Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής

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

Γιάννης Θωμάς

Ακαδ. Έτος: 2023-24

(Βασισμένο σε διαφάνειες του Βασίλειου Σύρη)

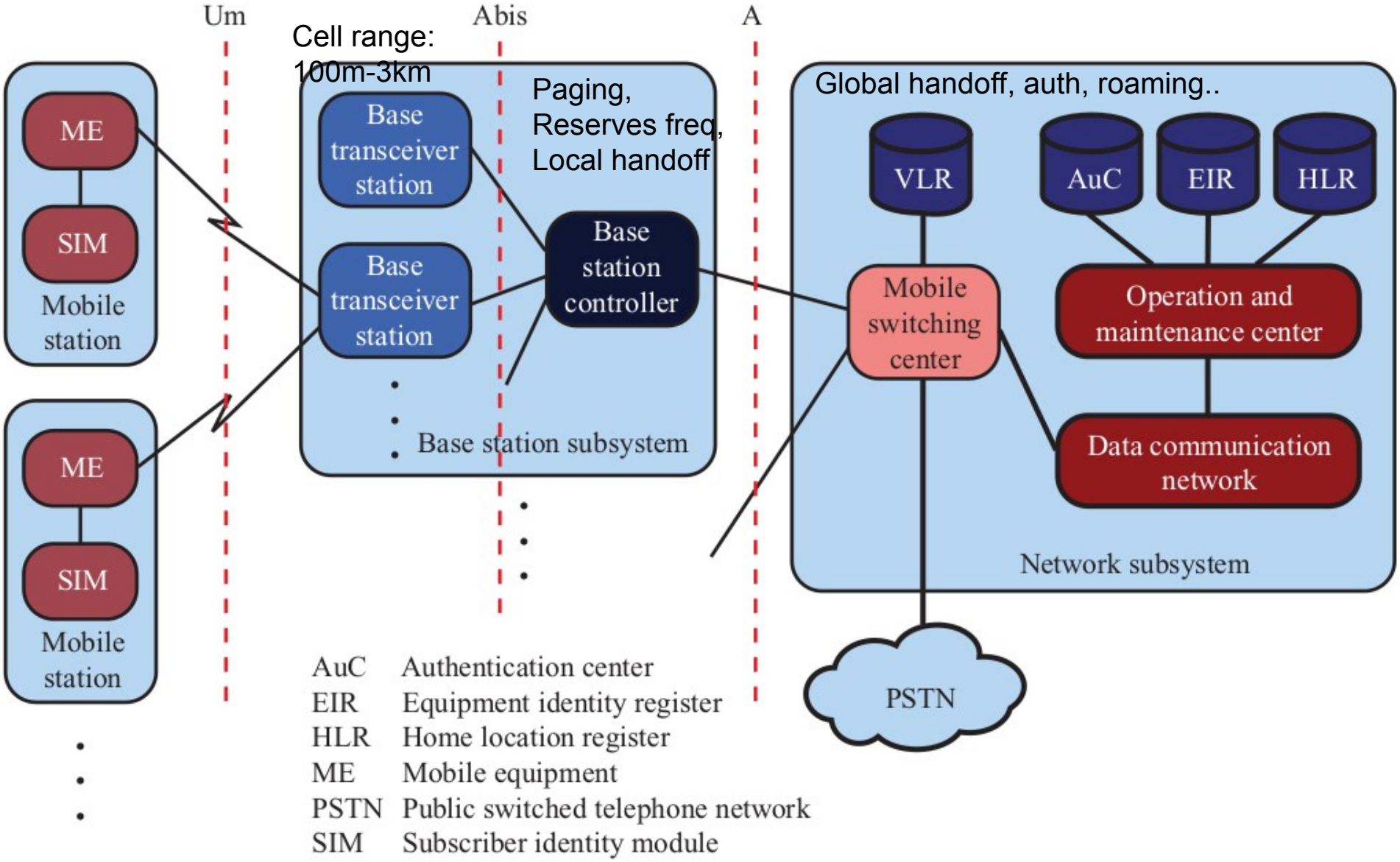
From 1st to 2nd Gen (~1990)

- AMPS, quickly became highly popular,
- Scarcity of capacity
  - even with frequency reuse
- Goals:
  - Higher data rates
  - Higher-quality signals
  - Greater capacity
- Key differences:
  - **Digital** traffic channel, **encryption**, **Error** detection and correction, **TDMA** & **CDMA**

GSM frequency bands (common)

- **G**lobal **S**ystem for **M**obile Communications
  - (In Need for) a common 2nd Gen technology for Europe so that the same subscriber units could be used throughout the continent.
    - Tech Consistency / homomorphism
- 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

GSM architecture



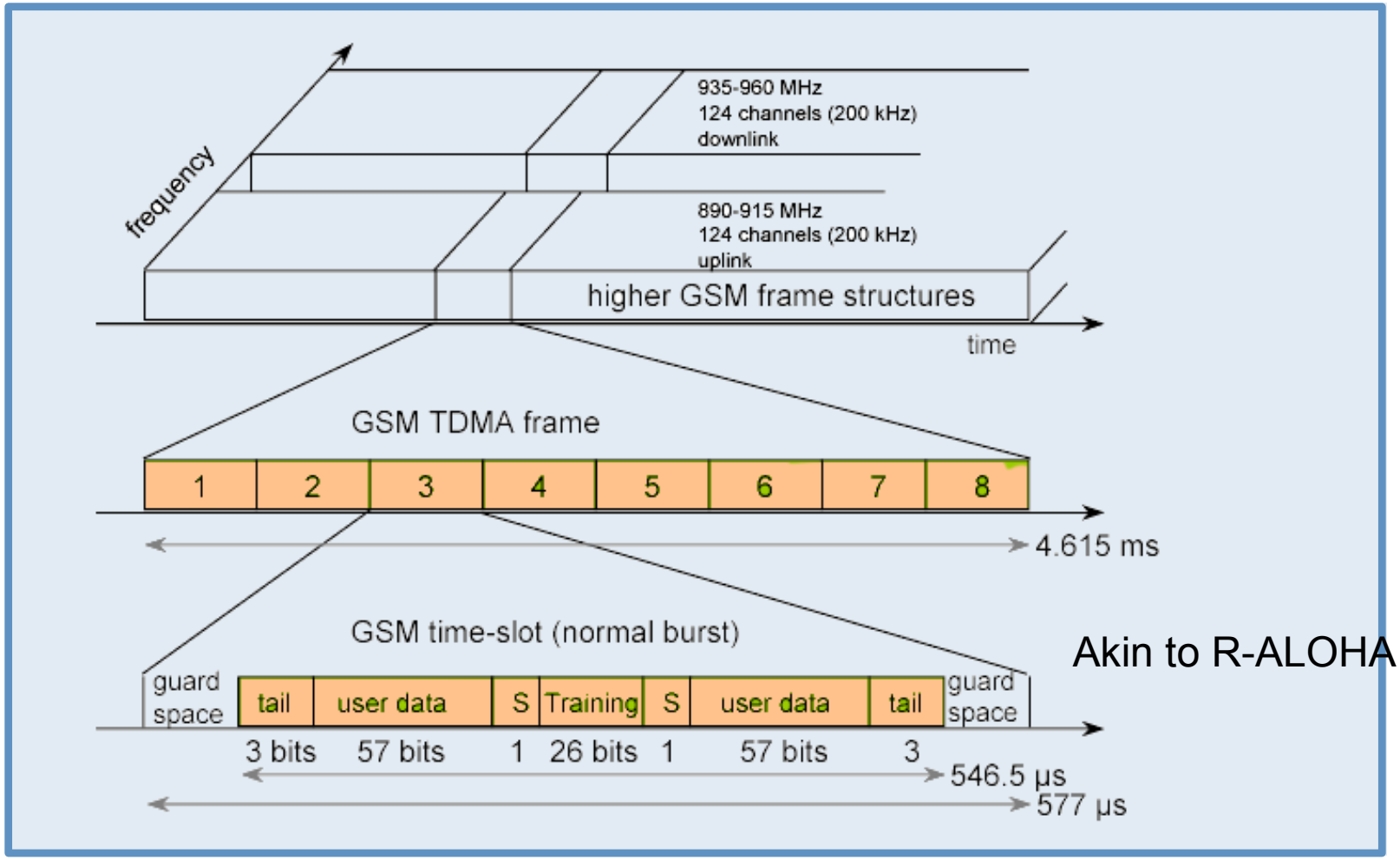
A5 stream cipher (from wikipedia)

- A5/1 is used in Europe and the United States. A5/2 was a deliberate weakening of the algorithm for certain export regions.
- Both were initially kept secret, the general design was leaked in 1994 and the algorithms were entirely reverse engineered in 1999 by Marc Briceno from a GSM telephone.
- In 2000, around 130 million GSM customers relied on A5/1 to protect the confidentiality of their voice communications.
- Security researcher Ross Anderson [1994]: "there was a terrific row between the NATO signal intelligence agencies in the mid-1980s over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the Warsaw Pact; but the other countries didn't feel this way, and the algorithm as now fielded is a French design."

GSM specs

- 25MHz for base transmission
- 25MHz for mobile transmission
- 125 full-duplex channels
  - Every 200kHz
  - 270kbps
- Traffic and control channels
- TDMA and CDMA
  - 1G freq reservation was considered wasteful

GSM FDMA/TDMA: frame hierarchy



Akin to R-ALOHA

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)

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

- 3 Types of control channels

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

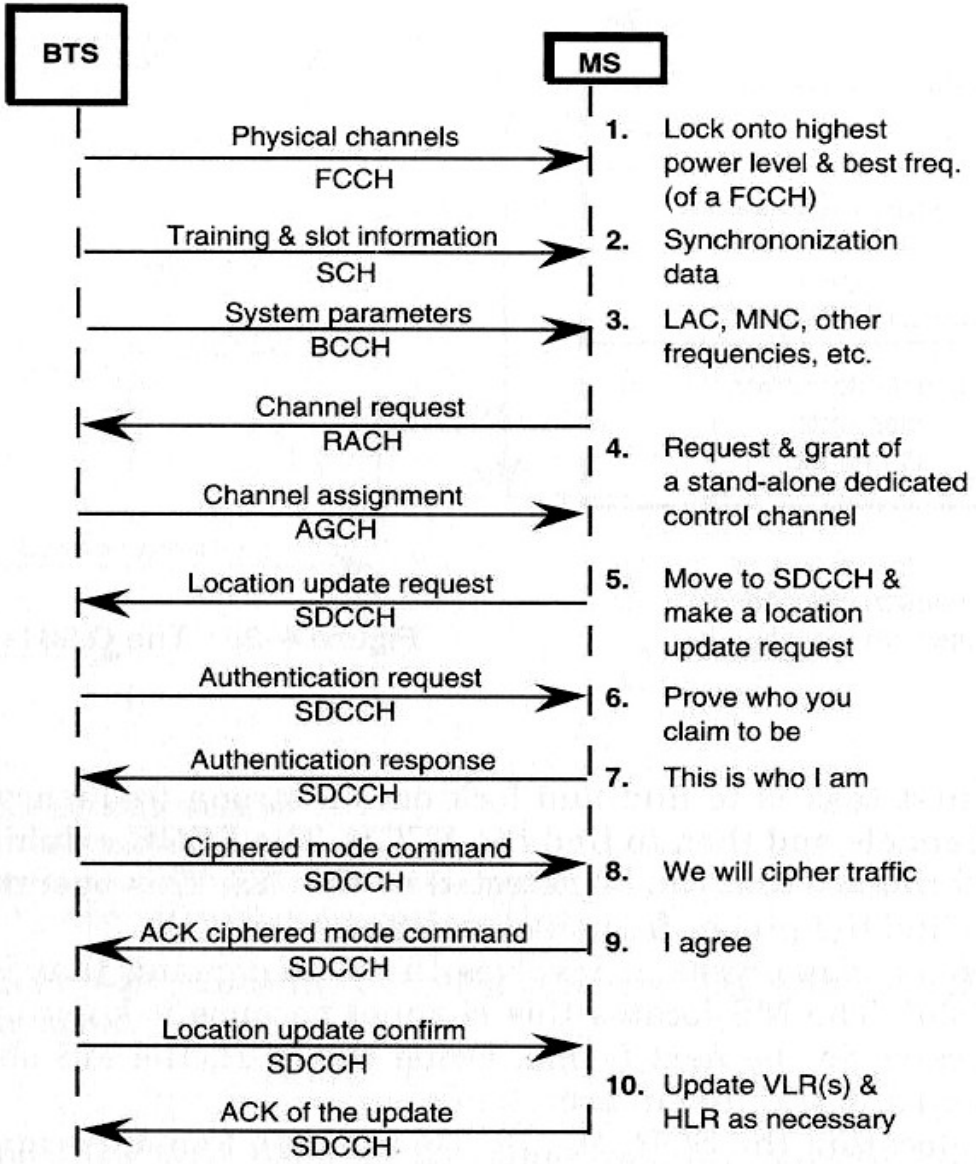
Common Control Channels

- 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

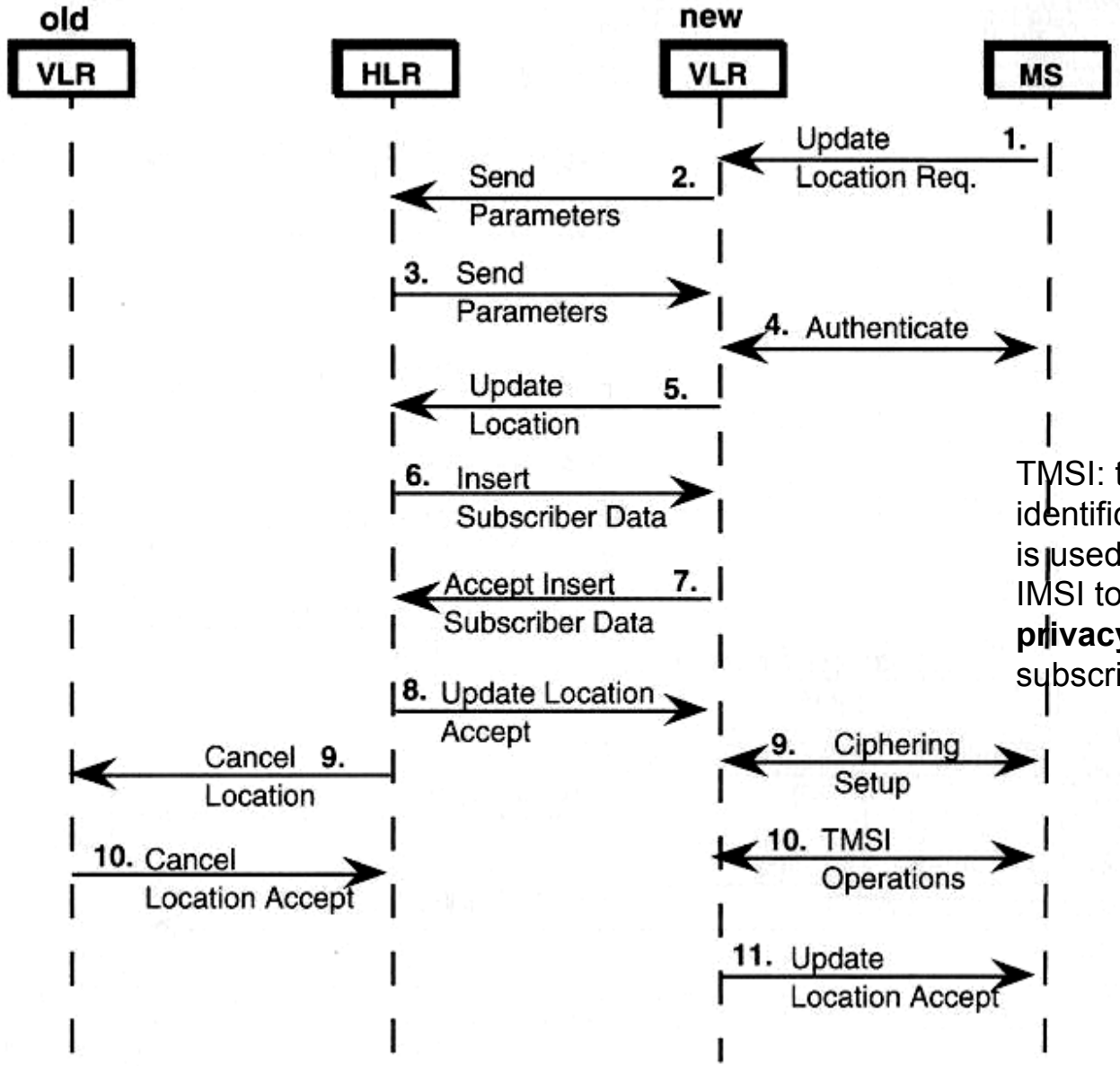
Dedicated and Control Channels

- 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

Mobile initialization



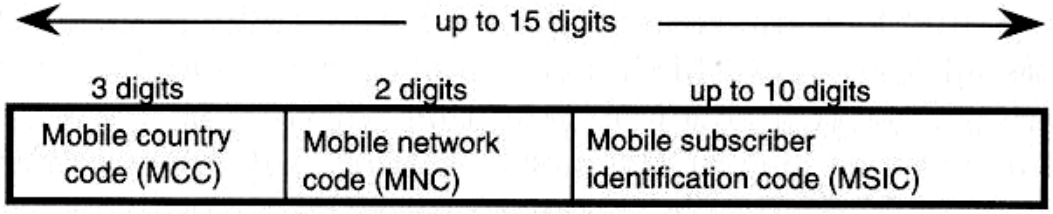
Location update



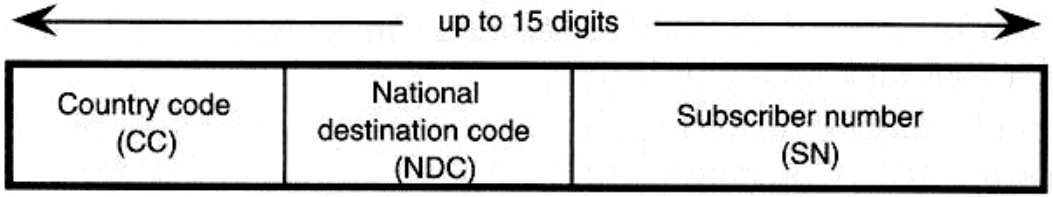
TMSI: temporary identification number that is used instead of the IMSI to ensure the **privacy** of the mobile subscriber.

GSM identifiers

- IMSI: **non-dialable** number
  - MCC Greece: 202
  - Bound to SIM
- MS ISDN number (**dialable**)
  - Different MS ISDN associated to same SIM



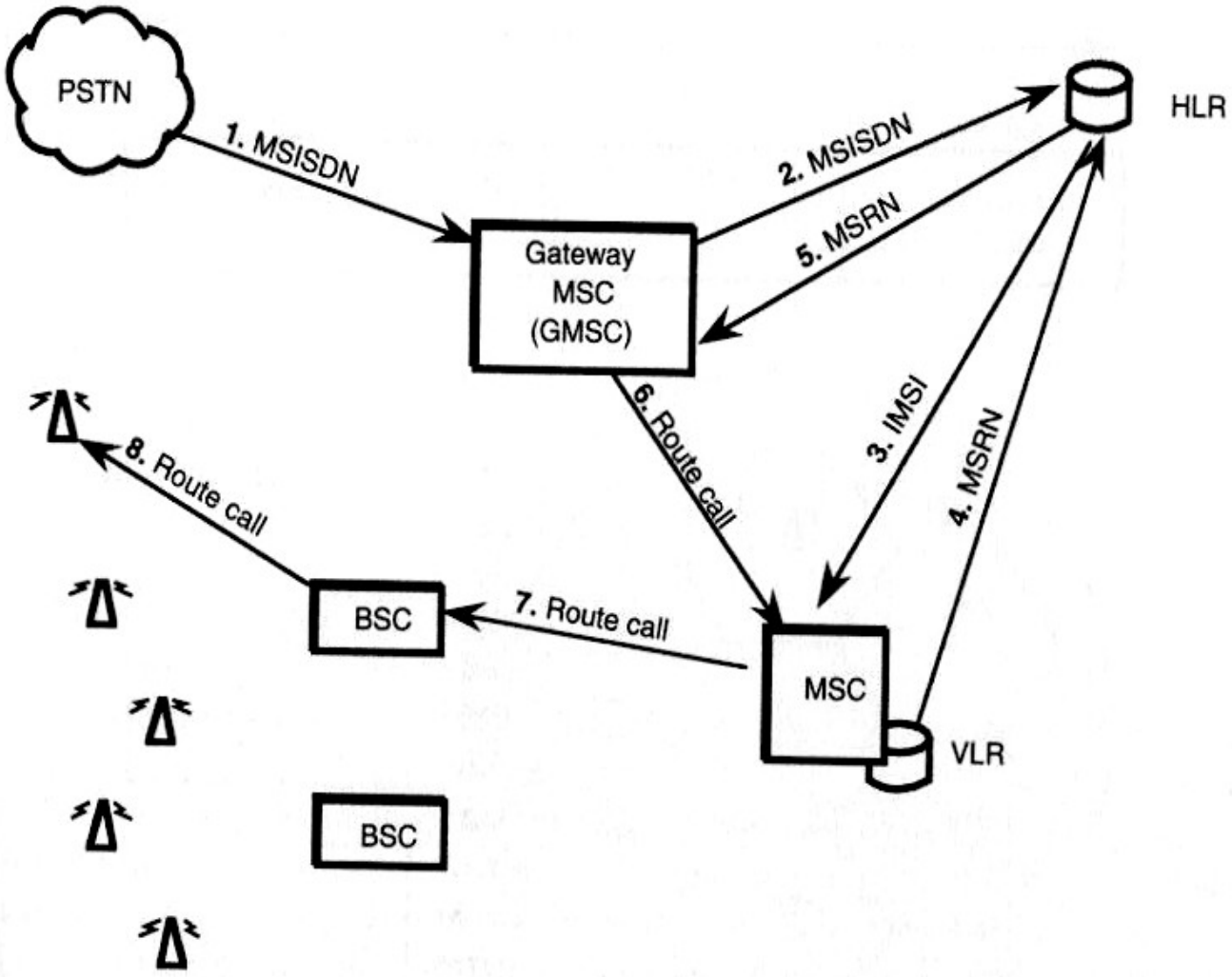
(a) International mobile subscriber number (IMSI)



(b) The mobile station ISDN number (MSISDN)

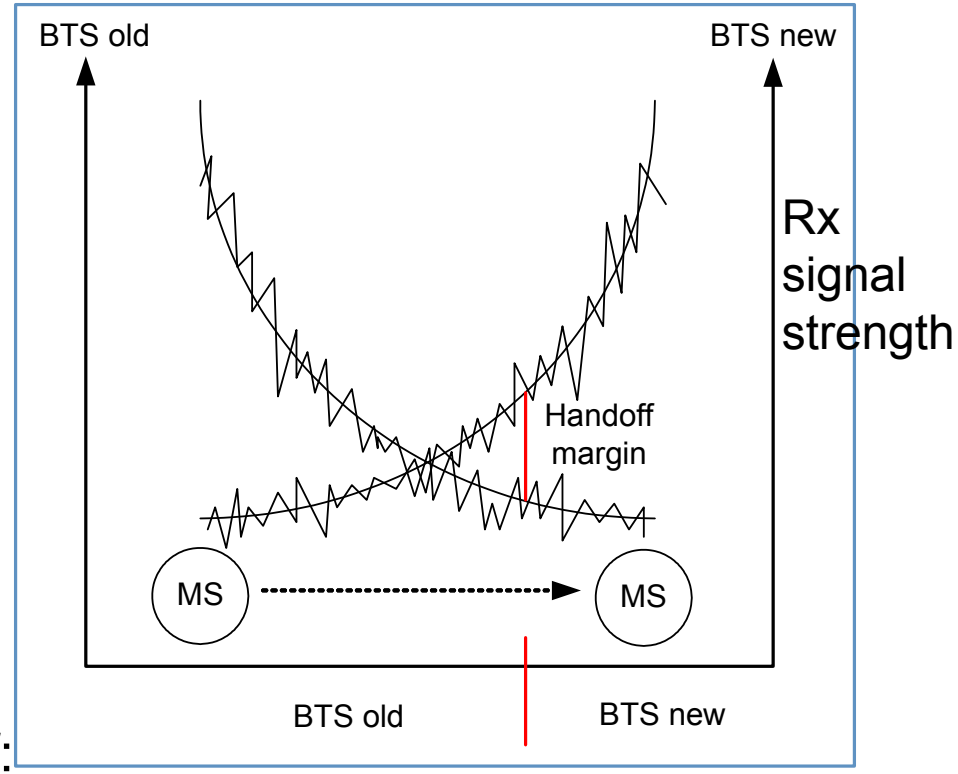
Call routing

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

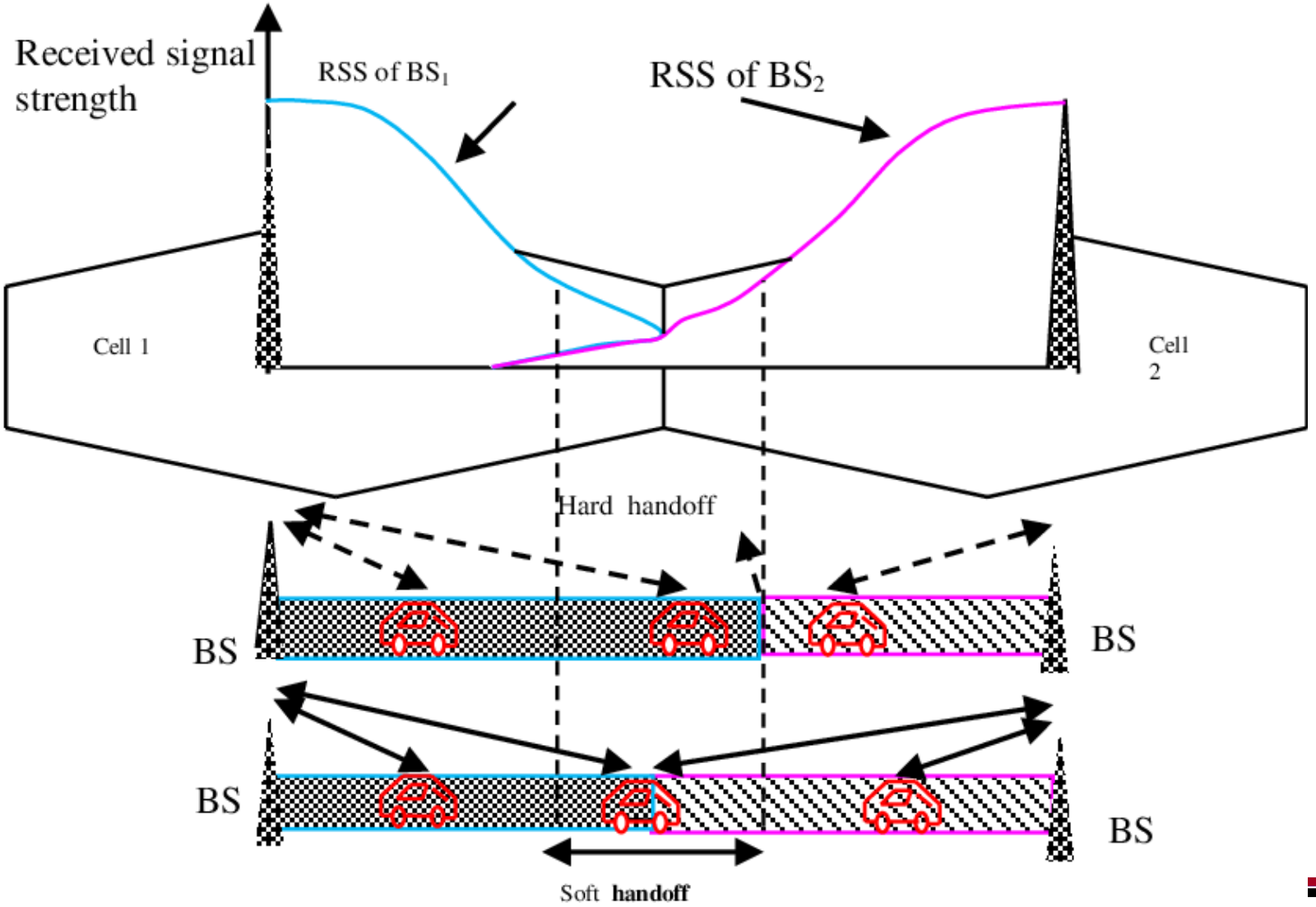


Mobility management

- 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

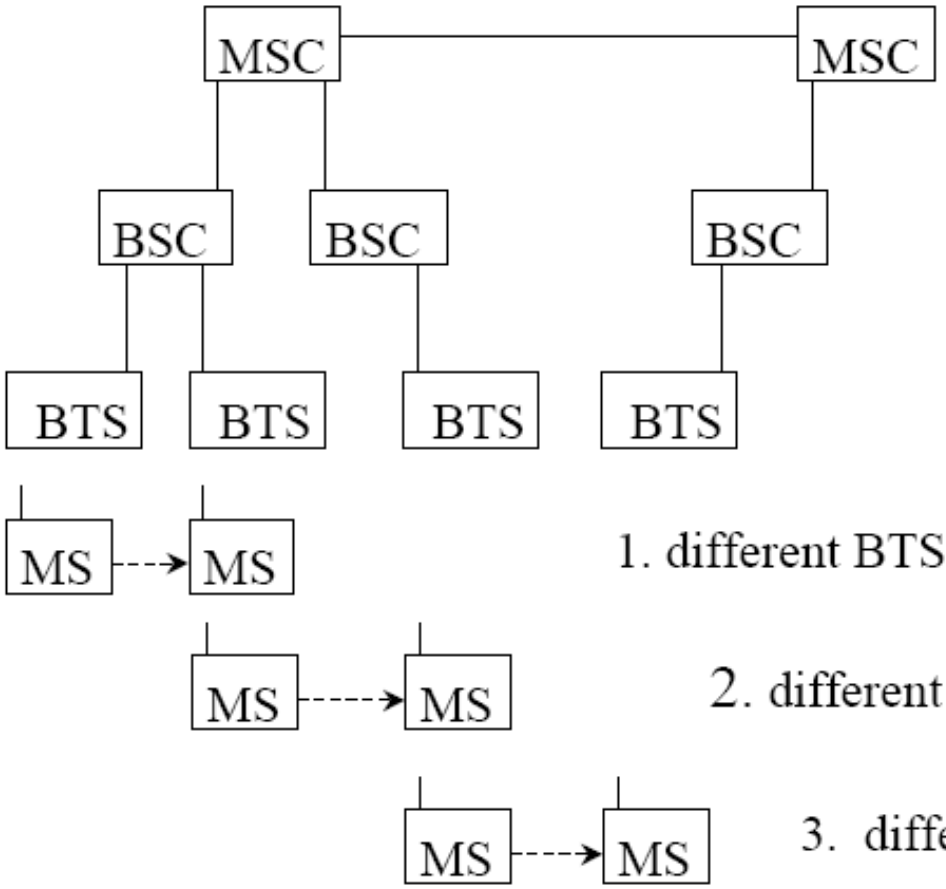


Soft Vs. Hard handoff



Src: https://www.researchgate.net/figure/Comparison-of-Hard-Handoff-and-Soft-Handoff_fig1_31827183

Three cases of handovers



1. different BTS, same BSC

2. different BSC, same MSC

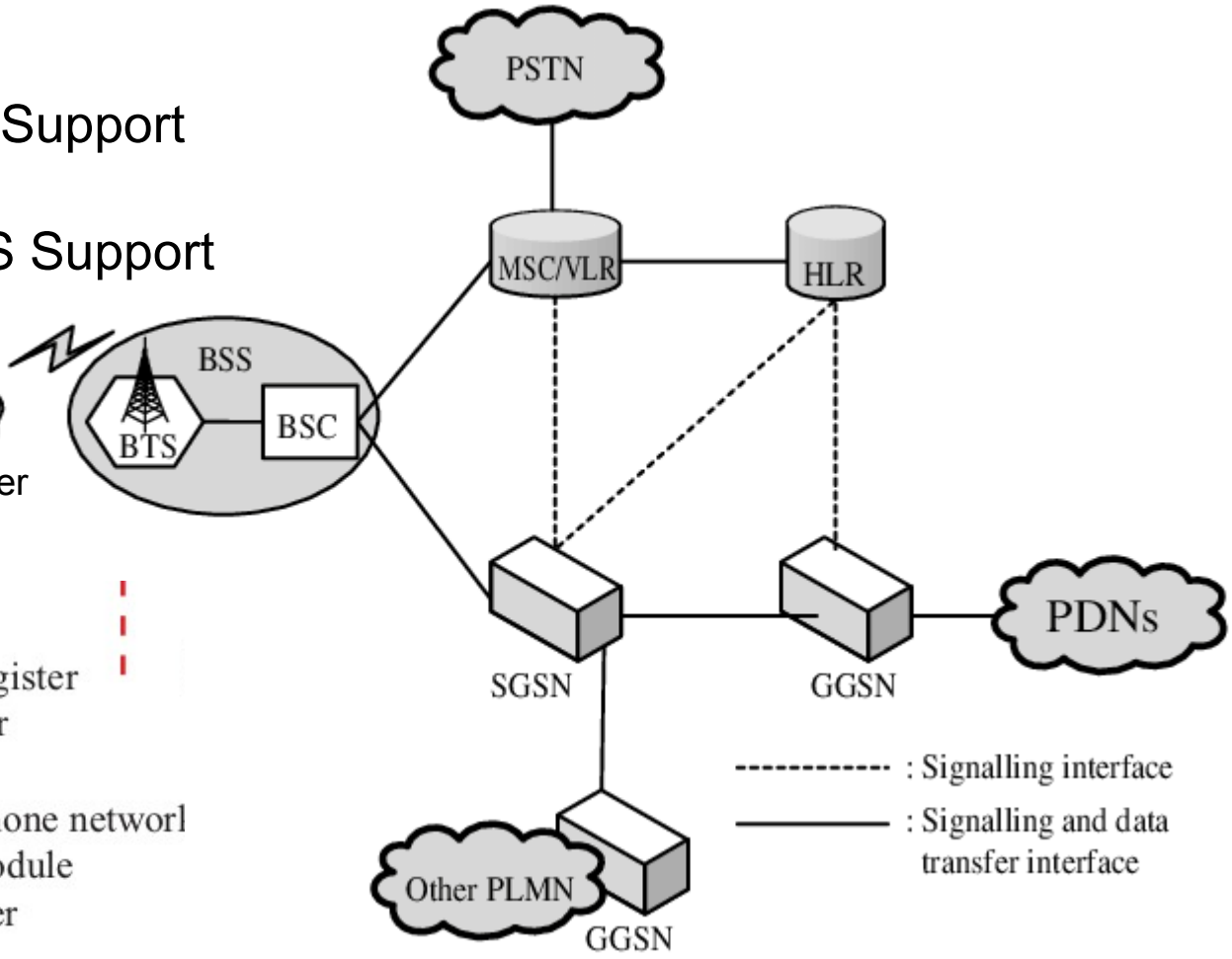
3. different MSC, same PLMN
(old MSC=anchor MSC
new MSC=relay MSC)

GPRS (General Packet Radio Service)

- The major GSM Phase 2+ enhancement and an important step to 3G
  - considered **2.5G**
- Goals:
  - *high bandwidth efficiency*
  - *"always on"* connectivity
- Key differencies
  - Higher data rates (21kbps per channel)
    - 171kbps by combining 8 time-slots
  - Faster connection setup via persistent data connections
    - But charging based on traffic (not connection time)

GPRS architecture

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



MSC MobileSwitchingCenter
PDN Packet Data Network
PLMN Public Land Mobile Network

AuC	Authentication center
EIR	Equipment identity register
HLR	Home location register
ME	Mobile equipment
PSTN	Public switched telephone networl
SIM	Subscriber identity module
VLR	Visitor location register

Gateway GPRS Support Node (GGSN)

- Interface between GPRS backbone and external Packet Data Networks (PDN) or other Public Mobile Land Networks
  - Outgoing packets: Converts GPRS packets into the appropriate packet data protocol (PDP) format (e.g. IP)
  - incoming packets: Converts the PDP addresses to GSM address of the destination user, and sends the *readdressed* packets to the responsible SGSN
- For external Internet devices GGSN is like a router to a “sub-network”
- Enables mobility: is anchor point keeping needed state

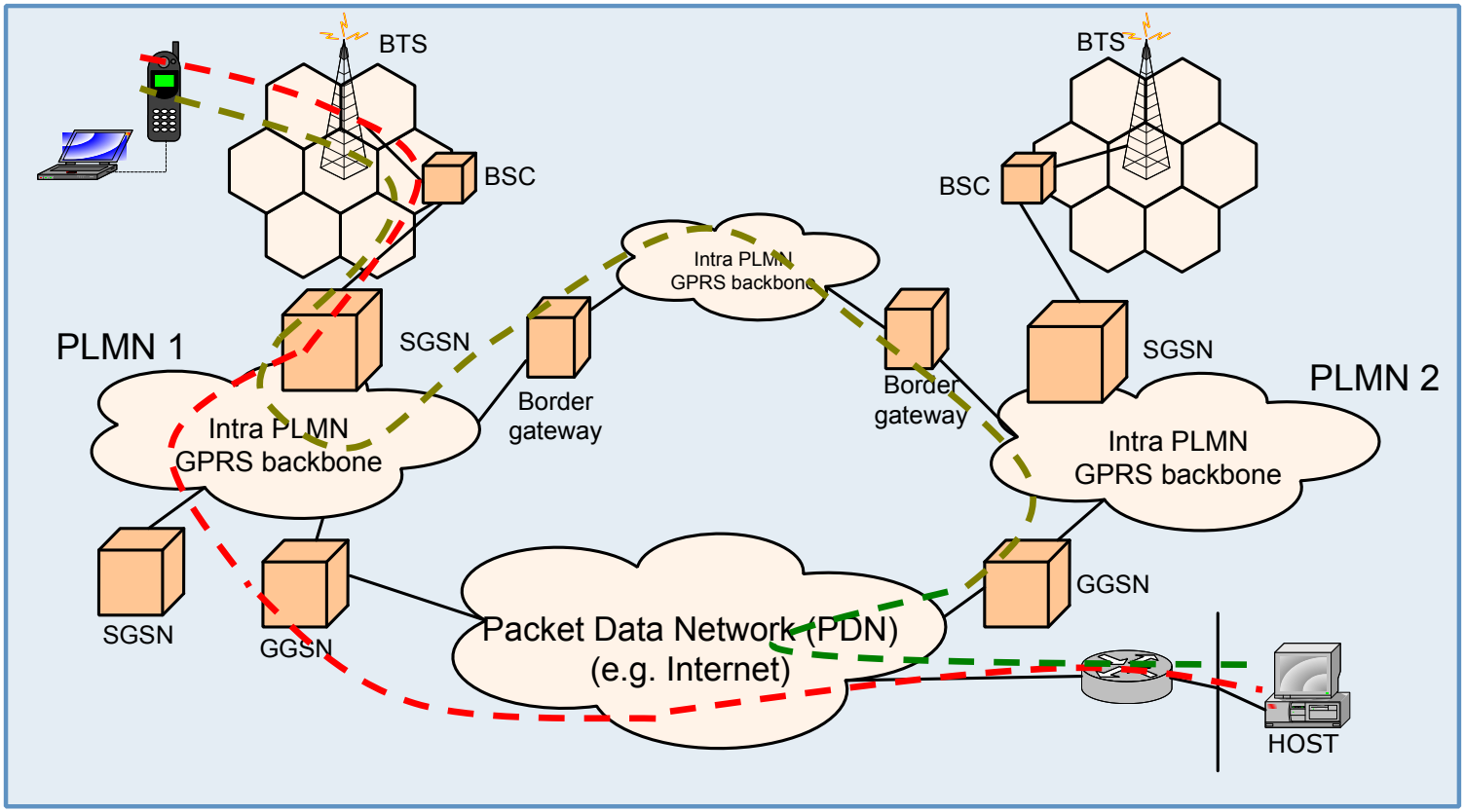
Serving GPRS Support Node (SGSN)

- Tasks:
  - Local: routing, mobility management, location management, authentication, charging
  - Receiving and delivering data packets
  - Address translation and mapping
  - Encapsulation
- Connected to BSC
  - Often collocated with MSC

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

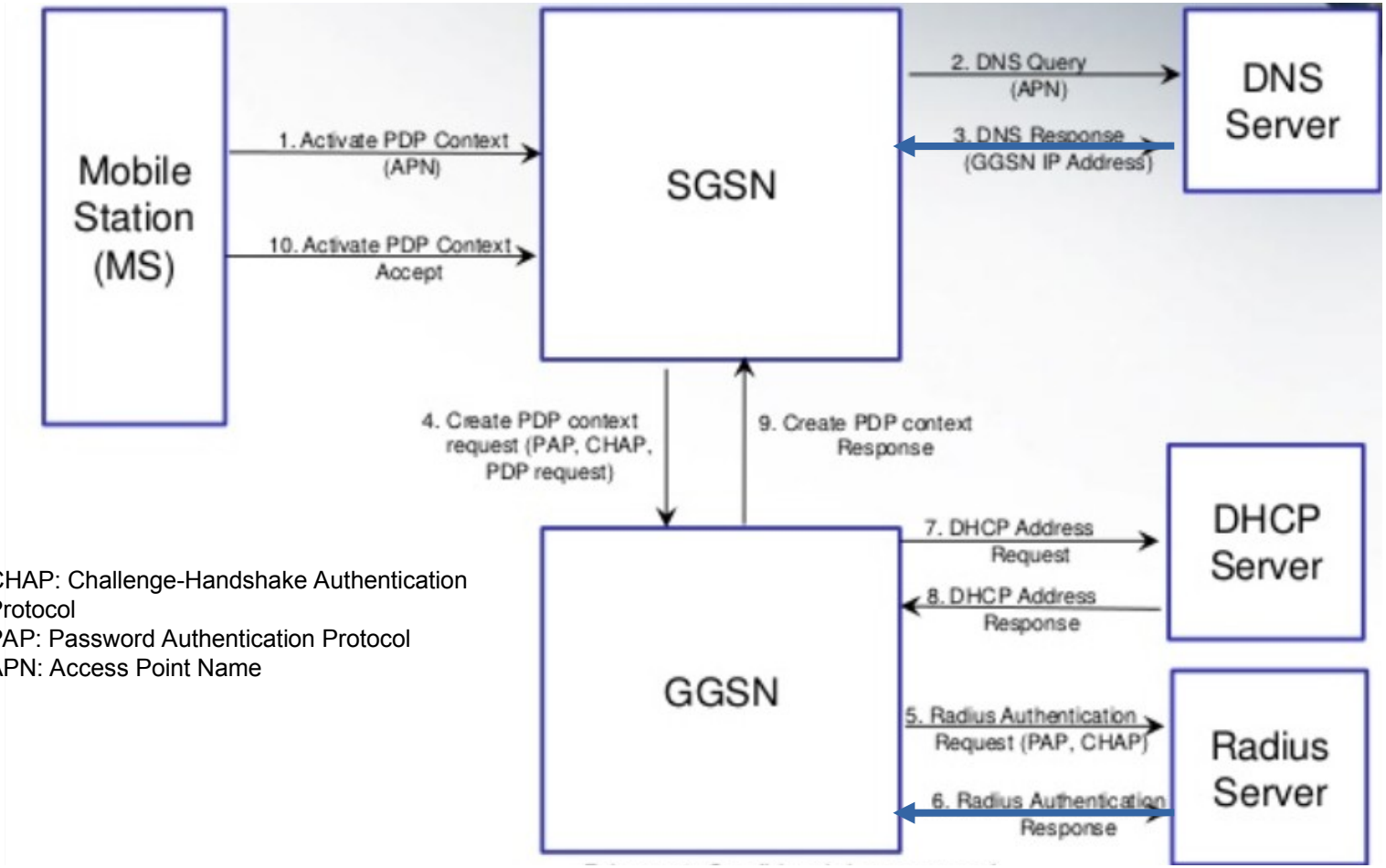
Routing Scenarios



GPRS processes

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

PDP activation process overview



- CHAP: Challenge-Handshake Authentication Protocol
- PAP: Password Authentication Protocol
- APN: Access Point Name

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)

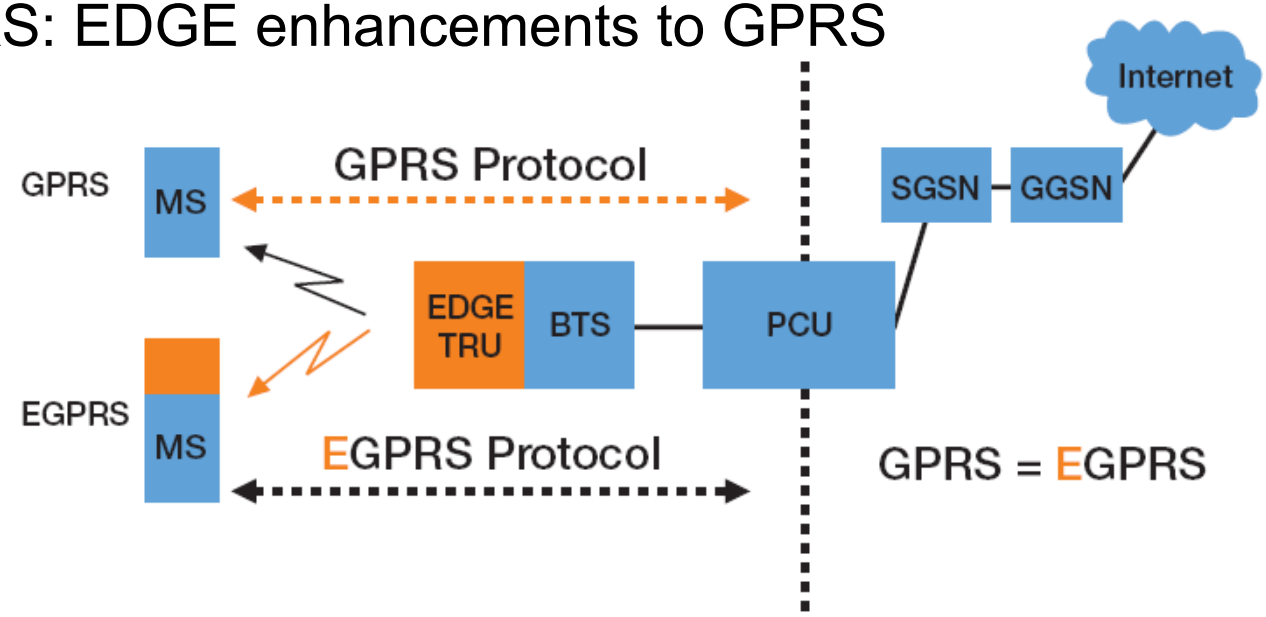
QoS

- GPRS Release 99 specified 4 traffic classes
- Network must satisfy those reqs

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			

EDGE: Enhanced Data for GSM Evolution (~1999)

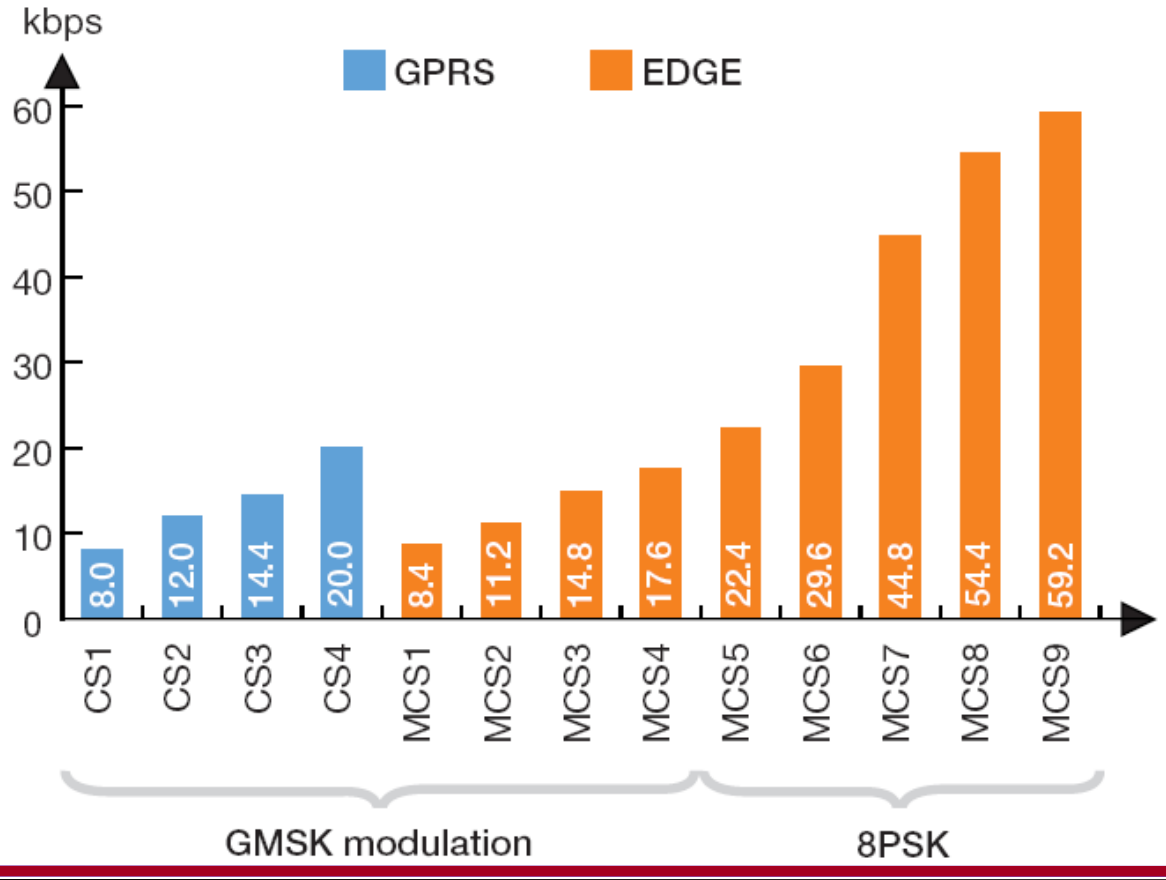
- Higher data rates using **8PSK** modulation
  - 3 bits/symbol: 68kbps per channel
- Software-only update
- EGPRS: EDGE enhancements to GPRS



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		

EDGE higher rates

- RLC data rate



Θα ξεκινήσουμε στις 12:15

Επιστρέφουμε 2:10