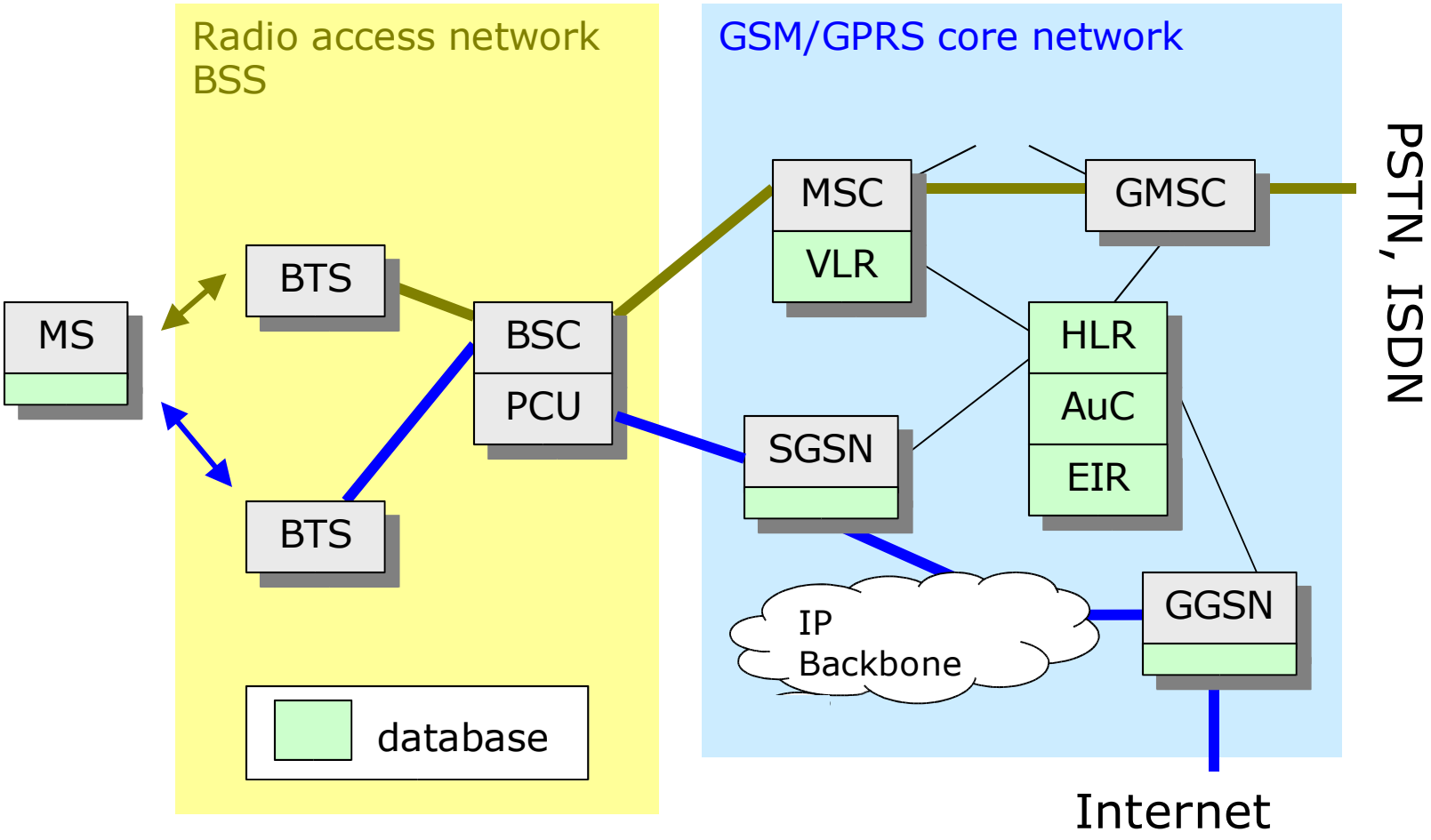
3G Technology and Concepts

Further information on 3G:

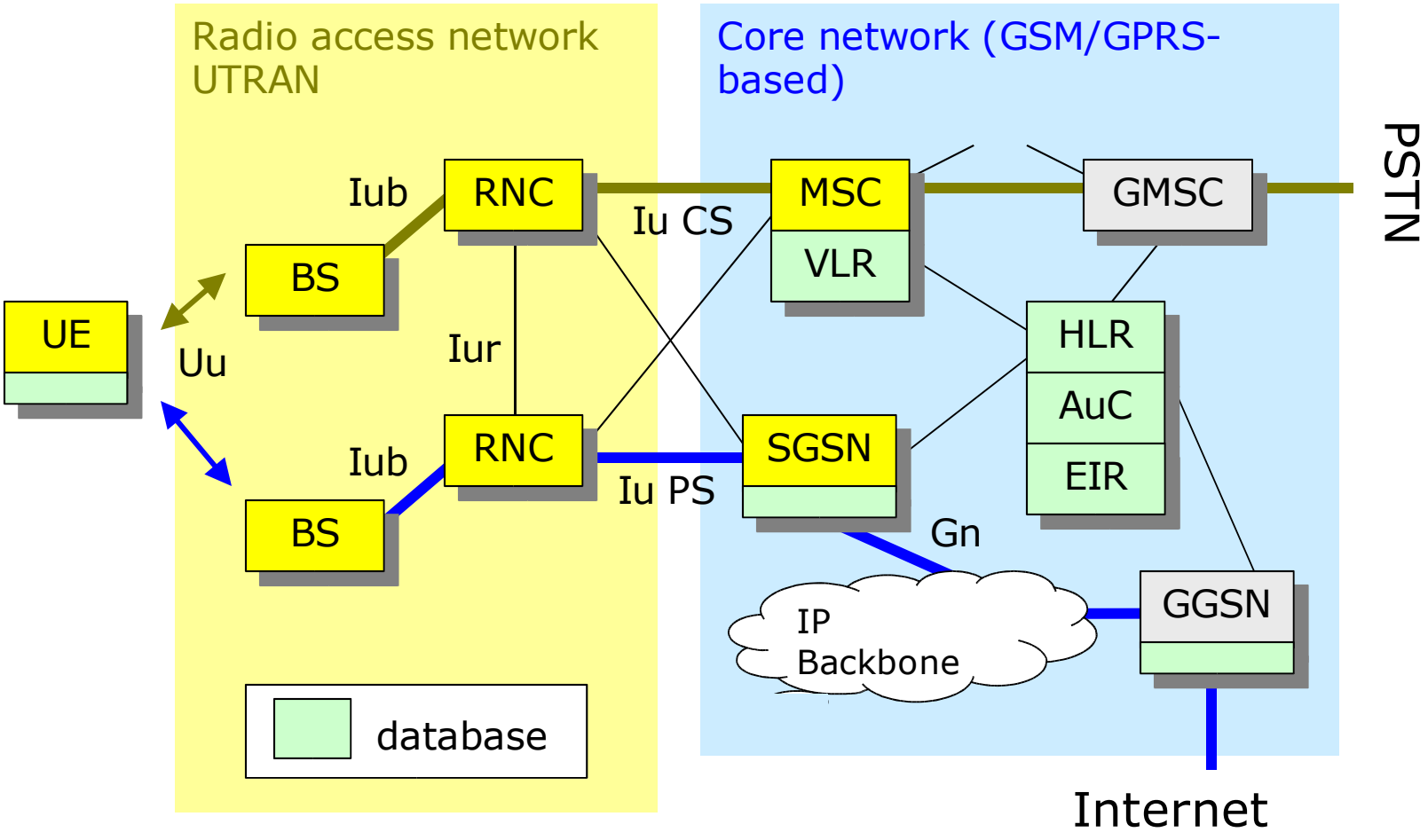
www.3gpp.org (freely available 3GPP standards)

www.umts-forum.org

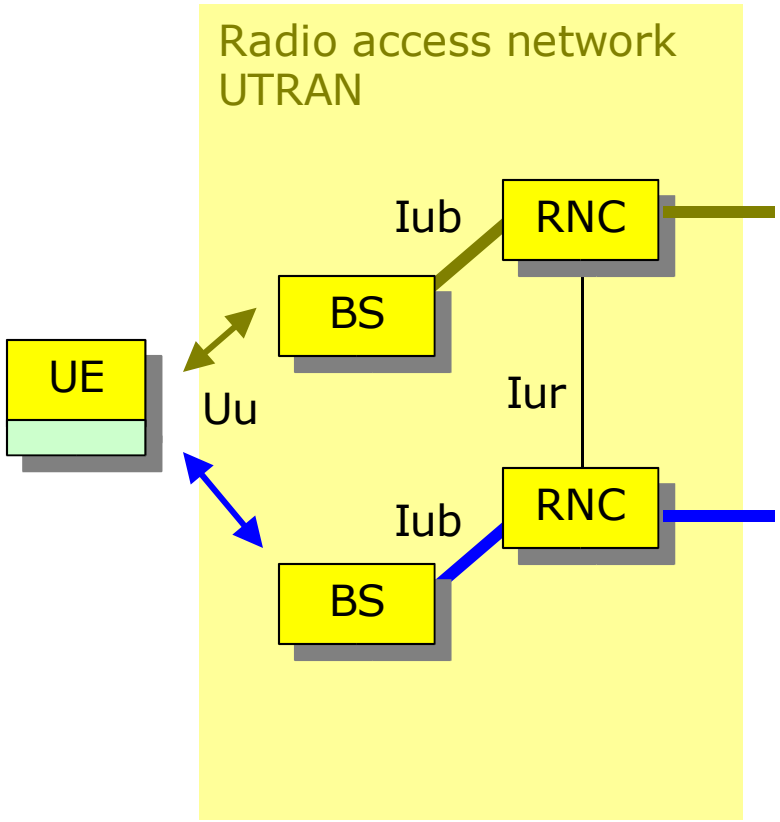
GSM/GPRS network architecture



3GPP Rel.'99 network architecture



3GPP Rel.'99 network architecture



2G => 3G ➡ MS => UE (User Equipment), often also called (user) terminal

New air (radio) interface based on WCDMA access technology

New RAN architecture (Iur interface is available for soft handover, BSC => RNC)

3GPP Rel.'99 network architecture

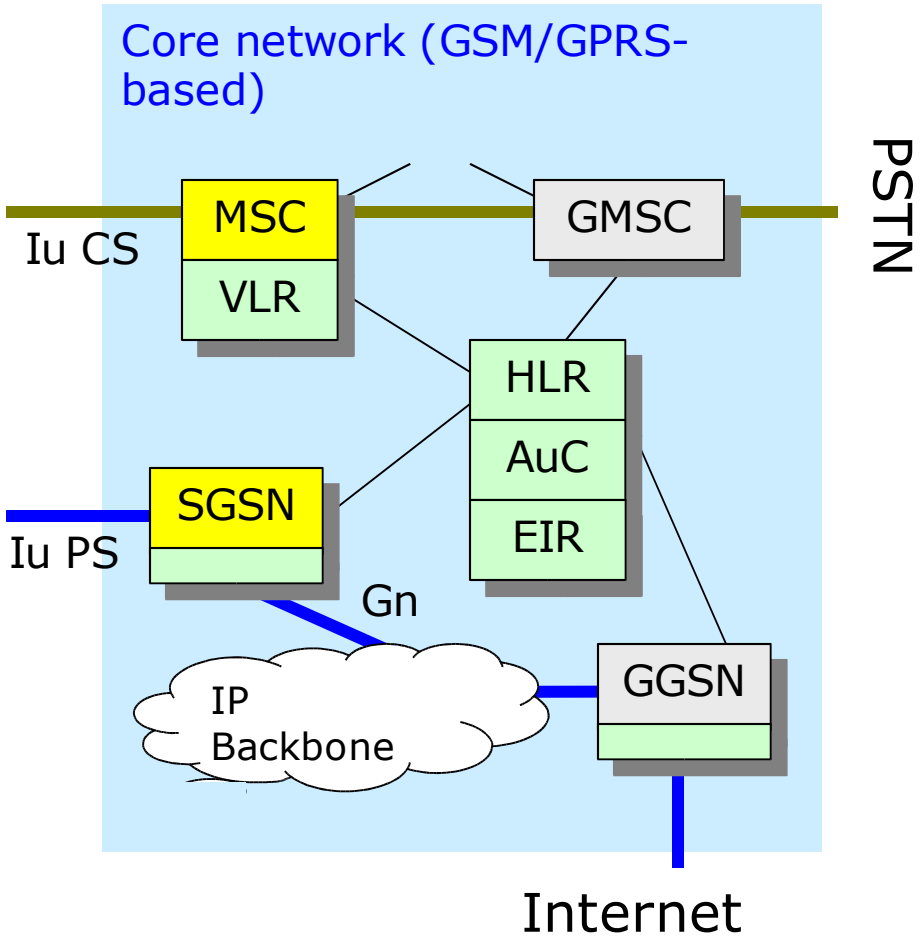
Changes in the core network:

MSC is upgraded to 3G MSC

SGSN is upgraded to 3G SGSN

GMSC and GGSN remain (essentially) the same

AuC is upgraded (more security features in 3G)

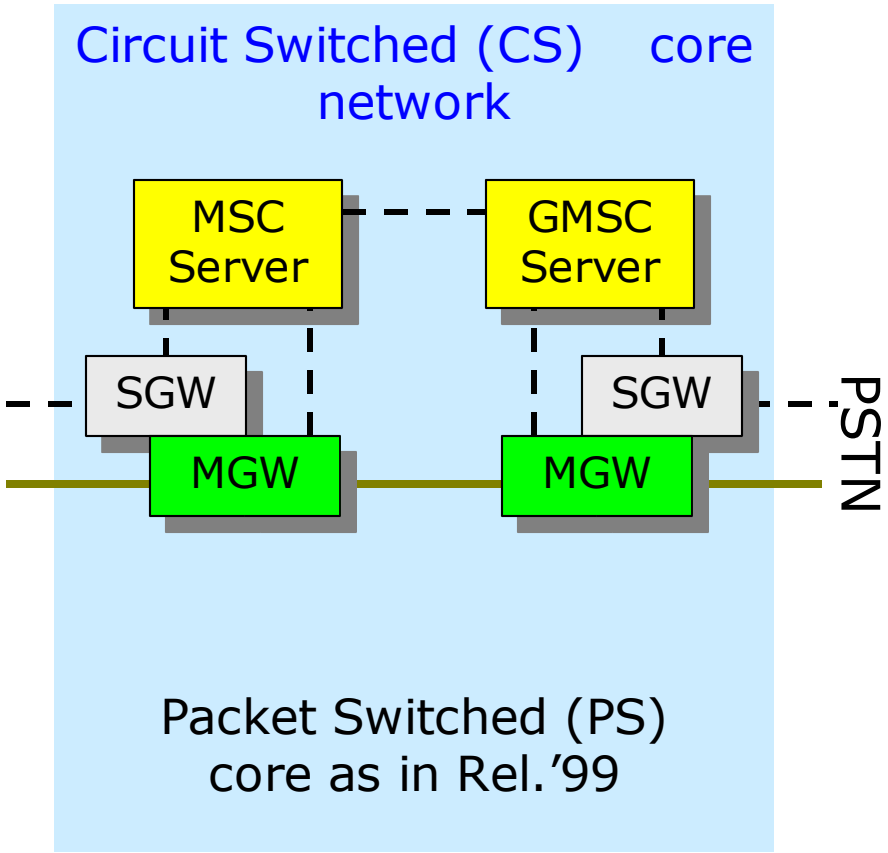


3GPP Rel.4 network architecture

UTRAN
(UMTS Terrestrial Radio Access Network)

New option in Rel.4:

GERAN
(GSM and EDGE Radio Access Network)

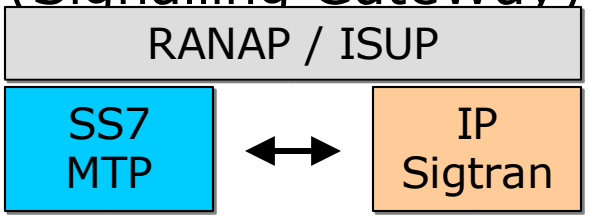


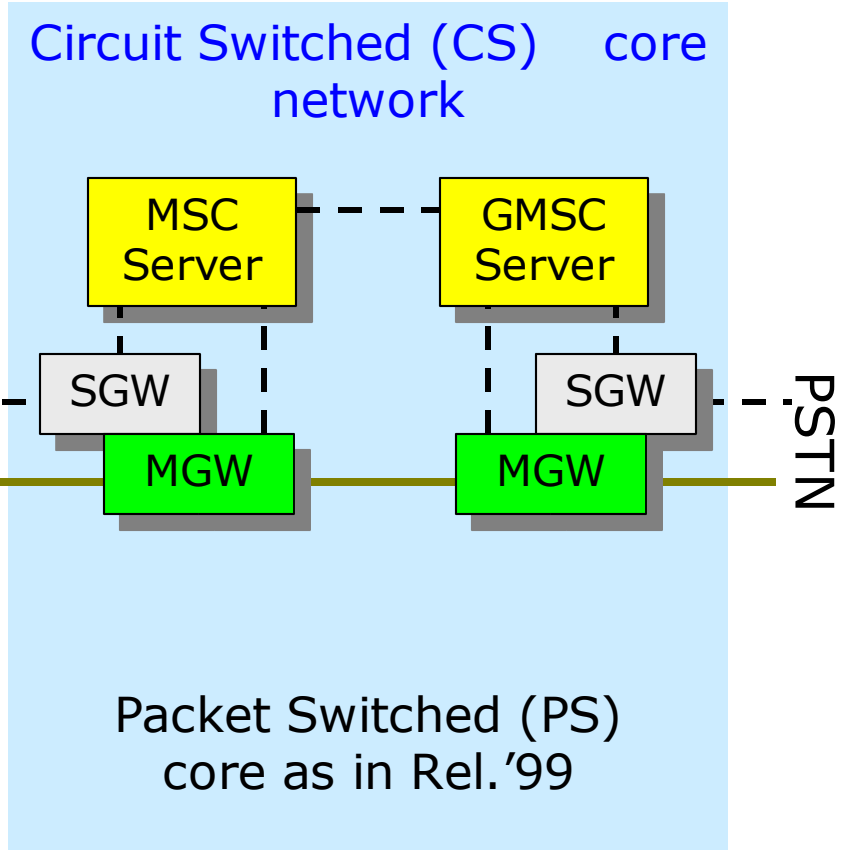
3GPP Rel.4 network architecture

MSC Server takes care of call control signalling

The user connections are set up via MGW (Media GateWay)

"Lower layer" protocol conversion in SGW (Signalling GateWay)

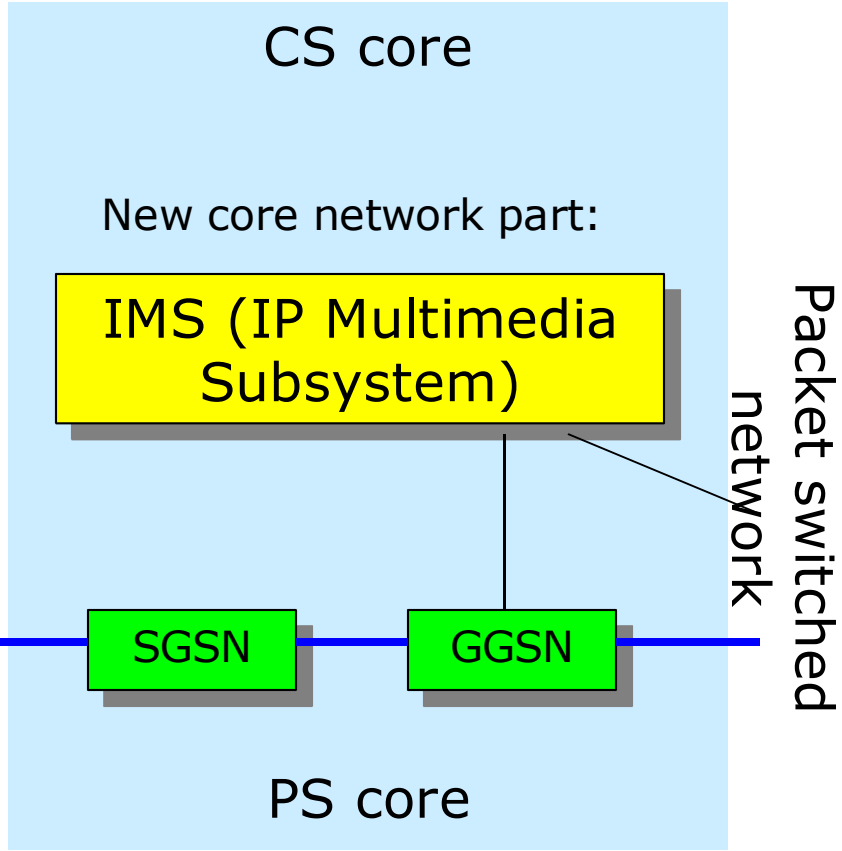




3GPP Rel.5 network architecture

UTRAN
(UMTS Terrestrial Radio Access Network)

GERAN
(GSM and EDGE Radio Access Network)



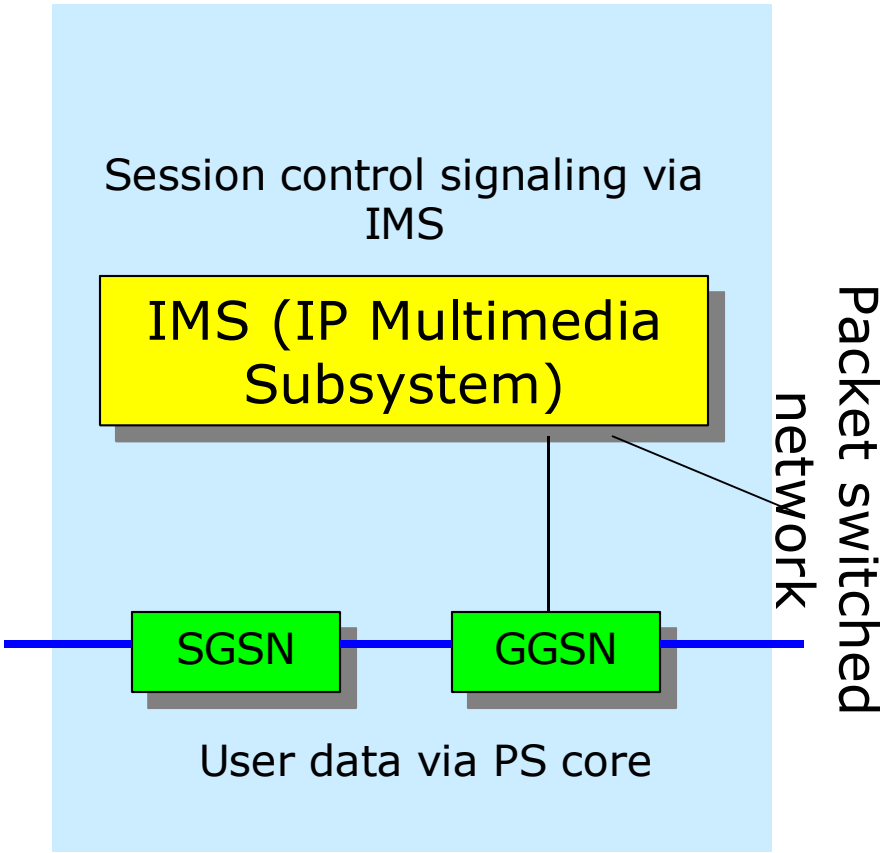
3GPP Rel.5 network architecture

The IMS can establish multimedia sessions between two or more user terminals (using IP transport)

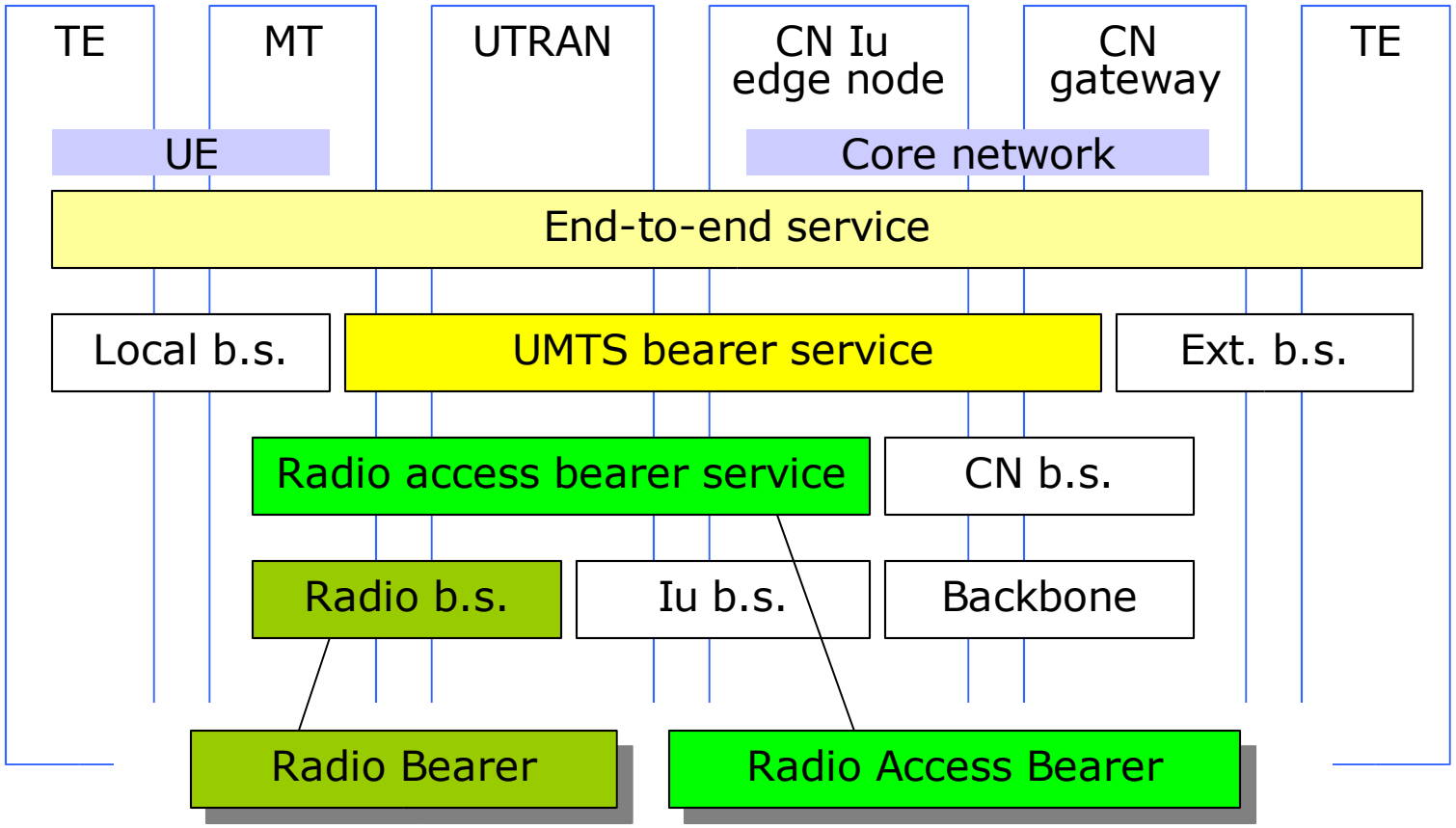
User data transport is always via PS core

Call/session control signaling is via IMS using SIP (Session Initiating Protocol)

More in last lecture of this course.



UMTS bearer service architecture



What is a bearer?

Bearer: a bearer capability of defined capacity, delay and bit error rate, etc. (as defined in 3GPP specs.)

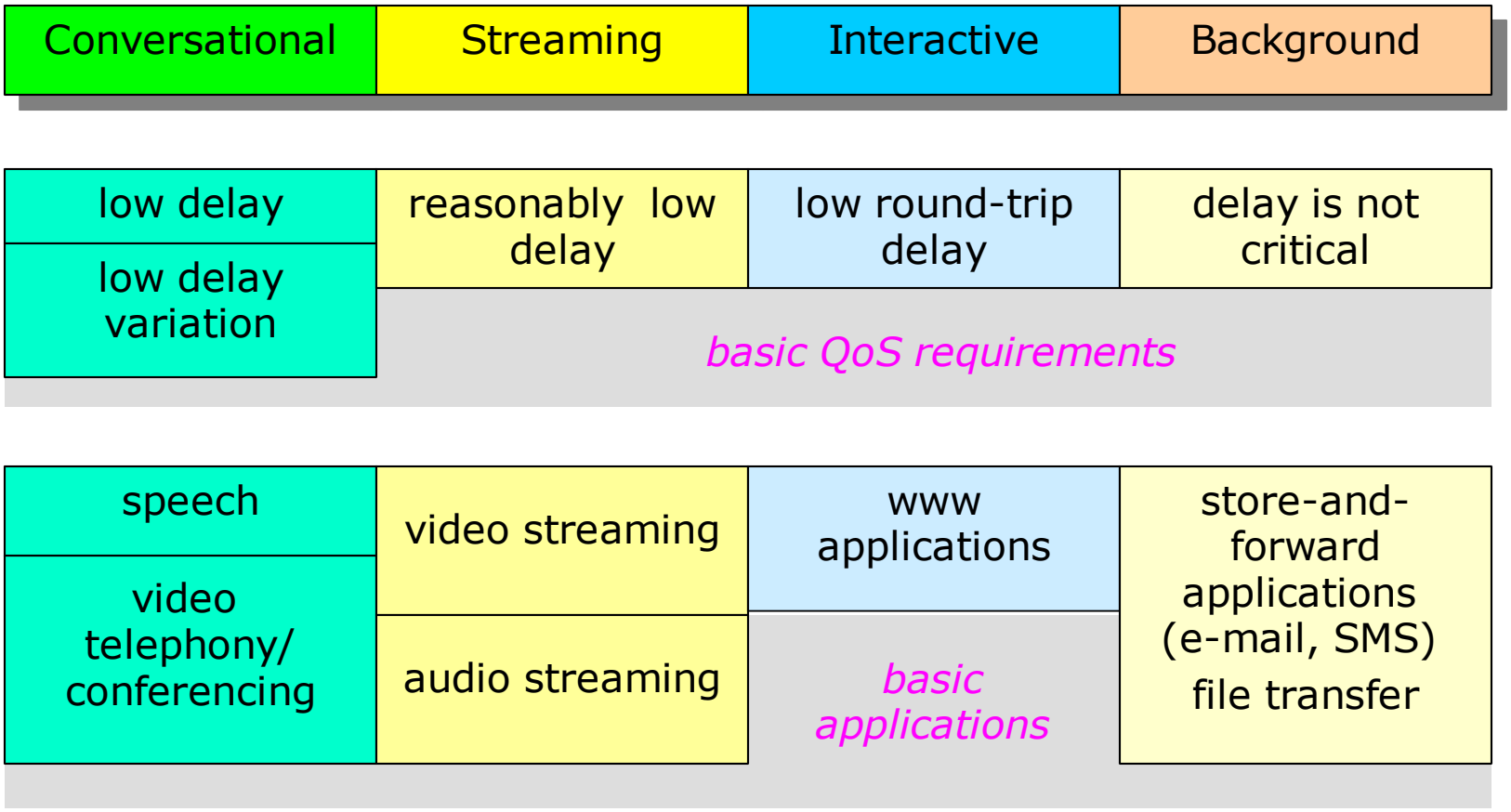
Bearer is a flexible concept designating some kind of ”bit pipe”

- at a certain network level (see previous slide)
- between certain network entities
- with certain QoS attributes, capacity, and traffic flow characteristics

Four UMTS QoS Classes

- conversational, streaming, interactive, background

UMTS QoS (service) classes



Four UMTS QoS (service) classes (1)

Conversational	Streaming	Interactive	Background

- low delay (< 400 ms) and low delay variation
- BER requirements not so stringent
- in the radio network => real-time (RT) connections

- speech (using AMR = Adaptive Multi-Rate speech coding)
- video telephony / conferencing:

  ITU-T Rec. H.324 (over circuit switched connections)

  ITU-T Rec. H.323 or IETF SIP (over packet switched connections)

Adaptive Multi-Rate coding

Adaptive

<=>

During the call, the AMR bit rate can be changed, using the values at the right

<=>

Codec negotiation between transcoders

kbit/s

12.2 (= GSM EFR)

10.2

7.95

7.40 (= US TDMA)

6.70

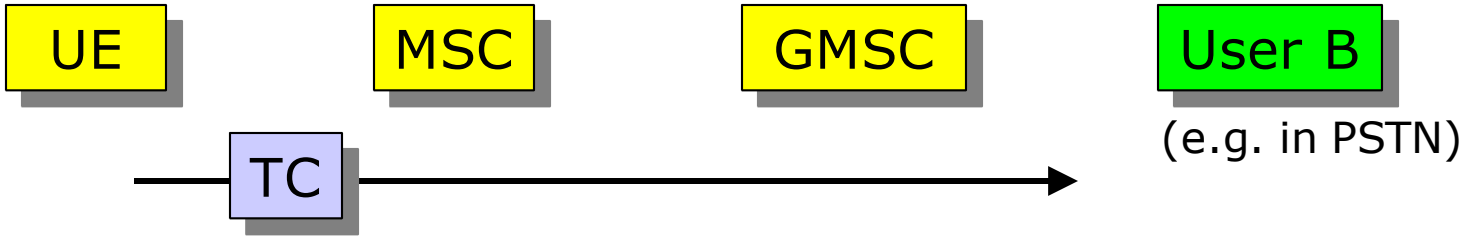
5.90

5.15

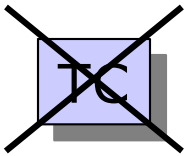
4.75

EFR = Enhanced Full Rate

Transcoding



Transcoder (AMR/PCM) should be located as far as possible to the right (transmission capacity savings)



(possible only if same coding is used at both ends of connection)

Transcoding should be avoided altogether (better signal quality)

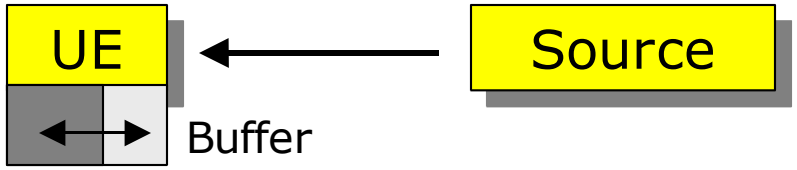
TFO = Tandem Free Operation (2G)
TrFO = Transcoder Free Operation (3G)

Four UMTS QoS (service) classes (2)

Conversational	Streaming	Interactive	Background

- reasonably low delay and delay variation
- BER requirements quite stringent
- traffic management important (variable bit rate)
- in the radio network => real-time (RT) connections

- video streaming
- audio streaming



video or audio information is buffered in the UE,
large delay => buffer is running out of content!

Four UMTS QoS (service) classes (3)

- low round-trip delay (< seconds)
- delay variation is not important
- BER requirements stringent
- in the radio network => non-real-time (NRT) connections
- web browsing
- interactive games
- location-based services (LCS)

Four UMTS QoS (service) classes (4)

Conversational	Streaming	Interactive	Background

- delay / delay variation is not an important issue
- BER requirements stringent
- in the radio network => non-real-time (NRT) connections
- SMS (Short Message Service) and other more advanced messaging services (EMS, MMS)
- e-mail notification, e-mail download
- file transfer

UMTS protocols

Different protocol stacks for user and control plane

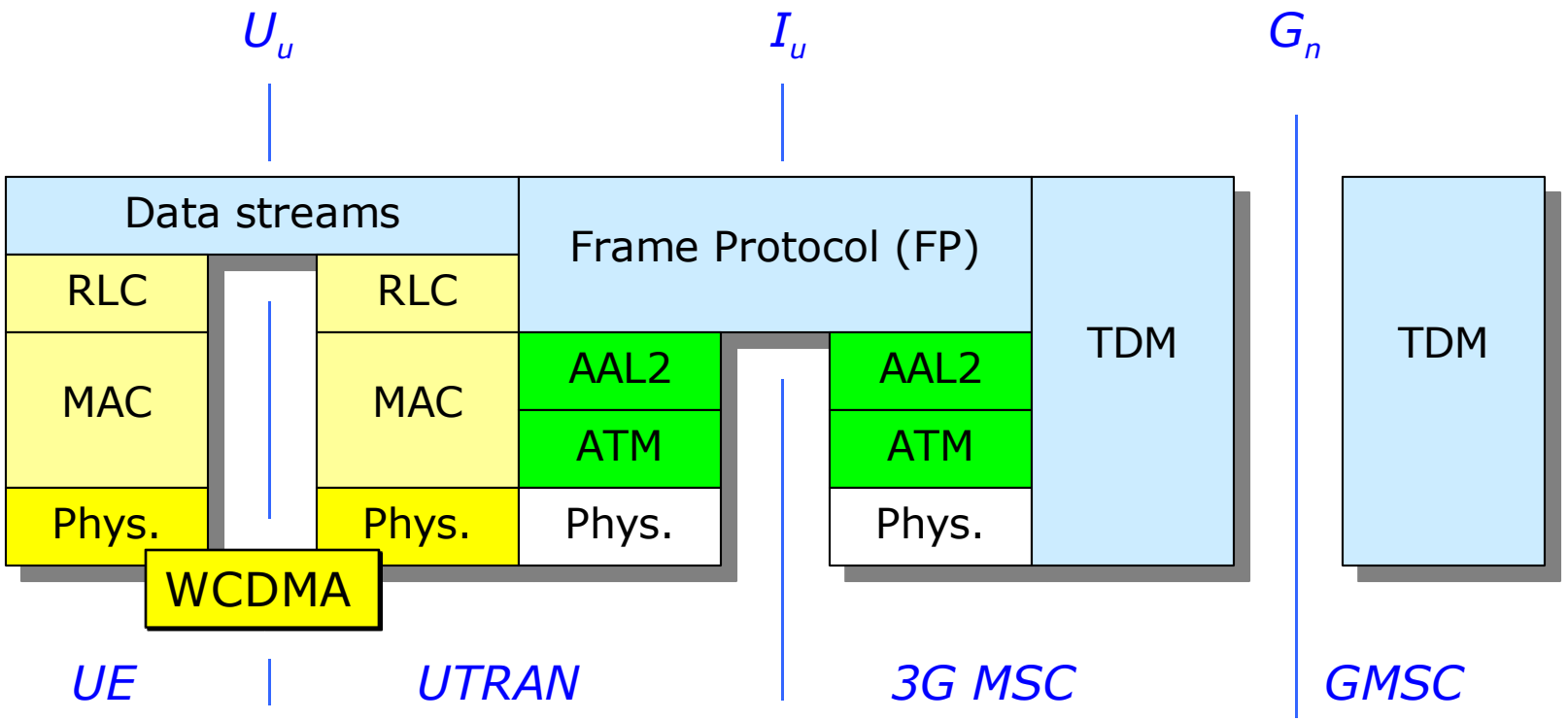
User plane (for transport of user data):

- *Circuit switched domain:* data within ”bit pipes”
- *Packet switched domain:* protocols for implementing various QoS or traffic engineering mechanisms

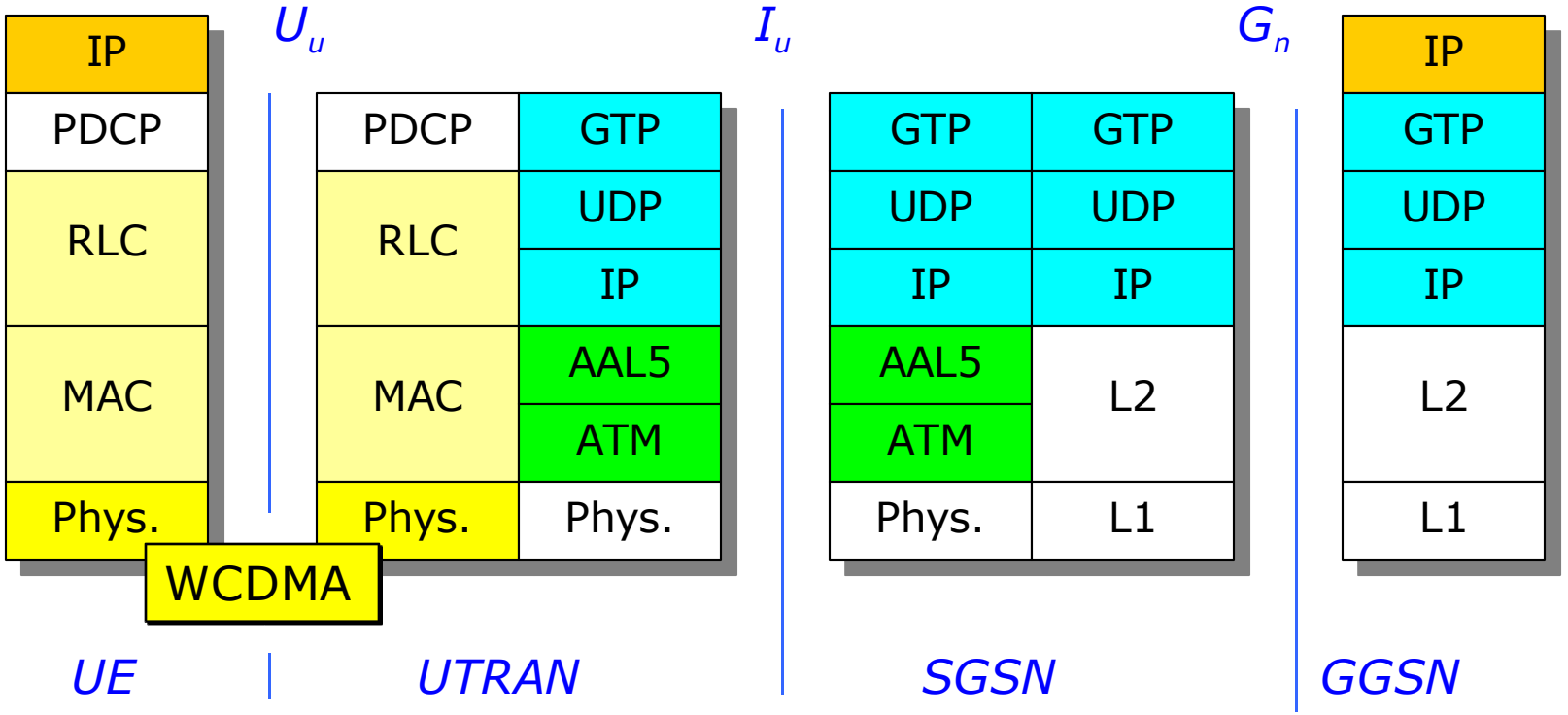
Control plane (for signalling):

- *Circuit switched domain:* SS7 based (in core network)
- *Packet switched domain:* IP based (in core network)
- *Radio access network:* UTRAN protocols

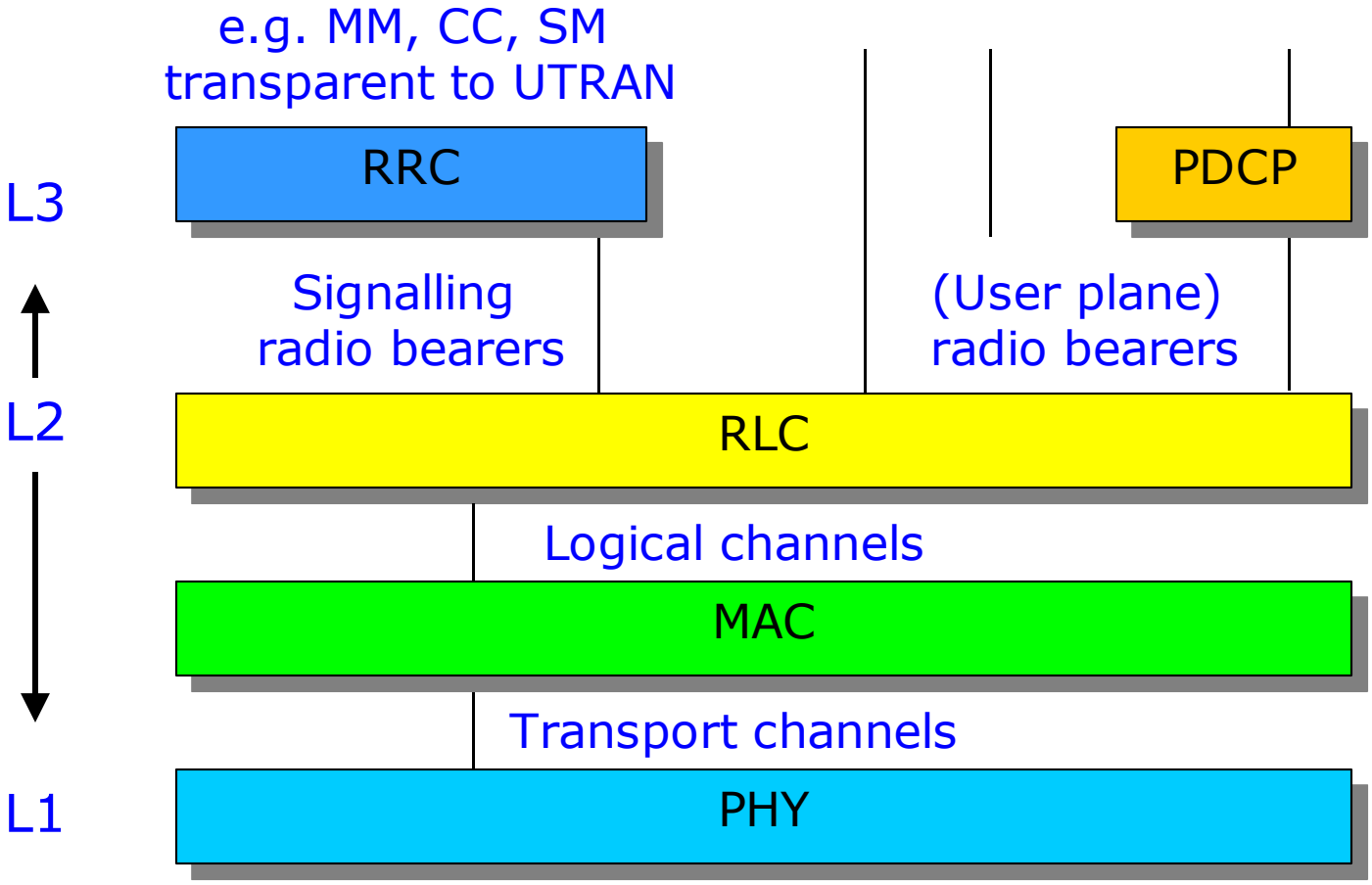
User plane protocol stacks (CS domain)



User plane protocol stacks (PS domain)



Uu (air, radio) interface protocols



Main tasks of Uu interface protocols

MAC (Medium Access Control):

- Mapping between logical and transport channels
- Segmentation of data into transport blocks

RLC (Radio Link Control):

- Segmentation and reassembly
- Link control (flow & error control)
- RLC is often a transparent layer

PDCP (Packet Data Convergence Protocol):

- IP packet header compression (user plane only)

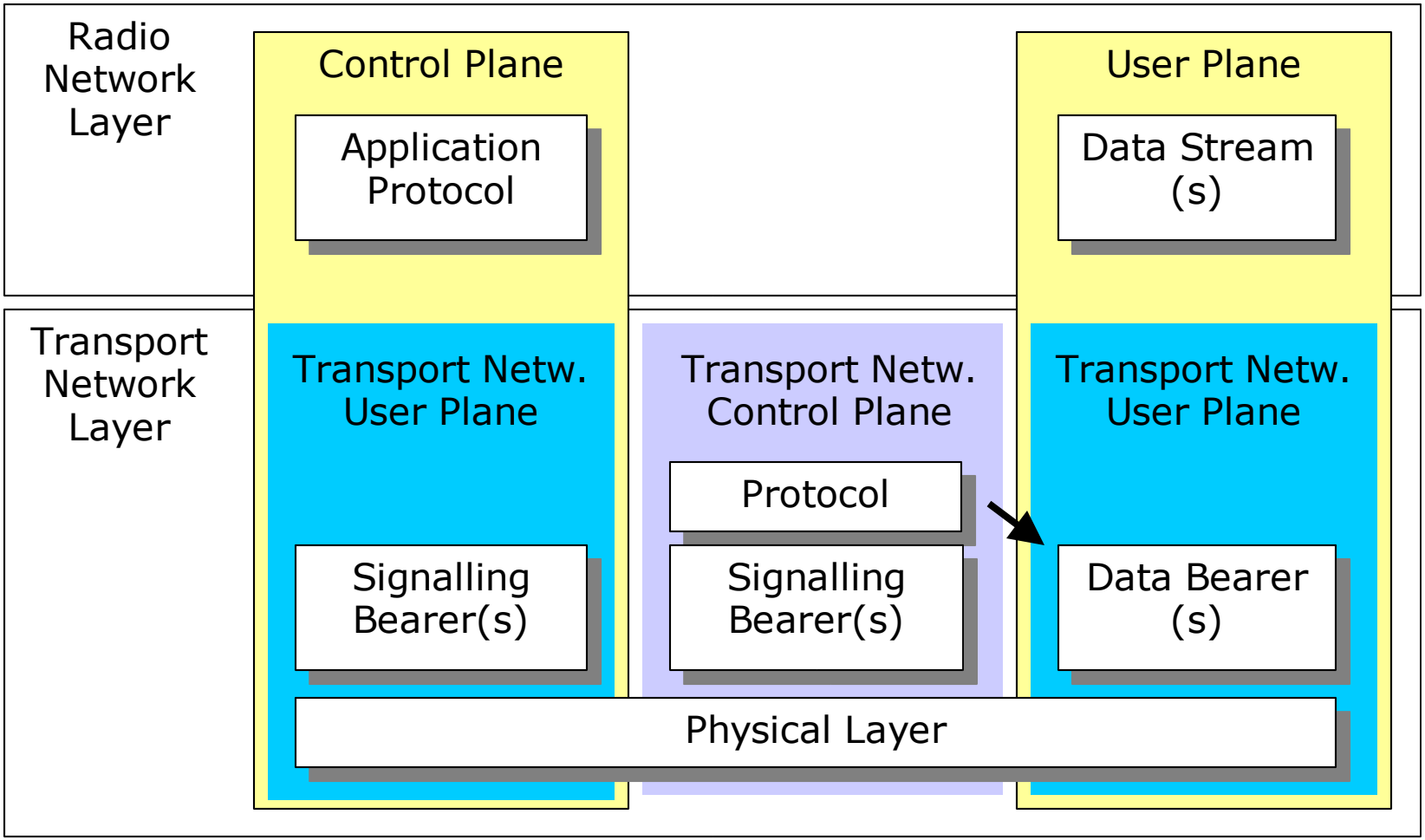
Main tasks of RRC protocol

Over the air interface, Radio Resource Control (RRC) messages carry all the relevant information required for setting up a Signalling Radio Bearer (during the lifetime of the RRC Connection) and setting up, modifying, and releasing Radio Bearers between UE and UTRAN (all being part of the RRC Connection).

RRC also participates in the co-ordination of other Radio Resource Management (RRM) operations, such as measurements and handovers.

In addition, RRC messages may carry in their payload higher layer signalling information (MM, CC or SM) that is not related to the air interface or UTRAN.

General protocol model for UTRAN



Control Plane (Iub, Iur and Iu interfaces)

Radio Network Layer: application protocols (NBAP, RNSAP and RANAP) are used for the actual signalling between base stations, RNC and core network.

Transport Network Layer: signalling bearer for the transport of application protocol messages is set up by O&M actions (i.e. on a permanent basis).

Transport Network Control Plane

A signalling bearer (set up by O&M actions) carries a protocol which is used only for the task of setting up data bearers (e.g. AAL 2 connections).

User Plane (Iub, Iur and Iu interfaces)

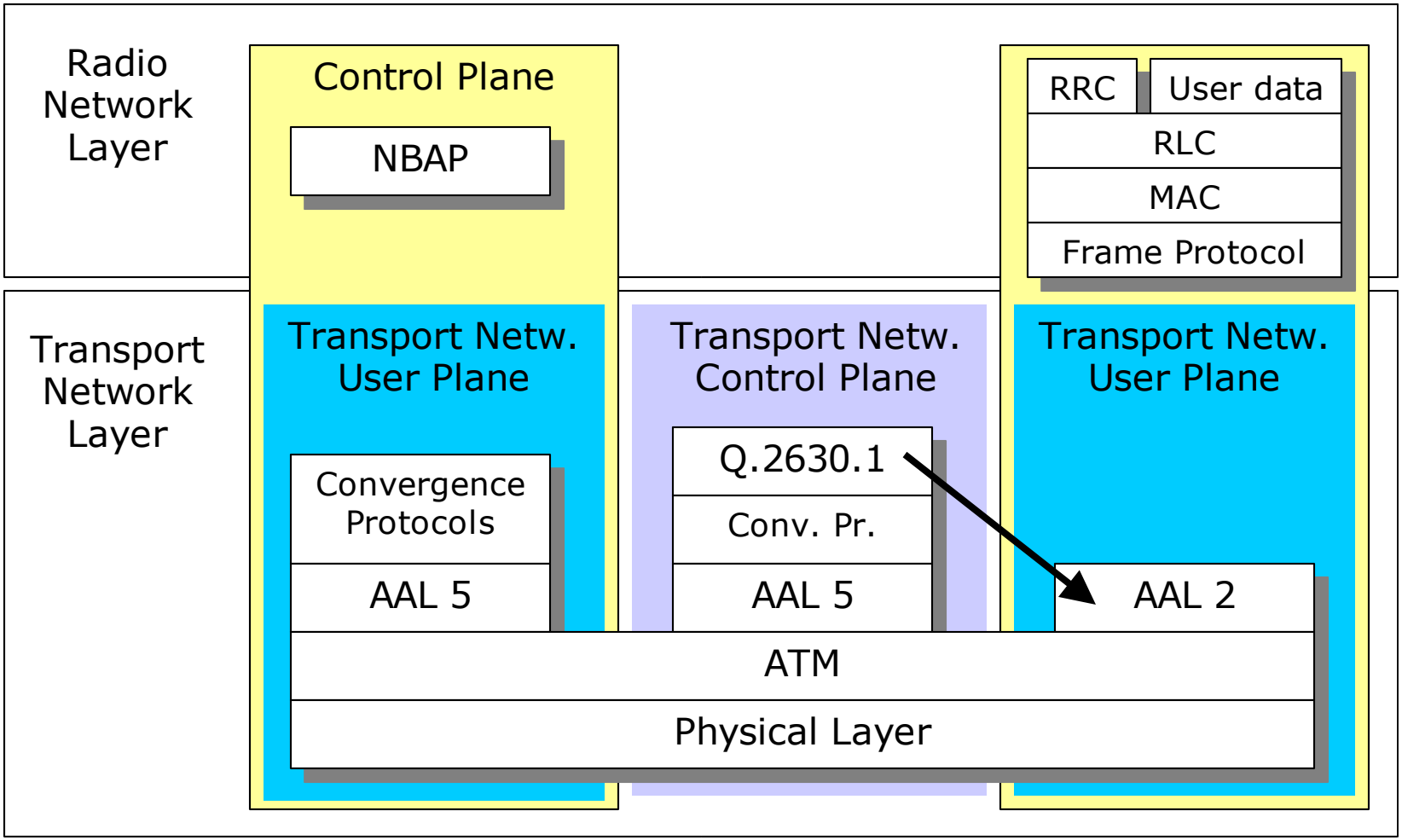
The User Plane is employed for transport of

- user information (speech, video, IP packets ...)
- RRC signalling messages (Iub, Iur)
- higher-layer protocol information at Iu interface (if not carried by RANAP).

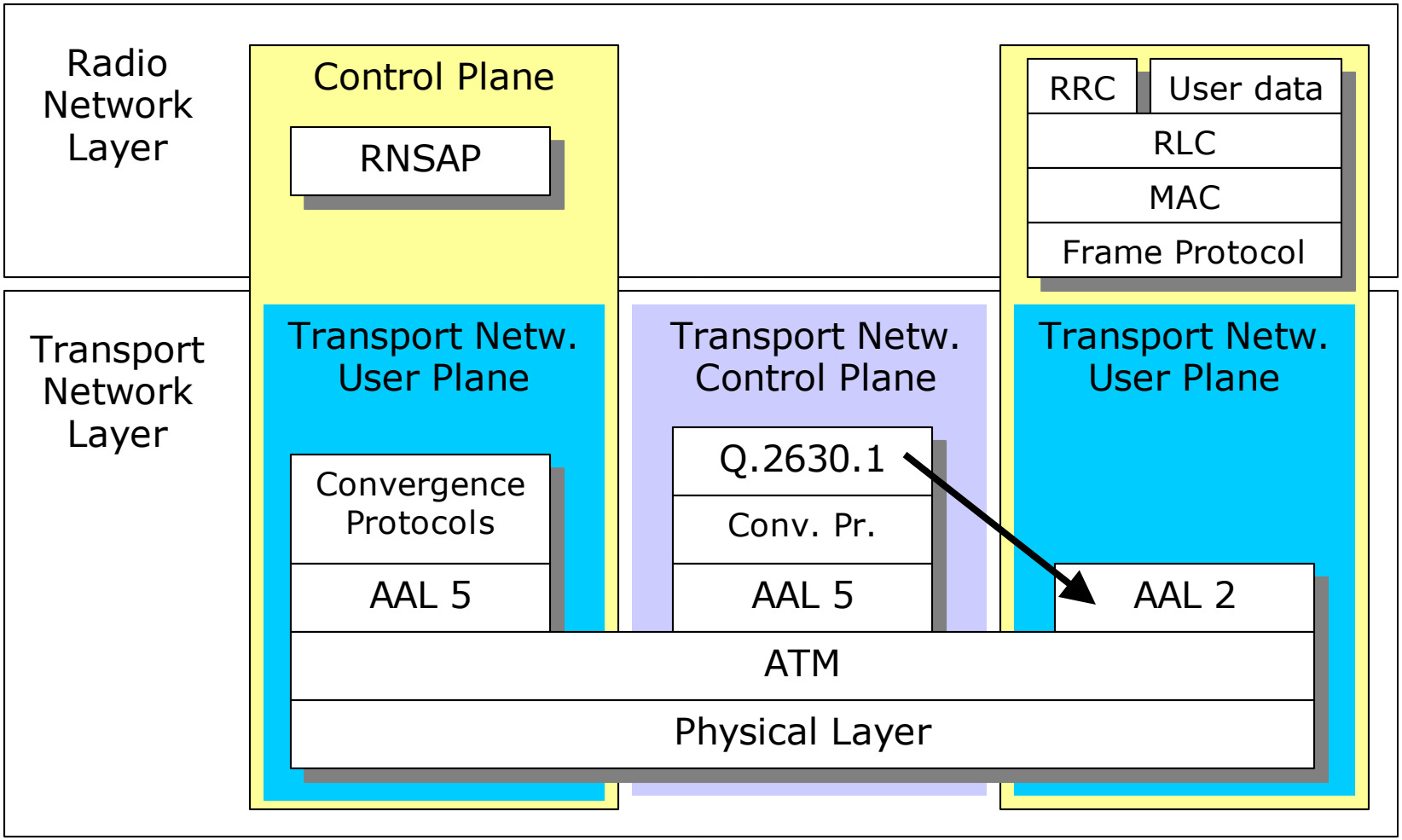
User plane data is carried by data bearers which use AAL 5 in case of Iu PS and AAL 2 in all other cases.

User data streams are packed in frame protocols (FP) which are used for framing, error & flow control, and carrying of parallel data flows that form the user data signal (e.g. AMR encoded speech).

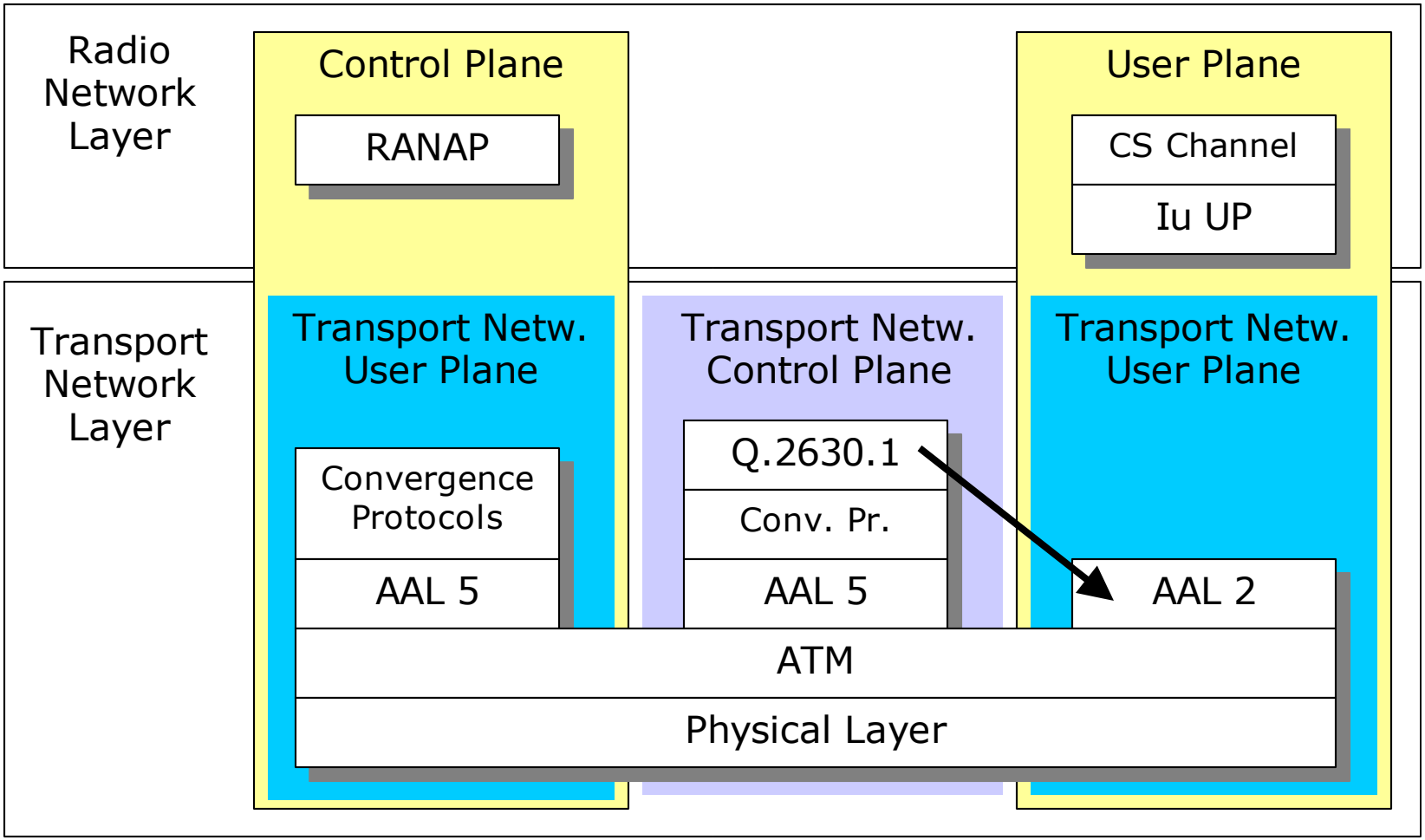
Protocol structure at Iub interface



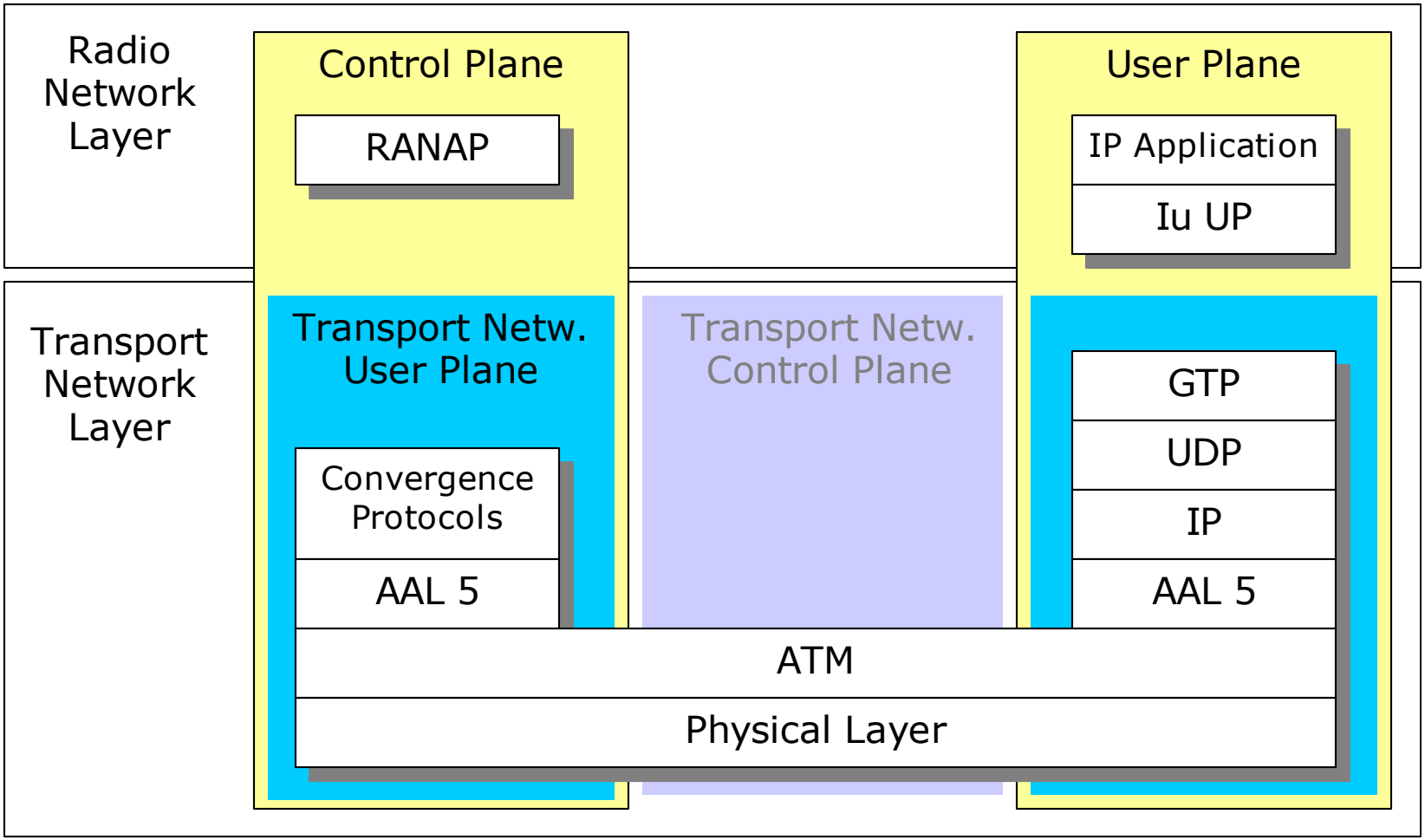
Protocol structure at Iur interface



Protocol structure at Iu CS interface



Protocol structure at Iu PS interface



Application protocols in UTRAN

Iub interface (between RNC and base station)

NBAP (Node B Application Part)

Iur interface (between Serving RNC and Drift RNC)

RNSAP (Radio Network Subsystem Application Part)

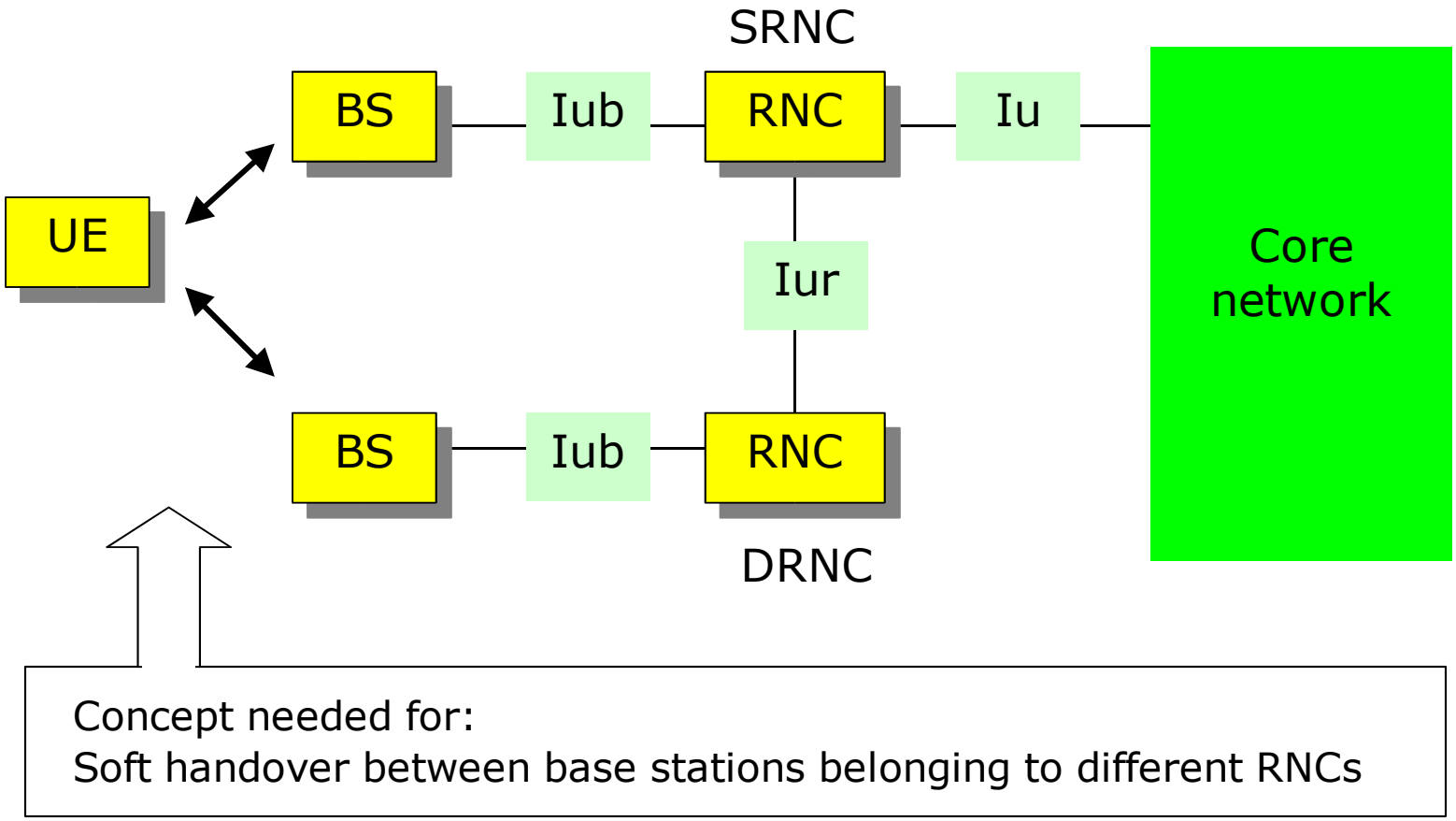
- Link management for inter-RNC soft handover

Iu interface (between RNC and core network)

RANAP (Radio Access Network Application Part)

- Radio Access Bearer (RAB) management
- SRNS Relocation
- Transfer of higher-level signalling messages

Serving RNC and Drift RNC in UTRAN



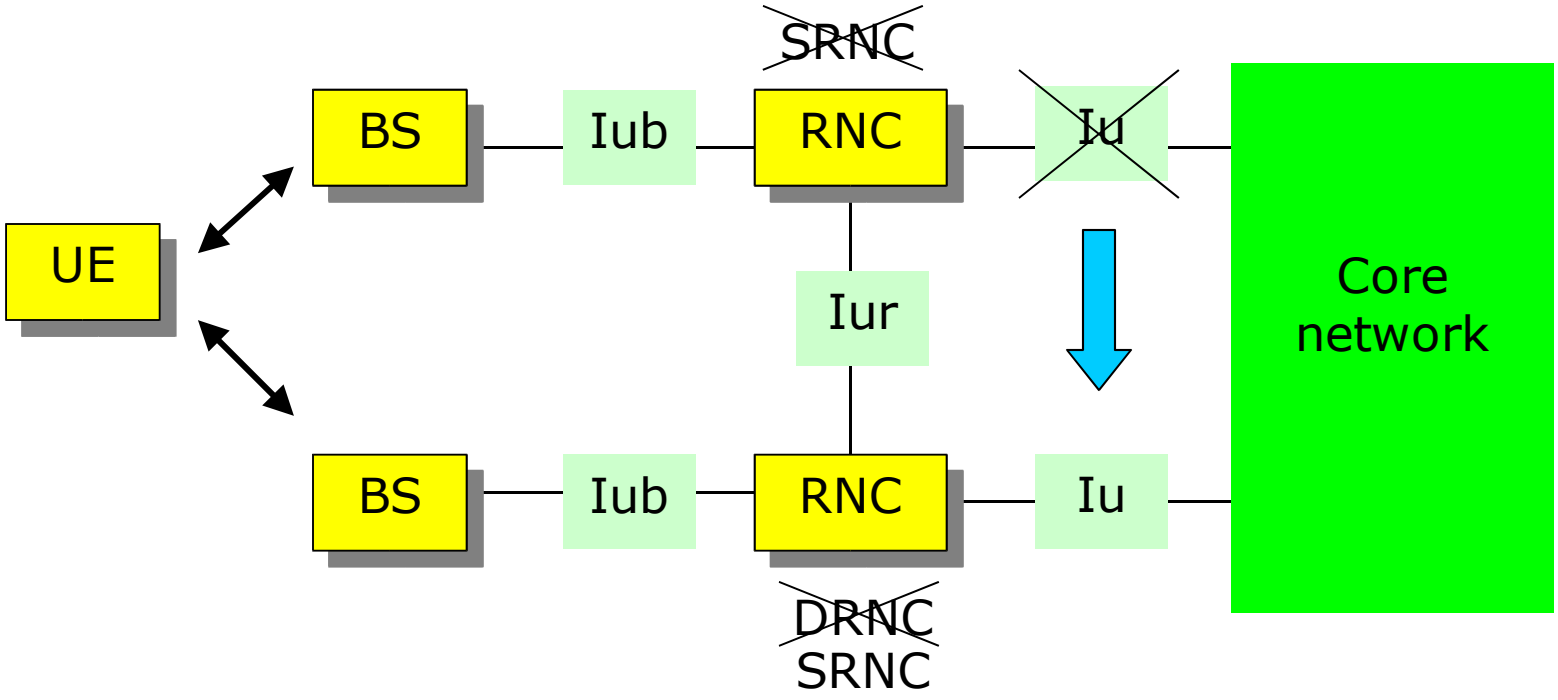
Serving RNS (SRNS) Relocation

RNS = Radio Network Sub-system =
RNC + all base stations controlled by this RNC

SRNS Relocation means that the Serving RNC functionality is transferred from one RNC (the "old" SRNC) to another (the "new" SRNC, previously a DRNC) without changing the radio resources and without interrupting the user data flow.

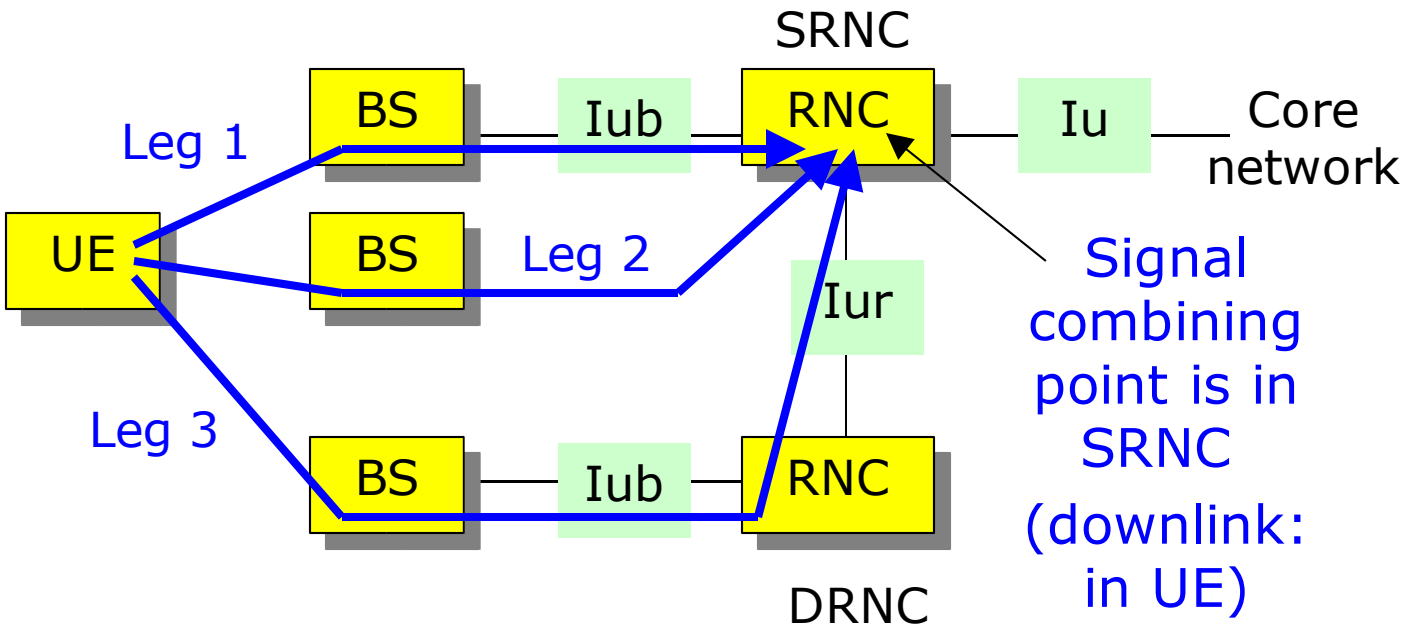
RANAP provides the signalling facilities over the two Iu interfaces involved (Iu interfaces to "old" and "new" SNRC) for performing SRNC Relocation in a co-ordinated manner.

SRNS Relocation (cont.)



SRNC provides: 1) connection to core network
2) macrodiversity combining point

Soft handover concept

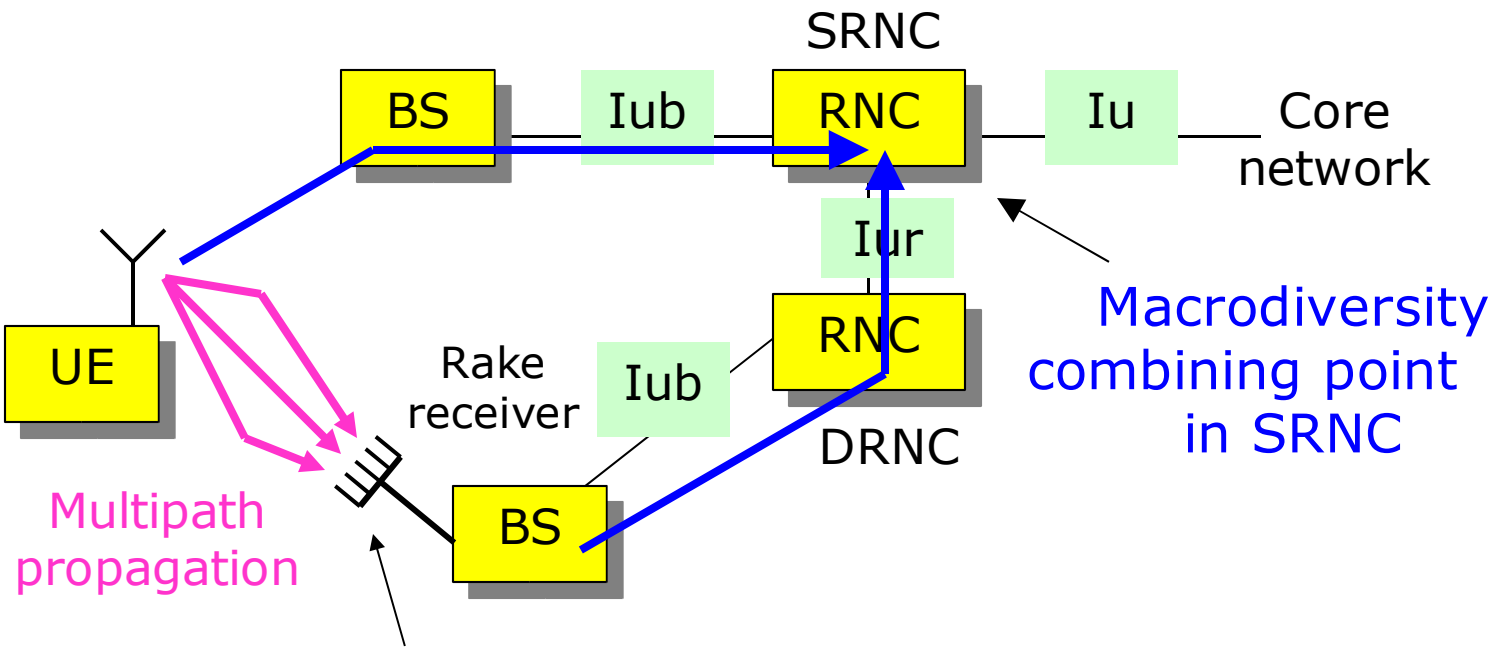


Legs 1 and 2: Iur interface is not needed

Leg 3 is added: Iur interface is needed!

Micro- / macrodiversity combining

(uplink)



Micro- / macrodiversity combining

(uplink)

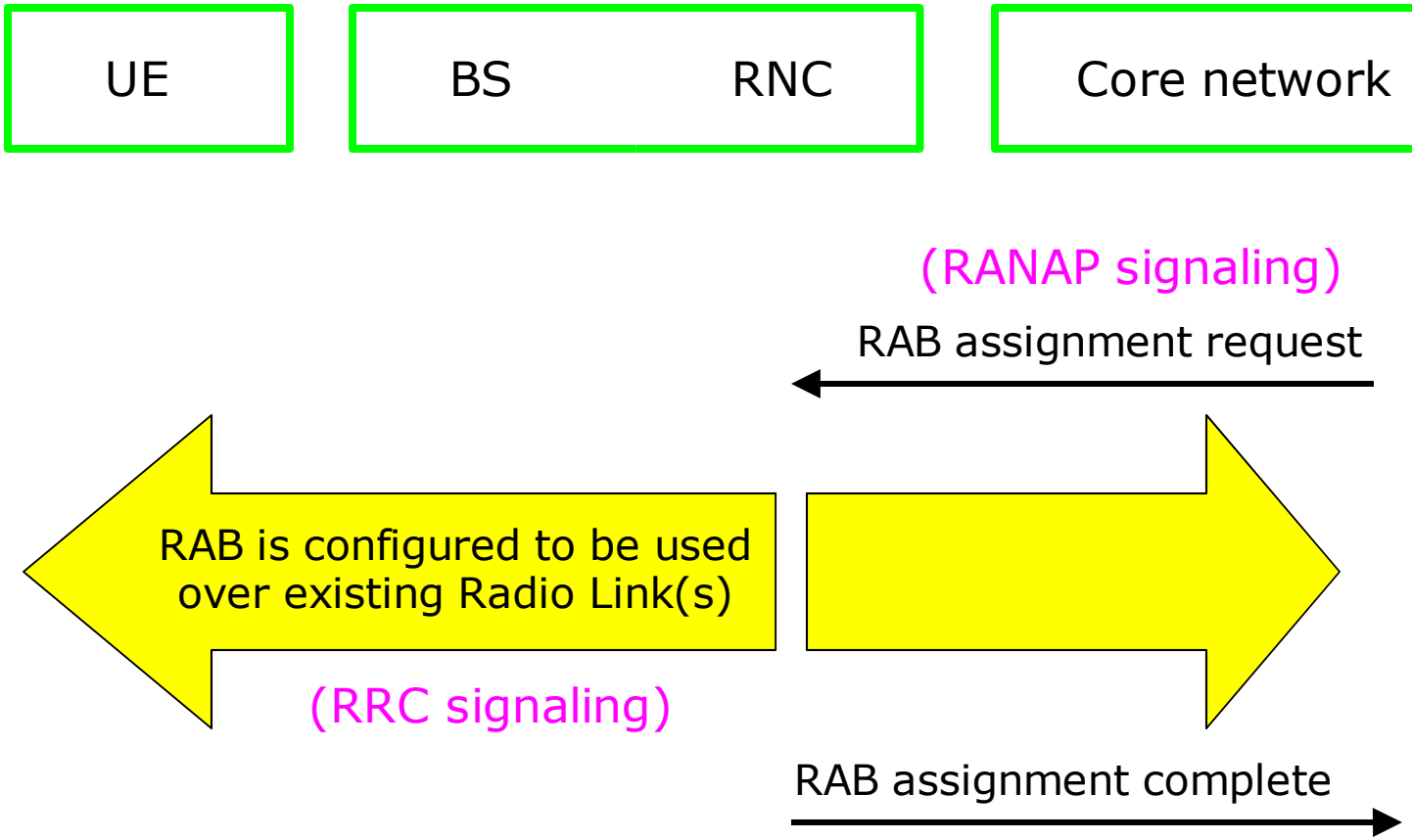
Microdiversity combining: multipath signal components are processed in Rake "fingers" and combined using MRC (Maximum Ratio Combining)

Macrodiversity combining: the bit sequences received via different legs (and with different bit error positions) are combined at the SRNC (usually: selection combining = the best quality bit sequence is selected).

Hard handover: slow (a lot of signalling)

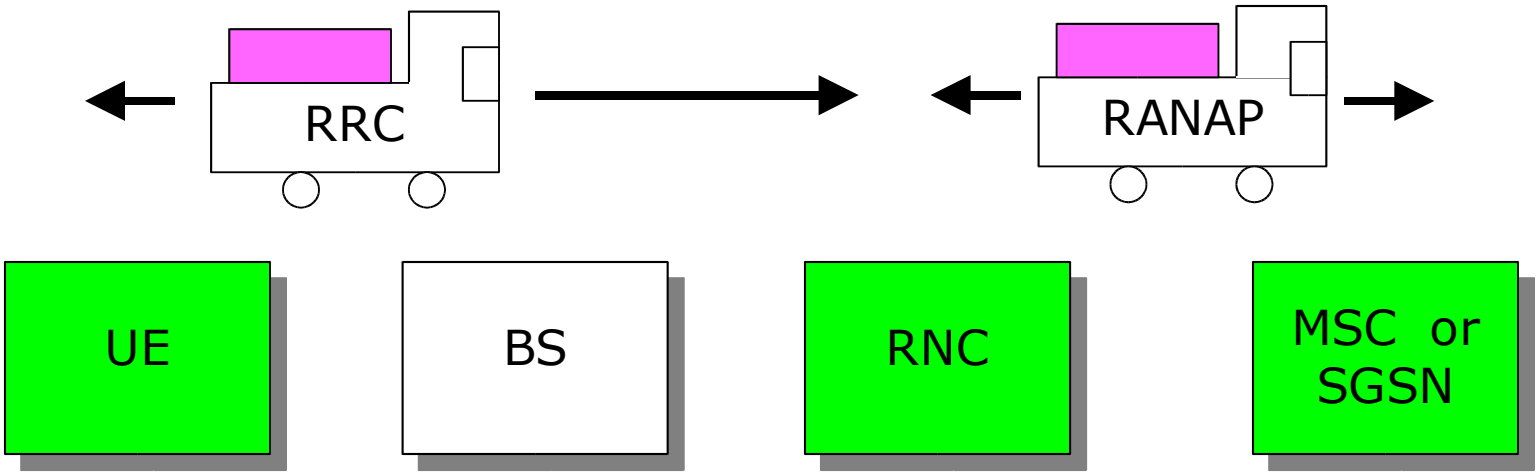
Soft handover: fast selection in SRNC

Radio Access Bearer (RAB) establishment

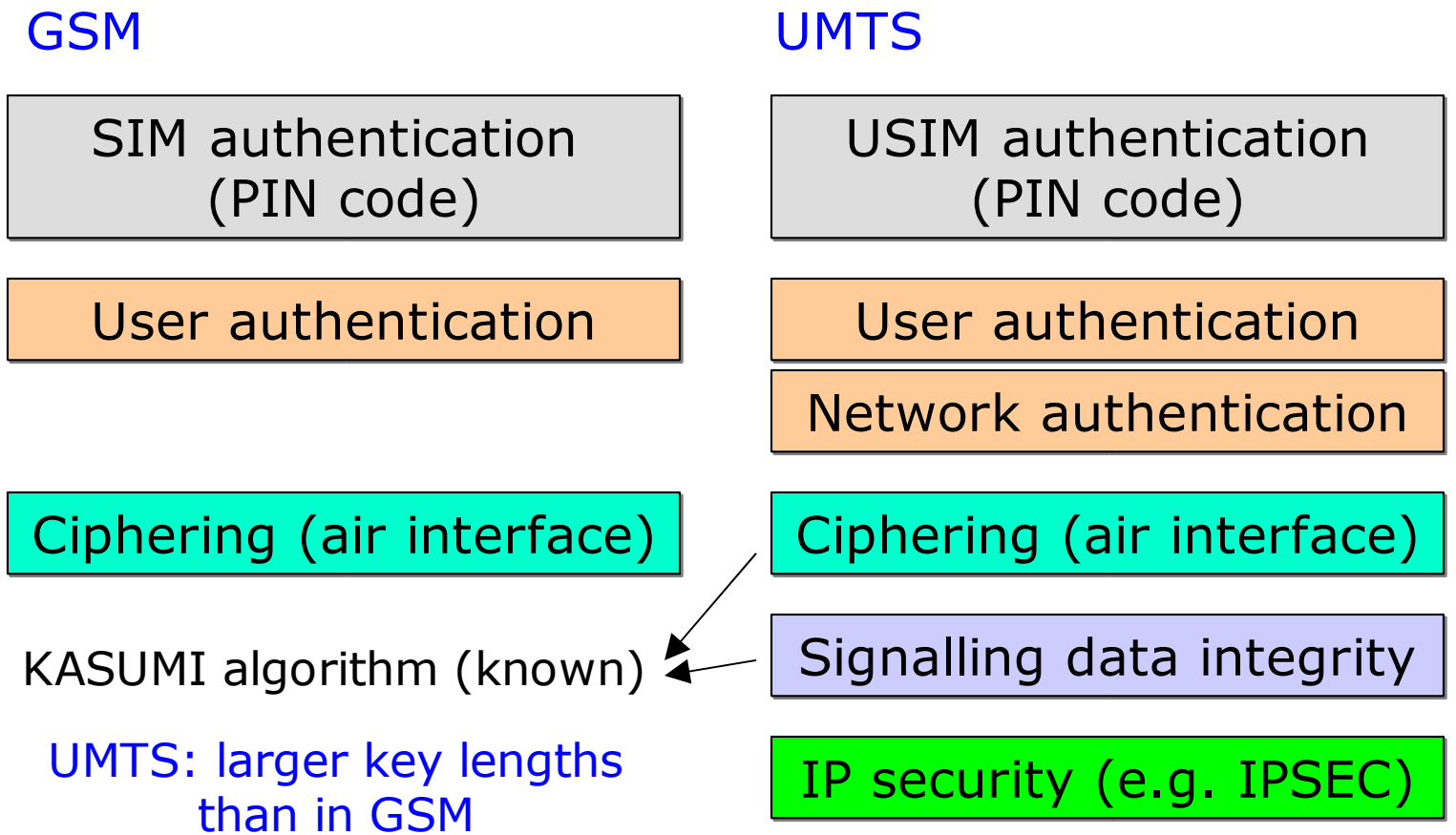


Signalling between UE and core network

NAS signalling messages (NAS = Non Access Stratum = “not related to UTRAN”) are sent transparently through UTRAN in the payload of RRC/RANAP protocol messages



Security in UMTS



Security in digital networks: terminology

Authentication:

- SIM authentication (PIN code)
- user authentication (GSM, UMTS, DECT, TETRA)
- network authentication (UMTS, TETRA)

Integrity:

- signalling data integrity (UMTS)

Confidentiality (≈ privacy):

- ciphering of signals over radio interface
- hiding of user identifiers over radio interface
- end-to-end encryption (offered by service provider)

Authentication

Authentication: Procedure of verifying the authenticity of an entity (user, terminal, network, network element). In other words, is the entity the one it claims to be?

- SIM authentication is local (network is not involved)
- In GSM, only user is authenticated
- In UMTS, both user and network are authenticated
- User/network is authenticated at the beginning of each user-network transaction (e.g. location updating or connection set-up) and always before ciphering starts.

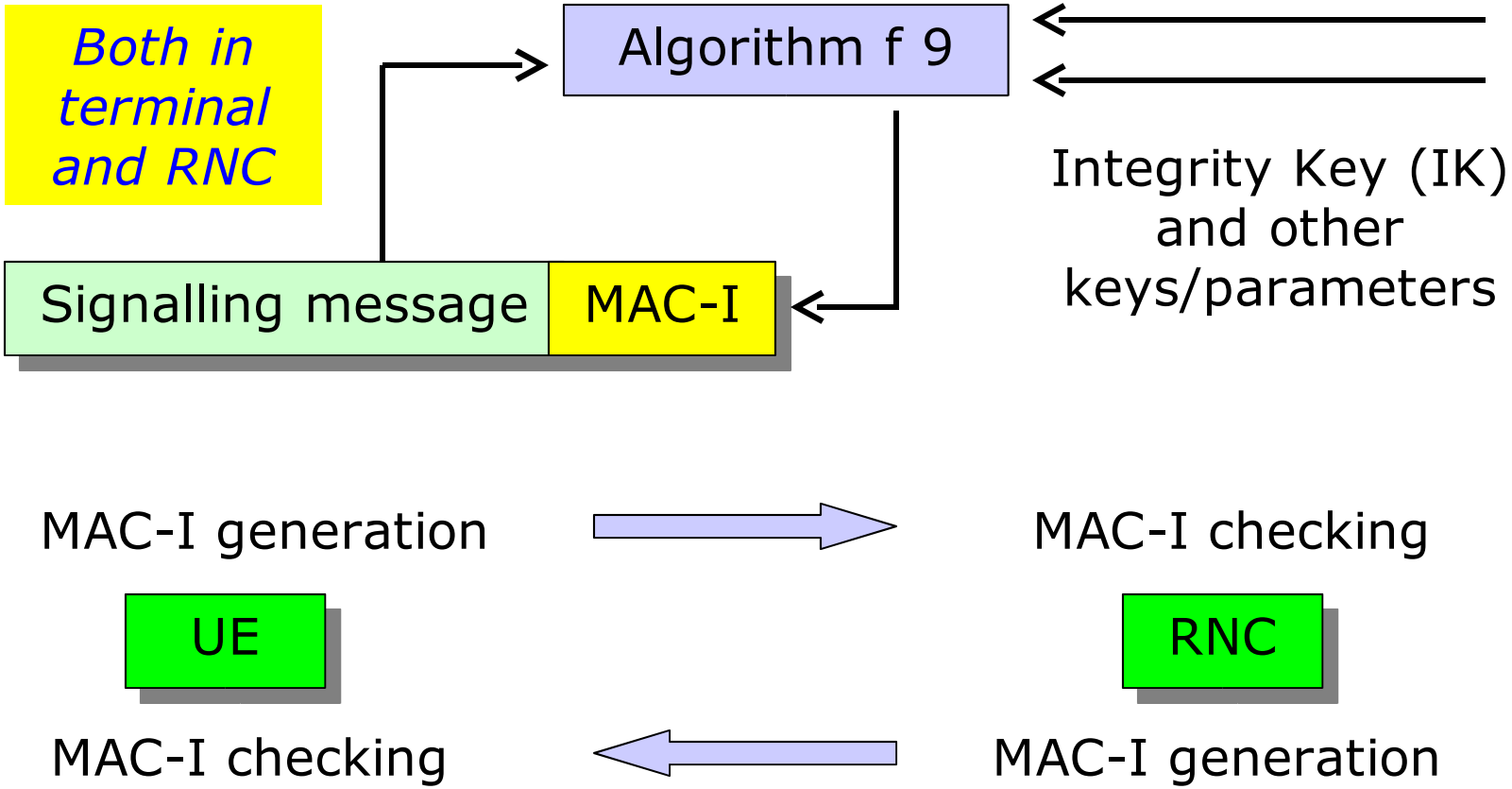
See Security in GSM for more details

Integrity

Data integrity: The property that data has not been altered in an unauthorised manner.

- "Man-in-the-middle" security attack, e.g. false BS
- Data integrity checking is not done in GSM
- In UMTS, signalling messages are appended with a 32 bit security field (MAC-I) at the terminal or RNC before transmission and checked at the receiving end
- In UMTS, also volume of user data (not the user data itself) is integrity protected

Signalling integrity protection in UMTS



Confidentiality

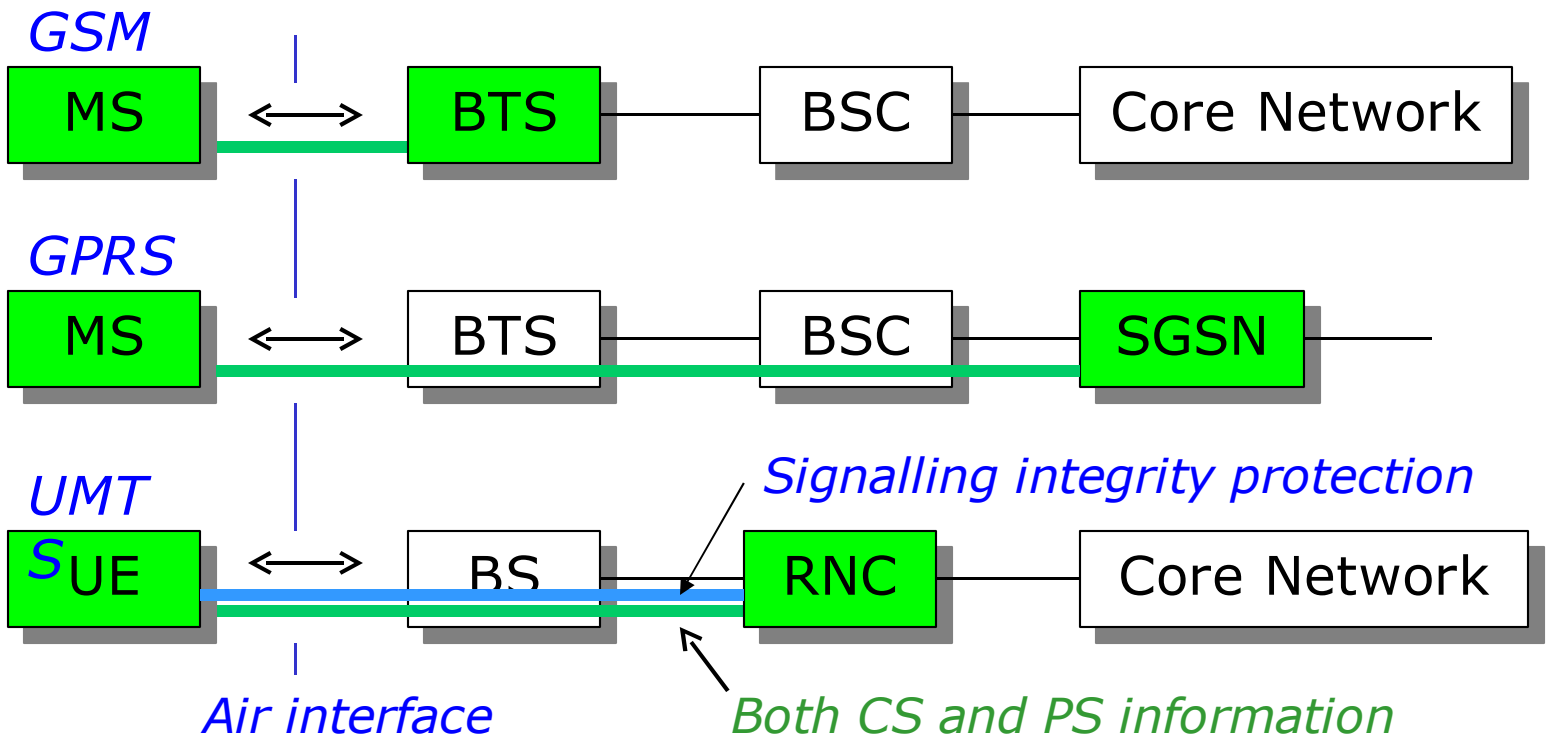
Confidentiality: The property that information is not made available to unauthorised individuals, entities or processes.

Example 1: Ciphering (encryption) over the air interface

Example 2: Preventing unencrypted transmission of user ID information such as IMSI number over the air interface

=> Temporary Mobile Subscriber Identity (TMSI) is generated (at the end of each MM or CM transaction) and is used at the beginning of the next transaction instead of IMSI.

Example 1: ciphering (encryption)

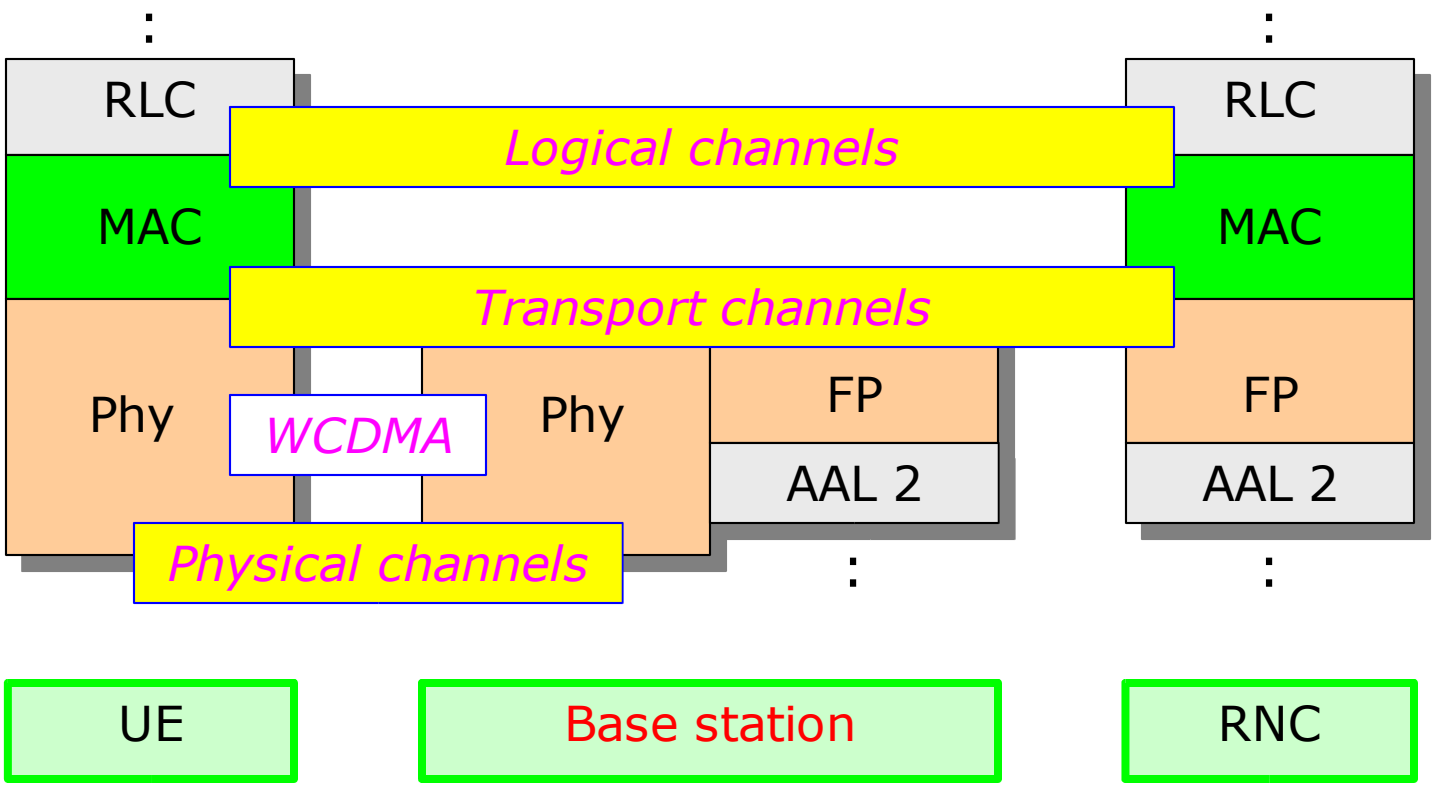


WCDMA Technology

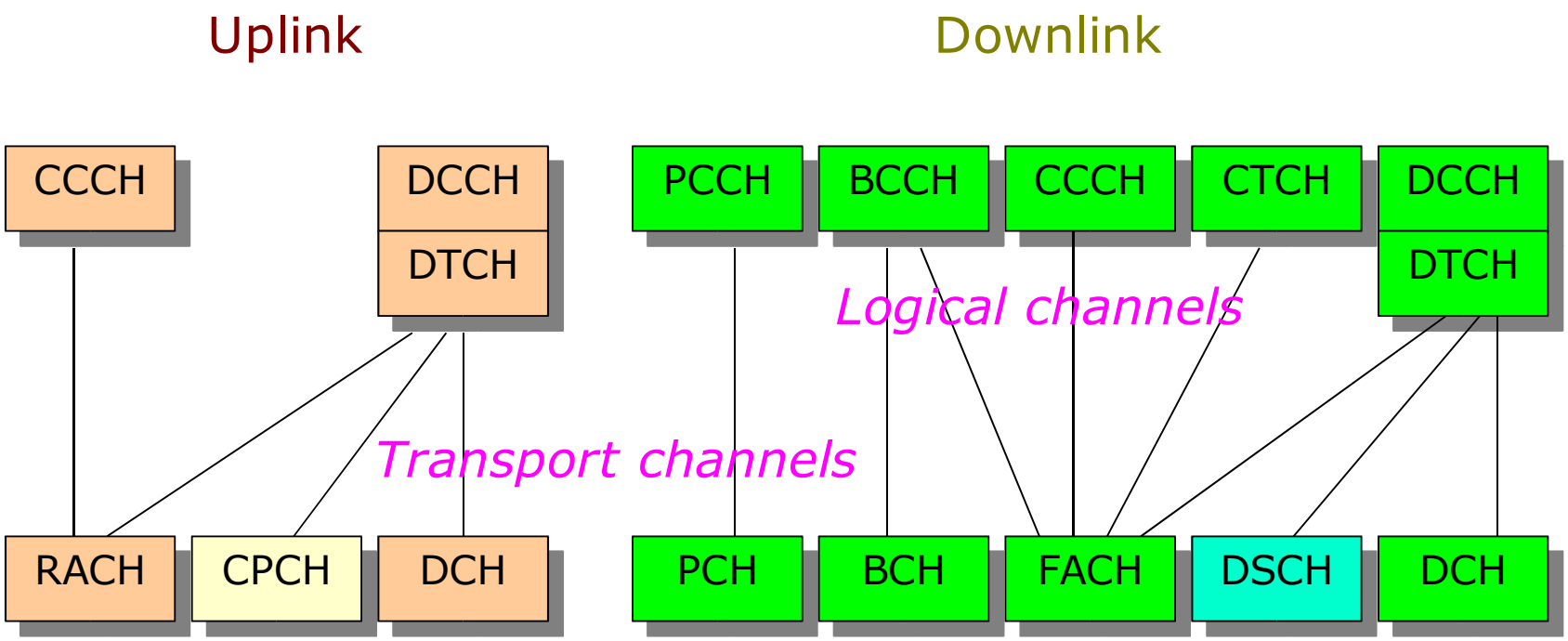
… just some basic concepts

(not required knowledge in this course)

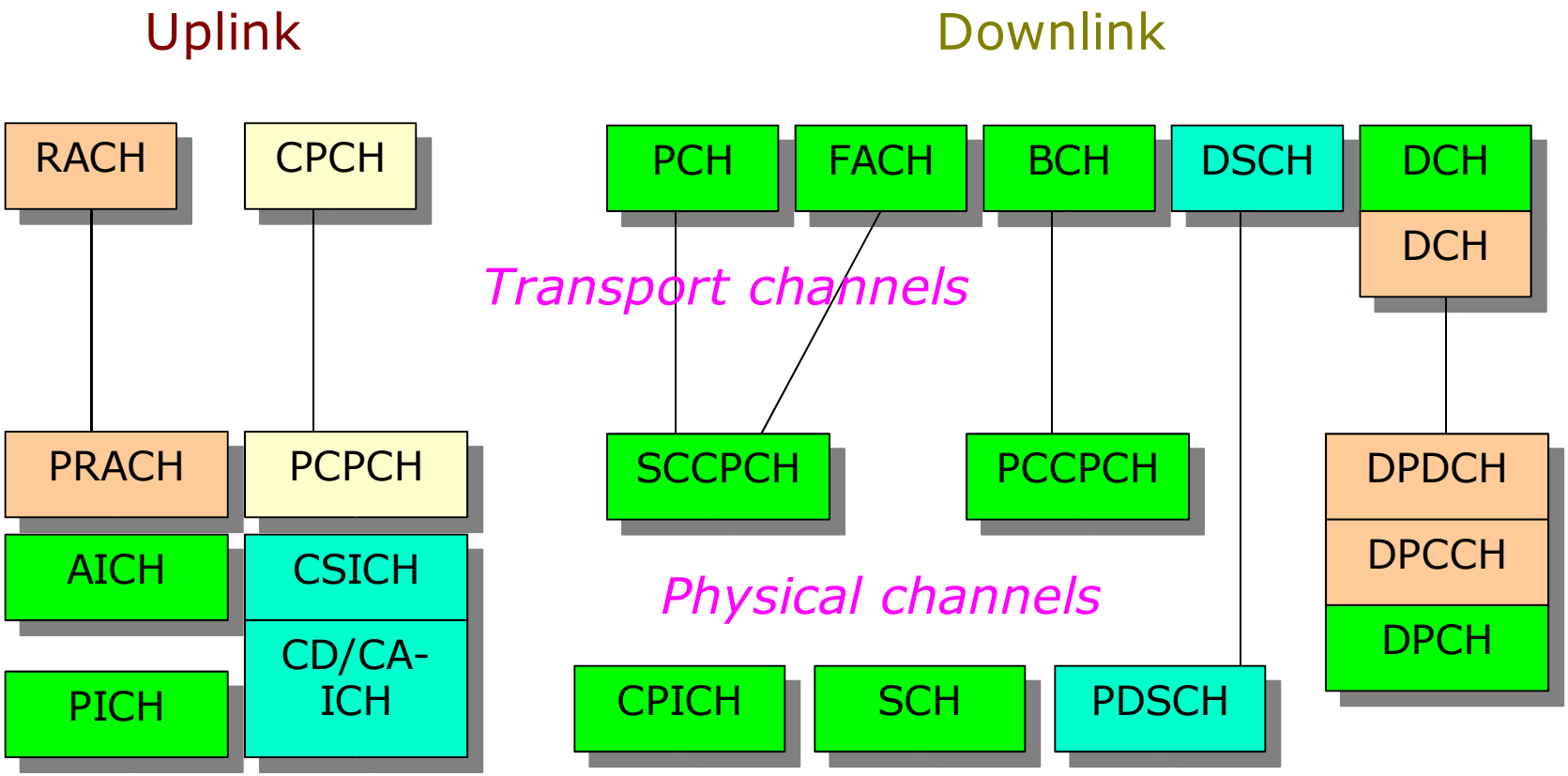
Logical / Transport / Physical channels



Logical / Transport channel mapping



Transport / Physical channel mapping



Physical channels in WCDMA

Bit sequences from different physical channels are

- multiplied with a channelization code (spreading)
- multiplied with a scrambling code (scrambling)
- multiplexed in code domain
- modulated using QPSK.

Downlink channels: conventional QPSK modulation

DPCH = Dedicated physical channel

Uplink channels: Dual-channel QPSK moduation

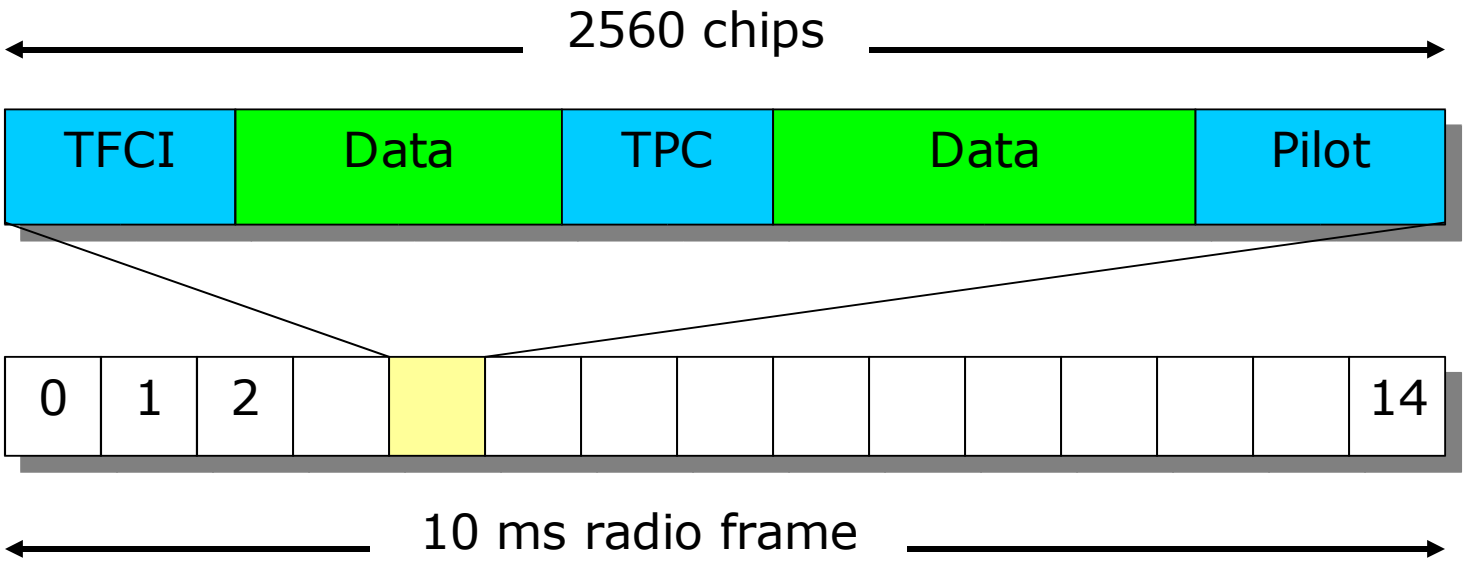
DPDCH = Dedicated physical data channel

DPCCH = Dedicated physical control channel

DPCH structure in downlink

(DPCH = Dedicated Physical Channel)

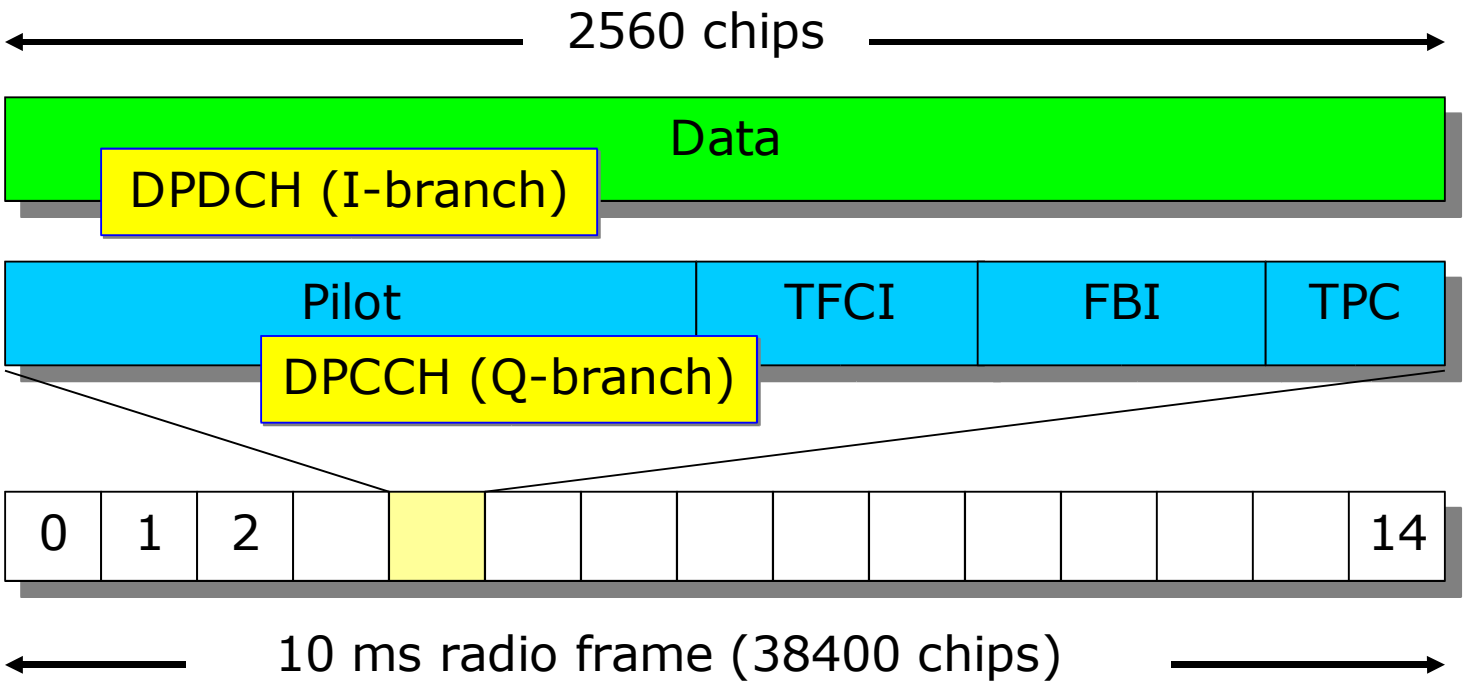
QPSK modulation,
time multiplexed data and control information:



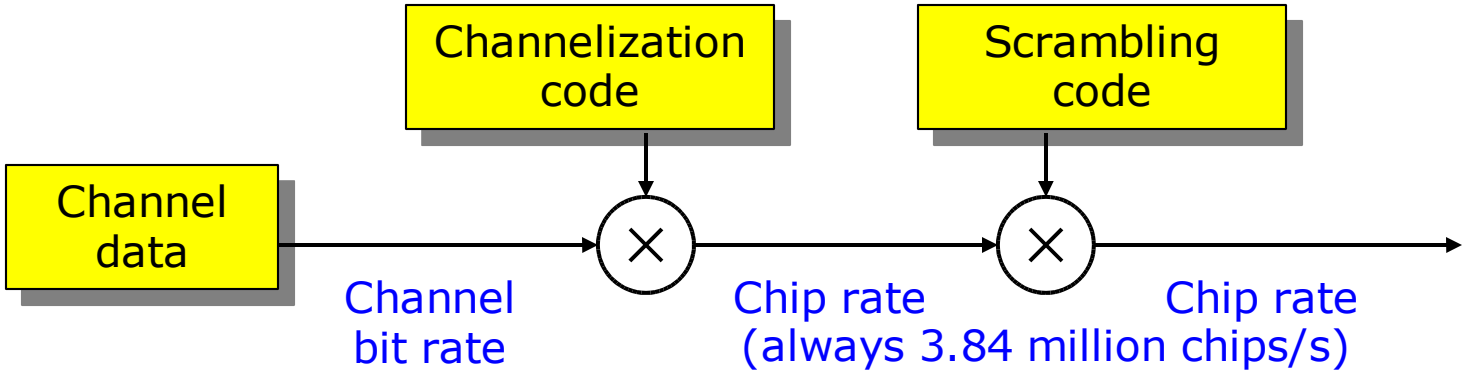
DPDCH / DPCCH structure in uplink

(Dedicated Physical Data/Control Channel)

Dual-channel QPSK modulation:



Spreading in WCDMA



Usage of code	Uplink	Downlink
Channelization code		User separation
Scrambling code	User separation	Cell separation

Spreading in WCDMA

Chip rate after spreading = 3.84 Mchips/s

Spreading factor (SF) is important in WCDMA

Chip rate = SF x channel bit rate

Uplink: DPCCH SF = 256, DPDCH SF = 4 - 256

Downlink: DPCH SF = 4 - 256 (512)

One bit consists of 4 chips

One bit consists of 256 chips

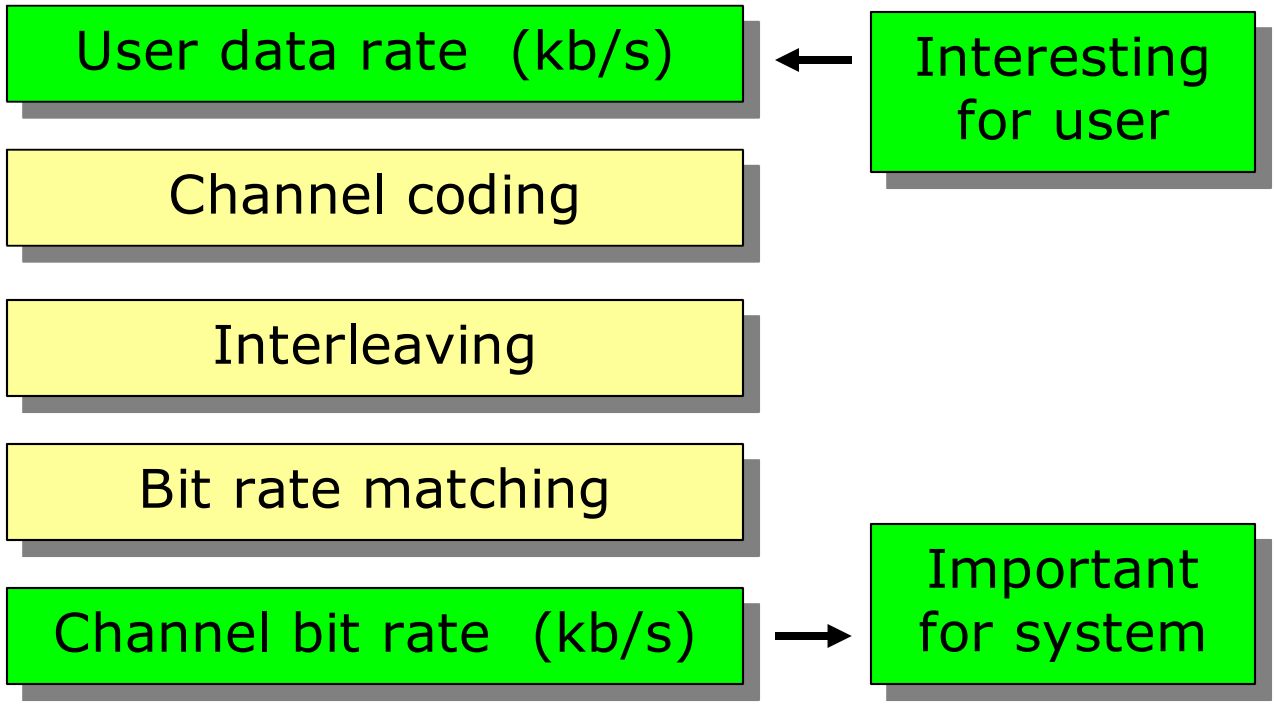
Uplink DPDCH bit rates

SF	Channel bit rate (kb/s)	User data rate (kb/s)
256	15	approx. 7.5
128	30	approx. 15
64	60	approx. 30
32	120	approx. 60
16	240	approx. 120
8	480	approx. 240
4	960	approx. 480

Downlink DPDCH bit rates

SF	Channel bit rate (kb/s)	User data rate (kb/s)
512	15	approx. 1-3
256	30	approx. 6-12
128	60	approx. 20-24
64	120	approx. 45
32	240	approx. 105
16	480	approx. 215
8	960	approx. 456
4	1920	approx. 936

User data rate vs. channel bit rate

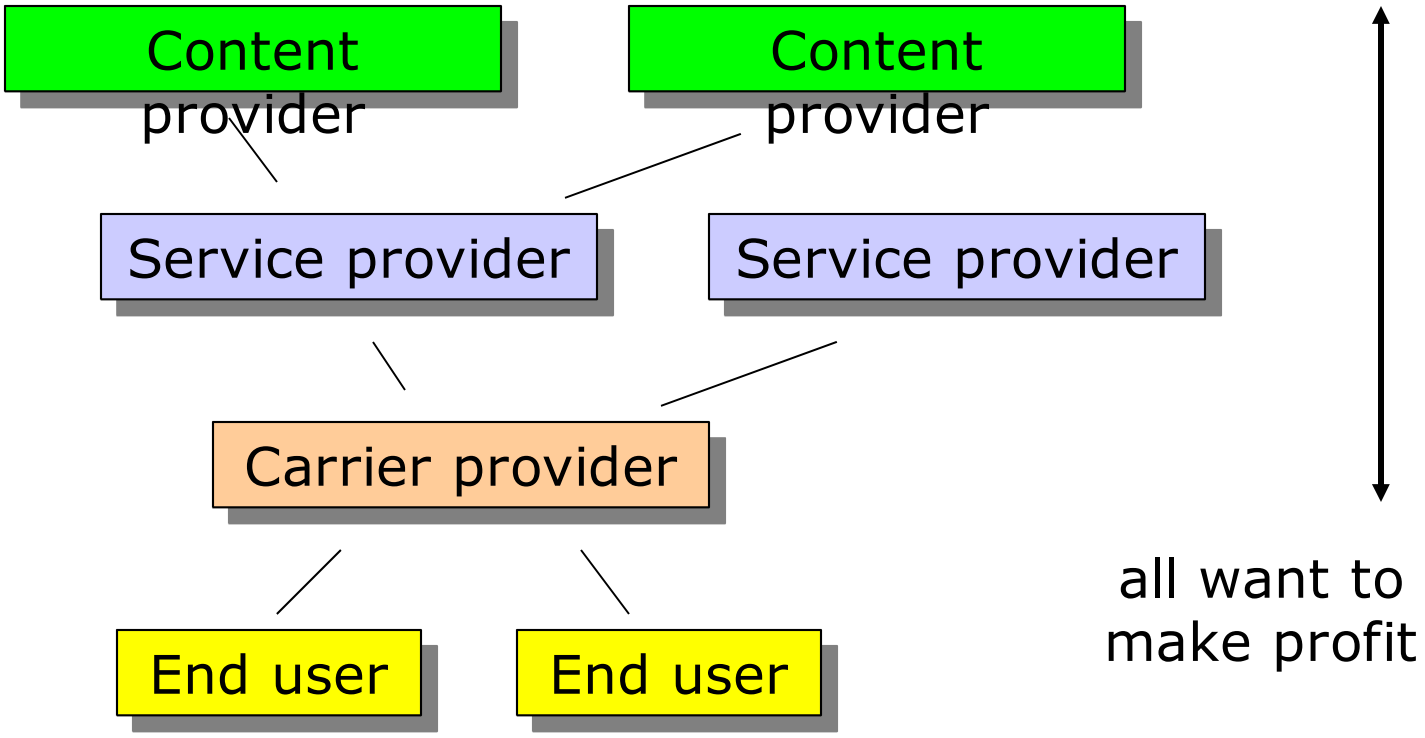


Services for 3G (and partly 2G)

… just some basic concepts

(not required knowledge in this course)

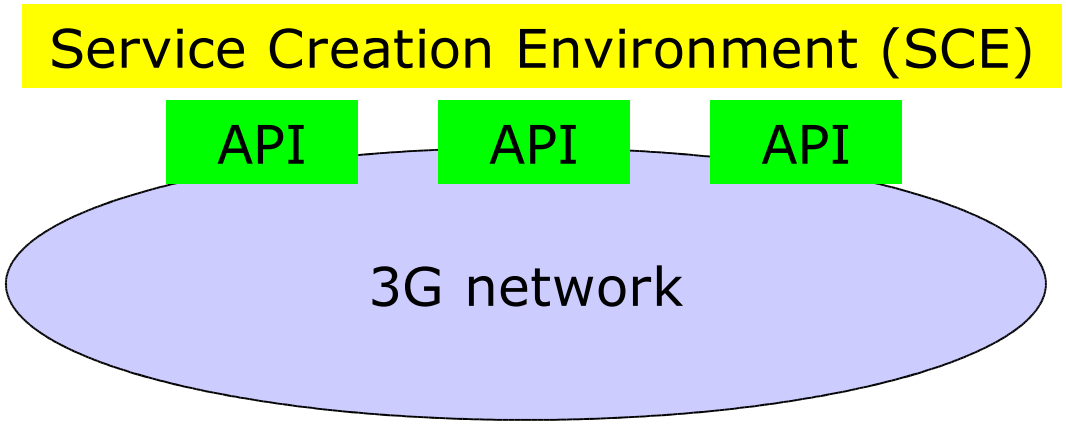
New service concept



OSA (Open Services Architecture/Access)

OSA is being standardised, so that services provided by different service/content providers can be created and seamlessly integrated into the 3G network (this is the meaning of "open" architecture)

OSA means in practice:



API = Application Programming Interface (Standardised)

CAMEL (2G & 3G)

CAMEL (Customised Applications for Mobile network Enhanced Logic) is a set of "IN" type functions and procedures that make operator-specific IN services available to subscribers who roam outside their home network.

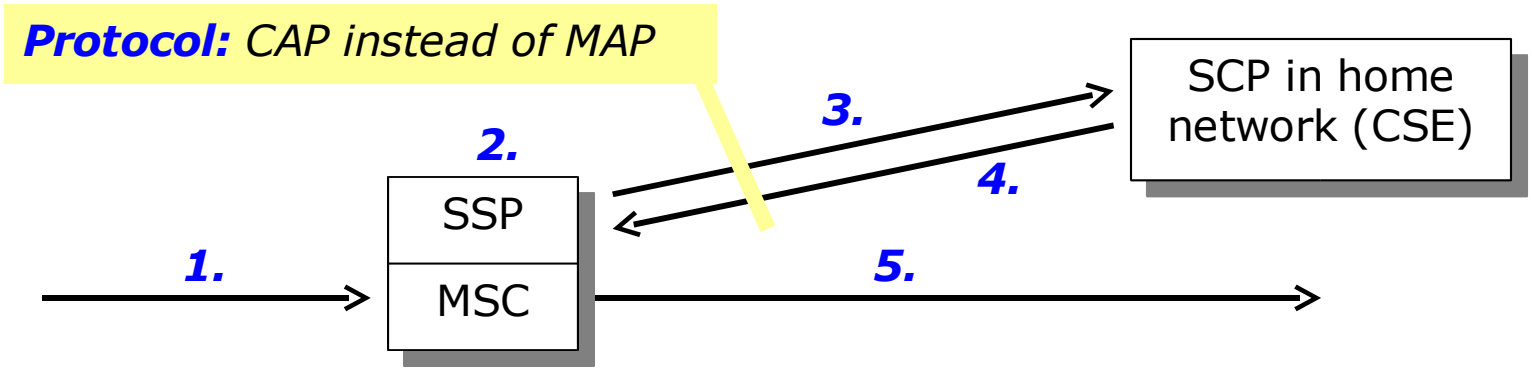
CAMEL = IN technology + global mobility

CAMEL Service Environment (CSE) is a logical entity in the subscriber's home network which processes IN related procedures

CSE ≈ SCP in home network

CAMEL Phase 1

Circuit switched call-related IN procedures



1. *Call control proceeds up to MSC*

2. *Trigger activated in basic call state model at SSP*

3. *SSP requests information from CSE*

4. *CSE provides information*

5. *Call control continues*

Typical triggers:

Calling number
Called number
Cell ID

CAMEL Phase 2

Non-call-related procedures possible

1. *Call control proceeds as normal*
2. *Call control is interrupted*
   (e.g. for announcement)
3. *Call control resumes*

Typical application:

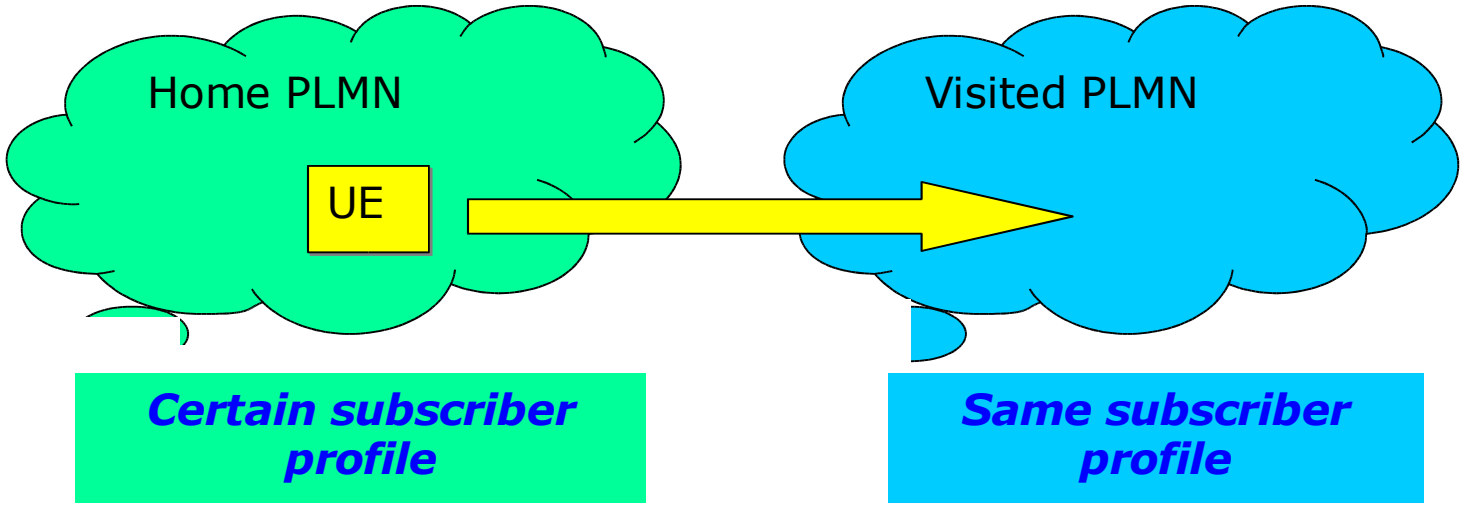
In prepaid service: announcement "your prepaid account is approaching zero"

CAMEL Phase 3

IN functionality is extended to include packet switched sessions...

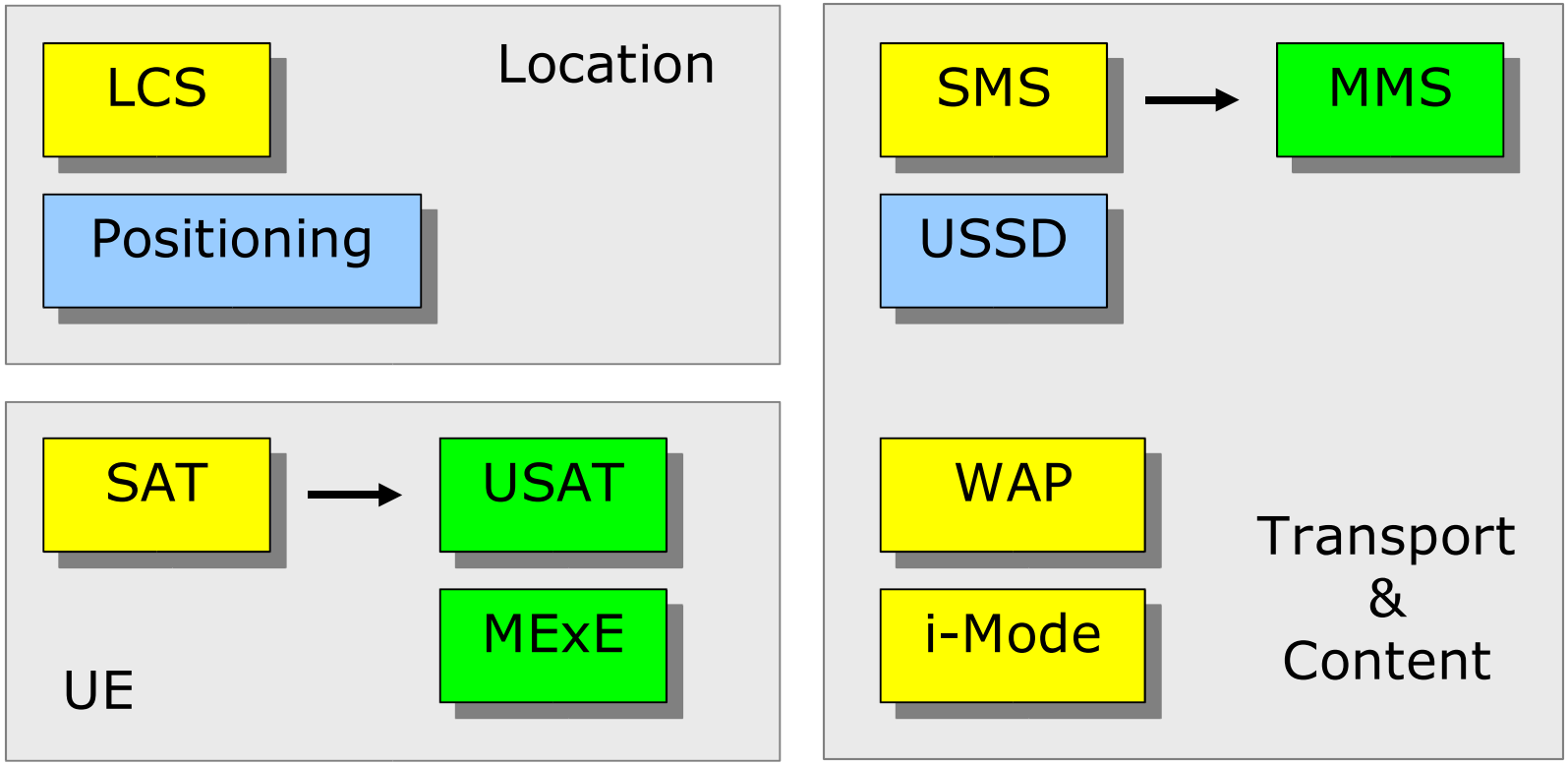
Virtual Home Environment (VHE)

Same subscriber profile & charging/numbering information can be utilised in any UMTS network



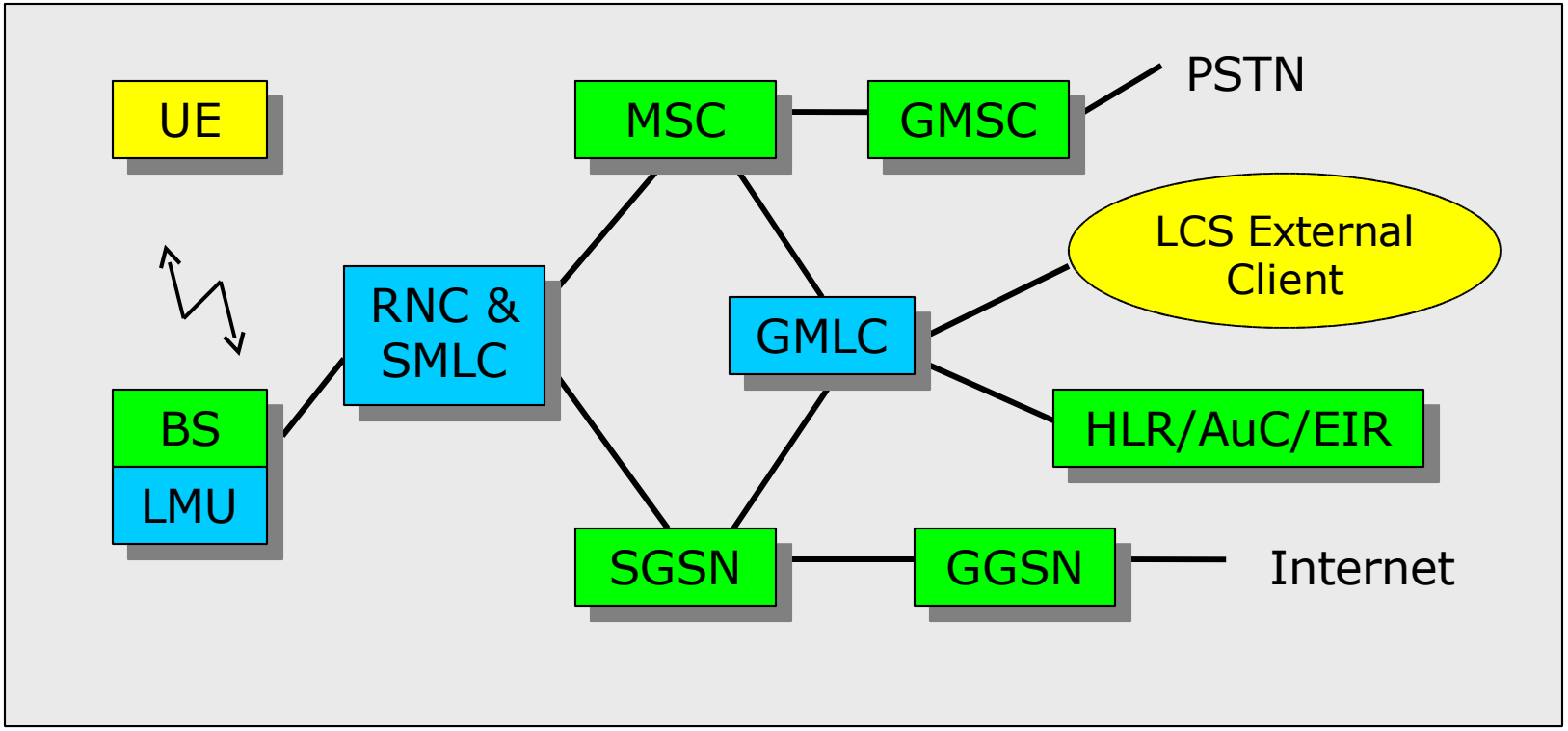
Supporting technologies and services

- many are already possible in 2G
- will (at least partly) be used in 3G



Location services (LCS)

- may or may not use UE positioning techniques
- general LCS architecture in UMTS:



Location services (cont.)

GMLC = Gateway Mobile Location Center

receives service requests from external LCS clients (or UE) and manages the location information

SMLC = Serving Mobile Location Center

assists in positioning of the UE (e.g. performs calculations based on measurement results), is usually integrated with RNC

LCS client = typically any server requesting location information (to be able to provide the relevant location service to the user), may also be the UE

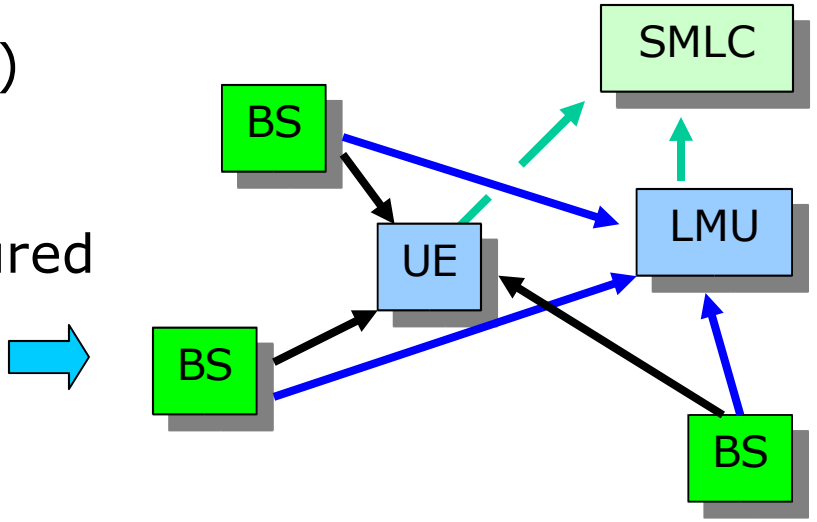
Positioning methods

Cell ID based location information

- no expensive positioning solutions required
- inexpensive (and will therefore be widely used)

E-OTD (2G), OTDOA (3G)

- differential delays measured from which the position is calculated (in SMLC)

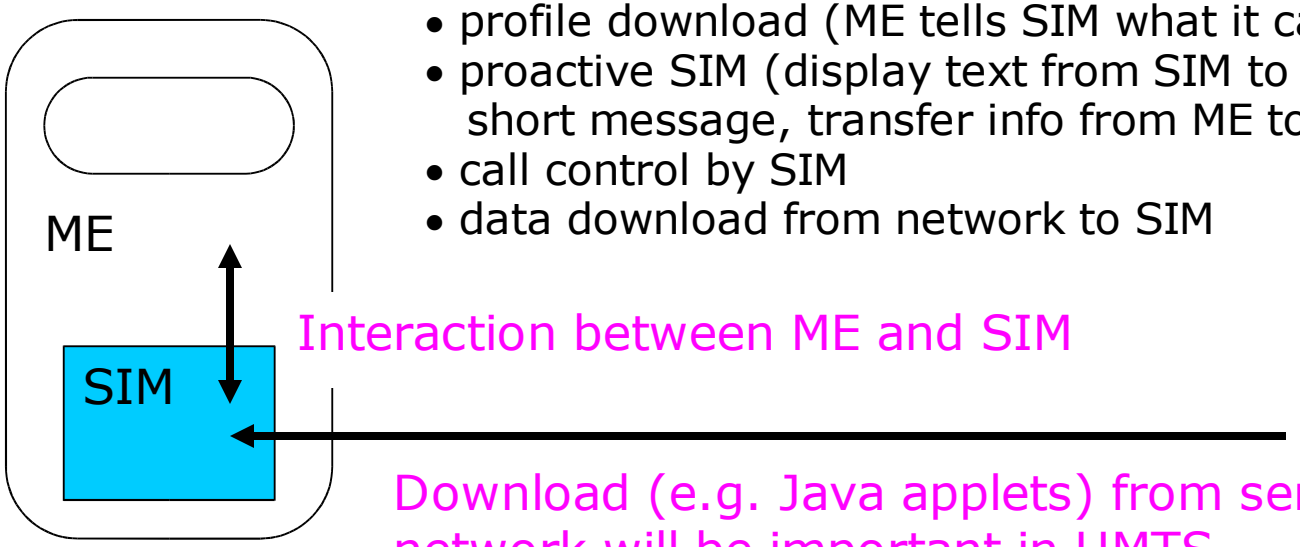


Assisted GPS

- greatest precision, GPS receiver in UE
- network must “assist” in indoor environment

SAT (= USAT in 3G)

SAT (SIM Application Toolkit) is a set of standardized functions for communication between SIM and ME



Applications (GSM 11.14):

- profile download (ME tells SIM what it can do)
- proactive SIM (display text from SIM to ME, send short message, transfer info from ME to SIM,...)
- call control by SIM
- data download from network to SIM

MExE

Mobile Execution Environment (MExE) provides standardized application execution environments for UE, defined in classmarks:

MExE Classmark 1	UE is WAP compatible (i.e. contains WAP browser)
MExE Classmark 2	UE can execute PersonalJava applications (subset of J2SE)
MExE Classmark 3	UE is J2ME compatible
:	

Standard Edition

Micro Edition

see: www.mexeforum.org

Evolution continues ...

SMS vs. USSD

SMS = Short Message Service
USSD = Unstructured Supplementary Services Data

SMS

- 160 ASCII characters (max)
- in all GSM terminals
- store-and-forward service (=> delay)
- transport of messages
- SMS transaction always initiated by terminal

very popular

USSD

- 182 ASCII characters (max)
- in all GSM terminals
- connection oriented transactions (small delay)
- transport of technical data
- terminal or application in network initiates session

not much used (yet)

MMS

MMS = Multimedia Messaging System

Offers the possibility to send messages to/from MMS capable handsets comprising a combination of

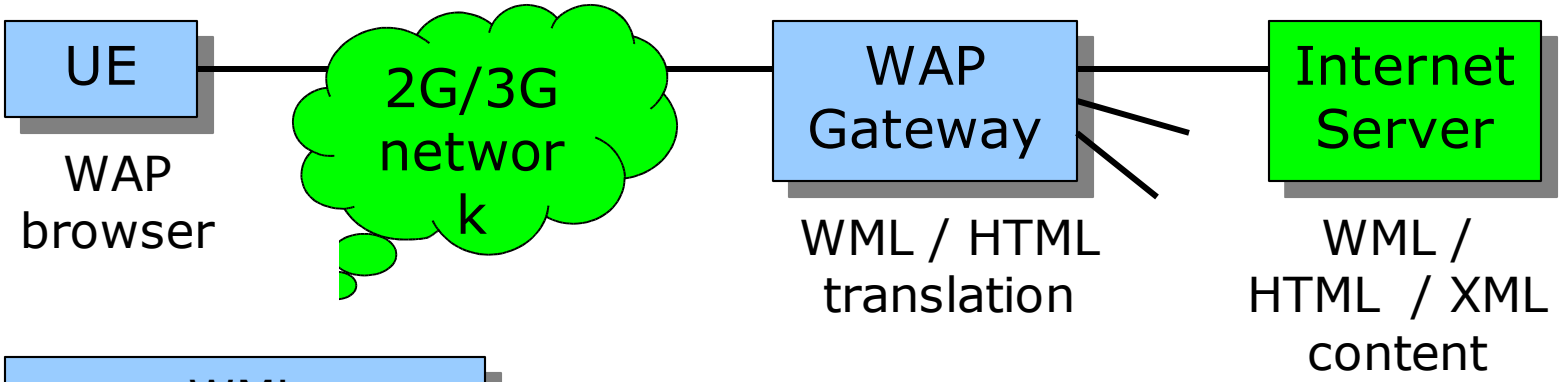
- text
- sounds
- images
- video

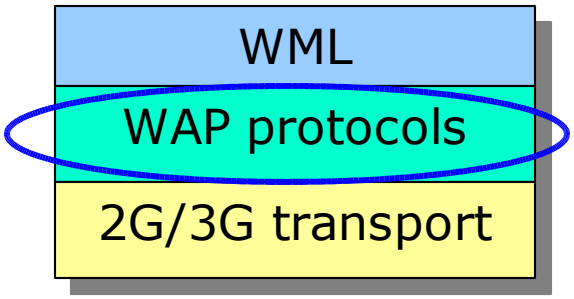
GPRS or 3G packet domain can be used for transport.

When combined with LCS information and IN (CAMEL) features, interesting new services can be implemented.

WAP 1 (Wireless Application Protocol)

Transports WML (Wireless Markup Language) information between terminal and WAP Gateway using its own set of protocols





WML is a subset of XML

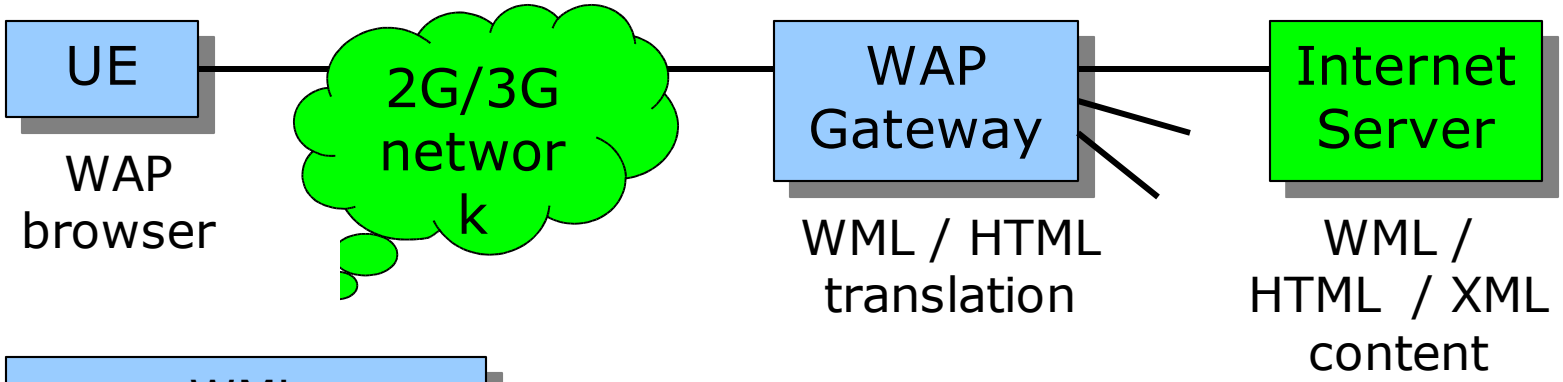
e.g. WTP (similar functionality as HTTP)

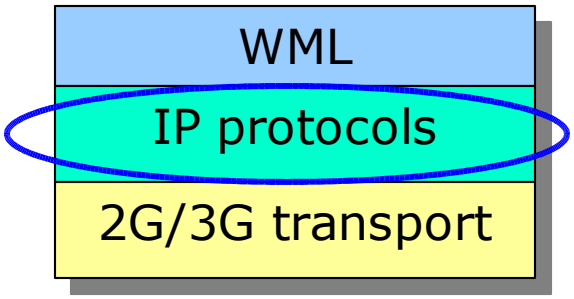
SMS, USSD, GPRS, 3G packet transport ...

WAP 2.0

http://www.wapforum.org/what/WAPWhite_Paper1.pdf

Transports WML (Wireless Markup Language) information between terminal and WAP Gateway using IP protocol stack





WML is a subset of XML

e.g. HTTP, TCP

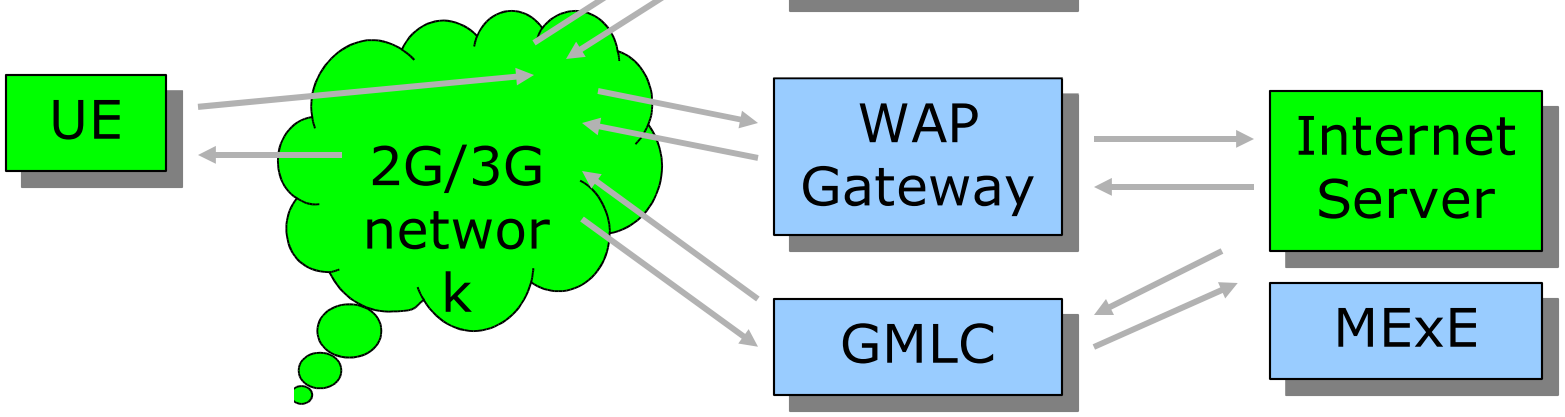
SMS, USSD, GPRS, 3G packet transport ...

Service interaction example

3G subscriber is hungry and asks for a list of nearby located restaurants (from appropriate "Internet Server").

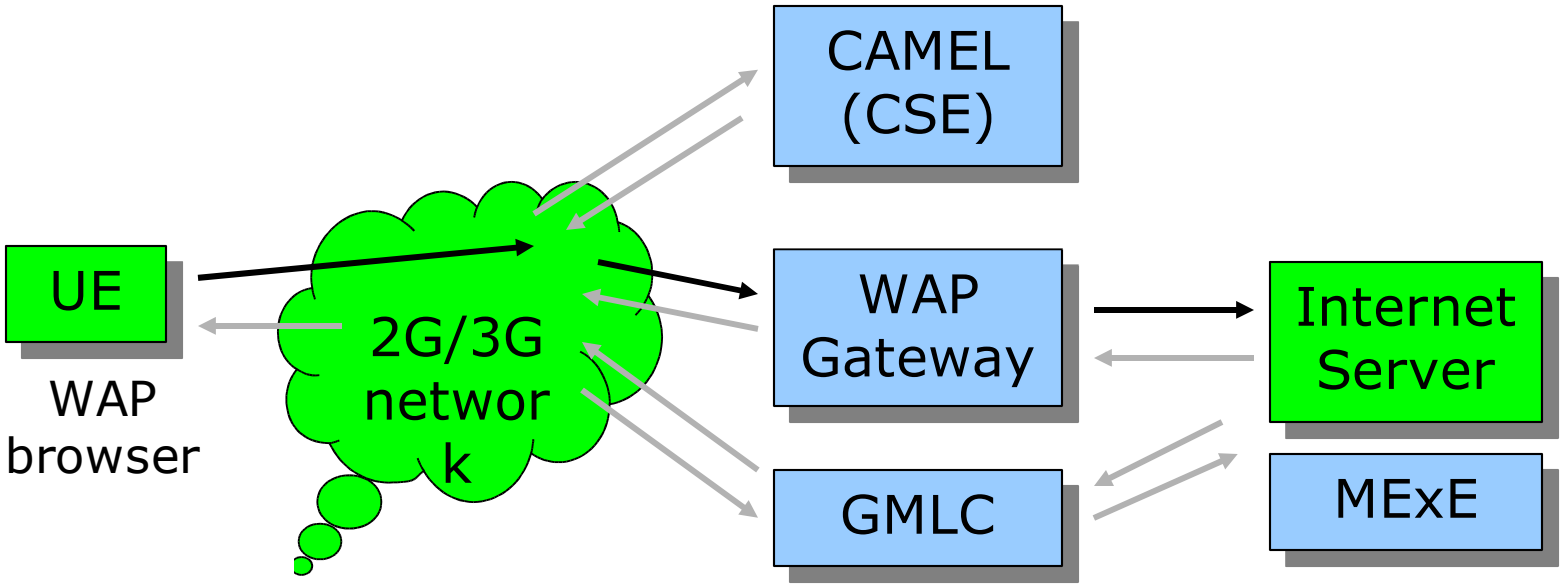
See:
Kaaranen et al:
UMTS Networks

Network scenario:



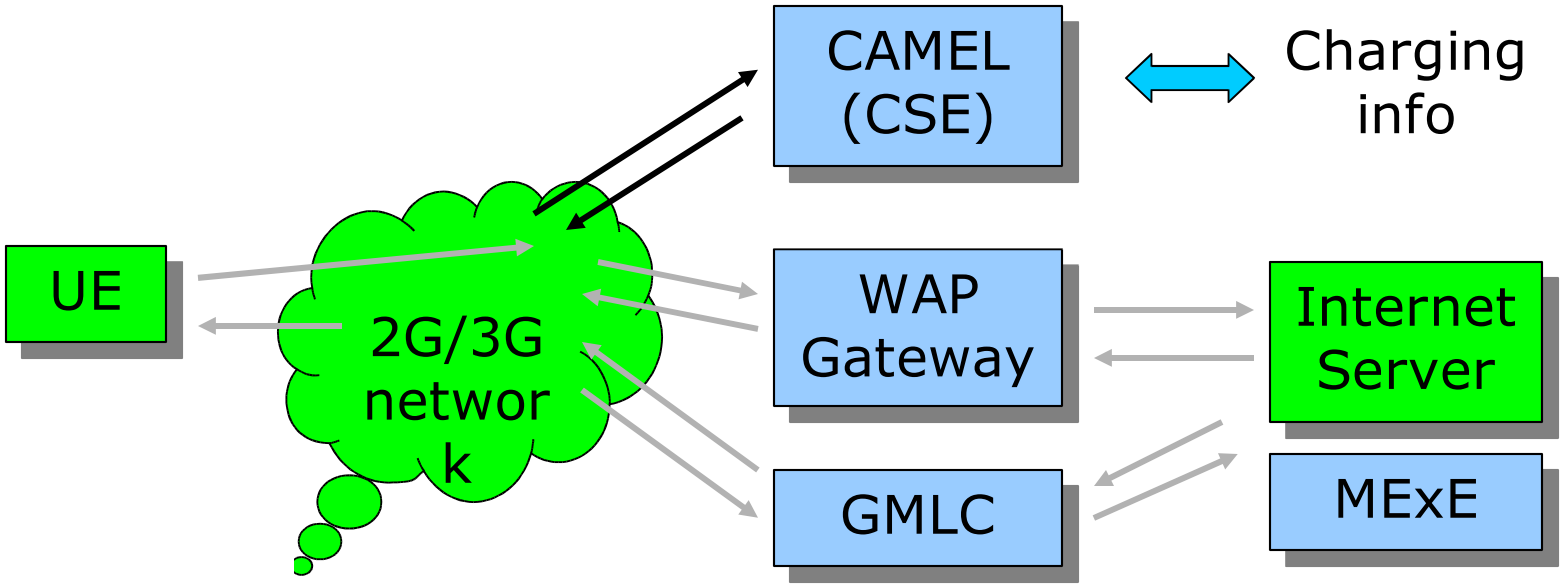
Example, Step 1

By use of his/her WAP browser in the UE, user contacts (via WAP Gateway) the "Internet Server" containing relevant information.



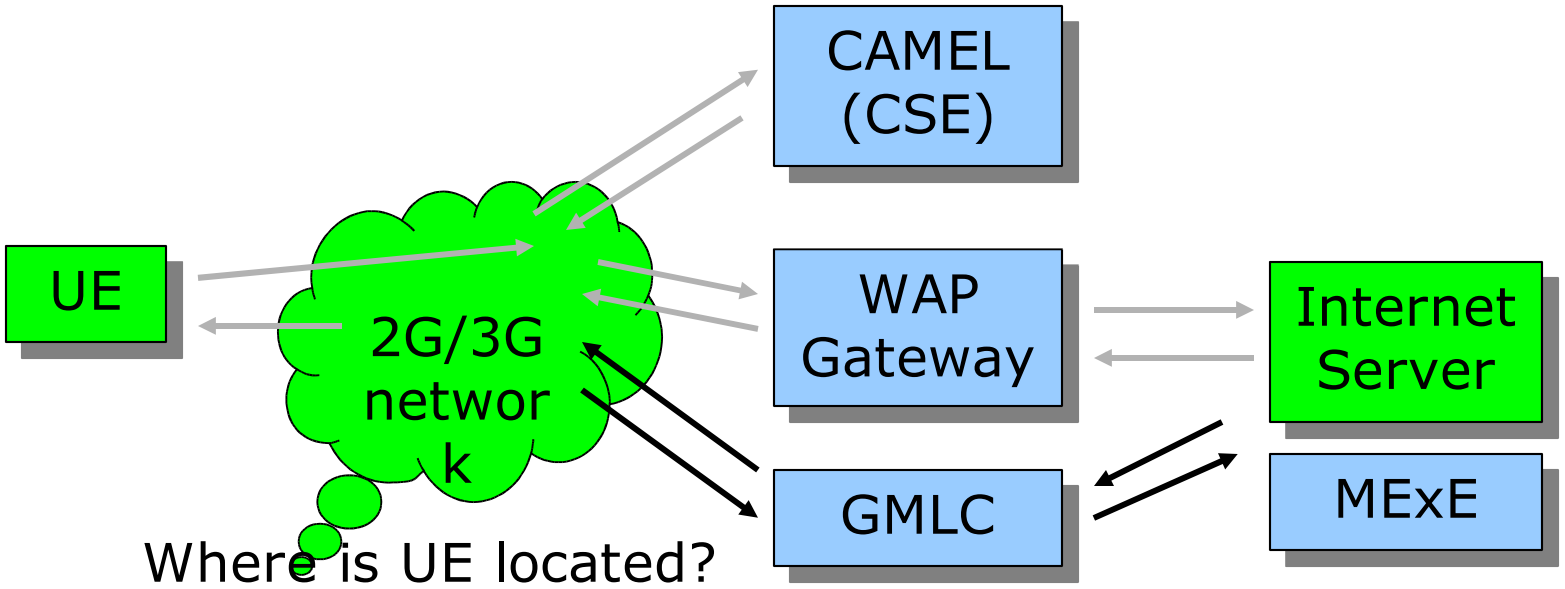
Example, Step 2

The 2G/3G network retrieves subscription information (e.g. state of “prepaid” account) from the user’s CSE (Camel Service Environment).



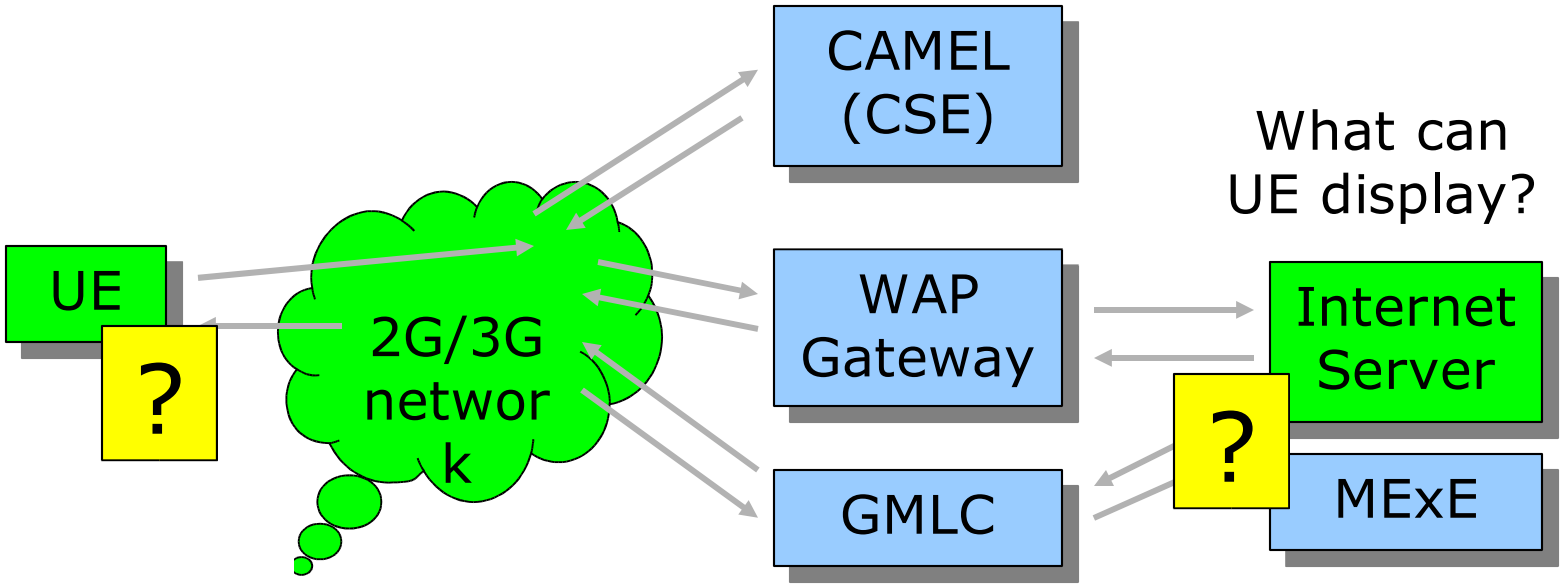
Example, Step 3

"Internet Server" acts as a "LCS client" and requests the 2G/3G network to investigate where the user is located.



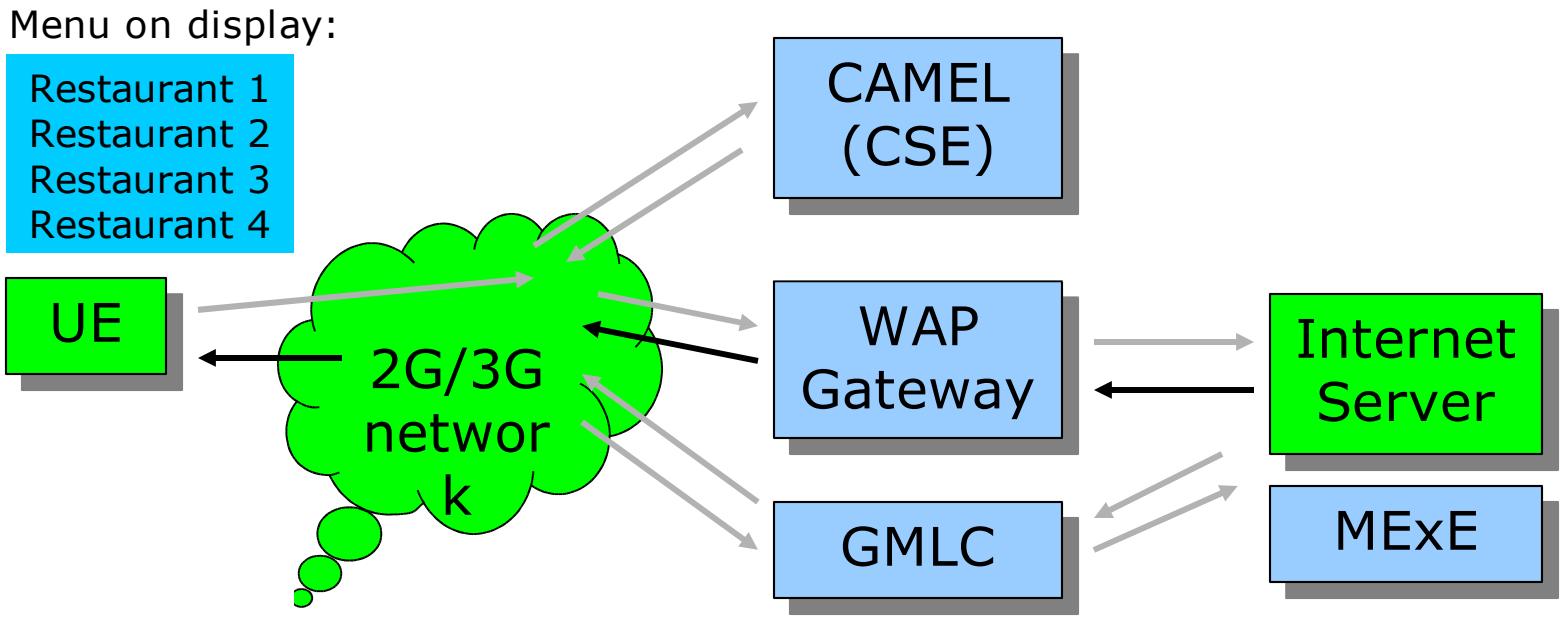
Example, Step 4

The “MExE compatible Internet Server” prepares the information according to the MExE capabilities of UE (in this case MExE Classmark 1: WAP).



Example, Step 5

Now the “local restaurants” information is downloaded to the user and displayed in the appropriate form.



Further information on 3G systems and services

Links: see slides

Books:

Kaaranen et al., *UMTS Networks: Architecture, Mobility and Services*, Wiley, 2001, ISBN 0-471-48654-X

Korhonen, *Introduction to 3G Mobile Communications*, Artech House, 2001, ISBN 1-58053-287-X

Many books on WCDMA technology (i.e. the radio interface) are available. However, understanding of WCDMA basics is not required in this course.