GSM System Overview

Outlines

- Introduction
- GSM Architecture
- GSM Mobility Management
- Security
- GSM Data Services
- Unstructured Supplementary Service Data
- Summary

Introduction

- Global System for Mobile Communications (GSM) is a digital wireless network standard.
- It was developed by Group Special Mobile of Conference Europeenne des Postes et Telecommunications (CEPT) and European Telecommunications Standards Institute (ETSI).
- GSM Phases 1 and 2 define digital cellular telecommunications system.
- GSM Phase 2+ targets on Speech Codec and Data Service.

The Basic Requirements of GSM (1/3)

- Services.
  - The system will provide service portability; that is, MS can be used in all participating countries.
- Quality of Services and Security.
  - The quality for voice telephony of GSM will be at least as good as the previous analog systems.
  - The system will be capable of offering information encryption with lightly extra cost.

The Basic Requirements of GSM (2/3)

- Radio Frequency Utilization.
  - The system will permit a high level of spectrum efficiency.
  - The system will be capable of operating in the entire allocated frequency band, and coexist with the earlier system in the same frequency band.
- Network.
  - The identification and numbering plans will be based on relevant ITU recommendations.

The Basic Requirements of GSM (3/3)

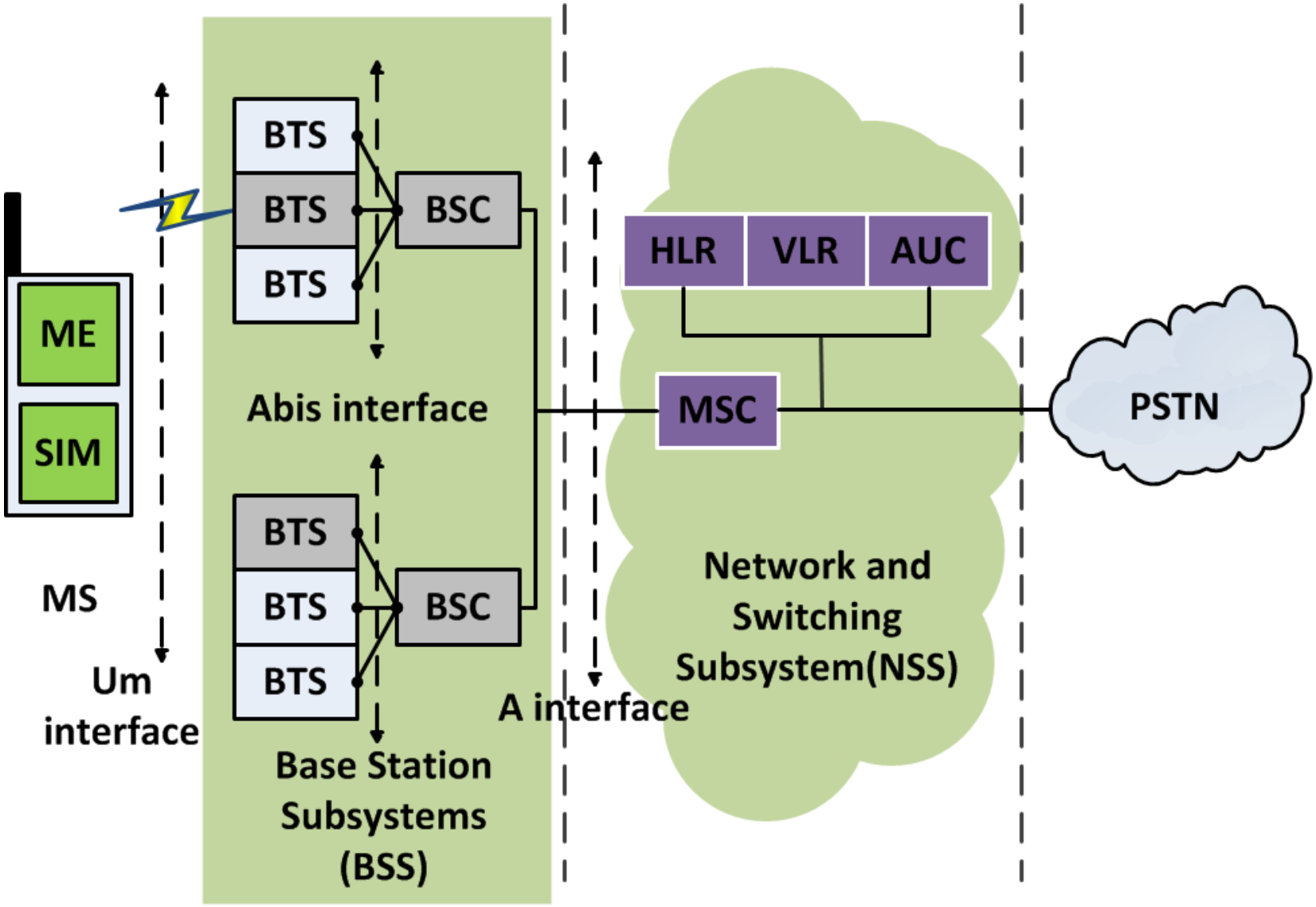
- An international standardized signaling system will be used for switching and mobility management.
- The exiting fixed public networks should not be significantly modified.

- Cost.
  - The system parameters will be chosen with a view to limiting the cost of the complete system, in particular MS.

PART I

GSM Architecture

GSM Architecture



Mobile Station (MS) / Mobile Terminal (MT)

- The MS consists of two parts:
  - the Subscriber Identity Module (SIM) and
  - the Mobile Equipment (ME).
- In a broader definition, the MS also includes a third part called
  - Terminal Equipment (TE), which can be a PDA or PC connected to ME.

Subscriber Identity Module (SIM) (1/4)

- A SIM can be
  - A smart card, usually the size of a credit card
  - A smaller-sized “plug-in SIM”
  - A smart card that can be perforated, which contains a plug-in SIM that can be broken out of it.

Subscriber Identity Module (SIM) (2/4)

- The SIM is protected by a Personal Identity Number (PIN) between 4 to 8 digits.
  - To use MS, the user is asked to enter the PIN.
  - If the number is not correctly entered in 3 time, the SIM is locked.
  - To unlock SIM, the user is asked to enter the 8-digit PIN unblocking Key (PUK).

Subscriber Identity Module (SIM) (3/4)

- Subscriber-Related Information includes
  - PIN, and PUK codes,
  - A list of abbreviated and Customized Short Dialing Numbers,
  - Short Message Received when the subscriber is not present, and
  - Names of Preferred Networks to provide service.

Subscriber Identity Module (SIM) (4/4)

- Parts of the SIM information can be modified by the subscriber either by keypad or a PC using an RS232 connection.
- The SIM card can be updated over the air through SIM Toolkit.

Mobile Equipment (ME)

- The ME contains
  - The Noncustomer-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.
- Usually, the MS is the property of the subscriber.
- The SIM is the property of the service provider.

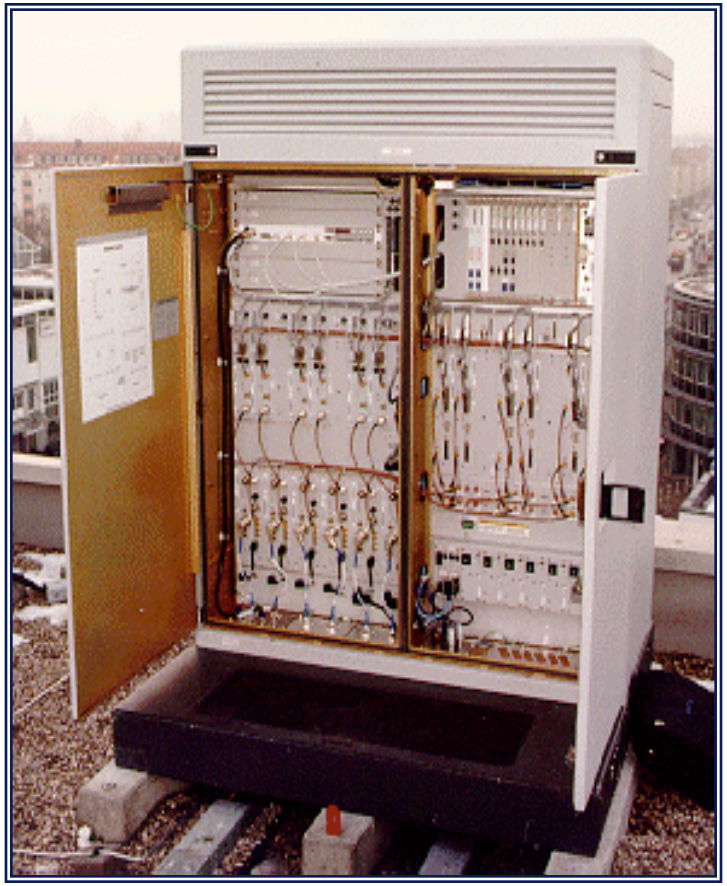
Base Station System (BSS): BTS

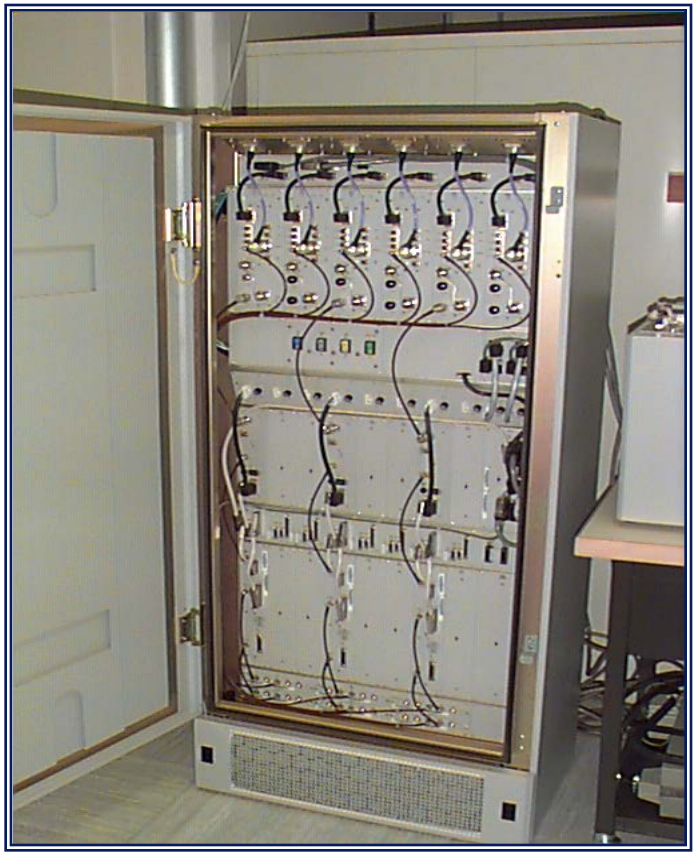
- Base Transceiver Station (BTS) contains
  - Transmitter, Receiver, and
  - Signaling Equipment Specific to the radio interface in order to contact the MSs.
  - Transcoder/Rate Adapter Unit (TRAU) carries out GSM-specific speech encoding/decoding and rate adaptation in data transmission.

Base Station System (BSS): BSC

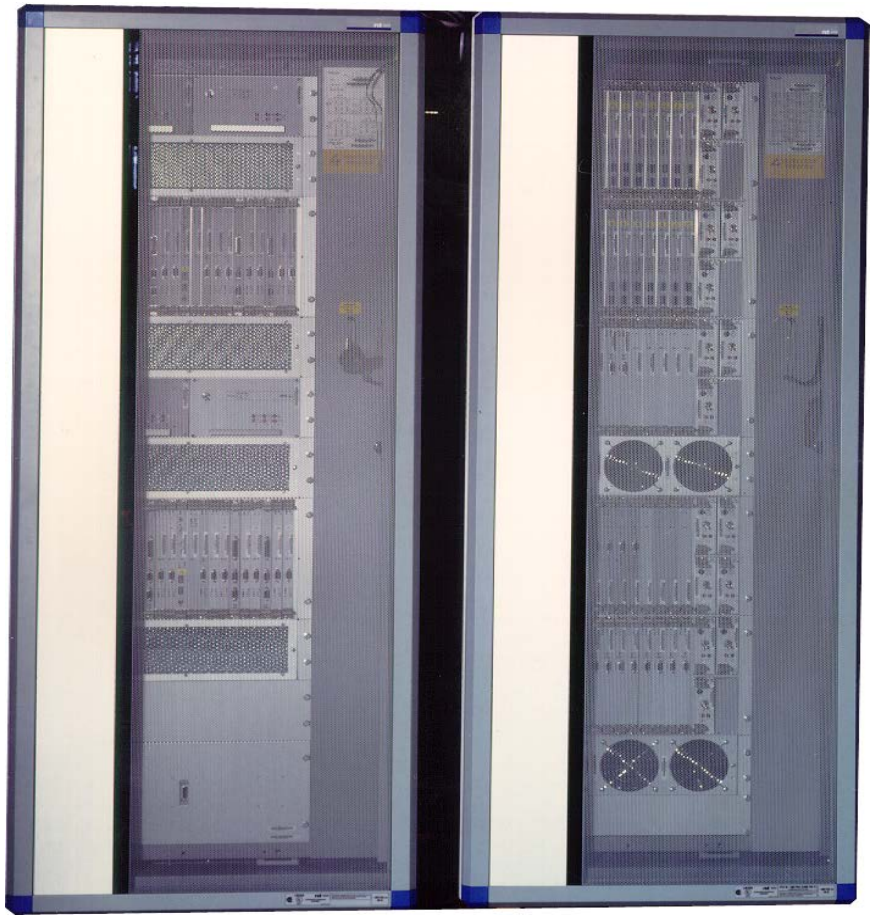
- Base Station Controller (BSC)
  - is responsible for the switching functions in the BSS, and
  - is in turn connected to an MSC in the NSS.
  - The BSC supports radio channel allocation/release and handoff management.
  - A BSC may connect to several BTSs and maintain cell configuration data of these BTSs.
  - The BSC communicates with the BTSs using ISDN protocols via the A-bis.
  - Capacity planning for BSC is very important.

GSM BTS (by courtesy of Nortel ©)





GSM BSC (by courtesy of Nortel ©)



Network and Switching Subsystem (NSS) (1/2)

- MSC performs the basic switching function following a signaling protocol used in the telephone network.
- HLR and VLR maintain the current location of the MS.
- Authentication Center (AuC) is used in the security data management for the user.

Network and Switching Subsystem (NSS) (2/2)

- Gateway MSC (GMSC) routes an incoming call to an MSC by interrogating the HLR directory.
  - A MSC can function as the GMSC by including appropriate software and HLR interrogation functions.

Radio Interface — Um Interface

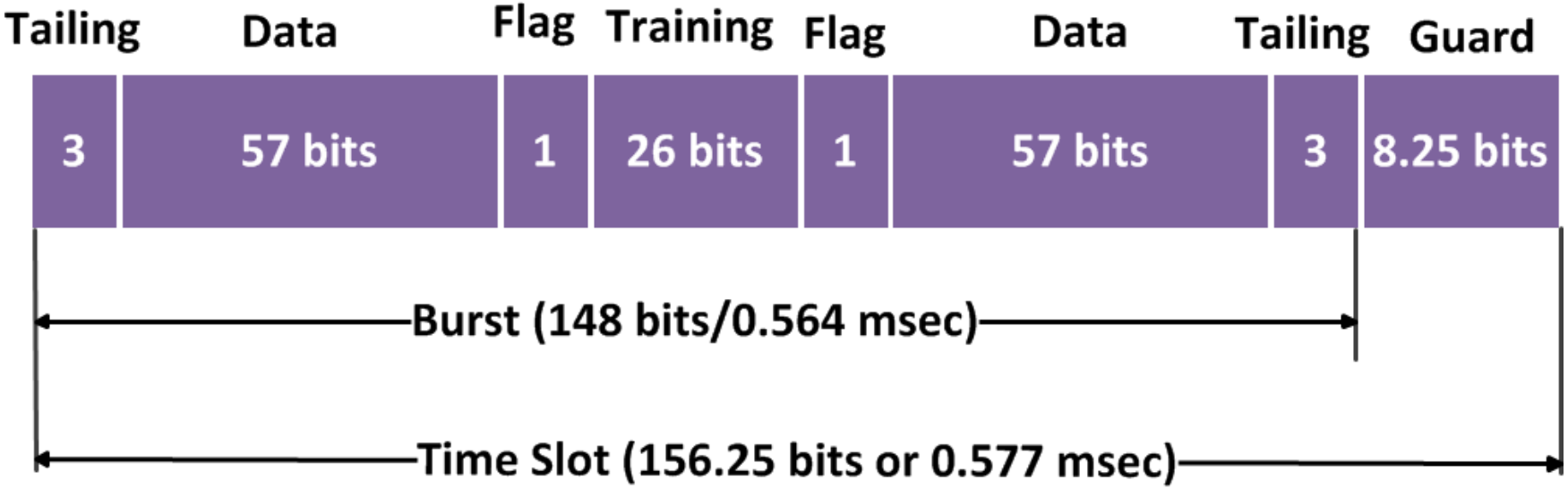
- The GSM radio link uses both FDMA and TDMA technologies.
- 935-960 MHz (downlink); 890-915 MHz (uplink)
- 124 pairs × 200 KHz
- Discontinuous transmission/reception is used to save the power consumption of the MS.

The Frame Structure

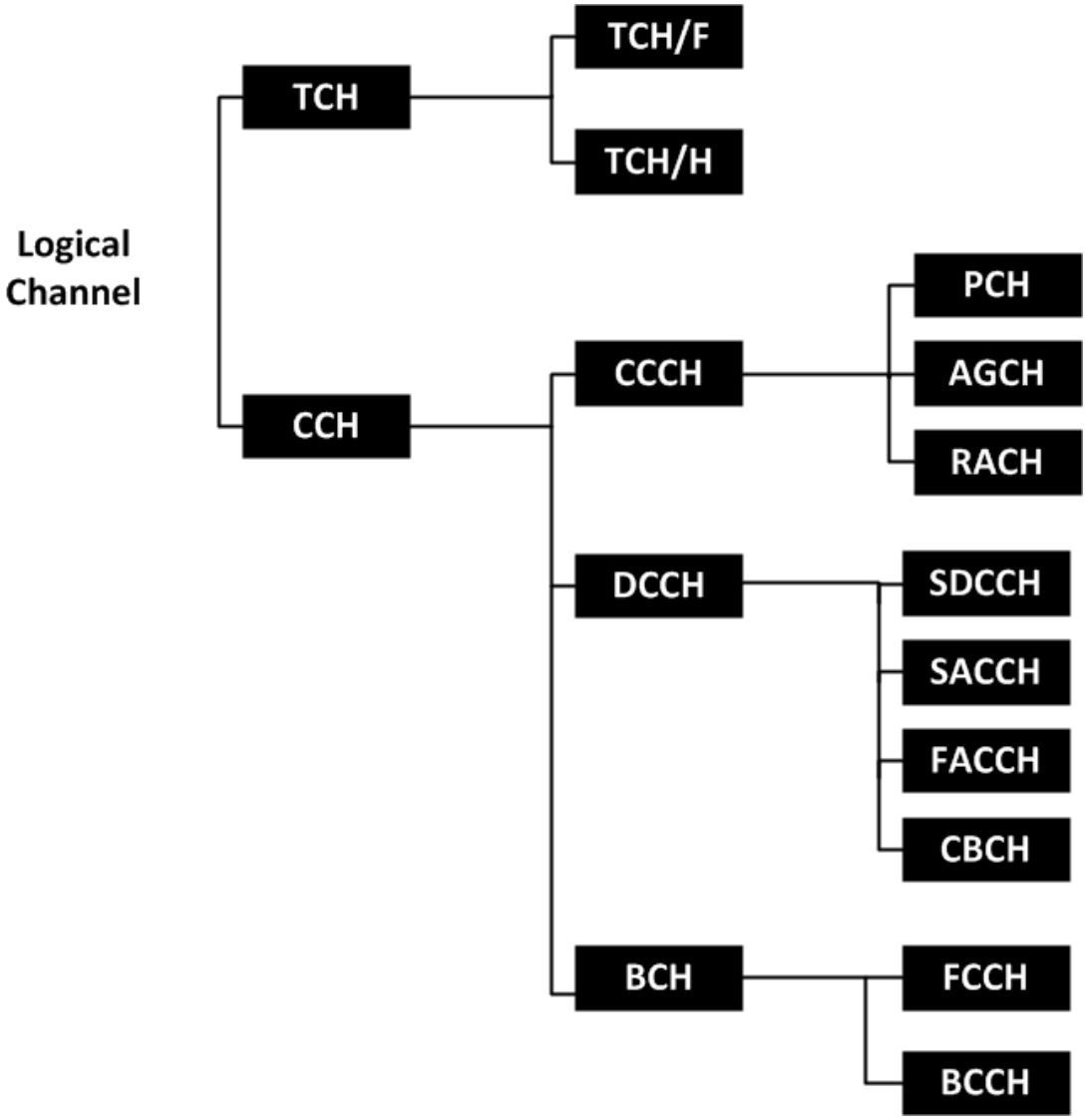
- The length of GSM frame in a frequency carrier is 4.615 msec.
- A frame consists 8 bursts (time slot) (each 0.577 msec).
- The delay between uplink and downlink is 3 time slots.
- Timing Advance: the exact shift between downlink and uplink seen by MS

GSM Burst Structure

- Begin with 3 head bits, and end with 3 bits.
- Two groups are separated by an equalizer training sequence of 26 bits.
- The flags indicates whether the information carried is for speech/data, signaling.



Logical Channels



Traffic Channel (TCH)

- TCHs are intended to carry user information (speech or data).
  - Full-rate TCH (TCH/F) provides transmission speed of 13 Kbps for speech or 9.6, 4.8 or 2.4 Kbps for data. Enhanced full-rate (EFR) speech coders have been implemented to improve the speech quality.
  - Half-rate TCH (TCH/H) allows transmission of 6.5 Kbps speech, or 4.8 or 2.4 Kbps of data.

Common Control Channel (CCCH) (1/2)

- Paging Channel (PCH) (down link) used by the network to page the destination MS in call termination.
- Access Grant Channel (AGCH) (down link) used by the network to indicate radio link allocation upon prime access of an MS.

Common Control Channel (CCCH) (2/2)

- Random Access Channel (RACH) (up link) used by the MSs for initial access to the network.
- Several MSs may access the same RACH, potentially resulting in collisions. The slotted Aloha protocol is adopted in GSM to resolve access collision.

Dedicated Control Channel (DCCH) (1/3)

- (DCCH) is for dedicated use by a specific MS.
- Standalone Dedicated Control Channel (SDCCH; Downlink/Uplink) used only for signaling and for short message.

Dedicated Control Channel (DCCH) (2/3)

- Slow Associated Control Channel (SACCH; Downlink/Uplink)
  - associated with either a TCH or and SDCCH.
  - This SACCH is used for non-urgent procedures,
  - mainly the transmission of power and time alignment control information over the downlink,
  - and measurement reports from the MS over the uplink.

Dedicated Control Channel (DCCH) (3/3)

- Fast Associated Control Channel (FACCH; Downlink/Uplink)
  - Used for time-critical signaling, such as cell-establishing progress, authentication of subscriber, or handoff.
  - The FACCH makes use of the TCH during a call; thus, there is a loss of user data because the FACCH “steals” the bandwidth of the TCH.
- Cell Broadcast Channel (CBCH; downlink)
  - Carries only the short message service cell broadcast messages, which use the same time slot as the SDCCH.

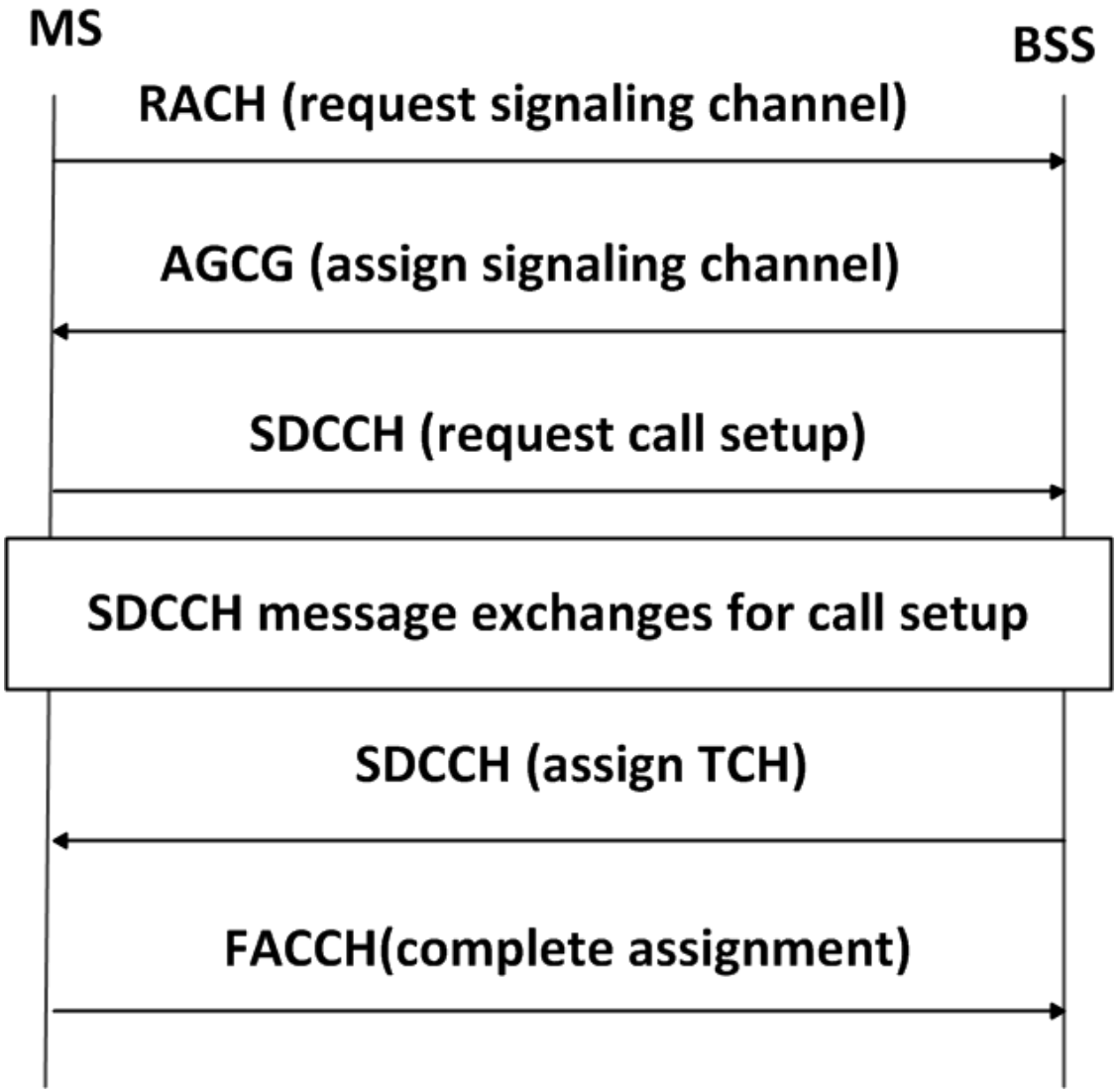
Broadcast Channels (BCHs) (1/2)

- BCHs are used by BTS to broadcast information to the MSs in its coverage area.
- Frequency Correction Channel (FCCH) and Synchronization Channel (SCH)
  - carry information from the BBS to the MS.
  - The information allows the MS to acquire and stay synchronized with the BSS.

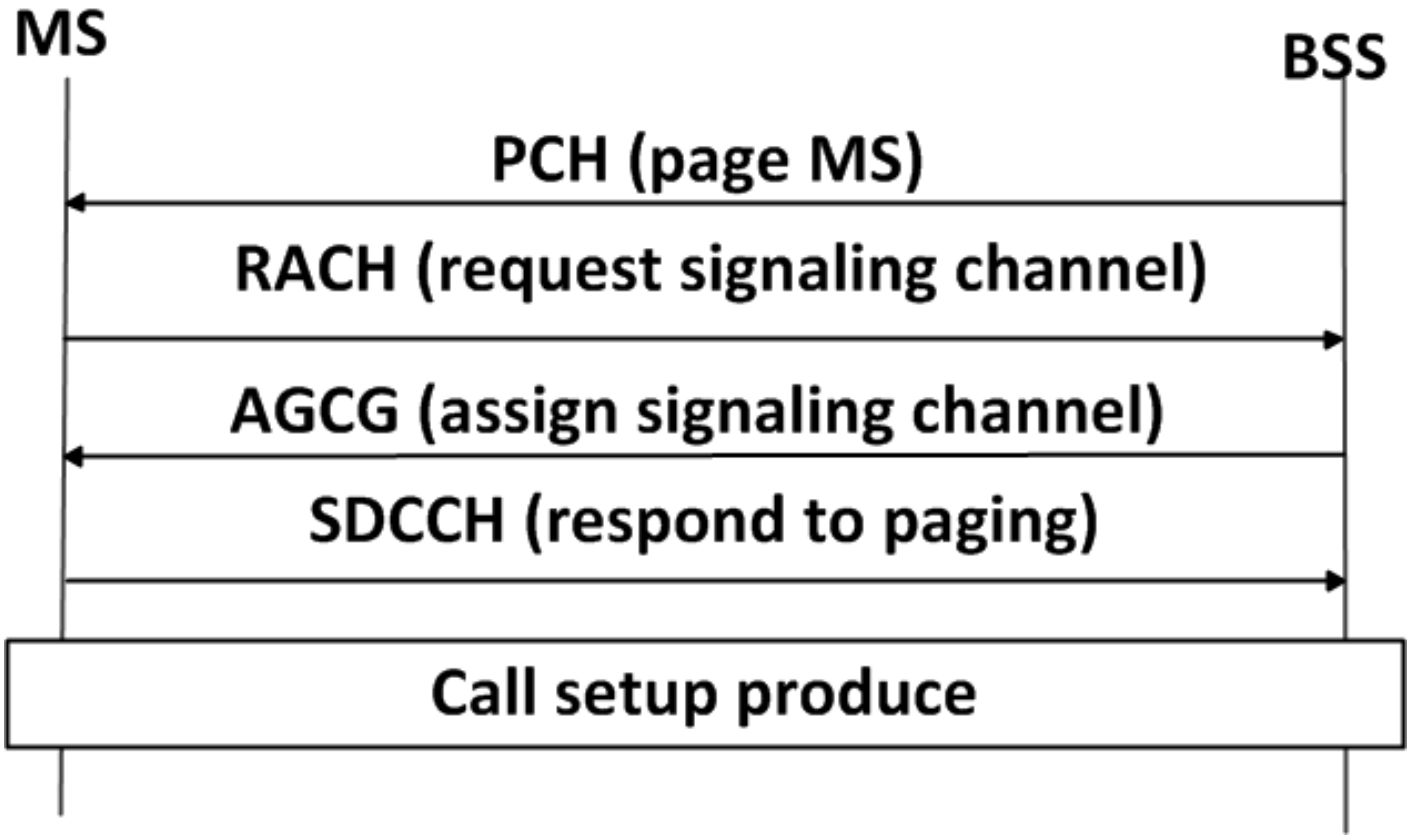
Broadcast Channels (BCHs) (2/2)

- Broadcast 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)



GSM Call Termination (Radio Aspect)



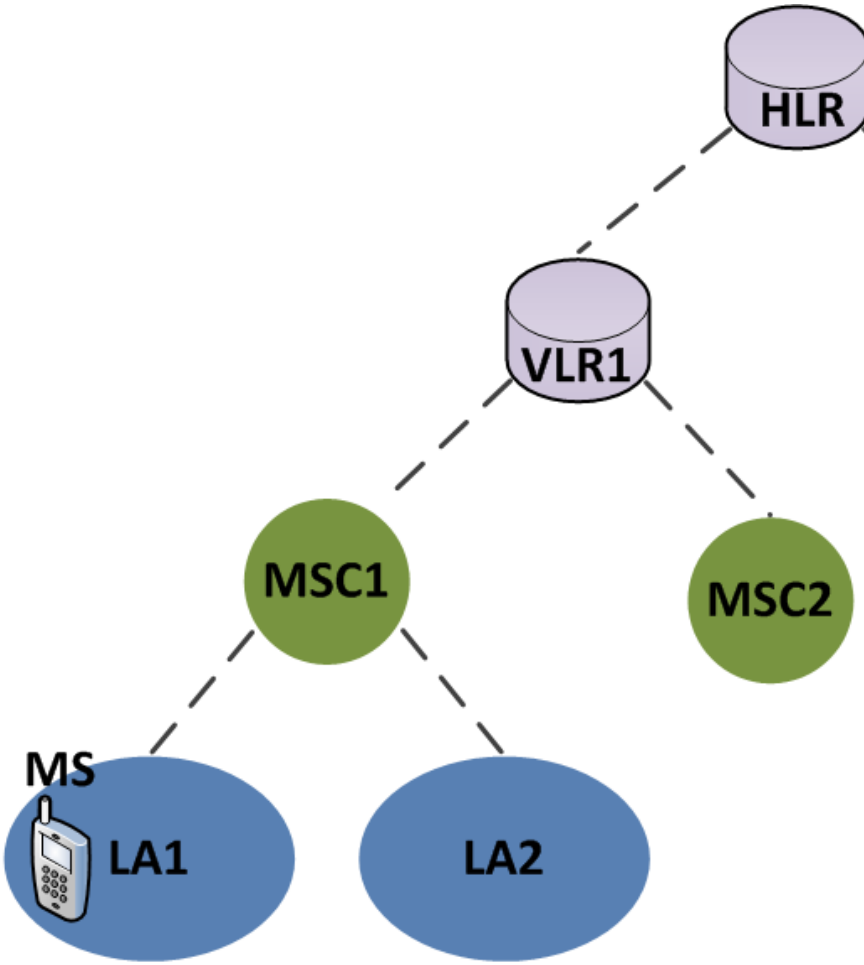
PART II

GSM Mobility Management

GSM MM

- 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.

GSM Location Area Hierarchy



HLR: Home Location Register
VLR: Visitor Location Register
MSC: Mobile Switching Center
LA: Location Area
MS: Mobile Station

Identification Numbers in GSM

- Mobile system ISDN (MSISDN)
- Mobile Station Roaming Number (MSRN)
- International Mobile Subscriber Identity (IMSI)
- Temporary Mobile Subscriber Identity (TMSI)
- International Mobile station Equipment Identity (IMEI)

MSISDN

- Mobile System ISDN
  - MSISDN uses the same format as the ISDN address (based on ITU-T Recommendation E.164).
  - HLR uses MSISDN to provide routing instructions to other components in order to reach the subscriber.

Total up to 15 digits

Country code (CC)	National destination code (NDC)	Subscriber number (SN)

MSRN

- Mobile Station Roaming Number
- The routing address to route the call to the MS through the visited MSC.
  - MSRN=CC+NDC+SN

IMSI

- International Mobile Subscriber Identity
  - Each mobile unit is identified uniquely with an IMSI.
  - IMSI includes the country, mobile network, mobile subscriber.
  - Total up to 15 digits

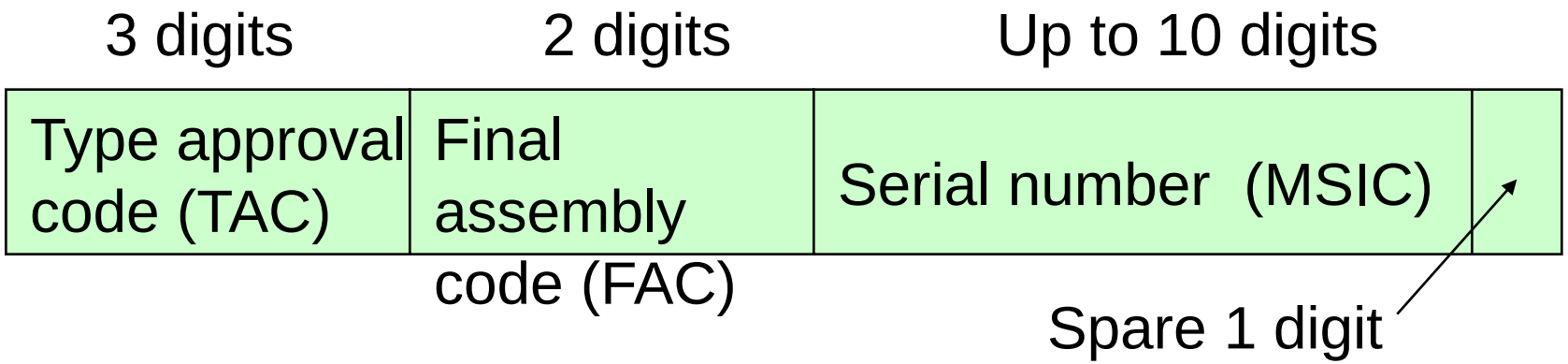
3 digits	1- 2 digits	Up to 10 digits
Mobile country code (MCC)	Mobile network code (MNC)	Mobile subscriber identification code (MSIC)

TMSI

- Temporary Mobile Subscriber Identify
  - TMSI is an alias used in place of the IMSI.
  - This value is sent over the air interface in place of the IMSI for purposes of security.

IMEI

- International Mobile Station Equipment Identity
  - IMEI is assigned to the GSM at the factory.
  - When a GSM component passes conformance and interoperability tests, it is given a TAC.
  - Up to 15 digits



LAI

- Location Area Identity
  - LAI identifies a location area (LA).
  - When an MS roams into another cell, if it is in the same LAI, no information is exchanged.
  - Total up to 15 digits

3 digits	1-2 digits	Up to 10 digits
Mobile country code (MCC)	Mobile network code (MNC)	Location area code (LAC)

CGI

- Cell Global Identity
- CGI = LAI + CI

  = MCC + MNC + LAC + CI

  – CI : Cell Identity

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.

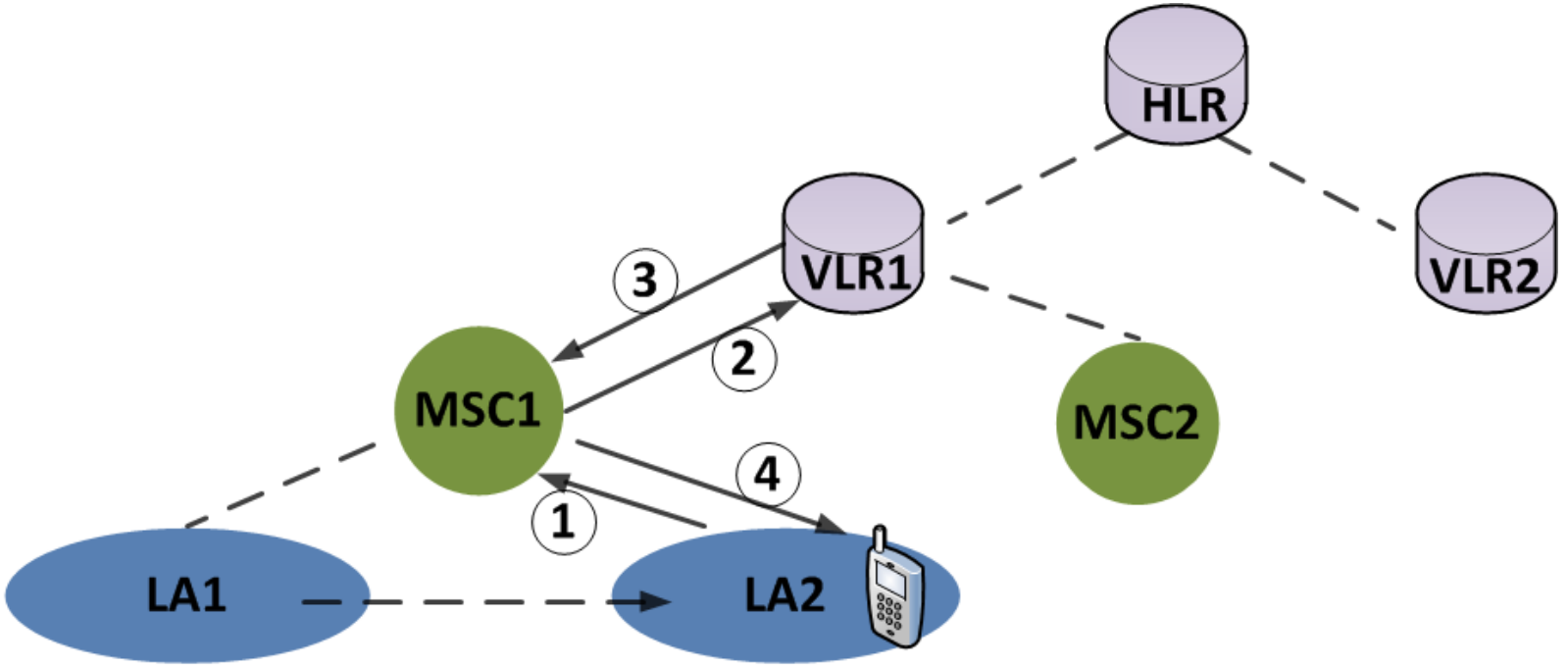
GSM Basic Location Update Procedure

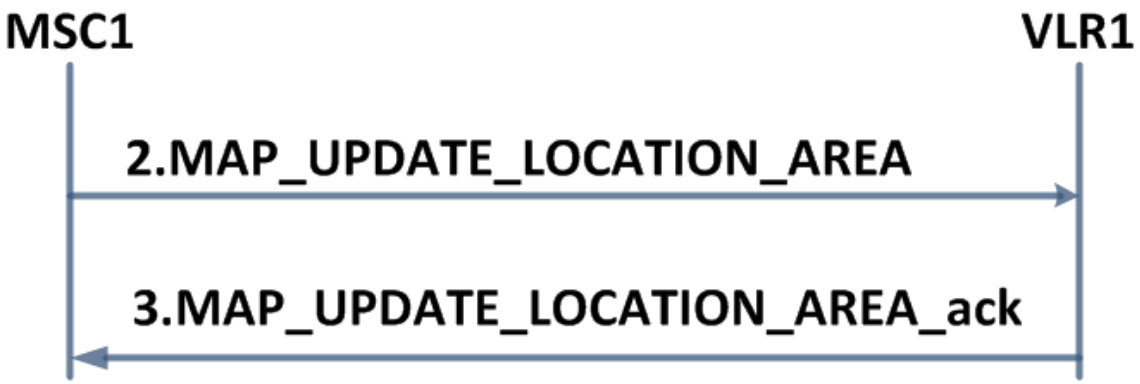
- Case 1. Inter-LA Movement
- Case 2. Inter-MSC Movement
- Case 3. Inter-VLR Movement

GSM Basic Location Update: Inter-LA Movement (1/4)

- 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.

Inter-LA Registration Message Flow





GSM Basic Location Update: Inter-LA Movement (2/4)

- 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.

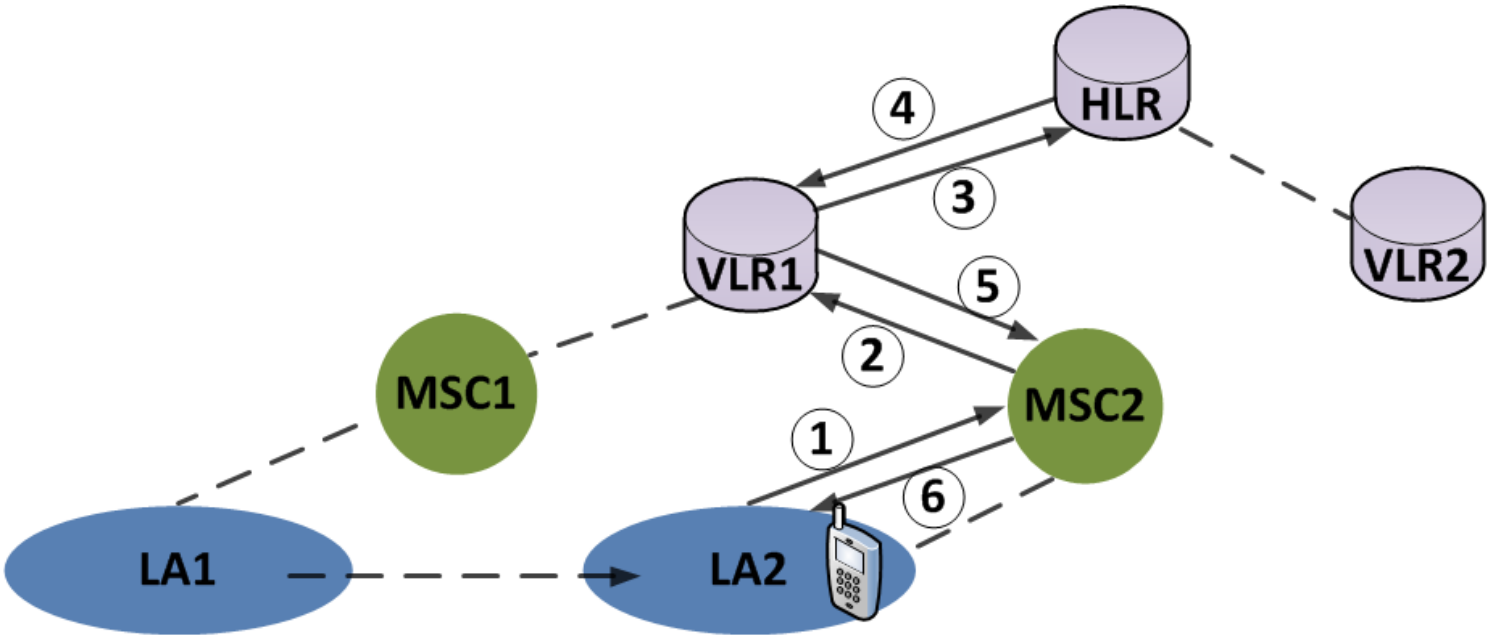
GSM Basic Location Update: Inter-LA Movement (3/4)

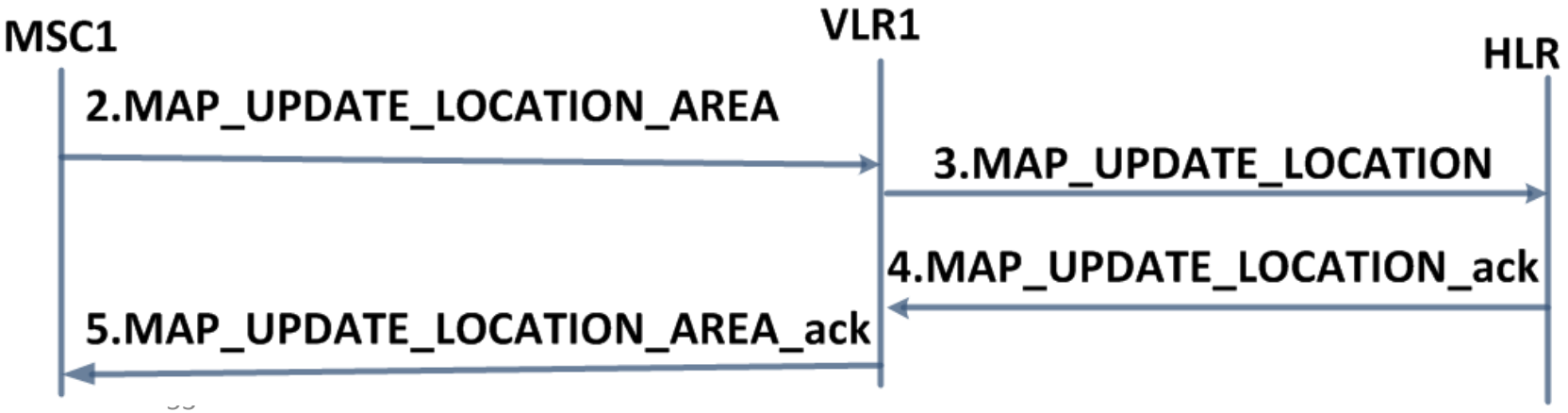
- Step 2. The MSC forwards the location update request to the VLR by a TCAP message, MAP_UPDATE_LOCATION_AREA.
  - This message includes (Address of the MSC, TMSI of MS, Prev. Location Area Identification (LAI), Target LAI, Other Related Information).

GSM Basic Location Update: Inter-LA Movement (4/4)

- 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.

Inter-MSC Registration Message Flow





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

- The two LAs belong to different MSCs of the same VLR.
- Steps 1 and 2. The location update request is sent from the MS to the VLR.
- Step 3.
  - Part I. The VLR notices that the Prev. LA and the Target LA belong to MSC1 and MSC2, which are connected to the same VLR, respectively.

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

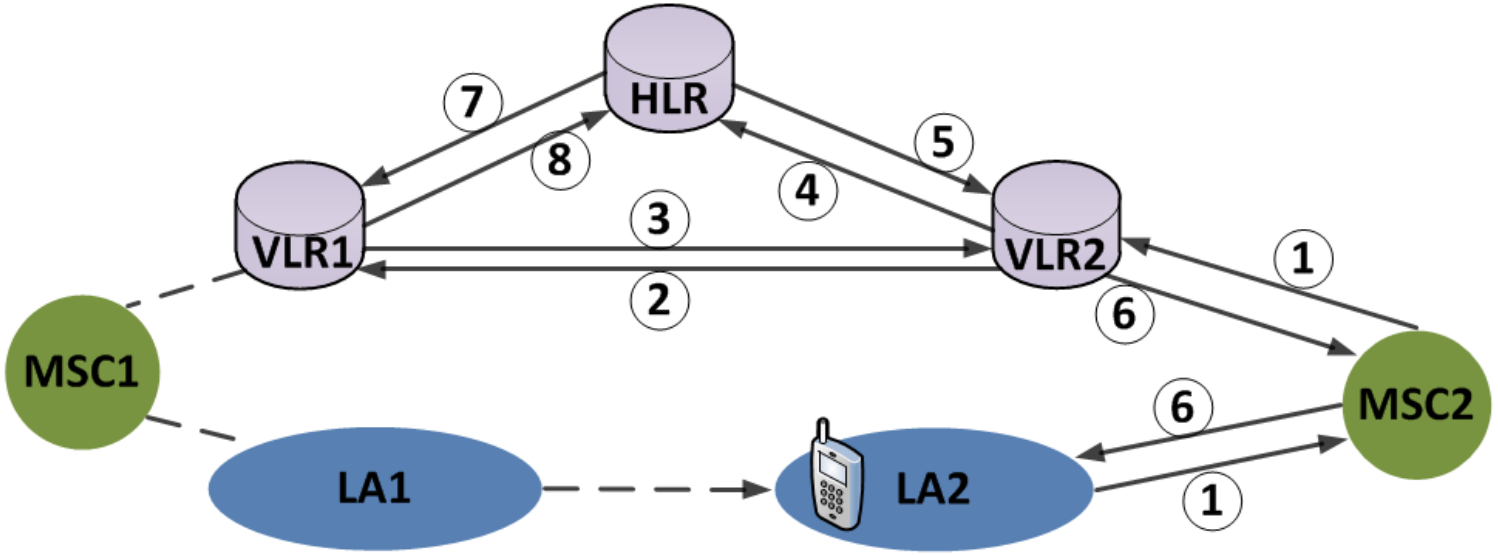
- Part II. The VLR updates the LAI and the MSC fields of the VLR record.
- Part IV. The VLR derives the HLR address of the MS from the MS's IMSI stored in the VLR record.
- Part V. The VLR sends the MAP_UPDATE_LOCATION to the HLR.

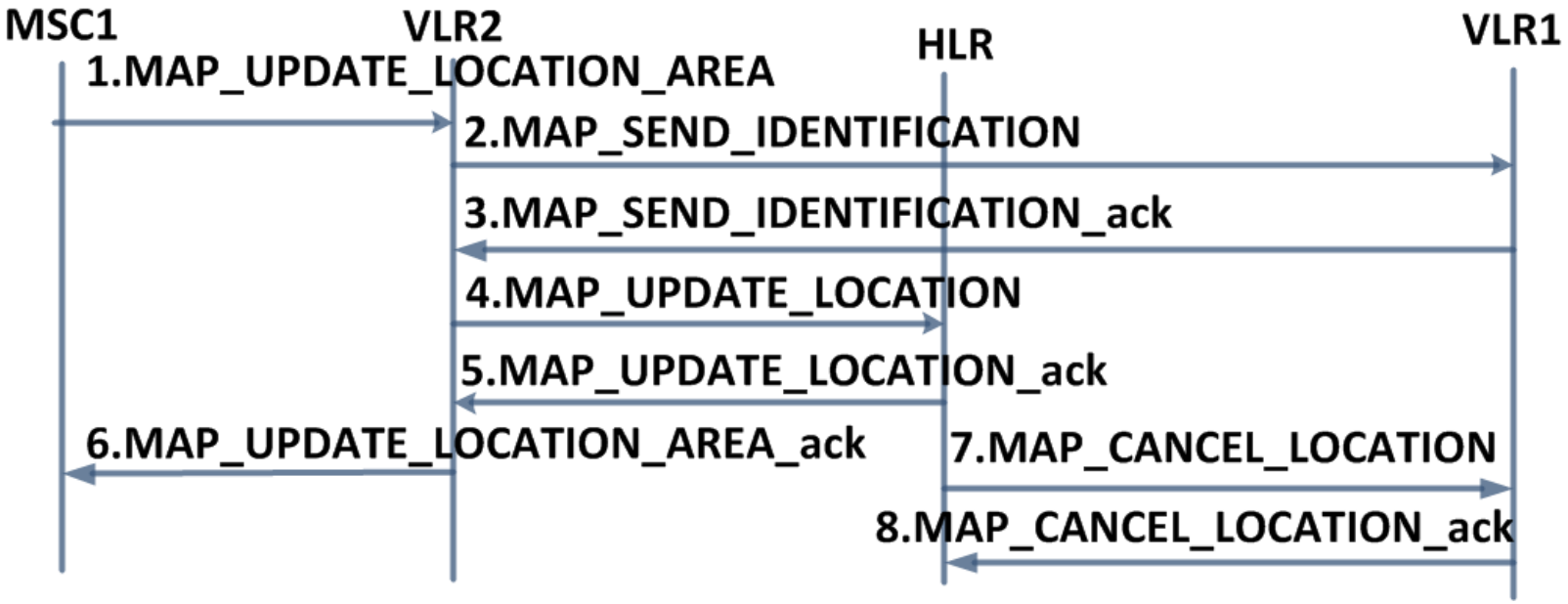
(IMSI of MS, Target MSC Address, Target VLR Address, other related information)

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

- Step 4.
  - Part I. By using the received IMSI, the HLR identifies the MS's record.
  - Part II. The MSC number field of the record is updated.
  - Part III. An acknowledgement is sent VLR.
- Steps 5 and 6. Similar to steps 3 and 4 in Inter-BTS movement, the acknowledgement is forwarded to the MS.

Inter-VLR Registration Message Flow





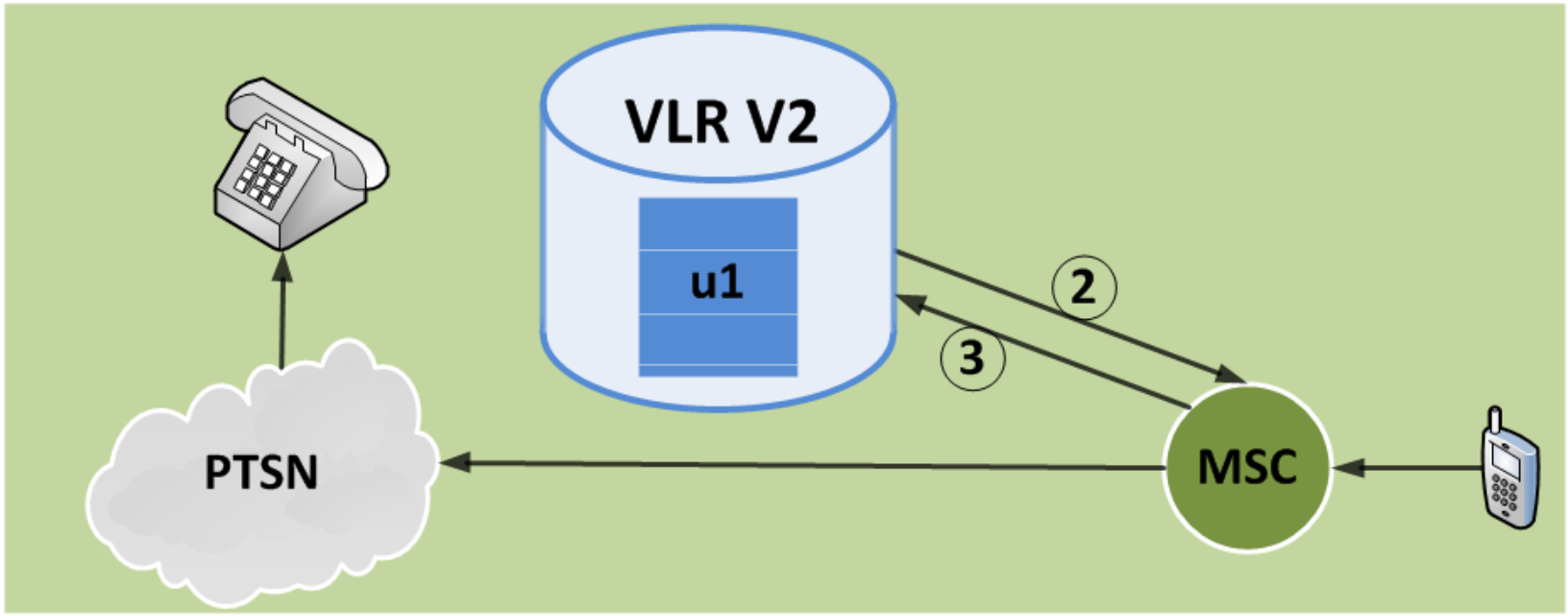
GSM Basic Location Update: Inter-VLR Movement (1/2)

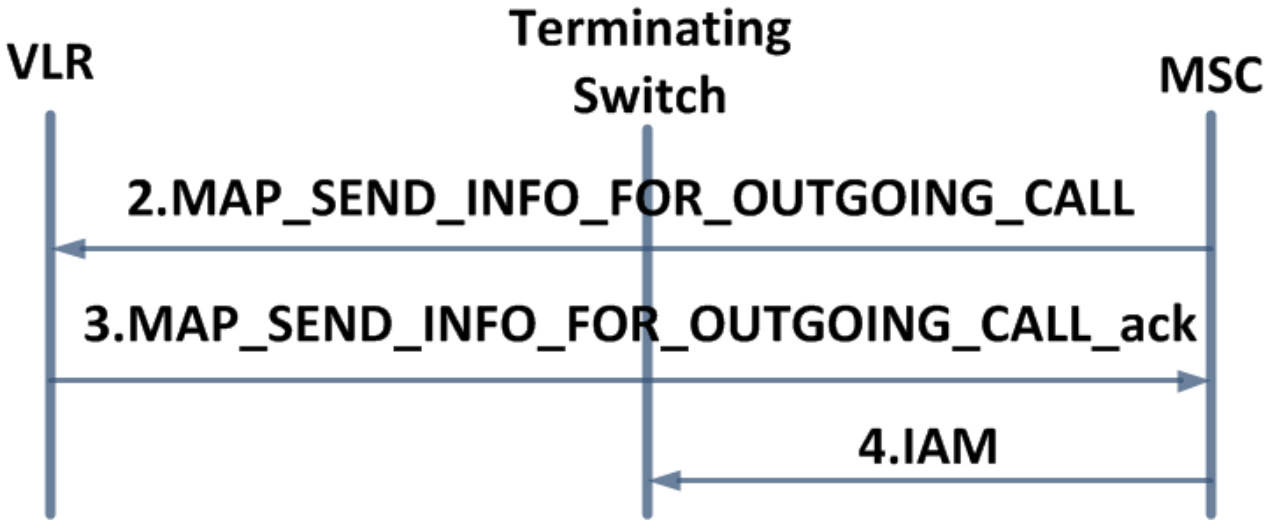
- Step 1. The location update request is sent from MS to the VLR.
- Steps 2 and 3.
  - Part I. Since the MS moves from VLR1 to VLR2, VLR2 does not have a VLR record of the MS, and the IMSI of the MS is not known.
  - Part II. From the MAP_UPDATE_LOCATION_AREA message, VLR2 identifies the address the VLR1.
  - Part III. VLR2 sends MAP_SEND_IDENTIFICATION to VLR1.
  - Note that to enhance security, confidential data (IMSI) typically is not sent over the air.

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

- Steps 4 and 5.
  - VLR2 creates a VLR record for the MS, and sends a registration message to update the HLR.
  - The HLR updates the record of the MS.
  - An acknowledge is sent back to VLR2.
- Step 6.
  - VLR2 generates a new TMSI and sends it to the MS. In GSM, the TMSI is changed from time to time to avoid fraudulent usage.
- Steps 7 and 8. The obsolete record of the MS in VLR1 is deleted.

Call Origination Operation

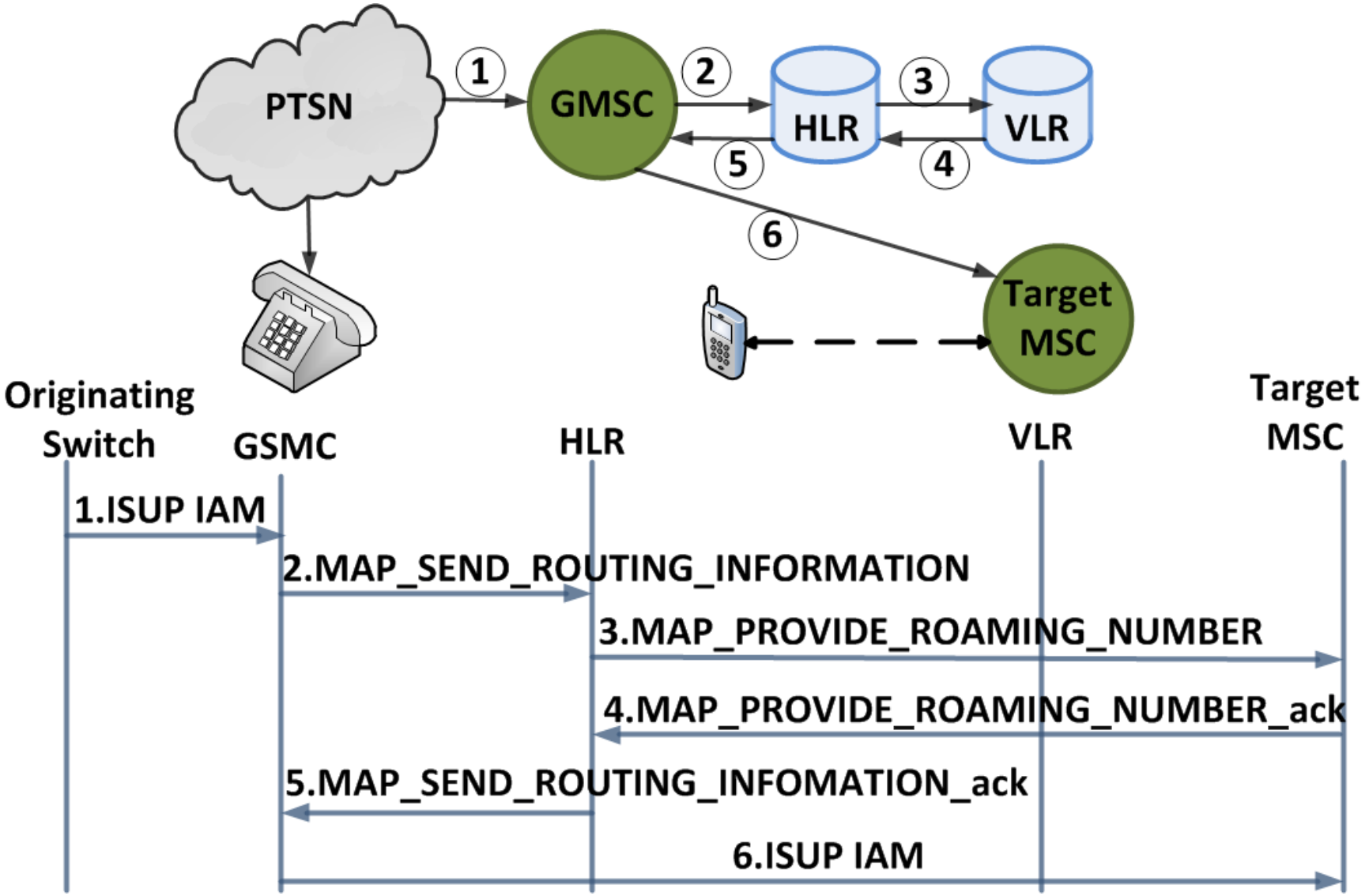




GSM Basic Call Origination

- Step 1. The MS u1 sends the call origination request to the MSC.
- Step 2. The MSC forwards the requets to the VLR by sending MAP_SEND_INFO_FOR_OUTGOING_CALL.
- Step 3. The VLR checks the u1's profile and sends MAP_SEND_INFO_FOR_OUTGOING_CALL_ack to the MSC to grant the call request.
- Step 4. The MSC sets up the trunk according to the standard PSTN call setup procedure.

Call Termination Message Flow (Simplified Version)



GSM Basic Call Termination (1/3)

- Step 1. When the MSISDN number is dialed by a PSTN user, the call is routed to a gateway MSC by an SS7 ISUP IAM message.
- Step 2. To obtain the routing information, the GMSC or ISDN exchange interrogates the HLR by sending MAP_SEND_ROUTING_INFORMATION to the HLR.
  - The message contains the MSISDN of the MS and other related info.

GSM Basic Call Termination (2/3)

- Step 3. The HLR sends a MAP_PROVIDE_ROAMING_NUMBER message to the VLR to obtain the Mobile Subscriber Roaming Number (MSRN).
  - The message consists of IMSI of the MS, the MSC number.

GSM Basic Call Termination (3/3)

- Steps 4 and 5. The VLR creates the MSRN by using the MSC number stored in the VLR record of the MS. This roaming number is sent back to the gateway MSC through the HLR.
- Step 6. The MSRN provides the address of the target MSC where the MS resides. An SS7 ISUP IAM message is directed from the gateway MSC to the target MSC to setup the voice trunk.

PART III

Security

Security: Authentication (1/3)

- Ki is used to achieve authentication.
  - Ki is stored in the AuC and SIM.
  - Ki is not known to the subscriber.
- RAND
  - A 128-bit random number generated by the home system.
- A3
  - A security function.
  - The inputs are RAND and Ki, and the output is SRES.

Security: Authentication (2/3)

- Step 1. The home system of the MS generates a RAND.
- Step 2. The home system sent the RAND to the MS.
- Step 3. Both the network (AuC) and the MS (SIM) use Ki and RAND to generate SRES by executing A3.

Security: Authentication (3/3)

- Step 4. The MS sends the SRES to the home system.
- Step 5. The SRES generated by the MS is compared with the SRES generated by the home system at AuC.
- Note that if (SRES, RAND) generated by the AuC are sent from the HLR to the visited VLR in advance, the comparison can be done at the visited VLR.

Security: Encryption (1/3)

- Kc is generated by algorithm A8 for the Encryption.
- A8
  - An algorithm stored in the home system of the MS (AuC) and the MS (SIM).
  - The inputs are Ki and RAND.
  - The output is Kc.

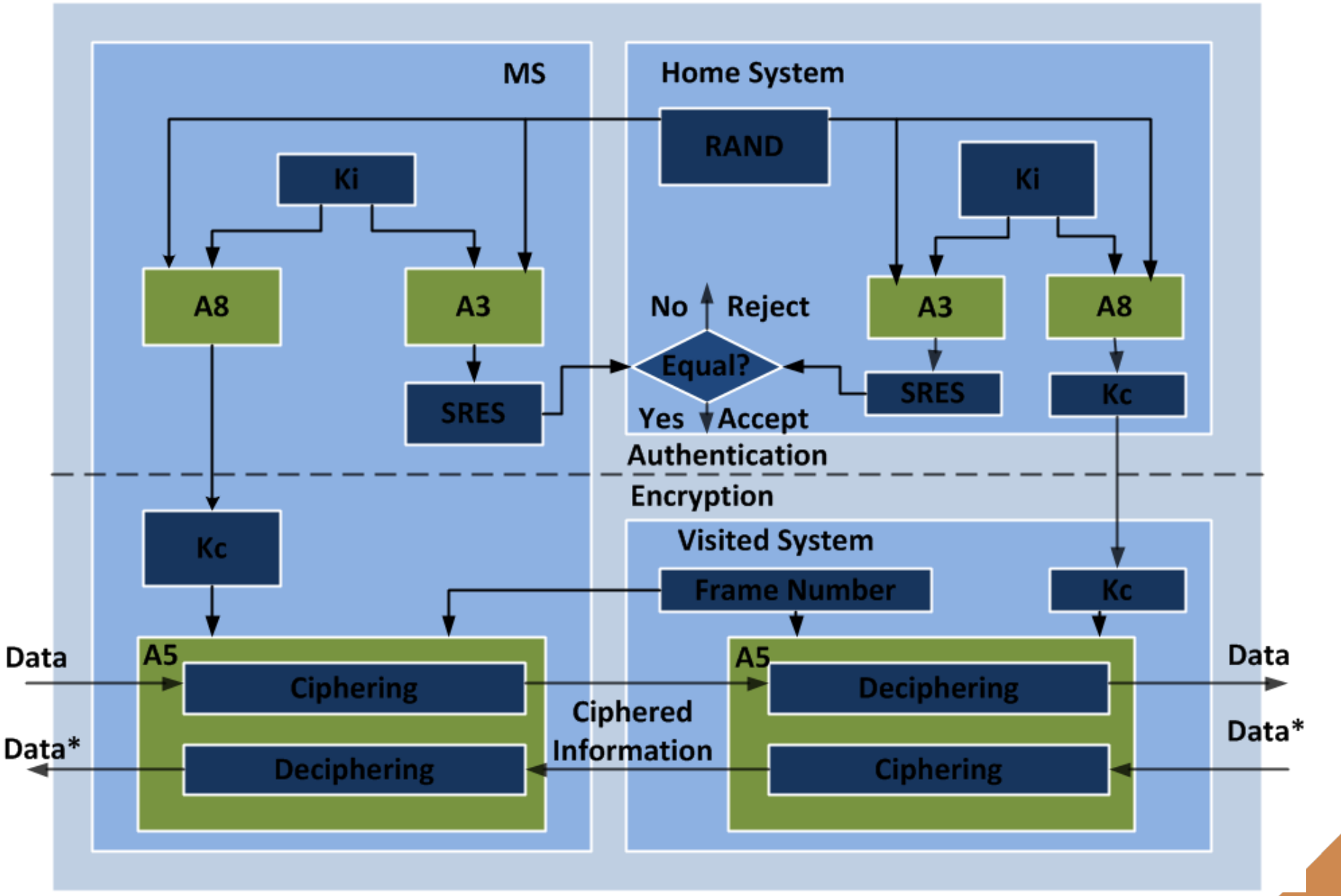
Security: Encryption (2/3)

- Frame Number
  - A TDMA frame number encoded in the data bits.
- A5
  - An algorithm stored in the MS (handset hardware) and the visited system.
  - Is used for the data ciphering and deciphering.

Security: Encryption (3/3)

- Step 1. If the MS is accepted for access, an Kc is produced by an algorithm A8 with Ki and RAND as inputs.
- Step 2. After the home system has generated Kc, this Kc is sent to the visited system.
- Step 3. Kc and the TDMA frame number encode in the data bits are used by A5 to cipher and decipher the data steam between the MS and the visited system.

Authentication and Encryption



PART IV

DATA SERVICES

Data Services(1/2)

- GSM phase 2 standard supports two data services.
  - Short Message Services (SMS)
  - Bearer Services are similar to the ISDN services, and the maximum data rate is 9.6 Kbps.

Data Services(2/2)

- GSM phase 2+ standard supports two data services.
  - High-Speed Circuit-Switched Data (HSCSD) for high-speed file transfers and mobile video applications
  - General Packet Radio Service (GPRS) for bursty data applications such as e-mail and WWW.
  - The data rates are expected to be raised from 9.6 Kbps to 28.8 Kbps or higher.

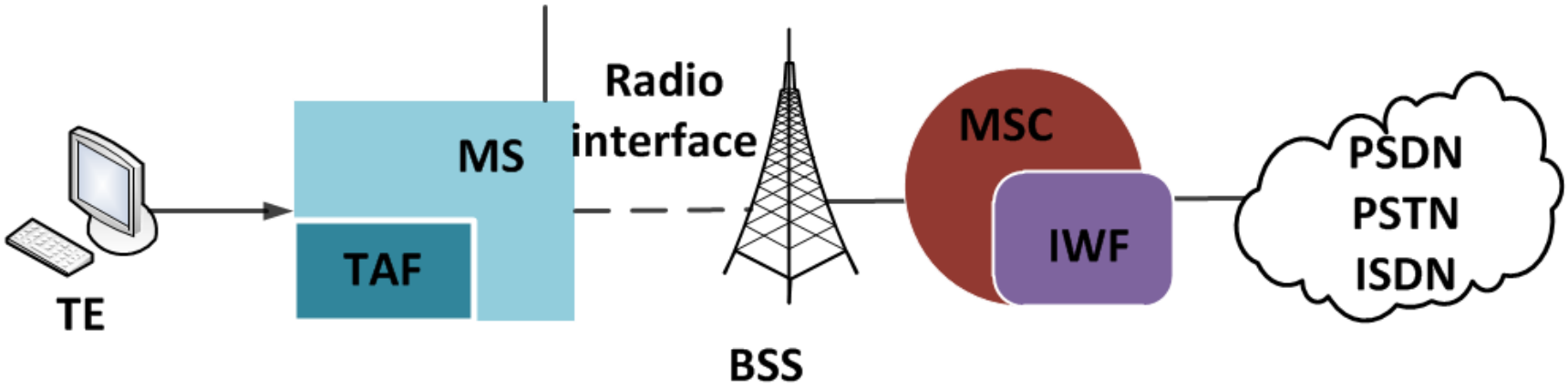
High-Speed Circuit-Switched Data (HSCSD)(1/2)

- HSCSD is a circuit-switched protocol for large file transfer and multimedia applications.
- The physical layer of HSCSD is the same as that for the Phase 2 GSM data services.
- The data rate of HSCSD has been increased by using multiple TDMA time slots (up to 8).

High-Speed Circuit-Switched Data (HSCSD)(2/2)

- The radio interface is the same as that of the current GSM system except that multiple, independent time slots can be utilized to provide high-speed link.
- The radio link protocol (RLP) has been enhanced in HSCSD to support multi time-slot operation.
- In June 1999, Nokia announced Card Phone 2.0 for HSCSD with 43.2 Kbps.

HSCSD Architecture

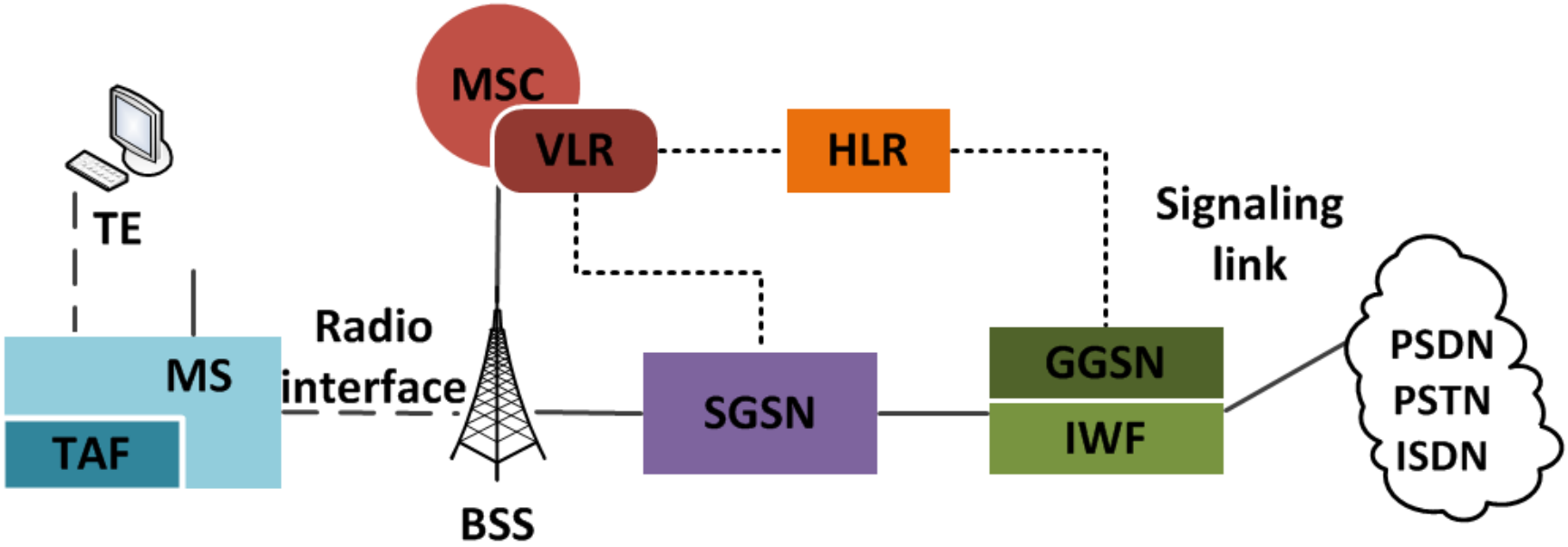


MSC : Mobile Switching Center
MS : Mobile Station (Handset)
BSS : Base Station Subsystem
TAF : Terminal Adaption Functions
TE : Terminal Equipment
IWF : Interworking Functions
PSTN : Public Switched Telephone Network
PSDN : Public Switched Data Network

General Packet Radio Service (GPRS) (1/2)

- GPRS is a packet-switched protocol for applications (e.g., Web).
- GPRS has its own transport network for the transmission of bursty data.
- Two new entities:
  - Serving GPRS Support Node (SGSN) receives and transmits packets between the MS their counterparts in the Public-Switched Data Network (PSDN).
  - Gateway GPRS Support Node (GGSN) inter-works with PSDN using connectionless networks (e.g., IP or X.25).
  - The HLR is enhanced to accommodate GPRS.

GPRS Architecture



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

General Packet Radio Service (GPRS) (2/2)

- A new radio link protocol is introduced to the GPRS air interface
  - to guarantee fast call setup procedure and low-bit error rate for data transfer between the MSs and the BSs.
  - A packet radio media access control (MAC) for packet switching.
  - GPRS supports up to 100 users with one to eight channels.
- A new infrastructure is introduced to GPRS for the packet services.

PART V

Unstructured Supplementary Service Data

USSD

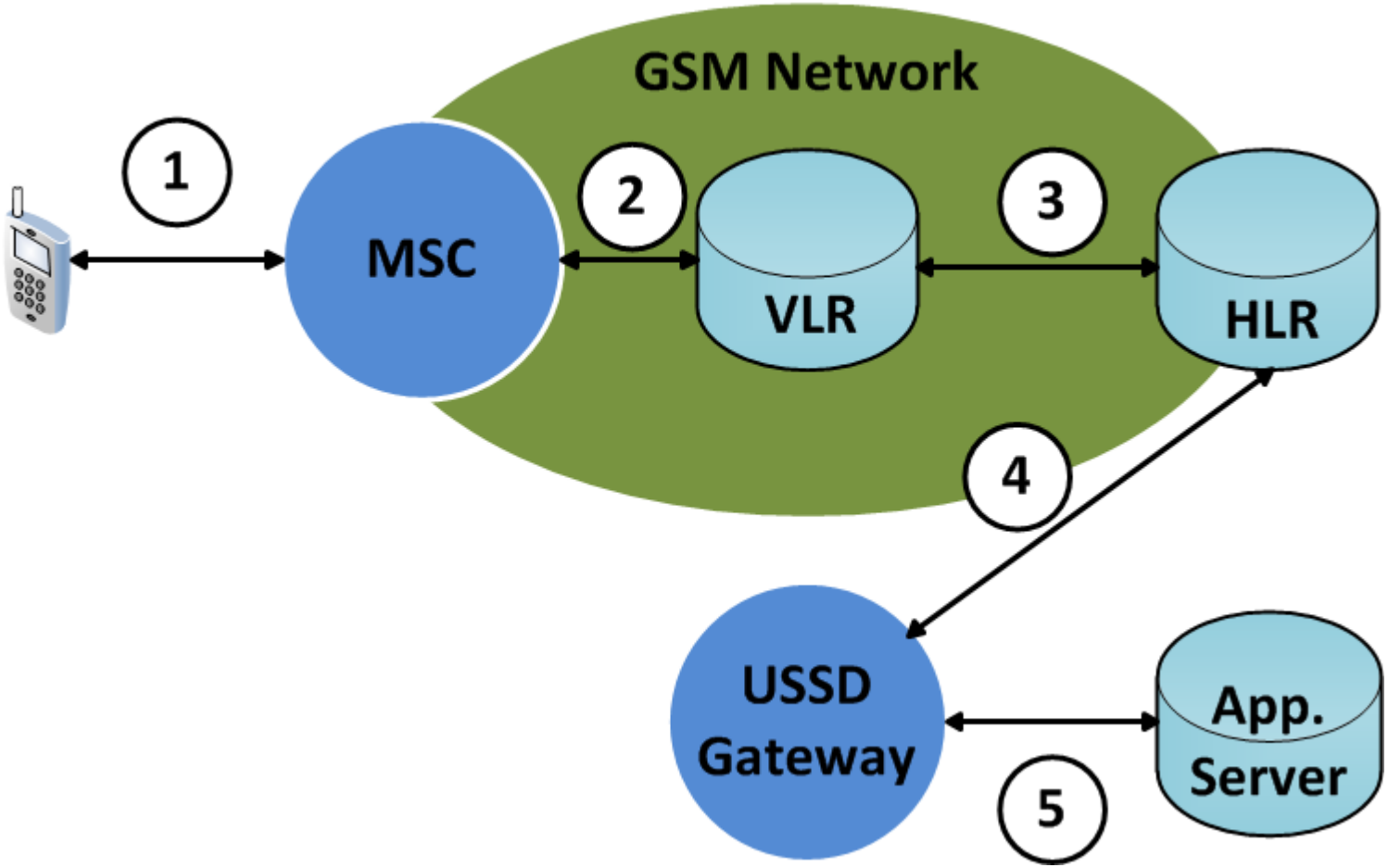
- During the evolution of GSM, supplementary services have bee introduced in various stages. These new services may not be supported in old MSs.
- To support the new services in old MSs, USSD was introduced in GSM 02.90, 03.90, and 04.90 Spec.
- USSD is used as a GSM transparent bearer for old MSs.

The Usage of USSD

- USSD is flexible in terms of message length and content.
- It uses all digits 0-9 plus “*” and “#” keys.
- A USSD string is a command code
  - Typically 2 or 3 digits followed by several parameters.
  - The parameters (supplementary information) have variable lengths and are separated by “*”.
  - The whole string ends with “#”.

*159*5288128#

USSD Architecture



USSD Functionalities

- The USSD provides interaction between a GSM node (MSC, VLR, or HLR) and the MS.
- If the USSD service node is an MSC, the USSD messages are exchanged through path (1).
- If the service node is a VLR (or HLR), the messages are exchanged through path (1)<->(2) (or (1)<->(2)<->(3)).

An Example for USSD Services(1/2)

- Suppose that a new USSD service that enables subscribers to obtain real-time stock quotes is implemented at the home work.
- USSD messages would be exchanged between the MS and the HLR.

An Example for USSD Services(2/2)

- Advantages. Since the MS communicates directly with the HLR, the subscriber can monitor stock values even when roaming to another country.
- HLR is expensive to modified.
  - The solution is to introduce an USSD gateway between HLR and Application servers.
  - GSM MAP (used between HLR and USSD Gateway), TCP/IP (used between USSD Gateway and Application Servers).

Summary

- GSM Architecture
  - MS, BSS, NSS
  - Radio Interface
- Location Tracking
  - Registration
  - Mobile Call Termination
- Security
  - Authentication
  - Encryption
- Data Services
  - HSCSD
  - GPRS
- USSD Services