Chapter: 9 GSM System Overview

Prepared by: Prajapati Tejas K.

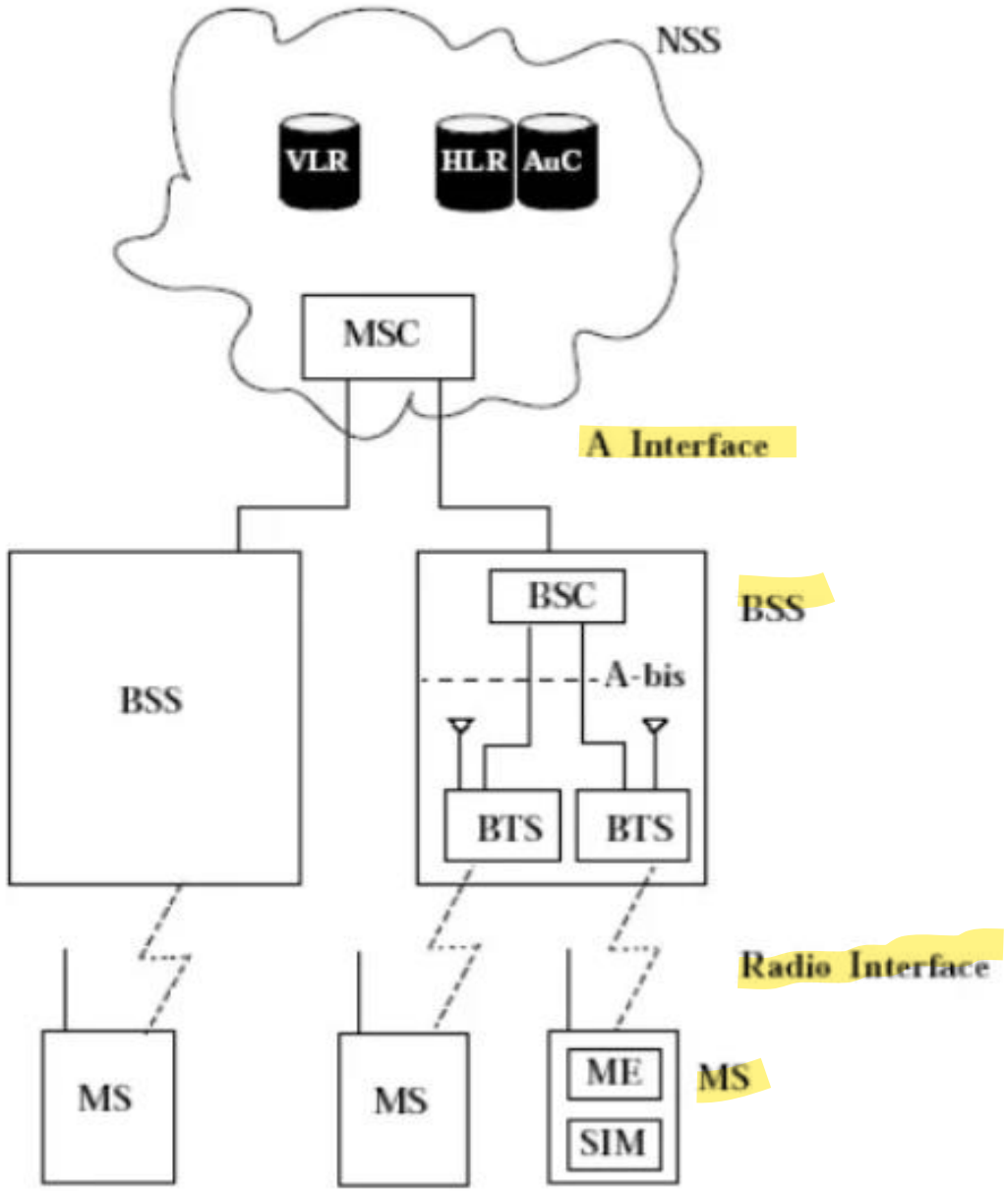
Introduction

- Global System for Mobile Communications (GSM) is a digital wireless network standard designed by standardization committees from major European telecommunications operators and manufacturers.
- Provides a common set of compatible services and capabilities to all mobile users across Europe and several million customers world wide.

The basic requirements of GSM

- **Services:** The system shall provide service portability
- **QoS and Security:** The quality for voice telephony of GSM shall beat least as good as the previous analog systems over the practical operating range.
- **Radio Frequency Utilization:** permit a high level of spectrum efficiency and state-of-the-art subscriber facilities
- **Network:** The identification and numbering plans shall be based on relevant ITU recommendations.
- **Cost:** The system parameters shall be chosen with a view to limiting the cost of the complete system, in particular the MSs.

GSM Architecture



- Mobile station (MS) communicates with a base station system(BSS) through the radio interface.
- BSS is connected to the network and switching subsystem (NSS) by communicating with a mobile switching center (MSC) using the A

Mobile Station (MS)

- The MS consists of two parts : the subscriber identity module (SIM) and the mobile equipment (ME).
- A SIM can be a smart card, a smaller sized "plug-in SIM", a smart card that can be performed, which contains a plug-in SIM that can be broken out of it.
- The ME contains the non-customer-related hardware and software specific to the radio interface.
- When the SIM is removed from an MS, the remaining ME cannot be used for reaching the service except for emergency calls.

Base Station System (BSS)

- The BSS connects the MS and the NSS.
- The BSS consists of two parts : the base transceiver station (BTS) and the base station controller(BSC).
- The BTS contains transmitter, receiver, and signaling equipment specific to the radio interface in order to contact the MSs.
- The BSC is responsible for the switching functions in the BSS, and is in turn connected to an MSC in the NSS.
- The BSC supports radio channel allocation/ release and handoff management.

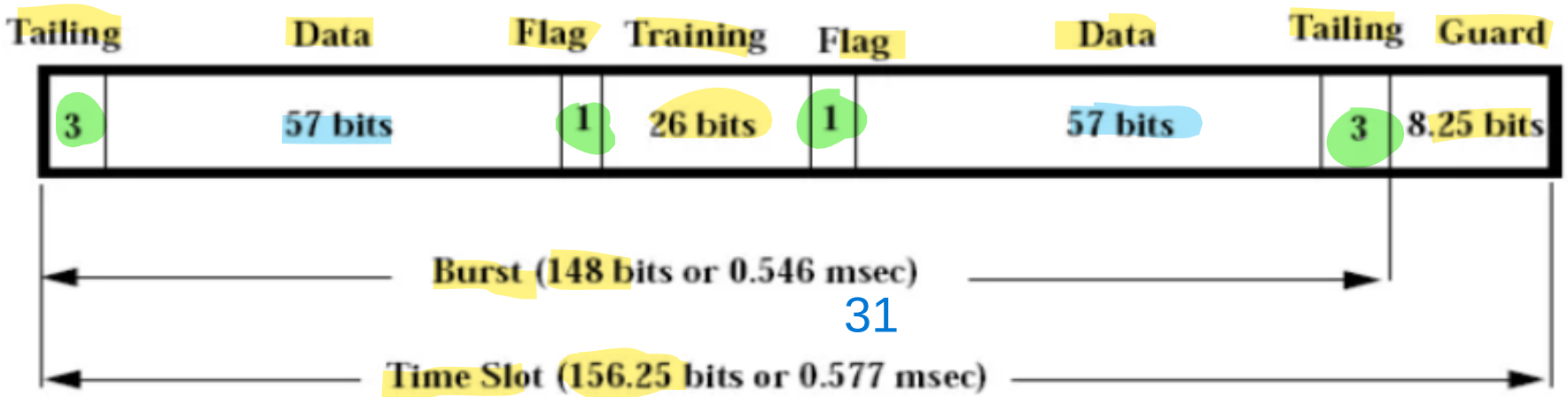
Network and Switching Subsystem (NSS)

- The NSS supports the switching functions, subscriber profiles, and mobility management.
- The basic switching function in the NSS is performed by the MSC.
- An incoming call is routed to an MSC, unless thefixed network is able to interrogate the HLR directly. That MSC is called the gateway MSC (GMSC).

Radio Interface

- The GSM radio link uses both FDMA and TDMA technologies.
- The frequency bands for the GSM down link signal and the uplink signal are 935-960 MHz and 890-915 MHz, respectively.
- The frequency band is divided into 124 pairs off frequency duplex channels with 200 KHz carrier spacing.
- To save MS power, uplink frequencies in mobile systems are always the lower band of frequencies.

GSM Burst Structure



- The length of a GSM frame in a frequency channel is 4.615 msec. 0.577*8 = 4.615
- The frame is divided in to 8 bursts (timeslots) of length 0.577 msec.

GSM Burst Structure

- Depending on the information carried by a time slot, i.e., the in formation bits in figure, two types of logical channels are defined : the **traffic channels (TCHs)** and **the control channels (CCHs)**.
- **Two kinds of TCHs are defined :**

✓ Full rate TCH (TCH/F) provides transmission speed of 13Kb/s for speech or 9.6, 4.8 or 2.4Kb/s for data. Enhanced Full Rate (EFR) speech coders have been implemented to improve the speech quality of a TCH/F.

✓ Half rate TCH(TCH/H) allows transmission of 5.6Kb/s speech or 4.8 or 2.4Kb/s data.

GSM Burst Structure

- The CCHs are in tended to carry signaling in formation.
- Three types of CCHs are defined in GSM:

✓ **Common control channels (CCCHs)** include the following channel types: The paging channel (PCH) is used by the network to page the destination MS in call termination, The access grant channel (AGCH) is used by the network to indicate radio link allocation up on prime access of an MS, The random access channel (RACH) is used by the MSs for initial access to the network.

GSM Burst Structure

- ✓ **Dedicated control channels** are supported in GSM for dedicated use by a specific MS.
- ✓ The **standalone dedicated control channel (SDCCH)** is used only for signaling and for short messages.
- ✓ The **slow associated control channel (SACCH)** is associated with either a TCH or an SDCCH.
- ✓ The **fast associated control channel (FACCH)** is used for time critical signaling such as call establishing progress, authentication of subscriber, or handoff.

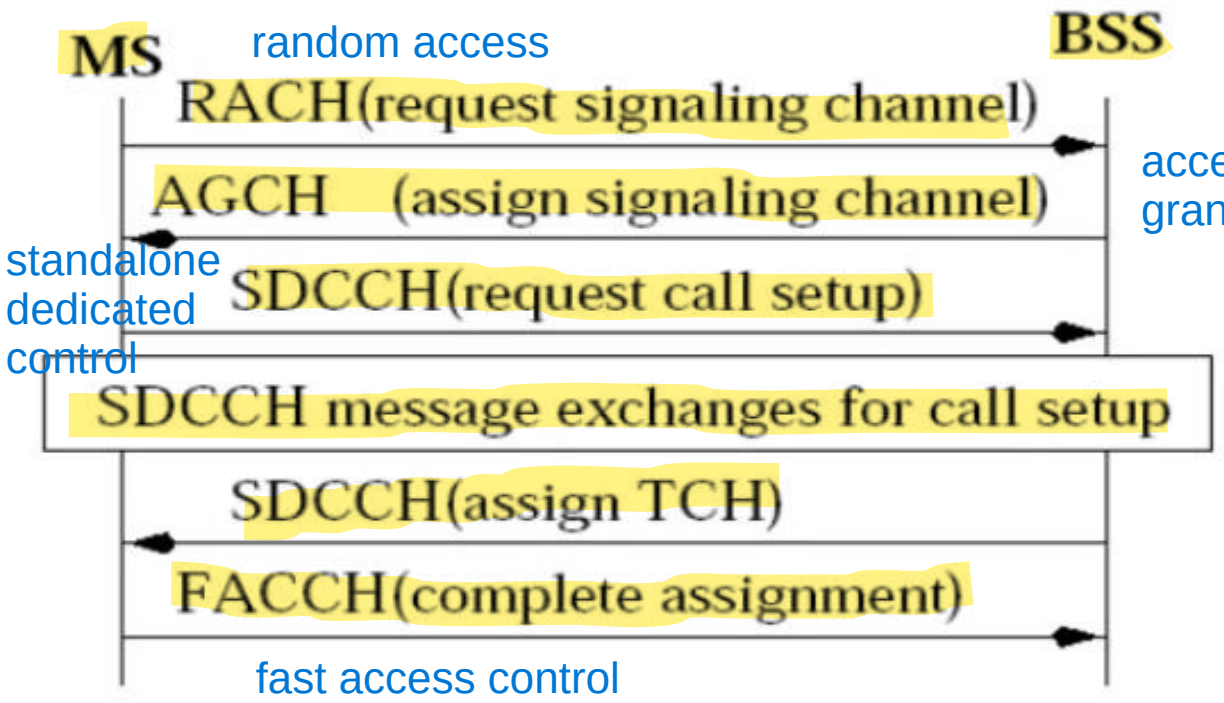
GSM Burst Structure

- ✓ The **cell broad cast channel (CBCH)** only carries the short message service cell broad cast messages, which uses the same time slot as the SDCCH.
- ✓ **Broad cast channels (BCHs)** is used by the BTS to broad cast information to the MSs in its coverage area.
- ✓ The **frequency correction channel (FCCH)** and the **synchronization channel (SCH)** carry information from the BSS to the MS. The information allows the MS to acquire and stay synchronized with the BSS.

GSM Burst Structure

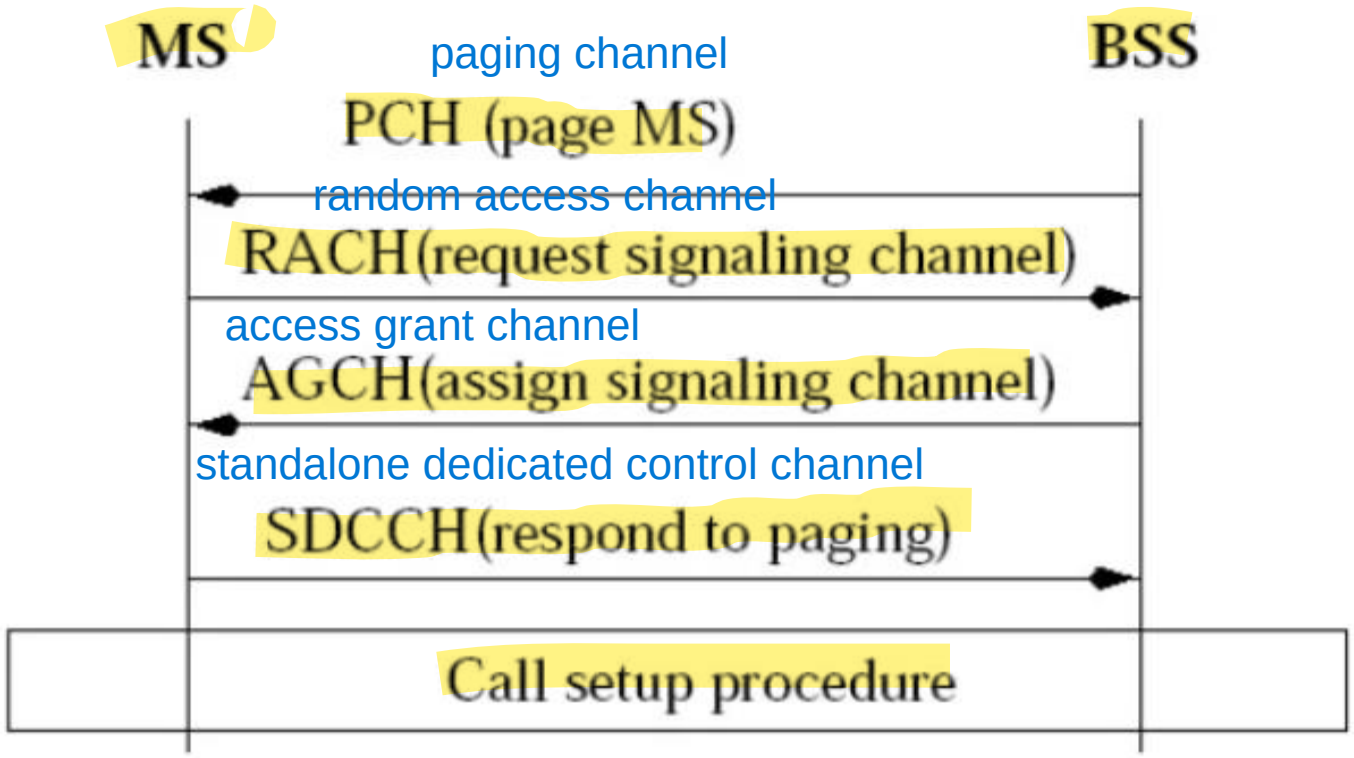
- ✓ The **broad cast control channel (BCCH)** provides system information such as access information for the selected cell and information related to the surrounding cells to support cell selection and location registration procedures in an MS.

GSM Call Origination (Radio Aspect)



- To initiate the call setup, the MS sends a signaling channel request to the network through RACH.
- The BSC informs the MS of the allocated signaling channel (SDCCH) through AGCH.
- Then the MS sends the call origination request via SDCCH. The MSC instructs the BSC to allocate a TCH for this call.
- Finally, both the MS and the

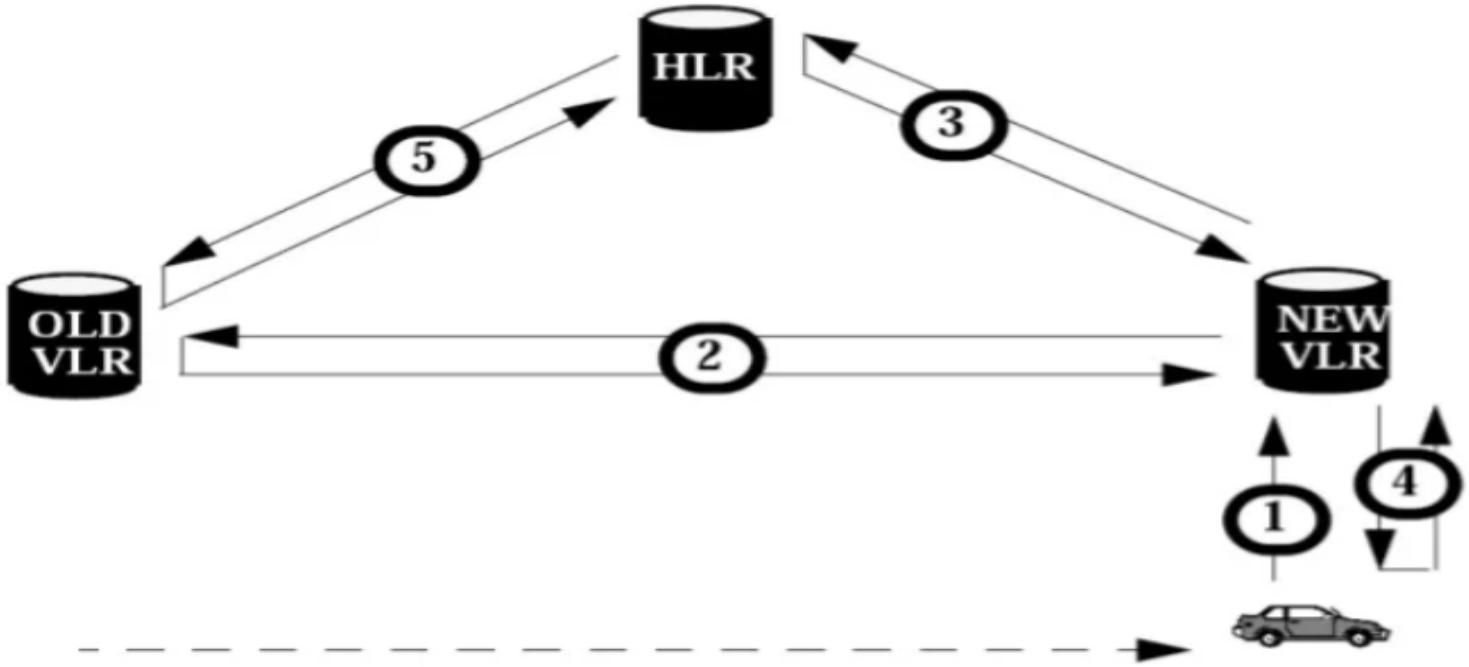
GSM Call Termination (Radio Aspect)



- In this case the MSC requests the BSS to page the MS.
- The BSCs instruct the BTSs in the desired LA to page the MS by using PCH.
- When the destination MS receives the paging message, it requests for a SDCCH.
- The BTS assigns the SDCCH, which is used to setup the call as in

Location Tracking and Call Setup

- **The MS Registration Process**



•**Step1.** The MS periodically listens to the BCCH broad cast from the BSS. broadcast control channel

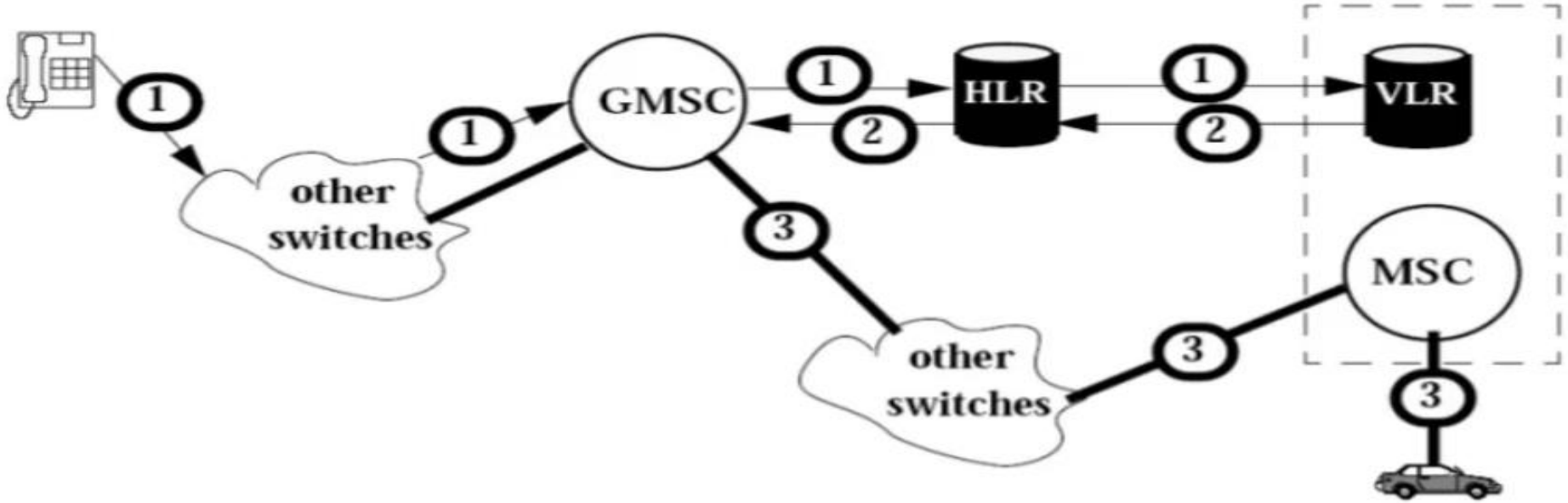
•**Step2.**The new VLR communicates with the old VLR tofind the HLR of the MS.

•**Step3.** After the MS is authenticated, the new VLR sends a registration message to the HLR.

•**Step4.** The new VLR informs the MS of the successful registration.

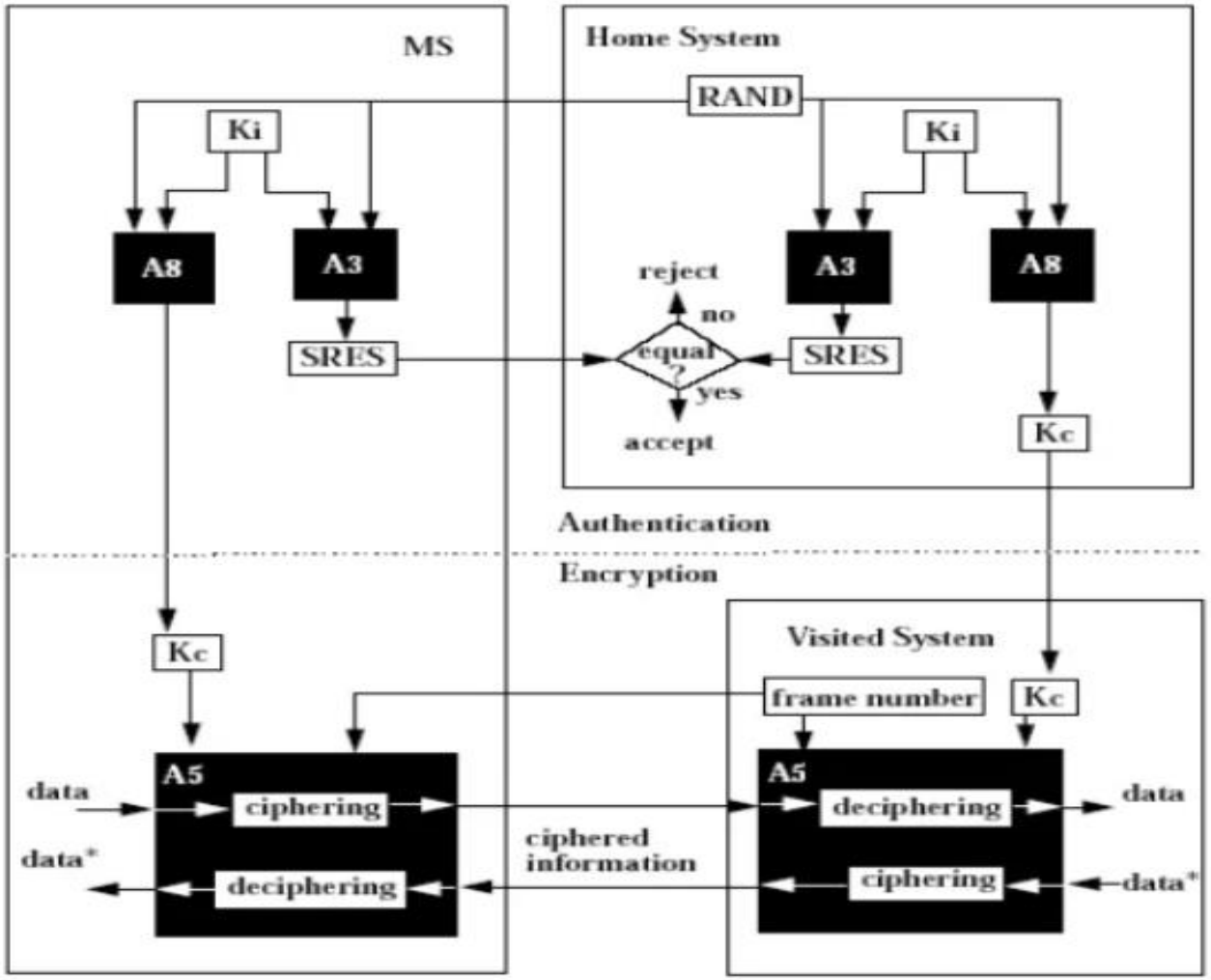
•**Step5.** After Step3, the HLR sends a deregistration (cancellation) message to the old VLR.

- **The Mobile Call Termination (Delivery) Procedure**



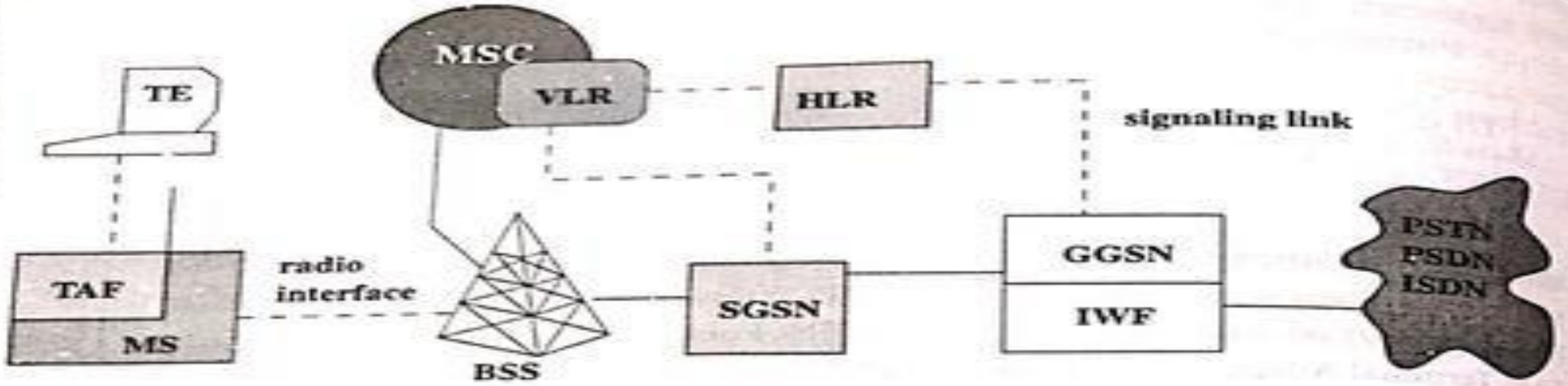
- **Step1.** When the MSISDN is dialed, the call is forwarded to the GMSC, a switch that has the capability to interrogate the HLR for routing in formation.
- **Step2.** The VLR returns the MSRN(mobile station roaming number) to the GMSC through the HLR.
- **Step3.** The GMSC uses the MSRN to route the call to the MS through the visited MSC.

Security



- GSM security is addressed in two aspects: authentication and encryption.
- Authentication avoids fraudulent access of a cloned MS.
- Encryption avoids unauthorized listening.

Data Services in GSM GPRS



HLR: Home Location Register
VLR: Visitor Location Register
MSC: Mobile Switching Center
MS: Mobile Station (Handset)
BSS: Base Station Subsystem
TAF: Terminal Adaption Functions

SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
TE: Terminal Equipment
IWF: Interworking Functions
PSTN: Public Switched Telephone Network
PSDN: Public Switched Data Network

GPRS introduces new network elements

• Serving GPRS Support Node (SGSN)

• authentication & authorization, GTP tunneling to GGSN, ciphering & compression, mobility

management, session management, interaction with HLR,MSC/VLR, charging & statistics,

as well as NMS interfaces.

• Gateway GPRS Support Node (GGSN)

• interfacing to external data networks (basically it is a network router)

encapsulating data packets in GTP and forwarding them to right SGSN,

routing mobile originated packets to right destination, filtering end user traffic, as well as collecting charging and statistical information of data network usage.

GPRS is the result of committees trying to “adapt” Mobile IP to GSM systems.

Introduction

- To exercise location tracking, a mobile service area is partitioned into several Location Areas (LA) or registration areas.
  - **Every LA consists of a group of BTSs.**
- The major task of mobility management is to update the location of an MS when it moves from one LA to another.

Location Update Concept (Registration)

- The location update (registration) procedure is initiated by the MS.
- **Step 1.** The BTs periodically broadcast the corresponding LA addresses to the MSs.
- **Step 2.** When an MS receives an LA address different from the one stored in it memory, it sends a registration message to the network.
- **Note that**
  - **Every VLR maintains the information of a group of LAs. When an MS visits an LA, a temporary record of the MS is created in the VLR to indicate its location (i.e. LA address).**
  - **For every MS, a permanent record is maintained in HLR. The record stores the address of VLR visited by the MS.**

Two Issues of GSM Mobility Databases

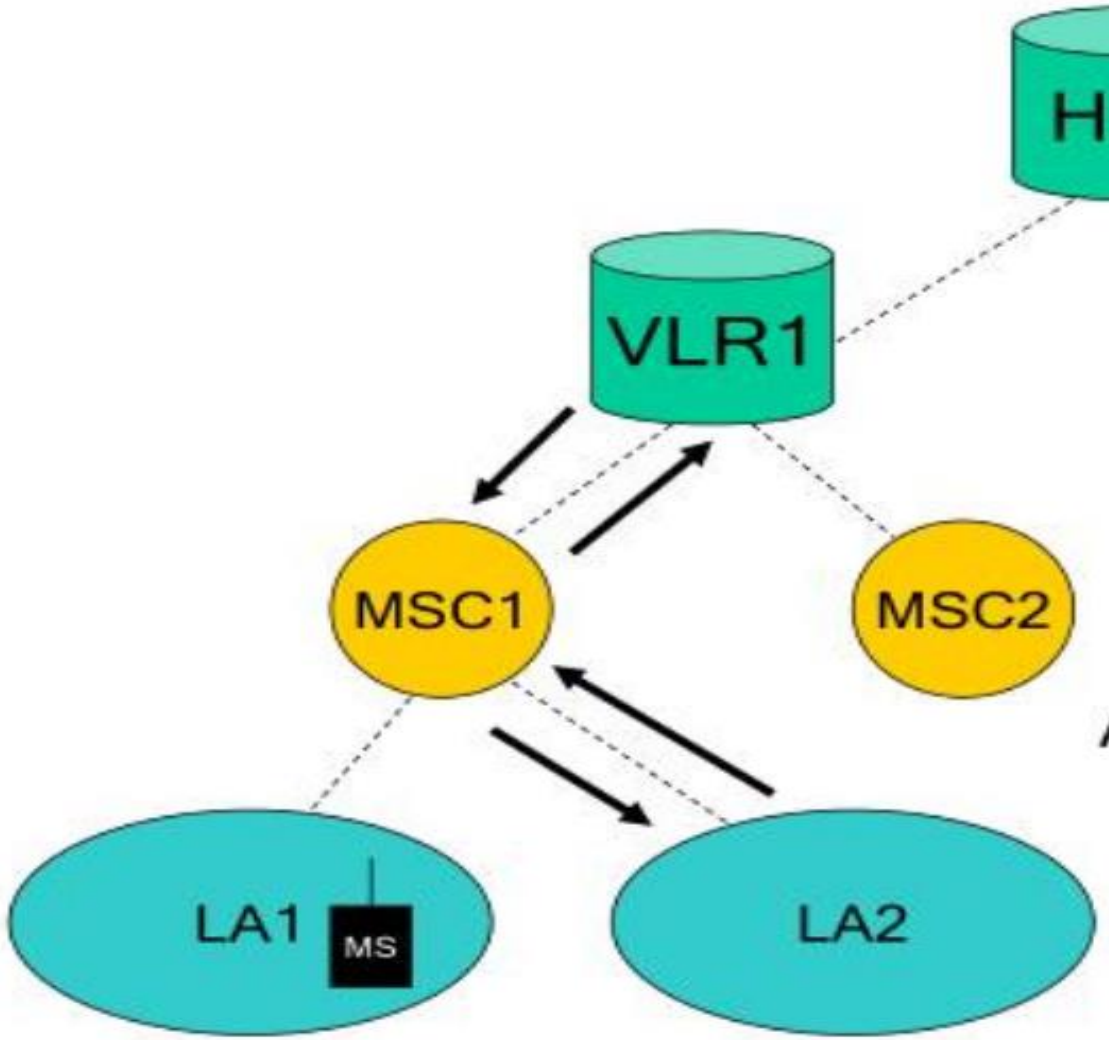
- **Fault Tolerance.**
  - If the location database fail, the loss or corruption of location information will seriously degrade the service offered to the subscribers.
- **Database Overflow.**
  - The VLR may overflow if too many users move into the VLR-controlled area in a short period.
  - If the VLR is full when a mobile user arrives, the user fails to register in the database, and thus cannot receive cellular service.
  - This phenomenon is called VLR overflow.

GSM Basic Location Update Procedur e

- **Case 1.** Inter-LA Movement
- **Case 2.** Inter-MSC Movement
- **Case 3.** Inter-VLR Movement

Basic Location Update Procedure(1/3)

- Case 1: Inter-LA Movement



HLR: Home Location Register

VLR: Visitor Location Register

MSC: Mobile Switching Center

LA: Location Area

MS: Mobile Station

GSM Basic Location Update: Inter-LA Movement (1/3)

- The MS moves from LA1 to LA2, where both LAs are connected to the same MSC.
- In GSM 04.08, Nine message are exchanged between the MS and the MSC, and ten messages are exchanged between the MSC and the VLR.
- Four major steps are discussed here.

GSM Basic Location Update: Inter-LA Movement (2/3)

⌘ Step 1.

- A location update request message is sent (MS->BTS->MSC) .

  Location Update Request (Prev. LA, Prev. MSC, Prev. VLR). Note that New MSC = Prev. MSC, New VLR = Prev. VLR

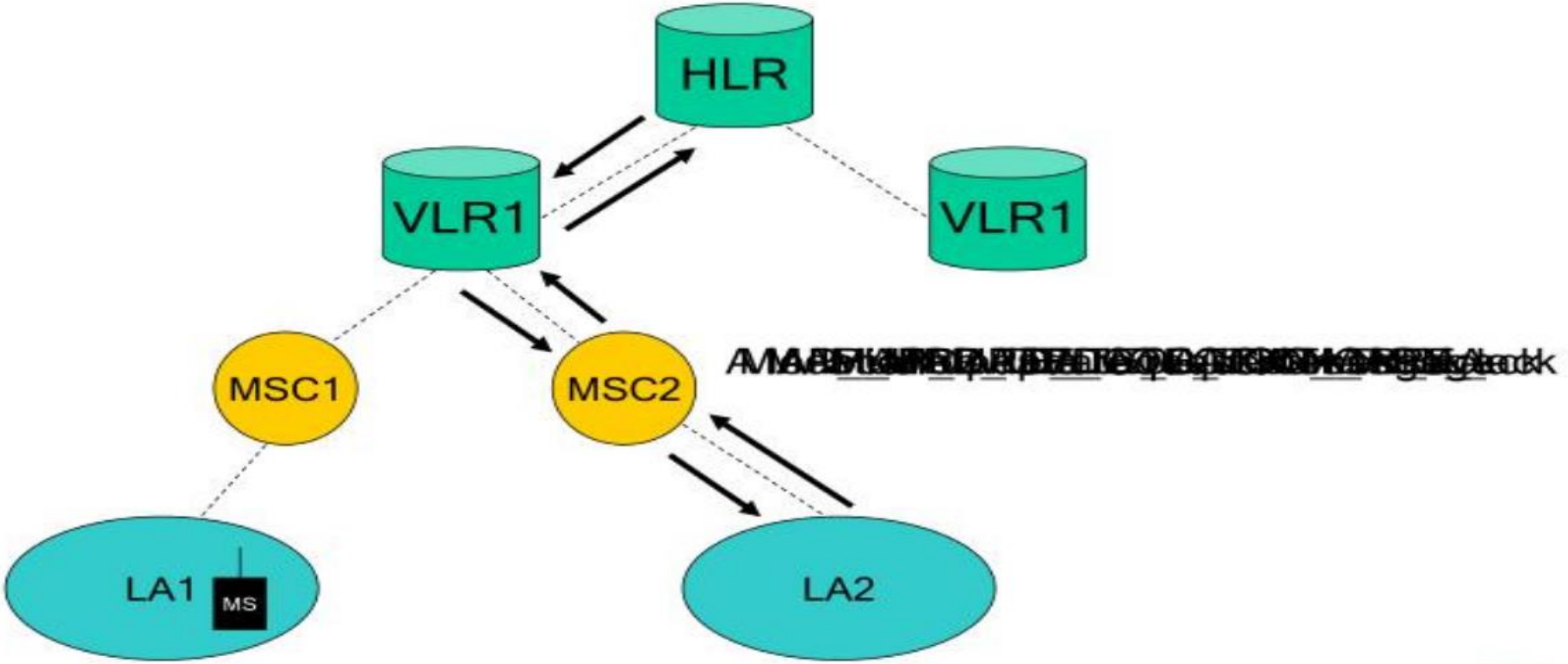
- The MS identifies itself by the Temporary Mobile Subscriber Identity (TMSI), which is an alias for IMSI.
- IMSI (International Mobile Subscriber Identity) is used to identify the called. IMSI is not known to the User but GSM network.
- TMSI is used to avoid sending the IMSI on the radio path, which is temporary identity is allocated to an MS by the VLR at inter-VLR registration, and can be changed by the VLR.

GSM Basic Location Update: Inter-LA Movement (3/3)

- **Step 2.** The MSC forwards the location update request to the VLR by a TCAP message, MAP_UPDATE_LOCATION_AREA.
  - **This message includes (Address of the MSC, TMSI of MS, Prev. Location Area Identification (LAI), Target LAI, Other Related Information).**
- **Steps 3 and 4.**
  - **Part I. The VLR notices that both LA1 and LA2 belong to the same MSC.**
  - **Part II. The VLR updates the LAI field of the VLR record.**
  - **Part III. The VLR replies an ACK to the MS through the MSC.**

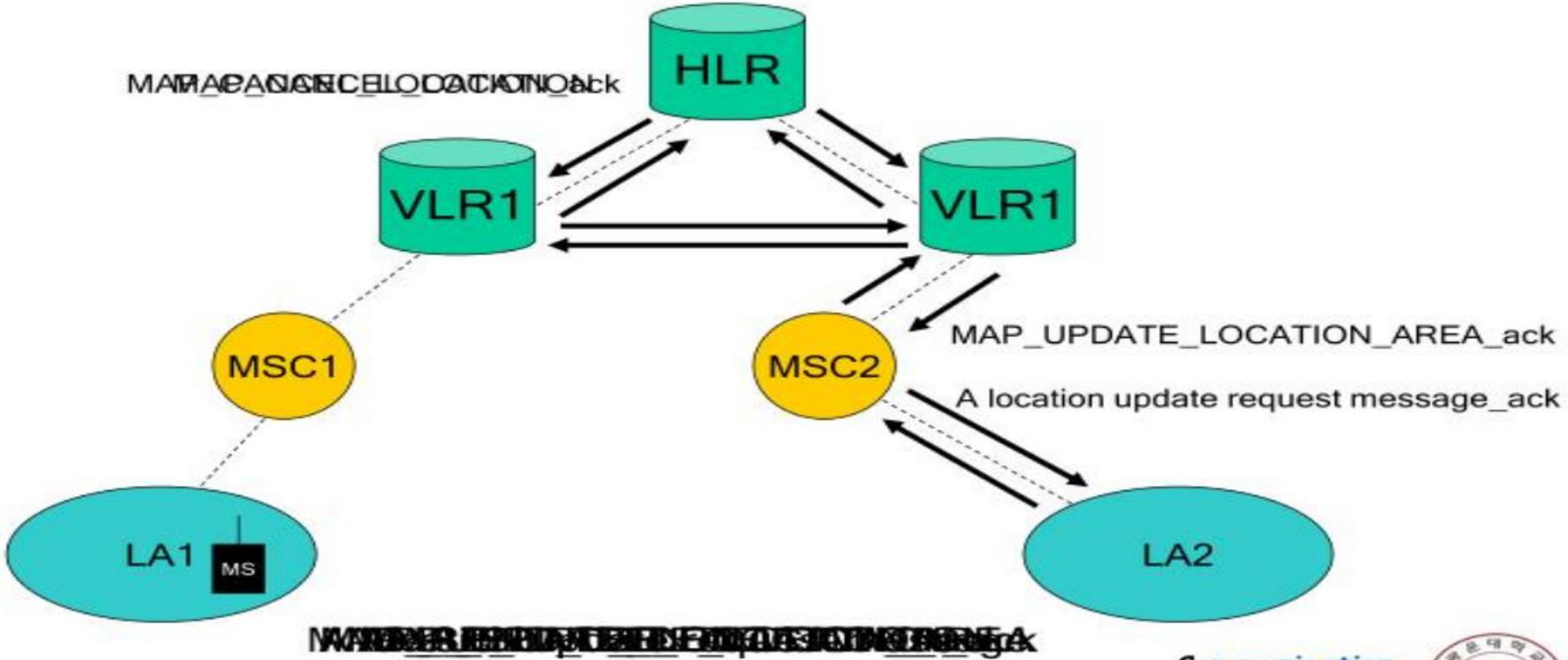
Basic Location Update Procedure(2/3)

- Case 2: Inter-MSC Movement



Basic Location Update Procedure(3/3)

- Case 3: Inter-VLR Movement



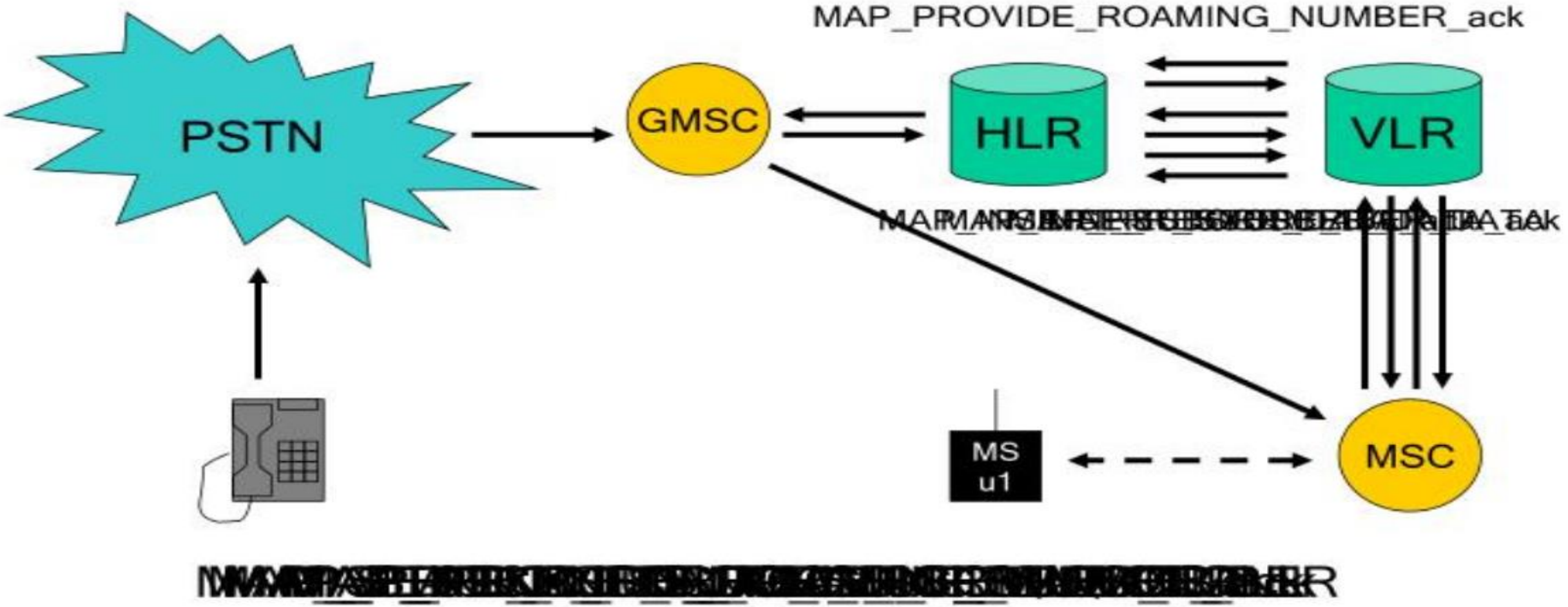
VLR Failure Restoration(1/2)

- MS registration
  - A case of inter-VLR movement
  - Recovered by the normal registration procedure
  - Can't be recognized TMSI
  - Be asked to send IMSI

- MS call origination
  - System error : "unidentified subscriber"
  - Be asked to initiate the location registration procedure

VLR Failure Restoration(2/2)

- MS call termination



VLR Failure Restoration

- **Service Information** of a VLR record recovered by
  - **The first contact between the VLR and the HLR of the corresponding MS.**
- **Location Information** of a VLR record recovered by
  - **First radio contact between the VLR and the MS**
- **Mobile Station Information** of a VLR record recovered by
  - **Either by contact with the HLR or the MS**

VLR Record Restoration Initiation Event 1—MS Registration

- The VLR considers the registration as a case of inter-VLR movement.
- Following the normal registration procedure defined in inter-VLR movement.
- In this case, the TMSI sent from the MS to the VLR cannot be recognized, and the MS is asked to send IMSI over the air.

VLR Record Restoration Initiation Event 2—MS Call Origination

- When the VLR receives the call origination request **MAP_SEND_INFO_OUTGOING_CALL** from the MSC, the VLR record of the MS is not found.
- The VLR considers the situation as a system error, with the cause "**unidentified subscriber**".
- The request is rejected, and the MS is asked to initiate the location registration procedure.

VLR Record Restoration Initiation Event 3—MS Call Termination (1/)

- **Steps 1-3.** Similar to the first three steps of the basic call termination procedure, the VLR is queried to provide the MSRN.
  - **Note that since the record has been erased after the failure, the search fails. The VLR creates a VLR record for the MS.**
  - **Neither the service nor the location info is available.**
- **Steps 4 and 7.**
  - **Since the VLR does not have the routing information, it uses the MSC number provided by MAP_PROVIDE_ROAMING_NUMBER message to create MSRN.**
  - **The number is sent back to the gateway MSC to setup the call in Step 8.**

VLR Record Restoration Initiation Event_3—MS Call Termination (2/)

⌘ **Steps 5 and 6.**

- **The VLR recovers the service information of the VLR record by sending a MAP_PROVIDE_ROAMING_NUMBER message to the HLR.**
- **The HLR sends the service information to the VLR using the MAP_INSERT_SUBSCRIBER_DATA message.**
- **At this point, the service information of the VLR record has been recovered.**
- **However, the location information, specifically, the LAI number, still not available. This information will be recovered at Step 11.**

⌘ **Note that** Steps 4 and 5 can be executed in parallel.

VLR Record Restoration Initiation Event 3—MS Call Termination (3/)

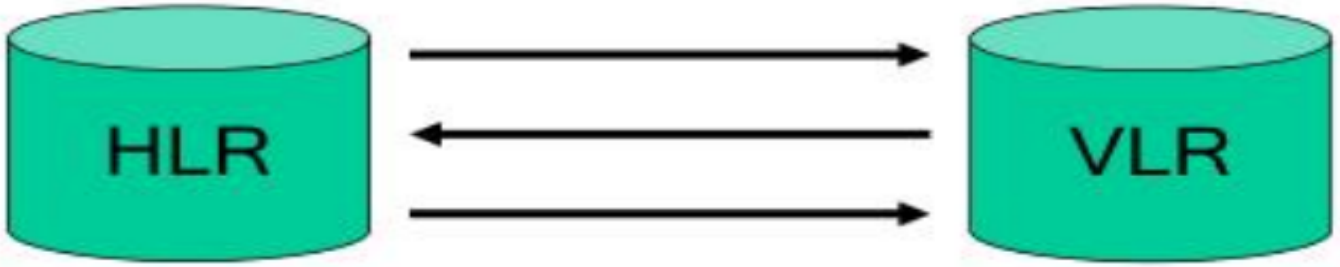
- **Step 8.** After the gateway MSC receives the MSRN in Step 7, the SS7 ISUP message IAM is sent to the target MSC.
- **Steps 9-11.**
  - **The target MSC does not have the LAI info of the MS.**
  - **In order to proceed to set up the call, the MSC sends the message MAP_SEND_INFO_FOR_INCOMING_CALL to the VLR.**
  - **Unfortunately, the VLR does not have the LAI info either.**
  - **Hence the VLR asks the MSC to determine the LA of the MS by sending a MAP_SEARCH_FOR_MOBILE_SUBSCRIBER message.**

VLR Record Restoration Initiation Event 3—MS Call Termination (4/4)

- **Steps 12 and 13.**
  - The MSC initiates paging of the MS in all LAs.
  - If the paging is successful, the current LA address of the MS is sent back to the VLR by the MAP_PROCESS_ACCESS_REQUEST message.
  - At this point, the location information of the VLR record is recovered.
- Note that
  - MAP_SEARCH_FOR_MOBILE_SUBSCRIBER is an expensive operation because every BTS connected to the MSC must perform the paging operation.
  - To avoid this “Wide Area Paging”, the GSM system may periodically asks the MSs to re-register.

HLR Failure Restoration

- Uncovered period
- HLR restoration procedure



MAP_RESTORE_DATA
MAP_INSERT_SUBSCRIBER_DATA
MAP_DELETE_SUBSCRIBER_DATA
MAP_SEND_INFORMATION_ACK

HLR Restoration Procedure (1/3)

- After an HLR failure, the data in the backup are reloaded into the HLR.
- An Uncovered Period = the time interval after **the last backup operation** and **before the restart of the HLR**.
- Data that have been changed in the uncovered period can not be recovered.

HLR Restoration Procedure (2/3)

- **Step 1.** The HLR sends an SS7 TCAP message **MAP_RESET** to the VLRs where its MSs are located.
- **Step 2.** All the VLRs derive all MSs of the HLR. For each MS, they send an SS7 TCAP message, **MAP_UPDATE_LOCATION**, to the HLR.

HLR Restoration Procedure (3/3)

- The HLR restoration procedure is not robust.
  - **An MS may move into a VLR (which does not have any other MSs from the given HLR residing) during the uncovered period.**
  - **The new location is not known to the HLR at the last check- pointing time.**
  - **If so, the HLR will not be locate the VLR of the MS during Step 1 of HLR restoration.**
- VLR Identification Algorithm is to solve the problem.

Thank you