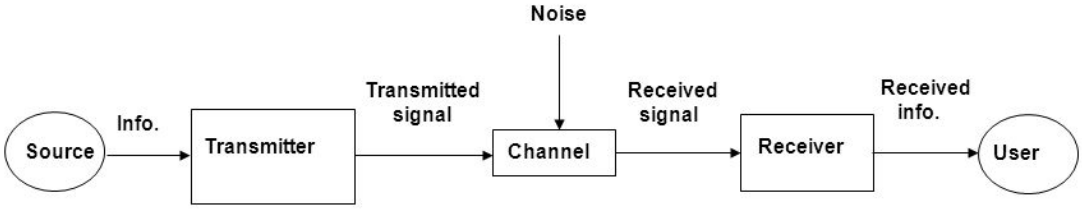
FOURTH SEMESTER B.C.A. DEGREE EXAMINATION, APRIL 2018

DATA COMMUNICATION

1.a)Define communication network. List the services of Network. -4M-

Ans:A communication network can be defined as "When two or more devices are connected together through a wired medium or wireless medium and If they are able to exchange information among them it forms a communication network."



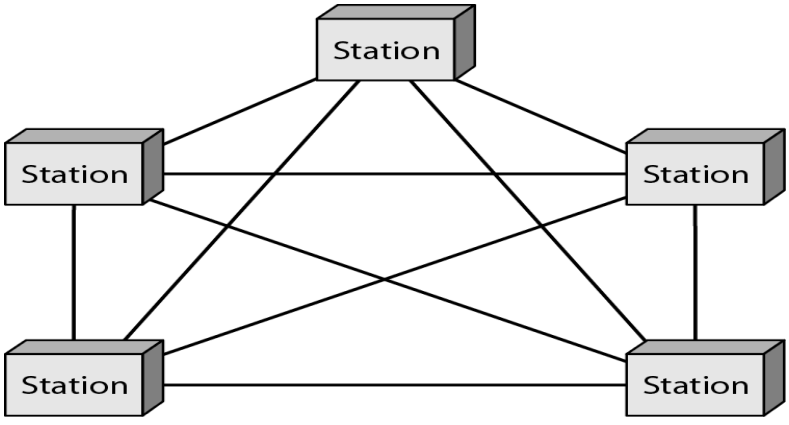
Services of Network

Email Services, Telephone Services, Telegram services, Mobile Services etc

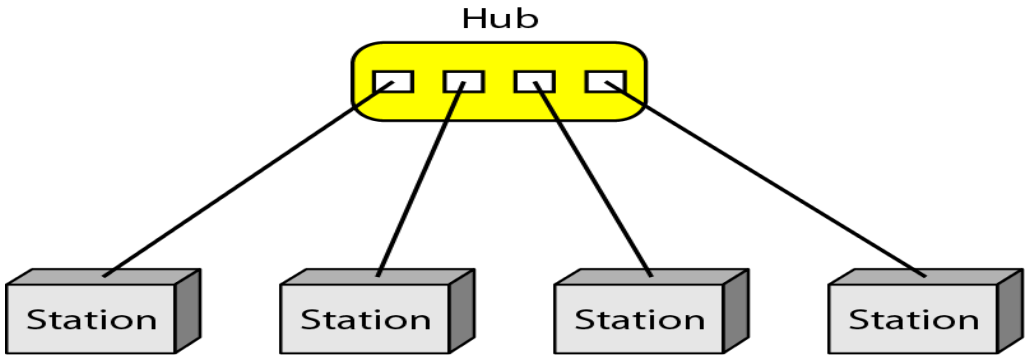
1.b)What is network topology? Explain different LAN topologies. -4M-

Ans: The term Network topology refers to the way in which a network is laid out physically. Two or more devices connect to form a link, two or more links form a topology. The topology of a network is the geometric representation of relationship of all the links and devices(nodes) to one another.

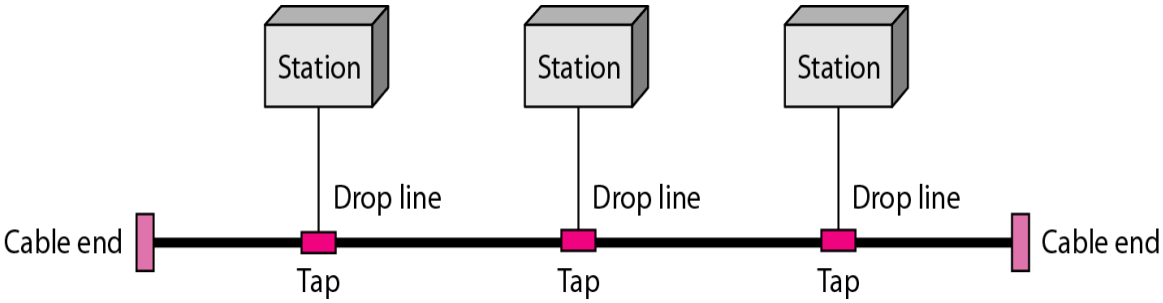
Mesh topology: It is used in some networks that do not have a large number of nodes involved.It is so named because each station has dedicated point to point link to every other station. It is robust if one link become unusable it doesn't incapacitate the entire system.



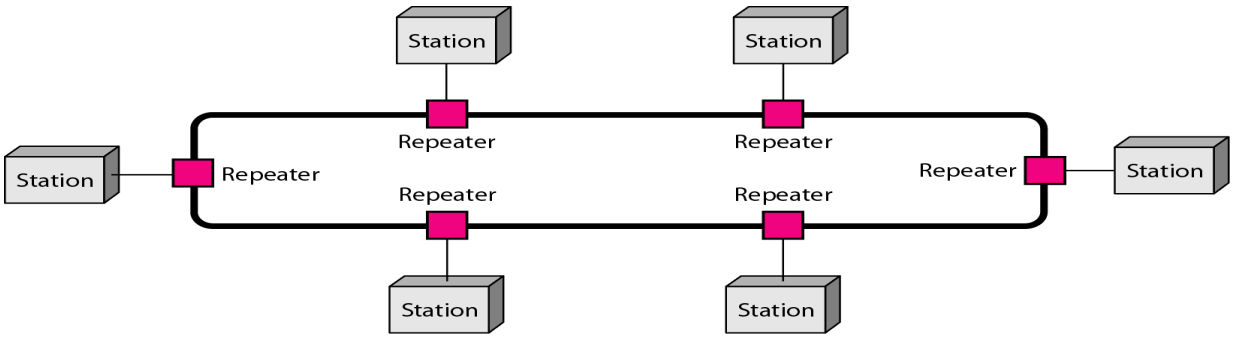
Star topology: In this topology, eachdevice has dedicated point to point link only to a central controller called HUB. The devices are not directly link to one another. It is widely used in networks that are based on private branch exchanges and message switches.



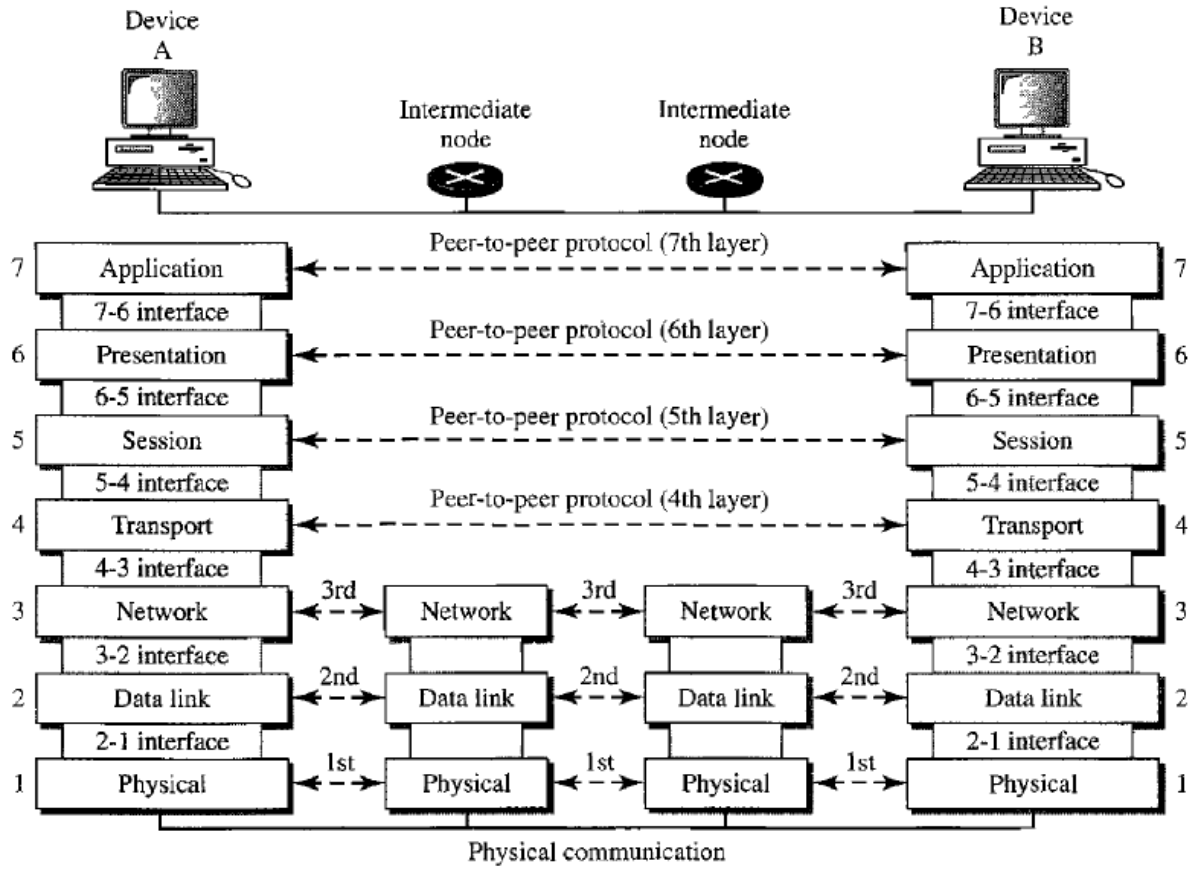
Bus topology: It has a multipoint connection. One long cable act as backbone to link all the devices in a network. Nodes are connected to the bus cable by droplines and tabs.



Ring topology: In this each device has a dedicated point to point connection with only two devices on either side of it. Each station is attached to the ring and receives all messages on the ring. The ring is usually unidirectional.



1.c)Explain the OSI reference model in detail. -8M-



1)Physical Layer :It coordinates the functions required to carry a bit stream over a physical medium. It deals with mechanical and electrical specifications of the interface and transmission medium. It is also responsible for physical characteristics of interface and medium, Transmission modes and physical topology.

2)Data Link Layer : It transforms the physical layer, It makes the physical layer appear error free to the upper layer. It is also responsible for framing of data packets, physical addressing, Error control and flow control.

3)Network Layer :It is responsible for the source to destination delivery of packets across multiple networks, whereas the datalink layer oversees the delivery of the packet between two systems on the same network, the network layer ensures that each packet delivered in different networks. It is responsible for logical addressing.

4)Transport Layer : It is responsible for process-to-process deliveryof the entire message. A process is an application program running on a host. Whereas network source-to-destination delivery of individual packets, it doesn't recognise any relationship between those packets.It is also responsible for segmentation and reassembly of data packets.

5)Session Layer :The services provided by the first three layers(Physical, Datalink and Network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains and synchronises the interaction among communication system.

6)Presentation Layer :It is concerned with the syntax and semantics of the information exchange between two systems. It is also responsible for Translation, Encryption and Compression.

7)Application Layer :It enables the user to access the network. It provide user interfaces and support applications. It is also responsible for File transfer, access and Network Virtual Terminal.

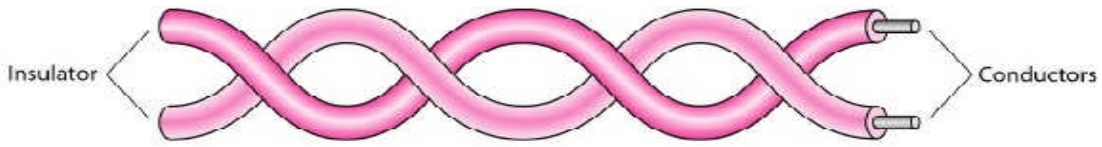
2.a)Define transmission medium. Explain twisted pair and co-axial transmission medium in detail. -8M-

Ans: A transmission medium can be defined as anything that can carry information from source to the destination.The transmission media are usually located below the physical layer and are directly controlled by the physical layer.

Eg:The transmission medium for two people having a conversation is the air.

In telecommunication, transmission media can be divided into Guided and Unguided media.Guided media are those that provide a transmission channel from one device to another. It includes Twisted pair, Coaxial cable and fibre optic table.

Twisted Pair Cable : It consists of two conductors which are insulated by using a plastic cover as shown in figure below. One of the wire is used to carry signals to the receiver and other is used only as aground reference.

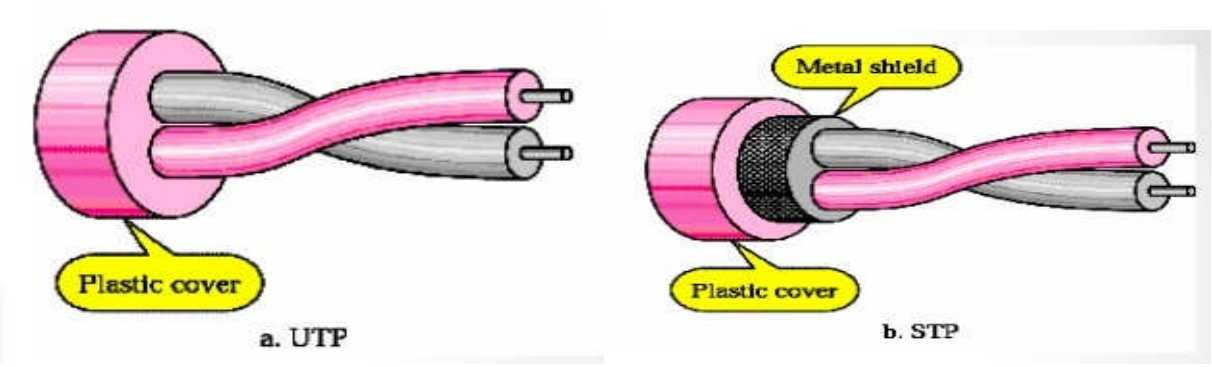


The most common twisted pair cable used in communication is Unshielded Twisted Pair (UTP). IBM has also produced a version of twisted pair cable called Shielded Twisted Pair (STP).

Applications:Twisted pair cables are used in telephone lines to provide voice and data channels. The local loop the line that connects subscribers to the central telephone office commonly consist of one Shielded Twisted pair cable.

The DSL lines that are used by the telephone companies to provide high data rate connections also used the high bandwidth capability of Unshielded Twisted Pair cable.

Local-area networks, such as 10Base-T and 100Base-T, also use Twisted Pair cables.



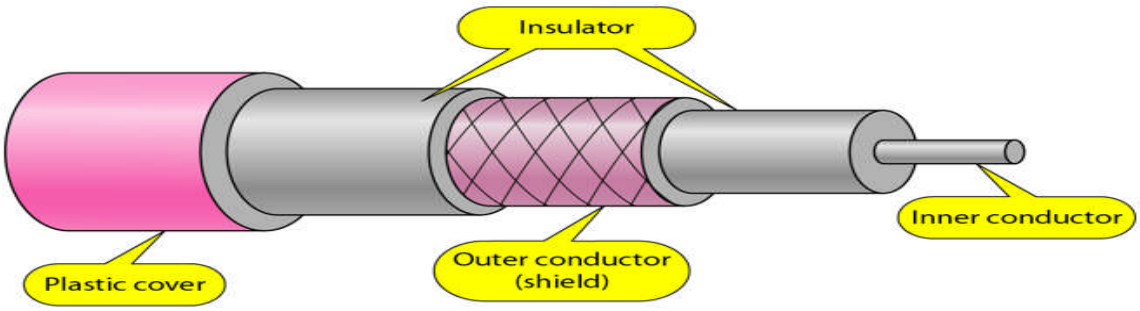
Coaxial Cable:It carries signal of higher frequency ranges then those in twisted pair cable because two media are constructed differently. Instead of having two wires coaxial has central core conductor usually copper enclosed in an insulating sheath which is intern covered with outer conductor of metal foil, braid or combination of the two. The outer metallic wrapping serves both as a sheath against noise also as second conductor which completes the circuit.

Applications:

Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600Mbps. However, coaxial cable in telephone network has largely been replaced today with fibre optic cable.

Cable TV networks also use coaxial cables. In the traditional cable TV network, The entire network use coaxial cable.

Another common application of coaxial cable is in traditional Ethernet LANs. Because of is high bandwidth and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs.



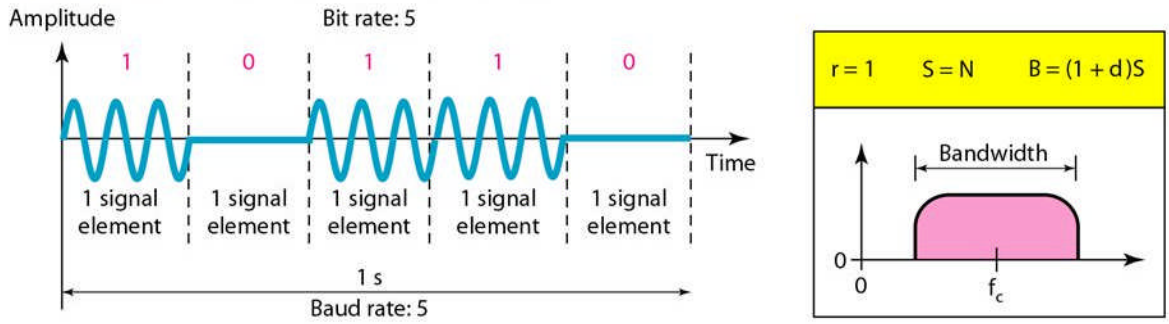
2.b)What is modulation? Explain Digital modulation. -8M-

Ans: Modulation is the process of superimposing the information contents of a modulating signal on a carrier signal(which of high frequency) by varying characteristic of carrier signal according to modulating signal.

Digital modulation includes 3 techniques

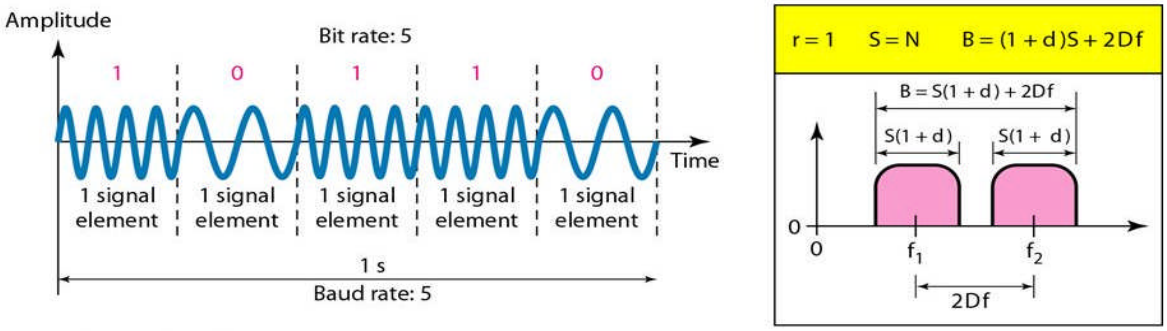
1)Amplitude Shift Keying (ASK)

- Strength of carrier signal is carried to represent binary 1 or 0.
- Both Frequency and Phase remain constant while Amplitude changes.
- Commonly one of the amplitudes is zero.
    - Advantage: It is simple.
    - Disadvantage: It is very susceptible to noise interface-noise usually affects amplitude, therefore ASK modulation technique most affected by noise.
    - Application: It is used to Transmit digital data over optical fibre.



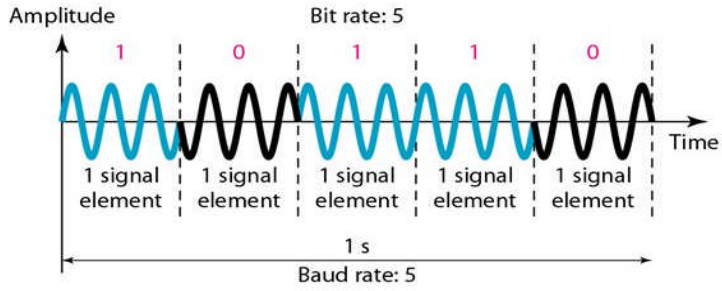
2)Frequency Shift Keying (FSK)

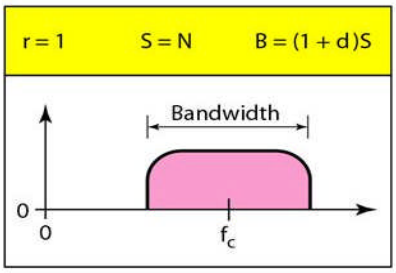
- It uses digital signal to adjust the frequency of wave carrier.
- Pros less susceptible to noise.
- Cons theoretically requires larger bandwidth than ASK.
- Popular in modern systems



3)Phase Shift Keying (PSK)

- Phase of carrier signal is varied to represent binary 1 or 0.
- Peak amplitude and Frequency remain constant during each bit interval.
    - Advantage: PSK is less susceptible to errors than ASK, while it requires the same bandwidth as ASK. More efficient use of bandwidth are possible, compared to FSK.
    - Disadvantage: more complex signal detection, recovery process than in ASK and FSK.





3.a)Distinguish between circuit switched network with packet switched network. -6M-

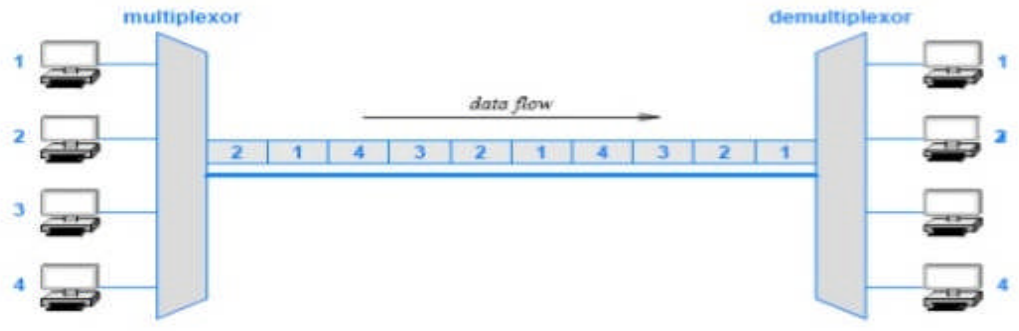
	Circuit Switched Network	Packet Switched Network
1	Done at physical layer.	Done at Network layer.
2	Direct physical connection between sender and receiver.	No direct specific path for transferring data so only data transfer takes place directly.
3	Since pre-defined path is there, There are 3 different stages like connection establishment, Data transfer and teardown/connection closing.	No specific path for transferring data so only data transfer takes place directly.
4	Total message goes at once so no header is required.	Since message gets segmented into different pieces, headers are required to identify at destination side.
5	Data will go as it is in the same order.	Data will go out of order and will be swapped.
6	Data processed only once at source.	At each intermediate network data will be processed including source.
7	If data is big, it is useful.	If data is small, packet switching is useful.
8	Guarantees that total message will be received with same order, So more reliable communication.	There is possibility that one of data packet may lose, so no reliable communication.
9	Requires more resources even for less communication.	Requires fewer resources.

3.b) Define Multiplexing. Explain TDM and WDM. -6M-

Ans: Multiplexing is a technique that allows simultaneous transmission of multiple signal lines into a single data link. Multiplexing is done using a device called Multiplexer that combine n input line to generate single output line.

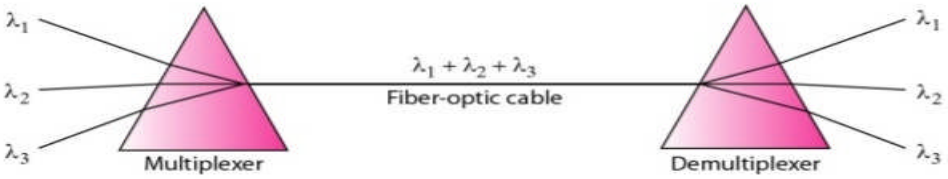
Time Division Multiplexing

- It is the digital multiplexing technique.
- Channel/Link is divided on the basis of time not on the basis of frequency.
- Total time available in the channel is divided between several users.
- Each user is allotted a particular time interval called Time slot or Slice.
- In TDM, the data rate capacity of transmission medium should be greater than the data rate required by sending device.



Wavelength Division Multiplexing: It is designed to use the high-data-rate capability of fibre optic cable.

- WDM is an Analog multiplexing technique.
- WDM is conceptually the same as FDM, except that multiplexing and demultiplexing involve optical signals transmitted through fibre optic channels.
- We are combining different signals of different frequencies. The difference is that the frequencies are very high.
- We want to combine multiple light sources into single light at multiplexer and do the reverse at the demultiplexer.



3.c) Write a short note on error detection. -4M-

Ans: Data can be corrupted during transmission. Some applications require that errors be detected and corrected. If the following two conditions are met, the receiver can detect a change in the original codeword.

i)The receiver has a list of valid codewords.

ii)The original codeword has changed to an invalid one.

The sender creates codewords out of datawords by using a generator that applies the rules and procedures of encoding. Each codeword sent to the receiver may change during transmission. If the received codeword is the same as one of the valid codewords, the word is accepted; the corresponding dataword is extracted for use. If the received codeword is not valid, it is discarded. However, if the codeword is corrupted during transmission but the received word is still matches a valid codeword, the error remains undetected. This is type of coding can be detect only single errors. Two or more errors may remain undetected.

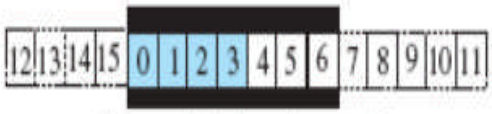
4.a)What are sliding window protocol? Explain types of sliding window protocol. -8M-

Ans: Since the sequence numbers use modulo 2*m*, a circle can represent the sequence numbers from 0 to 2*m* −1. The buffer is represented as a set of slices, called the***sliding window,*** that occupies part of the circle at any time.

At the sender site, when apacket is sent, the corresponding slice is marked. When all the slices are marked, it meansthat the buffer is full and no further messages can be accepted from the application layer.

When an acknowledgment arrives, the corresponding slice is unmarked. If some consecutive slices from the beginning of the window are unmarked, the window slides overthe range of the corresponding sequence numbers to allow more free slices at the end of thewindow. The sliding window at the sender. The sequence numbers arein modulo 16 ($m = 4$) and the size of the window is 7. Note that the sliding window is justan abstraction: the actual situation uses computer variables to hold the sequence numbersof the next packet to be sent and the last packet sent.

Most protocols show the sliding window using linear representation. The idea is the same, but it normally takes less space on paper.

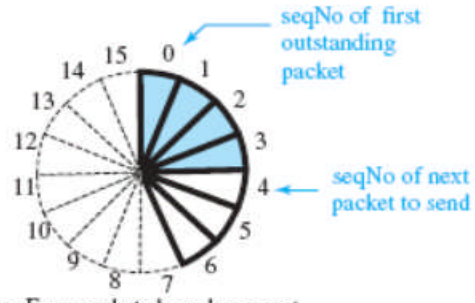


a. Four packets have been sent.

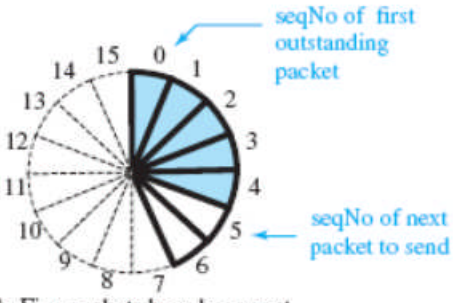
b. Five packets have been sent.

c. Seven packets have been sent; window is full.

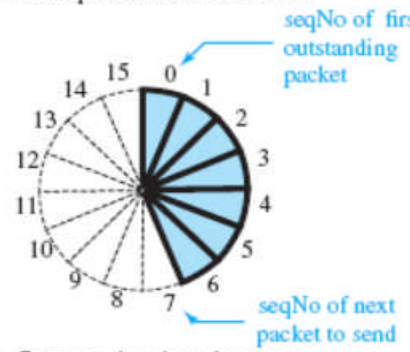
d. Packet 0 has been acknowledged; window slides.



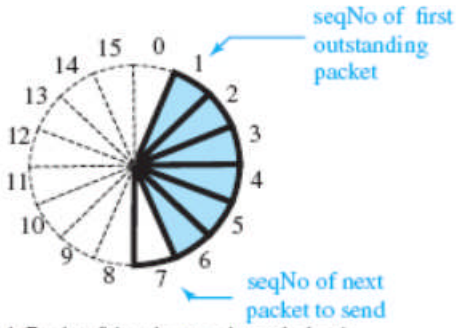
a. Four packets have been sent.



b. Five packets have been sent.



c. Seven packets have been sent; window is full.

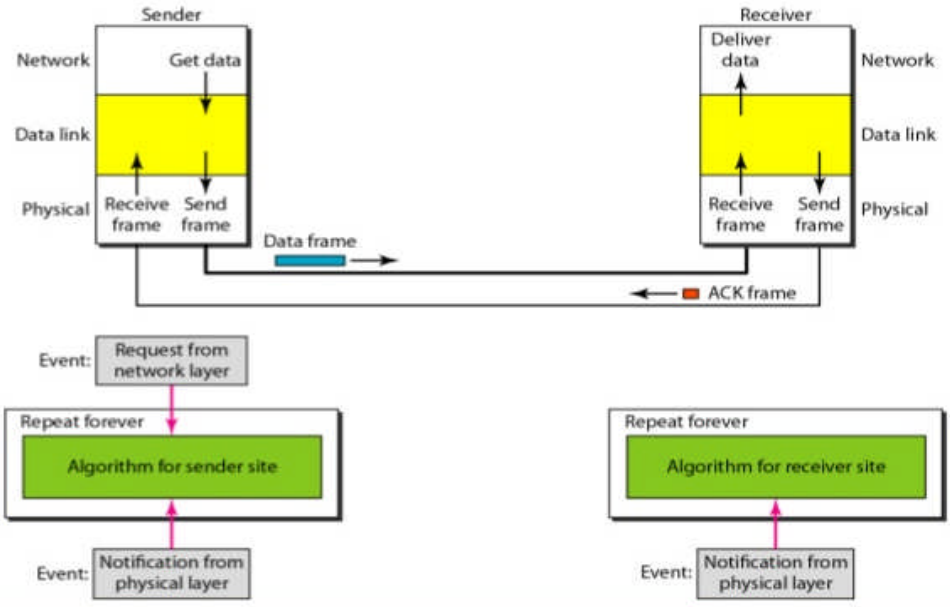


d. Packet 0 has been acknowledged; window slides.

4.b)Define ARQ. Explain stop and wait ARQ in detail. **-8M-**

Ans: Automatic Repeat Request is a protocol for error control in data transmission when the receiver detects an error in the packet it automatically requests the transmitter to resend the packet.

Stop-and-wait ARQ



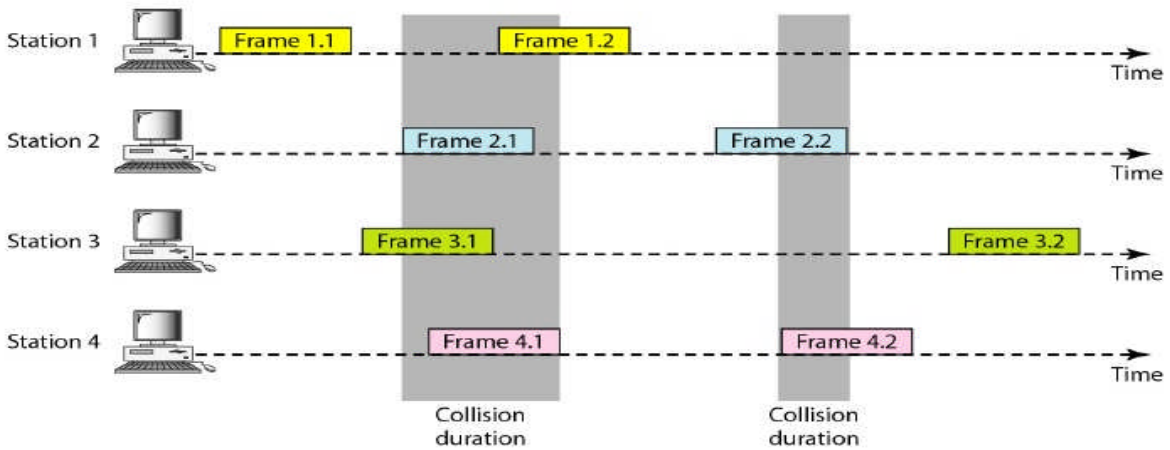
In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one. To detect corrupted frames, we need to add a CRCto each data frame. When a frame arrives at the receiver site, it ischecked. If its CRC is incorrect, the frame is corrupted and silently discarded. Thesilence of the receiver is a signal for the sender that a frame was either corrupted or lost.Every time the sender sends a frame, it starts a timer. If an acknowledgment arrivesbefore the timer expires, the timer is stopped and the sender sends the next frame (if ithas one to send). If the timer expires, the sender resends the previous frame, assumingthat the frame was either lost or corrupted. This means that the sender needs to keep a copy of the frame until its acknowledgment arrives. When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.Error detection in Stop-and-wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the time expires. In Stop-and-wait ARQ, we use sequence numbers to number the frames. The sequence numbers are based on modulo-2 arithmetic. In Stop-and -wait ARQ, the acknowledgement number always announces in modulo-2arithmetic the sequence number of the next frame expected.

5.a)What is Aloha? Explain two types of Aloha. -6M-

Ans: In 1970 Norman Abramson and his colleagues devised a new and elegant method to solve channel allocation problem. Abramson's work, called ALOHA system, used ground-based ratio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.There are two types of aloha-Pure and Slotted.

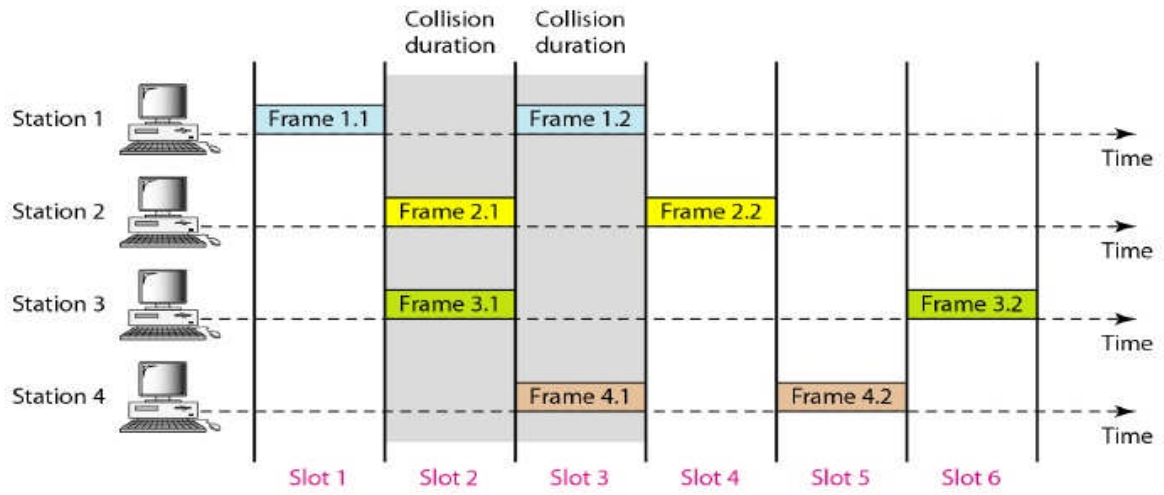
Pure Aloha :The basic idea of aloha system is simple.Let users transmit whenever they have data to be sent. There will be collisions, of course, and the colliding frames will be damaged. However due to the feedback property of broadcasting, a sender can always find out whether its frame was destroyed by listening to the channel, the same way the other users do.

- If you have a packet just send it.
- If multiple people try it and so there is collision then try resending it later.
- Theoretical analysis(based on Passion distribution)shows through put of 18% to reach the destination.



Slotted Aloha :

- Synchronous that is time is divided into slots.
- Slot size is equal to the transmission time of packet.
- When you are ready to transmit at the start of the time slot.
- Doubles the efficiency of Aloha.
- But requires Synchronisation.



5.b)Explain all CSMA protocols. -6M-

Ans: Carrier Sense Multiple Access (CSMA) is a network protocol that listens to or senses network signals on the carrier /medium before transmitting any data.

Persistent and nonpersistent CSMA protocols are an improvement over ALOHA because they ensure that no station begins to transmit when it senses the channel busy. Another improvement is for stations to abort their transmissions as soon as they detect a collision. In other words, if two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately. Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the collection is detected. Quickly terminating damaged frames saves time and bandwidth.

This protocol, known as CSMA/CD(CSMA with Collision Detection) is widely used on LANs in the MAC sublayer. In particular, it is the basis of the popular Ethernet LAN, so it is worth devoting some time to looking at it in detail. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments

5.c)Write a note on PPP. -4M-

Ans: One of the most common protocols for point-to-point access is the **Point-to-Point Protocol (PPP).** Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer. But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data-link layer. PPP is by far the most common.

Services of PPP

- PPP defines the format of the frame to be exchanged between devices.
- It also defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP is designed to accept payloads from several network layers (not only IP). Authentication is
- also provided in the protocol, but it is optional.
- The new version of PPP, called *Multilink PPP*, provides connections over multiple links. One interesting feature of PPP is that it providesnetwork address configuration.
- This is particularly useful when a home user needs atemporary network address to connect to the Internet

6.a) Explain IEEE 802-3 frame structure in detail. -8M-

Ans:

Preamble :The first field of the 802.3frame contains 7 bytes(56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not part of the frame.

Start Frame Delimiter (SFD):The second field signals(1byte) the beginning of the frame. The SFD warns the stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

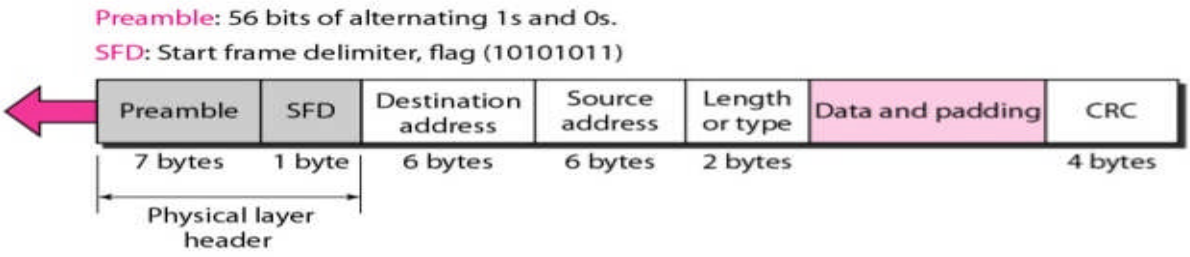
Destination Address:The DA field is of 6 bytesand contains the physical address of the destination stations to receive the packet.

Source Address: The SA field is of 6 bytes and contains the physical address of the sender of the packet.

Length or Type: The original Ethernet used this field as type field to define the upper layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.

Data :This field carries data encapsulated from the upper-layer protocols. It is minimum of 46 and a maximum of 1500 bytes.

CRC :The last field contains error detection information, in this case a CRC-32



6.b) Explain the term: -8M-

6.b.i) Reservation system

In the**reservation**method, a station needs to make a reservation before sending data.Time is divided into intervals. In each interval, a reservation frame precedes the dataframes sent in that interval.If there are *N* stations in the system, there are exactly *N* reservation minislots in thereservation frame. Each minislot belongs to a station. When a station needs to send adata frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame.

6.b.ii) Token passing

On a local area network, Token passing is a channel access method where a signal called a token is passed between nodes to authorize that node to communicate. In contrast to polling access methods, there is no pre-defined “master” node.

6.c.iii) LLC layer

In the IEEE 802 reference model of computer networking, the logical link control(LLC) data communication protocol layer is the upper sublayer of the data link layer of the seven layer of OSI reference model. The LLC sublayer acts as an interface between the media access control(MAC) sublayer and network layer.

6.b.iv) Random access

In **random-access** or **contention** methods, no station is superior to another station and none is assigned control over another. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy). In other words, each station can transmit when it desires on the condition that it follows the predefined procedure, including testing the state of the medium.

7.a) What is routing in network? Compare static routing with Dynamic routing. -6M-

Ans: In routing a packet is routed, hop by hop, from its source to its destination bythe help of forwarding tables. The source host needs no forwarding table because itdelivers its packet to the default router in its local network. The destination host needsno forwarding table either because it receives the packet from its default router in its
local network.

Static Routing	Dynamic Routing
The static routing algorithm do not base their routing decision on measurements of the current traffic and topology. Instead the choice of the route to use is computed in advance of line and downloaded to the routers when the network is booted or started. It includes the following algorithms- i)Flooding Algorithm ii)Bellman-Ford Algorithm iii)Dijkstra's Algorithm	In adaptive /dynamic routing the router changes the routes based on the traffic and topology while routing data packets. The router also reacts to congestion. The router reacts accordingly and decides the path through which the packets have to be sent. It includes the following algorithms i)Distance Vector algorithm ii)Link State Algorithm iii)HierarchicalAlgorithm

7.b)Explainshortest path first routing algorithm. -6M-

Ans: To create a least-cost tree for itself, using the shared LSDB, each node needs to run the famous **Dijkstra Algorithm.** This iterative algorithm uses the following steps:
1.The node chooses itself as the root of the tree, creating a tree with a single node, and sets the total cost of each node based on the information in the LSDB.
2. The node selects one node, among all nodes not in the tree, which is closest to the root, and adds this to the tree. After this node is added to the tree, the cost of all other nodes not in the tree needs to be updated because the paths may have been changed.
3. The node repeats step 2 until all nodes are added to the tree.

The heart of distance-vector routing is the famous **Bellman-Ford** equation. This equation is used to find the least cost (shortest distance) between a source node, ***x***, and a destination node, ***y***, through some intermediary nodes (**a, b, c,** . . .) when the costs between the source and the intermediary nodes and the least costs between the intermediary nodes and the destination are given. The following shows the general case in which D***ij***is the shortest distance and c***ij***is the cost between nodes ***I***and ***j***.
D*xy*= min {(c*xa*+ D*ay*), (c*xb*+ D*by*), (c*xc* + D*cy*), }

In distance-vector routing, normally we want to update an existing least cost with a least cost through an intermediary node, such as ***z***, if the latter is shorter. In this case, the equation becomes simpler, as shown below:

7.c) Write a note on leakybucket algorithm. -4M-

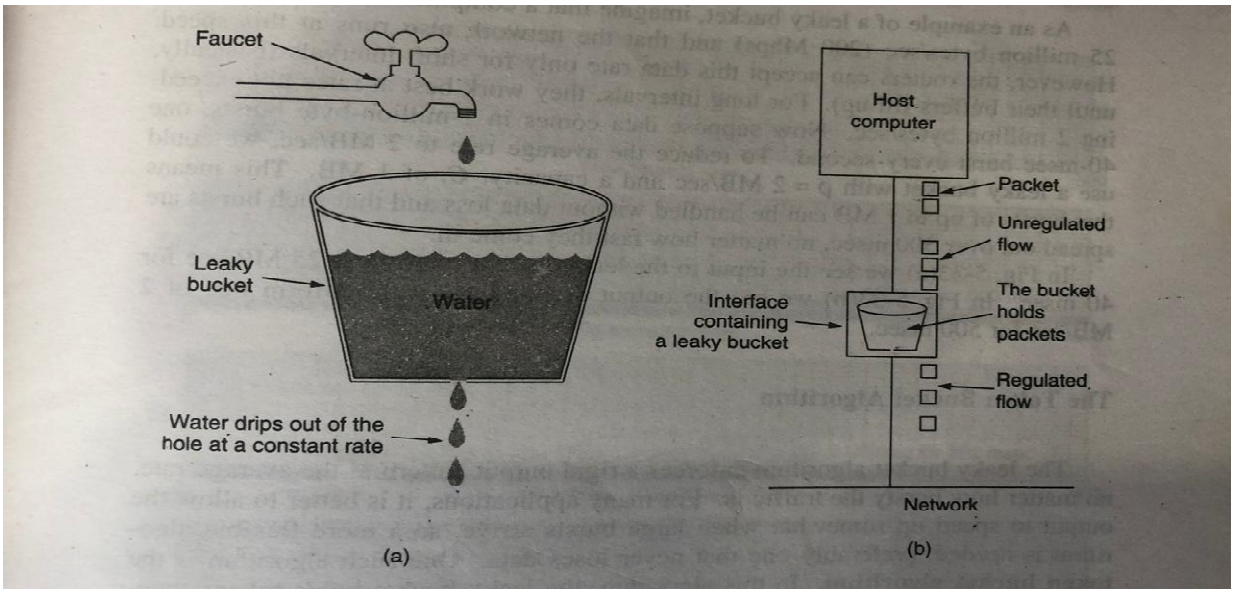
Ans: Leaky bucket algorithm is a method of temporarily storing a variable number of requests and organising them into a set-rate output of packets in an asynchronous transfer mode(ATM) network.

The leaky bucket is used to implement traffic policing and traffic shaping in Ethernet and cellular data networks. The algorithm can also be used to control metered-bandwidth internet connections to prevent going over the allotted bandwidth for a month, thereby avoiding extra charges.

The leaky algorithm works similarly to the way an actual leaky bucket hold water: The leaky bucket takes data and collects it up to a maximum capacity. Data in the bucket is only released

from the bucket at a set rate and size of packet. When the bucket runs out of data, the leaking stops. If incoming data would overfill the bucket, then the packet is considered to be non-conformant and is not added to the bucket. Data is added to the bucket as space becomes available for conforming packets.

The leaky bucket algorithm can also detect both gradually increasing and dramatic memory error increases by comparing how the average and peak data rates exceed set acceptable



background amounts.

8.Write short notes on: **-4M-**

8.a) Arpanet

ARPANET was the network that became the basis for the Internet. Based on a concept first published in 1967, ARPANET was developed under the direction of the U.S. Advanced Research Projects Agency (ARPA). In 1969, the idea became a modest reality with the interconnection of four university computers. The initial purpose was to communicate with and share computer resources among mainly scientific users at the connected institutions.

ARPANET took advantage of the new idea of sending information in small units called packets that could be routed on different paths and reconstructed at their destination. The development of the TCP/IP protocols in the 1970s made it possible to expand the size of the network, which now had become a network of networks, in an orderly way.

Because ARPA's name was changed to Défense Advanced Research Projects Agency (DARPA) in 1971, ARPANET is sometimes referred to as DARPANET. (DARPA was changed back to ARPA in 1993 and back to DARPA again in 1996.) The history of ARPANET and developments leading up to today's Internet.

8.b) Bridge: A network bridge is a computer networking device that creates a single aggregate network from multiple communication network segments. This function is called network bridging. Bridging distinct from routing.

First many university and corporate departments have their own LANs, primarily to connect their own personal computers, workstations, and servers. Since the goals of the various departments differ. Different department choose different LANs, without regard to what other departments are doing. Sooner or later, there is a need for interaction, so bridges are needed.

Second, the organisation may be geographically spread over several buildings separated by considerable distances.It may be cheaper to have separate LANs in each building and connect them with bridges and laser links than to run a single cable over the entire site.

Third, it may be necessary to split what is logically a single LAN into separate LANs to accommodate the load. At many universities, for example, thousands of workstations are available for student and faculty computing. Files are normally kept on file server machines and are downloaded to users' machine upon request.

8.c) IP

IP stands for Internet Protocol. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine with IP with a higher-level protocol called transmission Control Protocol (TCP) which establishes a virtual connection between a destination and a Source.

- It allows you to address a package and drop it in the system, but there's no direct link between you and recipient.
- Internet Protocol defines the basic unit of data transfer (IP Datagram).
- IP softwareperforms the routing function.
- IP includes a set of rules that process the idea of unreliable packet delivery.
    - How hosts and routers should process packets.
    - The conditions under which packets can be discarded.
    - How and When error messages should be generated.

8.d) Microwaves

Microwave radiation are movement in which microwave energy travels. The wavelength can be from as long as one meter to as short as one millimetre. Microwaves have a frequency of 0.3GHz to 300GHz.

They are found between the radio waves and infrared waves in the electromagnetic spectrum. Microwaves takes a straight-line path. They can pass throughnon-metal materials but get reflected off metal surfaces. Microwaves are absorbed by materials that have a water content and produce heat.

Microwaves are used for unicast communication such as cellular telephones, satellite networks and wireless LANs. Higher frequency ranges cannot penetrate walls. Use directional Antennas-point to point line of sight communications.

8.e) Flooding

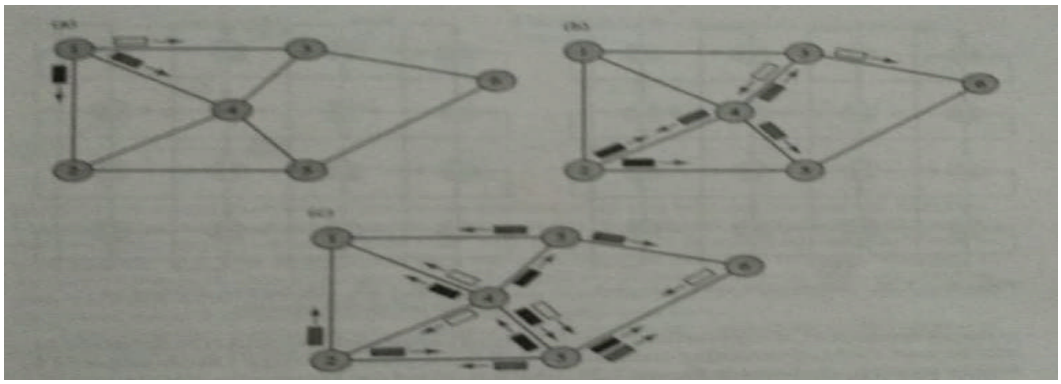
Flooding is a computer network routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on.

Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, including OSPF, DVMRP and those used in ad-hoc wireless networks.

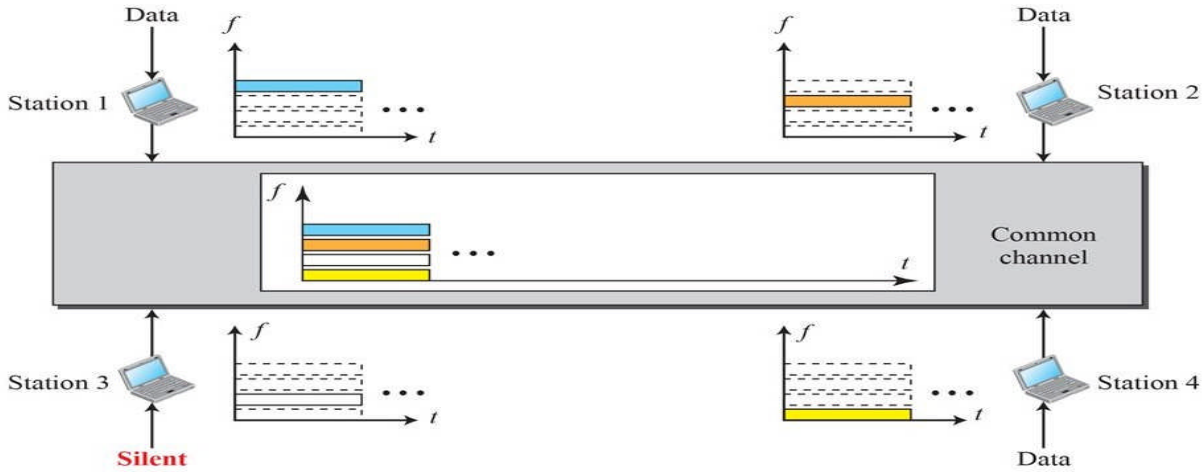
There are several varieties of flooding algorithms. Most work through as follows-

i)Each node act as both transmitter and a receiver.

ii)Each node tries to forward every message to every one of its neighbours except the source node.Algorithms may need to be more complex than this, since, in some case, precautions have to be taken to avoid wasted duplicate deliveries and infinite loops, and to allow messages to eventually expire from the system.



8.f) FDMA: Frequency Division Multiple Access the available bandwidth is divided in to frequency bands. Each station is allocated band to send its data. In other words, each band is received for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies. To prevent station interfaces the allocated bands are separated from one another by small guard bands.



Advantages of FDMA:

- It allocates dedicated frequencies to different stations.
- Moreover, there are separate bands for both uplink and downlink. Hence stations transmit and receive continuously at their allocated frequencies.
- It is very simple to implement with respect to hardware resources.