Printed Pages:02 **Sub Code: KCA303**

Paper Id: **Roll No.**

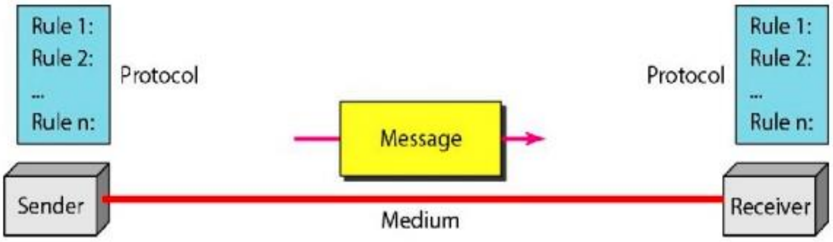
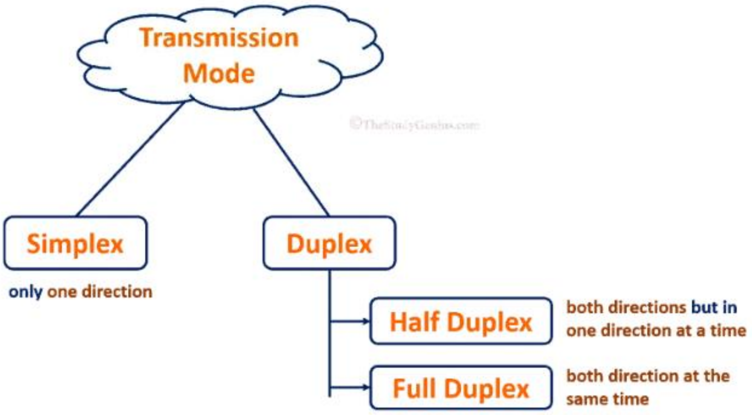
B. Tech.
(SEM III) THEORY EXAMINATION 2022-23
COMPUTER NETWORKS

Time: 3 Hours ***Total Marks: 100***

Note: Attempt all Sections. If you require any missing data, then choose suitably.

SECTION A

1. Attempt *all* questions in brief. **2*10 = 20**

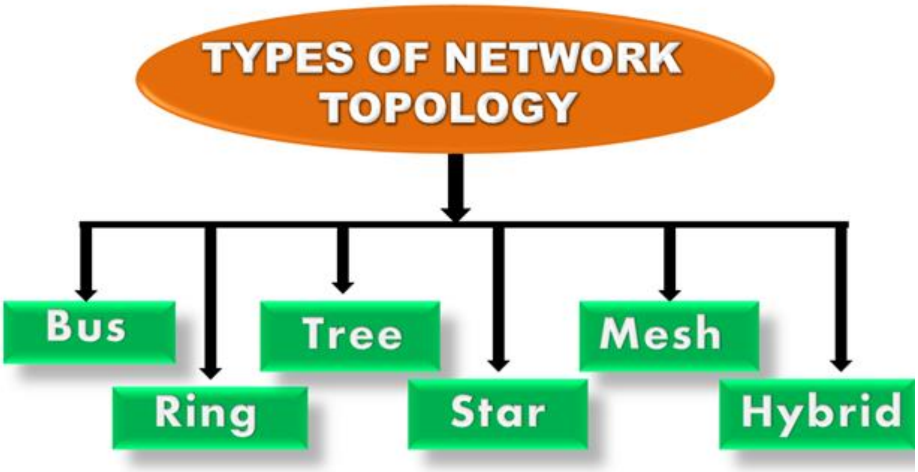
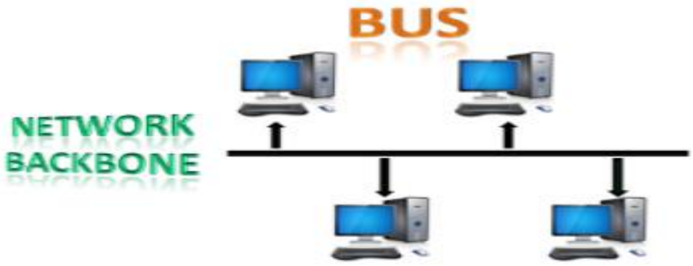
Qno	Questions	CO
(a)	**Question:** List out components of data communication system. **Answer:** The components of data communication system are as follows: 1. Data 2. Sender 3. Receiver 4. Transmission Medium 5. Protocol  Rule 1: Rule 2: ... Rule n: Protocol Protocol Rule 1: Rule 2: ... Rule n: Message Sender Medium Receiver	1
(b)	**Question:** Discuss various transmission modes. **Answer:** Various transmission modes are as follows:  Transmission Mode ©TheStudyGenius.com Simplex only one direction Duplex Half Duplex both directions but in one direction at a time Full Duplex both direction at the same time	1
(c)	**Question:** Discover how many times a packet has to visit the network layer and data link layer during a transmission from S to D? Assume that Source S and Destination D are connected through an intermediate router R. **Answer:** Network layer-3 times and Data link layer - 4 times	
(d)	**Question:** Discuss CSMA/CD. **Answer:** Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates	

	in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free. The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.	
(e)	**Question:** Discuss Dynamic Host Configuration Protocol(DHCP). **Answer:** Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network. DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.	
(f)	**Question:** Explain Round-Trip Time (RTT). **Answer:** Round-trip time (RTT) is the duration, measured in milliseconds, from when a browser sends a request to when it receives a response from a server. It's a key performance metric for web applications and one of the main factors, along with Time to First Byte (TTFB), when measuring page load time and network latency.	
(g)	**Question:** Describe sockets with respect to communication system. **Answer:** A socket is one endpoint of a two-way communication link between two programs running on the network. A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to. An endpoint is a combination of an IP address and a port number	
(h)	**Question:** What is three-way handshaking? **Answer:** Transmission Control Protocol (TCP) provides a secure and reliable connection between two devices using the 3-way handshake process. TCP uses the full-duplex connection to synchronize (SYN) and acknowledge (ACK) each other on both sides. There are three steps for both establishing and closing a connection. They are − SYN, SYN-ACK, and ACK. ➢ **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with ➢ **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received, and SYN signifies with what sequence number it is likely to start the segments with ➢ **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.	
(i)	**Question:** Discuss role of SMTP in email communication system. **Answer:** SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After	

	successfully establishing a TCP connection the client process sends the mail instantly.	
(j)	**Question:** Define cookies with respect to computer networks. **Answer:** A cookie is a piece of data from a website that is stored within a web browser that the website can retrieve at a later time. Cookies are used to tell the server that users have returned to a particular website.	

SECTION B

2. Attempt any *three* of the following: 10*3 = 30

Qno	Questions	CO
(a)	**Question:** Discuss various computer network topologies with suitable diagrams. **Answer:** Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topologies: physical and logical topology. **Types of Network Topology:** Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.  TYPES OF NETWORK TOPOLOGY Bus Tree Mesh Ring Star Hybrid 1) 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.	1

- 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:

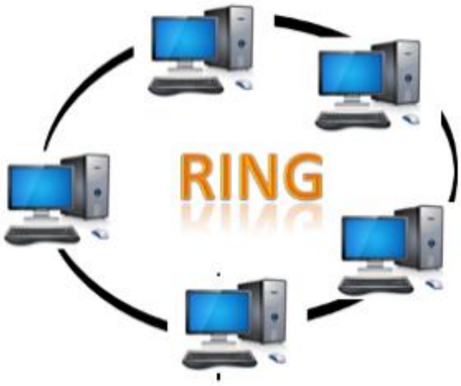
- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar 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.

2) 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:

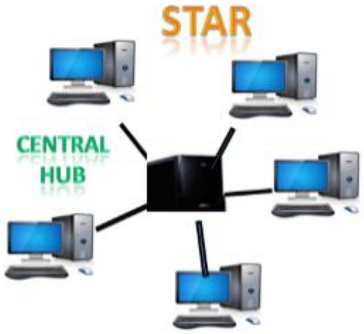
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.

- **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.

3) 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

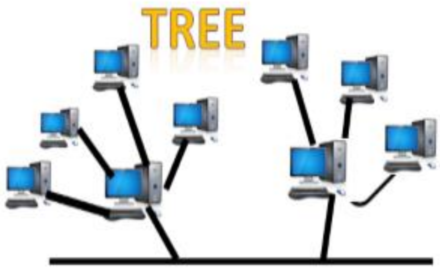
- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator 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.

4) 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

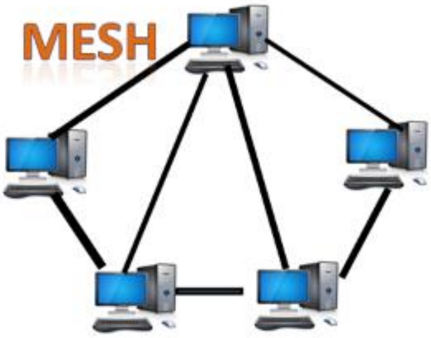
- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.

- **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.

5) Mesh topology

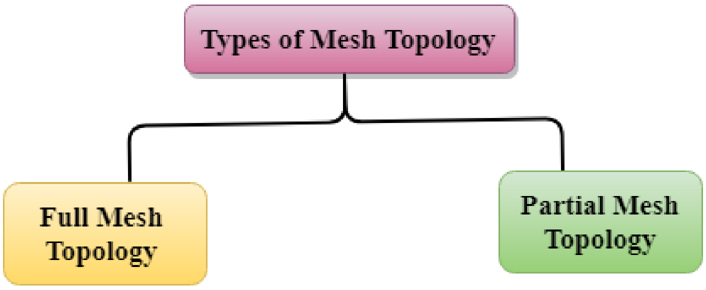


- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point 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.

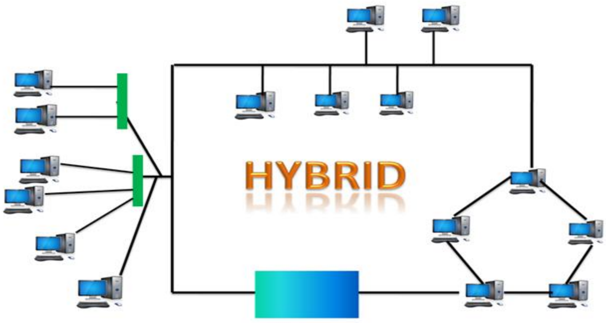
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

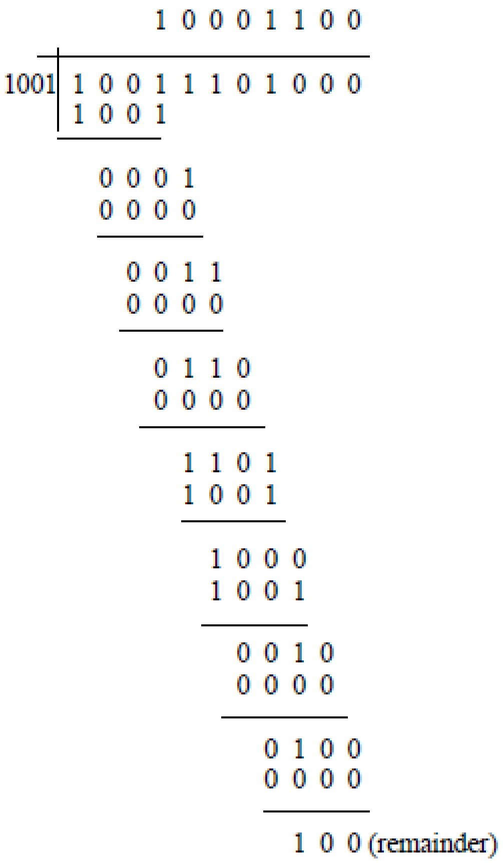
- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication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

6) Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.

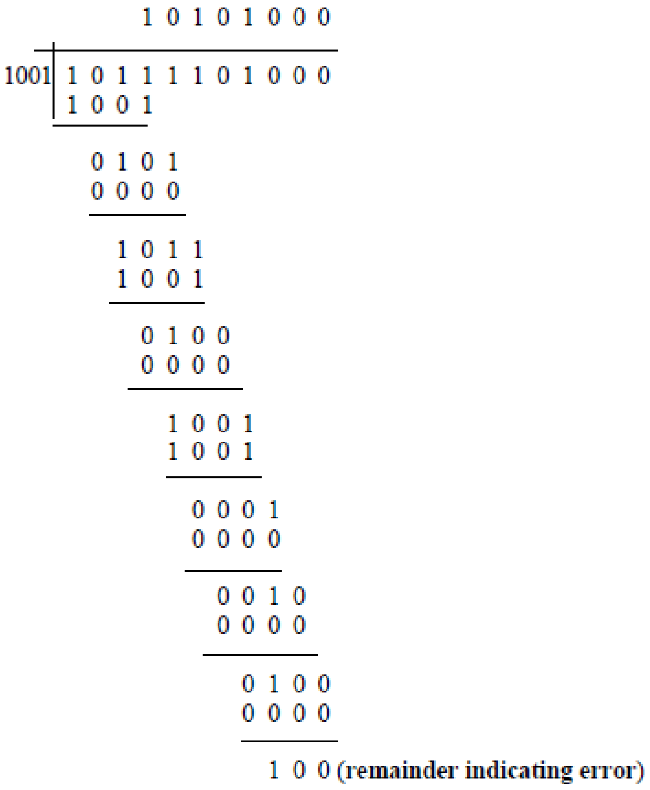
	○ A Hybrid topology is a connection between different links and nodes to transfer the data. ○ When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist 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 a. **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network. b. **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network. c. **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization. d. **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.	
(b)	**Question:** A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is x^3 + 1. Show the actual bit string transmitted. Suppose the third bit from the left is inverted during transmission. Show that this error is detected at the receiver's end. **Answer:** Our generator G(x) = $x^3 + 1$ encoded as 1001. Because the generator polynomial is of the degree three, we append three zeros to the lower end of the frame to be transmitted. Hence after appending the 3 zeros the bit stream is **10011101000**. On dividing the message by generator after appending three zeros to the frame we get a remainder of 100. We do modulo 2 subtractions thereafter of the remainder from the bit stream with the three zeros appended. **The actual frame transmitted is 10011101100**. See below.	2



```
              1 0 0 0 1 1 0 0
          _______________________
    1001 | 1 0 0 1 1 1 0 1 0 0 0
         | 1 0 0 1
           -------
             0 0 0 1
             0 0 0 0
             -------
               0 0 1 1
               0 0 0 0
               -------
                 0 1 1 0
                 0 0 0 0
                 -------
                   1 1 0 1
                   1 0 0 1
                   -------
                     1 0 0 0
                     1 0 0 1
                     -------
                       0 0 1 0
                       0 0 0 0
                       -------
                         0 1 0 0
                         0 0 0 0
                         -------
                           1 0 0 (remainder)
```

Actual frame transmitted: 10011101000 – 100 = 10011101100 (modulo 2 subtraction)

Now suppose the third bit from the left is garbled and the frame is received as 10111101100. Hence on dividing this by the polynomial generator we get a remainder of 100 which shows that an error has occurred. Had the received frame been error free we would have got a remainder of zero. See below.



```
              1 0 1 0 1 0 0 0
          _______________________
    1001 | 1 0 1 1 1 1 0 1 0 0 0
         | 1 0 0 1
           -------
             0 1 0 1
             0 0 0 0
             -------
               1 0 1 1
               1 0 0 1
               -------
                 0 1 0 0
                 0 0 0 0
                 -------
                   1 0 0 1
                   1 0 0 1
                   -------
                     0 0 0 1
                     0 0 0 0
                     -------
                       0 0 1 0
                       0 0 0 0
                       -------
                         0 1 0 0
                         0 0 0 0
                         -------
                           1 0 0 (remainder indicating error)
```

(c)	**Question:** Consider an IP address 196.10.19.10 /26. Solve the following: a. Network Address	3

b. Custom subnet mask
c. Total Number of available subnets
d. Total number of host addresses
e. Subnet address and broadcast address of every subnet.

Answer: The solution is as follows:

a. 196.10.19.0
b. 255.255.255.192
c. 64

(d) **Question:** Justify the statement "TCP is reliable than UDP". Also elaborate format for TCP packet. 4

Answer: The TCP stands for Transmission Control Protocol. If we want the communication between two computers and communication should be good and reliable. For example, we want to view a web page, then we expect that nothing should be missing on the page, or we want to download a file, then we require a complete file, i.e., nothing should be missing either it could be a text or an image. This can only be possible due to the TCP. It is one of the most widely used protocols over the TCP/IP network.

- TCP is Reliable as it provides reliability of delivery of packets to the receiver while UDP is non-reliable and does not give information about the packets.
- TCP is Connection oriented it means connection is to be setup before data is sent that is done in form of 3-way handshake while UDP is Connectionless.
- TCP provides flow control and error control characteristics while UDP doesn't provide it.
- TCP gives guarantee that a packet will reach on the destination without any duplication and the order of data will also be same.

Services offered by TCP are:

- Process-to-Process communication
- Stream delivery Service
- Full-Duplex Communication
- Connection-oriented Service
- Reliable Service

(e) **Question:** Write short notes on any two: 5

1. Domain Name Systems:
2. Telnet
3. FTP

Answer: The short notes are as follows:

1. **Domain Name Systems:** An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

DNS stands for Domain Name System: DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address. DNS is required for the functioning of the internet.
Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots. DNS is a service that translates the domain name into IP addresses. This allows the users of networks to

utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address. DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

- Generic Domains: It defines the registered hosts according to their generic behavior. Each node in a tree defines the domain name, which is an index to the DNS database. It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations.
edu	educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations

- **Country Domain :** The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three-character organizational abbreviations.

Label	Description
au	Australia
in	India
cl	Chile
fr	France
us	United States
za	South Africa
uk	United Kingdom
jp	Japan

- Inverse Domain: The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS: DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client. Client requests contain a name which is converted into an IP address known as a forward DNS lookup while requests containing an IP address which is converted into a name known as reverse DNS lookups. DNS implements a distributed database to store the name of all the hosts available on the internet. If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

2. **Telnet:** The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand. The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for Terminal Network. Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

There are two types of logins:

- **Local Login:** When a user logs into a local computer, then it is known as local login. When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program. However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters has special meanings such as control character with "z" means suspend. Such situations do not create any problem as the terminal driver knows the meaning of such characters. But it can cause the problems in remote login.
- **Remote login:** When the user wants to access an application program on a remote computer, then the user must perform remote login.

Remote login occurs Process:

- **At the local site:** The user sends the keystrokes to the terminal driver; the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack.
- **At the remote site:** The commands in NVT forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore, it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

3. **File transfer protocol (FTP):** FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another. It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet. It is also used for downloading the files to computer from other servers. Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

There are two types of connections in FTP:

- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

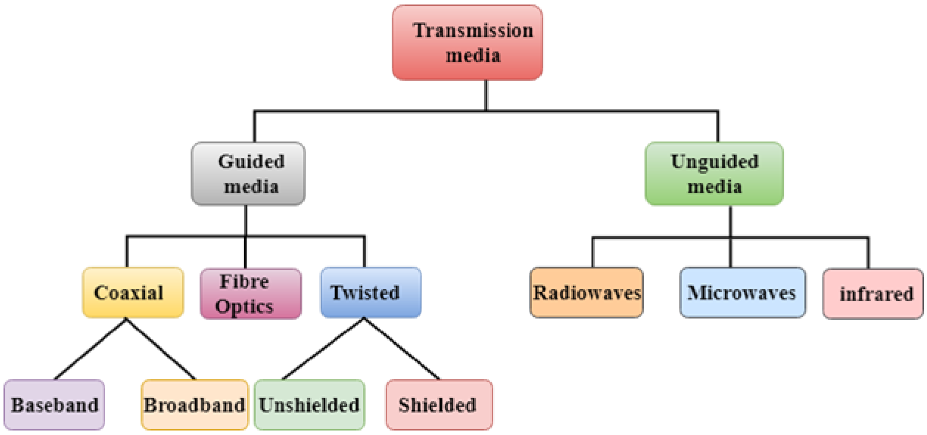
Advantages of FTP:

- Speed: One of the biggest advantages of FTP is speed. The FTP is one of the fastest ways to transfer the files from one computer to another computer.
- Efficient: It is more efficient as we do not need to complete all the operations to get the entire file.

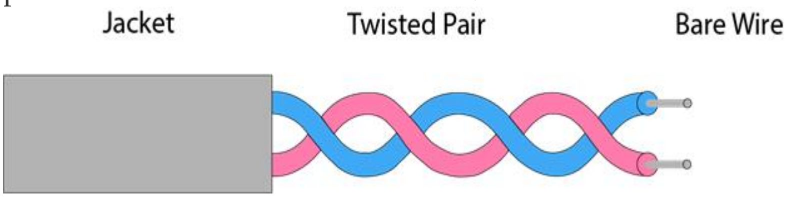
	➢ Security: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure. ➢ Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server. **Disadvantages of FTP:** ➢ The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption. ➢ FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers. ➢ Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password. ➢ It is not compatible with every system.	

SECTION C

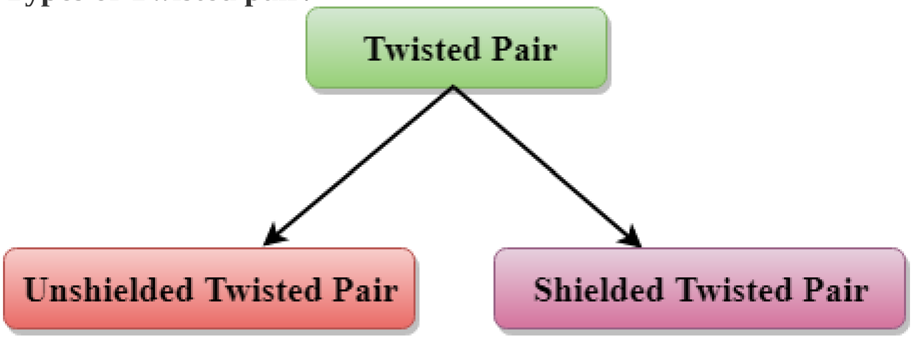
3. Attempt any *one* part of the following: 10*1 = 10

Qno	Questions	CO
(a)	**Question:** Discuss various types of transmission media with their applications areas. **Answer:** Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals. Classification of Transmission Media:  Transmission media Guided media Unguided media Coaxial Fibre Optics Twisted Radiowaves Microwaves infrared Baseband Broadband Unshielded Shielded **Guided Media:** It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media. **Twisted pair:** Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a	1

lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz. A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



Unshielded Twisted Pair: An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair: A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

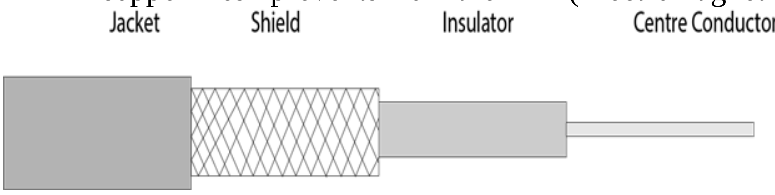
Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.

- ✓ The name of the cable is coaxial as it contains two conductors parallel to each other.
- ✓ It has a higher frequency as compared to Twisted pair cable.
- ✓ The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- ✓ The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

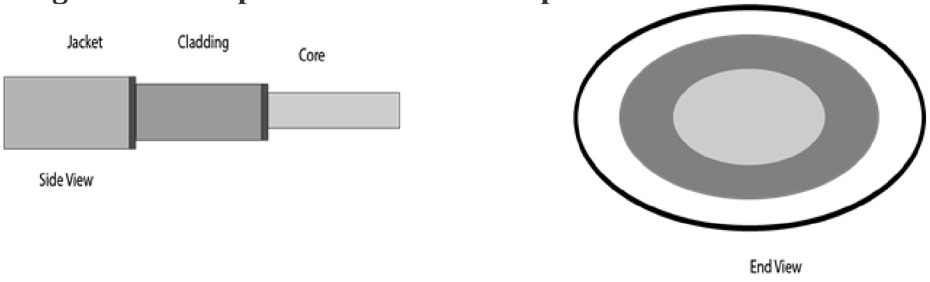
Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

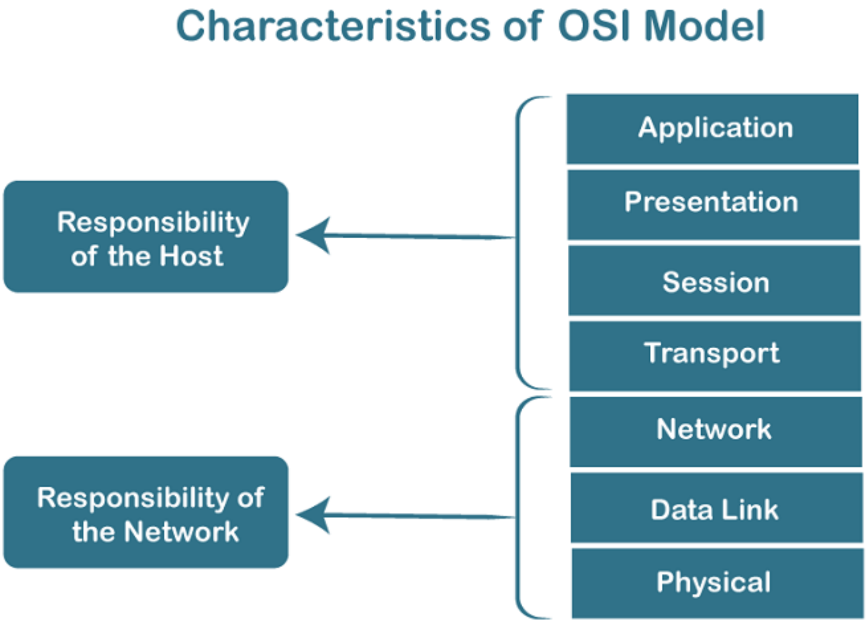
- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:



Basic elements of Fibre optic cable:

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

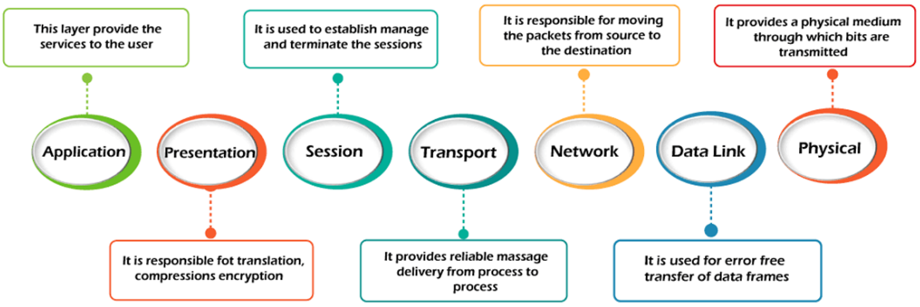
	○ **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection. **Following are the advantages of fibre optic cable over copper:** ○ **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable. ○ **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed. ○ **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable. ○ **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable. ○ **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.	
(b)	**Question:** Explain responsibilities each layer in ISO/OSI Model with suitable diagrams. **Answer:** OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer. OSI consists of seven layers, and each layer performs a particular network function. It was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications. It divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task. Each layer is self-contained, so that task assigned to each layer can be performed independently. **Characteristics of OSI Model:**  Characteristics of OSI Model Responsibility of the Host Responsibility of the Network Application Presentation Session Transport Network Data Link Physical ○ The OSI model is divided into two layers: upper layers and lower layers.	1

- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

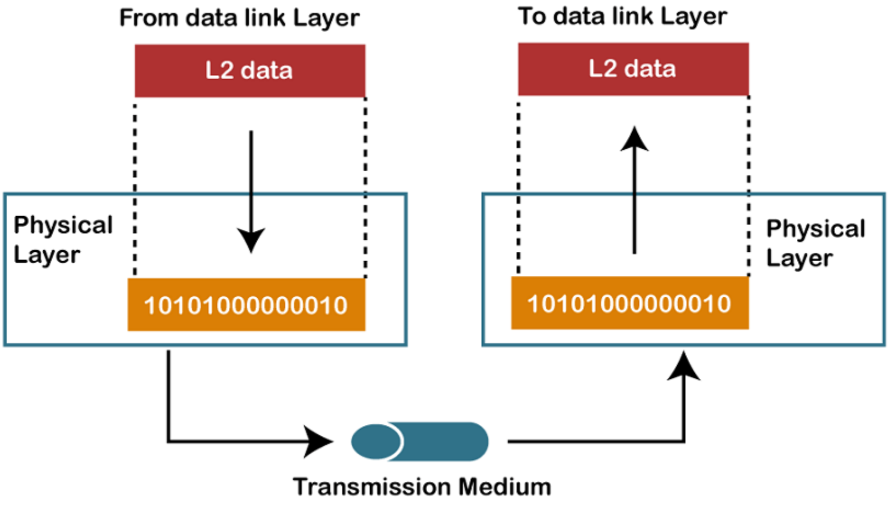
7 Layers of OSI Model

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

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


This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames

1) Physical layer



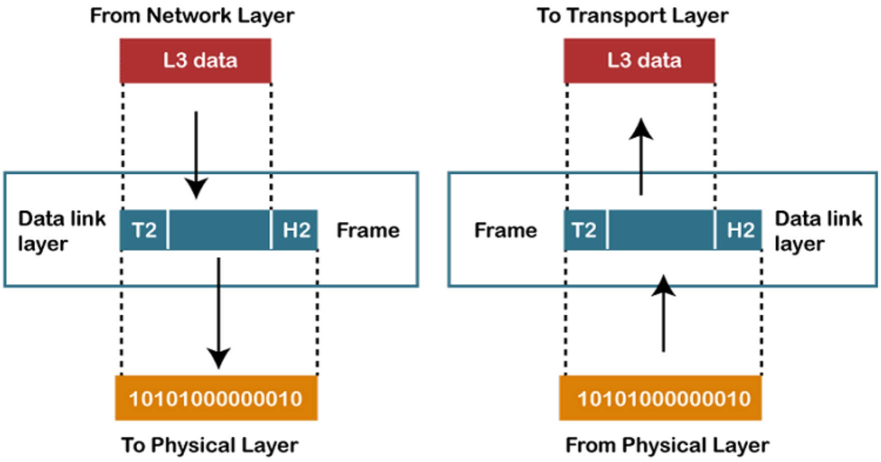
- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- Line Configuration: It defines the way how two or more devices can be connected physically.

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

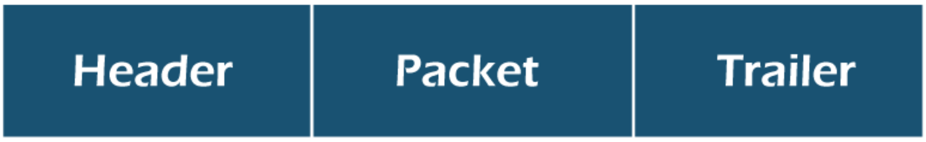
2) Data-Link Layer



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
  - Logical Link Control Layer
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  - Media Access Control Layer
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the Data-link layer

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

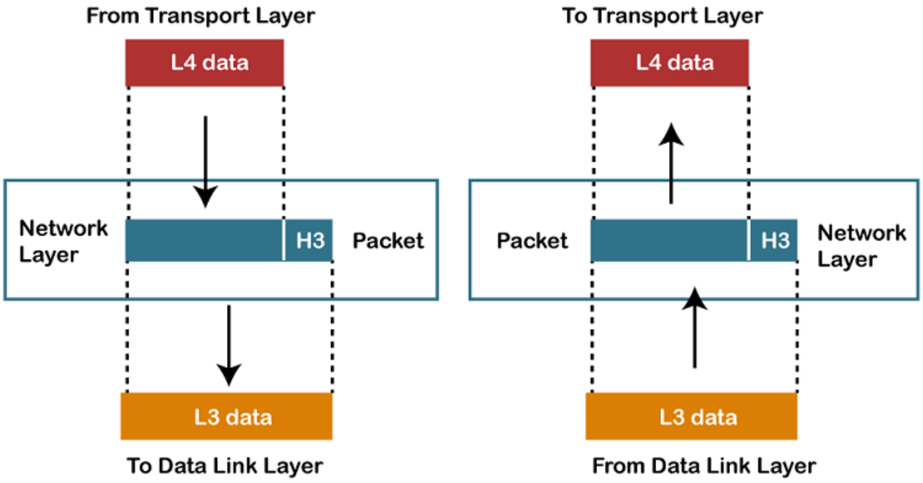


- Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is

maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

- Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3) Network Layer

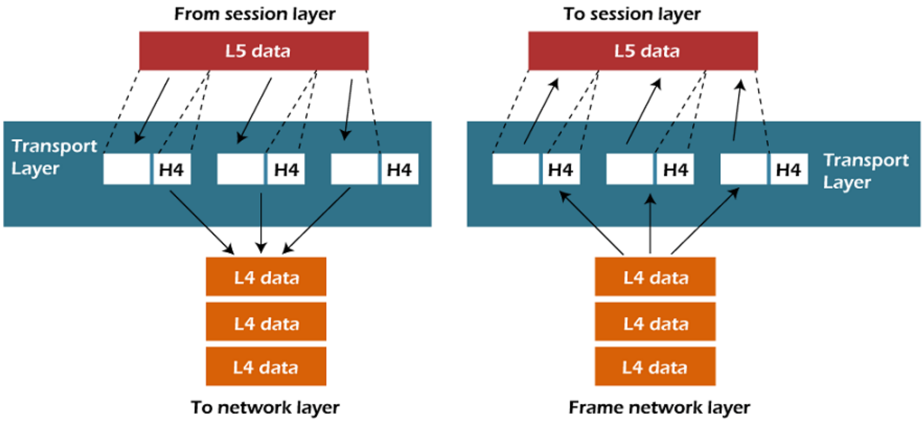


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and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

Functions of Network Layer:

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

4) Transport Layer



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

The two protocols used in this layer are:

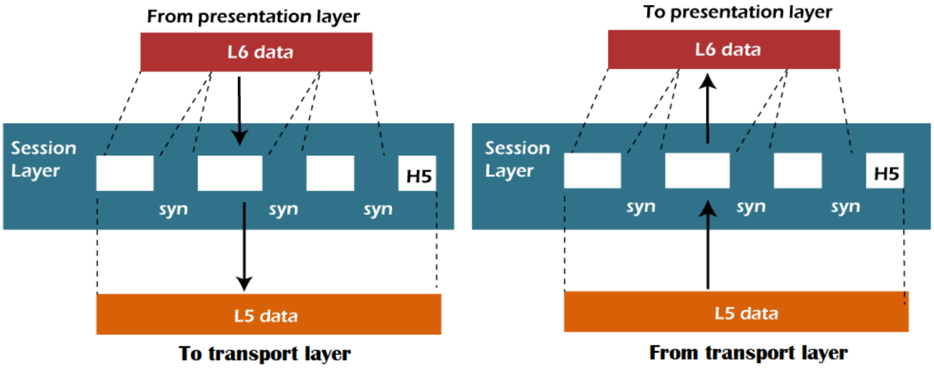
- Transmission Control Protocol
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- User Datagram Protocol
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- Service-point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- Flow control: The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer

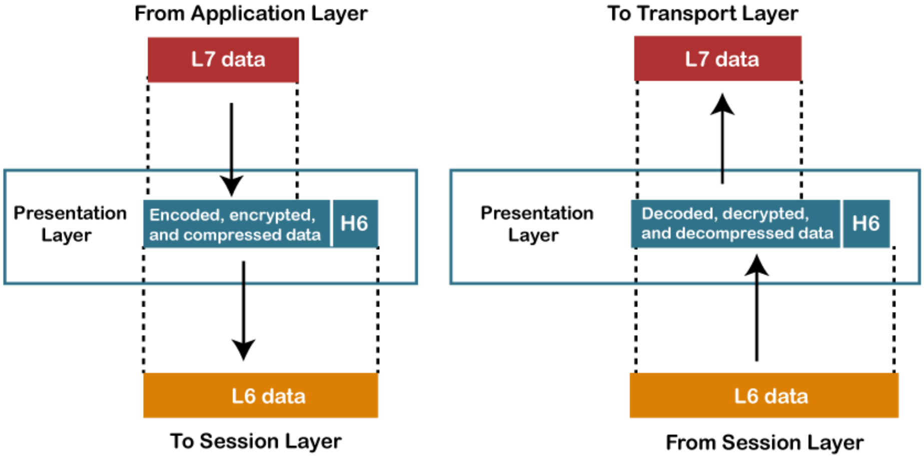


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes, or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6) Presentation Layer



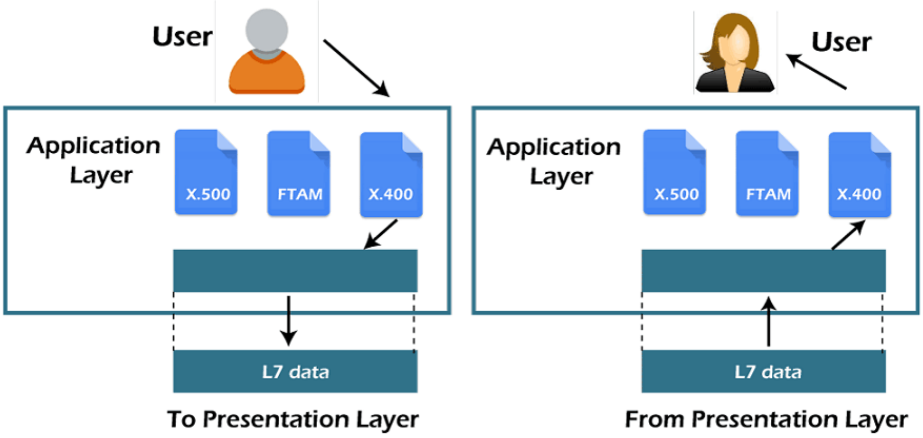
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.

- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

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

7) Application Layer



An application layer serves as a window for users and application processes to access network service.

It handles issues such as network transparency, resource allocation, etc.

An application layer is not an application, but it performs the application layer functions.

This layer provides the network services to the end-users.

Functions of Application layer:

File transfer, access, and management (FTAM): An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

Mail services: An application layer provides the facility for email forwarding and storage.

Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

4. Attempt any *one* part of the following: 10 *1 = 10

Qno	Questions	CO
(a)	**Question:** Explain Selective Reject and Go-Back-N-ARQ with reference to sliding window protocol. **Answer:** Both Go-Back-N Protocol and Selective Repeat Protocol are the types of sliding window protocols. The main difference between these two protocols is that after finding the suspect or damage in sent	2

frames go-back-n protocol re-transmits all the frames whereas selective repeat protocol re-transmits only that frame which is damaged.

Go-Back-N Protocol:

The Go-Back-N protocol is a sliding window protocol used for reliable data transfer in computer networks. It is a sender-based protocol that allows the sender to transmit multiple packets without waiting for an acknowledgement for each packet. The receiver sends a cumulative acknowledgement for a sequence of packets, indicating the last correctly received packet. If any packet is lost, the receiver sends a negative acknowledgement (NACK) for the lost packet, and the sender retransmits all the packets in the window starting from the lost packet. The sender also maintains a timer for each packet, and if an acknowledgement is not received within the timer's timeout period, the sender retransmits all packets in the window.

The key features of the Go-Back-N (GBN) protocol include:

- Sliding window mechanism
- Sequence numbers
- Cumulative acknowledgements
- Timeout mechanism
- NACK mechanism
- Simple implementation.

Selective Repeat Protocol:

The Selective Repeat protocol is another sliding window protocol used for reliable data transfer in computer networks. It is a receiver-based protocol that allows the receiver to acknowledge each packet individually, rather than a cumulative acknowledgement of a sequence of packets. The sender sends packets in a window and waits for acknowledgements for each packet in the window. If a packet is lost, the receiver sends a NACK for the lost packet, and the sender retransmits only that packet. The sender also maintains a timer for each packet, and if an acknowledgement is not received within the timer's timeout period, the sender retransmits only that packet.

key features include:

- Receiver-based protocol
- Each packet is individually acknowledged by the receiver.
- Only lost packets are retransmitted, reducing network congestion.
- Maintains a buffer to store out-of-order packets.
- Requires more memory and processing power than Go-Back-N
- Provides efficient transmission of packets.

Similarities between the two protocols are:

- Both protocols use a sliding window mechanism to allow the sender to transmit multiple packets without waiting for an acknowledgement for each packet.
- Both protocols use sequence numbers to ensure the correct order of packets.
- Both protocols use a timer mechanism to handle lost or corrupted packets.
- Both protocols can retransmit packets that are not acknowledged by the receiver.
- Both protocols can reduce network congestion by only retransmitting lost packets.

- Both protocols are widely used in modern communication networks.

Now, we shall see the difference between them:

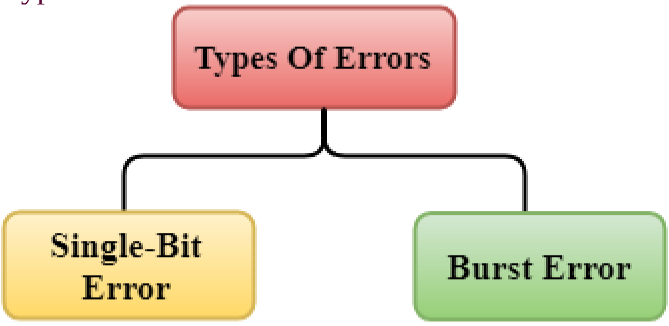
S.NO	Go-Back-N Protocol	Selective Repeat Protocol
1.	In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.	In selective Repeat protocol, only those frames are re-transmitted which are found suspected.
2.	Sender window size of Go-Back-N Protocol is N.	Sender window size of selective Repeat protocol is also N.
3.	Receiver window size of Go-Back-N Protocol is 1.	Receiver window size of selective Repeat protocol is N.
4.	Go-Back-N Protocol is less complex.	Selective Repeat protocol is more complex.
5.	In Go-Back-N Protocol, neither sender nor at receiver need sorting.	In selective Repeat protocol, receiver side needs sorting to sort the frames.
6.	In Go-Back-N Protocol, type of Acknowledgement is cumulative.	In selective Repeat protocol, type of Acknowledgement is individual.
7.	In Go-Back-N Protocol, Out-of-Order packets are NOT Accepted (discarded) and the entire window is re-transmitted.	In selective Repeat protocol, Out-of-Order packets are Accepted.
8.	In Go-Back-N Protocol, if Receives a corrupt packet, then also, the entire window is re-transmitted.	In selective Repeat protocol, if receives a corrupt packet, it immediately sends a negative acknowledgement and hence only the selective packet is retransmitted.
9.	Efficiency of Go-Back-N Protocol is N/(1+2*a)	Efficiency of selective Repeat protocol is N/(1+2*a)

(b)

Question: What do you mean error handling at data link layer. Discuss hamming code with suitable example.

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

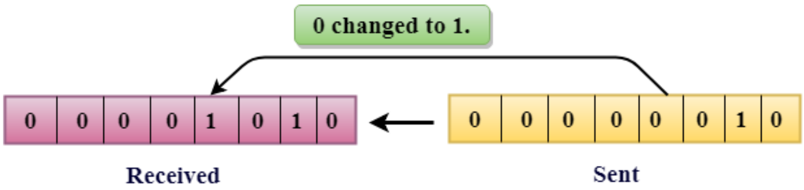
Types Of Errors



Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

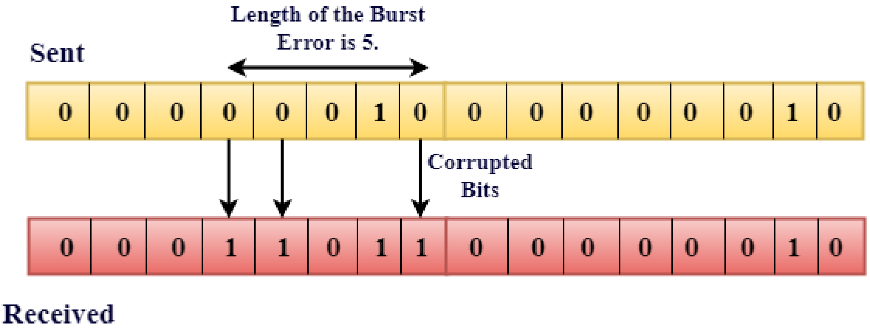
Single-Bit Error: The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1. Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wires is noisy, then single bit is corrupted per byte.

Burst Error: The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error. The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

The number of affected bits depends on the duration of the noise and data rate.

2

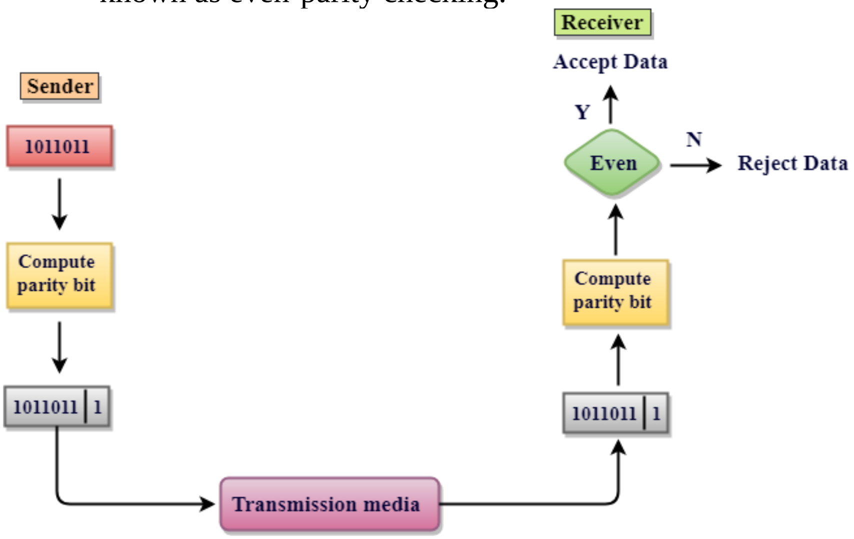
Error Detecting Techniques:

The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

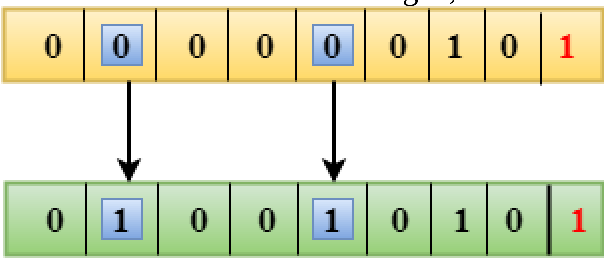
Single Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



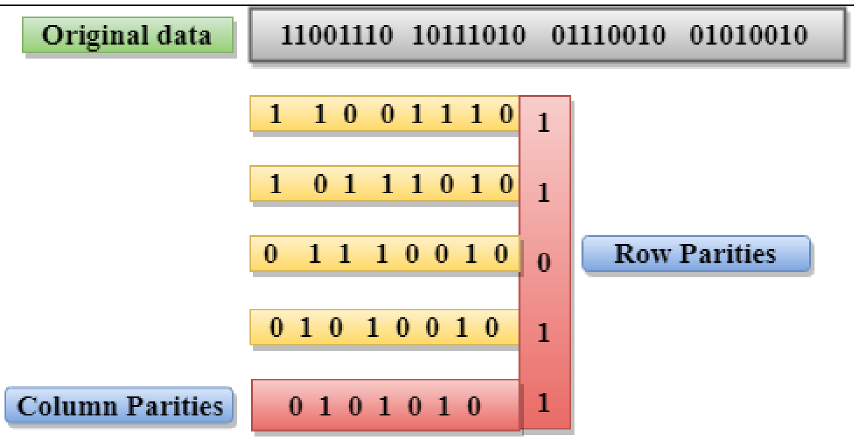
Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



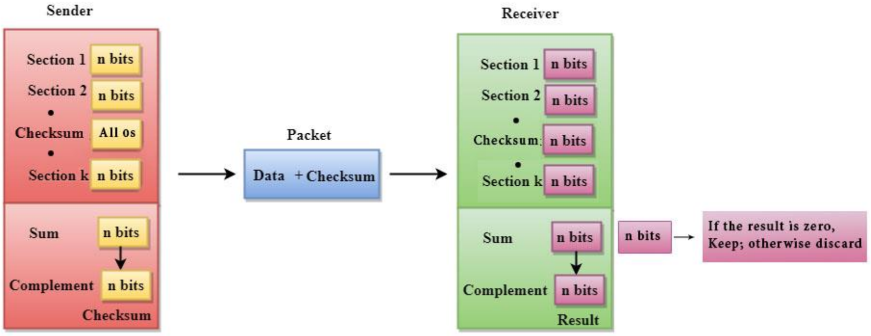
Drawbacks Of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

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

Checksum Generator: A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

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



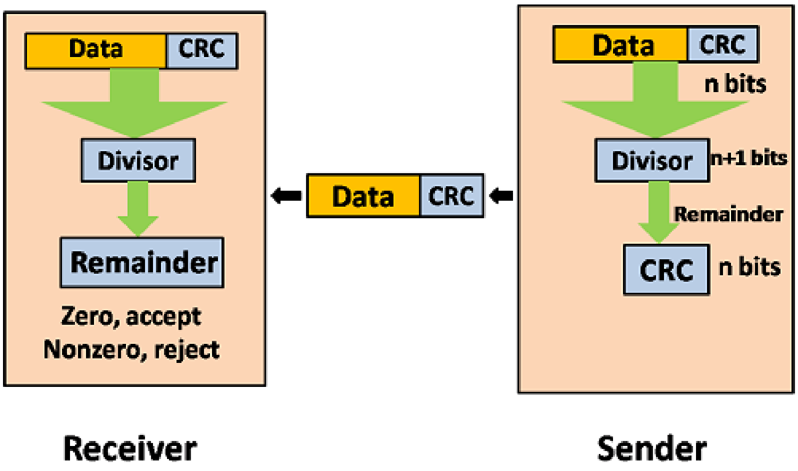
The Sender follows the given steps:

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

Cycle Redundancy Check: CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.



- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

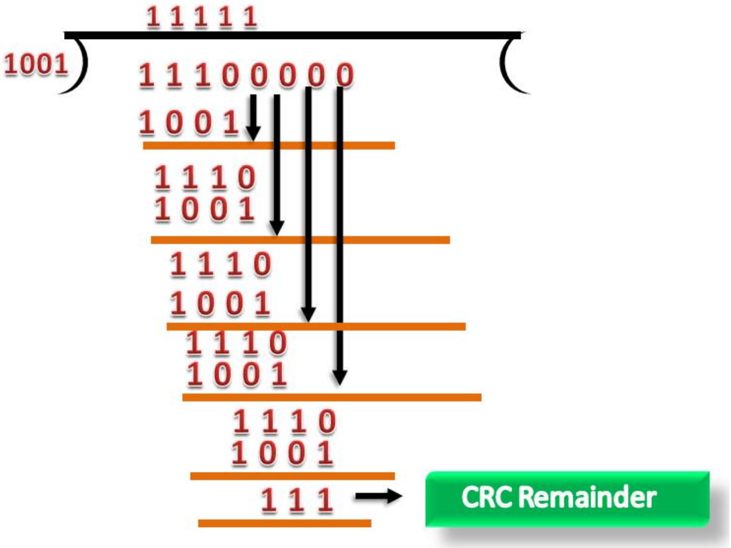
If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

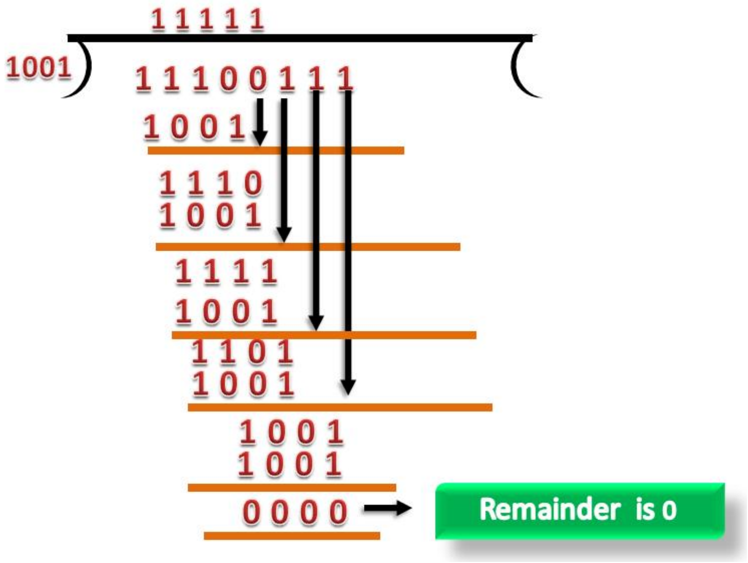
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

- An information of 'd' bits are added to the redundant bits 'r' to form d+r.
- The location of each of the (d+r) digits is assigned a decimal value.
- The 'r' bits are placed in the positions 1,2,.....2^{k-1}.
- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Relationship b/w Error position & binary number.

Error Position	Binary Number
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Let's understand the concept of Hamming code through an example:
Suppose the original data is 1010 which is to be sent.

Total number of data bits 'd' = 4

Number of redundant bits r : 2^r >= d+r+1

2^r>= 4+r+1

Therefore, the value of r is 3 that satisfies the above relation.

Total number of bits = d+r = 4+3 = 7;

Determining the position of the redundant bits

The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are 1, 2^1, 2^2.

1. The position of r1 = 1
2. The position of r2 = 2
3. The position of r4 = 4

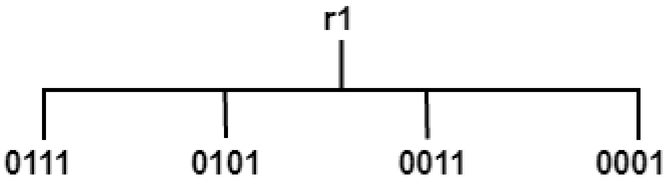
Representation of Data on the addition of parity bits:

7	6	5	4	3	2	1
1	0	1	r4	0	r2	r1

Determining the Parity bits

Determining the r1 bit

The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.

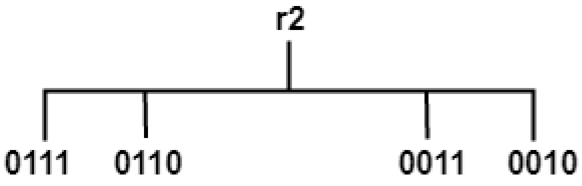


7	6	5	4	3	2	1
1	0	1	r4	0	r2	r1

We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is even, therefore, the value of the r1 bit is 0.

Determining r2 bit

The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.

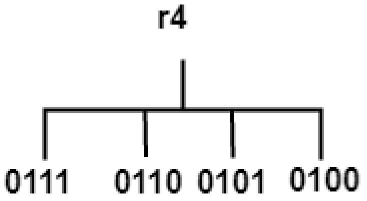


7	6	5	4	3	2	1
1	0	1	r4	0	r2	0

We observe from the above figure that the bit positions that includes 1 in the second position are 2, 3, 6, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r2 is odd, therefore, the value of the r2 bit is 1.

Determining r4 bit

The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



7	6	5	4	3	2	1
1	0	1	r4	0	1	0

We observe from the above figure that the bit positions that includes 1 in the third position are 4, 5, 6, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r4 is even, therefore, the value of the r4 bit is 0.

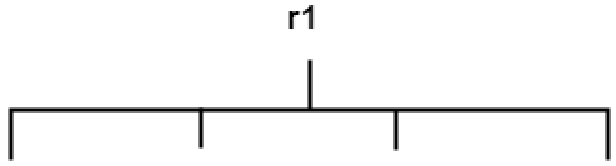
Data transferred is given below:

7	6	5	4	3	2	1
1	0	1	0	0	1	0

Suppose the 4th bit is changed from 0 to 1 at the receiving end, then parity bits are recalculated.

R1 bit

The bit positions of the r1 bit are 1,3,5,7

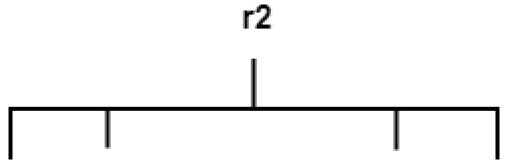


7	6	5	4	3	2	1
1	0	1	1	0	1	0

We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the even-parity check, the total number of 1s appearing in the r1 bit is an even number. Therefore, the value of r1 is 0.

R2 bit

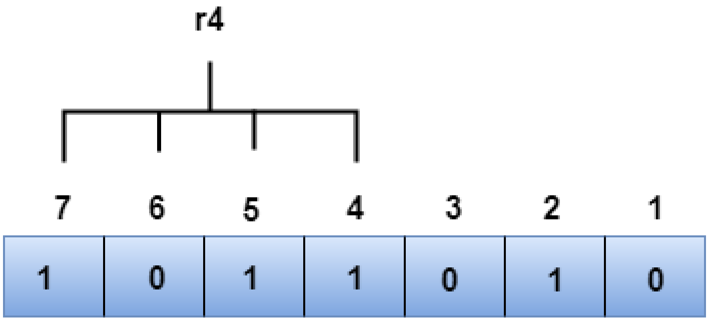
The bit positions of r2 bit are 2,3,6,7.



7	6	5	4	3	2	1
1	0	1	0	0	1	0

We observe from the above figure that the binary representation of r2 is 1001. Now, we perform the even-parity check, the total number of 1s appearing in the r2 bit is an even number. Therefore, the value of r2 is 0.

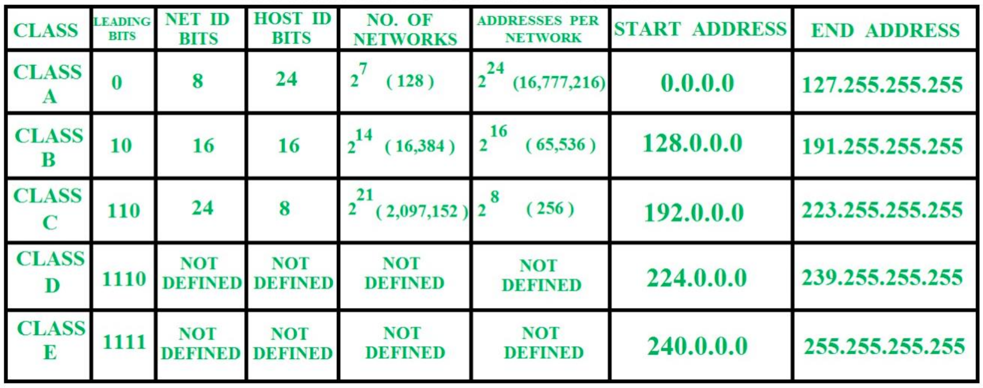
R4 bit

	The bit positions of r4 bit are 4,5,6,7.  We observe from the above figure that the binary representation of r4 is 1011. Now, we perform the even-parity check, the total number of 1s appearing in the r4 bit is an odd number. Therefore, the value of r4 is 1. ○ The binary representation of redundant bits, i.e., r4r2r1 is 100, and its corresponding decimal value is 4. Therefore, the error occurs in a 4th bit position. The bit value must be changed from 1 to 0 to correct the error.	

5. Attempt any *one* part of the following: 10*1 = 10

Qno	Questions	CO
(a)	Question: What is need of IP address? Discuss Classful addressing in IPv4. Answer: All the computers of the world on the Internet network communicate with each other with underground or underwater cables or wirelessly. If I want to download a file from the internet or load a web page or literally do anything related to the internet, my computer must have an address so that other computers can find and locate mine in order to deliver that particular file or webpage that I am requesting. In technical terms, that address is called IP Address or Internet Protocol Address. The working of IP addresses is similar to other languages. It can also use some set of rules to send information. Using these protocols we can easily send, and receive data or files to the connected devices. There are several steps behind the scenes. Let us look at them • Your device directly requests your Internet Service Provider which then grants your device access to the web. • And an IP Address is assigned to your device from the given range available. • Your internet activity goes through your service provider, and they route it back to you, using your IP address. • Your IP address can change. For example, turning your router on or off can change your IP Address. • When you are out from your home location your home IP address doesn't accompany you. It changes as you change the network of your device. **Types of IPv4 Address:** IPv4: Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole	3

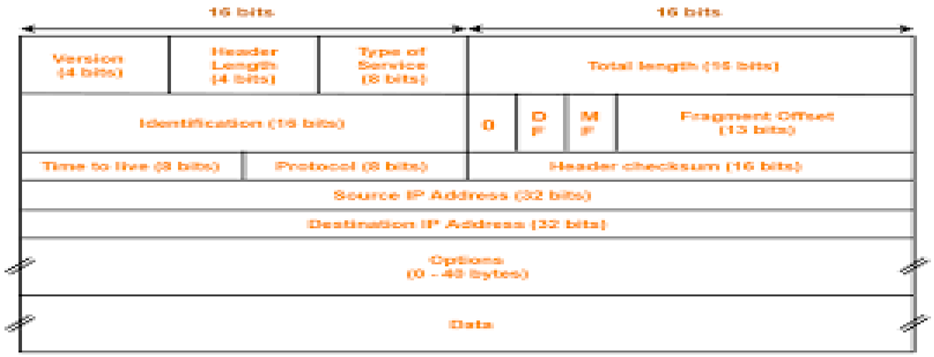
IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4. IPv4 can be written as: 189.123.123.90.Classes of IPv4 Address: There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let's understand it with a simple example. If you have to find a word from a language dictionary, how long will it take? Usually, you will take less than 5 minutes to find that word. You are able to do this because words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionary that doesn't use any sequence or order to organize the words, it will take an eternity to find the word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses. For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes.



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^{7} (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^{8} (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

(b) **Question:** Discuss IPv4 packet format with suitable diagram the at network layer. 3

Answer: The network layer is the third layer (from bottom) in the OSI Model. The network layer is concerned with the delivery of a packet across multiple networks. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. This layer contains hardware devices such as routers, bridges, firewalls, and switches, but it actually creates a logical image of the most efficient communication route and implements it with a physical medium. Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it. Internet Protocol and Netware IPX/SPX are the most common protocols associated with the network layer. The IPv4 packet and its format is as follows:

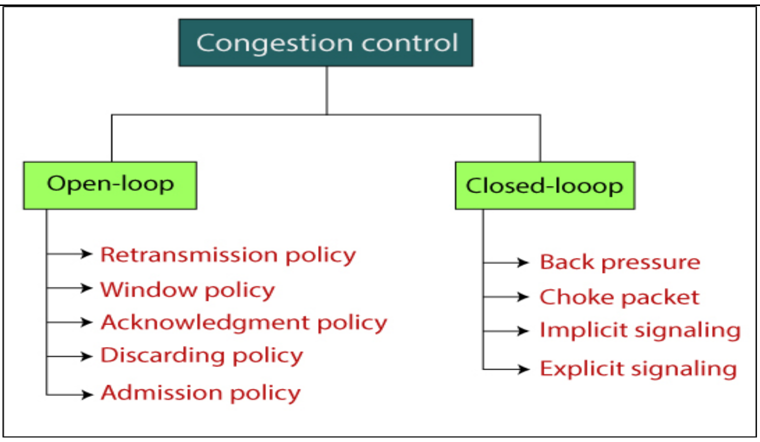


IPv4 Header

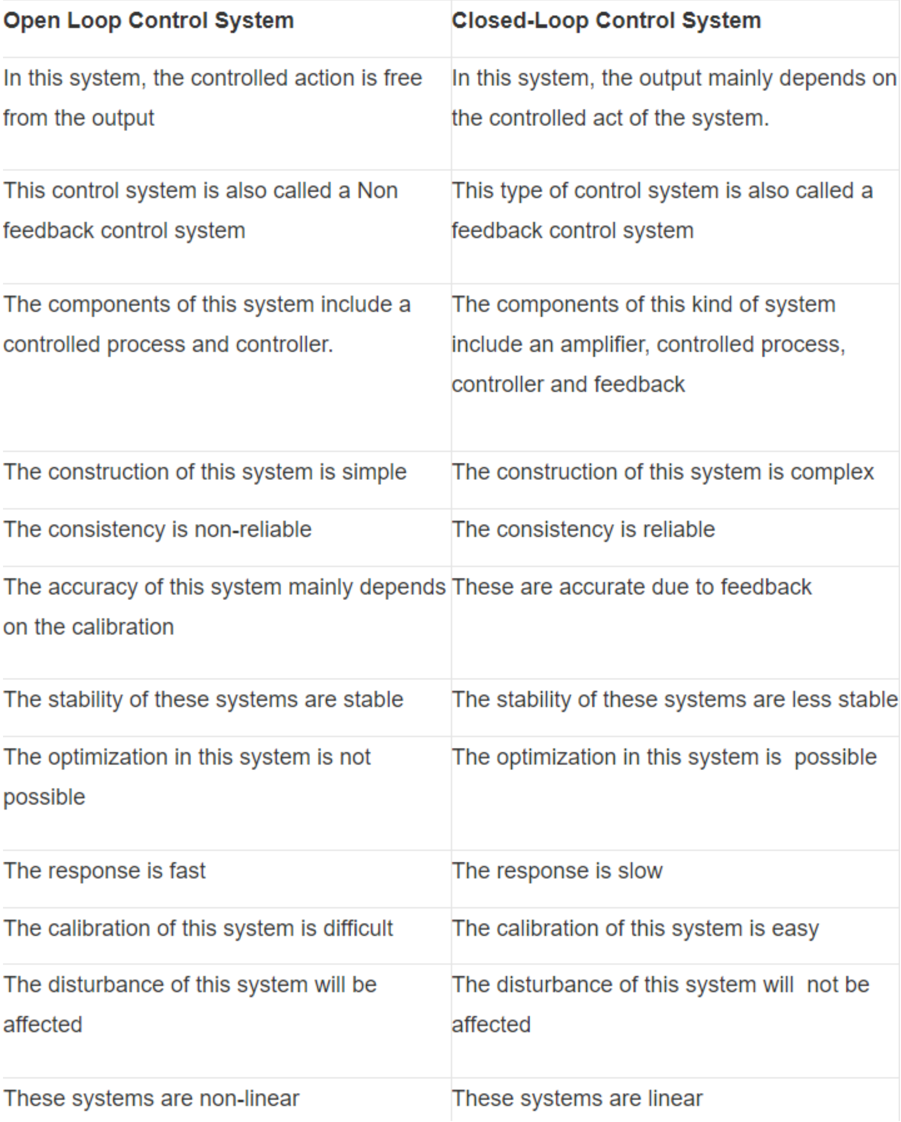
	The size of the IPv4 header is 20 to 60 bytes. ➢ **VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4 ➢ **HLEN:** IP header length (4 bits), which is the number of 32bit words in the header. The minimum value for this field is 5 and the maximum is 15. ➢ **Type of service:** Low Delay, High Throughput, Reliability (8 bits) ➢ **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes, and the maximum is 65,535 bytes. ➢ **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits) ➢ **Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order) ➢ **Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes. ➢ **Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination. ➢ **Protocol:** Name of the protocol to which the data is to be passed (8 bits) ➢ **Header Checksum:** 16 bits header checksum for checking errors in the datagram header. ➢ **Source IP address:** 32 bits IP address of the sender ➢ **Destination IP address:** 32 bits IP address of the receiver ➢ **Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not. Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).	

6. Attempt any *one* part of the following: 10*1 = 10

Qno	Questions	CO
(a)	**Question:** Differentiate between Open Loop and Closed Loop Congestion Control at transport layer. **Answer:** Congestion is a state occurs in the network layer when the message traffic is so heavy that it slows down network response time. Congestion causes choking of the communication medium. When too many packets are displayed in a method of the subnet, the subnet's performance degrades. Hence, a network's communication channel is called congested if packets are traversing the path and experience delays mainly over the path's propagation delay.	4



The difference between Open Loop and Closed Loop Congestion Control are as follows:



Open Loop Control System	Closed-Loop Control System
In this system, the controlled action is free from the output	In this system, the output mainly depends on the controlled act of the system.
This control system is also called a Non feedback control system	This type of control system is also called a feedback control system
The components of this system include a controlled process and controller.	The components of this kind of system include an amplifier, controlled process, controller and feedback
The construction of this system is simple	The construction of this system is complex
The consistency is non-reliable	The consistency is reliable
The accuracy of this system mainly depends on the calibration	These are accurate due to feedback
The stability of these systems are stable	The stability of these systems are less stable
The optimization in this system is not possible	The optimization in this system is possible
The response is fast	The response is slow
The calibration of this system is difficult	The calibration of this system is easy
The disturbance of this system will be affected	The disturbance of this system will not be affected
These systems are non-linear	These systems are linear

(b) **Question:** Explain various traffic shaping algorithms. 4

Answer: Traffic Shaping is a mechanism to control the amount and the rate of traffic sent to the network. Approach of congestion management is called Traffic shaping. Traffic shaping helps to regulate the rate of data transmission and reduces congestion.

There are 2 types of traffic shaping algorithms:

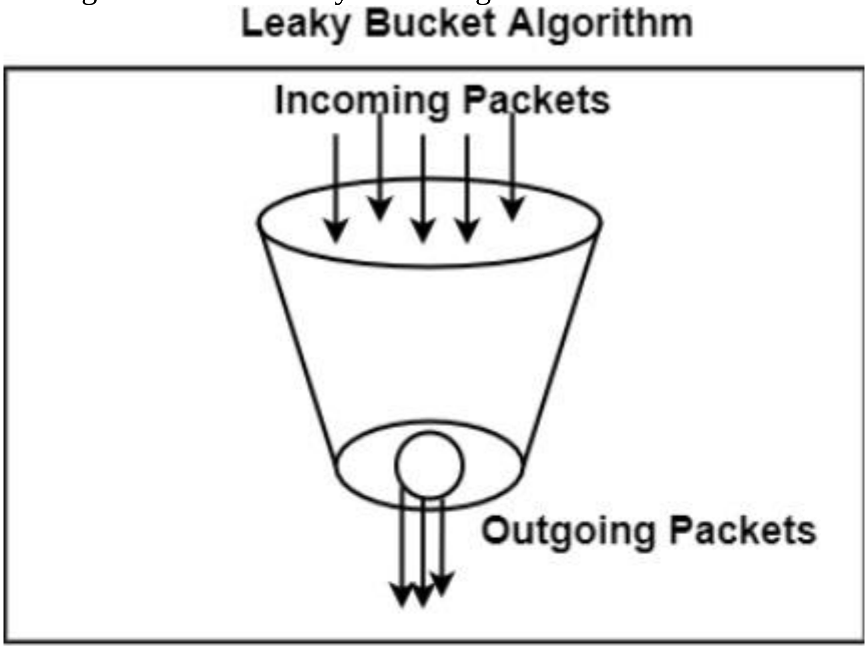
1. Leaky Bucket
2. Token Bucket

Leaky Bucket

The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting. The algorithm allows controlling the rate at which a record is injected into a network and managing burstiness in the data rate.

A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms. This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.

The figure shows the leaky bucket algorithm.



In this algorithm, a bucket with a volume of, say, b bytes and a hole in the Notes bottom is considered. If the bucket is null, it means b bytes are available as storage. A packet with a size smaller than b bytes arrives at the bucket and will forward it. If the packet's size increases by more than b bytes, it will either be discarded or queued. It is also considered that the bucket leaks through the hole in its bottom at a constant rate of r bytes per second.

The outflow is considered constant when there is any packet in the bucket and zero when it is empty. This defines that if data flows into the bucket faster than data flows out through the hole, the bucket overflows.

The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources. The leak rate is a fixed parameter. In the case of the traffic, volume is deficient, the large area of network resources such as bandwidth is not being used effectively. The leaky-bucket algorithm does not allow individual flows to burst up to port speed to effectively consume network resources when there would not be resource contention in the network.

Token Bucket Algorithm

The leaky bucket algorithm has a rigid output design at the average rate independent of the bursty traffic. In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.

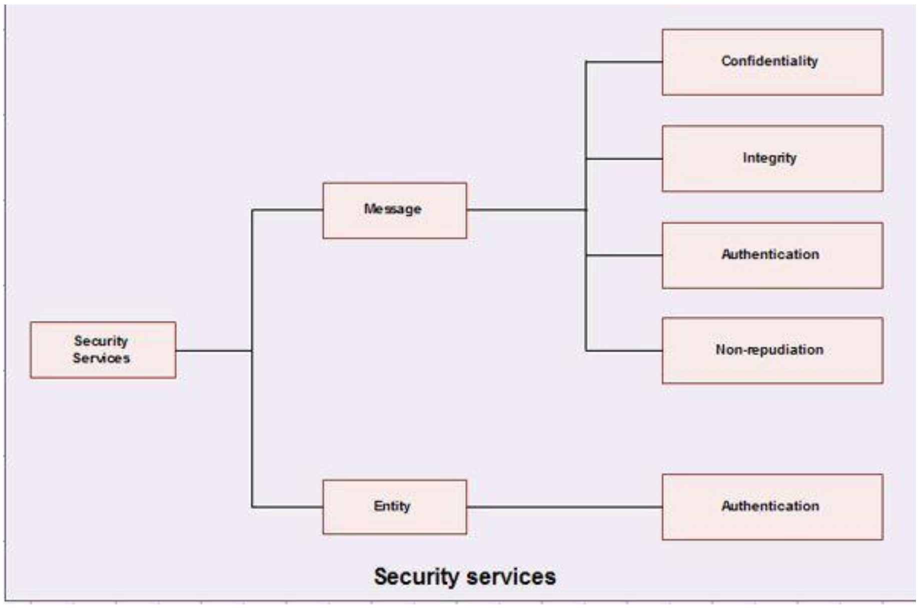
It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket. The bucket

	contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet. When tokens are shown, a flow to transmit traffic appears in the display of tokens. No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket. Thus, the token bucket algorithm adds a token to the bucket each 1 / r seconds. The volume of the bucket is b tokens. When a token appears, and the bucket is complete, the token is discarded. If a packet of n bytes appears and n tokens are deleted from the bucket, the packet is forwarded to the network. When a packet of n bytes appears but fewer than n tokens are available. No tokens are removed from the bucket in such a case, and the packet is considered non-conformant. The non-conformant packets can either be dropped or queued for subsequent transmission when sufficient tokens have accumulated in the bucket. They can also be transmitted but marked as being non-conformant. The possibility is that they may be dropped subsequently if the network is overloaded.	

7. Attempt any *one* part of the following: 10*1 = 10

Qno	Questions	CO
(a)	**Question:** Define network security and discuss various network security services in computer networks. **Answer:** Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats. The most basic example of Network Security is password protection which the user of the network oneself chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as: 1. Users 2. Locations 3. Data 4. Devices 5. Applications **Benefits of Network Security:** Network Security has several benefits, some of which are mentioned below: 1. Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats. 2. Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident. 3. It overall protects the reputation of the organization as it protects the data and confidential items.	5

Various network security services in computer networks are as follows:



Security services

1. Message confidentiality: It means that the content of a message when transmitted across a network must remain confidential, i.e. only the intended receiver and no one else should be able to read the message. The users; therefore, want to encrypt the message they send so that an eavesdropper on the network will not be able to read the contents of the message.

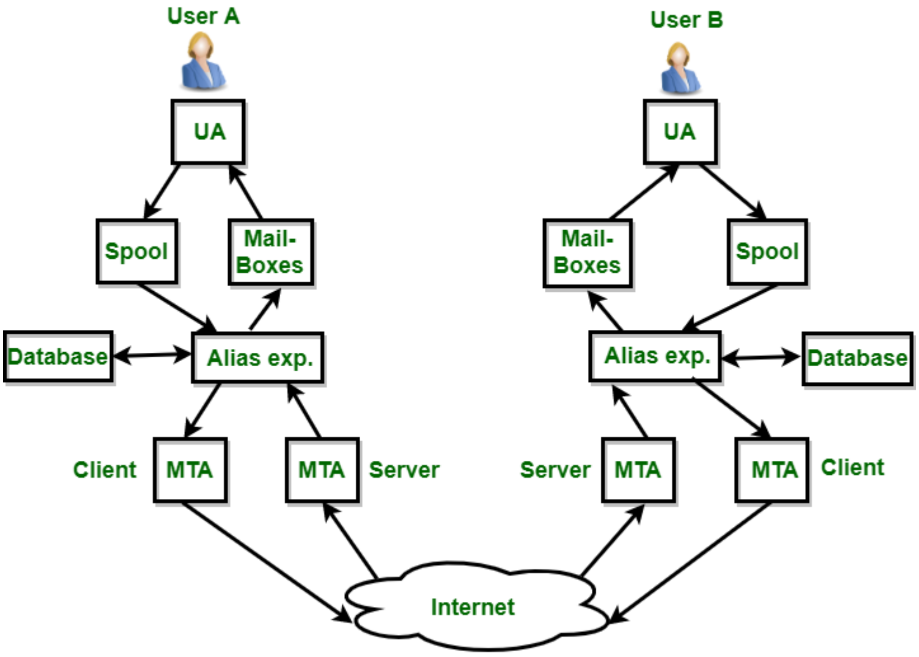
2. Message Integrity: It means the data must reach the destination without any adulteration i.e., exactly as it was sent. There must be no changes during transmission, neither accidentally nor maliciously. Integrity of a message is ensured by attaching a checksum to the message. The algorithm for generating the checksum ensures that an intruder cannot alter the checksum or the message.

3. Message Authentication: In message authentication the receiver needs to be .sure of the sender’s identity i.e., the receiver has to make sure that the actual sender is the same as claimed to be.There are different methods to check the genuineness of the sender :

- The two parties share a common secret code word. A party is required to show the secret code word to the other for authentication.
- Authentication can be done by sending digital signature.
- A trusted third party verifies the authenticity. One such way is to use digital certificates issued by a recognized certification authority.

	4. Message non-reproduction: non-repudiation means that a sender must not be able to deny sending a message that it actually sent. The burden of proof falls on the receiver. Non-reproduction is not only in respect of the ownership of the message; the receiver must prove that the contents of the message are also the same as the sender sent. Non-repudiation is achieved by authentication and integrity mechanisms. **5. Entity Authentication:** In entity authentication (or user identification) the entity or user is verified prior to access to the system resources .	
(b)	**Question:** Discuss E-mail architectures with its components. **Answer:** Electronic mail, commonly known as email, is a method of exchanging messages over the internet. Here are the basics of email: ➢ An email address: This is a unique identifier for each user, typically in the format of name@domain.com. ➢ An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook, or Apple Mail. ➢ An email server: This is a computer system responsible for storing and forwarding emails to their intended recipients. **To send an email:** ➢ Compose a new message in your email client. ➢ Enter the recipient's email address in the "To" field. ➢ Add a subject line to summarize the content of the message. ➢ Write the body of the message. ➢ Attach any relevant files if needed. ➢ Click "Send" to deliver the message to the recipient's email server. ➢ Emails can also include features such as cc (carbon copy) and bcc (blind carbon copy) to send copies of the message to multiple recipients, and reply, reply all, and forward options to manage the conversation. Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a message in formatted manner (mail) to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called sender and person who receives mail is called recipient. It is just like postal mail service. Components of E-Mail System : The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below. 1. **User Agent (UA) :** The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes. 2. **Message Transfer Agent (MTA**): MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is	5

in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.



3. **Mailbox:** It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.
4. **Spool file:** This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an alias, to represent several different e-mail addresses. It is known as mailing list, Whenever user have to sent a message, system checks recipient's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system :

- Composition – The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- Transfer – Transfer means sending procedure of mail i.e. from the sender to recipient.
- Reporting – Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- Displaying – It refers to present mail in form that is understand by the user.
- Disposition – This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

Advantages of email:

- Convenient and fast communication with individuals or groups globally.

	• Easy to store and search for past messages. • Ability to send and receive attachments such as documents, images, and videos. • Cost-effective compared to traditional mail and fax. • Available 24/7. **Disadvantages of email:** • Risk of spam and phishing attacks. • Overwhelming number of emails can lead to information overload. • Can lead to decreased face-to-face communication and loss of personal touch. • Potential for miscommunication due to lack of tone and body language in written messages. • Technical issues, such as server outages, can disrupt email service. • It is important to use email responsibly and effectively, for example, by keeping the subject line clear and concise, using proper etiquette, and protecting against security threats.		