MSc Telecommunications programmes

Mobile Communications Systems (MCS)

UCL

Mobile Communications Systems (MCS)

GSM System Operation

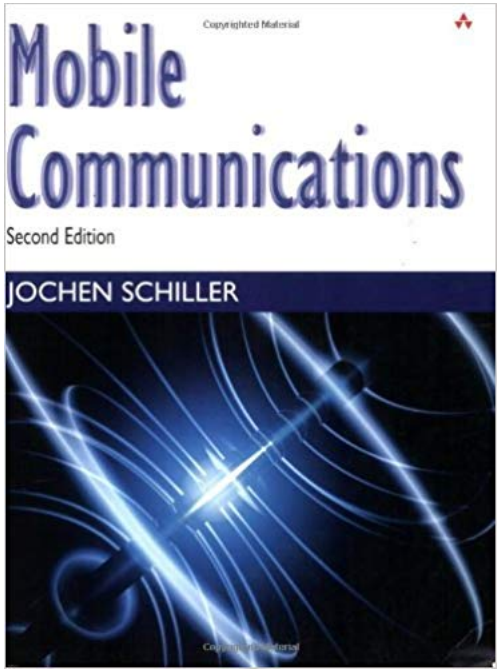
Professor Izzat Darwazeh

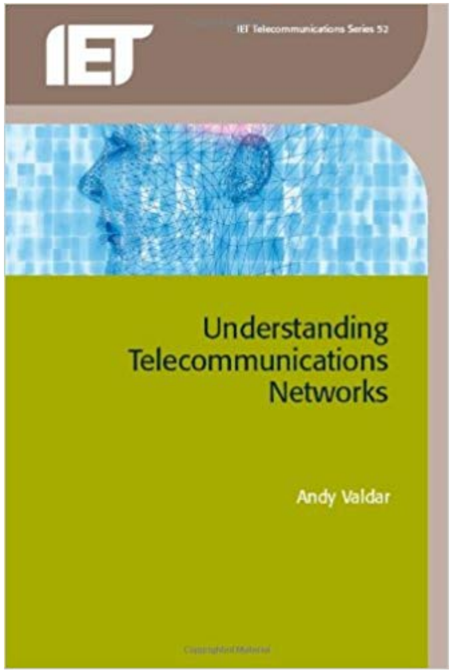
October/November 2020

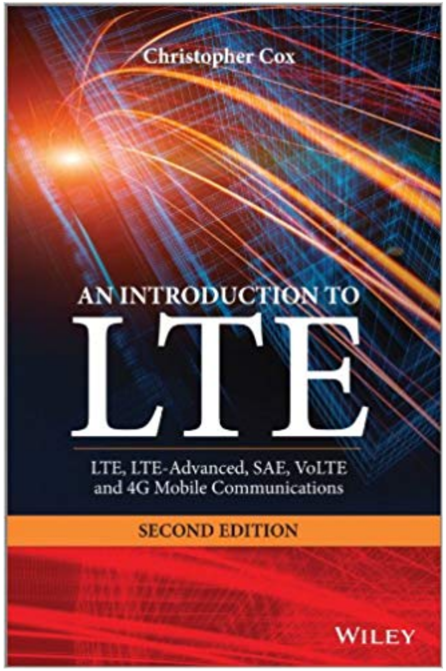
Contents

- GSM Numbering systems
- MO and MT call setup
- Handover
- SMS
- GSM Subscriber Authentication
- GSM Roaming

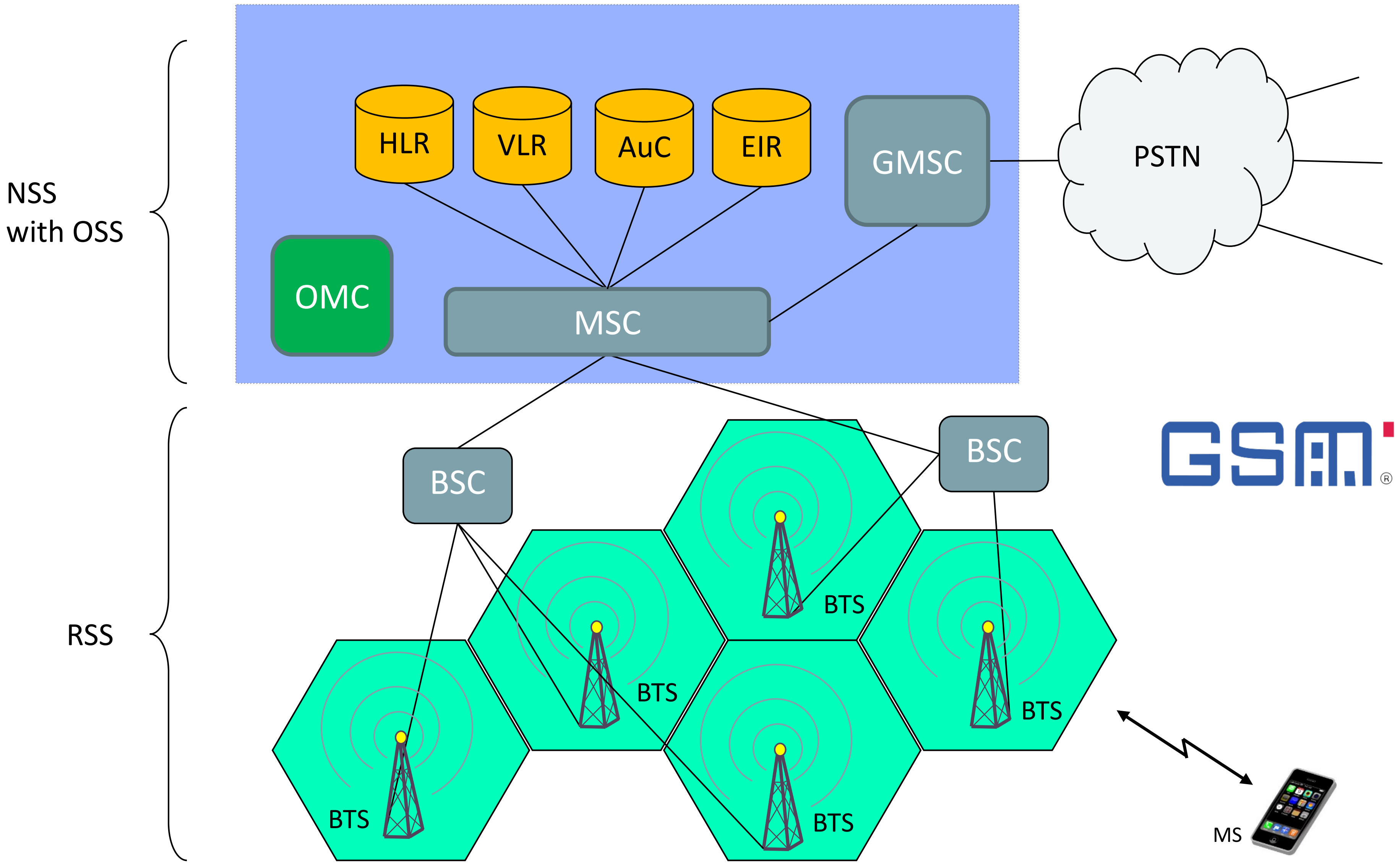
Suggested reference texts




IET
IET Telecommunications Series 52
Understanding Telecommunications Networks
Andy Valdar
Copyrighted Material

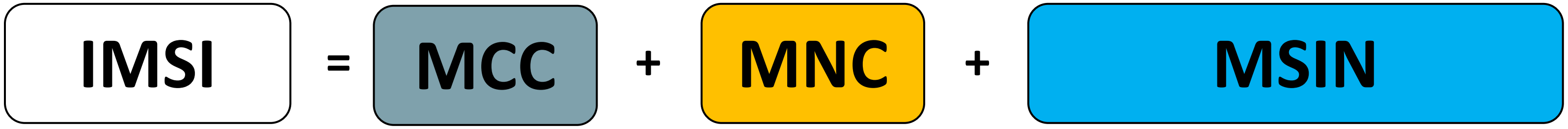


Recap : GSM Network Overview



GSM Numbering : IMSI

International Mobile Subscriber Identification number (IMSI)



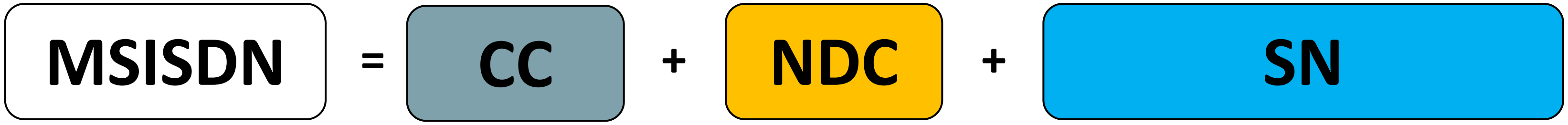
E.212 numbering format

- MCC = Mobile Country Code (3 digits, e.g. 635 for Rwanda)
- MNC = Mobile Network Code (2 digits, e.g. 10 for MTN, 12 for Rwandatel)
- MSIN = Mobile Subscriber Identity Number (≤10 digits)

- The IMSI is a unique identification associated with each GSM and UMTS mobile phone user.
- IMSI is stored as a 64 bit field in the SIM inside the phone and is sent by the phone to the network, where it is stored in the HLR.
- IMSI is based on the ITU-T E.212 numbering plan and cannot be used for routing a circuit-switched call (exchanges or switching centers do not understand such numbers).

GSM Numbering : MSISDN

Mobile Subscriber ISDN Number（MSISDN）



MSISDN = CC + NDC + SN

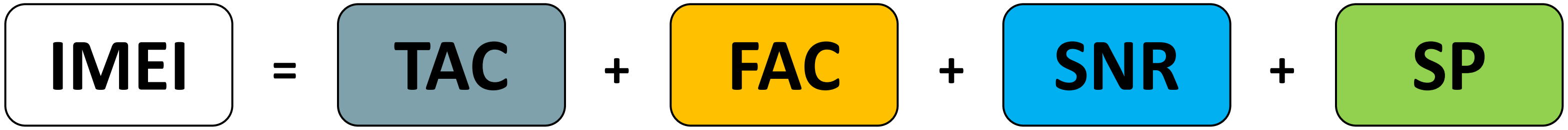
E.164 numbering format

- CC = Country Code (1-3 digits, e.g 250 for Rwanda)
- NDC = National Destination Code (1-3 digits)
- SN = Subscriber Number

- The MSISDN is the number uniquely identifying a subscriber in a GSM or a UMTS mobile network. The MSISDN is basically the “telephone number” of the SIM card in a mobile/cellular phone.
- Mobile station ISDN (MSISDN) numbers are based on the ITU-T E.164 numbering plan and can therefore be used for routing a circuit-switched call.
- When the calling (PSTN or PLMN) user dials an MSISDN number, the call is routed to the gateway MSC (GMSC) located in the home network of the called (mobile) user.

GSM Numbering : IMEI

International Mobile Equipment Identification code (IMEI)



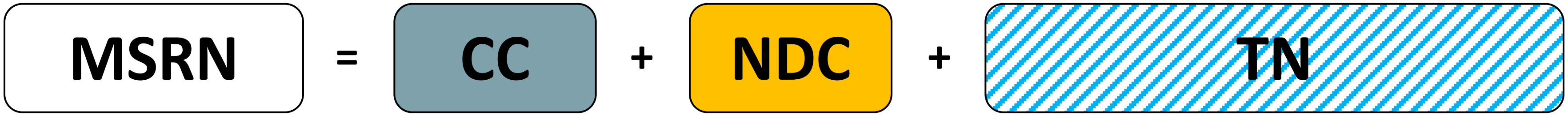
IMEI = TAC + FAC + SNR + SP

- TAC=model ratification code, 6 digits
- FAC=factory assembling code, 2 digits
- SNR=sequence code, 6 digits
- SP=reserved, 1 digit

- The IMEI uniquely identifies every Mobile Station
- The IMEI is a decimal number of 15 digits.
- The IMEI is programmed into the MS at the factory and is not changed throughout the live of the equipment.

GSM Numbering : MSRN

Mobile Subscriber Roaming Number (MSRN)


MSRN = CC + NDC + TN

E.164 numbering format

CC = Country Code (1-3 digits)
NDC = National Destination Code (1-3 digits)
TN = Temporary Number

- The MSRN is temporarily allocated to the subscriber by the VLR according to the request by the HLR when this subscriber is called.
- The MSRN is a temporary number which is only used for call set-up then immediately released to be assigned to other subscriber.
- MSRN are also based on the ITU-T E.164 numbering plan and is in the same format as the MSISDN.

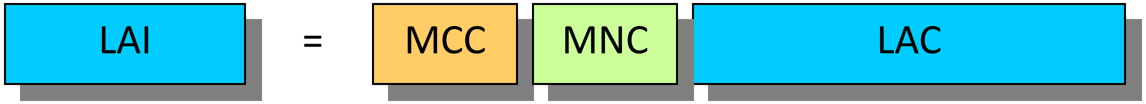
GSM Numbering : TMSI

Temporarily Mobile Subscriber Identification Number (TMSI)

- The TMSI is a 32-bit number (4 octets) that is temporarily assigned to a **MS** by the **VLR** and is used to ensure security of the **IMSI** by substituting for the IMSI in over the air communication .
- The TMSI It is designed to protect the privacy of the subscriber and prevent the IMSI from being discovered.
- The VLR will assign the TMSI to a MS when it registers in that **Location Area**.
- The network may also require the VLR to assign a new TMSI to a MS periodically or even every time it completes a transaction.
- The TMSI is stored on the **SIM** card.
- The TMSI is always assigned when in cipher mode. (traffic is encrypted).
- The TMSI is the same format as the IMSI

GSM Numbering : LAI

Location area Identity (LAI)


LAI = MCC MNC LAC

E.212 numbering format

MCC = Mobile Country Code (3 digits)
MNC = Mobile Network Code (2 digits)
LAC = Location Area Code (≤10 digits)

The location area identity (LAI) points to a location area belonging to a certain MSC/VLR. This identity must be stored in the HLR so that mobile terminated calls can be routed to the correct serving MSC/VLR.

Location Management in GSM

GSM provides international roaming that relies on the mobile’s location being known to the network. Areas of national networks are divided into Location Areas each with a unique identity broadcast on the BCCH. A mobile will update its location with the network when it detects a change in location area.

Each location area has an MSC containing a HLR and a VLR.

- The HLR is a database of all mobiles normally resident in that location area.
- The VLR is a database of all mobiles not normally resident but visiting that location area.

Location updating is carried out via the fixed network using the following procedure:

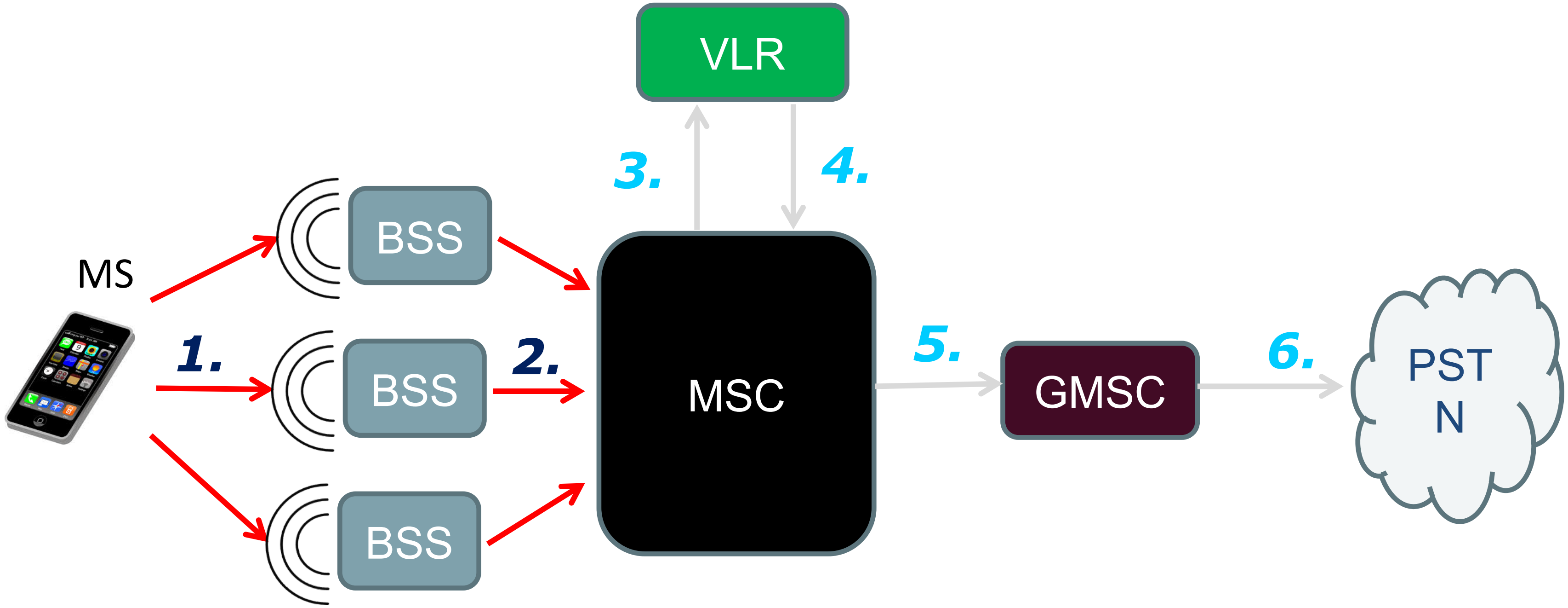
The VLR issues a Mobile Subscriber Roaming Number (MSRN) to be associated with the actual mobile identity (i.e. the International Mobile Subscriber Identity – IMSI) over the radio path.

Both the IMSI and MSRN are conveyed to the mobile’s HLR over the fixed network.
Information on the mobile’s user-profile is conveyed from the mobile’s HLR to the VLR.
The HLR now contains the subscriber’s telephone number, the mobile’s IMSI and the MSRN that points to the mobile’s actual location.

Ref : Schiller p119

Mobile Originated Call – Steps 1 & 2

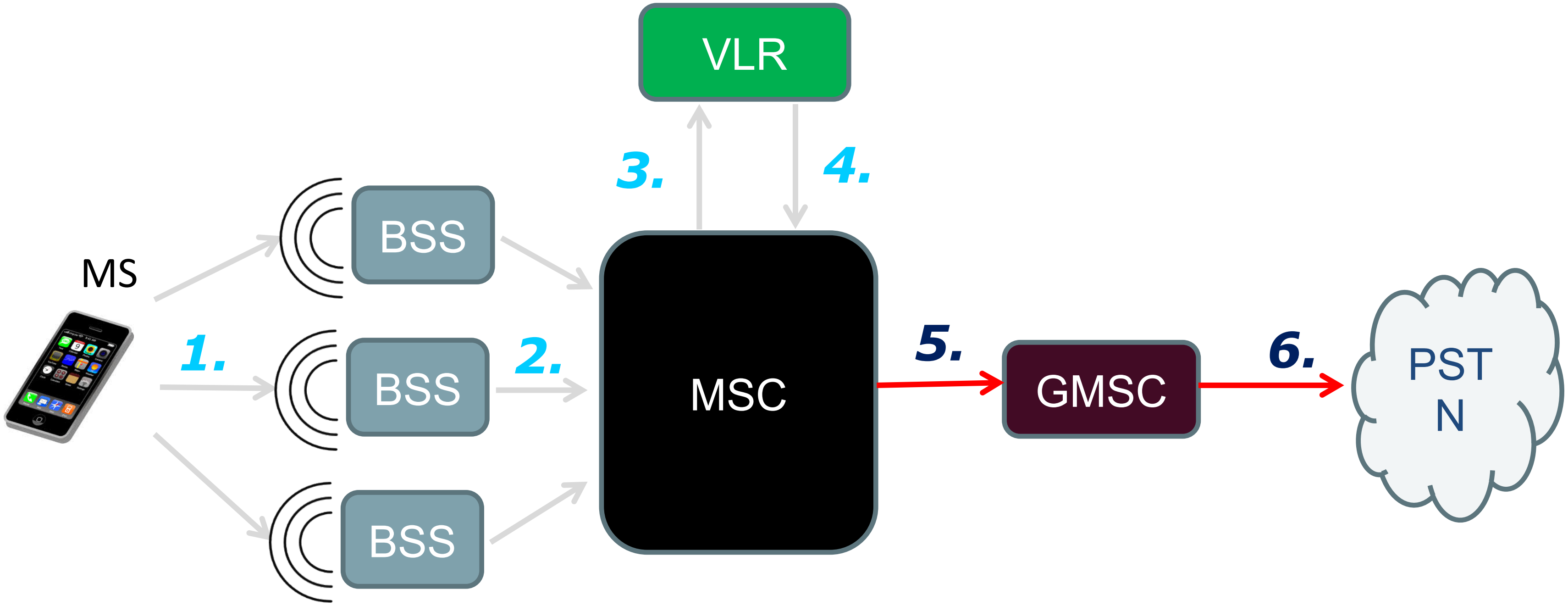
- Step 1 : The MS transmits a request for a new connection to the BSS
- Step 2 : The BSS passes the request to the MSC.



Ref : Schiller p115

Mobile Originated Call – Steps 5 & 6

- Step 5 : the MSC instructs the GMSC to set up the call.
- Step 6 : the GMSC routes the call through the PSTN



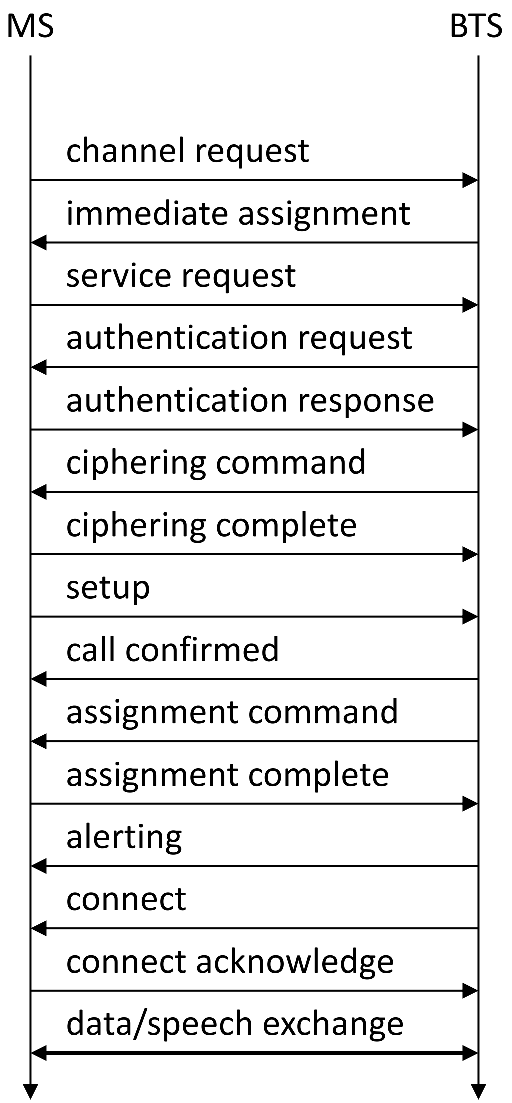
Ref : Schiller p115

Summary of MOC messaging

- **Ciphering** is a security procedure designed to protect the subscriber identity and data, and is an optional procedure in GSM.

- When ciphering is active, all information exchanged between the mobile and the network on the dedicated radio channels is **encrypted**.

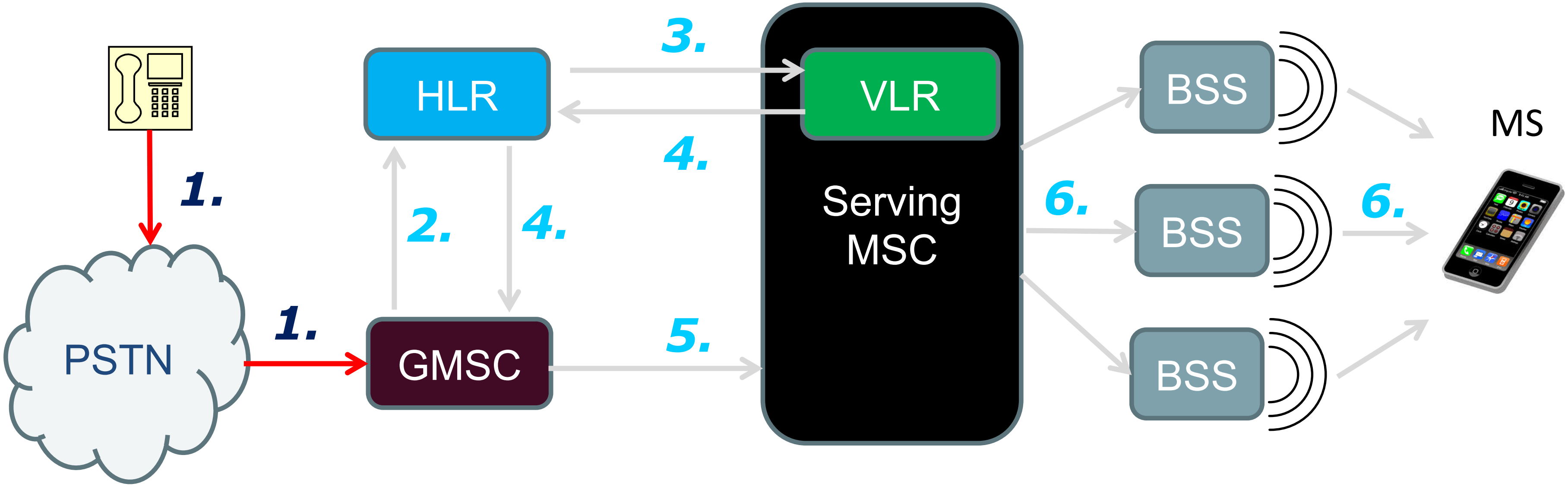
- The key previously set between the network and the MS is used to encipher and to decipher the encrypted information that is sent over the air.



Ref : Schiller p116

Mobile Terminated Call – Step 1

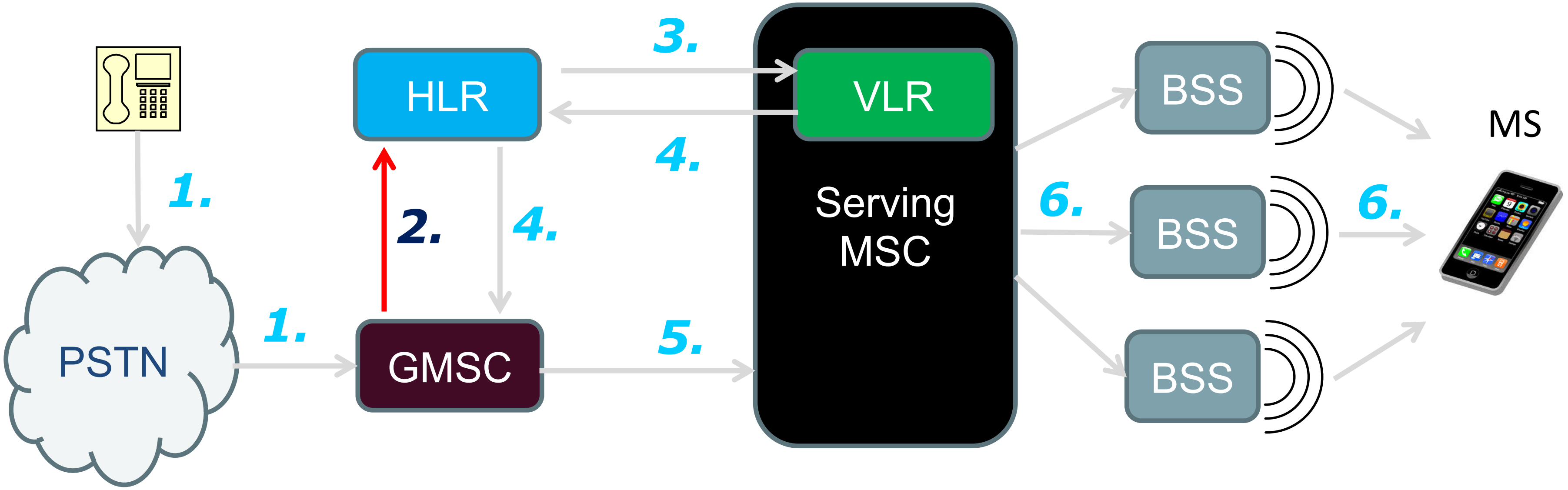
- The calling party dials the MSISDN of the target mobile subscriber from either a land line or a mobile.
- The call is routed through the PSTN to the GMSC in the home network of the called mobile user using this MSISDN and standard SS7/ISUP signalling.



Ref : Schiller p115

Mobile Terminated Call – Step 2

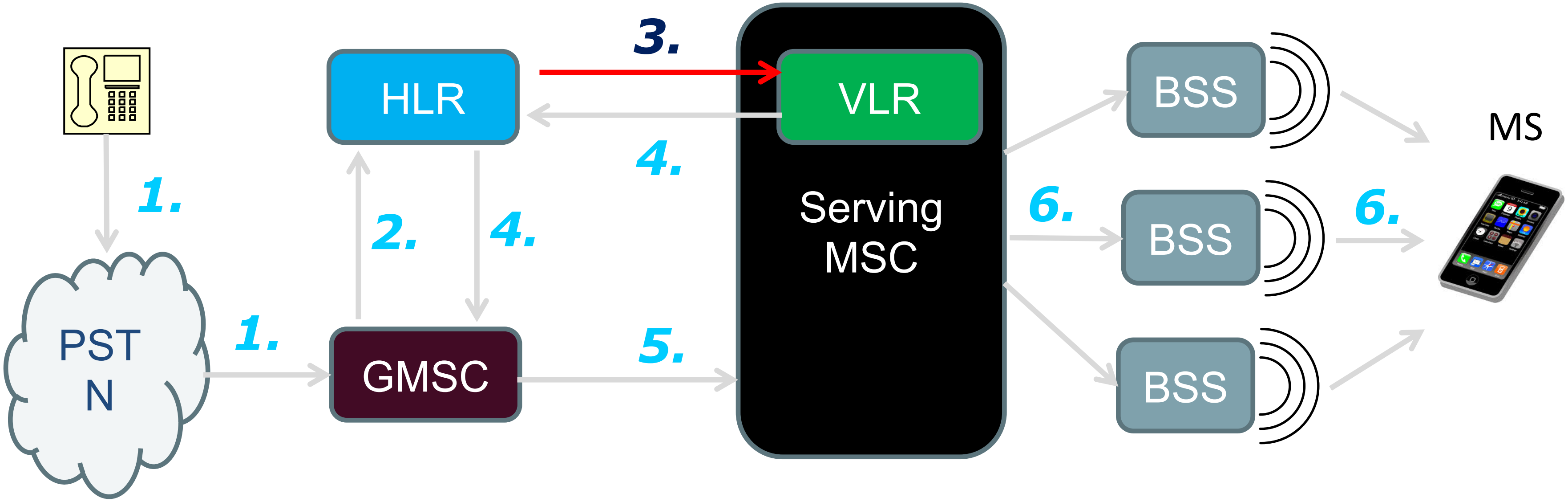
- The GMSC interrogates the HLR of the called mobile user.
- This SS7/MAP signalling message contains the MSISDN number which points to the mobile user record in the HLR database.
- The HLR record contains the IMSI, LAI where the subscriber is roaming, etc.



Ref : Schiller p115

Mobile Terminated Call – Step 3

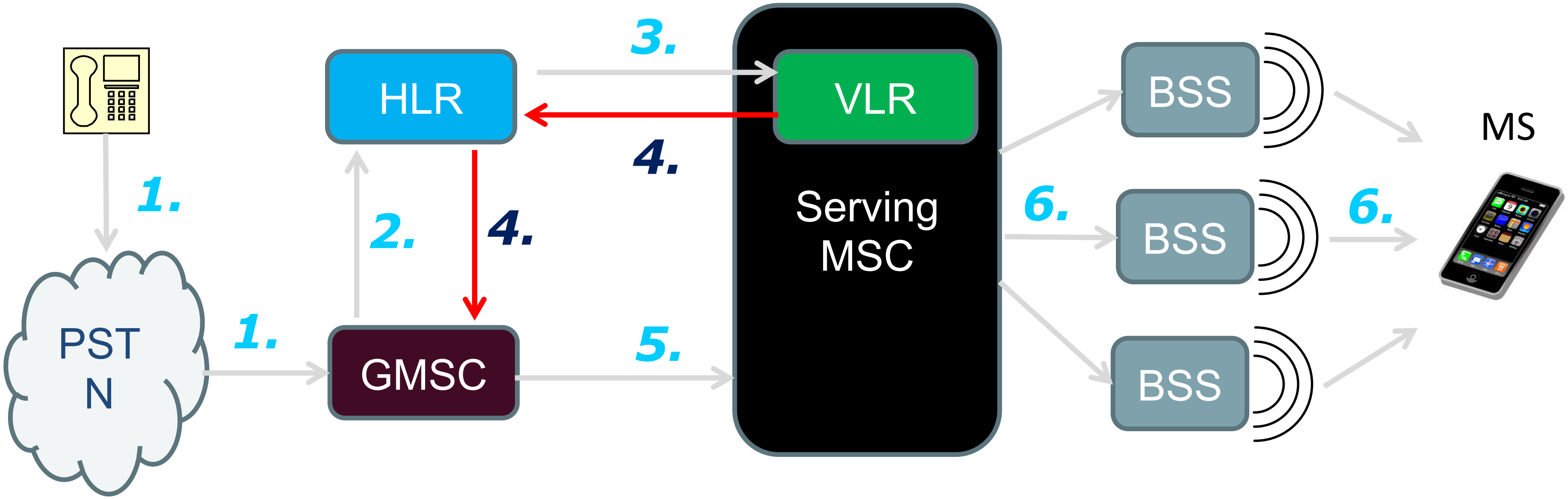
- Using global title translation (GTT), the HLR translates the IMSI and LAI information into the signalling **point code** of the serving MSC/VLR, which may be in a foreign network (Roaming).
- The HLR sends the SS7/MAP request "Provide roaming number" (i.e. provide an MSRN) to the VLR.



Ref : Schiller p115

Mobile Terminated Call – Step 4

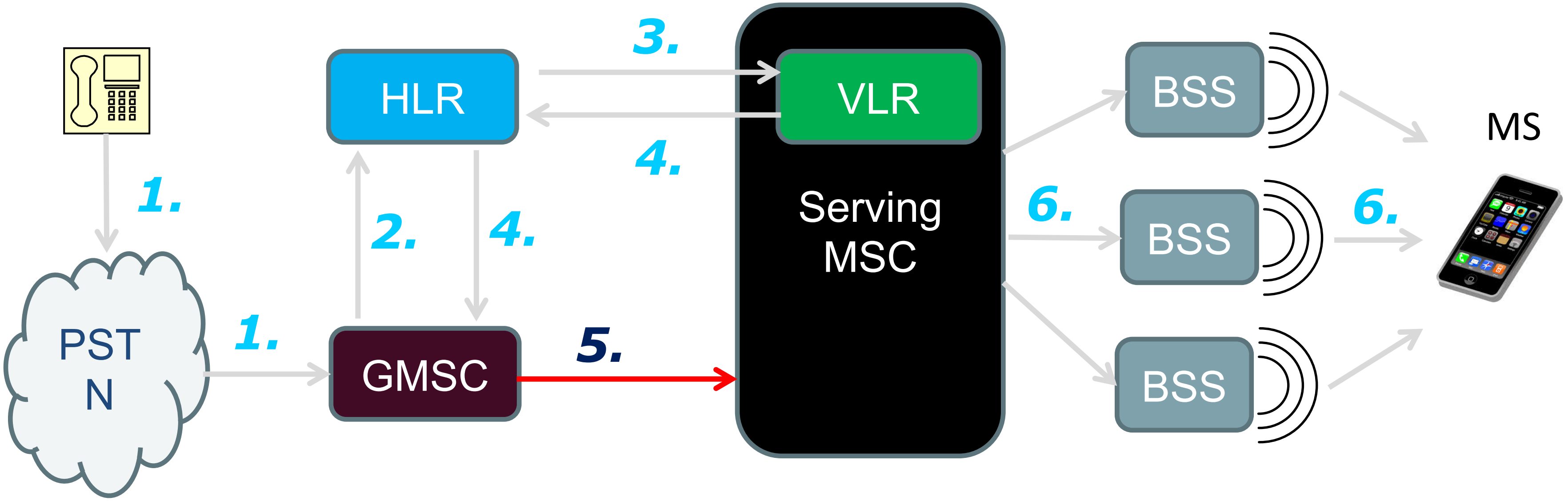
- The VLR generates an MSRN for this subscriber from the pool of available MSRNs and sends this MSRN back to the GMSC via SS7/MAP signalling.



Ref : Schiller p115

Mobile Terminated Call – Step 5

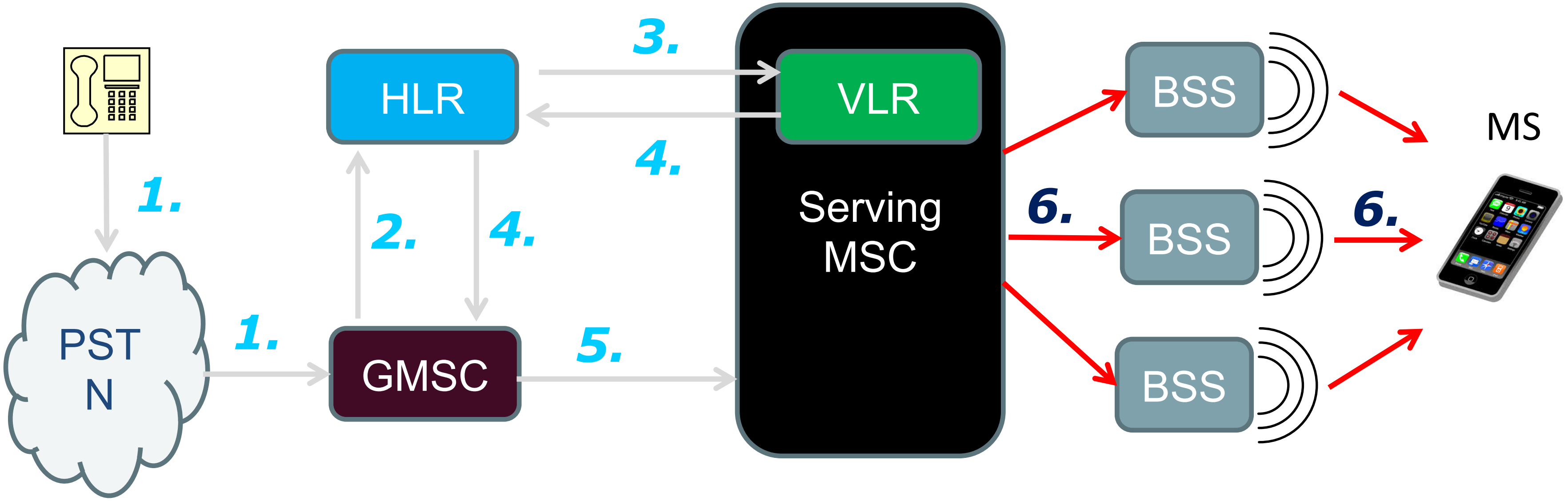
- Using the MSRN number and standard SS7/ISUP signalling, the call is routed to the serving MSC.
- The subscriber could be roaming, so serving the MSC/VLR may be located anywhere the world.
- There may be several intermediate switching centres in between the GMSC and the Serving MSC.



Ref : Schiller p115

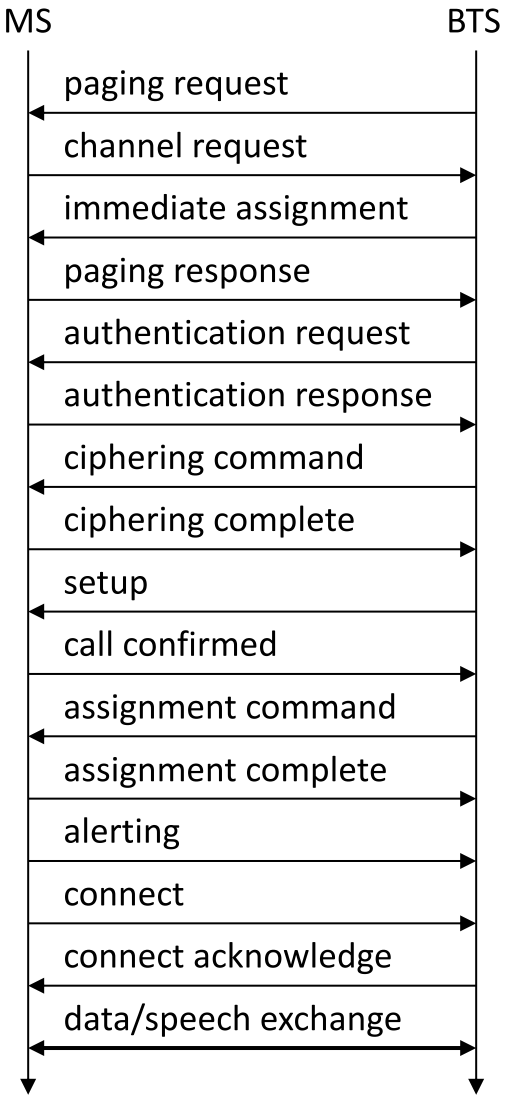
Mobile Terminated Call – Step 6

- MSC/VLR starts **paging** within the location area (LA) in which the called mobile user is located, using TMSI for identification.
- Only the mobile user with the corresponding TMSI responds to the paging via the random access channel (RACH).
- Once the MS has been identified, the call is connected over the air via the TCH



Ref : Schiller p115

Summary of MTC messaging

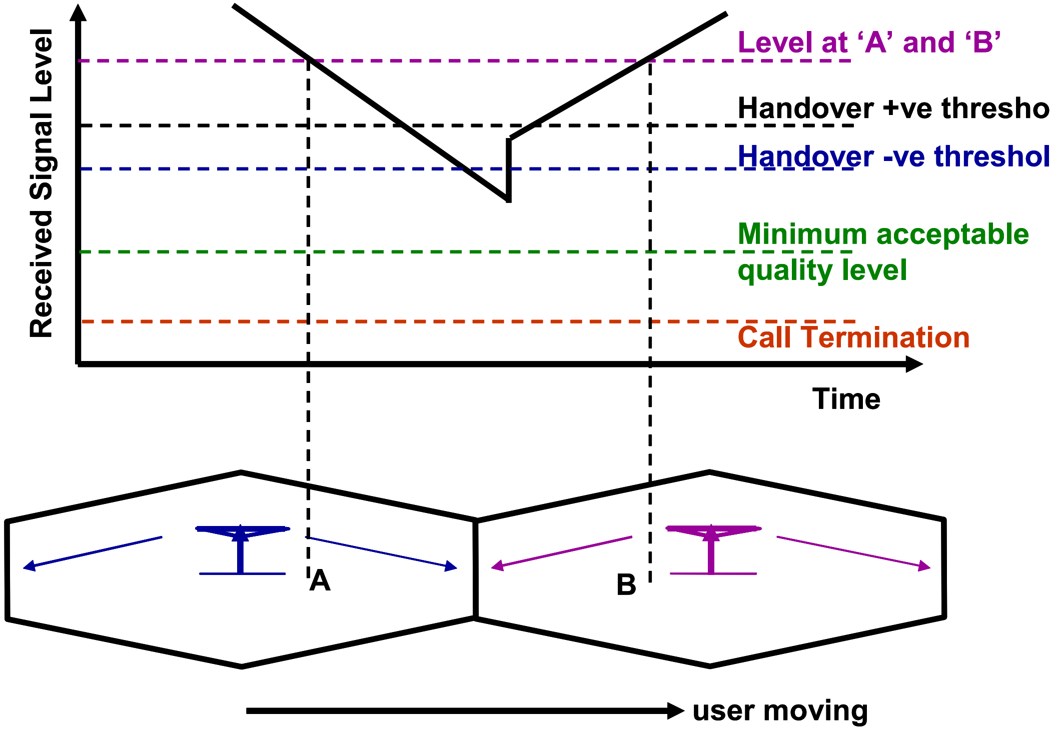


Ref : Schiller p116

Handover

- Handover is the process of transferring a call from one base station to another as the user moves and the received signal quality deteriorates.
- Handovers should be fast (so overlaps of areas of cells can be minimised); reliable (dropped calls are more frustrating than blocked calls - some channels can be reserved for handovers); infrequent (minimise system resources required)
- 1G systems measured signal strength of users with poor reception at current base station. The mobile did not participate in handoff at all. 2G & 3G systems use **"mobile assisted handover" (MAHO):** the mobile looks for a new base station, and requests the handover.

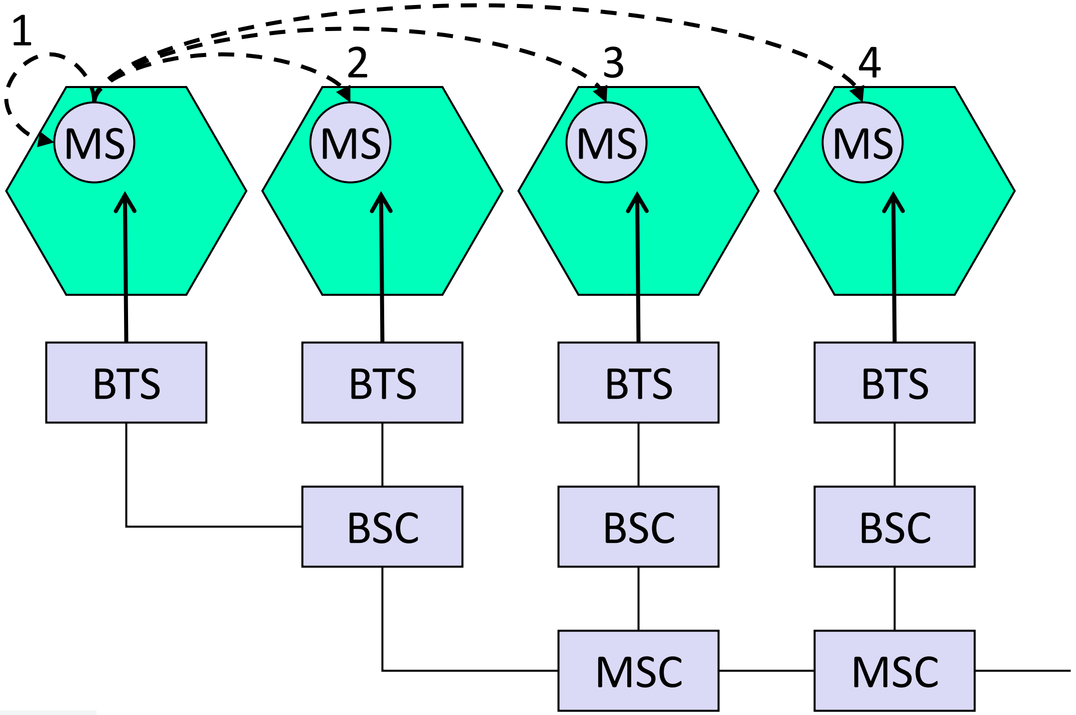
Note the slight hysteresis in threshold levels: this prevents too many handovers.



Types of GSM handover

There are 4 types of handover :

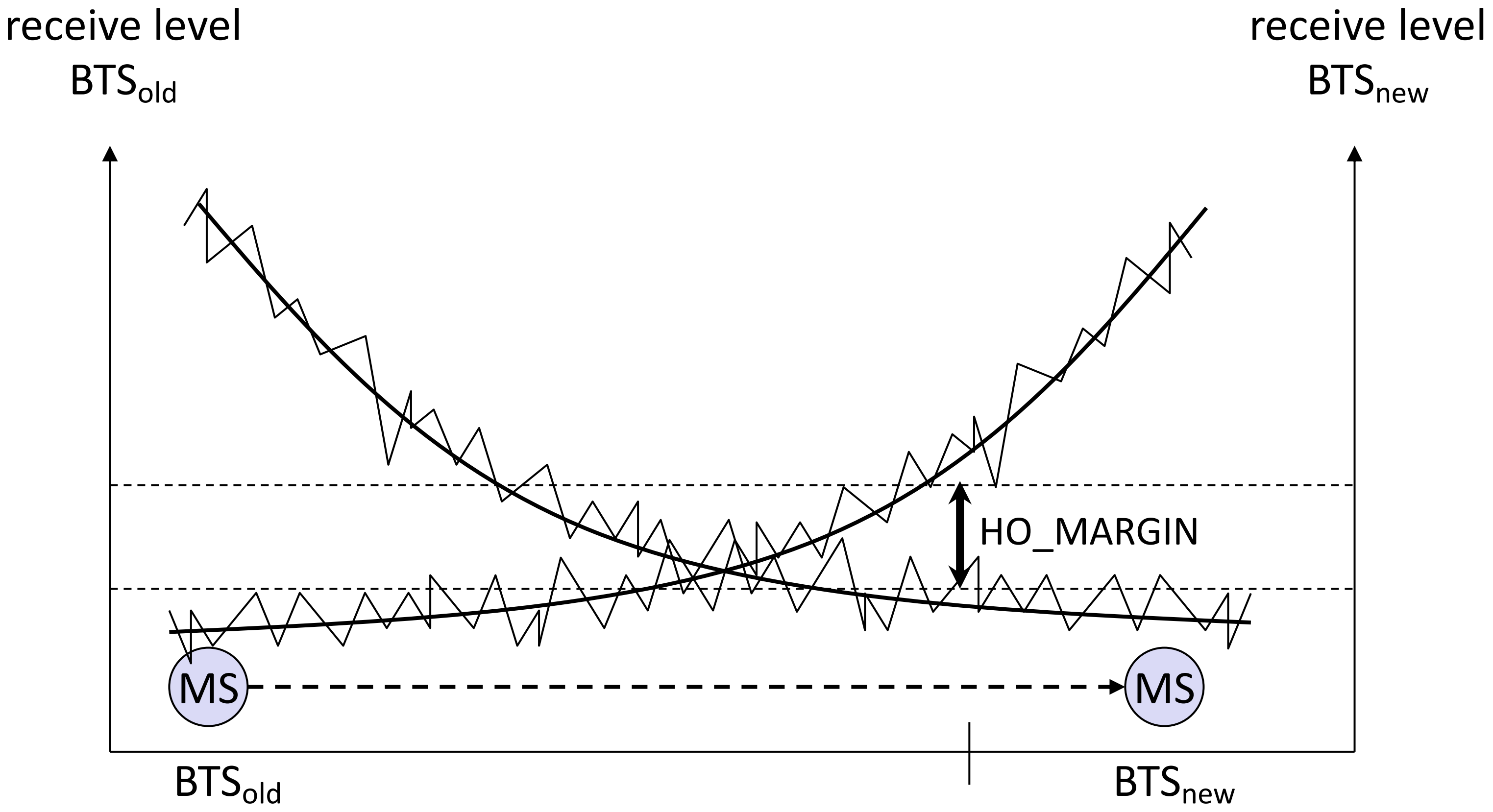
1. **Intra-cell handover :** Within a cell, narrow-band interference could make transmission as a certain frequency impossible. The BSC could then decide to change the carrier frequency.
2. **Inter-cell, intra-BSC handover :** This is a typical handover scenario. The MS moves from one cell to another but stays within the same BSC. Handover is controlled by the BSC.
3. **Inter-BSC, intra-MSC handover :** When the MS moves out of one BSC area into another. Handover is controlled by the MSC
4. **Inter MSC handover :** A handover between two cells belonging to different MSCs



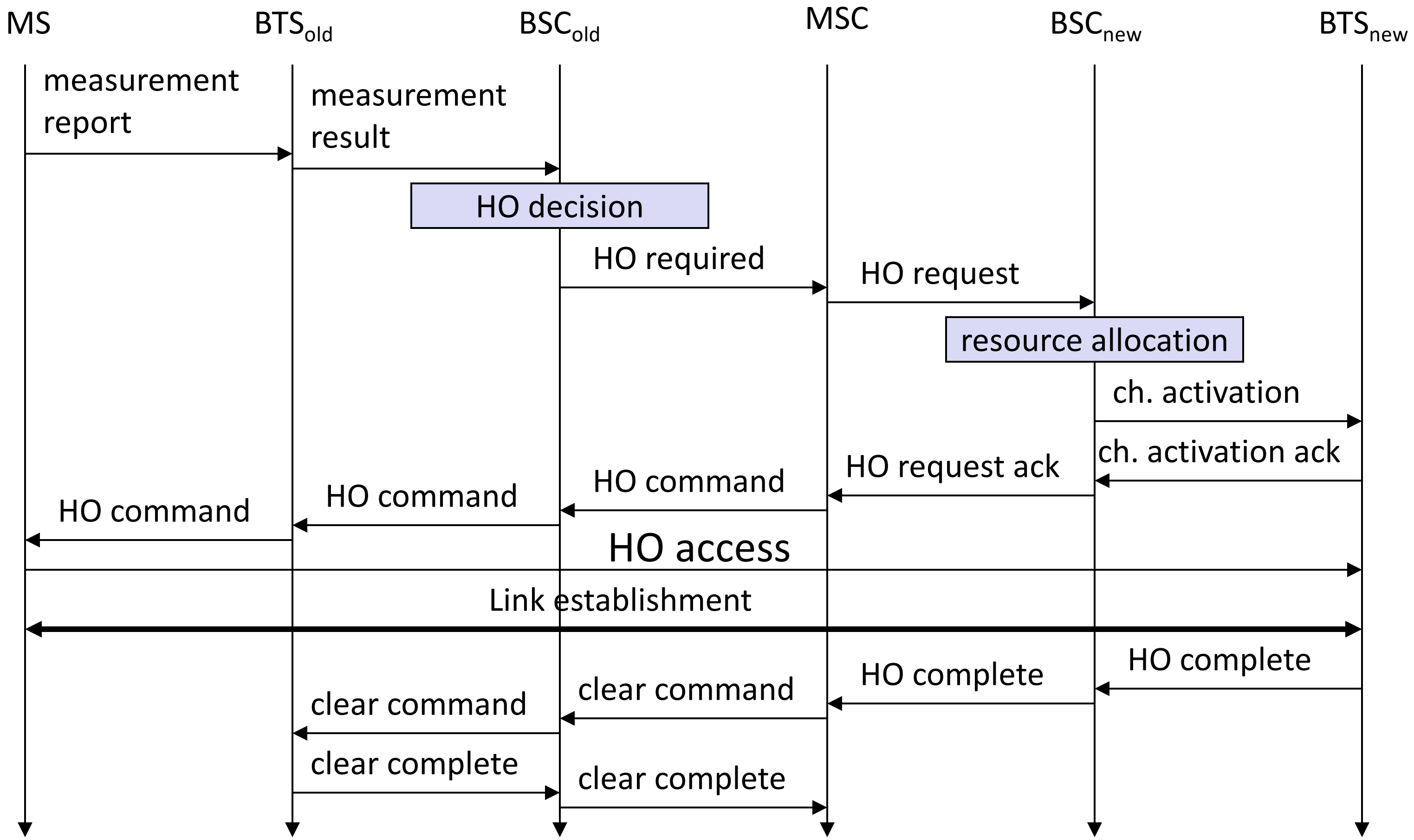
Ref : Schiller p119

Handover decision

Handover occurs when the received signal strength at the MS received from the "old" BTS falls below a defined threshold, and the received signal from a "new" BTS exceeds it by a defined margin.



Handover procedure



MS

BTS$_{old}$

BSC$_{old}$

MSC

BSC$_{new}$

BTS$_{new}$

measurement report

measurement result

HO decision

HO required

HO request

resource allocation

ch. activation

ch. activation ack

HO request ack

HO command

HO command

HO command

HO access

Link establishment

HO complete

HO complete

clear command

clear command

clear complete

clear complete

Ref : Schiller p119

Mobile Speech coding

- Traditionally fixed line telephony uses conventional Pulse Code modulation (PCM) :
  - Speech bandwidth : 3.4kHz
  - Sampling rate : 8,000 samples / second.
  - Sample size : 8 bits
  - Therefore, aggregate bit rate = 8 x 8,000 = **64k bits/second**
- PCM is not suitable for mobile telephony. A much higher bandwidth efficiency is required.
- To achieve higher bandwidth efficiency in voice transmission, an **Audio Codec** or **Vocoder** is used to compress/decompress the voice signal.
- Modern audio codecs use a technique known as **linear prediction**, which involves constructing a mathematical model of the human vocal tract.

Mobile voice codec algorithms

- **Code Excited Linear Prediction (CELP) :** The most widely used codec algorithms and the basis of other voice codecs including ACELP, RCELP, VSELP, etc. The main principle behind the CELP codec is that is uses a principle known as "**Analysis by Synthesis**“ wherein encoding is performed by perceptually optimising the decoded signal in a closed loop system.

- **Algebraic Code Excited Linear Prediction (ACELP) :** A development of the CELP model. However the ACELP codec codebooks have a specific algebraic structure as indicated by the name.

- **Vector Sum Excitation Linear Prediction codec (VSELP) :** One of the major drawbacks of the VSELP codec is its limited ability to code non-speech sounds. This means that it performs poorly in the presence of noise. As a result this voice codec is not now as widely used, other newer speech codecs being preferred and offering far superior performance.

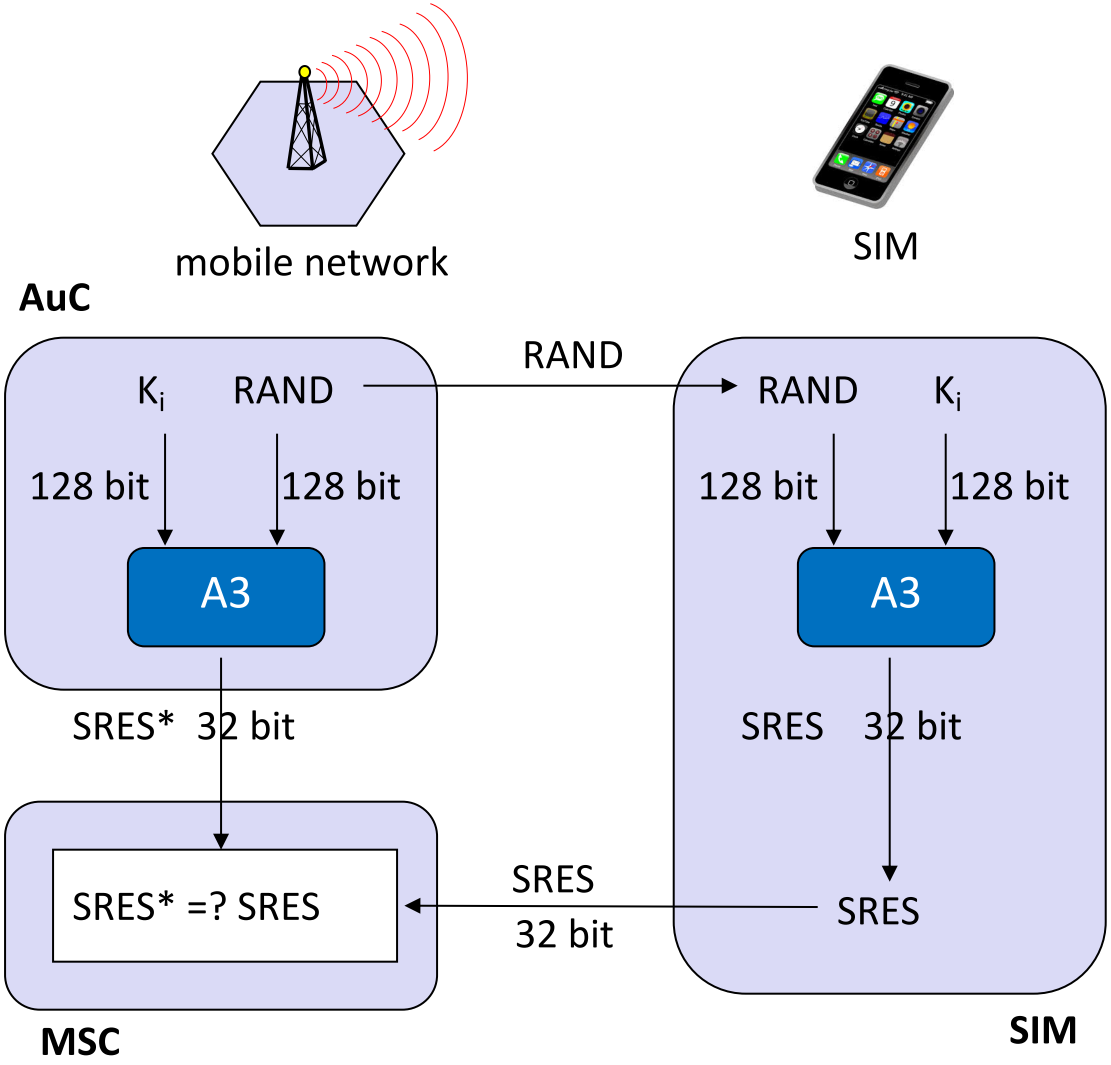
Mobile Speech coding standards

Mobile System	Speech coding Algorithm	Bitrate
GSM (Full rate)	RPE-LTP	13 kbps
GSM (Half rate)	VSELP	5.6 kbps
GSM (Enhanced full rate)	ACELP	12.2 kbps
UMTS (AMR)	ACELP	12.2 to 4.75 kbps

Compare the above with standard PCM : 64k bps

GSM authentication

- Each SIM contains a secret key **Ki** unknown to the user but known by the network and stored in the mobile's HLR record.
- To authenticate a user, the network generates and sends a random number, **RAND,** to the mobile which then uses Ki and RAND as input parameters to a secret algorithm **A3** that generates a response, **SRES,** which is returned to the network.
- The network also generates SRES in the mobile's HLR using Ki , RAND and A3.
- If both SRESs are the same then the mobile is accepted.
- While the computation of SRES from Ki and RAND is straight-forward, the computation of Ki from RAND and SRES is not.



K_i: individual subscriber authentication key

SRES: signed response

GSM Roaming

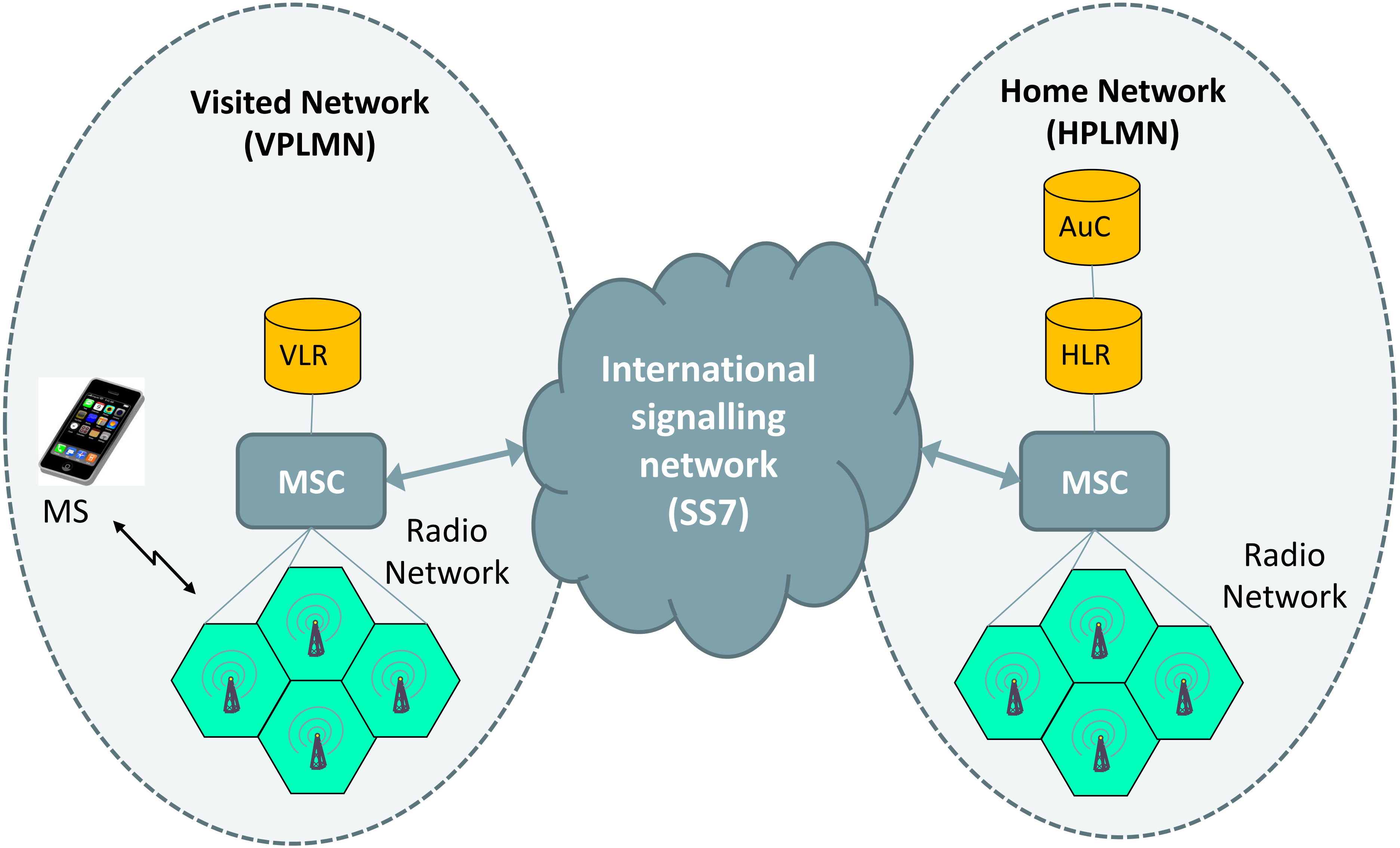
- International roaming, i.e. the facility for the subscriber to take their GSM handset to another country and use it on another network, without having to change SIMs, was one of the core requirements of the original GSM specifications.
- International roaming was the key differentiator between GSM and the earlier 1G (analogue) systems
- The necessary conditions for roaming are :

1. A handset which can receive and send on the frequencies used by the GSM network in the country you are visiting.
2. A roaming agreement between your operator and the one you wish to connect to in the country you are visiting
3. Roaming function enabled on your phone (may depend on you tariff plan).

GSM Roaming

- When the mobile device is turned on or is transferred via a handover to a new network, the new (**visited**) network recognises that the handset is not registered as one of its own subscribers, and then attempts to identify the home network from the IMSI (which is stored in the SIM).
- If there is no roaming agreement between the two networks, the visited network denies service.
- If roaming is allowed, the **visited** network contacts the **home** network HLR over the SS7 network and copies the subscriber profile from the home network HLR to the visited network VLR.
- The visited network begins to maintain a temporary subscriber record for the device in the VLR. Likewise, the home network updates its information to record the location of the subscriber on the visited network, so that any information sent to that device can be correctly routed.

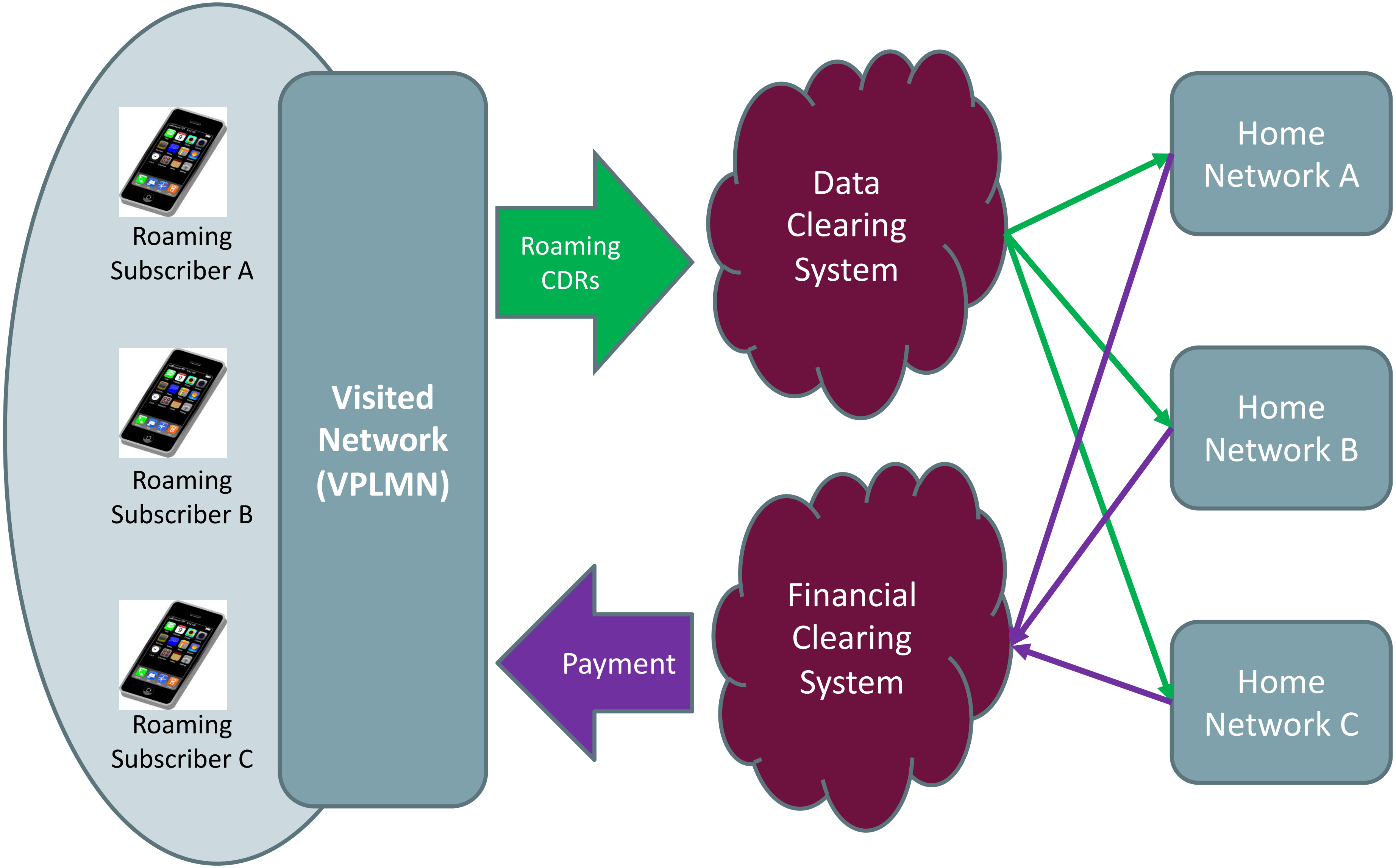
GSM Roaming


Visited Network
(VPLMN)
VLR
MSC
MS
Radio
Network
International
signalling
network
(SS7)
Home Network
(HPLMN)
AuC
HLR
MSC
Radio
Network

GSM Roaming : MT calls

- When someone calls a roaming subscriber, the call is routed on the MSISDN to the home network GMSC.
- The home network HLR records indicate that the subscriber is roaming. The HLR record also contains the exact location (LAI) of the subscriber, which has been continuously updated every time the MS has moved from on BTS to another.
- The VLR assigns a Mobile Station Roaming Number (MSRN) to the roaming subscriber which is a unique virtual number to which incoming calls can be routed. Once the incoming call is established, the MSRN is released back into the pool and can be re-used.

GSM Roaming billing



GSM Roaming : billing

- The retail charge for all traffic generated by a roaming subscriber (MO or MT) whilst they are on the visited network will appear on their monthly (?) bill which is issued by their home network. This normally appears on the subscribers bill as “roaming charges”.
- How does the home network know how much usage there has been when the subscriber was roaming?
- The visited network MSC generates **Call Detail Records (CDRs)** for all the MS on their network, including roamers.
- Every day, the visited network sends it’s CDR files to a **Data Clearing House** which sorts the CDRs according to home network ID (MNC code) which is contained in the IMSI.
- The Data Clearing House collates the CDRs according to home network ID, rates them according to **Inter-Operator Tariff (IOT)** and sends them off to the relevant parties.
- At the end of the month (?) the various home networks settle the wholesale cost of their roaming subscribers usage on the various visited networks, according to the rated CDRs they have received through Data Clearing. Payment is done through a **Financial Clearing House**.
- The Financial Clearing House collates all the payments from the various home networks and delivers them to the correct visited network.