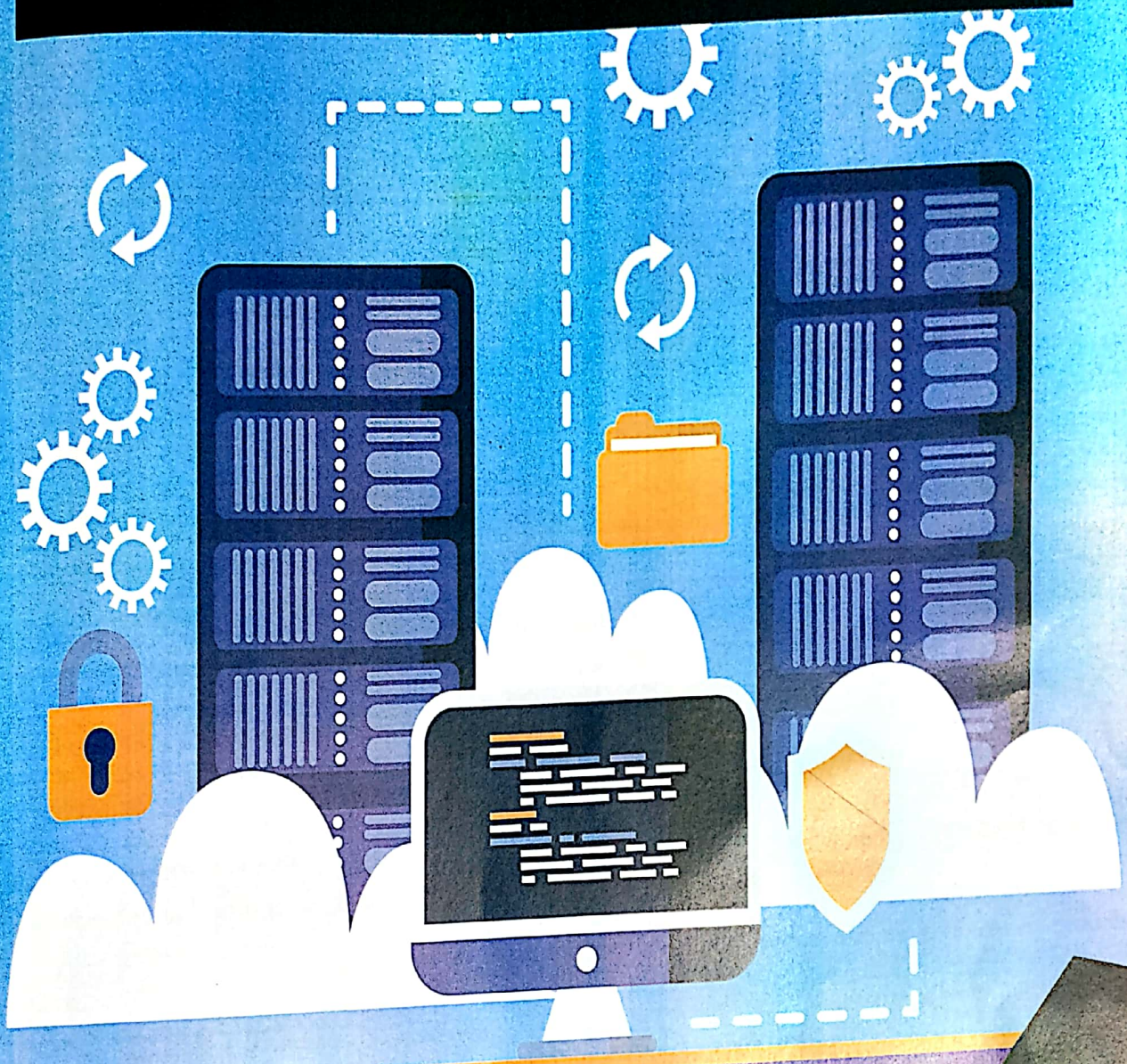
TOPPER'S SOLUTIONS

....In Search of Another Topper



MOBILE COMMUNICATION & COMPUTING

(BE - COMPUTER)

7 SEM

Jul 2019 Edition

As per Revised Syllabus w.e.f 2019-20

Scanned by CamScanner

Syllabus:

Exam	TT-1	TT-2	AVG	Term Work	Oral/Practical	End of Exam	Total
Marks	20	20	20	25	25	80	150

#	Module	Details Contents	No.
1.	Introduction to Mobile Computing	▪ Introduction to Mobile Computing, Telecommunication Generations, Cellular systems, ▪ Electromagnetic Spectrum, Antenna, Signal Propagation, Signal Characteristics, Multiplexing, Spread Spectrum: DSSS & FHSS	01
2.	GSM Mobile services	▪ GSM Mobile services, System Architecture, Radio interface, Protocols , Localization and Calling, Handover, security (A3,A5 & A8) ▪ GPRS system and protocol architecture ▪ UTRAN , UMTS core network ; Improvements on Core Network	15
3.	Mobile Networking	▪ Medium Access Protocol, Internet Protocol and Transport layer ▪ Medium Access Control: Motivation for specialized MAC, , Introduction to multiple Access techniques (MACA) ▪ Mobile IP: IP Packet Delivery, Agent Advertisement and Discovery, Registration, Tunneling and Encapsulation, Reverse Tunneling, Routing (DSDV,DSR) ▪ Mobile TCP: Traditional TCP, Classical TCP Improvements like Indirect TCP, Snooping TCP & Mobile TCP, Fast Retransmit/ Fast Recovery, Transmission/Timeout Freezing, Selective Retransmission ▪	39
4.	Wireless Local Area Networks	▪ Wireless Local Area Networks: Infrastructure and ad-hoc network ▪ IEEE 802.11:System architecture , Protocol architecture , Physical layer, Medium access control layer, MAC management, 802.11a, 802.11b ▪ Wi-Fi security: WEP ,WPA, Wireless LAN Threats , Securing Wireless Networks ▪ HiperLAN 1 & HiperLAN 2 ▪ Bluetooth: Introduction, User Scenario, Architecture, protocol stack.	51
5.	Mobility Management	▪ Mobility Management: Introduction, IP Mobility, Optimization, IPv6 ▪ Macro Mobility: MIPv6, MIPv6 ▪ Micro Mobility: CellularIP, HAWAII, HMIPv6	72
6.	Long-Term Evolution (LTE) of 3GPP	▪ Long-Term Evolution (LTE) of 3GPP : LTE System Overview, Evolution from UMTS to LTE ▪ LTE/SAE Requirements, SAE Architecture ▪ EPS: Evolved Packet System, E-UTRAN, Voice over LTE (VoLTE), Introduction to LTE-Advanced ▪ System Aspects, LTE Higher Protocol Layers, LTE MAC layer, LTE PHY Layer ▪ Self Organizing Network (SON-LTE), SON for Heterogeneous Networks (HetNet), Introduction to 5G	78

Scanned by CamScanner

CHAP - 1: INTRODUCTION TO MOBILE COMPUTING

Q1. What is an antenna? Explain different types of antennae

Ans: [P | Medium]

ANTENNA:

1. An antenna is a transducer that converts **radio frequency (RF)** fields into **alternating current** or vice versa.
2. There are both receiving and transmission antennas for sending or receiving radio transmissions.
3. Antennas play an important role in the operation of all radio equipment.
4. They are used in **wireless local area networks, mobile telephony** and **satellite communication**.
5. Antennas can be Omni-directional, directional or arbitrary.

TYPES OF ANTENNA:

I) Isotropic Antenna:

1. Isotropic Antenna is said to be the type of antenna which radiates equally in all directions.
2. This type of antenna is considered to be ideal antenna.
3. It has a perfect **360 degree** spherical radiation pattern.
4. There is no actual physical isotropic antenna.
5. However, an isotropic antenna is often used as a reference antenna for the antenna gain.
6. The antenna gain is often specified in dBi, or decibels over isotropic.
7. This is the power in the strongest direction divided by the power that would be transmitted by an isotropic antenna emitting the same total power.
8. Figure 1.1 represents radiation pattern of isotropic antenna.

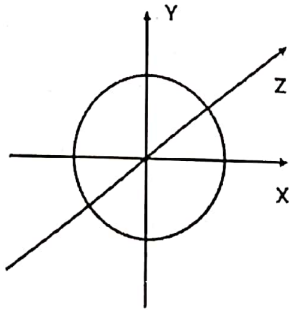


Figure 1.1: Radiation Pattern of Isotropic Antenna.

II) Dipole Antenna:

1. Dipole antenna is also known as **doublet**.
2. It is the simplest and most widely used class of antenna.
3. The dipole is the prototypical antenna on which a large class of antennas are based.
4. A basic dipole antenna consists of two conductors (usually metal rods or wires) arranged symmetrically with one side of the balanced feed line from the transmitter or receiver attached to each.
5. The length of the dipole is half of the wavelength of the signal.
6. **Hertzian dipole** is most commonly used dipole antenna.
7. Figure 1.2 represents Radiation pattern of Hertzian dipole.

Scanned by CamScanner

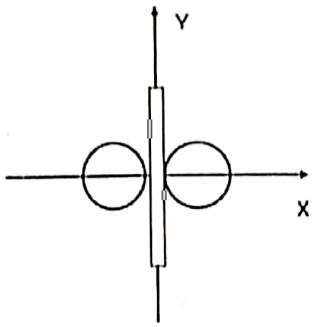


Figure 1.2: Radiation pattern of Hertzian Dipole (side view).

III) Monopole Antenna:

1. A monopole antenna is a class of radio antenna consisting of a straight rod-shaped conductor.
2. It is often mounted perpendicularly over some type of conductive surface, called a **ground plane.**
3. It is also known as **Markoni Antenna**.
4. The length of the monopole is one fourth of the wavelength of the signal.
5. Figure 1.3 represents ideal vertical monopole antenna.

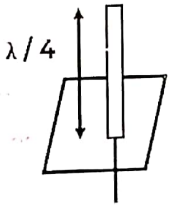


Figure 1.3: Ideal Vertical Monopole Antenna.

IV) Antenna Arrays:

1. Array antennas consist of multiple antennas working as a single antenna.
2. Typically they consist of arrays of identical driven elements, usually dipoles fed in phase, giving increased gain over that of a single dipole.
3. Different diversity schemes are possible.
4. One such scheme is selection diversity, where the receiver always uses the antenna element with the largest output.
5. The other type of diversity is diversity combining, in which a combination of power of all the signals is taken to produce gain.
6. Figure 1.4 represents antenna arrays.

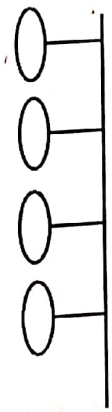


Figure 1.4: Antenna Arrays.

Scanned by CamScanner

V) Loop Antenna:

1. Loop antennas consist of a loop (or coil) of wire.
2. There are essentially two broad categories of loop antennas: big loops and small loop.
3. Loops with circumference of a wavelength are naturally resonant and act somewhat similarly to the half-wave dipole.
4. Figure 1.5 represents Loop Antennas.

Figure 1.5: Loop Antenna.

VI) Aperture antennas:

1. Aperture antennas are the main type of directional antennas used at microwave frequencies and above.
2. They consist of a small dipole or loop feed antenna inside a three-dimensional guiding structure large compared to a wavelength, with an aperture to emit the radio waves.
3. Since the antenna structure itself is non-resonant they can be used over a wide frequency range by replacing or tuning the feed antenna.
4. Figure 1.6 represents aperture antenna.

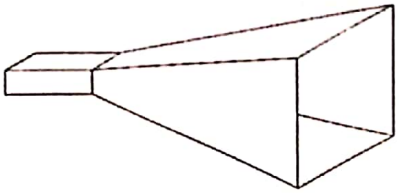


Figure 1.6: Aperture Antenna.

Q2. What is frequency reuse concept in cellular communication?

Ans: **[P | Medium]**

FREQUENCY REUSE IN CELLULAR COMMUNICATION:

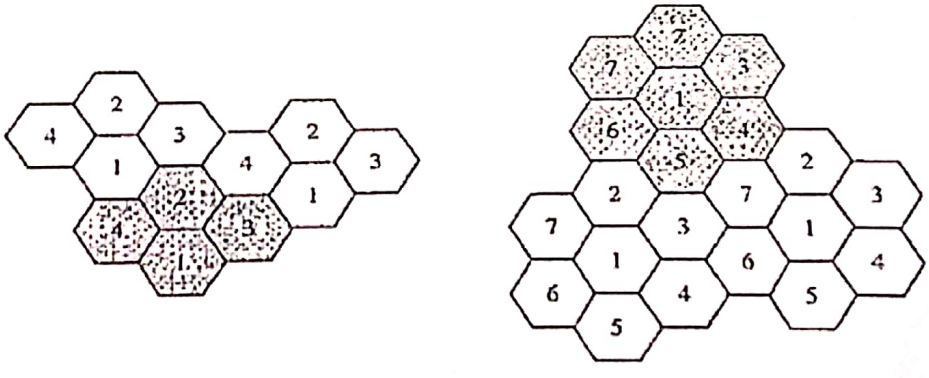


Figure 1.7: Frequency reuse patterns.

Scanned by CamScanner

1. In general, neighboring cells cannot use the same set of frequencies for communication because it may create **interference** for the users located near the cell boundaries.
2. However, the set of frequencies available is limited, and frequencies need to be reused.
3. A frequency reuse pattern is a configuration of N cells, N being the **reuse factor**, in which each cell uses a unique set of frequencies.
4. When the pattern is repeated, the frequencies can be reused.
5. There are several different patterns.
6. Figure 1.7 shows two of them.
7. The numbers in the cells define the **pattern**.
8. The cells with the same number in a pattern can use the same set of frequencies.
9. We call these cells the **reusing cells.**
10. As Figure 1.7 shows, in a pattern with reuse factor 4, only one cell separates the cells using the same set of frequencies.
11. In the pattern with reuse factor 7, two cells separate the reusing cells.
12. So, frequency reuse, or, frequency planning, is a technique of reusing frequencies and channels within a communication system to improve capacity and spectral efficiency.

REUSE DISTANCE:

1. The closest distance between the centers of two cells using the same frequency (in different clusters) is determined by the choice of the cluster size 'C' and the lay-out of the cell cluster.
2. This distance is called the **frequency 'reuse' distance**.

FREQUENCY REUSE OFFERS THE FOLLOWING BENEFITS:

1. Allows communications within cell on a given frequency
2. Limits escaping power to adjacent cells
3. Allows re-use of frequencies in nearby cells
4. Uses same frequency for multiple conversations
5. 10 to 50 frequencies per cell

Q3. Draw and Explain Electromagnetic Spectrum for communication.

Ans: **[P | High]**

ELECTROMAGNETIC SPECTRUM FOR COMMUNICATION:

1. The electromagnetic spectrum is the range of frequencies (the spectrum) of electromagnetic radiation and their respective wavelengths and photon energies.
2. It is nothing but a characteristic distribution of electromagnetic radiation emitted or absorbed by that particular object.
3. When electrons move, they create electromagnetic waves that can propagate through free space.
4. All modern communication depends on manipulating and controlling signals within the electromagnetic spectrum.
5. The electromagnetic spectrum ranges from extremely low-frequency radio waves of 30Hz to high-frequency cosmic rays of more than 10 million trillion Hz.

Scanned by CamScanner

6. The electromagnetic spectrum as demonstrated in Figure 1.1, can be expressed in term of wavelength, frequency, or energy.
7. Wavelength (λ), frequency (ν) are related by the expression: $\lambda = c / \nu$
8. The higher the frequency, the higher the energy.
9. Therefore in communication system, smaller carrier Wavelength represent Higher Bandwidth.

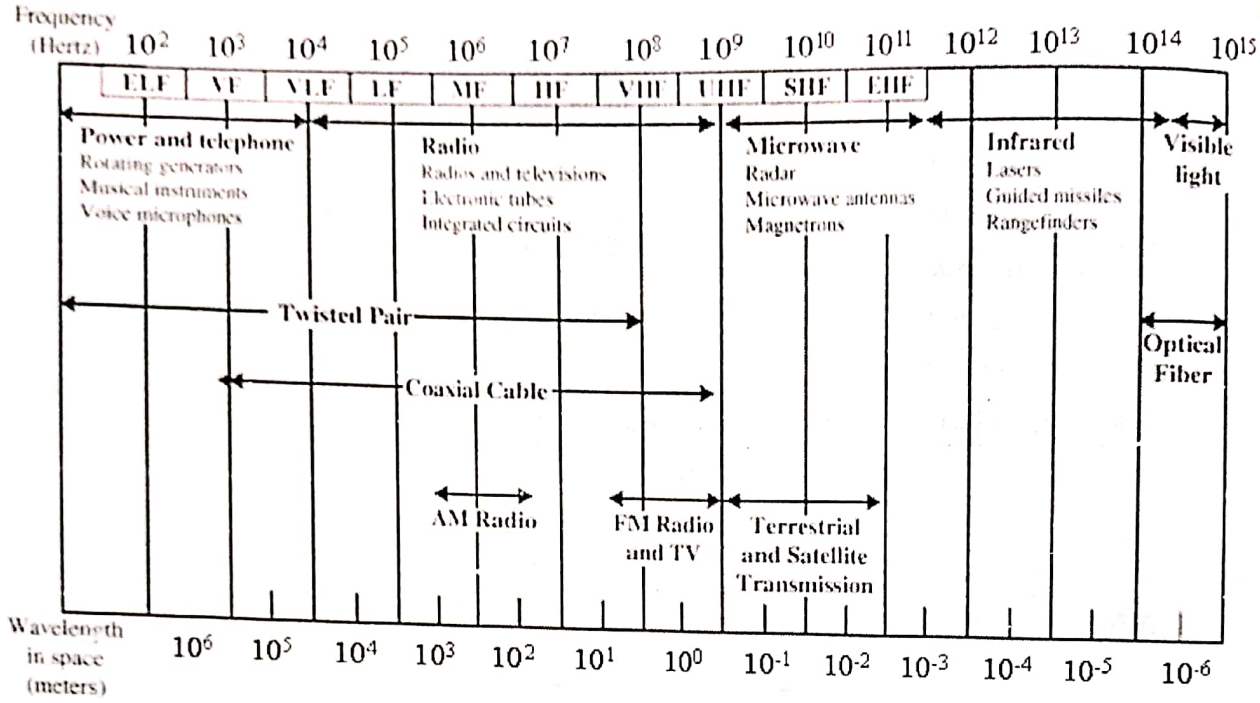


Figure 1.8: Electromagnetic Spectrum for communication.

Band	Full Forms	Frequency Range	Propagation	Uses
ELF	Extremely Low Frequency	30 – 300Hz	Ground	Power line frequencies
LF	Low Frequency	3 – 300 KHz	Ground	Marine Communications, communication over twisted pair
MF	Medium Frequency	300KHz –3MHz	Sky	AM radio, communication over coaxial cables
HF	High Frequency	3 – 30 MHz	Sky	Aircraft and ship communications
VHF	Very High Frequency	30 – 300 MHz	Sky and Line – of - Sight	FM radio, TV
UHF	Ultra High Frequency	300 MHz – 3GHz	Line – of - Sight	TV, cellular phone
SHF	Super High Frequency	3 – 30 GHz	Line – of - Sight	Satellite, microwave links
EHF	Extremely High Frequency	3 – 300GHz	Line – of - Sight	Radar, satellite

Scanned by CamScanner

Infrared	Infrared Rays	300 Ghz – 400THz	Line – of - Sight	Consumer electronic goods
Visible Light	Visible Light rays	400 THz – 900 THz	Line – of - Sight	Fiber optic communications

Q4. Spread Spectrum?

Ans: **[P | Medium]**

SPREAD SPECTRUM:

1. Spread Spectrum is an important form of **encoding for wireless communications**.
2. Spread-spectrum techniques are methods by which a signal generated with a particular bandwidth is deliberately spread in the frequency domain.
3. It results in a signal with a **wider bandwidth**.
4. It involves spreading the bandwidth that is needed to transmit the data.

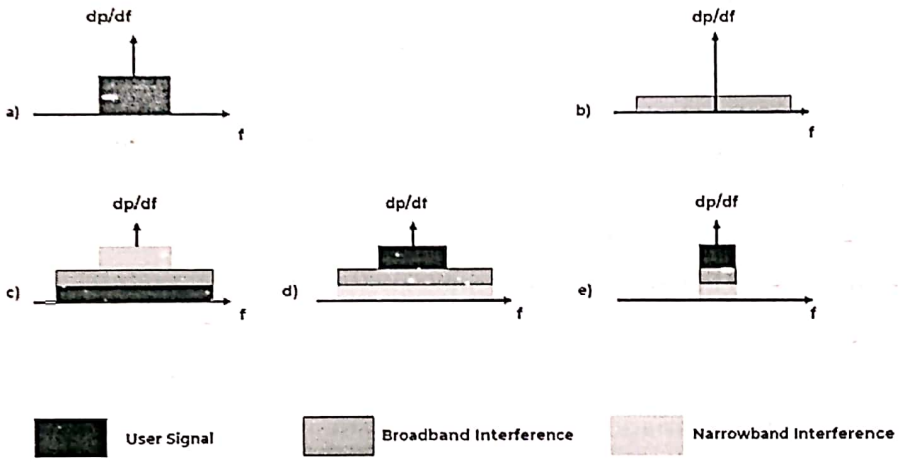


Figure 1.9: Spread Spectrum: Spreading & Despreading.

STEPS:

1. The process of Spreading & Despreading is shown in Figure 1.9.
2. An idealized narrow band signal is transmitted by the sender as shown in Figure 1.9 (a).
3. The narrow band signal is converted into broadband signal i.e. signal is spread as shown in Figure 1.9 (b).
4. The energy need to transmit the signal is still the same.
5. During transmission, narrow band as well as broadband interference gets added to the spread signal as shown in Figure 1.9 (c).
6. The receiver now has to de spread the received signal.
7. The original broadband signal (containing user data) is converted back to a narrowband signal.
8. The narrowband interference that was added is spread whereas the broadband interference is left as it is.
9. The signal is now applied to a band pass filter that cuts off the frequencies to the left and right of the narrowband signal as shown in Figure 1.9 (e).
10. The original user signal can now be recovered.

Scanned by CamScanner

ADVANTAGES:

1. It provides the resistance to narrowband interference.
2. It is used in military application.
3. Cross-talk elimination
4. Better security & Reduction in noise.

DISADVANTAGES:

1. Increased complexity of the sender and receivers.
2. It requires large frequency band.

Q5. Explain DSSS?

Ans: **[P | Medium]**

DSSS:

1. DSSS stands for **Direct Sequence Spread Spectrum.**
2. It is also known as Direct Sequence Code Division Multiple Access (DS-CDMA).
3. It is one of two approaches to spread spectrum modulation for digital signal transmission over the airwaves.
4. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces.
5. Each of which is allocated across to a frequency channel across the spectrum.
6. A data signal at the point of transmission is combined with a higher data-rate bit sequence (also known as a chipping code) that divides the data according to a spreading ratio.
7. The redundant chipping code helps the signal resist interference and also enables the original data to be recovered if data bits are damaged during transmission.
8. Figure 1.10 and 1.11 shows DSSS Transmitter & Receiver.

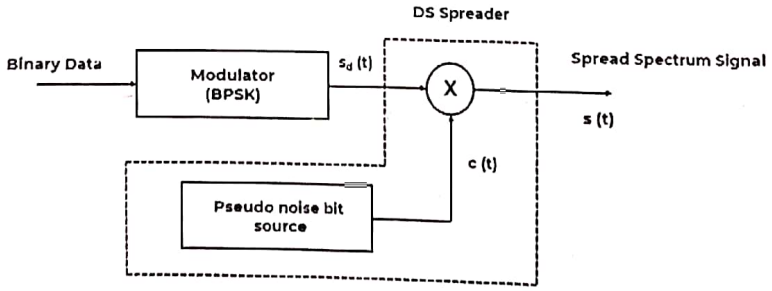


Figure 1.10: DSSS Transmitter

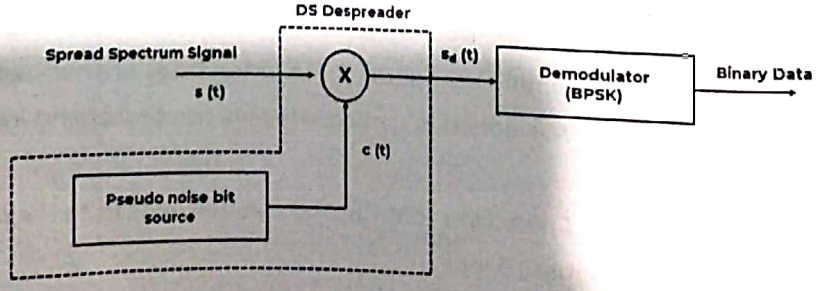
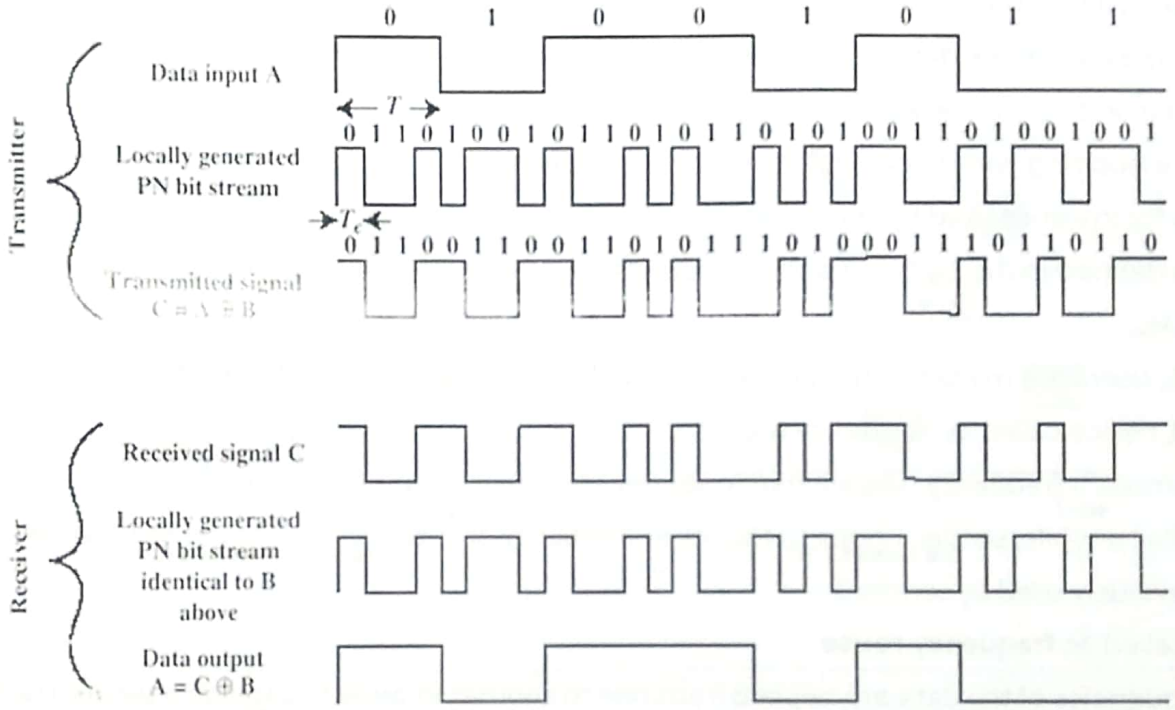


Figure 1.11: DSSS Receiver

Scanned by CamScanner

EXAMPLE:

1. 10 bit spreading code spreads signal across 10 times bandwidth of 1 bit code
2. One method: Combine input with spreading code using XOR
   a. Input bit 1 inverts spreading code bit
   b. Input zero bit doesn't alter spreading code bit.



ADVANTAGE OF DSSS:

1. This system has very high degree of discrimination against the multipath signal. Therefore interference called by multipath reception is minimized successfully.
2. The performance of DSSS system in presence of noise is superior to other system such as FHSS system.
3. This system combats the intentional interference (jamming) most effectively.

DISADVANTAGE OF DSSS:

1. With the serial search system, the acquisition time is too large this makes DSSS system slow.
2. The sequence generated at the PN code generator output must have high rate. The length of such sequence needs to be long enough to make the sequence truly random.
3. The channel bandwidth required is very large, but this bandwidth is less than that of FHSS system.
4. The synchronization is affected by the variable distance between the transmitter and receiver.

Scanned by CamScanner

Q6. Explain FHSS?

Ans: [P | Medium]

FHSS:

1. FHSS stands for **Frequency Hoped Spread Spectrum**.
2. It is a spread spectrum technique used in radio transmission systems.
3. In a FHSS systems the data is sent using a transmission frequency that moves from one frequency to another in a "hop" sequence.
4. Hence, a hopping pattern can be observed in the spectrum.
5. FHSS is for instance used by Bluetooth.
6. FHSS is defined in the 2.4 GHz band and operates in around 79 frequencies ranging from 2.402 GHz to 2.480 GHz.
7. In FHSS, users are made to change the frequencies of usage, from one to another in a specified time interval, hence called as frequency hopping.
8. For example, a frequency was allotted to sender 1 for a particular period of time.
9. Now, after a while, sender 1 hops to the other frequency and sender 2 uses the first frequency, which was previously used by sender 1.
10. This is called as **frequency reuse**.
11. The frequencies of the data are hopped from one to another in order to provide a secure transmission.
12. The amount of time spent on each frequency hop is called as **Dwell Time**.
13. Figure 1.12 and 1.13 shows FHSS Transmitter & Receiver.

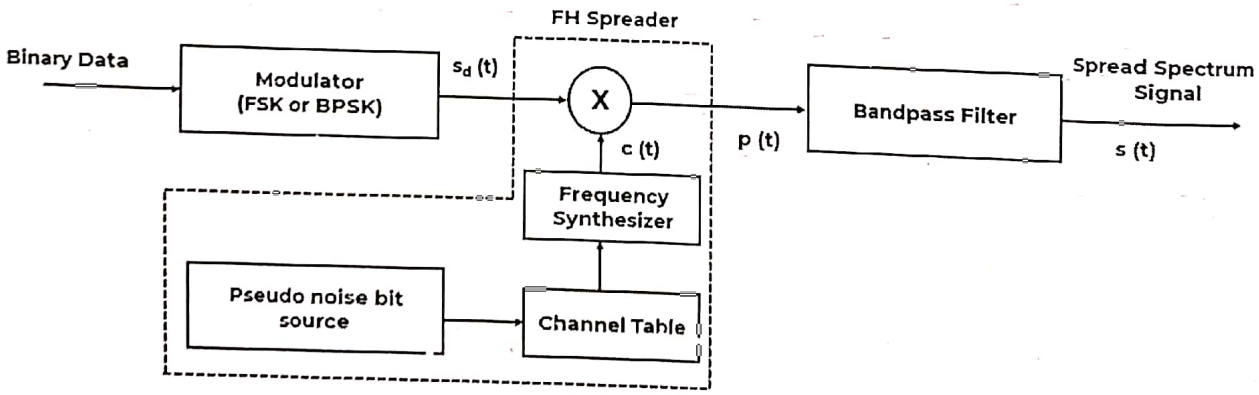


Figure 1.12: FHSS Transmitter

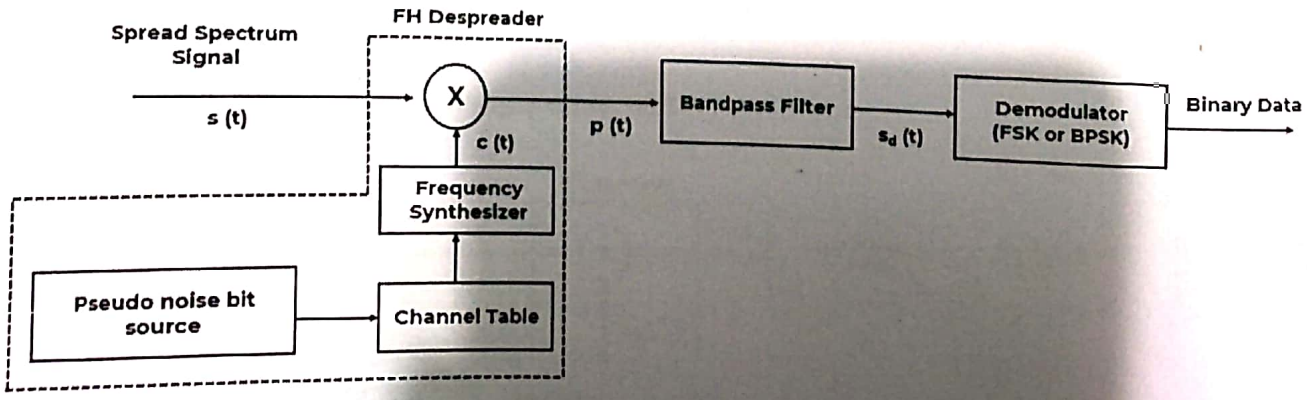
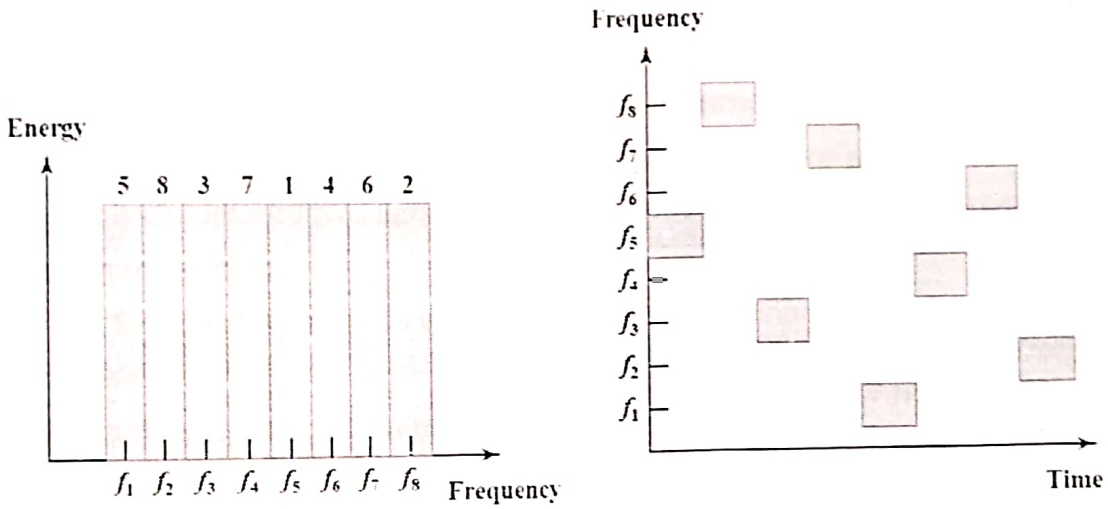


Figure 1.13: FHSS Receiver

Scanned by CamScanner

EXAMPLE:

1. In a frequency-hopping spread spectrum (FHSS) system, the transmitted signal is spread across multiple channels, as shown below.
2. In the example, the full bandwidth is divided into 8 channels, centered at f1 through f8.
3. The signal "hops" between them in the following sequence: f5, f8, f3, f6, f1, f7, f4, f2.



Q7. Compare FHSS & DSSS **[P | Medium]**

Ans:

COMPARISON BETWEEN FHSS AND DSSS/CDMA:

FHSS	DSSS / CDMA
Multiple frequencies are used.	Single frequency is used.
Hard to find the user's frequency at any instant of time.	User frequency, once allotted is always the same.
Frequency reuse is allowed.	Frequency reuse is not allowed.
Sender need not wait.	Sender has to wait if the spectrum is busy.
Power strength of the signal is high.	Power strength of the signal is low.
Stronger and penetrates through the obstacles.	It is weaker compared to FHSS.
It is never affected by interference.	It can be affected by interference.
It is cheaper.	It is expensive.
This is the commonly used technique.	This technique is not frequently used.

Scanned by CamScanner

Q8. Explain in detail 3G architecture [P | Medium]

Ans:

3G:

1. 3G Stands for **Third Generation Cellular Systems**.
2. It is the third generation of wireless mobile telecommunications technology.
3. It satisfies **International Mobile Telecommunications -2000** standard.
4. It is the upgrade for 2G and 2.5G GPRS networks, for faster internet speed.
5. 3G uses **Circuit switching** for voice communication, and **Packet switching** for Data Communication.
6. 3G finds application in wireless voice telephony, mobile internet access, fixed wireless internet access, video calls and mobile TV.

FEATURES:

1. Enhanced audio and video streaming.
2. Videoconferencing support.
3. Web and WAP browsing at higher speeds.
4. The transfer rate for 3G networks is between 128 and 144 kbps (kilobits per second) for devices that are moving fast, and 384 kbps for slow ones.
5. 3G offers greater security features than 2G like Network Access Security, Network Domain Security, User Domain Security and Application Security.

3G ARCHITECTURE:

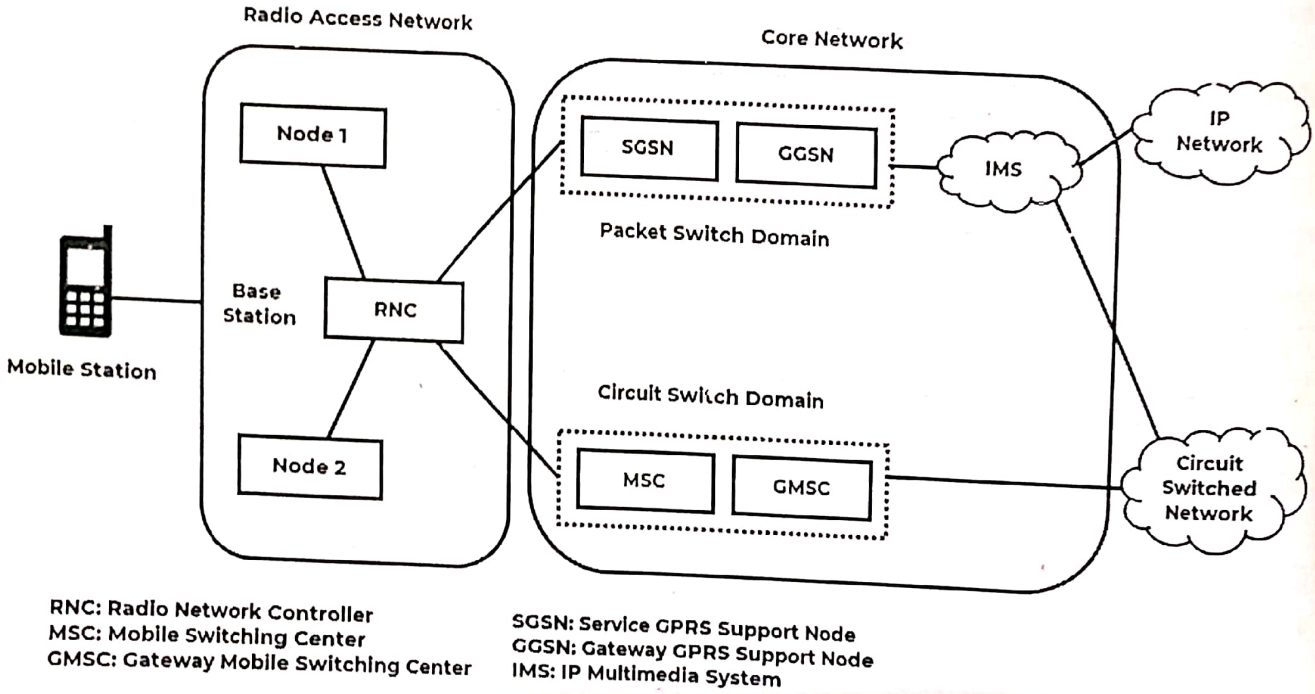


Figure 1.14: 3G Network Architecture Model.

The Constituent parts of 3G UMTS network are:

I) Mobile Station:

1. It could be anything like data and voice-enabled mobile phones, tabs or computers which could be used as an end user.

Scanned by CamScanner

II) **RAN (Radio Access Network):**

1. It consists of base stations and radio access controller which bridges the gap between Mobile Station and Core Network.
2. It also controls and manages the air interface for the whole network.

III) **CN (Core Network):**

1. It provides the main processing and management of subsystems.
2. The 3G UMTS network Architecture is migrated from GSM with some enhancements in core network elements.

The core network is divided into two parts i.e. Circuit Switched Domain and Packet-switched domain.

I) **Circuit Switched Domain:**

1. It uses Circuit Switched Network in which dedicated link or channel is provided for a particular time slot to set of users.
2. The two blocks shown in Circuit Switched Domain are:
   a. **MSC:** Mobile Switching Centre manages circuit switched calls.
   b. **GMSC:** Gateway MSC acts as an interface between external and internal networks.

II) **Packet-switched Domain:**

1. It uses IP Network where IP's are responsible for transmitting and receiving data between two or more devices.
2. The two blocks shown in Packet Switched Domain are:
   a. **SGSN (Serving GPRS Support Node):** The various functions provided by SGSN are mobility management, session management, billing, interaction with other areas of the network.
   b. **GGSN (Gateway GPRS Support Node):** It can be considered as a very complex router and handles the internal operations between the external packet switched networks and UMTS packet switched network.

IMS (IP Multimedia Subsystem): It is an Architectural framework which delivers IP multimedia services.

ADVANTAGES OF 3G:

1. It uses 2G frequency bands with bandwidths up to 230MHz are used to achieve global roaming and multi-services.
2. Wideband radio channel to support high-speed services.
3. Radio carrier channel uses bandwidth up to 20M which improvises chip rate and anti-multipath fading.
4. To improve the performance of the **downlink transmission** channel, fast closed loop power control technology is applied.

Scanned by CamScanner

Q9. Explain in detail 4G Architecture. [P | Medium]

Ans:

4G:

1. 4G Stands for **Fourth Generation Cellular Systems**.
2. 4G is the evolution of 3G to meet the forecasted rising demand.
3. It is an integration of various existing technologies including GSM, GPRS, CDMA one, IMT-2000 and Wireless LANs.
4. Data rates in 4G systems will range from **20 to 100 Mbps**.

FEATURES:

1. Fully IP Based Mobile System.
2. It supports interactive multimedia, voice, streaming video, internet and other broadband services.
3. It has better spectral efficiency.
4. It supports **Adhoc and multi hop networks**.

4G ARCHITECTURE:

1. Figure 1.16 shows the 4G Generic Mobile Communication Architecture.
2. As shown in figure 4.6, the 4G Network is an integration of all heterogeneous wireless access network such as Adhoc, cellular, hotspot and satellite radio component.
3. Technologies Used in 4G are Smart Antennas for multiple - input and multiple - output (MIMO), IPv6, VoIP, OFDM and Software Defined Radio (SDR) System.

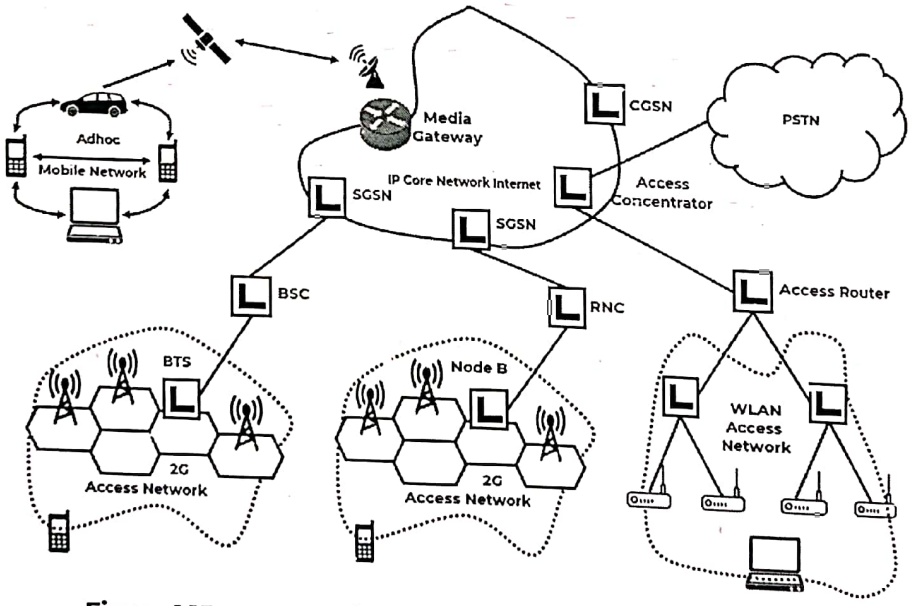


Figure 1.15: 4G Generic Mobile Communication Architecture.

Smart Antennas:

1. Smart Antennas are Transmitting & receiving antennas.
2. It does not require increase power or additional frequency.

IPv6 Technology:

1. 4G uses IPv6 Technology in order to support a large number of wireless enabled devices.
2. It enables a number of applications with better multicast, security and route optimization capabilities.

Scanned by CamScanner

VoIP:

1. It stands for **Voice over IP**.
2. It allows only packets (IP) to be transferred eliminating complexity of 2 protocols over the same circuit.

OFDM:

1. OFDM Stands for **Orthogonal Frequency Division Multiplexing**.
2. It is currently used as WiMax and WiFi.

SDR:

1. SDR Stands for **Software Defined Radio**.
2. It is the form of open wireless architecture.

Advantages:

1. It provides better spectral efficiency.
2. It has high speed, high capacity and low cost per bit.

Disadvantages:

1. Battery usage is more.
2. Hard to implement.

Scanned by CamScanner

CHAP - 2: GSM MOBILE SERVICES

Q1. Explain GPRS architecture in detail

Ans: [P | Medium

GPRS:

1. GPRS Stands for **General Packet Radio System/Service**.
2. GPRS Standard was defined by **European Telecommunications Standards Institute (ETSI)** in 1994.
3. GPRS is a **packet oriented mobile data service** on the 2G & 3G cellular communication systems.
4. It reuses the existing **GSM infrastructure** to provide end to end switched services.

FEATURES:

1. GPRS is an overlay network over GSM.
2. It provides data packet delivery service.
3. It supports leading internet communication protocols.
4. It has high data speed rate of 14.4 – 115 kbps.

GPRS ARCHITECTURE:

Figure 2.1 shows simplified GPRS Network Architecture.

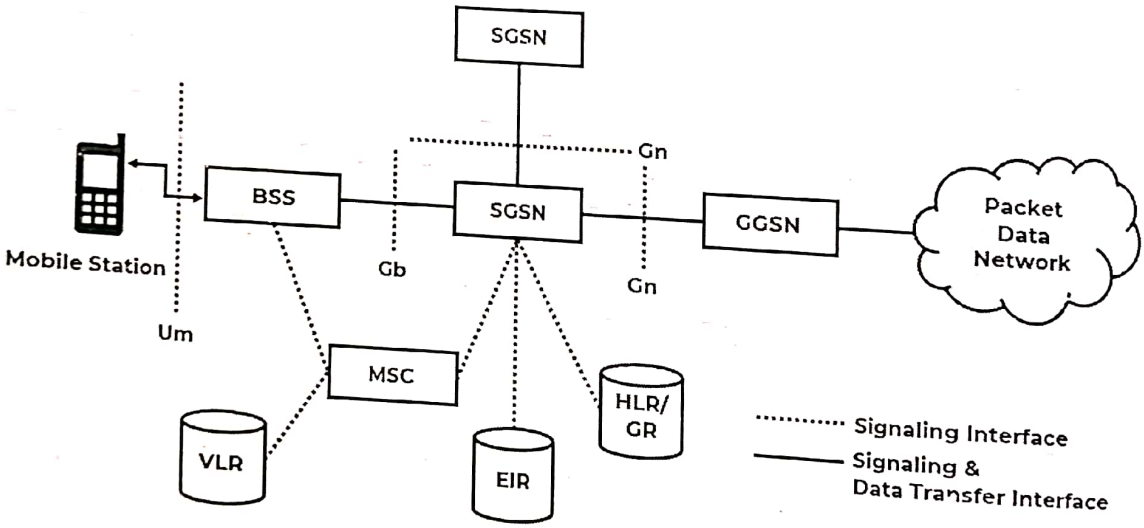


Figure 2.1: GPRS Network Architecture.

GPRS architecture includes:

I) SGSN:

1. SGSN stands for **Serving GPRS Support Node**.
2. It is equivalent to MSC of the GSM network.
3. It supports the Mobile Station (Ms) via the Gb interface.
4. There must be at least one SGSN in a GPRS network.
5. It has following functions:
   a. Data compression.
   b. User authentication.
   c. Mobility management.
   d. Protocol conversation.

Scanned by CamScanner

II) GGSN:

1. GGSN stands for **Gateway GPRS Support Node**.
2. It is the gateway to external networks.
3. It is consider as the internetworking unit between the GPRS network and external Packet Data Network (PDN).
4. This node contains routing information for GPRS user.
5. It connects to external networks via Gi interface and transfers packet to the SGSN via Gn interface.

III) Mobile Station (MS):

1. A GPRS MS consists of **Mobile Terminal** (MT) and **Terminal Equipment** (TE).
2. An MT communicates with the BSS over the air.
3. A TE can be a computer attached to the MT.

IV) BSS:

1. BSS Stands for **Base Station System**.
2. The BSS should manage GPRS-related radio resources such as allocation of packet data traffic channels in cells.

V) HLR:

1. HLR Stands for **Home Location Register**.
2. To accommodate GPRS subscription and routing information, new fields in the MS record are introduced in HLR, which are accessed by SGSN and GGSN using the IMSI as the index key.

VI) Mobile Switching Center/Visitor Location Register (MSC/VLR):

1. In MSC/VLR, a new filed SGSN number is added to indicate the SGSN currently serving the MS.
2. The MSC/VLR may contact SGSN to request location information or paging for voice calls.

Q2. Explain GSM in detail?

Ans: **[P | Medium]**

GSM:

1. GSM Stands for **Global System for Mobile Communication**.
2. It is the most successful mobile communication system in the world and it is used by over 3 billion people in more than 210 countries.
3. More than 75% of all digital mobile phones use GSM.
4. The specifications for GSM are provided by the European Telecommunications Standard Institute (ETSI)
5. It is typically 2G System designed to replace 1G Analog System.

GSM CHARACTERISTICS:

1. Mobile Wireless Communication is possible in GSM.
2. It supports both voice and data services.
3. **International access:** Chip card enables use of access points of different providers.
4. **Worldwide localization:** The same number can be used worldwide.
5. Provides authentication via chip card and PIN.

Scanned by CamScanner

GSM ARCHITECTURE:

GSM has complex hierarchical architecture consisting of many entities, interfaces and acronyms. It has 3 main subsystems a shown in figure 2.2.

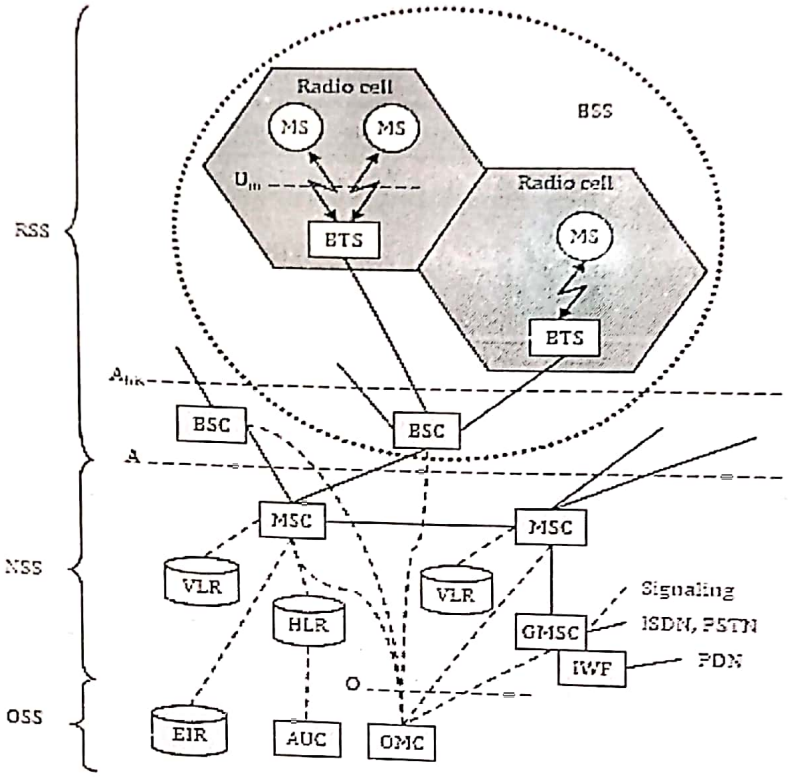


Figure 2.2: GSM System Architecture.

RADIO SUB-SYSTEM (RSS):

1. It comprises of cellular mobile network up to the switching centers.
2. The various components of RSS are as follows:

I) Base Station Subsystem (BSS):

1. GSM network comprises of many BSSs.
2. Each BSS contains several BTSs.
3. Each BSS is controlled by a Base Station Controller (BSC)
4. **Functions:**
   a. Coding/Decoding of voice.
   b. Maintain necessary connections to MS.

II) Base Transceiver Station (BTS):

1. BTS comprises of all the radio equipment's such as Antenna, Digital Signal Processor and Amplifiers.
2. It operates in the region called CELL.
3. **Functions:**
   a. Transcoding and rate adaption.
   b. Time and frequency synchronizing.

III) Base Station Controller (BSC):

1. It is used to manage the BTSs.
2. The main function is to multiplex radio channels onto fixed network connections at the interface.

Scanned by CamScanner

3. **Functions:**
   a. Control of frequency hopping.
   b. Power management.

IV) Mobile Station (MS):

1. It comprise of all the hardware and software required by a user to communicate with the GSM network and access its services.
2. It has User Equipment which is transmitter receiver unit.
3. It has as Subscriber Identity Module (SIM) to store all the user specific data.

NETWORK AND SWITCHING SUBSYSTEM (NSS):

1. It is the main component of GSM Architecture.
2. It is responsible for switching, mobility management, and interconnection to the other networks, system control, charging and accounting.
3. It consists of following components:

I) Mobile Service Switching Center (MSC):

1. MSC are basically high performance ISDN switches.
2. A single MSC manages several BSCs in a particular area.
3. **Functions:**
   a. Handover management & Billing.
   b. Location registration.
   c. Synchronizing the BSS.

II) Gateway MSC (GMSC):

1. It has additional connections to fixed networks like PSTN and ISDN.
2. Using additional Interworking Functions, MSC can also connect to Public Data Networks such as X.25.

III) Home Location Register (HLR):

1. It is the central master database containing user data, permanent and semi-permanent data of all subscribers assigned to HLR.
2. It supports charging and accounting.
3. It comprises of following information:
   a. Mobile Subscriber ISDN number.
   b. International Mobile Subscriber Identity.
   c. Current location area.
   d. Mobile Subscriber Roaming number (MSRN).

IV) Visitor Location Register (VLR):

1. Each MSC has a corresponding VLR.
2. It stores all the important information about users who are currently in the location area corresponding to the MSC.
3. This information includes IMSI number, MSISDN, the HLR address etc.

Scanned by CamScanner

2. OSS accesses other entities via signaling.
3. It has following components:

I) Authentication Center (AuC):

1. It is responsible for protection of user identity and data over air interface.
2. It contains the algorithm for **authentication (A3)** as well as the keys for encryption (Kc).

II) Operation and Maintenance (OMC):

It is responsible for various functions like:

1. Traffic monitoring.
2. Subscriber and security management.
3. Status report of network entities.
4. Accounting and billing.

III) Equipment Identity Register (EIR):

1. It contains **IMEI** of all the user equipment's.
2. With the help of IMEI number, stolen or malfunctioning mobile stations can be locked and sometimes even localized.
3. Thus EIR contains the following lists.
   a. A black list containing IMEI of stolen/ locked devices.
   b. A white list containing IMEI of valid devices.
   c. A grey list containing IMEI of malfunctioning devices.

Q3. Compare GSM and GPRS? **[P | Medium]**

Ans:

GSM ARCHITECTURE VS GPRS ARCHITECTURE:

Table 1.1: GSM v/s GPRS

Points	GSM Architecture	GPRS Architecture
Type of Connection	Circuit Switched Technology.	Packet Switched Technology.
Data Rates	9.6 Kbps.	14.4 to 115.2 Kbps
TDMA	It uses 1 out of 7 Time Slots.	It uses 4 + 1 Time Slots.
Billing	Based on Duration of Connection	Based on Amount of Data Transferred.
Paging Channel	No required.	Required to control bursty traffic.
Area Concept	Location Area Concept is used.	Routing Area Concept is Used.

Scanned by CamScanner

Q4. What are the modifications required to an existing GSM network to be upgraded to GPRS, Explain with the help of diagram.

Ans: **[P | Medium]**

GSM NETWORK:

1. GSM Stands for **Global System for Mobile**.
2. GSM is a standard developed by the **European Telecommunications Standards Institute (ETSI)**.
3. It is used to describe the protocols for **second-generation (2G)** digital cellular networks used by mobile phones.
4. The main goal of GSM was to provide voice services that are compatible to ISDN and other PSTN systems.

GPRS NETWORK:

1. GPRS Stands for **General Packet Radio System**.
2. GPRS Standard was defined by **European Telecommunications Standards Institute (ETSI)** in 1994.
3. GPRS is a **packet oriented mobile data service** on the 2G & 3G cellular communication systems.
4. It reuses the existing **GSM infrastructure** to provide end to end switched services.

Modifications required to an existing GSM network to be upgraded to GPRS:

GSM NETWORK TO BE UPGRADED TO GPRS ARCHITECTURE:

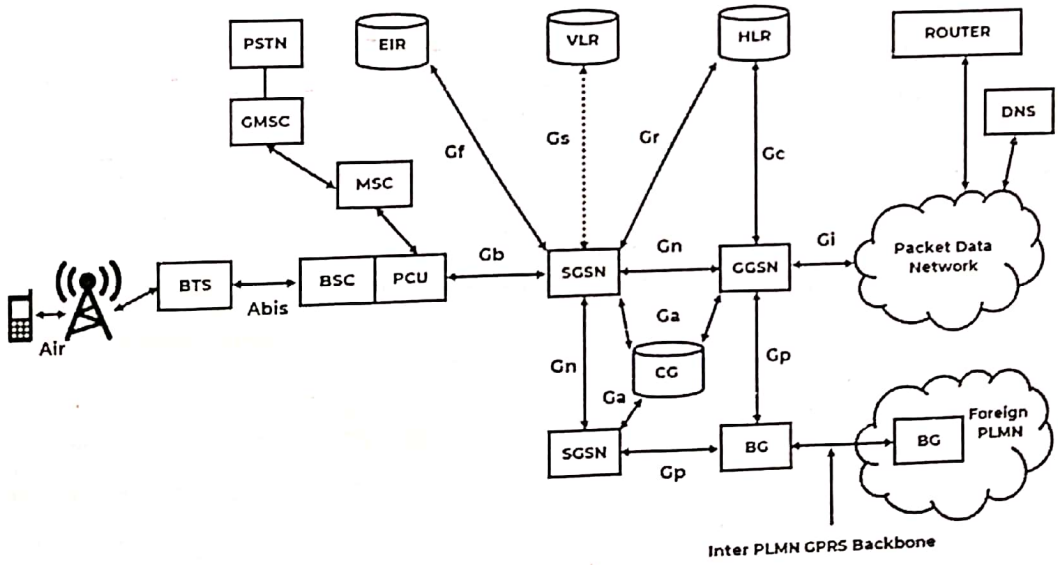


Figure 2.3: GSM Network to be upgraded to GPRS Architecture.

1. As shown in Figure 2.3, the existing GSM Nodes are upgraded with GPRS functionality.
2. GSM Network only provides **Circuit Switched Services**.
3. Therefore to upgrade to GPRS Network, two new network nodes were defined to support **Packet Switched Services**.
4. They are **Gateway GPRS Support Node (GGSN)** & **Serving GPRS Support Node (SSGN)**.
5. GPRS uses GSM's **Base Station System** (BSS) but with enhanced functionality to support GPRS.
6. BSS is now used for both Circuit Switched & Packet Switched Network element to ensure backward compatibility.

Scanned by CamScanner

7. Additional **Packet Control Unit (PCU)** has been added to BSC to segregate voice and data packets
8. Circuit switched data are send to 'A' interface on the MSC and Packet switched data are sent to the SGSN into the GPRS backbone as shown in Figure 2.3.
9. The **Base Station Controller** (BSC) of GSM is given new functionality for Mobile Management for handling GPRS paging.
10. The new **traffic and signaling interface** form the SGSN is now terminated in the BSC.
11. Therefore to upgrade to GPRS, the existing GSM network requires all above components such as GGSN, SGSN, PCU, BSC, HLR.

Q5. Explain the data rate enhancement with the help of GPRS network model. What is the maximum data rate obtained by GPRS network? [P] | Medium

Ans:

GPRS:

1. GPRS Stands for **General Packet Radio System/Service.**
2. GPRS Standard was defined by **European Telecommunications Standards Institute (ETSI)** in 1994.
3. GPRS is a **packet oriented mobile data service** on the 2G & 3G cellular communication systems.
4. It reuses the existing **GSM infrastructure** to provide end to end switched services.

FEATURES:

1. GPRS is an overlay network over GSM.
2. It provides data packet delivery service.
3. It supports leading internet communication protocols.

DATA RATE IN GPRS:

1. GPRS uses unused time slots of GSM system to transmit packet data.
2. GPRS can allocate **one to eight time slots** within a **TDMA frame**.
3. Allocation of time slots is an on demand basis instead of fixed and predetermined.
4. This allocation depends on current network load and the operator preference.
5. Depending upon the coding, the transfer rate up to **171.2 kbits/s** is possible.
6. GPRS operators offer a minimum of one time slot per cell to ensure at least minimum data rate.
7. Charging in GPRS is based on the volume of data exchanged and not on the connection.
8. The available user data rate depends upon the **coding scheme** and the number of TDMA time slots allocated.
9. *Table 1.2 lists* the data rates available in GPRS.

Table 1.2: GPRS Data Rates

Coding Scheme	*1 Slot*	*2 Slots*	*3 Slots*	*4 Slots*	*5 Slots*	*6 Slots*	*7 Slots*	*8 Slots*
CS-1	9.05	18.1	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

Scanned by CamScanner

Q6. Explain GSM Frame Hierarchy.

Q7. Explain in short Time slot hierarchy of GSM System.

Ans: [P | High]

GSM TIME HIERARCHY:

1. **GSM Time Hierarchy** is also known as **GSM Frame Hierarchy**.
2. In GSM, frequency band of 25 MHz is divided into 200 KHz of smaller bands.
3. Each carry one RF carrier, this gives **125 carriers**.
4. Out of 125 carriers, one carrier is used as **guard channel** between GSM and other frequency bands and other 124 carriers are useful RF channels.
5. This division of frequency pool is called **FDMA**.
6. Now each RF carrier will have 8 time slots.
7. This time wise division is called **TDMA**.
8. Here each RF carrier frequency is shared between **8 users**.
9. Hence in GSM system, the basic radio resource is a time slot with duration of about **577 µs**.
10. This time slot carries 156.25 bits which leads to bit rate of **270.833 kbps**.
11. This is explained below in TDMA GSM frame structure.
12. The GSM frame structure is designated as hyperframe, superframe, multiframe and frame.
13. One GSM hyperframe composed of 2048 superframes.
14. Each GSM superframe composed of multiframes (either 26 or 51 as described below in Figure 2.2).
15. Each GSM multiframe composed of frames (either 51 or 26 based on multiframe type).
16. Each frame composed of **8 time slots**.
17. Hence there will be total of **2715648 TDMA frames** available in GSM and the same cycle continues.
18. As shown in the Figure 2.4 below, there are two variants to multiframe structure.

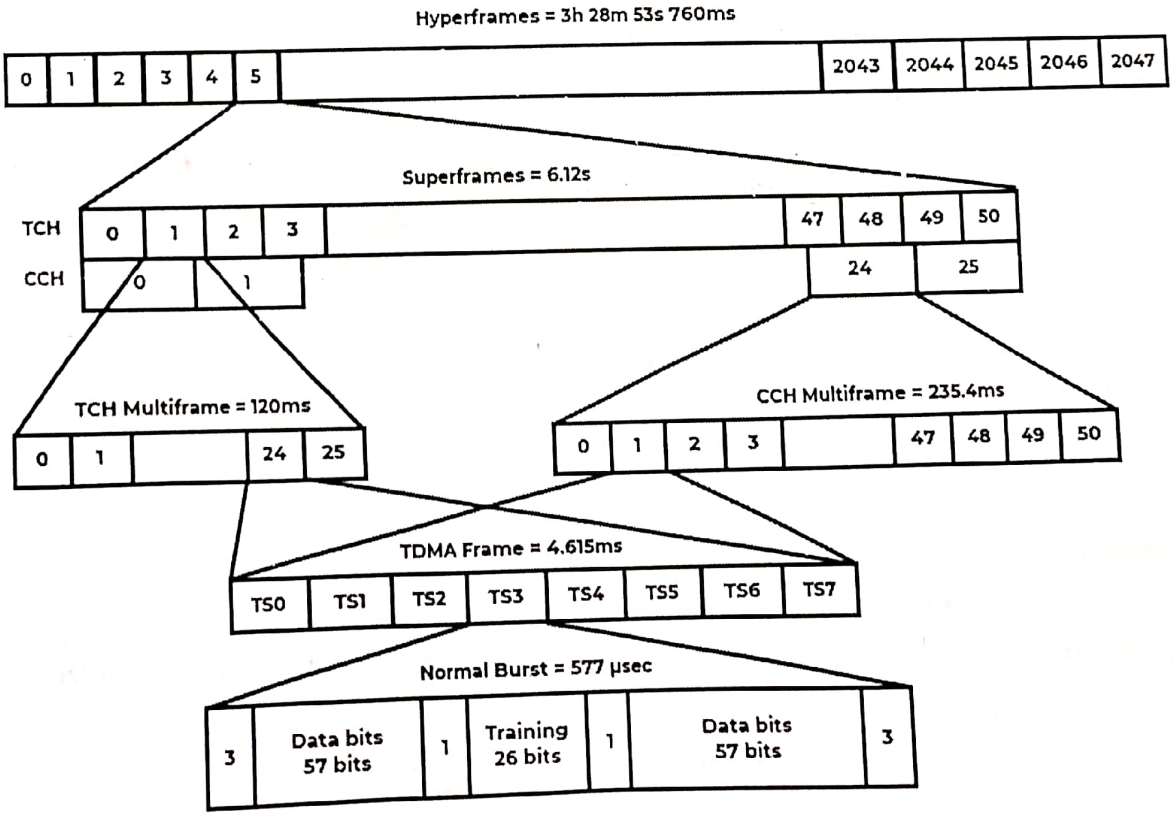


Figure 2.4: GSM Time (or Frame) Hierarchy.

Scanned by CamScanner

I) 26 Frame Multiframe:

1. It is called as **Traffic Multiframe**.
2. It composed of 26 bursts in a duration of 120ms, out of these 24 are used for traffic, one for SACCH and one is not used.

II) 51 Frame Multiframe:

1. It is called as **Control Multiframe**.
2. It composed of 51 bursts in a duration of 235.4 ms.
3. This type of multiframe is divided into logical channels.
4. These logical channels are time scheduled by BTS.

Q8. Privacy and Authentication in GSM.

Q9. Explain in detail how Subscriber Authentication is done in GSM.

Ans: **[P | Medium]**

GSM:

1. GSM Stands for **Global System for Mobile**.
2. GSM is a standard developed by the **European Telecommunications Standards Institute (ETSI)**.
3. It is used to describe the protocols for **second-generation (2G)** digital cellular networks used by mobile phones.
4. The main goal of GSM was to provide voice services that are compatible to ISDN and other PSTN systems.

PRIVACY IN GSM:

1. GSM is the most secured cellular telecommunications system available today.
2. GSM has its **security methods standardized**.
3. It maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.
4. GSM offers the following security services:
   - **I) Access Control and Authentication:**
     a. This includes the user authentication.
     b. User must enter a secret PIN number to access SIM.
     c. It is also responsible for subscriber authentication.
   - **II) Confidentially:**
     a. In this the entire user related data is **encrypted**.
     b. This confidentially exists only between MS and BTS.
   - **III) Anonymity:**
     a. Anonymity is provided to the user by encrypting all the data before the transmission.
     b. Along with the encryption the GSM uses Temporary Identifiers such as **TMSI and MSRN**.
5. GSM uses three algorithms to provide security services:
   a. Algorithm A3 is used for **Authentication**.
   b. Algorithm A5 is used for **Encryption**.
   c. Algorithm A8 is used for **Generation of a cipher key**.

Scanned by CamScanner

AUTHENTICATION IN GSM:

1. Before accessing any GSM service the user must be **authenticated**.
2. The authentication process is based on SIM and it uses a **challenge response method**.
3. SIM stores the **Authentication Key K_i, User Identification Number IMSI** and **Authentication Algorithm A3**.

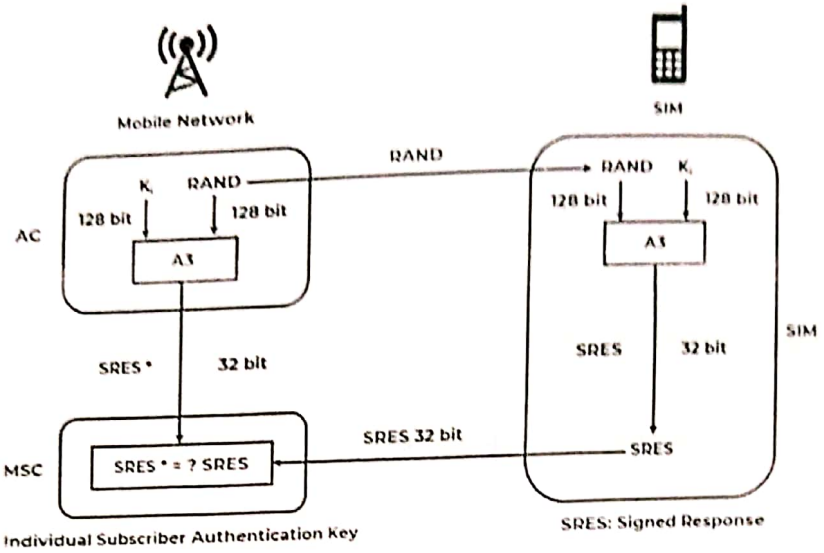


Figure 2.5: Authentication in GSM.

Authentication involves:

1. Figure 2.5 shows the Authentication process in GSM.
2. The Access Control (AC) generates a 128 bit Random Number (RAND) as a challenge.
3. VLR sends RAND to the SIM.
4. SIM now calculates a Signed Response (SRES) from RAND and Authentication key Ki by applying authentication algorithm A3.
5. Similarly, the access control also calculates a Signed Response called SRES*
6. MSC now compares the values SRES and SRES*.
7. It the values are same the subscriber is accepted else rejected.

ENCRYPTION IN GSM:

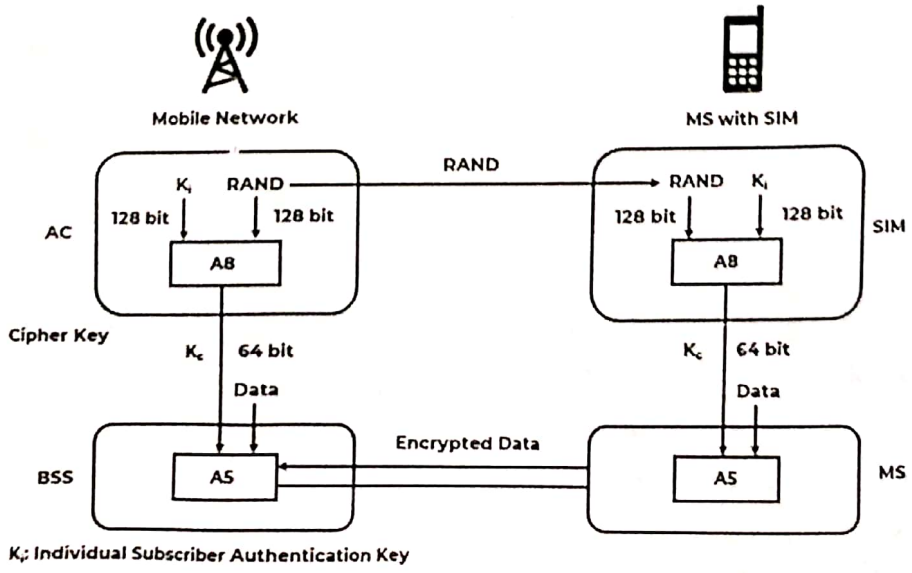


Figure 2.6: Encryption in GSM.

Scanned by CamScanner

1. Once authentication is done MS and BTS can start using Encryption.
2. Figure 2.6 shows the Encryption Process in GSM.

Encryption involves following steps:

a. SIM and Access Control generates Cipher Key K_c from authentication key Ki and a 128 bit random number (RAND) by applying the algorithm A8.
b. MS and BTS can now Encrypt and Decrypt the data using this 64 bit cipher key (K_c) and the Encryption algorithm A5.
c. The 64 bit K_c is just enough to provide to provide protection against simple eavesdropping and is not very strong.
d. Also in certain implementations it so happens that 10 of the 64 bits are always set to 0, thus the real length of the key now is only 54.
e. This makes the **encryption much weaker.**

Q10. Explain various types of handoffs in GSM network. **[P | Medium]**

Ans:

HANDOFFS/ HANDOVER IN GSM NETWORK:

1. Both **Handover** and **Handoff** is used to describe the same process.
2. GSM systems require a procedure known as a Handover to maintain the **continuity of the call**.
3. This is because a single cell does not cover the whole service area e.g. a whole city or country.
4. Therefore Handover/Handoff basically means changing the point of connection while communicating.
5. The number of handovers to be performed depends on two factors:
   a. **Cell Size:** The smaller is the size of cell more the handovers required.
   b. **Speed of MS:** Higher the speed of MS more handovers are required.

TYPES OF HANDOFFS/HANDOVER:

There are four basic types of handoffs in GSM network:

I) Intra-cell Handover:

1. This handover takes place **within a cell**.
2. Such a kind of handover is performed to optimize the traffic load in the cell or to improve quality of a connection by changing carrier frequency.
3. Figure 2.7 shows the Intra-cell Handover.

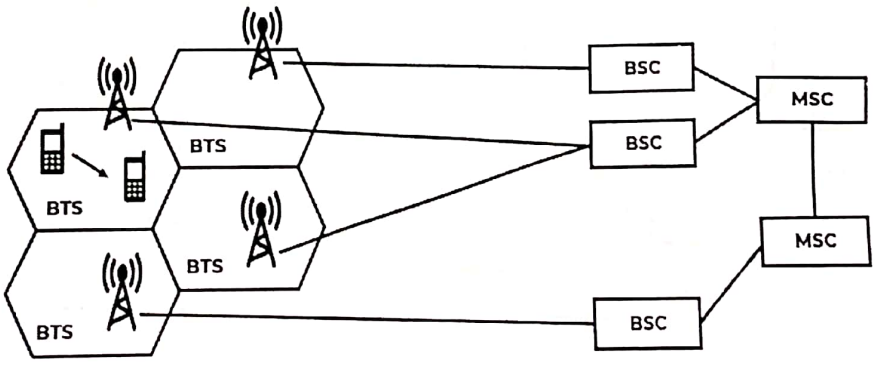


Figure 2.7: Intra Cell Handover.

Scanned by CamScanner

II) Inter-cell Handover:

1. It is also known as **Intra-BSC Handover**.
2. This type of handover is performed when a mobile station moves from one cell to another but remains within the same BSC (Base station controller).
3. Here the BSC handles the handover process.
4. Figure 2.8 shows the Inter-cell Handover.

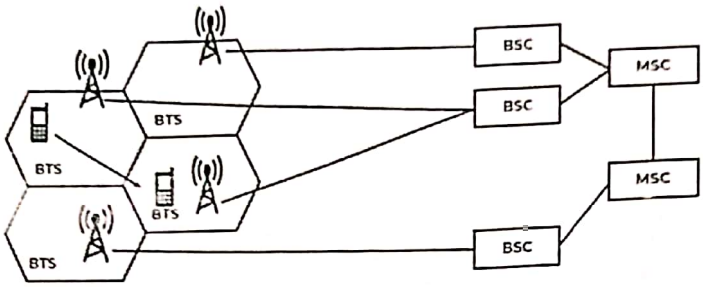


Figure 2.8 Inter Cell Handover.

III) Inter-BSC Handover:

1. It is also called as **Intra-MSC Handover**.
2. This handover takes place between two cells managed by different BSCs.
3. As BSC can control only a limited number of cells, we might usually need to transfer a mobile from one BSC to another BSC.
4. Here the MSC handles the handover process.
5. Figure 2.9 shows the Inter-cell Handover.

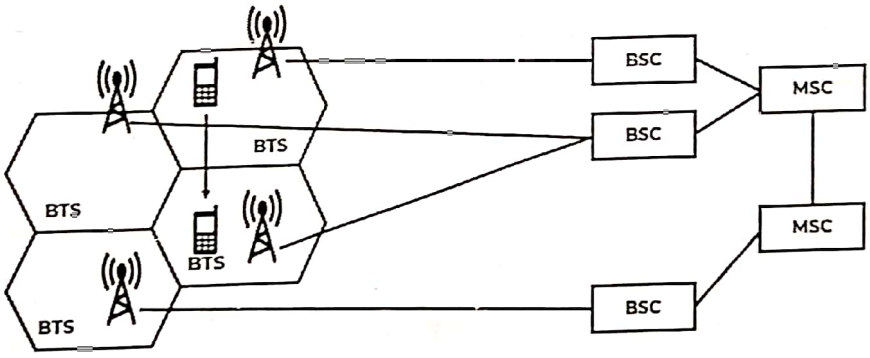


Figure 2.9: Inter BSC Handover.

IV) Inter-MSC Handover:

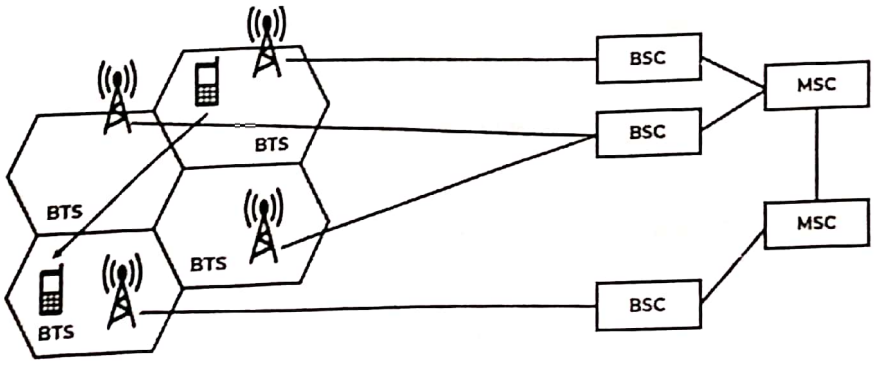


Figure 2.10: Inter MSC Handover.

Scanned by CamScanner

1. It occurs when a mobile moves from one MSC region to another MSC.
2. MSC cover a large area.
3. It can be imagined as a handover from Gujarat MSC to Maharashtra MSC while travelling.
4. Figure 2.10 shows the Inter-cell Handover.

Q11. Explain different types of Interface in GSM? [P | Lo

Ans:

GSM INTERFACE:

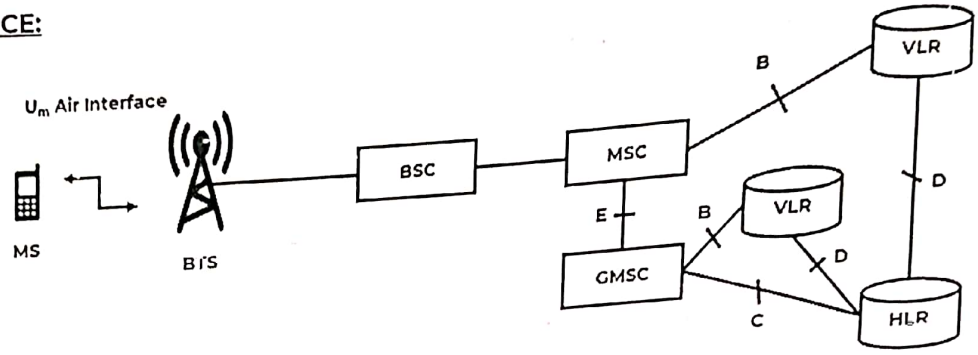


Figure 2.11: GSM Interfaces.

I) U_m Interface:

1. U_m Interface is the **Air Interface of the GSM Mobile Telephone Standard**.
2. It is the interface between the Mobile Station (MS) and the Base Transceiver Station (BTS).
3. It is called Um because it is the mobile analog to the U interface of ISDN.
4. The GSM Air Interface uses the Time Division Multiple Access (TDMA) technique to transmit and receive traffic and signaling information between the GSM's BTS and the GSM Mobile Station.
5. The TDMA technique is used to divide each carrier into 8 time slots.
6. These time slots are then assigned to specific users, allowing up to eight conversations to be handled simultaneously by the same carrier.
7. The international telecommunication union (ITU) which manages the allocation of radio spectrums has allocated the following bands for GSM Um Interface:
   a. **Uplink:** 890-915 MHz (Mobile station to Base station)
   b. **Downlink:** 935-960 MHz (Base station to mobile station)

II) B Interface:

1. B Interface is also known as **Internal Interface**.
2. B Interface Exist between the MSC and the VLR.
3. It uses a protocol known as the **MAP/B Protocol**.
4. This interface is used whenever the MSC needs to communicate with the VLR in order to access data regarding an MS located in its area.

III) C Interface:

1. C Interface Exist between the HLR and the GMSC.
2. It uses a protocol known as **MAP/C Protocol**.
3. It is used to provide communication between the HLR & the GMSC.

Scanned by CamScanner

IV) D Interface:

1. The VLR & the HLR communicates via D Interface.
2. It uses a protocol known as **MAP/D Protocol**.
3. The information related to the location of MS is exchanged between the VLR and HLR over this interface.

V) E Interface:

1. This Interface is used to provide communication between two MSCs.
2. It uses a protocol known as **MAP/E Protocol**.

Q12. Explain how Mobile originated call (MOC) work.

Ans: **[P | Medium]**

MOBILE ORIGINATED CALL (MOC):

1. Initially, the user enters the called number and presses the call key.
2. Then the MS establishes a signaling connection to the BSS on a radio channel.
3. This may involve **authentication and ciphering**.
4. Once this has been established the call setup procedures will take place according to the sequence show in the Figure 2.12.

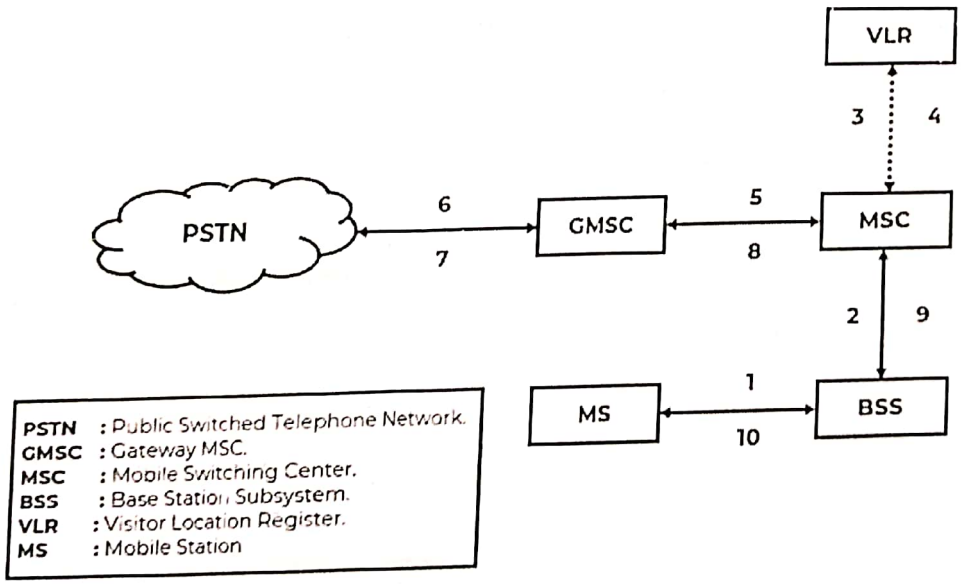


Figure 2.12: Mobile Originated Call (MOC)

Working:

1. The MS sends the dialed number indicating service requested to the MSC (via BSS) as shown in step 1 & 2.
2. Then MSC checks from the VLR if the MS is allowed for the requested service as shown in step 3 & 4.
3. If so, MSC asks the BSS to allocate necessary resource for the call.
4. If the call is allowed, the MSC routes the call to the **GMSC (Gateway MSC)** as shown in step 5.
5. The GMSC routes the call to the local exchange of called user via **public switched telephone network** (PSTN) as shown in step 6.
6. The PSTN alert (applies ringing) the called **terminal**.
7. Answer back (ring back tone) from the called terminal to PSTN.

Scanned by CamScanner

8 Answer back signal is routed back to the MS through the serving MSC which also completes the speech path to the MS as shown in step 7, 8, 9 and10.

Q13. Explain Mobile call termination in GSM

Ans:

[P | Medium]

MOBILE TERMINATED CALL (MTC):

1. Initially the user dials the mobile number.
2. It reaches the PSTN where it is identified as a GSM call as shown in step 1.
3. Then GSM forwards it to the gateway MSC i.e. GMSC as shown in step 2.
4. The GMSC identifies the HLR for the subscriber and signals the call set-up to the HLR as shown in step 3.
5. The HLR then checks if the number is a valid number and whether that user has subscribed to this particular service.
6. If so then an **MSRN (Mobile Subscriber Roaming Number)** is requested from the subscriber's current VLR as shown in step 4.
7. After receiving the MSRN, the HLR determines the MSC responsible for the mobile station as shown in step 5.
8. Then HLR sends this informatio.. to the GMSC as shown in step 6.
9. The GMSC then forwards the call setup request to the concerned MSC as shown in step 7.
10. MSC requests the current status of Mobile Station from VLR as shown in step 8 & 9.
11. If the MS is available then the MSC initiates paging in all cells as shown in step 10.
12. The BTSs of all BSSs transmit this paging signal to the MS as shown in step 11.
13. The MS answers as shown in step 12 & 13.
14. If any response is found by any BTS, the VLR performs a **security check** (encryption etc.) as shown in step 14 & 15.
15. The VLR then asks the MSC to connect to the MS as shown in step 16 & 17.
16. Finally connection is setup.
17. Figure 2.13 represents the working of Mobile Terminated Call.

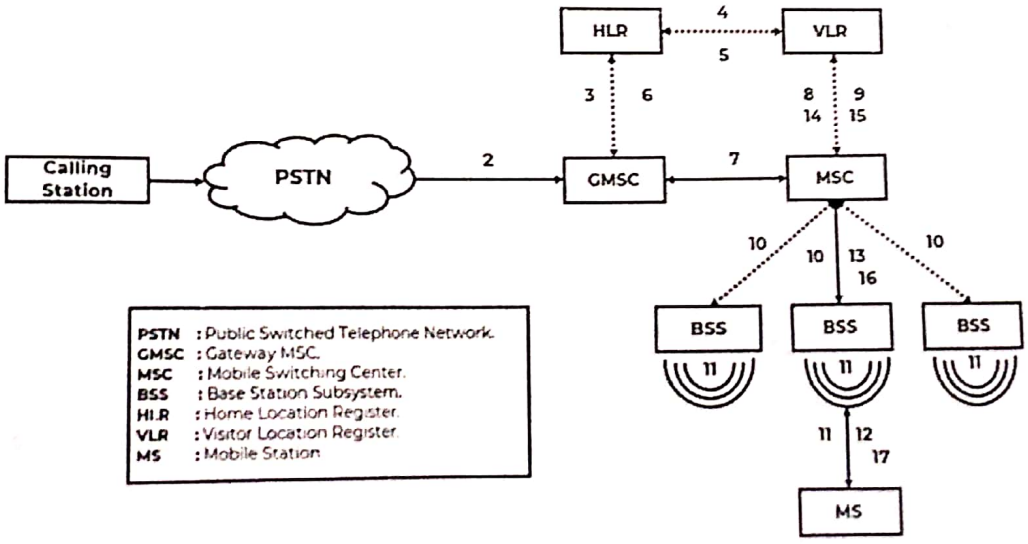


Figure 2.13: Mobile Terminated Call (MTC)

Scanned by CamScanner

Q14. Explain MSRN, IMSI & TMSI [P | Medium]

Ans:

MSRN:

1. MSRN stands for **Mobile Station Roaming Number**.
2. It is a telephone number used to route telephone calls in a mobile network from a GMSC to the target MSC.
3. It can also be defined as a **directory number** temporarily assigned to a mobile for a mobile terminated call.
4. A MSRN is assigned for every mobile terminated call.
5. MSRN is used to **hide the identity of the subscriber** during the course of the call.

IMSI:

1. IMSI stands for **International Mobile Subscriber Identity**.
2. GSM uses the IMSI for **Internal Unique Identification** of a subscriber.
3. IMSI consists of a Mobile Country Code, Mobile Network Code & Mobile Subscriber Identification Number.
4. It is used for acquiring other details of the mobile in the home location register (HLR) or as locally copied in the visitor location register.

TMSI:

1. TMSI stands for **Temporary Mobile Subscriber Identity.**
2. It is a temporary identification number that is used in the GSM network instead of the IMSI to ensure the privacy of the mobile subscriber.
3. The TMSI prohibits tracing of the identity of a mobile subscriber by interception of the traffic on the radio link.
4. The TMSI is assigned to a mobile subscriber by the **Authentication Centre** (AUC) for the duration that the subscriber is in the service area of the associated Mobile Switching Centre (MSC).
5. MS identifies itself by the Temporary Mobile Subscriber Identity (TMSI).

Q15. Explain how Mobile Terminated Call works detailing the role of HLR and VLR. [P | Medium]

Ans:

ROLE OF HLR IN MOBILE TERMINATED CALL SETUP:

1. The HLR basically acts just as a **parent guide** towards a MS.
2. GMSC contacts the HLR for the MS Location.
3. HLR sends Mobile Subscriber Roaming Number (MSRN) to GMSC.

ROLE OF VLR IN MOBILE TERMINATED CALL SETUP:

1. The VLR basically acts as a **central point of contact** for the MSC.
2. It is also responsible for the authentication of a MS once it has been located by the MSC.
3. The VLR provides MSRN to HLR.
4. The VLR also contains other parameters with respect to a MS like Location area Code (LAC) and TMSI.

Scanned by CamScanner

Q16. What is the relationship between the Base Station and Mobile Switching Centre? Discuss the role of EIR entity of GSM network.

[P | Medium]

Ans:

RELATIONSHIP BETWEEN THE BASE STATION AND MOBILE SWITCHING CENTRE:

1. Cellular telephony is designed to provide communications between two moving units, called mobile stations (MSs), or between one mobile unit and one stationary unit, often called a land unit.
2. A service provider must be able to locate and track a caller, assign a channel to the call, and transfer the channel from base station to base station as the caller moves out of range.
3. To make this tracking possible, each cellular service area is divided into small regions called **cells**.
4. Each cell contains an antenna and is controlled by a solar or AC powered network station, called the **base station (BS)**.
5. Each base station, in turn, is controlled by a switching office called as **mobile switching center (MSC)**.
6. The MSC coordinates communication between all the base stations and the telephone central office.
7. It is a computerized center that is responsible for connecting calls, recording call information, and billing as shown in figure 2.14.

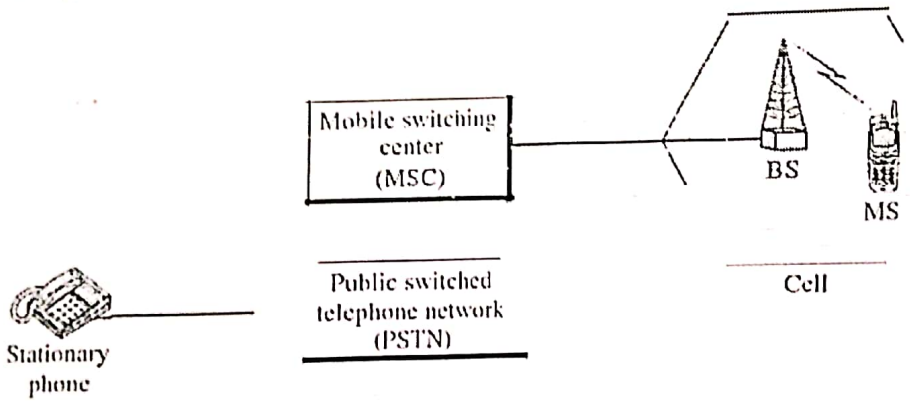


Figure 2.14: Cellular System.

8. Cell size is not fixed and can be increased or decreased depending on the population of the area.
9. The typical radius of a cell is 1 to 12 mi.

EQUIPMENT IDENTITY REGISTER (EIR):

1. It contains IMEI of all the user equipment's.
2. With the help of IMEI number, stolen or malfunctioning mobile stations can be locked and sometimes even localized.
3. Thus EIR contains the following lists.
   a. A black list containing IMEI of stolen/ locked devices.
   b. A white list containing IMEI of valid devices.
   c. A grey list containing IMEI of malfunctioning devices.

Scanned by CamScanner

Q17. Looking at the HLR/VLR database used in GSM how does this architecture limit the scalability in terms of users, especially moving users? Explain the control channels of GSM.

[P | Medium]

Ans:

1. GSM uses only **two levels of hierarchy**.
2. The network operators store all user related information in the HLR.
3. All information related to visitors within a certain location area is stored in a VLR.
4. Capacities of HLRs is up to several million customers.
5. Capacities of VLRs is up to a million i.e. within the location area a maximum of example one million users can be active (registered).
6. If many users move between location areas updates have to take place, i.e., the HLR always gets the information about the new VLR.
7. These updates happen independently on the user's activity (data transmission, calls etc.).
8. For standard scenarios – most users stay most of the time within their location area.
9. In such scenarios, the 2-level hierarchy works well.
10. However, if, example, many tourists move frequently then the updating process puts some load on the network as the HLR in the home network of the tourists always requires update information – probably around the globe.
11. More levels of hierarchy could improve scalability but also raises complexity.

CONTROL CHANNELS OF GSM:

1. Control channels are communication channels used in a system (such as a radio control channel), which are dedicated to the sending and/or receiving of command messages between devices (such as a base station and a mobile radio).
2. On the GSM system, the control channel sends messages that include paging (alerting), access control (channel assignment) and system broadcast information (access parameters and system identification).
3. Many different control channels are used in GSM to control medium access, allocating of traffic channels or mobility management.
4. Figure 2.15 represents hierarchy of control channels.

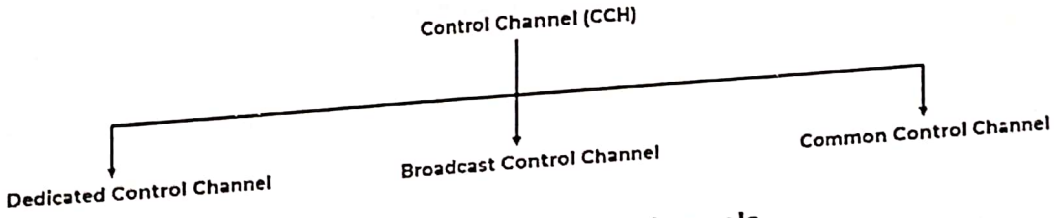


Figure 2.15: GSM Control Channels

I) Broadcast Control Channel (BCCH):

1. Broadcast control channels are transmitted in **downlink direction only** i.e. only transmitted by BTS.
2. The broadcast channels are used to broadcast synchronization and general network information to all the MSs within a cell.
3. Such as **Location Area Identity (LAI) and maximum output power**.
4. It has two types: Frequency Correction Channel, Synchronization Channel.

Scanned by CamScanner

a. **Frequency Correction Channel (FCCH):**
   - It is used for the frequency correction / synchronization of a mobile station.
   - The repeated (every 10 sec) transmission of Frequency Bursts is called FCCH.
   - FCCH is transmitted on the downlink, point-to-multipoint.

b. **Synchronization Channel (SCH):**
   - It allows the mobile station to synchronize time wise with the BTS.
   - Repeated broadcast (every 10 frames) of Synchronization Bursts is called SCH.
   - SCH is transmitted on the downlink, point-to-multipoint.

II) **Common Control Channel:**

1. Common Control Channel are communication channels that are used to coordinate the control of mobile devices operating within its cell radio coverage area.
2. GSM control channels include the random access channel (RACH), paging channel (PCH), and access grant channel (AGCH).
3. They are used by an MS during the **paging and access procedures**.
4. It is **unidirectional channel**.

a. **Random Access Control Channel:**
   - Transmitted by the mobile when it wishes to access to the system.
   - This occurs when mobile initiates a call or responds to a page.
   - It uses multiple access slotted ALOHA to access medium.

b. **Paging Channel:**
   - Transmitted by the BTS when it wishes to contact a mobile.
   - The reason for contact may be an incoming call or short message.

c. **Access Grant Control Channel:**
   - It carries data which instructs the mobile to operate in a particular physical channel (Time slot)
   - The AGCH is used by the network to grant, or deny, an MS access to the network by supplying it with details of a dedicated channel, i.e. TCH or SDCCH, to be used for subsequent communications.

III) **Dedicated Control Channel:**

1. They are communication channels that transfer signaling messages to specific devices.
2. It is a **bi-directional channel**.
3. Signaling information is carried between an MS and a BTS using associated and dedicated control channels during or not during a call.
4. It includes:

a. **Standalone Dedicated Control Channel (SDCCH):**
   - It is used by the MS for signaling as long as TCH is not established with BTS.
   - It also carries information for call forwarding and Transmission of short message.
   - It can be used for **authentication and registration**.

b. **Slow Associated Control Channel (SACCH):**
   - It is used to **exchange system information** like channel quality and signal power level.
   - SACCH messages may be sent once every 480ms, i.e. approximately every 2s.

Scanned by CamScanner

c. **Fast Associated Control Channel (FACCH):**

- FACCH is transmitted instead of a TCH.
- The FACCH steal the TCH bust and inserts its own information.
- The FACCH is used to carry out **user authentication and handover**.
- A complete FACCH message may be sent once in every 20 ms.

Q18. Explain UMTS architecture **[P | High]**

Ans:

UMTS:

1. UMTS Stands for **Universal Mobile Telecommunication System**.
2. It is a 3G mobile cellular technology for network based on the GSM standard.
3. It was developed by 3GG (3rd Generation Partnership Project)
4. It is the component of International Telecommunications Union IMT-2000 standard set.
5. It supports both **connections less and connection oriented services** for point to point and point to multipoint communication.

UMTS SERVICES:

1. It support **real-time** and **non-real-time services**.
2. It also supports circuit switched & packet switched transmission.
3. It provides variable data rates for uplink and downlink.
4. It is compatible with GSM, ATM, IP & ISDN based networks.

UMTS ARCHITECTURE:

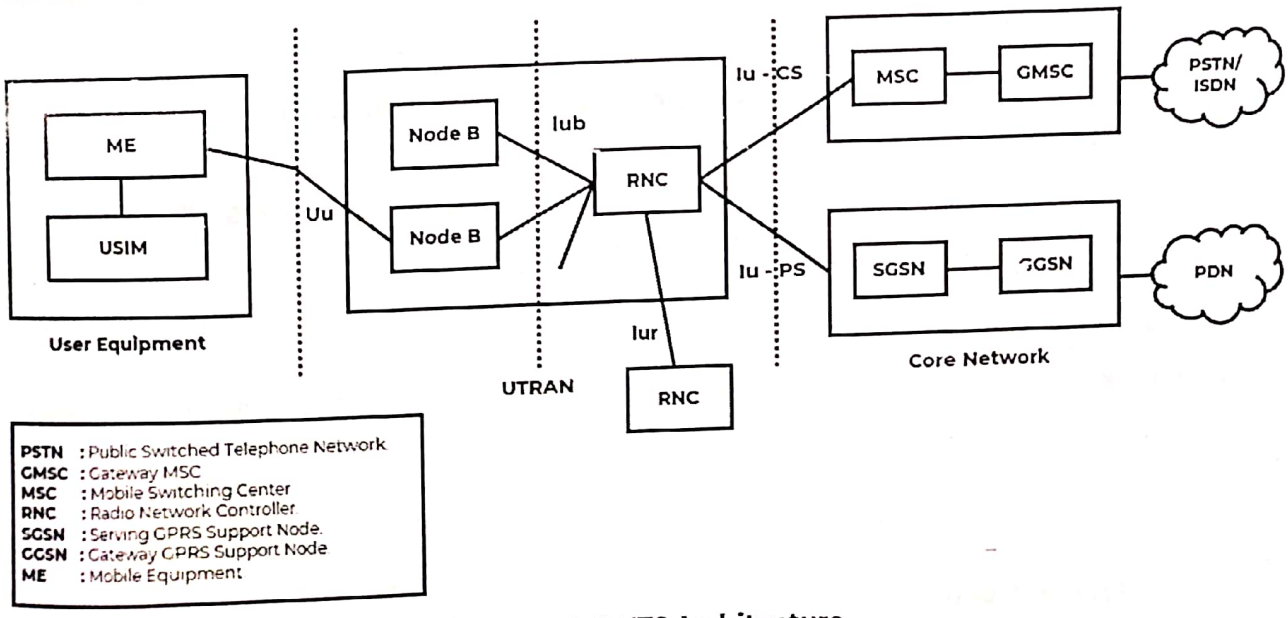


Figure 2.16: UMTS Architecture.

1. Figure 2.16 shows UMTS Architecture.
2. It has following components:

I) User Equipment (UE):

1. User Equipment consists of equipment that the subscriber uses to connect to the UMTS system.
2. It contains SIM and Mobile Equipment (ME)

Scanned by CamScanner

II) Universal Terrestrial Radio Access Network (UTRAN):

1. UTRAN handles the cell level mobility and comprises of many Radio Network Subsystems.
2. It is connected to user equipment via the radio interface Uu.
3. It has following functions:
   a. Admission control.
   b. Channel coding.
   c. Handover control.
   d. Access control.

III) Core Network (CN):

1. Core Network communicates with UTRAN via the Iu interface.
2. It contains components such as HLR, VLR, MSC, GMSC, SGSN and GGSN.
3. It has following functions:
   a. Inter-system handover.
   b. Location management.

Q18. Explain UTRA-FDD and TDD modes

Ans: [P | Mediun

UTRA:

1. UTRA stands for **UMTS Terrestrial Radio Access**.
2. UTRA is the radio interface of UMTS.
3. The UMTS radio interface has two different modes, an UMTS-FDD mode and a UMTS-TDD mode.

UTRA-FDD:

1. UTRA - FDD stands for **UMTS Terrestrial Radio Access – Frequency Division Duplex**.
2. It is 3GPP standardized version of UMTS networks.
3. The UTRA-FDD uses wideband CDMA (W-CDMA) with **direct sequence spreading (DSS)**.
4. It makes use of paired bands for the **uplink and the downlink**.
5. The UTRA-FDD uses the following frequency band for transmission
   a. **Uplink:** 1920 to 1980 MHz.
   b. **Downlink:** 2110 to 2170 MHz.
4. It provides soft handover.
5. It uses QPSK for modulation.
6. It requires complex power control.

UTRA-FDD Frame Structure:

a. Figure 2.17 shows UTRA-FDD Frame Structure.
b. A radio frame contains 15 time slots.
c. The duration of each frame is 10 msec.
d. A radio frame consists of 38400 chips.
e. Each time slot is of 666.6 μs and consists of 2560 chips.
f. Each WCDMA channel occupies 4.4 to 5 MHz bandwidth.

Scanned by CamScanner

g. Time slots in WCDMA are not used for user separation but to support periodic functions.

h. In contrast to GSM where time slots are used to separate users.

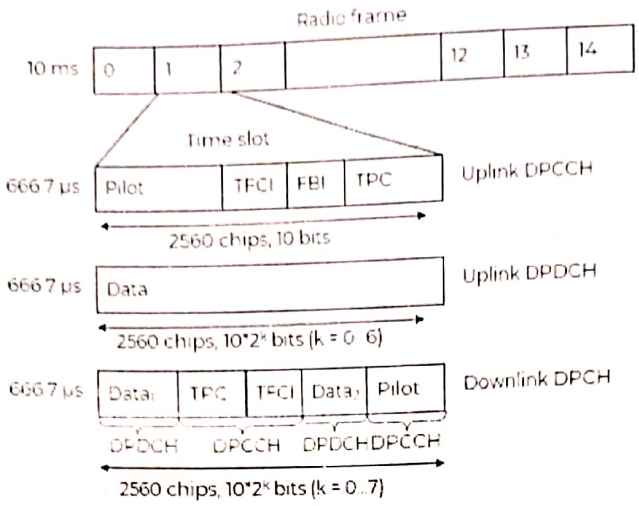


Figure 2.17: UTRA-FDD Frame Structure.

FBI: Feedback Information

TPC: Transmit Power Control

TFCI: Transport Format Combination Indicator

DPCCH: Dedicated Physical Control Channel

DPDCH: Dedicated Physical Data Channel

DPCH: Dedicated Physical Channel

UTRA-TDD:

1. UTRA - TDD stands for **UMTS Terrestrial Radio Access – Time Division Duplex**.
2. It is a 3GPP standardized version of UMTS networks.
3. It is a combination of TDMA and CDMA using TDD.
4. It separates up link and down link in time domain.
5. It has two bands available: 1900-1920 MHz and 2010-2025 MHz.
6. The radio interface of the unpaired bands makes use of Time Duplex CDMA (TD-CDMA and TD-SCDMA).
7. This mode is used for high bit rates at hot spots with low mobility.

UTRA-TDD Frame Structure:

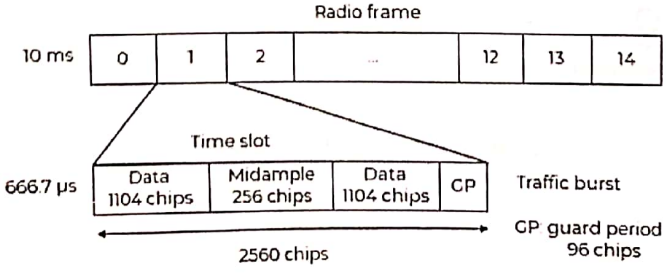


Figure 2.18: UTRA-TDD Frame Structure.

a. Figure 2.18 shows UTRA-TDD Frame Structure.

b. If the users have different data rates, the TDD frames can be symmetrical/Unsymmetrical.

Scanned by CamScanner

c. The system has the capacity to change the up-link/downlink spreading factor as a function of data rates.

d. Guard space can loosen the synchronization needs a bit.

Q19. UTRAN [P | Medium]

Ans:

UTRAN:

1. UTRAN stands for **UMTS Terrestrial Radio Access Network.**
2. It is the fixed network infrastructure that contains the facilities for the transmission to and from the mobile users over radio.
3. The components of the UTRAN are the base stations, which are called Node B in UMTS, and control nodes, which are called Radio Network Controller (RNC).
4. The Radio Network Controllers are connected to the Core Network (CN).
5. UTRAN can carry many traffic types from real-time Circuit Switched to IP based Packet Switched.
6. Figure 2.19 shows UTRAN Structure.
7. There are four interfaces connecting the UTRAN internally or externally to other functional entities Iu, Uu, Iub and Iur.
8. The Iu interface is an external interface that connects the RNC to the Core Network (CN).
9. The Uu is also external, connecting the Node B with the User Equipment (UE).
10. The Iub is an internal interface connecting the RNC with the Node B.
11. And at last there is the Iur interface which is an internal interface most of the time, but can exceptionally be an external interface too for some network architectures.
12. The Iur connects two RNCs with each other.

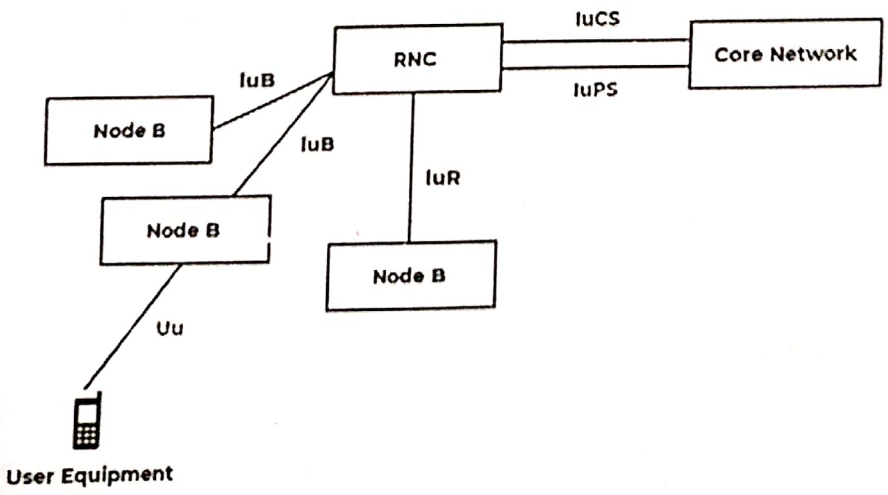


Figure 2.19: UTRAN Structure.

Scanned by CamScanner

Q20. Explain difference in GSM, GPRS and UMTS.

Ans: **[P | Medium]**

Table 2.1: Comparison between GSM, GPRS & UMTS.

Parameter	GSM	GPRS	UMTS
Full Form	Global System for Mobile Communication.	General Packet Radio Service.	Universal Mobile Telecomrnunication System.
System Generation	2G Technology.	2.5G Technology.	3G Technology.
Base System	TDMA.	GSM.	GSM & GPRS.
Packet Upload Rate	14.4 Kbps.	26.8 Kbps.	128 Kbps.
Packet Download Rate	14.4 Kbps.	53.6 Kbps.	384 Kbps.
Switching Technology	Circuit Switched.	Circuit Switched and Packet Switched.	Circuit Switched and Packet Switched.
Carrier Channels	200 KHz.	200 KHz.	5 MHz/1.6 MHz.
Frame Duration	4.615 ms.	4.615 ms.	10 ms.
Frequency Band	850 MHz, 900 MHz, 1800 MHz, 1800 MHz and 1900 MHz.	850 MHz, 900 MHz, 1800 MHz, 1800 MHz and 1900 MHz.	Band – I to Band VI.
Network Components	MS, BSS, MSC & Operational Subsystem.	All Components of GSM and additional components such as GGSN, SGSN and PCU.	User Equipment, Radio Access Network and Core Network.

Scanned by CamScanner

CHAP - 3: MOBILE NETWORKING

Q1. M-TCP

Ans: [P | Medium]

MOBILE-TCP:

1. The occurrence of lengthy and/or frequent disconnection is the major problem in wireless networks.
2. To overcome this problem, **Mobile TCP** is used.
3. Mobile TCP deals with the lengthy and/or frequent disconnections.
4. Mobile TCP splits up the connection into two parts:
   a. An unmodified TCP fixed network to Supervised Host.
   b. An optimized TCP Supervisory Host to Mobile Host.

FEATURES:

1. To improve overall throughput.
2. To lower the delay.
3. To maintain end-to-end semantics of TCP.
4. To provide a more efficient handover.

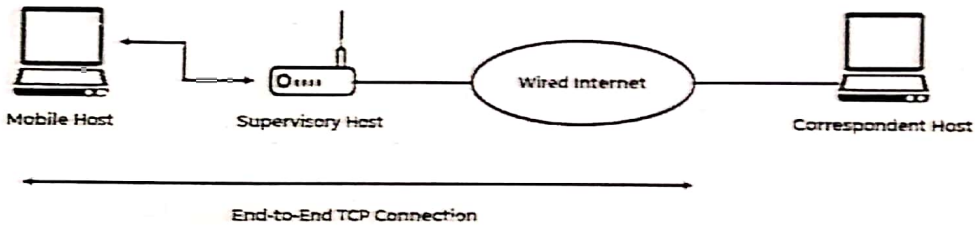


Figure 3.1: Mobile TCP.

WORKING:

1. Figure 3.1 shows the Mobile TCP Network.
2. Here packets are sends to the **Mobile Host** by a **Corresponding Host**.
3. If any packet is lost on the wireless link, then the original sender retransmits the packet.
4. Thus in Mobile TCP, **End-to-End Semantics** is maintained.
5. All the packets send to Mobile Host are monitored by the Supervisory Host.
6. Mobile Host send the **ACK packets** for all the packets it has received.
7. After a set amount of time, if the Supervisory Host still does not receive any ACK, it assumes that the Mobile Host is disconnected.
8. Supervisory Host set sender's Window size to **zero** and thus **chokes the sender**.
9. Once the window size is set to zero, the sender is forced to go into a **persistent mode**.
10. In the persistent mode, independent of the receiver's period of disconnected state, the state of the sender will not change.
11. Once the Supervisory Host detects the connectivity again, the sender's window size is again set to the old value, enabling the sender to send at full speed.

Scanned by CamScanner

Q20. Explain difference in GSM, GPRS and UMTS. **[P | Medium]**

Ans:

Table 2.1: Comparison between GSM, GPRS & UMTS.

Parameter	GSM	GPRS	UMTS
Full Form	Global System for Mobile Communication.	General Packet Radio Service.	Universal Mobile Telecomrnunication System.
System Generation	2G Technology.	2.5G Technology.	3G Technology.
Base System	TDMA.	GSM.	GSM & GPRS.
Packet Upload Rate	14.4 Kbps.	26.8 Kbps.	128 Kbps.
Packet Download Rate	14.4 Kbps.	53.6 Kbps.	384 Kbps.
Switching Technology	Circuit Switched.	Circuit Switched and Packet Switched.	Circuit Switched and Packet Switched.
Carrier Channels	200 KHz.	200 KHz.	5 MHz/1.6 MHz.
Frame Duration	4.615 ms.	4.615 ms.	10 ms.
Frequency Band	850 MHz, 900 MHz, 1800 MHz, 1800 MHz and 1900 MHz.	850 MHz, 900 MHz, 1800 MHz, 1800 MHz and 1900 MHz.	Band – I to Band VI.
Network Components	MS, BSS, MSC & Operational Subsystem.	All Components of GSM and additional components such as GGSN, SGSN and PCU.	User Equipment, Radio Access Network and Core Network.

Scanned by CamScanner

CHAP - 3: MOBILE NETWORKING

Q1. M-TCP [P | Medium]

Ans:

MOBILE-TCP:

1. The occurrence of lengthy and/or frequent disconnection is the major problem in wireless networks.
2. To overcome this problem, **Mobile TCP** is used.
3. Mobile TCP deals with the lengthy and/or frequent disconnections.
4. Mobile TCP splits up the connection into two parts:
   a. An unmodified TCP fixed network to Supervised Host.
   b. An optimized TCP Supervisory Host to Mobile Host.

FEATURES:

1. To improve overall throughput.
2. To lower the delay.
3. To maintain end-to-end semantics of TCP.
4. To provide a more efficient handover.

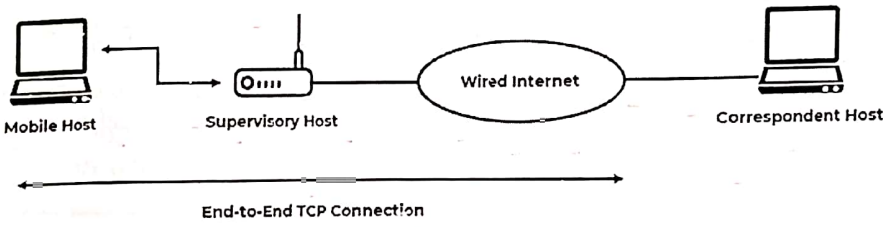


Figure 3.1: Mobile TCP.

WORKING:

1. Figure 3.1 shows the Mobile TCP Network.
2. Here packets are sends to the **Mobile Host** by a **Corresponding Host**.
3. If any packet is lost on the wireless link, then the original sender retransmits the packet.
4. Thus in Mobile TCP, **End-to-End Semantics** is maintained.
5. All the packets send to Mobile Host are monitored by the Supervisory Host.
6. Mobile Host send the **ACK packets** for all the packets it has received.
7. After a set amount of time, if the Supervisory Host still does not receive any ACK, it assumes that the Mobile Host is disconnected.
8. Supervisory Host set sender's Window size to **zero** and thus **chokes the sender**.
9. Once the window size is set to zero, the sender is forced to go into a **persistent mode**.
10. In the persistent mode, independent of the receiver's period of disconnected state, the state of the sender will not change.
11. Once the Supervisory Host detects the connectivity again, the sender's window size is again set to the old value, enabling the sender to send at full speed.

Scanned by CamScanner

Advantages:

1. End-to-End Semantics is maintained.
2. It avoids unnecessary retransmissions, if the Mobile Host is disconnected.

Disadvantages:

1. It requires new network elements like **bandwidth manager**.
2. Losses on Wireless Link are propagated to the Wired Link.

Q2. List the entities of mobile IP **[P | Medium]**

Ans:

ENTITIES OF MOBILE IP:

I) Mobile Node (MN):

1. Mobile Node is an **Internet-connected device** whose location and point of attachment to the Internet may frequently be changed.
2. This kind of node is often a **cellular telephone** or **handheld** or **laptop computer**.
3. Although a mobile node can also be a router.

II) Correspondent Node (CN):

1. Correspondent Node can be **Fixed** or **Mobile**.
2. It is a node that is intended to communicate with a Mobile Node.
3. **Example:** Web Server.

III) Home Network (HN):

1. Home Network is the network on which Mobile Node's permanent **IP address is defined**.
2. In this Network, the device receives its **Home Address**.

IV) Foreign Network (FN):

1. A Foreign Network is any network other than the home network to which a mobile device may be connected.

V) Home Agent (HA):

1. Home Agent is a router on the Home Network that provides services to Mobile Node.
2. Home Agent maintains a **location registry**.

VI) Foreign Agent (FA):

1. The Foreign Agent is a router in the Foreign Network to which the mobile node is currently attached.
2. The FA can provide several services to the MN during its visit to the foreign network.

VII) Care-of-Address (COA):

1. The Care-of-Address defines the **current location** of the Mobile Node.
2. It is usually the **IP Address** of the Foreign Agent.
3. It is send by Foreign Agent to Home Agent when Mobile Node is attached.

Scanned by CamScanner

Q3. Describe data transfer from a mobile node to a fixed node and vice versa. [P | Medium]

Ans:

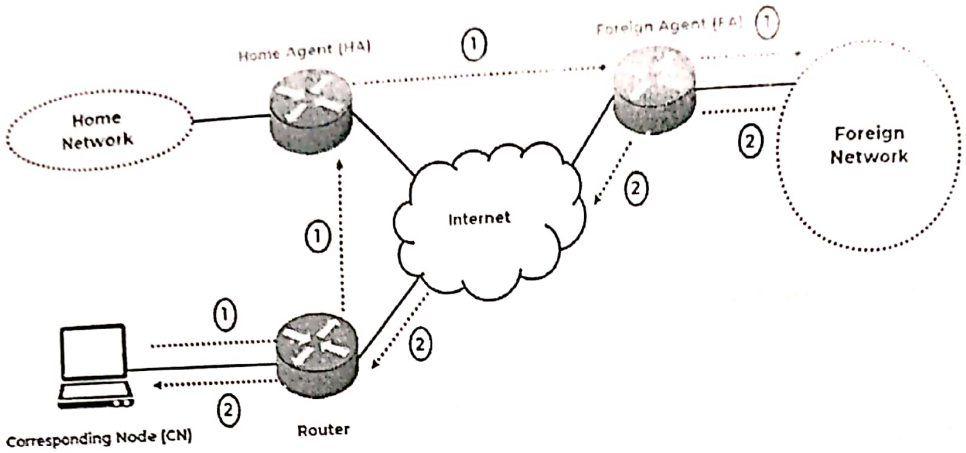


Figure 3.2: Data Transfer to and from the Mobile Node.

DATA TRANSFER FROM A MOBILE NODE TO A FIXED NODE:

1. Let the Fixed Node be the Corresponding Node (CN) as shown in figure 3.2.
2. As shown in figure 3.2, the packet is sent by the Mobile Node (MN) with its original address as the sourc address.
3. The destination address of the packet is CN's IP Address.
4. Foreign Agent (FA) responsible for the foreign network acts as a default router.
5. It forwards the packet to the router responsible for the CN.
6. The router responsible for the CN then forwards the packet to CN.

DATA TRANSFER FROM A FIXED NODE TO A MOBILE NODE:

1. Let the Fixed Node be the Corresponding Node (CN) as shown in figure 3.2.
2. Since the CN does not known the current location of Mobile Node (MN), so it sends the Packet to th IP Address of the MN.
3. Here the source address of the packet is CN's IP Address.
4. The destination address of the packet is MN's original IP Address.
5. The packet is then routed via the **standard routing mechanism** o **the internet** to the route responsible for the MN's Home Network.
6. The Home Network's router implements the Home Agent.
7. The HA now detects that the MN is currently not in its home network.
8. Now HA, instead of forwarding the packet into the subnet as usual, the packet is encapsulated and i tunnel to the COA of the MN.
9. A new header is added in front of the old IP header indicating MN's COA as the new destination an HA as the source of the encapsulated packet.
10. Foreign Agent now decapsulates the packet and forwards the original packet with CN as sourc and MN as destination.

Scanned by CamScanner

Q4. **Explain the functioning of I-TCP and SNOOP-TCP, giving advantages and disadvantages of both.**

[P | Medium]

Ans:

I-TCP:

1. I-TCP stands for **Indirect TCP**.
2. I-TCP separates a TCP Connection into two parts: **a fixed part and a wireless part**.
3. A fixed part is between the mobile support router and the fixed host **over the fixed network**.
4. A Wireless part is between the Mobile Host and its access point **over the wireless medium**.

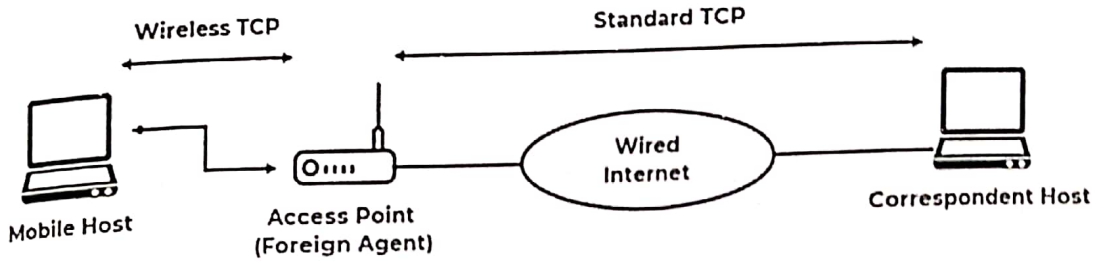


Figure 3.3: I-TCP.

5. The figure 3.3 shows a mobile host connected via a **wireless link to an access point** (AP).
6. Access node is connected to the internet via the wired Internet.
7. **Standard TCP** is used to connect to the AP from fixed computer (Corresponding Host).
8. When there is a change to the TCP, no computer over the internet recognize it.
9. The Access point acts as a Foreign Agent of mobile host and terminates the TCP connection.
10. Therefore, the fixed computer now sees the AP as mobile host; on other hand the mobile host sees AP as the fixed computer.
11. Now Foreign Agent (FA) relays data in both directions.
12. When the Fixed Computer sends data, FA sends back an acknowledgement to it.
13. When the mobile host receives a packet from FA, the mobile host also sends back an acknowledgement.
14. This acknowledgement is a local acknowledgement. It will not be forwarded to the Fixed Computer.
15. If a packet is lost in wireless transmission then FA will try re-transmitting it again.

Advantages:

1. I-TCP does not require any changes in TCP protocol as used by the different hosts in network.
2. Transmission error on the wireless link will not propagate to the wired link. Therefore, flow will always be in a sequence.

Disadvantages:

1. The end-to-end connection for which TCP has been designed will fail if the Foreign Agent (FA) crashes.
2. In practical terms increased handover may latency may be much more problematic.

SNOOP-TCP:

1. The main drawback of I-TCP is the **segmentation** of the single TCP connection into two TCP connections, which losses the original end-to-end semantics.

Scanned by CamScanner

2. This drawback is overcome using Snoop-TCP.
3. It is based on **End-to-End TCP semantic**.
4. The main function is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss.
5. The figure 3.4 shows a Snooping TCP as a transparent TCP extension.
6. In Snoop TCP, foreign agent buffers all packet with **destination mobile host**.
7. It then 'snoops' each packet flowing in both the directions for reading acknowledgements.
8. The foreign agent buffers every packet until it receives an acknowledgment from the mobile host.
9. If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgment has been lost.

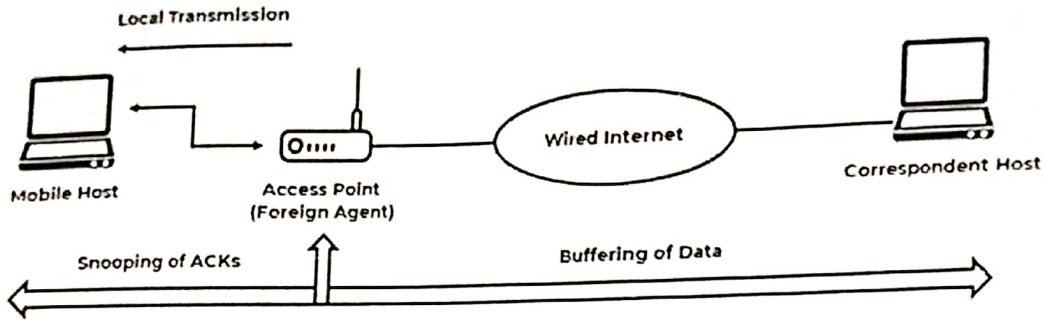


Figure 3.4: Snoop-TCP.

10. Alternatively a foreign agent could receive a duplicate ACK which also shows the loss of packet.
11. In such a situation, the FA retransmit the packet directly from the buffer thus performing a faster retransmission compared to correspondent host.
12. To maintain transparency, the FA doesn't send acknowledgement to the correspondent host as in I-TCP.
13. The acknowledgement is send by the Mobile host itself.
14. The FA keeps on monitoring it.
15. When the data flows for mobile host to CN, the FA snoops and checks the sequence of acknowledgement number.
16. If a gap is found, FA sends signal to re-transmit.

Advantages:

1. The original TCP sematic i.e. end-to-end connection is preserved.
2. No need for handoff.

Disadvantages:

1. If any encryption is applied at both ends, the snooping and buffering process would be a waste of time as no data can be read by FA.
2. Cannot snoop encrypted datagrams.

Scanned by CamScanner

Q5. How the agent can be discovered using Mobile IP? Give the overlay of agent advertisement packet which includes mobility extension. **[P | Medium]**

Ans:

AGENT DISCOVERY:

1. When a mobile node is first turned on, it can either be in its home network or a foreign network.
2. Hence, the first thing that is must do is to determine where it is, and if it is not at home, then it must begin the process of setting up **datagram forwarding** from its home network to the current location.
3. This process is accomplished by communicating with a local router serving as an agent through the process called **Agent Discovery**.
4. A mobile node uses a method known as **agent discovery** to determine the following information:
   a. When the node has moved from one network to another
   b. Whether the network is the node's home or a foreign network
   c. What is the foreign agent care-of address offered by each foreign agent on that network
5. After moving to another network one initial problem is how to find a foreign agent.
6. For this purpose, mobile IP describes two messages: **Agent Advertisement** and **Agent Solicitation**.

AGENT ADVERTISEMENT IN MOBILE IP:

1. **Mobility** is an important feature of Mobile IP.
2. Due to mobility, it is very important to track where the user's cell has moved.
3. Tracking means to locate the MN's foreign agent (FA).
4. One method to find it is by using the method called as **Mobile Agent Advertisement**.
5. Mobile nodes use agent advertisements to determine their current point of attachment to the Internet.
6. An agent advertisement is an **Internet Control Message Protocol** (ICMP) router advertisement.
7. In Agent Advertisement, the Home Agent (HA) & Foreign Agent (FA) advertise their presence and services using messages.
8. Agent Advertisement messages are periodically broadcast.
9. An Agent Advertisement has the following Functions:
   a. It allows mobile nodes to discover **foreign agents** (FA) and get **Care of Address** (COA).
   b. It allows mobile nodes to know the **services** provided by the foreign agent.
   c. It allows mobile nodes to determine whether an agent is its **home agent or foreign agent**.
10. Figure 3.5 shows the Agent Advertisement Message.
11. Some of the fields used are as follows:
    a. **Type:** It is set to 9 for ICMP.
    b. **Code:** Code is set to 0, if agent routes traffic from non-mobile nodes as well or else 16
    c. **#Addresses:** It indicates the number of router addresses advertised in this message.
    d. **Lifetime**: It denotes the length of time for which the advertisement is valid.
    e. **Preference level:** Preference for each router address is specified. It helps a node to choose the router.

Scanned by CamScanner

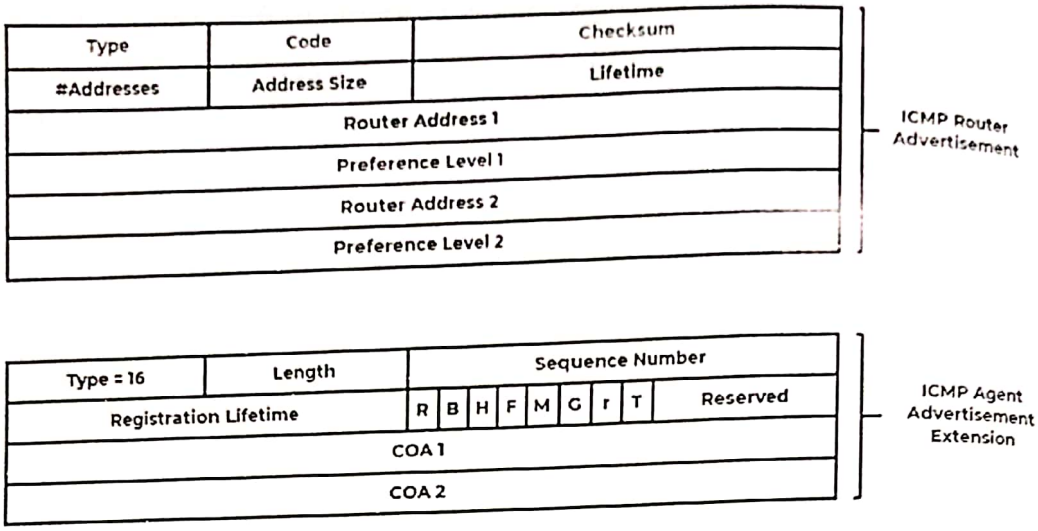


Figure 3.5: Agent Advertisement Message.

Q6. Explain IP-in-IP Techniques of encapsulation of mobile IP Packet. [P | Medium

Ans:

IP-IN-IP ENCAPSULATION:

1. IP-in-IP Encapsulation is defined in **RFC 2003**.
2. It is the simplest approach.
3. IP in IP is an IP tunneling protocol that encapsulates one IP packet in another IP packet.
4. Figure 3.6 shows the IP-in-IP Encapsulation format.

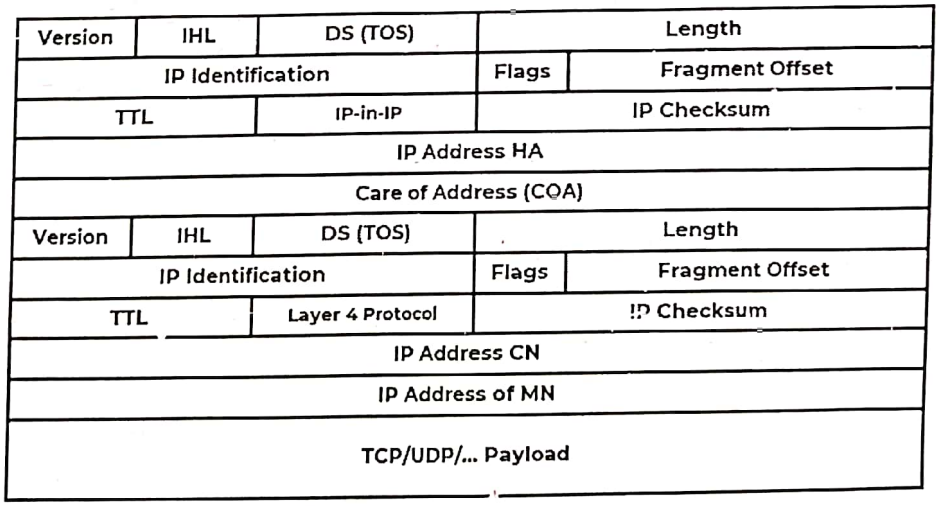


Figure 3.6: IP-in-IP Encapsulation.

The various field in the outer header are:

I) Version:

1. Version field denotes the version number.
2. It is set to 4 for IPv4.

II) IHL (Internet Header Length):

1. IHL indicates the length of the outer header.

III) DS (TOS):

1. It is just copied from the inner header.

Scanned by CamScanner

IV) Length:

1. It denotes the complete length of the encapsulated packet.

V) TTL (Time to Live):

1. It indicates the period of validity of the packet.
2. TTL should be high enough so the packet can reach the tunnel endpoint.

VI) IP-in-IP:

1. It denotes the type of protocol used in the IP Payload.

VII) IP Checksum:

1. This is used for error detection mechanism.

The fields of inner header are almost same as the outer header, the only differences are:

a. The **address fields** consists of the address of the original sender and receiver.
b. The **TTL Value** of the inner header is decremented by 1

Advantages: It is simple to implement and it is a default encapsulation mechanism.

Disadvantages: Most of the outer header fields are same as inner header, so this method increases redundancy.

Q7. Why is Mobile IP packet required to be forwarded through a tunnel? Explain minimal techniques of encapsulation of Mobile IP packet.

[P | Medium]

Ans:

MOBILE IP:

1. Mobile IP is a **communication Protocol**.
2. It was developed by **Internet Engineering Task Force (IETF) Standard**.
3. It is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.
4. Mobile IP provides an efficient, scalable mechanism for node mobility within the internet.

NEED OF TUNNEL:

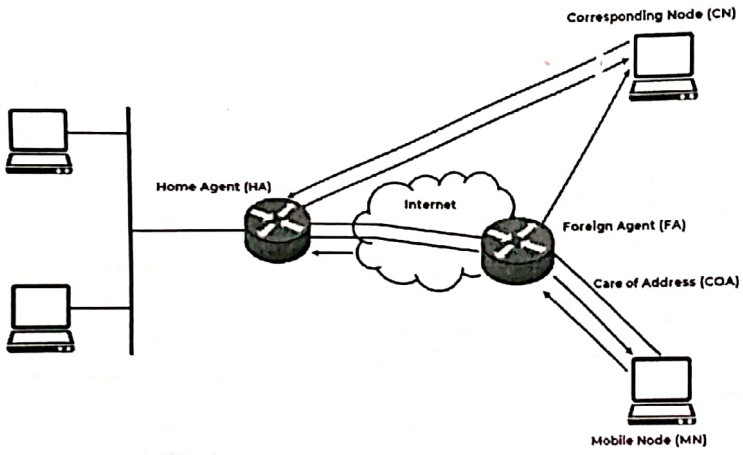


Figure 3.7: Mobile IP Packet Routing Using Tunnel.

Scanned by CamScanner

1. Consider a situation when a Correspondent Node (CN) wants to send an IP Packet to a Mobile Node (MN).
2. CN knows the **IP Address** of the MN.
3. So CN sends IP Packets to MN's IP Address.
4. This Packet is then routed to the Home Router of the MN also called as Home Agent (HA) through Internet.
5. HA then **encapsulates and tunnels** the Packet to the Care of Address (COA).
6. The COA defines the current location of the MN from an IP point of view.
7. Since internet routes are created based on the header contents of an IP Packet.
8. So to route IP Packets from HA to COA, new header for the packet to be transmitted is required.
9. As shown in Figure 3.8, the new header on top of the original header is made.
10. Now it is possible to set a new direct route (a tunnel) to the MN from HA as it is roaming.
11. Thus Tunneling is the process of creating a tunnel by the HA to the COA to route packets to the Mobile Node as it roams.
12. It established a pipe wherein the data is inserted and moves in FIFO order.

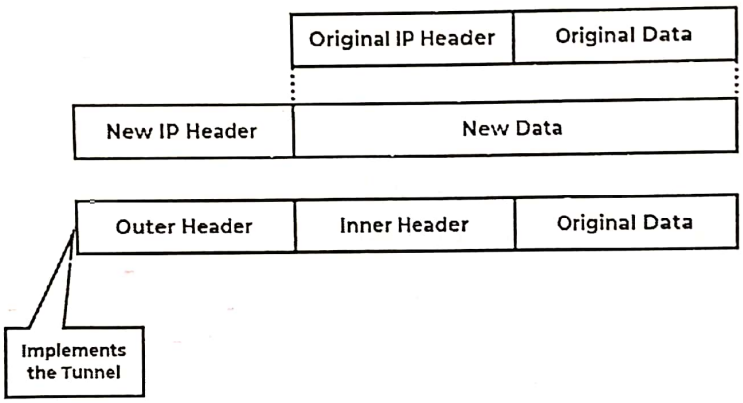


Figure 3.8: Encapsulation.

MINIMAL ENCAPSULATION:

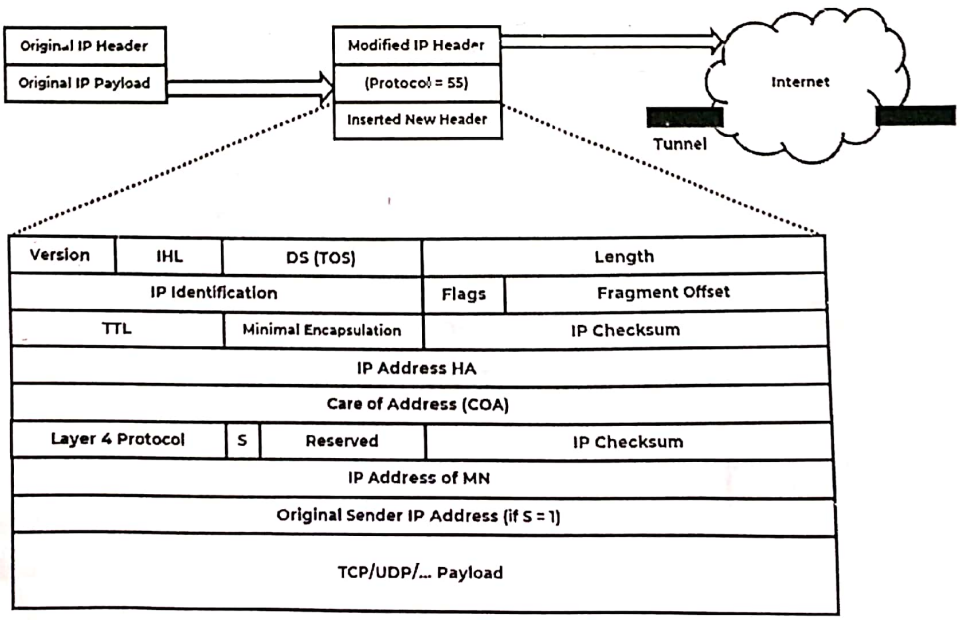


Figure 3.9: Minimal Encapsulation.

Scanned by CamScanner

1. Minimal Encapsulation is defined in **RFC 2004**.
2. In IP-in-IP Encapsulation, several fields are redundant.
3. Minimal Encapsulation will **remove these redundancy**.
4. Figure 3.9 shows the Minimal Encapsulation.
5. The outer header fields in Minimal Encapsulation are almost same as for IP encapsulation; the only difference is in the Type field.
6. It is set to 55.
7. The various field in the outer header are:
   a. **Version:**
   - Version field denotes the version number.
   - It is set to 4 for IPv4.

   b. **IHL (Internet Header Length):**
   - IHL indicates the length of the outer header.

   c. **DS (TOS):**
   - It is just copied from the inner header.

   d. **Length:**
   - It denotes the complete length of the encapsulated packet.

   e. **TTL (Time to Live):**
   - It indicates the period of validity of the packet.
   - TTL should be high enough so the packet can reach the tunnel endpoint.

   f. **Minimal Encapsulation:**
   - It denotes the type of protocol used in the IP Payload.

   g. **IP Checksum:**
   - This is used for error detection mechanism.
8. The inner header is much smaller than IP Encapsulation packet.
9. The **S bit** indicates whether the original sender's IP Address is included in the header or not.
10. **Value 0** indicates sender's IP Address can be omitted.

Advantages: Lower Overhead as compared to IP-in-IP Encapsulation as it avoids redundancy.

Disadvantages: It does not support fragmentation to deal with tunnel with smaller path maximum transmission unit (MTU).

Q8. Explain Generic techniques of encapsulation of Mobile IP packet. **[P | Medium]**

Ans:

GENERIC ROUTING ENCAPSULATION:

1. Generic Routing Encapsulation (GRE) is defined in **RFC 1701**.
2. It is a **Tunneling Protocol** developed by Cisco Systems.
3. It can **encapsulate** a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.
4. Figure 3.10 shows the Generic Routing Encapsulation.

Scanned by CamScanner

5. The GRE header is prepended to the packet of one protocol suite with the original header and data.

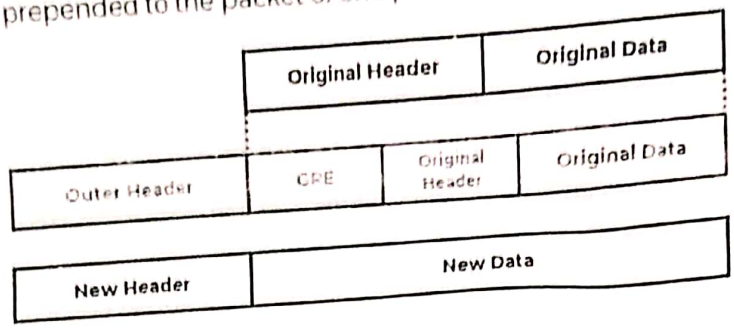


Figure 3.10: Generic Routing Encapsulation.

6. The various fields of the GRE header that follows the outer header are described as follows:

a. Protocol Type:

- It defines the type of protocol used.
- Protocol Type is set to 47 for GRE Encapsulation.

b. C bit:

- If C bit is set, the checksum field contains the valid IP checksum of the GRE header and the payload.

c. R bit:

- If R bit is set, it indicates that the **offset and routing fields** are present and contains valid information.

d. K bit:

- If it is set, it indicates the key field is present and may be used for **authentication**.

e. S bit:

- If set, it indicates that the **sequence number** is present.

f. s bit:

- If set, it indicates that the **strict source routing** is used.

g. Recursion Control:

- It represents a counter that shows the number of allowed **recursive encapsulations**.

h. Reserved:

- This field is reserved for future use.

i. Version:

- Version field denotes the version number.

j. Protocol:

- It indicates the protocol used by the packet.

k. Checksum:

- It contains a valid IP checksum of the GRE header and the payload.

l. Offset:

- It represents the offset in bytes for the first source entry.

m. Key:

- It contains a key that can be used for **authentication**.

n. Routing:

- It is a variable length field and contains the fields for **source routing**.

Scanned by CamScanner

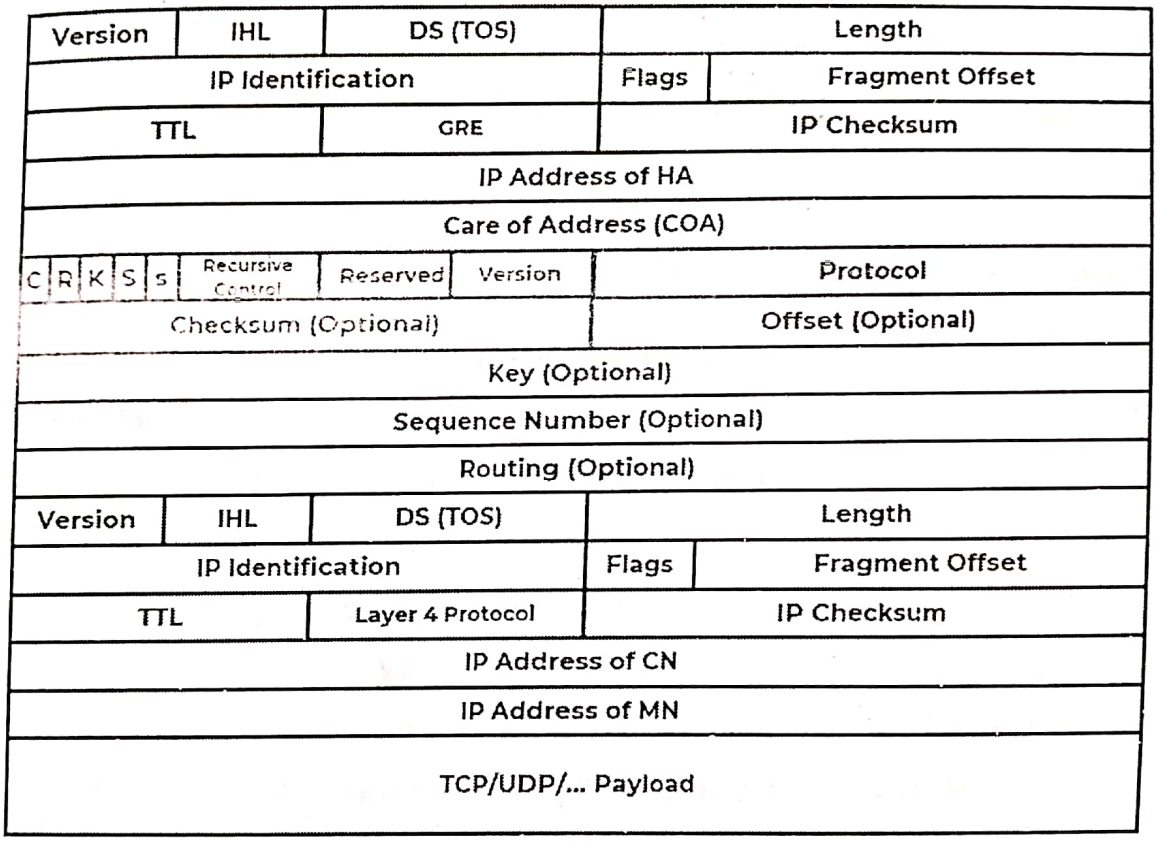


Figure 3.11: Generic Routing Encapsulation.

Advantages:

1. It support more than one level of encapsulation.
2. It support other network layer protocols in addition to IP.

Scanned by CamScanner

CHAP - 4: WIRELESS LOCAL AREA NETWORKS

Q1. Wireless Local Loop

Ans: [P | Medium]

WIRELESS LOCAL LOOP:

1. The need of internet is increasing day by day across the globe.
2. This leads to providing broadband internet to users in the office premises as well as residential places.
3. There are various ways internet can be provided to the users such as fiber optic cable, DSL line and wireless connectivity.
4. Providing fixed wireless connection for broadband internet is referred as WLL or Wireless Local Loop.
5. Wireless Local Loop is used to replace the **wire line technology**.
6. Wireless Local Loop uses a radio link to provide a telephone connection.
7. So sometimes it is called as **Radio in the Loop (RITL)** or **Fixed Radio Access (FRA)**.
8. By using a wireless link, construction period is shorten and installation and operating costs is reduced.

WLL ARCHITECTURE:

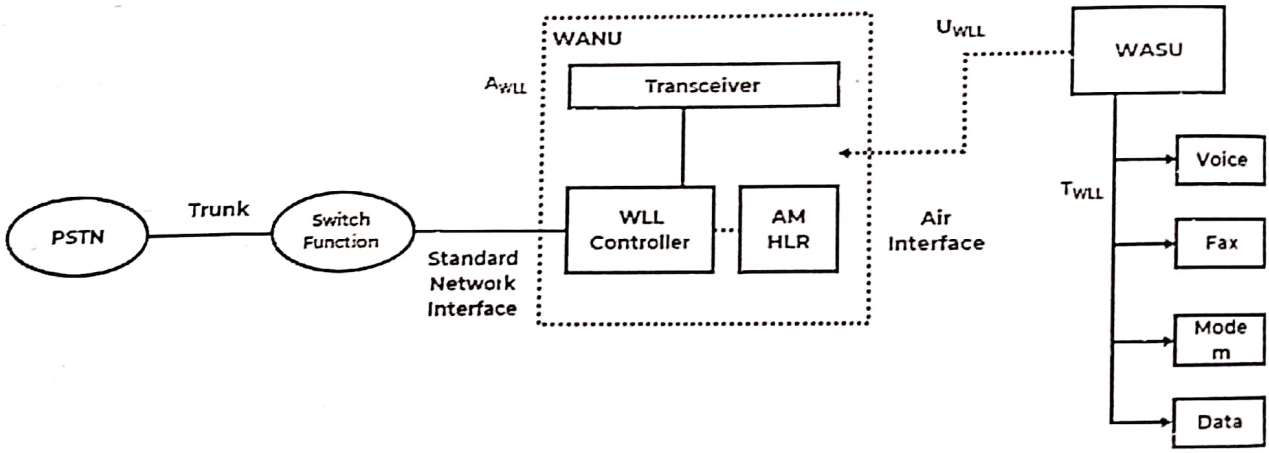


Figure 4.1: Wireless Local Loop Architecture.

1. Figure 4.1 shows the Wireless Local Loop Architecture.
2. The WLL Architecture consists of three major components i.e. WANU, WASU and SF

WANU:

1. WANU Stands for **Wireless Access Network Unit**.
2. It is connected to the switch via A_{WLL} Interface.
3. It consists of various components which includes:
   a. Base Stations Transceivers or Radio Ports (RP)
   b. Radio port control unit.
   c. Access manager (AM)
   d. HLR.
4. It provides various functionalities like:
   a. Authentication.
   b. Operations and Maintenance.

Scanned by CamScanner

c. Routing.

d. Billing.

WASU:

1. WASU Stands for **Wireless Access Subscriber Unit**.
2. It is a [illegible] interface between the network and the subscriber.
3. It is connected to the network via U_{WLL} interface and to the subscriber's unit via a traditional T_{WLL} interface.
4. The interface includes:
   a. Protocol conversion and transcoding
   b. Authentication functions
   c. Signaling functions

SF:

1. SF Stands for **Switching Function**.
2. It is associated with a switch that can be digital switch with or without Advanced Intelligent Network (AIN) capability, an ISDN switch or a Mobile Switching Centre (MSC).
3. The A_{WLL} interface between the WANU and the SF can be ISDN-BRI or IS-634 or IS-653.

Q2. Explain in detail Bluetooth Protocol Architecture.

Ans: **[P | Medium]**

BLUETOOTH:

1. Bluetooth is a **wireless technology standard** for exchanging data over short distances.
2. It was invented by **Ericson** in 1994.
3. Bluetooth is managed by the **Bluetooth Special Interest Group (SIG).**
4. Initially it can connect up to seven devices, overcoming problems that older technologies had when attempting to connect to each other.

BLUETOOTH PROTOCOL ARCHITECTURE:

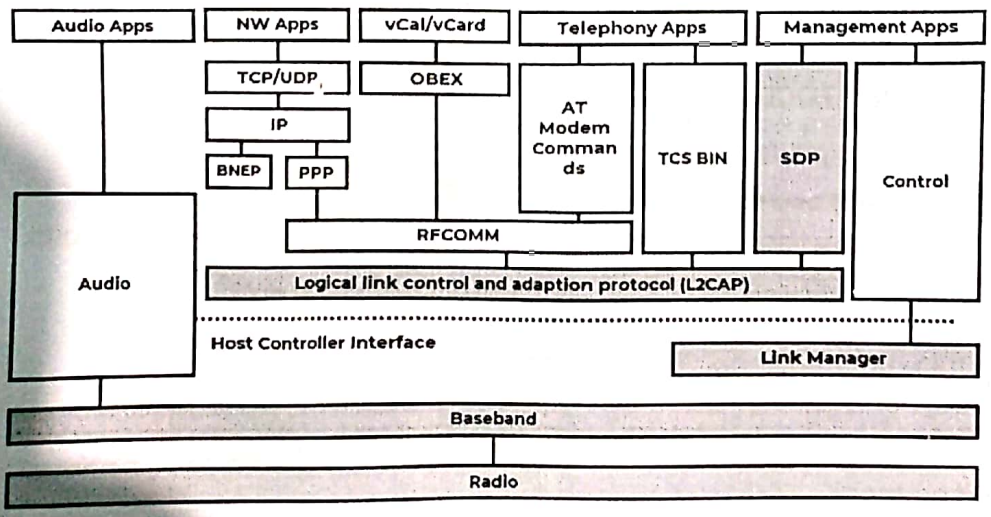


Figure 4.2: Bluetooth Protocol Architecture.

Scanned by CamScanner

1. It is also known as **Bluetooth Protocol Stack**.
2. Bluetooth Protocol Stack consists of Core Protocols, Cable Replacement Protocol, Telephony Control Protocols and Adopted Protocols.
3. Figure 4.2 shows the Bluetooth Protocol Architecture.
4. It consists of following components:

CORE PROTOCOLS:

I) Radio Layer:

1. The Radio Layer defines the requirements for a Bluetooth transceiver.
2. Bluetooth uses 2.4 GHz ISM band.

II) Baseband Layer:

1. Baseband Layer uses **frequency hopping technique**.
2. It defines physical links and timing & power control algorithms required for establishing connection between bluetooth devices within piconet.

III) Link Manager Protocol:

1. The Link Manager Protocol (LMP) is used by the Link Managers for link set-up and control.
2. This protocol performs the following functions:
   a. Authentication.
   b. Encryption.
   c. Power Control.
   d. QoS Negotiation.

IV) Logical Link Control and Adaptation Protocol (L2CAP):

1. It is the layer over the Baseband Layer and resides in the data link layer.
2. L2CAP take care of both **connection oriented and connectionless services**.
3. It provides segmentation and reassembly operation.

V) Service Discovery Protocol (SDP):

1. Service related queries including device information can be taken care at this protocol so that connection can be established between bluetooth devices.
2. It only defines the discovery of services not about their usage.

CABLE REPLACEMENT PROTOCOL:

1. Serial ports are used to provide serial communication between devices.
2. Bluetooth uses **RFCOMM** as cable replacement protocol.
3. RFCOMM functions as virtual serial port and does transport of binary digital data bits.
4. It basically emulates RS232 specifications over bluetooth physical layer.

TELEPHONY CONTROL PROTOCOLS:

1. TCS-BIN is the protocol is used as Telephony Control Protocol.
2. It is bit oriented protocol.
3. It specifies call control signals and mobility management procedures.
4. These signals take care of establishing speech and data calls.

Scanned by CamScanner

ADOPTED PROTOCOLS:

1. These protocols are already defined by other standard bodies which are incorporate without any change in the bluetooth protocol stack architecture.
2. The protocols are PPP, TCP/UDP/IP, OBEX and WAE/WAP.
3. **PPP** is a point to point protocol used to transfer IP datagrams.
4. **TCP/UDP and IP** are part of basic TCP/IP model.
5. **OBEX** is an object exchange protocol developed by IrDA and it is similar to HTTP. It is a session level protocol.

WAE provides Wireless Application Environment and **WAP** provides Wireless Application Protocol.

Q3. Describe Bluetooth architecture. Also, discuss its limitations.

Ans:

[P | Medium]

BLUETOOTH ARCHITECTURE:

Bluetooth Architecture defines two types of networks.

I) Piconet:

1. Piconet is a Bluetooth network that consists of 1 master node and 7 active slave nodes.
2. Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
3. There can be only one master station in each piconet.
4. The communication between the master and the slave can be one-to-one or one-to-many.
5. All communication is between master and a slave. Salve-slave communication is not possible.
6. In addition to seven active slave station, a piconet can have upto 255 parked nodes.
7. These parked nodes are slave stations and cannot take part in communication until it is moved from parked state to active state.
8. Figure 4.3 represents Piconet.

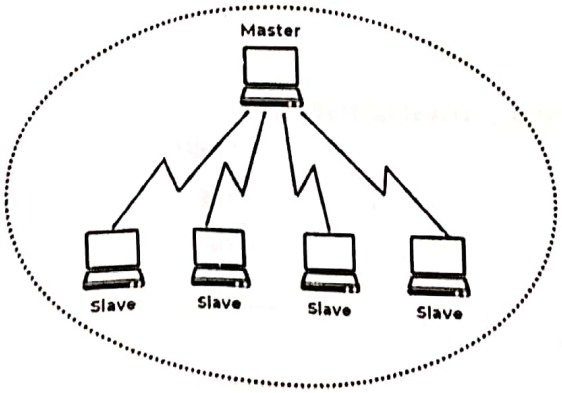


Figure 4.3: Piconet.

II) Scatternet:

1. Scatternet is formed by combining various piconets.
2. A slave in one piconet can act as a master in other piconet.

Scanned by CamScanner

3. A station or node can receive messages from the master in the first piconet and deliver the mess to its slaves in other piconet where it is acting as master.
4. This node is also called **bridge slave**.
5. Thus a station can be a member of two piconets.
6. A station cannot be a master in two piconets.
7. Figure 4.4 represents Scatternet.

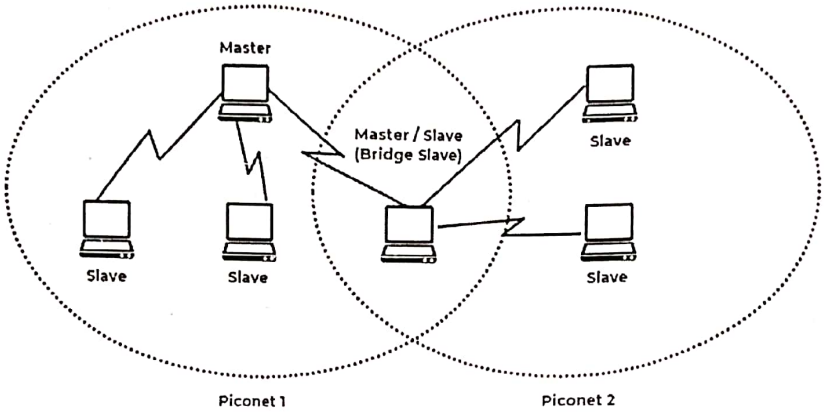


Figure 4.4: Scatternet.

LIMITATIONS:

1. One of the big disadvantages of bluetooth is **security**.
2. This is due to the fact that it operates on Radio frequency and hence can penetrate through walls.
3. It is advisable not to use it for critical business or personal data transfer.
4. As HomeRF technology operates on same frequency, It has interference from it.
5. The bandwidth is lower compare to WiFi.
6. Battery usage is more compare to the condition when bluetooth is powered OFF.

Q4. Explain how a Bluetooth network is established using baseband state translations.

Ans: **[P | Medi**

DEVICE DISCOVERY & NETWORK ESTABLISHMENT:

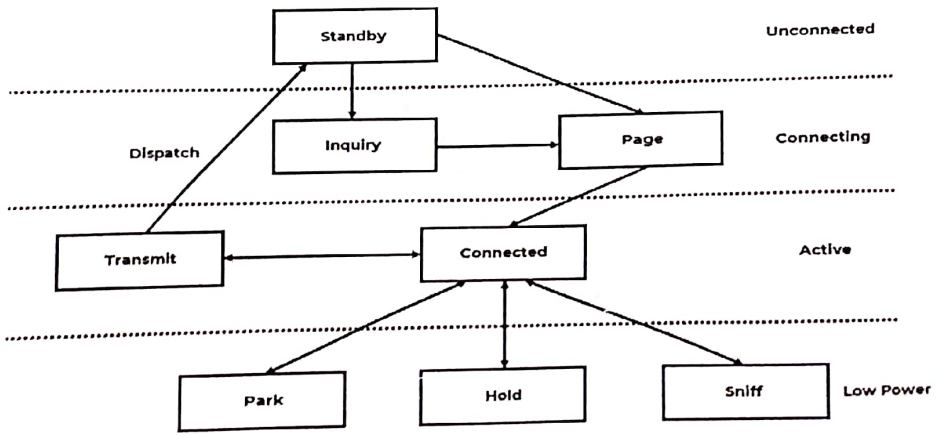


Figure 4.5: Baseband Stages.

Scanned by CamScanner

1. As shown in figure 4.5, the establishment of a Bluetooth network goes through five stages i.e. Standby, Inquiry, Page, Transmit and connected.
2. Initially, all devices within the standard range (10m) are in the **standby mode**, and they do not know about each other.
3. To know about its neighbors, the device initiates an **inquiry** as a request for information about other devices in its vicinity.
4. The inquired devices respond by sending an inquiry response to the inquiring devices.
5. After this phase, the inquiring device becomes aware of other devices in its range, but no connection is yet established.
6. To start a connection, the device sends a **page** to the intended device.
7. The paged device will respond and starts a connection procedure and the two get **connected**.
8. A device in the connected state can also inquiry and page, this is used to establish scatternets.
9. If the device is not **transmitting**, it can disconnect itself and go to standby by detach method.
10. Once the device is connected, a Bluetooth has the choice to go into either of the three low-power states which are:

a. Sniff:

- Out of all the three low power states, this one has maximum power consumption.
- It is used to sniffs data.

b. Hold:

- The device here stops all ACL link transmissions.
- If no activity is there in the piconet, the slave reduce the power consumption or participates in another piconet.

c. Park:

- This state has the lower duty cycle and lowest power consumption of the three.
- It remains a member of the piconet but gives a chance for another device to become active.

Q5. Explain functioning of Bluetooth Baseband layer. **[P | Medium]**

Ans:

BLUETOOTH BASEBAND LAYER:

1. The Baseband is the **physical layer** of the Bluetooth.
2. This layer lies on top of the Bluetooth radio layer in the bluetooth protocol stack.
3. The access method used in Bluetooth Baseband Layer is **TDMA**.
4. It is responsible for following functions:
   a. Constructing and decoding packets.
   b. Encoding and managing error correction.
   c. Encrypting and decrypting for secure communications.
   d. Maintaining synchronization.
   e. Controlling the radio.

Scanned by CamScanner

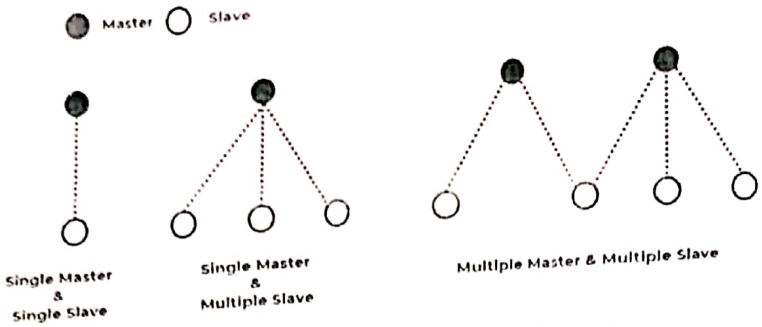


Figure 4.6: Bluetooth Baseband Spectrum.

1. Figure 4.6 shows the Bluetooth Baseband Spectrum of master & slave.
2. Bluetooth operates in 2.4 GHz ISM Band.
3. Bluetooth baseband layer uses physical channel.
4. This channel is represented by a **pseudo-random hopping sequence** hopping through the 79 or 23 RF channels.
5. Two or more Bluetooth devices using the same channel form a **piconet**.
6. There is one master and one or more slave(s) in each piconet.
7. The hopping sequence is unique for the piconet and is determined by the Bluetooth device address (BD_ADDR) of the master.
8. The phase in the hopping sequence is determined by the Bluetooth clock of the master.
9. The channel is divided into **time slots** where each slot corresponds to an RF hop frequency.

BASEBAND HANDLES TWO TYPES OF LINKS:

SCO (Synchronous Connection-Oriented) Link:

1. The SCO link is a symmetric point-to-point link between a master and a single slave in the piconet.
2. The SCO link mainly carries voice information.

ACL (Asynchronous Connection-Less) Link:

1. The ACL link is a point-to-multipoint link between the master and all the slaves participating on the piconet.
2. Only a single ACL link can exist.

PACKET FORMAT:

Access Code	Header	Payload

I) Access Code:

1. Access code is used for timing synchronization, offset compensation, paging and inquiry.
2. There are three different types of Access code:
   a. Channel Access Code (CAC).
   b. Device Access Code (DAC).
   c. Inquiry Access Code (IAC).

Scanned by CamScanner

3. The channel access code identifies a unique piconet while the DAC is used for paging and its responses. IAC is used for inquiry purpose.

II) **Header:** The header contains information for packet acknowledgement, packet numbering, flow control, slave address and error check for header.

III) **Payload:** The packet payload can contain either voice field, data field or both. It has a data field; the payload will also contain a payload header.

Q6. What is hidden and exposed terminal problem in WLAN? Discuss solutions to these problems [P | High]

Ans:

HIDDEN & EXPOSED TERMINAL PROBLEM:

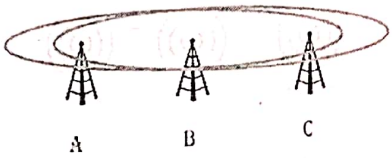


Figure 4.7: Hidden & Exposed Station Problem.

1. Consider following three mobile phone as shown in figure 4.7.
2. The transmission range of A reaches B but not C.
3. Similarly, the transmission range of C reaches B but not A.
4. And the transmission range of B reaches both A and C.

HIDDEN STATION (TERMiNAL):

1. Initially, 'A' sense the channel and since it finds the channel free, 'A' transmits to 'B'.
2. While 'A' is transmitting, 'C' also wants to transmit to 'B'.
3. Now 'C' sense the channel.
4. 'C' does not hear A's transmission because 'A' is out of range of 'C'.
5. 'C' concludes that the channel is free and starts transmitting to 'B'.
6. Signal from 'A' and 'C' both collide at 'B'.
7. 'A' is hidden to 'C' and vice versa.
8. Thus, hidden terminals may cause collisions.

EXPOSED TERMINAL:

1. Exposed terminals only cause **unnecessary delays**.
2. Consider a situation that 'B' wants to send data to 'A'.
3. 'B' sense the channel and finds it free and hence transmits to 'A'.
4. Now 'C' also wants to talk to some other mobile phone outside the interference ranges of 'A' and 'B'. Example: 'D'
5. 'C' senses the carrier and detects that the carrier is busy.
6. 'C' concludes that the channel is busy and does not transmit.

Scanned by CamScanner

SOLUTION TO HIDDEN TERMINAL:

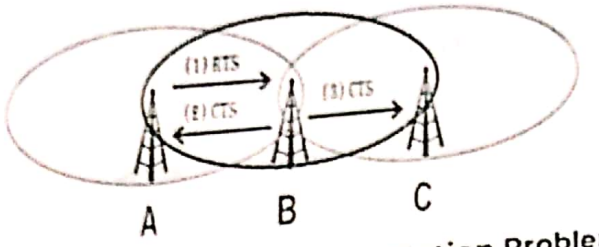


Figure 4.8: Solution to Hidden Station Problem.

1. As shown in Figure 4.8, terminal C is hidden from A and vice versa.
2. Initially A transmits a RTS signal to B.
3. This RTS contains:
   a. Name of Sender i.e. A
   b. Name of Receiver i.e. B.
   c. Length of Future Transmission.
4. This RTS is not heard by C as it is not within A's range.
5. On receiving RTS, B sends a CTS signal to A, indicating that it is ready to receive data.
6. This CTS is also heard by C.
7. C now knows that the medium is reserved by B and it does not try to transmit to B for the duration of time indicated by CTS.
8. Thus, there can be no collision at B and hence hidden terminal problem is solved.

SOLUTION TO EXPOSED TERMINAL:

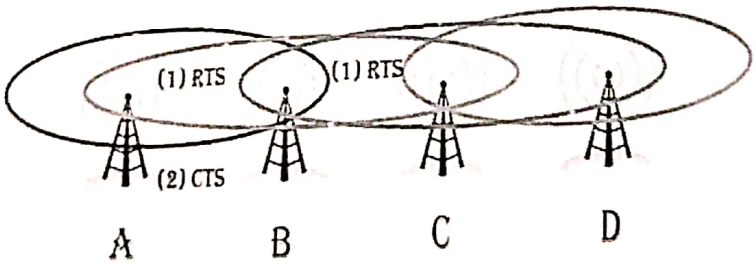


Figure 4.9: Solution to Exposed Station Problem.

1. As shown in Figure 4.9, terminal 'C' is exposed from 'B'.
2. 'B' wants to send data to 'A'.
3. 'C' also wants to send data to someone else let say it as 'D'.
4. Initially 'B' sends a RTS signal to 'A'.
5. This RTS is also heard by 'C'.
6. On receiving RTS, 'A' sends a CTS signal to 'B', indicating that it is ready to receive data.
7. However, this CTS is not heard by 'C'.
8. Hence 'C' can conclude that A is outside its detection range.

Thus, 'C' can start transmission to 'D' as it known that it cannot cause a collision at A

Scanned by CamScanner

Q7. Explain in detail HIPERLAN/1 physical layer.

Ans: **[P | Medium]**

HIPERLAN/1:

1. HiperLAN stands **High Performance Radio LAN**.
2. It is **Wireless LAN Standard**.
3. It is defined by the **European Telecommunications Standards Institute (ETSI).**
4. HiperLAN 1 is the first version of HiperLAN.
5. HiperLAN 1 supports both **Infrastructure based** and **Adhoc Networks**.

HIPERLAN/1 PHYSICAL LAYER:

1. The functions of HiperLAN/1 Physical Layer are as follows:
   a. Modulation and Demodulation.
   b. Bit and frame synchronization.
   c. Forward error correction mechanisms.
   d. Channel Sensing.
2. HiperLAN/1 provides **3 mandatory** and **2 optional channels**.

   Mandatory Channels:
   a. **Channel 0:** 5.18 GHz.
   b. **Channel 1:** 5.20 GHz.
   c. **Channel 2:** 5.22 GHz.

   Optional Channels:
   a. **Channel 3:** 5.25 GHz.
   b. **Channel 4:** 5.27 GHz.
3. HiperLAN/1 uses **Non Differential Gaussian Minimum Shift Keying** (GMSK).
4. It uses **Decision Feedback Equalizer** (DFE) to remove inter symbol interference.
5. To minimize the error at physical layer, it uses **BCH Error Correcting Codes**.
6. This code is able to correct a single error and detect two random errors.
7. Figure 4.10 shows HiperLAN/1 Data Packet format used at physical layer.
8. It shows the Data Packet & ACK Packet.

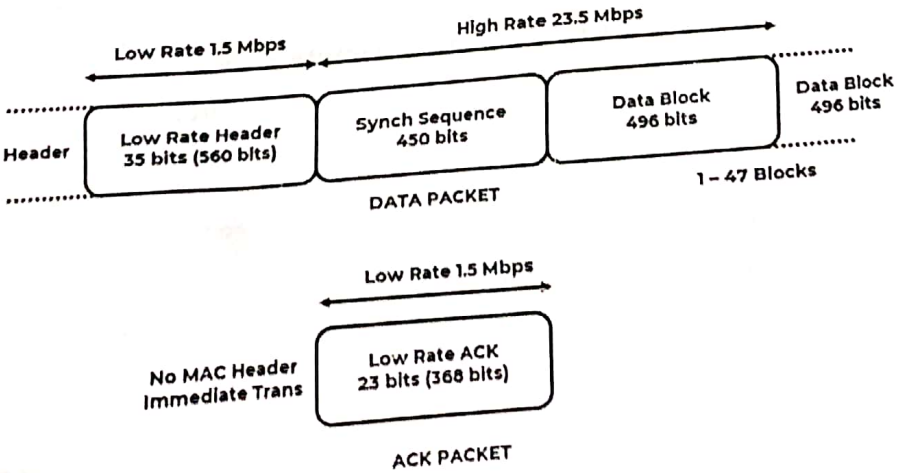


Figure 4.10: HiperLAN/1 Physical Layer Packet Format.

Scanned by CamScanner

Q8. Explain Hiperlan2 [P | Medium]

Ans:

HIPERLAN 2:

1. HiperLAN stands **High Performance Radio LAN**.
2. It is **Wireless LAN Standard**.
3. It is defined by the **European Telecommunications Standards Institute (ETSI).**
4. HiperLAN 2 is the second version of HiperLAN.
5. HiperLAN 2 allows interconnection in almost any type of fixed network.

FEATURES:

1. It operates at 5 GHz frequency band.
2. It provides connection oriented service.
3. It provides security and mobility support.
4. Power saving feature is available.
5. It provides quality of service support.
6. It is network and application independent.
7. High speed transmission up to 54 Mbit/s.

HIPERLAN 2 ARCHITECTURE:

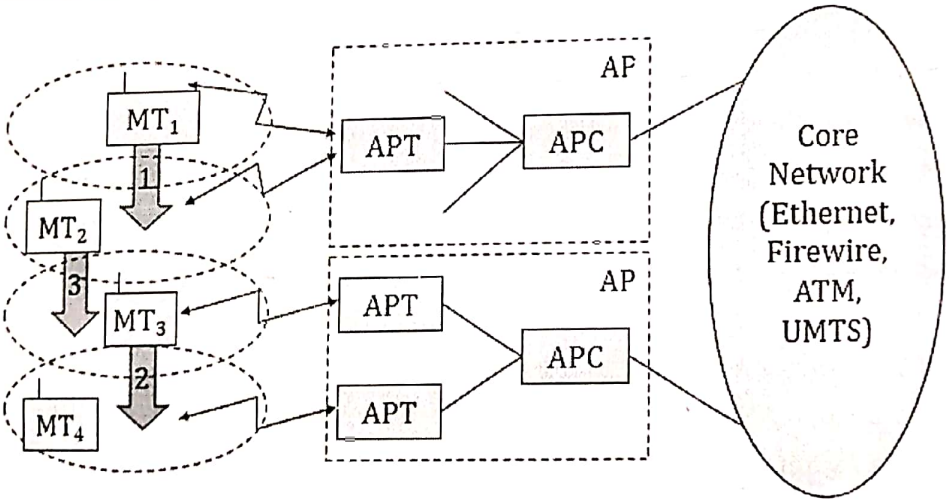


Figure 4.11: HiperLAN 2 Architecture.

1. HIPERLAN/2 is designed to work in two configurations: business environment and home environment.
2. Business environment is an access network which consists of several APs connected by a core network.
3. Each AP serves a number of mobile terminals.
4. HIPERLAN/2 also allows roaming between the AN.
5. In home environment, an ad hoc network is created.
6. Figure 4.11 presents the standard architecture of HIPERLAN/2 network.
7. Two access points are connected to a core network.
8. The Core network might be an ATM network, Ethernet LANs, UMTS 3G cellular network etc.
9. Each access point contains two parts: an Access Point Controller (APC) and one or more Access Point Transceiver (APT).

Scanned by CamScanner

10. Four mobile terminals (MT) are also shown in Figure 6.10.
11. These MTs can move from one cell area to another.
12. The access point automatically selects a frequency by using (dynamic frequency selection) DFS.

NETWORK OPERATING MODES IN HIPERLAN 2:

I) Centralized Mode (CM):

1. This is an infrastructure based and mandatory mode.
2. All APs are connected to a core network and MTs are associated with Aps.
3. If two MTs share the same cell then all data is transferred by AP.
4. AP takes complete control of everything.

II) Direct Mode (DM):

1. This is an ad-hoc and optional mode.
2. In this mode, data is directly exchanged other between MTs if they can receive each other.
3. But the network is still controlled by AP that contains a central controller (CC).
4. The central controller can be connected to a core network and can operate in both centralized and direct modes.

Q9. Explain in Detail IEEE 802.11 MAC sublayer **[P | Medium]**

Ans:

IEEE 802.11:

1. IEEE 802.11 is a set of standards for implementing **Wireless Local Area Network** (WLAN).
2. It operates in 2.4, 3.6 and 5 GHz frequency bands.
3. They are created and maintained by the **Institute of Electrical and Electronics Engineers** (IEEE) **LAN/MAN Standards Committee** (IEEE 802).
4. 802.11 has various versions such as 802.11a, 802.11b, 802.11g etc.

IEEE 802.11 MAC SUBLAYER:

1. IEEE 802.11 MAC Sublayer is used to **define addressing and frame format**.
2. It is also used to **handle access mechanism**.
3. IEEE 802.11 defines two MAC Sub layers i.e. **DCF & PCF**.
4. **DFC:**
   a. DCF Stands for **Distributed Coordination Function**.
   b. It provides Asynchronous Data Service.
   c. It is mandatory traffic services.
5. **PCF:**
   a. PCF Stands for **Point Coordination Function**.
   b. It provides Time-Bounded Service.
   c. It is optional traffic services.

Scanned by CamScanner

MAC SUBLAYER FRAME FORMAT:

Figure 4.12 shows the general MAC Sublayer Frame Format of IEEE 802.11

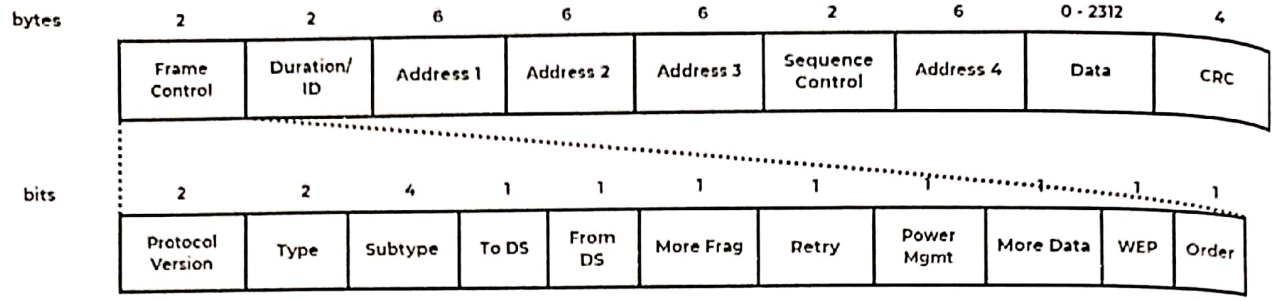


Figure 4.12: IEEE 802.11 MAC Sublayer Frame Format.

1. **Frame Control:** It carries the instructions on the nature of the packet. It contains several sub-fields.
   a. **Protocol Version:** It shows the current protocol version.
   b. **Type:** It determines the functions of a frame.
   c. **Subtype:** It determines the sub functions of a frame.
   d. **To DS/From DS:** It is used to control meaning of the address field.
   e. **More Fragments:** It should be set to 1 to provide more fragments.
   f. **Retry:** It is used to retry the retransmission of previous frame.
   g. **Power Management:** It is used to control the Power. Set 1 for Power Save Mode.
   h. **More Data:** This field indicates a receiver that sender has more data to send than the current frame.
   i. **Wired Equivalent Privacy (WEP):** It indicates the Standard Security Mechanism.
   j. **Order:** It indicates that the received frames must be proceeded in strict order when it is set to 1.
2. **Duration/ID:** This field is used to define the period of time.
3. **Address 1 to 4:** Four Address fields are used to identify the source, destination and access point.
4. **Sequence Control:** It is used to control Sequence numbering.
5. **Checksum:** It is used to protect frame.

Q10. Explain synchronization in 802.11 MAC management layer for both infrastructure as well Adhoc WLANs.

Ans: **[P | Medium]**

SYNCHRONIZATION:

1. Synchronization in Mobile Computing is adjustment of a clock to show the same time as another.
2. Each node in IEEE 802.11 network maintains an internal clock.
3. IEEE 802.11 uses Timing Synchronization Function (TSF) to synchronize the clocks of all nodes.
4. This synchronize clocks are needed for:
   a. Power Management.
   b. Synchronization in FHSS Hopping Sequence.

SYNCHRONIZATION PROCESS FOR INFRASTRUCTURE BASED NETWORK:

1. In Infrastructure Based Network, an access point (AP) coordinates the synchronization process.
2. Access Point transmits a special frame called **Beacon.**

Scanned by CamScanner

3. It is transmitted periodically.
4. A Beacon frame consists of a **timestamp** and other management information used for power management and roaming.
5. Other wireless nodes adjust their local clocks with beacon timestamp.
6. Node is not required to hear every beacon to stay synchronized.
7. From time to time, clock of every node is adjusted.
8. If the medium is busy, the access point postpones the transmission of the beacon frame.
9. Figure 4.13 shows Beacon Transmission in 802.11 Infrastructure Based Network.

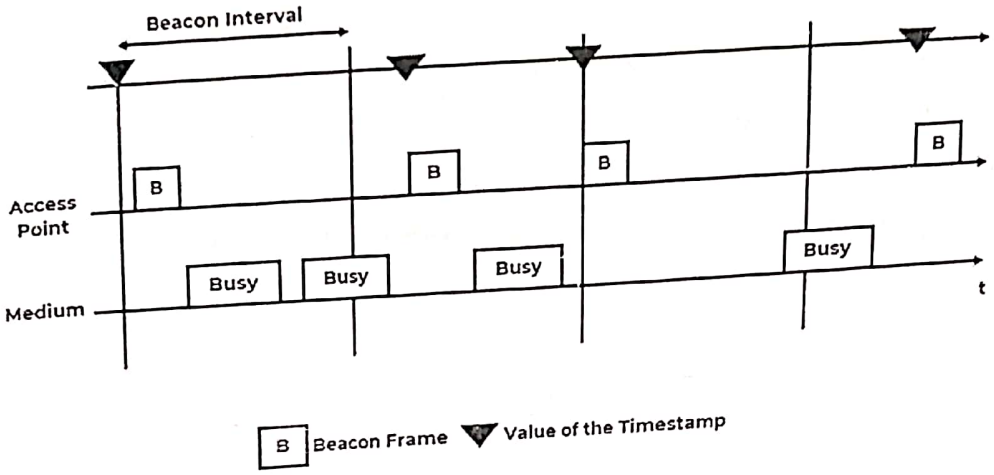


Figure 4.13: Beacon Transmission in 802.11 Infrastructure Based Network.

SYNCHRONIZATION PROCESS FOR ADHOC NETWORKS:

1. In Adhoc Network, each node within the network is responsible for synchronization process.
2. There is no Access point.
3. After each beacon interval, all stations choose random **back-off time**.
4. Only one station whose random delay time is less becomes the winner.
5. Winner can send the beacon frame.
6. All the other stations or nodes should adjust their local clock accordingly.
7. Figure 4.14 shows Beacon Transmission in 802.11 Adhoc Network.

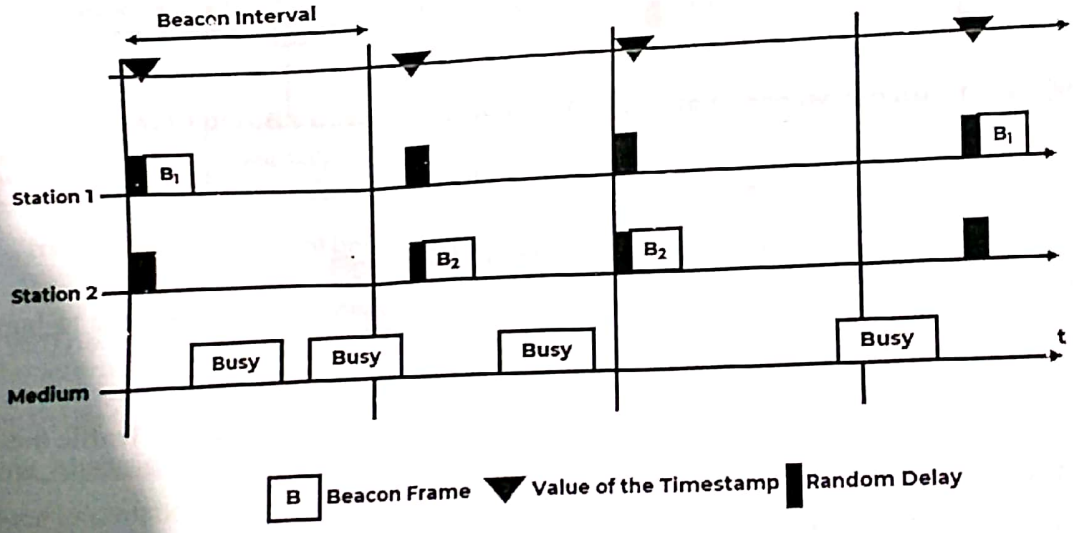


Figure 4.14: Beacon Transmission in 802.11 Adhoc Network.

Scanned by CamScanner

Q11. Explain power management in IEEE 802.11 infrastructure networks and ad-hoc networks. [P | Medium]

Ans:

POWER MANAGEMENT:

1. Power Management is the feature that turns off the power or switches the system to a low power state when inactive.
2. The basic idea to save power in WLAN is to switch off the transceiver whenever it is not needed.

POWER MANAGEMENT IN INFRASTRUCTURE BASED NETWORK:

1. In Infrastructure Based Network, an Access Point is responsible for the power management.
2. Access Point buffers data packets for all sleeping stations.
3. Access Point transmits a **Traffic Indication Map (TIM)** with a beacon frame.
4. TIM consists of a list of destinations of buffered data.
5. Additionally, the access point also maintains a **Delivery Traffic Indication Map (DTIM)** interval.
6. DTIM is used for sending broadcast/multicast frames.
7. The DTIM interval is always a multiple of TIM Intervals.
8. All stations wake up prior to an expected TIM and DTIM.
9. Figure 4.15 shows Power Management in IEEE 802.11 Infrastructure Based Network.

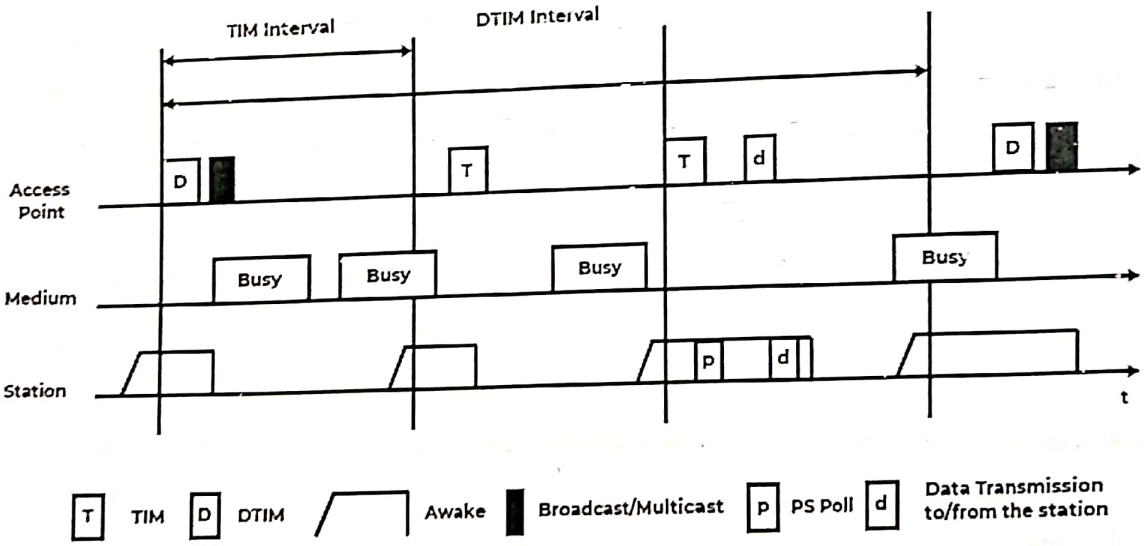


Figure 4.15: Power Management in IEEE 802.11 Infrastructure Based Network.

POWER MANAGEMENT IN ADHOC NETWORK:

1. In Adhoc Network, each station buffers data that it wants to send to power saving stations.
2. There is no access point.
3. In Adhoc Network, all stations announce a list of buffered frame during a period when they are all awake.
4. All stations announce destinations for which packets are buffered using **Adhoc Traffic Indication Map (ATIM)** during the ATIM interval.
5. Figure 4.16 shows Power Management in IEEE 802.11 Adhoc Network.

Scanned by CamScanner

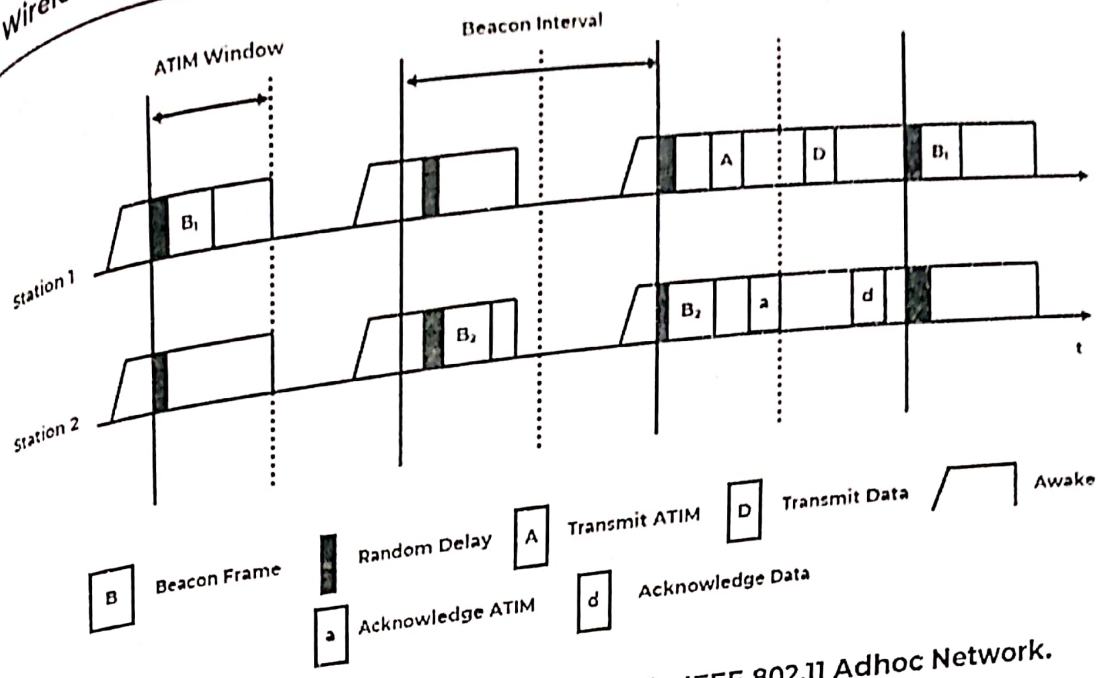


Figure 4.16: Power Management in IEEE 802.11 Adhoc Network.

Q12. **Explain Security issues in wireless communication.** **[P | High]**

Ans:

WIRELESS SECURITY:

1. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks.
2. The most common types of wireless security are **Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).**

SECURITY ISSUES IN MOBILE AND WIRELESS COMMUNICATION:

Wireless Security Issues:

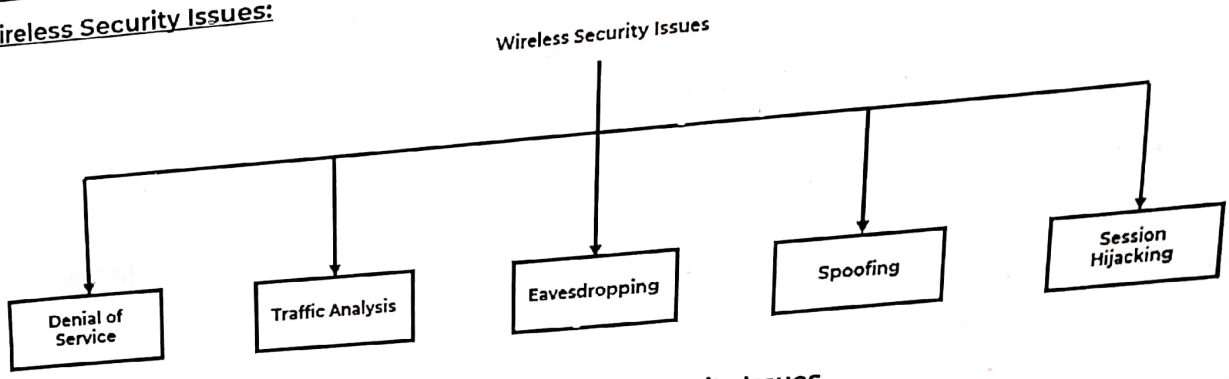


Figure 4.17: Wireless Security Issues.

I) **Denial of Service:** Denial-of-service (DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them.

II) **Traffic Analysis:** Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted.

Scanned by CamScanner

III) **Eavesdropping:** Eavesdropping is the act of intercepting communications between two points. This is done in two main ways: Directly listening to digital or analog voice communication or the interception or sniffing of data relating to any form of communication.

IV) **Spoofing:** Spoofing is a type of attack where an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user.

V) **Session Hijacking:** Session Hijacking is the act of taking control of a user session after successfully obtaining of an authenticate session id.

Device Security Issues:

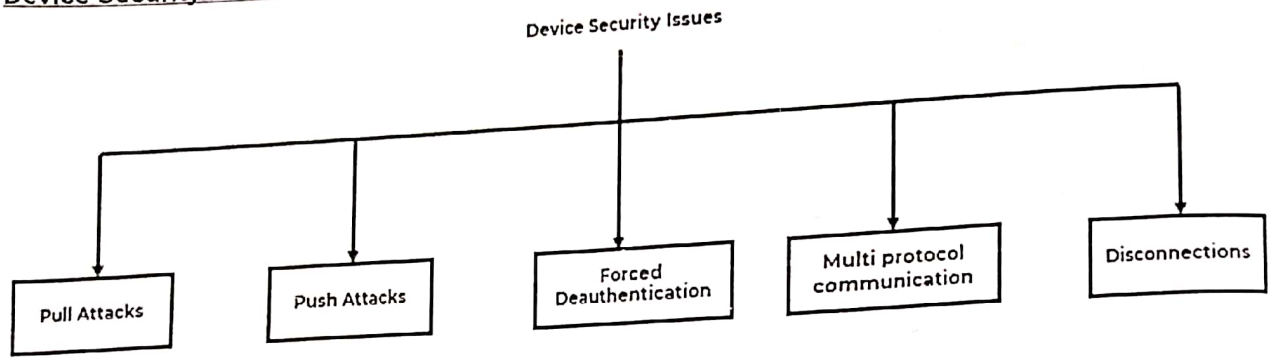


Figure 4.18: Device Security Issues.

I) **Pull Attacks:** In Pull Attack, the attacker controls the device as source of propriety data and control information.

II) **Push Attacks:** Push Attack is creation a malicious code at mobile device by attacker and he may spread it to affect on other elements of the network.

III) **Forced De-authentication:** The attacker convinces the mobile end-point to drop its connection and reconnection to get new signal, then he inserts his device between a mobile device and the network.

IV) **Multi-protocol Communication:** It is the ability of many mobile devices to operate using multiple protocols.

V) **Disconnections:** When the mobile devices cross different places it occurs a frequent disconnections caused by external party resulting **handoff.**

Q13. WEP

Ans: **[P | Medium]**

WEP:

1. *WEP* Stands for **Wired Equivalent Privacy.**
2. *It is a security protocol.*
3. *Wired Equivalent Privacy* is the encryption algorithm built into the 802.11 (Wi-Fi) standard.
4. *WEP encryption* uses the RC4stream cipher with 40 or 104 bit keys and a 24 bit initialization vector.
5. *It is defined by the IEEE* 802.11 standard and is intended to provide a level of data confidentiality that is *equivalent to a wired network.*
6. *WEP provides data confidentiality* by encrypting the data sent between wireless nodes.
7. *WEP encryption is indicated* by setting a WEP flag in the MAC header of the 802.11 frame.

Scanned by CamScanner

WEP provides data integrity for random errors by including an integrity check value (ICV) in the encrypted portion of the wireless frame.

WEP defines two shared keys:

a. The multicast/global key is an encryption key that protects multicast and broadcast traffic between a wireless AP and all of its connected wireless clients.

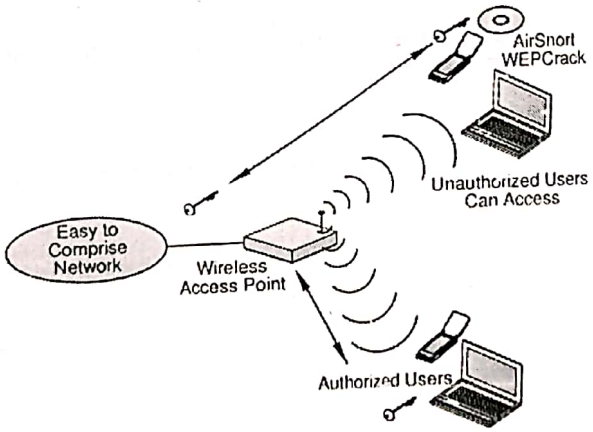
b. The unicast session key is an encryption key that protects unicast traffic between a wireless client and a wireless AP, and multicast and broadcast traffic sent by the wireless client to the wireless AP.

WEP ENCRYPTION:

An encrypted frame is produced as follows:

1. A 24-bit integrity check value (ICV) is calculated to provide data integrity for the MAC frame.
2. The ICV is appended to the end of the frame data.
3. A 24-bit initialisation vector (IV) is appended to the WEP encryption key.
4. The combination of [IV+WEP encryption key] is used as the input to a pseudo-random number generator (PRNG) to generate a bit sequence the same size as the combination of [data+ICV].
5. The PRNG bit sequence, also known as the key stream, is bit-wise exclusive ORed (XORed) with [data+ICV] to produce the encrypted portion of the payload sent between the wireless AP and the wireless client.
6. The IV is prepended to the encrypted [data+ICV] to create the payload for the wireless MAC frame. The result is IV+encrypted [data+ICV].

WEP SECURITY ISSUES:



1. WEP has led a troubled existence due to many security issues.
2. The security issues with Wired Equivalent Privacy (WEP) include:
   a. A high percentage of wireless networks have WEP disabled because of the administrative overhead of maintaining a shared WEP key.
   b. WEP has the same problem as all systems based upon shared keys: any secret held by more than one person soon becomes public knowledge.
   c. The initialization vector that seeds the WEP algorithm is sent in the clear.
   d. The WEP checksum is linear and predictable.

Scanned by CamScanner

Q14. WPA

Ans: [P | Medium]

WPA

1. WPA stands for **Wi-Fi Protected Access**.
2. WPA is a security protocol designed to create secure wireless (Wi-Fi) networks.
3. It is similar to the WEP protocol, but offers improvements in the way it handles security keys and the way users are authorized.
4. For an encrypted data transfer to work, both systems on the beginning and end of a data transfer must use the same encryption/decryption key.
5. While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that the systems use.
6. This prevents intruders from creating their own encryption key to match the one used by the secure network.
7. WPA also implements something called the Extensible Authentication Protocol (EAP) for authorizing users.
8. Instead of authorizing computers based soley on their MAC address, WPA can use several other methods to verify each computer's identity.
9. This makes it more difficult for unauthorized systems to gain access to the wireless network.
10. WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets.
11. TKIP is much stronger than a CRC, but the algorithm used in WPA2 is stronger.

Q15. Explain the difference between Adhoc Network and infrastructure based wireless networks. [P | High]

Ans:

Table 4.1: Difference between Adhoc Network and Infrastructure Based Network.

Infrastructure Based Network	Adhoc Network
It is Infrastructure depended network.	It is Infrastructure less network.
All communication process is done through Access Point.	All communication is direct.
It requires Association.	It does not requires Association.
High setup cost.	Cost – Effective.
Large setup time is required.	Less setup time is required.
Centralized Routing is used.	Distributed Routing is used.
It has Single hop Wireless link.	It has Multi hop wireless link.
IEEE 802.11 & HIPERLAN 2 are based on Infrastructure based Network.	Bluetooth is based on Adhoc Network.
It uses TDMA based protocols.	It uses CSMA Protocols.
Stable Connectivity.	Irregular Connectivity.

Scanned by CamScanner

Q16. Compare various IEEE 802.11x standards (a/b/g/i/n etc.). [P | Low]

Ans:

Table 4.2: Difference between Various IEEE 802.11X Standards.

Parameters	IEEE 802.11	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Operates at	2.4 GHz.	5 GHz.	2.4 GHz.	2.4 GHz.	5 GHz or 2.4 GHz.
Channel Width	20 MHz.	20 MHz.	20 MHz.	20 MHz.	20 MHz or 40 MHz.
Maximum Data Rate	2 Mbps.	54 Mbps.	11 Mbps.	54 Mbps.	300 Mbps.
Modulation	DSSS & FHSS.	OFDM.	DSSS or CCK.	DSSS or CCK or OFDM.	DSSS or CCK or OFDM.
Typical Range	66 Feet.	75 Feet.	100 Feet.	150 Feet.	150 Feet.
Antenna Configuration	1x1 SISO.	1x1 SISO.	1x1 SISO.	1x1 SISO(Single Input-Single Output)	4x4 MIMO (Multiple Input-Multiple Output)
Applications	WLAN	WLAN	WLAN		-

Q17. Comparison between IEEE 802.11, HIPERLAN 1, HIPERLAN 2 and Bluetooth. [P | High]

Ans:

Table 4.3: Comparison between IEEE 802.11, HIPERLAN 1, HIPERLAN 2 and Bluetooth.

Parameters	IEEE 802.11a	IEEE 802.11 b	HIPERLAN 1	HIPERLAN 2	Bluetooth
Architecture	Infrastructure based Architecture with additional support for Adhoc Networks.	Infrastructure based Architecture with additional support for Adhoc Networks.	Infrastructure based Architecture with additional support for Adhoc Networks.	Infrastructure based Architecture with additional support for Adhoc Networks.	Adhoc Network
Connection	Point-to-Point.	Point-to-Multipoint.	Provide Multi hop routing.	Point-to-Multipoint.	Point-to-Multipoint.
Connectivity	Connectionless.	Connectionless.	Connectionless.	Connection-oriented.	Connectionless and Connection-oriented.
Application	Wireless Network.	Wireless Network.	Wireless LAN.	Access to ATM Fixed Network.	Wireless Network.
Network Support	Ethernet.	Ethernet.	Ethernet.	Ethernet, IP, ATM, PPP and UMTS.	PPP and Ethernet.

Scanned by CamScanner

Regional Support	US.	US/Asia.	Europe.	Europe.	Worldwide.
Power	Medium High.	Medium.	Medium.	Medium High.	Very Low.
Cost	High.	Medium.	Medium.	High.	Very Low.
Multiple Access Technology	OFDM.	DSSS.	GMSK.	ODFM.	FHSS.
Frequency	2.4 GHz.	5 GHz.	5 GHz.	5 GHz.	2.4 GHz.
Max Data Rate	2 Mbps.	54 Mbps.	23.5 Mbps.	54 Mbps.	< 1 Mbps.
User Throughput	6 Mbps.	34 Mbps.	< 20 Mbps.	34 Mbps.	< 1 Mbps.
Error Control	ARQ.	ARQ and FEC at physical layer.	FEC at physical layer.	ARQ/FEC at physical layer.	ARQ/FEC at MAC layer.
Authentication	None.	None.	None.	x.509.	Yes.
Medium Access	CSMA/CA.	CSMA/CA.	Variant of CSMA/CA.	CSMA/CA.	Master is responsible for Medium Access.

Scanned by CamScanner

CHAP - 5: MOBILITY MANAGEMENT

Q1. Cellular IP [P | Medium]

Ans:

CELLULAR IP:

1. Cellular IP is a **network protocol standard** of routing functionality for mobile subscribers in IP Networks.
2. It allows **hierarchical routing** in collaboration with Mobile IP.
3. Cellular IP is robust, simple and flexible protocol for highly mobile hosts.
4. It complements Mobile IP by supporting **Local Mobility**.

CELLULAR IP ARCHITECTURE:

1. Figure 5.1 shows the Architecture of Cellular IP.
2. It consists of three major components:
   a. Cellular IP Gateway.
   b. Cellular IP Node or the Base Station (BS).
   c. Cellular IP Mobile Host.

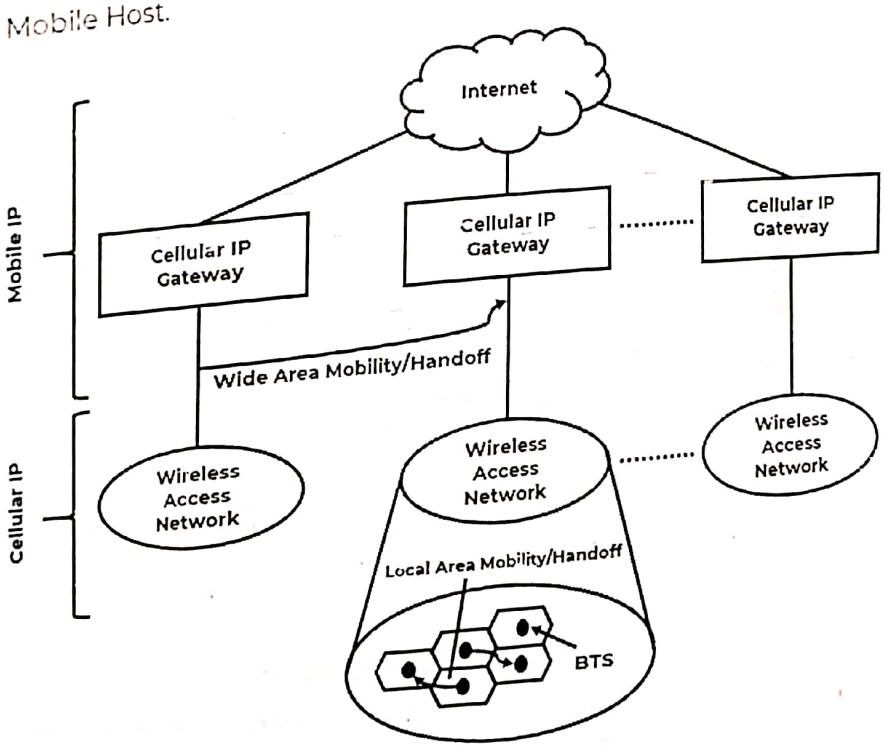


Figure 5.1: Cellular IP Architecture.

3. An important component of a cellular IP network is the base station.
4. A cellular IP network consists of several interconnected BSs.
5. The BS communicates with Mobile Hosts via **Wireless Interface**.
6. Cellular IP Gateway router connects a cellular IP network and the regular internet.

Advantages:

1. Cellular IP Provides easy global migration.
2. Flexible Handoff.

Scanned by CamScanner

Q2. MIPv6 [P | Medium]

Ans:

MIPV6:

1. MIPv6 is a protocol developed as a subset of Internet Protocol version 6 (IPv6) to support mobile connections.
2. Mobile **IPv6** provides mobility support for **IPv6**.
3. It allows you to keep the same internet address all over the world, and allows applications using that address to maintain transport and upper-layer connections when changing locations.
4. It allows **mobility across homogenous and heterogeneous media**.
5. MIPv6 allows a mobile node to transparently maintain connections while moving from one subnet to another.
6. Each device is identified by its home address although it may be connecting to through another network.
7. When a mobile node is away from home:
   a. It sends information about its current location to a home agent.
   b. The home agent intercepts packets addressed to the mobile node and tunnels them to the mobile node's present location.
8. Figure 5.2 shows MIPv6 scenario.

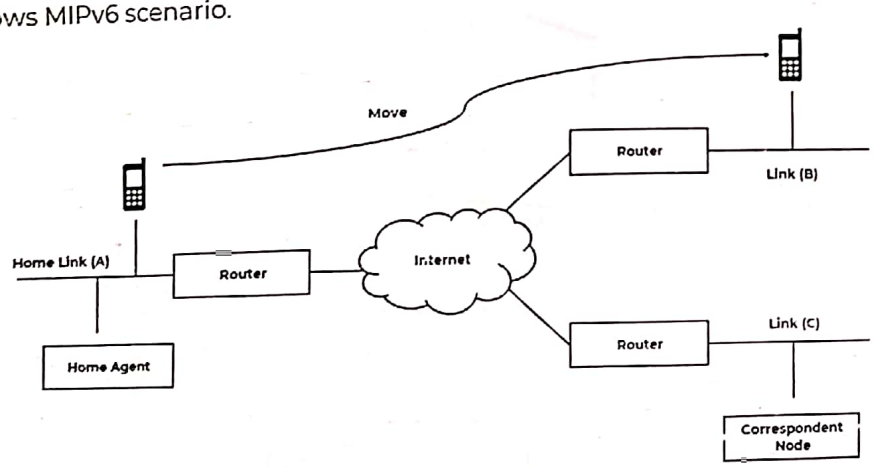


Figure 5.2: MIPv6 scenario.

9. MIPv6 supports mobility for the MN by providing it with at least two addresses: a Home Address (HoA) And Care-of Address (CoA)
10. HoA is a fixed address provided by the Home Agent (HA)
11. CoA is obtained in the foreign access network and changes when MN moves to a new subnet.

MIPV6 LOCATION UPDATE PROCEDURE:

1. When an MN stays in the home domain, it is able to receive packets destined to its HoA and being forwarded by means of conventional IP routing mechanisms.
2. When the MN crosses the boundary of its current serving network and attaches to another Access Router (AR), movement detection is performed in order to identify its new point of attachment and a new CoA is acquired.

Scanned by CamScanner

3. Once configured with a new CoA, the MN needs to send a Binding Update (BU) message to HA to register its new location.

PACKET DELIVERY PROCEDURE:

1. When the MN is away from home, the HA has a legal mobility binding and it will act as MN's proxy entity.
2. This means that any packet addressed to the MN will end up at the HA because the HA will respond to all the Neighbor Solicitation (NS) requests for the MN.
3. Once the HA has intercepted a packet, it will encapsulate the packet in a tunnel and forward it to the MN's current CoA.
4. The tunnel header will have a source address of the HA's address and destination address of the MN's CoA.
5. The MN decapsulates the packet upon its arrival to reveal the original packet, as if the Corresponding Node (CN) had sent it directly to the MN.
6. When the MN has not established a connection with its CN, it should send the packets destined to the CN via the HA using the reverse tunneling procedure.

[P | Medium]

3. FMIPv6

Ans:

FMIPV6:

1. FMIPv6 stands for **Fast Handovers for Mobile IPv6**.
2. Fast Handovers for Mobile IPv6 is an extension to Mobile IPv6.
3. Its goal is to reduce the number of packets that are lost during a handover by allowing the mobile node to use its previous Care of Address until the mobile node has completed the registration of its new Care of Address at the new access point.
4. This is done by establishing a tunnel between the two access points that allows the mobile node to send packets as if it was connected to its old access point while it is completing its handover signaling at its new access point.
5. The protocol consists of several improvements to Mobile IPv6, and the draft divides the protocol into three phases: handover initiation, tunnel establishment, and packet forwarding.
6. Figure 5.3 shows Handover in Fast Handovers for Mobile IPv6.

TERMINOLOGY OF FMIPV6:

1. **Mobile Node (MN):** A Mobile IPv6 host.
2. **Access Point (AP6):** A Layer 2 device connected to an IP subnet that offers wireless connectivity to an MN.
3. **Access Router (AR):** The MN's default router.
4. **Previous Access Router (PAR):** The MN's default router prior to its handover.
5. **New Access Router (NAR):** The MN's default router subsequent to its handover.
6. **Previous CoA (PCoA):** The MN's Care of Address valid on PAR's subnet.

Scanned by CamScanner

7. **New CoA (NCoA):** The MN's Care of Address valid on NAR's subnet.
8. **Handover:** A process of terminating existing connectivity and obtaining new IP connectivity.
9. **Router Solicitation for Proxy Advertisement (RtSolPr):** A message from the MN to the PAR requesting information for a potential handover.
10. **Proxy Router Advertisement (PrRtAdv):** A message from the PAR to the MN that provides information about neighboring links facilitating expedited movement detection.
11. **Assigned Addressing:** A particular type of NCoA configuration in which the NAR assigns an IPv6 address for the MN. The method by which NAR manages its address pool is not specified in this document.
12. **Fast Binding Update (FBU):** A message from the MN instructing its PAR to redirect its traffic (toward NAR).
13. **Fast Binding Acknowledgment (FBack):** A message from the PAR in response to an FBU.
14. **Fast Neighbor Advertisement (FNA):** A message from the MN to the NAR to announce attachment, and to confirm the use of NCoA when the MN has not received an FBACK.
15. **Handover Initiate (HI):** A message from the PAR to the NAR regarding an MN's handover.
16. **Handover Acknowledge (HAck):** A message from the NAR to the PAR as a response to HI.

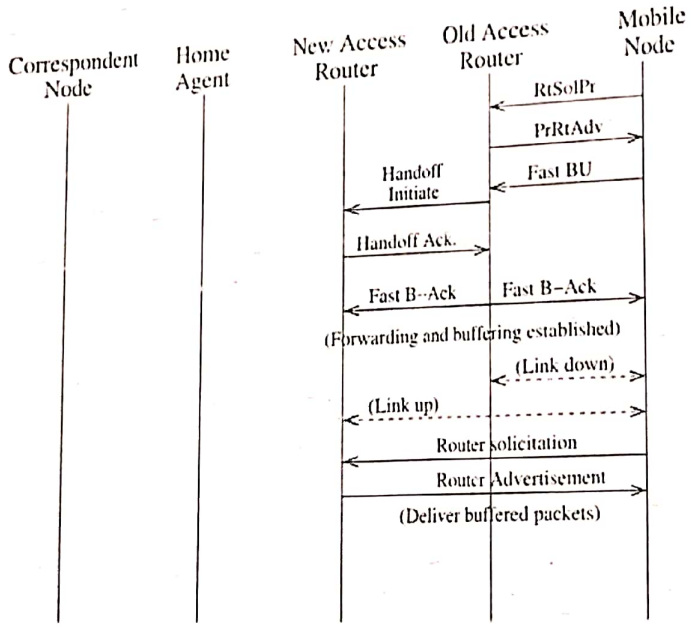


Figure 5.3: Handover in Fast Handovers for Mobile IPv6

Q4. HMIPv6

Ans:

[P | Medium]

HMIPV6:

1. HMIPv6 stands for **Hierarchical Mobile IPv6**.
2. Hierarchical Mobile IPv6 (HMIPv6) is the proposed enhancement of Mobile IPv6.
3. It is designed to reduce the amount of signaling required and to improve handoff speed for mobile connections.

Scanned by CamScanner

4. HMIPv6 is a proposed standard from the **Internet Engineering Task Force**
5. MIPv6 defines a means of managing global (between-site) mobility, but doesn't address the issue of local (within-site) mobility separately.
6. Instead, it uses the same mechanisms in both cases, which is an inefficient use of resources in the case of local mobility.
7. HMIPv6 adds another level, built on MIPv6 that separates local from global mobility.
8. In HMIPv6, global mobility is managed by the MIPv6 protocols, while local handoffs are managed locally.
9. A new node in HMIPv6 called the Mobility Anchor Point (MAP) serves as a local entity to aid in mobile handoffs.
10. The MAP, which replaces MIPv4's foreign agent, can be located anywhere within a hierarchy of routers.
11. In contrast to the foreign agent, there is no requirement for a MAP to reside on each subnet.
12. The MAP helps to decrease handoff-related latency because a local MAP can be updated more quickly than a remote home agent.
13. Figure 5.4 represents HMIPv6 Architecture

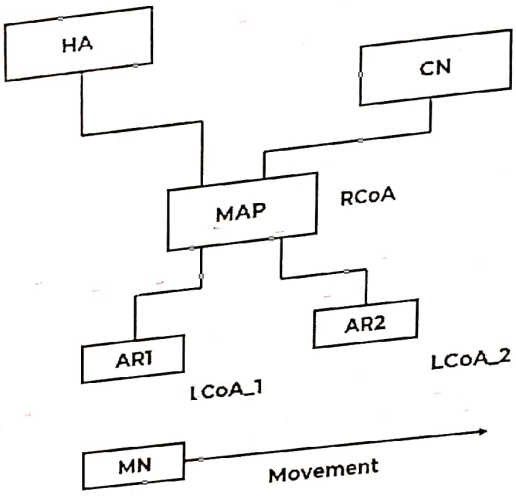


Figure 5.4: HMIPv6 Architecture.

ADVANTAGES:

1. Local COAs can be hidden, which provides some location privacy.
2. Direct routing between CNs sharing the same link is possible (but might be dangerous)

Q5. HAWAII **[P | Medium]**

Ans:

HAWAII:

1. HAWAII stands for **Handoff-Aware Wireless Access Internet Infrastructure.**
2. It is a domain-based approach for supporting mobility.
3. HAWAII also supports IP paging.
4. The architecture of HAWAII is shown in 5.5.

Scanned by CamScanner

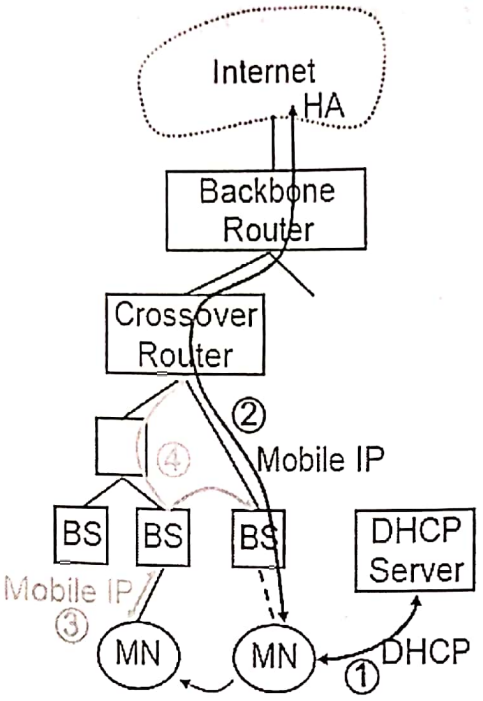


Figure 5.5: HAWAII Architecture.

Operation:

1. No HA is involved when MN is in home domain where MN is identified by its IP address.
2. When MN moves to HAWAII domain (foreign domain) , it obtains Co-located COA (CCoA)(step 1)
3. And registers with HA (step 2)
4. This CCoA remains unchanged as long as MN in foreign domain (therefore no need to notify HA unless MN moves to new domain)
5. MN sends registration request to new BS (step 3)
6. The BS intercepts registration request and sends out hand-off update message, which reconfigures all routers on the paths from the old and new BS to the so-called crossover router (step 4)
7. The BS then sends a registration reply to MN as if it were the FA

Security provisions:

1. MN-FA authentication mandatory.
2. Challenge/Response Extensions mandatory.

Advantages:

1. HAWAII is mostly transparent to mobile nodes.
2. Explicit support for dynamically assigned home addresses.

Disadvantages:

1. Security: There are no provision regarding the setup of IPSec (IP security) tunnels.
2. Implementation: No private address support is possible because of co-located COAs.

Scanned by CamScanner

CHAP - 6: LONG-TERM EVOLUTION (LTE) OF 3GPP

Q1. LTE [P | Medium]

Ans:

LTE:

1. LTE stands for **Long Term Evolution**.
2. It is a standard for 4G wireless broadband technology that offers increased network capacity and speed to mobile device users.
3. LTE offers higher peak data transfer rates -- up to 100 Mbps downstream and 30 Mbps upstream.
4. The high-level network architecture of LTE is comprised of following three main components:
   a. The User Equipment (UE).
   b. The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
   c. The Evolved Packet Core (EPC).
5. The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem.
6. The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown in figure 6.1

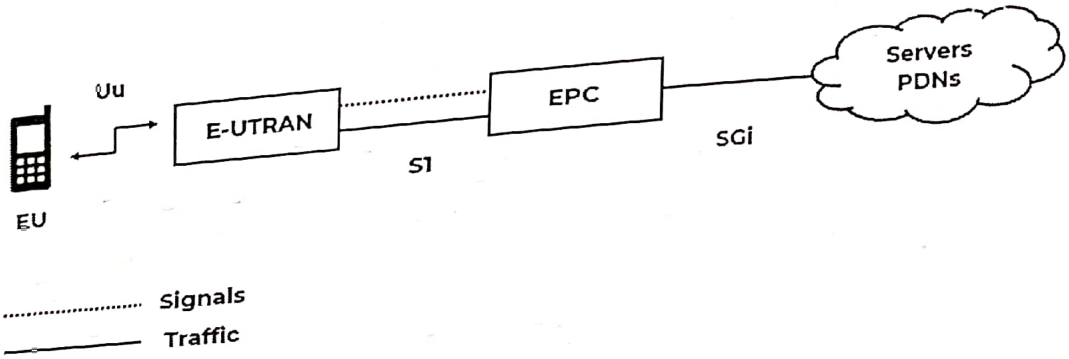


Figure 6.1: LTE Network Architecture

I) User Equipment (UE):

1. The User Equipment (UE), comprised of the following important modules:
   a. Mobile Termination (MT): Handles all the communication functions.
   b. Terminal Equipment (TE): Terminates the data streams.
   c. Universal Integrated Circuit Card (UICC): It is known as the SIM card for LTE equipment's. It runs an application known as the Universal Subscriber Identity Module (USIM)

II) E-UTRAN (The access network):

1. Handles the radio communications between the mobile and the evolved packet core.
2. E-UTRAN includes one component, the evolved base stations, called eNodeB or eNB.
3. Each eBN connects with the EPC by means of the S1 interface.
4. It can also be connected to nearby base stations by the X2 interface, which is mainly used for signaling and packet forwarding during handover.

Scanned by CamScanner

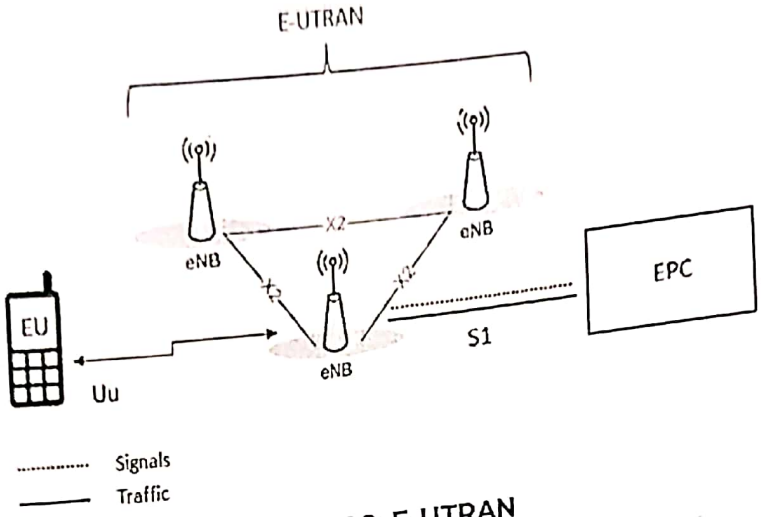


Figure 6.2: E-UTRAN

III) The Evolved Packet Core (EPC):

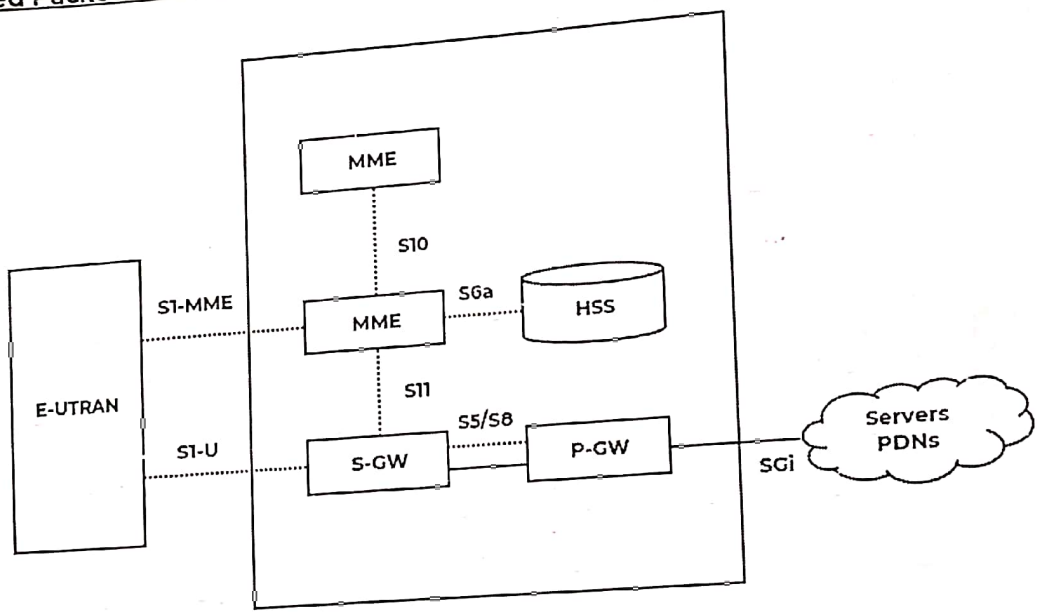


Figure 6.3: EPC

It includes following components:

1. **Home Subscriber Server (HSS):** A central database that contains information about all the network operator's subscribers.
2. **Packet Data Network (PDN) Gateway (P-GW):** It Communicates with the packet data networks PDN, using SGi interface.
3. **Serving Gateway (S-GW):** Acts as a router, and forwards data between the base station and the PDN gateway.
4. **Mobility management Entity (MME):** Controls the high-level operation of the mobile by means of signaling messages and HSS.
5. **Policy Control and Charging Rules Function (PCRF):** It is responsible for policy control decision making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF), which resides in the P-GW

Scanned by CamScanner

Q2. LTE Advanced **[P | Medium]**

Ans:

LTE Advanced (LTE - A):

1. LTE Advanced is a mobile communication standard and a major enhancement of the Long Term Evolution (LTE) standard.
2. It is a standard for mobile communication that is one generation beyond LTE (Long Term Evolution).
3. Whereas LTE was a 3G communication standard, LTE-A is a 4G or fourth generation communication standard.

LTE-A FEATURES:

1. Peak data rates: Downlink - 1 Gbps; Uplink - 500 Mbps.
2. Spectrum efficiency: 3 times greater than LTE.
3. Scalable channel bandwidth up to 40 MHz.
4. Seamless connectivity with smooth handovers across networks.
5. Global roaming with universal connectivity.
6. Service sufficient for multimedia support.

ARCHITECTURE:

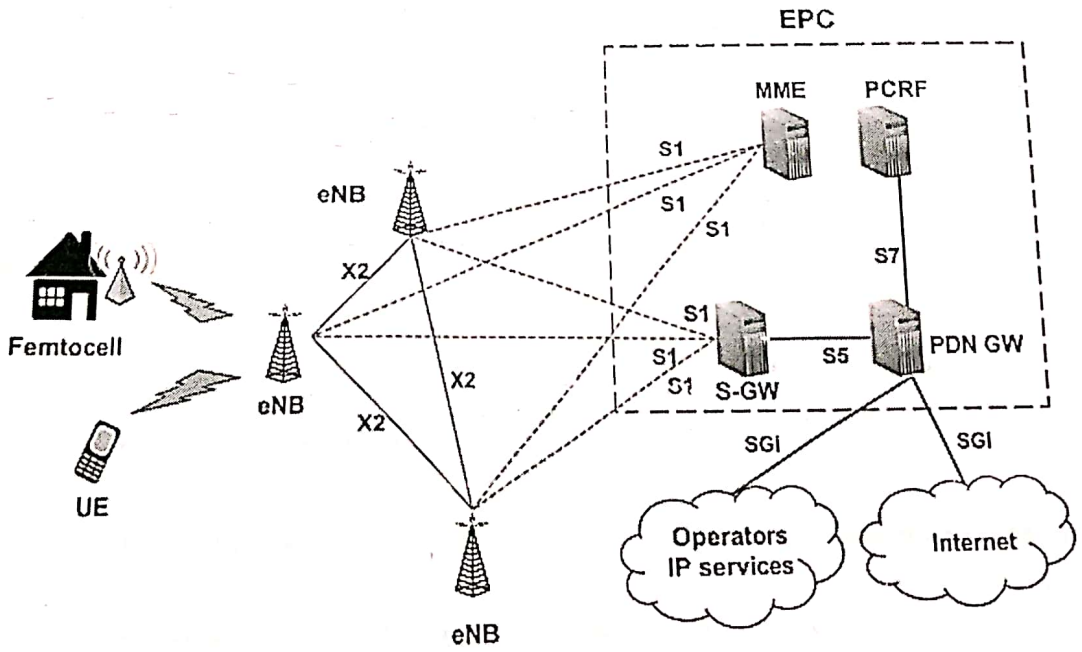


Figure 6.4: LTE Advanced Architecture.

The figure 6.4 depicts LTE Advanced (LTE-A) Architecture and consists of following components:

PDN-GW:

1. It stands for PDN Gateway.
2. It interfaced with S-GW using S5 interface and with operator's IP services using SGi interface.
3. It has connectivity with PCRP using Gx interface.

Scanned by CamScanner

Q2. LTE Advanced [P | Medium]

Ans:

LTE Advanced (LTE – A):

1. LTE Advanced is a mobile communication standard and a major enhancement of the Long Term Evolution (LTE) standard.
2. It is a standard for mobile communication that is one generation beyond LTE (Long Term Evolution).
3. Whereas LTE was a 3G communication standard, LTE-A is a 4G or fourth generation communication standard.

LTE-A FEATURES:

1. Peak data rates: Downlink - 1 Gbps; Uplink - 500 Mbps.
2. Spectrum efficiency: 3 times greater than LTE.
3. Scalable channel bandwidth up to 40 MHz.
4. Seamless connectivity with smooth handovers across networks.
5. Global roaming with universal connectivity.
6. Service sufficient for multimedia support.

ARCHITECTURE:

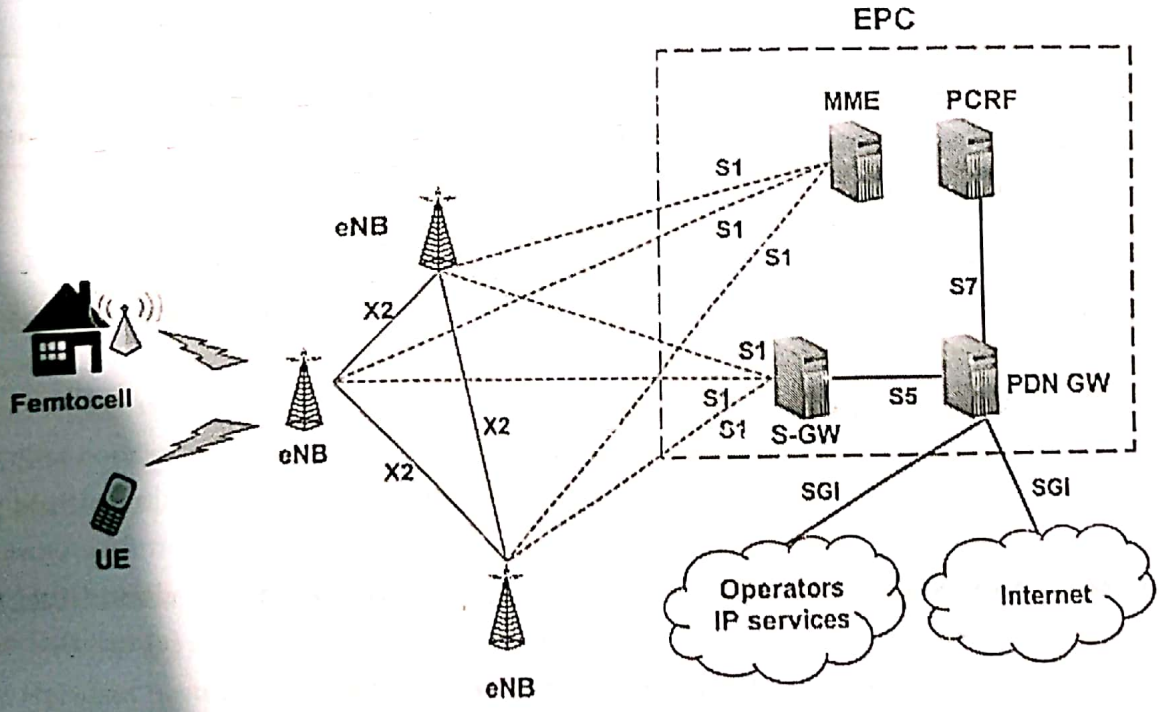


Figure 6.4: LTE Advanced Architecture.

The figure 6.4 depicts LTE Advanced (LTE-A) Architecture and consists of following components:

PDN-GW:

1. It stands for PDN Gateway.
2. It interfaced with S-GW using S5 interface and with operator's IP services using SGi interface.
3. It has connectivity with PCRP using Gx interface.

Scanned by CamScanner

4. It connects UE to packet data networks.
5. P-GW assigns IP address to the UE.
6. One UE can have connectivity with more than one PGWs in order to have access to multiple PDNs.
7. It takes care of packet filtering, policy enforcement and charging related services. Moreover it fulfils connectivity between 3GPP (LTE, LTE-A) and non 3GPP (WiMAX, CDMA etc.) technologies.

S-GW:

1. It stands for Serving Gateway.
2. It interfaces with MME using S11 interface and with SGSN using S4 interface.
3. It connects with PDN-GW using S5 interface as mentioned above.
4. EPC gets terminated at this node/entity.
5. It is connected with E-UTRAN via S1-U interface.
6. Each UE in LTE-A is associated to unique S-GW which has several functions.
7. It helps in inter-eNB handover as well as inter-3GPP mobility.
8. It helps in inter-operator charging. It does packet routing and packet forwarding.

MME:

1. It stands for Mobility Management Entity.
2. It is major control plane element in LTE advanced architecture.
3. It takes care of authentication, authorization and NAS signaling related security functions.
4. It takes care of selecting either S-GW or PDN-GW or P-GW.

S1-MME: It provides connectivity between EPC and eNBs.

eNB:

1. It is main building block or system in LTE-A.
2. It provides interface with UEs or LTE-A phones.
3. It has similar functionality as base station used in GSM or other cellular systems.
4. Each of the eNBs serve one or several E-UTRAN cells.
5. Interface between two eNBs is known as X2 interface.

HeNB:

1. It stands for Home eNodeB or Home eNB.
2. It is known as Femtocell.
3. It is used to improve coverage in the indoor region of office or home premises.
4. It can be interfaced directly to EPC or via Gateway.

HeNB-GW:

1. It provides connectivity of HeNB with S-GW and MME.
2. It aggregates all the traffic from number of Home eNBs to core network.
3. It uses S1 interface to connect with HeNBs.

Relay Node: It is used for improving network performance.

Scanned by CamScanner

Q3. VoLTE

Ans: **[P | Medium]**

VoLTE:

1. VoLTE stands for **Voice over LTE**.
2. It is a standard for high-speed wireless communication for mobile phones and data terminals
3. VoLTE is the method of **sending voice over an LTE bearer.**
4. It was introduced as the global scheme to provide seamless integration of voice and short messaging into LTE networks.

FEATURES OF VOLTE:

1. Eliminates the need to have voice on one network and data on another.
2. Improved coverage and connectivity.
3. It provides Fast Call Setup.
4. Provides a more efficient use of spectrum than traditional voice.
5. Increases handset battery life by 40 per cent (compared with VoIP).
6. Provides rapid call establishment time.

VoLTE BUILDING BLOCKS:

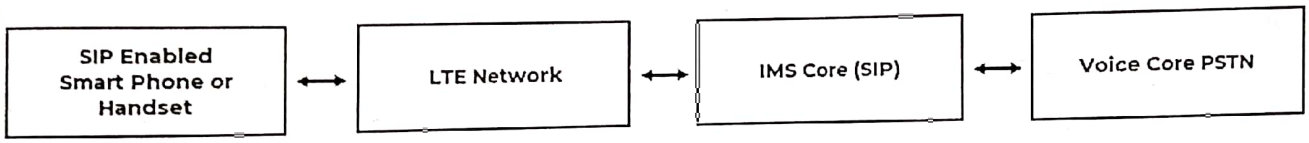


Figure 6.4: VoLTE Building Blocks.

SIP Enabled User Equipment:

1. Handset or Smartphone needs to be VoLTE Compliant where SIM should support ISIM.
2. SIP User Agent is used for making VoLTE Calls based on SIP Technology.
3. VoLTE SIM consists of following:
   a. **IP Multimedia Private Identity (IMPI):** IMPI is a global identity allocated by home network. IMPI contains home operator's domain information
   b. **IP Multimedia Public Identity (IMPU):** IMPU acts like a telephone number which can either be a SIP URI (sip:@:) or a tel URI as defined in RFC 39664 (tel :)
4. VoLTE Handset hosts Binary Application containing SIP User Agent (SIP-UA).
5. This resides in the User equipment to transmit & receive SIP messages.
6. It Provides basic telephony functionality & can act in two different roles:
   a. **User Agent Server (UAS):** Acting as Server to receive requests and send response
   b. **User Agent Client (UAC):** Acting as Client to send SIP request

LTE Network:

1. Figure 6.5 shows LTE Network in VoLTE.
2. It includes Control Plane and User Plane.

Scanned by CamScanner

3. Control plane are responsible for User Authentication.
4. Control plane nodes include EnodeB, MME, HSS, OCS & PCRF
5. User Plane includes EnodeB SGW & PGW.
6. EnodeB is Radio cell site of LTE Network & is used in both Control & User Plane.
7. PGW is also used for both User & Control Plane traffic.
8. LTE Network is just used as Bridge acting as IP Supporting Carrier for this communication.

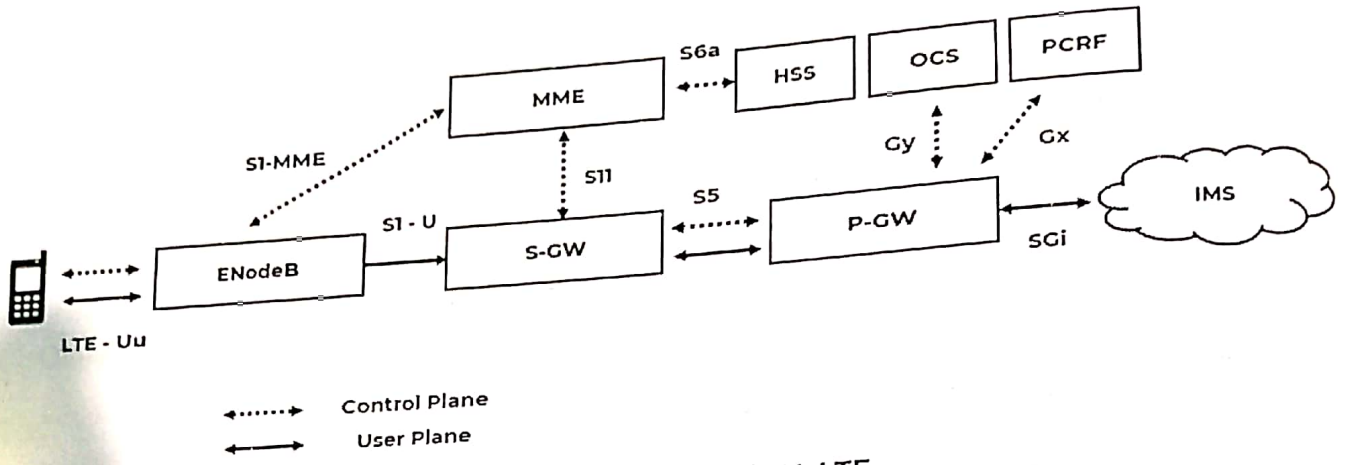


Figure 6.5: LTE Network in VoLTE

SIP Server:

1. Users are going to register with SIP Server which is Part of Control Plane & Signaling.
2. This SIP Server will setup Media Part or Payload of Voice Call with Media Gateway which is further connected to PSTN
3. SIP Server is anchoring point for Session set-up, session tear-down, session control and CDR Generation.

IMS Core:

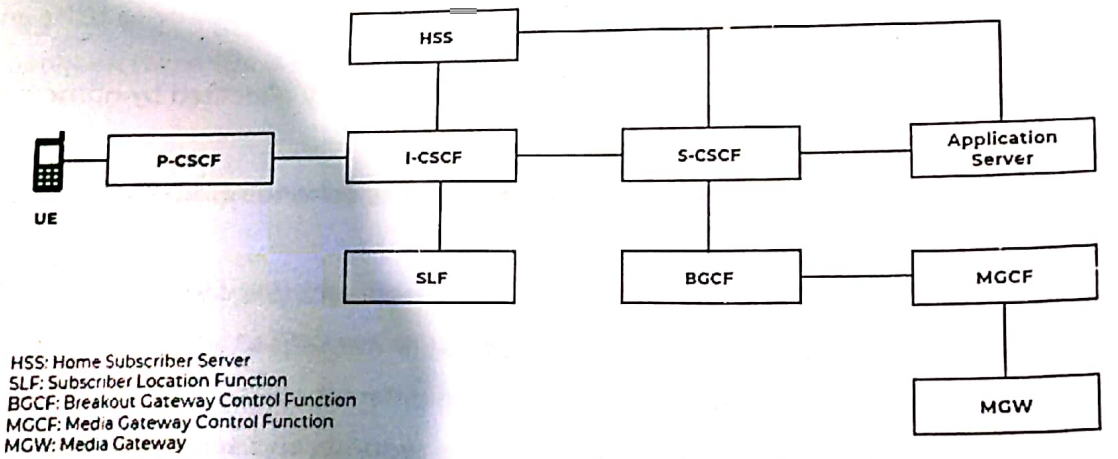


Figure 6.6: IMS Core.

IMS core has the following important nodes:

I) Call Session Control Function (CSCF)

1. CSCF is responsible for establishing, monitoring, supporting and releasing multimedia sessions.
2. It has three different functional elements which may or may not be separate physical entities.

Scanned by CamScanner

a. **Proxy CSCF:** P-CSCF is seen as the initial point of contact from any SIP User Agent. It handles all requests from the UE and is, from the UE's point of view, the "SIP proxy" to the entire subsystem.

b. **Serving CSCF:** S-CSCF has knowledge about the user and what applications are available to the user. It acts as a decision point and it's main job is to decide whether or not the user's SIP messages will be forwarded to the application servers.

c. **Interrogating CSCF:** I-CSCF is the entity that initiates the assignment of a user to an S-CSCF (by querying the HSS) during registration.

II) Home Subscriber Server (HSS):

1. HSS is a database that maintains user profile and location information and is responsible for name/address resolution.
2. HSS is also responsible for authentication and authorization.

III) Subscriber Location Function (SLF):

1. SLF is responsible for assigning HSS to user in home network.
2. To achieve this function SLF keeps track of all HSSes.

IV) Media Gateways:

1. Media Gateway resides at the interface between SIP based IMS network and traditional PSTN network.

V) Media Gateway Control Function (MGCF):

1. Media Gateway Control Function controls media gateways, converts codecs where necessary and may serve as a breakout to a circuit-switched network.
2. In the case when MGCF works as a breakout to CS network it is also responsible for managing the conversion of signaling messages, converting SIP messaging to the Bearer Independent Call Control (BICC) and ISDN User Part (ISUP) protocols used in legacy systems.

VI) Breakout Gateway Control Function (BGCF):

1. When Media Gateway Control Function does not include breakout to circuit-switched network, BGCF takes care of this functionality.

Q4. LTE SON **[P | Medium]**

Ans:

LTE SON:

1. The LTE SON stands for **Self Organizing Networks**.
2. This concept of SON is introduced in LTE and LTE-advanced based networks to provide simple and fast installation and maintenance of the cellular networks.
3. The LTE SON features can be applied to all available types of network architectures viz. centralized, hybrid and distributed.
4. LTE SON is further divided into three major subcategories: Self configuration, Seld optimization & Self healing

Scanned by CamScanner

LTE SON FEATURES:

Following table mentions LTE SON features as per LTE standard release 8, release 9 and release 10.

LTE SON Release	Features
Release 8	▪ Automatic downloading of software. ▪ Automatic Neighbor Relation. ▪ Automatic Inventory. ▪ Automatic PCI (Physical Cell ID) assignment
Release 9	▪ RACH channel optimization. ▪ Load balancing optimization. ▪ Robustness in mobility features. ▪ Optimization of handover procedures ▪ ICIC (Inter cell interference coordination)
Release 10	▪ Self healing functionalities ▪ Coverage optimization. ▪ Capacity optimization. ▪ eICIC (enhanced inter cell interference coordination) ▪ Cell out-age detection as well as compensation. ▪ Energy savings. ▪ Avoidance of drive tests

Q5. SAE Architecture **[P | Medium]**

Ans:

SAE ARCHITECTURE:

1. SAE stands for **System Architecture Evolution**.
2. It is a new network architecture designed to simplify LTE networks and establish a flat architecture similar to other IP based communications networks.
3. SAE uses an eNB and Access Gateway (aGW) and removes the RNC and SGSN from the equivalent 3G network architecture to create a simpler mobile network.
4. This allows the network to be built with an "All-IP" based network architecture.
5. SAE also includes entities to allow full inter-working with other related wireless technology (WCDMA, WiMAX, WLAN, etc.).
6. These entities can specifically manage and permit the non-3GPP technologies to interface directly with the network and be managed from within the same network.

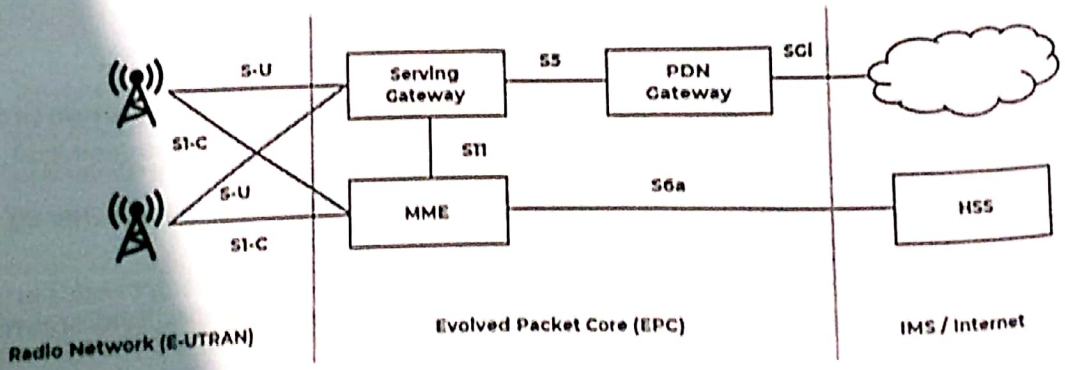


Figure 6.7: System Architecture Evolution

Scanned by CamScanner

the EPC is a key part of SAE. Major subcomponents of the LTE EPC include the MME, SGW, and PGW.

I) MME (Mobility Management Entity):

1. The MME is an important controller node in the LTE network.
2. It is responsible for:
   a. Idle mode UE (User Equipment) tracking.
   b. Paging procedure such as re-transmissions.
   c. Bearer activation and deactivation process.
   d. S-GW selection for a UE at the initial attach.
   e. Intra-LTE handover with Core Network node relocation.
   f. User authentication with HSS.
3. When the signaling of Non-Access Stratum (NAS) terminates at the MME, it generates and allocates temporary identities to UEs.
4. Then, it authorizes the UE for the Public Land Mobile Network (PLMN).
5. It is also responsible for the enforcement of UE roaming restrictions.
6. The MME handles the ciphering/integrity protection for NAS signaling and the security key management.
7. It supports lawful interception of signaling, and the control plane function for mobility between LTE and legacy networks with the S3 interface.
8. The S6a interface connects the MME to the HSS for roaming UEs.

II) SGW (Serving Gateway):

1. The main function of the Serving Gateway is routing and forwarding of user data packets.
2. It is also responsible for inter-eNB handovers in the U-plane and provides mobility between LTE and other types of networks, such as between 2G/3G and P-GW.
3. The DL data from the UEs in idle state is terminated at the SGW, and arrival of DL data triggers paging for the UE.
4. The SGW keeps context information such as parameters of the IP bearer and routing information, and stores the UE contexts when paging happens.
5. It is also responsible for replicating user traffic for lawful interception.

III) PGW (PDN Gateway):

1. The PDN Gateway is the connecting node between UEs and external networks.
2. It is the entry point of data traffic for UEs.
3. In order to access multiple PDNs, UEs can connect to several PGWs at the same time.
4. The functions of the PGW include:
   a. Policy enforcement.
   b. Packet filtering.
   c. Charging support.
   d. Lawful interception.
   e. Packet screening.

IV) HSS (Home Subscriber Server): This is a central database that contains user-related and subscription-related information.

Scanned by CamScanner

Q6. HetNet **[P | Medium]**

Ans:

HetNet:

1. HetNet stands for **Heterogeneous Network.**
2. Heterogeneous networks (HetNet) is a term used for modern mobile communications networks.
3. A modern mobile communications network is comprised of a combination of different cell types and different access technologies.
4. A typical HetNet uses a combination of legacy systems (e.g. GSM en UMTS) and modern radio access technologies such as LTE, possibly completed with Wi-Fi.
5. Figure 6.8 shows Architecture of HetNet.

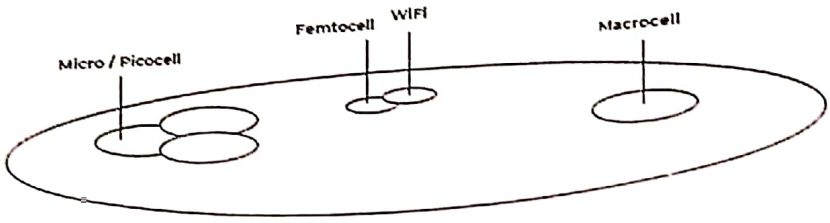


Figure 6.8: Architecture of HetNet.

Macro Cells:

1. Macro cells are the common cells sites supporting technologies like HSPA+ and LTE.
2. The normal range may vary from a few hundred meters to a few kilometres.
3. Output power is of the order of tens of watts.

Microcells:

1. Microcells typically cover smaller areas maybe up to a kilometre.
2. They usually transmit within a range of milliwatts to a few watts.
3. Microcells are deployed for providing temporary cellular coverage and capacity to places like sports stadiums, convention centres etc.
4. Sometimes, microcells may use distributed antenna systems (DAS) to improve bandwidth and reliability.

Pico Cells:

1. Pico cells offer capacities and coverage areas, supporting up to 100 users over a range of less than 250 yards.
2. Pico cells are frequently deployed indoors to improve poor wireless and cellular coverage within a building, such as an office floor or retail space.

Femtocells:

1. Femtocells are typically user-installed to improve coverage area within a small vicinity, such as home office or a dead zone within a building.
2. Femtocells can be obtained through the service provider or purchased from a reseller.
3. Unlike pico cells and microcells, femtocells are designed to support only a handful of users and is only capable of handling a few simultaneous calls.

Scanned by CamScanner

Q7. 5G [P | Medium]

Ans:

5G:

1. 5G is the **Fifth Generation technology**.
2. The 5G technology is expected to provide a new (much wider than the previous one) frequency bands along with the wider spectral bandwidth per frequency channel.

FEATURES:

1. High increased peak bit rate.
2. Larger data volume per unit area (i.e. high system spectral efficiency)
3. High capacity to allow more devices connectivity concurrently and instantaneously.
4. Lower battery consumption.
5. Better connectivity irrespective of the geographic region, in which you are.
6. Larger number of supporting devices.
7. Lower cost of infrastructural development.
8. Higher reliability of the communications.

ADVANTAGES:

1. High resolution and bi-directional large bandwidth shaping.
2. Technology to gather all networks on one platform.
3. More effective and efficient.
4. Technology to facilitate subscriber supervision tools for the quick action.
5. Most likely, will provide a huge broadcasting data (in Gigabit), which will support more than 60,000 connections.
6. Easily manageable with the previous generations.
7. Technological sound to support heterogeneous services (including private network).
8. Possible to provide uniform, uninterrupted, and consistent connectivity across the world.

DISADVANTAGES:

1. Technology is still under process and research on its viability is going on.
2. The speed, this technology is claiming seems difficult to achieve (in future, it might be) because of the incompetent technological support in most parts of the world.
3. Many of the old devices would not be competent to 5G, hence, all of them need to be replaced with new one — expensive deal.
4. Developing infrastructure needs high cost.
5. Security and privacy issue yet to be solved.

Scanned by CamScanner