ನಹಿ ಜ್ಞಾನೇನ ಸದೃಶಮ್

ಶ್ರೀ ಮೇಧಾ ಪದವಿ ಮತ್ತು ಪದವಿ-ಪೂರ್ವ ಮಹಾವಿದ್ಯಾಲಯ

SHREE MEDHA DEGREE AND PRE-UNIVERSITY COLLEGE

ISO 9001-2015 Certified College

#3 Fort Rd, Ballari

DEPARTMENT OF COMPUTER SCIENCE

# PREVIOUS YEAR's Q&A

# COMPUTER NETWORK

Mr. Chaitanya Reddy S V

2021

# 2m Questions & Answers

**01. Define computer networks [2019]**

**Ans.**

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes. The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies.

**02. Mention any four layers of OSI Model [2019, 2017]**

**Ans.**

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer.

**03. Expand PCM and IP [2019, 2017]**

**Ans.**

**PCM-** (Pulse Code Modulation).

**IP-** (Internet Protocol).

**04. What is spread spectrum? [2019]**

**Ans.**

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes. The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies.



**05. Define Switching? [2019, 2018, 2016]**

**Ans.**

**Switching-** In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

**06. What is Framing? [2019]**

**Ans.**

Frame is continuously used in Time Division Multiplexing process. Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer.

**07. Expand HDLC [2019]**

**Ans.**

**HDLC: (**High-Level Data Link Control).

**08. What is fast Ethernet? [2019]**

**Ans.**

Fast Ethernet was introduced in 1995 as the IEEE 802.3u standard and remained the fastest version of Ethernet for three years before the introduction of Gigabit Ethernet. The acronym GE/FE is sometimes used for devices supporting both standards.

**09. Define repeaters and Bridges [2019, 2018, 2017]**

**Ans.**

**Repeater**-A Repeater enables signals to travel longer distances over a network. Repeaters work at the OSI's Physical layer. A repeater regenerates the received signals and then retransmits the regenerated (or conditioned) signals on other segments.

**Bridges**-Like a repeater, a bridge can join segments or workgroup LANs. However, a bridge can also divide a network to isolate traffic or problems. For example, if the volume of traffic from one or two computers or a single department is flooding the network with data and slowing down entire operation, a bridge can isolate those computers or that department.

**10. What is Internetworking? [2019]**

**Ans.**

Internetworking is the practice of interconnecting multiple computer networks, such that any pair of hosts in the connected networks can exchange messages irrespective of their hardware-level networking technology. The resulting system of interconnected networks are called an internetwork, or simply an internet.

**11. Name the fundamental characteristics on which the data communication system depends [2018, 2017]**

**Ans.**

The fundamental characteristics in which the data communication system depends are:

- Delivery
- Accuracy
- Timeliness
- Jitter.

**12. Explain Composite signals [2018]**

**Ans.**

A composite signal is a combination of two or more simple sine waves with different frequency, phase and amplitude.

**13. Expand the following a) RARP b) PCM [2018]**

**Ans.**

RARP: (Reverse Address Resolution Protocol).
PCM: (Pulse Code Modulation).

**14. What is line coding? [2019, 2017, 2018]**

**Ans.**

Line coding is the process of converting digital data to digital signals. Data, in the form of text, Numbers, graphical images, audio, or video, are stored in computer memory as sequences of bits.

Line coding converts a sequence of bits to a digital signal. At the sender, digital data are encoded into a digital signal; at the receiver, the digital data are recreated by decoding the digital signal.

**15. How delay effects in Virtual-Circuit Networks [2018]**

**Ans.**

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. The virtual-circuit shares characteristics of both. Packets form a single message travel along the Same path.

**16. What is Hamming Distance? [2018]**

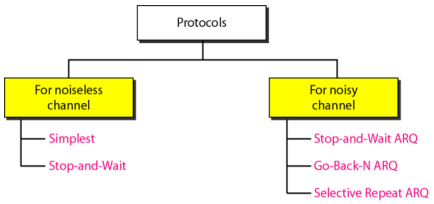
**Ans.**

Hamming distance is a metric for comparing two binary data strings. While comparing two binary strings of equal length, hamming distance is the number of bit positions in which the two bits are different. It is used for error detection or error correction when data is transmitted

**17. Mention the protocols used in Noisy Channels [2018]**

**Ans.**

- Stop-and-Wait Automatic Repeat Request.
- Go-Back-N Automatic Repeat Request.
- Selective Repeat Automatic Repeat Request.




**18. What is Ethernet and Token-passing? [2018]**

**Ans.**

Ethernet is a way of connecting computers together in a local area network or LAN. It has been the most widely used method of linking computers together in LANs since the 1990s. The basic idea of its design is that multiple computers have access to it and can send data at any time.

Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area network (WAN).

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

In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens.
A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
In Token ring, token is passed from one station to another adjacent station in the ring whereas in case of Token bus, each station
uses the bus to send the token to the next station in some predefined order.

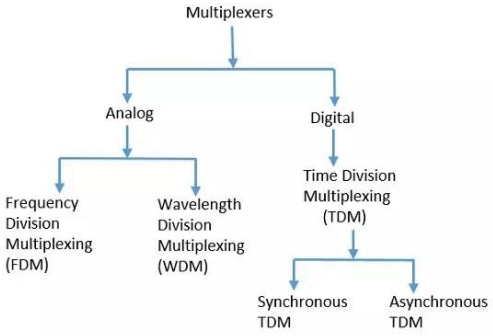
**19. Define Multiplexing, Mention the types of Multiplexing [2017]**

**Ans.**

Multiplexing is the process of combining multiple signals into one signal, over a shared medium. If analog signals are multiplexed, it is Analog Multiplexing and if digital signals are multiplexed, that process is Digital Multiplexing.

**Types of Multiplexers:**

There are mainly two types of multiplexers, namely analog and digital.
They are further divided into FDM, WDM, and TDM.



**20. What is a routing table? Give an Example [2017]**

**Ans.**

A Router is a networking device that forwards data packets between computer network. This device is usually connected to two or more different networks. When a data packet comes to a router port, the router reads address information in packet to determine out which port the packet will be sent. For example, a router provides you with the internet access by connecting your LAN with the Internet.

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed.

**21. What are the different types of errors? [2017]**

**Ans.**

Errors are normally classified in three categories

- Systematic error
- Random error
- Blunders

**22. What is error control and flow control? [2017]**

**Ans.**

Error control: - the error control function of data link layer detects
The errors in transmitted frames and re-transmit all the erroneous frames.
Flow control: - it is an important function of the data link layer. It refers to a sender how much data it can transmit before waiting for acknowledgement
From the receiver.

**23. What is tunneling? [2017]**

**Ans.**

A tunnelling protocol is a communications protocol that allows for the movement of data from one network to another. It involves allowing private network. Communications to be sent across a public network (such as the internet)
Through a process called encapsulation.

**24. Define Communication Networks. [2016]**

**Ans.**

Organizational members connect into a various number of groups and as members of the group, they interact with each other in a specific manner. The path along which they interact is called communication network.
It is type of pattern in which information flows between the members of the group.

**25. Explain Analog Signal. [2016]**

**Ans.**

An analog signal is any continuous signal for which the time- varying feature of the signal is a representation of some other time-varying quantity.

**26. How delay distortion effects communication? [2016]**

**Ans.**

Delay distortion is a guided transmission media phenomenon where network data signals are transmitted via a medium at a certain frequency and speed this means that all signals do not arrive at same time, resulting in distortion of the signal.

**27. With an example explain single bit error. [2016]**

**Ans.**

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.

Example: if eight wires are used to send the eight bits of a byte, if one the wire is noisy, then single-bit is corrupted per byte.

**28. What is the use of negative acknowledgement? [2016]**

**Ans.**

The negative-acknowledgement (NAK or NACK) signal is sent to reject a previously received message or to indicate some kind of error. Acknowledgement inform a sender of the receiver's sate so that it can adjust its own state accordingly.

**29. Explain the role of CSMA in increasing the performance. [2016]**

**Ans.**

The CSMA/CA is protocol used in the case of IEEE 802.11 standard 19 that allows nodes to share the channel in a competitive way while avoiding collisions. The nodes starts transmission if the medium is idle during the whole DIFS period. Otherwise, it should delay its transmission until the medium becomes available 19.

**30. Define IPV4 address. what is its length? [2016]**

**Ans.**

IPV4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation.

A 32-bit address contains two primary parts the network prfix and the host number. All hosts within a single network share the same network address. Each host also has an address that unique identifies it.

## 5m Questions & Answers

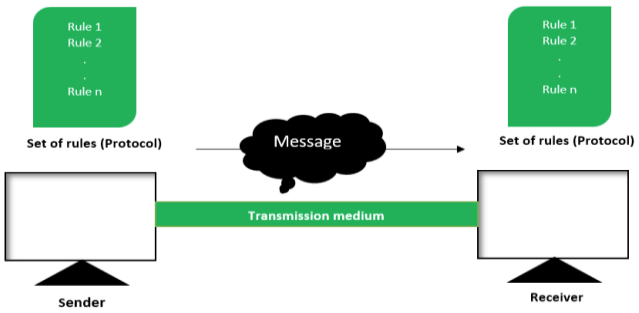
**01. what is data communication? Explain the components of data communication [2019, 2017]**

**Ans.**

Data communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum Communication, communicating devices must be part of communication system made up of a combination of hardware or software devices and programs.

Data communication system components

There are mainly five components of a data communication system




- Message
- Sender
- Receiver
- Transmission medium
- Set of rules(protocol)
- Message: This is most useful asset of a data simply refers to data or piece of information which is to be communicated.

  A message could be in any form, it may be in form of text , file, an audio file, a video file, etc.
- Sender: To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data.

Communication system it is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video, camera, or a workstation, etc.

- Receiver: it is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.
- Transmission medium: in entire process of data communication, there must be something which could act as a bridge between sender and receiver, transmission medium plays that part. It is physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires)
  Example: - twisted pair cable, fibre optical cable, radio waves, microwaves, etc.

Set of rules(protocol): To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communication devices.

**02. what is line coding? Explain different types of line coding schemes [2019]**

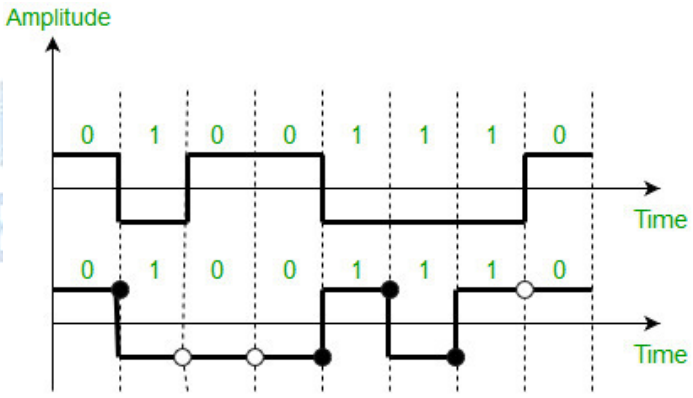
**Ans.**

Line coding is the process of converting digital data to digital signals. By this technique we convert a sequence of bits to a digital signal. At the sender side digital data are encoded into a digital signal and at the receiver side the digital data are recreated by decoding the digital signal.

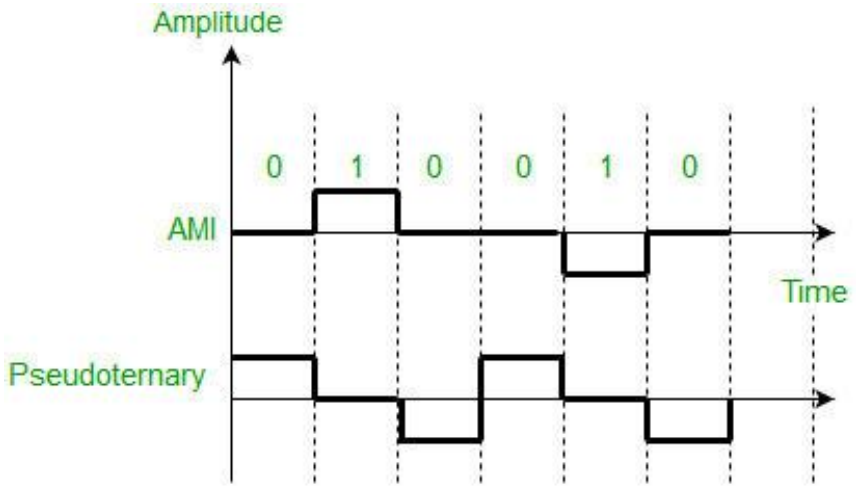
There are three types of line coding schemas: -

I. Polar
II. Bipolar
III. Manchester

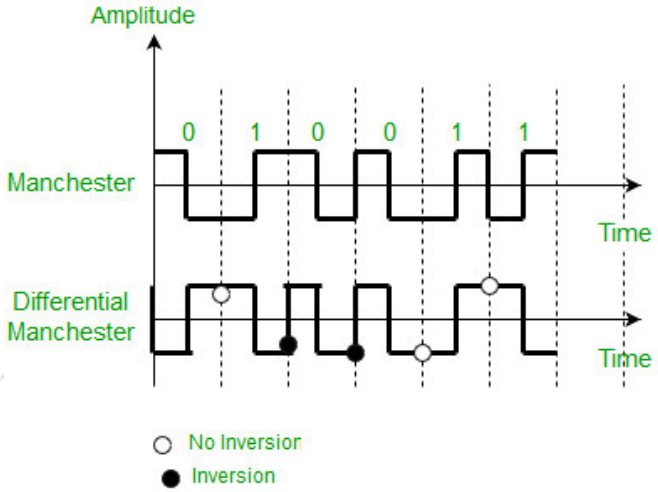
Polar: - binary 1's and 0's are represented by equal positive and negative levels.




Bipolar: binary 1's are represented by alternating positive or negative values. The binary 0 is represented by a zero level. The term seditionary refers to the rules to the use of 3 encoded signal levels to represent two-level (binary) data. This is also called alternate mark inversion (AMI) signalling.




Manchester: each binary 1 is represented by a positive half-bit period pulse followed by a negative half-bit period pulse. Similarly, a binary 0 is represented by a negative half-bit period pulse followed by positive half-bit period pulse this type of a signalling is also called split-phase encoding.




**03. Explain virtual circuit networks [2019]**

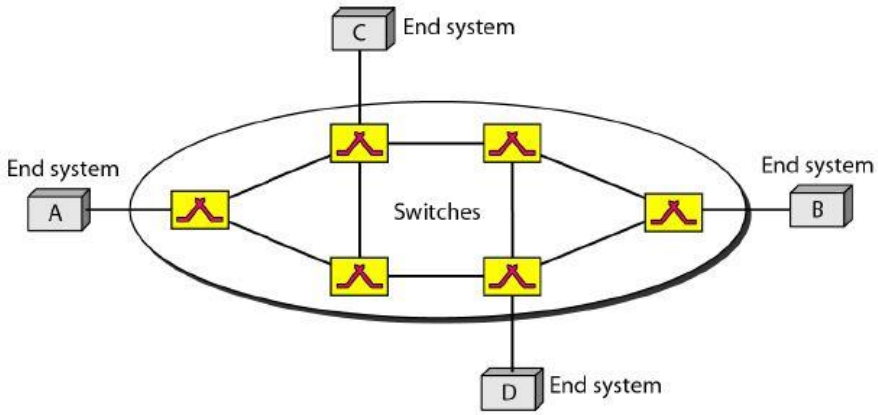
**Ans.**

It is also known as connection oriented switched.

In the case of virtual circuit switching preplanner root is established before the message are sent.

In this approach the path is fixed for the duration of logical connection.

A virtual circuit (VC) is a means of transporting data over a packet-switched network in such a way that it appears as though there is a dedicated physical link between the source and destination end systems of this data. the term virtual circuit is synonymous with virtual connection. Before a connection or



virtual circuit may be used, it must be established between two or more nodes or software applications by means of call setup. After that, a bit stream or byte stream may be delivered between the nodes; hence, a virtual circuit protocol allows higher-level protocols to avoid dealing with the division of the data into protocol data units. Many virtual circuit protocols, but not all, provide reliable communication service through the use of the data retransmission invoked by error detection and automatic repeat request (ARQ).

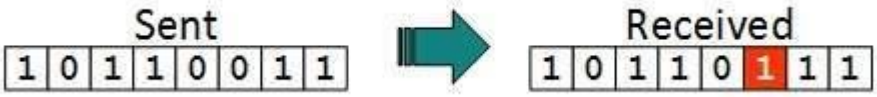
**04. What is an error? Explain the types of errors with an example [2019]**

**Ans.**

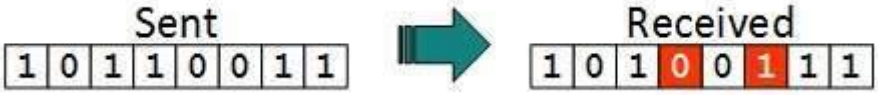
It is the problem of lost and changed appearing bits while data bits are transmitted between sender and receiver in a computer network
Bit errors are of 3 types:

1. Single bit error
2. Multiple bit error
3. Burst error

Single bit error: -in single bit error only one error is occurred.
The only one bit of a given data unit is changed from 1 to 0 or from 0 to,
The term single-bit error means that only one bit of given data unit (such as a byte, character, or data unit).




2. multiple bit error: - In data sequence, if there is a change in two or more bits of a data sequence of a transmitter to receiver, it is known as multiple bit error. This type of error mostly occurs in both serial and parallel type data communication networks.




3. Burst error: - this change of the set of bits in data sequence is known as burst error this type of data error is calculated in from the first-bit change to last bit change.


**05. Explain any five connecting devices [2019]**

**Ans.**

Here is the common network device list

- Hub
- Switch
- Router

- Bridge
- Gateway
- Modem

**Hub**: - Hubs connect multiple computer networking devices together. A hub also acts as repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.

**Switch**: - switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and allows connections to systems like hubs or routers.

**Router**: - routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. Routers are intelligent devices, and they store information about the networks they're connected to.

**Bridge**: - bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware media access control (MCA) addresses for transferring frames.

**Gateway**: - gateways normally work at the transport and session layers of the OSI model. At the transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as open system interconnection and transmission control protocol/ internet protocol.

**Modems**: - modems are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location. The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer.

**06. Write a different between IPV4 and IPV6 [2019]**

**Ans.**

**IPV4: -**

- IPV4 is 32-bit IP address.
- IPV4 is a numeric addressing method.
- IPV4 is the binary bits are separated by dot(.)
- IPV4 offers 12 header files
- IPV4 supports broadcast.
- IPV4 has check sum files.
- It is simple.
- Small address space
- IPV4 supports VLSM (virtual length submet mark)
- IPV4 length of header filed is 20.

**IPV6: -**

- IPV6 is 128-bit IP address.
- Ipv6 is an alpha numerical addressing method.
- IPV6 the binary bits are separated by colon (;)

- IPV6 offers 8 header files.
- IPV6 does not support broad cost.
- IPV6 does not have check sum fields.
- It is complex.
- Large address space
- IPV6 does not supports VLSM.
- IPV6 length of header fields is 40.

| IPV4 | IPV6 |
|---|---|
| IPv4 has 32-bit address length | IPv6 has 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end connection integrity is Unachievable | In IPv6 end to end connection integrity is Achievable |
| It can generate $4.29\times10^9$ address space | Address space of IPv6 is quite large it can produce $3.4\times10^{38}$ address space |
| Security feature is dependent on application | IPSEC is inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation performed only by sender |
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses flow label field in the header |
| In IPv4 checksum field is available | In IPv6 checksum field is not available |
| It has broadcast Message Transmission Scheme | In IPv6 multicast and any cast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| IPv4 has header of 20-60 bytes. | IPv6 has header of 40 bytes fixed |

**07. Define topology Explain categories of topology with a neat diagram [2018]**
**Ans.**

The Actual Geographical Appearance of the Computer System and its resources in the network or Layout of the networking is termed as Network Topology.

The different types of Topologies are: -

1. Bus Topology.
2. Ring Topology.

3. Star Topology.
4. Tree Topology.
5. Mesh Topology.

**1. Bus or Linear Topology: -**

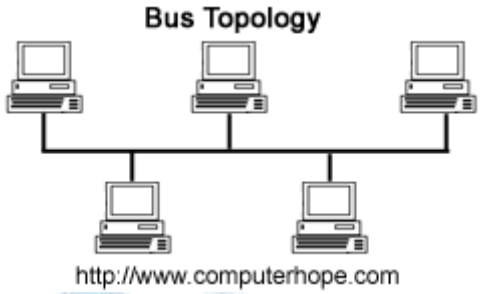
- This Consists of the single length of the transmission medium onto which the various nodes are attached.
- The transmitted data travels in the bus in the both directions and can be received by any of the workstations. The bus has the terminator at either end which absorbs the signals, removing it from the bus.

**Advantages: -**

- The short cable and the simple writing layout.
- The Resilient (easy) Architecture.
- Easy to Extend.

**Disadvantages: -**

- Fault diagnosis is difficult.
- The Repeater configuration.
- Node must be the intelligent.




**2. Ring or Circular Topology: -**

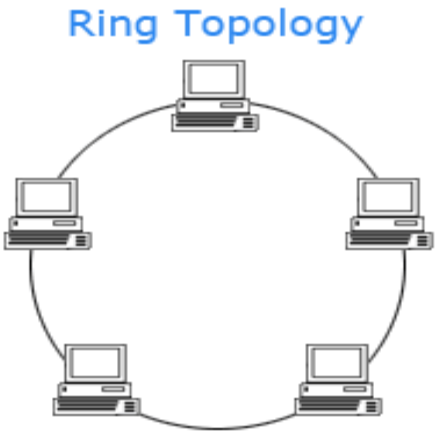
- In this type of topology each node is connected to the two ends only the two neighbouring nodes and is transmitted onwards to another. Thus, the data travels in one direction only, from node to node around the ring.
- In this type of network, the communication are always in only one direction, and the data being transmitted is passed only through the each of the node in the particular ring.

**Advantages: -**

- The short cable length.
- Signal degeneration is low (each workstation participating in the network is responsible for regenerating the weak signal).

**Disadvantages: -**

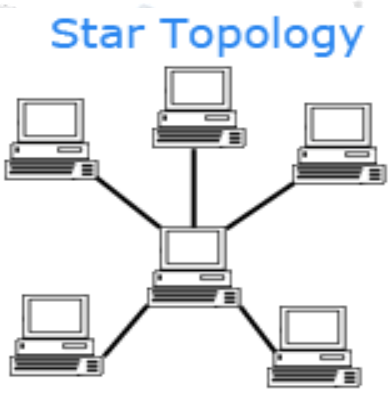
- The node failure is the main cause for the network failure.
- It is very much difficult to diagnose the faults.
- The Network reconfiguration is very difficult.




3. **Star Topology: -**
   - This type of topology consists of the central node to which all other nodes are connected by the signal path.
   - In the star topology, each node is connected directly to the central computer called HUB.
   - All of the communications between the nodes have to be passed through the central computer.

   **Advantages: -**
   - One device per connection.
   - Easy to install and wire.
   - No disruptions to the Network when connecting or removing devices.

   **Disadvantages: -**
   - Requires more cable length than a linear bus topology.
   - If the connecting network devices fails, nodes are attached to the HUB are disabled and cannot participate in computer network communications.
   - More expensive.

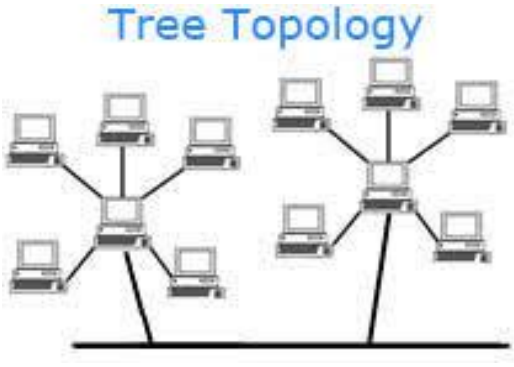



4. **Tree topology: -**
   - Tree topology integrates the characteristics of star and bus topology. In tree topology, nodes of the underlying bus network topology are replaced with a complete star topology.
   - A network structure which requires a root node, intermediate parent node, and leaf nodes in the star topology.

   **Advantages: -**
   - High scalability, as leaf nodes can add more nodes in the hierarchical chain.
   - Easy Maintenance and fault Identification.
   - Other nodes in a network are not affected, if one of their nodes get damaged.

   **Disadvantages: -**
   - Large cable is required.

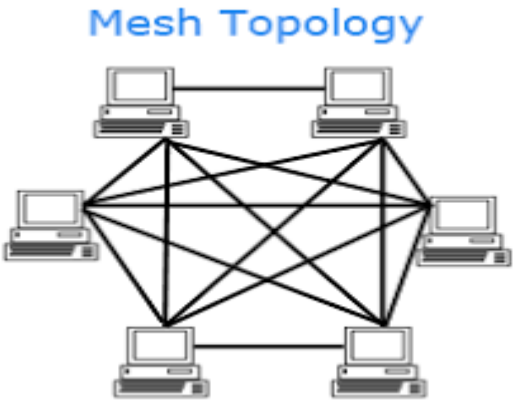
- On the failure of the root node (HUB), the entire network fails.
- It is very difficult to configure than other network topologies.




5. **Mesh Topology: -**
   - Mesh Topology is a network topology in which all the network nodes are individually connected to most of the other nodes. There is not a concept of a central point of communication to pass on the messages.

**Mesh Topology is divides into two kinds: -**

- Fully Connected Mesh topology: - All the nodes Connected to every other node.
- Partially Connected Mesh topology: - All the nodes are not connected to each other.




**Advantages: -**

- Each connection can carry its own data load.
- It is robust.
- A fault is diagnosed easily and provides security and privacy.

**Disadvantages: -**

- Installation and configuration are difficult.
- Cabling cost is more (mostly in fully connected mesh topology.
- Bulk wiring is required.

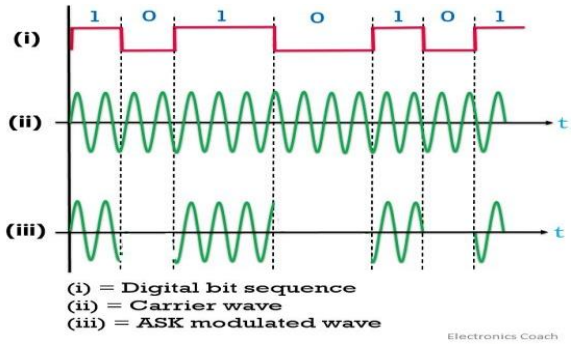
**08. Explain amplitude shift key, frequency shift key and phase shift key in analog transmission [2018]**

**Ans.**

**Amplitude Shift Key: -**

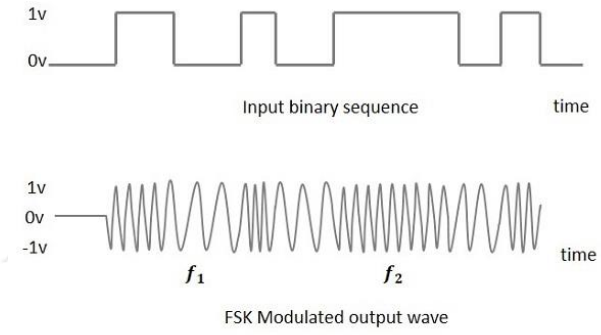
Amplitude Shift key is a form of amplitude modulation that represents digital data as variations in the amplitude of a carrier wave. In an amplitude shift key system, a symbol, representing one or more bits, is sent by transmitting a fixed-amplitude carrier wave at a fixed frequency for a specific time duration. For example: if each symbol

represents a single bit, then the carrier signal will be transmitted when the input value is 1, but will not be transmitted when the input value is 0.

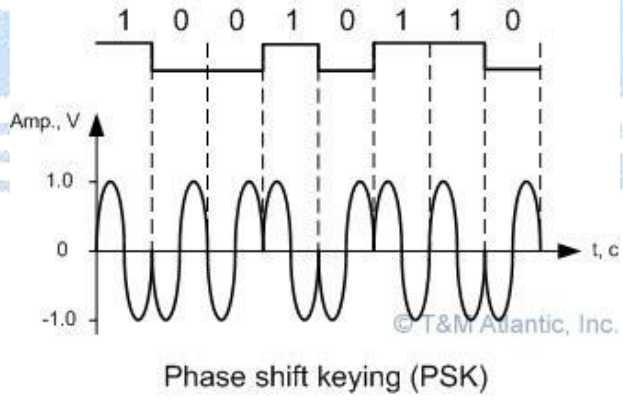



**Frequency shift key**: -

Frequency Shift Keying is the digital modulation technique in which the frequency of the carrier signal varies according to the digital signal changes. FSK is a scheme of frequency modulation. The output of a FSK modulated wave is high in frequency for a binary High input and is low in frequency for a binary Low input. The binary **1s** and **0s** are called Mark and Space frequencies. The following image is the diagrammatic representation of FSK modulated waveform along with its input.




**Phase-shift keying** (**PSK**)




**09. Explain frequency hopping spread spectrum (FHSS)** **[2018, 2016]**

**Ans.**

Frequency hopping spread spectrum (FHSS) is a method of transmitting radio signals by shifting carriers across numerous channels with pseudorandom sequence which is already known to the sender and receiver. Frequency hopping spread spectrum is defined in the 2.4 GHz band and operates in around 79 frequencies ranging from 2.402 GHz to 2.480 GHz. Every frequency is GFSK modulated with channel width of 1MHz and rates defined as 1 Mbps and 2 Mbps respectively.

This is frequency hopping technique, where the users are made to change the frequencies of usage, from one to another in a specified time interval, hence called as frequency hopping. For example, a frequency was allotted to sender 1 for a particular period of time. Now, after a while, sender 1 hops to the other frequency and sender 2 uses the first frequency, which was previously used by sender 1. This is called as frequency reuse.

The frequencies of the data are hopped from one to another in order to provide a secure transmission. The amount of time spent on each frequency hop is called as Dwell time.

**10. Explain circuit switched networks [2018]**

**Ans.**

In circuit switching network resources (bandwidth) is divided into pieces and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established. Telephone system network is the one of example of Circuit switching. **TDM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing)** are two methods of multiplexing multiple signals into a single carrier.

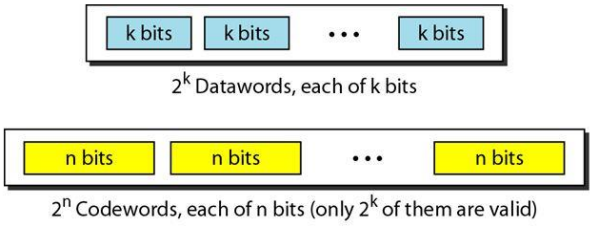
- **Frequency Division Multiplexing:** *Divides into multiple bands* Frequency Division Multiplexing or FDM is used when multiple data signals are combined for simultaneous transmission via a shared communication medium. It is a technique by which the total bandwidth is divided into a series of non-overlapping frequency sub-bands, where each sub-band carry different signal. Practical use in radio spectrum & optical fibre to share multiple independent signals.
- **Time Division Multiplexing:** *Divides into frames* Time-division multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line. TDM is used for long-distance communication links and bears heavy data traffic loads from end user. Time division multiplexing (TDM) is also known as a digital circuit switched.

**11. Explain how error detection and error correction can be implemented in block coding with an example [2018, 2016]**

**Ans.**

In block coding, we divide our message into blocks, each of k bits, called data words. We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called code words.

For example, we have a set of data words, each of size k, and a set of code words, each of size of n. With k bits, we can create a combination of 2k data words, with n bits; we can create a combination of 2n code words. Since n > k, the number of possible code words is larger than the number of possible data words. The block coding process is one-to-one; the same data word is always encoded as the same code word. This means that we have 2n-2k code words that are not used. We call these code words invalid or illegal. The following figure shows the situation.



**Error Detection:**

If the following two conditions are met, the receiver can detect a change in the original code word by using Block coding technique.

1. The receiver has (or can find) a list of valid code words.
2. The original code word has changed to an invalid one.

**Error Correction:**

Error correction is much more difficult than error detection. In error detection, the receiver needs to know only that the received code word is invalid, in error correction the receiver needs to find (or guess) the original code word sent. So, we need more redundant bits for error correction than for error detection.

**12. Explain Controlled access protocols [2018]**

**Ans.**

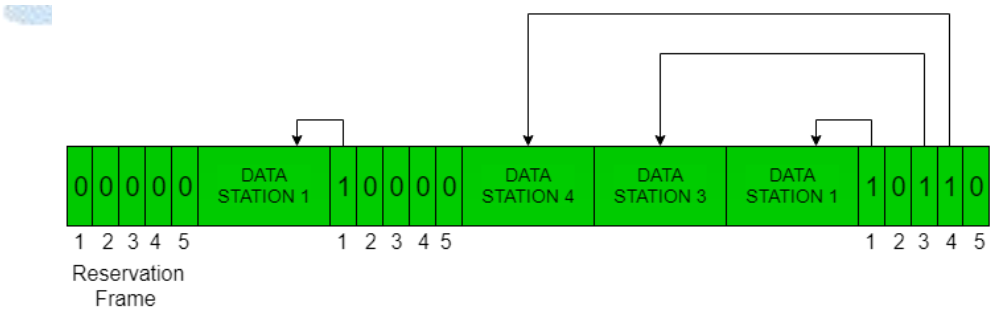
In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid collision of messages on shared medium.

The three controlled-access methods are:

1. Reservation
2. Polling
3. Token Passing

1. **Reservation**:

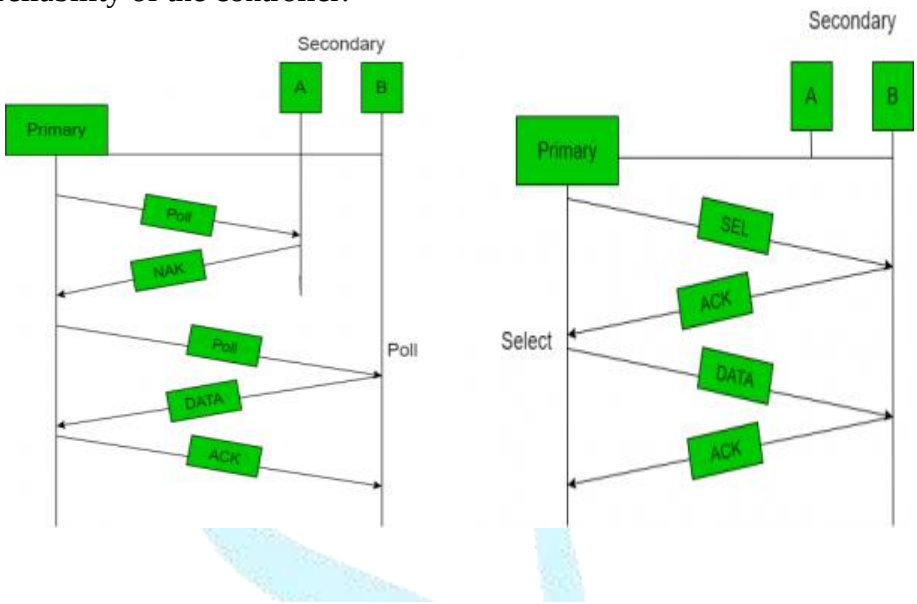
- In the reservation method, a station needs to make a reservation before sending data.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, $i^{th}$ station may announce that it has a frame to send by inserting a 1 bit into $i^{th}$ slot. After all N slots have been checked, each station knows which stations wish to transmit.



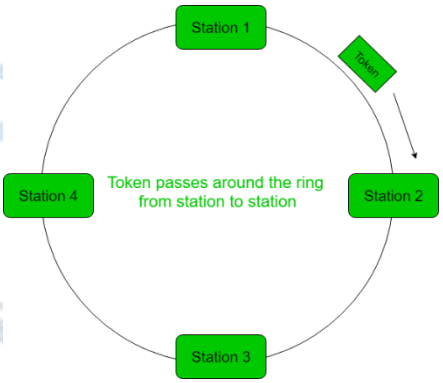

**Polling:**

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station (controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.

- Although all nodes receive the message but the addressed one responds to it and sends data, if any. If there is no data, usually a "poll reject" (NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.




**Token Passing**




- In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas in case of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 station to send a frame, if they have one.

  There exist problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.

**13. Briefly explain the factors that affect the performance of a network [2017]**

**Ans.**

Performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. The characteristics that measure the performance of a network are:

- Bandwidth
- Throughput
- Latency (Delay)
- Bandwidth – Delay Product

- Jitter

**BANDWIDTH:**

One of the most essential conditions of a website's performance is the amount of bandwidth allocated to the network. Bandwidth determines how rapidly the web server is able to upload the requested information. While there are different factors to consider with respect to a site's performance, bandwidth is every now and again the restricting element.

Bandwidth is characterized as the measure of data or information that can be transmitted in a fixed measure of time. The term can be used in two different contexts with two distinctive estimating values. In the case of digital devices, the bandwidth is measured in bits per second (bps) or bytes per second. In the case of analog devices, the bandwidth is measured in cycles per second, or Hertz (Hz).

**THROUGHPUT:**

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio and the hardware limitations. The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption. The terms 'throughput' and 'bandwidth' are often thought of as the same, yet they are different. Bandwidth is the potential measurement of a link, whereas throughput is an actual measurement of how fast we can send data.

Throughput is measured by tabulating the amount of data transferred between multiple locations during a specific period of time, usually resulting in the unit of bits per second(bps), which has evolved to bytes per second(Bps), kilobytes per second(KBps), megabytes per second(MBps) and gigabytes per second(GBps). Throughput may be affected by numerous factors, such as the hindrance of the underlying analog physical medium, available processing power of the system components, and end-user behaviour. When numerous protocol expenses are taken into account, the useful rate of the transferred data can be significantly lower than the maximum achievable throughput.

**LATENCY**

In a network, during the process of data communication, latency (also known as delay) is defined as the total time taken for a complete message to arrive at the destination, starting with the time when the first bit of the message is sent out from the source and ending with the time when the last bit of the message is delivered at the destination. The network connections where small delays occur are called "Low-Latency-Networks" and the network connections which suffer from long delays are known as "High-Latency-Networks".

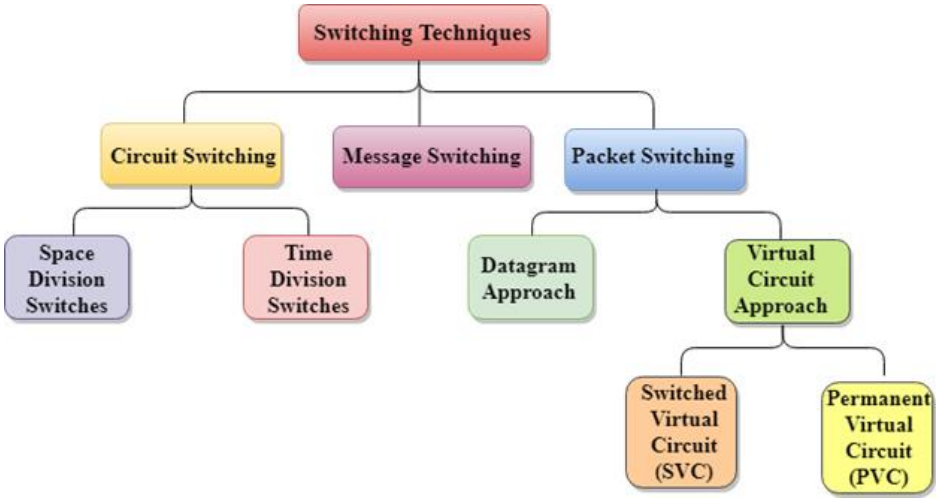
High latency leads to creation of bottlenecks in any network communication. It stops the data from taking full advantage of the network pipe and conclusively decreases the bandwidth of the communicating network. The effect of the latency on a network's bandwidth can be temporary or never-ending depending on the source of the delays. Latency is also known as a ping rate and measured in milliseconds (ms).

**14. What is switching? Explain datagram networks [2017]**

**Ans.**

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.



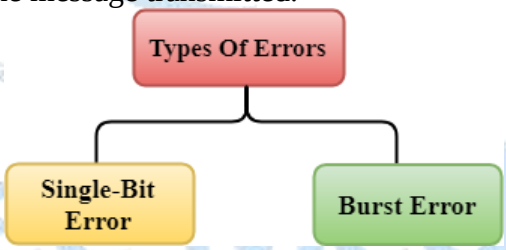

**Datagram Packet switching:**

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

**15. Explain how error detection is done using cyclic codes [2017]**

**Ans.**

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.




**Error Detecting Techniques:**

The most popular Error Detecting Techniques are

i. Single parity check
ii. Two-dimensional parity check
iii. Checksum
iv. Cyclic redundancy check

**Checksum:**

A Checksum is an error detection technique based on the concept of redundancy. It is divided into two parts:

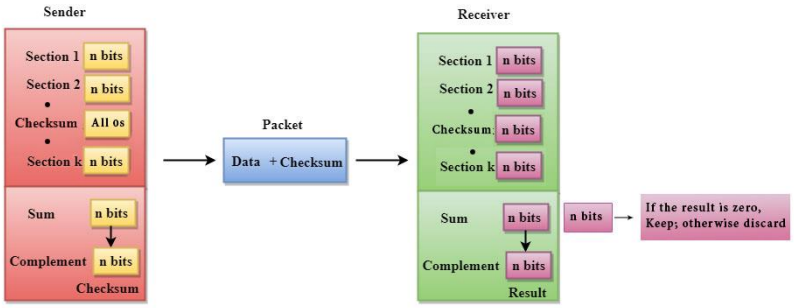
- Checksum Generator
- Checksum Checker

**Checksum Generator:**

A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using

one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Suppose L is the total sum of the data segments, then the checksum would be? L




The Sender follows the given steps:

1. The block unit is divided into k sections, and each of n bits.
2. All the k sections are added together by using one's complement to get the sum.
3. The sum is complemented and it becomes the checksum field.

**Checksum Checker:**

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

The Receiver follows the given steps:

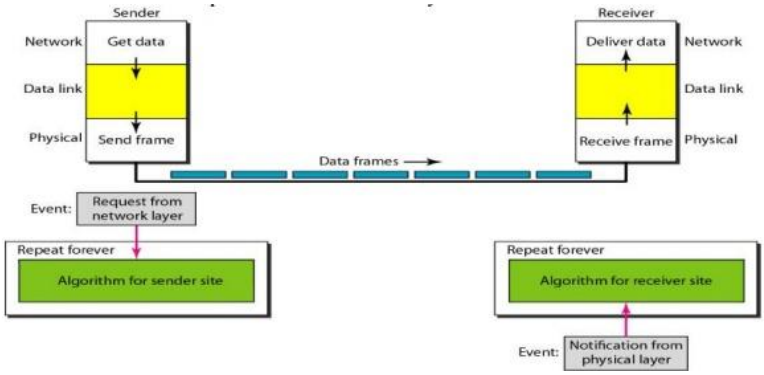
- The block unit is divided into k sections and each of n bits.
- All the k sections are added together by using one's complement algorithm to get the sum.
- The sum is complemented.
- If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

**16. Write a note on simplest and stop-and-wait noiseless channels [2017]**
**Ans.**

An ideal channel in which no frames are lost, duplicated or corrupted is regarded as Noiseless Channel.

**Simplest Protocol:**

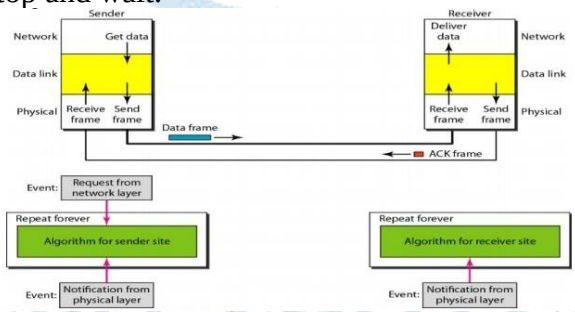
- In simplest protocol, there is no flow control and error control mechanism. It is a unidirectional protocol in which data frames travel in only one direction (from sender to receiver).
- Also, the receiver can immediately handle any received frame with a processing time that is small enough to be negligible.
- The protocol consists of two distinct procedures: a sender and receiver. The sender runs in the data link layer of the source machine and the receiver runs in the data link layer of the destination machine. No sequence number or acknowledgements are used here.




It has no flow or error control. It is a unidirectional protocol in which data frames are traveling in only one direction from the sender to receiver. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately.

**Stop and Wait Protocol:**

- The simplest retransmission protocol is stop-and-wait.
- Transmitter (Station A) sends a frame over the communication line and then waits for a positive or negative acknowledgement from the receiver (station B).
- If no error occurs in the transmission, station B sends a positive acknowledgement (ACK) to station A.
- Now, the transmitter starts to send the next frame. If frame is received at station B with errors, then a negative acknowledgement (NAK) is sent to station A. In this case, station 'A' must retransmit the old packet in a new frame.
- There is also a possibility that the information frames or ACKs may get lost.
- Then, the sender is equipped with a timer. If no recognizable acknowledgement is received when the timer expires at the end of time out interval, the same frame is sent again.
- The sender which sends one frame and then waits for an acknowledgement before process is known as stop and wait.




If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. In Stop-and-Wait Protocol the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.

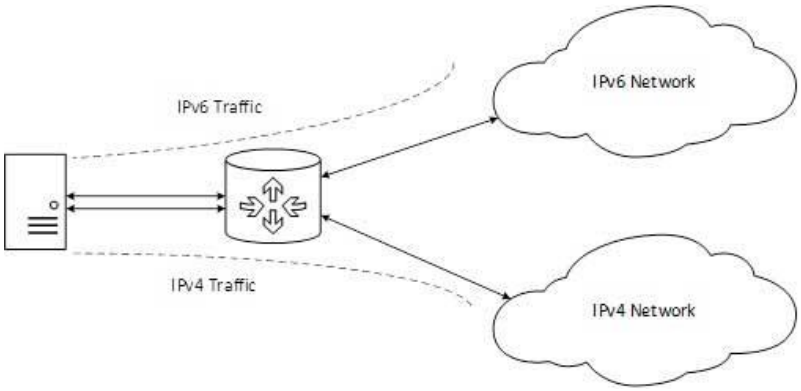
**17. Describe the transition from IPV4 to IPV6 [2017]**

**Ans.**

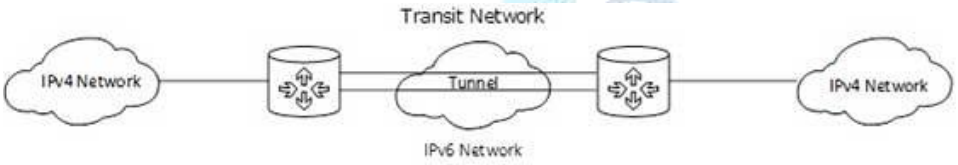
Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is backward compatible so the older system can still work with the newer version without any additional changes.

To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.

Dual Stack Routers:
A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.

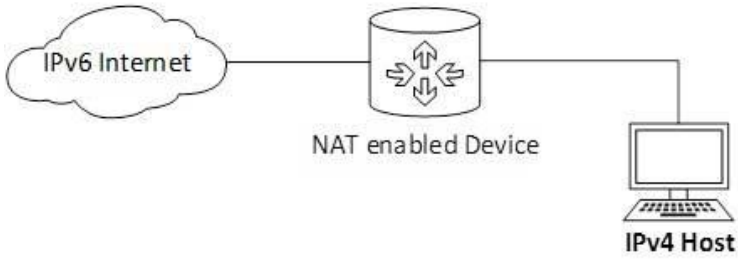



In the above diagram, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a Dual Stack Router. The Dual Stack Router, can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.
Tunneling:
In a scenario where different IP versions exist on intermediate path or transit networks; tunnelling provides a better solution where user's data can pass through a non-supported IP version.




The above diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6. Vice versa is also possible where the transit network is on IPv6 and the remote sites that intend to communicate are on IPv4.

NAT Protocol Translation:
This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. See the diagram below:

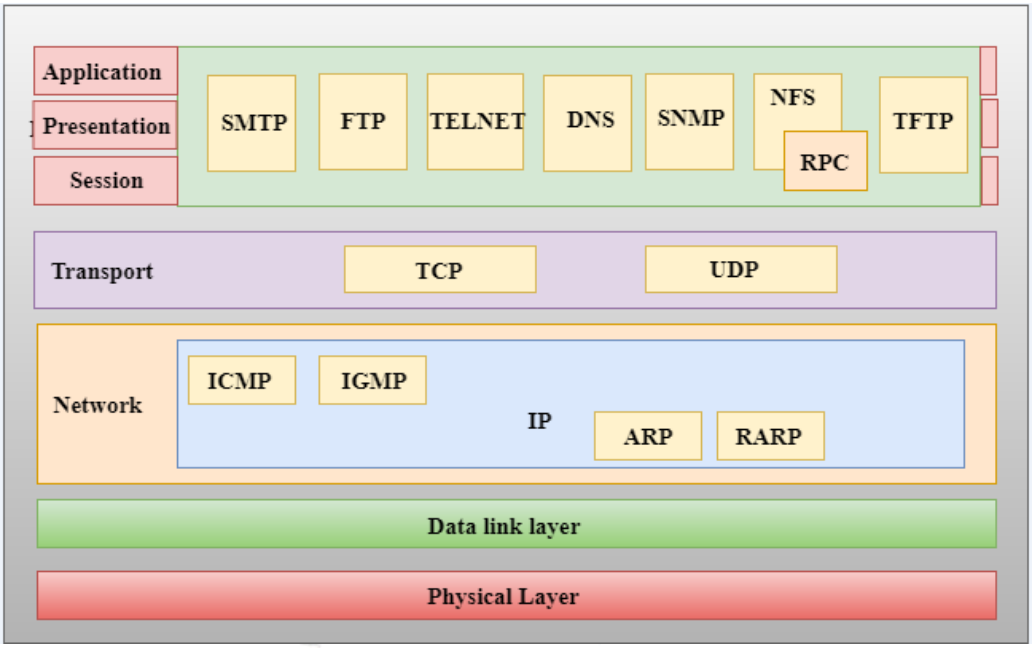



A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.

**18. With a neat diagram explain TCP/IP [2016]**

**Ans.**

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.




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.

Transport Layer

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

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.

**19. Explain briefly unipolar NRZ Scheme [2016]**

**Ans.**

A line code is the code used for data transmission of a digital signal over a transmission line. This process of coding is chosen so as to avoid overlap and distortion of signal such as inter-symbol interference.

Types of Line Coding

There are 3 types of Line Coding

- Unipolar
- Polar
- Bi-polar

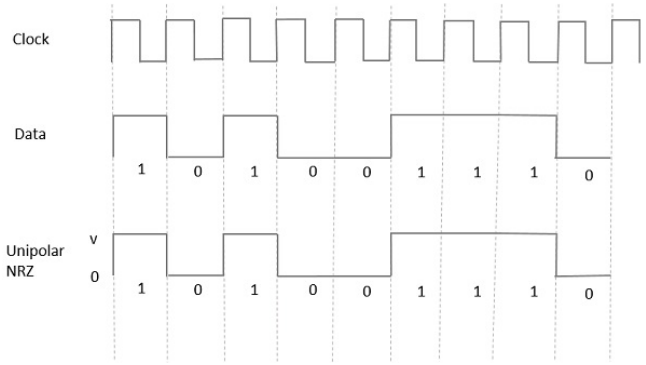
Unipolar:

In Unipolar we are simply representing a signal in a graphical form where positive voltage represents logical or binary 1 and zero voltage represents logical zero. We can say that it's the simplest line code. The drawback of this scheme is that it is not self-clocking which means that it can't be decoded without a separate clock signal or any other synchronization source. And as we discussed in the characteristics section that there should be no DC component present which it significantly contains, which can be halved by returning to zero in the middle of the bit period.

NRZ (Non-Return to Zero):

The term Non-Return to Zero (NRZ) means that the signal (the red line in the above diagram) will not return to zero in middle of the bit (i.e. either 0 or 1). Unipolar schemes were generally designed as NRZ schemes. But if we compare it to the polar NRZ scheme, this scheme leads to wastage of power i.e. the normalized power (i.e. the power required to send 1-bit per resistance) is almost double as compared to polar NRZ.

Because of all these reasons unipolar encoding is not normally used in data communications today.



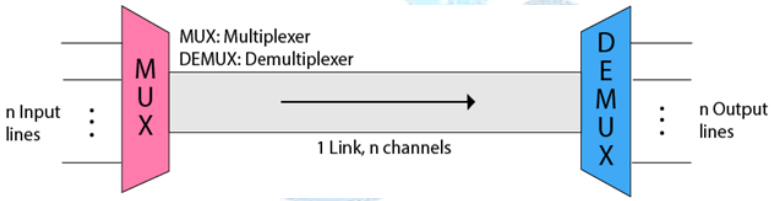
It is unipolar line coding scheme in which positive voltage defines bit 1 and the zero voltage defines bit 0. Signal does not return to zero at the middle of the bit thus it is called NRZ. For example: Data = 10110.
But this scheme uses more power as compared to polar scheme to send one bit per unit line resistance. Moreover, for continuous set of zeros or ones there will be self-synchronization and base line wandering problem.

**20. What is Multiplexing? Explain FDM [2016]**

**Ans.**

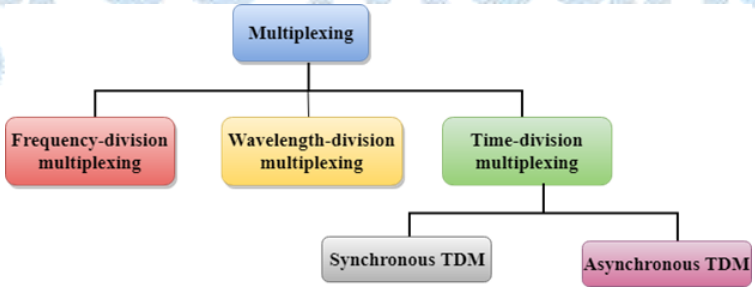
Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

- 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.
- Transmission services are very expensive.



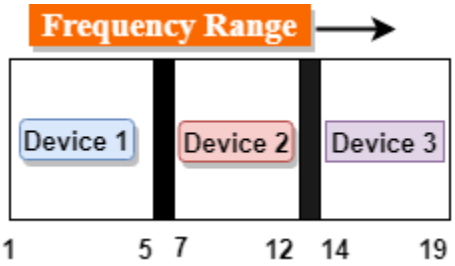

The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

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

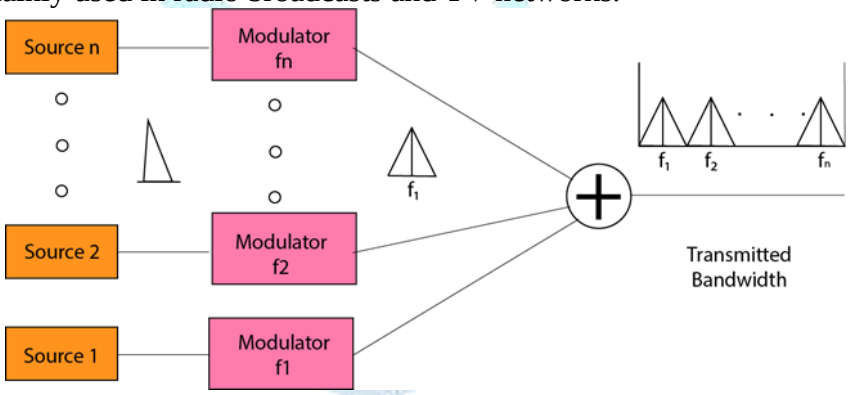



Frequency-division Multiplexing (FDM):

- It is an analog technique.
- Frequency Division Multiplexing is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.




- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as sub-carriers. They are represented as f1,f2..fn.
- FDM is mainly used in radio broadcasts and TV networks.

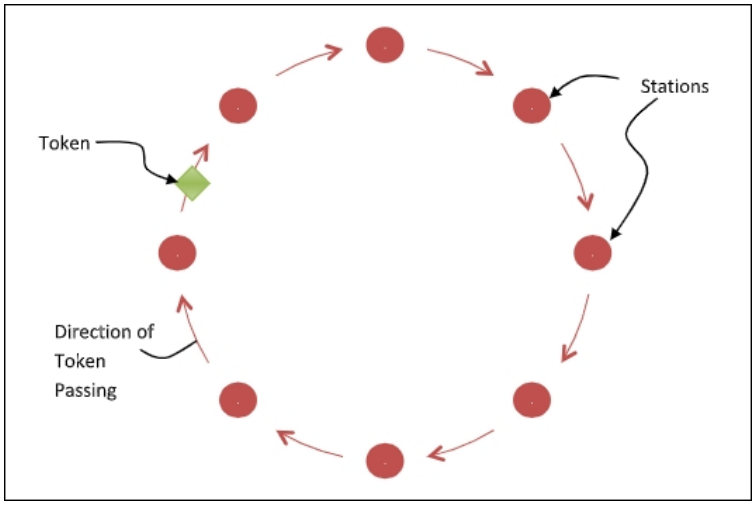



FDM is used for analog signals.
FDM process is very simple and easy modulation.
A Large number of signals can be sent through an FDM simultaneously.
It does not require any synchronization between sender and receiver.

**21. What is token passing? Explain [2016]**

**Ans.**

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise, it simply passes the token to the next station.




In the above configuration, passing the token comprise of receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. The token may be generated by the station that wants to send the frame or the station that wants to receive the frame. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed.

"On a local area network, token passing is a channel access method where a signal called a token is passed between nodes to authorize that node to communicate. In contrast to polling access methods, there is no pre-defined "master" node. The most well-known examples are IBM Token Ring and ARCNET, but there were a range of others, including FDDI (Fiber Distributed Data Interface), which was popular in the early to mid-1990s."

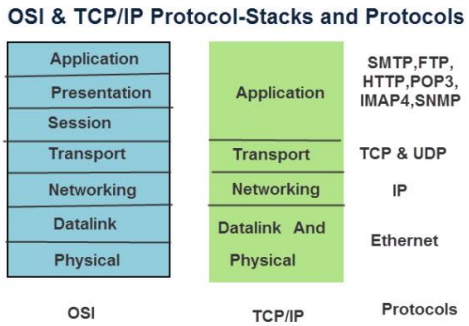
## 10m Questions & Answers

**01. Explain TCP/IP protocol suite with a neat diagram [2019, 2017]**
**Ans.**

A protocol is a set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another.

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.



**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.

**Transport Layer**

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

**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.

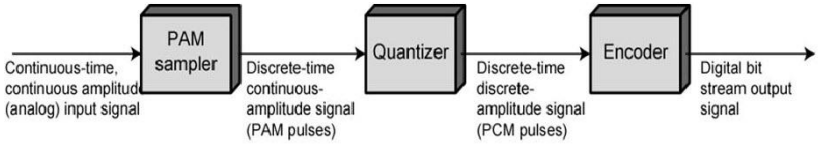
There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

The TCP/IP protocol suite is a collection of protocols that are used on the Internet. It is named after two of the main protocols (TCP and IP) and uses a 4 layer networking model.

**02. Write a note on Pulse Code Modulation [2019, 2017]**

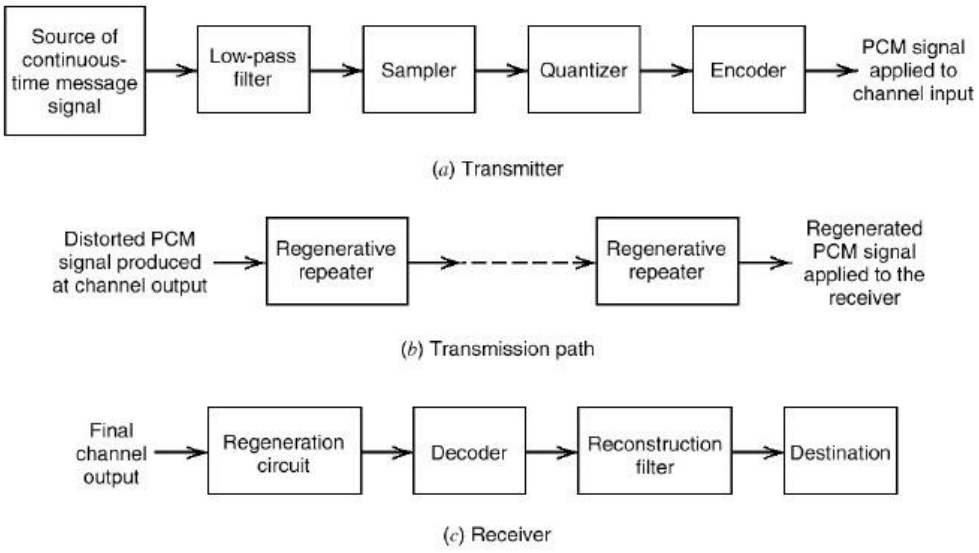
**Ans.**

Pulse code modulation is a method that is used to convert an analog signal into a digital signal so that a modified analog signal can be transmitted through the digital communication network. PCM is in binary form, so there will be only two possible states high and low (0 and 1). We can also get back our analog signal by demodulation. The Pulse Code Modulation process is done in three steps Sampling, Quantization, and Coding. There are two specific types of pulse code modulations such as differential pulse code modulation (DPCM) and adaptive differential pulse code modulation (ADPCM).

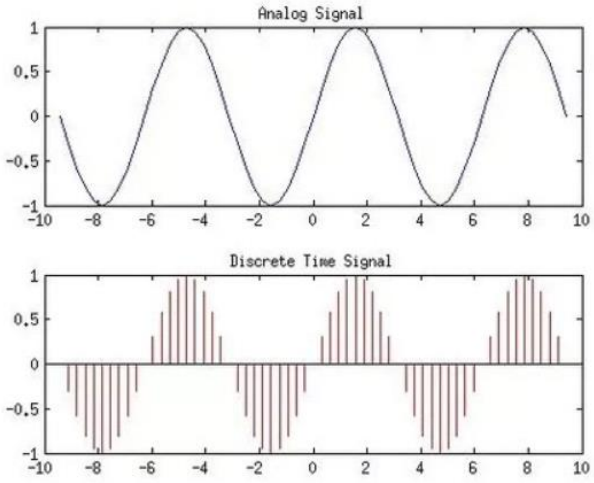



Here is a block diagram of the steps which are included in PCM. In sampling, we are using a PAM sampler that is Pulse Amplitude Modulation Sampler which converts continuous amplitude signal into Discrete-time- continuous signal (PAM pulses). The basic block diagram of PCM is given below for better understanding.

To get a pulse code modulated waveform from an analog waveform at the transmitter end (source) of a communications circuit, the amplitude of the analog signal samples at regular time intervals. The sampling rate or the number of samples per second is several times the maximum frequency. The message signal converted into the binary form will be usually in the number of levels which is always to a power of 2. This process is called quantization.




The above block diagram describes the whole process of PCM. The source of the continuous-time message signal is passed through a low pass filter and then sampling, Quantization, Encoding will be done. We will see each in detail step by step.



The main function of a decoder circuit is to decode the pulse-coded signal to repeat the actual signal. This circuit works like a demodulator. PCM is two types of Differential Pulse Code Modulation (DPCM), Adaptive Differential Pulse Code Modulation (ADPCM) & Linear Pulse Code Modulation.

- PCM technique is mainly used to change the signal from analog to digital signal so that an analog signal which is changed can be broadcasted throughout the digital communication network. This modulation is available in binary form, so the available possible states will be two types like high & low.
- Pulse-code modulation (PCM) is a technique used to represent sampled analog signals digitally. It is the normal form of digital audio within computers, digital telephony, compact discs & other digital audio applications.
- These modulations can be used for temperature regulation, cold or heat storage through high storage density & thermal comfort within buildings that need a narrow range of temperature. Thus, if the solar energy is stored efficiently, then it can be used for night cold.
- The pulse code modulation refers to the utilization of a precise set of rules for changing a signal into a stream of digits.

**03. Explain in detail about Frequency Hopping Spread Spectrum [2019]**

**Ans.**

Frequency Hopping Spread Spectrum: A transmission technology in which the data signal is modulated by a narrowband carrier signal which changes frequency ("hops") over a wide band of frequencies. The hopping seems random but is prescribed by an algorithm known to the receiving system.

This is frequency hopping technique, where the users are made to change the frequencies of usage, from one to another in a specified time interval, hence called as frequency hopping. For example, a frequency was allotted to sender 1 for a particular period of time. Now, after a while, sender 1 hops to the other frequency and sender 2 uses the first frequency, which was previously used by sender 1. This is called as frequency reuse.

The frequencies of the data are hopped from one to another in order to provide a secure transmission. The amount of time spent on each frequency hop is called as Dwell time.

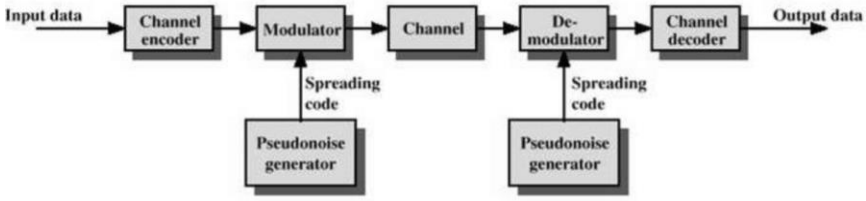
Frequency hopping spread spectrum (FHSS) is a method of transmitting radio signals by shifting carriers across numerous channels with pseudorandom sequence which is already known to the sender and receiver. Frequency hopping spread spectrum is defined in the 2.4 GHz band and operates in around 79 frequencies ranging from 2.402 GHz to 2.480 GHz. Every frequency is GFSK modulated with channel width of 1MHz and rates defined as 1 Mbps and 2 Mbps respectively.

This is frequency hopping technique, where the users are made to change the frequencies of usage, from one to another in a specified time interval, hence called as frequency hopping. For example, a frequency was allotted to sender 1 for a particular period of time. Now, after a while, sender 1 hops to the other frequency and sender 2 uses the first frequency, which was previously used by sender 1. This is called as frequency reuse.

The frequencies of the data are hopped from one to another in order to provide a secure transmission. The amount of time spent on each frequency hop is called as Dwell time.

- Multiple frequencies are used.

- Hard to find the user's frequency at any instant of time.
- Frequency reuse is allowed.
- Sender need not wait.
- Power strength of the signal is high.
- Stronger and penetrates through the obstacles.
- It is never affected by interference.
- It is cheaper.
- This is the commonly used technique.




**04. Explain about HDLC [2019]**

**Ans.**

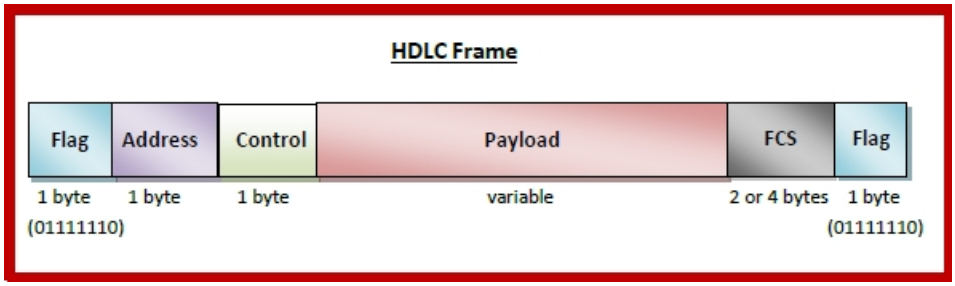
High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- Normal Response Mode (NRM)
- Asynchronous Balanced Mode (ABM)

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

**Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
**Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
**Control** − It is 1 or 2 bytes containing flow and error control information.
**Payload** − This carries the data from the network layer. Its length may vary from one network to another.
**FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



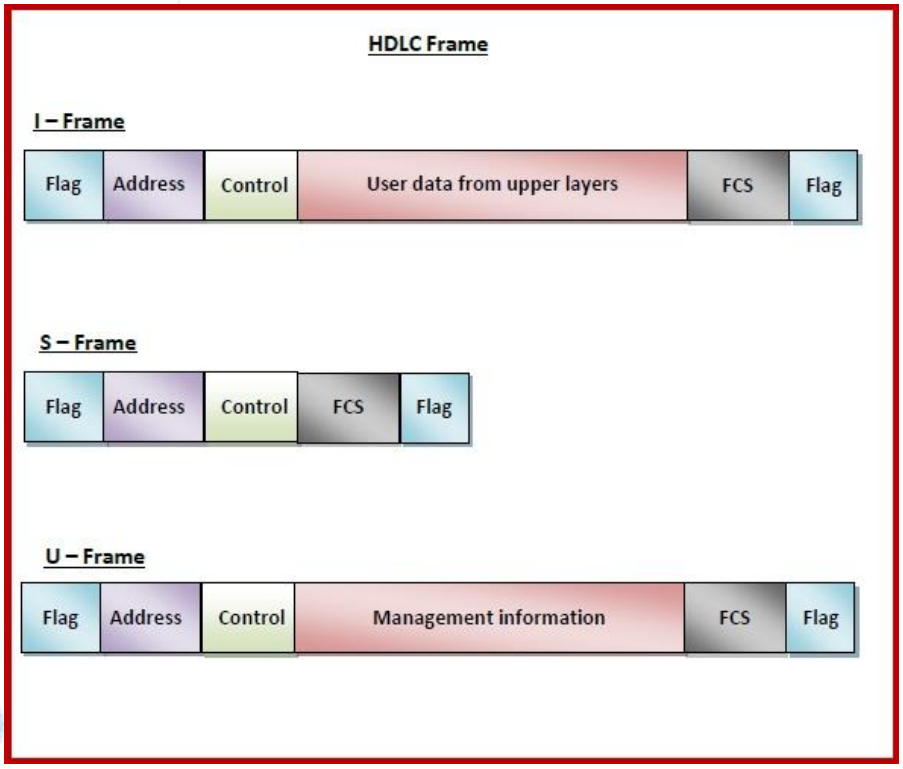
**Types of HDLC Frames**

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

**I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.

**S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.

**U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.




**05. What is Gigabit Ethernet? Explain in detail [2019]**

**Ans.**

In computer networks, Gigabit Ethernet (GbE) is the family of Ethernet technologies that achieve theoretical data rates of 1 gigabit per second (1 Gbps). It was introduced in 1999 and was defined by the IEEE 802.3ab standard.

The committee began working on a faster Ethernet, quickly dubbed gigabit Ethernet. The goal was to increase performance while maintaining all Ethernet standards. Gigabit Ethernet had to provide service with both unicast and broadcast using the same 48-bit address scheme and also maintaining the same frame format.

The popular varieties of fast Ethernet are 1000Base-SX, 1000Base-LX, 1000BASE-T and 1000Base-CX.

**1000BASE-CX**

- Defined by IEEE 802.3z standard
- The initial standard for Gigabit Ethernet

- Uses shielded twisted pair cables with DE-9 or 8P8C connector
- Maximum segment length is 25 metres
- Uses NRZ line encoding and 8B/6B block encoding

**1000BASE-SX**

- Defined by IEEE 802.3z standard
- Uses a pair of fibre optic cables of a shorter wavelength having 770 – 860 nm diameter
- The maximum segment length varies from 220 – 550 metres depending upon the fiber properties.
- Uses NRZ line encoding and 8B/10B block encoding

**1000BASE-LX**

- Defined by IEEE 802.3z standard
- Uses a pair of fibre optic cables of a longer wavelength having 1270 – 1355 nm diameter
- Maximum segment length is 500 metres
- Can cover distances up to 5 km
- Uses NRZ line encoding and 8B/10B block encoding

**1000BASE-T**

- Defined by IEEE 802.3ab standard
- Uses a pair four lanes of twisted-pair cables (Cat-5, Cat-5e, Cat-6, Cat-7)
- Maximum segment length is 100 metres
- Uses trellis code modulation technique

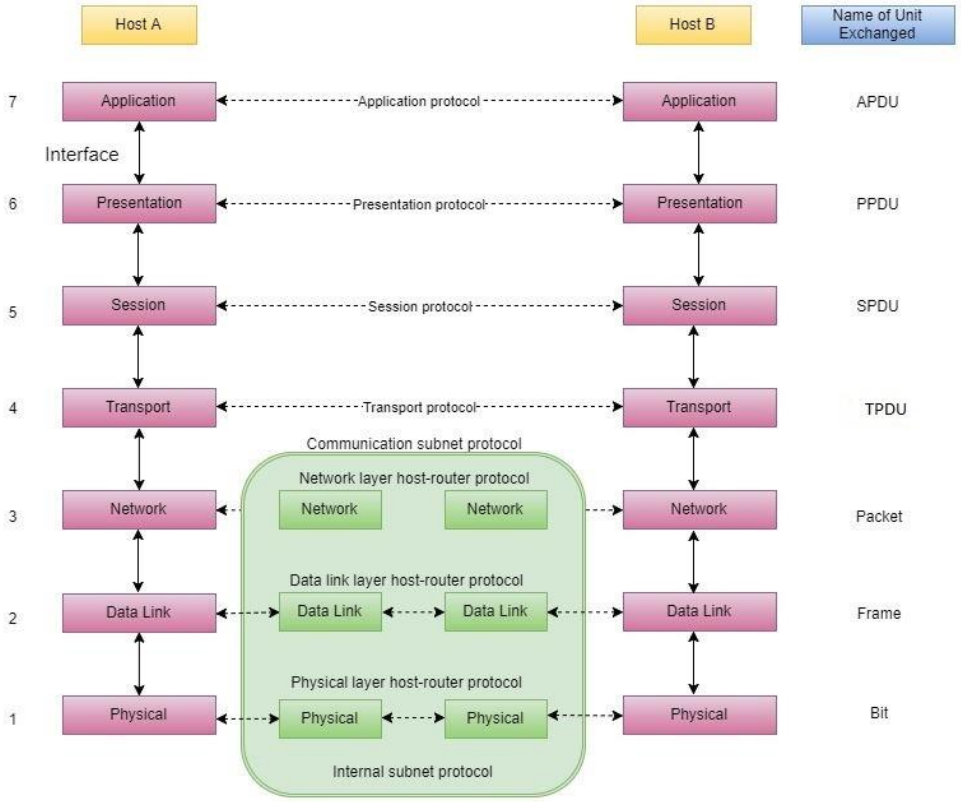
| Name | Cable | Max. Segment | Advantages |
|---|---|---|---|
| 1000Base-SX | Fiber optics | 550m | Multimode fiber (50, 62.5 microns) |
| 1000Base-LX | Fiber optics | 5000m | Single(10 μ) or multimode(50, 62.5 μ) |
| 1000Base-CX | 2 pairs of STP | 25m | Shielded twisted pair |
| 1000Base-T | 4 pairs of UTP | 100m | Standard category 5 UTP |



**Features of Gigabit Ethernet:**

- It supports two different modes i.e. full-duplex mode and half-duplex mode. Full-duplex mode allows traffic in two directions at the same time. When a central switch connected to computers on the periphery this mode is used.
- In this, all lines are buffered so each computer and switch is free to send frames whenever it wants to. In this mode, contention is not possible.
- The computer is the only possible sender to the switch, and transmission will succeed even if the switch is currently sending a frame to the computer.
- A half-duplex mode is used when computers are connected to a hub rather than a switch. A hub does not buffer incoming frames.
- All the lines are electrically connected internally, simulating the multi-drop cable used in classic Ethernet. Standard CSMA/CD protocol is required in this mode because collisions are possible. Because a 64-byte frame can now be transmitted 100 times faster than in classic Ethernet, the maximum cable length must be 100 times less or 25 meters.

**06. Explain ISO/OSI model layers with a neat diagram [2018, 2016]**
**Ans.**




**Feature of OSI Model**

- Big picture of communication over network is understandable through this OSI model.
- We see how hardware and software work together.
- We can understand new technologies as they are developed.
- Troubleshooting is easier by separate networks.
- Can be used to compare basic functional relationships on different networks.

**Principles of OSI Reference Model**

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldly.

**OSI Model Layer 1: The Physical Layer**

- Physical Layer is the lowest layer of the OSI Model.
- It activates, maintains and deactivates the physical connection.

- It is responsible for transmission and reception of the unstructured raw data over network.
- Voltages and data rates needed for transmission is defined in the physical layer.
- It converts the digital/analog bits into electrical signal or optical signals.
- Data encoding is also done in this layer.

**OSI Model Layer 2: Data Link Layer**

- Data link layer synchronizes the information which is to be transmitted over the physical layer.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- Transmitting and receiving data frames sequentially is managed by this layer.
- This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
- 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.

**OSI Model Layer 3: The Network Layer**

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

**OSI Model Layer 4: Transport Layer**

- Transport Layer decides if data transmission should be on parallel path or single path.
- Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
- It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
- 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.

**OSI Model Layer 5: The Session Layer**

- Session Layer manages and synchronize the conversation between two different applications.
- 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.

**OSI Model Layer 6: The Presentation Layer**

- 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.
- While receiving the data, presentation layer transforms the data to be ready for the application layer.
- Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.

- It performs Data compression, Data encryption, Data conversion etc.

**OSI Model Layer 7: Application Layer**

- Application Layer is the topmost layer.
- 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.
- This layer mainly holds application programs to act upon the received and to be sent data.

**Merits of OSI reference model**

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

**Demerits of OSI reference model**

- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.
- It is just used as a reference model.

**07. What are Analog and Digital signals? Explain line coding Schemes [2018, 2017]**
**Ans.**

| Analog signals | Digital signals |
|---|---|
| Analog signals are difficult to get analysed at first. | Digital signals are easy to analyse. |
| Analog signals are more accurate than digital signals. | Digital signals are less accurate. |
| Analog signals take time to be stored. It has infinite memory. | Digital signals can be easily stored. |
| To record an analog signal, the technique used, preserves the original signals. | In recording digital signal, the sample signals are taken and preserved. |
| There is a continuous representation of signals in analog signals. | There is a discontinuous representation of signals in digital signals. |
| Analog signals produce too much noise. | Digital signals do not produce noise. |
| Examples of analog signals are Human voice, | Examples of digital signals are Computers, Digital Phones, Digital pens, etc. |

| | |
|---|---|
| Thermometer, Analog phones etc. | |

A line code is the code used for data transmission of a digital signal over a transmission line. This process of coding is chosen so as to avoid overlap and distortion of signal such as inter-symbol interference.

Properties of Line Coding
Following are the properties of line coding –

- As the coding is done to make more bits transmit on a single signal, the bandwidth used is much reduced.
- For a given bandwidth, the power is efficiently used.
- The probability of error is much reduced.
- Error detection is done and the bipolar too has a correction capability.
- Power density is much favorable.
- The timing content is adequate.
- Long strings of 1s and 0s is avoided to maintain transparency.

**There are 3 types of Line Coding**

- Unipolar
- Polar
- Bi-polar

**08. Explain Stop-And-Wait ARQ protocol and Go-Back-N ARQ protocol in Noisy channels [2018, 2016]**

**Ans.**

Before understanding the stop and Wait protocol, we first know about the error control mechanism. The error control mechanism is used so that the received data should be exactly same whatever sender has sent the data. The error control mechanism is divided into two categories, i.e., Stop and Wait ARQ and sliding window. The sliding window is further divided into two categories, i.e., Go Back N, and Selective Repeat. Based on the usage, the people select the error control mechanism whether it is stop and wait or sliding window.

Here **stop and wait** means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

Simplex Stop – and – Wait protocol for noisy channel is data link layer protocol for data communications with error control and flow control mechanisms. It is popularly known as Stop – and –Wait Automatic Repeat Request (Stop – and –Wait ARQ) protocol. It adds error control facilities to Stop – and – Wait protocol.

In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.

Frames from a sending station are numbered sequentially. However, because we need to include the sequence number of each frame in the header, we need to set a limit. If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to 2m - 1.

**09. Explain ALOHA and CSMA in random access protocols [2018]**

**Ans.**

**ALOHA Random Access Protocol**

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

- Any station can transmit data to a channel at any time.
- It does not require any carrier sensing.
- Collision and data frames may be lost during the transmission of data through multiple stations.
- Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
- It requires retransmission of data after some random amount of time.

**CSMA (Carrier Sense Multiple Access)**

It is a carrier sense multiple access based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

**CSMA Access Modes**

**1-Persistent**: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

**Non-Persistent**: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

**P-Persistent**: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a P probability. If the data is not transmitted, it waits for a (q = 1-p probability) random time and resumes the frame with the next time slot.

**O- Persistent**: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.

**10. Briefly explain IPV4 addresses [2018]**

**Ans.**

Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier

definition (RFC 760, January 1980). This tutorial will help you in understanding IPv4 and its associated terminologies along with appropriate references and examples.

IP stands for Internet Protocol and v4 stands for Version Four (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.
IP version four addresses are 32-bit integers which will be expressed in hexadecimal notation.
Example- 192.0.2.126 could be an IPv4 address.

**Characteristics of IPv4**

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields are twelve and the length of the header filed is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to mack address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

**Advantages of IPv4**

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
- Data communication across the network becomes a lot of specific in multicast organizations.

**Disadvantages of IPv4**

- Limits net growth for existing users and hinders the use of the net for brand new users.
- Internet Routing is inefficient in IPv4.
- IPv4 has high System Management prices and it's labor intensive, complex, slow & frequent to errors.
- Security features are nonobligatory.
- Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

**11. What is spread spectrum? Explain the types of spread spectrum [2017]**
**Ans.**

Spread spectrum is a technique used for wireless communications in telecommunication and radio communication. In this technique, the frequency of the transmitted signal, i.e., an electrical signal, electromagnetic signal, or acoustic signal, is deliberately varied and generates a much greater bandwidth than the signal would have if its frequency were not varied.

In other words, "Spread Spectrum is a technique in which the transmitted signals of specific frequencies are varied slightly to obtain greater bandwidth as compared to initial bandwidth."

Now, spread spectrum technology is widely used in radio signals transmission because it can easily reduce noise and other signal issues.

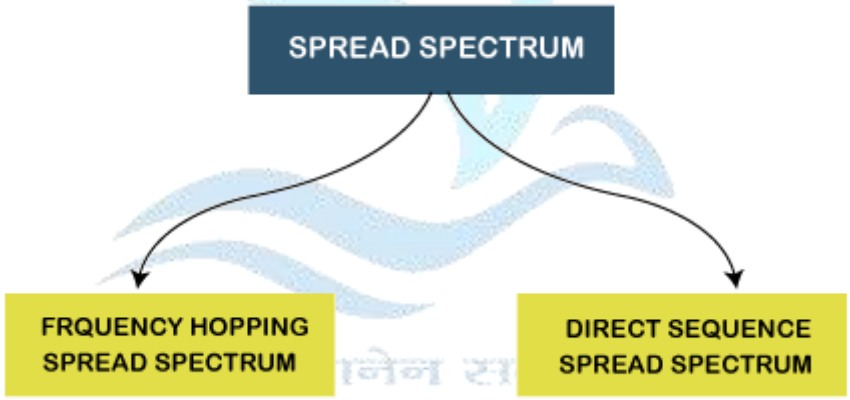
Reasons to use Spread Spectrum

- Spread spectrum signals are distributed over a wide range of frequencies and then collected and received back to the receiver. On the other hand, wide-band signals are noise-like and challenging to detect.
- Initially, the spread spectrum was adopted in military applications because of its resistance to jamming and difficulty intercepting.
- Now, this is also used in commercial wireless communication.
- It is most preferred because of its useful bandwidth utilization ability.

Types of Spread Spectrum

Spread Spectrum can be categorized into two types:

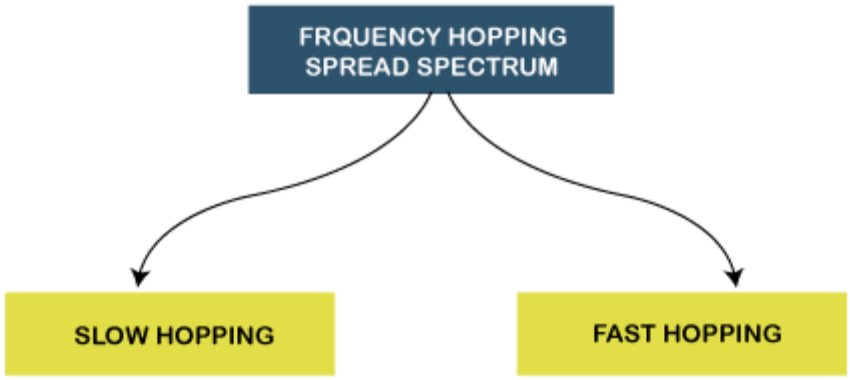
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum(DSSS)



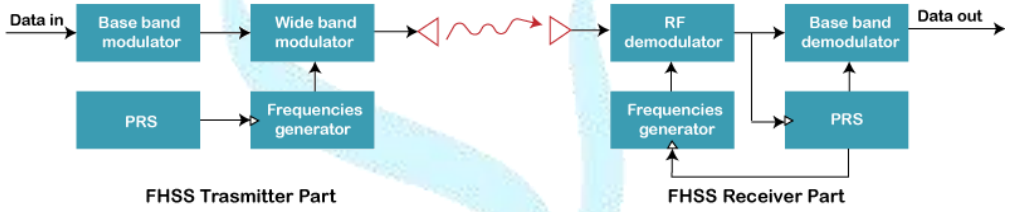

**Frequency Hopping Spread Spectrum (FHSS)**

- The Frequency Hopping Spread Spectrum or FHSS allows us to utilize bandwidth properly and maximum. In this technique, the whole available bandwidth is divided into many channels and spread between channels, arranged continuously.
- The frequency slots are selected randomly, and frequency signals are transmitted according to their occupancy.
- The transmitters and receivers keep on hopping on channels available for a particular amount of time in milliseconds.
- So, you can see that it implements the frequency division multiplexing and time-division multiplexing simultaneously in FHSS.

**The Frequency Hopping Spread Spectrum or FHSS can also be classified into two types:**




- **Slow Hopping:** In slow hopping, multiple bits are transmitted on a specific frequency or same frequency.
- **Fast Hopping:** In fast hopping, individual bits are split and then transmitted on different frequencies.




### Advantages of Frequency Hopping Spread Spectrum (FHSS)

- The biggest advantage of Frequency Hopping Spread Spectrum or FHSS is its high efficiency.
- It requires a shorter time for acquisition.
- We can easily program it to avoid some portions of the spectrum.
- It provides a very large bandwidth.
- It can be simply implemented as compared to DsSS.

### Disadvantages of Frequency Hopping Spread Spectrum (FHSS)

The following are some disadvantages of Frequency Hopping Spread Spectrum (FHSS):

- FHSS is less Robust, so sometimes it requires error correction.
- FHSS needs complex frequency synthesizers.
- FHSS supports a lower data rate of 3 Mbps as compared to the 11 Mbps data rate supported by DSSS.
- It is not very useful for range and range rate measurements.
- It supports the lower coverage range due to the high SNR requirement at the receiver.
- Nowadays, it is not very popular due to the emerging of new wireless technologies in wireless products.

### Applications of Frequency Hopping Spread Spectrum (FHSS)

Following is the list of most used applications of Frequency Hopping Spread Spectrum or FHSS:

- The Frequency Hopping Spread Spectrum or FHSS is used in wireless local area networks (WLAN) standard for Wi-Fi.
- FHSS is also used in the wireless personal area networks (WPAN) standard for Bluetooth.

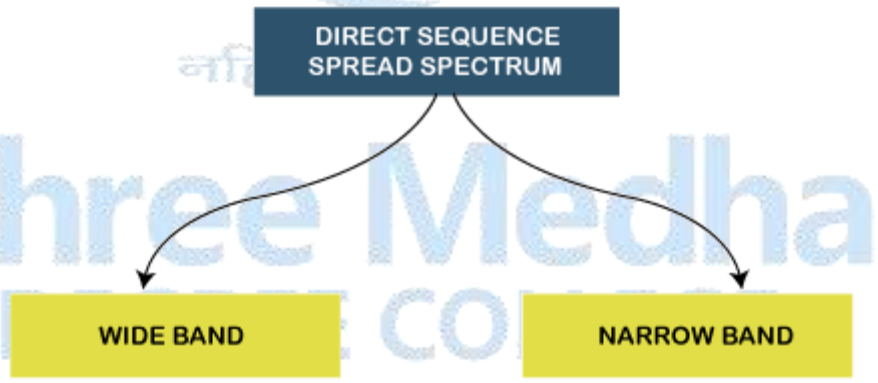
### Direct Sequence Spread Spectrum (DSSS)

The Direct Sequence Spread Spectrum (DSSS) is a spread-spectrum modulation technique primarily used to reduce overall signal interference in telecommunication. The Direct Sequence Spread Spectrum modulation makes the transmitted signal wider in bandwidth than the information bandwidth. In DSSS, the message bits are modulated by a bit sequencing process known as a spreading sequence. This spreading-sequence bit is known as a chip. It has a much shorter duration (larger bandwidth) than the original message bits. Following are the features of Direct Sequence Spread Spectrum or DSSS.

- In Direct Sequence Spread Spectrum or DSSS technique, the data that needs to be transmitted is split into smaller blocks.
- After that, each data block is attached with a high data rate bit sequence and is transmitted from the sender end to
- the receiver end.
- Data blocks are recombined again to generate the original data at the receiver's end, which was sent by the sender, with the help of the data rate bit sequence.
- 
- If somehow data is lost, then data blocks can also be recovered with those data rate bits.
- The main advantage of splitting the data into smaller blocks is that it reduces the noise and unintentional inference.

**The Direct Sequence Spread Spectrum or DSSS can also be classified into two types:**

- Wide Band Spread Spectrum
- Narrow Band Spread Spectrum




### Advantages of Direct Sequence Spread Spectrum (DSSS)

The following are some advantages of Direct Sequence Spread Spectrum or DSSS:

- Direct Sequence Spread Spectrum or DSSS is less reluctant to noise; that's why the DSSS system's performance in the presence of noise is better than the FHSS system.
- In Direct Sequence Spread Spectrum or DSSS, signals are challenging to detect.
- It provides the best discrimination against multipath signals.
- In Direct Sequence Spread Spectrum, there are very few chances of jamming because it avoids intentional interference such as jamming effectively.

### Disadvantages of Direct Sequence Spread Spectrum (DSSS)

The following are some disadvantages of Direct Sequence Spread Spectrum or DSSS:

- The Direct Sequence Spread Spectrum or DSSS system takes large acquisition time; that's why its performance is slow.
- It requires wide-band channels with small phase distortion.
- In DSSS, the pseudo-noise generator generates a sequence at high rates.

**Applications of Direct Sequence Spread Spectrum (DSSS)**

Following is the list of most used applications of Direct Sequence Spread Spectrum or DSSS:

- Direct Sequence Spread Spectrum or DSSS is used in LAN technology.
- Direct Sequence Spread Spectrum or DSSS is also used in Satellite communication technology.
- DSSS is used in the military and many other commercial applications.
- It is used in the low probability of the intercept signal.
- It supports Code division multiple access.

**12. What is a point-to-point Protocol (PPP)? Explain the services provided by PPP [2017]**

**Ans.**

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

The main services provided by Point - to - Point Protocol are −

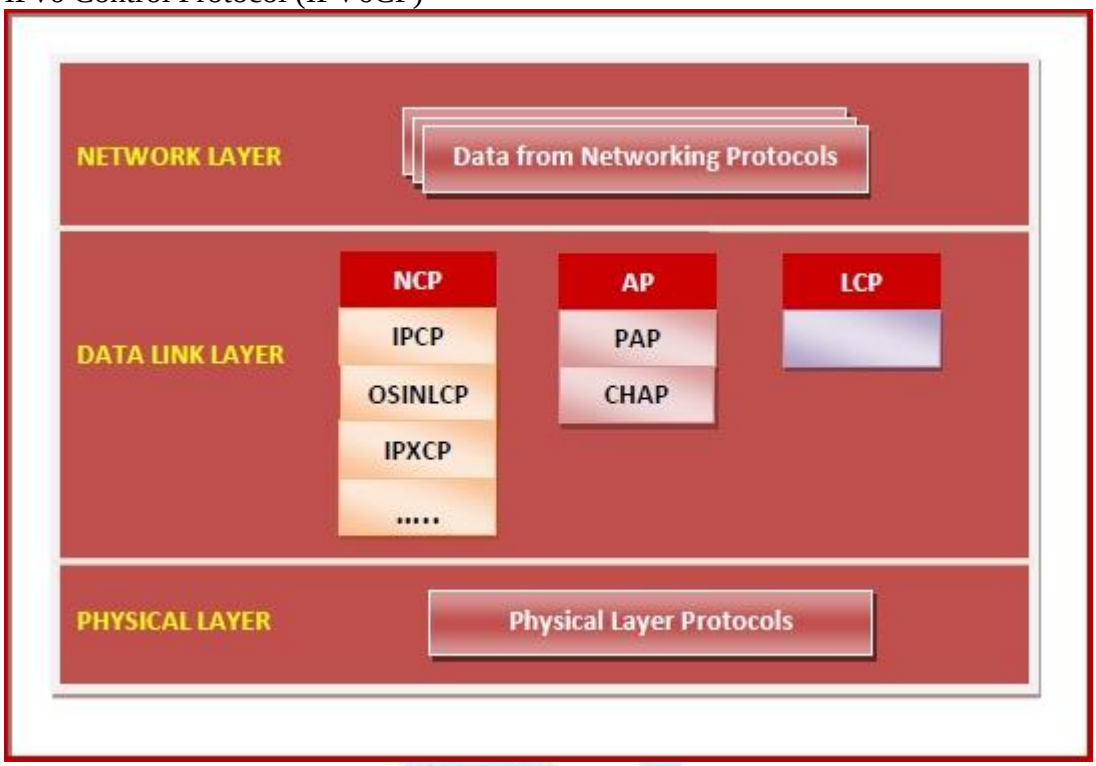
- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.
- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range os services.

Components of PPP

Point - to - Point Protocol is a layered protocol having three components −

- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are −
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are −
  - Internet Protocol Control Protocol (IPCP)
  - OSI Network Layer Control Protocol (OSINLCP)
  - Internetwork Packet Exchange Control Protocol (IPXCP)
  - DECnet Phase IV Control Protocol (DNCP)
  - NetBIOS Frames Control Protocol (NBFCP)

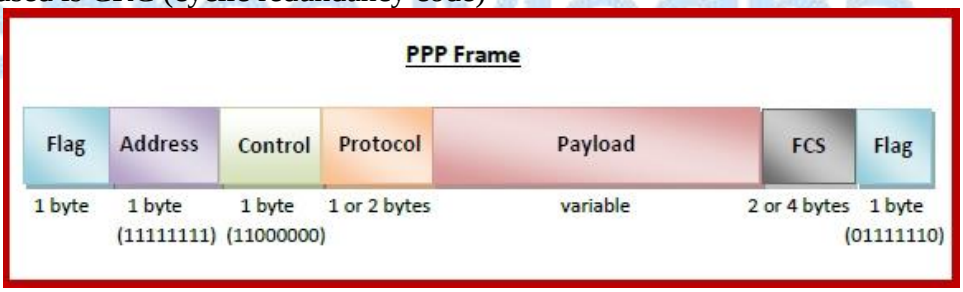
- IPv6 Control Protocol (IPV6CP)




PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are −

- **Flag** − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − 1 byte which is set to 11111111 in case of broadcast.
- **Control** − 1 byte set to a constant value of 11000000.
- **Protocol** − 1 or 2 bytes that define the type of data contained in the payload field.
- **Payload** − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)




**Byte Stuffing in PPP Frame** − Byte stuffing is used is PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

**13. Explain FDMA and TDMA channelization protocols [2017]**

**Ans.**

**CHANNELIZATION:**

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. In this section, we have three channelization protocols namely:

- FDMA (Frequency-Division Multiple Access).
- TDMA (Time- Division Multiple Access).
- CDMA (Code- Division Multiple Access).

**A) Frequency-Division Multiple Access (FDMA):**

- In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data.
- In other words, each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies.
- To prevent station interferences, the allocated bands are separated from one another by small guard bands to avoid crosstalk and noise.

FDMA specifies a predetermined frequency band for the entire period of communication. This means that stream data (a continuous flow of data that may not be packetized) can easily be used with FDMA. We need to emphasize that although FDMA and FDM conceptually seem similar, there are differences between them. FDM, is a physical layer technique that combines the loads from low-bandwidth channels and transmits them by using a high-bandwidth channel. The channels that are combined are low-pass. The multiplexer modulates the signals, combines them, and creates a bandpass signal. The bandwidth of each channel is shifted by the multiplexer.

FDMA, on the other hand, is an access method in the data link layer. The data link layer in each station tells its physical layer to make a bandpass signal from the data passed to it. The signal must be created in the allocated band. There is no physical multiplexer at the physical layer. The signals created at each station are automatically bandpass-filtered. They are mixed when they are sent to the common channel.

**B) Time-Division Multiple Access (TDMA):**

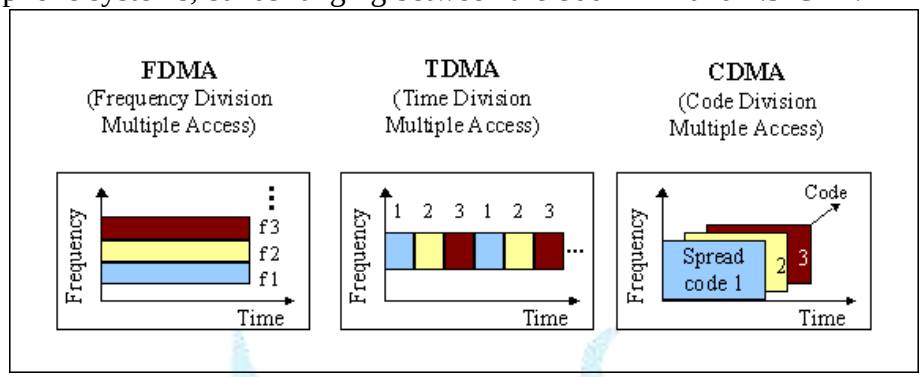
- In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data. Each station transmits its data in is assigned time slot.
- However, there is an overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot.
- Another issue with TDMA is propagation delay which is resolved by addition of guard band.

The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot. This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area. To compensate for the delays, we can insert guard times. Synchronization is normally accomplished by having some synchronization bits (normally referred to as preamble bits) at the beginning of each slot. We also need to emphasize that although TDMA and TDM conceptually seem the same, there are differences between them. TDM, is a physical layer technique that combines the data from slower channels and transmits them by using a faster channel. The process uses a physical multiplexer that interleaves data units from each channel. TDMA, on the other hand, is an access method in the data link layer. The data link layer in each station tells

its physical layer to use the allocated time slot. There is no physical multiplexer at the physical layer.

**C) Code-Division Multiple Access (CDMA):**

Code Division Multiple Access (CDMA) is a sort of multiplexing that facilitates various signals to occupy a single transmission channel. It optimizes the use of available bandwidth. The technology is commonly used in ultra-high-frequency (UHF) cellular telephone systems, bands ranging between the 800-MHz and 1.9-GHz.




**14. with a suitable diagram explain the architecture of Bluetooth in detail [2017]**

**ans.**

**Bluetooth**

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.
- The devices, sometimes called gadgets, find each other and make a network called a piconet.
- A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.
- A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.
- Bluetooth technology has several applications. **Peripheral devices** such as a wireless mouse or keyboard can communicate with the computer through this technology. **Monitoring devices** can communicate with sensor devices in a small health care center.
- Home security devices can use this technology to connect different sensors to the main security controller.
- Conference attendees can synchronize their laptop computers at a conference.
- Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. Blaatand translates to Bluetooth in English. Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

**ARCHITECTURE:**

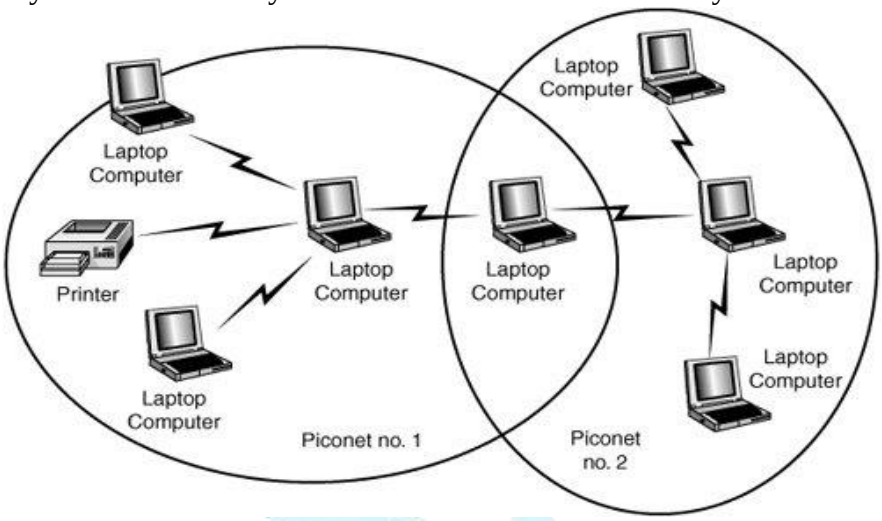
Bluetooth defines two types of networks:

1) Piconet and

2) Scatternet.

**Piconets:**

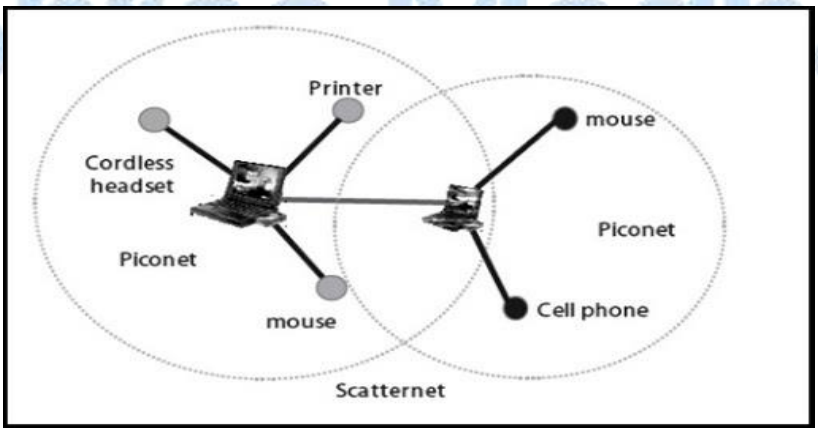
A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary the rest are called secondary. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.




Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

**Scatternet:**

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.




**15. With a suitable example explain serial and parallel transmission modes [2016]**

**Ans.**

**Transmission Modes:**

There are two methods used for transferring the data between computers which are given below:

1. Serial Transmission Mode.
2. Parallel Transmission Mode.

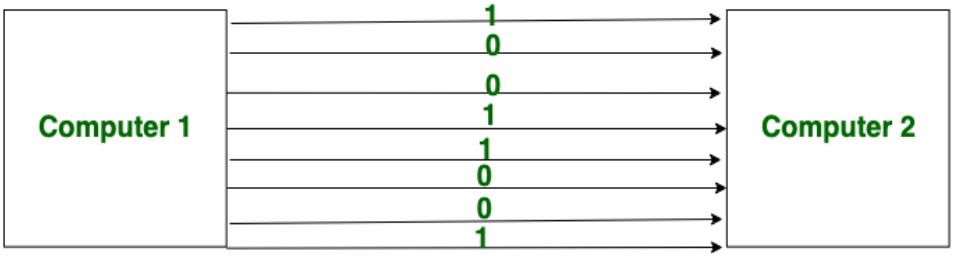
**Serial Transmission Mode:**

- Serial Transmission is the type of transmission in which a single communication link is used to transfer the data from an end to another.
- In case of Serial Transmission only one bit is transferred at one clock pulse.
- As single link is used in Serial Transmission, comparatively low cost is required for its implementation hence it is cost efficient.
- As single bit gets transmitted per clock in case of Serial Transmission, its performance is comparatively lower as compared to Parallel Transmission.
- As single bit gets transmitted per clock and only single link is implemented in Serial Transmission, it is more preferred for long distance transmission.
- Already mentioned due to single link implementation circuit having Serial Transmission is less complex as compared to that of Parallel Transmission.
- The circuit used in serial transmission is simple.


Serial Transmission

**Parallel Transmission Mode:**

- On other hand Parallel Transmission is the transmission in which multiple parallel links are used that transmit each bit of data simultaneously.
- On other hand in case of Parallel Transmission, eight bits transferred at one clock pulse.
- On other hand multiple links need to be implemented in case of Parallel Transmission hence more cost is required and hence it is not cost efficient.
- However on other hand as already mentioned that 8 bits get transferred per clock in case of Parallel transmission hence it is more efficient in performance.
- However on other hand as multiple bits get transferred and multiple links need to be implemented in case of Parallel Transmission, it is preferred only for short distance.
- However on other hand due to multiple link implementation circuit having Parallel Transmission is more complex as compared to that of Serial Transmission.
- The circuit used in parallel transmission is relatively complex.




Parallel Transmission

**16. Explain the different types of switching techniques [2016]**

**a. circuit switching**

**b. Message switching**
**c. Packet switching**

**Ans.**

**SWITCHING:**

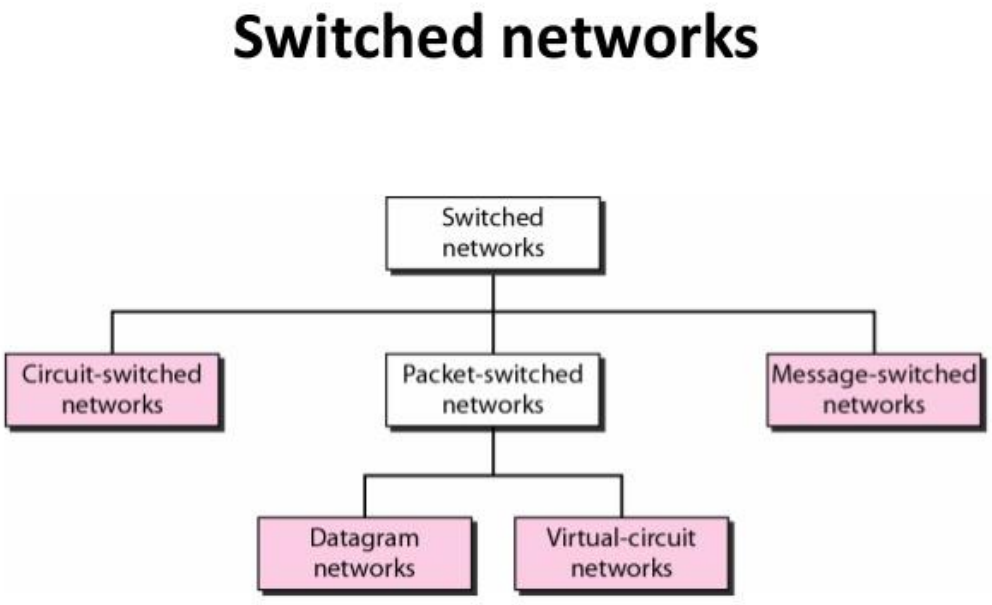
In large networks we need some means to allow one-to-one communication between any two nodes. In LANs this is achieved using one of three methods:

- Direct point-to-point connection (mesh)
- Via central controller (star)
- Connection to common bus in a multipoint configuration (bus/hup)

None of the previous works in larger networks with large physical separation or consisting of a large number of computers because it requires too much infrastructure and majority of those links would be idle for most of the time. Thus, better solution is a switching network. It consists of a series of interlinked nodes called switched. Switches are capable to create temporary connections between two or more devices. Some of these nodes are connected to the end system and others are used only for routing. End systems can be computers or telephones.

There are three types of Switched Network namely:

- Circuit Switched Network
- Packet Switched Network and
- Message Switched Network




**CIRCUIT SWITCHING:**

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. Each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM. The link can be permanent (leased line) or temporary (telephone).

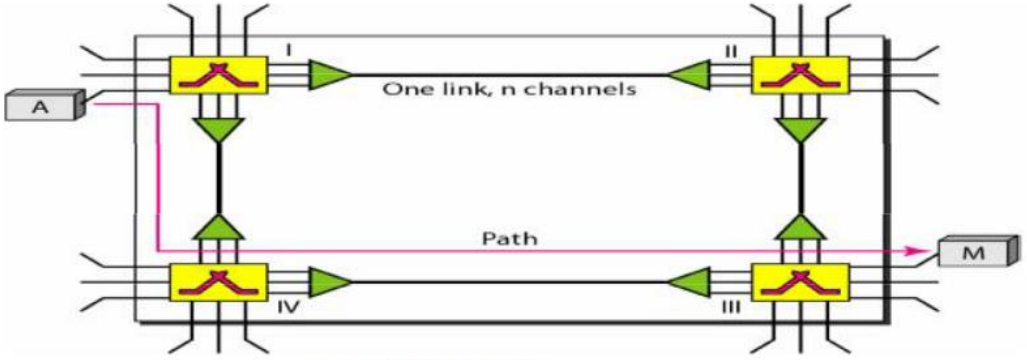



Fig 2.3 Circuit Switching

Switching takes place at physical layer. Resources can be bandwidth in FDM and time slot in TDM, switch buffer, switch processing time or switch I/O ports. Data transferred are not packetized, but it is a continuous flow. No addressing involved during data transfer. There are three transmission phases in circuit switching namely Setup phase, data transfer phase and tear down phase.

It can be argued that circuit-switched networks are not as efficient as the other two types of networks resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation. However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time. In this case, allowing resources to be dedicated means that other connections are deprived.

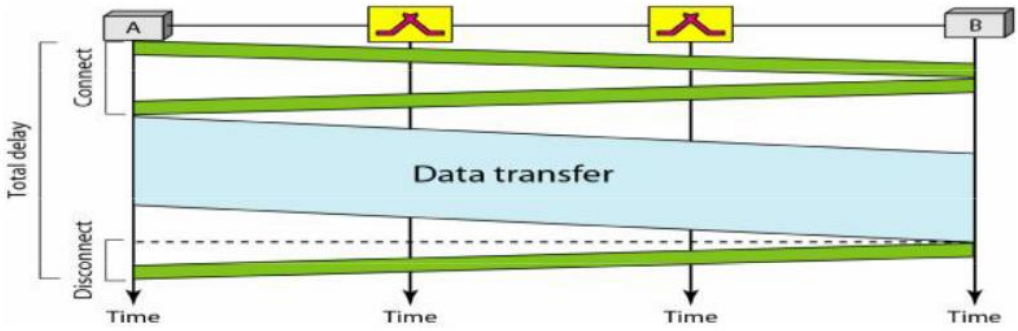



Fig 2.4 Delay in Circuit Switching

**B) PACKET SWITCHING:**

- In packet Switching, flow of data is not continuous rather it flows in the form of packets. The size of the packet is determined by the network and the governing protocol.
- This type of switching further classify into datagram networks and virtual circuit networks.
- The internet is a packet switched network.
- Message is broken into individual chunks called as packets.
- Each packet is sent individually.
- Each packet will have source and destination IP address with sequence number also.
- This sequence numbers will help receivers to – reorder the packets, detect missing packets, and send acknowledgements.

Packet switching is divided into two approaches:

1. Datagram approach.
2. Virtual approach.

**Datagram approach:**

- Datagram switching is also known as connectionless switching.

- Each independent entity is called as datagram.
- Datagram contains destination information and the intermediary devices uses this information to follow datagram to write destinations.
- In datagram packet switching approach, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.

**Virtual circuit approach:**

- Virtual circuit is also known as connection-oriented switching.
- In the case of virtual circuit switching a pre-planned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this approach the path is fixed for the duration of a logical connection.

**Message switching:**

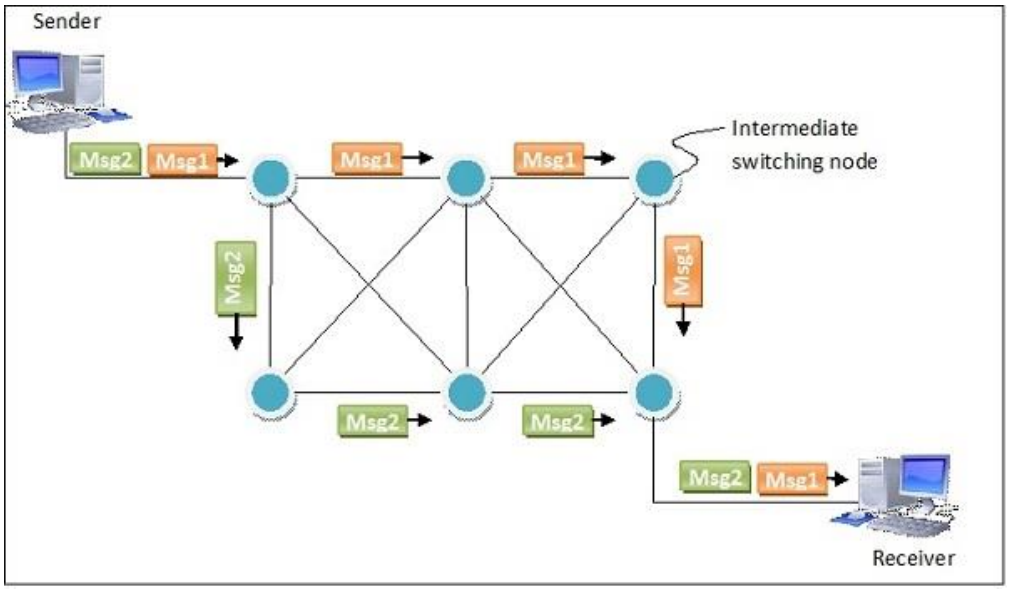
Message switching is a connectionless network switching technique where the entire message is routed from the source node to the destination node, one hop at a time. It was a precursor of packet switching.

**Process**

Packet switching treats each message as an individual unit. Before sending the message, the sender node adds the destination address to the message. It is then delivered entirely to the next intermediate switching node. The intermediate node stores the message in its entirety, checks for transmission errors, inspects the destination address and then delivers it to the next node. The process continues till the message reaches the destination.

In the switching node, the incoming message is not discarded if the required outgoing circuit is busy. Instead, it is stored in a queue for that route and retransmitted when the required route is available. This is called store and forward network.

The following diagram represents routing of two separate messages from the same source to same destination via different routes, using message switching –




**Advantages and Disadvantages of Message Switching**

**Advantages**

- Sharing of communication channels ensures better bandwidth usage.
- It reduces network congestion due to store and forward method. Any switching node can store the messages till the network is available.

- Broadcasting messages requires much less bandwidth than circuit switching.
- Messages of unlimited sizes can be sent.
- It does not have to deal with out of order packets or lost packets as in packet switching.

**Disadvantages**

- In order to store many messages of unlimited sizes, each intermediate switching node requires large storage capacity.
  Store and forward method introduce delay at each switching node. This renders it unsuitable for real time applications.

**17. Write a short note on [2016]**

**a. Fast Ethernet**

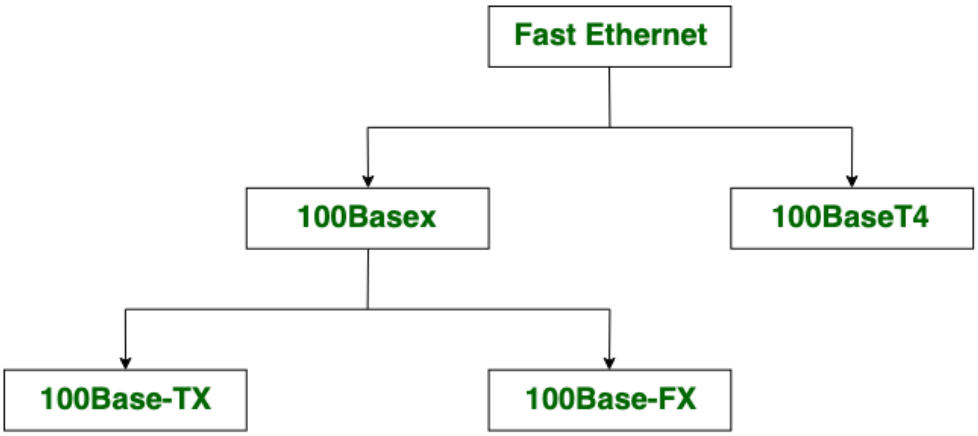
**b. Gigabit Ethernet**

**Ans.**

**Fast Ethernet** is the Successor of 10-Base-T Ethernet. It is more popular than Gigabit Ethernet because its configuration and implementation is simple. It is faster than its successors. Its variants are:

1. 100Base-T4
2. 100Base-Tx
3. 100Base-Fx

The coverage limit of Fast Ethernet is up to 10 km and its round-trip delay in Fast Ethernet is 100-to-500-bit times.




Categories of Fast Ethernet



- Fast Ethernet provides 100 Mbps speed.
- Fast Ethernet is simple configured.
- Fast Ethernet generate more delay comparatively.
- The coverage limit of Fast Ethernet is up to 10 km.
- The round-trip delay in Fast Ethernet is 100 to 500 bit times.
- Fast Ethernet is the Successor of 10-Base-T Ethernet.

**Gigabit Ethernet:**

**Gigabit Ethernet** is the successor of Fast Ethernet. It can produces upto 1 Gbps speed. It is less popular than Fast Ethernet because its configuration and implementation is complicated than Fast Ethernet. The coverage limit of Gigabit Ethernet is up to 70 km.

- Gigabit Ethernet offers 1 Gbps speed.
- While Gigabit Ethernet is more complicated than Fast Ethernet.
- Gigabit Ethernet generate less delay than Fast Ethernet.

- The coverage limit of Gigabit Ethernet is up to 70 km.
- The round-trip delay in Gigabit Ethernet is 4000 bit times.
- Gigabit Ethernet is the Successor of Fast Ethernet.

**18. Explain the IPV6 Architecture [2016]**
**Ans.**

| IPV4 | IPV6 |
|---|---|
| • 32-bit address length.<br>• Single header format for all datagrams.<br>• It is simple.<br>• Specifies all possible protocol features.<br>• Small address space.<br>• Address representation of IPV4 is in decimal.<br>• Fragmentation performed by sender and forwarding routers.<br>• In IPV4 end to end connection integrity is unachievable.<br>• In IPV4 encryption and authentication facility not provided.<br>• In IPV4 packet flow identification is not available.<br>• In IPV4 checksumfield is available.<br>• IPV4 is a numeric addressing method.<br>• IPV4 has header of 20-60 bytes.<br>• Security is dependent on applications. | • 128-bit address length.<br>• Information encoded into spate headers, base header followed by zero or more extension headers, followed by data.<br>• It is complex.<br>• Extensible protocol, more flexible, new features can be added.<br>• Large address space.<br>• Address representation of IPV6 is in hexadecimal.<br>• In IPV6 fragmentation performed by only sender.<br>• In IPV6 end to end connection integrity is achievable.<br>• In IPV6 encryption and authentication facility are provided.<br>• In IPV6 packet flow identification are available and uses flow label field in the header.<br>• In IPV6 checksumfield is not available.<br>• IPV6 is an alphanumeric addressing method.<br>• IPV6 has header of 40 bytes fixed.<br>• IPSec(Internet protocol Security) is built in IPV6 protocol. |