University of Antwerp
Faculty of Science

Advanced Wireless & 5G Networks

Prof. Dr. Ir. Michael Peeters — 2023–2024

Topics for today

- **2. Technology baselining/refresher**
  - 2G (continued)
- **3. From 2 to 5G**
  - We jump 2 generations.

Planning

Session	Date	Topic
1	20231006	~~Introduction, history, market, industry, bands, licensed vs. unlicensed, …~~
2	20231013	~~Technology baselining (a.k.a. refreshing what you should have known): 2G, WiFi, …~~
	20231020	~~Cancelled~~
3	20231027	~~Shannon/Friis continued. 2G as a "low-complexity" example~~
4	~~20231110~~	~~L 2G~~
5	20231117	L 3GPP 2G-3G-4G-5G architecture evolution. 5G
6	20231124	L 5G
7	20231201	U IEEE Wifi Network Architecture: 802.11 abgn
8	20231208	U QoS, 802.11 ac,ax and 802.11 ad,ay
9	**20231215 – 3h**	U short range 802.15.4: Zigbee, BLE, and UWB
10.5	**20231222 – 3h**	U Specials: LoRa, Sigfox (perhaps), proprietary, 802.11p
(12)	TBD	Extra: Technology enablers and acronyms you need to be aware of: ADC, FEM, PA, LSA, and other key analog and digital HW blocks, mMIMO, Beam management, 802.11be, AI, 6G, THz and their implications to the network

Your expectations

- How it is possible that, in a world where the number of devices continue to grow, every device can get mobile wireless connectivity with the internet without saturating the network.
- How do 4G/5G/... technologies actually work.
- How do you go about designing a good WiFi network, both on the physical end (devices, access point locations, ...) and on the configuration end.
- What are the technologies behind the current advancement in Cellular and Wi-Fi networks?
- Be able to understand the need for improved and efficient networking technologies, and how to approach solving the drawbacks of current technologies.
- What are the limitations of 5G in regard to the latest trends in Ai, AR/VR and technologies that require very low latency.
- What is next?
- Wifi 6 & 7 – new features.
- Link to cloud.
- How do modern mobile networks work and how have they changed from the previous ones?
- What are the main problems or limitations faced by different types of networks? If it is possible, what are the best ways to solve them?
- How will wireless and mobile networks possibly evolve in the near future?
- ~~To better understand historical challenges in wireless that companies such as blackberry faced.~~
- To better understand wireless technologies such as Zigbee and LoRaWan and their use in IOT projects.
- What role data science could have in this field?
- Can networks be perfected to the point where we don't need to keep on creating new ones or upgrade the existing ones?
- ~~Can governments stop the development of networks?~~
- ~~Will connectivity ever be available underwater or underground?~~
- Security of wireless networks.

2. Baselining

(concepts & toy examples)

What will we cover

- ~~Mobile vs. Wireless vs. Fixed~~
- ~~Shannon's law, to calculate capacity and compare technologies~~
- ~~Friis's equation, to calculate coverage~~
- Cellular and 2G as a reference system

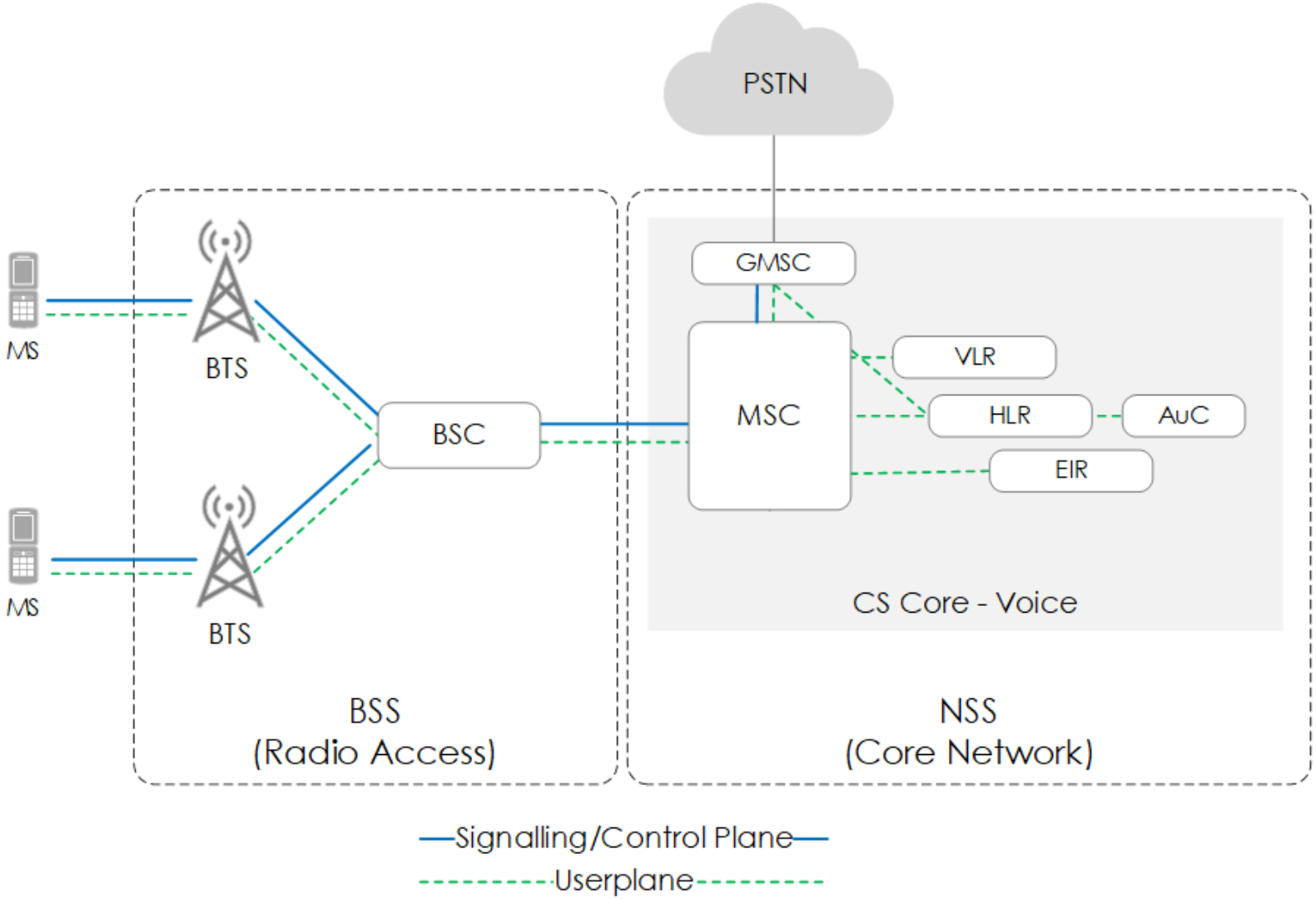
2G system specification

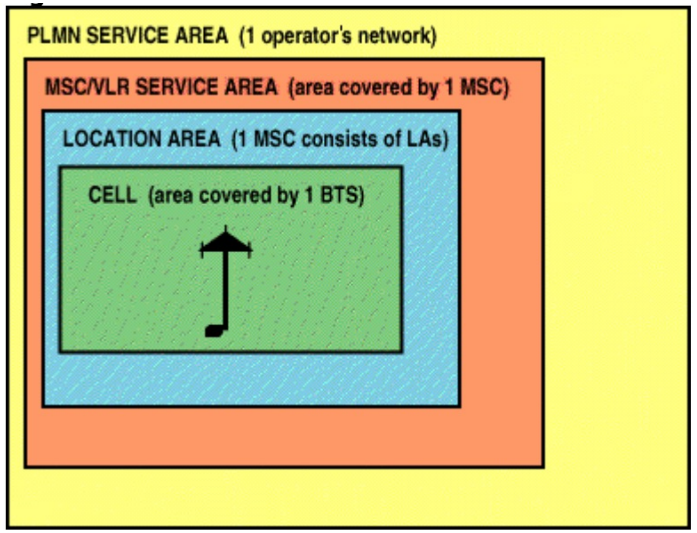
SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms

Important: application influences the PHY most of all (e.g. 5G NSA/SA)

2G architecture





LAI = Location area identity

We’re making a 2G voice call (simplified)

Now, let’s really start from the application

Circuit Switching Vs Packet Switching

Circuit Switching	Packet Switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission

We are going to ignore this (for now)

3

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

2G system specification

SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms

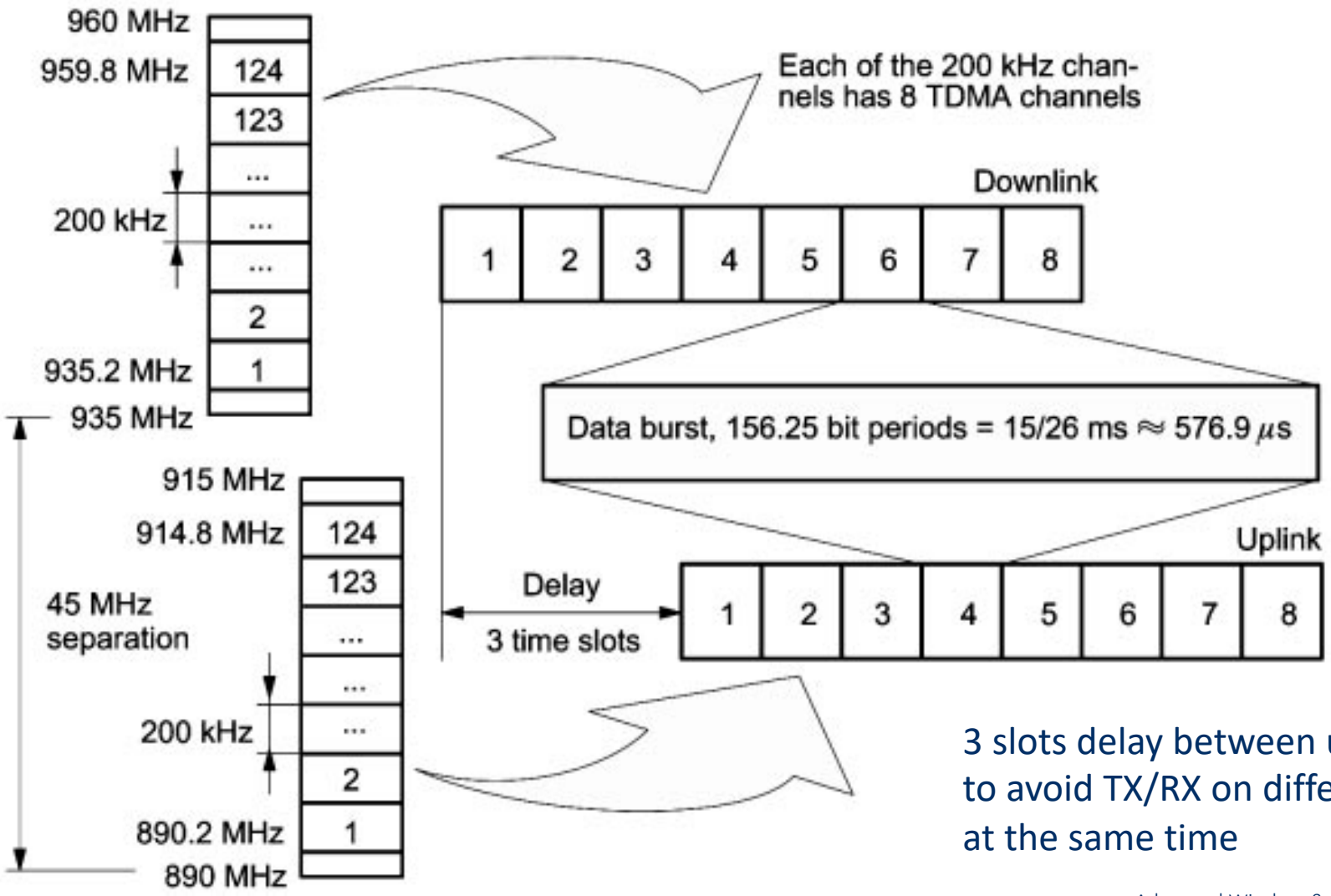
2G Multiple Access Control Scheme

- **Multiple Access in GSM : combination of**
  - Frequency Division Multiple Access (FDMA)
  - Time Division Multiple Access (TDMA)
  - Frequency hopping
- **Unit of transmission:** burst (+/- 148 bits)
- Burst is sent in Frequency/Time window
  - called a slot, with duration Burst Period
  - frequencies : every 200 kHz
  - time : every 15/26ms (~ 0.577ms)

GSM slot structure

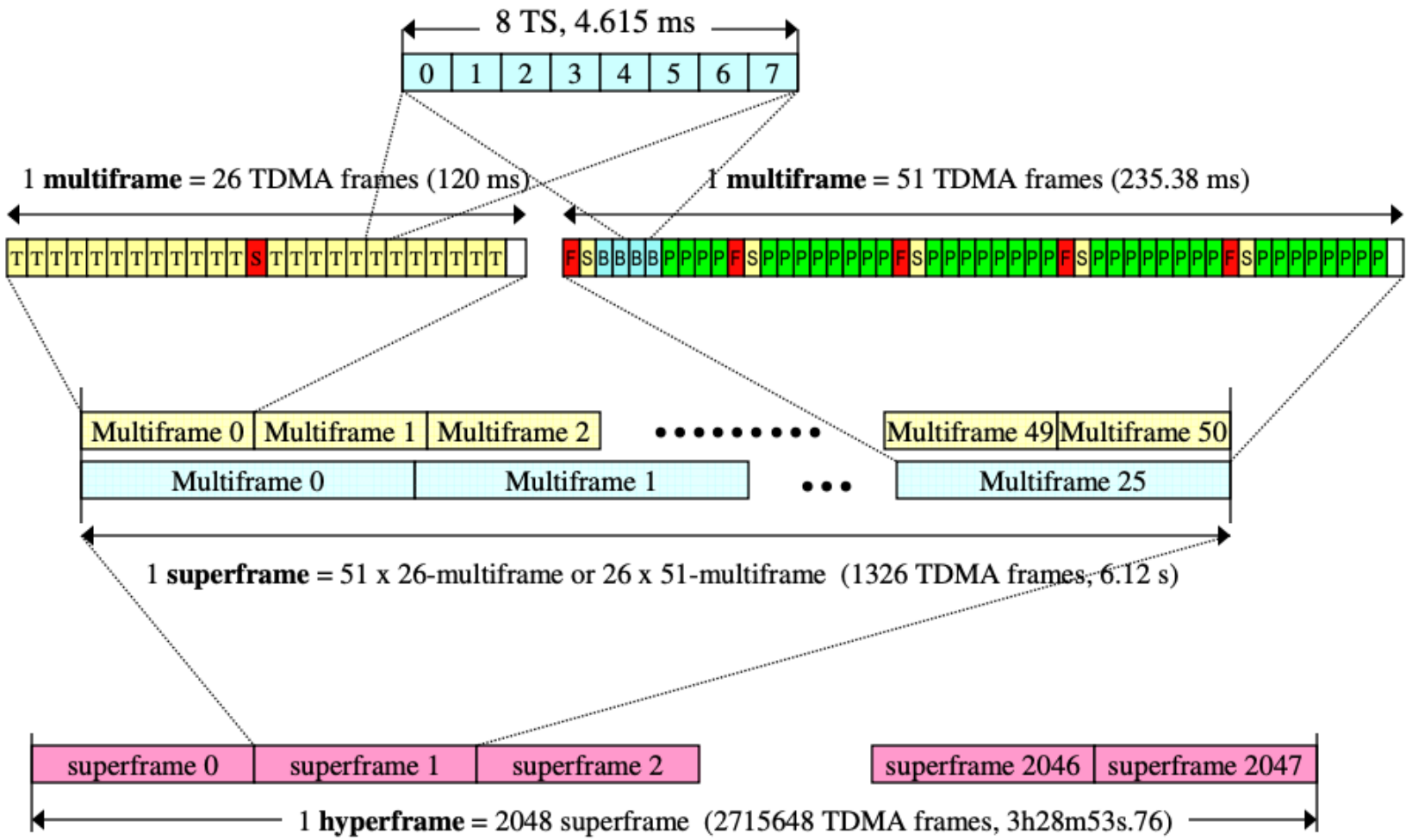
Downlink

Uplink



3 slots delay between up- and downlink to avoid TX/RX on different frequencies at the same time

GSM frame hierarchy



GSM hyperframe:

- Counter
- Every slot: unique sequential number comprising the frame number and time slot number.

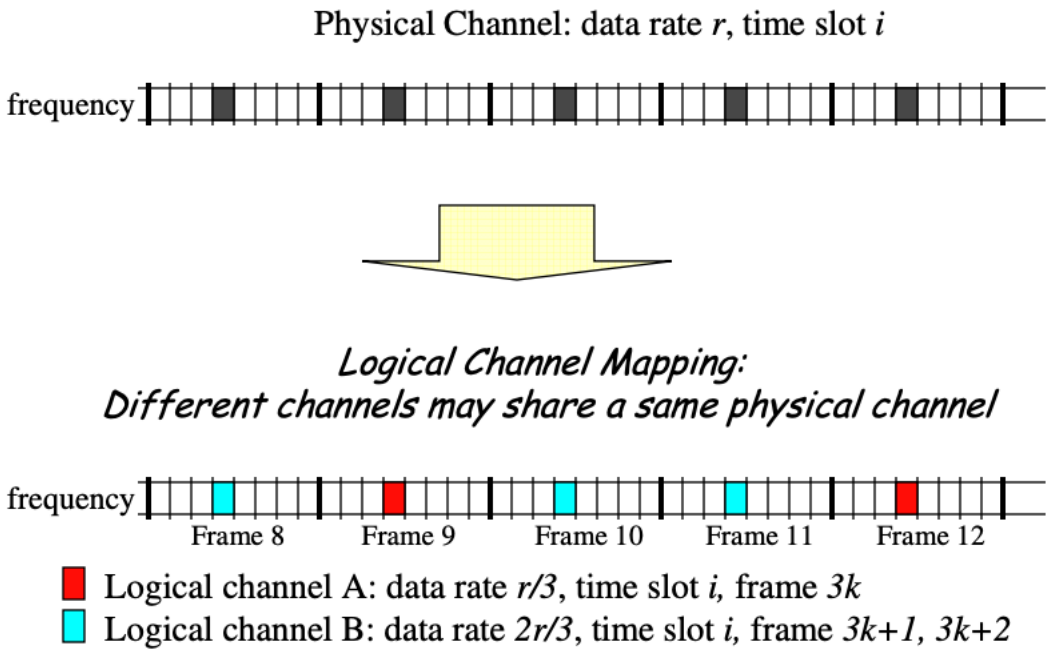
Frequency hopping

- for it to work, the transmitter and receiver must be synchronised so they hop to the same frequencies at the same time.

Encryption

- the encryption process will repeat with each hyperframe. However, it is unlikely that the cellphone conversation will be over 3 hours.

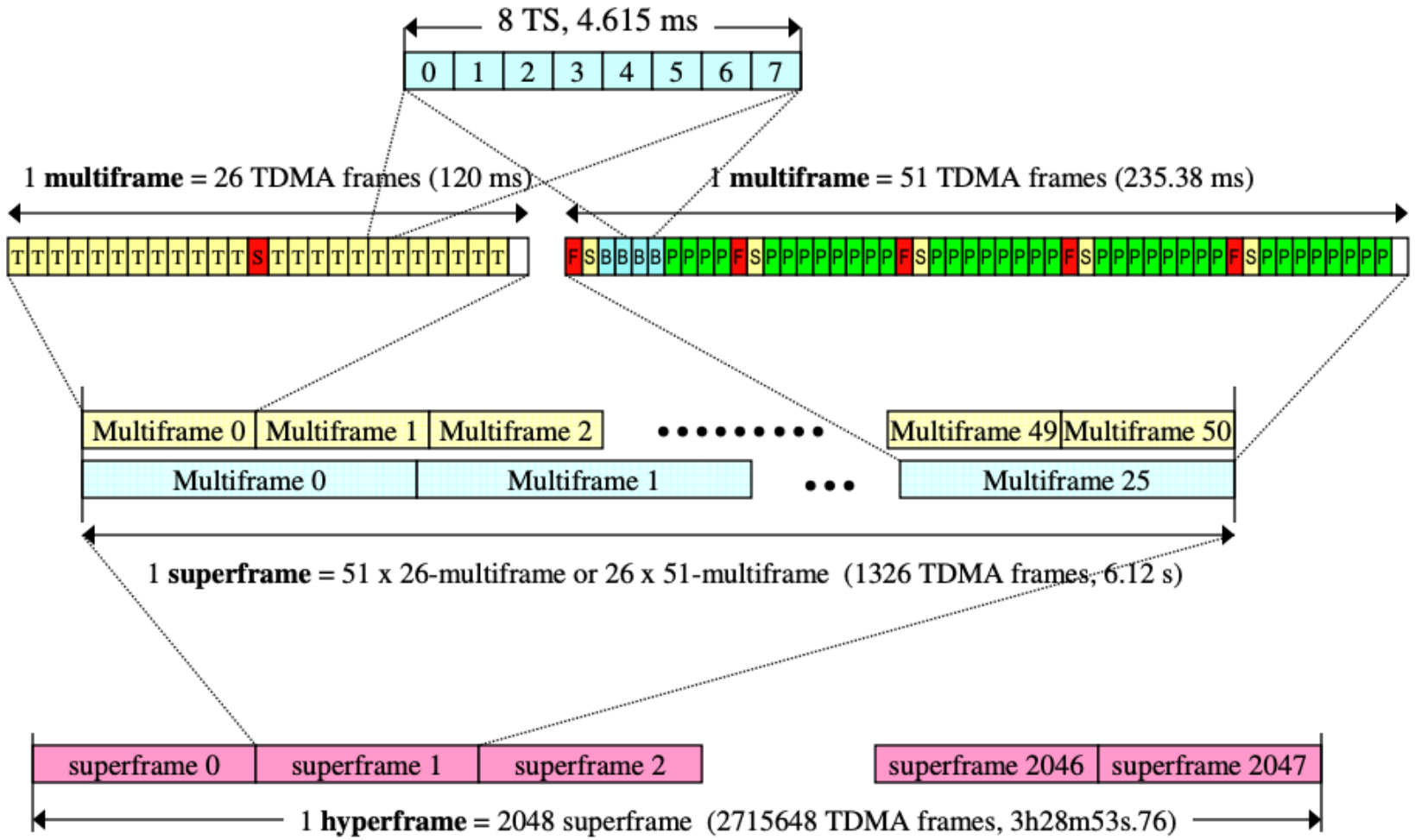
Physical and logical channels



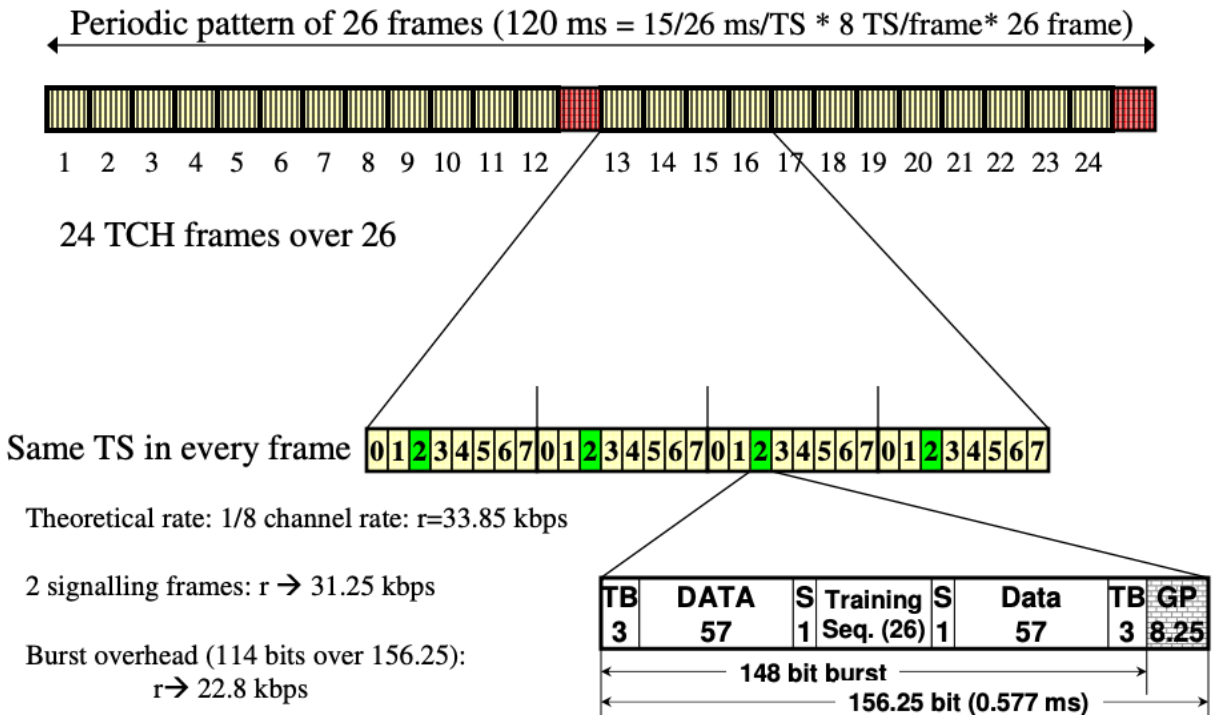
Logical channels

Traffic channel (TCH)	**TCH/F**	TCH full rate	MS←→BSS
	TCH/H	TCH half Rate	MS←→BSS
Broadcast channel	**BCCH**	Broadcast control	BSS→MS
(same information to all MS in a cell)	**FCCH**	Frequency Correction	BSS→MS
	SCH	Synchronization	BSS→MS
Common Control channel (CCCH)	**RACH**	Random Access	MS→BSS
(point to multipoint channels)	**AGCH**	Access Grant	BSS→MS
(used for access management)	**PCH**	Paging	BSS→MS
Dedicated Control channel (DCCH)	**SDCCH**	Stand-alone Dedicated control	MS←→BSS
(point-to-point signalling channels)	**SACCH**	Slow associated control	MS←→BSS
(dedicated to a specific MS)	**FACCH**	Fast associated control	MS←→BSS

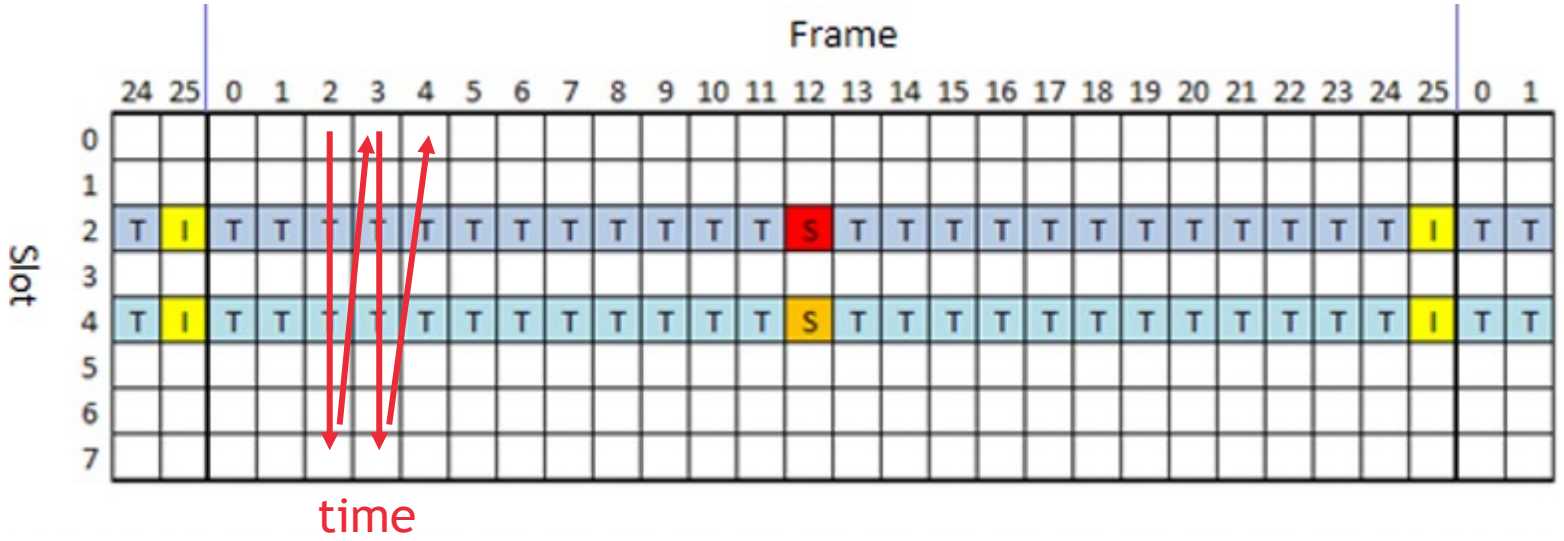
GSM frame hierarchy



Traffic channels

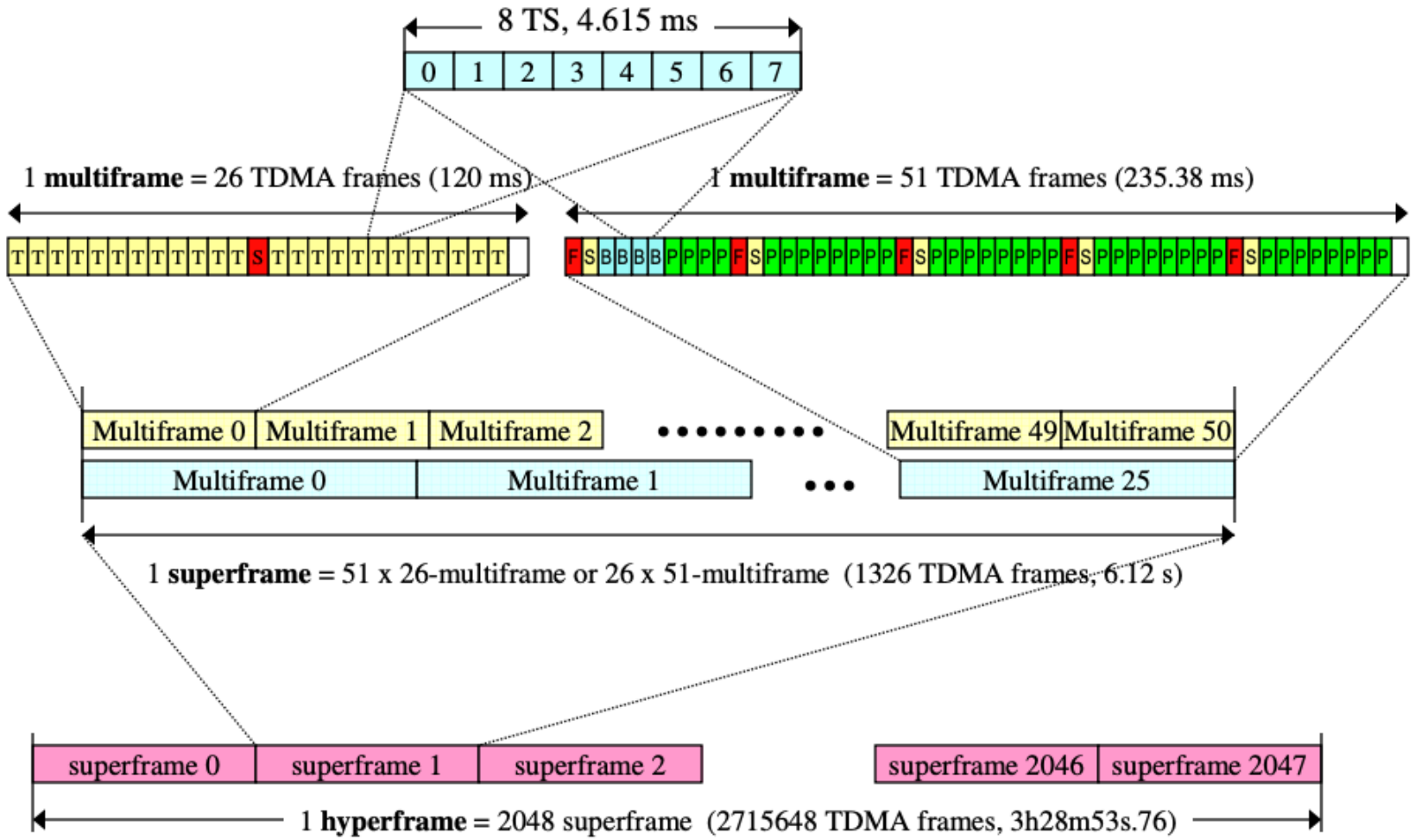


How to visualize this: at one frequency



8 physical channels
Each having multiple logical ones.

GSM frame hierarchy

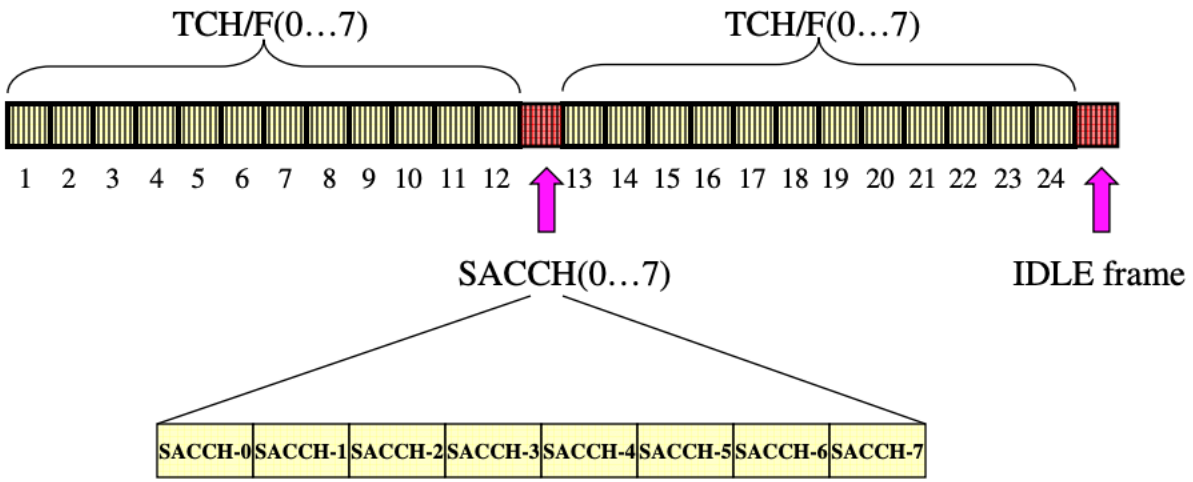


Control for a user during traffic: SACCH

➔ **Always associated to instaurated call on TCH (TCH + SACCH = TACH)**

➔ On the same Time Slot

➔ **Periodic (order of ½ second) time-scale information for radio link control**



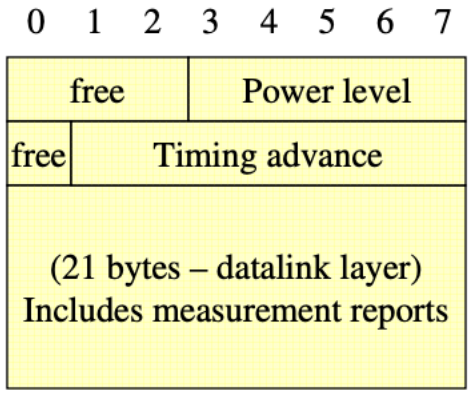
1 SACCH burst (per TCH) every 26 frames (120 ms)

SACCH?

➔ **184 bits = 23 bytes**

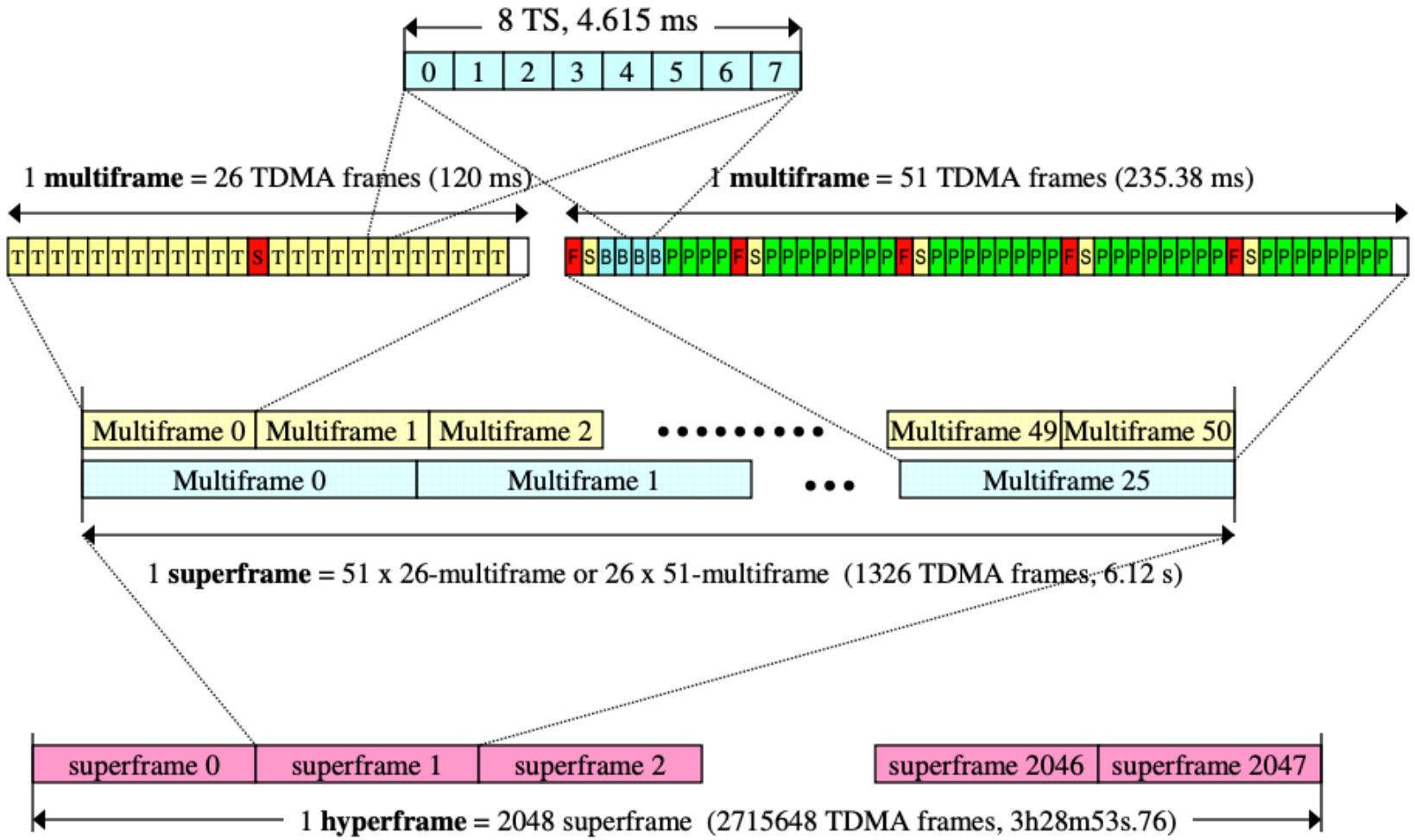
➔ **Power level**
➔ **Timing advance**
➔ **Measurement reports for link quality**
➔ **Measurement reports for handover management**

➔ **When available space: SMS**
⇨ When call in progress!



- **Power level**
  - Some MS/UE are farther, some are closer
- **Timing advance**
  - Some MS/UE are farther, some are closer
- **Measurement reports**
  - “this is what I see”
- **SMS**

GSM frame hierarchy



Logical channels

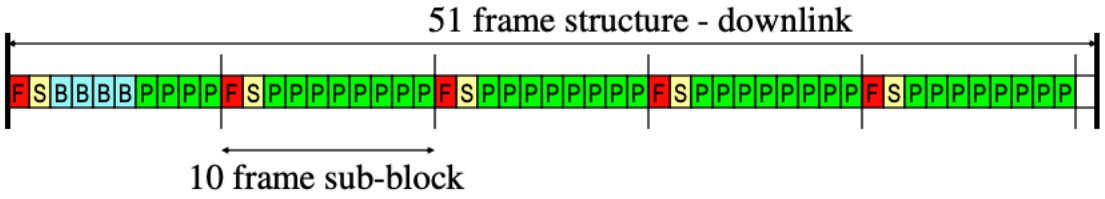
Traffic channel (TCH)	**TCH/F**	TCH full rate	MS←→BSS
	TCH/H	TCH half Rate	MS←→BSS
Broadcast channel	**BCCH**	Broadcast control	BSS→MS
(same information to all MS in a cell)	**FCCH**	Frequency Correction	BSS→MS
	SCH	Synchronization	BSS→MS
Common Control channel (CCCH)	**RACH**	Random Access	MS→BSS
(point to multipoint channels)	**AGCH**	Access Grant	BSS→MS
(used for access management)	**PCH**	Paging	BSS→MS
Dedicated Control channel (DCCH)	**SDCCH**	Stand-alone Dedicated control	MS←→BSS
(point-to-point signalling channels)	**SACCH**	Slow associated control	MS←→BSS
(dedicated to a specific MS)	**FACCH**	Fast associated control	MS←→BSS

Broadcast channel

➔ **51 frame structure vs 26**
- ⇨ 235.38 ms period (vs 120 ms)

➔ **Sub-blocks with 10 frames**
- ⇨ Starting with Frequency Correction Channel (FCCH)
- ⇨ Immediately followed by Synchronization Channel (SCH)

➔ **Other frames (numbered from #0 to #50):**
- ⇨ #50 idle
- ⇨ #2,3,4,5 BCCH
- ⇨ Remaining: Paging (PCH) / Access Grant (AGCH) [=PAGCH]

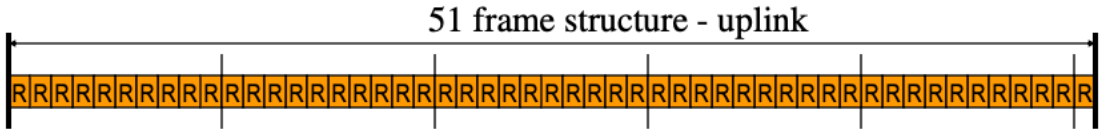


Where is it placed?

➔**On Downlink**

⇨Corresponding uplink dedicated to Random Access Channel

Uplink:



Broadcast

➔**On one frequency per cell (beacon)**

➔**MUST BE on Time Slot #0**

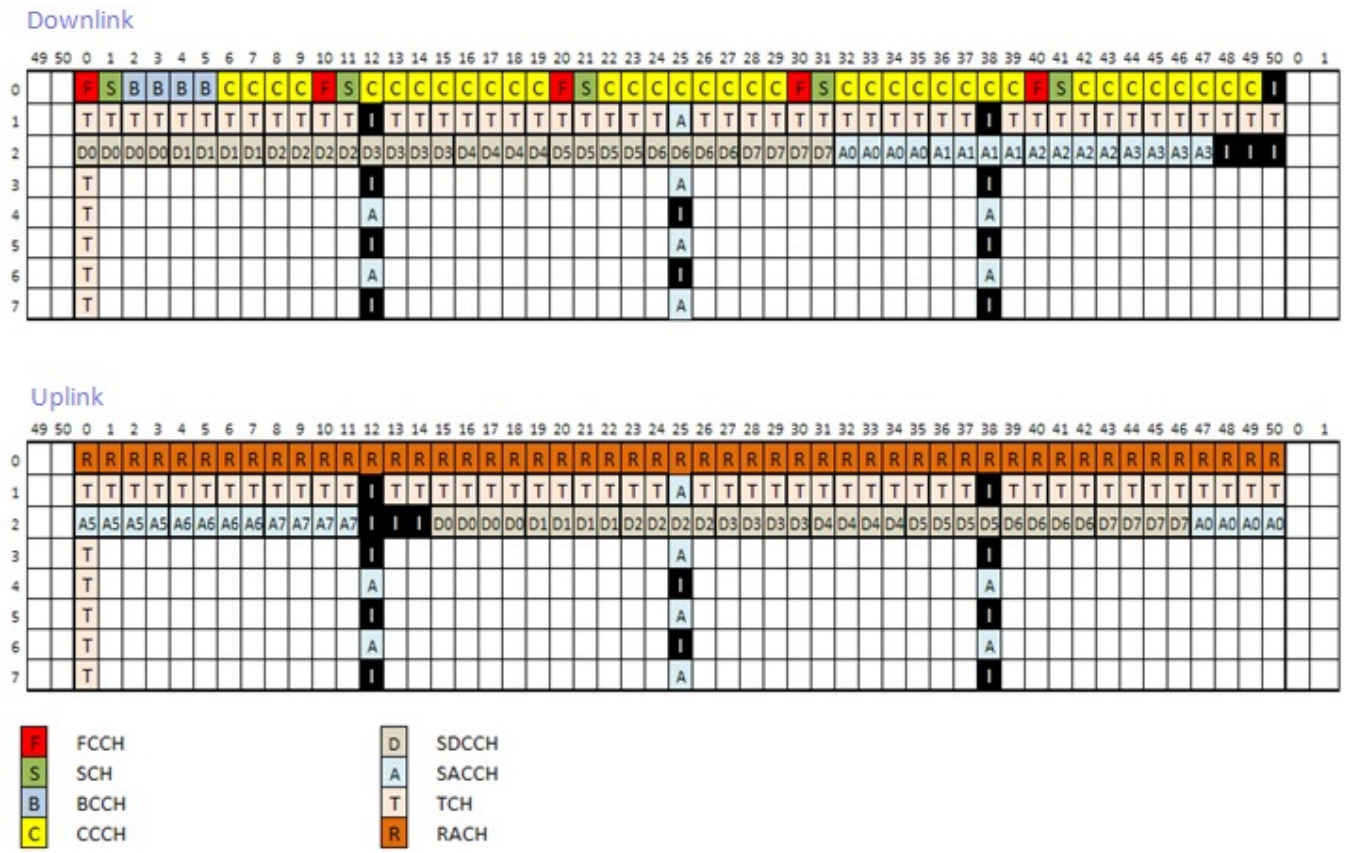
➔**Other Time slots may be used by TCH**

Provided that:

- All empty slots are filled with DUMMY bursts
- Downlink power control must be disabled

https://www.sharetechnote.com/html/FrameStructure_GSM.html

What does this look like, in reality



5 main bursts

Traffic channel (TCH)	**TCH/F**	TCH full rate	MS←→BSS
	TCH/H	TCH half Rate	MS←→BSS
Broadcast channel	**BCCH**	Broadcast control	BSS→MS
(same information to all MS in a cell)	**FCCH**	Frequency Correction	BSS→MS
	SCH	Synchronization	BSS→MS
Common Control channel (CCCH)	**RACH**	Random Access	MS→BSS
(point to multipoint channels)	**AGCH**	Access Grant	BSS→MS
(used for access management)	**PCH**	Paging	BSS→MS
Dedicated Control channel (DCCH)	**SDCCH**	Stand-alone Dedicated control	MS←→BSS
(point-to-point signalling channels)	**SACCH**	Slow associated control	MS←→BSS
(dedicated to a specific MS)	**FACCH**	Fast associated control	MS←→BSS

Normal

3 start bits	58 bits of encrypted data	26 training bits	58 bits of encrypted data	3 stop bits	8.25 bits guard period

FCCH burst

3 start bits	142 fixed bits of all zeroes	3 stop bits	8.25 bits guard period

SCH burst

3 start bits	39 bits of encrypted data	64 bits of training	39 bits of encrypted data	3 stop bits	8.25 bits guard period

RACH burst

8 start bits	41 bits of synchronization	36 bits of encrypted data	3 stop bits	68.25 bit extended guard period

Dummy burst

3 start bits	58 mixed bits	26 training bits	58 mixed bits	3 stop bits	8.25 bits guard period

Data Link not just for multiplexing …

- **Data link layer improves the quality of physical layer**
  - error detection and error correction
    - parity check
    - longitudinal check
    - cyclic redundancy check
  - flow control
    - Stop-and-Wait
    - Sliding window
    - Stop-and-Wait ARQ (Automatic repeat request)
    - Go-back-N ARQ
    - Selective-reject ARQ

https://en.wikipedia.org/wiki/International_Standard_Book_Number#ISBN-10_check_digits
https://en.wikipedia.org/wiki/Luhn_algorithm

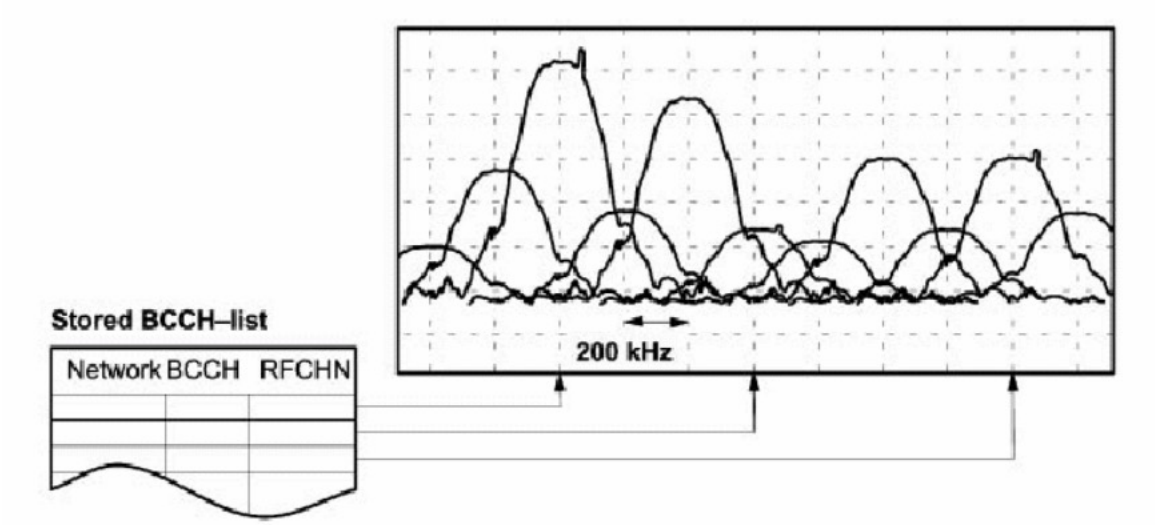
Error detection & correction

- **ISBN**
  - The two most common errors in handling an ISBN (e.g. when typing it or writing it down) are a single altered digit or the transposition of adjacent digits. It can be proven mathematically that all pairs of valid ISBN-10s differ in at least two digits. It can also be proven that there are no pairs of valid ISBN-10s with eight identical digits and two transposed digits.
- **Credit card (Luhn's)**
  - The Luhn algorithm will detect all single-digit errors, as well as almost all transpositions of adjacent digits. It will not, however, detect transposition of the two-digit sequence 09 to 90 (or vice versa). It will detect most of the possible twin errors (it will not detect 22 ↔ 55, 33 ↔ 66 or 44 ↔ 77).

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits~~ ~~for multiple users~~
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

Listening to the broadcast channel



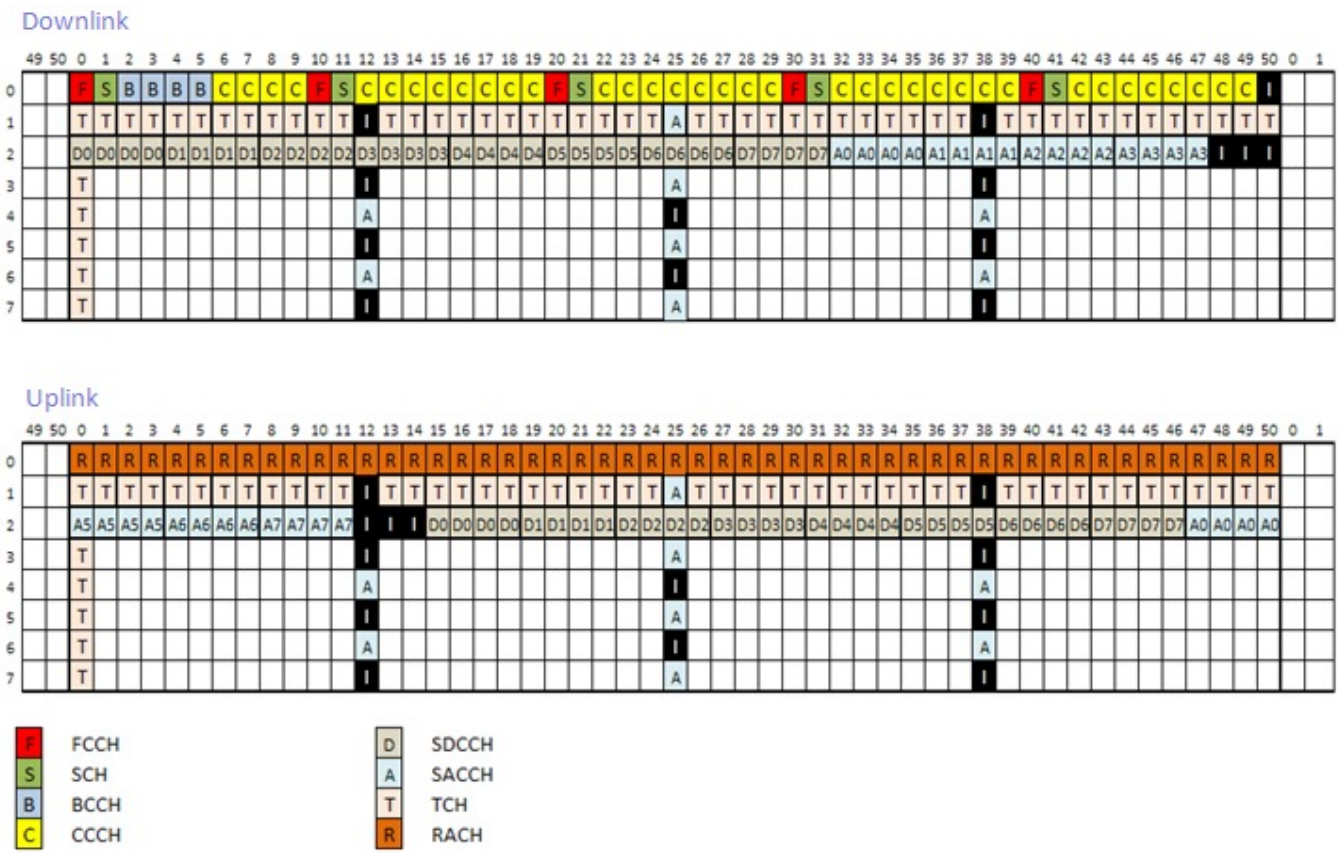
First operation when MS turned ON: spectrum analysis
(either on list of up to 32 Radio Frequency Channel Numbers of current network)
(or on whole 124 carriers spectrum)

Tune to the right frequency

- **MS will listen to strongest beacon for a pure sine wave (FCCH)**
  - Coarse bit synchronization
  - Oscillator correction
- **Then, we use the SCH burst**
  - Fine tuning of synchronization
  - Specialized sequences
- **Now we can read BCCH**
  - Parameters of the cell like RACH backoff, power, allowed, list of carriers, other BCCH, neighbors

https://www.sharetechnote.com/html/FrameStructure_GSM.html

What does this look like, in reality



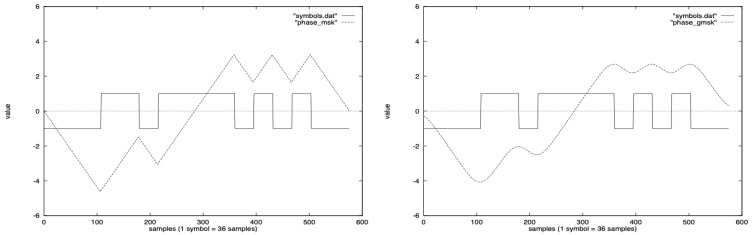


Figure 1: Symbols and phase (in radians) of MSK and GMSK signal vs samples

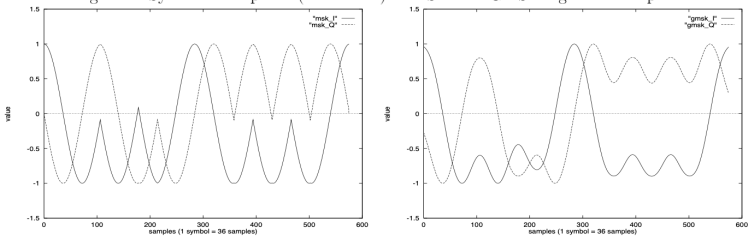


Figure 2: Baseband (I,Q) MSK and GMSK signals vs samples for fsT=36

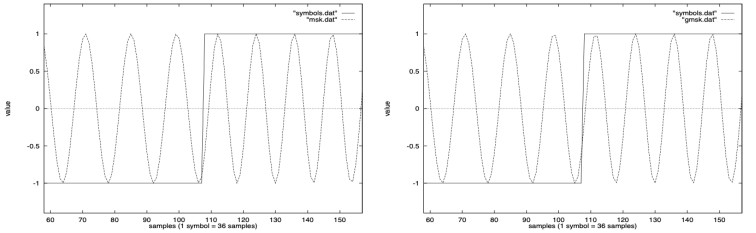


Figure 3: MSK and GMSK signal vs samples for fsT=36

https://www.rfwireless-world.com/Terminology/GSM-system-information-messages.html

Which information do you get? System Information (SI)!

GSM System Information message type	**SI Description**
System information-1(SI1)	Cell ARFCN, RACH parameters required to access the system by MS and hopping related information are sent in this SI message.
System information-2(SI2)	Neighbour BCCH frequencies and PLMN information are sent in this SI. MS uses these frequencies for signal strength measurements required for handover.
System information-2bis(SI-2bis)	RACH control and BCCH extension on neighbor cells
System information-2ter(SI-2ter)	Information of BCCH extended allocated on which neighbor cells are provided in this SI. Broadcasted optionally on BCCH by the network to all the MSs.
System information-2 Quarter (SI-2Quater)	3G neighbor cell related information
System information-3 (SI3)	Carry following : 1. LAI of the current location area, 2. Cell identity, 3. Control channel information required to calculate paging group, 4. Cell options to achieve good performance in the cell, 5. cell selection parameters required by MS.
System information-4 (SI4)	CBCH and CBCH related frequency information, LAI, Cell selection parameters and RACH control information are carried by this SI4 message.

Which frequencies ?

Which neighbors ?

Extensions

Who am I, and how do you talk to me?

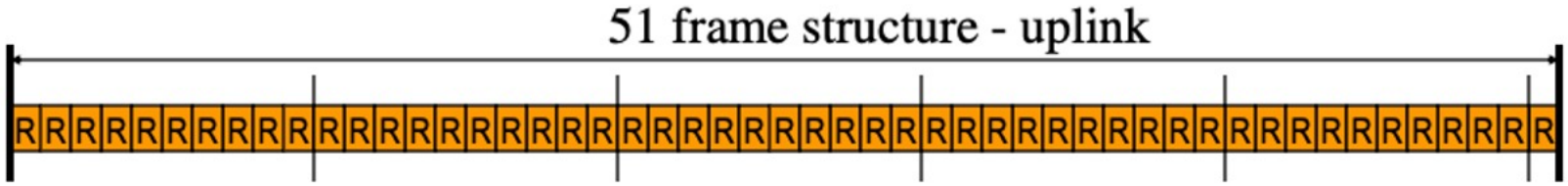
What optional things do I have ?

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits~~ ~~for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

Medium Access Control (MAC)

- **Medium Access Control (MAC) :**
  - mechanism to share the access to a common medium
- **Assumptions for further studies:**
  - N independent stations sharing common channel
  - collision when frames are sent simultaneous
  - slotted or unslotted access system
  - with or without carrier sensing
  - centralized or distributed control



Types of MAC Protocols (1)

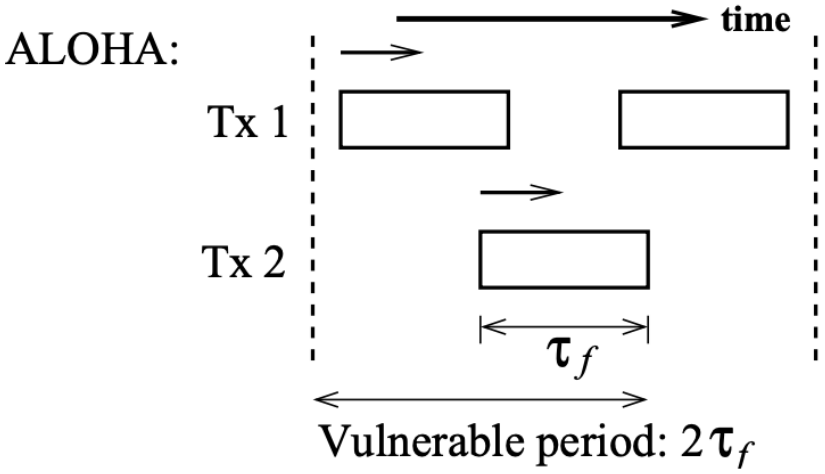
- **Random Access Protocols**
  - Transmission is random among stations
  - More than one station can transmit packets at the same time, hence, collisions are possible
  - Each station transmits at the full rate of the medium
  - In case of a collision, each node has to retransmit the packet.
  - Examples:
    - ALOHA
    - CSMA (Carrier Sensing Multiple Access) protocols

Types of MAC Protocols (2)

- **Taking-Turns Protocols**
  - Nodes take turns to transmit their packets
  - Example: polling protocol
    - One of the nodes is designated as master node
    - The master node polls each of the nodes in a round-robin fashion
  - No collisions

Example: ALOHA Protocol

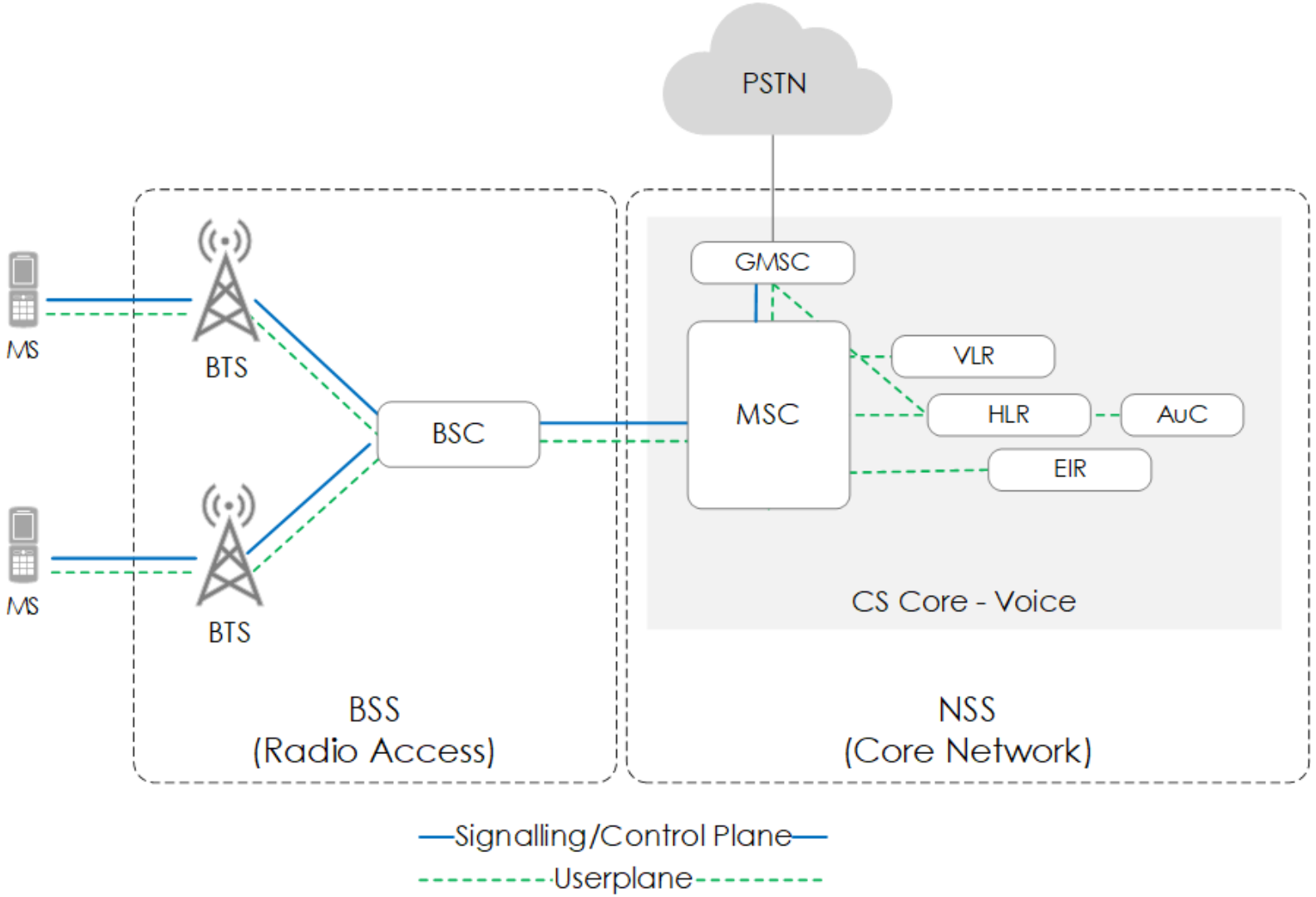
- **ALOHA**
  - packet radio network (Univ. Hawaii, 1970)
  - used in many systems (e.g. GSM)
- **Operation of ALOHA**
  - station transmits when frame is available
  - station is able to check if a collision occurs
  - If a collision occurs, the station waits for a random time before sending again the frame (this waiting time is non-deterministic)



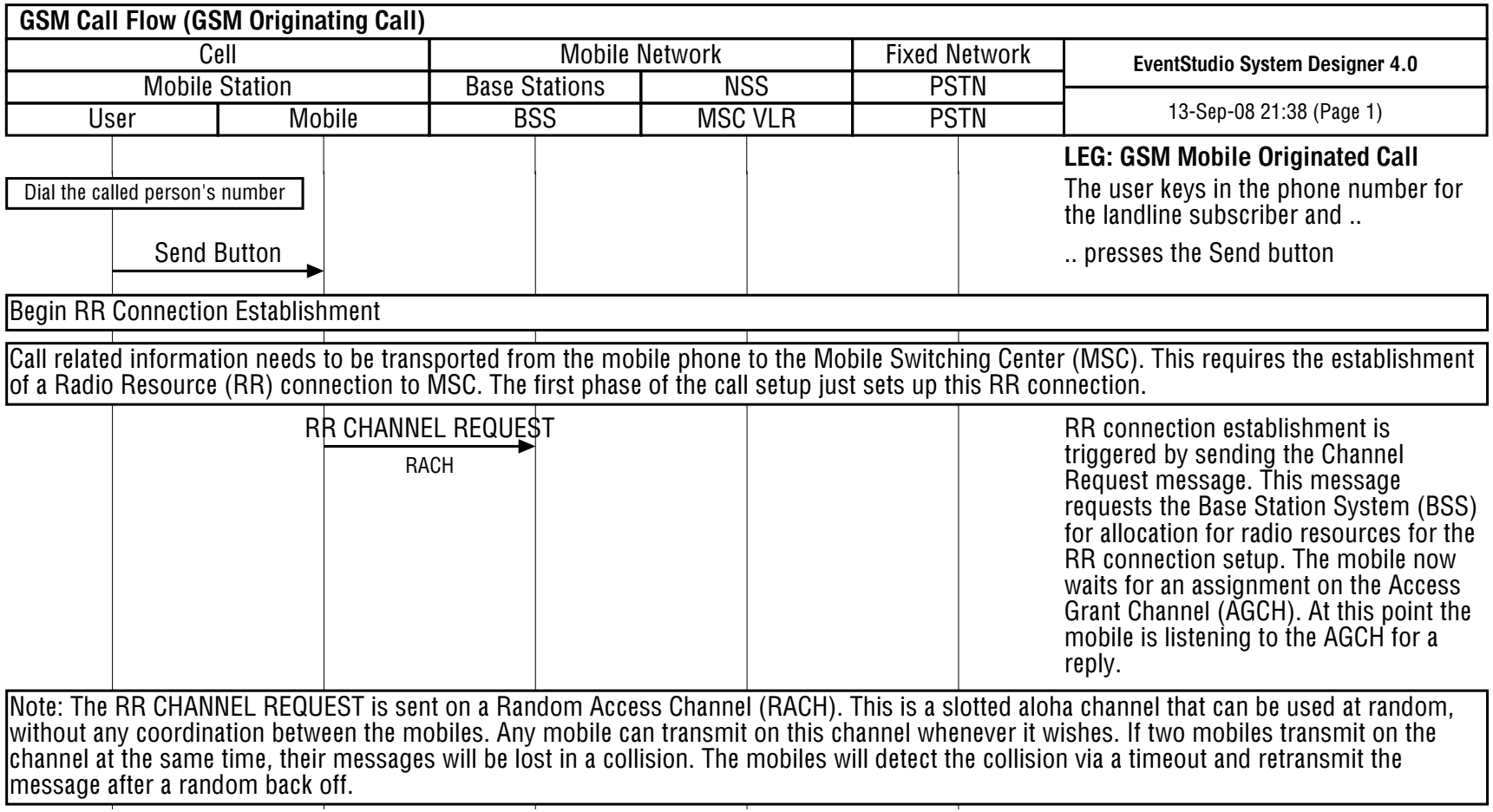
What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits~~ ~~for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Pick a time to send~~
7. ~~Wait for a response (try again)~~
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

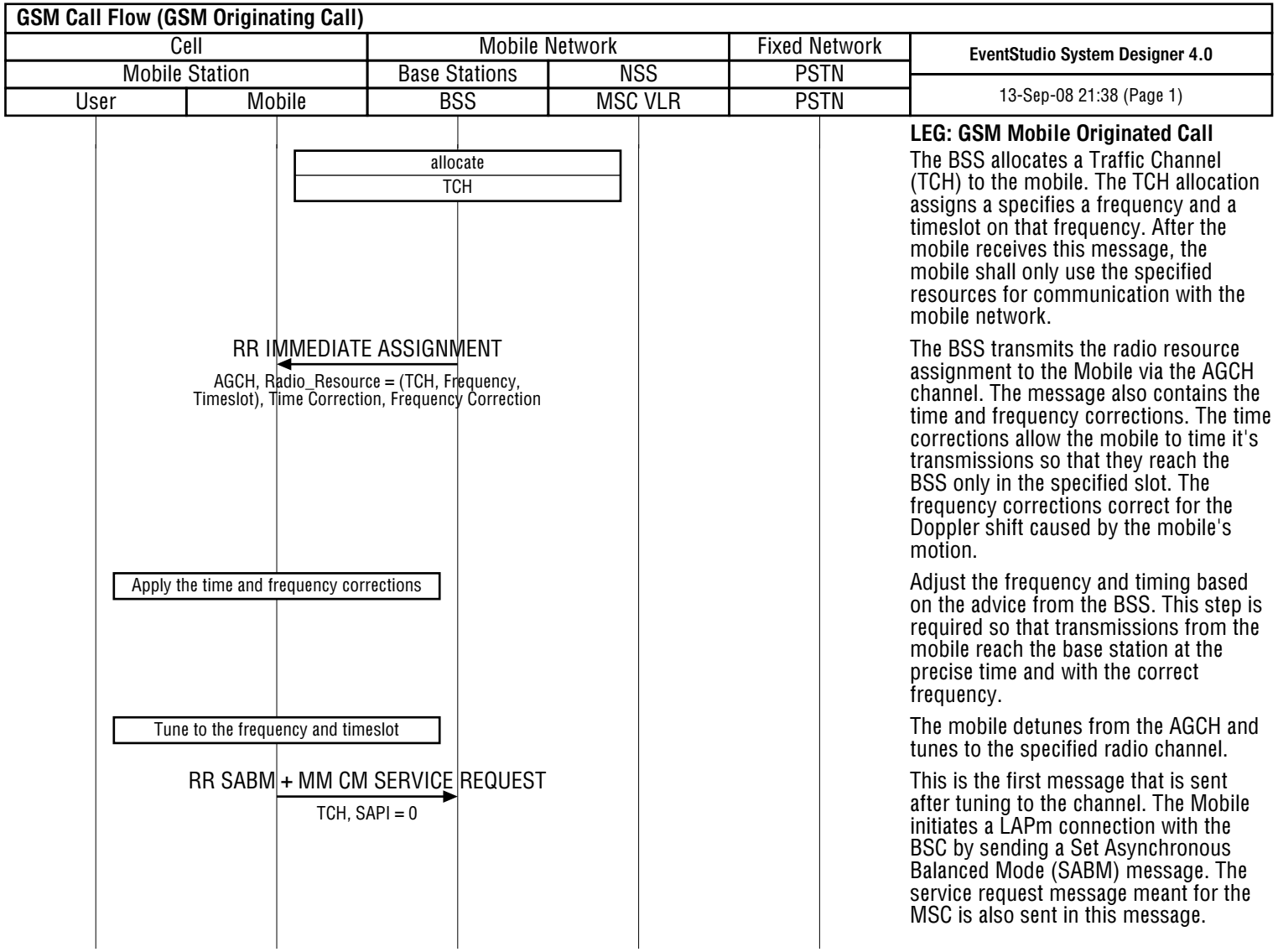
2G architecture



2G flow (1)


GSM Call Flow (GSM Originating Call)
Cell
Mobile Network
Fixed Network
EventStudio System Designer 4.0
Mobile Station
Base Stations
NSS
PSTN
User
Mobile
BSS
MSC VLR
PSTN
13-Sep-08 21:38 (Page 1)
LEG: GSM Mobile Originated Call
The user keys in the phone number for the landline subscriber and ..
.. presses the Send button
Dial the called person's number
Send Button
Begin RR Connection Establishment
Call related information needs to be transported from the mobile phone to the Mobile Switching Center (MSC). This requires the establishment of a Radio Resource (RR) connection to MSC. The first phase of the call setup just sets up this RR connection.
RR CHANNEL REQUEST
RACH
RR connection establishment is triggered by sending the Channel Request message. This message requests the Base Station System (BSS) for allocation for radio resources for the RR connection setup. The mobile now waits for an assignment on the Access Grant Channel (AGCH). At this point the mobile is listening to the AGCH for a reply.
Note: The RR CHANNEL REQUEST is sent on a Random Access Channel (RACH). This is a slotted aloha channel that can be used at random, without any coordination between the mobiles. Any mobile can transmit on this channel whenever it wishes. If two mobiles transmit on the channel at the same time, their messages will be lost in a collision. The mobiles will detect the collision via a timeout and retransmit the message after a random back off.

2G flow (2)



LEG: GSM Mobile Originated Call

The BSS allocates a Traffic Channel (TCH) to the mobile. The TCH allocation assigns a specifies a frequency and a timeslot on that frequency. After the mobile receives this message, the mobile shall only use the specified resources for communication with the mobile network.

The BSS transmits the radio resource assignment to the Mobile via the AGCH channel. The message also contains the time and frequency corrections. The time corrections allow the mobile to time it's transmissions so that they reach the BSS only in the specified slot. The frequency corrections correct for the Doppler shift caused by the mobile's motion.

Adjust the frequency and timing based on the advice from the BSS. This step is required so that transmissions from the mobile reach the base station at the precise time and with the correct frequency.

The mobile detunes from the AGCH and tunes to the specified radio channel.

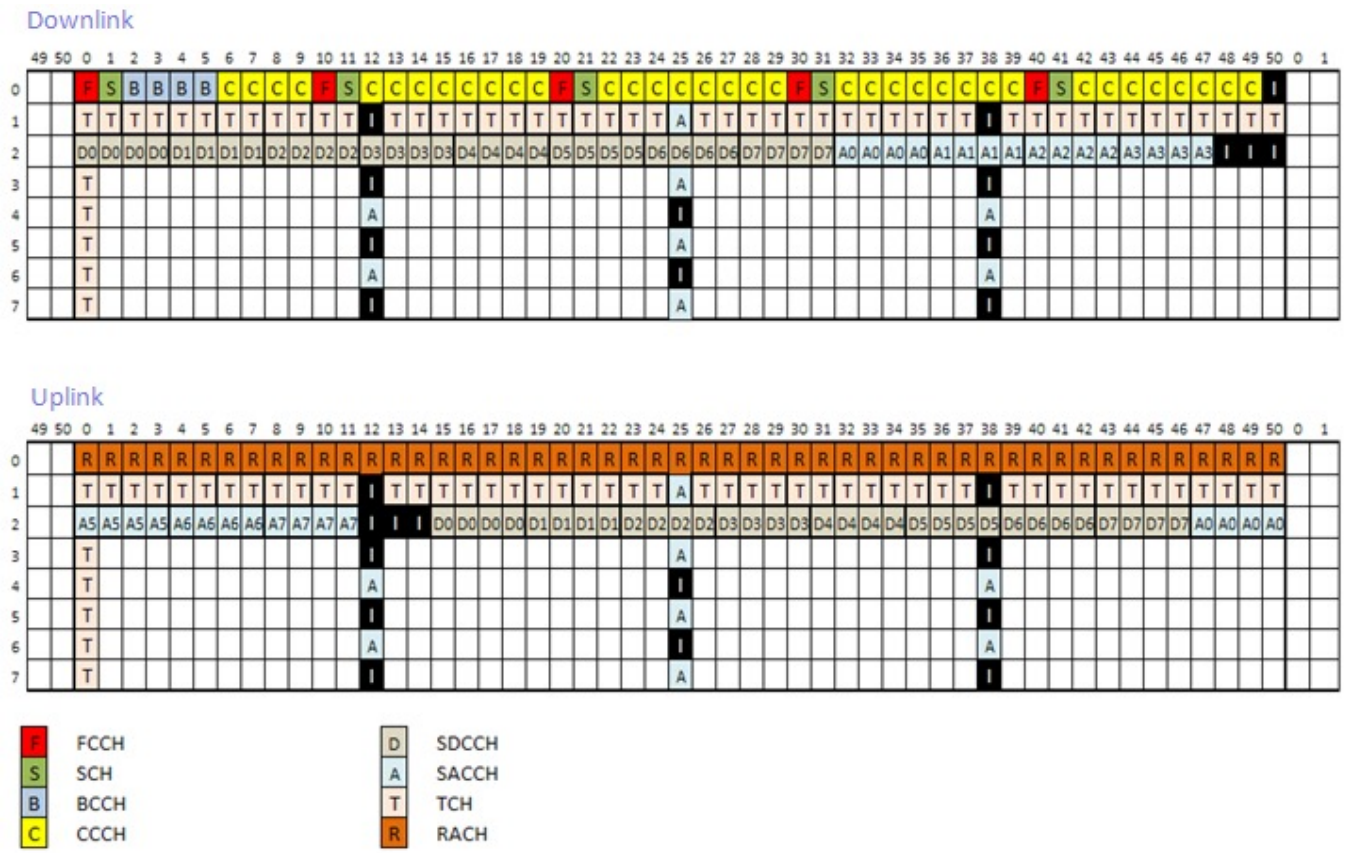
This is the first message that is sent after tuning to the channel. The Mobile initiates a LAPm connection with the BSC by sending a Set Asynchronous Balanced Mode (SABM) message. The service request message meant for the MSC is also sent in this message.

Logical channels

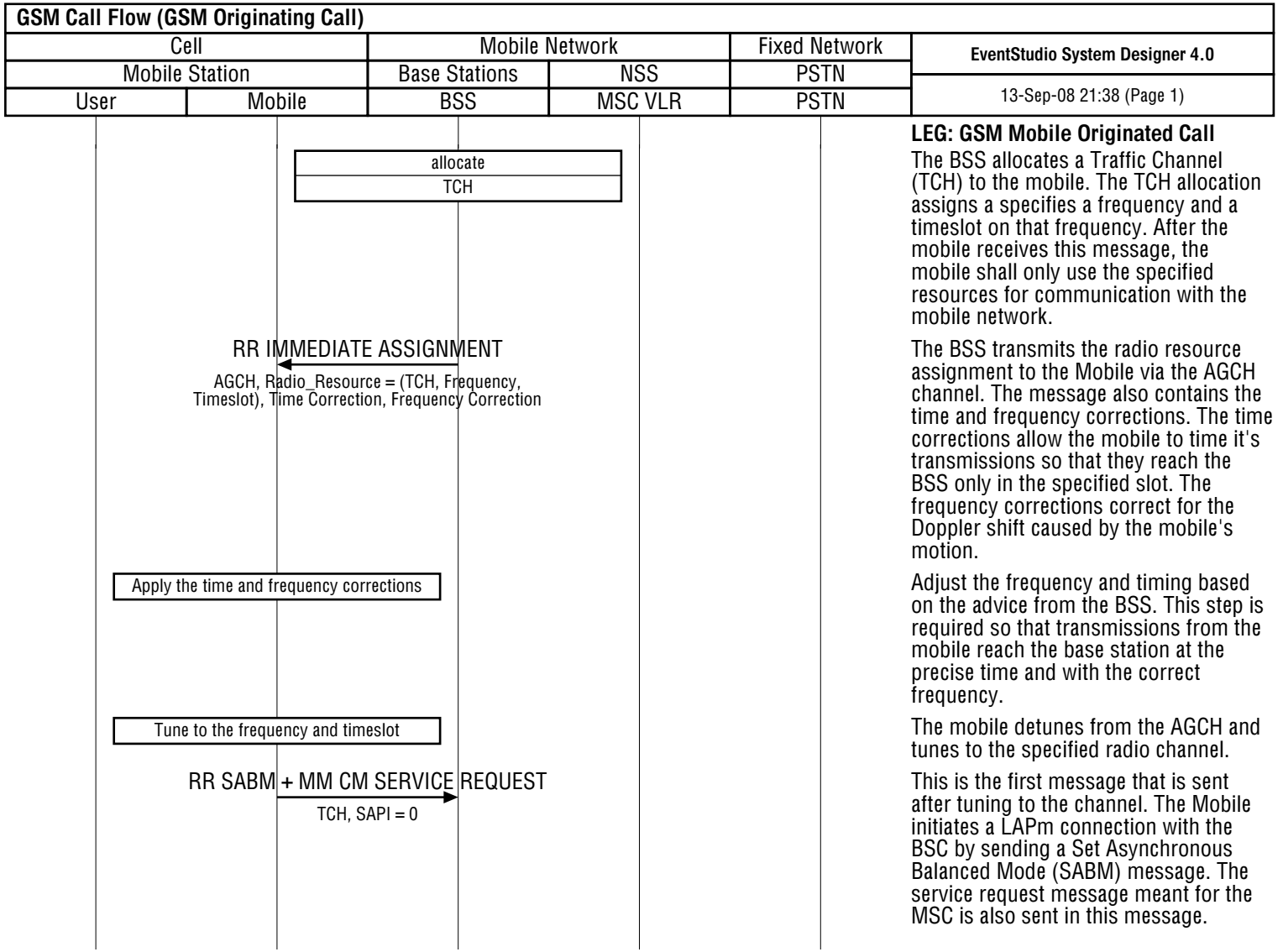
Traffic channel (TCH)	**TCH/F**	TCH full rate	MS←→BSS
	TCH/H	TCH half Rate	MS←→BSS
Broadcast channel	**BCCH**	Broadcast control	BSS→MS
(same information to all MS in a cell)	**FCCH**	Frequency Correction	BSS→MS
	SCH	Synchronization	BSS→MS
Common Control channel (CCCH)	**RACH**	Random Access	MS→BSS
(point to multipoint channels)	**AGCH**	Access Grant	BSS→MS
(used for access management)	**PCH**	Paging	BSS→MS
Dedicated Control channel (DCCH)	**SDCCH**	Stand-alone Dedicated control	MS←→BSS
(point-to-point signalling channels)	**SACCH**	Slow associated control	MS←→BSS
(dedicated to a specific MS)	**FACCH**	Fast associated control	MS←→BSS

https://www.sharetechnote.com/html/FrameStructure_GSM.html

What does this look like, in reality



2G flow (2)



LEG: GSM Mobile Originated Call

The BSS allocates a Traffic Channel (TCH) to the mobile. The TCH allocation assigns a specifies a frequency and a timeslot on that frequency. After the mobile receives this message, the mobile shall only use the specified resources for communication with the mobile network.

The BSS transmits the radio resource assignment to the Mobile via the AGCH channel. The message also contains the time and frequency corrections. The time corrections allow the mobile to time it's transmissions so that they reach the BSS only in the specified slot. The frequency corrections correct for the Doppler shift caused by the mobile's motion.

Adjust the frequency and timing based on the advice from the BSS. This step is required so that transmissions from the mobile reach the base station at the precise time and with the correct frequency.

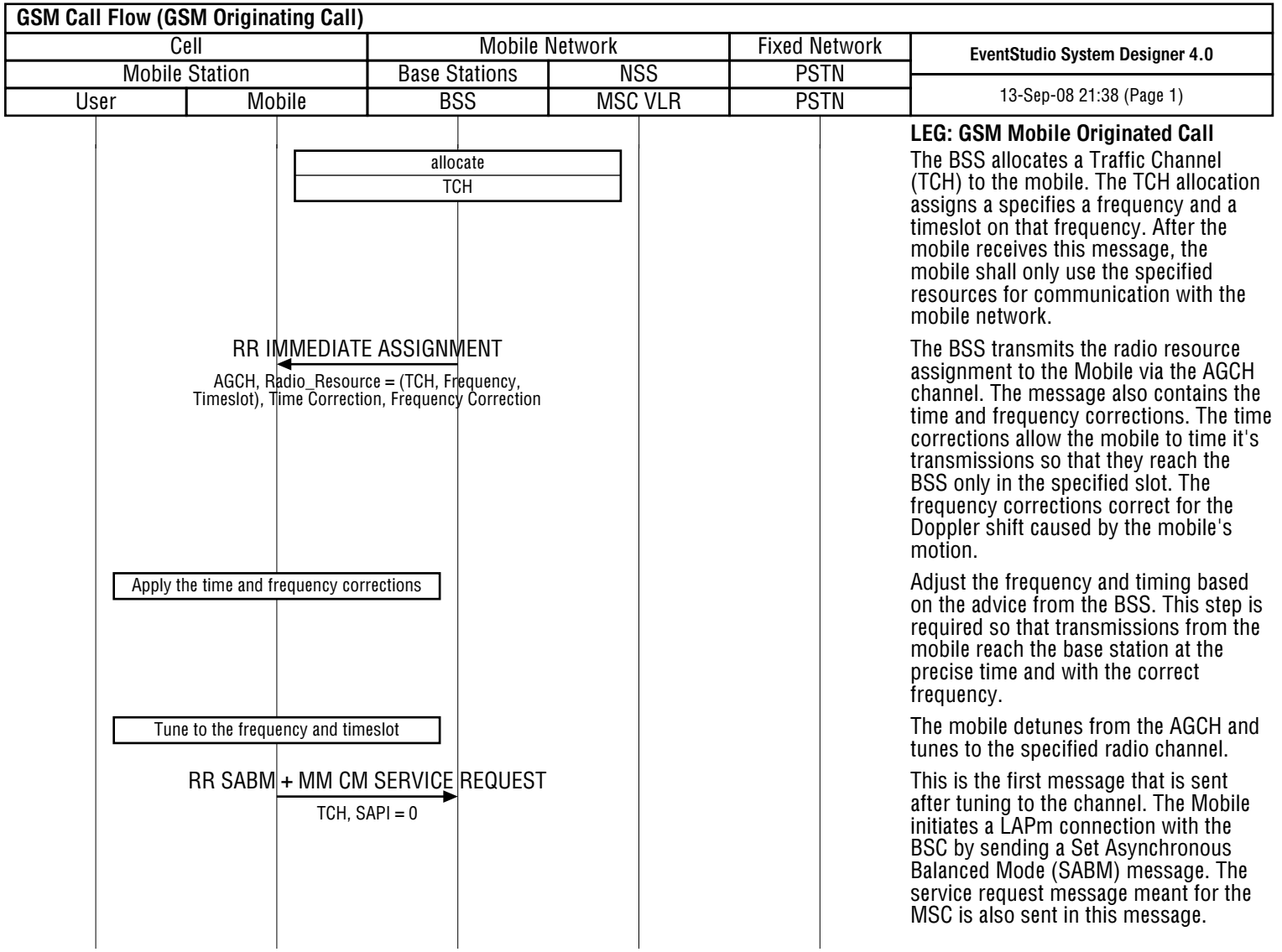
The mobile detunes from the AGCH and tunes to the specified radio channel.

This is the first message that is sent after tuning to the channel. The Mobile initiates a LAPm connection with the BSC by sending a Set Asynchronous Balanced Mode (SABM) message. The service request message meant for the MSC is also sent in this message.

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits~~ ~~for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Pick a time to send~~
7. ~~Wait for a response (try again)~~
8. ~~Get a control channel assigned~~
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

2G flow (2)



LEG: GSM Mobile Originated Call

The BSS allocates a Traffic Channel (TCH) to the mobile. The TCH allocation assigns a specifies a frequency and a timeslot on that frequency. After the mobile receives this message, the mobile shall only use the specified resources for communication with the mobile network.

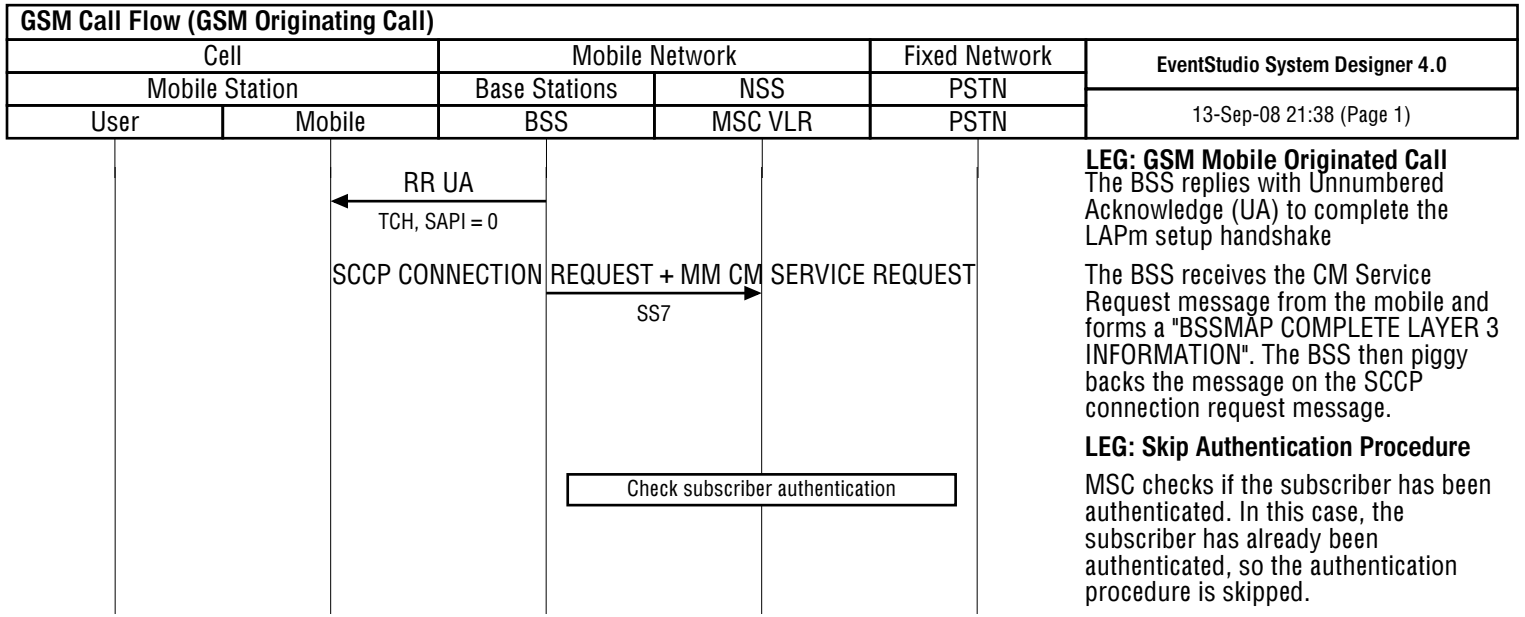
The BSS transmits the radio resource assignment to the Mobile via the AGCH channel. The message also contains the time and frequency corrections. The time corrections allow the mobile to time it's transmissions so that they reach the BSS only in the specified slot. The frequency corrections correct for the Doppler shift caused by the mobile's motion.

Adjust the frequency and timing based on the advice from the BSS. This step is required so that transmissions from the mobile reach the base station at the precise time and with the correct frequency.

The mobile detunes from the AGCH and tunes to the specified radio channel.

This is the first message that is sent after tuning to the channel. The Mobile initiates a LAPm connection with the BSC by sending a Set Asynchronous Balanced Mode (SABM) message. The service request message meant for the MSC is also sent in this message.

2G flow (3)

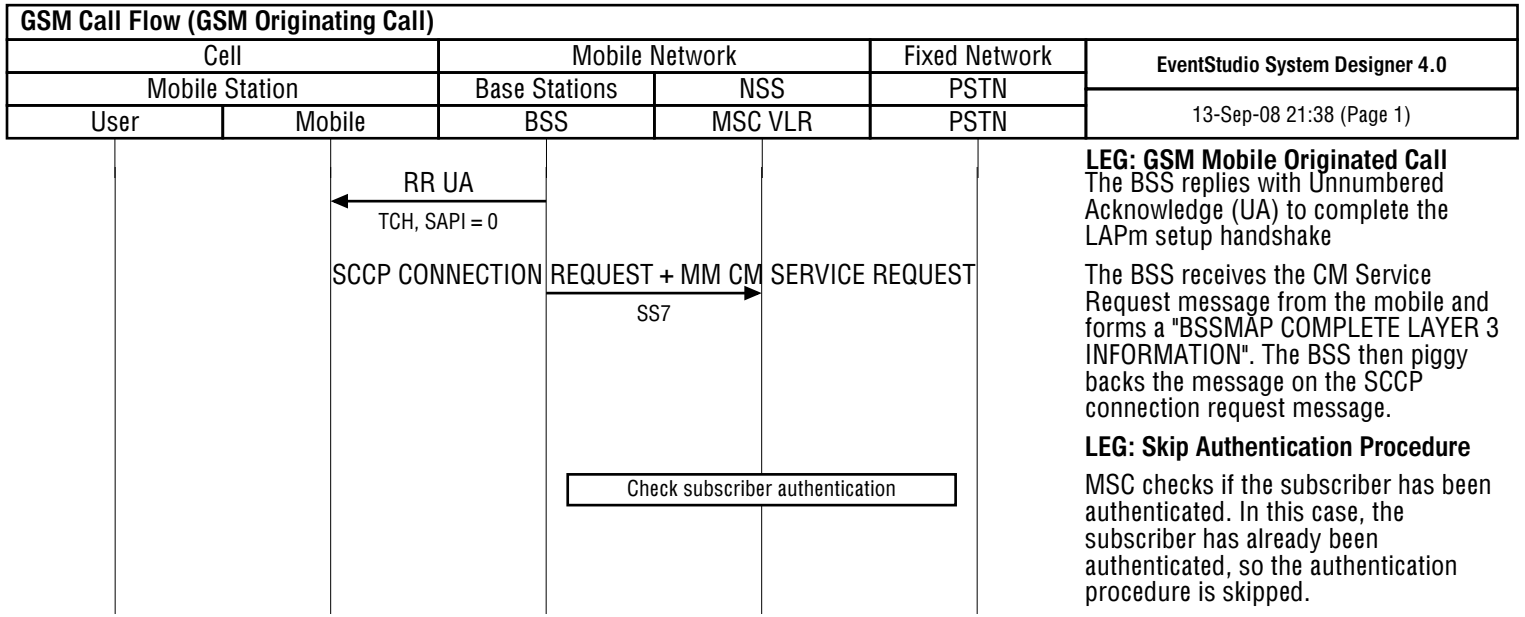


SCCP: signalling connection and control part
MM: mobility management
CM: call management

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits~~ ~~for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Pick a time to send~~
7. ~~Wait for a response (try again)~~
8. ~~Get a control channel assigned~~
9. ~~Ask to make a call~~
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

2G flow (3)



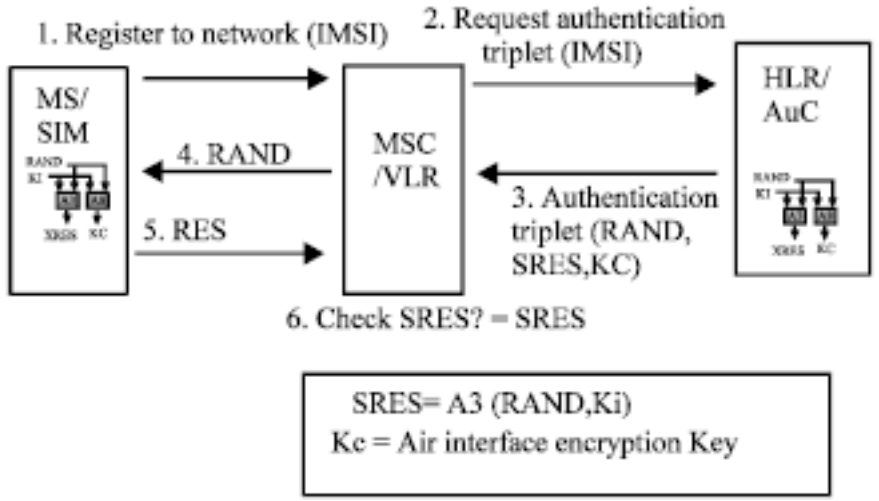
LEG: GSM Mobile Originated Call
The BSS replies with Unnumbered Acknowledge (UA) to complete the LAPm setup handshake

The BSS receives the CM Service Request message from the mobile and forms a "BSSMAP COMPLETE LAYER 3 INFORMATION". The BSS then piggy backs the message on the SCCP connection request message.

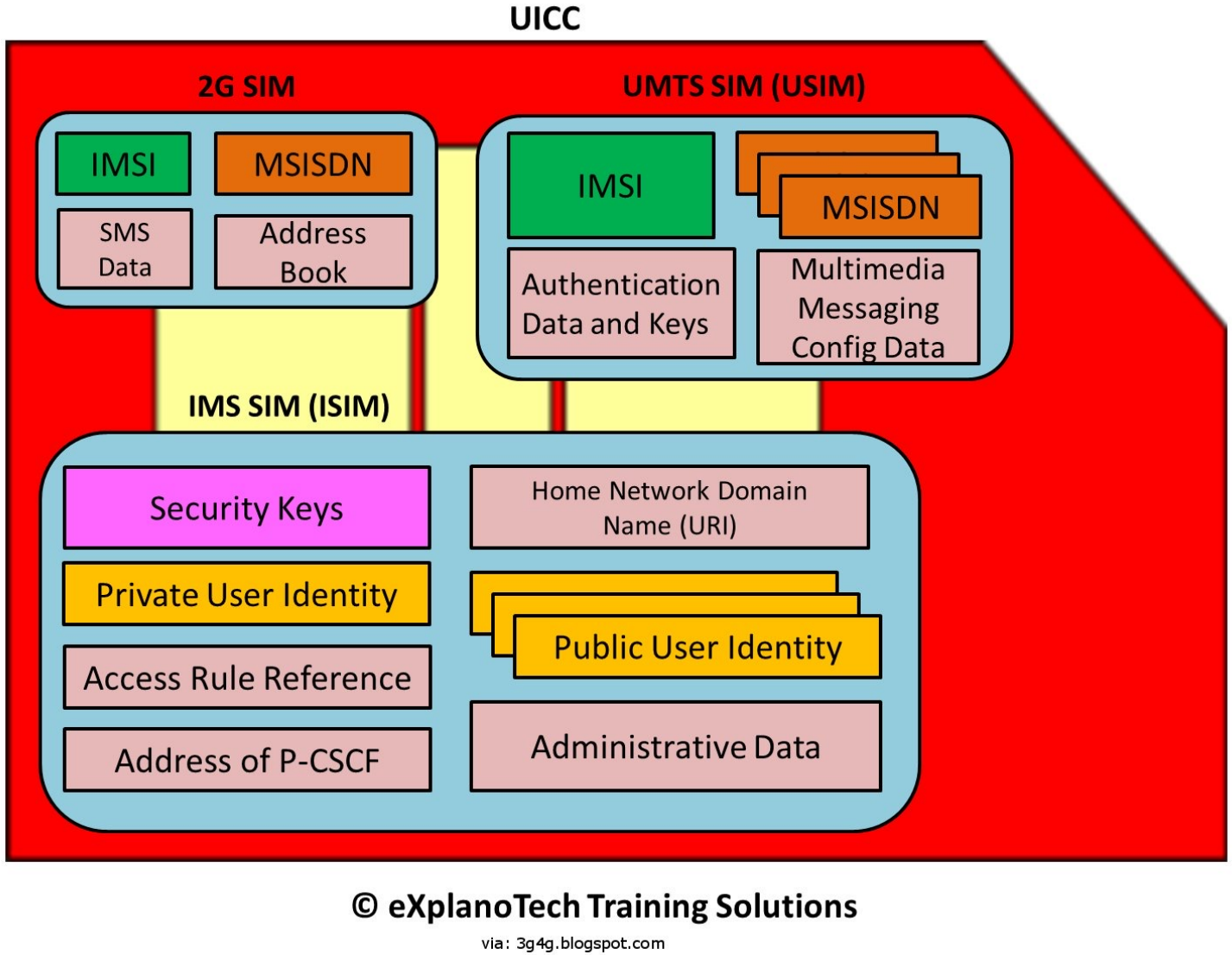
LEG: Skip Authentication Procedure

MSC checks if the subscriber has been authenticated. In this case, the subscriber has already been authenticated, so the authentication procedure is skipped.

Authentication:



All on the MS SIM

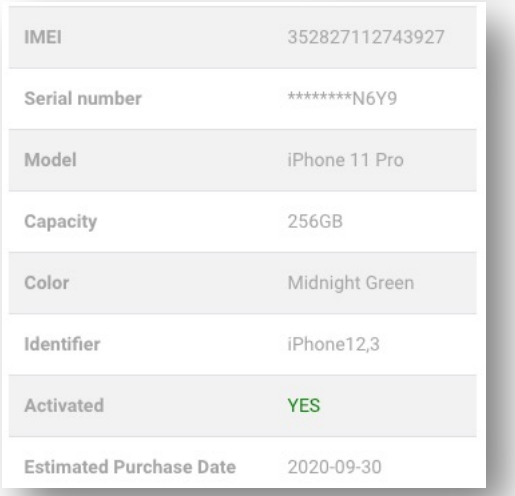


UICC: Universal Integrated Circuit Card.
SIM (Subscriber Identification Module)

Numbering: IMEI (not on SIM)

- International Mobile Equipment Identification: It will uniquely identify a mobile station. It is a decimal number of 15 digits. Its structure is:

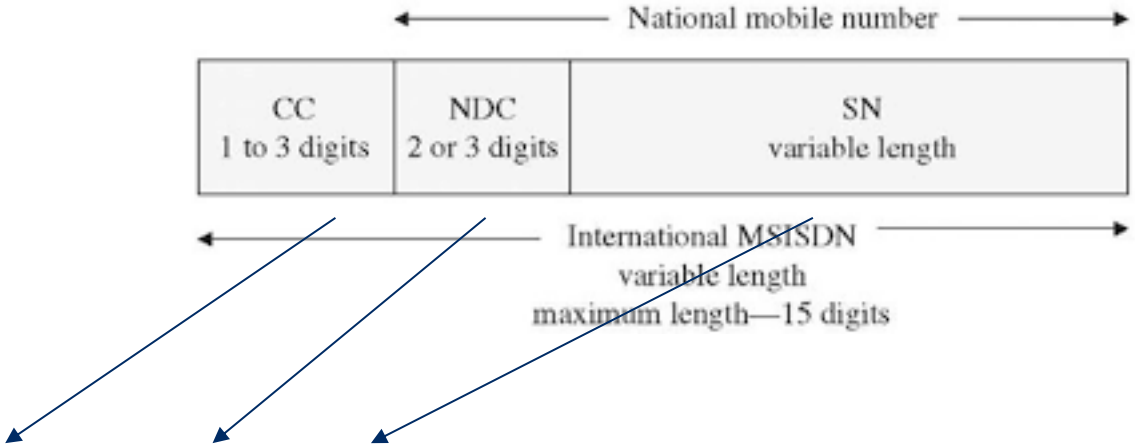
- TAC+FAC+SNR+SP
- TAC=model ratification code, 6 digits
- FAC=factory assembling code, 2 digits
- SNR=sequence code, 6 digits
- SP=reserved, 1 digit (Luhn check)



- On any phone *#06#

Numbering: MSISDN

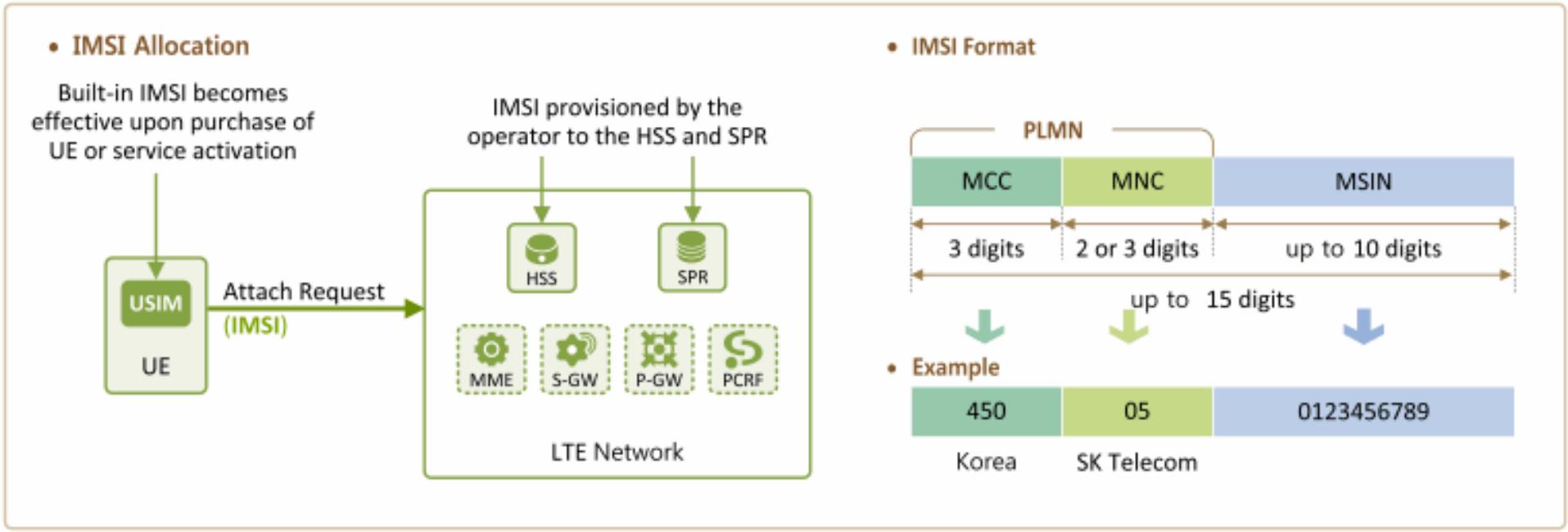
- **Mobile Station International Subscriber Directory Number**



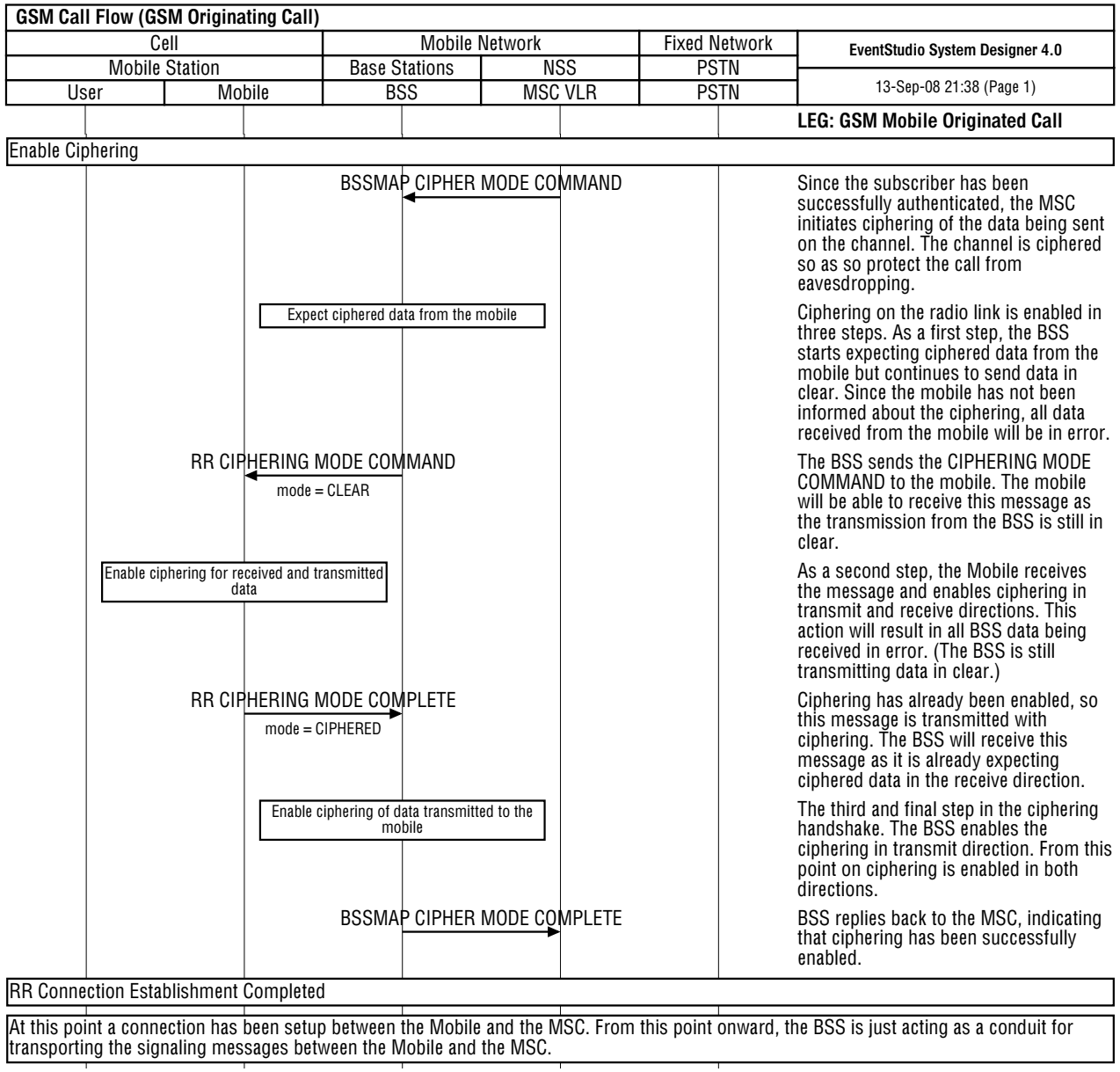
- **e.g. +32 (0)478 21 23 22 (random number!)**

Numbering: IMSI

- **International Mobile Subscriber Identification number: It identifies a unique international universal number of a mobile subscriber, which consists of MCC+MNC+MSIN.**



2G flow (4)



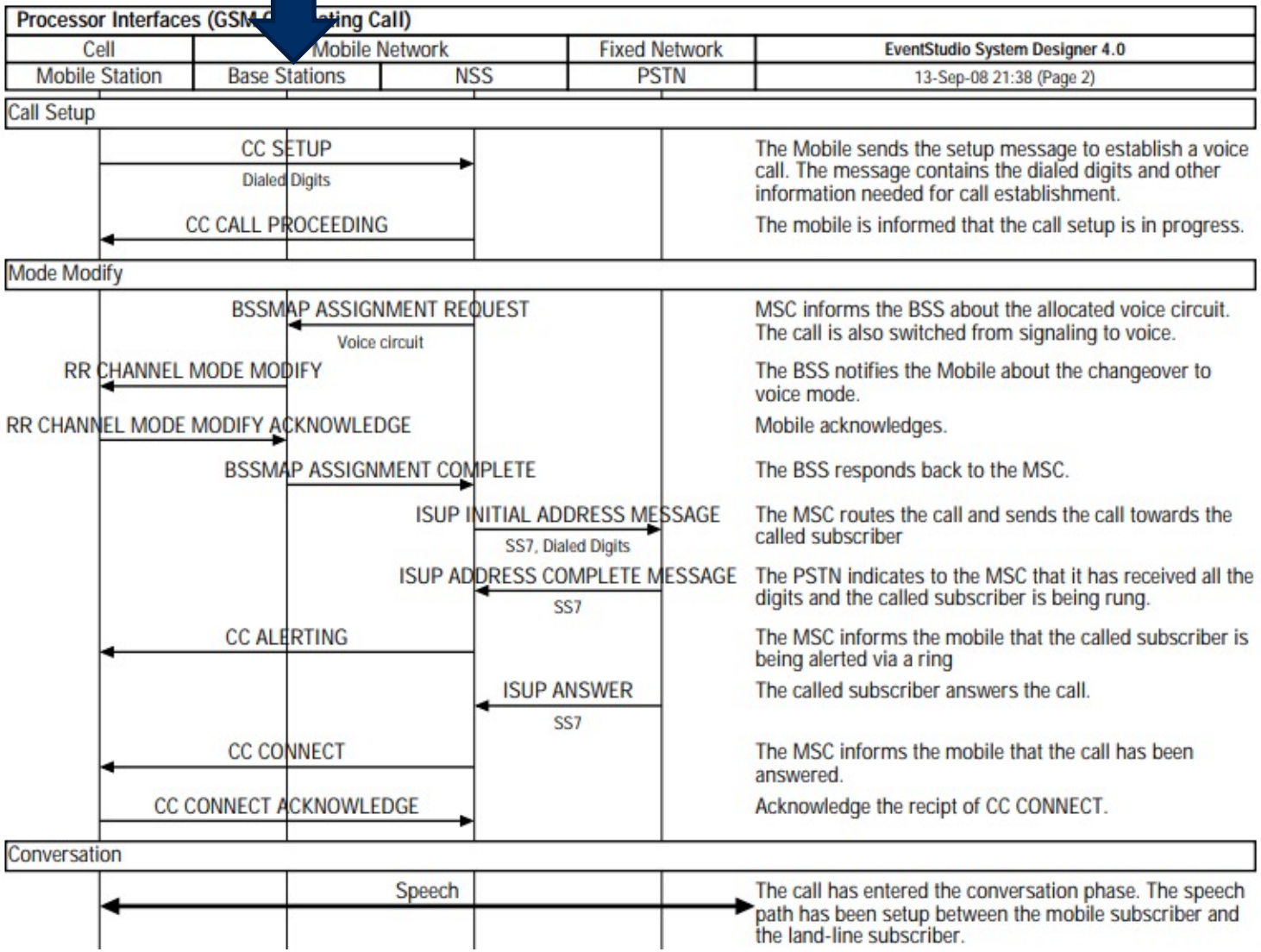
And continues to Call Setup…

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits~~ ~~for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Pick a time to send~~
7. ~~Wait for a response (try again)~~
8. ~~Get a control channel assigned~~
9. ~~Ask to make a call~~
10. ~~Authenticate~~
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

Full Call

Note: less granularity – RAN is just a conduit

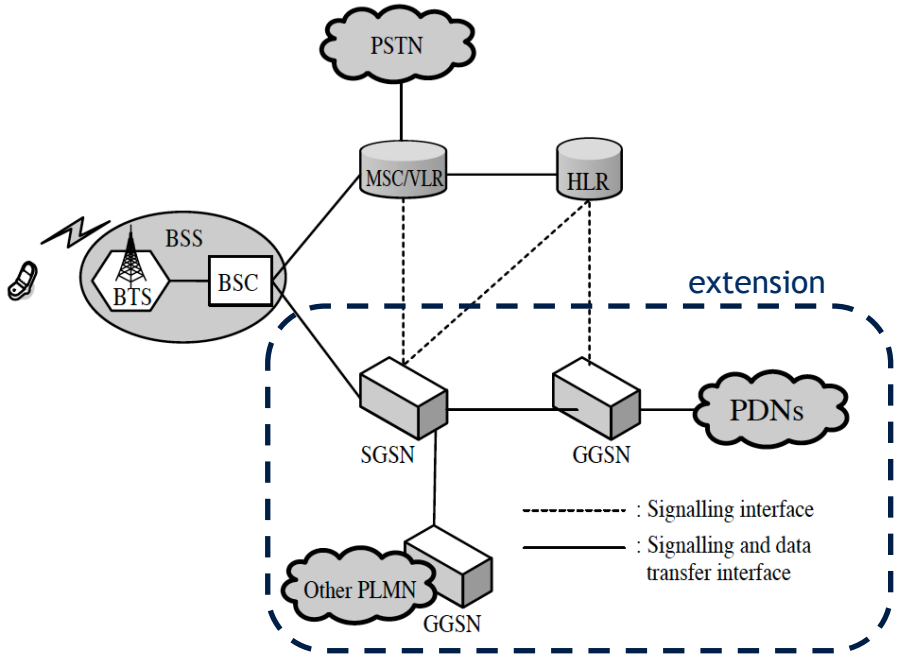


What about data?

- **There is no data except for SMS.**

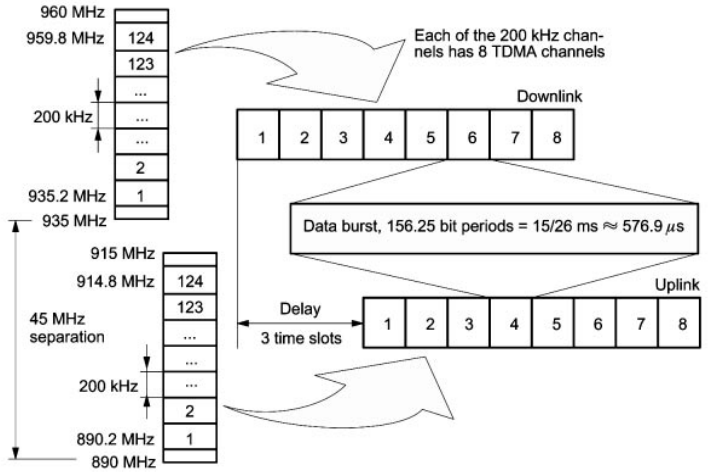
GPRS objectives

- **Internet applications over GSM :**
  - low available bandwidth
  - long connection set-up times
  - inefficient use of radio capacity (bursty traffic)
- **Objectives of GPRS**
  - reduced connection set-up times
  - support of existing packet oriented protocols (X.25, IP)
  - flexible and optimized usage of radio resources



Radio Resource Management

- **Allocation of channels: GSM ≠ GPRS**
  - Single MS can use multiple slots of TDMA frame (up to 8)
  - Uplink and downlink allocation separate to allow asymmetric data traffic (browsing)
  - GPRS channels allocated
    when data is sent or received
    and released afterwards
  - Packet Random Access Channel
    (PRACH) used by MS to request
    one or more data traffic channels
    (PDTCH; new)



SGSN: Serving GPRS Support Node

- SGSN (serving GPRS support node) interfaces between GPRS backbone and radio access network
- Functions of the SGSN
  - packet routing and transfer to correct BSS
  - mobility management (attach/detach, location management)
  - Connection to data bases (HLR, MSC/VLR)
  - ciphering, authentication and charging

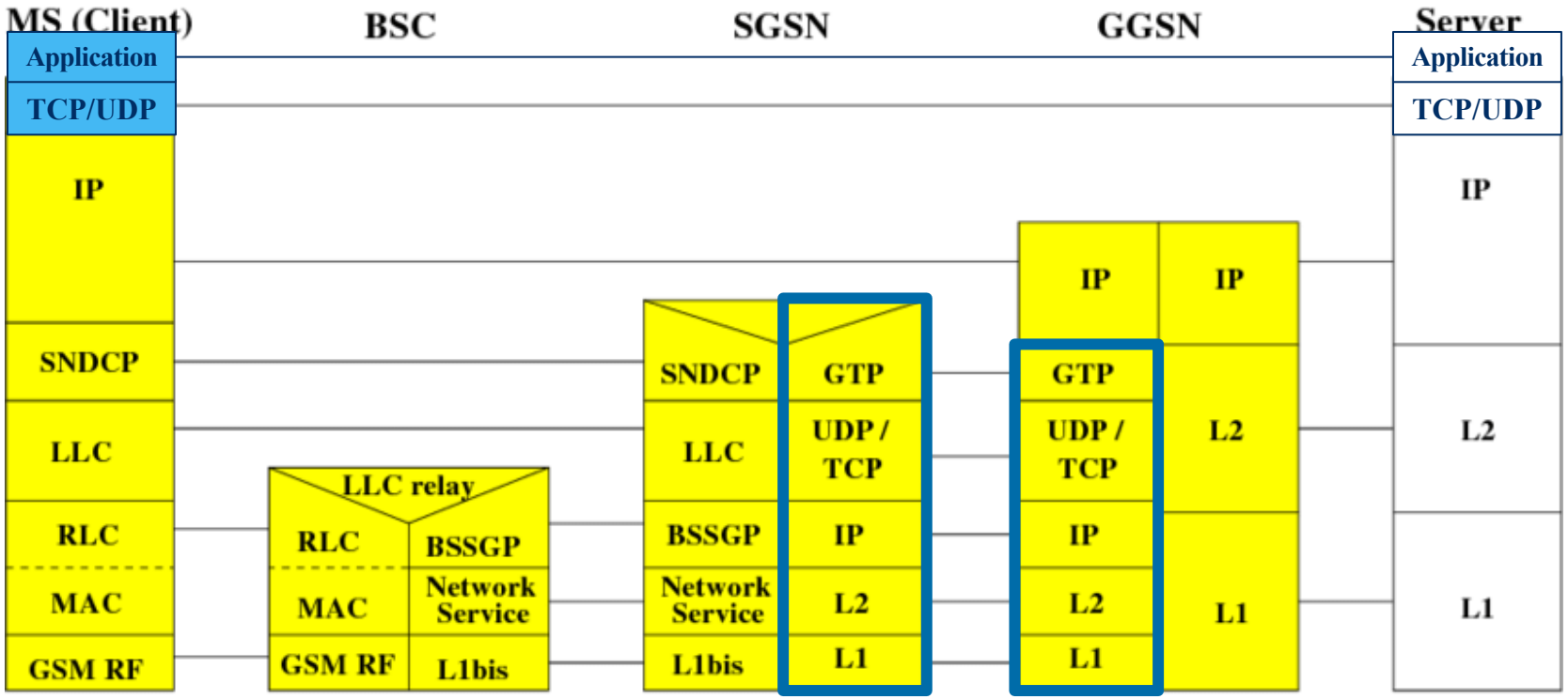
GGSN: Gateway GPRS Support Node

- GGSN (gateway GPRS support node) acts as interface between GPRS backbone network and external PDN
- Functions of GGSN
  - converts GPRS packets into PDP (Packet Data Protocol) format of external PDN (e.g. IP or X.25) and transfers packets
  - PDP addresses are converted to GPRS address of the destination and packets are sent to correct SGSN
  - Authentication and charging functions
  - If PDN is IP network : firewall and packet-filtering mechanisms

GPRS Backbone Protocols

- **GPRS Tunneling Protocol (GTP)**
  - packets are encapsulated and tunneled between GSNs
  - GTP header contains a tunnel point identifier
- **TCP/UDP**
  - used to transport the packets through the backbone (X.25 : TCP; IP : UDP)
- **IP**
  - used to route packets through the backbone
- **Below IP**
  - any of ATM, Ethernet, ISDN

GPRS: the move to IP, TCP/UDP

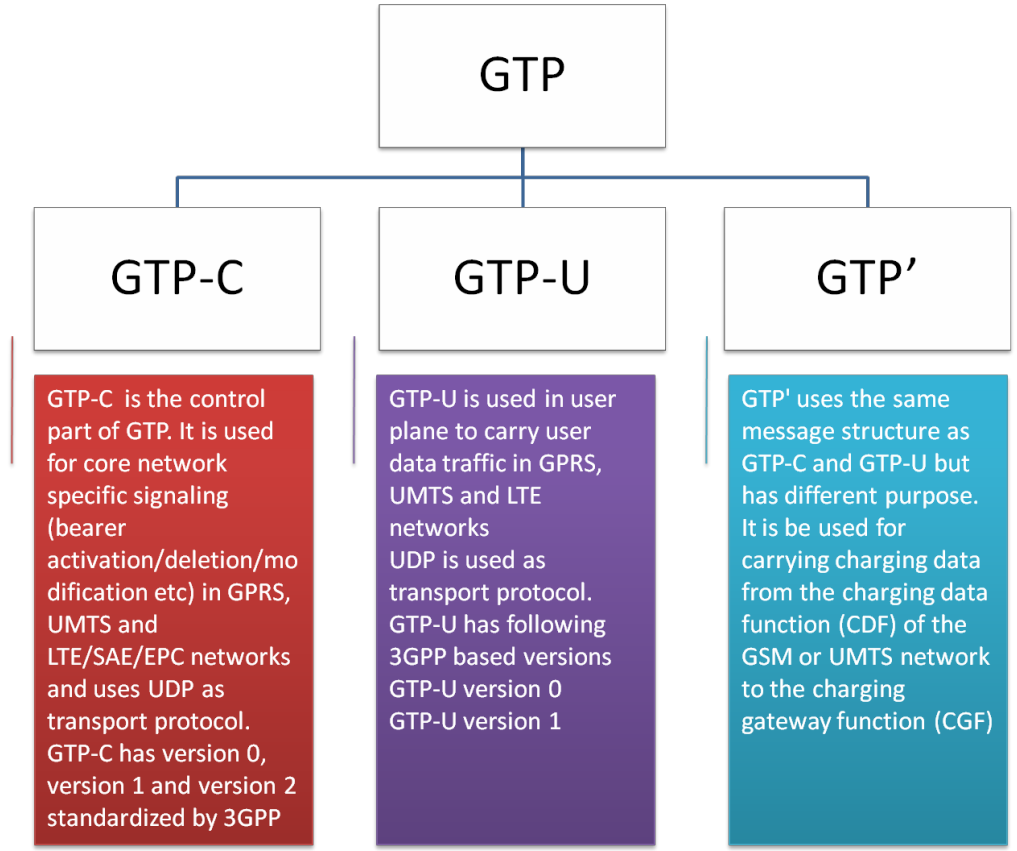


SNDCP: Subnetwork Dependent Convergence Protocol
LLC: Logical Link Control
RLC: Radio Link Control

MAC: Medium Access Control
GSM RF: GSM Radio Frequency
BSSGP: BSS Gateway Protocol

GTP: GPRS Tunnel Protocol
L1, L2: OSI protocol layers 1 and 2
IP: Internet Protocol (version 4 or 6)

3GPP Mobile networks tunnel TCP/IP via



3. 2G to 5G

(concepts & toy examples)

Remember ITU-R?

World Radiocommunication Conference (WRC)
Revises the Radio Regulations

	Rec. ITU-R M.1645 (IMT-2000/IMT-Advanced)	Rep. ITU-R M.2134 (IMT-Advanced)	Rec. on Vision (IMT-2020)
Year of approval	2003	2008	2015
Mobile terminal mobility	250 km/h	350 km/h	500 km/h
Peak transmission rate	0.1–1 Gbit/s	1 Gbit/s	20 Gbit/s
User throughput	–	10 Mbit/s	0.1–1 Gbit/s
Mobile terminal density	–	10^5/km^2	10^6/km^2
Radio link latency	–	10 ms	1 ms
Power efficiency (/bit)	–	–	100 times that of IMT-Advanced
Spectrum use efficiency	–	–	2–5 times that of IMT-Advanced
Area traffic capacity	–	0.1 Mbit/s/m^2	10 Mbit/s/m^2

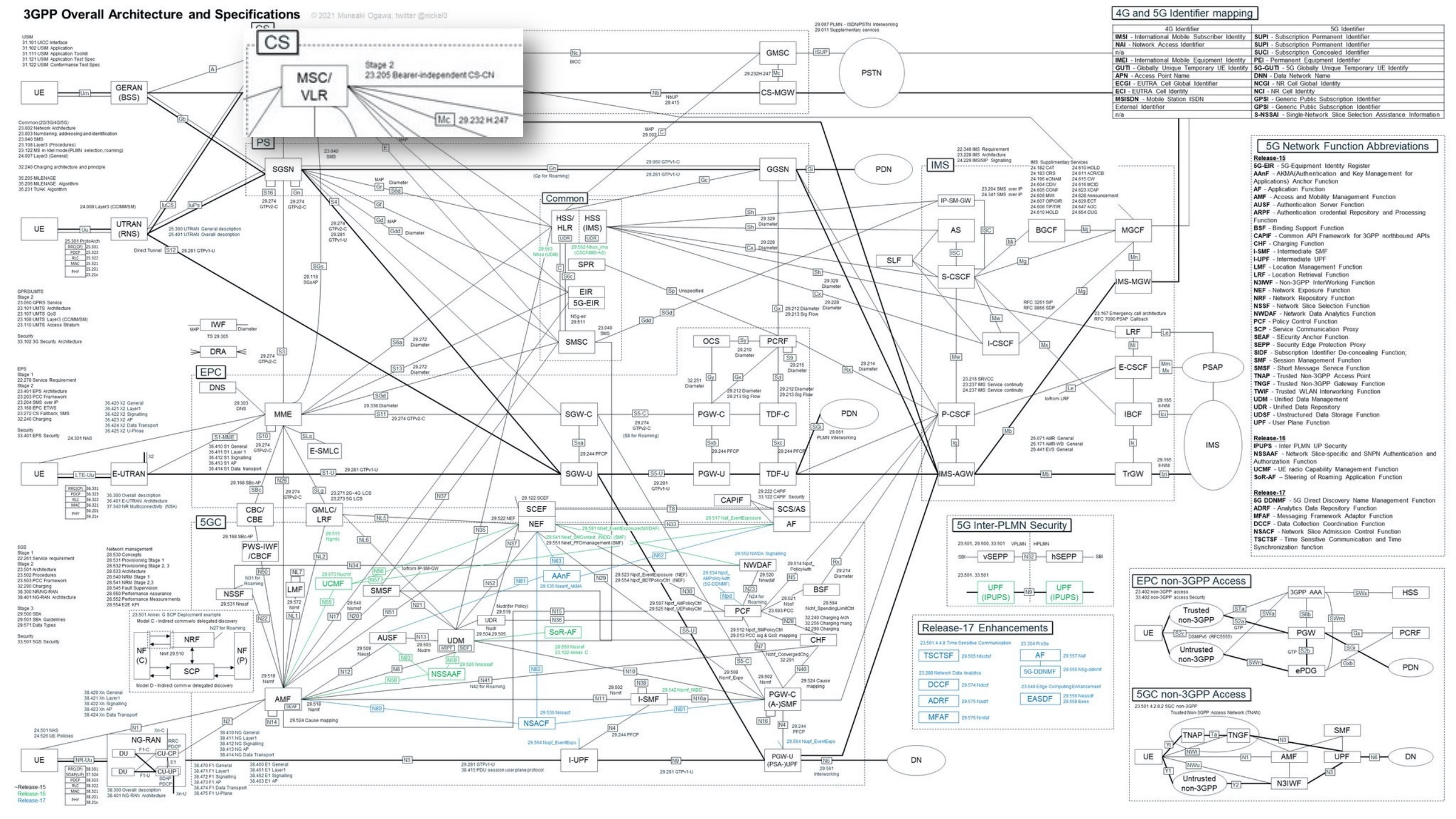
"3G" "4G" "5G"

Bureau

	Scope of Work
WP 5A	Land mobile service above 30 MHz (excluding IMT); wireless access in fixed services; amateur and amateur-satellite services
WP 5B	Maritime mobile service including Global Maritime Distress and Safety System (GMDSS); aeronautical mobile service and radiodetermination service
WP 5C	Fixed wireless systems; HF and other systems below 30 MHz in fixed and land mobile services
WP 5D	IMT systems

	Scope of work
SG 1: Spectrum management	Spectrum management principles and techniques, general principles of sharing and spectrum monitoring
SG 3: Radiowave propagation	Propagation of radio waves in ionized and non-ionized media, and the characteristics of radio noise
SG 4: Satellite services	Systems and networks for fixed-satellite, mobile-satellite, broadcasting-satellite, and radiodetermination-satellite services
SG 5: Terrestrial services	Systems and networks for fixed, mobile, radiodetermination, amateur, and amateur-satellite services
SG 6: Broadcasting service	Radiocommunication broadcasting including vision, sound, multimedia, and data services principally intended for delivery to the general public
SG 7: Science services	Systems for space operation, space research, earth exploration and meteorology; systems for remote sensing including passive and active sensing systems, radio astronomy, and standard frequency and time signals

3GPP Overall Architecture and Specifications



4G and 5G Identifier mapping

4G Identifier	5G Identifier
IMSI - International Mobile Subscriber Identity	**SUPI** - Subscription Permanent Identifier
NAI - Network Access Identifier	**SUPI** - Subscription Permanent Identifier
n/a	**SUCI** - Subscription Concealed Identifier
IMEI - International Mobile Equipment Identity	**PEI** - Permanent Equipment Identifier
GUTI - Globally Unique Temporary UE Identity	**5G-GUTI** - 5G Globally Unique Temporary UE Identity
APN - Access Point Name	**DNN** - Data Network Name
ECGI - EUTRA Cell Global Identifier	**NCGI** - NR Cell Global Identity
ECI - EUTRA Cell Identity	**NCI** - NR Cell Identity
MSISDN - Mobile Station ISDN	**GPSI** - Generic Public Subscription Identifier
External Identifier	**GPSI** - Generic Public Subscription Identifier
n/a	**S-NSSAI** - Single-Network Slice Selection Assistance Information

5G Network Function Abbreviations

Release-15

5G-EIR - 5G-Equipment Identity Register
AAnF - AKMA(Authentication and Key Management for Applications) Anchor Function
AF - Application Function
AMF - Access and Mobility Management Function
AUSF - Authentication Server Function
ARPF - Authentication credential Repository and Processing Function
BSF - Binding Support Function
CAPIF - Common API Framework for 3GPP northbound APIs
CHF - Charging Function
I-SMF - Intermediate SMF
I-UPF - Intermediate UPF
LMF - Location Management Function
LRF - Location Retrieval Function
N3IWF - Non-3GPP InterWorking Function
NEF - Network Exposure Function
NRF - Network Repository Function
NSSF - Network Slice Selection Function
NWDAF - Network Data Analytics Function
PCF - Policy Control Function
SCP - Service Communication Proxy
SEAF - SEcurity Anchor Function.
SEPP - Security Edge Protection Proxy
SIDF - Subscription Identifier De-concealing Function;
SMF - Session Management Function
SMSF - Short Message Service Function
TNAP - Trusted Non-3GPP Access Point
TNGF - Trusted Non-3GPP Gateway Function
TWIF - Trusted WLAN Interworking Function
UDM - Unified Data Management
UDR - Unified Data Repository
UDSF - Unstructured Data Storage Function
UPF - User Plane Function

Release-16

IPUPS - Inter PLMN UP Security
NSSAAF - Network Slice-specific and SNPN Authentication and Authorization Function
UCMF - UE radio Capability Management Function
SoR-AF - Steering of Roaming Application Function

Release-17

5G DDNMF - 5G Direct Discovery Name Management Function
ADRF - Analytics Data Repository Function
MFAF - Messaging Framework Adaptor Function
DCCF - Data Collection Coordination Function
NSACF - Network Slice Admission Control Function
TSCTSF - Time Sensitive Communication and Time Synchronization function

5G Inter-PLMN Security

Release-17 Enhancements

EPC non-3GPP Access

5GC non-3GPP Access

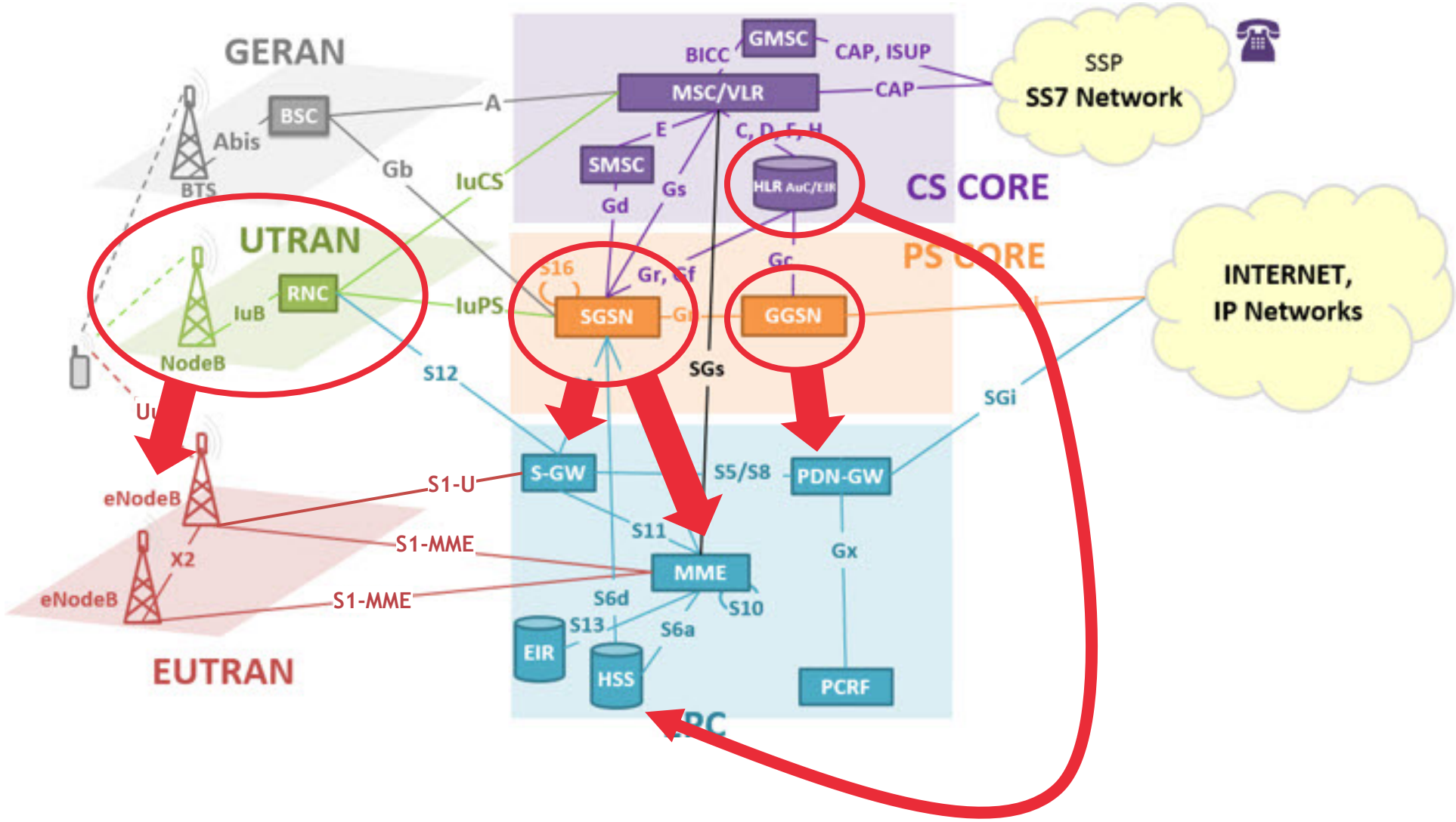
Release-15
Release-16
Release-17

Historical evolution

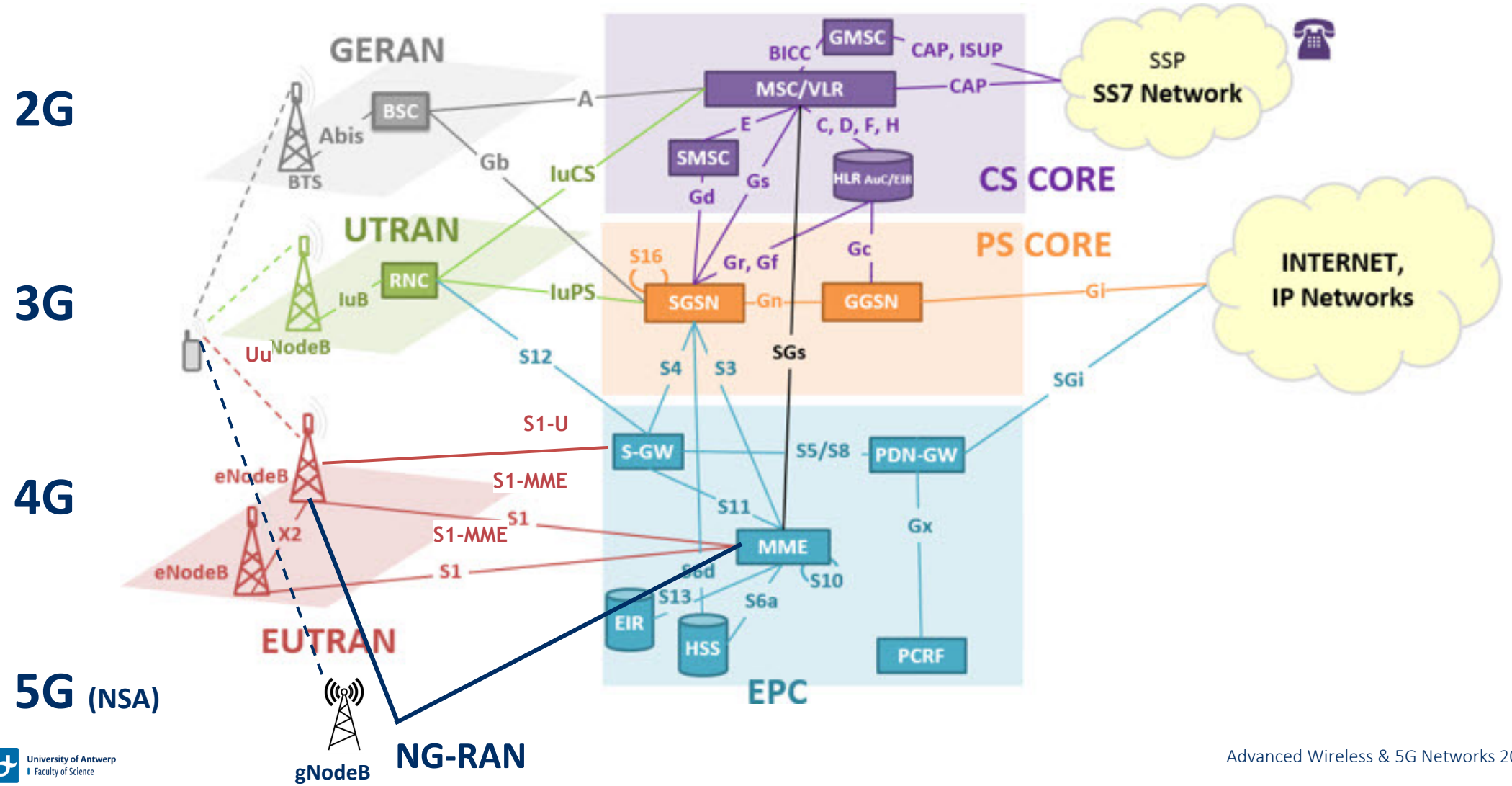
2G

3G

4G



The 3GPP Universe: from GPRS to …



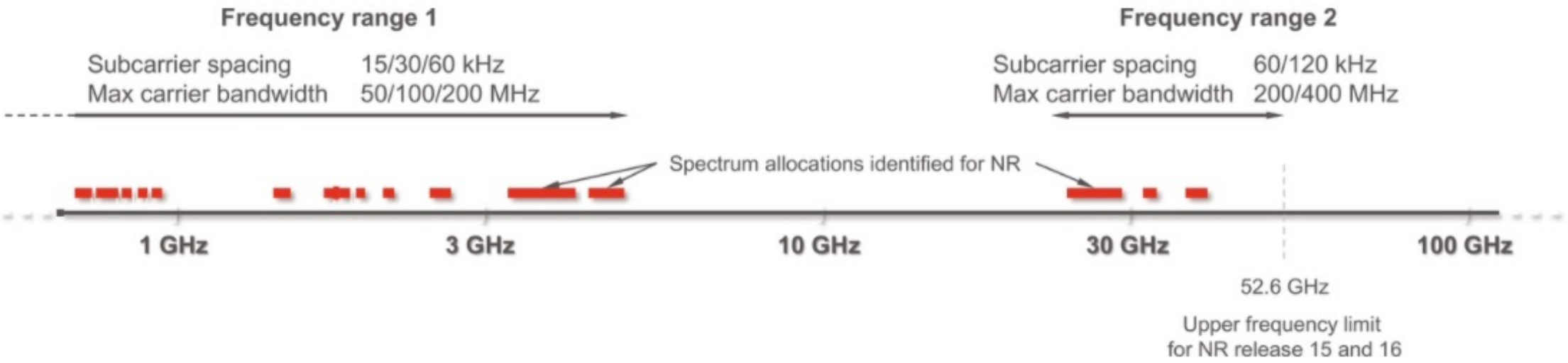
What are the steps?

1. Switch on the mobile (& infrastructure)
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel
8. Authenticate
9. Ask to send data (or get some data)
10. Ask to make a call
11. Move around
12. … (location update, release call, handover, etc …)

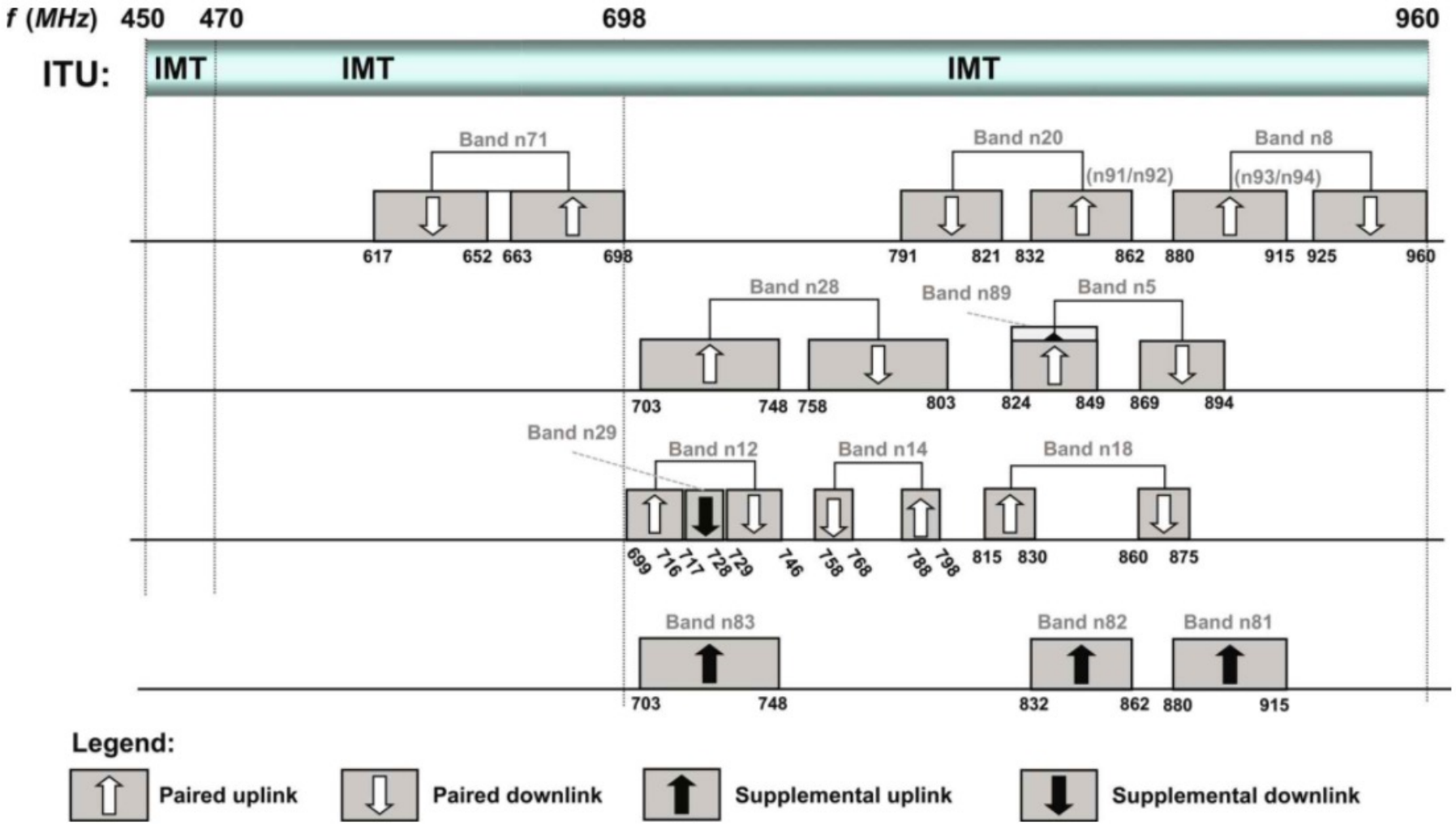
What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel
8. Authenticate
9. Ask to send data (or get some data)
10. Ask to make a call
11. Move around
12. … (location update, release call, handover, etc …)

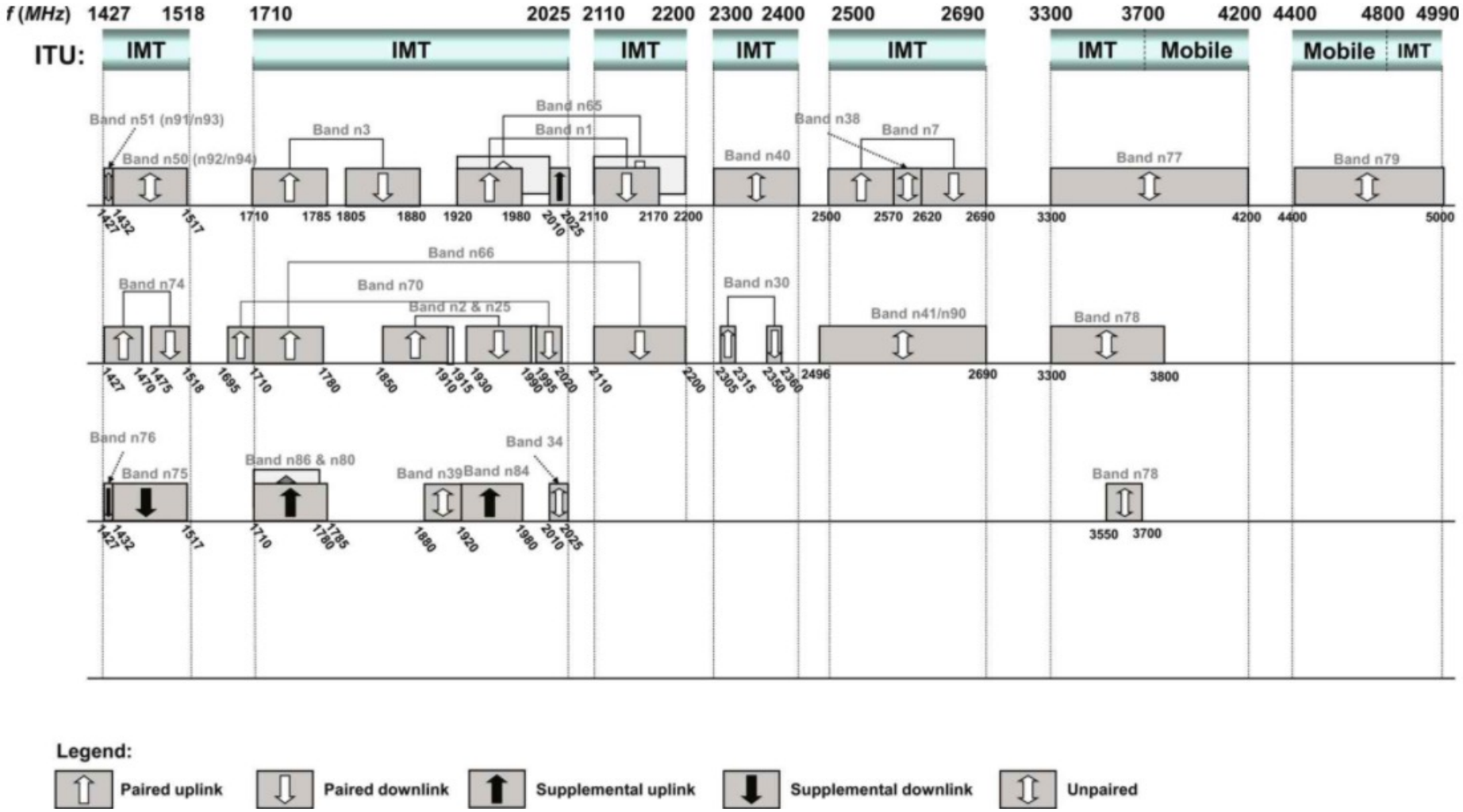
Frequency Ranges for NR



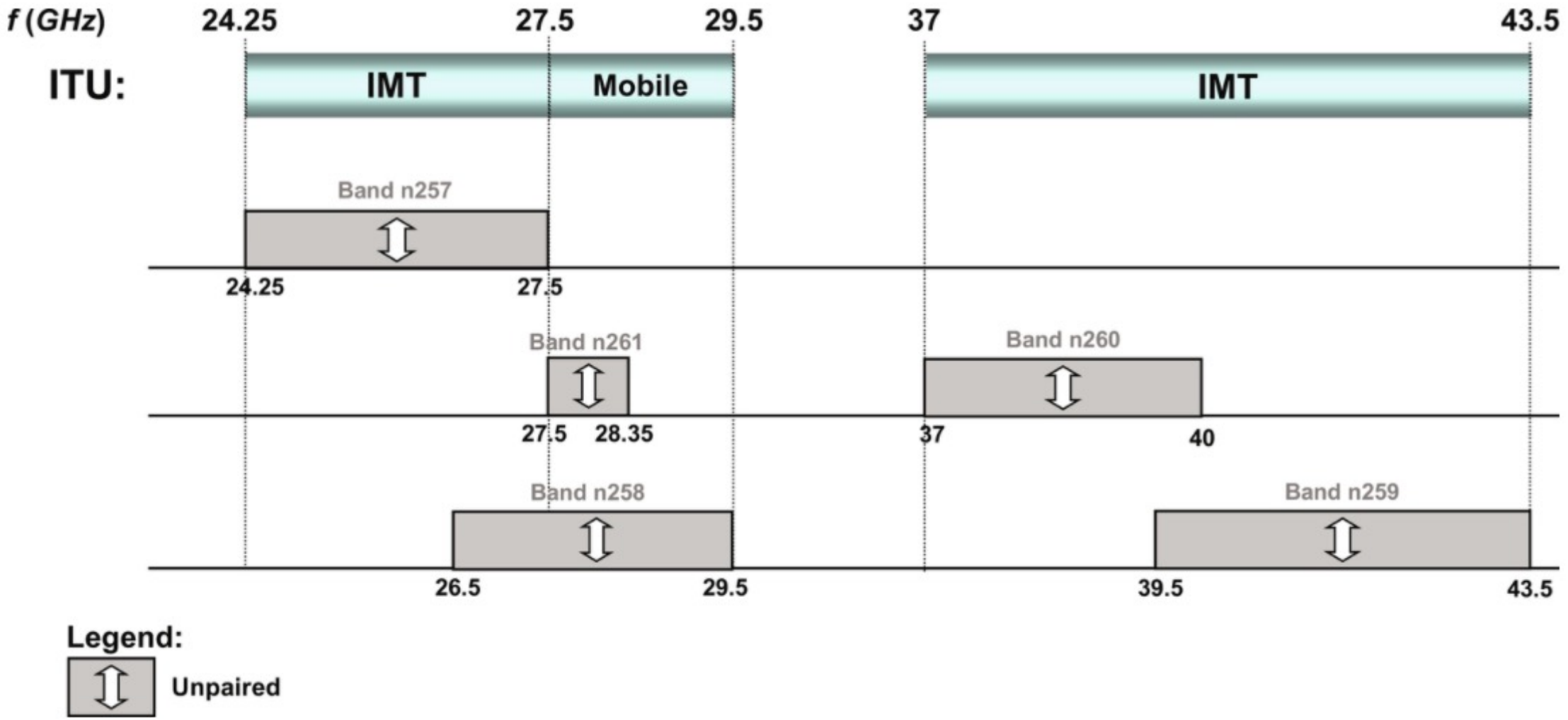
FR1 below 1 GHz



FR1 up to 6 GHz



FR2 from 26GHz to 52GHz



Refresher (1)

FREQUENCY

- The number of crests that pass a given point within one second is described as the frequency of the wave. One wave—or cycle—per second is called a Hertz (Hz), after Heinrich Hertz who established the existence of radio waves. A wave with two cycles that pass a point in one second has a frequency of 2 Hz.

WAVELENGTH

- Electromagnetic waves have crests and troughs similar to those of ocean waves. The distance between crests is the wavelength. The shortest wavelengths are just fractions of the size of an atom, while the longest wavelengths scientists currently study can be larger than the diameter of our planet!

ENERGY

- An electromagnetic wave can also be described in terms of its energy—in units of measure called electron volts (eV). An electron volt is the amount of kinetic energy needed to move an electron through one volt potential. Moving along the spectrum from long to short wavelengths, energy increases as the wavelength shortens. Consider a jump rope with its ends being pulled up and down. More energy is needed to make the rope have more waves.

Refresher (2)

- **bandwidth**—the range of a channel's limits; the broader the bandwidth, the faster data can be sent
- **bits per second (bps)**—a single on-off pulse of data; eight bits are equivalent to one byte
- **frequency**—the number of cycles per unit of time; frequency is measured in hertz (Hz)
- **kilo (k)**—kilo is the designation for 1,000; the abbreviation kbps represents 1,000 bits per second
- **megahertz (MHz)**—1,000,000 hertz (cycles per second)
- **milliseconds (ms)**—one-thousandth of a second
- **watt (W)**—a measure of power of a transmitter

$$\Delta P_{dB} = 10\log_{10}\frac{P_2}{P_1} = 20\log_{10}\frac{A_2}{A_1}$$

$$P_{dBm} = 10\log_{10}\frac{P}{1\text{mW}}$$

$$c = v_{light} = 300.000 \text{ km/s}$$

$$= 300 \text{ km/ms} = \frac{\lambda}{f}$$

- **frequency band**—The frequency range specified for GSM is 1,850 to 1,990 MHz (mobile station to base station).
- **duplex distance**—The duplex distance is 80 MHz. Duplex distance is the distance between the uplink and downlink frequencies. A channel has two frequencies, 80 MHz apart.
- **channel separation**—The separation between adjacent carrier frequencies. In GSM, this is 200 kHz.
- **modulation**—Modulation is the process of sending a signal by changing the characteristics of a carrier frequency. This is done in GSM via Gaussian minimum shift keying (GMSK).
- **transmission rate**—GSM is a digital system with an over-the-air bit rate of 270 kbps.
- **access method**—GSM utilizes the time division multiple access (TDMA) concept. TDMA is a technique in which several different calls may share the same carrier. Each call is assigned a particular time slot.
- **speech coder**—GSM uses linear predictive coding (LPC). The purpose of LPC is to reduce the bit rate. The LPC provides parameters for a filter that mimics the vocal tract. The signal passes through this filter, leaving behind a residual signal. Speech is encoded at 13 kbps.