Q1. Explain osi model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.
-

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical layer

- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- This layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the data from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the

transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

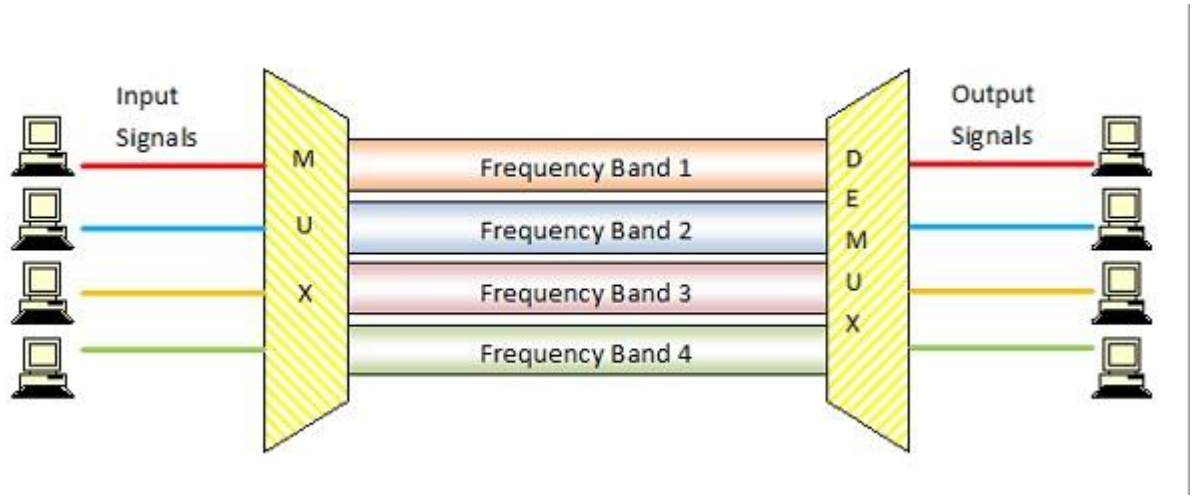
Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

Q2. Explain fdm and tdm with figures

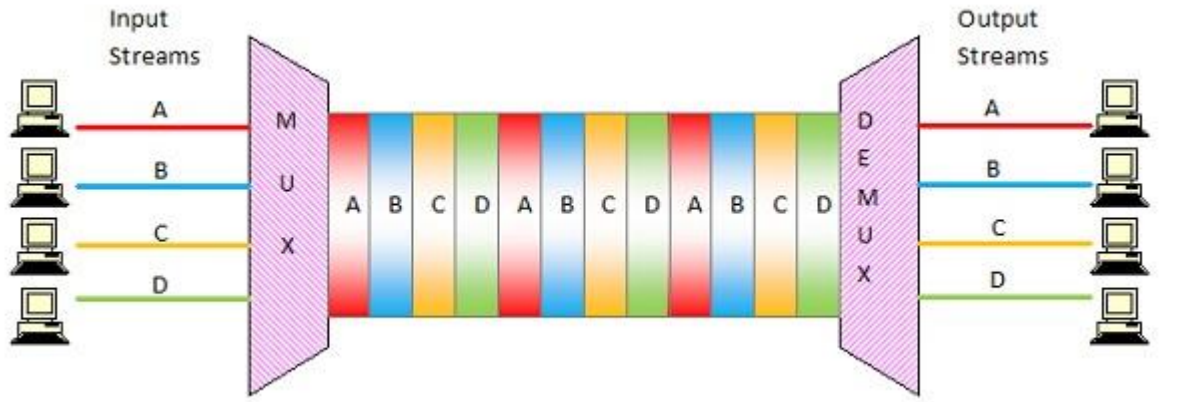
In FDM, the total bandwidth is divided to a set of frequency bands that do not overlap. Each of these bands is a carrier of a different signal that is generated and modulated by one of the sending devices. The frequency bands are separated from one another by strips of unused frequencies called the guard bands, to prevent overlapping of signals.

The modulated signals are combined together using a multiplexer (MUX) in the sending end. The combined signal is transmitted over the communication channel, thus allowing multiple independent data streams to be transmitted simultaneously. At the receiving end, the individual signals are extracted from the combined signal by the process of demultiplexing (DEMUX).



tdm

In TDM, the data flow of each input stream is divided into units. One unit may be 1 bit, 1 byte, or a block of few bytes. Each input unit is allotted an input time slot. One input unit corresponds to one output unit and is allotted an output time slot. During transmission, one unit of each of the input streams is allotted one-time slot, periodically, in a sequence, on a rotational basis. This system is popularly called round-robin system.



Q3. Guided transmission media

Guided Media is also known as **Wired or Bounded** transmission media. A signal travelling the media is directed and confined by the physical limits of the medium.

Advantage of guided media

- More **secure**
- Provides **high speed**
- Used for **shorter distances**

Disadvantage of guided media

- **Need Physical link**
- **Time Consuming**

Three Types of Guided Media

There are three **types of guided media** which are **Twisted-Pair Cable**, **Coaxial Cable** and **Fiber-Optic Cable** are explained below.

Twisted-Pair Cable

Twisted-Pair Cable consists of **two insulated conductors wire wound** (normally copper), twisted together. In which one wire is to carry the signal to destination and other is used as a ground reference. **Twisting is done** so that the **noise will equally affect the wire from the external environment**.

Advantage of Twisted Pair Cable

1. The frequency range is 0 to 3.5 kHz
2. Repeater spacing is 2 KM

Disadvantage of Twisted Pair Cable

1. No capacity to carrying a signal over long distances without the use of repeaters.
2. Not suitable for broadband applications because of low bandwidth capacity.
3. Poor security and easy to tap.

Applications of Twisted Pair Cables

1. It is used in telephone lines.
2. Also used in the DSL line (ADSL)
3. ISDN (Integrated Services Digital Network).

Coaxial Cable

Coaxial cable has a **central core conductor of stranded or solid wire** (usually copper) enclosed in an insulating protection cover, which is, in turn, encased in an outer conductor of metal foil or a combination of the two. The outer metallic work as a shield against noise and as a conductor, which complete the circuit. The whole cable is covered by a plastic cover.

Two types of Coaxial Cable

1. **BaseBand**: (50 ohms) used for digital transmission.
2. **BroadBand**: uses for analog transmission on standard TV cable.

Coaxial cable advantages

1. Carries signals of higher data rate and bandwidth.
2. Used in analog telephone networks and traditional Cable TV networks.

Coaxial cable disadvantages

1. The network depends on a single cable.
2. Expensive and difficult to install when compared with twisted pair.

Applications of Coaxial cable

- Used in **analog telephone networks**, could carry 10,000 voice signals.

Fiber-Optic Cable

Fiber-Optic Cable is **made of glass** and transmits of data is based on the concept of **reflection of light through glass**. A glass core is surrounded by less dense glass called **cladding**.

Q4. Explain tcp/ip model

TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Some of the protocols followed are: **IP,ARP**

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.

- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer: http,snmp,smtp

Q5. What are the uses of CN?

- **Information and Resource Sharing** − Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.
- **Retrieving Remote Information** − Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.
- **Speedy Interpersonal Communication** − Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by manifold times through social networking services.
- **E-Commerce** − Computer networks have paved way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.
- **Highly Reliable Systems** − Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.
- **Cost–Effective Systems** − Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.
- **VoIP** − VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

Q6. Write a note on network hardware

Network Cables

Network cables are the transmission media to transfer data from one device to another. A commonly used network cable is category 5 cable with RJ – 45 connector, as shown in the image below:

Routers

A router is a connecting device that transfers data packets between different computer networks. Typically, they are used to connect a PC or an organization's LAN to a broadband internet connection. They contain RJ-45 ports so that computers and other devices can connect with them using network cables.

Repeaters, Hubs, and Switches

Repeaters, hubs and switches connect network devices together so that they can function as a single segment.

A repeater receives a signal and regenerates it before re-transmitting so that it can travel longer distances.

A hub is a multiport repeater having several input/output ports, so that input at any port is available at every other port.

A switch receives data from a port, uses packet switching to resolve the destination device and then forwards the data to the particular destination, rather than broadcasting it as a hub.

Bridges

A bridge connects two separate Ethernet network segments. It forwards packets from the source network to the destined network.

Gateways

A gateway connects entirely different networks that work upon different protocols. It is the entry and the exit point of a network and controls access to other networks.

Network Interface Cards

NIC is a component of the computer to connect it to a network. Network cards are of two types: Internal network cards and external network cards

E1. Explain network software wrt protocol hierarchies

E2. Explain unguided transmission media

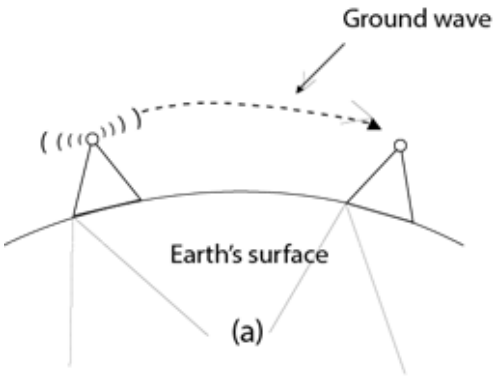
UnGuided Transmission

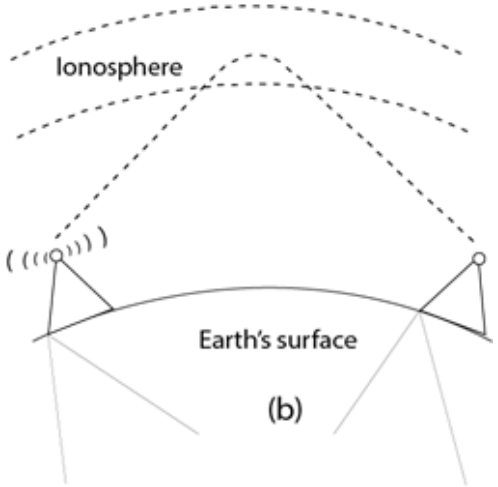
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.





Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.

- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

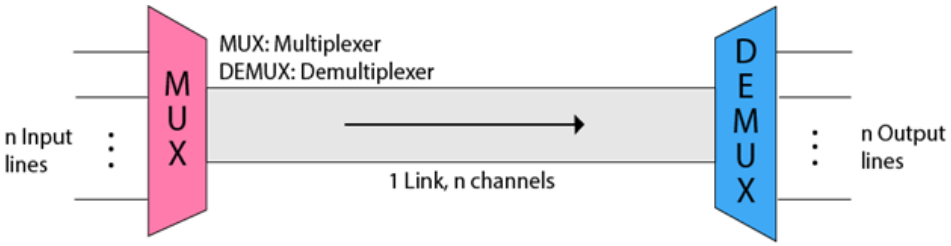
E3. Explain multiplexing in detail

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

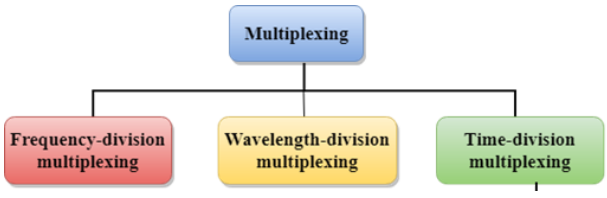
- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.



- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.



E4. Describe pstn.

PSTN (public switched telephone network) is the world's collection of interconnected voice-oriented public telephone networks.

How PSTN works

A public switched telephone network is a combination of telephone networks used worldwide, including telephone lines, fiber optic cables, switching centers, cellular networks, satellites and cable systems. A PSTN lets users make landline telephone calls to one another.

A PSTN is made up of switches at centralized points on a network that function as nodes to enable communication between two points on the network. A call is placed after being routed through multiple switches. Voice signals can then travel over the connected phone lines.

The PSTN phone line is used with traditional dial-up network modems to connect a computer to the Internet. Dial-up Internet connections support up to 56 Kbps. In the early days of the Internet, this was the main method for home Internet access but it became obsolete with the introduction of broadband Internet services

PSTN structure

The traditional PSTN has a hierarchical architecture and a star structure. The individual subscriber lines are connected to a local exchange, which communicates with trunk exchanges as well as main and central exchanges. The lines within a local exchange typically have the same area code. A user who wants to call a number outside the local exchange has to add an area code. To make an international call, a user has to dial the country code

Unit 2

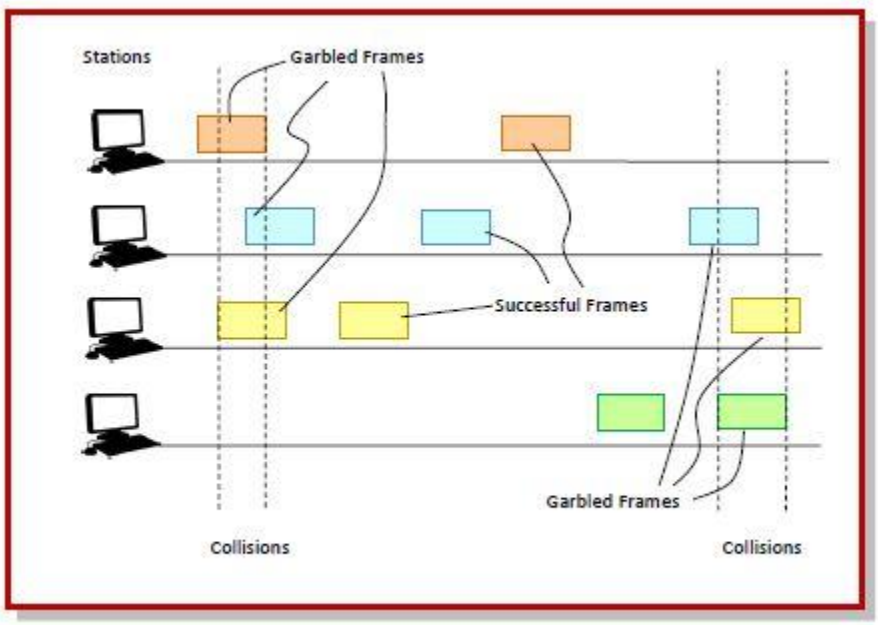
Q1. Explain Pure aloha and slotted aloha protocol

In pure ALOHA, the time of transmission is continuous. Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a **random** amount of time before retransmitting it.

Working Principle

After transmitting a frame, a station waits for a finite period of time to receive an acknowledgement. If the acknowledgement is not received within this time,the station assumes that the frame has been destroyed due to collision and resends the frame.

A collision occurs if more than one frame tries to occupy the channel at the same time



Throughput=S, is calculated as the number of transmission attempts per frame time, G, multiplied by the probability of success, $P(0)$

$$S=G.P(0)S=G.P(0)$$

$$S=G.e-2G$$

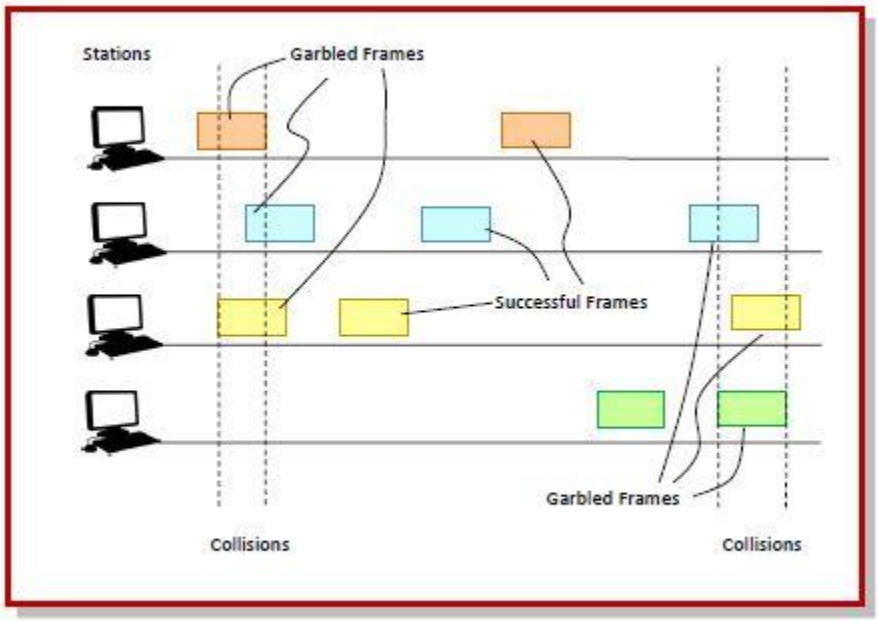
Maximum efficiency is 18.4%

Slotted ALOHA was introduced in 1972 by Robert as an improvement over pure ALOHA. Here, time is divided into discrete intervals called slots, corresponding to a frame.

Working Principle

The communicating stations agree upon the slot boundaries. Any station can send only one frame at each slot. Also, the stations cannot transmit at any time whenever a frame is available. They should wait for the beginning of the next slot.

However, there still can be collisions. If more than one frame transmits at the beginning of a slot, collisions occur. The collision duration is 1 slot. The situation is depicted in the following diagram−



The throughput, S, is calculated as the number of transmission attempts per frame time, G, multiplied by the probability of success, PP(0).

$$S=G.P(0)S=G.P(0)$$

or

$$S=Ge−G$$

maximum efficiency is 36.8%

Q2,6. With a neat figures, explain briefly i) Go Back N ii) Selective Repeat ARQ Protocols

1.Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request.

2. It is a data link layer protocol that uses a sliding window method.

3. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

4. The size of the sender window is N in this protocol.

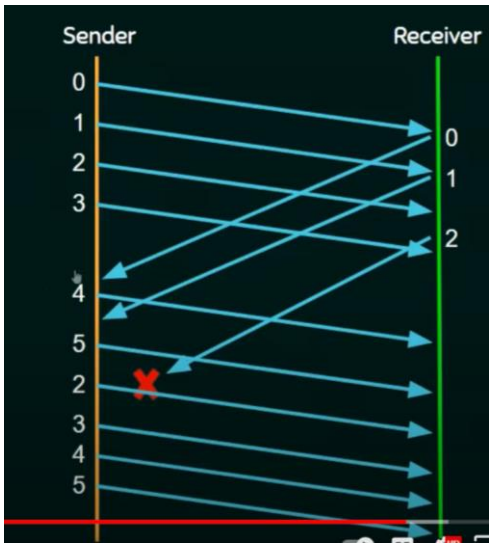
5. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

6. If the receiver receives a corrupted frame, it cancels it.

7. The receiver does not accept a corrupted frame.

8. When the timer expires, the sender sends the correct frame again.

9. The design of the Go-Back-N ARQ protocol is shown below



Selective Repeat ARQ:

1. Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method.

2. The Go-back-N ARQ protocol works well if it has fewer errors

. 3. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again.

4. So, we use the Selective Repeat ARQ protocol.

5. In this protocol, the size of the sender window is always equal to the size of the receiver window.

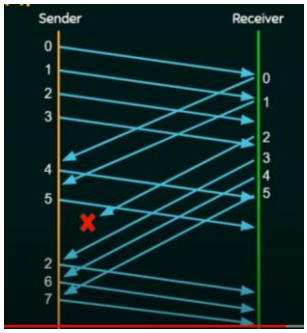
6. The size of the sliding window is always greater than 1.

7. If the receiver receives a corrupt frame, it does not directly discard it.

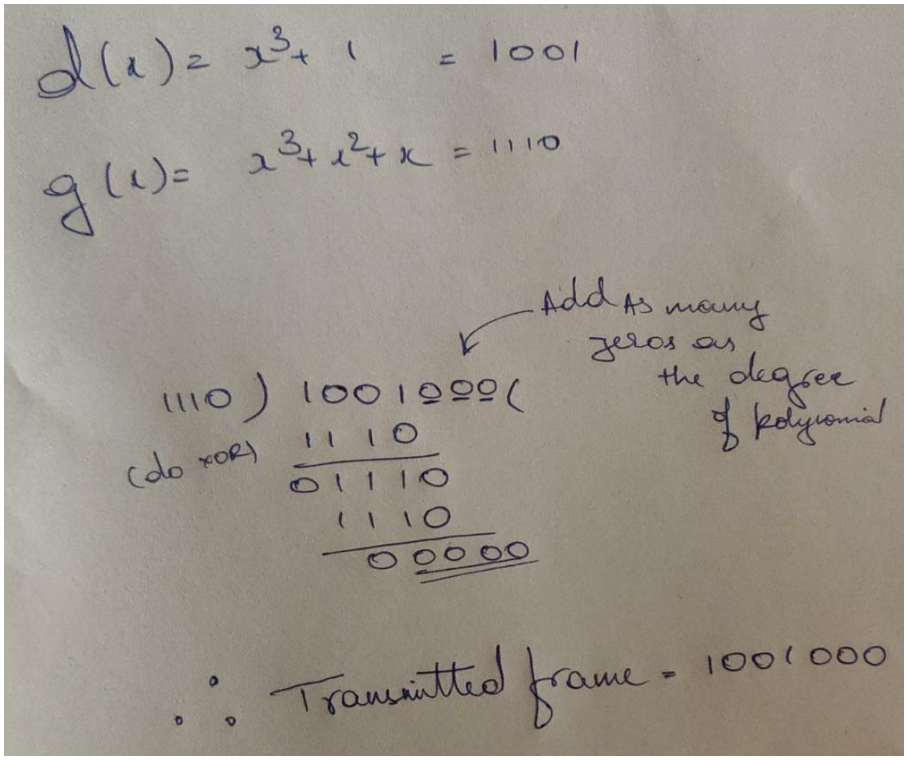
8. It sends a negative acknowledgment to the sender.

9. The sender sends that frame again as soon as on the receiving negative acknowledgment.

10. There is no waiting for any time-out to send that frame.



Q3. Find the code word C(X), using CRC for the information d(X) =X3+1 with generator polynomial g(X) = X3+X2+X



Q4. EXPLAIN DATALINK LAYER DESIGN ISSUES

The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

Services to the Network Layer

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer.The primary function of this layer is to provide a well defined service interface to network layer above it

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer

Error Control

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

Flow Control

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

- Feedback based flow control
- Rate based flow control

Q5. EXPLAIN CSMA,CSMA/CD PROTOCOL IN DETAIL

Carrier Sense Multiple Access (CSMA) is a network protocol for carriertransmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and transmits if the channel is not busy. Using CMSA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.

Working Principle

When a station has frames to transmit, it attempts to detect presence of the carrier signal from the other nodes connected to the shared channel. If a carrier signal is detected, it implies that a transmission is in progress. The station waits till the ongoing transmission executes to completion, and then initiates its own transmission. Generally, transmissions by the node are received by all other nodes connected to the channel.

Since, the nodes detect for a transmission before sending their own frames,collision of frames is reduced. However, if two nodes detect an idle channel at the same time, they may simultaneously initiate transmission. This would cause the frames to garble resulting in a collision.

CSMA / CD:

CSMA / CD stands for Carrier Sense Multiple Access / Collision Detection. This access control method works as follows

Step-01: Sensing the Carrier

- Any station willing to transmit the data senses the carrier.
- If it finds the carrier free, it starts transmitting its data packet otherwise not.

How?

- Each station can sense the carrier only at its point of contact with the carrier.
- It is not possible for any station to sense the entire carrier.
- Thus, there is a huge possibility that a station might sense the carrier free even when it is actually not.

Step-02: Detecting the Collision In CSMA / CD,

• It is the responsibility of the transmitting station to detect the collision.

• For detecting the collision, CSMA / CD implements the following condition.

• This condition is followed by each station-

• Transmission delay >= 2 x Propagation delay Meaning According to this condition,

• Each station must transmit the data packet of size whose transmission delay is at least twice its propagation delay.

• If the size of data packet is smaller, then collision detection would not be possible.

Step-03: Releasing Jam Signal

1. Jam signal is a 48-bit signal.

2. It is released by the transmitting stations as soon as they detect a collision.

3. It alerts the other stations not to transmit their data immediately after the collision.

4. Otherwise, there is a possibility of collision again with the same data packet.

5. Ethernet sends the jam signal at a frequency other than the frequency of data signals.

6. This ensures that jam signal does not collide with the data signals undergone collision.

Step-04: Waiting for Back Off Time

1. After the collision, the transmitting station waits for some random amount of time called as back off time.

2. After back off time, it tries transmitting the data packet again.

3. If again the collision occurs, then station again waits for some random back off time and then tries again.

4. The station keeps trying until the back off time reaches its limit.

5. After the limit is reached, station aborts the transmission.

Q7,check page 13