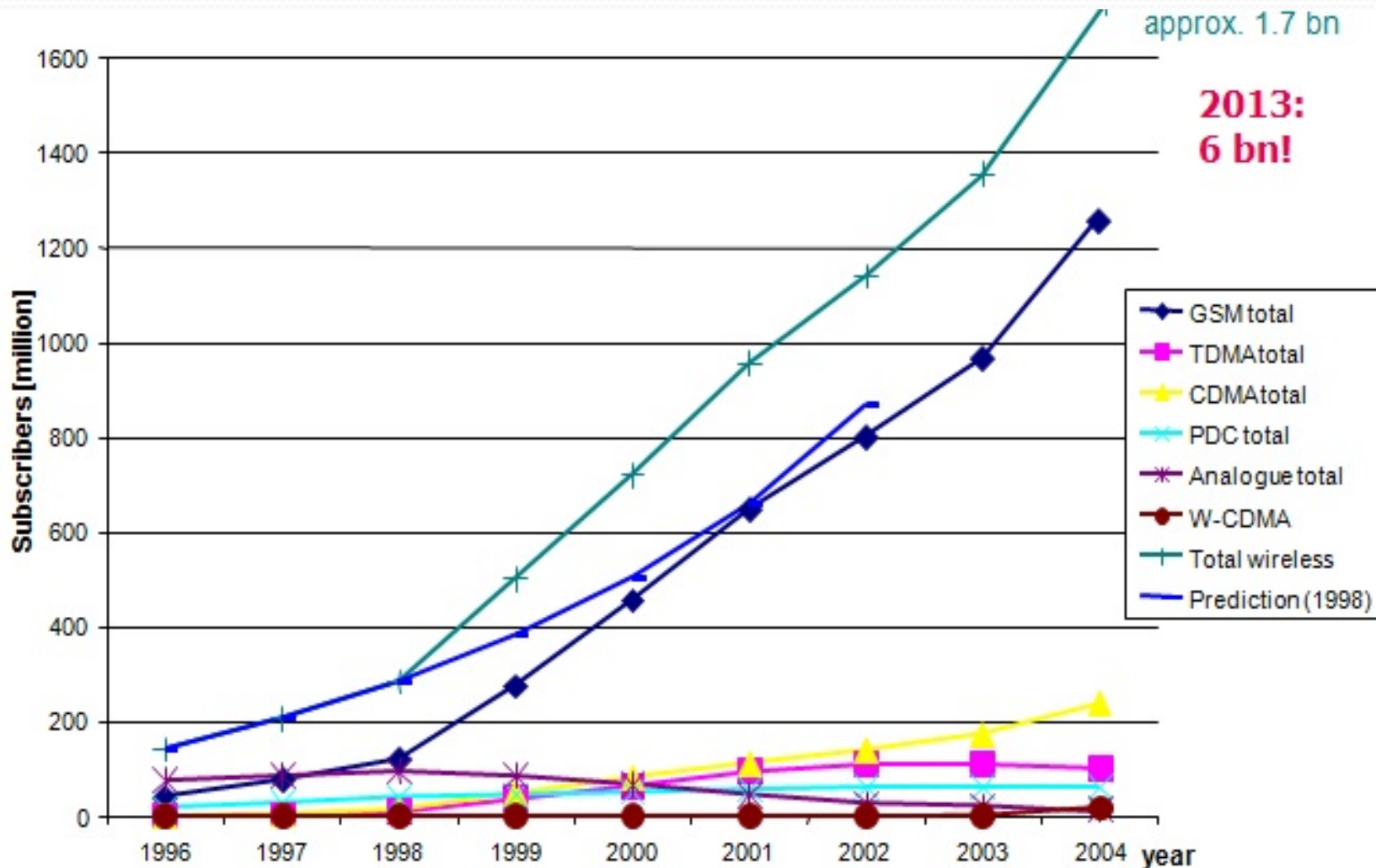


Mobile Computing – Telecommunication Systems

- **Digital Cellular Networks:** used for mobile and wireless devices.
- DCN are the wireless extensions of traditional PSTN or ISDN networks and allows for seamless roaming.
- Basically used for voice traffic
- Technology for wireless data transmission using cellular systems.

Mobile phone subscribers worldwide



GSM: Overview

- GSM
 - Formerly: Groupe Spéciale Mobile (founded 1982)
 - Now: Global System for Mobile Communication
- Today many providers all over the world use GSM
 - more than 4,2 billion subscribers
 - more than 75% of all digital mobile phones use GSM

Performance characteristics of GSM (wrt. analog sys.)

- 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 localization
- 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

Disadvantages of GSM

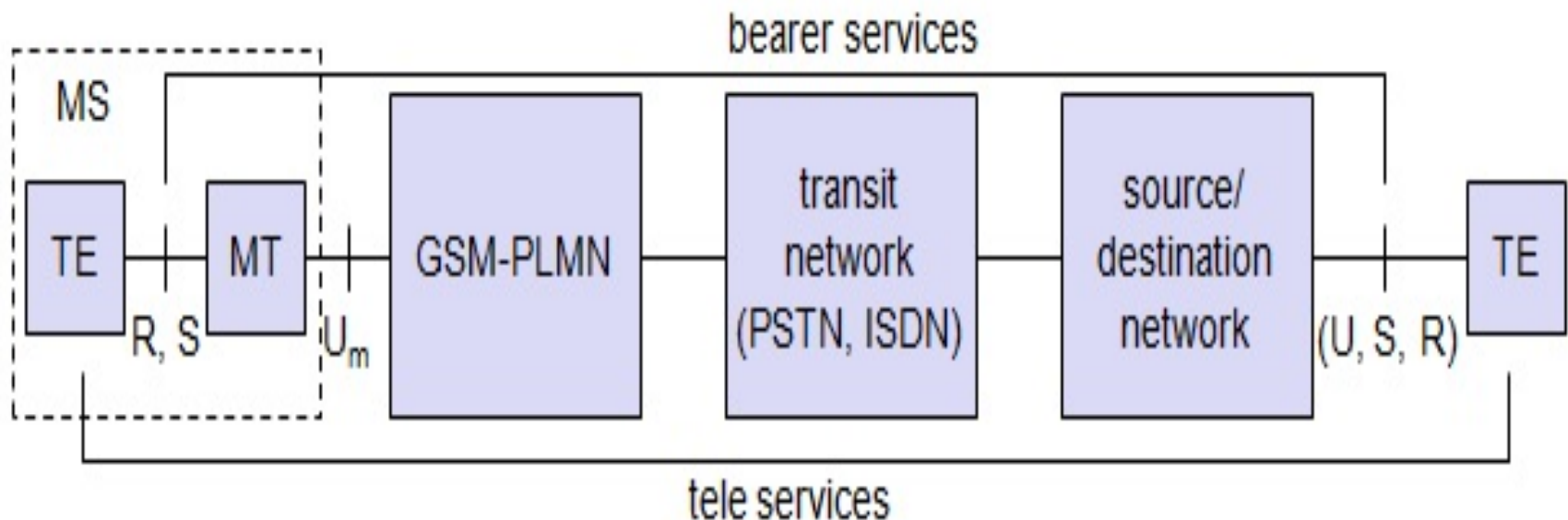
- There is no perfect system!!
 - Security issues
 - Less bandwidth
- Electromagnetic radiation
- Abuse of private data possible
- Roaming profiles accessible
- High complexity of the system
- Several incompatibilities within the GSM standards

GSM: Mobile Services

- GSM offers
 - several types of connections
 - voice connections, data connections, short message service
 - multi-service options (combination of basic services)
- Three service domains
 - Bearer Services
 - Service that allows transmission of information signals between network interfaces
 - These services give the subscriber the capacity required to transmit appropriate signals between certain access points, i.e. user network interfaces
 - Tele Services
 - Voice calls: most basic service
 - Video text access, speech, etc
 - Supplementary Services
 - Call forwarding
 - Call hold
 - Call waiting

Bearer and Tele services Reference Model

- MS- Mobile Station, TE- Terminal, MT – Mobile Termination, PLMN – Public Land Mobile Network, PSTN – Public Switched Telephone Network, ISDN – Integrated Services Digital Network



Bearer Services

- Telecommunication services to transfer data between access points
- Specification of services up to the terminal interface (OSI layers 1-3)
- Different data rates for voice and data (original standard)
 - **Transparent bearer service** (use only physical layer to transmit data – Forward error correction (FEC) only)
constant delay and throughput
 - **Non transparent bearer service** (use protocols of layer 2 and 3 to implement error correction and flow control)
- Data rates of approx. 50 kbit/s possible – (even more with new modulation)

Tele Services I

- Telecommunication services that enable voice communication via mobile phones
- All these basic services have to obey cellular functions, security measurements etc.
- Offered services
 - Mobile Telephony
primary goal of GSM was to enable mobile telephony offering the traditional bandwidth of 3.1 kHz
 - Emergency Number
common number throughout Europe (112); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)
 - Multinumbering
several ISDN phone numbers per user possible

Tele Services II

- Additional services
 - Non-Voice-Teleservices
 - Fax
 - Voice mailbox (implemented in the fixed network supporting the mobile terminals)
 - Electronic mail (MHS- Message Handling System, implemented in the fixed network)
 - Short Message Service (SMS)

Alphanumeric data transmission to/from the mobile terminal (160 characters) using the signaling channel, thus allowing simultaneous use of basic services and SMS.

Supplementary services

- Services in addition to the basic services.
- Similar to ISDN services besides lower bandwidth due to the radio link
- May differ between different service providers, countries and protocol versions
- Important services
 - Identification: forwarding of caller number
 - Suppression of number forwarding
 - Automatic call-back
 - Conferencing with many participants.
 - Locking of the mobile terminal (incoming or outgoing calls)

GSM Requirements - Application Devices



GSM Requirements - Antennas



Infrastructure (cabling & base stations)



Base Stations



Cabling



Microwave links



Infrastructure (Monitoring & Switching Units)



Switching units



Management

Data bases

Monitoring



Architecture of the GSM system

- GSM is a PLMN (Public Land Mobile Network)
 - 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

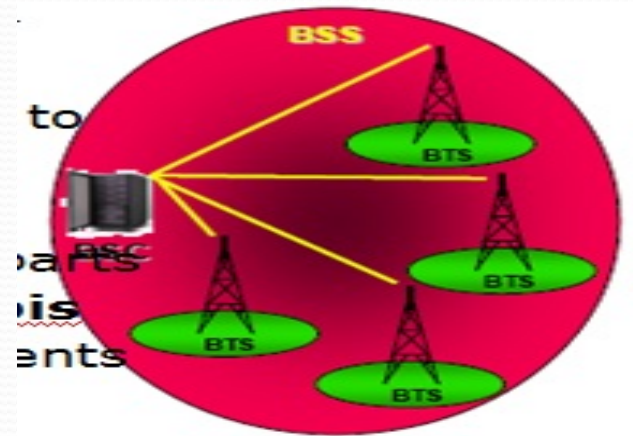
GSM System Architecture

- Radio Subsystem (RSS)
 - Mobile Station (MS)
 - Mobile Equipment (ME)
 - Subscriber Identity Module (SIM)
 - Base Station Subsystem (BSS)
 - Base Transceiver Station (BTS)
 - Base Station Controller (BSC)
- Network Switching Subsystem(NSS)
 - Mobile Switching Center (MSC)
 - Home Location Register (HLR)
 - Visitor Location Register (VLR)
- Operation Subsystem (OSS)
 - Operation and Maintenance Center (OMC)
 - Authentication Center (AUC)
 - Equipment Identity Register (EIR)

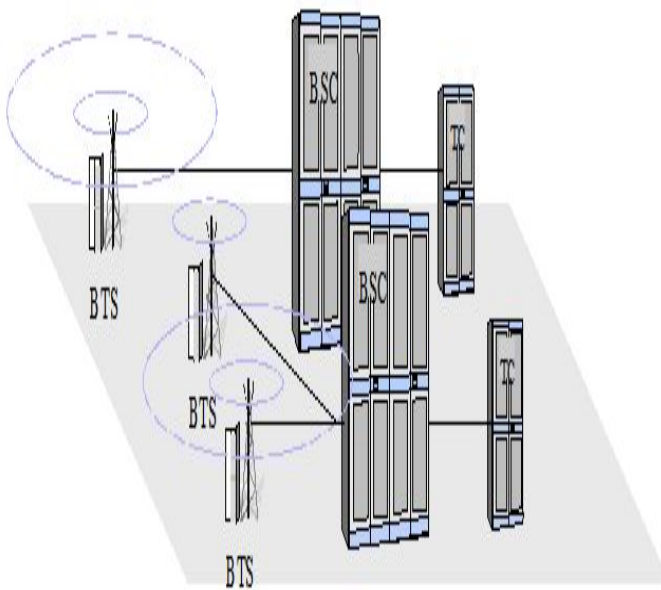
Base Station



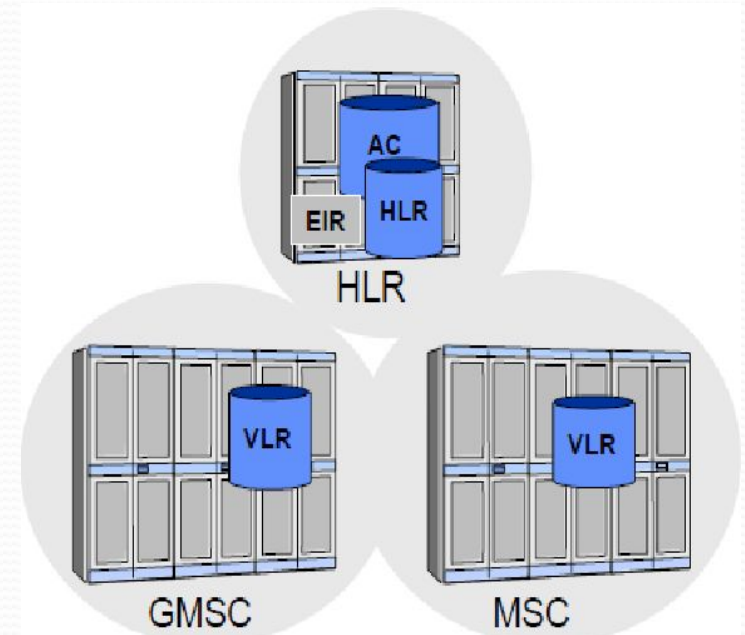
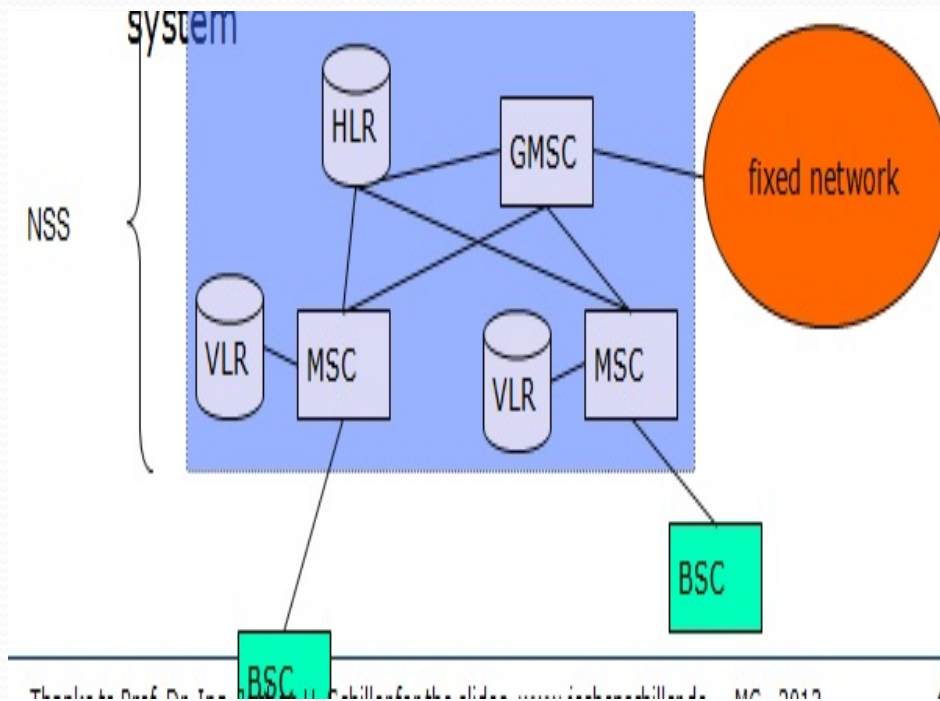
Base Transceiver Station



Base Station Controller



Network Switching Subsystem



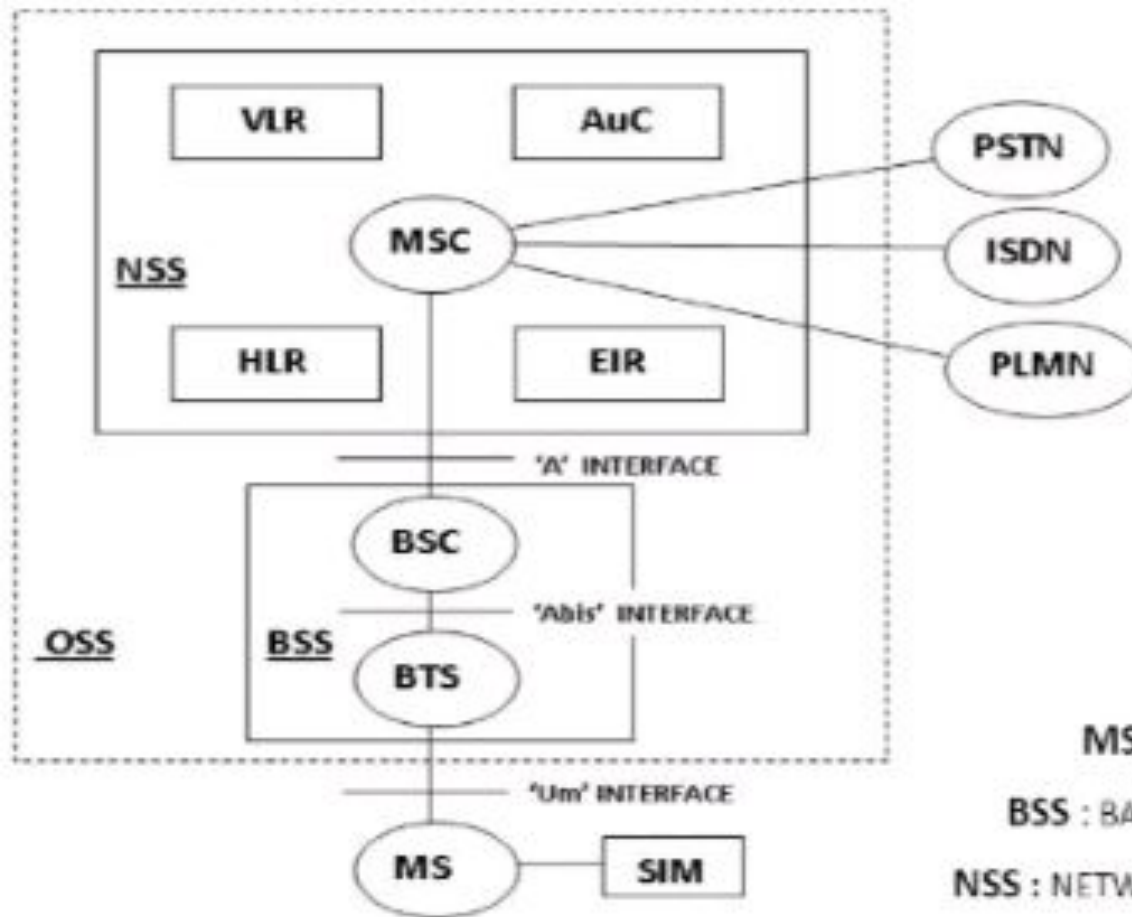
Mobile Switching Center



Home Location Register (HLR)



Operation Subsystem



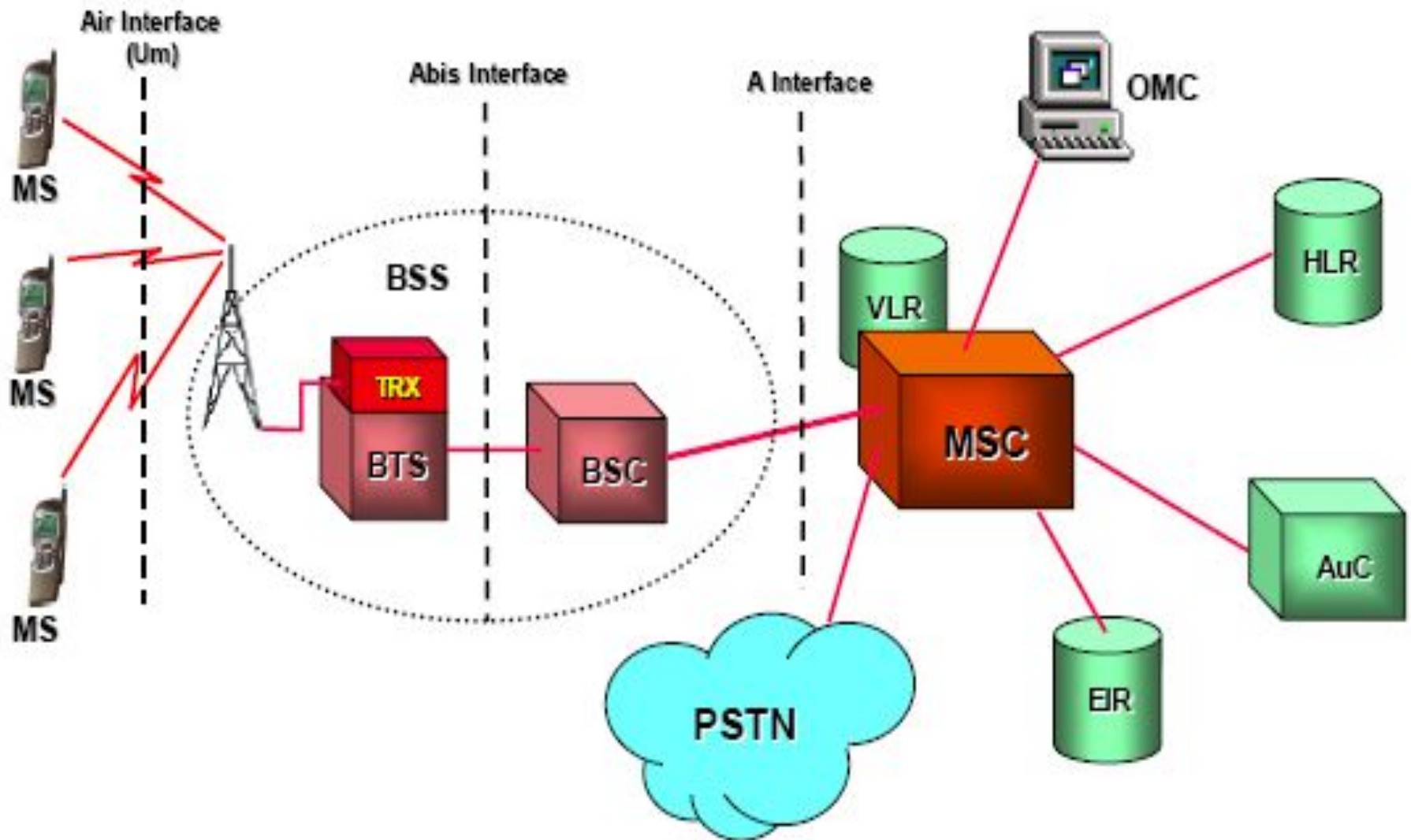
MS : MOBILE STATION

BSS : BASE STATION SUBSYSTEM

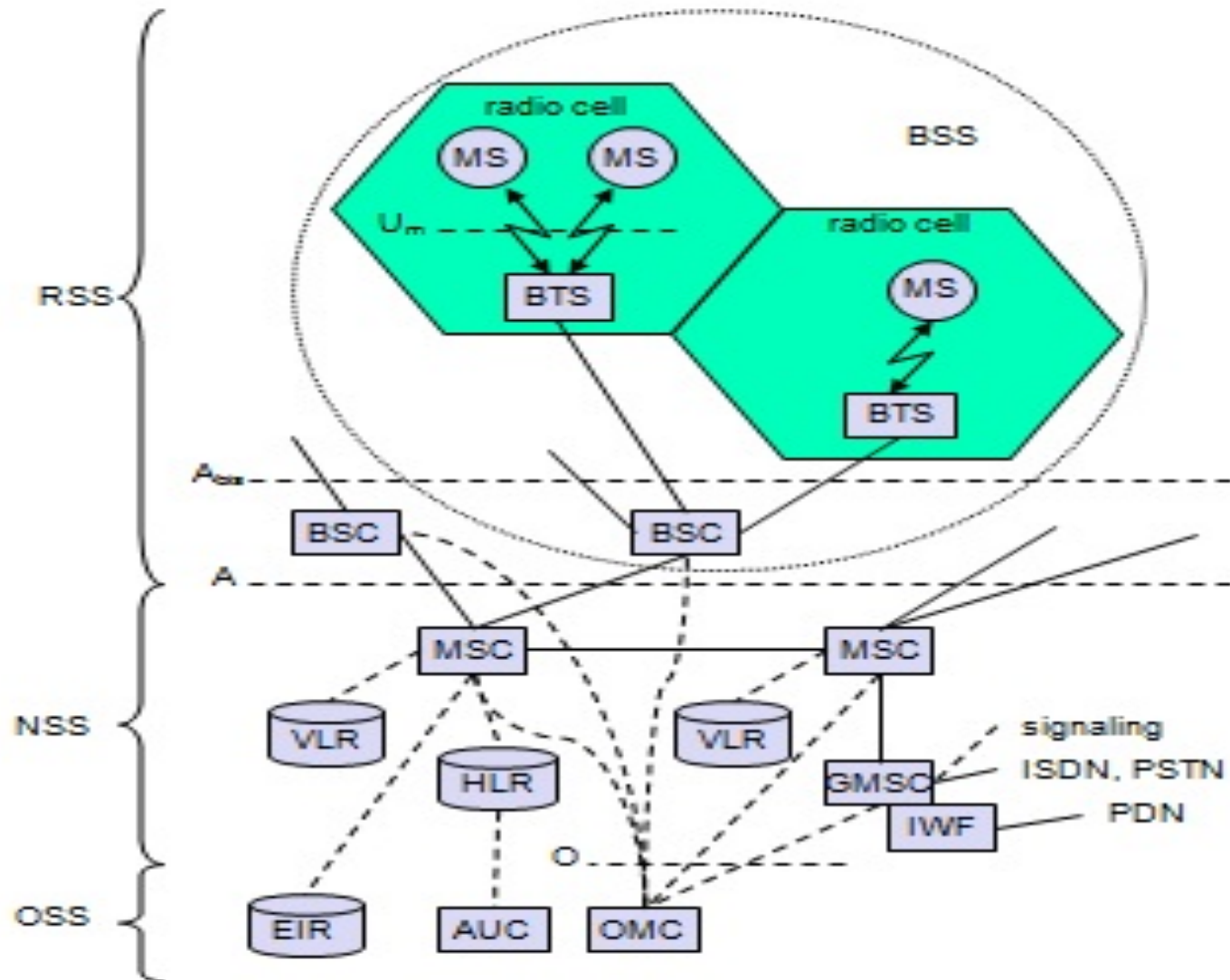
NSS : NETWORK SWITCHING SUBSYSTEM

OSS : OPERATION SUPPORT SUBSYSTEM

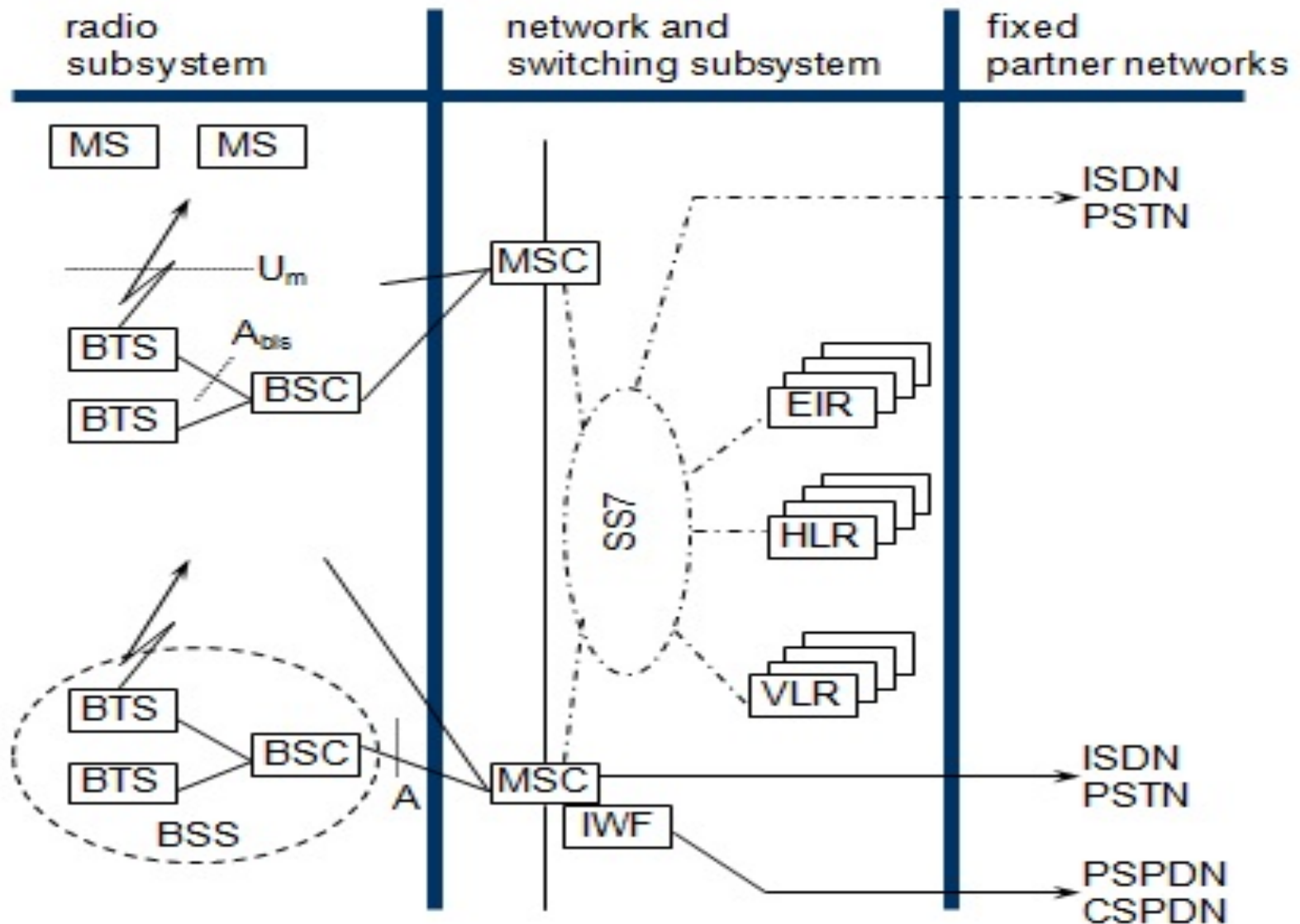
GSM Architecture



GSM: elements and interfaces



GSM: system Architecture



Radio Subsystem

- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
 - Mobile Stations (MS)
 - 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
 - $BSS = BSC + \text{sum}(BTS) + \text{interconnection}$

RSS: The Mobile Station (MS)

- The mobile station consists of:
 - Mobile Equipment (ME)
 - Subscriber Identity Module (SIM)
- The SIM stores all specific data that is relevant to GSM - permanent and temporary data about the mobile, the subscriber and the network, including:
 - The International Mobile Subscriber Identity (IMSI)
 - MS ISDN number of subscriber (phone number)
 - Authentication key and algorithms for authentication check
 - Charging information, list of subscribed services
 - Personal identity number (PIN), and PIN unblocking key (PUK)
 - Temporary location information while logged onto GSM system
 - Temporary mobile subscriber identity (TMSI)
 - Location area identification (LAI)

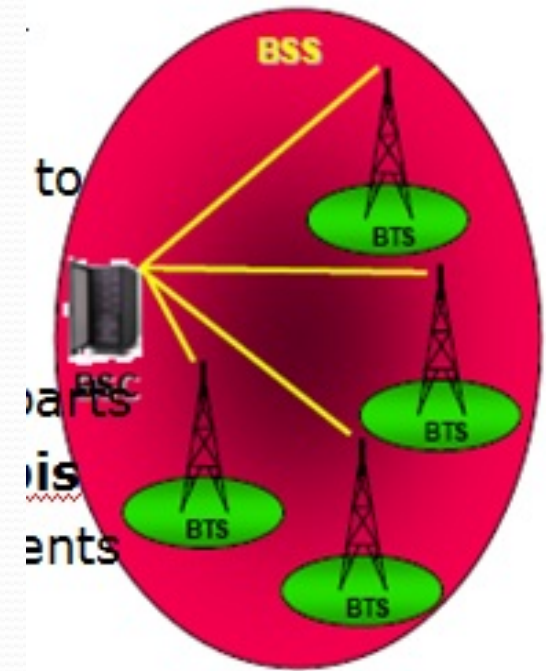


RSS: The Mobile Station (MS)

- The mobile equipment has a unique International Mobile Equipment Identity (**IMEI**) which is used for theft protection
- Without the SIM, only emergency calls are possible
- For GSM 900, MS transmits power of up to 2W, for GSM 1800 1W due to smaller cell-size
- MS can also have other components and services for the user (display, loudspeaker, Bluetooth interface,). These are non GSM features.

RSS: The Base Station Sub-System (BSS)

- A GSM network comprises many BSSs.
- The BSS performs all the functions necessary to maintain radio connection to an MS (coding/decoding of voice, rate adaptation,...)
- Base Station Subsystem is composed of two parts that communicate across the standardized **Abis** interface allowing operation between components made by different suppliers:
 - Base Station Controller (BSC)
 - One or more Base Transceiver Stations (BTSs)
- BTS contains:
 - Radio Transmitter/Receiver (TRX)
 - Signal processing and control equipment
 - Antennas and feeder cables



RSS: The Base Station Sub-System (BSS)

- The purpose of the BTS is to:
 - Provide radio access to the mobile stations
 - Manage the radio access aspects of the system
 - Encode, encrypt, multiplex, modulate and feed the RF signals to the antenna.
 - Frequency hopping
 - Communicates with Mobile station and BSC
- The BSC:
 - Allocates a channel for the duration of a call
 - Maintains the call:
 - Monitoring quality
 - Controlling the power transmitted by the BTS or MS
 - Generating a handover to another cell when required
- BTSs can be linked to parent BSC by microwave, optical fiber or cable

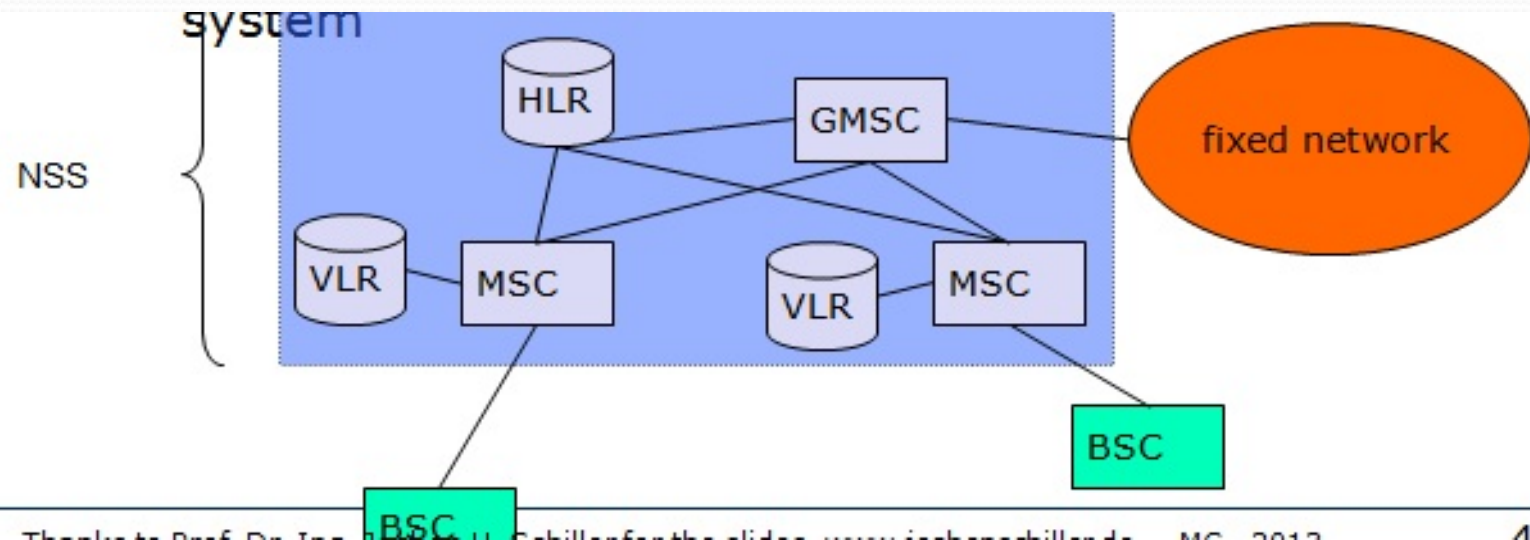
Network and switching subsystem (NSS)

- NSS is the main component and the heart of the GSM system
 - Connects the wireless network with standard public networks (manages communication between GSM and other networks)
 - Performs handover between different BSSs
 - Supports roaming of users between different providers in different countries
 - Performs functions for worldwide localization of users
 - Charging and billing information, accounting information

In summary switching, mobility management, interconnection to other networks, system control are the main functions of NSS

NSS- components

- Components
 - Mobile Services Switching Center (MSC)
 - Gateway Mobile Switching Center
 - Databases (important: scalability, high capacity, low delay)
 - Home Location Register (HLR)
 - Visitor Location Register (VLR)
- All components connect using the SS7 signaling system protocols (set up & tear down telephone calls)



NSS - Mobile Services Switching Center

- MSCs are high-performance digital ISDN switches
- They set-up and control connections to other MSCs and to BSCs via the A-interface
- They form the backbone network of a GSM system
- Typically, an MSC manages several BSCs in a geographical region
- Controls all connections via a separated network to/from a mobile terminal within the domain of the MSC

NSS - Mobile Switching Centre (MSC)

- Functions of the MSC:
 - Switching calls, controlling calls and logging calls
 - specific functions for paging and call forwarding
 - mobility specific signaling
 - Mobility management over the radio network and other networks.
 - Radio Resource management – handovers between BSCs
 - Billing Information
 - 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
 - Interface with PSTN, ISDN, PSPDN (Packet Switched Public Data Network) - interworking functions via Gateway MSC (GMSC)

NSS-MSC Gateway Mobile Switching Centre (GMSC)

- A particular MSC can be assigned to act as a GMSC (Gateway Mobile Switching Centre)
- A GMSC is a device which routes traffic entering a mobile network to the correct destination
- The GMSC accesses the network's HLR to find the location of the required mobile subscriber
- The operator may decide to assign more than one GMSC

NSS- Home Location Register (HLR)

- Most important database in GSM system, stores all user-relevant information permanent and semi-permanent
 - Static information such as mobile subscriber ISDN number, subscribed services (e.g call forwarding, roaming restrictions), and the International mobile subscriber identity (IMSI))
 - Dynamic information such as the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC.

As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network

- All these user-specific information elements only exist once for each user in a single HLR which also supports charging and accounting.

HLR Implementation

- There is logically one HLR in a Network, although it may consist of several separate computers
- May be split regionally
- HLRs can manage data for several million customers
- Contain highly specialised databases to fulfill real-time requirements and answer requests within certain time bounds.
- Stand alone computer – no switching capabilities
- May be located anywhere on the SS7 (signaling system) network
- Combine with AuC

NSS – Visitor Location Register (VLR)

- Each MSC has a VLR
- VLR is a dynamic local database which stores all important information needed for MS users currently in the LA (location area) associated to the MSC (the domain of the VLR)
- If a new MS comes into the LA of the VLR, it copies all relevant information for this user from the HLR, and stores this data temporarily.
- Information stored includes:
 - International Mobile Subscriber Identity (IMSI)
 - Mobile Station ISDN Number (MSISDN)
 - Mobile Station Roaming Number (MSRN)
 - Temporary Mobile Station Identity (TMSI)
 - Local Mobile Station Identity
 - The location area where the mobile station has been
 - Supplementary service parameters



Operation Subsystem (OSS)

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems. It accesses other components via SS7 signaling. It consists of the following three components:
 - Operation and Maintenance Center (OMC)
 - Authentication Center (AuC)
 - Equipment Identity Register (EIR)
- Operation and Maintenance Center (OMC)
 - different control capabilities for the radio subsystem and the network subsystem via the O-interface (SS7)
 - Traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing

OSS – Authentication Center (AuC)

- Authentication Center (AuC)
 - **User Identity** and Data Transmission (wireless part)
 - **Authentication parameters** used for authentication of mobile terminals and **encryption of user data** on the air interface within the GSM system
 - Generates user specific authentication parameters on request of a VLR
 - Situated in a special protected part of the HLR



OSS – Equipment Identity Register (EIR)

- EIR is a database for all IMEI (International Mobile Equipment Identity). It stores all device identifications registered for this network
- The EIR controls access to the network by returning the status of a mobile in response to an IMEI query
- Possible status levels are:
 - White-listed - The terminal is allowed to connect to the network
 - Grey-listed - The terminal is under observation by the network for possible problems
 - Black-listed - The terminal has either been reported stolen, or is not a type approved for a GSM network. The terminal is not allowed to connect to the network.