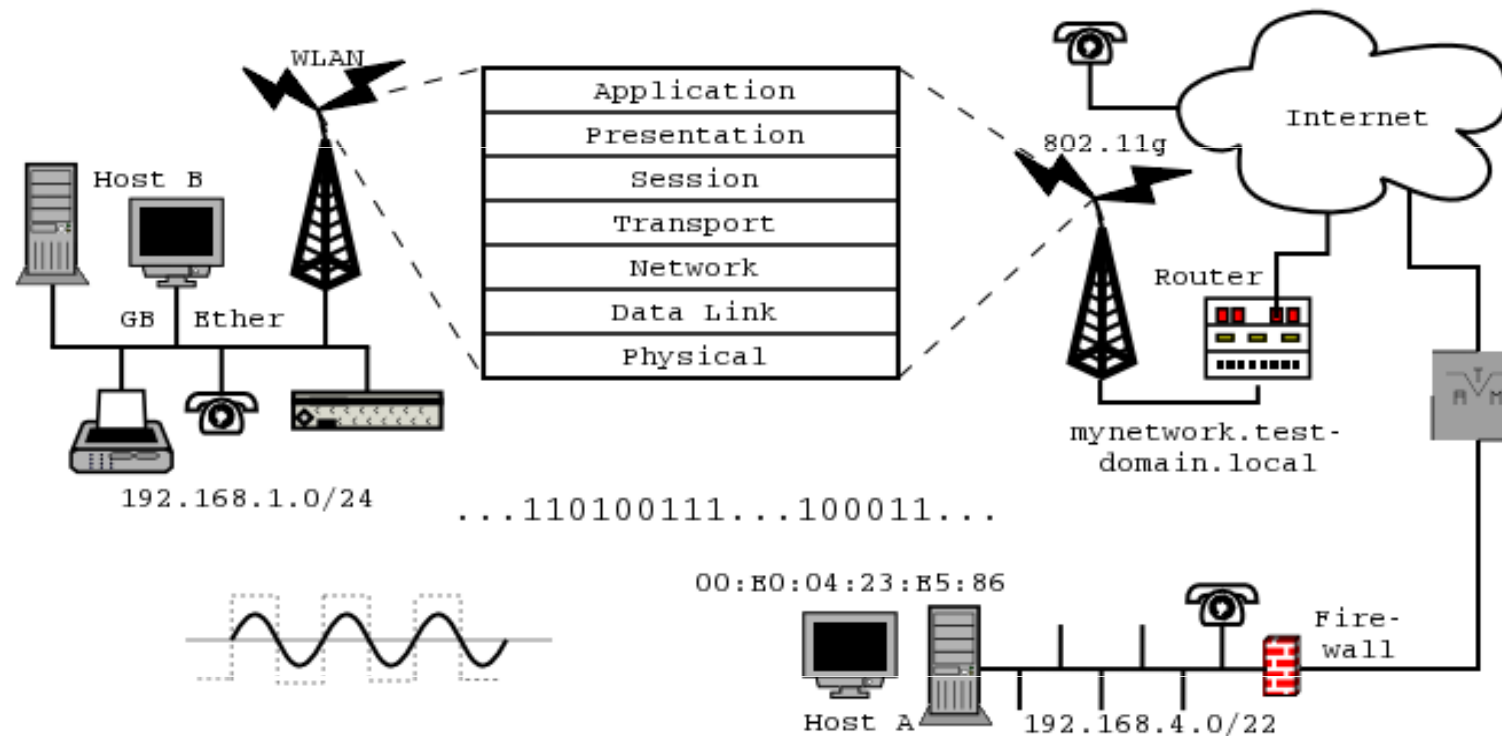


# Communication Systems

## 12<sup>th</sup> lecture

... <http://www.ks.uni-freiburg.de/inetnetwork> ....



Chair of Communication Systems  
Department of Applied Sciences  
University of Freiburg  
2006

# Communication Systems

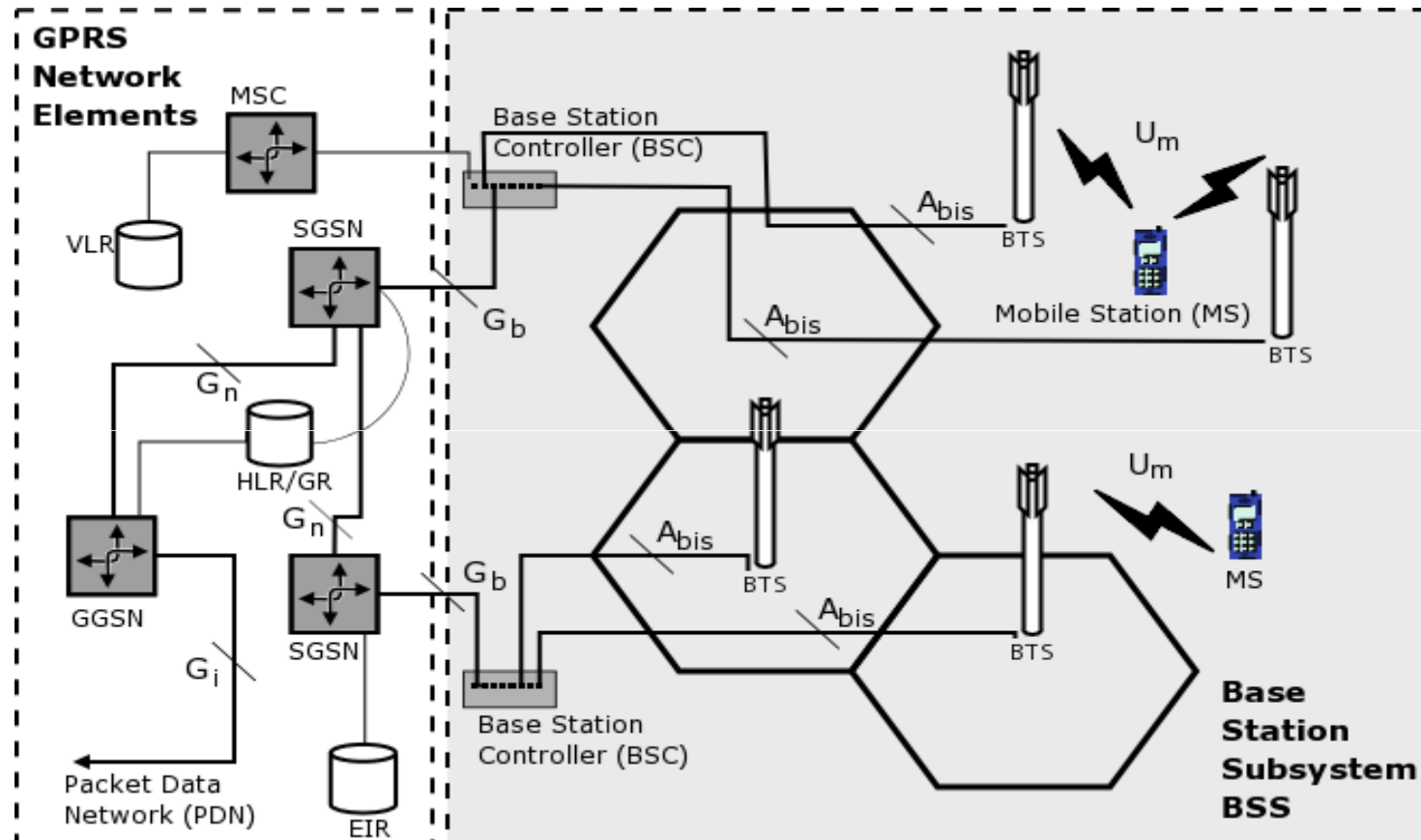
## *Last lecture – GSM data services, GPRS*

- Standardization of GPRS was important cornerstone for the development of UMTS network
  - GPRS defines an add-on for data services within the GSM networks - packet orientated approach to data switching
  - Allocation of channels request-driven
  - Today's bandwidth of 53,6 kbit/s (4 full rate traffic channels à 13,4 kbit/s), up to 107,2 kbit/s with 8 channels
  - GPRS usually operates asynchronous with more bandwidth for down than for upstream
- GPRS bases on an additional infrastructure: GSN – GPRS Support Nodes as an extension to GSM
  - SGSN (Serving GSN), GGSN (Gateway GSN)

# Communication Systems

## Last lecture – GSM data services, GPRS

- Main GSM components, like MSC, VLR and HLR used for GPRS too, additional infrastructure: GSN – GPRS Support Nodes



# ***Communication Systems***

## ***Last lecture – GSM, logical structure of the network***

- SGSN – serving GSN to support the MSC for localization, billing and security
- GGSN – gateway GSN is the gateway to the packet data network – usually the Internet
- GR – GPRS register to support the HLR (home location register), used for user address mapping
- Several new interface definition between network components

# ***Communication Systems***

## ***Plan for this lecture***

- UMTS as the world wide 3G mobile standard
  - Short history of developments, today's and future revisions
  - Network architecture and interfaces
  - User equipment and USIM
  - Core network functionality and protocols (packet switched and circuit switched domain)
  - UTRAN – UTM's radio network subsystem
    - RNS, RNC, Node B
  - Network based and connection based functions
  - Power control and hand-over
  - Authentication and security

# ***Communication Systems***

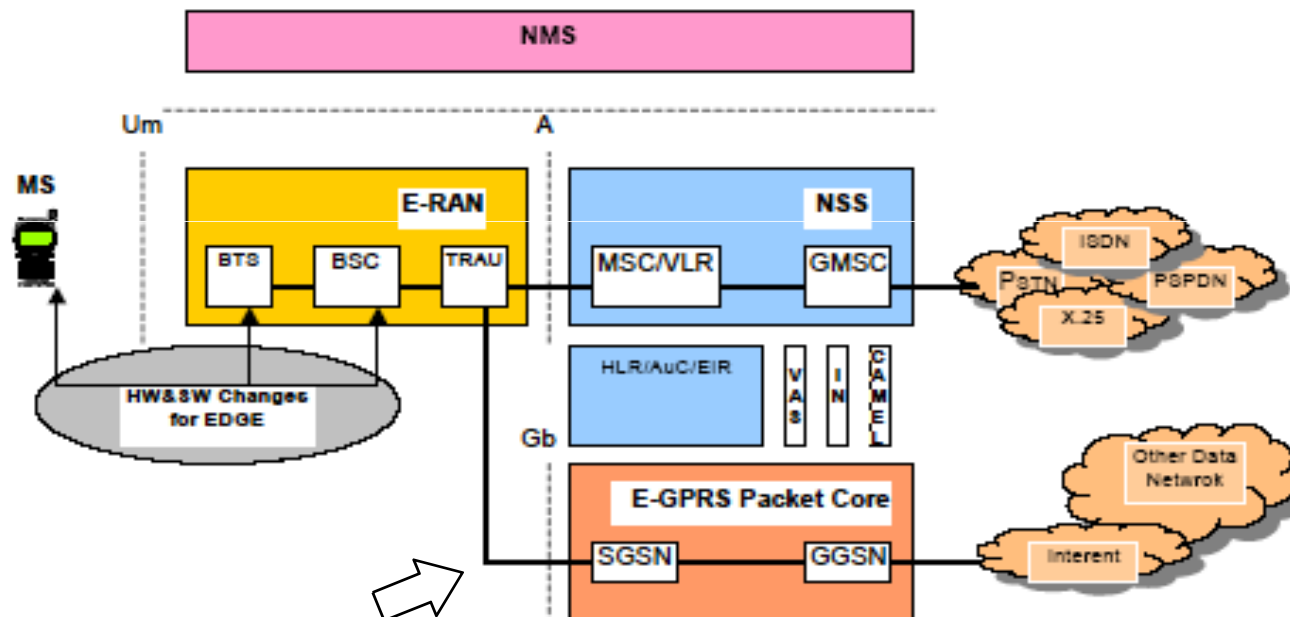
## ***UMTS – history and planned standards***

- Requirements toward a 3G standard
  - Fully specified and world-widely valid
  - Major interfaces should be standardized and open
- Services must be independent from radio access technology and is not limited by the network infrastructure
- Support of multimedia and all of its components
- Convergence of existing networks

# Communication Systems

## UMTS – history and planned standards

- Definition of GPRS (specific GPRS network elements are reused in 3G specification)
  - Reuse of operation and management components of GSM
  - Reuse of packetized data services infrastructure of GPRS



# *Communication Systems*

## *UMTS – history and planned standards*

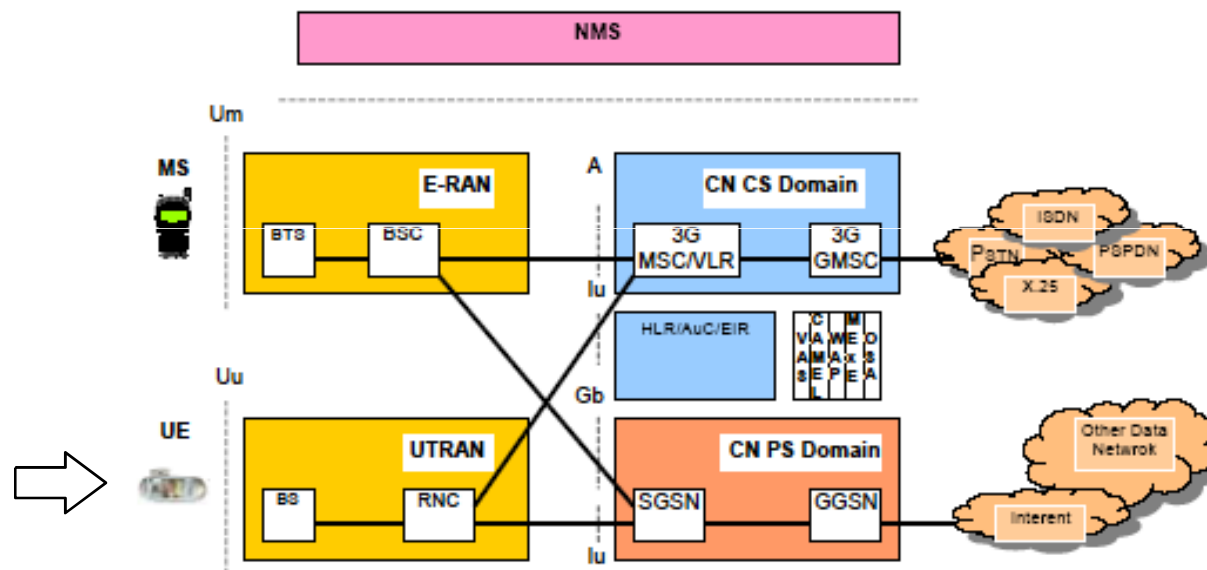
- February 1995 **UMTS Task Force** established; "The Road to UMTS" report
- December 1996 The **UMTS Forum** established. "European" WCDMA standard known as Universal Mobile Telecommunications System (UMTS)
- June 1997 UMTS Forum produces **first report**: "A regulatory Framework for UMTS"
- October 1997 ERC decided on UMTS **core band**.
- January 1998 ETSI meeting: **W-CDMA and TD-CDMA** proposals **combined** to UMTS air interface specification



# Communication Systems

## UMTS – history and planned standards

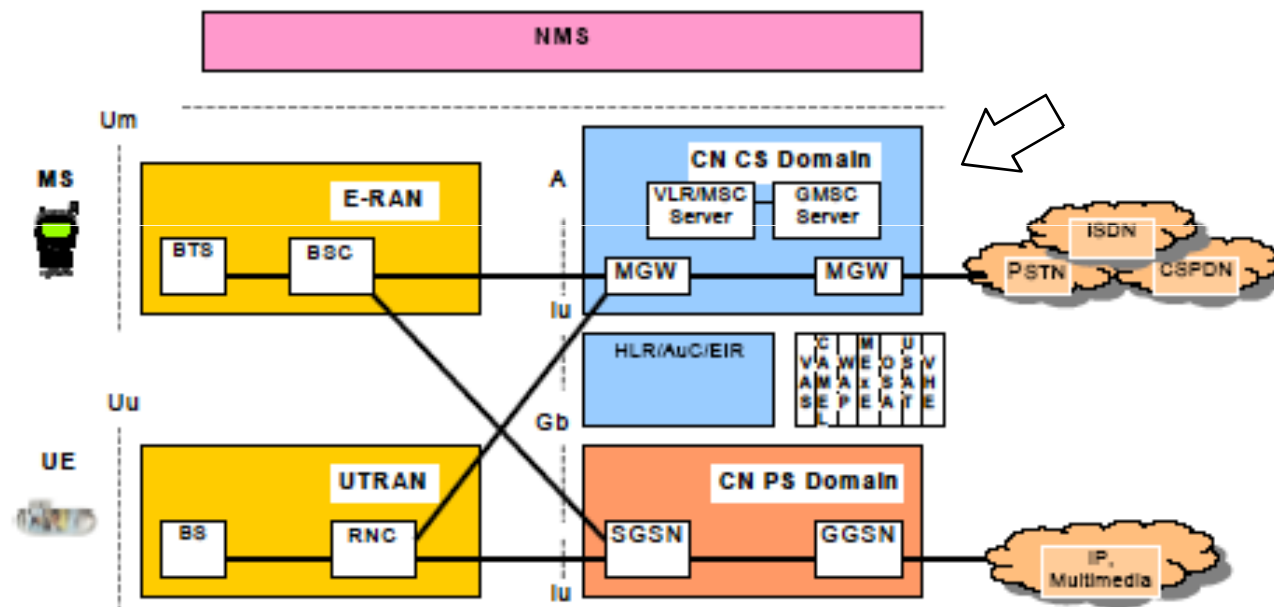
- June 1998 Terrestrial **air interface proposals** (UTRAN, WCDMA(s), CDMA2000(s), EDGE, EP-DECT, TD-SCDMA) were handed into ITU-R
- 3GPP Release '99



# Communication Systems

## UMTS – history and planned standards

- December 1999 in Nice ETSI Standardisation finished for UMTS Release 1999 specifications both for FDD and TDD
- March 2001 in Palm Springs 3GPP approves UMTS Release 4 specification





# ***Communication Systems***

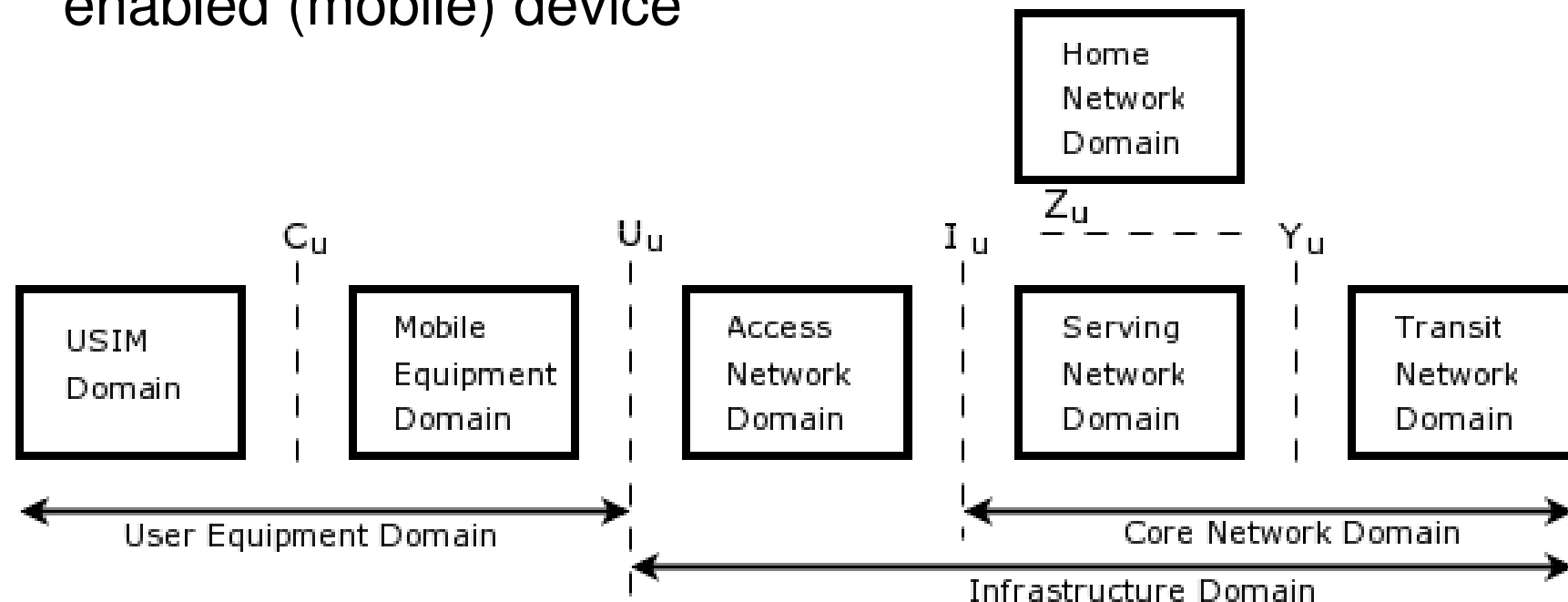
## ***UMTS – history and planned standards***

- Release 6
  - Extended location based services (LBS), with built in anonymization
  - Packet switches streaming services, with adaptation to available network resources (GERAN/GPRS, UMTS, WLAN)
  - Of course :-) DRM
  - Charging Management Framework (for extended payment systems)
  - For more see [www.3gpp.org](http://www.3gpp.org)

# Communication Systems

## UMTS network architecture and interfaces

- UMTS network architecture has several similarities to GSM, but you will find different names for some components
- As for GSM in UMTS several interfaces are defined
- UE – user equipment means more generally any UMTS enabled (mobile) device



# ***Communication Systems***

## ***UMTS network domains***

- User Equipment Domain handles the access of the user onto the UMTS services
- USIM – User Services Identity Module
  - Extended SIM functionality
  - Functions for user identification, authentication and encryption
  - Integrated into SIM card (of the established format)
  - Most recent Mobile Equipment can handle both SIM and USIM
- Mobile Equipment Domain responsible for air interface
  - User interface for end-to-end connections

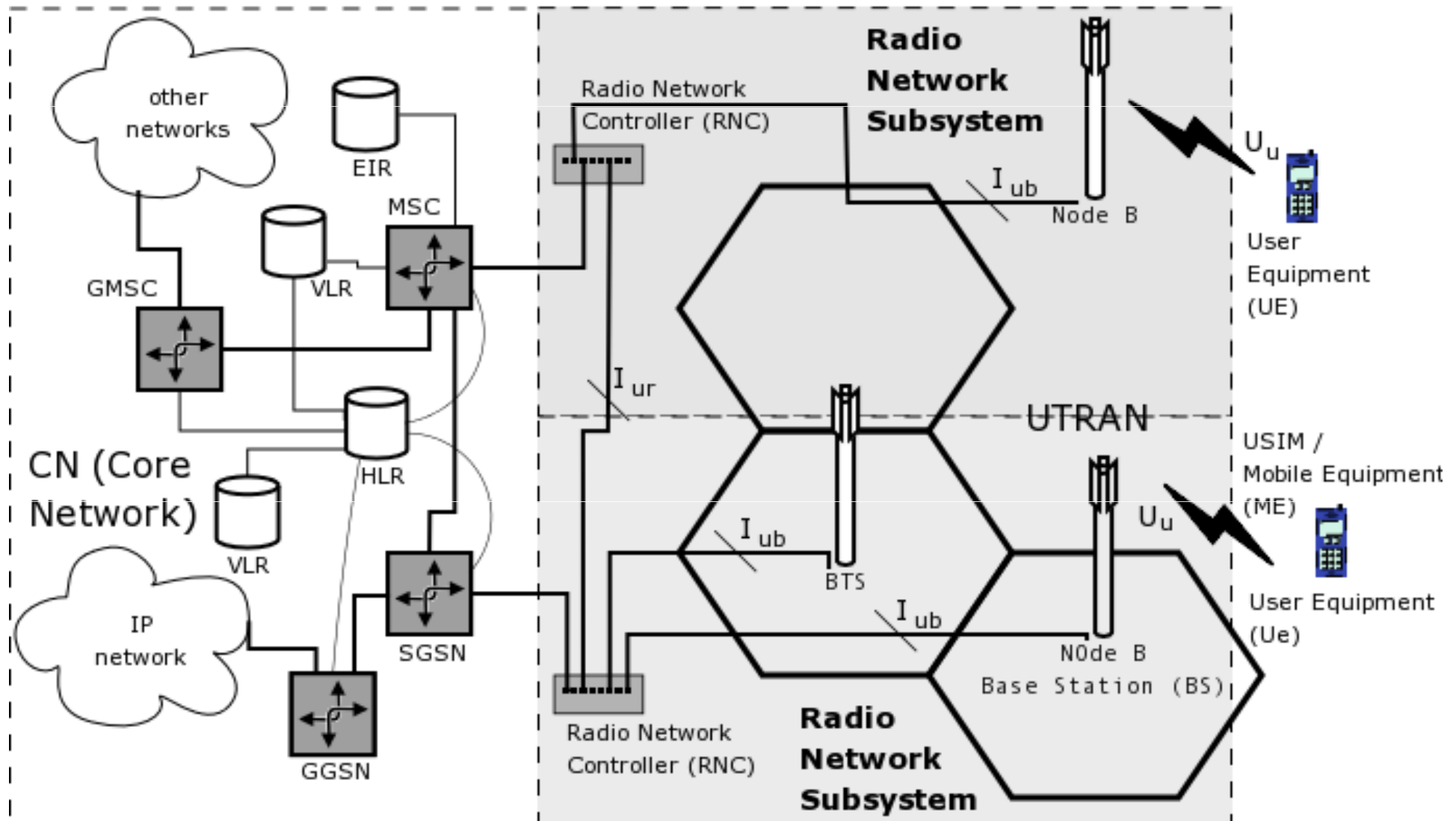
# ***Communication Systems***

## ***UMTS network domains - CN***

- Infrastructure Domain
  - Shared between all users
  - Offers services to all authenticated users
- CN – Core Network the (mobile) telephony backend infrastructure
  - Functions which are independent on access network
  - Handover between different systems
  - Location management if there is no dedicated link between UE and UTRAN
  - Inter-connection of different bearer networks

# Communication Systems

## UMTS network architecture – Core Network, UTRAN, UE





# ***Communication Systems***

## ***UMTS network domains - CN***

- CN infrastructure consists of
  - Serving network domain – network which actually provides the user access
  - Home network domain – functionality and information which is independent of actual user location
  - Transit network domain – infrastructure between several network components, different kind of networks and different network providers, operators

# ***Communication Systems***

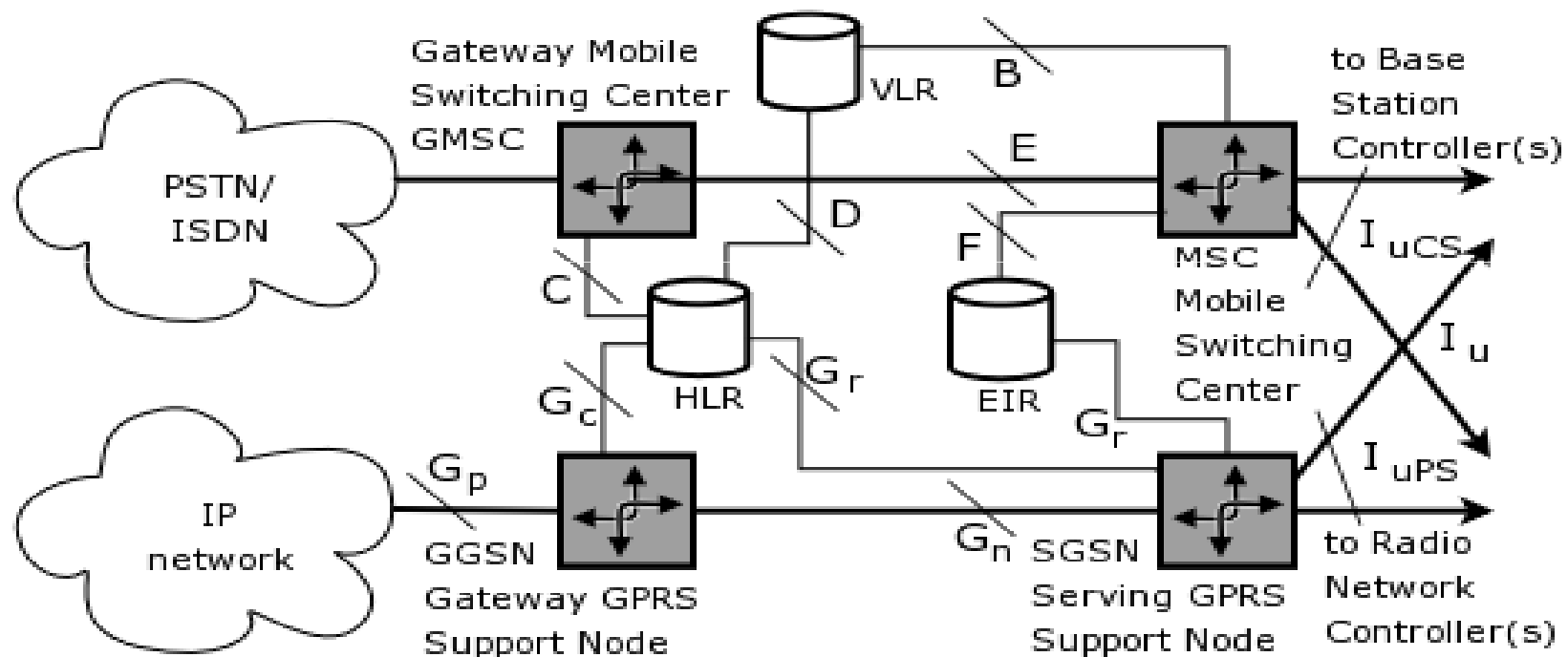
## ***UMTS network domains - CN***

- CN infrastructure split into two logical networks
  - Both may serve the two different radio networks via either BSC and RNS
  - Circuit switched domain (CSD)
    - IuCS interface
    - Traditional circuit switched data connection and signaling
    - Resource reservation on connection setup
    - GSM components (MSC, GMSC, HLR, VLR, EIR, ...)

# Communication Systems

## UMTS network domains - CN

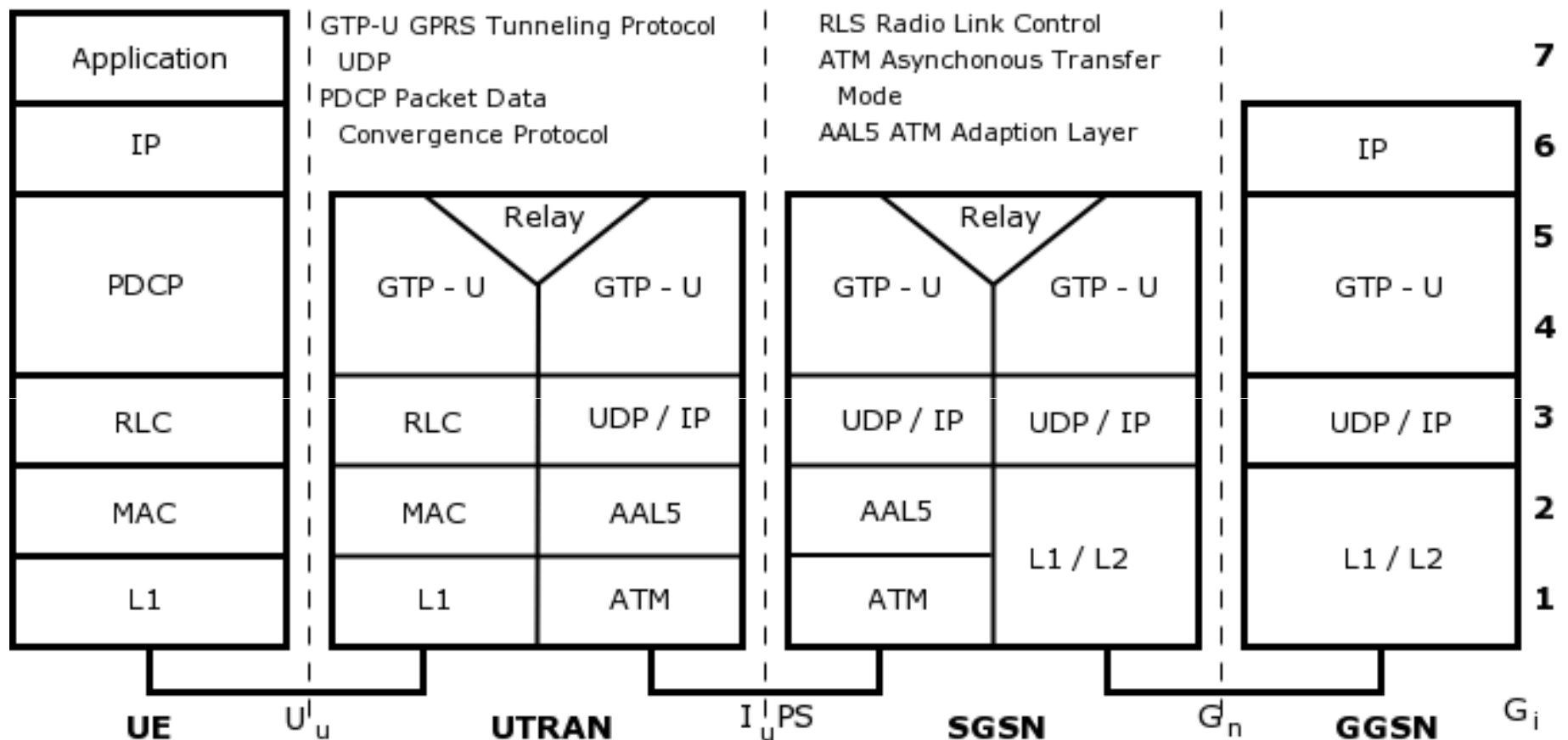
- Packet switched domain (PSD)
  - IuPS interface
  - Packet orientated services
  - GPRS components (SGSN, GGSN)



# Communication Systems

## UMTS network – packet switching domain

- The UMTS packet switching domain protocol stack follows the GPRS design



# ***Communication Systems***

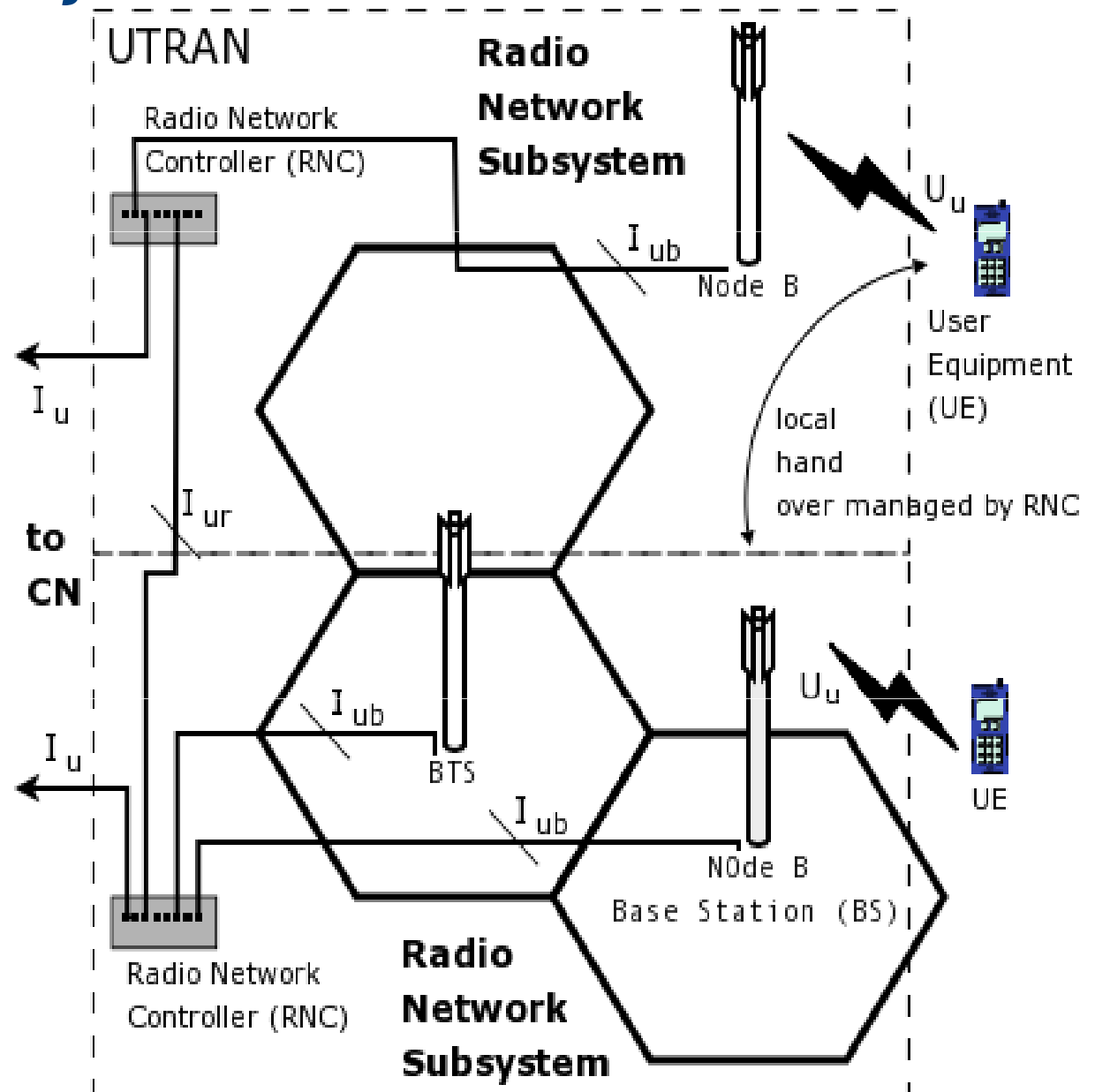
## ***UMTS network - UTRAN***

- UTRAN (UTRA network) is the UMTS transceiver radio interface network part
  - Manages mobility on cell level – handover decision
  - Composed of several Radio Network Subsystems (RNS) connected to the Core Network through the Iu interface
- Every Radio Network Subsystem is managed by Radio Network Controller (RNC)
  - RNC also handles radio resource management (RRM) operations
- RNC is responsible for the local handover process and the combining/multicasting functions related to macro diversity between different Node-Bs (Drift RNC - DRNC)

# Communication Systems

## UTRAN - RNS

- RNSs can be directly interconnected through the Iur interface (interconnection of the RNCs)
- Node B may contain a single BTS or more than one (typically 3) controlled by a site controller



# ***Communication Systems***

## ***UMTS network - UTRAN***

- UTRAN functions
  - Controls cell capacity and interference in order to provide an optimal utilization of the wireless interface resources
  - Includes Algorithms for Power Control, Handover, Packet Scheduling, Call Admission Control and Load Control
  - Encryption of the radio channel
  - Congestion control to handle situations of network overload
  - System information broadcasting
  - Micro and macro diversity (explained later)

# *Communication Systems*

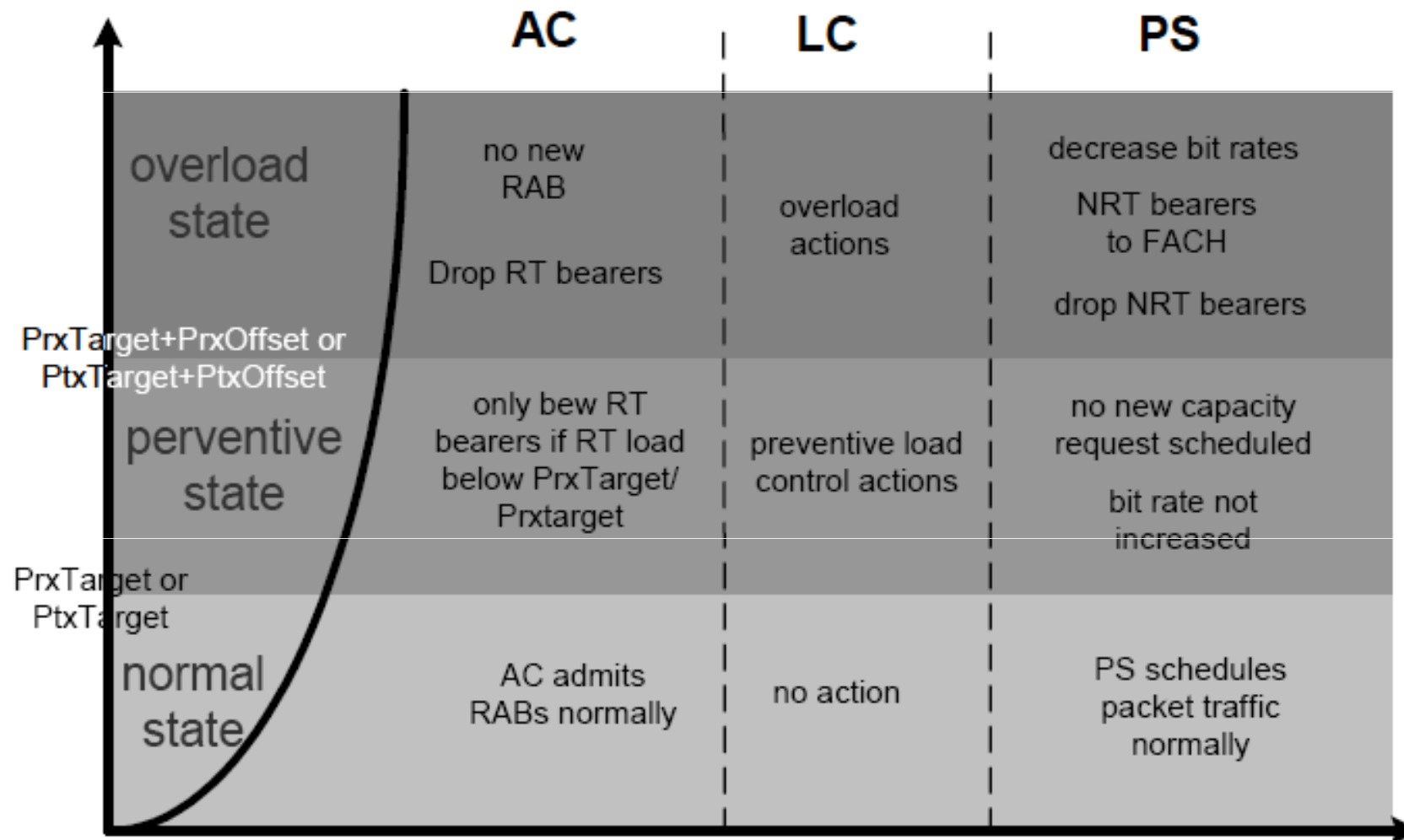
## *UMTS network - UTRAN*

- Network based functions
  - Packet Scheduling
    - Controls the UMTS packet access
    - Handles all non real time traffic, (packet data users)
    - Decides when a packet transmission is initiated and the bit rate to be used
  - Load Control
    - Ensures system stability and that the network does not enter an overload state
  - Admission control to avoid network overload
    - Decides whether or not a call is allowed to generate traffic in the network



# Communication Systems

## UTRAN network function – Load Control



# *Communication Systems*

## *UMTS network - UTRAN*

- Connection based functions
  - Power Control
    - Manages radio link quality - Uplink is handled per mobile (UE), downlink per physical channel
    - Ensures that transmission powers are kept at a minimum level and that there is adequate signal quality and level at the receiving end
  - Handover
    - guarantees user mobility in a mobile communications network
    - SRNS (Serving RNS) relocation

# ***Communication Systems***

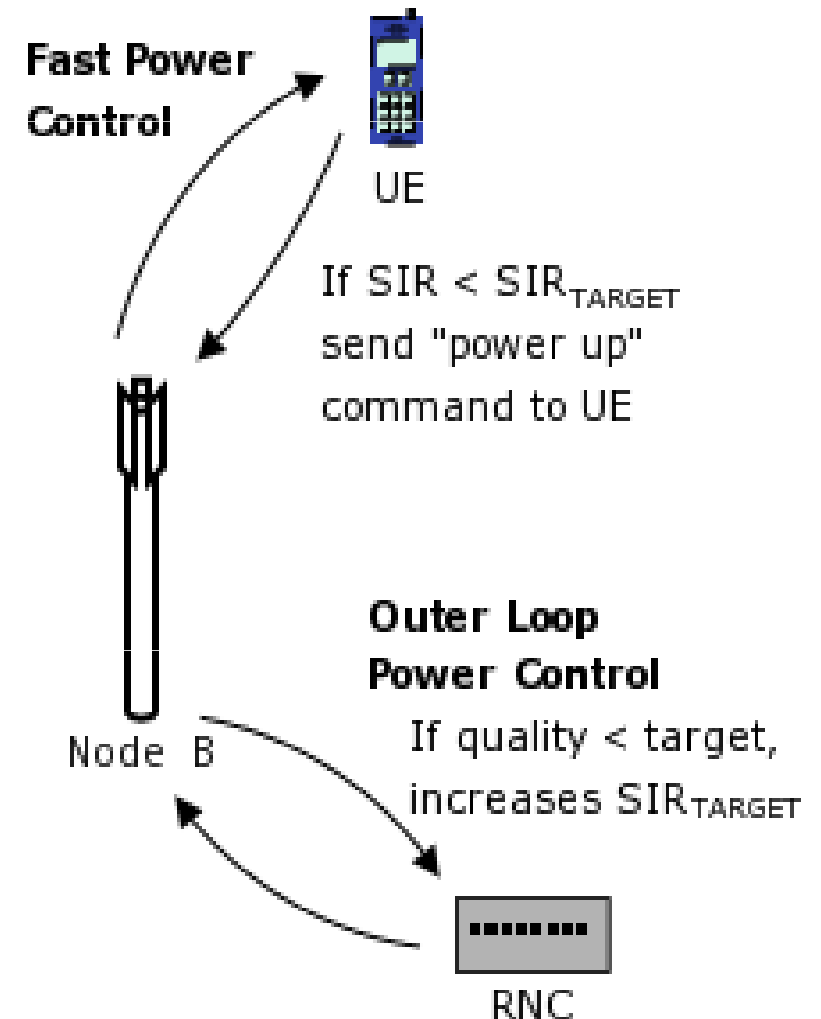
## ***UTRAN - connection based functions***

- Power Control handles
  - Setting of transmit power to keep QoS in required limits (regarding data rate, delay, BER, ...)
  - Path loss (near-far problem), shadowing (log-normal fading)
  - Fast fading (Rayleigh-, Rician-Fading)
  - Environment (delay spread, UE speed) which implies different performance of the de-interleaver and decoder
- Three types: Inner loop, outer loop (SIR-target adjusting), open loop (power allocation)
- Open-Loop Power Control
  - Rough estimation of path loss from receiving signal
  - Initial power setting, or when no feedback channel exist

# Communication Systems

## UTRAN - connection based functions

- Closed-Loop Power Control
  - Feedback loop with 1.5kHz cycle to adjust uplink / downlink power to its minimum
  - Even faster than the speed of Rayleigh fading for moderate mobile speeds
- Outer Loop Power Control
  - Adjust the target SIR (Signal to Interference Ratio) setpoint in base station according to the target BER, commanded by RNC



# ***Communication Systems***

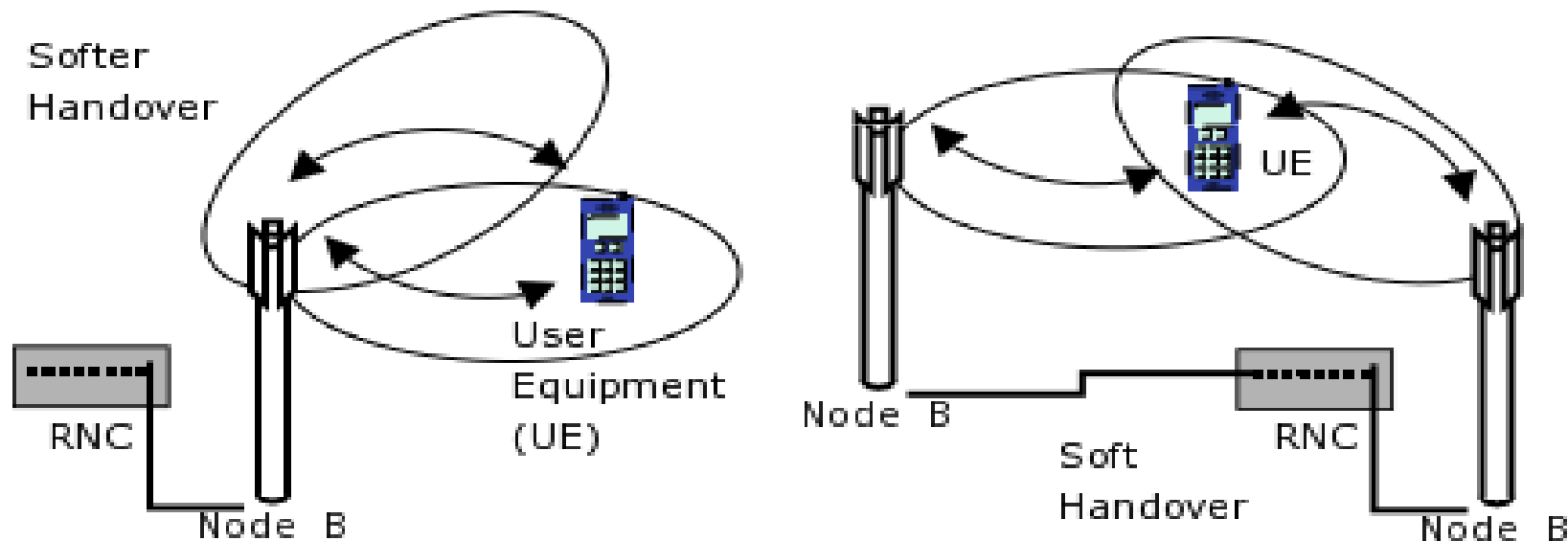
## ***UTRAN - connection based functions***

- UMTS provides several handover procedures
  - Intra Node B handover (softer)
  - Inter Node B handover, inter-frequency, intra-frequency (hard and soft)
  - Inter RNC (hard, soft and soft-softer)
  - Inter MSC
  - Inter SGSN
  - Inter System (UMTS - GSM)
- Hard Handover
  - Connection to a Node B is destroyed before a new one (to another Node B) is started

# Communication Systems

## UTRAN - connection based functions

- Soft Handover
  - A MS is in the overlapping coverage of **2 different base stations (Node B)**
  - Concurrent communication via 2 air interface channels
  - Downlink: Maximal combining with rake receiver
  - Uplink: Routed to RNC for selection combining, according to a frame reliability indicator by the base station



# *Communication Systems*

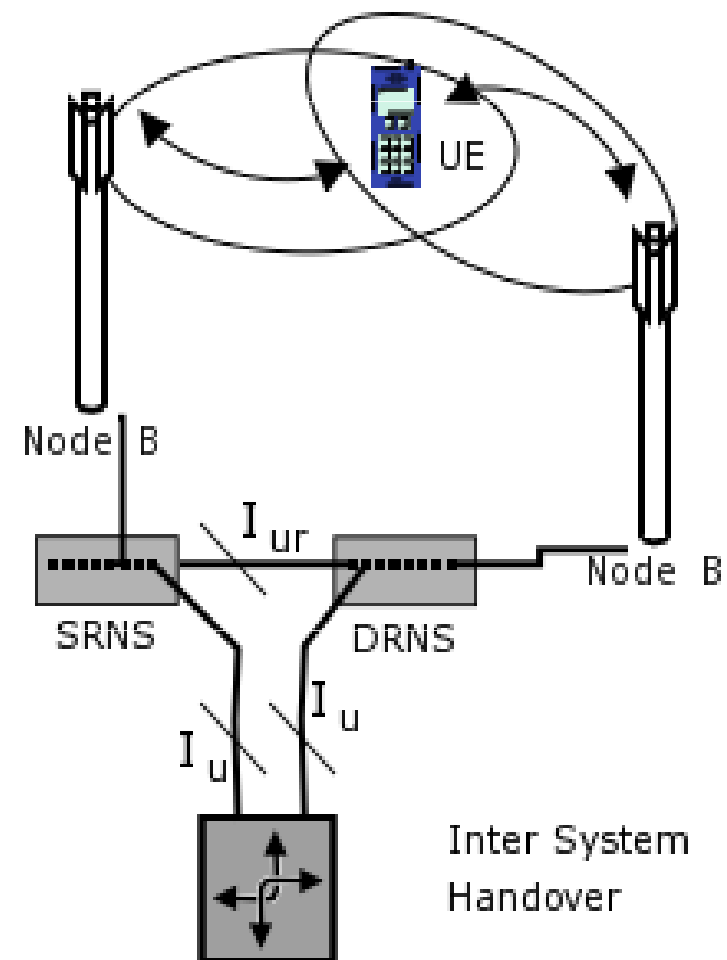
## *UTRAN - connection based functions*

- Softer Handover
  - A MS is in the overlapping coverage of **2 sectors of a base station**
  - Concurrent communication via 2 air interface channels
  - 2 channels are maximally combined with rake receiver
- Soft Softer Handover
  - Soft and softer handover combined
- Inter system handover from UMTS to GSM or vice versa
  - RNS the UE is connected to is the Serving RNS
  - RNS which provides additional resources, e.g for handover procedure is Drift RNS

# Communication Systems

## UTRAN - connection based functions

- Network crossing handovers
  - End-to-end connection between UE and CN is handled over the Iu interface of the SRNS (Serving Radio Network Subsystem)
  - Exchange of SRNS will lead to change of Iu
  - Initiated by SRNS
  - Handled by RNC and CN





# ***Communication Systems***

## ***UTRAN – Base Stations (Node B) – Radio Interface***

- Base Station – Node B
  - Main task of node B is to establish the physical implementation of the Uu interface (communication with the UE) and the implementation of Iub interface (Communication with the RNC)
  - Providing the Uu interface means that the Base Station implements WCDMA radio access *Physical Channels* and transfer information from Transport Channels to the Physical Channels based on arrangements determined by the RNC
  - The term Physical Channels means different kinds of bandwidth allocated for different purposes over Uu interface

# ***Communication Systems***

## ***UMTS - Air Interface***

- UTMIS uses Wideband CDMA (Code Division Multiple Access) on two different duplex mechanisms
- CDMA allows frequency reuse factor of 1 (GSM 4 ... 18)
  - 5MHz Bandwidth allows multipath diversity using „Rake Receiver“
  - Variable Spreading Factor (VSF) to offer Bandwidth on Demand (BoD) up to 2MHz
  - Fast (1.5kHz) Power Control for Optimal Interference Reduction
- Services multiplexing with different QoS
- Real-time / Best-effort
  - 10% Frame Error Rate to  $10^{-6}$  Bit Error Rate

# Communication Systems

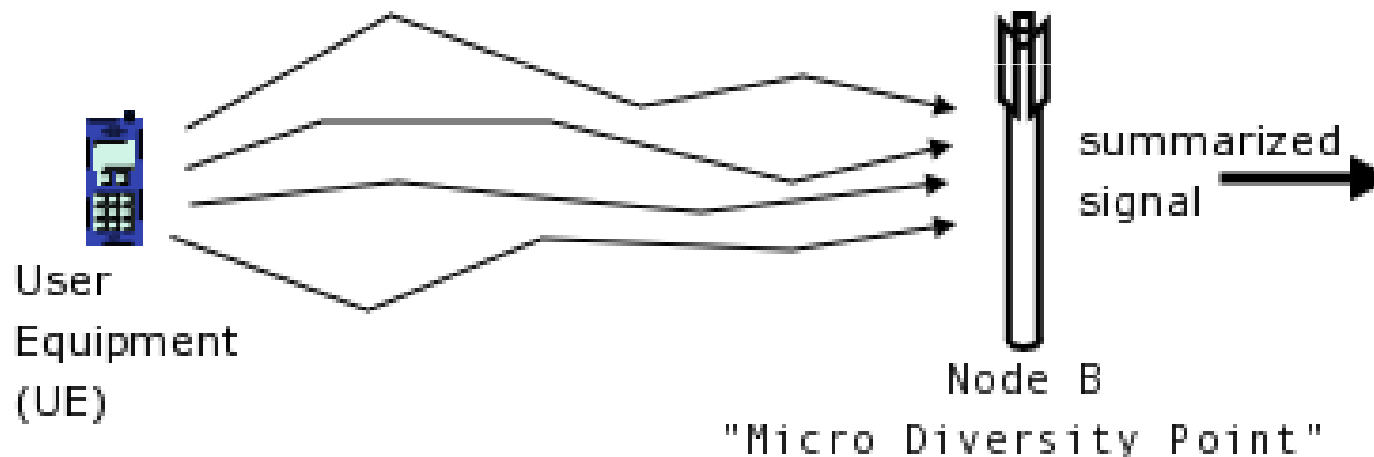
## UMTS – QoS classes

Traffic class	Conversational class	Streaming class	Interactive class	Background
<b>Fundamental characteristics</b>	<p>Preserve time relation between information entities of the stream</p> <p>Conversational pattern (stringent and low delay)</p>	<p>Preserve time relation between information entities of the stream</p>	<p>Request response pattern</p> <p>Preserve data integrity</p>	<p>Destination is not expecting the data within a certain time</p> <p>Preserve data integrity</p>
<b>Example of the application</b>	Voice, videotelephony, video games	Streaming multimedia	Web browsing, network games	Background download of emails

# *Communication Systems*

## *UMTS – Rake Receiver*

- Radio receiver designed to counter the effects of multipath fading
  - rake receiver is so named because of its analogous function to a garden rake, each finger collecting bit or symbol energy similarly to how tines on a rake collect leaves
  - Commonly used in a wide variety of CDMA and W-CDMA radio devices



# *Communication Systems*

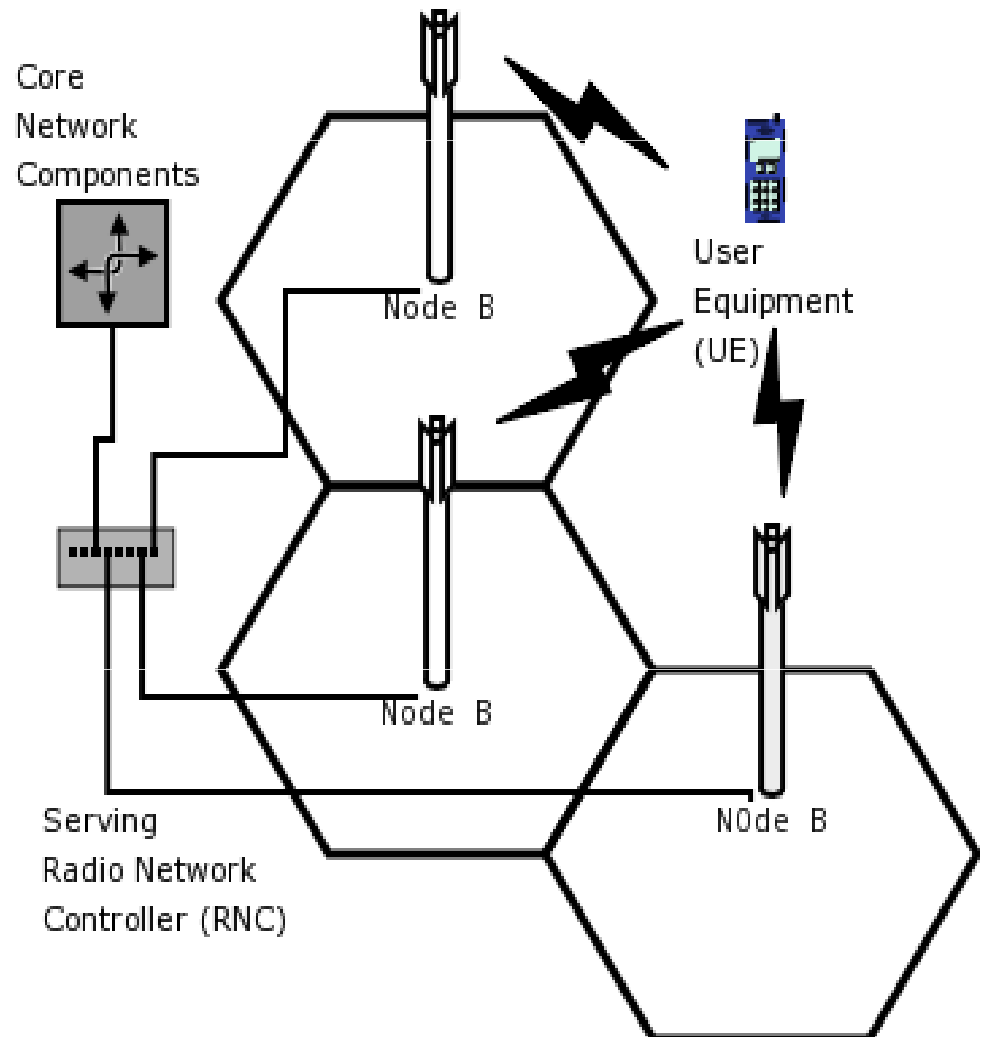
## *UMTS – Rake Receiver*

- Radio receiver
  - Uses several "sub-receivers" each delayed slightly in order to tune in to the individual multipath components
  - Each component decoded independently, but at a later stage combined in order to make the most use of the different transmission characteristics of each path
  - Results in higher Signal-to-noise ratio (or  $E_b/N_0$ ) in a multipath environment than in a "clean" environment
  - Multipath fading is a common problem in wireless networks especially in metropolitan areas
- Another "trick" to increase connection quality and reliability is macro diversity

# Communication Systems

## UMTS – Macro Diversity

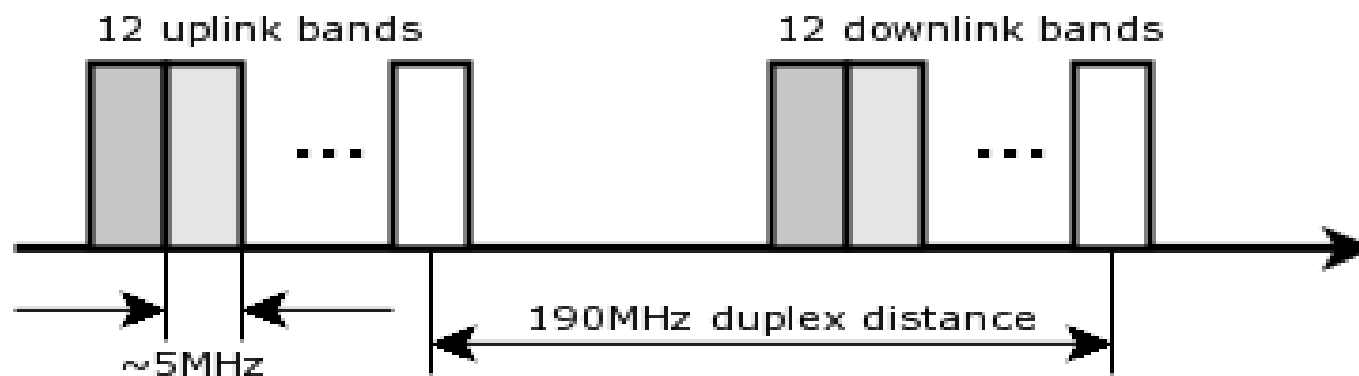
- Same data stream is sent over different physical channels
- Uplink – UE sends its data to different Node B
- Data stream is reassembled, reconstructed in Node B, SRNC or NC
- Downlink – receiving same data from different cells on different spread codes



# *Communication Systems*

## *UMTS - Air Interface*

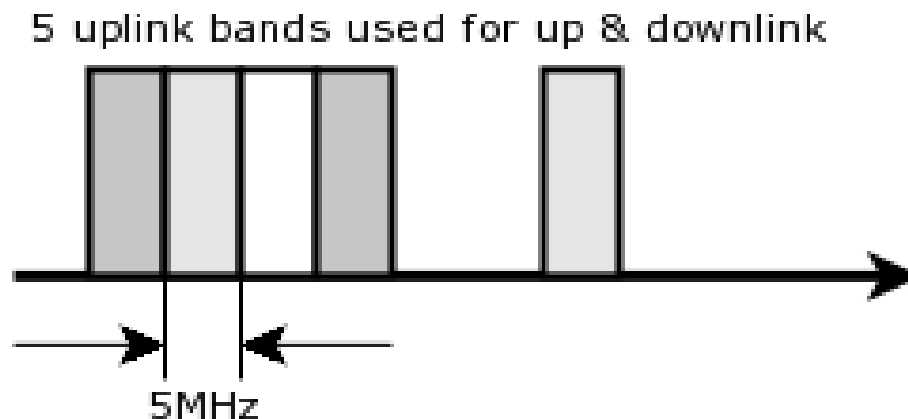
- UMTS FDD (Frequency Division Duplex)
  - Uplink: 1920 - 1975 MHz
  - Downlink: 2110 - 2165 MHz
  - 190 MHz duplex distance
  - ca. 5MHz (variable) carrier spacing (DS CDMA – Direct Sequence CDMA)
  - 12 bands in uplink & downlink



# Communication Systems

## UMTS - Air Interface

- UMTS TDD (Time Division Duplex)
- Uplink & Downlink: 1900 - 1920 MHz and 2020 - 2025 MHz
  - 5 carriers in total, 15 timeslots per frame
  - a user may use one or several timeslots
  - a timeslot can be assigned to either uplink or downlink





# *Communication Systems*

## *UMTS – Cell Breathing*

- Advantages of UMTS W-CDMA
  - Power Control - solves the near-far problem
- Soft capacity, dynamic cell sizes
  - Different to GSM, where
    - fixed cell size
    - Number of logged in users has no influence on cell size
- In UMTS cell size is tightly interrelated with its capacity
  - Size depends on signal/noise ratio because of both maximum Tx power and number of active users (interference in the same cell through other users and with other cells) which results in cell breathing

# ***Communication Systems***

## ***UMTS – Cell Breathing***

- Interference increases noise in signal
  - UE on the cell edge is transmitting with max power
  - Another UE becomes active – results in increased interference
  - The received signal from the UE on the cell edge is too weak and communication becomes impossible
  - Restriction of participants needed
  - Effective cell size decreases with increasing number of users
  - There is a trade-off between capacity and coverage
  - Results in cell breathing and imposes greater difficulties on network planning

# Communication Systems

## Differences and similarities of GSM and UMTS

Key differences between WCDMA and GSM		
	WCDMA	GSM
Carrier size	5 MHz CDMA	200 kHz TDMA (Time Division Multiple Access)
Frequency reuse	1	~4-18
Intra-system Handoff	Soft handoff (simultaneous communication with multiple base stations)	Hard handoff (connection with one cell breaks before next connection is made)
Frequency diversity	Rake receiver demodulates multipath signals for diversity gain	Equalization and frequency hopping reduce multipath interference; not a diversity gain
System capacity	Soft, depending on loading threshold and intra-system interference	Hard, depending on frequency reuse scheme
Power control	1500 MHz both links	2 Hz or less (very slow)
Cell search procedure	Using Synchronization channel and scrambling code	Using frequency channels
Transmit diversity	Supported on downlink	Not supported

# Communication Systems

## Differences and similarities of GSM and UMTS

Key similarities and differences between WCDMA and IS-95 CDMA		
	WCDMA	IS-95 CDMA
Carrier size and chip rate	5 MHz / 3.84 Mcps chip rate	1.25 MHz / 1.2288 Mcps chip rate
Intra-system Handoff	Soft / softer handoff supported	Soft / softer handoff supported
Inter-system Handoff	Handoff to GSM supported via slotted mode measurements	Handoff to AMPS supported
Multipath reception	Yes (rake receiver), can resolve more multipath signals due to ~3x wider bandwidth relative to cdma2000 1X	Yes (rake receiver)
Power control	Both links fast at 1500 Hz	Uplink at 800 Hz; slow power control on forward link

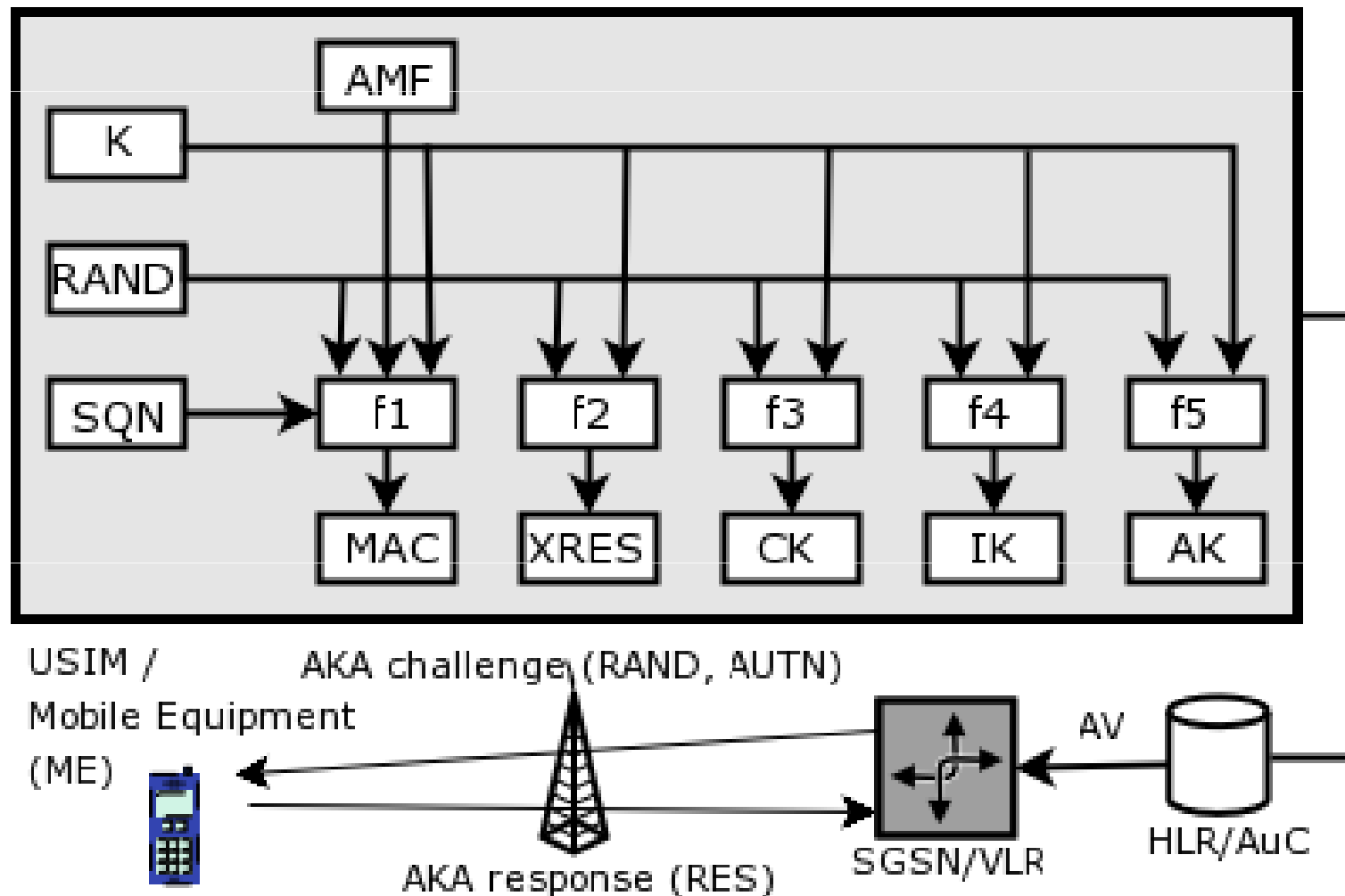
# ***Communication Systems***

## ***UMTS – security and authentication***

- Security in GSM is weak by our todays standards, mostly broken and only one way (client-to-network auth)
- Authentication in UMTS
  - Basis is a common secret key  $K$ , which is only known by the USIM (User Services Identity Module) in the UE and by the HLR/AuC of the provider
  - The VLR or SGSN which should authenticate the user requests from the HLR/AuC 1..n AV(Auth Vectors)
  - Each AV is a 5-tupel consisting of
    - RAND (random challenge) and XRES (expected response) for the user authentication
    - CK (cipher key) for protection of confidentiality, IK (integrity key) for protection of integrity, AUTN (auth token) for network authentication

# Communication Systems

## UMTS – security and authentication



# ***Communication Systems***

## ***UMTS – security and authentication***

- RAND and AUTN are sent to the UE/USIM, which checks AUTN and computes the response RES to the challenge RAND
  - RES is sent to the VLR/SGSN which compares it to XRES
- Integrity and confidentiality
  - By request of MSC/VLR or SGSN the communication can be encrypted with CK or IK between UE and RNC
  - Encryption takes place on the RLC layer and prevents forgery of data and encryption

# ***Communication Systems***

## ***UMTS – security and authentication***

- Functions for authentication and key agreement (AKA)
  - f1: computation of MAC (Message Auth. Code)
  - f2: computation of MAC, probably shortened
  - f3, f4, f5: computation of a key from a random number
  - $\otimes$  XOR,  $||$  concatenation
- Generation of AV (within HLR/AuC)
  - Generation of random Sequence Number (SEQ, once at the beginning)
  - Generation of random challenge RAND (per AV)
  - AMF (Authentication Key Management Field) to distinguish several different algorithms



# ***Communication Systems***

## ***UMTS – security and authentication***

- Computation of the several values (within HLR/AuC)
  - $MAC = f_1(SQN \parallel RAND \parallel AMF)$
  - $XRES = f_2(RAND)$
  - $CK = f_3(RAND)$
  - $IK = f_4(RAND)$
  - $AK = f_5(RAND)$  , anonymity key to anonymize SQN
  - $AUTN = ((SQN \otimes AK) \parallel AMF \parallel MAC)$
  - $AV = (RAND \parallel XRES \parallel CK \parallel IK \parallel AUTN)$

# *Communication Systems*

## *UMTS – security and authentication*

- Computation of the several values (within USIM)
  - Reception of RAND and AUTN from VLR or SGSN
  - $AK = f_5(RAND)$
  - $SQN = (SQN \otimes AK) \otimes AK$
  - $XMAC = f_1(SQN || RAND || AMF)$  (eXpected MAC)
  - Comparison of XMAC and MAC (from AUTN)
    - If this procedure fails the authentication of network does not succeed and the UE sees the cell as forbidden
  - Check if sequence number is from the expected range
  - $RES = f_2(RAND)$

# ***Communication Systems***

## ***UMTS – security and authentication***

- Computation of the several values (within USIM, cont.)
  - Send response to VLR or SGSN with RES
  - $CK=f_3(RAND)$
  - $IK=f_4(RAND)$
  - IK, CK used for RLC encryption
- Operation within VLR or SGSN
  - Reception of RES from the USIM
  - Comparison of RES with XRES (eXpected RES, from AV sent by HLR/AuC)
    - If not equal user authentication failed

# ***Communication Systems***

## ***UMTS – some aspects left ...***

- Explanation of the Code Division Multiple Access
  - “Chips” instead of combined TDM, FDM
  - TDD and FDD frame structure
  - ...
- Then: Switch over to other wireless technology for packet networks / IP, like
  - WLAN, Bluetooth, ...

# ***Communication Systems***

## ***UMTS literature***

- German text books:
  - Jochen Schiller, Mobilkommunikation
  - Bernhard Walke, Mobilfunknetze und ihre Protokolle, Grundlagen GSM, UMTS, ...
- Link:
  - <http://www.ks.uni-freiburg.de/download/papers/telsemWS05/UMTS-nextGeneration/UMTS-Seminararbeit-Stefan%20Nagy.pdf>