

ASSIGNMENT-2

1. Explain EM (Electro-Magnetic) waves, its properties and effects of environments on EM waves. Explain different modes of propagation in detail.

Ans. **Electromagnetic Waves** also called Electromagnetic Radiations are basically defined as superimposed oscillations of an Electric and a Magnetic Field in space with their direction of propagation perpendicular to both of them. In simple words, electromagnetic waves are oscillations produced due to crossing over of an electric and a magnetic field. The direction of the propagation of such waves is perpendicular to the direction of the force of either of these fields as seen in the above figure. Like all waveforms, these have some properties as well.

Properties of electromagnetic wave propagation:

- These waves travel at the speed of light.
- These waves do not require any medium for propagation.
- Electromagnetic waves travel in a transverse form.
- Electromagnetic waves are not deflected by electric or magnetic field.
- These waves can be polarized.
- Electromagnetic Waves undergo interference and diffraction.

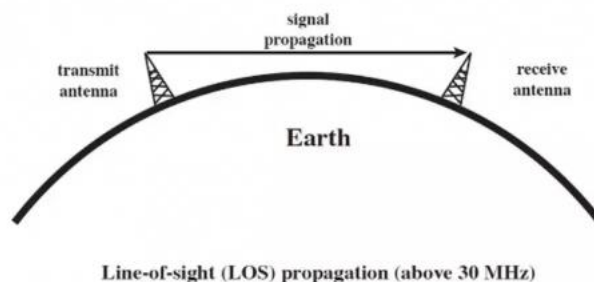
Effects on environment:

- Animals such as birds, bats are strongly dependent on magnetic fields orientation.
- Animals such as sharks and rays that possess electric sense organs.

The **mode of propagation** of electromagnetic waves in the atmosphere and in free space may be divided into the following three categories:

- The line of sight (LOS) propagation:

Among the modes of propagation, this line-of-sight propagation is the one, which we would have commonly noticed. In the line-of-sight communication, as the name implies, the wave travels a minimum distance of sight. Which means it travels to the distance up to which a naked eye can see. Then we need to employ an amplifier cum transmitter here to amplify the signal and transmit again.



The line-of-sight propagation will not be smooth if there occurs any obstacle in its transmission path. As the signal can travel only to lesser distances in this mode, this transmission is used for infrared or microwave transmissions.

- Ground wave propagation

Ground wave propagation of the wave follows the contour of the earth. Such a wave is called a direct wave. The wave sometimes bends due to the Earth's magnetic field and gets reflected the receiver. Such a wave can be termed as a reflected wave. The following figure depicts ground wave propagation.

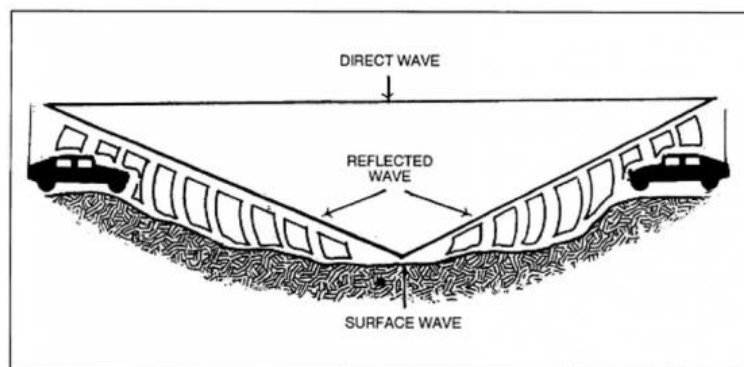
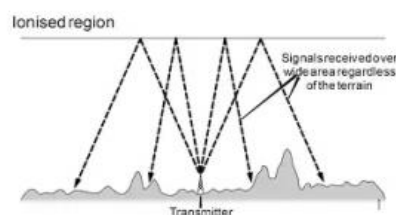


Figure Components of ground wave.

The wave then propagates through the Earth's atmosphere is known as a ground wave. The direct wave and reflected wave together contribute the signal at the receiver station. When the wave finally reaches the receiver, the lags are cancelled out. In addition, the signal is filtered to avoid distortion and amplified for clear output.

- Skywave propagation

Skywave propagation is preferred when the wave has to travel a longer distance. Here the wave is projected onto the sky and it is again reflected back to the earth.



The sky wave propagation is well depicted in the above picture. Here the waves are shown to be transmitted from one place and where it is received by many receivers. Hence, it is an example of broadcasting. The waves, which are transmitted from the transmitter antenna, are reflected from the ionosphere. It consists of several layers of charged particles ranging in altitude from 30-250 miles above the surface of the earth.



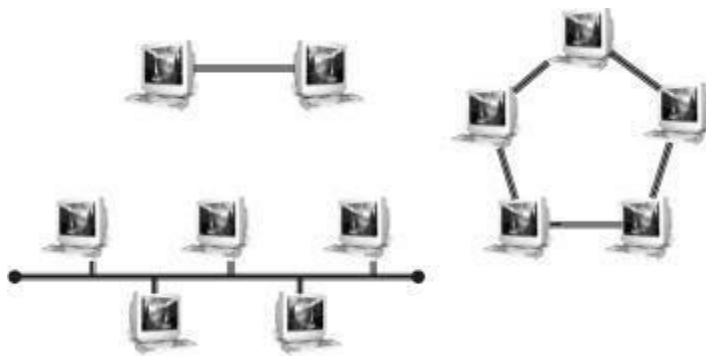
Such travel of the wave from the transmitter to the ionosphere and from there to the receiver on Earth is known as Sky Wave Propagation. The ionosphere is the ionized layer around the Earth's atmosphere, which is suitable for skywave propagation.

2. Explain physical & logical architecture of wireless network. What are essential functional differences between 1st Generation, 2nd Generation, 3rd Generation and 4th Generation of networks?

Ans. **Physical architecture:**

The topology of a wired network refers to the physical configuration of links between networked devices or nodes, where each node may be a computer, an end-user device such as a printer or scanner, or some other piece of network hardware such as a hub, switch or router.

The building block from which different topologies are constructed is the simple point-to-point wired link between two nodes, shown in Figure



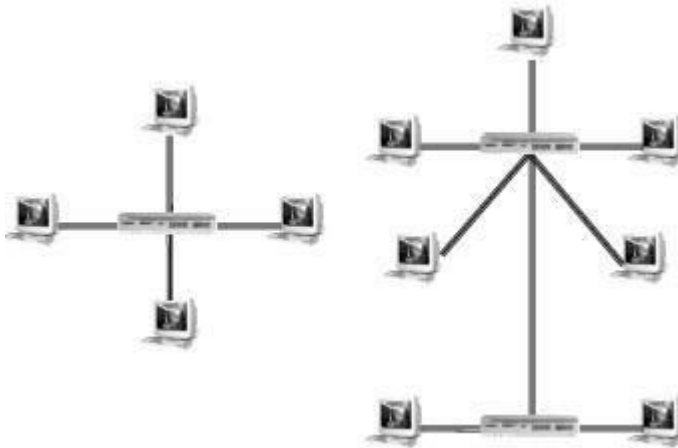
For the ring topology, there are two possible variants depending on whether the inter-node links are simplex (one-way) or duplex (two-way). Repeating this element results in the two simplest topologies for wired networks — bus and ring.

In the simplex case, each inter-node link has a transmitter at one end and a receiver at the other, and messages circulate in one direction around the ring, while in the duplex case each link has both transmitter and receiver (a so-called transceiver) at each end, and messages can circulate in either direction.

Bus and ring topologies are susceptible to single-point failures, where a single broken link can isolate sections of a bus network or halt all traffic in the case of a ring. The step that opens up new possibilities is the introduction of specialised network hardware nodes designed to control the flow of data between other networked devices.

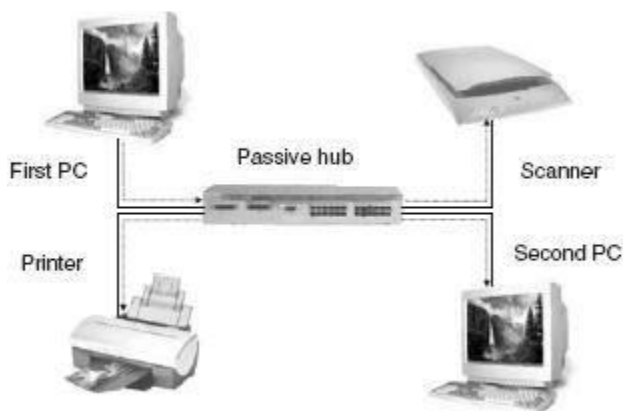
The simplest of these is the passive hub, which is the central connection point for LAN cabling in star and tree topologies, as shown in Figure 2.





An active hub, also known as a repeater, is a variety of passive hub that also amplifies the data signal to improve signal strength over long network connections. For some PAN technologies, such as USB, star and tree topologies can be built without the need for specialised hardware, because of the daisy-chaining capability of individual devices.

An active or passive hub in a star topology LAN transmits every received data packet to every connected device. Each device checks every packet and decodes those identified by the device's MAC address. The disadvantage of this arrangement is that the bandwidth of the network is shared among all devices, as shown in Figure 3.



Logical architecture:

The logical architecture of a network refers to the structure of standards and protocols that enable connections to be established between physical devices, or nodes, and which control the routing and flow of data between these nodes.

Since logical connections operate over physical links, the logical and physical architectures rely on each other, but the two also have a high degree of independence, as the physical configuration of a network can be changed without changing its logical architecture, and the same physical network can in many cases support different sets of standards and protocols.



The OSI Network Model

The Open Systems Interconnect (OSI) model was developed by the International Standards Organisation (ISO) to provide a guideline for the development of standards for interconnecting computing devices.

The OSI model is a framework for developing these standards rather than a standard itself — the task of networking is too complex to be handled by a single standard. The OSI model breaks down device to device connection, or more correctly application to application connection, into seven so-called “layers” of logically related tasks.

1. **Physical layer** - Standards to control transmission of the data stream over a particular medium, at the level of coding and modulation methods, voltages, signal durations and frequencies.
2. **Data link layer** - Standards to specify the way in which devices access and share the transmission medium (known as Media Access Control or MAC) and to ensure reliability of the physical connection (known as Logical Link Control or LLC).
3. **Network layer** - Standards to define the management of network connections — routing, relaying and terminating connections between nodes in the network.
4. **Transport layer** - Standards to ensure reliable completion of data transfers, covering error recovery, data flow control, etc. Makes sure all data packets have arrived.
5. **Session layer** - Standards to manage the communication between the presentation layers of the sending and receiving computers. This communication is achieved by establishing, managing and terminating “sessions”.
6. **Presentation layer** - Standards to control the translation of incoming and outgoing data from one presentation format to another.
7. **Application layer** - Standards to define the provision of services to applications — such as checking resource availability, authenticating users, etc.

Differences between 1st Generation, 2nd Generation, 3rd Generation and 4th Generation of networks

	1G	2G	3G	4G	5G
Bandwidth	150/900MHz	900MHz	100MHz	100MHz	1000x BW pr unit area
Frequency	Analog signal (30 KHz)	1.8GHz (digital)	1.6 – 2.0 GHz	2 – 8 GHz	3 – 300 GHz
Data rate	2kbps	64kbps	144kbps – 2Mbps	100Mbps – 1Gbps	1Gbps <
Characteristic	First wireless communication	Digital	Digital broadband, increased speed	High speed, all IP	
Technology	Analog cellular	Digital cellular (GSM)	CDMA, UMTS, EDGE	LTE, WiFi	WWWW



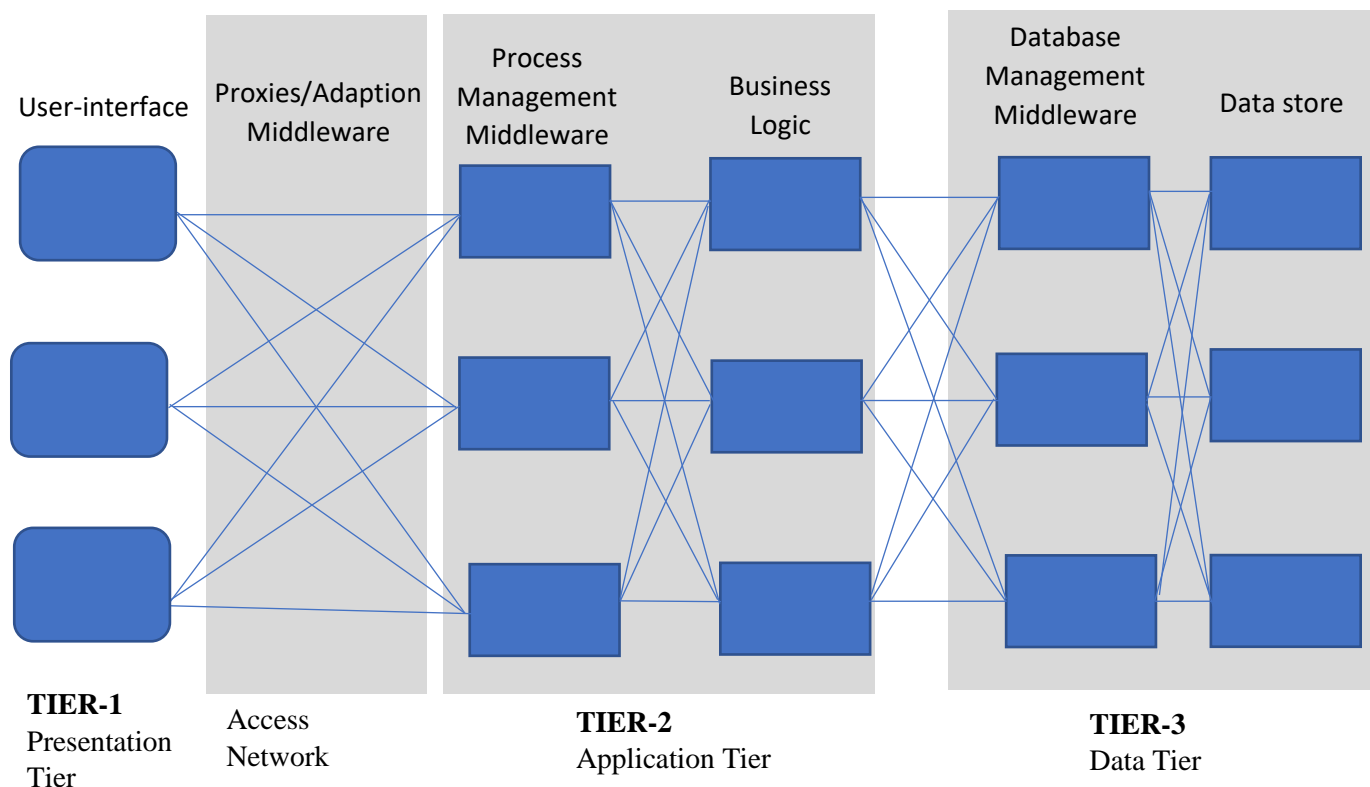
Access system	FDMA	TDMA/CDM A	CDMA	CDMa	OFDM/BDM A
Core network	PSTN	PSTN	Packet network	Internet	Internet

3. Define Mobile Computing and Communication. Explain why mobile computing is more popular? Draw and explain 3-tier architecture for mobile computing. Write different applications of mobile computing, its benefits and challenging technical issues. Also discuss design consideration of mobile computing.

Ans. **Mobile computing** is human–computer interaction in which a computer is expected to be transported during normal usage, which allows for transmission of data, voice and video.

Mobile Communication is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables). Mobile communication makes our life easier, and it saves time and effort.

3-tier architecture for mobile computing:



A 3-tier architecture is an application program that is organized into three major parts, comprising of:

- The data access layer tier at the bottom,
- The application tier (business logic) in the middle and
- The client tier (presentation) at the top.



Each tier is distributed to a different place or places in a network. These tiers do not necessarily correspond to physical locations on various computers on a network, but rather to logical layers of the application.

1. Presentation Layer (UI):

- This layer presents data to the user and optionally permits data manipulation and data entry, also this layer requests the data from Business layer.
- This layer accomplished through use of Dynamic HTML and client-side data sources and data cursors.

2. Business Logic Layer:

- The business logic acts as the server for client requests from workstations. It acts according Business rules fetch or insert data through the Data Layer.
- In turn, it determines what data is needed (and where it is located) and acts as a client in relation to a third tier of programming that might be located on a local or mainframe computer.
- Because these middle-tier components are not tied to a specific client, they can be used by all applications and can be moved to different locations, as response time and other rules require.

3. Data Access Layer:

- The third tier of the 3-tier system is made up of the DBMS that provides all the data for the above two layers.
- This is the actual DBMS access layer.
- Avoiding dependencies on the storage mechanisms allows for updates or changes without the application tier clients being affected by or even aware of the change.

Different applications of mobile computing

- Banking
- Education
- Industries
- Entertainments
- Hospitals
- Data processing

Its benefits:

- Increase productivity
- Entertainment.
- Probability
- Cloud Computing

Challenging technical issues



- Battery consumption hindrance
- Interference is persisted in shielding.
- Inefficient bandwidth in transmission.
- Connection losses over entire network.
- Network stability.
- Interoperability problem.
- Protection constraints.

4. What is active RFID? Describe two applications of RFID. How is active RFID different from passive RFID? Describe two applications of passive RFID.

Ans. Active RFID(Radio-Frequency Identification) is an on-board power source is used to for operating tags. It may be a battery or a cell, for example, enabling both tag performance and data transmission. Active RFID is commonly used for real time location tracking.

Applications of active RFID:

- Timing marathons and races are one of the most popular uses of RFID.
- Certain areas requires an expected level of security and access. From doors to parking lots RFID access control tags restrict access to only those pre-approved.

Difference:

- The primary difference between active and passive tags is that active tags have their own power source and passive tags rely on the RFID reader's propagation signal to power the tag.

Applications of passive RFID:

- Tracking inventory
- Access control
- Brand protection in manufacturing, wholesale and retail sectors.

5. What is a LMP? List three security services under LMP.

Ans. **Link Management Protocol (LMP)** is designed to ease the configuration and management of optical network devices. Such devices may be interconnected by thousands of data-bearing links, which are aggregated into a smaller number of traffic engineering (TE) links. LMP provides automatic configuration of such devices, negotiation of capabilities, and localization of faults.

Security services under LMP:

- Authentication
- Confidentiality
- Authorisation



6. What is Bluetooth? List functions of Bluetooth. State the modes possible when the slave is in connection state in Bluetooth. Differentiate piconet and scatternet in Bluetooth technology.

Ans. **Bluetooth** wireless technology features low-bandwidth, short-range connection between two devices enabled to receive the data. The structure behind this technology is complicated, and the extent of operation is implementation specific.

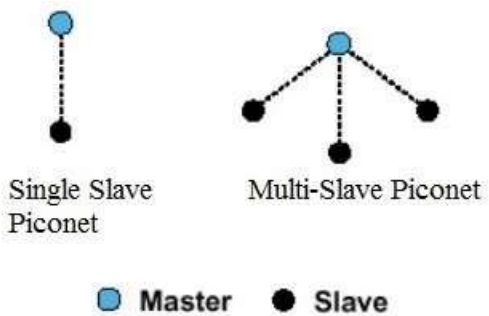
Functions of Bluetooth:

- Bluetooth Tethering
- Transfer Files Between Two Devices
- Play Multiplayer Games Over Bluetooth
- Connect Different Devices
- Control Home Security Gadgets
- Connect Different Devices

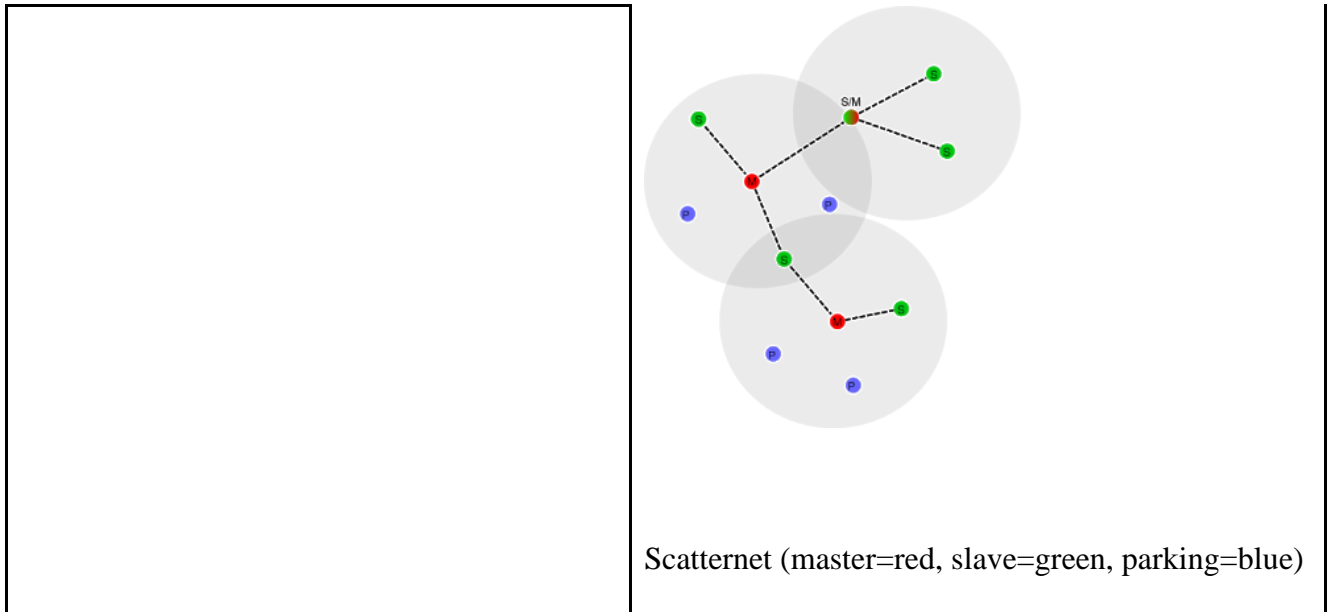
The modes possible when the slave is in connection state in Bluetooth:

- **SNIFF mode:** In this a slave device listens to the piconet at a reduced rate, thus reducing its duty cycle. The SNIFF interval is programmable and depends on the application.
- **PARK mode:** In this a device is still synchronized to the piconet but does not participate in the traffic.

Difference between piconet and scatternet in Bluetooth technology

Piconet	Scatternet
In this bluetooth network, device can function either as master or slave.	In this bluetooth network, device can function as master or slave or (master+slave)
It serves smaller coverage area.	It serves larger coverage area.
It supports maximum 8 nodes.	It supports more than 8 nodes.
It allows less efficient use of available bluetooth channel bandwidth.	It allows more efficient use of available bluetooth channel bandwidth.
 <p>Single Slave Piconet Multi-Slave Piconet</p> <p>● Master ● Slave</p>	





7. What is known as ad hoc network topology? State the uses of mobile ad hoc networks. Compare ad hoc and infrastructure network topologies.

Ans. **Ad hoc network** is also known as IBSS (Independent Basic Service Set) configuration. Ad hoc WLANs include a number of nodes or wireless stations that communicate directly with one another on a peer-to-peer basis, without using an access point (AP) or any connection to a wired network.

The uses of mobile ad hoc networks:

- Router Free
- Mobility
- Speed

Compare ad hoc and infrastructure network topologies:

	Infrastructure	Ad hoc
Characteristics		
Communication	Through an access point	Directly between devices
Security	More security options	WEP or no security
Range	Determined by the range and number of access points	Restricted to the range of individual devices on the network
Speed	Usually faster	Usually slower
Requirements for all devices		
Unique IP address for each device	Yes	Yes



	Infrastructure	Ad hoc
Mode set to	Infrastructure mode	Ad hoc mode
Same SSID	Yes, including the access point	Yes
Same channel	Yes, including the access point	Yes

8.How does a MN identify that it has moved? What are the contents of mobility binding? Define encapsulation and care of address.

Ans. Each mobile node is identified by its home address disregarding its current location in network.

- While away from its home network, a mobile node is associated with a care of address which identifies its current location and its home address is associated with local endpoint of a tunnel to its home agent.
- Encapsulation: It is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.
- Care-of-address: It is a temporary IP address for a mobile device. This allows a home agent to forward messages to mobile device.

9.State any 4 features of IPv6.

Ans.

- **Larger Address Space**

In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×10^{38} different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

- **Simplified Header**

IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 provided the fact that IPv6 address is four times longer.

- **End-to-end Connectivity**

Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

- **Auto-configuration**

IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.



10. What is DHCP? What is the functionality of it?

Ans. Dynamic Host Configuration Protocol (**DHCP**) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP.

Functionality:

A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired.

11. Differentiate FDMA, TDMA and SDMA.

	SDMA	TDMA	FDMA
Idea	Segment spaced into cells or sectors.	Segments sending time into disjoint time slots demand driven or fixed patterns.	Segment the frequency band into disjoint sub-bands.
Signal Separation	Cell structure, directed antennas.	Synchronization in time domain.	Filtering in the frequency domain.
Cell Capacity	Depends on the cell area.	Limited	Limited
Terminals	Only one terminal can be active in one cell or one sector.	All terminals are active for short periods of time on same frequency.	Every terminal has its own frequency uninterrupted.
Transmission Scheme	Continuous	Discontinuous	Continuous
Advantages	Very simple & increases performance capacity.	Flexible & established fully digital.	Simple, established, robust.
Disadvantages	It is inflexible as antennas are typically fixed.	Guard space needed (multipath propagation), synchronization difficulty.	Inflexible, frequencies are a scarce resource.
Note	Only useful in combination with TDMA, FDMA or CDMA.	It is a standard in fixed networks. Also together with FDMA or SDMA used in many mobile networks.	Typically combined with TDMA and SDMA.

12. Explain DSSS and FHSS with example.



Ans. **DSSS:** DSSS, direct sequence spread spectrum is a form of spread spectrum transmission which uses spreading codes to spread the signal out over a wider bandwidth than would normally be required. The technique behind direct sequence spread spectrum, DSSS is at first sight counter-intuitive, but DSSS is used in a number of areas where it enables considerable benefits to be gained.

The first part of the process is to generate the DSSS signal. Take as an example that the data to be transmitted is 1001, and the chip or spreading code is 0010. For each data bit, the complete spreading code is used to multiple the data, and in this way, for each data bits, the spread or expanded signal consists of four bits.

1	0	0	1	Data to be transmitted
0010	0010	0010	0010	Chip or spreading code
1101	0010	0010	1101	Resultant spread data output

With the signal obtained and transmitted, it needs to be decoded within the remote receiver:

1101	0010	0010	1101	Incoming CDMA signal
0010	0010	0010	0010	Chip or spreading code
1111	0000	0000	1111	Result of de-spreading
1	0	0	1	Integrated output

NB: $1 \times 1 = 0$ $1 \times 0 = 1$

In this way it can be seen that the original data is recovered exactly by using the same spreading or chip code. Had another code been used to regenerate the CDMA spread spectrum signal, then it would have resulted in a random sequence after de-spreading. This would have appeared as noise in the system.

The spreading code used in this example was only four bits long. This enabled the process to be visualised more easily. Commonly spreading codes may be 64 bits, or even 128 bits long to provide the required performance.

FHSS:

This is frequency hopping technique, where users are made to change the frequency of usage, from one to another in a specified time interval, hence called as frequency hopping. For example, a frequency was allotted to sender-1 for a particular period of time. Now after a while, sender-1 hops to the other frequency and sender-2 uses the first frequency, which was previously used by sender-1. This is called as frequency reuse. The frequencies of the data are hopped from one to another in order to provide a secure transmission. The amount of time spent on each frequency hop is called as dwell time.

13. What is meant by GEO? Compare GEO and LEO.



Ans. Geosynchronous Equatorial Orbit, also known as Geostationary satellites. These satellites are called Geostationary because they appear fixed as they move at the same angular velocity as the Earth and orbit along a path parallel to Earth's rotation, providing coverage to a specific area. From the ground, GEO satellites appear to be well stationary. At about 35,000 kilometres (22,000 miles) above the Earth's surface, this type of orbit was first used in 1964 for NASA's Syncom III, an experimental satellite for communications aboard the Delta-D rocket. Unfortunately, due to the curvature of the Earth, a geostationary satellite cannot provide continuous service above or below approximately ± 70 degrees latitude.

Orbits	LEO	GEO
Orbital period	1.5 to 2 h	24 h
Altitude range	500 to 1500 km	35,863 km
Visibility duration	15 to 20 min/pass	Permanent
Elevation	Rapid variations , high and low angles	No variations, low angles at high latitudes
Round-trip propagation delay	Several milliseconds	≈ 250 ms
Instantaneous ground coverage (diameter at 10deg elevation)	≈ 6000 km	16,000km
examples	Iridium, globalstar, teledesic, skybridge, orbcomm	Intelsat, interspoutnik, Inmarsat

14. What is WiMax (Wireless Broadband)? How is it different from WiFi? Explain the WiMax Physical layer.

Ans. WiMAX is

- Acronym for **Worldwide Interoperability for Microwave Access**.
- Based on Wireless MAN technology.
- A wireless technology optimized for the delivery of IP centric services over a wide area.
- A scalable wireless platform for constructing alternative and complementary broadband networks.
- A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. The IEEE 802.16 Working Group develops standards that address two types of usage models –
 - A fixed usage model (IEEE 802.16-2004).
 - A portable usage model (IEEE 802.16e).

Different from WiFi:

WiFi uses Radio waves to create wireless high-speed internet and network connections. A wireless adapter is needed to create hotspots. **WiMax** uses spectrum to deliver connection to network and handle a larger inter-operable network.

WiMax Physical layer:

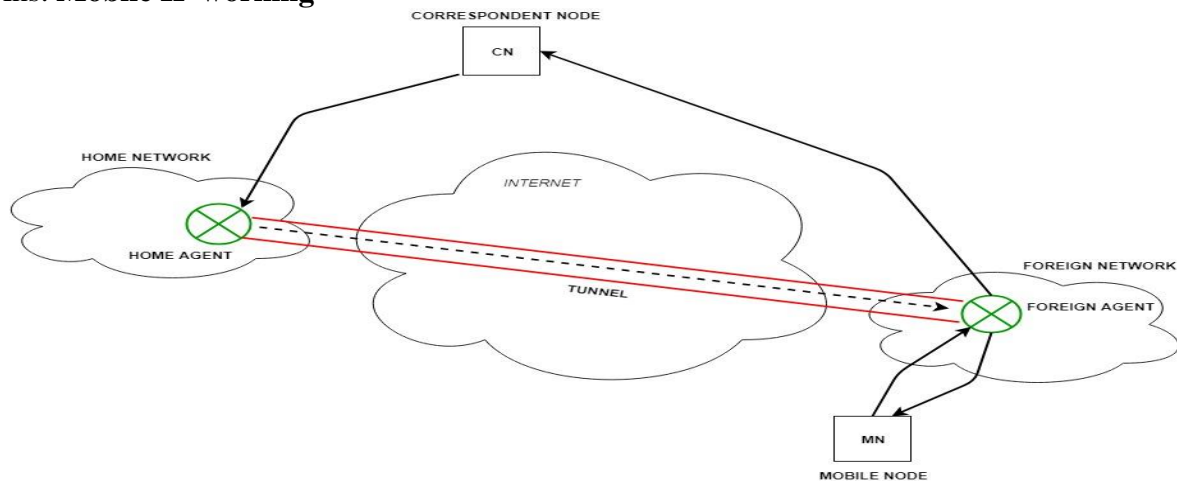


The WiMAX physical layer is based on orthogonal frequency division multiplexing. OFDM is the transmission scheme of choice to enable high-speed data, video, and multimedia communications and is used by a variety of commercial broadband systems, including DSL, Wi-Fi, Digital Video Broadcast-Handheld (DVB-H), and MediaFLO, besides WiMAX.

OFDM is an elegant and efficient scheme for high data rate transmission in a non-line-of-sight or multipath radio environment.

15. How does Mobile IP work? What are the challenges with mobile IP with respect to high speed mobility? Explain advertisement and registration with respect to Mobile IP.

Ans. **Mobile IP working**



Correspondent node sends the data to the mobile node. Data packets contains correspondent node's address (Source) and home address (Destination). Packets reaches to the home agent. But now mobile node is not in the home network, it has moved into the foreign network. Foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunnelling.

Tunnelling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

Now, home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address and sends it through the tunnel to the foreign agent. Foreign agent, on other side of the tunnel receives the data packets, decapsulates them and sends them to the mobile node. Mobile node in response to the data packets received, sends a reply in response to foreign agent. Foreign agent directly sends the reply to the correspondent node.

Challenges with mobile IP with respect to high speed mobility

(1) "Triangle routing" Problem

The Communication Host (CH) has to send packets to the Mobile Host (MH) via the Home



Agent (HA), while the MH sends packets directly to the CH. As the communication in the two directions follows different routes, the problem of "triangle routing" arises, which leads to low efficiency especially when the MH is far away from the HA and the CH is near to the MH.

(2) Handoff Problem

Handoff problem means that the HA sends the IP packets of the MH to the original foreign network via the tunnel because it doesn't know the latest Care of Address (CoA) of the MH during the period starting when the MH leaves the original foreign network and ending when the HA receives the new registration address of the MH. As a result, these dropped IP packets have an influence on the communication between the MH and the CH especially when handoff occurs frequently or the MH is far away from the HA.

(3) Problem of Intra-Domain Movement

The frequent intra-domain movement of the MH within a small area will lead to frequent handoff. Consequently, a great number of registered messages are generated in the network and the network performance is greatly affected.

(4) QoS Problem

In the mobile environment, it is hard to provide QoS over Mobile IP due to dynamically varying wireless network topologies, limited network resources, unpredictable effective bandwidth and high error rate.

Advertisement and registration with respect to Mobile IP

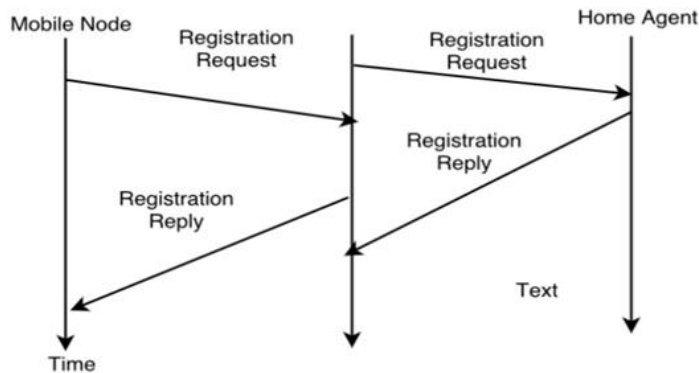
Advertisement: Mobile nodes use agent advertisements to determine their current point of attachment to the Internet or to an organization's network. An agent advertisement is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension.

A foreign agent can be too busy to serve additional mobile nodes. However, a foreign agent must continue to send agent advertisements. This way, mobile nodes that are already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed.

Also, a foreign agent that supports reverse tunnels must send its advertisements with the reverse tunnel flag set on.

Registration: The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.





Registration can be done in two ways depending on the location of the COA.

- **If the COA is at the FA**, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a **mobility binding** containing the mobile node's home IP address and the current COA.

Additionally, the mobility binding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so a mobile node should register before expiration. After setting up the mobility binding, the HA send a reply message back to the FA which forwards it to the MN.

- **If the COA is co-located**, registration can be very simpler. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

16. Discuss Limitation of Traditional/Classical TCP in case of wireless communication.

Ans. **Limitation:**

- Slow Start mechanism in fixed networks decreases the efficiency of TCP if used with mobile receivers or senders.
- Error rates on wireless links are orders of magnitude higher compared to fixed fiber or copper links. This makes compensation for packet loss by TCP quite difficult.
- Mobility itself can cause packet loss. There are many situations where a soft handover from one access point to another is not possible for a mobile end-system.
- Standard TCP reacts with slow start if acknowledgements are missing, which does not help in the case of transmission errors over wireless links and which does not really help during handover. This behaviour results in a severe performance degradation of an unchanged TCP if used together with wireless links or mobile nodes

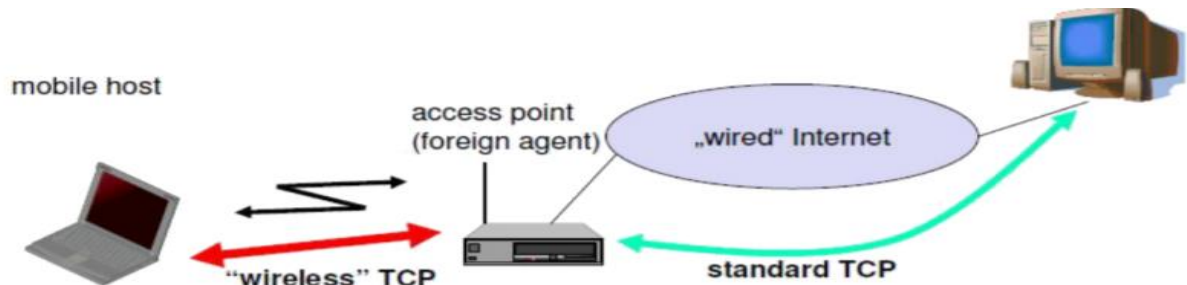
17. Explain Indirect-TCP, Snooping-TCP and Mobile-TCP with its advantage & disadvantage.

Ans. **Indirect-TCP**

Indirect TCP or I-TCP segments the connection



- no changes to the TCP protocol for hosts connected to the wired Internet, millions of computers use (variants of) this protocol
- optimized TCP protocol for mobile hosts
- splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
- hosts in the fixed part of the net do not notice the characteristics of the wireless part

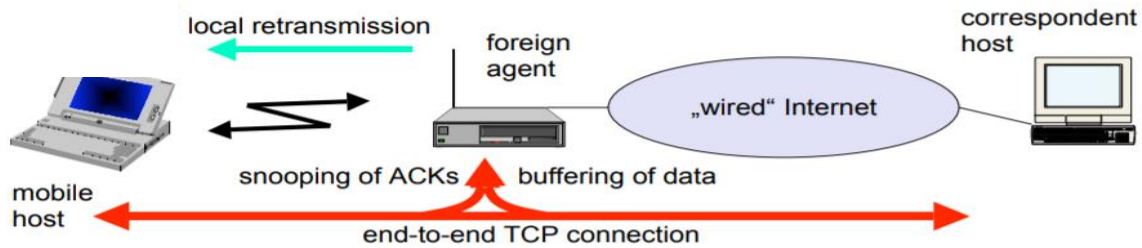


- Advantages of I-TCP
 - No changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
 - Simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
 1. transmission errors on the wireless link do not propagate into the fixed network
 2. therefore, a very fast retransmission of packets is possible, the short delay on the mobile hops known
 - It is always dangerous to introduce new mechanisms in a huge network without knowing exactly how they behave.
 - New optimizations can be tested at the last hop, without jeopardizing the stability of the Internet. It is easy to use different protocols for wired and wireless networks.
- Disadvantages of I-TCP
 - Loss of end-to-end semantics: - an acknowledgement to a sender no longer means that a receiver really has received a packet, foreign agents might crash.
 - Higher latency possible: - due to buffering of data within the foreign agent and forwarding to a new foreign agent
 - Security issue: - The foreign agent must be a trusted entity

Snooping-TCP

- Transparent extension of TCP within the foreign agent
- buffering of packets sent to the mobile host
- lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called "local" retransmission)
- the foreign agent therefore "snoops" the packet flow and recognizes acknowledgements in both directions, it also filters ACKs
- changes of TCP only within the foreign agent (+min. MH change)





- Data transfer to the mobile host
 - FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
 - fast retransmission possible, transparent for the fixed network
- Data transfer from the mobile host
 - FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
 - MH can now retransmit data with only a very short delay
- Advantages:
 - Maintain end-to-end semantics
 - No change to correspondent node
 - No major state transfer during handover
- Disadvantages:
 - Snooping TCP does not isolate the wireless link well
 - May need change to MH to handle NACKs
 - Snooping might be useless depending on encryption schemes

Mobile TCP:

- Special handling of lengthy and/or frequent disconnections
- M-TCP splits as I-TCP does
 - unmodified TCP fixed network to supervisory host (SH)
 - optimized TCP SH to MH
- Supervisory host
 - no caching, no retransmission
 - monitors all packets, if disconnection detected
 - set sender window size to 0
 - sender automatically goes into persistent mode
 - old or new SH reopen the window
- Advantages
 - maintains semantics,
 - supports disconnection,
 - no buffer forwarding
- Disadvantages
 - loss on wireless link propagated into fixed network
 - adapted TCP on wireless link

