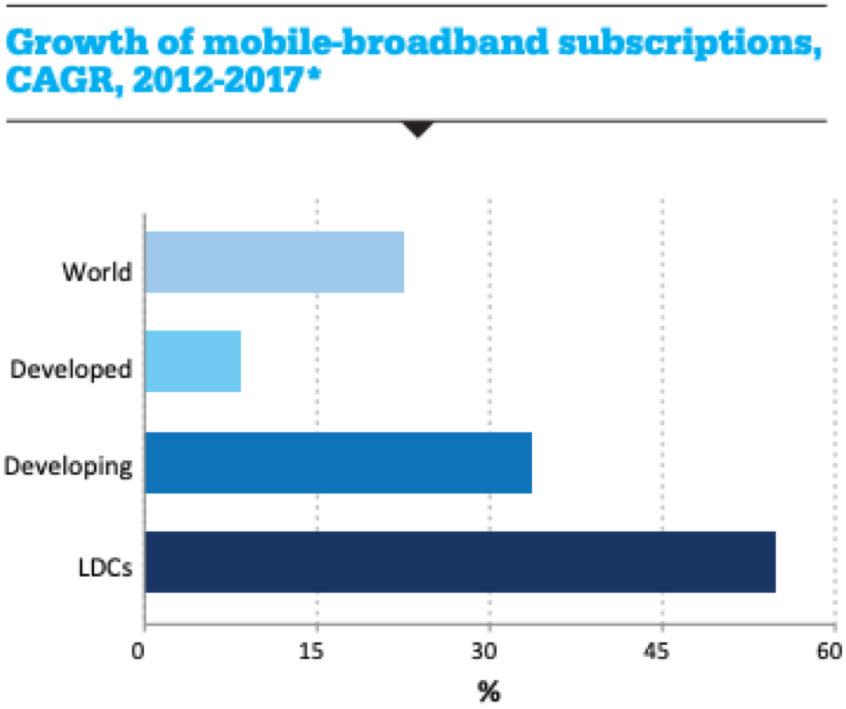
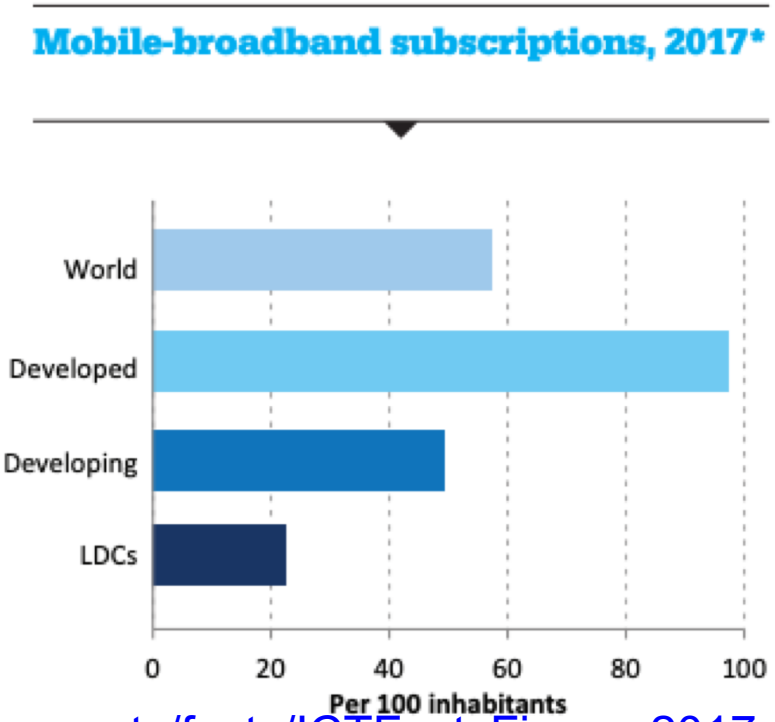
INTRODUCTION TO WIRELESS AND MOBILE NETWORKS

Cellular Networks - GSM

Overview

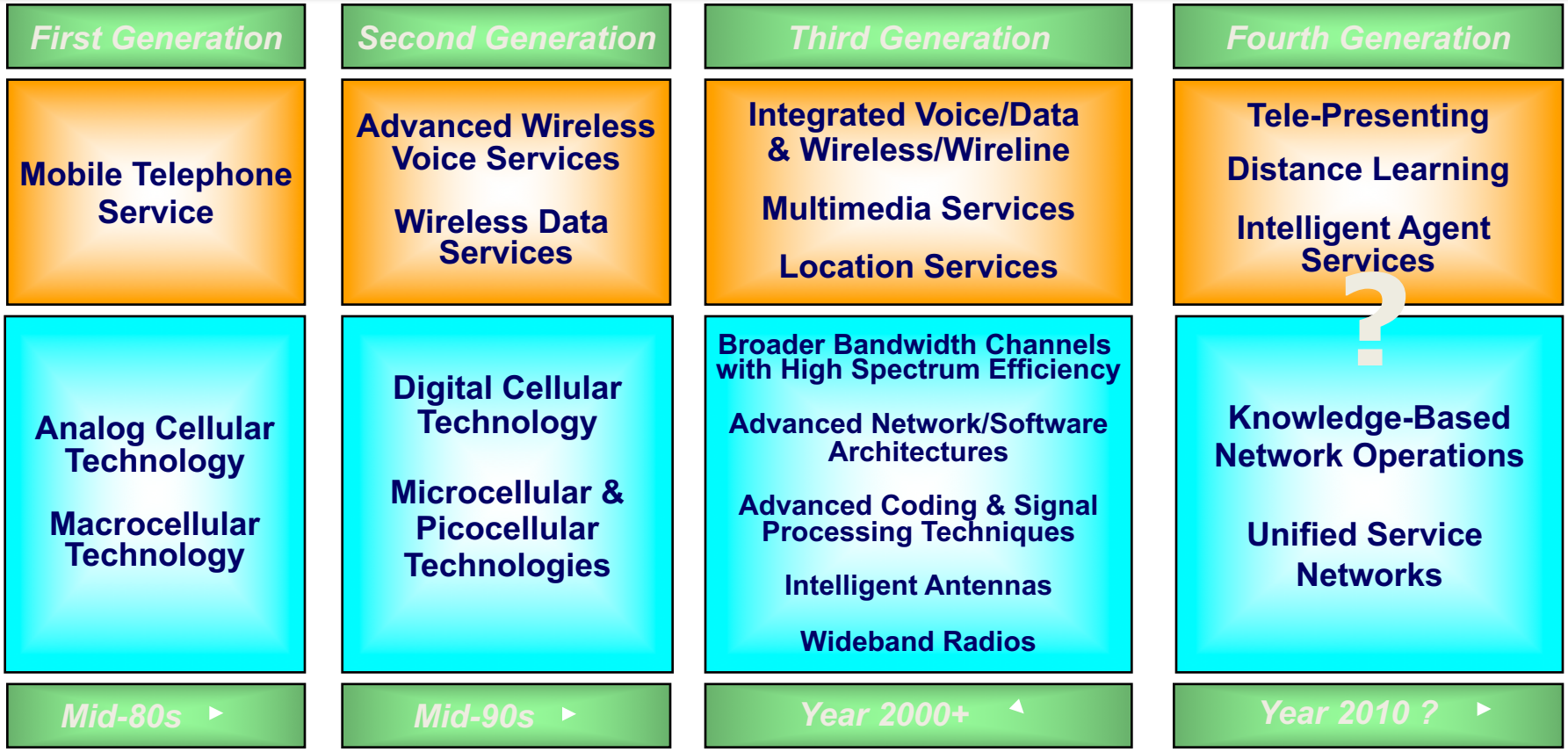
- 6 Billion mobile phone users (end of 2011) *
- The world population is 7 Billion!





https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf

Global Wireless Services and Network Evolution



AMPS
USDC
ETACS

GSM
IS-54/ 136 TDMA
IS-95/ cdmaOne
PDC
DECT

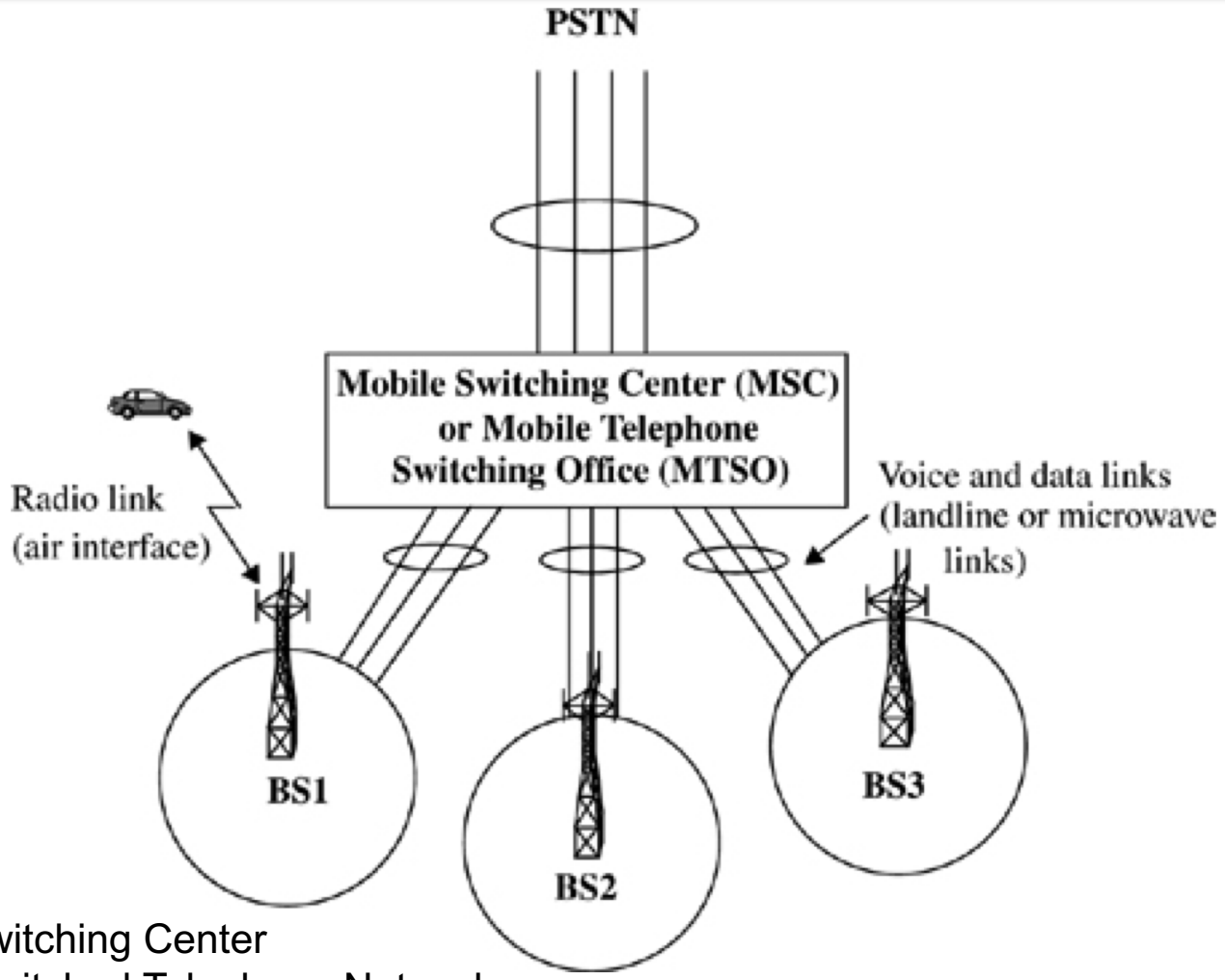
W-CDMA
UWC-136
cdma2000

Source: IEEE Communications Magazine

Major 3G Standards Organizations

Standard Organization	Region
International Telecommunications Union (ITU)	International
European Telecommunications Standard Institute (ETSI)	Europe
Telecommunications Industry Association (TIA)	North America
Association of Radio Industries and Business (ARIB)	Japan
American National Standard Institute (committee TIPI)	North America

Block diagram of a cellular system



MSC: Mobile Switching Center
PSTN: Public Switched Telephone Network

Communication signaling in 1G systems

Reverse=uplink
Forward=downlink

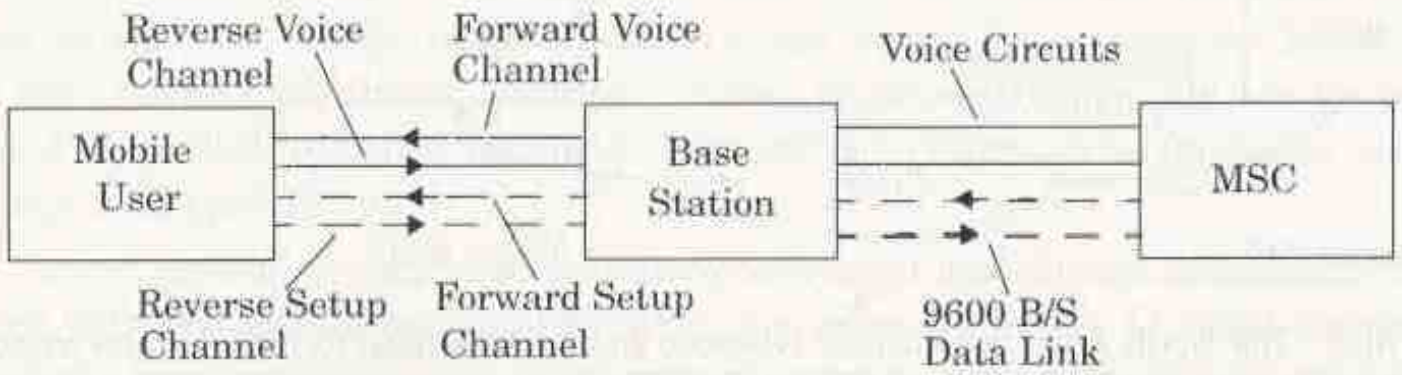


Figure 10.4 Communication signaling between mobile, base station, and MSC in first generation wireless networks.

All first generation cellular systems use FM modulation. A typical example of 1G is AMPS. The system control resides in MSC. MSC maintains all mobile related information and controls each mobile handoff. MSC performs all of the network management functions.

Block diagram of a 1G cellular radio network

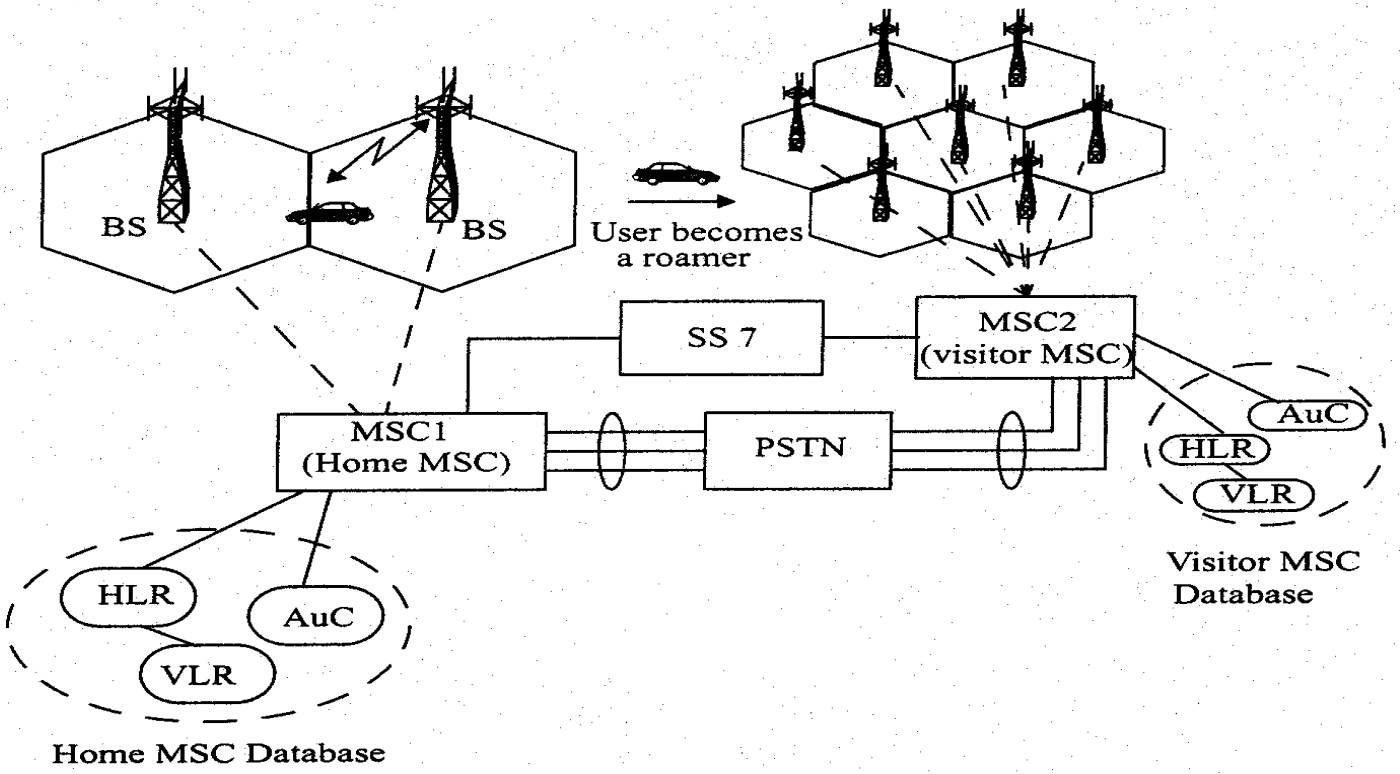


Figure 9.5
Block diagram of a cellular radio network.

SS7 and Network Architecture of 1G

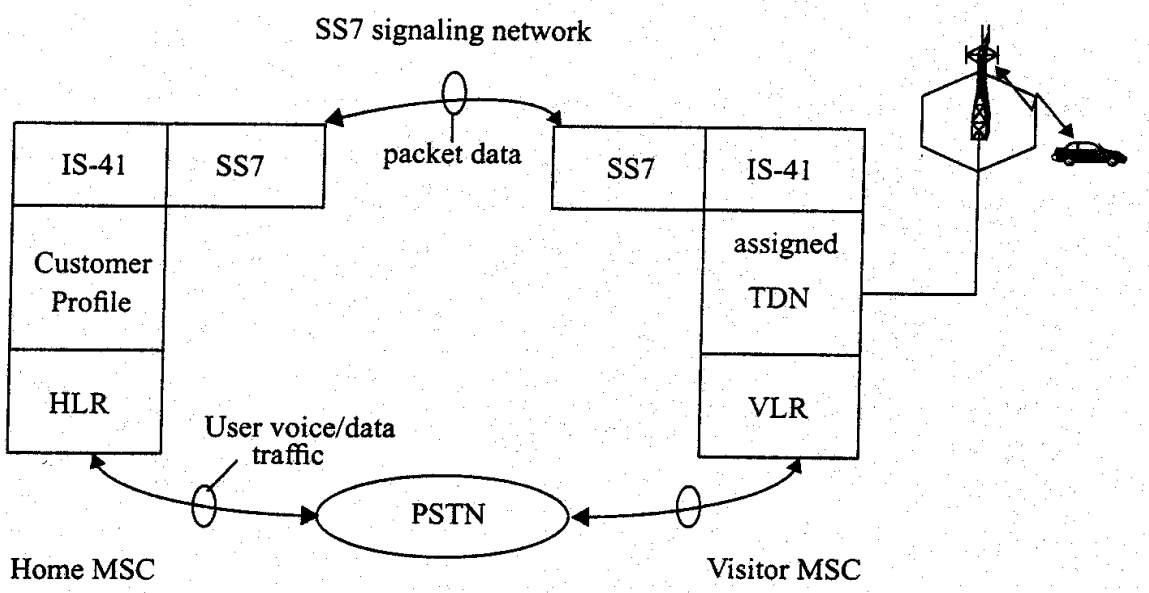


Figure 9.6
The North American Cellular Network architecture used to provide user traffic and signaling traffic between MSCs [From [NAC94] © IEEE]. The components of the SS7 network and their applications are described later in this chapter.

Long distance voice traffic is carried on the PSTN.
SS7: Signaling System No. 7 that is used to interconnect most of the cellular MSCs in the US
TDN: Temporary directory number
IS-41 is a network protocol standard

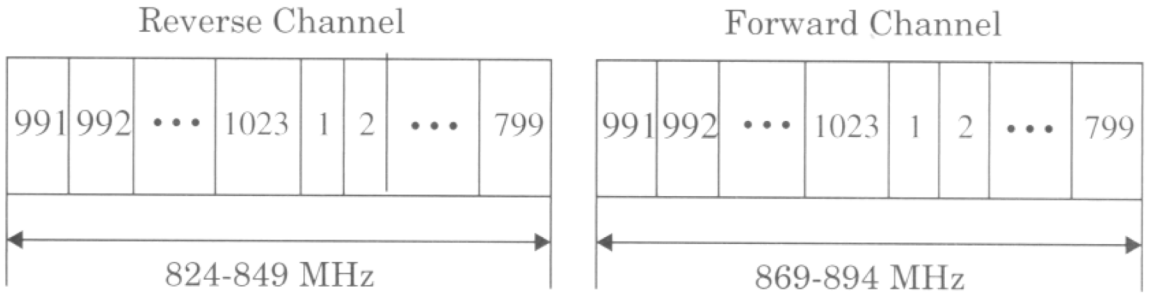
Signaling System No. 7 (SS7)

- A high-speed and high-performance packet-based communications protocol
- SS7 implements out-of-band signaling protocols, carried in a separate signaling channel,
  - Signalling and voice lines are seperated
- The term signaling refers to the exchange of control information associated with the establishment of a telephone call on a telecommunications circuit.
  - Ex. Dialed number
- SS7 can communicate significant amounts of information when setting up a call, during the call, and at the end of the call.
  - call forwarding (busy and no answer), voice mail, call waiting, conference calling, calling name and number display, call screening,
- http://www.ss7-training.net/

First Generation (1G) Wireless Networks

- **AMPS**
- first deployed in 1983 with a total of 40 MHz of spectrum in the 800 MHz band
- in 1989, an additional 10 MHz was added
- mobile to base station = 824 MHz ---- 849 MHz
- base station to mobiles = 869 MHz ---- 894 MHz
- uses 7-cell reuse pattern; N=7
- channel bandwidth= 30KHz
- SIR (signal to interference ratio) =18 dB
- voice modulation: FM

AMPS



	Channel Number	Center Frequency (MHz)
Reverse Channel	$1 \le N \le 799$	$0.030N + 825.0$
	$991 \le N \le 1023$	$0.030(N - 1023) + 825.0$
Forward Channel	$1 \le N \le 799$	$0.030N + 870.0$
	$991 \le N \le 1023$	$0.030(N - 1023) + 870.0$

(Channels 800–990 are unused)

Figure 1.2 Frequency spectrum allocation for the U.S. cellular radio service. Identically labeled channels in the two bands form a forward and reverse channel pair used for duplex communication between the base station and mobile. Note that the forward and reverse channels in each pair are separated by 45 MHz.

First Generation (1G) Wireless Networks

- ETACS (The European Total Access Communication System)
  - developed in the mid 1980s
  - virtually identical to AMPS, except it is scaled to fit 25 KHz channel bandwidth (as opposed to 30 KHz)

First Generation (1G) Wireless Networks

Table 10.1 AMPS and ETACS Radio Interface Specifications

Parameter	AMPS Specification	ETACS Specification
Multiple Access	FDMA	FDMA
Duplexing	FDD	FDD
Channel Bandwidth	30 kHz	25 kHz
Traffic Channel per RF Channel	1	1
Reverse Channel Frequency	824 - 849 MHz	890 - 915 MHz
Forward Channel Frequency	869 - 894 MHz	935 - 960 MHz
Voice Modulation	FM	FM
Peak Deviation: Voice Channels Control/Wideband Data	±12 kHz ±8 kHz	±10 kHz ±6.4 kHz
Channel Coding for Data Transmission	BCH(40,28) on FC BCH(48,36) on RC	BCH(40,28) on FC BCH(48,36) on RC
Data Rate on Control/Wideband Channel	10 kbps	8 kbps
Spectral Efficiency	0.33 bps/Hz	0.33 bps/Hz
Number of Channels	832	1000

ETACS: European Total Access Communication System, which was developed in the mid 1980s.

First Generation (1G) Wireless Networks

- N-AMPS (Narrowband AMPS)
  - Motorola developed an AMPS-like system called N-AMPS
  - provides 3 users in a 30 KHz AMPS channel using FDMA and 10 KHz channels
  - provides three times the capacity of AMPS at the expense of reducing the S/(N+I) (i.e., SNIR) which degrades the audio quality with respect to AMPS

First Generation (1G) Wireless Networks

- USDC (United States Digital Cellular)
  - was standardized as Interim Standard 54 (IS-54) by EIA/TIA
  - was developed in the late 1980s to support more users in a fixed spectrum allocation
  - uses 45 MHz FDD scheme as AMPS
  - employs TDMA
  - offers as much as six times the capacity of AMPS

Table 1.2 Major Mobile Radio Standards in Europe

Standard	Type	Year of Introduction	Multiple Access	Frequency Band	Modula-tion	Channel Bandwidth
ETACS	Cellular	1985	FDMA	900 MHz	FM	25 kHz
NMT-450	Cellular	1981	FDMA	450-470 MHz	FM	25 kHz
NMT-900	Cellular	1986	FDMA	890-960 MHz	FM	12.5 kHz
GSM	Cellular /PCS	1990	TDMA	890-960 MHz	GMSK	200 kHz
C-450	Cellular	1985	FDMA	450-465 MHz	FM	20 kHz/ 10 kHz
ERMES	Paging	1993	FDMA	Several	4-FSK	25 kHz
CT2	Cordless	1989	FDMA	864-868 MHz	GFSK	100 kHz
DECT	Cordless	1993	TDMA	1880-1900 MHz	GFSK	1.728 MHz
DCS-1800	Cordless /PCS	1993	TDMA	1710-1880 MHz	GMSK	200 kHz

- Second Generation Wireless Networks
  - GSM
  - IS-95 (cdmaOne)

GSM

- formerly: Groupe Spéciale Mobile (founded 1982), but Pan-European standard (ETSI, European Telecommunications Standardisation Institute) published phase 1 of the GSM specification in 1990
- now, called Global System for Mobile Communication

GSM

- simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations (Germany: D1 and D2)
  and seamless roaming within Europe possible
- today many providers all over the world use GSM (more than 130 countries in Asia, Africa, Europe, Australia, America)
- more than 5 billion subscribers

Performance characteristics 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 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!!
- no end-to-end encryption of user data
- no full ISDN bandwidth of 64 kbit/s to the user
- reduced concentration while driving
- electromagnetic radiation
- abuse of private data possible
- roaming profiles accessible
- high complexity of the system

GSM System Architecture

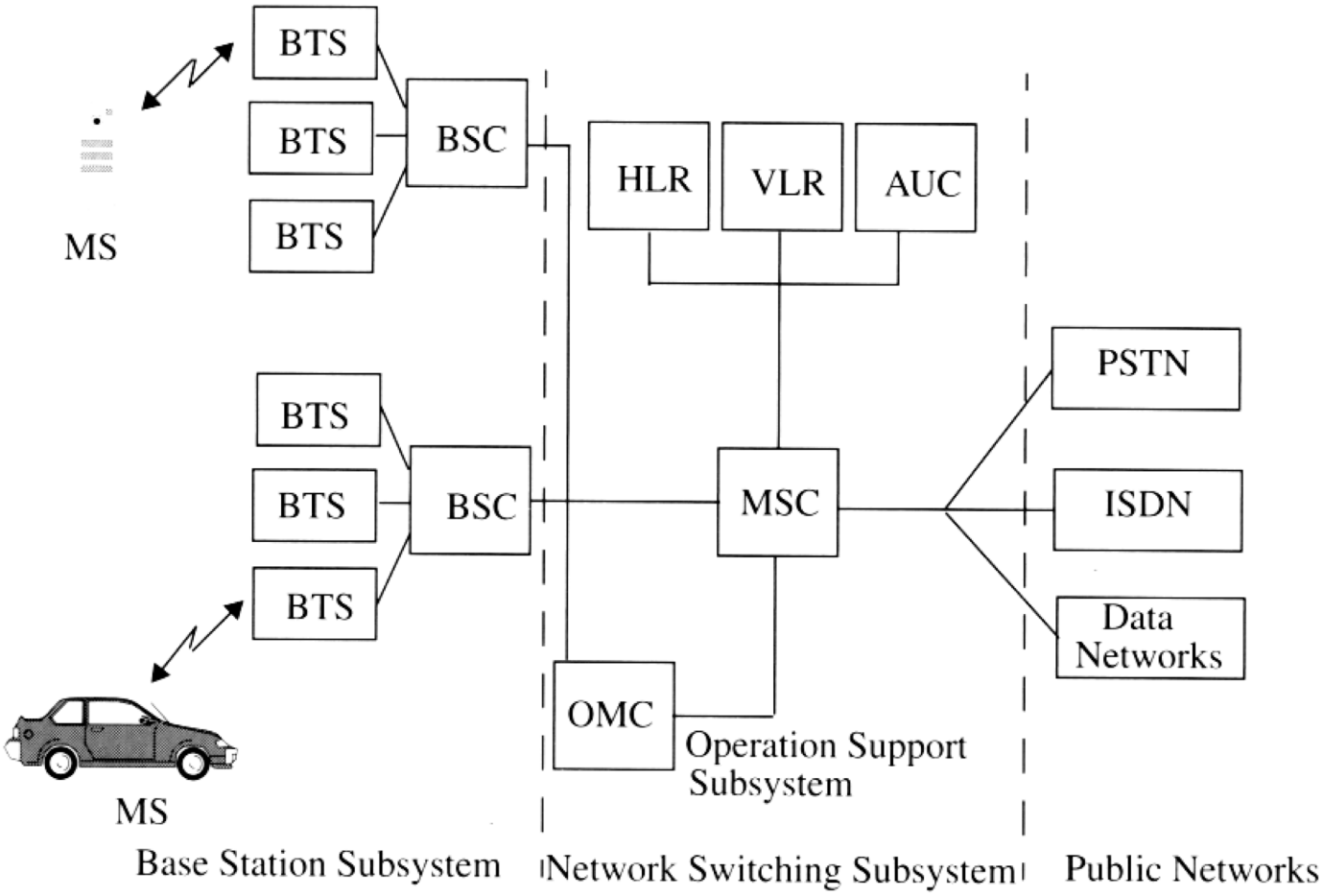


Figure 11.5 GSM system architecture.

GSM System Architecture

Table 10.3 GSM Air Interface Specifications Summary

Parameter	Specifications
Reverse Channel Frequency	890 - 915 MHz
Forward Channel Frequency	935 - 960 MHz
ARFCN Number	0 to 124 and 975 to 1023
Tx/Rx Frequency Spacing Tx/Rx Time Slot Spacing	45 MHz 3 Time slots
Modulation Data Rate	270.833333 kbps
Frame Period	4.615 ms
Users per Frame (Full Rate)	8
Time slot Period	576.9 μs
Bit Period	3.692 μs
Modulation	0.3 GMSK
ARFCN Channel Spacing	200 kHz
Interleaving (max. delay)	40 ms
Voice Coder Bit Rate	13.4 kbps

GSM: Mobile Services

- GSM offers
  - several types of connections
    - voice connections, data connections, short message service
  - multi-service options (combination of basic services)

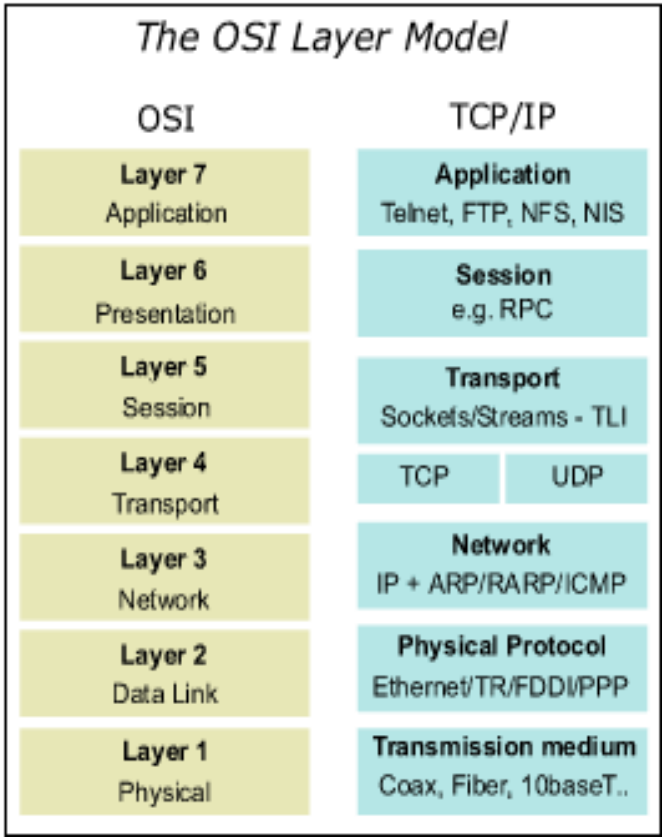
Definitions for GSM

•Telecommunication service: a service offered by a PLMN (public land mobile network) operator or service provider to its customers in order to satisfy a specific telecommunication requirement. It is divided into two broad families:

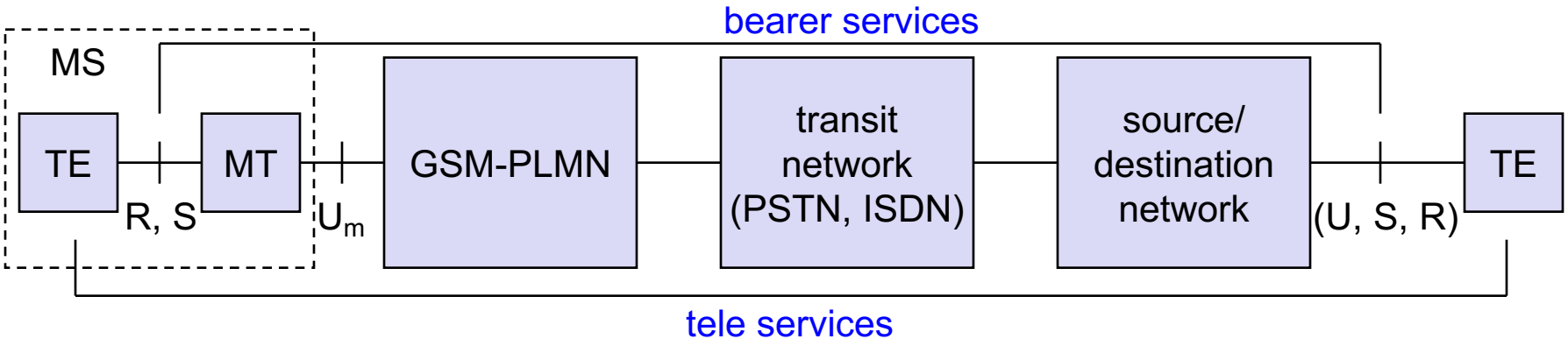
- bearer services (bearer service is a type of telecommunication service that provides the capability of transmission of signals between access points)
- tele services (teleservice is a type of telecommunication service that provides the complete capability for communication between users according to standardized protocols and transmission capabilities)

GSM: Mobile Services

- GSM defines three service domains
  - Bearer Services (need OSI layers 1-3)
  - Tele Services (may need OSI layers 1-7)
  - Supplementary Services



GSM: Mobile Services



GSM-PLMN is the infrastructure needed for the GSM network.

MS: mobile station
TE: terminal
MT: mobile termination

PLMN: Public land mobile network
PSTN: public switched telephone network
R,S,U: interfaces
S: interface for data transmission

Bearer Services

- Part of GSM Phase 2
- **Data services:** comprise all services that enable the transparent transmission of **data** between the interfaces to the network
- telecommunication services that transfer data between access points
- in GSM, bearer services are connection oriented and circuit- or packet-switched
  - data service (circuit switched)
    - 300 - 1200 bit/s
  - data service (packet switched)
    - 300 - 9600 bit/s

Tele Services

- GSM mainly focuses on voice-oriented tele services
- 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)

Tele Services II

- Additional services
  - Non-Voice-Teleservices
    - group 3 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 using the signaling channel, thus allowing simultaneous use of basic services and SMS

Supplementary services

- Services in addition to the basic services, cannot be offered stand-alone
- 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 up to 7 participants
  - locking of the mobile terminal (incoming or outgoing calls)

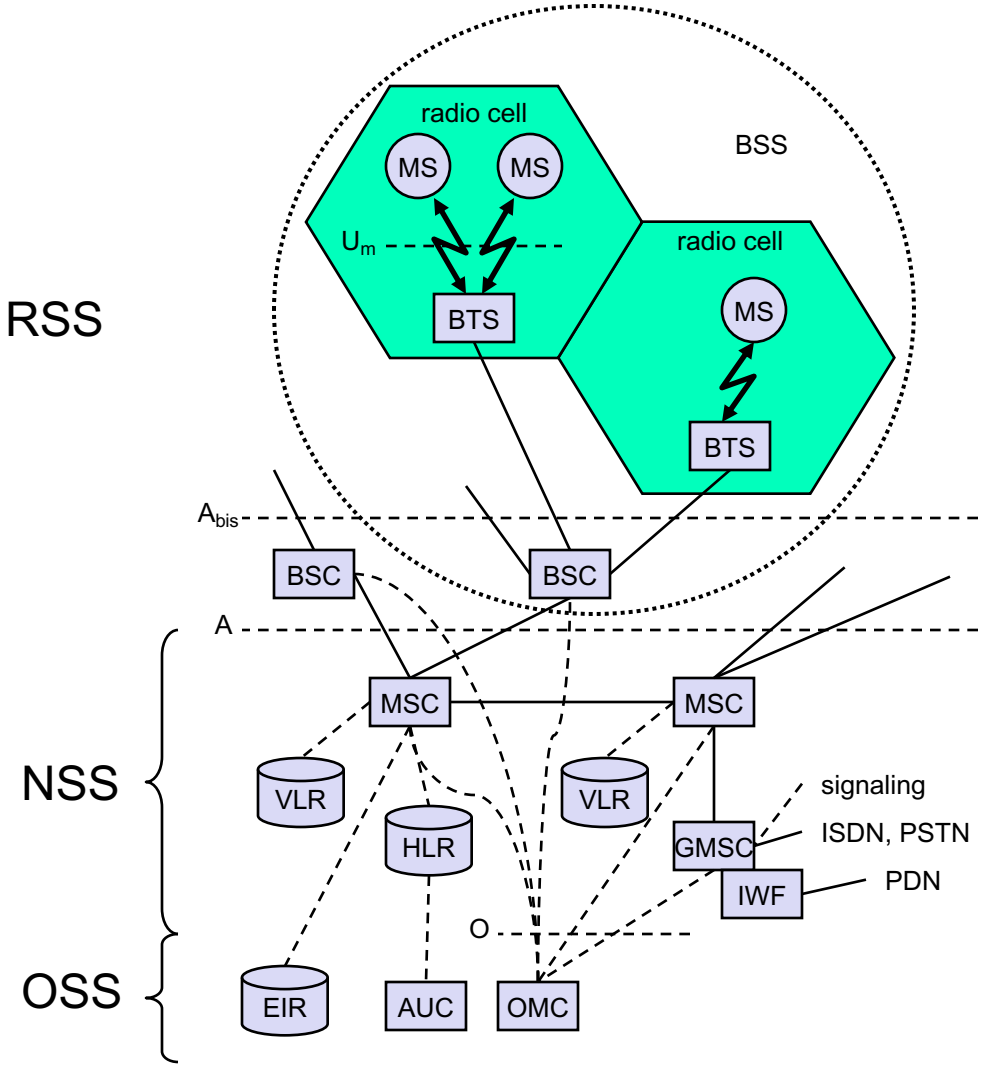
Architecture of the GSM system

- 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)

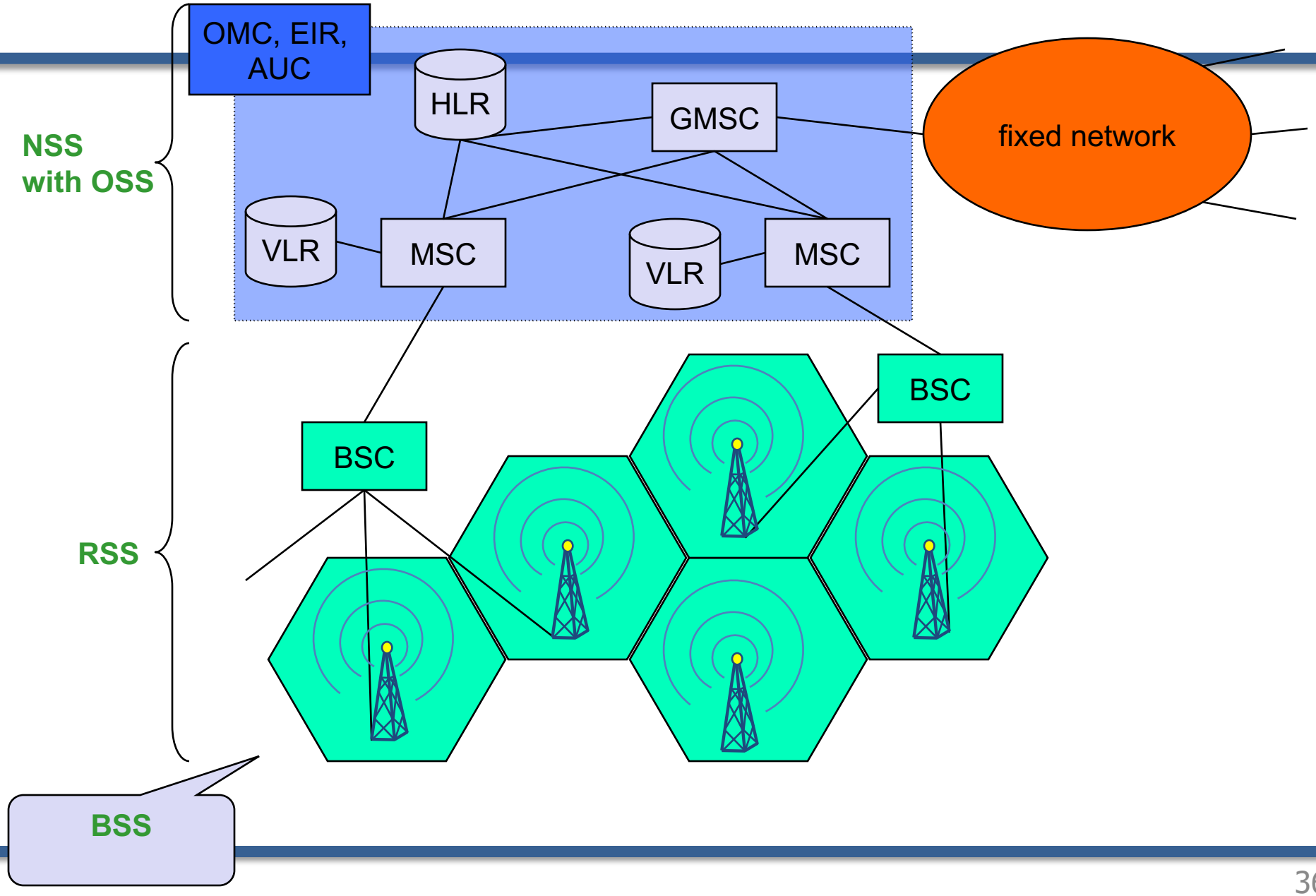
Architecture of the GSM system

- subsystems
  - RSS (radio subsystem): covers all radio aspects
    - RSS is also called BSS (Base Station Subsystem)
  - NSS (network and switching subsystem): call forwarding, handover, switching
  - OSS (operation subsystem): management of the network

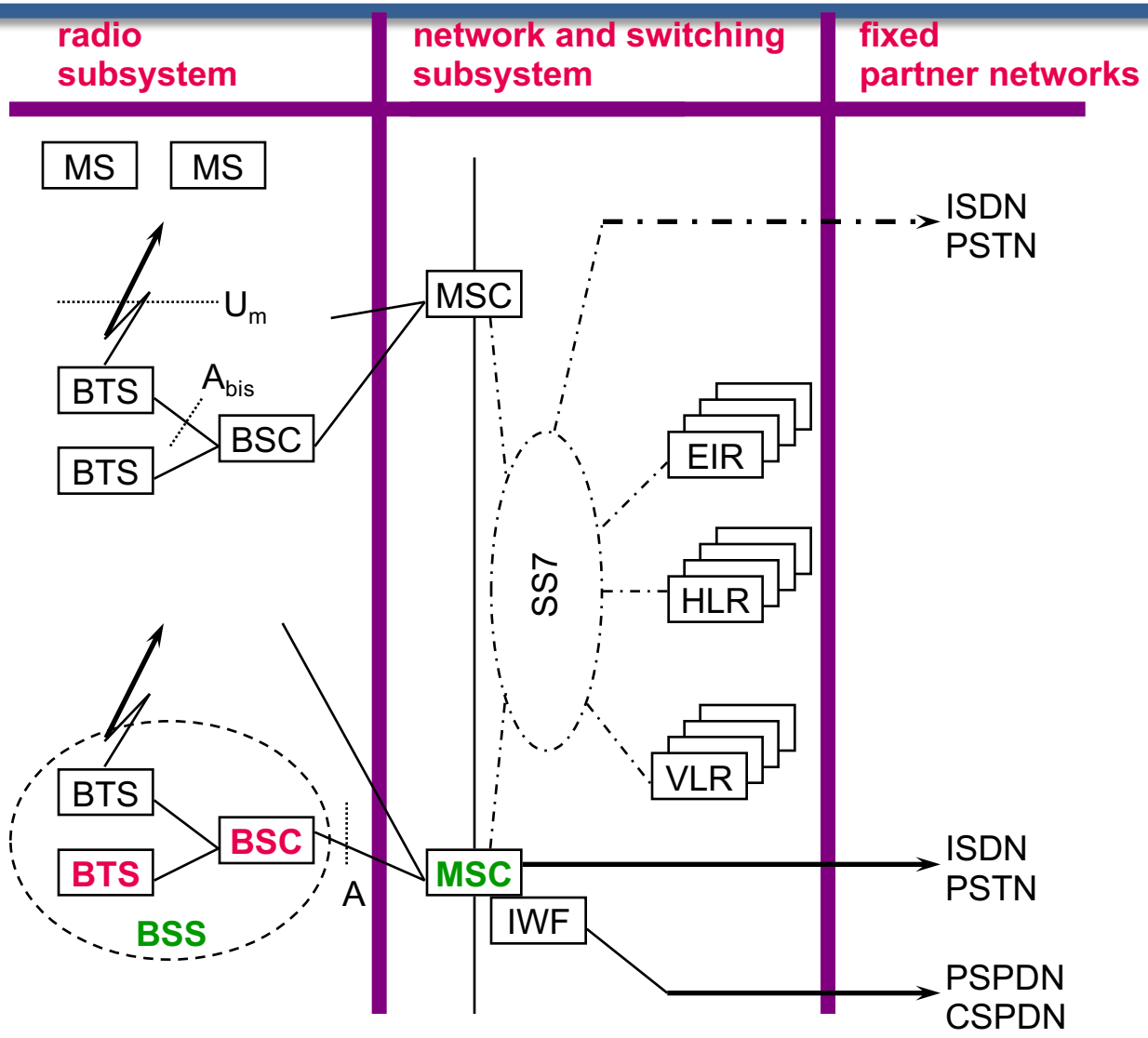
GSM: elements and interfaces



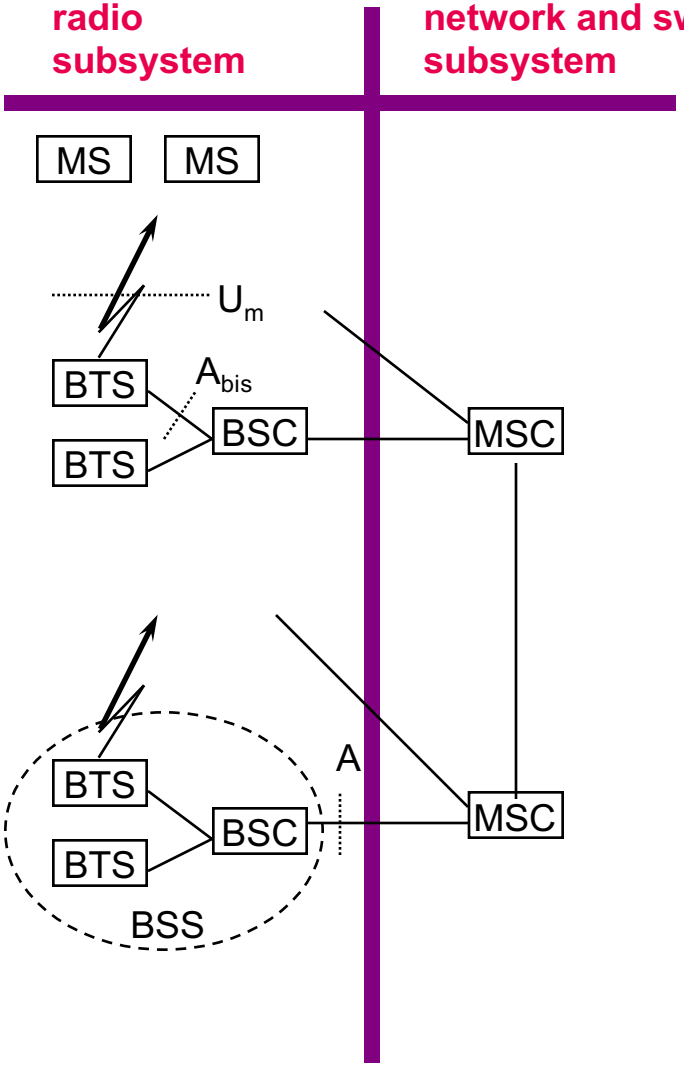
GSM: overview



GSM: system architecture

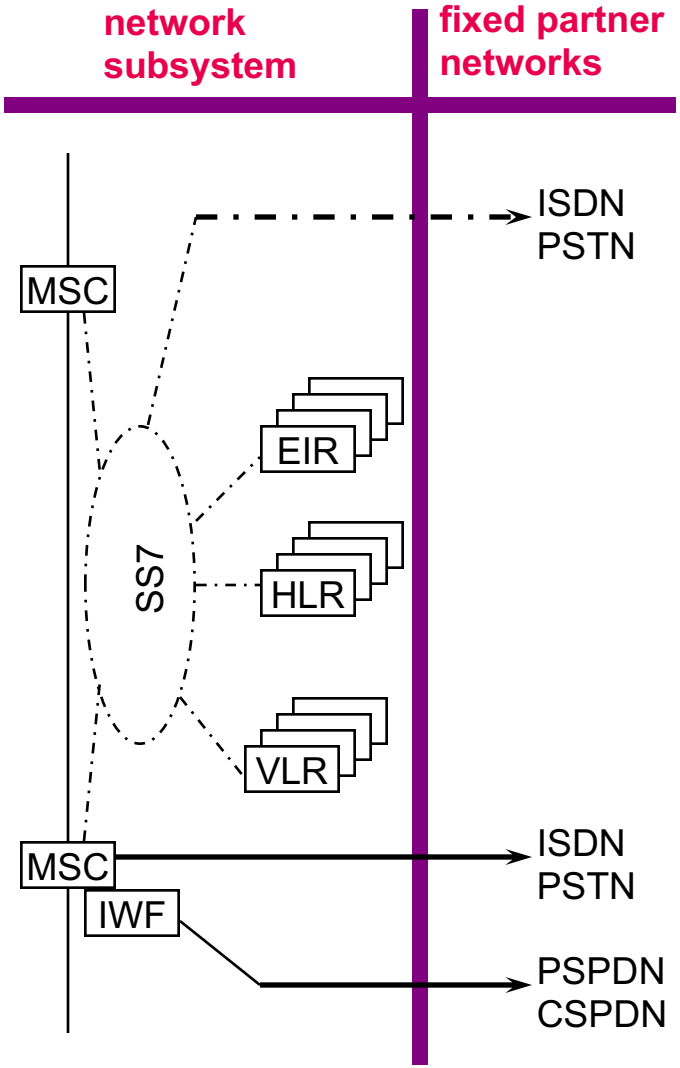


System architecture: radio subsystem



- Components
  - *MS* (Mobile Station)
  - *BSS* (Base Station Subsystem): consisting of
    - *BTS* (Base Transceiver Station): sender and receiver
    - *BSC* (Base Station Controller): controlling several transceivers
- Interfaces
  - U_m : radio interface
  - A_{bis} : standardized, open interface with 16 kbit/s user channels
  - *A*: standardized, open interface with 64 kbit/s user channels

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

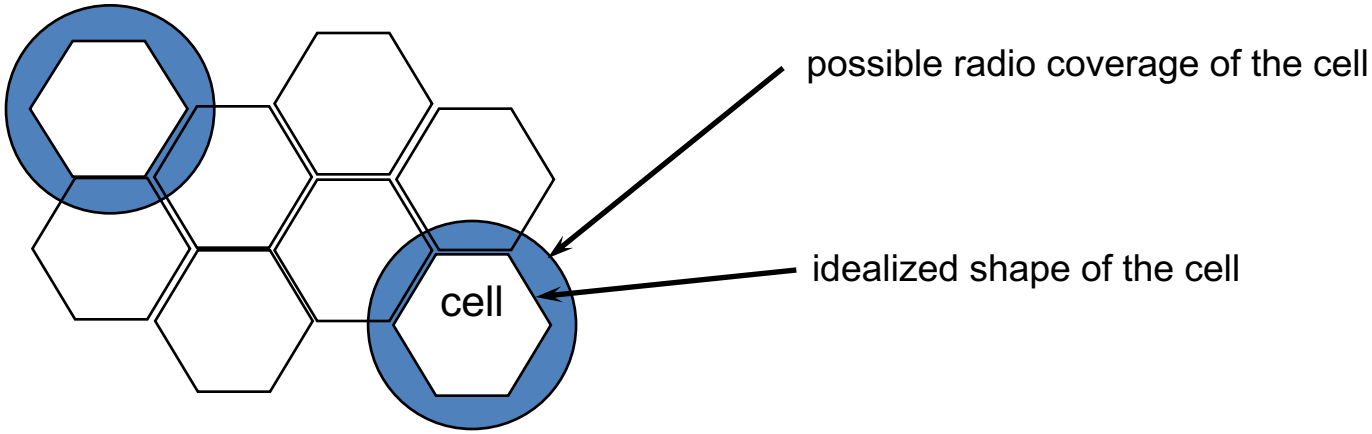
- *HLR* (Home Location *R*egister)
- *VLR* (Visitor Location *R*egister)
- *EIR* (Equipment Identity Register)

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 + sum(BTS) + interconnection
  - Mobile Stations (MS)

GSM: cellular network

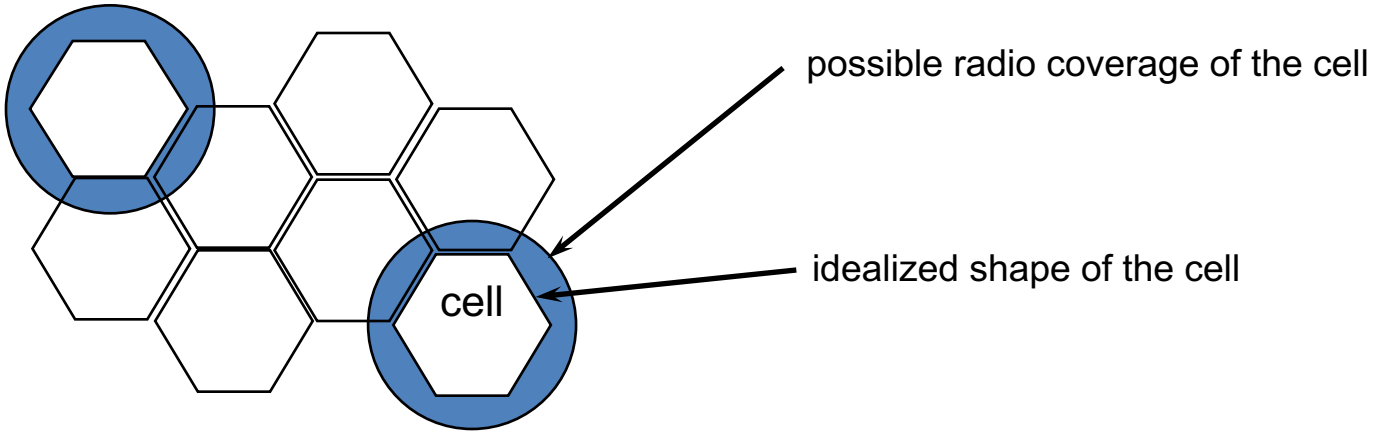
segmentation of the area into cells



- 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.

GSM: cellular network

segmentation of the area into cells



hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)

if a mobile user changes cells

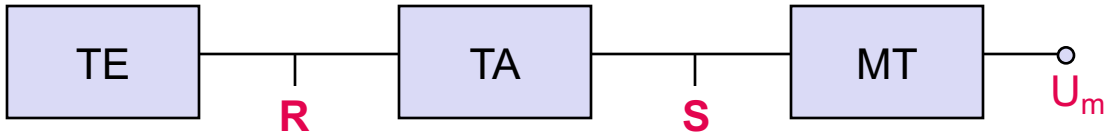
➪ handover of the connection to the neighbor cell

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

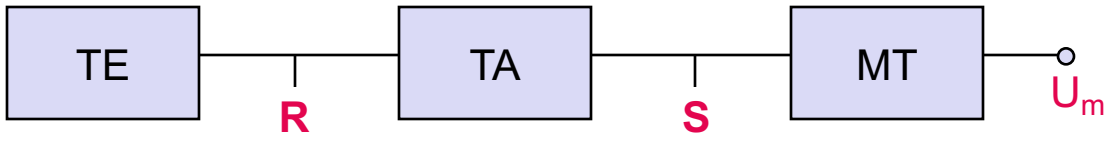
Mobile station (I)

- Terminal for the use of GSM services
- A mobile station (MS) comprises several functional groups
  - MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - corresponds to the network termination (NT) of an ISDN access
    - end-point of the radio interface (U_m)



Mobile station (II)

- Other functional groups in mobile station
  - TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics
  - TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - does not contain GSM specific functions
  - SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters



Network and switching subsystem (I)

- **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

Network and switching subsystem (II)

- 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

Network and switching subsystem (III)

- 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

Network and switching subsystem (IV)

- Other Components of NSS
  - 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, including data about all user currently in the domain of the VLR

Operation subsystem (I)

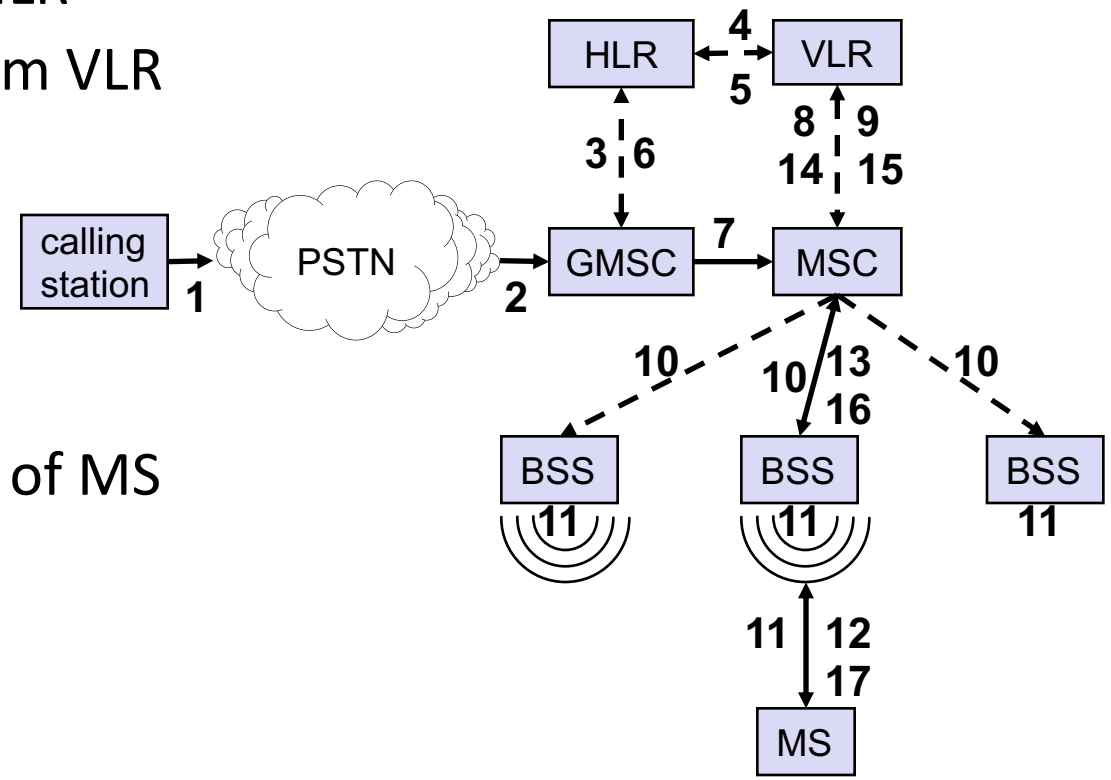
- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system

Operation subsystem (II)

- Other components of OSS
  - 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

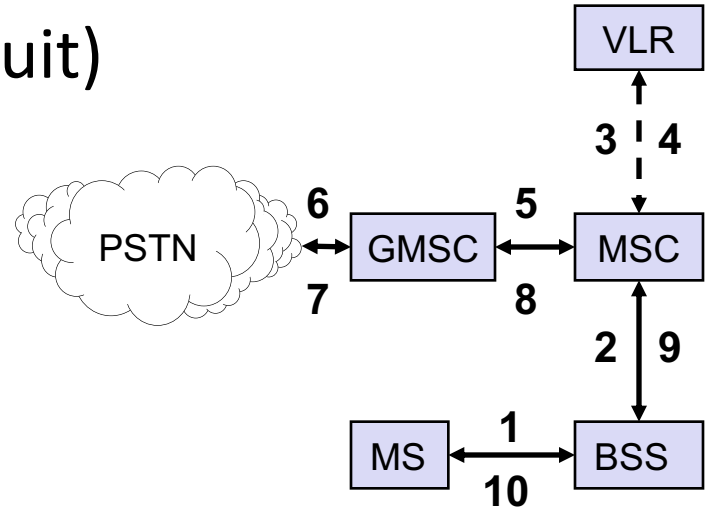
Mobile Terminated Call (MTC)

- 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 (MOC)

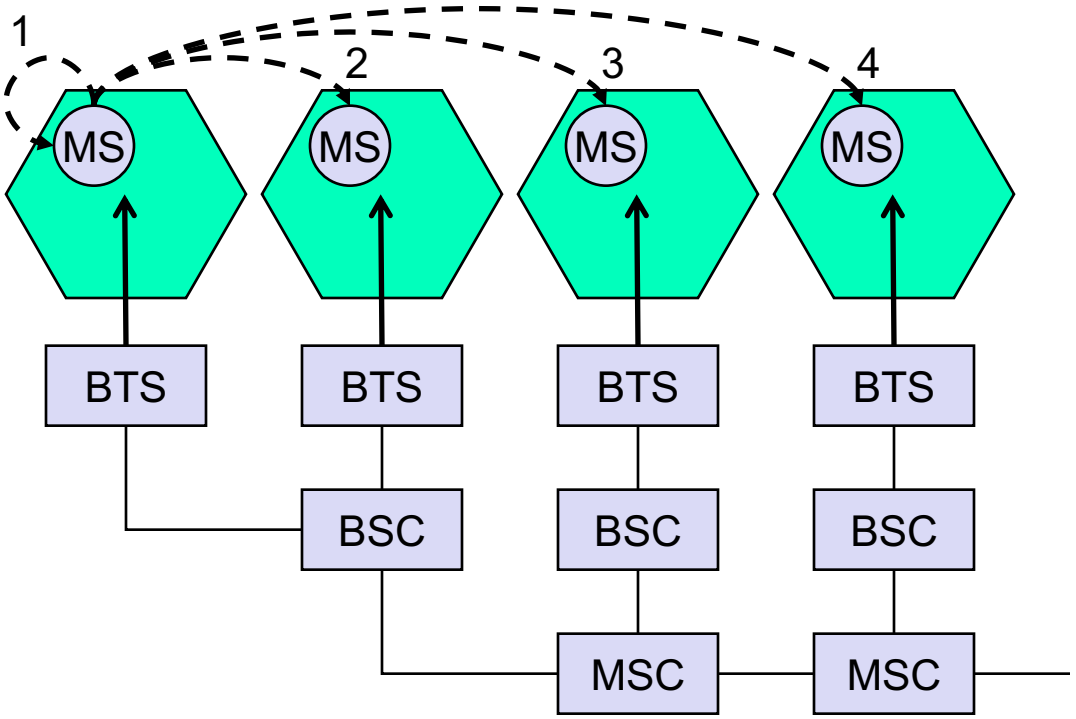
- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



Handover

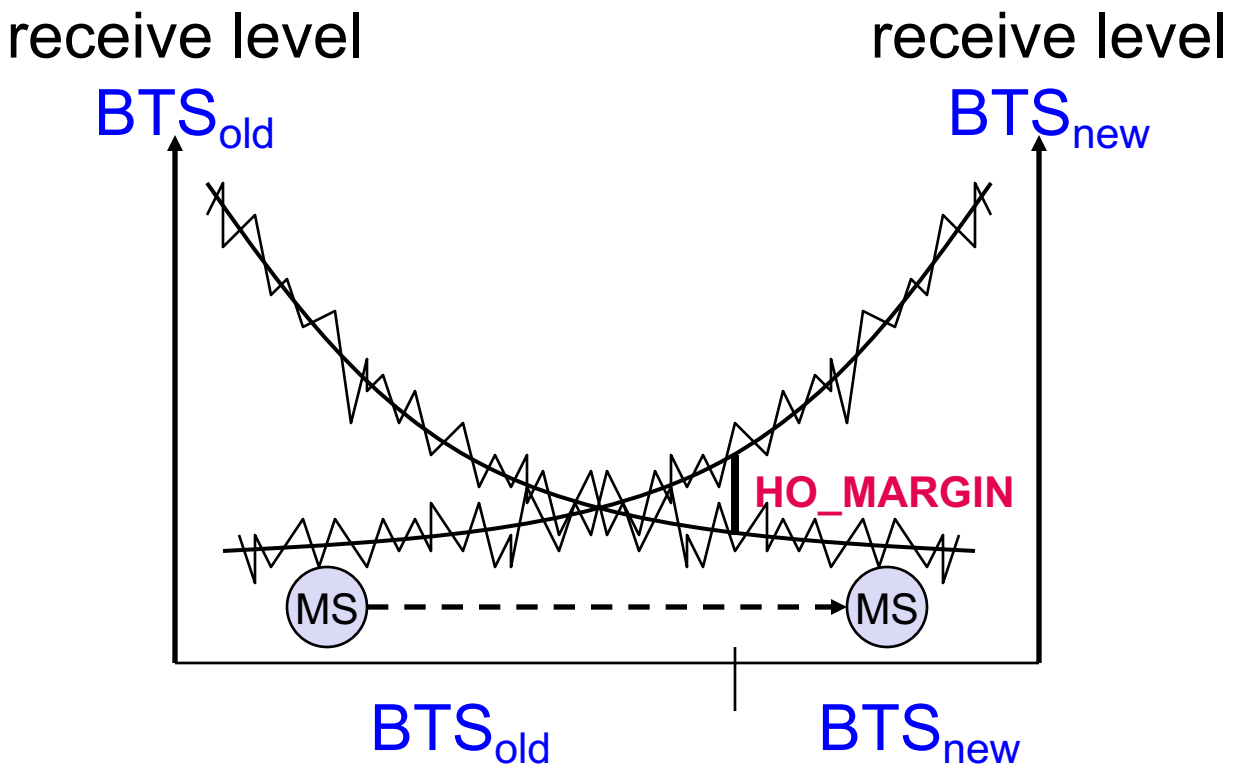
- GSM handover is hard-handover type.
  - First, the old connection is disconnected, then the new connection is established. Break-before-make
  - It is done if the base station is moving away or the cell capacity is full.
  - Handover decision is made by BSC in line with the information received from BTS and MS.
  - Performed by Handover BSC or MSC

Four handover types



1 Intra-cell
2 Inter-cell, intra-BSC
3 Inter-BSC, intra-MSC
4 Inter MSC

Handover decision



Handover procedure