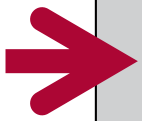
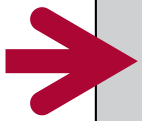
UNIVERSITÄT OSNABRÜCK

Cellular Phone Network

Mobile Communication, WS 2014/2015, Kap.4

Prof. Dr. Nils Aschenbruck





4.1. GSM – How does is work?

JS

- How can the system **locate a user**?
- Why **don't** all phones **ring at the same time**?
- What happens if **two users talk simultaneously**?
- Why don't I get the bill from my neighbor?
- Why can an **Australian use her phone in Berlin**?
- Why can't I simply overhear the neighbor's communication?
- How secure is the mobile phone system?
- What are the **key components** of the mobile phone network?

- GSM
  - formerly: **Groupe Spéciale Mobile** (founded 1982)
  - now: **Global System for Mobile Communication**
  - Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
  - simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations (Germany: D1 and D2)
    ➔ **seamless roaming within Europe** possible

- Today **many providers all over the world use GSM**
  (219 countries in Asia, Africa, Europe, Australia, America)
  - more than 4,2 billion subscribers in more than 700 networks
  - more than 75% of all digital mobile phones use GSM
  - over 29 billion SMS in Germany in 2008, (> 10% of the revenues for many operators) [be aware: these are only rough numbers…]
  - See e.g. www.gsmworld.com/newsroom/market-data/index.htm

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

In Germany **networks A, B, C**
- analogue systems
- restricted functionality (e.g. location, roaming, …)

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

In Germany **GSM networks D, E**
- digital systems
- so called “2nd generation”

Disadvantages of GSM

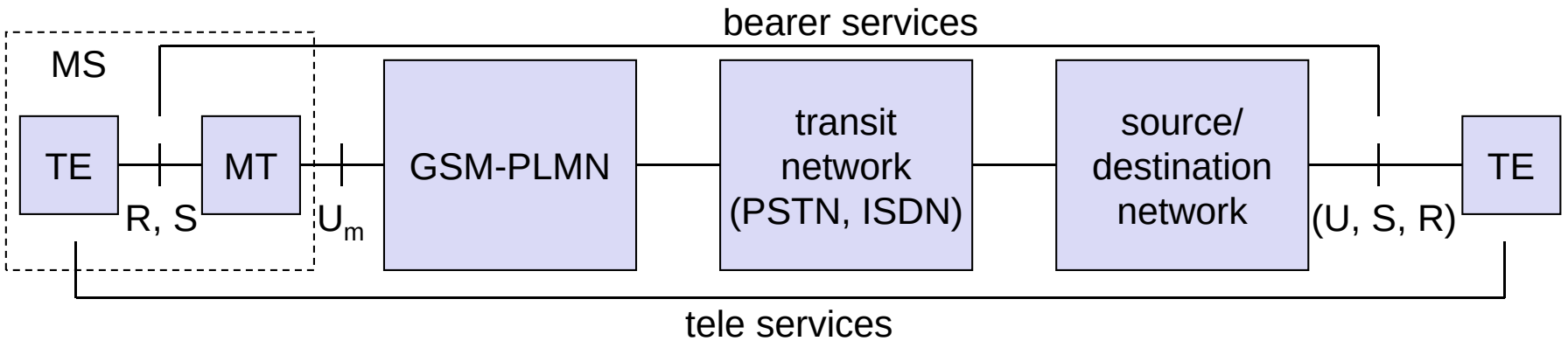
- There is no perfect system!!
  - no end-to-end encryption of user data
  - no full ISDN bandwidth of 64 kbit/s to the user, no transparent B-channel

- reduced concentration while driving
- electromagnetic radiation

- abuse of private data possible
- roaming profiles accessible

- high complexity of the system
- several incompatibilities within the GSM standards

- **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
  - Telematic Services
  - Supplementary Services



TE = Terminal Equipment
MT = Mobile Termination

- **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

(OSS not discussed in our lecture)

Ingredients 1: Mobile Phones, PDAs & Co.

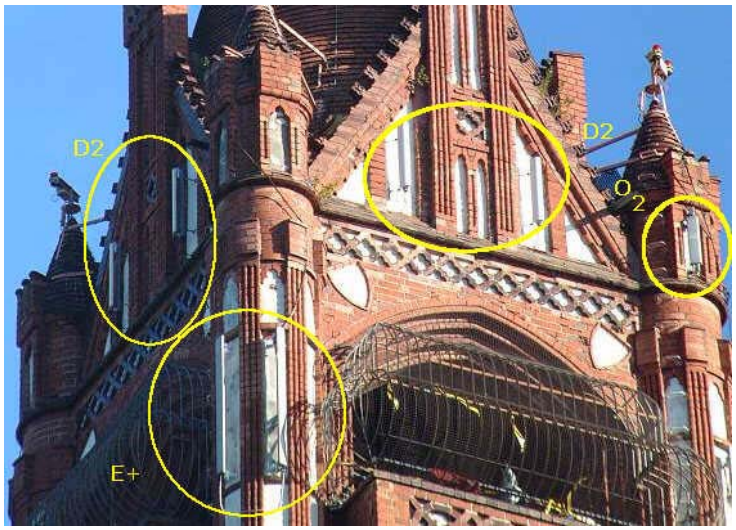
JS

Pictures from avm.de and t-mobile.de

The visible but smallest part of the network!

Ingredients 2: Antennas

JS



Still visible – cause many discussions…

Base Stations

Cabling

Microwave links

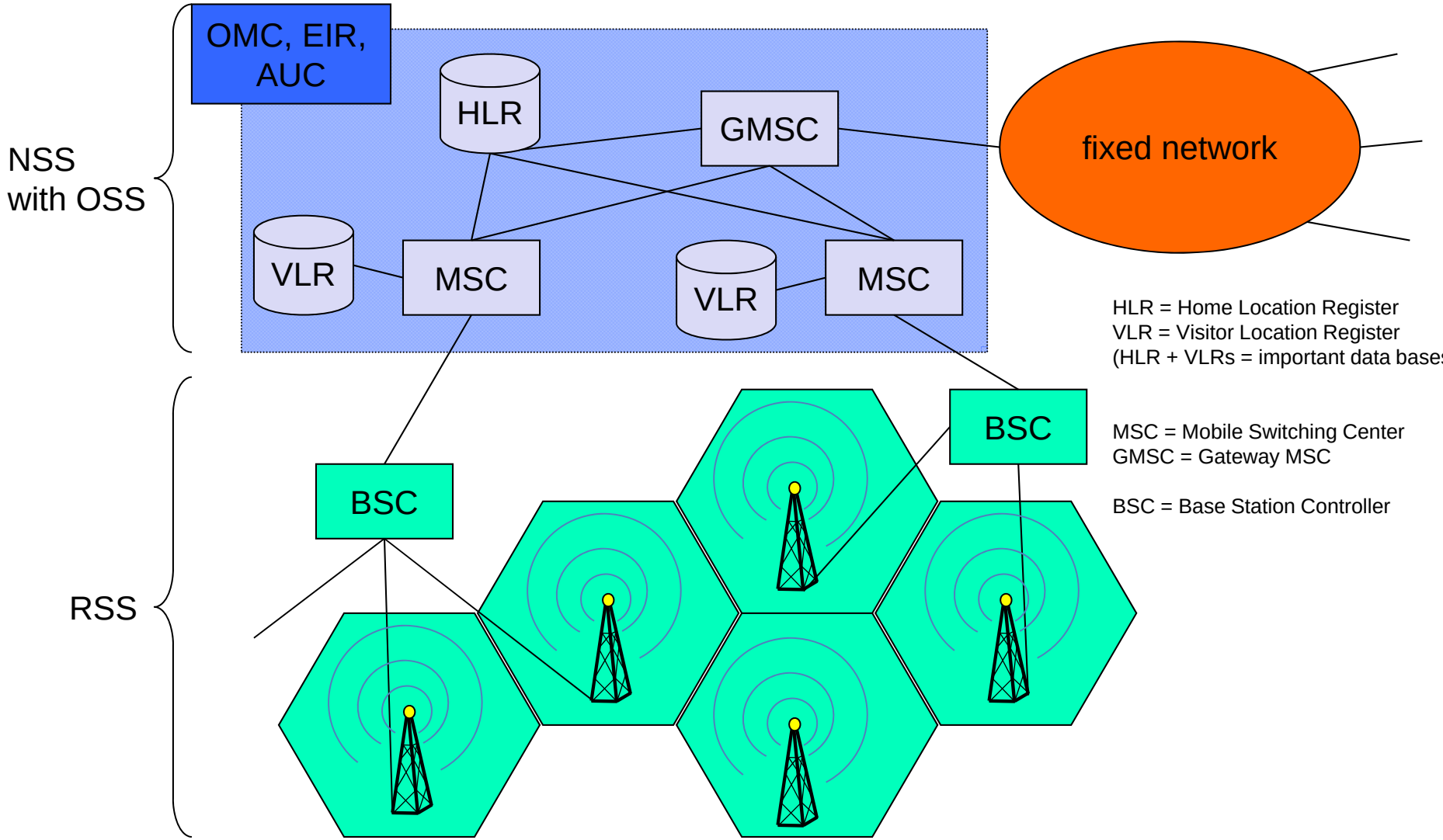
Switching units

Management

Data bases

Monitoring

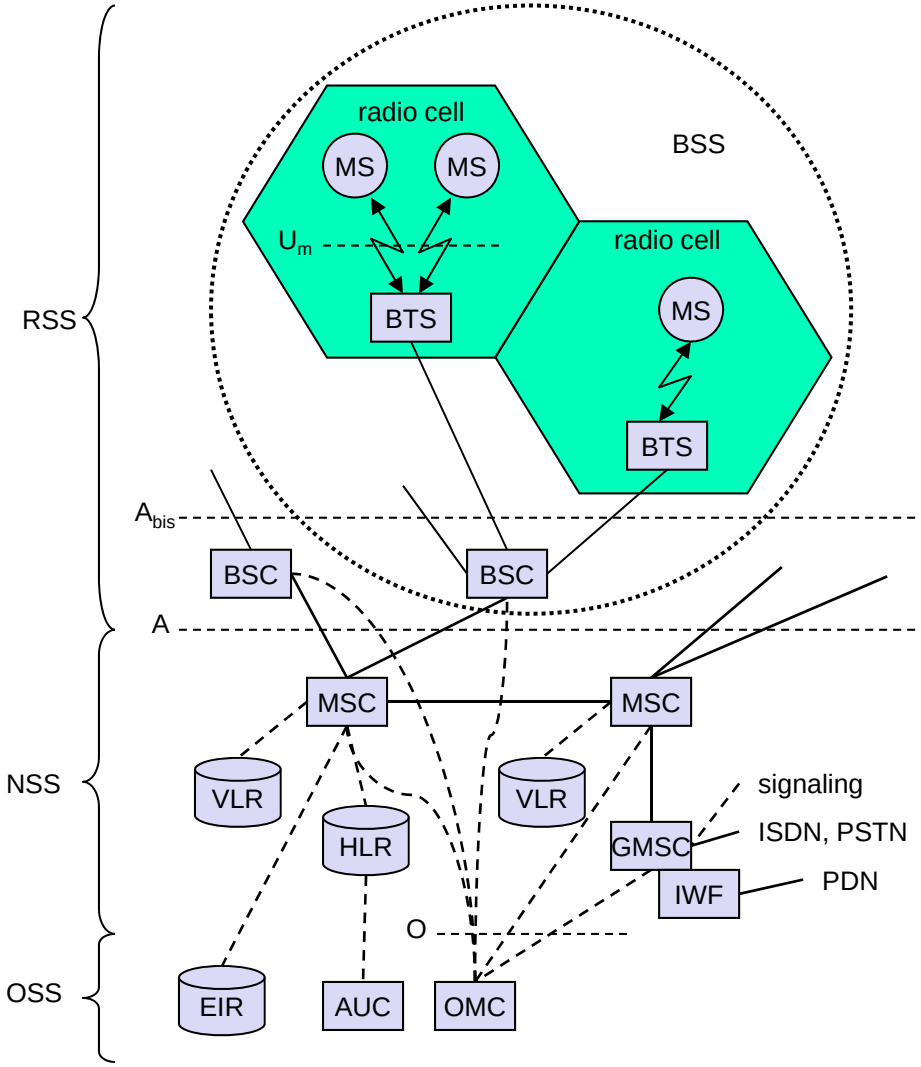
Not „visible“, but comprise the major part of the network (also from an investment point of view…)



HLR = Home Location Register
VLR = Visitor Location Register
(HLR + VLRs = important data bases)

MSC = Mobile Switching Center
GMSC = Gateway MSC

BSC = Base Station Controller



Interfaces
- U_m
- A_{bis}
- A
- O

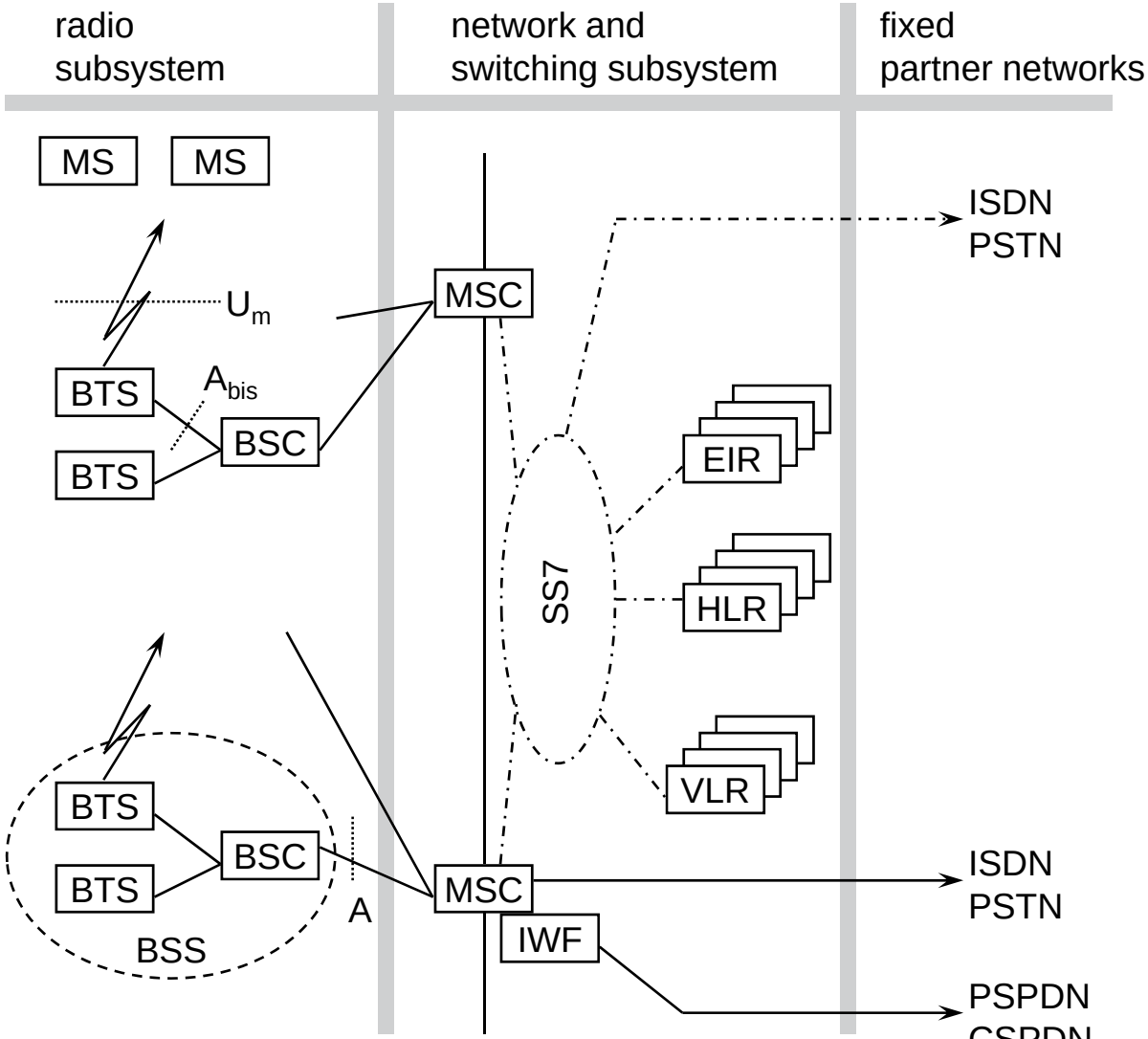
MS = Mobile Station
BTS = Base Transceiver Station

BSC = Base Station Controller

HLR = Home Location Register
VLR = Visitor Location Register

MSC = Mobile Switching Center
GMSC = Gateway MSC
IWF = Interworking Function

details on following slides



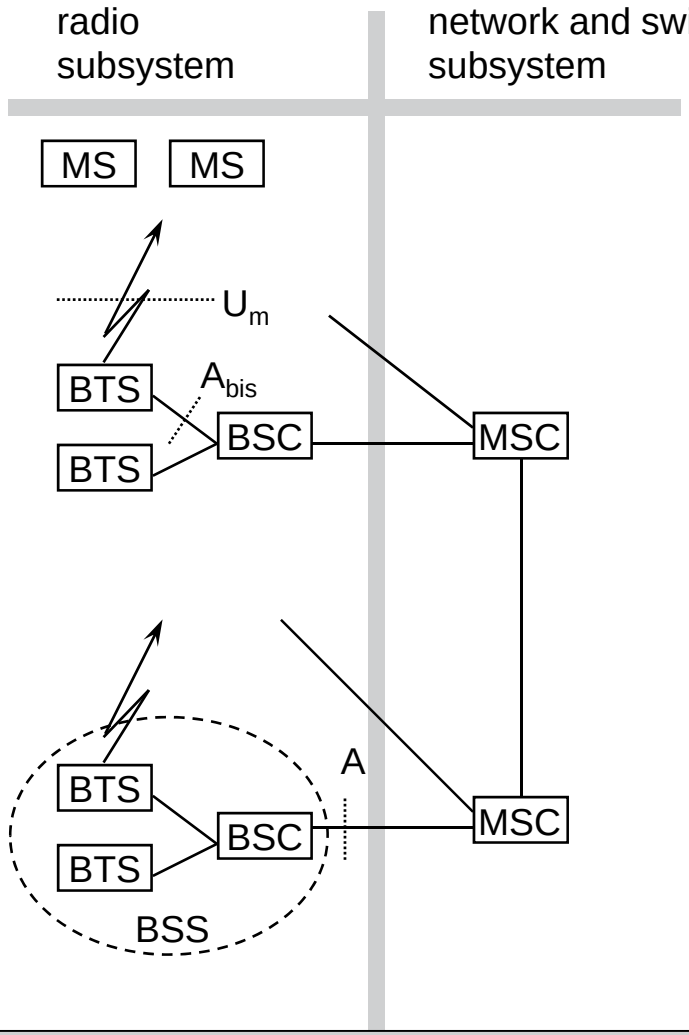
MS = Mobile Station
BTS = Base Transceiver Station

BSC = Base Station Controller

HLR = Home Location Register
VLR = Visitor Location Register

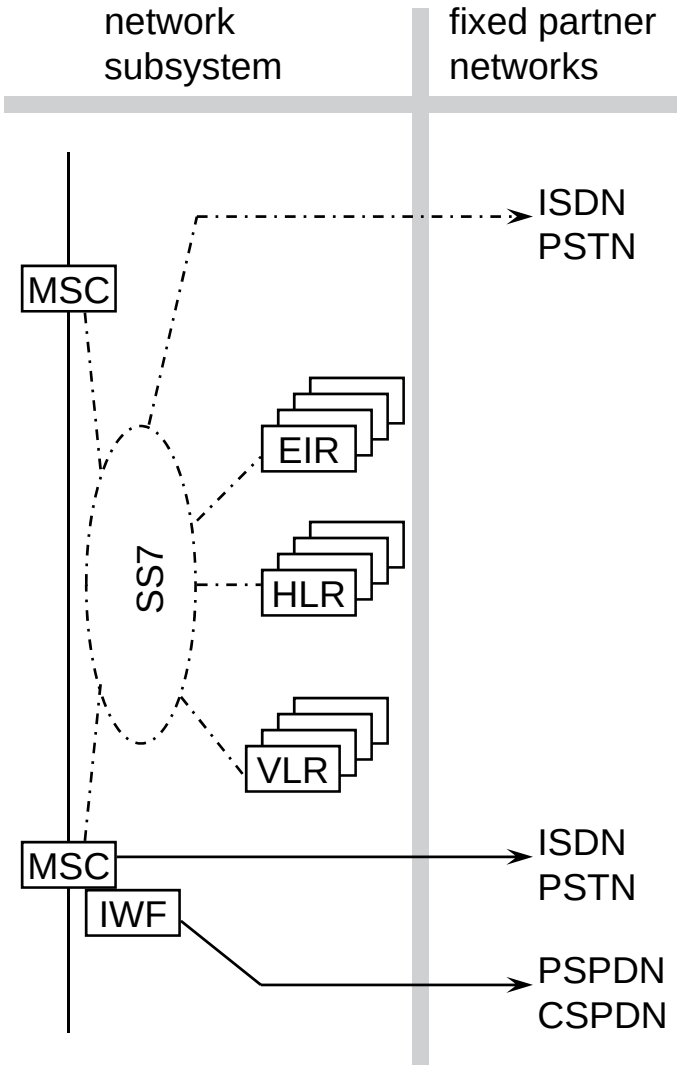
MSC = Mobile Switching Center
GMSC = Gateway MSC
IWF = Interworking Function

details on following slides



clearly defined interfaces (open system)
compatible to ISDN (wired) telephone system

- **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



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)

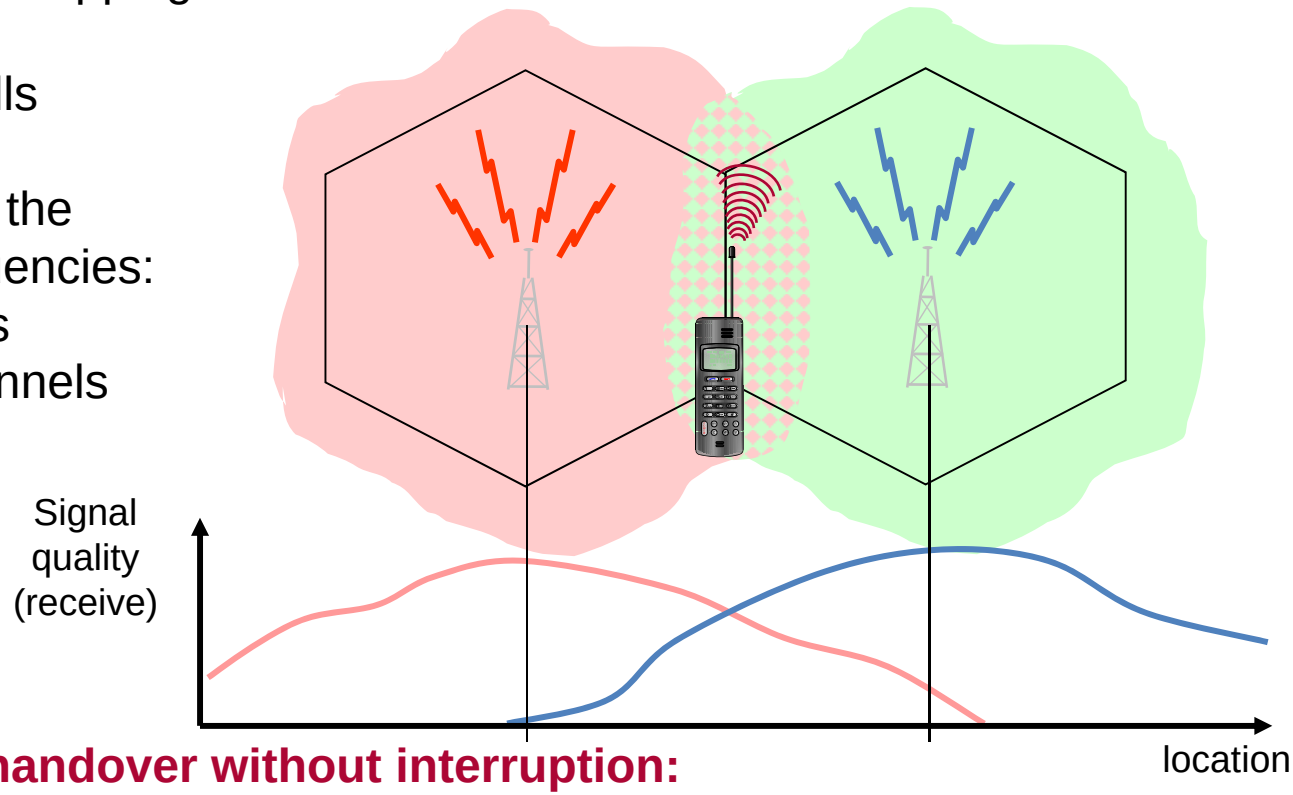
- **The Radio Subsystem** (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - **Base Station Subsystem** (BSS):
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - 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)**

Cellular network principle

Purpose

- base station (cell) only has limited capacity
- coverage of large areas
  by using small overlapping cells
- use different frequencies
  in neighboring cells

- cellular principle reduces the number of available frequencies:
  < 125 frequencies
  < 1000 phys. channels



Overlap of cells enables handover without interruption:

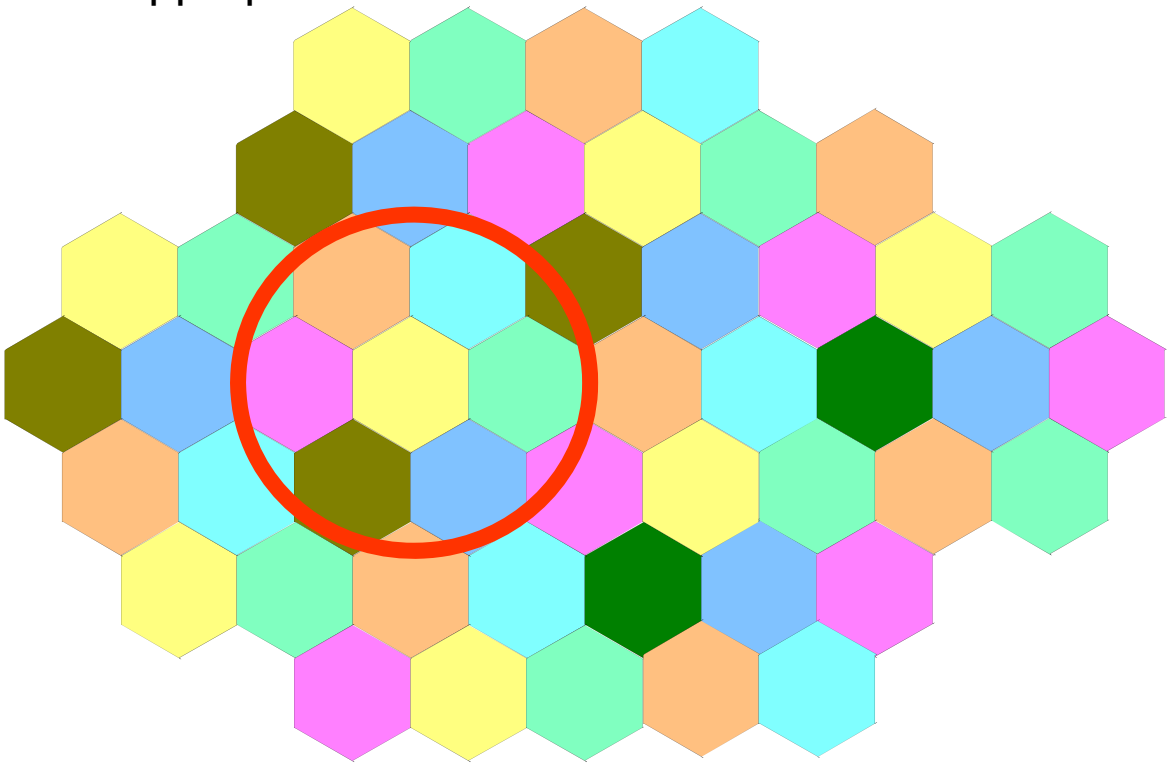
MS (Mobile Station) is still in contact with old BTS (Base Transceiving Station)

- new BTS receive quality is better than from old BTS
- prepare handover with old BTS
- switch to new BTS (almost no interruption)

Cellular network (2)

Reuse of frequencies

- Use a subset of all available frequencies in a single cell
- all direct neighbour cells use different subset (to avoid interference)
- reuse of same frequency subset in appropriate distance



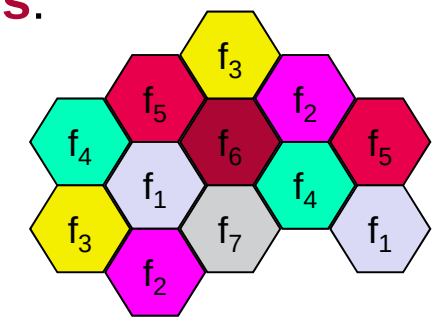
Cell clustering

- a typical representation of a cell is a hexagon
- a cluster of cells use different subsets of frequencies
- the same subsets repeat in further clusters

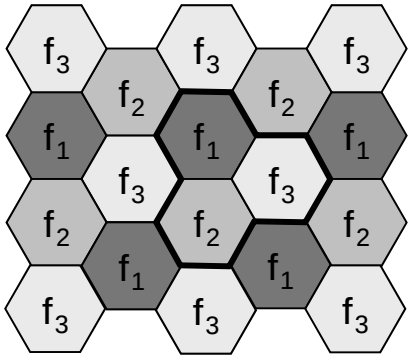
Typical values

- k = 7 (number of cells per cluster)
- D ≈ 4,4 • radius of cell (distance between cells with identical frequency subset)

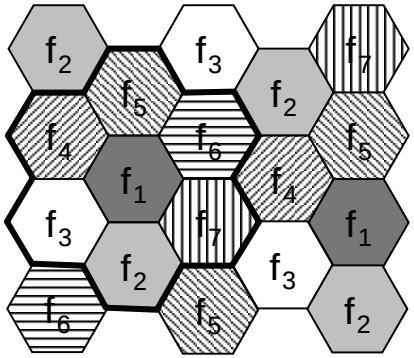
- Frequency reuse only with a certain distance between the base stations
- **Standard model using 7 frequencies**:



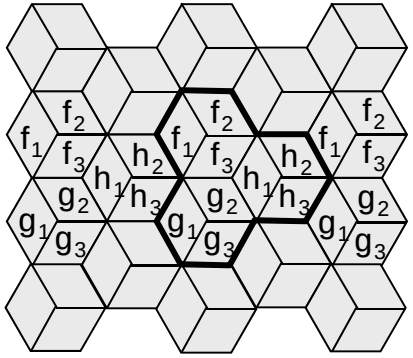
- **Fixed frequency assignment**:
  - certain frequencies are assigned to a certain cell
  - problem: different traffic load in different cells
- **Dynamic frequency assignment**:
  - base station chooses frequencies depending on the frequencies already used in neighbor cells
  - more capacity in cells with more traffic
  - assignment can also be based on interference measurements



3 cell cluster



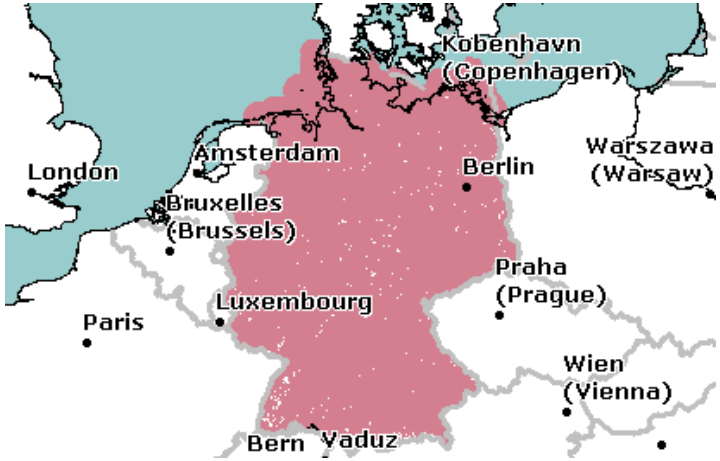
7 cell cluster



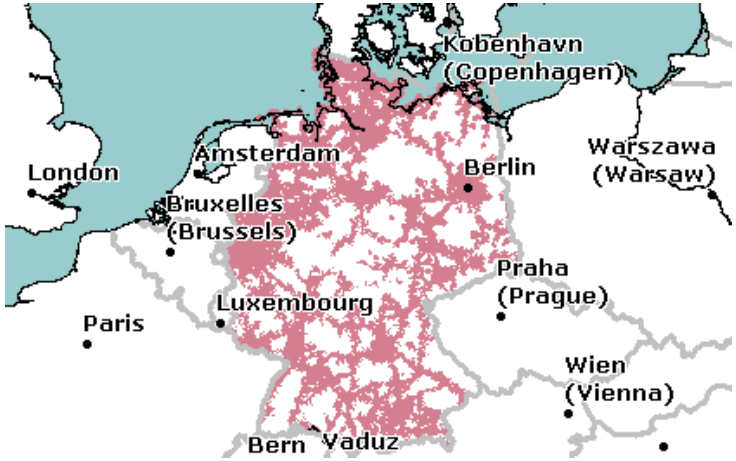
3 cell cluster
with 3 sector antennas

Example coverage of GSM networks (www.gsmworld.com) JS

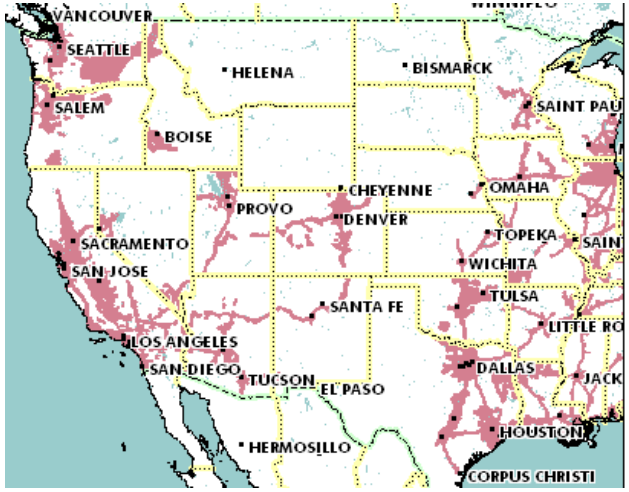
T-Mobile (GSM-900/1800) Germany



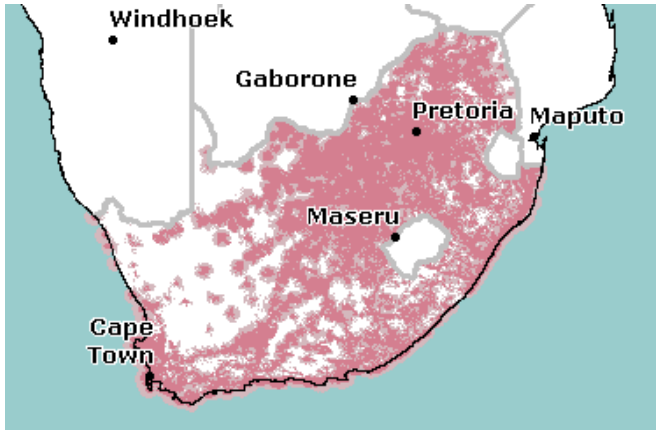
O_2 (GSM-1800) Germany



AT&T (GSM-850/1900) USA



Vodacom (GSM-900) South Africa



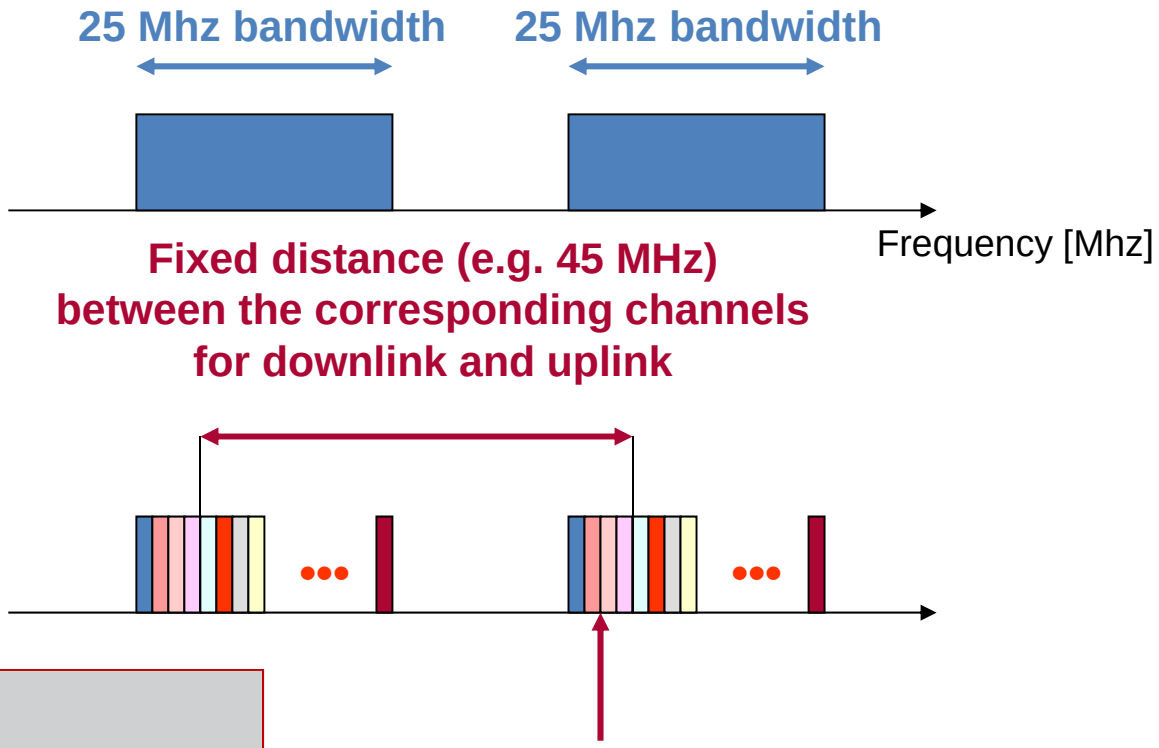
Concepts for Multiple Access: FDMA in GSM

Goal of Multiple Access: Several mobile stations intend to communicate „in parallel“ with the same base station.

The access to the shared medium „air“ (the radio frequencies) has to be coordinated in a deterministic manner (provide QoS for voice transmission, i.e. no collisions allowed)

Frequency Division Multiple Access (FDMA) in GSM:

- two bands of 25 MHz (each for uplink and downlink = Frequency Division Duplex) are divided into 125 channels of 200 kHz bandwidth

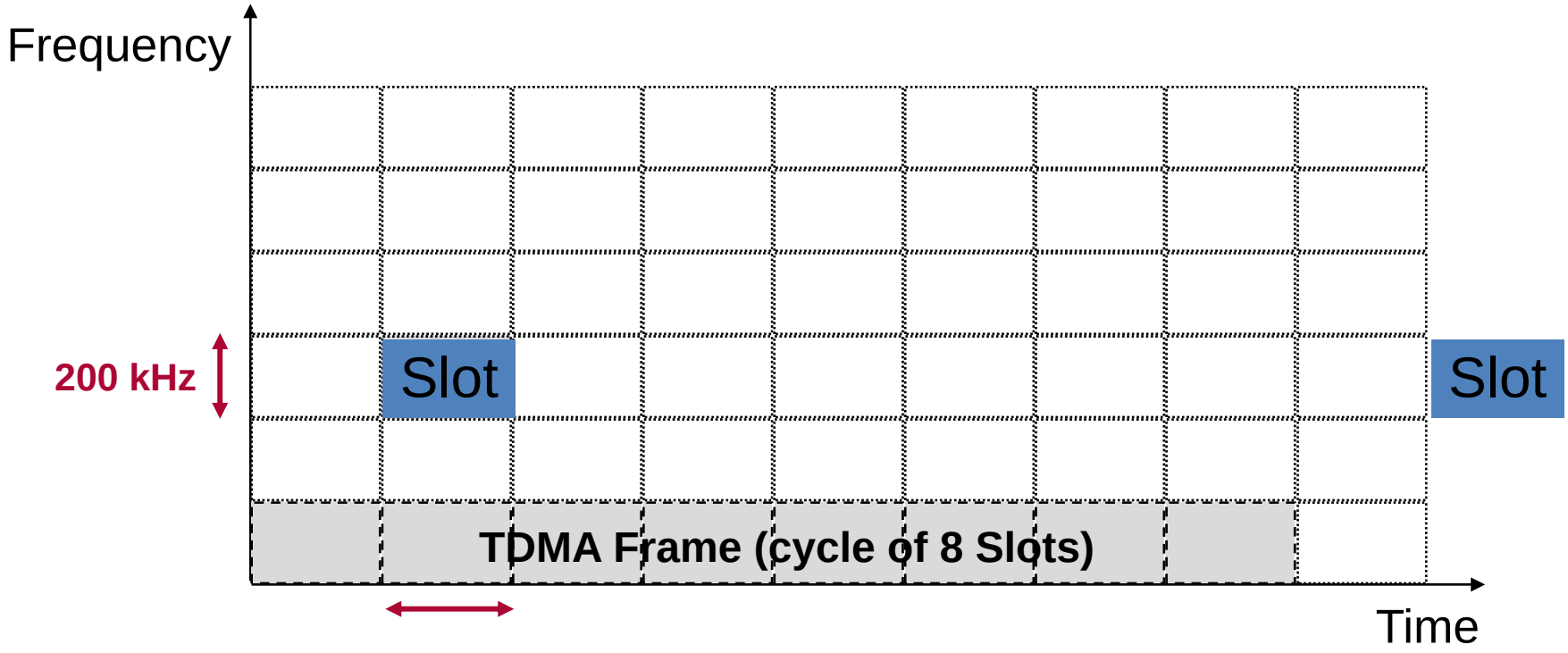


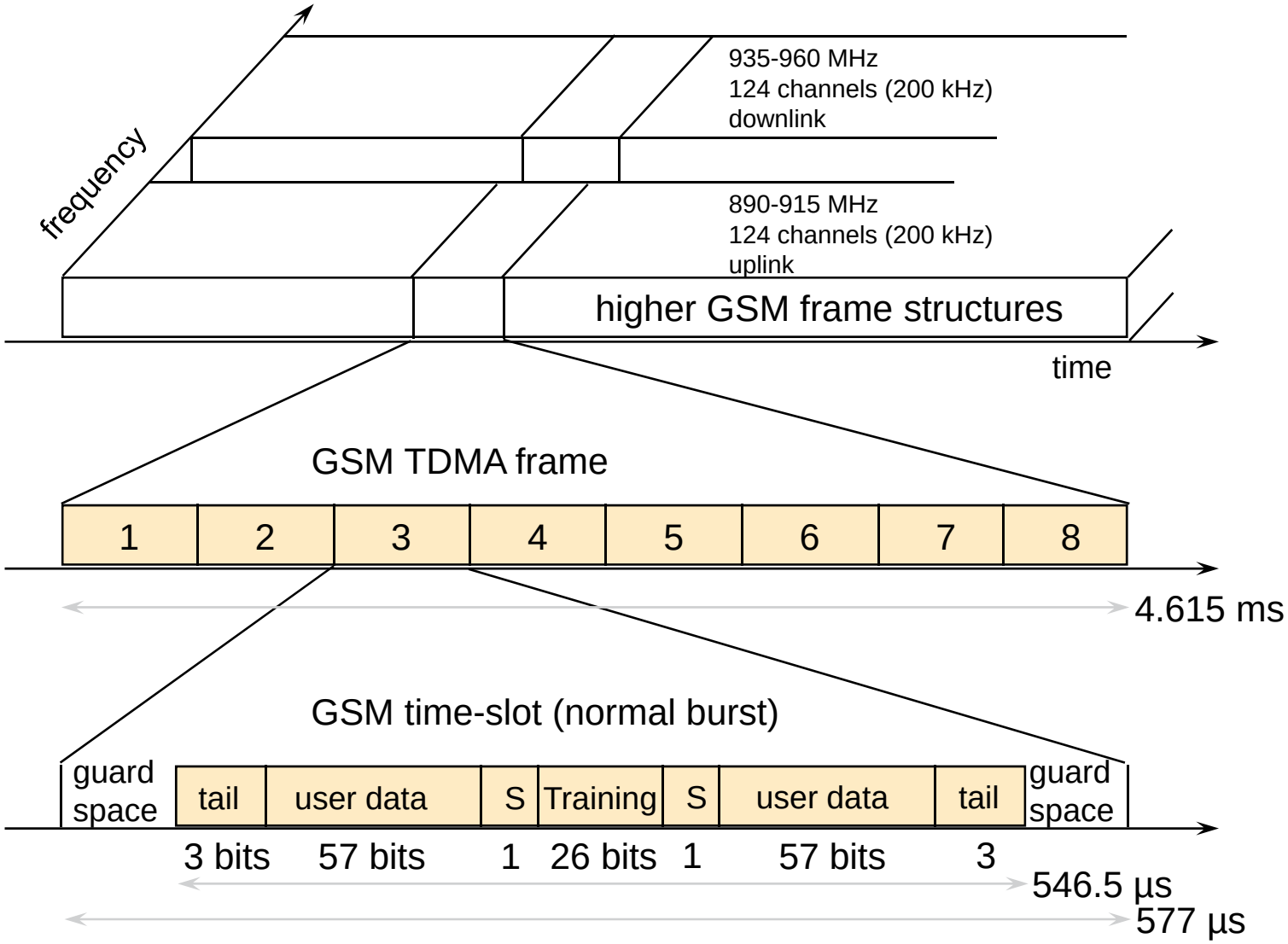
=> cf. chapter
2. Wireless Communication Basics

Time Division Multiple Access (TDMA):

- each channel (of FDMA) is divided into 8 time slots (= 1 cycle)
- the raw datarate in a 200 kHz channel amounts to 271 kbit/s
- the raw datarate per time-slot (TDMA channel) is 33,875 kbit/s

Result: **8 physical channels** (33,875 kbit/s each) **per frequency channel,**
Altogether 125 • 8 = **1000 physical channels** in 25 Mhz





Question: All time slots/frequencies available for voice channels?

Answer: **NO!**

Several channels are needed for control purposes **within each GSM cell**:

- Downlink: **Broadcast channel**, announce identity of cell, GSM network, …
  (similar to WLAN beacon)

- Uplink (UL): **Random Access CHannel** (RACH)
  initial access of mobile phones to GSM network
  goal: set up a dedicated control channel
  collisions in RACH are possible!

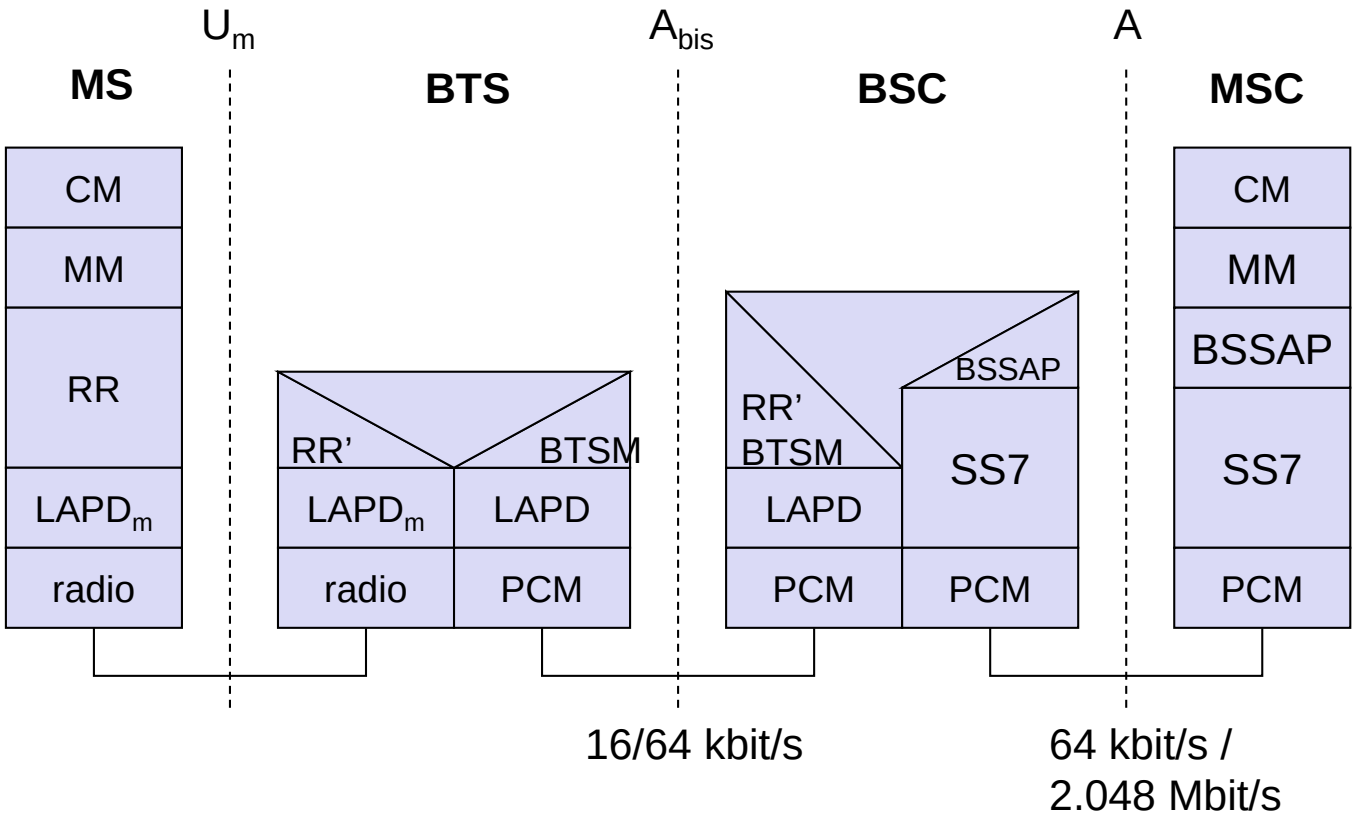
- Downlink (DL): **Access Grant Channel**, answer to requests in RACH
- Downlink (DL): **Paging Channel**, GSM network initiating contact to mobile phone

- DL/UL: **dedicated control channel**
  used for signalling before set up of voice channel

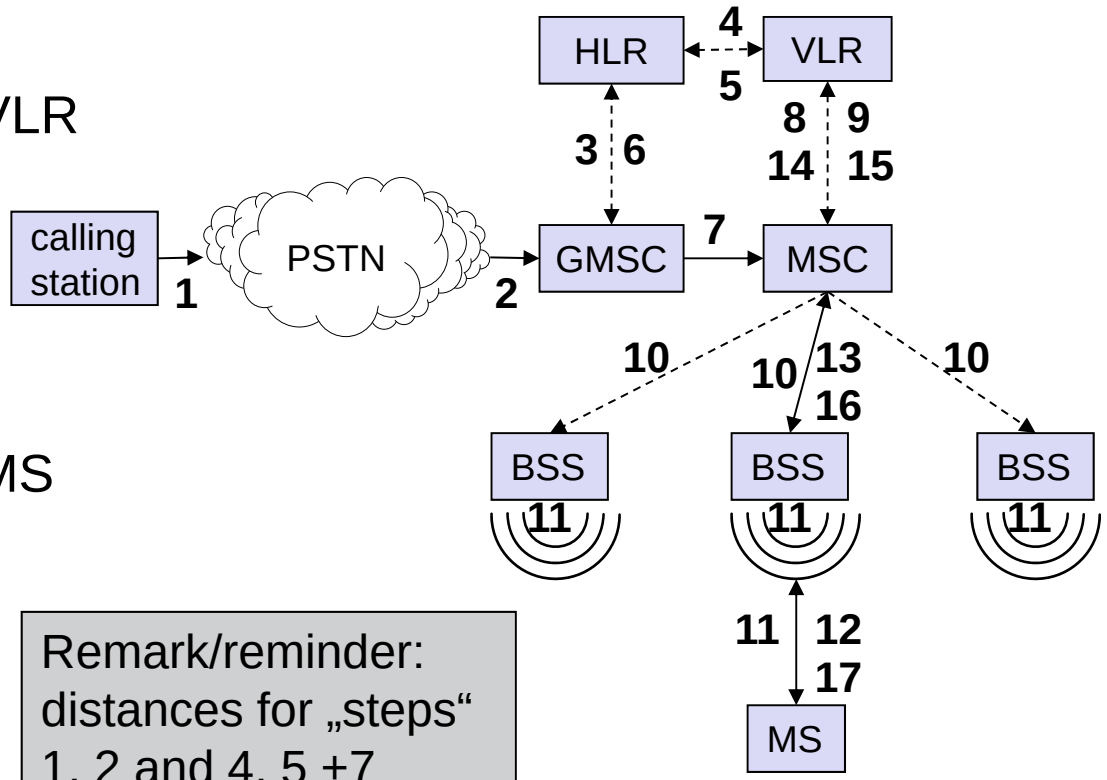
- DL/UL, within assigned voice channel:
  in-band low bandwidth signalling channel
  (e.g. used for handover control)

- **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, including data about all user currently in the domain of the VLR

- 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**

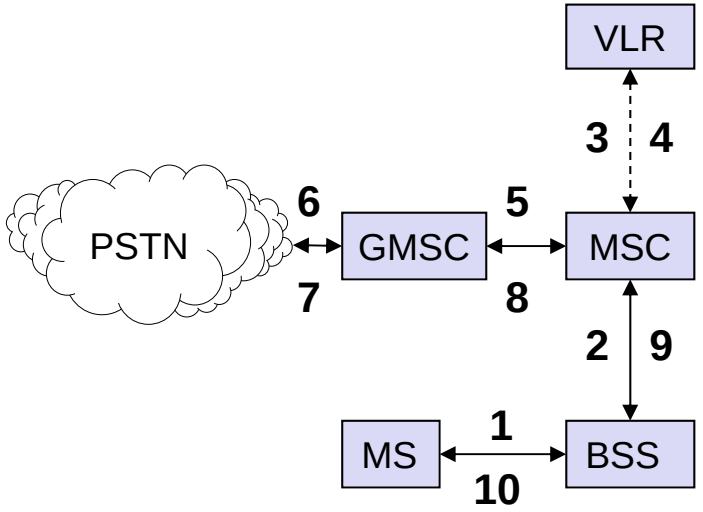


- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4, 5: request MSRN from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: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



Remark/reminder:
distances for „steps“
1, 2 and 4, 5 +7
might be (very) large!

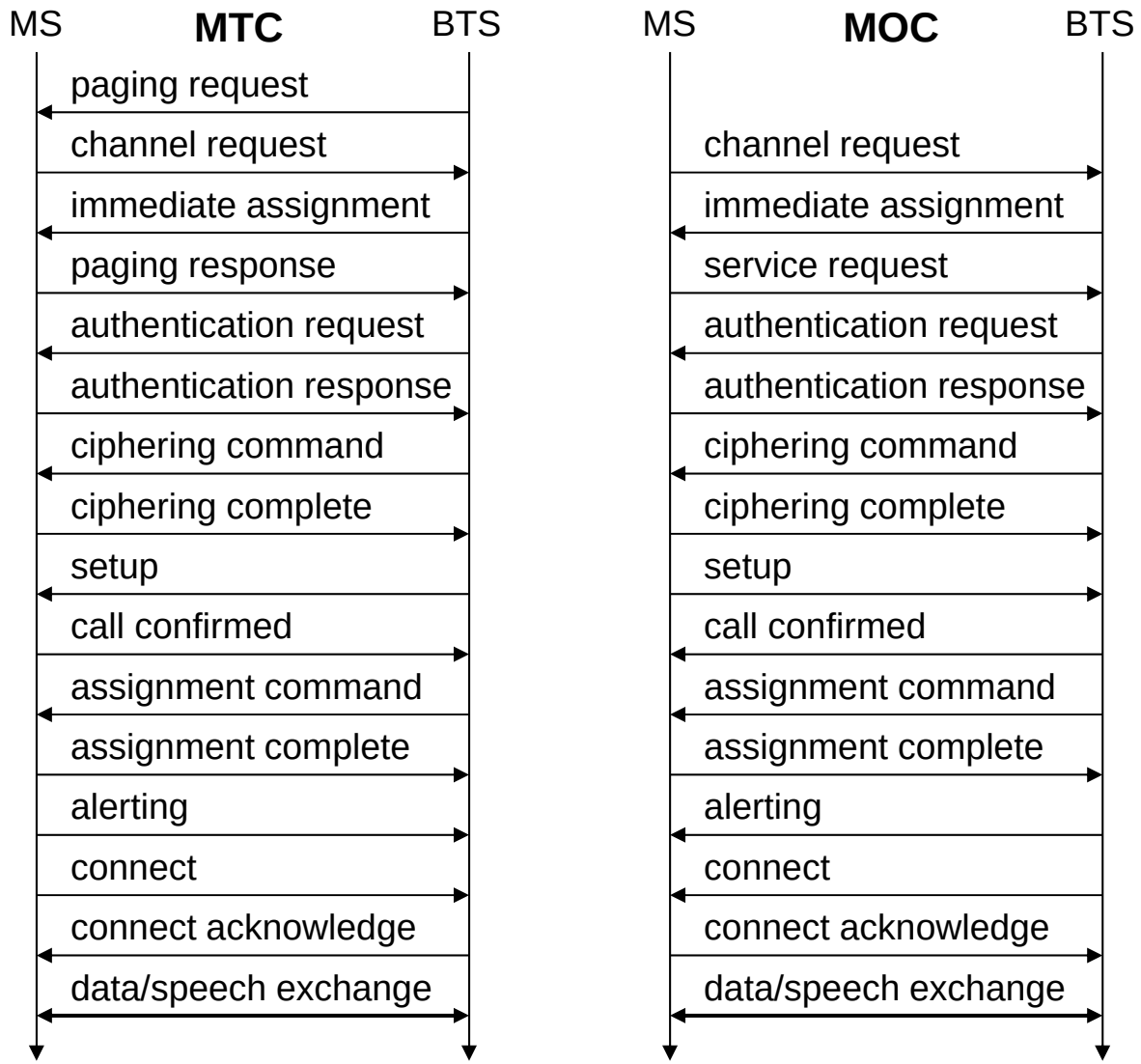
- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



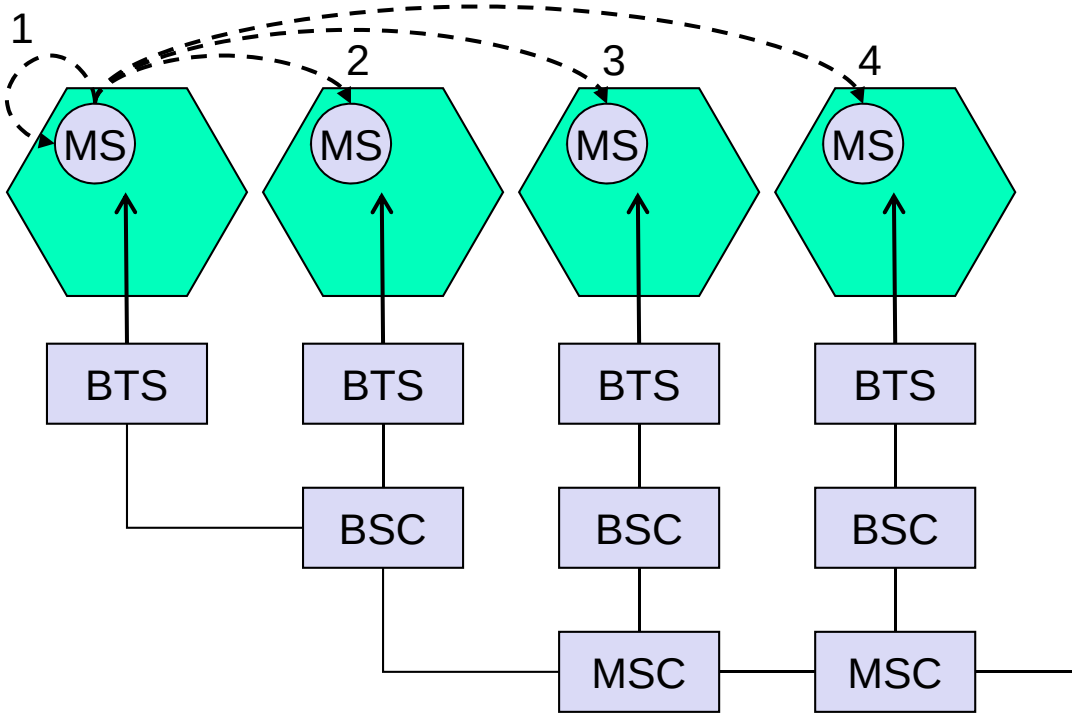
cf. network failure of April 2009
mobile originated call is possible without HLR interaction
(at least for a certain time period)

Air interface traffic for MTC/MOC

JS



Four Types of Handover

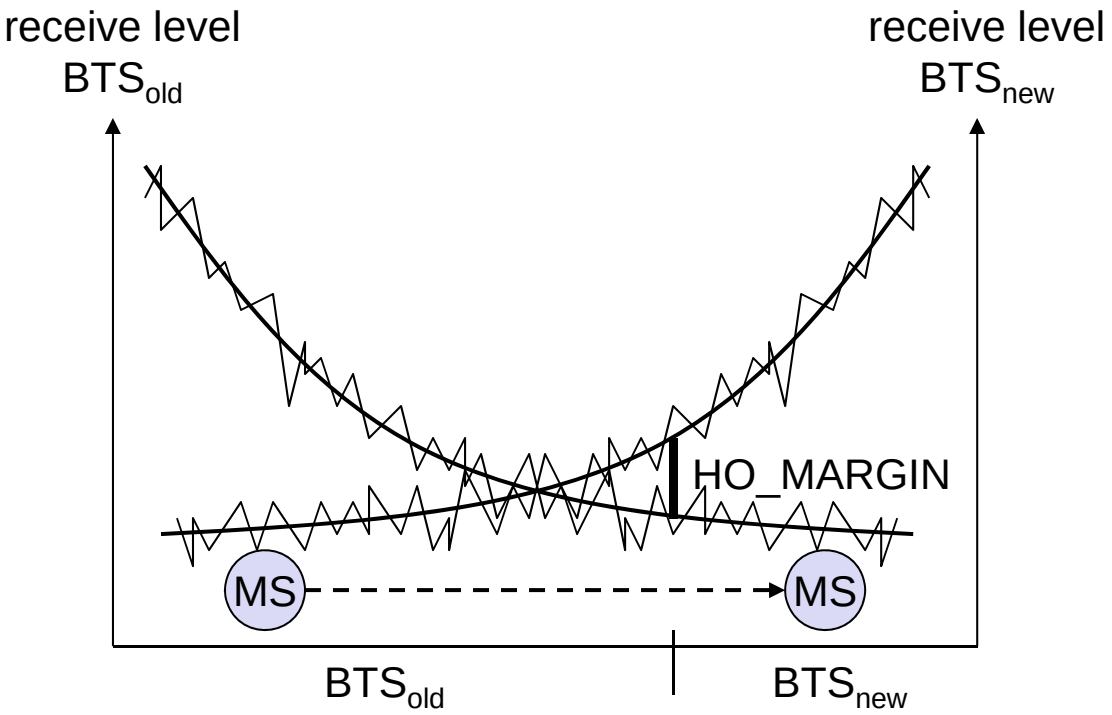


1: Intra-Cell, Intra-BTS

2: Inter-BTS (same BSC)

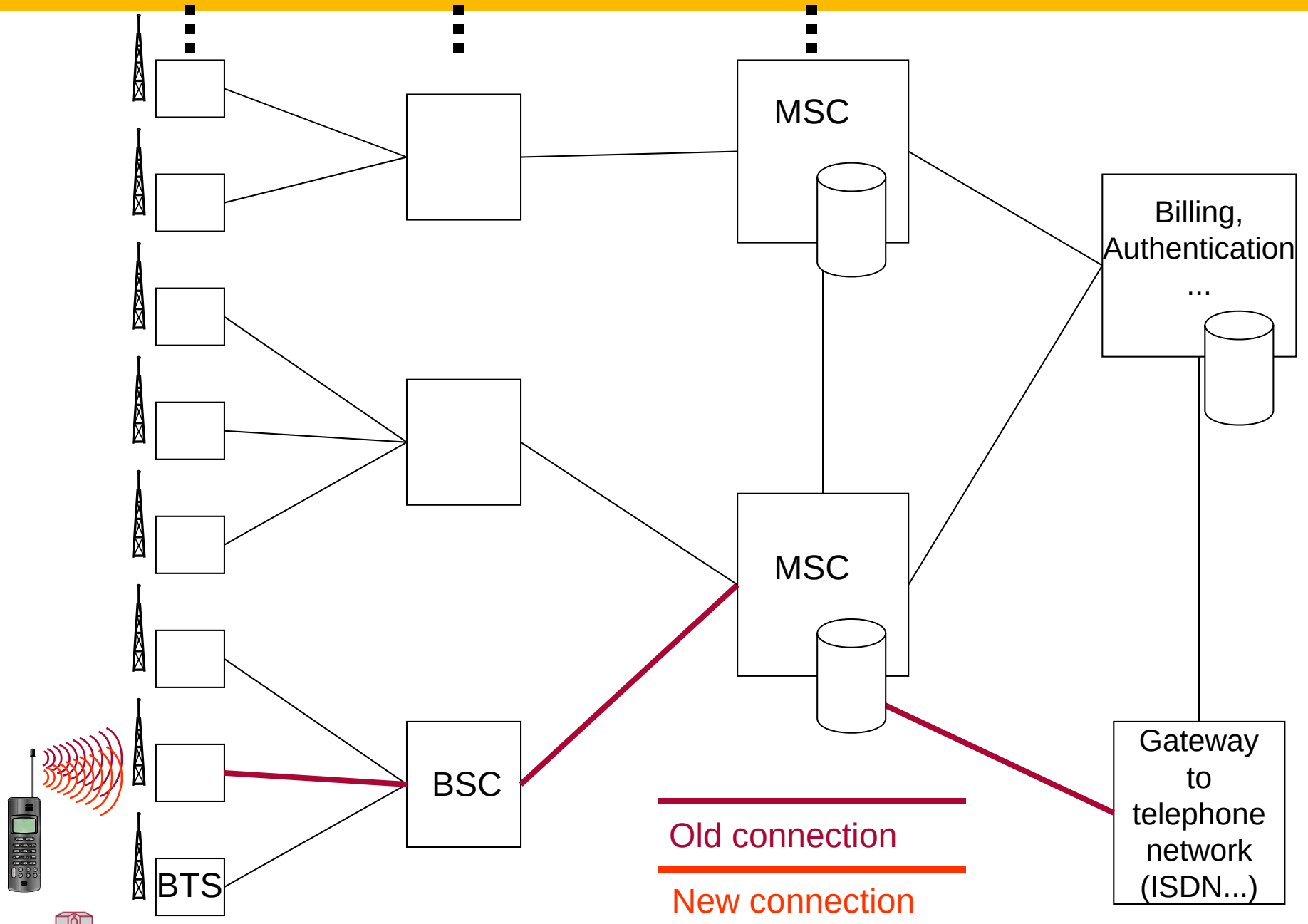
3: Inter-BSC (same MSC)

4: Inter-MSC

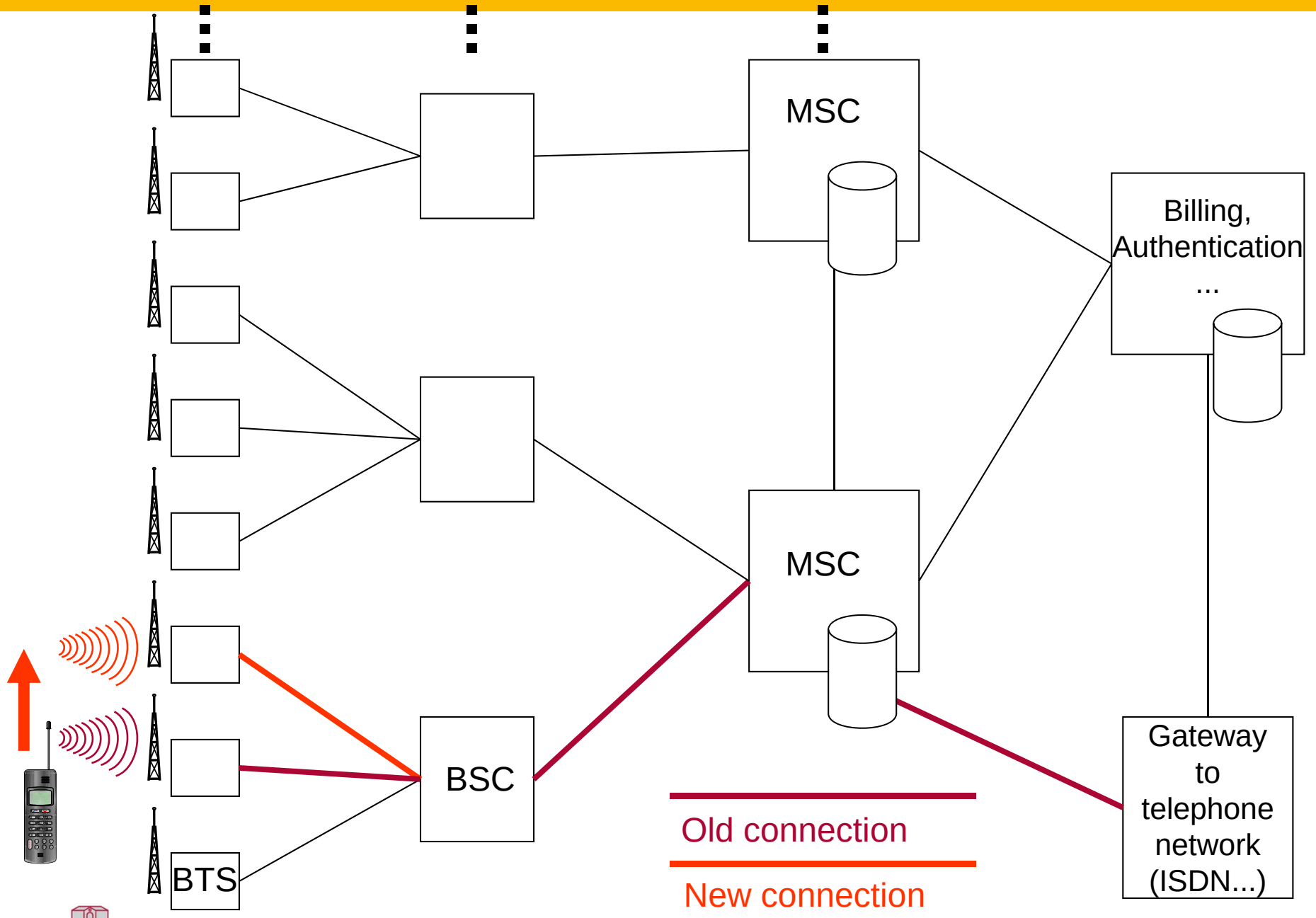


- when moving (slowly) between BTS old and new, a **“ping pong” effect** may occur
- “ping pong” = **switching back and forth** between new and old BTS (several times)
- may be prevented (or reduced) by defining a **hysteresis for handover decision** (HO_MARGIN)

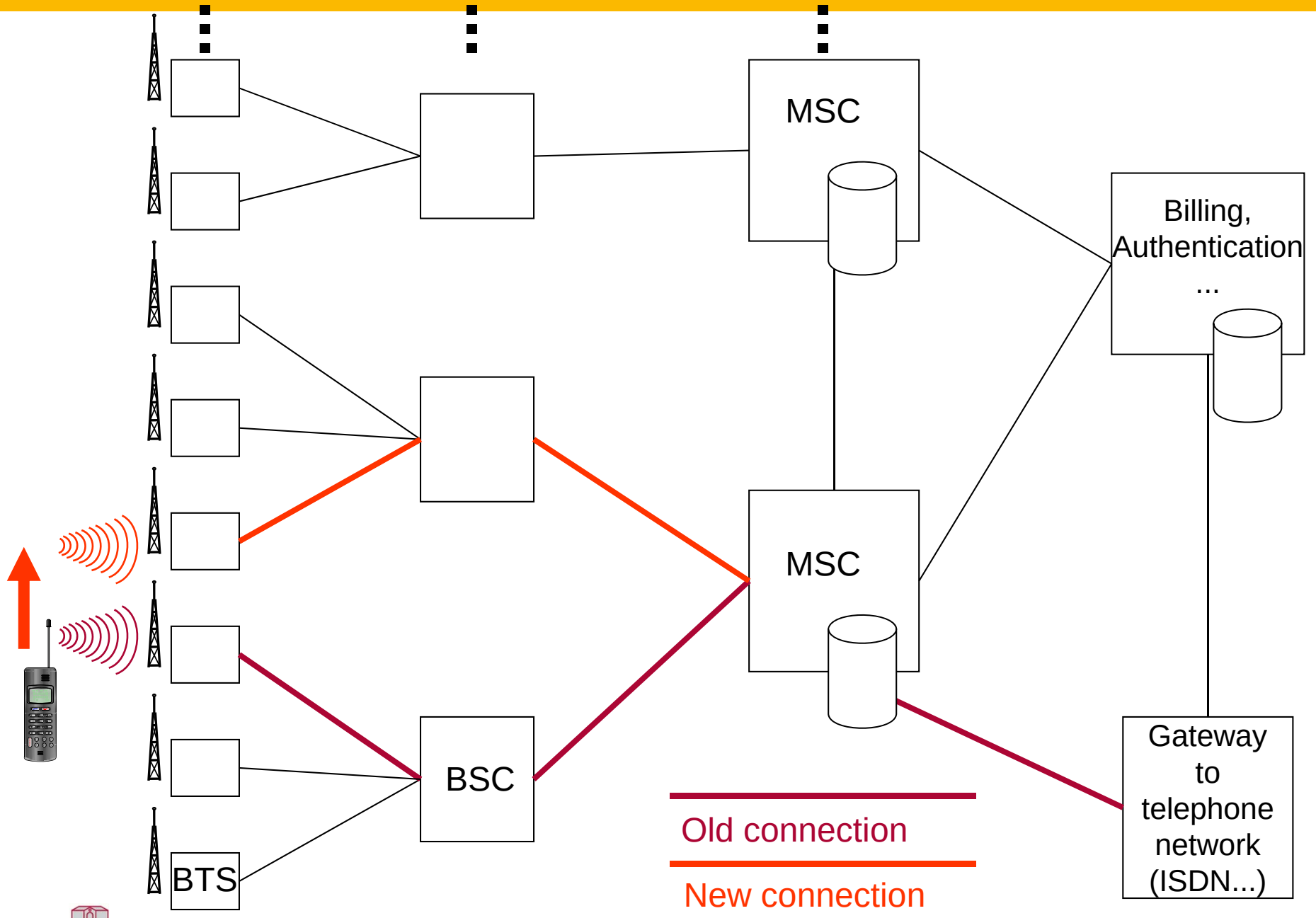
Overview handover types: Intra-Cell Handover



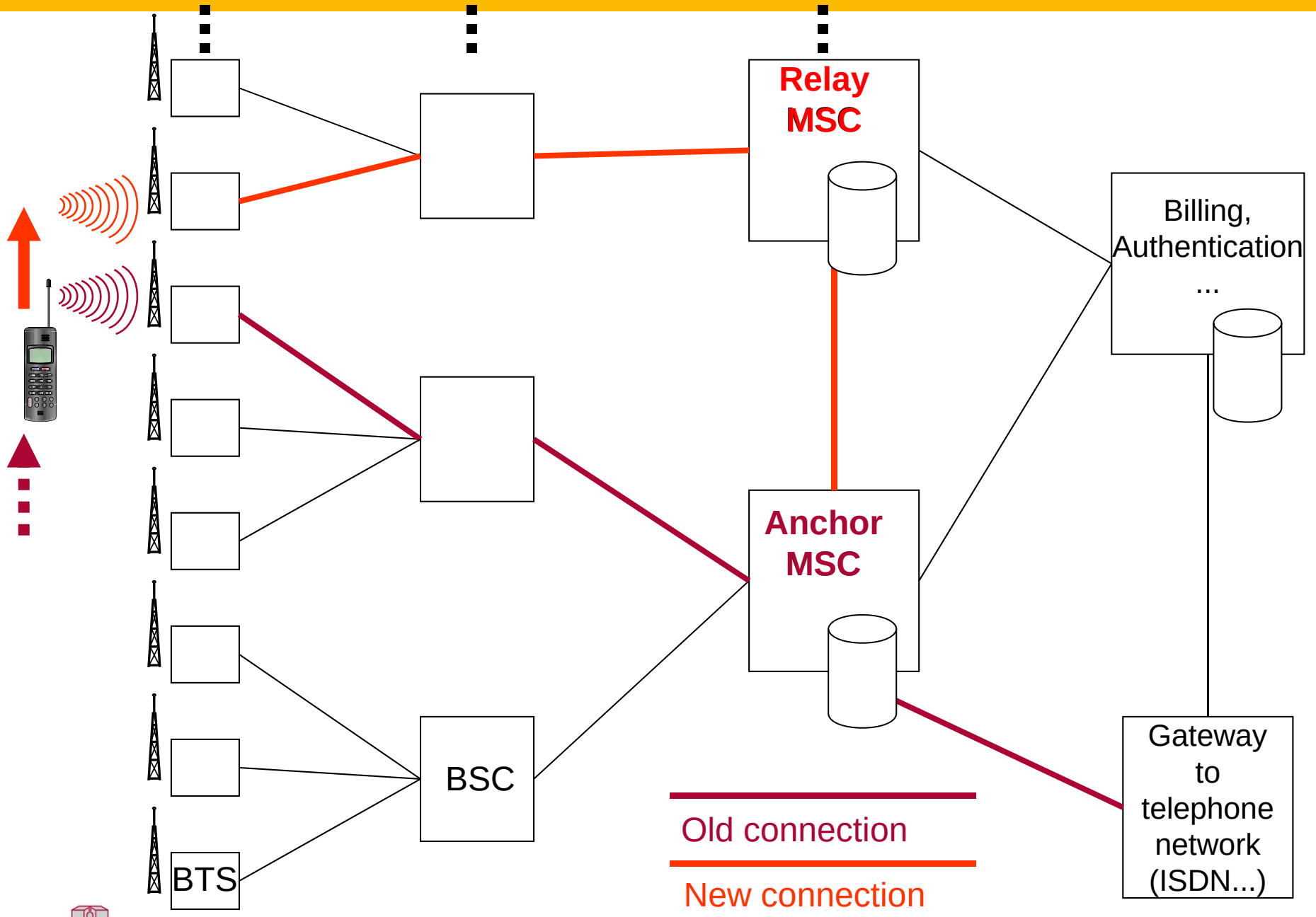
Overview handover types: BTS-BTS Handover



Overview handover types: BSC-BSC Handover



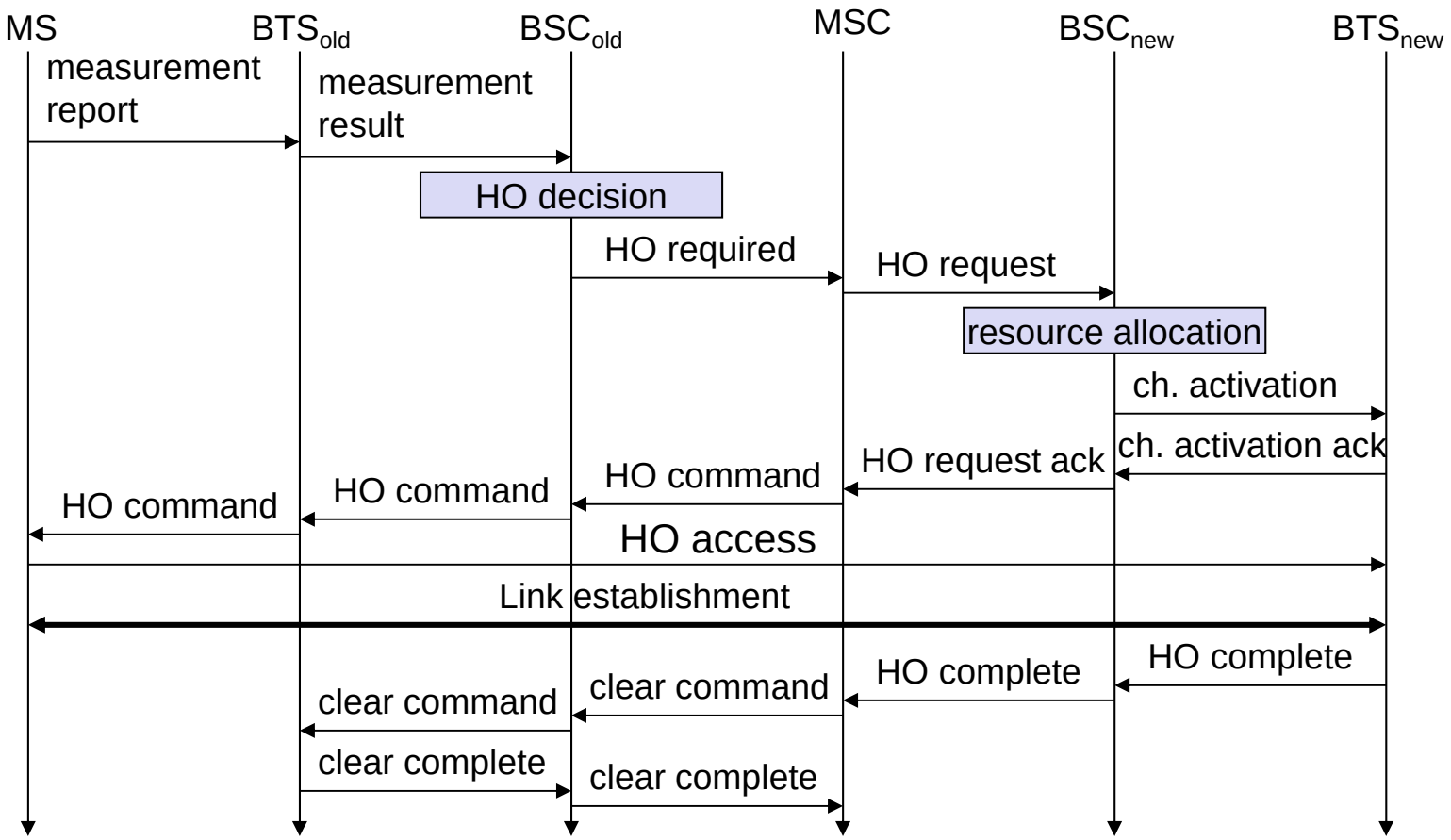
Overview handover types: MSC-MSC Handover



Handover procedure (BSC-BSC handover)

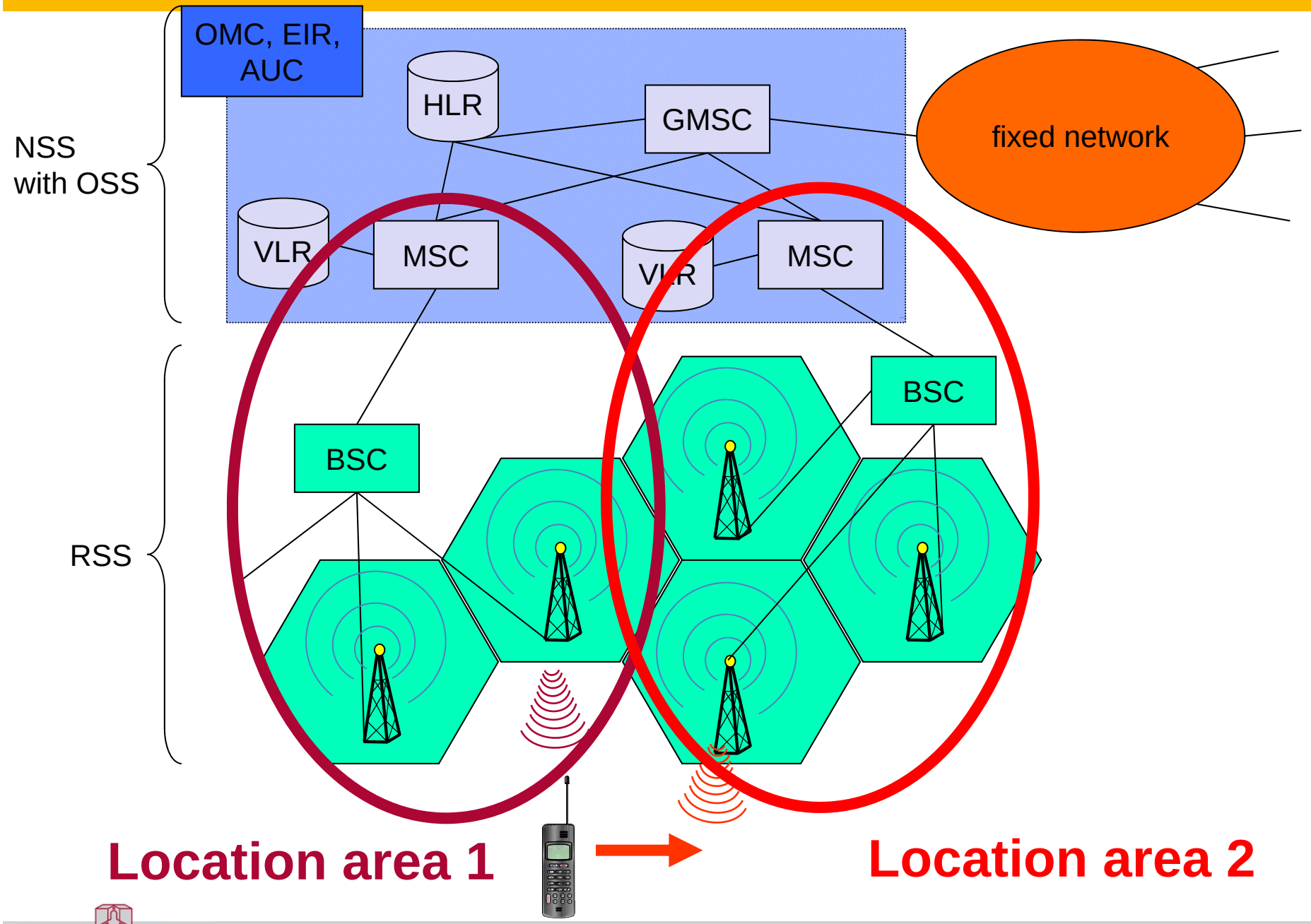
JS

(BTS and BSC change, MSC stays the same)



Location update overview

JS



Important procedure to update location information in HLR and VLR

Location update - prerequisite

- mobile station is switched on
- but MS is “idle” (= no phone call going on – in contrast to handover)

Carrying out location update

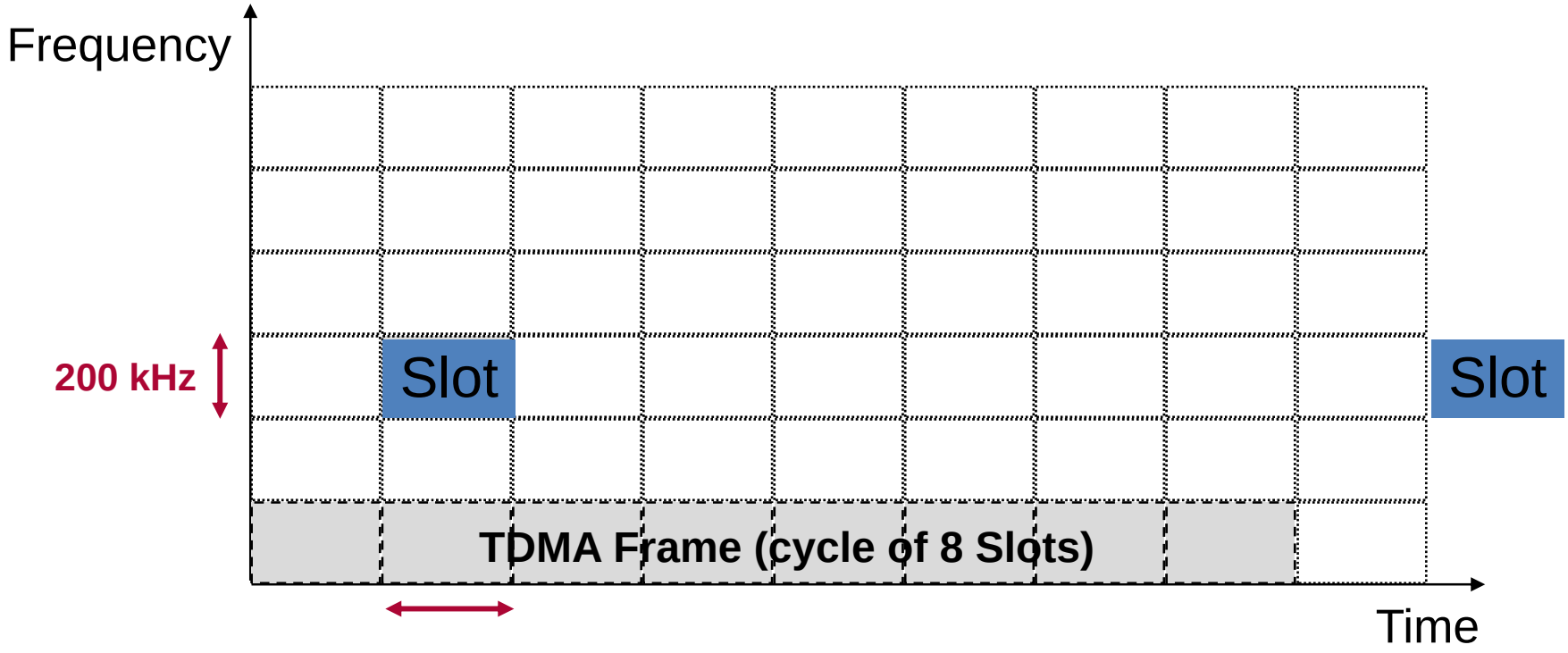
- mobile station frequently measures reception quality of BTSs
- MS decides to “camp on a cell” (select best BTS)
- MS analyses location area identity (LAI) as broadcasted from BTS

- if LAI has changed when moving from old BTS to new BTS

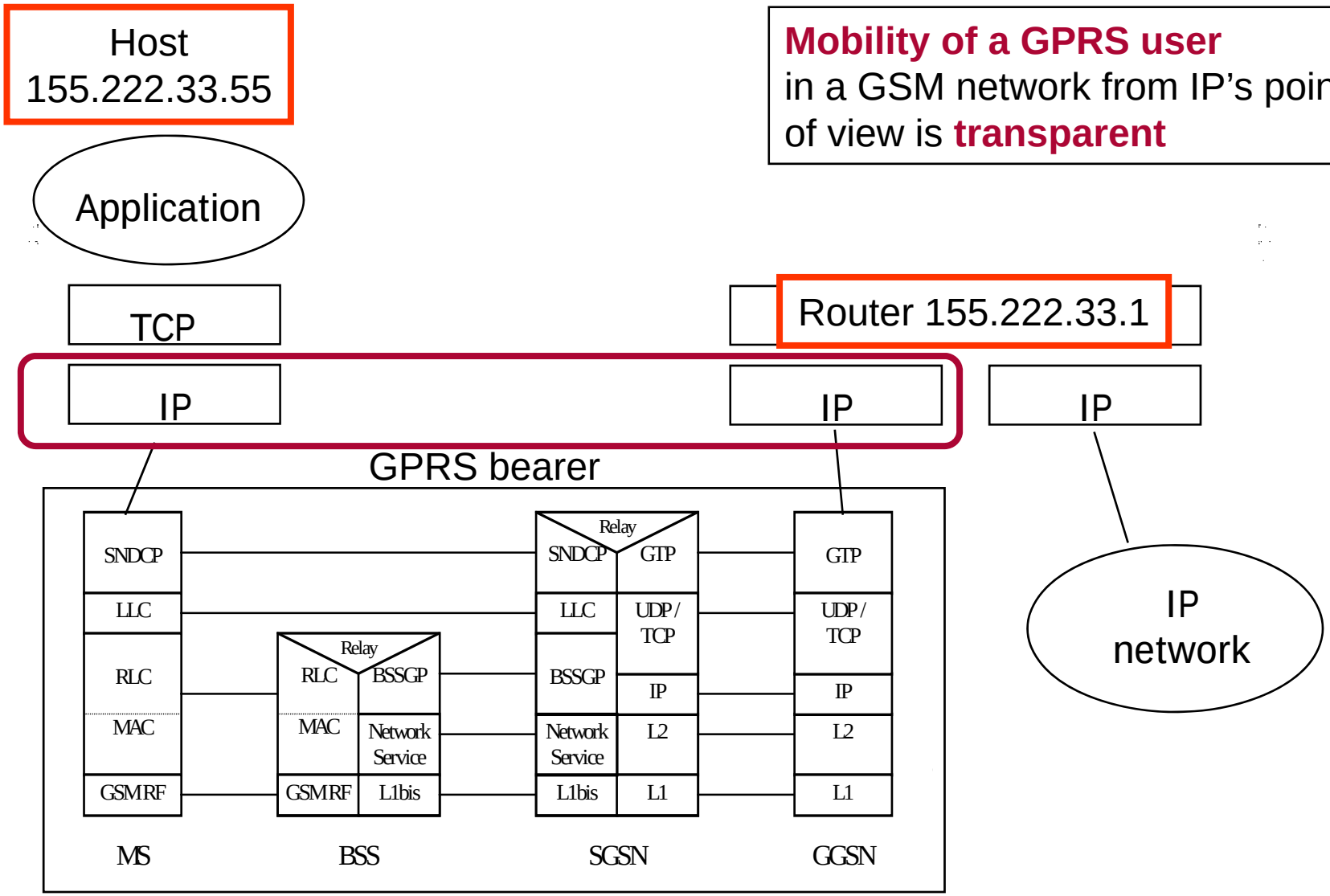
=> MS initiates location update

Data Services based on GSM

- basic GSM — 9,6 – 14,4 kbit/s
- HSCSD (High-Speed Circuit Switched Data) — 57.6 kbit/s using 4 slots @ 14.4
- GPRS (General Packet Radio Service) — 50 kbit/s using 4 slots temporarily



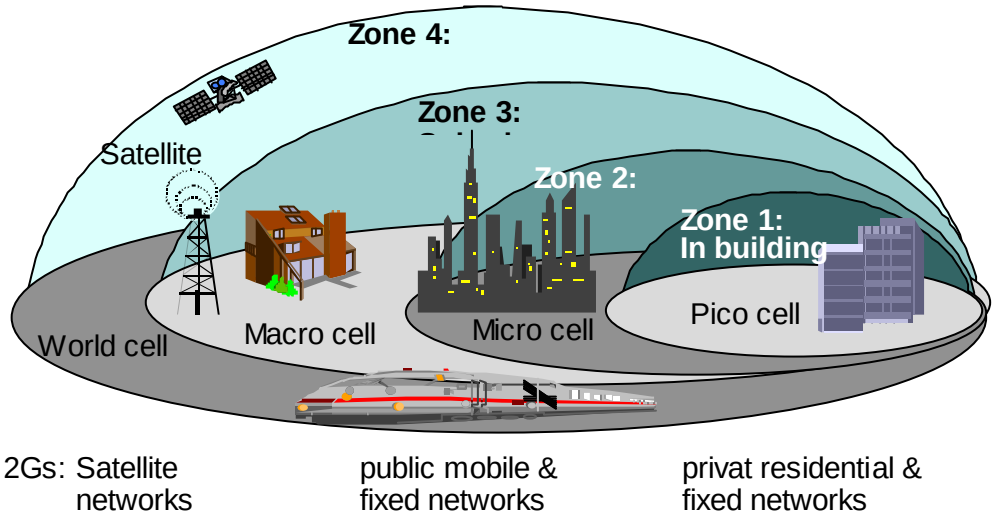
GPRS User Plane Protocols



Mobility of a GPRS user in a GSM network from IP's point of view is **transparent**

Handovers between different SGSN is supported within the GSM/GPRS network

4.2. Overview of 3G/UMTS and its architecture



(Fig. source: Report No. 6 from the UMTS Forum, www.umts-forum.org)

- **Global System**: national terrestrial components and global (world-wide) satellite technology
- Multi-mode and multi-band technology includes systems of second generation (2G, 2.5G)

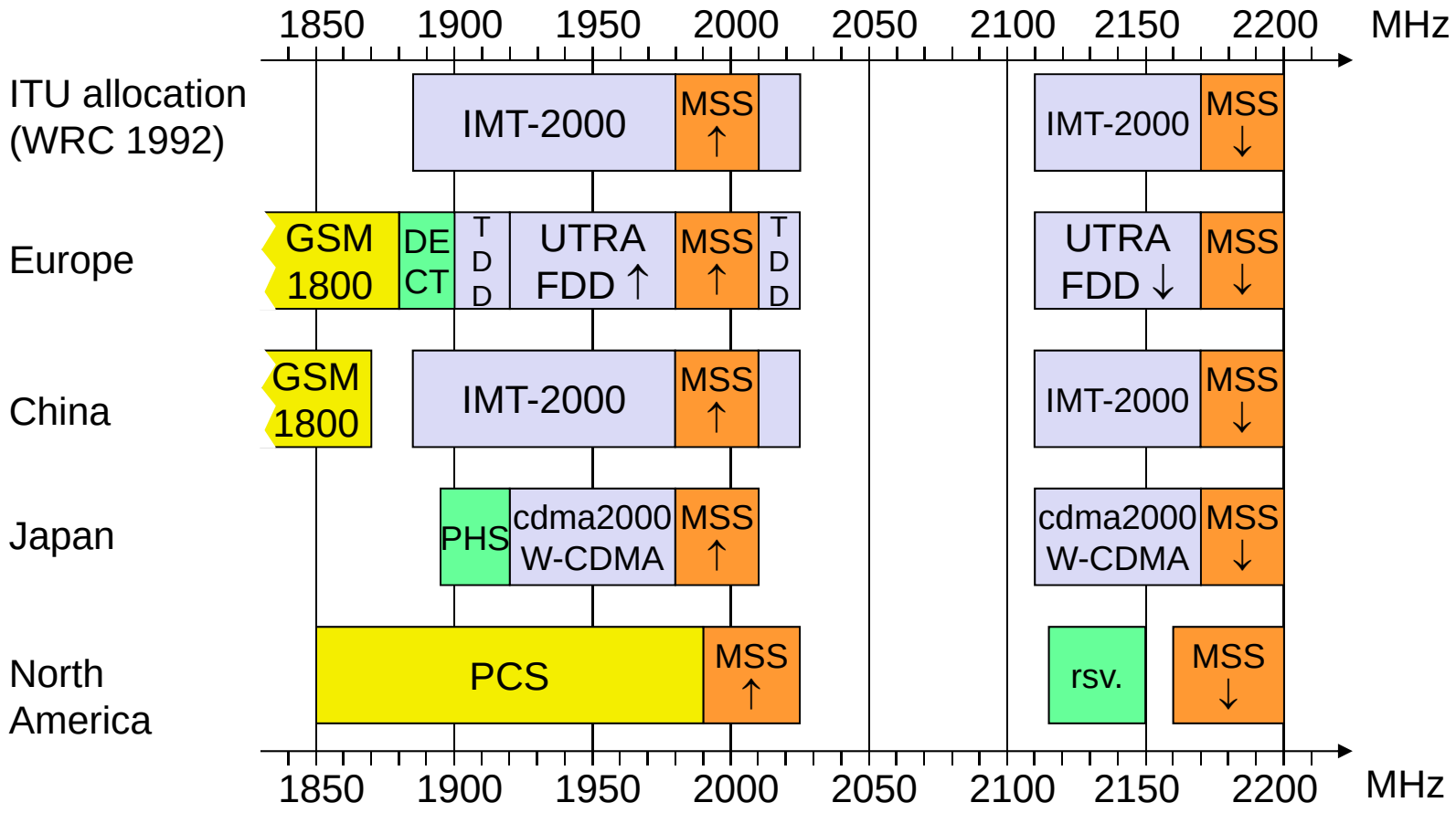
- First goal: **Personal communication, roaming without limitations**:
  - private network(s)
  - Pico (building) or Micro (regional) public cellular networks
  - Macro/Wide Area Network
  - Global world-wide satellite technology

- Second goal: **Consistent "Look and Feel"** independent of location and network
  - "Virtual Home Environment" VHE

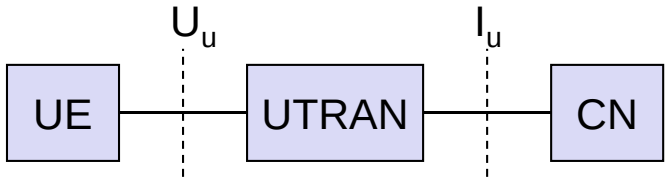
- Proposals for IMT-2000 (International Mobile Telecommunications)
  - UWC-136, cdma2000, WP-CDMA
  - UMTS (Universal Mobile Telecommunications System) from ETSI
- UMTS
  - UTRA (was: UMTS, now: Universal Terrestrial Radio Access)
  - enhancements of GSM
    - EDGE (Enhanced Data rates for GSM Evolution): GSM up to 384 kbit/s
    - CAMEL (Customized Application for Mobile Enhanced Logic)
    - VHE (virtual Home Environment)
  - fits into GMM (Global Multimedia Mobility) initiative from ETSI
  - requirements
    - min. 144 kbit/s rural (goal: 384 kbit/s)
    - min. 384 kbit/s suburban (goal: 512 kbit/s)
    - up to 2 Mbit/s urban

Frequencies for IMT-2000

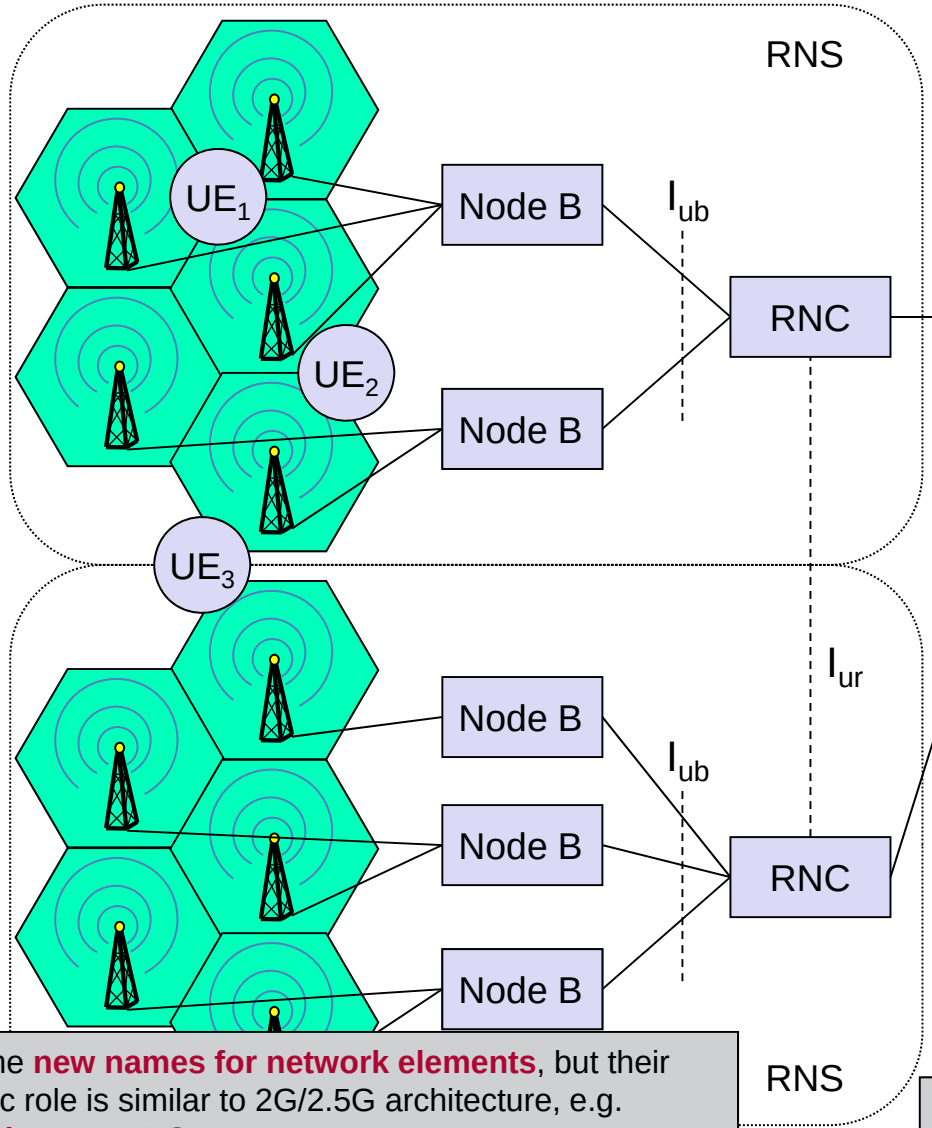
JS



- UTRAN (UTRA Network)
  - Cell level mobility
  - Radio Network Subsystem (RNS)
  - Encapsulation of all radio specific tasks
- UE (User Equipment)
- CN (Core Network)
  - Inter system handover
  - Location management if there is no dedicated connection between UE and UTRAN



(UTRAN = Universal Terrestrial Radio Access Network)



RNC: Radio Network Controller

RNS: Radio Network Subsystem

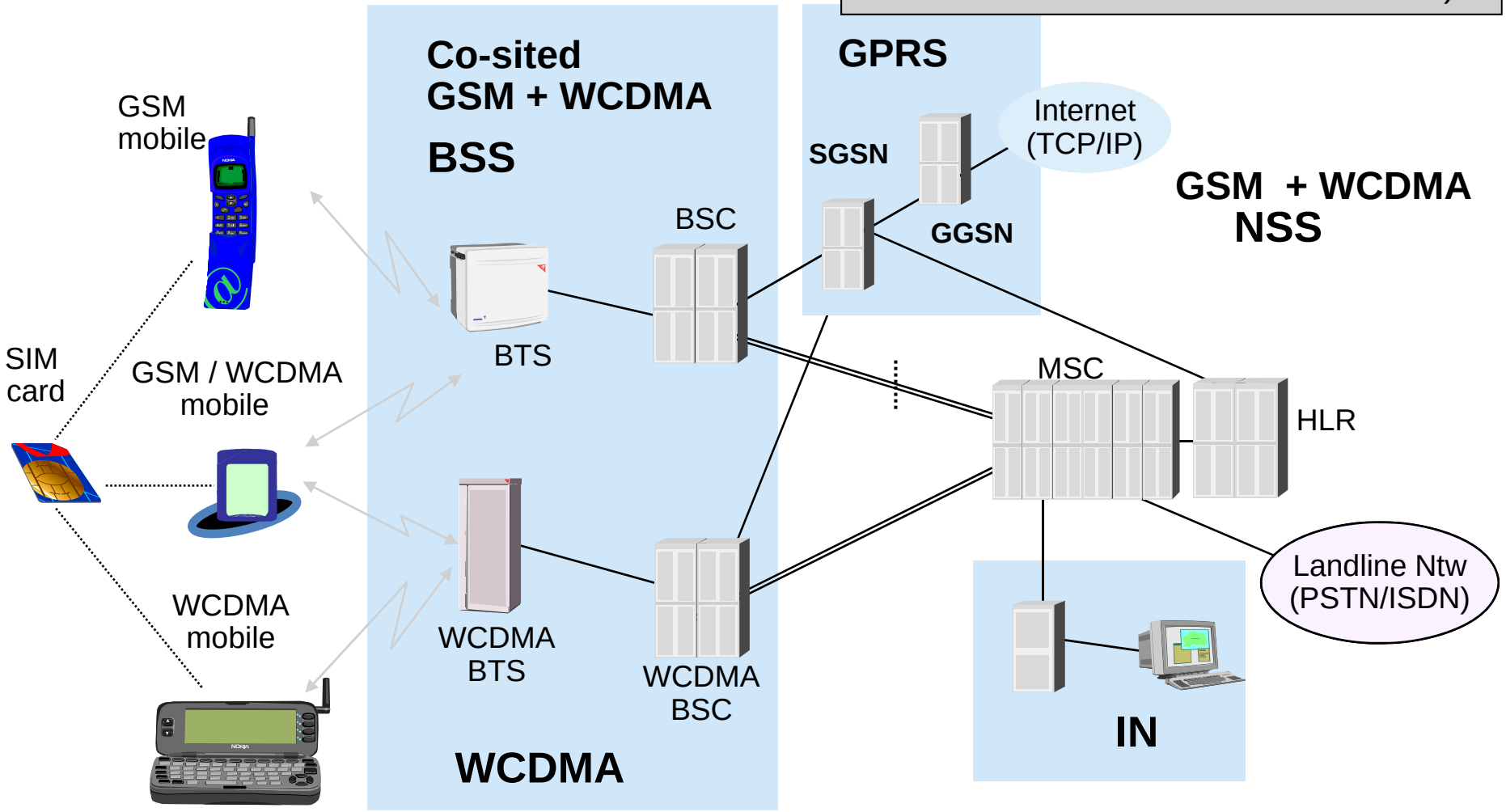
- UTRAN comprises several RNSs
- Node B can support FDD or TDD or both
- RNC is responsible for handover decisions requiring signalingto the UE
- Cell offers FDD or TDD

Some **new names for network elements**, but their basic role is similar to 2G/2.5G architecture, e.g.
„**Node B**“ as BTS,
„**RNC**“ as BSC,
„**RNS**“ as BSS, …

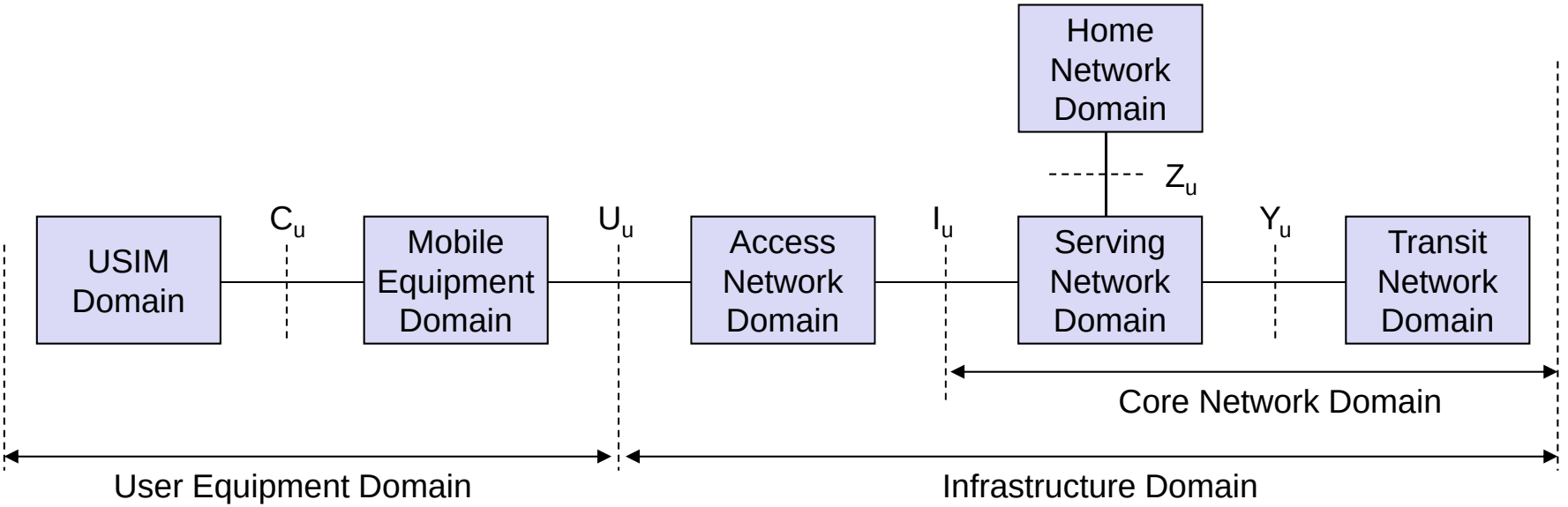
One **new interface**, the **I_{ur}** between RNCs, needed for macro diversity/soft handover

UMTS Architecture (2)

UMTS/WCDMA complementing the existing 2G/2.5G architecture
(in particular using core network for CS-services and GPRS backbone for data)



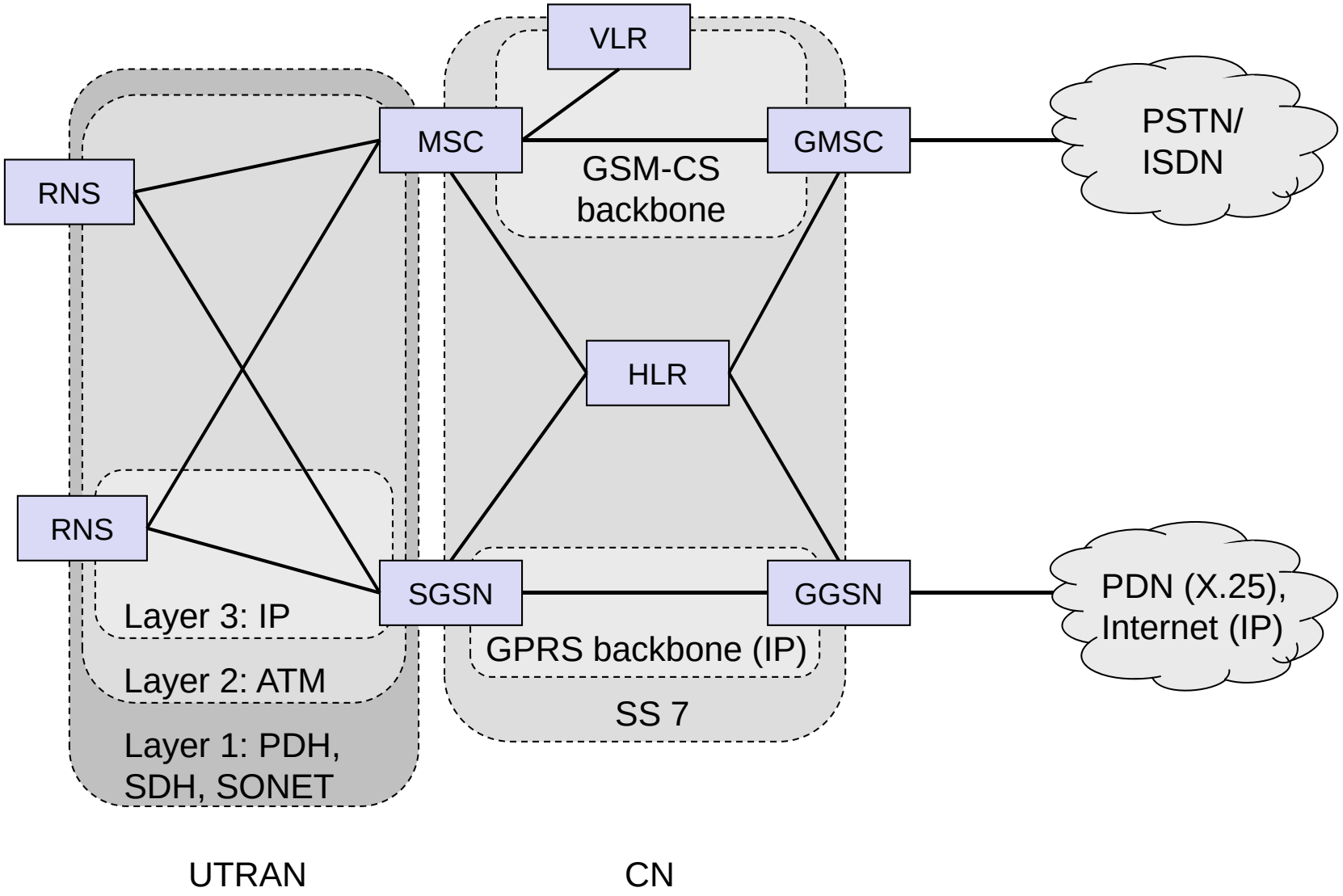
Multi-mode/Multi-band using several radio access network technologies.



- User Equipment Domain
  - Assigned to a single user in order to access UMTS services
- Infrastructure Domain
  - Shared among all users
  - Offers UMTS services to all accepted users

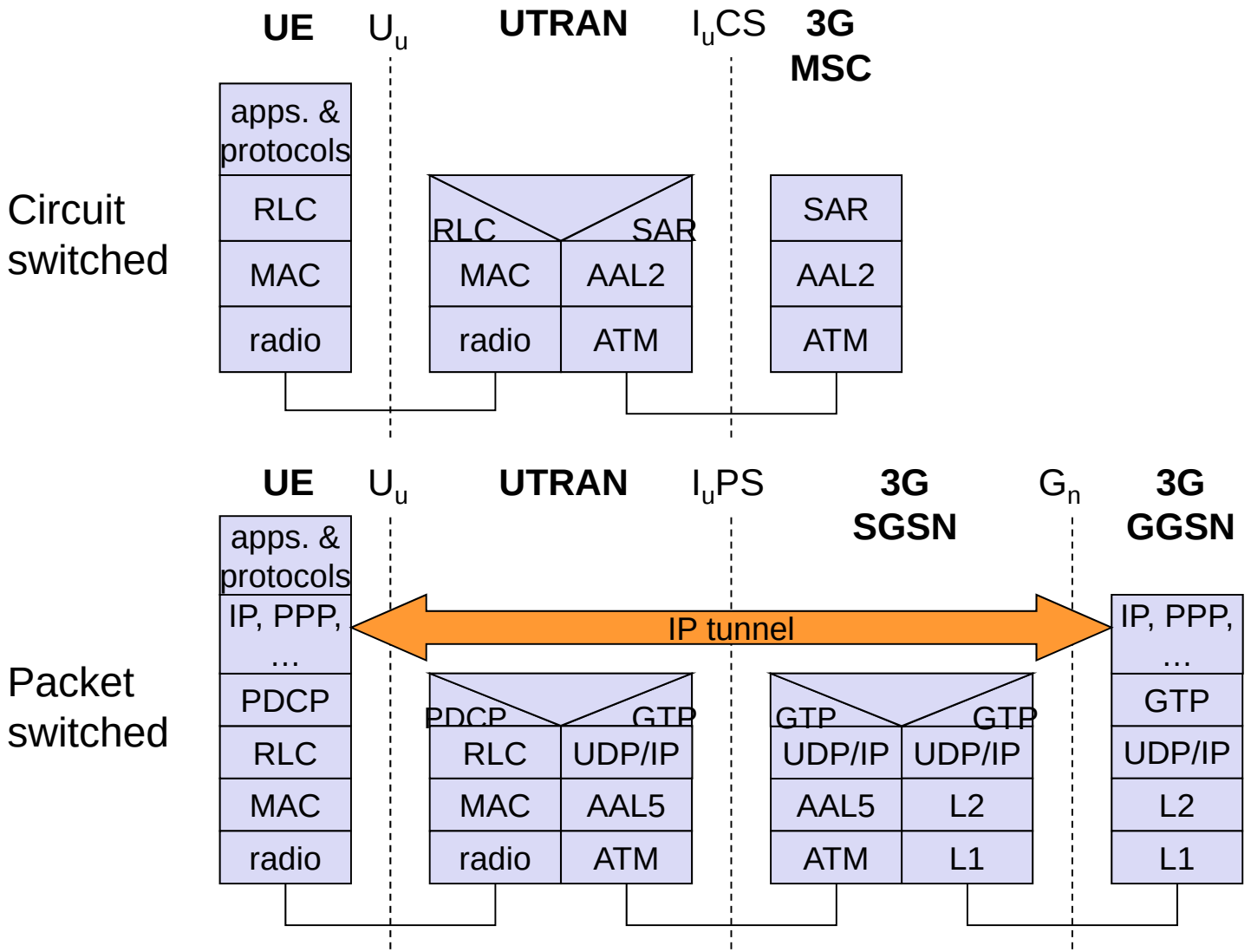
Core network: protocols

JS



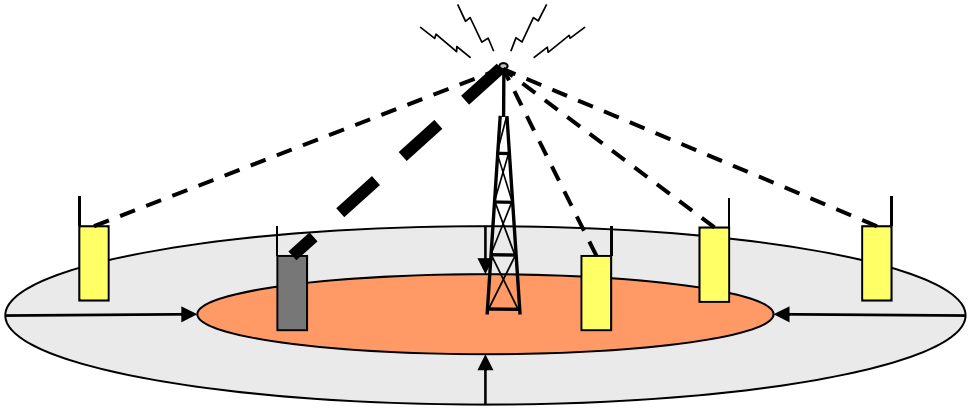
UMTS protocol stacks (user plane)

JS



Cell breathing

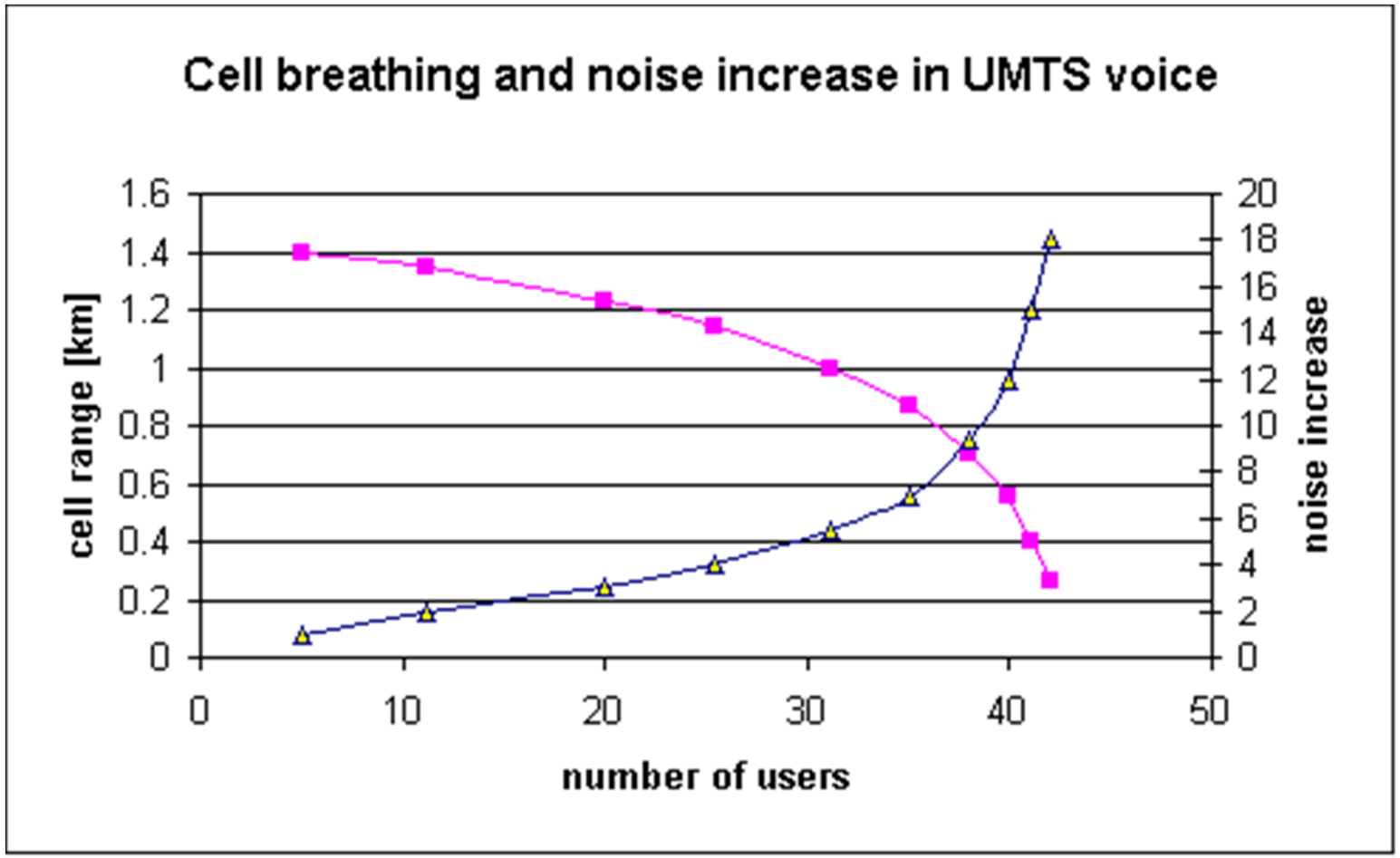
- CDM systems: cell size depends on current load
- Additional traffic appears as noise to other users
- If the noise level is too high users drop out of cells



- GSM
  - Mobile device gets exclusive signal from the base station
  - Number of devices in a cell does not influence cell size

- UMTS
  - Cell size is closely correlated to the cell capacity
  - Signal-to-noise ratio determines cell capacity
  - Noise is generated by interference from
    - other cells
    - other users of the same cell
  - Interference increases noise level
  - Devices at the edge of a cell cannot further increase their output power (max. power limit) and thus drop out of the cell
    ⇨ no more communication possible
  - Limitation of the max. number of users within a cell required
  - Cell breathing complicates network planning

Breathing Cells: Example



- GSM
  - **EMS/MMS**
    - EMS: 760 characters possible by chaining SMS, animated icons, ring tones, was soon replaced by MMS (or simply skipped)
    - MMS: transmission of images, video clips, audio
  - **EDGE (Enhanced Data Rates for Global [was: GSM] Evolution)**
    - 8-PSK instead of GMSK, up to 384 kbit/s
    - new modulation and coding schemes for GPRS ➔ EGPRS
      - MCS-1 to MCS-4 uses GMSK at rates 8.8/11.2/14.8/17.6 kbit/s
      - MCS-5 to MCS-9 uses 8-PSK at rates 22.4/29.6/44.8/54.4/59.2 kbit/s

Some current UMTS enhancements

JS

- **HSDPA (High-Speed Downlink Packet Access)**
  - initially up to 10 Mbit/s for the downlink, later > 20 Mbit/s using MIMO- (Multiple Input Multiple Output-) antennas
  - can use 16-QAM instead of QPSK (ideally > 13 Mbit/s)
  - user rates e.g. 3.6 or 7.2 Mbit/s
- **HSUPA (High-Speed Uplink Packet Access)**
  - initially up to 5 Mbit/s for the uplink
  - user rates e.g. 1.45 Mbit/s
- **HSPA+ (Evolved HSPA)**
  - Rel-7/Rel-8/Rel-9/…
  - Downlink 28/42/84/> 100 Mbit/s
  - Uplink 11/23/>23 Mbit/s
  - 2x2 MIMO, 64 QAM
- **Dual-/Multi-Carrier HSPA (DC-/MC-HSPA)**
  - Connect 2 (Rel-8/9) or more carriers (Rel-11) e.g. of two cells offering up to 672 Mbit/s (4x4 MIMO)

- Initiated in 2004, focus on enhancing the Universal Terrestrial Radio Access (UTRA) and optimizing 3GPP's radio access architecture.
- Targets: **Downlink 100 Mbit/s, uplink 50 Mbit/s**

- Downlink: **OFDM, QPSK, 16QAM, and 64QAM**
- Uplink: **SC-FDMA, BPSK, QPSK, 8PSK and 16QAM**
- Channel bandwidths between 1.25 and 20 MHz
- 4 x Increased Spectral Efficiency, 10 x Users Per Cell (**MIMO**), **reduced RTT**
- **FDD and TDD** supported, **co-existence with earlier 3GPP** standards incl. handover
- Core network: System Architecture Evolution (SAE), optimizing it for packet mode and in particular for the IP-Multimedia Subsystem (IMS)

Long Term Evolution (LTE)

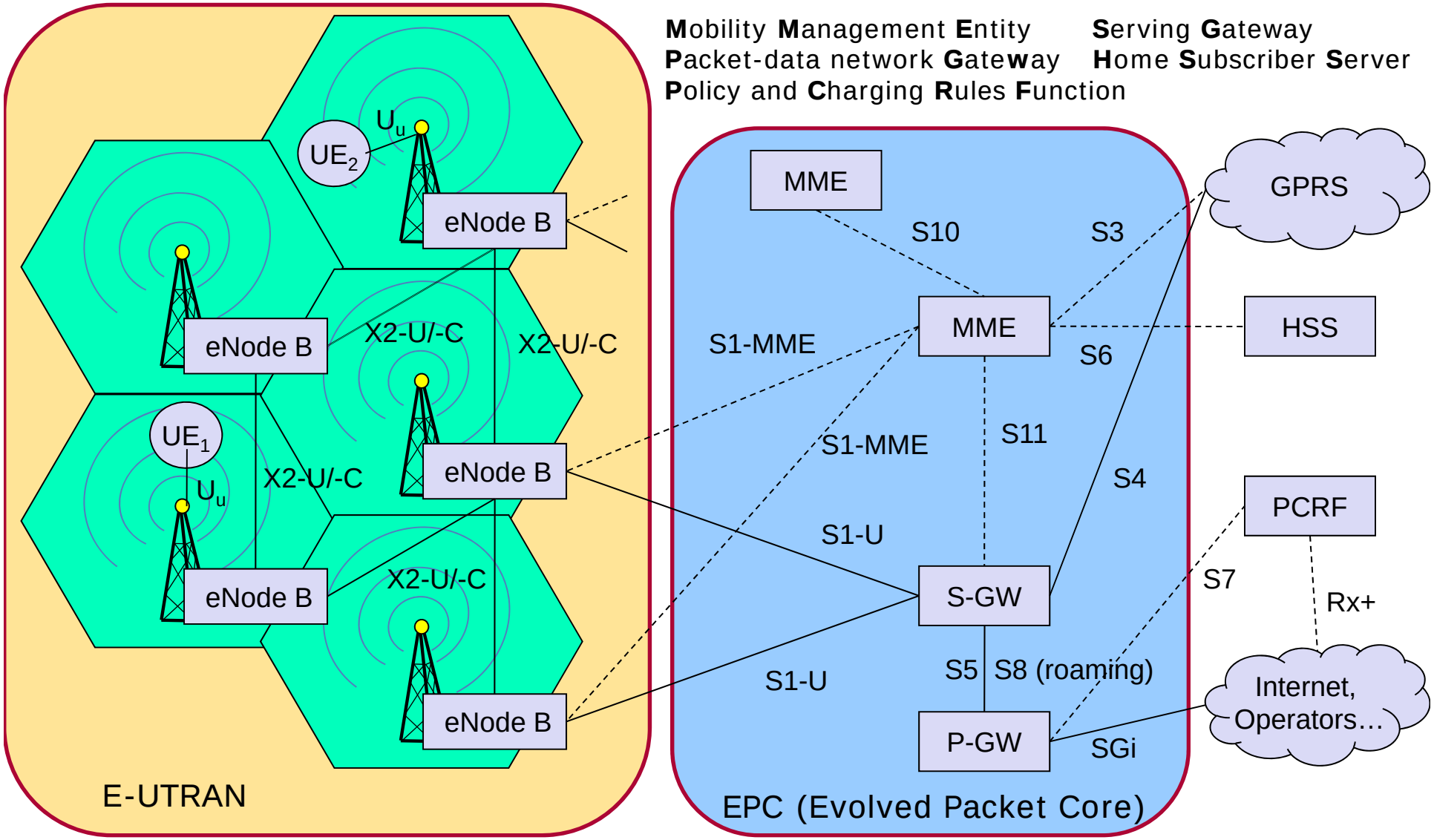
- 2007: E UTRA progressed from the feasibility study stage to the first issue of approved Technical Specifications
- 2008: stable for commercial implementation.

- 2009: first public LTE service available (Stockholm and Oslo)
- 2010: LTE starts in Germany

- LTE is not 4G – sometimes called **3.9G**
  - Does not fulfill all requirements for IMT advanced

Key LTE features

- **Simplified network architecture** compared to GSM/UMTS
  - Flat **IP-based network** replacing the GPRS core,
  - optimized for the IP-Multimedia Subsystem (IMS),
  - no more circuit switching
- Network should be in parts self-organizing
- Scheme for **soft frequency reuse** between cells
  - Inner part uses all subbands with less power
  - Outer part uses pre-served subbands with higher power
- Much **higher data throughput** supported by multiple antennas
- Much **higher flexibility** in terms of spectrum, bandwidth, data rates
- Much **lower RTT** – good for interactive traffic and gaming
- Smooth transition from W-CDMA/HSPA, TD-SCDMA and cdma2000 1x EV-DO – but completely different radio!



IMT Advanced – from www.itu.int

JS

- Key features of ´IMT-Advanced´ a high degree of commonality of functionality worldwide while retaining the flexibility to support a wide range of services and applications in a cost efficient manner;
- compatibility of services within IMT and with fixed networks;
- capability of interworking with other radio access systems;
- high quality mobile services;
- user equipment suitable for worldwide use;
- user-friendly applications, services and equipment;
- worldwide roaming capability; and,
- enhanced peak data rates to support advanced services and applications (**100 Mbit/s for high and 1 Gbit/s for low mobility** were established as targets for research).
- These features enable IMT-Advanced to address evolving user needs and the capabilities of IMT-Advanced systems are being continuously enhanced in line with user trends and technology developments.

- GSM – UMTS - LTE
  - LTE advanced as candidate for IMT-advanced
- Worldwide functionality & roaming
- Compatibility of services
- Interworking with other radio access systems
- Enhanced peak data rates to support advanced services and applications (100 Mbit/s for high and 1 Gbit/s for low mobility)
- 3GPP will be contributing to the ITU-R towards the development of IMT-Advanced via its proposal for LTE-Advanced.
- Relay Nodes to increase coverage
- 100 MHz bandwidth (5x LTE with 20 MHz)

- first LTE advanced devices available since 2014
  - e.g., Samsung Galaxy S5 LTE+ (LTE-Advanced up to 300 MBit/s Downstream)
- LTE base stations just need a software update