❑ GSM Procedures

- Security Procedures
- Network Access
- Mobility
- Originated Call (Call Set Up)
- Handovers
- Terminated Call (Paging)

Mobile Radio Networks

❑Security procedures

Security procedures

- Authentication:
  - has the task of verifying the user's identity and protecting against fraudulent use of identifiers
- Encryption:
  - it has the task of making the data flow to and from the MS not easily decodable by intruders
- In GSM, the authentication and encryption procedures are closely linked in the first stage of secret key management

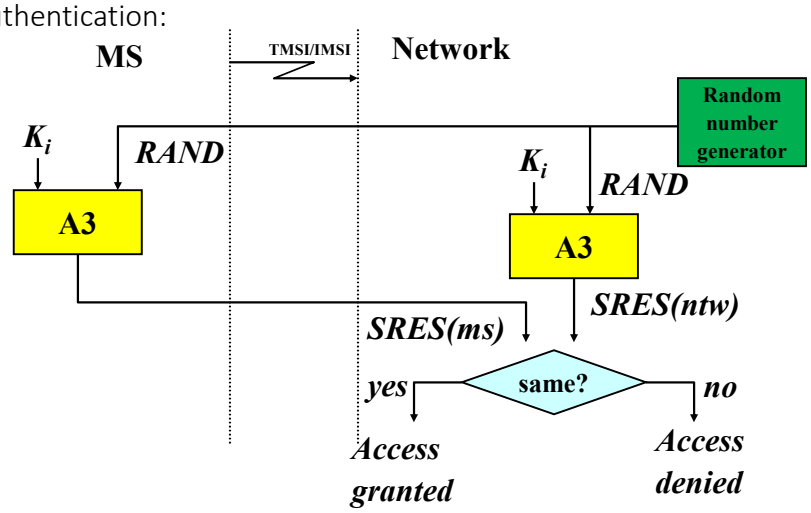
Security procedures

- Elements of procedures:
  - K_i
    - 128-bit user authentication key stored in the AuC and in the SIM
  - *RAND*
    - 128-bit random number generated by the AuC and then sent to the MSC
  - *A3*
    - authentication algorithm stored in the AuC and in the SIM
  - *A8*
    - algorithm that determines the encryption key K_c, stored in the AuC and in the SIM
- Results of procedures:
  - K_c
    - encryption key
  - *SRES*
    - result of the authentication algorithm

Triples
($RAND$, $SRES$, K_c)
are generated in sequence for each IMSI and stored in the HLR

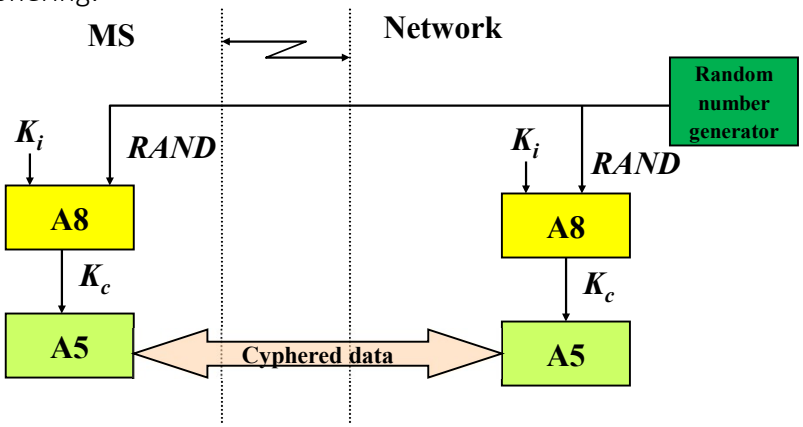
Security procedures

- Authentication:



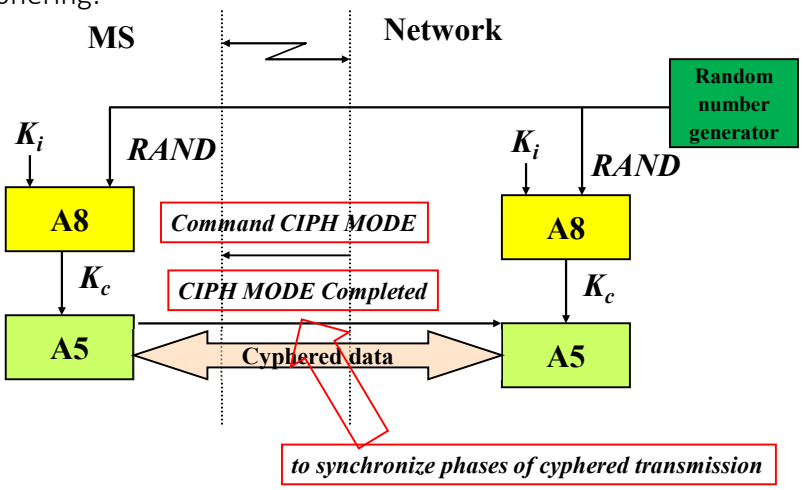
Security procedures

- Cyphering:



Security procedures

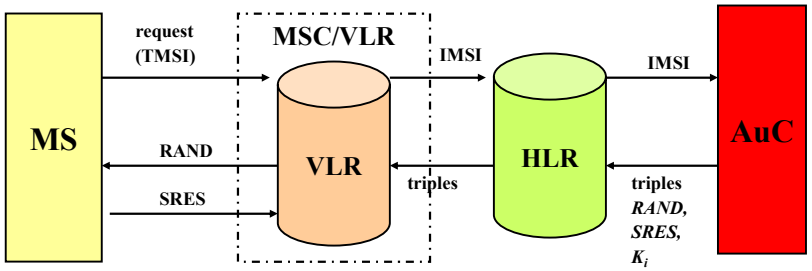
- Cyphering:



Security procedures: Roles of network elements

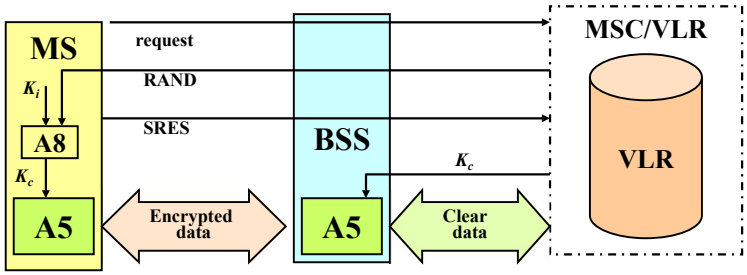
AuC

- Authentication Centre (AuC)
  - It stores secret keys K_i of all users
  - Generates random numbers and calculates *SRES* and encryption keys K_c
  - Provides triples to the other network elements



Security procedures: Roles of network elements

- Role of the BSC in the encryption:



❑Registration and Location Update

Turning on a UE

- When a mobile phone is turned on the following procedures are performed:
  - Cell Selection: the MS selects the BTS for the connection
  - Registration: the MS informs the MSC that it is active and updates information on the Location Area

Cell Selection

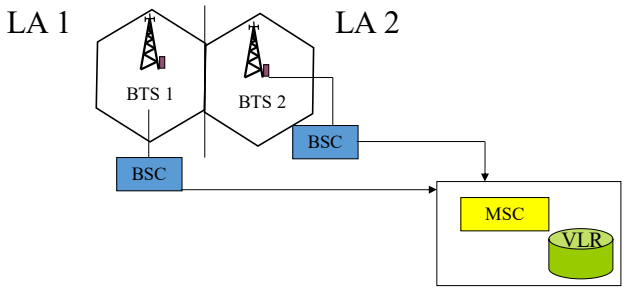
- The MS scans the radio carriers
  - The carriers on which the BCCH is transmitted are called c0
  - These carries are at constant power (dummy bursts are used) and frequency hopping is disabled
- Through the FCCH the MS synchronizes with the BTS carrier
- Through the SCH the MS synchronizes slot and frame and receives the BSIC
- The MS can now decode the BCCH that includes
  - LAC (Location Area Code)
  - CGI (Cell Glocal Identity)
  - MCC (Mobile Country Code)
  - MNC (Mobile Network Code)
- The MS selects the BTS with the strongest c0 carrier

Registration

- Two possible cases:
  - IMSI attach: The LAI received is the same stored in the SIM (phone turned off and then turned on in the same LA). An IMSI attach procedure is initiated and the IMSI is marked as active in the VLR.
  - Location Update: No LAI stored or LAI received different from the stored one (phone turned off and then on in a different LA). A Location Update procedure is initiated

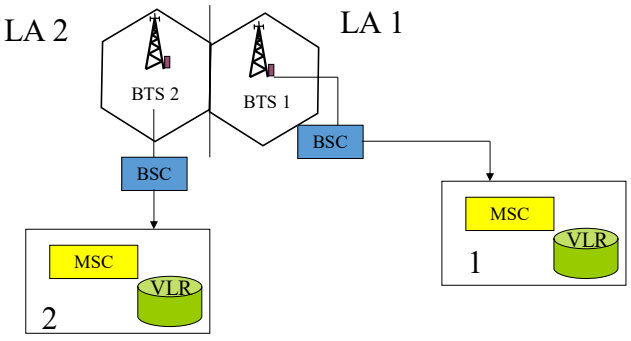
Location Update (1)

- Two types of Location Update:
  - (1) Source and destination LAs refer to the same MSC/VLR (simplest case)

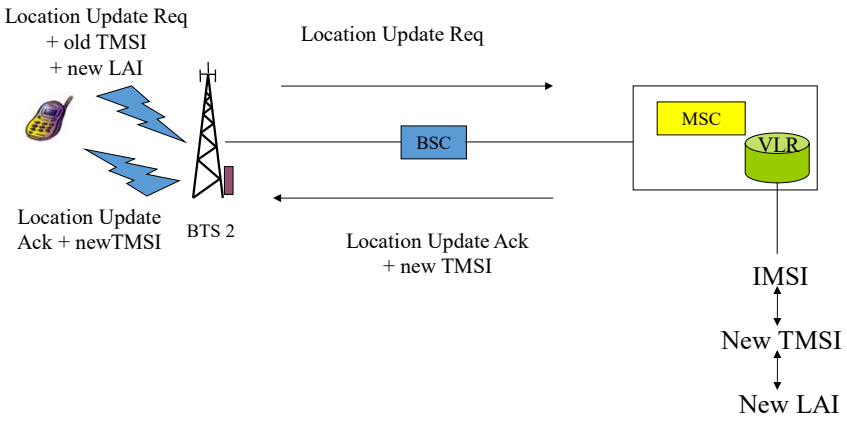


Location Update (2)

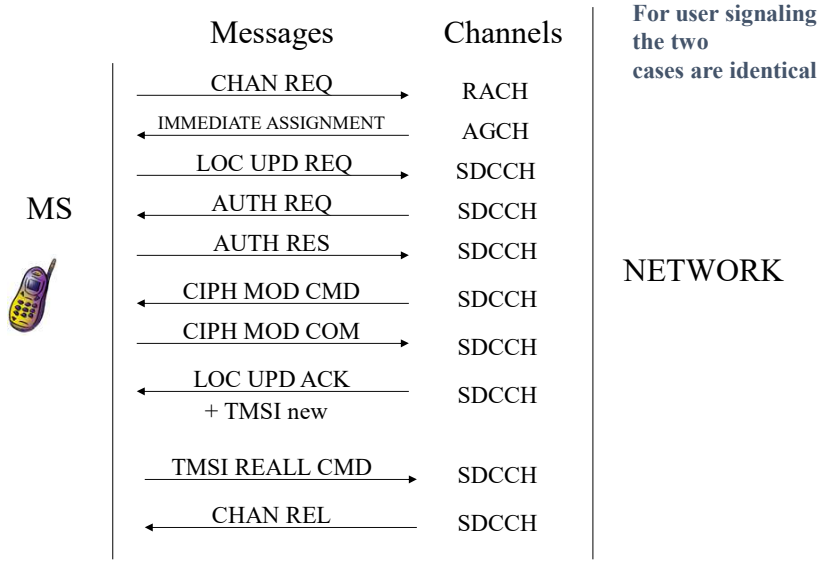
- (2) Roaming across LAs referring to different MSC/VLR



Location Update - Intra MSC

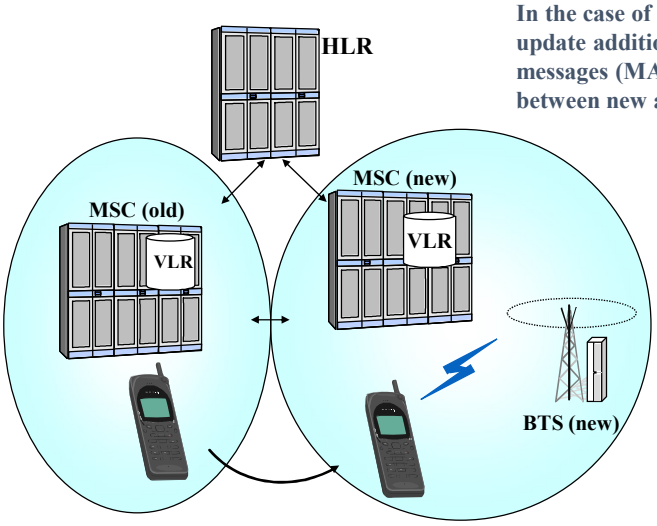


Location Update - Intra MSC

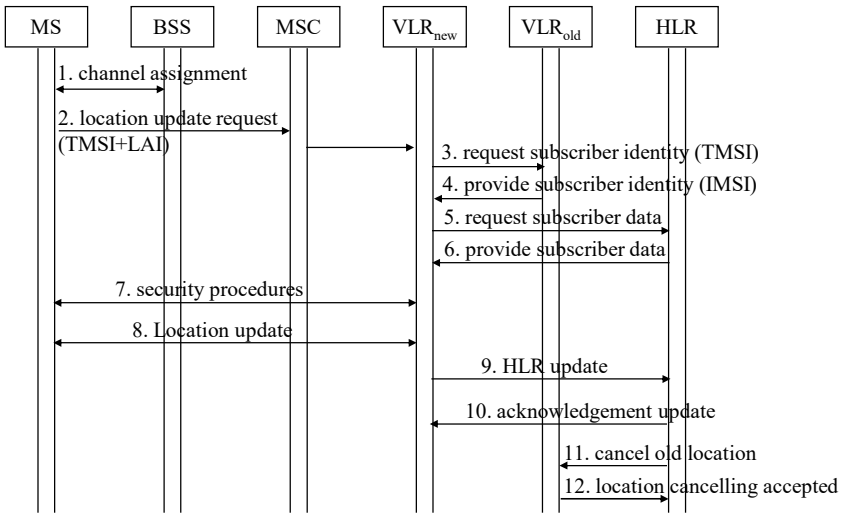


Location Update inter MSC

In the case of Inter-MSC location update additional signaling messages (MAP) are exchanged between new and old MSC/VLR

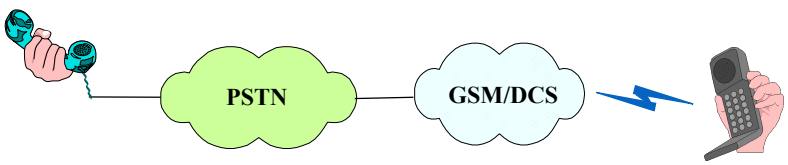


Location Update inter MSC



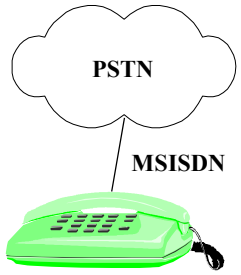
❑Call Set Up

- Establishing communication on a fixed network is in itself "difficult"
- Establishing communication between the fixed network and the mobile network requires even more effort



Call setup: mobile terminated call Step by Step (1)

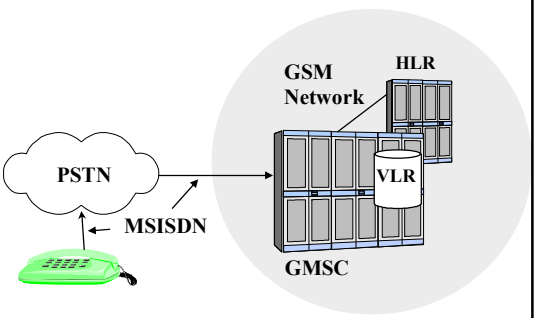
- The PSTN/ISDN user digits the Mobile Subscriber International ISDN Number (MSISDN) of the called user



MSISDN: +39 347 6527268
39 = Country Code (Italy)
347 = National Destination code
6527268 = Subscriber Number

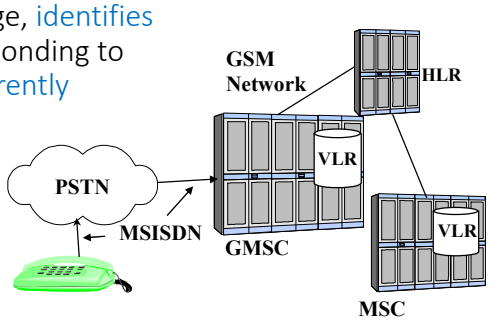
Call setup: mobile terminated call Step by Step (2)

- The PSTN/ISDN network analyzes the number and routes the call to the GMSC of the PLMN making use of the National Destination Code (NDC)
- The GMSC receive the call setup request through the SS7 network with the MSISDN called



Call setup: mobile terminated call Step by Step (3)

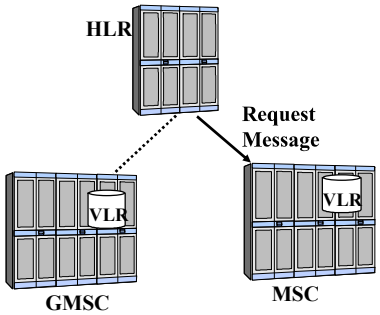
- The GMSC identifies the HLR of the called user through the MSISDN (the GMSC does not know the MS position!)
- The GMSC send a "HLR Inquiry" message to the HLR
- The HLR analyzes the message, identifies in its record the IMSI corresponding to the MSISDN and the VLR currently visited by the MS



Call setup: mobile terminated call Step by Step (4)

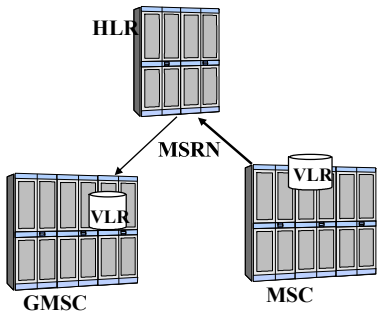
- The HLR sends a "Routing information request" to the MSC/VLR (MAP message)
- The MSC/VLR allocates temporarily a Mobile Station Roaming Number (MSRN) for the call

- The MSRN is similar to the MSISDN, and it can be used for routing the call
- MSRN = CC + NDC + SN
  - CC = Country Code
  - NDC = National Destination Code
  - SN = Subscriber Number



Call setup: mobile terminated call Step by Step (5)

- The MSC forwards the MSRN to the HLR
- The HLR forwards it to the GMSC
- The GMSC routes the call by using MSRN to the MSC/VLR



Call setup: mobile terminated call Step by Step (6)

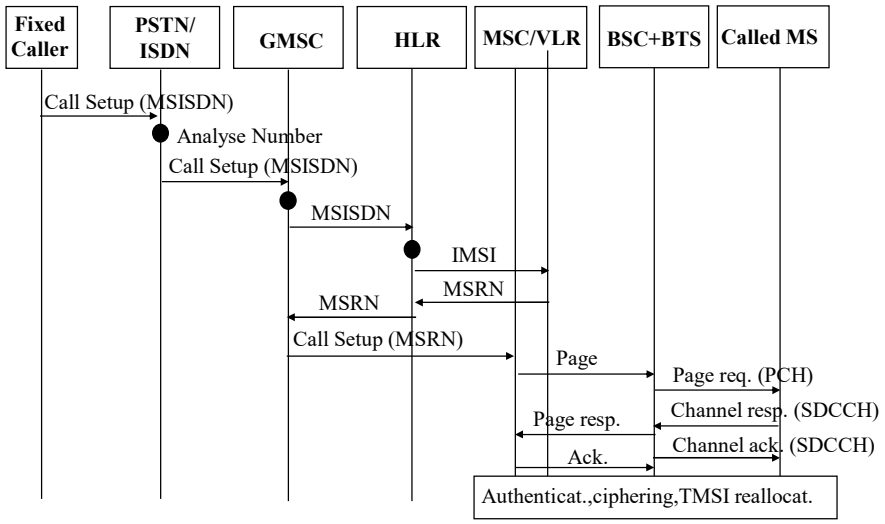
- The MSC/VLR activates the paging procedure
  - It identifies the currently visited LA
  - It sends a paging command to BSCs of the area
- BSCs activate paging on their BTSs using the PCH (paging message contains the TMSI of the MS)
- The MS replies to the paging message starting an access procedure on the RACH and get a SDCCH assigned

The procedure continues like a setup of a mobile initiated call

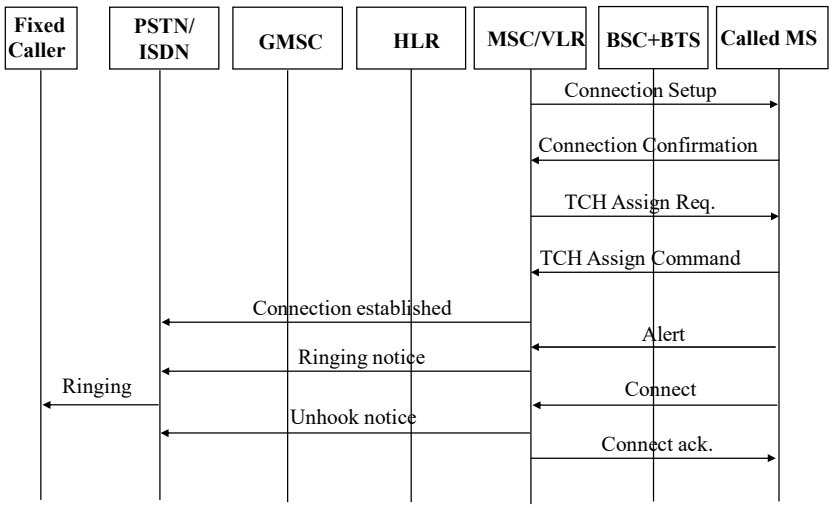
Call setup: mobile terminated call Step by Step (7)

- The MSC/VLR activates the authentication and encryption procedures
- The network assigns a traffic channel (TCH) for communication
- MSC/VLR notifies the caller that the called telephone is ringing
- The called party is notified that the caller has answered
- The connection is established

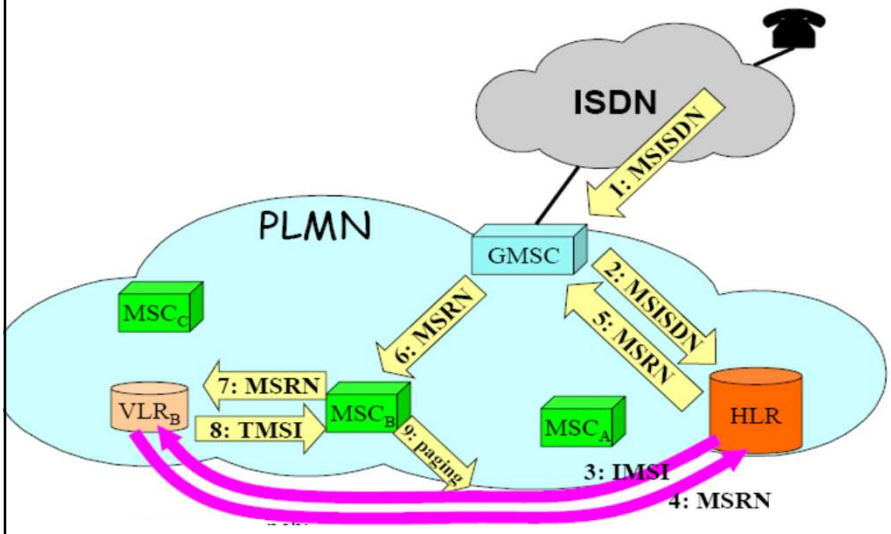
Summary of the Call Set-up Steps (1)



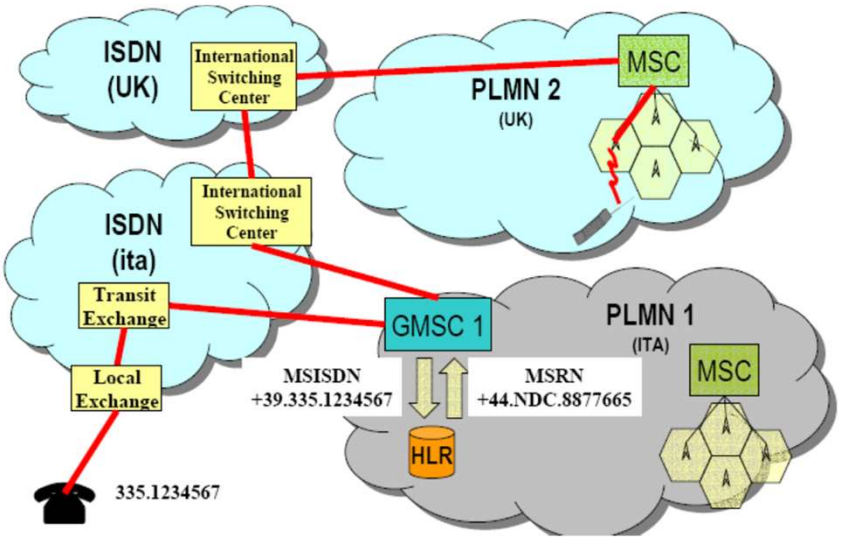
Summary of the Call Set-up Steps (2)



Call setup: mobile terminated call



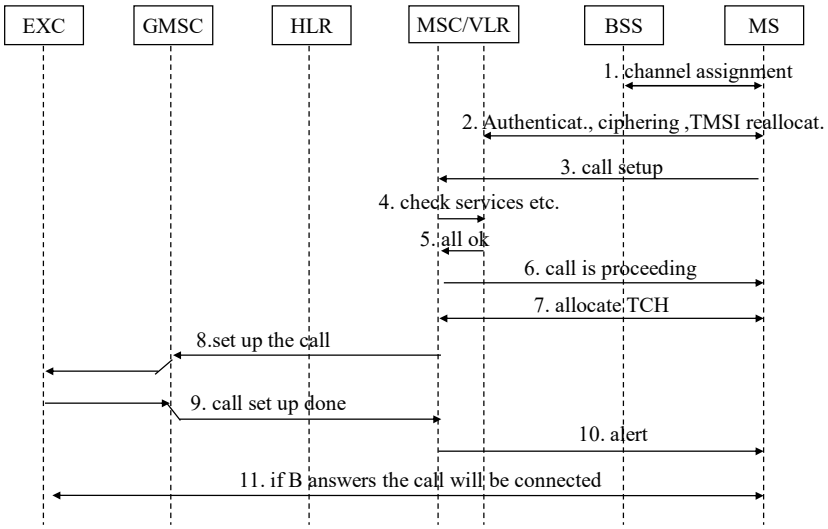
Call setup: mobile terminated call (international roaming)



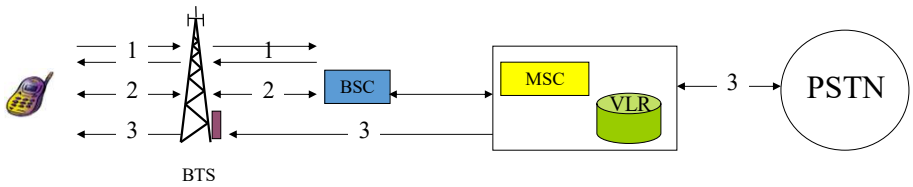
Call setup: MS originated call

- MS dials the number
- The serving MSC analyzes the caller data and:
  - authorize or deny the call
  - activate the routing procedure
- If the caller belongs to the same GSM network, an "HLR inquiry" procedure is initiated to obtain the MSRN
  - the procedure is similar to that for calls originating from PSTN
- If the called party does not belong to the same network as the caller, the call is forwarded to the GMSC.

Summary of the Call Set-up Steps

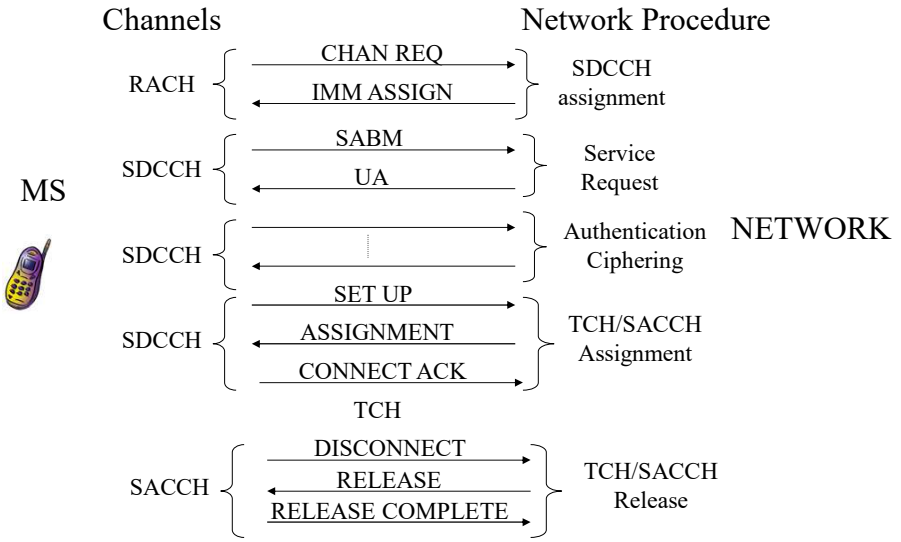


Call setup: MS originated call



1 - Access and allocation of resources for reporting
2 - Authentication and encryption, caller ID exchange and traffic channel allocation
3 - Routing of the call

Call setup: MS originated call



Mobile Radio Networks

- Handover

Handover in GSM

- In GSM the handover procedure is decided by the network, however the decision is essentially made on the basis of measurements made by MS
- When MS connects to a cell, the relative BSC communicates it a list of "alternative channels" (BCCH of 6 adjacent cells), on which to carry out RF power measurements;
- The result of these measurements is transmitted to the BSC on the SACCH channel every 480 msec
- The BSC analyzes the measurements from the mobile, integrates them with the measurements made by the BTS and eventually decides the handover

Activation parameters

MS side measurements

- Intensity of the signal received on the BCCH carriers of the adjacent cells (RXLEVNCELLn)
- Received signal strength on active TCH traffic channel (RXLEV)
- Quality of active traffic channel TCH (RXQUAL)

BTS side measurements

- Signal strength received from the MS on the traffic channel (RXLEV)
- MS traffic channel quality (RXQUAL)
- Distance from the MS, using the Timing Advance technique

Requirements and reasons for a Handover

Requirements:

- The procedure requires
  - criteria for identifying the need for a handover
  - procedures for switching a communication from one radio channel to another
- All of this must be invisible to the user

Reasons:

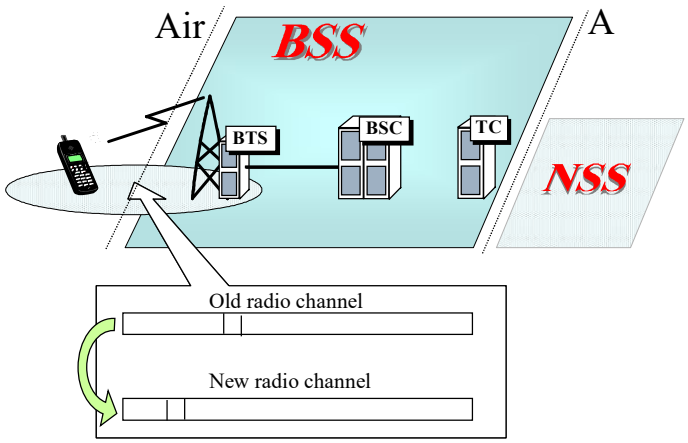
- Inadequate transmission quality (RXLEV and/or RXQUAL fall below a certain threshold)
- Distance MS/BTS goes above a maximum limit
- Traffic reasons (cell too "loaded")
- Inspection and maintenance needs

Types of Handovers

4 types of handovers:

- Intra Cell - Intra BSC
- Inter Cell - Intra BSC
- Inter Cell - Inter BSC
- Inter MSC

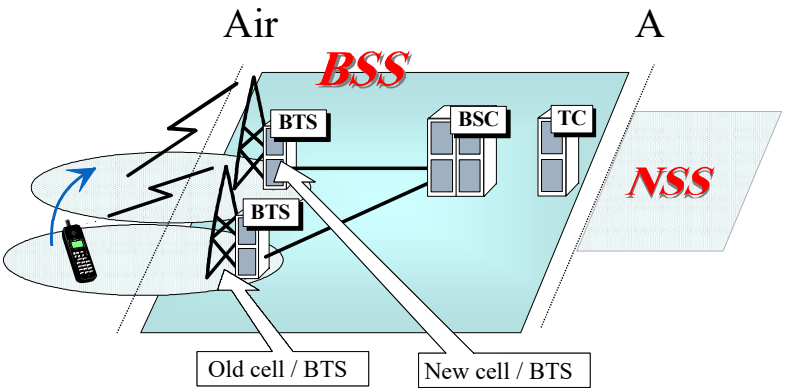
Intra Cell - Intra BSC Handover



Intra Cell - Intra BSC Handover

- Easier handover, decided independently by the BSC
- Changing the traffic channel (TCH) and generally also the frequency within a BTS
- Caused by:
  - insufficient quality of the TCH channel
  - no other BTS can guarantee better quality

Inter Cell - Intra BSC Handover



The MS moves to a new cell controlled by the same BSC

Inter Cell-Intra BSC Handover

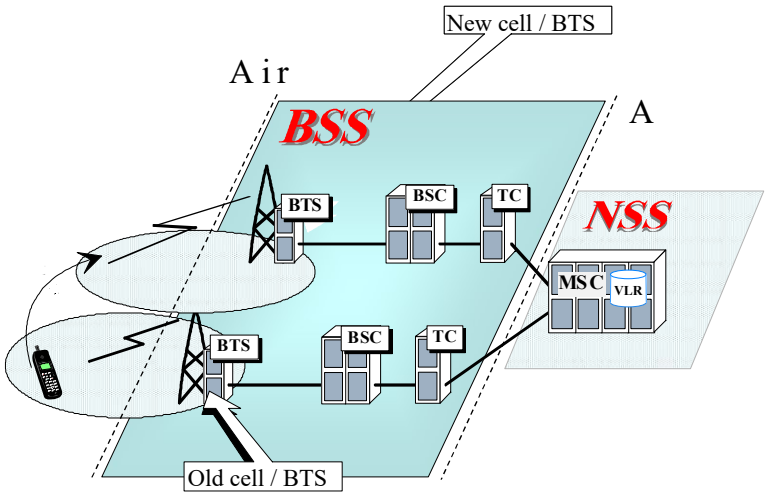
The handover procedure is fully controlled by the BSC

- the BSC identifies the best BTS and the best TCH for MS
- the BSC establishes a connection to the new BTS and reserves the new TCH channel
- the BSC orders the MS to tune to the new channel and the old radio carrier is released
- the MS starts sending traffic on the new channel
- the old connection is released
- the BSC informs the MSC/VLR of the successful handover

Additional Operations

- After the handover the MS must acquire information on the new adjacent cells through the Slow Associated Control CHannel (SACCH)
- If the handover has resulted in a change of LA, the MS must request a Location Update procedure

Inter Cell - Inter BSC Handover

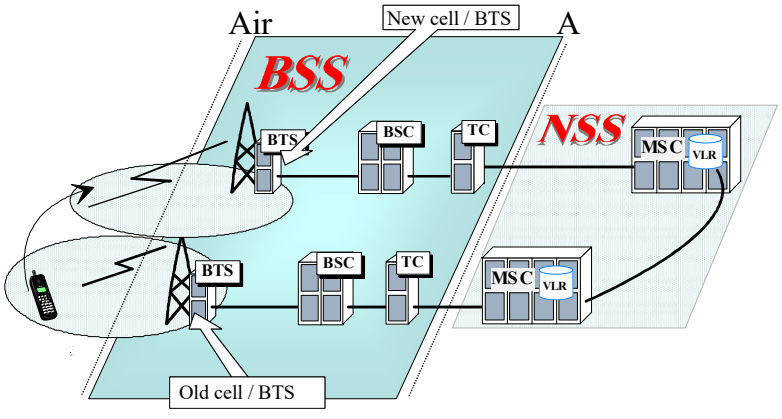


Inter Cell-Inter BSC Handover

The handover procedure is initiated by the BSC

- the BSC identifies the best BTS and the best TCH for MS
- the current BSC sends a message to the MSC/VLR because the new BTS is controlled by another BSC
- the MSC establishes a connection to the new BSC
- the new BSC reserves a radio channel for the MS and the old carrier is released
- the new BSC commands the MS to tune to the new radio channel (TCH)
- the MS starts sending traffic on the new radio channel, after the MSC has switched the connection to the new BSC
- the old connection is released

Inter MSC Handover



More complex handover because it involves different MSC/VLR

- **The call is routed from the initial MSC (Anchor) to the final MSC**

Inter MSC Handover (1)

The procedure is initiated by the BSC

- the current BSC decides the handover to a BTS controlled by another MSC/VLR
- the current BSC sends a handover request command to the initial MSC/VLR
- the initial MSC/VLR sends a request to the final MSC/VLR
- the final MSC/VLR allocates a HandOver Number (HON) and transmits it to the initial MSC/VLR

Inter MSC Handover (2)

- The final MSC/VLR establishes a connection to the new BSC
- the new BSC reserves a traffic channel for the MS
- the MS tunes to the new channel
- the MS starts sending traffic on the new channel after the MSC has switched the call to the new BSC
- the old connection is released

HandOver Number

- Same format as MSRN and MSISDN
- HON = CC + NDC + SN
  - CC = Country Code
  - NDC = National Destination Code
  - SN = Subscriber Number
- SN points to a database
  - in case of MSISDN located in the HLR
  - in case of HON and MSRN located in VLR
- HON contains enough information to allow the GMSC to route the call to the destination MSC