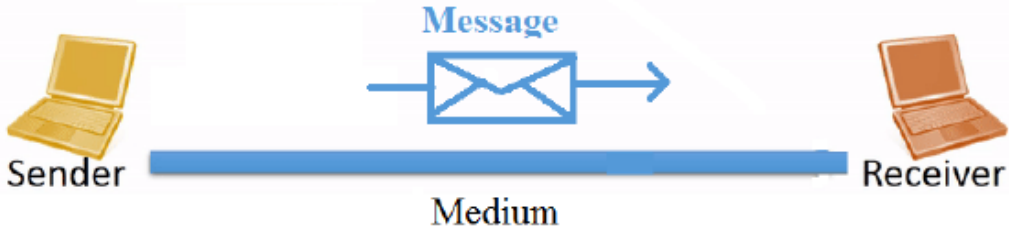


**Chapter 1: Fundamentals of Data Communication and Computer Networks**

<b>Q.1</b>	<b>Draw and explain block diagram of communication system.</b>
<b>Ans.</b>	<div><p>Sender <span style="margin-left: 150px;">Medium</span> Receiver</p></div> <p>Considering the communication between two computers , the communication system is as shown in above diagram</p> <p><b>It has following five components:</b></p> <ol style="list-style-type: none"><li>1. Message</li><li>2. Sender</li><li>3. Medium</li><li>4. Receiver</li><li>5. Protocol</li></ol> <p><b>Message:</b></p> <ul style="list-style-type: none"><li>• Message is the information or data which is to be sent from sender to the receiver</li><li>• A message can be in the form of sound, text, picture, video or combination of them(multimedia)</li></ul> <p><b>Sender:</b></p> <ul style="list-style-type: none"><li>• Sender is device such as host, camera, workstation, telephone etc. which sends the message over medium</li></ul> <p><b>Medium:</b></p> <ul style="list-style-type: none"><li>• The message originated from sender needs a path over which it can travel to the receiver. Such path is called as medium or channel</li></ul> <p><b>Receiver:</b></p> <ul style="list-style-type: none"><li>• It is the device which receives the message and reproduces it. A receiver can be host, camera, workstation, telephone etc.</li></ul> <p><b>Protocol:</b></p> <ul style="list-style-type: none"><li>• A protocol is defined as set of rules agreed by sender and receiver. Protocol governs the exchange of data in true sense.</li></ul>

<b>Q.2</b>	<b>Define Computer Network and state its types.</b>
<b>Ans.</b>	<p>Definition:</p> <p>A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource sharing among a wide range of users.</p> <p>Types of Computer Networks:</p> <ul style="list-style-type: none"><li>• Local Area Networks (LAN)</li><li>• Personal Area Networks (PAN)</li><li>• Home Area Networks (HAN)</li><li>• Wide Area Networks (WAN)</li><li>• Metropolitan Area Networks (MAN)</li><li>• The Internet</li></ul>
<b>Q.3</b>	<b>State various Computer Network applications</b>
<b>Ans</b>	<p>Computer Network Applications:</p> <ol style="list-style-type: none"><li>1. File Sharing</li><li>2. Printer Sharing</li><li>3. Application Services</li><li>4. E-mail Services</li><li>5. Remote access</li><li>6. Internet &amp; Intranet</li></ol>
<b>Q.4</b>	<b>Classify the network based on geographical area and transmission technology</b>
<b>Ans</b>	<p><b>Classification of networks based on geography:</b></p> <p>LAN - Local Area Network MAN - Metropolitan Area Network WAN - Wide Area Network CAN - Campus Area Network PAN - Personal Area Network</p> <p><b>LAN:</b> LAN is local area network. LAN is privately-owned networks covering a small geographic area(less than 1 km), like a home, office, building or group of buildings. LAN transmits data with a speed of several megabits per second.</p> <p><b>MAN:</b> A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area or campus. 2. A MAN typically covers an area up to 10 kms (city). The best example of MAN is the cable Television network, available in many cities.</p>

**WAN:** WAN is wide area network. WAN is a long-distance communication network that covers a wide geographic area, such as state or country. The most common example is internet.

**The transmission technology can be categorized broadly into two types:**

### 1. Broadcast Networks

Broadcast networks have a single communication channel that is shared or used by all the machines on the network. Short messages called packets sent by any machine are received by all the others. Broadcast systems generally use a special code in the address field for addressing a packet to all the concerned computers. This mode of operation is called broadcasting.

### 2. Point-to-Point Networks

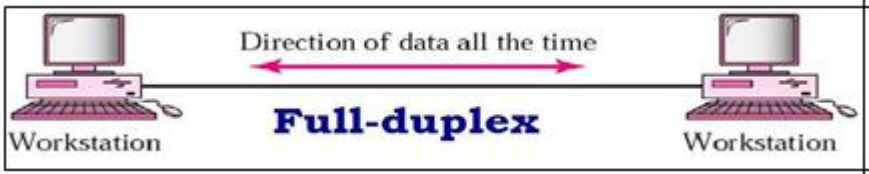
Point to point networks consists of many connections between individual pairs of machines. To go from the source to the destination a packet on these types of network may have to go through intermediate computers before they reach the desired computer.

## Q.5 Compare Analog and Digital signal

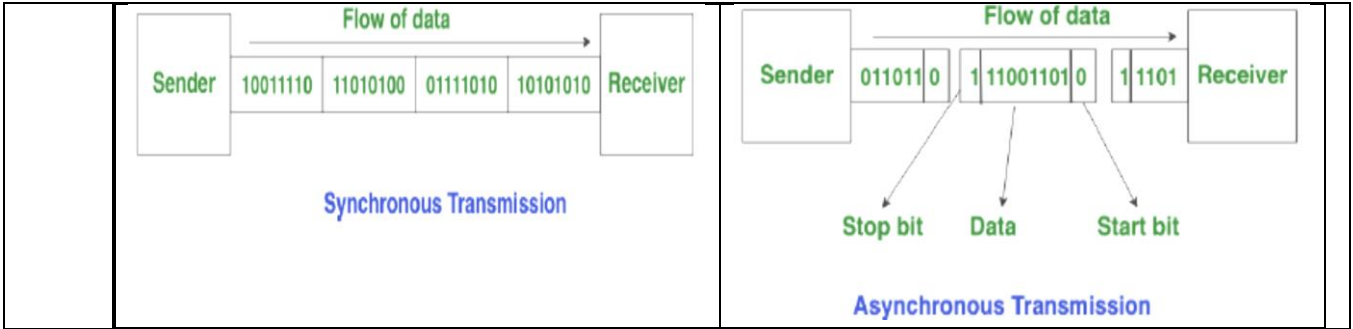
**Ans**

<b>Analog signal</b>	<b>Digital signal</b>
An analog signal is a continuous wave that changes over a time period.	A digital signal is a discrete wave that carries information in binary form.
An analog signal is represented by a sine wave.	A digital signal is represented by square waves.
Analog signal has no fixed range.	Digital signal has a finite numbers i.e. 0 and 1.
An analog signal is described by the amplitude, period or frequency, and phase.	A digital signal is described by bit rate and bit intervals.
An analog signal is more prone to distortion.	A digital signal is less prone to distortion.
An analog signal transmits data in the form of a wave.	A digital signal carries data in the binary form i.e. 0 and 1.

<b>Q. 6</b>	<b>Describe the process of data communication in various modes</b>
<b>Ans</b>	<p>Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called Communication Mode. These modes direct the direction of flow of information. There are three types of transmission modes.</p> <p>They are:</p> <ul style="list-style-type: none"> <li>• Simplex Mode</li> <li>• Half duplex Mode</li> <li>• Full duplex Mode</li> </ul> <p>a. In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.</p> <p>-Keyboards, traditional monitors and printers are examples of simplex devices.</p> <div data-bbox="402 1010 1323 1207" data-label="Diagram"> <p>The diagram illustrates Simplex Mode. On the left is a 'Mainframe' (represented by a rack of hardware) and on the right is a 'Monitor'. A single horizontal line connects them. A pink arrow points from the Mainframe to the Monitor, with the text 'Direction of data' above it. Below the line, the words 'Simplex Mode' are written in blue.</p> </div> <p>a. In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction -for example :Walkie-talkies.</p> <div data-bbox="363 1516 1330 1761" data-label="Diagram"> <p>The diagram illustrates Half-duplex mode. Two 'Workstation' icons (each with a monitor and keyboard) are connected by a horizontal line. Two pink arrows show the direction of data flow at different times. The top arrow points from the left workstation to the right workstation, labeled 'Direction of data at time 1'. The bottom arrow points from the right workstation to the left workstation, labeled 'Direction of data at time 2'. Below the line, the words 'Half-duplex' are written in blue.</p> </div> <p>b. In full-duplex mode both stations can transmit and receive data simultaneously. The transmission medium sharing can occur in two ways,</p>

	<p>namely, either the link must contain two physically separate transmission paths or the capacity of the channel is divided between signals traveling in both directions.</p> <p>-One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.</p>  <p>The diagram illustrates full-duplex communication between two workstations. A horizontal line connects two computer icons, each labeled 'Workstation'. Above the line, a double-headed arrow points in both directions, with the text 'Direction of data all the time' written above it. Below the line, the word 'Full-duplex' is written in a large, bold, blue font.</p>
<b>Q.7</b>	<b>Give the advantages of Computer Network.</b>
Ans:	<ol style="list-style-type: none"> <li>1. File Sharing</li> <li>2. Printer Sharing</li> <li>3. Application Services</li> <li>4. E-mail Services</li> <li>5. Remote access</li> <li>6. Internet &amp; Intranet</li> </ol>
<b>Q.8</b>	<b>List different characteristics of data communication system.</b>
Ans	<ol style="list-style-type: none"> <li>1. Delivery</li> <li>2. Accuracy</li> <li>3. Timeliness</li> <li>4. Jitter</li> </ol>
<b>Q.9</b>	<b>Define Bit rate &amp; Baud rate.</b>
Ans:	<p><b>Bit Rate:</b> Bit rate is simply the number of bits (i.e., 0's and 1's) transmitted per unit time.</p> <p><b>Baud Rate:</b> Baud rate is the number of signal units transmitted per unit time that is needed to represent those bits.</p>

<b>Q.10</b>	<b>Comparison between LAN,WAN,MAN</b>																												
<b>Ans:</b>	<p style="text-align: center;"><b>Differences between LAN, WAN, &amp; MAN</b></p> <table> <tr> <th>LAN</th><th>MAN</th><th>WAN</th></tr> <tr> <td>1. Connection in small and physical area.</td><td>1. Cover a larger geographic area than LAN .</td><td>1. Cover a largest distance.</td></tr> <tr> <td>2. Best LAN types used with Ethernet.</td><td>2. Used with in internet &amp; Ethernet.</td><td>2. Best WAN types used with Internet.</td></tr> <tr> <td>3. Faster than WAN.</td><td>3. Higher speed.</td><td>3. Less speed than LAN.</td></tr> <tr> <td>4. Cheaper.</td><td>4. Competitive price</td><td>4. More expensive.</td></tr> <tr> <td>5. More likely need password validation as it will have specific user rights.</td><td>5. Need password validation as it will have specific user rights.</td><td>5. Less likely need password validation as it will have specific user rights.</td></tr> <tr> <td>6. More private.</td><td>6. High security.</td><td>6. Less private.</td></tr> <tr> <td>7. Hardware focus on sharing resources.</td><td>7. Hardware focus on data transmission.</td><td>7. Hardware focus on communication.</td></tr> <tr> <td>8. Operate on peer to peer</td><td>8. Operated by organizations and public utilities</td><td>8. Operate on client to server.</td></tr> </table>		LAN	MAN	WAN	1. Connection in small and physical area.	1. Cover a larger geographic area than LAN .	1. Cover a largest distance.	2. Best LAN types used with Ethernet.	2. Used with in internet & Ethernet.	2. Best WAN types used with Internet.	3. Faster than WAN.	3. Higher speed.	3. Less speed than LAN.	4. Cheaper.	4. Competitive price	4. More expensive.	5. More likely need password validation as it will have specific user rights.	5. Need password validation as it will have specific user rights.	5. Less likely need password validation as it will have specific user rights.	6. More private.	6. High security.	6. Less private.	7. Hardware focus on sharing resources.	7. Hardware focus on data transmission.	7. Hardware focus on communication.	8. Operate on peer to peer	8. Operated by organizations and public utilities	8. Operate on client to server.
LAN	MAN	WAN																											
1. Connection in small and physical area.	1. Cover a larger geographic area than LAN .	1. Cover a largest distance.																											
2. Best LAN types used with Ethernet.	2. Used with in internet & Ethernet.	2. Best WAN types used with Internet.																											
3. Faster than WAN.	3. Higher speed.	3. Less speed than LAN.																											
4. Cheaper.	4. Competitive price	4. More expensive.																											
5. More likely need password validation as it will have specific user rights.	5. Need password validation as it will have specific user rights.	5. Less likely need password validation as it will have specific user rights.																											
6. More private.	6. High security.	6. Less private.																											
7. Hardware focus on sharing resources.	7. Hardware focus on data transmission.	7. Hardware focus on communication.																											
8. Operate on peer to peer	8. Operated by organizations and public utilities	8. Operate on client to server.																											
<b>Q.9</b>	<b>Differentiate between synchronous and asynchronous communication.</b>																												
<b>Ans</b>	<p><b>Synchronous Communication</b></p> <p>In Synchronous Transmission, data is sent in form of blocks or frames.</p> <p>Sender and Receiver use the same clock signal</p> <p>It is more efficient and more reliable than asynchronous transmission to transfer the large amount of data.</p> <p>Synchronous transmission is fast.</p> <p>In Synchronous transmission, time interval of transmission is constant.</p>	<p><b>Asynchronous Communication</b></p> <p>In Asynchronous Transmission, data is sent in form of byte or character.</p> <p>Does not need clock signal between the sender and the receiver</p> <p>In this transmission start bits and stop bits are added with data.</p> <p>Asynchronous transmission is slow.</p> <p>In asynchronous transmission, time interval of transmission is not constant, it is random.</p>																											



**Chapter 2: Transmission Media and Switching**

<b>Q.1</b>	<b>List any four Unguided Transmission Media.</b>
<b>Ans</b>	<p>Unguided Media or Wireless media:</p> <ol style="list-style-type: none"><li>1. Radio wave</li><li>2. Microwave</li><li>3. Infrared</li><li>4. Satellite</li></ol>
<b>Q.2</b>	<b>Define Guided and Unguided communication media.</b>
<b>Ans.</b>	<p><b>Guided communication media:</b> Guided transmission media are known as the wired communication. The electromagnetic signals travel between the communicating devices through a physical medium/conductor.</p> <p><b>Unguided communication media:</b> The unguided media is also called wireless communication. It does not require any physical medium to transmit electromagnetic signals. In unguided media, the electromagnetic signals are broadcasted through air to everyone.</p>
<b>Q.3</b>	<b>State the two advantages and disadvantages of unguided media</b>
<b>Ans.</b>	<p><b>Advantages:</b></p> <ol style="list-style-type: none"><li>1. Use for long distance communication</li><li>2. High speed data transmission.</li><li>3. Many receiver stations can receive signals from same sender station</li></ol> <p><b>Disadvantages :</b></p> <ol style="list-style-type: none"><li>1. Radio waves travel through Lowest portion of atmosphere which can have lot of noise and interfering signals</li><li>2. Radio wave communication through unguided media is an insecure communication.</li><li>3. Radio wave propagation is susceptible to weather effects like rain, thunder and storm etc.</li></ol>

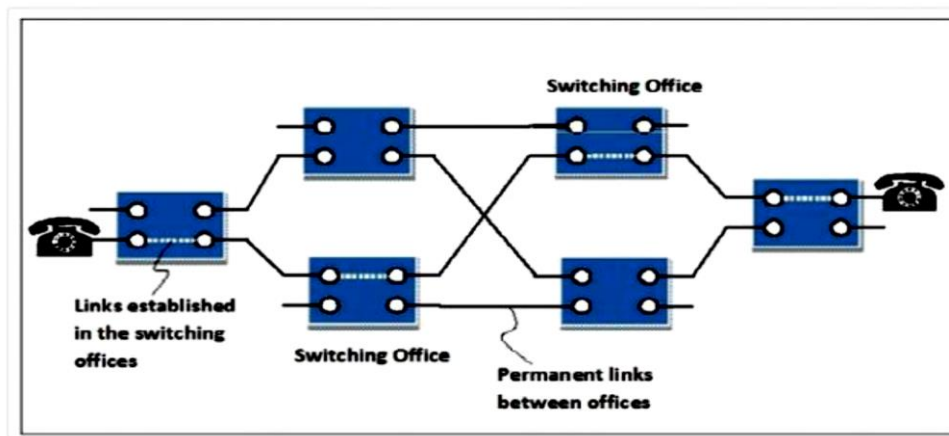


<b>Q.4</b>	<b>Draw structural diagram of fiber optic cable and write its functions</b>
Ans	<div data-bbox="475 254 1133 688" data-label="Image"> <p>The diagram shows a cross-section of a fiber optic cable. At the center is a red 'Core (silica)'. Surrounding it is a white 'Cladding (silica)'. This is followed by a thin grey 'Silicone coating', then a thicker white 'Buffer Jacket'. Outside the buffer jacket are 'Strength members' (represented by grey lines). The entire assembly is encased in a thick grey 'Black polyurethane outer jacket'. A bracket at the bottom right labels the inner components as the 'Optical fiber'.</p> </div> <p data-bbox="516 709 1390 751">Fig. Structural diagram for Fibre Optic Cable Functions of</p> <p data-bbox="272 793 505 835"><b>Optical Cable:</b></p> <ol data-bbox="272 877 1539 1050" style="list-style-type: none"> <li>1. <b>Single-mode fibers</b> - Used to transmit one signal per fiber (used in telephones and cable TV)</li> <li>2. <b>Multi-mode fibers</b> - Used to transmit many signals per fiber (used in computer networks, local area networks)</li> </ol>
<b>Q.5</b>	<b>Draw and explain Fiber Optic Cable.</b>
Ans.	<div data-bbox="565 1161 1328 1480" data-label="Image"> <p>The diagram shows a cross-section of a fiber optic cable. It starts with a grey 'Core' and a white 'Cladding'. This is followed by a blue 'Coating'. Then, there are yellow 'Strengthening Fibers'. The entire assembly is encased in an orange 'Cable Jacket'.</p> </div> <p data-bbox="272 1512 570 1554"><b>Fiber Optic Cable:</b></p> <ul data-bbox="272 1585 1539 1858" style="list-style-type: none"> <li>• A fiber-optic cable is made up of glass or plastic.</li> <li>• It transmits signals in the form of light.</li> <li>• The outer jacket is made up of PVC or Teflon.</li> <li>• Kevlar strands are placed inside the jacket to strengthen the cable.</li> <li>• Below the Kevlar strands, there is another plastic coating which acts as a cushion.</li> <li>• The fiber is at the center of the cable, and it consists of cladding and glass core.</li> <li>• The density of the cladding is less than that of the core.</li> <li>• Optical fibers use the principle of 'reflection' to pass light through a channel.</li> </ul>

Q.6	What advantages does TDM have over FDM in a circuit switched network?														
Ans	<p>In TDM, each signal uses all of the bandwidth some of the time, while for FDM, each signal uses a small portion of the bandwidth all of the time.</p> <p>TDM uses the entire frequency range but dynamically allocates time, certain jobs might require less or more time, which TDM can offer but FDM is unable to as it cannot change the width of the allocated frequency.</p> <p>TDM provides much better flexibility compared to FDM.</p> <p>TDM offers efficient utilization of bandwidth</p> <p>Low interference of signal and minimizes cross talk</p>														
Q.7	Differentiate between FDM and TDM														
	<table><tr><th>Frequency Division Multiplexing</th><th>Time division Multiplexing</th></tr><tr><td>FDM divides the channel into two or more frequency ranges that do not overlap</td><td>TDM divides and allocates certain time periods to each channel in an alternating manner</td></tr><tr><td>Frequency is shared</td><td>Times scale is shared</td></tr><tr><td>Used with Analog signals</td><td>Used with both Digital signals and analog signals</td></tr><tr><td>Interference is high</td><td>Interference is Low or negligible</td></tr><tr><td>Utilization is Ineffective</td><td>Efficiently used</td></tr></table>	Frequency Division Multiplexing	Time division Multiplexing	FDM divides the channel into two or more frequency ranges that do not overlap	TDM divides and allocates certain time periods to each channel in an alternating manner	Frequency is shared	Times scale is shared	Used with Analog signals	Used with both Digital signals and analog signals	Interference is high	Interference is Low or negligible	Utilization is Ineffective	Efficiently used		
Frequency Division Multiplexing	Time division Multiplexing														
FDM divides the channel into two or more frequency ranges that do not overlap	TDM divides and allocates certain time periods to each channel in an alternating manner														
Frequency is shared	Times scale is shared														
Used with Analog signals	Used with both Digital signals and analog signals														
Interference is high	Interference is Low or negligible														
Utilization is Ineffective	Efficiently used														
Q.8	Why is circuit switching preferred over packet switching in voice communication?														
Ans.	<p>Switching is a mechanism by which data/information sent from source towards destination which are not directly connected. Networks have interconnecting devices, which receives data from directly connected sources, stores data, analyse it and then forwards to the next interconnecting device closest to the destination.</p> <p>Switching can be categorized as:</p> <ul style="list-style-type: none"><li>• Circuit switching</li><li>• Packet switching</li><li>• Message switching</li></ul> <p>Circuit switching is preferred over packet switching in voice communication because:</p> <ul style="list-style-type: none"><li>• In circuit switching, a dedicated path is established between sender and receiver which is maintained for entire duration of conversation.</li><li>• It provides continuous and guaranteed delivery of data.</li></ul>														

	<ul style="list-style-type: none"> <li>• During the data transfer phase, no addressing is needed.</li> <li>• Delays are small.</li> <li>• It uses connection oriented service.</li> <li>• Message received in order to the destination</li> </ul>
<b>Q.9</b>	<b>State the advantages of coaxial cable.</b>
<b>Ans</b>	<ul style="list-style-type: none"> <li>• Due to skin effect, coaxial cable is used in high frequency applications (&gt; 50 MHz) using copper clad materials for center conductor. Skin effect is result of high frequency signals propagating along outer surface of the conductor. It increases tensile strength of the cable and reduces weight.</li> <li>• The cost of coaxial cable is less.</li> <li>• The outer conductor in coaxial cable is used to improve attenuation and shield effectiveness. This can be further enhanced with the use of second foil or braid known as jacket (C2 as designated in the figure-1). The jacket is used as protective cover from the environment and makes overall coaxial cable as flame retardant.</li> <li>• It is less susceptible to noise or interference (EMI or RFI) compare to twisted pair cable.</li> <li>• It supports high bandwidth signal transmission compare to twisted pair.</li> <li>• It is easy to wire and easy to expand due to flexibility.</li> <li>• It allows high transfer rates with coaxial cable having better shielding materials.</li> </ul>
<b>Q.10</b>	<p><b>What is meant by circuit switching and give its advantages.</b></p> <p style="text-align: center;"><b>OR</b></p> <p><b>Explain circuit switching networks with neat sketch.</b></p>
<b>Ans.</b>	<p>Circuit switching is a connection-oriented network switching technique. Here, a dedicated route is established between the source and the destination and the entire message is transferred through it.</p> <p><b>Phases of Circuit Switch Connection:</b></p> <p><b>Circuit Establishment:</b> In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centers. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.</p> <p><b>Data Transfer:</b> Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.</p>

**Circuit Disconnection:** When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver



The diagram represents circuit established between two telephones connected by circuit switched connection. The blue boxes represent the switching offices and their connection with other switching offices. The black lines connecting the switching offices represent the permanent link between the offices.

**Advantages:**

- In circuit switching, a dedicated path is established between sender and receiver which is maintained for entire duration of conversation.
- It provides continuous and guaranteed delivery of data.
- During the data transfer phase, no addressing is needed.
- Delays are small.
- It uses connection oriented service.
- Message received in order to the destination

**Q.11 Enlist any four communication bands for unguided media with frequency range**

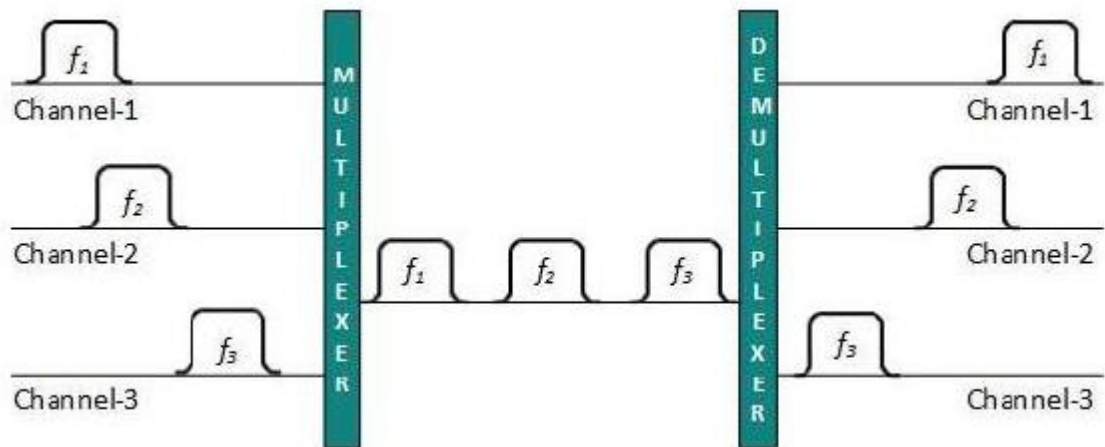
**Ans.** There are 3 major types of Unguided Media:

**(i) Radiowaves**

- These are easy to generate and can penetrate through buildings.
- The sending and receiving antennas need not be aligned.
- Frequency Range: 3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.

	<ul style="list-style-type: none"> <li>• Further Categorized as (i) Terrestrial and (ii) Satellite.</li> </ul> <p><b>(ii) Microwaves</b></p> <ul style="list-style-type: none"> <li>• It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other.</li> <li>• The distance covered by the signal is directly proportional to the height of the antenna.</li> <li>• Frequency Range: 1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.</li> </ul> <p><b>(iii) Infrared</b></p> <ul style="list-style-type: none"> <li>• Infrared waves are used for very short distance communication.</li> <li>• They cannot penetrate through obstacles.</li> <li>• This prevents interference between systems.</li> <li>• Frequency Range: 300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.</li> </ul>
<b>Q.12</b>	<b>Explain working of Packet switching</b>
<b>Ans.</b>	<p>Packet switching is a digital network transmission process in which data is broken into suitably-sized pieces or blocks for fast and efficient transfer via different network devices. When a computer attempts to send a file to another computer, the file is broken into packets so that it can be sent across the network in the most efficient way. These packets are then routed by network devices to the destination.</p> <p>Packet switching can be used as an alternate to circuit switching. In the packet switched networks, data is sent in discrete units that have variable length. They are called as packets. There is a strict upper bound limit on the size of packets in a packet switch network. The packet contains data and various control information. The packet switched networks allow any host to send data to any other host without reserving the circuit. Multiple paths between a pair of sender and receiver may exist in a packet switched network.</p> <p>One path is selected between source and destination. Whenever the sender has data to send, it converts them into packets and forwards them to next computer or router. The router stores this packet till the output line is free.</p> <p>The packet is transferred to next computer or router (called as hop). This way, it moves to the destination hop by hop. All the packets belonging to a transmission may or may not take the same route. The route of a packet is decided by network layer protocols.</p>

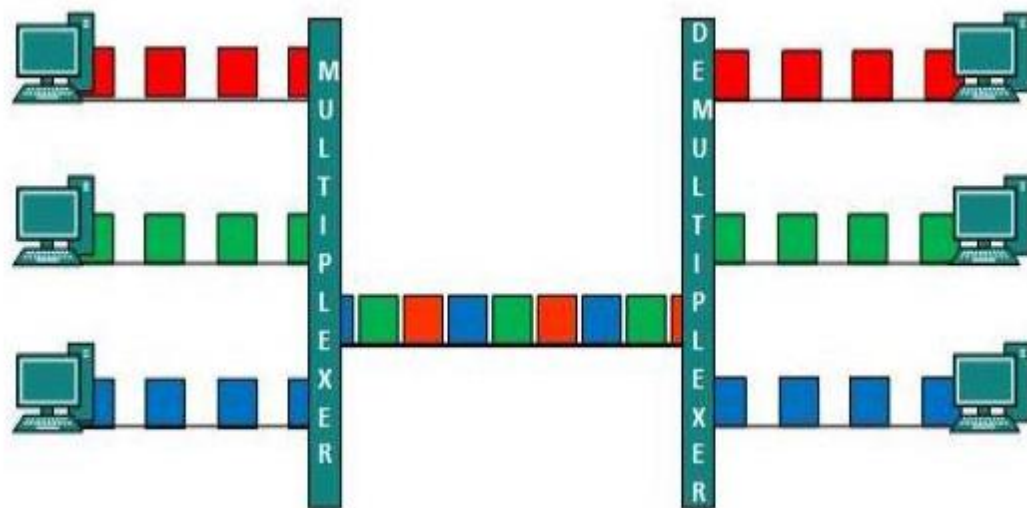
	<p><b>Advantages of Packet Switching</b></p> <ol style="list-style-type: none"><li>1. The main advantage of packet switching is the efficiency of the network. In circuit switching network, a reserved circuit cannot be used by others, till the sender and receiver leave it. Even if no data is being sent on a reserved circuit, no one else can access the circuit. This results in network bandwidth wastage. The packet switching reduces network bandwidth wastage.</li><li>2. The other advantage is that the packet switching is more faults tolerant. In case of circuit switching, all the packets are lost if a router in the circuit is down as all the packets follow the same route. But, in case of packet switching network, the packets can be routed over the malfunctioning component of the network. This is because all the packets may follow a different route to the destination.</li></ol>
<b>Q.13</b>	<b>What is multiplexing? List types and explain any one.</b>
<b>Ans.</b>	<p>Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams. Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing. When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.</p> <p>Different multiplexing techniques are</p> <ol style="list-style-type: none"><li>1. Frequency Division multiplexing</li><li>2. Time division multiplexing</li></ol> <p><b>Frequency Division Multiplexing:</b> When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.</p>



### Frequency Division Multiplexing

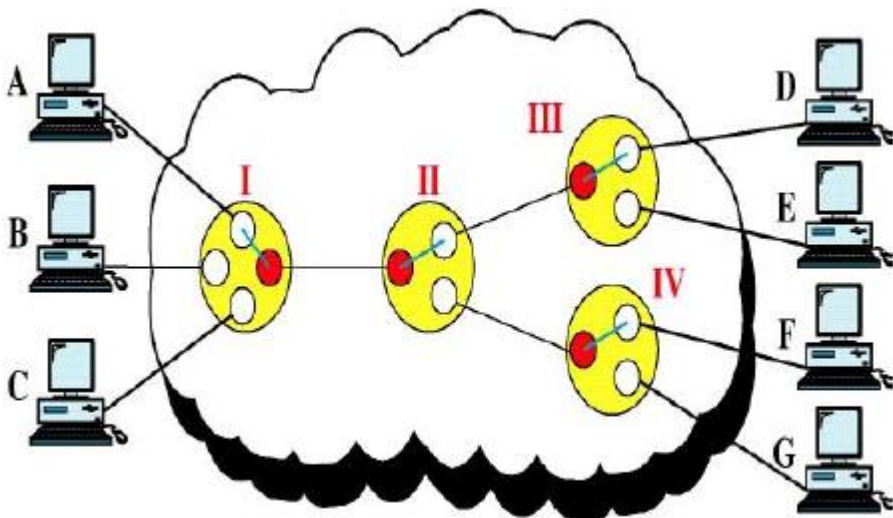
**Time Division Multiplexing:** TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

TDM works in synchronized mode. Both ends, i.e. Multiplexer and Demultiplexer are timely synchronized and both switch to next channel simultaneously.



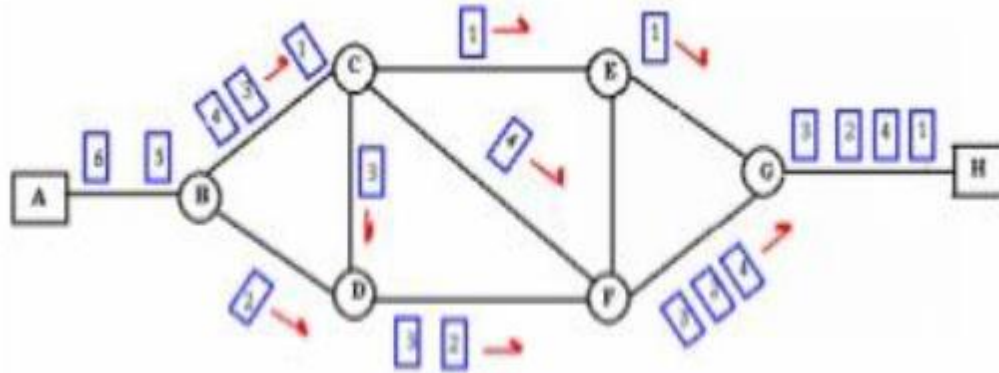
### Time Division Multiplexing

When channel A transmits its frame at one end, the De-multiplexer provide media to channel A on the other end. As soon as the channel A's time slot expires, this

	side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner
<b>Q.14</b>	<b>Describe the principles of packet switching and circuit switching techniques with neat diagram.</b>
<b>Ans.</b>	<p><b>Circuit Switching:</b> When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.</p> <p>Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:</p> <ul style="list-style-type: none"> <li>• Establish a circuit</li> <li>• Transfer the data</li> <li>• Disconnect the circuit</li> </ul>  <p style="text-align: center;"><b>Circuit Switching</b></p> <p>Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between callers and called is established over the network.</p> <p><b>Packet Switching:</b> The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.</p> <p>It is easier for intermediate networking devices to store small size packets and they</p>



do not take much resource either on carrier path or in the internal memory of switches.



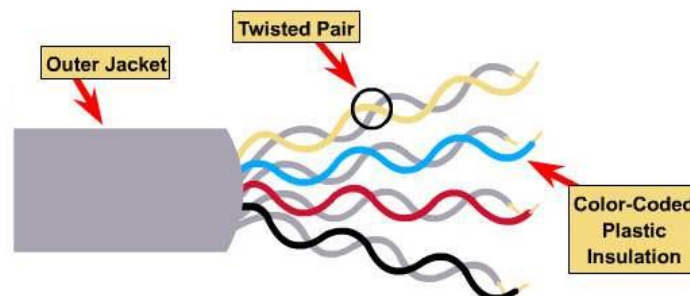
### Packet Switching

Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

**Q.15 Explain UTP and STP in transmission media?**

**Ans.** 1. **Unshielded Twisted Pair (UTP):**

### Unshielded Twisted Pair (UTP)



This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

#### Advantages:

- Least expensive
- Easy to install
- High speed capacity

**Disadvantages:**

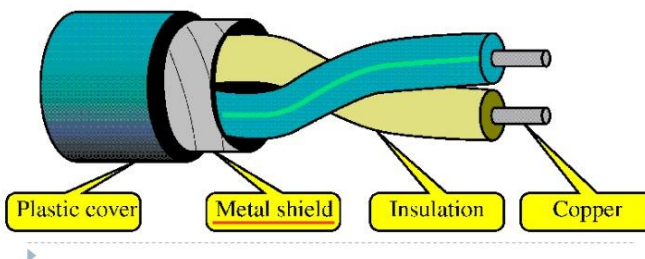
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

**2. Shielded Twisted Pair (STP):**

Shielded twisted pair (STP) cable combines the technique of shielding, cancellation and wire twisting. Each pair of wires is wrapped in a metallic foil. The four pairs of wires then are wrapped in an overall metallic braid of foil. STP cable is used to eliminate inductive and capacitive coupling.

**Shielded Twisted-Pair (STP)**

- ▶ STP cables are similar to UTP cables, except there is a metal foil or braided-metal-mesh cover that encases each pair of insulated wires



This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

**Advantages:**

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparitively faster

**Disadvantages:**

- Comparitively difficult to install and manufacture
- More expensive
- Bulky

**Chapter 3: Error Detection, correction and wireless transmission**

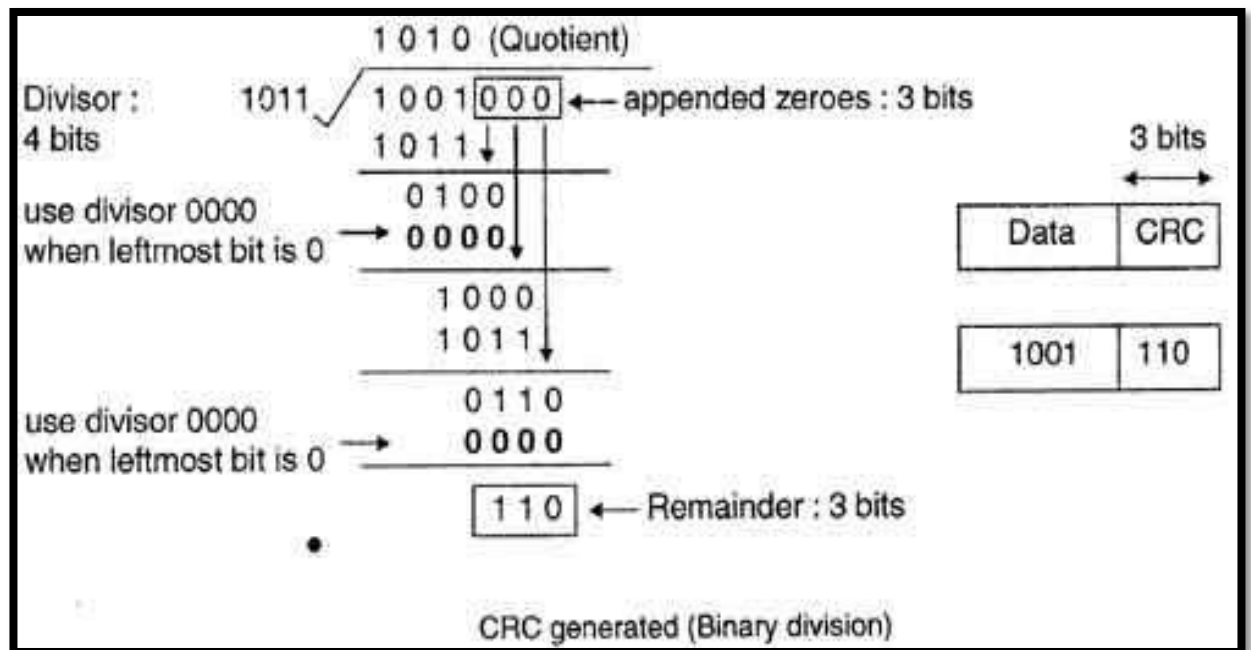
<b>Q.1</b>	<b>List types of Errors</b>
<b>Ans.</b>	Content Error Flow Integrity error
<b>Q.2</b>	<b>List IEEE 802 X standards for networks</b>
<b>Ans.</b>	1. 802.3: Ethernet  2. 802.4:Token Bus  3. 802.5:Token Ring  4. 802.11:Wi Fi(Wireless Fidelity)
<b>Q.3</b>	<b>Describe various IEEE standards for network topologies.</b>
<b>Ans.</b>	A set of network standards developed by the IEEE. They include: <ul style="list-style-type: none"> <li>• IEEE 802.1: Standards related to network management.</li> <li>• IEEE 802.2: General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sublayers -- the logical link control (LLC) layer and the media access control (MAC) layer. The MAC layer varies for different network types and is defined by standards IEEE 802.3 through IEEE 802.5.</li> <li>• IEEE 802.3: Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard.</li> <li>• IEEE 802.4: Defines the MAC layer for bus networks that use a token- passing mechanism (token bus networks).</li> <li>• IEEE 802.5: Defines the MAC layer for token-ring networks.</li> <li>• IEEE 802.6: Standard for Metropolitan Area Networks (MANs).</li> <li>• IEEE 802.11 Wireless Network Standards: 802.11 is the collection of standards setup for wireless networking.</li> </ul>
<b>Q.4</b>	<b>What is the MAC protocol used in TOKEN ring LAN's? What happens if the token is lost?</b>
<b>Ans.</b>	Token ring local area network (LAN) network is a communication protocol for local area networks.it uses special three-byte frame called a “token” that travels around a logical ring of workstations or servers. This token passing is a channel access method providing fair access for all stations, and eliminating the collision of contention-based access methods.  Introduced by IBM in 1984, it was then standardized with protocol IEEE 802.5 and was fairly successful, particularly in the corporate environments, but gradually eclipsed by the later versions of Ethernet.

	<p>The IEEE 802.5 Token ring technology provides for data transfer rates of either 4 or 16 Mbps.</p> <p>It works in the following manner:</p> <ol style="list-style-type: none"> <li>1. Empty information frames are continuously circulated on the ring.</li> <li>2. When a computer has a message to send, it inserts a token in an empty frame (simply changing a 0 to a 1 in the token bit part of the frame) and a message and a destination identifier in the frame.</li> <li>3. The frame is then examined by each successive workstation. If workstation sees that it is the destination of the message, it copies the message from the frame and changes the token back to 0.</li> <li>4. When the frame gets back to originator, it sees that message has been copied and received.</li> </ol> <p>The Fibre Distributed Data Interface (FDDI) also uses a Token ring protocol.</p> <p>If one device does not receive a token within a specified period, it can issue an alarm. The alarm alerts the network administrator to the problem and its location. Then, network administrator generates a new, free token</p> <p style="text-align: center;"><b>OR</b></p> <p>· There are two error conditions that could cause the token ring to break down.</p> <ul style="list-style-type: none"> <li>• One is the lost token in which case there is no token in the ring.</li> <li>• Other is the busy token that circulates endlessly.</li> </ul> <p>To overcome these problems, the IEEE 802 standard specifies that one of the stations must be designated as “active monitor”. The monitor detects the lost condition using a timer by time-out mechanism and recovers by using a new free token</p>
<b>Q.5</b>	<b>A system uses CRC on a block of 8 bytes. How many redundant bits are sent per block? What is the ratio of useful bits to total bits?</b>
<b>Ans.</b>	CRC is one of the most common and powerful error detecting code which can be describe as follows. The polynomial code also known as CRC with co-efficient of

0s and 1s. In this method the sender and receiver must agree upon generator polynomial  $g(x)$  in advance. Both the high and low order bits of the generator (divisor) must be 1. To compute the checksum for some frame (data) with  $m$  bits, the frame must be longer than generator polynomial. The idea is to append checksum to the end of frame in such a way that the polynomial represented by the checksum frame is divisible by  $g(x)$ . When the receiver gets the checksum frame it tries dividing it by  $g(x)$ . If there is remainder there has been a transmission error and zero remainder means no error in the transmission.  $r$  is degree of  $g(x)$  polynomial.

### Step by step procedure:

1. Append a string of  $r$  zero bits to the lower order end of data word( $m$ ) where  $r$  is less than the number of bits pre-decided divisor by 1 bit i.e. if divisor = 5 bits then  $r = 4$  zeros. Now data word contains  $m+r$  bits
2. Divide the newly generated data unit in step 1 by the divisor. It is module – 2 division
3. The remainder obtained after division is the  $r$  bit CRC.
4. This CRC will replace the  $r$  zeros appended to the data unit to get the code word to be transmitted.



**NOTE:** The polynomial code for calculation of redundant bits is not given .hence the data given is insufficient for calculating redundant bits and the ratio of useful bits to total bits.

Q.6	<b>Explain different types of transmission errors.</b>
Ans.	<p><b>Types of transmission errors :</b></p> <p>These interferences can change the timing and shape of the signal. If the signal is carrying binary encoded data, such changes can alter the meaning of the data. These errors can be divided into two types: Single- bit error and Burst error.</p> <p><b>Single-bit Error</b></p> <p>The term single-bit error means that only one bit of given data unit (such as a byte, character, or data unit) is changed from 1 to 0 or from 0 to 1 as shown in Fig</p> <div data-bbox="574 709 1255 877" data-label="Diagram"> <p style="text-align: center;">Single bit change (1 is changed to 0)</p> </div> <p style="text-align: center;"><b>Single Bit Error</b></p> <p>Single bit errors are least likely type of errors in serial data transmission. To see why, imagine a sender sends data at 10 Mbps. This means that each bit lasts only for 0.1 <math>\mu</math>s (micro-second). For a single bit error to occur noise must have duration of only 0.1 <math>\mu</math>s (micro-second), which is very rare. However, a single-bit error can happen if we are having a parallel data transmission. For example, if 16 wires are used to send all 16 bits of a word at the same time and one of the wires is noisy, one bit is corrupted in each word.</p> <p><b>Burst Error:</b></p> <p>The term burst error means that two or more bits in the data unit have changed from 0 to 1 or vice-versa. Note that burst error doesn't necessary means that error occurs in consecutive bits. The length of the burst error is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not be corrupted.</p> <div data-bbox="537 1650 1300 1881" data-label="Diagram"> <p style="text-align: center;">Bits in error</p> <p style="text-align: center;">Length of burst (6 bits)</p> </div> <p style="text-align: center;"><b>Burst Error</b></p>

	<p>Burst errors are mostly likely to happen in serial transmission. The duration of the noise is normally longer than the duration of a single bit, which means that the noise affects data; it affects a set of bits.</p>
<b>Q.7</b>	<p><b>Describe Piconet and scatter net architecture with neat diagram.</b></p> <p><b>OR</b></p> <p><b>Describe Bluetooth architecture technologies.</b></p>
<b>Ans</b>	<p>Bluetooth Architecture</p> <p>Bluetooth architecture defines two types of networks:</p> <ol style="list-style-type: none"> <li>1. Piconet</li> <li>2. Scatternet</li> </ol> <p><b>1. Piconet</b></p> <ul style="list-style-type: none"> <li>• Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.</li> <li>• Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.</li> <li>• There can be only one primary or master station in each piconet.</li> <li>• The communication between the primary and the secondary can be one-to-one or one-to-many.</li> </ul> <div data-bbox="532 1354 1421 1732" data-label="Diagram"> <p>The diagram illustrates a Piconet, which is a Bluetooth network. It consists of one Primary/Master node (represented by a computer monitor icon) at the top, connected by four lightning-bolt-like lines to four Secondary/Slave nodes (also represented by computer monitor icons) arranged in a row below. The entire group of nodes is enclosed within a light green oval boundary. The label 'Piconet' is centered below the oval. The labels 'Primary/Master' and 'Secondary/Slave' are placed next to their respective icons.</p> </div> <p><b>Piconet</b></p> <ul style="list-style-type: none"> <li>• All communication is between master and a slave. Slave-slave communication</li> </ul>

is not possible.

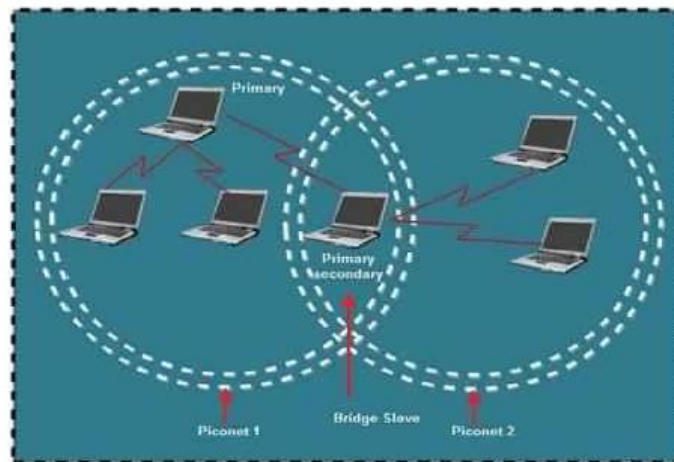
- In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

## 2. Scatternet

- Scatternet is formed by combining various piconets.
- A slave in one piconet can act as a master or primary in other piconet.
- Such 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.



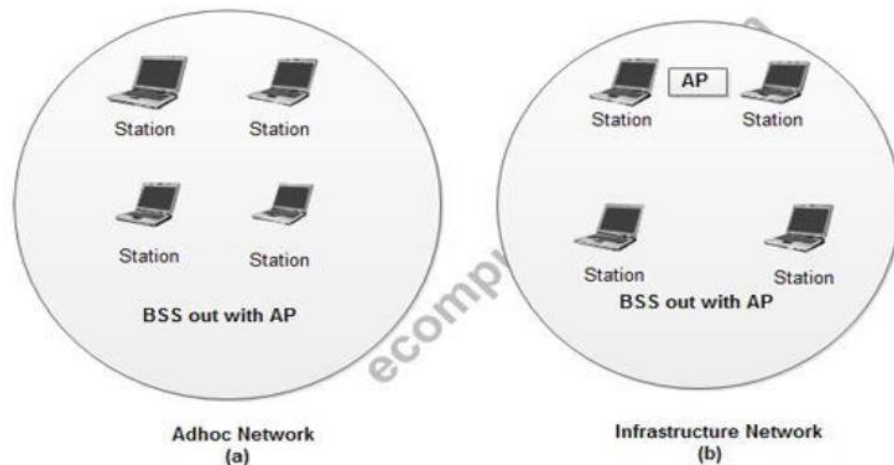
**Scatternet**

**Q.8** **Classify mobile generations**

**Ans** First Generation (1G)  
 Second Generation (2G)  
 Third Generation (3G)  
 Fourth Generation (4G) or LTE  
 Fifth Generation (5G)



Q.9	Compare LRC and CRC	
Ans	<b>LRC</b>	<b>CRC</b>
	LRC stands for Longitudinal Redundancy Check	<b>CRC stands for</b> Cyclic Redundancy Check
	LRC is a method in which a block of bits is organized in table(rows and columns)calculate the parity bit for each column and the set of this parity bit is also sending with original data. From the block of parity we can check the redundancy	CRC is one of the most common and powerful error detecting codes in which a sequence of redundant bits, called the CRC is appended to the end of the unit so that the resulting data unit become exactly divisible by a second, predetermined binary number.
	LRC of n bits can easily detect	CRC is more powerful than
	Burst error of n bits.	VRC and LRC in detecting errors
	LRC is an error detection method based on binary addition	CRC is based on binary division.
Q.10	Explain wireless LAN 802.11 architecture.	
Ans	<b>Wireless LAN 802.11:</b> The IEEE 802.11 standard defines the physical layer and media access control (MAC) layer for a wireless local area network. Wireless LANs transmit and receive data over the atmosphere, using radio frequency (RF) or infrared optical technology, thereby; eliminating the need for fixed wired connections.	
	<b>802.11 Architecture:</b> The 802.11architecture defines two types of services: 1. Basic services set (BSS) 2. Extended Service Set (ESS) <b>1. Basic Services Set (BSS)</b> <ul style="list-style-type: none"><li>• The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP).</li><li>• The use of access point is optional.</li><li>• If the access point is not present, it is known as stand-alone network. Such a BSS cannot send data to other BSSs. This type of architecture is known as adhoc architecture.</li><li>• The BSS in which an access point is present is known as an infrastructure network.</li></ul>	

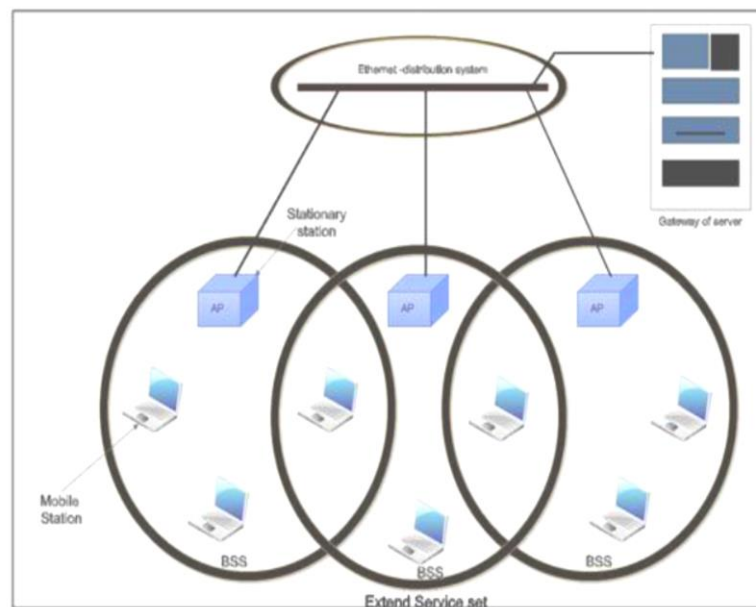


### Basic Service Sets

## 2. Extend Service Set (ESS)

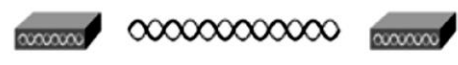
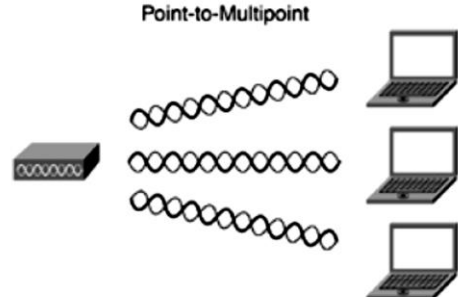
An extended service set is created by joining two or more basic service sets (BSS) having access points (APs).

These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.



There are two types of stations in ESS:

- (i) **Mobile stations:** These are normal stations inside a BSS.
- (ii) **Stationary stations:** These are AP stations that are part of a wired LAN.

<b>Q.11</b>	<b>Describe wireless infrastructure components in detail</b>
<b>Ans.</b>	<p><b>Wireless Network Infrastructures</b></p> <p>The infrastructure of a wireless network interconnects wireless users and end systems. The infrastructure might consist of base stations, access controllers, application connectivity software, and a distribution system. These components enhance wireless communications and fulfill important functions necessary for specific applications.</p> <p><b>1. Base Stations</b></p> <p>The base station is a common infrastructure component that interfaces the wireless communications signals traveling through the air medium to a wired network? Often referred to as a distribution system. Therefore, a base station enables users to access a wide range of network services, such as web browsing e-mail access, and database applications. A base station often contains a wireless NIC that implements the same technology in operation by the user's wireless NIC.</p> <p>Residential gateways and routers are more advanced forms of base stations that enable additional network functions.</p> <p>As show in Figure a base station might support point-to-point or point-to-multipoint communications.</p> <div data-bbox="714 1218 1169 1722"><p style="text-align: center;">Point-to-Point</p><p style="text-align: center;">Point-to-Multipoint</p></div> <p style="text-align: center;"><b>Base Stations Support Different Configurations</b></p>

**Access Controllers**

In the absence of adequate security, quality of service (QoS), and roaming mechanisms in wireless network standards, companies offer access-control solutions to strengthen wireless systems. The key component to these solutions is an access controller, which is typically hardware that resides on the wired portion of the network between the access points and the protected side of the network. Access controllers provide centralized intelligence behind the access points to regulate traffic between the open wireless network and important resources. In some cases, the access point contains the access control function.

**Application Connectivity Software**

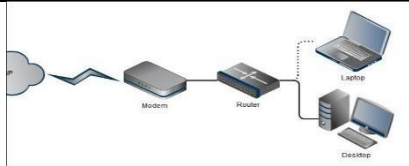
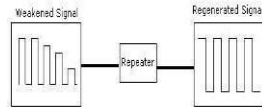
Web surfing and e-mail generally perform well over wireless networks. All it takes is a browser and e-mail software on the client device. Users might lose a wireless connection from time to time, but the protocols in use for these relatively simple applications are resilient under most conditions.

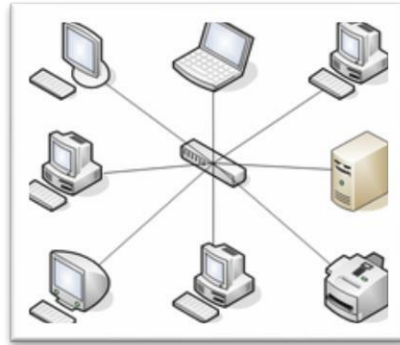
Special application connectivity software is necessary as an interface between a user's computer device and the end system hosting the application's software or database.

**Distribution System**

A wireless network is seldom entirely free of wires. The distribution system, which often includes wiring, is generally necessary to tie together the access points, access controllers, and servers. In most cases, the common Ethernet comprises the distribution system.

### Chapter 4: Network topologies and Network devices

Q.1	State different types of Network topologies		
Ans.	1. Mesh Topology 2. Star Topology 3. Bus Topology 4. Ring Topology 5. Hybrid Topology		
Q.2	Compare Router and Repeater.		
Ans.	<b>Router</b>	<b>Repeater</b>	
	A router is a device like a switch that routes data packets based on their IP addresses.	Repeater regenerates the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.	
	Router is mainly a Network Layer device.	A repeater operates at the physical layer.	
			
Q.3	With suitable diagram describe (i) STAR Topology (ii) RING Topology		
Ans.	<p><b>(i) STAR Topology</b></p> <p>Star topology is a network topology where each individual piece of a network is attached to a central node (often called a hub or switch). The attachment of these network pieces to the central component is visually represented in a form similar to a star.</p> <p>The hub and hosts, and the transmission lines between them, form a graph with the topology of a star. Data on a star network passes through the hub before continuing to its destination. The hub manages and controls all functions of the network. It also acts as a repeater for the data flow.</p>		



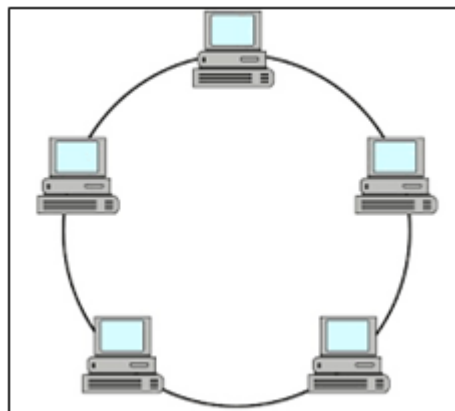
**Fig a: Star topology**

The star network is one of the most common computer network topologies.

**(ii) RING Topology**

A ring network is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node - a ring.

Data travels from node to node, with each node along the way handling every packet.



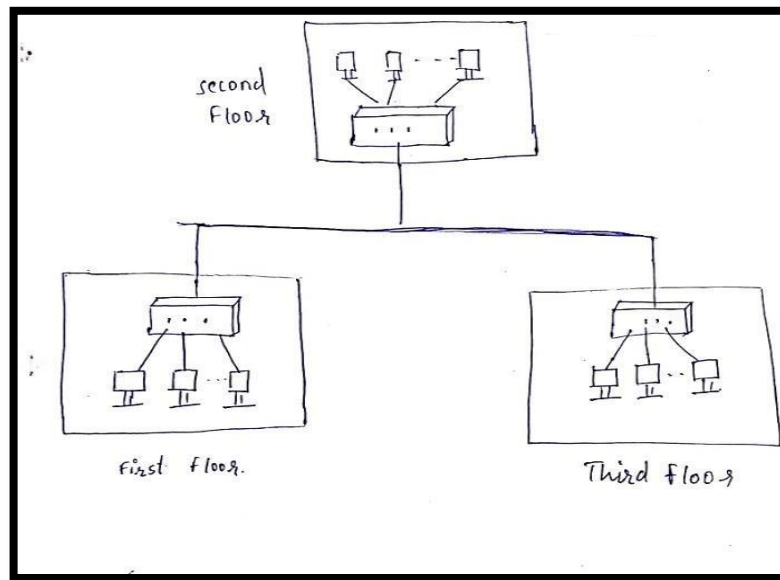
**Fig b: Ring Topology**

Ring topology refers to a specific kind of network setup in which devices are connected in a ring and pass information to or from each other according to their adjacent proximity in the ring structure. This type of topology is highly efficient and handles heavier loads better than bus topology.

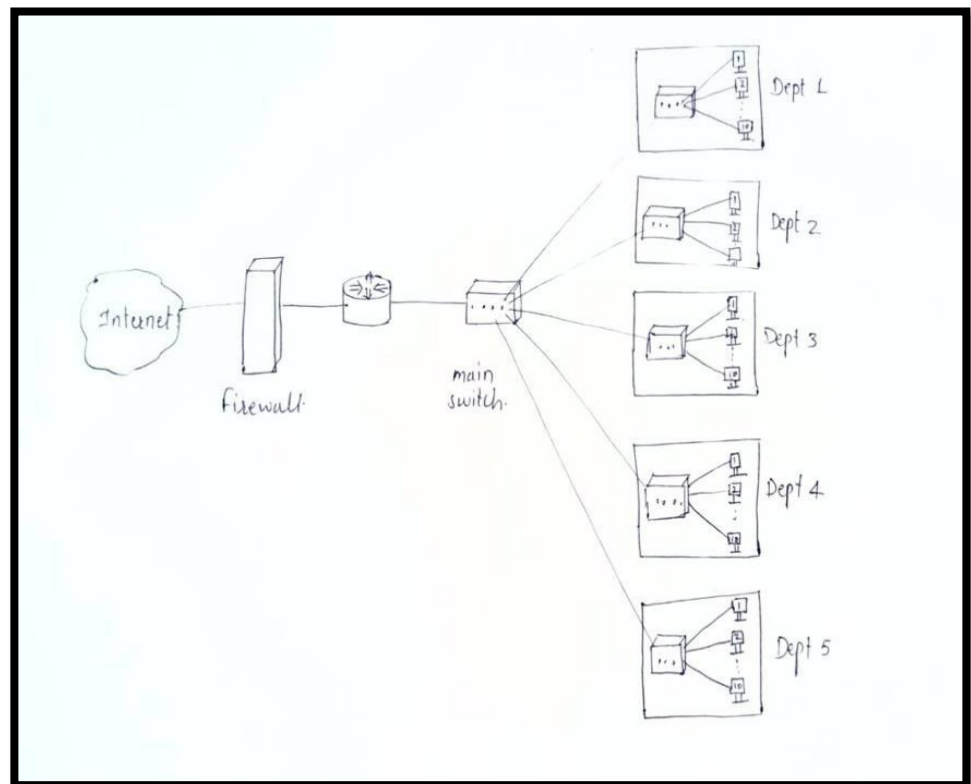
<b>Q.4</b>	<b>Describe different connecting devices used in computer network.</b>
<b>Ans.</b>	<p>Network Connecting devices are:</p> <ol style="list-style-type: none"><li>1. Repeater</li><li>2. Hub</li><li>3. Switch</li><li>4. Bridge</li><li>5. Router</li><li>6. Gateway</li><li>7. Modem</li></ol> <p><b>Repeater:</b></p> <ul style="list-style-type: none"><li>• It is used to take the distorted, weak and corrupt input signal and regenerate this signal at its output.</li><li>• It ensures that the signals are not distorted or weak before it reaches the destination.</li><li>• It recreates the bit pattern of the signal, and puts this regenerated signal back on to the transmission medium</li><li>• It works in the physical layer with no intelligent function.</li></ul> <p><b>Hub:</b></p> <ul style="list-style-type: none"><li>• It is also known as multiport repeater.</li><li>• It is normally used for connecting stations in a physical star topology.</li><li>• It is the broadcasting device.</li><li>• It sends packets to all nodes in the network.</li></ul> <p><b>Switch:</b></p> <ul style="list-style-type: none"><li>• It is used to connect multiple computers in which it can direct a transmission to its specific destination. (Unicast the signals).</li><li>• It is a unicasting device.</li><li>• It avoids unnecessary network traffic.</li><li>• It operates in both the physical and the data link layer.</li></ul> <p><b>Bridge:</b></p> <ul style="list-style-type: none"><li>• It is a device which connects two or more segment of a network.</li><li>• A bridge filters data traffic at a network boundary.</li><li>• Bridges reduces the amount of traffic on a LAN by dividing it into two segments.</li><li>• It inspects incoming traffic and decides whether to forward or discard it.</li><li>• It sends packets between two networks of same type.</li><li>• A bridge operates in both the physical and the data link layer.</li></ul> <p><b>Gateway:</b></p> <ul style="list-style-type: none"><li>• It is a node in a computer network, a key stopping point for data on its way to or from other networks.</li><li>• Gateway is protocol converter.</li></ul>

	<ul style="list-style-type: none"> <li>• Gateway enables communication between different network architecture and environments.</li> <li>• It works at all layers of OSI model.</li> </ul> <p><b>Router:</b></p> <ul style="list-style-type: none"> <li>• It is a device that helps in determining the best and shortest path out of the available paths, for a particular transmission.</li> <li>• Routers use logical and physical addressing to connect two or more logically separate networks.</li> <li>• Router read complex network address in packet and efficiently directs packets from one network to another, reducing excessive traffic.</li> <li>• It works at Physical, Data-Link and Network Layer of OSI model</li> <li>• It Connect dissimilar networks.</li> </ul> <p><b>Modem:</b></p> <ul style="list-style-type: none"> <li>• Modem works as modulator as well as demodulator.</li> <li>• It is the device used to converts digital signals generated by the computer into analog signals which can be transmitted over a telephone or cable line transforms incoming analog signals into their digital equivalents.</li> <li>• A two way communication is established.</li> </ul>
<b>Q.5</b>	<b>Draw and describe architecture for network using tree topology for an office in 3-storeys building.</b>
<b>Ans.</b>	<p>A tree topology is a special type of structure in which many connected elements are arranged like the branches of a tree</p> <p>Here in the diagram the main switch is connected with three separate switches.</p> <p>For each floor separate switch is connected with multiple terminals.</p> <div data-bbox="565 1329 1308 1850" data-label="Diagram"> <pre> graph TD     MS[main switch] --- F1[1st floor switch]     MS --- F2[2nd floor switch]     MS --- F3[3rd floor switch]     F1 --- T1_1[ ]     F1 --- T1_2[ ]     F1 --- T1_3[ ]     F2 --- T2_1[ ]     F2 --- T2_2[ ]     F2 --- T2_3[ ]     F3 --- T3_1[ ]     F3 --- T3_2[ ]     F3 --- T3_3[ ]   </pre> </div>

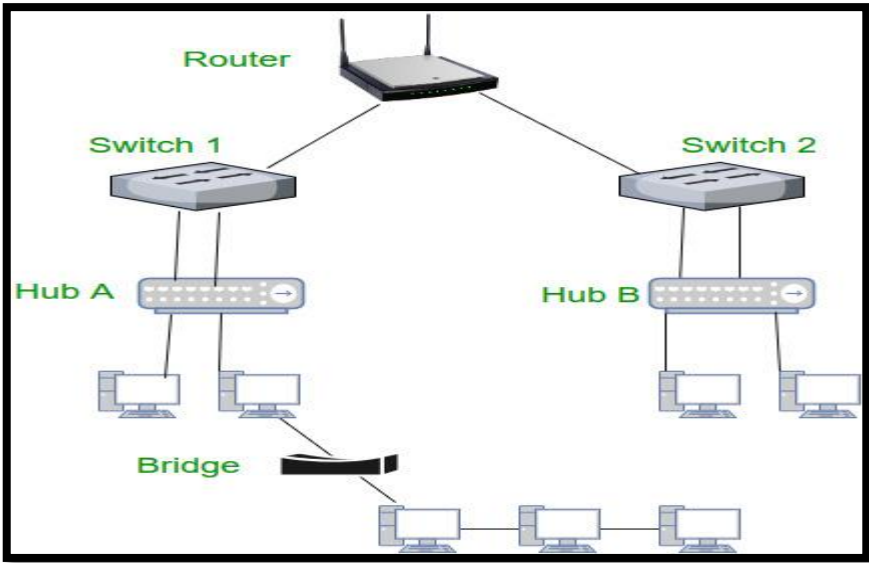


**Q.6**

Design suitable network layout for an organization with five department

**Ans.**

<b>Q.7</b>	<b>Define topology. List any 2 types of topologies</b>																																											
<b>Ans</b>	<p>Network topology refers to the physical or logical layout of a network. It defines the way different nodes are placed and interconnected with each other. Alternately, network topology may describe how the data is transferred between these nodes.</p> <p><b>Types of topologies</b></p> <p>Bus Topology  Star Topology  Ring Topology  Tree Topology  Mesh Topology  Hybrid Topology</p>																																											
<b>Q.8</b>	<b>Differentiate between Hub and Switch.</b>																																											
<b>Ans.</b>	<table> <tr> <th></th><th>Hub</th><th>Switch</th></tr> <tr> <td><b>Layer</b></td><td>Physical layer. Hubs are classified as Layer 1 devices per the OSI model.</td><td>Data Link Layer. Network switches operate at Layer 2 of the OSI model.</td></tr> <tr> <td><b>Function</b></td><td>To connect a network of personal computers together, they can be joined through a central hub.</td><td>Allow to connect multiple device and port can be manage, Vlan can create security also can apply</td></tr> <tr> <td><b>Data Transmission form</b></td><td>Electrical signal or bits</td><td>Frame (L2 Switch) Frame &amp; Packet (L3 switch)</td></tr> <tr> <td><b>Transmission Type</b></td><td>Hubs always perform frame flooding; may be unicast, multicast or broadcast</td><td>First broadcast; then unicast &amp; multicast as needed.</td></tr> <tr> <td><b>Ports</b></td><td>4/12 ports</td><td>Switch is multi port Bridge. 24/48 ports</td></tr> <tr> <td><b>Device Type</b></td><td>Passive Device (Without Software)</td><td>Active Device (With Software) &amp; Networking device</td></tr> <tr> <td><b>Used in (LAN, MAN, WAN)</b></td><td>LAN</td><td>LAN</td></tr> <tr> <td><b>Table</b></td><td>A network hub cannot learn or store MAC address.</td><td>Switches use content accessible memory CAM table which is typically accessed by ASIC (Application Specific Integrated chips).</td></tr> <tr> <td><b>Transmission Mode</b></td><td>Half duplex</td><td>Half/Full duplex</td></tr> <tr> <td><b>Broadcast Domain</b></td><td>Hub has one Broadcast Domain.</td><td>Switch has one broadcast domain [unless VLAN implemented]</td></tr> <tr> <td><b>Definition</b></td><td>An electronic device that connects many network device together so that devices can exchange data</td><td>A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send msg to device that needs or request it</td></tr> <tr> <td><b>Spanning-Tree</b></td><td>No Spanning-Tree</td><td>Many Spanning-tree Possible</td></tr> <tr> <td><b>Collisions</b></td><td>Collisions occur commonly in setups using hubs.</td><td>No collisions occur in a full-duplex switch.</td></tr> </table>			Hub	Switch	<b>Layer</b>	Physical layer. Hubs are classified as Layer 1 devices per the OSI model.	Data Link Layer. Network switches operate at Layer 2 of the OSI model.	<b>Function</b>	To connect a network of personal computers together, they can be joined through a central hub.	Allow to connect multiple device and port can be manage, Vlan can create security also can apply	<b>Data Transmission form</b>	Electrical signal or bits	Frame (L2 Switch) Frame & Packet (L3 switch)	<b>Transmission Type</b>	Hubs always perform frame flooding; may be unicast, multicast or broadcast	First broadcast; then unicast & multicast as needed.	<b>Ports</b>	4/12 ports	Switch is multi port Bridge. 24/48 ports	<b>Device Type</b>	Passive Device (Without Software)	Active Device (With Software) & Networking device	<b>Used in (LAN, MAN, WAN)</b>	LAN	LAN	<b>Table</b>	A network hub cannot learn or store MAC address.	Switches use content accessible memory CAM table which is typically accessed by ASIC (Application Specific Integrated chips).	<b>Transmission Mode</b>	Half duplex	Half/Full duplex	<b>Broadcast Domain</b>	Hub has one Broadcast Domain.	Switch has one broadcast domain [unless VLAN implemented]	<b>Definition</b>	An electronic device that connects many network device together so that devices can exchange data	A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send msg to device that needs or request it	<b>Spanning-Tree</b>	No Spanning-Tree	Many Spanning-tree Possible	<b>Collisions</b>	Collisions occur commonly in setups using hubs.	No collisions occur in a full-duplex switch.
	Hub	Switch																																										
<b>Layer</b>	Physical layer. Hubs are classified as Layer 1 devices per the OSI model.	Data Link Layer. Network switches operate at Layer 2 of the OSI model.																																										
<b>Function</b>	To connect a network of personal computers together, they can be joined through a central hub.	Allow to connect multiple device and port can be manage, Vlan can create security also can apply																																										
<b>Data Transmission form</b>	Electrical signal or bits	Frame (L2 Switch) Frame & Packet (L3 switch)																																										
<b>Transmission Type</b>	Hubs always perform frame flooding; may be unicast, multicast or broadcast	First broadcast; then unicast & multicast as needed.																																										
<b>Ports</b>	4/12 ports	Switch is multi port Bridge. 24/48 ports																																										
<b>Device Type</b>	Passive Device (Without Software)	Active Device (With Software) & Networking device																																										
<b>Used in (LAN, MAN, WAN)</b>	LAN	LAN																																										
<b>Table</b>	A network hub cannot learn or store MAC address.	Switches use content accessible memory CAM table which is typically accessed by ASIC (Application Specific Integrated chips).																																										
<b>Transmission Mode</b>	Half duplex	Half/Full duplex																																										
<b>Broadcast Domain</b>	Hub has one Broadcast Domain.	Switch has one broadcast domain [unless VLAN implemented]																																										
<b>Definition</b>	An electronic device that connects many network device together so that devices can exchange data	A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send msg to device that needs or request it																																										
<b>Spanning-Tree</b>	No Spanning-Tree	Many Spanning-tree Possible																																										
<b>Collisions</b>	Collisions occur commonly in setups using hubs.	No collisions occur in a full-duplex switch.																																										

Q.9	Explain following devices. a) Router b) Bridge
Ans.	<p><b>Router</b></p> <p>A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each point-of-presence on the Internet. A router is often included as part of a network switch.</p> <p><b>Bridge</b></p> <p>A <b>bridge</b> is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or Token Ring). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street.</p> 

## Chapter 5: Reference Models

Q.1	State functions of Network layer							
Ans	<p>Functions of network layer:</p> <ol style="list-style-type: none"><li>1. Logical addressing</li><li>2. Routing.</li><li>3. Congestion control</li><li>4. Accounting and billing</li><li>5. Address transformation</li><li>6. Source host to destination host error free delivery of packet.</li></ol>							
Q.2	Draw and explain layered architecture of OSI model.							
Ans	<p>OSI model (Open System Interconnection) model was developed by ISO (international standard organization) which provides way to understand how internetwork operates. It gives guidelines for creating network standard.</p> <p>OSI model has 7 layers as shown in the figure. Application Layer, Presentation Layer ,Session Layer ,Transport Layer ,Network Layer ,Data link Layer and Physical Layer</p> <p><b>Physical (Layer 1)</b> OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects.</p> <p><b>Data Link (Layer 2)</b> At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.</p> <table><tr><td>Application Layer</td></tr><tr><td>Presentation Layer</td></tr><tr><td>Session Layer</td></tr><tr><td>Transport Layer</td></tr><tr><td>Network Layer</td></tr><tr><td>Data link Layer</td></tr><tr><td>Physical Layer</td></tr></table> <p>OSI Model</p>	Application Layer	Presentation Layer	Session Layer	Transport Layer	Network Layer	Data link Layer	Physical Layer
Application Layer								
Presentation Layer								
Session Layer								
Transport Layer								
Network Layer								
Data link Layer								
Physical Layer								

	<p><b>Network (Layer 3)</b> Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.</p> <p><b>Transport (Layer 4)</b> Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer from source to destination.</p> <p><b>Session (Layer 5)</b> This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.</p> <p><b>Presentation (Layer 6)</b> This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax &amp; semantics.</p> <p><b>Application (Layer 7)</b> OSI Model, Layer 7, supports application and end-user processes. Everything at this layer is application-specific. This layer provides application services for file.</p>
<b>Q.3</b>	<b>Draw and explain TCP/IP model.</b>
<b>Ans.</b>	<p>TCP/IP that is Transmission Control Protocol and Internet Protocol has following features</p> <ul style="list-style-type: none"> <li>• Support for a flexible architecture. Adding more machines to a network was easy.</li> <li>• The network is robust, and connections remained intact until the source and destination machines were functioning. The main idea was to allow one application on one computer to talk to (send data packets) another application running on different computer.</li> </ul> <p>Different Layers of TCP/IP Reference Model Below:</p> <p><b>Layer 1: Host-to-network Layer</b></p> <ol style="list-style-type: none"> <li>1. Lowest layer of the all.</li> <li>2. Protocol is used to connect to the host, so that the packets can be sent over it.</li> <li>3. Varies from host to host and network to network.</li> </ol>

**Layer 2: Internet layer**

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called an internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer. The various functions performed by the Internet Layer are:
  - o Delivering IP packets
  - o Performing routing
  - o Avoiding congestion

**Layer 3: Transport Layer**

1. It decides if data transmission should be on a parallel path or a single path.
2. Functions such as multiplexing, segmenting or splitting of the data is done by the transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arranges the packets to be sent, in sequence.

**Layer 4: Application Layer**

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. Telnet is a two-way communication protocol which allows connecting to a remote machine and running applications on it.
2. FTP (File Transfer Protocol) is a protocol that allows file transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP.

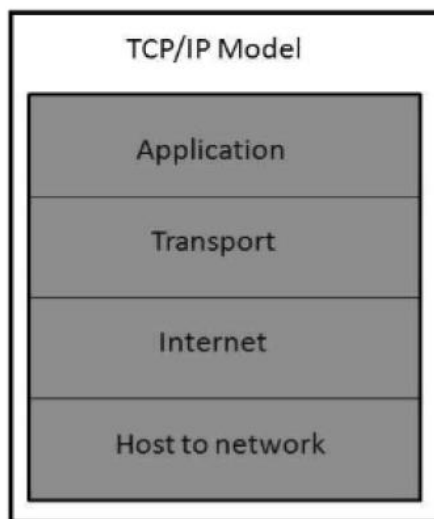


Fig: TCP/IP reference model

<b>Q.4</b>	<b>Describe the major functions of network layer in TCP/IP protocol suite</b>
<b>Ans.</b>	<p><b>Internetworking:</b> This is the main duty of network layer. It provides the logical connection between different types of networks.</p> <p><b>Addressing:</b> Addressing is necessary to identify each device on the internet uniquely. This is similar to telephone system. The address used in the network layer should uniquely and universally define the connection of a computer.</p> <p><b>Routing:</b> In a network, there are multiple roots available from a source to a destination and one of them is to be chosen. The network layer decides the root to be taken. This is called as routing.</p> <p><b>Packetizing:</b> The network layer encapsulates the packets received from upper layer protocol and makes new packets. This is called as packetizing. It is done by a network layer protocol called IP (Internetworking Protocol).</p>
<b>Q.5</b>	<b>State the functions of any two layers of OSI Model</b>
<b>Ans.</b>	<p><b>Functions of the physical layer are :</b></p> <ol style="list-style-type: none"> <li>1. <b>Bit synchronization:</b> The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.</li> <li>2. <b>Bit rate control:</b> The Physical layer also defines the transmission rate i.e. the number of bits sent per second.</li> <li>3. <b>Physical topologies:</b> Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.</li> <li>4. <b>Transmission mode:</b> Physical layer also defines the way in which the data flows between the two connected devices. The various transmission</li> </ol>

modes possible are: Simplex, half-duplex and full-duplex.

**Functions of data link layer:**

1. **Framing:** Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.
2. **Addressing:** Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
3. **Synchronization:** When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
4. **Error Control:** Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
5. **Flow Control:** Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.
6. **Multi-Access:** When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

**Functions of the Network layer are as follows:**

1. It is responsible for routing packets from the source host to the destination host. The routes can be based upon static tables that are rarely changed, or they can be automatically updated depending upon network conditions.
2. The data link layer assigns the physical address locally. When the data packets are routed to remote locations, a logical addressing scheme is required to differentiate between the source system and the destination system. This is provided by the network layer.
3. This layer also provides mechanisms for congestion control.
4. The network layer tackles issues like transmission delays, transmission time, avoidance of jitters, etc.



**Functions of Transport Layer**

1. **Service Point Addressing:** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling:** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
3. **Connection Control:** It includes 2 types:
  - a. **Connectionless Transport Layer:** Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
  - b. **Connection Oriented Transport Layer:** Before delivering packets, connection is made with transport layer at the destination machine.
4. **Flow Control:** In this layer, flow control is performed end to end.
5. **Error Control:** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

**Functions of the Session layer are :**

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is resynchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**Functions of the presentation layer are :**

1. **Translation:** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for

	<p>encrypting as well as decrypting data.</p> <p>3. <b>Compression:</b> Reduces the number of bits that need to be transmitted on the network.</p> <p><b>Functions of the Application layer are :</b></p> <ol style="list-style-type: none"><li>1. Network Virtual Terminal</li><li>2. FTAM-File transfer access and management</li><li>3. Mail Services</li><li>4. Directory Services</li></ol>
<b>Q.6</b>	<b>Describe types of IP address classes.</b>
<b>Ans.</b>	<p><b>Class A:</b> Class A range for first byte is 0-127. Class A type of IP addresses have First byte consisting of Network address with first bit as 0 and the next 3 bytes with host id. Hence, number of hosts are more when compared to number of networks. The default subnet masks for class A networks is 255.0.0.0. Class A networks have their network addresses from 1.0.0.0 to 126.0.0.0, with the zero's being replaced by node addresses.</p> <p><b>Class B:</b> Class B range for first byte is 128-191. This type has first two bytes specifying network ID with starting two bits as 10 and last two bytes referring to host ID. The default subnet masks for class B is 255.255.0.0. Network addresses for these ranges from 128.0.0.0 to 191.0.0.0.</p> <p><b>Class C:</b> Class C range for first byte is 192-223. This class has first three bytes referring to network with starting bits as 110 and last byte signifies Host ID. Here, number of networks is more when compared to number of hosts in each network. The default subnet masks for class C is 255.255.255.0 The network IP addresses for these range from 192.0.0.0 to 223.0.0.0.</p> <p><b>Class D:</b> Class D range for first byte is 224-239 Class D is used for multicasting and its starting bits are 1110</p> <p><b>Class E:</b> Class E range for first byte is 240-255 .Class E is reserved for future use and its starting bits are 1111</p>

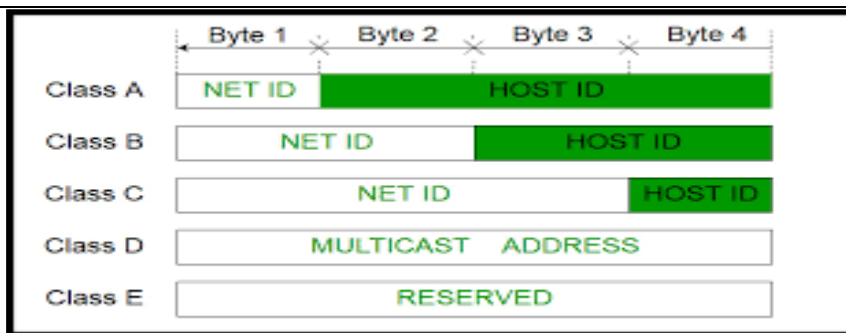


Fig : IP address classes

<b>Q.7</b>	<b>List classes of IP addressing with their IP address range.</b>
<b>Ans.</b>	<p>An IP address is an address used to uniquely identify a device on an IP network.</p> <p><b>Classes and range:</b></p> <p><b>Class A</b> - 1.0.0.1 to 126.255.255.254</p> <p><b>Class B</b> - 128.1.0.1 to 191.255.255.254</p> <p><b>Class C</b> - 192.0.1.1 to 223.255.254.254</p> <p><b>Class D</b> - 224.0.0.0 to 239.255.255.255</p> <p><b>Class E</b> - 240.0.0.0 to 254.255.255.254</p>
<b>Q.8</b>	<b>Your company has the network id 165.130.0.0. You are responsible for creating subnets on the network, and each subnet must provide at least 1000 host ids. What subnet mask meets the requirement for the minimum number of host ids and provides the highest number of subnets?</b>
<b>Ans.</b>	<p>The given network id 165.130.0.0 is class B (Range of class B is 128.0.0.0 to 191.255.255.255) with subnet mask of 255.255.252.0 creates 62 subnets with 1022 host each.</p> <p>In binary format subnet mask reads: 11111111.11111111.11111100.00000000.</p> <p>To calculate the number of host ids available for each subnet is based on the number of digits remaining in the network address.</p> <p>The number of possible host ids in each subnet ranges from 00000001 through 11111110.</p> <p>So, in the network 165.130.0.0/22, host addresses can range from 165.130.0.1 through 165.130.254</p>
<b>Q.9</b>	<b>Describe the process of DHCP server configuration.</b>
<b>Ans.</b>	<p>Configuring the DHCP Server</p> <p>To configure the DHCP server:</p> <ol style="list-style-type: none"> <li>1. From the Control Panel, go to Administrative Tools &gt;&gt; Computer Management &gt;&gt; Services and Application &gt;&gt; DHCP.</li> </ol>

2. From the Action menu, select New Scope. The New Scope wizard is displayed.
3. Enter the following information as prompted:
  - Scope name and description:
  - IP address range (for example, 192.168.0.170 to 192.168.0.171)
  - Subnet mask (for example, 255.255.255.0)
  - Add exclusions (do not exclude any IP addresses)
  - Lease duration (accept the default of 8 days)
  - Router (default gateway) of your subnet (for example, 192.168.0.1)
  - Domain name, WINS server (these are not needed)
  - Activate Scope? (select “Yes, I want to activate this scope now”)
4. Click Finish to exit the wizard. The contents of the DHCP server are listed.
5. Right-click Scope [iPad dress] scope-name and select Properties.
6. In the Scope Properties box, click the Advanced tab.
7. Select BOOTP only, set the lease duration to Unlimited, and click OK.
8. Right-click Reservations. The Controller A Properties box is displayed.
9. Enter the IP address and the MAC address for Controller A. Click Add. The Controller B Properties box is displayed.
10. Enter the IP address and the MAC address for Controller B. Click Add. The controllers are added to the right of the Reservations listing.
11. Right-click Scope [iPad dress] scope-name to disable the scope.
12. Click Yes to confirm disabling of the scope.
13. Right-click Scope and select Activate.

Q.10	Compare IPv4 with IPv6																																
Ans.	<table><tr><th>IP Service</th><th>IPv4</th><th>IPv6</th></tr><tr><td>IP header</td><td>Consists of a 20-byte field containing multiple fields.</td><td>Consists of a 40-byte field containing fewer fields, making it simpler, and provides better routing efficiency.</td></tr><tr><td>Addressing range</td><td>Requires a 32-bit dotted-decimal address to provide <math>4.3 \times 10^9</math> (4.3 billion) addresses.</td><td>Requires a 128-bit hexadecimal address to provide <math>3.4 \times 10^{28}</math> addresses with multiple scopes.</td></tr><tr><td>Address types</td><td>Includes unicast, multicast, and broadcast addresses.</td><td>Includes unicast, multicast, and anycast addresses. No broadcast addresses means that it is not susceptible to broadcast storms.</td></tr><tr><td>Autoconfiguration</td><td>Supports stateful configuration (Dynamic Host Configuration Protocol, DHCP).</td><td>Supports stateless autoconfiguration or stateful configuration (DHCPv6).</td></tr><tr><td>Security</td><td>IPsec must be configured.</td><td>IPsec is a mandatory part of the stack, but it still has to be configured.</td></tr><tr><td>Mobility</td><td>Mobility is not built in, but it supports mobile IP.</td><td>Mobile IP is built in, with optimized routing.</td></tr><tr><td>Quality of service (QoS)</td><td>Supports differentiated service and integrated service.</td><td>Supports differentiated service and integrated service, but the header compresses better because of fewer fields.</td></tr><tr><td>IP multicast</td><td>Heavy application use.</td><td>Heavy application and protocol stack use.</td></tr><tr><td>ICMP</td><td>Mostly used to provide messaging information.</td><td>Used extensively to provide messaging and protocol functions.</td></tr></table>			IP Service	IPv4	IPv6	IP header	Consists of a 20-byte field containing multiple fields.	Consists of a 40-byte field containing fewer fields, making it simpler, and provides better routing efficiency.	Addressing range	Requires a 32-bit dotted-decimal address to provide $4.3 \times 10^9$ (4.3 billion) addresses.	Requires a 128-bit hexadecimal address to provide $3.4 \times 10^{28}$ addresses with multiple scopes.	Address types	Includes unicast, multicast, and broadcast addresses.	Includes unicast, multicast, and anycast addresses. No broadcast addresses means that it is not susceptible to broadcast storms.	Autoconfiguration	Supports stateful configuration (Dynamic Host Configuration Protocol, DHCP).	Supports stateless autoconfiguration or stateful configuration (DHCPv6).	Security	IPsec must be configured.	IPsec is a mandatory part of the stack, but it still has to be configured.	Mobility	Mobility is not built in, but it supports mobile IP.	Mobile IP is built in, with optimized routing.	Quality of service (QoS)	Supports differentiated service and integrated service.	Supports differentiated service and integrated service, but the header compresses better because of fewer fields.	IP multicast	Heavy application use.	Heavy application and protocol stack use.	ICMP	Mostly used to provide messaging information.	Used extensively to provide messaging and protocol functions.
IP Service	IPv4	IPv6																															
IP header	Consists of a 20-byte field containing multiple fields.	Consists of a 40-byte field containing fewer fields, making it simpler, and provides better routing efficiency.																															
Addressing range	Requires a 32-bit dotted-decimal address to provide $4.3 \times 10^9$ (4.3 billion) addresses.	Requires a 128-bit hexadecimal address to provide $3.4 \times 10^{28}$ addresses with multiple scopes.																															
Address types	Includes unicast, multicast, and broadcast addresses.	Includes unicast, multicast, and anycast addresses. No broadcast addresses means that it is not susceptible to broadcast storms.																															
Autoconfiguration	Supports stateful configuration (Dynamic Host Configuration Protocol, DHCP).	Supports stateless autoconfiguration or stateful configuration (DHCPv6).																															
Security	IPsec must be configured.	IPsec is a mandatory part of the stack, but it still has to be configured.																															
Mobility	Mobility is not built in, but it supports mobile IP.	Mobile IP is built in, with optimized routing.																															
Quality of service (QoS)	Supports differentiated service and integrated service.	Supports differentiated service and integrated service, but the header compresses better because of fewer fields.																															
IP multicast	Heavy application use.	Heavy application and protocol stack use.																															
ICMP	Mostly used to provide messaging information.	Used extensively to provide messaging and protocol functions.																															

Q.11	Compare OSI and TCP/IP network models																						
Ans.	<table><tr><th>TCP/IP</th><th>OSI</th></tr><tr><td>Implementation of OSI model</td><td>Reference model</td></tr><tr><td>Model around which Internet is developed</td><td>This is a theoretical model</td></tr><tr><td>Has only 4 layers</td><td>Has 7 layers</td></tr><tr><td>Considered more reliable</td><td>Considered a reference tool</td></tr><tr><td>Protocols are not strictly defined</td><td>Stricter boundaries for the protocols</td></tr><tr><td>Horizontal approach</td><td>Vertical approach</td></tr><tr><td>Combines the session and presentation layer in the application layer</td><td>Has separate session and presentation layer</td></tr><tr><td>Protocols were developed first and then the model was developed</td><td>Model was developed before the development of protocols</td></tr><tr><td>Supports only connectionless communication in the network layer</td><td>Supports connectionless and connection-oriented communication in the network layer</td></tr><tr><td>Protocol dependent standard</td><td>Protocol independent standard</td></tr></table>	TCP/IP	OSI	Implementation of OSI model	Reference model	Model around which Internet is developed	This is a theoretical model	Has only 4 layers	Has 7 layers	Considered more reliable	Considered a reference tool	Protocols are not strictly defined	Stricter boundaries for the protocols	Horizontal approach	Vertical approach	Combines the session and presentation layer in the application layer	Has separate session and presentation layer	Protocols were developed first and then the model was developed	Model was developed before the development of protocols	Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer	Protocol dependent standard	Protocol independent standard
TCP/IP	OSI																						
Implementation of OSI model	Reference model																						
Model around which Internet is developed	This is a theoretical model																						
Has only 4 layers	Has 7 layers																						
Considered more reliable	Considered a reference tool																						
Protocols are not strictly defined	Stricter boundaries for the protocols																						
Horizontal approach	Vertical approach																						
Combines the session and presentation layer in the application layer	Has separate session and presentation layer																						
Protocols were developed first and then the model was developed	Model was developed before the development of protocols																						
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer																						
Protocol dependent standard	Protocol independent standard																						
Q.12	Define Subnet and Supernet.																						
Ans.	<p>A <b>subnet</b> is a logical partition of an IP network into multiple, smaller network segments. It is typically used to subdivide large networks into smaller, more efficient subnetworks.</p> <p>A <b>supernet</b> is created by combining several Internet Protocol (IP) networks or subnets into one network with a single classless interdomain routing (CIDR) prefix. The new combined network has the same routing prefix as the collection of the prefixes of the subnets. The procedure used to create a supernet is commonly called supernetting.</p>																						

Q.13	Differentiate between TCP and UDP.																																	
Ans.	<table><tr><th colspan="3">UDP v/s TCP</th></tr><tr><th>Characteristics/Description</th><th>UDP</th><th>TCP</th></tr><tr><td>General Description</td><td>Simple High speed low functionality “wrapper” that interface applications to the network layer and does little else</td><td>Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.</td></tr><tr><td>Protocol connection Setup</td><td>Connection less data is sent without setup</td><td>Connection-oriented; Connection must be Established prior to transmission.</td></tr><tr><td>Data interface to application</td><td>Message base-based is sent in discrete packages by the application.</td><td>Stream-based; data is sent by the application with no particular structure</td></tr><tr><td>Reliability and Acknowledgements</td><td>Unreliable best-effort delivery without acknowledgements</td><td>Reliable delivery of message all data is acknowledged.</td></tr><tr><td>Retransmissions</td><td>Not performed. Application must detect lost data and retransmit if needed.</td><td>Delivery of all data is managed, and lost data is retransmitted automatically.</td></tr><tr><td>Features Provided to Manage flow of Data</td><td>None</td><td>Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms</td></tr><tr><td>Overhead</td><td>Very Low</td><td>Low, but higher than UDP</td></tr><tr><td>Transmission speed</td><td>Very High</td><td>High but not as high as UDP</td></tr><tr><td>Data Quantity Suitability</td><td>Small to moderate amounts of data.</td><td>Small to very large amounts of data.</td></tr></table>	UDP v/s TCP			Characteristics/Description	UDP	TCP	General Description	Simple High speed low functionality “wrapper” that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.	Protocol connection Setup	Connection less data is sent without setup	Connection-oriented; Connection must be Established prior to transmission.	Data interface to application	Message base-based is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure	Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged.	Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.	Features Provided to Manage flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms	Overhead	Very Low	Low, but higher than UDP	Transmission speed	Very High	High but not as high as UDP	Data Quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data.
UDP v/s TCP																																		
Characteristics/Description	UDP	TCP																																
General Description	Simple High speed low functionality “wrapper” that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.																																
Protocol connection Setup	Connection less data is sent without setup	Connection-oriented; Connection must be Established prior to transmission.																																
Data interface to application	Message base-based is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure																																
Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged.																																
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.																																
Features Provided to Manage flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms																																
Overhead	Very Low	Low, but higher than UDP																																
Transmission speed	Very High	High but not as high as UDP																																
Data Quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data.																																
Q.14	Explain configuration of TCP/IP protocol in network																																	
Ans.	<p>Before beginning configuration procedure, the following are the prerequisites.</p> <ul style="list-style-type: none"><li>• Network hardware is installed and cabled. .</li><li>• TCP/IP software is installed.</li></ul> <p>To configure your TCP/IP network, the following steps are followed:</p> <ul style="list-style-type: none"><li>• Read TCP/IP protocols for the basic organization of TCP/IP.</li><li>• Minimally configure each host machine on the network.</li></ul> <p>This means adding a network adapter, assigning an IP address, and assigning a host name to each host, as well as defining a default route to your network. For background information on these tasks, refer to TCP/IP network interfaces, TCP/IP addressing, and Naming hosts on your network.</p> <ul style="list-style-type: none"><li>• Configure and start the intend daemon on each host machine on the network. Read TCP/IP daemons and then follow the instructions in Configuring the intend daemon.</li><li>• Configure each host machine to perform either local name resolution or to use a name server. If a hierarchical Domain Name networks being set up, configure at least one host to function as a name server.</li></ul>																																	

	<ul style="list-style-type: none"><li>• If the network needs to communicate with any remote networks, configure at least one host to function as a gateway. The gateway can use static routes or a routing daemon to perform inters network routing.</li><li>• Decide which services each host machine on the network will use. By default, all services are available. Follow the instructions in Client network services if you wish to make a particular service unavailable.</li><li>• Decide which hosts on the network will be servers, and which services a particular server will provide. Follow the instructions in Server network services to start the server daemons you wish to run.</li><li>• Configure any remote print servers that are needed.</li><li>• Optional: If desired, configure a host to use or to serve as the master time server for the network.</li></ul>
--	---