Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής

Ευφυή Κινητά Δίκτυα: Σύστημα Κινητής Τηλεφωνίας 2ης γενεάς (2G): GSM και GPRS

Εαρινό Εξάμηνο 2024-25

Βασίλειος Σύρης

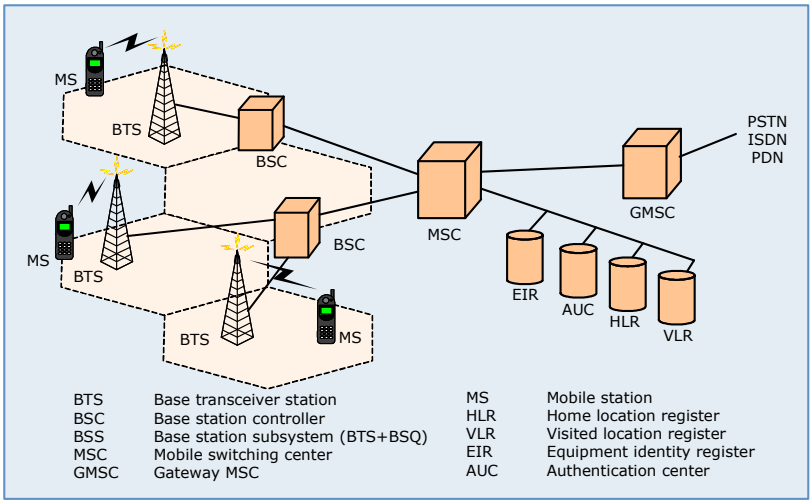
1

GSM frequency bands (common)

- GSM-900 and GSM-1800
  - Europe, Middle East, Africa, most of Asia
- GSM-850 and GSM-1900
  - USA, Canada, other countries in America
- GSM-400 and GSM-450 rarer

2

Network architecture



3

Network elements

- Mobile Station
  - Mobile Equipment
    - Identified by the International Mobile Equipment Identity (IMEI)
  - Subscriber Identity Module (SIM)
    - Contains a unique identification number called IMSI
    - It is removable, thus irrespective of a specific terminal

4

- Base Station Subsystem (BSS)
  - Base Transceiver Station (BTS)
    - A BTS is comprised of radio transceivers, antennas, the interface to the PCM facility
    - BTS is the entity that connects the mobiles to a cellular network
  - Base Station Controller (BSC)
    - Its primary function is call maintenance, by deciding when to initiate a handover, changing the BTS transmitter power, etc.
    - A BSC is connected to a group of BTSs and manages the radio resources for them

5

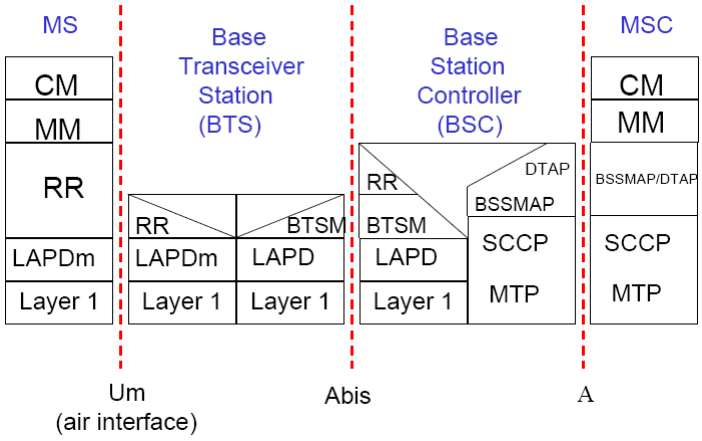
- Network Subsystem
  - Mobile Switching Center (MSC)
    - MSC provides functions such as registration, authentication, location updating, handovers and call routing to a roaming subscriber
  - Home Location Register (HLR)
    - The HLR contains all the administrative information and current location of each subscriber registered in the corresponding GSM network
  - Visitor Location Register (VLR)
    - Contains subscription information needed for call control, for all mobiles in the area of the associated MSC
  - Equipment Identity Register (EIR)
    - EIR is a database that contains a list of all valid mobile equipment on the network
  - Authentication Center (AUC)
    - Stores the secret key held in each user's SIM card

6

- Application Service Centers are responsible for GSM network add-on services
  - Operation and Maintenance Center (OMC)
    - Monitoring and control the network
    - Usually connect with MSC, BSC, HLR, and other service centers
  - Short Message Service Center (SMSC)
    - provide short message services
    - usually connect to MSC
  - Unstructured Supplementary Service Data Center (USSDC)
    - provide USSD service in the form of *ID*ID*info#
    - usually connect to HLR

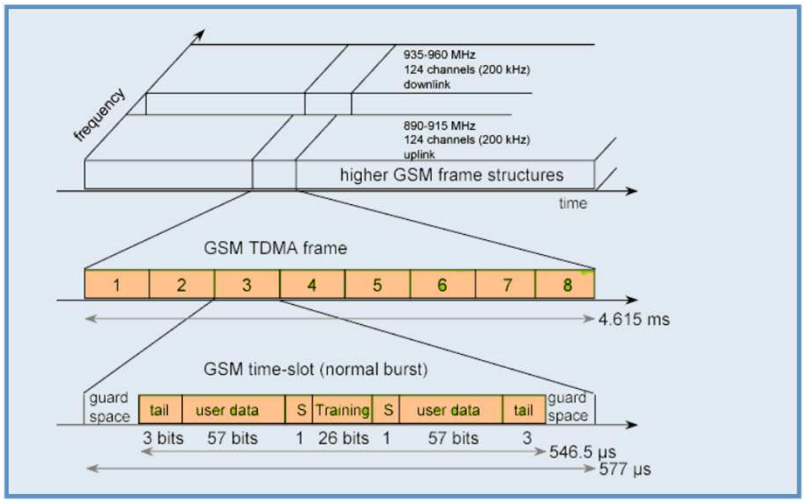
7

Protocol stack



8

GSM FDMA/TDMA



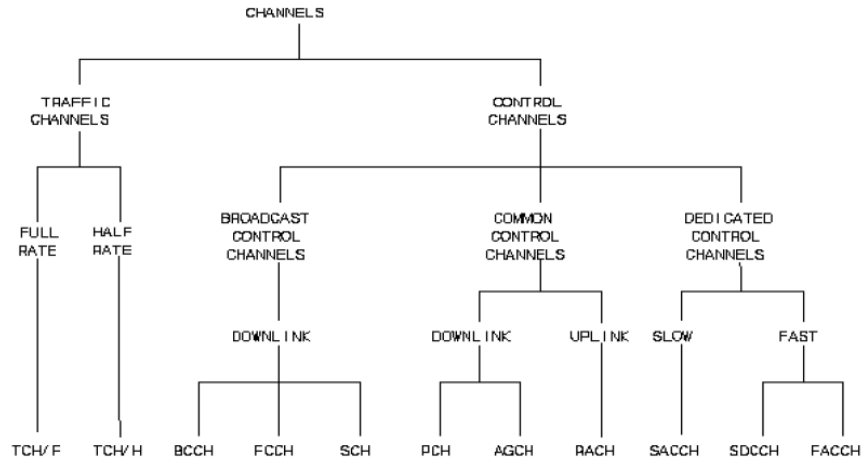
9

GSM channels

- Physical channel: specific time slot and channel/carrier frequency
- Logical channels
  - run over physical channels (not necessarily in all time slots)
  - two types: traffic and control
  - managed: setup, maintenance, tear-down
- Control channels interspersed with traffic channels in well-defined ways

10

GSM logical channels



11

Traffic channels

- Full rate: 22.8 kbps
  - speech data: 13 kbps voice data + FEC
  - packet data: 12,6,3.6 kbps + FEC
- Half rate: 11.4 kbps
- To achieve higher rates multiple logical channels have to be allocated (GPRS does this)

12

Control channels

- Help MS locate control channels
- Provide information about
  - voice and control channel repetition cycle.
  - parameters in the cell
  - surrounding cells
  - paging
- Allow random access attempts by the MS

13

Broadcast Control Channels

- FCCH (Frequency Correction Channel)
  - carrier synchronization
  - base station “beacon” signal
- SCH (Synchronization Channel)
  - frame synchronization
- BCCH (Broadcast Control Channel)
  - cell ID, available services, etc

14

Common Control Channels

- PCH (Paging Channel) - downlink
  - page a mobile
- AGCH (Access Grant Channel) - downlink
  - reply to a random access request, assign dedicated control channel
- RACH (Random Access Channel) – uplink
  - used by mobile to request dedicated control channel
  - messages from several mobiles can collide
  - Slotted Aloha used for contention resolution

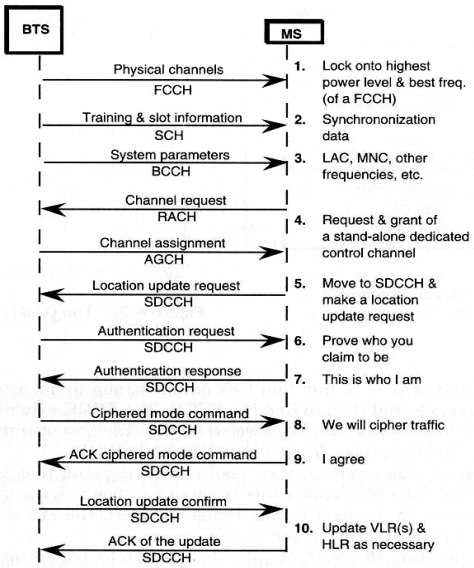
15

Dedicated and Control Channels

- SACCH (Slow Associated Control Channel)
  - in-band signaling
  - downlink: system info, power control
  - uplink: measurements
- FACCH (Fast Associated Control Channel)
  - in-band time-critical signaling
  - call establishment progress, authentication, handover signaling
- SDCCH (Stand-alone Dedicated Control Channel)
  - out-of-band signaling
  - call setup signaling, SMS, location update

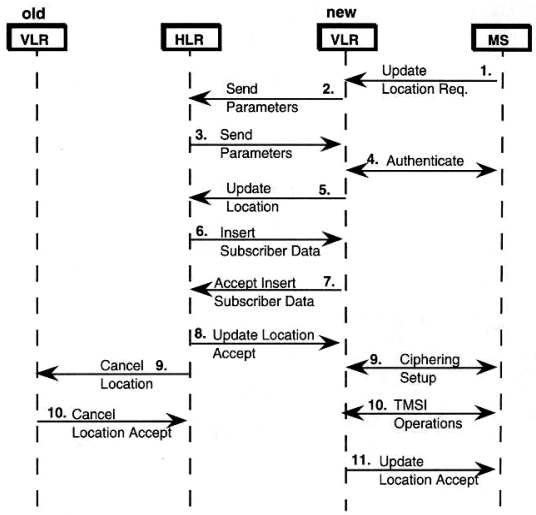
16

Mobile initialization



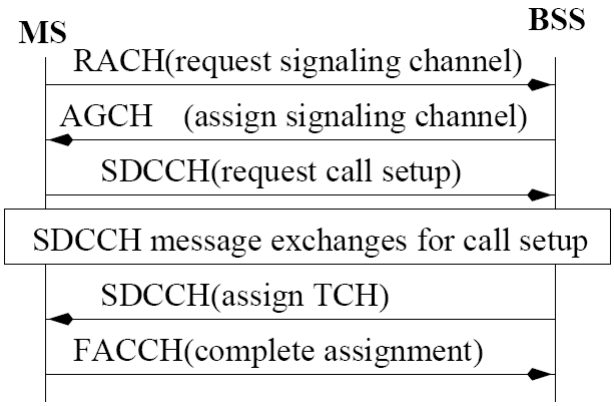
17

Location update



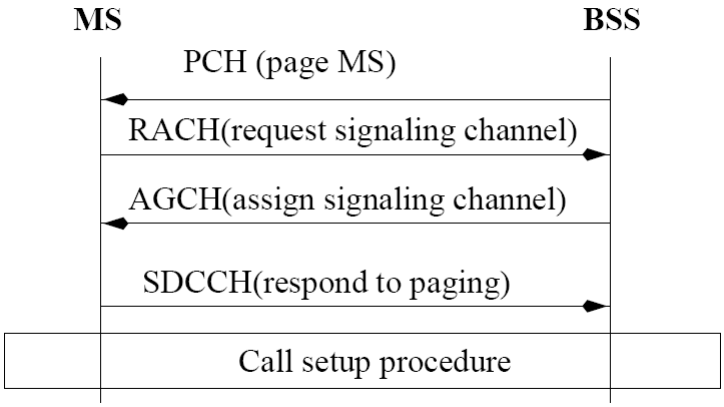
18

Call origination (MS->BSS)



19

Call termination (BSS->MS)



20

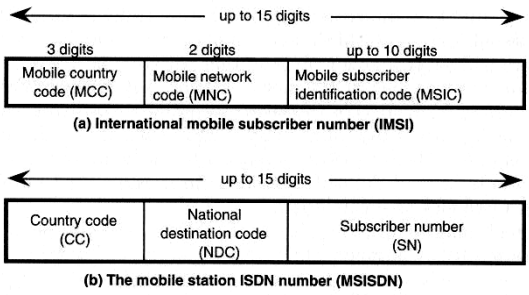
Network elements

- Mobile Station
  - Mobile Equipment
    - Identified by the International Mobile Equipment Identity (IMEI)
  - Subscriber Identity Module (SIM)
    - Contains a unique identification number called IMSI
    - It is removable, thus irrespective of a specific terminal

21

GSM identifiers

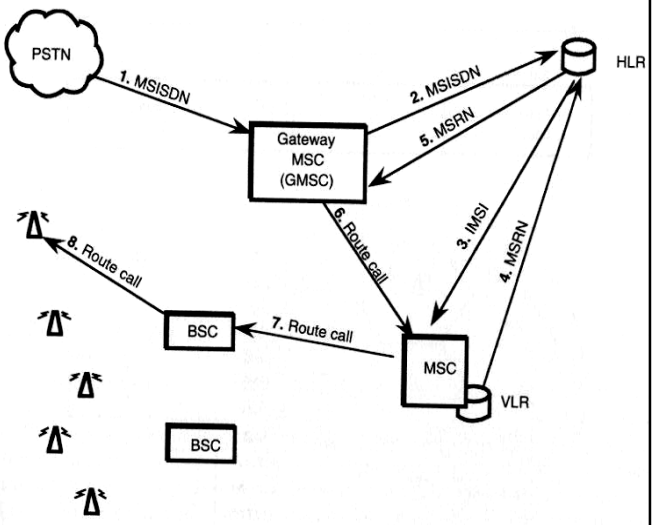
- IMSI: non-dialable number
  - MCC Greece: 202
  - Bound to SIM
- TMSI: Temporary MSI (confidentiality)
- MS ISDN number (dialable)
  - Different MS ISDN associated to same SIM



22

Call routing

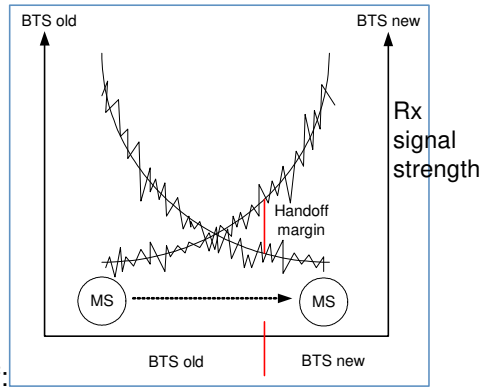
- IMSI: International Mobile Subscriber Identifier
- MSISDN: MS ISDN (called number)
- MSRN: Mobile Station Routing Number



23

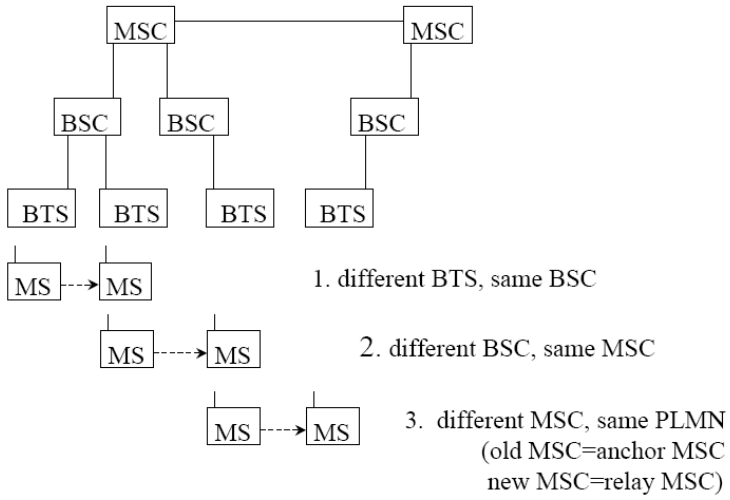
Mobility management

- Location Registration
- Call delivery
- Handoff Management
  - Handoff is caused by:
    - signal strength deterioration
    - user mobility
  - There are two kinds of handoff:
    - soft handoff
    - hard handoff
  - There are three ways to handoff:
    - network-controlled handoff
    - mobile-assisted handoff
    - mobile-controlled handoff



24

Three cases of handovers



25

Power control

- Operator-dependant
- Mobile:
  - Peak Tx power classes: GSM-900: 8,5,2,0.8 Watt (39,37,33,29 dBm), GSM-1800: 1,0.25,4 Watt (30,24,36 dBm)
  - minimum Tx power: GSM-900: 19mW, GSM-1800: 15mW
  - step: 2dBm
- Base station:
  - 8 classes: 320-2.5 Watt (55-34dBm)
- Base station controller decides power control changes for both
  - Mobile measures signal strength, quality (BER) and reports to Base station
  - Goal: operate at lowest power level while maintaining acceptable signal quality

26

GPRS (General Packet Radio Service)

- The major GSM Phase 2+ enhancement and an important step to 3G
  - considered 2.5G
- Aims at providing data services to mobile users with high bandwidth efficiency and “always on” connectivity
- Address shortcomings of GSM
  - Low data rates (up to 9.6 kbps)
  - Long connection setup
  - Expensive
  - Circuit-switched

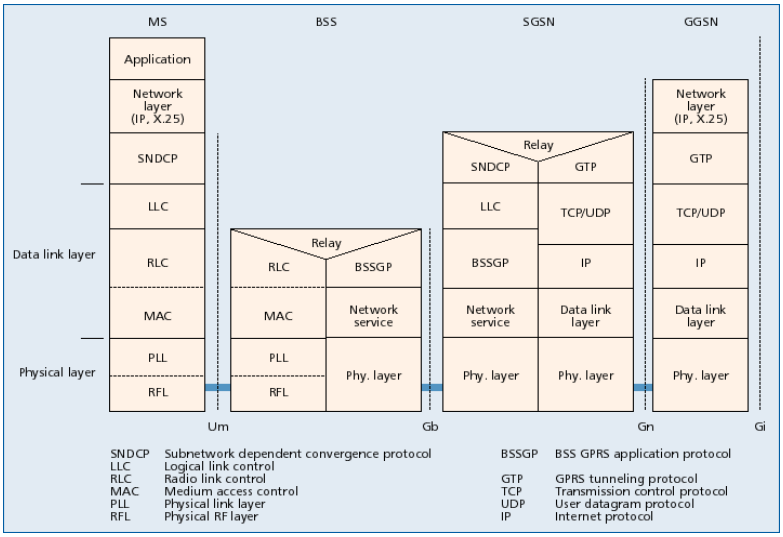
27

GPRS features

- Data rates up to 172 kbps
- Fast call setup times
- “Always on” connectivity
- Integrates IP infrastructure into the GSM network
- Uses packet-switched mechanisms
  - more efficient for bursty traffic
  - allow volume-based charging

28

Protocol architecture



29

Channel coding & transmission rate

- Coding used in every digital communication system to
  - increase channel capacity
  - protect against errors
- GPRS uses 4 different coding schemes, depending on channel conditions **physical layer**

Coding Scheme	Data Rate kbit/s	Channel Conditions
CS-1	9.05	Tough
CS-2	13.4	Tough to Moderate
CS-3	15.6	Moderate
CS-4	21.4	Good

- Up to 8 slots can be combined

Coding	Number of Timeslots			
	1	2	3	8
CS-1	9.05	18.1	27.15	72.4
CS-2	13.4	26.8	40.2	107.2
CS-3	15.6	31.2	46.8	124.8
CS-4	21.4	42.8	64.2	171.2

(Raw) Data Rate (Kb/s)

30

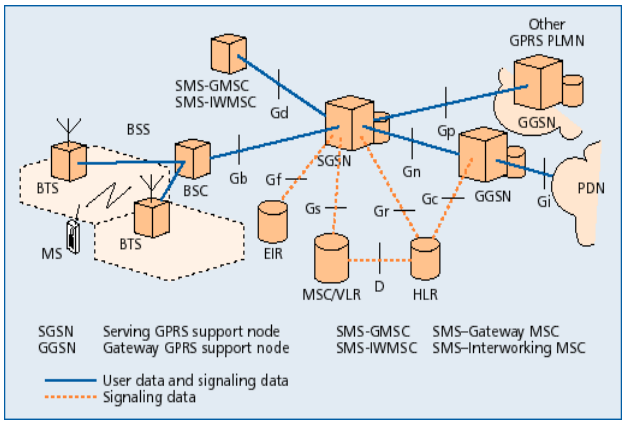
QoS

- GPRS Release 99 specified 4 traffic classes

Traffic Class	Medium	Application	Data Rate (kbps)	One-way Delay
Conversational	Audio Data	Telephony Telnet	4-25 <8	<150 ms <250 ms
Streaming	Audio Video Data	Streaming (HQ) One-way FTP	32-128 32-384 -	<10 s <10 s <10 s
Interactive	Audio Data	Voice Messaging Web-Browsing	4-25 <8	<1 s <4 s/page
Backround	Only Bit Integrity Is Required			

31

GPRS architecture



- 2 new nodes .
  - Serving GPRS Support Node (SGSN)
  - Gateway GPRS Support Node (GGSN)

32

Serving GPRS Support Node (SGSN)

- Serving GPRS Support Node (SGSN) is responsible for:
  - Admission control
  - Routing, mobility management, location management, authentication, charging
  - Receiving and delivering data packets
  - Address translation and mapping
  - Encapsulation

33

Gateway GPRS Support Node (GGSN)

- Gateway GPRS Support Node (GGSN)
  - acts as interface between GPRS backbone and external Packet Data Networks (PDN) or other Public Mobile Land Networks
  - converts GPRS packets coming from SGSN into the appropriate packet data protocol (PDP) format (e.g. IP)
  - converts the PDP addresses of incoming data packets to the GSM address of the destination user, and sends the readdressed packet sto the responsible SGSN

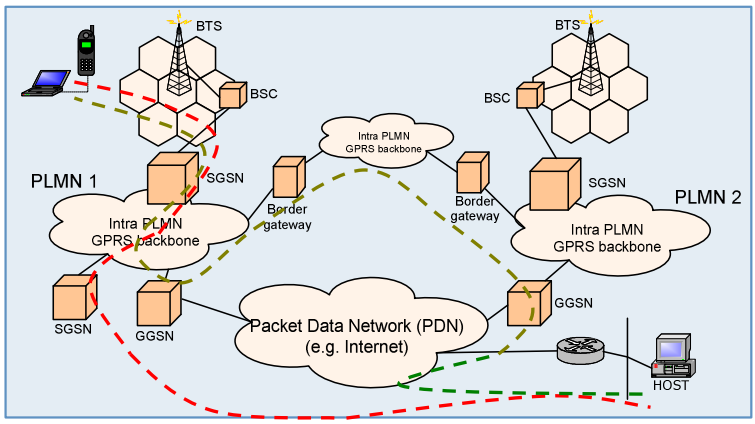
34

Additional enhancements

- Base Station System (BSS): enhanced to recognize and send user data to the SGSN that is serving the area
- Home Location Register (HLR): enhanced to register GPRS user profiles and respond to queries originating from SGSNs

35

Routing Scenarios



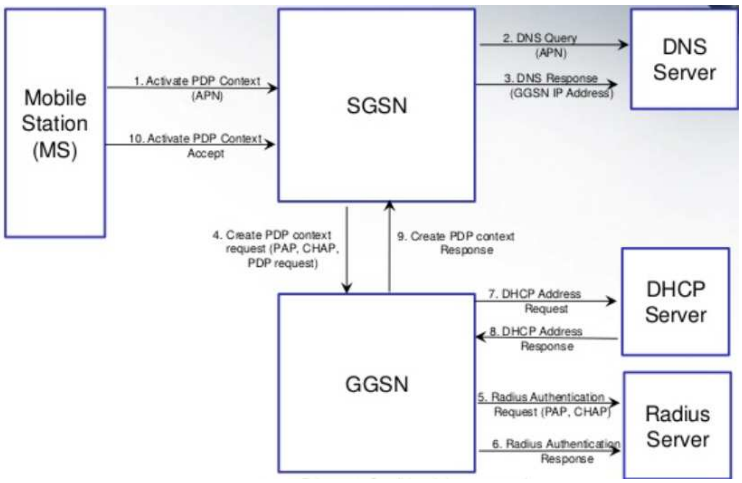
36

GPRS processes

- Attach process
- Authentication process
- PDP (Packet Data Protocol) activation process
- Detach process

37

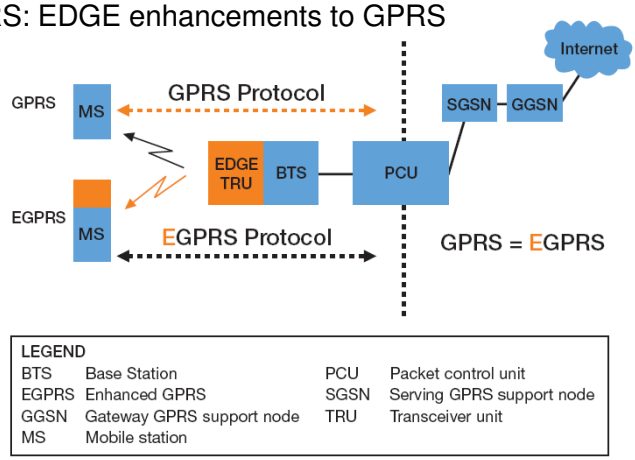
PDP context activation



38

Enhanced Data for GSM Evolution (EDGE)

- Higher data rates using 8PSK modulation
  - user rate 384 kbps (GPRS: 115 kbps)
- Software-only update (Release 99)
- EGPRS: EDGE enhancements to GPRS



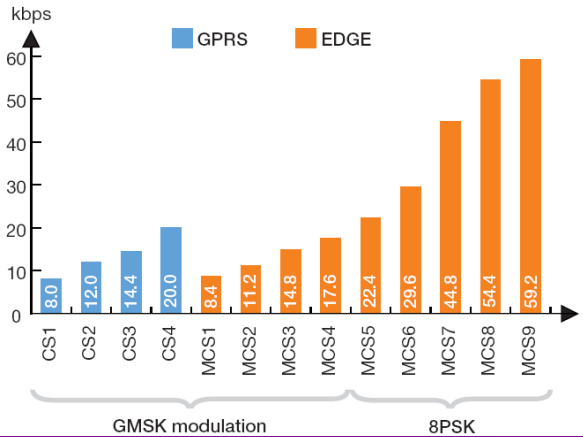
LEGEND

BTS	Base Station	PCU	Packet control unit
EGPRS	Enhanced GPRS	SGSN	Serving GPRS support node
GGSN	Gateway GPRS support node	TRU	Transceiver unit
MS	Mobile station		

39

EDGE higher rates

- RLC data rate



40