



The GSM technology

GLOBAL SYSTEM FOR MOBILE COMMUNICATION





HISTORY

1946

- **First Car Phone by St. Louis.**

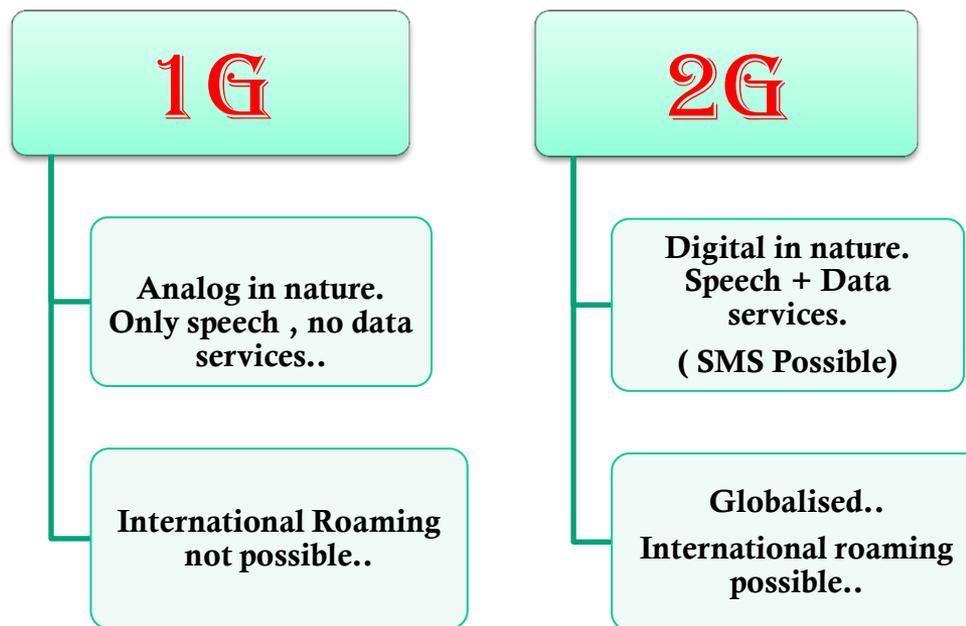
1973

- **First hand-held mobile phone by Martin Cooper.**

1980's

- **1G Cellular technology launched.**
- **TACS , NMT , AMPS etc. analog systems launched in American & UK countries.**
- **Digital 2G Cellular technology launched.**
- **GSM , CDMA etc. launched with GSM being the standard.**





**In 2001 the first commercial launch of 3G was done in Japan.
With 3G following services are available :**

- ✓ **Video Conferencing**
- ✓ **online games**
- ✓ **net surfing..**





introduction

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation.

GSM Services

➔ **TELE SERVICES** : Includes mobile phones, emergency calling etc.

➔ **DATA SERVICES** : Includes SMS (Short message service), fax, voicemail, electronic mail.

➔ **SUPPLYMENTARY SERVICES** : I/C & O/G calls, call forwarding, call hold, call waiting, conference, etc.





Advantages of GSM

- ✓ **Communication**
 - mobile, wireless communication, support for voice and data services
- ✓ **Total mobility**
 - international access, chip-card enables use of access points of different providers.
- ✓ **Worldwide connectivity**
 - one number, the network handles every location.
- ✓ **High capacity**
 - better frequency efficiency, smaller cells, more customers per cell.
- ✓ **High transmission quality**
 - high audio quality and reliability for wireless, uninterrupted phone calls at higher speeds (e.g., from cars, trains).
- **Security functions**
 - access control, authentication via chip-card and PIN





GSM Specifications

➤ RF Spectrum

GSM 900

Mobile to BTS (uplink):
890-915 MHz

BTS to
Mobile(downlink):935-960
MHz

Bandwidth : 2* 25 MHz

GSM 1800

Mobile to BTS (uplink):
1710-1785 MHz

BTS to Mobile(downlink)
1805-1880 MHz

Bandwidth : 2* 75 MHz

➤ Carrier Separation :
200 KHz

➤ Duplex Distance :
45 MHz

➤ No. of RF carriers :
124

➤ Access Method :
TDMA/FDMA

➤ Modulation Method :
GMSK

➤ Modulation data rate
: 270.833 Kbps



A colorful logo featuring a globe with various communication symbols like a telephone, a mail envelope, and a network tower, surrounded by radiating lines.

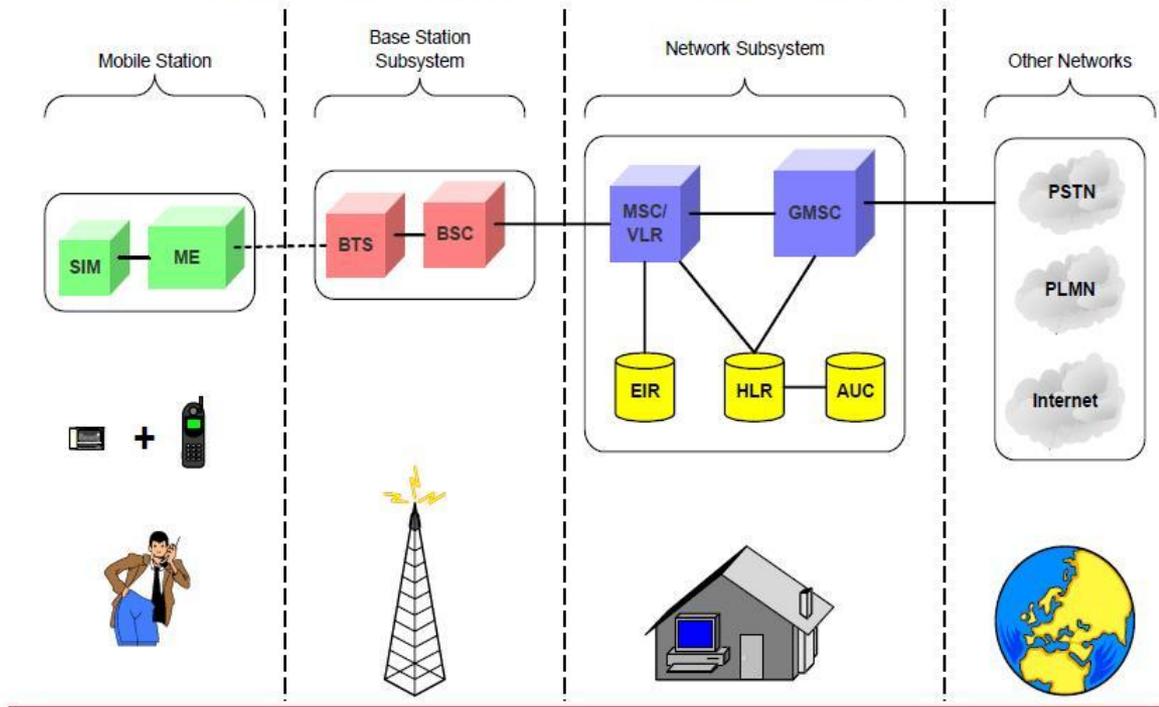
GSM architecture

- **Network sub-system**
- **Radio sub-system**
- **Operation and maintenance sub-system**





Architecture of a GSM Network

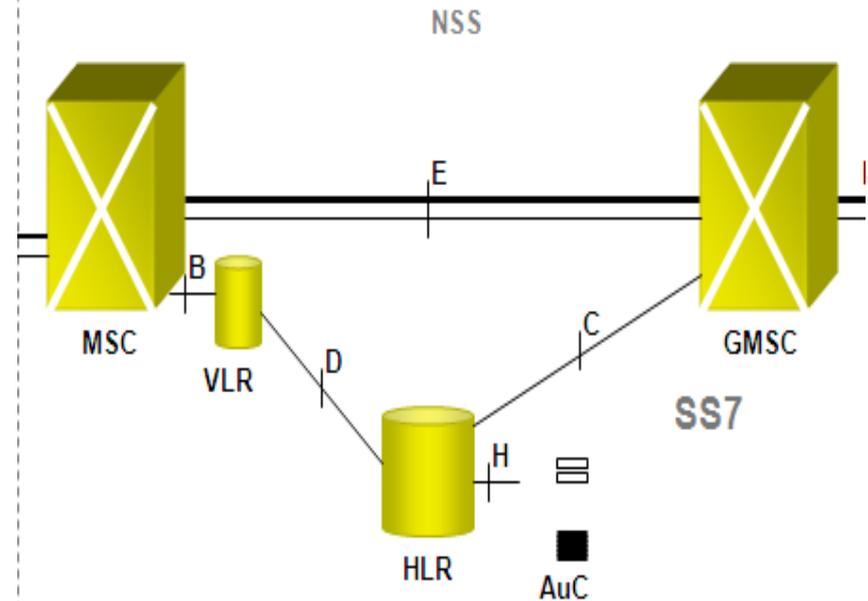




Network subsystem

Performs call processing and subscriber related functions. It includes:

- MSC:** Mobile Switching Centre
- HLR:** Home Location Register
- VLR :** Visitor Location Register
- AuC:** Authentication Centre
- EIR:** Equipment Identity Register
- GMSC:** Gateway MSC.





Mobile switching centre

Network
subsystem

- It is included in the GSM system for call-switching. Its overall purpose is the same as that of any telephone exchange.

The functions carried out by the MSC are listed below:

- **Call Processing**
Includes control of data/voice call setup, inter-BSS and inter-MSC handovers and control of mobility management (subscriber validation and location).
- **Operations and Maintenance Support**
Includes database management, traffic metering and measurement, and a man-machine interface.
- **Internetwork Interworking**
Manages the interface between the GSM network and the PSTN.

When the MSC provides the interface with the other networks in the GSM network it is known as a Gateway MSC.



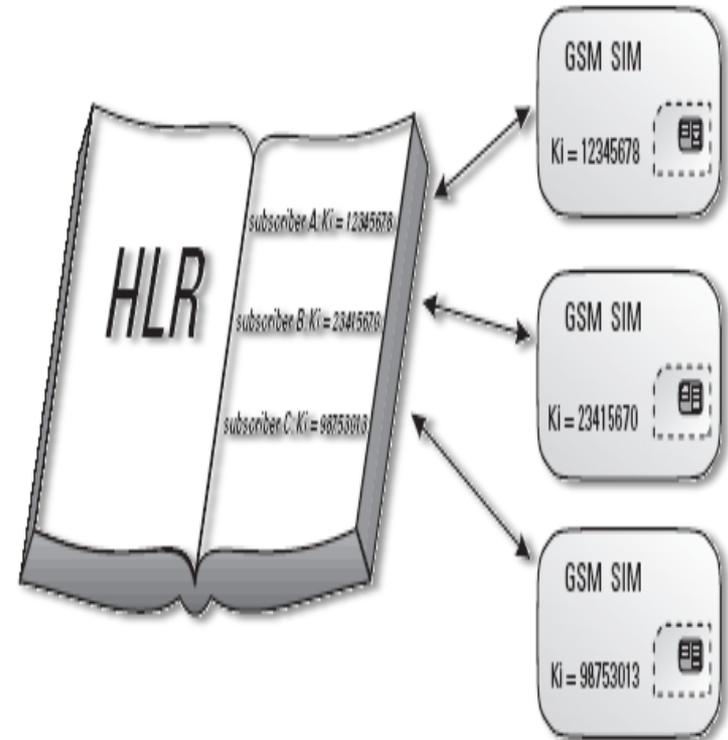


Home location register

Network
subsystem

Reference database for subscriber parameters.

- **Subscriber ID (IMSI & MSISDN).**
- **Current location of subscriber.**
- **Subscriber status (registered/unregistered)**
- **Authentication key and AUC functionality.**
- **Mobile subscriber roaming number.**





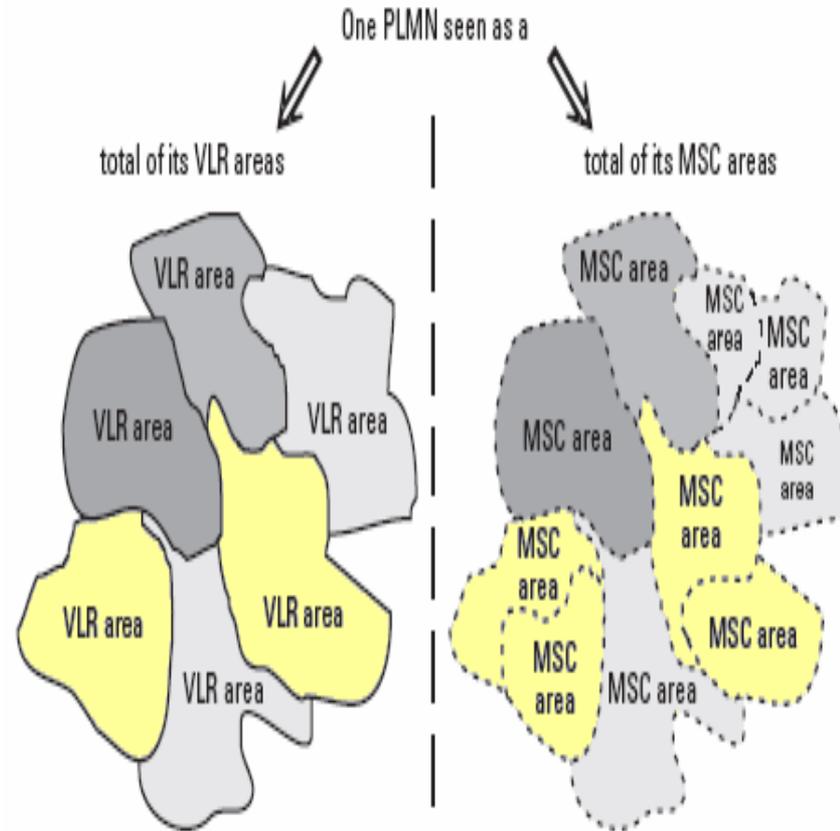
Visitor location register

Network
subsystem

- It provides local database for the subscribers wherever they are physically located within a PLMN, this may or may not be the “home” system. It is a local database and contains copy of most of the data stored in HLR.

It contains:

- Mobile status(busy/free/no ans)
- Location area identity(LAI)
- TMSI AND MSRN .





Authentication centre

Network
subsystem

- **It provides authentication and encryption parameters for verification of subscriber identity.**
- **It ensures confidentiality of each cell.**
- **It protects network operators from frauds in today's cellular world.**
- **It is associated with HLR.**
- **The authentication process will usually take place each time the subscriber “initializes” on the system.**



EQUIPMENT IDENTITY REGISTER



Network
subsystem

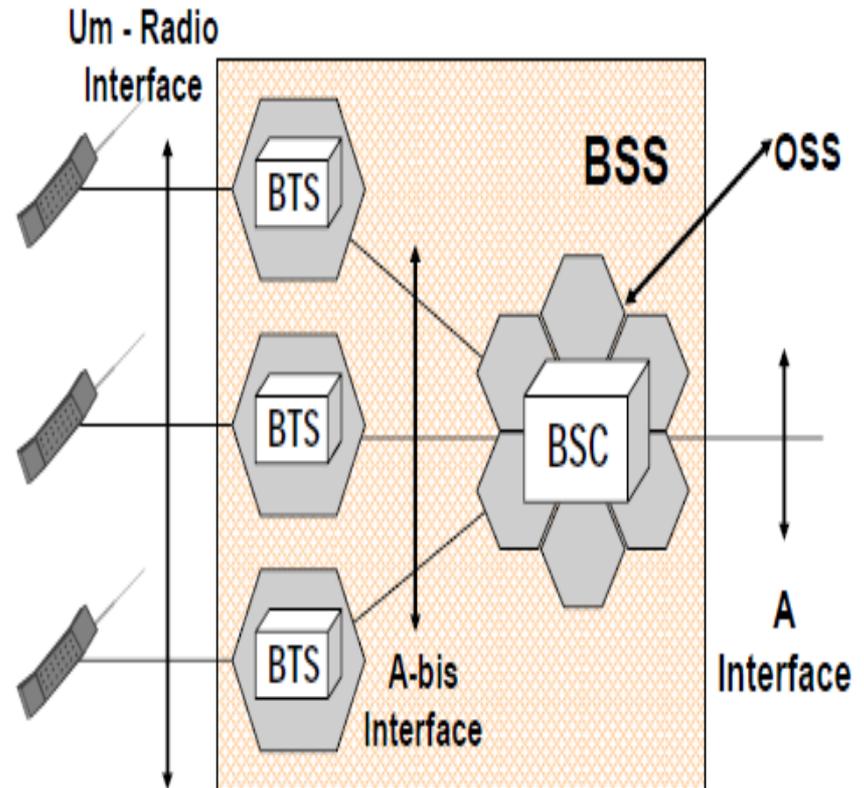
- **The EIR contains a centralized database for validating the International Mobile Equipment Identity (IMEI).**
- **It contains three lists:**
 - **White List**
Contains those IMEIs which are known to have been assigned to valid MS equipment.
 - **Black List**
Contains IMEIs of MS which have been reported stolen or which are to be denied service for some other reason.
 - **Grey List**
Contains IMEIs of MS which have problems (for example, faulty software). These are not, however, sufficiently significant to warrant a “black listing”.





radio subsystem

- Management of radio network and is controlled by a MSC . One MSC controls many radio subsystem.
- It consists of :
- **BSC: Base station controller.**
- **BTS: Base transceiver station.**

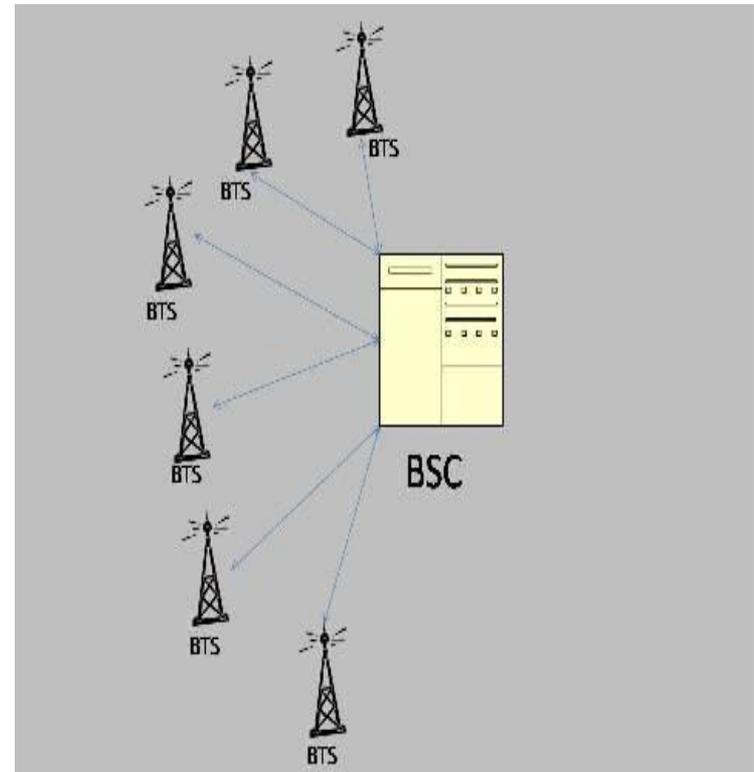




base station controller

RADIO
subsystem

- It is connected to MSC.
- Controls one or more BTS.
- Switches traffic and signaling to/from BTSs and MSC.
- Connects terrestrial circuits and channels on air interface.
- Controls handover performed by BTS.
- Frequency allocation and power control.

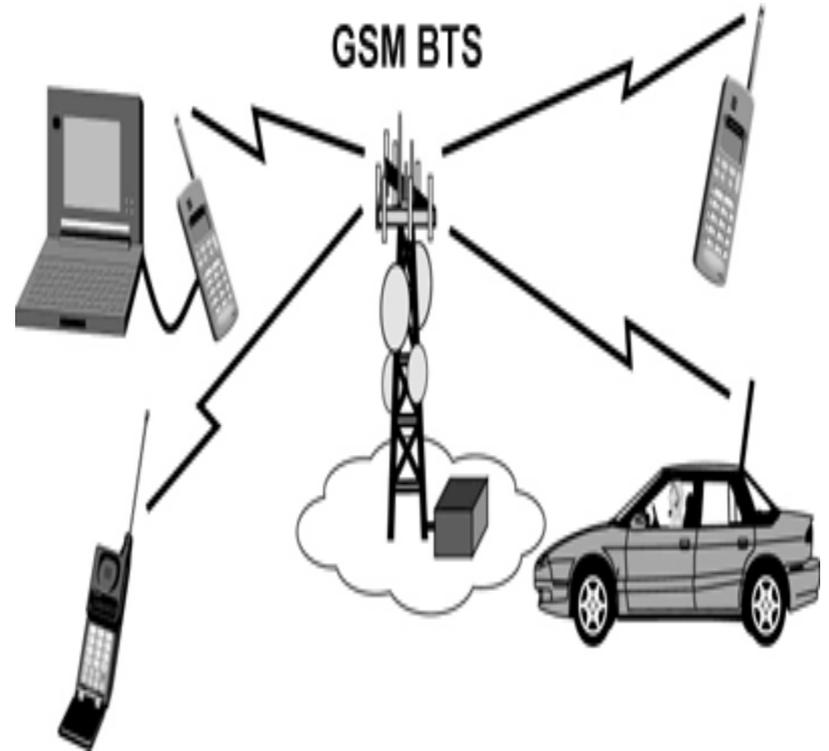




base transceiver station

RADIO
SUBSYSTEM

- **Maintains air interface and minimize transmission problems.**
- **Paging information.**
- **Radio level power control.**
- **BTS identification.**
- **Ciphering**
- **Speech processing.**





OPERATION AND MAINTENANCE SUBSYSTEM

- **Dynamic monitoring and controlling of network.**
- **operation and maintenance data function.**
- **Configuration management.**
- **Fault report and alarm handling.**
- **Performance supervision.**
- **Storage of software and data.**
- **Stores data for minimum one year.**



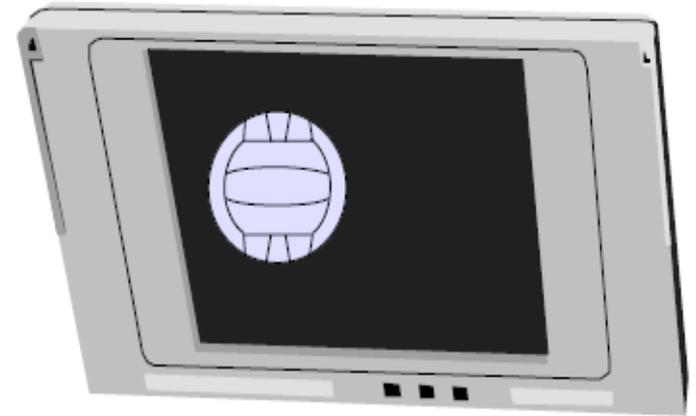


MOBILE STATION (MS)

Mobile Hand set



Subscriber Identity Module



Mobile Equipment Capabilities

- ✓ Encryption capability
- ✓ Frequency capability
- ✓ Short messages service capability.
- ✓ Location updates.
- ✓ Voice and data recognition.

Identified by IMEI no.(International Mobile Equipment Identity)

SIM is a removable module that goes into mobile set. Each SIM has a unique number called IMSI number.

➤ Stores user addresses

- IMSI
- MSISDN
- Temporary addresses for location, roaming, etc

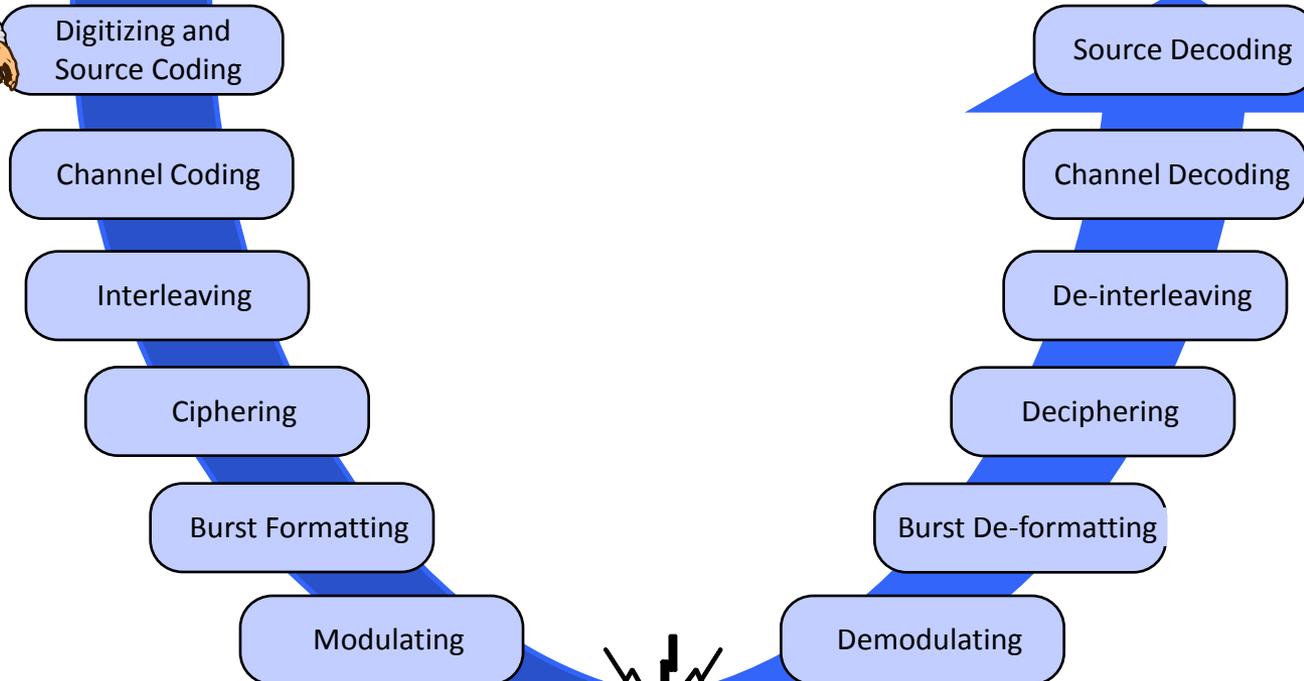




FROM SPEECH TO RADIO TRANSMISSION



Blah... Blah... Blah...

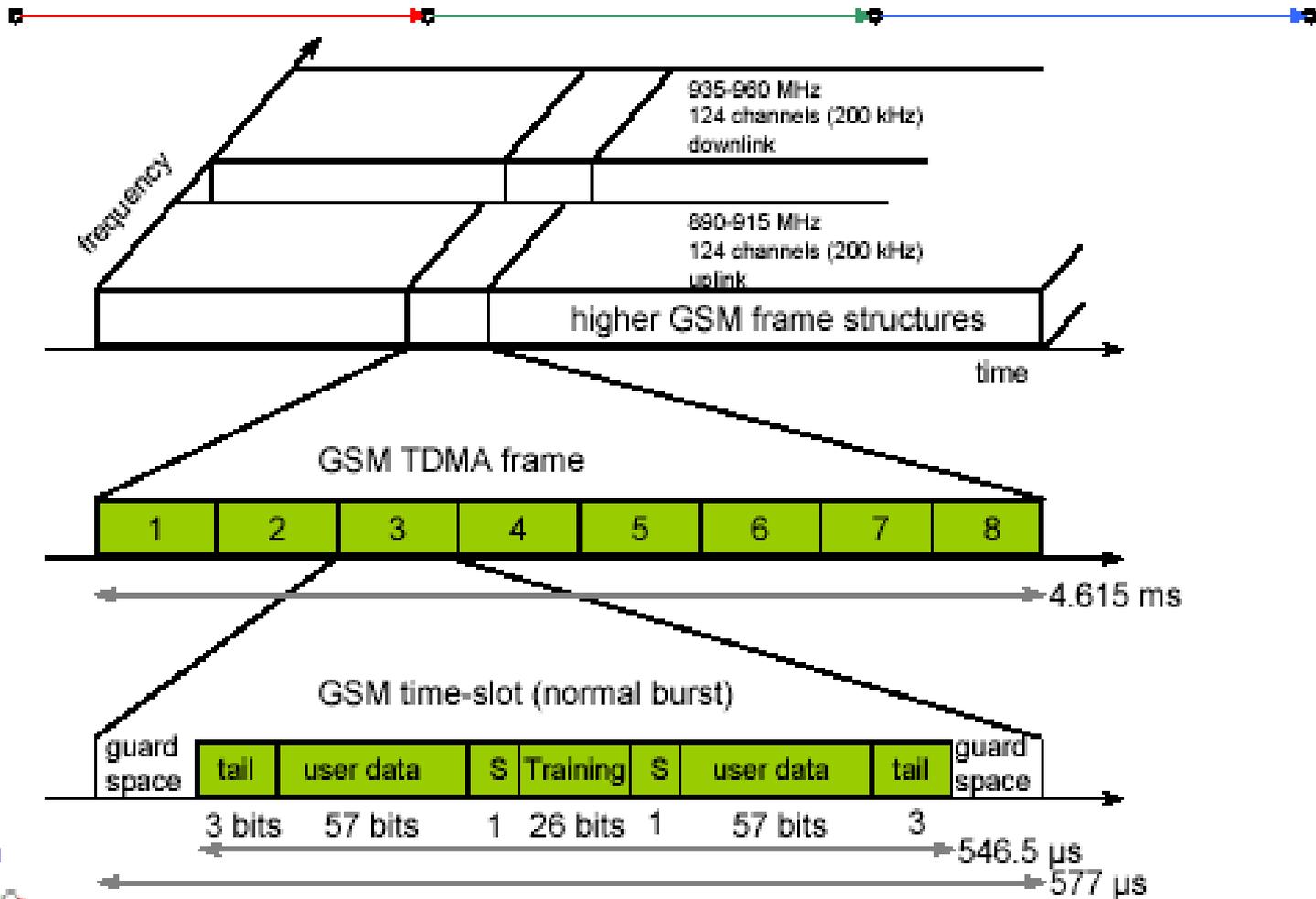


Blah... Blah... Blah...



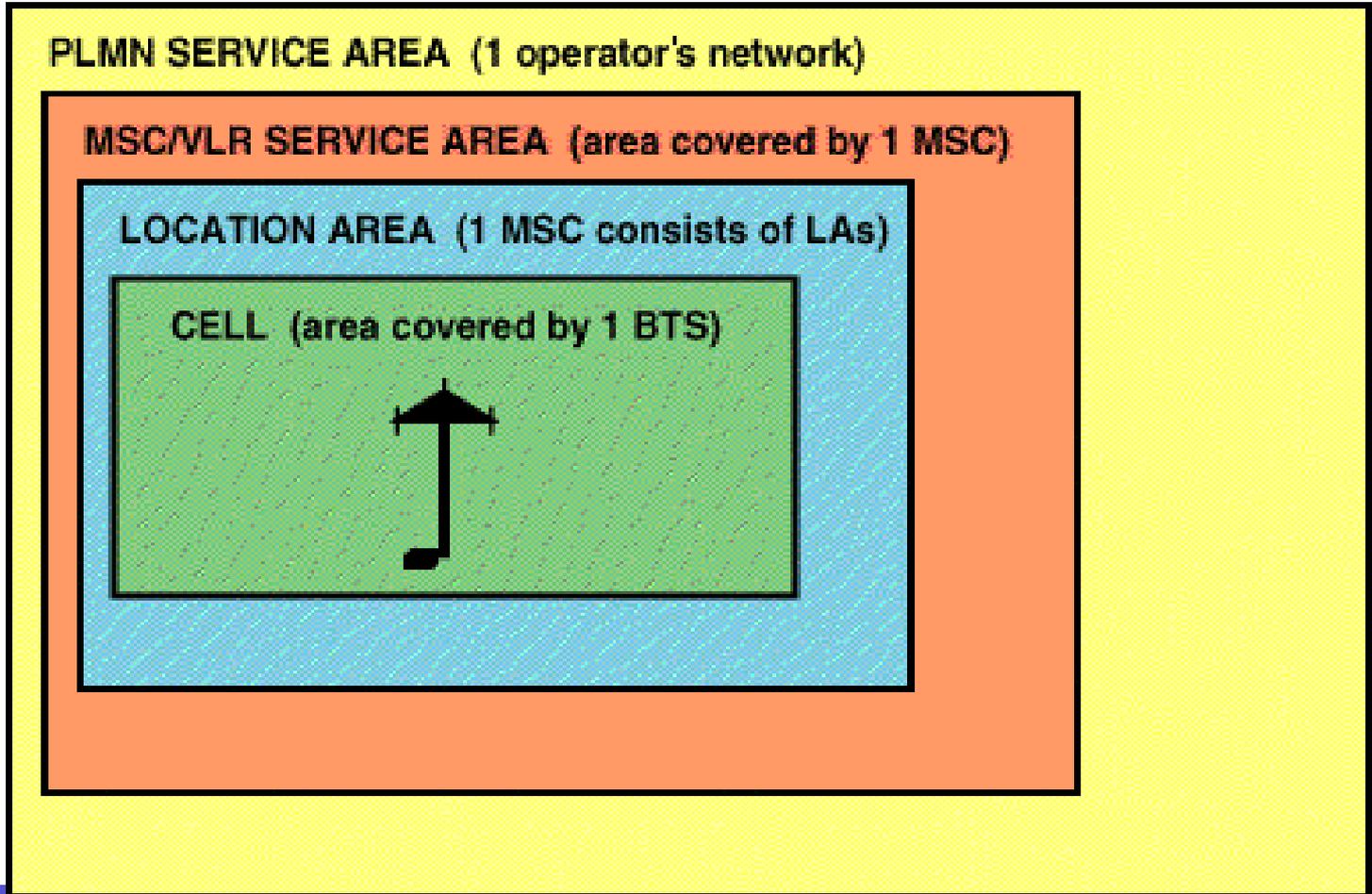
GSM - FRAME STRUCTURE

GSM - TDMA/FDMA

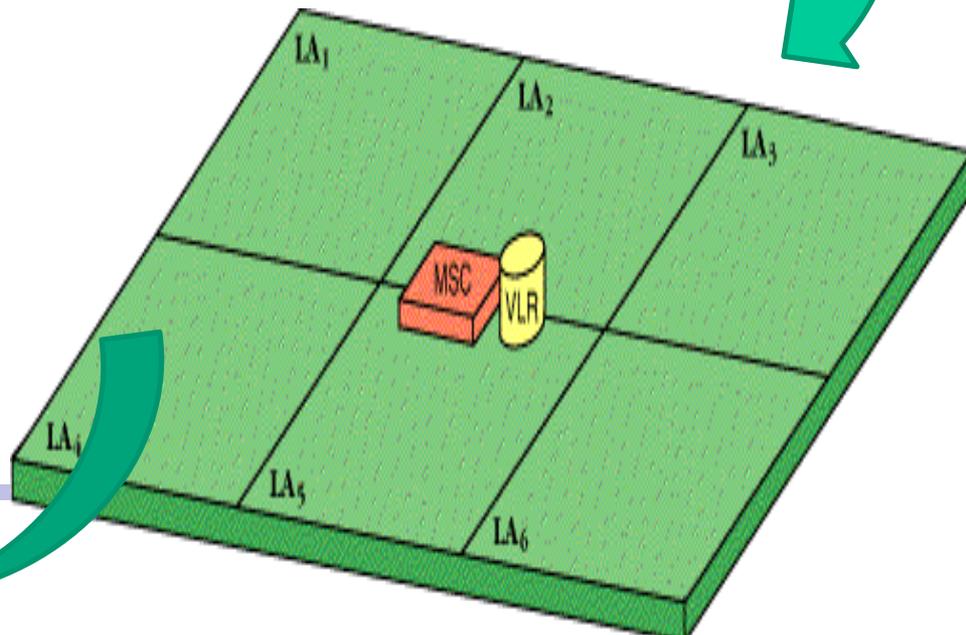
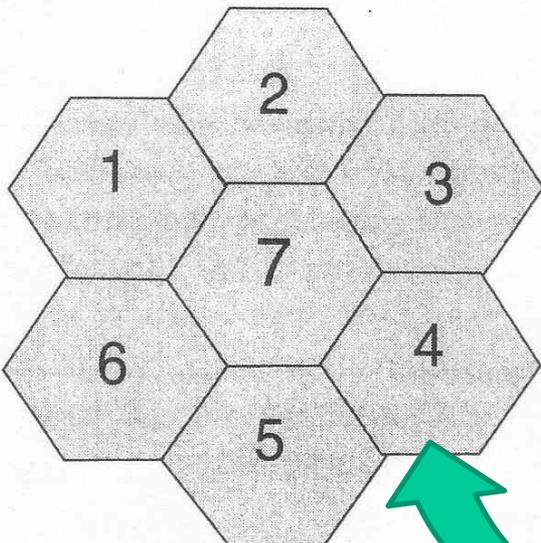
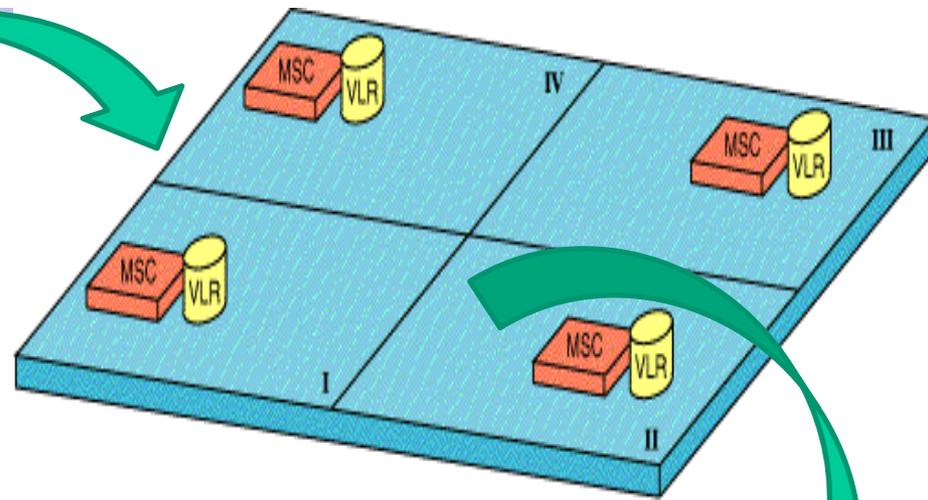
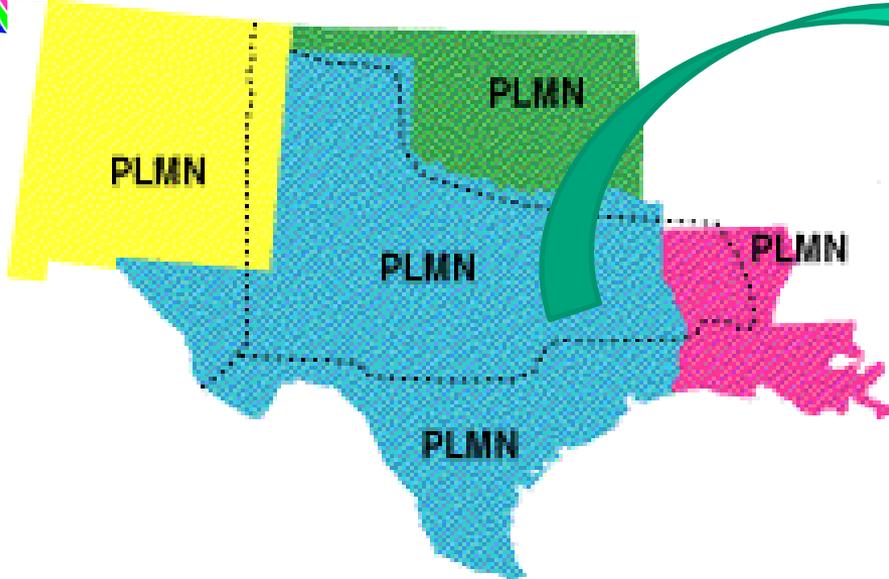




GSM NETWORK AREA



GSM NETWORK AREA CONTD...





MOBILE IDENTIFICATION NUMBERS/ MOBILE IDENTIFIERS

1. International Mobile Equipment Identity

- ✓ Uniquely identifies the mobile equipment.
- ✓ A 15 digit hierarchical address assigned to user at time of manufacturing.

2. International Mobile Subscriber Identity

- ✓ Uniquely identifies the user (SIM CARD).
- ✓ A 15 digit hierarchical address assigned by operator to SIM card upon subscription .

MCC – 3 digits (Mobile Country Code)	MNC – 2 digits (Mobile Network Code)	MSIN – max 10 digits (Mobile Subscriber Identification Number)
Internationally standardized; identifies operator country	Identifies operator network (PLMN) within country	Uniquely identifies subscriber in the operator network





CONTINUED...

3. Mobile Subscriber ISDN Number (MSISDN)

→ MSISDN: the “usual” telephone number

- ⇒ Follows international ISDN numbering plan (ITU-T E.164 recommendations)
- ⇒ Structure:

CC – up to 3 digits (Country Code)	NDC – 3 digits (for PLMN) (National Destination Code)	SN – max 10 digits (Subscriber Number)
---------------------------------------	--	---

4. TEMPORARY ADDRESS

→ TMSI - Temporary Mobile Subscriber Identity

- ⇒ 32 bits
- ⇒ assigned by VLR within an administrative area
 - has significance only in this area
- ⇒ transmitted on the radio interface instead of IMSI

→ MSRN - Mobile Station Roaming Number

- ⇒ An MSISDN number
 - CC, NDC of the visited network
 - SN assigned by VLR
- ⇒ Used to route calls to a roaming MS



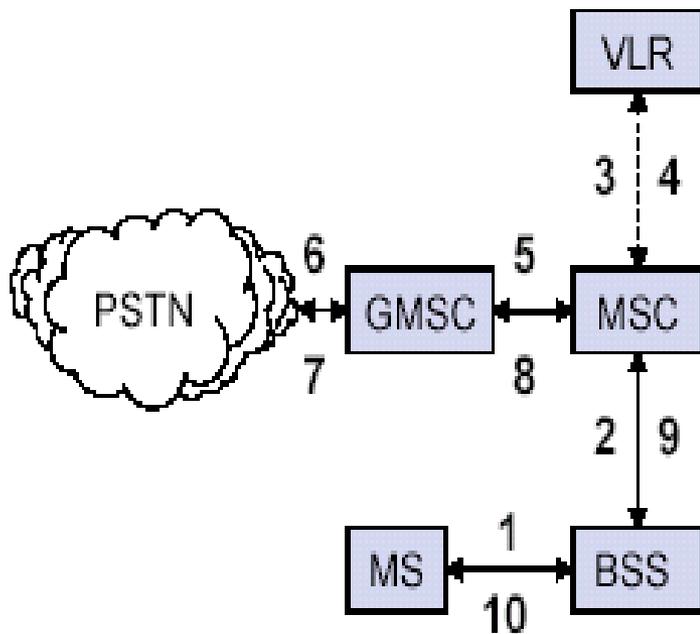


CALL ROUTING

- Call Originating from MS
- Call termination to MS

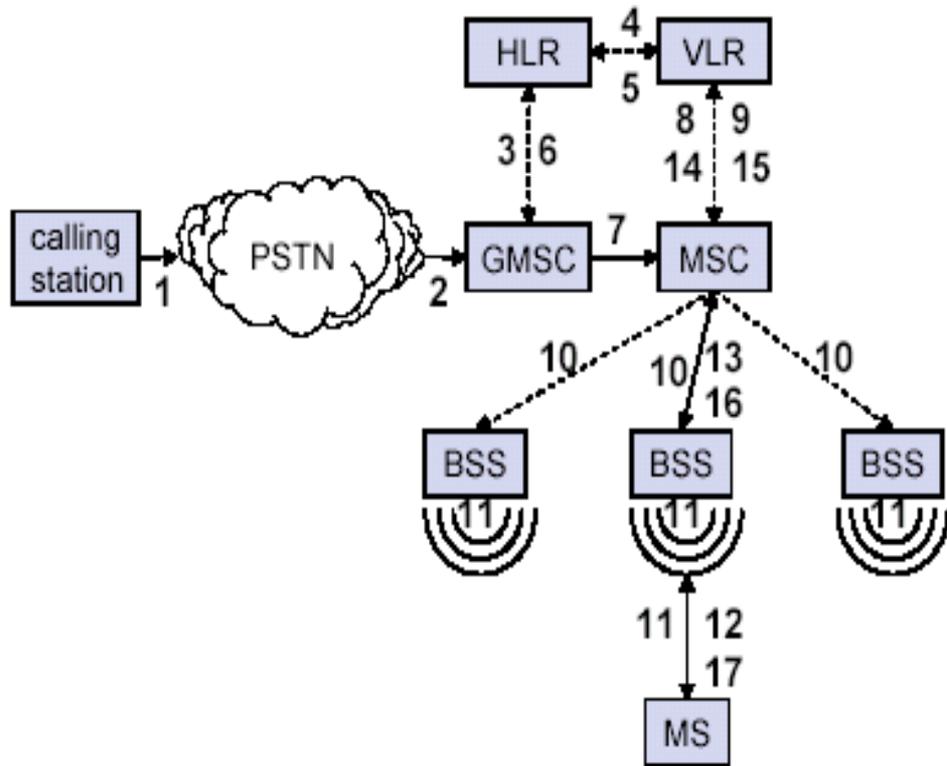


OUTGOING CALL



1. MS sends dialed number to BSS
2. BSS sends dialed number to MSC
- 3,4 MSC checks VLR if MS is allowed the requested service. If so, MSC asks BSS to allocate resources for call.
- 5 MSC routes the call to GMSC
- 6 GMSC routes the call to local exchange of called user
- 7, 8,
- 9,10 Answer back (ring back) tone is routed from called user to MS via GMSC, MSC, BSS

INCOMING CALL



1. Calling a GSM subscribers
2. Forwarding call to GSMC
3. Signal Setup to HLR
4. 5. Request MSRN from VLR
6. Forward responsible MSC to GMSC
7. Forward Call to current MSC
8. 9. Get current status of MS
- 10.11. Paging of MS
- 12.13. MS answers
- 14.15. Security checks
- 16.17. Set up connection

FUTURE OF GSM

❖ 2nd Generation

- ❑ GSM -9.6 Kbps (data rate)

❖ 2.5 Generation (Using now in Iraq)

- ❑ HSCSD (High Speed ckt Switched data)

 - Data rate : 76.8 Kbps (9.6 x 8 kbps)

- ❑ GPRS (General Packet Radio service)

 - Data rate: 14.4 - 115.2 Kbps

- ❑ EDGE (Enhanced data rate for GSM Evolution)

 - Data rate: 547.2 Kbps (max)

❖ 3 Generation

- ❑ WCDMA(Wide band CDMA)

 - Data rate : 0.348 – 2.0 Mbps



Architecture of the GSM system

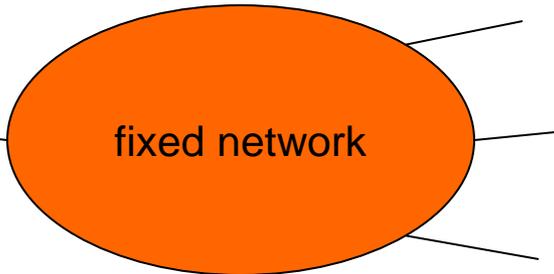
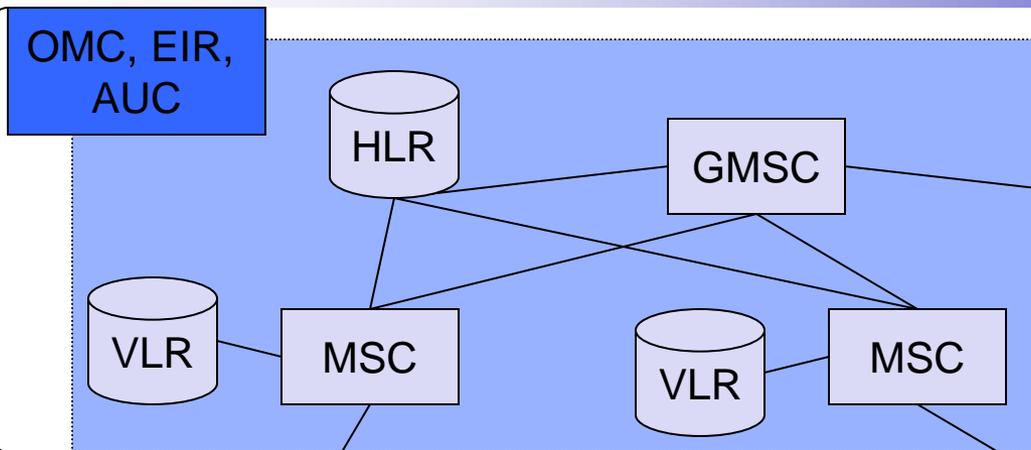
- **GSM is a PLMN (Public Land Mobile Network)**
 - ❑ **several providers setup mobile networks following the GSM standard within each country**
 - ❑ **components**
 - MS (mobile station)
 - BS (base station)
 - MSC (mobile switching center)
 - LR (location register)
 - ❑ **subsystems**
 - RSS (radio subsystem): covers all radio aspects
 - NSS (network and switching subsystem): call forwarding, handover, switching
 - OSS (operation subsystem): management of the network



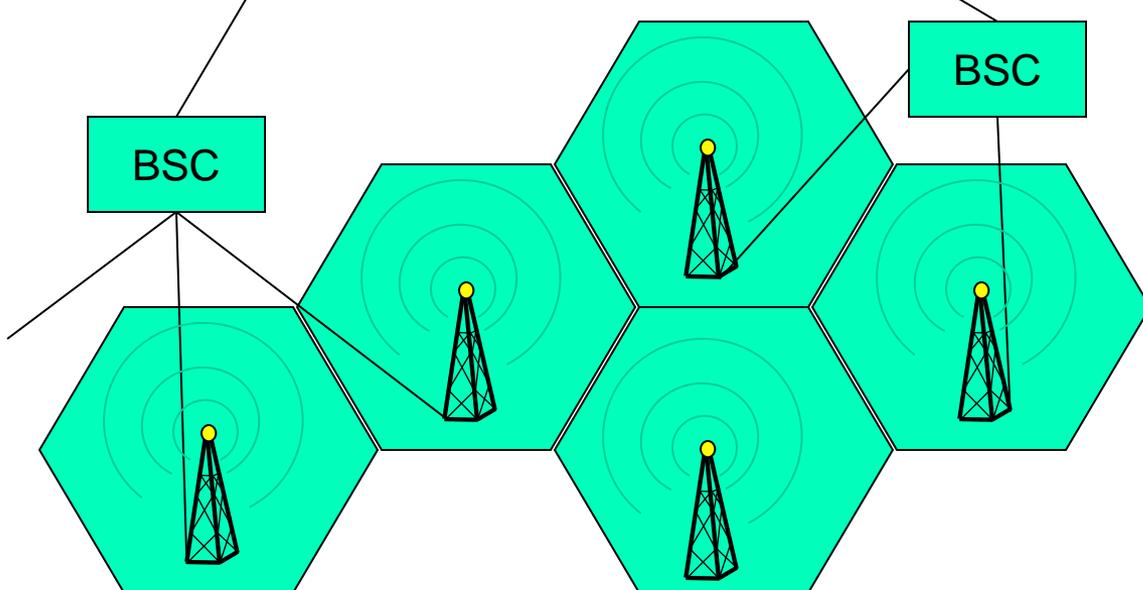


GSM: overview

NSS
with OSS

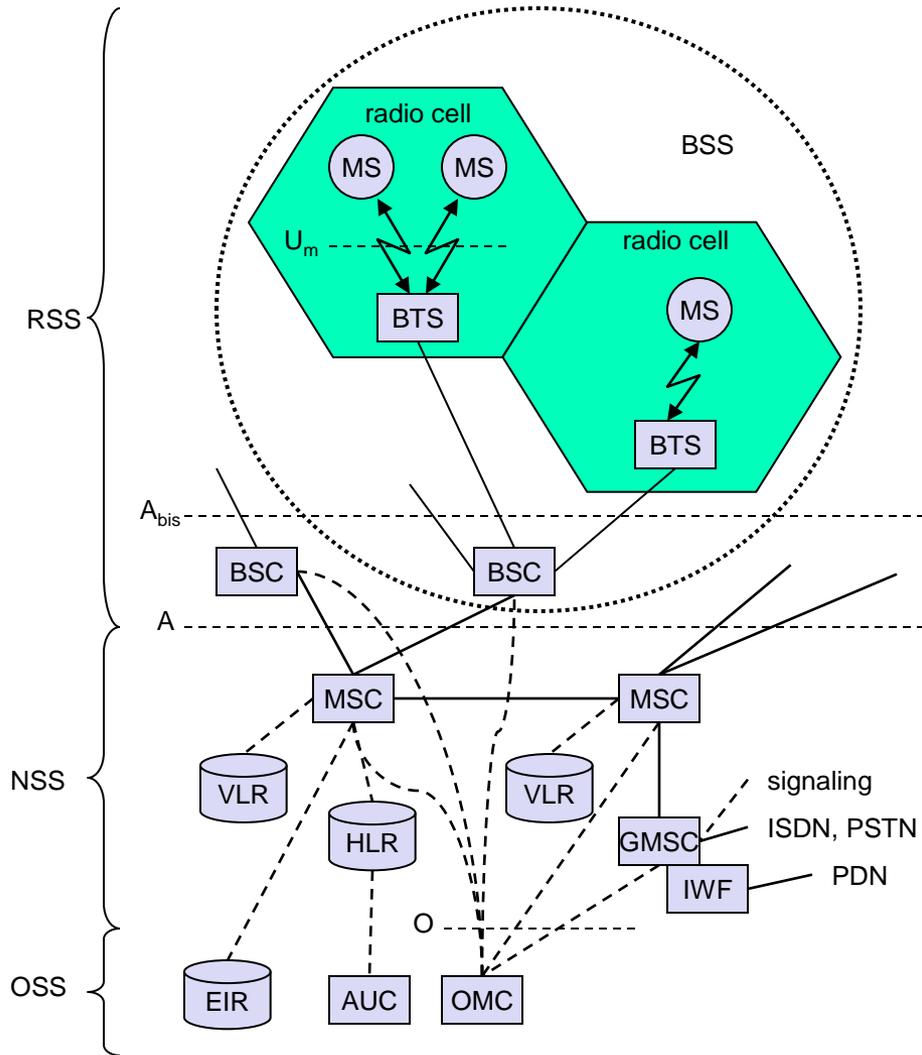


RSS



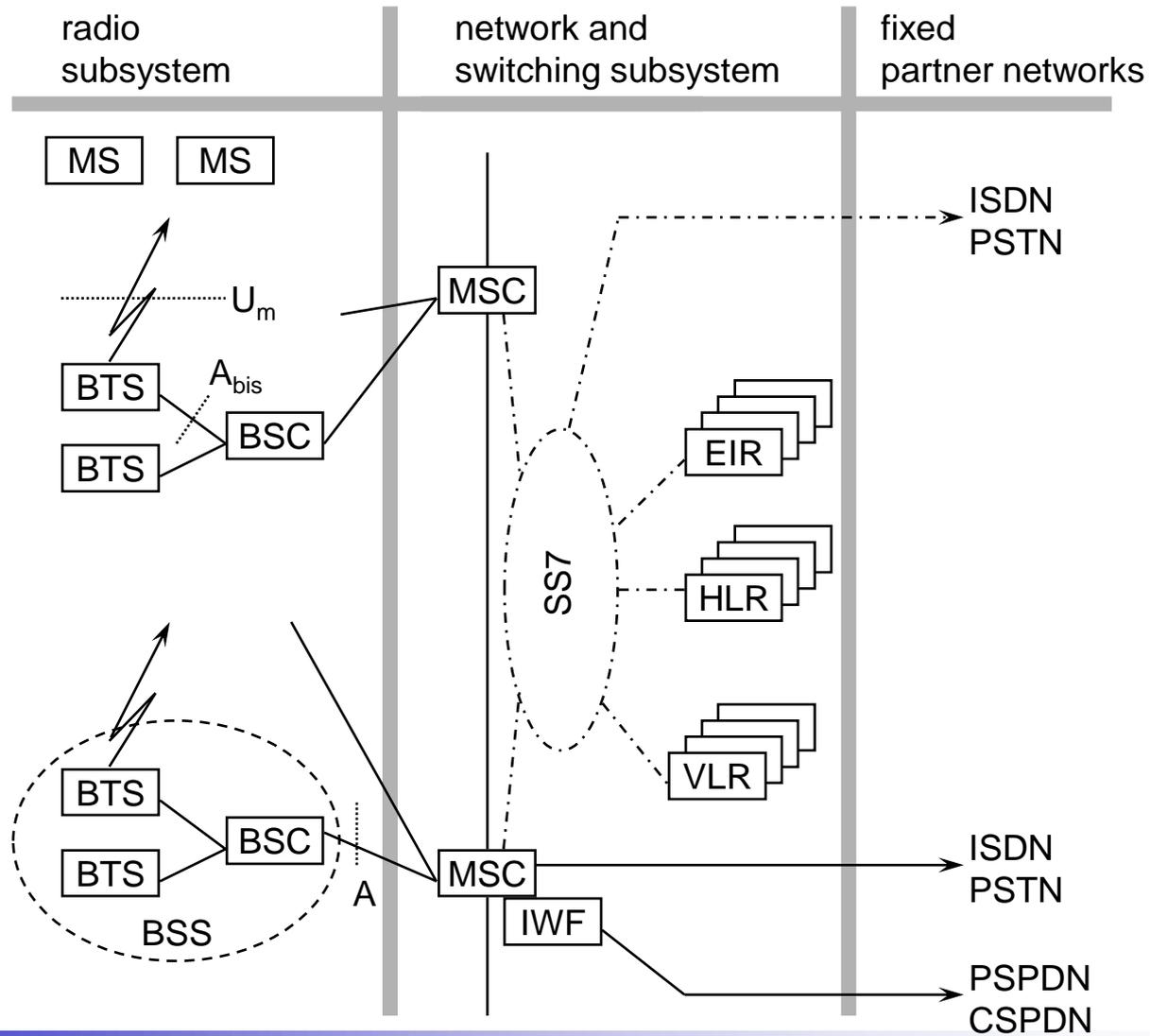


GSM: elements and interfaces



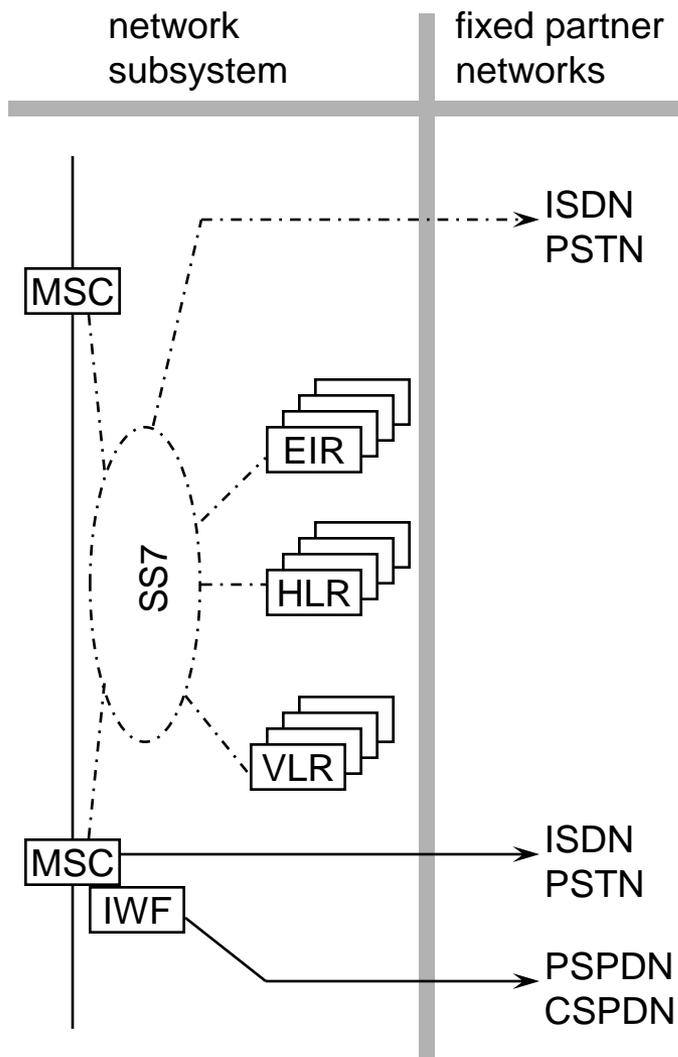


GSM: system architecture





System architecture: network and switching subsystem



Components

- MSC* (Mobile Services Switching Center):
- IWF* (Interworking Functions)

- ISDN* (Integrated Services Digital Network)
- PSTN* (Public Switched Telephone Network)
- PSPDN* (Packet Switched Public Data Net.)
- CSPDN* (Circuit Switched Public Data Net.)

Databases

- HLR* (Home Location Register)
- VLR* (Visitor Location Register)
- EIR* (Equipment Identity Register)





Radio subsystem

- **The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers**
- **Components**
 - ❑ **Base Station Subsystem (BSS):**
 - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
 - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (U_m) onto terrestrial channels (A interface)
 - $BSS = BSC + \text{sum}(BTS) + \text{interconnection}$
 - ❑ **Mobile Stations (MS)**





Cellular systems generations

- **1G (first generation) – voice-oriented systems based on analog technology; ex.: Advanced Mobile Phone Systems (AMPS) and cordless systems**
 - **2G (second generation) - voice-oriented systems based on digital technology; more efficient and used less spectrum than 1G; ex.: Global System for Mobile (GSM) and US Time Division Multiple Access (US-TDMA)**
 - **3G (third generation) – high-speed voice-oriented systems integrated with data services; ex.: General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA)**
 - **4G (fourth generation) – still experimental, not deployed yet; based on Internet protocol networks and will provide voice, data and multimedia service to subscribers**
-





Frequency reuse

- is a method used by service providers to improve the efficiency of a cellular network and to serve millions of subscribers using a limited radio spectrum
- is based on the fact that after a distance a radio wave gets attenuated and the signal falls below a point where it can no longer be used or cause any interference
- a transmitter transmitting in a specific frequency range will have only a limited coverage area
- beyond this coverage area, that frequency can be reused by another transmitter





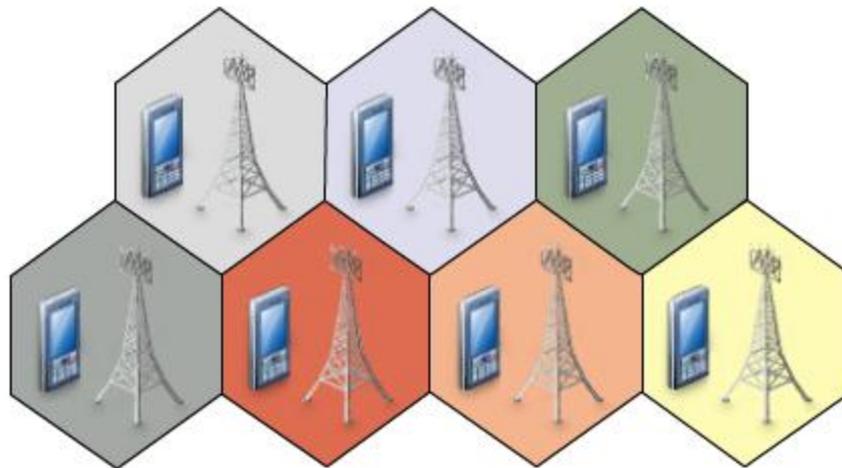
Network Cells

- the entire network coverage area is divided into cells based on the principle of frequency reuse
- a cell = basic geographical unit of a cellular network; is the area around an antenna where a specific frequency range is used; is represented graphically as a hexagonal shape, but in reality it is irregular in shape
- when a subscriber moves to another cell, the antenna of the new cell takes over the signal transmission
- a cluster is a group of adjacent cells, usually 7 cells; no frequency reuse is done within a cluster
- the frequency spectrum is divided into subbands and each subband is used within one cell of the cluster

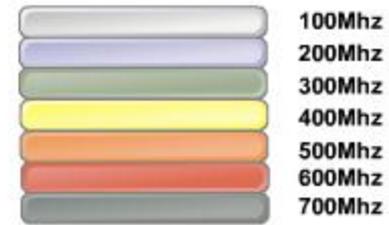




Network cells (2)



Cell Cluster



Frequency Spectrum





Types of cells

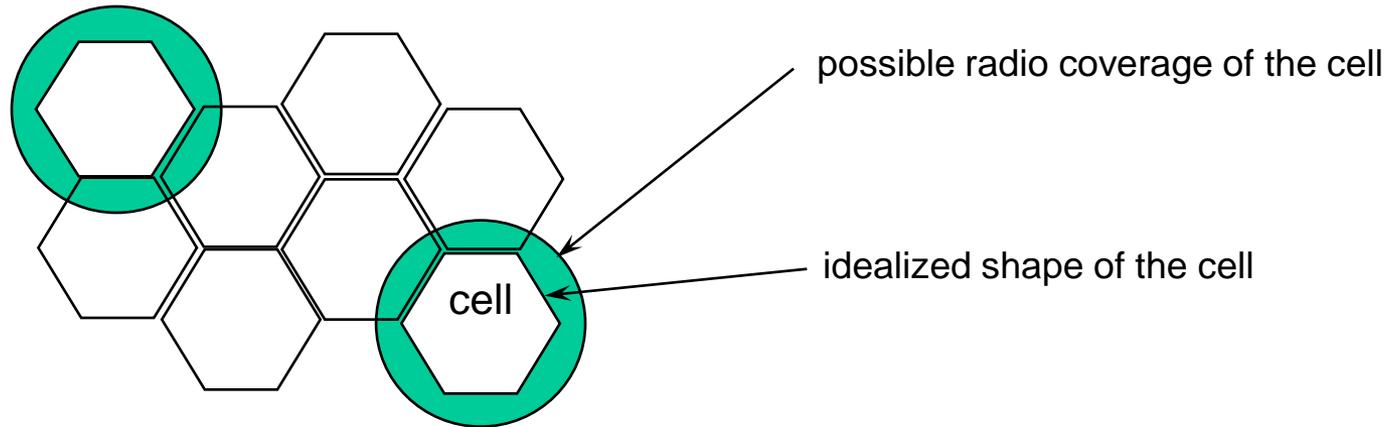
- **macrocell** – their coverage is large (aprox. 6 miles in diameter); used in remote areas, high-power transmitters and receivers are used
- **microcell** – their coverage is small (half a mile in diameter) and are used in urban zones; low-powered transmitters and receivers are used to avoid interference with cells in another clusters
- **picocell** – covers areas such as building or a tunnel





GSM: cellular network

segmentation of the area into cells



- ❑ use of several carrier frequencies
- ❑ not the same frequency in adjoining cells
- ❑ cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- ❑ hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- ❑ if a mobile user changes cells
 ↓ handover of the connection to the neighbor cell





Base Transceiver Station and Base Station Controller

- **Tasks of a BSS are distributed over BSC and BTS**
- **BTS comprises radio specific functions**
- **BSC is the switching center for radio channels**

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





Network and switching subsystem

- **NSS is the main component of the public mobile network GSM**
 - ❑ **switching, mobility management, interconnection to other networks, system control**
- **Components**
 - ❑ **Mobile Services Switching Center (MSC)**
controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
 - ❑ **Databases (important: scalability, high capacity, low delay)**
 - Home Location Register (HLR)
central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
 - Visitor Location Register (VLR)
local database for a subset of user data - data about all users currently visiting in the domain of the VLR





Mobile Services Switching Center

- **The MSC (mobile switching center) plays a central role in GSM**
 - ❑ switching functions
 - ❑ additional functions for mobility support
 - ❑ management of network resources
 - ❑ interworking functions via Gateway MSC (GMSC)
 - ❑ integration of several databases
- **Functions of a MSC**
 - ❑ specific functions for paging and call forwarding
 - ❑ termination of SS7 (signaling system no. 7)
 - ❑ mobility specific signaling
 - ❑ location registration and forwarding of location information
 - ❑ provision of new services (fax, data calls)
 - ❑ support of short message service (SMS)
 - ❑ generation and forwarding of accounting and billing information





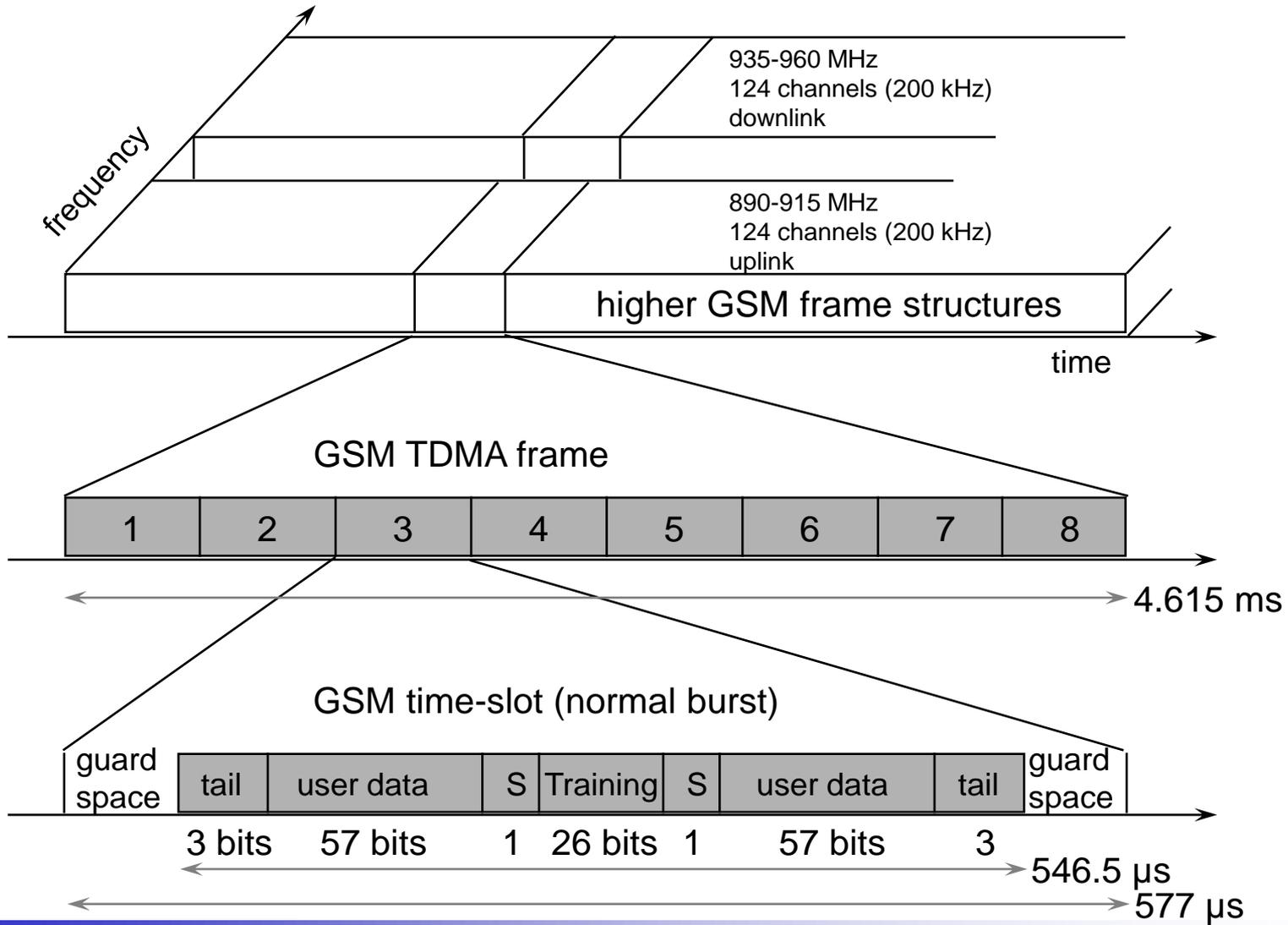
Operation subsystem

- **The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems**
- **Components**
 - ❑ **Authentication Center (AUC)**
 - generates user specific authentication parameters on request of a VLR
 - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
 - ❑ **Equipment Identity Register (EIR)**
 - registers GSM mobile stations and user rights
 - stolen or malfunctioning mobile stations can be locked and sometimes even localized
 - ❑ **Operation and Maintenance Center (OMC)**
 - different control capabilities for the radio subsystem and the network subsystem





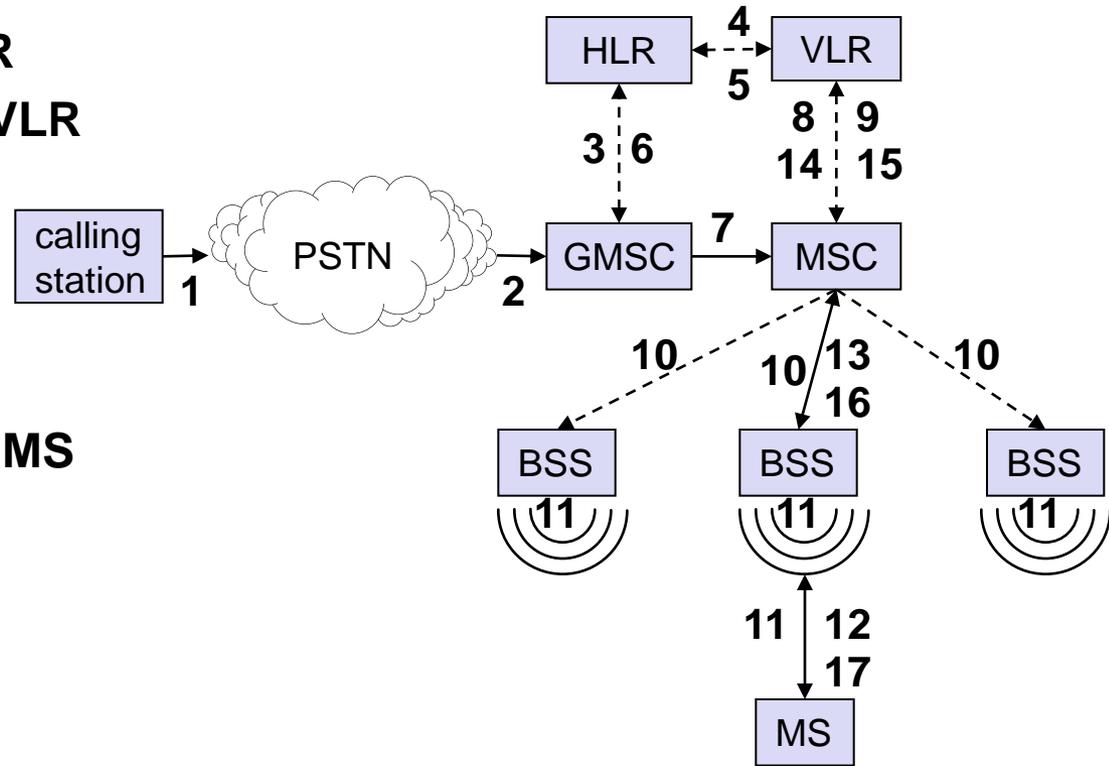
GSM Radio Interface - TDMA/FDMA





Mobile Terminated Call

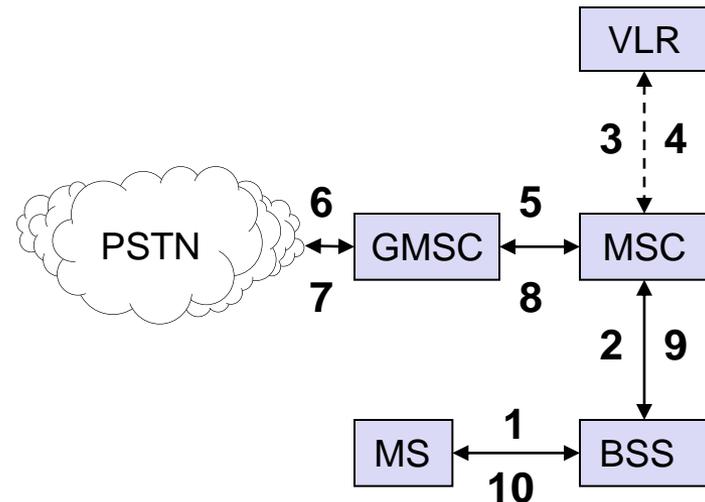
- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4, 5: request MSRN from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: set up connection





Mobile Originated Call

- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call





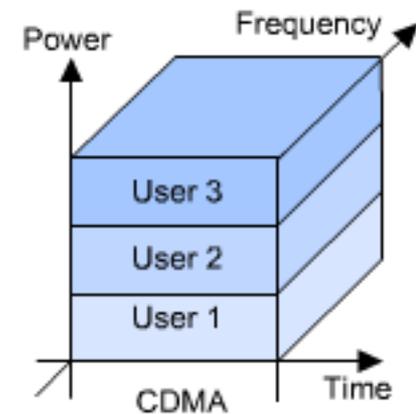
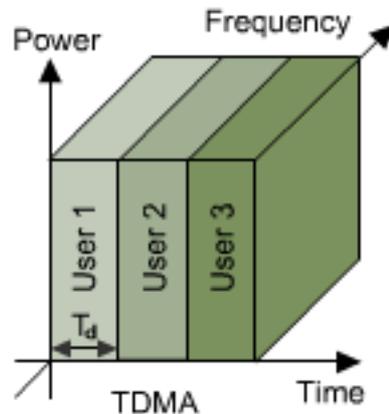
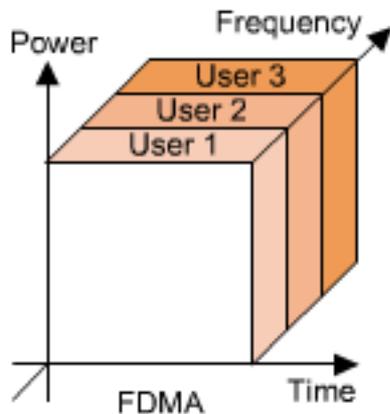
Other cellular concepts

- **handover = moving a call from one zone (from the transmitter-receiver from one zone) to another zone due to subscriber's mobility**
- **roaming = allowing the subscriber to send/receive calls outside the service provider's coverage area**





Multiple access schemes



Frequency Division Multiple Access

- when the subscriber enters another cell a unique frequency is assigned to him; used in analog systems

Time Division Multiple Access

- each subscriber is assigned a time slot to send/receive a data burst; is used in digital systems

Code Division Multiple Access

- each subscriber is assigned a code which is used to multiply the signal sent or received by the subscriber





The control channel

- **this channel is used by a cellular phone to indicate its presence before a frequency/time slot/code is allocated to him**





Cellular services

- **voice communication**
- **Short Messaging Service (SMS)**
- **Multimedia Messaging Service (MMS)**
- **Global Positioning System (GPS)**
- **Wireless Application Protocol (WAP) – to access the Internet**





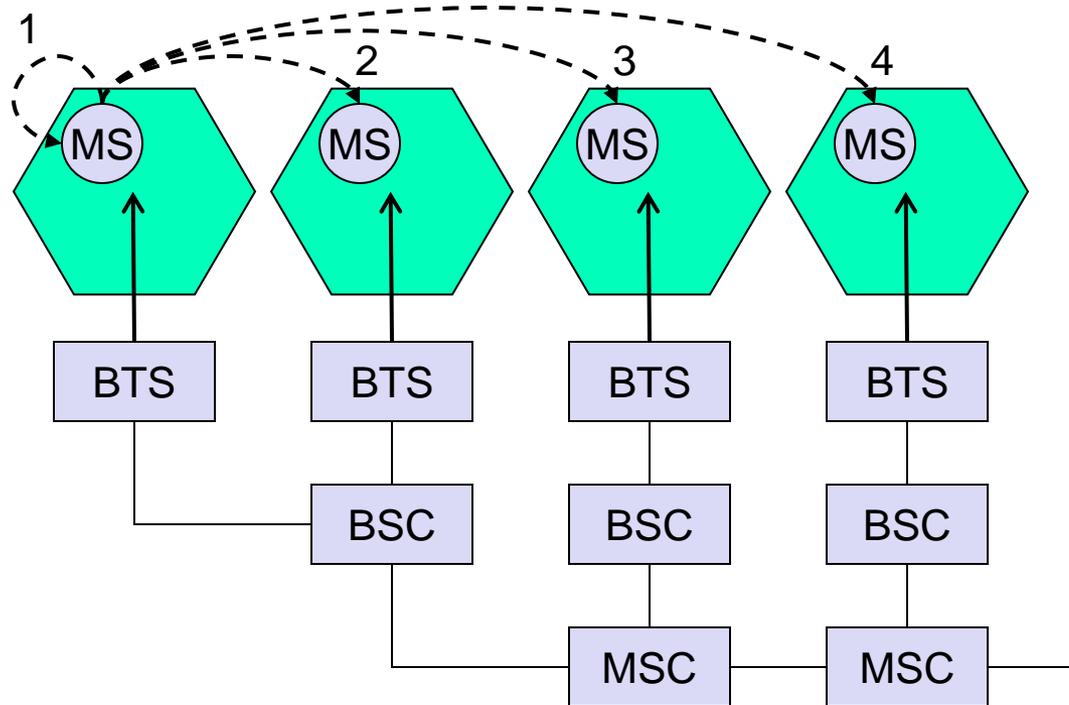
Handoffs

- GSM uses **mobile assisted hand-off (MAHO)**. Signal strength measurements are sent to the BS from the mobile.
- The MSC decides when to do a handoff and it informs the new BS and the mobile.
- When a mobile switches to a new BS it sends a series of shortened bursts to adjust its timing (giving the bS time to calculate it and send it) and allow the new BS to synchronize its receiver to the arrival time of the messages





4 types of handover





Handover decision

