Section -A

Unit-1

1. **Write any two examples of data communication modes?**
   - **Simplex mode: Ex: T.V transmission**
   - **Half-duplex mode: Ex: Internet browsing**
   - **Full-duplex mode: Ex: Telephone communication**
2. **Expand NIC and TCP**
   - **NIC: network interface cards**
   - **TCP: transmission control protocol**
3. **What is a switch?**

   A *network switch* is a hardware device that channels incoming data from multiple input ports to a specific output port that will take it toward its intended destination. It is a small device that transfers data packets between multiple *network* devices such as computers, routers… A switch network consists of several devices interlinked by a series of nodes called switch.

4. **Write any two difference between analog and digital signals?**

Analog signal	Digital signal
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.
Analog signal has no fixed range.	Digital signal has a finite numbers i.e. 0 and 1.

5. **Define SNR?**

   SNR is ratio of the signal power to the noise power

$$\text{SNR} = \frac{\text{Average signal power}}{\text{Average noise power}}$$

6. **What is modem?**

Modem is abbreviation for Modulator – Demodulator. Modems are used for data transfer from one computer network to another computer network through telephone lines.

7. **What is FTP?**

FTP is application protocol used to transfer a file from one computer to another .it is intended to operate across different computers even when they are running different operating system.

8. What do you mean by IP utility? Give an ex.

IP provides several handy tools or utilities for troubleshooting, investigating, and analyzing the network

Examples:

- **PING**
- **TRACE ROUTE.**

9. What is Network Topology? List out any two network topologies.

Network Topologies define layout, virtual shape or structure of network, not only physically but also logically.

Examples

- **Bus topology**
- **Star topology**

10. Define attenuation?

Attenuation, when a signal travel through transmission media it loses some of its energy in overcoming the resistance of the medium. To compensate attenuation, amplifier are used to strengthen the signal.

11.Write any two differences between analog and digital signals.

ANALOG SIGNALS	DIGITAL SIGNALS
a) An analog signal is a continuous wave that changes over a time period.	a)A digital signal is a discrete wave that carries information in binary form
b) An analog signal is represented by a sine wave.	b) A digital signal is represented by square waves.

12. What is telnet? How it differs from FTP ?

TELNET is a terminal network . It is a TCP\IP protocol which provides a means of accessing resources on a remote computer where the initiated computer is treated as local to the remote computer.

FTP provides access to files only. It is driven either by command line interpreter or graphical user interface.

13. What ismeant by protocol and internet protocol suite ?

In telecommunication, a communication protocol is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity.

Internet protocol is one of the major protocols in the TCP\IP protocols suite. It works at the internet layer of the TCP\IP model.

14. Define encoding and decoding.

Encoding is the process by which information from a source is converted into symbols to be communicated.

Decoding is the reverse process, converting these code symbols back into information understandable by a receiver.

15.Define datagram and packet.

Datagram is a basic transfer unit associated with a packet switched network it provides a connectionless communication service across a packet switched network.

Packet is a unit of data made into a single package that travels along a given network path.

16. Define bit rate and baud rate.

Bit rate is the number of bits transmitted per second.

Baud rate is the number of signal units transmitted per second

17. Define multiplexing?

Multiplexing **is a method by which multiple analog or digital signals are combined into one signal over a shared medium. ... For example, in telecommunications, several telephone calls may be carried using one wire.**

18. What is cellular telephone network?

A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land areas called "cells", each served by at least one fixed-location transceiver, but more normally, three cell sites or base transceiver stations.

19. What do you mean by Nyquist signaling rate ? explain.

The Nyquist frequency, named after electronic engineer Harry Nyquist, is half of the sampling rate of a discrete signal processing system.The Nyquist rate is twice the maximum component frequency of the function being sampled.

Formula : $C = 2 * B * \log_2 M$

20. Expand HDLC and PPP?

HDLC – high level data link control

PPP – point to point protocol

21. What is framing?

A frame is a digital data transmission unit in computer networking and telecommunication. A frame typically includes frame synchronization features consisting of a sequence of bits or symbols that indicate to the receiver the beginning and end of the payload data within the stream of symbols or bits it receives.

22. What is the use of repeaters?

A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.

23. Expand FDDI and CSMA

- **FDDI – Fiber Distributed Data Interface.**
- **CSMA- Carrier Sense Multiple Access.**

24. What is reservation?

The Resource *Reservation* Protocol (RSVP) is a transport layer protocol designed to *reserve* resources across a *network* using the integrated services model. ... RSVP can be used by hosts and routers to request or deliver specific levels of quality of service (QoS) for application data streams.

25. What do you mean by centralized pooling?

A central controller transmits polling messages to stations according to a certain order

26. What is Ethernet?

Ethernet is the traditional technology for connecting wired local area networks (LANs), enabling devices to communicate with each other via a protocol-- a set of rules or common network language.

27.What is meant by choke pocket?

A choke packet is used in network maintenance and quality management to inform a specific node or transmitter that its transmitted traffic is creating congestion over the network. This forces the node or transmitter to reduce its output rate.

28.What are the two types of LAN standards?

(I) Ethernet or IEEE 802.3 standard

(II) Token bus or IEEE 802.4 standard

29. What is flooding?

Flooding is a simple routing technique in computer networks where a source or node sends packets through every outgoing link. Flooding, which is similar to broadcasting, occurs when source packets (without routing data) are transmitted to all attached network nodes.

30. What is Ethernet?

Ethernet is the traditional technology for connecting wired local area networks (LANs), enabling devices to communicate with each other via a protocol-- a set of rules or common network language.

31.What do you mean by IEEE 802.11 standards?

IEEE 802.11 refers to the set of standards that define communication for wireless LANs (wireless local area networks, or WLANs). The technology behind 802.11 is branded to consumers as Wi-Fi. As the name implies, IEEE 802.11 is overseen by the IEEE, specifically the IEEE LAN/MAN Standards Committee (IEEE 802).

32. What do you mean by flooding? Explain.

In a network, flooding is the forwarding by a router of a packet from any node to every other node attached to the router except the node from which the packet arrived. The Internet's Open Shortest Path First (OSPF) protocol, which updates router information in a network, uses flooding.

33. What is the difference between Ethernet and fast Ethernet?

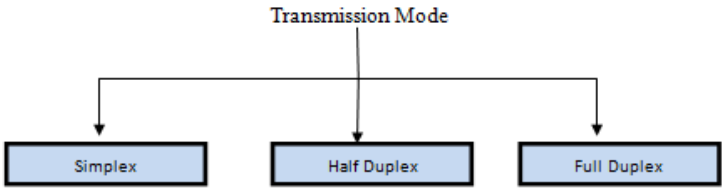
ETHERNET	FAST ETHERNET
Offers 100 Mbps speed.	Provide 1 Gbps speed.
Generate more delay.	Less comparatively.
Simple	Complicated and create more errors.
Can cover distance up to 10 km.	Has the limit of 70 km.
Successor of 10-Base-T Ethernet.	A successor of fast Ethernet.

Section B (5marks)

1. Explain types of transmission modes?

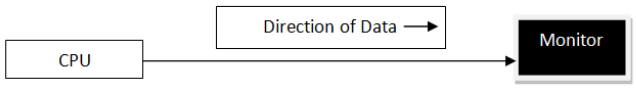
Ans:Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called Communication Mode. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

1. **Simplex Mode**
2. **Half duplex Mode**
3. **Full duplex Mode**

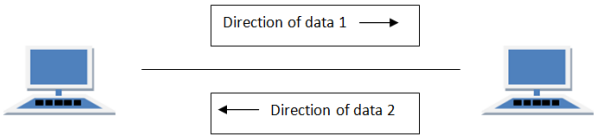


Simplex mode : In this type of transmission mode, data can be sent only in one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems where we just need to send a command/signal, and do not expect any response back.

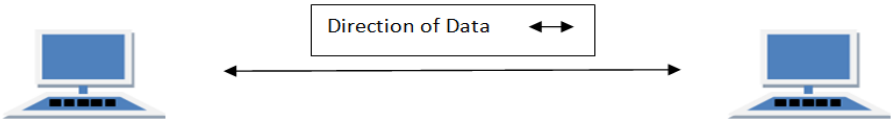
Examples of simplex Mode are loudspeakers, television broadcasting, television and remote, keyboard and monitor etc.



Half duplex mode : Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time



Full duplex mode : In full duplex system we can send data in both the directions as it is bidirectional at the same time in other words, data can be sent in both directions simultaneously.



2. Compare mesh topology with star topology?

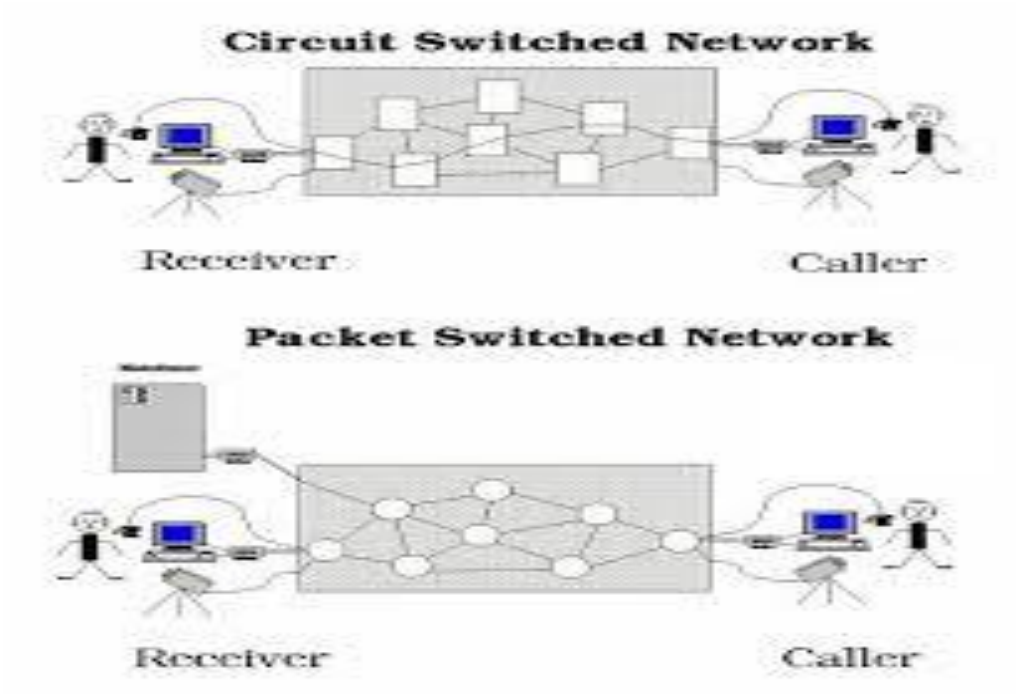
Mesh topology	Star topology
It contains at least two nodes with two or more paths between them.	The peripheral nodes are connected to the central node(ex. hub, switch or router).
Information is directly routed from one device to another.	All the information is routed from the central network connection.
Expensive due to extensive cabling.	Cost is Comparatively less
Quite complex	Simple0
Highly robust	Intermediate

3. Differentiate datagrams with virtual circuits

Virtual circuits	Datagrams
1.It is connection-oriented simply meaning that there is a reservation of resources like buffers, CPU, bandwidth, etc. for the time in which the newly setup VC is going to be used by a data transfer session.	1.It is connectionless service. There is no need for reservation of resources as there is no dedicated path for a connection session.
2. First packet goes and reserves resources for the subsequent packets which as a result follow the same path for the whole connection time	2. All packets are free to go to any path on any intermediate router which is decided on the go by dynamically changing routing tables on routers.
3. Since all the packets are going to follow the same path, a global header is required only for the first packet of the connection and other packets generally don't require global headers.	3. Since every packet is free to choose any path, all packets must be associated with a header with proper information about the source and the upper layer data.
4. Since data follows a particular dedicated path, packets reach inorder to the destination.	4. The connectionless property makes data packets reach the destination in any order, means they need not reach in the order in which they were sent.
5. In Virtual Circuit Switching, it is sure the all the packets will definitely reach to the Destination. No packet will discard due to unavailability of resources.	5. Datagram networks are not reliable as Virtual Circuits.

4. Explain packet switching.

Packet switching is a method of grouping data that is transmitted over a digital network into *packets*. Any message exceeding the maximum-defined length of the packet is broken up into packets. Packet switching overcomes the drawbacks of circuit switching and message switching. Packets are made of a header,user data, trailer. Data in the header are used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software Each packet contains header, user data and trailer. The header specifies the beginning of a packet and contains control information like source and destination addresses, packet number, priority codes etc. the user data contains information. The trailer contains a cyclic redundancy checksum used for error detection and correction.



5. Explain Shannon capacity.

Transmission channels are noisy. The presence of noise can corrupt one or more bits. If data rate is increased, then more bits will occur in the interval of a noise spike, and hence more errors will occur. Claude Shannon introduced a formula, called Shannon capacity, to determine the theatrical highest data rate for a noisy channel.

C = B * log2 (1+SNR)

Where,

C is the capacity of the channel in bits per second

B is the bandwidth of the channel

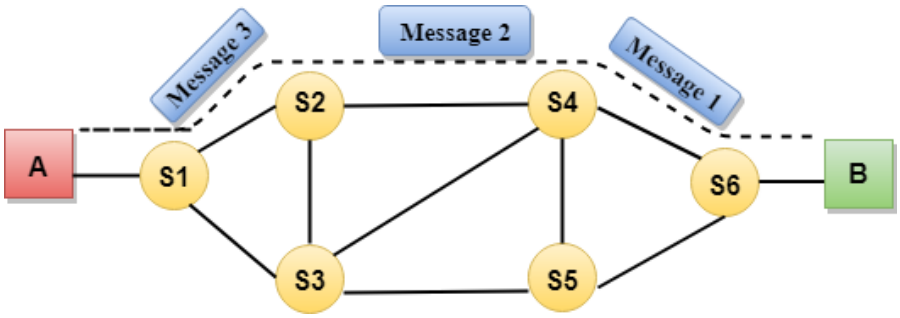
SNR is the Signal-to-noise Ratio.

6. Explain circuit switching.

In circuit switching a dedicated physical connection is established between the source and destination and then data is transmitted. Communication via circuit switching involves three phases.Circuit establishment: Before any data can be transmitted, an end to end dedicated connection is established.

Data transfer: once the connection is established data is transmitted on the link.

Circuit disconnect: After the data transmission is completed, the circuit is terminated and the resources are deallocated



Advantages:

- **Data is transmitted without delays.**
- **This method suitable for long continuous transmission.**

Disadvantages:

- **Long connection establishment delay**
- **Network does not provide flow control or error control.**

7. How many layers are there in TCP\IP model? Mention the function of each layer.

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the Internet. These protocols offer simple naming and addressing schemes. TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines

Host-to-network layer

- **Lowest layer of the all.**
- **Protocol is used to connect to the host, so that the packets can be sent over it.**
- **Varies from host to host and network to network. It is equivalent to the combination of physical and datalink layer.**

Internet layer

- **Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.**
- **It is the layer which holds the whole architecture together.**
- **It helps the packet to travel independently to the destination.**
- **Order in which packets are received is different from the way they are sent.**
- **IP (Internet Protocol) is used in this layer.**

Transport layer

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

Application layer

- **TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.**
- **FTP (File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.**
- **SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.**
- **DNS (Domain Name Server) The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.**
-

8. Explain concept of checksum?

- **A checksum is an error-detection method the transmitter computes a numerical value according to the number of set or unset bits in a message and sends it along with each message frame.**
- **At the receiver end, the same checksum function (formula) is applied to the message frame to retrieve the numerical value. If the received checksum value matches the sent value, the transmission is considered to be successful and error free. A checksum may also be known as a hash sum.**
- **A mismatched checksum shows that the entire message has not been transmitted. TCP/IP and User Datagram Protocol (UDP) provide a checksum count as one of their services.**
- **The procedure of generating checksums from messages is called a checksum function and is performed using a checksum algorithm. Efficient checksum algorithms produce different results with large probabilities if messages are corrupted. Parity bits and check digits are special checksum cases suitable for tiny blocks of data. Certain error-correcting codes based on checksums are even capable of recovering the original data.**

9. Explain types of errors?

- **Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal.**

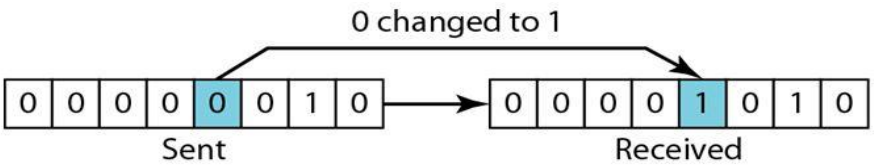
There are three types of errors.

1.single bit

2.multiple bit

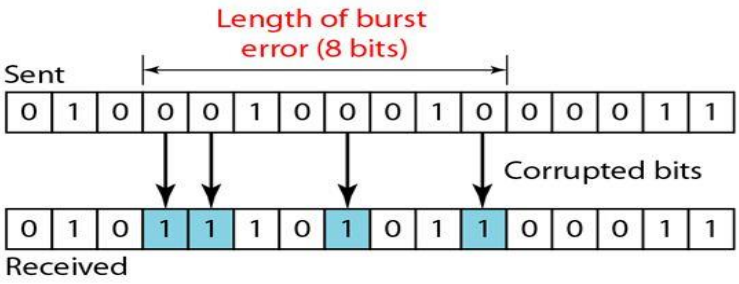
3.burst error

- **The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.**
- **The following figure shows the effect of a single-bit error on a data unit. To understand the impact of the change, imagine that each group of 8 bits is an ASCII character with a 0 bit added to the left. In the figure 00000010 (ASCII STX) was sent, meaning start of text, but 00001010 (ASCII LF) was received, meaning line feed.**



Burst Error:

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.The following figure shows the effect of a burst error on a data unit. In this case, 0100010001000011 was sent, but 0101110101100011 was received. Note that a burst error does not necessarily mean that the errors occur in consecutive bits. The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.



Multiple bit error: multiple bit error means that two or more non-consecutive bits in the data unit have changed from 1 to 0 or from 0 to 1

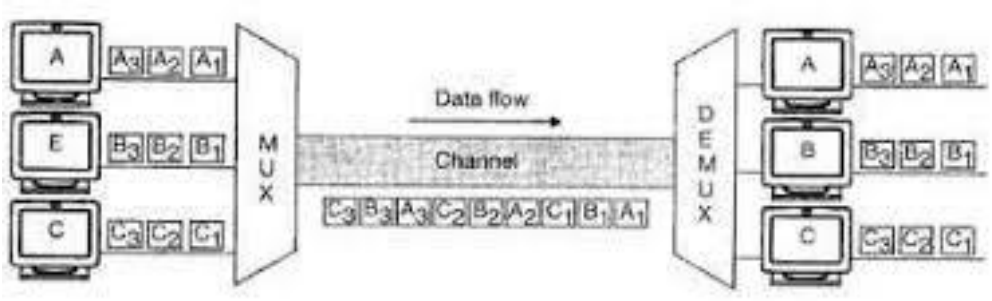
10. What is multiplexing? Explain TDM

- **Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.**

TDM (Time division multiplexing)

- **Time-division multiplexing (TDM) is a method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. ... The composite signal thus contains data from multiple senders.**
- **Time-division multiplexing is used primarily for digital signals, but may be applied in Analog multiplexing in which two or more signals or bit streams are transferred appearing simultaneously as sub-channels in one communication channel, but are**

physically taking turns on the channel.



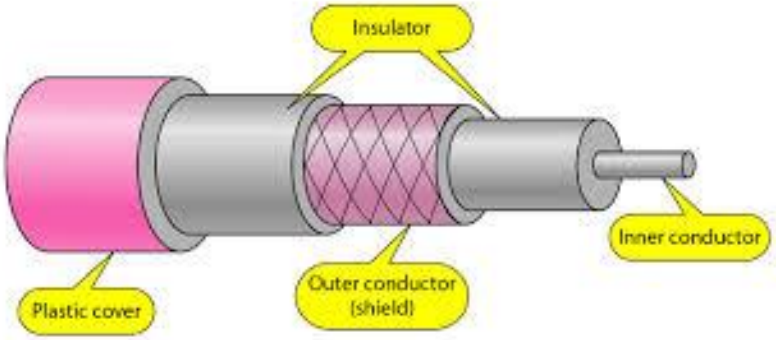
Time Division Multiplexing (TDM)

11. Differentiate connectionless and connection oriented services

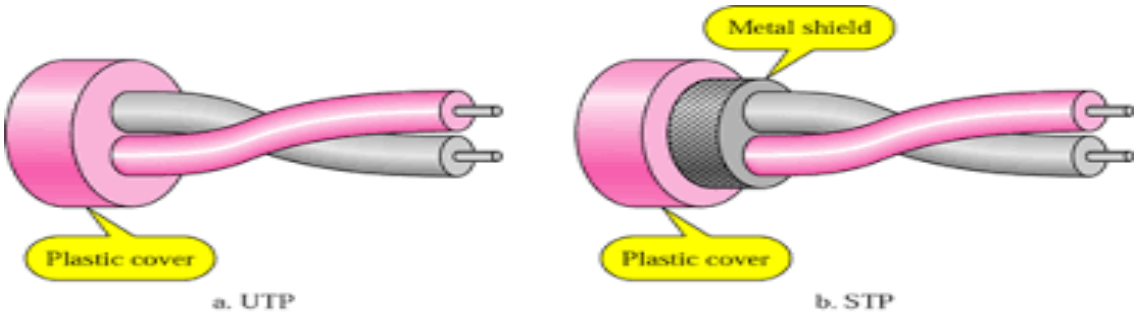
NO	CONNECTION-ORIENTED SERVICE	CONNECTION-LESS SERVICE
1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give the guarantee of reliability.

12. Explain twisted pair cable as transmission medium.

- A twisted pair can be used as a balanced line, which as part of a balanced circuit can greatly reduce the effect of noise currents induced on the line by coupling of electric or magnetic fields. The idea is that the currents induced in each of the two wires are very nearly equal. The twisting ensures that the two wires are on average the same distance from the interfering source and are affected equally. The noise thus produces a common-mode signal which can be cancelled at the receiver by detecting the difference signal only, the latter being the wanted signal.



- **Shielded twisted pair: Shielded twisted pair is a special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground.**
- **Unshielded twisted pair :Unshielded twisted pair (UTP) cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25-pair colour code originally developed by AT&T Corporation.**



Advantages

- **Cheapest form of cable available for networking purposes.**
- **Easy to handle and install.**

13. Explain 2-dimensional parity check for error detection.

- **When a large amount of data is to be transmitted two dimensional parity checks can be employed. In this method, the data words are arranged one above another and is organized in a form of two dimensional binary matrix. For each row and column of the matrix parity-check bit is calculated.**
- **A message consisting of n characters with 8-bits per character will now become n+1 character with 9-bits per character and is transmitted.**
- **The whole matrix is then sent to the receiver. At the receiver end, the sum of the bits in the block of data is added again, and if the calculated sum is different than what was**

transmitted, then an error is indicated. Then the original block must be transmitted or written again. This scheme can detect up to three errors that occur anywhere in the table.

1100111	1011101	0111001	0101001

- **Ex: Original data**

1 1 0 0 1 1 1 1
1 0 1 1 1 0 1 1
0 1 1 1 0 0 1 0
0 1 0 1 0 0 1 1
0 1 0 1 0 1 0 1 **column parities**

Row parities

11001111	10111011	01110010	0101001	01010101

14. Explain the difference between connection and connectionless services.

S.NO	CONNECTION-ORIENTED SERVICE	CONNECTION-LESS SERVICE
1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by busty communication.
3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give the guarantee of reliability.
7.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.

15. Explain the structure of HDLC frames

An HDLC frame is structured as follows:

FLAG	ADDRESS	CONTROL	INFORMATION	FCS	FLAG
8 bits	8 bits	8 / 16 bits	variable	8	8 bits

FRAME FIELDS

FLAG

- **The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110, same as PPP flag field which indicates the beginning and end of the frame.**

ADDRESS

- **The second field of an HDLC frame contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary creates the frame, it contains a from address.**

CONTROL

- **The control field is used for flow and error control. It also determines the type of the frame**

INFORMATION FIELD

- **The information field contains the user's data from the network layer or management information.**

FCS FIELD:

- **The frame check sequence is the HDLC error detection field. It contains either a 2 or 4-byte CRC**

16. Illustrate CSMA

Carrier Sense Multiple Access with collision avoidance(CSMA/CA) was invented for this network. Collisions are avoided through the use of three CSMA/CA strategies:

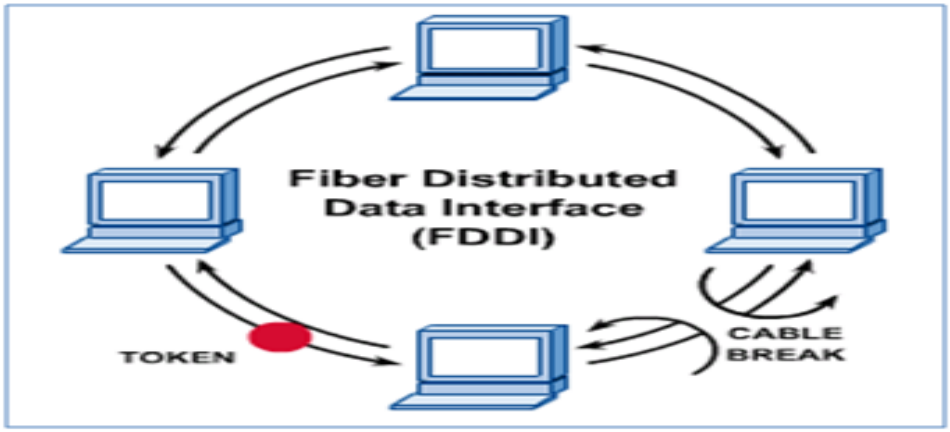
- ✓ **Interface space(IFS): In this method when a station senses the channel id idle, it does not send immediately. It waits for a period of time called the Inter-frame space. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.**
- ✓ **Contention Window: The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its**

wait time. The number of slots in the window changes according to the binary exponential back-off strategy

- ✓ **Acknowledgement: With all these precautions, there may be collision resulting in destroyed data. The positive acknowledgement and the time-out timer can help the receiver has received the frame.**

17. Describe FDDI

- **FDDI uses dual-ring architecture with traffic on each ring flowing in opposite directions. The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. When the frames are transmitted through the primary ring at each and every station the destination address is checked, if it matches then it stops at the destination else will be transferred through the ring again until exact address is matched got. If there is any break in the ring, unlike Token-Ring, the frame takes opposite direction of flow and is transmitted on the secondary ring.**



18. Write Bellman Ford Algorithm

The Bellman Ford algorithm calculates the shortest path to all nodes in the graph from a single source. The principle states that "Each neighbor of source node knows the shortest path to the destination node.

The steps involved in bellman ford algorithm is:

1. **Intially mark all the nodes except source as infinity.**
2. **And the distance to destination D_d=0.**
3. **Find minimum distance to the destination through neighbours: for each i=/d D_i-$\min_j(c_{ij}+D_j)$, for all j=/i**
4. **Repeat step 2 until destination is reached.**

Consider the following figure. Suppose we want to find the shortest path from node 2 to node 6

To reach destination from node 2, we must go through either node1, node4, node5. Suppose the shortest path from node 1(through node 3), node4 and node 5 to the destination node 6 are 3,3,2.

- **Then for the packet from node 2 through node 1, the total distance is(3+3)=6**
- **Similarly, for the packet from node 2 through node 4 and node 5 are (1+3)=4 and (4+2)=6 respectively**

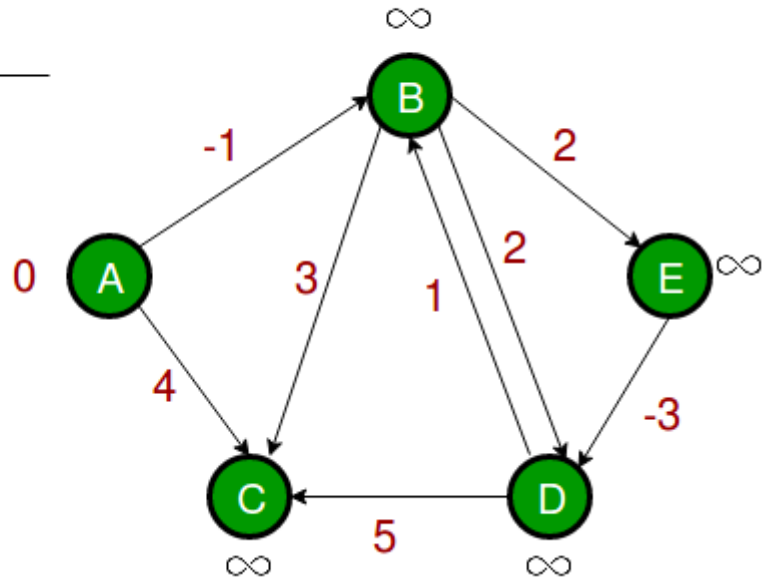
Then the shortest distance according to Bellman ford algorithm from node 2 to destination node 6 is through node 4.

Example

Let us understand the algorithm with following example graph. The images are taken from this source.

Let the given source vertex be 0. Initialize all distances as infinite, except the distance to source itself. Total number of vertices in the graph is 5, so *all edges must be processed 4 times.*

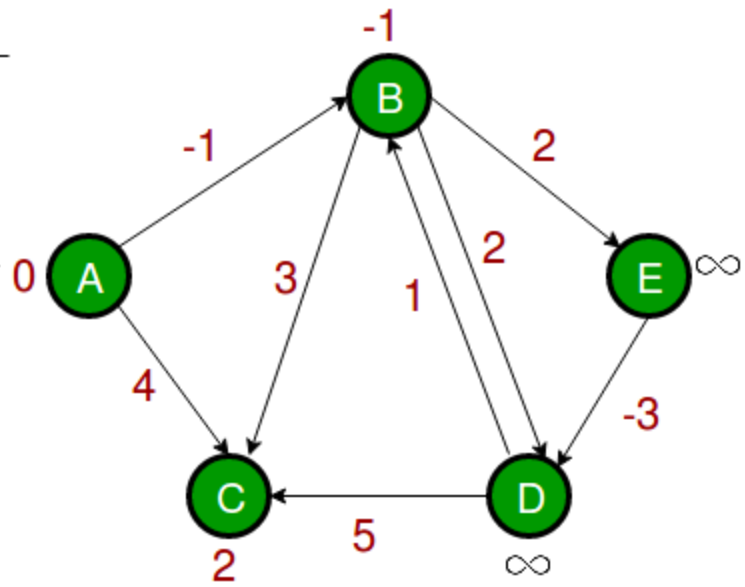
A	B	C	D	E
0	∞	∞	∞	∞



Let all edges are processed in following order: (B, E), (D, B), (B, D), (A, B), (A, C), (D, C), (B, C), (E, D). We get following distances when all edges are processed first time. The first row in shows initial distances. The second row shows distances when edges (B,

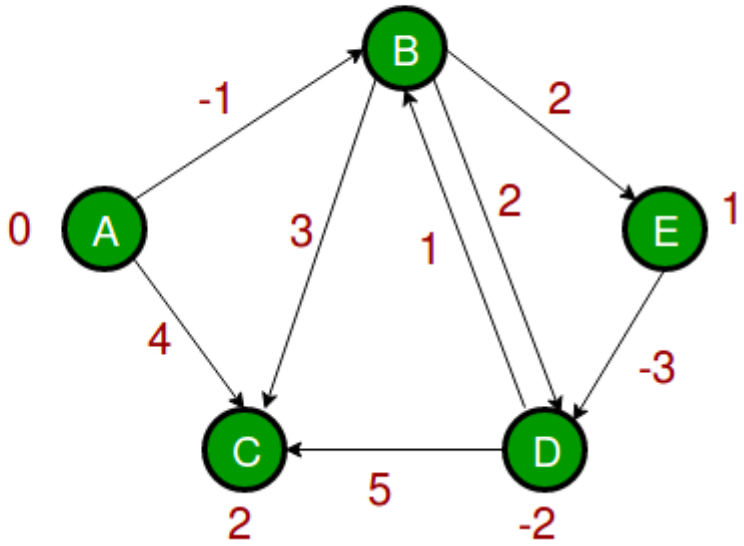
E), (D, B), (B, D) and (A, B) are processed. The third row shows distances when (A, C) is processed. The fourth row shows when (D, C), (B, C) and (E, D) are processed.

A	B	C	D	E
0	∞	∞	∞	∞
0	-1	∞	∞	∞
0	-1	4	∞	∞
0	-1	2	∞	∞



The first iteration guarantees to give all shortest paths which are at most 1 edge long. We get following distances when all edges are processed second time (The last row shows final values).

A	B	C	D	E
0	∞	∞	∞	∞
0	-1	∞	∞	∞
0	-1	4	∞	∞
0	-1	2	∞	∞
0	-1	2	∞	1
0	-1	2	1	1
0	-1	2	-2	1



The second iteration guarantees to give all shortest paths which are at most 2 edges long. The algorithm processes all edges 2 more times. The distances are minimized after the second iteration, so third and fourth iterations don't update the distances.

19. Explain the role of the following network devices:

- **Hub**
- **Switch**
- **Bridge**
- **Router**
- **Repeater**
- **Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.**
- **Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (large number of ports imply less traffic) and performance. Switch is data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.**
- **Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.**
- **Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.**
- **Repeater – A repeater operates at the physical layer. Its job is to regenerate 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. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.**

Section-C

1. **A) Explain the types of network?**

LAN

- **LAN refers to a group of computers that all belong to the same organization and that are linked within a small geographic area using a network and often the same technology (the most widespread being Ethernet).**

- **A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps, such as for an Ethernet network, and 1 gbps, as with FDDI or Gigabit Ethernet. A local area network can reach as many as 100, or even 1000, users. MAN**

- **MANs connect multiple geographically close LANs (over an area of up to several dozen miles) to one another at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network.A MAN is made from switches or routers connected to one another with high-speed links (usually fibre optic cables).**

WANs

- **A WAN connects multiple LANs to one another over great geographic distances. The speed available on a WAN varies depending on the cost of the connections, which increases with distance, and may be low.WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node.**
  The most well-known WAN is the Internet.

b) Explain OSI reference model with a neat diagram. Repeated [Nov-Dec 2018]

Layer 1: The Physical Layer

1. **Physical Layer is the lowest layer of the OSI Model.**
2. **It activates, maintains and deactivates the physical connection.**
3. **It is responsible for transmission and reception of the unstructured raw data over network.**
4. **Voltages and data rates needed for transmission is defined in the physical layer.**
5. **It converts the digital /analog bits into electrical signal or optical signals.**
6. **Data encoding is also done in this layer.**

Layer 2: Data Link Layer

1. **Data link layer synchronizes the information which is to be transmitted over the physical layer.**
2. **The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.**
3. **Transmitting and receiving data frames sequentially is managed by this layer.**

4. **This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.**
5. **This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.**

Layer 3: The Network Layer

1. **Network Layer routes the signal through different channels from one node to other.**
2. **It acts as a network controller. It manages the Subnet traffic.**
3. **It decides by which route data should take.**
4. **It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.**

Layer 4: Transport Layer

1. **Transport Layer decides if data transmission should be on parallel path or single path.**
2. **Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer**
3. **It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.**
4. **Transport layer can be very complex, depending upon the network requirements.**

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer

1. **Session Layer manages and synchronize the conversation between two different applications.**
2. **Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided**

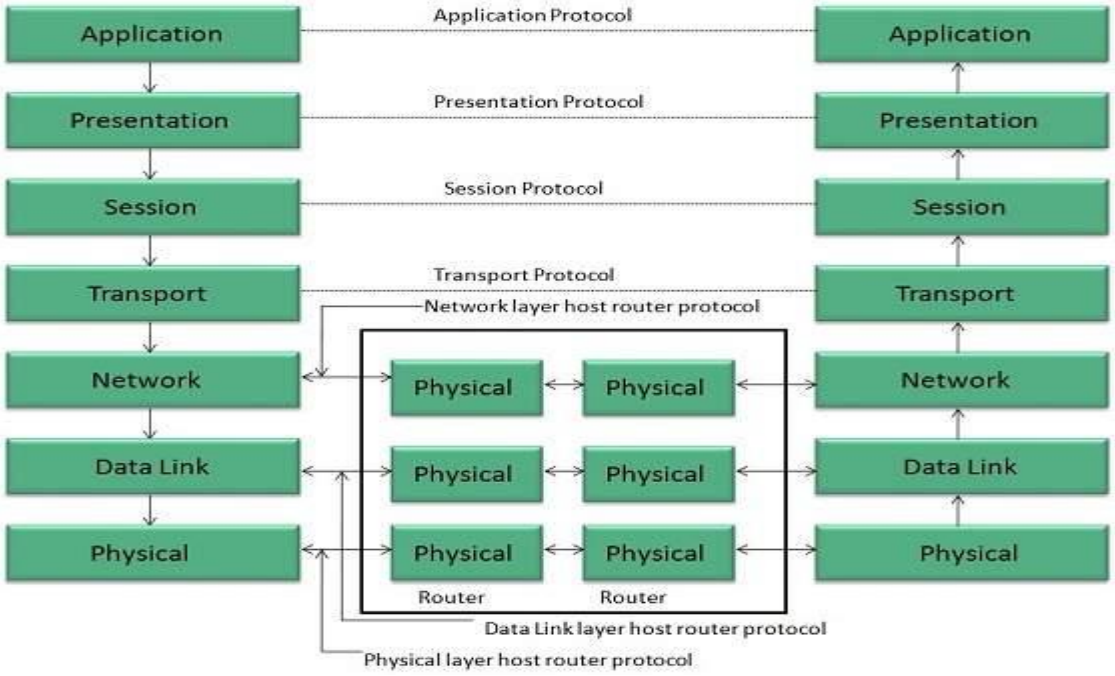
Layer 6: The Presentation Layer

1. **Presentation Layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.**
2. **While receiving the data, presentation layer transforms the data to be ready for the application layer.**
3. **Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.**
4. **It performs Data compression, Data encryption, Data conversion etc.**

Layer 7: Application Layer

1. **Application Layer is the topmost layer.**
2. **Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.**
3. **This layer mainly holds application programs to act upon the received and to be sent data.**

DIAGRAM OF OSI MODEL



3.What is digital modulation? Explain the digital modulation techniques.

DM stands for Digital Modulation and is a generic name for modulation techniques that uses discrete signals to modulate a carrier wave.

Three types of digital modulation

- **Amplitude Modulation (AM)**
- **Frequency Modulation (FM)**
- **Phase Modulation (PM)**

Amplitude Modulation

Amplitude modulation was developed in the beginning of the 20th century. It was the earliest modulation technique used to transmit voice by radio. This type of modulation technique is used in electronic communication. In this modulation, the amplitude of the carrier signal varies

in accordance with the message signal, and other factors like phase and frequency remain constant.

Frequency Modulation

In this type of modulation, the frequency of the carrier signal varies in accordance with the message signal, and other parameters like amplitude and phase remain constant. Frequency modulation is used in different applications like radar, radio and telemetry, seismic prospecting and monitoring new-borns for seizures via EEG, etc.

Phase Modulation

In this type of modulation, the phase of the carrier signal varies in accordance with the message signal. When the phase of the signal is changed, then it affects the frequency. So, for this reason, this modulation is also comes under the frequency modulation.

4. Explain digital representation of information.

Applications that run over networks involve the transfer of information of various types. Some of them may involves blocks of text characters like e-mail and others involve stream of information such as telephony.

Information can be classified into two broad categories

1. Block oriented information: this occurs naturally in form of a single block. These blocks of information range from a few bytes to several hundred kilobytes and occasionally several megabytes. Normal files of this form usually contain fair amount of redundancies. Hence, data compression utilities such as compress, zip and other methods are used to encode the original information into blocks which will now take fewer bits to transfer and less disk storage space.

2. Stream information: this id produced continuously and must be transmitted as it is produced. These signals are analog signals that are digitalized before transmission. The first step in digitalizing and analog signal is to obtain sample values of the signal every T seconds. The second step is quantizing each of the sample values. The last step is to convert them into digital signals. Video signals are succession of pictures that gives illusion to the human eye the appearance of continuous motion.

Transmission of digital signals

1. Baseband transmission: Base band is defined as one that uses digital signaling , which is inserted in the transmission channel as voltage pulses .

2. Broadband transmission: These systems use analog signaling to transmit information using a carrier of high frequency.

Transmission impairment

1. Attenuation: When a signal travels through a medium it loses some of its energy in overcoming the resistance of the medium. To compensate attenuation, amplifiers are used to strengthen the signal.

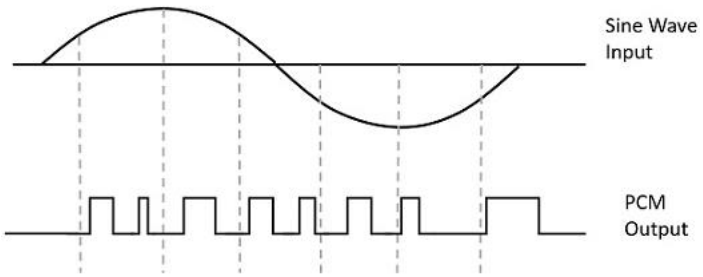
2. Distortion: It means that the signal changes its form or shape. It can occur in a composite signal made of different frequencies.

3. Noise: It is the disturbance in the medium caused due to heat, crosstalk, spike in energy, lighting. Noise corrupts the signal.

5. Explain the following?

A) Pulse Code Modulation (PCM).

- **A signal is pulse code modulated to convert its analog information into a binary sequence, i.e., 1s and 0s. The output of a PCM will resemble a binary sequence. The following figure shows an example of PCM output with respect to instantaneous values of a given sine wave.**



- **Instead of a pulse train, PCM produces a series of numbers or digits, and hence this process is called as digital. Each one of these digits, though in binary code, represent the approximate amplitude of the signal sample at that instant.**
- **In Pulse Code Modulation, the message signal is represented by a sequence of coded pulses. This message signal is achieved by representing the signal in discrete form in both time and amplitude.**

B) SONET

- **Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or light-emitting diodes (LEDs). Lower data rates can also be transferred via an electrical interface. The method was developed to replace the**

Plesiochronous Digital Hierarchy (PDH) system for transporting larger amounts of telephone calls and data traffic over the same fiber without synchronization problems. SONET generic criteria are detailed in Telcordia Technologies Generic Requirements document GR-253-CORE.Generic criteria applicable to SONET and other transmission systems (e.g., asynchronous fiber optic systems or digital radio systems) are found in Telcordia GR-499-CORE.

- **SONET and SDH, which are essentially the same, were originally designed to transport circuit mode communications (e.g., DS1, DS3) from a variety of different sources, but they were primarily designed to support real-time, uncompressed, circuit-switched voice encoded in PCM format.The primary difficulty in doing this prior to SONET/SDH was that the synchronization sources of these various circuits were different. This meant that each circuit was actually operating at a slightly different rate and with different phase. SONET/SDH allowed for the simultaneous transport of many different circuits of differing origin within a single framing protocol. SONET/SDH is not itself a communications protocol *per se*, but a transport protocol.**

Co-coaxial cable

- **Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses. It is also sometimes used by telephone companies to connect central offices to telephone poles near customers. Some homes and offices use coaxial cable, too, but its widespread use as an Ethernet connectivity medium in enterprises and data centres has been supplanted by the deployment of twisted pair cabling.**

5. Illustrate polynomial code with an example.Repeated [Nov-Dec 2018]

Polynomial codes are used extensively in error detection and correction. Polynomial codes can be easily implemented using shift-register circuits. A k-bit data-word can be represented as a polynomial with k terms ranging from x_{k-1} to x_0 as

$$I(x)= i_{k-1}x^{k-1} + i_{k-2}\, x^{k-2} +\ldots\ldots\ldots\ldots+i_1\, x +I_0 .$$

For example, let's take a 8-bit message 10011010. The corresponding polynomial is represented

$$M(x) = 1.x^7 +0.x^6 + 0.x^5 +1.x^4 + 1.x^3 + 0.x^2 + 1.x1 + 0.x^0$$

$$=x^7 + x^4 + x^3+ x^1$$

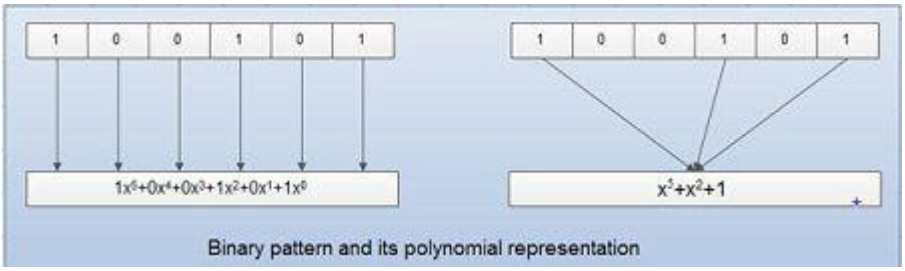
-

- **Polynomial codes involve generating check bits in the form of a cyclic redundancy check(CRC). For these reasons they are also known as CRC codes.**
- **When applying the CRC method, both the sender and the receiver must agree upon a common generator polynomial G(x). To compute the checksum for frame with M bits, corresponding to the polynomial M(x), the frame M must be longer than the generator polynomial. The polynomial M(x)is divided by G(x) to generate checksum. The checksum, is appended at the end of the frame, in such a way that the transmitted polynomial is completely divisible by G(x). if there is no remainder, it indicates no transmission error.**
- **The most common CRC is the CCITT CRC-16 and CRC-32 used for many today's applications.**

CRC-16=$X^{16}+X^{15}+X^2+1$

CRC-CCITT=$X^{16}+X^{12}+X^5+1$

CRC-32=$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+1$



Binary pattern and its polynomial representation

7. Describe twisted pair cable.

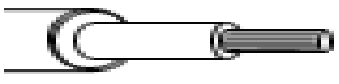
A twisted-pair cable is a cable made by intertwining two separate insulated wires.

There are two twisted pair types:

- **Shielded twisted pair**
- **Unshielded twisted pair**


Unshilded twisted-pair cable


Shielded twisted-pair cable


Coaxial cable

A STP (Shielded Twisted Pair) cable has a fine wire mesh surrounding the wires to protect the transmission a UTP (Unshielded Twisted Pair) cable does not. Shielded cable is used in older telephone networks, as well as network and data communications to reduce outside interference. The illustration gives an example of how the inside of these looks.

ADVANTAGES

- **Electrical noise going into or coming from the cable can be prevented.**
- **Crosstalk is minimize.**
- **Cheapest form of cable available for networking purposes.**
- **Easy to handle and install.**

DISADVANTAGES

- **It is incapable carrying a signal over long distances without the use of repeaters only because of high attenuation.**
- **It is not suitable for broadband applications only because of its low bandwidth capabilities**

8.Explain SONET.

Synchronous optical networking (SONET) is a standardized digital communication protocol that is used to transmit a large volume of data over relatively long distances using a fiber optic medium. With SONET, multiple digital data streams are transferred at the same time over optical fiber using LEDs and laser beams.

PHYSICAL CONFIGURATION

1. **STS Multiplexer:**
   - **Performs multiplexing of signals**
   - **Converts electrical signal to optical signal**
2. **STS De-multiplexer:**
   - **Performs de-multiplexing of signals**
   - **Converts optical signal to electrical signal**
3. **Regenerator:**

   It is a repeater, that takes an optical signal and regenerates (increases the strength) it.
4. **Add/Drop Multiplexer:**

   It allows to add signals coming from different sources into a given path or remove a signal.

10. Explain optical fibre as transmission medium

• Optical fibre transmission systems were introduced in 1970. It offered greater advantages over copper based digital transmission systems.

• A thin flexible fibre with a glass core through which light signals can be sent.

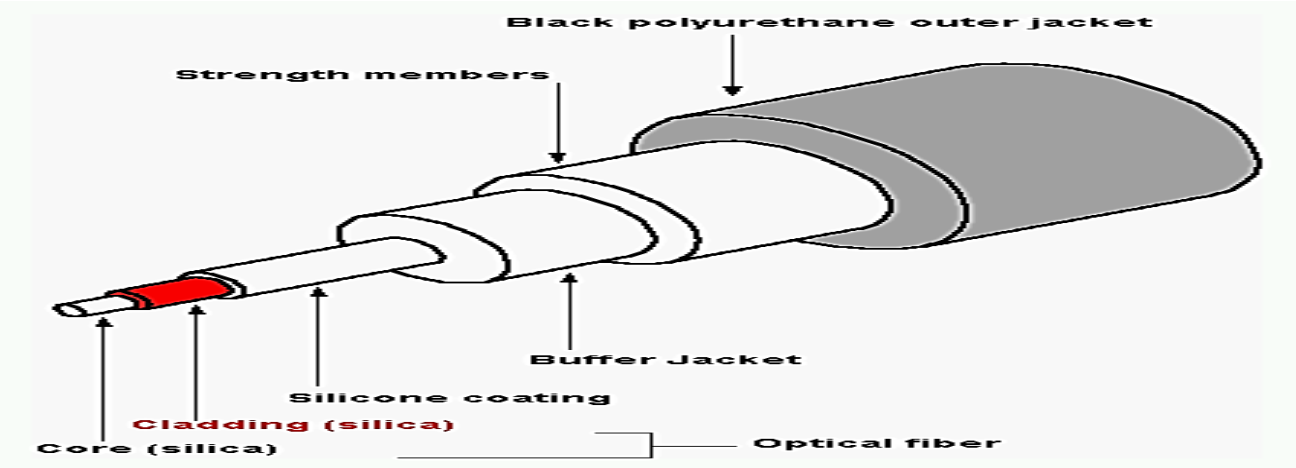
• Fibre optic cable has the ability to transmit signals over much longer distances.

• Optical fibre are immune to interference and cross talk

• A fibre optic cable is made of centre glass core surrounded by a concentric layer of glass(cladding).

• The information is transmitted thru the glass core in the form of light.

• An important characteristic of fibre optic is refraction. Refraction is the characteristic of a material to either pass or reflect the light. When a light passes thru the medium, it bends as it passes from one medium to another.



•Wave length Division Multiplexing is an effective approach to explore the bandwidth that is available in optical fibre. In WDM multiple wave length are used to carry several information simultaneously over the same fibre.

Advantages

• It supports higher bandwidth

• It runs greater distance.

• Electromagnetic noise cannot affect fibre optic cables

• Usage of glass makes more resistant than copper

Disadvantages

• Installation and maintenance is difficult.

• Unidirectional light propagation. Two fibres are used for bidirectional propagation

• The cable and the interfaces are more expensive.

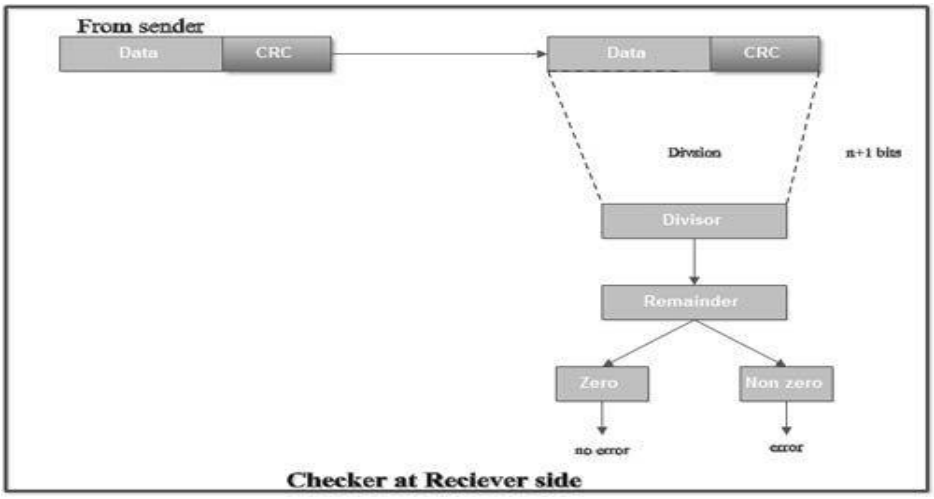
11. Explain the following?

a) CRC method

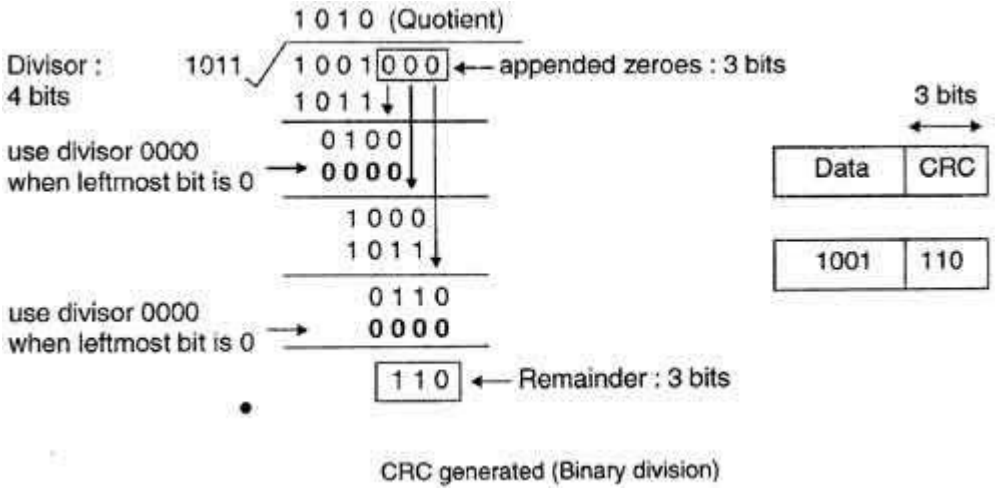
- **Error detection mechanism in which a special number is appended to a block of data in order to detect any changes introduced during storage (or transmission). The CRe is recalculated on retrieval (or reception) and compared to the value originally transmitted, which can reveal certain types of error. For example, a single corrupted bit in the data results in a one-bit change in the calculated CRC, but multiple corrupt bits may cancel each other out.**
- **A CRC is derived using a more complex algorithm than the simple CHECKSUM, involving MODULO ARITHMETIC (hence the 'cyclic' name) and treating each input word as a set of coefficients for a polynomial.**
- **CRC is more powerful than VRC and LRC in detecting errors.**
- **It is not based on binary addition like VRC and LRC. Rather it is based on binary division.**
- **At the sender side, the data unit to be transmitted IS divided by a predetermined divisor (binary number) in order to obtain the remainder. This remainder is called CRC.**
- **The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of n+ 1 bit.**
- **The sender appends this CRC to the end of data unit such that the resulting data unit becomes exactly divisible by predetermined divisor *i.e.* remainder becomes zero.**

• For example, if data to be transmitted is 1001 and predetermined divisor is 1011. The procedure given below is used:

- **String of 3 zeroes is appended to 1011 as divisor is of 4 bits. Now newly formed data is 1011000.**



1. Data unit 1011000 is divided by 1011.



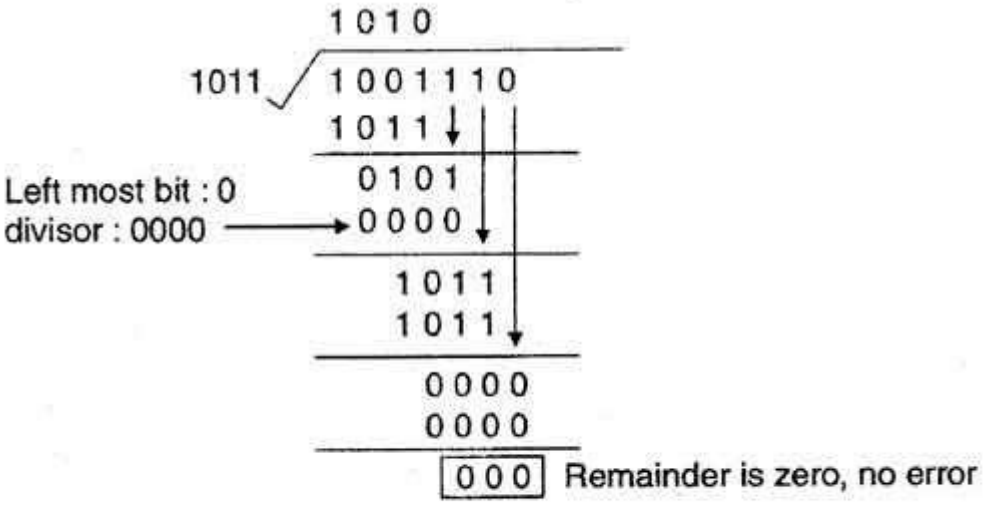
CRC generated (Binary division)

2. During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.

3. At the receiver side, data received is 1001110.

4. This data is again divided by a divisor 1011.

5. The remainder obtained is 000; it means there is no error.



CRC decoded (binary division)

b) Stop –and-Wait –ARQ algorithm

Characteristics

- **Used in Connection-oriented communication.**
- **It offers error and flow control**
- **It is used in Data Link and Transport Layers**
- **Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1**

Useful Terms:

- **Propagation Delay: Amount of time taken by a packet to make a physical journey from one router to another router.**

Propagation Delay = (Distance between routers) / (Velocity of propagation)

- **RoundTripTime (RTT) = 2* Propagation Delay**
- **TimeOut (TO) = 2* RTT**
- **Time To Live (TTL) = 2* TimeOut. (Maximum TTL is 180 seconds)**

Simple Stop and Wait

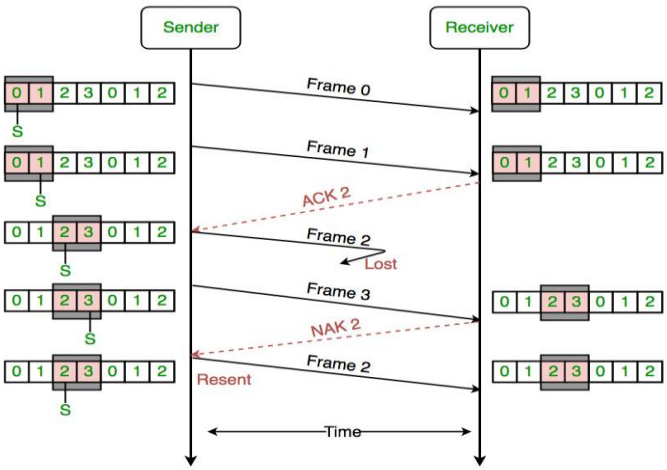
Sender:

Rule1) Send one data packet at a time.
Rule 2)Send next packet only after receiving acknowledgement for previous.

Receiver:

Rule 1) Send acknowledgement after receiving and consuming of data packet.

Rule 2) After consuming packet acknowledgement need to be sent (Flow Control).



12. Describe selective repeat ARQ.

Selective repeat protocol, also called Selective Repeat ARQ (Automatic Repeat reQuest), is a data link layer protocol that uses sliding window method for reliable delivery of data frames. ... The size is half the maximum sequence number of the frame

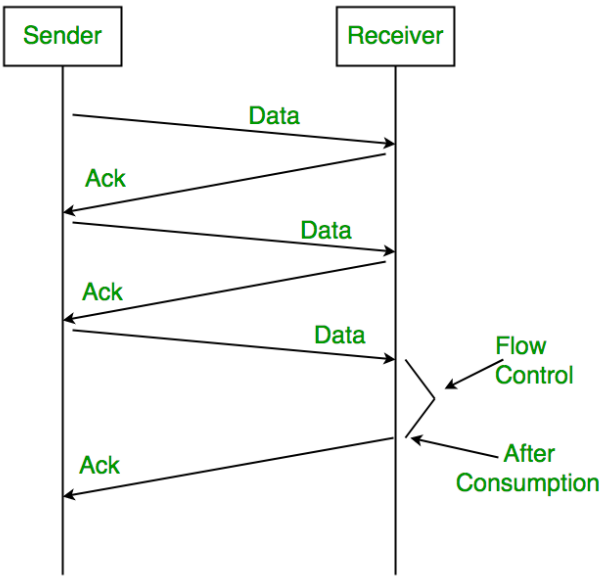
Features required for Selective Repeat ARQ

- **To support Go-Back-N ARQ, a protocol must number each PDU which is sent. (PDUs are normally numbered using modulo arithmetic, which allows the same number to be re-used after a suitably long period of time. The time period is selected to ensure the same PDU number is never used again for a different PDU, until the first PDU has "left the network" (e.g. it may have been acknowledged)).**
- **The local node must also keep a buffer of all PDUs which have been sent, but have not yet been acknowledged.**
- **The receiver at the remote node keeps a record of the highest numbered PDU which has been correctly received. This number corresponds to the last acknowledgement PDU which it may have sent.**

Recovery of lost PDUs using Selective Repeat ARQ

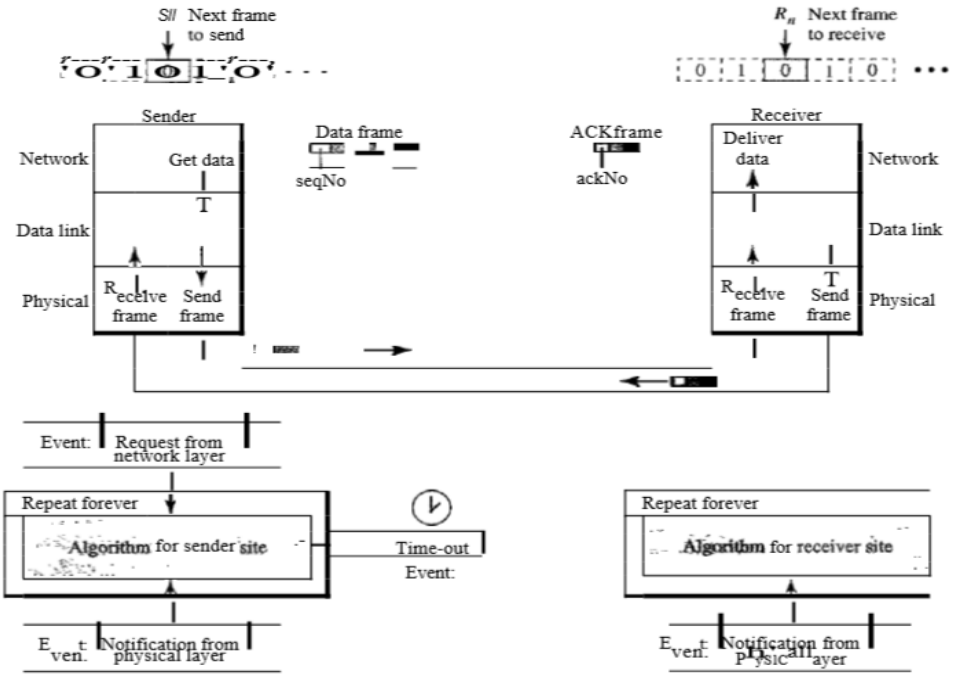
The recovery of a corrupted PDU proceeds in four stages:

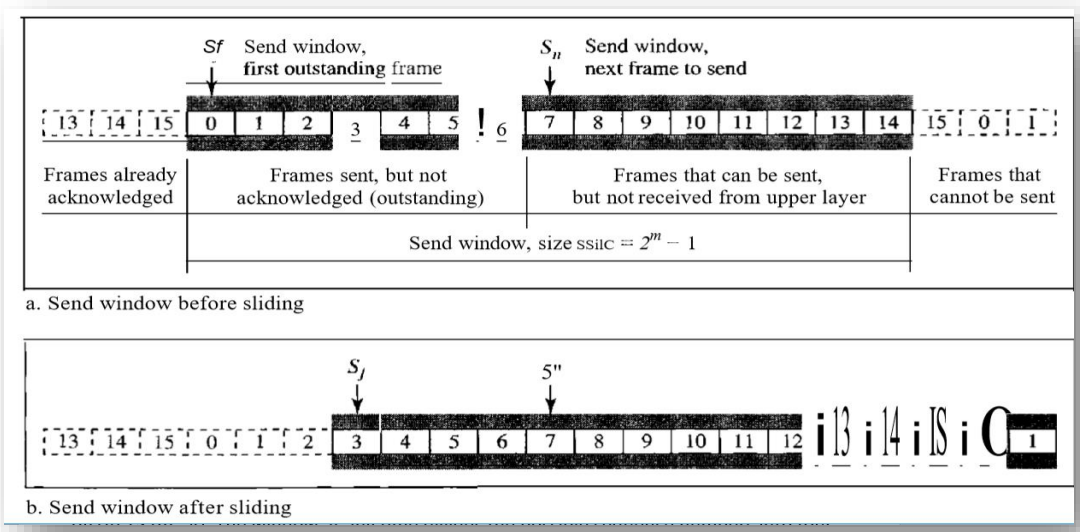
- **First, the corrupted PDU is discarded at the remote node's receiver.**
- **Second, the remote node requests retransmission of the missing PDU using a control PDU (sometimes called a Selective Reject). The receiver then stores all out-of-sequence PDUs in the receive buffer until the requested PDU has been retransmitted.**
- **The sender receives the retransmission request and then transmits the lost PDU(s).**
- **The receiver forwards the retransmitted PDU, and all subsequent in-sequence PDUs which are held in the receive buffer.**



14. Explain sliding window method of flow control.

In this protocol (and the next), the sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, the sender and receiver need to deal with only part of the possible sequence numbers. The range which is the concern of the sender is called the send sliding window; the range that is the concern of the receiver is called the receive sliding window.





The send window is an imaginary box covering the sequence numbers of the data frames which can be in transit. In each window position, some of these sequence numbers define the frames that have been sent; others define those that can be sent. The window at any time divides the possible sequence numbers into four regions.

- **The first region, from the far left to the left wall of the window, defines the sequence numbers belonging to frames that are already acknowledged. The sender does not worry about these frames and keeps no copies of them.**
- **Defines the range of sequence numbers belonging to the frames that are sent and have an unknown status. The sender needs to wait to find out if these frames have been received or were lost. We call these outstanding frames.**
- **The third range, white in the figure, defines the range of sequence numbers for frames that can be sent; however, the corresponding data packets have not yet been received from the network layer.**
- **Finally, the fourth region defines sequence numbers that cannot be used until the window slides, as we see next.**

The window itself is an abstraction; three variables define its size and location at any time. We call these variables (send window, the first outstanding frame), Sn (send window, the next frame to be sent), and Size (send window, size). The variable Sf defines the sequence number of the first (oldest) outstanding frame.

The variable Sn holds the sequence number that will be assigned to the next frame to be sent. Finally, the variable Size defines the size of the window, which is fixed in our protocol.

The send window is an abstract concept defining an imaginary box of size 2m ~ 1 with three variables: Sf Sm and Size'

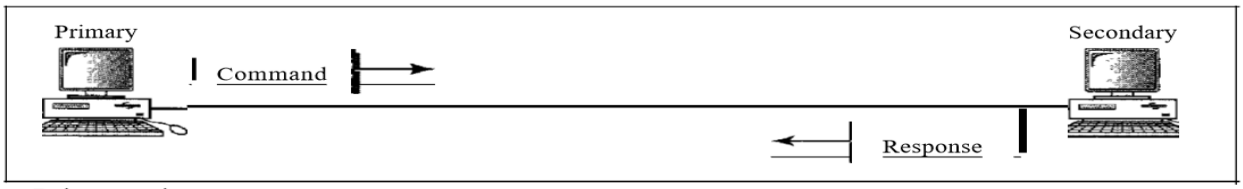
How a send window can slide one or more slots to the right when an acknowledgment arrives from the other end. As we will see shortly, the acknowledgments in this protocol are cumulative, meaning that more than one frame can be acknowledged by an ACK frame.

Frames 0, I, and 2 are acknowledged, so the window has slid to the right three slots. Note that the value of Sf is 3 because frame 3 is now the first outstanding frame.

15.What do you mean by peer-to-peer protocol? Compare PPP and HDLC.

Peer to Peer Protocol:

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.



a. Point-to-point

BASIS FOR COMPARISON	HDLC	PPP
Expands to	High-level Data Link Layer Protocol	Point-to-Point Protocol
Type of protocols	Bit-oriented protocol	Byte oriented protocol
Used in	Only synchronous media	Synchronous as well as asynchronous media
Authentication	No provision of authentication	Provides authentication
Dynamic addressing	Does not offer dynamic addressing.	Dynamic addressing is used.
Implemented in	Point-to-point and multipoint configurations.	Only point-to-point configurations.
Compatibility with other protocols	Can not be operated with non-Cisco devices.	Interoperable with non-Cisco devices also.

Unit 4

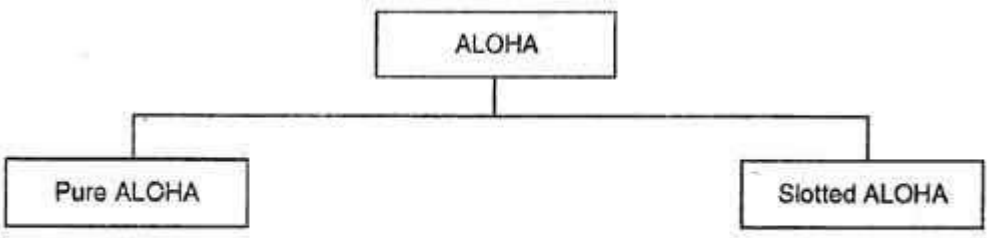
16 .a) Write short notes on ALOHA protocol.

ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision.

There are two different versions of ALOHA



Types of ALOHA

Pure ALOHA

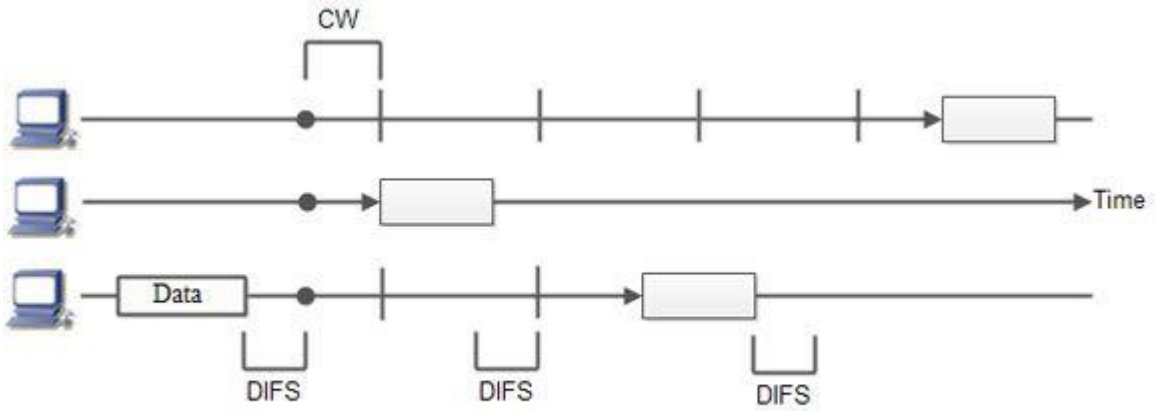
- **In pure ALOHA, the stations transmit frames whenever they have data to send.**
- **When two or more stations transmit simultaneously, there is collision and the frames are destroyed.**

Slotted ALOHA

- **Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.**
- **In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.**
- **The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.**

b) Explain CSMA protocols.

- **CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.**



Sharing time with CSMA method.

CSMA works on the principle that only one device can transmit signals on the network, otherwise a collision will occur resulting in the loss of data packets or frames. CSMA works when a device needs to initiate or transfer data over the network. Before transferring, each CSMA must check or listen to the network for any other transmissions that may be in progress. If it senses a transmission, the device will wait for it to end. Once the transmission is completed, the waiting device can transmit its data/signals. However, if multiple devices access it simultaneously and a collision occurs, they both have to wait for a specific time before reinitiating the transmission process.

17.Explain FDMA, TDMA and CDMA

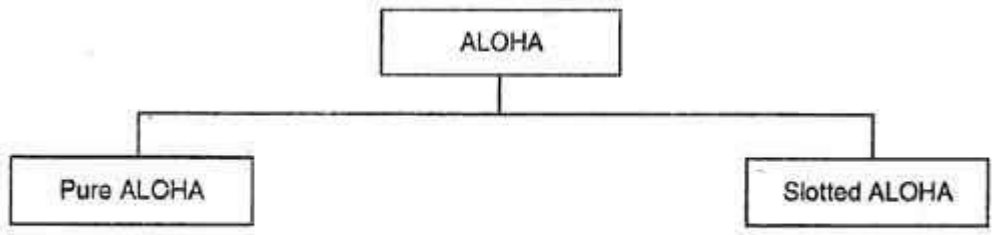
- **Frequency division multiple access(FDMA): In FDMA, the available bandwidth of the channel is divided into frequency bands and each frequency band is allocated to different stations. Each station on demand is allocated a predetermined band to send its all the time. To prevent station interference the allocated bands are separated from one another by small guard bands.**

- **Time division multiple access (TDMA) : In TDMA, the stations take turns to share the entire bandwidth of the channel. Each station is allocated a time slot during which it can transmit data for the complete bandwidth. Since TDMA transmissions are slotted, the receiver must be synchronized with the sender. Each station needs to know the beginning of its slot and the location of its slot for transmission.**

- **Code division multiple access(CDMA): In TDMA and FDMA data transmission from different stations are clearly separated either by time or by frequency. Code division multiple access is a digital wireless technology that uses spread spectrum techniques. CDMA does not assign a specific frequency to each user. Instead, every station uses the full available spectrum.**

18.Explain ALOHA and slotted ALOHA

- **ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.**
- **A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time.**
- **In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.**
- **There are two different versions of ALOHA**



Types of ALOHA

Pure ALOHA

- **In pure ALOHA, the stations transmit frames whenever they have data to send.**
- **When two or more stations transmit simultaneously, there is collision and the frames are destroyed.**

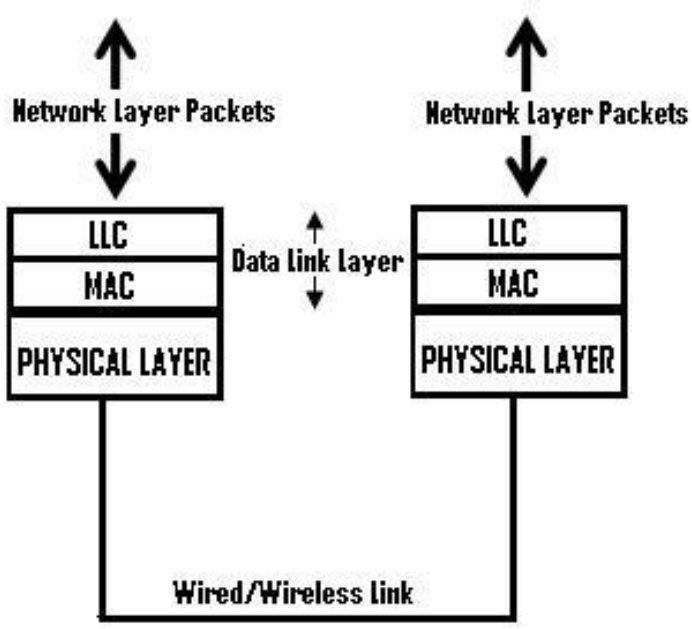
Slotted ALOHA

- **Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.**
- **In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.**

- **The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.**

20.Explain LLC and MAC sub layers of data link layer.

The data link layer is divided into two sublayers namely LLC (Logical Link Control) **and** MAC (Media Access Control)**.**



<u>Logical Link Control (LLC) sublayer</u> provides the logic for the data link. Thus, it controls the synchronization, flow control, and error checking functions of the data link layer.

<u>Media Access Control (MAC) sublayer</u> provides control for accessing the transmission medium. It is responsible for moving data packets from one network interface card (NIC) to another, across a shared transmission medium. Physical addressing is handled at the MAC sublayer. MAC is also handled at this layer. This refers to the method used to allocate network access to computers and prevent them from transmitting at the same time, causing data collisions. Common MAC methods include Carrier Sense Multiple Access/Collision Detection (CSMA/CD), used by Ethernet networks, Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), used by AppleTalk networks, and token passing, used by Token Ring and Fiber Distributed Data Interface (FDDI) networks.

Unit 5

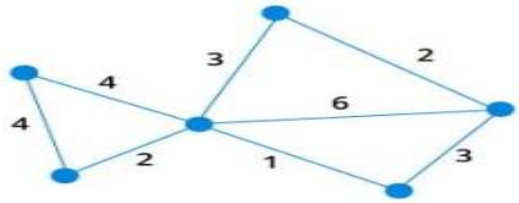
21. Explain the following:

a) Dijikstra's algorithm

- **Dijkstra's algorithm is a step-by-step process we can use to find the shortest path between two vertices in a weighted graph. This algorithm enables us to find shortest distances and minimum costs, making it a valuable tool.**

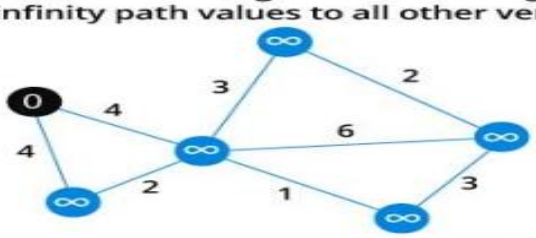
1

Start with a weighted graph



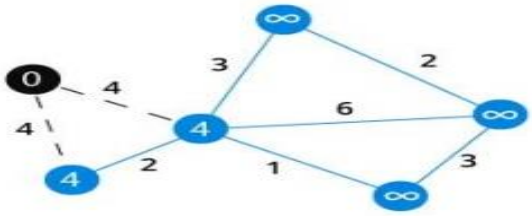
2

Choose a starting vertex and assign infinity path values to all other vertices



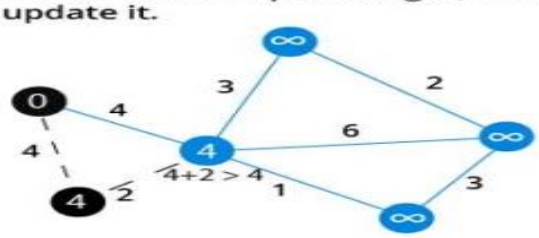
3

Go to each vertex adjacent to this vertex and update its path length



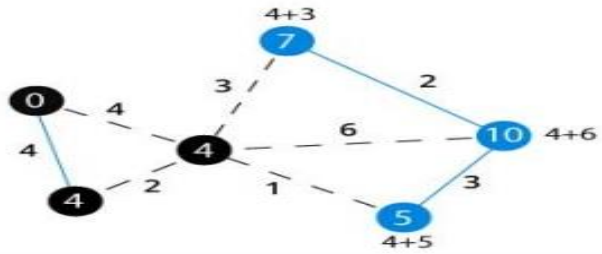
4

If the path length of adjacent vertex is lesser than new path length, don't update it.



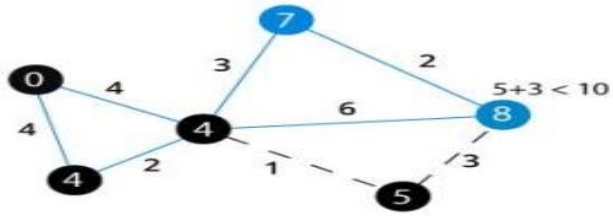
5

Avoid updating path lengths of already visited vertices



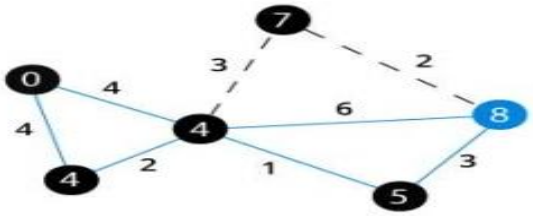
6

After each iteration, we pick the unvisited vertex with least path length. So we chose 5 before 7



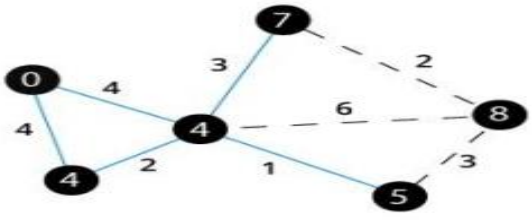
7

Notice how the rightmost vertex has its path length updated twice



8

Repeat until all the vertices have been visited



b) Token bucket algorithm.

- **The token bucket algorithm is based on an analogy of a fixed capacity bucket into which tokens, normally representing a unit of bytes or a single packet of predetermined size, are added at a fixed rate.**
- **When a packet is to be checked for conformance to the defined limits, the bucket is inspected to see if it contains sufficient tokens at that time. If so, the appropriate number of tokens, e.g. equivalent to the length of the packet in bytes, are removed ("cashed in"), and the packet is passed, e.g., for transmission.**
- **The packet does not conform if there are insufficient tokens in the bucket, and the contents of the bucket are not changed. Non-conformant packets can be treated in various ways:**

Algorithm

- **A token is added to the bucket every seconds**
- **The bucket can hold at the most tokens. If a token arrives when the bucket is full, it is discarded.**
- **When a packet (network layer PDU) of *n* bytes arrives,**
- **if at least *n* tokens are in the bucket, *n* tokens are removed from the bucket, and the packet is sent to the network.**
- **if fewer than *n* tokens are available, no tokens are removed from the bucket, and the packet is considered to be *non-conformant*.**

22. What is a bridge? Explain the various types of bridges.Repeated [Nov-Dec 2018]

- **It is type of computer network device that provides interconnection with other bridge network that uses same protocol**

Types of bridges:

- **Transparent bridges: The term transparent refers to the fact that stations are completely unaware of the presence of bridges in the network. When a transparent is added or removed from the system, reconfiguration of the stations in unnecessary.**
- **Source Routing Bridges: Source routing bridges were developed by the IEEE 802.5 Committee and are primarily used to interconnect token-ring networks. Unlike transparent bridges where filtering frames, forwarding and blocking functions are implemented in bridges, source routing bridges put these burden on the end stations. The main idea of source routing is that each station should determine the route to the destination when it wants to send a frame and therefore include the route information in the header of the frame.**

24.Illustrate open-loop congestion control

Open-loop policies, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or destination.

- **Admission control: Admission control is a quality-of-service mechanism that computes the resource requirements of a network flow and determines whether the resources are available for the flow. If the QoS of the new flow can be satisfied without violating QoS of existing flow, the flow is accepted; otherwise, the flow is rejected.**
- **Traffic shaping: one of the main causes of congestion is that traffic is often bursty data. When a source tries to send packets; it may not know exactly what its traffic flow looks like. if the source wants to ensure that the traffic flow conforms to the parameters of QoS, it should alter its traffic flow**

25.Explain different types of bridges in computer networks.

There are three types of bridges

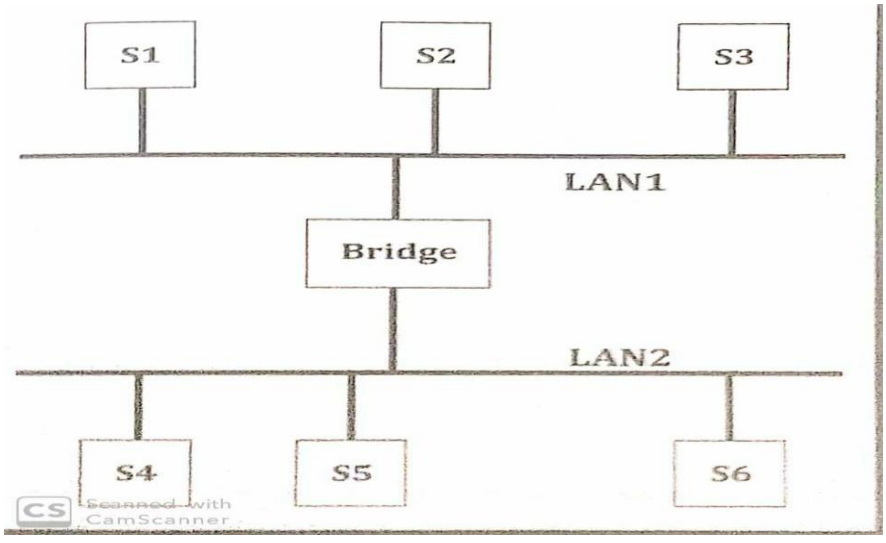
1. **Transparent bridges: The term transparent refers to the fact that stations are completely unaware of the presence of bridges in the network. When a transparent is added or removed from the system, reconfiguration of the stations is unnecessary.**

A transparent bridge performs the following 3 basic functions:

A. Forwards frames from one LAN to another

B. Learns where stations are attached to the LAN

C. Prevents loops in the topology



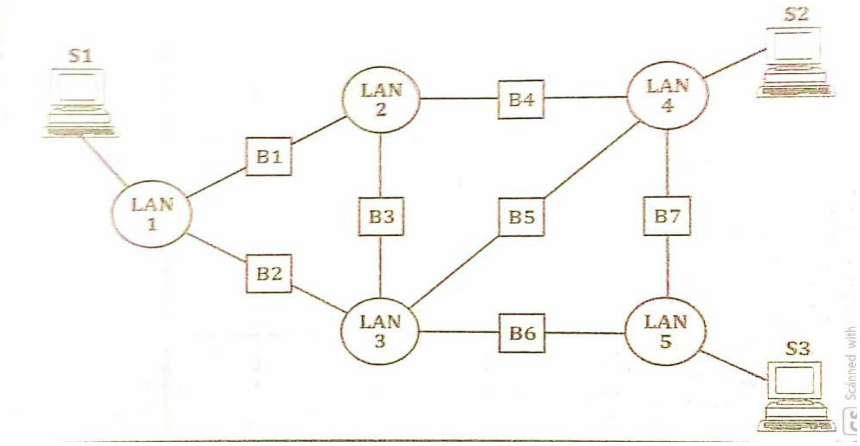
2. Source Routing bridges: It was developed by the IEEE 802.5 committee an are primarily used to interconnect token ring networks Unlike transparent bridges where filtering frames, forwarding and blocking functions are implemented in bridges, source routing

bridges put these burden on the end stations. The main idea of this is that reach station should determine the route to the destination when it wants to send a frame and therefore include the route information in the header of the frame. thus the problem boils down to finding good routes efficiently.

The solution is to first find all the paths from source to destination then calculate the distance for all the route the less distance path will be taken for transferring the frame from source to destination

As an example, if S1 wants to send a frame to S2, then a possible route is

a. **LAN 1 – B1 – LAN 2 – B4 – LAN 4**
b. **LAN 1 – B2 – LAN 3 – B5 – LAN 4**
c. **LAN 1 – B2 – LAN 3 – B3 LAN 2 – B4 – LAN 4**
d. **LAN 1 – B2 – LAN3 – B6 – LAN 5 – B7 LAN 4**



2. **Mixed Media Bridges: Bridges that interconnect LAN of different type are referred to as Mixed Media Bridge. This type of interconnection is not simple. Mixed media bridges can be discussed in terms of the interconnection of Ethernet and token ring LAN. These two LAN differ in their frame structure, their operation and their speed, and the bridge needs to take these difference into accounts.**

Section D

26. Compare packet switching with circuit switching.

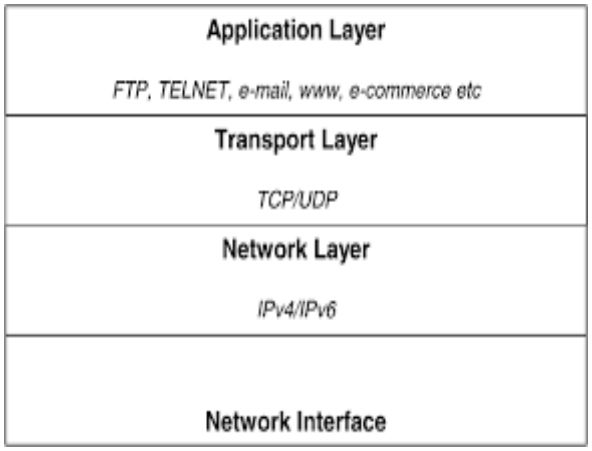
Packet switching	Circuit switching
1. Packet switching is connectionless which means the data is transmitted into small units called packets and a dynamic route is established for each pack	1. Circuit switching is a type of networking protocol in which a dedicated channel is established between two end points in a network for the duration of a transmission. Data transfer takes place after the circuit is established
2.Data is divided into small units called packets with each packet carrying small header containing signalling information	2. A physical path is established which is dedicated to a single connection between the two end points.
3.Dynamic route is established for each packet which carries the routing information.	3. Data transmission takes place after the circuit is established for the duration of the transmission.
4.Each data packet may take a different route to reach the destination, making it flexible throughout the session.	4. A dedicated routing path is followed throughout the transmission and no other user is allowed to use the circuit.
5. There is no end to end reservation of links.	5. It follows a uniform path throughout the session.
6.Each data packet carries the signalling information containing source and destination addresses in the packet header.	6. Data doesn't carry the signalling information and moves on its own.
7.It's mainly used for data and voice communication, and the delay is not uniform.	7. It's ideal for voice communication and the delay is uniform.

34. Explain TCP/IP model with a neat diagram.

TCP/IP model layers

TCP/IP functionality is divided into four layers, each of which include specific protocols.

- ***The application layer*** **provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).**
- ***The transport layer*** **is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.**
- ***The network layer*****, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.**
- ***The physical layer*** **consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).**



35. Explain OSI reference model in detail.

The model is proposed by the ISO (International Standards Organization). It is called ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems. The OSI Reference Model has 7 layers.

a. Physical Layer:

- **It is concerned with the actual physical attachment to the network i.e. it deals with the means of connecting two nodes in a network.**
- **It deals with transmitting raw bits over the communication channel.**
- **The design issues here deal with mechanical, electrical, timing interfaces and the physical transmission medium which lies below the physical layer.**

b. Data Link Layer:

- **It breaks the data into frames and passes it to the network layer. It also does:**
- **Error Control: To control transmission errors.**
- **Flow Control: To prevent the drowning of slow receiver by fast transmitter.**
- **Access Control: Control access to the shared channel. A special section of the DLL called the Medium Access Control sub layer deals with this.**

c. Network Layer:

- **It has the responsibility of preforming source to destination delivery of packets. It focuses on:**
- **Dynamic routing**
- **Congestion control**
- **Quality of service**
- **Addressing**
- **Integration of heterogeneous networks.**

e. Transport Layer:

- **It deals withControl of data flow in the network.**
- **Ensuring no loss of data.**
- **Ensuring that destination is not inundated with data.**
- **Ensuring that all pieces arrive correctly at the other end.**
- **It is a true end to end layer.**

e. Session Layer: Its features are:

- **Dialogue Control: Keeping track of whose turn it is to transmit.**
- **Token management: Preventing two parties from attempting the same critical operation at the same time.**

- **Synchronization: Check pointing long transmissions to allow them to continue from where they were after a crash.**

f. Presentation Layer: It is concerned with the following:

- **Syntax of information.**
- **Semantics of information.**
- **Compression**
- **Encoding of information.**

g. Application Layer: Application layer provide user interface and support for services like:

- **E-mail.**
- **Remote file access.**
- **File transfer**
- **Shared database management.**

Advantages of OSI Reference Model:

- **OSI Model distinguish between the services, interfaces and protocols.**
- **Protocols of OSI Model are very well hidden.**
- **They can be replaced by new protocols as technology changes.**
- **Supports connection oriented as well as connectionless service.**

Disadvantages of OSI Reference Model:

i. **Model was devised before the invention of protocols.**

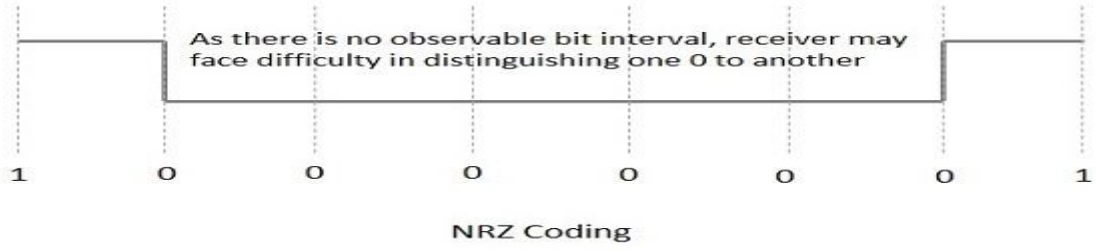
ii. **Fitting of protocols is a tedious task.**

36. Illustrate polar line encoding scheme.

A: Non Return to Zero (NRZ)

NRZ Codes has 1 for High voltage level and 0 for Low voltage level. The main behavior of NRZ codes is that the voltage level remains constant during bit interval. The end or start of a bit will not be indicated and it will maintain the same voltage state, if the value of the previous bit and the value of the present bit are same.

The following figure explains the concept of NRZ coding.



NRZ Coding

If the above example is considered, as there is a long sequence of constant voltage level and the clock synchronization may be lost due to the absence of bit interval, it becomes difficult for the receiver to differentiate between 0 and 1.

There are two variations in NRZ namely −

NRZ - L (NRZ – LEVEL)

There is a change in the polarity of the signal, only when the incoming signal changes from 1 to 0 or from 0 to 1. It is the same as NRZ, however, the first bit of the input signal should have a change of polarity.

NRZ - I (NRZ – INVERTED)

If a 1 occurs at the incoming signal, then there occurs a transition at the beginning of the bit interval. For a 0 at the incoming signal, there is no transition at the beginning of the bit interval.

NRZ codes has a disadvantage that the synchronization of the transmitter clock with the receiver clock gets completely disturbed, when there is a string of 1s and 0s. Hence, a separate clock line needs to be provided.

Bi-phase Encoding

The signal level is checked twice for every bit time, both initially and in the middle. Hence, the clock rate is double the data transfer rate and thus the modulation rate is also doubled. The clock is taken from the signal itself. The bandwidth required for this coding is greater.

There are two types of Bi-phase Encoding.

- **Bi-phase Manchester**
- **Differential Manchester**

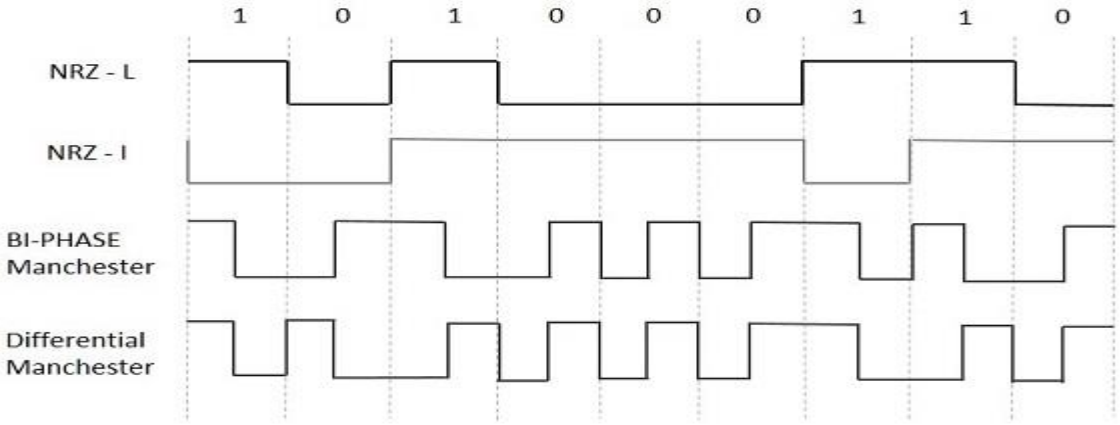
Bi-phase Manchester

In this type of coding, the transition is done at the middle of the bit-interval. The transition for the resultant pulse is from High to Low in the middle of the interval, for the input bit 1. While the transition is from Low to High for the input bit 0.

Differential Manchester

In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is 0. If no transition occurs at the beginning of the bit interval, then the input bit is 1.

The following figure illustrates the waveforms of NRZ-L, NRZ-I, Bi-phase Manchester and Differential Manchester coding for different digital inputs.



37.Explain the following:

a) Modems:Modem is abbreviation for Modulator – Demodulator. Modems are used for data transfer from on computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.

Modulator converts information from digital mode to analog mode at the transmitting end and demodulator converts the same from analog to digital at receiving end. The process of converting analog signals of one computer network into digital signals of another computer network so they can be processed by a receiving computer is referred to as digitizing.

Types of Modems

• Modems can be of several types and they can be categorized in a number of ways.

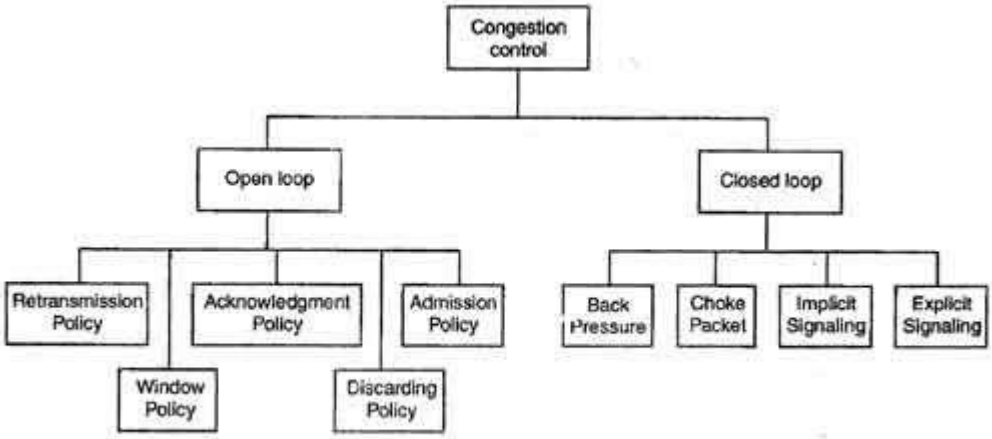
• Categorization is usually based on the following basic modem features:

1. Directional capacity: half duplex modem and full duplex modem.

2. Connection to the line: 2-wire modem and 4-wire modem.

3. Transmission mode: asynchronous modem and synchronous modem.

b).Congestion control.Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.). Network congestion occurs in case of traffic overloading.



Types of Congestion Control Methods

38. Explain any routing algorithms.

Routing is process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes which data packets follow. Various routing algorithm are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach destination efficiently.

Classification of Routing Algorithms: The routing algorithms can be classified as follows:

1.Adaptive Algorithms –These are the algorithms which change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops and estimated transit time.

2.Non-AdaptiveAlgorithms–These are the algorithms which do not change their routing decisions once they have been selected. This is also known as static routing as route to be taken is computed in advance and downloaded to routers when router is booted.

Further these are classified as follows:

(a) Flooding – Flooding is the static routing algorithm. In this algorithm, every incoming packet is sent on all outgoing lines except the line on which it has arrived.

(b) Random walk – In this method, packets are sent host by host or node by node to one of its neighbours randomly. This is highly robust method which is usually implemented by sending packets onto the link which is least queued.