Table of Contents

SEMINAR

- General
  - Standarts
  - Migration
  - bandAndCat
- CellConsepts
  - bandAndCat
  - frqReuse
  - cellUnit
  - capacity
  - segments
  - ms
  - handovers
  - roaming
- RadioConsepts
  - propagation
  - attenuation
  - dopler
  - snr
  - multiPath
  - intreSymbol
  - transmission
  - channelCoding
  - interleaving
- SIM
  - content
  - imsi
  - timsi
  - ptimsi
  - uicc
  - usim
  - isim
  - embedsim
  - euicc
- 2G
  - Arch
- lteProtocol
  - ueCAT

General Cellular staff

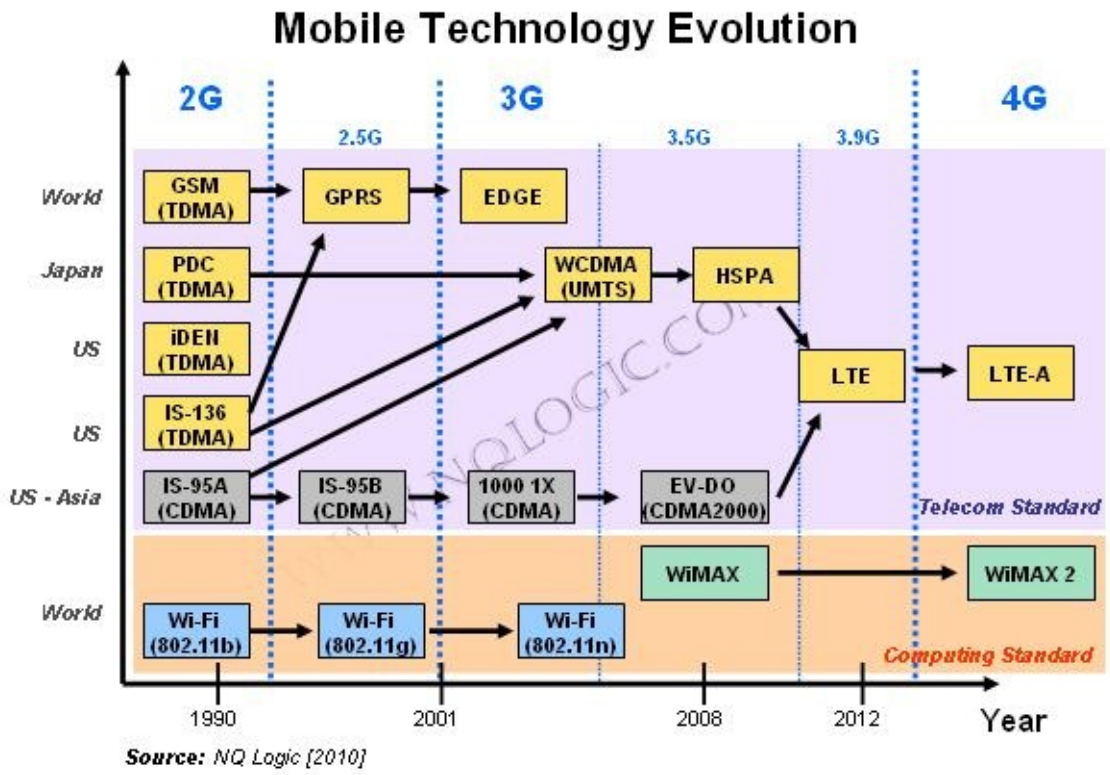
Standardization

- ITU
- IMT2000
- 3GPP (1&2)

```
3GPP now encompasses seven SDOs:
  ETSI (Europe and rest of world),
  ATIS (USA),
  ARIB and TTC (Japan),
  TTA (South Korea),
  CCSA (China)
  TSDSI (India)
```

migration

- 1G - analog voice
- 2G - Digital Voice ; GSM / CDMA
- 2.5G - Packet data ; GPRS / CDMA-1xRTT
- 2.75 - inetrmidiata multimedia ;
- 3G - multimedia ; UMTS-HSPA / CDMA2000-EVDO
- 4G - ; LTE / NR
- 5G - ALl ip



Release Band and Cat

- user equipment define it category
- each category is defined in 3gpp release
- since rel-12 there may be separate downlink and uplink catergory
- since rel-12 there is NB categories for iot

Release

- releases map
- release to generation

band

TBD

cat

- catList
- lpwan
- iotCats
- how to read UE cat

short summary

- ue basic categories form 0 to 16
- rel13 DL : cat 17-19
- rel14 DL : cat 20-21

for iot:

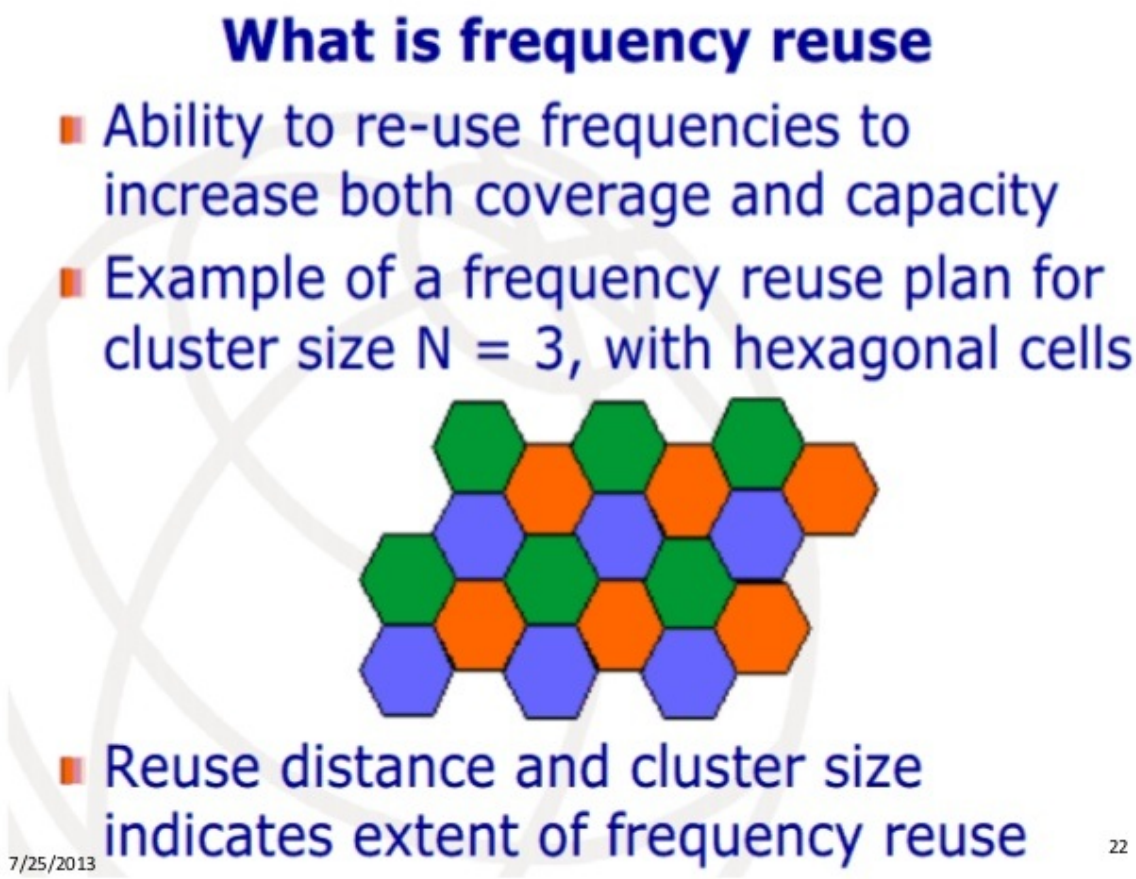
- cat 1 - rel8 - (LTE) - (;dw10Mbit/s;up5Mbit/s) (1.25-0.75 Mb/s)
- cat 4 - rel8 - (LTE) - (20Mhz;dw150Mbit/s;up50Mbit/s) (18.75-6.25 MB/s)
- cat 0 - rel12 - (LTE-ADVANCED) - (20Mhz; dw1Mbit/s;up1Mbit/s) (0.125 MB/s)
- cat M1 -rel13 - (LTE-ADVANCED) - (1.4Mhz;dw1Mbit/s;up1Mbit/s) (0.125 MB/s)
- cat M2 -rel14 - (LTE-ADVANCED-PRO) (5Mhz;dw4Mbit/s;up7Mbit/s) (0.5-0.8Mb/s)
- cat NB1-rel13 - (LTE-ADVANCED) - (200Khz;dw26kbit/s;up66kbit/s)
- cat NB2-rel14 - (LTE-ADVANCED-PRO)(200Khz;dw200kbit/s;up200kbit/s) (0.025 MB)

Consepts

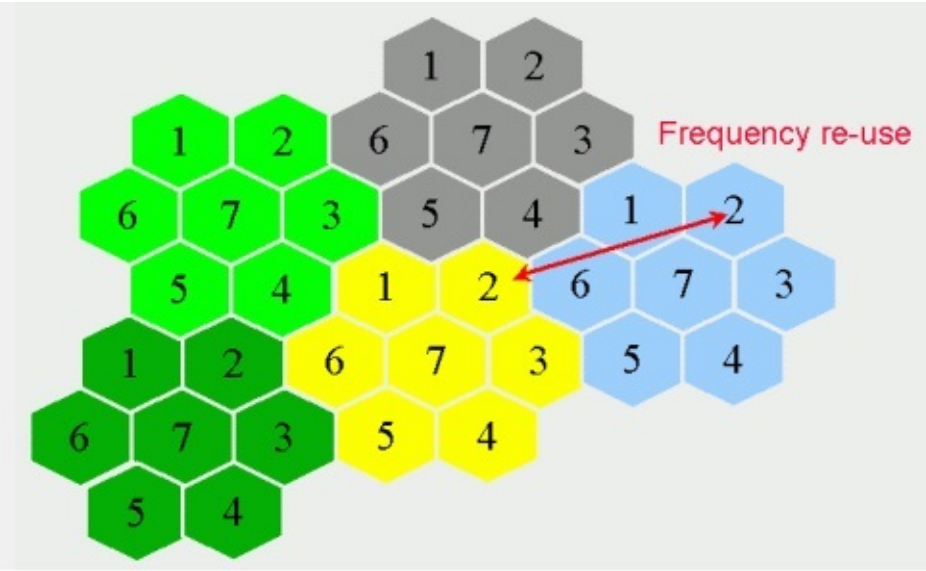
- bandAndCat

Frequency Reuse

reuse 3



reuse 7



Cell UNIT

TBD

method to increse capacity

Frequency borrowing

- assign freq dynamically

Cell Splitting

- smaller cell in high density aread

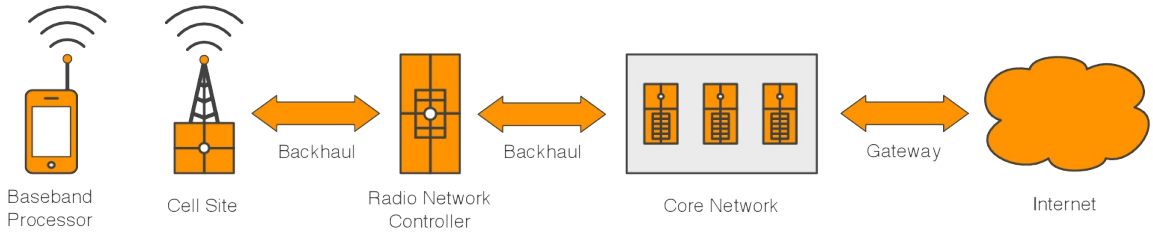
Cell Sectoring

- divide cell into sectors

Small Cells

- move cells from hills to buildings

Cellular network segments



Mobile station equipment

- portabel
- iniquely identified by IMEI
- voice and data transmission
- monitor power and signal of surrounding cells
- sms

Handovers

TBD

Radio Concepts

Propagation

- direct radiation
- reflection
- diffraction
- scattering

Attenuation

pass loss

- loss in large scope of the spread

slow fading

- loss due to buillding and hills

fast fading

- decline rapidly in a few dozens wavelength path
- rayleigh distribution - non line pf sight
- Rice distirbuition - line of sight

Dopler

SNR -Signal to Noise Ratio

Multi path propagation

Inter Symbil Interference

Transmission Procedure

Channel Coding

purpose

- adding redundant information - detect and correct error signal
- error correction

principle

- convolutional coding
- turbo coding
- increase redundancy and transmission time

Interleaving

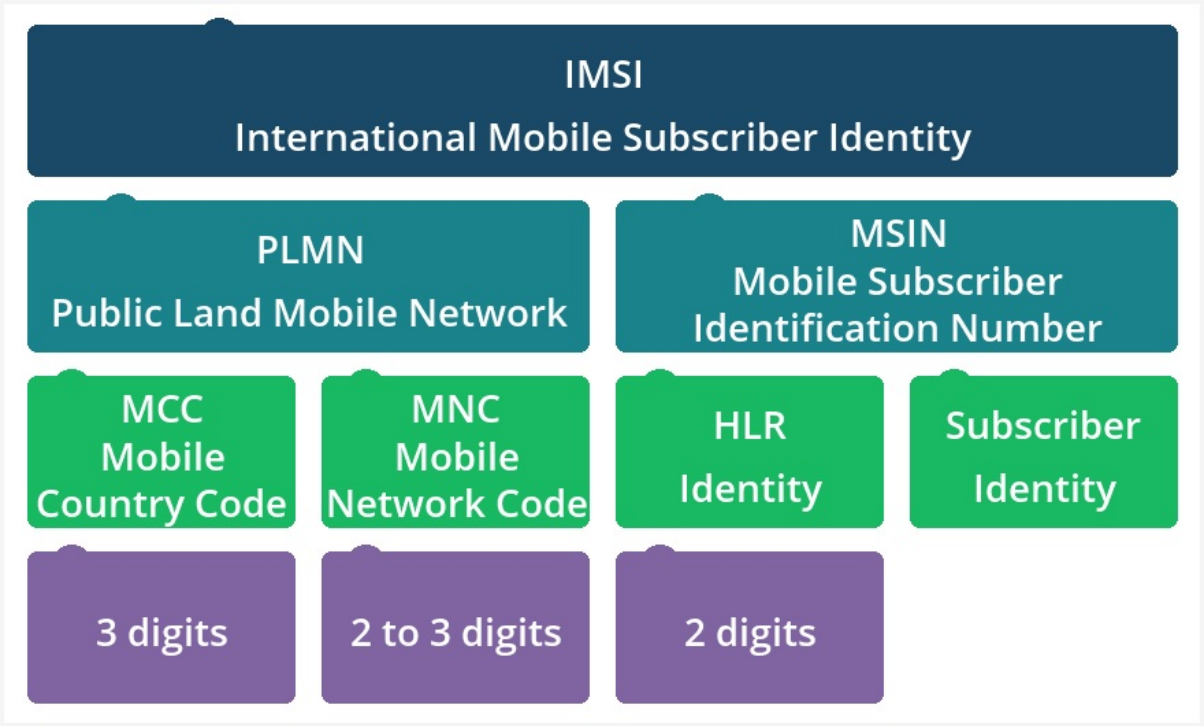
SIM - Subscripber Identity Module

- euicc

Sim Content

- IMSI - International Mobile Subscriber Identify
- Encryption keys
- TMSI - Temporary Mobile Subscriber Identify
- MSISDN - phone number
- card protection pin (4-8 digits)
- Roaming Data
- SMS msgs
- personal data like phone bumbers and settings

IMSI


IMSI
International Mobile Subscriber Identity
PLMN
Public Land Mobile Network
MSIN
Mobile Subscriber
Identification Number
MCC
Mobile
Country Code
MNC
Mobile
Network Code
HLR
Identity
Subscriber
Identity
3 digits
2 to 3 digits
2 digits

TMSI

- The TIMSI (Temporary IMSI) is a pseudo-random number generated from the IMSI (International Mobile Subscriber Identity) number.
- The TIMSI is utilized in order to remove the need to transmit the IMSI over-the-air. This helps to keep the IMSI more secure.
- To track a GSM user via the IMSI/TIMSI, an eavesdropper must intercept the GSM network communication where the TIMSI is initially negotiated. In addition, because the TIMSI is periodically renegotiated, the eavesdropper must intercept each additional TIMSI re-negotiation session.
- used in CS domain allocated by VLR
- timsi has only local significane withing a VLR and the area controlled by a VLR

PTMSI

- used on PS domain , allocated by SGSN
- has only local significance

UICC - universal intergrated circuit card

- platform to store multi applications (like usim)
- NAA (Network Access Application) defined for UICC:
  - USIM
  - ISIM

USIM

- Universal subscriber identity module

ISIM

- IP-multimedia subsystem subscriber identity module

Embedded SIM

- alowing over the air provisioning
- change sybscription from one operator to another

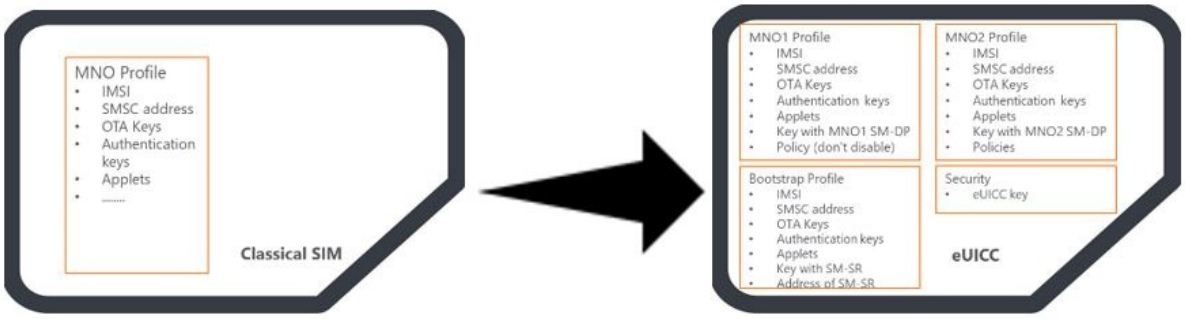
eUICC

links

- https://www.gsma.com/newsroom/resources/?kw=sgp
- https://www.youtube.com/watch?v=wIXXkRervh8
- https://www.avnet.com/wps/portal/silica/products/new-products/npi/avnet-euicc/

about

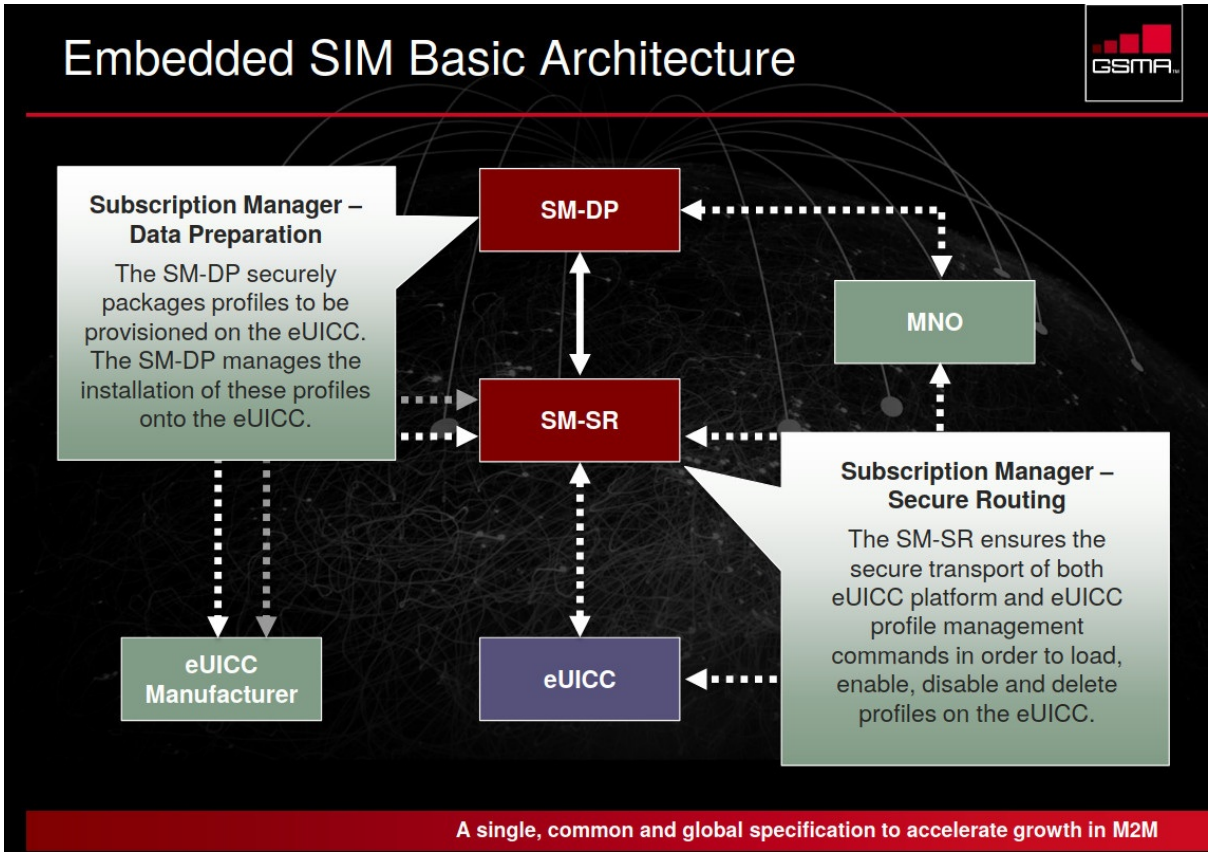
- eSIM specifications from the GSMA describe two main components: the eUICC (embedded UICC) which is considered as the next evolution of the SIM cards and the Subscription Management platform (SM).
- eUICC can store multiple operator profiles instead of only one.
- eSIM architecture enables over-the-air replacement of the mobile network operator (MNO) profile (virtual SIM)
- eUICCs can be manufactured with just a bootstrap profile that enables the customer’s device to connect to subscription management (SM) platform



Classical SIM vs. eUICC

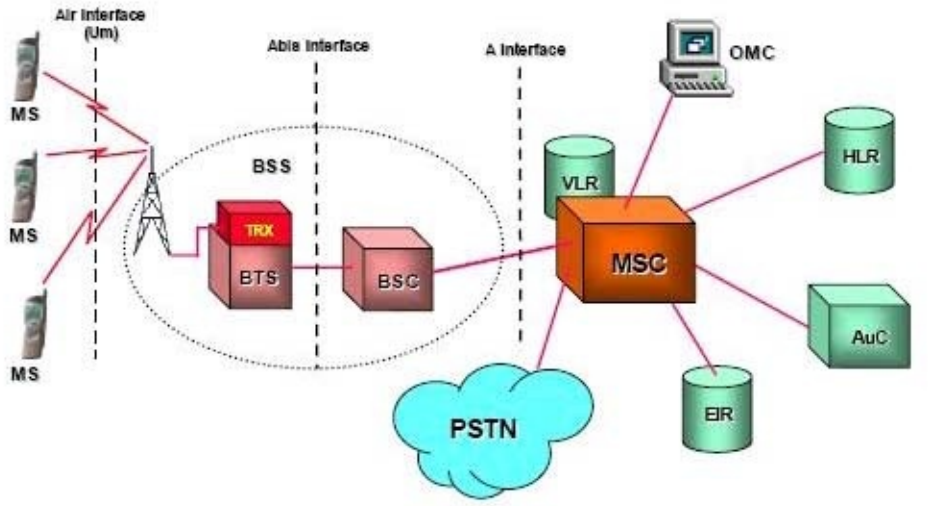
SM

- subscription Management platform
- consists of two components: Subscription Management Secure Routing (SM-SR) and the subscription Management Data Preparation (SM-DP).
- the vendor of the eUICC registers the card (e.g., certificate, identity) at the SM-SR
- The SM-SR is the only entity that can contact the eUICC for the purpose of subscription management directly and maintains a secure connection to the eUICC
- SM-SR enforce the Profile policies (allow disablement of a profile) and route the commands from the MNO and SM-DP to the eUICC
- SM-DP has a secure connection to the SM-SR and is responsible for preparing and saving the MNO profiles in a format compatible with the eUICC


Embedded SIM Basic Architecture
GSMA
Subscription Manager – Data Preparation
The SM-DP securely packages profiles to be provisioned on the eUICC. The SM-DP manages the installation of these profiles onto the eUICC.
SM-DP
MNO
SM-SR
Subscription Manager – Secure Routing
The SM-SR ensures the secure transport of both eUICC platform and eUICC profile management commands in order to load, enable, disable and delete profiles on the eUICC.
eUICC Manufacturer
eUICC
A single, common and global specification to accelerate growth in M2M

2g

2G Architecture



layers

- transport plane (voice)
- signaling plane (ss7)

parts:

- ms - mobile equipment
- BTS - base transceiver station
- BSC - base station controller
- bss - bts + bsc = base system subsystem
- msc - mobile service switching controller
  - hlr : home location register
  - vlr : visitor location register
  - eir : equipment identity register
  - gmsc : gateway MSC
  - auc : authentication center
  - smsc : short sms center
- pstn :

BSS

- communicate over standard ABIS interface
- allow communication over different vendors

BTS

- encode / encrupt / multiplexes / modulates / feeds the RF signal
- communicate with mobule station and BSC

- consist of TRx units

BSC

- manage radio resources of bts
- assign freq and time slots for all MS
- call set up
- handover
- radio power controller
- communicate with msc and BTS

MSC

- ran to core interface
- perform switching and signaling
- call setup
- call routing
- billing
- communication between GSM and other networks
- mobility management
- gateway functionality

HLR

- db of mobile subscribers
- identification
  - imsi / msisdn
  - ms category
- service
  - roaming restrictions
  - services (call forward)
- security
  - authentication and encruption keys
- location
  - VLR
  - MSC
  - roaming data - MSRN (mobile subscriber roaming net)

VLR

- temporary db
- asssign tmsi
- less quires to hlr

AUC

- secure data of subscriber (identity and keys)
- algorithms for generating authentication

EIR

- validate mobile equipment hardware identity
- manage ms status list
  - black list
  - gray list
  - white list

LTE PROTOCOL

UE category

- https://www.sharetechnote.com/html/LTE_Advanced_UE_Category.html#RRC_Message
- https://www.sharetechnote.com/html/Handbook_LTE_RRC_IE_UE_Capability.html

```
ueCapabilityInformation-r8

    ue-CapabilityRAT-ContainerList: 2 items

        Item 0

            UE-CapabilityRAT-Container

                rat-Type: eutra (0)

                ueCapabilityRAT-Container:

                UE-EUTRA-Capability

                    accessStratumRelease:

                    ue-Category: X           //!!!!!!!!!!!!!!!!!!!!!!!!//
```