Cellular Mobile Networks - UMTS

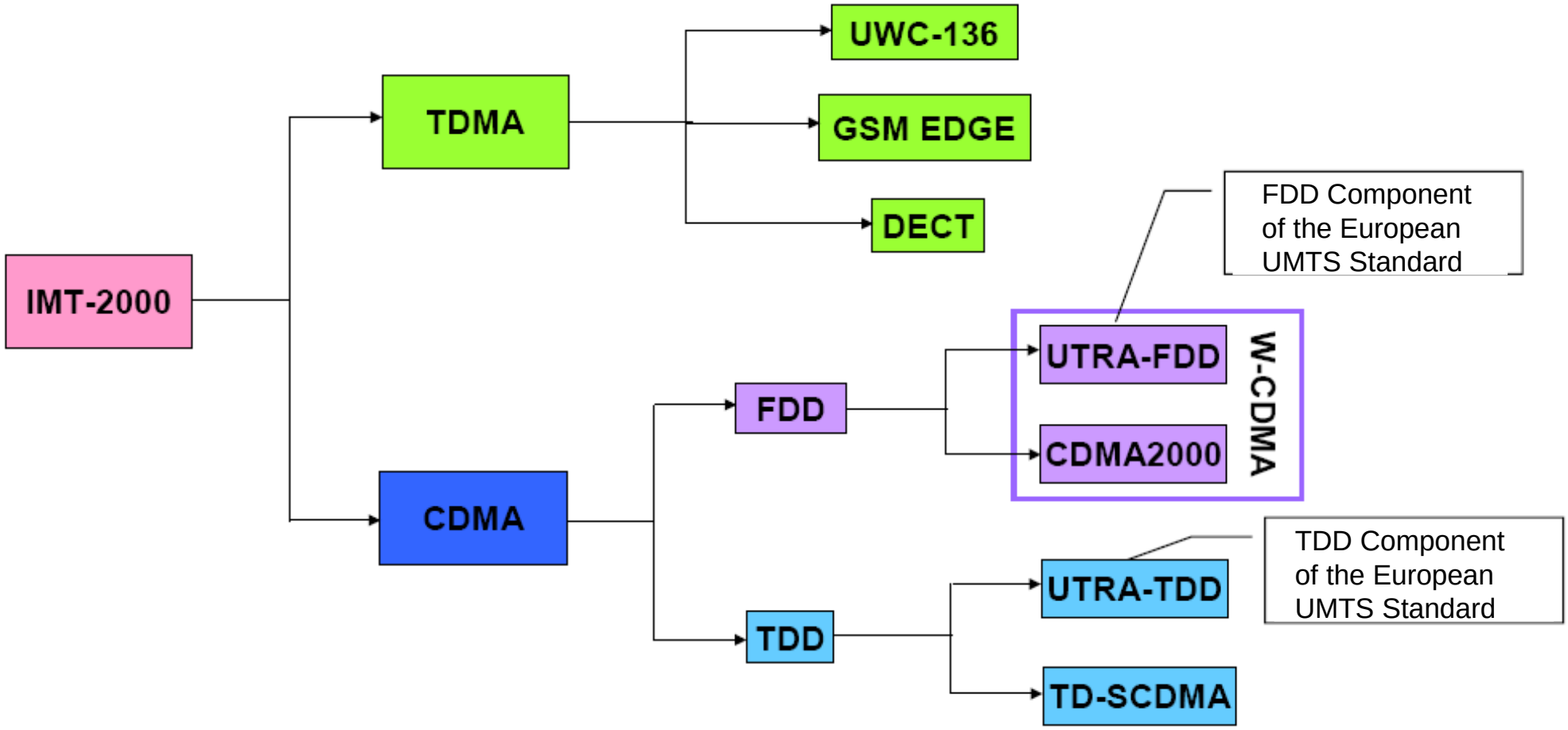
Contents - UMTS

Cellular Mobile Networks - UMTS
UMTS Introduction

Objectives for 3rd Generation Mobile Networks

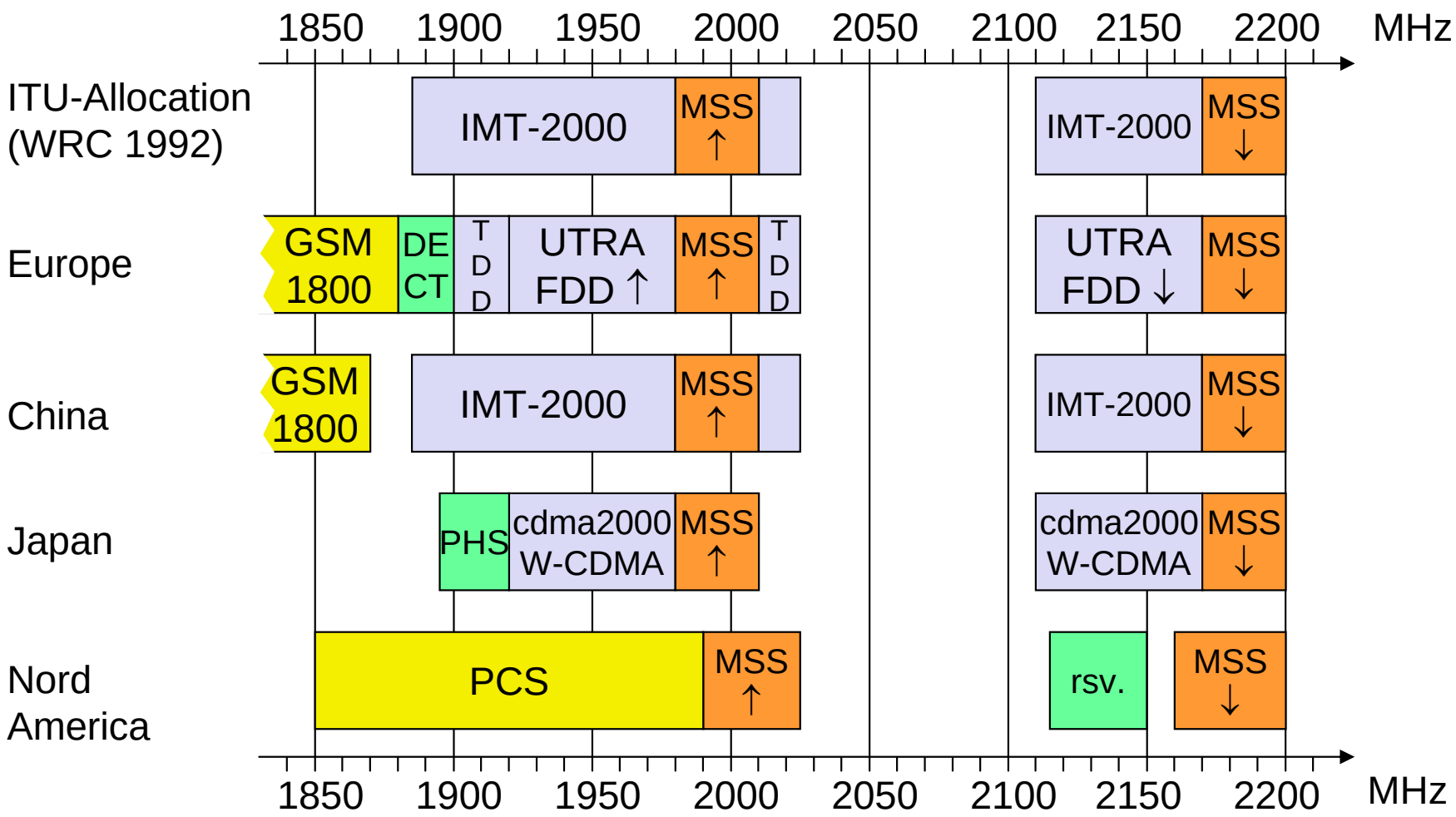
- Compatibility to / Coexistence with GSM
- High transmission rates (up to 2 Mbit/s) for circuit- and packet-switches services
- Adjustable QoS: applicability for all future services and applications (e.g. for Voice over IP or Multimedia over IP)
- Support of Multimedia services
- Flexibility wrt. the introduction of new services
- Improved speech quality
- Improved spectral efficiency

The European UMTS Standard within IMT-2000



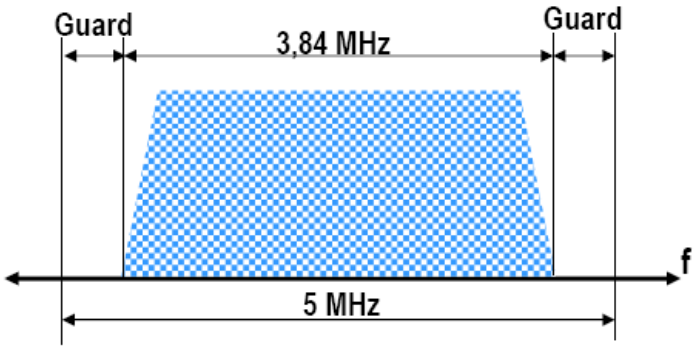
Industry Consortia:
- 3GPP (Third Generation Partnership Project): W-CDMA and TD-(S)CDMA, primarily promoted by Europe, Japan and China
- 3GPP2: CDMA2000, promoted by USA

Global Spectrum Allocation for IMT-2000

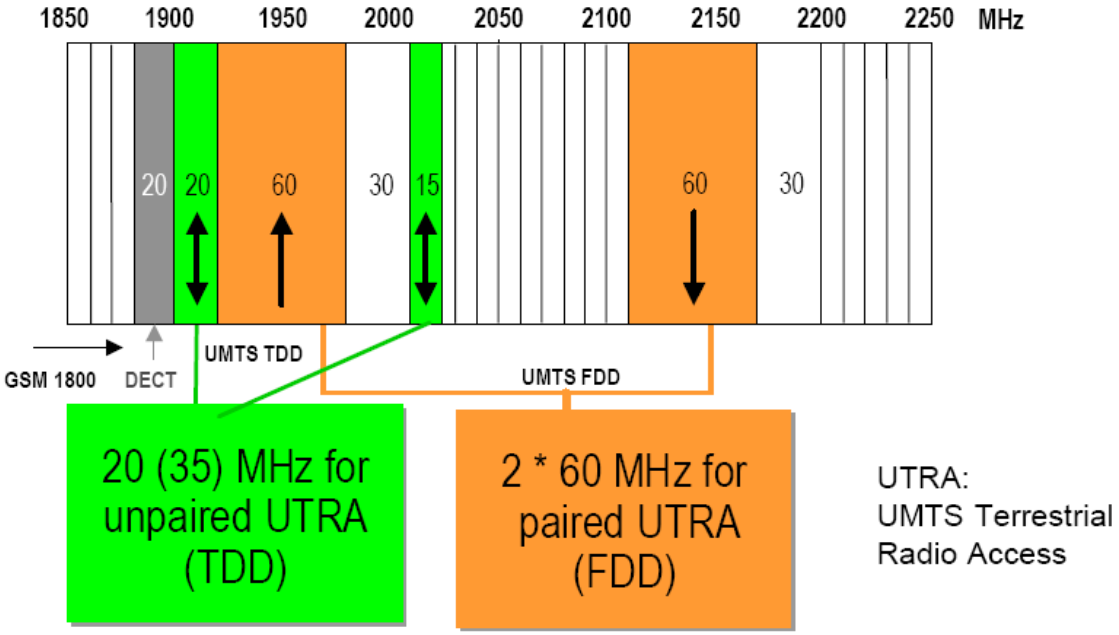


Spectrum Allocation for UMTS in Europe

- 5MHz bandwidth per channel

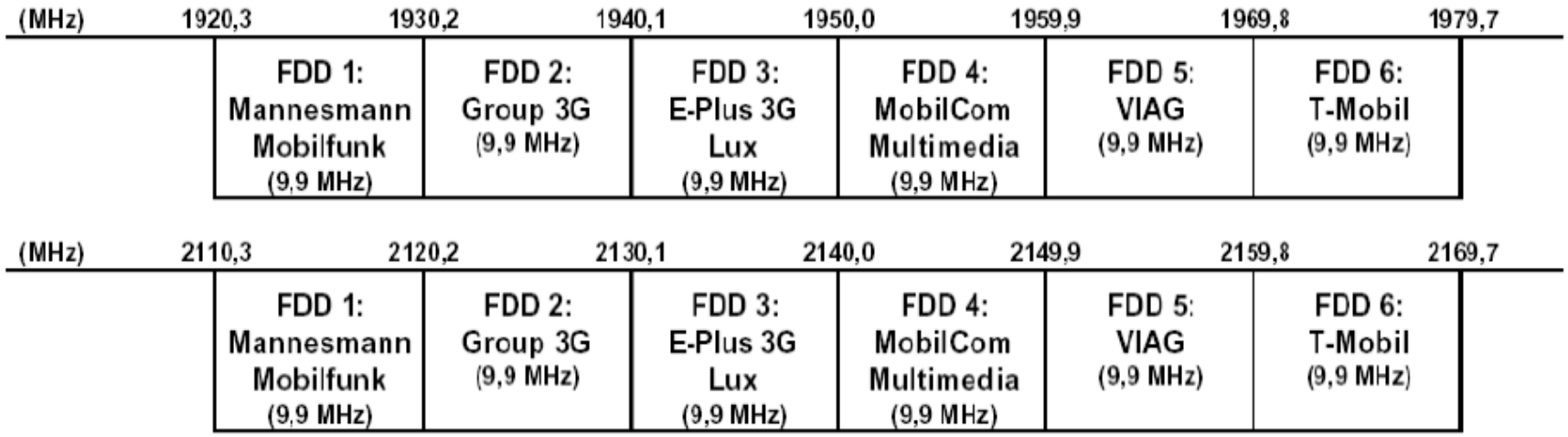


- 12 paired channels (for UMTS FDD)
  - UL: 1920 - 1980MHz
  - DL: 2110 - 2170MHz
- 7 unpaired Channels (for UMTS TDD)
  - 1900 - 1920MHz and 2010 - 2025MHz

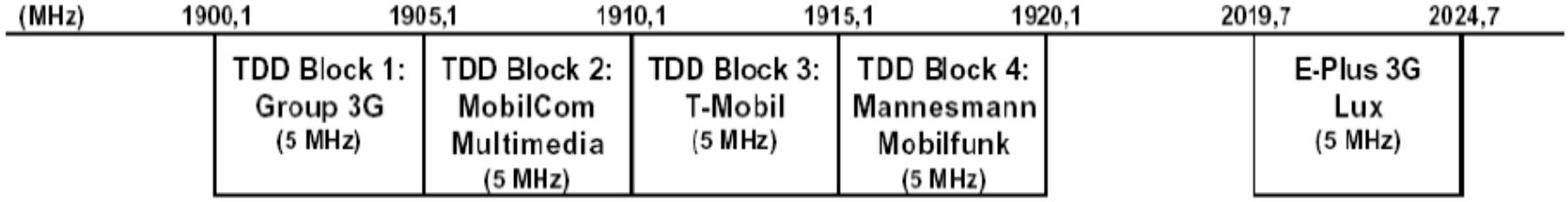


UMTS Licences in Germany

- Results of the UMTS licence auction in Germany (August 2000)
  - FDD licences (frequency blocks)



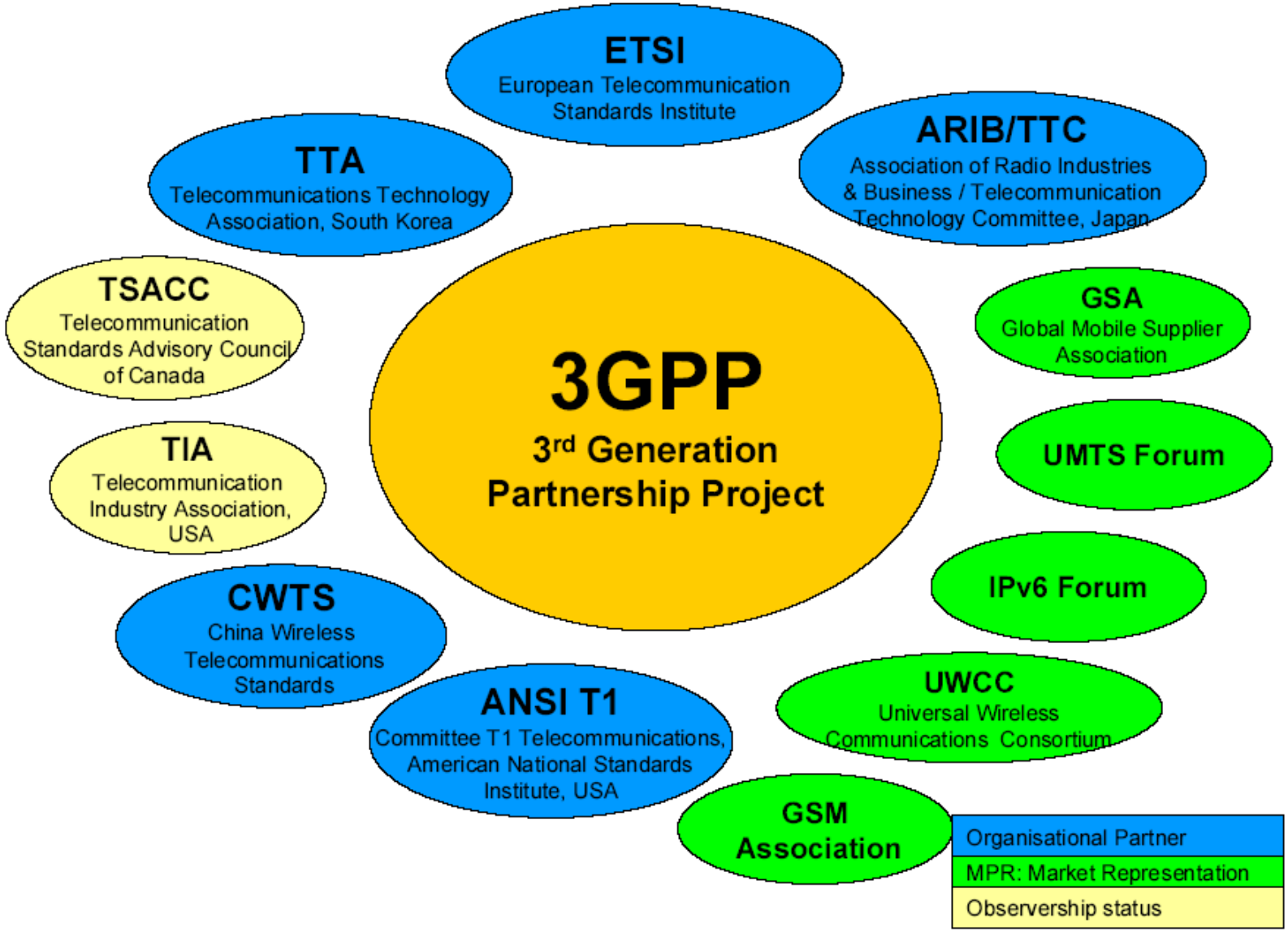
  - TDD licenses (frequency blocks)



UMTS Standardization - 3GPP

- 3GPP = Third Generation Partnership Project
- Goal: global 3G Standard (that allows large dissemination)
  - guarantee of global reachability and compatibility
- 3GPP administrates and coordinates the Standards
  - for WCDMA (UMTS FDD and UMTS TDD)
  - and in the meantime also for GSM, GPRS and EDGE
- 3GPP homepage: http://www.3gpp.org
- 3GPP2 = Standardization in USA (parallel to 3GPP)
  - Standardization of Cdma2000 as evolution of IS-95 (2G Standard in USA)
  - Cdma2000 is based on Multi-Carrier CDMA (MC-CDMA) and FDD only
  - 3GPP2 homepage: http://www.3gpp2.org

UMTS Standardization - 3GPP



Comparison of most relevant 3G Standards

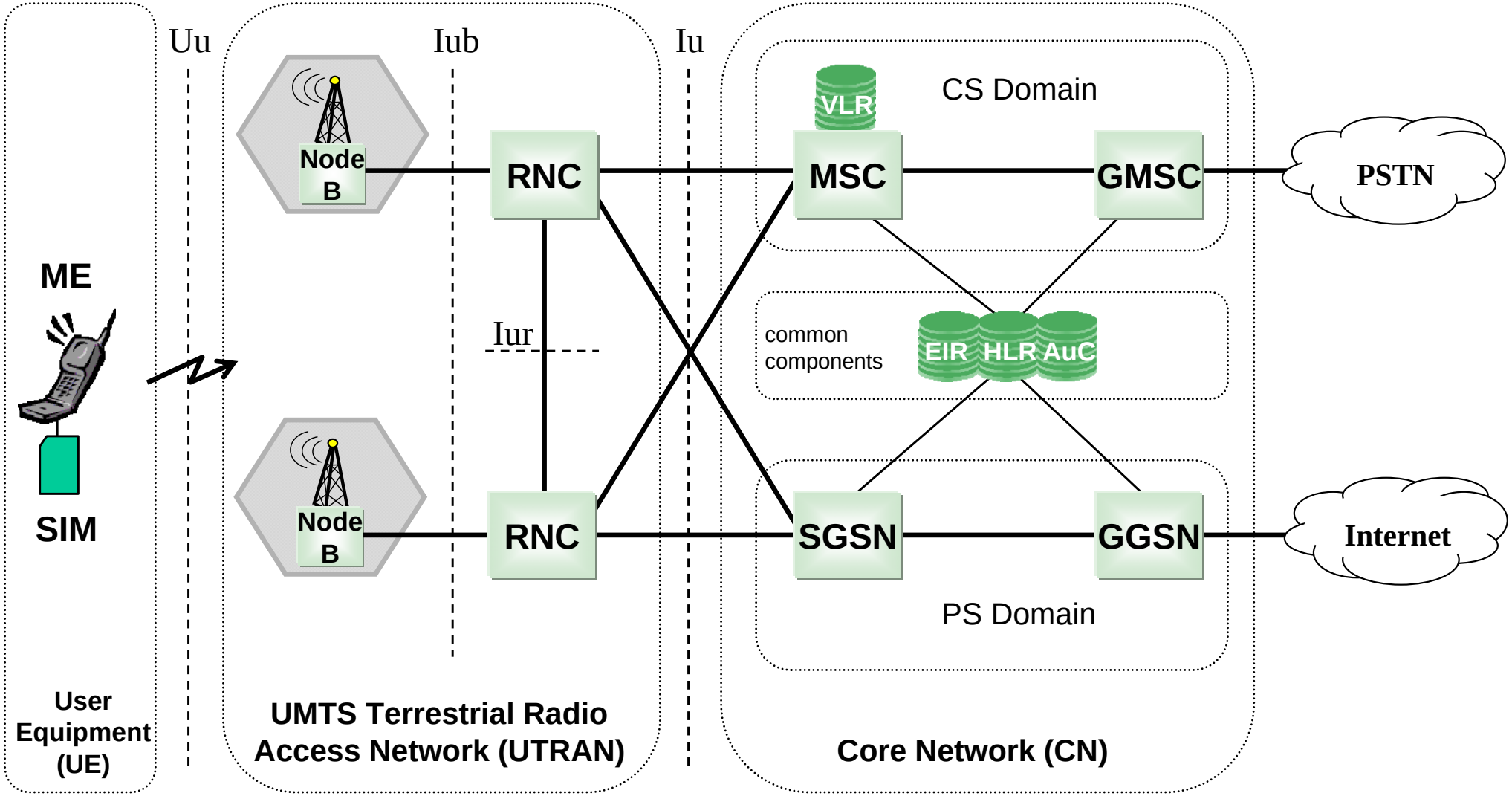
	EDGE	GERAN	UMTS				CDMA2000		
			W-CDMA	TD-CDMA	TD-SCDMA	HSDPA	1xRTT	1xEV-DO	1xEV-DV
Carrier bandwidth [MHz]	0.2		5		1.6	According to base technology	1.25		
Min. spectrum required [MHz]	2x 2.4 (due to BCCH for 4/12)		2x 5	1x 5	1x 1.6		2x 1.25		
Multiple access principle	Time & frequency		code	code & time			code	UL: code DL: code & time	
Chip rate [Mcps]	Not applicable		3.84		1.28		1.2288		
Modulation	GMSK, 8-PSK		QPSK		QPSK, 8-PSK	QPSK, 16QAM	BPSK, QPSK	BPSK, QPSK, 8-PSK, 16QAM	
Peak user data rate [kbps] [1]	473		384 [2048 [2]]	2048	2048	10000 [3]	307 [625 [4]]	2400	3100
System asymmetry (UL:DL)	1:1		1:1	2:13-14:1	1:6-6:1	1:1-5:1	1:1	1:1-4:1	
QoS classes	3 & 4	1 … 4					None	3 classes of service only	
Transport network	PCM (CS), FR (PO)	PCM, FR, ATM	ATM for both CS and PO service domains				Sonet for CS domain, IP-network (PPP and SDLC) for PO domain		
Mobility support	MAP						IS-41, IP protocols for data		

[1] according to presently defined framing, coding and modulation schemes and assuming ideal radio conditions, [2] for pico cells

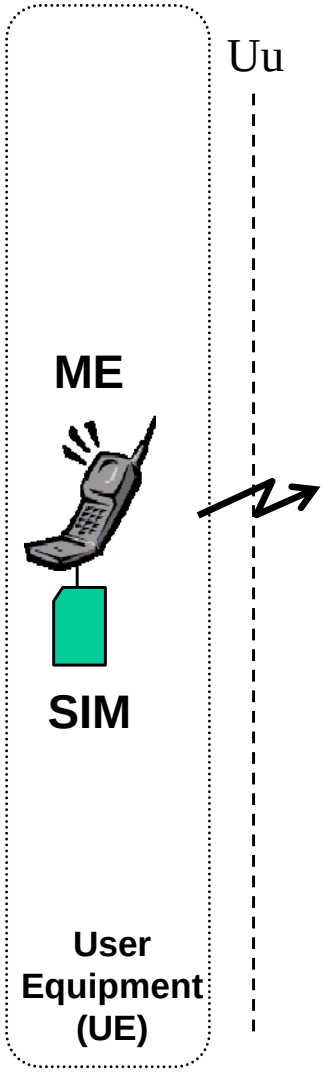
[3] present assumptions, [4] second phase

Cellular Mobile Networks - UMTS
UMTS System Architecture

UMTS Network Architecture - Overview (simplified)



UMTS User Equipment (UE)



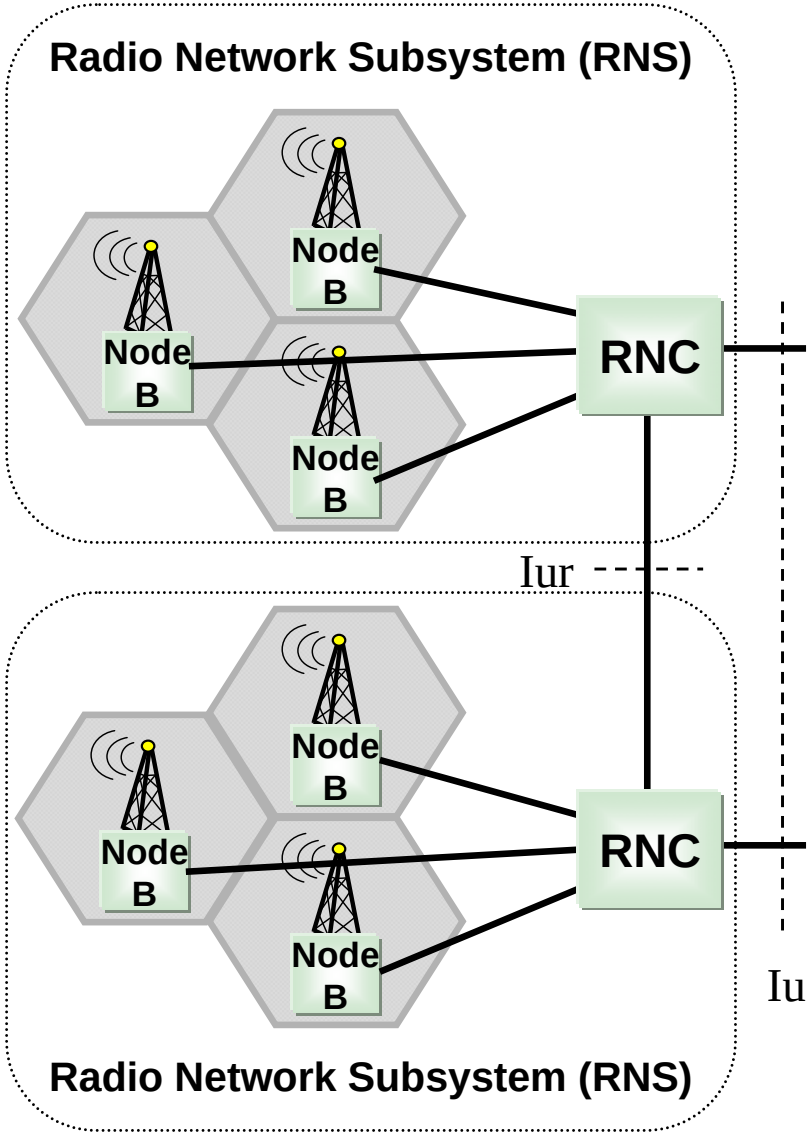
Subscriber Identity Module (SIM):

- stores data:
  - for user identification (via IMSI)
  - to support user authentication and encryption
  - contains a list of allowed / non-allowed mobile networks
  - directory entries
- stores software:
  - for applications, security functions, etc.

Mobile Equipment (ME):

- spreading / despreading (CDMA)
- modulation / demodulation
- power control
- measurement of Connection Quality and Signal Strenght
- encryption
- mobility Management

UMTS Terrestrial Radio Access Network (UTRAN)



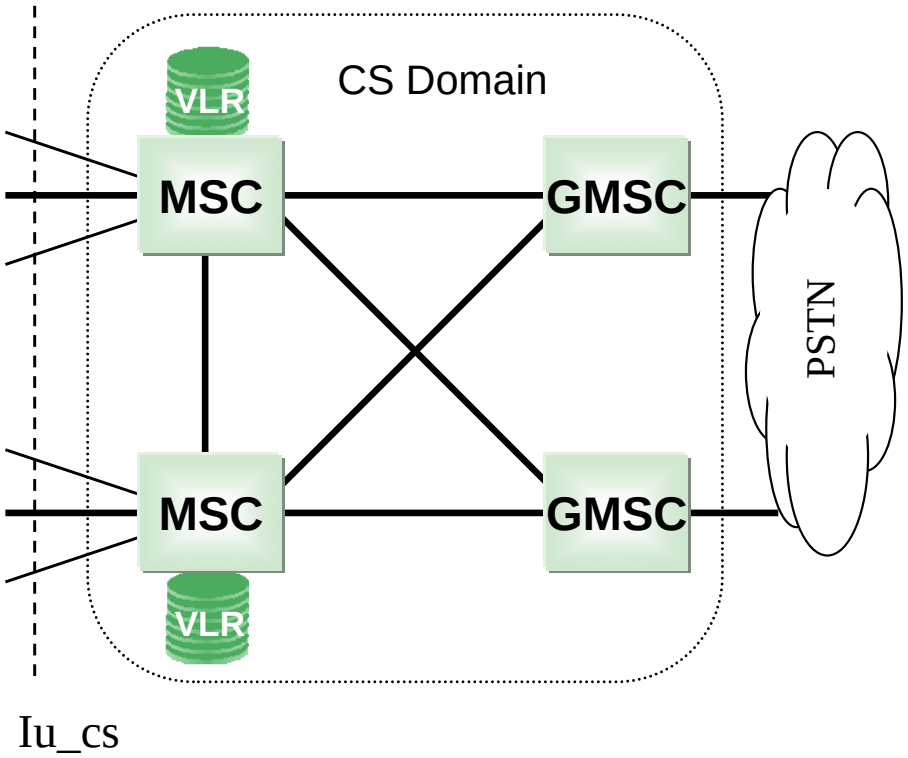
Node B:

- realization of the radio link towards UE:
  - spreading / despreading (CDMA)
  - modulation / demodulation
  - power control (inner control loop)
  - measurement of Connection Quality and Signal Strenght
  - Intra Node B handover execution

Radio Network Controller (RNC):

- Radio Resource Management (RRM) within RNS area:
  - admission control (to radio ressources)
  - encryption
  - codemanagement
  - power control (outer control loop)
  - handover control (at UTRAN level)
  - Intra & Inter RNC handover execution

UMTS Core Network - CS Domain



Mobile Switching Center (MSC):

- switching of CS connections to/from users with the MSC area
- admission control and authentication
- Intra & Inter MSC handover execution

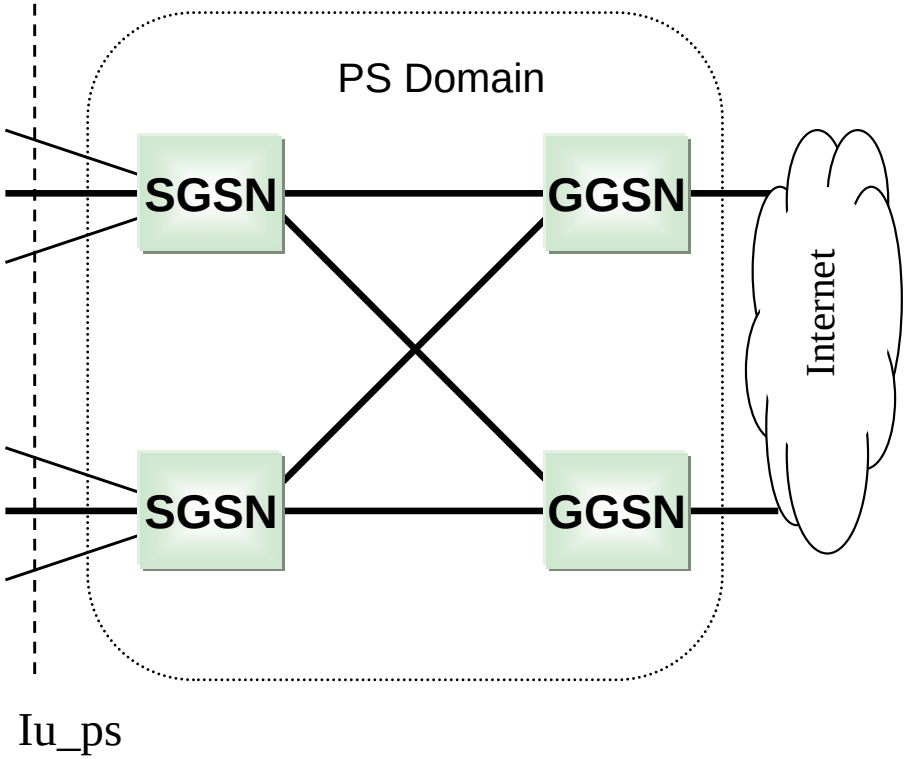
Visitor Location Register (VLR):

- database with infos about all currently registered users in the MSC area (e.g. user location, subscribed services)
- usually integrated in MSC

Gateway Mobile Switching Center (GMSC):

- switching of CS connections between the mobile network and the PSTN (general: to/from networks that don't have access to the HLR)
- gateway-functionality

UMTS Core Network - PS Domain



Serving GPRS Support Node (SGSN):

- packet forwarding between UTRAN and GGSNs
- contains a database with infos about all currently registered users in the SGSN area (e.g. user location, subscribed services, PDP context infos)
- admission control and authentication
- Intra & Inter SGSN handover execution

Gateway GPRS Support Node (GGSN):

- packet forwarding between SGSNs and the Internet (or other packet data networks, PDNs)
- gateway-functionality

UMTS Core Network - Common Components

common components

Home Location Register (HLR):

- database for user-related infos:
  - user location related infos: address of the VLR (or GR/SGSN) the area of which the user is located
  - user subscription related infos: subscribed services, PDP-context infos, etc.

Authentication Center (AuC):

- database für security related infos:
  - supports user authentication and encryption
  - usually integrated in HLR

Equipment Identification Register (EIR):

- database for mobile equipment (ME) related infos:
  - contains lists for identification of misused or specially used MEs (white, grey, black list)

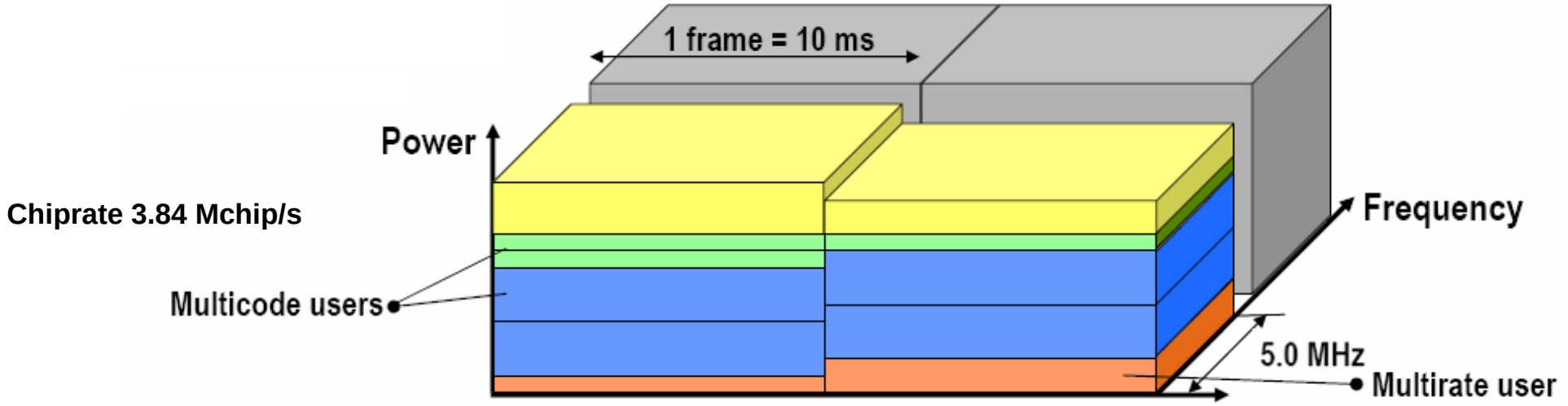
Cellular Mobile Networks - UMTS
UMTS Radio Interface (UTRA)
(UMTS Terrestrial Radio Access)

UMTS Radio Interface - Contents

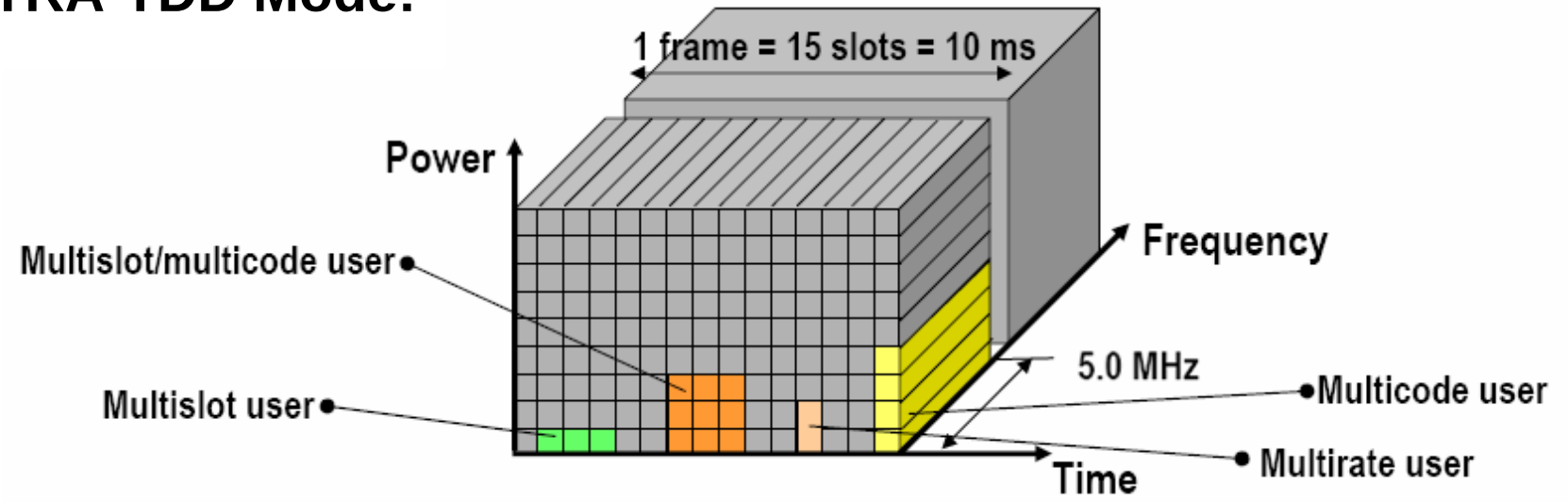
- Multiplex and Duplex Options: UTRA-FDD, UTRA-TDD
- Realization of variable Bitrates
- UMTS Cell Types
- Spreading and Scrambling (Spreizung und Verwürfelung)
- Power Control
- Logical, Physical and Transport Channels

Multiplex and Duplex Options: UTRA-FDD / UTRA-TDD

UTRA-FDD Mode:

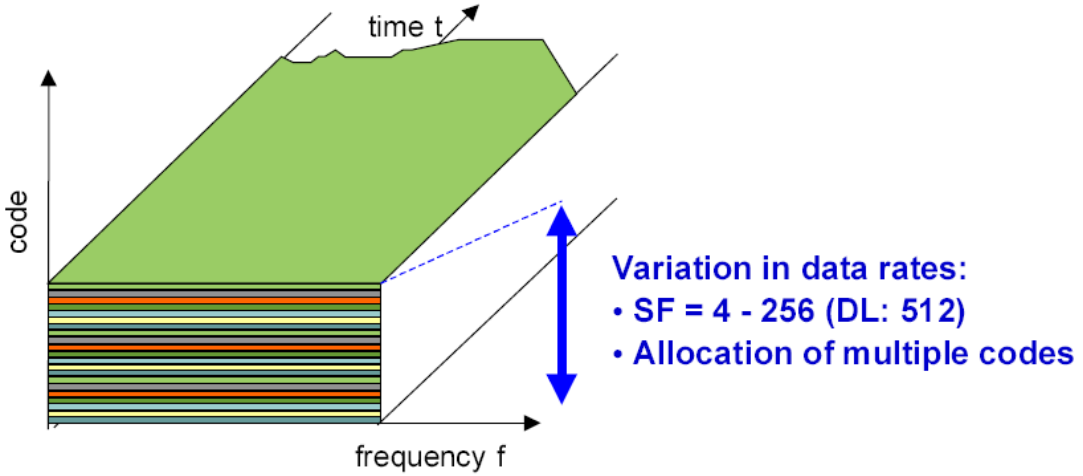


UTRA-TDD Mode:

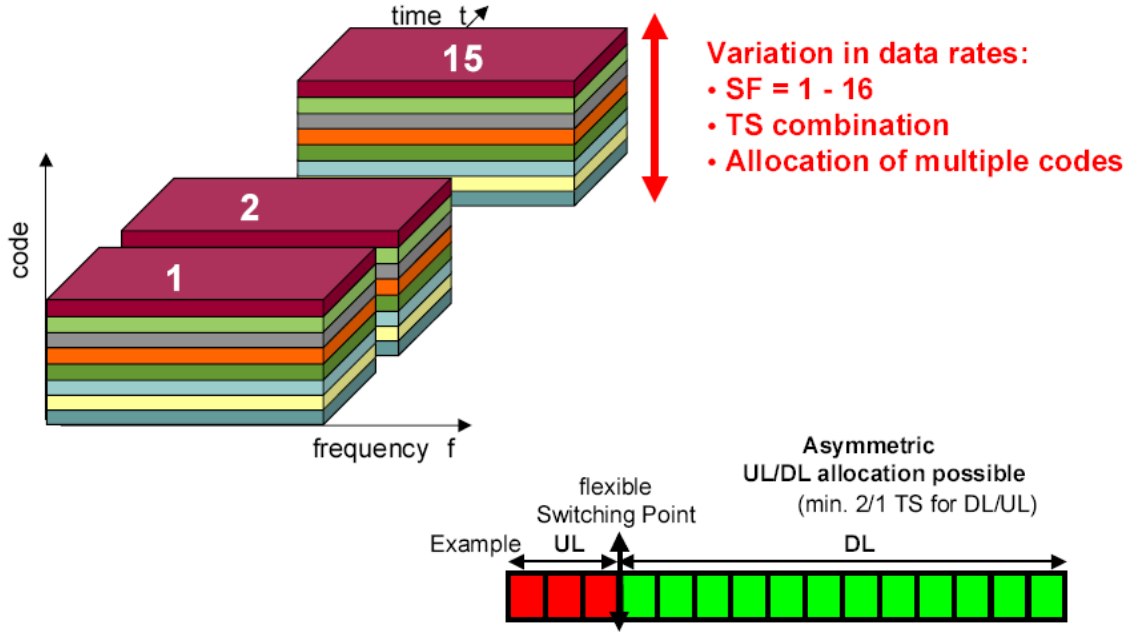


Realization of variable Bitrates

UTRA-FDD:



UTRA-TDD:



Realization of variable User Bitrates - Example

- Bitrate (after channelcoding) · Spreading Factor = Chiprate (3,84 Mchip/s)
- Example:
  - User Bitrates (after channelcoding) and Spreading Factors for FDD:

Nutzdatenrate (kanalkodiert)	*	Spreizfaktor	=	Chiprate
960 kbit/Sek.	*	4	=	3.84 Mchip/Sek.
480 kbit/Sek.	*	8	=	3.84 Mchip/Sek.
240 kbit/Sek.	*	16	=	3.84 Mchip/Sek.
120 kbit/Sek.	*	32	=	3.84 Mchip/Sek.
60 kbit/Sek.	*	64	=	3.84 Mchip/Sek.
30 kbit/Sek.	*	128	=	3.84 Mchip/Sek.
15 kbit/Sek.	*	256	=	3.84 Mchip/Sek.
7.5 kbit/Sek.	*	512	=	3.84 Mchip/Sek.

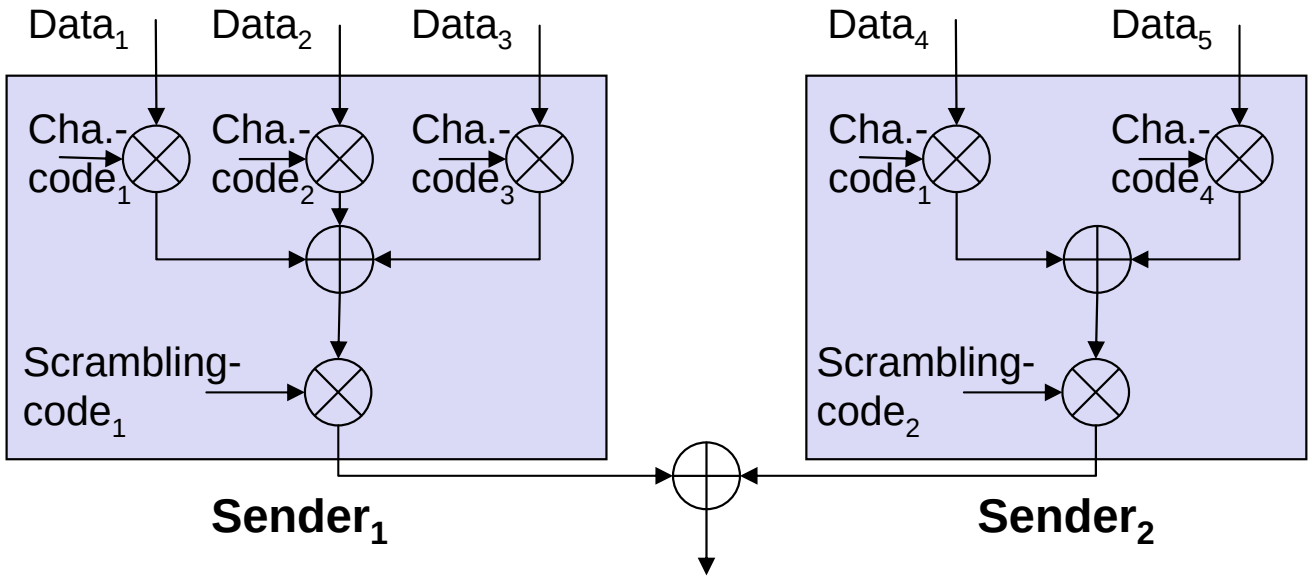
  - Spreading Factors for TDD: 1, 2, 4, 8, 16

UMTS Cell Types

Cell Type	Coverage Area [m]	Bitrate [kB/s]	Power [W]	Duplex	Usage
Macro	>1000	144	1-10	FDD	- most common cell type - maximization of coverage area and minimization of infrastructure costs
Micro	<1000	384	0.1-1	FDD or TDD	- cell type for coverage of urban areas - compact base stations installed on lampposts and buildings
Pico	5-30	2048	0.01-0.1	TDD	- In-house coverage - areas with high terminal density
Satellite	global	144-384	1-10	FDD or TDD	- cell type for serving coverage gaps of other cell types - handover support for high velocities in micro-cells

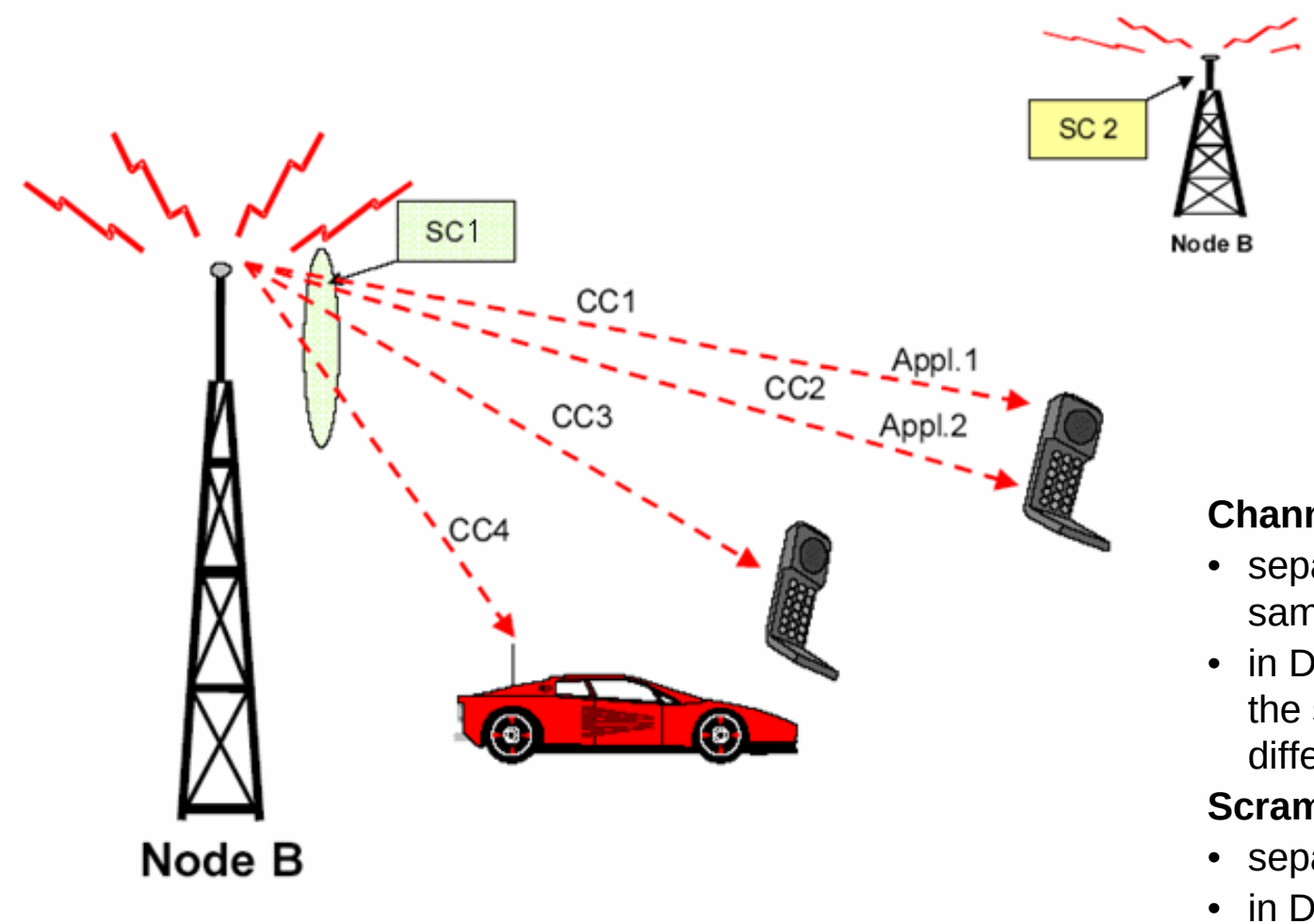
Spreading and Scrambling (Spreizung und Verwürfelung)

- Twofold application of code sequences:
  - multiplication with **Channelization-Codes** ⇒ Spreading and Multiplex (user/channels)
  - multiplication with (quasi-orthog.) **Scrambling-Codes** ⇒ Sender-Separation (cell/UE)
- Advantages:
  - sender don't need to be separated by orthogonal spreading codes
  - simple administration of codes: each station can use the same orthogonal channelization codes
  - no precise synchronization between stations required - scrambling codes stay orthogonal also in case of imprecise synchronization



Spreading and Scrambling - Application in Downlink

- Application in Downlink (Sender = BTS/Node B):



Channelization Codes:

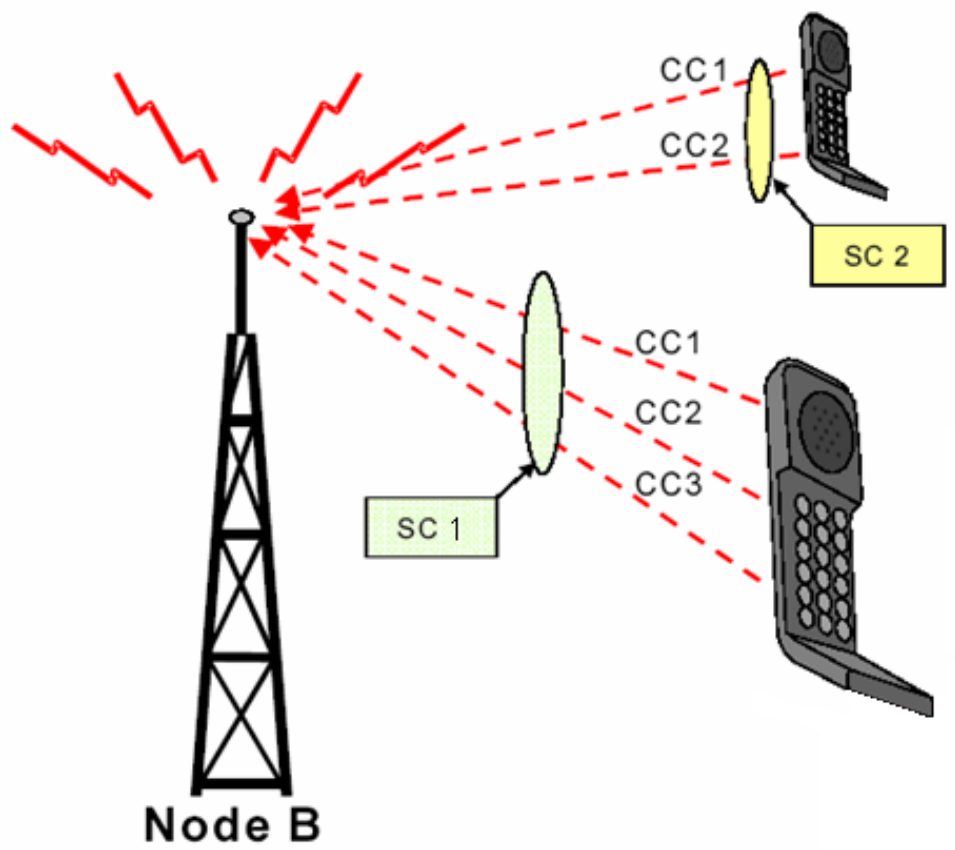
- separates channels of the same source
- in DL: separates channels of the same BTS, e.g. for different UE and applications

Scrambling Codes:

- separates different sources
- in DL: separates different BTS

Spreading and Scrambling - Application in Uplink

- Application in Uplink (Sender = UE):



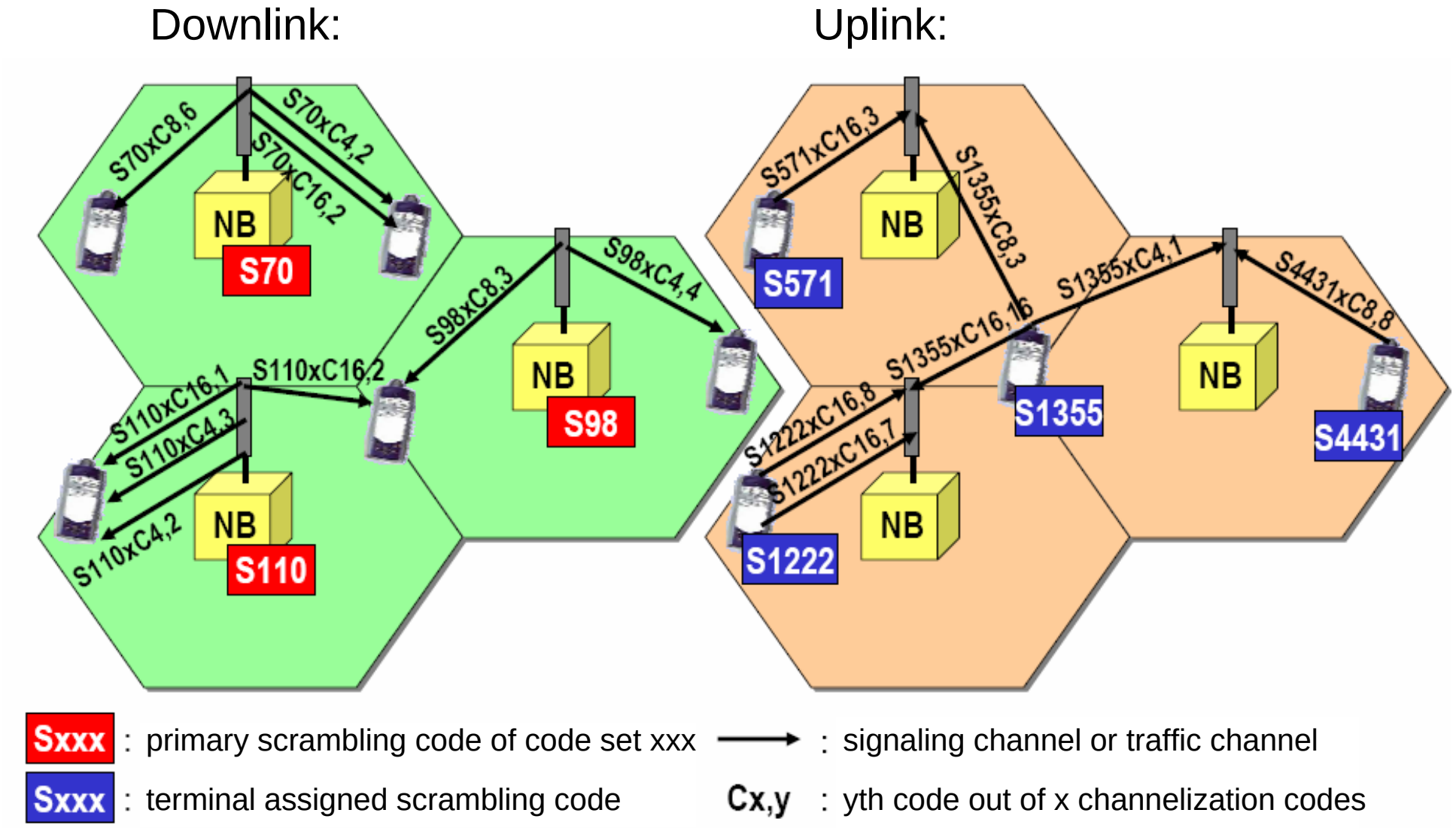
Channelization Codes:

- separates channels of the same source
- in UL: channels of the same UE, e.g. for different applications (max. 6 SF)

Scrambling Codes:

- separates different sources
- in UL: separates different UE in a cell

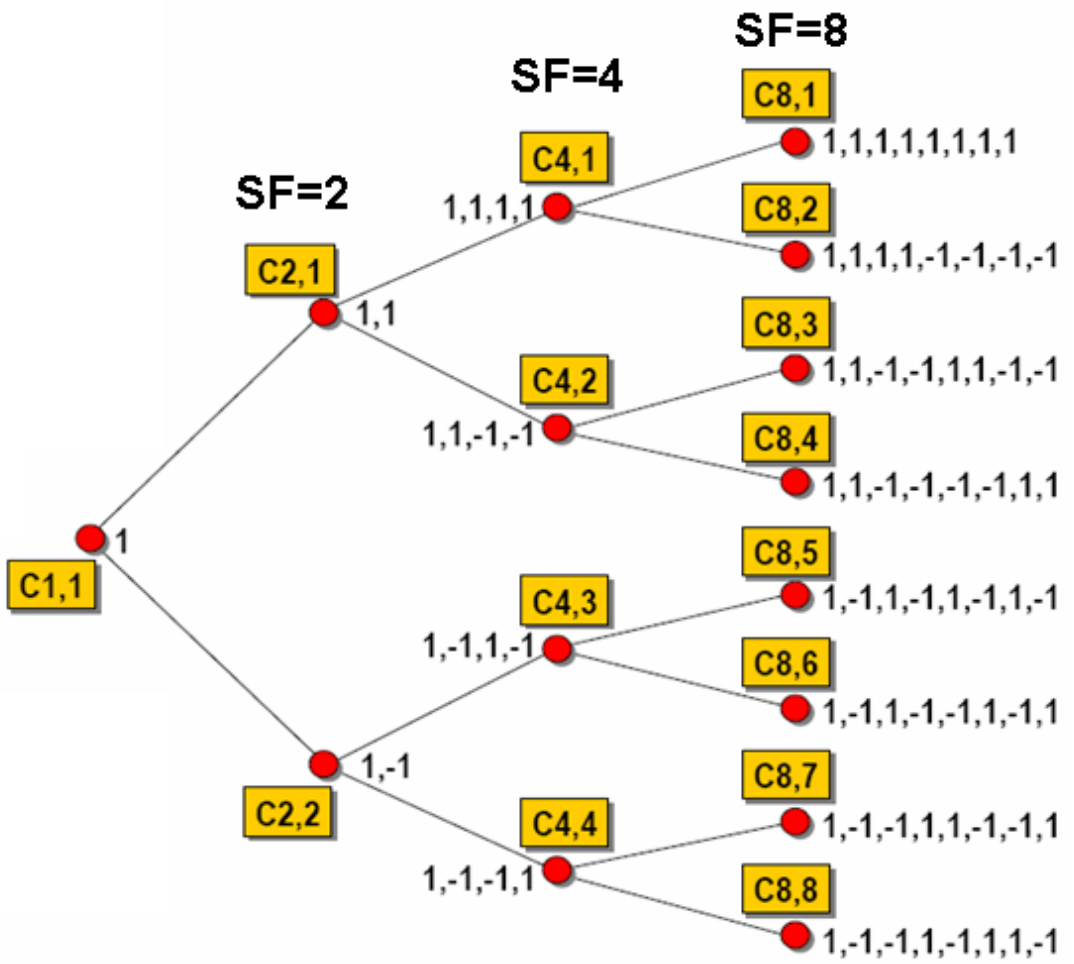
Spreading and Scrambling - Example



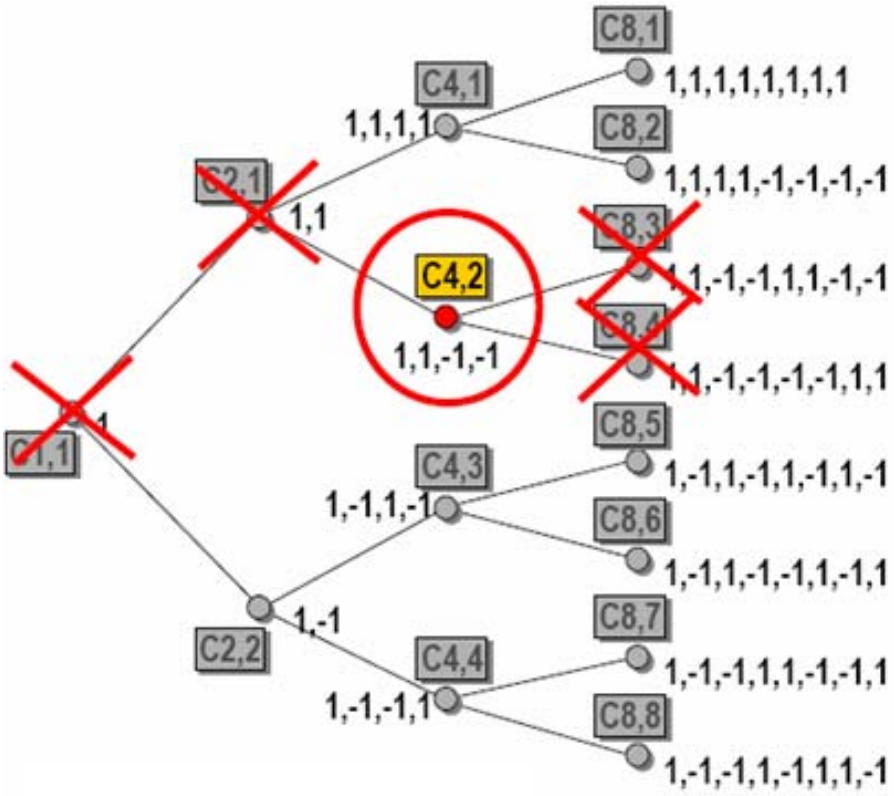
Spreading and Scrambling - Channelization-Codes (1)

Generation of OVSF codes:

- Orthogonal Variable Spreading Factor (OVSF): method to obtain variable length orthogonal codes that preserve orthogonality between different rates and spreading factors
- recursive generation of variable orthogonal codes using a tree structure
  - a node adopts the code from its predecessor and concatenates it either with a copy of this code (first successor) or with its inverse (second successor)
  - codes of the same layer are orthogonal
  - any two codes of different layers are orthogonal except for the case that one of the two codes is a mother code of the other



Spreading and Scrambling - Channelization-Codes (2)



Bit rate	Spreading factor	Chip rate
960 kb/s	4	3.84 Mcps
480 kb/s	8	3.84 Mcps
240 kb/s	16	3.84 Mcps
120 kb/s	32	3.84 Mcps
60 kb/s	64	3.84 Mcps
30 kb/s	128	3.84 Mcps
15 kb/s	256	3.84 Mcps
7.5 kb/s	512	3.84 Mcps

bit rate * spreading factor = 3.84 Mcps

- Example:
  - C4,2 is assigned to a user
  - codes C8,3 and C8,4 generated from this code cannot be assigned to other users requesting lower bit rates
  - mother codes C1,1 and C2,1 cannot be assigned to users requesting higher rates

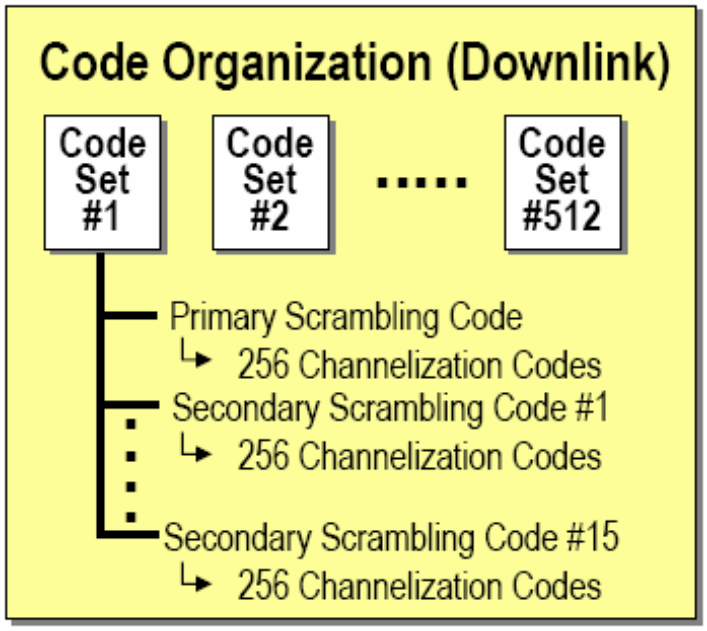
Spreading and Scrambling - Scrambling-Codes

Scrambling Codes in Downlink:

- for sector/cell separation
- scrambling codes are divided into 512 sets each having a **primary scrambling code** and 15 **secondary scrambling codes**
- length: 38400 chips or 10ms (corresponds to the length of one frame)
- **primary scrambling codes**
  - must be used for certain signaling channels to ease cell search
  - may also be used for user traffic channels
- **secondary scrambling codes**
  - may be used for traffic channels
- cells using the same scrambling code set must be arranged as far as possible to avoid interferences

Scrambling Codes in Uplink:

- for user/terminal separation
- 16.78 million different codes
- long codes: length of 38400 chips or 10 ms
- short codes: length of 256 chips or 66,7 µs (if node B is equipped with advanced (expensive) receivers)

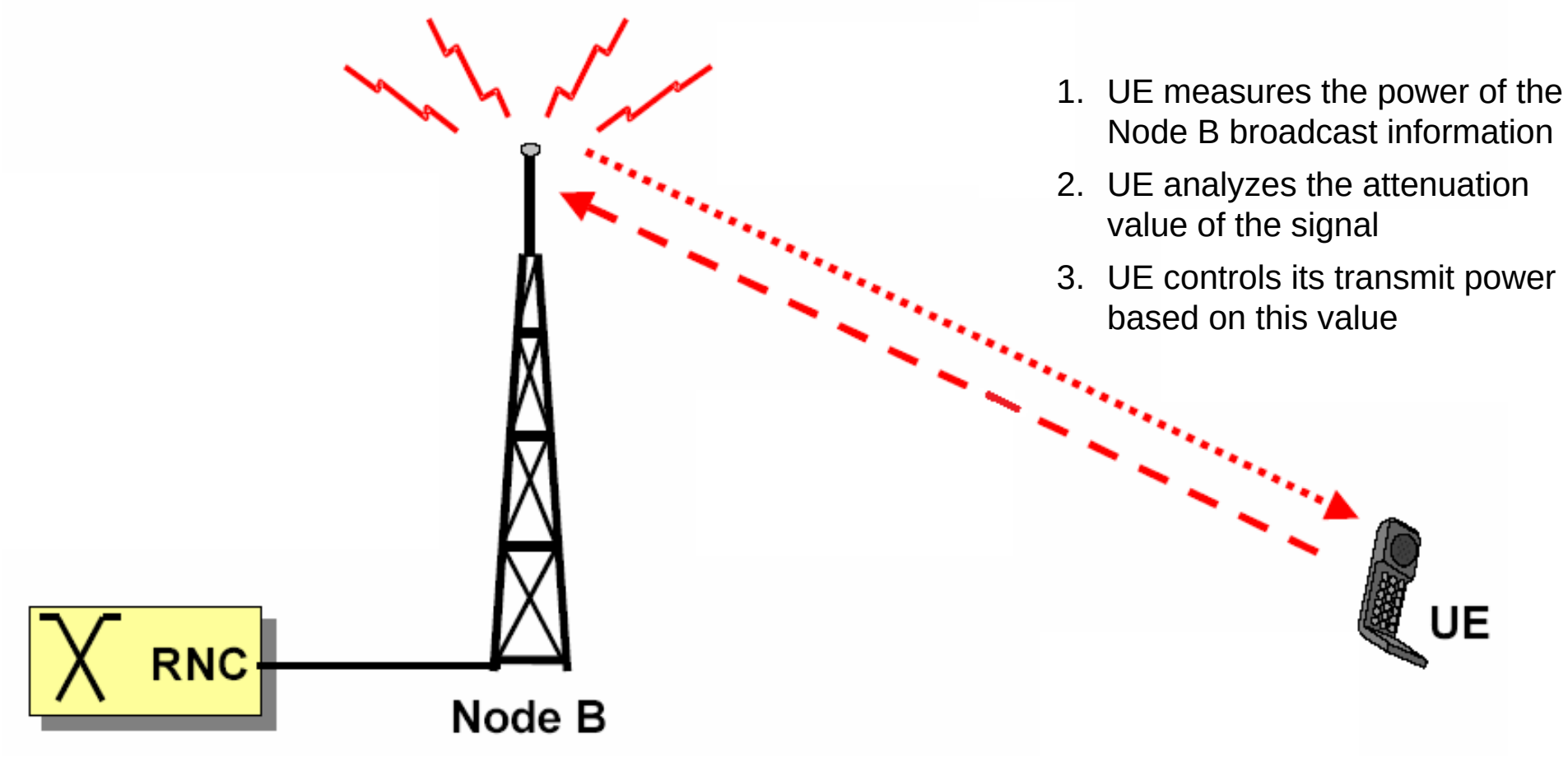


Spreading and Scrambling - Summary

	Channelization Code	**Scrambling Code**
Usage	• Uplink: separation of physical data and control channels • Downlink: separation of downlink connections to different terminals within one cell	• Uplink: separation of terminals • Downlink: separation of cells (and sectors)
Length	• 4 - 256 chips (1.0 - 66.7 µs) • in Downlink also 512 chips	• Uplink: 10 ms = 38400 chips (long codes) or 66.7 µs = 256 chips (short codes) • Downlink: 10ms = 38400 chips
Number of Codes	• number of codes under one scrambling code = spreading factor	• Uplink: 2^{24} = 16.84 mio. • Downlink: 8191 = 512·16
Code Family	• Orthogonal Variable Spreading Factor	• Gold Codes
Spreading	• yes, increases transmission bandwidth	• no, does not affect transmission bandwidth

Power Control - Open Loop Power Control (Uplink)

- Open Loop Power Control (in Uplink) - **for initial Transmission only**

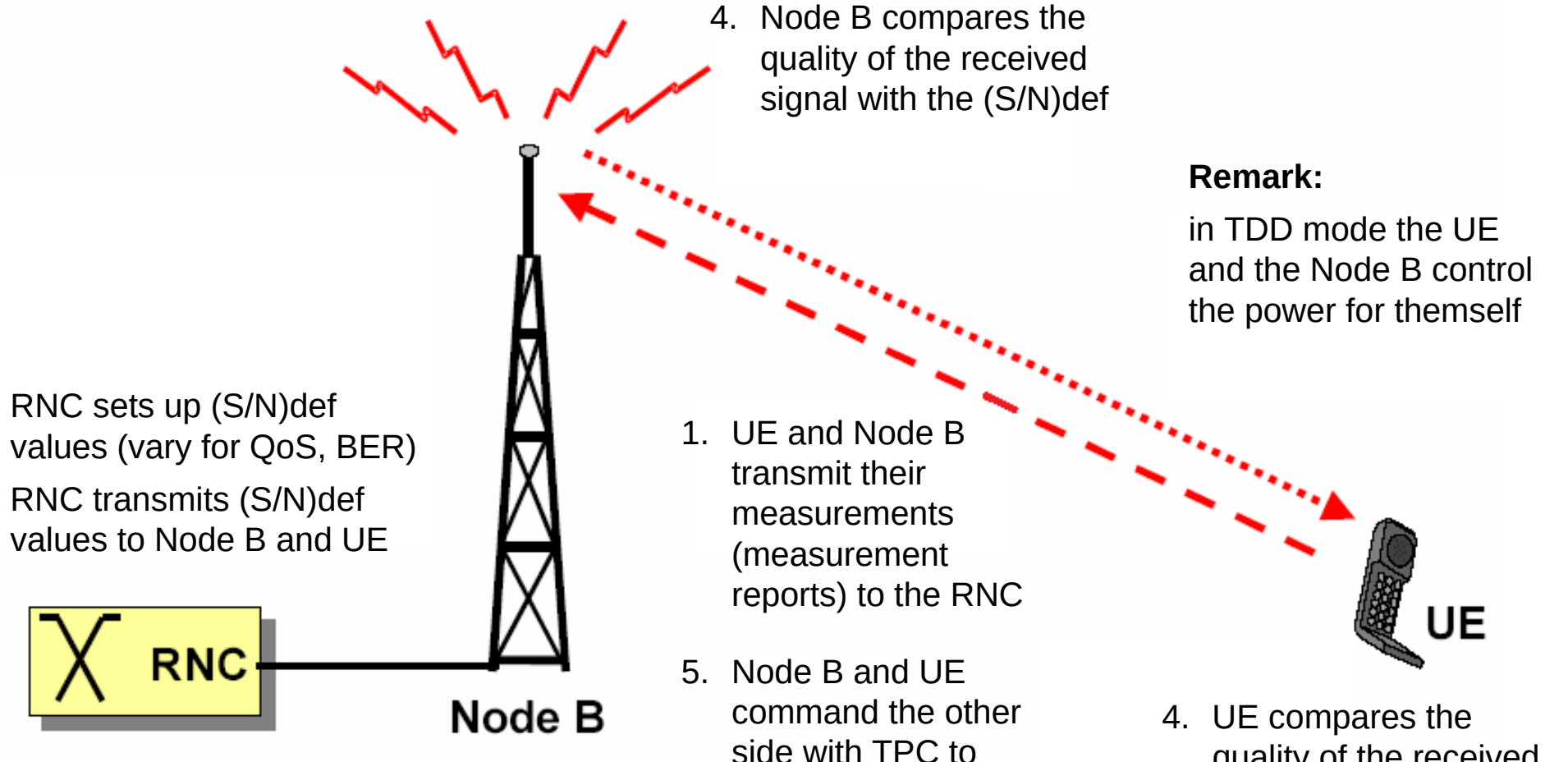


Power Control - Open Loop Power Control (Uplink)

- Open Loop Power Control (in Uplink) - **for initial Transmission only**
  - Open Loop Power Control is used for UL transmissions to control the initial transmission power (e.g. for random access) of UE
  - the original power of the BTS is radiated together with other systems parameters as broadcast information
  - the attenuation of the transmission power of the BTS is analyzed by the UE as part of the control
  - the UE transmit power is initially controlled on the basis of the analyzed attenuation
  - this initial control can only be coarse because the UL and DL attenuations (for FDD) can differ

Power Control - Inner (closed) Loop Power Control

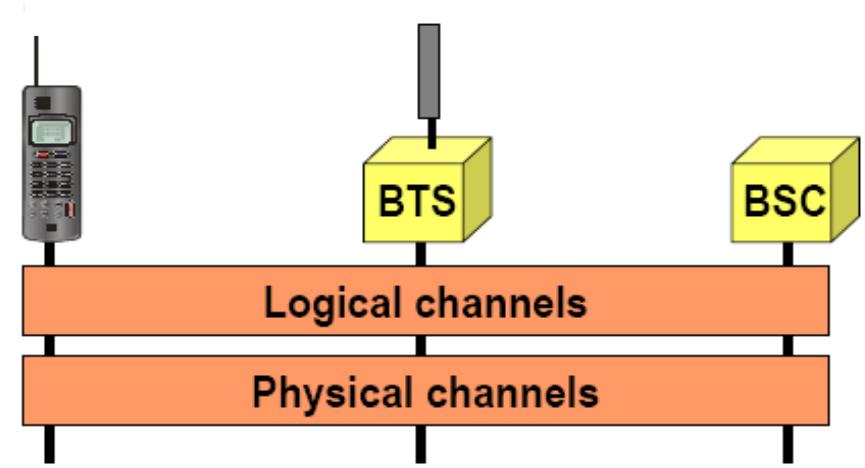
- Inner Loop Power Control - **during Transmission**

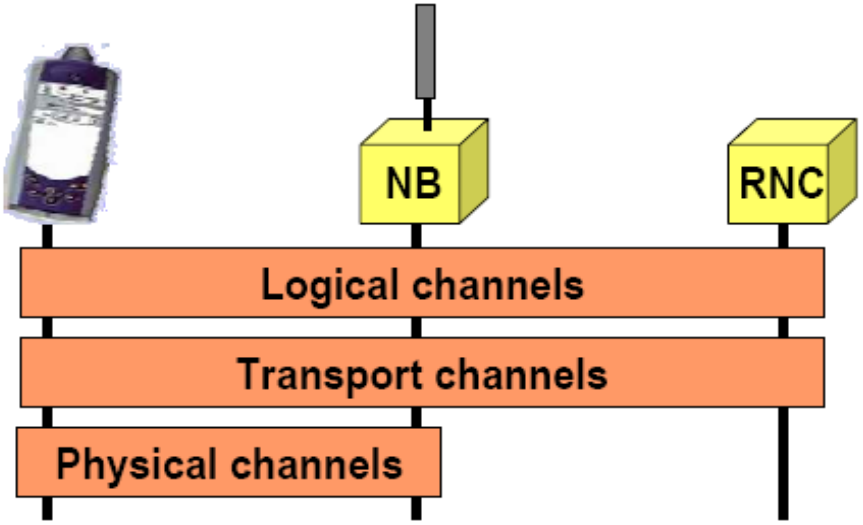


Power Control - Inner (closed) Loop Power Control

- Inner Loop Power Control - **during Transmission**
  - for Inner Loop Power Control the BTS or UE compare the signal-to-noise ratio (S/N) of the received signals with a specific target value - the so called defined signal-to-noise ratio (S/N)def; (S/N)def describes the ratio of the wanted received signal power (signal) and the unwanted interference from other sources (noise)
  - if the measured (S/N) is better than (S/N)def, the BTS or UE transmit a command to the corresponding opposite side to reduce the transmission power; if the analyzed (S/N) is lower than (S/N)def, an increase in transmission power is requested; the commands are covered by the term Transmit Power Control (TPC); values for TPC are „Up“ and „Down“
  - in the FDD mode, the Inner Loop Power Control is also referred to as a Closed Loop Power Control
  - in the TDD mode, the BTS and UE independently control the power for themselves according to the completed (S/N) measurements and specified values (S/N)def
  - the specification of the (S/N)def values used in the Inner Loop Power Control is made by Serving RNC (SRNC); the SRNC has access to estimates of the actual transmission quality using measurement reports for Node B's and UE; the quality can vary due to modified transmission conditions (e.g. due to the speed of UEs); to assure transmission quality, the SRNC must be able to vary the (S/N)def values

Logical, Physical and Transport Channels - GSM vs. UMTS





GSM

- initially designed for one air interface
- the BSC is aware of physical channels and must be significantly modified when introducing new air interfaces

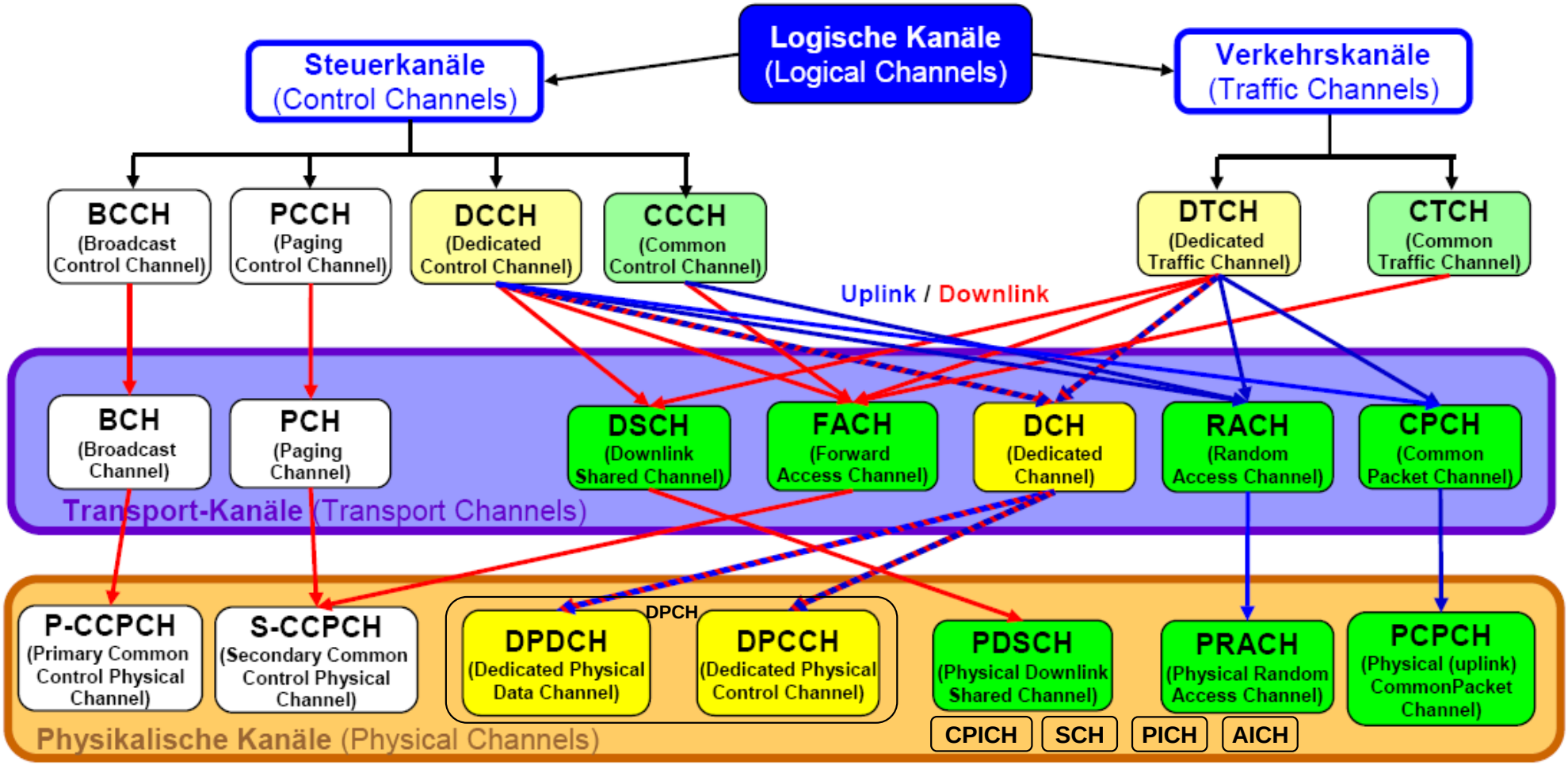
UMTS

- designed for multiple air interfaces (UTRAN/TDD, UTRAN/FDD)
- introduction of new transport channels which are independent of the air interface
- Physical Channels are not visible for the RNC
- Logical Channels describe what is transported (i.e. the types of information to be transmitted)
- Transport Channels describe how the Logical Channels are to be transmitted
- Physical Channels represent the transmission media providing the platform through which the information is actually transferred

Logical, Physical and Transport Channels - Definitions

- **Logical Cannels:**
  - Comparable to GSM, a set of logical channel types is defined in UMTS for different kinds of data transfer services. Each logical channel type is defined by „what type of information“ is transferred. The UMTS Logical Channels are described in 3GPP TS 25.301
- **Transport Channels:**
  - Different to GSM, in UMTS a new concept - the concept of Transport Channels - has been defined. Transport Channels are described by „how and with what characteristics data are transferred over the radio interface“. Different Logical Channels can be mapped together onto one Transport Channel.
  - The Transport Channels can be sub-divided into two general classes:
    - Common Transport Channels, where there is a need for in-band identification of the UEs when particular UEs are addressed
    - Dedicated Transport Channels, where the UEs are identified by the physical channel, i.e. code and frequency (for FDD) and code, time slot and frequency (for TDD)
  - The UMTS Transport Channels are described in 3GPP TS 25.301. The mapping of Logical Channels onto Transport Channels is described in 3GPP TS 25.301, too
- **Physical Channels:**
  - Physical channel describe the physical transmission of the information over the radio interface. In UMTS Physical Channels for FDD are characterized by the code and frequency (UL & DL) and for TDD they are characterized by code, frequency and time slot TS
  - The UMTS Physical Channels and the mapping of Transport Channels onto Physical Channels are described in 3GPP TS 25.211 for FDD and in 3GPP TS 25.221 for TDD
  - A general overview of the UMTS physical layer is given in 3GPP TS 25.201. Details of the physical layer are given in 3GPP TS 25.211-25.215 for FDD, and in 3GPP TS 25.221–25.225 for TDD

Logical, Physical and Transport Channels in UMTS (FDD)



Logical Channels - Overview

- **Control Channels**
  - **Broadcast Control Channel (BCCH)**
    - downlink channel for broadcasting system control information
  - **Paging Control Channel (PCCH)**
    - downlink channel that transfer paging information
  - **Common Control Channel (CCH)**
    - bi-directional channel for transmitting control information between network and UEs
  - **Dedicated Control Channel (DCCH)**
    - point-to-point bi-directional channel that transmits dedicated control information between a UE and the network
  - **Shared Channel Control Channel (SHCCH) (TDD only)**
- **Traffic Channels**
  - **Dedicated Traffic Channel (DTCH)**
    - point-to-point channel in the uplink or downlink, dedicated to one UE, for the transfer of user information
  - **Common Traffic Channel (CTCH)**
    - point-to-multipoint unidirectional channel for transfer of dedicated user information for all UEs or a group of specified UEs

Transport Channels - Overview

- **Common Transport Channels**
  - **Random Access Channel (RACH)**
    - contention-based uplink channel used for transmission of relatively small amounts of data (examples: initial access or non-real-time dedicated control or traffic)
  - **Common Packet Channel (CPCH) (FDD only)**
    - contention-based channel used for uplink transmission of bursty data traffic
    - shared by the UEs in a cell
  - **Forward Access Channel (FACH)**
    - common downlink channel used for transmission of relatively small amount of data
  - **Downlink Shared Channel (DSCH) (FDD only)**
    - downlink channel shared by several UEs carrying dedicated control or traffic data
  - **UL Shared Channel (USCH) (TDD only)**
    - similar to DSCH, but in uplink
  - **Broadcast Channel (BCH)**
    - downlink channel used for broadcast of system information into an entire cell
  - **Paging Channel (PCH)**
    - downlink channel used for broadcast of control information into an entire cell
    - used for paging and notification
- **Dedicated Transport Channels**
  - **Dedicated Channel (DCH)**
    - channel dedicated to one UE used in uplink or downlink

Physical Channels - Overview (1)

- **Common Physical Channels (1)**
  - **Primary Common Control Physical Channel (P-CCPCH)**
    - DL physical channel used to carry the BCH transport channel
  - **Secondary Common Control Physical Channel (S-CCPCH)**
    - DL physical channel used to carry the transport channels FACH and PCH
    - FACH and PCH can be mapped to the same or separate S-CCPCHs
  - **Physical Downlink Shared Channel (PDSCH)**
    - DL physical channel associated with a DL DPCH
    - shared by several users based on code-multiplexing
  - **Physical Uplink Shared Channel (USCH) (TDD only)**
    - UL physical channel associated with USCH
  - **Physical Random Access Channel (PRACH)**
    - contention-based UL physical channel carrying RACH data
    - used for initial network access and to carry small non-real-time data packets on common resources in the UL
  - **Physical Common Packet Channel (PCPCH) (FDD only)**
    - contention-based UL physical channel for infrequent data packets on common resources
    - can be regarded as PRACH extension

Physical Channels - Overview (2)

- **Common Physical Channels (2)**
  - **Common Pilot Channel (CPICH) (FDD only)**
    - fixed rate DL physical channel carrying a predefined bit sequence (cell scrambling code)
  - **Synchronisation Channel (SCH)**
    - DL physical channel used for cell search
    - needed by the UE for time synchronisation on basis of a chip, time slot and frame
    - provides the scrambling code group of a cell
  - **Page Indication Channel (PICH)**
    - DL physical channel used to provide UEs with efficient sleep-mode operation
    - carries the Page Indicators PI
  - **Acquisition Indication Channel (AICH) (FDD only)**
    - DL physical channel used to indicate the reception of the PRACH/PCPCH preamble
    - carries the Acquisition Indicators AI
  - **Physical Node B Synchronization Channel (PNBSCH) (TDD only)**
    - DL only

Physical Channels - Overview (3)

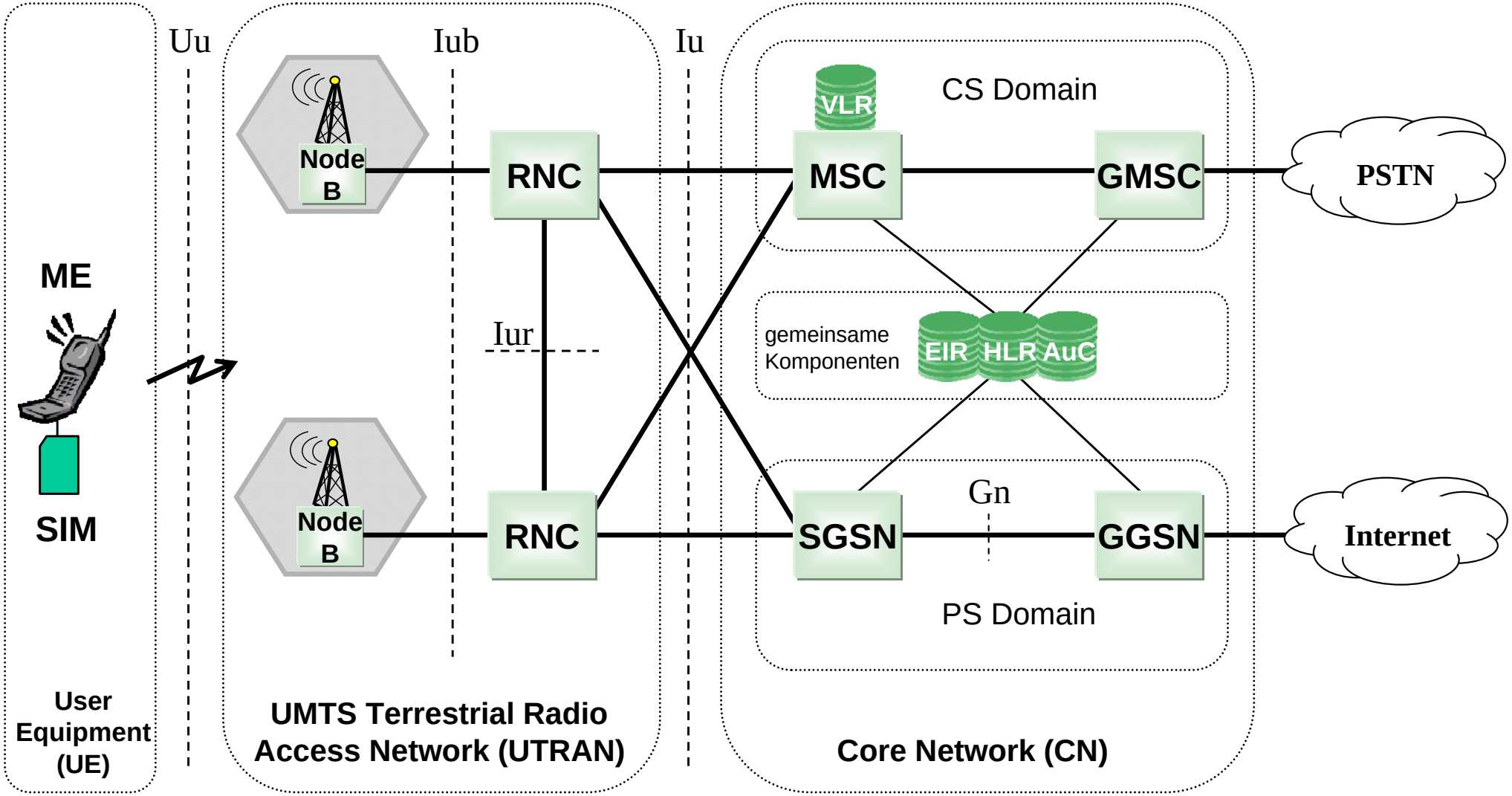
- **Dedicated Physical Channels - FDD**
  - **Dedicated Physical Data Channel (DPDCH)**
    - contains the user data including higher layer control information
  - **Dedicated Physical Control Channel (DPCCH)**
    - contains the physical layer control information necessary to maintain the connection

  Remark: DPDCH and DPCCH are multiplexed onto the same signal:
  - DPDCH and DPCCH are code multiplexed in uplink
  - DPDCH and DPCCH are time multiplexed (on the basis of one timeslot) onto the dedicated physical channel (DPCH) in downlink

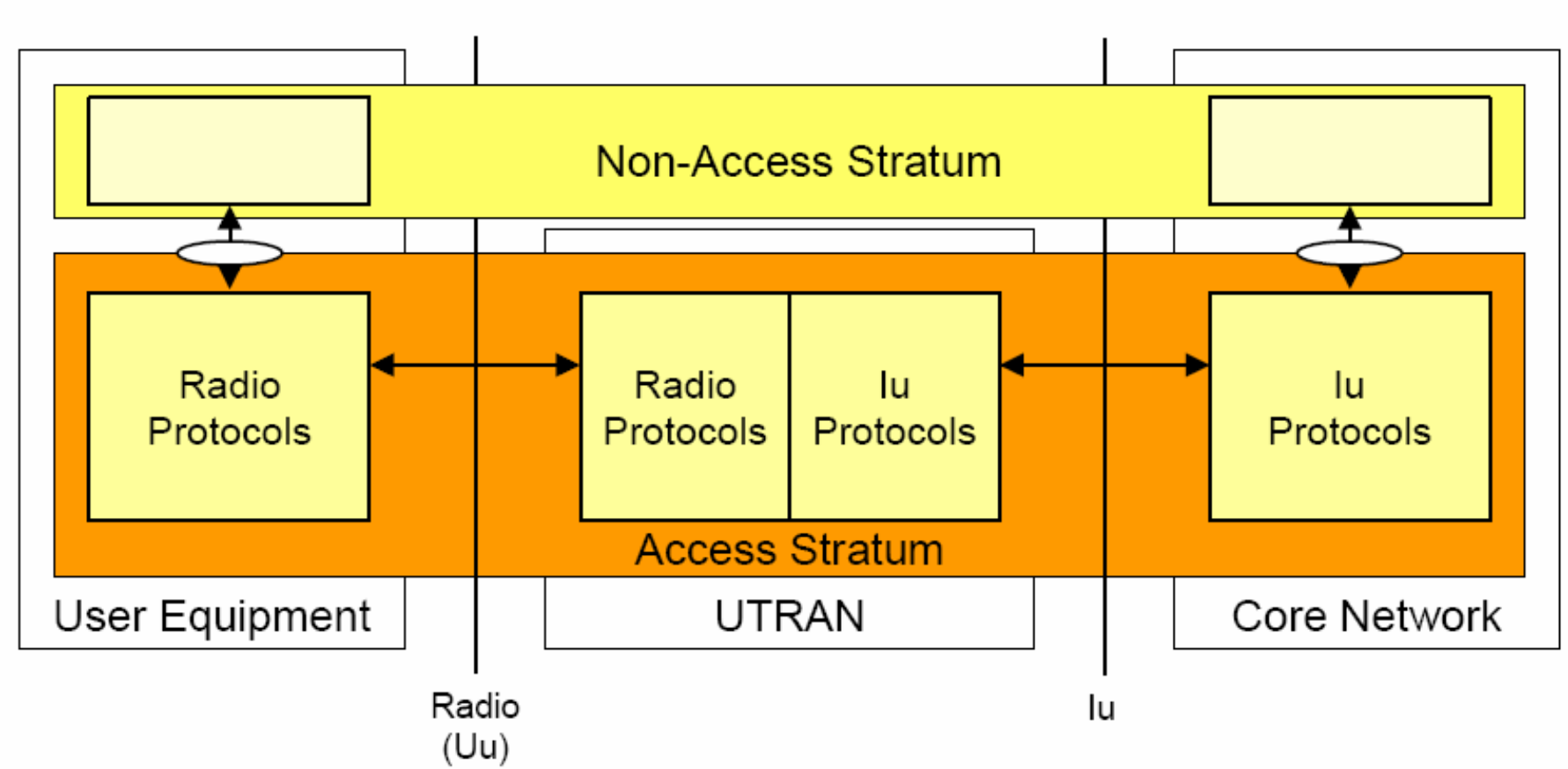
- **Dedicated Physical Channels -TDD**
  - **Dedicated Physical Channel (DPCH)**
    - characterized by spreading code and timeslot

Cellular Mobile Networks - UMTS
UMTS Protocol Architecture

UMTS System Architecture



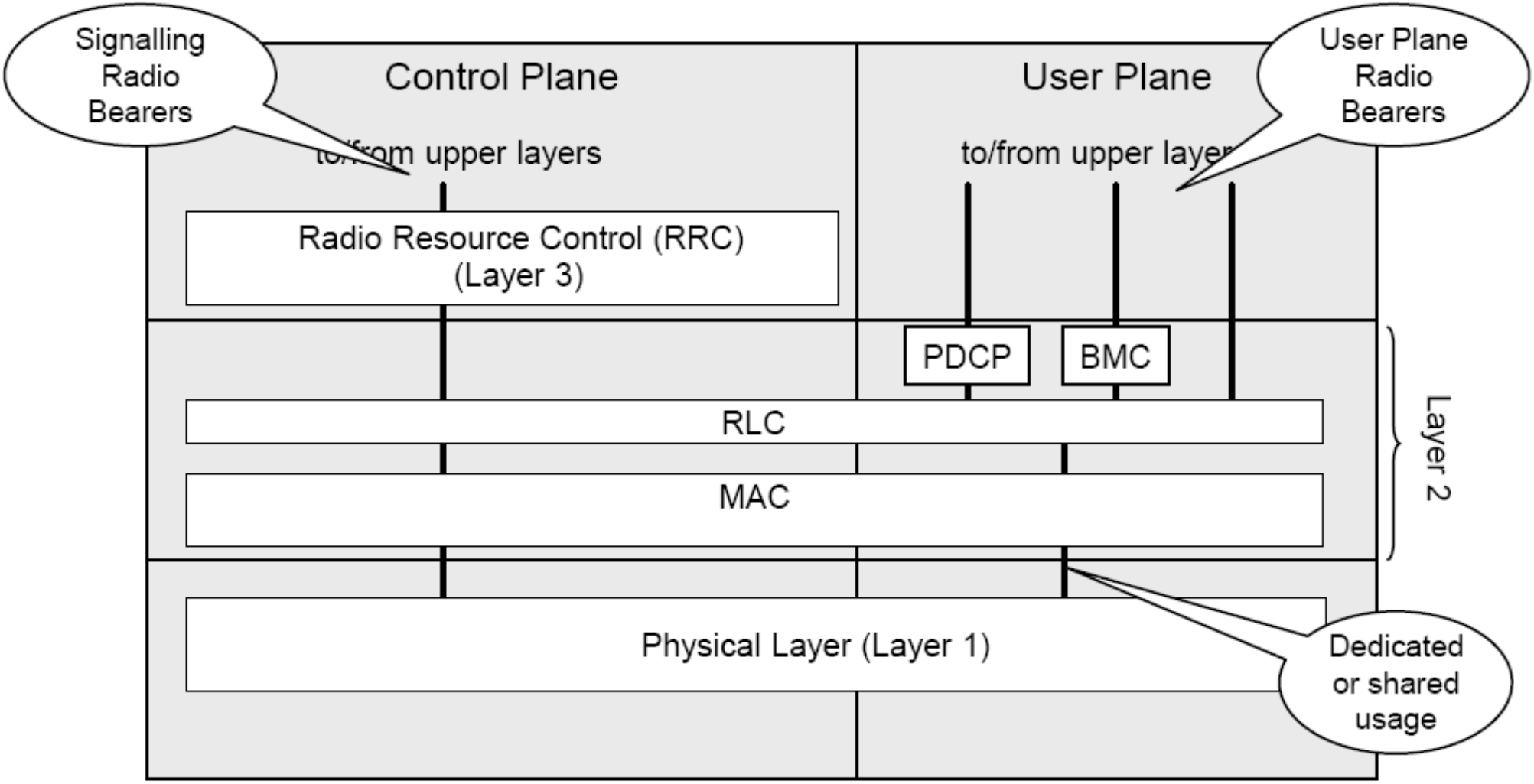
UMTS Protocol Architecture



Remark: the UMTS Non-Access Stratum signalling is much like in GSM/GPRS:

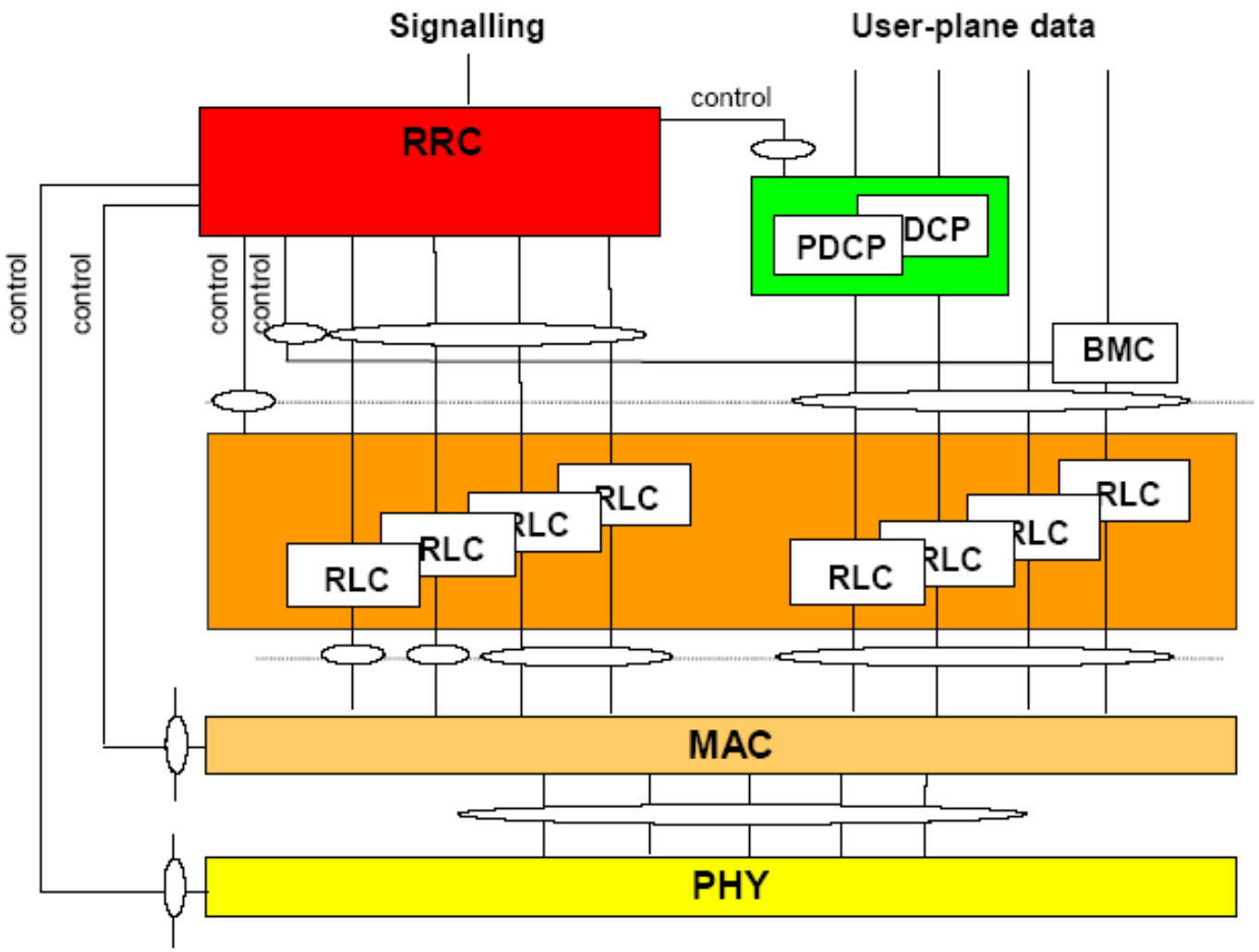
- Connection Control
- (GPRS) Mobility Management
- Session Management

Radio Interface (U_U) Protocols - Overview



PDCP = Packet Data Convergence Protocol
BMC = Broadcast/Multicast Control Protocol

Radio Interface (U_U) Protocols - Details



Radio Resource Control:
Control of radio resources and bearers

Packet Data Convergence Protocol:
Header Compression

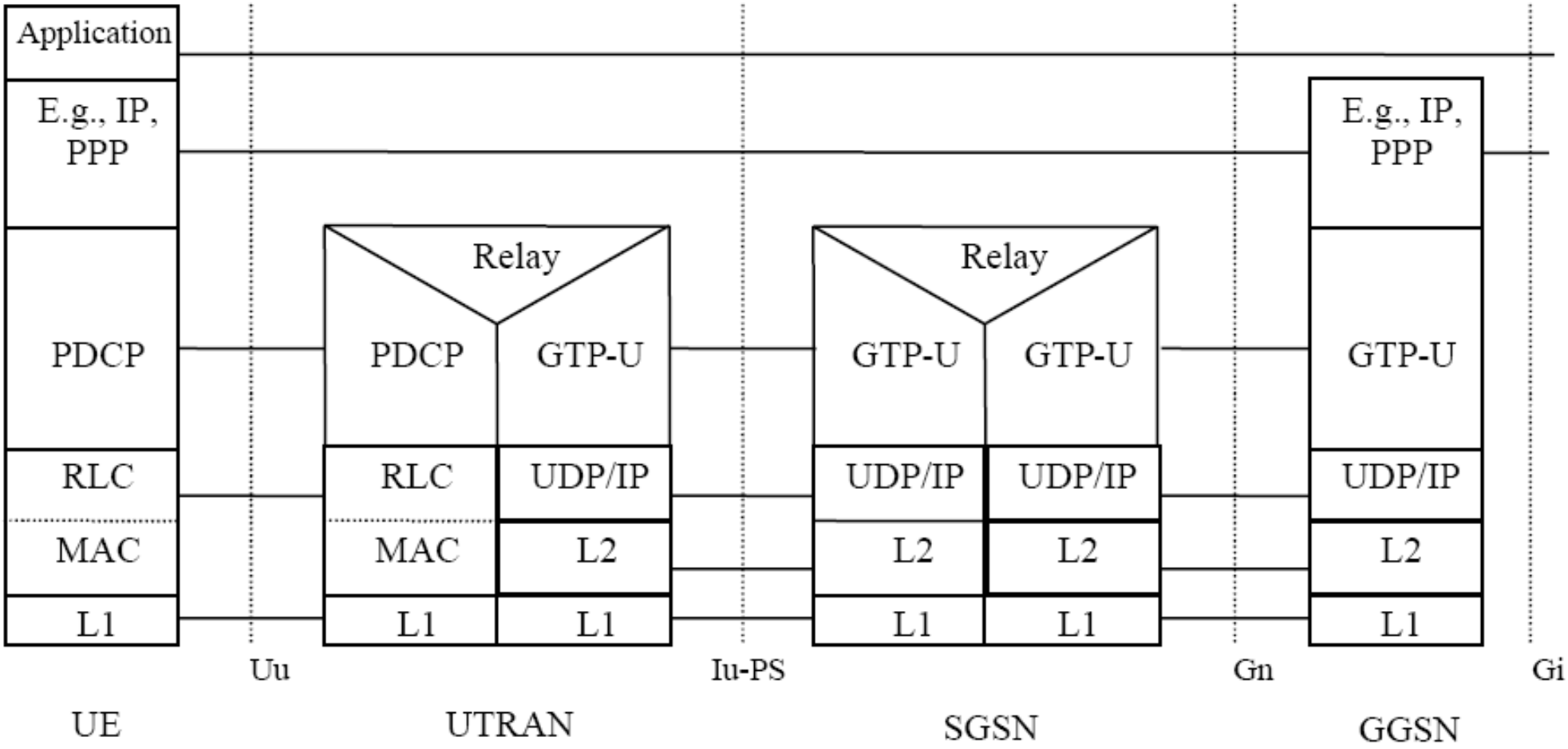
Broadcast/Multicast Control

Radio Link Control:
Error and flow control

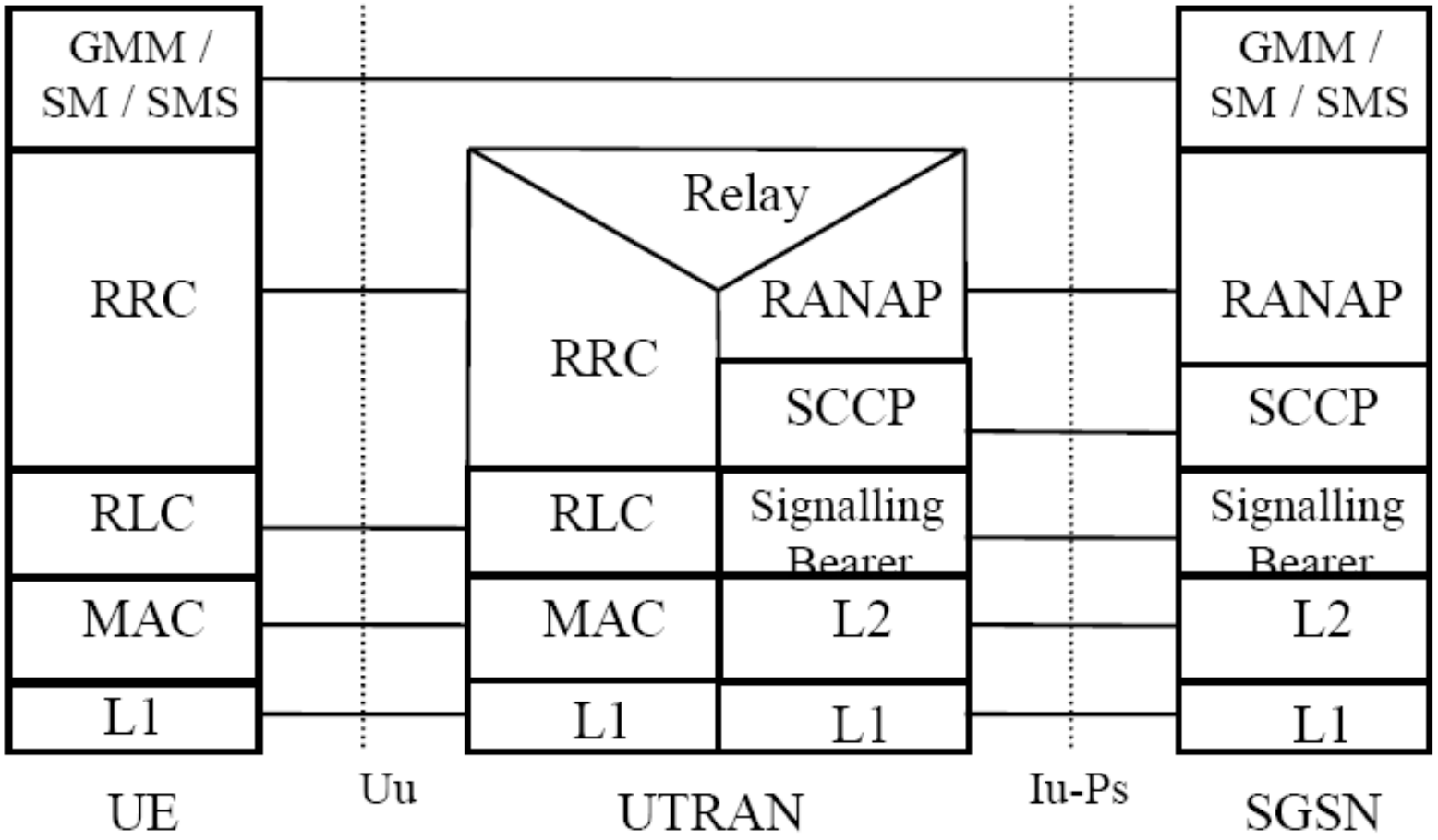
Medium Access Control:
Scheduling of radio resources

Physical Layer:
Coding and radio transmission

User Plane Protocols (PS Domain) - Overview



Control Plane Protocols (PS Domain) - Overview



Radio Interface (U_U) Protocols - Details

Packet Data Control Protocol (PDCP) Functions (User Plane, PS):

- Header compression and decompression of IP data streams (e.g. TCP/IP and RTP/UDP/IP headers for IPv4 and IPv6) at the transmitting and receiving entity, respectively
- Transfer of user data; this function is used for conveyance of data between users of PDCP services
- Maintenance of PDCP sequence numbers for radio bearers that are configured to support loss-less SRNS Relocation

Broadcast and Multicast Control (BMC) Functions (User Plane, PS):

- Scheduling and delivery of cell broadcast and multicast messages

Radio Interface (U_U) Protocols - Details

Radio Resource Control (RRC) Functions (Control Plane):

- Broadcast of information related to the non-access stratum
- Broadcast of information related to the access stratum
- Establishment, maintenance and release of an RRC connection between UE and UTRAN
- Establishment, reconfiguration and release of Radio Bearers
- Assignment, reconfiguration and release of radio resources for the RRC connections
- RRC connection mobility functions
- Control of requested QoS
- UE measurement reporting and control of the reporting
- Outer loop power control
- Control of ciphering
- Slow Dynamic Channel Allocation (TDD mode)
- Paging
- Initial cell selection and cell re-selection
- Arbitration of radio resources on uplink DCH
- RRC message integrity protection
- Timing advance (TDD mode)
- Cell Broadcast Service control

Radio Interface (U_U) Protocols - Details

Radio Link Control (RLC) Functions:

- Management of RLC connections
- Transfer of data: RLC supports three types of operation:
  - Acknowledged Mode (with ARQ and optional in-sequence delivery)
  - Unacknowledged Mode (including sequence numbers)
  - Transparent Mode (no overhead introduced, ciphering in MAC)
- Segmentation and Re-Assembly
- Padding
- Flow Control
- Ciphering
- Error detection
- Support of a suspend/resume mechanism

Radio Interface (U_U) Protocols - Details

Medium Access Control Protocol (MAC) Functions:

- Mapping between logical channels and transport channels (what → how)
- Selection of an appropriate Transport Format for each Transport Channel depending on the instantaneous source rate
- Priority handling between data flows of one UE (MAC-d)
- Priority handling between UEs by means of dynamic scheduling (MAC-c/sh)
- Identification of UEs on common transport channels
- Multiplexing/demultiplexing of upper layer PDUs into/from transport blocks delivered to/from the physical layer on common transport channels
- Multiplexing/demultiplexing of upper layer PDUs into/from transport block set delivered to/from the physical layer on dedicated transport channels
- Traffic volume measurement
- Transport channel type switching
- Ciphering for transparent mode RLC

Non-Access Stratum (Control Plane) Protocols

Non-Access Stratum Protocols:

- **Mobility Management (GMM):**

  The main purpose of mobility management is to support the mobility of the mobile station; in addition, some security functions for authentication and for the protection of the user identity are included

- **Session Management (SM):**

  For each session, a so-called PDP context is created, which describes the characteristics of the session; once a mobile station has an active PDP context, it is visible in the external Packet Data Network and can send and receive data packets

RAN (I_U, I_{Ur}, I_{Ub}) (Control Plane) Protocols - Details

RANAP (I_U) Functions (1):

- Overall Radio Access Bearer (RABs) management; this function is responsible for setting up, modifying and releasing RABs
- Queuing the set-up of RABs; the purpose of this function is to allow placing some requested RABs into a queue and indicate the peer entity about the queuing
- Requesting RAB release; while the overall RAB management is a function of the CN, the RNC has the capability to request the release of RAB
- RNS Relocation; this function enables to change the serving RNC functionality as well as the related I_U resources (RAB(s) and Signalling connection) from one RNC to another
- Release of all I_U connections resources; this function is used to explicitly release all resources related to one I_U connection
- Requesting the release of all I_U connection resources; while the I_U release is managed from the CN, the RNC has the capability to request the release of all I_U connection resources from the corresponding I_U connection

RAN (I_U, I_{Ur}, I_{Ub}) (Control Plane) Protocols - Details

RANAP (I_U) Functions (2):

- SRNS context forwarding function; this function is responsible for transferring SRNS context from the RNC to the CN for intersystem change in case of packet forwarding
- Controlling overload in the I_U interface; this function allows adjusting the load in the I_U interface.
- Resetting the I_U; this function is used for resetting an I_U interface
- Sending the UE Common ID (permanent NAS UE identity) to the RNC; this function makes the RNC aware of the UE's Common ID
- Paging the user; this function provides the CN with the capability to page the UE
- Controlling the tracing of the UE activity; this function allows setting the trace mode for a given UE; this function also allows the deactivation of a previously established trace

RAN (I_U, I_{Ur}, I_{Ub}) (Control Plane) Protocols - Details

RANAP (I_U) Functions (3):

- Transport of NAS information between UE and CN; this function has two sub-classes:
  - Transport of the initial NAS signalling message from the UE to CN; this function transfers transparently the NAS information; as a consequence also the I_U signalling connection is set up
  - Transport of NAS signalling messages between UE and CN; this function transfers transparently the NAS signalling messages on the existing I_U signalling connection; it also includes a specific service to handle signalling messages differently
- Controlling the security mode in the UTRAN; this function is used to send the security keys (ciphering and integrity protection) to the UTRAN, and setting the operation mode for security functions
- Controlling location reporting; this function allows the CN to operate the mode in which the UTRAN reports the location of the UE
- Location reporting; this function is used for transferring the actual location information from the RNC to the CN

RAN (I_U, I_{Ur}, I_{Ub}) (Control Plane) Protocols - Details

RANAP (I_U) Functions (4):

- Data volume reporting function; this function is responsible for reporting unsuccessfully transmitted DL data volume over UTRAN for specific RABs
- Reporting general error situations; this function allows reporting of general error situations, for which function specific error messages have not been defined
- Location related data; this function allows the CN to either retrieve from the RNC deciphering keys (to be forwarded to the UE) for the broadcasted assistance data, or request the RNC to deliver dedicated assistance data to the UE

RAN (I_U, I_{Ur}, I_{Ub}) (Control Plane) Protocols - Details

NBAP (I_{Ub}) Functions:

- Radio Link Management and Supervision
- Cell Configuration Management
- Common Transport Channel Management
- Physical Shared Channel Management
- System Information Management
- Measurements on Common and Dedicated Resources
- Downlink Power Control Correction
- Error Indication
- Information Exchange

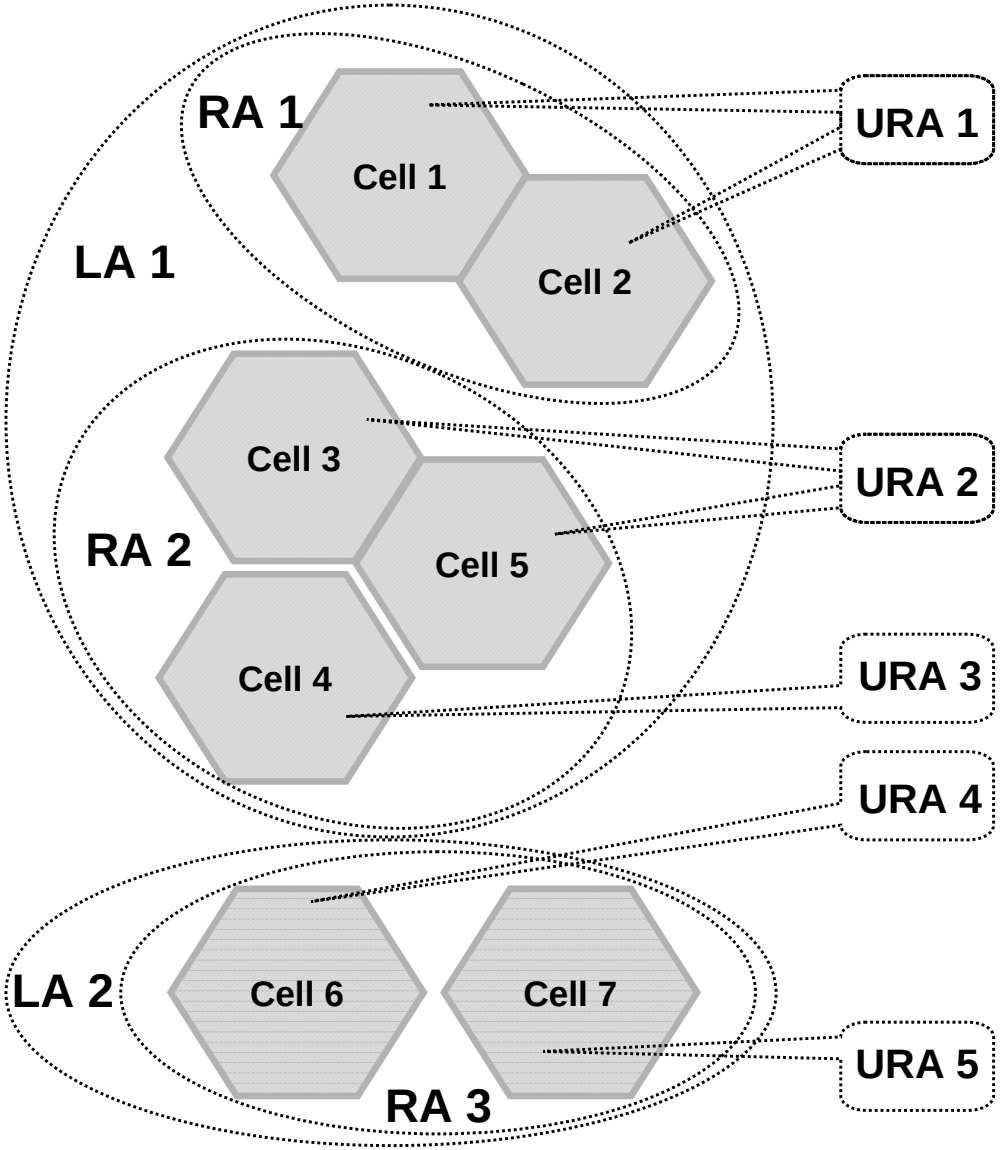
RAN (I_U, I_{Ur}, I_{Ub}) (Control Plane) Protocols - Details

RNSAP (I_{Ur}) Functions:

- Support of Mobility within UTRAN, e.g.:
  - support of SRNS relocation
  - paging support
  - transfer of CCCH signalling
- Control of dedicated transport channels over the I_{Ur}
- Control of common transport channels over the I_{Ur}
- Global procedures for information exchange between RNCs, e.g.:
  - exchange of radio resource management information

Cellular Mobile Networks - UMTS
UMTS Mobility Management

Location Regions: Location Area, Routing Area, URA



Location Area (LA):

- location region that consists of one or more cells for CS services
- explicitly assigned to one **MSC/VLR**
- may contain one or more RAs

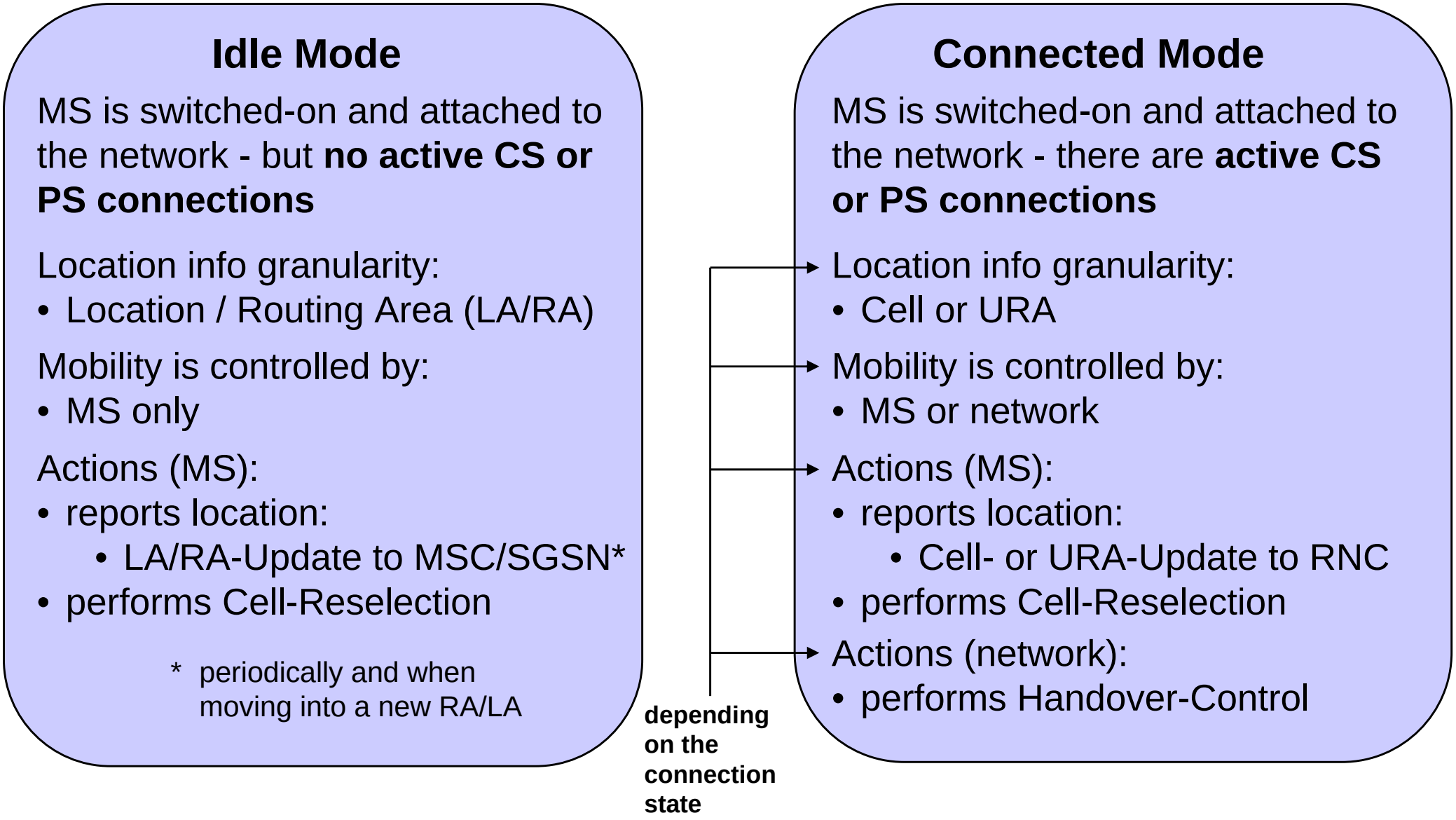
Routing Area (RA):

- location region that consists of one or more cells for PS services
- explicitly assigned to one **SGSN**
- smaller or equal size than LA
- may contain one or more URAs

UTRAN Registration Area (URA):

- location region that consists of one or more cells for PS services
- explicitly assigned to one **RNC**
- smaller or equal size than RA
- only used in Connected Mode

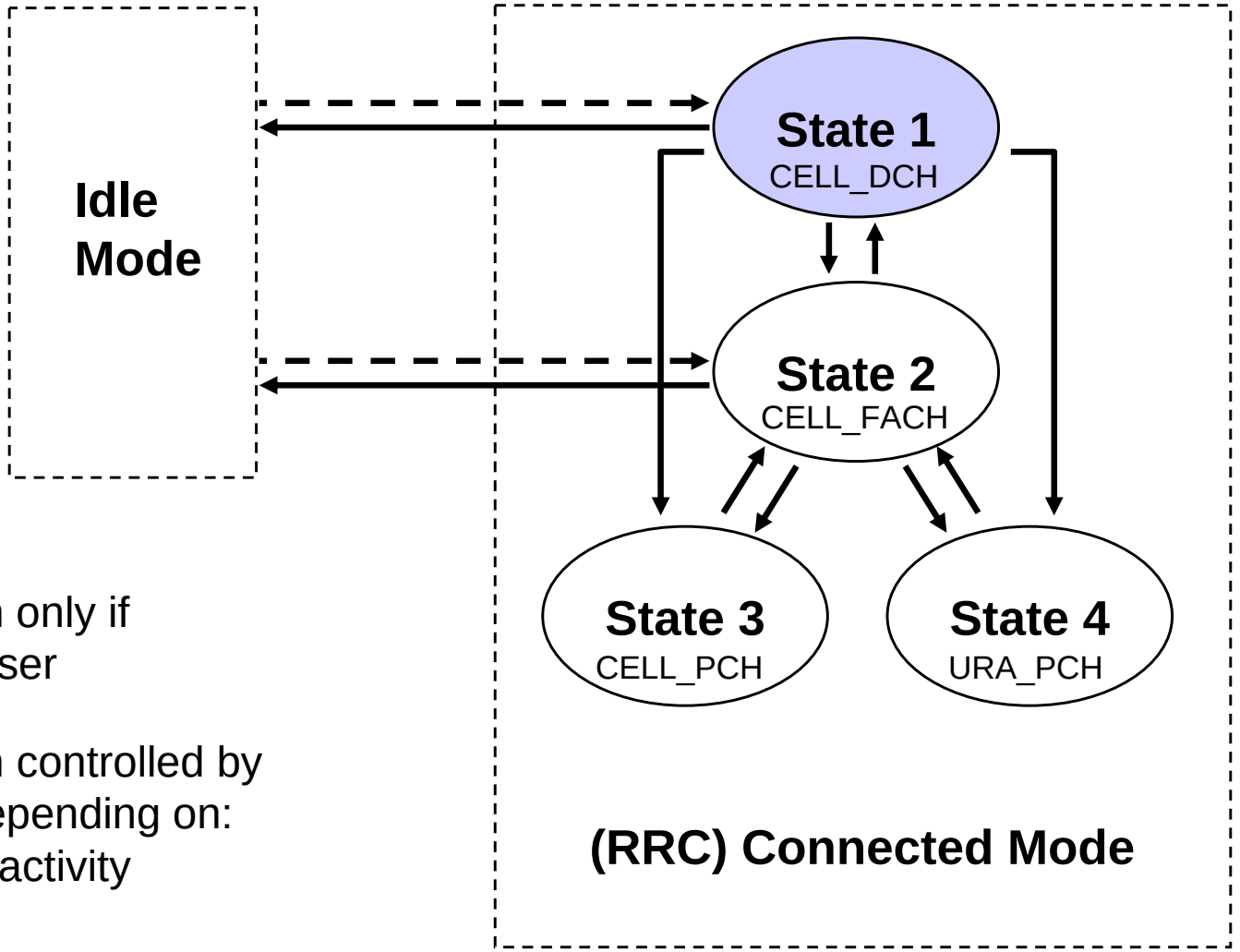
Mobility Functions in Idle and Connected Mode



Mobility in Connected Mode wrt. Connection State

	Cell Change	Location Reporting	Mobility Control	Examples
State 1)	via **Handover-Control**		**Network**	• CS connection • PS connection with high quality (e.g. VoIP) or high activity
State 2)	via **Handover-Control**		**Network**	• PS connection with average activity
	Cell-Reselection	**Cell-Update** to Serving-RNC (periodically and when moving into a new cell)	**MS**	
State 3)	**Cell-Reselection**	**Cell-Update** to Serving-RNC (periodically and when moving into a new cell)	**MS**	• PS connection with low activity
State 4)	**Cell-Reselection**	**URA-Update** to Serving-RNC (periodically and when moving into a new URA)	**MS**	• PS connection with very low activity

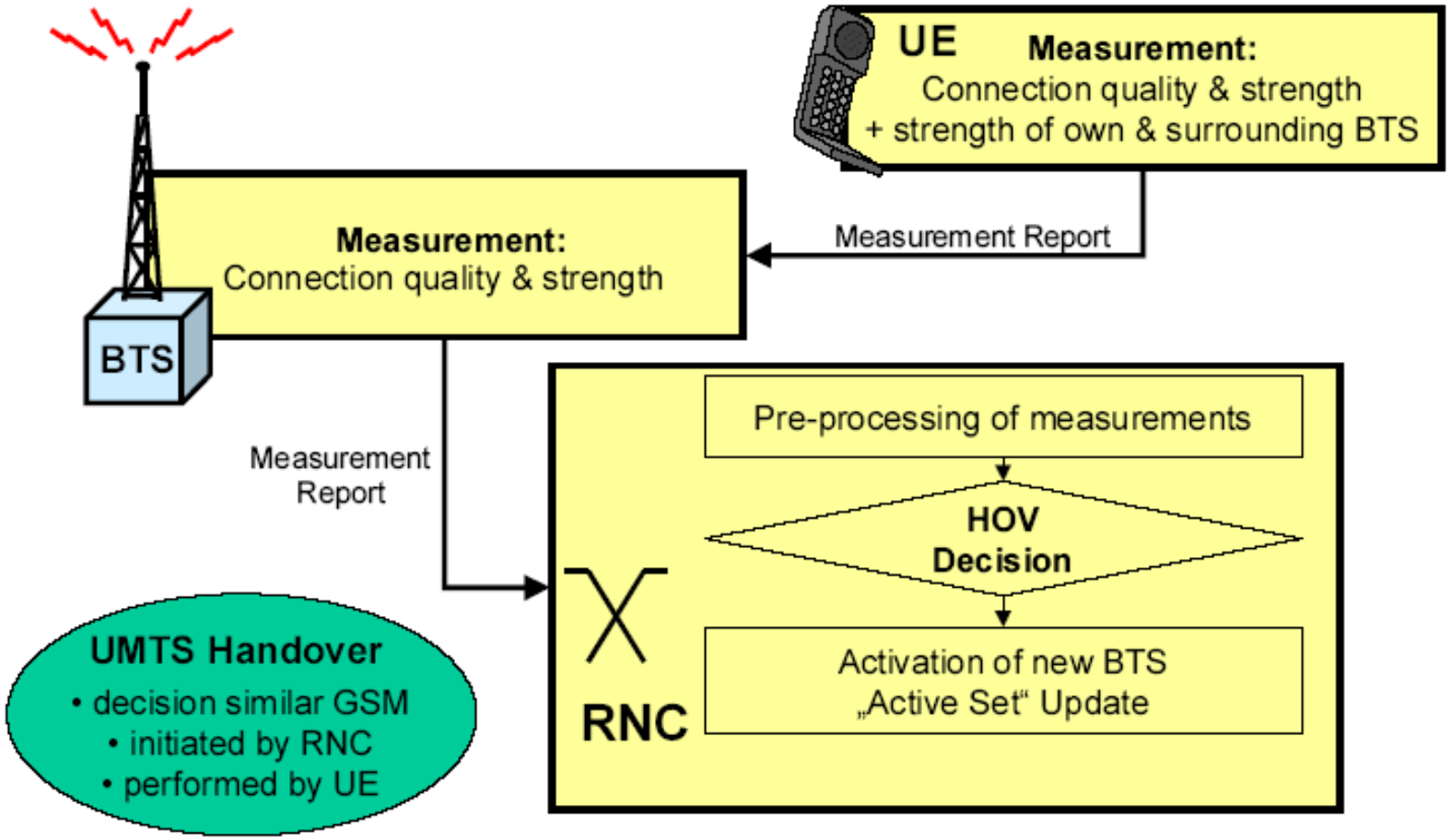
Feasible State Transitions



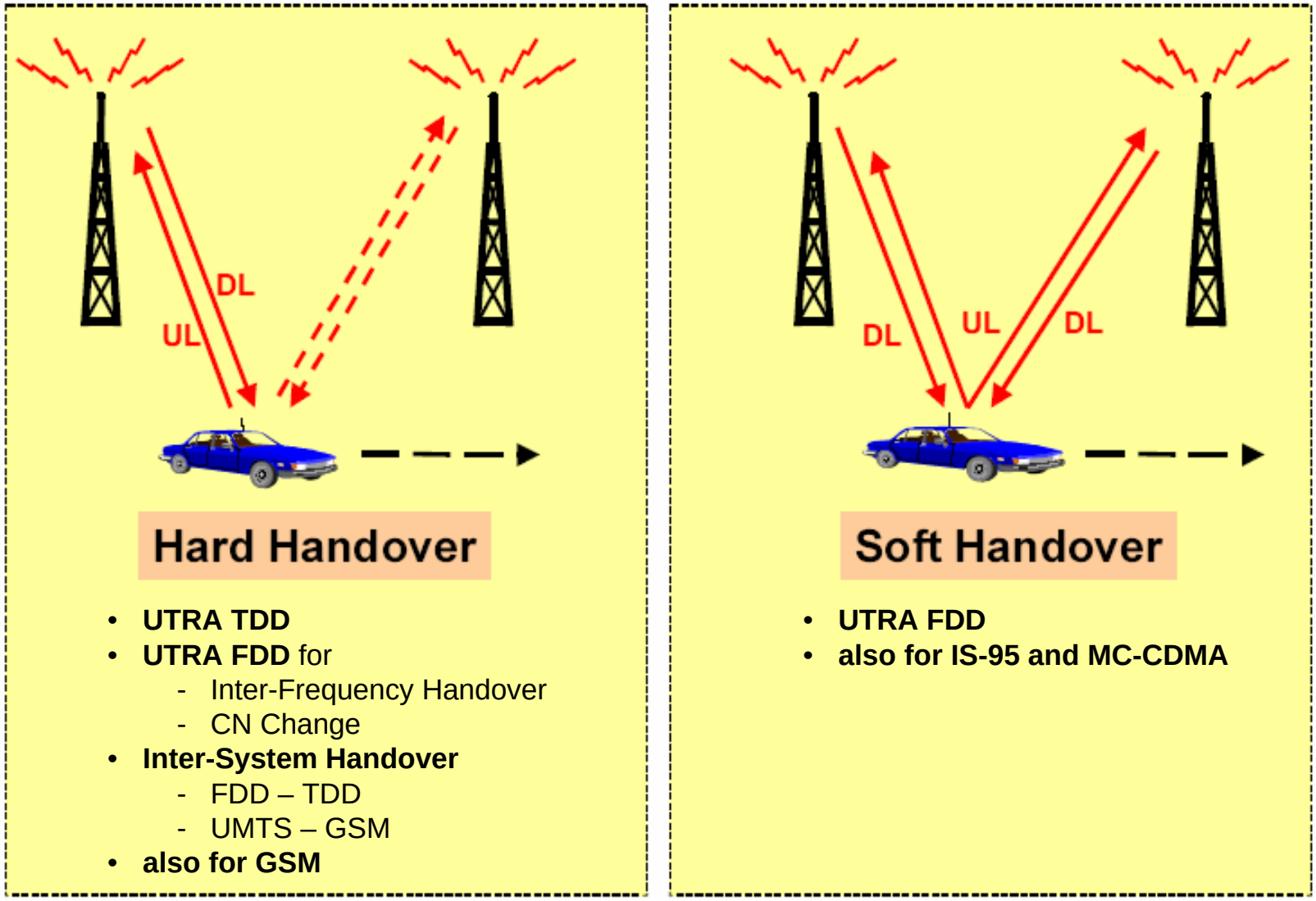
- - - state transition only if approved by user

——— state transition controlled by the network depending on:
- (data traffic) activity
- user velocity
- load, etc.

UMTS Handover Decision



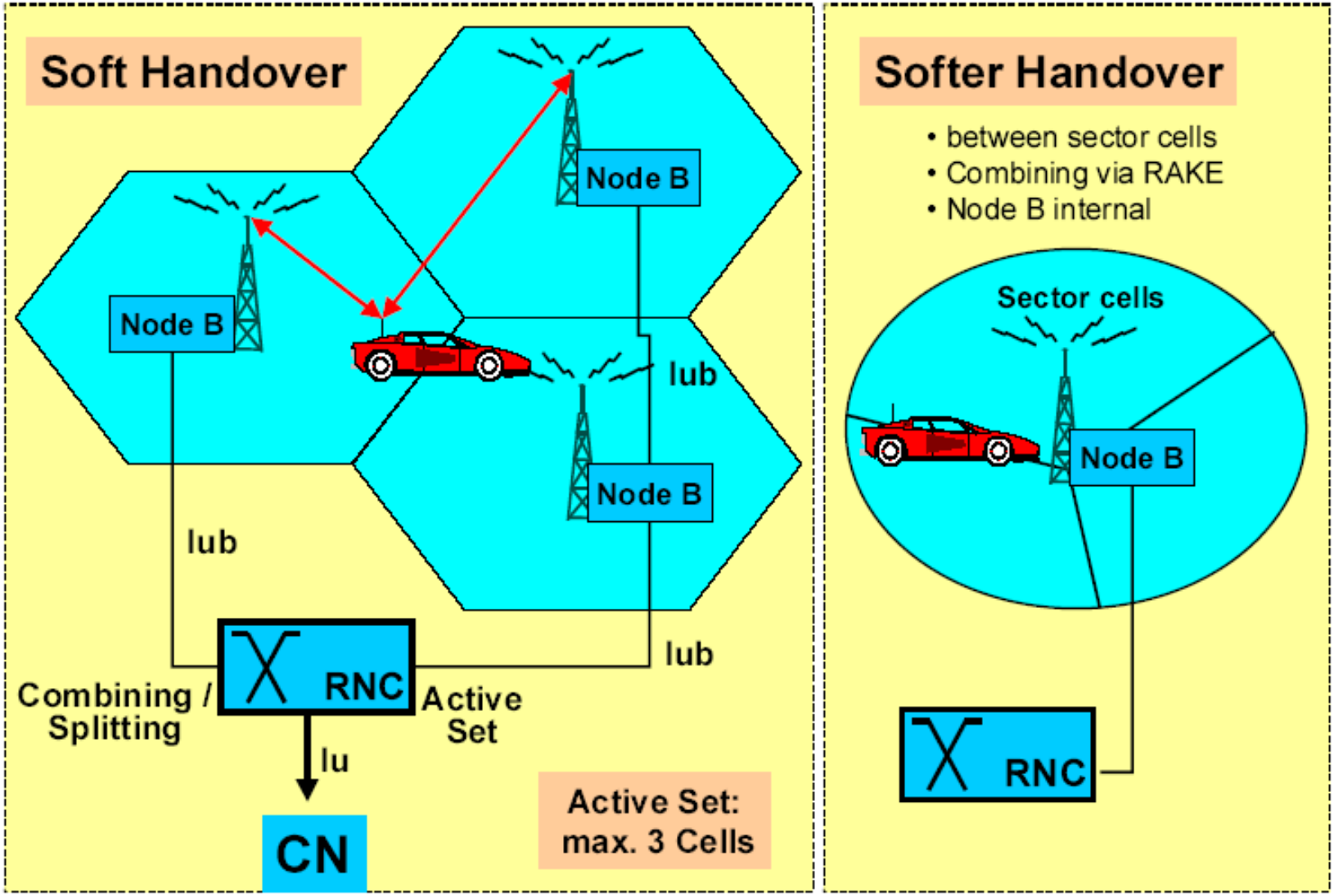
UMTS Handover Types - Hard vs. Soft Handover



- **UTRA TDD**
- **UTRA FDD** for
  - Inter-Frequency Handover
  - CN Change
- **Inter-System Handover**
  - FDD – TDD
  - UMTS – GSM
- **also for GSM**

- **UTRA FDD**
- **also for IS-95 and MC-CDMA**

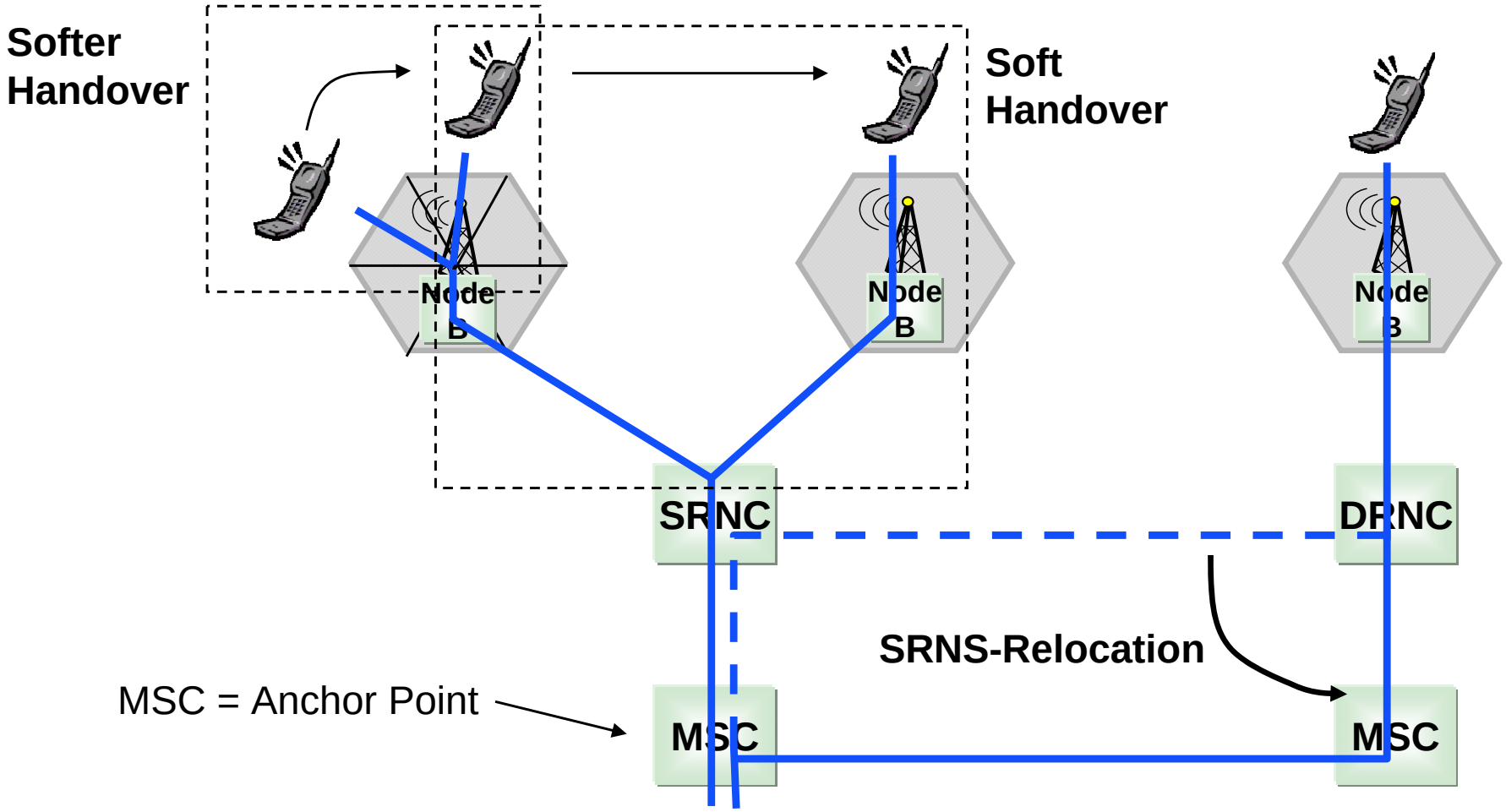
UMTS Handover Types - Soft vs. Softer Handover



UMTS Handover Types - Hard, Soft, Softer Handover

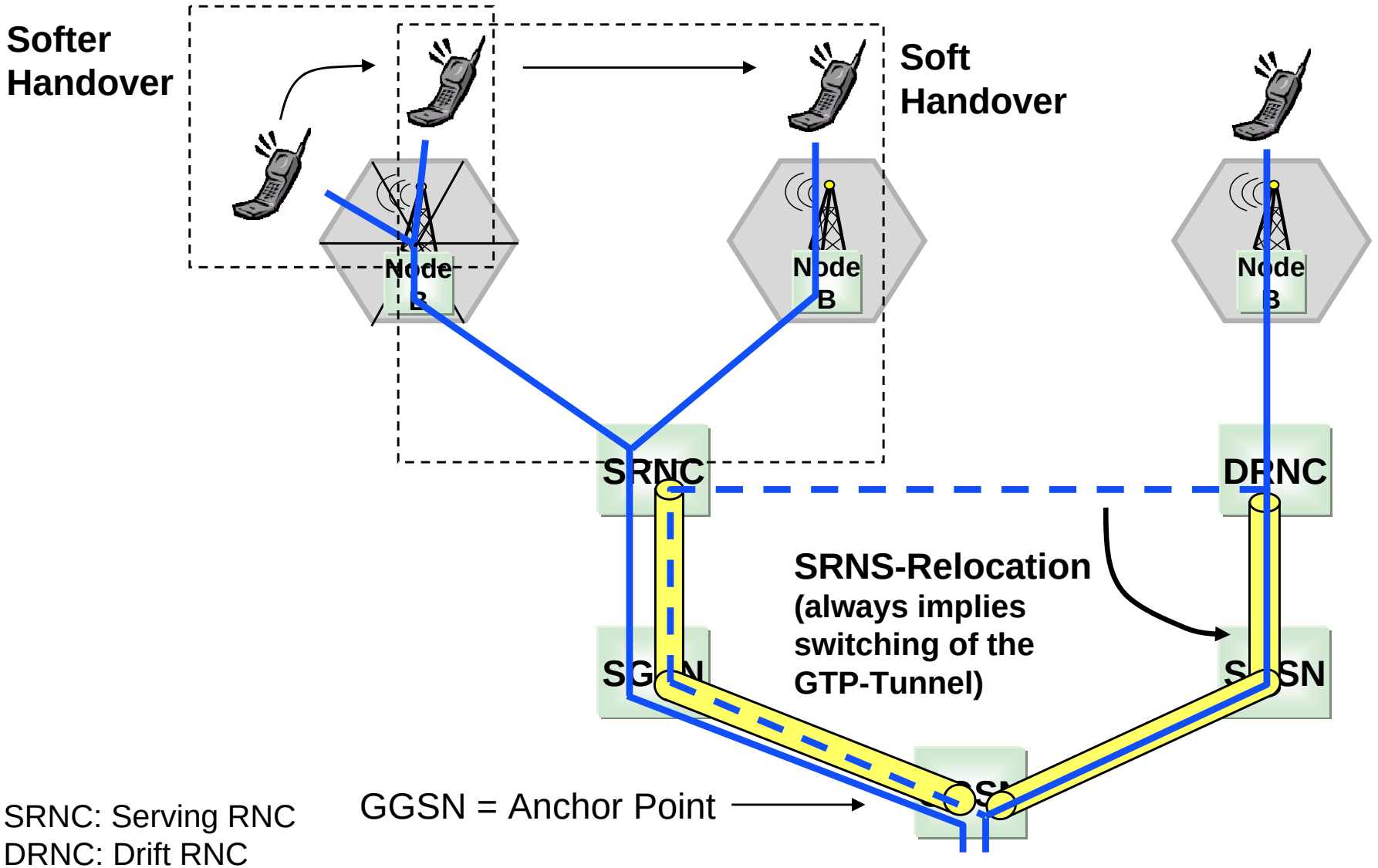
- Hard Handover:
  - Hard Handovers refer to handovers in which a mobile station (MS) transmits its user information only via one base station at any one time. Up until the time of the handover command, the MS communicates with the old base station over a specific physical channel. After the handover command, the MS changes the physical channel and then communicates with the new base station.
  - Hard handovers are used in GSM and the following cases in UMTS
    - during TDD / TDD handovers
    - during FDD handovers if the frequency (inter frequency handover) or the Core Network is changed
    - during inter-system handovers - e.g. when changing from FDD to TDD or from UMTS to GSM
- Soft Handover:
  - Soft Handovers refer to handovers in which a mobile station (MS) transmits its user information via more than one base station at the same time. Soft handovers can be used in CDMA systems in order to prevent an increase in power of the MS in boundary areas between different cells. This reduces the interference level and therefore increases the capacity of the system. Moreover, the contact with more than on base station ensures the connection to a moving MS in difficult terrain.
  - Soft handovers are used in IS-95 and MC-CDMA and in the following cases in UMTS:
    - during FDD / FDD handovers (without frequency changes)
- Softer Handover:
  - Softer Handovers are handovers between sector cells in the same Node B. The transmission information received via the antennas of the different sector cells is handled by different RAKE receivers and combined in the Node B itself (Maximum Ratio Combining - MRC). Softer handovers are internal Node B affairs. Additional (I_{Ub}) transmission capacity to the RNC is not required. The gain due to reception of additional signals in softer handovers is also known as macro diversity.

Handover and SRNS-Relocation for CS Connections



SRNC: Serving RNC
DRNC: Drift RNC

Handover and SRNS-Relocation for PS Connections



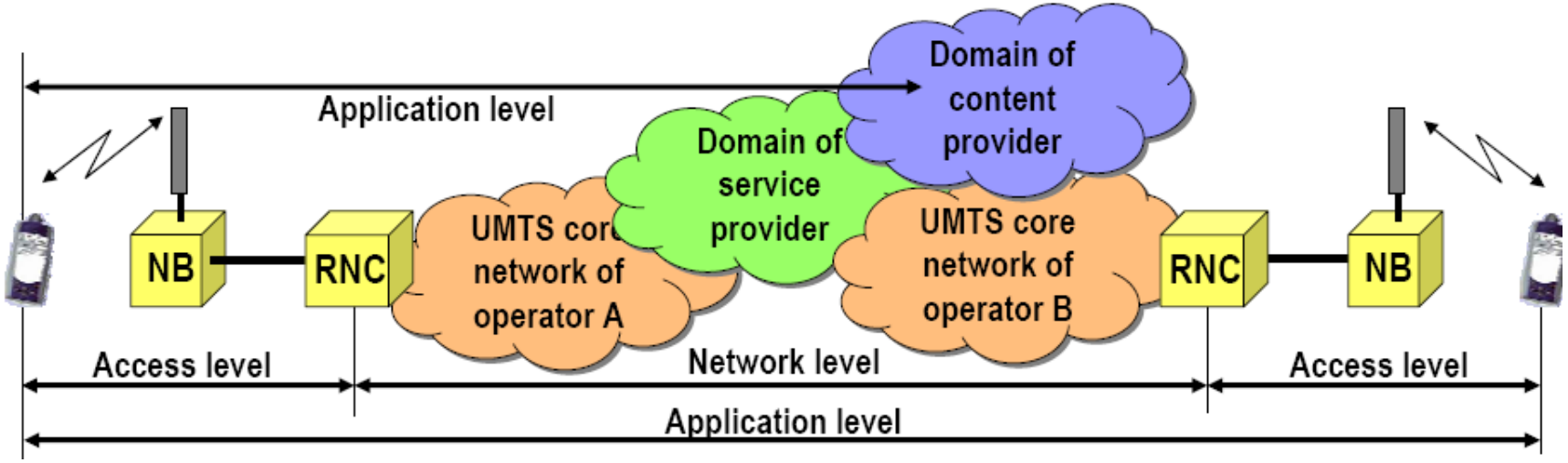
SRNC: Serving RNC
DRNC: Drift RNC

Cellular Mobile Networks - UMTS
UMTS Security Concept

Shortcomings of the GSM Security Concept

- Active Attacks
  - base station equipment may masquerade as a legitimate network element
  - corrupted terminal or corrupted base station
- Lack of confidence in cryptic algorithms
  - keys used for radio interface ciphering become vulnerable to brute force attacks where somebody tries all possible keys until one matches
- Encryption terminates too soon
  - sensitive control data, e.g. keys used for radio interface ciphering, are sent between different networks without ciphering
- Lawful interception
  - has not been considered during the GSM design phase and is thus not implemented
- Openness
  - parts of the security architecture are kept secret, e.g. the cryptic algorithms: this does not create trust in them in the long run because they are not publicly available for analysis and global secrets tend to be revealed sooner or later
- Flexibility
  - security functions cannot be upgraded and/or improved over time
- Lack of visibility
  - no indication to the user that encryption is on
  - no explicit confirmation to home network that authentication is properly used when customers roam

UMTS Security - Overview



- **Security at the access level**
  - secure user access to the UMTS network
  - security of connections at the access network level
  - based on the GSM access security model (but several enhancements have been made)
- **Security at the network level**
  - secure connections inside a UMTS network and between networks that are controlled by different operators and providers respectively
  - no enhancements in 3GPP R99 compared to GSM (major changes are expected for subsequent releases)
- **Security at the application level**
  - independent of the UMTS network itself
  - implemented according to the OSI model
  - includes SSL, S-MIME, PGP, S-HTTP, …

UMTS (Access Level) Security Features and Principles

- UMTS Security Features
  - mutual authentication of both the user and the network
  - use of temporary identities (similar to GSM)
  - radio access network encryption
  - protection of signaling integrity inside UTRAN
- Principles
  - build on the security concepts of GSM
    - adopt the security features from GSM that have proved to be needed and robust
    - try to ensure compatibility with GSM in order to ease interworking and inter-system handover
  - correct the problems with GSM addressing its real and perceived security weakness
  - requires minimal trust in serving network, but delegation of authentication to serving network
  - algorithms used for encryption and integrity protection are publicly available
  - algorithm for mutual authentication and generation of keys are operator-specific

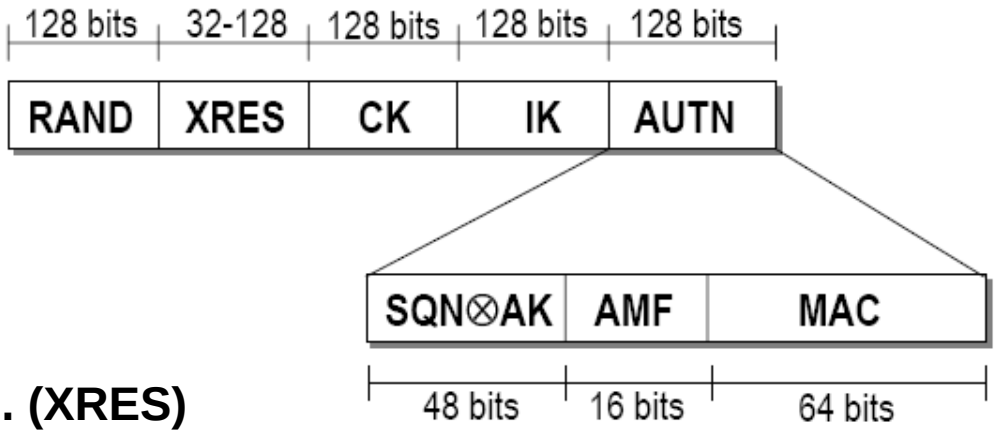
UMTS Cryptic Algorithms and Keys (1)

- Cryptic Algorithms: one-way functions f1...f5, f8, f9
  - properties of the one-way functions:
    - if the output of one function is known there exists no efficient algorithm to deduce any input that would produce the output
    - from the output of one function no information about the outputs of the other functions can be deduced
  - f1...f5: compute authentication vectors each including a CK and an IK
  - f8: generates the keystream block used for ciphering
  - f9: generates an identifier for integrity check (MAC-I)

UMTS Cryptic Algorithms and Keys (2)

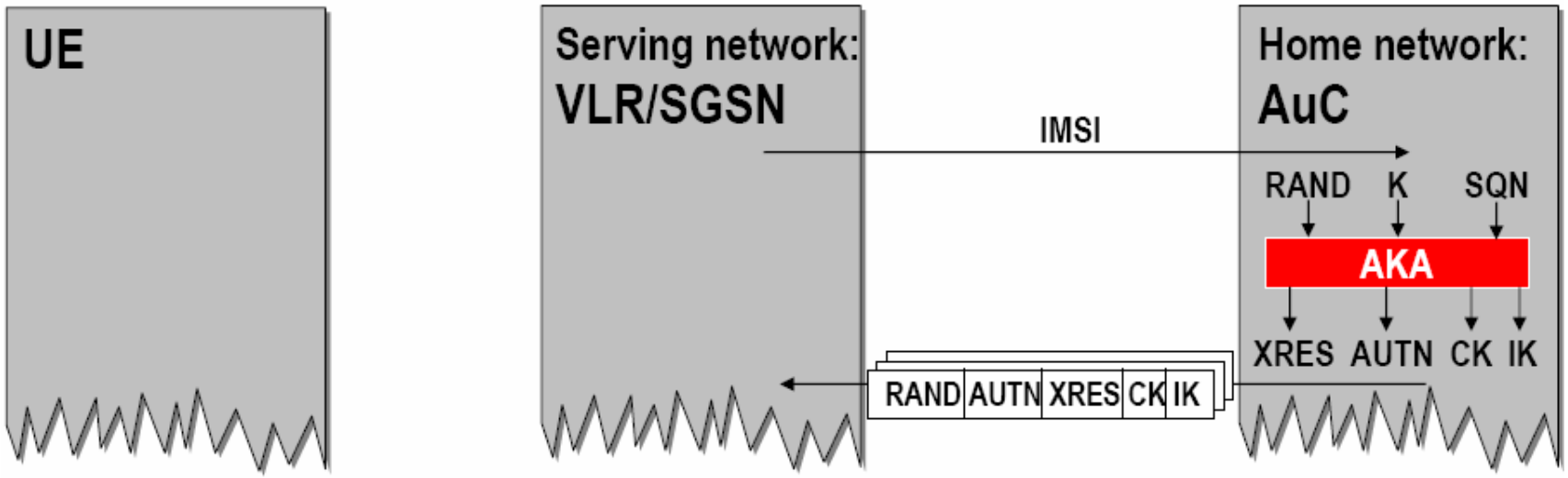
- Master Key K
  - counterpart of GSM´s secret key K_i
  - shared between the USIM of the user and the home network database
  - permanent secret with a length of 128 bits
- Cipher Key CK
  - counterpart of GSM´s secret key K_C
  - used for ciphering / deciphering with a stream cipher
  - generated during authentication and shared between the serving core network and the terminal
  - lenght 128 bits
- Integrity Key IK
  - used for generating a Message Authentication Code which is concatenated with each signaling message
  - generated during authentication and shared between the serving core network and the terminal
  - lenght 128 bits

UMTS Authentication Vector



- **Random Bit String (RAND)**
  - unpredictable, generated by the AuC
- **Response (RES) and Expected Resp. (XRES)**
  - needed for challenge-response mechanism
  - used for subscriber authentication (see GSM)
- **Authentication Token (AUTN)**
  - carries data which is analyzed by the USIM for network authentication
  - **Sequence Number (SQN)**
    - generated in an increasing order to prove later to the user that the generated authentication vector has not been used before
  - **Authentication Key (AK)**
    - used to cipher SQN (optional)
  - **Authentication Management Field (AMF)**
    - used for administrative purposes
  - **Message Authentication Code (MAC) and Expected MAC (X-MAC)**
    - compared with each other in order to finally verify that the serving network is trusted by the home network

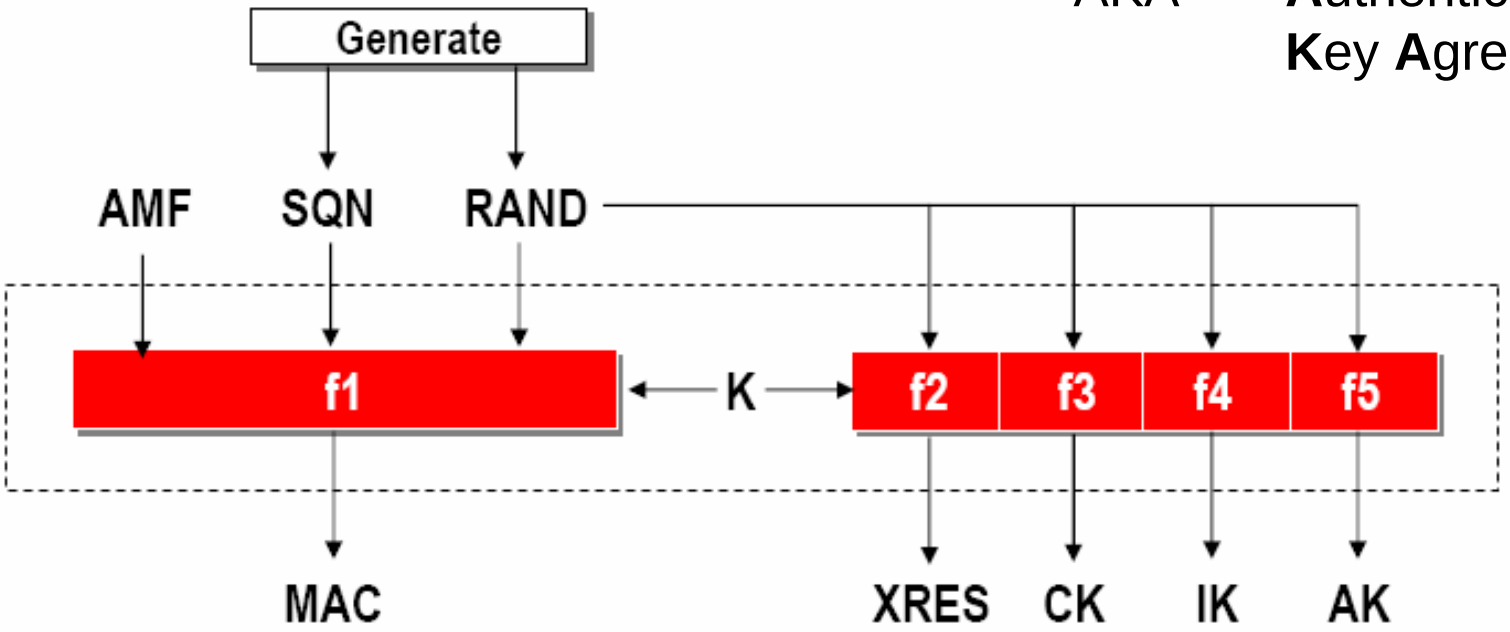
Authentication Vector Generation in the AuC (Home Netw.)



- In the serving network, one authentication vector is needed for each run of the authentication procedure
- AKA is started after the user is identified in the serving network, i.e. when the identity of the user (IMSI or TMSI) has been transmitted to the VLR/SGSN
- The home network generates a set of several authentication vectors
- Long distance signaling between serving and home network is not needed for each authentication event
- The VLR/SGSN may fetch new authentication vectors from AuC well before the number of stored vectors runs out

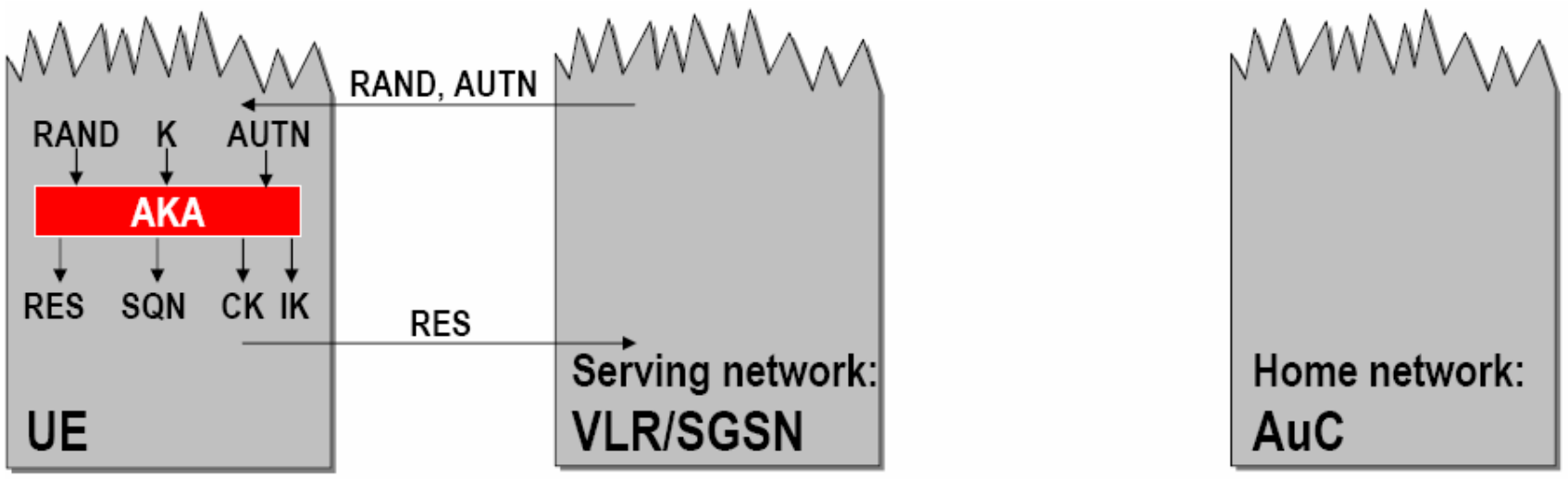
Authentication Vector Generation in the AuC - Details

AKA = **A**uthentication and **K**ey **A**greement



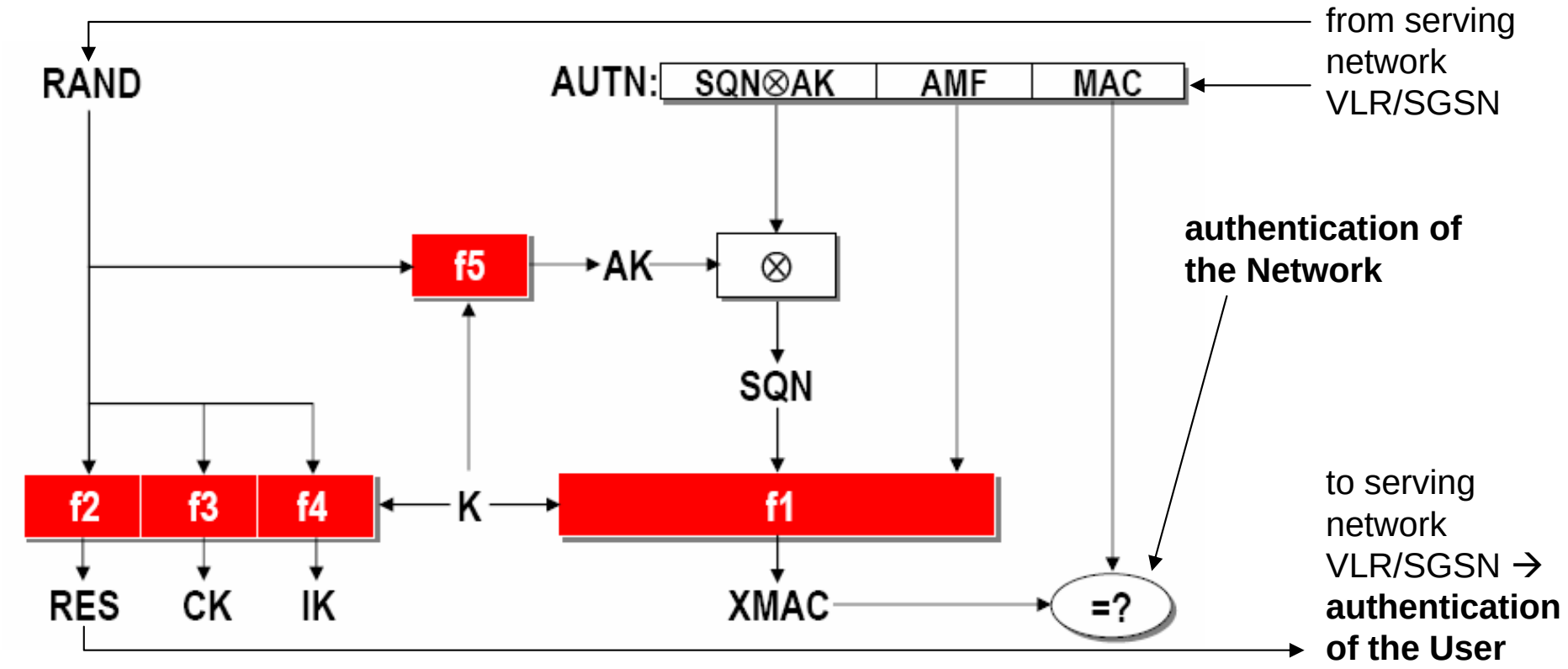
- f1: generation of MAC for later network authentication on the user side; SQN is picked up in an increasing order to prove to the user that the generated authentication vector has not been used before
- f2: generation of expected response XRES for user authentication by challenge-response mechanism
- f3 and f4: generation of cipher key CK and integrity key IK
- f5: generation of authentication key AK for ciphering SQN

User/Network Authentication



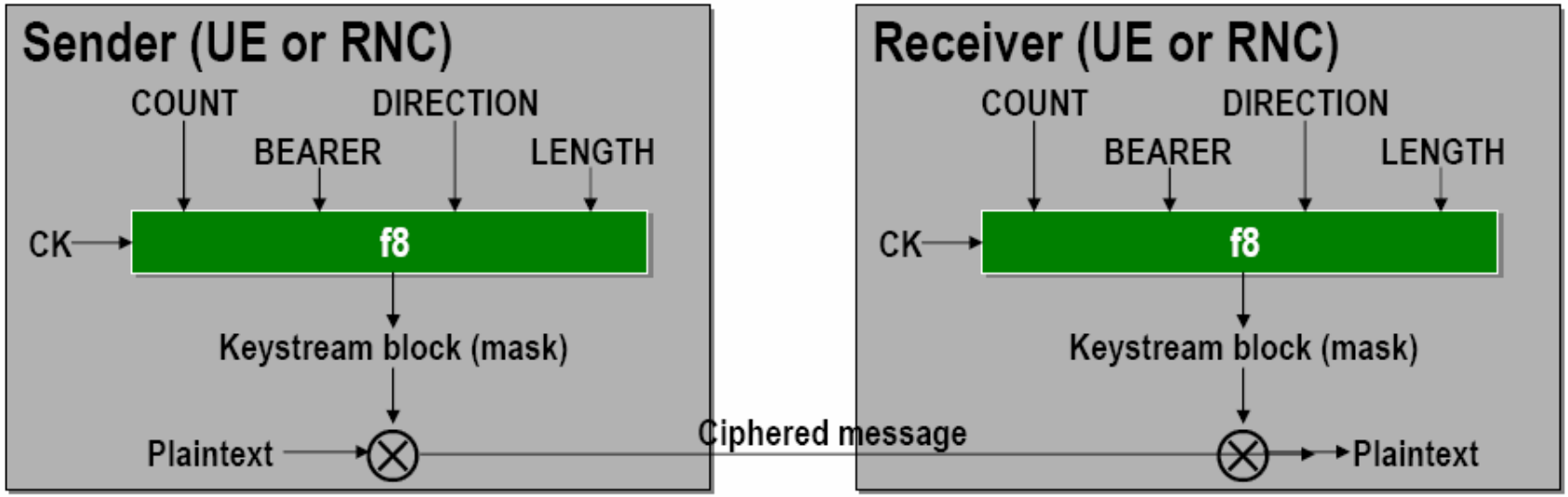
- The serving network sends a user authentication request to the terminal: RAND and AUTN are transferred into the USIM
- The USIM carries out a computation that is similar to the generation of authentication vectors in AuC
- The USIM is able to verify whether RAND and AUTN have been indeed generated in AuC and, in the positive case, the computed parameter RES is sent back to the VLR/SGSN
- The VLR/SGSN compares the user response RES with the expected response XRES - in the case of match, the authentication ends positively

User/Network Authentication - Details



- f5 has to be applied before f1 since f5 is used to cipher the SQN - this concealment prevents eavesdroppers from getting information about the user identify through the SQN
- If there is a match between MAC (generated at the AuC) and XMAC (generated at the UE), it implies that RAND and AUTN have been created by some entity that knows the master key K (i.e. the AuC of the user's home net)

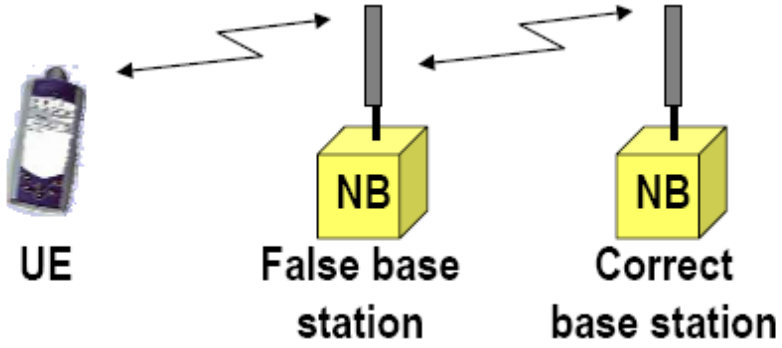
Ciphering (Encryption) of User Traffic in the UTRAN



- Ciphering / deciphering takes place in the terminal and the RNC for signaling and user data and is optional in UMTS (it may even not be allowed in some countries)
- Ciphering is done by adding plain text and the keystream block (mask) bit-by-bit
- Deciphering is done in the same way
- The keystream (mask) is generated for each frame separately and is based on
  - the cipher key, CK (128 bit)
  - the frame number, COUNT (32 bit)
  - the bearer identity, BEARER (5 bit)
  - the DIRECTION (1 bit)
  - the length of the keystream block, LENGTH (16 bits)

Integrity Protection of Signalling Traffic

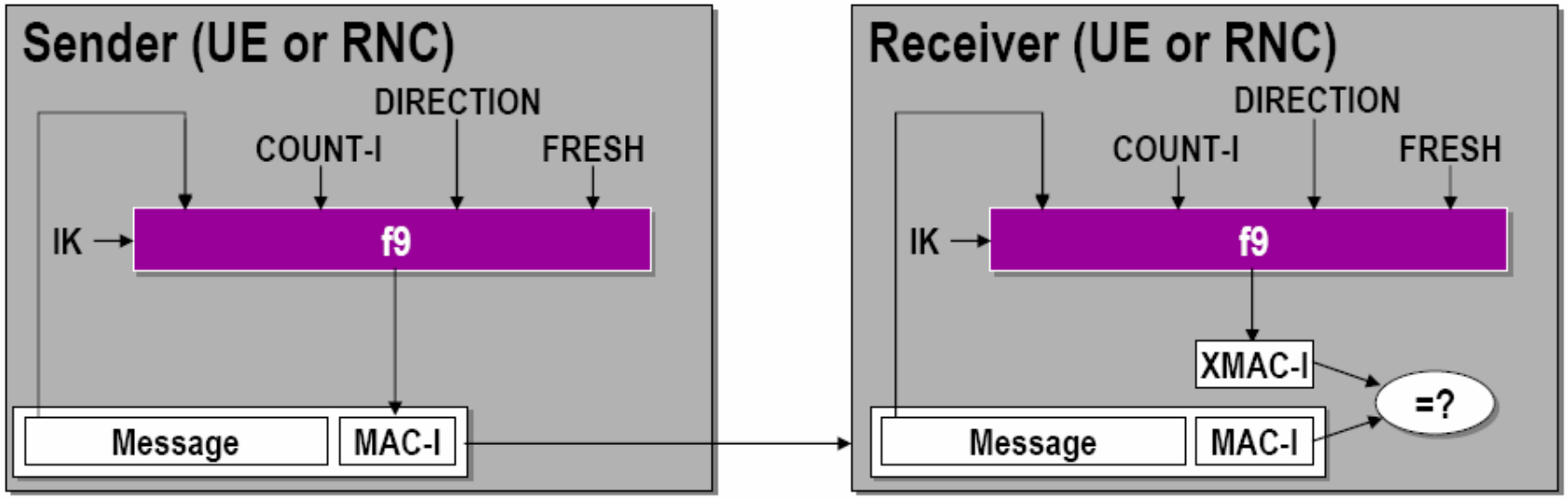
- Motivation of Integrity Protection of signalling messages
  - ciphering is optional in UMTS and may not be used in some cases (e.g. due to legal restrictions in some countries)
  - the authentication prodecure gives assurance to the identities of the communicating parties only at the time of the authentication
- Example
  - a false base station acts as a simple relay and delivers all messages in their correct from until the authentication procedure is completely executed
  - after that, the false base station may begin to manipulate messages
  - therefore signalling messages must be protected individually in order to observe deliberate manipulation of messages and discard false ones



Integrity Protection of Signalling Traffic

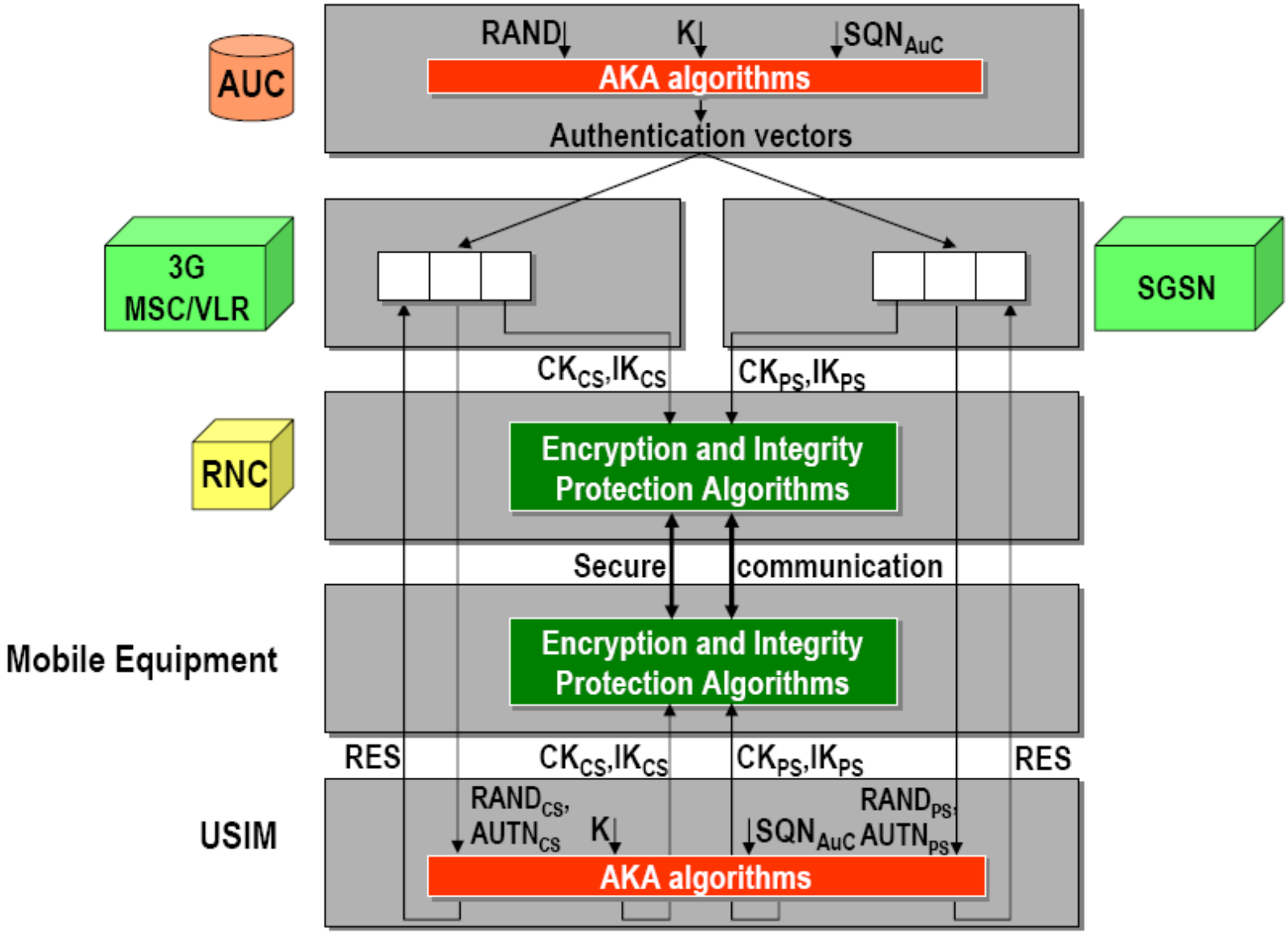
- Possible manipulations of signalling messages by intruders
  - deliberate manipulation
  - accidental modification
    (protected by error correction and detection)
  - insertion
  - replaying
  - deletion
- Integrity protection in UMTS guarantees that signaling data has not been altered or destroyed in an unauthorized manner

Integrity Protection of Signalling Traffic



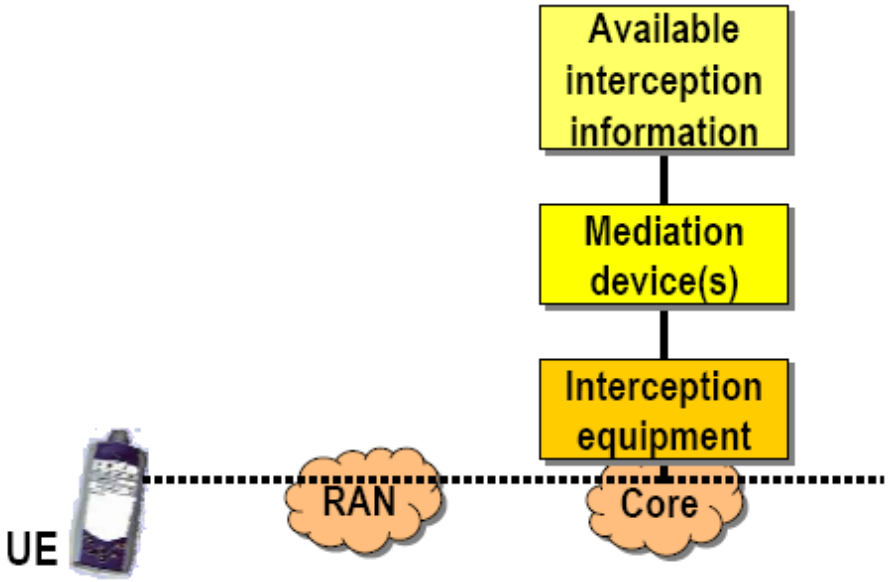
- f9 is an one-way function to calculate the Message Authentication Code for Integrity (MAC-I)
- IK may be used for several consecutive connections
- MAC-I (32 bit lenght) must not be calculated twice from the same COUNT-I/FRESH/IK triple in consecutive messages or connections (in order to avoid replay attacks)
- COUNT-I
  - counter for messages initialized in the UE and incremented for each message
  - protects user side from replay or deletion attacks
- FRESH
  - generated by the RNC for each connection and sent to the UE (whereupon COUNT-I is initialized)
  - provides replay and deletion protection for the network side

UMTS (Access Level) Security Concept - Summary



Lawful Interception - Overview

- Crucial goal in security is to encrypt information in such a way that it is available only for the correct receiver
- Exception: laws and local authorities in many countries set limits for encryption in order to have a way for access to sensitive information and subscriber observation
- Authorities must have a chance to listen to the calls or monitor data traffic (circuit and packet switched) → Lawful Interception
- Interception equipment collects items predetermined by local authorities
- Meditation devices provides filtering functions which show only the informations the local authorities define
- The filtered data is called Interception Information



Lawful Interception - Collected Interception Items (Extract)

Collected Item	Explanation
MSISDN	MSISDN of the monitored subscriber
IMSI	IMSI of the monitored subscriber
IMEI	IMEI of the monitored subscriber
Event type	Description which type of event is delivered: establishment, answer, supplementary service, handover, release, SMS, location update, …
Event date	Date of the event generation
Event time	Time of the event generation
Dialed number	Dialed number before digit modification
Connected number	Number of the answering party
Call direction	Information whether the monitored subscriber is calling or called
Local information	LAI that is present at the network at the time of event record production
Basic service	Information about tele or bearer service
Supplementary service	Supplementary service used by the monitored subscriber, e.g. call waiting, call forwarding, ..
Forwarded to number	Forwarded to number at call forwarding
Call release reason	Call release reason of the monitored call
SMS message	SMS content with header, including SMS-center address
PDP address	PDP address of the monitored subscriber (might be dynamic)
PDP type	The used PDP type, for instance IP or X 25
Access point name	GGSN of the other party
Routing area code	Routing area of the monitored subscriber

Cellular Mobile Networks - UMTS
UMTS QoS Framework

UMTS QoS Classes

- UMTS QoS is offered by the UMTS Bearer Service
- 4 QoS classes are defined:
  - conversational class (e.g. voice, video conferencing)
  - streaming class (e.g. video streaming)
  - interactive class (e.g. Web browsing, gaming)
  - background class (e.g. Background email download)
- These classes are characterized by e.g.:
  - guaranteed / maximum bitrate
  - maximum packet size
  - transfer delay
  - traffic handling priority

UMTS QoS Classes - Overview

Class	Traffic Class	Class Description	Example	Relevant QoS Requirements
1	Conversational	Preserves time relation between entities making up the stream conversational pattern based on human perception; real-time	Voice Video telephony Video gaming Video conferencing	Low jitter Low delay
2	Streaming	Preserves time relation between entities making up the stream; real-time	Multimedia Video on demand Webcast Real-time video	Low jitter
3	Interactive	Bounded response time Preserves the payload content	Web-browsing Database retrieval	Low round trip delay time Low BER
4	Background	Preserves the payload content	E-mail SMS File transfer	Low BER

UMTS QoS Classes - Details

Value ranges for UMTS Bearer Service Attributes from 23.107

Traffic class	Conversational class	Streaming class	Interactive class	Background class
Maximum bitrate (kbps)	< 2 048 (1) (2)	< 2 048 (1) (2)	< 2 048 - overhead (2) (3)	< 2 048 - overhead (2) (3)
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size (octets)	<=1 500 or 1 502 (4)	<=1 500 or 1 502 (4)	<=1 500 or 1 502 (4)	<=1 500 or 1 502 (4)
SDU format information	(5)	(5)		
Delivery of erroneous SDUs	Yes/No/- (6)	Yes/No/- (6)	Yes/No/- (6)	Yes/No/- (6)
Residual BER	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-6}	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)
SDU error ratio	10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Transfer delay (ms)	100 – maximum value	250 – maximum value		
Guaranteed bit rate (kbps)	< 2 048 (1) (2)	< 2 048 (1) (2)		
Traffic handling priority			1,2,3 (8)	
Allocation/Retention priority	1,2,3 (8)	1,2,3 (8)	1,2,3 (8)	1,2,3 (8)

SDU - Service Data Unit (packet)

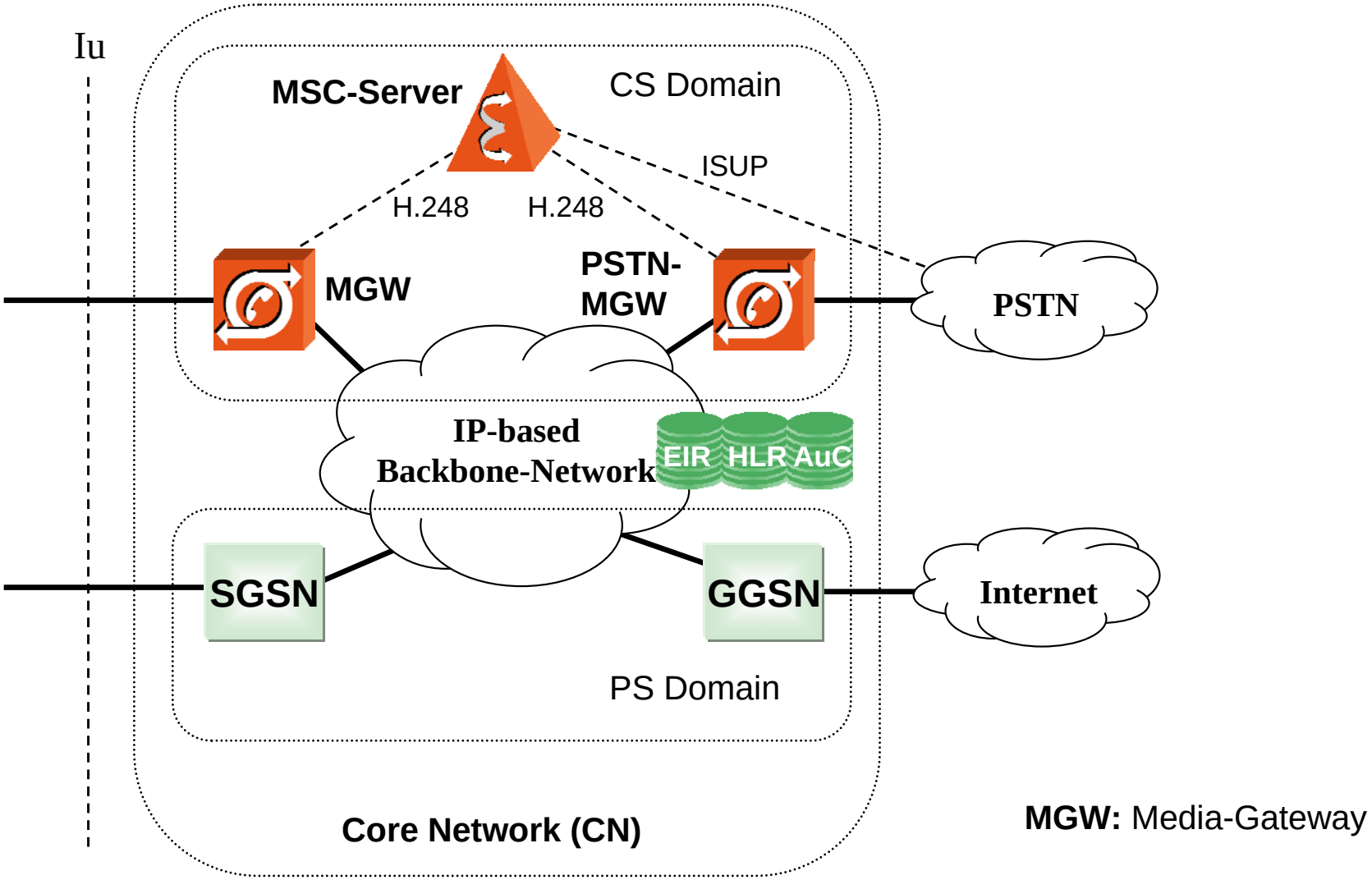
BER - Bit Error Rate

Cellular Mobile Networks - UMTS
UMTS Evolution

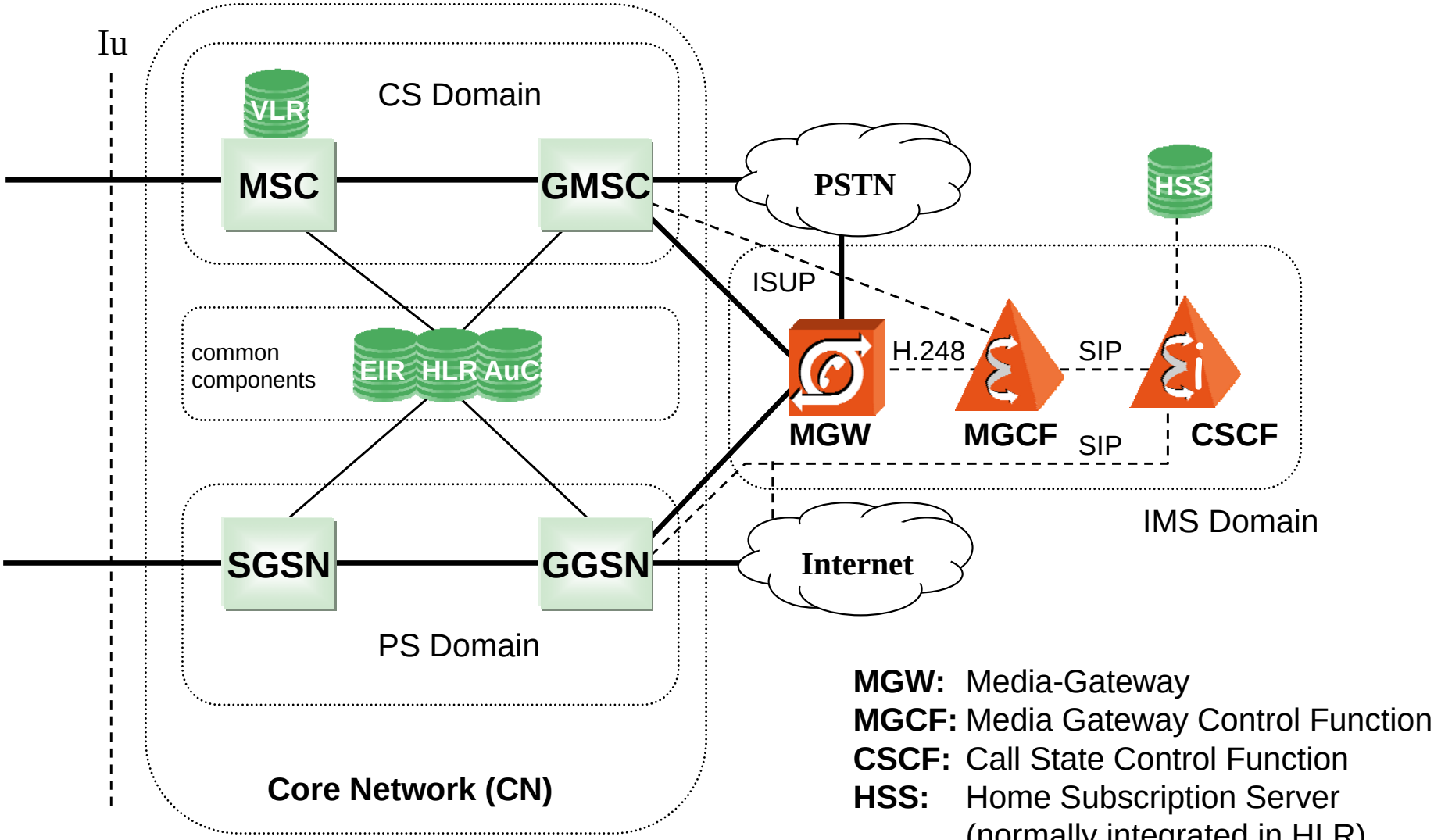
UMTS Development in Standardization

- Release 99 (R99) → Release 3 (R3)
  - foundation for the first UMTS systems
  - same Bearer, Tele and Supplementary Services like GSM
  - R3 Core Network based on GSM Phase 2+
  - new: UTRAN (W-CDMA, macrodiversity, different function split compared to GSM RAN)
- Release 4 (R4)
  - change in CS CN: separation of transport and control of CS connections, introduction of IP-based transport
  - transport of CS connections over IP (VoIP); RAN and CN are coupled via Media Gateways (MGWs); control of CS connections via MSC-Server (one MSC-Server typically controls several MGWs)
- Release 5 (R5)
  - Goal: elimination of the CS-Domain; VoIP in PS-Domain, controlled via IMS
  - Changes in RAN: IP transport; $I_{U\ flex}$ Interface; HSDPA
  - GSM/EDGE RAN (GERAN) is connected to UMTS CN via I_U Interface
- Release 6 (R6)
  - Goal: optimization of the UMTS architecture (WLAN-Interworking, MBMS, new services)

UMTS R4 - Separated Architecture in CS-Domain



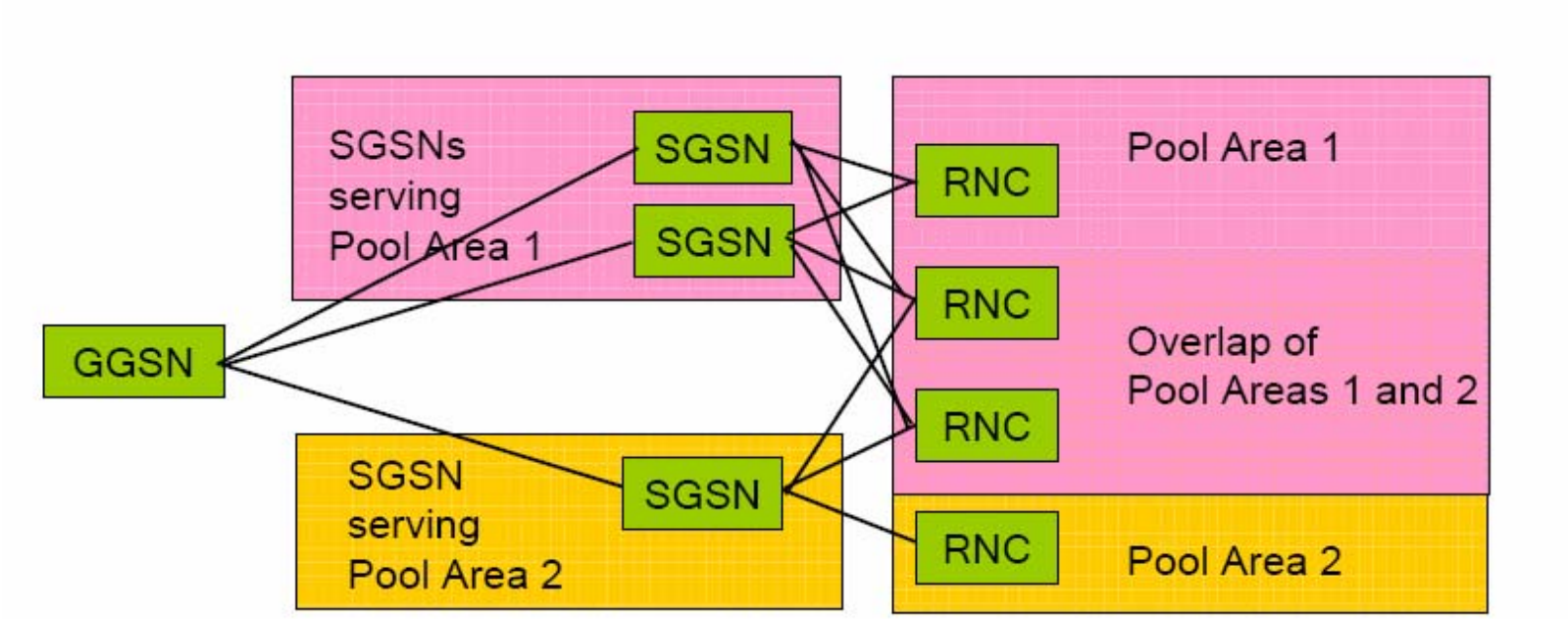
UMTS R5 - IP based Multimedia Subsystem (IMS)



MGW: Media-Gateway
MGCF: Media Gateway Control Function
CSCF: Call State Control Function
HSS: Home Subscription Server (normally integrated in HLR)

UMTS R5 - $I_{U\ flex}$ Interface

- $I_{U\ Flex}$ allows a many-to-many relation of RNCs and SGSNs (and MSCs)
  - RNCs and SGSNs are grouped as belonging to „Pool Areas“
  - a Pool Area is served by one or more SGNSs in parallel
  - all the cells controlled by a RNC belong to the same one (or more) Pool Area(s)
  - UE may roam in an Pool Area without the need to change the serving SGSN



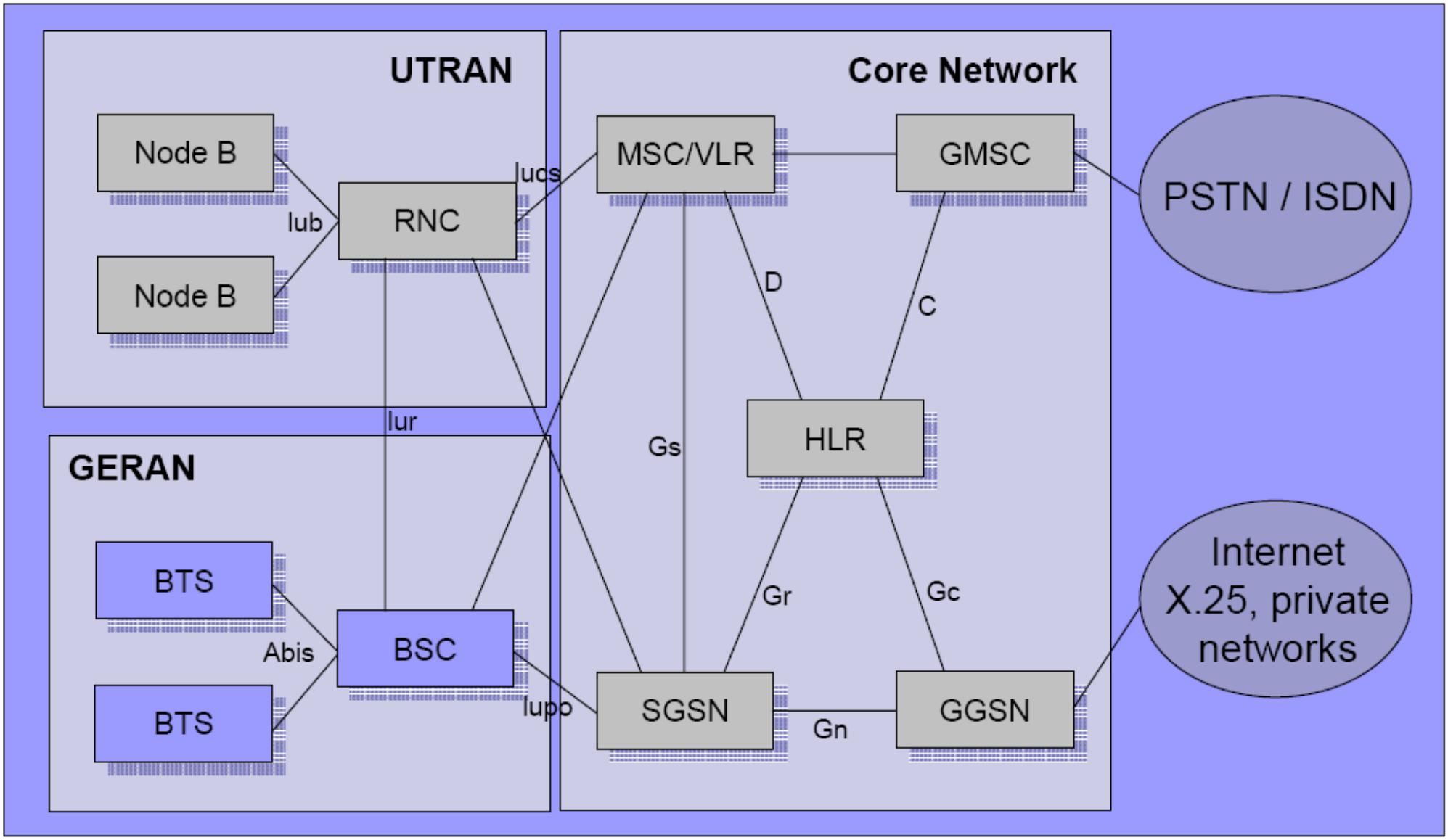
UMTS R5 - HSDPA

- HDSPA Features
  - new shared downlink channel: HS-DSCH (High-Speed Downlink Channel)
    - associated with up- and downlink feedback / control channels
    - can be allocated to a single PDP context or to multiple PDP contexts of several subscribers
  - HSPA can accommodate peak bitrates up to 16 Mbit/s and sustained bitrates of 1-5 Mbit/s (depending on cell size)
- Technical Realisation of HSPA
  - 16 QAM modulation used in addition to QPSK
    - codes 4 bits per phase / amplitude shift
  - Node B based scheduling
    - reduces delay
  - Node B based adaption of code rate and modulation
    - code rate and modulation scheme is adapted depending on the currently necessary throughput
  - Hybrid-ARQ
    - information is encoded redundantly in each transmission; retransmission doesn't resend the complete information, but only some more redundancy, complementing the redundant data that has already been sent (Hybrid ARQ)
  - Turbo Codes
    - powerful error correcting / encoding scheme suited for low S/N-ratios

UMTS R5 - GERAN

- GERAN (GSM/EDGE Radio Access Network):
  - harmonisation of the GSM/GPRS/EDGE PS services with UMTS
  - new I_U Interfaces defined at GSM BSC towards UMTS: $I_{U\,CS}$ und $I_{U\,PO}$
  - all UMTS QoS classes are also supported by GERAN
  - backward compatibility to GSM/GPRS architecture: in this case only the QoS classes 3 and 4 are supported for PS services

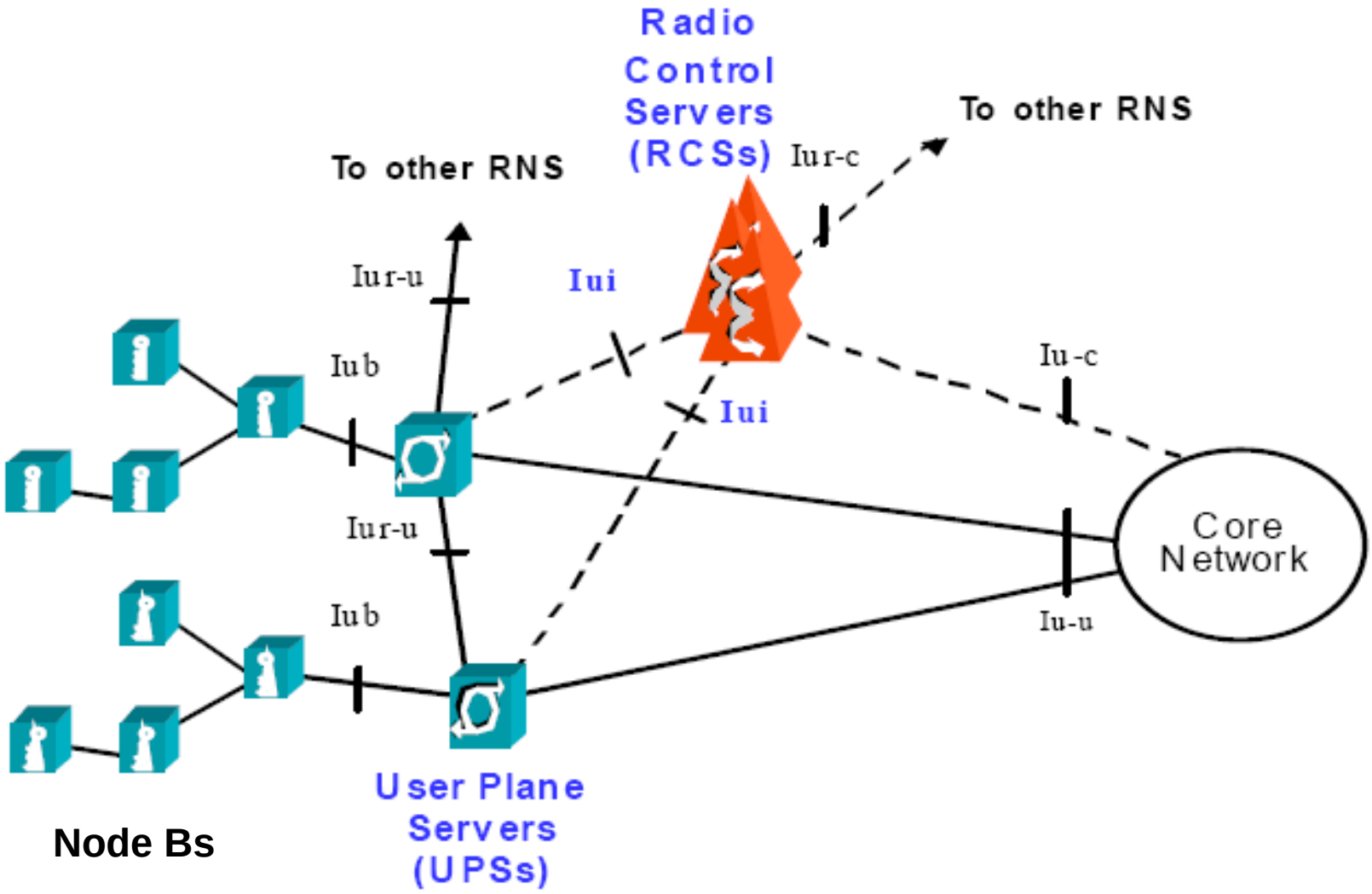
UMTS R5 - GERAN



UMTS R6 - Goals and Requirements

- UMTS R6 Goals and Requirements:
  - IP-based transport
  - new function split in RAN network elements (Node B, RNC)
  - performance improvements
  - scalability
  - backward compatibility to existing architectures
  - open, standardized Interfaces
  - no changes at the U_U Interface
  - maximum reuse of existing protocols
  - separate optimization of Control and User Plane

UMTS R6 - Separated RAN Architecture



UMTS R6 - Interworking to non-3GPP Access (e.g. WLAN)

- 6 Interworking Scenarios are defined:
  - Scenario 1:
    - common billing and customer care (e.g. receive only one bill)
  - Scenario 2:
    - common access control (authentication and authorisation) using a (U)SIM-based solution and charging
  - Scenario 3:
    - access to all 3GPP packet-switched services (e.g. IMS, Push etc.) and services like SMS or MMS
  - Scenario 4:
    - service continuity between different accesses like WLAN and UTRAN (i.e. service must not be set up again, if access technology is changed)
  - Scenario 5:
    - seamless mobility between WLAN and 3GPP access networks
  - Scenario 6:
    - seamless handover even for CS services
- In UMTS R6 presumably only scenarios 1-3 will be supported

UMTS R6 - New Services: Push Service, Push-to-Talk

- Push Service
  - pushing of information from network to UE
  - technical realization support via
    - SMS service: push information using SMS
    - network-initiated PDP context activation (TS 23.060 must be changed; need mapping of „user ID“ onto IMSI)
    - IMS / SIP (query CSCF to find users IP address and contact user with SIP INVITE message)
- Push-To-Talk (PTT)
  - multicast of speech to predetermined list of parties („CB Funk“)
  - Half Duplex operation: only one person can speak at a time
    - whoever pushes the button first
  - no dialing necessary, just „push“
    - uses „always-on“ functionality
  - already possible with GPRS (in 2004)
  - with IMS support PTT is presumably more efficient
    - relying on other IMS services, e.g. group management, multiparty conferencing

UMTS R6 - New Services: IMS Feature Extensions

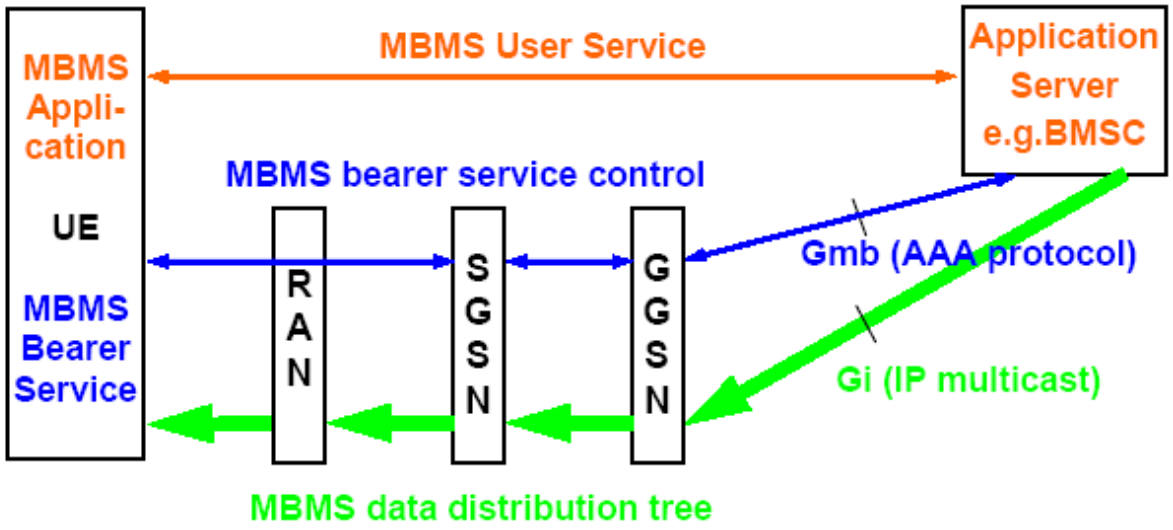
- IMS Group Management
  - setting up and maintaining user groups
  - supporting service (enabling service) for other services e.g. for multiparty conferencing or Push-To-Talk
- IMS Presence Service
  - user defined visibility to others
  - user can find out presence of others
- IMS Messaging
  - SIP-based messaging
  - Instant Messaging, „Chat Room“, Deferred Messaging (equivalent to MMS)
  - interworks with Presence Service to determine if addressee is available
- Multiparty-multimedia conferencing service in IMS
  - utilizes the IMS MRF
- Location-based services in IMS
  - UE may indicate that it wishes to use local service; S-CSCF then routes the request back to the visited network
  - mechanism for UE to retrieve / receive information about locally available services

UMTS R6 - New Services: MBMS (1)

- MBMS = Multimedia Broadcast and Multicast Service
- MBMS enables a resource and cost efficient data transfer to many users in parallel
- MBMS applications:
  - multicast of e.g. sport events
  - broadcast of emergency informations
  - download of software (games)
  - multiparty conferencing
  - Push-To-Talk
- two reception modes:
  - „streaming type reception“: present data as it is received
  - „download type reception“: store data and replay later

UMTS R6 - New Services: MBMS (2)

- Technical Realization
  - multicast / broadcast data is send via the G_i Interface
    - the application server may be realized by a MBCS (Broadcast Multicast Service Center) or e.g. by the MRF
  - control data is send via the G_{mb} interface
    - for authorisation, for sending encryption keys, …
    - for network resource configuration
  - in multicast mode, data is transmitted only to cells with UEs that joined the MBMS service



4th Generation Mobile Networks - Challenges (1)

- Lower cost/bit (than 3G)
- Bandwidth on the air interface > 2 Mbit/s („translate desktop experience to mobile world“)
- „All-IP“
- Transparent, seamless integration of heterogeneous access technologies
  - any fixed access and RAN technology (UTRAN, WLAN, Bluetooth,..) - integrated by means of the IP-layer
  - IP-based core network
- Reconfigurable multi-mode multiband terminals
  - terminals can be adapted to local RAN technology by downloading appropriate software (SDR – Software Defined Radio)
- Smooth evolution path from 3G / integration of 3G

4th Generation Mobile Networks - Challenges (2)

- Empowerment of user to act as service provider
  - movement away from a provider-centric paradigm towards a decentralized peer-to-peer paradigm
  - intelligence moves towards the center of the network
- „Ambient Intelligence“
  - multitude of embedded, networked devices in the environment („ubiquitous computing“)
    - sensors, controls, „natural“ user interfaces
  - these devices interact with the person and personalize the surroundings
    - learning and adaptation to the environment
    - location-aware, context-aware, person-aware
  - this raises interesting security issues
    - what information is spread and stored where
    - user needs to stay in control („off-button“ must exist)

4th Generation Mobile Networks - Challenges (3)

- Integration of a multitude of interacting devices
  - moving networks
    - a network moves as a whole, thereby changing its point of attachment, e.g. passengers using train networks as access network
  - Ad-hoc networks
    - wireless devices communicating without infrastructure
    - all nodes can act as routers, e.g.
      - PANs (Personal Area Networks)
      - BANs (Body Area Networks)
      - WSNs (Wireless Sensor Networks)
      - Vehicular networks
- Ad-hoc autoconfiguring networks
  - ad-hoc network formation for specific, possibly short-lived tasks with involving variable network elements and devices
  - interwoven networks
    - devices may belong to several (logical) networks at once e.g. a laptop belongs to a PAN and also to a moving network