Mobile Communications

Semester B, Mandatory modules, ECTS Units: 3

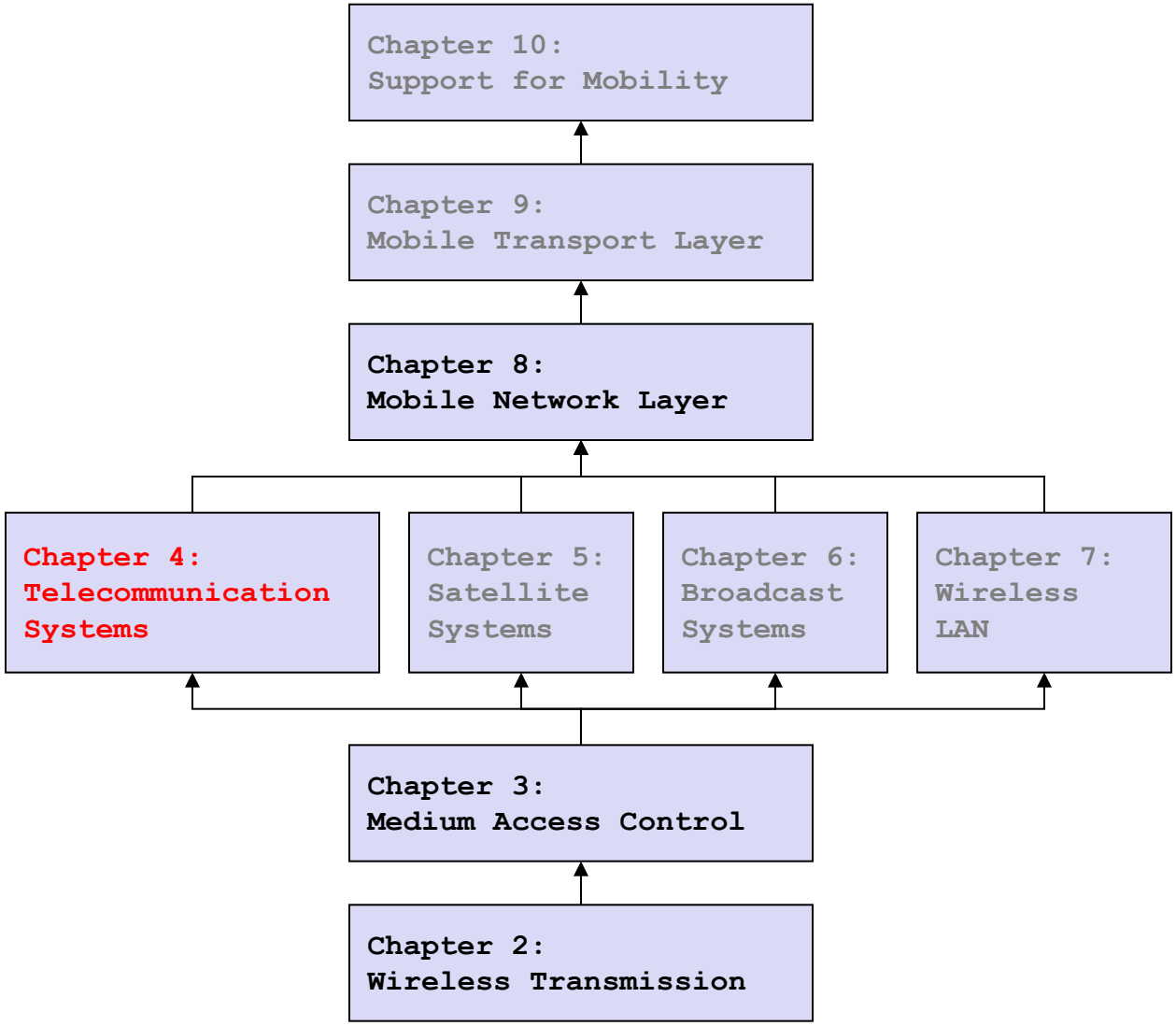
George Pavlides

http://georgepavlides.info

Book: Jochen H. Schiller, "Mobile Communications" Second Edition, Addison-Wesley, Pearson Education Limited, ISBN 0321123816

Presentation based on the course presentation by
Prof. Dr.-Ing. Jochen H. Schiller, Freie Universität Berlin - Computer Systems & Telematics

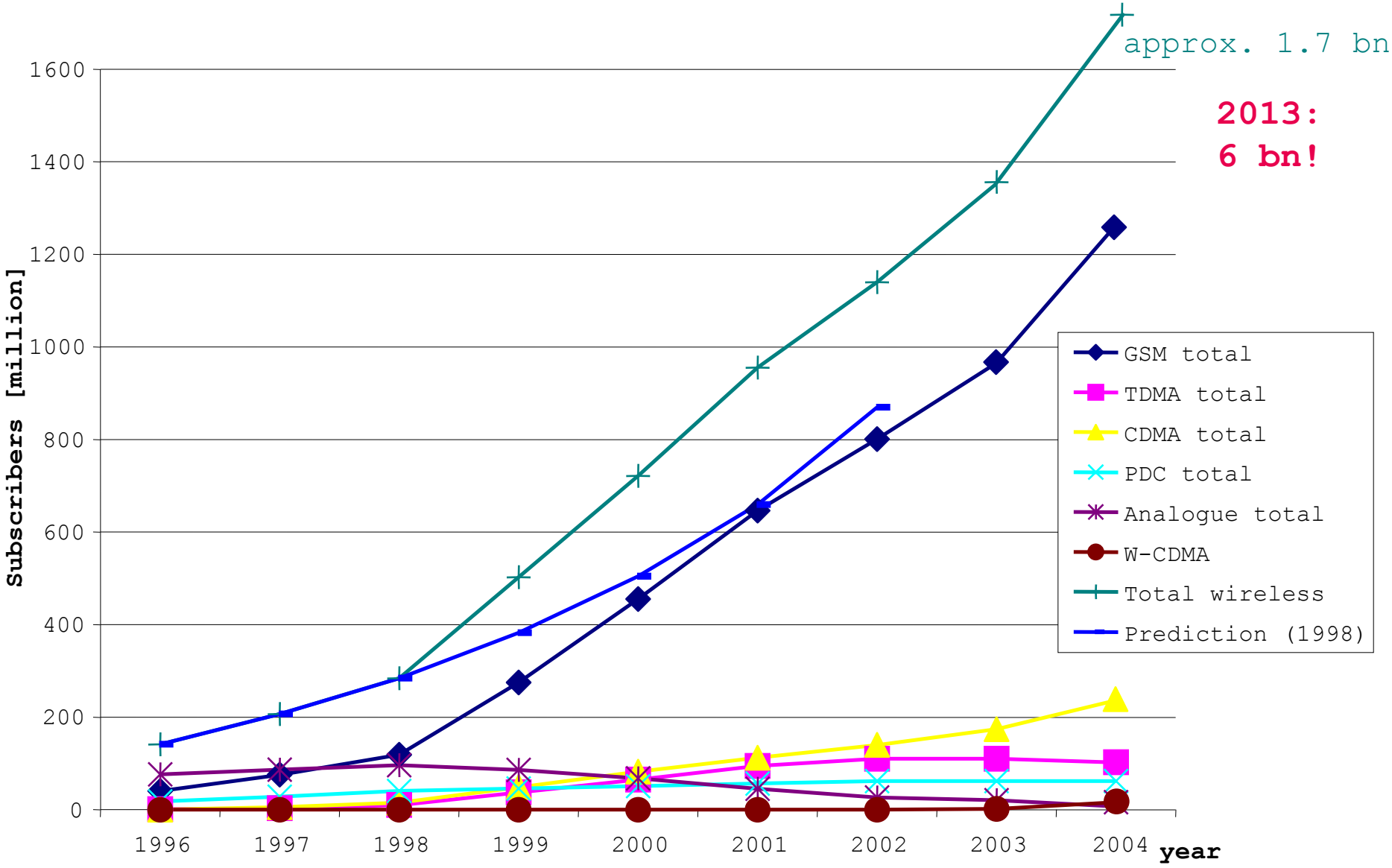
course outline



Wireless Telecommunication Systems

- Market view
- **GSM** (Global System for Mobile Communications, originally Groupe Spécial Mobile)
- **DECT** (Digital Enhanced Cordless Telecommunications or Digital European Cordless Telecommunications)
- **TETRA** (Terrestrial Trunked Radio formerly known as Trans-European Trunked Radio)
- **UMTS/IMT-2000** (Universal Mobile Telecommunications System - International Mobile Telecommunications-2000 band specification)
- **LTE** (Long Term Evolution)

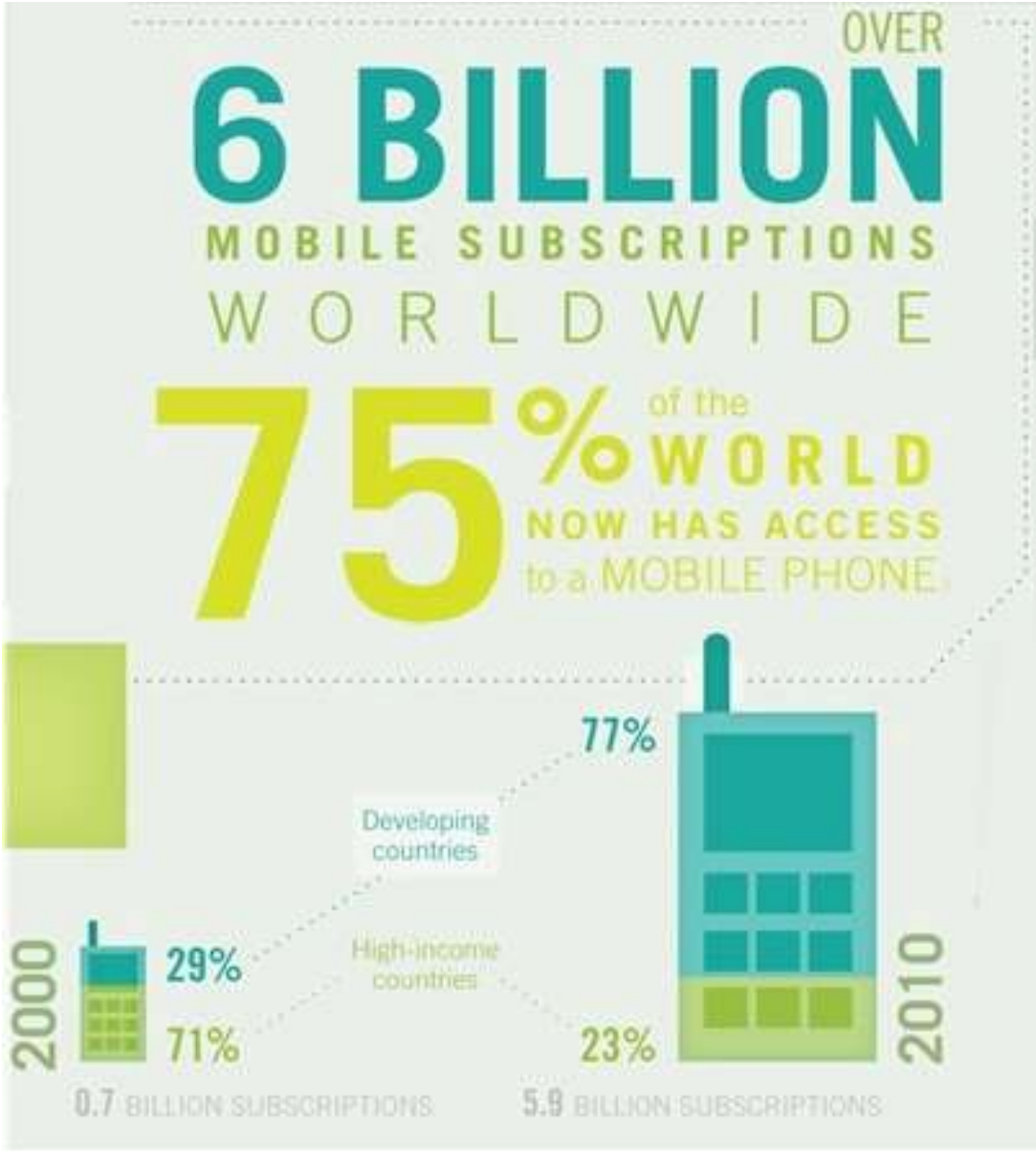
mobile phone subscribers worldwide



GSM Association, 2002

mobile phone subscribers worldwide

- **As of early 2012, more than 6bn.** mobile subscriptions were in use around the world (pre-paid and post-paid), providing mobile access for more than three-quarters (75%) of the world's inhabitants, according to a report by the World Bank.

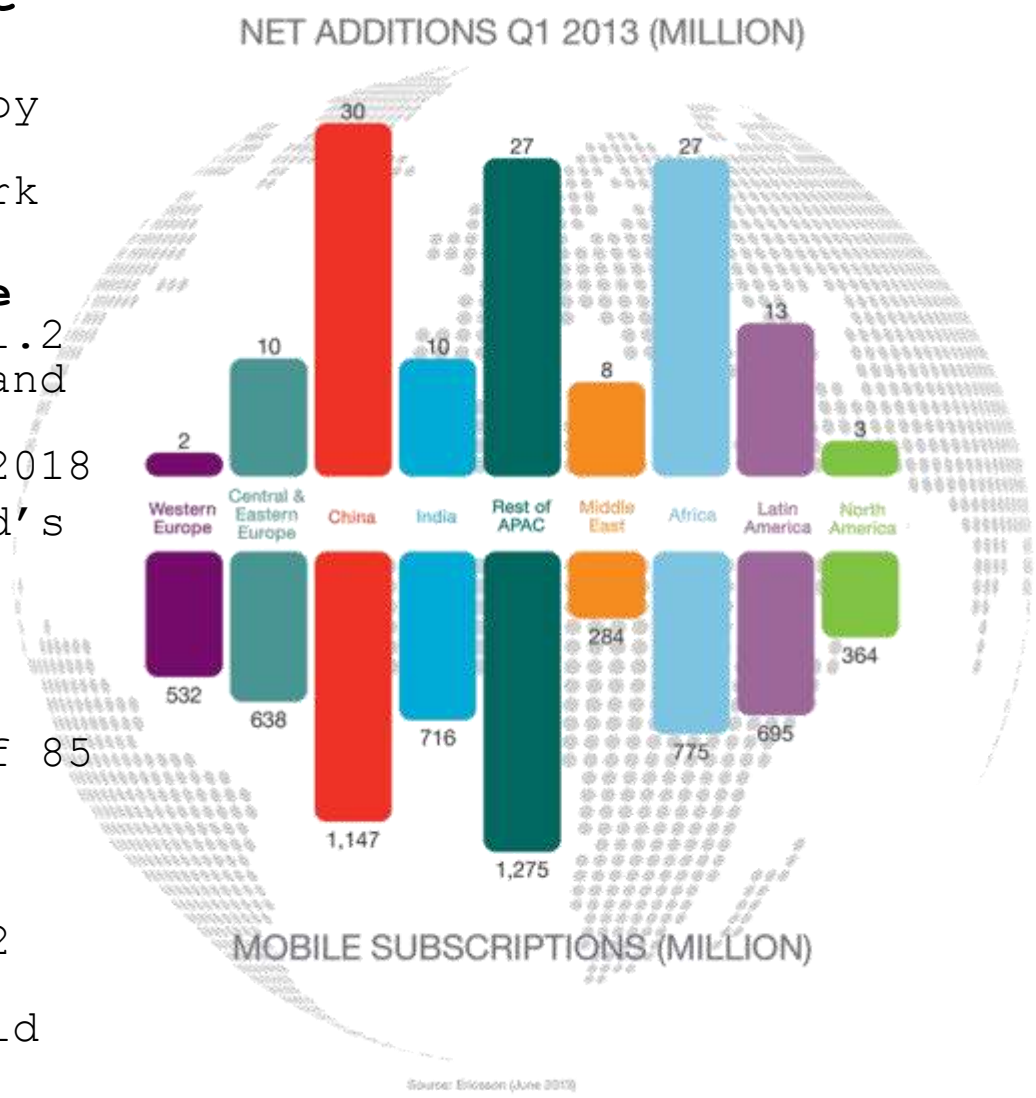


Source: Maximizing Mobile, ICT, World Bank, July 2012

- *World population counters*
  - http://goo.gl/ZtIV2p
  - http://goo.gl/yBXXrW

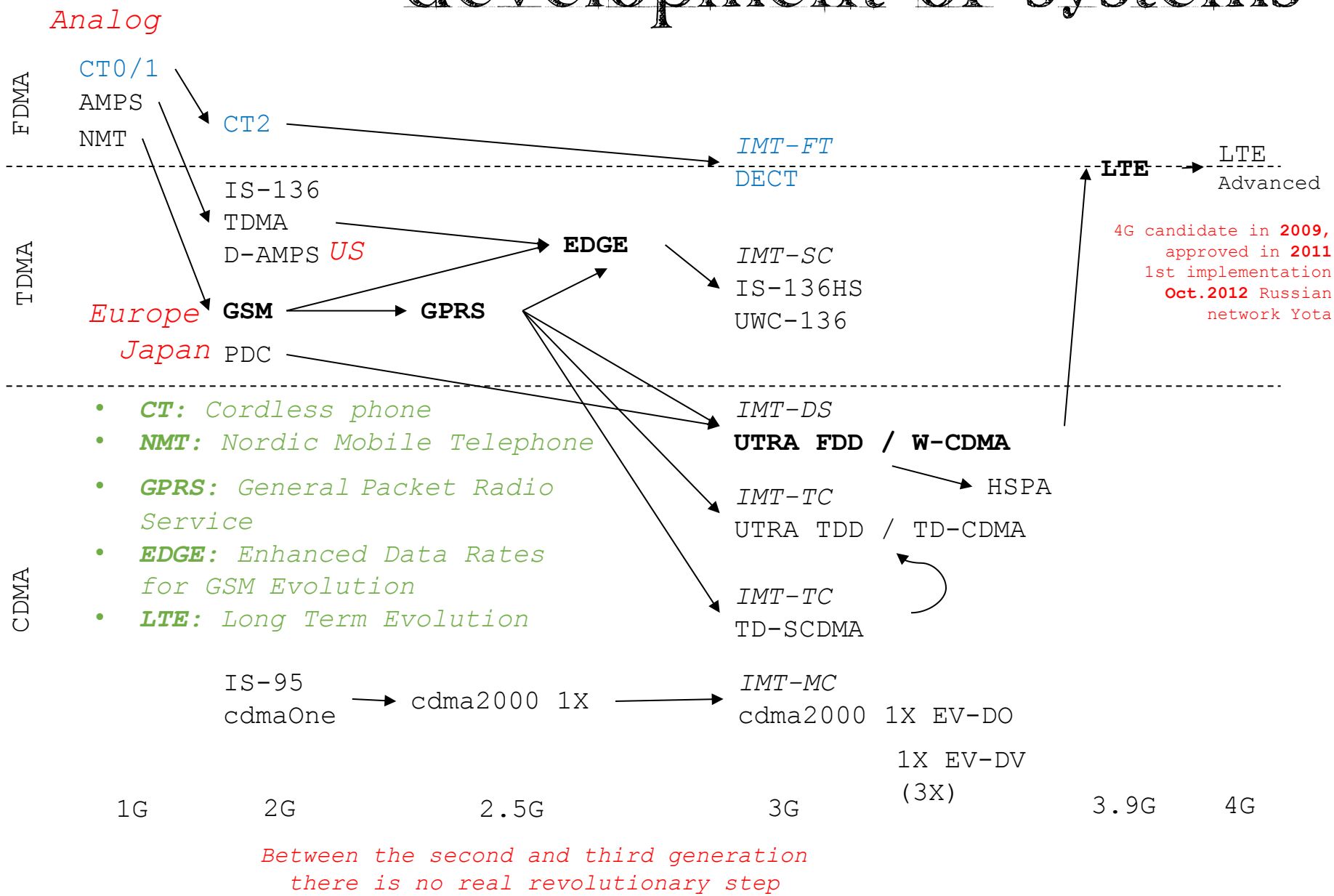
mobile phone subscribers worldwide

- **Ericsson Mobility Report 2013**
  - **Video traffic** growing by 60 percent annually, driven by better network Speeds
  - Total global **smartphone subscriptions** hit the 1.2 billion mark in 2012, and are due to reach 4.5 billion by the end of 2018
  - 60 percent of the world's population due to be **covered by LTE** in 2018
  - Smartphone users spend **most time on social networks:** an average of 85 minutes a day in some networks
  - **Data traffic volumes** doubled between Q1 2012 and Q1 2013, and are expected to grow 12-fold by 2018



See also a 2013 market analysis: http://goo.gl/TSJhWy

development of systems



- ***CT:*** *Cordless phone*
- ***NMT:*** *Nordic Mobile Telephone*
- ***GPRS:*** *General Packet Radio Service*
- ***EDGE:*** *Enhanced Data Rates for GSM Evolution*
- ***LTE:*** *Long Term Evolution*

4G candidate in **2009**, approved in **2011**
1st implementation **Oct.2012** Russian network Yota

Between the second and third generation there is no real revolutionary step

some press news...

- **16th April 2008:** The GSMA, the global trade group for the mobile industry, today announced that total connections to GSM mobile communications networks have now passed the **3 Billion** mark globally. The third billion landmark has been reached just four years after the GSM industry surpassed its first billion, and just two years from the second billionth connection. **The 3 Billion landmark has been surpassed just 17 years after the first GSM network launch in 1991.** Today more than 700 mobile operators across 218 countries and territories of the world are adding **new connections at the rate of 15 per second, or 1.3 million per day.**
- **11 February 2009:** The GSMA today announced that the mobile world has celebrated its **four billionth connection**, according to Wireless Intelligence, the GSMA's market intelligence unit. This milestone underscores the continued strong growth of the mobile industry and puts the global market on the path to reach a staggering **six billion connections by 2013.**
- By **2014 3.4bn** people will have **broadband**, 80% mobile

how does it work?

- 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: overview

- GSM
  - **Global System for Mobile Communications**
  - formerly: Groupe Spéciale Mobile
  - founded **1982**
  - 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

GSM: overview

- Today many providers all over the world use GSM
  - **>220 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)
  - See e.g. www.gsmworld.com

performance characteristics of GSM

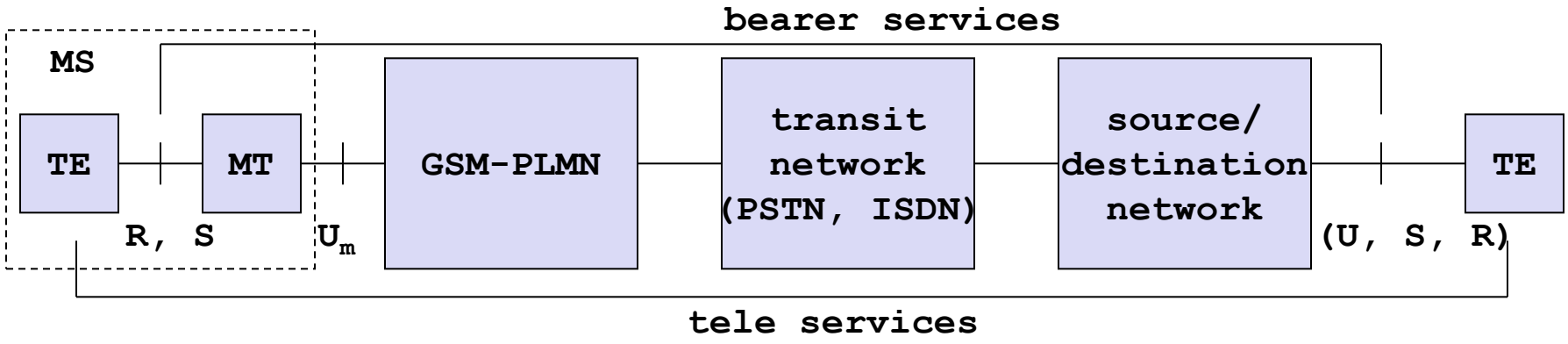
- **Communication**
  - mobile, wireless communication; support for voice and data services
- **Total mobility**
  - international access, chip-card enables use of access points of different providers
- **Worldwide connectivity**
  - one number, the network handles localization
- **High capacity**
  - 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 (SIM-Subscriber identity module)

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 (ISDN bearer in which the primary data or voice communication is carried)
- electromagnetic **radiation**
- **abuse of private** data possible
- **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 (SMS)
  - **multi-service** options (combination of basic services)
- Three service domains
  - Bearer Services
  - Telematic Services
  - Supplementary Services



reference model for GSM services

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)
  - data service (circuit switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 1200 bit/s
  - data service (packet switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 9600 bit/s
- Today: 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
    - 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 (**160 characters**) **using the signaling channel**, thus allowing simultaneous use of basic services and SMS
      - **almost ignored in the beginning** now the most successful add-on!
      - more and more replaced by IP-based messaging

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)
  - ...

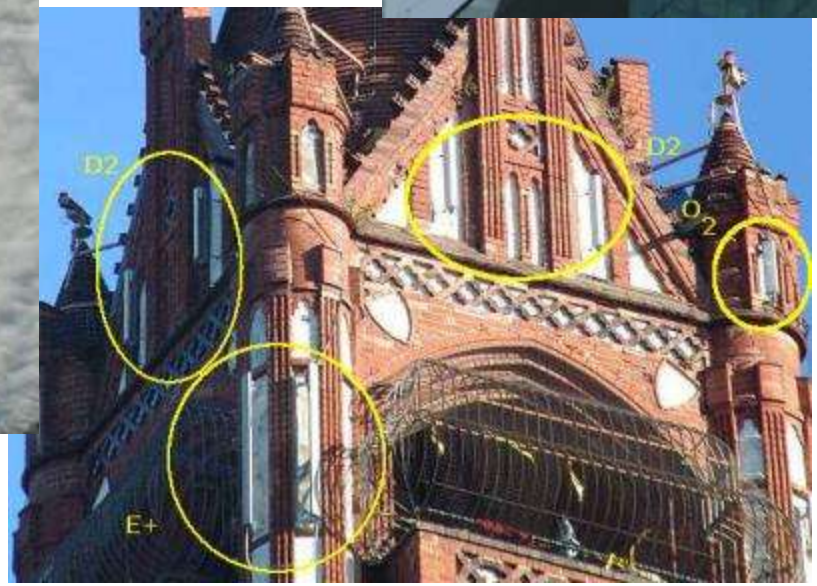
architecture of the GSM system

- 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)
  - subsystems
    - **RSS** (radio subsystem): covers all radio aspects
    - **NSS** (network and switching subsystem): call forwarding, handover, switching
    - **OSS** (operation subsystem): management of the network

ingredients 1: mobile phones, PDAs...

The visible but smallest part of the network!

ingredients 2: Antennas



Still visible – cause many discussions…

ingredients 3: infrastructure 1

Base Stations

Cabling

Microwave links

ingredients 3: infrastructure 2

Management

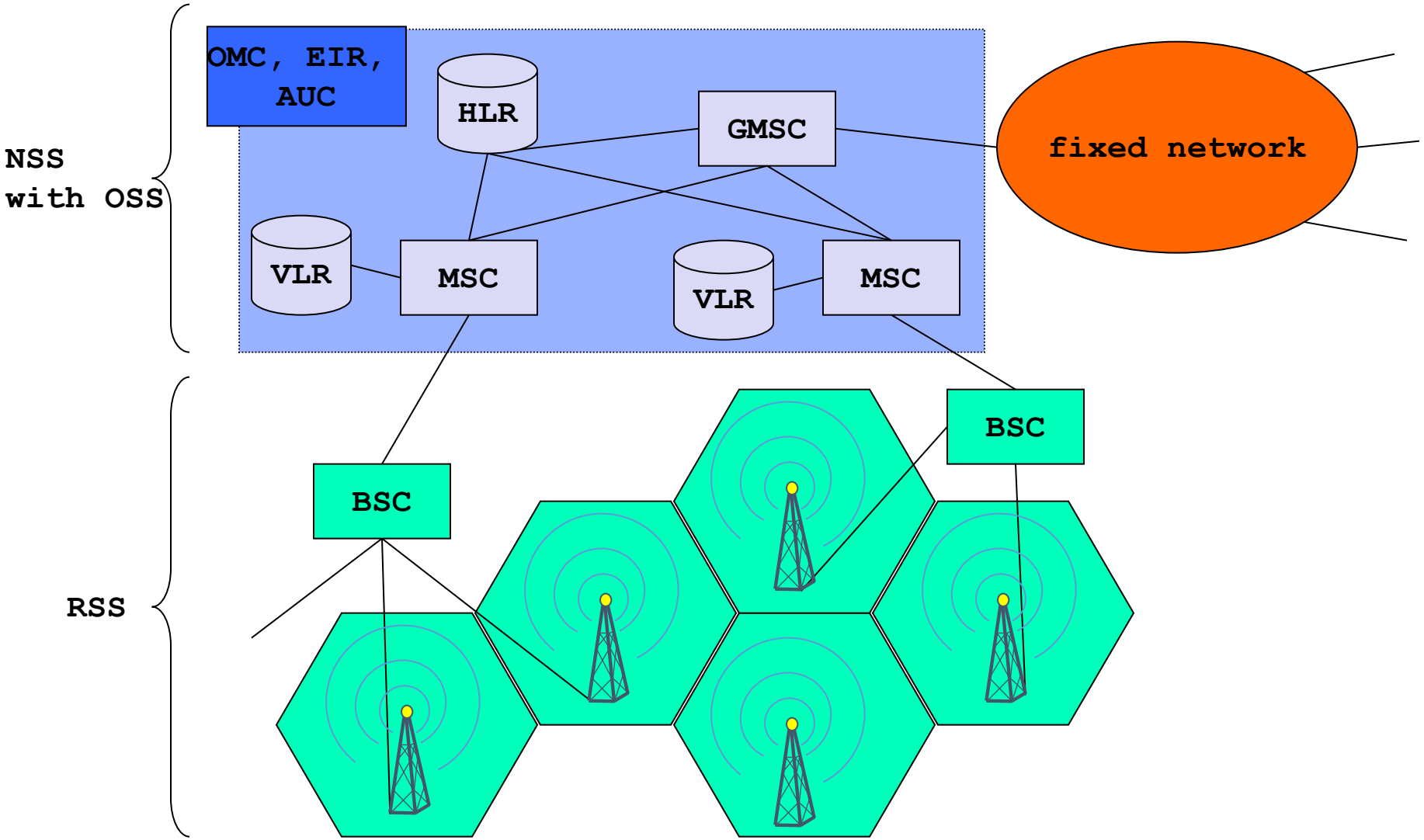
Data bases

Switching units

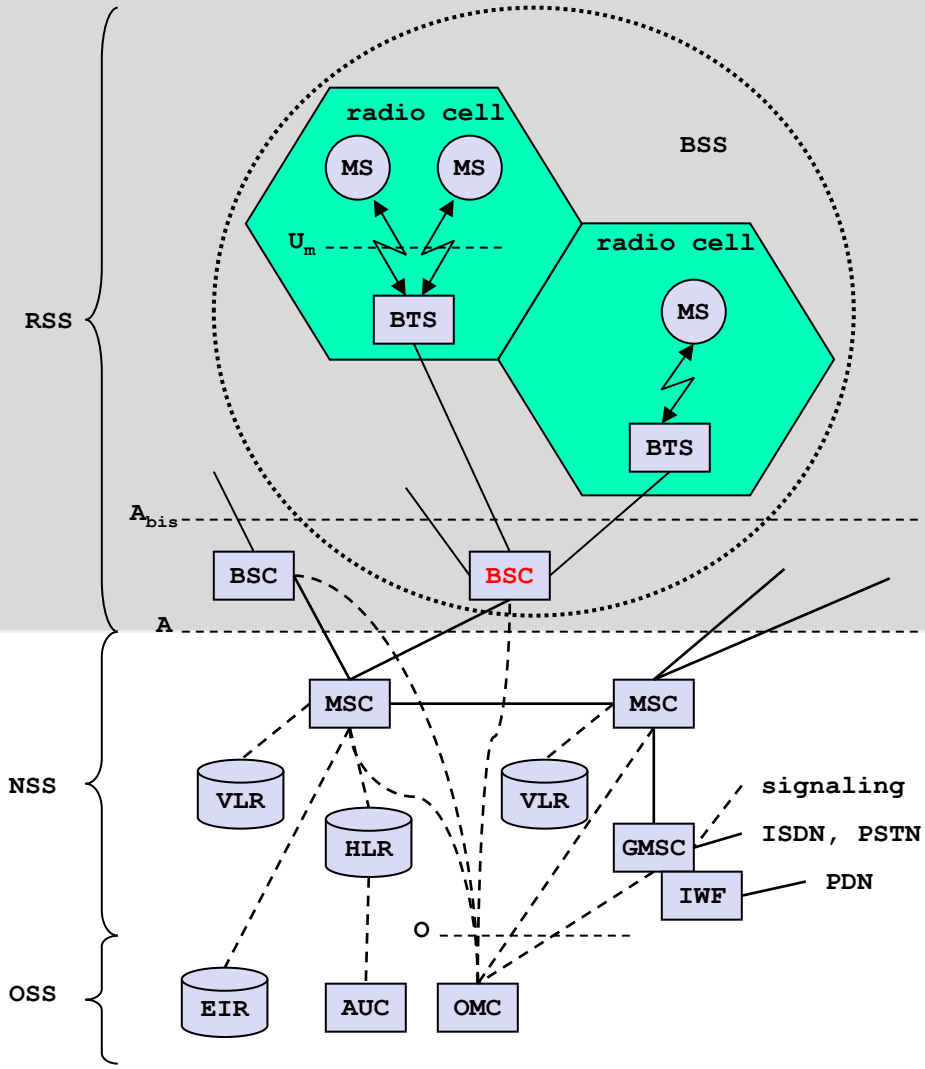
Monitoring

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

GSM: overview



GSM: elements and interfaces



RSS - Radio subsystem comprises all radio specific entities

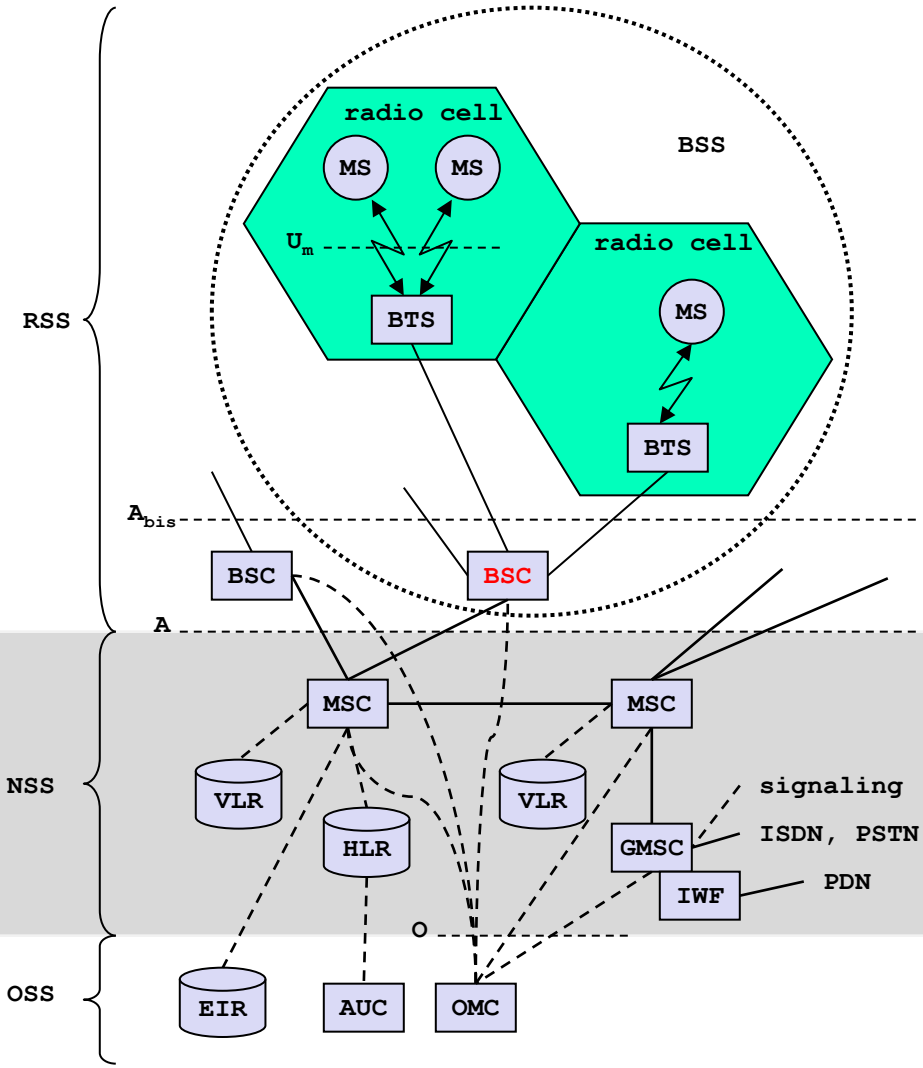
BSS - Base station subsystem are groups of cells controlled by a BSC (controller)

BTS - Base transceiver stations comprise all radio equipment

BSC – Base station controller manages the BTSs

CELL - A GSM cell can measure between some 100 m and 35 km depending on the environment but also expected traffic

GSM: elements and interfaces



NSS – Network and switching subsystem is the "heart" of the GSM system

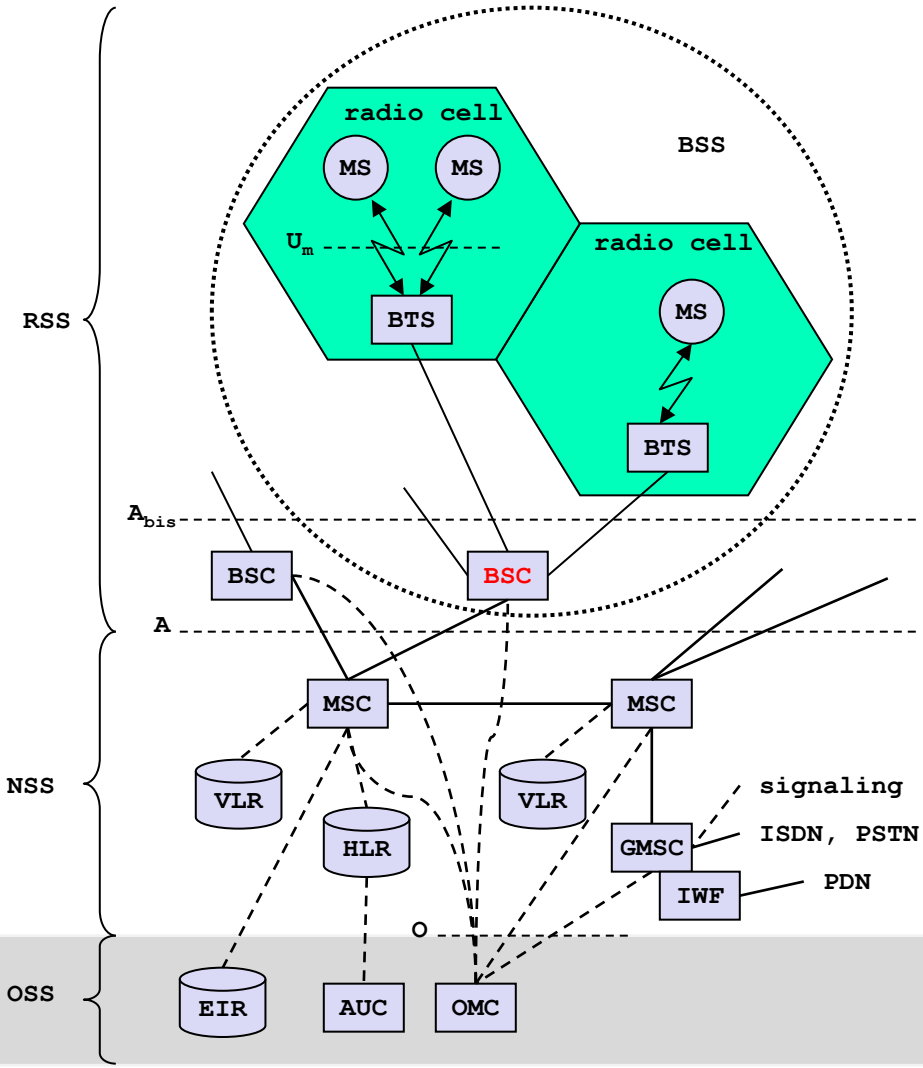
MSC – Mobile services switching centers form the fixed backbone of the network

GMSC – Gateway mobile services switching centers provides connections to other networks

HLR – Home location register is the user-relevant static database (ID, services, etc)

VLR – Visitor location register is a dynamic user-related database depending on location

GSM: elements and interfaces



OSS – operation subsystem contains the necessary functions for network operation and maintenance

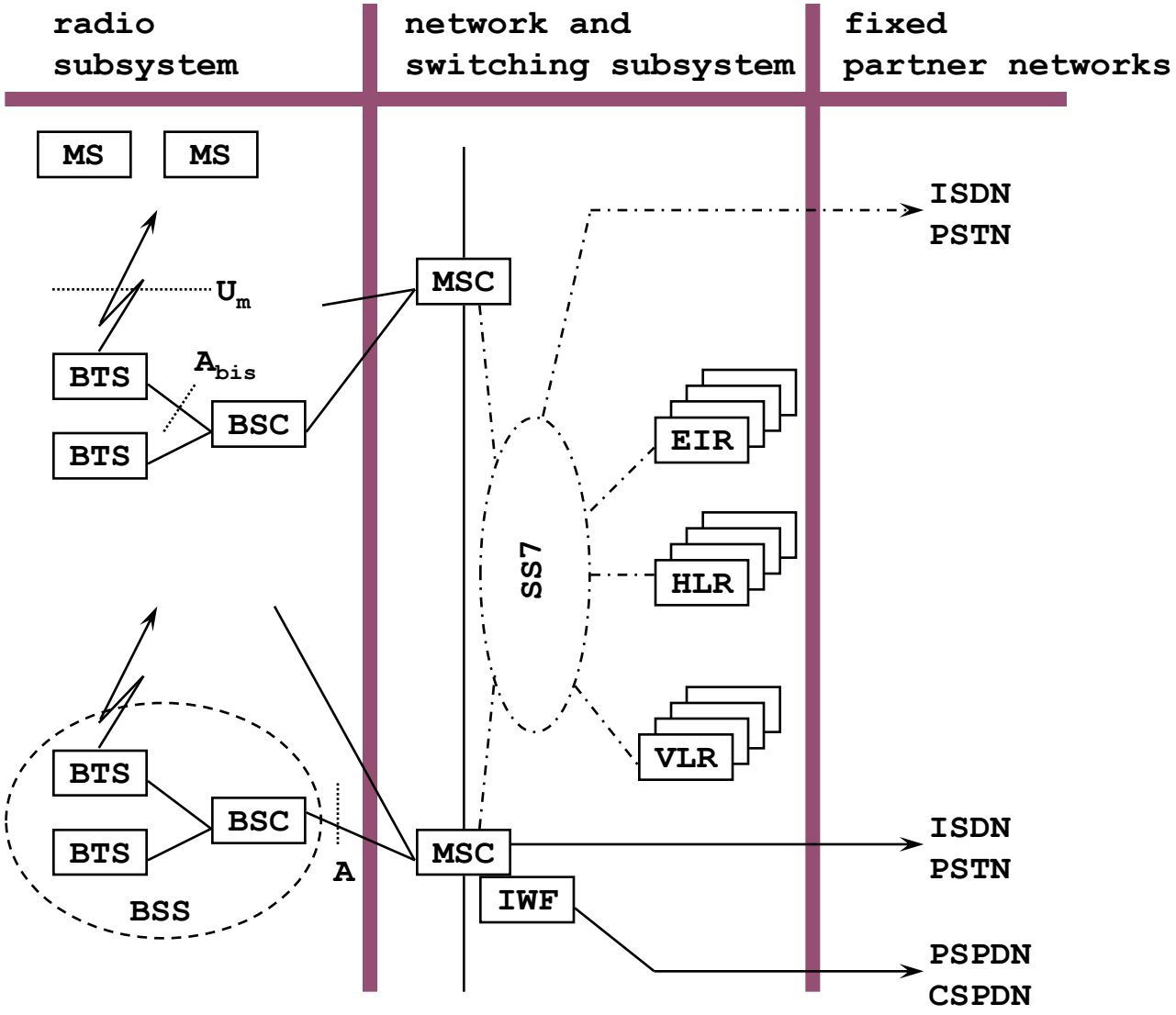
OMC – Operation and maintenance center (traffic moritoring, status reports, subscriber and security management, or accounting and billing)

AuC – Authentication center to protect user identity and data

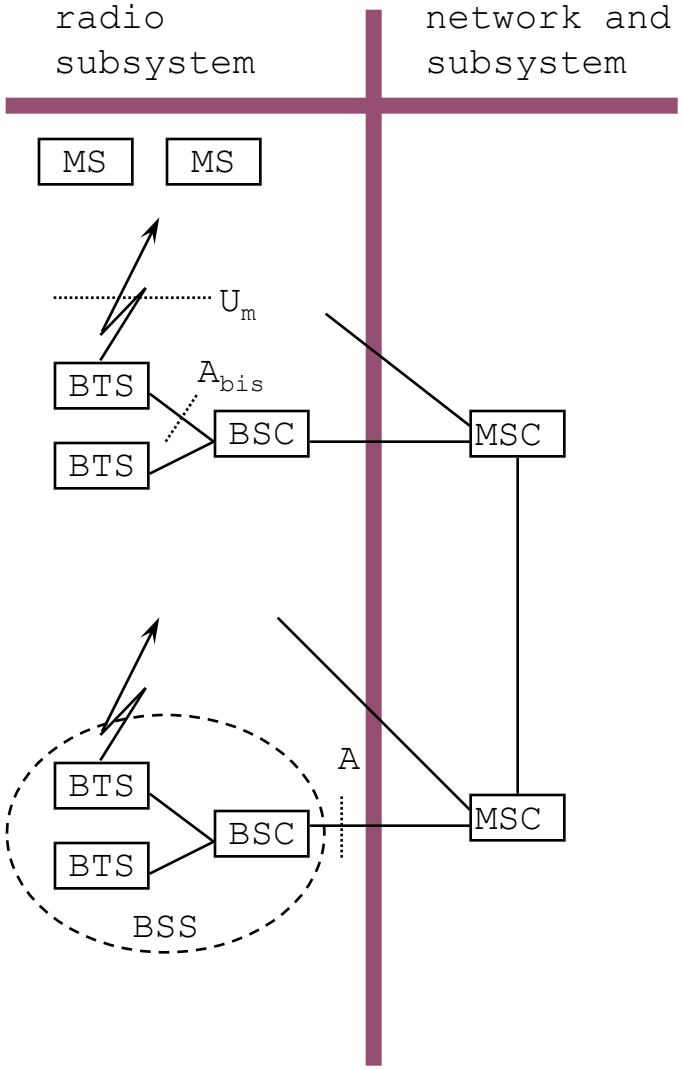
EIR – Equipment identity register is the IMEI database

** IMEI - International Mobile Station Equipment Identity*

GSM: system architecture

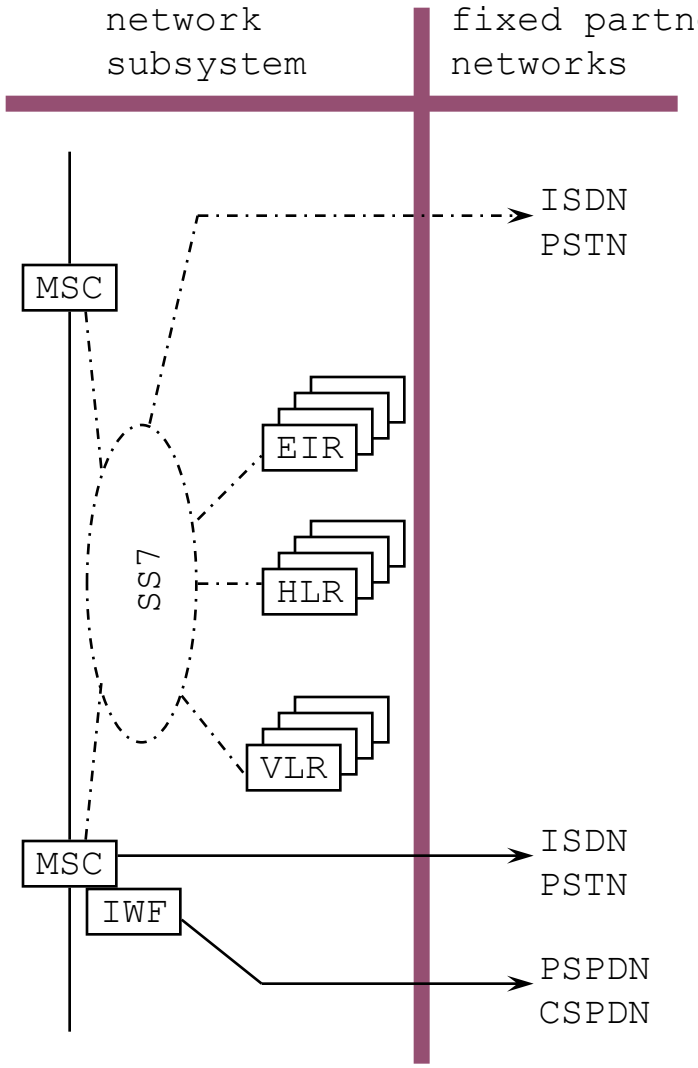


system architecture: radio subsystem



- 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



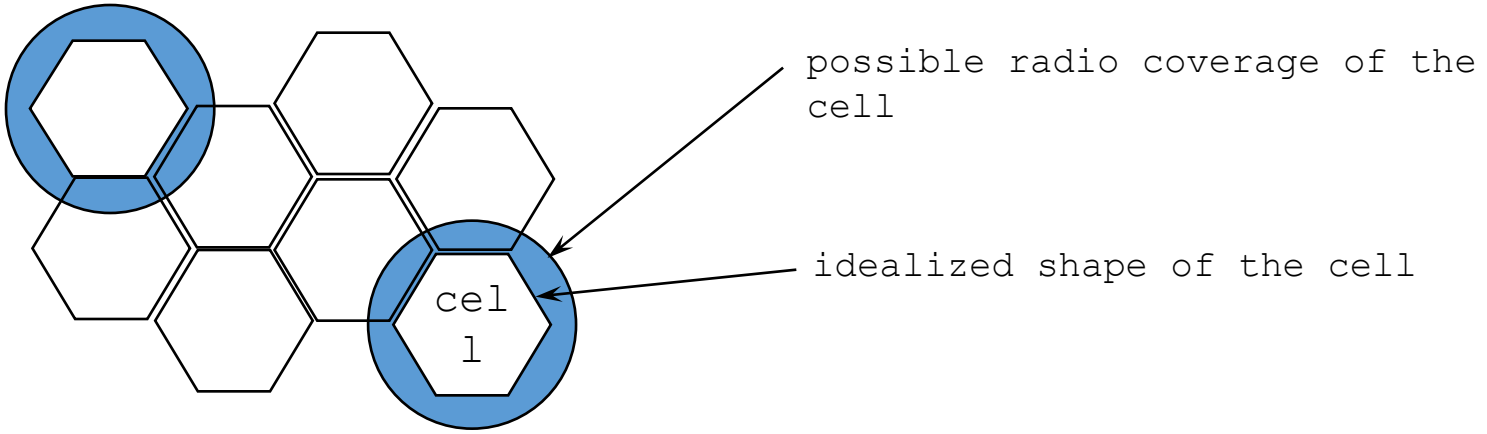
- Components
  - MSC (Mobile Services Switching Center):
  - IWF (Interworking Functions)
  - ISDN (Integrated Services Digital Network)
  - PSTN (Public Switched Telephone Network)
  - PSPDN (Packet Switched Public Data Net.)
  - CSPDN (Circuit Switched Public Data Net.)
- Databases
  - HLR (Home Location Register)
  - VLR (Visitor Location Register)
  - EIR (Equipment Identity Register)

radio subsystem

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

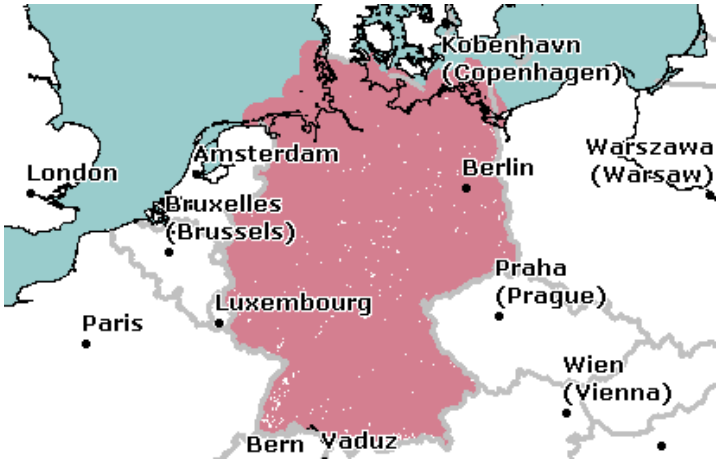
GSM frequency bands (examples)

Type	Channels	Uplink [MHz]	Downlink [MHz]
GSM 850	128-251	824-849	869-894
GSM 900	0-124, 955-1023	876-915	921-960
classical	124 channels	890-915	935-960
extended	+49 channels	880-915	925-960
GSM 1800	512-885	1710-1785	1805-1880
GSM 1900	512-810	1850-1910	1930-1990
GSM-R	955-1024, 0-124	876-915	921-960
exclusive	69 channels	876-880	921-925

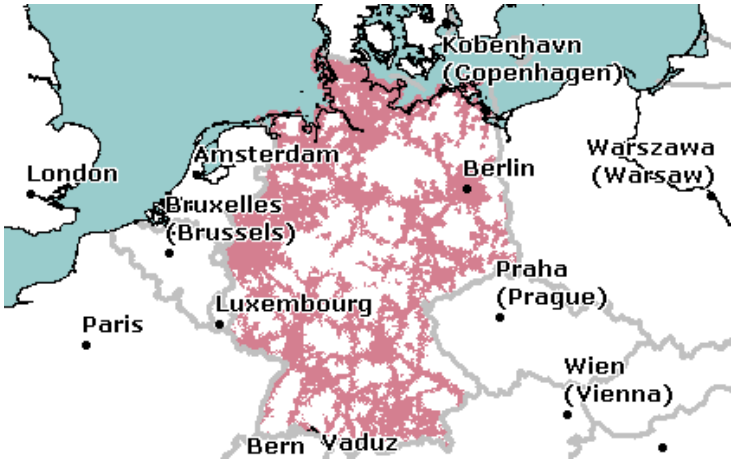
- Additionally: GSM 400 (also named GSM 450 or GSM 480 at 450-458/460-468 or 479-486/489-496 MHz)
- Please note: frequency ranges may vary depending on the country!
- Channels at the lower/upper edge of a frequency band are typically not used

example coverage of GSM networks

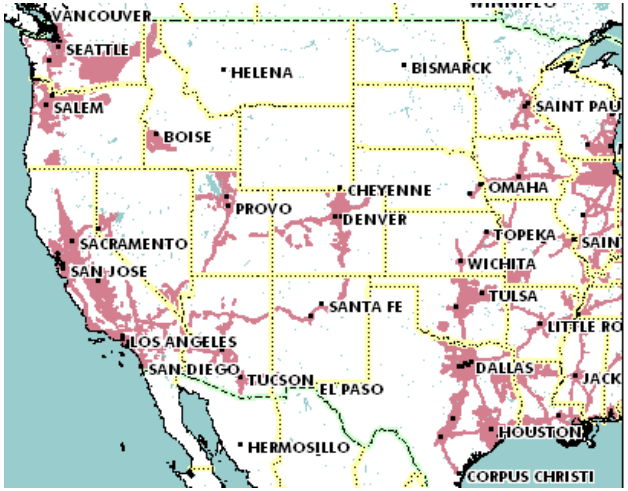
T-Mobile (GSM-900/1800) Germany



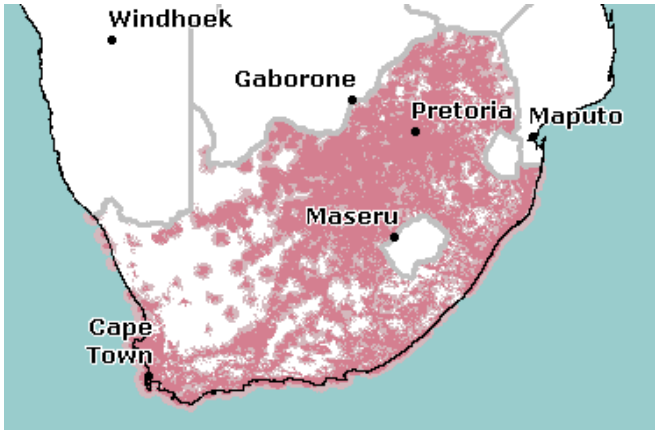
O_2 (GSM-1800) Germany



AT&T (GSM-850/1900) USA



Vodacom (GSM-900) South Africa



Source: http://www.gsmworld.com

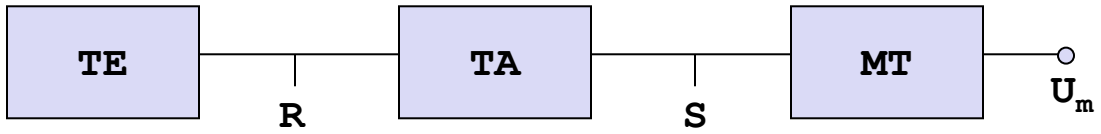
BTS & BSC

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

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

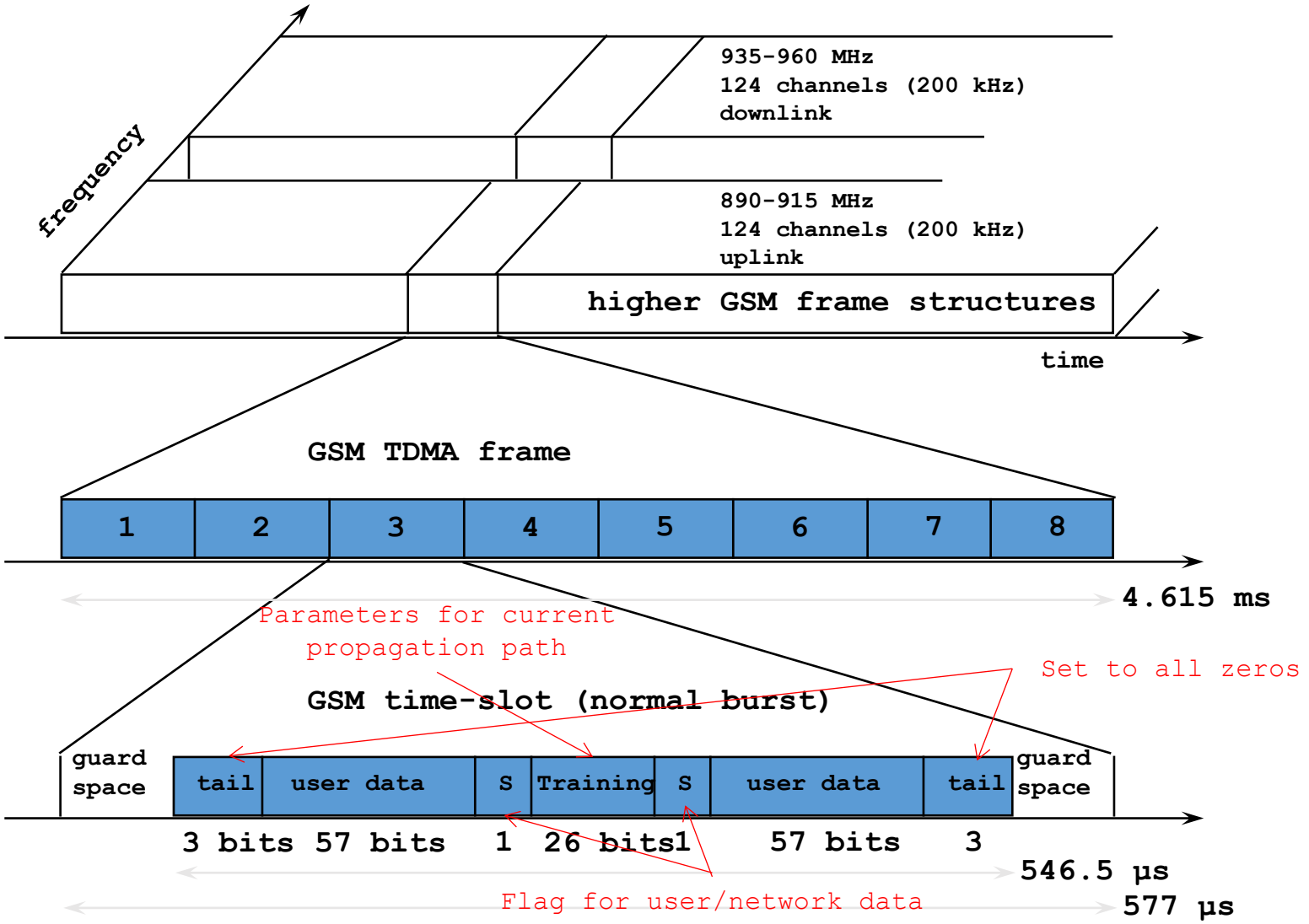
mobile station

- 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 (Um)
  - 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



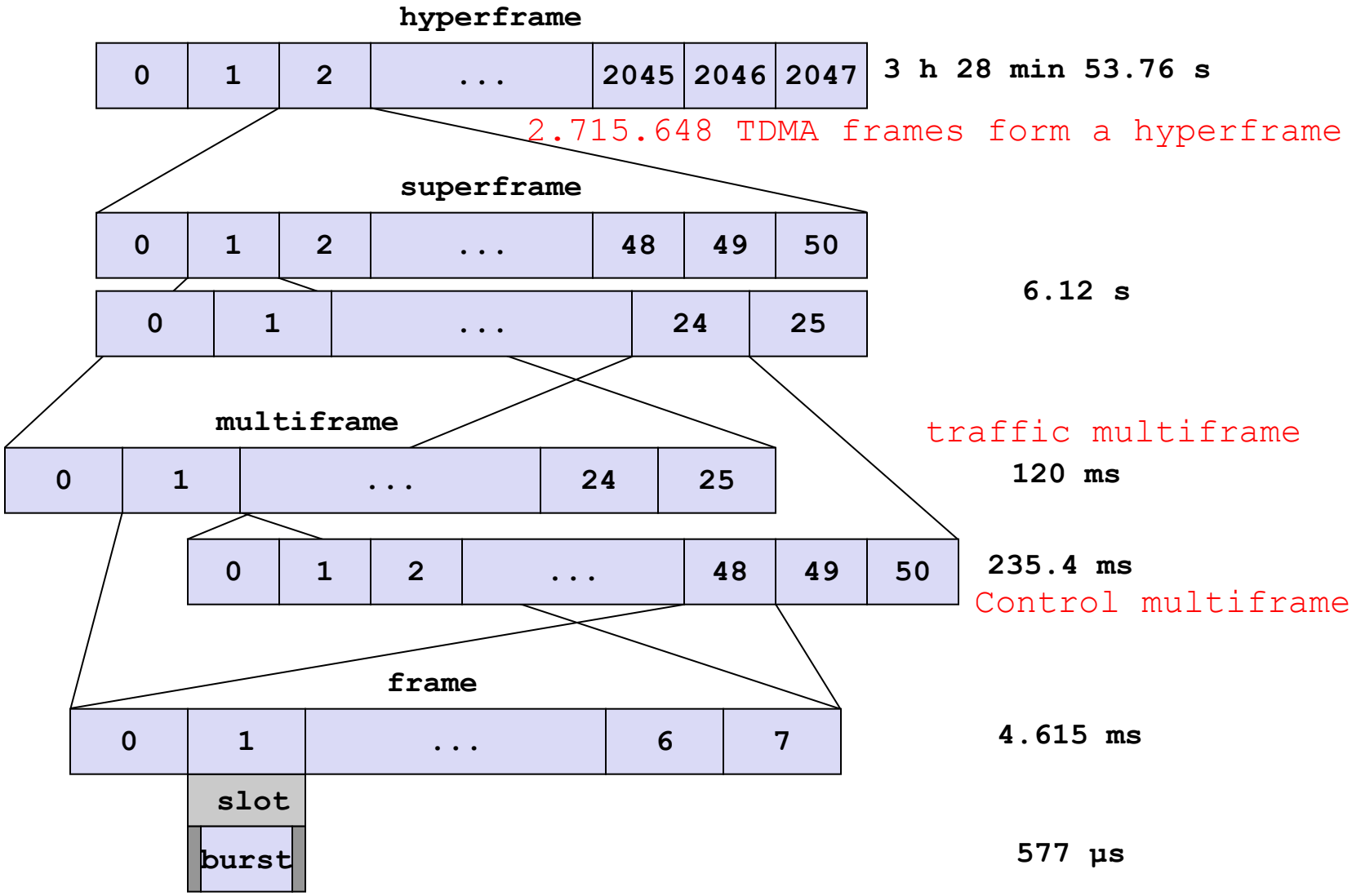
GSM - TDMA/FDMA

Data is transmitted in small portions, **bursts.**



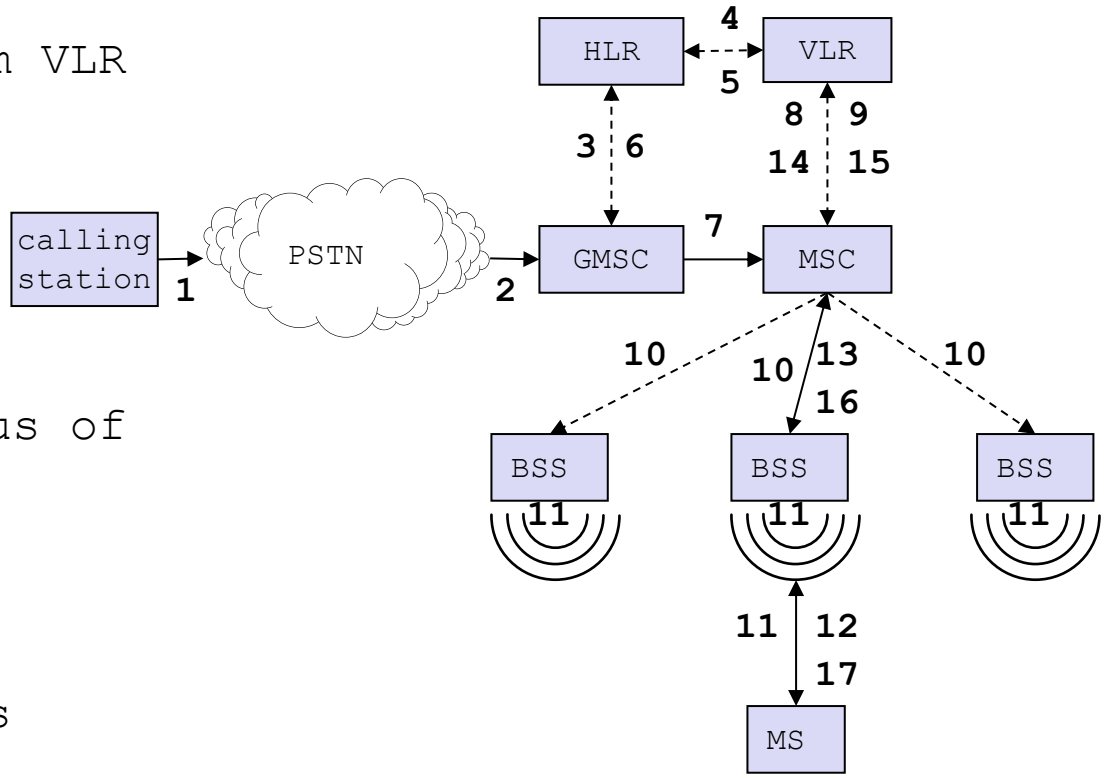
*A **normal burst** as used for data transmission inside a time slot*
*A total of 156.25 bit within 577 µs - **carries 114 bit user data***

GSM hierarchy of frames



mobile terminated call

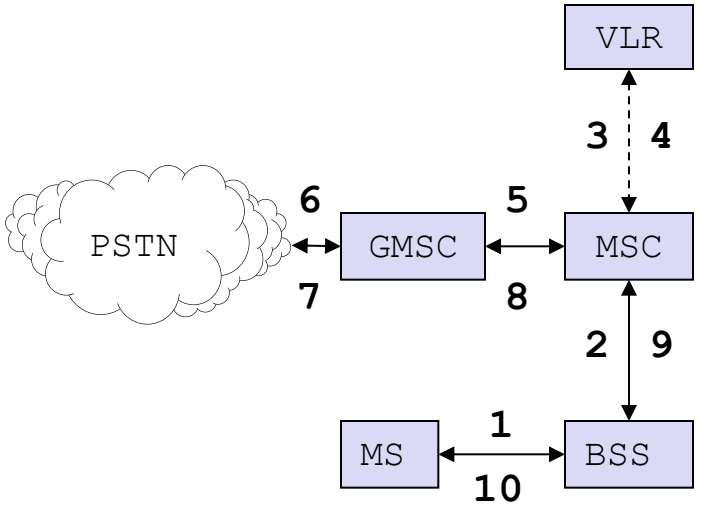
- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4, 5: request MSRN from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: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



the basic steps needed to connect the calling station with the mobile user

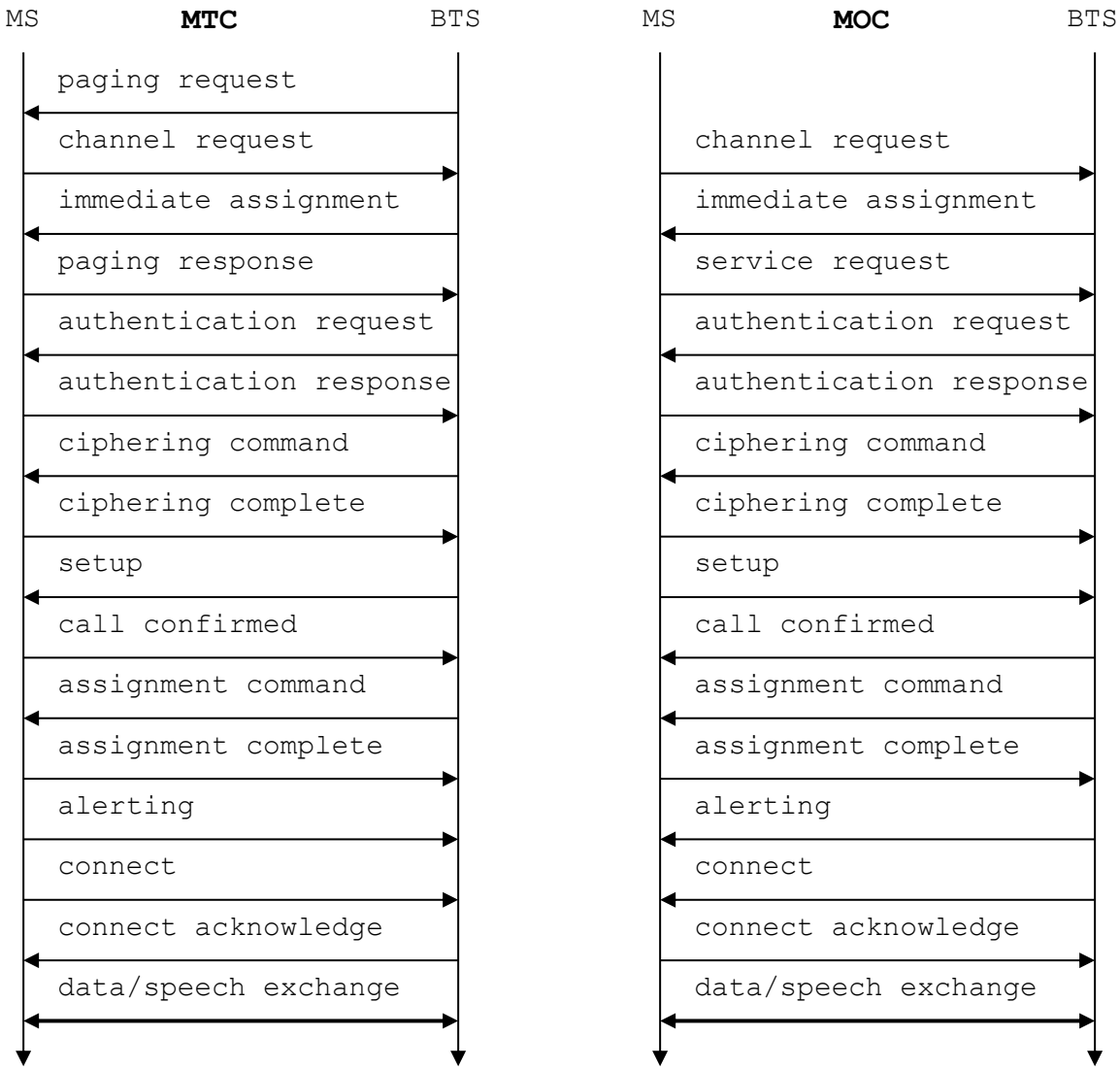
mobile originated call

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



the basic steps needed to connect a mobile originated call

MTC/MOC



Other message flow for Mobile-Terminated-Call and Mobile-Originating-Call during connection setup (in either direction)

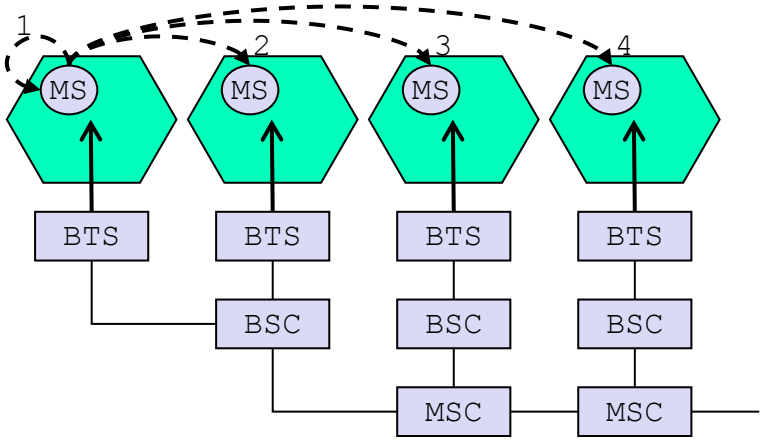
Can be often heard in loudspeakers as crackling noise before the phone rings

handover

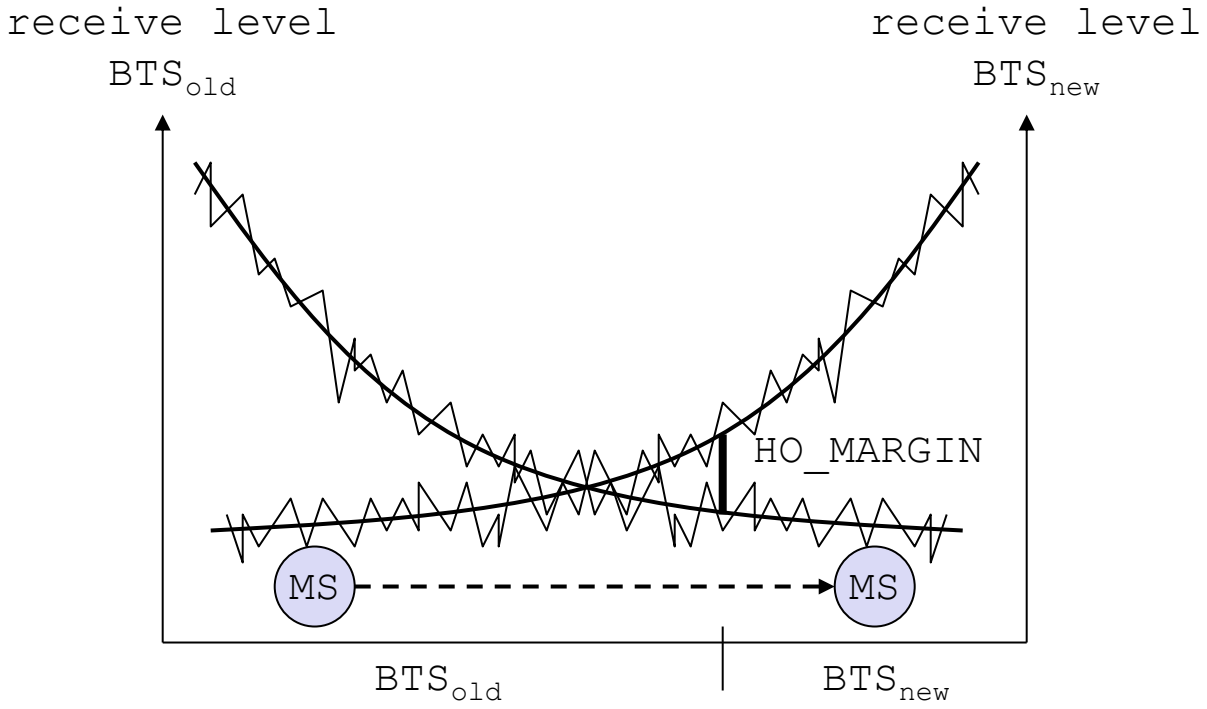
- Cellular systems require **handover** procedures, as single cells do not cover the whole service area
  - The smaller the cell size and the faster the movement of a mobile station through the cells (up to 250 km/h for GSM), the more handovers of ongoing calls are required
  - However, a handover should not cause a cut-off, also called call drop
    - **GSM aims at maximum handover duration of 60 ms**
- Two basic **reasons** for a handover (about 40 identified in the standard):
  - A mobile station moves **out of range** of a BTS
  - Too much traffic causes a handover for **load balancing**

4 types of handover

- **Intra-cell:** Within a cell, narrow-band interference could make transmission at a certain frequency impossible. The BSC could then decide to **change the carrier frequency** (scenario 1)
- **Inter-cell, intra-BSC:** This is a **typical handover scenario**. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2)
- **Inter-BSC, intra-MSC:** As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3)
- **Inter MSC:** A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4)



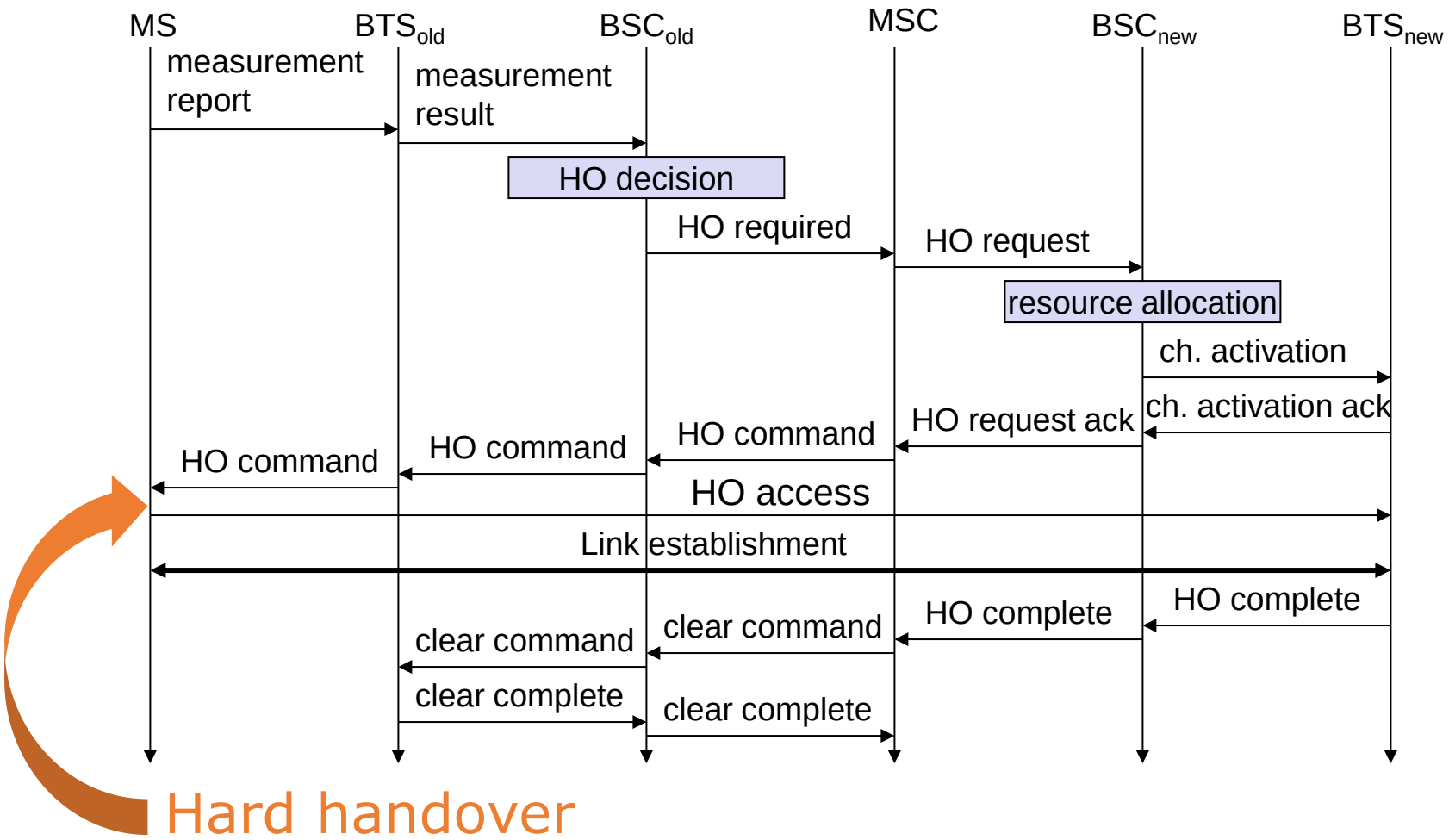
handover decision



Typical behavior of the received signal level while an MS moves away from one BTS (BTS$_{old}$) closer to another one (BTS$_{new}$) – **handover depends on the average value of the received signal level and a handover margin (HO_MARGIN) to avoid ping-pong effects**

handover procedure

- Typical signal flow during an inter-BSC, intra-MSC handover

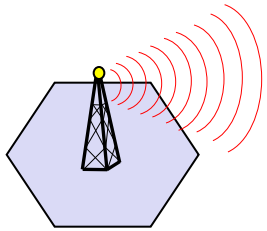


security in GSM

- Security services
  - access control/authentication
    - user → SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM → network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - temporary identity TMSI (Temporary Mobile Subscriber Identity)
    - newly assigned at each new location update (LUP)
    - encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication ("secret", open interface)
  - A5 for encryption (standardized)
  - A8 for key generation ("secret", open interface)

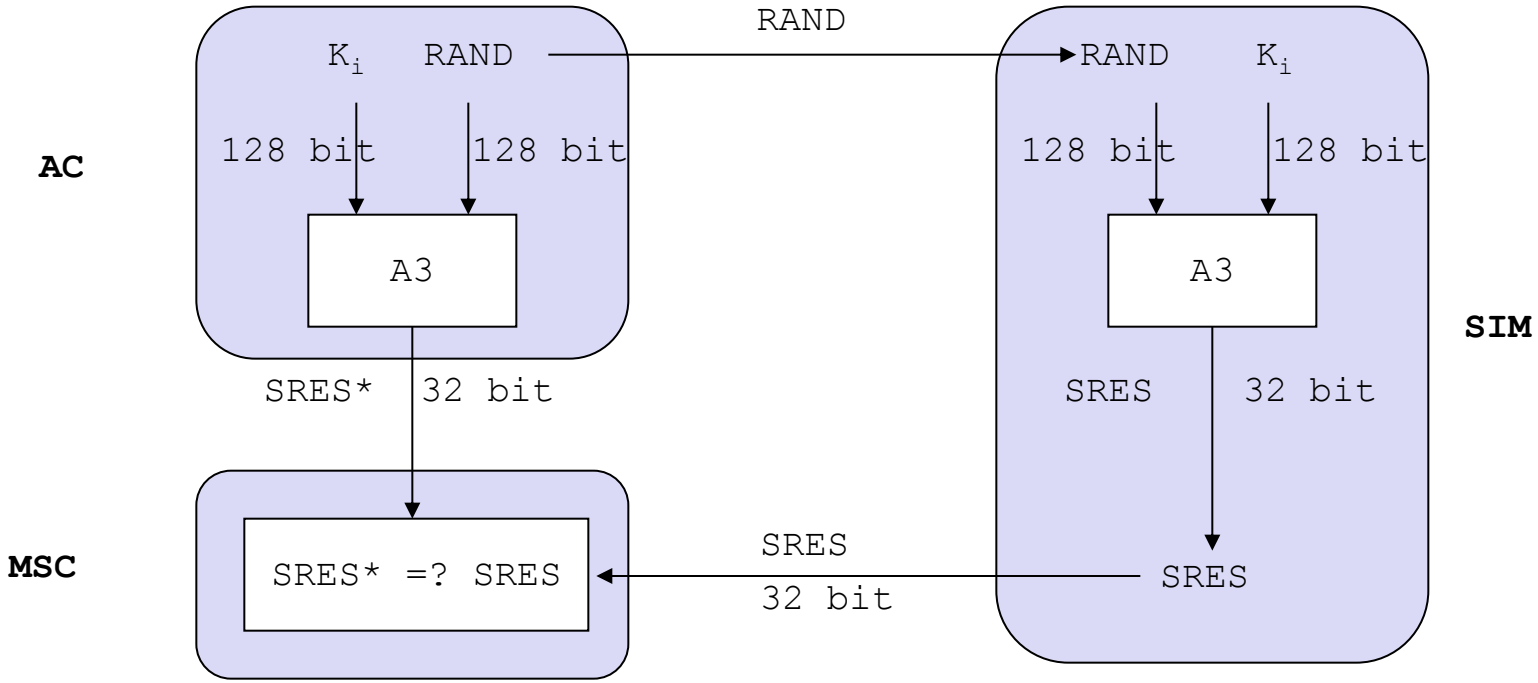
"secret":
• A3 and A8 available via the Internet
• network providers can (and do) use stronger mechanisms

authentication



mobile network

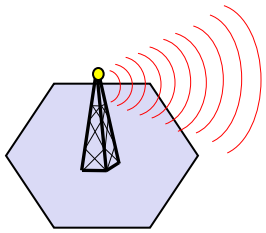
SIM



K_i: individual subscriber authentication key

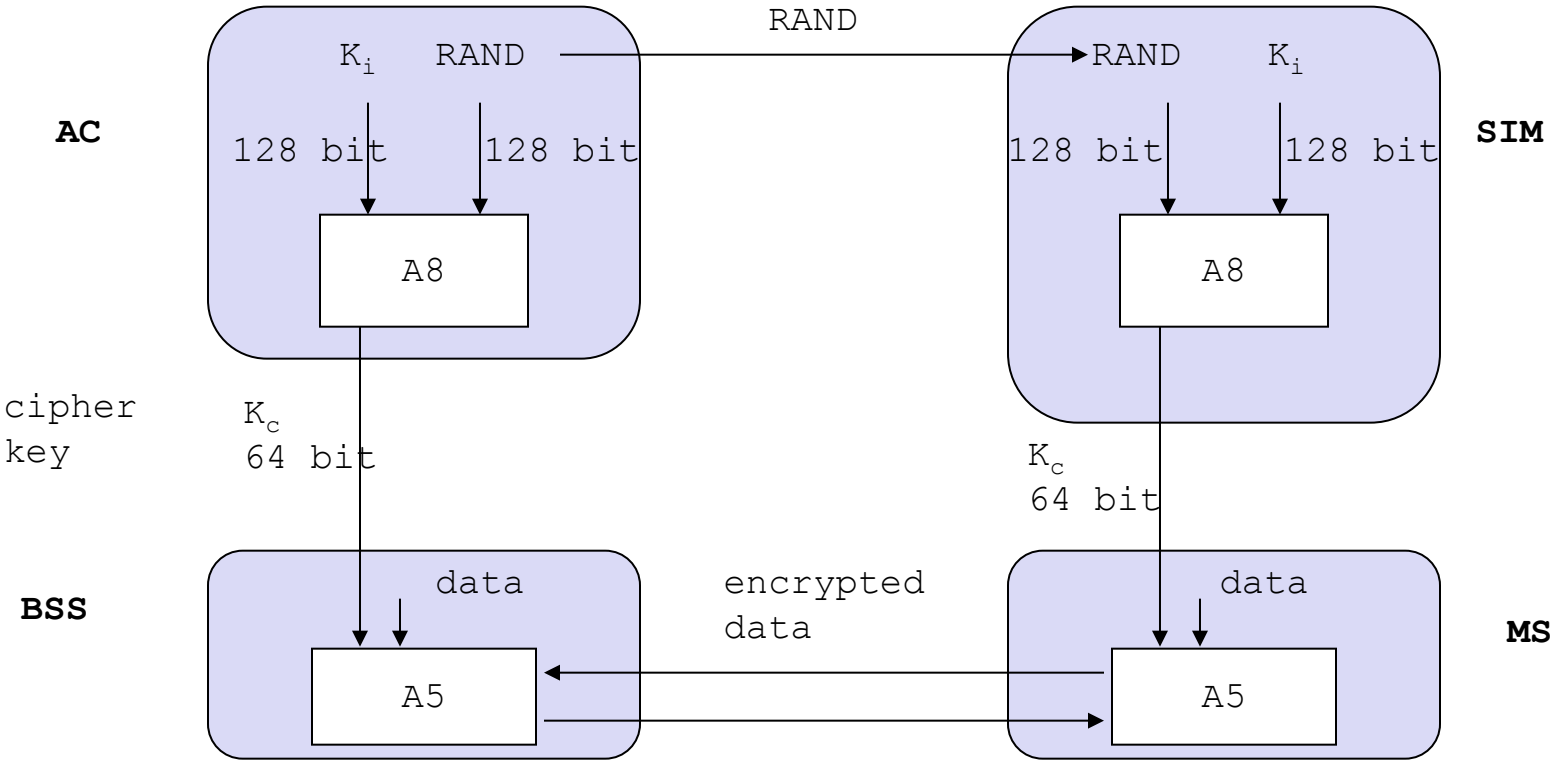
SRES: signed response

key generation and encryption



mobile network (BTS)

MS with SIM



Data services in GSM
GPRS

General Packet Radio Service

data services in GSM

- Data transmission standardized with only 9.6 kbit/s
  - advanced coding allows 14.4 kbit/s
  - good-enough for group-3 fax
  - not enough for Internet and multimedia applications
- Two approaches to increase bandwidth
  - **HSCSD – High speed circuit switched data**
    - As the basic GSM is based on connection-oriented traffic channels, e.g., with 9.6 kbit/s each, several channels could be combined to increase bandwidth
  - **GPRS - General Packet Radio Service**
    - packet-oriented traffic in GSM, i.e., shifting the paradigm from connections/telephone thinking to packets/internet thinking

data services in GSM

- **HSCSD (High-Speed Circuit Switched Data)**
  - mainly software update
  - bundling of several time-slots to get higher AIUR (Air Interface User Rate, e.g., 57.6 kbit/s using 4 slots @ 14.4)
  - **advantage:** ready to use, constant quality, simple
  - **disadvantage:** channels blocked for voice transmission

AIUR [kbit/s]	TCH/F4.8	TCH/F9.6	TCH/F14.4
4.8	1		
9.6	2	1	
14.4	3		1
19.2	4	2	
28.8		3	2
38.4		4	
43.2			3
57.6			4

permitted combinations of traffic channels (TCH) and allocated slots for services

data services in GSM

- **GPRS (General Packet Radio Service)**
  - packet switching
  - using free slots only if data packets ready to send
    (e.g., 50 kbit/s using 4 slots temporarily)
  - standardization 1998, introduction 2001
  - **Depending on the coding, a transfer rate of up to 170 kbit/s is possible**
  - **advantage:** one step towards UMTS (3G), more flexible – 'always on' characteristic
  - **disadvantage:** more investment needed (new hardware)

GPRS user data rates in kbit/s

- Data rates for all combinations of coding schemes & time slot allocations

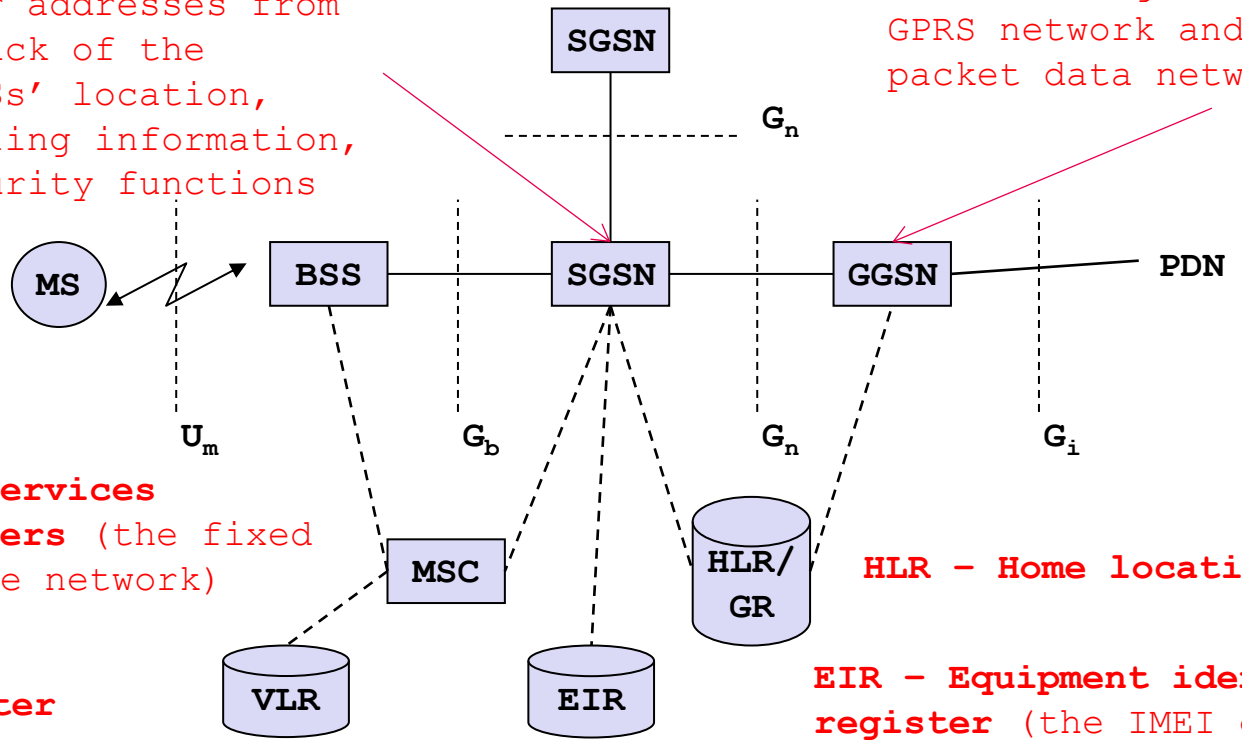
Coding scheme	1 slot	2 slots	3 slots	4 slots	5 slots	6 slots	7 slots	8 slots
CS-1	9.05	18.1	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

GPRS architecture and interfaces

- GPRS network elements
  - **GSN (GPRS Support Nodes):** GGSN and SGSN (routers)
    - **GGSN (Gateway GSN):** interworking unit between GPRS and PDN (Packet Data Network)
    - **SGSN (Serving GSN):** supports the MS (location, billing, security)
  - **GR (GPRS Register):** user addresses

serving GPRS support node requests user addresses from GR, keeps track of the individual MSs' location, collects billing information, performs security functions

gateway GPRS support node Interworking unit between the GPRS network and external packet data networks



MSC – Mobile services switching centers (the fixed backbone of the network)

HLR – Home location register

VLR – Visitor location register

EIR – Equipment identity register (the IMEI database)

examples for GPRS device classes

- The real **available data rate heavily depends on the current load of the cell** as GPRS typically only uses idle time slots
- The **transfer rate depends on the capabilities of the MS** as not all devices are able to send and receive at the same time

Today, a typical MS is a class 10 device using CS-2
This results in a receiving rate of 53.6 kbit/s and a sending rate of 26.8 kbit/s

Class	Receiving slots	Sending slots	Maximum number of slots
1	1	1	2
2	2	1	3
3	2	2	3
5	2	2	4
8	4	1	5
10	4	2	5
12	4	4	5

GPRS quality of service (errors)

- The **three reliability classes** together with the maximum error probabilities
  - *for a lost service data unit (SDU), a duplicated SDU, an SDU out of the original sequence, and the probability of delivering a corrupt SDU to the higher layer*
  - Reliability **class 1** could be used for **very error-sensitive applications** that cannot perform error corrections themselves
  - If applications exhibit **greater error tolerance, class 2** could be appropriate
  - Finally, **class 3** is the choice for **error-insensitive applications** or applications that can handle error corrections themselves

Reliability class	Lost SDU probability	Duplicate SDU probability	Out of sequence SDU probability	Corrupt SDU probability
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

GPRS quality of service (delays)

- The specified **maximum mean and 95 percentile delay values** for packet sizes of 128 and 1,024 byte
  - No matter which class, al**l delays are orders of magnitude higher than fixed network delays**
    - **very important** characteristic that has to be taken into account **when implementing** higher layer protocols such as TCP on top of GPRS networks
  - Typical round trip times (RTT) in fixed networks in the order of **10 to 100ms** - GPRS networks RTTs of **well above 1s** for even small packets (128-512 byte) are common
  - GPRS exhibits a large **jitter** compared to fixed networks (**several 100ms** are not uncommon)
    - has a strong impact on user experience when, e.g., interactive Internet applications are used on top of GPRS

Delay class	SDU size 128 byte		SDU size 1024 byte	
	mean	95 percentile	mean	95 percentile
1	< 0.5 s	< 1.5 s	< 2 s	< 7 s
2	< 5 s	< 25 s	< 15 s	< 75 s
3	< 50 s	< 250 s	< 75 s	< 375 s
4	unspecified			

some current GSM enhancements

- 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
    - not really successful, typically substituted by email with attached multimedia content
  - Today, more and more IP-based messaging used

- 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

GSM resources

- Further reading and resources
  - http://www.gsma.com/aboutus/gsm-technology/gsm
  - http://en.wikipedia.org/wiki/GSM
  - http://www.gsmarena.com/
  - http://www.etsi.org/WebSite/Technologies/gsm.aspx
  - http://www.etsi.org/WebSite/Technologies/gprs.aspx
  - http://www.etsi.org/WebSite/Technologies/edge.aspx

DECT

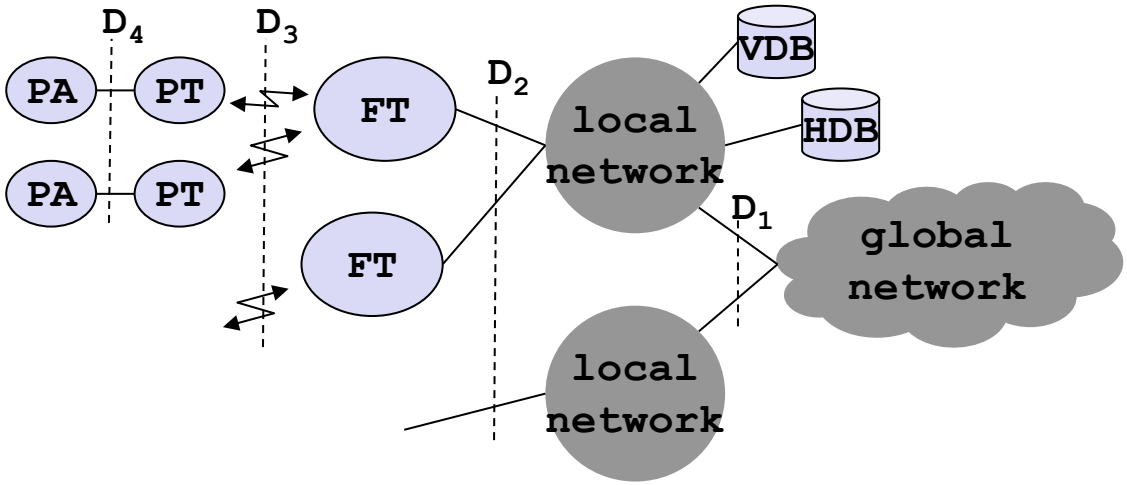
Digital Enhanced Cordless Telecommunications

DECT

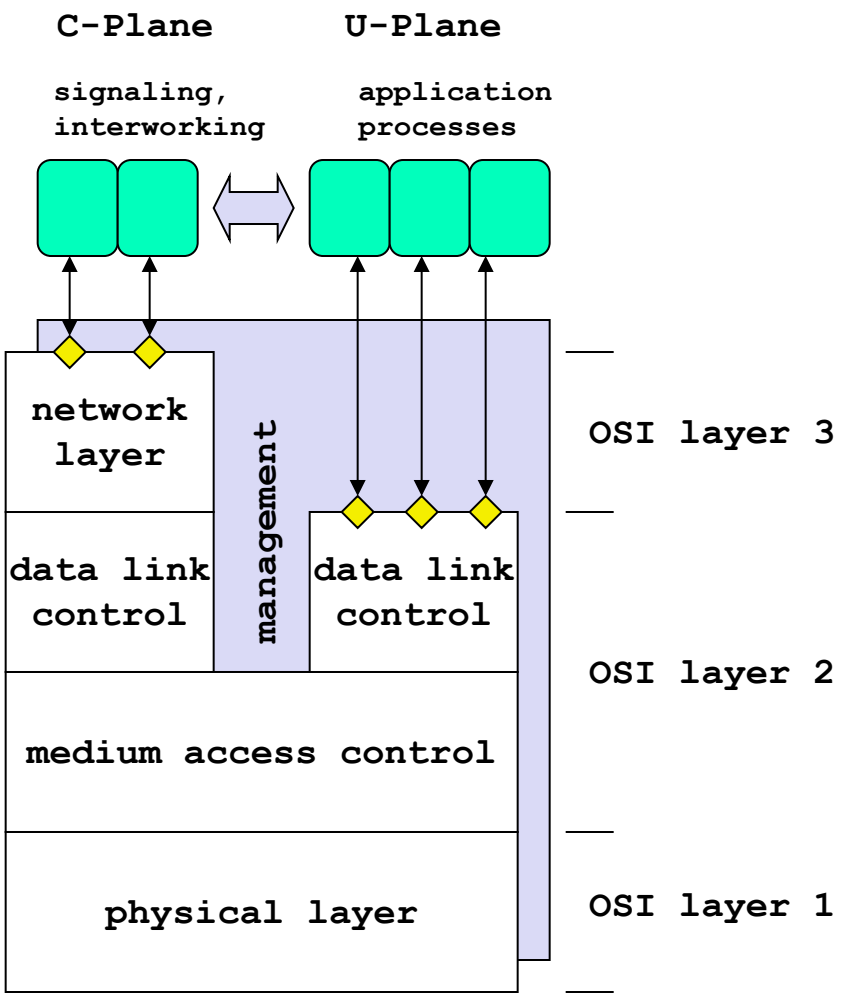
- **DECT (Digital European Cordless Telephone) standardized by ETSI (ETS 300.175-x) for cordless telephones**
  - standard describes air interface between base-station and mobile phone
  - DECT has been renamed for international marketing reasons into **'Digital Enhanced Cordless Telecommunication'**
  - Characteristics
    - **frequency**: 1880-1990 MHz
    - **channels**: 120 full duplex
    - **duplex mechanism**: TDD (Time Division Duplex) with 10 ms frame length
    - **multplexing scheme**: FDMA with 10 carrier frequencies, TDMA with 2x 12 slots
    - **modulation**: digital, Gaussian Minimum Shift Key (GMSK)
    - **power**: 10 mW average (max. 250 mW)
    - **range**: approx. 50 m in buildings, 300 m open space

DECT system architecture ref. model

- A DECT system, may have **various different physical implementation** depending on its actual use
- All implementations are based on **the same logical reference model** of the system architecture
- **Home data base** (HDB) and **visitor data base** (VDB) are also databases that support mobility with functions that are similar to those in the HLR and VLR in GSM
- The DECT core network consists of the **fixed radio termination** (FT) and the **portable radio termination** (PT)
  - basically only provides a multiplexing service
  - additionally, several portable applications (PA) can be implemented on a device



DECT reference model



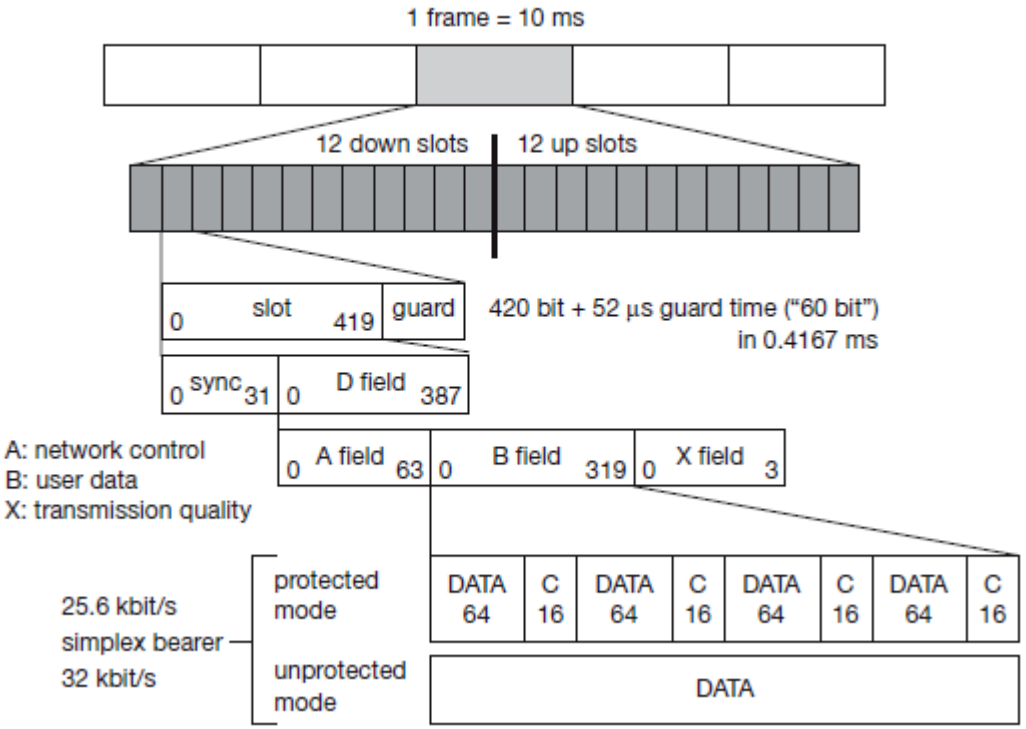
- close to the OSI reference model
- management plane over all layers
- several services in C(ontrol)- and U(ser)-plane

DECT layers

- **Physical layer**
  - functions for modulation/demodulation
  - generation of the physical channel structure with a guaranteed throughput
  - controlling of radio transmission
    - channel assignment on request of the MAC layer
    - detection of incoming signals
    - sender/receiver synchronization
    - collecting status information for the management plane
- **MAC layer**
  - maintaining basic services, activating/deactivating physical channels
  - multiplexing of logical channels
    - e.g., C: signaling, I: user data, P: paging, Q: broadcast
  - segmentation/reassembly
  - error control/error correction

DECT time multiplex frame

- The **standard TDMA frame structure** used in DECT and some typical data packets
  - If a mobile node receives data in slot s, it returns data in slot s+12
  - Each slot has a duration of 0.4167 ms



DECT layers

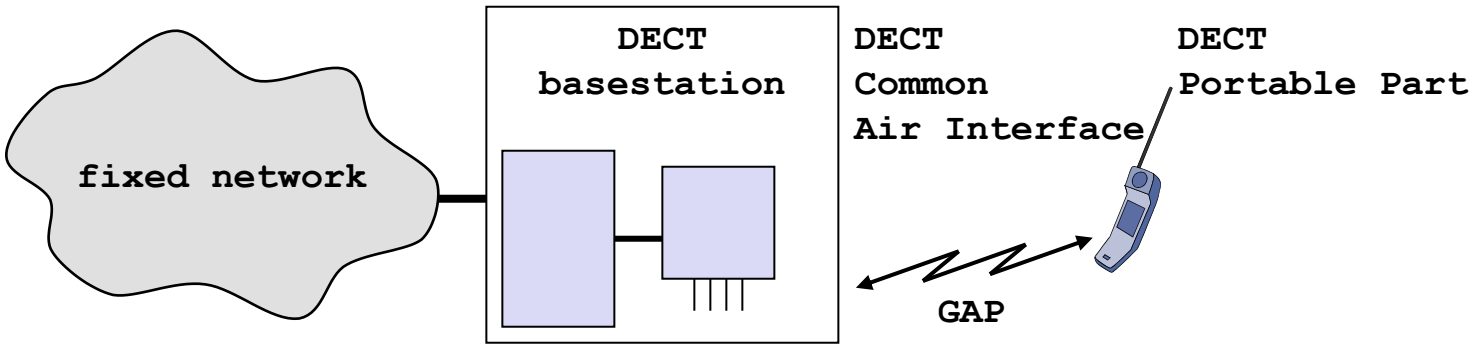
- **Data link control layer**
  - creates and maintains reliable connections between the mobile terminal and base station
  - **two services for the control plane (C-Plane)**
    - **connectionless broadcast service:** paging functionality
    - **Point-to-point (Lc+LAPC) protocol:** in-call signaling adapted to the underlying MAC service
  - **several services specified for the user plane (U-Plane)**
    - **null-service:** offers unmodified MAC services
    - **frame relay:** simple packet transmission
    - **frame switching:** time-bounded packet transmission
    - **error correcting transmission:** uses FEC, for delay critical, time-bounded services
    - **bandwidth adaptive transmission**
    - **"Escape" service:** for further enhancements of the standard

DECT layers

- Network layer
  - **similar to ISDN (Q.931) and GSM (04.08)**
  - **offers services** to request, check, reserve, control, and release resources at the base station and mobile terminal
  - main tasks
    - **call control:** setup, release, negotiation, control
    - **call independent services:** call forwarding, accounting, call redirecting
    - **mobility management:** identity management, authentication, management of the location register

enhancements of the standard

- Several 'DECT Application Profiles' in addition to the DECT specification
  - **GAP** (Generic Access Profile) standardized by ETSI in 1997
    - assures **interoperability** between DECT equipment of different manufacturers (minimal requirements for voice communication)
    - **enhanced management capabilities** through the fixed network: Cordless Terminal Mobility (CTM)



  - **DECT/GSM** Interworking Profile (GIP): connection to GSM
  - **ISDN** Interworking Profiles (IAP, IIP): connection to ISDN
  - **RAP** (Radio Local Loop Access Profile): public telephone service
  - **CAP** (CTM Access Profile): support for user mobility

DECT resources

- Further reading and resources
  - http://www.dect.org/
  - http://www.dect.org/userfiles/file/General%5CDECT%20Background/DECT_Technical%20Document_1997.pdf
  - http://www.wavelink.com.au/information/dect-the-standard-explained.php
  - http://en.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications

TETRA

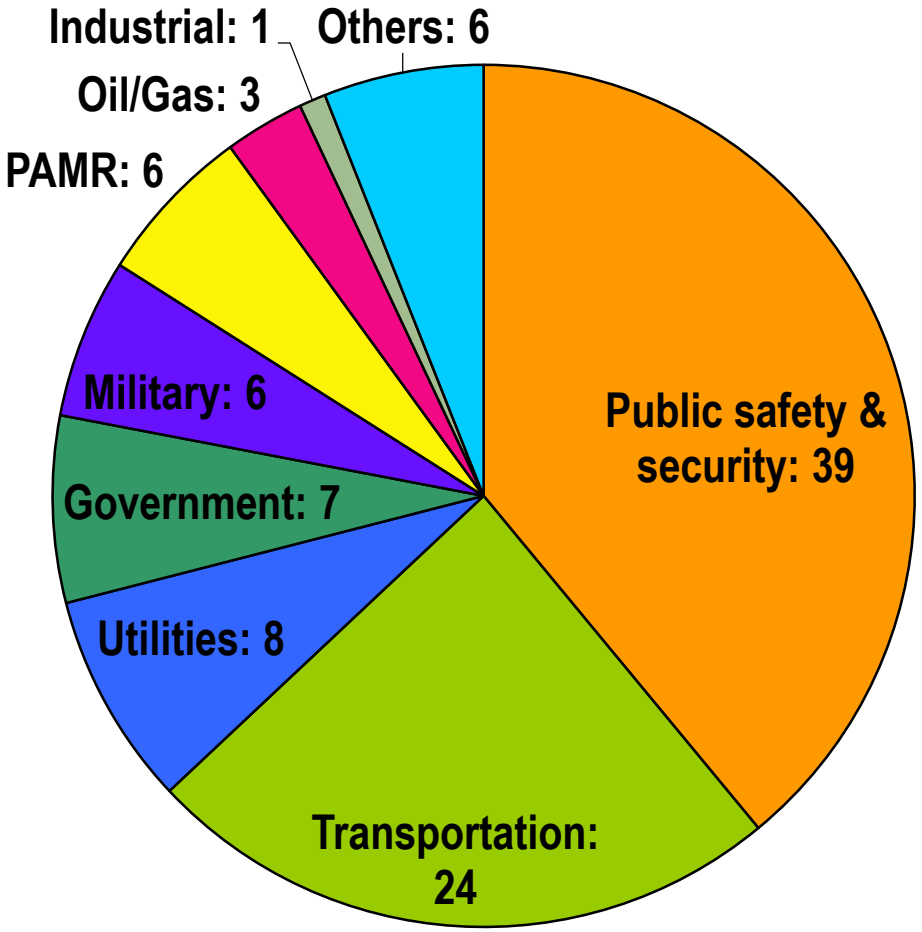
Terrestrial Trunked Radio

TETRA - terrestrial trunked radio

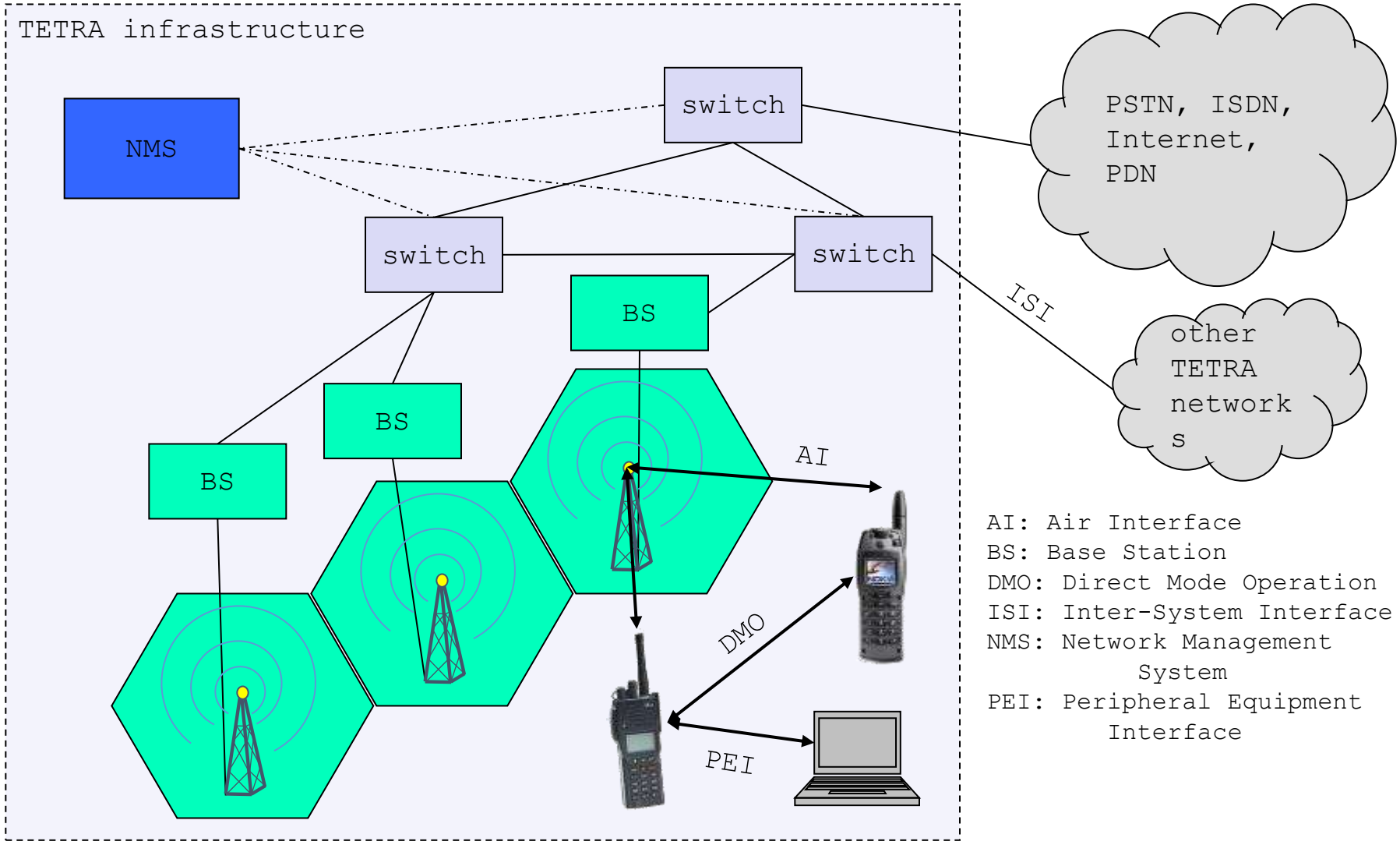
- Trunked radio systems
  - **many different radio carriers:** assign single carrier for a short period to one user/group of users
  - **support local usage:** taxi service, fleet management, rescue teams
  - **interfaces** to public networks, voice and data services
  - **pros:** very reliable, cheaper, fast call setup, local operation
- TETRA - ETSI standard (started 1991)
  - formerly: Trans European Trunked Radio
  - **point-to-point** and **point-to-multipoint**
  - **encryption** (end-to-end, air interface), **authentication** of devices, users and networks
  - group call, broadcast, sub-second group-call setup
  - **ad-hoc** ("direct mode" no base station), relay and infrastructure networks
  - **call queuing** with preemptive priorities

TETRA – contracts by sector (percentage)

Used in over 70 countries, more than 20 device manufacturers



TETRA – network architecture



AI: Air Interface
BS: Base Station
DMO: Direct Mode Operation
ISI: Inter-System Interface
NMS: Network Management System
PEI: Peripheral Equipment Interface

TETRA operation modes

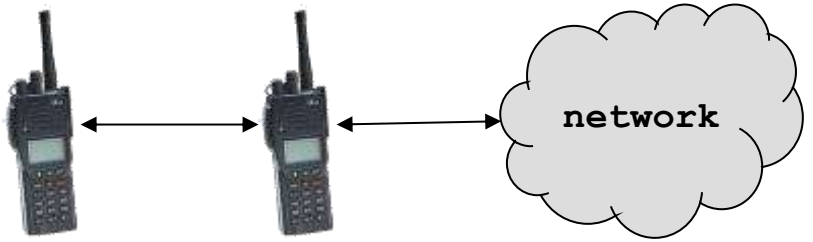
- Two modes of operation
  - Trunked Mode Operation (TMO) and Direct Mode Operation (DMO)
  - TMO means using TETRA **mobile radios in combination with network infrastructure** while
  - DMO is TETRA radio communication **between mobile radios** without using a TETRA network infrastructure
- **Trunked Mode Operation (TMO)**
  - When a TETRA mobile radio starts a groupcall by pressing the "Push To Talk" (PTT) audio will be transmitted to the selected TETRA basestation, while other radios that have the same talkgroup selected and are located in a different geographical area and are being served by a different TETRA basestation receive the audio via their basestation, using the **network intelligence** to assign a channels and transport the audio from sender to receiver
- **Direct Mode Operation (DMO)**
  - In DMO mode the TETRA mobile stations **communicate directly** with each other without using the TETRA infrastructure, while the stay within coverage of each other (DMO is often used in situation were coverage of TETRA network infrastructure is not available)

TETRA – direct mode

- **Direct Mode** enables ad-hoc operation and is one of the most important differences to pure infrastructure-based networks such as GSM, cdma2000 or UMTS.

Individual Call

Group Call



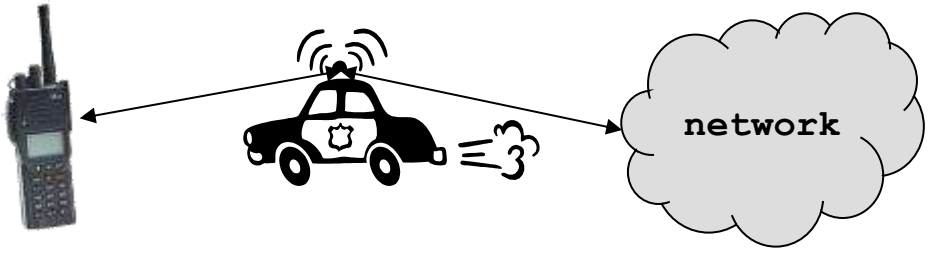
"Dual Watch" – alternating participation in Infrastructure and ad-hoc

Managed Direct Mode

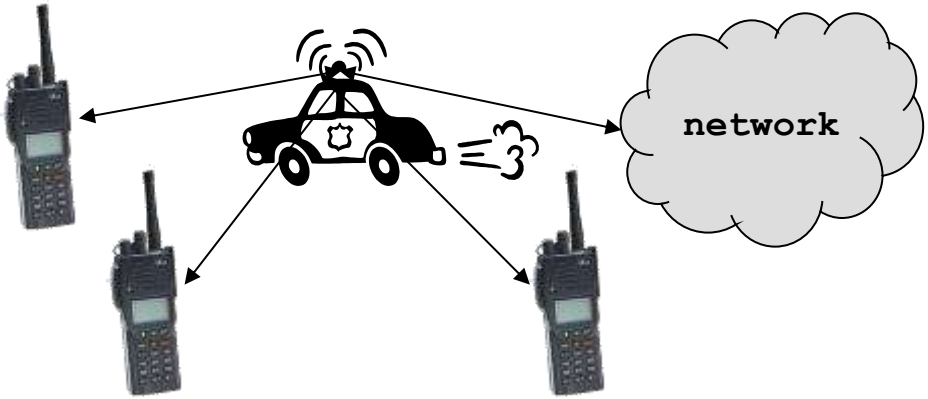
TETRA – direct mode

- An additional **repeater** may increase the transmission range (e.g. police car)
- Can aid even when **underground** or in **bad coverage** areas

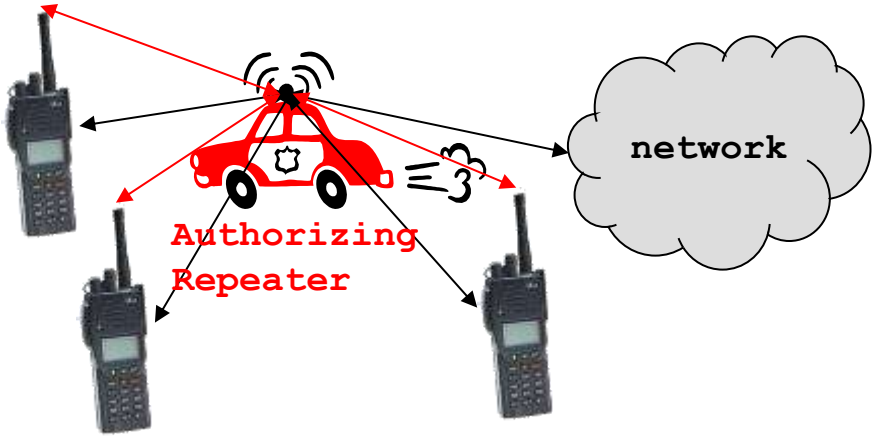
Direct Mode with Repeater



Direct Mode with Gateway



Direct Mode with Repeater/Gateway



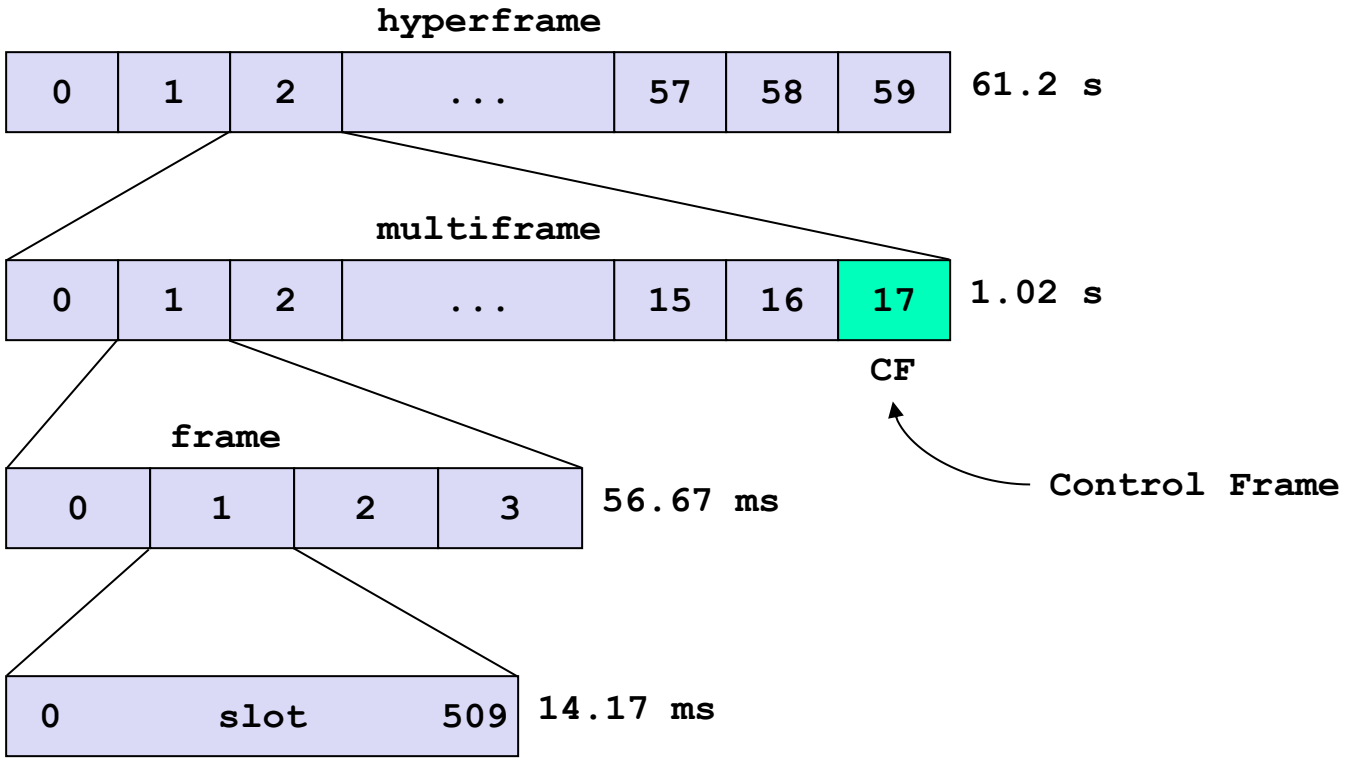
Managed Repeater/Gateway

TETRA – technology

- Services
  - Voice+Data (V+D) and Packet Data Optimized (PDO)
  - Short data service (SDS)
- Frequencies
  - Duplex: FDD, Modulation: DQPSK
  - Europe (in MHz, not all available yet)
    - 380-390 UL / 390-400 DL; 410-420 UL / 420-430 DL, 450-460 UL / 460-470 DL; 870-876 UL / 915-921 DL
  - Other countries
    - 380-390 UL / 390-400 DL; 410-420 UL / 420-430 DL, 806-821 UL / 851-866 DL

TDMA structure of the voice data system

- Typical **TDMA frame structure** of TETRA
  - Each **slot** carries 510 bits within 14.17 ms (i.e. 36 kbps)
  - Each **frame** consists of 4 slots (4 channels in the V+D service per carrier), with a duration of 56.67 ms
  - 16 frames together with one **control frame** (CF) form a **multiframe**
  - a **hyperframe** contains 60 multiframes



TETRA – data rates

- Infrastructure mode, V+D in kbit/s

No. of time slots	1	2	3	4
No protection	7.2	14.4	21.6	28.8
Low protection	4.8	9.6	14.4	19.2
High protection	2.4	4.8	7.2	9.6

- TETRA Release 2 – Supporting higher data rates
  - **TEDS (TETRA Enhanced Data Service)**
  - up to 100-500 kbit/s
    - depends on modulation (DQPSK, D8PSK, 4/16/64QAM) and channel width (25/50/100/150 kHz)
  - backward compatibility

TETRA resources

- Further reading and resources
  - http://www.tandcca.com/about/page/12030
  - http://www.tetra-consultancy.com/
  - http://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio

3G
UMTS and IMT-2000

Universal Mobile Telecommunications System

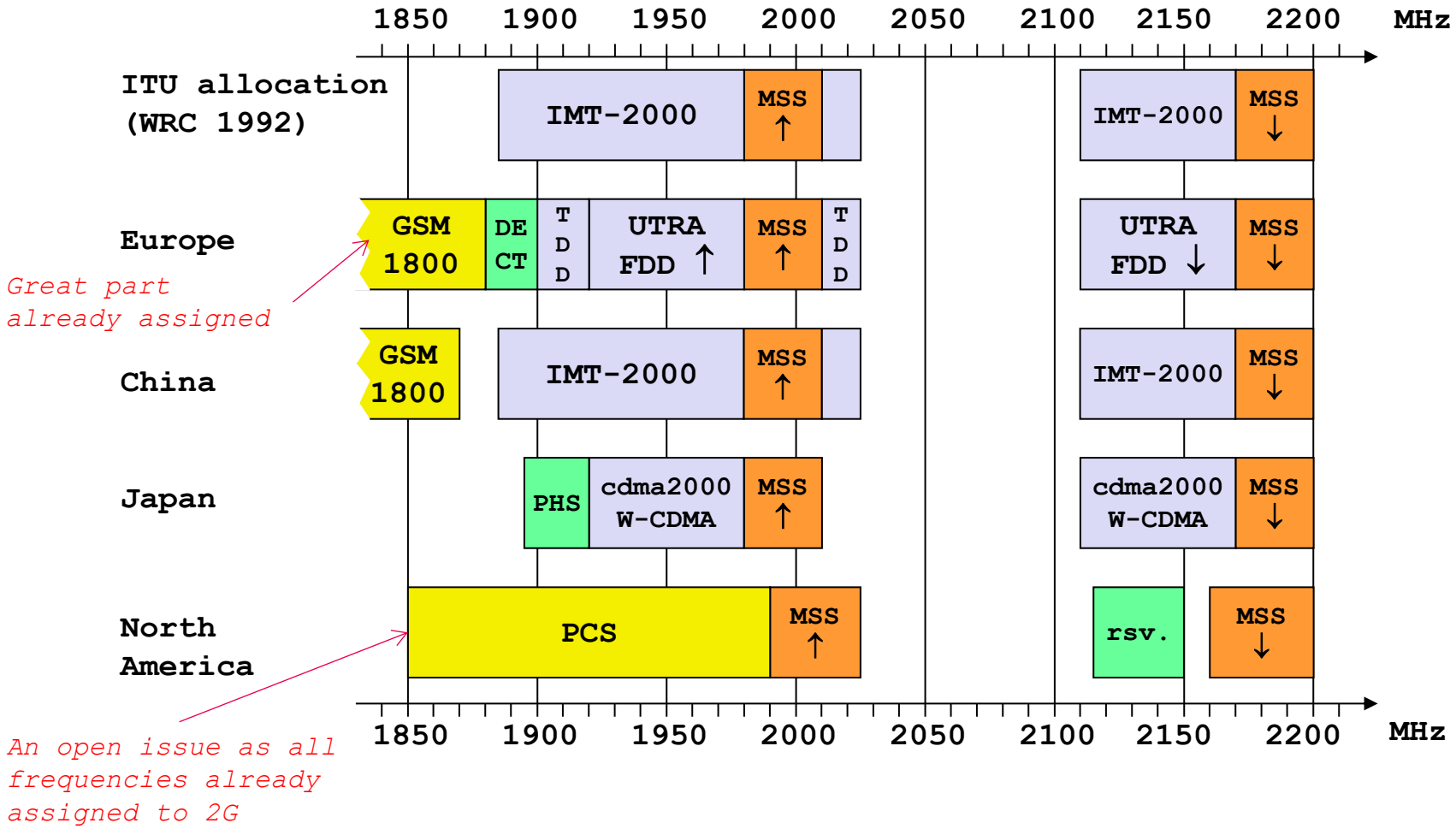
International Mobile Telecommunications-2000

UMTS and IMT-2000

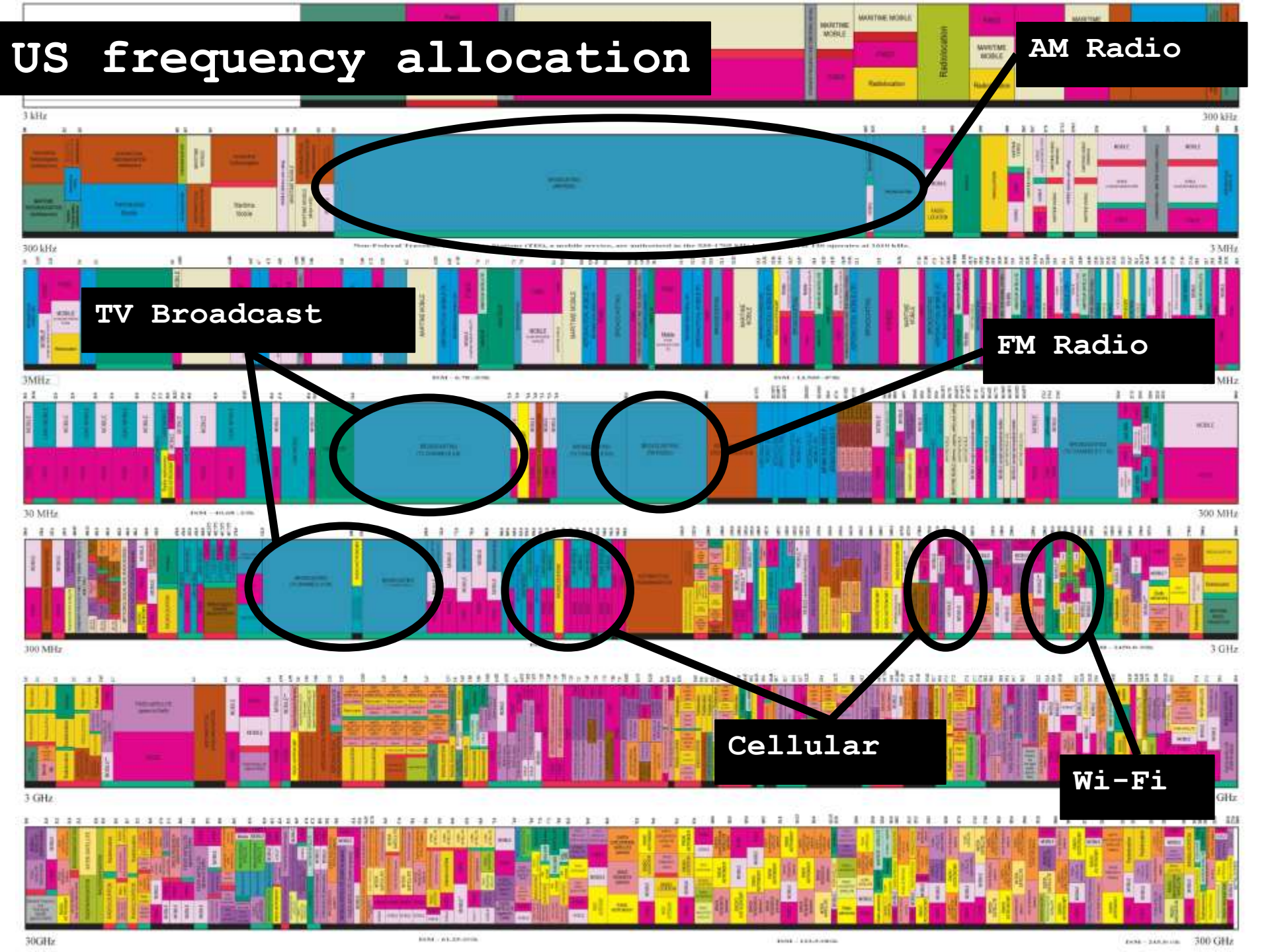
- It all started after an ITU request for proposals for IMT-2000 (International Mobile Telecommunications), 2002
  - formerly called Future Public Land Mobile Telecommunication System (FPLMTS)
  - 2000 stands for the years 200x and the spectrum used around 2000MHz
  - standards invovled: UWC-136 (EDGE), cdma2000, WP-CDMA, UMTS (Universal Mobile Telecommunications System) from ETSI (+DECT, WiMAX)
- UMTS
  - 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) – to support roaming
  - fits into GMM (Global Multimedia Mobility) ETSI initiative
  - 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

- ITU frequency allocation with examples from several regions that already indicate the problem of worldwide common frequency bands

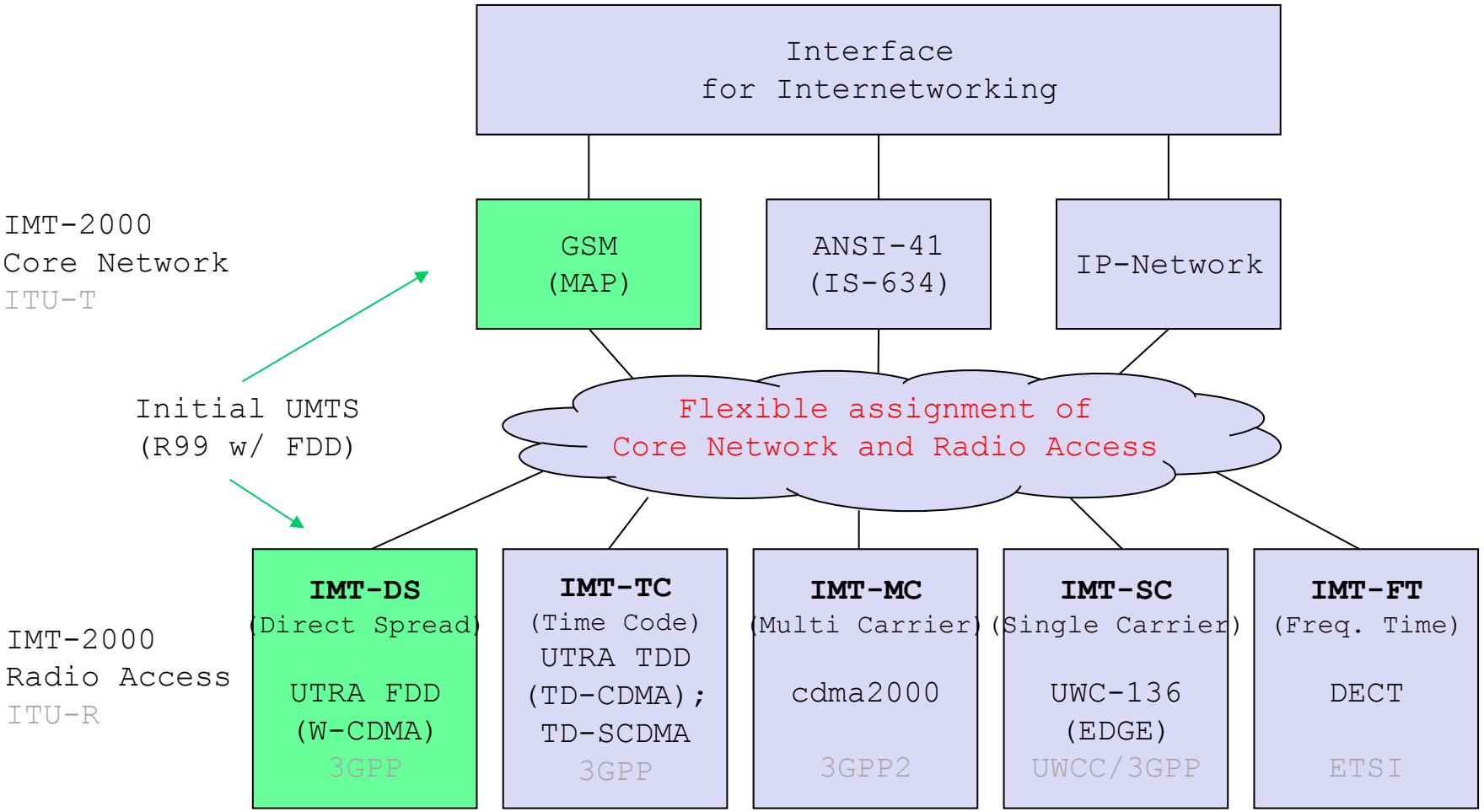


US frequency allocation



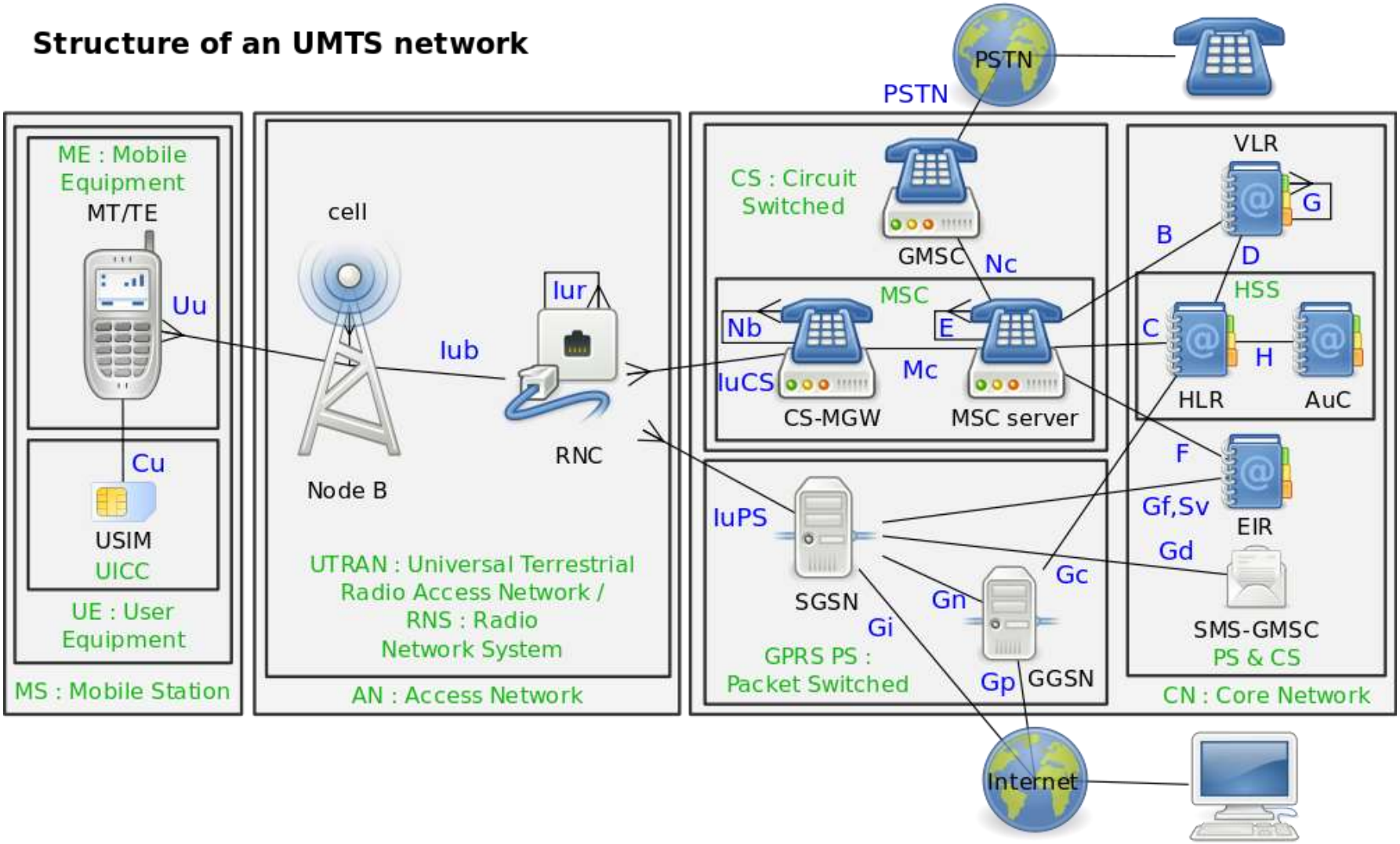
IMT-2000 family

- As a single standard could not be found, the ITU standardized **five groups** of 3G radio access technologies
- One great idea of IMT-2000 is the **flexible assignment** of a core network to a radio access system



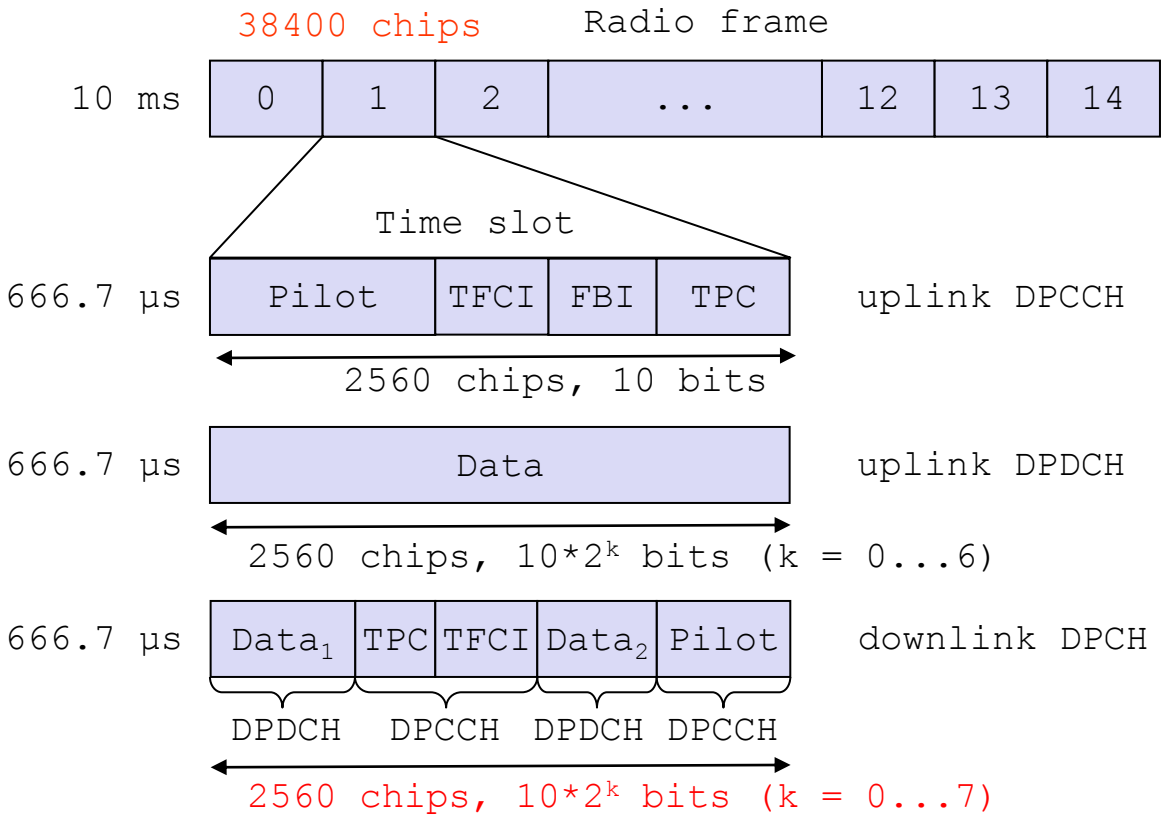
structure of a UMTS network

- Similar to GSM in principle



UMTS FDD frame structure

- FDD – frequency division duplexing



W-CDMA

- 1920-1980 MHz uplink
- 2110-2170 MHz downlink
- chipping rate: 3.840 Mchip/s
- soft handover
- QPSK
- complex power control (1500 power control cycles/s)
- spreading: UL: 4-256; DL:4-512

Time slots here are not used to seperate user as in GSM (they support periodic functions)

FBI: Feedback Information
TPC: Transmit Power Control
TFCI: Transport Format Combination Indicator
DPCCH: Dedicated Physical Control Channel
DPDCH: Dedicated Physical Data Channel
DPCH: Dedicated Physical Channel

typical UTRA-FDD uplink data rates

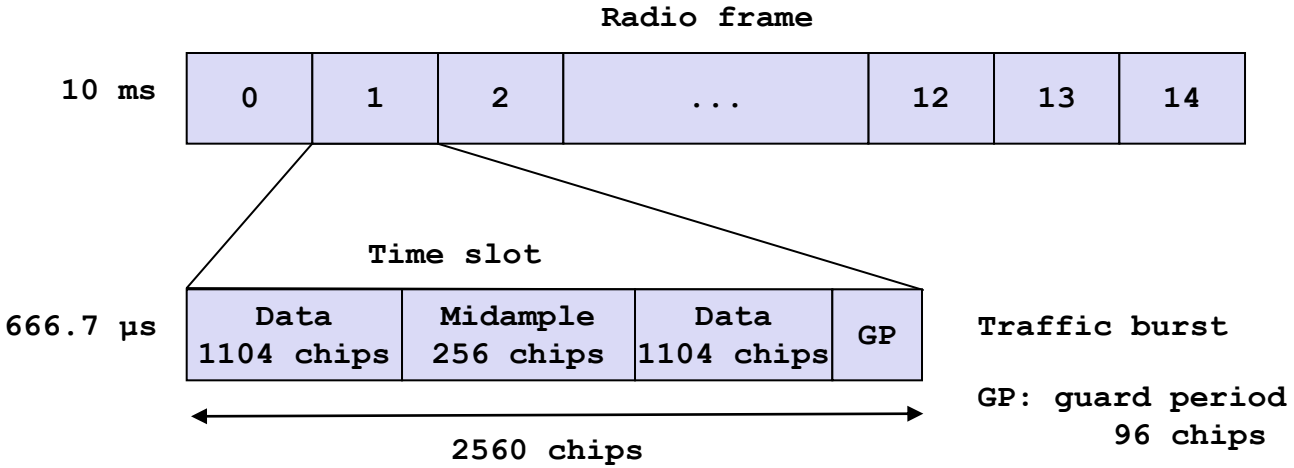
- Typical user data rates together with the required data rates on the physical channels
  - **Dedicated physical data channel (DPDCH):** This channel conveys user or signaling data, with spreading factor varying between 4 and 256
  - **Dedicated physical control channel (DPCCH):** This channel conveys control data for the physical layer only and uses the constant spreading factor 256

User data rate [kbit/s]	**12.2 (voice)**	**64**	**144**	**384**
DPDCH [kbit/s]	60	240	480	**960**
DPCCH [kbit/s]	15	15	15	15
Spreading	64	16	8	4

Example DPDCH: *960 kbit/s (spreading factor 4, 640 bits per slot, 15 slots per frame, 100 frames per second)*

UMTS TDD frame structure

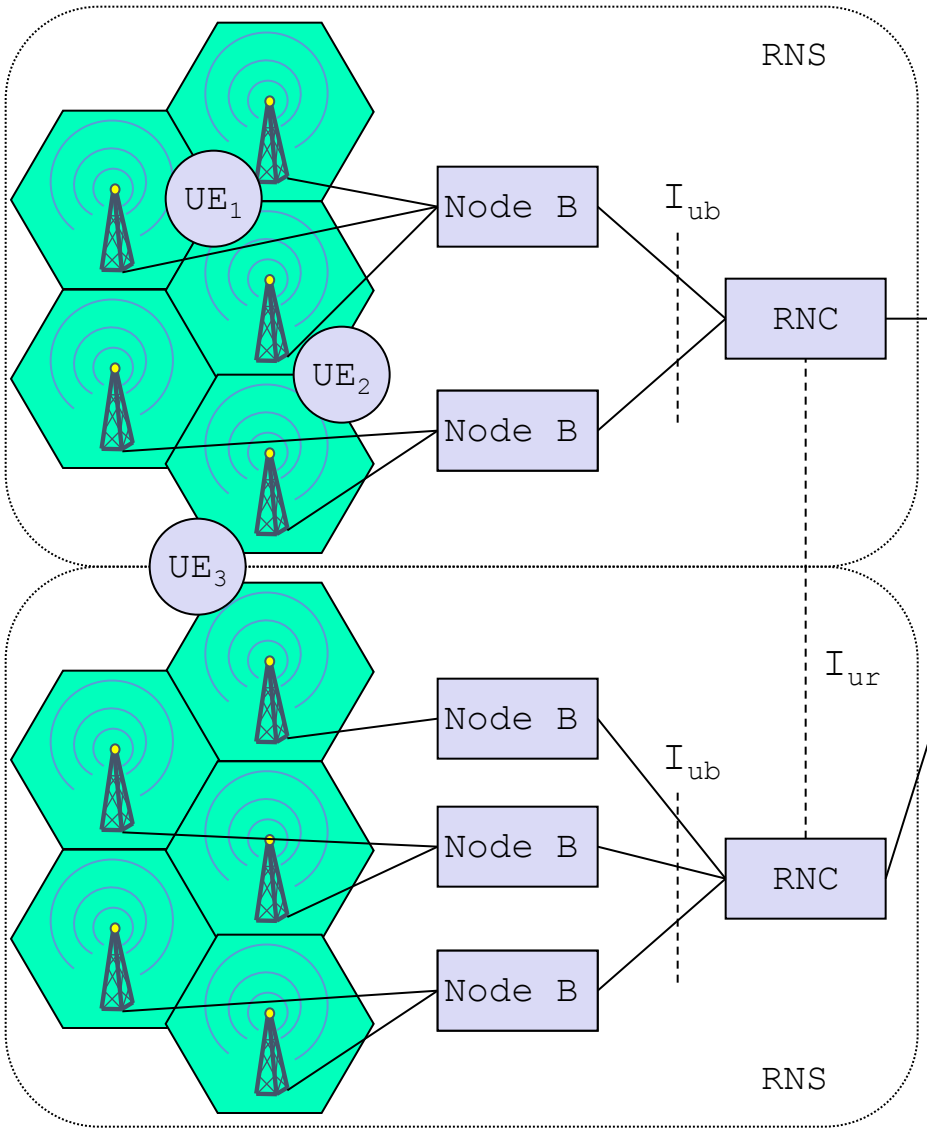
- TDD – time division duplexing



TD-CDMA

- 2560 chips per slot
- spreading: 1-16
- symmetric or asymmetric slot assignment to UL/DL (min. 1 per direction)
- tight synchronization needed
- simpler power control (100-800 power control cycles/s)

UTRAN architecture



CN: Core Network

RNC: Radio Network Controller

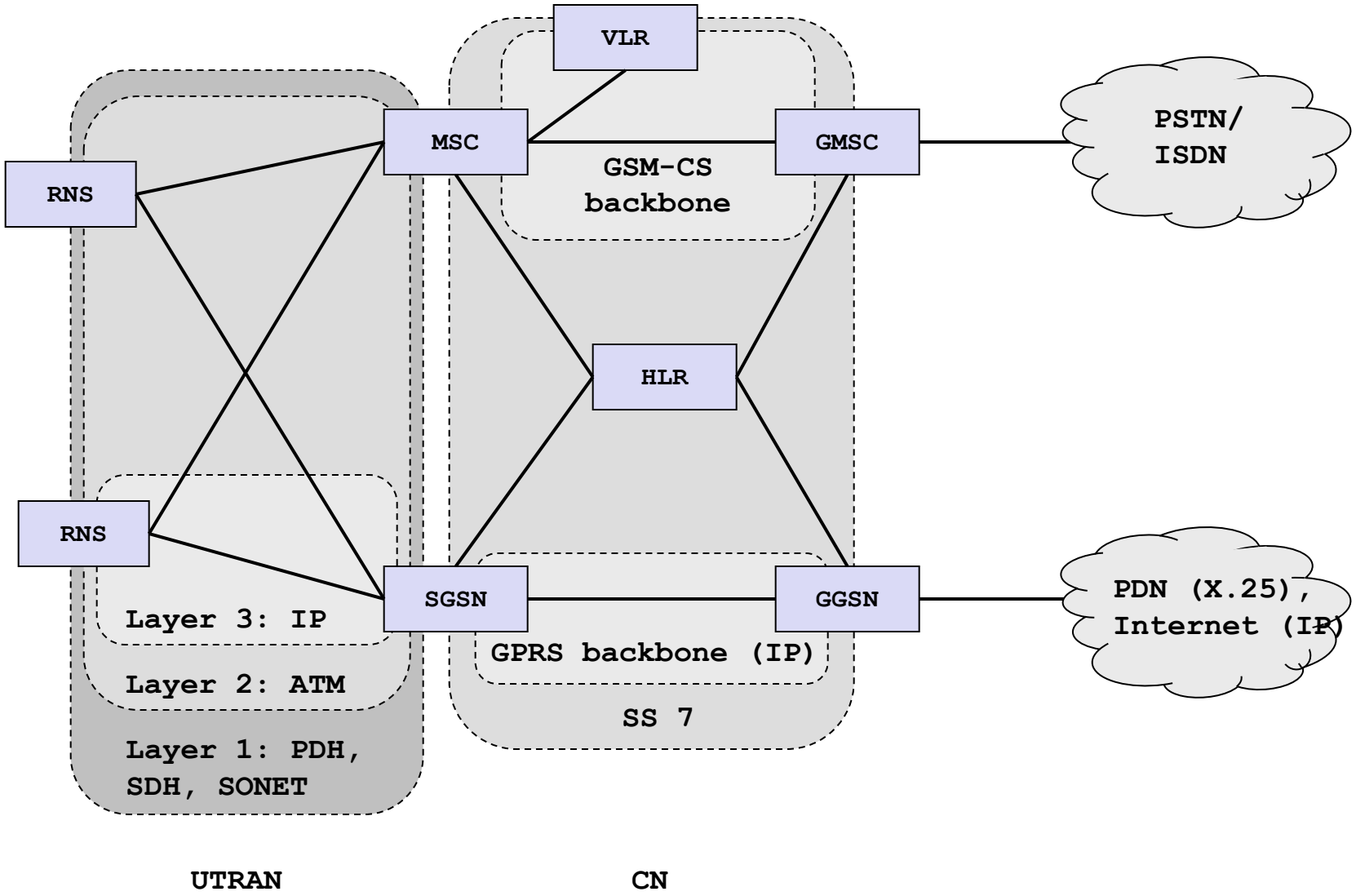
RNS: Radio Network Subsystem

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

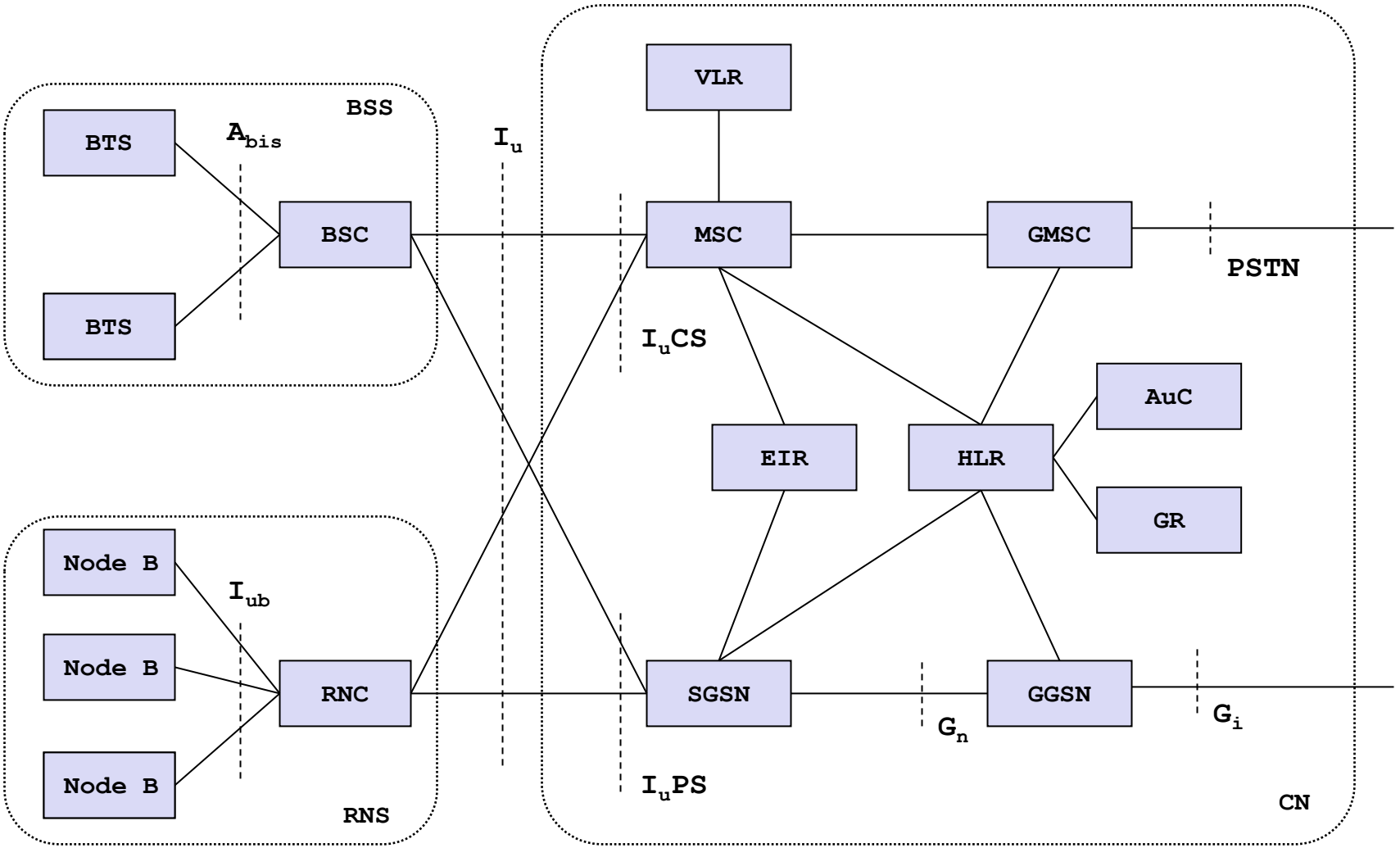
UTRAN RNC functions

- Admission control (traffic and interference)
- Congestion control (cyclic bandwidth allocation)
- System information broadcasting
- Radio channel encryption
- Handover
- RNS relocation
- Radio network configuration
- Channel quality measurements
- Macro diversity
- Radio carrier control
- Radio resource control
- Data transmission over the radio interface
- Outer loop power control (FDD and TDD)
- Channel coding
- Access control

core network: protocols



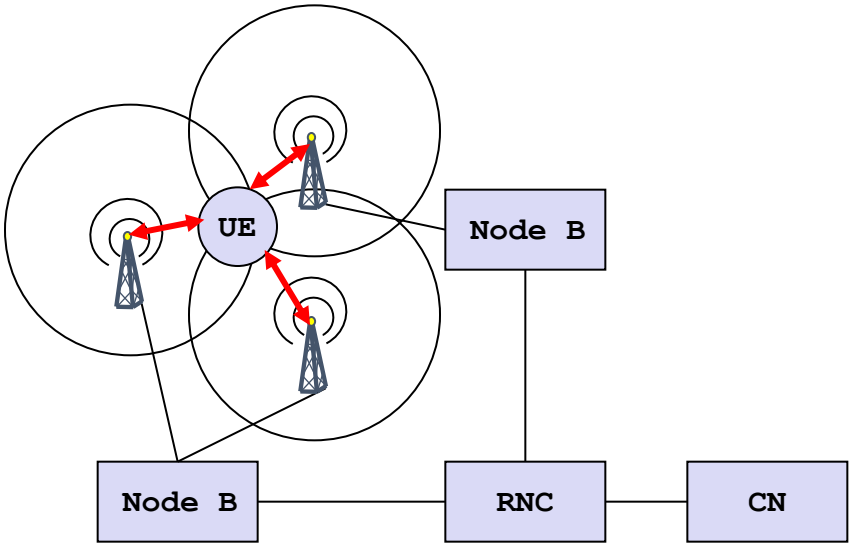
core network: architecture



core network

- The Core Network (CN) and thus the Interface I_u, too, are separated into two logical domains:
  - **Circuit Switched Domain (CSD)**
    - Circuit switched service incl. signaling
    - Resource reservation at connection setup
    - GSM components (MSC, GMSC, VLR)
    - I_uCS
  - **Packet Switched Domain (PSD)**
    - GPRS components (SGSN, GGSN)
    - I_uPS
- Release 99 uses the GSM/GPRS network and adds a new radio access!
  - Helps to save a lot of money …
  - Much faster deployment
  - Not as flexible as newer releases (5, 6, … 12)

support of mobility: macro diversity

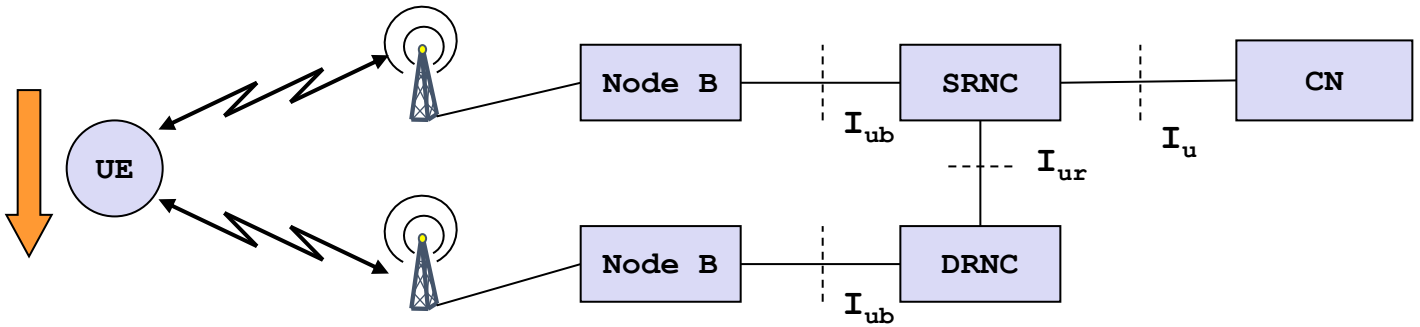


a UE can receive signals from up to three different antennas, which may belong to different Node Bs

- Multicasting of data via several physical channels
  - Enables soft handover
  - FDD mode only
- Uplink
  - simultaneous reception of UE data at several Node Bs
  - Reconstruction of data at Node B, SRNC or DRNC
- Downlink
  - Simultaneous transmission of data via different cells
  - Different spreading codes in different cells
- The UE combines the received data again

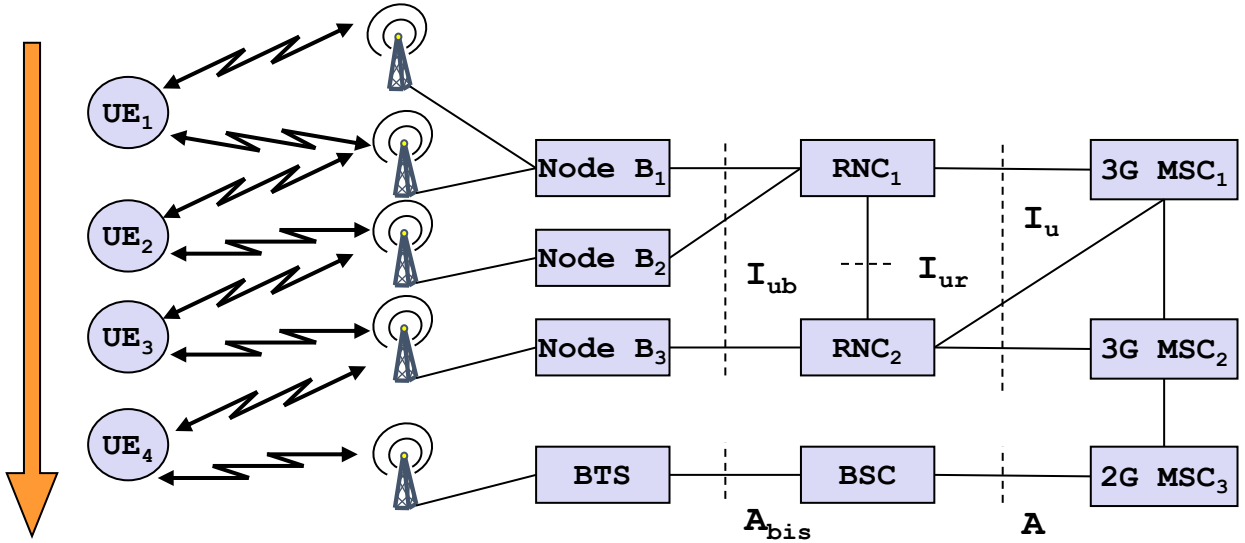
support of mobility: handover

- **From and to other systems** (e.g., UMTS to GSM)
  - This is a must as UMTS coverage will be poor in the beginning
- RNS controlling the connection is called SRNS (**Serving RNS**)
- RNS offering additional resources (e.g., for soft handover) is called **Drift RNS** (DRNS)
- End-to-end connections between UE and CN only via I_u at the SRNS
  - Change of SRNS requires change of I_u
  - Initiated by the SRNS
  - Controlled by the RNC and CN



example handover types in UMTS/GSM

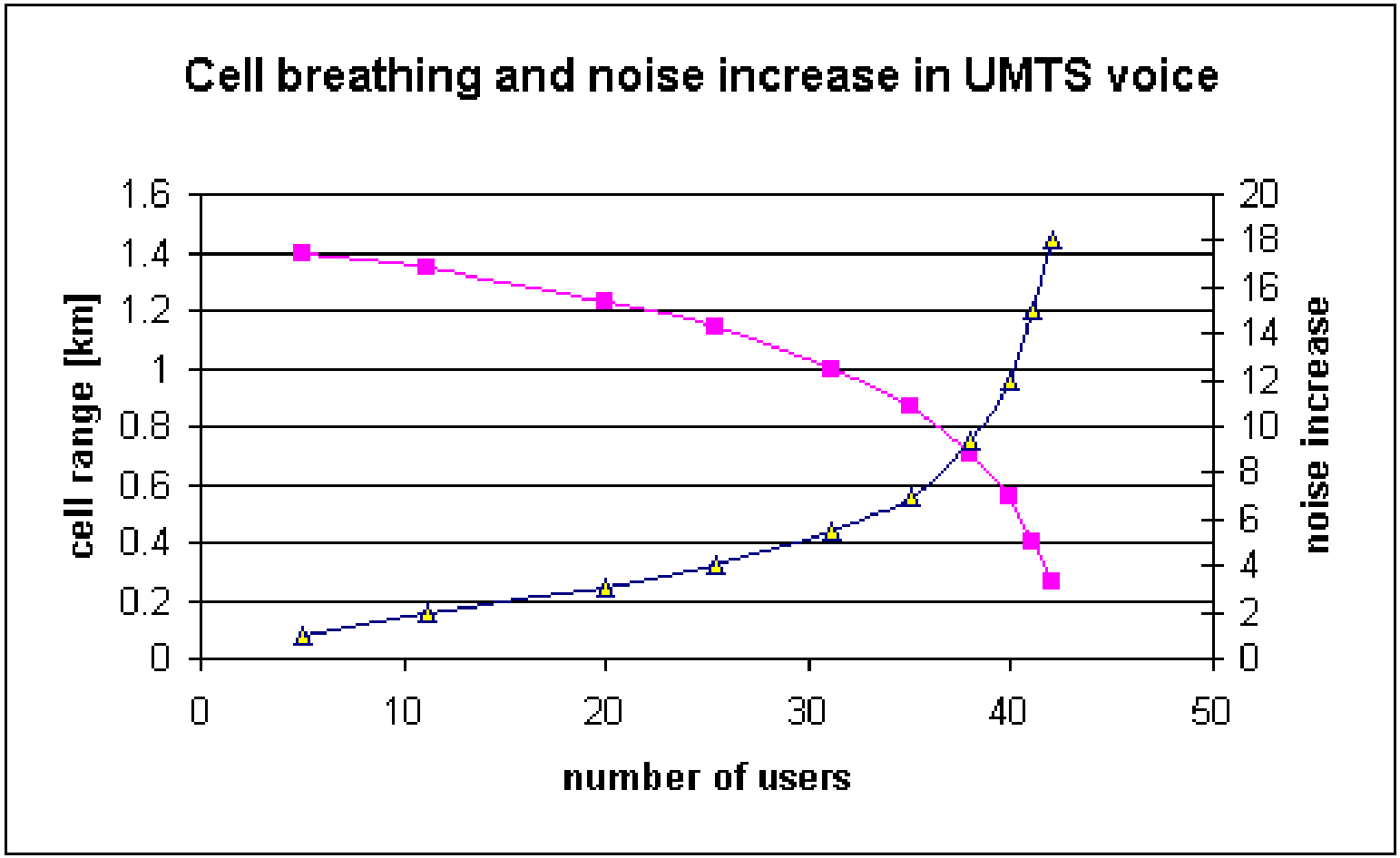
- Overview of several common handover types in a combined UMTS/GSM network (UMTS specifies ten different types which include soft and hard handover)
  - **Intra-node B, intra-RNC:** UE1 moves from one antenna of node B1 to another antenna (**softer handover)**
  - **Inter-node B, intra-RNC:** UE2 moves from node B1 to node B2. In this case RNC1 supports the **soft handover**
  - **Inter-RNC:** When UE3 moves from node B2 to node B3 two different types of handover can take place: **internal inter-RNC (**RNC1 acts as SRNC, RNC2 as DRNC) and **external inter-RNC**
  - **Inter-MSC:** It could be also the case that MSC2 takes over and performs a **hard handover** of the connection
  - **Inter-system:** UE4 moves from a 3G UMTS network into a 2G GSM network (**hard handover**)



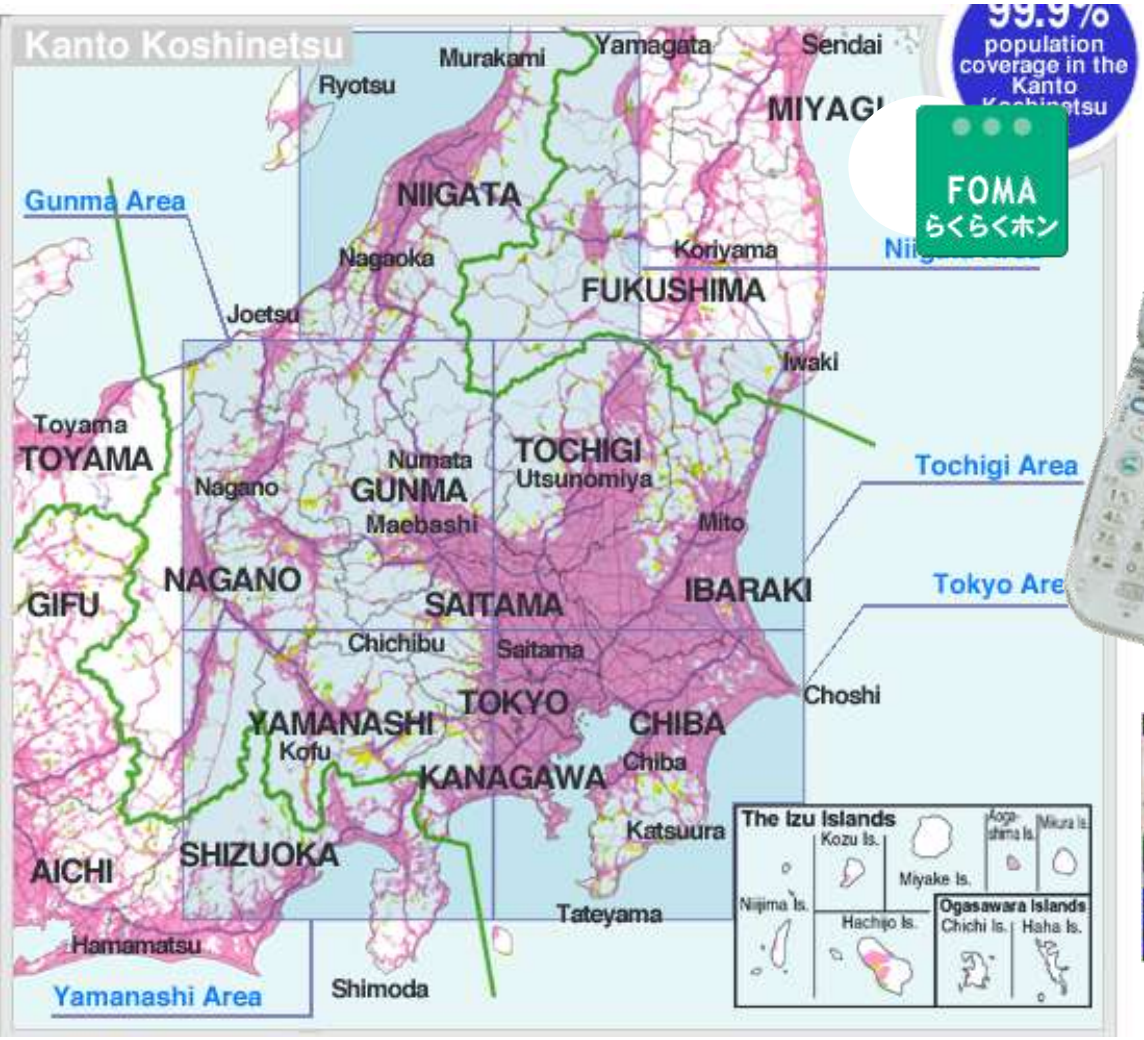
breathing cells

- **Cell breathing** is a mechanism that allows overloaded cells to offload traffic to neighboring cells by changing their size
- **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-nose 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



early 3G networks: Japan, 2001



FOMA (Freedom Of Mobile multimedia Access) in Japan

With Videophone you can enjoy conversations while facing each other.

Examples for FOMA phones

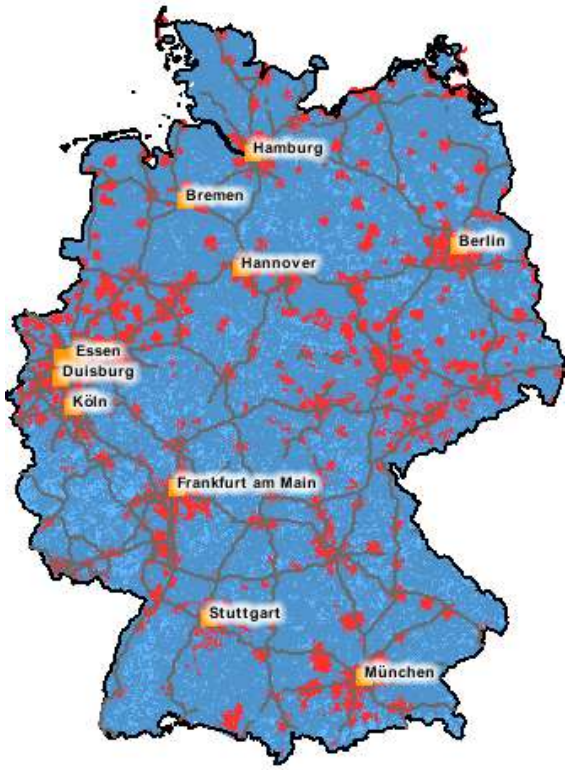
isle of Man, 2001 – start of UMTS in Europe

early 3G networks: Australia, 2002

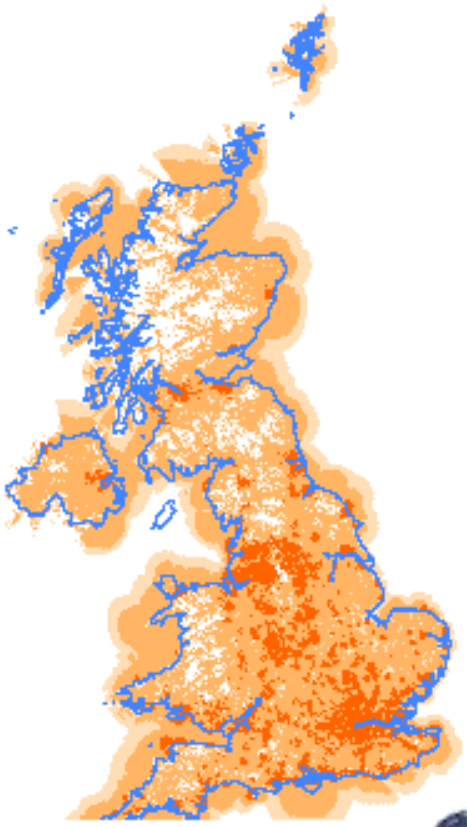
cdma2000 1xEV-DO in Melbourne/Australia

Examples for 1xEV-DO devices

early UMTS in Europe



Vodafone/Germany



Orange/UK

some current UMTS enhancements

- **HSDPA** (High-Speed Downlink Packet Access)
  - initially up to 10 Mbit/s for the downlink, later > 20 Mbit/s using MIMO 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)

IMT-2000/3G resources

- Further reading and resources
  - http://www.itu.int/osg/imt-project/docs/What_is_IMT2000.ppt
  - http://www.itu.int/ITU-D/imt-2000/DocumentsIMT2000/What_really_3G.pdf
  - http://tikonaplans.blogspot.in/2012/07/3g-cellular-standards-and.html
  - http://www.engpaper.com/3g-cellular-standards-and-patents.html
  - http://www.3gpp.org/
  - http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/imt-2000
  - http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/umts

Long Term Evolution

long term evolution (LTE)

- **Initiated in 2004 by NTT DoCoMo,** 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, RTT<10ms**
  - **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)
- **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**!
- Large step towards 4G – IMT advanced

- See www.3gpp.org for all specs, tables, figures etc

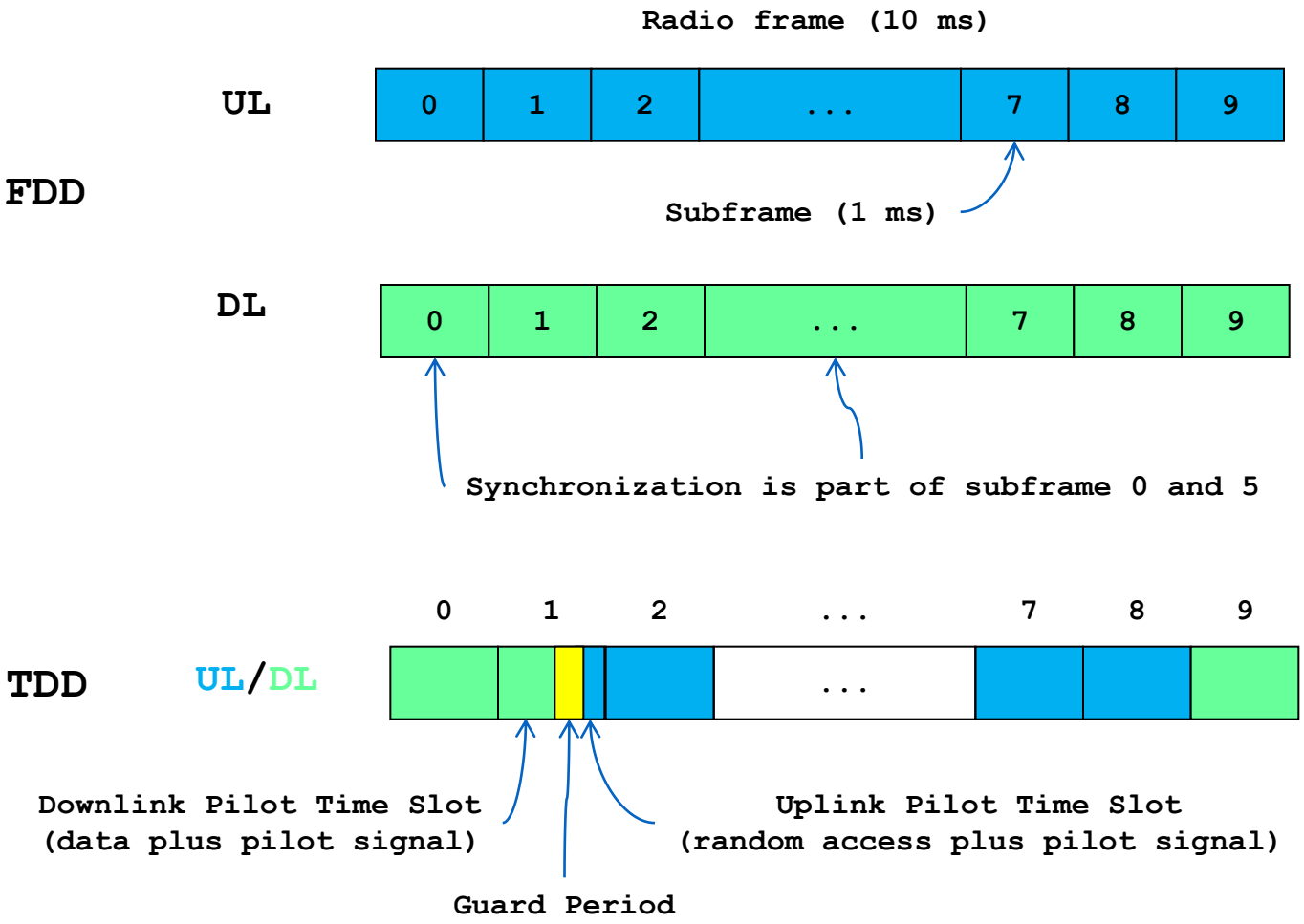
high flexibility

- E-UTRA (Evolved Universal Terrestrial Radio Access)
  - Operating bands 700-2700MHz
  - Channel bandwidth 1.4, 3, 5, 10, 15, or 20 MHz
  - TDD and FDD
- Modulation
  - QPSK, 16QAM, 64QAM
- Multiple Access
  - OFDMA (DL), SC-FDMA (UL)
- **Peak data rates**
  - 300 Mbit/s DL
  - 75 Mbit/s UL
  - Depends on UE category
- **Cell radius**
  - From <1km to 100km

E-UTRA Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	F_{UL_low} – F_{UL_high}	F_{DL_low} – F_{DL_high}	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6[1]	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD
7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9 MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
15	Reserved	Reserved	FDD
16	Reserved	Reserved	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
18	815 MHz – 830 MHz	860 MHz – 875 MHz	FDD
19	830 MHz – 845 MHz	875 MHz – 890 MHz	FDD
20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
21	1447.9 MHz – 1462.9 MHz	1495.9 MHz – 1510.9 MHz	FDD
...			
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD
36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD

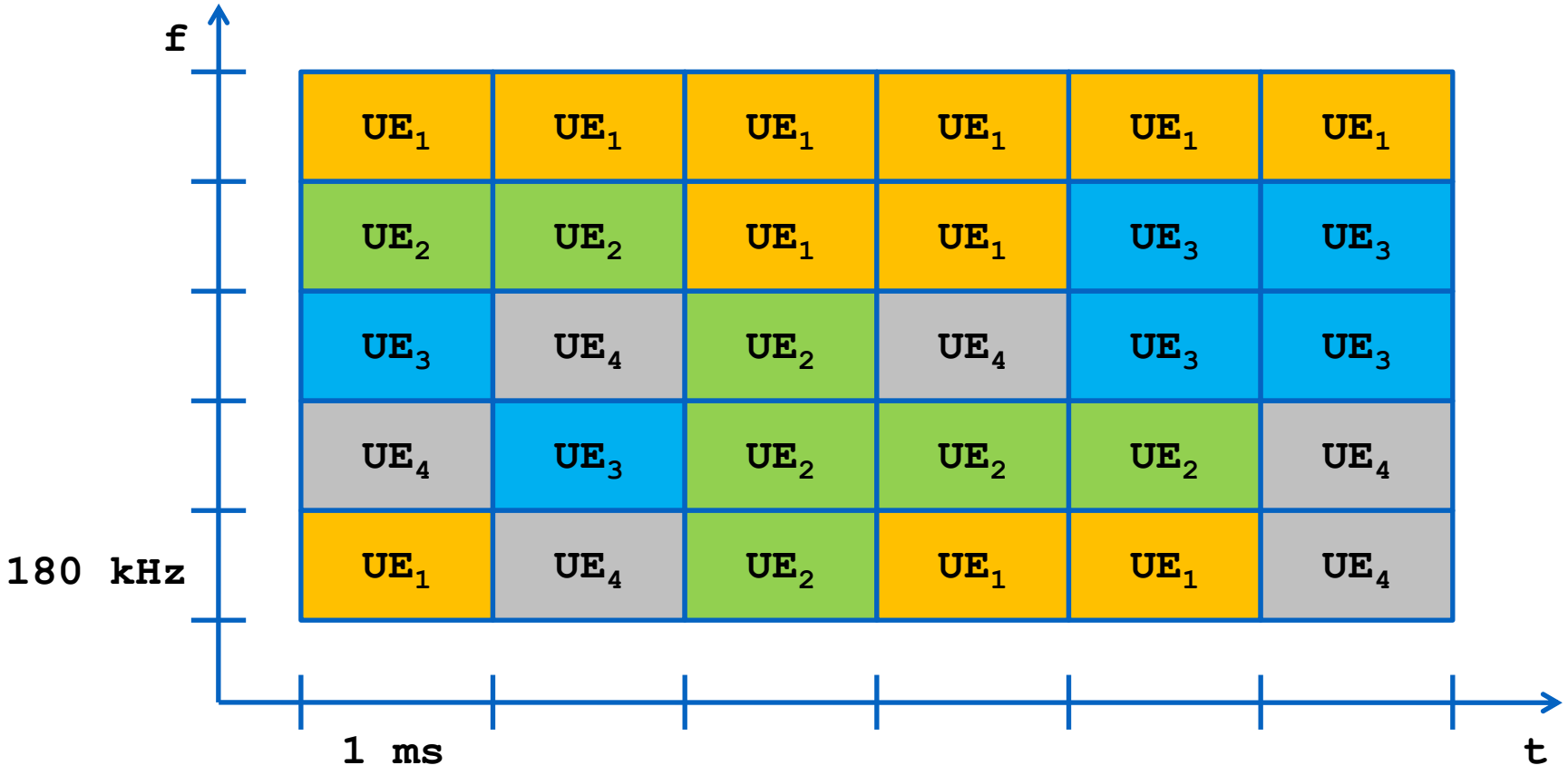
Note 1: Band 6 is not applicable

LTE frame structure



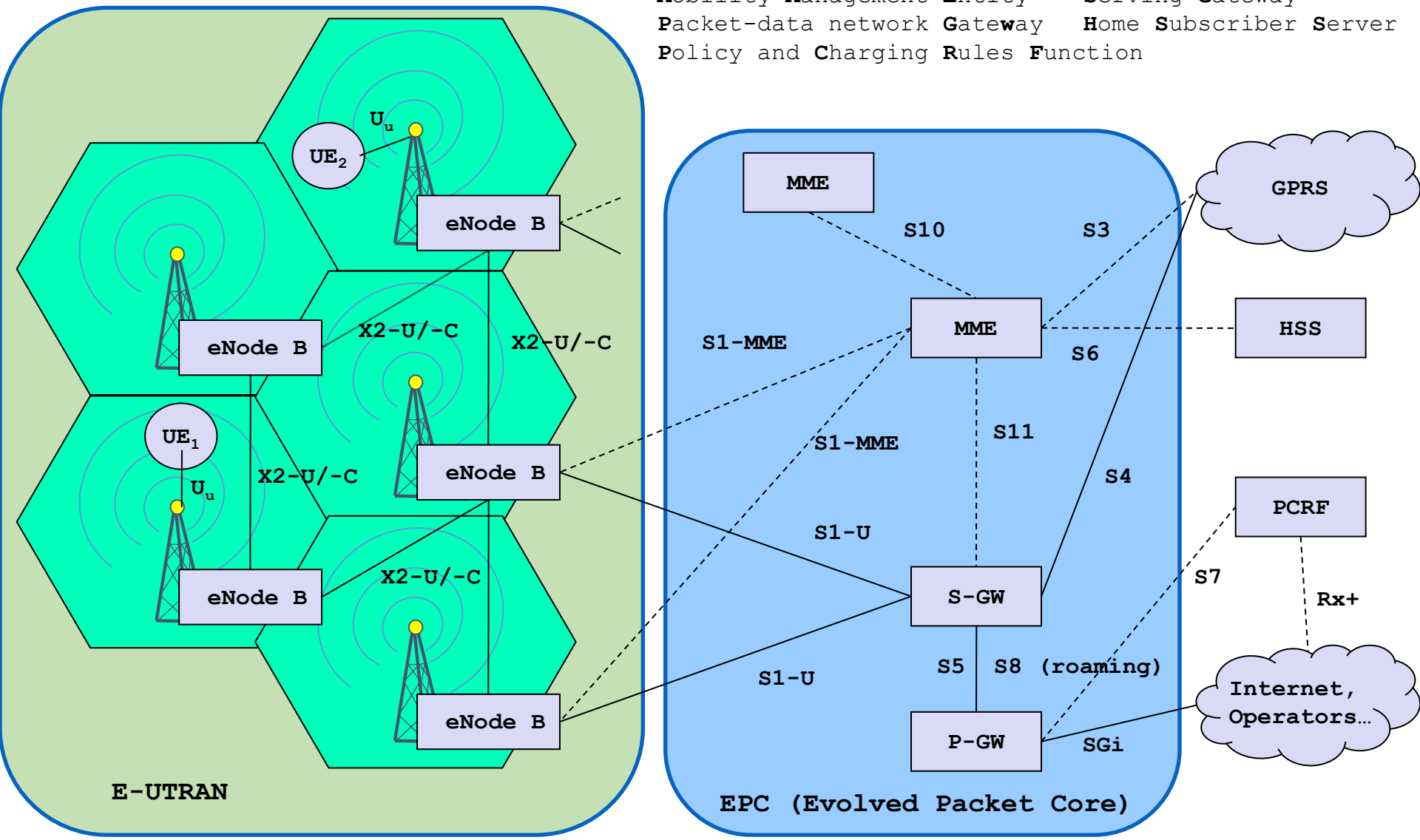
LTE multiple access

- Scheduling of UEs in time and frequency (simplified)



LTE architecture

Mobility **M**anagement **E**ntity **S**erving **G**ateway
Packet-data network **G**ate**w**ay **H**ome **S**ubscriber **S**erver
Policy and **C**harging **R**ules **F**unction



LTE resources

- Further reading and resources
  - LTE overview: http://www.mastertelecomfaster.com/lte/overview.php
  - http://en.wikipedia.org/wiki/LTE_(telecommunication)
  - http://www.etsi.org/technologies-clusters/technologies/mobile/long-term-evolution

IMT-advanced – 4G

International Mobile Telecommunications Advanced

IMT-advanced

- 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
- 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

LTE advanced

- 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)

IMT/LTE-advanced resources

- Further reading and resources
  - http://www.itu.int/ITU-R/index.asp?category=study-groups&rlink=rsg5-imt-advanced&lang=en
  - http://en.wikipedia.org/wiki/IMT-Advanced
  - http://en.wikipedia.org/wiki/4G
  - http://www.mastertelecomfaster.com/lte10/overview.php