ICT 9025

Mobile Applications & Technologies

Wireless Networks: GSM and GPRS

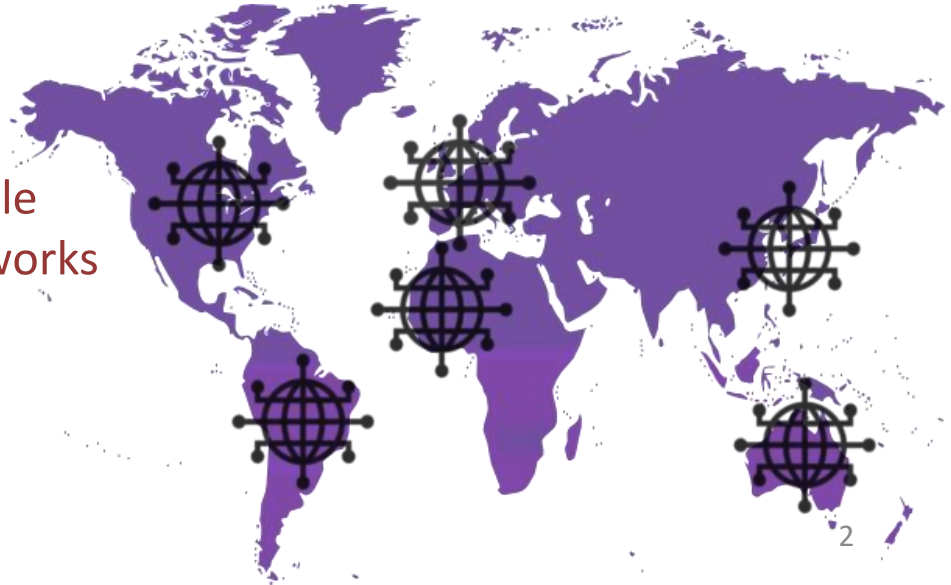
Lecture 2

Phyela Mbewe
LIS Department
University of Zambia

GSM History

- 1979:
  - Various mobile radio networks already established
    - However, the networks used different frequency bands (ranges) and different protocols
    - The networks were not compatible with each other

For example:
a mobile phone user in France would not be able to use their mobile phone in Britain, as the mobile networks would use different protocols and frequencies



GSM History

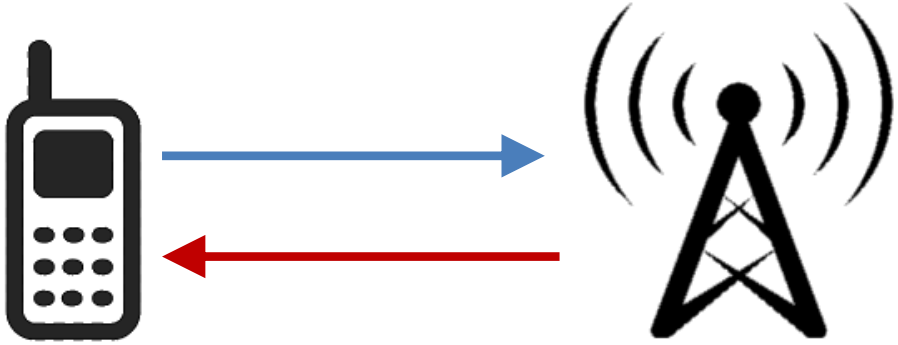
- 1982:
  - Groupe Spécial Mobile (GSM) group was formed
    - by the Confederation of European Posts and Telecommunications (CEPT)
    - This group was tasked with creating the specifications for the **Global System for Mobile Communications (GSM)**
      - A mobile network that could be utilized across Europe (and be extended to the work across the world)

GSM History

- 1986:
  - 900 MHz frequency band (range) was reserved for GSM
- 1989:
  - responsibility of the GSM project was transferred from CEPT to the European Telecommunications Standards Institute (ETSI)
- 1991:
  - Mobile services on a GSM network were first launched
    - GSM was first launched in Finland
    - former Finnish prime minister Harri Holkeri made the world's first GSM call on 1st July 1991

GSM History

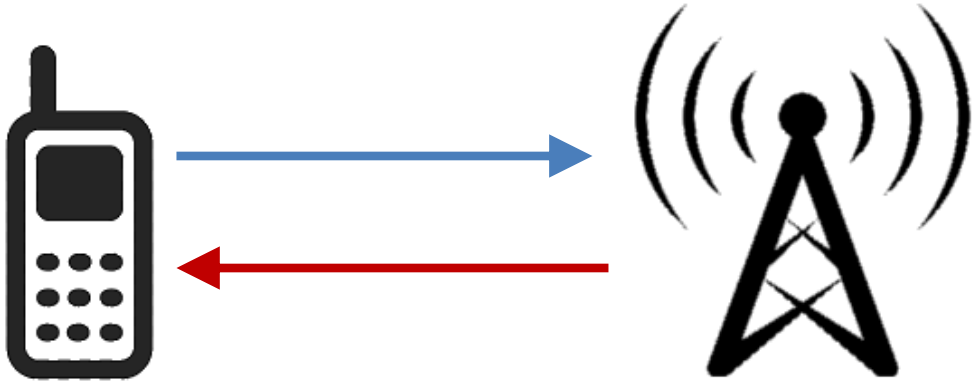
- 1991 (cont.):
  - **GSM 900** was in use in Europe



  - 890 MHz – 915 MHz (frequencies) reserved for the uplink
    - *i.e. data/information received by the base station, transmitted from the phone*
  - 935 MHz – 960 MHz reserved for the downlink
    - *i.e. data/information received by the phone, transmitted from the base station*

GSM History

- 1991 (cont.):
  - Later that same year (1991)
  - **GSM 1800** was introduced in Europe



  - 1710 MHz – 1785 MHz reserved for the uplink
  - 1805 MHz – 1880 MHz reserved for the downlink

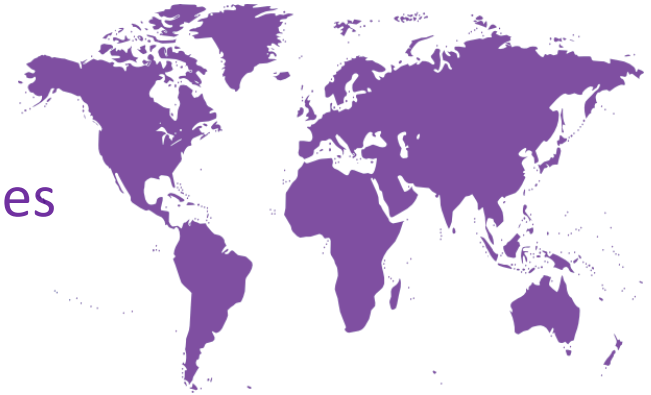
GSM History

- 1995
  - **GSM 1900** was implemented in USA

  - 1850 MHz – 1910 MHz reserved for the uplink
  - 1930 MHz – 1990 MHz reserved for the downlink

GSM History

- By 1996:
  - 120 GSM Networks worldwide
- By 2000:
  - 150 million GSM users
- By 2014:
  - over a billion GSM mobile phones
  - in use in over 168 countries.



GSM Criteria

- Criteria that was taken into consideration when GSM was designed:
  - ➢ Should work through out Europe
  - ➢ Offer high speech quality
  - ➢ Use frequencies efficiently
    - efficient use and allocation of frequencies
  - ➢ Be compatible with other data transmission methods
    - ie GSM network connecting with PSTN telephone networks, Fax and the Internet
  - ➢ High security
    - speech encryption is utilized in GSM

GSM Advantages

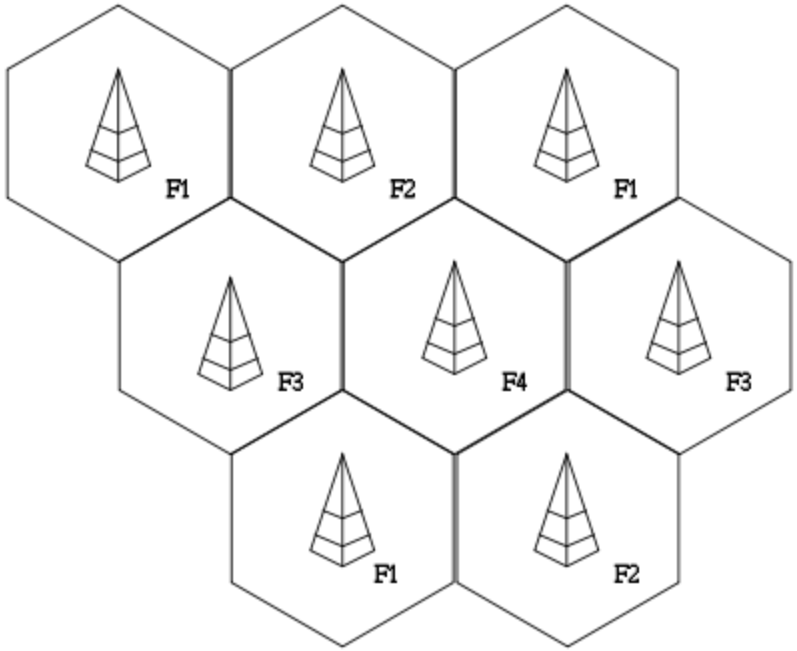
- Mobile communication
  - Mobile and wireless communication supported for voice and data services from different service providers
- High capacity
  - large coverage of customer per cells
  - efficient frequency allocation
- Worldwide connectivity
  - GSM networks have been used in over 168 countries
- High transmission quality
  - High audio quality and
  - uninterrupted phone calls while the mobile user is mobile

GSM Disadvantages

- Patented Technologies limiting availability
  - Most GSM technologies are patented by Qualcomm and hence licenses need to be obtained from Qualcomm
- Limited data rate capability
  - Original GSM maximum data rate was 9.6 kbps
  - Currently, even with GSM advancements: other technologies offer faster data rates
- Electronic Interference
  - GSM uses pulse based burst transmission technology which interferes with certain electronics. Hence why airplanes, petrol stations and hospitals will limit use of GSM mobile devices

GSM Cells – GSM is a Cellular Network

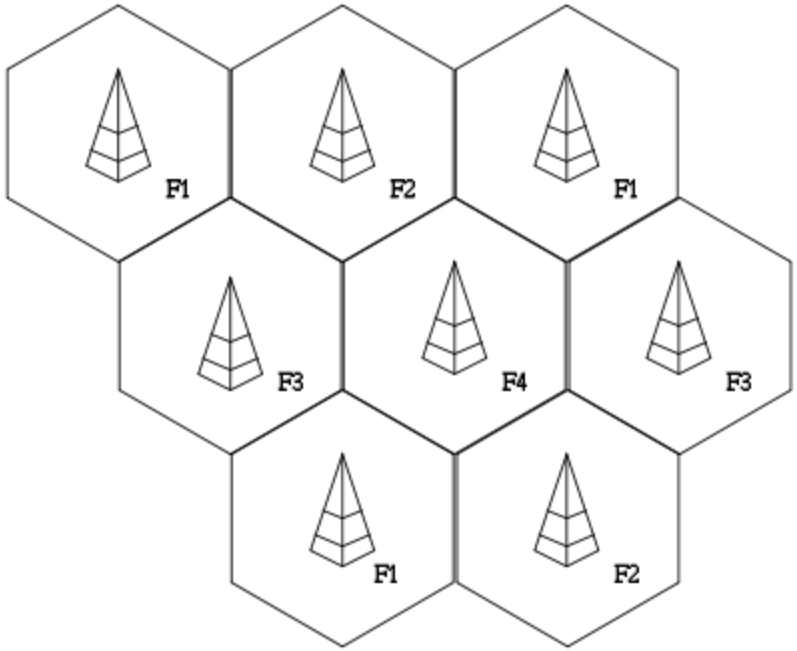
- A GSM cellular network is distributed over land through cells
- Each cell includes a fixed location transceiver known as a **base station.** Together the cells provide radio coverage over larger geographical areas.



See Lecture 01 Slides 22 - 22

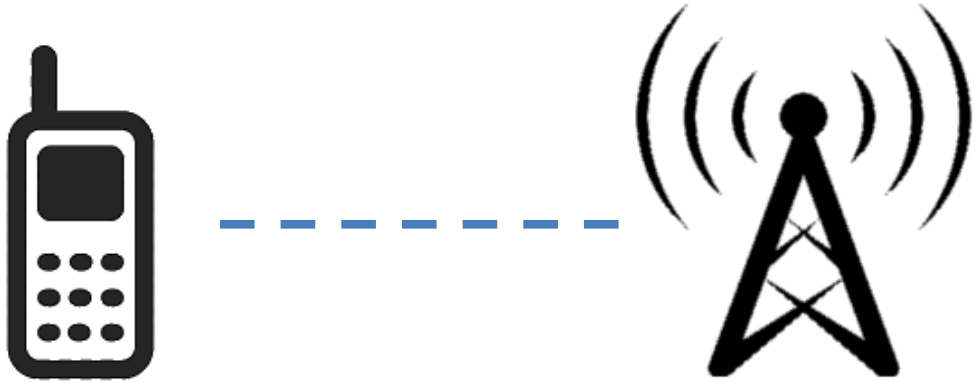
GSM Cells

- GSM Networks provided:
  - Speech communication
  - Data Services
- Over large geographical areas



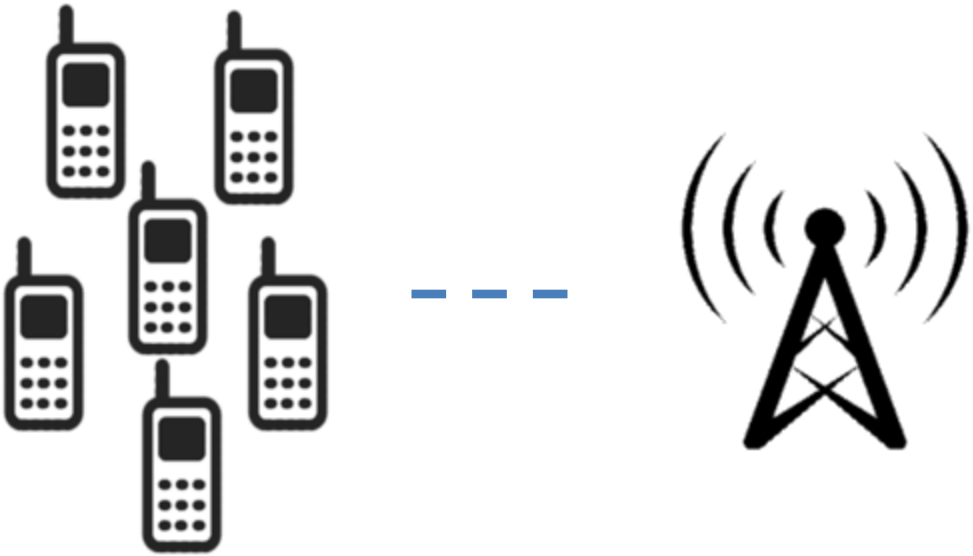
GSM Cells

- GSM allows for a maximum of **35 km** between a **mobile station (a mobile phone)** and a base station
  - such that the mobile station (MS) can remain connected to the network within a 35 km radius of a base station



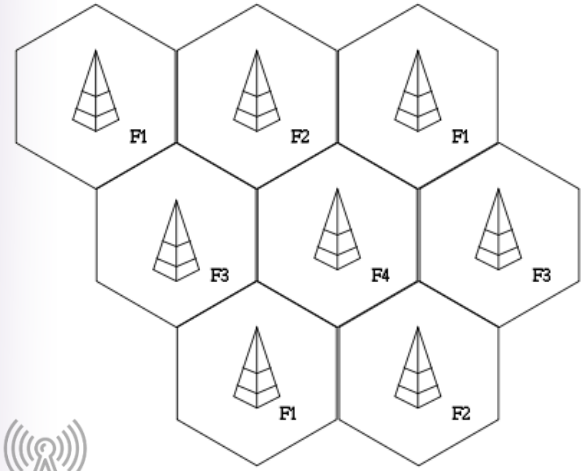
GSM Cells

- Not all cells are the same size in a GSM network
  - The cell size, will be influenced by the number of subscribers (GSM mobile phone users) in the area



GSM Cells

- **handoff (handover):**
  - the process of transferring an active call or data session from one cell in a cellular network to another

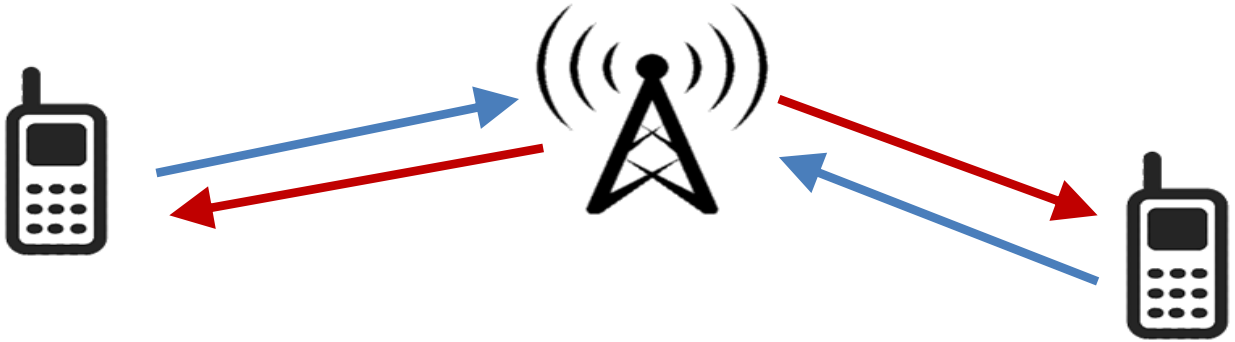


- When a subscriber moves from one cell to another, then their call / data session will be transferred to the base station of their current call /session without interruptions to their session

GSM Bandwidth

- GSM Network speed:

  - The data transmission speed (maximum bandwidth) for original GSM networks is **9.6kbps**



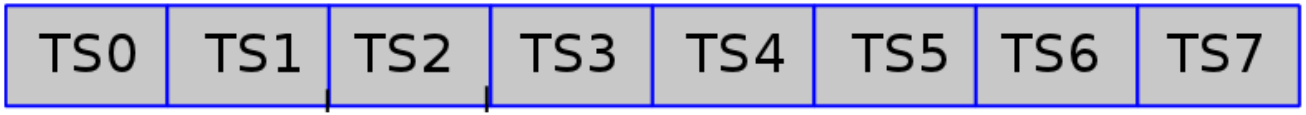
GSM Access

- GSM uses **Time Division Multiple Access (TDMA)** technology to increase the capacity of the network
  - i.e to increase the number of users that can connect to a base station ‘simultaneously’
- **TDMA**
  - a modulation technique which enables multiple users to share the same frequency by dividing each cellular channel (frequency) into different time slots.
  - As such a single frequency supports multiple and simultaneous data connections
    - with a two-time slot TDMA, two users can share the same frequency (each user on a different time-slot)

GSM Access

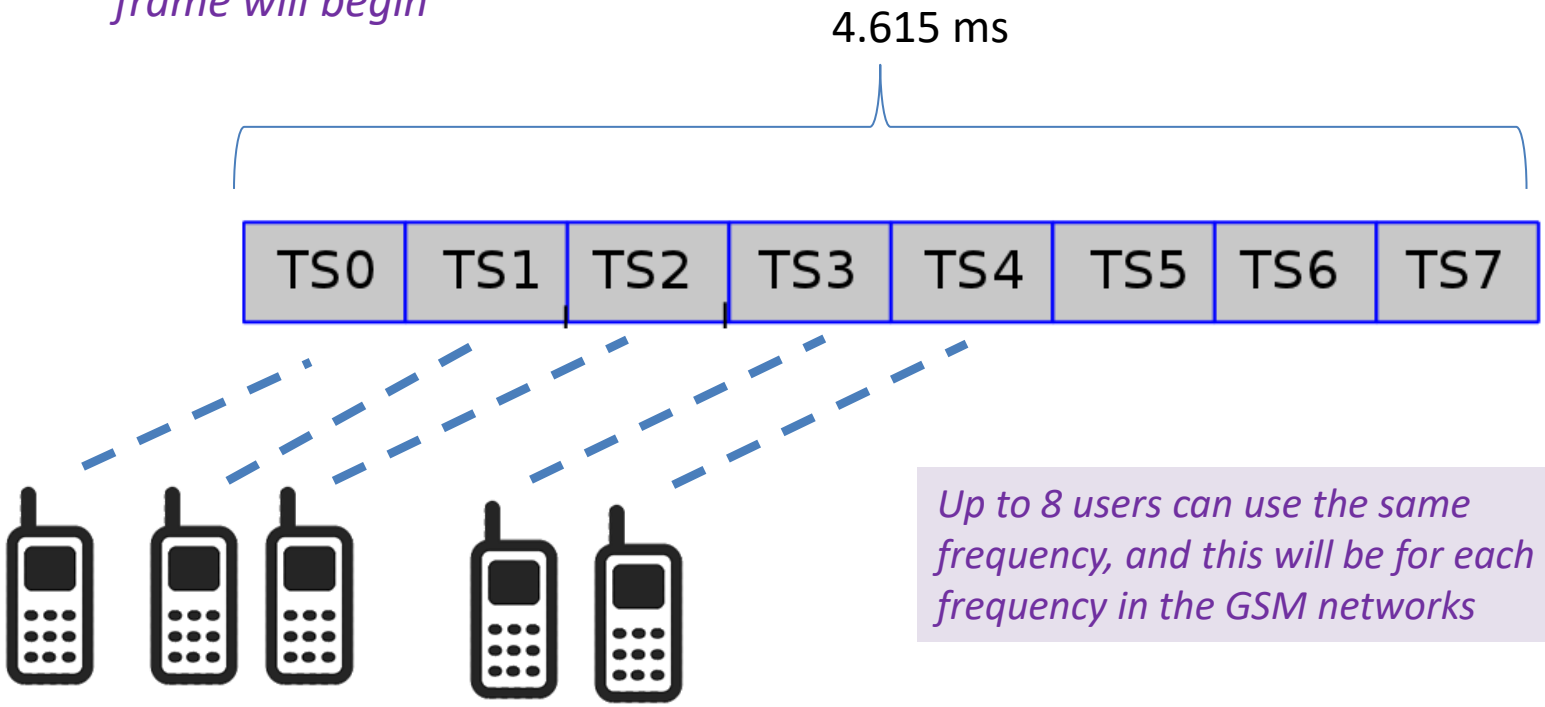
- TDMA
  - With a three-time slot TDMA, three users can share the same frequency

- GSM utilizes An **eight-time slot TDMA**, such that up to 8 users can share the same frequency



GSM Access

- Each time slot lasts **576.9 µs** (microseconds) The duration of a TDMA frame is 4.615 ms (milliseconds), *after which another frame will begin*



Up to 8 users can use the same frequency, and this will be for each frequency in the GSM networks

GSM Extension

- High Speed Circuit Switched Data (HSCSD)
  - An extension to the GSM technology which increases the data rate of a GSM network through two techniques:

1) HSCSD includes **error correction**
   - which improves the quality of a radio channel (frequency)
   - GSM with HSCSD has an increased the data rate to **14.4 kbps**

GSM Extension

- HSCSD

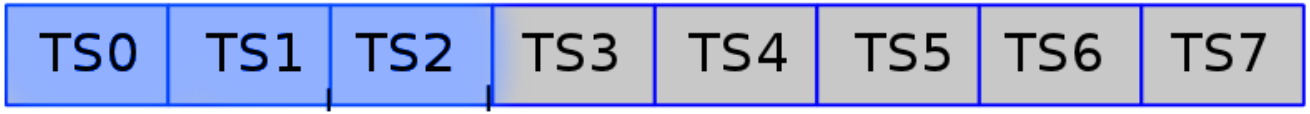
2) HSCSD allows one user to use **multiple time slots** of TDMA

- In theory, the max data rate would be 115.2 kbps if all eight time slots are allocated to the same user. (14.4×8)
- However, the number of multiple time slots a user can be allocated has been limited to 3 time-slots, for a speed of **43.2 kbps**

GSM Extension

- GSM with HSCSD

14.4 kbps for each time slot, GSM with HSCSD allocates 3 time slots to one user



➢ 3 times slots allocated to one user at a time:

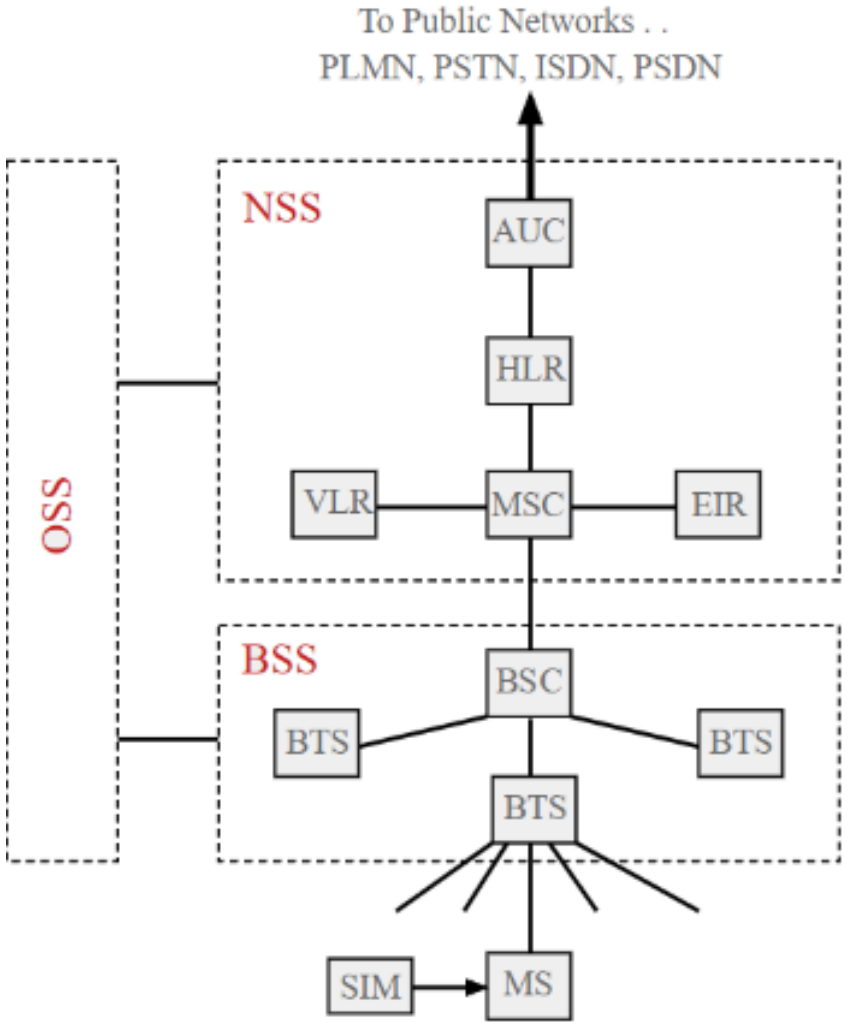
- 14.4 + 14.4 + 14.4 = **43.2 kbps**
- *An improvement from 9.6 kbps GSM used before HSCSD was implemented*

GSM Extension

- GSM with HSCSD Advantages:
  - Faster file transfer, emails and web browsing

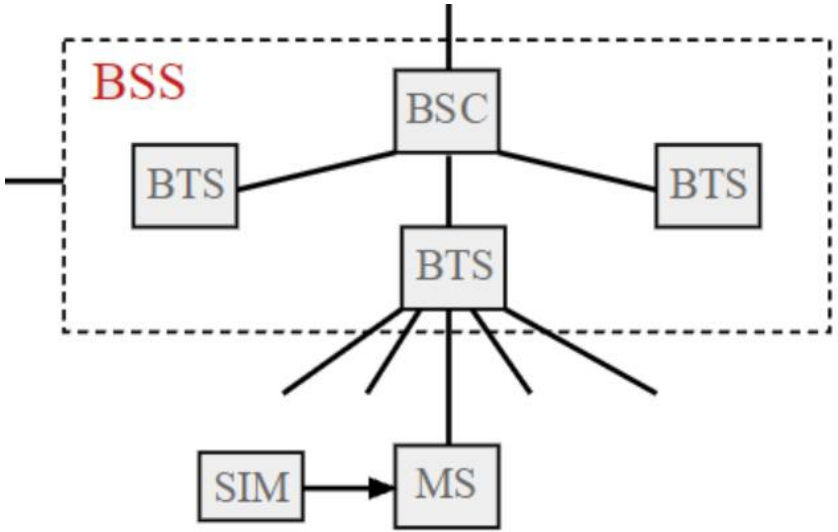
GSM Architecture

- A GSM Network consists of 3 subsystems:
- **Base Station Subsystem (BSS)**
- **Network and Switching Subsystem (NSS)**
- **Operation Subsystem (OSS)**



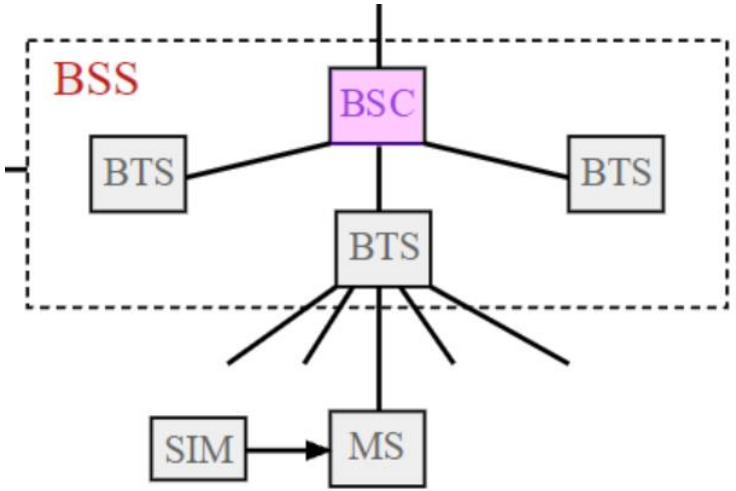
BSS

- **Base Station Subsystem (BSS)**
  - provides a connection between the mobile station (MS) i.e. a phone and the NSS (**Network and Switching Subsystem)**
  - A GSM network consists of **many BSSs**, each controlled by a **base station controller (BSC).** The BSS performs all functions necessary to maintain radio connections to an MS and coding/decoding of voice data



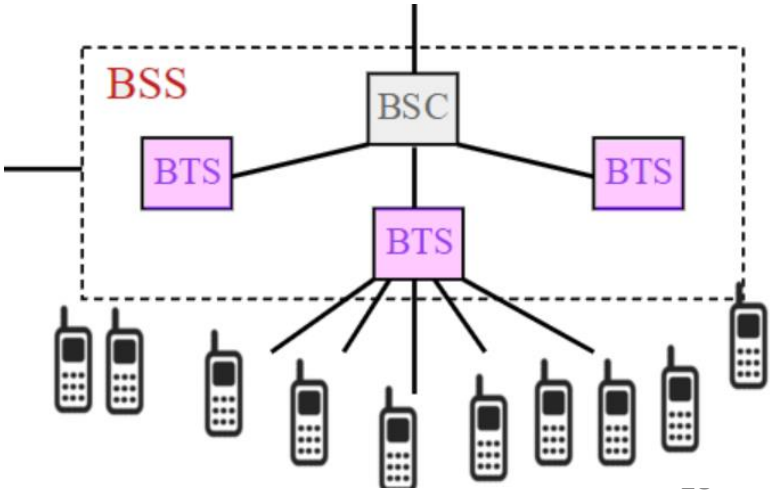
BSS

- **Base Station Controller (BSC)**
  - Manages and controls one or more BTS
  - It reserves radio frequencies and controls the time-slot allocations of the BTSs
  - controls handover from one BTS to another BTS within a BSS
  - identifies and keeps track of the MSs within a BSS and transmits this information to the **MSC** (within the NSS subsystem)



BSS

- **Base Transceiver Station (BTS)**
  - **Multiple users connect to the GSM network through the various BTS**
  - A BTS consists of all the radio equipment, (such as antennas, amplifiers etc.) necessary for radio transmission.



BSS

- **Base Transceiver Station (BTS)**
  - Note: at the base of every cell tower is a BTS which processes radio frequencies.

Cell tower examples

BSS

- Note: Base stations are usually un-attended

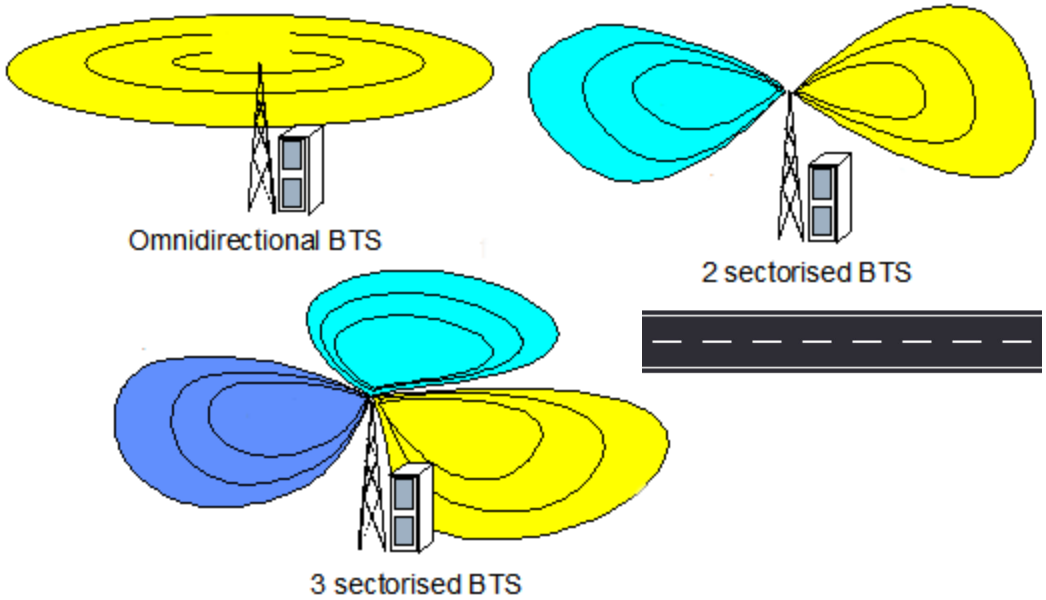
  - Base stations are sometimes located in remote locations without reliable electricity

BSS

- BTSs can have directional antennae or omnidirectional antennae
  - An **Omni-Directional antenna** radiates and receives the radiofrequency (RF) energy equally, providing a 360 degree radiation pattern
    - this allows connectivity in all directions.
  - A **Directional Antenna** has a radius of roughly 45 to 90 degrees
  - focusing RF energy in a required direction and limiting connectivity to that particular area.
    - This can help overcome interference and providing better and more structured coverage.

BSS

- **For example:** a directional antennae BTS may be setup by a road side whereby most mobile users will be using the network within the radius of the BTS
- Most urban (densely populated areas) will utilize a combination of BTSs (omnidirectional and directional) and the BTSs coverage areas will overlap

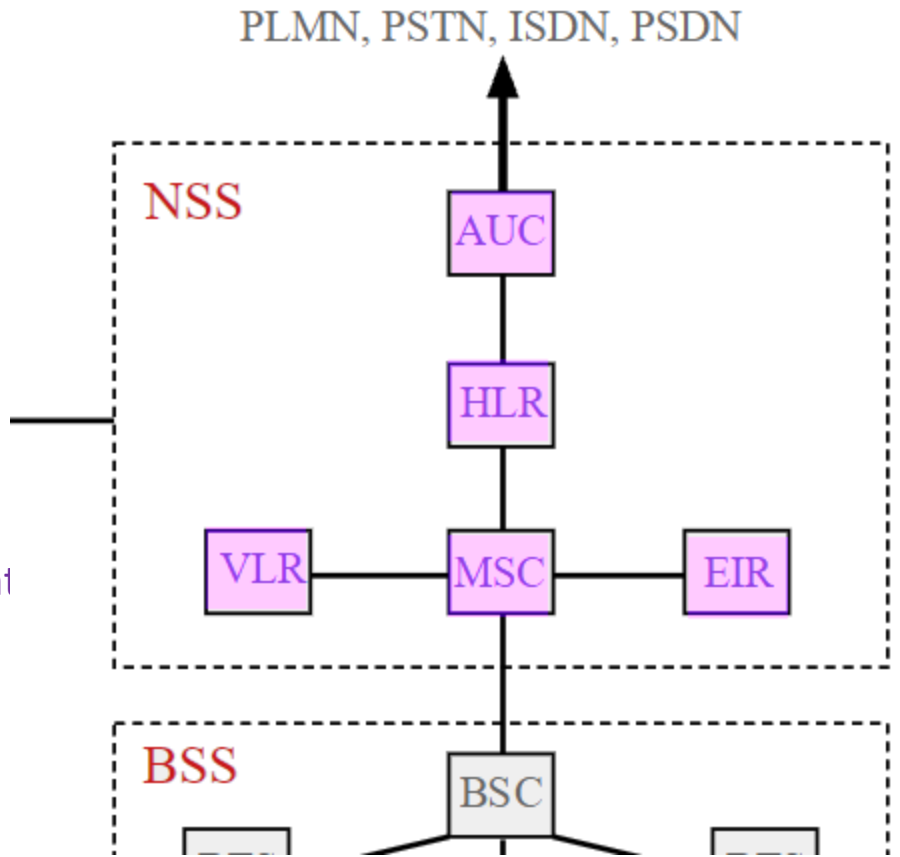


BSS

- BTS Data and Voice Encryption
  - Encryption is used in the GSM air interface (Um Interface) to protect the confidentiality of data
  - Two algorithms involved in the encryption process:
    - The **ciphering algorithm (A5)** implemented in the MS and at the BTS.
    - The **cipher key generation algorithm (A8)** implemented in the AuC and the SIM.

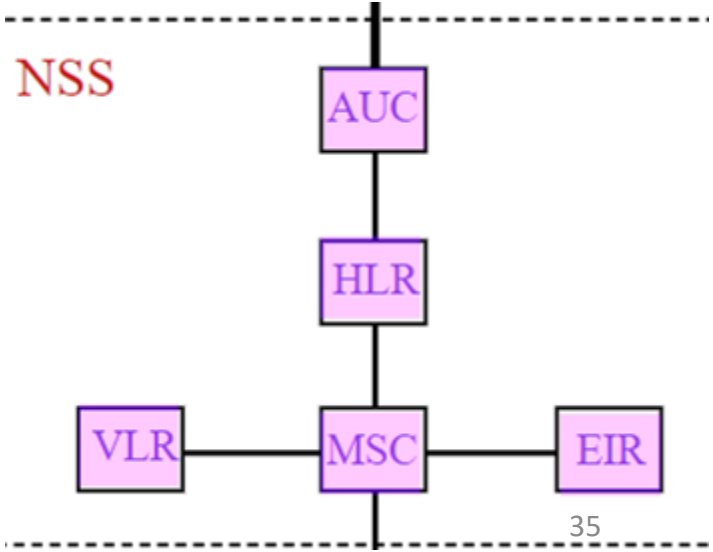
NSS

- **Network and Switching Subsystem (NSS)**
  - *Known as the heart of the GSM network*
  - The NSS connects the wireless network with standard public networks (such as telephone networks)
  - performs handovers between different BSSs
  - supports charging, accounting, and roaming of users between different providers in different countries



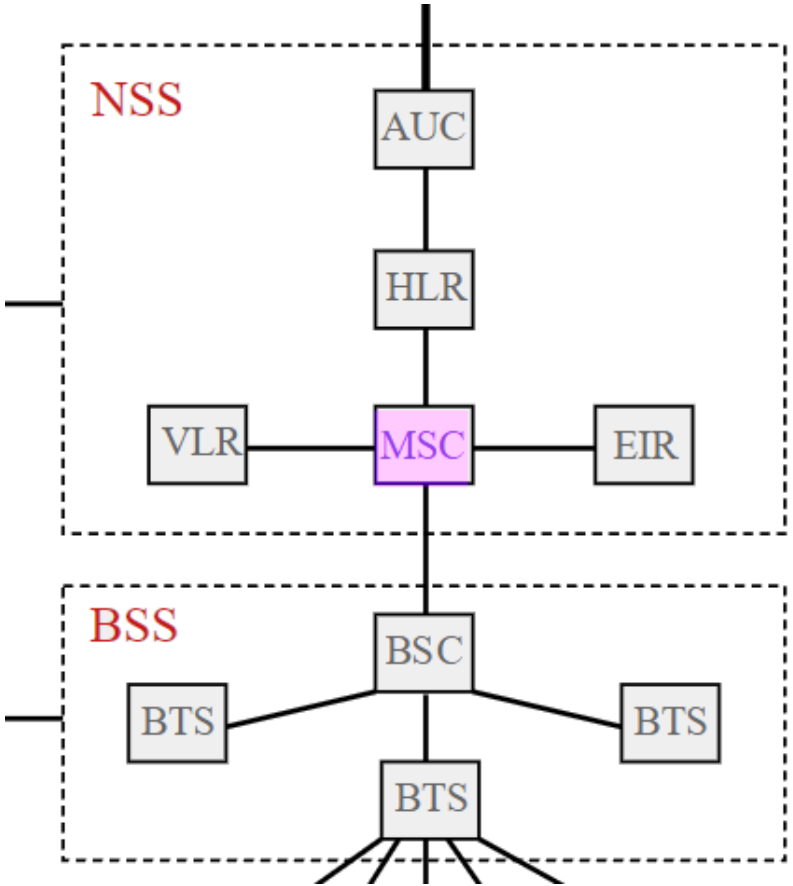
NSS

- **Network and Switching Subsystem (NSS)**
  - *NSS also provided automatic worldwide **localization of users***
    - whereby the system always knows where a user currently is, and the same phone number is valid worldwide



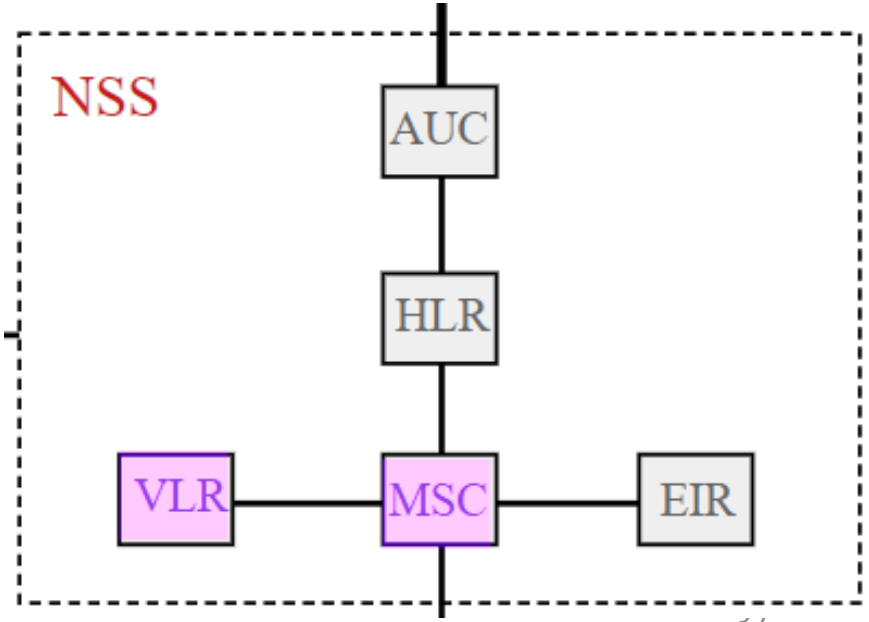
NSS

- **Mobile Switching Center (MSC)**
  - *Known as the backbone of the GSM network*
  - in the NSS
  - Controls setting up calls and controls handoffs between different BSSs
  - They set up connections to other MSCs and connect to BSCs
    - form the fixed ‘backbone’ network of a GSM system.



NSS

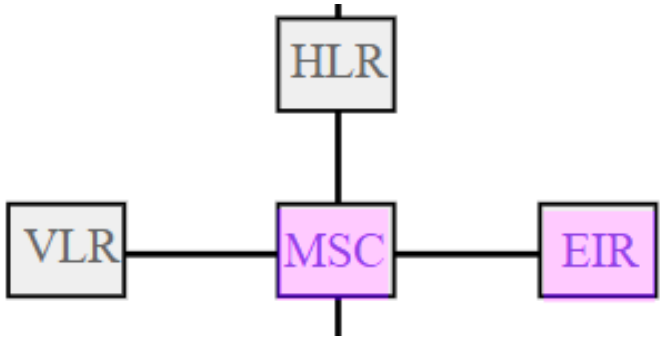
- **Visitor Location Register (VLR)**
  - A database within the MSC
  - Contains the location of the active Mobile Stations



- The VLR supports the MSC during call establishment and authentication
- a VLR database updates whenever a new MS enters (or leaves) its area
  - The update is supported by an **HLR database**

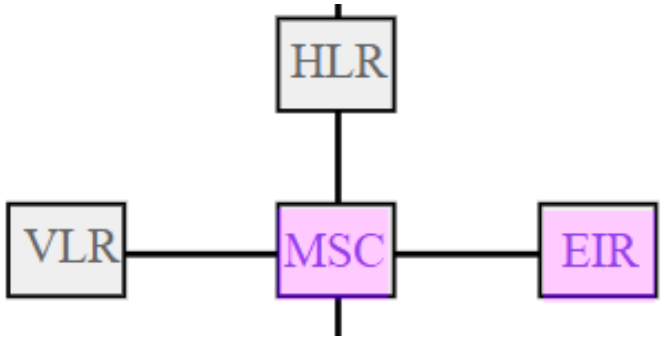
NSS

- **Equipment identity register (EIR)**
  - A database containing all IMEIs registered to a network
    - where by IMEIs are device identification numbers
    - the **International Mobile Station Equipment Identity (IMEI)** codes stored in the EIR, are used in identifying MSs
      - can also be used for blacklisting stolen phones



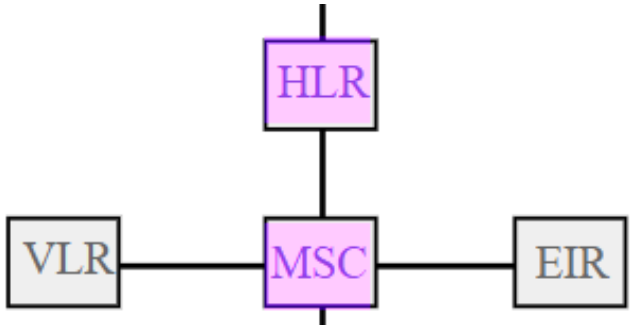
NSS

- **Equipment identity register (EIR)**
  - The EIR contains three lists:
    - **White list** of network nodes permitted on the network
    - **Black list** of network nodes blocked from the network.
    - **Gray list** of faulty equipment that may cause a problem but are still permitted on the network.



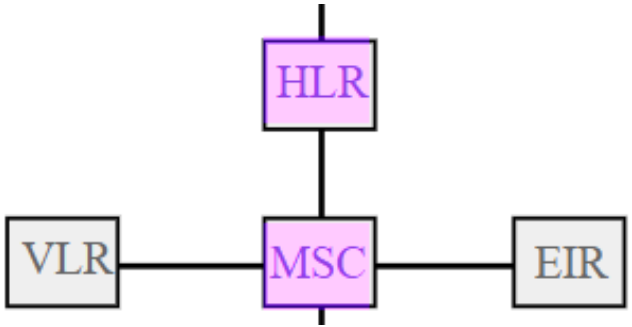
NSS

- **Home location register (HLR)**
  - ➢ *The most important database in a GSM system*
  - ➢ Stores all user-relevant information,
    - includes **static** and **dynamic** information for each user



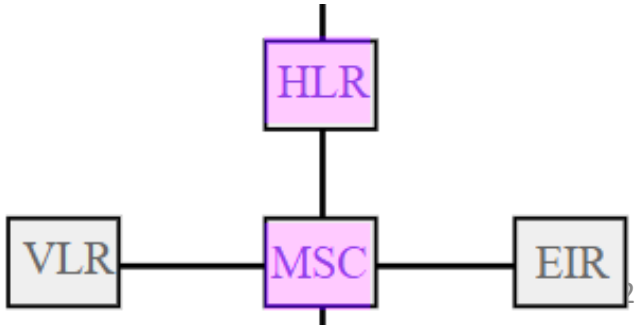
NSS

- **Home location register (HLR)**
  - ➢ Static Information in HLR:
    - **mobile subscriber ISDN number (MSISDN),**
    - **subscribed services** (e.g., call forwarding, roaming restrictions, GPRS)
    - **international mobile subscriber identity (IMSI).**



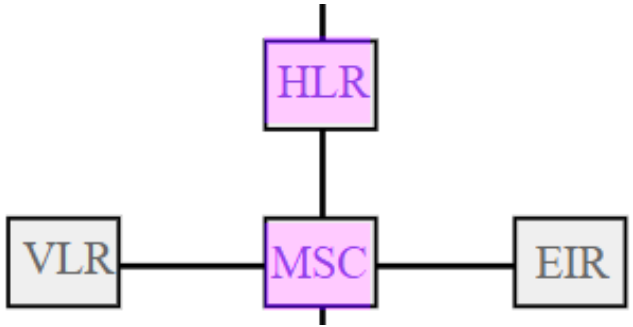
NSS

- **Home location register (HLR)**
  - Dynamic Information in HLR:
    - the current VLR and MSC of an MS
    - the current **location area (LA)** of an MS
    - the **mobile subscriber roaming number (MSRN)**
  - Immediately when an MS leaves its current LA, the information in the HLR is updated
    - as such the VLR will also be updated

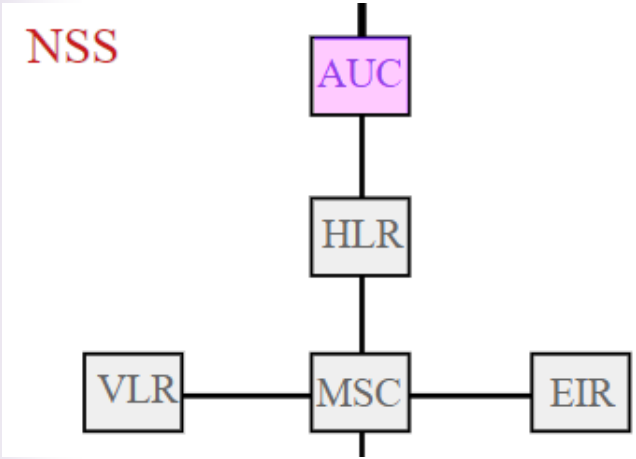


NSS

- **Home location register (HLR)**
  - Note: each operator (mobile services provider) will have one HLR database in their GSM network



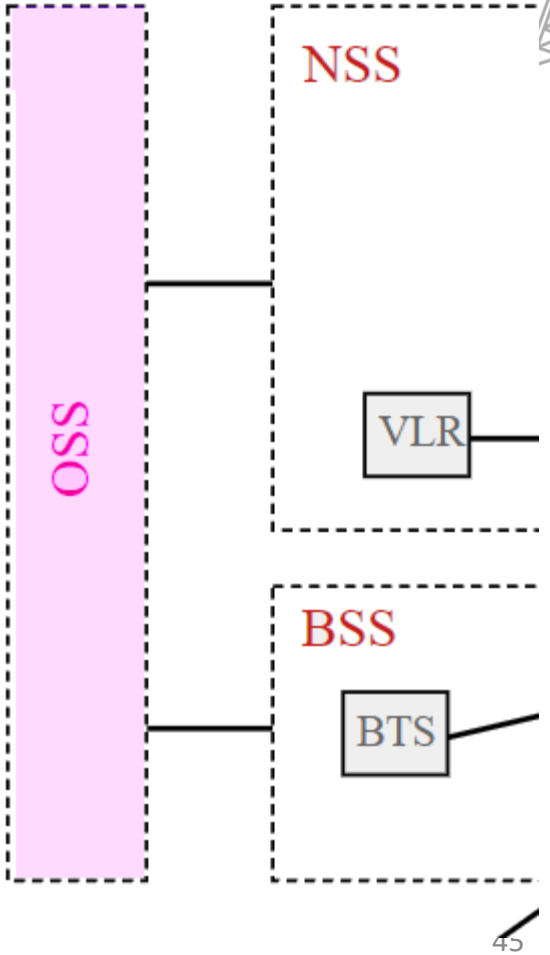
NSS



- **Authentication center (AUC)**
  - a separate authentication center is included in a GSM network's NSS to help protect user identity and data transmission
    - due to possible interception of radio transmissions (from attackers) between mobile stations and the BSSs: authentication is utilized in the GSM network and managed by an AUC

OSS

- Operation Subsystem
  - Focuses on management for the whole GSM network
    - Includes maintenance features of the GSM network
  - Usually operator dependent
    - i.e. different mobile service providers may have different setups of an OSS
    - Very loosely specified in the GSM standards

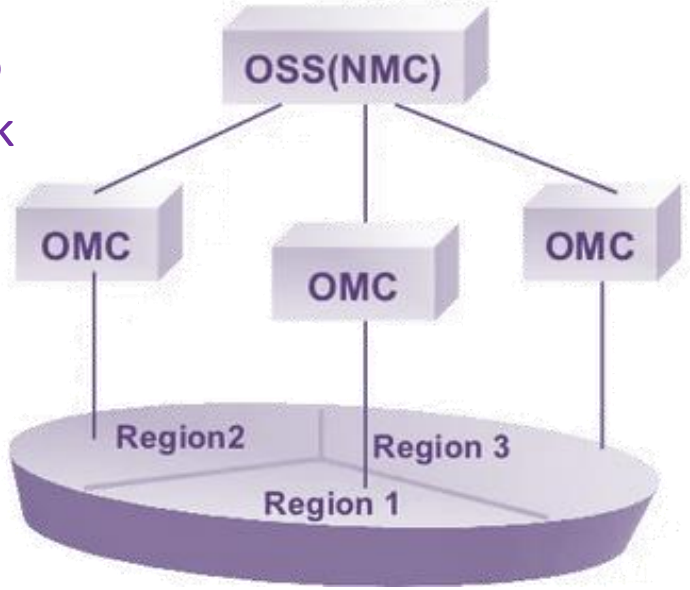


OSS

- **Operation and maintenance center (OMC)**
  - within OSS
  - OMC includes management functions such as
    - traffic monitoring,
    - status reports of network nodes,
    - subscriber and security management
    - accounting and billing information

OSS

- **Network Management Centre (NMC)**
  - *within OSS*
  - the central point from which the entire network may be controlled or managed.
  - an NMC can make use of several OMCs to control or upgrade different GSM network nodes in different areas



MS

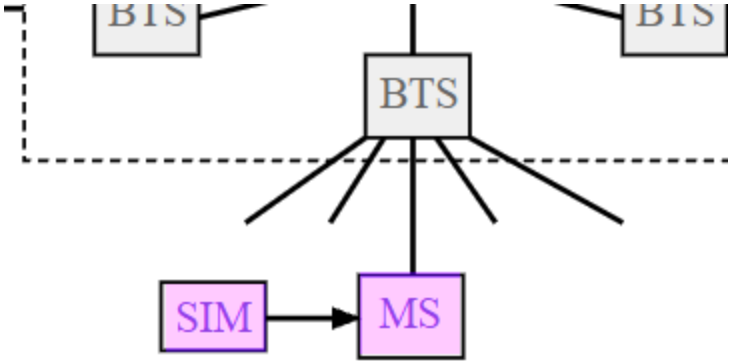
- Mobile Station (MS)
  - the user's handset (mobile phone), which has two parts:
    - **Mobile Equipment (ME)**
    - **Subscriber Identity Module (SIM)**

Evolution of Mobile Stations

MS

➢ Mobile Equipment (within an MS):

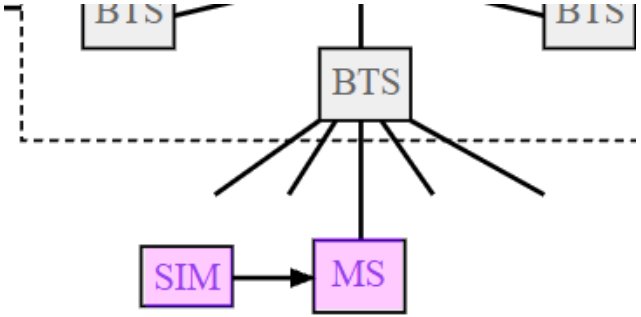
- Radio functionality
  - transmission of radio signals
- User interface
- Processing capability
- Encryption
- SMS Functionality
- Equipment IMEI number



MS

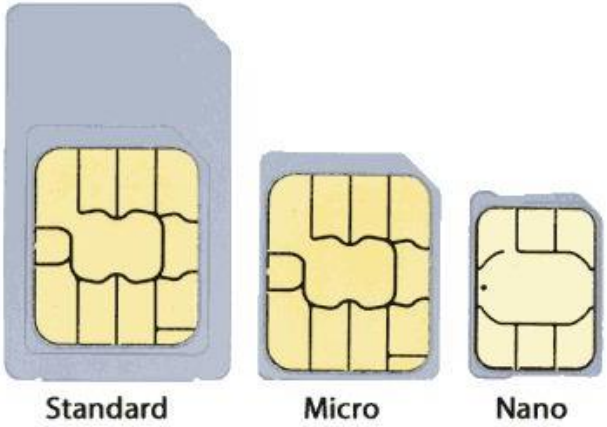
- **Subscriber Identity Module (within an MS):**
  - provides the MS with a unique identity
  - additionally, stores and processes security information
  - Can be moved from phone to phone

- The SIM stores:
  - Personal Identification Number (PIN)
  - Personal phone numbers
  - Short messages
  - Logs of calls (dialed phone numbers)
  - Security related information

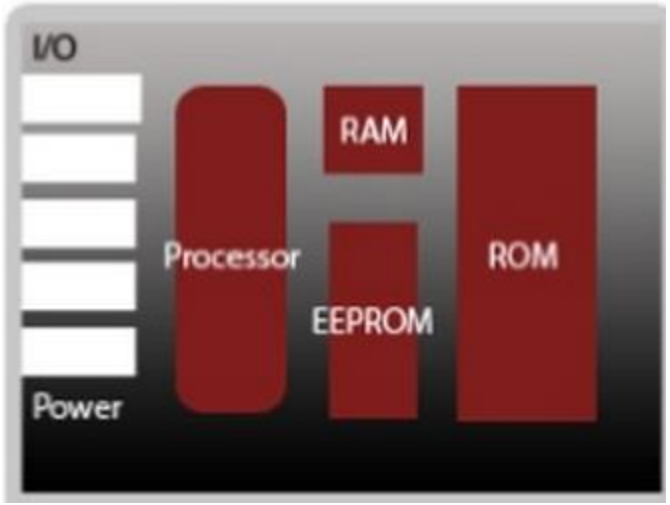


MS

- **Subscriber Identity Module (within an MS):**
  - Note that the SIM card contain a **complete microcomputer**, with a *processor*, RAM, ROM and a built-in OS

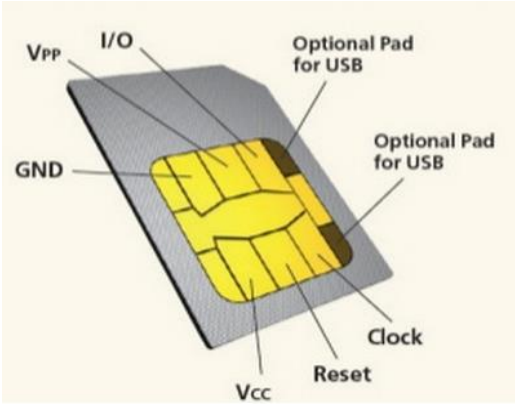


SIM card sizes



*Components of a **smart chip** within a SIM card*

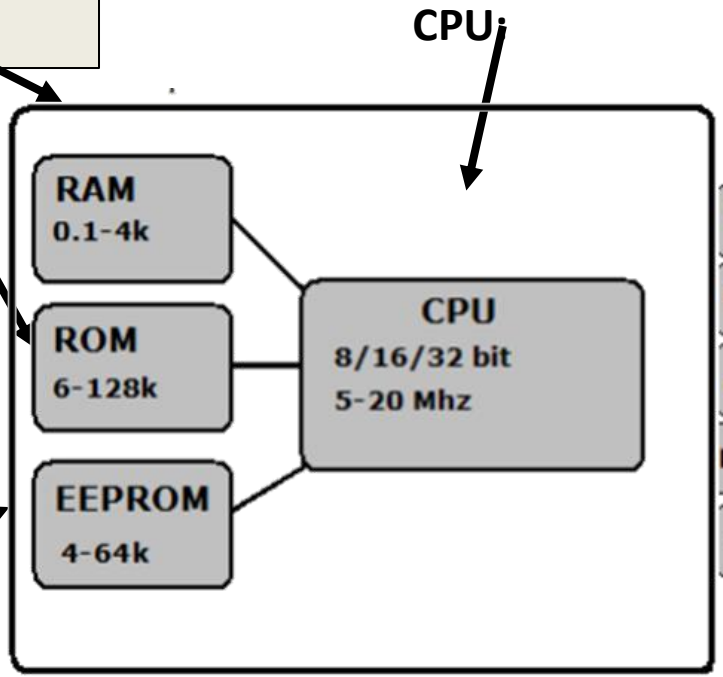
MS – SIM Card Components



RAM: Size ranges from few hundred bytes to several megabytes

ROM: Contains the smart cards core operating system and support libraries.

EEPROM: Stores the card's file system. Typically sizes are from 4 - 64k



VCC - 1.8v, 3v, 5v

Clock: 5-20 Mhz.

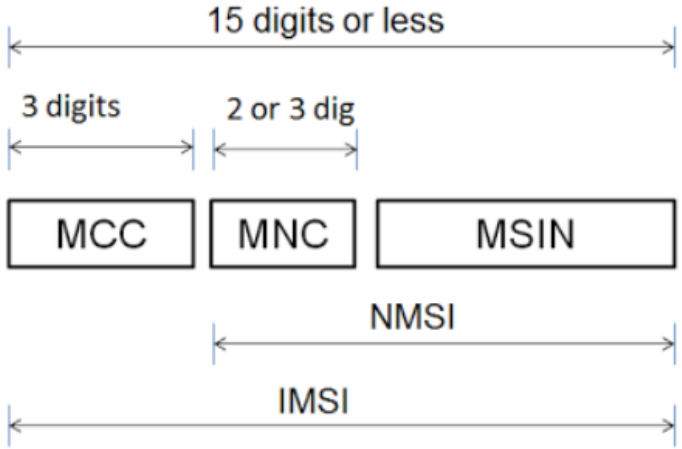
can initiate a reset protocol

Input/Output: controller

GSM - IMSI

The SIM card's smart chip contains an **IMSI**

- **International Mobile Subscriber Identity (IMSI)**
  - is a unique global identification number allocated to each mobile subscriber in every GSM system
  - IMSI includes:
    - Mobile Country Code (MCC)
    - Mobile Network Code (MNC)
    - Mobile Subcriber Identity (MSIN)



GSM - IMSI

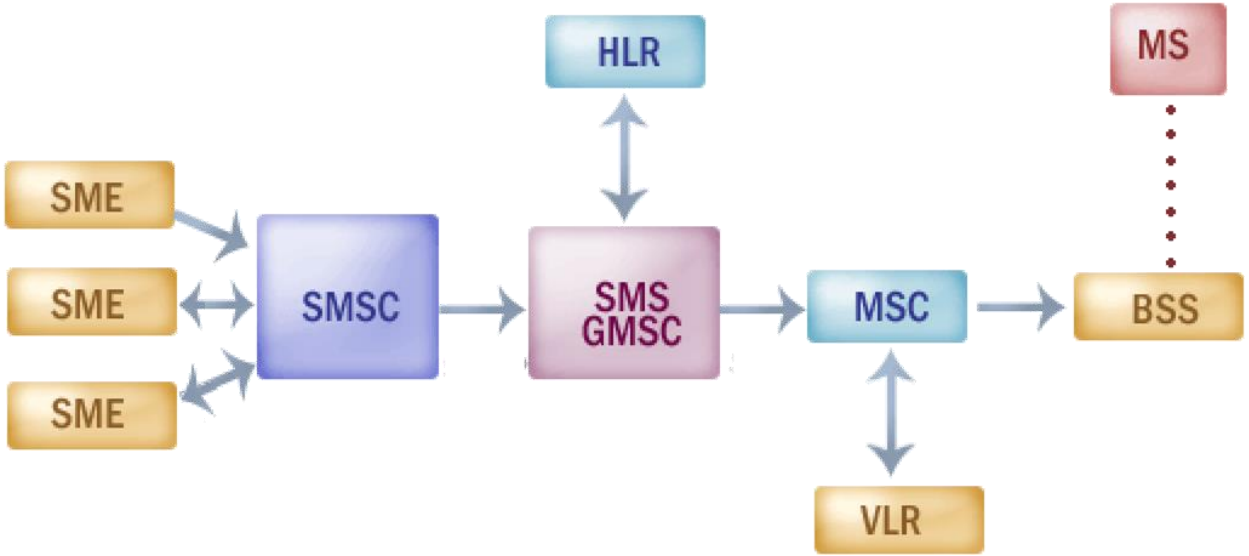
- **Temporary mobile subscriber identity (TMSI):**
  - A temporary ID number used to hide the IMSI,
    - since the IMSI would give away the exact identity of the user using the air interface
    - The TMSI is transmitted instead, for security
  - The TMSI is generated by the VLR
    - related to the time when it is created in order to avoid double allocation

GSM – Location Updates

- The cells overlap each other
  - usually a mobile station can identify (‘see’) several transceivers (BTSs)
  - When the mobile station reaches a new BSC’s area, it requests a location update
  - The MS’s update is forwarded to the MSC, entered into the VLR, the old BSC is notified and an acknowledgement is passed sent to the MSC

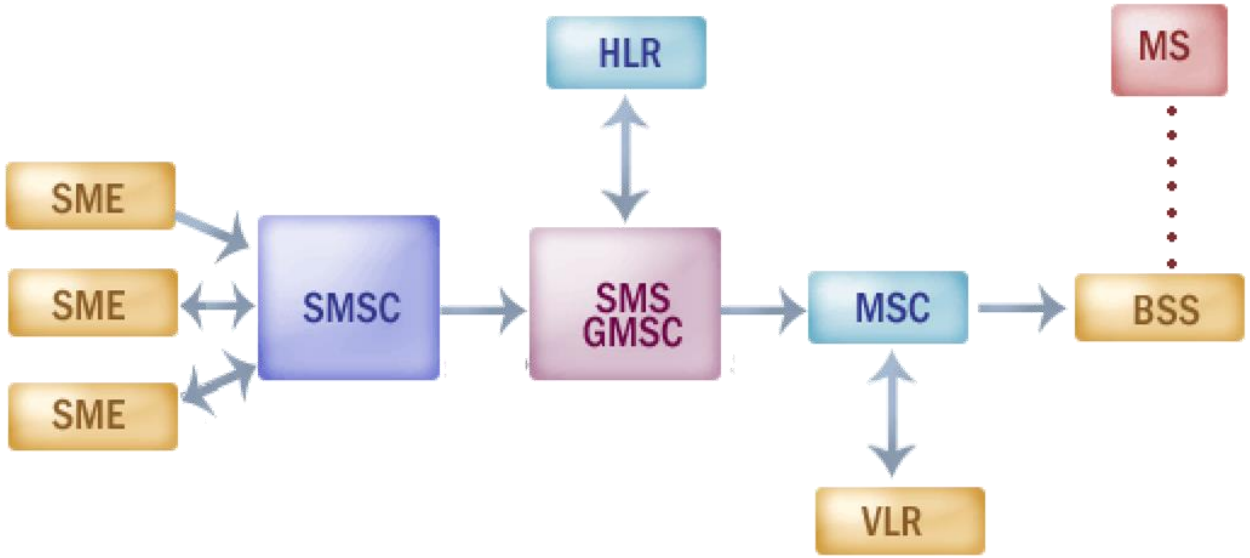
GSM and SMSC

- **SMS center (SMSC)**
  - is responsible for handling the SMS operations of a wireless network.
  - When an SMS message is sent from a mobile phone, it will reach an SMS center first. The SMS center then forwards the SMS message towards the destination



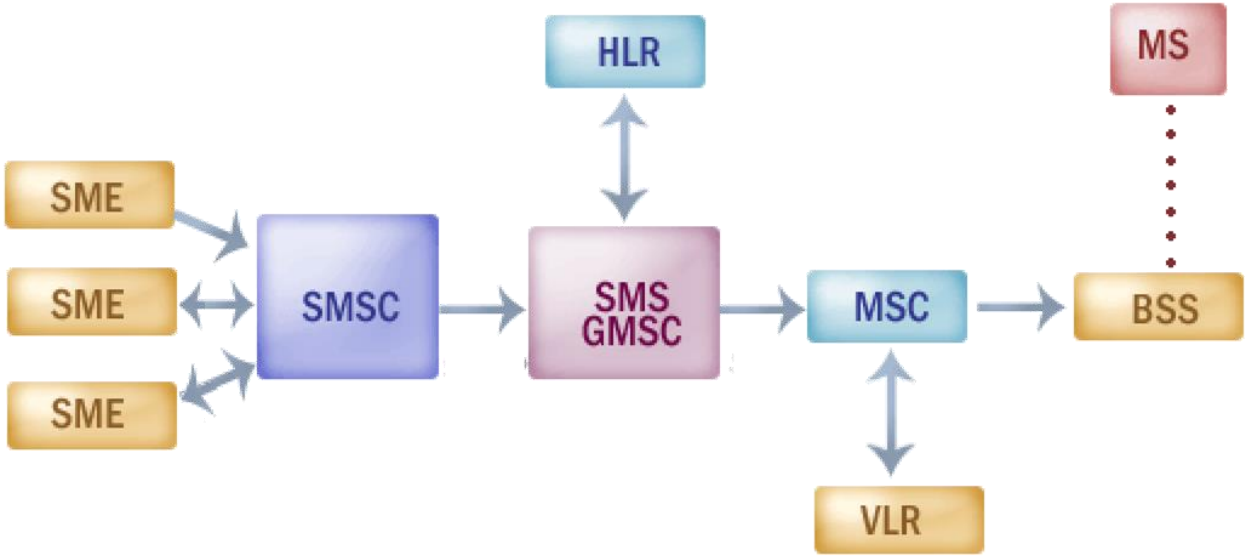
GSM and SMSC

- The **Short Messaging Entity** (**SMEs**)
  - are the starting points (the source) and the end points (the receiver) for SMS messages. They always communicate with a Short Message Service Center (SMSC)



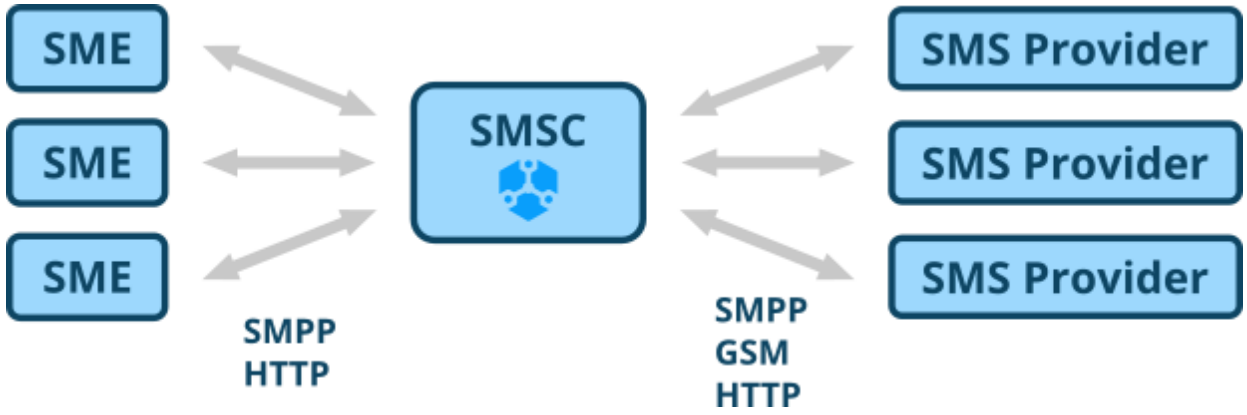
GSM and SMSC

- The **SMS-GMSC (Short Message Service Gateway Mobile Switching Centre)**
  - ➢ forwards short messages directed in different directions
    - can send messages from a GSM **MSC** to an **SMSC** and vice versa



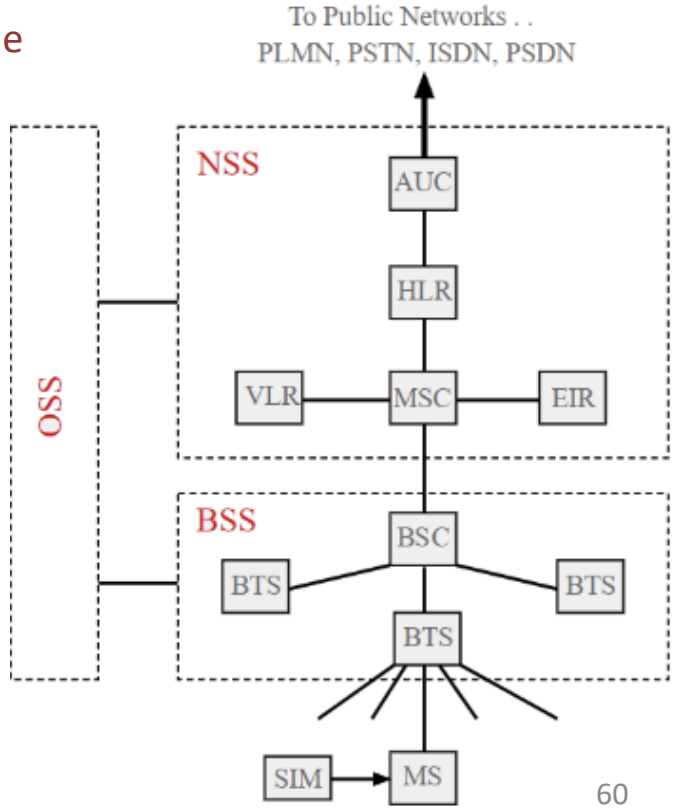
GSM and SMSC

- As such, the **SMSC** and **SMS-GMSC**
  - ➢ enables SMS functionality in a GSM network



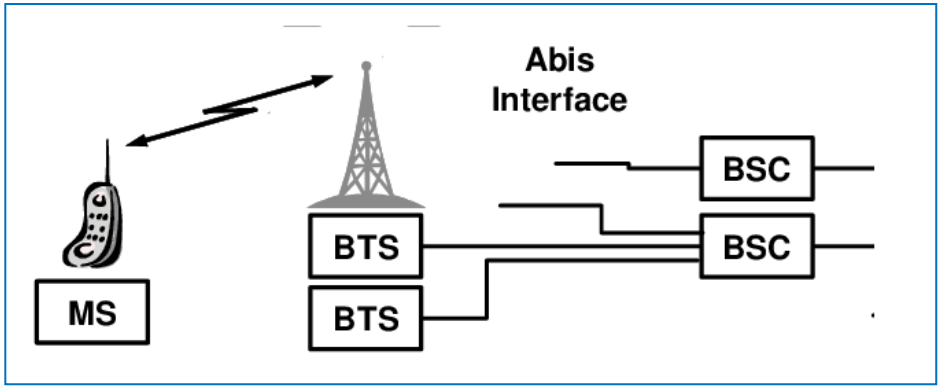
GSM Interfaces Overview

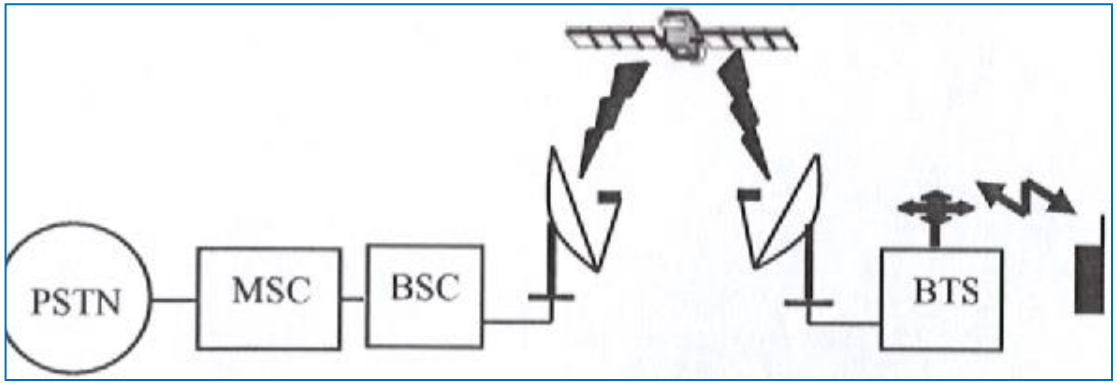
- GSM has 9 interfaces (connection types):
  1. **Um interface:** also known as the **air interface**
     - radio transmission travel between the MSs and the BTSs
  2. **A-bis interface:** Connects BTS to BSC
  3. **A interface:** Connects BSC to MSC
  4. **B:** Connects MSC to VLR
  5. **C** : Connects MSC to HLR
  6. **D:** Connects HLR to VLR
  7. **E:** Connects MSC to other MSCs
  8. **H:** Connects HLR to AUC
  9. **G:** Connects VLR to other VLRs



GSM Interface Overview

- Note: an **A-bi**s Interface can be wired or satellite based





The specifications and protocols of the 9 GSM interfaces are beyond our current scope

GSM Services

- GSM has 3 categories of services
  - Bearer service
  - Tele service
  - Supplementary service

GSM Services

- Bearer service
  - Provision of radiofrequency based data transmission over the GSM network
  - Data transmission has a constant delay and throughput if no transmission errors occur

- Tele service
  - GSM provides encrypted voice transmission and data communication with the PSTN or ISDN networks (e.g., fax).
  - provision of **high-quality digital voice transmission**, which is the main goal of the GSM network

GSM Services

- Supplementary service
  - **emergency number**
    - The same number can be used throughout Europe or throughout a region. This service is mandatory for all providers and can be free of charge.
  - **short message service (SMS)**
    - transmission of messages of up to 160 characters over the GSM network

GPRS

- **General Packet Radio Service (GPRS)**

➢ An upgrade of GSM that provides **IP-based packet data transmission** up to **114 kbps** *(whereby 172 kbps is the theoretical maximum data transfer speed)*
  - GPRS data transmission follows Internet Protocol standards and specifications

➢ GPRS provides ‘always on’ Internet access
  - no connection has to be set up prior to data transfer

➢ Users can ‘make calls and send data simultaneously

GPRS

- **General Packet Radio Service (GPRS)**

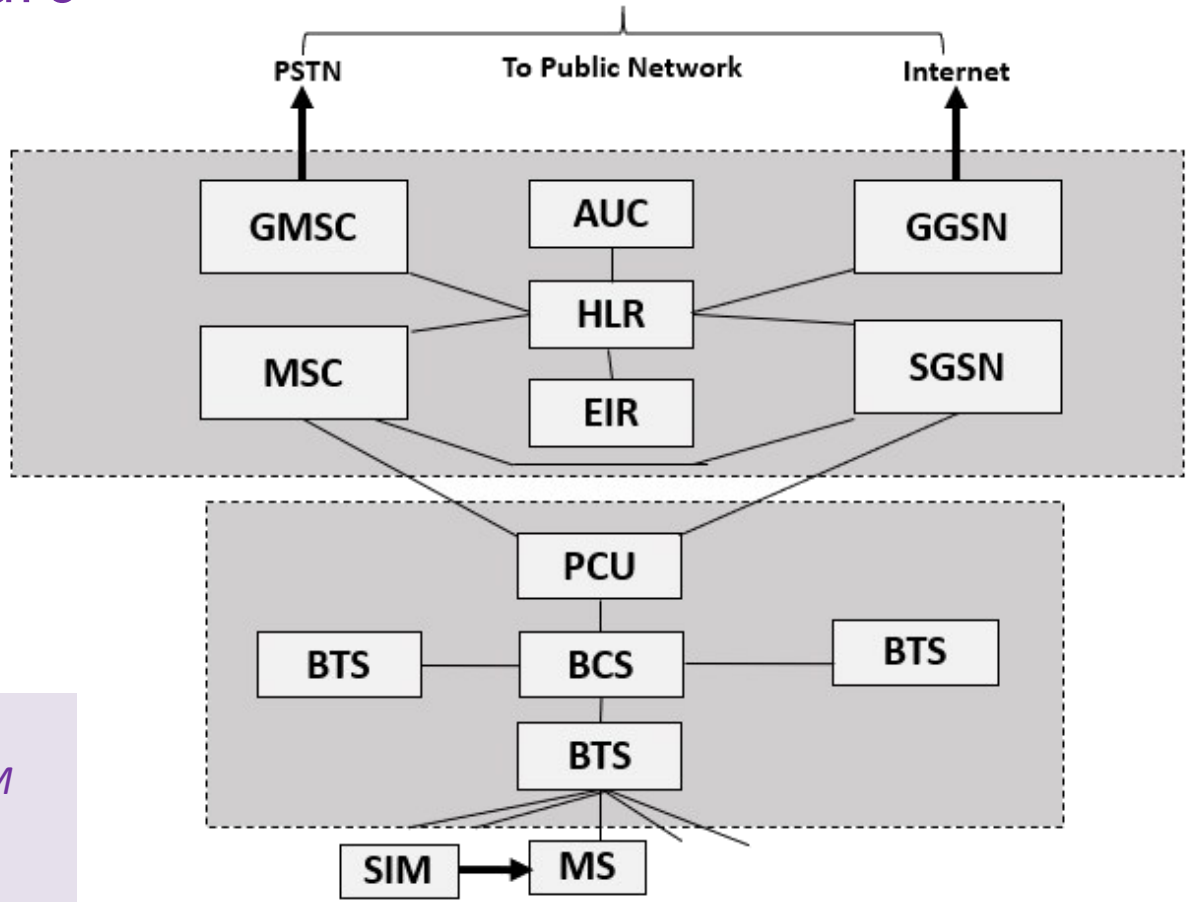
➢ Performance reduces as number of users increase

➢ Messaging Service (MMS) whereby users can send rich text, audio, video messages to each other

➢ Bearer services for GPRS offer end-to-end packet-switched data transfer

- Note: **Packet switching** is the transfer of small pieces of data across various networks. These data pieces or "packets" allow for faster, more efficient data transfer.
- ie. when a user sends a file across the network, it gets transferred in smaller data packets, which are reassembled at the destination of the packets

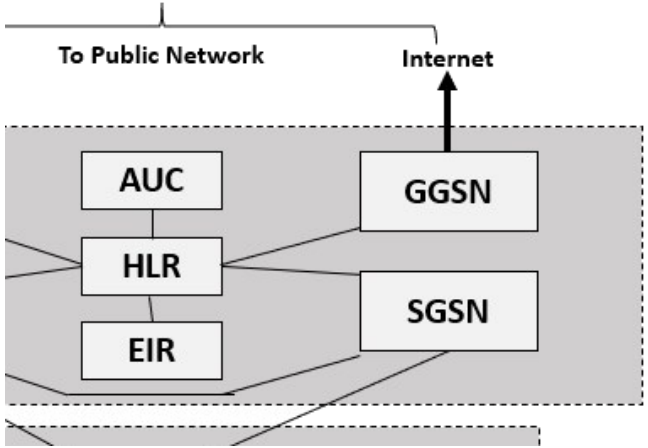
GPRS Architecture



Note, as GPRS is an upgrade of GSM, many components of a GSM network are used within a GPRS network

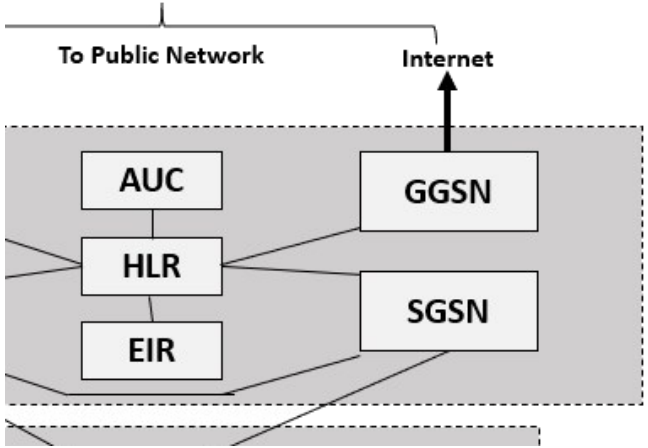
GPRS Architecture

- **Gateway GPRS Support Node (GGSN)**
  - connects GPRS and the Internet
  - performs routing, authentication and address conversion



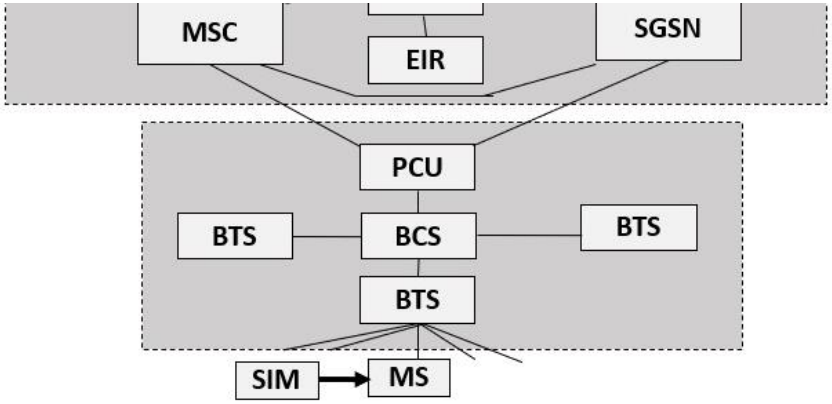
GPRS Architecture

- **Serving GPRS Support Node (SGSN)**
  - ➢ provides packet switching, security and authentication for GPRS users through the HLR



GPRS Architecture

- **Packet Control Unit (PCU)**
  - In the BSS
  - provides a connection between the SGSN and the radio network using frame relay technology
    - Frame Relay **sends data in as frames through a shared Frame Relay network**. Each frame contains all the information necessary to route it to the correct destination



GPRS and GSM Comparison

GSM	GPRS
Only circuit-switched	Supports circuit-switched and packet-switched functionality
No retransmission provided	MS utilizes automatic retransmission to re-transmit error frames
Single time-slot per user	Multiple time slots can be allocated to a single user
Simple time-based billing	More complex billing (including data usage)
GSM is knowns as a **2G** Network	GPRS is knowns as a **2.5G** Network