

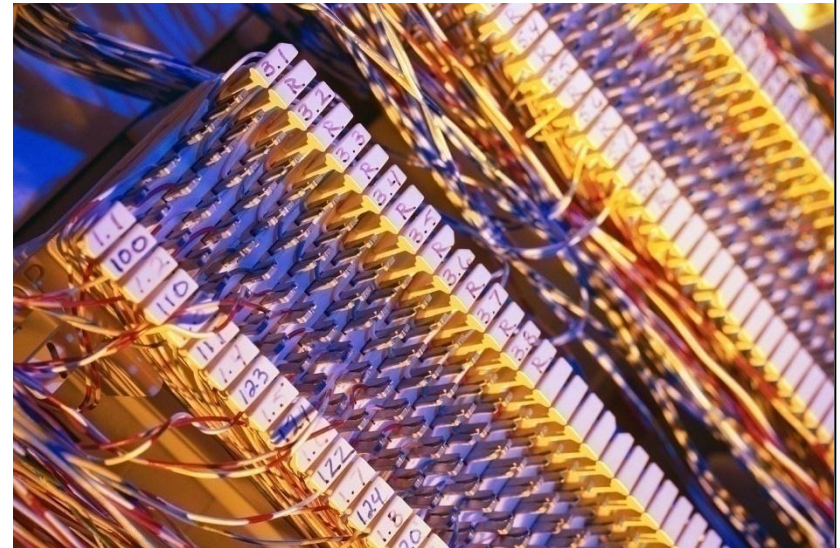
Lecture 2

Mobile Telecommunications
Infrastructures

Mobile Business I (WS 2011/12)

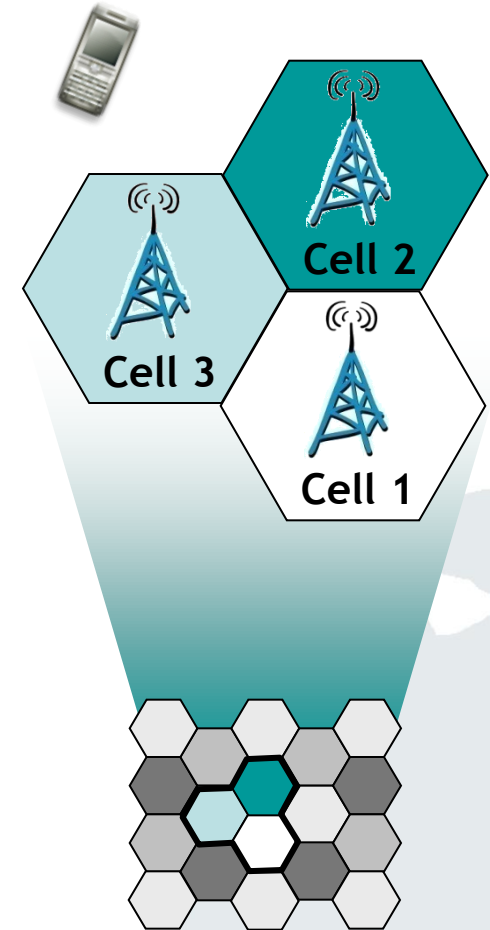
Prof. Dr. Kai Rannenberg

T-Mobile Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.



- Cell Based Communication (CBC)
 - Introduction
 - Basic Technology (Cells, Multiplexing)
- Mobile Telecommunication Infrastructures
 - Introduction
 - GSM (Technology, Authentication, Location Management) (2G)
 - UMTS (3G)
 - Long Term Evolution (3.9G, 4G)
- Roaming

- Cellular networks are radio networks consisting of several transmitters.
- Each transmitter or base station, covers a certain area ➔ *a cell*.
- Cell radii can vary from tens of meters to several kilometres.
- The shape of a cell is influenced by the environment (buildings, etc) and usually neither hexagonal nor a perfect circle, even though this is the usual way of drawing them.



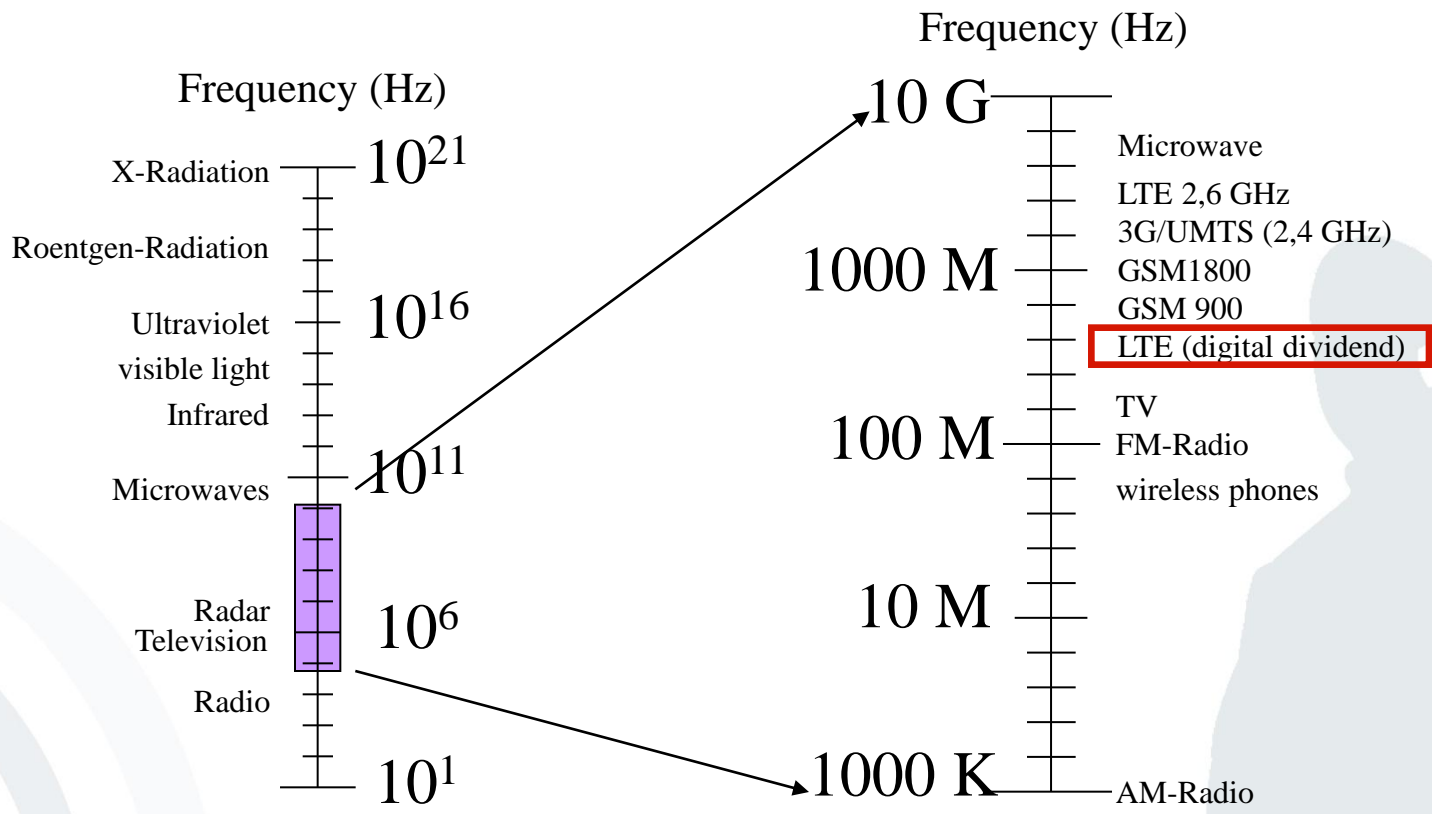
- Cellular networks offer a number of advantages compared to alternative solutions:
 - **Higher capacity:** Cells offer the possibility to “reuse” the transmission frequencies assigned to mobile devices (e.g. by multiplexing). In order to do so, the networks need a thorough planning of the position of base stations and their frequencies.
 - ➔ More users can use the infrastructure
 - **Reduced transmission power:** Reduced power usage for the mobile device, due to the fact that only a limited amount of transmission power is needed in a small cell, compared to a far away base station.
 - ➔ Reduced power consumption for mobile devices

- Cellular networks offer a number of advantages over alternative solutions:
 - **Robustness:** Cellular systems are decentralised with regard to their base stations. In the case that one antenna fails, only a small area gets affected.
 - ➔ Failure of one base station does not affect the complete infrastructure
 - **Better coverage:** Cells can be adapted to geographic conditions (mountains, buildings, etc.).
 - ➔ Better availability of the infrastructure

- However, there are also some drawbacks of cell based communication infrastructures :
 - **Required infrastructure:** A complex and costly infrastructure is required, in order to link all base stations. This includes switches, antennas, location registers, etc.
 - **Handover needed:** When changing from one cell to another, a handover mechanism is needed that allows a change of cells in real-time. These mechanisms are complex.
 - **Frequency planning:** The distribution of the frequencies being used for the base stations needs to be planned carefully, in order to minimise interferences, etc.

- Fundamental mechanism in communication system
- Describes how several users can share a medium (e.g. mobile network) with minimum or no interference.
- **Goal:** Most efficient usage of a medium
- **Abstract example:** Traffic (users) using a highway with several lanes (medium) without accidents (interference)

Frequency range of instruments of entertainment and communication electronics



- Cell Based Communication (CBC)
 - Introduction
 - Basic Technology (Cells, Multiplexing)
- Mobile Telecommunication Infrastructures
 - Introduction
 - GSM (Technology, Authentication, Location Management) (2G)
 - UMTS (3G)
 - Long Term Evolution (3.9G, 4G)
- Roaming

- **1st Generation (1G) - Analogue networks**
- **2nd Generation (2G) - GSM networks**
Global System for Mobile Communications
- **3rd Generation (3G/3.5G) - UMTS/HSPA/HSPA+**
Universal Mobile Telecommunications System
High Speed Packet Access / Evolved HSPA = HSPA+
- **3.9G or 4G - LTE**
Long Term Evolution
- **4th Generation (4G) - LTE Advanced**

Evolution of mobile telecommunication infrastructures

2G – GSM

3.9G/4G – LTE

1G

3G – UMTS

4G – LTE Advanced (2012)

- **1st mobile radio network in Germany: “A-Netz”**
 - Started in 1958 - decommissioned in 1977
 - Analogue network (Manual switching of calls, frequency range 150 MHz)
 - Price of terminal: 8.000-15.000 DM
 - For a call, the caller has to know the location of the callee (range from 30 to 50 km radius).
- **2nd mobile radio network in Germany: “B-Netz”**
 - Started in 1972 – decommissioned in 1994
 - Analogue network (Automatic dial switching by area code)
 - Caller needs to know the area code of callee
 - Terminal prices comparable with those of the A-Network

- ***3rd mobile radio network in Germany: “C-Netz”***
 - Started in 1985 – decommissioned in 2000
 - Analogue network
 - First ***cell based*** mobile radio system in Germany
 - The change of cells happens automatically by distance measuring to the nearest base station
 - The net can automatically detect the place of the call partner by use of a Home Location Register (HLR)
 - Uniform (location independent) area code “0161” for all participants
 - Telephone number is not allocated to the terminal but to the smart card (later: SIM)
 - Peak in 1993 with 850.000 participants

- In 1991, the first GSM (2G) network (“D-Netze”) started in a test run in Germany.
- By introducing the worldwide GSM-standards and roaming agreements among mobile operators cross-border mobile communication became possible.
- In 2003 the first *UMTS* (3G) networks became available.

- First digital mobile radio network with high voice quality and reliability (roaming)
- Global diffusion in more than 212 countries with more than 1 billion users.
- In February 2004 the first commercial mobile radio network (based on GSM) was launched in Iraq.
- GSM is the basis of data services like GPRS and EGDE.



[Sauter 2008]

- Third-generation (3G) mobile phone technology
- Provides high data transfer rates for multimedia communication services
- Germany's UMTS frequency licenses were sold by auction in 2000 for approx. 50bn €.
- Commercially available in Germany since 2004
- UMTS/3G is the underlying network and the basis of the data services HSPA and HSPA+.



[Sauter 2008]



2009-12-14:

- First Long Term Evolution Networks (3.9G/4G) became commercially available in Stockholm and Oslo

April and May 2010:

- the **digital dividend** frequency spectrum auctioned in Germany (4.4 bn €) for
 - use in Long Term Evolution Networks (3.9G/4G)
 - improving broadband coverage

- **LTE:** 100 Mbit/s downlink and 50 Mbit/s uplink speed is possible with the existing LTE technology (LTE-Release 8 User Equipment Category 3).
- **LTE Advanced (from ~2012)** will be backward compatible with LTE, the same frequency band is used
- **LTE Advanced** will make use of the frequency spectrum more efficiently, resulting in higher data rates (above 100 Mbit/s, towards 1 Gbit/s).
- Like GSM and UMTS/HSPA technologies, **LTE** and **LTE Advanced** are developed by the 3rd Generation Partnership Project (3GPP).



<http://www.3gpp.org/LTE>



<http://www.3gpp.org/LTE-Advanced>



	GSM	UMTS (WCDMA)	CDMA	PDC	TDMA
1997	<i>71,20</i>				
1998	<i>138,40</i>				
1999	<i>258,20</i>				
2000	<i>455,10</i>		<i>82,20</i>	<i>50,80</i>	<i>65,20</i>
2001	<i>636,40</i>		<i>110,00</i>	<i>52,90</i>	<i>90,00</i>
2002	<i>809,30</i>	<i>0,20</i>	<i>140,50</i>	<i>56,10</i>	<i>101,10</i>
2003	<i>1.012,00</i>	<i>2,80</i>	<i>183,60</i>	<i>58,10</i>	<i>100,10</i>
2004	<i>1.296,00</i>	<i>16,30</i>	<i>231,60</i>	<i>54,20</i>	<i>90,00</i>
2005	<i>1.709,20</i>	<i>50,00</i>	<i>296,70</i>	<i>46,30</i>	<i>48,50</i>
2006	<i>1.941,60</i>	<i>74,70</i>	<i>296,50</i>	<i>38,50</i>	<i>26,10</i>
Q1/2007	<i>2.278,10</i>	<i>114,70</i>	<i>290,00</i>	<i>27,90</i>	<i>16,20</i>
Q2/2009	<i>3.450,41</i>	<i>388,92</i>	<i>441,24</i>	<i>2,74</i>	<i>1,48</i>

* In Million subscribers [Source: Chair of Mobile Business 2007, Data: GSM2009]

- Cell Based Communication (CBC)
 - Introduction
 - Basic Technology (Cells, Multiplexing)
- Mobile Telecommunication Infrastructures
 - Introduction
 - GSM (Technology, Authentication, Location Management) (2G)
 - UMTS (3G)
 - Long Term Evolution (3.9G, 4G)
- Roaming

- Abbreviation for **Global System for Mobile Communications (GSM)**



- Originally 1982 driven by “*Groupe Spéciale Mobile*” in order to create a cross national standard contrary to national analogue standards

- European standard by *ETSI* (European Telecommunications Standardisation Institute). ETSI is a partner in the 3rd Generation Partnership Project (3GPP).



- Worldwide adoption of the standard in more than *212 countries and territories* (most successful mobile radio system up to now)
- Thus, worldwide roaming among different mobile network operators became possible.

■ GSM-Services

■ Carrier services

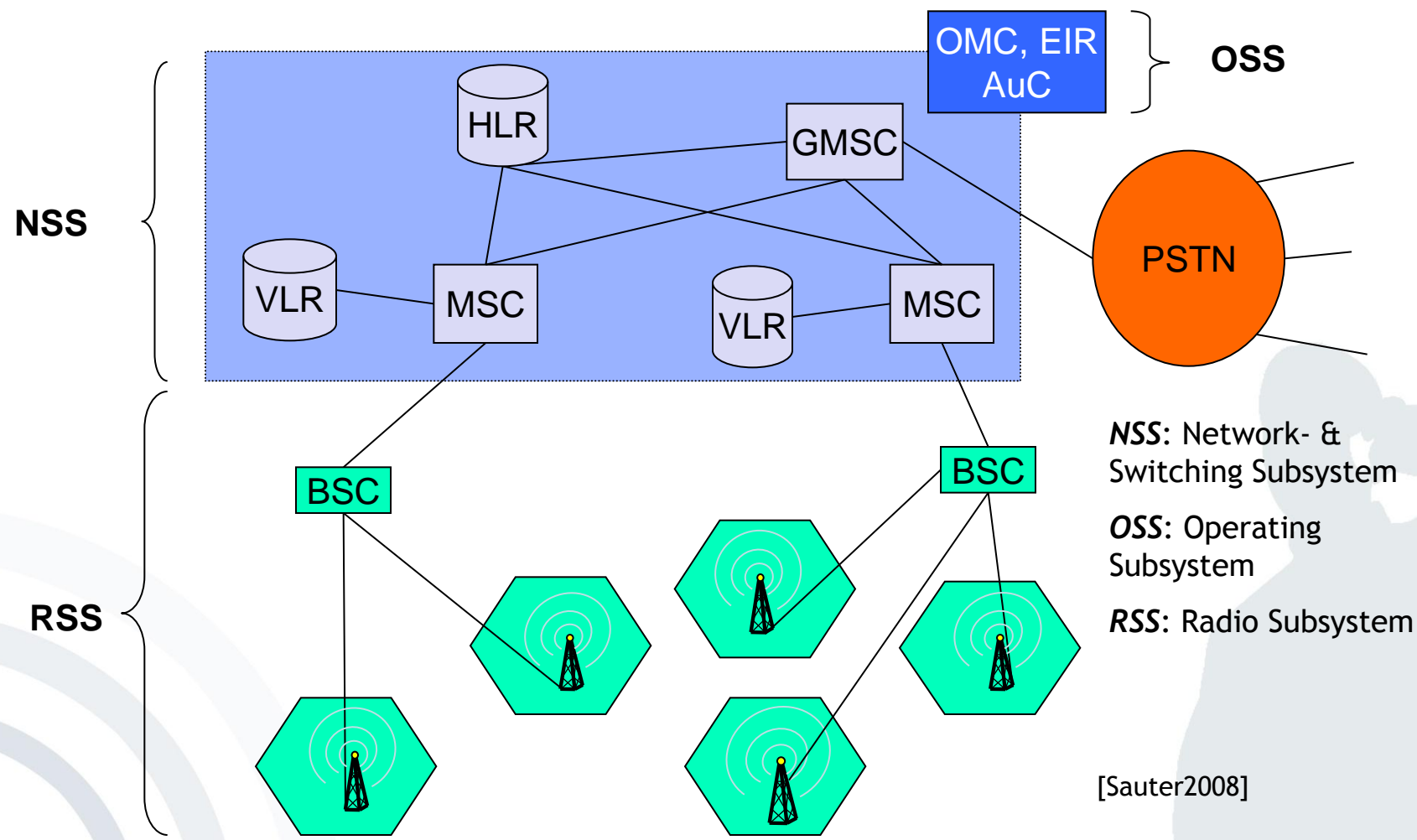
- Services to transfer signals over the GSM network
- The focus of GSM standardization was on voice services

■ Telecommunications services

- Telecommunication services (mainly voice) support the mobile communications among users
- Telecommunication services play a central role in the GSM standard

■ Supplementary services

- GSM provides a number of supplementary services (specific to network operators), such as caller ID, call redirect, closed user groups (e.g. company-internal network or GSM-R), Teleconference (up to 7 participants).



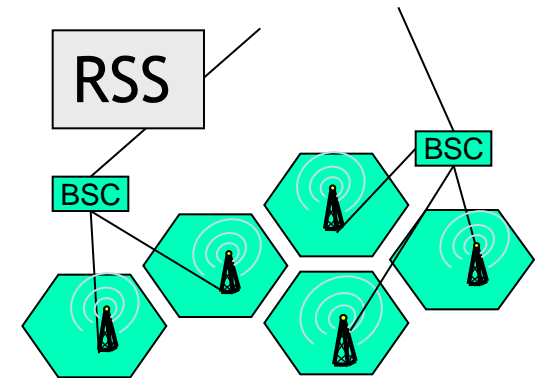
NSS: Network- & Switching Subsystem
OSS: Operating Subsystem
RSS: Radio Subsystem

[Sauter2008]

- **Radio Subsystem (RSS)**
 - System consisting of radio
 - Specific components

- **Components:**

- **Mobile Station (MS):** System of mobile terminal & SIM
- **Base Transceiver Station (BTS):** Radio facility for signal transfer. A BTS serves one GSM cell (~100m to ~30km radius).
- **Base Station Controller (BSC):** Administrates affiliated BTS and supervises e.g. frequency allocation and connection handover between cells.

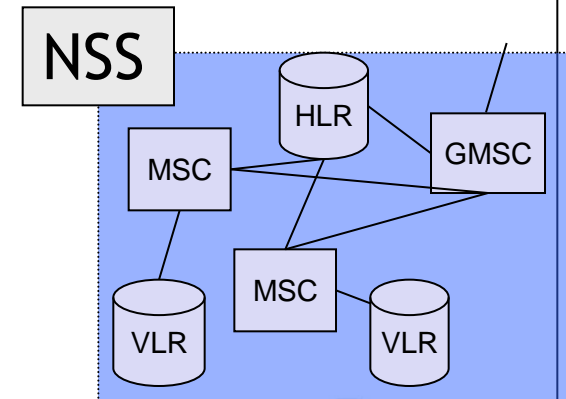


- **Network & Switching Subsystem (NSS)**

- Connects radio network with conventional networks
- Locates subscribers and monitors change of location

- **Components:**

- **Mobile Switching Centre (MSC):** Switching centre for initiation, termination and handover of connections
- **Home Location Register (HLR):** Central data base with subscribers' data (telephone numbers, keys, locations)
- **Visitor Location Register (VLR):** Data base assigned to every MSC with data of active subscribers in the MSC's range (HLR fraction copy).



- **Operation Subsystem (OSS)**

- Supervises operation and maintenance of the whole GSM network

OSS

OMC, EIR
AuC

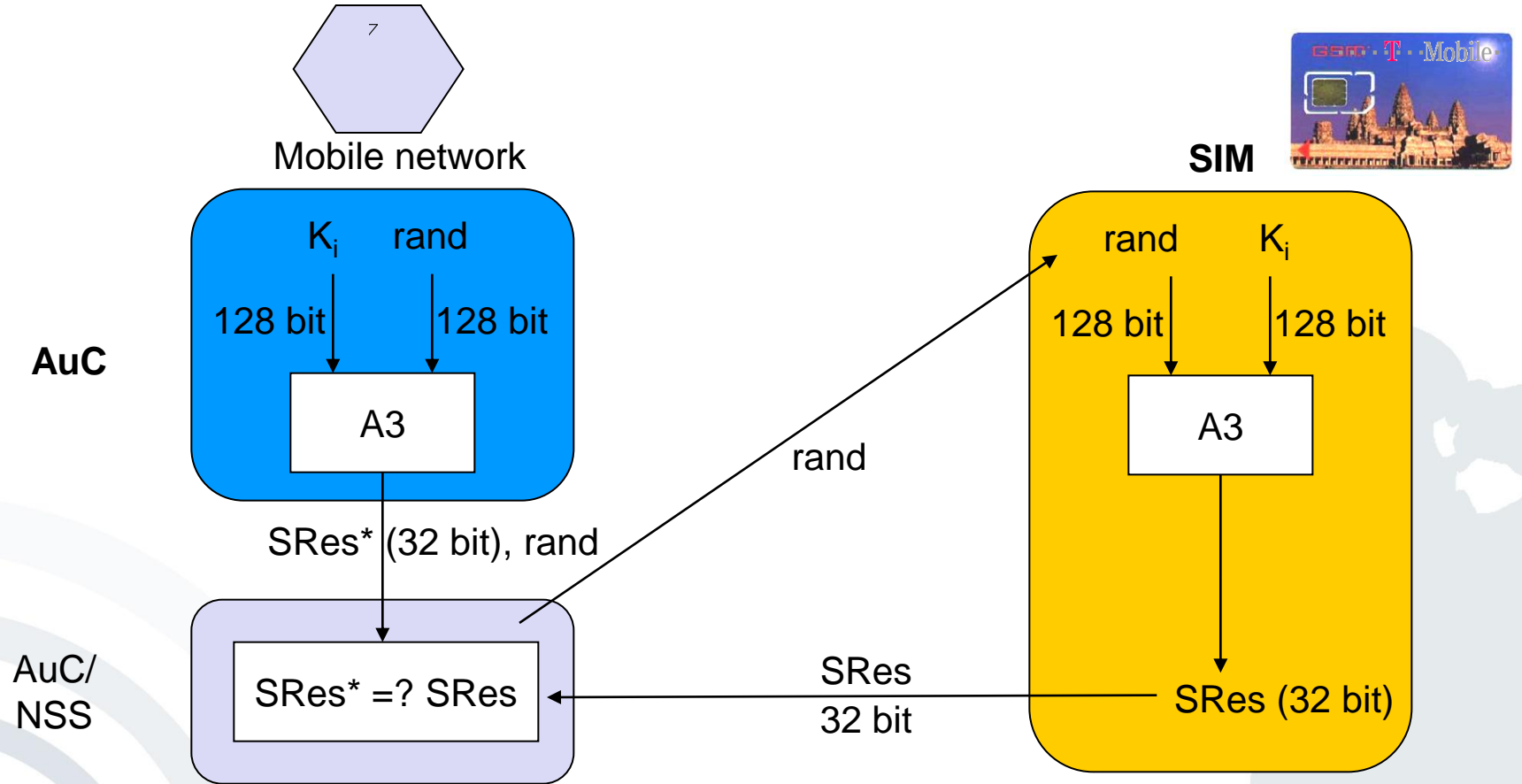
- **Components:**

- **Operation and Maintenance Centre (OMC):** Supervises each network component and creates status reports
- **Authentication Centre (AuC):** protects identity of participants & data transmission, administrates keys
- **Equipment Identity Register (EIR):** data base with identification list for devices, e.g. stolen terminals (whitelist, greylist, blacklist)

The GSM system offers different “security services“:

- **Access control and authentication:**
 - Authentication of the subscriber to the SIM by input of a PIN and to the GSM network by Challenge-Response-Procedure
- **Confidentiality:**
 - Data & voice transferred between mobile station and BTS are encrypted.
- **(Partial) Anonymity:**
 - No transfer of data which can identify the subscriber via radio, instead temporary identification
 - (Temporary Mobile Subscriber ID, TMSI)

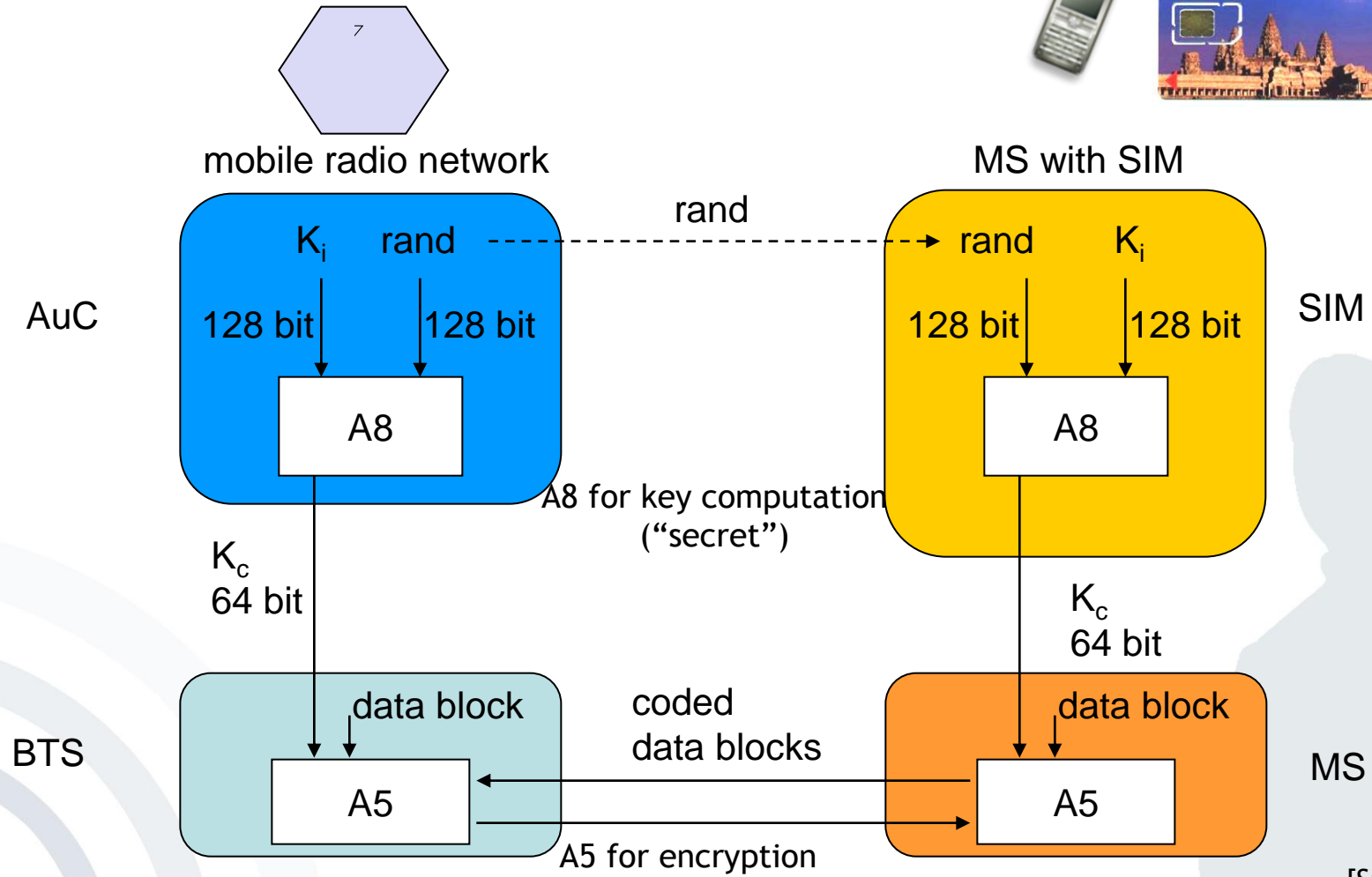
- Challenge response protocol



K_i : individual subscriber authentication key
 A3: („secret“) authentication algorithm

SRes: signed response

- Challenge-Response-Procedure (Subscriber Authentication)
Authentication is based on the individual key K_i , the subscriber identification IMSI and a secret algorithm A3.
- K_i and A3 are stored on the SIM and deposited in the AuC.
 1. AuC creates random number *rand*.
 2. AuC encrypts *rand* and K_i via A3 (->SRes*).
 3. AuC transfers *rand* and SRes* to VLR.
 4. VLR transfers exclusively *rand* to SIM.
 5. SIM computes with “own” K_i and A3 Signed Response SRes.
 6. The SRES computed by the SIM is transmitted to the VLR and is compared with SRES*.
 7. If SRES* and SRES are equal the subscriber is authenticated successfully.



- **GSM provides encryption of voice and data transferred via the air interface:**
 1. AuC creates random number rand.
 2. AuC generates the key K_c for the encryption of the transferred data via rand, K_i and A8.
 3. VLR transfers only rand to SIM.
 4. SIM computes the key K_c using A8, the rand received and the local K_i
 5. Mobile station and mobile radio network use generated K_c and algorithm A5 for encryption and decryption of sent and received data.

- Partial Anonymity:
 - In order to guarantee the anonymity of the users temporary user identification (TMSI) is used.
 - Temporary user identification is updated automatically from time to time or on demand.
 - Data which identify users are not transferred.
 - **Example:** Anonymous charging is (technically) possible via prepaid card.

- Solely authentication of the terminal/subscriber toward the GSM network. The network does not authenticate itself.
 - Assumption that the network is trustworthy per se
 - Security model was developed at a time with a provider monopoly
- Subscriber localization is almost exclusively controlled by the network.
 - Centralized movement tracking is possible
 - In order to avoid localization the subscriber must switch off the terminal.

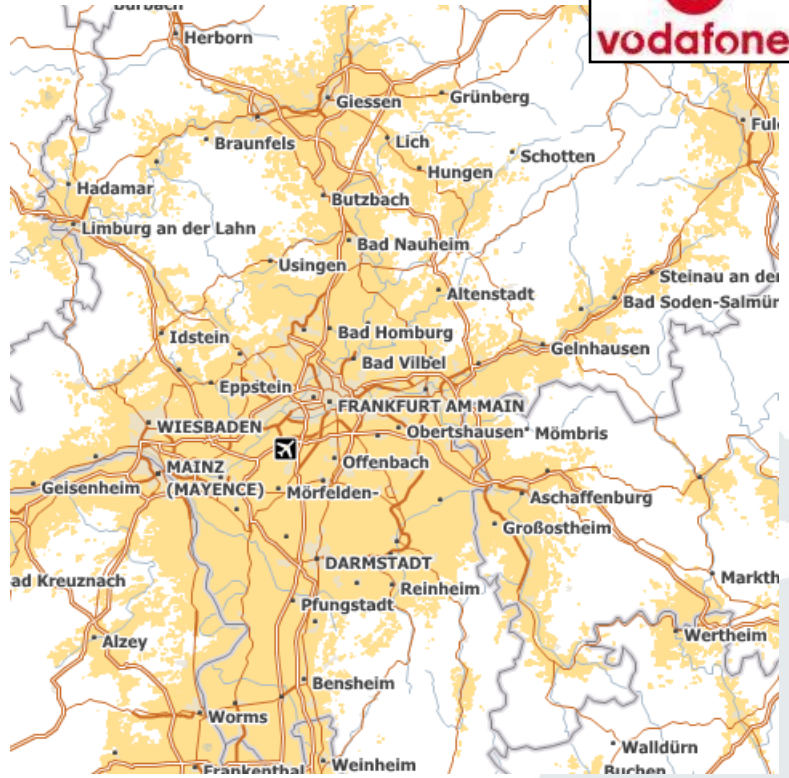
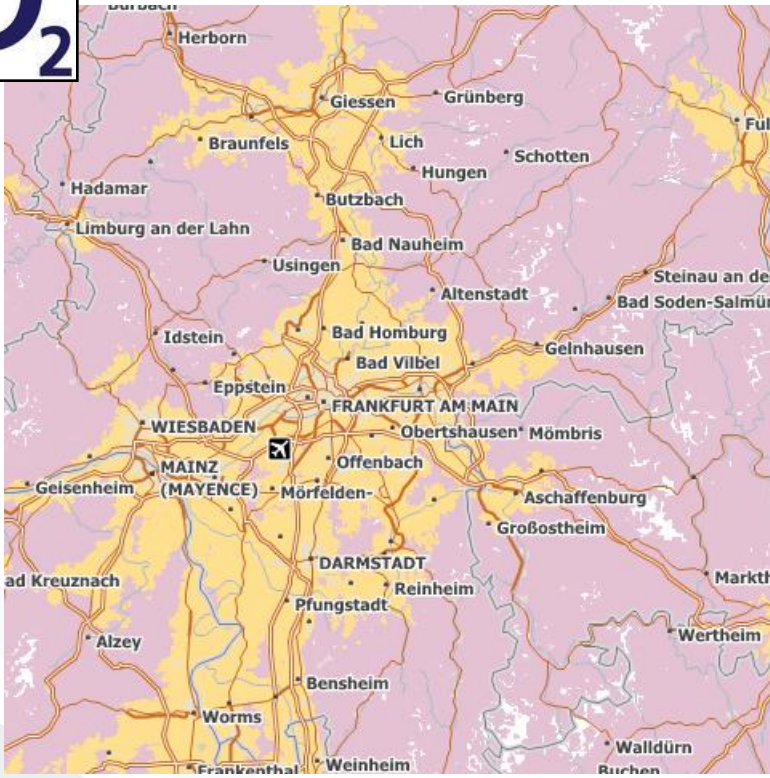
- Security model bases partly on secret encryption algorithms.
 - A3 and A8 were published without authorization.
 - Some operators use non-standardized algorithms.
- No encryption from terminal to terminal but solely over the air interface
 - Encryption deactivation by the network possible, without notification of the users
- Encryption comparatively “weak” because of key length (64 bit)
 - Sometimes the real key length is shorter.

- Cell Based Communication (CBC)
 - Introduction
 - Basic Technology (Cells, Multiplexing)
- Mobile Telecommunication Infrastructures
 - Introduction
 - GSM (Technology, Authentication, Location Management) (2G)
 - UMTS (3G)
 - Long Term Evolution (3.9G, 4G)
- Roaming

- Universal Mobile Telecommunications System (UMTS):
 - **Status of 2G-Networks:** Different standards in some different continents avoid worldwide roaming
 - **Demand for 3G-Networks:** Globally uniform standard

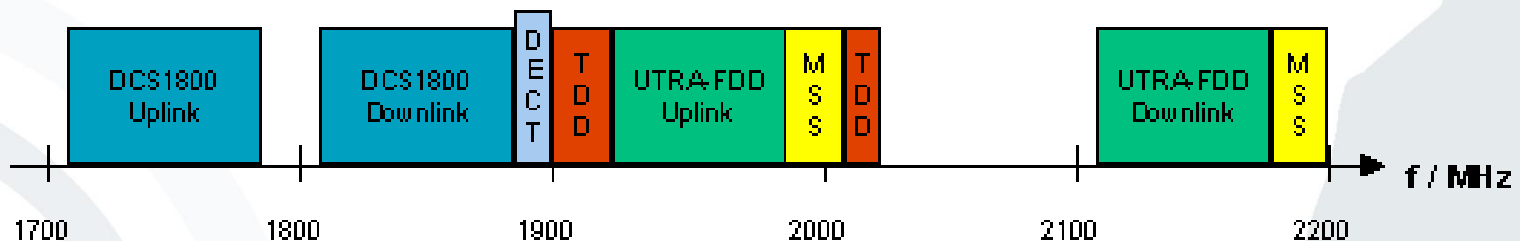
➔ Voting of regional & national regulation offices (e.g. ETSI, ARIB, ANSI) via the International Telecommunication Union (ITU)





[GSM2010]

- **Common approach:**
Worldwide reservation of frequencies in the 2GHz range
- **Problem of competing targets:**
 - Existing national networks and installed network technique shall preferably be transferred into the new standard.
 - ➔ The specification of 3G-Networks, introduced by the ITU, leaves room for national, partly incompatible implementations.
- UMTS (UTRA-FDD/TDD) frequency allocation in Europe:



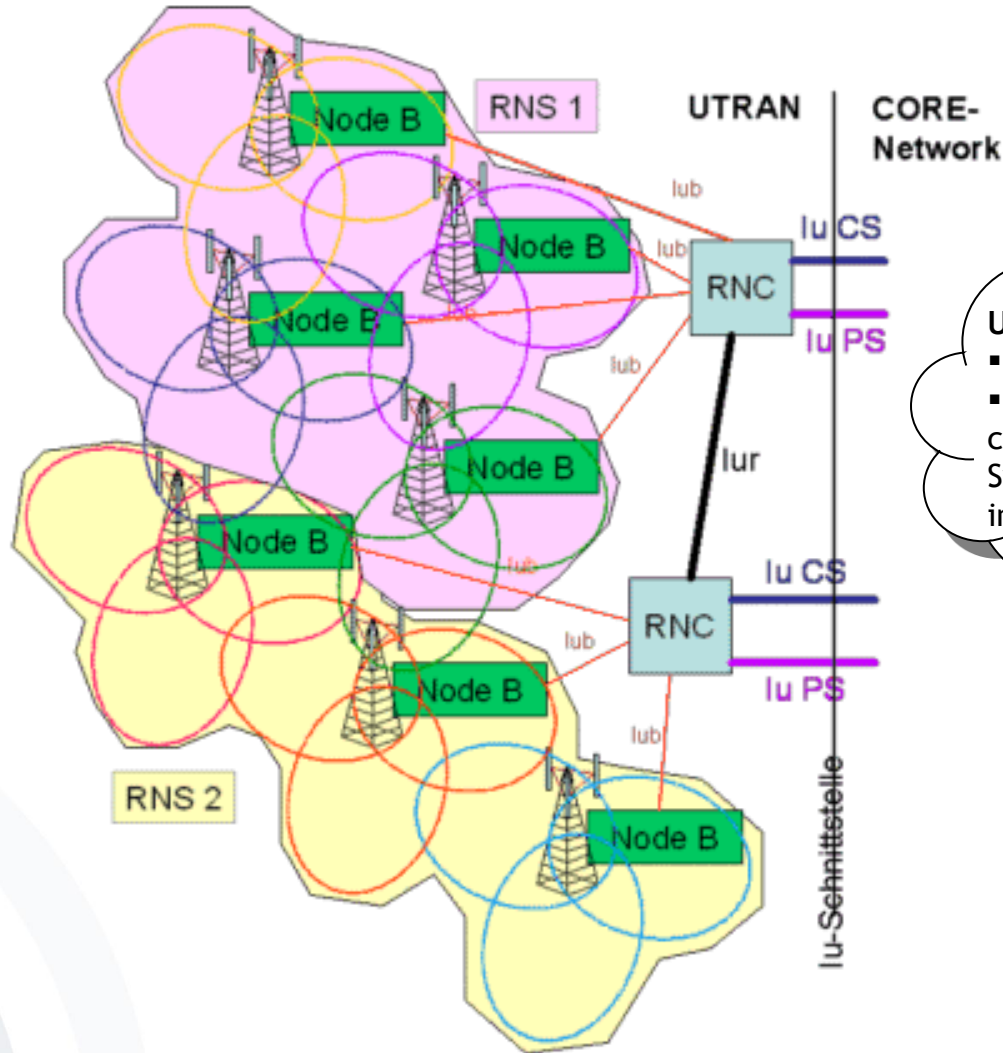
© 2001 UMTSlink.at

UTRA-FDD: UMTS Terrestrial Radio Access - Frequency Division Duplex

[UMTSLink2006]

UMTS (3G) System Architecture

- **UTRAN:**
UMTS
Terrestrial
Radio Access
Network
- **RNS:** Radio
Network
Subsystem
- **RNC:** Radio
Network
Controller
(controls the
Node Bs)
- **Node B:**
UMTS base
stations
(equivalent
to base
transceiver
stations
(BTS) in GSM)



UMTS Core network

- is not shown here in detail
- UMTS Core network corresponds to Network- & Switching Subsystem (NSS) in GSM

- 3G UMTS/HSPA/HSPA+ bandwidths
 - UMTS: 384 kbit/s downlink/uplink
 - High Speed Packet Access (HSPA) provides higher data speeds for downlink and uplink, e.g.
 - 7.2 or 14.0 Mbit/s downlink speed (HSDPA)
 - 1.4 or 5.7 Mbit/s uplink speed (HSUPA).
 - Evolved HSPA (HSPA+) using either *Multiple Input Multiple Output (MIMO)* or *Dual-Cell* technology provides
 - downlink speeds of e.g. 21,1 or 42,2 Mbit/s and
 - a maximum uplink speed of 11.5 Mbit/s.
 - But: Available bandwidth per user decreases if terminal is moving or if there are many participants in one radio cell.
- ➔ Bandwidths enable multimedia services

- UMTS complements the security mechanisms known by GSM:
 - Enhanced participant authentication (EMSI)
 - Network authentication
 - Integrity protection of data traffic
 - Transferred security keys are also encrypted in the fixed network (e.g. HLR-VLR)
 - Increased key length
 - End-to-End encryption is possible.

- The UMTS standard includes the following features:
 - Quality of Service (QoS) for data services
 - Multilateral Security (with regard to authentication)
 - Virtual Home Environment (VHE)
 - High Speed Downlink Packet Access (HSDPA)
 - ...
- However, not all of these features that have been standardised are actually implemented in existing networks, as they are optional and can be added on demand.

- Cell Based Communication (CBC)
 - Introduction
 - Basic Technology (Cells, Multiplexing)
- Mobile Telecommunication Infrastructures
 - Introduction
 - GSM (Technology, Authentication, Location Management) (2G)
 - UMTS (3G)
 - Long Term Evolution (3.9G, 4G)
- Roaming

- **Long Term Evolution (3.9G, 4G)** allows for 100 Mbit/s downlink and 50 Mbit/s uplink speed
 - LTE was originally not named a “4G network” due to stricter naming requirements.
 - The technology can be named either 3.9G or 4G network today.
- **LTE Advanced (4G)** will make use of the frequency spectrum more efficiently, resulting in higher data rates (above 100 Mbit/s, towards 1 Gbit/s).



<http://www.3gpp.org/LTE>

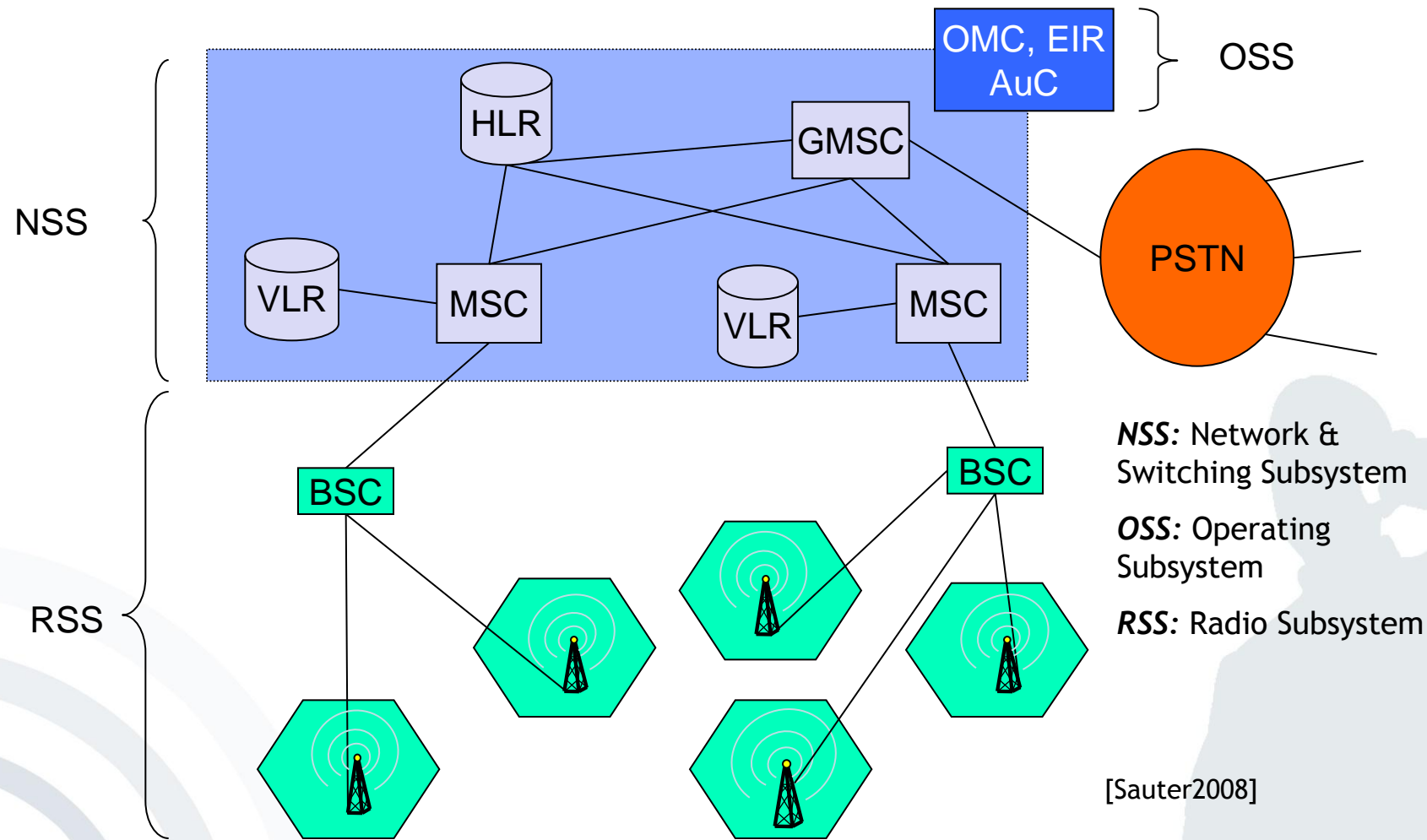


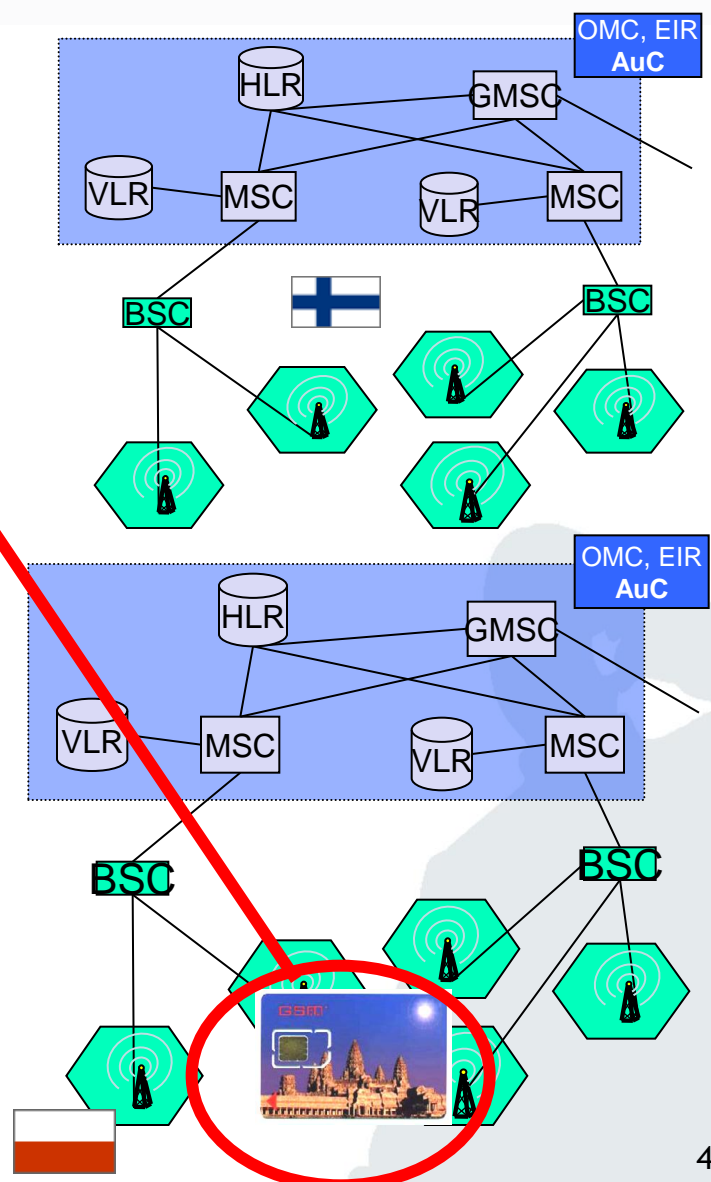
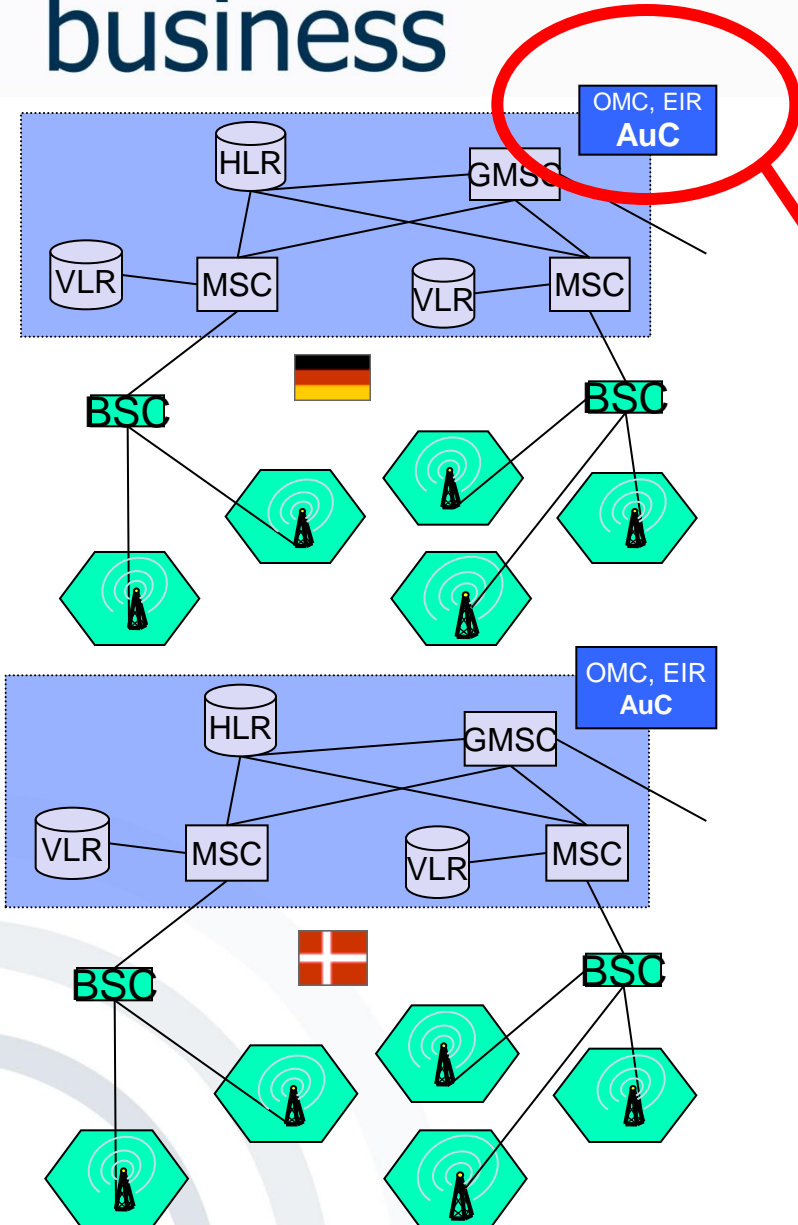
<http://www.3gpp.org/LTE-Advanced>

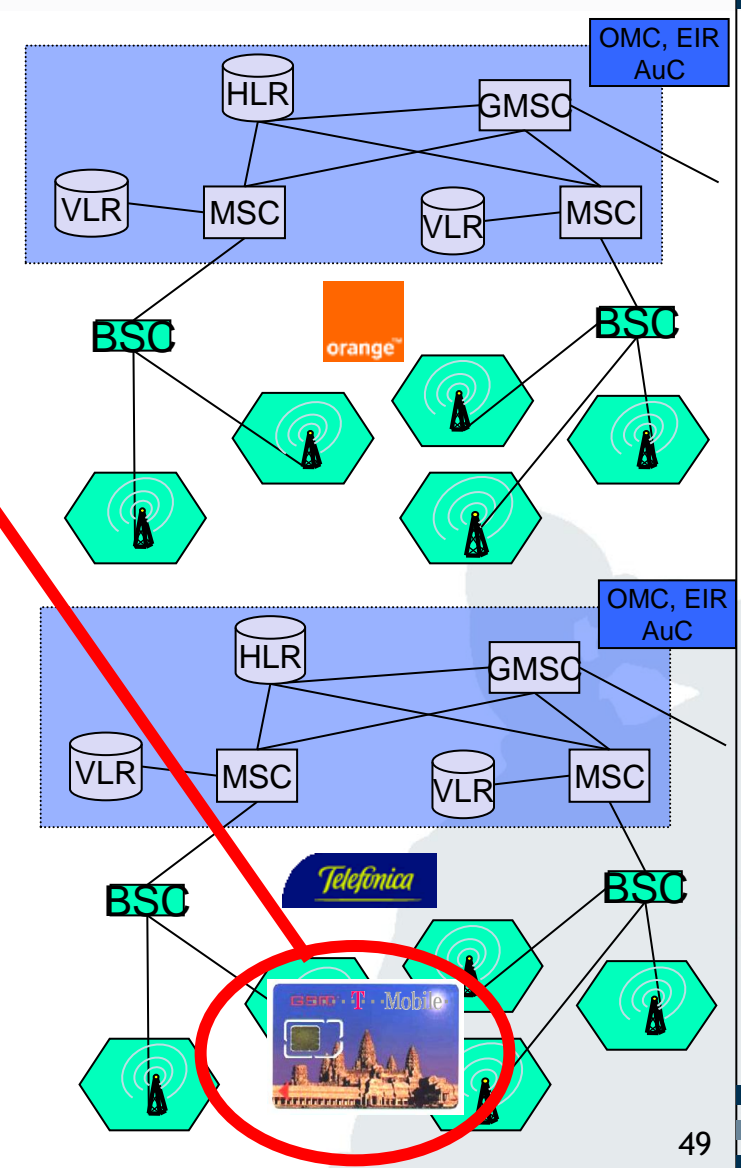
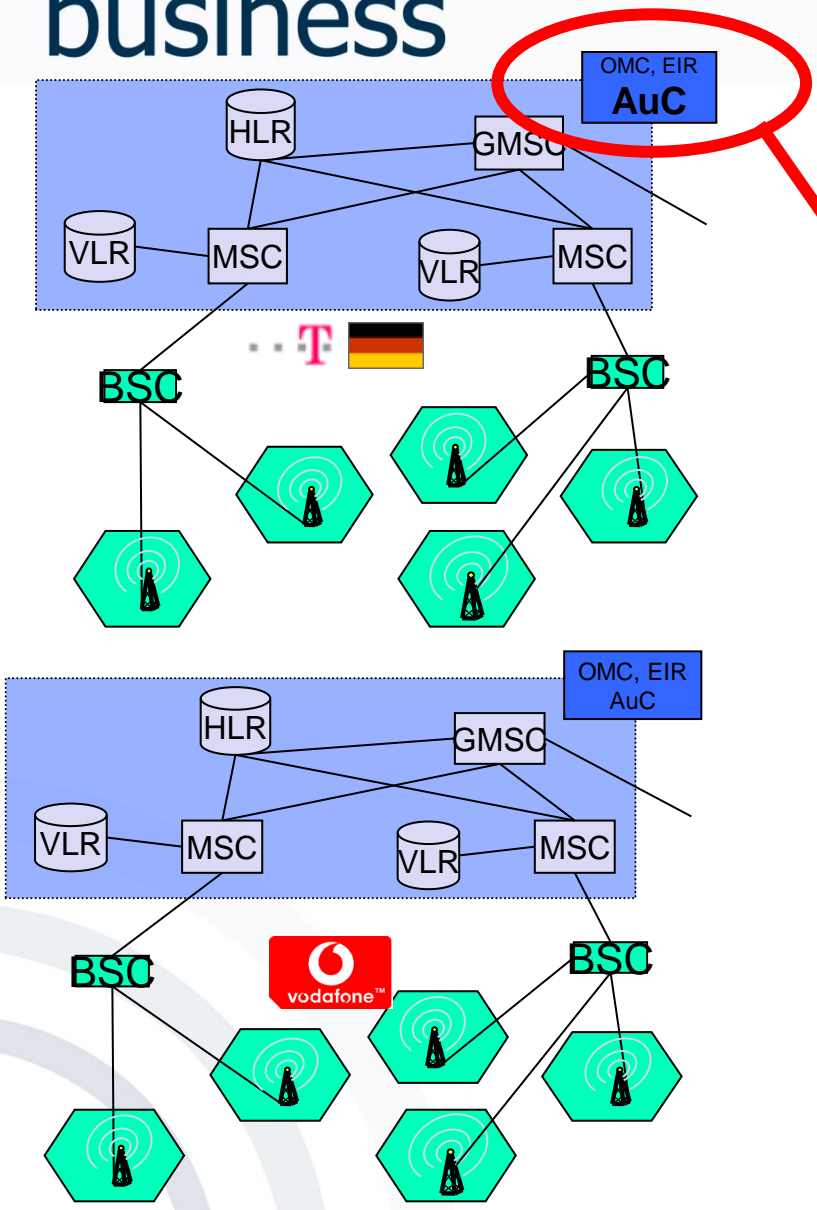
- Cell Based Communication (CBC)
 - Introduction
 - Basic Technology (Cells, Multiplexing)
- Mobile Telecommunication Infrastructures
 - Introduction
 - GSM (Technology, Authentication, Location Management) (2G)
 - UMTS (3G)
 - Long Term Evolution (3.9G, 4G)
- Roaming

- Roaming denotes a change of network access, e.g.:
 - Change of the GSM network operator
 - Change between different network systems (UMTS, GSM, WLAN, CDMA, PDC)
 - Cell change within the GSM system (Handover)
- Roaming usually means extensive changes, e.g. of the network technique or the network operator, and with a new authentication:
 - **Example:** The mobile device automatically logs into an available WLAN when a hotspot is entered (e.g. airport, conferences).

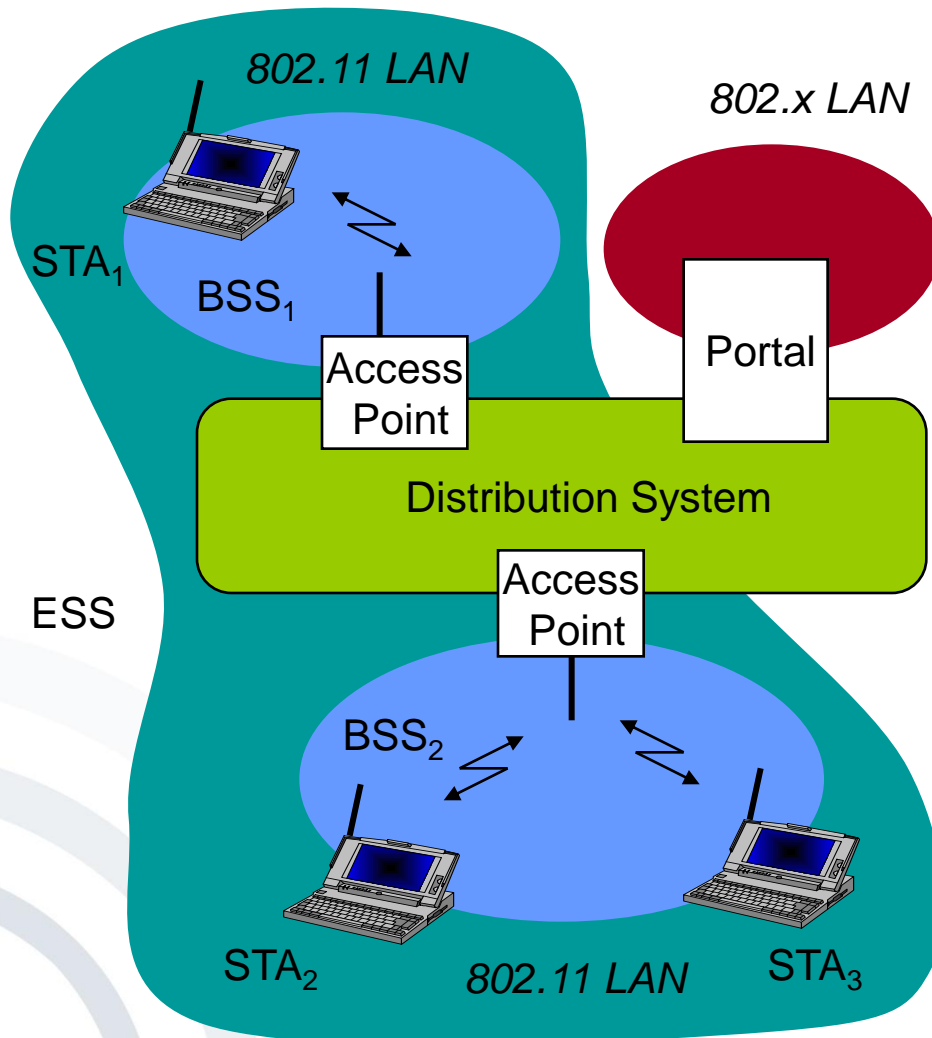
- If a user of a mobile device moves from one cell to another cell, the connection handover should be as smooth as possible.
- GSM manages the handover between radio cells in the range of 100 ms; this implies a short connection interruption.
- The reason for the interruption is, among others, an update of the VLR.







- No existing standard for “roaming” between:
 - Access points (AP)
 - Different providers of APs
- Change of AP leads to
 - Connection-interrupt
 - New connection/authentication
 - Non-uniform accounting / user administration



Station (STA)

- Computer with access to the wireless medium and therefore contact to the AP

Basic Service Set (BSS)

- Group of stations, which use the same radio frequency

Access Point (AP)

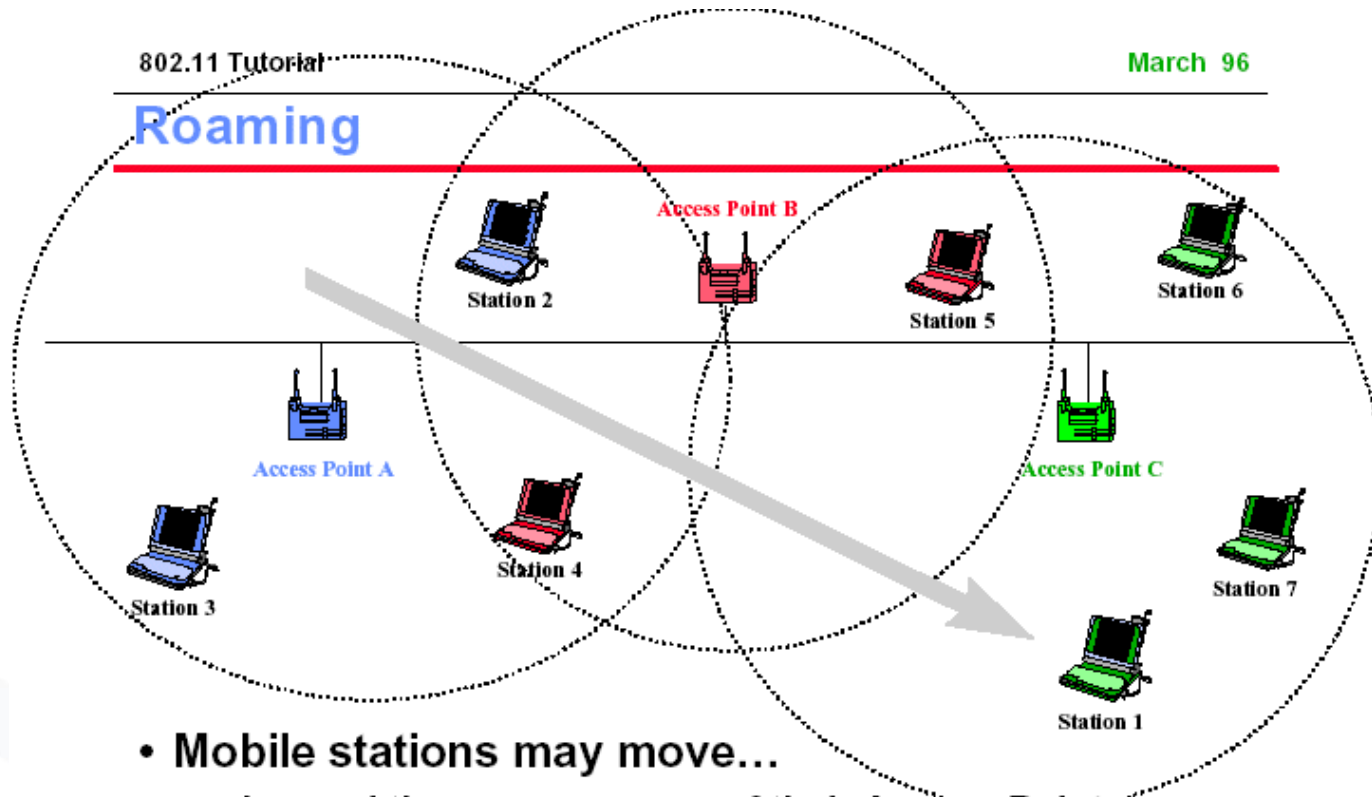
- Station which is integrated into the radio as well as the fixed local area network (distribution system)

Portal

- Transfer into another network

Distribution systems

- Connection of different cells for building up a larger network (EES: Extended Service Set)



- **Mobile stations may move...**
 - beyond the coverage area of their Access Point
 - but within range of another Access Point
- **Reassociation allows station to continue operation**

- By connecting multiple access points via a so called distribution-system, the transmission range could be expanded.
- Each access point provides one cell.
- A station scans for available access points and tries to log on when leaving a cell.
- Distribution-system and “former“ access point get information after successful log in.

- [3gtech.info 2010] 3gtech.info (2010): Defining 4G (I mean IMT-Advanced), <http://www.3gtech.info/tag/imt-advanced-4g-regulatory-requirements>, accessed 2010-10-10.
- [BITKOM2005] BITKOM (2005), UMTS Subscribers 2005, www.bitkom.org/de/markt_statistik/38511_38543.aspx, accessed 2006-10-13.
- [GSM2009] GSM Association (2009), Market Data Summary (Q2 2009) - Connections by Bearer Technology, http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm, accessed 2010-10-10.
- [GSM2010] GSM Association (2010), GSM Coverage Maps, <http://www.mobileworldlive.com/coverage.asp>, accessed 2010-10-10.
- [Royer2006] Royer, D. (ed.) (2006): FIDIS Deliverable D11.1, available online at <http://www.fidis.net/resources/deliverables/mobility-and-identity/int-d111000/>
- [Sauter2008] Sauter, M. (2008): Grundkurs Mobile Kommunikationssysteme (3., erweiterte Auflage), Vieweg, Wiesbaden.
- [UMTSLink2006] UMTSlink, www.umtslink.at, accessed 2006-10-13.