RV COLLEGE OF ENGINEERING®

(Autonomous Institution Affiliated To Visvesvaraya Technological University, Belagavi)

BENGALURU - 560 059

Department of Master of Computer Applications

Wireless Mobile Networks

18MCA531

Unit - 3

Faculty In-charge

Dr. Manjunath M

Assistant Professor

SEMESTER	***5th (Odd Semester)***
ACADEMIC YEAR	***2020 - 2021***

Contents

Second Generation Mobile Networks, 3G The Universal Mobile Telecommunication System (UMTS)

1. GSM Network Architecture

GSM was developed by Group Special Mobile which was contained by the CEPT (Conference of European Post and Telecommunication). The GSM network architecture as defined in the GSM specifications can be grouped into four main areas:

1. Mobile station (MS)
2. Base-Station Subsystem (BSS)
3. Network and Switching Subsystem (NSS)
4. Operation and Support Subsystem (OSS)

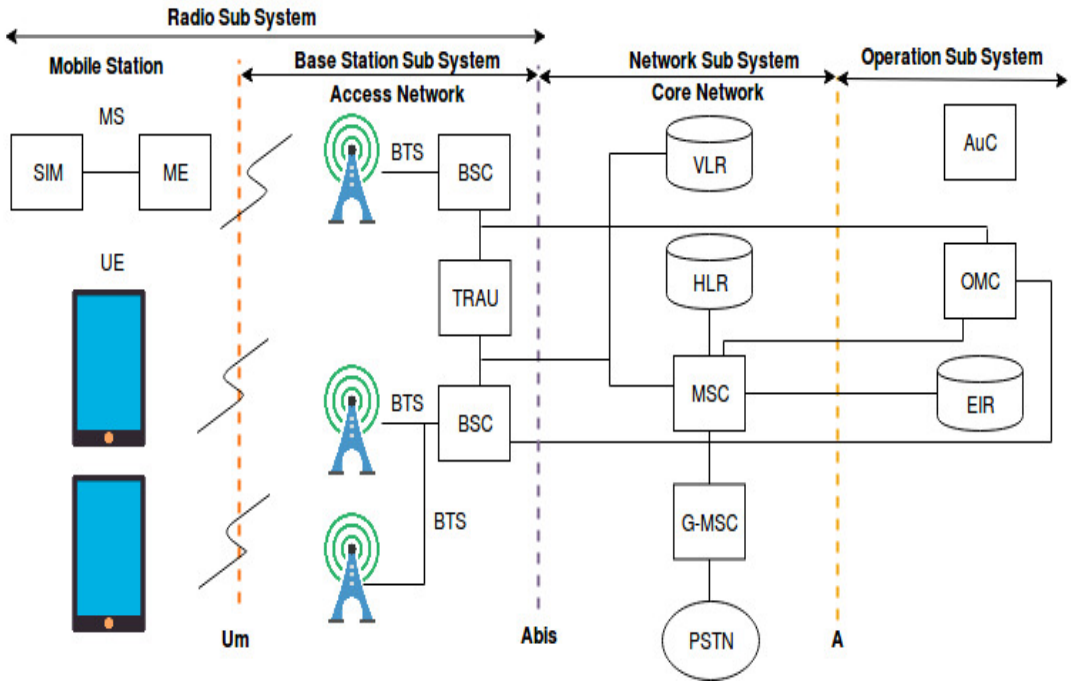

Figure 1: Representation of GSM Architecture

1.1 Mobile Station (MS)

- Mobile stations (MS) is a cell or mobile phones are the section of a GSM cellular network that the user operates. The main component of a Mobile Station is the SIM.
- The hardware contains a number known as the International Mobile Equipment Identity (IMEI). This is installed in the phone at manufacture and "cannot" be changed.
- The SIM or Subscriber Identity Module contains the information that provides the identity of the user to the network. It contains are variety of information including a number known as the International Mobile Subscriber Identity (IMSI).

1.2 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.
- With air interface BSS provides MS and NSS (Network Station Subsystem).
- BSS consists of following elements.

1.2.1 Base Transceiver Station (BTS)

:

- The BTS used in a GSM network comprises the radio transmitter receivers, and their associated antennas that transmit and receive to directly communicate with the mobiles.
- The BTS is the defining element for each cell. The BTS communicates with the mobiles and the interface between the two is known as the Um interface with its associated protocols.

1.2.2 Base Station Controller (BSC)

:

- The BSC forms the next stage back into the GSM network. It controls a group of BTSs, and is often co-located with one of the BTSs in its group.
- It manages the radio resources and controls items such as handover within the group of BTSs, allocates channels and the like.
- It communicates with the BTSs over what is termed the Abis interface.

1.3 Network Switching Subsystem (NSS)

1.3.1 Mobile Switching Centre (MSC)

- The Mobile Switching Centre (MSC) is a telephone exchange that makes the connection between mobile users within the network, from mobile users to the public switched telephone network and from mobile users to other mobile networks.
- The MSC also administers handovers to neighbouring base stations, keeps a record of the location of the mobile subscribers, is responsible for subscriber services and billing.

1.3.2 Gateway MSC (GMSC)

- The MSC with an interface to other network like Public Switched Telephone (PSTN) is called Gateway Main Switching Center.

1.3.3 Home Location Register (HLR)

- The Home Location Register is a database from a mobile network in which information from all mobile subscribers is stored.
- The HLR contains information about the subscribers identity, his telephone number, the associated services and general information about the location of the subscriber.

1.3.4 Visitor Location Register (VLR)

- The Visitor Location Register (VLR) is a database in a mobile communications network associated to a Mobile Switching Centre (MSC).
- 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.

1.4 Operation and Support Subsystem (OSS)

- The OSS or operation support subsystem is an element within the overall GSM network architecture that is connected to components of the NSS and the BSC.
- It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS.
- It must be noted that as the number of BS increases with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing savings in the cost of ownership of the system.

1.4.1 Authentication Center (AUC)

- 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 network.
- Authentication is done by identification and verification of the validity of the SIM.

1.4.2 Equipment Identity Register (EIR)

- The Equipment Identity Register (EIR) is a database that contains a record of the all the mobile stations (MS)that are allowed in a network as well as an database of all equipment that is banned, e.g. because it is lost or stolen.
- The identity of the mobile station is given by the International Mobile Equipment Identity (IMEI).
- Each time a call is made, the MSC requests the IMEI of the mobile station, which is then send to the EIR for authorization.

1.4.3 Operation and Maintenance Center

- Operation and Maintenance Center is the central location to operate and maintain the network.

2. 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 the time division multiplexing (TDM) schemes in addition with different interference reduction techniques, i.e., emission power control optimized handover decision methods.

2.1 Frequency Division Multiple Access (FDMA)

- 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 and downlink for this are 1710-1785 MHz and 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).

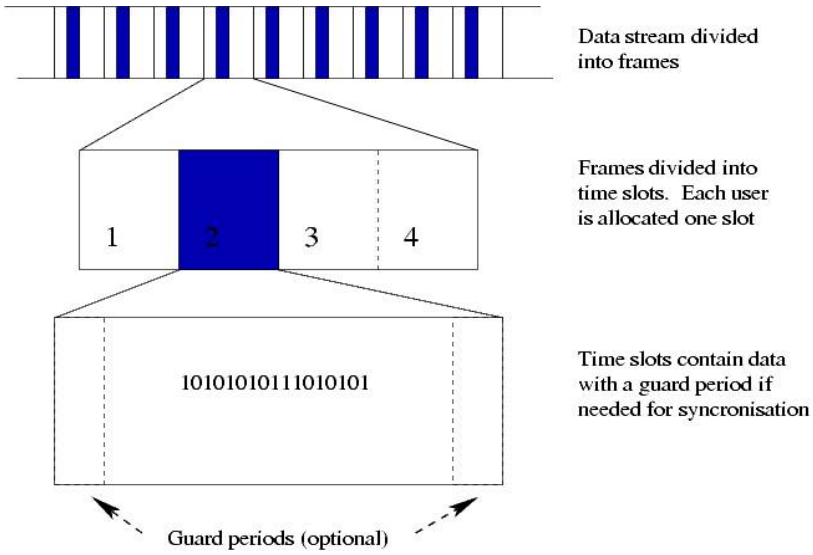

Figure 2: Time division multiple access (TDMA)

- Depending on the call size, propagation environments and cell organization, BS may select the reuse frequency considering the interference effects also.

2.2 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.

3. GSM Protocols

The GSM specifications define the interaction between system components through well-defined interfaces and protocols. The signaling protocol in GSM is structured into 3 general layers depending on the interface.

Layer 1 - Physical Layer

- The following section describes the Um interface protocols used at the MS and the BTS side.
- Layer 1, which is a radio interface, provides the functionality required to transfer the bit streams over the physical channels on the radio medium.
- The services provided by this layer to those above include:

- Channel mapping (logical to physical)
- Channel coding and ciphering
- Digital modulation
- Frequency hopping
- Timing advance and power control

Layer 2 - Data Link Layer

- Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm).
- Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used.

Layer 3 - Network Layer

- The third layer is divided into three sub-layers:
- Radio Resource Management (RR)
- Mobility Management (MM)
- Connection Management (CM)

Radio Resource Management (RR) Radio resource management (RR) comprises procedures required to establish, maintain, and release the dedicated radio connections.

Mobility Management (MM) The sub-layer handles functions and procedures related to mobility of the mobile user.

Connection Management (CM) The connection management (CM) sublayer contains the functions and procedures for call control. This includes procedures to establish, release, and access services and facilities. The CM consists of three sublayers, namely, Call Control (CC), Supplementary Services (SS), and Short Message Services (SMS).

3.1 U_m interface

The "air" or radio interface standard that is used for exchanges between a mobile (ME) and a base station (BTS / BSC). For signalling, a modified version of the ISDN LAPD, known as LAPDm is used.

3.2 A_{bis} Interface

This is a BSS internal interface linking the BSC and a BTS, and it has not been totally standardised. The Abis interface allows control of the radio equipment and radio frequency allocation in the BTS.

3.3 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 equipments being serviced by the BSSs. The messaging required within the network to enable handover etc to be undertaken is carried over the interface.

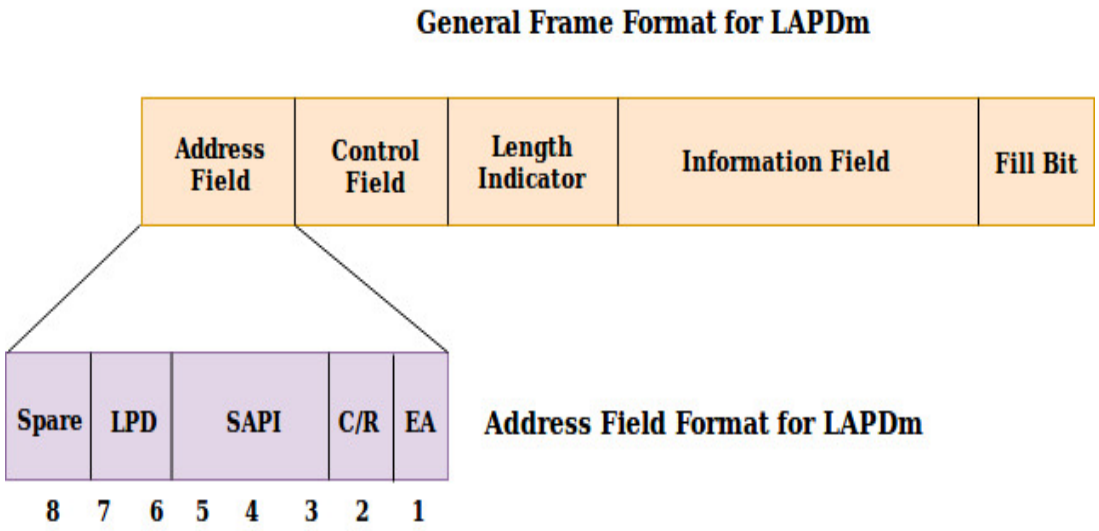

Figure 3: General Format and Address Field Format for LAPDm

3.4 Link Layer LAPDm Protocol

- The data link-layer over the radio link connects the MS to the BSS based on a LAPD- like protocol, called LAPDm.
- LAPDm does not use any flag or frame delimitation, rather the physical layer defining the frame boundaries does frame delimitation.
- There is a length indicator in LAPDm to distinguish the information-carrying field from the fill-in its used to fill the transmission frame.
- LAPDm uses a 3-bit Service Access Point Identifier (SAPI) as an address field.
- SAPI 0 is used for call control, MM and RR signaling.
- SAPI 3 is used for SMS.
- All the other fields are reserved for future purpose.
- The data-link layer also provides the priority assignment as low, normal and high priority to messages that are transferred in dedicated mode on SAPI 0.
- The general frame format for LAPDm is shown in
- There is the address field that has the frame format as shown in
- The two-bits Link Protocol Discriminator (LPD) is used to specify a particular recommendation of the use of LAPDm, the C/R is a single bit which specifies a command or response frame as used in LAPD, and a 1-bit Extended Address (EA) is used to extend the address field to more than one octet.
- The EA bit in the last octet of the address should be set to 1, otherwise it is set to 0. The 8-bit is reserved for future uses.
- The control field is to carry sequence numbers and to specify types of frame.
- There are three types of LAPDm frames, one for supervisory functions, unnumbered information transfer and control functions for unacknowledged mode and numbered information transfer for multiframe acknowledged mode.
- LAPDm has no Cyclic Redundancy Check (CRC) flag, as it is done by the combination of block convolutional coding used in the Layer 1 (Physical).

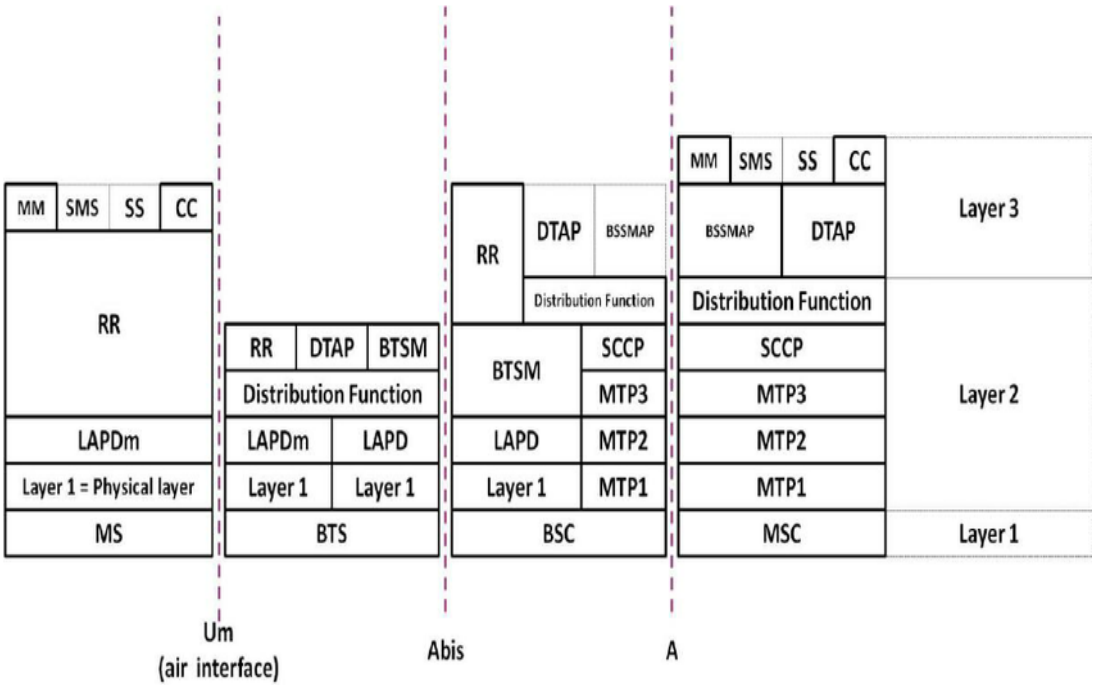

Figure 4: GSM Signaling Protocols

3.5 Message Layer Protocols

- Protocols above the link layer of the GSM signaling protocol architecture provide specific functions:

  1. Radio Resource Management
  2. Mobility Management
  3. Connection Management
  4. Mobile application part (MAP)
  5. BTS Management

- **Radio Resource Management (RR- Layer)** The RR-Layer is concerned with the management of RR-session, which is the time that a mobile is in dedicated mode, as well as the configuration of radio channels.

- In addition RR-Layer manages power control, discontinues transmission and reception, and handovers.

- There are four types of handovers

  1. Switching channels in the same cell
  2. Switching cells under control of the same Base Station Controller (BSC)
  3. Switching cells under the control of different BSCs, but belonging to the same Mobil service Switching Center (MSC)
  4. Switching cells under control of different MSC

- Control channels used by idle mode mobiles to exchange signaling information, required changing to dedicated mode. Mobiles in dedicated mode monitor the surrounding Base Stations for handover and other information.

- The Control channels include: Broadcast Control Channel (BCCH) serves for BS identification, broadcasts, and frequency allocations. Frequency Correction Channel (FCCH) and Synchronization Channel (SCH) – used for synchronization, and physical layer definition (time slots, burst time. . .) Random Access Channel (RACH) used by mobile to

request access to the network. Paging Channel (PCH) used for locating the mobile user Access Grant Channel (AGCH) used to obtain a dedicated channel.

- **Mobility Management (MM-Layer)** - Manages problem that arise from mobility of the subscriber.
- In GSM,a group of neighbor cells is grouped in one location area and subscriber updates its position when moving from one location area to another.
- Paging is done only in the current location area.
- **Connection Management** - This layer is based on application layer with respect to the other layers. E.g. An incoming mobile termination call is directed to Gateway MSC (GMSC). GMSC is basically a switch, which is able to interrogate the subscribers HLR to obtain routing information.
- **BSSAP** - The BSSAP user function is further subdivided into two separate functions: **(DTAP) & (BSSMAP)**
- In the case of point-to-point calls the BSSAP uses one signalling connection per active mobile station having one or more active transactions for the transfer of layer 3 messages.
- In the case of a voice group or broadcast call there is always one connection per cell involved in the call and one additional connection per BSS for the transmission of layer 3 messages.

  The Direct Transfer Application sub-Part (DTAP), also called GSM L3, is used to transfer messages between the MSC and the MS (Mobile Station); the layer-3 information in these messages is not interpreted by the BSS. The descriptions of the layer 3 protocols for the MS-MSC information exchange are contained in the series of GSM Technical Specifications.

4. Signaling Authentication and Security

- Authentication is the process to prove the identity of valid users claiming services of the network.
- It is important for any mobile network to identify its users.
- 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.
- This is sent back to AuC to be compared with the number generated by AuC.
- If matched, the subscriber is an authentic one.
- The authentication procedure is always initiated and controlled by the network.
- 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

(a) **White-listed**: The terminal is allowed to connect to the network.

(b) **Grey-listed**: The terminal is under observation from the network for possible problems.

(c) **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.

5. UMTS Network Architecture Release 99

The UMTS network architecture can be divided into three main elements: **User Equipment**

(UE): The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. The new name was chosen because the considerably greater functionality that the UE could have. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.

Node B The base station used in UMTS is known as 'Node B' that replaces BTS. It provides the physical radio link between the UE and the network. As the access technology is different from GSM/GPRS, Node B is capable to handle CDMA subscriber on the new frequency bands. It can also support higher data rates used for 3G. Node B is the termination point between the air interface and the transmission network of the RAN. It performs the necessary signal processing functionalities for the WCDMA air interface and is more complex than BTS. Node B is responsible for the following;

(i) **Power control**: Measures the actual signal-to-interface ratio (SIR), compares it with the threshold value and then may trigger the change of transmitting power of UE.

(ii) **Reports the RNC (Radio Network Controller)**: The measured values are reported to RNC

(iii) **Combines the received signals coming from multiple sectors of the antenna that a UE is connected to**: Converts the signals into a single data stream before it transmits to the RNC. This may help to soften the handover procedure for UMTS networks.

Three types of Node B are possible

* UTRA-FDD Node B

* UTRA-TDD Node B

* Dual Mode Node B, supporting both FDD and TDD modes.

Radio Network System (RNS): The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface fort he overall network.
The three types of RNCs

(a) **Serving RNC (SRNC)** - The SRNC controls a user's mobility within a UTRAN. It is a connection point to the core network towards MSC or SGSN.

(b) **Drift RNC (DRNC)** - The DRNC receives connected UEs that are drifted or handed over from the SRNC cell connected to a different RNS. The RRC (Radio Resource Controller) is still connected to the SRNC. The DRNC then exchanges the routing information between the SRNC and UE. Thus, the DRNC provides radio resources to the SRNC to allow soft handover.

(c) **Controlling RNC (CRNC)** - CRNC controls, configures and manages an RNS and communicates with the Node B application part (NABP) protocol with the physical resources of all Node Bs connected via the lub interfaces. Any access request from the UE is forwarded to the CRNC.

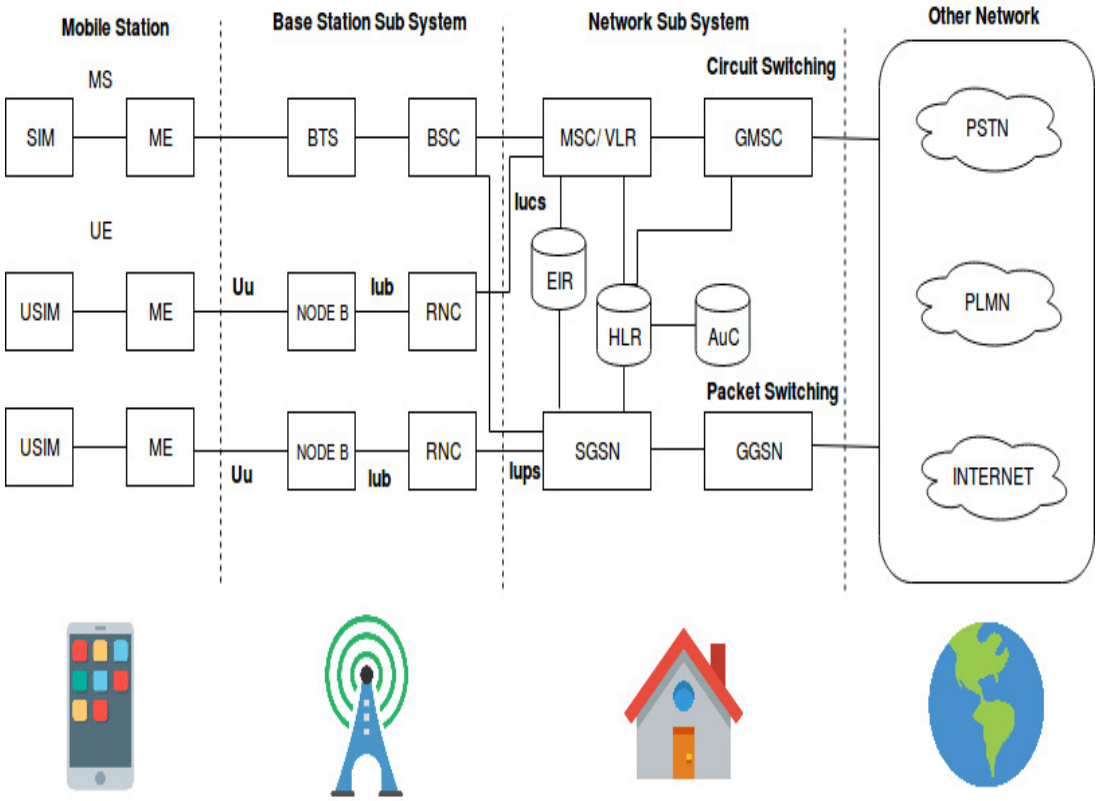

Figure 5: UMTS Network Architecture Release 99

6. UMTS Interfaces

- Apart from the interfaces used in GSM/GPRS networks, a number of other new interfaces are defined for implementation of UMTS services based on the new nodes for UMTS, namely RNC and Node B.
- The reason for defining interfaces is to operate the different UEs from different network operators accessing the UTRAN. The new interfaces that are introduced are:
  i. **Uu**: The radio interface between UE and Node B.
  ii. **Iub**: Interface between Node B and RNC
  iii. **Iur**: Interface between RNC and RNC
  iv. **Iu(CS)**: Interface between the RNC and MSC for circuit switching
  v. **Iu(PS)**: Interface between the RNC and the SGSN for packet switching
- Figure 6 shows the different interfaces used in UMTS network.
- All the new radio interfaces for UMTS are characterized through protocols that are divided into two groups; user plane protocols to carry user data and control plane protocols for controlling the connection between the UE and the network nodes.
- All these interfaces are standardized on ATM for Layer 2 except the Uu interface.
- ATM offers good QoS for all applications.
- Interface Iub transports both circuit and packet-switched data.
- The Iu (PS) transport packet-switched data is based on IP with the ATM adaptation Layer 5.
- But the interfaces Iur and Iu (CS) transport circuit-switched connection based on ATM adaptation Layer 2, suitable for real-time applications.

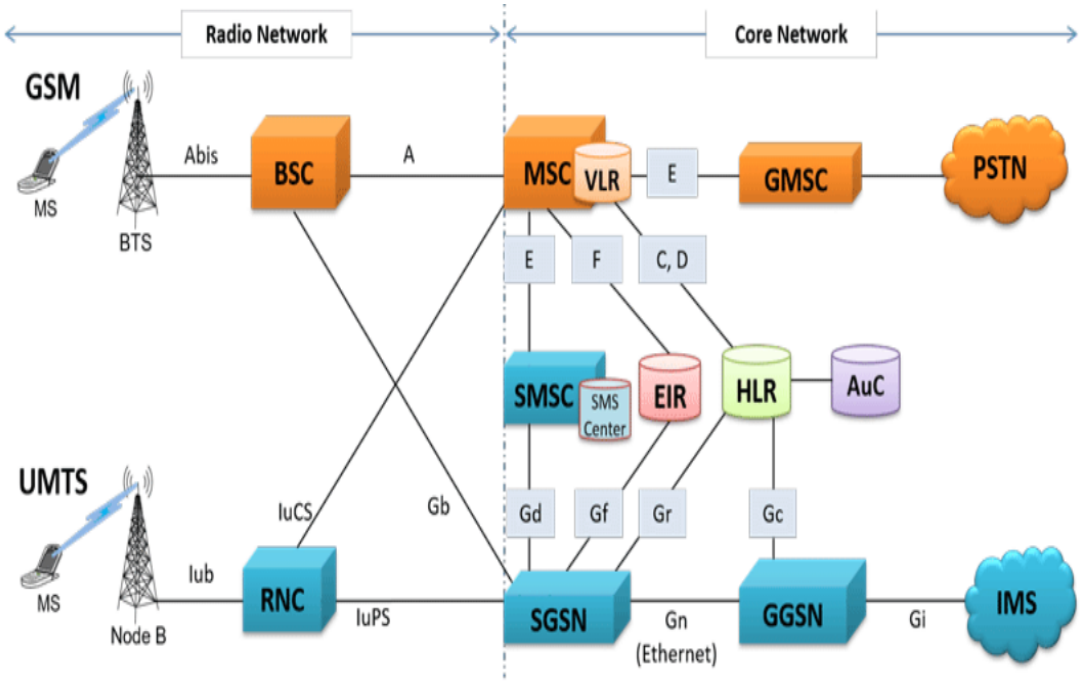

Figure 6: UMTS Interfaces

7. UMTS Networks Evolution

- A major enhancement for circuit-switched voice and data services has been specified with UMTS Release 4 (Refer Figure 7).
- The most important enhancement of UMTS Release 4 is a new concept called the bearer independent core network (BICN).
- Instead of using circuit-switched 64 kbit/s timeslots, traffic is now carried inside ATM or IP packets .
- In order to do this, the MSC has been split into an MSC server which is responsible for call control and mobility management and a media gateway which is responsible for handling the actual bearer (user traffic).
- The media gateway is also responsible for the transcoding of the user data for different transmission methods.
- This way it is possible for example to receive voice calls via the GSM A-interface via E-1 64 kbit/s timeslots at the MSC media gateway which will then convert the digital voice data stream onto a packet-switched ATM or IP connection towards another media gateway in the network.
- The two important Gateways in Release 4 architecture are
  i. ***Transport Signaling Gateway (T-SGW)-*** is used to convert call related signaling such as call setup and call release between PSTN(SS7) and Release 4 Network
  ii. **Routing Signaling Gateway (R-SGW)-** performs signaling conversion for roaming, mobility management between SS7 based signaling of pre Release 4 Network and IP based signaling of the Release 4 Network.

8. UMTS FDD and TDD

- The physical layer (L1) access for UMTS is based on Wideband Direct Sequence Code Division Multiple Access (WCDMA) Technology with two duplex modes
- FDD (Frequency Division Duplex) and TDD (Time Division Duplex).

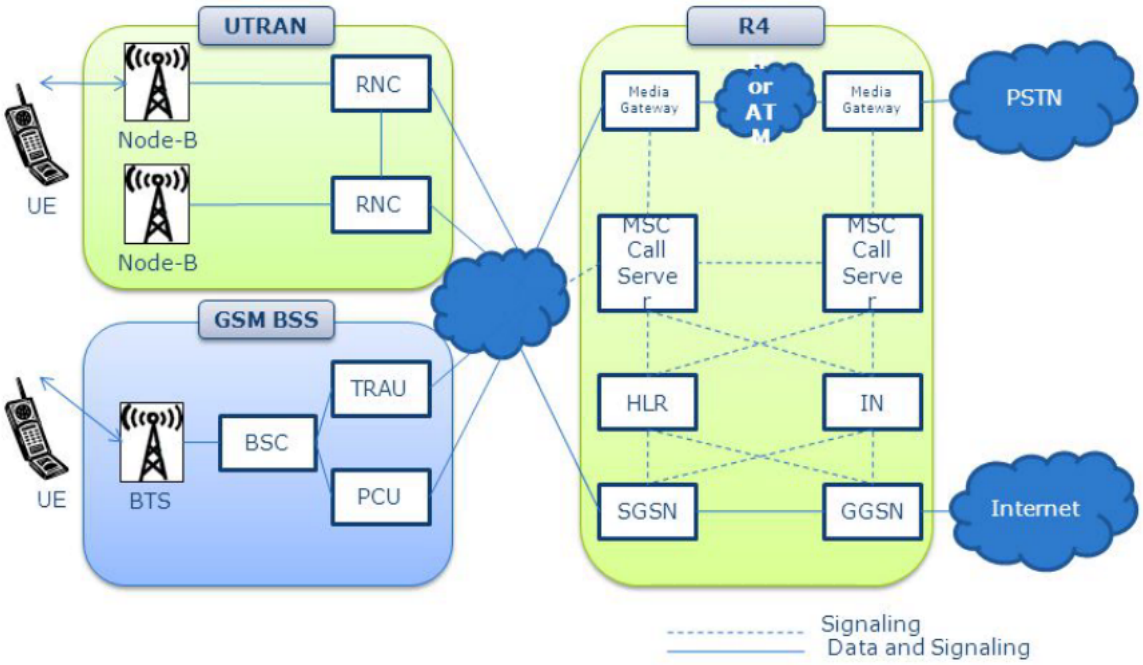

Figure 7: UMTS Release 4 Architecture

- A physical channel in FDD is defined by the code and frequency, whereas in TDD it is defined by code and time slot
- **FDD**: Uplink and downlink transmissions are separate frequency bands like GSM by placing different frequency channels.
- ITU-T spectrum usage for FDD is 1920-1980 MHz for uplink traffic and 2110-2170 MHz for downlink traffic as shown in
- The minimum paired frequency allocation required is 5 MHz, one for uplink and another for downlink.
- The frequency separation between uplink and downlink is 190 MHz.
- However, for better coverage and services, an operator needs 3-4 channels (2 * 15 MHz or 2 * 20 MHz) to be able to build a high-speed, high-capacity network.
- **TDD**: TDD system, on the other hand, requires only one 5 MHz unpaired band to operate.
- Time division multiplexing, i.e., allocating different time slots, separates the uplink and downlink traffic in TDD.
- The transmitter and receiver are not separated in frequency.
- Satellite uplink and downlink is 1980-2010 and 2170-2200 MHz.
- A UTRA Absolute Radio Frequency Channel Number (UARFCN) designates carrier frequencies. The general formula, relating frequency to UARFN, is

$$\text{UARFCN} = 5 * (\text{frequency in MHz})$$

- The difference between FDD and TDD is only on the lower layer radio interface.
- On the higher layers, the two systems are the same.
- The 10-ms frame structure is divided into 15 equal time slots of 2560 * Tc (Tc = chip rate) to be allocated either in uplink or downlink.

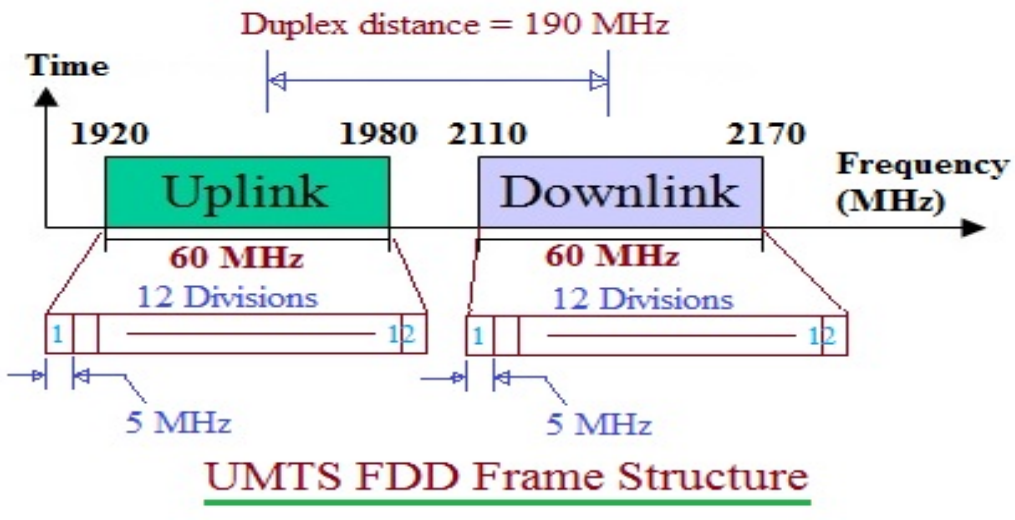

Figure 8: UMTS FDD Frame Structure

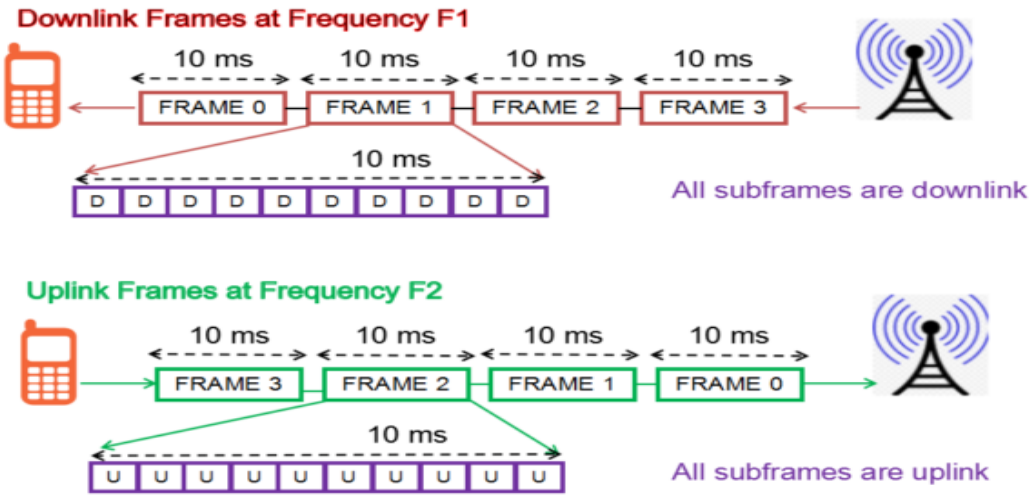

Figure 9: FDD Frame Structure Format

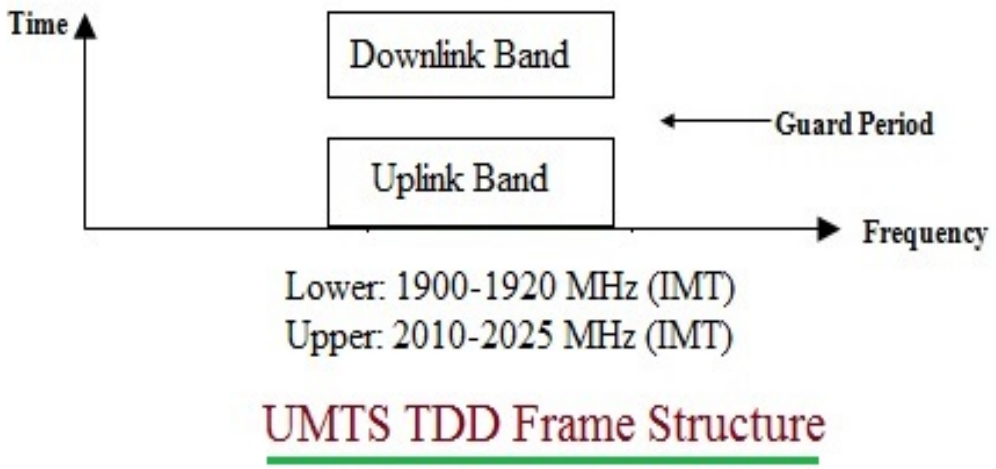

Figure 10: UMTS TDD Frame Structure

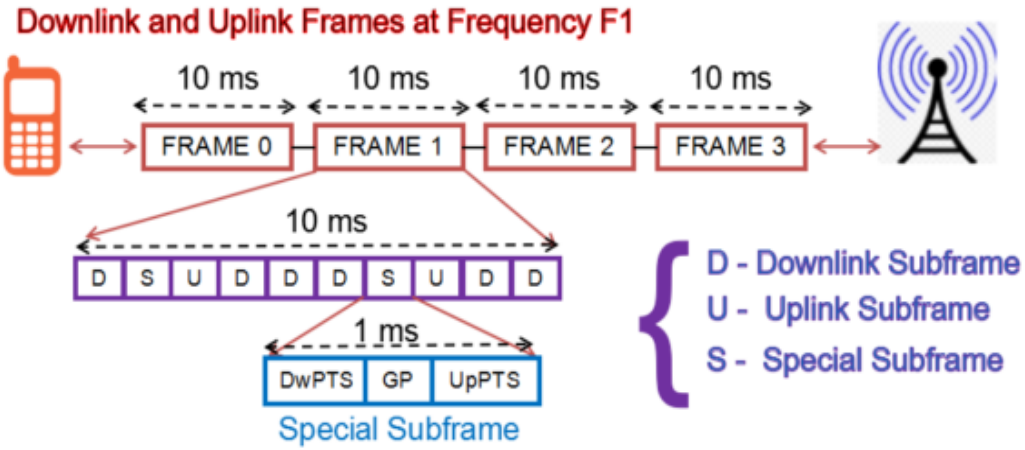

Figure 11: TDD Frame Structure Format

- With such flexibility, the TDD scheme becomes more adaptive between varied environment and deployment scenarios.
- In many cases, at least one time slot is allocated for downlink and at least one time slot for uplink.

9.UMTS Channels

- UMTS Channels posses three types of channels. viz. logical channels(RLC layer), transport channels(MAC layer) and physical channels(PHY layer).
- As they transverse between layers they map to other layer frames.
- For example logical channels are mapped to transport channels and transport channels are mapped to physical channels.

UMTS Logical Channels & Transport Channels

- UMTS/WCDMA logical channels are divided into control channels and traffic channels(DTCH, CTCH).
- As the name suggests traffic channels carry information(voice) and control channels carry signalling information useful to establish and maintain connection between UE and network(NodeB).

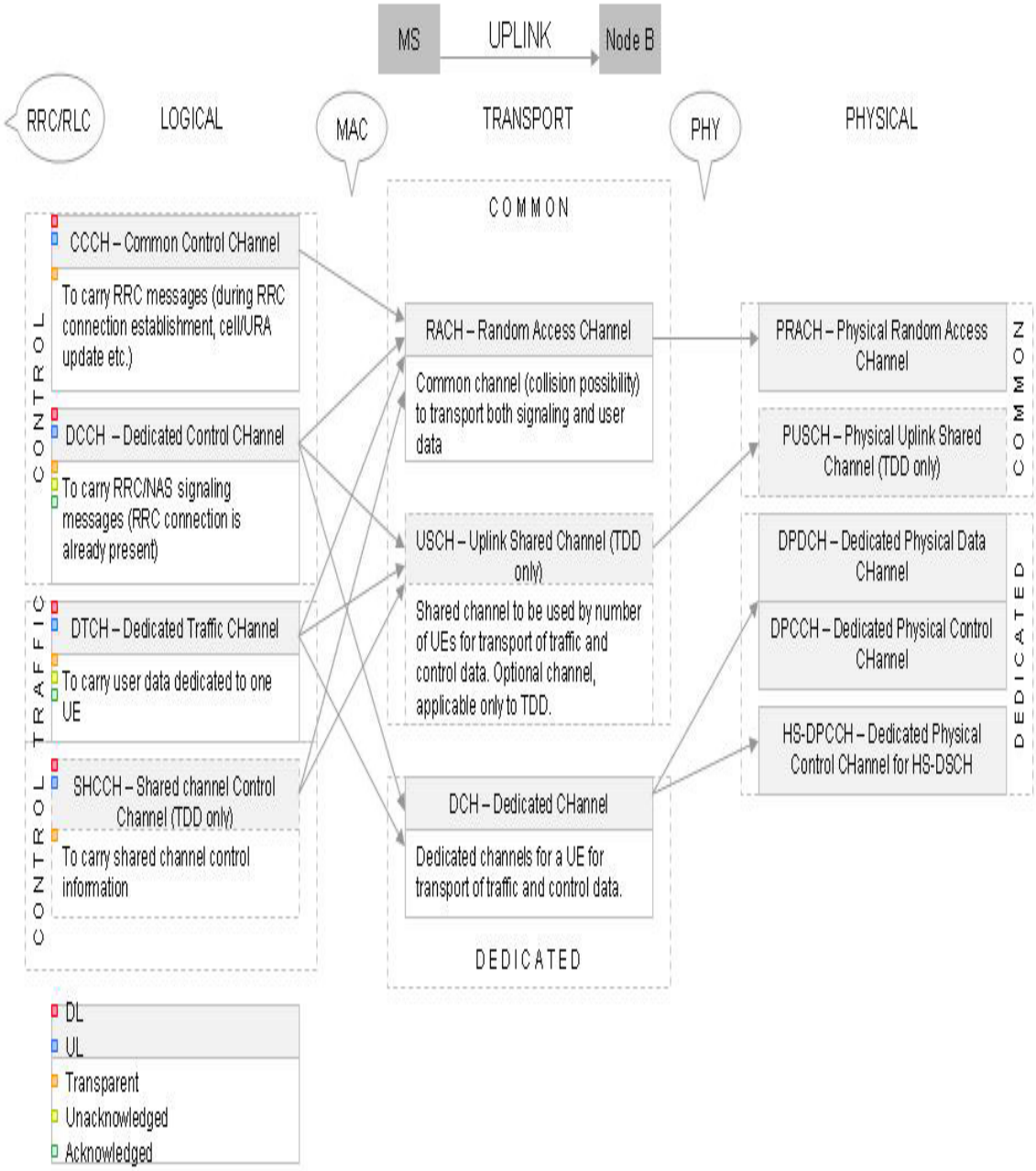

Figure 12: UMTS Uplink Channels

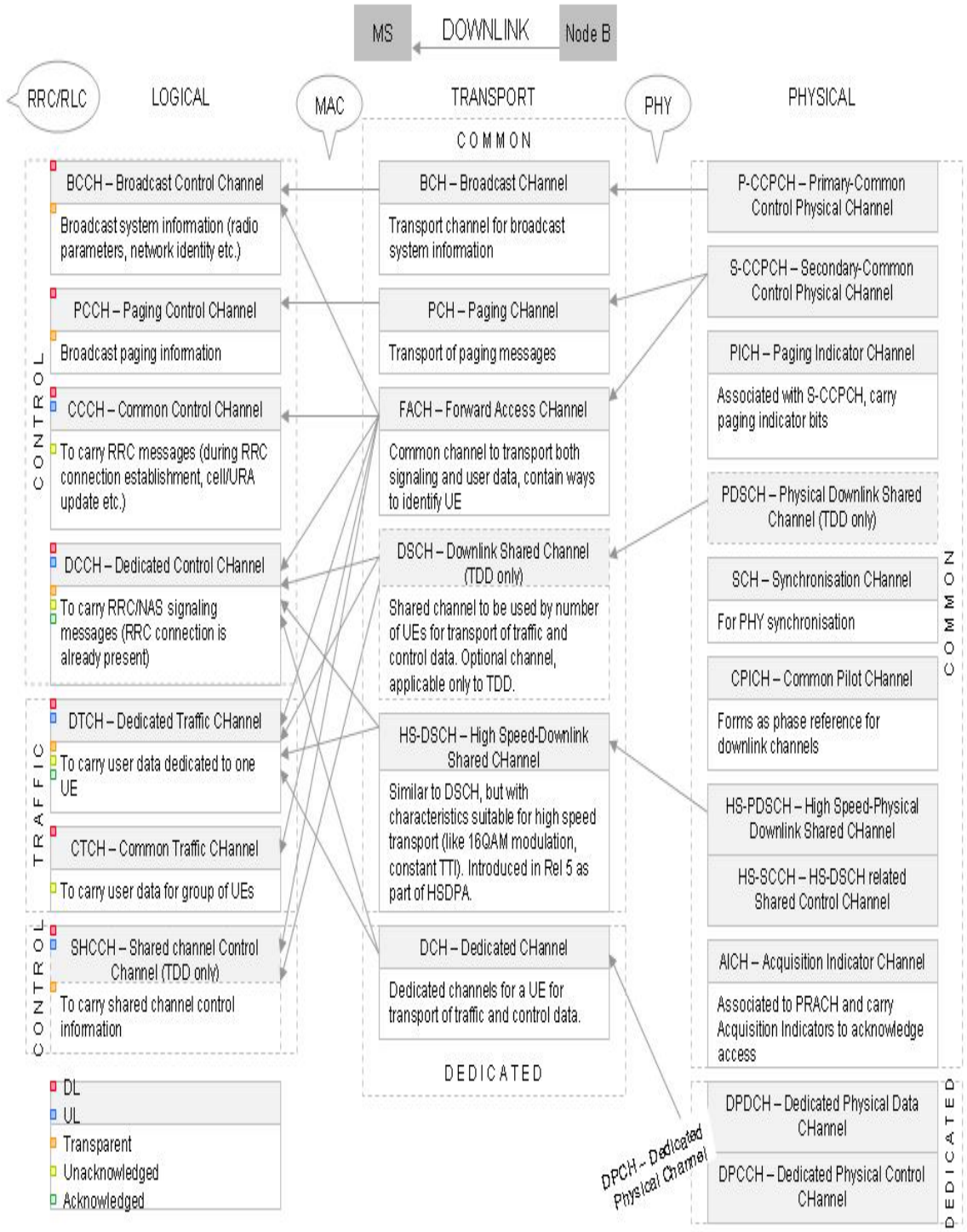

Figure 13: UMTS Downlink Channels

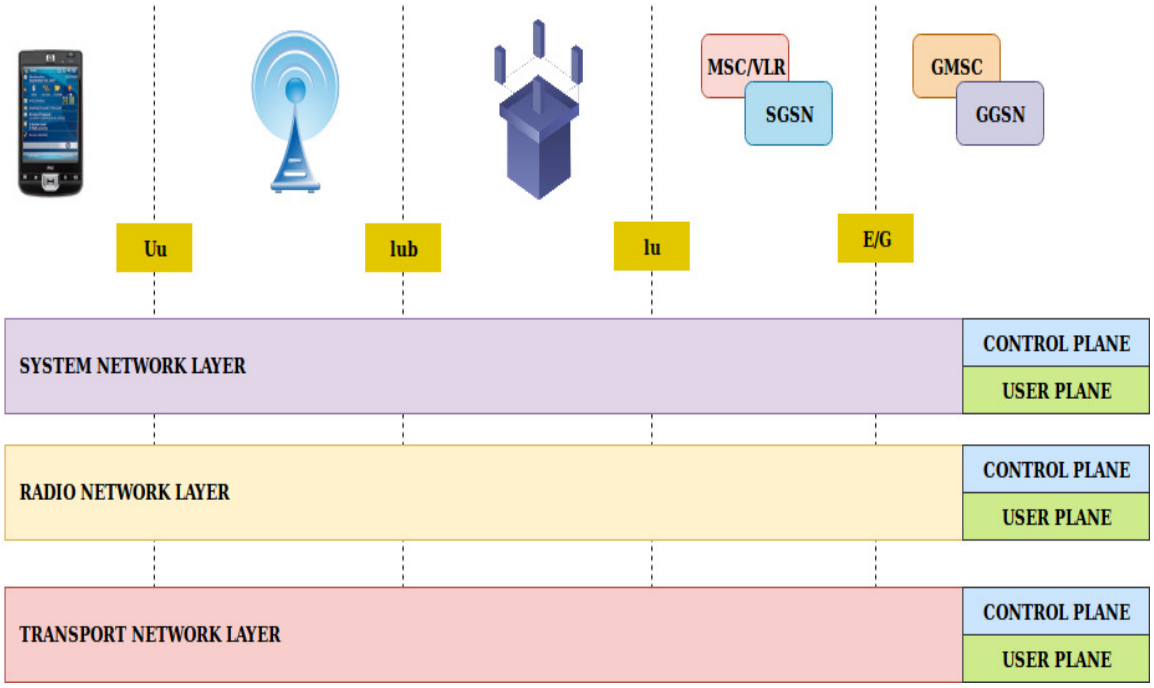

Figure 14: UMTS Network Protocol Architecture

10. UMTS Network Protocol Architecture

- The network protocol architecture for UMTS radio access network (UTRAN) is mainly divided into three layers. Each of the layers is again divided into control planes and user planes. Figure 14 shows the network protocol architecture for UMTS.
- **Transport Network Layer:** It allows communication between UTRAN and Core Network (CN).
- **Radio Network Layer:** Protocols and functions provide management of radio interface and communication between UTRAN components and between UTRAN and UE.
- **System Network Layer:** It allows communication between CN and UE.
- The general protocol model architecture for UMTS is shown in **Figure 15**.
- The structure is based on the principle that the layers and planes are logically independent of each other.
- Therefore, as and when required, the standardization body can easily alter protocol stacks and planes to fit future requirements.
- The Control Plane includes the Application Protocols, i.e., **RANAP (Radio Access Network Application Part), RNSAP (Radio Network Subsystem Application Part or NBAP (Node B Application Part))**, and the Signaling Bearer for transporting the Application Protocol messages.
- Among other things, the Application Protocol is used for setting up bearers (i.e., Radio Access Bearer or Radio Link) in the Radio Network Layer.
- The User Plane includes the data stream(s) and the data bearer(s) for the data stream(s). The data stream is characterized by one or more frame protocols specified for that interface.
- The **Transport Network Control Plane** does not include any radio network layer information, and is completely in the transport layer.
- It includes the ALCAP (Access Link Control Application Protocol) protocols that are needed to set up the transport bearers, i.e., data bearer for the user plane.

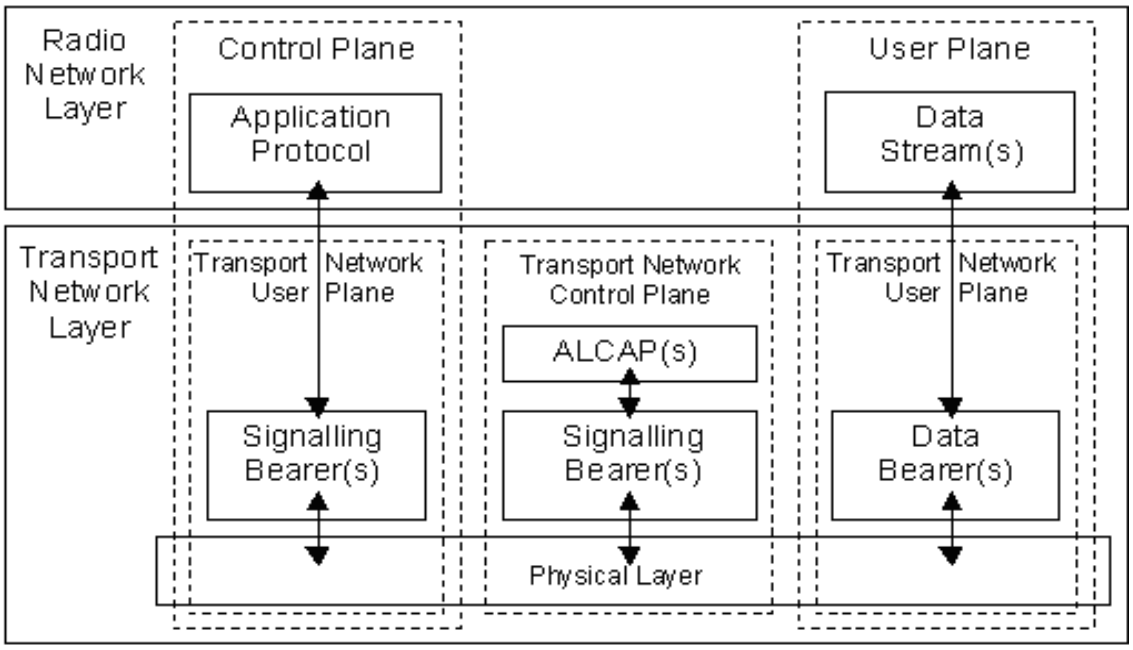

Figure 15: General Protocol Format

- It also includes the appropriate signaling bearer(s) needed for ALCAP protocols.
- The transport network control plane is a plane that acts between the control plane and the user plane.
- The introduction of the transport network control plane is performed in a way that the application protocol in the radio network control plane is kept completely independent of the technology selected for data bearer in the user plane.
- Indeed, the decision to actually use an ALCAP protocol is completely kept within the transport network layer.