Cellular Architectures and Protocols

Marceau Coupechoux

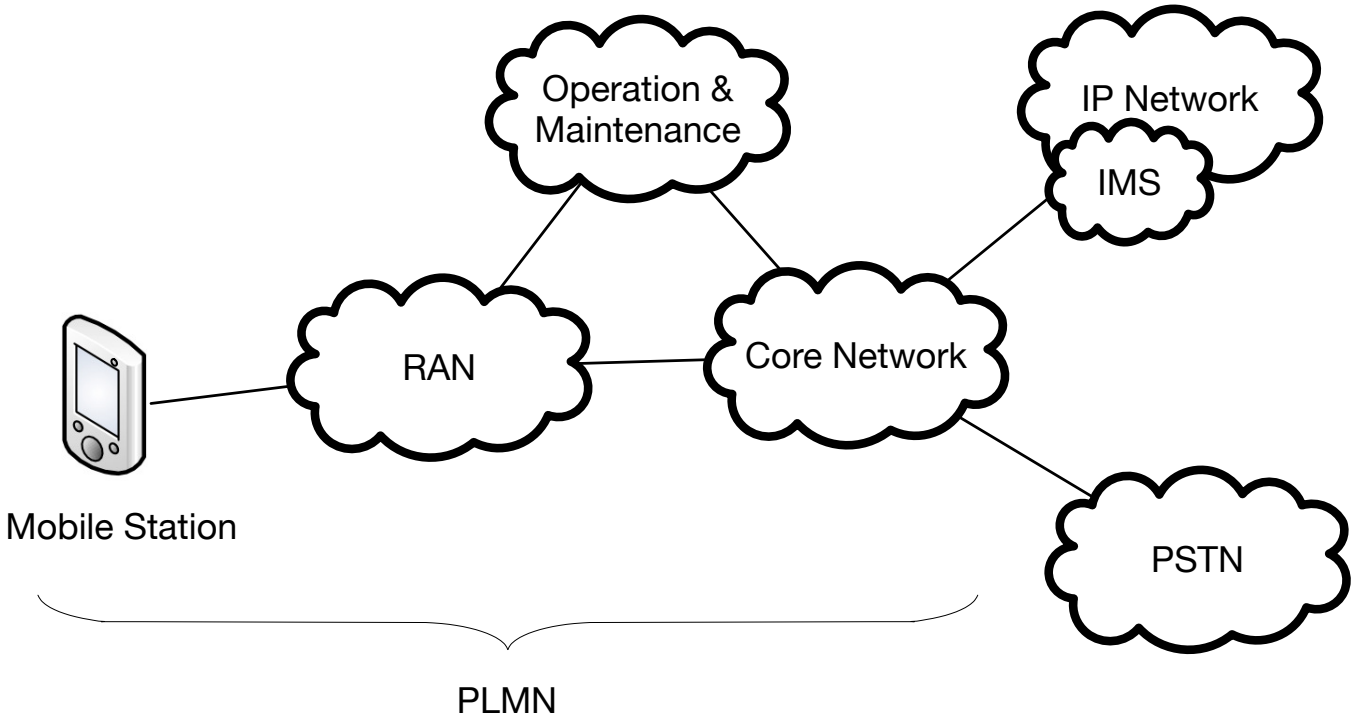
Acknowledgment: Ph. Godlewski, X. Lagrange, Ph. Martins, A. Vergne

12 mars 2018

Outlines

- Architectures
- Signaling and control plane
- Security
- Procedures in idle mode
- Procedures in connected mode
- Cell selection
- Calls
- Mobility : handover and roaming

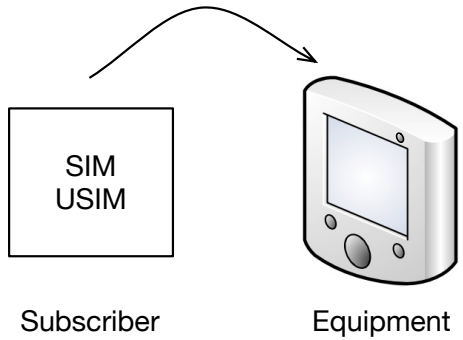
Architectures : Overview



RAN: Radio Access Network
PLMN: Public Land Mobile Network
PSTN: Public Switched Telephone Network
IMS: IP Multimedia Subsystem

Architectures : Mobile Station I

- User equipment able to connect to the cellular network.
- Includes : a terminal (or equipment), a SIM (Subscriber Identity Module) in 2G or USIM (Universal SIM) in 3G and 4G.
- Terminology : MS (Mobile Station) in 2G and UE (User Equipment) in 3G and 4G.
- Subscriber : entity that receives the service and pays fees.
- SIM : subscriber data, e.g., identity IMSI, location area, authorized services, PID.
- USIM : same as SIM + 3G services access, more memory, more security algos

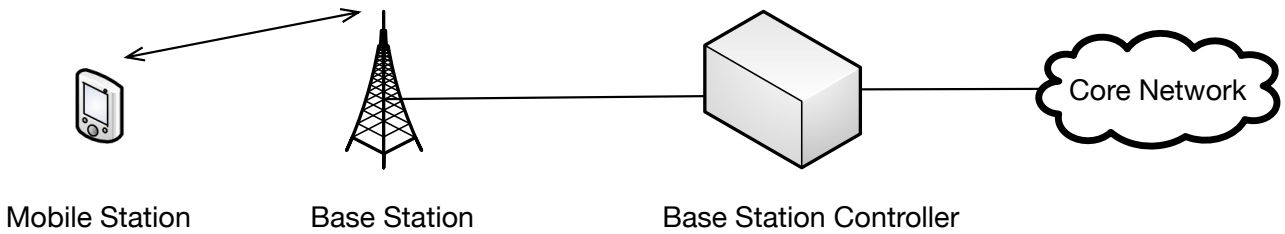


Architectures : Mobile Station II

- Subscribers identities :
  - MSISDN (MS ISDN Number) used to call him (no MSISDN in 4G, IP address).
  - IMSI (International Mobile Subscriber Identity) used by the network (15 digits=3 for country, 3 for network, 10 for subscriber) to uniquely identify the subscriber.
  - TMSI (Temporary Mobile Station Id) used to preserve the privacy of the user on the radio interface.
  - IMEI (Int. Mobile Equipment Id) to uniquely identify the equipment.

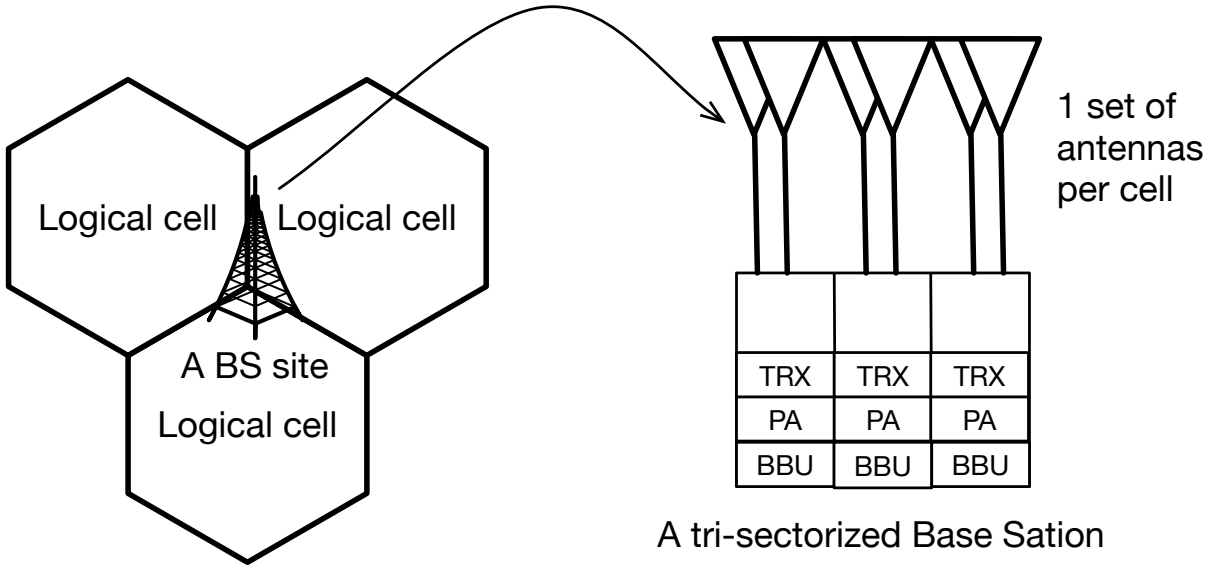
Architectures : Radio Access Network I

- Sub-system responsible for the connection between the MS and the core network.
- Includes : Base Stations (BS), BS controllers, backhaul network (copper lines, micro-waves, optical fibers) and related interfaces.
- Terminology :
  - BSS (Base Station Subsystem) in 2G.
  - GERAN (GSM Edge Radio Access Network) in 2.5G.
  - UTRAN (UMTS Terrestrial RAN) in 3G.
  - E-UTRAN (Evolved-UTRAN) in 4G.



Architectures : Radio Access Network II

Base station terminology :

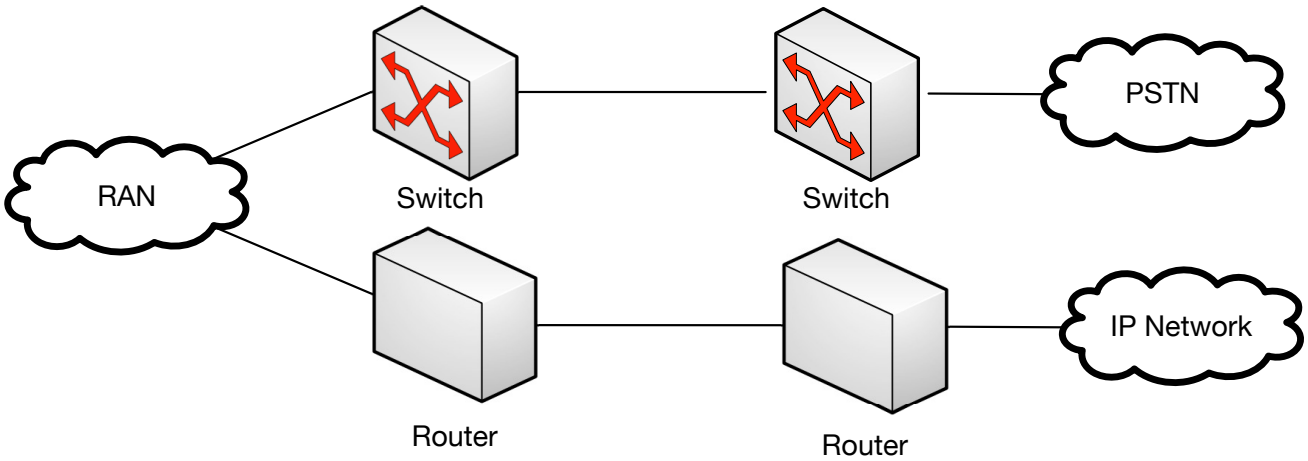


A tri-sectorized Base Sation

TRX: Transmit, receiver chains
PA: Power amplifier
BBU: Base band unit

Architectures : Core Network I

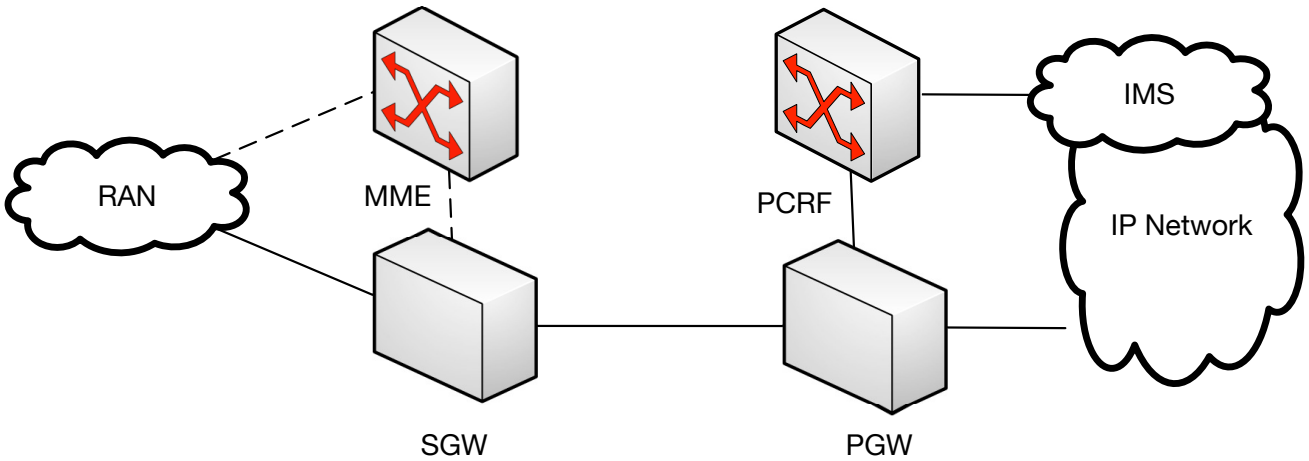
- Subsystem responsible for call switching and message routing towards or from the RAN and for mobility management.
- Includes : Switches (voice circuits), routers (data packets), data bases, backhaul network, and related interfaces.
- Terminology :
  - NSS (Network Switching Subsystem) in 2G.
  - CN (Core Network) in 3G.
  - EPC (Evolved Packet Core) in 4G.



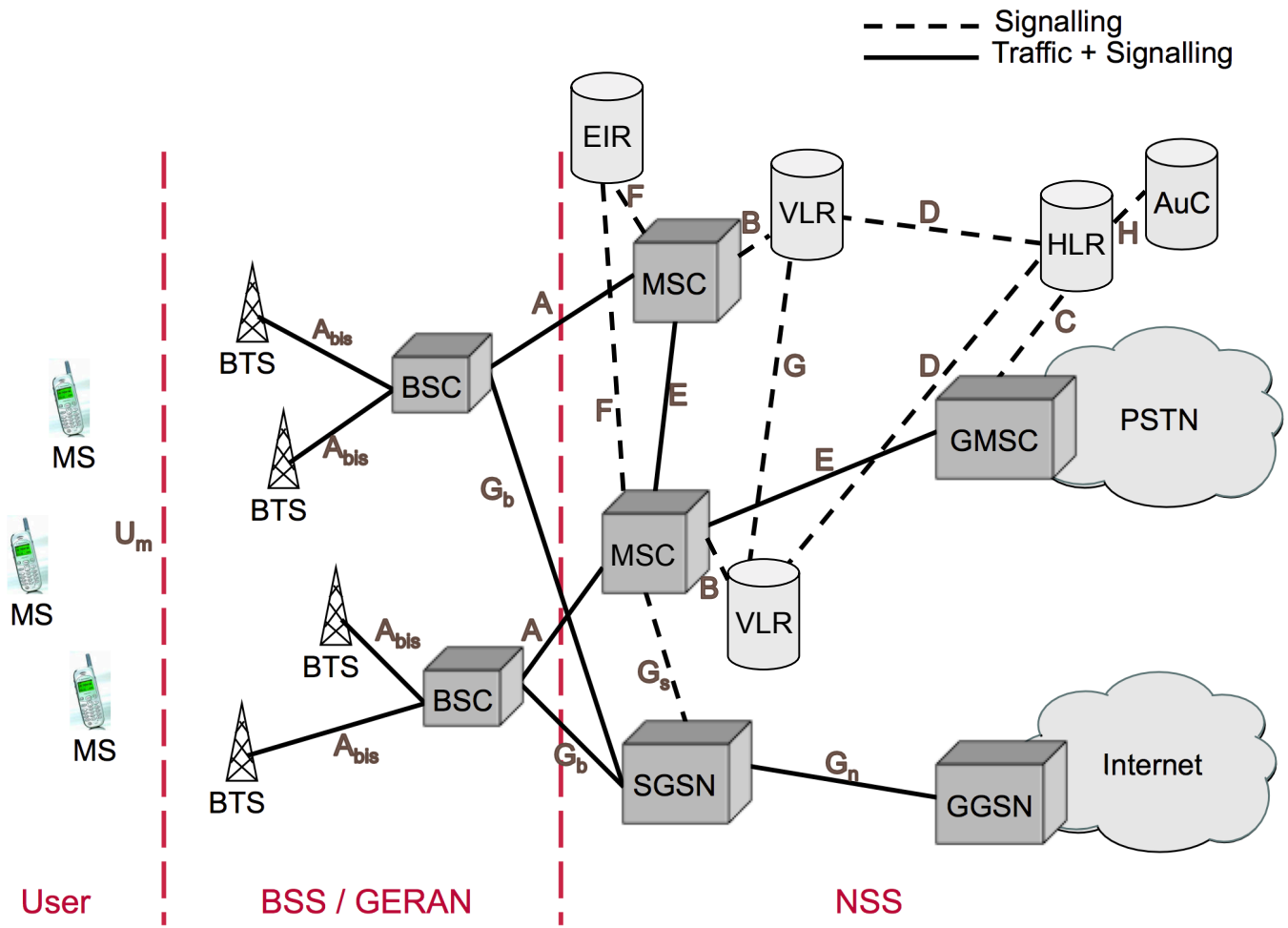
Architectures : Core Network II

New entities in 4G :

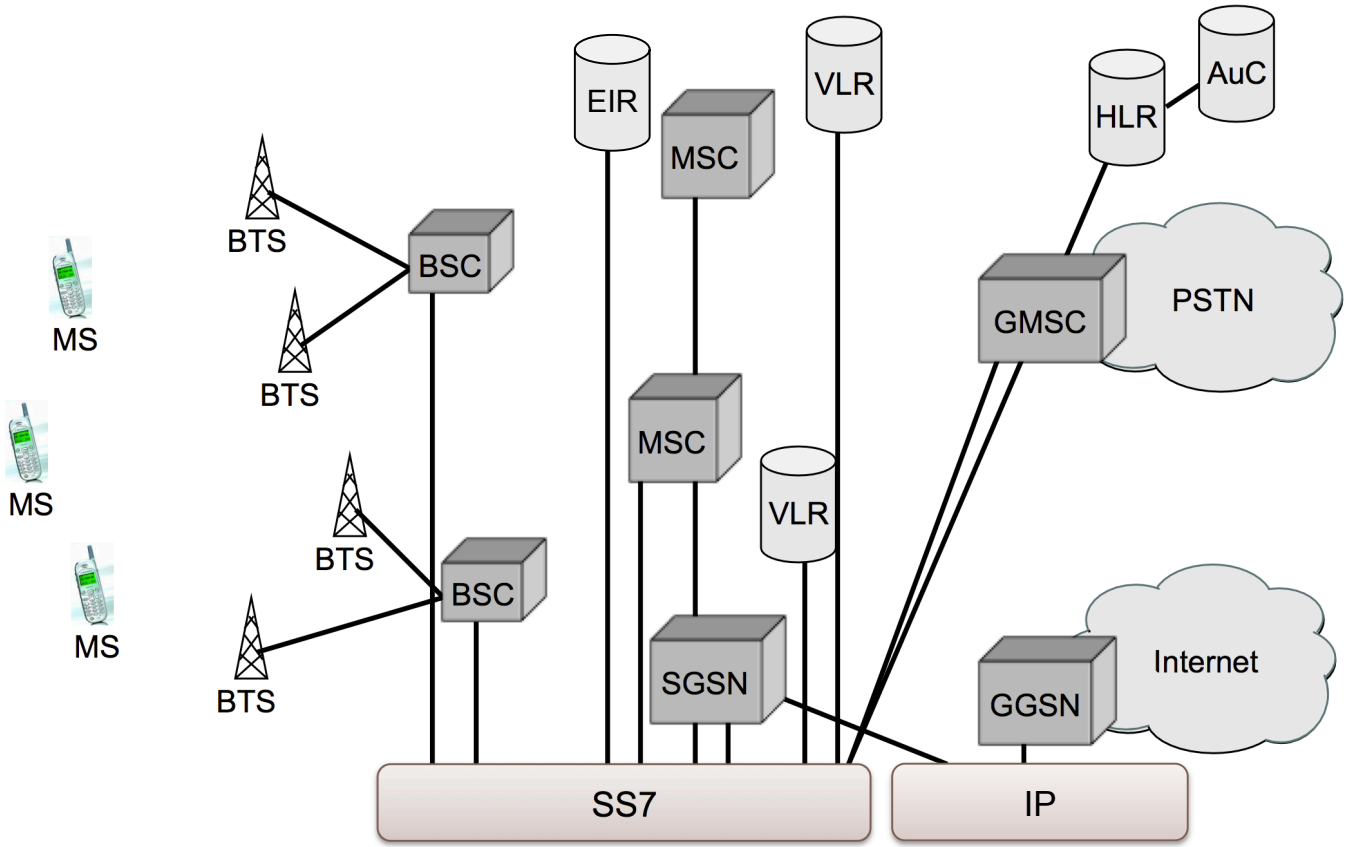
- MME (Mobility Management Entity) : mobility management, security, some handovers.
- PCRF (Policy and Charging Rule Function) : QoS based admission control and pricing.



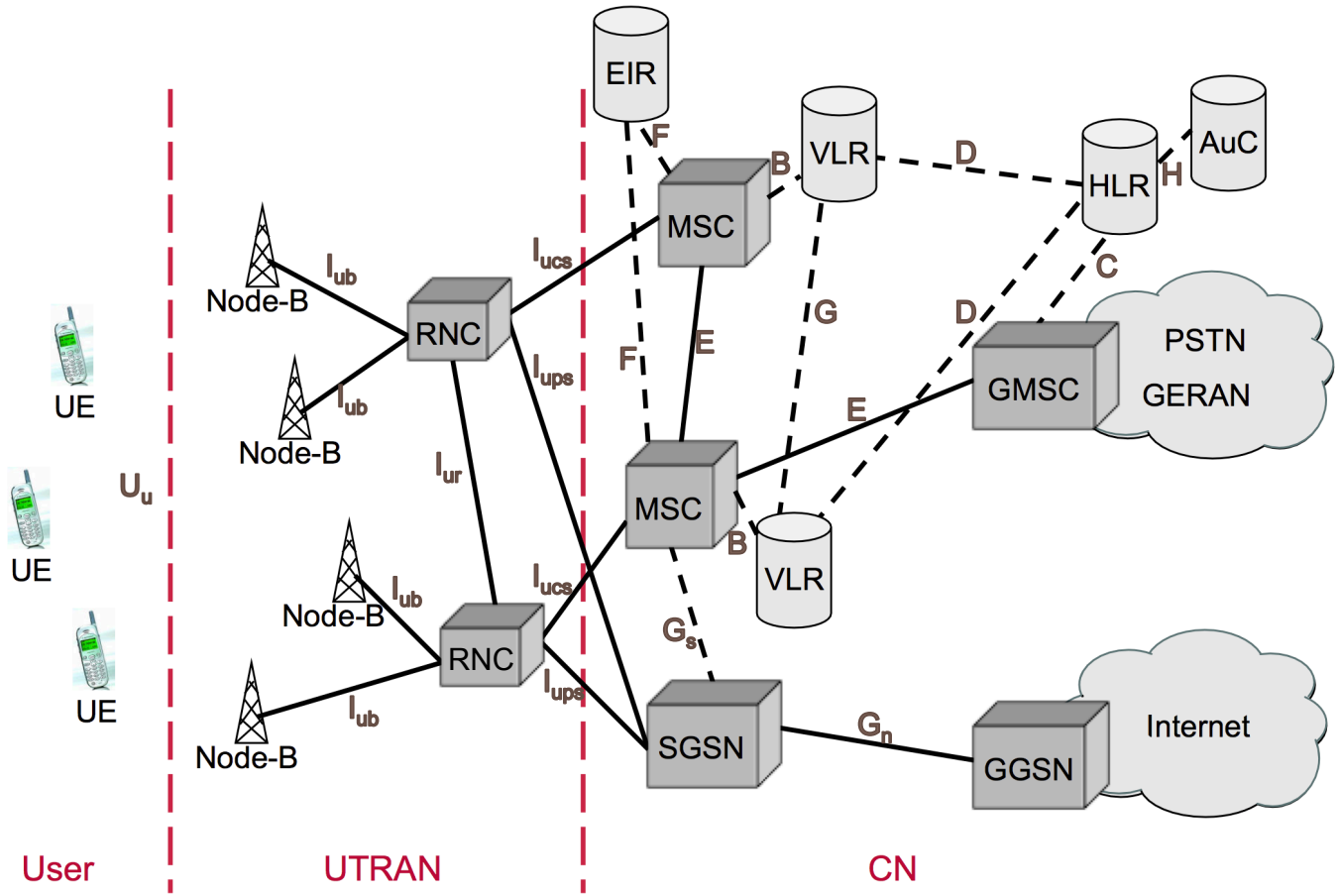
Architectures : 2G I



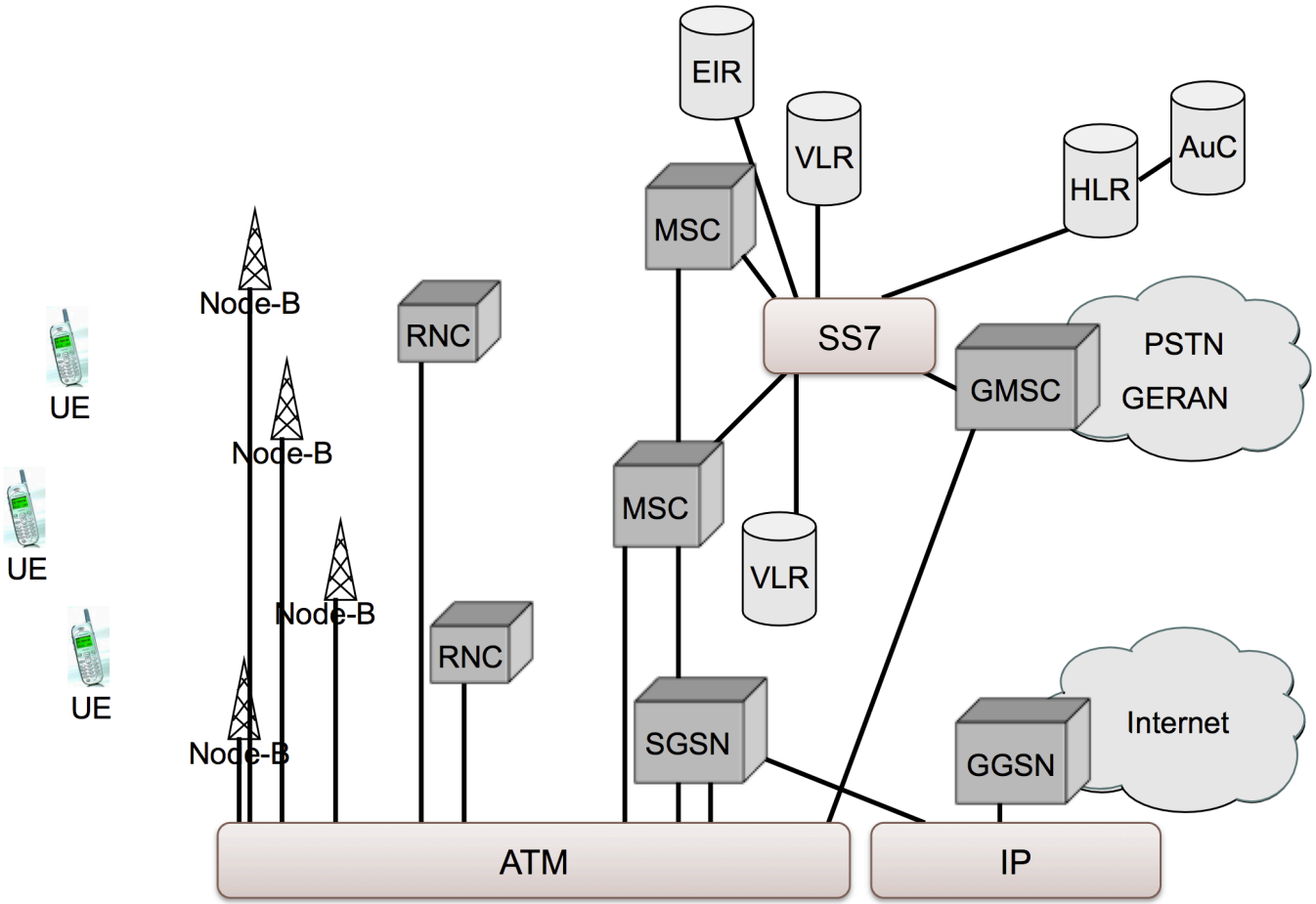
Architectures : 2G II



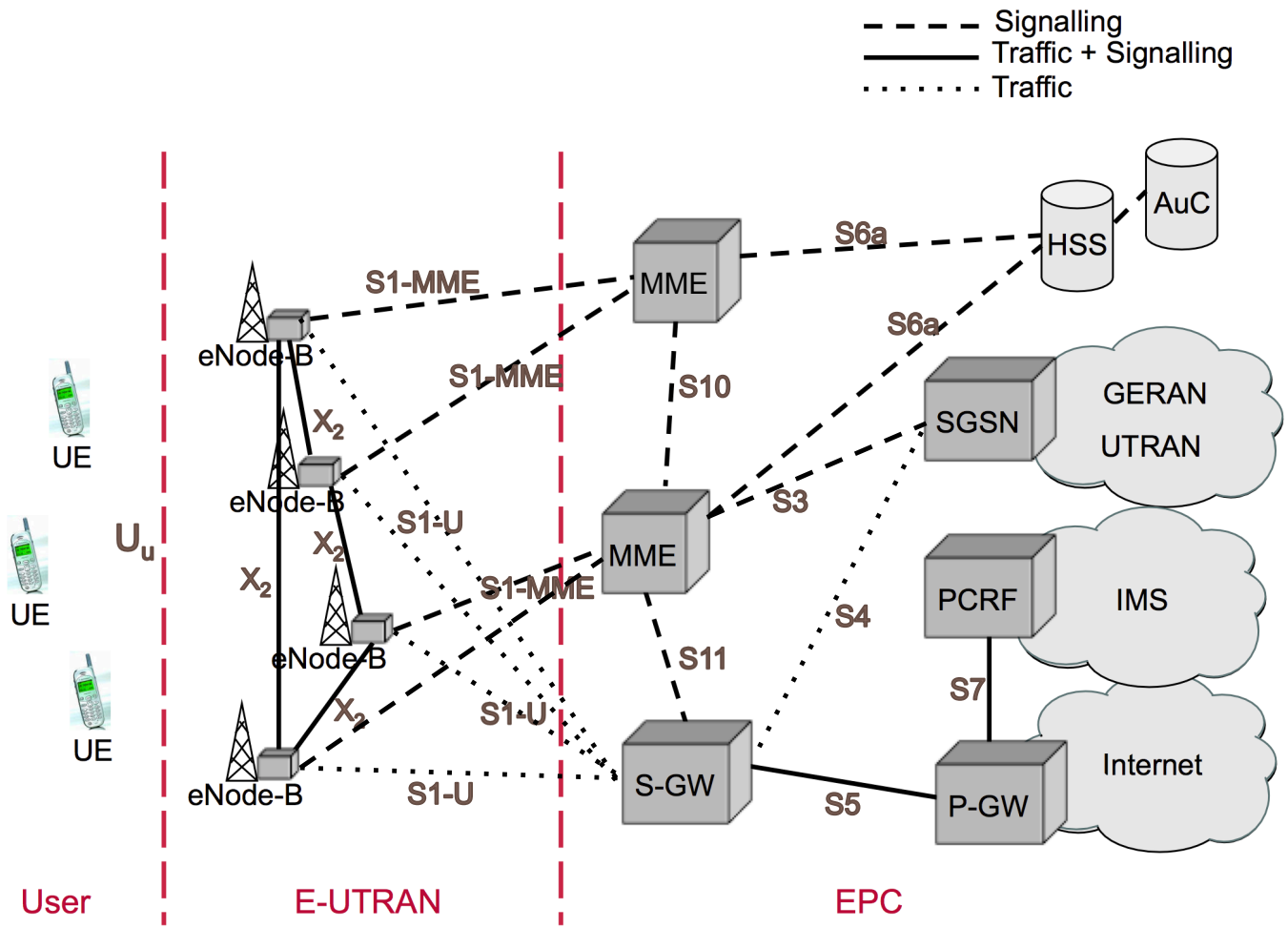
Architectures : 3G I



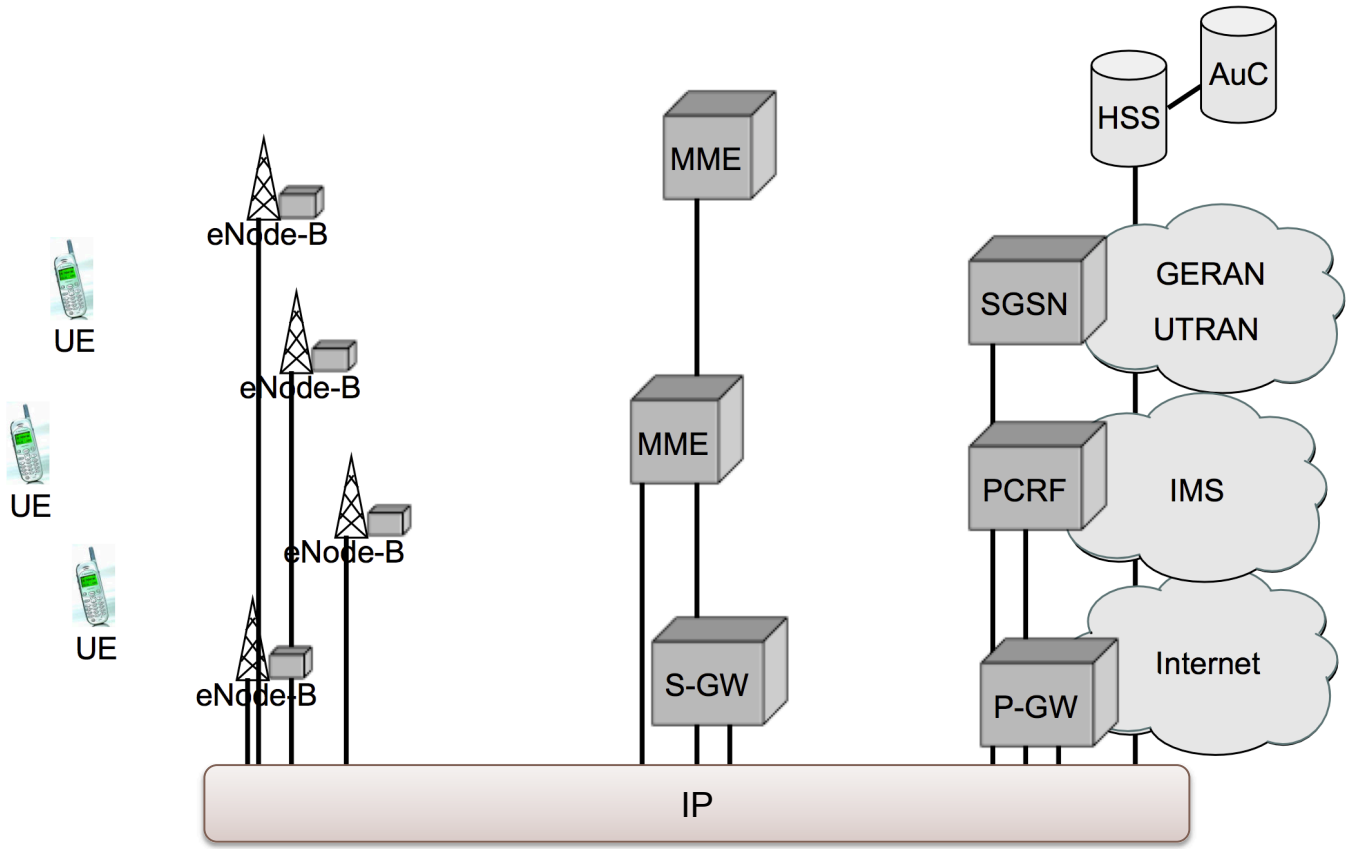
Architectures : 3G II



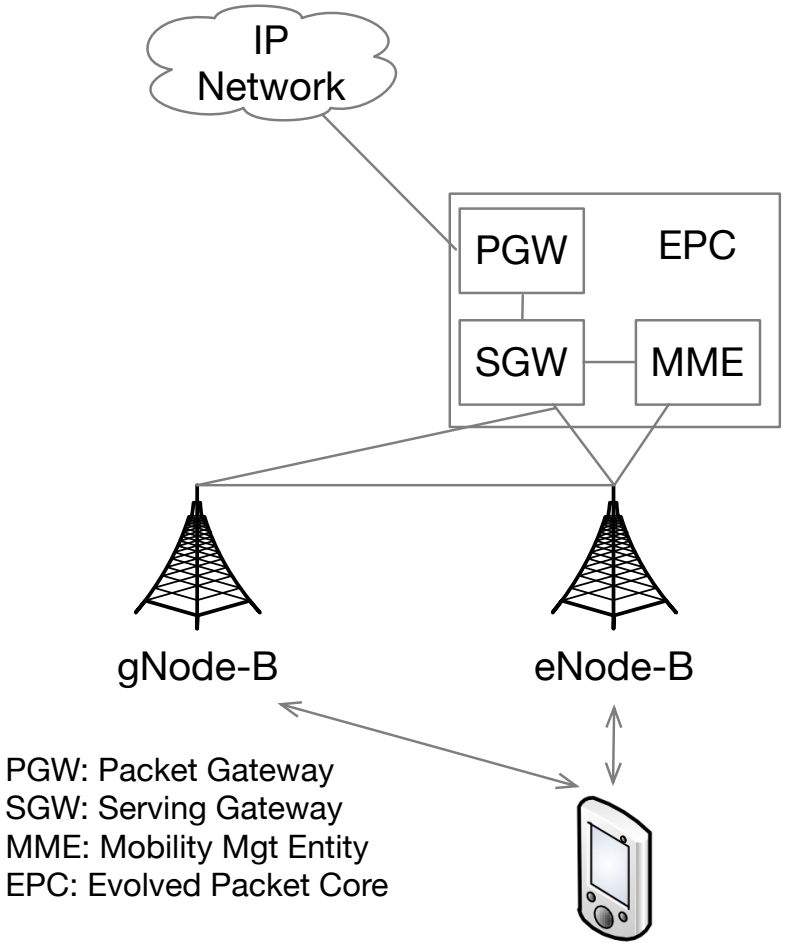
Architectures : 4G I



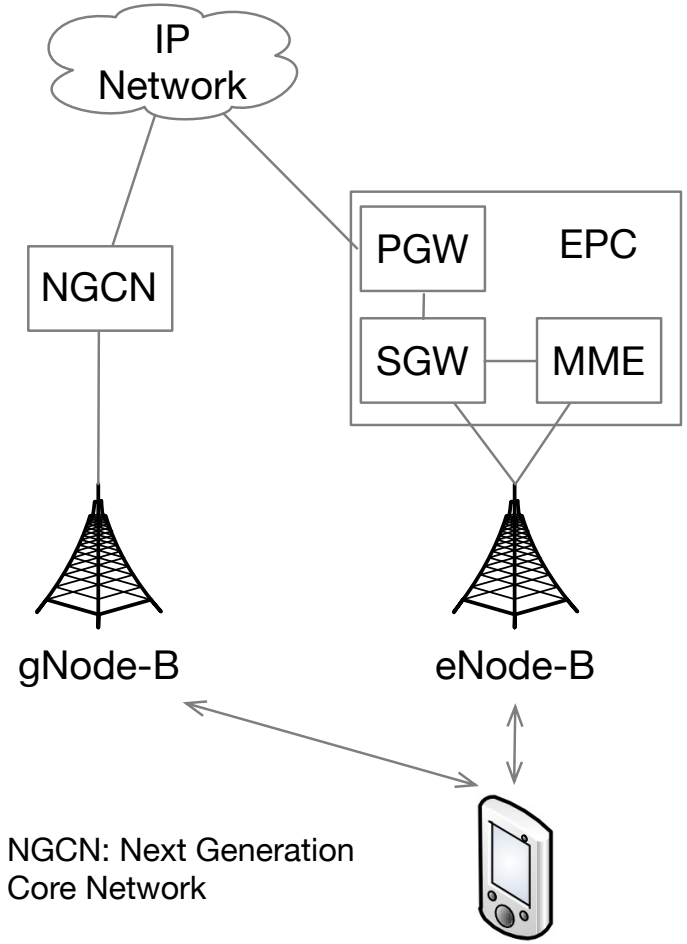
Architectures : 4G II



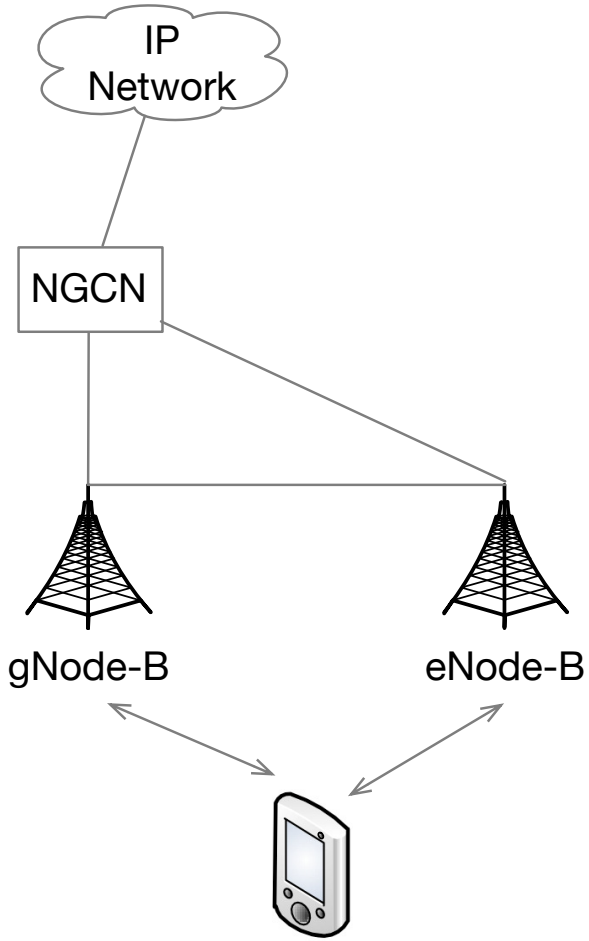
Architectures : 5G Phase 1



Architectures : 5G Phase 2



Architectures : 5G Phase 3



Signaling and control plane I

Signalling is typically performed for access, bearer services and call :

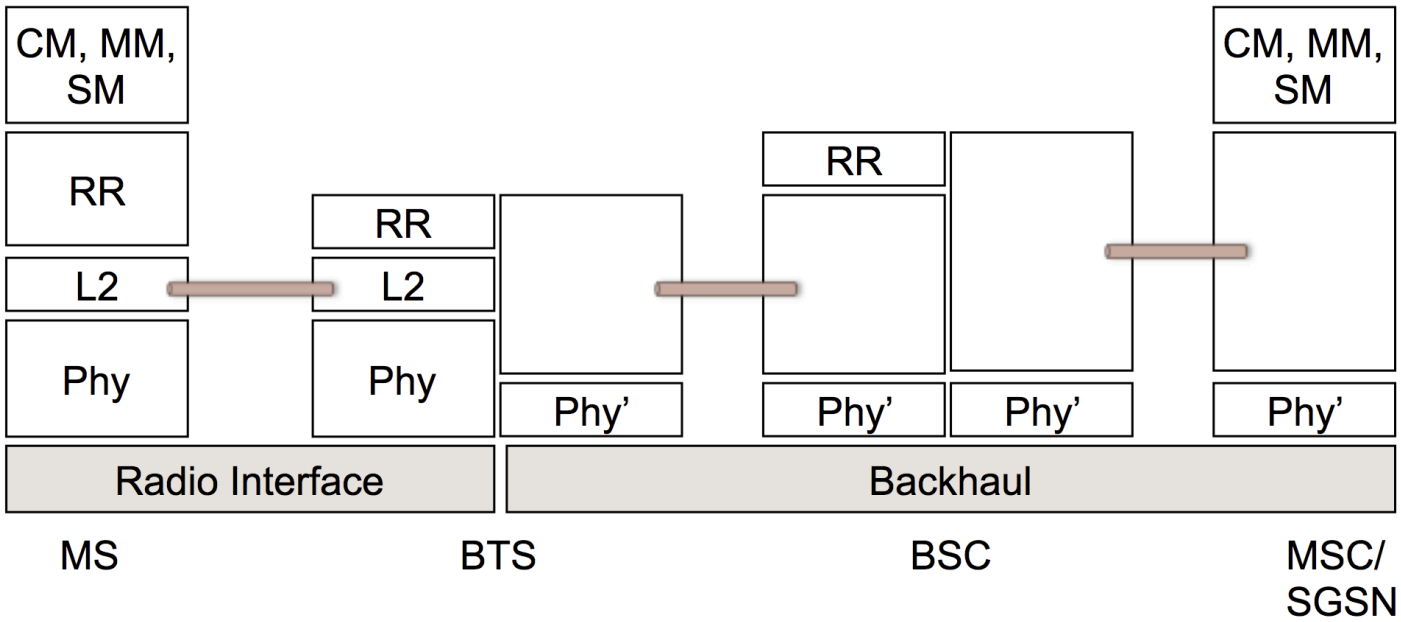
- Access : how to access the network, registration, how to contact a terminal.
- Bearer service : resource allocation on every link between caller and callee.
- Call, connection, session : end-to-end association between participants. Establishment of a global context.

In cellular networks, control plane is made of :

- Radio Resource Control (RR in 2G, RRC after) : resource management, ciphering, link control (power control, measurements), handovers.
- Mobility Management (MM, GMM for packet mobility in 2G, 3G, EMM in 4G) : registration, location update, security (authentication), TMSI allocation.
- Connection Management (CM in 2G, 3G) : call establishment, call control, SMS.
- Session Management (SM, ESM in 4G) : data session establishment.

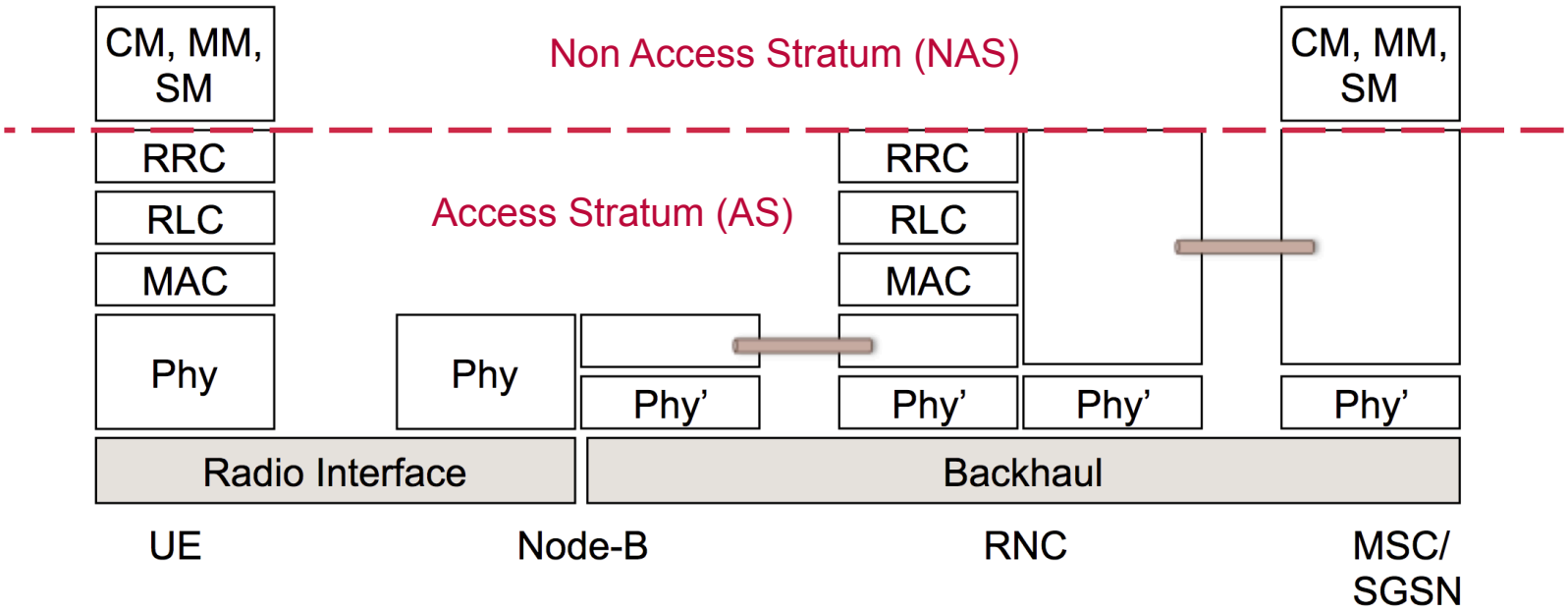
Signaling and control plane II

2G protocol stack (control plane) :



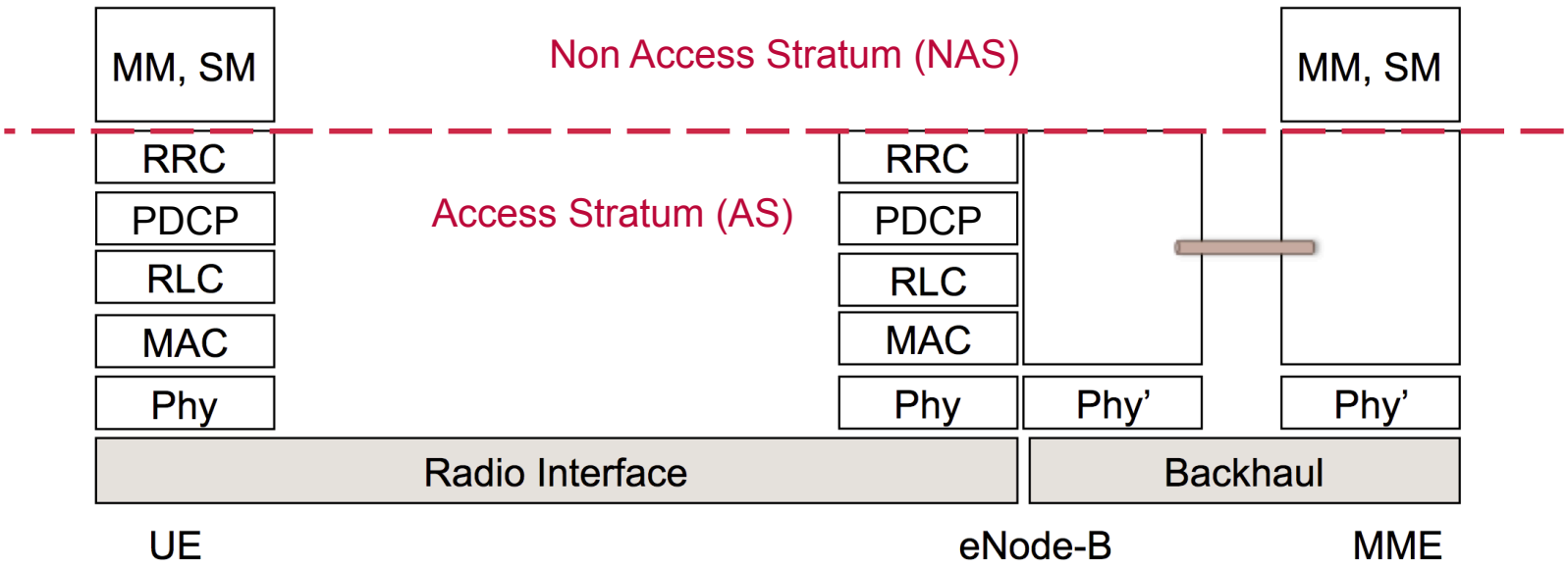
Signaling and control plane III

3G protocol stack (control plane) :



Signaling and control plane IV

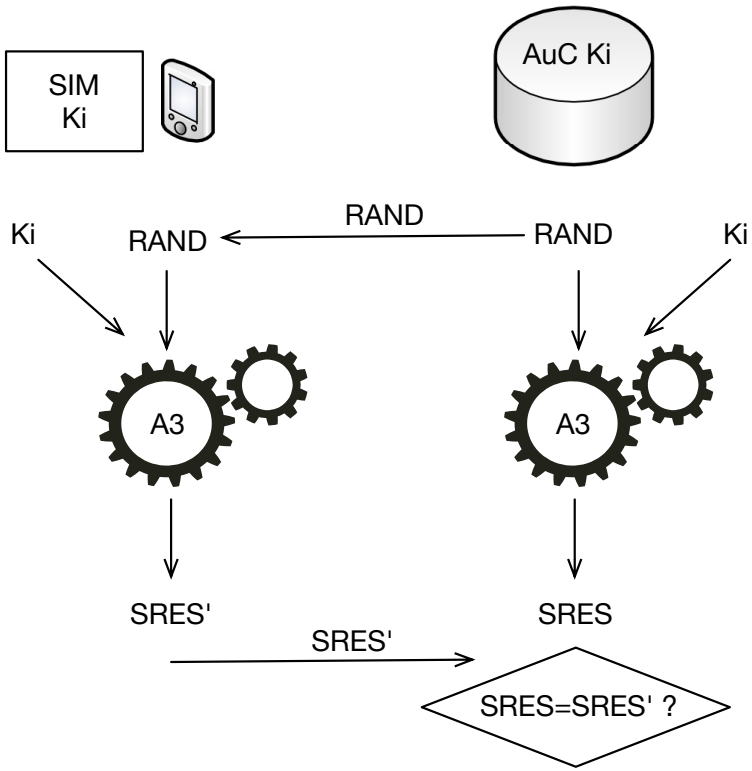
4G protocol stack (control plane) :



Security : Authentication (ex : GSM) I

- Goal : Verify that one really is who one pretends to be
- Thanks to an authentication key Ki which is never sent and stored in the SIM and in the AuC (Authentication Center)
- Authentication of the user in 2G, mutual authentication in 3G, 4G
- Involved equipments are SIM, AuC-MSC in 2G, 3G, AuC-MME in 4G

Security : Authentication (ex : GSM) II

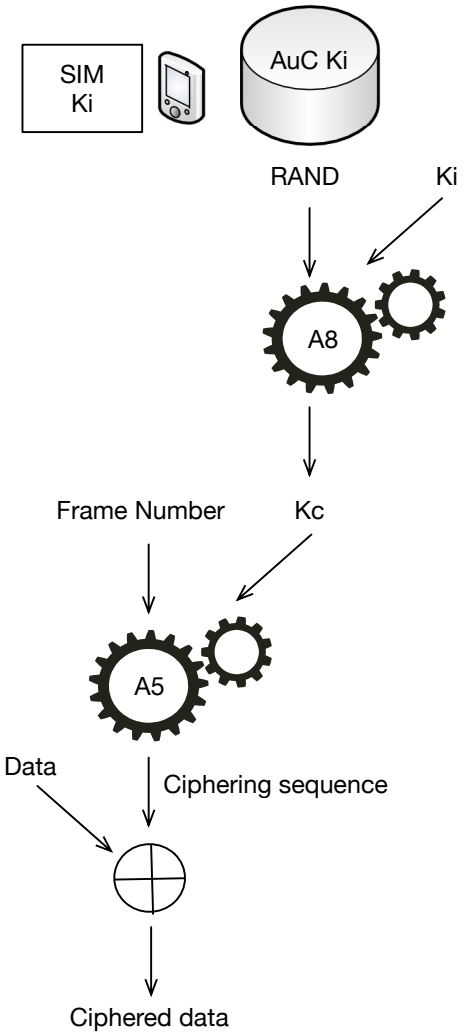


- AuC generates a random number RAND
- AuC computes the result SRES obtained thanks to algorithm A3, key Ki and RAND
- RAND is sent to the user
- The user uses its key Ki stored in the SIM, RAND and algorithm A3 to compute SRES'
- The MSC compares SRES and SRES'

Security : Ciphering (ex : GSM) I

- Signalling and traffic are ciphered on the radio interface.
- There is a new ciphering sequence for every user and every radio frame.
- Ciphering is done at physical layer in 2G, by RRC for 3G signalling, PDCP for 3G traffic and in 4G.
- Involved equipments are SIM, BTS in 2G, SGSN in 2.5G, RNC in 3G, eNode-B in 4G, MSC and MME give the command of ciphering.

Security : Ciphering (ex : GSM) II



- MS and AuC compute the ciphering key Kc thanks to A8, Ki and RAND
- AuC transmits Kc to the BTS
- Every frame is ciphered with A5, Kc and FN
- AuC transmits 3 numbers to the MSC/VLR for authentication and ciphering : RAND, SRES and Kc

Idle Mode : Definition

- No connection with the network.
- No physical channel has been allocated.
- Paging channel is decoded.
- BCCH is decoded for the current cell and neighboring cells.
- Received power is measured for the current cell and neighboring cells.
- The terminal decides itself if the current cell has to be changed (re-selection).
- Its localization is known by the network at location area level.

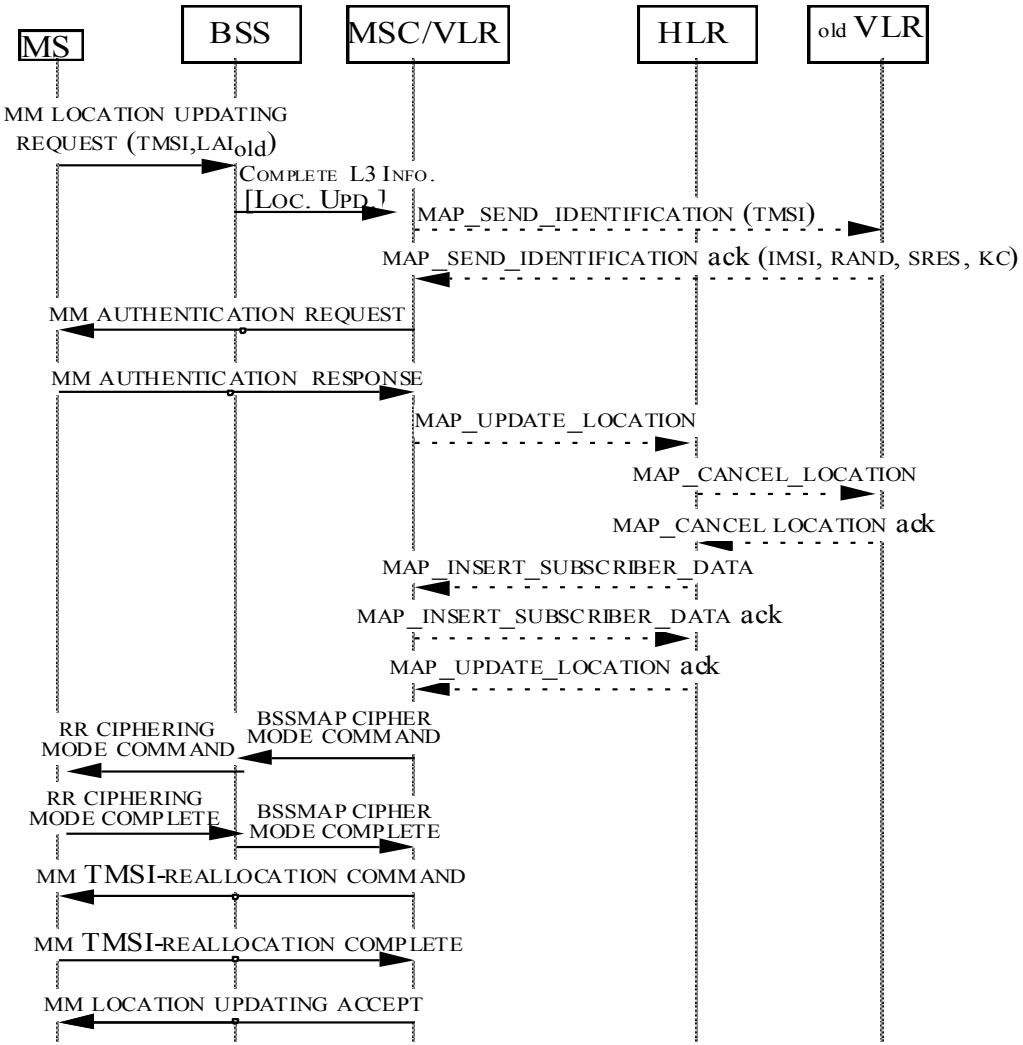
Idle Mode : Registration

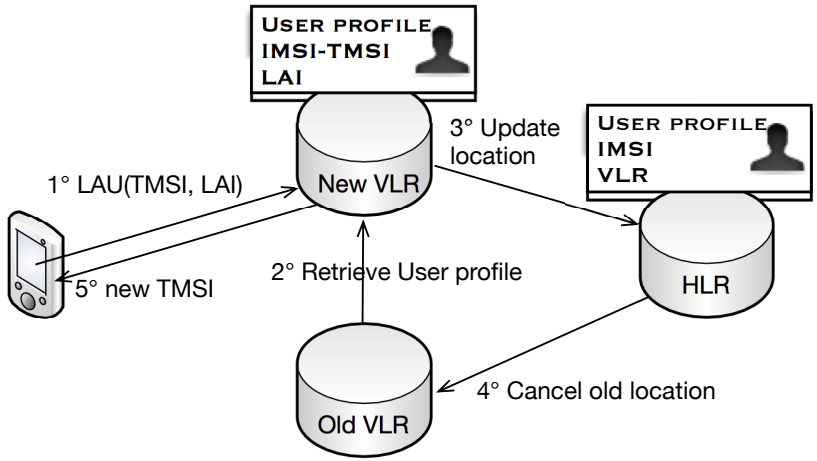
Registration to the network :

1. PLMN selection : based on SIM information or manual (roaming).
2. Cell selection : best cell received with a sufficient power.
3. BCCH decoding : the MS reads the location area id. If the MS has changed its area and periodically, the attachment procedure is launched.
4. Attachment procedure :
   - Location area update (2G-3G).
   - Routing area update (2G-3G).
   - Tracking area update (4G).

- Same VLR : the core network is not involved.
  Different VLR : exchange of informations with the HLR, authentication and ciphering, a new TMSI is allocated.

Idle Mode : Location Area Update

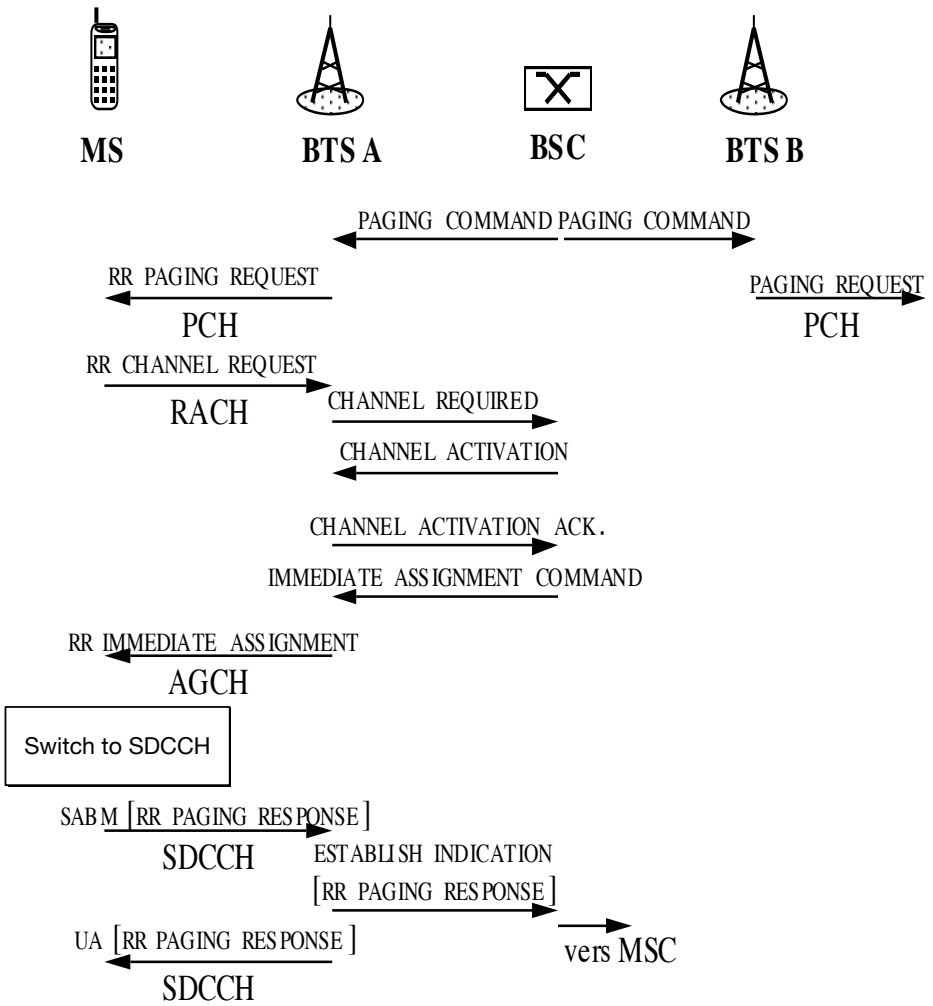


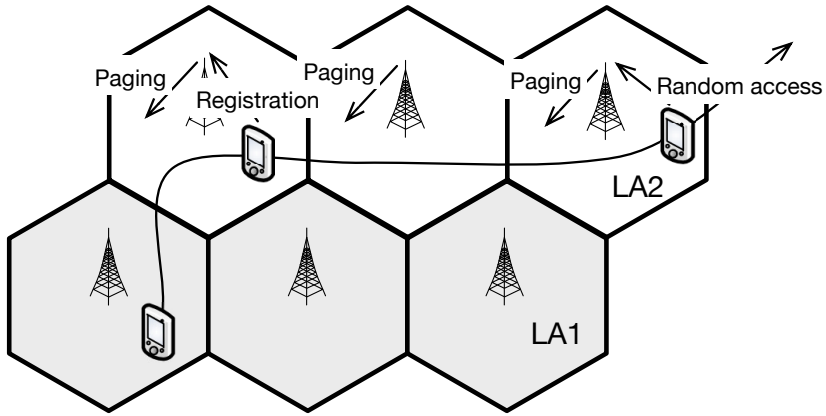


Idle Mode : Paging and Random Access I

- Paging is used for incoming calls or SMS.
- Paging messages include TMSIs of the users who need to be connected.
- They are sent by all BS of the location area.
- Upon reception of a paging message destined to it, the user performs a random access, which includes the reason of the access (here : paging response).
  In 3G-4G, random access asks for a RRC connection.
- Discontinous reception : based on their TMSIs, users decodes only a subset of paging messages.

Idle Mode : Paging and Random Access II

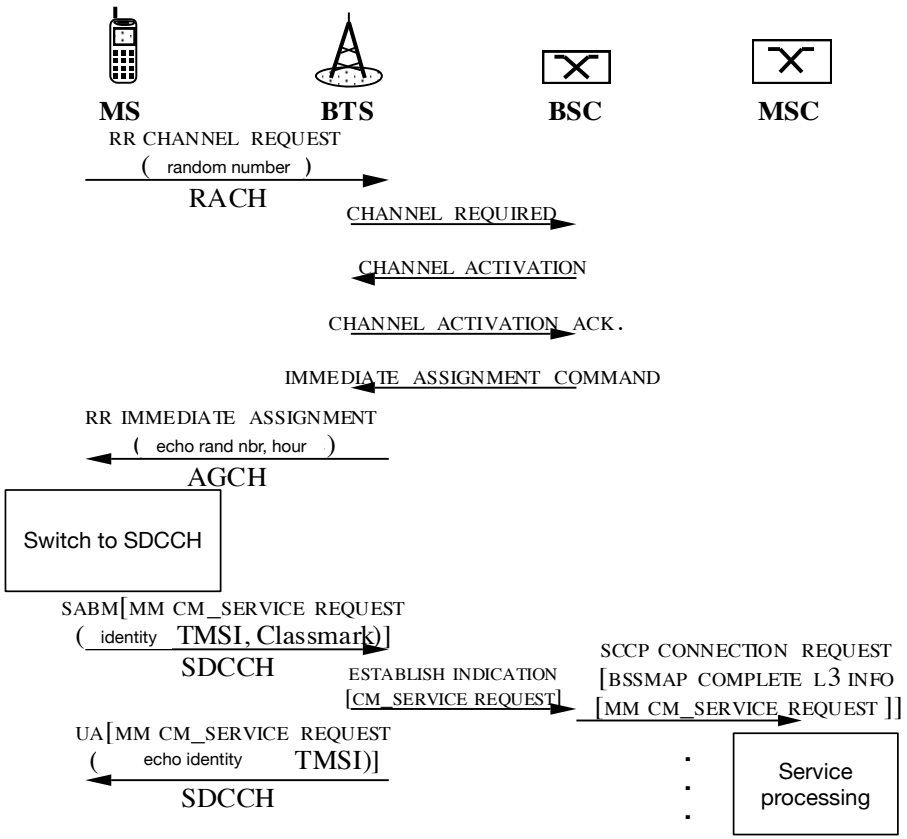




Connected Mode : Definition

- There is a connection with the network : L2 in 2G, RRC in 3G-4G.
- At least one signalling dedicated logical channel has been allocated : SDCCH in 2G, Signalling Radio Bearers in 3G-4G.
- There is a dedicated or shared physical channel for this user.
- The exchange of dedicated signalling (MM, CM, SM) or user traffic is possible.
- Received power level is measured in the current cell and in neighboring cells.
- Measurement reports are periodically sent to the current cell.
- The network decides if a handover is required.
- Localization is known by the network at cell level.

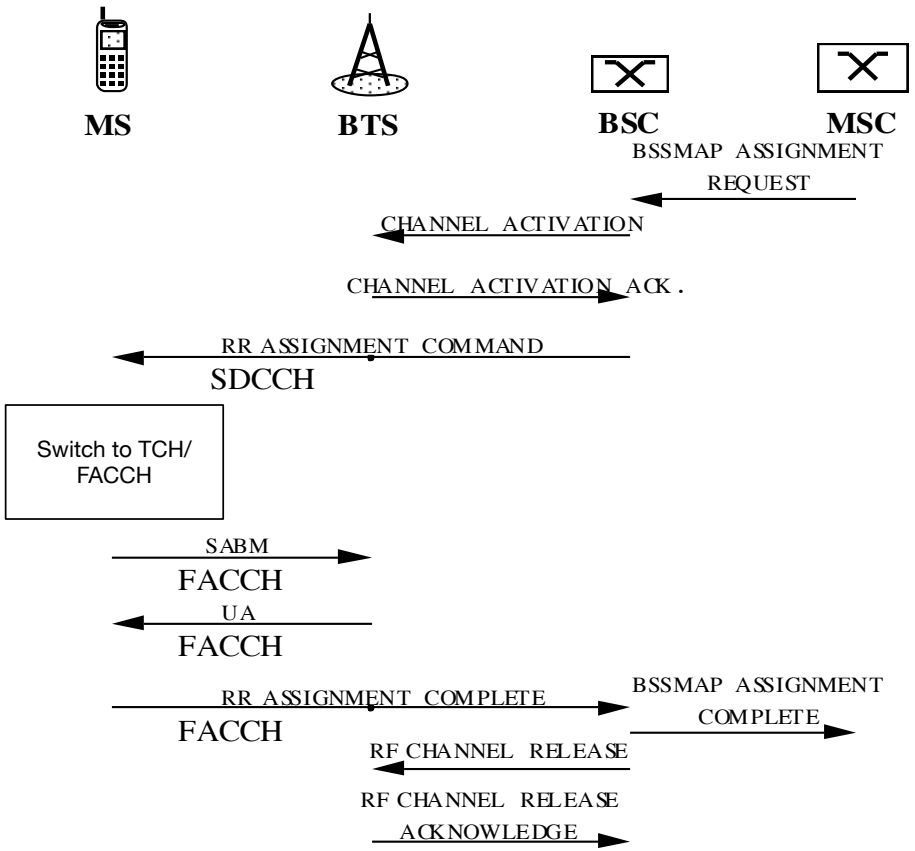
Connected Mode : Resource Allocation I



Signalling resource allocation

1. Random access.
2. Resource allocation decided by the BSC.
3. Random access response.
4. Service demand : connection reason, TMSI and classmark are transmitted.
5. Demand is acknowledged and processed by the MSC.

Connected Mode : Resource Allocation II



Traffic resource allocation

1. The MSC requests the allocation of a traffic channel.
2. The BSC activates a traffic channels in the BTS.
3. The BSC sends a command to switch to the traffic channel.
4. The MS leaves the SDCCH for the TCH/FACCH.
5. The MS informs the BSC and the BSC informs the MSC about the switch.
6. Signalling resources are released.

Cell selection : Suitable cells

1. PLMN selection : done by the NAS based on a list stored in the SIM, may be also manual
2. Cell selection : done by AS, find a cell in the selected PLMN, not barred, and received with sufficient power
3. Registration and location area update (2G), routing area update (2G-3G) or tracking area update (4G)

Cell selection : Power criterion I

Downlink :

- Received power margin = Received power - Min required power [dB]
- Margin > 0 : DL has enough quality, Margin < 0 : the MS is not covered
- Received power on BCCH : RXLEV in 2G, Qrxlevmeas in 3G-4G
- Min required power : broadcast by the BCCH, RXLEV_ACCESS_MIN in 2G, Qrxlevmin in 3G-4G

Uplink :

- Power deficit = Max authorized power - Terminal max transmit power [dB]
- Power deficit < 0 : UL is OK, Power deficit > 0 : UL may not be OK
- Max authorized power : broadcast by BCCH, MS_TXPWR_MAX_CCH in 2G, UE_TxPwr_Max_RACH in 3G, PEMAX_H in 4G
- Terminal max transmit power : defined by the manufacturer, P in 2G, P_Max in 3G, PPowerClass in 4G

Power criterion :

- C = Received power margin - max(Power deficit, 0) (C1 in 2G, Srxlevel in 3G-4G)
- The cell is suitable if $C > 0$

Cell selection : Power criterion II

Explanation :

- If Received power margin < 0 : DL is not covered and C < 0
- If Received power margin > 0 and power deficit < 0 : UE covered and C > 0
- If Received power margin > 0 and power deficit > 0, the UE is covered if :

$$\begin{aligned} P_{Tx}^{UE} - PL &> S \\ PL_{max} - PL + P_{Tx}^{UE} - PL_{max} &> S \\ RPM + P_{Tx}^{UE} - (P_{Tx}^{max} - S) &> S \\ RMP - PD &> 0 \end{aligned}$$

where P_{Tx}^{UE} is the UE max power, P_{Tx}^{max} is the max authorised power, PL_{max} is the path-loss at cell edge, S is the required min power at BS and we have $P_{Tx}^{max} - PL_{max} = S$.

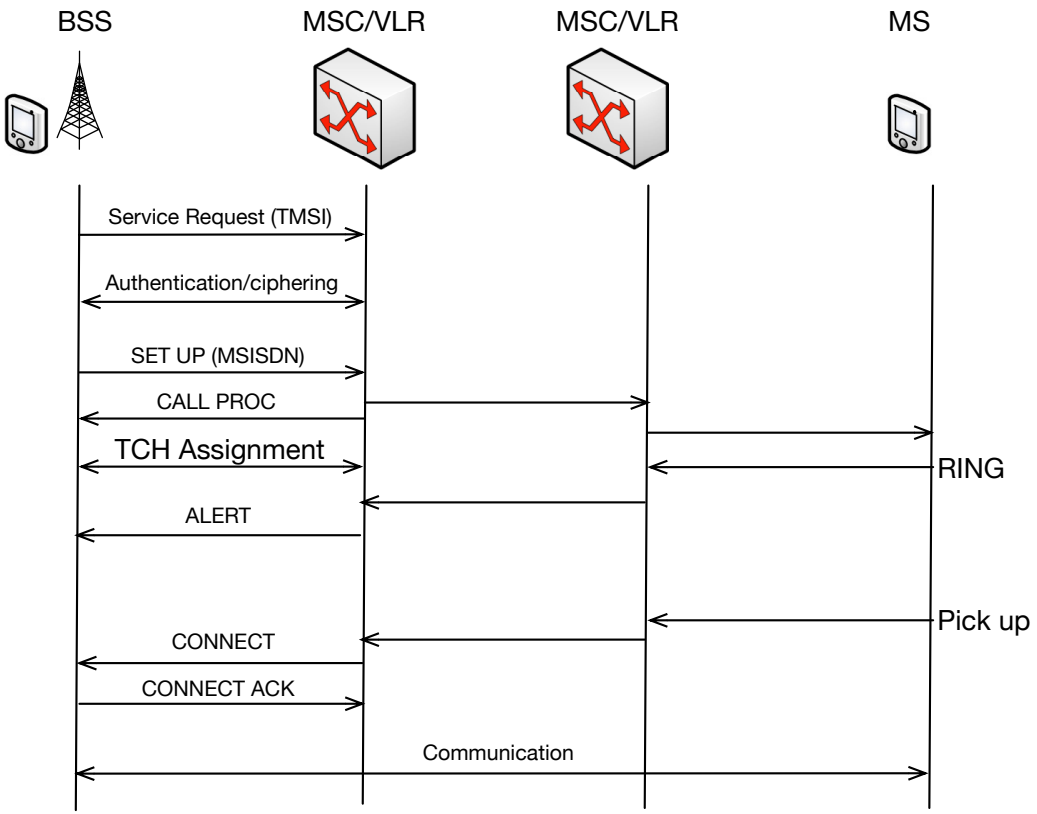
Cell reselection I

- In idle mode, the MS may change its current cell ; the decision algorithm is standardized and performed by the MS based on signal strengths and cell priorities
- Cells are ranked according to a reselection criteria (C2 in 2G, R in 3G-4G)
- Priorities : cell specific offsets are broadcast to give priorities to the cells, e.g., C2 = C1 - CELL_RESELECT_OFFSET
- Temporal aspects : new cell priorities are decreased for a certain duration to avoid reselecting a cell in which the MS won't stay too long (think about a vehicle traversing a small cell), e.g., C2 = C1 - CELL_RESELECT_OFFSET - TEMPORARY_OFFSET
- Hysteresis aspects : offsets are used to avoid too many reselections between neighboring cells or location areas, e.g., C2 = C1 - CELL_RESELECT_OFFSET - CELL_RESELECT_HYSTERESIS
- A new cell is selected if C1newcell $>$ 0 and C2newcell $>$ C2oldcell

Cell reselection II

- Measurement thresholds : if the current cell is received with sufficient power, there is no need to perform measurements on neighboring cells (3G-4G), measurements are performed only if the power level is below some threshold, thresholds are broadcast by the BCCH
- Mobility : 4G terminals count the number of reselections per second and estimate its mobility thanks to thresholds. In high and moderate mobility, hysteresis of the current cell and reselection time are increased

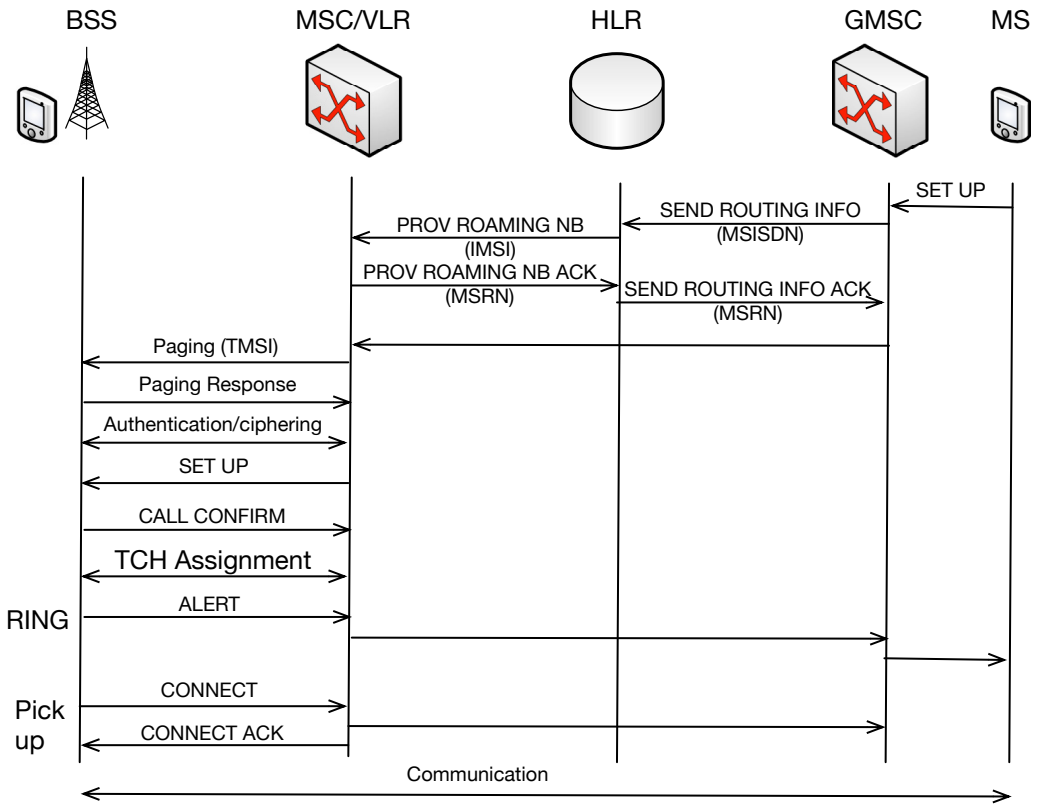
Originating call



Originating call steps :

1. Service request
2. Authentication and ciphering
3. Call setup (with callee phone number)
4. Traffic channel establishment
5. Call alert, ringing
6. Pick up

Terminating call I



Terminating call steps :

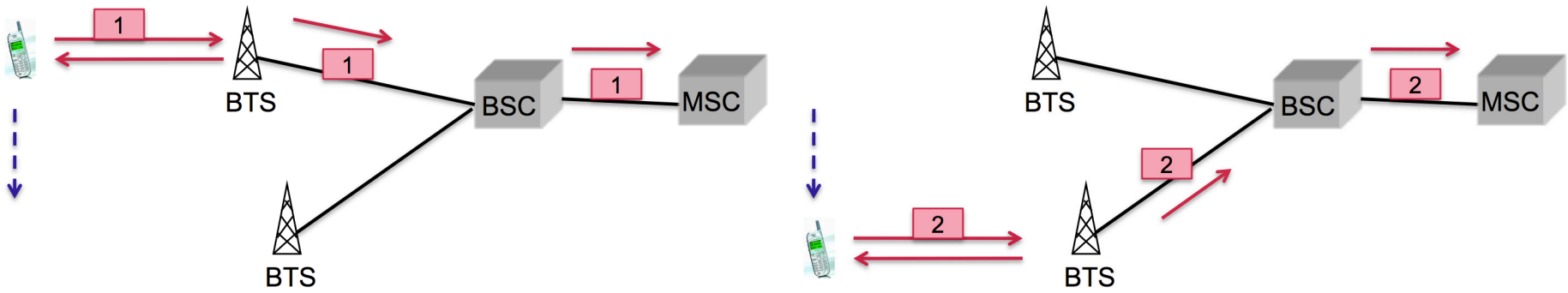
1. Routing information exchange for GMSC-MSC communication
2. Paging with TMSI, paging response
3. Authentication and ciphering
4. Call setup is forwarded to the MS
5. Traffic channel establishment
6. Call alert, ringing
7. Pick up

Handover : Definitions I

- Handover = mobility in connected mode
- Handover is activated when the MS is away from its cell (signal quality is poor) or for load balancing reasons (the communication is pushed to another cell, another band or another RAT).
- Vertical handover : inter-RAT handover, e.g., 4G to 3G.

Handover : Definitions II

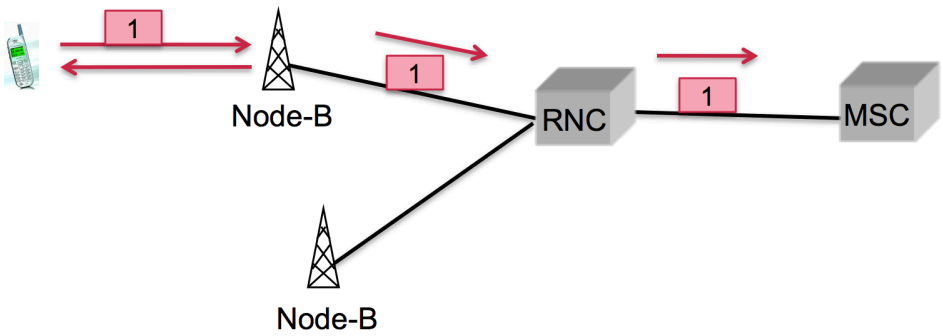
Hard handover :

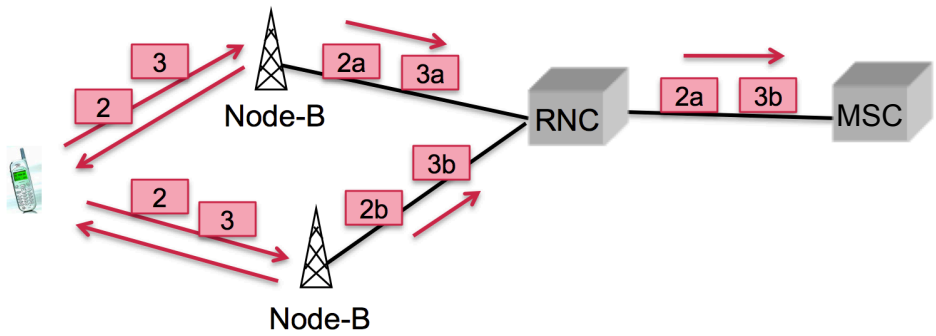


- The communication is interrupted : in 2G, for vertical handovers, for inter-frequency handovers in 3G and in 4G.

Handover : Definitions III

Soft handover :

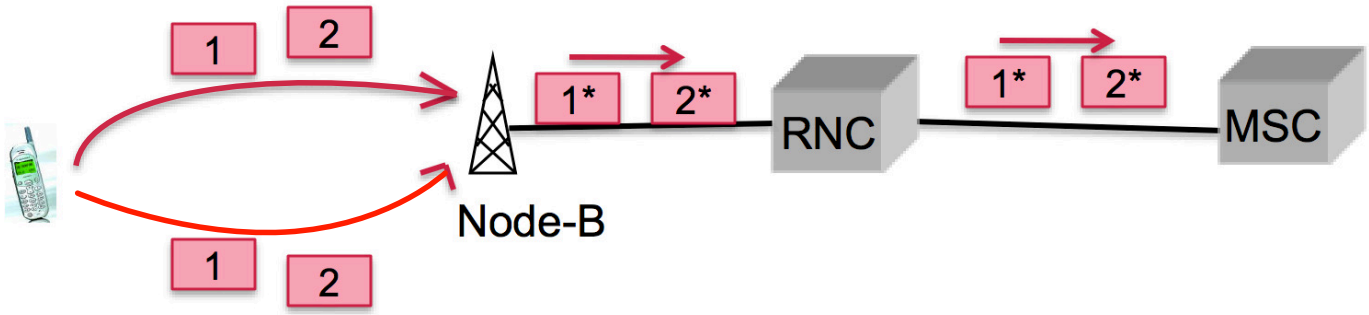




- The communication is not interrupted and frames are received (resp. transmitted) from (resp. to) several base stations. The RNC performs selection combining, i.e., chooses the frame with the best quality. Done in 3G.

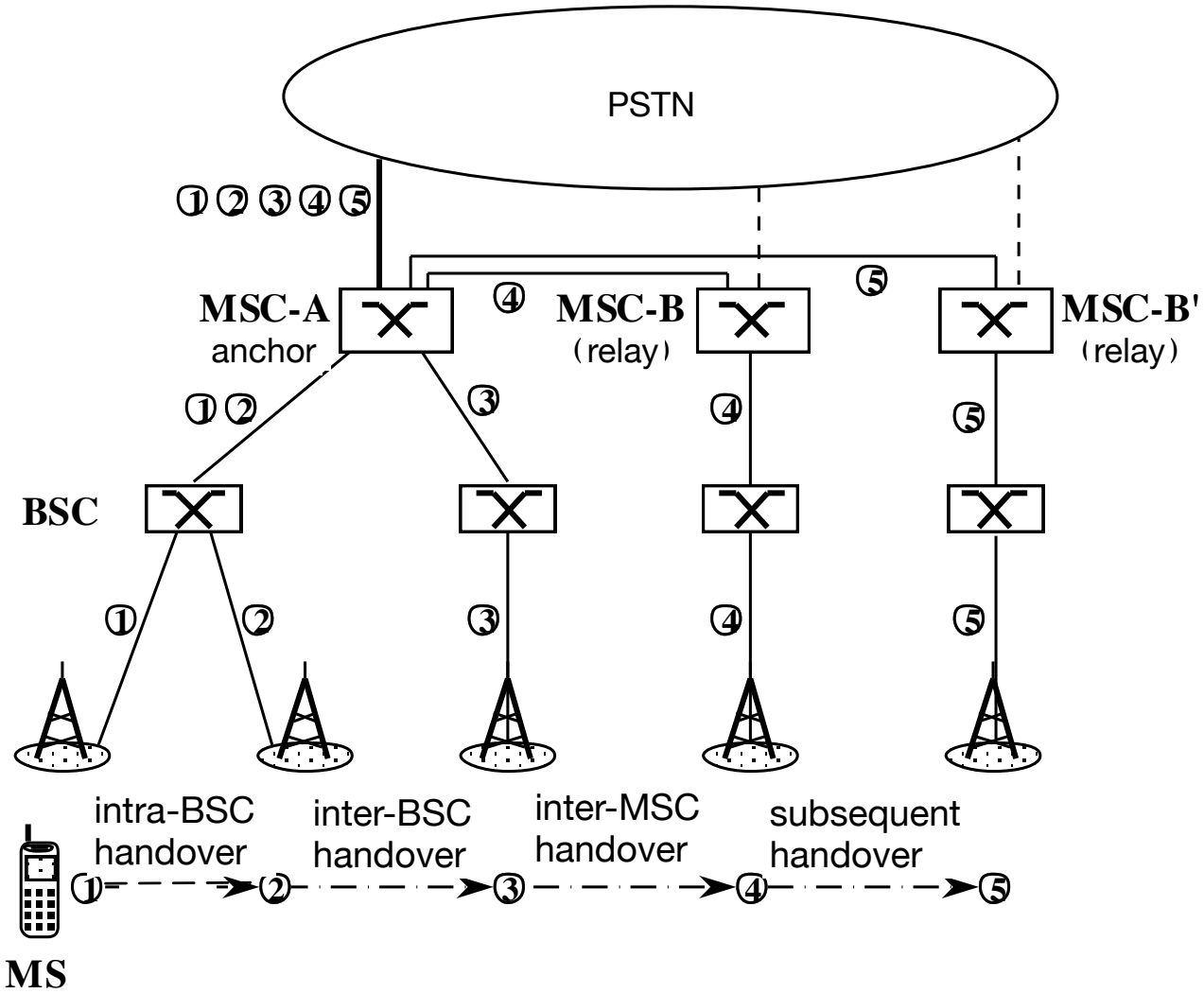
Handover : Definitions IV

Softer handover :

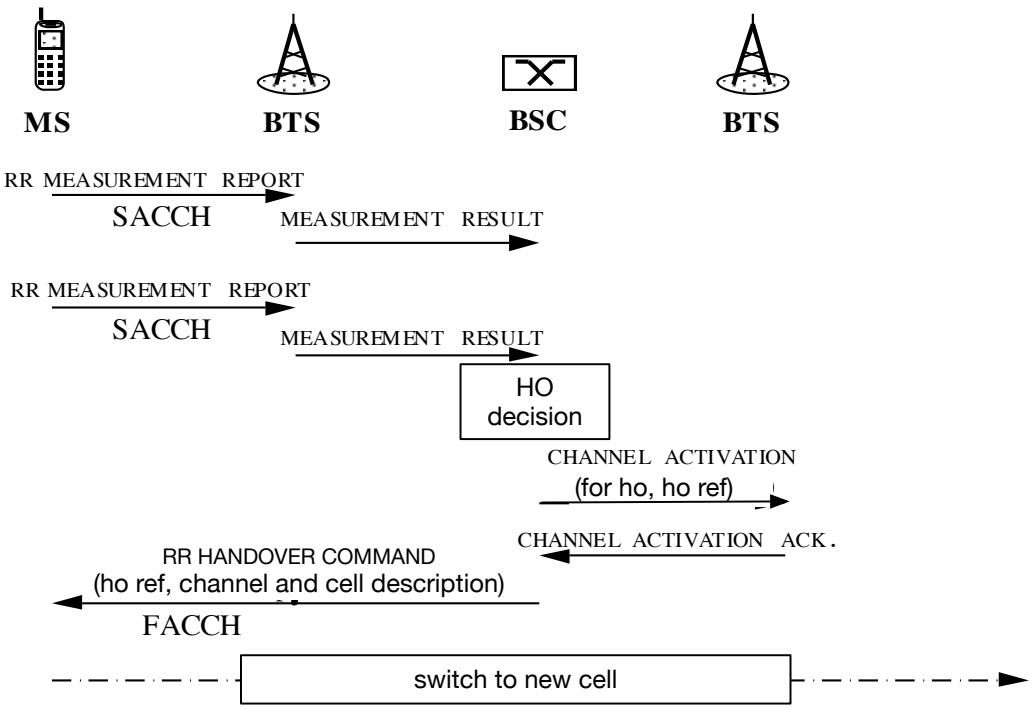


- The MS moves from one cell to another belonging to the same Node-B. Maximum ratio combining is performed at the base station and the combination is sent to the RNC. Done in 3G.

Handover : 2G I



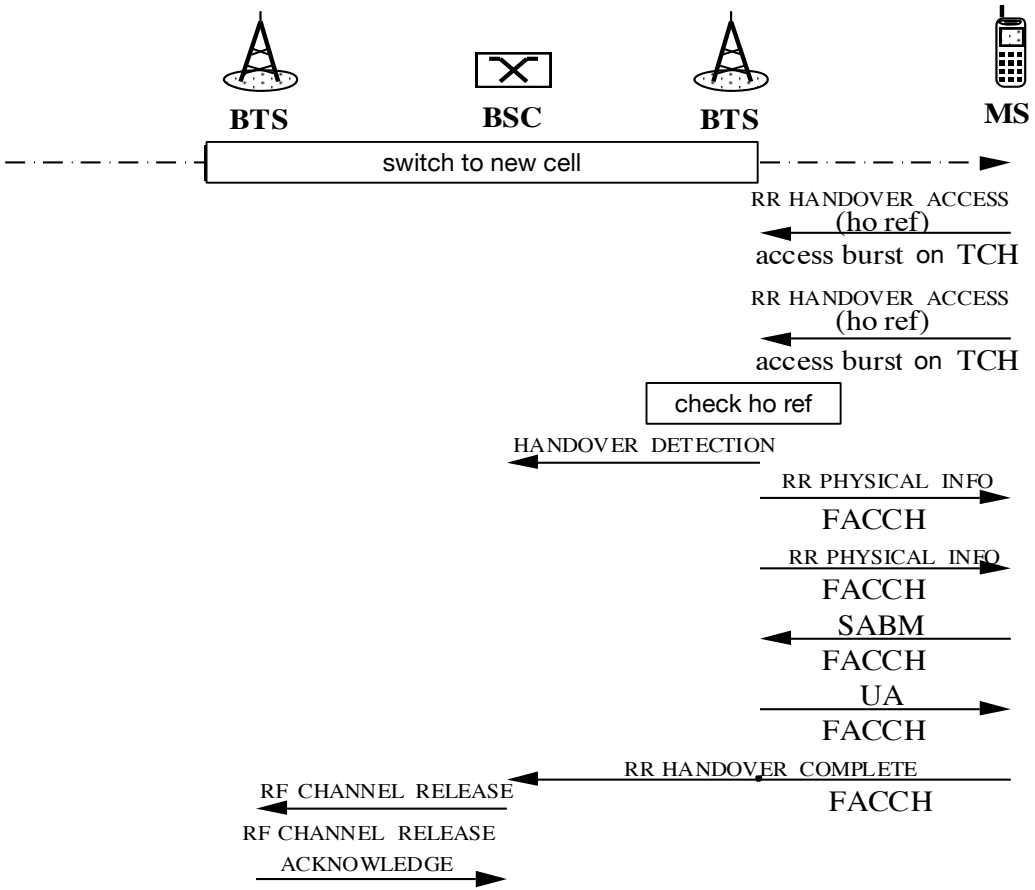
Handover : 2G II



Intra-BSC handover :

- HO decision and resource reservation are done by the same BSC
- The BSC commands the activation of a channel in the target cell
- HO order : reference of the HO, description of the physical channel in the new cell, characteristics of the new cell (BCCH frequency, BSIC, etc), transmit power and TA to use if possible, a ciphering command

Handover : 2G III

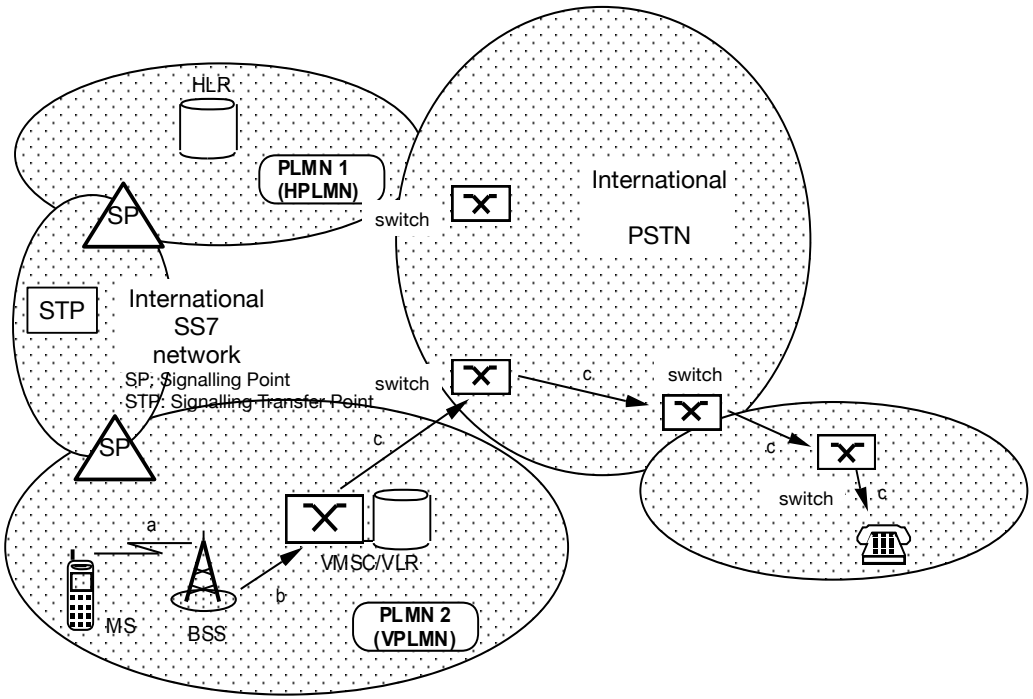


- Arrival in the new cell
- Random access on the TCH if the TA is not known (until a response is received), the access burst is used to estimate the TA, BSC is informed
- The TA to be applied is transmitted on the FACCH (unnumbered frame)
- Resources are released in the old cell by the BSC

Roaming : Definitions

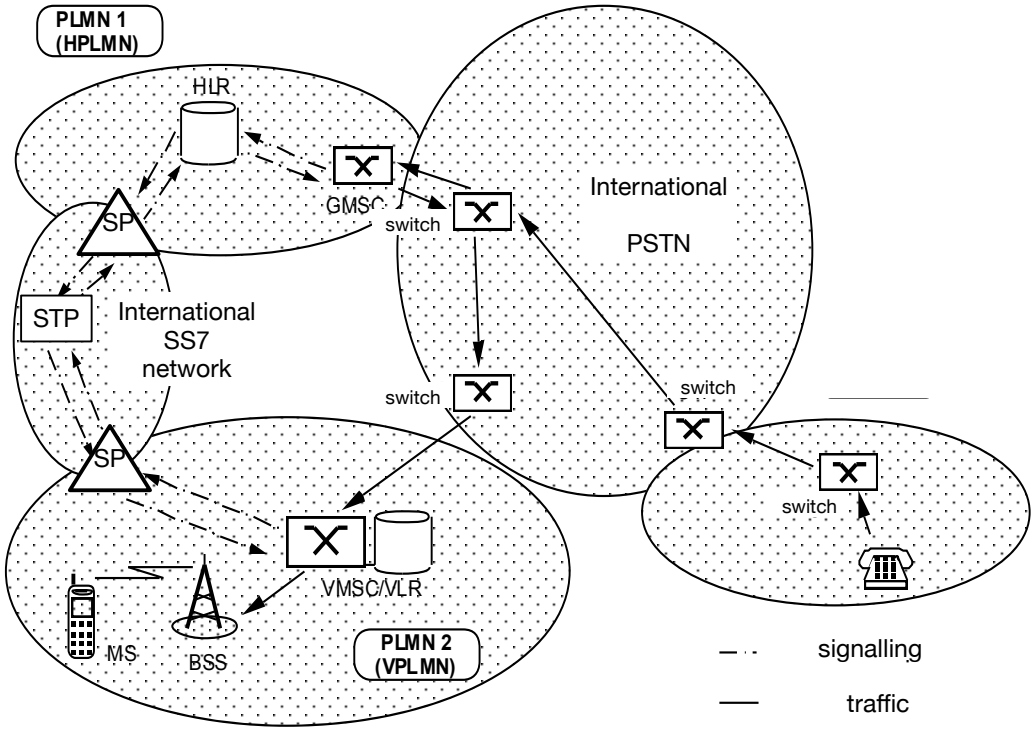
- Roaming : possibility for a subscriber to access its services via a network different from its home network
- National roaming : inter-operator agreements to improve the coverage of certain regions or for operators without 2G or 3G license (e.g. Free), or for overseas regions
- International roaming : based on inter-operator agreements

Roaming : International originating call



- PLMN1 : country of the subscriber
- PLMN2 : visited country
- Country 3 reached by the subscriber
- Signalling and voice are carried by the international networks from Country 2 to Country 3
- Pricing will be sent afterwards from PLMN2 to PLMN1

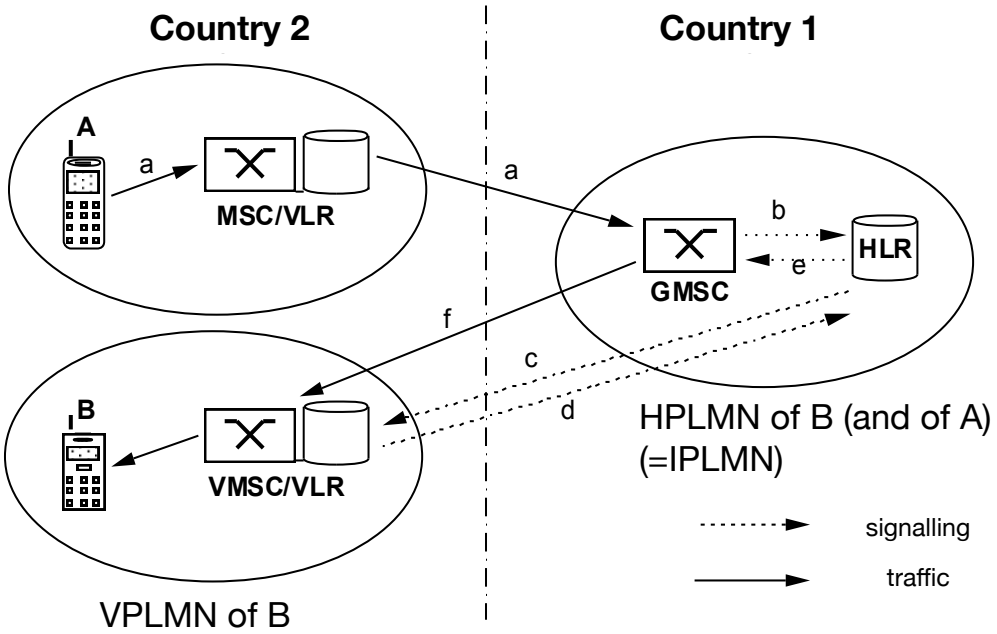
Roaming : International terminating call



Trombone effect :

- The call is first routed to PLMN1 (to the GMSC)
- The HLR (PLMN1) obtains the MSRN from the VMSC/VLR (PLMN2) through the international signalling network
- The GMSC establishes a voice circuit towards the VMSC in PLMN2
- Trombone effect : the voice circuit is established between Country 3 and PLMN2 via PLMN1

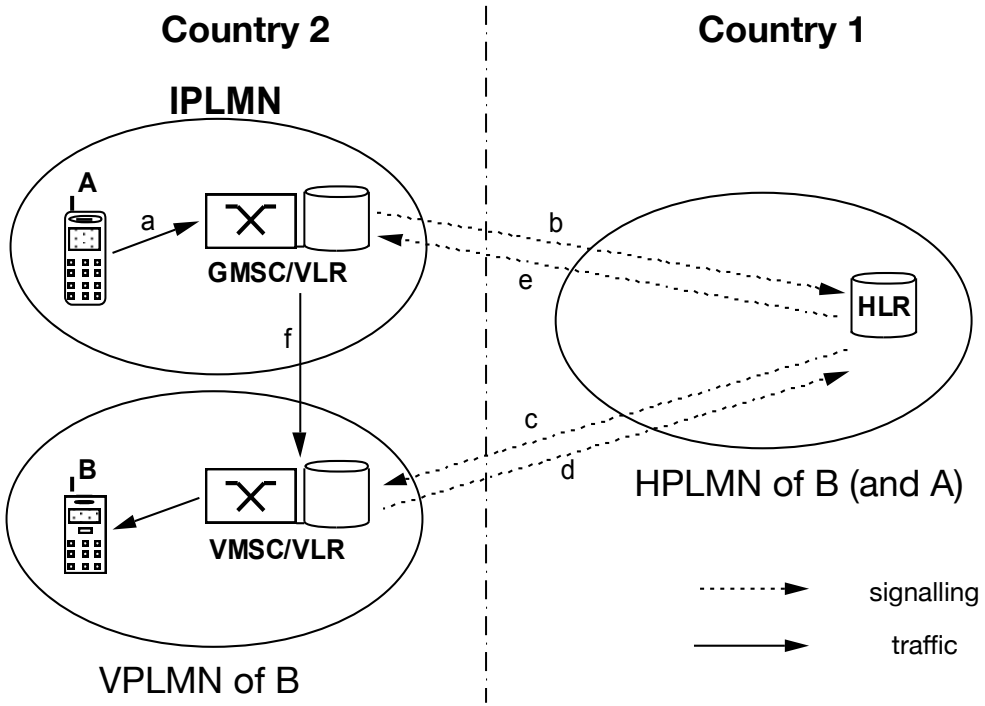
Roaming : international mobile to mobile call I



Trombone effect :

- A and B are subscribers of an operator in Country 1
- A and B are visiting Country 2 and may use a different operator
- Trombone effect : signalling and voice go through the operator of Country 1

Roaming : international mobile to mobile call II



Support of optimal routing :

- IPLMN : Interrogating PLMN
- The MSC of A detects that the call is for a MS and acts as a GMSC
- The GMSC of the IPLMN retrieves from the HLR in Country 1 the localization of B
- Optimal routing : only the signalling goes through Country 1, voice goes directly from operator 1 to operator 2.