MCC - Toppers Solutions

Mobile Communication & Computing (University of Mumbai)

---- Mobile Communication & Computing (MCC) ----

---- Marks Distribution ----

#	Chapter Name	MAY-15	DEC-15	MAY-16	DEC-16	MAY-17	DEC-17
1.	Intro. To Mobile.	15	10	19	29	20	15
2.	GSM cell.	30	15	14	18	25	15
3.	Mobile Network.	20	25	10	10	20	15
4.	3G & 4G Generation.	20	20	14	14	35	25
5.	Mobility Mgnt.	-	10	05	05	-	-
6.	WLAN Networks	35	30	34	30	25	35
7.	Intro. to Android	10	05	05	05	10	05
8.	Security Issues.	-	10	19	09	10	10
-	**Repeated Questions**	-	**30**	**30**	**60**	**95**	**40**

--- Analysis by Topper's Solutions Team ---

Last Minute Preparation:

Engineering is a notoriously demanding field of study. Being successful in engineering exams requires a **systematic and focused approach.** In order to do well, you will need to learn how to prepare for semester exam in engineering. Have you have already given up thinking, **"What the hell I can do at this moment? Tomorrow is exam!"** Think again! You are engineering student & last night studies are every engineering student's epitome.

"We engineers are known for our creativity"

Don't Worry entire **Topper's Solutions Team** is working out for betterment of students. Here are some techniques about **Mobile Computing & Communication (MCC)** Subject.

➢ **How to score first 40 – 50 marks:**

Study **any one** of the below set and make sure you can easily attempt any questions from below chapters included in particular set.

SET - 1

#	Chapter Name	Weightage (Marks)
1	Introduction to Mobile Computing	18
2	GSM cellular telephony arch. & System Aspects	20
4	Third and Fourth Generation Systems (V. IMP)	21
6	Wireless Local Area Networks (V. IMP)	32

OR

SET - 2

#	Chapter Name	Weightage (Marks)
2	GSM cellular telephony arch. & System Aspects	20
3	Mobile Network	17
4	Third and Fourth Generation Systems (V. IMP)	22
6	Wireless Local Area Networks (V. IMP)	32

➢ **How to score next 20 marks:**

Study the following 3 chapters.

#	Chapter Name	Weightage (Marks)
5	Mobility Management	7
7	Introduction to Android	7
8	Security Issues In Mobile Computing	12

Note: If you want to score good marks, study **ALL Chapters.**

Please Note: The Above Analysis is suggest by Topper's Solutions Team. Don't be completely dependent on it. It may change as per University of Mumbai Guidelines.

Contact No: 7507531198

Email ID: Support@ToppersSolutions.com

Website: www.ToppersSolutions.com

CHAPTER - 1: INTRODUCTION TO MOBILE COMPUTING

Q1] Draw and Explain Electromagnetic Spectrum for communication.

Ans: [5M – May15 & Dec15]

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.
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.

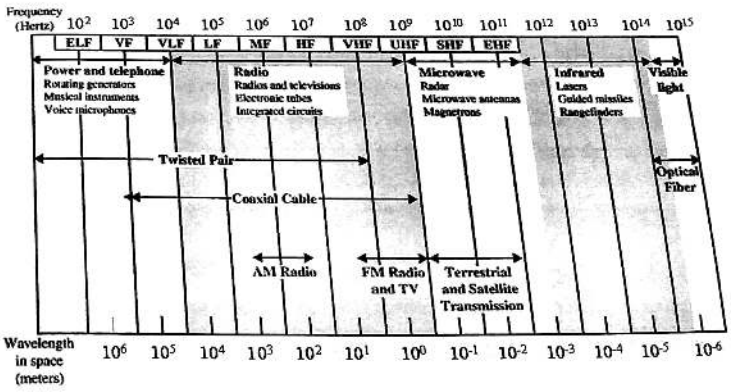


Figure 1.1: Electromagnetic Spectrum for communication.

I) **Very low frequency:**
- From 3 KHz onwards.
- They are long waves, having large wavelength.

II) **Low frequency (LF):**
- 30 KHz to 300 KHz.
- Used by submarines due to their water-penetrating ability and can also follow earth's surface.

III) **Medium frequency (MF):**
- 300 KHz to 3 MHz.
- Used for radio broadcast using AM/SW/FM modulation techniques and also used for aircraft navigation.

IV) **High frequency (HF):**
- 3 MHz to 30 MHz.
- Used for radio broadcast using AM/SW/FM modulation techniques.
- Also used for aircraft navigation.

V) **Very High Frequency (VHF):**
- 30 MHz to 300 MHz.
- TV broadcast range begins here and it is used for TV broadcast and Land mobile.

VI) **Ultra-High Frequency (UHF):**
- 300MHz to 3 GHz.
- WLANs, Analog-based mobile phones, cordless telephones, 3G cellular systems etc.

VII) **Super High Frequency (SHF):**
- 3 GHz to 30 GHz.
- Used for Directed microwave links, radar, satellite.

VIII) **Extremely High Frequency (EHF):**
- 30 GHZ to 300 GHz.
- Very close to the infrared region; also used for satellite, radar.

IX) **Infra-red:**
- 3 THz to 30 THz.
- Used for directed links, example to connect different buildings via laser links.

Q2] Satellite Orbits.

Q3] Satellites (GEO and LEO)

Ans: **[Q2 | 5M – Dec16] & [Q3 | 10M – May17]**

SATELLITE ORBITS:

1. An **orbit** is a regular, repeating path that one object in space takes around another one.
2. An object in an orbit is called a **Satellite.**
3. There are four different types of satellite orbits can be identified depending on the shape and diameter of the orbit.
4. Figure 1.2 shows the different types of satellite orbits around earth.

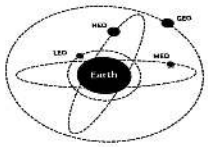


Figure 1.2: Satellite Orbits.

GEO:
- GEO Stands for **Geostationary Earth Orbit.**
- It has a distance of almost **36,000 km** to the earth surface.
- These satellites have a period of 24 hrs.
- This satellite is **synchronous** to earth rotation.
- It has fix antenna positions, no adjusting necessary.
- It is used for radio and **TV broadcasting.**

Advantages:
- It has wide coverage, three GEO satellites are enough for a complete coverage of almost any spot on earth.
- It does not require handover due to large footprint size.
- It has longer life span.
- GEOs usually does not exhibit any Doppler shift.

Disadvantages:
- There is big problem for **voice and data communication.**
- Launching a GEO satellite in to orbit is very expensive.
- It as high latency and high path loss.
- Due to large footprints, either frequencies cannot be reused.

Example: TV and Radio Broadcast Satellites.

MEO:

- MEO Stands for **Medium Earth Orbit**.
- It is also known as **Intermediate Circular Orbit (ICO)**.
- It has a distance of about **5000 - 12000 km** from earth.
- It has a period of about 6 hrs.
- Fewer satellites needed.
- It is used in **Land & Sea navigation**.

Advantages:

- 12 satellites are enough for global coverage.
- It is simple to design.

Disadvantages:

- Higher transmission power required.
- Special antennas required for focusing on a smaller footprint.

Example: GPS and ICO.

LEO:

- LEO Stands for **Low Earth Orbit**.
- It has a distance of about **500 - 1200 km** from earth.
- LEO satellites have a much shorter period of about **95 – 120 minutes**.
- Global radio coverage possible.
- More complex systems due to moving satellites.

Advantages:

- Transmission rates of about 2.4 Mbps can be achieved.
- It has smaller footprint size.
- It has **low deployment cost**.
- Smaller footprint allows **better frequency reuse**.
- It has **small path loss**.

Disadvantages:

- Large numbers of satellites are needed for global coverage.
- It has a **very short lifetime** of about five to eight years.
- Since more number of satellites used, LEOs need mechanism for routing of data packets from satellite to satellite.

Example: Iridium (start 1998, 66 satellites) & Global star (start 1999, 48 satellites)

HEO:

- HEO Stands for **Highly Elliptical Orbit**.
- This class comprises all satellites with non-circular orbits.
- It has a visibility of about **12 hours**.
- Satellite Lifeline is **20-25 years**.
- 2 – 3 Satellite are required.

Advantages:

- Lower launch cost.
- These systems have their perigee on large cities to improve communication quality.

Disadvantages:

- Inefficient for global coverage.
- Doppler effects are notable in this satellite.

Example: Soviet communication satellite uses such orbit.

Q4] Satellite Communication

Q5] Define footprint w.r.t satellite systems. Draw and explain how communication within the footprint happens?

Ans: **[Q4 | 5M - Dec15] & [Q5 | 5M - Dec17]**

SATELLITE COMMUNICATION:

1. **Satellite Communication** is use of artificial satellites to provide communication links between various points on Earth.
2. Satellite communications play a vital role in the **global telecommunications system**.
3. In satellite communication, **signal transferring** between the sender and receiver is done with the help of satellite.
4. In this process, the signal which is basically a beam of modulated microwaves is sent towards the satellite.
5. Then the satellite amplifies the signal and sent it back to the receiver's antenna present on the earth's surface.
6. So, all the signal transferring is happening in space.
7. Thus this type of communication is known as **Space Communication**.
8. As shown in figure 1.3, Depending on the type of satellite orbit (LEO, MEO or GEO) each satellite can cover a certain area on the earth with its beam.
9. It is called as **FootPrint**.
10. Within FootPrint, mobile users communicate with the satellite via **Mobile User Link**.

11. The base station can communicate with the satellite using **Gateway Link**.
12. Satellite communicate with each other via ISL – **Inter Satellite Link**.
13. This link provides direct communication between users with the different footprints without using base station or other networks on the earth.
14. The major challenge here is the smooth, seamless handover between a cellular network such as GSM, UMTS and a satellite system.
15. Figure 1.3 shows a typical satellite system for global mobile telecommunication.

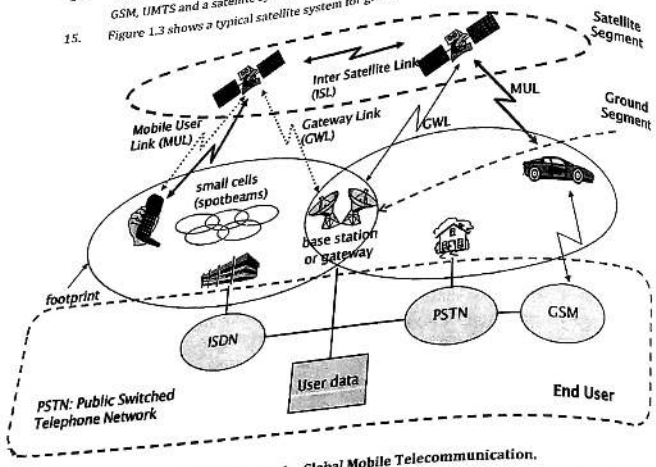


Figure 1.3: Satellite System for Global Mobile Telecommunication.

Q6] What are the general problems of satellite signals travelling from a satellite to a receiver?

[4M – May 16 & Dec16]

Ans:

1. In any satellite transmission, when the signal travels from the sender to the receiver, it experience various **types of losses from various sources.**
2. Some of the losses may due to **Attenuation** caused by the atmosphere, dust, rain, fog, snow.
3. It may be due to blocking of signals due to obstacles (buildings, mountains).
4. Different types of losses that the signal in satellite communication faces are as shown in Figure 1.4

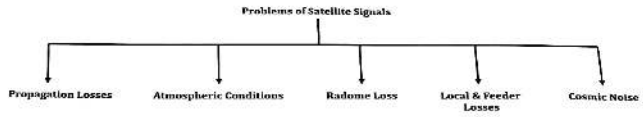


Figure 1.4: Different types of losses that the signal in satellite communication.

I) Propagation Losses:

- Propagation Loss results in the **loss of the strength** of the signal.
- It doesn't refer to attenuation of signal, but to its spreading through space.
- It includes:
  - **Blocking / Shadowing:** The signals with higher frequency behave like a straight line. These signals are blocked by even small obstacles like a wall, a car or a truck on a road. This phenomenon is called **blocking or shadowing**.
  - **Reflection:** When a signal encounters a surface that is large relative to the wavelength of the signal, a phenomenon is called reflection.
  - **Refraction:** This effect occurs because the velocity of the electromagnetic waves depends on the density of the medium through which it travels.
  - **Scattering:** If the object size is in the order of the wavelength of the signal or less, then the signal can be scattered into many small signals.
  - **Diffraction:** Diffraction occurs at the edge of an impenetrable body that is large as compared to the wavelength of a radio wave.

II) Atmospheric Condition:

- Atmospheric conditions such as **dust, rain, fog and snow** can result in loss of signal travelling from a satellite to a receiver.
- This kind of losses derives from the absorption of energy by atmospheric gases.

III) Radome Loss:

- Radome is a protective cover used with some antennas for shielding against weather effects.
- The Radome, being in the path of the signal, will scatter and absorb some of the signal energy.
- Thus it resulting in a **signal loss**.

IV) Local & Feeder Losses:

- Local Losses refer to loss of signal quality in each ground station.
- Local Losses is also called as **Equipment Losses.**
- Feeder Losses occur in the several components between the receiving antenna and the receiver device, such as filters, couplers and wavelengths.

V) **Cosmic Noise:**

- When the directional antenna is pointed towards the sky to receive the signal, other than the desired signal it also receives random noise from the galaxy
- The intensity of this noise varies very widely.
- This is referred as **cosmic noise**.

Q7] What are the different types of Handover in Satellite Systems? Explain in Detail. [10M – Dec16]

Ans:

HANDOVER IN SATELLITE SYSTEMS:

1. A handover in satellite system is a process in which a connected cellular call or a data session is transferred from one cell site to another without disconnecting the session.
2. Handover is important in satellite systems using MEOs and LEOs.
3. In Satellite System, each satellite **acts as a base station** for a mobile phone.
4. Since MEOs and LEOs satellites move very fast, the handover in such satellites are complex.

TYPES:

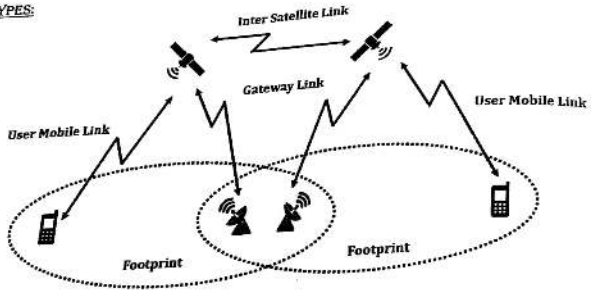


Figure 1.5: Types of Handover in Satellite Systems.

I) **Intra-Satellite Handover:**

- Handover between one spot beam to another spot beam of same satellite is called as Intra **Satellite Handover.**
- In this type of handover, the mobile station stills remains in the footprint of the satellite, but moves in another spot beam.
- Using special antennas, satellites can create several spot beams within the foot print.

II) **Inter-Satellite Handover:**

- Handover from one satellite to another satellite is called as **Inter Satellite Handover.**
- If a mobile station leaves the footprint of a satellite or the satellite moves away, a handover to the next satellite takes place.
- It can be Hard Handover or Soft Handover.
- It can also take place between satellites if they support Inter Satellite Link.

III) **Gateway Handover:**

- When satellite moves away from current gateway it is known as **Gateway Handover.**
- In this type of Handover, Mobile station still remains in the footprint of a satellite, but gateway leaves the footprint.

IV) **Inter System Handover:**

- The Handover from the satellite network to a terrestrial cellular network is called as **Inter System Handover.**
- Satellite systems are used in remote areas, if no other network is available.
- As soon as the traditional cellular network are available, user might switch to this type of network.
- Since terrestrial network is cheaper and has a lower latency etc.

Q8] Role of SUMR register in satellite roaming.

Ans: **[5M – May 16]**

SUMR REGISTER:

1. SUMR Stands for **Satellite User Mapping Register.**
2. It is the special Database that stores the **current position** of the satellites and a **mapping** of each user to the current satellite.
3. SUMR is used for **Localization.**
4. Localization in communication system is the process of finding the location of the specified user.
5. In SUMR, a satellite is assigned to a mobile station.

ROLES:

I) **Registration of a Mobile Station:**

- The mobile station initially sends a signal. This signal is received by one or more satellites.
- Satellite receiving such a signal reports this event to gateway.
- Therefore the gateway is now able to determine the location of user via the location of satellite.
- User Data is requested from the User's HLR, VLR & SUMR is updated.

II) **Calling a Mobile Station:**

- Calling a mobile is similar to GSM.
- Using HLR & VLR, call is forwarded to gateway.
- With the help of SUMR, the appropriate satellite for communication can be found and the connection can be set up.

Q9] Explain GPRS architecture in detail. Compare it with GSM architecture. [10M – May19]

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.
4. It has high data speed rate of 14.4 – 115 kbps.

GPRS ARCHITECTURE:

Figure 1.6 shows simplified GPRS Network Architecture.

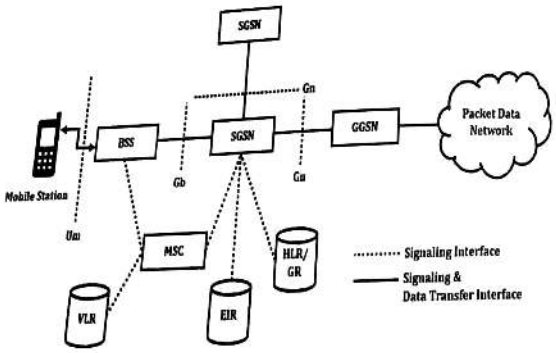


Figure 1.6: GPRS Network Architecture.

GPRS architecture includes:

I) **SGSN:**

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

II) **GGSN:**

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

III) **Mobile Station (MS):**

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

IV) **BSS:**

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

V) **HLR:**

- HLR Stands for **Home Location Register.**
- 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):**

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

GSM ARCHITECTURE VS GPRS ARCHITECTURE:

Table 1.1 shows the comparison between GSM & GPRS Architecture.

Table 1.1: GSM Architecture Vs GPRS Architecture.

	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.

Q10] What are the modifications required to an existing GSM network to be upgraded to GPRS, Explain with the help of diagram. **[10M – May16 & Dec**

Ans:

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 system.
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:

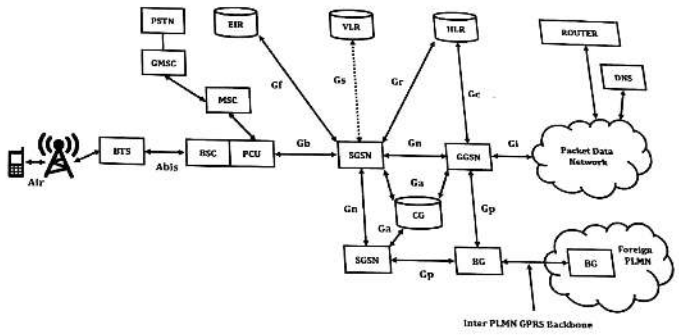


Figure 1.7: GSM Network to be upgraded to GPRS Architecture.

1. As shown in Figure 1.7, 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.
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 1.7.
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.

Q11] Explain the data rate enhancement with the help of GPRS network model. What is the maximum data rate obtained by GPRS network? [10M – Dec17]

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.
5. Refer figure 1.6.

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

Q12] What is an antenna? Explain different types of antennae [5M – May17]

Ans:

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:

- Isotropic Antenna is said to be the type of antenna which radiates equally in all directions.
- This type of antenna is considered to be ideal antenna.
- It has a perfect **360 degree** spherical radiation pattern.
- There is no actual physical isotropic antenna.
- However, an isotropic antenna is often used as a reference antenna for the antenna gain.
- The antenna gain is often specified in dBi, or decibels over isotropic.
- 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.
- Figure 1.8 represents radiation pattern of isotropic antenna.

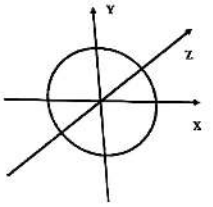


Figure 1.8: Radiation Pattern of Isotropic Antenna.

II) Dipole Antenna:

- Dipole antenna is also known as **doublet.**
- It is the simplest and most widely used class of antenna.

Q11] Explain the data rate enhancement with the help of GPRS network model. What is the maximum data rate obtained by GPRS network? [10M – Dec17]

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.
5. Refer figure 1.6.

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

Q12] What is an antenna? Explain different types of antennae [5M – May17]

Ans:

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:

- Isotropic Antenna is said to be the type of antenna which radiates equally in all directions.
- This type of antenna is considered to be ideal antenna.
- It has a perfect **360 degree** spherical radiation pattern.
- There is no actual physical isotropic antenna.
- However, an isotropic antenna is often used as a reference antenna for the antenna gain.
- The antenna gain is often specified in dBi, or decibels over isotropic.
- 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.
- Figure 1.8 represents radiation pattern of isotropic antenna.

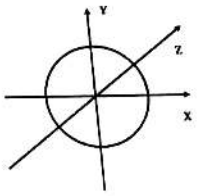


Figure 1.8: Radiation Pattern of Isotropic Antenna.

II) Dipole Antenna:

- Dipole antenna is also known as **doublet.**
- It is the simplest and most widely used class of antenna.

- The dipole is the prototypical antenna on which a large class of antennas are based.
- 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.
- The length of the dipole is half of the wavelength of the signal.
- **Hertzian dipole** is most commonly used dipole antenna.
- Figure 1.9 represents Radiation pattern of Hertzian dipole.

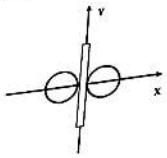


Figure 1.9: Radiation pattern of Hertzian Dipole (side view).

III) **Monopole Antenna:**

- A monopole antenna is a class of radio antenna consisting of a straight rod-shaped conductor.
- It is often mounted perpendicularly over some type of conductive surface, called a **ground plane**.
- It is also known as **Markoni Antenna**.
- The length of the monopole is one fourth of the wavelength of the signal.
- Figure 1.10 represents ideal vertical monopole antenna.

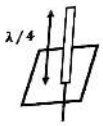


Figure 1.10: Ideal Vertical Monopole Antenna.

IV) **Antenna Arrays:**

- Array antennas consist of multiple antennas working as a single antenna.
- Typically they consist of arrays of identical driven elements, usually dipoles fed in phase, giving increased gain over that of a single dipole.
- Different diversity schemes are possible.
- One such scheme is selection diversity, where the receiver always uses the antenna element with the largest output.

- The other type of diversity is diversity combining, in which a combination of power of all the signals is taken to produce gain.
- Figure 1.11 represents antenna arrays.

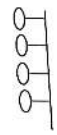


Figure 1.11: Antenna Arrays.

V) **Loop Antenna:**

- Loop antennas consist of a loop (or coil) of wire.
- There are essentially two broad categories of loop antennas: big loops and small loop.
- Loops with circumference of a wavelength are naturally resonant and act somewhat similarly to the half-wave dipole.
- Figure 1.12 represents Loop Antennas.

Figure 1.12: Loop Antenna.

VI) **Aperture antennas:**

- Aperture antennas are the main type of directional antennas used at microwave frequencies and above.
- 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.
- Since the antenna structure itself is non-resonant they can be used over a wide frequency range by replacing or tuning the feed antenna.
- Figure 1.13 represents aperture antenna.

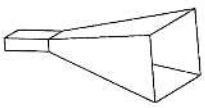


Figure 1.13: Aperture Antenna.

Q13] What is frequency reuse concept in cellular communication? [5M – May17]

Ans:

FREQUENCY REUSE IN CELLULAR COMMUNICATION:

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 1.14 shows two of them.

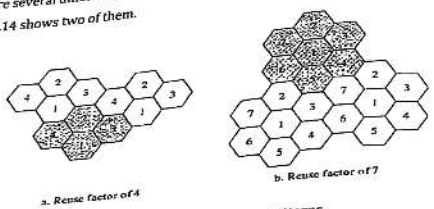


Figure 1.14: Frequency reuse patterns.

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 1.14 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:

- 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.
- This distance is called the **frequency 'reuse' distance.**
- It can be shown that the reuse distance 'ru', normalized to the size of each hexagon, is

$$r_u = \text{SQRT}\{3\,C\}$$

- For hexagonal cells, i.e., with 'honeycomb' cell layouts commonly used in mobile radio, possible cluster sizes are $C = i^2 + ij + j^2$.
- Integers i and j determine the relative location of co-channel cells.
- The cells which have been allotted same group of channels are called **co-channels.**
- Figure 1.15 shows 7 cell frequency reuse with i = 2 and j = 1.

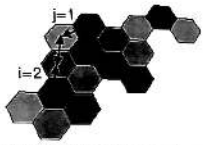


Figure 1.15: 7 Cell Frequency Reuse.

---- EXTRA QUESTIONS ----

Q1] Spread Spectrum?

Ans:

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.

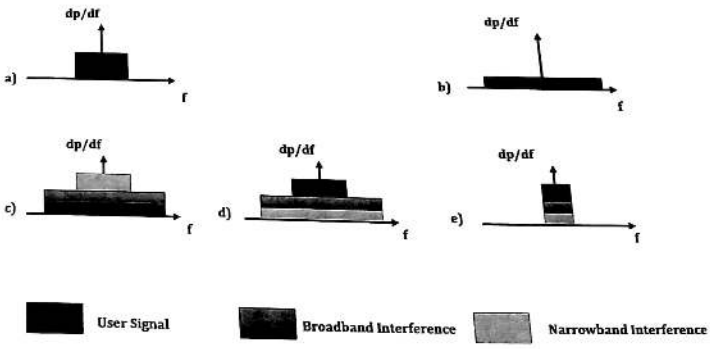


Figure 1.16: Spread Spectrum: Spreading & Despreading.

STEPS:

- The process of Spreading & Despreading is shown in Figure 1.16.
- An idealized narrow band signal is transmitted by the sender as shown in Figure 1.16 (a).
- The narrow band signal is converted into broadband signal i.e. signal is spread as shown in fig. 1.16 (b).
- The energy need to transmit the signal is still the same.
- During transmission, narrow band as well as broadband interference gets added to the spread signal as shown in Figure 1.16 (c).
- The receiver now has to de spread the received signal.
- The original broadband signal (containing user data) is converted back to a narrowband signal.
- The narrowband interference that was added is spread whereas the broadband interference is left as it is.
- 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 1.16 (e).
- The original user signal can now be recovered.

Advantages:

- It provides the resistance to narrowband interference.
- It is used in military application.

Disadvantages:

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

Q2] Comparison of GEO, LEO and MEO

Ans:

Table 1.3 shows the comparison of GEO, LEO & MEO.

Table 1.3: Comparison of GEO, LEO & MEO.

Parameter	GEO	MEO	LEO
Full Form	Geostationary Earth Orbit.	Medium Earth Orbit.	Low Earth Orbit.
No. of Satellite Required	3 – 4	12 – 14	50 – 200
Orbital Period	24 Hrs.	Approx. 2 -8 Hrs.	90 – 120 Mins.
Distance from Earth	35800 km.	5000 – 12000 km.	500 – 1500 km.
Life Time	Longer life Approx. 15 yrs.	Moderate life time Approx. 9 – 12 yrs.	Shorter life Approx. 5 – 8 yrs.
Deployment Cost	High.	Less compared to GEO.	Low.
Transmit Power Required	High 10W.	Moderate.	Low 1W.
Path Loss	High path loss.	Significant path loss due to more travelling distance.	Smaller path loss.
Propagation Delay	High 0.25 sec.	Moderate 70 – 80 msec.	Low 10 msec.
Handover Needed	Due to larger footprint no handover needed.	Fewer handover required as compared to LEO.	Due to smaller footprints frequent handover required.

CHAPTER – 2: GSM CELLULAR TELEPHONY ARCHITECTURE AND SYSTEM ASPECTS

Q:] Explain GSM in detail? [10M – Mar

Ans:

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 1 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:

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

GSM ARCHITECTURE:

GSM has complex hierarchical architecture consisting of many entities, interfaces and acronyms but main subsystems a shown in figure 2.1.

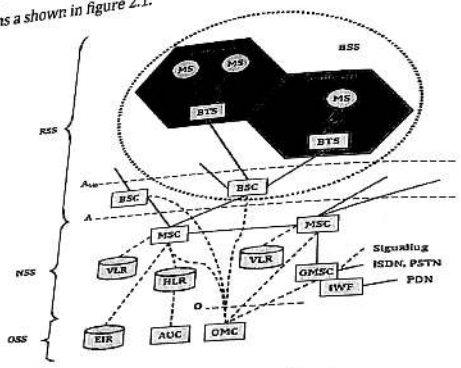


Figure 2.1: GSM System Architecture.

I) 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:

Base Station Subsystem (BSS):

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

Base Transceiver Station (BTS):

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

Base Station Controller (BSC):

- It is used to manage the BTSs.
- The main function is to multiplex radio channels onto fixed network connections at the interface.
- **Functions:**
  - Control of frequency hopping.
  - Power management.

Mobile Station (MS):

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

II) 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 network system control, charging and accounting.

3. It consists of following components:

Mobile Service Switching Center (MSC):

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

Gateway MSC (GMSC):

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

4. NSS maintains the following Databases:

Home Location Register (HLR):

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

Visitor Location Register (VLR):

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

III) Operational Subsystem (OSS):

1. It enables centralized operation, management and maintenance of all GSM subsystems.
2. OSS accesses other entities via signaling.
3. It has following components:

Authentication Center (AuC):

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

Operation and Maintenance (OMC):

- It is responsible for various functions like:
  - Traffic monitoring.
  - Subscriber and security management.
  - Status report of network entities.
  - Accounting and billing.

Equipment Identity Register (EIR):

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

Q2] Explain GSM Frame Hierarchy.

Q3] Explain in short Time slot hierarchy of GSM System.

Ans: **[Q2 | 5M – May15] & [Q3 | 4M – Dec16]**

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 2.2 below, there are two variants to multiframe structure.

I) **26 Frame Multiframe:**
- It is called as **Traffic Multiframe**.
- It composed of 26 bursts in a duration of 120ms, out of these 24 are used for traffic, one for SMG and one is not used.

II) **51 Frame Multiframe:**
- It is called as **Control Multiframe**.
- It composed of 51 bursts in a duration of 235.4 ms.
- This type of multiframe is divided into logical channels.
- These logical channels are time scheduled by BTS.

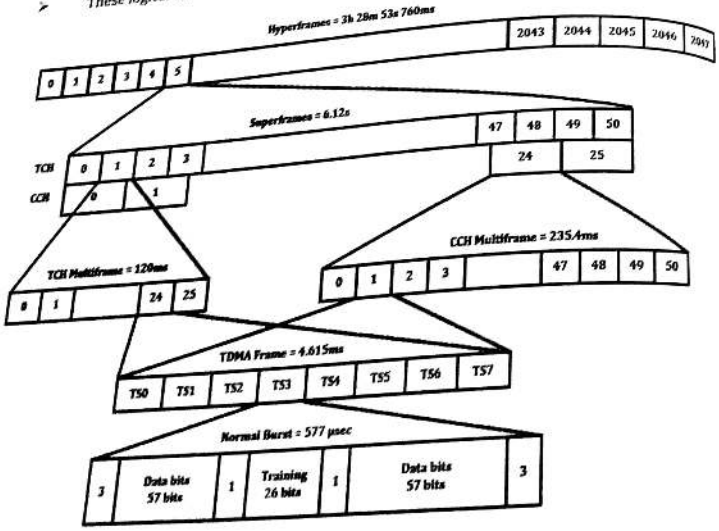


Figure 2.2: GSM Time (or Frame) Hierarchy.

Q4] Privacy and Authentication in GSM.

Q5] Explain in detail how Subscriber Authentication is done in GSM.

Ans: **[Q4 | 10M – May15] & [Q5 | 10M – Dec16]**

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:**
   - This includes the user authentication.
   - User must enter a secret PIN number to access SIM.
   - It is also responsible for subscriber authentication.

   II) **Confidentially:**
   - In this the entire user related data is **encrypted.**
   - This confidentially exists only between MS and BTS.

   III) **Anonymity:**
   - Anonymity is provided to the user by encrypting all the data before the transmission.
   - Along with the encryption the GSM uses Temporary Identifiers such as **TMSI and MSRN.**

5. GSM uses three algorithms to provide security services:
   - Algorithm A3 is used for **Authentication.**
   - Algorithm A5 is used for **Encryption.**
   - Algorithm A8 is used for **Generation of a cipher key.**

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.**

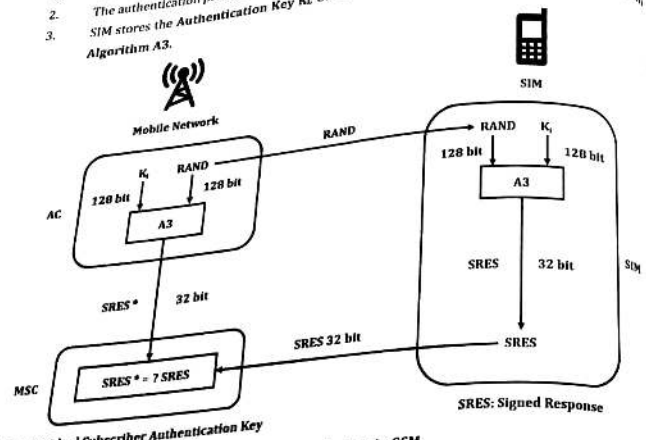


Figure 2.3: Authentication in GSM.

Authentication involves:

- Figure 2.3 shows the Authentication process in GSM.
- The Access Control (AC) generates a 128 bit Random Number (RAND) as a challenge.
- VLR sends RAND to the SIM.
- SIM now calculates a Signed Response (SRES) from RAND and Authentication key Ki by applying authentication algorithm A3.
- Similarly, the access control also calculates a Signed Response called SRES*
- MSC now compares the values SRES and SRES*.
- It the values are same the subscriber is accepted else rejected.

ENCRYPTION IN GSM:

1. Once authentication is done MS and BTS can start using Encryption.
2. Figure 2.4 shows the Encryption Process in GSM.

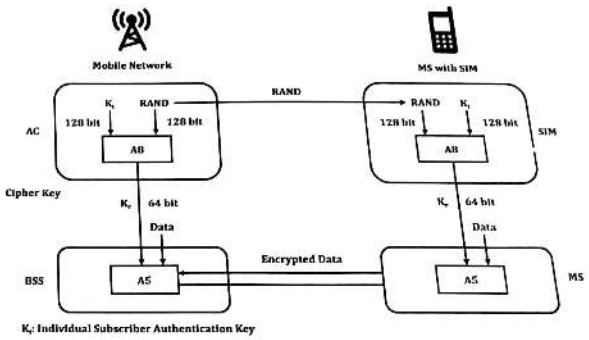


Figure 2.4: Encryption in GSM.

Encryption involves following steps:

- 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.
- MS and BTS can now Encrypt and Decrypt the data using this 64 bit cipher key (K_c) and the Encryption algorithm A5.
- The 64 bit K_c is just enough to provide to provide protection against simple eavesdropping and is not very strong.
- 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.
- This makes the **encryption much weaker.**

Q6] Explain various types of handoffs in GSM network.

Q7] what are the different types of Handover in GSM? Explain in Detail Intra-MSC handover.

Ans: **[Q6 | 5M – May15 & May17] & [Q7 | 10M – May16]**

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:

- This handover takes place **within a cell.**
- 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.
- Figure 2.5 shows the Intra-cell Handover.

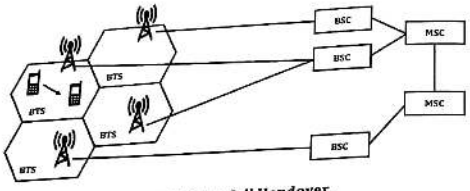
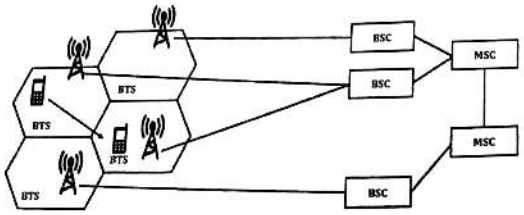


Figure 2.5: Intra Cell Handover.

II) Inter-cell Handover:

- It is also known as **Intra-BSC Handover.**
- This type of handover is performed when a mobile station moves from one cell to another bu remains within the same BSC (Base station controller).
- Here the BSC handles the handover process.
- Figure 2.6 shows the Inter-cell Handover.



III) Inter-BSC Handover:

- It is also called as **Intra-MSC Handover.**
- This handover takes place between two cells managed by different BSCs.
- As BSC can control only a limited number of cells, we might usually need to transfer a mobile from one BSC to another BSC.
- Here the MSC handles the handover process.
- Figure 2.7 shows the Inter-cell Handover.

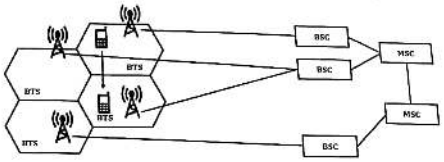


Figure 2.7: Inter BSC Handover.

IV) Inter-MSC Handover:

- It occurs when a mobile moves from one MSC region to another MSC.
- MSC cover a large area.
- It can be imagined as a handover from Gujarat MSC to Maharashtra MSC while travelling.
- Figure 2.8 shows the Inter-cell Handover.

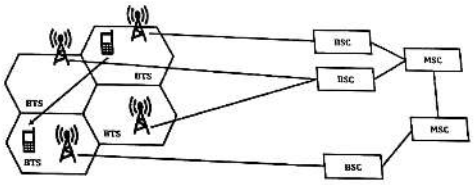


Figure 2.8: Inter MSC Handover.

*** Note: Inter-BSC, Intra-MSC handover in detail is asked For Q7.**

INTER-BSC, INTRA-MSC HANDOVER:

1. Figure 2.9 shows the typical signal flow during Inter-BSC, Intra-MSC Handover.
2. MS sends its **periodic measurement reports** to the BTS_{old}.
3. Then BTS_{old} forwards these reports to the BSC_{old} together with its own measurements.
4. Based on these values the BSC_{old} decides to perform a handover and sends the mes HO_required to the MSC.

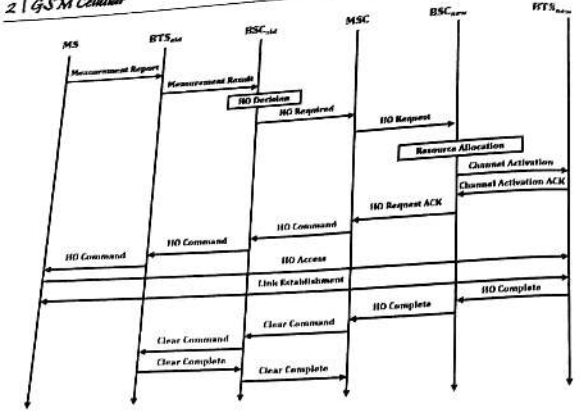


Figure 2.9: Inter BSC, Intra MSC Handover Process.

5. The MSC then requests the resources needed for the handover from the new BSC.
6. This BSC_{new} checks, if enough resources are available.
7. If the resources are available then it activates a physical channel at the BTS_{new} for the MS.
8. BTS_{new} sends acknowledgement of successful channel activation to BSC_{new} and BSC_{new} acknowledges the handover request.
9. The MSC then issues a handover command that is forwarded to the MS.
10. The MS now breaks the old connection and accesses the new BTS.
11. Now a new radio link is established between the MS and BTS_{new}.
12. All the reserved resources at the old BSC and BTS are released.

Q8] Explain how Mobile originated call (MOC) work.

[4M – May16 & Dec16]

Ans:

1. There are different methods and protocols are used for establishing connection and maintaining communication in calling to and from mobile devices in a GSM network.
2. The various types of calls handled by a GSM network are:
   a. Mobile Originated Call (MOC)
   b. Mobile Terminated Call (MTC)

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 2.10.

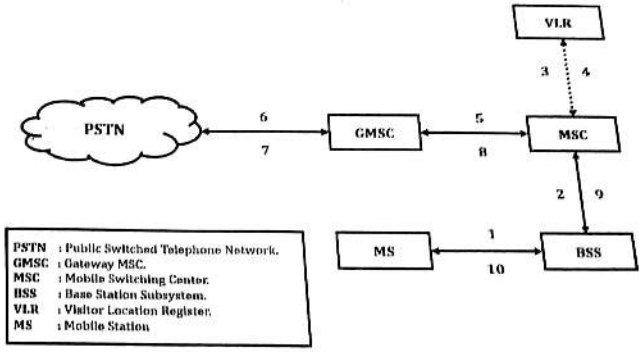


Figure 2.10: Mobile Originated Call (MOC)

Working:

- The MS sends the dialed number indicating service requested to the MSC (via BSS) as shown in step 1 & 2.
- Then MSC checks from the VLR if the MS is allowed for the requested service as shown in step 3 & 4.
- If so, MSC asks the BSS to allocate necessary resource for the call.
- If the call is allowed, the MSC routes the call to the **GMSC (Gateway MSC)** as shown in step 5.
- The GMSC routes the call to the local exchange of called user via **public switched telephone network** (PSTN) as shown in step 6.
- The PSTN alert (applies ringing) the called **terminal.**
- Answer back (ring back tone) from the called terminal to PSTN.
- 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 and 10.

Q9] Explain Mobile call termination in GSM, detailing the need and the use of MSRN, IMSI, TMSI no.s [10M – Dec15]

Ans:

1. There are different methods and protocols used for establishing connection and maintaining communication in calling to and from mobile devices in a GSM network.
2. The various types of calls handled by a GSM network are:
   a. Mobile Originated Call (MOC)
   b. Mobile Terminated Call (MTC)

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 information 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 os 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 2.11 represents the working of Mobile Terminated Call.

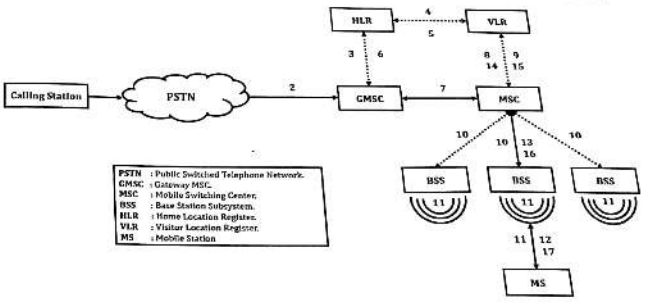


Figure 2.11: Mobile Terminated Call (MTC)

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:

2. IMSI stands for **International Mobile Subscriber Identity**.
3. GSM uses the IMSI for **Internal Unique Identification** of a subscriber.
4. IMSI consists of a Mobile Country Code, Mobile Network Code & Mobile Subscriber Identification Number.
5. 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).

Q10] Explain how Mobile Terminated Call works detailing the role of HLR and VLR.

[10M – May15 & May17]

Ans:

MOBILE TERMINATED CALL:

Refer Q9 for Mobile Terminated Call.

ROLE OF HLR IN MOBILE TERMINATED CALL SETUP:

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

ROLE OF VLR IN MOBILE TERMINATED CALL SETUP:

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

Q11] What is the relationship between the Base Station and Mobile Switching Centre? Discuss the role of EIR entity of GSM network.

[5M – Dec17]

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 2.12.

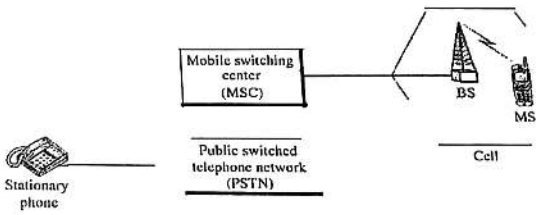


Figure 2.12: Cellular System.

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):

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

Q12] 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.

[10M – Dec 17]

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 2.13 represents hierarchy of control channels.

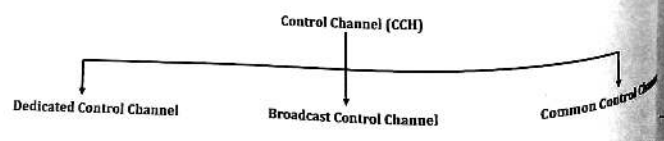


Figure 2.13: GSM Control Channels

I) **Broadcast Control Channel (BCCH):**

Broadcast control channels are transmitted in **downlink direction only** i.e. only transmitted by BTS.

The broadcast channels are used to broadcast synchronization and general network information to all the MSs within a cell.

Such as **Location Area Identity (LAI) and maximum output power.**

It has two types: Frequency Correction Channel, Synchronization Channel.

- **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.
- **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:**

Common Control Channel are communication channels that are used to coordinate the control of mobile devices operating within its cell radio coverage area.

GSM control channels include the random access channel (RACH), paging channel (PCH), and access grant channel (AGCH).

They are used by an MS during the **paging and access procedures.**

It is **unidirectional channel.**

- **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.
- **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.
- **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.

Q12] 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.

[10M – Dec17]

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 millio users can be active (registered).
6. If many users move between location areas updates have to take place, i.e., the HLR always ge 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 loa on the network as the HLR in the home network of the tourists always requires upda 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 channe which are dedicated to the sending and/or receiving of command messages between devic (such as a base station and a mobile radio).
2. On the GSM system, the control channel sends messages that include paging (alerting), acce control (channel assignment) and system broadcast information (access parameters and syste identification).
3. Many different control channels are used in GSM to control medium access, allocating of tra channels or mobility management.
4. Figure 2.13 represents hierarchy of control channels.

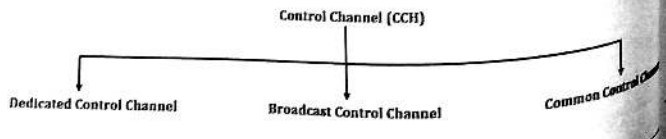


Figure 2.13: GSM Control Channels

I) **Broadcast Control Channel (BCCH):**

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

  - **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.
  - **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:**

Common Control Channel are communication channels that are used to coordinate the control of mobile devices operating within its cell radio coverage area.

GSM control channels include the random access channel (RACH), paging channel (PCH), and access grant channel (AGCH).

They are used by an MS during the **paging and access procedures.**

It is **unidirectional channel.**

- **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.
- **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.
- **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:**

- They are communication channels that transfer signaling messages to specific devices.
- It is a **bi-directional channel.**
- Signaling information is carried between an MS and a BTS using associated and dedicated control channels during or not during a call.
- It includes:
  - **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.**
  - **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.
  - **Fast Associated Control Channel (FACCH):**
    - FACCH is transmitted instead of a TCH.
    - The FACCH steal the TCH burst 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.

Q13] Explain the U_m interface of GSM [5M – Dec

Ans:

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 U_m 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 trans and receive traffic and signaling information between the GSM's BTS and the GSM Mobile Stat
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 t handled simultaneously by the same carrier.
7. The **international telecommunication union** (ITU) which manages the allocation of r spectrums has allocated the following bands for GSM U_m Interface:
   a. **Uplink:** 890-915 MHz (Mobile station to Base station)
   b. **Downlink:** 935-960 MHz (Base station to mobile station)
8. Figure 2.14 shows U_m Interface between MS and BSS.

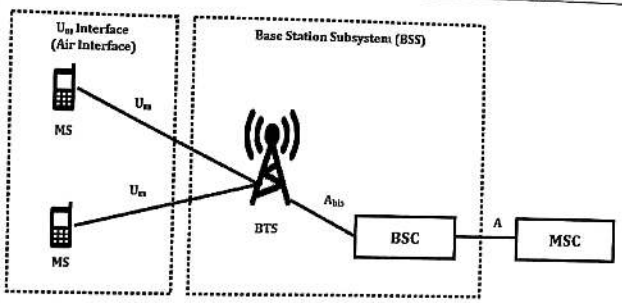


Figure 2.14: U_m Interface between MS and BSS.

---- EXTRA QUESTION ----

Q1] Explain different types of Interface in GSM?

Ans:

GSM INTERFACE:

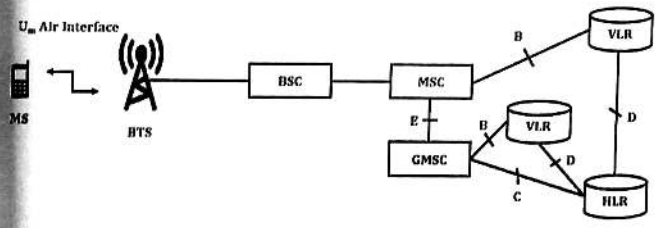


Figure 2.15: GSM Interfaces.

I) **U_m Interface:**

- **Refer Q13.**

II) **B Interface:**

- B Interface is also known as **Internal Interface.**
- B Interface Exist between the MSC and the VLR.
- It uses a protocol known as the **MAP/B Protocol.**
- 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:**

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

IV) **D Interface:**

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

V) **E Interface:**

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

CHAPTER - 3: MOBILE NETWORK

Q1] Why is Mobile IP packet required to be forwarded through a tunnel? Explain minimal techniques of encapsulation of Mobile IP packet.

Ans: **[10M – May15 & May17]**

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:

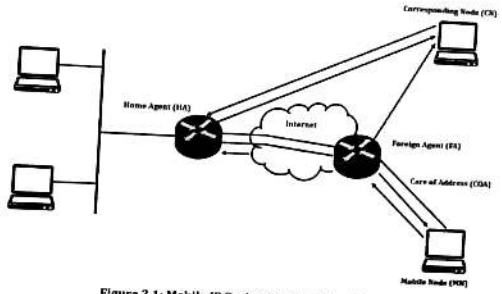


Figure 3.1: Mobile IP Packet Routing Using Tunnel.

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 3.2, 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 Mobile Node as it roams.
12. It established a pipe wherein the data is inserted and moves in FIFO order.

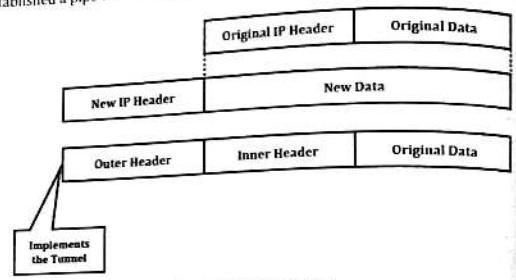


Figure 3.2: Encapsulation.

MINIMAL ENCAPSULATION:

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 3.3 shows the Minimal Encapsulation.

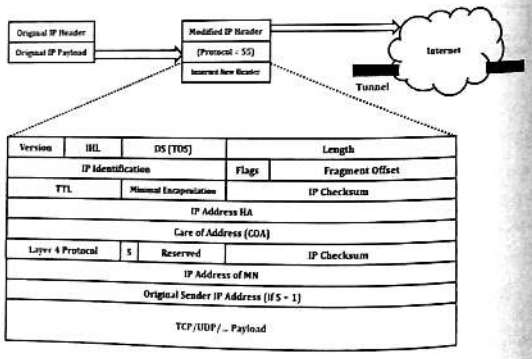


Figure 3.3: Minimal Encapsulation.

5. The outer header fields in Minimal Encapsulation are almost same as for IP encapsulation only difference is in the Type field.
6. It is set to 55.
7. The various field in the outer header are:

I) **Version:**
- Version field denotes the version number.
- It is set to 4 for IPv4.

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

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

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

V) **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.

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

VII) **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).

Q2] Why does the Mobile IP packet required to be forwarded through a tunnel. Explain Generic techniques of encapsulation of Mobile IP packet.

Ans: **[10M – Dec15]**

Refer Mobile IP & Need of Tunnel Section from Q1.

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 3.4 shows the Generic Routing Encapsulation.
5. The GRE header is prepended to the packet of one protocol suite with the original header and data.

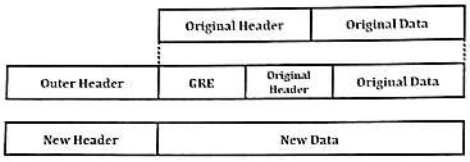


Figure 3.4: Generic Routing Encapsulation.

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

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

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

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

IV) **K bit:**
- If it is set, it indicates the key field is present and may be used for **authentication.**

V) **S bit:**
- If set, it indicates that the **sequence number** is present.

VI) **s bit:**
- If set, it indicates that the **strict source routing** is used.

VII) **Recursion Control:**
- It represents a counter that shows the number of allowed **recursive encapsulations.**

VIII) **Reserved:**
- This field is reserved for future use.

IX) **Version:**
- Version field denotes the version number.

X) **Protocol:**
- It indicates the protocol used by the packet.

XI) **Checksum:**
- It contains a valid IP checksum of the GRE header and the payload.

XII) **Offset:**
- It represents the offset in bytes for the first source entry.

XIII) **Key:**
- It contains a key that can be used for **authentication.**

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

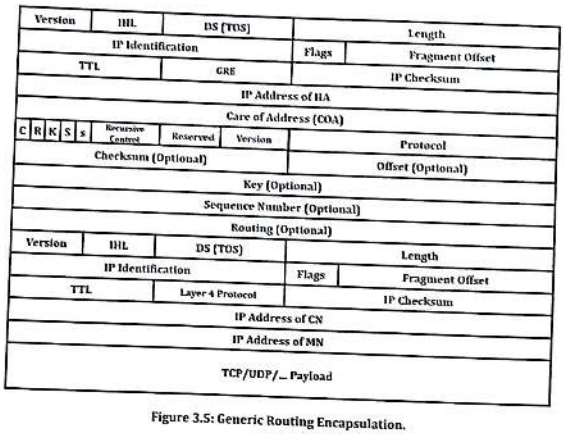


Figure 3.5: Generic Routing Encapsulation.

Advantages:
- It support more than one level of encapsulation.
- It support other network layer protocols in addition to IP.

Q3] Why is Mobile IP Packet required to be forwarded through a tunnel. Explain IP-in-IP Techniques of encapsulation of mobile IP Packet. **[10M – May16]**

Ans:

Refer Mobile IP & Need of Tunnel Section from Q1.

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.

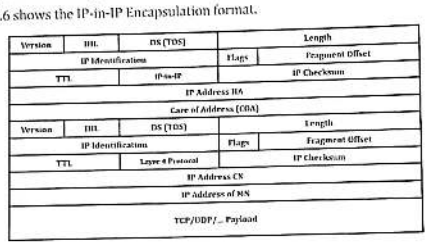


Figure 3.6: IP-in-IP Encapsulation.

5. The various field in the outer header are:

I) Version:

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

II) IHL (Internet Header Length):

- IHL indicates the length of the outer header.

III) DS (TOS):

- It is just copied from the inner header.

IV) Length:

- It denotes the complete length of the encapsulated packet.

V) 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.

VI) IP-in-IP:

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

VII) IP Checksum:

- This is used for error detection mechanism.

6. 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.

Q4] How the agent can be discovered using Mobile IP? Give the overlay of agent advertisement packet which includes mobility extension. Also, discuss how tunneling works for Mobile IP using IP-in-IP encapsulation.

Ans: **[10M – Dec17]**

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 3.7 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 choose the router.

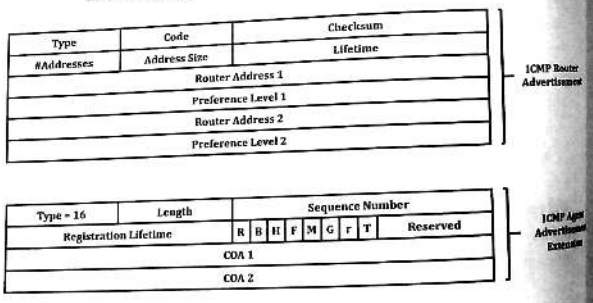


Figure 3.7: Agent Advertisement Message.

IP-IN-IP ENCAPSULATION

Refer Q3 (IP-in-IP Encapsulation Part).

Q5] Explain agent Advertisement in Mobile IP

Ans: **[5M – Dec15]**

AGENT ADVERTISEMENT IN MOBILE IP:

Refer Q4 (Agent Advertisement in Mobile IP Part).

Q6] Explain the functioning of Mobile- TCP.

Q7] M-TCP

Ans: **[Q6 |10M – Dec15] & [Q7 | 10M - Dec17]**

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.

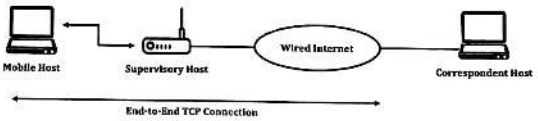


Figure 3.8: Mobile TCP.

WORKING:

1. Figure 3.8 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 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.

Advantages:

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

Disadvantages:

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

Q8] List the entities of mobile IP and describe data transfer from a mobile node to fixed node and vice versa.

[10M – Dec

Ans:

ENTITIES OF MOBILE IP:

I) Mobile Node (MN):

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

II) Correspondent Node (CN):

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

III) Home Network (HN):

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

IV) Foreign Network (FN):

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

V) Home Agent (HA):

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

VI) Foreign Agent (FA):

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

VII) Care-of-Address (COA):

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

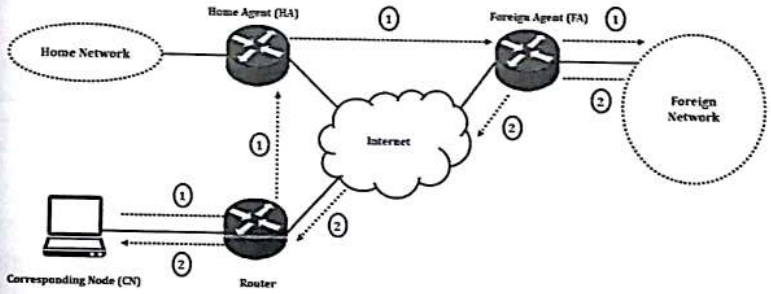


Figure 3.9: Data Transfer to and from the Mobile Node.

Figure 3.9 shows the 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 3.9.
2. As shown in figure 3.9, the packet is sent by the Mobile Node (MN) with its original address as the source 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 3.9.
2. Since the CN does not known the current location of Mobile Node (MN), so it sends the Packet to the 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 of 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 an is 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 destinati and HA as the source of the encapsulated packet.
10. Foreign Agent now decapsulates the packet and forwards the original packet with CN as sour and MN as destination.

Q9] Explain the functioning of I-TCP and SNOOP-TCP, giving advantages a disadvantages of both.

Ans: **[10M – May15 & May**

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.**

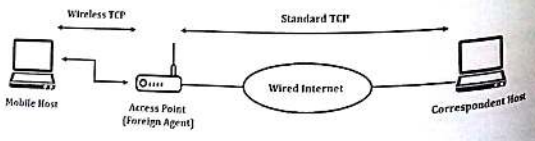


Figure 3.10: I-TCP.

5. The figure 3.10 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:

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

Disadvantages:

- The end-to-end connection for which TCP has been designed will fail if the Foreign Agent (FA) crashes.
- 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.
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 3.11 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.

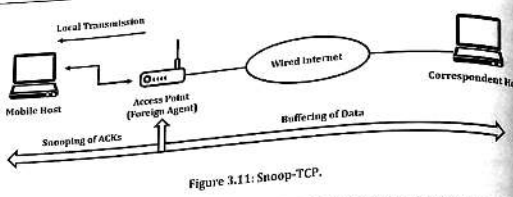


Figure 3.11: Snoop-TCP.

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 fast retransmission compared to correspondent host.
12. To maintain transparency, the FA doesn't send acknowledgement to the correspondent host as 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 acknowledgement number.
16. If a gap is found, FA sends signal to re-transmit.

Advantages:

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

Disadvantages:

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

CHAPTER - 4: THIRD & FOURTH GENERATION SYSTEMS

Q1] Explain UMTS architecture. Explain UTRA-FDD and TDD modes

Q2] UMTS

Q3] Explain UTRA-FDD and TDD modes

Ans: [Q1 | 10M – May15 & Dec15], [Q2 | 10M – May17] & [Q3 | 10M – May17]

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:

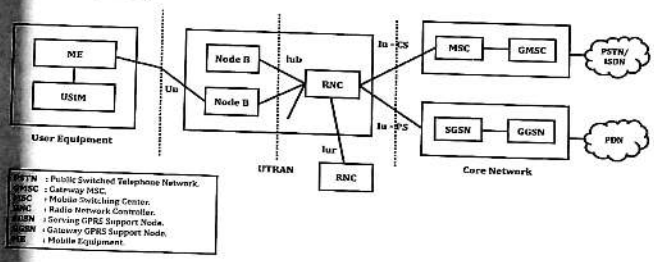


Figure 4.1: UMTS Architecture.

1. Figure 4.1 shows UMTS Architecture.
2. It has following components:

User Equipment (UE):

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

Universal Terrestrial Radio Access Network (UTRAN):

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

Core Network (CN):

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

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:

- Figure 4.2 shows UTRA-FDD Frame Structure.
- A radio frame contains 15 time slots.
- The duration of each frame is 10 msec.
- A radio frame consists of 38400 chips.
- Each time slot is of 666.6 µs and consists of 2560 chips.
- Each WCDMA channel occupies 4.4 to 5 MHz bandwidth.
- Time slots in WCDMA are not used for user separation but to support periodic functions.
- In contrast to GSM where time slots are used to separate users.

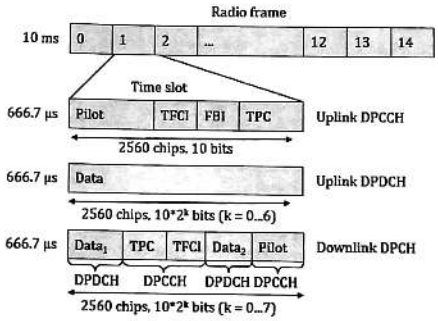


Figure 4.2: UTRA-FDD Frame Structure.

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 4.3 shows UTRA-TDD Frame Structure.
- If the users have different data rates, the TDD frames can be symmetrical/Unsymmetrical.
- The system has the capacity to change the up-link/downlink spreading factor as a function of the rates.
- Guard space can loosen the synchronization needs a bit.

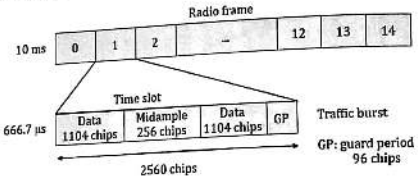


Figure 4.3: UTRA-TDD Frame Structure.

Q4] Explain in short Wireless Local Loop Architecture.

Q5] Wireless Local Loop.

Q6] Explain wireless local loop

Ans: [Q4 | 4M – Dec16], [Q5 | 10M – May15 & 5M - Dec17] & [Q6 | 5M – May

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 resid places.
3. There are various ways internet can be provided to the users such as fiber optic cable, DS and wireless connectivity.
4. Providing fixed wireless connection for broadband internet is referred as WLL or Wireless 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:

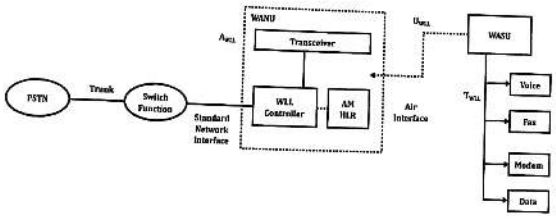


Figure 4.4: Wireless Local Loop Architecture.

1. Figure 4.4 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.
   c. Routing.
   d. Billing.

WASU:

1. WASU Stands for **Wireless Access Subscriber Unit.**
2. It acts as an 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

OR

1. SI 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 Ane interface between the WANU and the SI can be ISDN-BRI or IS-634 or IS-653.

Q7] What are the Deployment issues of WLL? [4M – May

Ans:

1. The cost of WLL should be competitive with its **wire line counterpart**.
2. To compete with other local loop technologies, WLL needs to provide
   a. Sufficient coverage and capacity
   b. High circuit quality
   c. Efficient data services
3. Various issues are considered in WLL development which include

I) Spectrum:

- Efficient spectrum management is the **key challenge**.
- The implementation of WLL should be flexible to accommodate different flexible bands as well as non-continuous bands.
- Most of these bands are licensed by government.

II) Service Quality:

- Quality offered by the WLL must be same or better than the services offered by its wire line counterpart.
- The quality requirements include link quality, reliability and fraud immunity.

III) Network Planning:

- Unlike Mobile System, WLL assumes that customer is stationary, not moving.
- Also the network penetration should be greater than 90%.
- Therefore WLL should be installed based on parameters like Population Density etc.

IV) Economics:

- In wire line local loop, the main cost is due to the cost of copper wires and the cost required to install them.
- In WLL, the major cost is electronic equipment's.
- In current scenario, the cost of such electronic equipment is reducing periodically.

Q8] Explain in detail 3G architecture

Ans:

3G: [10M – May17]

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 /UMTS ARCHITECTURE:

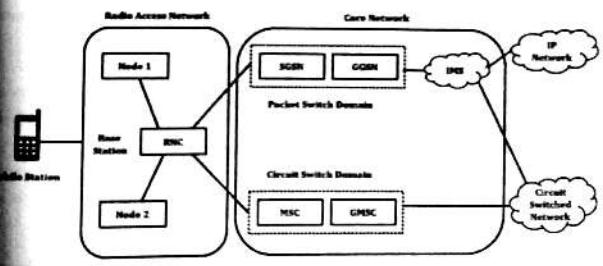


Figure 4.5: 3G Network Architecture Model.

Figure 4.5 shows 3G /UMTS Network.

The Constituent parts of 3G UMTS network are:

I) **Mobile Station:**
- It could be anything like data and voice-enabled mobile phones, tabs or computers which could be used as an end user.

II) **RAN (Radio Access Network):**
- It consists of base stations and radio access controller which bridges the gap between Mobile Station and Core Network.
- It also controls and manages the air interface for the whole network.

III) **CN (Core Network):**
- It provides the main processing and management of subsystems.
- 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:**
- It uses Circuit Switched Network in which dedicated link or channel is provided for a particular time slot to set of users.
- The two blocks shown in Circuit Switched Domain are:
  - **MSC:** Mobile Switching Centre manages circuit switched calls.
  - **GMSC:** Gateway MSC acts as an interface between external and internal networks.

II) **Packet-switched Domain:**
- It uses IP Network where IP's are responsible for transmitting and receiving data between two or more devices.
- The two blocks shown in Packet Switched Domain are:
  - **SGSN (Serving GPRS Support Node):** The various functions provided by SGSN are mobility management, session management, billing, interaction with other areas of the network.
  - **GGSN (Gateway GPRS Support Node):** It can be considered as a very complex router that 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:
- It uses 2G frequency bands with bandwidths up to 230MHz are used to achieve global roaming and multi-services.
- Wideband radio channel to support high-speed services.
- Radio carrier channel uses bandwidth up to 20M which improvises chip rate and anti-multipath fading.
- To improve the performance of the **downlink transmission** channel, fast closed loop power control technology is applied.

Q9] QoS in 3G **[5M – Dec17]**

Ans:

QOS:

1. Quality of Service (QoS) in cellular networks is defined as the capability of the cellular service providers to provide a satisfactory service.
2. Service includes voice quality, signal strength, low call blocking and dropping probability, high data rates for multimedia and data applications etc.

QOS FACTORS:
- **Throughput:** Throughput is the rate at which the packets go through the network. Maximum rate is always preferred.
- **Delay:** This is the time which a packet takes to travel from one end to the other. Minimum delay is always preferred.
- **Packet Loss Rate:** The rate at which a packet is lost. This should also be as minimum as possible.
- **Packet Error Rate:** This is the errors which are present in a packet due to corrupted bits. This should be as minimum as possible.
- **Reliability:** The availability of a connection. (Links going up/down).

QOS IN 3G:

1. In a 3G network, subscriber traffic is classified based on **traffic classes**.
2. Each traffic class is associated with a maximum bit rate and a guaranteed bit rate, which can be configured independently for uplink and downlink subscriber traffic.
3. To define the packet-forwarding treatment for bearer requests received on the broadband gateway, each traffic class is mapped to a forwarding class and packet loss priority (PLP) in a QoS classifier profile.
4. And if traffic is not mapped to a forwarding class and packet loss priority, the classification specified in the bearer request, coming from either the Gn or Gi interface, is carried over.

Table 4.1 shows the supported traffic classes as defined in the 3GPP standards.

Table 4.1: Traffic Classes for a 3G Network.

Traffic Class	Description	Example
Conversational	Conversational pattern with very low delay and jitter. This is the most delay-sensitive traffic class.	Voice and real-time multimedia messaging such as VoIP and video conferencing.
Streaming	Delay and jitter requirements are not as strict as with conversational traffic class.	Streaming type applications such as video on demand.
Interactive	Interactive class enables prioritization between Packet Data Protocol (PDP) contexts, which allows end-user or service prioritization. Interactive class is associated with a traffic handling priority (THP). THP values can be 1 through 3.	Streaming type applications such as video on demand, Web browsing, and Telnet.
Background	Best effort is acceptable for data delivery. This is the least delay-sensitive traffic class.	Background type applications such as e-mail and FTP.

Q10] Explain in detail 4G Architecture.

Ans: **[10M – May**

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, DECT 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 4.6 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.

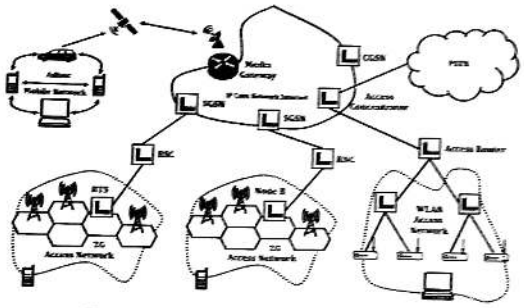


Figure 4.6: 4G Generic Mobile Communication Architecture.

Smart Antennas:

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

IPv6 Technology:

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

VoIP:

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

OFDM:

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

SDR:

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

Advantages:

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

Disadvantages:

- Battery usage is more.
- Hard to implement.

Q11] Draw and explain the architecture of TETRA and specify the standards and services offed by TETRA **[10M – Dec**

Ans:

TETRA:

1. TETRA Stands for **Terrestrial Trunked Radio.**
2. It is a set of standards developed by the European Telecommunications Standardization Institute (ETSI)
3. It is **digital radio trunking system.**
4. It offers another way of wireless data transmission.
5. It uses many different radio carriers but assign a specific carrier to a certain user according to demand for a short period of time.
6. **For example:** Taxi Services, Transport Companies with fleet management systems all can share a whole group of frequencies in trunked radio system for better frequency reuse via FDD or TDD

FEATURES:

1. End-to-End Encryption.
2. Call holding and call waiting.
3. Call queuing with pre-emptive priorities.
4. Authentication of devices.
5. User's Authentication.
6. Point-to-point and point-to-multipoint support.
7. System is fully digital.
8. It offers interfaces to the fixed telephone network.
9. Short number addressing.

TETRA ARCHITECTURE:

1. The system architecture of TETRA is shown in Figure 4.7.
2. The mobile station (MS) connects to the switching and management infrastructure via the Um interface (shown as AI — air interface in Figure).
3. The switching and management infrastructure contains the user databases (HDB, VDB), the base station and interfaces to PSTN, ISDN or PDN.
4. Though the architecture of TETRA is similar to GSM, the system itself is much simpler in real implementation compared to GSM as no handover is needed.
5. Taxis usually remain in a certain area which can be covered by one TETRA cell.

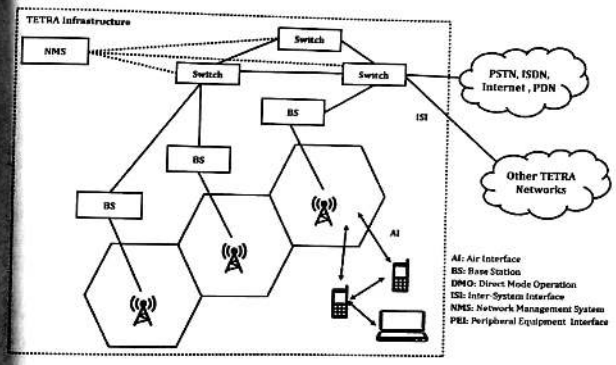


Figure 4.7: TETRA Architecture.

TETRA SERVICES:

TETRA offers two standards:

1) **Voice + Data (V + D) Service:**

- It offers **circuit-switched voice and data transmission.**
- This mode comprises unicast and broadcast connections.
- It also provides group communication within a certain protected group.
- It provides direct ad-hoc mode without a base station.
- The direct ad-hoc mode is shown in Figure 4.8.
- Direct Mode of TETRA enables ad-hoc operation and is one of the most important differences to pure infrastructure-based networks such as GSM, cdma2000 or UMTS.

SDR:

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

Advantages:

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

Disadvantages:

- Battery usage is more.
- Hard to implement.

Q11] Draw and explain the architecture of TETRA and specify the standards and services offed by TETRA **[10M – Decem**

Ans:

TETRA:

1. TETRA Stands for **Terrestrial Trunked Radio.**
2. It is a set of standards developed by the European Telecommunications Standardization Institute (ETSI)
3. It is **digital radio trunking system.**
4. It offers another way of wireless data transmission.
5. It uses many different radio carriers but assign a specific carrier to a certain user according to the demand for a short period of time.
6. **For example:** Taxi Services, Transport Companies with fleet management systems all can share a whole group of frequencies in trunked radio system for better frequency reuse via FDD or TDD

FEATURES:

1. End-to-End Encryption.
2. Call holding and call waiting.
3. Call queuing with pre-emptive priorities.
4. Authentication of devices.
5. User's Authentication.
6. Point-to-point and point-to-multipoint support.
7. System is fully digital.
8. It offers interfaces to the fixed telephone network.
9. Short number addressing.

TETRA ARCHITECTURE:

1. The system architecture of TETRA is shown in Figure 4.7.
2. The mobile station (MS) connects to the switching and management infrastructure via the Um interface (shown as AI — air interface in Figure).
3. The switching and management infrastructure contains the user databases (HDB, VDB), the base station and interfaces to PSTN, ISDN or PDN.
4. Though the architecture of TETRA is similar to GSM, the system itself is much simpler in real implementation compared to GSM as no handover is needed.
5. Taxis usually remain in a certain area which can be covered by one TETRA cell.

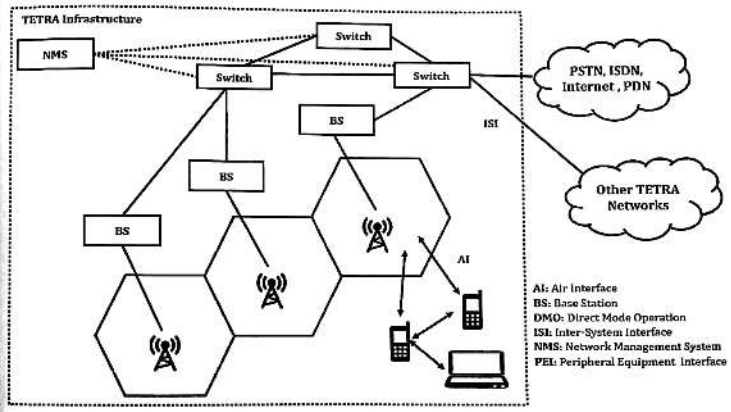


Figure 4.7: TETRA Architecture.

TETRA SERVICES:

TETRA offers two standards:

I) Voice + Data (V + D) Service:

- It offers **circuit-switched voice and data transmission.**
- This mode comprises unicast and broadcast connections.
- It also provides group communication within a certain protected group.
- It provides direct ad-hoc mode without a base station.
- The direct ad-hoc mode is shown in Figure 4.8.
- Direct Mode of TETRA enables ad-hoc operation and is one of the most important differences to pure infrastructure-based networks such as GSM, cdma2000 or UMTS.

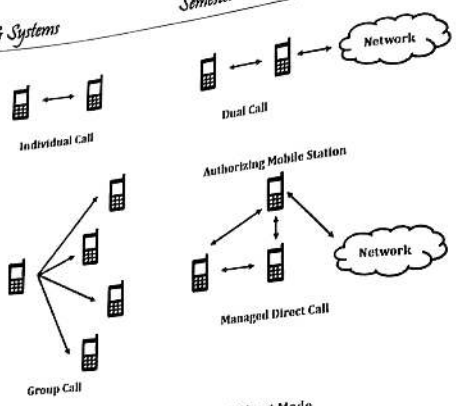


Figure 4.8: TETRA Direct Mode.

II) Packet Data Optimized (PDO) Service:

- PDO offers only packet data transmission.
- It provides both connection-oriented as well as connectionless service for data transmission.
- PDO may be point-to-point or point-to-multipoint.

In addition to these two services TETRA also offers Bearer Services.

Bearer Service:

Following services are offered in the V+D type of services.

- 7.2 - 28.8 kbit/s circuit-switched, for unprotected speech and data transmission.
- 4.8 - 19.2 kbit/s circuit-switched, for minimally protected data transmission.
- 2.4 - 9.6 kbit/s circuit-switched, for highly protected data transmission.
- Connection-oriented point-to-point packet transmission.
- Connection less point-to-point packet transmission in a standard format.
- Connection less transmission in a special format i.e. point to point, multi-point broadcast.

The last three services are also offered in PDO mode of TETRA.

ADVANTAGES:

- Very long reach because of up to 20W power emission.
- End-to-End security using strong encryption.
- Direct Mode allows infrastructure free operation.
- Good for fleet-control systems.

Q12] Compare 3G and 4G.

Ans: **[10M – Dec16]**

Table 4.2 shows the comparison between 3G & 4G.

Table 4.2: Comparison between 3G & 4G

Parameter	3G	4G
Packet Upload Rate	5 Mbps.	500 Mbps.
Packet Download Rate	100 Mbps.	1 Gbps.
Internet Service	Broadband.	Ultra Broadband.
Mobile TV Resolution	Low.	High.
Speed	384 Kbps to 2 Mbps.	20 to 100 Mbps in Mobile Node.
Bandwidth	5 – 20 MHz.	100 + MHz.
Network Architecture	Width Area Network.	Hybrid Network.
IP	Multiple Versions.	IPv6.
Access Technology	WCDMA/ CDMA 2000.	OFDM.
Switched Technology	Circuit Switched and Packet Switched.	Only Packet Switched.
Handoff	Horizontal.	Horizontal & Vertical.
Core Network	Packet Network.	Internet.
Service	Integrated high quality audio, video and data.	Dynamic information access and wearable devices.
Forward Error Correction	Turbo and convolution.	IPv6.
Applications	CDMA 2000, UMTS, EDGE Etc.	WiMax2 and LTE-Advance.

Q13] Explain difference in GSM, GPRS and UMTS.

Ans: **[10M – Dec15]**

Table 4.3 shows the difference in GSM, GPRS and UMTS.

Table 4.3: Comparison between GSM, GPRS & UMTS.

Parameter	GSM	GPRS	UMTS
Full Form	Global System for Mobile Communication.	General Packet Radio Service.	Universal Mobile Telecommunication 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.

Q14] Compare WCDMA and CDMA 2000 **[5M – Dec'**

Ans:

Table 4.4 shows the difference between WCDMA and CDMA 2000.

Table 4.4: Comparison between WCDMA and CDMA 2000.

Parameter	WCDMA	CDMA 2000
Signaling	GSM – MAP.	ANSI – 41.
Frame Duration	10 ms.	20 ms.
Base Station Synchronization	Asynchronous.	Synchronous.
Power Control Rate	1500 times/s.	800 times/s.
Modulation	BPSK.	Forward link: QPSK Reverse link: BPSK.
Chip Rate	4.096 MHz.	3.6864 MHz.
Multi-carrier spreading option	No.	Yes.
Modes of operation	FDD and TDD.	FDD.
Voice coder	AMR.	EVRC.
Overhead	High (because of non-shared, pilot code channel).	Low (because of shared pilot code channel)
Peak data rate	2 Mbps.	614 kbps.

---- EXTRA QUESTION ----

Q1] IMT 2000?

Ans:

IMT 2000:

1. IMT-2000 Stands for **International Mobile Telecommunications 2000.**
2. It was proposed by International Telecommunication Union (ITU).
3. Initially it was proposal for **3G Networks.**
4. After many political discussions this idea was dropped and so-called family of 3G Standards was developed.
5. The European proposal for IMT-2000 prepared by ETSI is called as **Universal Mobile Telecommunication Systems (UMTS).**

FEATURES:

1. It used for all Radio Environments.
2. It supports both packet switched and circuit switched data transmissions.
3. It offers high spectrum efficiency.
4. It supports wide range of telecommunications services like voice, data, multimedia and internet.

IMT 2000 ARCHITECTURE:

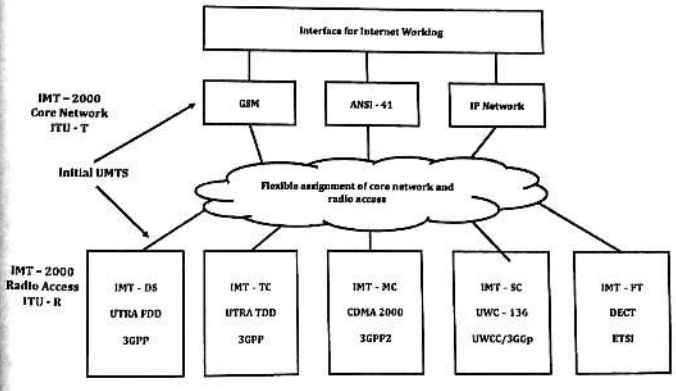


Figure 4.9: IMT-2000 Architecture.

1. Figure 4.9 shows the IMT – 2000 Architecture.
2. As shown in figure 4.9, the ITU standardize 5 groups of 3G for radio access technology.

IMT-DS:

- It uses the **Direct Spread Technology**.
- It is also called as Wideband CDMA.
- It is the part of Third Generation Partnership Project (3GPP).

IMT-TC:

- It uses **Time Code Technology**.
- It is further divided into 2 standards: TDD and TD-SCDMA.

IMT-MC:

- It uses **Multi-Carrier Technology**.
- CDMA-2000 is a multi-carrier technology and is a part of 3GPP2.

IMT-SC:

- It uses **Single-Carrier Technology**.
- It is enhancement of US TDMA Systems.

IMT-FT:

- It uses **Frequency-Time Technology**.
- It is enhancement version of the digital cordless telephone standard DECT.

CHAPTER - 5: MOBILITY MANAGEMENT

Q1] PSTN **[5M - Dec15]**

Ans:

PSTN:

1. PSTN Stands for **Public Switched Telephone Network.**
2. It is also called as **Plain Old Telephone Service.**
3. It is inter connected voice oriented public telephone networks.
4. It uses **Circuit-Switching Network.**

FEATURES:

1. It provides Analog & Digital Signaling.
2. It provides Mobile Wireless Access.
3. PSTN allow different networks in different countries to interconnect seamlessly.
4. It also provides **Automatic Call Distribution.**

PSTN ARCHITECTURE:

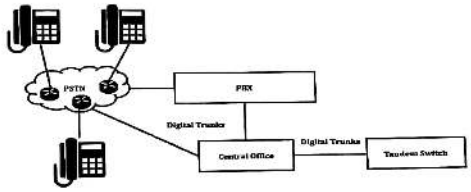


Figure 5.1: Basic PSTN Architecture.

1. Figure 5.1 shows Basic PSTN Architecture.
2. As shown in figure, Central Office is connected locally through Tandem switch.
3. Central Office is also known as **Local Exchange.**
4. Tandem Switch is also known as **Backbone Switch or Core Switch.**
5. Digital Trunks are used between Central Office Switches.
6. Information transfer in PSTN takes place over trunked lines comprised of fiber optic cables, microwave links and satellite links.
7. **Private Branch Exchange (PBX)** in PSTN is used for providing the telephony service within an organization or office.
8. PSTN network makes uses of combination of **mesh topology and hierarchical tree.**

Q2) Cellular IP. **[5M - Dec15 & Dec19]**

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 5.2 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.

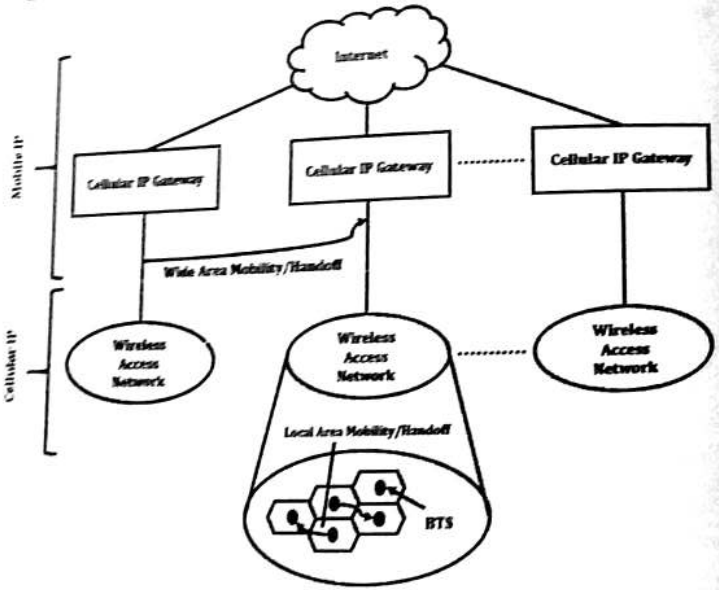


Figure 5.2: Cellular IP Architecture.

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:

- Cellular IP Provides easy global migration.
- Flexible Handoff.

Q3] Location management HLR-VLR Scheme.

Ans: **[5M - May16]**

HLR-VLR SCHEME:

1. HLR-VLR Scheme is used in **Local Management.**
2. It is a static location update scheme.
3. It is also known as **two level hierarchical database scheme.**
4. The HLR stores the user profiles of its assigned subscribers.
5. These user profiles contain information such as the type of services subscribed, the quality-of-service (QoS) requirements and the current location of the mobile terminals.
6. Each VLR stores replications of the user profiles of the subscribers currently residing in its associated Location Area (LA).
7. In order to effectively locate a mobile terminal when a call arrives, each mobile terminal is required to report its location whenever it enters a new LA.
8. This reporting process is called **location update.**
9. On receiving a location update message, the MSC updates its associated VLR and transmits the new location information to the HLR.
10. We call this register update process as **location registration.**
11. The HLR will acknowledge the MSC for the successful registration and it will also deregister the mobile terminal at the VLR of old LA.
12. Figure 5.3 shows the HLR-VLR Architecture regarding Location management.

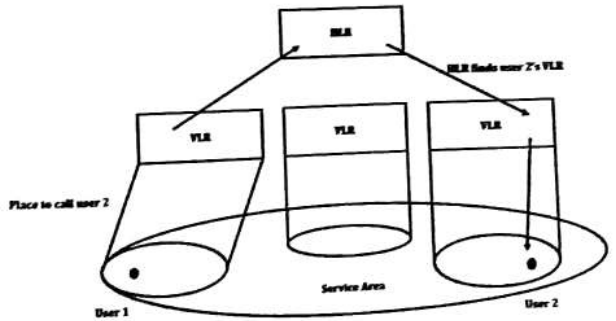


Figure 5.3: HLR-VLR Architecture.

--- EXTRA QUESTIONS ---

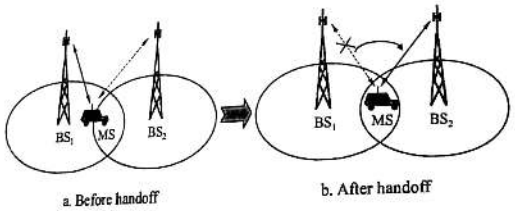
Q1] Explain types of handoff?

Ans:

1. Handoff is the technique which enables a call to proceed uninterrupted when the user moves from one cell to another.
2. Handoff process involves 3 main stages:
   a. Handoff Initiation.
   b. Establishing a new connection.
   c. Data transfer to new connection.
3. There are two basic types of Handoffs:

HARD HANDOFF:

1. It is also known as **"Break before Make" connection**.
2. In this type of handoff, the link to the old Base Station (BS) is terminated before the Mobile Station (MS) establishes a link with the new Base Station.
3. It is used in FDMA/TDMA based mobile systems.
4. Figure 5.4 shows the Mechanisms of Hard Handoff.



a. Before handoff b. After handoff

Figure 5.4: Mechanism of Hard Handoff.

5. Hard Handoff is further classifies as:

I) Intra Cell Handoff:

- In Intra Cell Handoff, the handover occurs within the same cell.
- Intra-cell handover switches a call in progress from one physical channel of a cell to another physical channel of the same cell.

II) Inter Cell Handoff:

- In Inter Cell Handoff, the handover occurs between two cells.
- The inter-cell handover switches a call in progress from one cell to another cell.

- It can be of two types:
  - **Inter BSC:** Here the MS moves from one cell to another cell controlled by the different BSCs.
  - **Inter MSC:** Here the MS moves from one cell to another cell controlled by different MSCs.

III) Inter System Handoff:

- In Inter System Handoff, the handover occurs between two systems.
- This type of handoff occurs when the mobile unit moves from one cellular systems to a different cellular system.
- Example: From GSM to UMTS.

SOFT HANDOFF:

1. It is also called as **Mobile Directed Handoff or "Make-before-Break" Connection.**
2. In this type of handoff, the link to the old Base Station (BS) is not terminated before the Mobile Station (MS) establishes a link with the new Base Station.
3. Once the link is established the connection to old BS is terminated.
4. It is used in UMTS to improve the signal quality.
5. It is more seamless handover.
6. Figure 5.5 shows the Mechanisms of Soft Handoff.

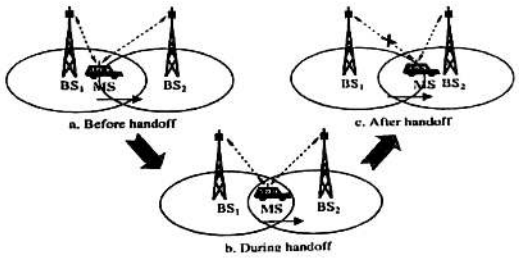


Figure 5.5: Mechanism of Soft Handoff.

--- EXTRA QUESTIONS ---

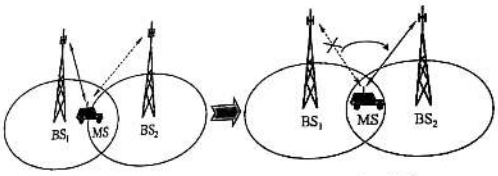
Q1] Explain types of handoff?

Ans:

1. Handoff is the technique which enables a call to proceed uninterrupted when the user moves from one cell to another.
2. Handoff process involves 3 main stages:
   a. Handoff Initiation.
   b. Establishing a new connection.
   c. Data transfer to new connection.
3. There are two basic types of Handoffs:

HARD HANDOFF:

1. It is also known as **"Break before Make" connection.**
2. In this type of handoff, the link to the old Base Station (BS) is terminated before the Mobile Station (MS) establishes a link with the new Base Station.
3. It is used in FDMA/TDMA based mobile systems.
4. Figure 5.4 shows the Mechanisms of Hard Handoff.



a. Before handoff b. After handoff

Figure 5.4: Mechanism of Hard Handoff.

5. Hard Handoff is further classifies as:

I) **Intra Cell Handoff:**

- In Intra Cell Handoff, the handover occurs within the same cell.
- Intra-cell handover switches a call in progress from one physical channel of a cell to another physical channel of the same cell.

II) **Inter Cell Handoff:**

- In Inter Cell Handoff, the handover occurs between two cells.
- The inter-cell handover switches a call in progress from one cell to another cell.

- It can be of two types:
  - **Inter BSC:** Here the MS moves from one cell to another cell controlled by the different BSCs.
  - **Inter MSC:** Here the MS moves from one cell to another cell controlled by different MSCs.

III) **Inter System Handoff:**

- In Inter System Handoff, the handover occurs between two systems.
- This type of handoff occurs when the mobile unit moves from one cellular systems to a different cellular system.
- Example: From GSM to UMTS.

SOFT HANDOFF:

1. It is also called as **Mobile Directed Handoff or "Make-before-Break" Connection.**
2. In this type of handoff, the link to the old Base Station (BS) is not terminated before the Mobile Station (MS) establishes a link with the new Base Station.
3. Once the link is established the connection to old BS is terminated.
4. It is used in UMTS to improve the signal quality.
5. It is more seamless handover.
6. Figure 5.5 shows the Mechanisms of Soft Handoff.

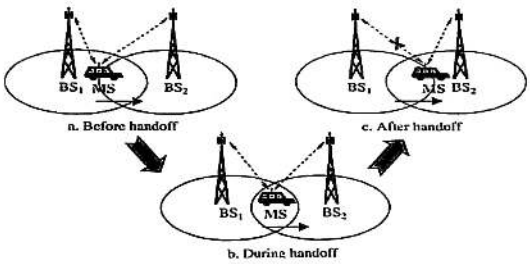


Figure 5.5: Mechanism of Soft Handoff.

--- EXTRA QUESTIONS ---

Q1] Explain types of handoff?

Ans:

1. Handoff is the technique which enables a call to proceed uninterrupted when the user moves from one cell to another.
2. Handoff process involves 3 main stages:
   a. Handoff Initiation.
   b. Establishing a new connection.
   c. Data transfer to new connection.
3. There are two basic types of Handoffs:

HARD HANDOFF:

1. It is also known as **"Break before Make" connection.**
2. In this type of handoff, the link to the old Base Station (BS) is terminated before the Mobile Station (MS) establishes a link with the new Base Station.
3. It is used in FDMA/TDMA based mobile systems.
4. Figure 5.4 shows the Mechanisms of Hard Handoff.

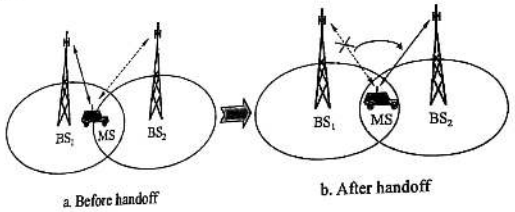


Figure 5.4: Mechanism of Hard Handoff.

5. Hard Handoff is further classifies as:

I) **Intra Cell Handoff:**

- In Intra Cell Handoff, the handover occurs within the same cell.
- Intra-cell handover switches a call in progress from one physical channel of a cell to another physical channel of the same cell.

II) **Inter Cell Handoff:**

- In Inter Cell Handoff, the handover occurs between two cells.
- The inter-cell handover switches a call in progress from one cell to another cell.

- It can be of two types:
  - **Inter BSC:** Here the MS moves from one cell to another cell controlled by the different BSCs.
  - **Inter MSC:** Here the MS moves from one cell to another cell controlled by different MSCs.

III) **Inter System Handoff:**

- In Inter System Handoff, the handover occurs between two systems.
- This type of handoff occurs when the mobile unit moves from one cellular systems to a different cellular system.
- Example: From GSM to UMTS.

SOFT HANDOFF:

1. It is also called as **Mobile Directed Handoff or "Make-before-Break" Connection.**
2. In this type of handoff, the link to the old Base Station (BS) is not terminated before the Mobile Station (MS) establishes a link with the new Base Station.
3. Once the link is established the connection to old BS is terminated.
4. It is used in UMTS to improve the signal quality.
5. It is more seamless handover.
6. Figure 5.5 shows the Mechanisms of Soft Handoff.

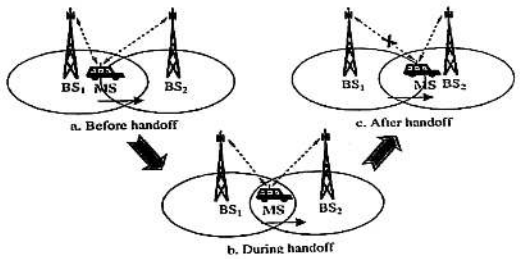


Figure 5.5: Mechanism of Soft Handoff.

Q2] Explain handoff management techniques?

Ans:

1. Handoff management is sometimes also known as **Handover Management.**
2. When a call moves into/ a different cell, the MSC automatically transfer the call to a new channel belonging to the new base station. This process is called Handoff Management.
3. Three measurements are used for handoff management.
   a. Word error indicator (WEI).
   b. Received signal strength indicator (RSSI): 80db— 100db
   c. Quality indicator (QI): 5db-25db.
4. Handoff management involves handoff detection.
5. Handoff Detection defines the occurrence of handoff whenever the call is transferred from one base station to another base station or we can say whenever subscriber moves from one cell to another.
6. There are 3 types of handoff detection strategies:

I) Mobile Controlled Handoff:

- In Mobile Controlled Handoff, the MS control the handoff process.
- MS chooses the best base station where the signal strength quality is good.
- MS monitors received signal strength and quality of signal from current BS and then choose the best BS for call processing.
- Mobile Controlled Handoff is used in **DECT and PACS.**

II) Network Controlled Handoff:

- Network Controlled Handoff is a centralized handoff protocol, in which the network makes handoff decision based on measurements of the signal strength and quality of mobile station.
- In this the surrounding BS's measures the signal from the MS, and the network initiates the handoff process when some handoff criteria are met.
- Network Controlled Handoff is used in **CT-2 plus and AMPS.**

III) Mobile Assisted Handoff:

- Mobile Assisted Handoff is a variant of Network Controlled Handoff.
- In this the network asks the MS to measure the signal from the surrounding BS's.
- The network makes the handoff decision based on reports from the MS.
- Mobile Assisted Handoff is used in **GSM and IS-95 CDMA.**

CHAPTER - 6: WIRELESS LOCAL AREA NETWORK

Q1] Explain in detail Bluetooth Protocol Architecture.

Ans: **[10M – May16, Dec16 & May17]**

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:

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 6.1 shows the Bluetooth Protocol Architecture.

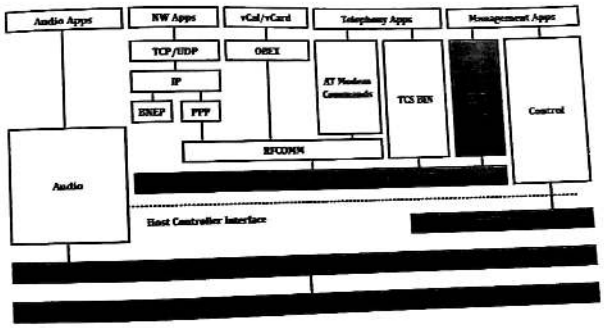


Figure 6.1: Bluetooth Protocol Architecture.

It consists of following components:

CORE PROTOCOLS:

I) Radio Layer:

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

II) **Baseband Layer:**

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

III) **Link Manager Protocol:**

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

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

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

V) **Service Discovery Protocol (SDP):**

- Service related queries including device information can be taken care at this protocol so that connection can be established between bluetooth devices.
- 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.

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

Q2] Describe Bluetooth architecture and protocol stack. Also, discuss its limitations.

Ans: **[10M – Dec17]**

BLUETOOTH:

Refer Q1.

BLUETOOTH ARCHITECTURE:

Bluetooth Architecture defines two types of networks.

I) **Piconet:**

- Piconet is a Bluetooth network that consists of 1 master node and 7 active slave nodes.
- Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
- There can be only one master station in each piconet.
- The communication between the master and the slave can be one-to-one or one-to-many.
- All communication is between master and a slave. Salve-slave communication is not possible.
- In addition to seven active slave station, a piconet can have upto 255 parked nodes.
- These parked nodes are slave stations and cannot take part in communication until it is moved from parked state to active state.
- Figure 6.2 represents Piconet.

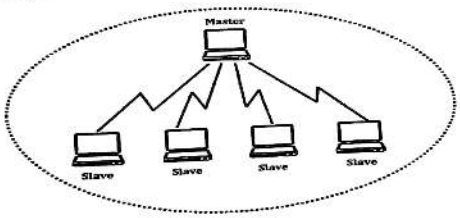


Figure 6.2: Piconet.

II) **Scatternet:**

- Scatternet is formed by combining various piconets.
- A slave in one picunet can act as a master in other piconet.
- A station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master.
- This node is also called **bridge slave.**
- Thus a station can be a member of two piconets.
- A station cannot be a master in two piconets.
- Figure 6.3 represents Scatternet.

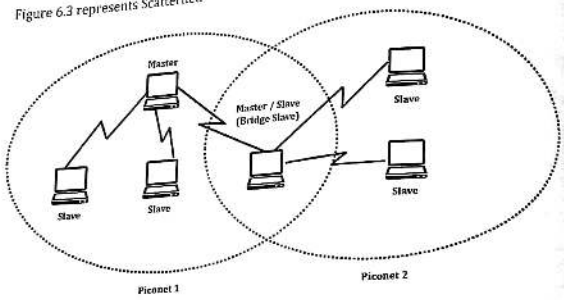


Figure 6.3: Scatternet.

BLUETOOTH PROTOCOL STACK:

Refer Q1.

LIMITATIONS:

- One of the big disadvantages of bluetooth is **security.**
- This is due to the fact that it operates on Radio frequency and hence can penetrate through walls.
- It is advisable not to use it for critical business or personal data transfer.
- As HomeRF technology operates on same frequency, It has interference from it.
- The bandwidth is lower compare to WiFi.
- Battery usage is more compare to the condition when bluetooth is powered OFF.
- The new technology known as BLE or bluetooth low energy or bluetooth smart is developed to enhance the battery life further.

Q3] Explain how a Bluetooth network is established using baseband state translations.

Ans:

DEVICE DISCOVERY & NETWORK ESTABLISHMENT: **[10M – Dec15]**

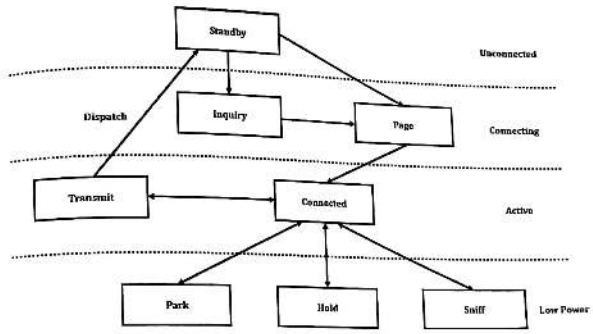


Figure 6.4: Baseband Stages.

1. As shown in figure 6.4, 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:**
        i. Out of all the three low power states, this one has maximum power consumption.
        ii. It is used to sniffs data.

b. **Hold:**
   i. The device here stops all ACL link transmissions.
   ii. If no activity is there in the piconet, the slave reduce the power consumption or participates in another piconet.

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

Q4] Explain functioning of Bluetooth Baseband layer. **[10M – May18]**

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.

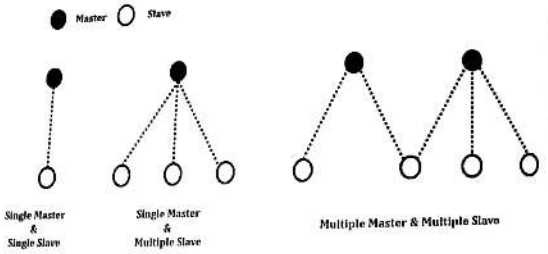


Figure 6.5: Bluetooth Baseband Spectrum.

1. Figure 6.5 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:

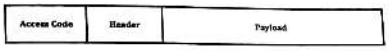
SCO (Synchronous Connection-Oriented) Link:

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

ACL (Asynchronous Connection-Less) Link:

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

PACKET FORMAT:



I) **Access Code:**
- Access code is used for timing synchronization, offset compensation, paging and inquiry.
- There are three different types of Access code:
  - Channel Access Code (CAC).
  - Device Access Code (DAC).
  - Inquiry Access Code (IAC).
- 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.

Q5] Explain Hidden station and exposed station problems in WLAN. **[5M – May18]**

Ans:

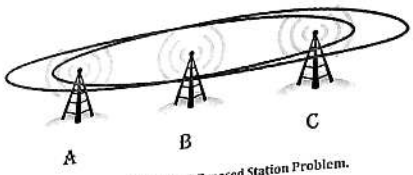


Figure 6.6: Hidden & Exposed Station Problem.

1. Consider following three mobile phone as shown in figure 6.6.
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.
7. In such situation, 'C' is exposed to 'B'.

Q6] Explain in short how Hidden Station Problem is avoided in WLAN.

Q7] What is hidden and exposed terminal problem? Discuss solutions to these problems

Q8] Why do Hidden and Exposed terminal problems arise? How would you propose to solve it

Ans: **[Q6 | 5M – May15], [Q7 | 5M – May17] & [Q8 | 5M – Dec17]**

HIDDEN & EXPOSED TERMINAL PROBLEM:

Refer Q5.

SOLUTION:

1. Hidden and Exposed Terminal Problems can be solved by using **Multiple Access with Collision Avoidance (MACA).**
2. MACA uses short signaling packets to avoid collisions.
3. The signaling packets are of two types as follows:
   a. **Request To Send (RTS):** The sender first send this packet to the receiver when it has some data to send.
   b. **Clear To Send (CTS):** The receiver sends this packet to a sender as soon as it is ready to receive packets.

SOLUTION TO HIDDEN TERMINAL:

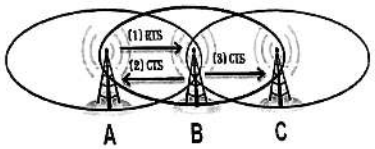
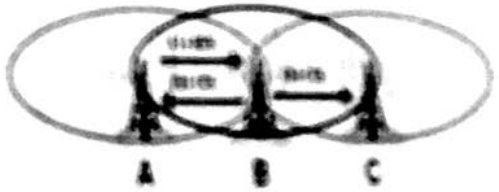


Figure 6.7: Solution to Hidden Station Problem.

1. As shown in Figure 6.7, 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.



Q5] Explain Hidden station and exposed station problems in WLAN. **[5M – May15]**

Ans:

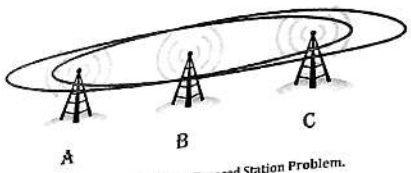


Figure 6.6: Hidden & Exposed Station Problem.

1. Consider following three mobile phone as shown in figure 6.6.
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.
7. In such situation, 'C' is exposed to 'B'.

Q6] Explain in short how Hidden Station Problem is avoided in WLAN.
Q7] What is hidden and exposed terminal problem? Discuss solutions to these problems
Q8] Why do Hidden and Exposed terminal problems arise? How would you propose to solve it

Ans: **[Q6 | 5M – May15], [Q7 | 5M – May17] & [Q8 | 5M – Dec17]**

HIDDEN & EXPOSED TERMINAL PROBLEM:

Refer Q5.

SOLUTION:

1. Hidden and Exposed Terminal Problems can be solved by using **Multiple Access with Collision Avoidance (MACA).**
2. MACA uses short signaling packets to avoid collisions.
3. The signaling packets are of two types as follows:
   a. **Request To Send (RTS):** The sender first send this packet to the receiver when it has some data to send.
   b. **Clear To Send (CTS):** The receiver sends this packet to a sender as soon as it is ready to receive packets.

SOLUTION TO HIDDEN TERMINAL:

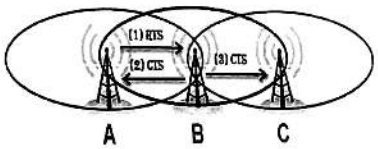


Figure 6.7: Solution to Hidden Station Problem.

1. As shown in Figure 6.7, 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.

4. C now knows that the medium is reserved by B and is down and try not to transmit to B for the duration of some indicated by CTS.
5. Thus, there can be no collision at B and hence hidden terminal problem is solved.

SOLUTION TO EXPOSED TERMINAL

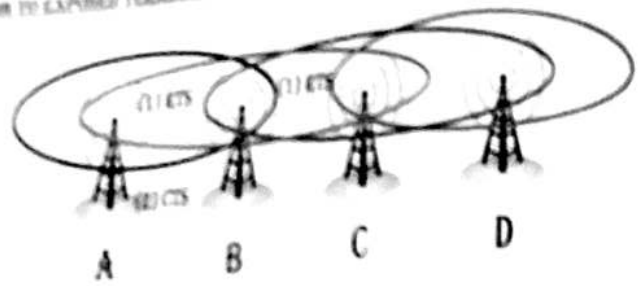


Figure 6.8: Solution to Exposed Station Problem.

1. As shown in Figure 6.8, terminal 'C' is exposed from 'B'.
2. 'B' wants to send data to 'A'.
3. 'C' also wants to send data to someone else as say 'D' to '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.
9. Thus, 'C' can start transmission to 'D' as it knows that it cannot cause a collision at A.

Qu] Explain in detail HIPERLAN/1 physical layer. **[10M – May08]**

Ans:

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

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.

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.

1. HiperLAN/1 uses **Non Differential Gaussian Minimum Shift Keying** (GMSK).
2. It uses **Decision Feedback Equalizer** (DFE) to remove other symbol interference.
3. To minimize the error at physical layer, it uses **BCH Error Correcting Codes**.
4. This code is able to correct a single error and detect two random errors.
5. Figure 6.9 shows HiperLAN/1 Data Packet format used at physical layer.
6. It shows the Data Packet & ACK Packet.

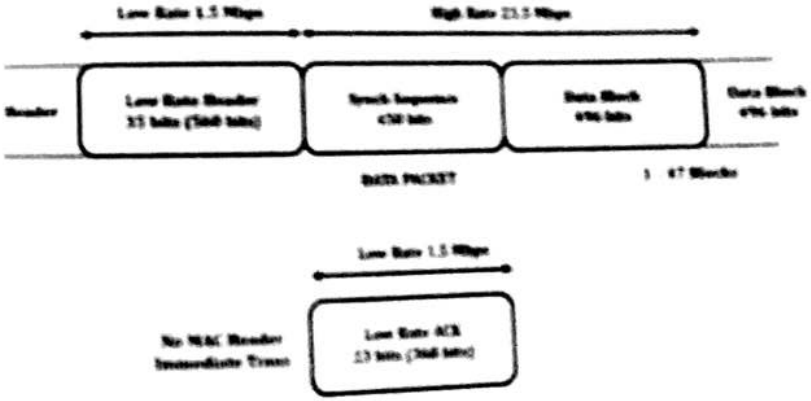


Figure 6.9: HiperLAN/1 Physical Layer Packet Format.

- 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:

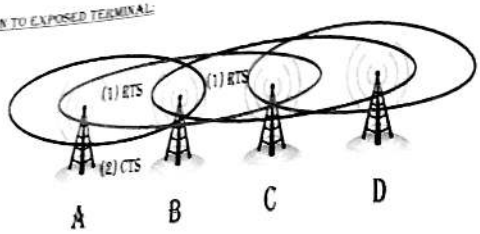


Figure 6.8: Solution to Exposed Station Problem.

1. As shown in Figure 6.8, 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.
9. Thus, 'C' can start transmission to 'D' as it known that it cannot cause a collision at A.

Q9) Explain in detail HIPERLAN/1 physical layer.

Ans: **[10M – May16]**

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 6.9 shows HiperLAN/1 Data Packet format used at physical layer.
8. It shows the Data Packet & ACK Packet.

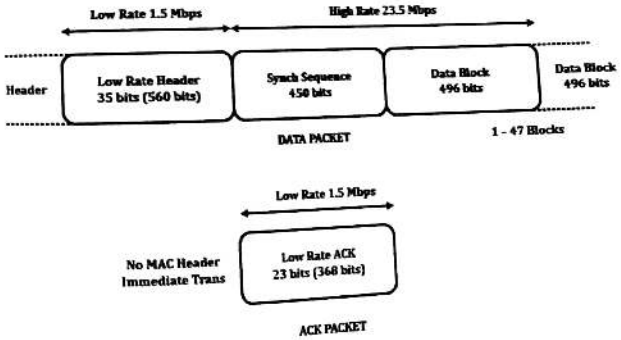


Figure 6.9: HiperLAN/1 Physical Layer Packet Format.

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:

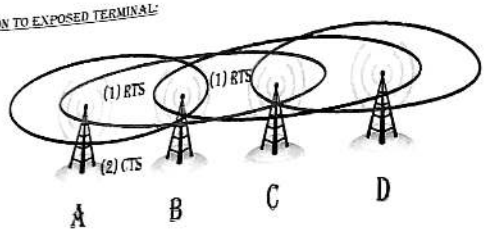


Figure 6.8: Solution to Exposed Station Problem.

1. As shown in Figure 6.8, 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.
9. Thus, 'C' can start transmission to 'D' as it known that it cannot cause a collision at A.

Q9] Explain in detail HIPERLAN/1 physical layer.

Ans: **[10M – May16]**

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 6.9 shows HiperLAN/1 Data Packet format used at physical layer.
8. It shows the Data Packet & ACK Packet.

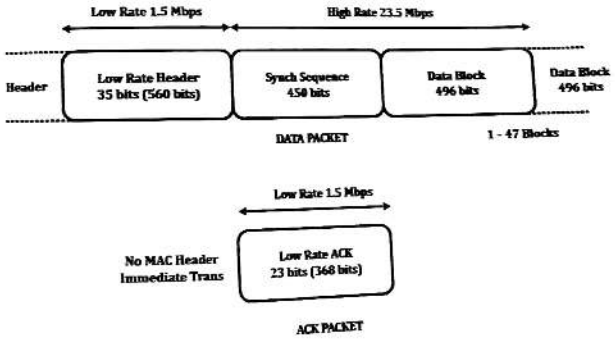


Figure 6.9: HiperLAN/1 Physical Layer Packet Format.

Q10] Explain Hiperlan2 **[10M – May17]**

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:

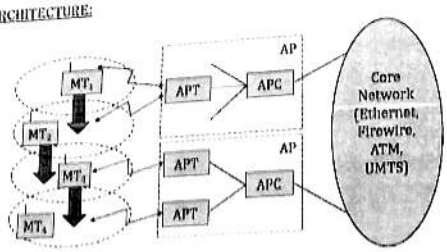


Figure 6.10: HiperLAN 2 Architecture.

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 6.10 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).
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):**
- This is an infrastructure based and mandatory mode.
- All APs are connected to a core network and MTs are associated with Aps.
- If two MTs share the same cell then all data is transferred by AP.
- AP takes complete control of everything.

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

Q11] Explain in Detail IEEE 802.11 MAC sublayer **[10M – Dec16]**

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.

MAC SUBLAYER FRAME FORMAT:

Figure 6.11 shows the general MAC Sublayer Frame Format of IEEE 802.11

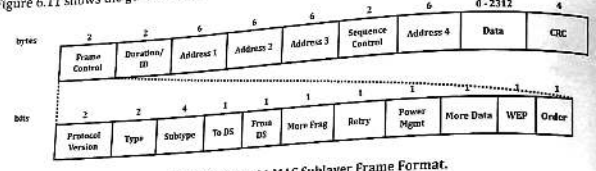


Figure 6.11: IEEE 802.11 MAC Sublayer Frame Format.

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.

Q12) Explain synchronization in 802.11 MAC management layer for both infrastructure as well Adhoc WLANs.

Ans:

SYNCHRONIZATION: **[10M – May15]**

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:

- In Infrastructure Based Network, an access point (AP) coordinates the synchronization process.
- Access Point transmits a special frame called **Beacon.**
- It is transmitted periodically.
- A Beacon frame consists of a **timestamp** and other management information used for power management and roaming.
- Other wireless nodes adjust their local clocks with beacon timestamp.
- Node is not required to hear every beacon to stay synchronized.
- From time to time, clock of every node is adjusted.
- If the medium is busy, the access point postpones the transmission of the beacon frame.
- Figure 6.12 shows Beacon Transmission in 802.11 Infrastructure Based Network.

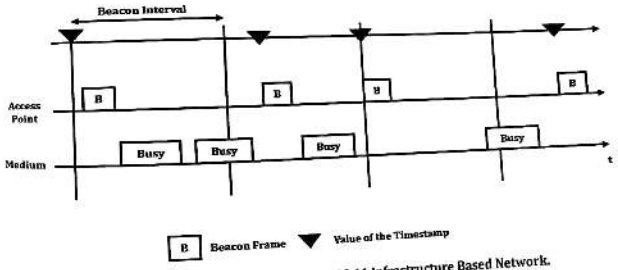


Figure 6.12: Beacon Transmission in 802.11 Infrastructure Based Network.

SYNCHRONIZATION PROCESS FOR ADHOC NETWORKS:

- In Adhoc Network, each node within the network is responsible for synchronization process.
- There is no Access point.

- After each beacon interval, all stations choose random **back-off time**.
- Only one station whose random delay time is less becomes the winner.
- Winner can send the beacon frame.
- All the other stations or nodes should adjust their local clock accordingly.
- Figure 6.13 shows Beacon Transmission in 802.11 Adhoc Network.

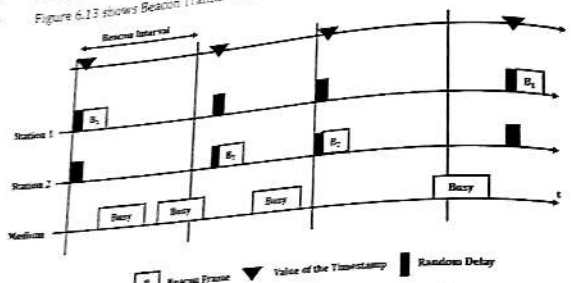


Figure 6.13: Beacon Transmission in 802.11 Adhoc Network.

Q13] Explain power management in IEEE 802.11 infrastructure networks and ad-hoc networks. **[10M – Dec17]**

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.

4. Figure 6.14 shows Power Management in IEEE 802.11 Infrastructure Based Network.

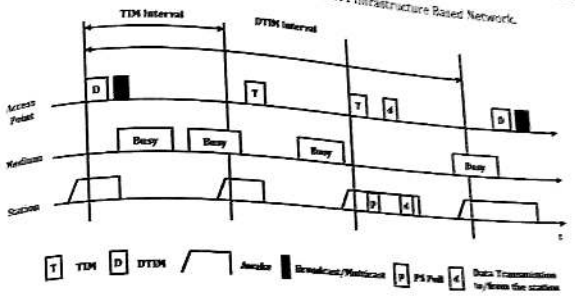


Figure 6.14: Power Management in IEEE 802.11 Infrastructure Based Network.

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 6.15 shows Power Management in IEEE 802.11 Adhoc Network.

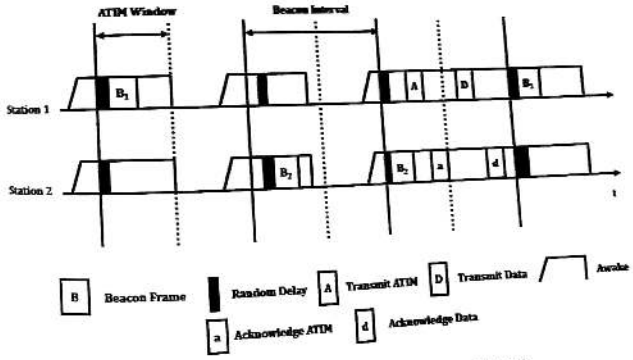


Figure 6.15: Power Management in IEEE 802.11 Adhoc Network.

Q14] Explain the difference between Adhoc Network and infrastructure based wireless networks. **[5M – Dec15]**

Ans:

Table 6.1 shows the difference between Adhoc Network and Infrastructure Based Network.

Table 6.1: 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.

Q15] Compare various IEEE 802.11x standards (a/b/g/i/n etc.). **[10M – Dec15]**

Ans:

Table 6.2 shows the difference between Various IEEE 802.11X Standards.

Table 6.2: Difference between Various IEEE 802.11X Standards.

Parameters	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	-	-

Q16] Compare HIPERLAN-1, HIPERLAN-2 and 802.11 W-LAN.

Q17] HIPERLAN 1 Vs HIPERLAN 2.

Q18] Compare HIPERLAN 2, BLUETOOTH, IEEE 802.11.

Ans: **[Q16 | 10M – May15], [Q17 | 5M – Dec15] & [Q18 | 10M – May16 & Dec16]**

Table 6.3: Comparison between IEEE 802.11, HIPERLAN 1, HIPERLAN 2 and Bluetooth.

Parameters	IEEE 802.11b	IEEE 802.11i	HIPERLAN1	HIPERLAN2	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 HMTS.	PPP and Ethernet.
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.

Q19] Compare and contrast HIPERLAN 2 and IEEE 802.11

[10M – Dec17]

Ans:

Refer Q18.

CHAPTER - 7: INTRODUCTION TO ANDROID

Q1] Android Framework.

Ans: **[10M – May15 | 5M – Dec15 & Dec16]**

ANDROID:

1. Android is a mobile operating system developed by **Google.**
2. It is based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets.

ANDROID FRAMEWORK:

Android operating system is a stack of software components which is roughly divided into **five sections** and **four main layers** as shown below in the Figure 7.1.

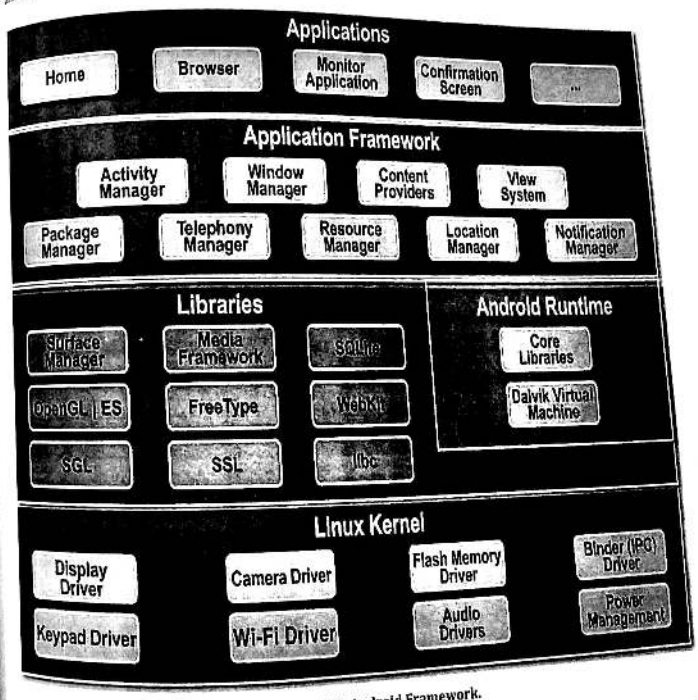


Figure 7.1: Android Framework.

I) **Linux kernel:**

- It is the **heart of android architecture** that exists at the root of android architecture.
- Linux kernel is responsible for device drivers, power management, memory management, device management and resource access.

II) **Native Libraries:**

- On the top of linux kernel, there are Native libraries such as WebKit, OpenGL, FreeType, SQLite, Media, C runtime library (libc) etc.
- The WebKit library is responsible for browser support, SQLite is for database, FreeType for font support, Media for playing and recording audio and video formats.

III) **Android Runtime:**

- In android runtime, there are **core libraries** and **DVM (Dalvik Virtual Machine)** which is responsible to run android application.
- DVM is like JVM but it is optimized for mobile devices.
- It consumes less memory and provides fast performance.

IV) **Android Framework:**

- On the top of Native libraries and android runtime, there is android framework.
- Android framework includes Android API's such as UI (User Interface), telephony, resources, locations, Content Providers (data) and package managers.
- It provides a lot of classes and interfaces for android application development.

V) **Applications:**

- On the top of android framework, there are applications.
- All applications such as home, contact, settings, games, browsers are using android framework that uses android runtime and libraries.
- Android runtime and native libraries are using linux kernel.

Q2] Android Components.

Ans: **[5M - May16] & [10M – May17]**

ANDROID:

1. Android is a mobile operating system developed by **Google.**
2. It is based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets.

ANDROID COMPONENTS:

There are four primary components of Android Application.

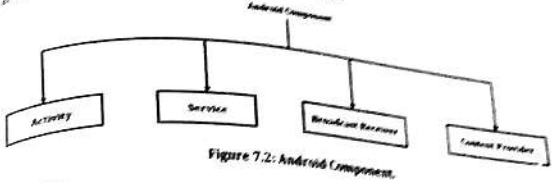


Figure 7.2: Android Component.

I) **Activity:**

- An activity represents a single screen with a user interface.
- An activity in android is like your computer welcome screen which presents single user display.
- For example, an email application may have one activity that demonstrates a rundown of new emails, another activity to form an email, and another activity for perusing/reading emails.

II) **Service:**

- A service component runs in background.
- A service component doesn't provide any user interface.
- For example, a service may play music out of sight while the client is in an alternate application.

III) **Broadcast Receiver:**

- The Android Broadcast Receivers are also known as **Communicate Receivers**.
- Broadcast Receivers is used to provide alerts/notifications.
- Broadcast Receiver doesn't provide any user interface.

IV) **Content Provider:**

- Content providers component supplies information from one application to others on solicitation/request.
- With Content Provider other applications can query and modify data, if permitted to do so.
- We can store data in SQLite, Web or any other persistent storage format.

Additional Components:

There are additional components which can be used in the construction of above components. They are:

1. Fragments.
2. Views & Layouts.
3. Intents & Resources.
4. Manifest.

Q3] Dalvik Virtual Machine (DVM) **[5M – Dec17]**

Ans:

DALVIK VIRTUAL MACHINE:

1. Java Virtual Machine (JVM) has **high performance** and provides excellent **memory management.**
2. But it needs to be optimized for low-powered handheld devices as well.
3. So Dalvik Virtual Machine is used.
4. The Dalvik Virtual Machine (DVM) is an android virtual machine **optimized for mobile devices.**
5. It optimizes the virtual machine for memory, battery life and performance.
6. Dalvik is a name of a town in Iceland.
7. The Dalvik VM was written by **Dan Bornstein.**
8. The role of Dalvik Virtual Machine is that, in java we write and compile java program using java compiler and run that bytecode on the java virtual machine.
9. On the other side, In android we still write and compile java source file (bytecode) on java compiler, but at that point we recompile it once again using dalvik compiler to dalvik bytecode (dx tool converts java .class file into .dex format)
10. This dalvik bytecode is then executed on the dalvik virtual machine.
11. So the Dex compiler converts the class files into the .dex file that run on the Dalvik VM.
12. Multiple class files are converted into one dex file.
13. Figure 7.3 shows compiling and packaging process from the source file.

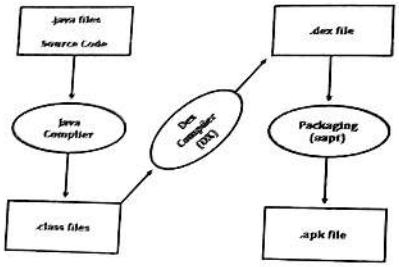


Figure 7.3: Compiling and packaging process.

14. The java compiler tool compiles the java source file into the class file.
15. The dx tool takes all the class files of your application and generates a single .dex file.
16. It is a **platform-specific tool.**
17. The Android Assets Packaging Tool (aapt) handles the packaging process.

CHAPTER - 8: SECURITY ISSUES IN MOBILE COMPUTING.

Q1] Explain Security issues in wireless communication, typically for cellular networks.

Q2] what are the security issues in Mobile Computing?

Q3] Security issues in mobile computing

Q4] Explain the various security issues involved in mobile computing

Ans: [Q1 | 10M – Dec15], [Q2 | 10M – May16], [Q3 | 10M – May17] & [Q4 | 10M – Dec17]

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:

General Security Issues:

Figure 8.1: General Security Issues.

I) **Confidentiality:** Confidentiality is ensuring that the information stored on the system or transmitted over communication links is accessed by only authorized users.

II) **Authentication:** Authentication ensures that the user accessing the information is the right person.

III) **Integrity:** Integrity ensures that the information exchanged between different parties is not altered or tampered during transmission.

IV) **Authorization:** Authorization ensures that the user has the right to access the information requested. It is giving different access to different types of users.

V) **Availability:** Availability ensures that the resources is available all the time for users.

VI) **Non-repudiation:** Non repudiation means the users cannot disavow about sending and receiving the message.

Wireless Security Issues:

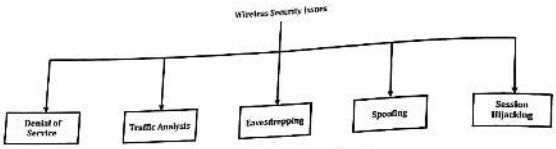


Figure 8.2: Wireless Security Issues.

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.

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:

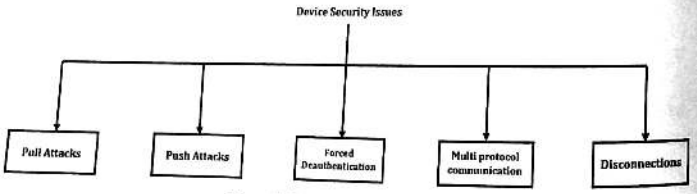


Figure 8.3: Device Security Issues.

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.**

Q5] What are the characteristics of SIM?

Ans: **[4M – May16 & Dec16]**

SIM:

1. SIM Stands for **Subscriber Identity Module.**
2. It is a smart card that is designed to fit into the mobile equipment.
3. It contains the identification of the subscriber i.e. **International Mobile Subscriber Identity (IMSI).**
4. It allows the users to send and receive calls and receive other subscribed services.

CHARACTERISTICS OF SIM:

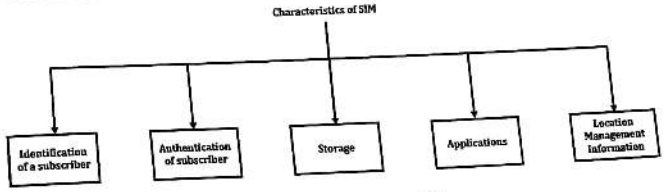


Figure 8.4: Characteristics of SIM.

I) **Identification of a subscriber:** SIM contains IMSI number that actually provides identity to a subscriber.

II) **Authentication of a subscriber:** SIM stores the information such as Authentication Algorithms, Authentication Key (K_i), Encryption Algorithm (K_c) etc. which are required to authenticate the user with a network.

III) **Storage:** It is used to store phone numbers and SMS.

IV) **Applications:** SIM Toolkit or GSM allows creating applications on the SIM to provide basic information on demand and other applications for E-commerce, Chatting, and Phonebook Backup etc.

V) **Location Management Information:** SIM uses **Temporary Mobile Subscriber Identity (TMSI)** number and **Location Area Identification (LAI)** for Location Management.

Q6] Digital Signature. **[5M – May16]**

Ans:

DIGITAL SIGNATURE:

1. Digital Signature is a type of **electronic signature.**
2. It encrypts documents with **digital codes** that are particularly difficult to duplicate.
3. A digital signature takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint."
4. It is used to validate the authenticity and integrity of a message, software or digital document.
5. Figure 8.5 shows the processes of Digital Signature.

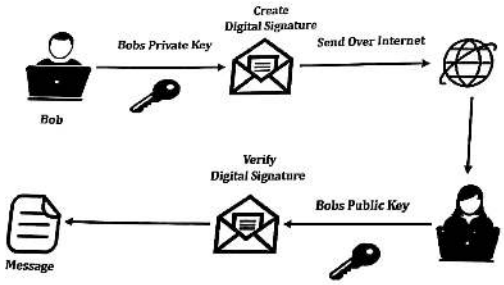


Figure 8.5: Digital Signature Process.

APPLICATIONS:

- Used in E-Procurement.
- Used in Banks & Financial Institute.
- Online Income Tax form filling.
- Online Railway Ticket Booking.

Q7] Digital Certificate. **[5M – Dec16]**

Ans:

DIGITAL CERTIFICATE:

1. It is also known as **Public Key Certificate.**
2. A Digital Certificate is a **digital file** that certifies the identity of an individual or institution.
3. It is issued by a **Certificate Authority.**
4. It is a form of an electronic credential for the internet.
5. It is standardized by X.509.
6. Figure 8.6 represents Digital Certificate.

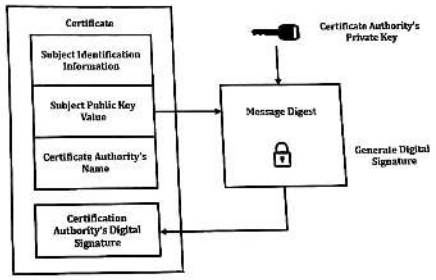


Figure 8.6: Digital Certificate.

The digital Certificate Contains:

- The Digital Signature.
- The name of person owning the public key.
- Public Key.