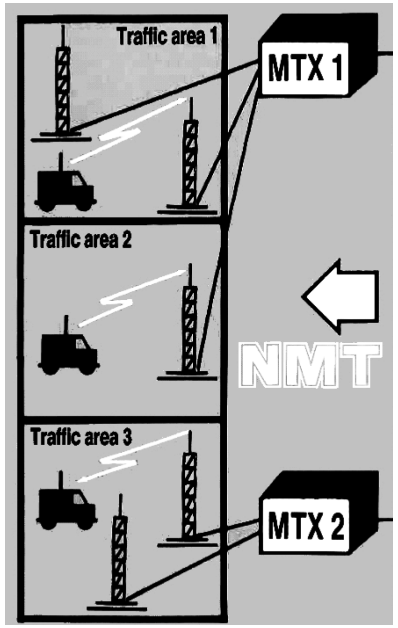
- 1st NMT mobile network operated by Eurotel Praha a Eurotel Bratislava introduced in ČSFR in 1991
  - ~70k-120k subscribers
  - 450 Mhz
  - Company has been established by Správa pôšt a telekomunikácií 51% a US based Atlantic West B.V (US West a Bell Atlantic operators) 49%
  - Slovak Telecom has bought shares from Atlantic West B.V. in 2004
  - The Slovak branch was rebranded to T-mobile (DT) in 2005, the Czech branch to O2 in 2006

- 2G GSM standard introduced in 1997
  - Another mobile operator Globtel in SK (Orange from 2002)
  - ČR: Eurotel -> O2, Paegas -> T-Mobile, Oskar -> Vodafone



1G / NMT450 characteristics

- NMS architecture
  - MS (Mobile Station)
  - BS (Base Station) is a node without switching function between the wire toward MTX and radio path
  - MTX (Mobile Telephone Exchange) controls traffic between MSes and supervises BSes
  - HLR (Home Location Register), integrated in MTX or sometimes as a separate node



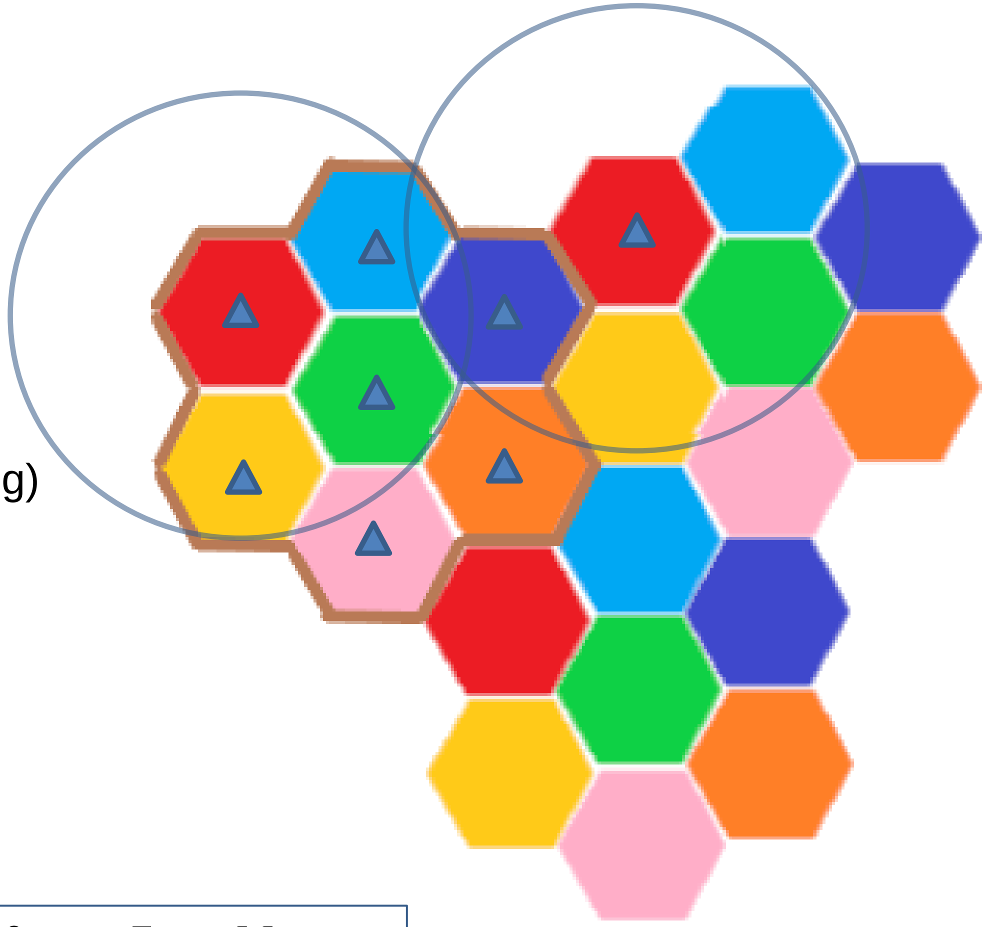
- Frequency range 450-470 MHz
  - 462.500 - 467.500 MHz (downlink); 452.500 - 457.500 MHz (uplink)
  - Channel spacing 25kHz, optionally 12.5KHz
  - 200 uplink + 200 downlink channels (5Mhz/25kHz)
  - Cell coverage radius 2-40 km
  - Mobile station transmit power: up to 15 Watts (1 Watts hand-held)
  - Base station transmit power: 50 Watts

- Signalling / control high level
  - MS sweeps through all the supported channels and identifies the channel type (voice or traffic / control)
  - MTX indicates free voice channels to MSes, if MS initiates call, picks up the free channel and send a message to MTX, MTX removes the channel from the free list, performs handshaking and waits for number
  - MTX manages handover between cells based on signal strength measurements on the channels

Cellular concept

- Why not large radio tower and large service area?
  - Number of simultaneous users would be very limited
  - Mobile handset would have greater power requirements

- Cellular concept means small cells with frequency reuse
  - Cluster - group of cells with different frequencies
  - Hand-off between cells must be supported
  - Different frequency sets in neighboring cells (red, blue, etc) in order to eliminate interference
  - Track user location to route incoming calls/messages
  - Sectoring - cell divided into 3 (120° sectoring) or 6 (60° sectoring) equally sized sectors (2G and later)



- Let define
  - **T** total number of duplex channels per system
  - **K** cells in single cluster , (often 3,4,7,12,21)
  - **K** depends on interference toleration and path loss
  - **N** = **T / K** number of channels per cluster
  - **M** times replicated cluster in the area
  - System capacity = **M * T**

T=200, K=7 cells -> N=~28 channels per sector

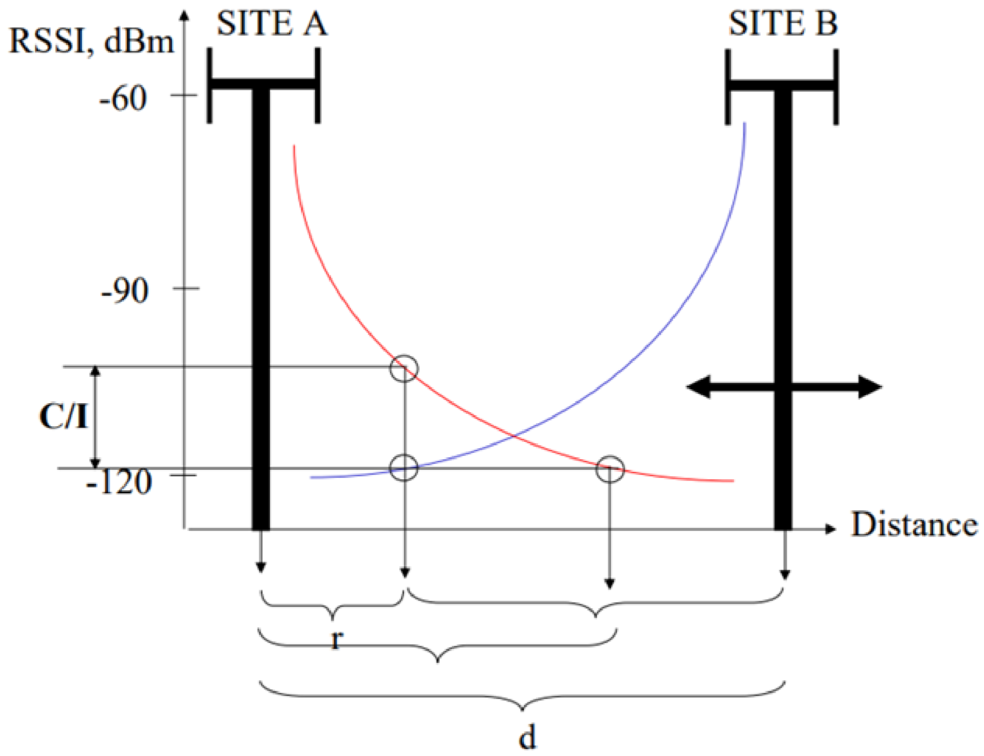
Frequency reuse

- Reuse the same EM spectrum in another geographical region
- Carrier-to-Interference ratio (C/I) - ratio of power in an RF carrier to the interference power in the channel
- Typical C/I values used in practice are 13-18 dB, digital systems have lower C/I (13-15 dB)
- Once the frequency reuse cluster size and frequency allocation determined frequencies must be assigned to cells
- r - radius of cell
- d – distance in between BSes with the same frequency

From hexagonal geometry $d = r\sqrt{3K}$

$$\frac{d}{r} = \left(\frac{6C}{I}\right)^{1/\alpha}$$

$$K = \frac{1}{3}\left(\frac{6C}{I}\right)^{2/\alpha}$$

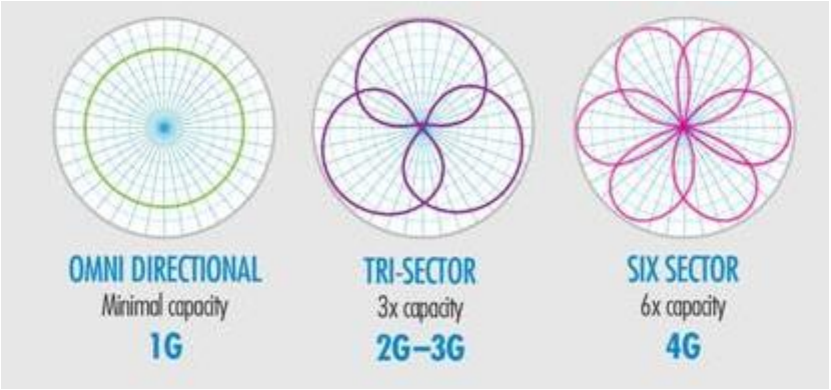


- α - path loss coefficient [dB]
  - suburban propagation environment with α = ~ 4
- Power gain: dB = 10log(P1/P2)
- 18 dB => P1/P2 = 63.1

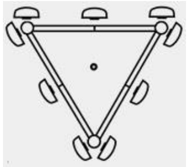
- K = 1/3 * (6* 63.1) ^ (1/2) = 6.49 = ~7

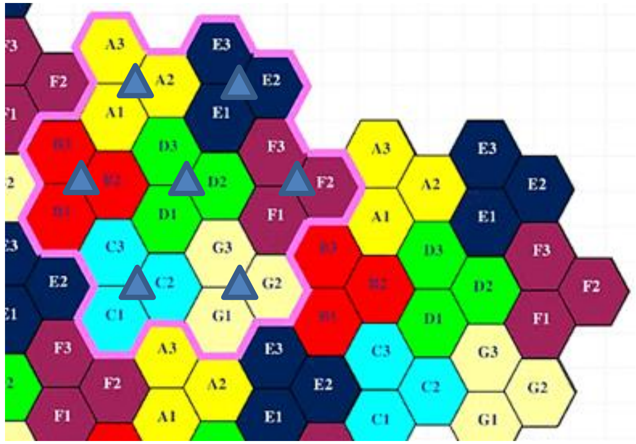
Sectoring

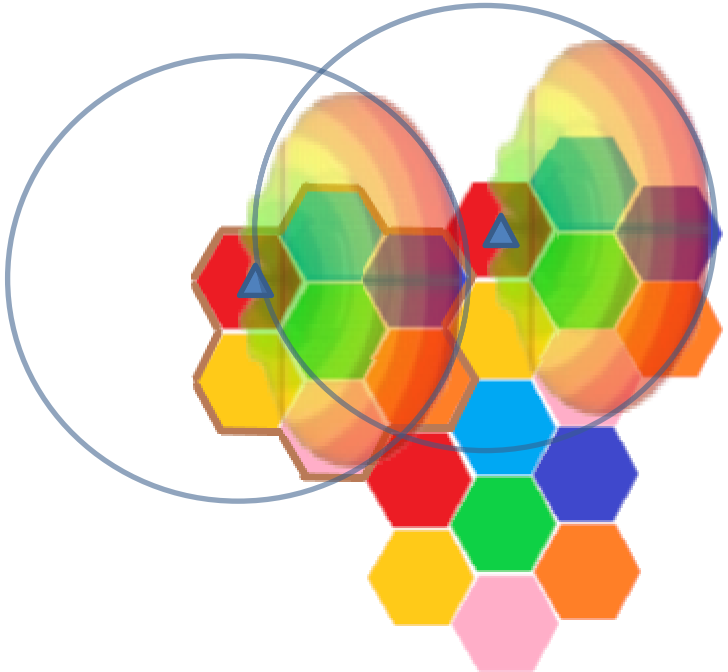
- Used to improve C/I ratio, makes geographical size of cluster K smaller -> therefore greater system capacity
- Use directional antennas reduces co-channel interference
- Cells divided into 3 or 6 sectors
- Frequency channels assigned to cells must be partitioned into 3 (6) disjoint sets
- Disadvantage – intra-cell hand-off, complexity
- Cells & Sectors in a single cluster
  - 21 cells with no sectors or
  - 7 cells with 3 sectors (21/7)
  - but also 12/4, 9/3
- T=200, K=21 sectors
  - N = T/K = ~9 channels per sector
  - 27 channels per cell
  - Cell size can be smaller



Cell types







2G / GSM
Global System for Mobile communication

GSM

GSM

- Motivation for 2G Digital Cellular
  - Increase System Capacity
  - Add additional services/features (SMS, caller ID, data)
  - Reduce Cost
  - Improve Security
  - Interoperability with other systems

GSM - history

- GSM is a standard developed by the European Telecommunications Standards Institute (ETSI, based in Sophia-Antipolis, France) to describe the protocols for the 2nd generation (2G) digital cellular networks

- GSM initiative (R&D labs, operators, vendors and universities) became part of ETSI committee in 1988

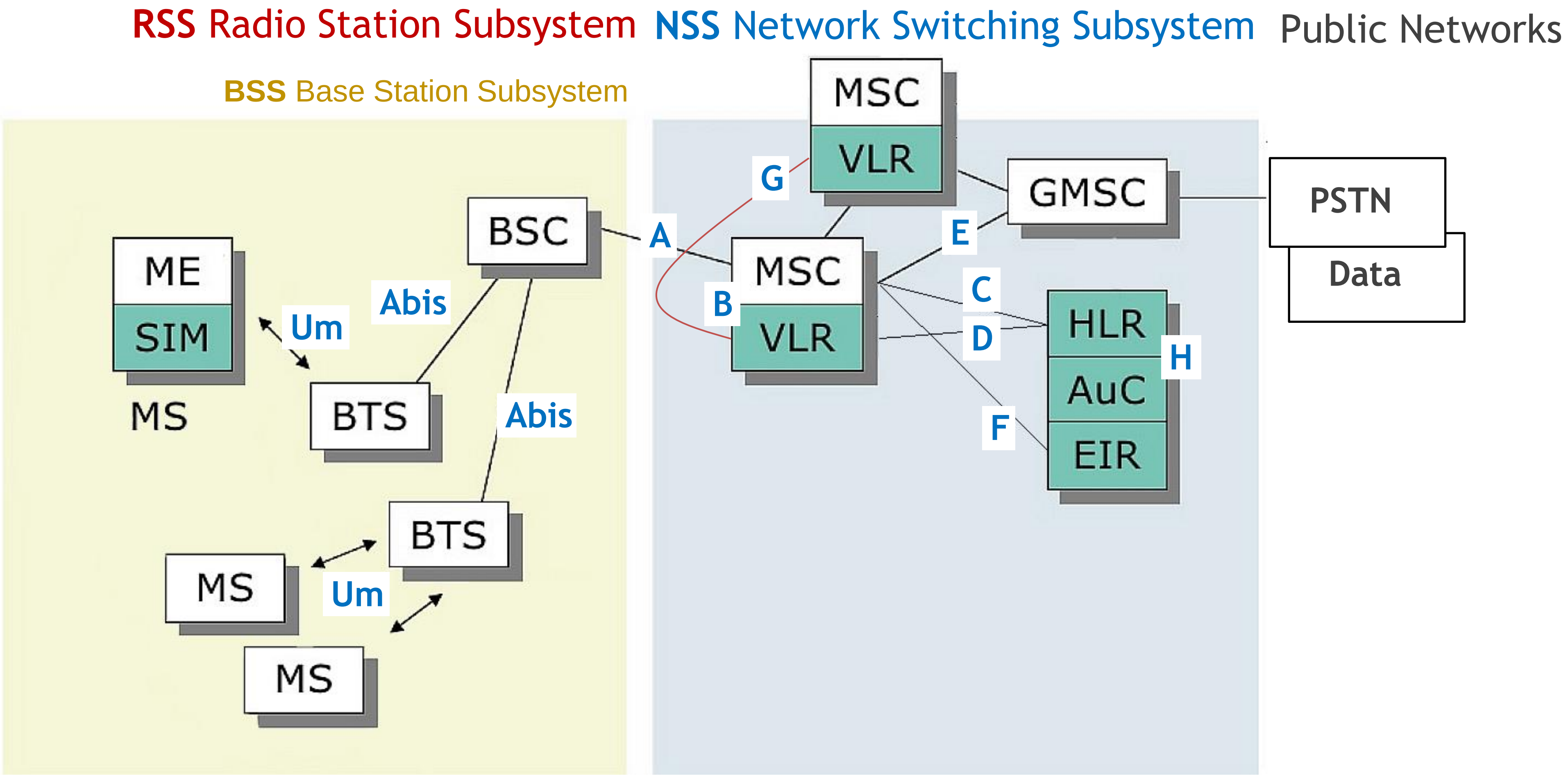
- 1st GSM network launched in 1991, Finland

- In 1998 over 270 GSM networks with ~70 million of subscribers worldwide

- Launch of GPRS (General Packet Radio Service) - packet data transport - in 2000

- GSM systems and services are described in a set of standards governed by ETSI
  - ETSI has been established in 1988 and has over 800 members (full or associate members outside of EU)
  - Active in the field of information and communications mainly in EU
  - https://www.etsi.org/

GSM architecture and interfaces



BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
PSTN	Public Switched Telephone Network

ISDN	Integrated Service Digital Network
HLR/VLR	Home/Visitor Location Register
AUC	Authentication Center
EIR	Equipment Identity Register

GSM architecture

Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	X
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurements	X	
Traffic measurement		X
Handover management		X

BSS - Base Station Subsystem is responsible for transcoding of speech channels, allocation of radio channels to mobile phones, paging, transmission and reception over the air interface

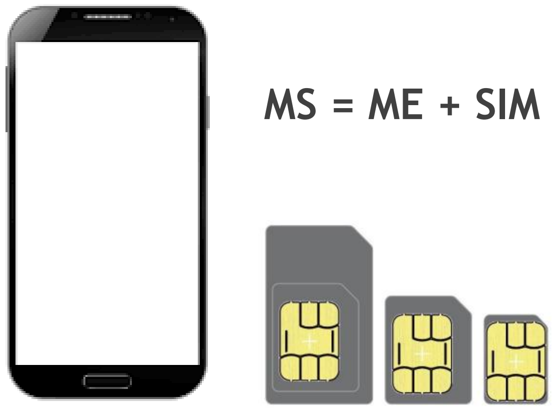
- BTS (Base Transceiver Station) is a term used to denote a Base station in GSM terminology. A BTS consists of an antenna and the digital radio equipment necessary to communicate by radio with a Mobile Station (MS). Each BTS covers a defined area, known as a cell. A BTS is under control of a BSC, which is in turn under control of a MSC (Mobile Switching Centre)
  - Typically has several so called “Transceivers” (TRXs) which allow it to serve several different frequencies and different sectors of the cell
- BSC (Base Station Controller) is in control of and supervises a tens or hundreds of BTSes. The BSC is responsible for the allocation of radio resources to a mobile call and for the handovers that are made between base stations under his control. Other handovers are under control of the MSC. Maps radio channels “Um” to terrestrial channels “A”

GSM architecture

NSS - Network Switching Subsystem is the main component of the public mobile network GSM - switching, mobility management, interconnection to other networks, system control

- MSC (Mobile Services Switching Center) - controls all connections to/from a mobile terminal within the domain of the MSC, several BSCs can belong to a MSC
  - MS registration and switching functions
  - Mobility support
  - Management of network resources
  - Interworking functions via GW MSC
  - SMS support
  - Generating billing information
- Databases (important: scalability, high capacity, low delay)
  - HLR (Home Location Register) - central master database containing static user data, (mobile number, billing address, service subscribed, etc.) and dynamic data of all subscribers last VLR location
  - VLR (Visitor Location Register) - local dynamic database for a subset of HLR data, including data about all user currently in the domain of the MSC attached to VLR

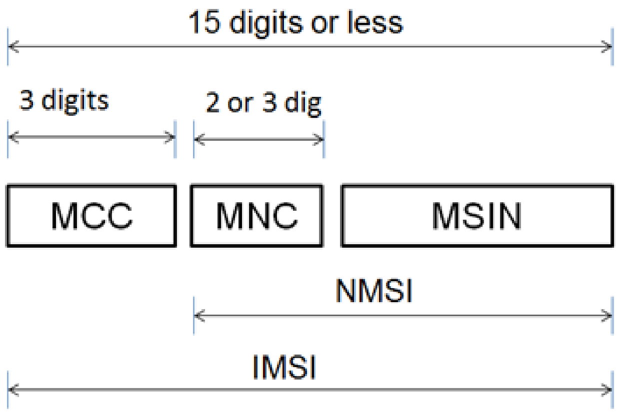
Mobile Station



- MS Mobile Station
- ME Mobile Equipment
- SIM Subscriber Identity Module (Mini, Micro, Nano) - an integrated circuit that is intended to securely store the IMSI (International Mobile Subscriber Identity) number and its related unique authentication key, two passwords a PIN (Personal Identification Number) for ordinary use, and a PUK (Personal Unblocking Key) for PIN unlocking. It is also possible to store contacts.
- Each SIM is internationally identified by its ICCID (Integrated Circuit Card Identifier)

IMSI - uniquely identifies every user of a cellular network. It is stored as a 64-bit field and is sent by the mobile device to the network.

- IMSI = MCC + MNC + MSIN
- **MCC** (Mobile Country Code) and **MNC** (Mobile Network Code) identifies an operator
- **MSIN** (Mobile Subscriber Identification Number) – max 10 digits
- Not visible to the subscriber



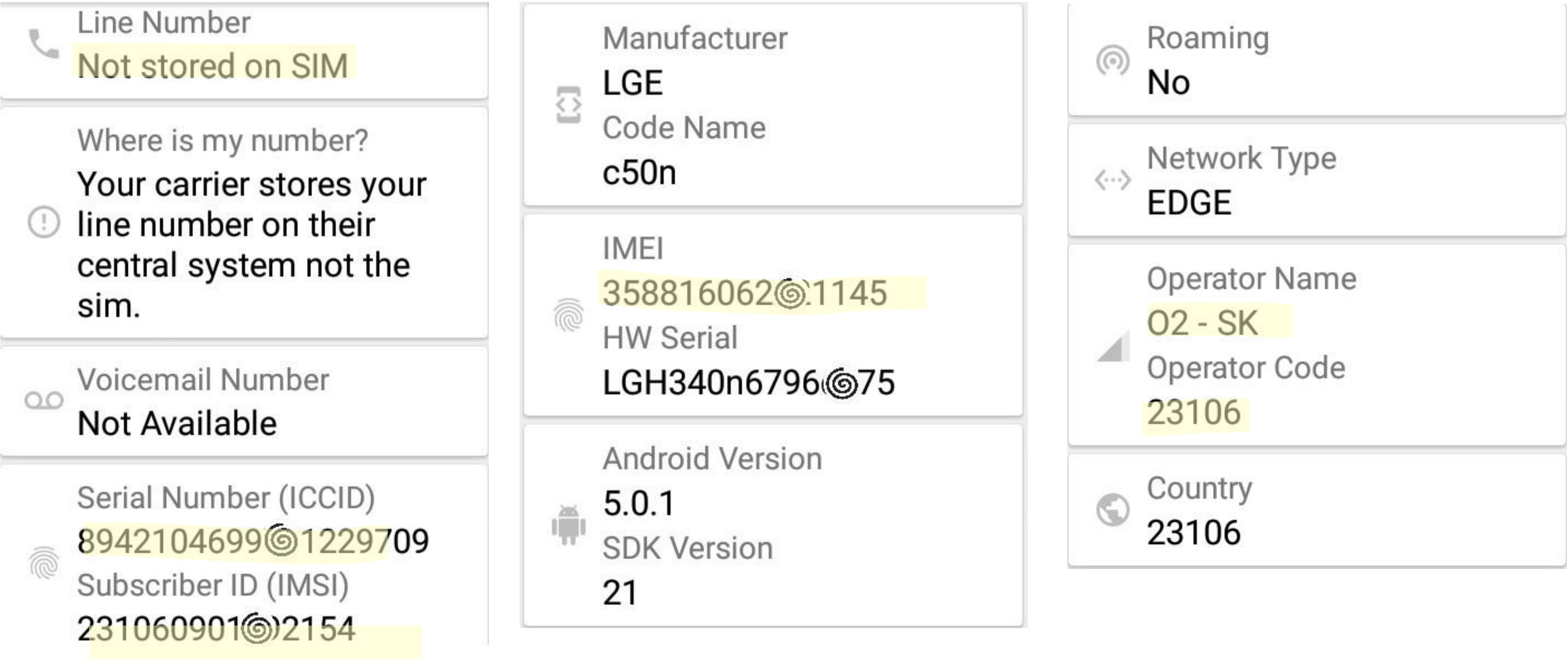
MSISDN (Mobile Subscriber Integrated Services Digital Network Number)

- Dialed number to reach a GSM user
- MSISDN = CC (Country Code) + NDC (National Destination Code) + SN (Serial Number) of the subscriber

MCC	MNC	CC	Network
231	3	421	4Ka
231	6	421	O2
231	1	421	Orange
231	5	421	Orange
231	15	421	Orange
231	2	421	T-Mobile
231	4	421	T-Mobile
231	99	421	ZSR

IMEI (International Mobile Equipment Identity) is a unique number to identify mobile phones

MS - SIM, device and network information example



Conventional versus Distributed BTS site

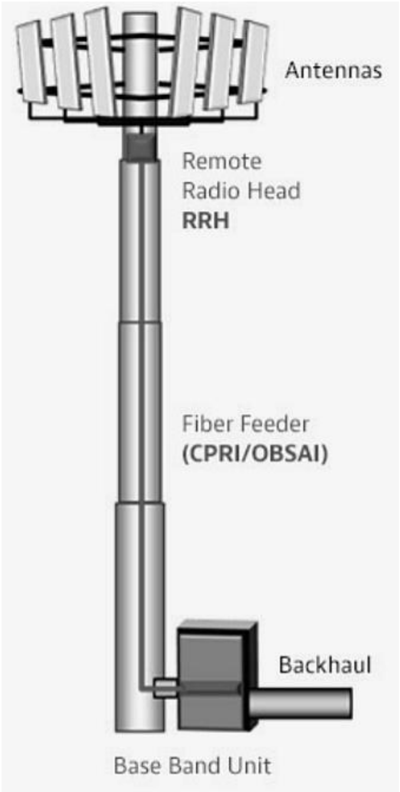
Cell site with coaxial feeders

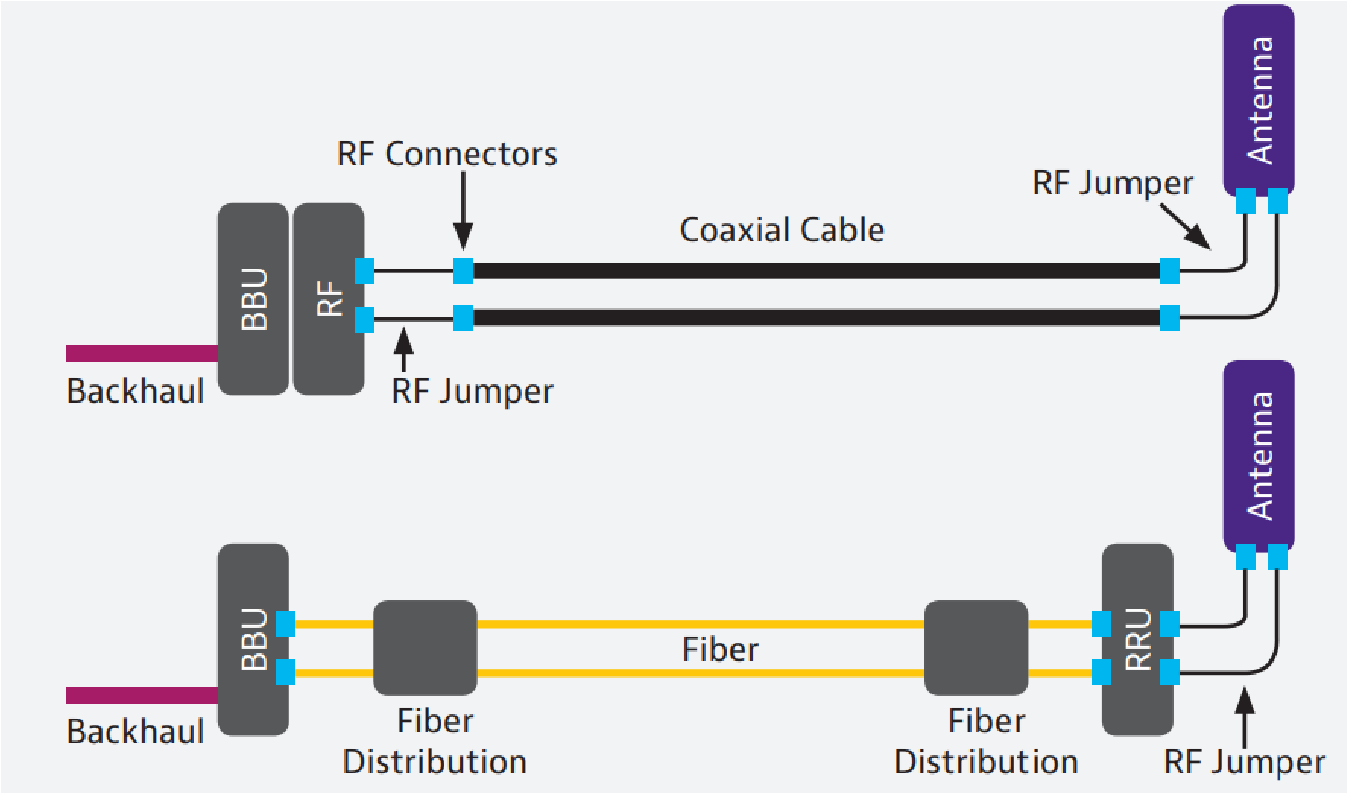
+ RF access for interference analysis from the cabinet
- High loss, signal reflection, passive intermodulation

Distributed cell site

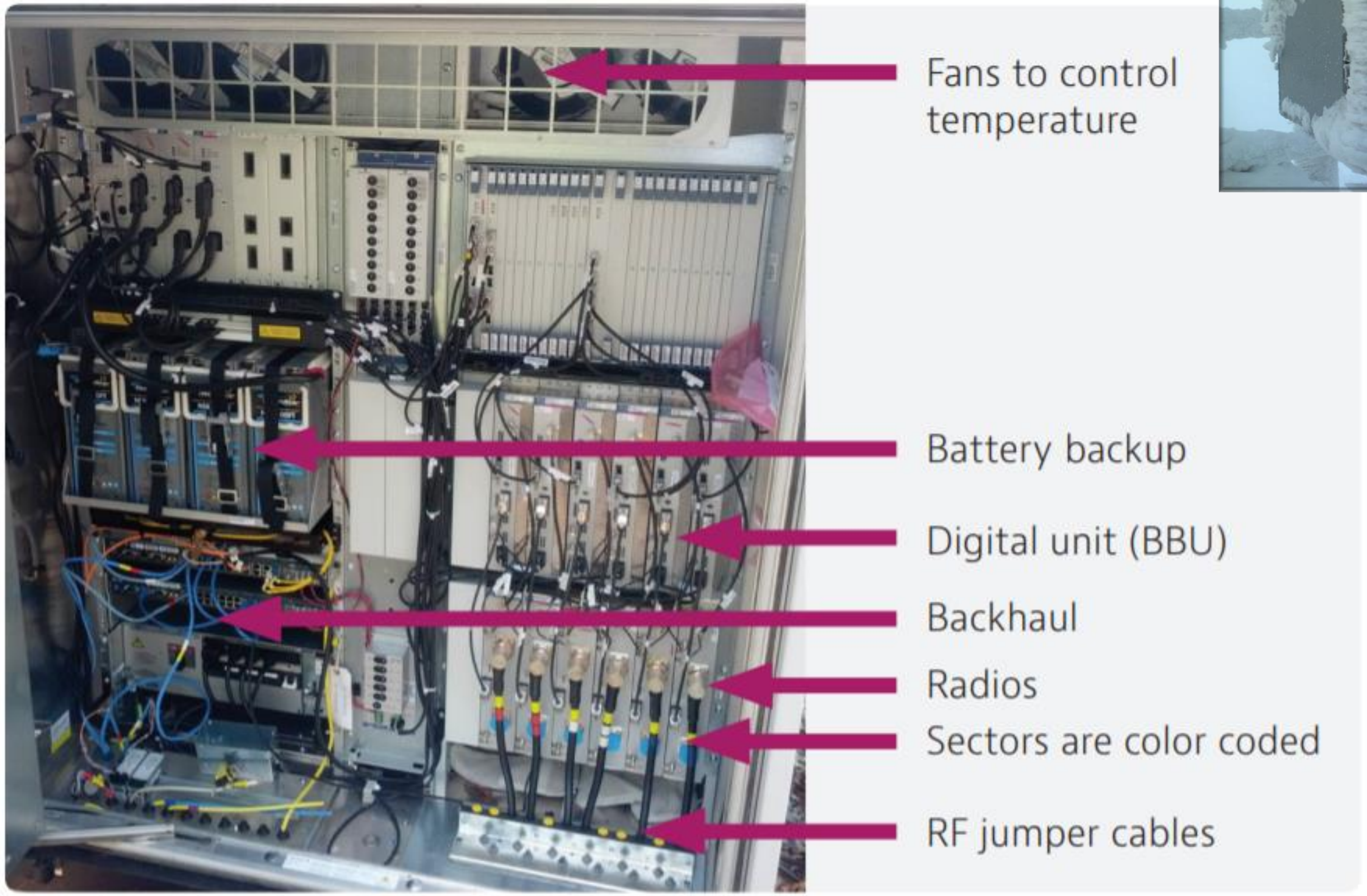
- RF access from RRH only
- extra power feeds for RRH needed

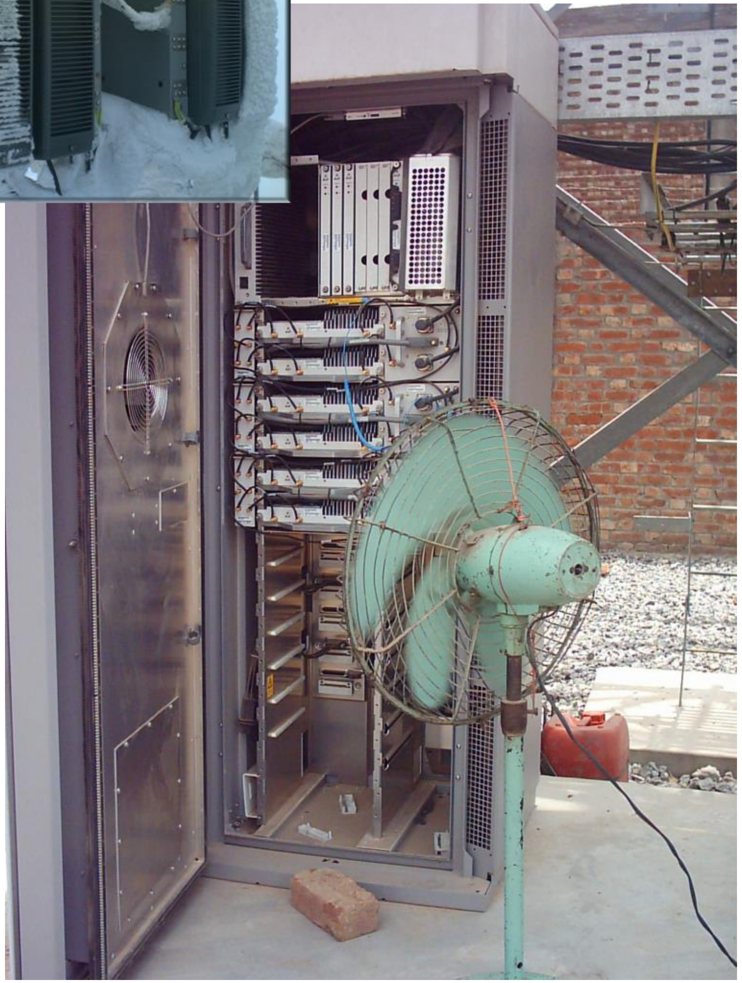
+ small loss & signal reflection & passive intermodulation





BTS outdoor cabinet





Generally located at the base of the tower, sometimes on a rooftop

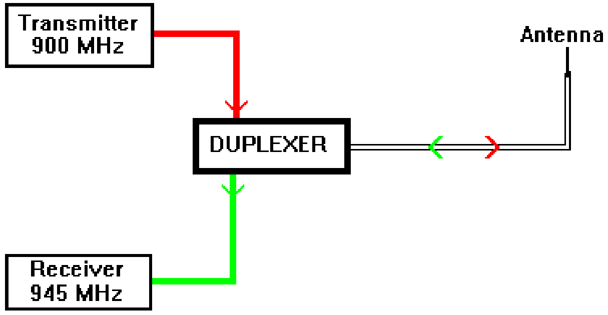
Cooling is important

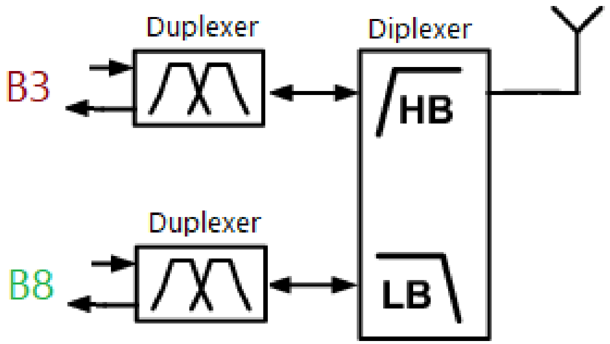
BTS components

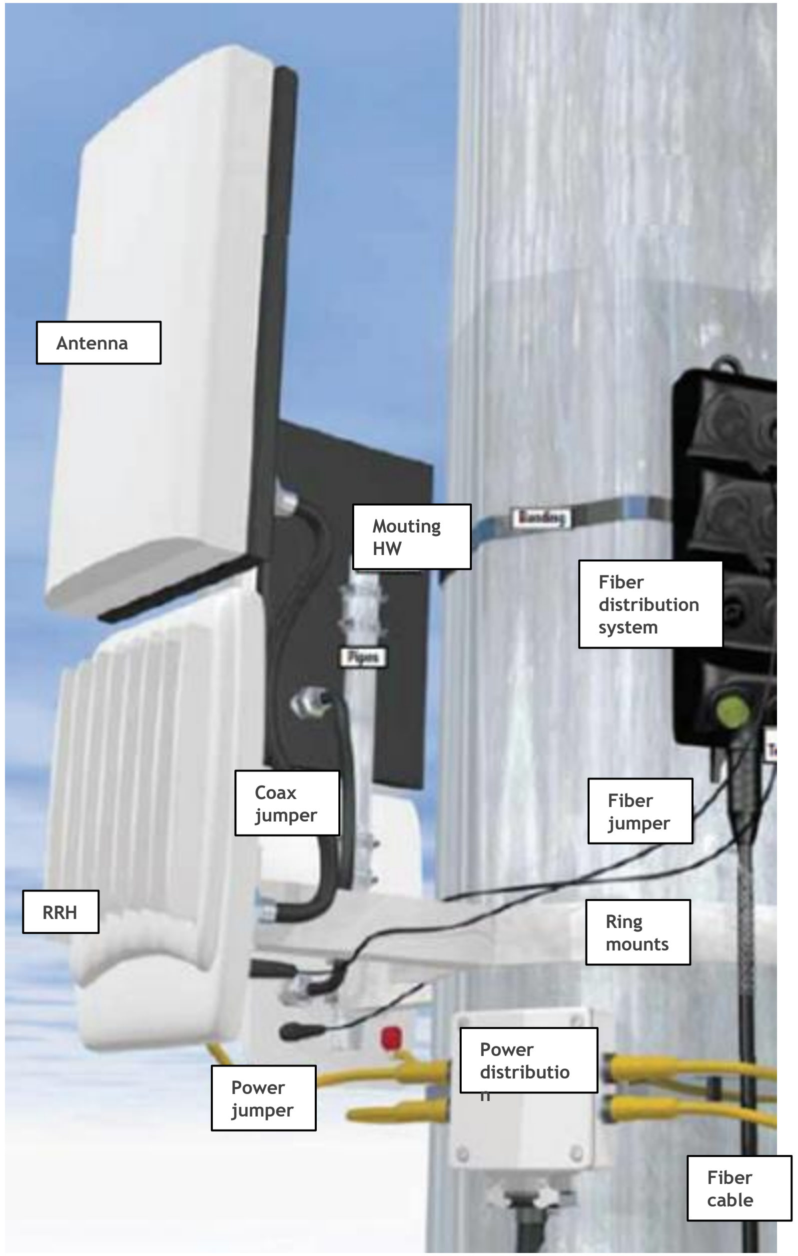
- <u>Duplexer</u> is a device that allows the use of a single antenna for both a transmitter and a receiver

- <u>Diplexers</u> separate two different frequency bands in the receive path and combine them in the transmit path. Useful in reducing the number of cables running up the cell-tower.

- <u>MHA</u> (Mast Head Amplifier) is a low-noise amplifier mounted as close as practical to the antenna, the receiver at the base station is able to receive weaker signals from the cell phone (mobile transmit power is limited and generally transmits around 200 mW)

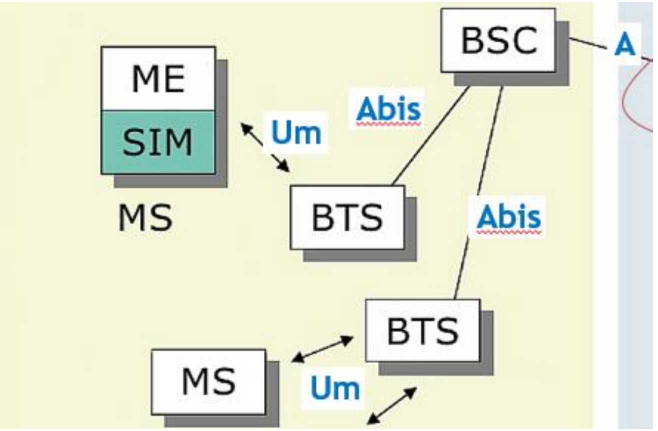






GSM air interface Um

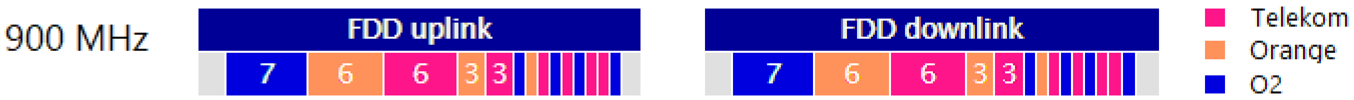
- GSM uses FDD (Frequency Division Duplexing) where the uplink and downlink of each channel operates on a different frequency; uplink / downlink bands often separated by 20 MHz
- ARFCN (Absolute Radio Frequency Channel Number) is unique number given to each radio channel in GSM
  - In GSM each channel is 200 KHz wide
- Also each band has a “class name”; 900Mhz GSM-900 or B8 for LTE
- GSM-900 and GSM-1800 are used in most parts of the world
- GSM-900 is the most common one
- GSM-1900 and GSM-850 are used in most of North, South and Central America
- Most mobile phones support multiple bands as used in different countries to facilitate roaming
- There are also standardized other frequency bands, rarely in use



	Band class	Uplink (MHz)	Downlink (MHz)
GSM	GSM 850	824~849	869~894
	GSM 900	880~915	925~960
	PCS 1800	1710~1785	1805~1880
	PCS 1900	1850~1910	1930~1990
CDMA	BC0 (850)	824~849	869~894
	BC1 (1900)	1850~1910	1930~1990
WCDMA	B5 (850)	824~849	869~894
	B8 (900)	880~915	925~960
	B2 (1900)	1850~1910	1930~1990
	B1 (2100)	1920~1980	2110~2170
LTE (TDD)	B38	2570~2620	2570~2620
	B41	2496~2690	2496~2690
LTE (FDD)	B1	1920~1980	2110~2170
	B2	1850~1910	1930~1990
	B3	1710~1785	1805~1880
	B4	1710~1755	2110~2155
	B5	824~849	869~894
	B7	2500~2570	2620~2690
	B8	880~915	925~960
	B12	699~716	729~746
	B13	778~787	746~756
	B17	704~716	734~746
	B20	823~862	791~821
	B25	1850~1915	1930~1995

Band	ARFCN	Uplink (MHz)	Downlink (MHz)
GSM 900 (primary)	0–124	890–915	935–960
GSM 900 (extended)	975–1023, 0–124	880–915	925–960
GSM 1800	512–885	1710–1785	1805–1880
GSM 1900 (North America)	512–810	1850–1910	1930–1990
GSM 850 (North America)	128–251	824–849	869–894
GSM-R	0–124, 955–1023	876–915	921–960

Optimal use of GSM frequencies



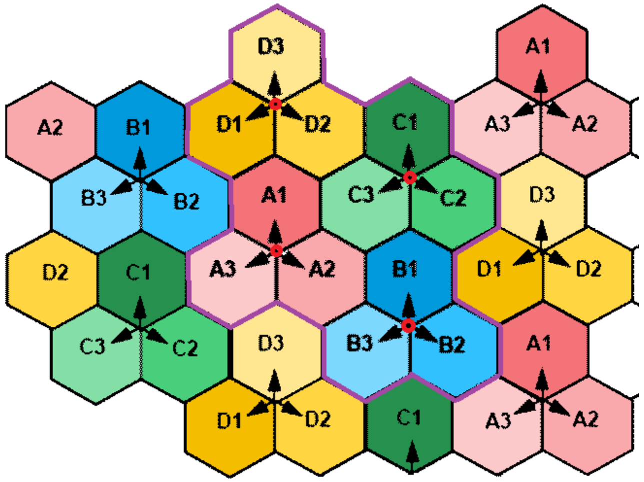
Example:

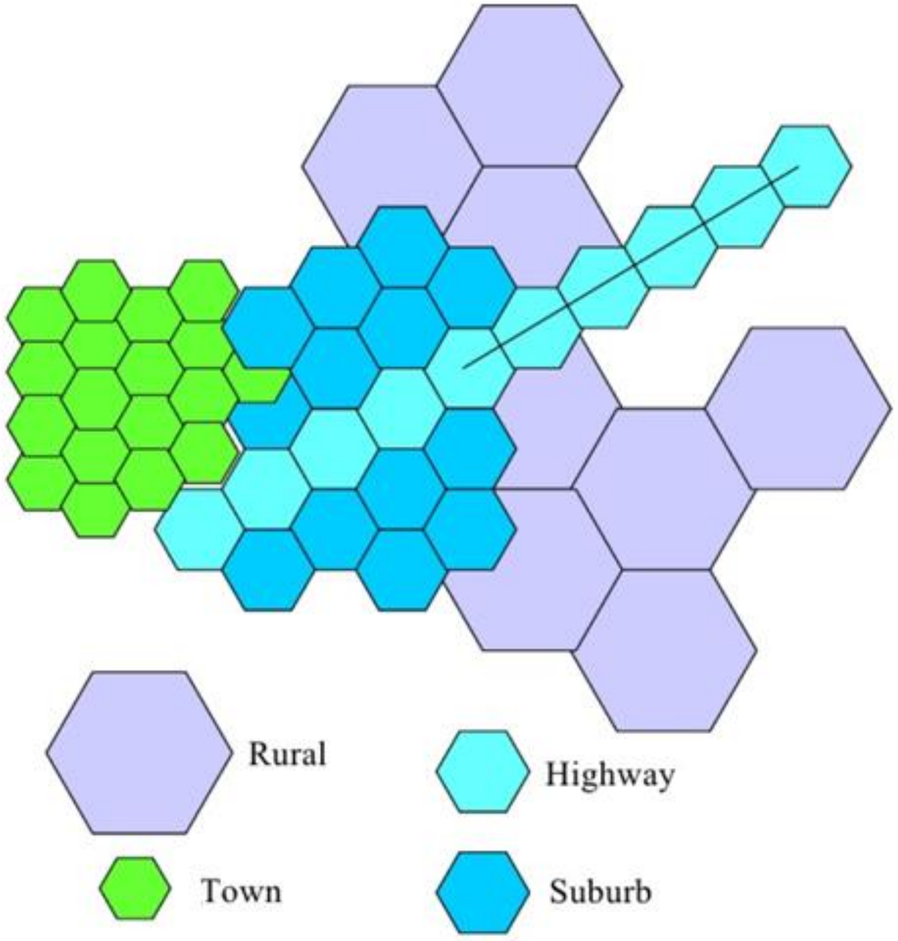
- Operator’s bandwidth of 6Mhz from GSM-900
- **K** factor = 12 (or 4 cells with 3 sectors in cell) - 12/4 cluster

- **T** (total number of channels) 6MHz / 200KHz = 30 carriers * 8 slots
- **N** = 30*8 / 12 = 240 / 12 = ~20 channels per sector (often an integer value of TRX units which satisfy radio & signal processing (Tx & Rx carriers) per sector)

- = ~ 3 TRXes per sector
  - 1 TRX represents typically ~ 6-7 voice calls (the rest for control purposes)

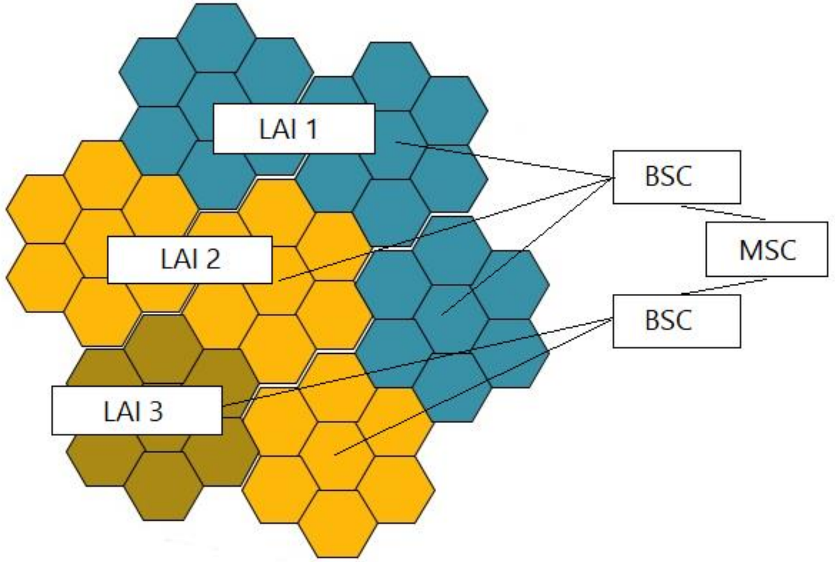
12/4 cluster



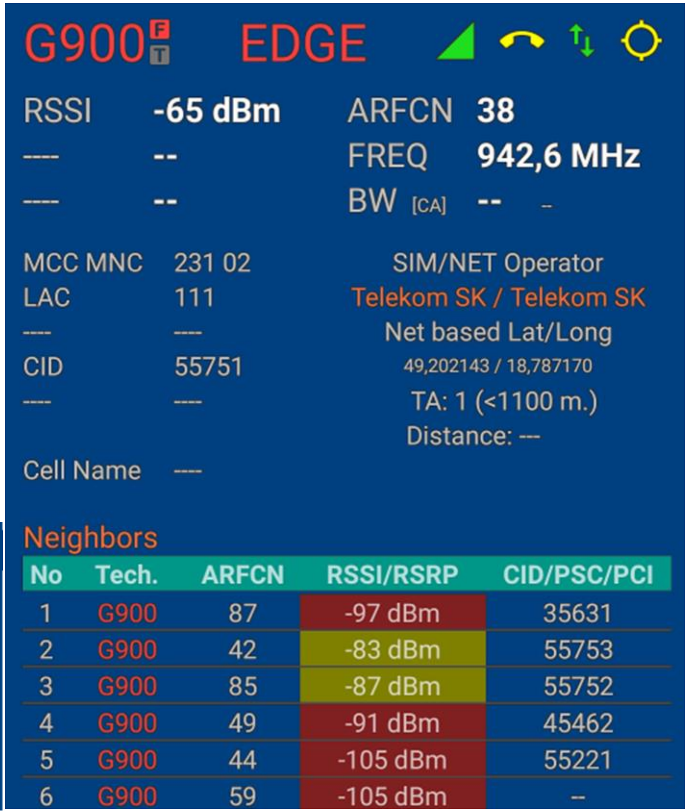


Cell distribution example in a mobile network

Location area and cell identification



- **PLMN** (Public Land Mobile Network) - network identifier = MCC (mobile country code) + MNC (mobile network code)
- **LAC (**Location Area Code) – identifies area within PLMN
- **LAI** (Location area Identity)
  - LAI = MCC+MNC+LAC
- **CID** (Cell ID) – unique ID of the cell/sector
- **BSIC** (BTS Identity Code)
- **TMSI** (Temporary Mobile Station Identity) – 4B MS temporary identifier. Used instead of IMSI for security reasons
- **RSSI** (Received Signal Strength Indicator), in dBm, measurement of the Radio Frequency (RF) power present in a received radio signal at the mobile device
- **ASU** (Arbitrary Strength Unit) – integer value proportional to the received signal, ASU maps to RSSI
- **TA** (Time Advance) - value corresponds to the length of time a signal takes to reach the base station from a mobile phone; radio waves travel at the finite speed of light, the precise arrival-time within the slot can be used by the base station to determine the distance to the mobile phone. 1 unit = 3.69 microsec (~1100m RTT or 550m one way)
- **ARFCN** (Absolute Radio Frequency Channel Number)

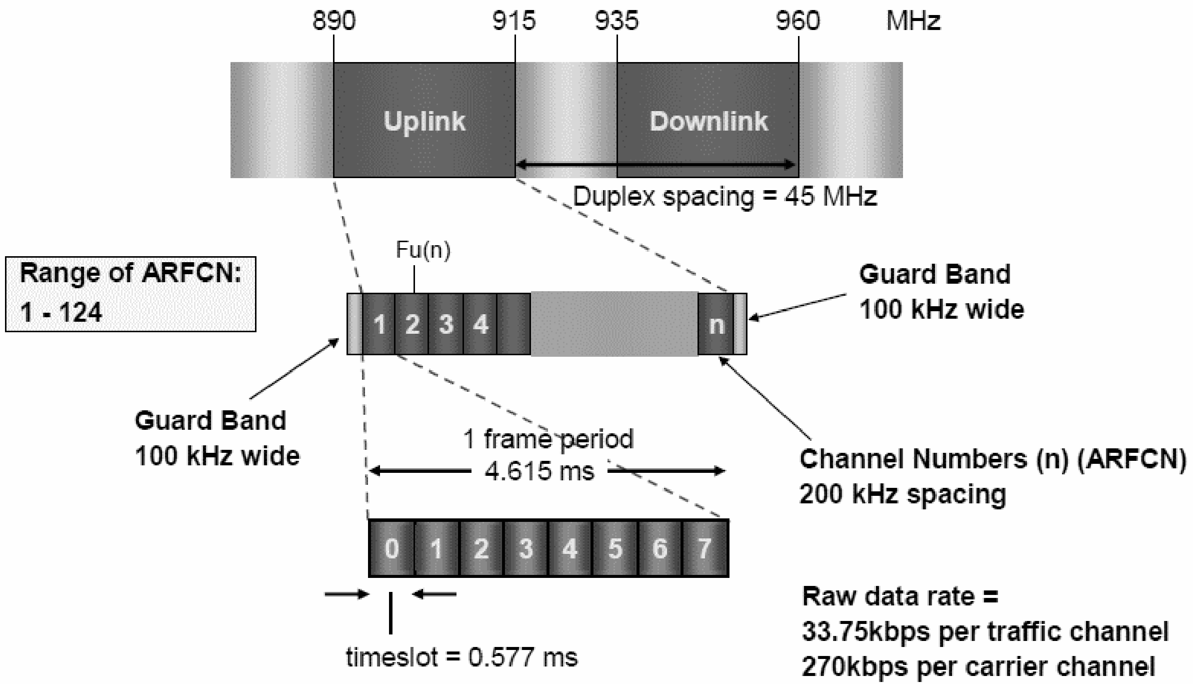


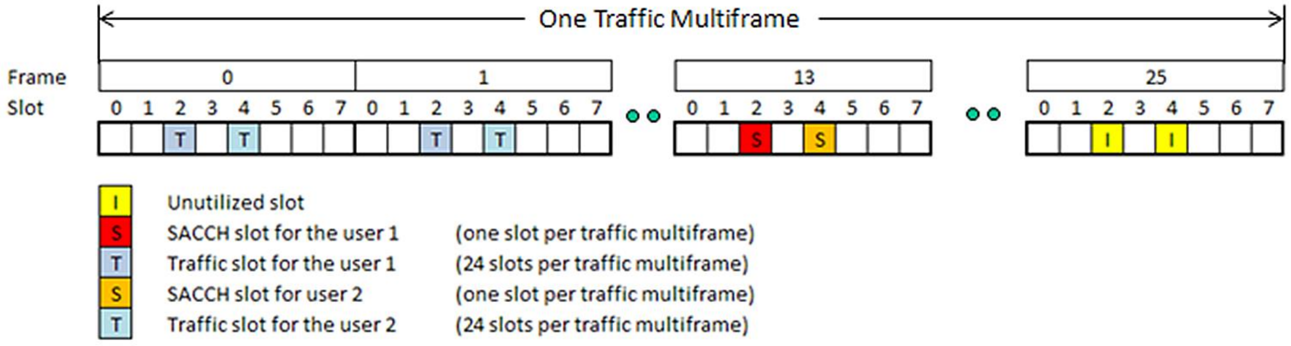
GSM-900 frequency and time channel allocation

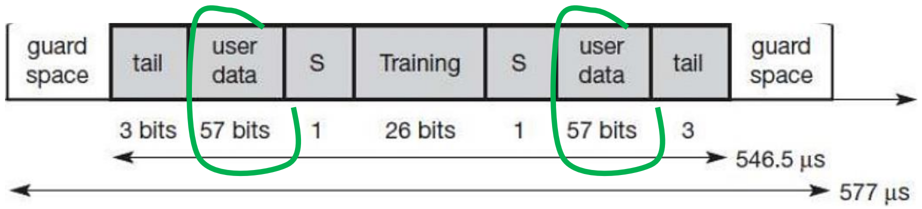
- FDMA/TDMA combined physical channel structure

- <u>FDMA part:</u>
  - 124 * 200kHz (25Mhz) channels
  - 2*100 kHz guard bands

- <u>TDMA part:</u>
  - Each GSM carrier channel is subdivided by time into 8 timeslots
  - Single <u>timeslot</u> is 0.577ms
  - TDMA <u>frames</u> repeated every 4.615ms (8 slots)
  - TDMA <u>multi-frame</u> = 26 TDMA frames (120 msec)
  - Different “Burst structure” types of data mapped into the timeslot – Normal, Sync, Freq. correction, Access







Frame timeslot (0.577 ms) – Normal data burst structure

- TCH traffic channel
- SACCH - Slow Associated Control Channel – associated to the TCH, in downlink provides timing advance and transmit power control info, in uplink carries received signal strength

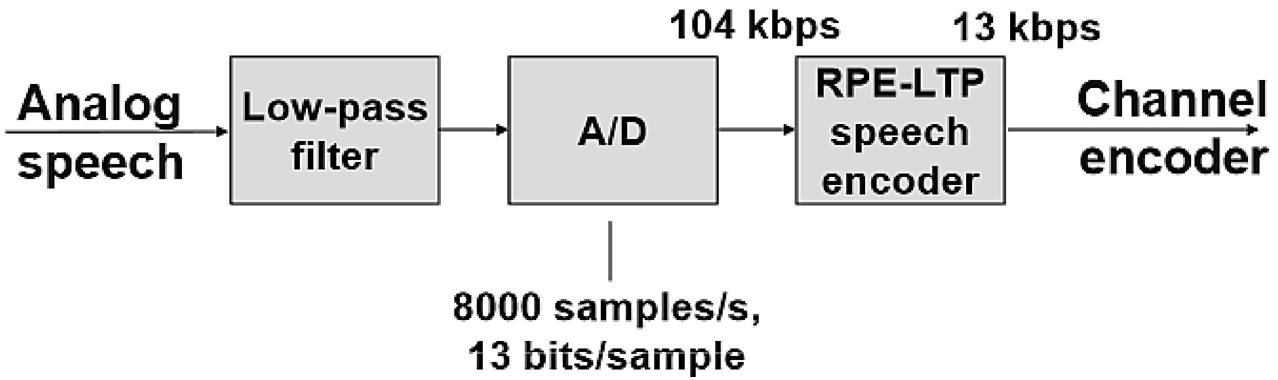
Uplink and Downlink channels have a 3 slot offset – so that MS doesn’t have to transmit and receive simultaneously

GSM speech coding

- **Full Rate** (FR or GSM-FR) was the first digital speech coding standard used in the GSM digital mobile phone system from 1990. It uses linear predictive coding (LPC). The bit rate of the codec is 13 kbit/s.
  - RPE-LTP (Regular Pulse Excitation – Long Term Prediction) coding scheme for reducing the amount of data between MS and BTS
  - When a voltage level of a particular speech sample is quantified, the mobile station's internal logic predicts the voltage level for the next sample. When the next sample is quantified, the packet sent by the MS to the BTS contains only the error (the signed difference between the actual and predicted level of the sample)
  - Input 160 * 13bit samples / 20 msec (160*13*50 = 104 kbps)
  - Output 260 bits / 20 msec to channel encoder (260*50 = 13 kbps)

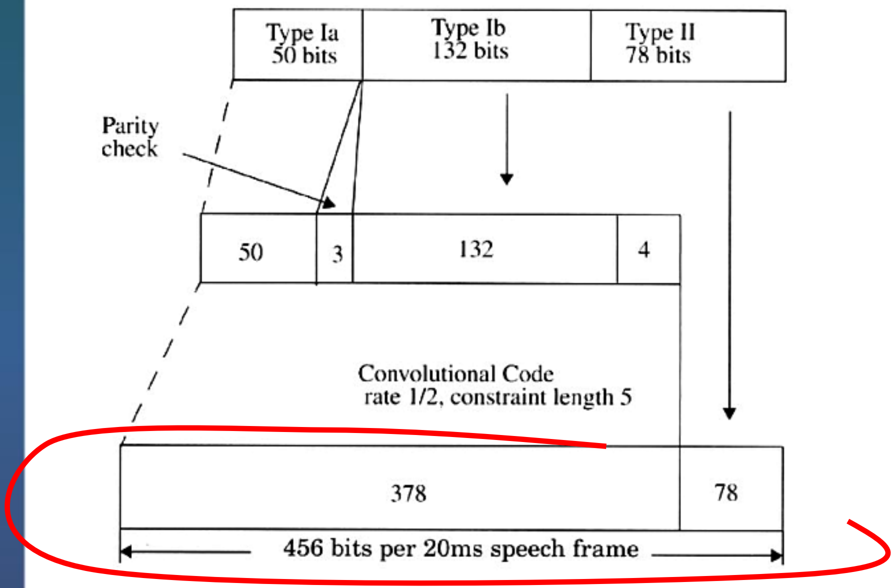
- **Half Rate** (HR or GSM-HR) is a speech coding system for GSM operating at 5.6 kbit/s, requires half the bandwidth of the Full Rate codec, network capacity for voice traffic is doubled, at the expense of audio quality
  - The coding scheme is called Vector Sum Excited Linear Prediction (VSELP) coding

GSM-FR coding

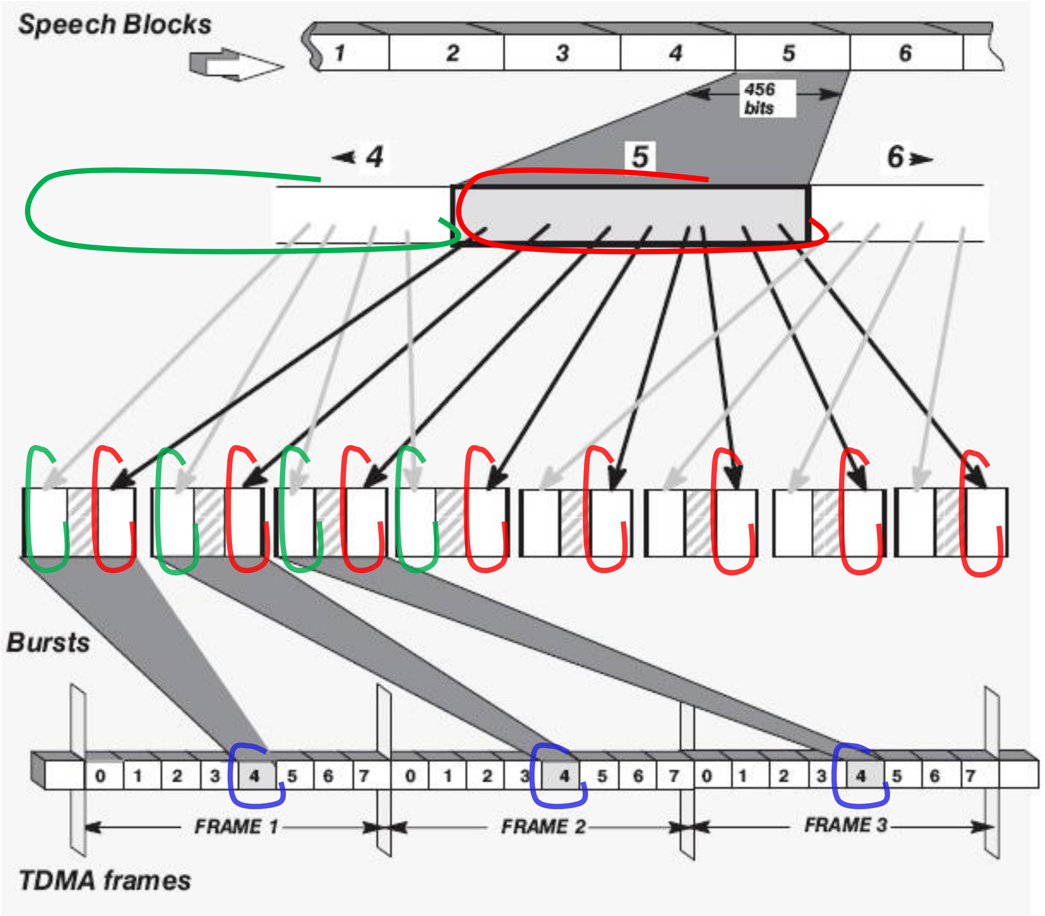


Speech data mapping into the frame (with interleaving)

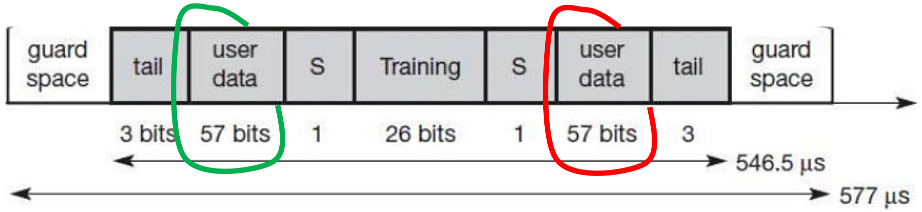
260 bits / 20 ms from codec
Importance classes of bits



Error protection for speech signals in GSM



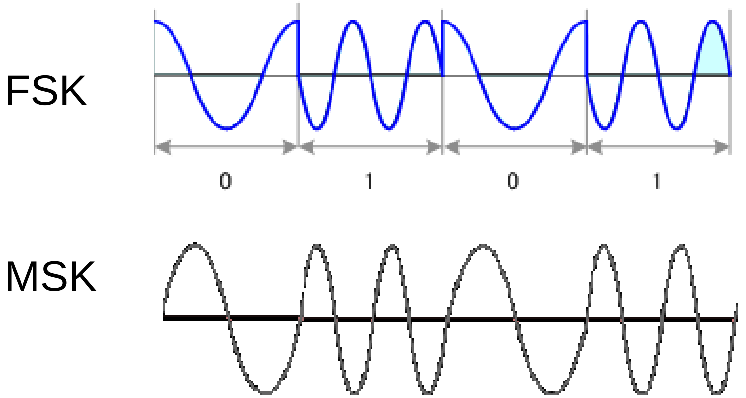
- 456 bit block (per 20 msec) is mapped into 8 frames
- 456 / 8 = 57 bits per slot

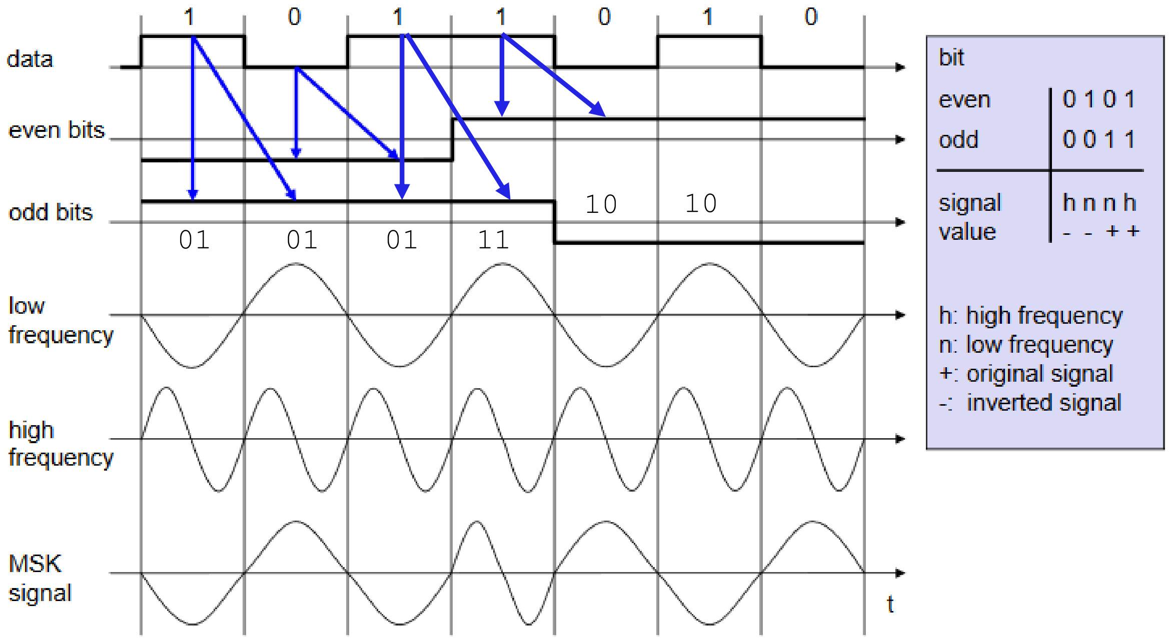


- Coded data blocks are interleaved due to the reason that transmission erros tends to occur in bursts as the mobile phone moves
- Single speech channel occupies a single slot in frame

GSM modulation

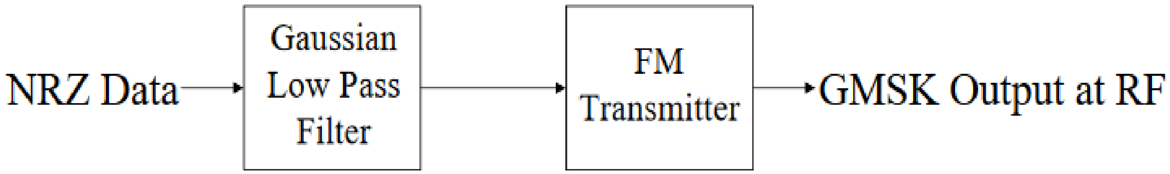
- **FSK** (Frequency Shift Keying) - digital information is transmitted by changing the frequency of a carrier signal
  - discontinuous phase changes, generates unwanted spectrum
- **MSK** (Minimum Shift Keying) modulation is based on FSK but having <u>no phase discontinuities</u> because the <u>frequency changes occur at the carrier zero crossing points</u>
  1. Bit stream is separated into 2 parallel bit streams - even and odd bits, the duration of each bit is doubled
  2. The frequency of one carrier (data rate) is twice the frequency of the other (half of data rate)
  3. Depending on the bit values (even, odd) the higher or lower frequency, original or inverted is chosen

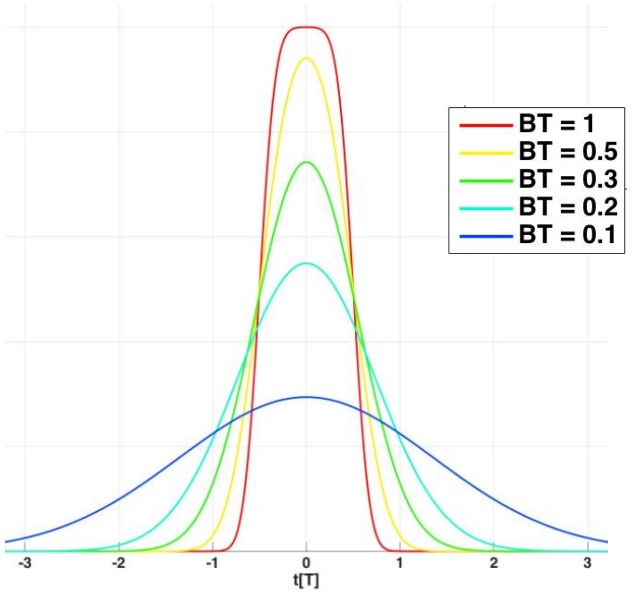




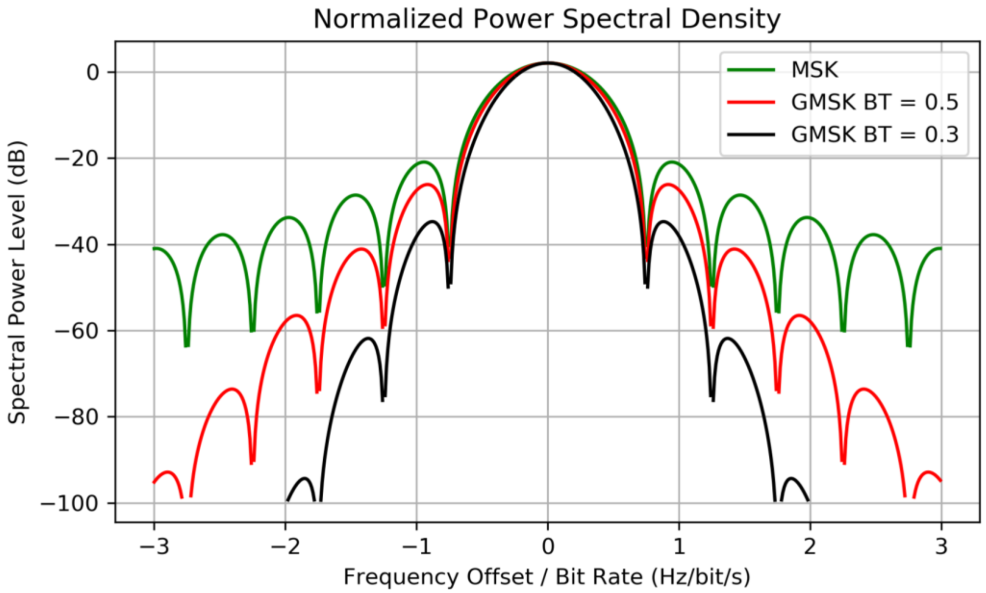
GSM modulation

- GSM uses **GMSK** (Gaussian Minimum-Shift Keying) is similar to standard MSK; however, the digital data stream is first shaped with a Gaussian filter ("smoothing" signal)





- **BT** – Bandwidth-Time factor, symbol spread factor over "n" bits time period duration
  - BT=1 the symbol spreads over one bit period duration
  - BT=0.3 the spread is over approximately 3 bit periods



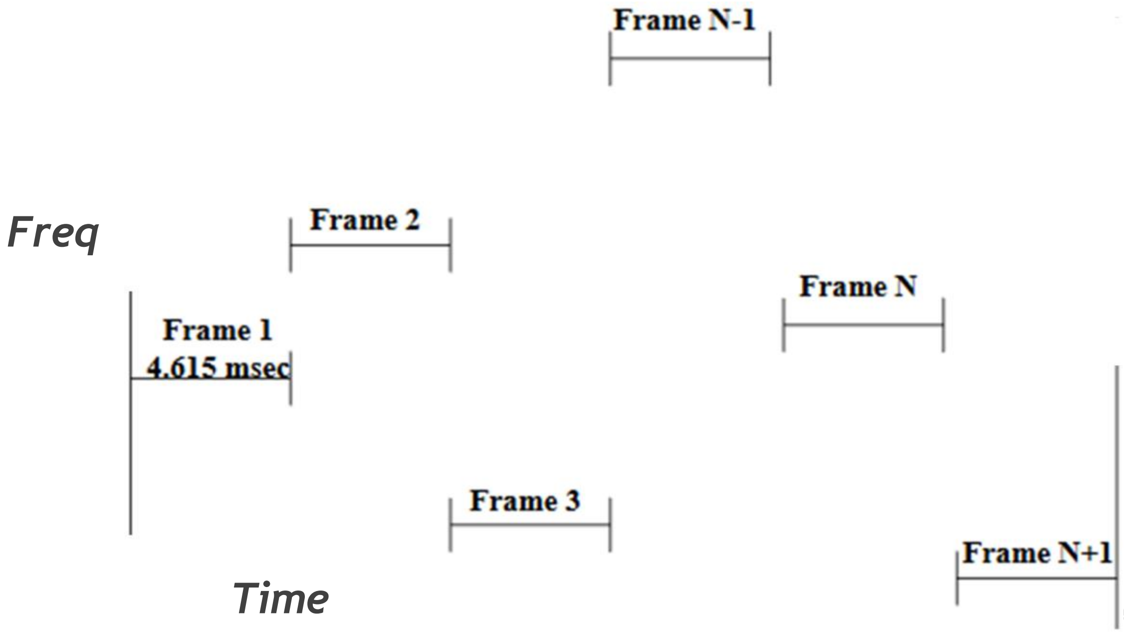
- Why GMSK and not BPSK or QPSK?
  - The side-lobes of MSK are lower (−23 dB) than in both BPSK and QPSK cases (−10 dB)

- GSM uses BT=0.3 for GMSK
  - More efficient spectrum use

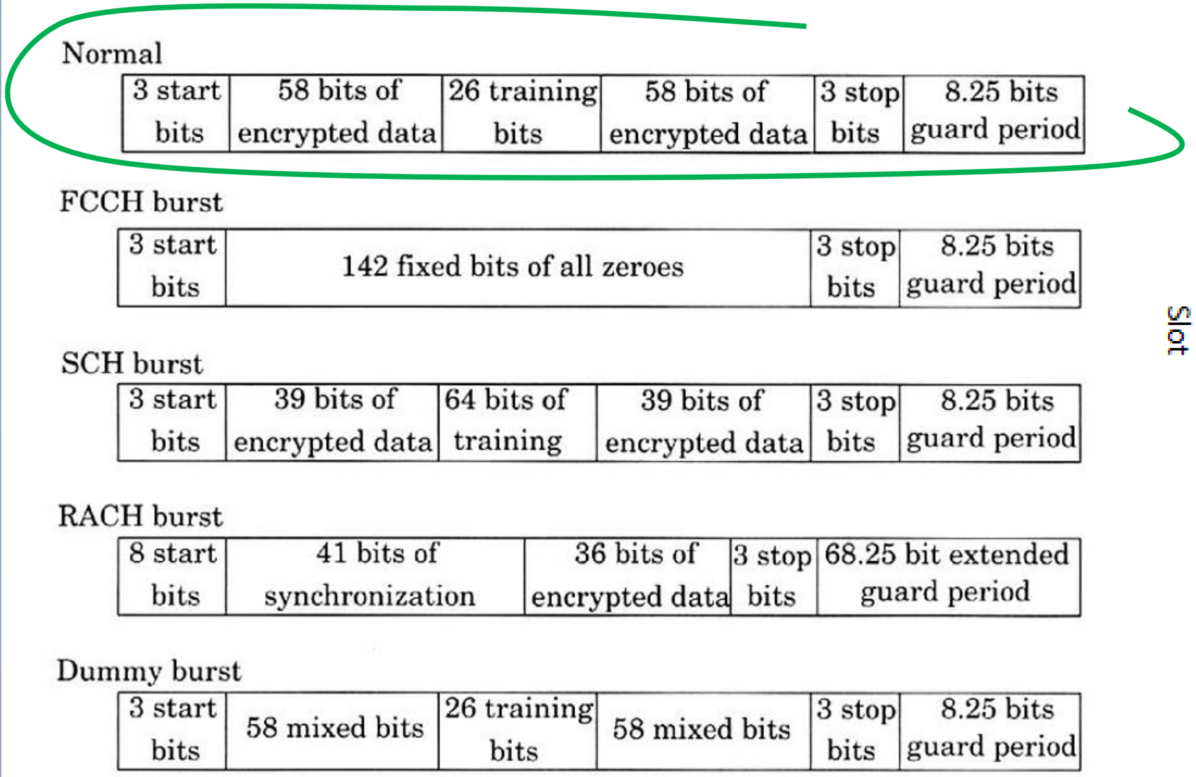
Frequency hopping

- Technique of improving the signal to noise ratio in a link by adding frequency diversity.
- The BTS commands MS to activate frequency hopping as MS moves toward the edge of a cell or into an area of high interference.
- When frequency hopping is activated in MS, BTS assigns to MS a set of RF channels, rather than a single RF channel. A frequency hopping algorithm is also assigned.

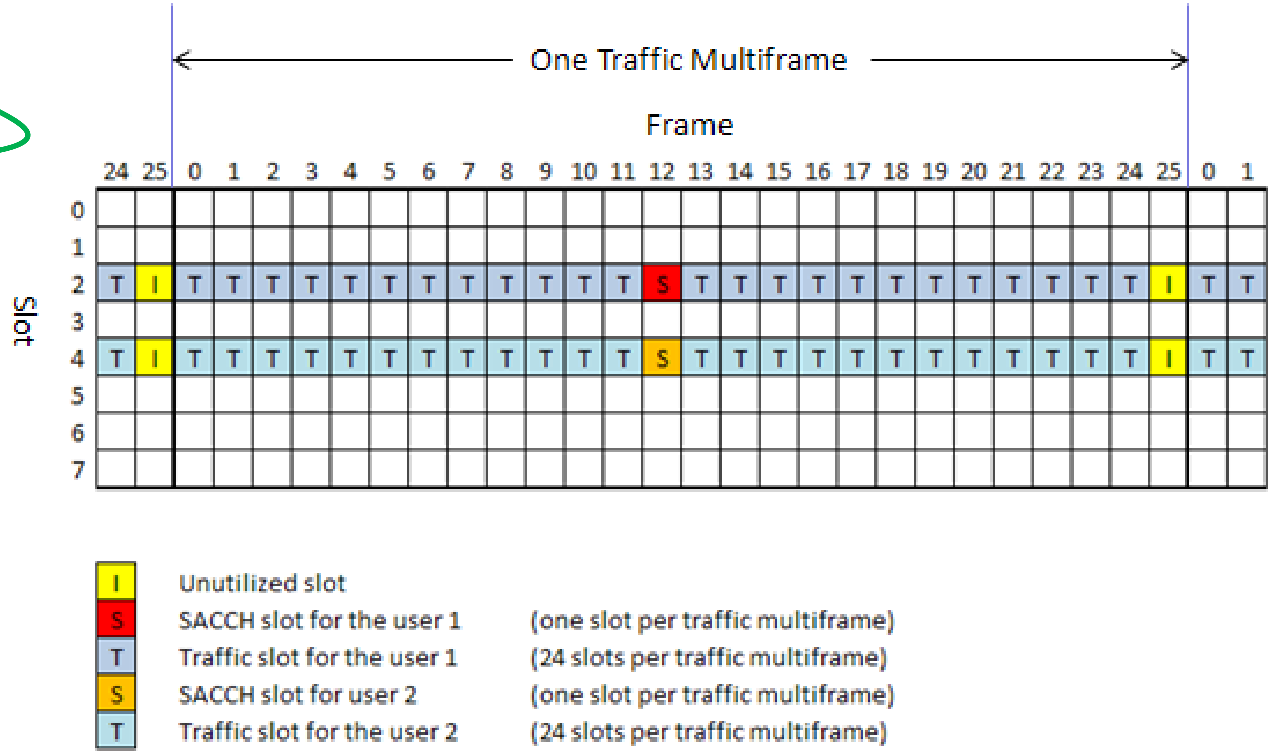
- The advantages that frequency hopping offers are:
  - Improved voice quality and prevention of dropped calls in GSM
  - Improved data throughput in GPRS and EGPRS



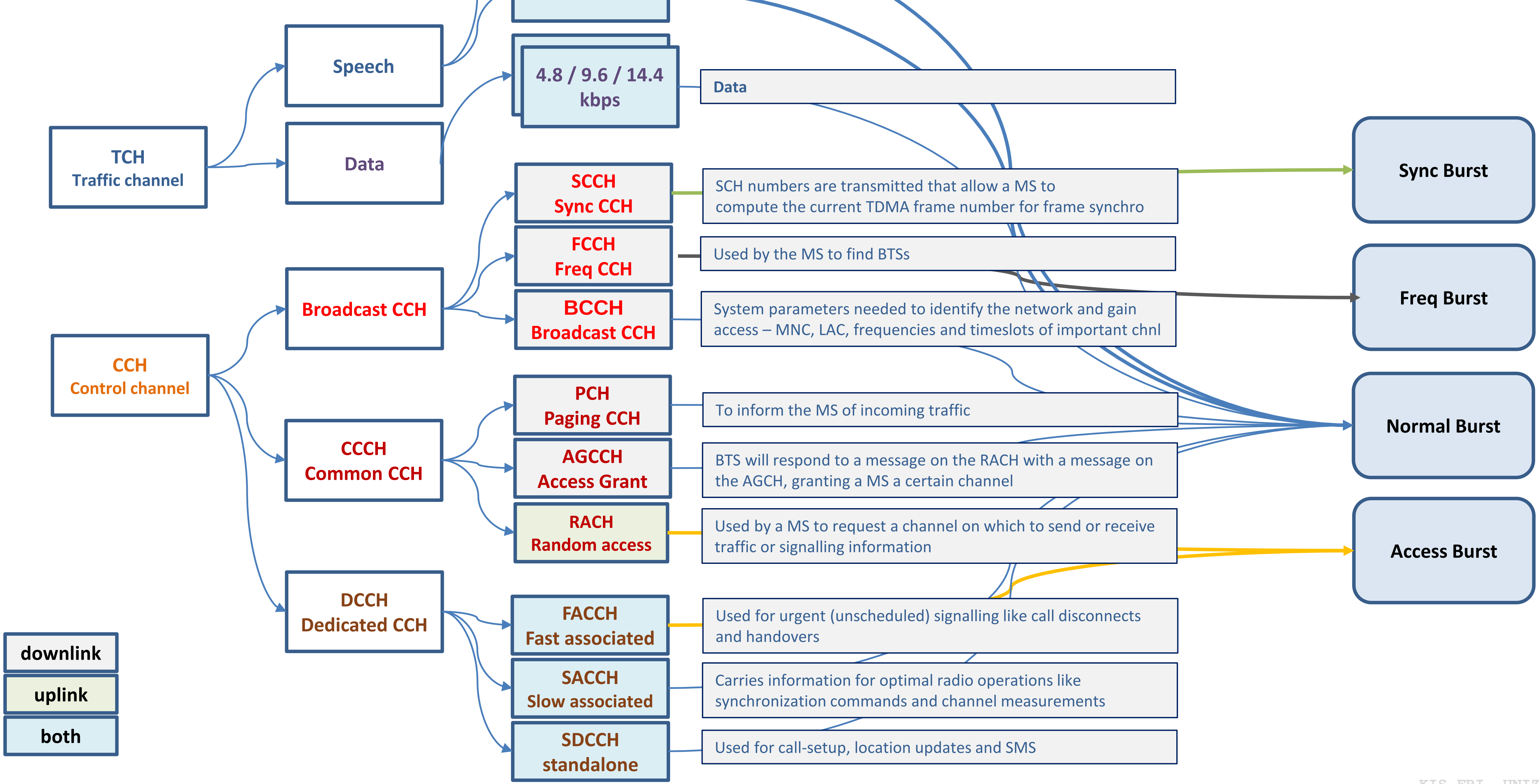
Major GSM frame bursts – data and control



Time slot formats



Radio Channels types



GSM Protocol Stack

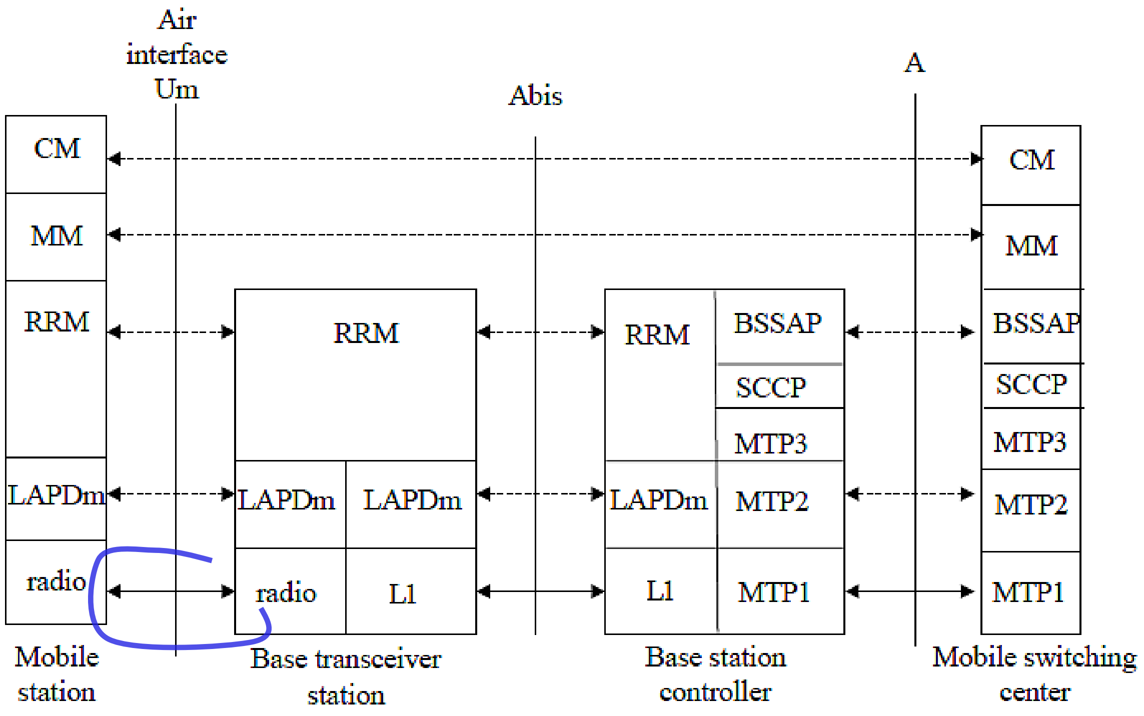
Physical layer

- Physical air interface (Um interface) already discussed, see previous slides
- Other interfaces might be MW link, Ethernet, SDH, other
- MTP Level 1 (Message Transfer Part), physical layer between BSC and MSC, part of SS7 (Signalling System 7) signalling used in PSTN

Link layer

- LAPDm (Link Access Protocol on D channel) link layer protocol, derived from HDLC, only for signalling channels (not speech), provides error correction and flow control
- MTP Level 2 - link layer protocol

No IP packet switching at all !



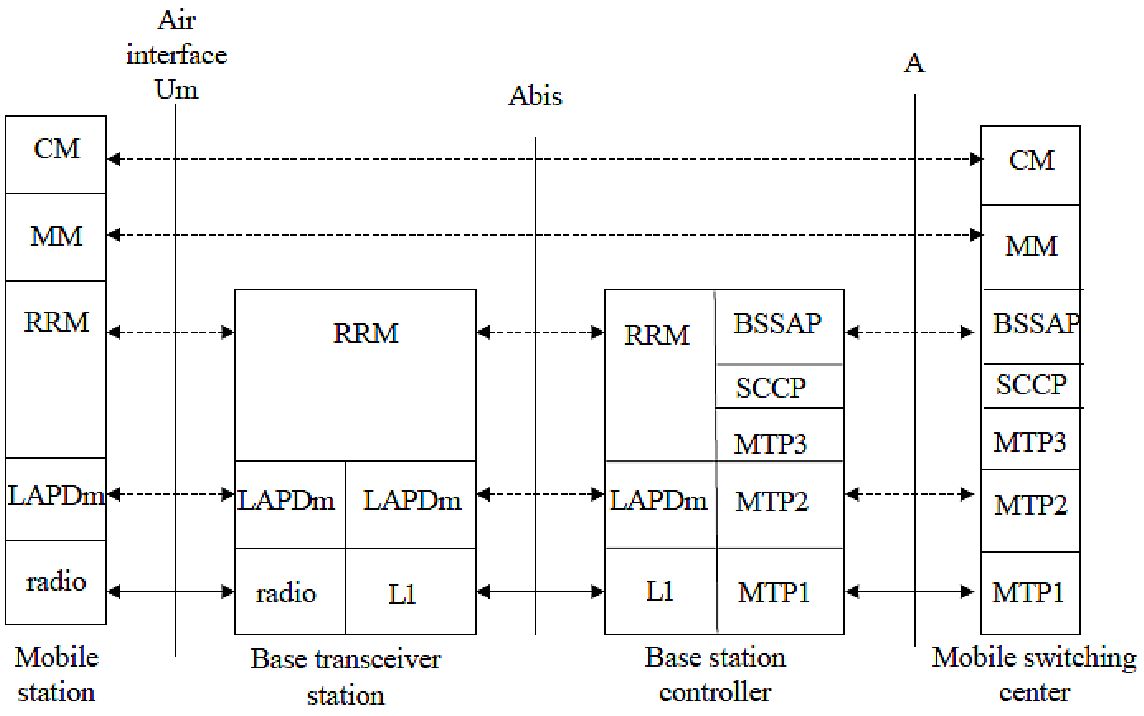
GSM Protocol Stack

Network layer

- RRM (Radio Resource Management) – establishment, maintenance and termination of radio channel connections
- SCCP (Signalling Connection Control Part) - extended routing, flow control, segmentation, connection-orientation, and error correction facilities in SS7 telecommunications networks. SCCP relies on the services of MTP for basic routing and error detection
- BSSAP (BSS Application Part) - provides resource management and handover control between MSC and BSS and is used to transfer MM and CM messages
- MTP Level 3 – provides network functional level for signalling messages

Upper layers

- CM (Call management) – establishment, maintenance and termination of the call
- MM (Mobility Management) – registration, authentication and location tracking



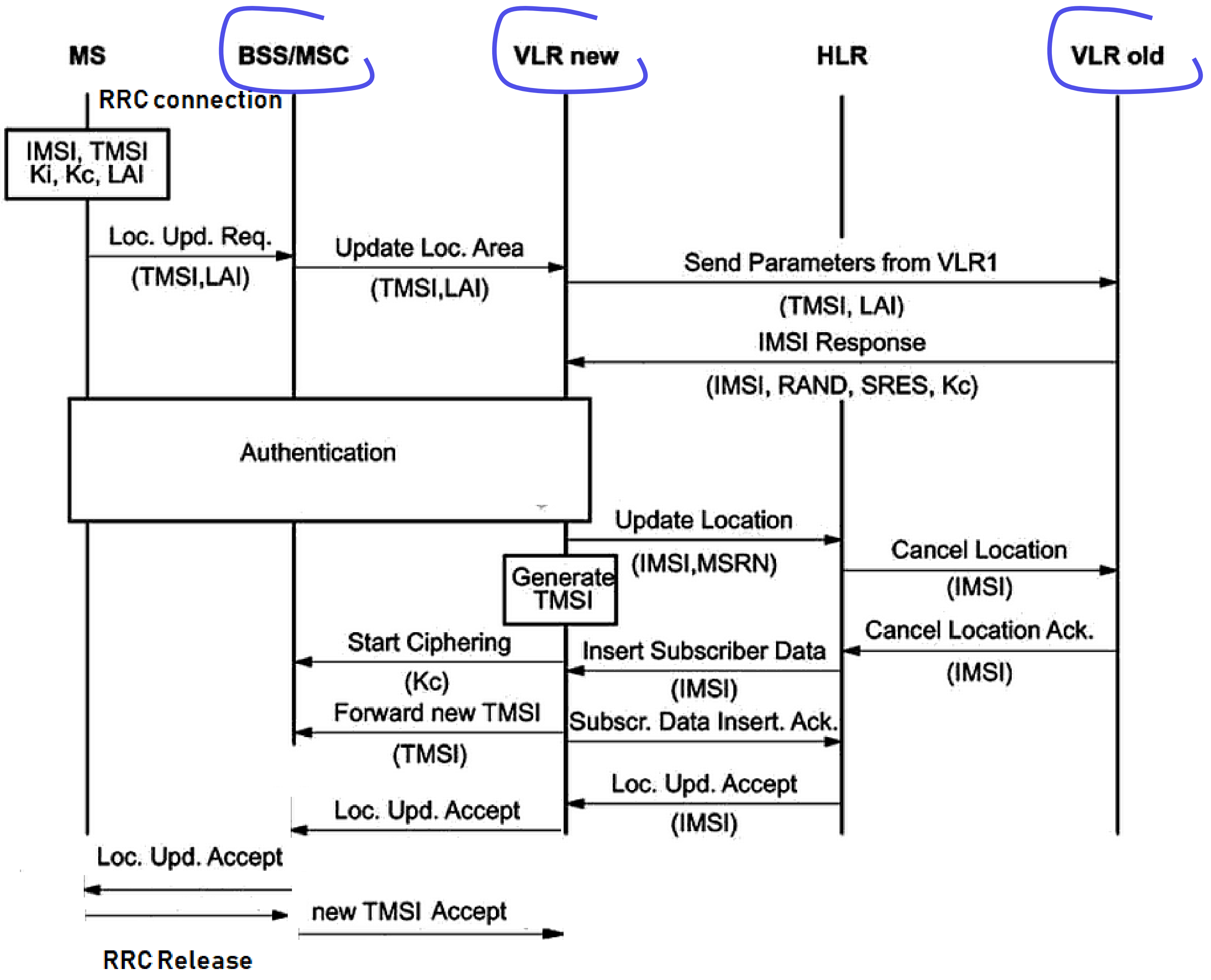
GSM MM - Mobility Management

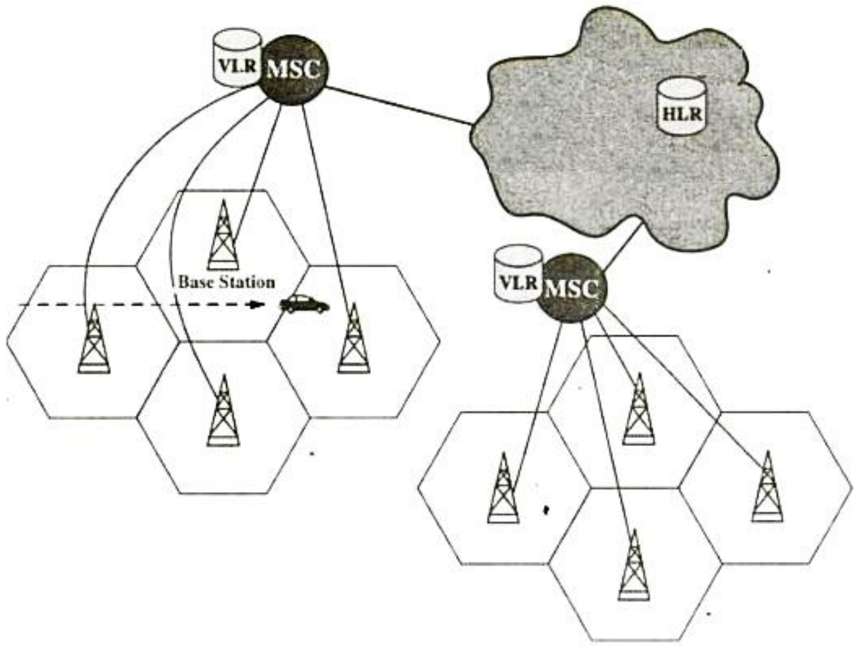
1. MM sublayer provides basic mobility service to upper sublayer CM (Call Management)
2. Dynamic subscriber data management at MSC/VLR
3. Provides subscriber’s authentication

- **Tracks location of MSes for incoming calls and SMSes** (MS in IDLE state)
  a. LAI periodically broadcasted by each cell, MS listens to it, if different then performs a Location Update with VLR
  b. Two level hierarchy of the database, HLR points to VLR where mobile is located, VLR points to LA where mobile is located
     1. IMSI Attach / Registration
     2. Normal Location Update
        - Old and new LA in the same VLR area, location updated in VLR
        - Old and new LA in different VLR area, old VLR removes data, HLR update, new VLR registers MS
     3. Periodic Location Update – no LA change, typically several hours due to the signalling traffic optimization

- **Call in progress mobility** (MS in call CONNECTED state) - hand-off the call (p2p connection) from one BTS to another BTS
  a. Intra-cell hand-off: Handoff between sectors of the same cell
  b. Intra-BSS hand-off : if old and new BTSs are attached to the same BSC, MSC is not involved
  c. Intra-MSC hand-off : if old and new BTSs are attached to different BSCs but within same MSC
  d. Inter-MSC hand-off : if MSCs are changed

GSM – MM
Inter-MSC/VLR Location Update example (IDLE state)

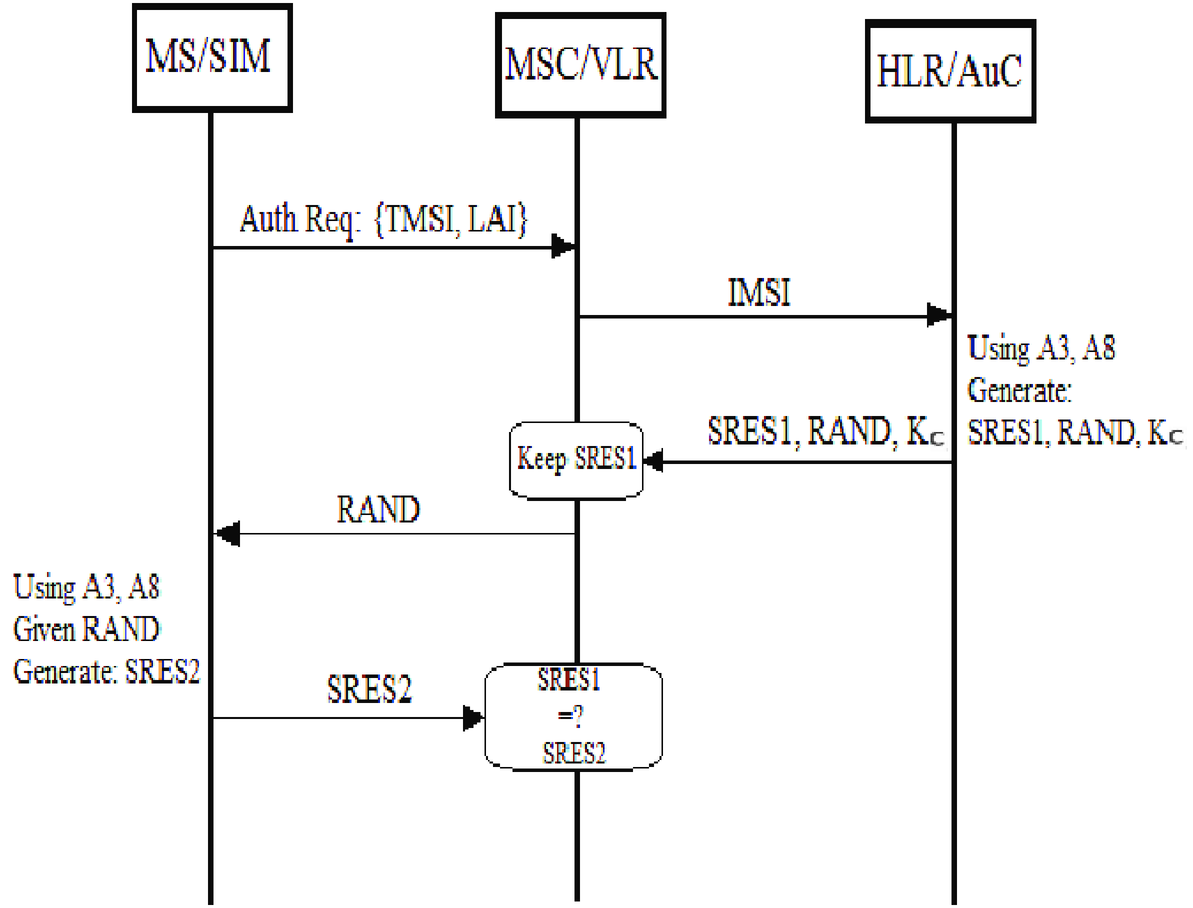




GSM MM - authentication and encryption

1. Authentication triplet (RAND, SRES, Kc) used to check the validity of a mobile subscriber
2. GSM encryption standards for voice frames
   - A5/0 no encryption, A5/1, A5/2, A5/3

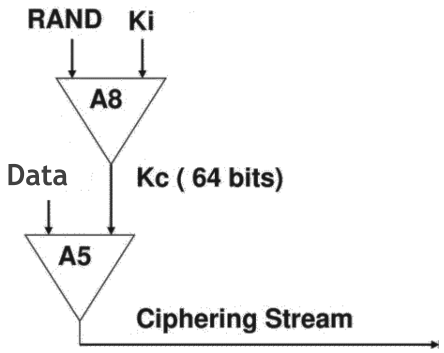
- When a new GSM subscriber turns on his phone for the first time
- Its IMSI is transmitted to AuC on the network.
- After which, a TMSI is assigned to the subscriber, along with authentication parameters
- After this point, the IMSI is very rarely transmitted, unless it is necessary



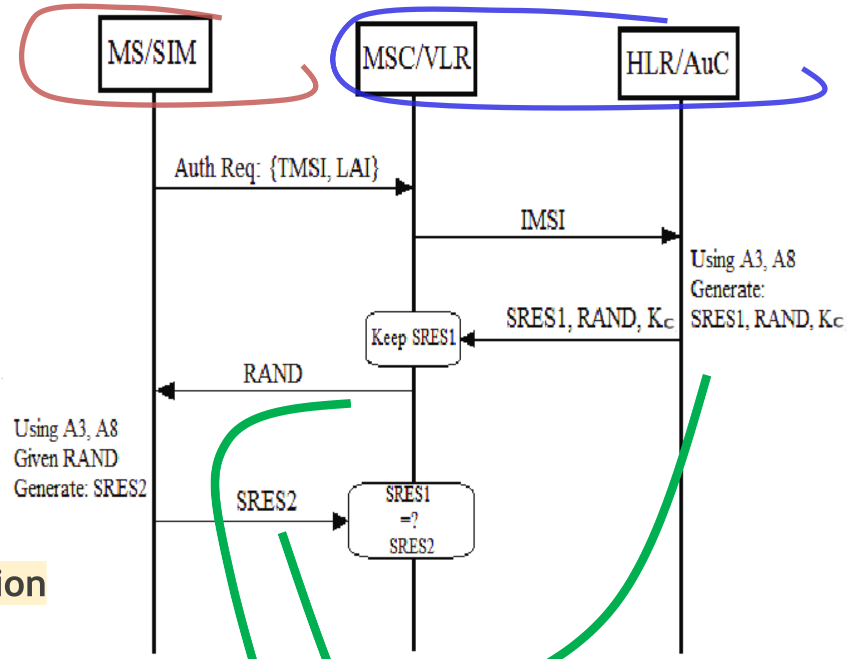
GSM MM - authentication and encryption

- **Ki** (128 bits) Identification Key - never transmitted over the network, stored in SIM and HLR
- **Kc** (64 bits) Ciphering Key - used to encrypt data over radio interface
- **RAND** (128 bits) Random number, sent as a cleartext
- **SRES** (32 bits) Signed RESponse

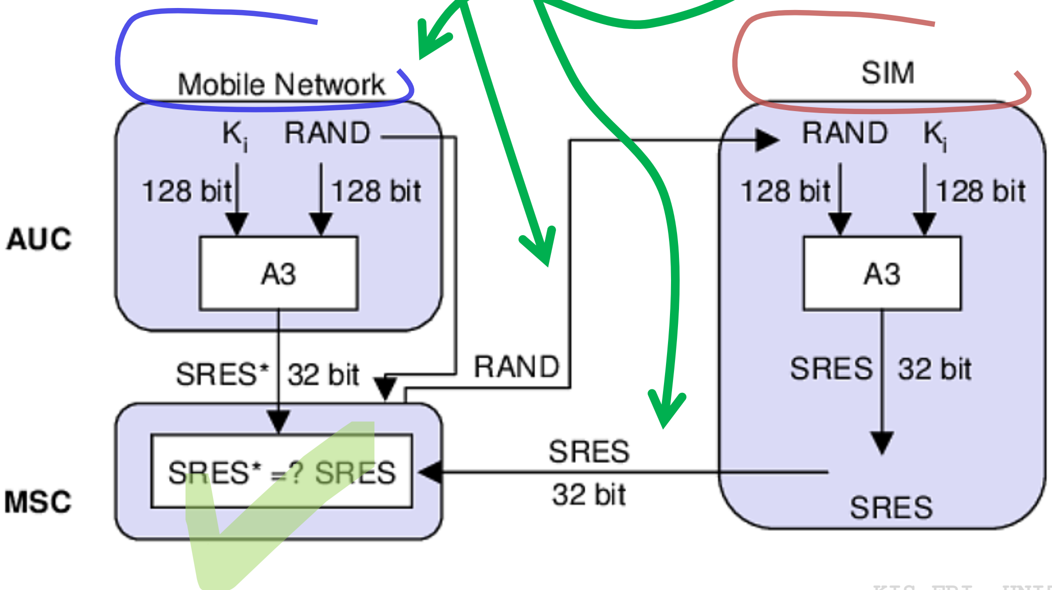
- A3 Authentication algorithm
  - RAND + Ki -> output is SRES
- A5 Ciphering algorithm
  - Data + Kc -> encrypted data
- A8 Authentication algorithm
  - RAND + Ki -> output is Kc



Encryption



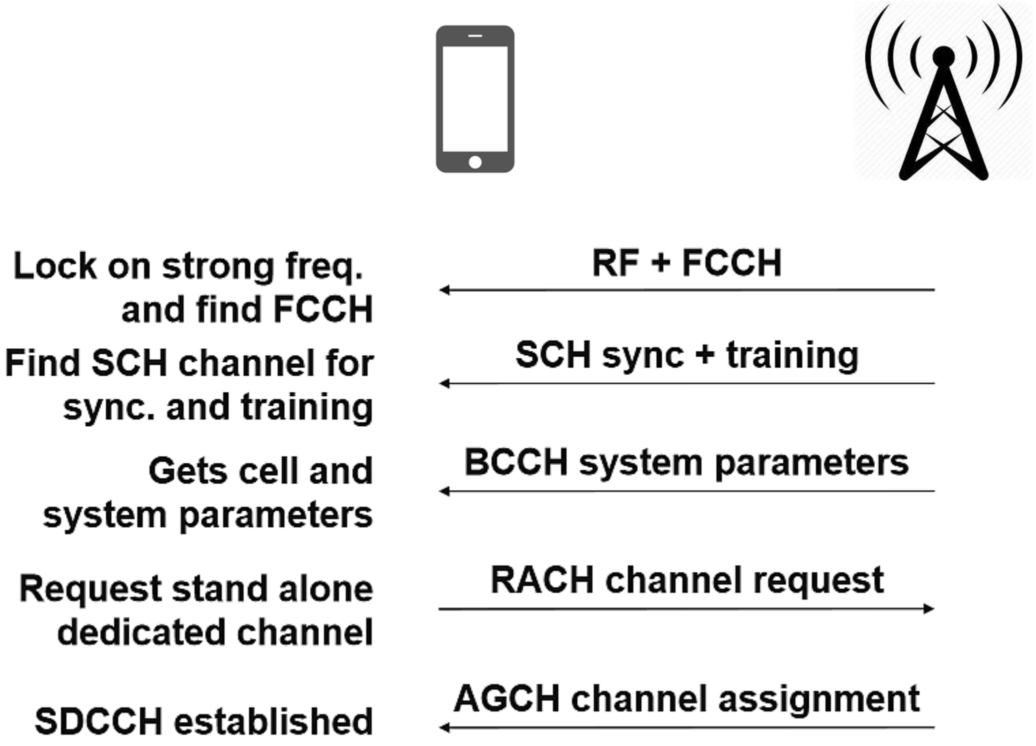
Authentication



GSM CM - Call Management

A. Registration

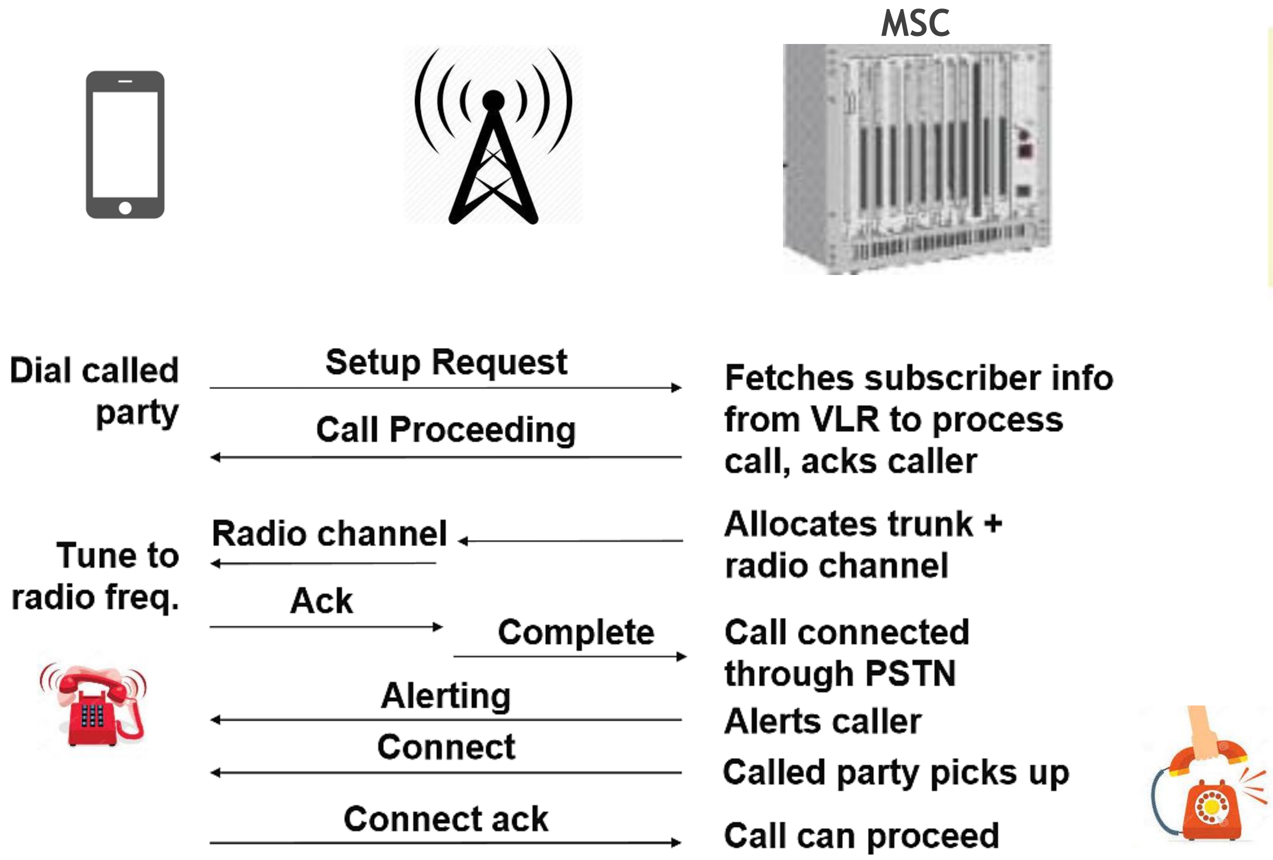
- Upon powering up, the MS scans control channels (CCH) and locks onto the frequency channel with strongest signal
- Searches for FCCH (Frequency CCH) on RF carrier, finds SCCH to synch up
- After synchronization the MS decodes BCCH (Broadcast CCH) with network system’s info – decides whether to update location / register or not

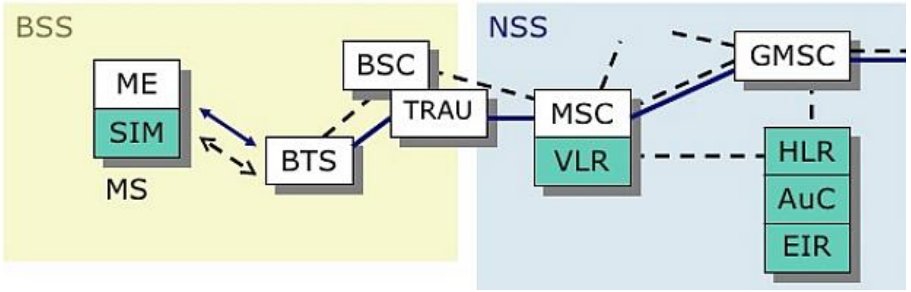


- RACH request used by a MS to request a channel on which to send or receive traffic or signalling information. Requested over common CCH
- SDCCH (standalone dedicated CCH) Used for call-setup, location updates and SMS
- BTS will respond to a message on the RACH with a message on the AGCH, granting a MS a certain channel

GSM CM - Call Management

A. **MOC -** Mobile originating call





--- Signaling

__ Circuit Switched Connection

TRAU (Transcoding and Rate Adaptation Unit) – 13kbps transcoded to PCM signal 64kbps

Calling party

Called party

Selected GSM Features

DTX - Discontinuous Transmission

- If no speech detected NO information is transmitted
- Saves battery power in mobile
- Reduces co-channel and adjacent channel interference
- Comfort noises periodically played back if long silence period

Power control

- Both mobile and BTS regulate power (increase and decrease) by evaluating RX signal over air
- Conserves battery power in mobile
- Reduces interference

MAHO - Mobile Assisted Hand-off

- Process used in GSM cellular networks where a mobile phone assists/helps the cellular base station to transfer a call to another base station
- Mobile takes measurements of signals strength of radio channels in adjacent cells, reports it to BSC and MSC
- Via SACCH
- MSC decides on handoff based on MS measurements of Frame Error Rate, signal levels of neighbour carriers, distance from BS calculated from TA and interference level measured in idle time slots

Sleep Mode or **DRX** (Discontinuous Reception)

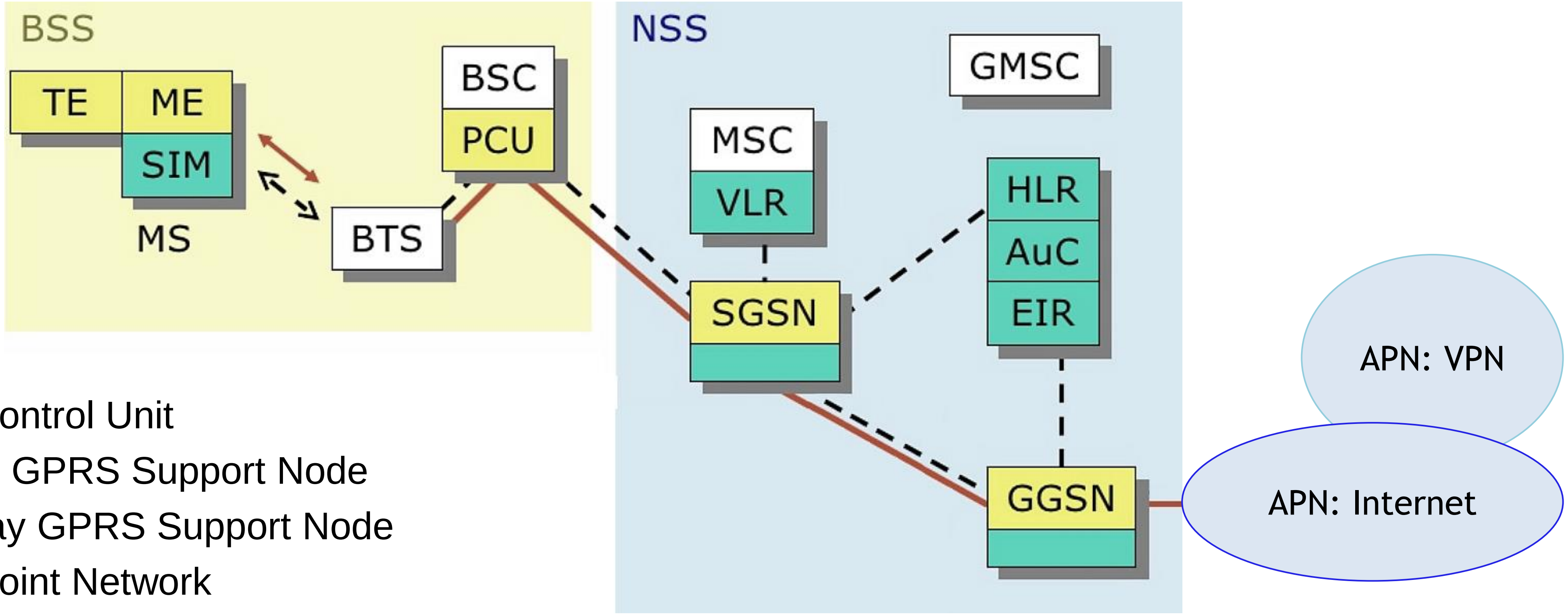
- Handset (MS) once registered with network will be assigned a sleep mode level
- Checks paging channel for page/SMS periodically
- DRX feature depends on the network configuration

2G / GSM
Global System for Mobile communication

2.5 GPRS

2.5G - GPRS (General Packet Radio Service)

- Introduced in 2000 as an extension to GSM (2.5G), enables packet mode communication
- Resources are reserved only when needed and charged accordingly
- Flexible channel allocation
- Data rates 14.4 – 160 kbps (GSM up to 9.6kbps only)



- PCU - Packet Control Unit
- SGSN - Serving GPRS Support Node
- GGSN - Gateway GPRS Support Node
- APN - Access Point Network

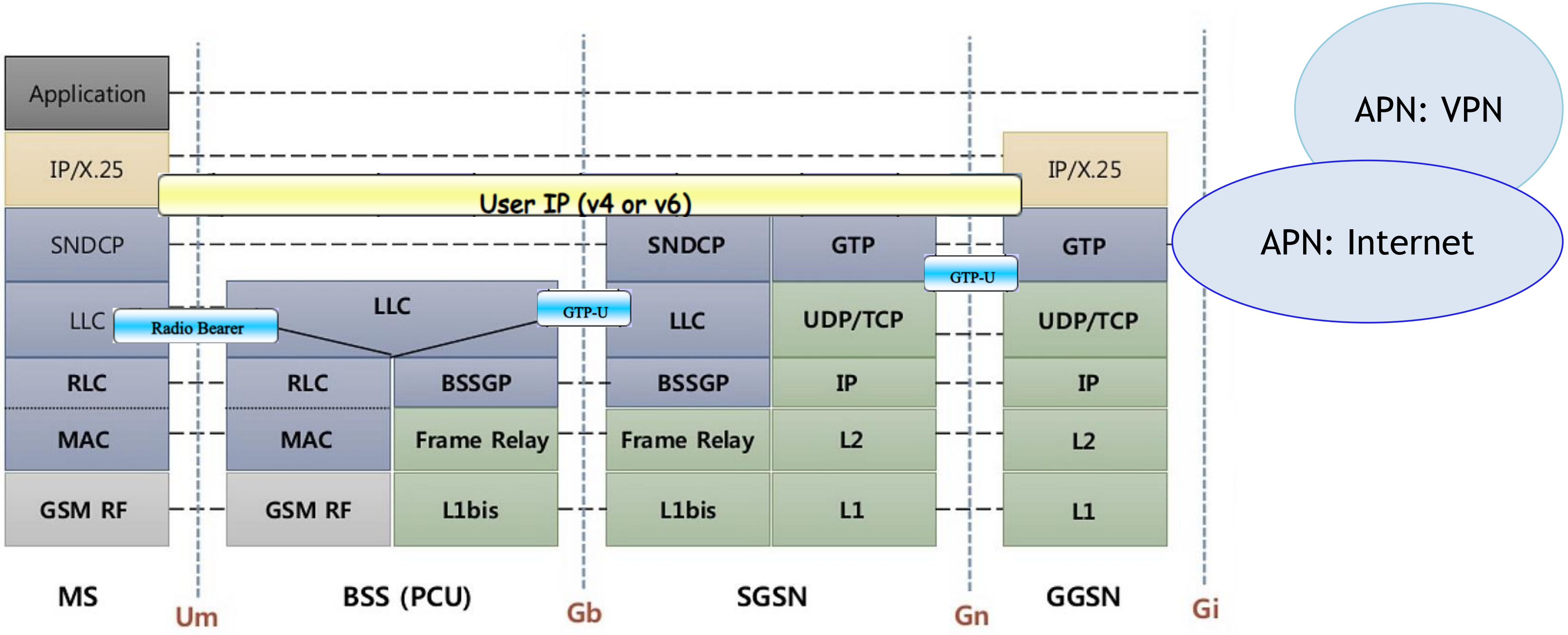
2.5G - GPRS - new components

- **PCU** (Packet Control Unit) provides a physical and logical <u>data</u> interface to the BSS for packet data traffic, packet segmentation & reassembly, buffering, retransmission, radio channel management

- **SGSN** (Serving GPRS Support Node) stores subscriber data and is responsible for control plane:
  - authentication and registration of GPRS capable MSes in the network
  - mobility management
  - Packet routing and stores not-acknowledged packets in case of cell change
  - collecting information on charging – flat, per packets/data, etc. ; **CDR** (Call Data Record)

- **GGSN** (Gateway GPRS Support Node) acts as an interface and a <u>router to external networks</u>, also stores subscriber data for data active subscribers
  - the anchor point that enables the mobility, routes packets toward right SGSN
  - allocates resources for connections, IP, etc.
  - also collects charging info and sends CDRs

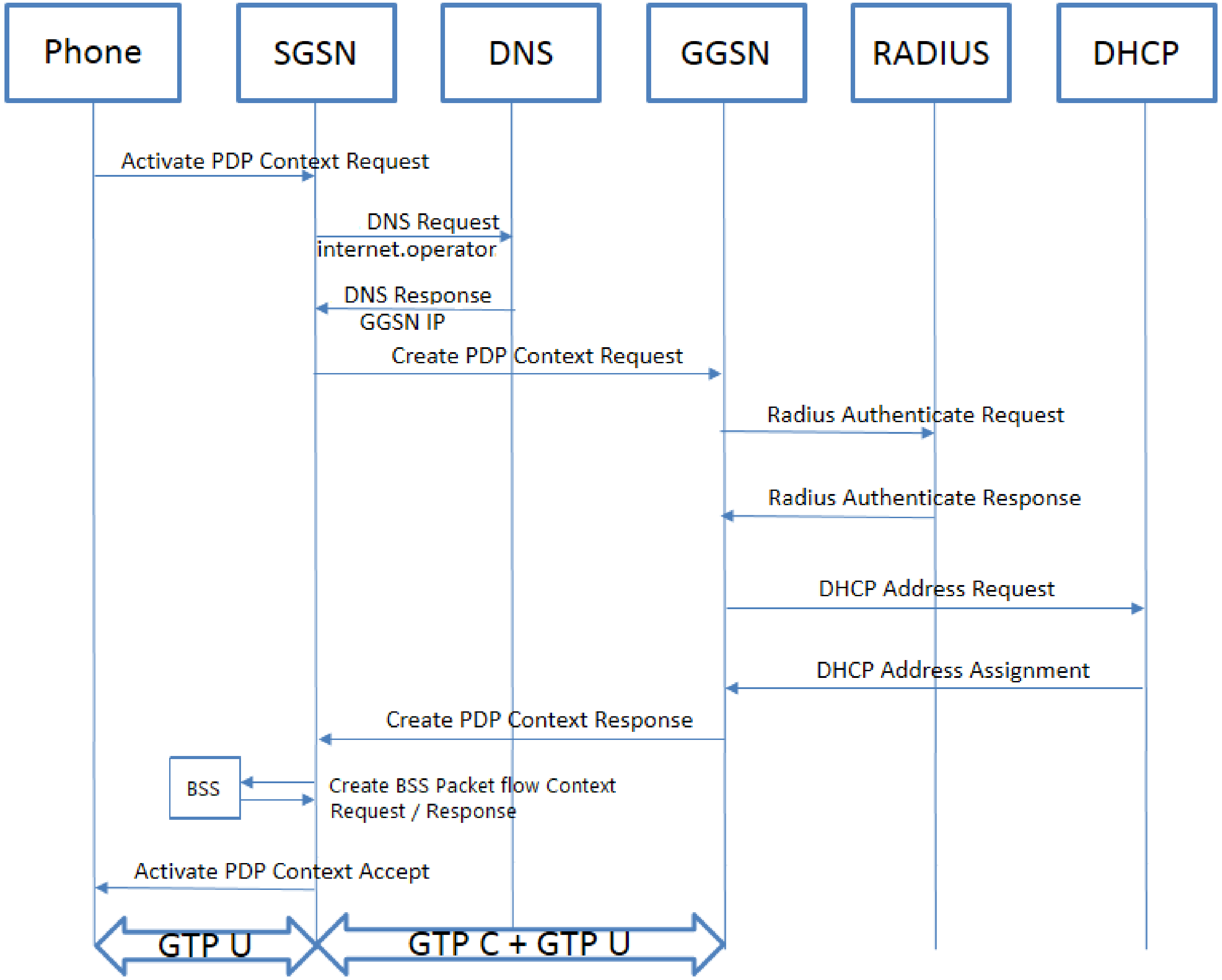
2.5G - GPRS - new components



- **PDP context** (Packet Data Protocol) represents a connection/tunnel between MS and the TEID (“end address”) on GGSN
- **GTP** (GPRS Tunnelling Protocol)
- **GTP-U** for data between MS, SGSN and GGSN
- **GTP-C** for signalling between SGSN and GGSN, session management
- **TEID** (Tunnel Endpoint ID)
- **APN** (Access Point Network) – during the process of PDP activation, MS transmits the name of the network / VPN it wants to be connected, APN is a logical name, used on GGSN for VRF identification

- **SNDCP** Sub Network Dependent Convergence Protocol
- **BSSGP** Base Station Subsystem GPRS Protocol
- **RLC** Radio Link Control
- **LLC** Logical Link Control

2.5G - GPRS - simplified PDP context activation




```
> Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface unknown, id 0
> Ethernet II, Src: VMware_e3:c6:4d (00:0c:29:e3:c6:4d), Dst: VMware_da:d1:de (00:0c:29:da:d1:de)
> Internet Protocol Version 4, Src: 192.168.40.179, Dst: 192.168.40.178
> User Datagram Protocol, Src Port: 2152, Dst Port: 2152
v GPRS Tunneling Protocol
  v Flags: 0x32
      001. .... = Version: GTP release 99 version (1)
      ...1 .... = Protocol type: GTP (1)
      .... 0... = Reserved: 0
      .... .0.. = Is Next Extension Header present?: No
      .... ..1. = Is Sequence Number present?: Yes
      .... ...0 = Is N-PDU number present?: No
    Message Type: T-PDU (0xff)
    Length: 88
    TEID: 0x00000001 (1)
    Sequence number: 0x28db (10459)
> Internet Protocol Version 4, Src: 202.11.40.158, Dst: 192.168.40.178
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xbee7 [correct]
    [Checksum Status: Good]
    Identifier (BE): 0 (0x0000)
    Identifier (LE): 0 (0x0000)
    Sequence number (BE): 10363 (0x287b)
    Sequence number (LE): 31528 (0x7b28)
    [Response frame: 2]
    Timestamp from icmp data: Dec  9, 2009 22:05:08.867828000 Central Europe Standard Time
    [Timestamp from icmp data (relative): 49706.573683000 seconds]
  > Data (48 bytes)
```

2.5G - GPRS - air interface timeslot allocation

- GPRS uses the existing GSM resources, the same TDMA frame
- GPRS air interface can dynamically allocate resources / timeslots
- New “packet” set of logical channels defined
- Flexible channel allocation
  - 1 to 8 timeslots
  - Up / down link channels reserved separately
- Timeslot (0.577msec) can carry ~150bits -> raw ~34 kbps per timeslot
  - or ~271 kbps per radio channel
  - 4 levels of channel GMSK Coding Schemes (CS-1 to CS-4), if radio quality is bad then CS-1 is applied with highest level of error correction
  - following data rates in [kbps] can be achieved (with MAC and RLC overhead):

Scheme	Coding Rate	Paylaod	Max. Throughput
CS1	1/2	181	9.05
CS2	2/3	268	13.4
CS3	3/4	312	15.6
CS4	1	428	21.4

Multislot Class	Downlink Slots	Uplink Slots	Active Slots
4	3	1	4
5	2	2	4
6	3	2	4
7	3	3	4
8	4	1	5
9	3	2	5
10	4	2	5
11	4	3	5
12	4	4	5

- Depending upon the network capacity as well as the number of active users in the cell. Depending on amount of data the network will configure 3+2 or 4+1
- Shared by multiple users

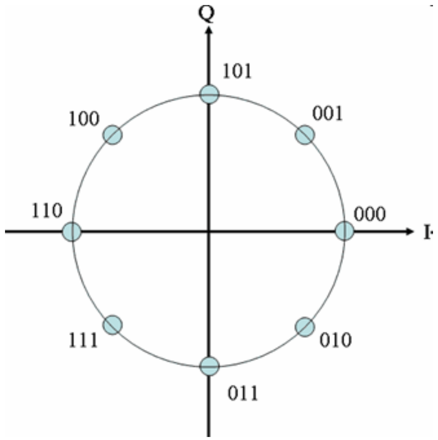
Technology	Download (kbit/s)	Upload (kbit/s)	TDMA timeslots allocated (DL+UL)
GPRS	85.6	21.4 (Class 8 & 10 and CS-4)	4+1
GPRS	64.2	42.8 (Class 10 and CS-4)	3+2

2G / GSM
Global System for Mobile communication

2.75 EDGE

2.75G - EDGE

- **EDGE** – (Enhanced Data Rates for GSM Evolution), also called as Enhanced GPRS
- EDGE is a superset to GPRS and can function on any network with GPRS deployed on it
- **GERAN** (GSM/EDGE Radio Access Network) enabled the evolution of GSM towards next generation networks, included introducing support for generic real-time services as well as internal interfacing to an all-IP
- New modulation technique 8PSK added – each symbol represents 3 bits instead of one
- Improved link adaptation mechanism
- MCS-9 provides little error correction



0 0 0	0
0 0 1	+π / 4
0 1 0	+3π / 4
0 1 1	+2π / 4
1 0 0	−π / 4
1 0 1	−2π / 4
1 1 0	+π
1 1 1	−3π / 4

Multislot Class	Downlink /kbits	Uplink/kbits	DL TS	UL TS	Active TS
1	59.2	59.2	1	1	2
2	118.4	59.2	2	1	3
3	118.4	118.4	2	2	3
4	177.6	59.2	3	1	4
5	118.4	118.4	2	2	4
6	177.6	118.4	3	2	4
7	177.6	177.6	3	3	4
8	236.8	59.2	4	1	5
9	177.6	118.4	3	2	5
10	236.8	118.4	4	2	5
11	236.8	177.6	4	3	5
12	236.8	236.8	4	4	5
30	296	59.2	5	1	6
31	296	118.4	5	2	6
32	296	177.6	5	3	6
33	296	236.8	5	4	6
34	296	296	5	5	6

Scheme (MCS)	(kbit/s/slot)	w/o overhead (kbit/s/slot)	Modulation
MCS-1	9.20	8.00	GMSK
MCS-2	11.60	10.40	GMSK
MCS-3	15.20	14.80	GMSK
MCS-4	18.00	16.80	GMSK
MCS-5	22.80	21.60	8PSK
MCS-6	30.00	28.80	8PSK
MCS-7	45.20	44.00	8PSK
MCS-8	54.80	53.60	8PSK
MCS-9	59.60	58.40	8PSK

GPRS	85.6	21.4 (Class 8 & 10 and CS-4)	4+1
GPRS	64.2	42.8 (Class 10 and CS-4)	3+2
EGPRS (EDGE)	236.8	59.2 (Class 8, 10 and MCS-9)	4+1
EGPRS (EDGE)	177.6	118.4 (Class 10 and MCS-9)	3+2

Ďakujem za pozornosť.

roman dot kaloc at uniza dot sk

Vytvorené v rámci projektu KEGA 026TUKE-4/2021