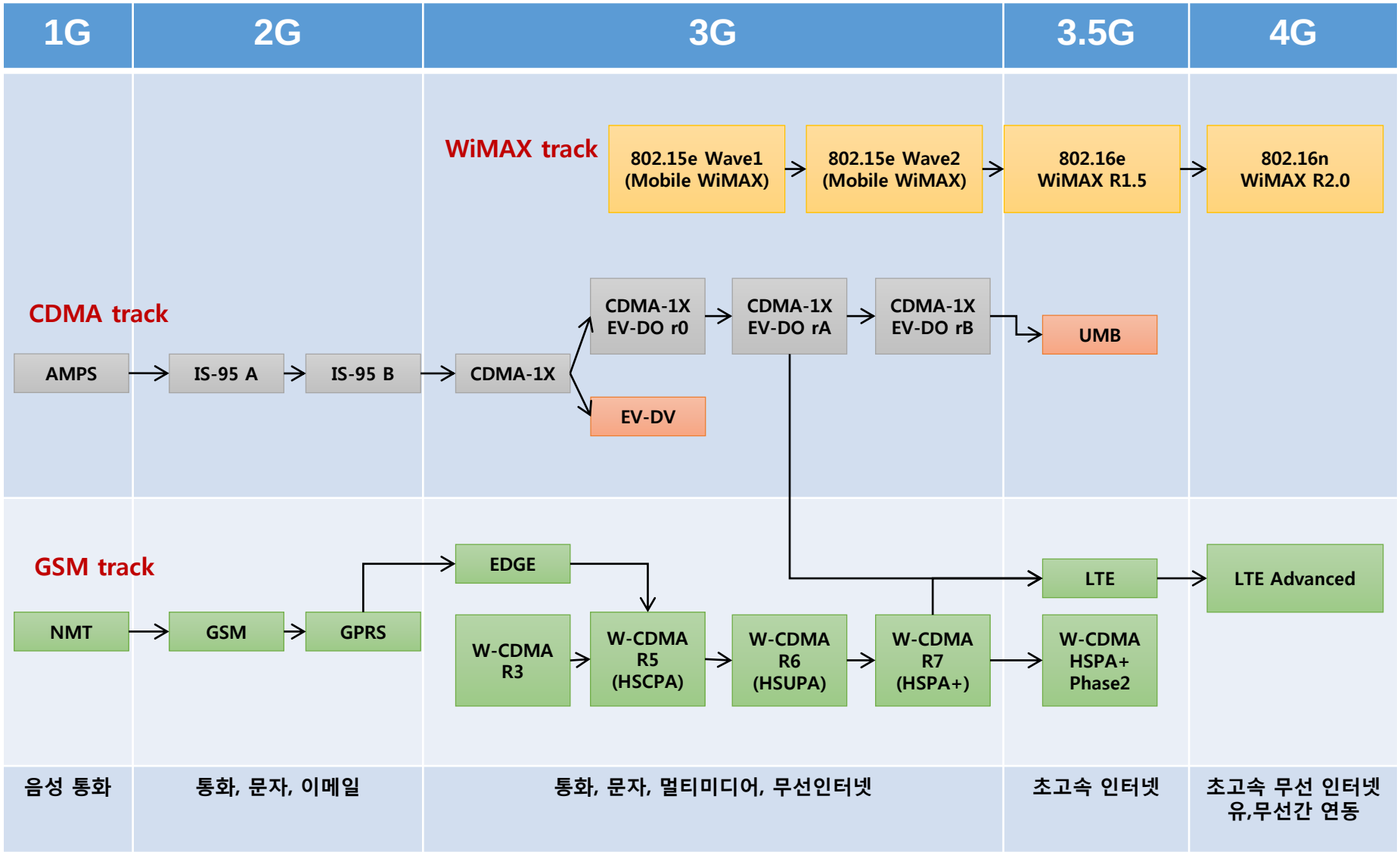
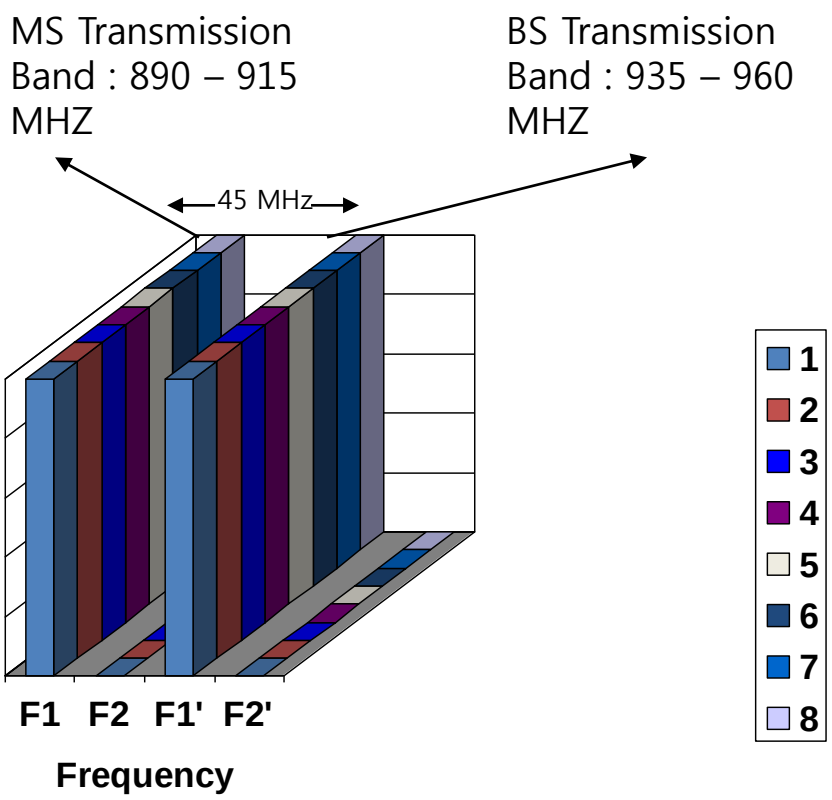
Telecommunication Basics
(GSM Network)

Software Engineering Lab - 김영기 책임

Remember Again !!!

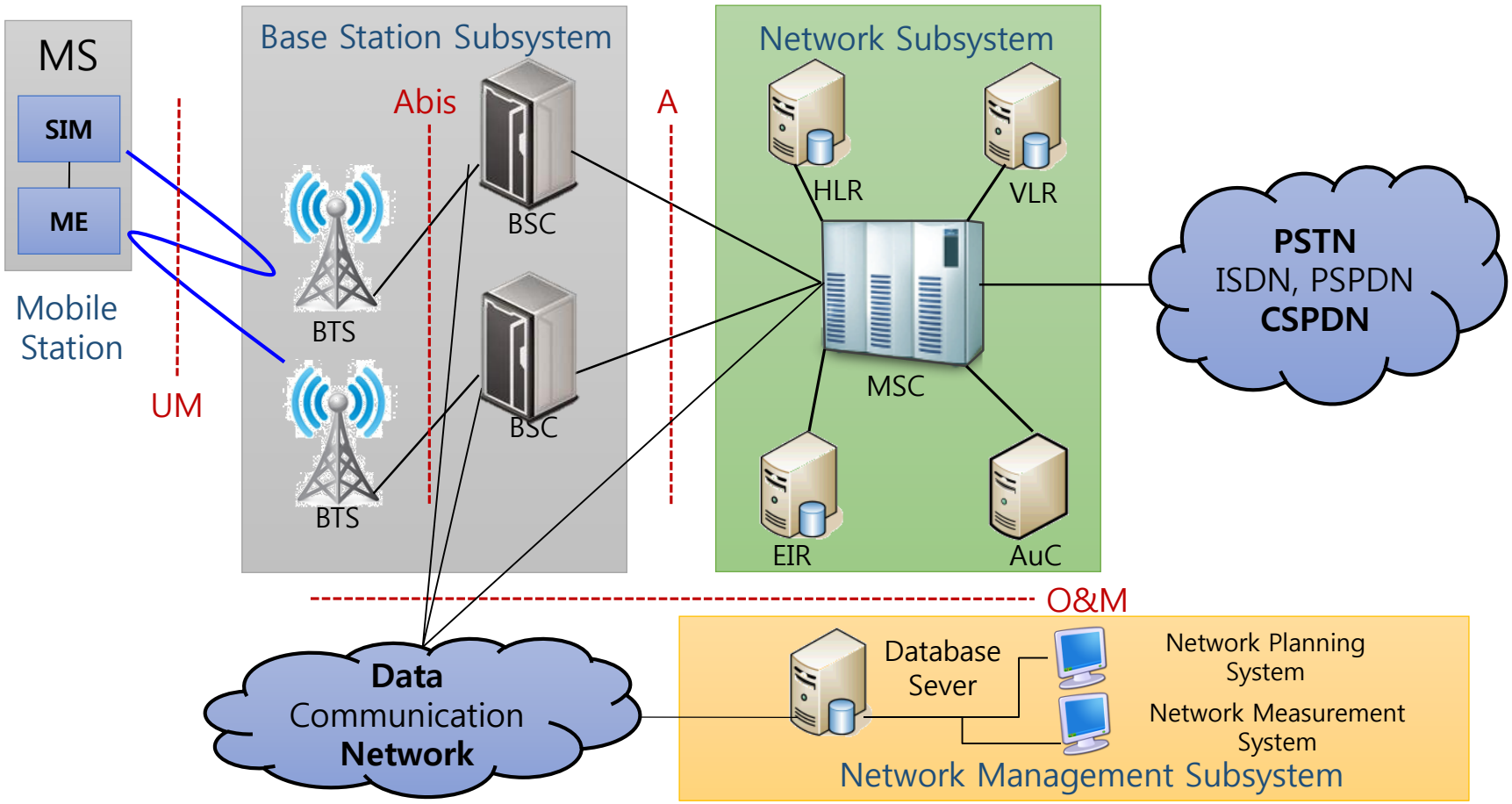


GSM Characteristics



Year Introduced	**1990**
Access method	**TDMA**
Channel Bandwidth	**200 kHz**
Number of duplex channels	**125**
Users per channel	**8**
Speech coding bit rate	**13 kbps**
Data coding bit rate	**12 kbps**
Frame size	**4.6 ms**

GSM Nework Architecture



SIM : Subscriber Identity Module

ME : Mobile Equipment

MS : Mobile Station

BTS : Base Transceiver Station

BSC : Base Station Controller

HLR : Home Location Register

VLR : Visitor Location Register

EIR : Equipment Identify Register

MSC : Mobile Service Switching Station

AuC : Authentication Center

UM : Radio Link

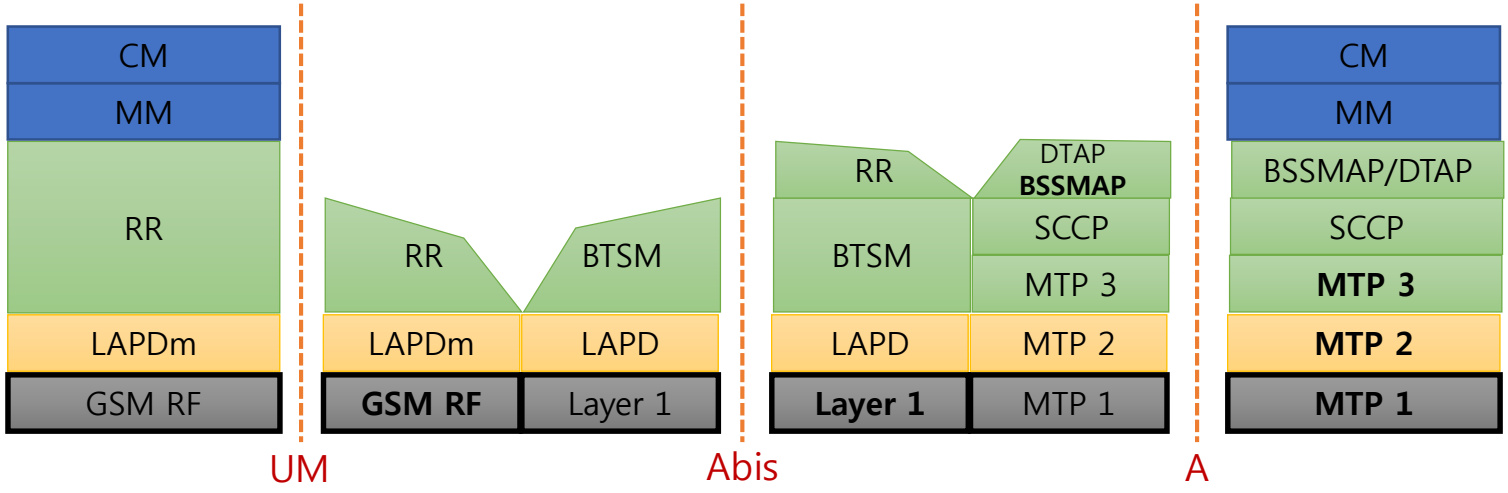
NMS : Network Management System

GSM Interface (1/2)

Interface	Description
Um Interface	▪ The "air" or radio interface standard that is used for exchanges between a mobile (ME) and a base station (BTS / BSC). For signaling, a modified version of the ISDN LAPD, known as LAPDm is used
Abis Interface	▪ This is a BSS internal interface linking the BSC and a BTS, and it has not been totally standardized. The Abis interface allows control of the radio equipment and radio frequency allocation in the BTS
A Interface	▪ The A interface is used to provide communication between the BSS and the MSC. The interface carries information to enable the channels, timeslots and the like to be allocated to the mobile equipment being serviced by the BSSs. The messaging required within the network to enable handover etc to be undertaken is carried over the interface
B Interface	▪ The B interface exists between the MSC and the VLR . It uses a protocol known as the MAP/B protocol. As most VLRs are collocated with an MSC, this makes the interface purely an "internal" interface. The interface is used whenever the MSC needs access to data regarding a MS located in its area
C Interface	▪ The C interface is located between the HLR and a GMSC or a SMS-G. When a call originates from outside the network, i.e. from the PSTN or another mobile network it ahs to pass through the gateway so that routing information required to complete the call may be gained. The protocol used for communication is MAP/C, the letter "C" indicating that the protocol is used for the "C" interface. In addition to this, the MSC may optionally forward billing information to the HLR after the call is completed and cleared down
D Interface	▪ The D interface is situated between the VLR and HLR. It uses the MAP/D protocol to exchange the data related to the location of the ME and to the management of the subscriber
E Interface	▪ The E interface provides communication between two MSCs. The E interface exchanges data related to handover between the anchor and relay MSCs using the MAP/E protocol

GSM Interface (1/2)

Interface	Description
F Interface	▪ The F interface is used between an MSC and EIR. It uses the MAP/F protocol. The communications along this interface are used to confirm the status of the IMEI of the ME gaining access to the network
G Interface	▪ The G interface interconnects two VLRs of different MSCs and uses the MAP/G protocol to transfer subscriber information, during e.g. a location update procedure
H Interface	▪ The H interface exists between the MSC the SMS-G. It transfers short messages and uses the MAP/H protocol
I Interface	▪ The I interface can be found between the MSC and the ME. Messages exchanged over the I interface are relayed transparently through the BSS

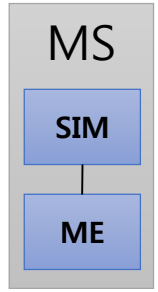


The layered model of the GSM architecture integrates and links the peer-to-peer communications between two different systems

Mobile Station

GSM MSs consist of

- Mobile Equipment
- SIM (Subscriber Identity Module)



Mobile Station

Functions of Mobile Station

- Voice and data transmission & receipt
  - ✔ Can receive, store, send SMS up to 160 charactors
- Frequency and time synchronization
- Monitoring of power and signal quality of the surrounding cells
  - ✔ Power levels of 20W, 8W, 5W, 2W and .8W
- Provision of location updates even during inactive state
- MS identified by unique IMEI shown on pressing "*#06#"

SIM (Subscriber Identity Module) (1/2)

❖ SIM has microprocessor and memory

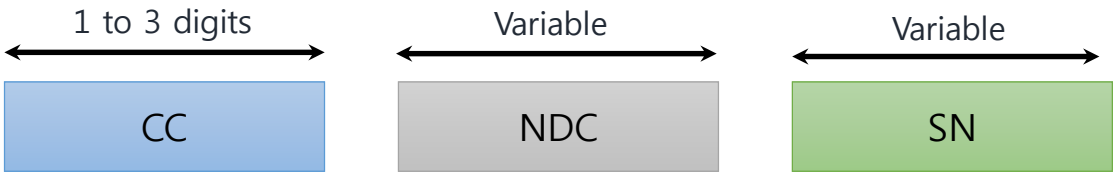
- Fixed data stored for the subscription
  - ✔ IMSI
  - ✔ Authentication Key , Ki
  - ✔ Security Algorithms : Kc, A3, A8
  - ✔ PIN & PUK

❖ Network Identities

- IMEI (International Mobile Equipment Identity)
  - ✔ Unique Code and is checked in the EIR
  - ✔ White List, Grey List, Black List

White list : IMEI, assigned to valid ME.
Black list : IMEI reported stolen
Gray list : IMEI having problems like faulty software, wrong make of equipment etc.

- MSISDN (Mobile Station ISDN Number)
  - ✔ Is register in the telephone directory and used by the calling party for dialing
  - ✔ Shall not exceed 15 digits



NDC : National Destination Code
SN : Subscriber Number

SIM (Subscriber Identity Module) (2/2)

❖ Network Identities (cont.)

- IMSI (International Mobile Subscriber Identity)
  - ✔ An unique identity which is used internationally and used within the network to identify the mobile subscribers
  - ✔ Stored in the SIM, the HLR, VLR database
- TMSI (Temporary Mobile Subscriber Identity)
  - ✔ Is a temporary IMSI No. made known to an MS at registration
  - ✔ The VLR assigns a TMSI to each mobile subscribers entering the VLR area
  - ✔ Assigned only after successful authentication
- MSRN (Mobile Station Roaming Number)
  - ✔ Used in the GMSC to setup a connection to the visited MSC/VLR
  - ✔ Is a temporary identity which is assigned during the establishment of a call to a roaming subs

NSS (Network Subsystem)

Network Subsystem contains

- MSC, VLR, HLR, AC and EIR

Main Functions

- Call control
  - ✔ Identifies the subscriber, establish a call, and clear connection
- Charging
  - ✔ Collect the charging information about a call and transferers it to the Billing Center
- Mobility management
  - ✔ Maintain information about subscriber's location
- Signaling
  - ✔ Interface with the BSS and PSTN
- Subscriber data handling
  - ✔ Permanent data → HLR
  - ✔ Temporary data → VLR

NSS Entities

Entity	Functionality
MSC **(**Mobile service Switching Center**)**	▪ Call control (Switching and call routing) ▪ Initiation of paging ▪ Charging data collection ▪ Service provisioning ▪ Communication with other NEs (HLR, VLR, MSCs, BSCs)
VLR **(**Visitor Location Register**)**	▪ Temporary data (data valid when subscriber is within its service area) ▪ Identification numbers of the subscribers ▪ Security information for authentication of the SIM card and for ciphering ▪ Services that the subscriber can use ▪ Data in VLR : IMSI & TMSI, MSISDN, MSRN, Location Area, Supplementary service parameters, MS category, Authentication Key
HLR **(**Home Location Register**)**	▪ Permanent data ▪ Keeps track of the current location of its customers ▪ Same functionality the VLR
AC **(**Authentication Center**)**	▪ Provides security information to the network (for verify the SIM cards) - TRIPLET : RAND, SRES, Kc
EIR **(**Equipment Identity Register**)**	▪ Responsible for IMSI checking (for verify the mobile equipment) ▪ Only one EIR per PLMN

BSS (Base Station Subsystem)

Base Satation Subsystem contains

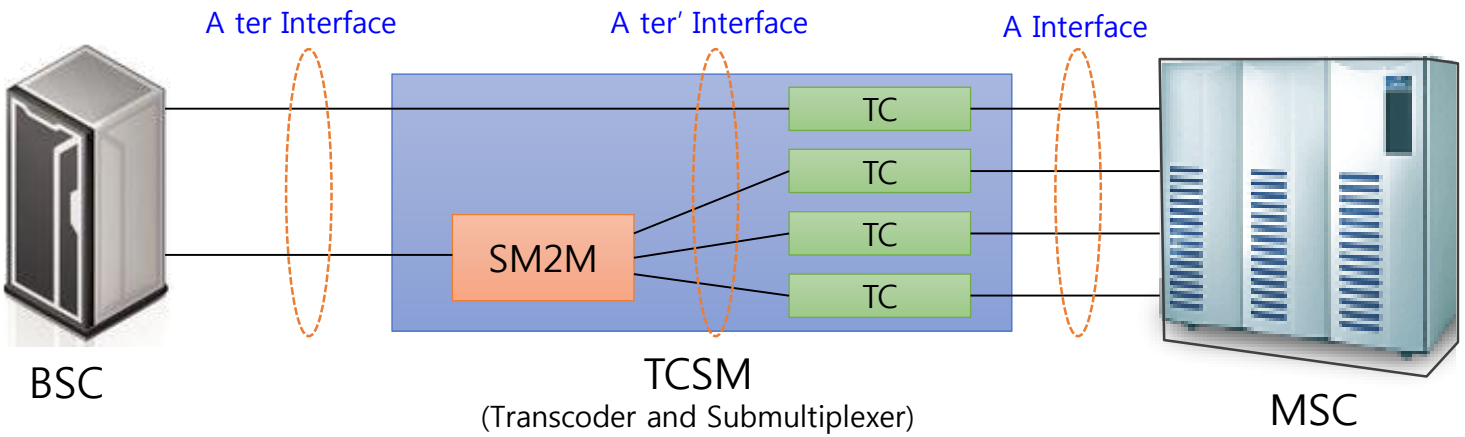
- BSC, BTS and TC (Transcoder)

Main Functions

- Radio path control
  - ✔ Taking care of radio resources (channel allocation and quality of the radio connection)
- Synchronisation
  - ✔ It is a critical issue in the GSM network due to the nature of the information transferred
- Air-and A-interface signalling
- Connection establishment between the MS and the NSS
  - ✔ May be either Signalling connection or a traffic(speech, data) connection
- Mobile management and speech transcoding
  - ✔ Handover and transcoding

BSS Entities

Entity	Functionality
BSC **(**Base Station Controller**)**	▪ Connection establishment between the MS and the NSS ▪ Mobility management (Handling of MS connections) ▪ Statistical raw data collection (Internal BSC O&M) ▪ Air-and A-interface signaling support (Radio Resource Management) ▪ BTS and TC control
BTS **(**Base Transceiver Station**)**	▪ Air interface signaling (Radio resource, Signaling link management) ▪ Ciphering (Synchronization) ▪ Speech processing (Signal processing)
TC(SM) **(**Transcoder (SubMultiplexer)**)**	▪ To enable an efficient transmission, the digital speech signal is compressed



TC is a device that takes 13 KBPS speech data and multiplexes four of them into standard 64 Kbps data

NMS (Network Management Subsystem)

Network Management Subsystem contains

- Workstation, Servers, and router, etc

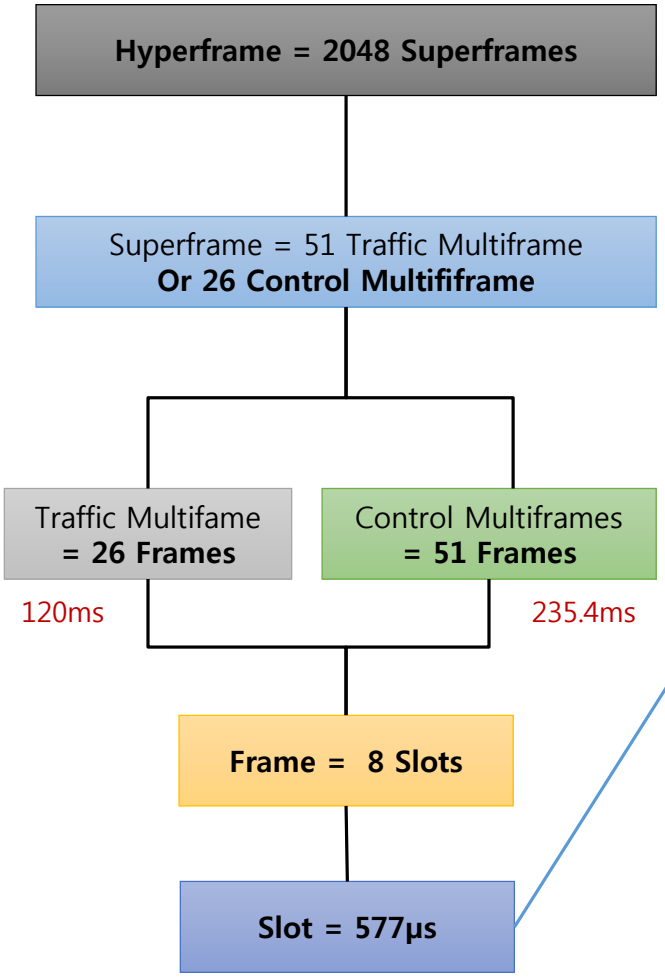
Main Functions

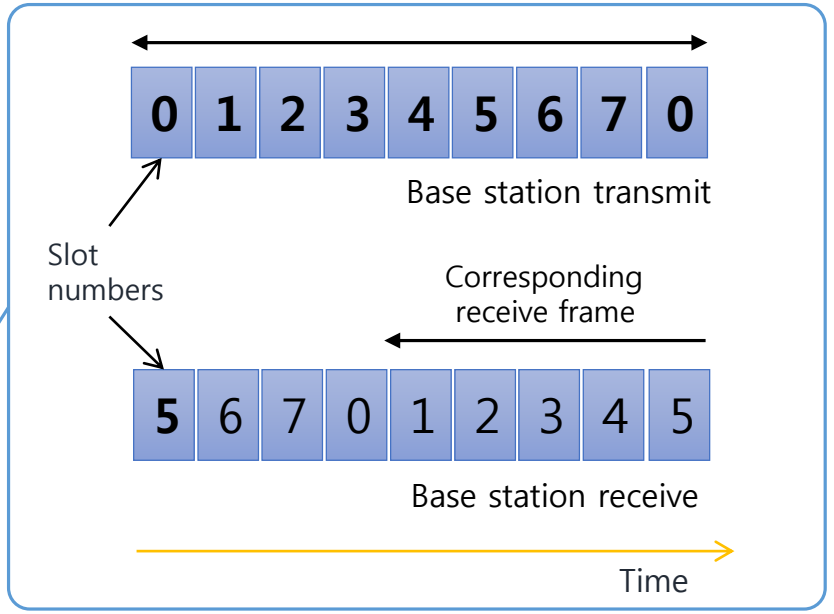
- Fault management
  - ✔ Ensure the smooth operation of the network
  - ✔ Rapid correction of any kind of problems that are detected
- Configuration management
  - ✔ Maintain up-to-date information about operation and configuration status of NE
  - ✔ Including management of the radio network, S/W and H/W , time synchronization, security operation
- Performance management
  - ✔ Collects measurement data from individual network elements and stores it in a database
  - ✔ Network operator is able to compare the actual performance of the network with the planned performance

OMC (Operations and Maintenance Centre)

- **Dynamic monitoring & Controlling of the network**
  - The centralized operation of the various units in the system and functions needed to maintain the subsystems
  - Functions
    - ✔ O&M data function
    - ✔ Configuration management
    - ✔ Fault report and alarm handling
    - ✔ Performance supervision/management
    - ✔ Storage of system software and data

GSM Frame Structure



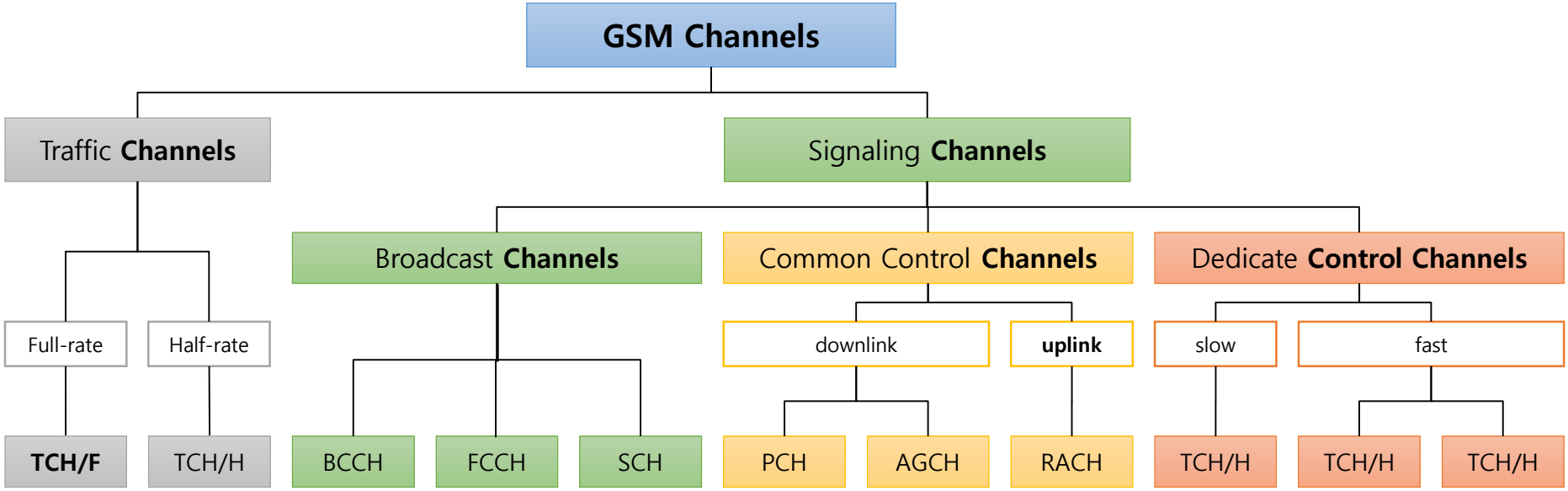


Traffic multiframe: The Traffic Channel frames are organised into multiframes consisting of 26 bursts and taking 120 ms. In a traffic multiframe, 24 bursts are used for traffic. These are numbered 0 to 11 and 13 to 24. One of the remaining bursts is then used to accommodate the SACCH, the remaining frame remaining free. The actual position used alternates between position 12 and 25.

Control multiframe: the Control Channel multiframe that comprises 51 bursts and occupies 235.4 ms. This always occurs on the beacon frequency in time slot zero and it may also occur within slots 2, 4 and 6 of the beacon frequency as well. This multiframe is subdivided into logical channels which are time-scheduled

- Frequency correction burst, Synchronization burst
- Broadcast channel (BCH), Paging and Access Grant Channel (PACCH), Stand Alone Dedicated Control Channel (SDCCH)

GSM Channels



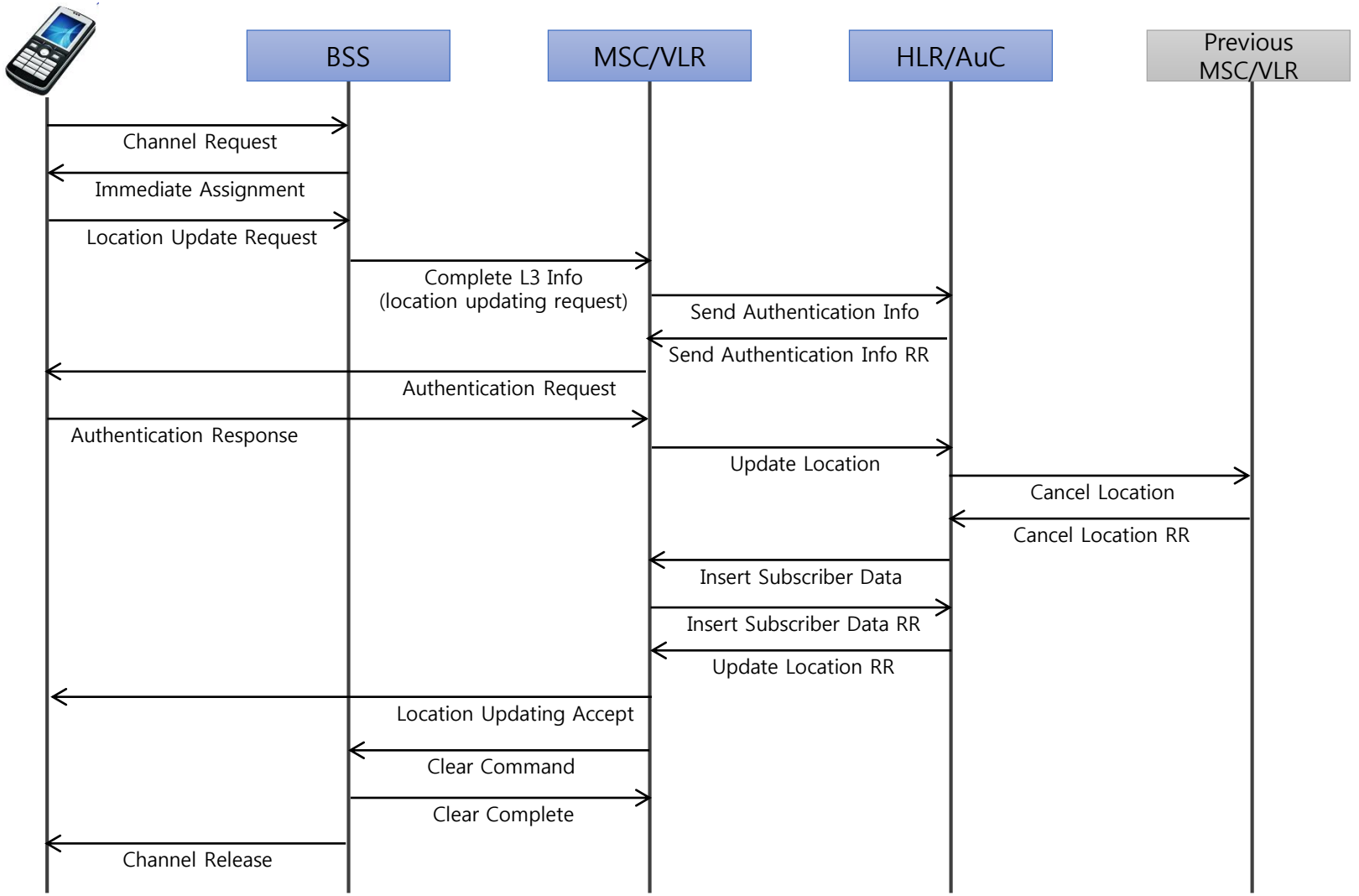
Common Channel	▪ The forward common channels are used for paging to inform a mobile of an incoming call, responding to channel requests, and broadcasting bulletin board information. ▪ The return common channel is a random access channel used by the mobile to request channel resources before timing information is conveyed by the BSS
Dedicate Channel	▪ The signaling channels are used for maintenance of the call and for enabling call set up, providing facilities such as handover when the call is in progress, and finally terminating the call. ▪ The traffic channels handle the actual payload

TCHf : Full rate traffic channel.
TCH h : Half rate traffic channel.
BCCH : Broadcast Network information,
SCH : Synchronisation of the MSs.
FCHMS : frequency correction.
AGCH : Acknowledge channel requests from MS and allocate a SDCCH.
PCHMS : terminating call announcement.

RACHMS : access requests, response to call announcement, location update, etc.
FACCHt : For time critical signalling over the TCH (e.g. for handover signalling)
SACCHt : TCH in-band signalling, (e.g. for link monitoring)
SDCCH : For signalling exchanges, (e.g. during call setup, registration / location updates)
FACCHs : FACCH for the SDCCH.
SACCHs : SDCCH in-band signalling (e.g. for link monitoring)

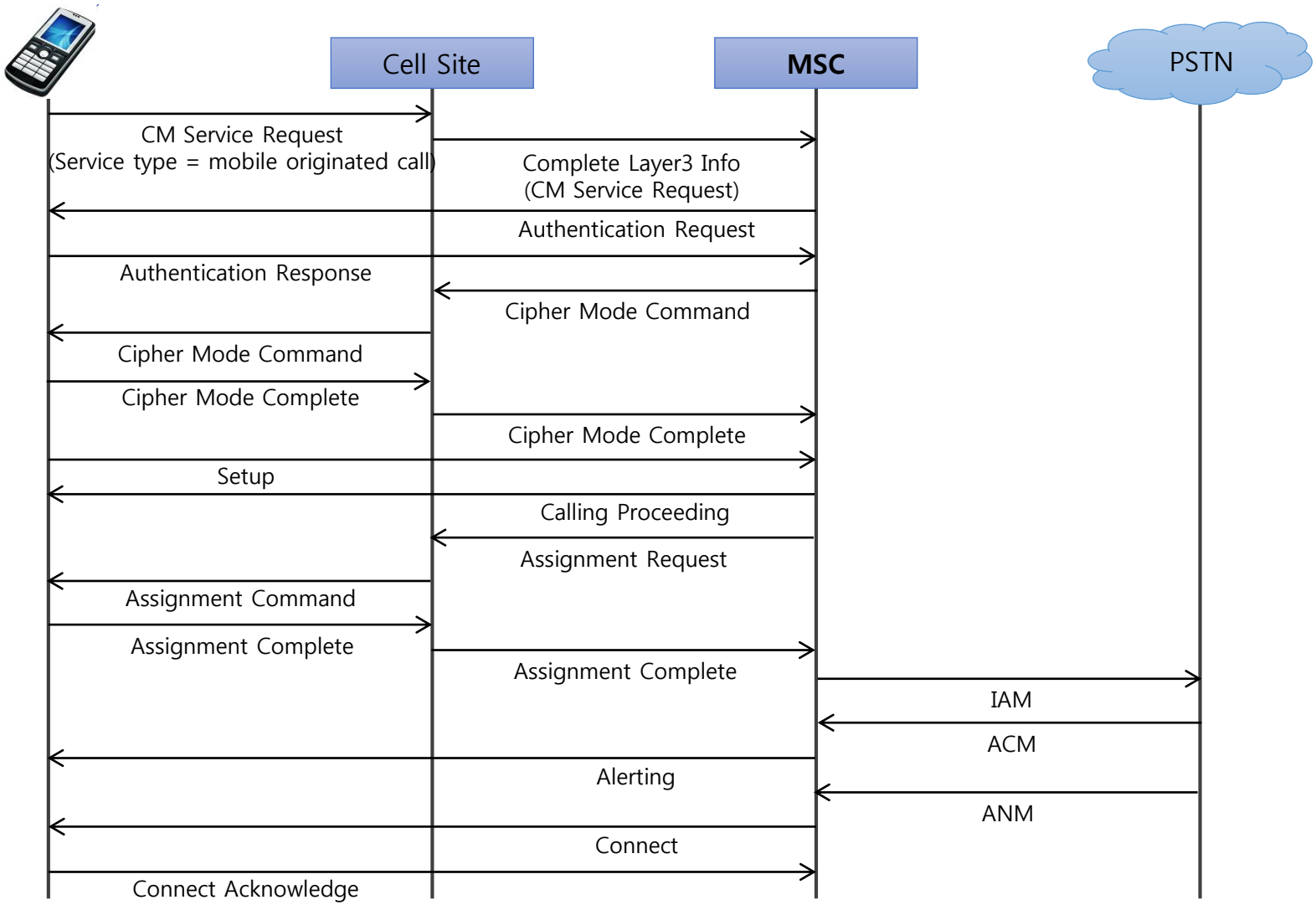
GSM Call Scenario 1

❖ Location update



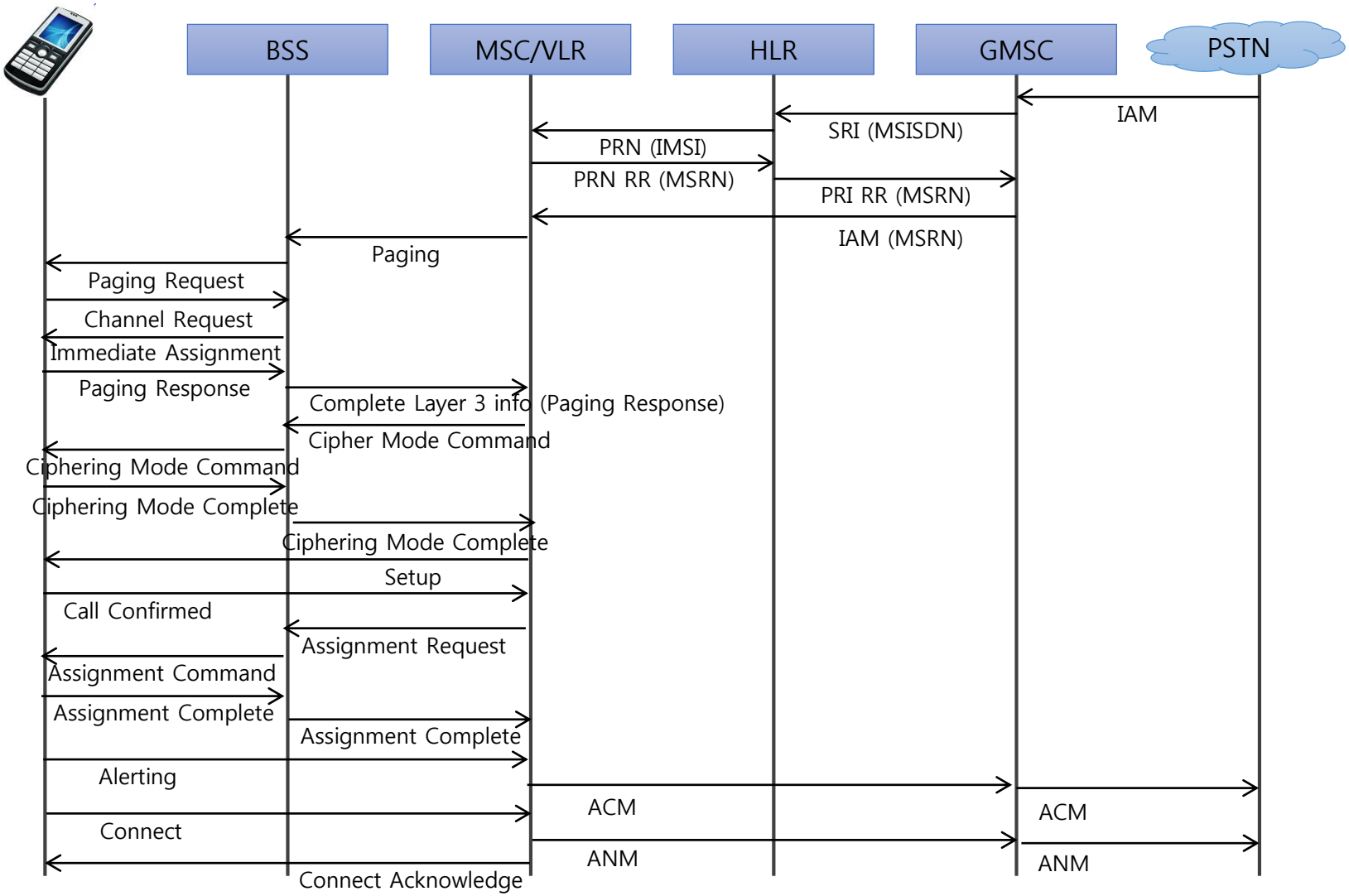
GSM Call Scenario 2

❖ Mobile to Network



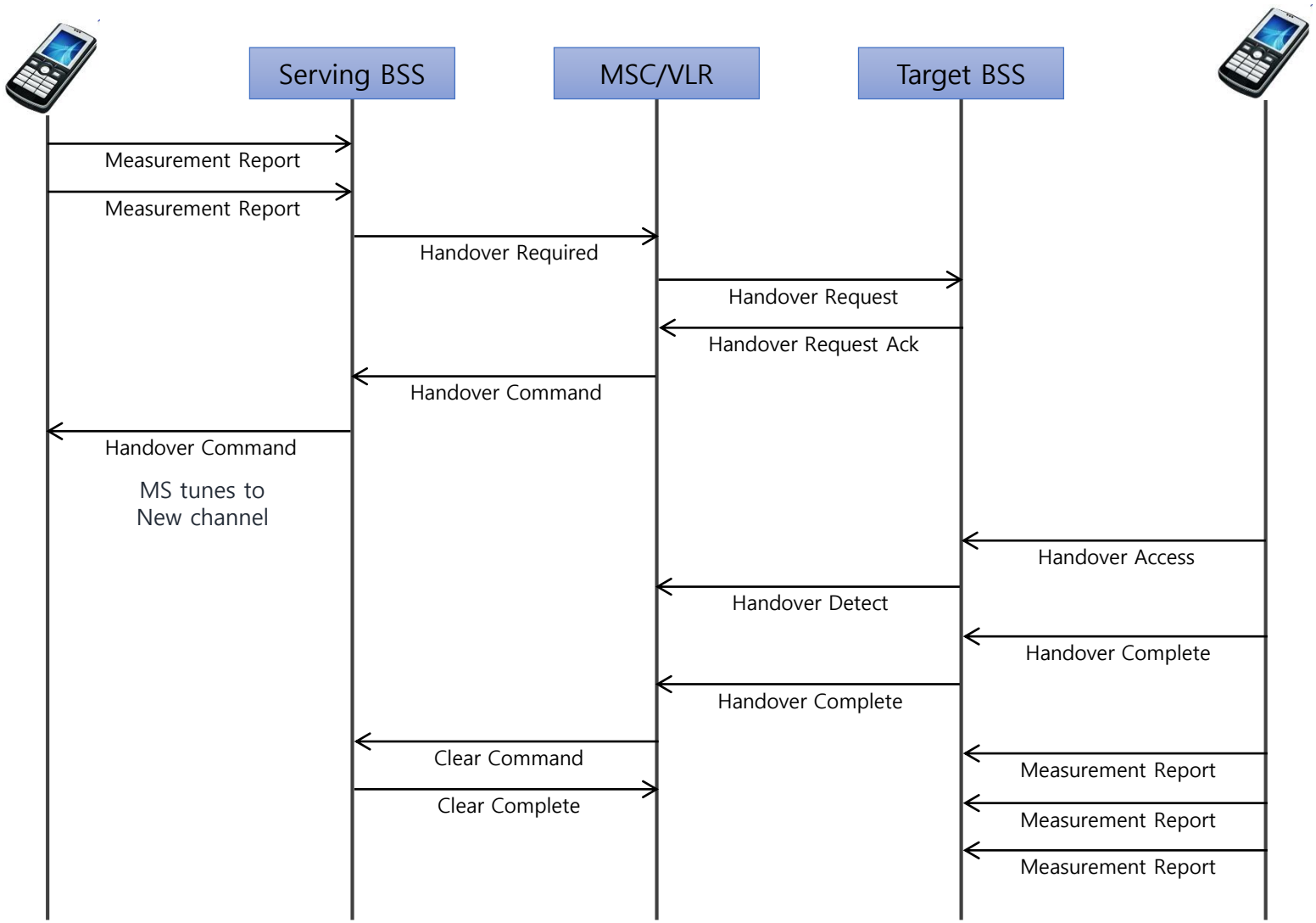
GSM Call Scenario 3

- **Network to Mobile**



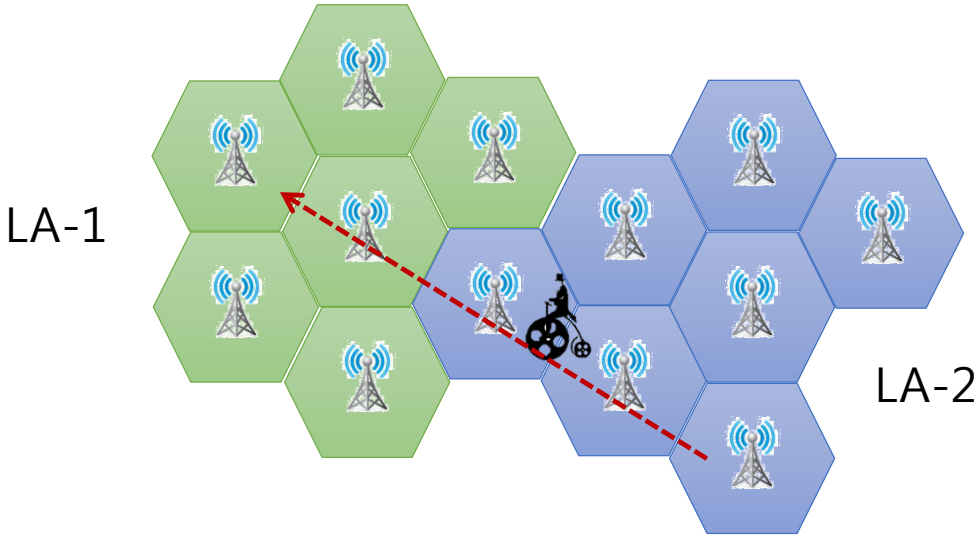
GSM Handover Scenario

❖ Handover between BSCs



Appendix : Mobility Management

- **In-session mobility management**
  - Move during an active call
  - Hand-off management
- **Out-of-session mobility management**
  - Move in standby mode
  - Location management : Update (Registration) and Paging

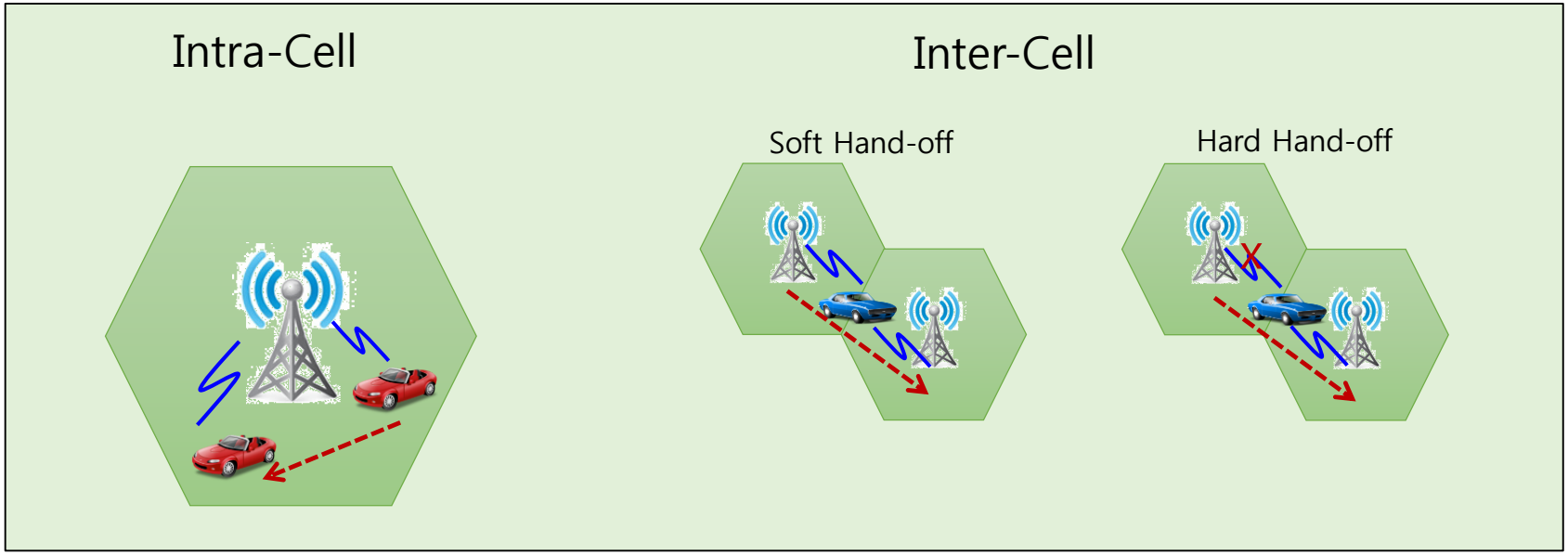


Appendix : Hand-off

❖ Hand-off = Handover

- Transfer of a MS from one cell to another
- Each BS constantly monitors the received power from each MS
- When power drops below given threshold
- BS asks neighbor station (with stronger received power) to pic up the MS, on a new channel

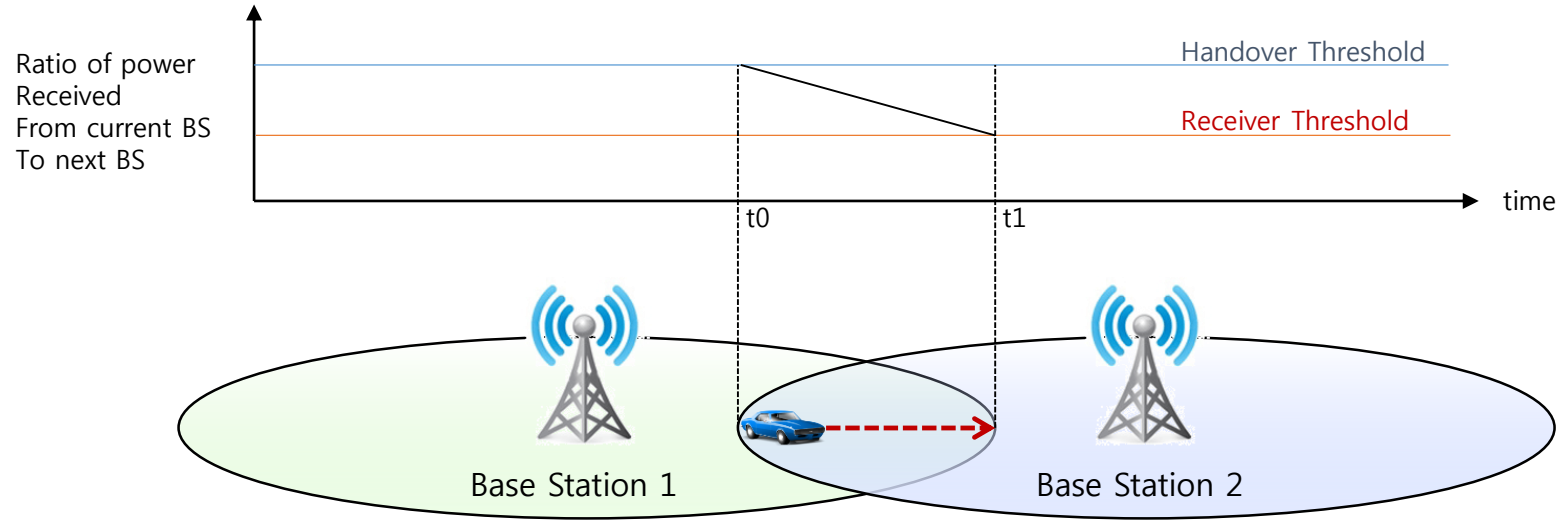
❖ Hand-off Types



Appendix : Hand-off Problem

Hand-off is

- the process of switching from one frequency channel to another by the user in midst of a communication
- Normally induced by …
  - ✔ Received Signal Strength (RSS)
  - ✔ Signal-to-Noise Ration (SNR)
  - ✔ Bit Error Rate (BER)
- Triggered either by the BS or the mobile station
  - ✔ In GSM, MAHO (Mobile-Assisted HandOver)




Thank You !