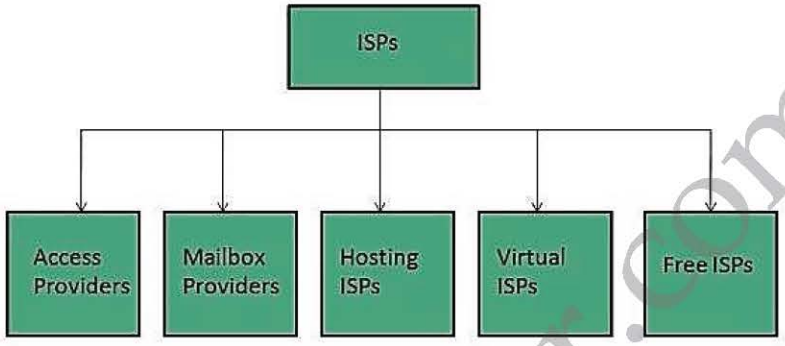
MCS-218: Data Communication and Computer Networks
Guess Paper-1

Q1. What is ISP? Explain the types of ISP?

Ans. Internet Service Provider (ISP) is a company offering access to internet. They offer various services:

- Internet Access
- Domain name registration
- Dial-up access
- Leased line access

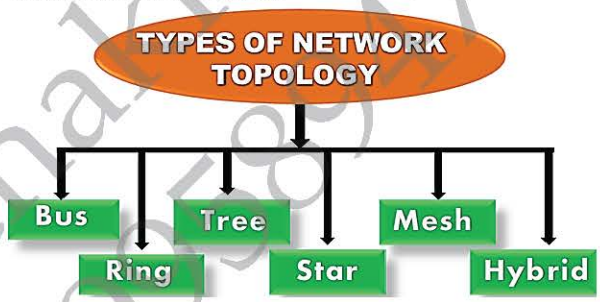
ISP Types: ISPs can broadly be classified into six categories as shown in the following diagram:



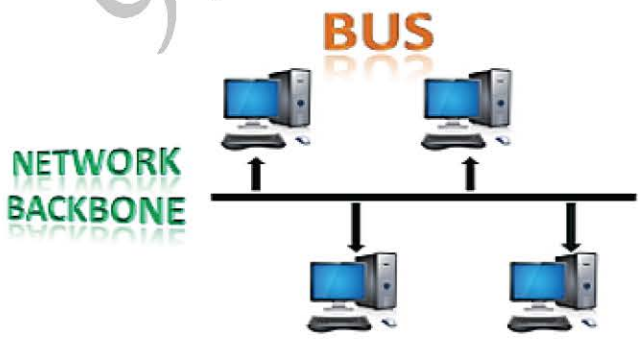
Access providers: They provide access to internet through telephone lines, cable wi-fi or fiber optics.
Mailbox Provider: Such providers offer mailbox hosting services.
Hosting ISPs: Hosting ISPs offers e-mail, and other web hosting services such as virtual machines, clouds etc.
Virtual ISPs: Such ISPs offer internet access via other ISP services.
Free ISPs: Free ISPs do not charge for internet services.

Q2. What is network Topology? Explain each type of Topology in Detail?

Ans. Topology defines the structure of the network of how all the components are interconnected to each other. It is the geometric representation of all the nodes in a network.



Bus Topology



The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
The configuration of a bus topology is quite simpler as compared to other topologies.
The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations.
The most common access method of the bus topologies is CSMA (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

CSMA CD: CSMA CD (Collision detection) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "recovery after the collision".

CSMA CA: CSMA CA (Collision Avoidance) is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

Advantages of Bus topology:

Low-cost cable: In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.

Moderate data speeds: Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.

Familiar technology: Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.

Limited failure: A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is token passing.

Token passing: It is a network access method in which token is passed from one node to another node.

Token: It is a frame that circulates around the network.

Working of Token passing: A token moves around the network, and it is passed from computer to computer until it reaches the destination.

The sender modifies the token by putting the address along with the data.

The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.

In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

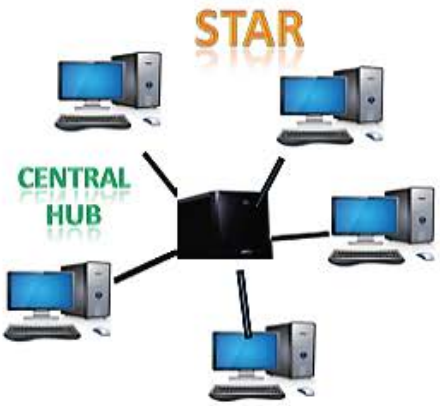
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.

- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology



Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
The central computer is known as a server, and the peripheral devices attached to the server are known as clients.
Coaxial cable or RJ-45 cables are used to connect the computers.
Hubs or Switches are mainly used as connection devices in a physical star topology.
Star topology is the most popular topology in network implementation.

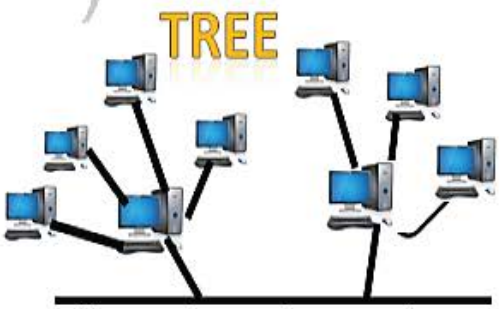
Advantages of Star topology:

Efficient troubleshooting: Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
Network control: Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
Limited failure: As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
Familiar technology: Star topology is a familiar technology as its tools are cost-effective.
Easily expandable: It is easily expandable as new stations can be added to the open ports on the hub.
Cost effective: Star topology networks are cost-effective as it uses inexpensive coaxial cable.
High data speeds: It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology:

A Central point of failure: If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
Cable: Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology



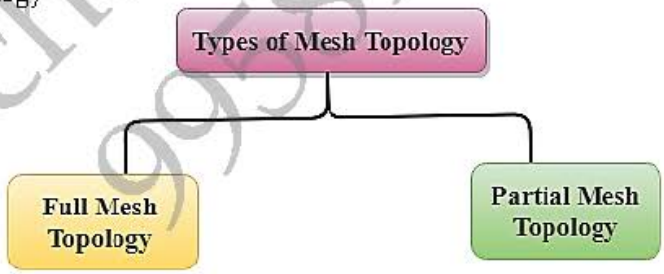
Tree topology combines the characteristics of bus topology and star topology.
A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology:

Support for broadband transmission: Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
Easily expandable: We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.

Easily manageable: In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
Error detection: Error detection and error correction are very easy in a tree topology.
Limited failure: The breakdown in one station does not affect the entire network.
Point-to-point wiring: It has point-to-point wiring for individual segments.
Disadvantages of Tree topology:
Difficult troubleshooting: If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
High cost: Devices required for broadband transmission are very costly.
Failure: A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
Reconfiguration difficult: If new devices are added, then it becomes difficult to reconfigure.
Mesh topology

Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
There are multiple paths from one computer to another computer.
It does not contain the switch, hub or any central computer which acts as a central point of communication.
The Internet is an example of the mesh topology.
Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
Mesh topology is mainly used for wireless networks.
Mesh topology can be formed by using the formula:
Number of cables = (n*(n-1))/2;
Where n is the number of nodes that represents the network.
Mesh topology is divided into two categories:
Fully connected mesh topology
Partially connected mesh topology



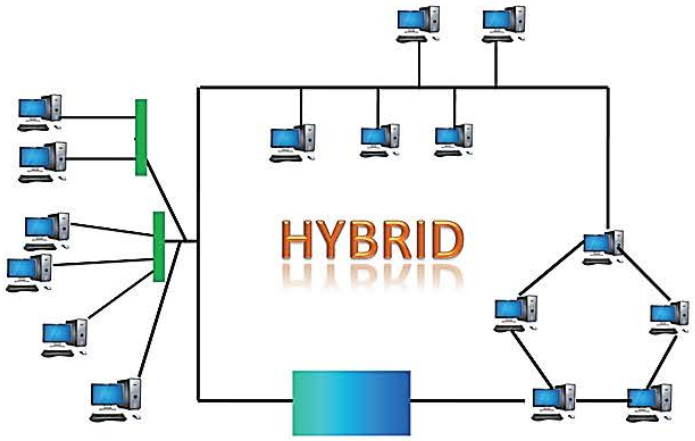
Full Mesh Topology: In a full mesh topology, each computer is connected to all the computers available in the network.
Partial Mesh Topology: In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.
Advantages of Mesh topology:

- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology:

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology



The combination of various different topologies is known as Hybrid topology.
A Hybrid topology is a connection between different links and nodes to transfer the data.
When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology:

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology:

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Q3. What is transmission media?

Ans. Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
The main functionality of the transmission media is to carry the information in the form of bits through LAN (Local Area Network). It is a physical path between transmitter and receiver in data communication. In a copper-based network, the bits in the form of electrical signals. In a fibre based network, the bits in the form of light pulses.
In OSI (Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component. The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
The transmission media is available in the lowest layer of the OSI reference model, i.e., Physical layer.

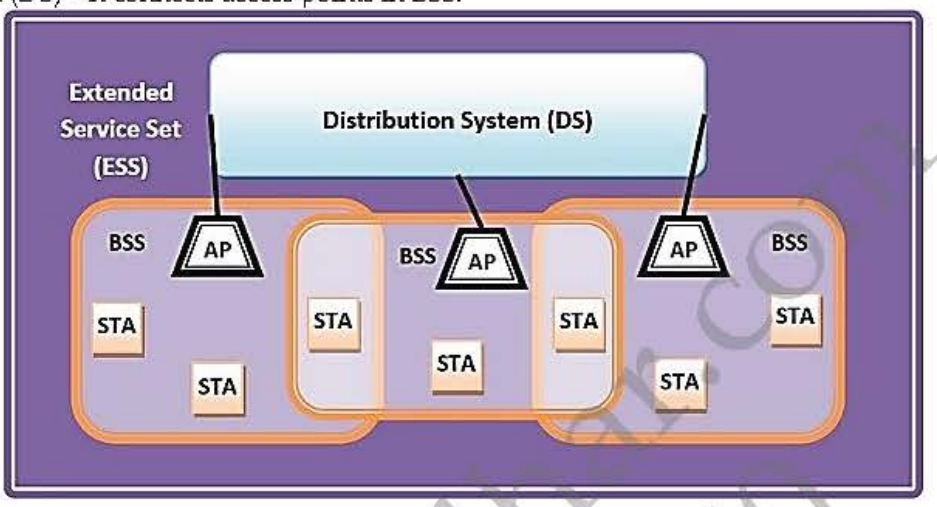
Q4. Briefly describe Wireless LAN?

Ans. Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.
Most WLANs are based upon the standard IEEE 802.11 standard or WiFi.
Components of WLANs
The components of WLAN architecture as laid down in IEEE 802.11 are:-

Stations (STA) – Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types –
Wireless Access Point (WAP or AP)
Client
Basic Service Set (BSS): A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories:

- Infrastructure BSS
- Independent BSS

Extended Service Set (ESS) – It is a set of all connected BSS.
Distribution System (DS) – It connects access points in ESS.



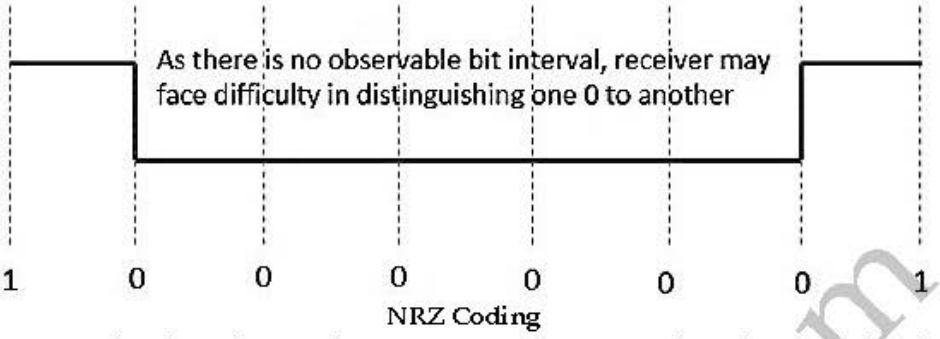
Types of WLANS:
WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.
Infrastructure Mode – Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
Ad Hoc Mode – Clients transmit frames directly to each other in a peer-to-peer fashion.
Advantages of WLANs:
They provide clutter-free homes, offices and other networked places.
The LANs are scalable in nature, i.e. devices may be added or removed from the network at greater ease than wired LANs.
The system is portable within the network coverage. Access to the network is not bounded by the length of the cables.
Installation and setup are much easier than wired counterparts.
The equipment and setup costs are reduced.
Disadvantages of WLANs:
Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
WLANs are slower than wired LANs.

Q5. What is encoding? Explain the different types of data encoding techniques?
Ans. Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of data. Decoding is the reverse process of encoding which is to extract the information from the converted format.
Data Encoding: It is the process of using various patterns of voltage or current levels to represent 1s and 0s of the digital signals on the transmission link.
The common types of line encoding are Unipolar, Polar, Bipolar, and Manchester.
Encoding Techniques: The data encoding technique is divided into the following types, depending upon the type of data conversion.
Analog data to Analog signals: The modulation techniques such as Amplitude Modulation, Frequency Modulation and Phase Modulation of analog signals, fall under this category.
Analog data to Digital signals: This process can be termed as digitization, which is done by Pulse Code Modulation PCMPCM. Hence, it is nothing but digital modulation. As we have already discussed, sampling and quantization are the important factors in this. Delta Modulation gives a better output than PCM.
Digital data to Analog signals: The modulation techniques such as Amplitude Shift Keying ASK, Frequency Shift Keying FSK, Phase Shift Keying PSK, etc., fall under this category.

Digital data to Digital signals - There are several ways to map digital data to digital signals. Some of them are:

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

The following figure explains the concept of NRZ coding.



NRZ Coding

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

There are two variations in NRZ namely –

NRZ - L NRZ–LEVELNRZ–LEVEL

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

NRZ - I NRZ–INVERTEDNRZ–INVERTED

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

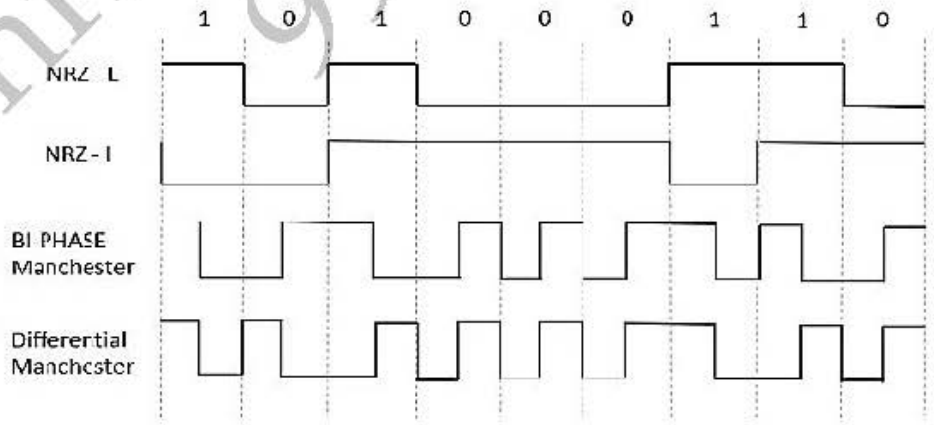
NRZ codes has a disadvantage that the synchronization of the transmitter clock with the receiver clock gets completely disturbed, when there is a string of 1s and 0s. Hence, a separate clock line needs to be provided.

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

There are two types of Bi-phase Encoding.

- **Bi-phase Manchester:** In this type of coding, the transition is done at the middle of the bit-interval. The transition for the resultant pulse is from High to Low in the middle of the interval, for the input bit 1, while the transition is from Low to High for the input bit 0.
- **Differential Manchester:** In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is 0. If no transition occurs at the beginning of the bit interval, then the input bit is 1.

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



Block Coding: Among the types of block coding, the famous ones are 4B/5B encoding and 8B/6T encoding. The number of bits are processed in different manners, in both of these processes.

4B/5B Encoding

In Manchester encoding, to send the data, the clocks with double speed is required rather than NRZ coding. Here, as the name implies, 4 bits of code is mapped with 5 bits, with a minimum number of 1 bits in the group.

The clock synchronization problem in NRZ-I encoding is avoided by assigning an equivalent word of 5 bits in the place of each block of 4 consecutive bits. These 5-bit words are predetermined in a dictionary.

The basic idea of selecting a 5-bit code is that, it should have one leading 0 and it should have no more than two trailing 0s. Hence, these words are chosen such that two transactions take place per block of bits.

8B/6T Encoding

We have used two voltage levels to send a single bit over a single signal. But if we use more than 3 voltage levels, we can send more bits per signal.

For example, if 6 voltage levels are used to represent 8 bits on a single signal, then such encoding is termed as 8B/6T encoding. Hence in this method, we have as many as 729 3636 combinations for signal and 256 2828 combinations for bits.

These are the techniques mostly used for converting digital data into digital signals by compressing or coding them for reliable transmission of data.

Q6. What are DLC protocols?

Ans. DLC (data link control) is the service provided by the Data Link layer of function defined in the Open Systems Interconnection (OSI) model for network communication.

The Data Link layer is responsible for providing reliable data transfer across one physical link (or telecommunications path) within the network. Some of its primary functions include defining frames, performing error detection or ECC on those frames, and performing flow control (to prevent a fast sender from overwhelming a slow receiver).

Many point-to-point protocols exist at the Data Link layer including High-level Data Link Control (HDLC), Synchronous Data Link Control (SDLC), Link Access Procedure Balanced (LAPB), and Advanced Data Communications Control Procedure (ADCCP). All of these protocols are very similar in nature and are found in older networks (such as X.25 networks). In the Internet, one of two point-to-point protocols are used at this layer: Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP) with PPP being the newer, approved standard. All of these protocols are used in point-to-point connections such as those on metropolitan area network (MAN) or wide area network (WAN) backbones or when we dial our Internet service provider (ISP) from home using a modem.

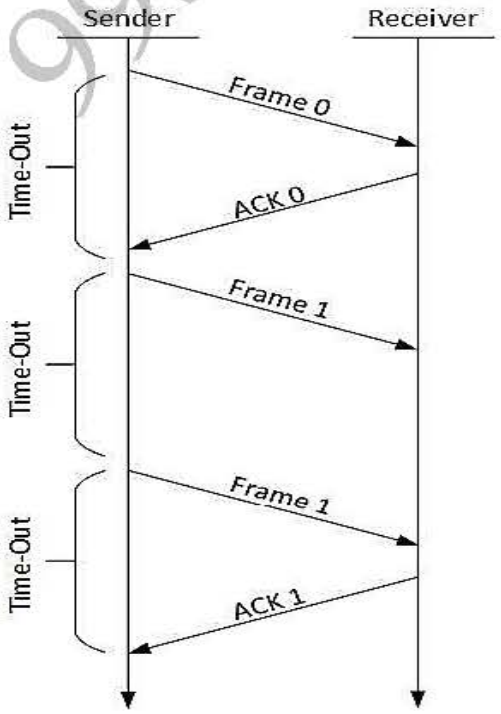
In local area networks (LANs) where connections are multipoint rather than point-to-point and require more line-sharing management, the Data Link layer is divided into two sublayers: the Logical Link Control layer and the Media Access Control layer. The Logical Link Control layer protocol performs many of the same functions as the point-to-point data link control protocols described above. The Media Access Control (MAC) layer protocols support methods of sharing the line among a number of computers. Among the most widely used MAC protocols are Ethernet (IEEE 802.3), Token Bus (IEEE 802.4), and token ring (IEEE 802.5) and their derivatives.

Q7. What is retransmission? Explain it techniques?

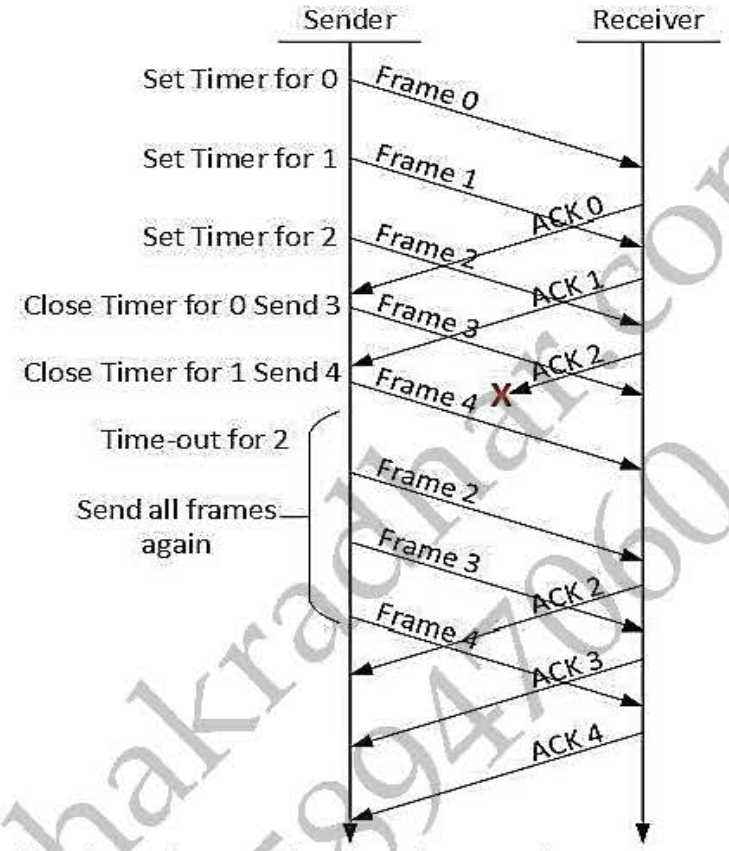
Ans. Retransmission: The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

Stop-and-wait ARQ



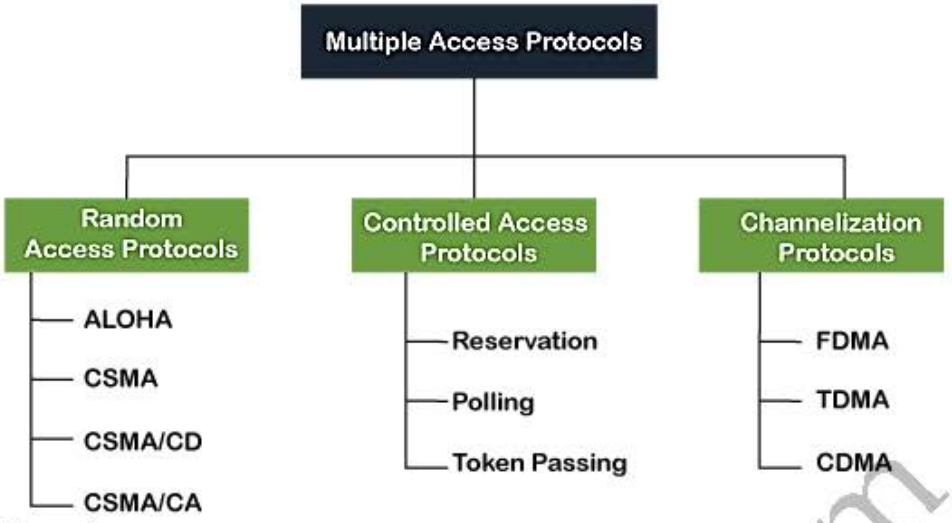
The following transition may occur in Stop-and-Wait ARQ:
The sender maintains a timeout counter.
When a frame is sent, the sender starts the timeout counter.
If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
If a negative acknowledgement is received, the sender retransmits the frame.
Go-Back-N ARQ
Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.



The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.
When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.
Selective Repeat ARQ
In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.

Q8. What is Media Access Protocols?

Ans. When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.
For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.
Following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

Aloha

CSMA

CSMA/CD

CSMA/CA

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

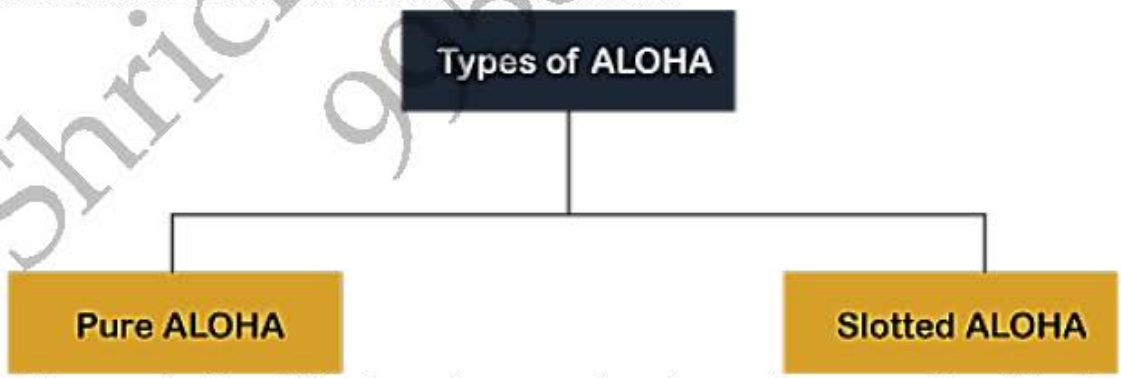
Any station can transmit data to a channel at any time.

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.

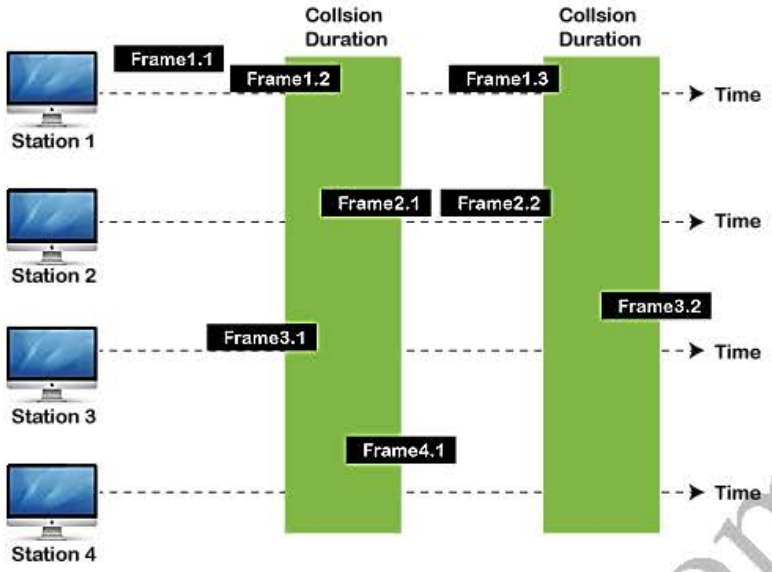


Pure Aloha: Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

The total vulnerable time of pure Aloha is 2 * Tfr.

Maximum throughput occurs when G = 1/ 2 that is 18.4%.

Successful transmission of data frame is S = G * e ^ - 2 G.



Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

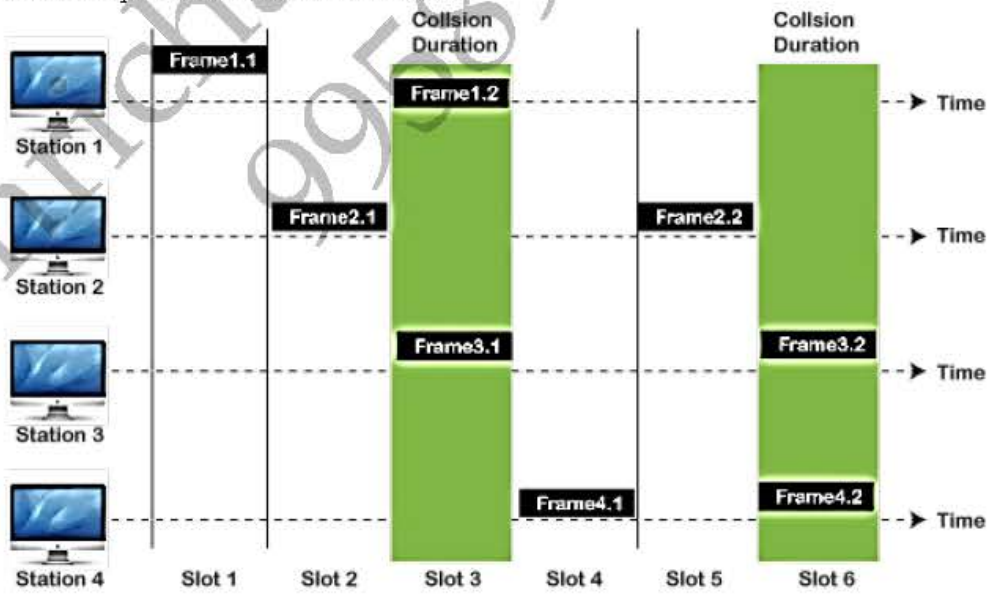
Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called slots. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.

The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.

The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

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.

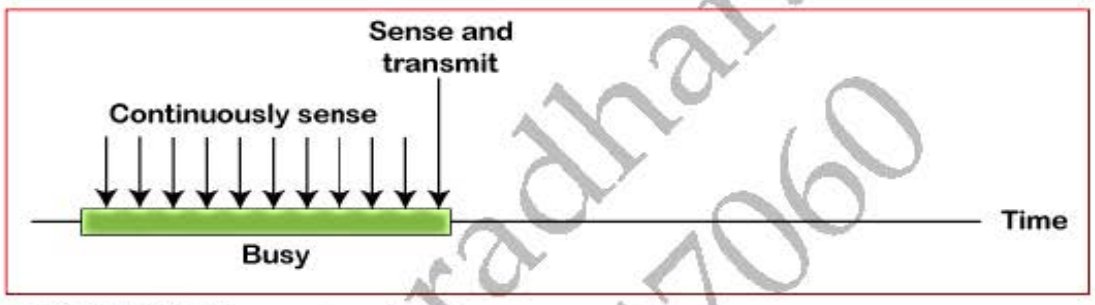
P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time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

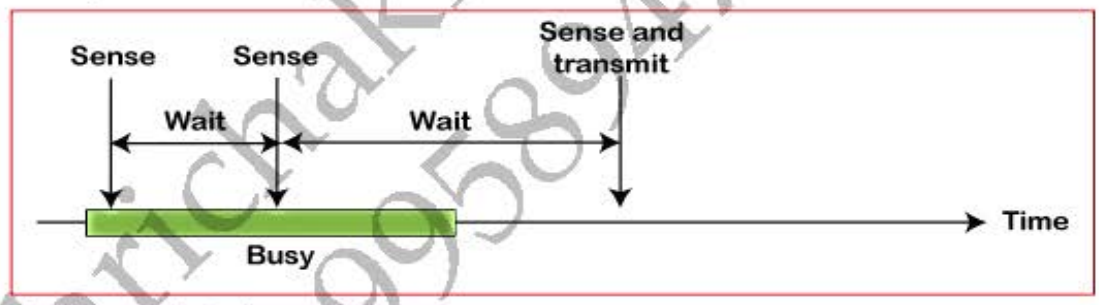
Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it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

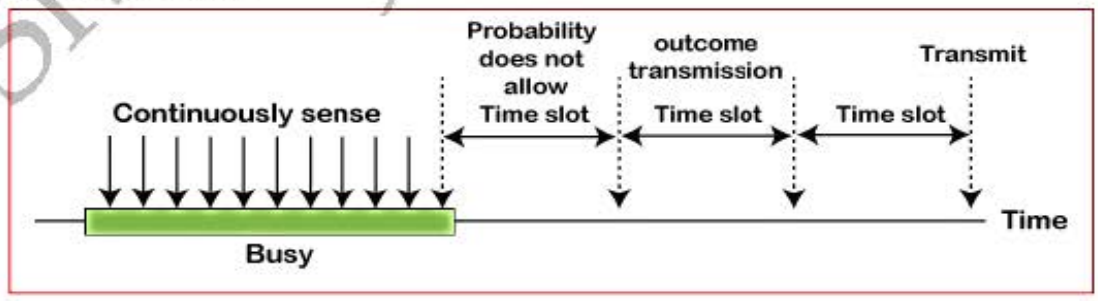
O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/CD

It is a carrier sense multiple access/ collision detection network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

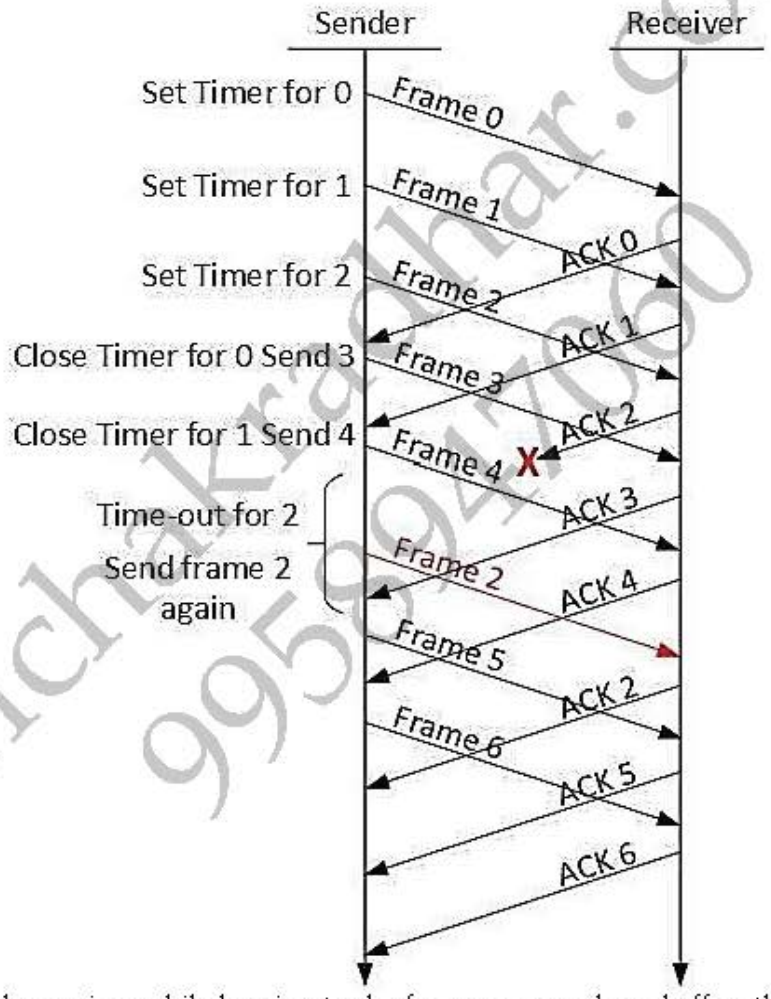
CSMA/ CA: It is a carrier sense multiple access/collision avoidance network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the Interframe space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.



In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

Q9. Differentiate between Bluetooth and Zigbee?

Ans. Bluetooth was developed under IEEE 802.15.1, which is used for providing wireless communication through radio signals. The frequency range supported in Bluetooth vary from 2.4 GHz to 2.483 GHz. It covers less distance than Zigbee. In bluetooth, GFSK modulation technique is used.

Whereas in Zigbee, BPSK and QPSK modulation techniques are used like UWB (Ultra-Wide Band). the frequency range supported in Zigbee mostly 2.4 GHz worldwide, it means 2.4 GHz is not supported all times. It covers more distance as compared with Bluetooth.

Both Bluetooth and ZigBee have a lot in common which are, each area unit styles of IEEE 802.15 WPANs. each run within the a pair of.4-GHz unlicensed band, and each use tiny kind factors and low power. Besides these similarities, there are some differences which are given below in tabular form.

S.NO	Bluetooth	Zigbee
1.	The frequency range supported in Bluetooth vary from 2.4 GHz to 2.483 GHz.	While the frequency range supported in Zigbee mostly 2.4 GHz worldwide.
2.	There are seventy nine RF channels in Bluetooth.	There are sixteen RF channels in zigbee.
3.	It uses GFSK modulation technique.	Whereas it also uses BPSK and QPSK modulation techniques like UWB.
4.	There is maximum of 8 cell nodes in Bluetooth.	While there is more than sixty five thousand (65000) cell nodes in zigbee.
5.	Bluetooth requires low bandwidth.	While zigbee also requires low bandwidth but greater than Bluetooth's bandwidth most of time.
6.	The radio signal range of Bluetooth is ten meters.	While the radio signal range of zigbee is ten to hundred meters.
7.	Bluetooth was developed under IEEE 802.15.1.	Whereas it was developed under IEEE 802.15.4.

Q10. Describe routing Algorithms?

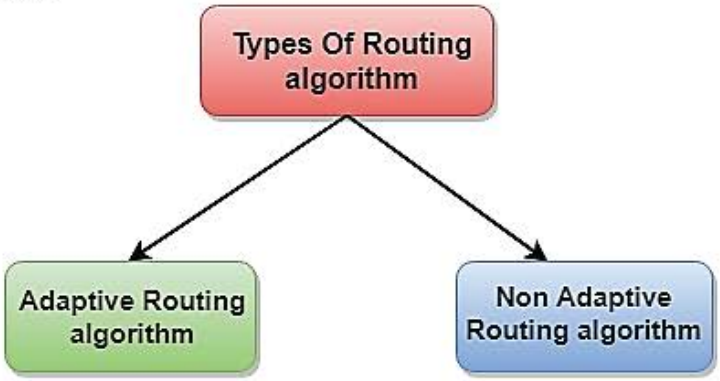
Ans. Routing algorithm: In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted. Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.

The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.

Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm: The Routing algorithm is divided into two categories:

Adaptive Routing algorithm
Non-adaptive Routing algorithm



Adaptive Routing algorithm
An adaptive routing algorithm is also known as dynamic routing algorithm.
This algorithm makes the routing decisions based on the topology and network traffic.
The main parameters related to this algorithm are hop count, distance and estimated transit time.
An adaptive routing algorithm can be classified into three parts:

(1) **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. Link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

(2) **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.

(3) **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm: Non Adaptive routing algorithm is also known as a static routing algorithm.
When booting up the network, the routing information stores to the routers.
Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.
The Non-Adaptive Routing algorithm is of two types:
Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.
Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.
Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

MCS-218: Data Communication and Computer Networks
Guess Paper-II

Q1.What is congestion? Explain leaky bucket algorithm?

Ans. A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion: As delay increases, performance decreases.

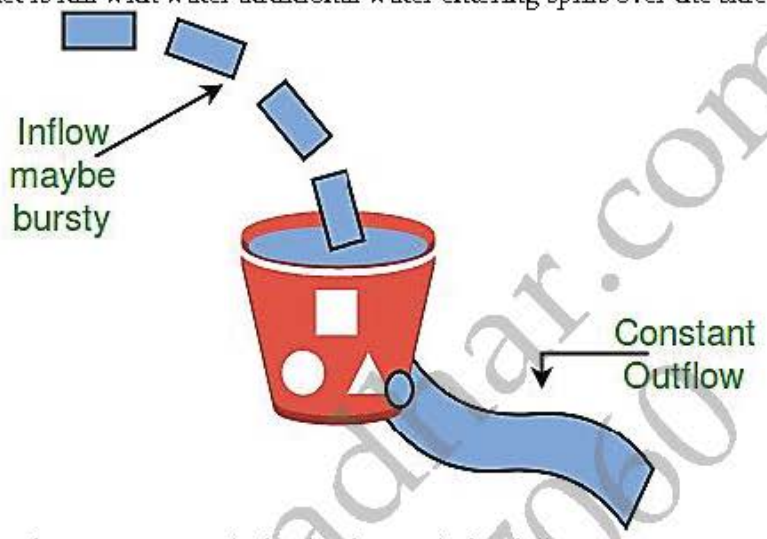
If delay increases, retransmission occurs, making situation worse.

Congestion control algorithms

Leaky Bucket Algorithm

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

When host wants to send packet, packet is thrown into the bucket.

The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

Bursty traffic is converted to a uniform traffic by the leaky bucket.

In practice the bucket is a finite queue that outputs at a finite rate.

Token bucket Algorithm

Need of token bucket Algorithm: The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

- In regular intervals tokens are thrown into the bucket. *f*
- The bucket has a maximum capacity. *f*
- If there is a ready packet, a token is removed from the bucket, and the packet is sent.
- If there is no token in the bucket, the packet cannot be sent.

Let's understand with an example,

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Ways in which token bucket is superior to leaky bucket: The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

Formula: $M * s = C + \varrho * s$

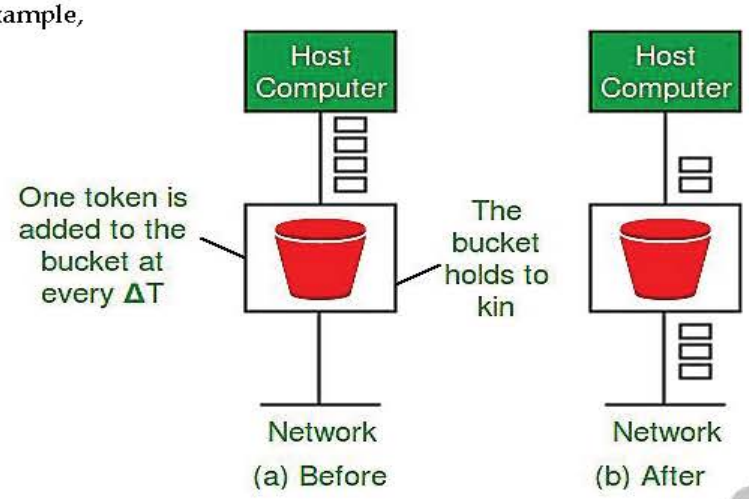
where S – is time taken

M – Maximum output rate

ϱ – Token arrival rate

C – Capacity of the token bucket in byte

Let's understand with an example,



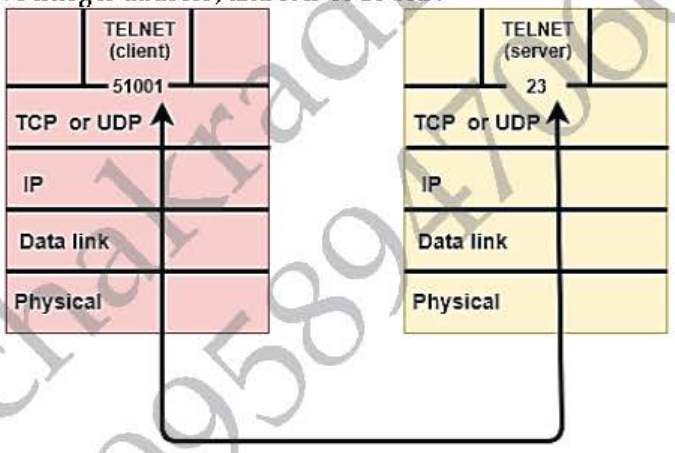
Q2. Describe transport layer Protocols?

Ans. The transport layer is represented by two protocols: TCP and UDP. The IP protocol in the network layer delivers a datagram from a source host to the destination host. Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process.

When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.

An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.

Each port is defined by a positive integer address, and it is of 16 bits.



UDP

UDP stands for User Datagram Protocol.

UDP is a simple protocol and it provides nonsequenced transport functionality.

UDP is a connectionless protocol.

This type of protocol is used when reliability and security are less important than speed and size.

UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.

The packet produced by the UDP protocol is known as a user datagram.

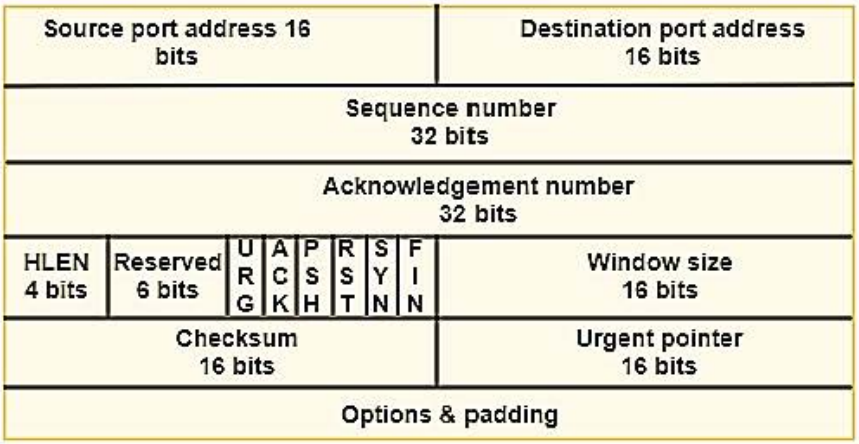
User Datagram Format

The user datagram has a 16-byte header which is shown below:

Where,

Source port address: It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.

Destination port address: It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
Total length: It defines the total length of the user datagram in bytes. It is a 16-bit field.
Checksum: The checksum is a 16-bit field which is used in error detection.
Disadvantages of UDP protocol
UDP provides basic functions needed for the end-to-end delivery of a transmission.
It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.
TCP
TCP stands for Transmission Control Protocol.
It provides full transport layer services to applications.
It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.
Features of TCP protocol
Stream data transfer: TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
Reliability: TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
Flow Control: When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
Multiplexing: Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
Logical Connections: The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
Full Duplex: TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
Establish a connection between two TCPs.
Data is exchanged in both the directions.
The Connection is terminated.
TCP Segment Format



Where,
Source port address: It is used to define the address of the application program in a source computer. It is a 16-bit field.

Destination port address: It is used to define the address of the application program in a destination computer. It is a 16-bit field.
Sequence number: A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
Acknowledgement number: A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
Header Length (HLEN): It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
Reserved: It is a six-bit field which is reserved for future use.
Control bits: Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.
There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.

Window Size: The window is a 16-bit field that defines the size of the window.
Checksum: The checksum is a 16-bit field used in error detection.
Urgent pointer: If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
Options and padding: It defines the optional fields that convey the additional information to the receiver.
Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	Slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

Q3. What is Symmetric Key Cryptography?
Ans. Symmetric Key Cryptography also known as Symmetric Encryption is when a secret key is leveraged for both encryption and decryption functions. This method is the opposite of Asymmetric Encryption where one key is used to encrypt and another is used to decrypt. During this process, data is converted to a format that cannot be read or inspected by anyone who does not have the secret key that was used to encrypt it.
The success of this approach depends on the strength of the random number generator that is used to create the secret key. Symmetric Key Cryptography is widely used in today's Internet and primarily consists of two types of algorithms, Block and Stream. Some common encryption algorithms include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). This form of encryption is traditionally faster than Asymmetric however it requires both the sender and the recipient of the data to have the secret key. Asymmetric cryptography does not rely on sharing a secret key and forms the basis of the FIDO authentication framework.
Q4. List some examples of a Cyber Attack?
Ans. Some examples of common cyber-attacks and types of data breaches:

- Identity theft, fraud, extortion
- Malware, phishing, spamming, spoofing, spyware, trojans and viruses

- Stolen hardware, such as laptops or mobile devices
- Denial-of-service and distributed denial-of-service attacks
- Breach of access
- Password sniffing
- System infiltration
- Website defacement
- Private and public Web browser exploitsv
- Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access

Q5. Difference between Virus, Worm and Trojan Horse.

Ans. Virus: Virus is a computer program or software that connect itself to another software or computer program to harm computer system. When the computer program runs attached with virus it perform some action such as deleting a file from the computer system. Virus can't be controlled by remote.

Worms: Worms is also a computer program like virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system. Worms can be controlled by remote.

Trojan Horse: Trojan Horse does not replicate itself like virus and worms. It is a hidden piece of code which steal the important information of user. For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.

Virus	Worm	Trojan Horse
Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.
Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility software.

Q6. Explain the term internet backbone?

Ans. An Internet backbone refers to one of the principal data routes between large, strategically interconnected networks and core routers on the Internet. An Internet backbone is a very high-speed data transmission line that provides networking facilities to relatively small but high-speed Internet service providers all around the world.

Internet backbones are the largest data connections on the Internet. They require high-speed bandwidth connections and high-performance servers/routers. Backbone networks are primarily owned by commercial, educational,

government and military entities because they provide a consistent way for Internet service providers (ISPs) to keep and maintain online information in a secure manner.

Some of the largest companies running different parts of the Internet backbone include UUNET, AT&T, GTE Corp. and Sprint Nextel Corp. Their routers are connected with high-speed links and support different range options like T1, T3, OC1, OC3 or OC48.

A few key features of an Internet backbones include:

- ISPs are either connected directly to their contingency backbones or to some larger ISP that is connected to its backbone.
- The smaller networks are interlinked to support the multi versatile backup that is required to keep the Internet services intact in case of failure. This is done through transit agreements and peering processes.
- The transit agreement is a monetary contract between several larger and smaller ISPs. It is initiated to share traffic loads or to handle data traffic in case of a partial failure of some networks. In peering, several ISPs also share features and traffic burden.
- The first Internet backbone was named NSFNET. It was funded by the U.S. government and introduced by the National Science Foundation (NSF) in 1987. It was a T1 line that consisted of approximately 170 smaller networks operated at 1.544 Mbps. The backbone was a combination of fiber-optic trunk lines, each of which had several fiber-optic cables wired together to increase capacity.

Q7. Define the terms extranet and Intranet?

Ans. Extranet: An extranet is a communication network based on the internet protocol such as Transmission Control protocol and internet protocol. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as MAN, WAN or other computer networks. An extranet cannot have a single LAN, atleast it must have one connection to the external network.

Intranet: An intranet is a private network based on the internet protocol such as Transmission Control protocol and internet protocol. An intranet belongs to an organization which is only accessible by the organization's employee or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Q8. Explain data Transmission Modes?

Ans. There are three modes of transmission, namely: simplex, half duplex, and full duplex. The transmission mode defines the direction of signal flow between two connected devices.

The primary difference between three modes of transmission is that in a simplex mode of transmission the communication is unidirectional, or one-way; whereas in the half duplex mode of transmission the communication is two-directional, but the channel is interchangeably used by both of the connected devices.

On the other hand, in the full duplex mode of transmission, the communication is bi-directional or two-way, and the channel is used by both of the connected devices simultaneously.

Comparison Chart

Basis for Comparison	Simplex	Half Duplex	Full Duplex
Direction of Communication	Unidirectional	Two-directional, one at a time	Two-directional, simultaneously
Send / Receive	Sender can only send data	Sender can send and receive data, but one a time	Sender can send and receive data simultaneously
Performance	Worst performing mode of transmission	Better than Simplex	Best performing mode of transmission
Example	Keyboard and monitor	Walkie-talkie	Telephone

Simplex: In simplex transmission mode, the communication between sender and receiver occurs in only one direction. The sender can only send the data, and the receiver can only receive the data. The receiver cannot reply to the sender.

Simplex transmission can be thought of as a one-way road in which the traffic travels only in one direction—no vehicle coming from the opposite direction is allowed to drive through.

To take a keyboard / monitor relationship as an example, the keyboard can only send the input to the monitor, and the monitor can only receive the input and display it on the screen. The monitor cannot reply, or send any feedback, to the keyboard.

Half Duplex: The communication between sender and receiver occurs in both directions in half duplex transmission, but only one at a time. The sender and receiver can both send and receive the information, but only one is allowed to send at any given time. Half duplex is still considered a one-way road, in which a vehicle traveling in the opposite direction of the traffic has to wait till the road is empty before it can pass through.

For example, in walkie-talkies, the speakers at both ends can speak, but they have to speak one by one. They cannot speak simultaneously.

Full Duplex: In full duplex transmission mode, the communication between sender and receiver can occur simultaneously. The sender and receiver can both transmit and receive at the same time. Full duplex transmission mode is like a two-way road, in which traffic can flow in both directions at the same time.

For example, in a telephone conversation, two people communicate, and both are free to speak and listen at the same time.

Key Differences of the Three Transmission Modes: In simplex mode, the signal is sent in one direction. In half duplex mode, the signal is sent in both directions, but one at a time. In full duplex mode, the signal is sent in both directions at the same time.

In simplex mode, only one device can transmit the signal. In half duplex mode, both devices can transmit the signal, but one at a time. In full duplex mode, both devices can transmit the signal at the same time.

Full duplex performs better than half duplex, and half duplex in turn performs better than simplex.

Simplex: The keyboard sends the command to the monitor. The monitor cannot reply to the keyboard.

Half duplex: Using a walkie-talkie, both speakers can communicate, but they have to take turns.

Full duplex: Using a telephone, both speakers can communicate at the same time.

The full duplex transmission mode offers the best performance among the three, on account of the fact that it maximises the amount of bandwidth available.

Q9. Describe the services provided by link layer?

Ans. Data Link Layer is generally representing protocol layer in program that is simply used to handle and control the transmission of data between source and destination machines. It is simply responsible for exchange of frames among nodes or machines over physical network media. This layer is often closest and nearest to Physical Layer (Hardware).

Types of Services provided by Data Link Layer: The Data link layer generally provides or offers three types of services as given below:

(1) **Unacknowledged Connectionless Service:** Unacknowledged connectionless service simply provides datagram styles delivery without any error, issue, or flow control. In this service, source machine generally transmits independent frames to destination machine without having destination machine to acknowledge these frames.

This service is called as connectionless service because there is no connection established among sending or source machine and destination or receiving machine before data transfer or release after data transfer.

In Data Link Layer, if anyhow frame is lost due to noise, there will be no attempt made just to detect or determine loss or recovery from it. This simply means that there will be no error or flow control. An example can be Ethernet.

(2) **Acknowledged Connectionless Service:** This service simply provides acknowledged connectionless service i.e. packet delivery is simply acknowledged, with help of stop and wait for protocol.

In this service, each frame that is transmitted by Data Link Layer is simply acknowledged individually and then sender usually knows whether or not these transmitted data frames received safely. There is no logical connection established and each frame that is transmitted is acknowledged individually.

This mode simply provides means by which user of data link can just send or transfer data and request return of data at the same time. It also uses particular time period that if it has passed frame without getting acknowledgment, then it will resend data frame on time period.

This service is more reliable than unacknowledged connectionless service. This service is generally useful over several unreliable channels, like wireless systems, Wi-Fi services, etc.

(3) **Acknowledged Connection-Oriented Service:** In this type of service, connection is established first among sender and receiver or source and destination before data is transferred.

Then data is transferred or transmitted along with this established connection. In this service, each of frames that are transmitted is provided individual numbers first, so as to confirm and guarantee that each of frames is received only once that too in an appropriate order and sequence.

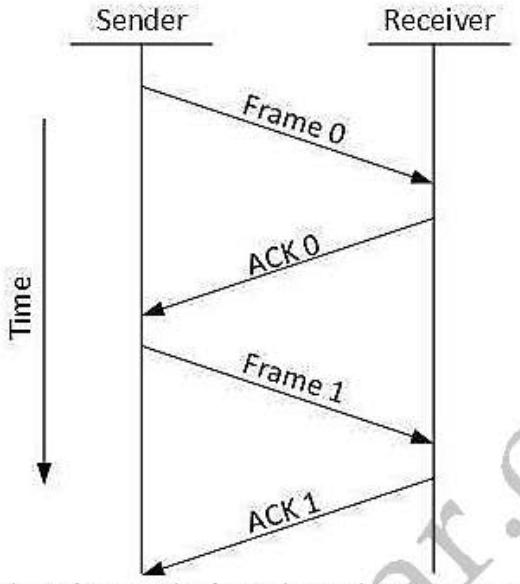
Q10. Explain the process of flow control?

Ans. When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process

and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

Stop and Wait: This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



Sliding Window: In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

MCS-218: Data Communication and Computer Networks
Guess Paper-III

Q1. Explain the services provided by Network Layer?

Ans. Network Layer: The Network Layer is the third layer of the OSI model.

It handles the service requests from the transport layer and further forwards the service request to the data link layer.

The network layer translates the logical addresses into physical addresses

It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.

The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.

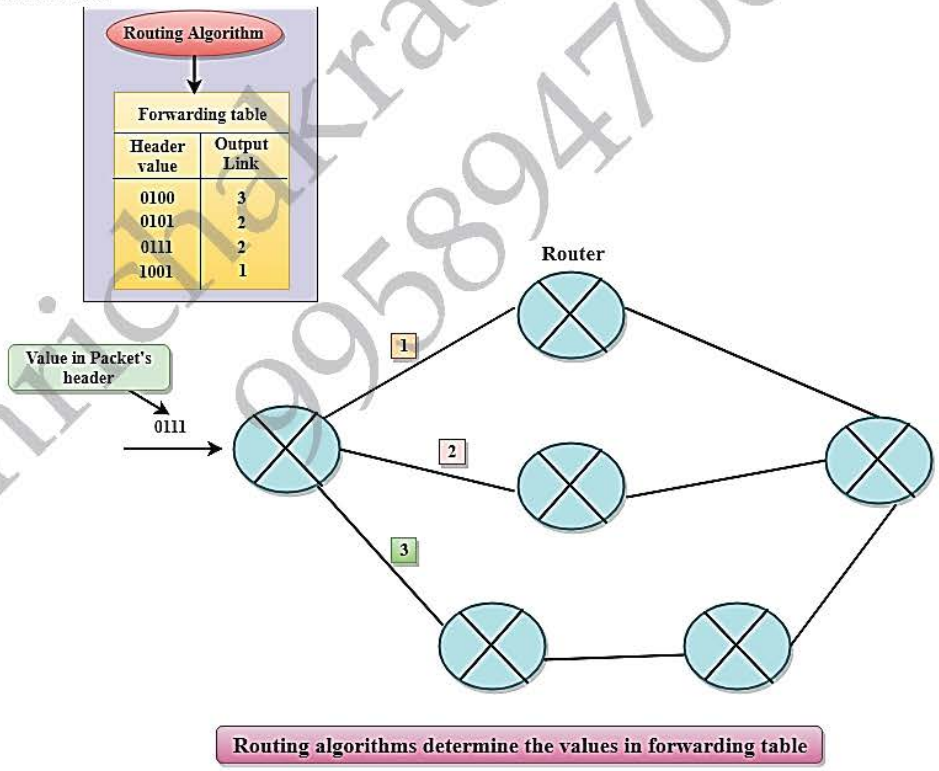
Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.

Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Forwarding & Routing: In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field and then using the header field value to index into the forwarding table. The value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

For example, the router with a header field value of 0111 arrives at a router, and then router indexes this header value into the forwarding table that determines the output link interface is 2. The router forwards the packet to the interface 2. The routing algorithm determines the values that are inserted in the forwarding table. The routing algorithm can be centralized or decentralized.



Services Provided by the Network Layer

Guaranteed delivery: This layer provides the service which guarantees that the packet will arrive at its destination.

Guaranteed delivery with bounded delay: This service guarantees that the packet will be delivered within a specified host-to-host delay bound.

In-Order packets: This service ensures that the packet arrives at the destination in the order in which they are sent.

Guaranteed max jitter: This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.

Security services: The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Q2. Explain Link state Routing?

Ans. Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Link State Routing has two phases:

Reliable Flooding

Initial state: Each node knows the cost of its neighbors.

Final state: Each node knows the entire graph.

Route Calculation: Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

Let's describe some notations:

c(i , j): Link cost from node i to node j. If i and j nodes are not directly linked, then c(i , j) = ∞.

D(v): It defines the cost of the path from source code to destination v that has the least cost currently.

P(v): It defines the previous node (neighbor of v) along with current least cost path from source to v.

N: It is the total number of nodes available in the network.

Algorithm

Initialization

N = {A} // A is a root node.

for all nodes v

if v adjacent to A

then D(v) = c(A,v)

else D(v) = infinity

loop

find w not in N such that D(w) is a minimum.

Add w to N

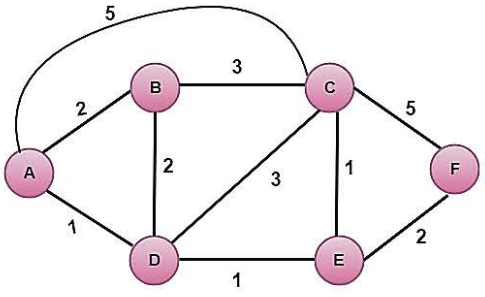
Update D(v) for all v adjacent to w and not in N:

D(v) = min(D(v) , D(w) + c(w,v))

Until all nodes in N

In the above algorithm, an initialization step is followed by the loop. The number of times the loop is executed is equal to the total number of nodes available in the network.

Let's understand through an example:



In the above figure, source vertex is A.

Step 1:

The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞

Step 2:

In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

(a) Calculating shortest path from A to B

v = B, w = D

D(B) = min(D(B) , D(D) + c(D,B))

= min(2, 1+2)>

= min(2, 3)

The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

(b) Calculating shortest path from A to C

v = C, w = D

D(B) = min(D(C) , D(D) + c(D,C))

= min(5, 1+3)

= min(5, 4)

The minimum value is 4. Therefore, the currently shortest path from A to C is 4.</p>

(c) Calculating shortest path from A to E

v = E, w = D

D(B) = min(D(E) , D(D) + c(D,E))

= min(∞, 1+1)

= min(∞, 2)

The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

Note: The vertex D has no direct link to vertex E. Therefore, the value of D(F) is infinity.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞

Step 3:

In the above table, we observe that both E and B have the least cost path in step 2. Let's consider the E vertex. Now, we determine the least cost path of remaining vertices through E.

(a) Calculating the shortest path from A to B.

v = B, w = E

D(B) = min(D(B) , D(E) + c(E,B))

= min(2 , 2+ ∞)

= min(2, ∞)

The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

(b) Calculating the shortest path from A to C.

v = C, w = E

D(B) = min(D(C) , D(E) + c(E,C))

= min(4 , 2+1)

= min(4,3)

The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

(c) Calculating the shortest path from A to F.

v = F, w = E

D(B) = min(D(F) , D(E) + c(E,F))

= min(∞ , 2+2)

= min(∞ ,4)

The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E

Step 4:

In the above table, we observe that B vertex has the least cost path in step 3. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through B.

(a) Calculating the shortest path from A to C.

v = C, w = B

D(B) = min(D(C) , D(B) + c(B,C))

= min(3 , 2+3)

= min(3,5)

The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

(b) Calculating the shortest path from A to F.

v = F, w = B

D(B) = min(D(F) , D(B) + c(B,F))

= min(4, ∞)

= min(4, ∞)

The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E

Step 5:

In the above table, we observe that C vertex has the least cost path in step 4. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through C.

a) Calculating the shortest path from A to F.

v = F, w = C

D(B) = min(D(F) , D(C) + c(C,F))

= min(4, 3+5)

= min(4,8)

The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E

Final table:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E
6	ADEBCF					

Disadvantage: Heavy traffic is created in Line state routing due to Flooding. Flooding can cause an infinite looping, this problem can be solved by using Time-to-leave field.

Q3. Define internet of things(IoT)?

Ans. The Internet of things (IoT) describes physical objects (or groups of such objects) that are embedded with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, and machine learning.

Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), independently and collectively enable the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. The IoT can also be used in healthcare systems.

Q4. What is Cryptography?

Ans. Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features of Cryptography are as follows:

- **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:** The creator/sender of information cannot deny his or her intention to send information at later stage.
- **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types of Cryptography: In general there are three types of cryptography:

- **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
- **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
- **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Q5. How does SSL or TLS work to secure TCP Connections?

Ans. When data gets send over the internet's network, it gets segmented using one of the Transport layer protocols, and most of the times it's TCP (the Transmission Control Protocol). And if you already know about TCP, it makes sure that data gets sent, with the correct sequence and to the right end host. However, the data a TCP segment encapsulates, is not secure, meaning any intruder on the network can read and understand the data part.

If you use services like ebay, Messenger and Gmail for example, and share credit card information and secure chat and whatever data that you don't want others to see. you need to have a secure connection between your computer and these services. For this need, a new and more secure version of TCP is created and called SSL (Secure Sockets Layer).

This new layer makes our data encrypted so that others can't interpret, and adds end-to-end authentication and data integrity. let's explain these one by one first:

To demonstrate the usage of SSL, let's follow this example:

Encryption: Makes data exhanged between end hosts unreadable by others.

Integrity: Makes data you send unable to be altered or chnaged on it's way to the reciever end.

Authentication: Making sure that data you send are actually sent to the right end, making it impossible for intruders to pretend being the other end.

SSL/TLS protocol makes TCP a secure protocol, and whenever an application needs to send sensitive information over the internet, it is a requirement to use the send over SSL. often times the SSL protocol is used to secure — the application network layer — HTTP protocol. however SSL can be used to secure more data protocols the relay on TCP or a connection based protocol.

if you visit a page on your browser, and at the address bar shows https://..., this means that the HTTP protocol runs over secure TCP, or SSL/TLS, this also means that all data exchanged by your browser and the visited website are encrypted and no intruder or man in the middle can manipulate. this feels safe, doesn't it.

The phases of an SSL connection: Here we have a simplified view of how SSL/TLS actually works to secure a TCP connection. an ssl connection runs over 3 phases; the handshake, key exchange and the actual data transfer. let's take an example of a secure connection happening between a Client and a Server.

Beforehand, The SSL Certificate

A servier needs firest to aquire a valid SSL Certificate with a public key signed by a Certificate Authority (CA), this certificate is sent to any party wanting to connect to this server over SSL, and then that party checks with the CA weather this server is the real server that it needs to connect to. This is called Authenticating the server.

Phase 1: The handshake

- The client makes a typical TCP connection to the server, by:
- sending a SYN packet
- recieving a SYN/ACK packet from the server
- and finally sending an ACK packet to the server.

Phase 2: Exchanging keys

- Then, after a TCP connection has established, comes the SSL part:
- the client sends a hello to the server
- the server sends back the singed certificate with the public key. it doesn't send it's private key.
- the client checks the certificate wheather it's valid.
- and if the certificate looks valid, the client generates it's own private key, encrypts it with the server's public key, and sends this all back to the server.
- the server unlooks the data with it's own private key, gets the client private key.
- the server uses the client's private key to unlook the data part of the packets send by the client.

Phase 3: Data Transfer

- Once a TCP connection is established, and the two parties able to encrypt and decrypt all transmitted data. The same proccess in last two steps in the second phase are repeated to send all segmented data over the created TCP connection using TCP segments.

These 3 phases mentioned above are just for demonstration and making things clear in the simplist way possible. However, a real SSL connection is way more complicated and has to handle data integrity with even an additional set of keys. This SSL/TLS protocol is updated with new encyption methods and to fix all security flaws that may arise.

Q6. What are cyber-attacks?

Ans. A cyber attack is an attempt to disable computers, steal data, or use a breached computer system to launch additional attacks. Cybercriminals use different methods to launch a cyber attack that includes malware, phishing, ransomware, man-in-the-middle attack, or other methods.

Types of Cyber Attacks

Malware: Malware is a term that describes malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

Phishing: Phishing is the method of sending fraudulent communications that seems to come from a reputable source, usually through email. The goal is to steal or get sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat.

Man-in-the-middle attack: Man-in-the-middle (MitM) attacks, also called eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks: On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.

Once malware has breached a device; an attacker can install software to process all of the victim's information.

Denial-of-service attack A denial-of-service attack fills systems, servers, or networks with traffic that exhaust resources and bandwidth. That makes the system incapable to fulfill legitimate requests. Attackers also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

SQL injection: A Structured Query Language (SQL) injection happens when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Zero-day exploit: A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

DNS Tunneling: DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS. There are various, legitimate reasons to utilize DNS tunneling. However, there are also malicious reasons to use DNS Tunneling VPN services. They can be used to disguise outbound traffic as

DNS, concealing data that is typically shared through an internet connection. For malicious use, DNS requests are manipulated to exfiltrate data from a compromised system to the attacker's infrastructure. It can also be used for command and control callbacks from the attacker's infrastructure to a compromised system.

Q7. What are the different Types of Viruses?

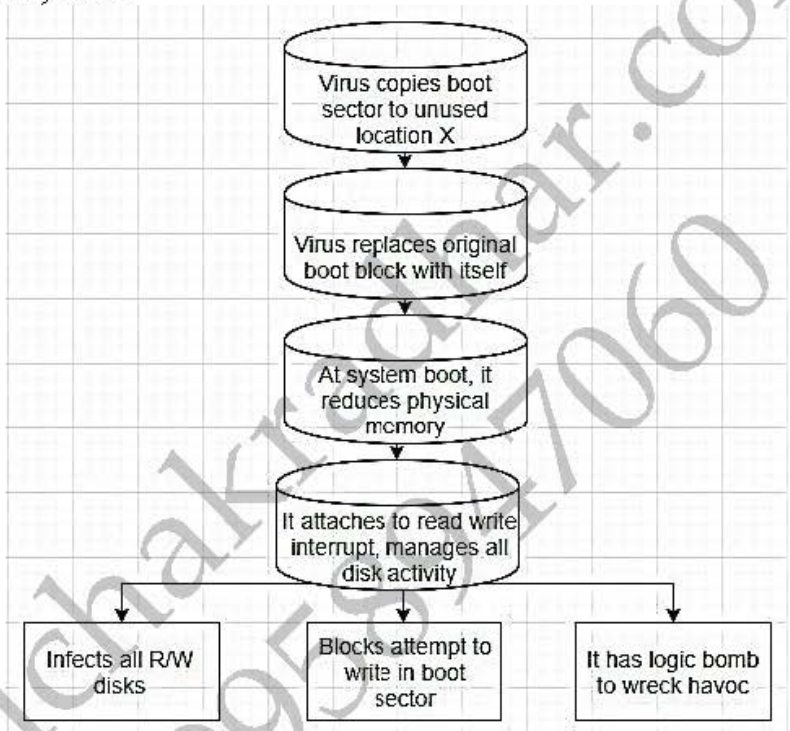
Ans. A virus is a fragment of code embedded in a legitimate program. Viruses are self-replicating and are designed to infect other programs. They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunctions. On reaching the target machine a virus dropper(usually a trojan horse) inserts the virus into the system.

For more details, refer to this.

Various types of viruses:

File Virus: This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a Parasitic virus because it leaves no file intact but also leaves the host functional.

Boot sector Virus: It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as memory viruses as they do not infect the file systems.



Macro Virus: Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

Source code Virus: It looks for source code and modifies it to include virus and to help spread it.

Polymorphic Virus: A virus signature is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

Encrypted Virus: In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

Stealth Virus: It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of viruses becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

Tunneling Virus: This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

Multipartite Virus: This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

Armored Virus: An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

Browser Hijacker: As the name suggests this virus is coded to target the user's browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.

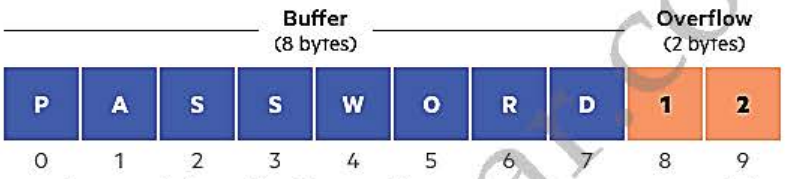
Resident Virus: Resident viruses installation store for your RAM and meddle together along with your device operations. They're so sneaky that they could even connect themselves for your anti-virus software program files.

Q8. What is Buffer Overflow?

Ans. Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.



Types of Buffer Overflow Attacks: Stack-based buffer overflows are more common, and leverage stack memory that only exists during the execution time of a function.

Heap-based attacks are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

How to Prevent Buffer Overflows: Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection.

In addition, modern operating systems have runtime protection. Three common protections are:

Address space randomization (ASLR)—randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.

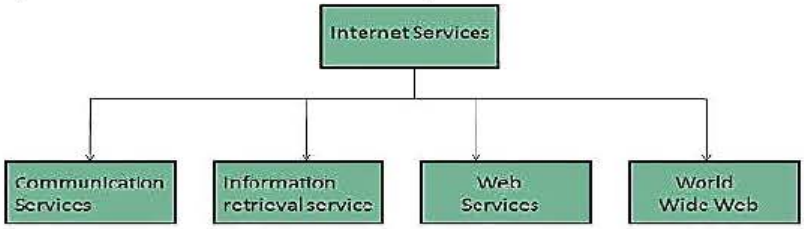
Data execution prevention—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.

Structured exception handler overwrite protection (SEHOP)—helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

Security measures in code and operating system protection are not enough. When an organization discovers a buffer overflow vulnerability, it must react quickly to patch the affected software and make sure that users of the software can access the patch.

Q9. Describe the internet services?

Ans. Internet Services allows us to access huge amount of information such as text, graphics, sound and software over the internet. Following diagram shows the four different categories of Internet Services.



Communication Services: There are various Communication Services available that offer exchange of information with individuals or groups. The following table gives a brief introduction to these services:

S.N.	Service Description
1	Electronic Mail Used to send electronic message over the internet.

2	Telnet Used to log on to a remote computer that is attached to internet.
3	Newsgroup Offers a forum for people to discuss topics of common interests.
4	Internet Relay Chat (IRC) Allows the people from all over the world to communicate in real time.
5	Mailing Lists Used to organize group of internet users to share common information through e-mail.
6	Internet Telephony (VoIP) Allows the internet users to talk across internet to any PC equipped to receive the call.
7	Instant Messaging Offers real time chat between individuals and group of people. Eg. Yahoo messenger, MSN messenger.

Information Retrieval Services: There exist several Information retrieval services offering easy access to information present on the internet. The following table gives a brief introduction to these services:

S.N.	Service Description
1	File Transfer Protocol (FTP) Enable the users to transfer files.
2	Archie It's updated database of public FTP sites and their content. It helps to search a file by its name.
3	Gopher Used to search, retrieve, and display documents on remote sites.
4	Very Easy Rodent Oriented Netwide Index to Computer Achieved (VERONICA) VERONICA is gopher based resource. It allows access to the information resource stored on gopher's servers.

Web Services: Web services allow exchange of information between applications on the web. Using web services, applications can easily interact with each other.

The web services are offered using concept of Utility Computing.

World Wide Web (WWW)

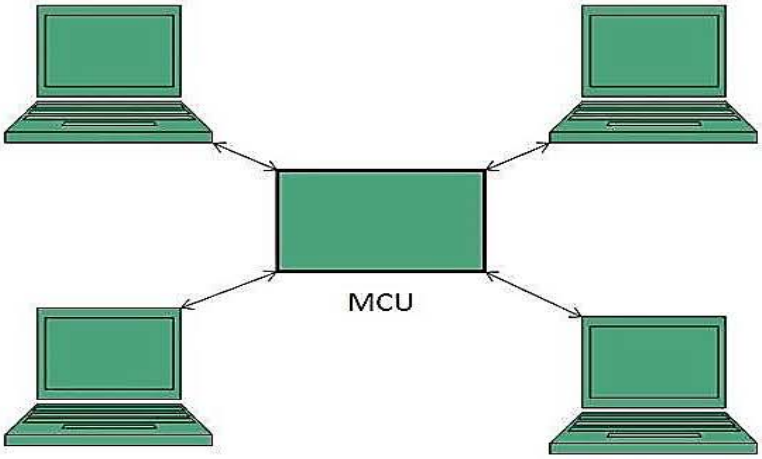
WWW is also known as W3. It offers a way to access documents spread over the several servers over the internet. These documents may contain texts, graphics, audio, video, hyperlinks. The hyperlinks allow the users to navigate between the documents.

Video Conferencing: Video conferencing or Video teleconferencing is a method of communicating by two-way video and audio transmission with help of telecommunication technologies.

Modes of Video Conferencing:

Point-to-Point: This mode of conferencing connects two locations only.

Multi-Point: This mode of conferencing connects more than two locations through Multi-point Control Unit (MCU).



Q10. Define the terms channel, baud, bandwidth and frequency?

Ans. Channel: A communication channel refers either to a physical transmission medium such as a wire, or to a logical connection over a multiplexed medium such as a radio channel in telecommunications and computer networking. A channel is used to convey an information signal, for example a digital bit stream, from one or several senders (or transmitters) to one or several receivers. A channel has a certain capacity for transmitting information, often measured by its bandwidth in Hz or its data rate in bits per second.

Baud: The baud rate is the rate at which information is transferred in a communication channel. Baud rate is commonly used when discussing electronics that use serial communication. In the serial port context, "9600 baud" means that the serial port is capable of transferring a maximum of 9600 bits per second.

Bandwidth: Bandwidth is measured as the amount of data that can be transferred from one point to another within a network in a specific amount of time. Typically, bandwidth is expressed as a bitrate and measured in bits per second (bps).

Bandwidth was originally measured in bits per second and expressed as bps.

However, today's networks typically have much higher bandwidth than can be comfortably expressed by using such small units.

Now it is common to see higher numbers that are denoted with metric prefixes, such as Mbps, (megabits per second), Gbps (gigabits per second), or Tbps (terabits per second).

K: kilo = 1,000 bits.

M: mega = 1,000 kilo = 1,000,000 bits.

G: giga = 1,000 mega = 1,000,000,000 bits.

T: tera = 1,000 giga = 1,000,000,000,000 bits.

Frequency: Frequency is a measure of the number of cycles that are done per unit of time and is generally measured in hertz (cycles per second). Data cabling is normally rated in kilohertz (kHz) or megahertz (MHz).