RV College of Engineering®

Go, change the world

Wireless Mobile Networks
18MCA531

Dr. Manjunath M

Assistant Professor,

Dept. of Computer Application

R.V College of Engneering

Bangalore

Second-Generation Mobile Networks
GSM:
Architecture and Protocols

1G

- It basically was a network with only voice call capabilities.
- It has called by name such as AMPS, MTS, IMTS
- It was Introduced in 1980s
- Uses FDMA, anaolg modulation
- Bulkier handsets

2G (GSM)

- Global System for Mobile (GSM)
- It is the 2nd generation Cellular Standard with its own communication protocol, interfaces and functional entities
- It was developed by **European Telecommunications Standard Institution (ETSI)** in **1991**
- GSM support voice and data services
- Uses **TDMA** and **Digital modulation**

- ***Low Cost & Size***
- ***GSM introduced SIM Cards***

GSM Network Architecture

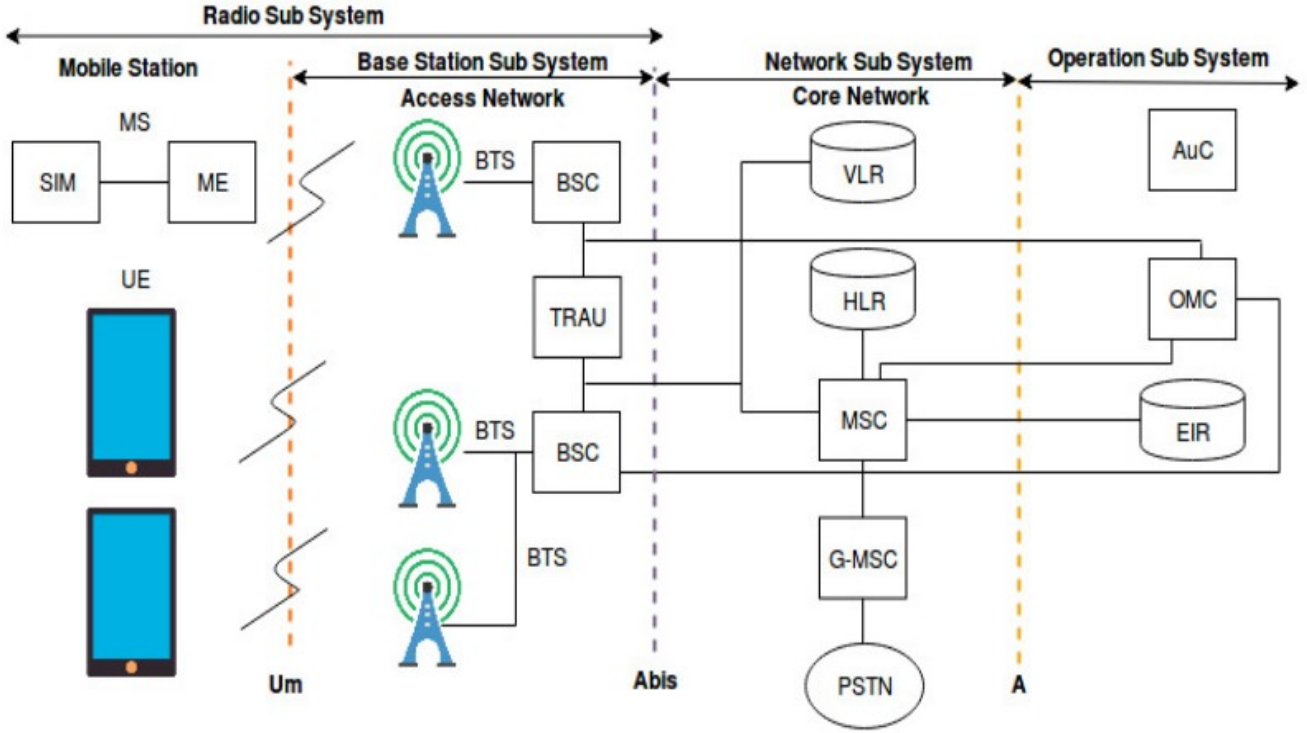


Figure 1: Representation of GSM Architecture

- ***Radio Subsystem (RSS)***
- ***Network Switching Sub-System (NSS)***
- ***Operation Support Sub-System (OSS)***

GSM Network Architecture

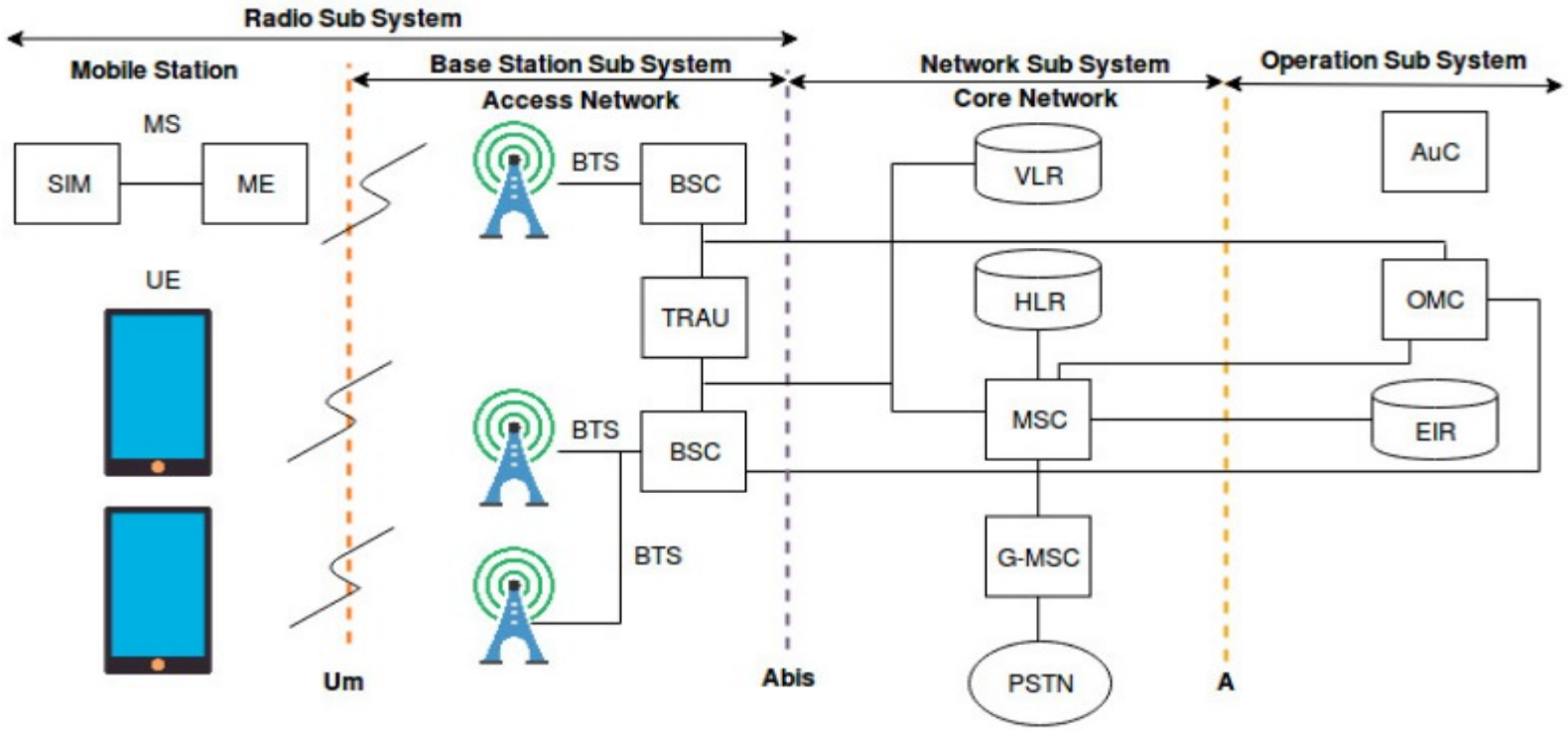


Figure 1: Representation of GSM Architecture

1. Radio Subsystem (RSS)

- It consists of
  - **Mobile Station (MS) &**
  - **Base Station Subsystem (BSS)**

Mobile Station (MS)

- The MS consists of Two Parts
  - **Mobile Equipment (cell)** :
    - Hardware used by the subscriber
    - It Contain International Mobile Equipment Identity (IMEI)
    - This is installed in the phone at manufacture and ”cannot” be changed.
  - **SIM (Subscriber Identity Module)**
    - Detachable Smartcard
    - It contains are variety of information including a number known as the International Mobile Subscriber Identity (IMSI).
    - Used to send and receive calls

Base Station Subsystem (BSS)

- The Base Station Subsystem (BSS) section of the GSM network architecture that is associated by communicating with the mobiles on the network.
- The BSS consists of Three Parts
  - **BTS (Base Transceiver Station)**
  - **BSC (Base Station Controller)**
  - **TRAU (Transcoding and Rate Adaptation Unit)**

1. Radio Subsystem (RSS)

BTS (Base Transceiver Station) :

- It allow the MS to communicate with the network through radio link
- Sends & Receive Signal from MS
- It also does Encoding, Multiplexing, Encryption, Modulation and so on
- It Handle many users at the same time

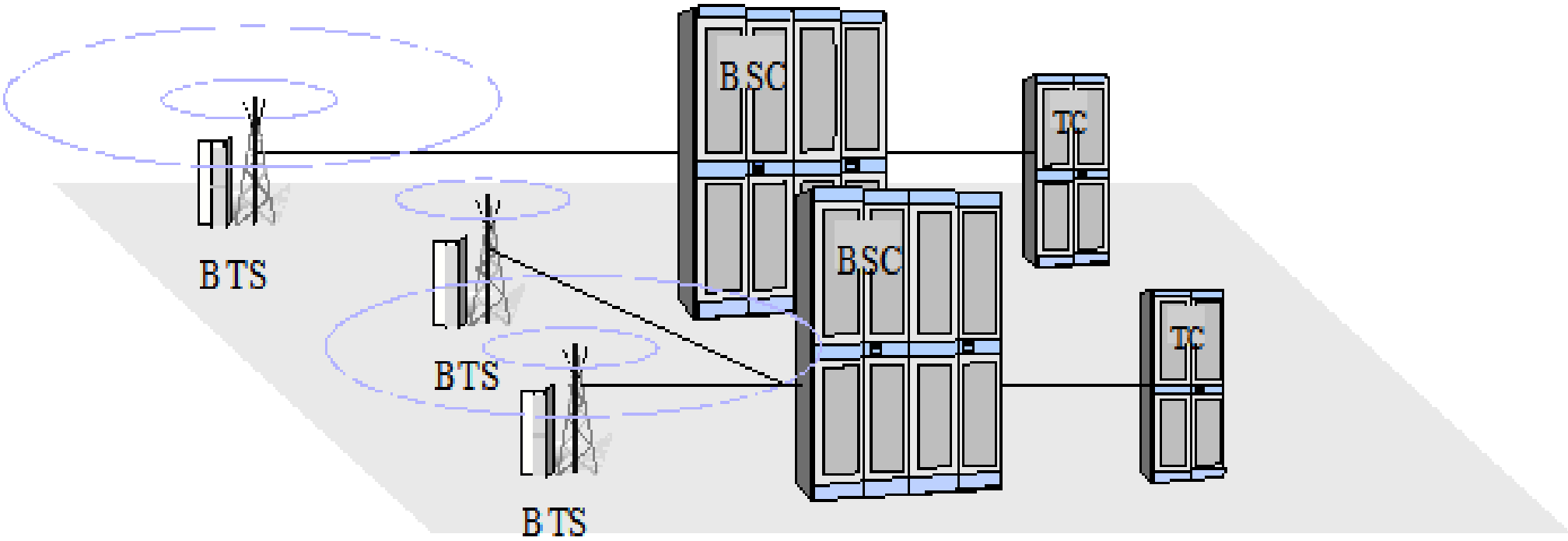
BSC (Base Station Controller)

- It controls a group of BTSs
- It allocates radio channels to BTS
- It also Handover from one BTS to another

TRAU (Transcoding and Rate Adaptation Unit)

- It is the logical part of BSS
- It convert the voice into binary stream through a complex process

1. Radio Subsystem (RSS)

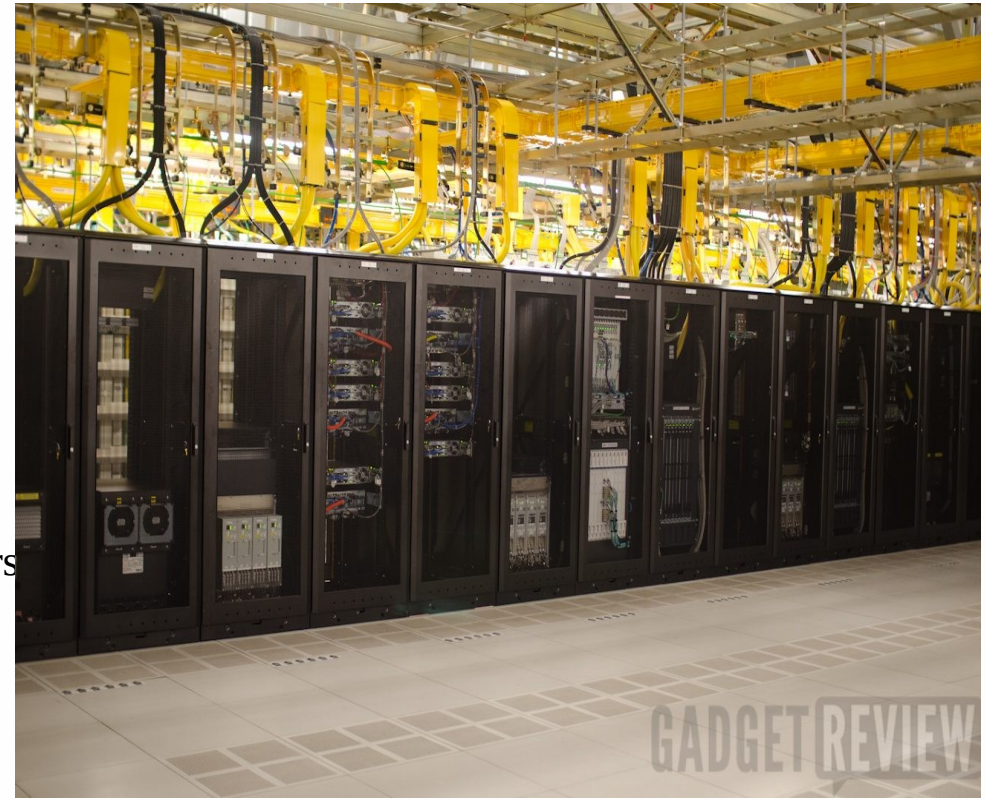


Network Switching Sub-System (NSS)

- The NSS consists of Three Parts
  - **MSC (Mobile Switching Center)**
  - **HLR (Home Location Register)**
  - **VLR (Vistor Location Register)**

MSC (Mobile Switching Center)

- Heart of GSM Network
- It is a telephone exchange that makes the connection between mobile users within the network,
  - From Mobile to PSTN or
  - From PSTN to Mobile or
  - From Mobile to Mobile.
- Peforms call routing, call setup & call switching
- The MSC also administers
  - handovers to neighbouring base stations,
  - keeps a record of the location of the mobile subscribers
  - Responsible for subscriber services and billing.
- Communicates with HLR, VLR and AUC



HLR (Home Location Register)

- It maintains all the information related to a mobile subscriber in it database.
- The HLR contains
  - information about the subscribers identity,
  - his telephone number,
  - the associated services and
  - general information about the location of the subscriber

VLR (Visitor Location Register)

- Subset of HLR
- It is another temporary database to which the scbscriber currently registers
- The VLR contains the exact location of all mobile subscribers currently present in the service area of the MSC
- This information is necessary to route a call to the right base station.
- The database entry of the subscriber is deleted when the subscriber leaves the service area.

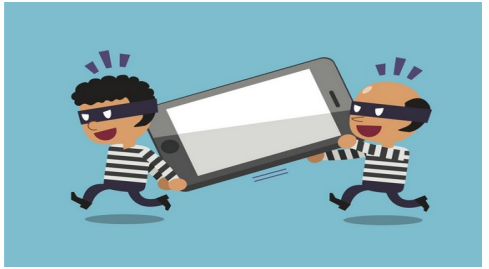
Operation Subsystem (OSS)

- It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS.
- The OSS consists of Three Parts
  - **AUC (Authentication Center)**
  - **EIR (Equipment Identity Register)**
  - **OMC (Opertion and Maintance Center)**

AUC (Authentication Center)

- The Authentication Centre (AUC) is a function in a GSM network used for the authentication a mobile subscriber that wants to be connected to the networ
- Authentication is done by identification and verification of the validity of the SIM.

EIR (Equipment Identity Register)



- Database containg all the valid handsets on network using IMEI number
- Marks IMEI as invalid, if handset is stolen

OMC (Opertion and Maintance Center)

- Monitors and controls the network elements for smooth running of the network
- Guarantees the best possible service quality for the network;
- It also perform network measurement & fault management

Simplified Architecture

User

MS

Tower

BST

Eqipment

BSC

Center

MSC

Telephone Network

PSTN, ISDN

GSM Multiple Access Scheme

GSM Multiple Access Schemes

- The limited radio spectrum is to be shared by all users in Public Land Mobile Telephone Networks (PLMN).
- For spectral efficiency, GSM works on a combination of
  - Frequency Division Multiplexing (FDM) and
  - Time Division Multiplexing (TDM) schemes

Frequency Division Multiplexing (FDM)

- In the FDMA system, one specific frequency is allocated to one user engaged in a call.
- In Europe, GSM 900 band reserves two frequency bands for
  - **Uplink (890-915 MHz) and**
  - **Downlink (935-960 MHz) so that there exists a duplex distance of 45 MHz.**
- Divided by frequency into 124 carriers, each separated by 200 kHz.
- The **Digital Cellular system (DCS)** 1800 standard developed by ETSI is based on the GSM recommendations.
- The frequency ranges for
  - **Uplink - 1710-1785 MHz**
  - **Downlink - 1805-1880 MHz** respectively.
- A total of 374 carrier frequencies are available to the system.
- One or more carrier frequency may be assigned to the base system (BS).

Time Division Multiple Access (TDMA)

- TDMA is a channel access method for shared medium (usually radio) networks.
- It allows several users to share the same frequency channel by dividing the signal into different timeslots.
- The users transmit in rapid succession, one after the other, each using his own timeslot.
- This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only the part of its bandwidth they require.
- TDMA is used in the digital 2G cellular systems such as Global System for Mobile Communications (GSM)
- TDMA is a type of Time-division multiplexing, with the special point that instead of having one transmitter connected to one receiver, there are multiple transmitters.
- The uplink from a mobile phone to a base station this becomes particularly difficult because the mobile phone can move around and vary the timing advance required to make its transmission match the gap in transmission from its peers.

GSM Protocols and Signaling

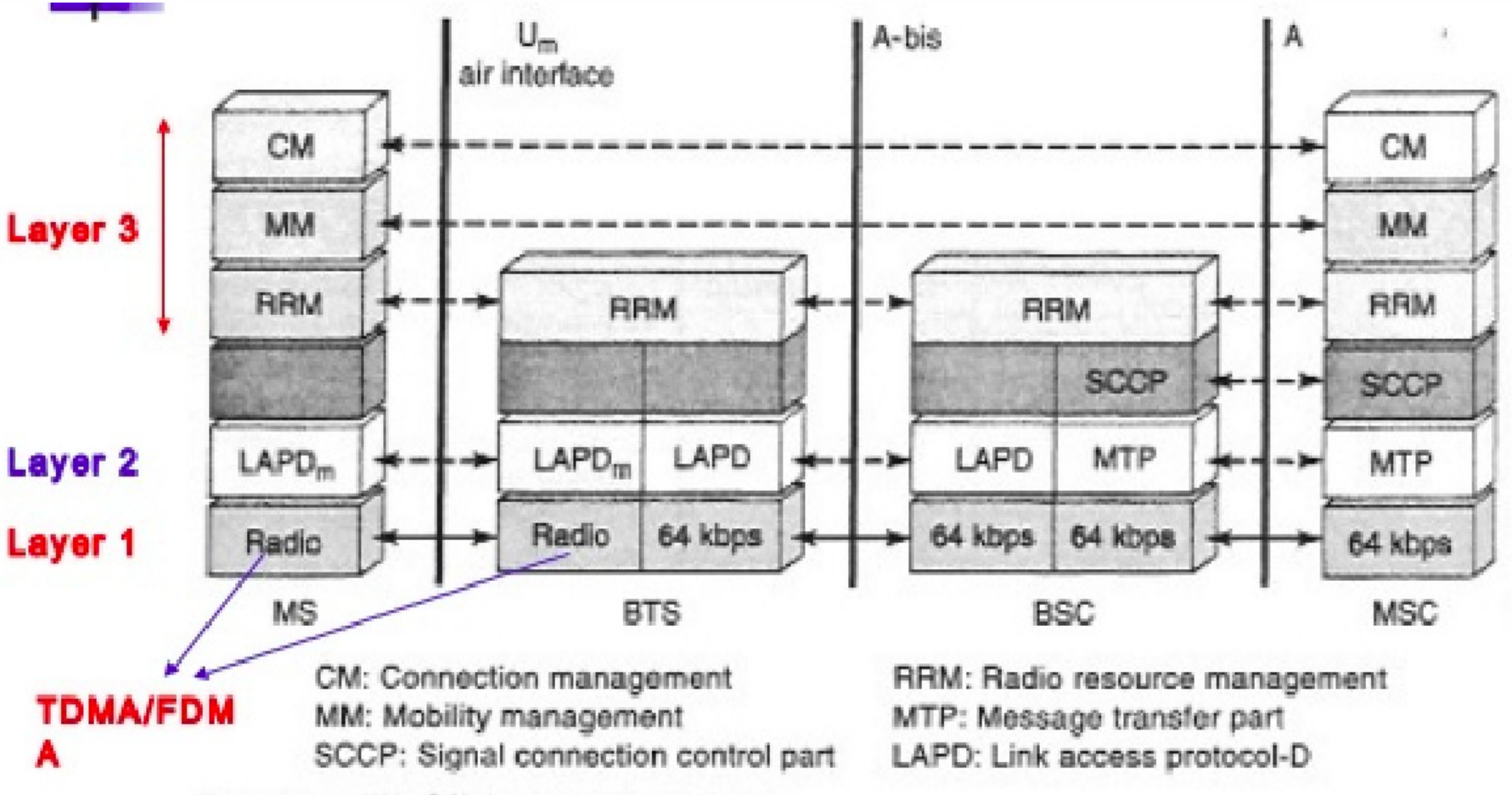
- Signalling refers to the exchange of information for
  - call set up;
  - payload refers to the data that is. transferred within a call, i.e. voice, video, fax etc.
  - For a mobile terminated GSM call, the signalling.

- The signaling protocol in GSM is structured into 3 general layers depending on the interface.
  - Layer 1 - Physical Layer
  - Layer 2 - Data Link Layer
  - Layer 3 - Network Layer

- The signaling protocol in GSM is structured into 3 general layers depending on the interface.
  - Layer 1 - Physical Layer
  - Layer 2 - Data Link Layer
  - Layer 3 - Network Layer

Layer 1 - Physical Layer

- Layer 1 is radio interface
- Provides the functionality required to transfer the bit streams over the physical channels on the radio medium.
- Services provided by this layer are
  - Channel mapping (logical to physical)
  - Channel coding and ciphering
  - Digital modulation
  - Frequency hopping
  - Timing advance and power control


U_m
air interface
A-bis
A
Layer 3
Layer 2
Layer 1
CM
MM
RRM
$LAPD_m$
Radio
RRM
$LAPD_m$
LAPD
Radio
64 kbps
RRM
SCCP
LAPD
MTP
64 kbps
64 kbps
CM
MM
RRM
SCCP
MTP
64 kbps
MS
BTS
BSC
MSC
TDMA/FDM
A
CM: Connection management
MM: Mobility management
SCCP: Signal connection control part
RRM: Radio resource management
MTP: Message transfer part
LAPD: Link access protocol-D

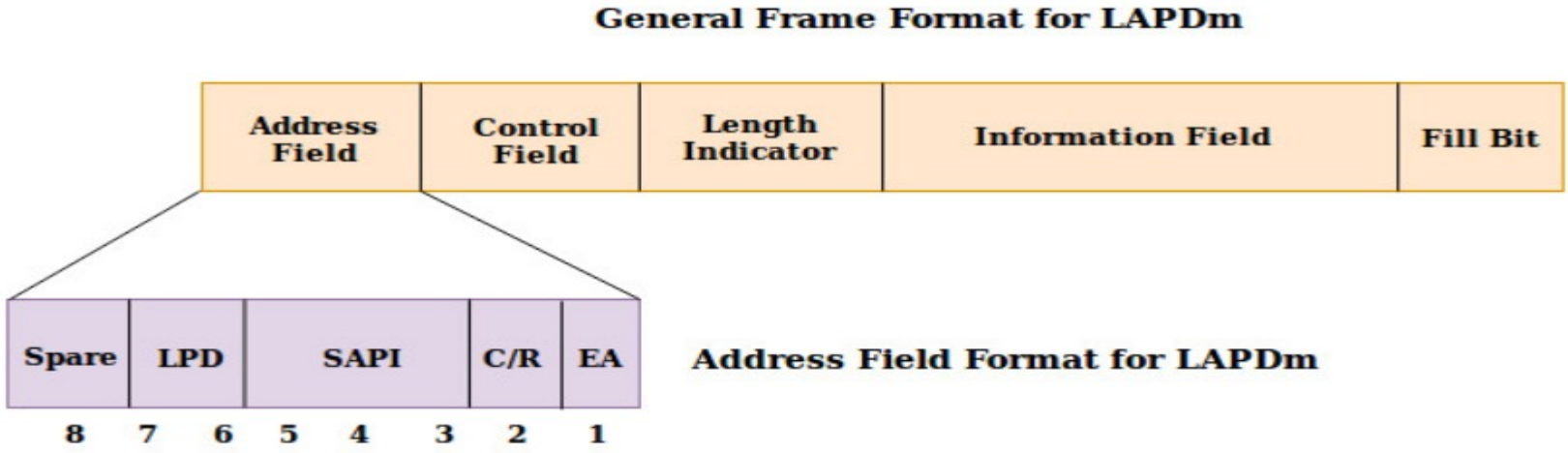


Figure 3: General Format and Address Field Format for LAPDm

- Control Field: is used to carry sequence number and specify the type of the frame(command or response)
- Length Indicator: Identify the length of the information field.
- Information Field: Carries the layer III Payload
- Fill Bits: all “1” bits. Which is variable to extend the length

Signaling Authentication and Security

- Authentication is the process to prove the identity of valid users claiming services of the Network.
- Two main entities are involved –
  - **The SIM card in the mobile device** and
  - **The Authentication Centre, AuC**.
- A secret key is provided to each user that is stored both in the SIM card and the AuC.
- A Signed Response (SRES) is generated randomly using this secret key and the **ciphering algorithm, A5.**
- Each of the GSM terminal is identified by a unique **International Mobile Equipment Identity (IMEI)** number.
- A list of IMEIs in the network is stored in the **Equipment Identity Register (EIR)**.
- For identification, the network may request a mobile user to provide the IMEI or IMSI.
- In reply, the MS should send its identity while RR connection exists between the mobile and the network.

- The status returned in response to an IMEI query to the EIR is one of the following
  - **White-listed:** The terminal is allowed to connect to the network.
  - **Grey-listed:** The terminal is under observation from the network for possible problems.
  - **Black-listed:** The terminal has either been reported stolen, or is not type approved, i.e., it is not the correct type of terminal for a GSM network. The terminal is not allowed to connect to the network then.