Times asked: 6 times
5 times
4 times
3 times
2 times
1 time

# indicates 5-mark question

# MC Question Bank

## 1.Introduction to Mobile Computing

1. What is spread spectrum? Why is it used? #
2. Explain DSSS and FHSS in detail.
3. Describe various applications of mobile devices for Vehicles, Emergency situations, Business, Entertainment.
4. Explain Signal propagation in detail. What are various signal propagation effects.
5. Compare all Mobile generations i.e. 1G, 2G, 3G, 4G and 5G.
6. Explain various types of antennas along with their radiation patterns.
7. Explain the concept of frequency reuse with clustering. #
8. What are various advantages and disadvantages of small cells in cellular systems. #
9. What is co channel interference. #

## 2. GSM Mobile Services

1. Explain GSM architecture in detail.
2. Explain handover mechanisms in GSM in detail.
3. Explain Security algorithms used in GSM for authentication and privacy (A3, A5, A8).
4. Explain GPRS architecture in detail.
5. Explain Mobile Terminated Call and Mobile Originated Call in detail.
6. What is the use of different interfaces used in GSM with diagram.
7. Explain UMTS architecture.
8. What are the roles of EIR and HLR entities in a GSM network. #
9. Discuss about the mobile services and data services in GSM. #
10. Write a short note on: CDMA #
11. Which components are new in GPRS as compared to GSM? What is their purpose?
12. Write a short note on UTRAN and UMTS network.

## 3. Mobile Networking

1. Explain packet delivery mechanism to and from mobile node with the help of Mobile IP network diagram.
2. What is Snooping TCP? What are its advantages and disadvantages.
3. Explain Mobile TCP with their merits and demerits. #
4. What do you mean by hidden and exposed station problem. How can they be avoided.
5. Write a short note on: Agent Advertisement and Agent Discovery. #

6. Explain Tunnelling and Encapsulation in brief. What are the various types of Encapsulation techniques.
7. Explain agent registration process in mobile communication.
8. What is reverse tunnelling? #
9. Explain selective transmission process at TCP.

## 4. Wireless Local Area Networks

1. Explain the protocol architecture of IEEE 802.11 with diagram.
2. Explain Wireless LAN threats.
3. Explain Bluetooth Protocol Stack in detail.
4. Compare Infrastructure based network with Ad-hoc network.
5. Discuss in detail about Wi-Fi security protocol.
6. Write a short note on: Bluetooth. #
7. Write a short note on: HIPERLAN #
8. What is the responsibility of MAC management in IEEE 802.11?
9. Explain the terms PICONET and Scatternet in terms of Bluetooth. #
10. How can we secure wireless networks. #

## 5. Mobility Management

1. Explain Cellular IP and its use in detail.
2. What is micro mobility, its need and its approaches?
3. Write a short note on: IPv6 #
4. How is IP mobility achieved in wireless network.

## 6. Long Term Evolution of 3GPP

1. What do you mean by Self Organizing Network. Explain the architecture of SON.
2. Explain self-organizing networks(SON) for heterogeneous networks.
3. Compare LTE and LTE advanced. #
4. Explain in short voice over LTE (VoLTE). #
5. Explain different components used in LTE architecture with diagram.

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 2024 Dec | 30 | 45 | 30 | 15 | 0 | 0 |
| 2024 May | 15 | 40 | 25 | 20 | 10 | 15 |
| 2023 Dec | 40 | 35 | 35 | 10 | 5 | 0 |
| 2023 May | 10 | 30 | 40 | 15 | 15 | 15 |
| 2022 Dec | 15 | 20 | 35 | 30 | 15 | 10 |
| **Last 5 Avg** | **20** | **35** | **35** | **15** | **15** | **15** |
| *2022 May | 20 | 30 | 10 | 20 | 10 | 0 |
| **Total** | 130 | 200 | 175 | 110 | 55 | 40 |

* 20-mark MCQs

# MC Answer Bank

multiple times asked questions highlighted
question asked once with red font
# indicates 5-mark question

## 1.Introduction to Mobile Computing

1. What is spread spectrum? Why is it used? #

**Spread Spectrum:**

- Spread Spectrum is a transmission technique in wireless communication, where the transmitted signal is spread over a wider frequency band than required for traditional transmission.
- Unlike narrowband transmission, spread spectrum is a wideband technology that enhances signal robustness and security.
- This makes the signal more resistant to interference, noise, and eavesdropping.

**Why is it used-**

- **Interference Resistance** – Reduces the impact of noise and jamming.
- **Security** – Difficult to intercept due to signal spreading.
- **Multiple Access** – Allows multiple users to share the same bandwidth efficiently (e.g., CDMA).
- **Low Probability of Detection:** Appears like noise, making it hard to detect by unintended receivers.

**Types of Spread Spectrum:**

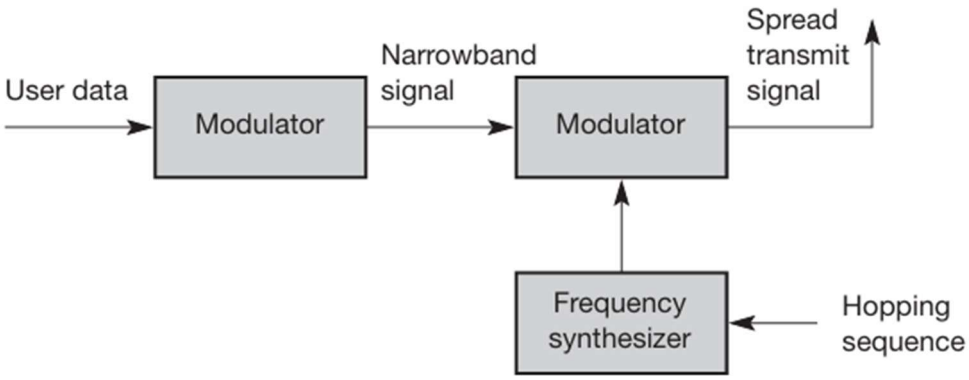
1. Frequency Hopping Spread Spectrum (FHSS)
2. Direct Sequence Spread Spectrum (DSSS)

2. Explain DSSS and FHSS in detail.

**Frequency Hopping Spread Spectrum (FHSS):**

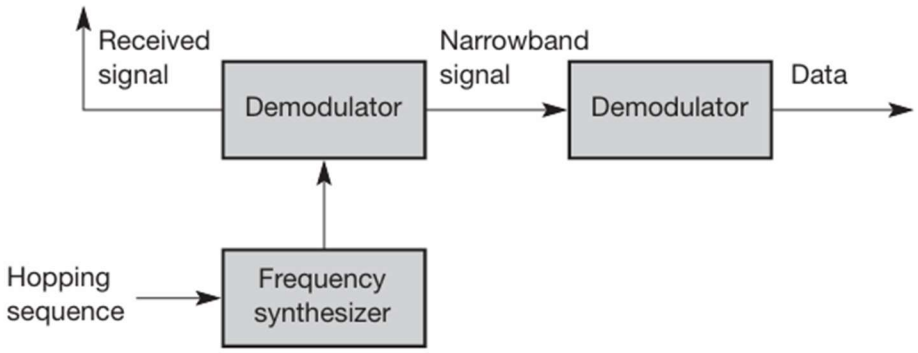
- FHSS uses TDM and FDM, splitting available bandwidth into smaller channels.
- Transmitter and receiver hop between channels after a set time.
- The hopping sequence defines the pattern of frequency changes.
- Dwell time is the duration spent on a frequency before hopping.
- Two types: **Slow hopping** (few hops per bit) and **Fast hopping** (multiple hops per bit).

**FHSS Transmitter:**




1. **Modulation**: User data is modulated using FSK or BPSK (e.g., $f_0$ for binary 0, $f_1$ for binary 1).
2. **Hopping Sequence**: Used to generate the carrier frequency $f_i$ via a frequency synthesizer.
3. **Final Modulation**: The spread signal is created with frequencies $f_i + f_0$ (for 0) and $f_i + f_1$ (for 1).

**FHSS Receiver:** The receiver reverses the FHSS transmission process to recover user data.

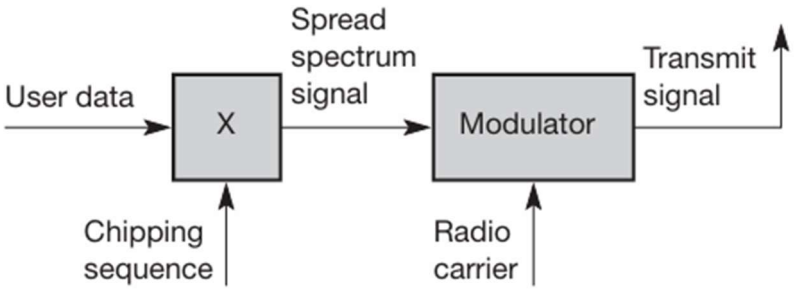



1. **Demodulation**: Uses the hopping sequence to extract the narrowband signal.
2. **Analog-to-Digital Conversion**: Converts the signal back to original binary data.

**DSSS (Direct Sequence Spread Spectrum)**

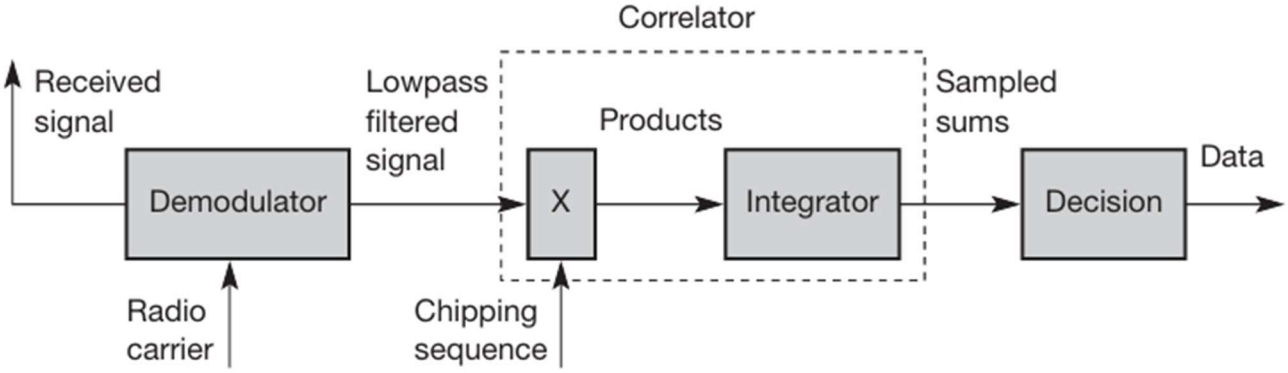
- DSSS spreads data by multiplying it with a high-rate pseudo-noise (PN) code (chip sequence).
- Each bit becomes multiple chips, increasing bandwidth and interference resistance.
- PN code must match at both ends for successful de-spreading.
- Offers good security, anti-jamming, and signal reliability.

**DSSS Transmitter:**




1. **Modulation:** User data is modulated using BPSK.
2. **Spreading:** Modulated signal is multiplied by a high-rate PN sequence to widen the bandwidth.
3. **Transmission:** The spread signal is sent over a carrier; each bit becomes multiple chips, improving resistance to interference.

**DSSS Receiver:**




1. **De-spreading:** The received wideband signal is multiplied again by the same PN sequence used at the transmitter to recover the original narrowband signal.
2. **Demodulation:** The de-spread signal is demodulated using BPSK to extract the binary data.
3. **Output:** The original user data is reconstructed after filtering and decoding.

3. Describe various applications of mobile devices for Vehicles, Emergency situations, Business, Entertainment.

**1. Vehicles**

Mobile devices are widely used in vehicles to enhance navigation, safety, and communication.

**Applications:**

- **GPS Navigation Systems** – Real-time route guidance, traffic updates.
- **Vehicle Diagnostics** – Mobile apps connect to the vehicle's system for fault detection.
- **Driver Assistance** – Voice commands, lane assist alerts, and mobile integration with smart dashboards.
- **Ride-Sharing Apps** – Platforms like Uber and Ola for on-demand transportation.

**2. Emergency Situations**

Mobile devices play a crucial role in responding to emergencies by providing real-time communication and alerts.

**Applications:**

- **Disaster Alerts** – Receive flood, earthquake, or weather warnings through government apps.
- **Emergency Calls & Location Sharing** – Quick access to dial emergency numbers and share live location.
- **Rescue Coordination** – Apps used by emergency responders for coordination (e.g., fire, ambulance).
- **Medical Emergency Apps** – Access to first-aid information, nearby hospitals, and SOS features.

**3. Business**

Mobile devices have transformed how businesses operate, enabling remote access and improved productivity.

**Applications:**

- **Email & Communication Apps** – Stay connected via Outlook, Slack, or Teams.
- **Business Analytics** – View dashboards, sales data, and KPIs from anywhere.
- **E-commerce Management** – Manage inventory, orders, and customer support via mobile apps.
- **Digital Payments** – Use mobile wallets or payment apps for transactions (e.g., Google Pay, Paytm).

**4. Entertainment**

Mobile devices are a major platform for on-demand, interactive, and social entertainment.

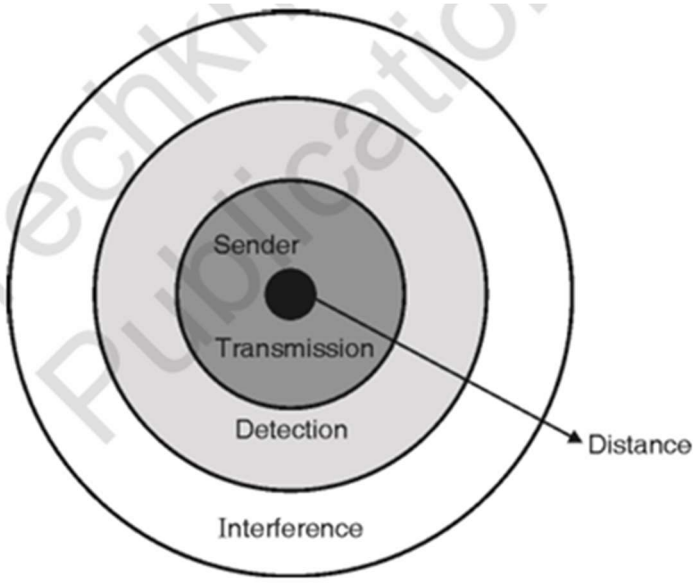
**Applications:**

- **Streaming Services** – Watch movies, series, or live sports (e.g., Netflix, Hotstar, YouTube).
- **Music Apps** – Stream or download music (e.g., Spotify, Gaana).
- **Gaming** – Mobile games from casual to AR-based experiences.
- **Social Media** – Share content, chat, and interact through platforms like Instagram or Snapchat.

4. Explain Signal propagation in detail. What are various signal propagation effects.

Signal propagation refers to the movement of electromagnetic waves from a transmitter to a receiver through a medium, influenced by environmental interactions. These interactions cause phenomena like shadowing, reflection, refraction, scattering, and multipath propagation, which significantly impact communication quality.

**Types of Signal Propagation Ranges:**




1. **Transmission Range:**
   The range within which the signal is strong enough for the receiver to decode it accurately with a low error rate.
2. **Detection Range:**
   The range beyond the transmission range where the receiver can sense the signal's presence but cannot decode the data.
3. **Interference Range:**
   The range where the signal is too weak to be detected or decoded by a receiver but still strong enough to interfere with other ongoing transmissions.

**Key Effects in Signal Propagation**

1. **Shadowing**
   - Occurs when large obstacles like buildings or hills block the signal.
   - Causes a significant drop in signal strength behind the obstacle (known as a shadow region).
   - Results in slow variations in signal strength over distance.
2. **Reflection**
   - Happens when signals bounce off large surfaces like walls, buildings, or the ground.
   - Creates multiple copies of the signal arriving at the receiver.
   - Can either strengthen or weaken the overall signal depending on phase alignment.

3. **Refraction**
    - Bending of the signal as it passes through materials with different densities (e.g., from air to glass or air layers with different temperatures).
    - Can cause signal distortion and path deviation.
4. **Scattering**
    - Caused by small objects or rough surfaces (e.g., trees, lampposts, street signs).
    - Signal is diffused in many directions.
    - Especially significant at higher frequencies like in 5G.
5. **Multipath Propagation**
    - A combination of reflection, scattering, and diffraction.
    - Multiple versions of the signal reach the receiver via different paths, each with different delays.
    - Can cause constructive or destructive interference leading to:
        - **Fading** (signal drops)
        - **Inter-symbol interference** (symbols overlap)

5. Compare all Mobile generations i.e. 1G, 2G, 3G, 4G and 5G.

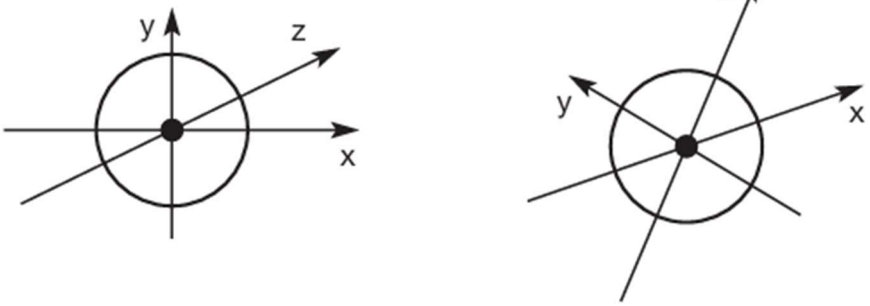
| Parameter | 1G | 2G | 3G | 4G | 5G |
|---|---|---|---|---|---|
| **Introduced in** | 1980 | 1993 | 2001 | 2009 | 2019 (Rollout started) |
| **Technology** | AMPS | GSM, IS-95 | W-CDMA, CDMA2000 | LTE, WiMAX | NR (New Radio), LTE Advanced, NOMA |
| **Multiplexing** | FDMA | TDMA/CDMA | CDMA | CDMA | All Packet Switching |
| **Switching Type** | Circuit | Circuit (Voice), Packet (Data) | Packet | All Packet | All Packet |
| **Speed** | 2.4–14.4 kbps | 14.4 kbps | 3.1 Mbps | 100 Mbps | Up to 10 Gbps |
| **Services** | Voice Only | Voice + Data | Multimedia, Video Call | HD Streaming, VoIP | IoT, AI, Autonomous Vehicles |
| **Bandwidth** | Analog | 25 MHz | 25 MHz | 100 MHz | 60 GHz+ |
| **Operating Frequency** | 800 MHz | 900/1800 MHz | 2100 MHz | 2600 MHz | 3–100 GHz |
| **Band Type** | Narrow | Narrow | Wide | Ultra-Wide | Extremely High Frequency |
| **Handover** | NA | Horizontal | Horizontal | Horizontal/Vertical | Horizontal /Vertical |
| **Advantages** | Simple | SMS, MMS, Internet | Security, Roaming | Speed, MIMO, Mobility | Ultra-fast, Low Latency, Global Coverage |
| **Disadvantages** | Low Capacity, No Security | Low Speed, Poor Coverage | High Power Use, Costly Spectrum | Hard to Implement | Expensive Infrastructure, Device Compatibility |
| **Applications** | Voice Calls | SMS, Browsing | Video Calls, GPS | Smart Devices, Wearables | Smart Cities, IoT, AR/VR, Automation |

6. Explain various types of antennas along with their radiation patterns.

**1. Isotropic Antenna**

**Explanation**:
An isotropic antenna is a hypothetical, ideal antenna that radiates equally in all directions—both horizontally and vertically. It is used as a standard reference to measure the gain of real antennas. Since it cannot be built in practice, it exists only in theory.

**Radiation Pattern**:
A perfect sphere, representing equal radiation in 360° in all direction.

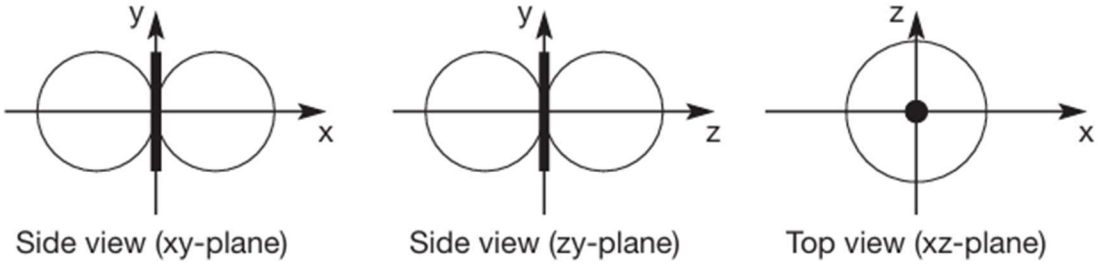



**Use**:
Used only as a benchmark for comparing antenna gains.

**2. Dipole Antenna (Hertzian Dipole)**

**Explanation**:
One of the simplest and most common antennas. It consists of two conductive elements (like rods) fed by a current in the centre. It radiates strongly in directions perpendicular to the antenna's axis and very weakly along its axis.

**Radiation Pattern**:
Figure-eight shaped in the horizontal plane when the antenna is vertical.

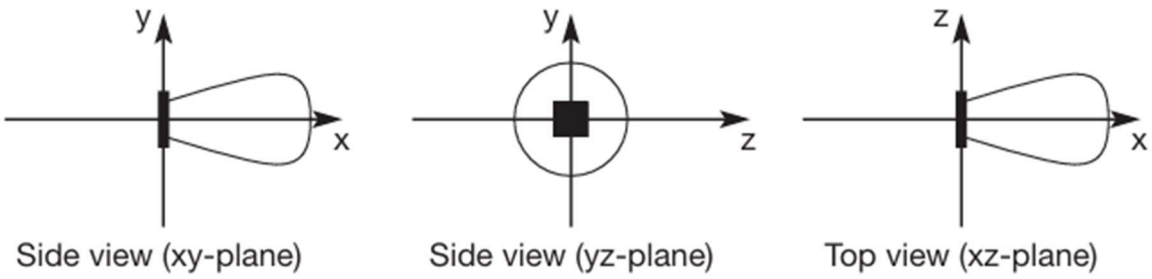



**Use**:
Radio and TV broadcasting, shortwave communication.

**3. Directional Antenna**

**Explanation**:
Directional antennas are designed to focus energy in one specific direction, giving them higher gain and range in that direction. They reduce interference from other directions and are ideal for long-distance communication.

**Radiation Pattern**:
A narrow, strong lobe in one direction with minimal radiation elsewhere.

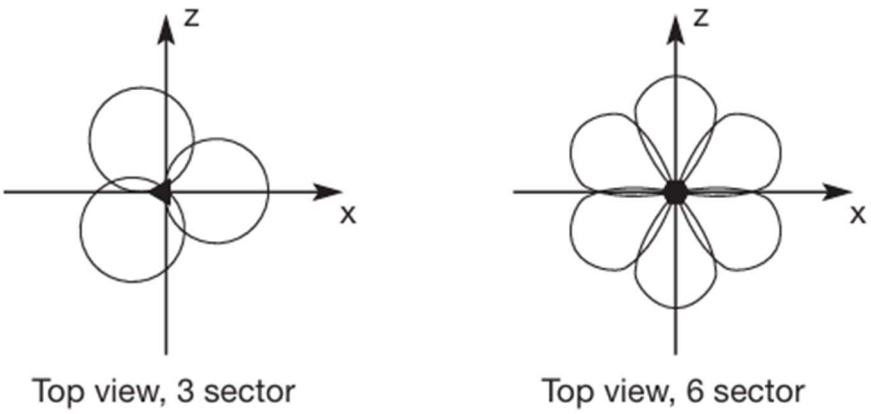



**Use**:
Satellite dishes, point-to-point communication systems.

**4. Sectorized Antenna**

**Explanation**:
A sector antenna is a type of directional antenna that radiates within a specific angular sector, such as 60°, 90°, or 120°. These are often used in groups to cover 360° by dividing it into multiple sectors. They provide a balance between omnidirectional and highly directional antennas.

**Radiation Pattern**:
Fan-shaped or wedge-shaped, covering a specific sector.




**Use**:
Cellular base stations (e.g., each antenna covers one sector of a cell).

7. Explain the concept of frequency reuse with clustering. #

**Frequency Reuse** is a technique used in cellular networks to efficiently use the limited radio frequency spectrum by reusing the same frequency channels in different geographical areas (called cells), without interference.

A **cluster** is a group of adjacent cells that use different frequency channels to avoid interference.

**How it works:**

- The area is divided into hexagon-shaped cells.
- Each cell gets a unique set of frequencies.
- A group of N nearby cells (clusters) uses different frequencies to avoid interference.
- The same set of frequencies is used again in other clusters far enough away.

**Benefits of Frequency Reuse with Clustering:**

- Efficient use of limited frequency spectrum
- Supports more users without interference

## 8. What are various advantages and disadvantages of small cells in cellular systems. #

**Advantages of Small Cells:**

1. **Improved Coverage:**
   - Provide better signal strength in weak coverage areas (like indoors or underground).
2. **Higher Data Rates:**
   - Serve fewer users per cell, allowing faster internet speeds and lower latency.
3. **Capacity Boost:**
   - Handle more simultaneous users in dense areas like stadiums, malls, or city centres.
4. **Energy Efficient:**
   - Consume less power than large macro cells.

**Disadvantages of Small Cells:**

1. **High Installation Cost in Large Numbers:**
   - Though cheap individually, deploying many small cells increases total cost.
2. **Interference Management:**
   - More cells close to each other may lead to signal interference if not properly managed.
3. **Handover Needed**
   - When a mobile device moves between cells, a handover process occurs, which can happen frequently with smaller cells and faster movements.

## 9. What is co channel interference. #

Co-channel interference refers to the interference that occurs when two or more transmitters use the same frequency in different locations, and their signals overlap or interfere with each other. This happens in a cellular network when cells that are geographically close or even farther apart, reuse the same frequency channels.

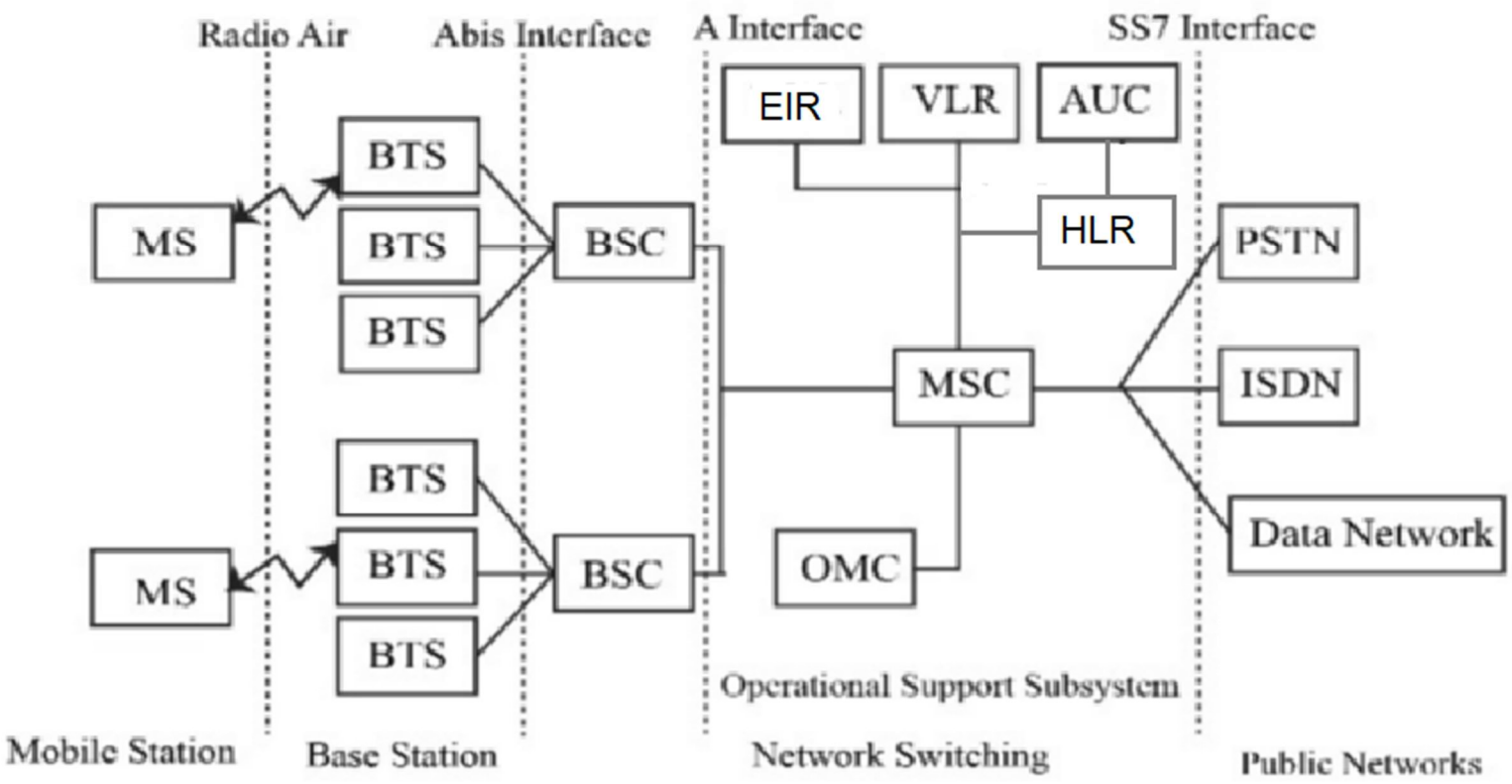
**Cause:** It typically arises when frequency channels are reused in nearby or distant cells that are not sufficiently separated in terms of distance or signal strength.

**Impact:** Co-channel interference reduces the signal quality and can lead to poor performance.

**Frequency Planning:** To mitigate co-channel interference, careful frequency planning is essential. For example: Techniques like frequency reuse.

# 2. GSM Mobile Services

**10.** Explain GSM architecture in detail.




**1. Mobile Station (MS)**

- Composed of:
  - **Mobile Equipment (ME)**: The user's mobile device (phone, tablet).
  - **SIM (Subscriber Identity Module)**: Stores subscriber information such as IMSI and keys.
- Communicates with BTS over the radio interface.

**2. Base Station Subsystem (BSS)**

Connects mobile devices to the network.

- **BTS (Base Transceiver Station)**:
  - Handles radio communication with MS.
  - Each BTS covers a cell and has antennas and transceivers.
- **BSC (Base Station Controller)**:
  - Manages multiple BTS's.
  - Responsible for handovers, frequency allocation, and power control.
- **Abis Interface**:
  - Connects BTS to BSC.

**3. Network Switching Subsystem (NSS)**

Core part responsible for call processing and mobility.

- **MSC (Mobile Switching Centre)**:
  - Handles voice calls, SMS, and circuit-switched services.
  - Interfaces with other networks (PSTN, ISDN, etc.).
- **HLR (Home Location Register)**:
  - Stores permanent subscriber data (IMSI, services).
- **VLR (Visitor Location Register)**:
  - Temporary data about subscribers currently in its area.
- **AUC (Authentication Centre)**:
  - Verifies user identity.
- **EIR (Equipment Identity Register)**:
  - Checks if the device is valid using the IMEI number.
  - Prevents stolen or blacklisted phones from accessing the network.
- **A Interface**:
  - Interface between BSC and MSC.

**4. Operation and Support Subsystem (OSS)**

- **OMC (Operations and Maintenance Centre)**:
  - Manages network operations like configuration, fault management, performance.

**5. Public Networks**

MSC connects to external networks such as:

- **PSTN** (Public Switched Telephone Network)
- **ISDN** (Integrated Services Digital Network)
- **Data Networks** (e.g., Internet)

**11.** Explain handover mechanisms in GSM in detail.

When a mobile user is engaged in conversation, the MS (Mobile Station) is connected to the BTS (Base Transceiver Station) via radio link. If the mobile user moves to the coverage area of another BTS, the radio link to the old BTS is eventually disconnected, and a radio link to the new BTS is established to continue the conversation. This process is called handover or handoff.

There are four types of handovers in GSM:

**1. Intra-Cell Handover**

- Occurs **within the same cell** but between **different frequency channels** or time slots.
- Used to reduce interference or improve signal quality.
- Example: A call remains in the same base station but switches to a different frequency.

**2. Inter-Cell Handover (Intra-BSC Handover)**

- Occurs **between two cells** controlled by the **same Base Station Controller (BSC)**.
- The Mobile Station (MS) moves from one Base Transceiver Station (BTS) to another, but the BSC remains unchanged.
- Example: A user moving from one cell to another within the same city under the same BSC.

**3. Inter-BSC Handover**

- Happens when a call is transferred **between two different BSCs** but within the **same Mobile Switching Centre (MSC)**.
- The MSC manages the handover process to ensure a smooth transition.
- Example: A user moves from one city area to another, and the call is handled by a different BSC.

**4. Inter-MSC Handover**

- Occurs when the mobile user moves between **two different MSCs**.
- Requires coordination between the two MSCs to transfer the call.
- Example: A person traveling between different states or large regions.

**12.** Explain Security algorithms used in GSM for authentication and privacy (A3, A5, A8).

**A3 – Authentication Algorithm**

**Purpose**: To authenticate the subscriber (SIM) to the GSM network and verify identity.

**Working**:

- GSM network sends a random number (RAND) to the mobile.
- SIM uses A3 algorithm with its secret key (Ki) to compute a response (SRES).
- Network uses the same A3 algorithm and Ki to verify SRES.

If both SRES values match, the user is authenticated.

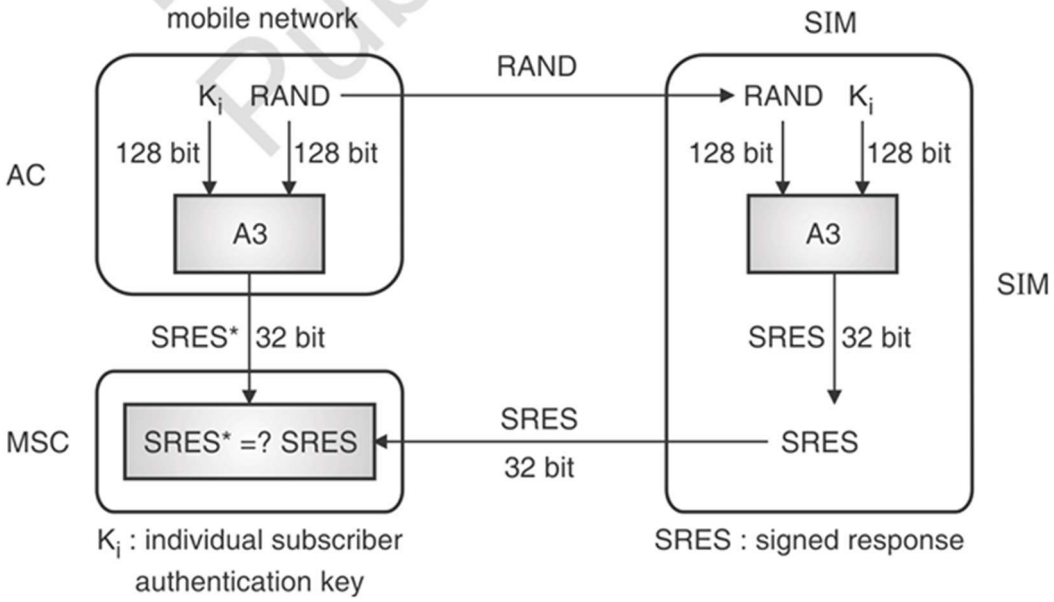



**Fig. 2.1.12 : Authentication in GSM**

**A8 – Ciphering Key Generation Algorithm**

**Purpose**: Generates the session key (Kc) for encryption.

**Working**:

- Takes RAND and Ki as input.
- Produces a 64-bit Kc.
- Kc is used with A5 algorithm for encryption of user data.

Helps maintain confidentiality during communication.

**A5 – Encryption Algorithm**

**Purpose**: Ensures privacy by encrypting the voice and data over the air.

**Working**:

- Uses Kc and the frame number to produce a keystream.
- This keystream is XORed with the user data for encryption.

Protects data from eavesdropping on the radio interface

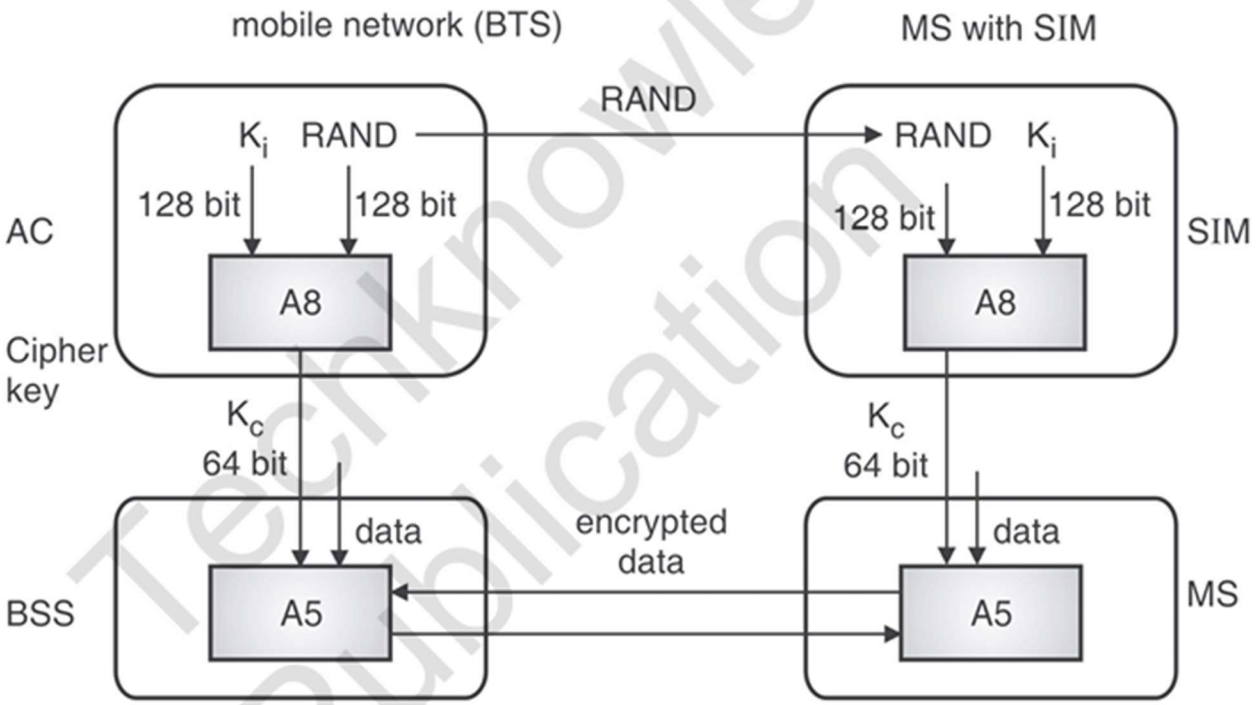



**Fig. 2.1.13 : Data encryption in GSM**

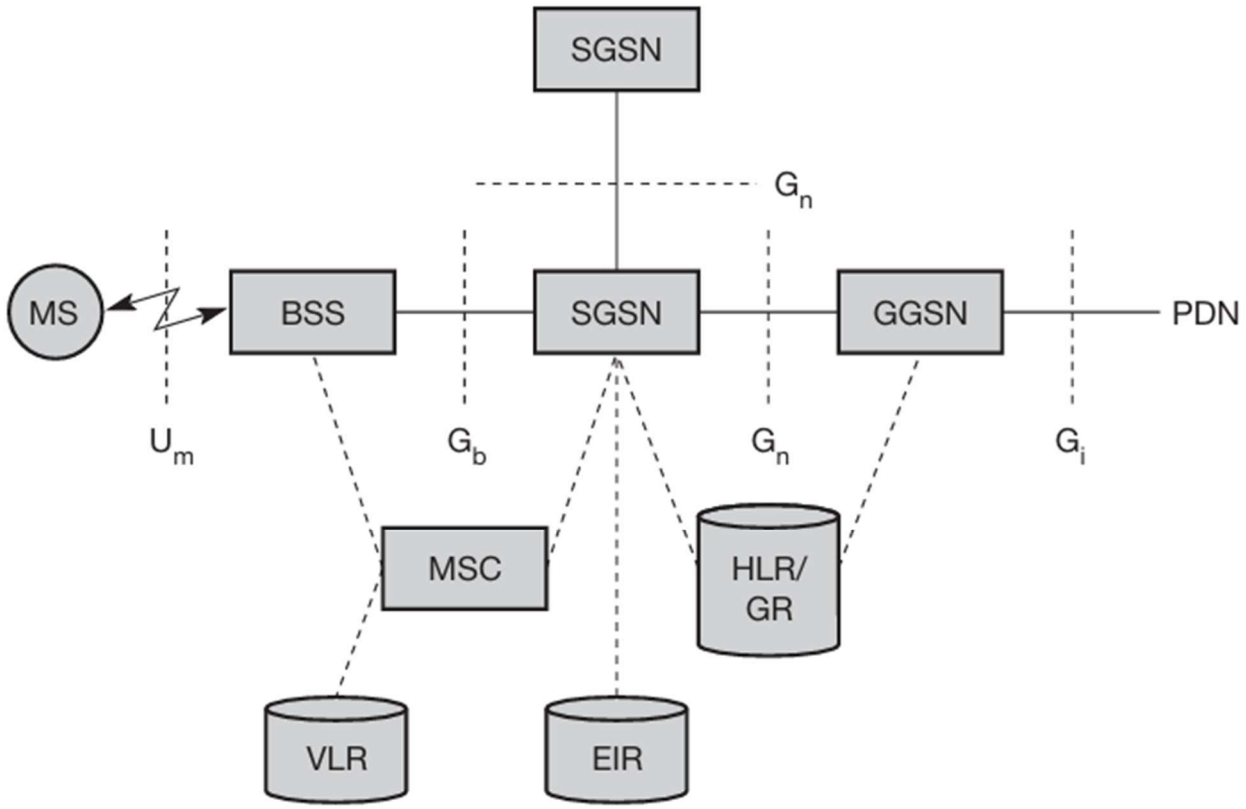
**Summary:**

1. **Random number(RAND)** sent by network.
2. SIM uses **A3** to generate **SRES** for authentication.
3. SIM uses **A8** to generate **Kc** for encryption.
4. **A5** uses **Kc** to encrypt/decrypt communication.

**Conclusion:**

The A3, A5, and A8 algorithms are essential components of GSM security.
They work together to authenticate users, generate session keys, and encrypt communication, ensuring confidentiality, integrity, and privacy in GSM networks.

**13.** Explain GPRS architecture in detail.




**1. Mobile Station (MS)**

- The user's mobile device (phone, tablet).
- Communicates with the network using the **Um** interface.

**2. Base Station Subsystem (BSS)**

- Includes **Base Transceiver Station (BTS)** and **Base Station Controller (BSC)**.
- Handles radio communication with the MS.
- Uses the **Gb** interface to connect to the SGSN.

**3. Mobile Switching Centre (MSC)**

- Handles voice calls, SMS, and circuit-switched services.
- Works alongside SGSN to provide seamless voice and data services.

**4. Serving GPRS Support Node (SGSN)**

- Manages packet-switched data services for mobile users.
- Handles mobility management, authentication, and data packet forwarding.
- Interfaces with:
  - **VLR (Visitor Location Register)**: Stores temporary subscriber data.
  - **EIR (Equipment Identity Register)**: Checks if the device is valid.
  - **HLR/GR (Home Location Register/Gateway Register)**: Stores subscriber profiles.

**5. Gateway GPRS Support Node (GGSN)**

- Acts as a bridge between the GPRS network and external networks (e.g., Internet, PDN).
- Assigns IP addresses to mobile users.
- Uses the **Gi** interface to connect to PDN and **Gn** to communicate with other SGSNs.

**6. Public Data Network (PDN)**

- External network such as the Internet, corporate intranet, or other IP-based services.
- GGSN facilitates data exchange between the PDN and mobile users.

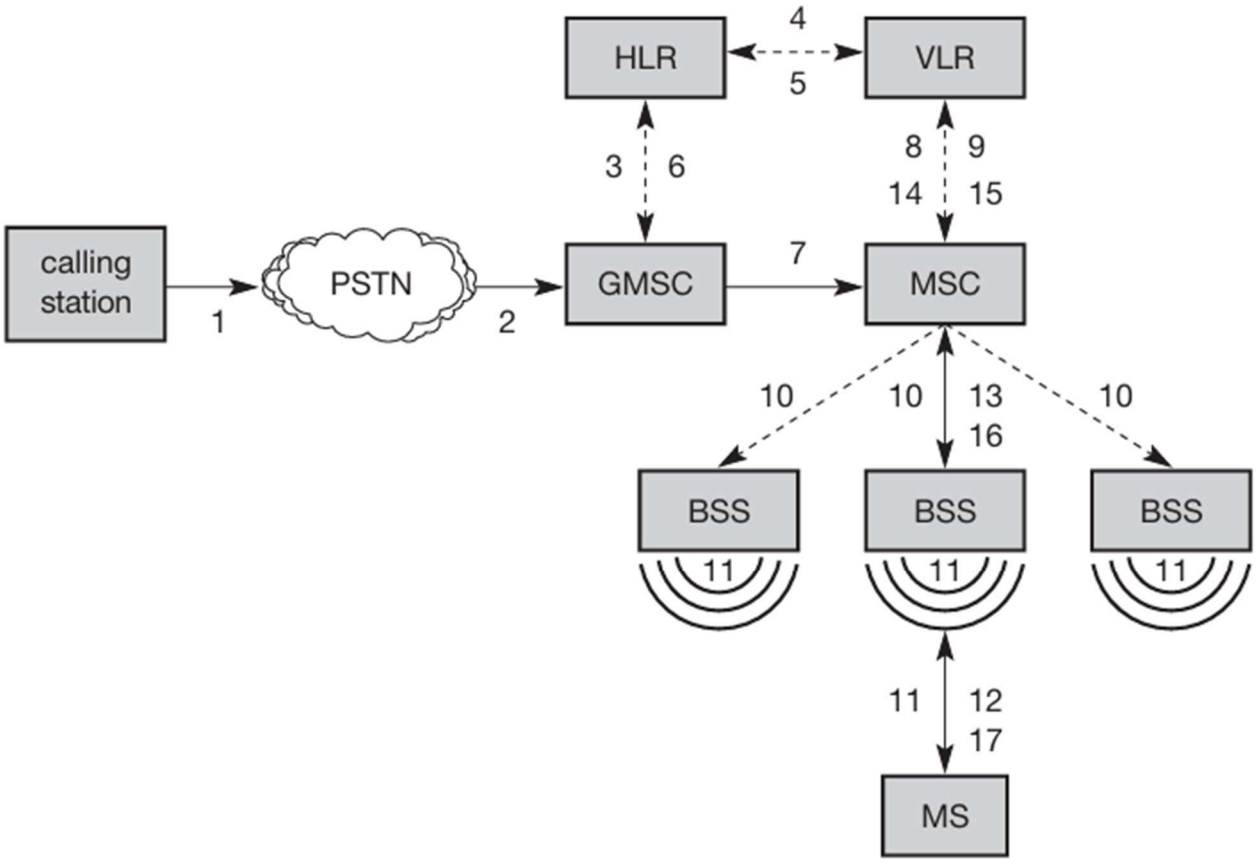
**Interfaces**

- **Um**: Wireless link between MS and BSS.
- **Gb**: Connects BSS to SGSN.
- **Gn**: Connects SGSN and GGSN.
- **Gi**: Connects GGSN to external networks (PDN).

**14.** Explain Mobile Terminated Call and Mobile Originated Call in detail.

**Mobile Terminated Call (MTC)**

An MTC refers to a call **received by the mobile user**. When a caller dials a mobile number, the GMSC (Gateway MSC) queries the HLR to locate the mobile subscriber. After locating the serving MSC and BSS, the network pages the MS, performs authentication, and sets up the call.

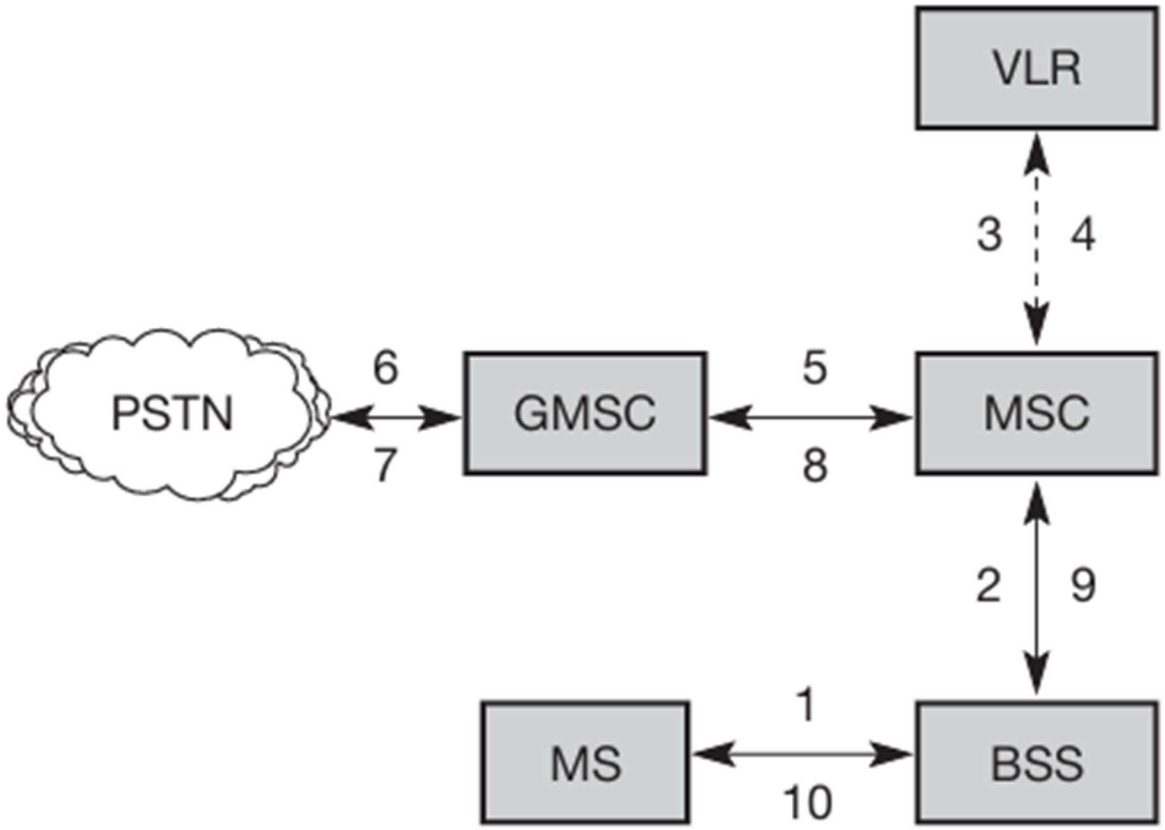



**Steps:**

**1–2:** Calling user dials MS number → Call reaches GMSC via PSTN.
**3:** GMSC queries HLR for MS location.
**4–5:** HLR contacts VLR to get routing info.
**6:** HLR sends routing info to GMSC.
**7:** GMSC forwards call to the serving MSC.
**8–9:** MSC checks MS status in VLR.
**10:** MSC pages BSSs in the area.
**11:** BSS pages the MS.
**12:** MS responds to BSS.
**13–14:** Authentication and setup via MSC & VLR.
**15–17:** Traffic channel allocated; call established.

**Mobile Originated Call (MOC)**

An MOC is a call **initiated by the mobile user**. The MS sends a request to the BSS, which forwards it to the MSC. The MSC then authenticates the user with the VLR and routes the call through the GMSC to reach the PSTN or other network.




**Steps:**

**1:** MS sends a request to BSS to make a call.

**2:** BSS forwards the request to MSC.

**3-4:** MSC authenticates MS with VLR.

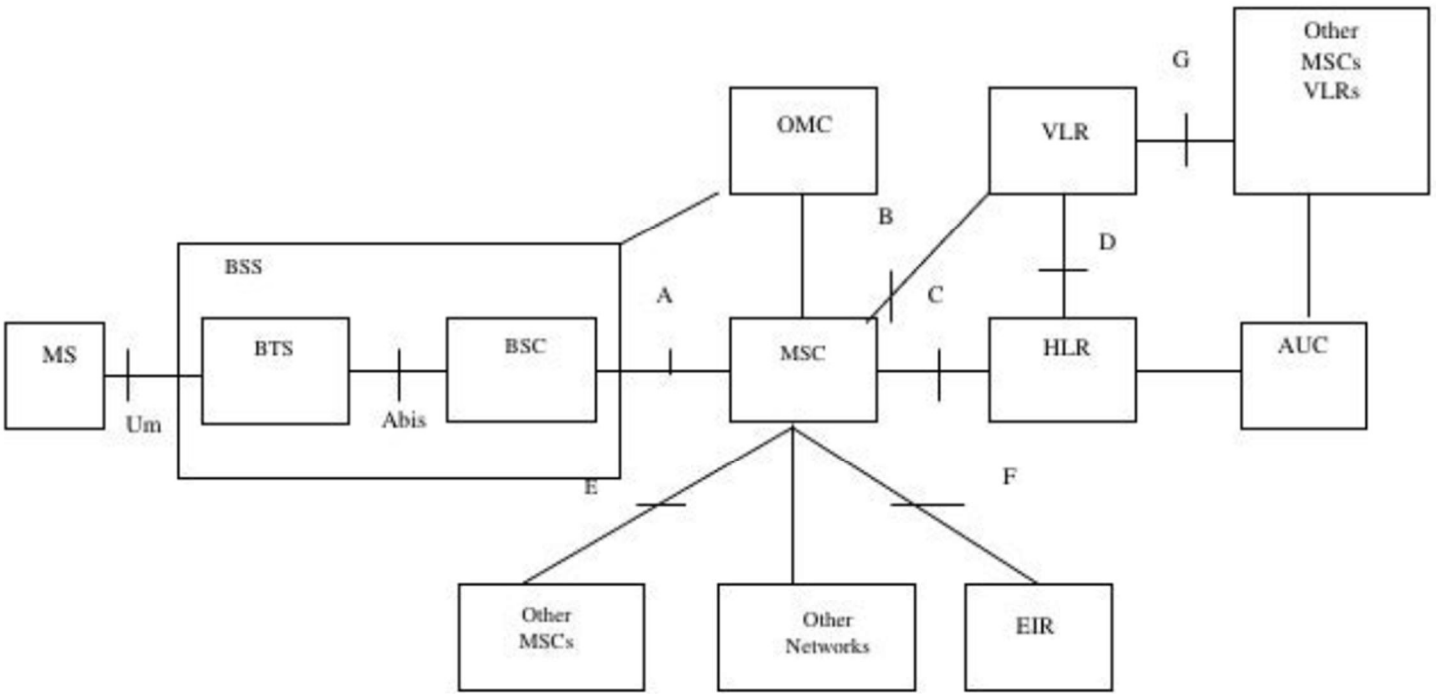
**5:** Call setup proceeds from MSC to GMSC.

**6– 7:** GMSC routes the call to PSTN (or other networks).

**8–9:** MSC allocates a channel for the call.

**10:** BSS connects the call to MS.

**15.** What is the use of different interfaces used in GSM with diagram.




1. **Um**
   – Between: **Mobile Station (MS) ↔ Base Transceiver Station (BTS)**
   – Purpose: Wireless air interface for communication between mobile and network.

2. **Abis**
   – Between: **BTS ↔ Base Station Controller (BSC)**
   – Purpose: Carries voice, data, and control signals; allows BSC to manage BTS.

3. **A**
   – Between: **BSC ↔ Mobile Switching Centre (MSC)**
   – Purpose: Manages call control, handovers, and mobility.

4. **B**
   – Between: **MSC ↔ Visitor Location Register (VLR)**
   – Purpose: Transfers temporary subscriber info for call/session handling.

5. **C**
   – Between: **MSC ↔ Home Location Register (HLR)**
   – Purpose: Retrieves permanent subscriber data for authentication and services.

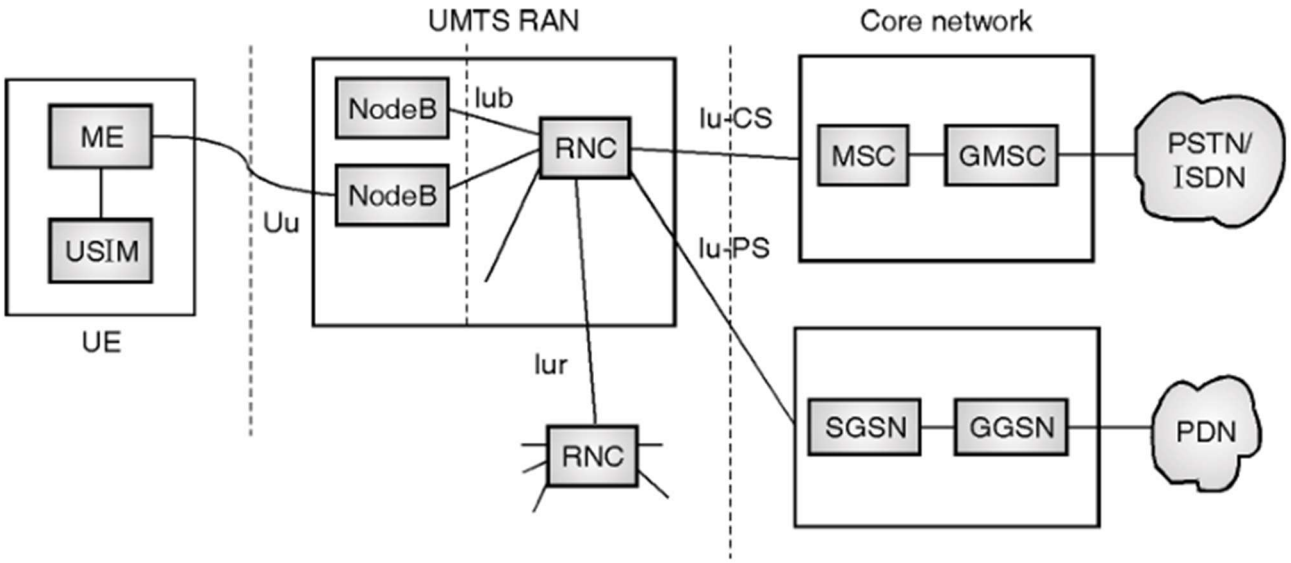
6. **D**
   – Between: **HLR ↔ Visitor Location Register (VLR)**
   – Purpose: Transfers subscriber data when a user roams into a new location area.

7. **E**
   – Between: **MSC ↔ Other MSCs**
   – Purpose: Supports inter-MSC handovers and call routing.

8. **F**
   – Between: **MSC ↔ Equipment Identity Register (EIR)**
   – Purpose: Verifies the device's IMEI to block stolen or invalid devices.

9. **G**
   – Between: **VLR ↔ Other VLRs**
   – Purpose: Transfers user data during inter-VLR handovers.

## 16. Explain UMTS architecture.




The UMTS (Universal Mobile Telecommunications System) architecture is designed to support 3G mobile services. It consists of three major components: the User Equipment (UE), the UMTS Terrestrial Radio Access Network (UTRAN), and the Core Network (CN). Here's a breakdown based on the diagram:

**1. User Equipment (UE)**

- **ME (Mobile Equipment)**: The mobile device (e.g., phone or tablet).
- **USIM (Universal Subscriber Identity Module)**: Stores user identity, security keys, and subscription data.
- **Interface**: Connects to the network via the Uu interface.

**2. UMTS RAN (UTRAN)**

- Handles radio communication between UE and the Core Network.
- **Node B**: Equivalent to a base station, it transmits and receives radio signals.
- **RNC (Radio Network Controller)**: Manages radio resources, handovers, and mobility.
    - **Iub interface**: Connects Node B and RNC.
    - **Iur interface**: Connects RNCs for handovers across cells.
    - **Iu interface**: Connects RNC to the Core Network.
        - **Iu-CS**: For Circuit-Switched services (e.g., voice).
        - **Iu-PS**: For Packet-Switched services (e.g., internet).

**3. Core Network (CN)**

Divided into two domains:

**a. Circuit-Switched (CS) Domain**

- **MSC (Mobile Switching Centre)**: Handles voice call routing.
- **GMSC (Gateway MSC)**: Interface to external networks like PSTN/ISDN.

**b. Packet-Switched (PS) Domain**

- **SGSN (Serving GPRS Support Node)**: Manages mobile data sessions, mobility, and authentication.
- **GGSN (Gateway GPRS Support Node)**: Connects to external packet data networks (PDN) like the internet.

## 17. What are the roles of EIR and HLR entities in a GSM network. #

### 1. Equipment Identity Register (EIR)

The EIR is a database that maintains records of mobile devices based on their IMEI (International Mobile Equipment Identity) numbers.

**Functions of EIR:**

- **Device Authentication:** Verifies the IMEI of a mobile device before allowing it to connect to the network.
- **Maintaining Device Lists:**
  - **Whitelist** – Devices allowed to access the network.
  - **Grey list** – Devices under monitoring (e.g., malfunctioning or suspicious devices).
  - **Blacklist** – Devices banned from the network due to theft or fraud.

### 2. Home Location Register (HLR)

The HLR is a central database that stores permanent subscriber information required for authentication, call routing, and roaming. It works in coordination with VLR (Visitor Location Register) and MSC (Mobile Switching Centre) to track and manage users.

**Functions of HLR:**

- **Subscriber Information Storage:** Maintains IMSI (International Mobile Subscriber Identity), MSISDN (phone number), service subscriptions, and authentication keys.
- **Location Management:** Keeps track of the current location of subscribers by storing the identity of the VLR they are registered with.
- **Authentication and Security:** Works with AuC (Authentication Centre) to verify subscribers and prevent unauthorized access.

## 18. Discuss about the mobile services and data services in GSM. #

### 1. Mobile Services in GSM

GSM offers three types of mobile services:

**a) Teleservices**

- Standard voice call services.
- Emergency calls (e.g., 112, 911).
- Short Message Service (SMS) for text messaging.
- Voice mail services.

**b) Bearer Services**

- Used for data transmission between devices.
- Supports speeds of 300 bps to 9.6 kbps.
- Enables internet access and fax transmission.

**c) Supplementary Services**

- **Call-related features:** Call waiting, call hold, call forwarding, call barring.
- **Security features:** Caller ID, PIN authentication.
- **Multiparty calls:** Conference calling support.

### 2. Data Services in GSM

GSM supports several data services for communication and internet access:

**a) Circuit-Switched Data (CSD)**

- Uses a dedicated circuit for data transfer.
- Supports speeds of 9.6 kbps.

**b) High-Speed Circuit-Switched Data (HSCSD)**

- Improved version of CSD with higher speeds (up to 57.6 kbps).
- Provides better quality for video calls and web browsing.

**c) General Packet Radio Service (GPRS)**

- Packet-based data transmission.
- Supports speeds of 56–114 kbps.

**d) Enhanced Data Rates for GSM Evolution (EDGE)**

- Enhanced version of GPRS.
- Provides data speeds up to 384 kbps.
- Enables faster browsing, video streaming, and file downloads.

## 19. Write a short note on: CDMA #

**CDMA (Code Division Multiple Access)** is a channel access method used in wireless communication systems. Unlike other methods that divide access by time or frequency, CDMA allows multiple users to share the same frequency band simultaneously.

**Key Concepts:**

- **Spread Spectrum Technique:** CDMA uses spread spectrum technology where a user's signal is spread over a wide frequency band using a unique pseudo-random code.
- **Unique Codes for Each User:** These codes help distinguish between different users even though they transmit on the same frequency at the same time.
- **Simultaneous Access:** Unlike FDMA or TDMA, CDMA allows multiple users to access the channel at the same time without interference.

**Advantages:**

- **Efficient Bandwidth Usage:** More users can share the same bandwidth without signal collision.
- **Better Signal Quality:** CDMA provides resistance to noise and interference, improving call quality.
- **Improved Privacy:** Signals are coded uniquely, making eavesdropping difficult.

## 20. Which components are new in GPRS as compared to GSM? What is their purpose?

GPRS (General Packet Radio Service) is an enhancement over GSM, allowing packet-switched data services. Several new components are introduced in the GPRS architecture that are not present in traditional GSM.

New GPRS Components and Their Purposes:

**1. Serving GPRS Support Node (SGSN)**

- Manages packet-switched data services for mobile users.
- Handles mobility management, authentication, and data packet forwarding.
- Interfaces with:
  - **VLR (Visitor Location Register)**: Stores temporary subscriber data.
  - **EIR (Equipment Identity Register)**: Checks if the device is valid.
  - **HLR/GR (Home Location Register/Gateway Register)**: Stores subscriber profiles.

**2. Gateway GPRS Support Node (GGSN)**

- Acts as a bridge between the GPRS network and external networks (e.g., Internet, PDN).
- Assigns IP addresses to mobile users.
- Uses the G**i** interface to connect to PDN and Gn to communicate with other SGSNs.

**3. PCU (Packet Control Unit)**

- Routes packet data from the mobile device to the SGSN via the BSC.
- Controls radio resources for GPRS.
- Manages packet scheduling and segmentation.

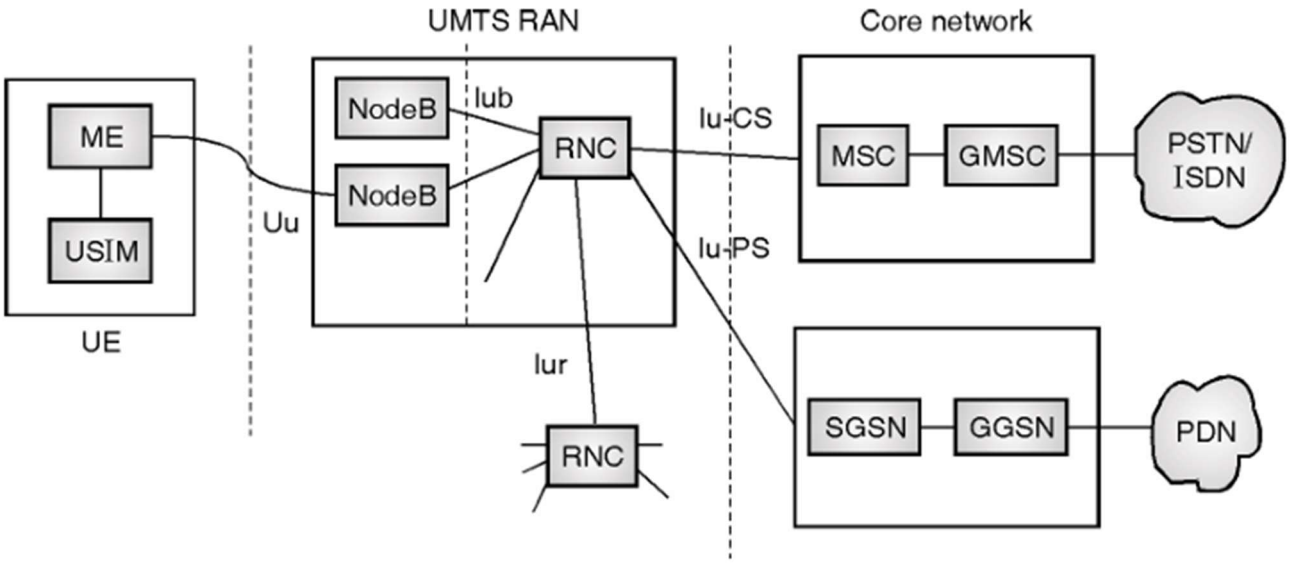
**4. GPRS Backbone Network**

- A new IP-based core network that links SGSN and GGSN.
- Handles routing, switching, and delivery of GPRS data packets.

**5. New Interfaces:**

- **Gb Interface:** Between BSC and SGSN for transferring GPRS data.
- **Gn Interface:** Connects SGSNs and GGSNs within the same network.
- **Gi Interface:** Connects GGSN to external IP networks like the internet.
- **Gr Interface:** Between SGSN and HLR for accessing subscriber info.
- **Gf Interface:** Between SGSN and EIR for equipment verification.

## 21. Write a short note on UTRAN and UMTS network.




**UMTS:** The UMTS (Universal Mobile Telecommunications System) architecture is designed to support 3G mobile services. It consists of three major components: the User Equipment (UE), the UMTS Terrestrial Radio Access Network (UTRAN), and the Core Network (CN).

**Key Features:**

- Supports up to 2 Mbps data rates.
- Enables services like video calling, mobile internet, and multimedia streaming.
- Offers global roaming and improved spectral efficiency.

**UTRAN** is the radio access network component of the UMTS architecture. It is responsible for wireless communication between user equipment (UE) and the core network.

**Components of UTRAN:**

- **Node B:** Equivalent to base stations; handles radio transmission/reception.
- **RNC (Radio Network Controller):** Manages radio resources, mobility, and handovers.

**Functions:**

- Radio resource control, mobility management, data encryption, and handover control.
- Connects to the Core Network (CN) via the Iu interface.

# 3. Mobile Networking

22. Explain packet delivery mechanism to and from mobile node with the help of Mobile IP network diagram.

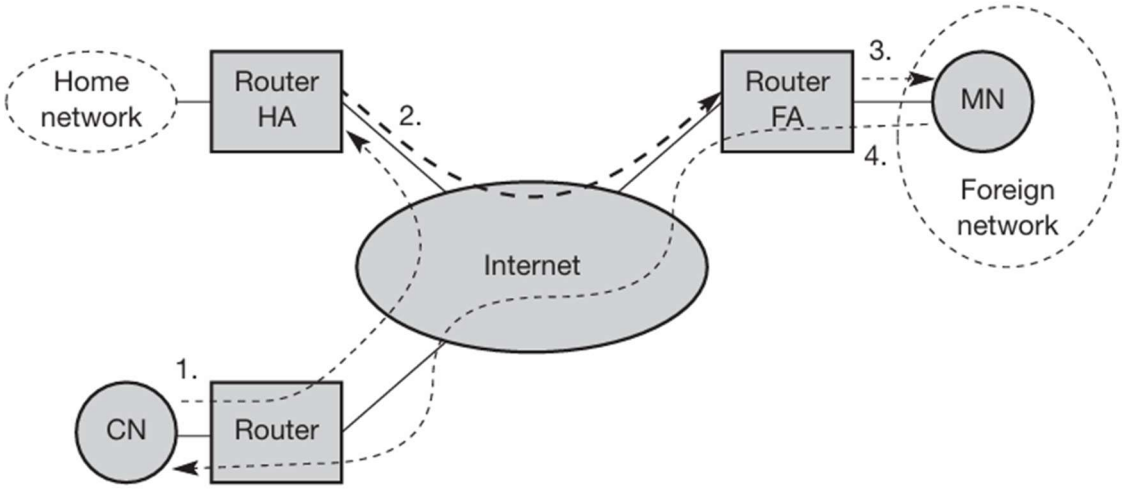



**Figure 8.2**
Packet delivery to and from the mobile node

**Entities Involved:**

- **MN (Mobile Node):** The mobile device moving between networks.
- **CN (Correspondent Node):** The device communicating with the MN.
- **HA (Home Agent):** A router on the MN's home network.
- **FA (Foreign Agent):** A router on the visited (foreign) network.
- **CoA (Care-of Address):** The temporary IP address in the foreign network.

**Packet Delivery Steps:**

**(a) From Correspondent node to Mobile node.**

1. **Step 1: CN → MN's Home IP:**
    - CN sends a packet to MN's permanent home IP.
    - This packet reaches the Home Agent (HA) via normal internet routing.
2. **Step 2: HA → CoA:**
    - HA detects that MN is away.
    - HA encapsulates the original packet using tunnelling (adds a new IP header with CoA as the destination).
    - The packet is sent to the FA at the foreign network.
3. **Step 3: FA → MN:**
    - FA decapsulates the tunnelled packet.
    - The original packet is delivered to the MN.

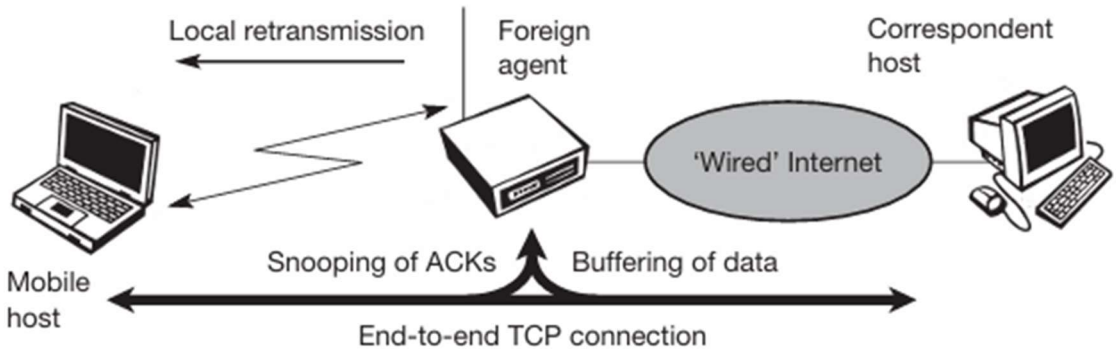
Result: MN receives the packet as if it were at home, maintaining transparency.

**(b) From Mobile node to Correspondent node.**

4. **Step 4: MN → CN:**
    - MN sends a packet using its permanent home IP as the source and CN's IP as the destination.
    - The FA simply forwards this packet into the internet.
    - Packet reaches CN via regular IP routing.

23. What is Snooping TCP? What are its advantages and disadvantages.

- Snooping TCP is a TCP-aware link-layer protocol used in wireless networks to improve TCP performance over unreliable wireless links. It is implemented at the base station, which "snoops" (monitors) TCP packets (both data and acknowledgments) passing through it.
- Traditional TCP interprets all losses as congestion, leading to unnecessary retransmissions and reduced performance, Snooping TCP helps mitigate this by handling retransmissions locally without involving the sender unnecessarily.




**Working:**

- **Mobile Host ↔ Foreign Agent ↔ Correspondent Host**:
  - The mobile host (e.g., laptop) communicates with a correspondent host via a foreign agent (e.g., base station/router).
  - The TCP connection is end-to-end between the mobile host and correspondent host.
- **Snooping Mechanism**:
  - The foreign agent "snoops" or monitors TCP ACKs from the mobile host.
  - It also buffers TCP data packets sent from the correspondent host to the mobile host.
- **Local Retransmission**:
  - If an ACK is not received within a certain time (indicating possible loss), the foreign agent locally retransmits the buffered data to the mobile host without involving the sender.

**Advantages of Snooping TCP:**

- **Maintains End-to-End Semantics**: The end-to-end TCP connection remains intact.
- **Local Recovery:** Wireless link errors are corrected quickly by the base station without involving the sender.
- **Improved Throughput:** Avoids unnecessary reduction of TCP window size, maintaining better flow.

**Disadvantages of Snooping TCP**

- **Not Fully Transparent**: Requires additional support like NACK at the mobile host, breaking transparency.
- **Wireless Link Dependency**: Performance depends on the wireless link; delays may trigger unnecessary retransmissions.
- **Fails with Encryption:** Encrypted TCP headers prevent snooping, making S-TCP ineffective.

24. Explain Mobile TCP with their merits and demerits. #

Mobile TCP (M-TCP) is a variant of TCP designed to improve performance over wireless and mobile networks. It focuses on maintaining the end-to-end semantics of TCP while handling the frequent disconnections and handoffs in mobile environments.

Mobile TCP splits the connection at the Foreign Agent (FA), so the link between the Correspondent Host (CH) and FA uses standard TCP, while the FA manages the link to the Mobile Host (MH) separately to better handle disconnections and handovers.

**Merits of Mobile TCP:**

1. **Keeps End-to-End Connection:**
   The connection between sender and receiver stays intact.
2. **Avoids Unnecessary Retransmissions:**
   Stops sending data when the mobile device is temporarily unreachable.
3. **Supports Smooth Handover:**
   Handles switching between networks without breaking the connection.

**Demerits of Mobile TCP:**

1. **Complex Foreign Agent:**
   Needs extra logic and control at the base station or agent.
2. **Not Widely Used:**
   Requires special setup, not supported everywhere.
3. **May Increase Delay:**
   Pausing the connection during movement can cause delays.

25. What do you mean by hidden and exposed station problem. How can they be avoided.

**1. Hidden Station Problem**

Occurs when two stations (e.g., A and C) are out of range of each other but both can communicate with a common station (e.g., B).

**Problem:**

- Station A senses the channel as idle and sends data to B.
- At the same time, station C (which cannot sense A) also sends data to B.
- Collision occurs at B, even though A and C could not detect each other.

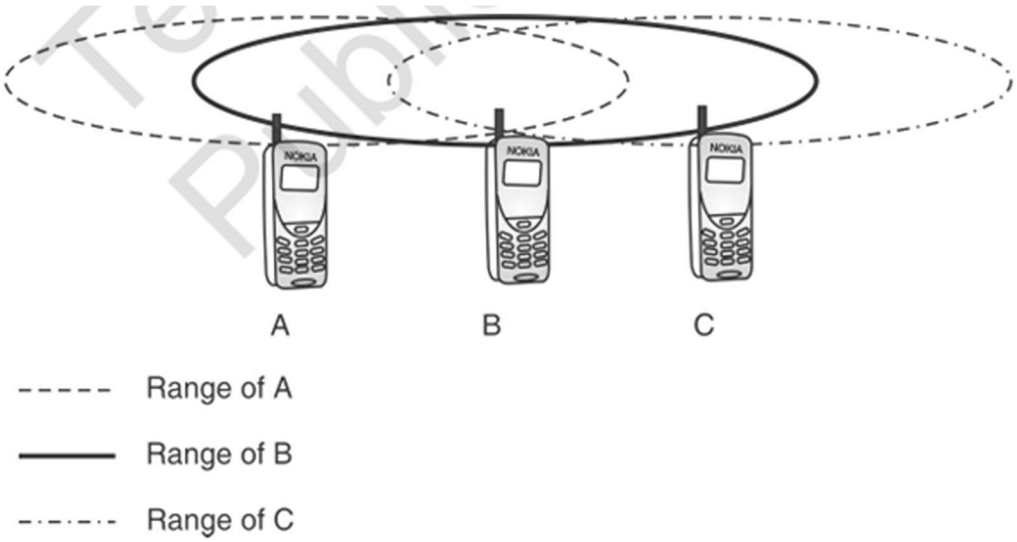



**Fig. 3.2.1 : Hidden station problem**

**Result:**

Increased collisions and reduced network performance.

**Solution:**

- Use RTS/CTS (Request to Send / Clear to Send) mechanism from IEEE 802.11 MAC protocol.
- Station A sends an RTS to B; B replies with CTS.
- CTS is heard by all nearby nodes (including C), so C stays silent, preventing collision.

**2. Exposed Station Problem**

Occurs when a station (e.g., C) refrains from transmitting due to sensing a nearby transmission (e.g., B → A), even though its transmission (C → D) would not interfere.

**Problem:**

- B senses the channel and finds it free. B starts transmitting data to A.
- C also wants to transmit data to D.
- C detects B's transmission, because B is within C's transmission range.

- C assumes the channel D is busy and delays its transmission, even though:
  - D is out of range of B's signal.
  - There would be no interference between B→A and C→D communication.

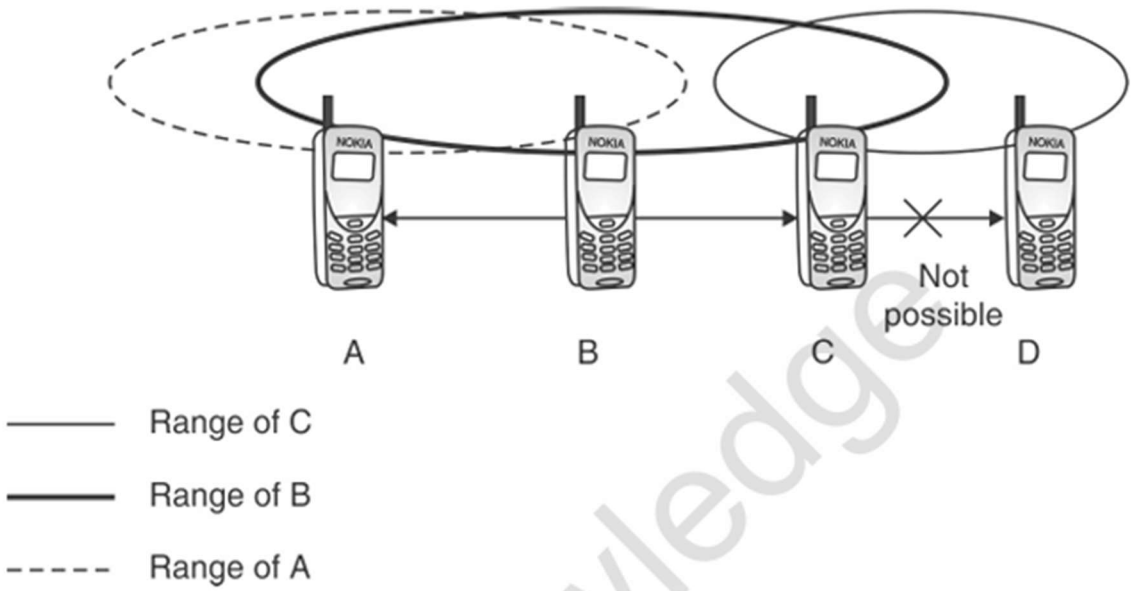



**Fig. 3.2.2 : Exposed Station (or Terminal) Problem**

**Result:**

Underutilization of the channel — reduced throughput.

**Solution:**

**Use RTS/CTS Mechanism:**

- C sends RTS to D.
- If D replies with CTS, it means the channel is clear for communication.
- Since D is not in range of B, it will respond, allowing C to send.

26. Write a short note on: Agent Advertisement and Agent Discovery. #

**1. Agent Advertisement:**

- Agents (Home or Foreign) periodically send Agent Advertisement messages.
- These messages are based on ICMP Router Advertisements with additional Mobile IP extensions.
- They inform mobile nodes of the agent's presence, type (Home or Foreign), and care-of address.
- Helps a mobile node determine if it is on its home or foreign network.

**2. Agent Discovery:**

- If no Agent Advertisements are received, a mobile node can actively send an Agent Solicitation message.
- Nearby agents respond with an Agent Advertisement.
- This process allows the mobile node to quickly discover available agents and register with the appropriate one for seamless IP connectivity.

27. Explain Tunnelling and Encapsulation in brief. What are the various types of Encapsulation techniques.

**Tunnelling:**

Tunnelling is the process of transmitting data packets from the Home Agent (HA) to the Mobile Node (MN) at its Care-of Address (COA) by encapsulating the original IP packet inside another IP packet.
It enables seamless packet delivery when the MN is away from its home network.

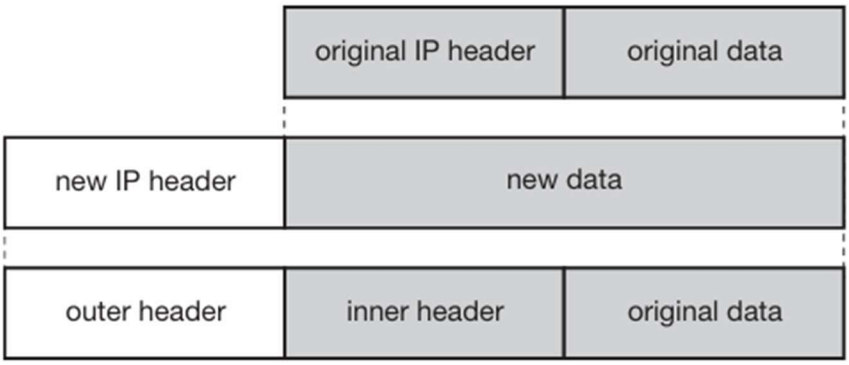
**Encapsulation:**

Encapsulation is the technique used in tunnelling to wrap the original IP packet inside a new packet with a new IP header.
This helps route the packet to the COA instead of the home address.

**Types of Encapsulation Techniques:**

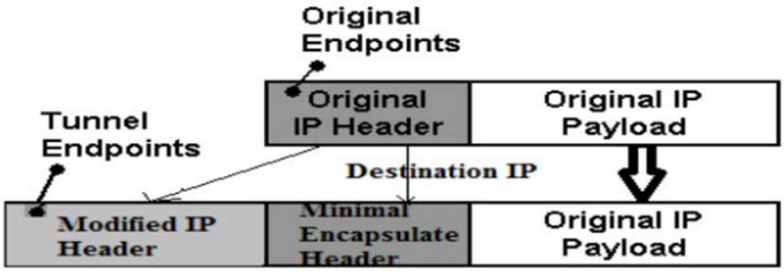
1. **IP-in-IP Encapsulation (RFC 2003):**

- Adds a new IP header in front of the original IP packet.
- Outer header: Source = HA, Destination = COA.
- Used when both HA and FA support IP-in-IP.



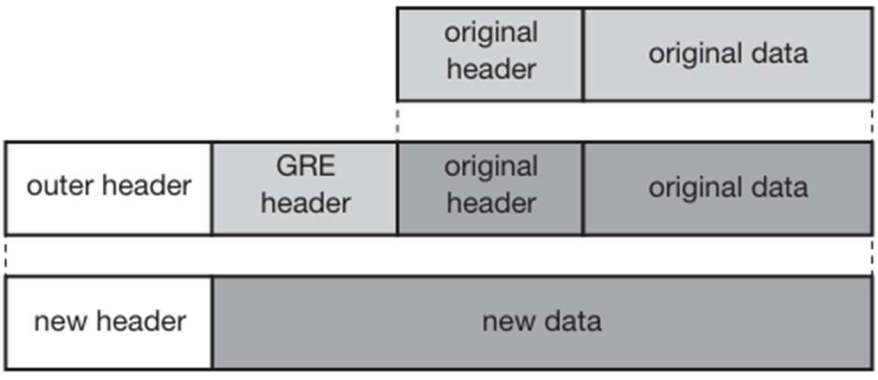

2. **Minimal Encapsulation (RFC 2004):**

- Reduces overhead by adding a minimal header instead of a full IP header.
- Used when saving bandwidth is important.




3. **Generic Routing Encapsulation (GRE) (RFC 1701):**

- Allows encapsulation of different network layer protocols.
- More flexible but adds extra overhead.
- Used when tunnelling across diverse network environments.



28. Explain agent registration process in mobile communication.

Agent registration is the process by which a Mobile Node (MN) registers its presence in a foreign network with its Home Agent (HA) through a Foreign Agent (FA). This allows the HA to forward packets to the MN's current location.

**Agent Registration Process in Mobile Communication:**

1. FA advertises its presence to nearby Mobile Nodes (MNs).
2. MN detects it's in a foreign network and obtains a Care-of Address (COA).
3. MN sends a Registration Request to the Home Agent (HA) via the Foreign Agent (FA) or directly.
4. FA forwards the request to HA if it's not a direct registration.
5. HA verifies the request and updates its mobility binding table with MN's COA.
6. HA sends a Registration Reply back to the FA or MN indicating success/failure.
7. FA (if used) forwards the reply to the MN.
8. MN receives the reply and starts receiving tunnelled packets at the COA.

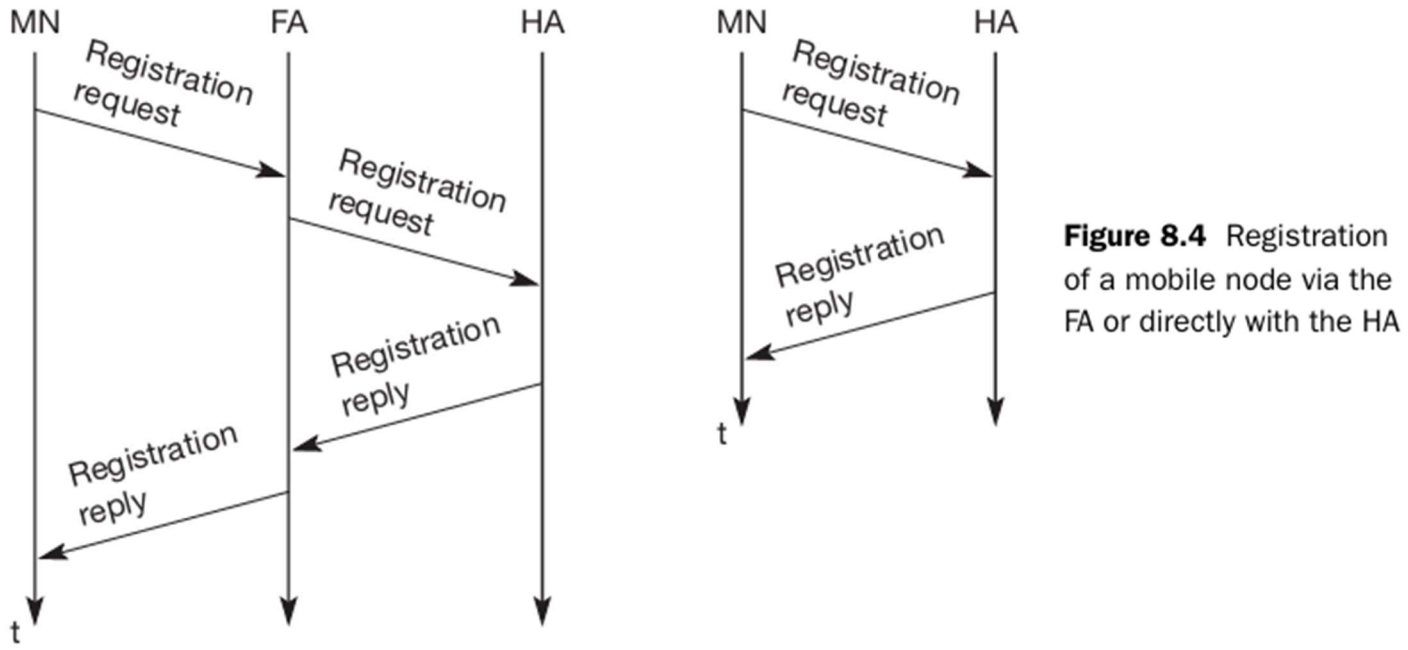
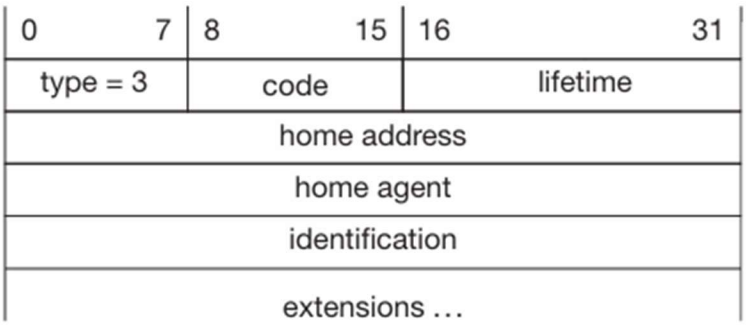



**Figure 8.4** Registration of a mobile node via the FA or directly with the HA


**Registration request message**




**Registration reply message**

**Registration Message Fields (Request & Reply)**

• **Type**:
– 1 for Registration Request
– 3 for Registration Reply

• **Lifetime**:
Indicates the time duration of registration.
– In Request: Requested by the Mobile Node.
– In Reply: Granted by the Home Agent.

• **Home Address**:
Permanent IP address of the Mobile Node (MN). Must match in both Request and Reply.

• **Home Agent**:
IP address of the Home Agent (HA) responsible for the MN.

• **Identification**:
Unique value used to prevent replay attacks. Must match between Request and Reply.

• **Extensions**:
Optional fields for authentication or additional information.

• **Flags (in Request only)**:
Control bits like S, B, D, M, G, r, T, x.
Enable features such as simultaneous bindings, reverse tunnelling, etc.

• **Care-of Address (COA) [Request only]**:
Temporary IP address where the MN is currently located (in the foreign network).

• **Code [Reply only]**:
Indicates registration status (e.g., success, denial, or error type).

## 29. What is reverse tunnelling? #

**Reverse Tunnelling** in Mobile Networking refers to a process where packets from a Mobile Node (MN) are sent back to the Home Agent (HA) before being forwarded to the Correspondent Node (CN), rather than going directly from the foreign network to the CN.

**Purpose of Reverse Tunnelling:**

1. **Security Compliance:** Many networks block traffic with a source IP address that doesn't match their range. Reverse tunnelling ensures packets appear to come from the mobile node's home network.
2. **Policy Enforcement:** Helps apply firewall rules, billing, and other policies based on home network rules.
3. **Simplifies Routing:** Avoids triangular routing (MN → CN, CN → HA → MN) and allows symmetrical paths through HA.

## 30. Explain selective transmission process at TCP.

Selective Transmission, also known as Selective Acknowledgment (SACK), is a process in TCP where the receiver informs the sender about specific segments that have been received correctly, even if they arrived out of order.

**Why it's needed:**

- In standard TCP (without SACK), if a segment is lost, the sender may retransmit several segments, even if only one was missing.
- This causes redundant retransmissions and wastes bandwidth.

**Working:**

1. **Data Transmission:**
   The sender sends multiple TCP segments.
2. **Loss Occurs:**
   Suppose a few segments are lost (e.g., segment 3 is lost, but 4 and 5 are received).
3. **SACK Option Enabled:**
   The receiver sends an acknowledgment with a SACK option, indicating:
   - "Segment 3 is missing"
   - "I have received segments 4 and 5"
4. **Selective Retransmission:**
   The sender only retransmits segment 3, not 4 or 5 again.
5. **Efficient Recovery:**
   This improves performance, especially in high-delay or high-loss networks.

**Advantages of Selective Transmission:**

- Reduces unnecessary retransmissions
- Increases TCP efficiency

# 4. Wireless Local Area Networks

31. Explain the protocol architecture of IEEE 802.11 with diagram.

The IEEE 802.11 standard defines the protocol architecture for Wireless Local Area Networks (WLANs). It describes how data is transmitted and managed over wireless networks.

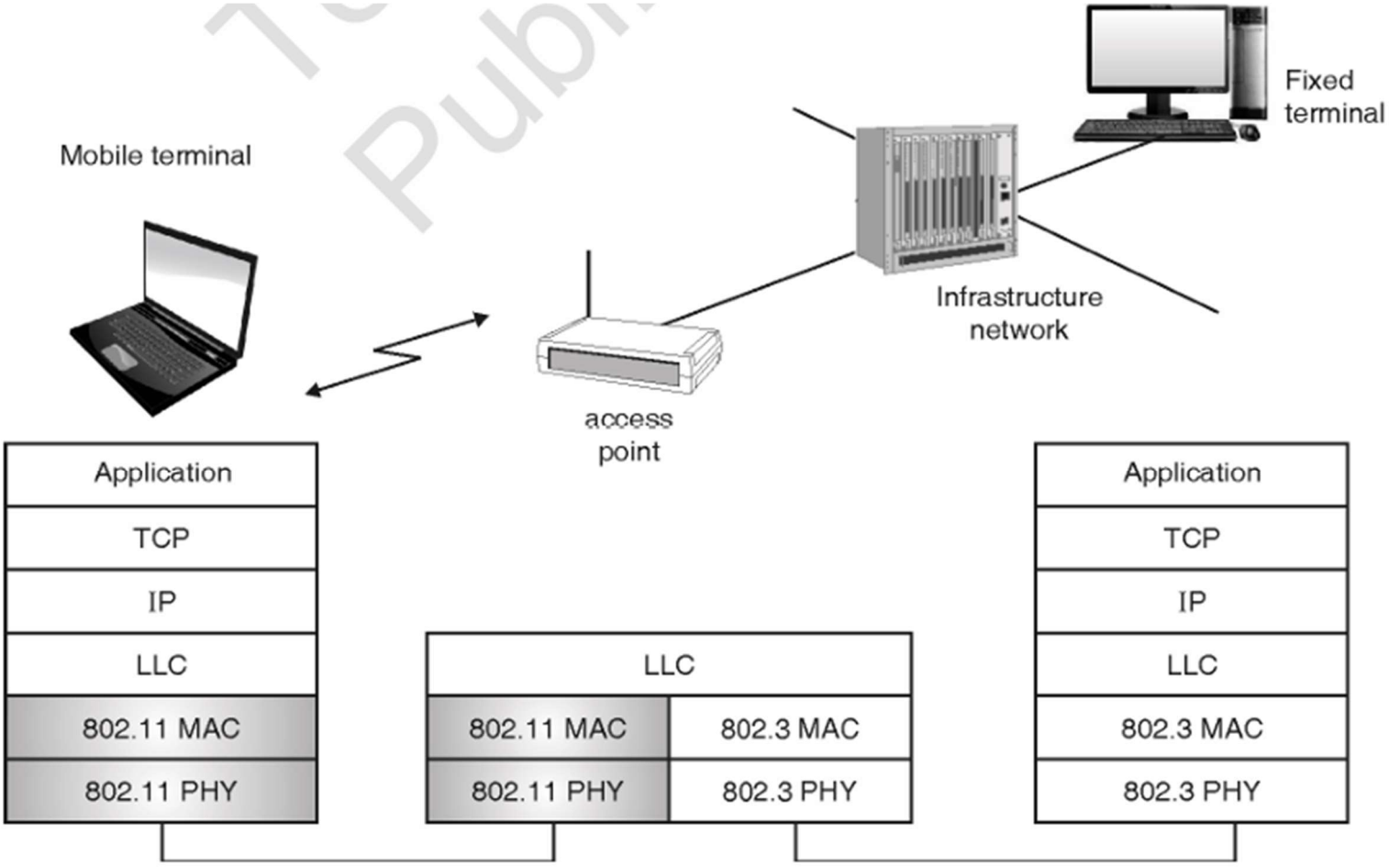



**Fig. 4.2.3 : IEEE 802.11 protocol architecture and bridging**

This diagram shows how a wireless device connects to a wired network using Wi-Fi (IEEE 802.11) through an Access Point (AP).
The AP bridges two networks:

- **Wireless (IEEE 802.11)**
- **Wired Ethernet (IEEE 802.3)**

Though they use different MAC and PHY layers, they share a common LLC layer, enabling communication.
The AP translates between the protocols, allowing both devices to use the same TCP/IP applications as web browsing or email.
This setup enables smooth communication in infrastructure-based wireless networks.

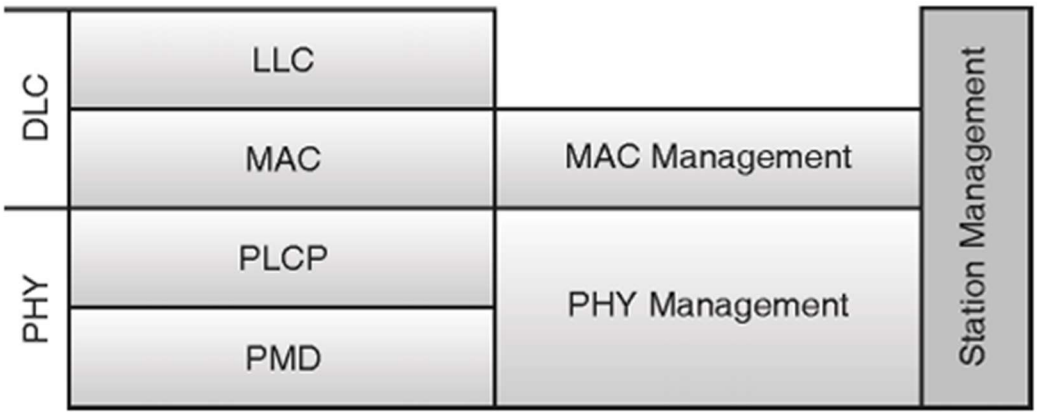



**Fig. 4.2.4 : IEEE protocol architecture and management**

1. **Physical Layer (PHY):**
    - Responsible for wireless signal transmission and reception.
    - Defines modulation techniques (e.g., OFDM, DSSS) and data rates.
    - Divided into three sublayers:
        - **PMD (Physical Medium Dependent):** Responsible for actual modulation and transmission of signals.
        - **PLCP (Physical Layer Convergence Protocol):** Prepares data for transmission and adds headers.
        - **PHY Management:** Coordinates physical layer functions.
2. **MAC Layer (Medium Access Control):**
    - **MAC (Medium Access Control):** Manages channel access, CSMA/CA for collision avoidance, and frame control.
    - **MAC Management:** Handles scanning, authentication, and association processes.
3. **LLC Layer (Logical Link Control):**
    - Provides flow and error control for data transmission.
    - Interfaces with higher network layers (e.g., TCP/IP).

32. Explain Wireless LAN threats.

**1. Eavesdropping:** Attackers use tools like Wireshark to intercept unencrypted wireless traffic and extract sensitive information.

**2. Rogue Access Points**: Malicious individuals set up unauthorized access points with similar SSIDs to legitimate networks, tricking users into connecting and exposing their credentials.

**3. Man-in-the-Middle (MITM) Attacks**: In MITM attacks, hackers intercept and manipulate data between two parties without their knowledge, leading to data breaches.

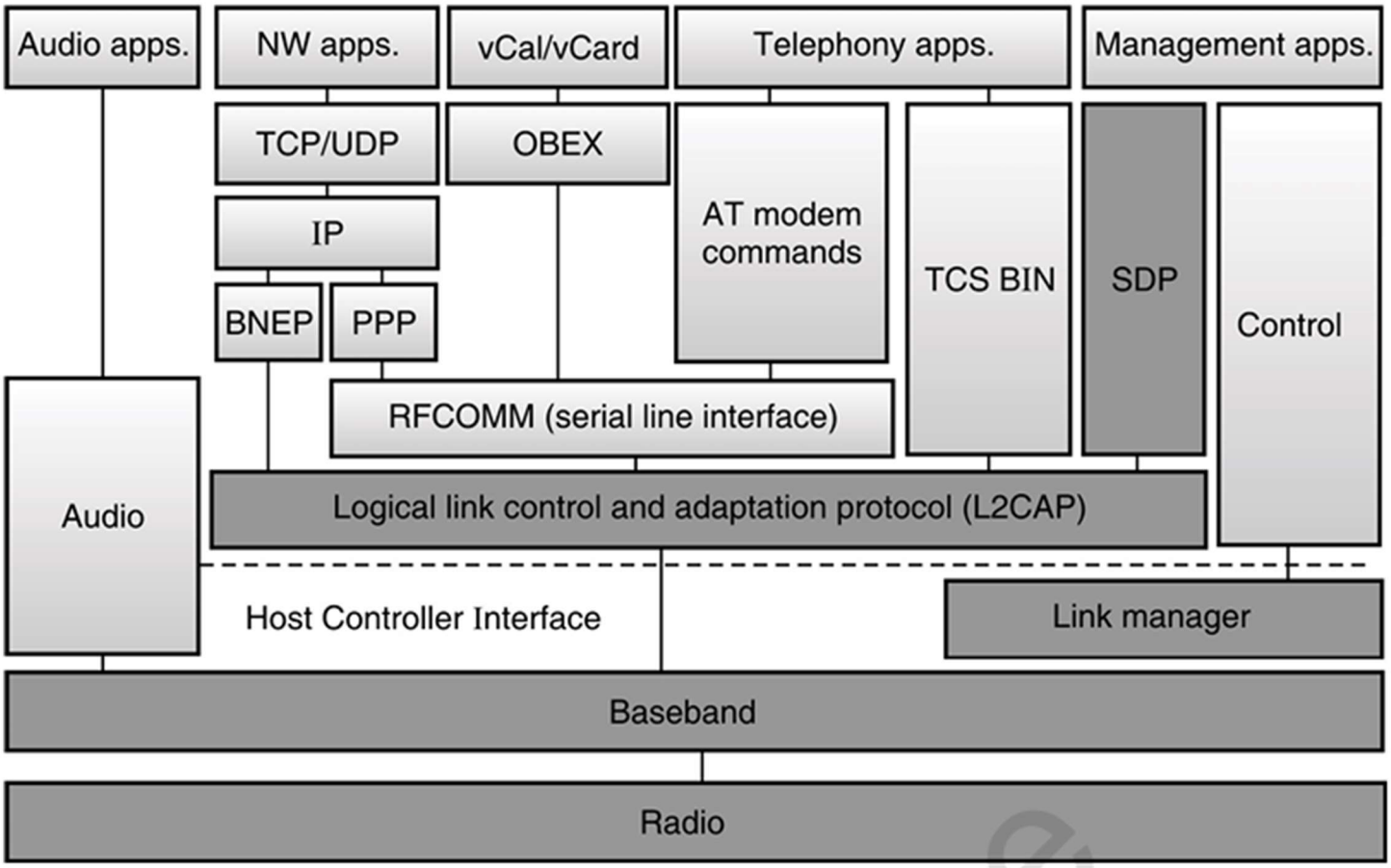
**4. Denial of Service (DoS) Attacks**: Attackers flood the Wi-Fi network with excessive traffic, causing it to slow down or crash, disrupting legitimate user access.

**5. Passive Capturing:** Eavesdropping on wireless networks without actively interfering. Attackers silently capture packets and later analyze them to extract sensitive data like passwords or session tokens.

**6. Configuration Problems:** Incorrect or incomplete settings on wireless routers or APs (e.g., open SSID, weak encryption). Leaves the network open to unauthorized users or easy to hack.

**7. Misbehaving Clients:** Sometimes clients form unauthorized Wi-Fi connections accidentally or intentionally. By doing this, they put themselves and corporate data at risk.

33. Explain Bluetooth Protocol Stack in detail.




The Bluetooth stack is divided into three main sections:

1. **Application Layer**
2. **Host Stack (Software)**
3. **Controller Stack (Hardware)**

**1. Application Layer**

This is where user applications work—such as:

i. **Audio apps:** For streaming music.

ii. **Network (NW) apps:** For internet sharing.

iii. **Telephony apps:** For calls.

iv. **vCal/vCard apps:** For sharing contacts and calendar events.

v. **Management apps:** For controlling and managing Bluetooth services.

**2. Host Stack (Software Protocols)**

**L2CAP (Logical Link Control and Adaptation Protocol)**

- Acts like a middleman to adapt different app needs to the Bluetooth baseband.
- Most protocols pass through L2CAP.

**RFCOMM**

- Emulates serial cable communication.
- Used by many Bluetooth profiles like file transfer and headset.

**SDP (Service Discovery Protocol)**

- Helps devices discover each other's services (e.g., check if a device supports file sharing).

**BNEP**

- Used for sending Ethernet packets.
- Part of Bluetooth PAN for network sharing.

**OBEX**

- Supports object exchange (used in file transfers)

**PPP**

- Used for dial-up networking over Bluetooth.

**TCS BIN & AT Commands**

- Used in telephony:
    - TCS BIN: Call control.
    - AT commands: Control modems (used in headsets or phones).

**Audio**

- Sends audio streams directly to the controller (bypasses L2CAP).

**Control**

- Handles device management functions like pairing, role switching, etc.

**3. Controller Stack (Firmware/Hardware)**

**Host Controller Interface (HCI)**

- Connects the Host (software) and Controller (hardware).
- Transports commands, data, and events.

**Link Manager**

- Handles link setup, authentication, encryption, and QoS negotiation.

**Baseband**

- Converts packets for wireless transmission. Handles error correction and flow control.

**Radio**

- Actual transmitter and receiver of Bluetooth signals in the 2.4 GHz ISM band.

## 34. Compare Infrastructure based network with Ad-hoc network. #

| Aspect | Infrastructure-Based Network | Ad-hoc Network |
|---|---|---|
| **Definition** | A network with a central device like a router or base station. | A network formed by devices communicating directly with each other. |
| **Control** | Centralized control. | Decentralized control. |
| **Setup** | Requires setup and configuration of access points. | No fixed setup; created dynamically. |
| **Communication** | Through access point or router. | Direct device-to-device communication. |
| **Mobility** | Limited mobility. | High mobility support. |
| **Scalability** | Easily scalable with more infrastructure. | Limited scalability due to device constraints. |
| **Power Consumption** | Less power used by devices, as central unit handles most tasks. | More power used by each device, as all share equal responsibility. |
| **Examples** | Wi-Fi in homes, cellular networks. | Bluetooth sharing, disaster recovery communication. |

## 35. Discuss in detail about Wi-Fi security protocol.

Wi-Fi security protocols are standards used to protect wireless communications between devices and access points. They ensure data confidentiality, integrity, and user authentication. Here's a detailed discussion of the major Wi-Fi security protocols:

**1. WEP (Wired Equivalent Privacy)**

- **Introduced:** 1997 (original IEEE 802.11 standard)
- **Key Features:**
  - Uses RC4 encryption with 40-bit or 104-bit keys.
  - Provides basic data encryption.
- **Weaknesses:**
  - Easily cracked due to weak key management and IV reuse.
  - Obsolete - not secure for modern networks.

**2. WPA (Wi-Fi Protected Access)**

- **Introduced:** 2003 (temporary improvement over WEP)
- **Key Features:**
  - Uses TKIP (Temporal Key Integrity Protocol) for dynamic key generation.
  - Message Integrity Check (MIC) to prevent packet tampering.
- **Weaknesses:**
  - Still relies on RC4 (like WEP).
  - Vulnerable to some attacks; not considered fully secure.

**3. WPA2 (Wi-Fi Protected Access II)**

- **Introduced:** 2004 (mandatory from 2006)
- **Key Features:**
  - Uses AES (Advanced Encryption Standard) — much stronger than RC4.
  - Supports **CCMP** (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).
  - Two modes:
    - **WPA2-Personal (PSK):** For home use (shared password).
    - **WPA2-Enterprise:** Uses RADIUS server for authentication.
- **Weaknesses:**
  - Vulnerable to brute-force attacks on weak passwords.
  - KRACK attack (2017) exploited flaws in key exchange.

**4. WPA3 (Wi-Fi Protected Access III)**

- **Introduced:** 2018
- **Key Features:**
  - **SAE (Simultaneous Authentication of Equals):** Replaces PSK — more secure handshake.
  - **Stronger encryption (192-bit)** for enterprise networks.
  - **Forward secrecy** — Past sessions stay secure even if the password is later compromised.
- **Advantages:**
  - More resistant to dictionary and brute-force attacks.
  - Improves security on open networks (e.g., public Wi-Fi).

**Summary:**

| Protocol | Encryption | Key Management | Security Level | Status |
|---|---|---|---|---|
| **WEP** | RC4 | Static key | Weak | Deprecated |
| **WPA** | RC4 (with TKIP) | Dynamic key | Moderate | Legacy |
| **WPA2** | AES (with CCMP) | Stronger key exchange | Strong | Widely used |
| **WPA3** | AES-192/SHA-384 (Enterprise) | SAE handshake | Very Strong | Latest Standard |

## 36. Write a short note on: Bluetooth. #

**Definition:**
Bluetooth is a short-range wireless communication technology used to exchange data between fixed and mobile devices over short distances.

**Key Features:**

- Operates in the 2.4 GHz ISM band.
- Range: typically, 10 meters, can go up to 100 meters (Class 1).
- Low power consumption, suitable for personal area networks (PAN).
- Uses frequency hopping to avoid interference.
- Supports voice and data transmission.

**Applications:**

- Wireless headsets, keyboards, mice.
- File sharing between smartphones.
- Smart home devices and wearables.

## 37. Write a short note on: HIPERLAN #

**Definition:**
HIPERLAN is a set of wireless communication standards developed by ETSI (European Telecommunications Standards Institute) to provide high-speed WLANs.

**Types:**

- **HIPERLAN/1**: Introduced in 1996, data rate up to 20 Mbps.
- **HIPERLAN/2**: Introduced in 2000, data rate up to 54 Mbps, similar to IEEE 802.11a.

**Key Features:**

- Operates in the 5 GHz frequency band.
- Supports QoS (Quality of Service) for multimedia.
- Provides stronger security and flexible architecture.
- Designed for high-speed indoor wireless access.

**Status:**

- Largely superseded by Wi-Fi (IEEE 802.11) standards due to wider adoption.

## 38. What is the responsibility of MAC management in IEEE 802.11?

In IEEE 802.11 (Wireless LAN), MAC Management is responsible for controlling and managing how devices communicate and stay connected within the network.

The key responsibilities of MAC Management include: synchronization, power management, association/reassociation, and maintaining the MAC Management Information Base (MAC MIB).

**1. Synchronization**

- In a wireless LAN, all stations (devices) must stay synchronized to ensure proper communication.
- Access Points (APs) send out beacon frames at regular intervals.
- These beacons contain timing information that helps stations adjust their clocks and maintain timing alignment.
- This is crucial for timing operations like sleep/wake cycles in power-saving modes.

**2. Power Management**

- Allows devices to conserve battery by entering low-power (sleep) mode when not transmitting or receiving.
- Stations can inform the AP when they enter power-saving mode.
- During this time, the AP buffers any incoming data for the sleeping device.
- Devices periodically wake up to check for buffered data (via beacon frames).

**3. Association / Reassociation**

- **Association**: The process where a station connects to an AP to gain access to the network.
    - Involves exchanging association request/response frames.
    - The AP assigns an Association ID (AID**)** to the station.
- **Reassociation**: Happens when a mobile station moves from one AP's range to another.
    - Ensures seamless handoff and continuous connectivity (important for roaming).

**4. MAC Management Information Base (MAC MIB)**

- It is a database of parameters and status information maintained by each station or AP.
- Contains:
    - Configuration settings (SSID, supported rates, etc.)
    - Current state (associated, authenticated, etc.)
    - Performance data (packet counts, error rates, etc.)
- Used by network management systems to monitor and control wireless communication effectively.

## 39. Explain the terms PICONET and Scatternet in terms of Bluetooth. #

**PICONET:**

- A Piconet is a small Bluetooth network formed by one master device and up to seven active slave devices.
- The master controls the communication and clock synchronization.
- Only one device acts as master at a time.
- All devices share the same physical channel (frequency hopping pattern).
- **Example:** A Bluetooth speaker (master) connected to a phone, tablet, and laptop (slaves).

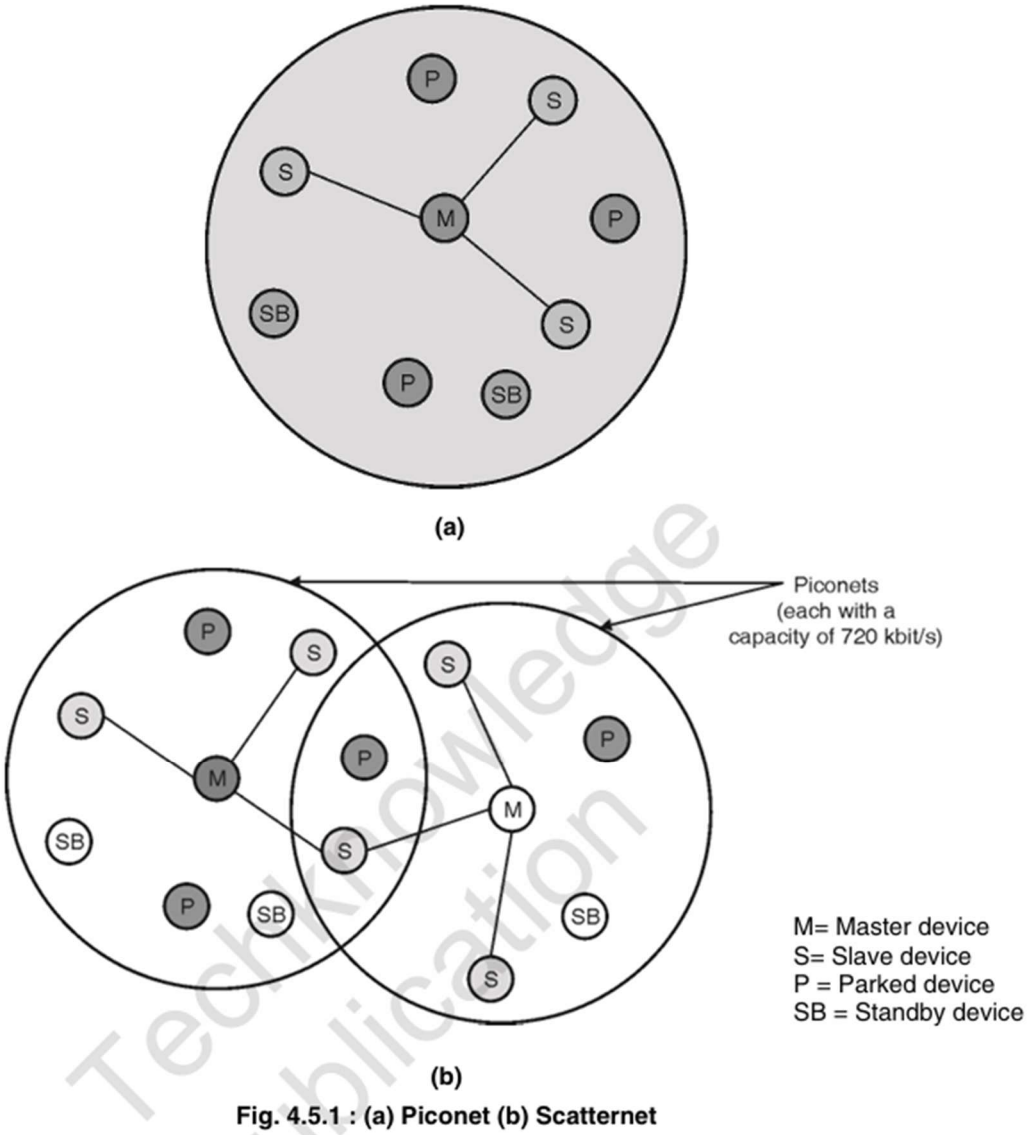



Fig. 4.5.1 : (a) Piconet (b) Scatternet

**SCATTERNET:**

- A Scatternet is formed when two or more piconets are interconnected through common devices.
- A device that participates in multiple piconets (as master in one and slave in another) acts as a bridge.
- This allows for larger and more flexible Bluetooth networks.
- **Example:** A phone connected to a smartwatch in one piconet and also to a laptop in another piconet.

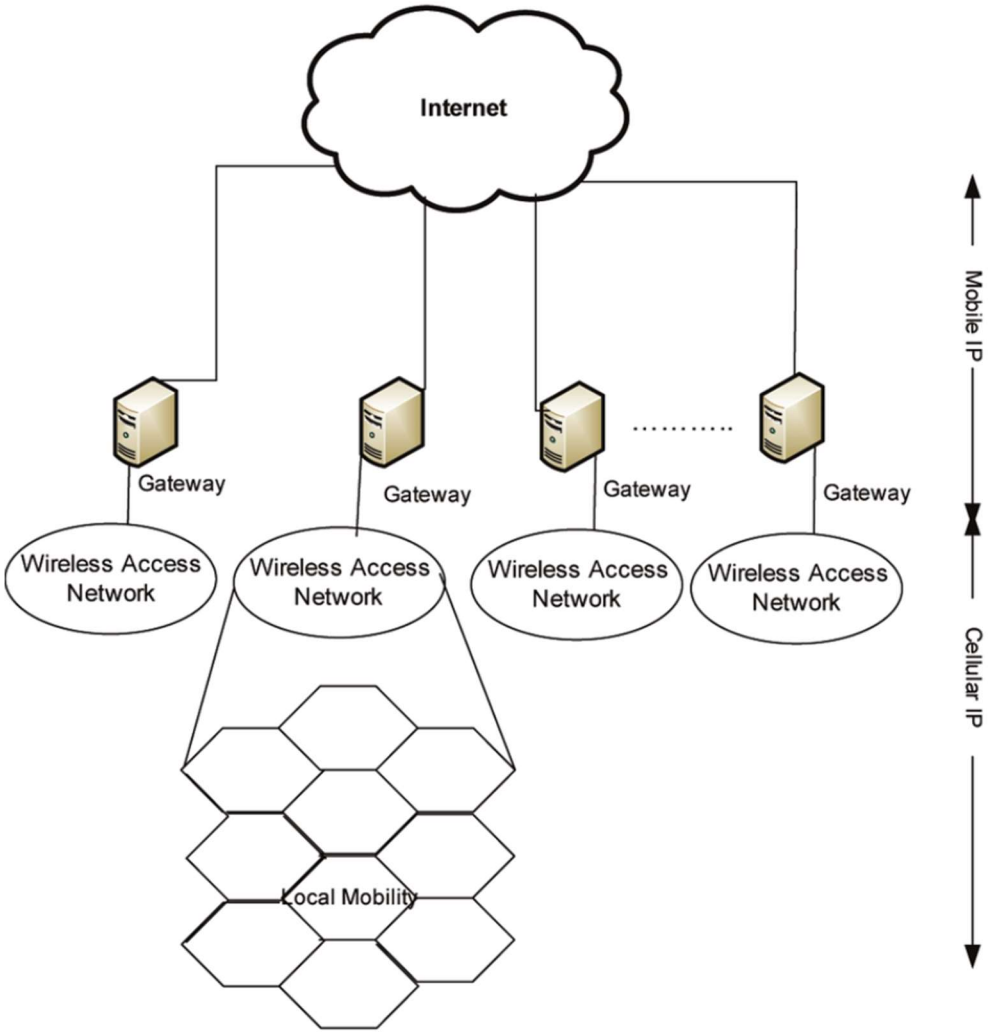
## 40. How can we secure wireless networks. #

1. **Use an uncommon network name (SSID)**
   Don’t use common names like "Wi-Fi" to avoid easy guessing by attackers.
2. **Use WPA3 with 802.1X authentication**
   Give each user a unique login so one stolen password doesn’t affect everyone.
3. **Use firewalls to protect Wi-Fi**
   A firewall blocks hackers and protects your devices from outside threats.
4. **Restrict access (MAC filtering)**
   Allow only known devices to connect using their unique hardware address.
5. **Encrypt data on your network**
   Use strong encryption like WPA3 so others can’t read your data.
6. **Keep antivirus updated**
   Regularly update antivirus software to block viruses and spyware.
7. **Use a VPN**
   A VPN hides your online activity and protects your data when connected remotely.

# 5. Mobility Management

41. Explain Cellular IP and its use in detail.

Cellular IP is a mobile IP protocol designed to support fast and efficient handover in wireless networks while minimizing signalling overhead. It is primarily used in cellular and wireless networks to ensure seamless mobility for users moving between different access points.




**Working of Cellular IP:**

1. Mobile Host (MH) moves inside a local domain (WAN).
2. It is always connected to the nearest base station.
3. Cellular IP routers maintain a routing cache by monitoring packets sent by the mobile node.
4. The routing cache creates a soft state path from the Gateway to the MN.
5. When the MN moves, this path is automatically updated.

**Advantages:**

- Lightweight protocol with low overhead.
- Fast handoff without heavy signalling.
- Suitable for high-speed movement in small regions.

**Limitations:**

- Not suitable for large-scale or global mobility.
- Requires all routers in the access network to support Cellular IP.

**Key Uses of Cellular IP:**

1. **Seamless Handover:**
    - Supports fast handover between base stations without disrupting ongoing connections.
2. **Efficient Packet Routing:**
    - Routes packets dynamically based on mobile node movements, reducing latency.
3. **Reduced Signalling Overhead:**
    - Uses passive monitoring of data packets to update routing tables, avoiding excessive control messages.
4. **Supports Local Mobility:**
    - Ideal for users moving within a specific network, like within a university campus or corporate office.
5. **Power Efficiency:**
    - Minimizes signalling, which helps save battery power in mobile devices.
6. **Scalability:**
    - Can support large numbers of mobile users without excessive network congestion.

42. What is micro mobility, its need and its approaches?

Micro-mobility manages seamless movement of mobile devices within a local or regional network, ensuring low-latency handovers within a single administrative domain. It is crucial for real-time applications like VoIP, online gaming, and video streaming.

**Need for Micro-Mobility**

1. **Reduces Handoff Latency**
    - Ensures faster handover between access points.
2. **Scalable Signalling**
    - Limits signalling to the local network, reducing global routing updates.
3. **Efficient Resource Usage**
    - Avoids overload on global mobility protocols like Mobile IP.

Three major protocols are Cellular IP, HAWAII, and HMIPv6.

**Cellular IP –** A micro-mobility protocol designed for seamless movement of mobile nodes within an IP-based network. Unlike global mobility protocols, it optimizes local handovers using a routing cache, ensuring uninterrupted connectivity with minimal overhead.

**Advantages of Cellular IP:**

1. **Seamless Local Handover:** Maintains uninterrupted connectivity by using routing cache during node movement.
2. **Low Overhead:** Optimizes local handovers without relying on global mobility protocols.

**HAWAII (Handoff-Aware Wireless Access Internet Infrastructure) –** Implements a hierarchical mobility management approach to enhance efficiency. By localizing handover processes, it minimizes global signalling overhead, making it ideal for scalable and efficient micro-mobility management.

**Advantages of HAWAII:**

1. **Reduced Global Signalling:** Localizes handover processes to minimize signalling overhead.
2. **Scalability:** Well-suited for large networks due to its hierarchical structure.

**Hierarchical Mobile IPv6 (HMIPv6) –** An advanced extension of Mobile IPv6 that introduces a dual-level mobility management system. By segmenting handovers into local and global domains, HMIPv6 significantly reduces signalling traffic, improves handoff speed, and enhances network performance for mobile users.

**Advantages of HMIPv6:**

1. **Improved Handoff Speed:** Segregates local and global domains for faster handovers.
2. **Lower Signalling Traffic:** Reduces global network load by handling updates locally.

## 43. Write a short note on: IPv6. #

**IPv6 (Internet Protocol version 6)** is the latest version of the Internet Protocol, developed to replace IPv4 due to address exhaustion and to support the growing number of internet-connected devices.

**Key Features:**

- **128-bit Addressing**: Supports an enormous number of IP addresses.
- **Simplified Header**: Speeds up packet processing.
- **Built-in IPsec**: Ensures data confidentiality and integrity.

**Advantages:**

- No more IP address shortage.
- Removes the need for NAT (Network Address Translation).
- Improved QoS (Quality of Service)

**Applications of IPv6:**

1. **Internet of Things (IoT):**
   IPv6 offers ample addresses for billions of smart devices.
2. **Cloud Computing:**
   Ensures scalable, secure, end-to-end cloud connectivity.

## 44. How is IP mobility achieved in wireless network.

**Mobility management** in wireless networks ensures that a mobile device (Mobile Node or MN) can maintain ongoing internet connections while moving across different networks. This is achieved through IP mobility protocols that allow seamless handover without changing the IP address.

**Mobile IP (IP Mobility)**

Mobile IP enables devices to have two IP addresses; The mobile device keeps its permanent Home Address but gets a temporary Care-of Address (CoA) in a foreign network. It registers the CoA with its Home Agent (HA), which forwards incoming packets to the CoA, allowing seamless connectivity while moving.

IP mobility is achieved using both macro and micro mobility approaches:

**Macro Mobility**

- Deals with inter-domain mobility (moving across different administrative domains or ISPs).
- **Mobile IPv6 (MIPv6)** is a protocol enhancement of IPv6 that enables devices to retain their IP addresses while moving between different networks.
- **Fast Mobile IPv6 (FMIPv6)** improves MIPv6 by reducing handover delays. It predicts movement and prepares a connection in advance, ensuring minimal packet loss.

**Micro Mobility**

- Handles intra-domain mobility (movement within the same network domain, e.g., a campus).
- **Cellular IP:** Routing-based local mobility with dynamic routes for fast handoff.
- **HAWAII:** Hierarchical routing that sets up paths only along the mobile node's route to reduce signalling.
- **HMIPv6:** Uses local Mobility Anchor Points to handle micro mobility and reduce load on the Home Agent.

# 6. Long Term Evolution of 3GPP

## 45. What do you mean by Self Organizing Network. Explain the architecture of SON.

A **Self-Organizing Network (SON)** is an automation technology in mobile networks that enables the network to automatically configure, optimize, and recover itself with minimal human intervention. SON is crucial for modern mobile networks (like LTE and 5G), helping operators manage growing complexity, improve performance, and reduce operational costs.

**Key Functions of SON**

- **Self-configuration**: Automatically sets up new network elements (e.g., base stations) for plug-and-play deployment.
- **Self-optimization**: Continuously adjusts network parameters to improve performance and user experience.
- **Self-recovery**: Detects and remedies network faults or outages, often by reconfiguring neighbouring elements

**Centralized SON:**

- All SON functions are located in the OAM (Operations, Administration, and Maintenance) system.
- The OAM is a centralized unit connected to all eNBs (base stations).
- Optimization algorithms (like load balancing, handover management) are executed at this central point.

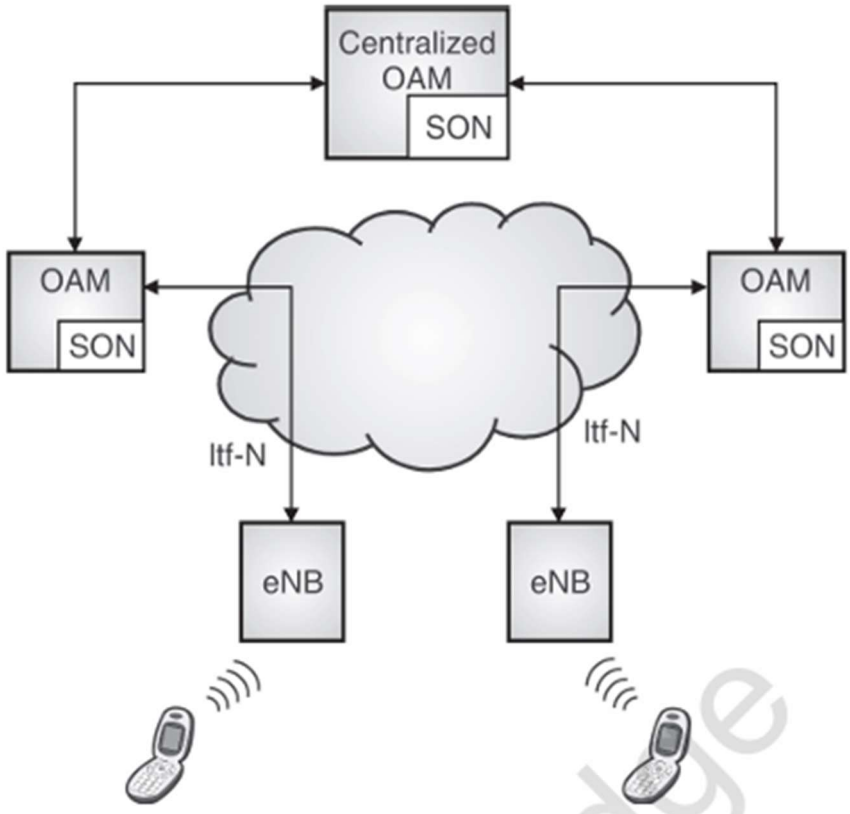



Fig. 6.8.2 : Centralized SON

**Distributed SON:**

- SON algorithms are executed inside each eNB (e.g., eNB1, eNB2, etc.).
- Each base station performs optimization based on local conditions (e.g., adjusting handover thresholds, interference control).
- SON logic is spread across multiple nodes at a lower architectural level.

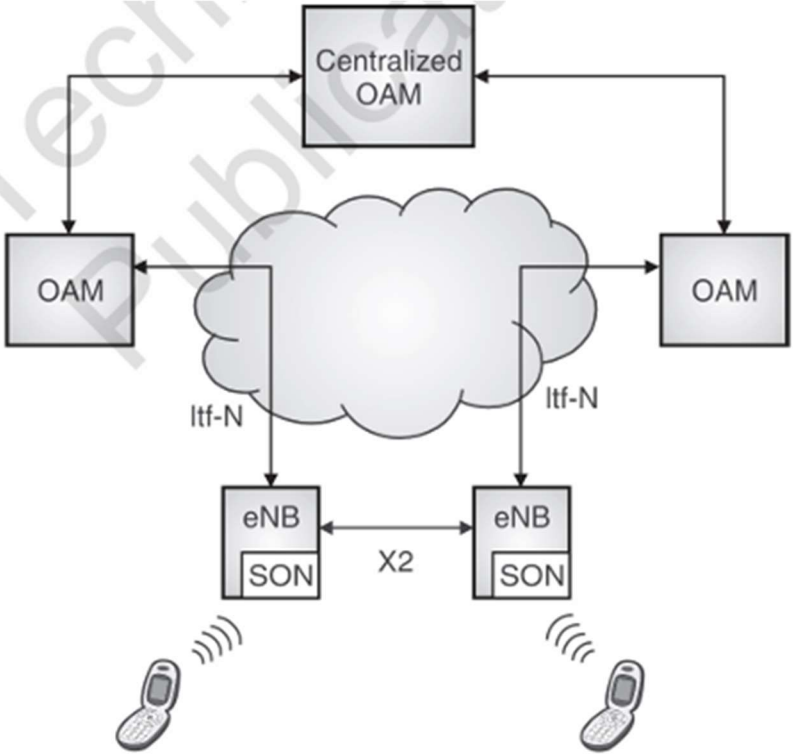



Fig. 6.8.3 : Distributed SON

**Hybrid SON:**

- A combination of both Centralized and Distributed SON.
- Simple and fast optimizations (like interference mitigation) are handled locally in eNBs.
- Complex, network-wide optimization tasks (like network-wide load balancing) are handled centrally at the OAM.

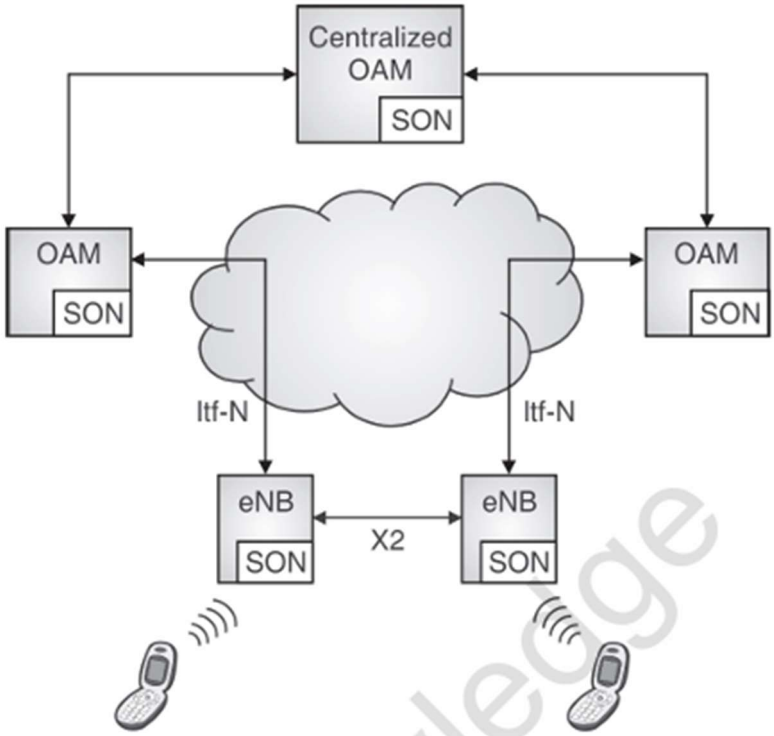



Fig. 6.8.4 : Hybrid SON

## 46. Explain self-organizing networks(SON) for heterogeneous networks.

- It was estimated that there would be 50 billion connected devices by 2020, and the demand for higher data rates continues to increase.
- High-quality video streaming, social networking, and machine-to-machine (M2M) communication over wireless networks are growing exponentially.
- As a result, a new paradigm called Heterogeneous Networks (HetNets) is being adopted by network operators.

**HetNet** involves a mix of radio technologies, different cell types, distributed antenna systems, and Wi-Fi working together seamlessly.

A HetNet includes the following aspects:

- Use of multiple radio access technologies.
- Operation of different cell sizes (macro, micro, pico, femto)
- Heterogeneous backhaul solutions (e.g., wired, wireless, fiber)

**1. Use of Multiple Radio Access Technologies (RATs)**

HetNets combine different wireless communication technologies—such as LTE, 5G NR, Wi-Fi, and even legacy technologies like 3G—into a unified network.
This allows users to:

- Stay connected using the best available technology.
- Seamlessly switch between Wi-Fi and cellular networks.
- Improve coverage and capacity, especially in high-traffic areas.

**2. Different sizes of cells**

| Characteristics | Femto | Pico | Micro | Macro |
|---|---|---|---|---|
| Indoor/Outdoor | Indoor | Indoor or outdoor | Outdoor | Outdoor |
| Number of users | 4 to 16 | 32 to 100 | 200 | 200 to 1000++ |
| Maximum cell radius | 10 to 50 m | 200 m | 2 km | 10 to 40 km |
| Bandwidth | 10 MHz | 20 MHz | 20 to 40 MHz | 60 to 75 MHz |

**3. Heterogeneous Backhaul Solutions**

Backhaul refers to the connection between the base station (or access point) and the core network. In HetNets, these connections can be:

- **Wired** (e.g., fiber optics, DSL)
- **Wireless** (e.g., microwave, mmWave)

- **Hybrid**

The use of different backhaul technologies allows:

- Flexible deployment of small cells.
- Cost-effective scaling of the network.
- Maintaining connectivity even in hard-to-wire locations.

## 47. Compare LTE and LTE advanced. #

| Feature | LTE (Long Term Evolution) | LTE-Advanced (LTE-A) |
|---|---|---|
| **Release** | 3GPP Release 8 | 3GPP Release 10 and beyond |
| **Peak Download Speed** | Up to 100 Mbps | Up to 1 Gbps |
| **Peak Upload Speed** | Up to 50 Mbps | Up to 500 Mbps |
| **Carrier Aggregation** | Not supported | Supported (combines multiple frequency bands) |
| **MIMO Support** | 2x2 MIMO | Up to 8x8 MIMO |
| **Latency** | ~10 ms | <5 ms |
| **Spectral Efficiency** | Moderate | Higher (more data per bandwidth) |
| **Relay Nodes** | Not supported | Supported (improves coverage & performance) |
| **Overall Performance** | Good | Much better in speed, coverage, and capacity |

## 48. Explain in short voice over LTE (VoLTE). #

**Voice over LTE** is a technology that enables voice calls to be transmitted over the LTE network using an all-Internet Protocol framework. It replaces traditional circuit-switched calling and offers benefits such as superior high-definition voice quality, faster call setup times, and the ability to use voice and data services simultaneously. Voice over LTE operates through the IP Multimedia Subsystem(IMS), which manages call signalling, authentication and session control.

**Call Flow in VoLTE**

1. **Call Setup:** The UE registers with the IMS core, and SIP (Session Initiation Protocol) is used to establish a call.
2. **Media Transport:** The voice packets are transmitted over LTE using RTP (Real-Time Transport Protocol).
3. **Call Handover:** If the LTE signal is weak, the call is handed over to a 3G network using SRVCC (Single Radio Voice Call Continuity).
4. **Call Termination:** The session ends when either party disconnects.

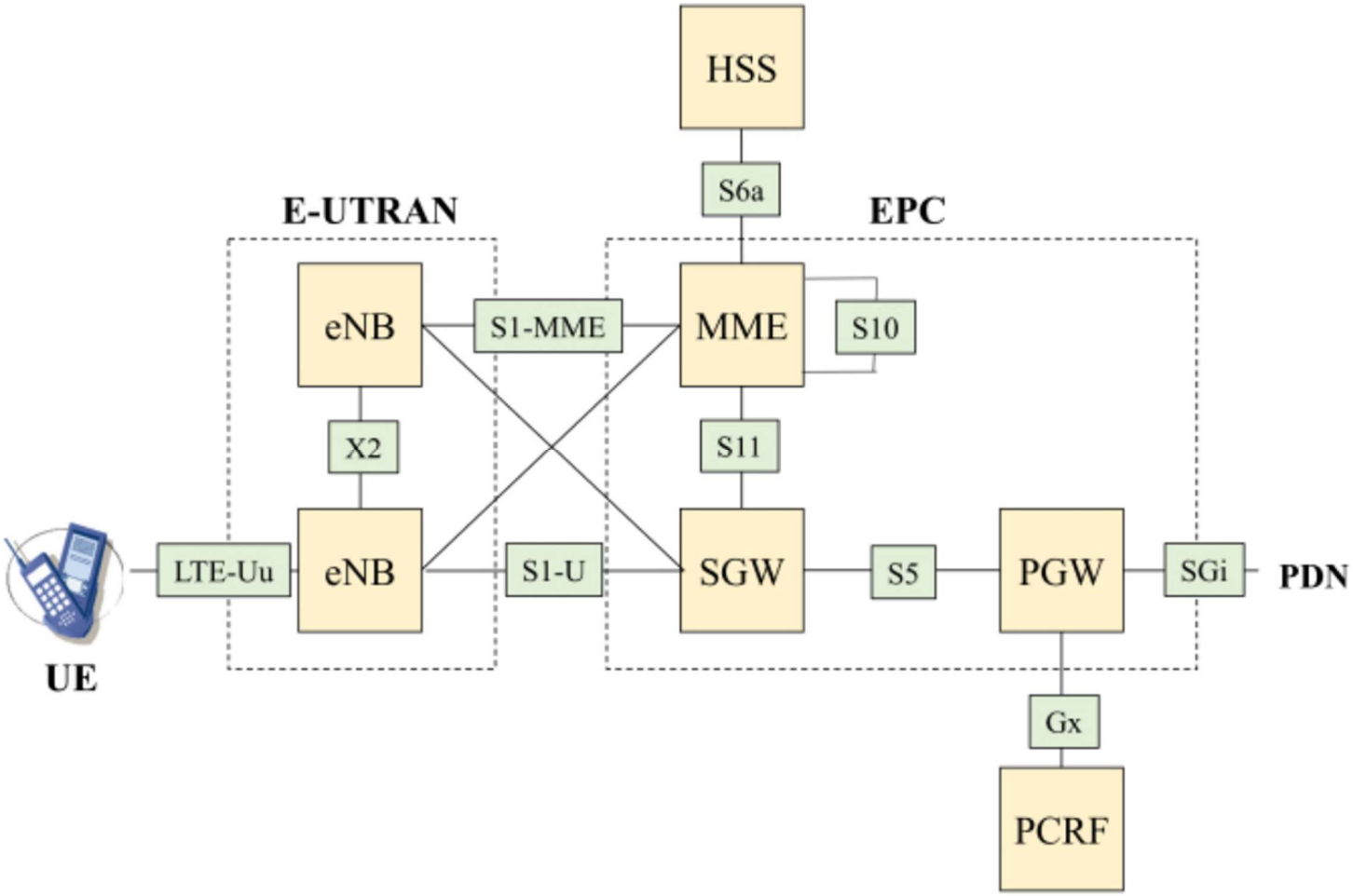
**Advantages of VoLTE:**

1. **Better Call Quality** – HD voice ensures clear audio with minimal distortion.
2. **Simultaneous Voice & Data –** Enables browsing while on a call.
3. **Faster Call Setup –** Quicker call connection times than 2G/3G.
4. **Lower Call Drop Rates –** More reliable than legacy voice networks.

**Challenges of VoLTE:**

1. **Requires LTE Coverage** – Not available in areas with only 2G/3G networks.
2. **Device Compatibility** – Only VoLTE-enabled smartphones can use this service.

## 49. Explain different components used in LTE architecture with diagram.




The high-level network architecture of LTE is comprised of following three main components :

1. The User Equipment (UE)
2. The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)
3. The Evolved Packet Core (EPC)

**1. User Equipment (UE):**

Mobile Devices (smartphones, tablets, laptops) that connect to the LTE network. Contains a SIM card for authentication and supports radio communication with the eNodeB.

**2. Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)**

Responsible for radio communication between UE and the core network. Consists of eNodeB (Evolved Node B), which replaces traditional base stations.

**eNodeB (eNB)**

- Manages radio resource control, scheduling, and handovers.
- Directly connects to the EPC via the S1 interface.

**3. EPC (Evolved Packet Core)**

The EPC is responsible for core network functions like mobility management, authentication, and data routing. It includes:

i. **MME (Mobility Management Entity)**:

- Handles UE authentication, session management, and mobility.

- Communicates with HSS (Home Subscriber Server) via the S6a interface to retrieve user profiles.
- Uses the S10 interface for MME-to-MME communication during handovers.

ii. **SGW (Serving Gateway)**:

- Routes user data between eNB and PGW.
- Supports mobility by maintaining data sessions when UE moves between eNBs.

iii. **PGW (Packet Data Network Gateway)**:

- Connects the LTE network to external packet data networks (PDN, e.g., the Internet).
- Manages IP address allocation and QoS (Quality of Service).
- Communicates with the PCRF (Policy and Charging Rules Function) via the Gx interface for policy enforcement.

iv. **HSS (Home Subscriber Server)**:

- Centralized database containing subscriber information, authentication credentials, and service profiles.

v. **PCRF (Policy and Charging Rules Function)**:

- Controls QoS, bandwidth allocation, and data charging policies.
- Ensures efficient network resource management.

**Interface Labels in Diagram**

- **LTE-Uu**: Radio interface between UE and eNB.
- **S1-MME / S1-U**: Connects eNB to MME and SGW.
- **X2**: Connects eNBs for inter-cell handovers.
- **S6a**: Links MME with HSS for authentication.
- **S5**: Connects SGW to PGW for data forwarding.
- **SGi**: Connects PGW to external networks (Internet, IMS, etc.).
- **Gx**: Connects PCRF to PGW for policy control.

~ *AJ*