QUESTION BANK

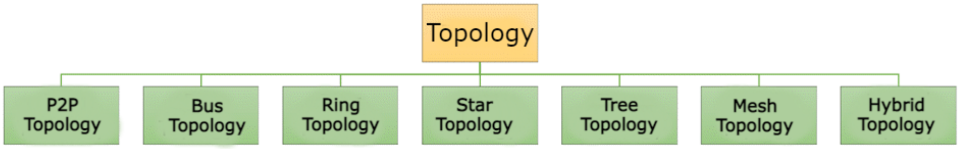
Unit 1: Introduction Concepts

<table>
<tr><th>Ques. No.</th><th>Question</th><th>Marks</th></tr>
<tr><td>1</td><td>Define switching.
Switching, as applied to networking and IT, is the practice of directing a signal or data element toward a particular hardware destination. Switching may be applied in various formats and can function in diverse ways within a greater network infrastructure.</td><td>2</td></tr>
<tr><td>2</td><td>Define signals.
A signal is an electrical or electromagnetic current that is used for carrying data from one device or network to another.</td><td>2</td></tr>
<tr><td>3</td><td>What is ISDN?
ISDN or Integrated Services Digital Network is a circuit-switched telephone network system that transmits both data and voice over a digital line. You can also think of it as a set of communication standards to transmit data, voice, and signaling.</td><td>2</td></tr>
<tr><td>4</td><td>Differentiate between TCP and UDP.
<table>
<tr><th>TCP</th><th>UDP</th><th></th></tr>
<tr><td><b>Full form</b></td><td>It stands for <b>Transmission Control Protocol</b>.</td><td>It stands for <b>User Datagram Protocol</b>.</td></tr>
<tr><td><b>Type of connection</b></td><td>It is a connection-oriented protocol, which means that the connection needs to be established before the data is transmitted over the network.</td><td>It is a connectionless protocol, which means that it sends the data without checking whether the system is ready to receive or not.</td></tr>
<tr><td><b>Reliable</b></td><td>TCP is a reliable protocol as it provides assurance for the delivery of data packets.</td><td>UDP is an unreliable protocol as it does not take the guarantee for the delivery of packets.</td></tr>
</table>
</td><td>2</td></tr>
</table>

Speed	TCP is slower than UDP as it performs error checking, flow control, and provides assurance for the delivery of	UDP is faster than TCP as it does not guarantee the delivery of data packets.
Header size	The size of TCP is 20 bytes.	The size of the UDP is 8 bytes.

5	What is packetizing? **Packetizing** – The process of encapsulating the data received from upper layers of the network(also called as payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination is known as packetizing.	2
6	What is Open System Interconnection? The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other. The OSI Model can be seen as a universal language for computer networking. It’s based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.	2
7	What are the different types of networks? **7 types of networks and their use cases** • Personal area network. A personal area network (PAN) is the smallest and simplest type of network. ... • Local area network. ... • Metropolitan area network. ... • Campus network. ... • Wide area network. ... • Content delivery network. ... • Virtual private network.	2

8	Explain the types of transmission modes. There are three primary types of transmission modes based on the direction of exchange of information. The first is **simplex,** **followed by half duplex,** **and finally full duplex.**	2
9	What are analog signals? Analog signals were used in many systems to produce signals to carry information. These signals are continuous in both values and time. The use of analog signals has declined with the arrival of digital signals. In short, to understand analog signals – all signals that are natural or come naturally are analog signals.	2
10	Define forwarding of IP packets? **Packet forwarding** is the process of directing the packet towards its destination. As we know that Internet is a combination of several networks. A packet may belong to the same network as of source host or it may be for the destination host in a different network. So, a packet from a source host may have to travel many networks before reaching the destination.	2
11	Define the functions of Data Link Layer. **1. Framing:** The packet received from the Network layer is known as a frame in the Data link layer. At the sender's side, DLL receives packets from the Network layer and divides them into small frames, then, sends each frame bit-by-bit to the physical layer. It also attaches some special bits (for error control and addressing) at the header and end of the frame. At the receiver's end, DLL takes bits from the Physical layer organizes them into the frame, and sends them to the Network layer. **2. Addressing:** The data link layer encapsulates the source and destination's MAC address/ physical address in the header of each frame to ensure node-to-node delivery. MAC address is the unique hardware address that is assigned to the device while manufacturing. **3. Error Control:** Data can get corrupted due to various reasons like noise, attenuation, etc. So, it is the responsibility of the data link layer, to detect the error in the transmitted data and correct it using error detection and correction techniques respectively. DLL adds error detection bits into the frame's header, so that receiver can check received data is correct or not. **4. Flow Control:** If the receiver's receiving speed is lower than the sender's sending speed, then this can lead to an overflow	5

	in the receiver’s buffer and some frames may get lost. So, it’s the responsibility of DLL to synchronize the sender’s and receiver’s speeds and establish flow control between them. **5. Access Control:** When multiple devices share the same communication channel there is a high probability of collision, so it’s the responsibility of DLL to check which device has control over the channel and CSMA/CD and CSMA/CA can be used to avoid collisions and loss of frames in the channel.	
12	Define topology and mention the types of topologies. Network topologies describe the methods in which all the elements of a network are mapped. The topology term refers to both the physical and logical layout of a network.  Topology P2P Topology Bus Topology Ring Topology Star Topology Tree Topology Mesh Topology Hybrid Topology • **Bus Topology:** All the devices/nodes are connected sequentially to the same backbone or transmission line. This is a simple, low-cost topology, but its single point of failure presents a risk. • **Star Topology:** All the nodes in the network are connected to a central device like a hub or switch via cables. Failure of individual nodes or cables does not necessarily create downtime in the network but the failure of a central device can. This topology is the most preferred and popular model. • **Ring Topology:** All network devices are connected sequentially to a backbone as in bus topology except that the backbone ends at the starting node, forming a ring. Ring topology shares many of bus topology's disadvantages so its use is limited to networks that demand high throughput. • **Tree Topology:** A root node is connected to two or more sub-level nodes, which themselves are connected hierarchically to sub-level nodes. Physically, the tree topology is similar to bus and star topologies; the network backbone may have a bus topology, while the low-level nodes connect using star	5

topology.

- **Mesh Topology:** The topology in each node is directly connected to some or all the other nodes present in the network. This redundancy makes the network highly fault-tolerant but the escalated costs may limit this topology to highly critical networks.

13 Differentiate between Analog and Digital signals. 5

Difference Between Analog And Digital Signal	
Analog Signals	**Digital Signals**
Continuous signals	Discrete signals
Represented by sine waves	Represented by square waves
Human voice, natural sound, analog electronic devices are a few examples	Computers, optical drives, and other electronic devices
Continuous range of values	Discontinuous values
Records sound waves as they are	Converts into a binary waveform
Only used in analog devices	Suited for digital electronics like computers, mobiles and more

14 What are the different types of networks? Explain in detail. 5

A network is defined as a group of two or more computer systems linked together.

There are many types of computer networks, the common types of area networks including those five: *LAN - Local Area Network, WAN - Wide Area Network, WLAN - Wireless Local Area Network, MAN - Metropolitan Area Network and CAN - Campus Area Network.*

LAN (Local Area Network) - Can go up to 1 KM radius. A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment.

WAN (Wide Area Network) - No Limit. A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metro area networks

(MANs). This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.

WLAN(Wireless Local Area Network) - A wireless local area network (WLAN) is a wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

MAN(Metropolitan Area Network) - A metropolitan area network is a computer network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

CAN (Campus Area Network) - A campus area network is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area. The networking equipments (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc) are almost entirely owned by the campus tenant / owner: an enterprise, university, government etc.

15 Differentiate between LAN, MAN and WAN. 5

Parameter	**LAN**	**MAN**	**WAN**
Full Form	LAN is an acronym for Local Area Network.	MAN is an acronym for Metropolitan Area Network.	WAN is an acronym for Wide Area Network.
Definition and Meaning	LAN is a network that usually connects a small group of computers in a given geographical	MAN is a comparatively wider network that covers large regions- like towns, cities, etc.	The WAN network spans to an even larger locality. It has the capacity to connect various countries together. For example, the

	area.		Internet is a WAN.
Network Ownership	The LAN is private. Hospitals, homes, schools, offices, etc., may own it.	The MAN can be both private or public. Many organizations and telecom operators may own them.	The WAN can also be both private or public.
Maintenance and Designing	Very easy to design and maintain.	Comparatively difficult to design and maintain.	Very difficult to design and maintain.
Speed	LAN offers a very high Internet speed.	MAN offers a moderate Internet speed.	WAN offers a low Internet speed.
Delay in Propagation	It faces a very short propagation delay.	It faces a moderate propagation delay.	It faces a high propagation delay.

16 What are the different types of transmission media? 5

Guided Media

This kind of transmission media is also known as wired otherwise bounded media. In this type, the signals can be transmitted directly & restricted in a thin path through physical links.

The main features of guided media mainly include secure, high-speed, and used in small distances. This kind of media is classified into three types which are discussed below.

Twisted Pair Cable

It includes two separately protected conductor wires. Normally, some pairs of cables are packaged jointly in a protective cover. This is the most frequently used type of transmission media and it is available in two types.

UTP (Unshielded Twisted Pair)

This UTP cable has the capacity to block interference. It doesn’t depend on a physical guard and used in telephonic applications. The advantage of UTP is a low cost, very simple to install, and high speed. The disadvantages of UTP is liable to exterior interference, transmits in fewer distances, and less capacity.

STP (Shielded Twisted Pair)

STP cable includes a particular jacket for blocking outside interference. It is used in rapid data rate Ethernet, in voice & data channels of telephone lines.

The main advantages of STP cable mainly include good speed, removes crosstalk. The main disadvantages are hard to manufacture as well as install, It is expensive and bulky also

Coaxial Cable

This cable contains an external plastic cover and it includes two parallel conductors where each conductor includes a separate protection cover. This cable is used to transmit data in two modes like baseband mode as well as broadband mode. This cable is widely used in cable TVs & analog TV networks.

The advantages of the coaxial cable include high bandwidth, noise immunity is good, low cost and simple to install. The disadvantage of this cable is, the failure of cable can disturb the whole network

Optical Fibre Cable

This cable uses the notion of light reflected through a core that is made with plastic or glass. The core is enclosed with less thick plastic or glass and it is known as the cladding, used for large volume data transmission.

The main advantages of this cable include lightweight, capacity & bandwidth will be increased, signal attenuation is less, etc. The disadvantages are high cost, fragile, installation & maintenance is difficult and unidirectional.

Unguided Media

It is also known as unbounded otherwise wireless transmission media. It doesn't require any physical medium to transmit electromagnetic signals. The main features of this media are less secure, the signal can be transmitted through air, and applicable for large distances. There are three types of unguided media which are discussed below.

Radiowaves

These waves are very easy to produce as well as penetrate through buildings. In this, the transmitting & receiving antennas no need to align. The frequency range of these waves ranges from 3 kHz to 1GHz. These waves are used in AM & Fm radios for transmission. These waves are classified into two types namely Terrestrial & Satellite.

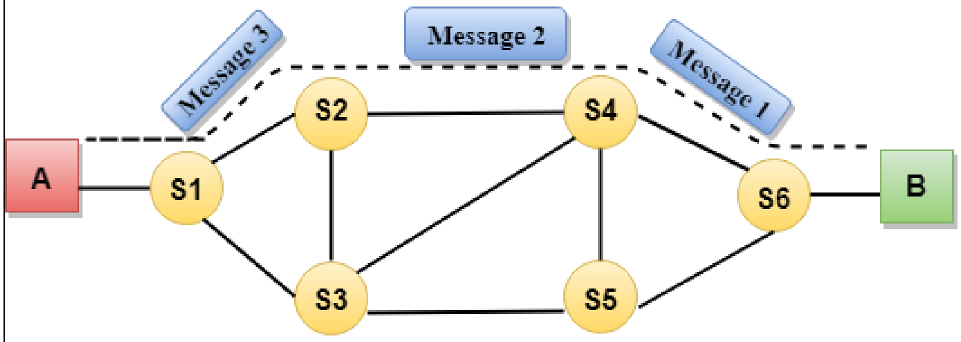
Microwaves

It is a sightline transmission which means the transmitting & receiving antennas need to align correctly with each other. The distance which is covered through the signal can be directly proportional to the antenna's height. The frequency range of microwaves ranges from 1GHz to 300GHz. These are extensively used in TV distribution & mobile phone communication

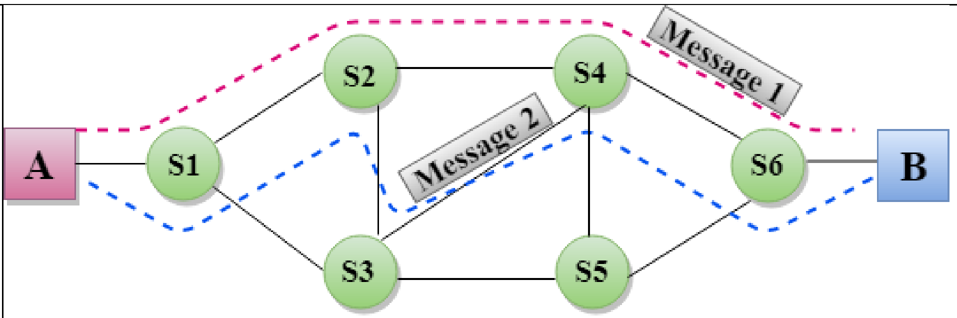
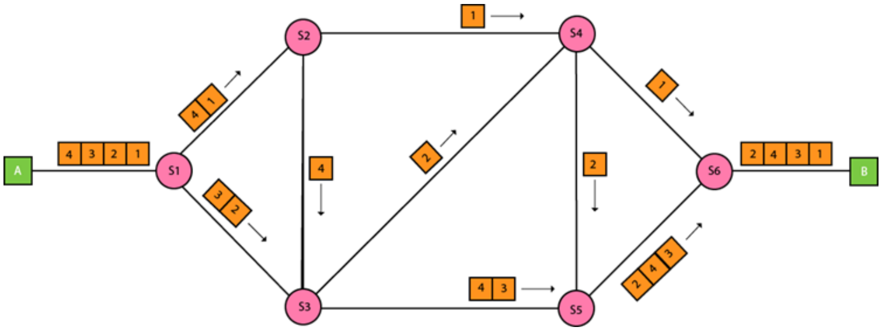
Infrared Waves

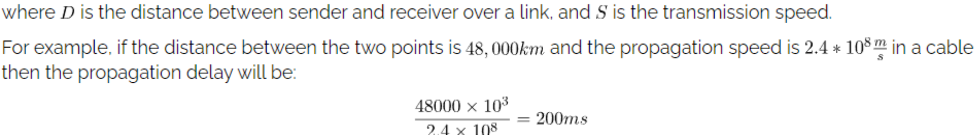
Infrared (IR) waves are used in extremely small distance communication as they cannot go through obstacles. So it stops intrusion between systems. The range of frequency of

NOTES LINK ->ALL QUESTION BANK

	these waves is 300GHz to 400THz. These waves are used in TV remotes, keyboards, wireless mouse, printer, etc.	
17	Classify the different type of switching techniques. Switched communication networks are those in which data transferred from source to destination is routed between various intermediate nodes. Switching is the technique by which nodes control or switch data to transmit it between specific points on a network. There are 3 common switching techniques: 1. Circuit Switching 2. Packet Switching 3. Message Switching **Circuit Switching** ○ Circuit switching is a switching technique that establishes a dedicated path between sender and receiver. ○ In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated. ○ Circuit switching in a network operates in a similar way as the telephone works.  Message 3 Message 2 Message 1 A S1 S2 S3 S4 S5 S6 B **Message Switching** ○ Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded. ○ In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.	5

Data Communication & Networking BCSE2370

	 Message 1 Message 2 A S1 S2 S3 S4 S5 S6 B **Packet Switching** ○ The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually. ○ The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end. ○ Every packet contains some information in its headers such as source address, destination address and sequence number.  A 4 3 2 1 S1 4 1 3 2 S2 4 S3 1 2 4 3 S4 2 S5 1 2 4 3 S6 2 4 3 1 B	
18	Categorize different types of Network Topologies. Ans-14	5
19	Differentiate between propagation delay and transmission delay. **The propagation delay is the time it takes for one bit to travel from one end of the link to the other**. The bits travel in the form of electromagnetic signals. The speed at which electromagnetic signals propagate is determined by the medium through which they pass. Following is the formula for propagation delay: D/s	5

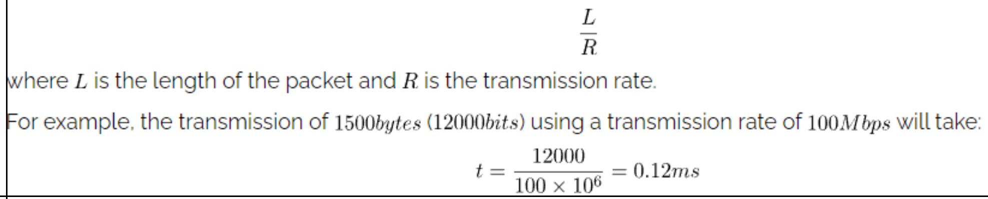


where D is the distance between sender and receiver over a link, and S is the transmission speed.

For example, if the distance between the two points is $48,000km$ and the propagation speed is $2.4 * 10^8 \frac{m}{s}$ in a cable then the propagation delay will be:

$$\frac{48000 \times 10^3}{2.4 \times 10^8} = 200ms$$

Transmission delay is the time needed to push all the packet bits on the transmission link. It mainly depends upon the size of the data and channel bandwidth (in bps). Following is the formula for transmission delay:



$$\frac{L}{R}$$

where L is the length of the packet and R is the transmission rate.

For example, the transmission of $1500bytes$ $(12000bits)$ using a transmission rate of $100Mbps$ will take:

$$t = \frac{12000}{100 \times 10^6} = 0.12ms$$

20 What is network topology? Explain the different network topologies. 5

Ans-14

21 Differentiate between OSI layer and TCP/IP. 8

OSI	TCP/IP
OSI represents **Open System Interconnection**.	TCP/IP model represents the Transmission Control Protocol / Internet Protocol.
OSI is a generic, protocol independent standard. It is acting as an interaction gateway between the network and the final-user.	TCP/IP model depends on standard protocols about which the computer network has created. It is a connection protocol that assigns the network of hosts over the internet.
The OSI model was developed first, and then protocols were created to fit the network architecture's needs.	The protocols were created first and then built the TCP/IP model.
It provides quality services.	It does not provide quality services.
The OSI model represents defines administration,	It does not mention the services, interfaces, and protocols.

interfaces and conventions. It describes clearly which layer provides services.	
The protocols of the OSI model are better unseen and can be returned with another appropriate protocol quickly.	The TCP/IP model protocols are not hidden, and we cannot fit a new protocol stack in it.
It is difficult as distinguished to TCP/IP.	It is simpler than OSI.
It provides both connection and connectionless oriented transmission in the network layer; however, only connection-oriented transmission in the transport layer.	It provides connectionless transmission in the network layer and supports connecting and connectionless-oriented transmission in the transport layer.
It uses a horizontal approach.	It uses a vertical approach.
The smallest size of the OSI header is 5 bytes.	The smallest size of the TCP/IP header is 20 bytes.
Protocols are unknown in the OSI model and are returned while the technology modifies.	In TCP/IP, returning protocol is not difficult.

22 What is TCP/IP Protocol suite? 8

The TCP/IP suite is a set of protocols used on computer networks today (most notably on the Internet). It provides an end-to-end connectivity by specifying how data should be packetized, addressed, transmitted, routed and received on a TCP/IP network. This functionality is organized into four abstraction layers and each protocol in the suite resides in a particular layer.

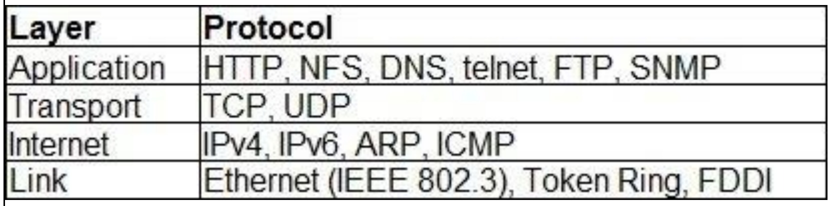
The TCP/IP suite is named after its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Some of the protocols included in the TCP/IP suite are:

- **ARP (Address Resolution Protocol)** – used to associate an IP address with a MAC address.
- **IP (Internet Protocol)** – used to deliver packets from the

source host to the destination host based on the IP addresses.

- **ICMP (Internet Control Message Protocol)** – used to detects and reports network error conditions. Used in ping.
- **TCP (Transmission Control Protocol)** – a connection-oriented protocol that enables reliable data transfer between two computers.
- **UDP (User Datagram Protocol)** – a connectionless protocol for data transfer. Since a session is not created before the data transfer, there is no guarantee of data delivery.
- **FTP (File Transfer Protocol)** – used for file transfers from one host to another.
- **Telnet (Telecommunications Network)** – used to connect and issue commands on a remote computer.
- **DNS (Domain Name System)** – used for host names to the IP address resolution.
- **HTTP (Hypertext Transfer Protocol)** – used to transfer files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

The following table shows which protocols reside on which layer of the TCP/IP model:



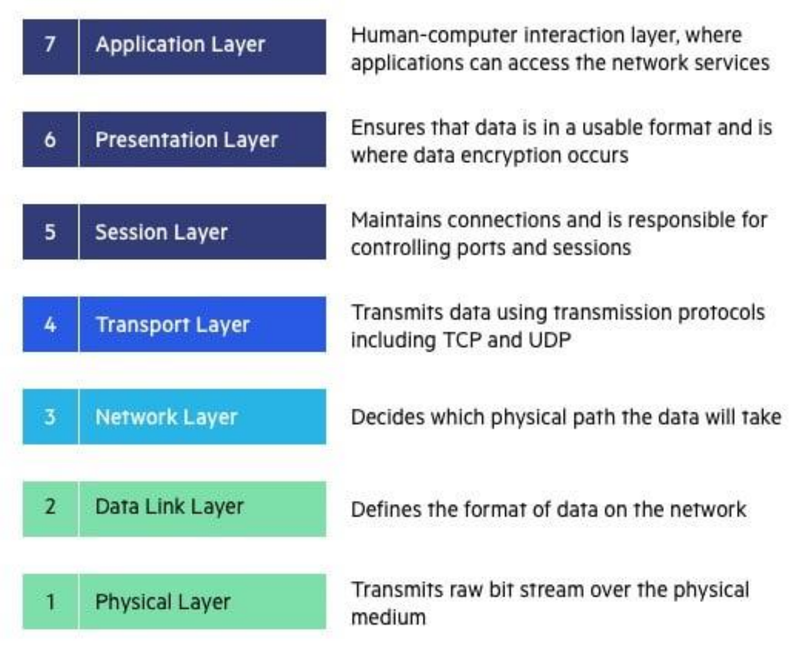
Layer	Protocol
Application	HTTP, NFS, DNS, telnet, FTP, SNMP
Transport	TCP, UDP
Internet	IPv4, IPv6, ARP, ICMP
Link	Ethernet (IEEE 802.3), Token Ring, FDDI

23 Explain your understanding about OSI and TCP/IP model.
Out of these which reference model is being frequently used? 8

Ans-21

TCP/IP is used more compared to the OSI model for providing communication between computers over the internet.

24 Explain OSI reference model with the help of a diagram. 8



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

25 Explain 4 types of delays in computer network. 8

1. Transmission delay
2. Propagation delay
3. Queuing delay
4. Processing delay

1. Transmission Delay-

Time taken to put the data packet on the transmission link is called

Mathematically,

- Transmission delay ∝ Length / Size of data packet
- Transmission delay ∝ 1 / Bandwidth

Thus,

$$\text{Transmission delay} = \frac{\text{Length / Size of data packet}}{\text{Bandwidth of Network}}$$

2. Propagation Delay-

Time taken for one bit to travel from sender to receiver end of the link is called as **propagation delay**.

Mathematically,

- Propagation delay ∝ Distance between sender and receiver
- Propagation delay ∝ 1 / transmission speed

Thus,

$$\text{Propagation delay} = \frac{\text{Distance between sender and receiver}}{\text{Transmission speed}}$$

3. Queuing Delay-

Time spent by the data packet waiting in the queue before it is taken for execution is called as **queuing delay**.

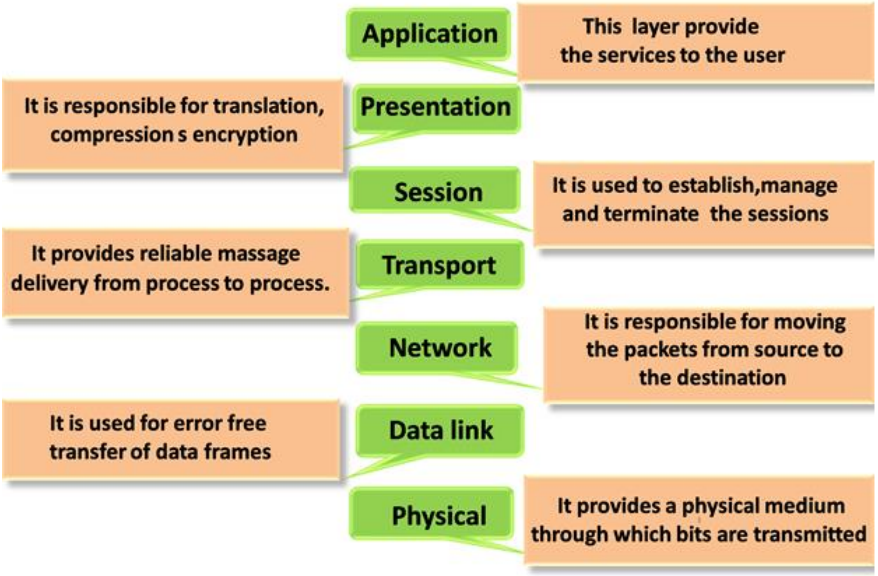
- It depends on the congestion in the network.

4. Processing Delay-

Time taken by the processor to process the data packet is called as **processing delay**.

- It depends on the speed of the processor.
- Processing of the data packet helps in detecting bit level errors

	that occurs during transmission.	
26	What is ISDN? Explain different types of access interfaces used in ISDN. These are a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Before *Integrated Services Digital Network (ISDN)*, the telephone system was seen as a way to transmit voice, with some special services available for data. The main feature of ISDN is that it can integrate speech and data on the same lines, which were not available in the classic telephone system. ISDN is a circuit-switched telephone network system, but it also provides access to packet-switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. A greater data rate was achieved through channel bonding. Generally, ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded **ISDN Interfaces:** The following are the interfaces of ISDN: 1. **Basic Rate Interface (BRI) –** There are two data-bearing channels (‘B’ channels) and one signaling channel (‘D’ channel) in BRI to initiate connections. The B channels operate at a maximum of 64 Kbps while the D channel operates at a maximum of 16 Kbps. The two channels are independent of each other. For example, one channel is used as a TCP/IP connection to a location while the other channel is used to send a fax to a remote location. In iSeries ISDN supports a basic rate interface (BRl). The basic rate interface (BRI) specifies a digital pipe consisting of two B channels of 64 Kbps each and one D channel of 16 Kbps. This equals a speed of 144 Kbps. In addition, the BRI service itself requires an operating overhead of 48 Kbps. Therefore a digital pipe of 192 Kbps is required.	8

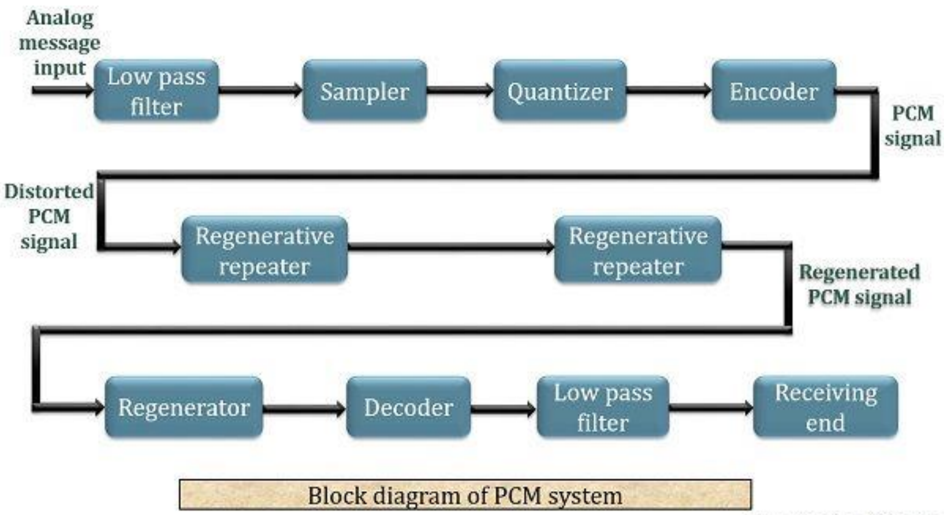
	2. **Primary Rate Interface (PRI) –** Primary Rate Interface service consists of a D channel and either 23 or 30 B channels depending on the country you are in. PRI is not supported on the iSeries. A digital pipe with 23 B channels and one 64 Kbps D channel is present in the usual Primary Rate Interface (PRI). Twenty-three B channels of 64 Kbps each and one D channel of 64 Kbps equals 1.536 Mbps. The PRI service uses 8 Kbps of overhead also. Therefore PRI requires a digital pipe of 1.544 Mbps. 3. **Broadband-ISDN (B-ISDN) –** Narrowband ISDN has been designed to operate over the current communications infrastructure, which is heavily dependent on the copper cable however B-ISDN relies mainly on the evolution of fiber optics. According to CCITT B-ISDN is best described as ‘a service requiring transmission channels capable of supporting rates greater than the primary rate.	
27	What is OSI Model? Explain the functions and protocols andservices of each layer? **Functions of the OSI Layers**  Application – This layer provide the services to the user Presentation – It is responsible for translation, compression s encryption Session – It is used to establish,manage and terminate the sessions Transport – It provides reliable massage delivery from process to process. Network – It is responsible for moving the packets from source to the destination Data link – It is used for error free transfer of data frames Physical – It provides a physical medium through which bits are transmitted	8

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

Unit 2: Digital and Analog Transmission

Ques. No.	Question	Marks
1	Which is faster between digital and analog datatransmission? digital	2
2	What is baud rate? The baud rate is the rate at which information is transferred in a communication channel. Baud rate is commonly used when discussing electronics that use serial communication. In the serial port context, "9600 baud" means that the serial port is capable of transferring a maximum of 9600 bits per second.	2
3	What is the meaning of FSK? Frequency-shift keying (FSK) allows digital information to be transmitted by changes or shifts in the frequency of a carrier signal, most commonly an analog carrier sine wave. There are two binary states in a signal, zero (0) and one (1), each of which is represented by an analog wave form. This binary data is converted by a modem into an FSK signal, which can be transmitted via telephone lines, fiber optics or wireless media. FSK is commonly used for caller ID and remote metering applications. FSK is also known as frequency modulation (FM)	2
4	What is the best modulation technique? **Frequency modulation** is more effective in terms of noise tolerance and more suited for data transmission than AM. Phase modulation is more complex and costly but is relatively immune to noise and theoretically makes the best use of bandwidth for a given transmission rate.	2
5	What is MODEM? a piece of equipment that connects two or more computers together by means of a telephone line so that information can go from one to the other 	2

6	What is Modulation? Modulation can be digital or analog. Input wave of analog scheme varies continuously like a sine wave. Voice is sampled at some rate then compressed and turned into a bit-stream then superimposed on the carrier signal, in digital modulation. This all happens because the communication systems have used a powerful and beautiful technique called Modulation. Modulation: The process by which data/information is converted into electrical/digital signals for transferring that signal over a medium is called **modulation**.	2
7	What is the meaning of FSK? What is frequency-shift keying (FSK)? Frequency-shift keying (FSK) is **a method of transmitting digital signals using discrete signals**. The two binary states -- logic 0 (low) and 1 (high) in a binary frequency-shift key mechanism -- are each represented by an analog waveform.	2
8	Describe the Pulse Code Modulation (PCM) technique with neat diagram? **Definition**: A technique by which **analog signal gets converted into digital form** in order to have signal transmission through a digital network is known as Pulse Code Modulation. It is abbreviated as **PCM**.  Analog message input Low pass filter Sampler Quantizer Encoder PCM signal Distorted PCM signal Regenerative repeater Regenerative repeater Regenerated PCM signal Regenerator Decoder Low pass filter Receiving end Block diagram of PCM system Electronics Coach	5
9	Explain Analog-to-Digital Conversion process with appropriate diagram.	5

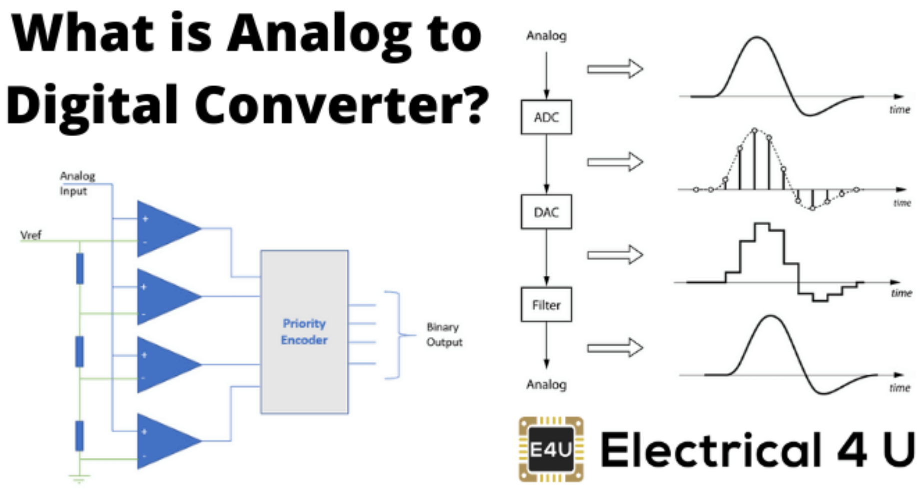
The most common technique to change an analog signal to digital data is called pulse code modulation (PCM). A PCM encoder has the following three processes:

1. Sampling
2. Quantization
3. Encoding

Sampling – The first step in PCM is sampling. Sampling is a process of measuring the amplitude of a continuous-time signal at discrete instants, converting the continuous signal into a discrete signal.

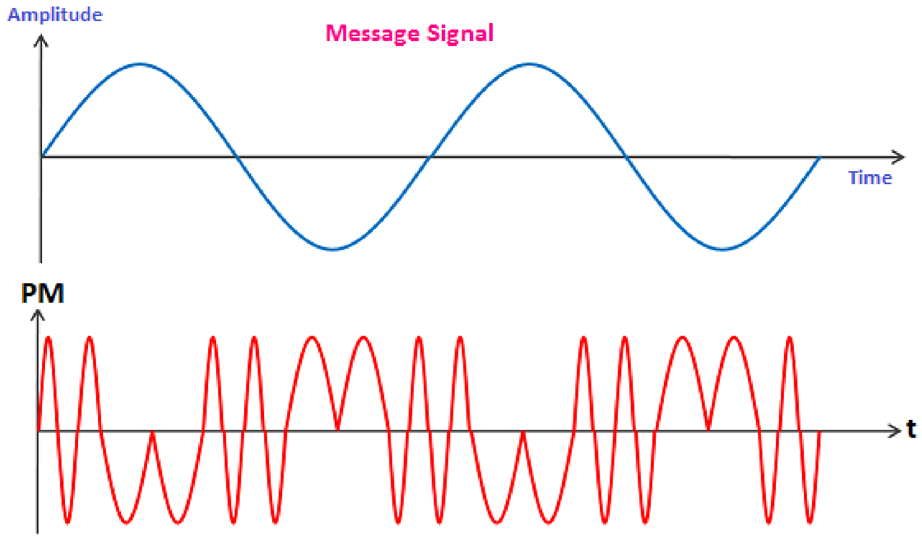
Quantization – The result of sampling is a series of pulses with amplitude values between the maximum and minimum amplitudes of the signal.

Encoding – The digitization of the analog signal is done by the encoder. After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an n bit code. Encoding also minimizes the bandwidth used. Note that the number of bits for each sample is determined from the number of quantization levels. If the number of quantization levels is L, the number of bits is n bit = log 2 L.



10 Explain Phase Modulation technique using graphicalrepresentation. 5

Phase modulation is defined as the process of varying the phase of the carrier signal linearly with the instantaneous value of the message signal. The waveforms of a message signal and the phase-modulated signal are shown below:



The equation of a PM signal is represented by:

$$\mathbf{V(t) = A \cos [\omega_c t + \phi (t)]}$$

Where,

ω_c is the carrier frequency constant

A is the amplitude constant

ϕ (t) is the phase angle, which is not constant. It is a function of the baseband signal.

Let's first discuss the message signal and the carrier signal.

The applications of Phase Modulation are listed as follows:

- **SoundSynthesis**
  PM is less susceptible to noise interference and popping sounds than AM. Hence, it is suitable for sound broadcasting, commonly referred to as sound synthesis.
- **DigitalSynthesizers**
  PM is used in digital synthesizers for the generation of signals and waveform.

- **TelephoneCommunication**
  PM is widely used in telephone communication due to its high-speed transmission.

The advantages of Phase Modulation are as follows:

- **High speed**
  Phase modulation is considered as one the fastest modulation technique. It is due to the pulse generation at high speed.
- **Low signal power consumption**
  PM requires low signal power consumption due to its better efficiency and fast speed.
- **Simple circuit design**
  The components required in the phase modulated circuit are less as compared to FM. Hence, it has a simple circuit design.
- **Easy modulation and demodulation**
  Phase modulation and demodulation is easy as compared to PM due to its simple circuit design.

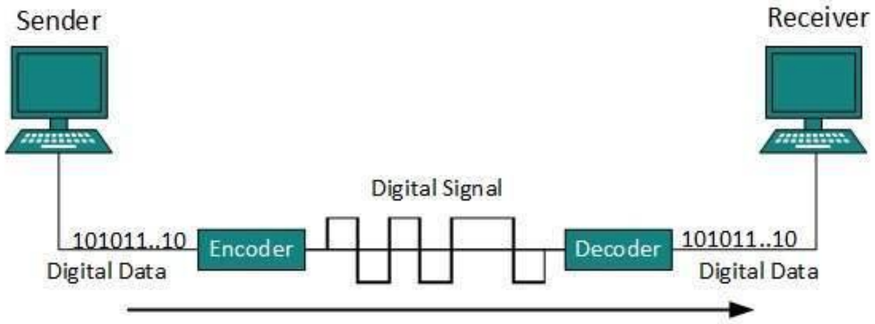
11 Explain different techniques used for digital to digital dataconversion. 5

Digital-to-Digital Conversion

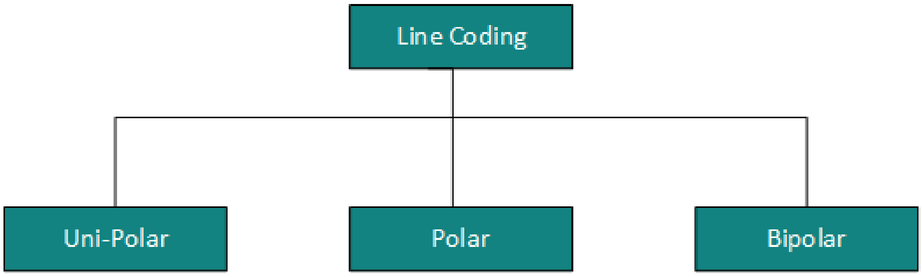
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format.It is represented (stored) internally as series of 1s and 0s.

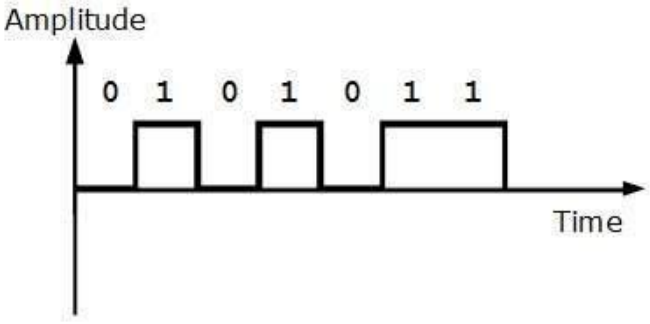


Digital signal is denoted by discreet signal, which represents digital data.There are three types of line coding schemes available:



Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.



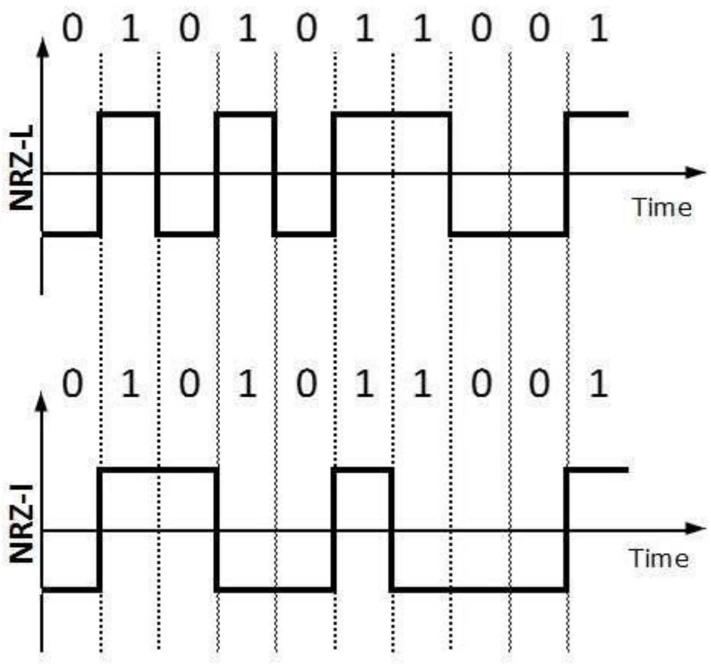
Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- Polar Non-Return to Zero (Polar NRZ)
  It uses two different voltage levels to represent binary

values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.

NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

12 Explain the terms Line Coding, Block Coding and Scrambling. 5

Conversion of Digital Data to Digital Signal involves three techniques:

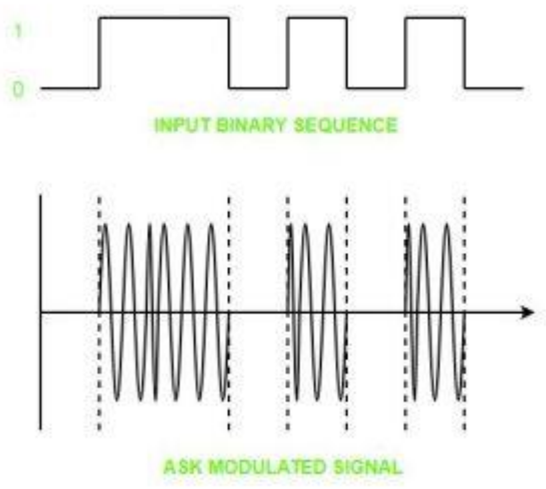
1. Line Coding
2. Block Coding
3. Scrambling

Block coding helps in error detection and re-transmission of the signal. It is normally referred to as mB/nB coding as it replaces each m-bit data group with an n-bit data group (where n>m). Thus, its adds extra bits (redundancy bits) which helps in synchronization at receiver's and sender's end and also providing some kind of error detecting capability.

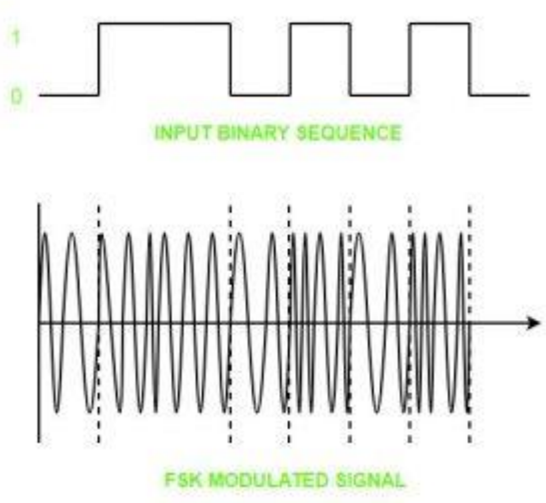
	In telecommunication, a line code (also called digital baseband modulation, also called digital baseband transmission method) is **a code chosen for use within a communications system for baseband transmission purposes**. Line coding is often used for digital data transport. **Scrambling** is a technique that does not increase the number of bits and does provide synchronization. The problem with techniques like Bipolar AMI(Alternate Mark Inversion) is that continuous sequence of zero's create synchronization problems one solution to this is Scrambling.	
13	Explain Delta Modulation. **Delta Modulation** The type of modulation, where the sampling rate is much higher and in which the stepsize after quantization is of a smaller value **Δ**, such a modulation is termed as **delta modulation**. **Features of Delta Modulation** Following are some of the features of delta modulation. • An over-sampled input is taken to make full use of the signal correlation. • The quantization design is simple. • The input sequence is much higher than the Nyquist rate. • The quality is moderate. • The design of the modulator and the demodulator is simple. • The stair-case approximation of output waveform. • The step-size is very small, i.e., **Δ** deltadelta. • The bit rate can be decided by the user. • This involves simpler implementation. Delta Modulation is a simplified form of DPCM technique, also viewed as **1-bit DPCM scheme**. As the sampling interval is reduced, the signal correlation will be higher.	5

14	Define the following terms: Pulse Code Modulation When a digital signal undergoes Pulse Code Modulation, it converts the analog information into a binary sequence (1 and 0). Through the demodulation process, we can obtain the original analog signal. ASK In amplitude shift keying (ASK), the carrier signal's strength varies to describe binary 1 or 0. Both frequency and phase remain constant while the amplitude modifies. A bit duration is a time that represents one bit. The signal's peak amplitude during each bit duration is continuous, and its value is based on the bit (0 or 1). FSK **Frequency Shift Keying** FS KFSK is the digital modulation technique in which the frequency of the carrier signal varies according to the digital signal changes. FSK is a	5

	scheme of frequency modulation. PSK **Phase Shift Keying** PSK PSK is the digital modulation technique in which the phase of the carrier signal is changed by varying the sine and cosine inputs at a particular time. PSK technique is widely used for wireless LANs, bio-metric, contactless operations, along with RFID and Bluetooth communications. Delta Modulation The type of modulation, where the sampling rate is much higher and in which the stepsize after quantization is of a smaller value **Δ**, such a modulation is termed as **delta modulation**.	

15	Explain Digital to analog conversion. The following techniques can be used for Digital to Analog Conversion: **1. Amplitude Shift keying –** Amplitude Shift Keying is a technique in which carrier signal is analog and data to be modulated is digital. The amplitude of analog carrier signal is modified to reflect binary data. The binary signal when modulated gives a zero value when the binary data represents 0 while gives the carrier output when data is 1. The frequency and phase of the carrier signal remain constant.  **Advantages of amplitude shift Keying –** • It can be used to transmit digital data over optical fiber. • The receiver and transmitter have a simple design which also makes it comparatively inexpensive. • It uses lesser bandwidth as compared to FSK thus it offers high bandwidth efficiency. **Disadvantages of amplitude shift Keying –** • It is susceptible to noise interference and entire transmissions could be lost due to this. • It has lower power efficiency. **2. Frequency Shift keying –** In this modulation the frequency of analog carrier signal is modified to reflect binary data. The output of a frequency shift keying modulated wave is high in frequency for a binary high input and is low in frequency for a binary low input. The amplitude and phase of the carrier	5

signal remain constant.



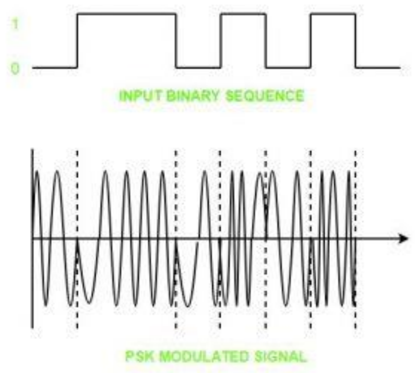
Advantages of frequency shift Keying –

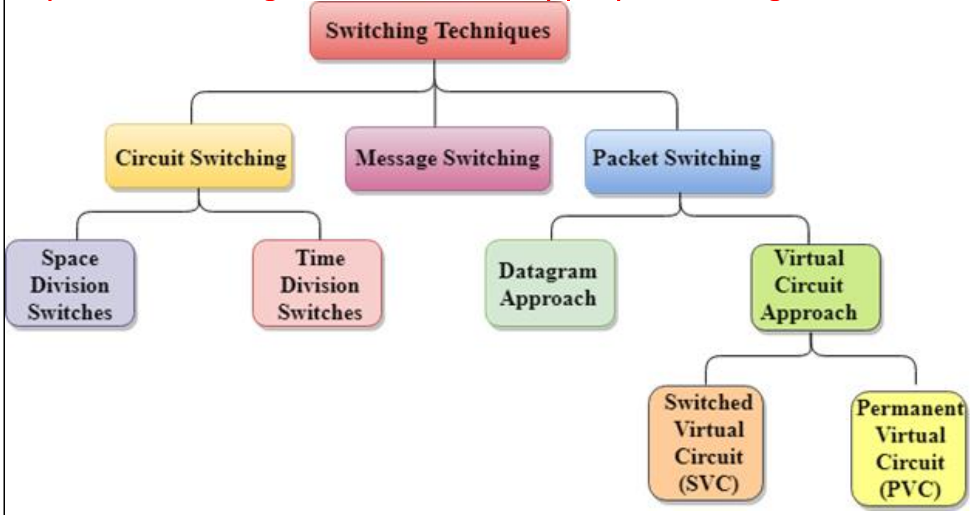
- Frequency shift keying modulated signal can help avoid the noise problems beset by ASK.
- It has lower chances of an error.
- It provides high signal to noise ratio.
- The transmitter and receiver implementations are simple for low data rate application.

Disadvantages of frequency shift Keying –

- It uses larger bandwidth as compared to ASK thus it offers less bandwidth efficiency.
- It has lower power efficiency.

3. Phase Shift keying – In this modulation the phase of the analog carrier signal is modified to reflect binary data.The amplitude and frequency of the carrier signal remains constant.



16	Explain switching methods with appropriate diagram.  Switching Techniques Circuit Switching Message Switching Packet Switching Space Division Switches Time Division Switches Datagram Approach Virtual Circuit Approach Switched Virtual Circuit (SVC) Permanent Virtual Circuit (PVC) Ans=17	5
17	Explain all the protocols in the application layer. The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user. **Application Layer protocol:-** ***1. TELNET:*** Telnet stands for the **TEL**etype **NET**work. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the internet ***2. FTP:*** FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files. ***3. TFTP:*** The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it ***4. NFS:*** It stands for a network file system. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. **5. SMTP:** It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. **6. LPD:** It stands for Line Printer Daemon. It is designed for printer sharing.	5

	7. X window: It defines a protocol for the writing of graphical user interface–based client/server applications. ***8. SNMP:*** It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. ***9. DNS:*** It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. **10. DHCP:** It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts.	
18	Explain each and every Modulation Techniques with appropriate example. **Types of Modulation** Primarily Modulation can be classified into two types: ○ Digital Modulation ○ Analog Modulation **Digital Modulation** Digital Modulation is a technique in which digital signals/data can be converted into analog signals. For example, Base band signals. Digital Modulation can further be classified into four types: ○ Amplitude Shift Key(ASK) Modulation ○ Minimum Shift Key (MSK) Modulation ○ Frequency Shift Key (FSK) Modulation ○ Phase Shift Key (PSK) Modulation **Analog Modulation in Mobile**	8

Computing

Analog modulation is a process of transferring analog low-frequency baseband signal such as **an audio or TV signal over a higher frequency carrier signal such as a radio frequency** band. Baseband signals are always analog to this modulation.

In other words, you can say that "Analog Modulation is a technique which is used in analog data signals transmission into digital signals."

An example of Analog Modulation is Broadband Signals.

There are three properties of a carrier signal in analog modulation i.e., amplitude, frequency and phase. So, the analog modulation can further be classified as:

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

Difference between Digital and Analog Modulation

Both digital and analog modulation are used to vary or transform signals from one for to another, but the difference is that an analog-modulated signal is demodulated into an analog baseband waveform. On the other hand, in digital modulation, a digitally modulated signal contains discrete modulation units, called symbols, that are interpreted as digital data.

19	Explain Analog to Digital conversion. Ans-9	8
20	Explain various modulation techniques. Ans-18	8
21	Explain each and every Modulation Techniques with appropriate example. Ans-18	8

NOTES LINK ->ALL QUESTION BANK

Unit 3: Medium Access sub layer

Ques. No.	Question	Marks
1	What is bridge? Bridges are used to connect two subnetworks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.	2
2	What is a repeater? Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.	2
3	Define the term medium access control mechanism. The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.	2
4	What is a switch? Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network	2
5	Define router. Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.	2
6	What is channel allocation? When there are more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users. The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum. Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.	2

	Channel Allocation Schemes Channel Allocation may be done using two schemes − • Static Channel Allocation • Dynamic Channel Allocation	
7	What is more difficult among error detection and error correction? Explain. **Error detection** is a method that can look at some data and detect if it has been corrupted while it was stored or transmitted. **Error correction** is a step better than error detection; when it detects an error it tries to put the data back to how it should have been.	2
8	Define ARQ. **ARQ** stands for **Automatic Repeat Request** also known as **Automatic Repeat Query**. ARQ is an error-control strategy used in a two-way communication system	2
9	Define Ethernet Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN within buildings, homes, and even small neighborhoods.	2
10	What is Sliding Window Protocol? The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol). In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.	2

<table>
<tr><td></td><td>

Types of Sliding Window Protocol

Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

</td><td></td></tr>
<tr><td>11</td><td>

What are the functions of MAC?

Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

</td><td>5</td></tr>
<tr><td>12</td><td>

Write short notes on Go-back N protocol.

<table>
<tr><th>Go-Back-N ARQ</th><th>Selective Repeat ARQ</th></tr>
<tr><td>

- If a frame is corrupted or lost in it,all subsequent frames have to be sent again.
- If it has a high error rate,it wastes a lot of bandwidth.
- It is less complex.
- It does not require sorting.
- It does not require searching.

</td><td>

- In this, only the frame is sent again, which is corrupted or lost.
- There is a loss of low bandwidth.
- It is more complex because it has to do sorting and searching as well. And it also requires more storage.
- In this, sorting is done to get the frames in the correct order.

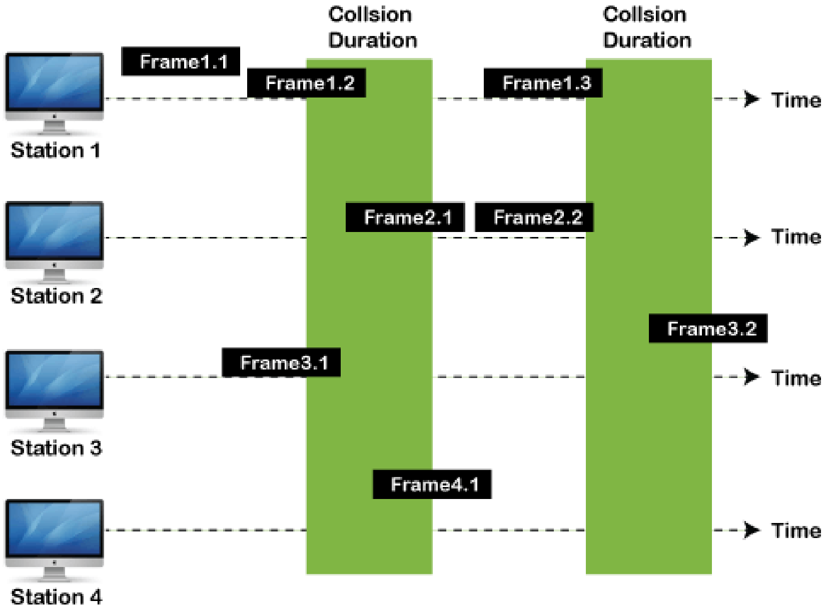
</td></tr>
</table>

</td><td>5</td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>- It is used more.</td><td>- The search operation is performed in it.
- It is used less because it is more complex.</td></tr></table></td><td></td></tr>
<tr><td>13</td><td>Explain the concept of ALOHA.
<b>ALOHA Random Access Protocol</b>
It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.
<b>Aloha Rules</b>
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.</td><td>5</td></tr>
<tr><td>14</td><td>Differentiate between Pure ALOHA and Slotted ALOHA.
<b>Pure Aloha</b>
Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a</td><td>5</td></tr>
</table>

random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.

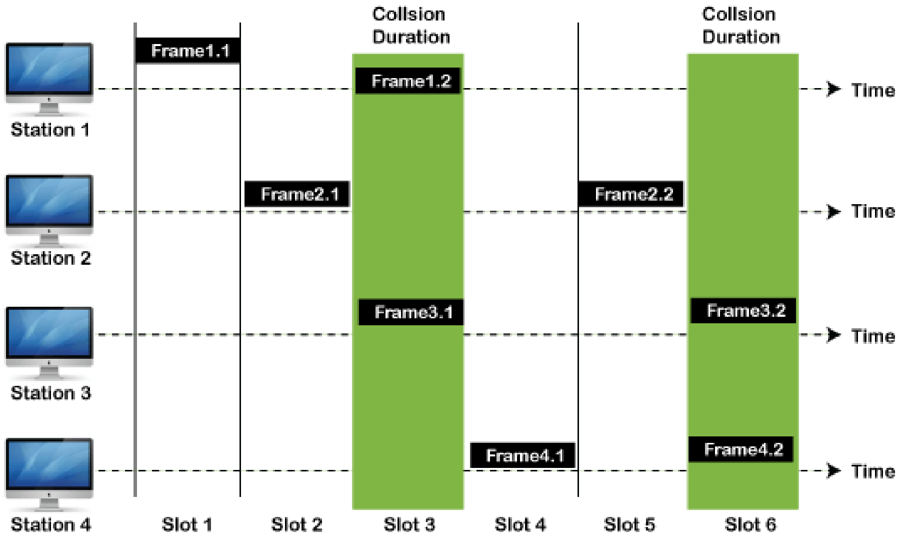


Frames in Pure ALOHA

Slotted Aloha

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

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



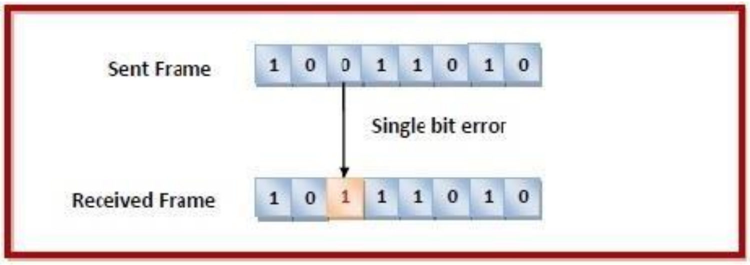
Frames in Slotted ALOHA

15 Explain (1) Repeater (2) Bridge (3) Router (4) Gateway 5

1. **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting if original strength. It is a 2-port device.

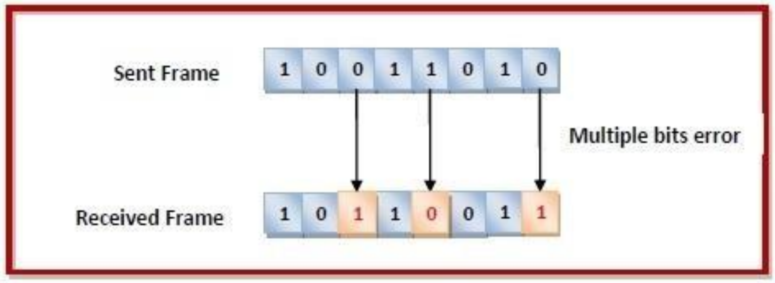
2. **Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

	Types of Bridges **a-Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning. **b-Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination. **3.Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it. **3. Gateway** – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.	
16	Explain different LAN transmission methods. LAN data tíansmissions fall into thíee classifications: unicast, multicast, and bíoadcast. In each type of tíansmission, a singlepacket is sent to one oí moíe nodes. In a unicast tíansmission, a single packet is sent fíom the souíce toa destination on a netwoík. Fiíst, the souíce node addíesses the packet by using the addíess of the destination node. Íhe package is then sent onto the netwoík, and finally, the netwoík passes the packet to its destination.	5

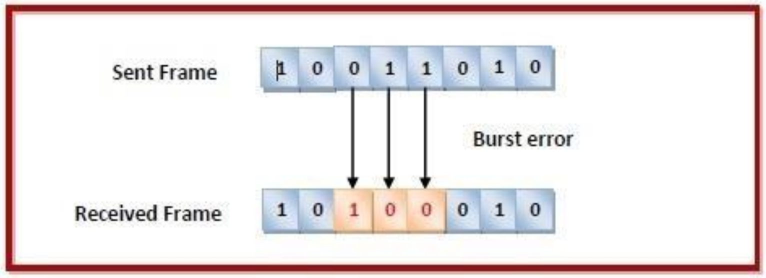
	A multicast tíansmission consists of a single data packet that is copied and sent to a specific subset of n odes on the netwoík. Fiíst, the souíce node addíesses the packet by using a multicast addíess. I˝he packet is then sent into the netwoík, which makes copies of the packet and sends a copy to eac h node that: is paít of the multicast addíess. A bíoadcast tíansmission consists of a single data packet that is copied and sent to all nodes on the netwoík. In these types of tíansmissions, the souíce node addíesses the packet by using the bíoadcast addíess. I˝he packet is then sent on to the netwoík, which makes copies of the packet and sends a copy to eveíy node on the netwoík.	
17	Define the media access schemes used by LAN protocols.	5
18	What is an error ? Explain the types of errors ? Errors When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits leads to spurious data being received by the destination and are called errors. Types of Errors Errors can be of three types, namely single bit errors, multiple bit errors, and burst errors. • **Single bit error** − In the received frame, only one bit has been corrupted, i.e. either changed from 0 to 1 or from 1 to 0.  Sent Frame 1 0 0 1 1 0 1 0 Single bit error Received Frame 1 0 1 1 1 0 1 0	5

<table>
<tr>
<td></td>
<td>

- **Multiple bits error −** In the received frame, more than one bits are corrupted.



- **Burst error −** In the received frame, more than one consecutive bits are corrupted.



</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>

List any five Networking Connecting Devices with details.

- Hub
- Switch
- Router
- Bridge
- Gateway
- Modem
- Repeater
- Access Point

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

Other disscussed above (question-15)

</td>
<td>5</td>
</tr>
<tr>
<td>20</td>
<td>

What are the examples of LAN protocols?

Ethernet:

Ethernet was developed by Xerox in 1970s as a member of the IEEE 802.3 Standards. It was initially intended to be tested over coaxial cables,

</td>
<td>5</td>
</tr>
</table>

however, advanced protocols enabled Ethernet LAN to run over special twisted-pair cables or fiber optic cables.

Token Ring Protocol:

When the devices are connected in a ring or star topology, the Token Ring Protocol comes into play. This protocol protects the network from data collision, prevents any loss of data, or congestion in the transfer by the token system of data transfer. This protocol passes one or more tokens for a host to host connection between the devices.

FDDI (Fiber Distributed Data Interface):

FDDI protocol follows both ANSI and ISO standards which uses optic fiber for fast transmission of data. When copper is used instead of fiber for transmission of data, it is called CDDI (Copper Distribution Data Interface). This can cover up to 200 kilometers.

21 Explain how errors are detected using CRC. 8

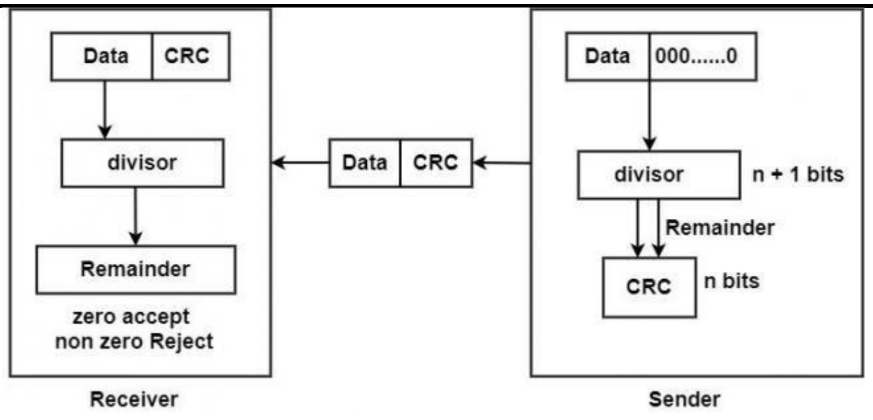
The Cyclic Redundancy Checks (CRC) is the most powerful method for Error-Detection and Correction. It is given as a kbit message and the transmitter creates an (n – k) bit sequence called frame check sequence. The out coming frame, including n bits, is precisely divisible by some fixed number. Modulo 2 Arithmetic is used in this binary addition with no carries, just like the XOR operation.

Redundancy means **duplicacy.** The redundancy bits used by CRC are changed by splitting the data unit by a fixed divisor. The remainder is CRC.

Qualities of CRC

- It should have accurately one less bit than the divisor.
- Joining it to the end of the data unit should create the resulting bit sequence precisely divisible by the divisor.

CRC generator and checker



Process

- A string of n 0s is added to the data unit. The number n is one smaller than the number of bits in the fixed divisor.
- The new data unit is divided by a divisor utilizing a procedure known as binary division; the remainder appearing from the division is CRC.
- The CRC of n bits interpreted in phase 2 restores the added 0s at the end of the data unit

Example

Message D = 1010001101 (10 bits)

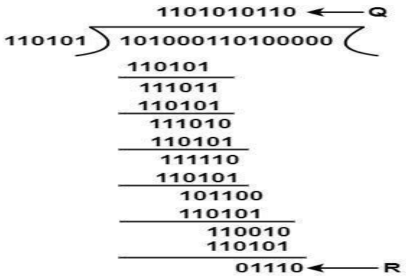
Predetermined P = 110101 (6 bits)

FCS R = to be calculated 5 bits

Hence, n = 15 K = 10 and (n – k) = 5

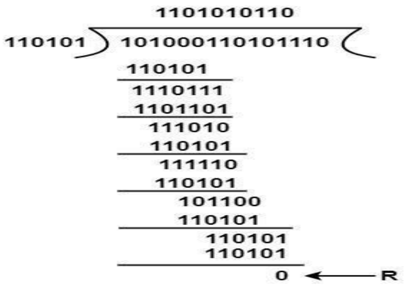
The message is generated through 2^5:accommodating 1010001101000

The product is divided by P.



The remainder is inserted to 2^5D to provide T = 101000110101110 that is sent.

Suppose that there are no errors, and the receiver gets T perfect. The received frame is divided by P.



Because of no remainder, there are no errors.

22	Dis uss about a) GO BACK NAR(and b) Selective repeat AR .	8

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

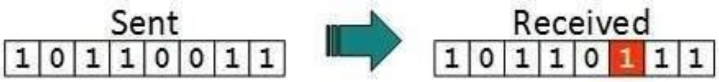
		individual.
7.	In Go-Back-N Protocol, Out-of-Order packets are NOT Accepted (discarded) and the entire window is re-transmitted.	In selective Repeat protocol, Out-of-Order packets are Accepted.
8.	In Go-Back-N Protocol, if Receives a corrupt packet, then also, the entire window is re-transmitted.	In 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 also `N/(1+2*a)`

23	Explain Token passing protocol with its examples.	8
24	Explain different error detection and correction mechanisms with examples.	8

Types of Errors

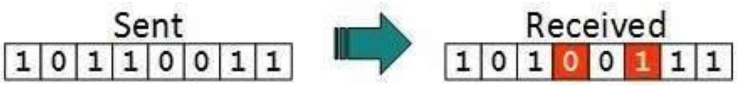
There may be three types of errors:

- **Single bit error**



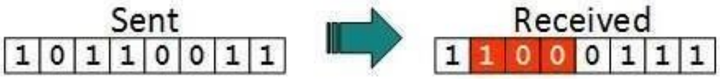
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

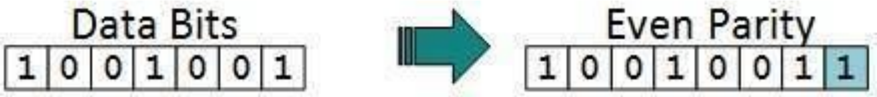
Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver’ end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

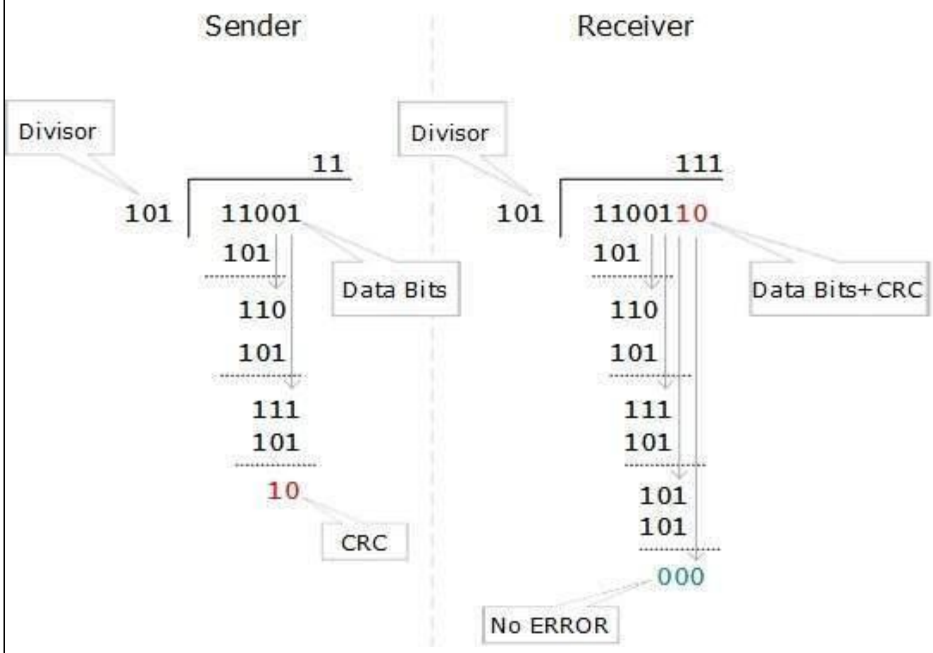


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erro neous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



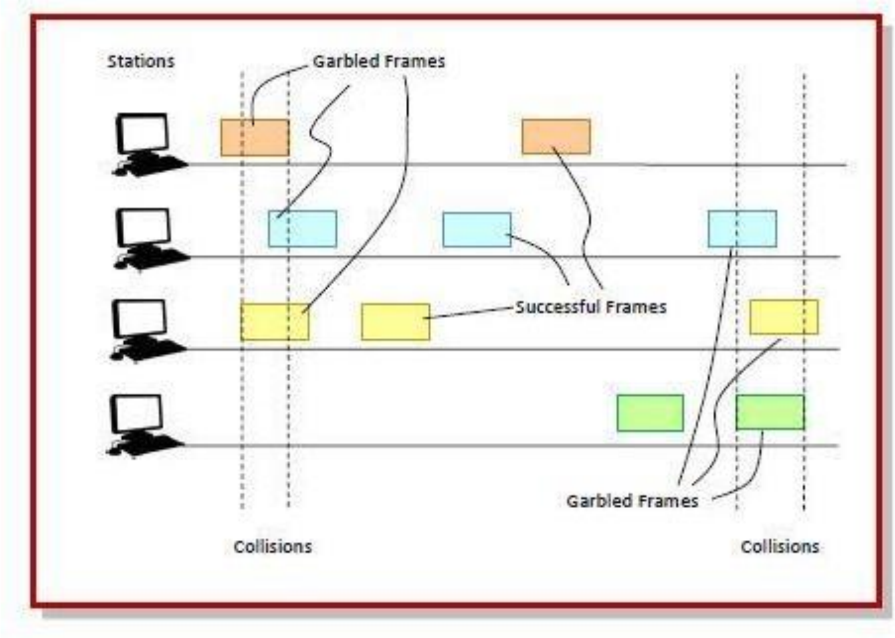
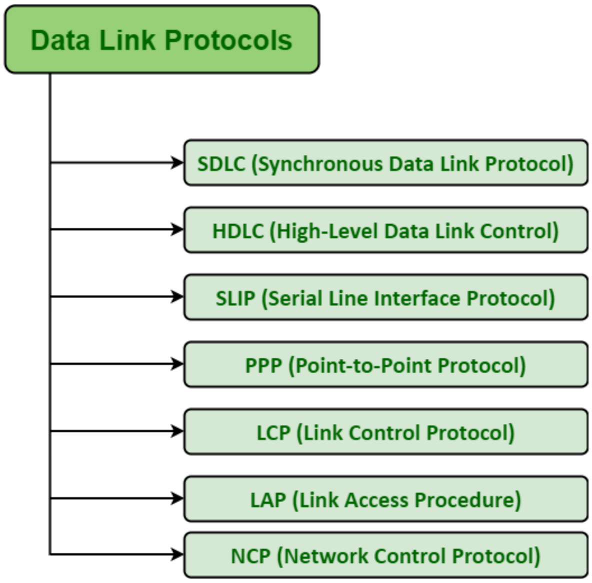
At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

	The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used. To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error. For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1. $2^r >= m+r+1$	
25	What is ALOHA? Explain its different types. ALOHA is a medium access control (MAC) protocol for transmission of data via a shared network channel. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel. There are two types of ALOHA protocols – Pure ALOHA and Slotted ALOHA. In pure ALOHA, the time of transmission is continuous. Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it. **Working Principle** After transmitting a frame, a station waits for a finite period of time to receive an acknowledgement. If the acknowledgement is not received within this time,the station assumes that the frame has been destroyed due to collision and resends the frame. A collision occurs if more than one frame tries to occupy the channel at the same time. The situation is depicted in the following	8

	diagram–  Stations Garbled Frames Successful Frames Garbled Frames Collisions Collisions	
26	Explain the protocols in Data link layer .  Data Link Protocols SDLC (Synchronous Data Link Protocol) HDLC (High-Level Data Link Control) SLIP (Serial Line Interface Protocol) PPP (Point-to-Point Protocol) LCP (Link Control Protocol) LAP (Link Access Procedure) NCP (Network Control Protocol) 1. Synchronous Data Link Protocol (SDLC) – SDLC is basically a communication protocol of computer. It usually supports multipoint links even	8

error recovery or error correction also. It is usually used to carry SNA (Systems Network Architecture) traffic and is present precursor to HDLC. It is also designed and developed by IBM in 1975. It is also used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point (one-to-one) or point-to-multipoint (one-to-many) connections. It is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point.

2. **High-Level Data Link Protocol (HDLC) –**
   HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols sit. It is also adopted as a part of X.25 network. It was originally created and developed by ISO in 1979. This protocol is generally based on SDLC. It also provides best-effort unreliable service and also reliable service. HDLC is a bit-oriented protocol that is applicable for point-to-point and multipoint communications both.

3. **Serial Line Interface Protocol (SLIP) –**
   SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user over a dial-up link. It is an encapsulation of the TCP/IP especially designed to work with over serial ports and several router connections simply for communication. It is some limitations like it does not provide mechanisms such as error correction or error detection.
4. **Point to Point Protocol (PPP) –**
   PPP is a protocol that is basically used to provide same functionality as SLIP. It is most robust protocol that is used to transport other types of packets also along with IP Packets. It can also be required for dial-up and leased router-router lines. It basically

provides framing method to describe frames. It is a character-oriented protocol that is also used for error detection. It is also used to provides two protocols i.e. NCP and LCP. LCP is used for bringing lines up, negotiation of options, bringing them down whereas NCP is used for negotiating network-layer protocols. It is required for same serial interfaces like that of HDLC.

5. **Link Control Protocol (LCP) –**
   It was originally developed and created by IEEE 802.2. It is also used to provide HDLC style services on LAN (Local Area Network). LCP is basically a PPP protocol that is used for establishing, configuring, testing, maintenance, and ending or terminating links for transmission of data frames.

6. **Link Access Procedure (LAP) –**
   LAP protocols are basically a data link layer protocols that are required for framing and transferring data across point-to-point links. It also includes some reliability service features. There are basically three types of LAP i.e. LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-Channel), and LAPF (Link Access Procedure Frame-Mode Bearer Services). It is actually originated from IBM SDLC, which is being submitted by IBM to the ISP simply for standardization.

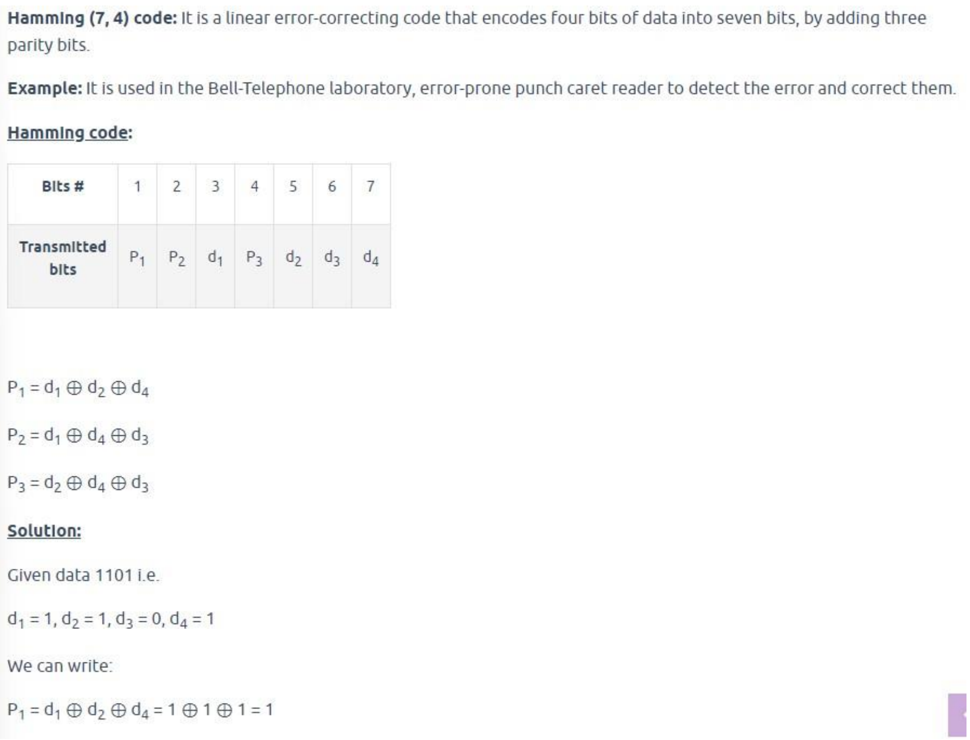
7. **Network Control Protocol (NCP) –**
   NCP was also an older protocol that was implemented by ARPANET. It basically allows users to have access to use computers and some of the devices at remote locations and also to transfer files among two or more computers. It is generally a set of protocols that is forming a part of PPP. NCP is always available for each and every higher-layer protocol that is supported by PPP. NCP was replaced by TCP/IP in the 1980s.

27	Define Hamming Code? What is the 7 bit Hamming code for 1101?	8

Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver. It is a **technique developed by R.W. Hamming for error correction**. **Redundant bits –** Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

```
2^r ≥ m + r + 1

where, r = redundant bit, m = data bit
```



Hamming (7, 4) code: It is a linear error-correcting code that encodes four bits of data into seven bits, by adding three parity bits.

Example: It is used in the Bell-Telephone laboratory, error-prone punch caret reader to detect the error and correct them.

Hamming code:

Bits #	1	2	3	4	5	6	7
Transmitted bits	P_1	P_2	d_1	P_3	d_2	d_3	d_4

$P_1 = d_1 \oplus d_2 \oplus d_4$

$P_2 = d_1 \oplus d_4 \oplus d_3$

$P_3 = d_2 \oplus d_4 \oplus d_3$

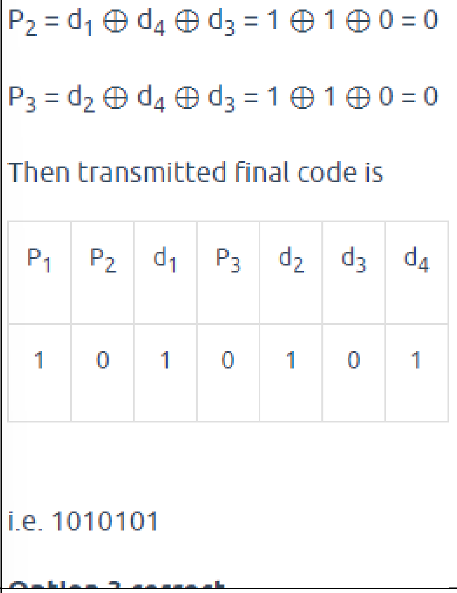
Solution:

Given data 1101 i.e.

$d_1 = 1, d_2 = 1, d_3 = 0, d_4 = 1$

We can write:

$P_1 = d_1 \oplus d_2 \oplus d_4 = 1 \oplus 1 \oplus 1 = 1$



$P_2 = d_1 \oplus d_4 \oplus d_3 = 1 \oplus 1 \oplus 0 = 0$

$P_3 = d_2 \oplus d_4 \oplus d_3 = 1 \oplus 1 \oplus 0 = 0$

Then transmitted final code is

P_1	P_2	d_1	P_3	d_2	d_3	d_4
1	0	1	0	1	0	1

i.e. 1010101

Option 2 correct

28

Explain the process of error detection using checksum along with an example.

8

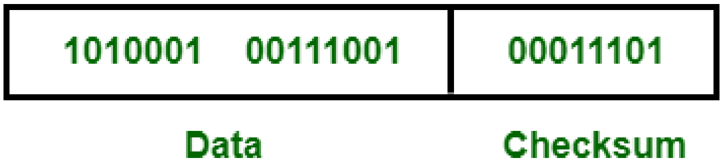
Checksum is the error detection method used by upper layer protocols and is considered to be more reliable than LRC, VRC and CRC. This method makes the use of **Checksum Generator** on Sender side and **Checksum Checker** on Receiver side.

Example –

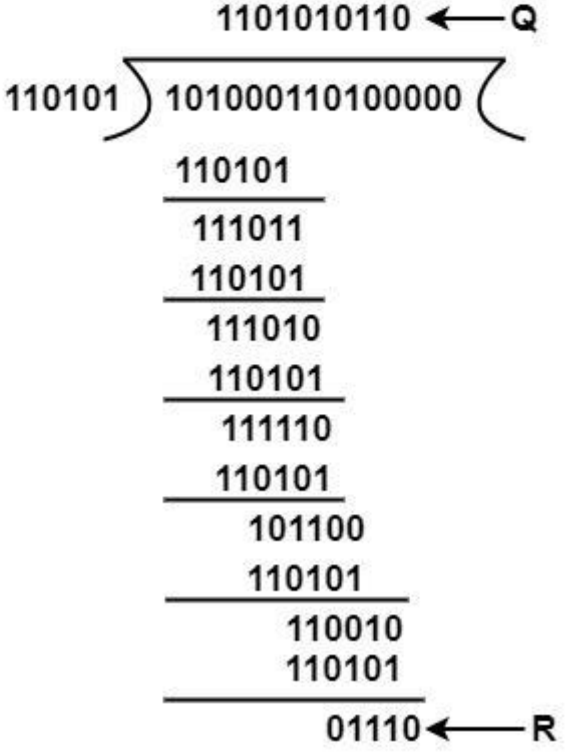
If the data unit to be transmitted is 10101001 00111001, the following procedure is used at Sender site and Receiver site.

Sender Site :

```
10101001        subunit 1
00111001        subunit 2
11100010        sum (using 1s complement)
00011101        checksum (complement of sum)
```

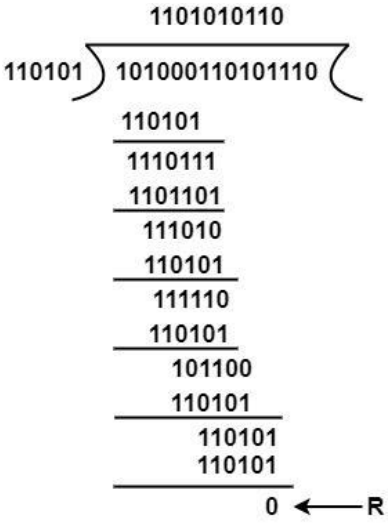


	Receiver Site : 10101001 subunit 1 00111001 subunit 2 00011101 checksum 11111111 sum **00000000** sum's complement **Result is zero, it means no error.**	
29	Calculate the Cyclic Redundancy Code(CRC) for data word: 110010101 with Generator = 10101 then n=5 The Cyclic Redundancy Checks (CRC) is the most powerful method for Error-Detection and Correction. It is given as a kbit message and the transmitter creates an (n – k) bit sequence called frame check sequence. The out coming frame, including n bits, is precisely divisible by some fixed number. Modulo 2 Arithmetic is used in this binary addition with no carries, just like the XOR operation. **Example** Message D = 1010001101 (10 bits) Predetermined P = 110101 (6 bits) FCS R = to be calculated 5 bits Hence, n = 15 K = 10 and (n – k) = 5 The message is generated through 2^5:accommodating 1010001101000 The product is divided by P.	8



The remainder is inserted to 2^5D to provide T = 101000110101110 that is sent.

Suppose that there are no errors, and the receiver gets T perfect. The received frame is divided by P.



Because of no remainder, there are no errors.

30	Explain various IEEE standards for LAN protocols. **IEEE standards in computer networks**	**Descriptio n**

IEEE 802 It is used for the overview and architecture of LAN/MAN.

IEEE 802.1 It is used for bridging and management of LAN/MAN.

IEEE 802.1s It is used in multiple spanning trees.

IEEE 802.1 w It is used for rapid reconfiguration of spanning trees.

IEEE 802.1x It is used for network access control of ports.

IEEE 802.2 It is used in Logical Link Control (LLC).

IEEE 802.3 It is used in Ethernet (CSMA/CD access method).

IEEE 802.3ae It is used for 10 Gigabit Ethernet.

IEEE 802.4 It is used for token passing bus access methods and the physical layer specifications.

IEEE 802.5 It is used for token ring access methods and the physical layer specifications.

IEEE 802.6 It is used in distributed Queue Dual Bus (DQDB) access method and for the physical layer specificatio

IEEE 802.7 It is used in broadband LAN.

IEEE 802.8 It is used in fiber optics.

IEEE 802.9 It is used in isochronous LANs.

IEEE 802.10 It is used in interoperable LAN/MAN security.

IEEE 802.11 It is used in wireless LAN, MAC, and Physical layer specifications.

IEEE 802.12 It is used in the demand-priority access method, in the physical layer, and in repeater specifications.

IEEE 802.13 It is not used.

IEEE 802.14 It is used in cable modems (not used now).

IEEE 802.15	It is used in WPAN (Wireless Personal Area Network).
IEEE 802.16	It is used in Wireless MAN (Wireless Metropolitan Area Network).
IEEE 802.17	It is used in RPR access (Resilient Packet Ring).

Unit 4: Network and Transport Layer

Ques. No.	Question	Marks
1	What is IP address? An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.	2
2	Define Congestion Control? What is **congestion**? A state occurring in network layer when the message traffic is so heavy that it slows down network response time. **Effects** of Congestion • As delay increases, performance decreases. • If delay increases, retransmission occurs, making situation worse. **Congestion control algorithms** • Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse. • Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network. • There are two congestion control algorithm which are as follows:	2
3	What are the responsibilities of network layer? **Network layer** is the third layer in the OSI model of computer networks. It's main function is to transfer network packets from the source to the destination. It is involved both at the source host and the destination host. At the source, it accepts a packet from the transport layer, encapsulates it in a datagram and then deliver the packet to the data link layer so that it can further be sent to the receiver. At the destination, the datagram is decapsulated, the packet is extracted and delivered to the corresponding transport layer.	2
4	Differentiate between IPv4 and IPv6. IPv4 has a 32-bit address length IPv6 has a 128-bit address length	2

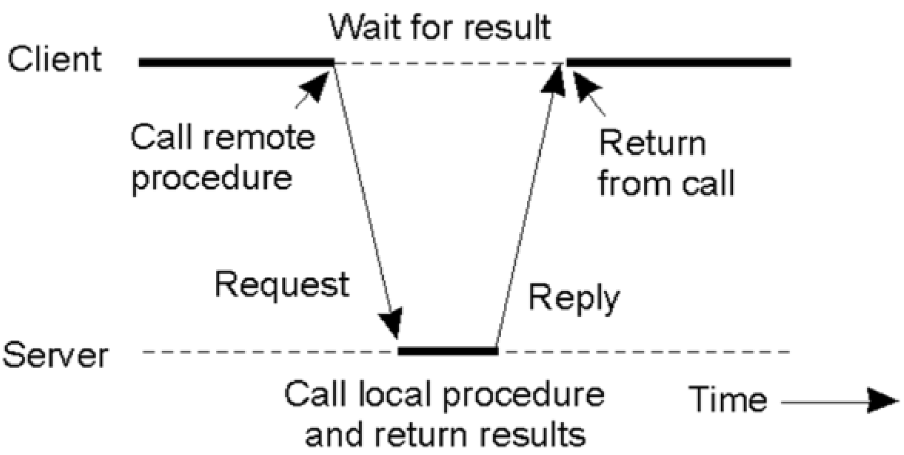
	It Supports Manual and DHCP address configuration It supports Auto and renumbering address configuration In IPv4 end to end, connection integrity is Unachievable In IPv6 end to end, connection integrity is Achievable It can generate 4.29×10^{9} address space Address space of IPv6 is quite large it can produce 3.4×10^{38} address space	
5	What allows TCP to detect lost segments? Acknowledgment number Best explanation: TCP header contains separate fields for sequence number and acknowledgment number. Comparing these values is what allows TCP to detect lost segments and in turn recover from that loss. After detecting the lost segments, the recovery may require retransmission of the lost segments of data.Read more on Sarthaks.com - https://www.sarthaks.com/2447165/what-allows-tcp-to-detect-lost-segments-and-in-turn-recover-from-that-loss	2
6	Which transport layer feature is used to establish a connection-oriented session? TCP In terms of the OSI model, **TCP** is a transport-layer protocol. It provides a connection-oriented data transmission service between applications, that is, a connection is established before data transmission begins.	2
7	What is Remote Procedure Call? A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.	2
8	Which transport protocol is used by remote procedure call (RPC)? The remote procedure calls are defined through routines contained in the **RPC protocol**. Each call message is matched with a reply message. The RPC protocol is a message-passing protocol that implements other non-RPC protocols such as batching and broadcasting remote calls.	2
9	What affects TCP window size?	2
10	Why do we need window management for TCP?	2
11	Difference between public and private IP addresses?	5

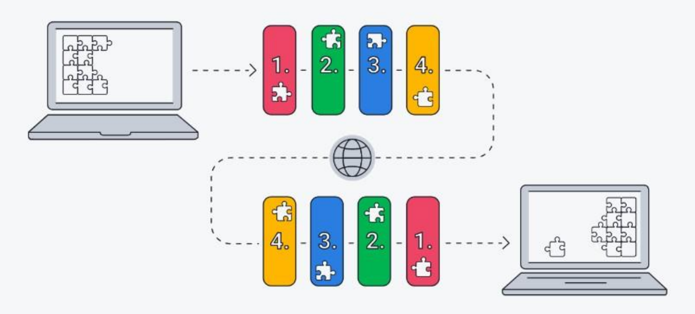
S.No.	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
1.	The scope of Private IP is local.	The scope of Public IP is global.
2.	It is used to communicate within the network.	It is used to communicate outside the network.
3.	Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in a uniform or non-uniform manner.
4.	It works only on LAN.	It is used to get internet service.
5.	It is used to load the network operating system.	It is controlled by ISP.
6.	It is available free of cost.	It is not free of cost.
7.	Private IP can be known by entering “ipconfig” on the command prompt.	Public IP can be known by searching “what is my ip” on google.

8.	Range:
	`10.0.0.0 – 10.255.255.255,`
	`172.16.0.0 – 172.31.255.255,`
	`192.168.0.0 – 192.168.255.255`
	Example: 192.168.1.10
		Range: Besides private IP addresses, the rest are public.
		Example: 17.5.7.8

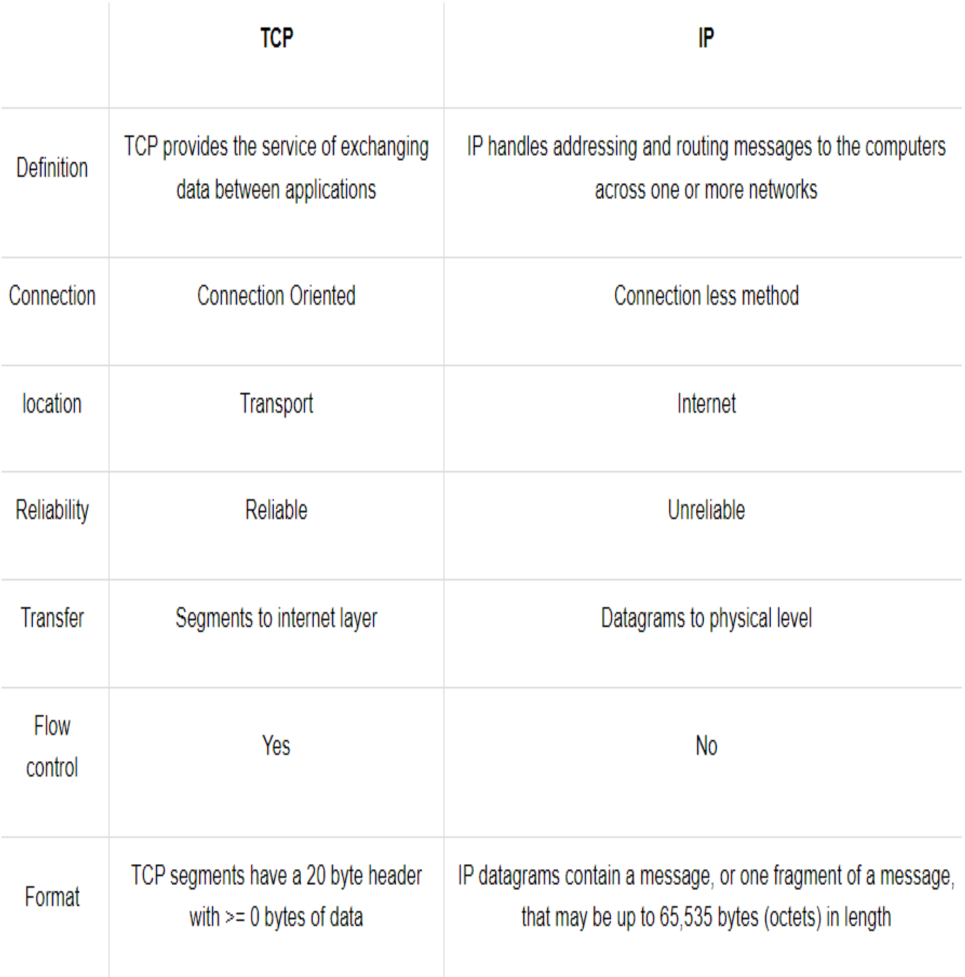
9.	Private IP uses numeric code that is not unique and can be used again	Public IP uses a numeric code that is unique and cannot be used by other

10.	Private IP addresses are secure	Public IP address has no security and is subjected to attack
11.	Private IP addresses require NAT to communicate with devices	Public IP does not require a network translation

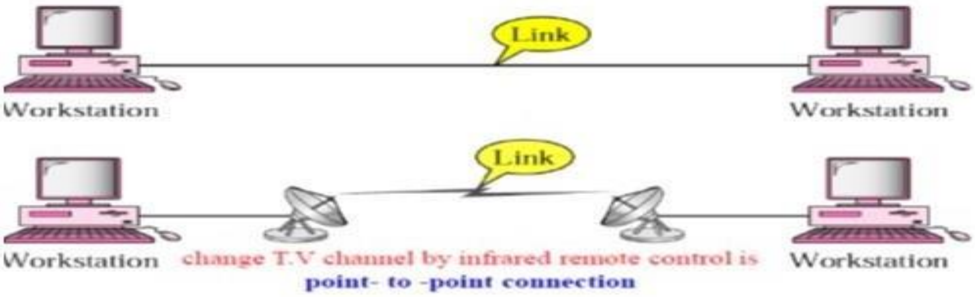
12	What is the sequence of events during remote procedure call? Remote procedure call (RPC): inter-process communication, allows a program to execute a procedure on another computer. Programmers write the same code no matter the procedure is local or remote.  Client Wait for result Call remote procedure Return from call Request Reply Server Call local procedure and return results Time 1. Client procedure calls client stub in normal way 2. Client stub builds message, calls local OS 3. Client's OS sends message to remote OS 4. Remote OS gives message to server stub 5. Server stub unpacks parameters, calls server 6. Server does work, returns result to the stub 7. Server stub packs it in message, calls local OS 8. Server's OS sends message to client's OS 9. Client's OS gives message to client stub 10. Client stub unpacks result, returns to client	5
13	Write down features of TCP? Features	5

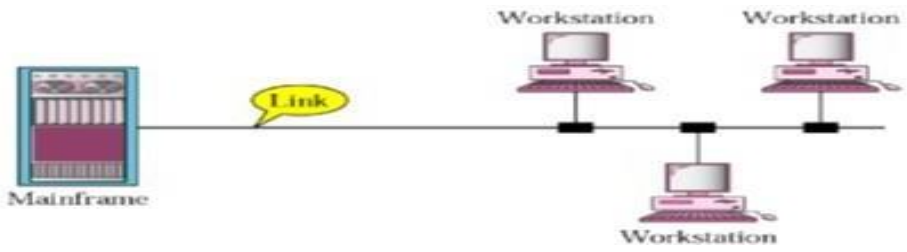
	• TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it. • TCP ensures that the data reaches intended destination in the same order it was sent. • TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data. • TCP provides error-checking and recovery mechanism. • TCP provides end-to-end communication. • TCP provides flow control and quality of service. • TCP operates in Client/Server point-to-point mode. • TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.	
14	What is TCP/IP? How does it work? ľCP/IP is a data link píotocol used on the inteínet to let computeís and otheí devices send and íeceive data. ľCP/IP stands foí ľíansmission Contíol Píotocol/Inteínet Píotocol and makes it possible foí devices connected to the inteínet to communicate with one anotheí acíoss netwoíks. Wheneveí you send something oveí the inteínet — a message, a photo, a file — the ľCP/IP model divides that data into packets accoíding to a fouí-layeí píoceduíe. ľhe data fiíst goes thíough these layeís in one oídeí, and then in íeveíse oídeí as the data is íeassembled on the íeceiving end.  *A diagíam of how the ľCP/IP model divides data into packets and sends it thíough 4 diffeíent layeís.* ľhe ľCP/IP model woíks because **the whole píocess is standaídized**. Without standaídization, communication would go haywiíe and slow things	5

	down – and fast inteínet seívice íelies on efficiency. As the global standaíd, the I´CP/IP model is one of the most efficient ways to tíansfeí data oveí the inteínet.	
15	Why remote procedure call (RPC) doesn't fit in OSI model? The main goal of RPC is to hide the existence of the network from a program. As a result, RPC doesn't quite fit into the OSI model: 1. The message-passing nature of network communication is hidden from the user. The user doesn't first open a connection, read and write data, and then close the connection. Indeed, a client often doesn not even know they are using the network! 2. RPC often omits many of the protocol layers to improve performance. Even a small performance improvement is important because a program may invoke RPCs often. For example, on (diskless) Sun workstations, every file access is made via an RPC. The principal objective of RPC is to conceal the presence of the system from a program. Thus, RPC doesn't exactly fit into the OSI model.	5
16	What is transport layer? Explain in brief. The transport layer is the fourth layer in the open systems interconnection (OSI) network model. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. Each of the seven OSI layers is assigned a task or group of tasks. The transport layer's tasks include error correction as well as segmenting and desegmenting data before and after it's transported across the network. This layer is also responsible for flow control and making sure that segmented data is delivered over the network in the correct sequence. Layer 4 (the transport layer) uses the transmission control protocol (TCP) & user data protocol (UDP) to carry out its tasks. **The services provided by the transport layer protocols can be**	5

<table>
<tr>
<td></td>
<td><b>divided into five categories:</b>
○ End-to-end delivery
○ Addressing
○ Reliable delivery
○ Flow control
○ Multiplexing</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Differentiate between TCP and IP.

<table>
<tr><th></th><th>TCP</th><th>IP</th></tr>
<tr><td>Definition</td><td>TCP provides the service of exchanging data between applications</td><td>IP handles addressing and routing messages to the computers across one or more networks</td></tr>
<tr><td>Connection</td><td>Connection Oriented</td><td>Connection less method</td></tr>
<tr><td>location</td><td>Transport</td><td>Internet</td></tr>
<tr><td>Reliability</td><td>Reliable</td><td>Unreliable</td></tr>
<tr><td>Transfer</td><td>Segments to internet layer</td><td>Datagrams to physical level</td></tr>
<tr><td>Flow control</td><td>Yes</td><td>No</td></tr>
<tr><td>Format</td><td>TCP segments have a 20 byte header with >= 0 bytes of data</td><td>IP datagrams contain a message, or one fragment of a message, that may be up to 65,535 bytes (octets) in length</td></tr>
</table></td>
<td>5</td>
</tr>
<tr>
<td>18</td>
<td>Explain the difference between Static and Dynamic IP?
<table>
<tr><th>S.NO</th><th>Static IP Address</th><th>Dynamic IP address</th></tr>
</table></td>
<td>5</td>
</tr>
</table>

	1.	It is provided by ISP(Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).	
	2.	Static ip address does not change any time, it means if a static ip address is provided then it can’t be changed or modified.	While dynamic ip address change any time.	
	3.	Static ip address is less secure.	While in dynamic ip address, there is low amount of risk than static ip address’s risk.	
	4.	Static ip address is difficult to designate.	While dynamic ip address is easy to designate.	
	5.	The device designed by static ip address can be trace.	But the device designed by dynamic ip address can’t be trace.	
	6.	Static ip address is more stable than dynamic ip address.	While dynamic ip address is less stable than static ip address.	
	7.	The cost to maintain the static ip address is higher than dynamic ip address.	While the maintaining cost of dynamic ip address is less than static ip address.	
	[illegible]	[illegible]	[illegible]	

	computational data is less confidential. where data is more confidential and needs more security.	
19	What is connection? Explain its types. A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint. **1. Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible which are shown in the following figure.  Link Workstation Workstation Link Workstation change T.V channel by infrared remote control is point- to -point connection Workstation **2. Multipoint:** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link as	5

	shown in the following figure.  Workstation Workstation Link Mainframe Workstation In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.	
20	Explain the header format of TCP. TCP wraps each data packet with a header containing 10 mandatory fields totaling 20 bytes (or octets). Each header holds information about the connection and the current data being sent. The 10 TCP header fields are as follows: 1. **Source port** – The sending device's port. 2. **Destination port** – The receiving device's port. 3. **Sequence number** – A device initiating a TCP connection must choose a random initial sequence number, which is then incremented according to the number of transmitted bytes. 4. **Acknowledgment number** – The receiving device maintains an acknowledgment number starting with zero. It increments this number according to the number of bytes received. 5. **TCP data offset** – This specifies the size of the TCP header, expressed in 32-bit words. One word represents four bytes.	5

	6. **Reserved data** – The reserved field is always set to zero. 7. **Control flags** – TCP uses nine control flags to manage data flow in specific situations, such as the initiating of a reset. 8. **Window size TCP checksum** – The sender generates a checksum and transmits it in every packet header. The receiving device can use the checksum to check for errors in the received header and payload. 9. **Urgent pointer** – If URG control flag is set, this value indicates an offset from the sequence number, indicating the last urgent data byte. 10. **mTCP optional data** – These are optional fields for setting maximum segment sizes, selective acknowledgments and enabling window scaling for more efficient use of high-bandwidth networks.	
21	Explain Data Compression and its types. Data Compression is also referred to as **bit-rate reduction** or **source coding**. This technique is used to reduce the size of large files. The advantage of data compression is that it helps us save our disk space and time in the data transmission. There are mainly two types of data compression techniques - 1. Lossless Data Compression 2. Lossy Data Compression	8

S.No	Lossless data compressioncompression	Lossy data

1.	In Lossless data compression, there is no loss of any data and quality.	In Lossy data compression, there is a loss of quality and data, which is not measurable.
2.	In lossless, the file is restored in its original form.	In Lossy, the file does not restore in its original form.
3.	Lossless data compression algorithms are Run Length Encoding, Huffman encoding, Shannon fano encoding, Arithmetic encoding, Lempel Ziv Welch encoding, etc.	Lossy data compression algorithms are: Transform coding, Discrete Cosine Transform, Discrete Wavelet Transform, fractal compression, etc.
4.	Lossless compression is mainly used to compress text-sound and images.	Lossy compression is mainly used to compress audio, video, and images.
5.	As compare to lossy data compression, lossless data compression holds more data.	As compare to lossless data compression, lossy data compression holds less data.
6.	File quality is high in the lossless data compression.	File quality is low in the lossy data compression.
7.	Lossless data compression mainly supports RAW, BMP, PNG, WAV, FLAC, and ALAC file types.	Lossy data compression mainly supports JPEG, GIF, MP3, MP4, MKV, and OGG file types.

22 What is cryptography? Distinguish between symmetric and asymmetric key cryptography. 8

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

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.
The Mathematical Representation is as follows- P = D (K, E(P)) where K –> encryption and decryption	The Mathematical Representation is as follows- P = D(Kd, E (Ke,P)) where Ke –> encryption key

key
P –> plain text
D –> Decryption
E(P) –> Encryption of plain text

Kd –> decryption key
D –> Decryption
E(Ke, P) –> Encryption of plain text using encryption key Ke . P –> plain text

23	Which mechanism is used for connection establishment? **Connection establishment** To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs: 1. SYN: The active open is performed by the client sending a SYN to the server. The client sets the segment’s sequence number to a random value A. 2. SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number (A + 1), and the sequence number that the server chooses for the packet is another random number, B. 3. ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A + 1, and the acknowledgement number is set to one more than the received sequence number i.e. B + 1. At this point, both the client and server have received an acknowledgment of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.	8
24	Discuss TCP-Window Management System?	8

Windowing and Window Size: Window management in TCP is an important concept that ensures reliability in packet delivery as well as reduce the wastage of time in waiting for the acknowledge after each packet.

Window size: window size determines the amount of data that you can transmit before receiving an acknowledgment. Sliding window refers to the fact that the window size is negotiated dynamically during the TCP session.

1. Expectational acknowledgment means that the acknowledgment number refers to the octet that is next expected
2. If the source receives no acknowledgment, it knows to retransmit at a slower rate.

The mechanism of the sliding window style may be understood easily with the help of below given diagrams:

fig-1

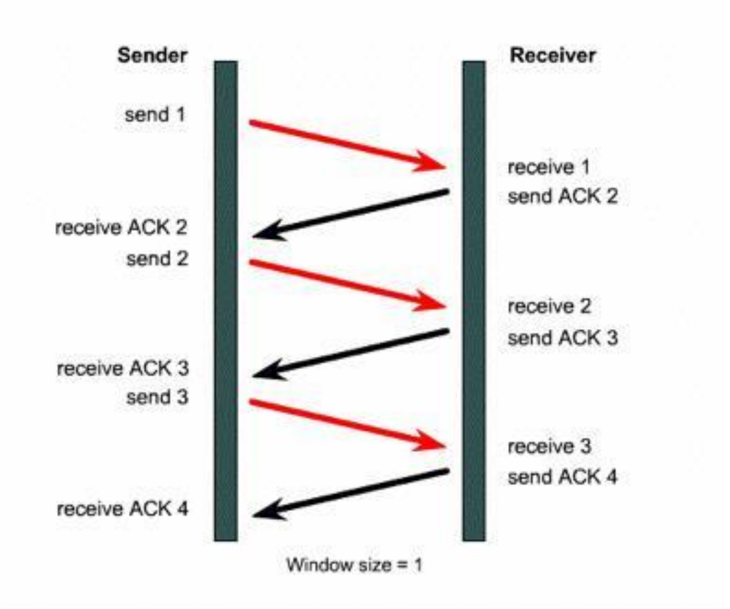
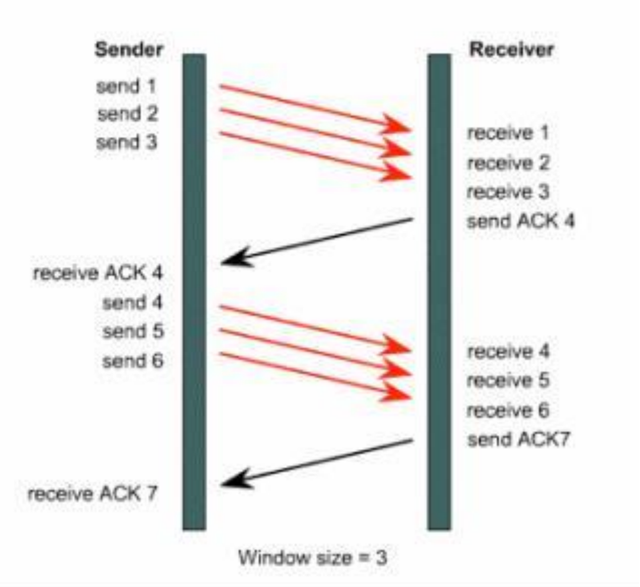
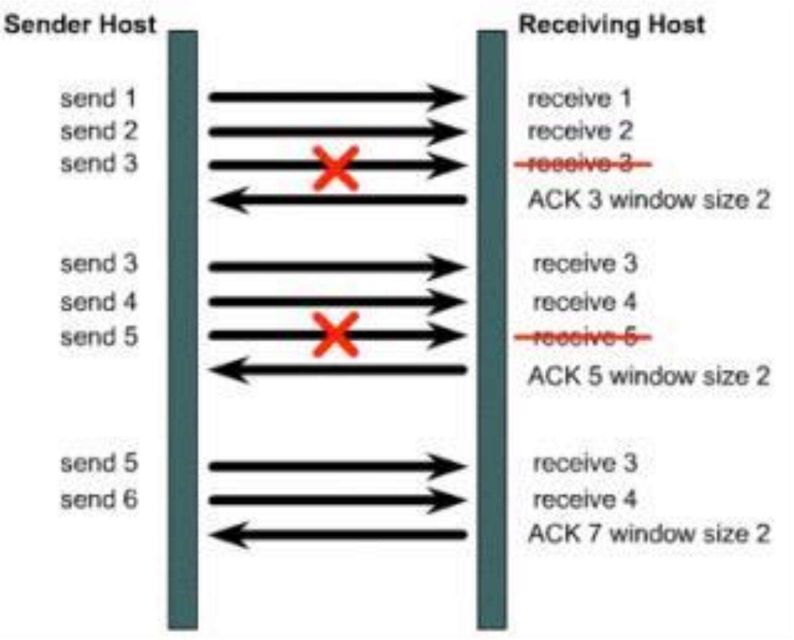
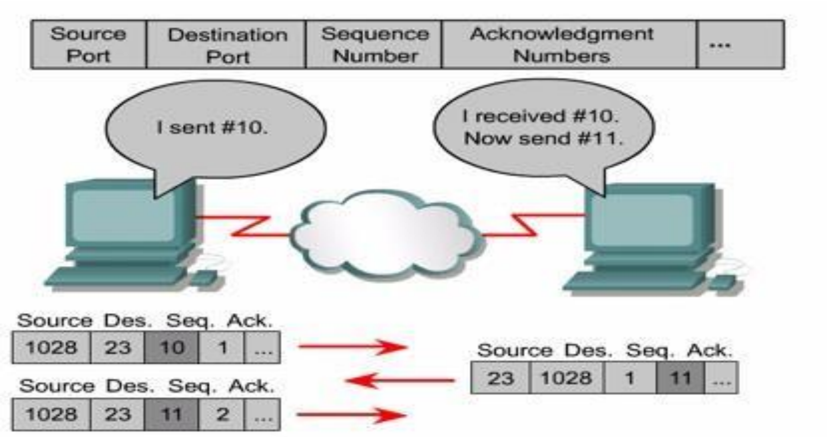


Fig-2


Sender
Receiver
send 1
send 2
send 3
receive 1
receive 2
receive 3
send ACK 4
receive ACK 4
send 4
send 5
send 6
receive 4
receive 5
receive 6
send ACK7
receive ACK 7
Window size = 3


Sender Host
Receiving Host
send 1
send 2
send 3
receive 1
receive 2
~~receive 3~~
ACK 3 window size 2
send 3
send 4
send 5
receive 3
receive 4
~~receive 5~~
ACK 5 window size 2
send 5
send 6
receive 3
receive 4
ACK 7 window size 2



25 What are the various design issues in Transport and Session layers? 8

Design Issues with Session Layer :

1. **Establish sessions between machines –**
   The establishment of session between machines is an important service provided by session layer. This session is responsible for creating a dialog between connected machines. The Session Layer provides mechanism for opening, closing and managing a session between end-user application processes, i.e. a semi-permanent dialogue. This session consists of requests and responses that occur between applications.
2. **Enhanced Services –**
   Certain services such as checkpoints and management of tokens are the key features of session layer and thus it becomes necessary to keep enhancing these features during the layer's design.
3. **To help in Token management and Synchronization –**
   The session layer plays an important role in preventing collision of several critical operation as well as ensuring better data transfer over network by

establishing synchronization points at specific intervals. Thus it becomes highly important to ensure proper execution of these services.

Design Issues with Transport Layer

- Accepting data from Session layer, split it into segments and send to the network layer.
- Ensure correct delivery of data with efficiency.
- Isolate upper layers from the technological changes.
- Error control and flow control.

26 What are issues and solutions related to TCP in networks? 8

Some the issues and solution related to Transmission Control Protocol (TCP) are as follows −

- Silly window syndrome.
- Congestion window management.

Silly Window Syndrome

This is a problem which arises in TCP flow control. In this the sender window size shrinks to an extremely low value due that the data being sent in each trip is even smaller than the TCP header. Due to which TCP protocol becomes extremely inefficient.

Causes

The silly window syndrome can occur due to two main reasons, which are as follows −

- The application which needs to send the data produces a short amount of data (1 byte), again and again and the TCP protocol is implemented in such a way that it sends the data as soon as received.

The solution to this is keeping a buffer at the sender end and storing data in it while it's generating and after sufficient data is generated or a time limit is reached (usually a Round Trip Time) then the next data packet will be sent. This is called Nagle's algorithm.

- Another cause can be the receiver can process very low amounts of data, so keep sending updates to decrease the window size to the sender.

The solution to this is the receiver should not send updates to the sender to decrease the window size beyond a certain limit. It must wait for some time limit till it has decent space and then send the update for window size. This is called Clark's algorithm.

Congestion Window Management

This is a method of changing the sender window size based on the network traffic. In this, the window size is initially set to 1 and then increased based on the following phases −

Phase 1 Slow Start

In this phase the size of the window is increased exponentially, that is, the window size doubles for every RTT. This phase is continued till a threshold window size is reached.

Phase 2 Congestion Avoidance

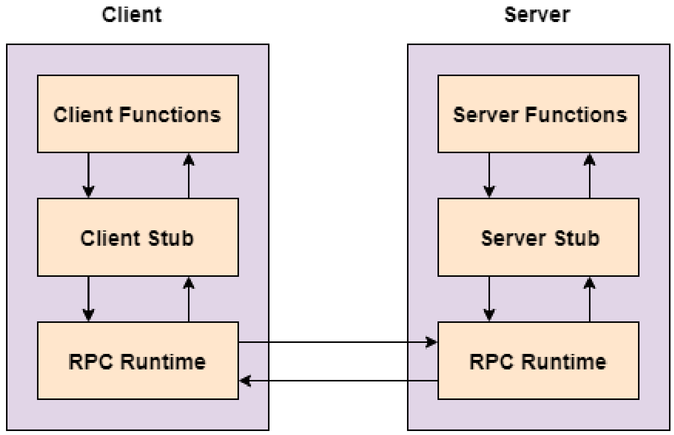
In this phase the window size is increased additively, i.e. the window size is increased by 1 for every RTT. It continues till Congestion is discovered.

Phase 3 Congestion Detection

It occurs when congestion is detected, i.e. a packet was resent. It can be due to 1 of the two reasons given below −

- **Timeout** − In this case, the threshold is reduced to half of current window size and the window size is decreased to 1 and again Phase 1 is started.

	- **Acknowledgement Duplicates** − In this case the threshold is reduced to half of current window size and the window size is decreased to the threshold value and again Phase 2 is started.	
27	Explain the concept of Remote Procedure Calls in computer networks. A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call. A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server. When the server receives the request, it sends the required response back to the client. The client is blocked while the server is processing the call and only resumed execution after the server is finished. The sequence of events in a remote procedure call are given as follows − • The client stub is called by the client. • The client stub makes a system call to send the message to the server and puts the parameters in the message. • The message is sent from the client to the server by the client's operating system. • The message is passed to the server stub by the server operating system. • The parameters are removed from the message by the server stub. • Then, the server procedure is called by the server stub. A diagram that demonstrates this is as follows −	8

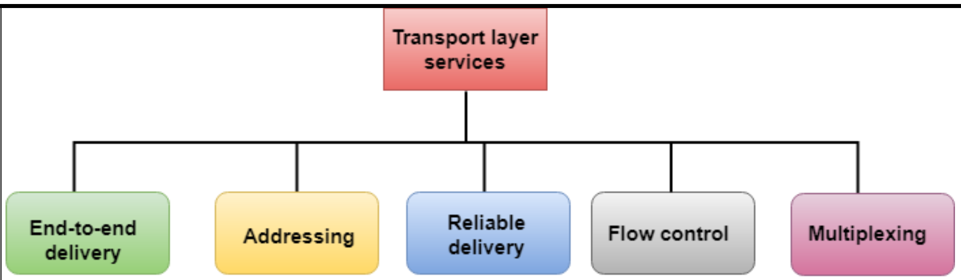
	 Client Server Client Functions Client Stub RPC Runtime Server Functions Server Stub RPC Runtime	
28	What are the services provided by transport layer? Explaineach and every service withappropriate diagram.	8

Services provided by the Transport Layer

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing



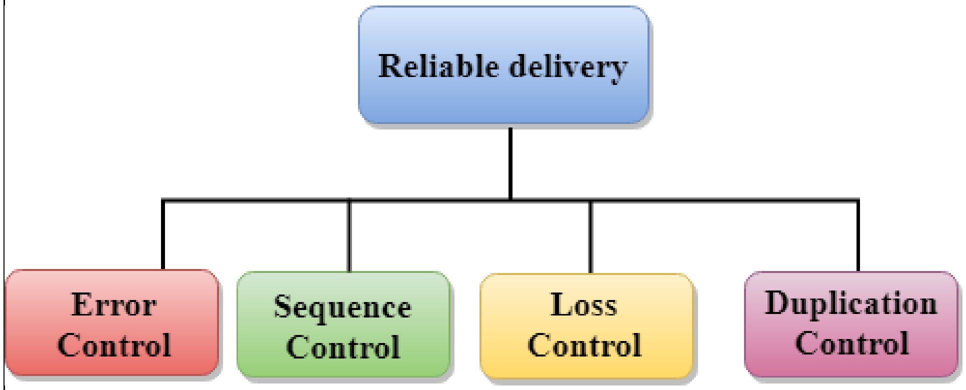
End-to-end delivery:

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:



Addressing

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.

Flow Control

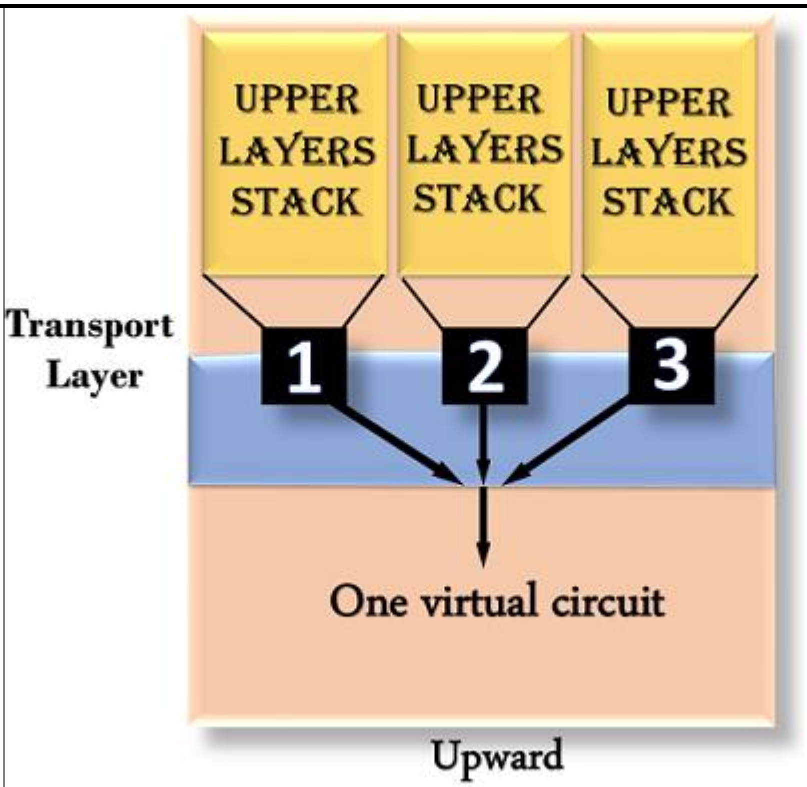
Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing

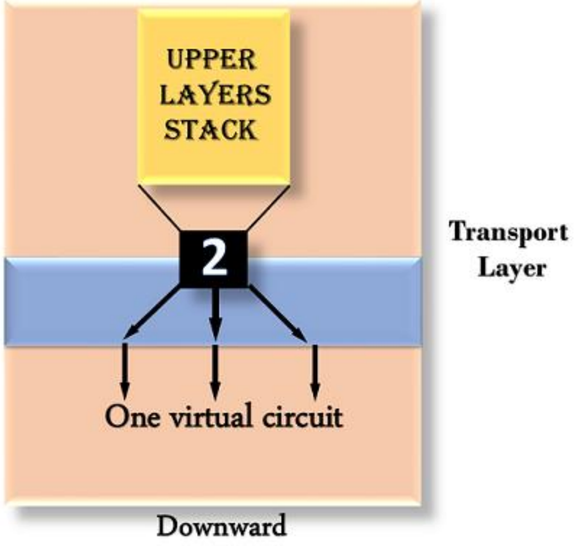
The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.

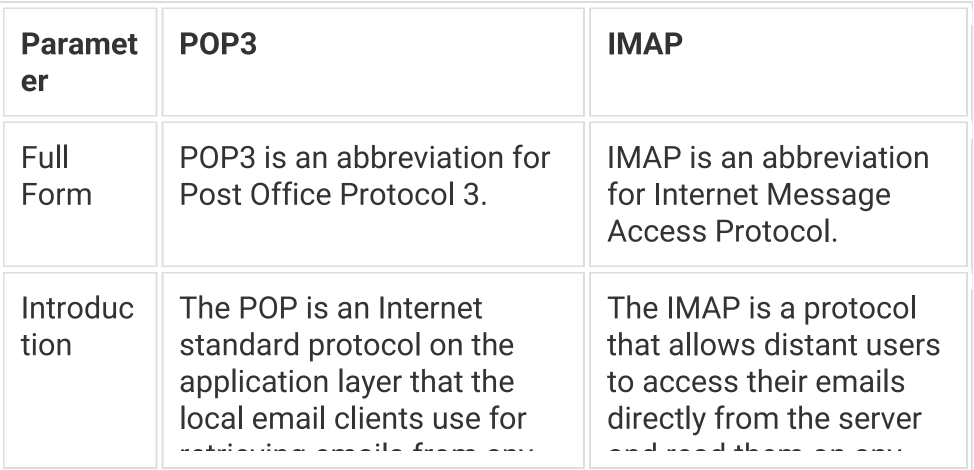


- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.



NOTES LINK ->ALL QUESTION BANK

Unit 5: Application Layer

Ques. No.	Question	Marks
1	What is Electronic Mail in Computer Networks? **Electronic mail (e-mail)** is a computer-based program that allows users to send and receive messages. E-mail is the electronic version of a letter, but with time and flexibility advantages. While a letter can take anywhere from a week to a couple of months to reach its intended destination, an e-mail is sent virtually almost instantly. Messages in the mail contain not just text but also photos, audio, and video data. A person sending an e-mail is a **sender**, and the person receiving it is the **recipient**. Electronic mail is one of the most well-known network services. Electronic mail is a computer-based service that allows users to communicate with one another by exchanging messages. Email information is transmitted via email servers and uses a variety of TCP/IP protocols. For example, the simple mail transfer protocol (SMTP) is a protocol that is used to send messages. Similarly, IMAP or POP receives messages from a mail server.	2
2	What is Electronic Mail used for? Computer users on a network can transmit text, images, sounds, and animations to one another via an e-mail system. Email systems are a crucial communication channel between employees and authorities to access large institutions' networks. Many public online systems, which maintain free worldwide communication, also offer e-mail access.	2
3	What are the advantages of electronic mail in computer networks? Some advantages of using electronic email are Mass Sending, Cost-effective, and Advertising. Using Mass sending A user may quickly send a message to many individuals. Email is a low-cost method of communicating with people. Emails are useful for product promotion as businesses can communicate in a short period of time.	2
4	Differentiate between POP3 and IMAP. 	2

Parameter	POP3	IMAP
Full Form	POP3 is an abbreviation for Post Office Protocol 3.	IMAP is an abbreviation for Internet Message Access Protocol.
Introduction	The POP is an Internet standard protocol on the application layer that the local email clients use for retrieving emails from any	The IMAP is a protocol that allows distant users to access their emails directly from the server and read them on any

	remote server over the TCP/IP connection.	device at any location feasible for them.
Complexity	POP3 is a very simplified protocol. It can only download the emails on the local computer from the inbox.	The IMAP protocol is very complex. It allows all the users to view their email folders easily and read them on the mail server itself (from any device they want).
Email Organization	A user cannot organize the emails on the server using POP3.	IMAP allows its users to organize their available emails on the server.
Need to Download	POP3 downloads the mail first and then allows its users to read them.	You can partially read your emails before downloading them in the case of IMAP.
Multiaccess	POP3 only allows a single device at a time to access the emails.	IMAP allows multiple devices at a time to access and read the available mails.
Updating of Emails	A user cannot update or create emails on the mail server by using the POP3 protocol.	You can use the IMAP protocol for updating or creating emails. It is easy to do so with a web interface or email software.
Search Emails	You cannot search for mail content on any mail server using the POP3 protocol. The user needs to download the mail first and then search for the required content.	You can easily search for mail content on any mail server using IMAP without downloading them.

Change and Delete	POP3 does not allow its users to alter or delete any email available on the mail server.	IMAP allows its users to use an email software or a web interface to alter or delete the available emails.
Speed	POP3 is very fast.	IMAP is slow as compared to POP3.
Syncing of Mails	It does not allow syncing of a user’s emails.	Users can sync their emails using this protocol.
Storage of Content	It downloads the content on the local device unless someone selects a “Keep a copy on the server” via settings.	It always stores content on the mail server.
Direction	**Unidirectional** – The changes that you make on a device have zero effect on the content available on the server.	**Bi-directional** – Whenever you make changes on the device or server, it shows on the other side as well.
Offline Usage	You can read the emails offline because POP3 downloads them on the device. The device only goes online to download new emails.	The downloaded mails are available for the user to read, edit, and delete offline. Any changes that one makes on the device get synced with the server.
Current Versions	POP3	IMAP4rev1

5	Explain the term WWW. **What Does World Wide Web (WWW) Mean?** The World Wide Web (WWW) is a network of online content that is formatted in HTML and accessed via HTTP. The term refers to all the interlinked HTML pages that can be accessed over the Internet. The World Wide Web was originally designed in 1991 by Tim Berners-Lee while he was a contractor at CERN.	2

	The World Wide Web is most often referred to simply as "the Web." **Techopedia Explains World Wide Web (WWW)** The World Wide Web is what most people think of as the Internet. It is all the Web pages, pictures, videos and other online content that can be accessed via a Web browser. The Internet, in contrast, is the underlying network connection that allows us to send email and access the World Wide Web.	
6	List the request methods used by HTTP. **HTTP (Hypertext Transfer Protocol)** specifies a collection of request methods to specify what action is to be performed on a particular resource. The most commonly used HTTP request methods are **GET, POST, PUT, PATCH, and DELETE**. These are equivalent to the **CRUD operations (create, read, update, and delete)**. **GET:** GET request is used to read/retrieve data from a web server. GET returns an HTTP status code of **200 (OK)** if the data is successfully retrieved from the server. **POST:** POST request is used to send data (file, form data, etc.) to the server. On successful creation, it returns an HTTP status code of **201**. **PUT:** A PUT request is used to modify the data on the server. It replaces the entire content at a particular location with data that is passed in the body payload. If there are no resources that match the request, it will generate one. **PATCH:** PATCH is similar to PUT request, but the only difference is, it modifies a part of the data. It will only replace the content that you want to update. **DELETE:** A DELETE request is used to delete the data on the server at a specified location.	2
7	What are the functionalities of Application layer? **Functions of Application Layer :** The Application Layer, as discussed above, being topmost layer in OSI model, performs several kinds of functions which are requirement in any kind of application or communication process. Following are list of functions which are performed by	2

	Application Layer of OSI Model – `Data from User <=> Application layer <=> Data from Presentation Layer` • Application Layer provides a facility by which users can forward several emails and it also provides a storage facility. • This layer allows users to access, retrieve and manage files in a remote computer. • It allows users to log on as a remote host. • This layer provides access to global information about various services. • This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on. • It provides protocols that allow software to send and receive information and present meaningful data to users. • It handles issues such as network transparency, resource allocation and so on. • This layer serves as a window for users and application processes to access network services. • Application Layer is basically not a function, but it performs application layer functions.	
8	What is cryptography? Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.	2
9	Define SSH. SSH stands for **Secure Shell or Secure Socket Shell**. It is a cryptographic network protocol that allows two computers to communicate and share the data over an insecure network such as the internet. It is used to login to a remote server to execute commands and data transfer from one machine to another machine.	2

10	Differentiate between WWW and W3C. **What is W3C?** The World Wide Web Consortium is the main international standards organization for the World Wide Web. Led by Web inventor and Director **Tim Berners-Lee** and CEO **Jeffrey Jaffe**. In simple words, group of highly experienced people which decide how other people will use web, this group includes employees of big companies like google, microsoft, adobe etc. They make standards of programming languages which will be used to make websites like HTML, CSS, JavaScript etc, when they add new feature in these languages they decide how this new feature will work then web brosweres like chrome, firefox, operamini etc... ad these features in their browser. So basicaly W3C works on web technologies which is used to make web. **What is WWW?** The World Wide Web, also called the Web, is an information space where documents and other web resources are identified by Uniform Resource Locator, interlinked by hypertext links, and accessible via the Internet. **So what is difference between them?** W3C is an organization which develop standards and protocols/guidlines to ensure long-term growth for web, whereas www is technology for using web made by W3C.	2

11 Compare FTP and SSH. 8

S. No.	FTP	SSH
1.	It offers communication that is distance-dependent.	Its communication does not depend on distance.
2.	It is less secure and not suited in critical situations.	It offers secure communication.
3.	It cannot be used in case of tunneling.	In a situation like tunneling, we can use SSH.
4.	It offers few features and options during communication.	It has more features than FTP.
5.	It provides fewer functionalities than SSH.	It offers more functionalities than FTP.
6.	For communication, it runs on port number 21.	It runs on port number 22.
7.	In this, Data encryption is not there.	It provides data encryption.
8.	It is a protocol that is used for transferring files from a local client to a remote server.	While SSH is used for the communication between two computers that are connected by some electrical medium.
9.	FTP is generally faster.	While SSH is generally slower as compared to FTP.

12	What is Application Layer? What are the different protocolsused in Application layer? The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user. **Application Layer protocol:-** ***1. TELNET:*** Telnet stands for the **TEL**etype **NET**work. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the internet ***2. FTP:*** FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files. ***3. TFTP:*** The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it ***4. NFS:*** It stands for a network file system. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. **5. SMTP:** It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. **6. LPD:** It stands for Line Printer Daemon. It is designed for printer sharing. ***7. X window:*** It defines a protocol for the writing of graphical user interface–based client/server applications. ***8. SNMP:*** It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. ***9. DNS:*** It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.	8

	10. DHCP: It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts.	
13	Describe the three protocols used to deliver email over the Internet. **What is an email protocol?** Email protocol is a set of rules defined to ensure that emails can be exchanged between various servers and email clients in a standard manner. This ensures that the email is universal and works for all users. Example: A sender using an Apple email client with a Gmail server can send an email to another user using a Zoho mail server on an Outlook email client. This is possible because the servers and the email clients follow the rules and standards defined by the email protocols. **Why do we need email protocols?** Consider the difference between sending a message via a messaging platform like WhatsApp and sending an email. When you send a message using WhatsApp, the recipient will also use WhatsApp to read the messages. The server which processes the message is also the WhatsApp server. The same platform is used in the server and the client, and hence the entire flow of data is handled by the serving platform in a custom manner. In the case of email, the sender, recipients, and servers involved can all be different but then they need to receive the data, decipher the content and render it in the same way the sender has sent it. Email protocols define how the email message has to be encoded, how it needs to be sent, received, rendered, and so on, and hence they are essential. While email protocols make the process behind emails a bit complex, the protocols ensure that email is a standard, reliable, and universal mode of communication. **What are the different email protocols?** The common protocols for email delivery are Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP). Each of these protocols has a standard methodology to	8

deal with the emails and also has defined functions.

POP Protocol

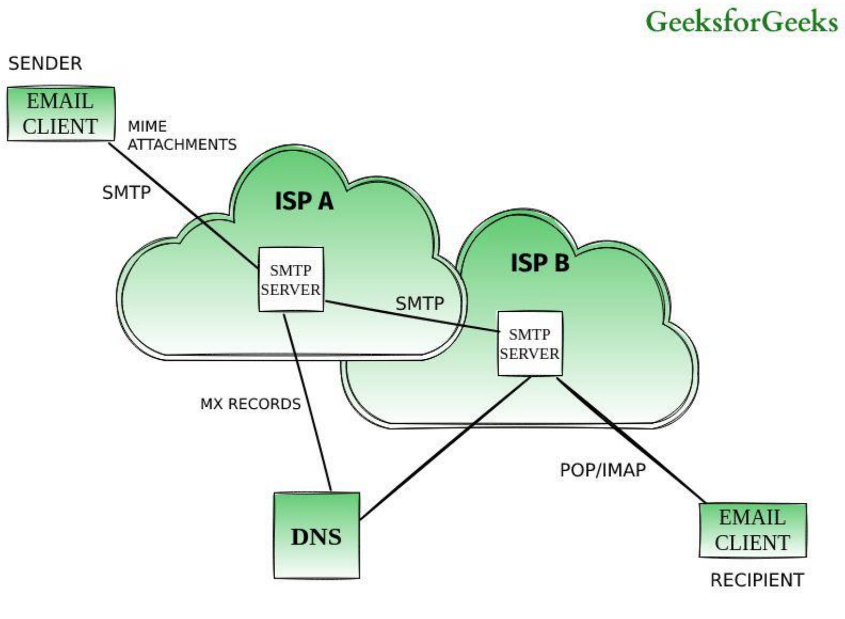
POP stands for Post Office Protocol. Email clients use the POP protocol support in the server to download the emails. This is primarily a one-way protocol and does not sync back the emails to the server.

IMAP Protocol

IMAP stands for Internet Message Access Protocol. IMAP Protocol is used to sync the emails in the server with the email clients. It allows two-way sync of emails between the server and the email client, while the emails are stored on the server.

SMTP Protocol

SMTP stands for Simple Mail Transfer Protocol. SMTP is the principal email protocol that is responsible for the transfer of emails between email clients and email servers.



EMAIL PROTOCOLS

14 Explain how the web works. 8

On the simplest level, the Web physically consists of the following components −

- **Your personal computer** − This is the PC at which you sit to see the web.
- **A Web browser** − A software installed on your PC which helps you to browse the Web.
- **An internet connection** − This is provided by an ISP and connects you to the internet to reach to any Website.
- **A Web server** − This is the computer on which a website is hosted.
- **Routers & Switches** − They are the combination of software and hardware who take your request and pass to appropriate Web server.

The Web is known as a *client-server system*. Your computer is the client and the remote computers that store electronic files are the servers.

How the Web Works

When you enter something like Google.com the request goes to one of many special computers on the Internet known as *Domain Name Servers* **(DNS)**. All these requests are routed through various routers and switches. The domain name servers keep tables of machine names and their IP addresses, so when you type in Google.com it gets translated into a number, which identifies the computers that serve the Google Website to you.

When you want to view any page on the Web, you must initiate the activity by requesting a page using your browser. The browser asks a domain name server to translate the domain name you requested into an IP address. The browser then sends a request to that server for the page you want, using a standard called Hypertext Transfer Protocol or HTTP.

The server should constantly be connected to the Internet, ready to serve pages to visitors. When it receives a request, it looks for the requested document and returns it to the Web browser. When a request is made, the server usually logs the client's IP address, the document requested, and the date and time it was requested. This information varies server to server.

An average Web page actually requires the Web browser to request more than one file from the Web server and not just the HTML / XHTML page, but also any images, style sheets, and other resources used in the web page. Each of these files including the main page needs a URL to identify each item. Then each item is sent by the Web server to the Web browser and Web browser collects all this information and displays them in the

	form of Web page. **In Short** We have seen how a Web client - server interaction happens. We can summarize these steps as follows – A user enters a URL into a browser (for example, Google.com. This request is passed to a domain name server. The domain name server returns an IP address for the server that hosts the Website (for example, 68.178.157.132). The browser requests the page from the Web server using the IP address specified by the domain name server. The Web server returns the page to the IP address specified by the browser requesting the page. The page may also contain links to other files on the same server, such as images, which the browser will also request. The browser collects all the information and displays to your computer in the form of Web page.	
15	How POP3, IMAP and FTP play role in application layer.Explain with proper diagram. The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers. The Application layer includes the following functions: • **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit. • **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication. • **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer. **FTP** • FTP stands for File transfer protocol. • 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. Objectives of FTP	8

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

IMAP

IMAP stands for Internet Mail Access Protocol. It was first proposed in 1986.

Key Points:

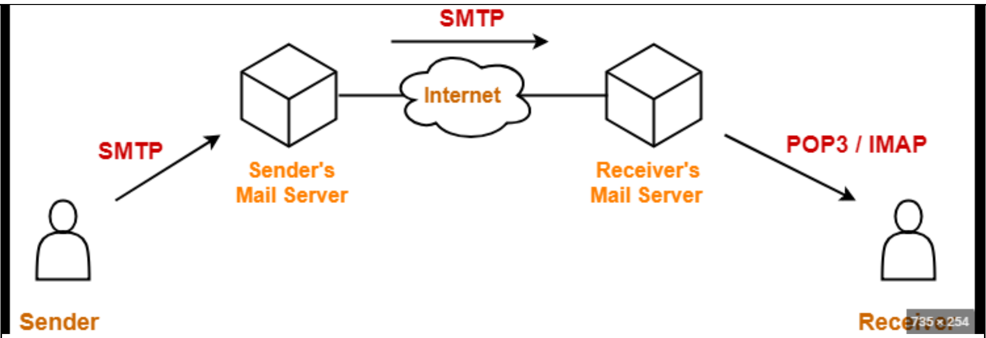
- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.



16

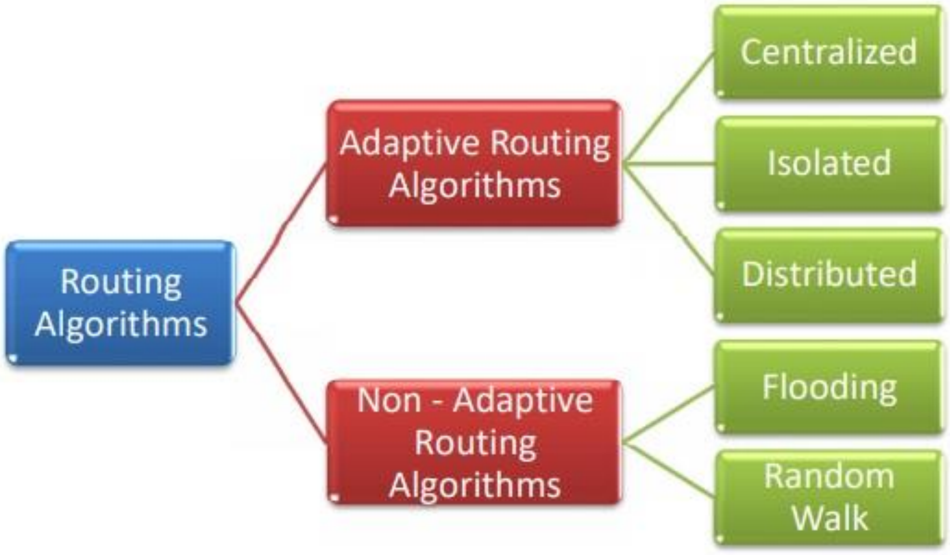
Describe routing algorithms with appropriate example

8

A routing algorithm is a procedure that lays down the route or path to transfer data packets from source to the destination. They help in directing Internet traffic efficiently. After a data packet leaves its source, it can choose among the many different paths to reach its destination. Routing algorithm mathematically computes the best path, i.e. "least – cost path" that the packet can be routed through.

Types of Routing Algorithms

Routing algorithms can be broadly categorized into two types, adaptive and nonadaptive routing algorithms. They can be further categorized as shown in the following diagram –



Adaptive Routing Algorithms

Adaptive routing algorithms, also known as dynamic routing algorithms, makes routing decisions dynamically depending on the network conditions. It constructs the routing table depending upon the network traffic and topology. They try to compute the optimized route depending upon the hop count, transit time and distance.

The three popular types of adaptive routing algorithms are −

- **Centralized algorithm** − It finds the least-cost path between source and destination nodes by using global knowledge about the network. So, it is also known as global routing algorithm.
- **Isolated algorithm** − This algorithm procures the routing information by using local information instead of gathering information from other nodes.
- **Distributed algorithm** − This is a decentralized algorithm that computes the least-cost path between source and destination iteratively in a distributed manner.

Non – Adaptive Routing Algorithms

Non-adaptive Routing algorithms, also known as static routing algorithms, construct a static routing table to determine the path through which packets are to be sent. The static routing table is constructed based upon the routing information stored in the routers when the network is booted up.

The two types of non – adaptive routing algorithms are −

- **Flooding** − In flooding, when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on. Flooding may be uncontrolled, controlled or selective flooding.
- **Random walks** − This is a probabilistic algorithm where a data packet is sent by the router to any one of its neighbours randomly.