CONTENTS

❑ *Publishers* : **KAMAL PUBLISHING HOUSE**
110/201, Laxmi Tower,
Near R.K. Mission School & Hospital,
R.K. Nagar, G.T. Road
Kanpur – 208 012
(Uttar Pradesh)
Contact No. : +91 9559401840
Email : kamalpubhouse@gmail.c
Website : www.kphindia.in

❑ *Composed by* : Komal Graphics
Kanpur.

SYLLABUS

	Topic
1.	**Data Communications** : Introduction, Data communication Components and characteristics, Data representation and Data flow. **Networks** : LAN, WAN, MAN, Topologies. **Protocols and Standards** : ISO-OSI model and TCP-IP Model. **Network Connecting Devices** : HUB, Bridge, Switch, Router and Gateways. **Transmission Media** : Guided and unguided Media **Classification and Arrangement** : Wired LANs and Wireless LANs
2.	**Data Link Layer** : Error Detection and Error Correction: Types of errors, LRC, VRC, Checksum, CRC, and Hamming Code. **Flow Control and Error Control** : Stop and Wait Protocol, Sliding Window, Go-back-N-ARQ Protocol and Selective-Repeat ARQ Protocol. **Channel Allocation Protocols** : Random Access, Controlled and Channelization techniques such as ALOHA, CSMA, CSMA/CD, CDMA/CA, TDMA, FDMA, Token Passing, etc.
3.	**Network Layer : Switching Techniques** : Circuit Switching, Packet Switching, and Message Switching. **Logical Addressing** : IPv4 and IPv6 Address schemes, Classes and subnetting. **Network Layer Protocols** : ARP, RARP, BOOTP and DHCP. **Routing Techniques** : Interdomain and Intradomain routing with examples.
4.	**Transport Layer** : Introduction to Transport Layer, Process-to-Process Delivery, Reliable and unreliable Connection, Port and Socket Addressing. **Transport Layer Protocols with Packet Formats** : User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Stream Control Transmission Protocol (SCTP). **Congestion Control** : Techniques for handling the Congestion Control. **Quality of Service (QoS)** : Flow Characteristics and techniques to improve QoS
5.	**Application Layer** : Basic Concept of Application Layer, Domain Name System, World Wide Web, Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login. **Introduction to Cryptography** : Definition, Goal, Applications, Attacks, Encryption, decryption, public-key and private key cryptography.

DATA COMMUNICATIONS

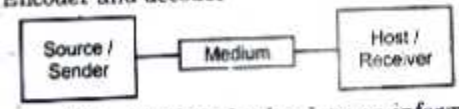
1. ◆ ***Define Data Communication. Describe Fundamental characteristics of Data Communication.*** **(2017-18)**
   ◆ ***Explain data communication and also explain its components.***

Data communication refers to the exchange of data between a source and a receiver. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.

The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.

Data communication is a process of transferring data electronically from one place to another. Data can be transferred by using different medium. The basic components of data communications are as follows :

(1) Message
(2) Sender
(3) Receiver
(4) Medium/ communication channel
(5) Encoder and decoder



Message : The message is the data or information to be communicated. It may consist of text, number, pictures, sound, video or any a combination of these.

Sender : Sender is a device that sends message. The message can consist of text, numbers, pictures etc. it is also called source or transmitter. Normally, computer is use as sender in information communication systems.

Receiver : Receiver is a device that receives message. It is also called sink. The receiver can be computer, printer or another computer related device. The receiver must be capable of accepting the message.

Medium : Medium is the physical path that connects sender and receiver. It is used to transmit data. The medium can be a copper wire, a fiber optic cable, microwaves etc. it is also called communication channel.

Encoder and Decoder : The encoder is a device that converts digital signals in a form that can pass through a transmission medium. The decoder is a device that converts the encoded signals into digital form. The receiver can understand the digital form of message. Sender and receiver cannot communicate successfully without encoder and decoder.

Characteristics of Data Communications

The effectiveness of a data communications system depends on four fundamental characteristics : delivery, accuracy, timeliness, and jitter.

(1) **Delivery :** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

(2) **Accuracy :** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

(3) **Timeliness :** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

(4) **Jitter :** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

2. *Explain data representation.*

Data Representation

(1) **Text :** Text represented as bit pattern, sequence of bits. Ex. Unicode, ASCII, EBCDIC, etc.

(2) **Numbers :** Represented as bit pattern. Ex. BCD, Hex, etc.

(3) **Images :** Represented as bit pattern. Image composed of matrix of pixels.

(4) **Audio :** Continuous not discrete.

(5) **Video :** Either be produced as a continuous entity by TV camera or it can be combination of images, each a discrete entity to convey an idea.

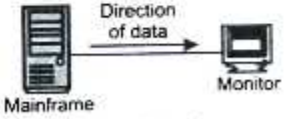


Figure : Simplex

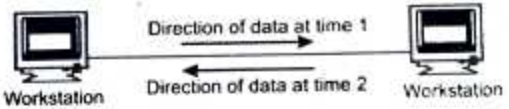


Figure : Half Duplex

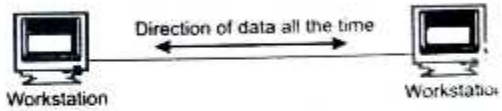


Figure : Full Duplex

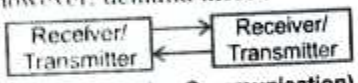
(Figure)

3. *Explain the data flow.*

(Figure : Simplex Communication)

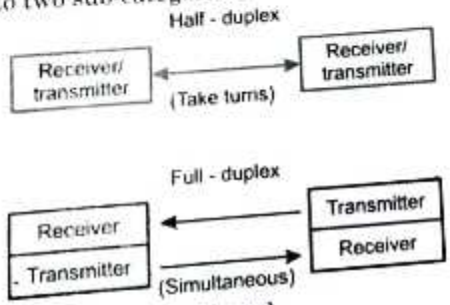
With simplex communication, all data flow is unidirectional: from the designated transmitter to the

designated receiver. Bogus Bus is an example of simplex communication, where the transmitter sent information to the remote monitoring location, but no information is ever sent back to the water tank. If all we want to do is send information one-way, then simplex is just fine. Most applications, however, demand more :



(Figure : Duplex Communication)

With duplex communication, the flow of information is bi-directional for each device. Duplex can be further divided into two sub-categories :



(Figure)

Half-duplex communication may be likened to two tin cans on the ends of a single taut string: Either can may be used to transmit or receive, but not at the same time. Full-duplex communication is more like a true telephone, where two people can talk at the same time and hear one another simultaneously, the mouthpiece of one phone transmitting the earpiece of the other, and vice versa. Full-duplex is often facilitated through the use of two separate channels or networks, with an individual set of wires for each direction of communication. It is sometimes accomplished by means of multiple-frequency carrier waves, especially in radio links, where one frequency is reserved for each direction of communication.

4. ◆ ***Explain the components of data communication.***
   ◆ ***Write short note on Protocols.***
   ◆ ***Write the five basic components of database communication.***

Data Communication Component

The following are the basic components for working of a communication system.

(1) Transmitter
(2) Receiver
(3) Medium
(4) Message
(5) Protocol

The transmitter sends the message and the receiver receives the message. The medium is the channel over which the message is sent and the protocol is the set of rules that guides how the data is transmitted from encoding to decoding. The message of course is central to all the components. The message is the data that is being communicated.

Relationship between the Five Components :

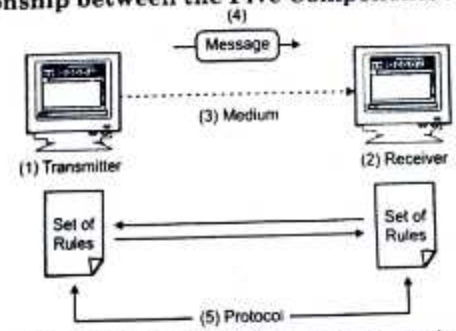


Figure : Data Communication Components

Transmitter : The transmitter is the device that sends the message. It can be a computer, workstation, telephone handset, video camera, and so on.

Receiver : The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

Medium : The transmission medium is the physical path by which a message travels from sender to receiver. It can consist of twisted pair wire, coaxial cable, fiber-optic cable, laser or radio waves (terrestrial or satellite microwave).

Message : The message is the transmission (data) to be communicated. It can consist of text, number, pictures, sound, or video or any combination of these.

Protocol : A protocol is a set of rules that governs data communication. It represents an agreement between the

communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking German cannot be understood by a person who speaks only Japanese.

5. *What are the two types of line configuration? And also explain how do we establish a connection?*

Line Configuration

Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another. For communication to occur, two devices must be connected in same way to the same link at the same time.

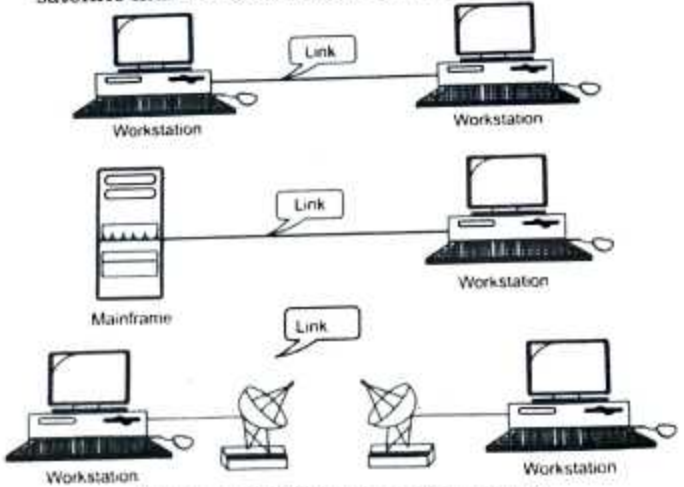
There are two possible line configurations.

(1) Point-to-Point.

(2) Multipoint.

Point-to-Point :

A **Point to Point Line Configuration** : Provide dedicated link between two devices use actual length of wire or cable to connect the two end including microwave & satellite link. Infrared remote control & tvs remote control.



(Figure : Point to Point Configuration)

The entire capacity of the channel is reserved for transmission between those two devices. Most point-to-point line configurations 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.

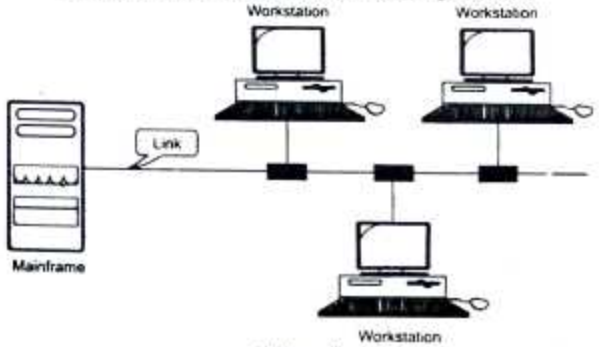
Point to point network topology is considered to be one of the easiest and most conventional network topologies. It is also the simplest to establish and understand. To visualize, one can consider point to point network topology as two phones connected end to end for a two way communication

Multipoint Configuration : Multipoint Configuration also known as Multidrop line configuration one or more than two specific devices share a single link capacity of the channel is shared.

More than two devices share the Link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line Config :

(1) **Spatial Sharing** : If several devices can share the link simultaneously, its called Spatially shared line configuration

(2) **Temporal (Time) Sharing** : If users must take turns using the link, then its called Temporally shared or Time Shared Line Configuration



(Figure)

6. ◆ *What is Network? Explain different types of Networks.* **(2018-19)**

◆ ***Discuss Network.***

Network

A computer network or data network is a digital telecommunications network which allows nodes to share resources. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols. This formidable collection of information technology requires skilled network management to keep it all running reliably.

Computer networks support an enormous number of applications and services such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as many others. Computer networks differ in the transmission medium used to carry their signals, communications protocols to organize network traffic, the network's size, topology and organizational intent. The best-known computer network is the Internet.

Types of Networks

There are three types of Computer Networks.

(1) **Local Area Network (LAN) :** LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

(2) **Metropolitan Area Network (MAN) :** MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

(3) **Wide Area Network (WAN) :** WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

7. *What are the applications of computer network?* **(2018-19)**

Applications of Computer Network

(1) Sharing of resources such as printers.
(2) Sharing of expensive software's and database.
(3) Communication from one computer to another computer.
(4) Exchange of data and information among users via network.
(5) Sharing of information over geographically wide areas.

8. *Differentiate between Baseband Transmission and Broadband Transmission.* **(2018-19)**

Difference Between Baseband Transmission and Broadband Transmission

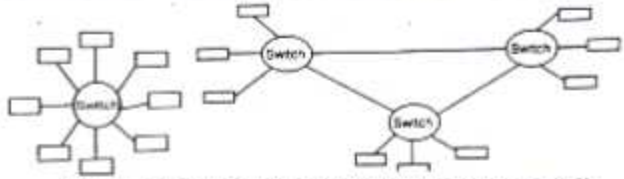
Basis for Comparison	Baseband Transmission	Broadband Transmission
Type of signaling used	Digital	Analog
Application	Work well with bus topology.	Used with a bus as well as tree topology.
Encoding Used	Manchester and Differential Manchester encoding.	PSK encoding.
Transmission	Bidirectional	Unidirectional
Signal range	Signals can be travelled over short distances	Signals can be travelled over long distances without being attenuated

9. ◆ ***What is Network topology. Explain different types of topologies.*** **(2017-18)**
   ◆ ***What do you mean by network topology? Explain in brief any three such network topologies.*** **(2013-14)**
   ◆ ***What do you understand by network topology?*** **(2010-11)**
   ◆ ***Define all types of network topology with advantages and disadvantages.***

LAN topologies define manner in which network drives are organized. Four common LAN topologies are defined below :

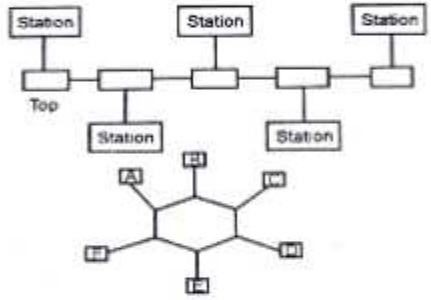
Star Topology : A star topology is a LAN architecture in which the end point network are connected to common central hub, or switch by dedicated links.

The simple star diagram of figure (i) illustrates the star topology with each station connected to a central switch by a dedicated physical link. The switch provides a path between any two devices wishing to communicate either physically in a circuit switch or logically in a packet switch. The main advantages of a star LAN are that access to the network. i.e. the decision on when a starting can or cannot transmit is under central control.



(Figure (i) : Simple Star (ii) : Complex (Snowflake))

Star LANs tend to imply simple attachment hardware at each station although the switches themselves can be complex and therefore expensive. Speeds are generally limited the central switch is an obvious potential source of catastrophic failure. Figure shows different types of star LANs.



(Figure)

Advantages :

(1) If one cable fails the other stations are not affected.
(2) Consistent performance even during heavy traffic.
(3) No problems with collisions as nodes are only connected to each other via the servers.
(4) Easy to add new stations without interrupting others.

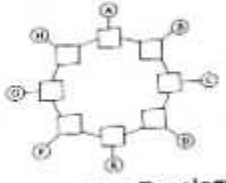
Disadvantages : May be costly to install because of the amount of cabling required. Cabling costs from a substantial part of installation costs.

Ring Topology : A ring LAN is one where the stations are connected by a loop of cable and each connection point called a repeater is responsible for passing on blocks or packets of data. The data is sent in packets and within each station there is a hardware controller board responsible for recognizing and receiving packets sent to that station. (i.e. addressed to that stating). The same

hardware is also controlling access to the ring i.e. decidi when is the turn for that stating to start transmittin Unlike star LAN is a ring the network access is not und central control. There are several methods available f effecting ring such distributed but coordinat decision-making.

The principal disadvantage of ring is that eve station is involved in the transfer of data and thus o failure of a repeater brings the whole ring LAN to a ha The second disadvantage lies in the ring cont mechanism required to determine as who should start the ring to determine that the packets are not corrupt a to prevent the same packet from going round the ri forever because of a station fault. Some ring LANs emp a special monitor station to do this job. Ring LANs ha the major advantage in speeds potential offered by fi optic cables. Ring limitations between stations of imposed by other topologies.

In ring topology type LAN architecture a series devices are connected to one another closed loop. B Token Ring/ IEEE 802.5 and FDDI networks implemen ring topology. Figure logical ring topology.



(Figure : Ring Topology)

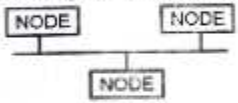
Bus Topology : Bus networks are the most com LANs. They have no switches and in their simplest for repeaters but simply share a common I communication medium. Each station requires a (hardware for attachment to the medium), which mu capable of delivering the signal to all the stations o bus.

The data is sent in packet and each station 'hea the transmission, picking up those addressed to it. bus networks have the advantages of being passive the active components are in the stations and a f affects only that one station. They can be somewhat l

in distance however and since usually only one station at a time can transmit there has to be a complex access mechanism at each station.

(Figure : Bus LAN Topology)

These topologies are logical architectures but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies for example are commonly organized physically as a star.



(Figure)

A bus topology is linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all others stations of the three most widely used LAN implementations Ethernet/IEEE 802.3 networks including 100 Base T implement a bus topology which is illustrated in figure.

Advantages :

(1) **Easy Expandability :** A note can be added but just extending the cable.

(2) **Cheap Cabling :** Bus is the cheapest solution for small LANs. No extra hardware required (link hub in star).

(3) Requires less cable length than a star topology.

Disadvantages :

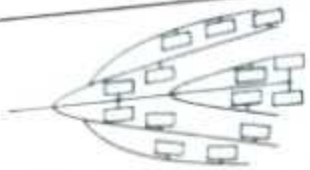
(1) Entire networks shuts down if there is a break in the main cable.

(2) Terminators are required at both ends of the backbone cable.

(3) Difficult to identify the problem if the entire network shut down.

(4) Not meant to be used as a stand-alone solution in a large building.

Tree Topology : A tree topology is a LAN architecture that is identical to the bus topology expect the branches with multiple nodes are possible in this case. Figure illustrates a logical tree topology.



(Figure A Logical Tree Topology Can Contain Multiple Nodes

Mesh Topology : It is a point-to-point connection to oth
nodes or devices. All the network nodes are connected
each other. Mesh has *n*(*n* 1)/2 physical channels to link
devices.

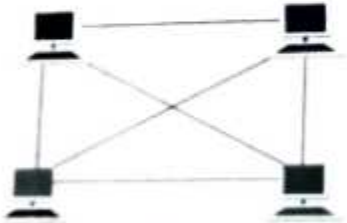
There are two techniques to transmit data over t
Mesh topology, they are :

(1) Routing

(2) Flooding

Routing : In routing, the nodes have a routing logic, as p
the network requirements. Like routing logic to direct t
data to reach the destination using the shortest distan
or routing logic which has information about the brok
links, and it avoids those node etc. We can even ha
routing logic to re-configure the failed nodes.

Flooding : In flooding, the same data is transmitt
to all the network nodes, hence no routing logic
required. The network is robust, and the its very unlik
to lose the data. But it leads to unwanted load over t
network.



(Figure)

10. ***What is Network Criteria? Write at least thr
criteria of Network.***

A network is selected on the basis of network crite
During the network selection, it is important to cons
these criteria for improving network functionality.

Three Criteria of Network

(1) **Performance** : Performance is the defined as the rate of transferring error free data. It is measured by the Respon-- Time. Response Time is the elapsed time between the end of an inquiry and the beginning of a response. Request a file transfer and start the file transfer. Factors that affect Response Time are :

- (a) **Number of Users** : More users on a network - slower the network will run.
- (b) **Transmission Speed** : Speed that data will be transmitted measured in bits per second (bps).
- (c) **Media Type** : Type of physical connection used to connect nodes together.
- (d) **Hardware Type** : Slow computers such as XT or fast such as Pentium+.
- (e) **Software Program** : How well is the network operating system (NOS) written.

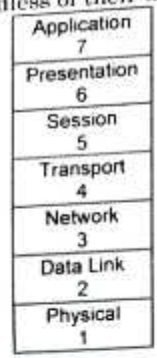
(2) **Reliability** : Reliability is the measure of how often a network is useable. MTBF (Mean Time Between Failures) is a measure of the average time a component is expected to operate between failures. Normally provided by the manufacturer. A network failure can be : hardware, data carrying medium and Network Operating System.

(3) **Recovery** : Recovery is the Network's ability to return to a prescribed level of operation after a network failure. This level is where the amount of lost data is nonexistent or at a minimum. Recovery i based on having Back-up Fil

11. ◆ ***Write at least three functions of each layer of ISO/OSI model.***
◆ ***Write two characteristics of Network Layer.***
◆ ***Draw the OSI model and explain three functions of each layer.***
◆ ***Explain the functions of each Layer of OSI model.***
◆ ***Explain OSI model in detail.***

An ISO standard that cover all aspects of network communications is Open System Interconnection model. It was first introduced in the late 1970s. An open system is a

set of protocols that allows any two different system communicate regardless of their underlying architectur



Layers in the OSI Model

Physical Layer : The physical layer coordinates functions required to carry a bit stream over a phy medium.

The physical layer is concerned with the following :

(1) **Physical Characteristics of Interfaces Medium** : Physical layer defines the characte of interfaces between the devices and transmission medium.

(2) **Data Rate** : The transmission rate, the numb bits sent each second is also define.

(3) **Physical Topology** : The physical topology d how devices are connected to make a network.

(4) **Transmission Mode** : The physical layer define the direction of transmission betwee devices i.e., simplex, half-duplex, or full-duplex.

Data Link Layer : The data link layer transfor physical layer, a raw transmission facility, to a re link. It is responsible for moving frame one hop to the Other responsibilities are :

(1) **Framing** : The data link layer divides the stre bits received from network layer into manag data units called frames.

(2) **Physical Addressing** : If frames are distributed to different system on the networ data link layer adds a header to the frame to the sender and receiver of the frame.

(3) **Flow Control** : If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender. The data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

(4) **Error Control** : The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.

Network Layer : The network layer is responsible for the source to destination delivery of a packet, possibly across multiple network. Other responsibilities of network layer are :

(1) **Logical Addressing** : The physical addressing implemented by the data link layer handles the addressing problem locally. The network layer add a header to the packet coming from upper layer include the logical addresses of the sender and receiver.

(2) **Routing** : When independent network are connected to create internet works or a large network. The connecting devices route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport Layer : The transport layer is responsible for process-to-process delivery of the entire message. The transport layer ensures that the whole message arrives interact and in order, overseeing both error control and flow control at the source-to - destination level. Other responsibilities are :

(1) **Segmentation and Reassembly** : A message is divided into transmittable segments with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

(2) **Connection Control** : The transport layer can be either connectionless or connection oriented. A Connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a

to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

Network Layer : The Internet layer responsibilities including addressing, packaging, and routing functions. The Internet layer is analogous to the Network layer of the OSI model. The core protocols for the IPv4 Internet layer consist of the following :

(1) The Address Resolution Protocol (ARP) resolves the Internet layer address to a Network Interface layer address such as a hardware address.

(2) The Internet Protocol (IP) is a routable protocol that addresses, routes, fragments and reassembles packets.

(3) The Internet Control Message Protocol (ICMP) reports errors and other information to help you diagnose unsuccessful packet. Delivery.

(4) The Internet Group Management Protocol (IGMP) manages IP multicast groups

Transport Layer : Transport Layer protocols define the rules of dividing a chunk of data into segments and then reassemble segments into the original chunk. Typical protocols are :

(1) **Transmission Control Protocol (TCP)** : Provid functions such as reordering and data resend.

(2) **User Datagram Service (UDP)** : Use when th message to be sent fit exactly into a datagram an Use also when a more simplified data format required.

(3) **Stream Control Transmission Protocol (SCTP)** SCTP provides support for newer applications such voice over the Internet.

Application Layer : Application layer protocols define th rules when implementing specific network applications. relies on the underlying layers to provide accurate a efficient data delivery. Typical protocols are :

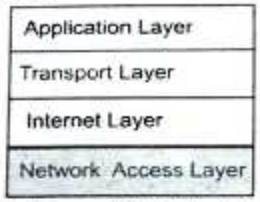
(1) **File Transfer Protocol (FTP)** : For file transfer

(2) **Remote terminal protocol (TELNET)** : For remo login on any other computer on the network.

(3) **Simple Mail Transfer Protocol (SMTP)** : For m transfer.

Hypertext Transfer Protocol (HTTP) : For Web browsing.

Diagram of TCP/IP :



(Figure : TCP/IP Model)

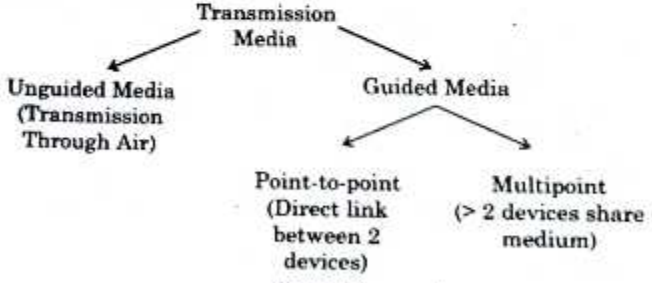
15. ◆ ***What is transmission medium? What are the different types of transmission medium?*** **(2018-19)**

◆ ***Explain Transmission media. Differentiate guided media from unguided media.*** **(2017-18)**

◆ ***Which types of transmission media are used at physical layer transmission? Give a comparative study of different transmission media is suitable for transmission?*** **(2008-09)**

Transmission Media

(1) The Transmission medium is the physical path between transmitter and receiver in a data transmission system.



(Figure)

(2) Transmission Medium can be :

(a) **Simplex** : Transmission in one direction only.

(b) **Half-Duplex** : Transmission in both directions, but not at the same time.

(c) **Full-Duplex (Duplex)** : Simultaneous transmission in both directions.

There are following Transmission Media :

Twisted Pair :

(1) Two insulated wires are twisted around each other and combined with others into a cable.

(2) Used to connect telephone subscribers to switching centers and for wiring local area networks.

(3) Two popular varieties :
- (a) **Category 3** : 10 *Mbps*
- (b) **Category 5** : 100 *Mbps*

Coaxial Cable :

(1) Like twisted pair a coaxial cable ("coax") has two conductors that are shielded.

(2) Used for digital transmissions in local area network (Example, Ethernet) and analog transmissions for cable television.

(3) Coaxial used for Cable TV supports a spectrum of 5 750 *MHz*.

Optical Fiber :

(1) Optical fiber is a thin, flexible medium capable of conducting an optical ray.

(2) Fiber is built of various glasses or plastics.

(3) Very high bandwidth (more than 10 *Gbps*).

(4) Used for long-distance trunks, local area network high-speed transmissions.

(5) Inherently unidirectional.

Types of Optical Fiber :

Multimode Fiber : Rays may take different paths (1 *Mbps, 2km*).

Single Mode Fiber :

(1) By reducing the radius of the fiber core to the order the wavelength, only the axial ray can pass.

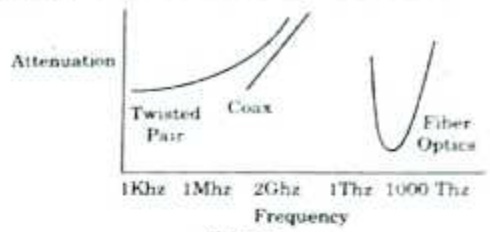
(2) Single mode fiber has superior performance but more expensive (2.4 *Gbps*, 40 *km*).

Guided Transmission Media :

(1) Twisted pair

(2) Coaxial cable

(3) Optical fiber



(Figure)

Media Selection :

Media	Network Type	Cost	Transmission Distance	Security	Error Rates	Speed
Guided Media						
Twisted Pair	LAN	Low	Short	Good	Low	Low-high
Coaxial Cable	LAN	Mod	Short-Mod	Good	Low	Low-high
Fiber Optics	Any	High	Mod-long	Very Good	Very Low	High-Very high
Radiated Media						
Radio	LAN	Low	Short	Poor	Mod	Low
Infrared	LAN	BN Low	Short	Poor	Mod	Low
Microwave	WAN	Mod	Long	Poor	Low-Mod	Mod
Satellite	WAN	Mod	Long	Poor	Low-Mod	Mod

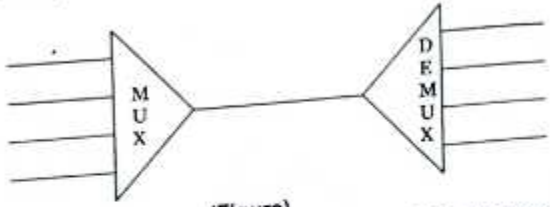
Difference Between Guided Media and Unguided Media :

Basis For Comparison	Guided Media	Unguided Media
Basic	The signal requires a physical path for transmission	The signal is broadcasted through air or sometimes water
Alternative name	It is called wired communication or bounded transmission media	It is called wireless communication or unbounded transmission media
Direction	It provides direction to signal for travelling	It does not provide any direction
Types	Twisted pair cable coaxial cable and fibre optic cable	Radio wave microwave and infrared

16. *What is multiplexing? Define all Categories of multiplexing.* (2018-19)

Multiplexing

It is a form of data transfer in which a communication channels is used for several transmission. In a multiplexed system lines share the bandwidth of one link.



(Figure)

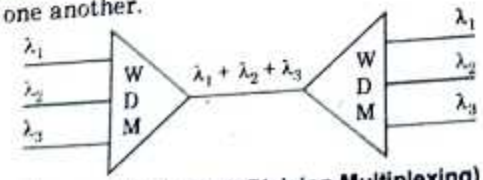
Above figure shows the operation of Multiplexer and Demultiplexer. At the sender end multiplexer combines four lines into a single stream and at the receive end that stream is fed into a demultiplexer which separates the stream back into its component transmissions and directs them into their corresponding.

Types of Multiplexing

There are Three types of Multiplexing :

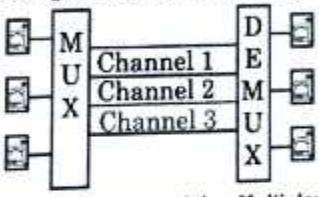
WDM (Wavelength-Division Multiplexing) : WDM is designed to use the high-data-rate capability of fiber optic cable. The optical fiber rate is higher than the data rate of metallic transmission cable. Using a fiber optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

The conceptual view of WDM multiplexer and demultiplexer very narrow band of light from different sources and combined to make wider band of light. At the receiver, the signals are separated by the demultiplexer. A new method called, Dense WDM (DWDM), can multiplex a very large number of channels by spacing channels very close to one another.



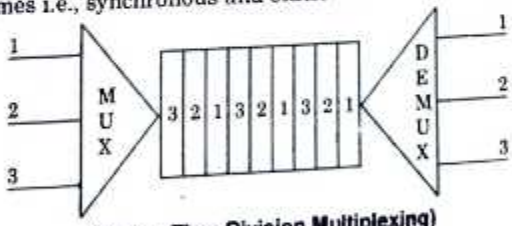
(Figure : Wavelength-Division Multiplexing)

FDM (Frequency-Division Multiplexing) : FDM is an analog technique that can be applied when the band width of a link (in *hertz*) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined to a single composite signal that can be transported by the link. These bandwidth ranges are the channel through which the various signals travel channel can be separated by strips of uncured bandwidth guard bands to prevent signals from over lapping.



(Figure : Frequency Division Multiplexing)

TDM (Time Division Multiplexing) : TDM is a digital process that allow several connections to share the high bandwidth of a link. Each connection occupies a portion of time in the link. We can divide TDM into two different schemes i.e., synchronous and statistical.



(Figure : Time Division Multiplexing)

17.
- ***Describe internetworking connecting devices in reference to layers.*** (2018-19)
- ***Explain any two connecting devices : hubs, link- layer switches and routers.*** (2017-18)
- ***Describe the Repeater and Gateway.***
- ***Describe the Hub and Switches.***
- ***What are different Network Connecting Devices? Write at least four network connecting devices.***

- *Difference between switch and hub.*
- *Explain the functions and draw the Working*
- *Explain the functions and draw the Working Producer at the level of the Network Layer :*
  (1) *HUB*
  (2) *Switch*
  (3) *Bridge*

Hub

At its simplest level, the USB physical connection can be described as two transceivers connected by four conductors, two for signal, one for voltage and one for ground. Before delivering further into the electrical aspects of the physical layer, some explanation of the USB topology and device types is required.

The 127 connections advertised for the USB are achieved by the use of a special class of devices called Hubs. Each Hub counts as one of the 127 connections. The top device in the structure is called a Root Hub and is a component of the USB control circuitry associated with the host computer. All Hubs are devices that switch and regenerate input signals for delivery on output ports. However, in some implementations, the Root Hub might only support one output port. Hubs and all other USB devices are connected in a tiered star architecture with a Hub as the center of each star, as shown below :

Hub belongs to Physical Layer. In general, a hub is the central part of a wheel where the spokes come together. The term is familiar to frequent fliers who travel through airport "hubs" to make connecting flights from one point to another. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. A hub usually includes a switch of some kind. (And a product that is called a "switch" could usually be considered a hub as well.) The distinction seems to be that the hub is the place where data comes together and the switch is what determines how and where data is forwarded from the place where data comes together. Regarded in its switching aspects, a hub can also include a router.

Modem

A modem is a device that lets one send digital signals over an ordinary telephone line not designed for digital signals. If telephone lines were all digitals then you wouldn't need a modem. It permits your computer to connect to and communicate with the rest of the world. When you use a modem, you normally use a communication program or web browser to utilize the modem and dial-out on a telephone line. Advanced modem users can set things up so that others may phone in to them and use their computer. This is called "dial-in".

There are four basic types of modems for a PC: external, USB, internal and built-in. The external and USB set on your desk outside the PC while the other two types are not visible since they are inside the PC. The external modem plugs into a connector on the back of the PC known as a "serial port". The USB modem plugs into the USB bus cable. The internal modem is a card that is inserted inside the computer. The built-in modem is part of the motherboard and is thus built into the computer. It's is just like an internal modem except it can't be removed or replaced. As of 2001, built-in modems are primarily for laptops. What is said in this HOWTO regarding internal modems will generally apply also to built-in modems.

When you get an internal, built-in, or USB modem, you also get a dedicated serial port (which can only be used with the modem and not with anything else such as another modem or a printer). In Linux, the serial ports are named ttyS0, ttyS1, etc. (usually corresponding respectively to COM1, COM2, etc. in Dos/Windows). Modems usually include the ability to send Faxes (Fax Modems). "Voice" modems can work like an automatic answering machine and handle voicemail.

Switch : In telecommunications, a switch is a network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.

Relative to the layered Open Systems Interconnect (OSI) communication model, a switch is usually associat with layer 2, the Data-Link layer. However, some ne switches also perform the routing functions of layer 3, Network layer. Layer 3 switches are also sometimes ca IP switches.

On larger networks, the trip from one switch poi another in the network is called a hop. The time a sw takes to figure out where to forward a data unit is ca its latency. The price paid for having the flexibility t switches provide in a network is this latency. Switches found at the backbone and gateway levels of a netw where one network connects with another and at subnetwork level where data is being forwarded close t destination or origin. The former are often known as switches and the latter as desktop switches.

In the simplest networks, a switch is not require messages that are sent and received within the netw For example, a local area network may be organized token ring or bus arrangement in which each pos destination inspects each message and reads any mes with its address.

Gateway : Gateway is used in Transport, Ses Presentation and Application layer. Used communications between different NOS's (i.e. Window and IBM SNA). Takes the packet, strips off the old pro and repackages it for the receiving network.

A gateway is a network point that acts as an entr to another network. On the Internet, a node or stop point can be either a gateway node or a host (end-p node. Both the computers of Internet users and computers that serve pages to users are host nodes. computers that control traffic within your comp network or at your local Internet service provider (ISP gateway nodes. In the network for an enterpri computer server acting as a gateway node is often acting as a proxy server and a firewall server. A gatew often associated with both a router, which knows wh direct a given packet of data that arrives at the gat and a switch, which furnishes the actual path in and the gateway for a given packet.

Bridge

The data link layer of the OSI Model is the foundation of a network. It puts messages together, attaches proper headers to be sent or received and assures messages are delivered between two points. The data link layer does all this with a hardware device called a bridge.

A bridge is a more advanced than a repeater found in the physical layer, because not only does it transfer data between LANs, it also decides which data is to be transferred. The bridge reads the destination address of each data frame and decides if the address is local or remote. If the address is local, the bridge does not allow the information to be passed to another LAN. The bridge only allows passage if the address is no local. The data link layer has a sub-layer called the MAC Sub layer Protocol (Media Access Control) which deals with Ethernet and Token Ring architectures. The bridge is able to differentiate between the address by using such protocols. These protocols contain source addresses as well as destination addresses. The bridge checks these source addresses and adds them to a table of known local nodes in order to determine whether the frame should be allowed to cross the bridge or not.

Bridges that connect LANs of similar data link formats (Ethernet to Ethernet or Token Ring to Token Ring) are known as transparent bridges. A bridge that can link Ethernet LANs to Token Ring LANs is known as a translator bridge. This type of bridge, also known as multiprotocol bridges that includes a format converter that allows the bridge to link the two different networks. A third type of bridge called an encapsulating bridge is used to bridge Ethernet and FDDI networks. This type of bridge takes the Ethernet data link layer message and stuffs it into an "envelope" or Data Frame which conforms to the FDDI data link layer. A fourth type of bridge is a source routing bridge specifically designed connecting Token Ring networks.

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 so as 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
When the signal becomes weak, they copy the signal
bit and regenerate it at the original strength. It is a
device.

18. ◆ ***Discuss different standards of Ethernet.*** (2018-
◆ ***Define Protocol. Give the need for Proto Layering.*** (2017-
◆ ***Differentiate among the following :*** (2010-
(1) ***Protocol***
(2) ***Interface***
(3) ***Standard***
(4) ***Service***

(1) **Protocol** : In information technology, a protoc the special set of rules that end points telecommunication connection use when communicate. Protocols specify interactions bet the communicating entities.

Protocols exist at several levels in telecommunication connection. For example, t are protocols for the data interchange at hardware device level and protocols for interchange at the application program level. In standard model known as Open Syst Interconnection (OSI), there are one or more prot at each layer in the telecommunication exchange both ends of the exchange must recognize observe. Protocols are often described in an indu or international standard. The TCP/IP Inte protocols, a common example, consist of :

(a) Transmission Control Protocol (TCP), which a set of rules to exchange messages with Internet points at the information packet lev
(b) Internet Protocol (IP), which uses a set of r to send and receive messages at the Inte address level.
(c) Additional protocols that include the Hype Transfer Protocol (HTTP) and File Tra Protocol (FTP), each with defined sets of ru

use with corresponding programs elsewhere on the Internet.

There are many other Internet protocols, such as the Border Gateway Protocol (BGP) and the Dynamic Host Configuration Protocol (DHCP).

The word protocol comes from the Greek protocol on, meaning a leaf of paper glued to a manuscript volume that describes the contents.

An agreed-upon format for transmitting data between two devices. The protocol determines the following :

(i) The type of error checking to be used
(ii) Data compression method, if any
(iii) How the sending device will indicate that it has finished sending a message
(iv) How the receiving device will indicate that it has received a message

There are a variety of standard protocols from which programmers can choose. Each has particular advantages and disadvantages; for example, some are simpler than others, some are more reliable, and some are faster.

From a user's point of view, the only interesting aspect about protocols is that your computer or device must support the right ones if you want to communicate with other computers. The protocol can be implemented either in hardware or in software.

(2) **Interface** : In computer networking, a NIC is also commonly referred to as an Ethernet card and network adapter provides the hardware interface between a computer and a network. An NIC technically is network adapter hardware in the form factor of an add-in card such as a PCI or PCMCIA card.

Some NIC cards work with wired connections while others are wireless. Most NICs support either wired Ethernet or Wi-Fi wireless standards. Ethernet NICs plug into the system bus of the PC and include jacks for network cables, while Wi-Fi NICs contain built-in transmitters / receivers (transceivers).

In new computers, many NICs are now installed by the manufacturer. All NICs featur speed rating such as 11 Mbps, 54 Mbps or 100 M that suggest the general performance of the unit.

Most of the new motherboards available to for PCs and server have the network interface integrated with the motherboard. Older compu and some newer computers do not provide onbo network interfaces, which will require NIC to added.

NICs provide computers with a connection to network, but they also handle important conversion function. Data travels parallel on the bus system, but the network medium demand serial transmission. The transceiver, a transmitte receiver, on the NIC has the ability to move data f parallel to serial and vice versa. This is not different than an automobiles travelling down a m lane superhighway where all lanes must merge one lane.

Network Interface cards also have the abili supplying a basic addressing system that can be to get data from one computer to another on Network. The hardware or MAC address is burn into a ROM chip on the NIC. This is referred to as MAC address because the media access proto layer is actually a sublayer of the OSIs model link layer.

(3) Standards : IEEE 802 refers to a family of I standards dealing with local area networks metropolitan area networks.

More specifically, the IEEE 802 standards restricted to networks carrying variable-size pack (By contrast, in cell relay networks data transmitted in short, uniformly sized units c cells Isochronous networks, where data transmitted as a steady stream of octets, or grou octets, at regular time intervals, are also out o scope of this standard.) The number 802 was si the next free number IEEE could assign, th "802" is sometimes associated with the date the meeting was held - February 1980.

The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC), so that the layers can be listed like this :

(a) Data link layer
(b) LLC Sublayer
(c) MAC Sublayer
(d) Physical layer

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

A set of network standards developed by the IEEE. They include :

(i) IEEE 802.1 : Standards related to network management.

(ii) IEEE 802.2 : General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sublayers – the logical link control (LLC) layer and the media access control (MAC) layer. The MAC layer varies for different network types and is defined by standards IEEE 802.3 through IEEE 802.5.

(iii) IEEE 802.3 : Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard. Also see the Ethernet Designations chart in the Quick Reference section of Webopedia.

(iv) IEEE 802.4 : Defines the MAC layer for bus networks that use a token-passing mechanism (token bus networks).

(v) IEEE 802.5 : Defines the MAC layer for token-ring networks.

(vi) IEEE 802.6 : Standard for Metropolitan Area Networks (MANs).

(4) **Service :** A PRIMITIVE means operations. A service in a computer network consists of a set of primitives. The primitives are to be used by the user to access the service. The primitives ask the service to do some action or to report on an action. The primitives are system calls. The primitives vary for different services. The following are some of the primitives used in a computer network. LISTEN means the block is waiting for an incoming connection. CONNECT means to establish a connection. RECEIVE means the block is waiting for an incoming message. SEND means to send a message. DISCONNECT means to terminate a connection.

19. *What is security goals? Explain different types of Network Attacks.* (2018-19)

Security Goals

Three primary goals of Network Security are

(1) Confidentiality
(2) Integrity
(3) Availability

These three pillars of Network Security are often represented as CIA Triangle, as shown below :

(Figure)

Confidentiality : The first goal of Network Security is "Confidentiality". The function of "Confidentiality" is in protecting precious business data (in storage or in motion) from unauthorized persons. Confidentiality part of Network Security makes sure that the data is available only to intended and authorized persons.

Integrity : The second goal of Network Security is "Integrity". Integrity aims at maintaining and assuring the accuracy and consistency of data. The function of Integrity is to make sure that the date is accurate and reliable and is not changed by unauthorized persons or hackers. The data

received by the recipient must be exactly same as the data sent from the sender, without change in even single bit of data.

Availability : The third goal of network security is "Availability". The function of "Availability" in Network Security is to make sure that the Data, Network Résources or Network Services are continuously available to the legitimate users, whenever they require it.

Types of Attack

There are two types of network security attack.

Active Attacks : Active attacks involve some modification of the data stream or the certain of a false stream and can be subdivided into four categories : masquerade, replay, modification of message, and denial of service.

(1) **Masquerade** : It take place when one entity pretends to be a different entity. A masquerade attack usually included one of other forms of active attack.
(2) **Replay** : It involves the passive capture of data unit and its subsequent retransmission to produce an unauthorized effect.
(3) **Modification of Messages** : It simply means that some portion of a legitimate message is altered or that message delayed or recorded to produce an unauthorized effect.
(4) **Denial of Service** : It prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target.

Passive Attacks : Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmissions. Two types of passive attacks are release of message contents and traffic analysis.

(1) **Release of Message Contents** : It is easily understood. A telephone conversation, an electronic mail message, and a transferred file may certain services or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.
(2) **Traffic Analysis :** It is subtler. Suppose that we had a way of making the contents of message and other information traffic so that opponents, even if they

captured the message, could not extract th information from the message. The comm technique for making content is encryption. If we ha encryption protection in place, an opponent migh still be able to observe the pattern of these message The opponent could determine the location an identity of communication hosts and observe th frequency and length of messages being exchange This information might be useful in guessing th nature of the communication that was taking place

20. ◆ ***Write minimum five comparison of TCP/IP and ISO/OSI model.***

◆ ***What are the difference and similarities between OSI reference model and TCP/IP reference model?***

Similarities

	OSI Seven-Layers Model	TCP-IP Reference Model
Application	It is the totality of all applications and their relating protocols that use networks and have not yet been represented by the lower layers.	Like OSI Model, contains all th higher-level protocols.
Presentation	Here are the standards necessary for unambiguously representing data and more generally, syntax of messages to be transmitted (simple text, executable code, pictures)	Because no need fo them was perceived Presentation and Session layers are not included in the TCP/IP Model
Session	It establishes a connection with another node and manages the data flow from the higher layers to the lower ones by managing the timing of data transmission and the memory buffer managing, when several applications try to transmit data at the same time	
Transport	It handles the transmission, reception & error checking of the data	The same as OS Model

Network Internet	It is concerned with the physical transmission of the data from computer to computer. There is one further level of software to be considered, the network level. It routes the packages across a particular network.	It is the linchpin that holds the whole architecture together it permits to send and receive packets, even if they are in random order
Link Host to	It handles the transmission of a framed set of data (usually a sequence of bits) from one point in a network (node) to another one. This layer also represents the boundary between hardware (e.g. CRC) and software implementation (e.g. physical addressing).	The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to
Physical Network	The physical medium used to transmit the information. To specify this layer, it is necessary to define the physical properties of the connection, such as mechanical properties, electrical/optical properties, functional aspects of the data transmission (modulation / demodulation for example) and procedural aspects of data transmission (e.g. bit stuffing to ensure that special signals are unequivocal).	Connect to the network using some protocol so it can send IP packets over it. This protocol is not defined and varies from host to host and network to network.

So, we can see that TCP/IP Reference Model and OSI Reference Model have a lot of things in common. Conceptually, it is useful to envision TCP/IP as a stack, each layer corresponding to a different facet of communication.

So we can introduce main differences between from these concepts.

Type of Difference	OSI Model Reference	TCP/IP Model Reference
Service, Interface and Protocol	Service, interface and protocol are not clearly defined. For example, the only real services offered by the Internet layer are -Send IP Packet	Protocols in the OSI model are better hidden and can be replaced relatively easily as the technology changes, which is one of the main objectives of

	- Receive IP Packet	layered protocols.
Functionalities	Because models were invented before protocols, functionalities put in each layer are not very optimized.	In this case, the protocols have been invented before models, so the functionalities are perfectly described.
Numbers of layers	Seven layers, Network (Internet), Transport and Application layers being similar to TCP/IP	Only four layers.
Connectionless/ Connection-oriented communication	Both connectionless and connection-oriented communications are supported in the network layer, but only connection-oriented communication in the transport layer.	Only one mode in the network layer (connectionless) but both modes in the transport layer are supported, giving the users a choice.

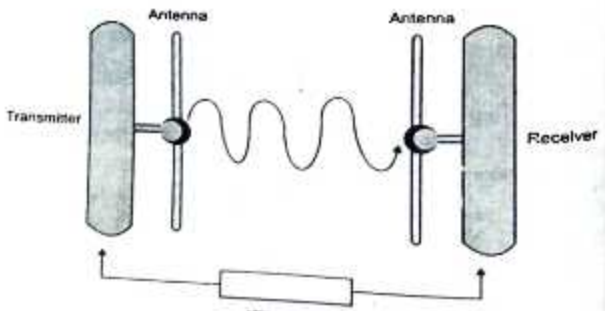
21. *Define Radio wave.* **(2017-18)**

Radio Wave

Radio waves are a type of electromagnetic radiation as are microwaves, infrared radiation, X-rays and gamma-rays. The best-known use of radio waves is for communication; television, cellphones and radios all receive radio waves and convert them to mechanical vibrations in the speaker to create sound waves that can be heard.

Radio waves have the longest wavelengths in the EM spectrum.

Radio Wave



(Figure)

22. *Explain Nyquist Bit Rate.* **(2017-18)**

Nyquist Bit Rate

Nyquist bit rate defines the theoretical maximum bit rate for a noiseless channel or ideal channel.

The formula for maximum bit rate in bits per second (bps) is :

$$\text{Maximum bit rate} = 2 \times BW \times \log_2 L$$

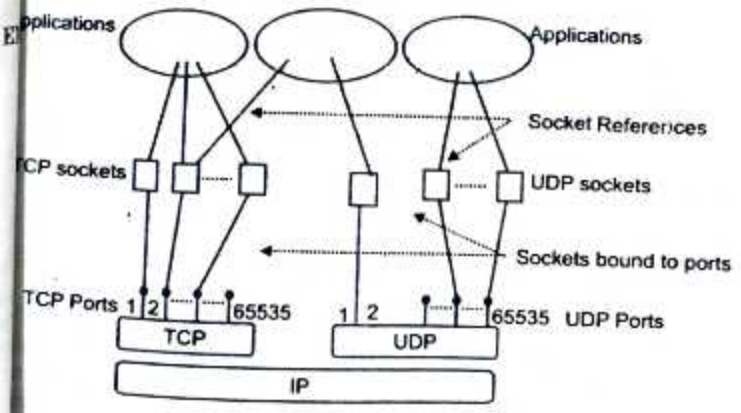
Where, BW = Bandwidth at channel

L = Number of signal levels used to represent data.

23. *Write about Socket.* **(2017-18)**

Socket

A socket is an abstraction through which an application may send and receive data, in much the same way as an open file handle allows an application to read and write data to stable storage. A socket allows an application to plug in to the network and communication with other applications that are plugged in to the same network. Information written to the socket by an application on one machine can be read by an application on a different machine and vice versa.



(Figure)

24. *Give different categorization of computer networks. What is internet works?*

Categorization of Computer Networks

It can be done in two ways based on :

(1) Transmission Technology

(2) Scale

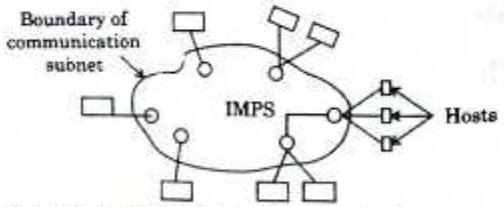
(1) **Transmission Technology :** There are two types design for the communication subnet :

(a) Point to point channels

(b) Broadcast channels

(a) **Point to Point Channels :** The netwo contains numerous cables or leased telepho lines each one connected a pair of IMPs if IM that do not share a cable never the lines wish communicate they must do this indirectly other IMPs.

(b) **Broad Cast Channels :** The second kind consumer certain architecture uses broad casti most local area network and small number WAN are of this type. In local area network IMP is reduced to a single chip embedded ins the host so there is always one host per I Where as in a wide area network there may many hosts per IMP.



(Figure : Relation between Host and Subnet)

(2) **Scale :**

(a) LAN

(b) MAN

(c) WAN

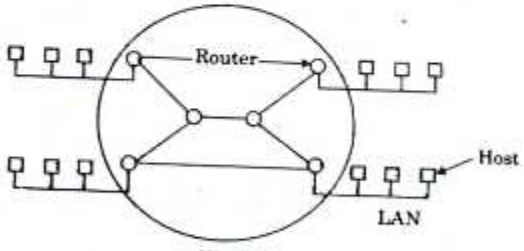
(d) **Wireless Networks :** To a first approxima wireless networks can be divided into three categories. System interconnection is all interconnecting the components of a com

using short-range radio. In wireless LANs, there are systems in which every computer has a radio modem and antenna will which it can communicate with other systems. The radio network used for cellular telephones is an example of a low-bandwidth wireless system.

(e) **Home Network :** Many devices are capable of being networks computers, entertainment (TV, DVD, VCR, MP3), tele-communication (telephone, mobile telephones, intercom, fax), Appliances (microwave, refrigerator, clock, furnace, lights), Telemetry (utility meter, smoke/burglan alarm) etc.

(f) **Internet Works :** People connected to one network wants to communicate with people attached to a different one. These different and incompatible networks are connected by gateways.

Inter Networks : A common form is a collection of LANs connected by a WAN. An Internet work is formed when distinct networks are interconnected.



(Figure)

In any network, there exists a collection of machine intended for running users programs. The following terminology is one of the most major networks the ARPANET and calls this machine host. The term end system is sometimes also used in the literature. The host is connected by the communication subnet or just subnet for short. There are different types of networks like LANs, MANs, WANs.

In WAN (Wide Area Network) subne consists of two distinct component Transmission lines and switching element Transmission lines (also called circuits, channel or trunks) move bits between machines.

The switching elements are specialize computer used to connect two or mor transmission lines switching element mu choose an outgoing line to forward them on.

In the ARPANET terminology IMP (Interface Message Processor) the term packe switch node, intermediate system and dat switching exchange are also commonly used.

25. *In mesh topology network with 25 computers, how much cabling is required?* **(2013-14)**

Number of cables = $n(n-1)/2 = 25(25-1)/2 = 300$.

26. *Which OSI layer performs of the following activities :*

(1) ***Error detection and correction***

(2) ***Routing***

(3) ***Responsibility for delivery between adjacent modes.***

(4) ***Reliable process to process data transportation.*** **(2013-14)**

(1) Error detection and correction : Data-Link Lay

(2) Routing : Network Layer

(3) Responsibility for Delivery between Adjace Modes : Data Link Layer

(4) Reliable Process to Process D Transportation : Transportation Layer.

27. *Explain baud rate with a suitable example. If binary signal is sent over a 3-kHz channel whos signal-to-noise ratio is 20 dB? What is th maximum achievable data rate?* **(2010-1**

Baud Rate

The baud rate of a data communications syste the number of symbols per second transferred. A sy

may have more than two states, so it may represent more than one binary bit (a binary bit always represents exactly two states). Therefore the baud rate may not equal the bit rate, especially in the case of recent modems, which can have (for example) up to nine bits per symbol.

Baud means "state changes of the line per second".

Baud Rate=2*Bit rate

Numerical Solution :

As Capacity = Bandwidth$*\log_2(1+SNR)$

Given : Bandwidth = 3 KHz =3000 Hz.

SNR ratio = 20 dB

Therefore, $C = 3000*(\log_{10}21/\log_{10}2)$

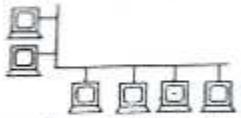
$C = 13177$ bps.

Data rate = 13177 bps.

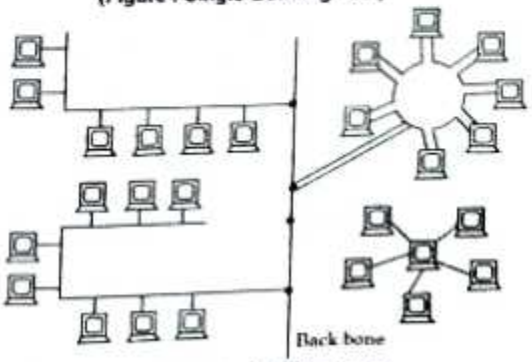
28. *What is a LAN? Explain any two LAN Access methods, giving example of at least one topology that uses them.*

LAN

A Local Area Network (LAN) is usually privately owned and links the devices in a single office, building or campus.



(Figure : Single-Building LAN)



(Figure : Multiple- Building LAN)

Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PC's and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals.

LAN is designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (example, a printer), software (example an Application program), or data.

(Figure : LAN Specification)

A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs.

Access Methods

There are a number of methods used as access protocols in LANs, major techniques being token passing, CSMA/CD and TDMA.

(1) **CSMA/CD** : (Carrier Sense Multiple Access, with Collision Detected) is used with bus and some star topologies. It operates by contention, each terminal competes for access to the bus. A terminal wishing to transmit attempts this when the bus is quiet. Simultaneously, received signals are monitored by this terminal to check for corruption resulting from collision with another transmission present at the same time. In the event of such a collision its effect on this terminal is enforced with the use of a jamming signal and all current transmissions are stopped. Repeated retransmissions are made with designed delays to reduce the probability of further collisions until successful transmission occurs. When carrying long data packets over short cables and with offered traffic of about 20% or less of maximum, the system works extremely well.

(2) **TDMA** : (Time Division Multiple Access) was originally devised for digital microwave and satellite communications systems. It is still used with many such systems as well as with some fiber optic systems. Fixed time slots are made available, regardless of whether they are actually used. The complete end to end bit sequences within each time slots are usually called a serial packets each of which comprises : source and destination address, data bits, control and status bits. The system is accessed through terminal stations and repeaters. Transmission is into an empty packet or packets and reception occurs via packet address recognition. A monitor station monitors the integrity of the system during normal operation and places framing bits around packets in the initializing process.

LAN Topologies : LAN Topologies define the manner in which network devices are organized. Four common LAN topologies exist bus Ring star and tree.

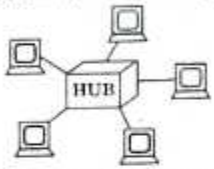
(Figure : Local Bus Topology)

These topologies are logical architectures, but the actual devices need not be physically organized in these configuration. Logical bus and ring topologies, for example, are commonly organized physically as a star. A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations, of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks including 100 Base T-implement a bus topology.

(Figure : Local Ring Topology)

A ring topology is a LAN architecture th consists of a series of devices connected to o another by unidirectional transmission links form a single closed loop. Both Token Ring/IEE 802.5 and FDDI networks implement a ri topology.

A star topology is a LAN architecture which the endpoints on a network are connected to common central hub, or switch, by dedicated links.



(Figure : Star Topology)

DATA LINK LAYER

1. ◆ ***Write three characteristics of data link layer.***
   ◆ ***Write the five functions of data link layer.***
   ◆ ***Draw and explain each function in detail.***
   ◆ ***Explain the functions of data link layer.***

The data link layer implemen[illegible] following functions :

(1) Grouping of bits on the physical layer into frames.

(2) Detecting and correcting transmission errors.

(3) Regulating the flow of frames (and hence the data rate) on the data link such that fast senders do not swamp receivers.

(4) Carrying out functions for data link management.

Each of these functions performed by the data link layer are described below :

(1) Framing : At the physical layer, information is transmitted as a raw bit stream. Due to transmission errors in the physical path, the bits received at the other end of the physical media may have different values than what was transmitted. Therefore the function of the data link layer is to detect, and if possible, correct the errors in the bit-stream received from the physical layer.

To achieve this, the data link layer computes a checksum over each chunk of information that it transfers over the physical layer. The chunk of information over which the checksum is computed is called a Frame.

(2) Error Control : Errors are commonly observed when transmitting over communication links. Bit errors are introduced by signal attenuation and electromagnetic noise in the communication link. A major source of noise for data transmission is impulse noise. Another major source of errors arises from the fact that the amplitude, propagation speed and phase of signals are all frequency dependent.

In order to overcome these transmission err protocols are introduced in the data link layer, wh detect such errors and correspondingly ta appropriate action. Thus error control includes one more of the following steps :

(a) Detection of corrupted frames.

(b) Correcting the errors in the corrupted frame case sufficient information is present in received frame for error correction.

(c) Sending negative acknowledgement to sender, in case the received error frame can be recovered, which may trigger re-transmiss at the sender's end.

(d) Managing timers and sequence numbers so a ensure that each frame is ultimately passed the network layer at the destination exa once.

(3) **Flow Control :** Flow control is a means used synchronize between the sender's sending capac and the receiver's receiving capacity. communication networks, flow control is mechanism used to control the flow of data betw the sender and the receiver's buffers do not overfl Flow control mechanisms are broadly classified in two categories : window-based flow cont mechanisms and rate-based flow control mechanism In a window-based flow control mechanism the foc is on tackling the memory-related bottlenecks. rate-based flow control mechanisms, on the oth hand, the focus is on tackling the link and process speed bottlenecks instead.

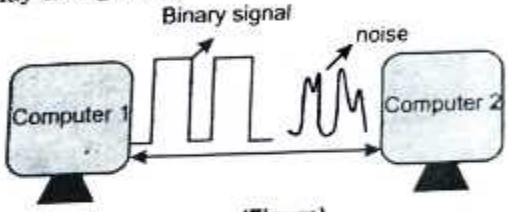
(4) **Link Management :** Another important function the data link layer is to manage the administration the data link, and to discipline the use of the d link. For connectionless services, this administrat is minimal and for connection-oriented services, it far more complex.

The master slave protocol is one kind of proto used for link management. Multiple other varieties protocols exist for link management.

2. *What is Error? Explain Error detection and Error correction.*

Error

Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.



(Figure)

Error-Detecting Codes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is parity check.

Error-Correcting Codes

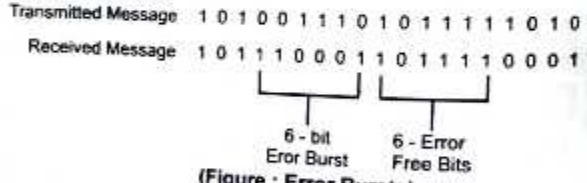
Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit.

In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message.

Detect and Correct Errors : To detect and correct the errors, additional bits are added to the data bits at the time of transmission.

The main advantage of this scheme is the detection two-bit error. As a simple parity bit can detect only sin bit error. If two-bit changes occur in the transmitted da the resultant parity bit is same as the parity of transmitted character. In the above scheme, if a two- error occurs in a transmitted character, the received par bit remains the same. But these two bit errors change t column parity at the receiver. Hence, the receiver c identify two-bit errors. But simultaneous occurrence two-bit errors in two characters at the same colum positions can be unnoticed by the receiver. Clearly, t probability of this occurring is much less than t probability of two-bit errors.

The simple parity and block sum check methods a well suited for applications in which random single b errors are present. More precautionary measures; are to taken to control continuous error burst. An error burst defined as the number of bits between two successive er bits, including the two incorrect bits. The length of t error burst is determined from the number B, t difference between the last erroneous bit in a burst and t first erroneous bit of the next burst. In this case, B corre bits separate the two bursts. The following figu illustrates the error bursts that occur in the transmitt sequence of bits.



(Figure : Error Bursts)

Parity or block sum check does not provide a reliab error detection scheme for burst error. A new techniqu called polynomial codes are used for the identification errors. Along with each block of data transmitted, a sing set of check-digits are also transmitted. The check - digi are generated based on a predefined method computation. At the receiver, the same computation again performed with the received set of data, and t results are compared with the received check digits. If bo the computed and the received check digits match, th

there is no error in the transmission. On the other hand, if they differ, then it is considered as an error in the transmission. The computed check digits are known as frame check sequence or cyclic redundancy check (CRC) digits. Following section gives details of CRC codes.

Cyclic Redundancy Check (CRC)

CRC is the most widely used error - detecting method alternative to the simple parity check codes. Instead of adding the number of bits to obtain the desired parity, in CRC a sequence of 'extra' redundant bits are added at the end of data. These bits are known as CRC bits. The CRC bits are derived from the original data bits. The method of deriving the CRC bits at the sending side is given below :

Step 1 : A sequence of bit stream is formed by appending n '0' bits to the data at the end.

Step 2 : A predetermined devisor of length n+ 1 bits is used to divide the sequence and the remainder is calculated. The remainder is known as CRC.

Step 3 : The remainder replaces the extra bits added to the data at the beginning.

Step 4 : The combined sequence of data plus CRC is transmitted by the sender.

At the receiving end the received data plus CRC is again divided by the same divisor as used at the sending side. If the remainder is zero then it is presumed that the data is error - free and the receiver accepts the data, on the other hand if the remainder is non-zero, the data is considered as corrupted and the received data is discarded. For example, consider the 6-bit data sequence "100110". Let us choose a 3-bit divisor 110at the sending side. As per the step 1, two 0s are added to the data sequence and the new sequence is "10011000". As per the second step, the new sequence is divided by 110 (Modulo-2 division is used), and produces a remainder of 10. This is the CRC. As stated in step 3, this CRC code is added to the data sequence to produce a sequence "10011010" and then transmitted.

At the receiver side, if the received sequence does not contain an error, the sequence "10011010" is again divided by the same divisor 110 and the remainder is 00. If an error is made in one or two bits (corrupted), then the remainder will not be a 00, hence, the receiver rejects the data.

Checksum Another method of error detection, oft used in higher order layers is checksum.

Checksum is computed at the sending end using t following steps.

Step 1 : The data sequence is divided into 'K' words same size n (8 or 16 bits).

Step 2 : All words are added using l's complement additi and the sum is computed.

Step 3 : The l's complement of the sum, known checksum is transmitted with the data.

At the receiver side, the following steps are carri out after receiving the data with checksum

Step 1 : The data sequence is divided into 'K+1' words same size 'n' (8 or 16 bits).

Step 2 : All words are added using l's complement additi and the sum is computed.

Step 3 : The sum is complemented, if it is 0, the data error – free and is accepted; otherwise the received data discarded.

Error Correcting Codes : Techniques covered so far de with error detection only. When error detecting techniqu are used, and the receiver receives the data with error, th receiver discards the data and asks for retransmission. O the other hand, error-correcting codes are used to identi the error bits in the received data and correct them. Th main problem with error-correcting codes is that th require more redundancy bits than the error-detecti codes. This leads to wastage of transmission bandwidth.

Single - Bit Error Correction : The key issue in erro correction is to identify the position of invalid error bit, order to correct it. For example, when 7-bit ASCII code transmitted, the error-correcting code must identify th position of the bit that contains an error. Hence, at leas three redundant bits are used to identify the possibility error in the seven positions in an ASCII characte However, if an error occurs at the redundant bi themselves, to identify it, additional bits are require Hence the total number of bits in the transmitted da contains m + k bits. M is the number of message bits and is the number of redundant bits.

The calculation of the total number of redundant bi for single bit error correction is straightforward. One bit

used for ensuring that the received data is error-free. Other bits are used to indicate one out of M message and K redundant bits that may contain an error. Hence, the value of K must be chosen such that 2K <: M+K+ 1. For example to correct single bit error in 7-bit ASCII code, at least 4 redundant bits are needed. Hence, the transmitted data contains 11bits for each data units.

Hamming Codes RW : Hamming illustrated the concept of hamming distance, which is useful in considering the properties of codes. Hamming distance is defined as the number of bit positions by which two states differ from each other. This parameter is very useful for error-detection and correction. Hamming introduced a code for single bit error correction by inserting multiple parity check bits at selected positions of data before transmission. The receiver recalculates the check - bits, compares it with the received check - bits, and determines the error bit. For 4~bitcode three check - bits are required for error-correction as shown in Figure.

Bit Posibon →	7	6	5	4	3	2	1	
				4		2	1	← Chek bit weight
	8	4	2		1			← Message weight
	M_4	M_3	M_2	K_3	M_1	K_2	K_1	
	0	0	0	0	0	0	0	$K_1 = M_1 \oplus M_2 \oplus M_4$
	0	0	0	1	1	1	1	$K_2 = M_1 \oplus M_3 \oplus M_4$
	0	0	1	1	0	0	0	$K_3 = M_2 \oplus M_3 \oplus M_4$
	0	0	1	1	1	1	0	
	0	1	0	1	0	1	0	
	0	1	0	1	1	0	1	

Modulo-2 addition is used for the formation of the K redundant check bits. If any of the message bit is corrupt, then the received check bits may appear as incorrect. For example if the message bit M2 of the third message unit is incorrect (see the encircled bit of the third row), it appears as 0 instead of 1. In this case, the receiver calculates the

check bits K1and K3as 0 and 0 respectively instead of 1 as it is now. The position of the error bit is computed by simply adding the weights of K1 (1) and K3 (4) that is 4+1=5, hence, bit at position 5, that isM2 is the error bit. Similarly, if anyone of the check bit is invalid (see the encircled bit of the last row), its weight indicates the position of the error bit (4 in this case). Hence hamming codes can be much useful to perform single bit error correction. For double bit and 3-bit errors the number of redundant bits required is more than that of the message size.

5. *Write short note on SONET.* **(2018-19)**

SONET

Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources primarily to support real-time, uncompressed, circuit switched voice encoded in PCM (Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

6. *Write short note on ATM.* **(2018-19)**

Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual

circuit must be established between two endpoints before the actual data exchange begins.

While the role of ATM is diminishing in favor of next-generation networks, it still plays a role in the last mile, which is the connection between an Internet service provider and the home user.

7. *Write short note on BLUETOOTH.* **(2018-19)**

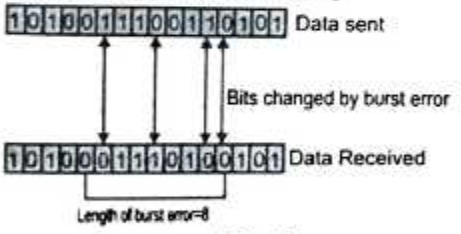
Bluetooth

Bluetooth is a wireless technology standard for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in the industrial, scientific and medical radio bands, from 2.400 to 2.485 GHz, and building personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables.

8. *Explain burst error.* **(2017-18)**

Burst Error

It means two or more bits in data unit are changed from 1 to 0 from 0 to 1 as shown in fig.



(Figure)

In burst error, it is not necessary that only consecutive bits are changed. The length of burst error is measured from first changed bit to last changed bit. As shown in fig. length of burst error is 8, although some bits are unchanged in between. Burst error is most likely to occur in a serial transmission. The noise occurring for a longer duration affects multiple bits. The number of bits affected depends on the data rate & duration of noise. For *e.g.* if data rate is 1 kbps, a noise of 1/100 second can affect 10 bits.

9. ◆ ***Describe hamming code. How it is used for error detection and correction? Illustrate with the help of a suitable example.*** **(2017-18)**
◆ ***What is Hamming code? For the following word pattern (message), find out the number of check bit and the bit at eleventh position. If any error is detected, show it.***
M = 1111 1010 0000 1110

Hamming Code

(1) Hamming code is the code that is used for the error detection and correction.

(2) The Hamming code can be applied to the data units of any length and uses the relationship between data and redundancy bit.

Example : 7 bit ASCII code requires 4 redundancy bits, that can be added to the end of the data unit or inter aspersed with the original data bits.

For 7 bit

$$2^r >= m + r + 1$$

$$M = 7$$

$$2^r >= m + r + 1$$

$$2^r > r + 8$$

$$\Rightarrow \quad r = 4$$

11	10	9	8	7	6	5	4	3	2	1
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

r_1	bits	1, 3, 5, 7, 9, 11
r_2	bits	2, 3, 6, 7, 10, 11
r_4	bits	4, 5, 6, 7
r_8	bits	8, 9, 10, 11

M = 1111 1010 0000 1110

$m + r = 16$

$\Rightarrow \quad 2^r \geq 16 + 1$

$\Rightarrow \quad 2^5 \geq 17$

$r = 5$ *bits*

$m = 11$ *bits*

r_{16}	d_{15}	d_{14}	d_{13}	d_{12}	d_{11}	d_{10}	d_9	r_8	d_7	d_6	d_5	r_4	d_3	r_2	r_1
1	1	1	1	1	0	1	0	0	0	0	0	1	1	1	0

Parity bits

r_1 = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21 = 1

r_2 = 2, 3, 6, 7, 10, 11, 14, 15, 18, 19 = 1

r_3 = 4, 5, 6, 7, 12, 13, 14, 15, 20, 21 = 1

r_8 = 8, 9, 10, 11, 12, 13, 14, 15 = 0

r_{16} = 16, 17, 18, 19, 20, 21 = 1

10111 = 23

Error is at Bit position 23 which does not exist, so no error.

10. ***Write and explain Protocol differentiate one of each other :***
(1) ***CSMA/CD***
(2) ***CSMA/CA***

(1) CSMA/CD : (Carrier Sense multiple Access Collision Detection) : This multiple access method is used in wired networks since it is possible to detect collision and then proceed with so used in LANs and WANs.

This is used by IEEE 802.3 standard Ethernet networks in which each node monitors the traffic in the line and if no traffic is available then a particular node can transmit. But at the same time if two are trying to transmit then it is known as a collision. This situation is sensed by the nodes in the given network. After that the stations which had the collision will try to send data again after some random time interval which are vary for each node. If again a collision takes place the random time taken is increased and waits again. This is the procedure used in CSMA CD networks and the method does not have any deterministic capability.

(2) CSMA/CA : (Carrier Sense Multiple Access Collision Avoidance) : This is the multiple access scheme used in layer 2 access method in which the following method is used when nodes are trying to transmit simultaneously in a shared network. Here

the node which wishes to transmit first has to listen to the medium for a pre determined period to assess the channel state. If the channel is idle then the node is capable of transmitting. Else the channel is said to be busy and node has to wait until the channel comes to idle mode.

This is implemented in IEEE 802.11 wireless LAN and other wireless networks and this is preferred since the wireless networks cannot detect collision while transmitting like wired networks. So the implementation of CSMA/CA will improve the packet dropping in wireless networks.

Difference Between CSMA/CD and CSMA/CA

(1) CSMA/CD is used in wired LANs and CSMA/CA is used in wireless LANs and other types of wireless networks.

(2) CSMA/CD is standardized in IEEE 802.3 and CSMA/CA is standardized in IEEE 802.11.

(3) CSMA/CD will not take steps to prevent transmission collision until it is taken place whilst CSMA/CA will take actions not to take place any collision since the latter has no means of knowing whether a collision has taken place.

11. *Write and explain with the help of example in the Transport Layers of Error Control :*
(1) *WRC*
(2) *VRC*
(3) *CRC*

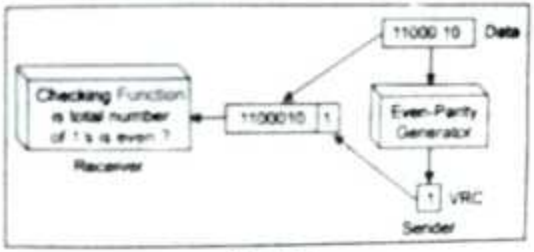
(1) WRC : To achieve at least some harmonization, the ITU-R holds the World Radio Conference (WRC) to periodically discuss and decide frequency allocations for all three regions. This is obviously difficult task as many regions or countries may have already installed a huge base of a certain technology and will be reluctant to change frequencies just for the sake of harmonization. Harmonization is, however, needed as soon as satellite communication is used.

(2) Vertical Redundancy Check (VRC) :

(a) Most common and inexpensive mechanism error detection which also called parity check.

(b) A redundant bit (parity bit) is appended to every data unit so that the total number of 1s in the unit becomes even, if there is even-parity check used.

(c) There are even-parity check and odd-parity check. For odd-parity check, the total number of 1s in the unit is odd. Suppose we want to transmit the binary data unit 1100001, adding the number of 1s gives us 3, an odd number. Before transmitting, a parity generator counts the 1s and appends the parity bit (a 1 in this case) to the end. The total number of 1 becomes 4 now (even number). The system now transmits the entire appended unit across the network link.



(Figure)

(d) When the data unit is reached its destination, the receiver puts all eight bits through an even-parity checking function. If the receiver sees 11100001, it counts and gets four 1s, an even number.

(e) But if the receiver sees 11100101, or total number of 1s is odd. The receiver knows that an error has been occurred into the data somewhere and therefore rejects the whole unit.

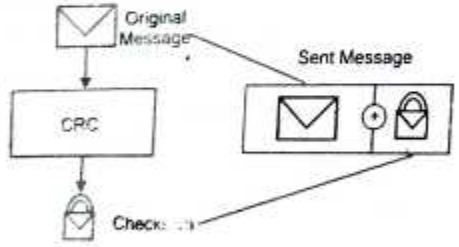
(f) For the odd-parity checking, the principle is same but the calculation is different.

(g) The advantages of VRC are it can detect all single-bit errors. It also can detect burst errors as long as the total number of bits changed is odd (1,3,5, etc). The same holds true for any odd number of errors.

The limitation is it cannot detect errors w the total number of bits changed is even, where two bits of the data unit are changed. In this case total number of 1s is still even. The VRC checker add them and return an even number although data unit contains two errors. Then the unit will p a parity check even through the data unit damaged. The same holds true for any even num of errors.

(3) Cyclic Redundancy Check : A cyclic redunda check (or CRC for short) is a power easy-to-implement data integrity control method. I the primary method of error detection used telecommunications.

Concept : Cyclic redundancy checking involv protecting data in blocks, called frames. Each fra is assigned a segment of data, called a control co (occasionally FCS for Frame Check Sequence in t case of a 32-bit sequence, and sometimes erroneou labeled a CRC). The CRC code contains da redundant with the frame, so that errors can be n merely detected, but fixed.



(Figure)

The concept f CRC involves treating bina sequences as binary polynomials, meaning polynomi whose coefficients correspond to the binary sequence. F example, the binary sequence 0110101001 may represented as a polynomial as shown here :

1 $0*X^9 + 1*X^8 + 1*X^7 + 0*X^6 + 1*X^5 + 0*X^4 + 1*X^3 + 0*X^2 + 0*X^1 + 1*$
2 Which is
3 $X^8 + X^7 + X^5 + X^3 + X^0$
4 or
5 $X^8 + X^7 + X^5 + X^3 + 1$

In this way, the lowest-weight bit in the sequence (the one furthest to the right) represents degree 0 of the polynomial ($X^0 = 1$), the 4th bit from the right represents degree 3 of the polynomial (X^3), and so on. An *n*-bit sequence, then, forms a polynomial of a maximum degree of *n-1*. All polynomial expressions are then manipulated using modulo 2.

In this error-detection process, a predefined polynomial (called the generator polynomial and shortened to G(X)) is known to both the sender and the recipient. The sender, to start the error detection mechanism, runs an algorithm on the frame bits in order to generate a CRC, and then transmits these two elements to the recipient. The recipient then performs the same calculation in order to check that the CRC is valid.

12. ◆ ***Write short note on the Go back N.***
◆ ***Compare two data link layer protocols, Go Back N and selective repeat in terms of flow control, error recovery and packet loss.***

Difference Between Go-Back-N and Selective Repeat Protocol

(Figure)

"Go-Back-N Protocol" and "Selective Repeat Protocol" are the sliding window protocols. The sliding window protocol is primarily an error control protocol, i.e. it is a method of error detection and error correction.

The basic difference between go-back-n protocol and selective repeat protocol is that the "go-back-n protocol" retransmits all the frames that lie after the frame which is damaged or lost. The "selective repeat protocol" retransmits only that frame which is damaged or lost.

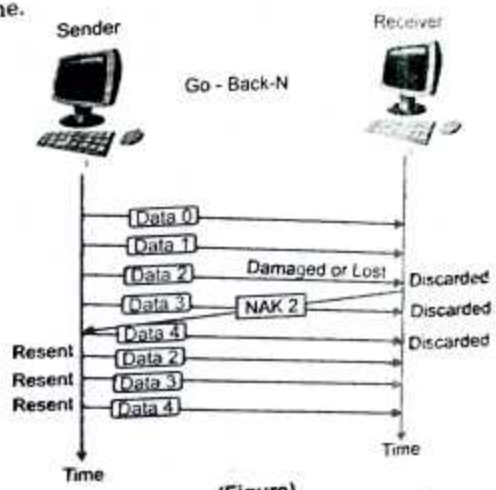
Comparison Chart :

Basis for Comparison	Go-Back-N	Selective Repeat
Basic	Retransmits all the frames that sent after the frame which suspects to be damaged or lost.	Retransmits only those frames that are suspected to lost or damaged.
Bandwidth Utilization	If error rate is high, it wastes a lot of bandwidth.	Comparatively less bandwidth is wasted in retransmitting.
Complexity	Less complicated.	More complex as it requires to apply extra logic and sorting and storage, at sender and receiver.
Window size	N-1	<= (N+1)/2
Sorting	Sorting is neither required at sender side nor at receiver side.	Receiver must be able to sort as it has to maintain the sequence of the frames.
Storing	Receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.	Receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.
Searching	No searching of frame is required neither on sender side nor on receiver	The sender must be able to search and select only the requested frame.
ACK Numbers	NAK number refer to the next expected frame number.	NAK number refer to the frame lost.
Use	It more often used.	It is less in practice because of its complexity.

Definition of Go-Back-N

Go-Back-N protocol is a sliding window protocol. It is a mechanism to detect and control the error in data link layer. During transmission of frames between sender and receiver, if a frame is damaged, lost, or an acknowledgement is lost then the action performed by sender and receiver is explained in the following content.

Damaged Frame : If a receiver receives a damaged frame or if an error occurs while receiving a frame then, the receiver sends the NAK (negative acknowledgement) for that frame along with that frame number, that it expects to be retransmitted. After sending NAK, the receiver discards all the frames that it receives, after a damaged frame.



(Figure)

The receiver does not send any ACK (acknowledgement) for the discarded frames. After the sender receives the NAK for the damaged frame, it retransmits all the frames onwards the frame number referred by NAK.

Lost Frame : The receiver checks the number on each frame, it receives. If a frame number is skipped in a sequence, then the receiver easily detects the loss of a frame as the newly received frame is received out of sequence. The receiver sends the NAK for the lost frame and then the receiver discards all the frames received after a lost frame.

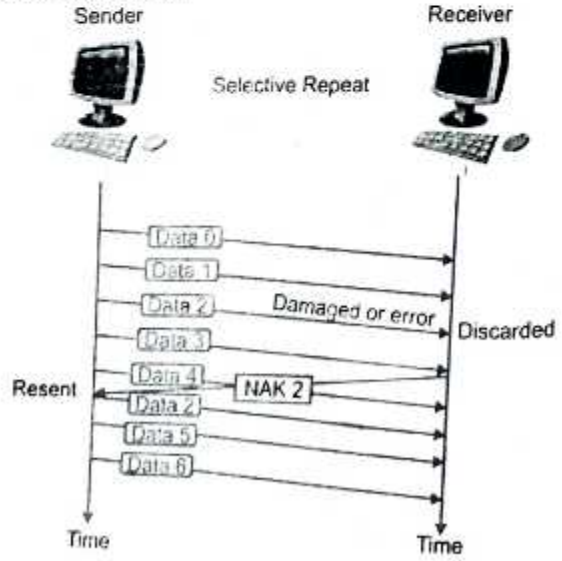
The receiver does not send any ACK (acknowledgement) for that discarded frames. After the sender receives the NAK for the lost frame, it retransmits the lost frame referred by NAK and also retransmits all the frames which it has sent after the lost frame.

Lost Acknowledgement : If the sender does not rece any ACK or if the ACK is lost or damaged in between transmission. The sender waits for the time to run out a as the time run-outs, the sender retransmits all the fra for which it has not received the ACK. The send identifies the loss of ACK with the help of a timer.

The ACK number, like NAK (negati acknowledgement) number, shows the number of frame, that receiver expects to be the next in sequence. T window size of the receiver is 1 as the data link layer on requires the frame which it has to send next to the netwo layer. The sender window size is equal to 'w'. If the err rate is high, a lot of bandwidth is lost wasted.

Definition of Selective Repeat

Selective repeat is also the sliding window protoc which detects or corrects the error occurred in the datali layer. The selective repeat protocol retransmits only th frame which is damaged or lost. In selective repe protocol, the retransmitted framed is received out sequence. The selective repeat protocol can perform t following actions :



(Figure)

(1) The receiver is capable of sorting the frame in proper sequence, as it receives the retransmitt

frame whose sequence is out of order of the receiving frame.

(2) The sender must be capable of searching the frame for which the NAK has been received.

(3) The receiver must contain the buffer to store all the previously received frame on hold till the retransmitted frame is sorted and placed in a proper sequence.

(4) The ACK number, like NAK number, refers to the frame which is lost or damaged.

(5) It requires the less window size as compared to go-back-n protocol.

Damaged Frames : If a receiver receives a damaged frame, it sends the NAK for the frame in which error or damage is detected. The NAK number, like in go-back-n also indicates the acknowledgement of the previously received frames and error in the current frame.

The receiver keeps receiving the new frames while waiting for the damaged frame to be replaced. The frames that are received after the damaged frame are not be acknowledged until the damaged frame has been replaced.

Lost Frame : As in a selective repeat protocol, a frame can be received out of order and further they are sorted to maintain a proper sequence of the frames. While sorting, if a frame number is skipped, the receiver recognizes that a frame is lost and it sends NAK for that frame to the sender.

After receiving NAK for the lost frame the sender searches that frame in its window and retransmits that frame. If the last transmitted frame is lost then the receiver does not respond and this silence is a negative acknowledgement for the sender.

Lost Acknowledgement : If the sender does not receive any ACK or the ACK is lost or damaged in between the transmission. The sender waits for the time to run out and as the time run-outs, the sender retransmits all the frames for which it has not received the ACK. The sender identifies the loss of ACK with the help of a timer.

Key Differences Between Go-Back-N and Selective Repeat

(1) Go-Back-N protocol is design to retransmit all the frames that are arrived after the damaged or a lost

frame. On the other hand, Selective Repeat prot retransmits only that frame that is damaged or lost.

(2) If the error rate is high i.e. more frames are bei damaged and then retransmitting all the frames th arrived after a damaged frame waste the lots bandwidth. On the other hand, selective repe protocol re-transmits only damaged frame hen minimum bandwidth is wasted.

(3) All the frames after the damaged frame are discard and the retransmitted frames arrive in a sequen from a damaged frame onwards, so, there is le headache of sorting the frames hence it is le complex. On the other hand, only damaged suspected frame is retransmitted so, extra logic h to be applied for sorting hence, it is more complicate

(4) Go-Back-N has a window size of N-1 and selecti repeat have a window size <= (N+1)/2.

(5) Neither sender nor receiver needs the sorti algorithm in Go-Back-N whereas, the receiver m be able to sort them as it has to maintain t sequence.

(6) In Go-Back-N receiver discards all the frames aft the damaged frame hence, it doesn't need to store an frames. Selective repeat protocol does not discard th frames arrived after the damaged frame instead stores those frames till the damaged frame arriv successfully and is sorted in a proper sequence.

(7) In selective repeat, NAK frame refers to the damag frame number and in Go-Back-N, NAK frame refe to the next frame expected.

(8) Generally, the Go-Back-N is more in use due to i less complex nature instead of Selective Repe protocol.

Conclusion : The selective repeat is a more efficie protocol as it does not waste bandwidth for the fram which are properly received but, its complexity a expense favours the use of the go-back-n protocol.

13. ◆ ***Write short note on the Sliding window.***
◆ ***Define all protocols in Data link. Control fo two channels with proper categorizatio Explain each of them also.***

The purpose of the data link layer is to transfer blocks of data without error between two adjacent devices. Adjacent devices are physically connected by a communication channel such as telephone lines, coaxial cables, optical fibers, or satellites. The implication of such a physical link is that the data bits are delivered in exactly the same order in which they are sent. The physical link has no inherent storage capacity; therefore the delay involved is the propagation delay over the link.

Transmission of data over the link would be very simple indeed if no error ever occurred. Unfortunately, this is not so in a real physical link for a number of reasons : Natural phenomena such as noises and interference are introduced into the link causing errors in detecting the data. There is a propagation delay in the link. There is a finite data processing time required by the transmitting and receiving stations. A data link protocol thus has to be designed to ensure an error-free transmission and also to achieve an efficiency of the data transfer as high as possible.

A Simplex Stop-and-Wait Protocol : In this protocol we assume that data are transmitted in one direction only no errors occur (perfect channel).

The receiver can only process the received information at a finite rate. These assumptions imply that the transmitter cannot send frames at a rate faster than the receiver can process them. The problem here is how to prevent the sender from flooding the receiver. A general solution to this problem is to have the receiver provide some sort of feedback to the sender. The process could be as follows : The receiver send an acknowledge frame back to the sender telling the sender that the last received frame has been processed and passed to the host; permission to send the next frame is granted. The sender, after having sent a frame, must wait for the acknowledge frame from the receiver before sending another frame. This protocol is known as stop-and-wait.

The protocol is as follows :

```
/* protocol 2 */
Sender() {
forever
    {
from_host(buffer);
```

```
            S.info = buffer;
        sendf(S);
        wait(event);
            }}
        Receiver()
        {
        forever
            {
        wait(event);
        getf(R);
        to_host(R.info);
        sendf(S);     }}
```

A Simplex Protocol for a Noisy Channel : In this protocol the unreal "error free" assumption in protocol 2 is dropped. Frames may be either damaged or lost completely. We assume that transmission errors in the frame are detected by the hardware checksum.

One suggestion is that the sender would send a frame, the receiver would send an ACK frame only if the frame is received correctly. If the frame is in error the receiver simply ignores it; the transmitter would time out and would retransmit it. One fatal flaw with the above scheme is that if the ACK frame is lost or damaged, duplicate frames are accepted at the receiver without the receiver knowing it. Imagine a situation where the receiver has just sent an ACK frame back to the sender saying that it correctly received and already passed a frame to its host. However, the ACK frame gets lost completely, the sender times out and retransmits the frame. There is no way for the receiver to tell whether this frame is a retransmitted frame or a new frame, so the receiver accepts this duplicate happily and transfers it to the host. The protocol thus fails in this aspect. To overcome this problem it is required that the receiver be able to distinguish a frame that it is seeing for the first time from a retransmission. One way to achieve this is to have the sender put a sequence number in the header of each frame it sends. The receiver then can check the sequence number of each arriving frame to see if it is a new frame or a duplicate to be discarded.

The receiver needs to distinguish only 2 possibilities : a new frame or a duplicate; a 1-bit sequence number is sufficient. At any instant the receiver expects a particular sequence number. Any wrong sequence numbered frame arriving at the receiver is rejected as a duplicate.

correctly numbered frame arriving at the receiver is accepted, passed to the host, and the expected sequence number is incremented by 1 (modulo 2).

The protocol is depicted below :

```
/* protocol 3 */
Sender()
{
    NFTS = 0;              /* NFTS = Next Frame To Send */
from_host(buffer);
forever
    {
S.seq = NFTS;
        S.info = buffer;
sendf(S);
start_timer(S.seq);
wait(event);
if(event == frame_arrival)
        {
from_host(buffer);
            ++NFTS;  /* modulo 2 operation */
        } }}
Receiver()
{
    FE = 0;                /* FE = Frame Expected */
forever
    {
wait(event);
if(event == frame_arrival)
        {
getf(R);
if(R.seq == FE)
            {
to_host(R.info);
                ++FE;  /* modulo 2 operation */
            }
sendf(S);     /* ACK */
        } }}
```

This protocol can handle lost frames by timing out. The timeout interval has to be long enough to prevent premature timeouts which could cause a "deadlock" situation.

Sliding Window Protocols

Piggybacking Technique : In most practical situations there is a need for transmitting data in both directions (i.e. between 2 computers). A full duplex circuit is required for the operation. If protocol 2 or 3 is used in these

situations the data frames and ACK (control) frames in the reverse direction have to be interleaved. This method is acceptable but not efficient. An efficient method is to absorb the ACK frame into the header of the data frame going in the same direction. This technique is known as piggybacking. When a data frame arrives at an IMP (receiver or station), instead of immediately sending a separate ACK frame, the IMP restrains itself and waits until the host passes it the next message. The acknowledgement is then attached to the outgoing data frame using the ACK field in the frame header. In effect, the acknowledgement gets a free ride in the next outgoing data frame. This technique makes better use of the channel bandwidth. The ACK field costs only a few bits, whereas a separate frame would need a header, the acknowledgement, and a checksum. An issue arising here is the time period that the IMP waits for a message onto which to piggyback the ACK. Obviously the IMP cannot wait forever and there is no way to tell exactly when the next message is available. For these reasons the waiting period is usually a fixed period. If a new host packet arrives quickly the acknowledgement is piggybacked onto it; otherwise, the IMP just sends a separate ACK frame.

Sliding Window : When one host sends traffic to another it is desirable that the traffic should arrive in the same sequence as that in which it is dispatched. It is also desirable that a data link should deliver frames in the order sent. A flexible concept of sequencing is referred to as the sliding window concept and the next three protocols are all sliding window protocols. In all sliding window protocols, each outgoing frame contains a sequence number SN ranging from 0 to $2^{(n-1)}$ (where n is the number of bits reserved for the sequence number field). At any instant of time the sender maintains a list of consecutive sequence numbers corresponding to frames it is permitted to send. These frames are said to fall within the sending window. Similarly, the receiver maintains a receiving window corresponding to frames it is permitted to accept. The size of the window relates to the available buffers of a receiving or sending node at which frames may be arranged into sequence. At the receiving node, any frame falling outside the window is discarded. Frames falling within the

receiving window are accepted and arranged into sequence. Once sequenced, the frames at the left of the window are delivered to the host and an acknowledgement of the delivered frames is transmitted to their sender. The window is then rotated to the position where the left edge corresponds to the next expected frame, RN. Whenever a new frame arrives from the host, it is given the next highest sequence number, and the upper edge of the sending window is advanced by one. The sequence numbers within the sender's window represent frames sent but as yet not acknowledged. When an acknowledgement comes in, it gives the position of the receiving left window edge which indicates what frame the receiver expects to receive next. The sender then rotates its window to this position, thus making buffers available for continuous transmission.

A One Bit Sliding Window Protocol : Protocol 4 : The sliding window protocol with a maximum window size 1 uses stop-and-wait since the sender transmits a frame and waits for its acknowledgement before sending the next one.

```
/* protocol 4 */
Send_and_receive()
{
      NFTS = 0;
      FE = 0;
from_host(buffer);
      S.info = buffer;
S.seq = NFTS;
S.ack = 1-FE;
sendf(S);
start_timer(S.seq);
forever
      {
wait(event);
if(event == frame_arrival)
         (
getf(R);
if(R.seq == FE)
               (
to_host(R.info);      ++FE;
               }
if(R.ack == NFTS)
               (
```

```
        from_host(buffer);
                        ++NFTS;
                    }
                }
                S.info = buffer;
        S.seq = NFTS;
        S.ack = 1-FE;
        sendf(S);
        start_timer(S.seq);
            }}
```

14. ◆ ***Write about CSMA/CD protocol.*** **(2017-18)**
◆ ***Compare and contrast CSMA/CD with CSMA/CA.*** **(2014-15)**

CSMA CA vs CSMA CD

Carrier Sense Multiple Access or CSMA is a Medi Access Control (MAC) protocol that is used to control th flow of data in a transmission media so that packets do no get lost and data integrity is maintained. There are tw modifications to CSMA, the CSMA CD (Collision Detection and CSMA CA (Collision Avoidance), each having its own strengths.

CSMA operates by sensing the state of the medium in order to prevent or recover from a collision. A collision happens when two transmitters transmit at the same time. The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it.

CSMA CD operates by detecting the occurrence of a collision. Once a collision is detected, CSMA CD immediately terminates the transmission so that the transmitter does not have to waste a lot of time in continuing. The last information can be retransmitted. In comparison, CSMA CA does not deal with the recovery after a collision. What it does is to check whether the medium is in use. If it is busy, then the transmitter waits until it is idle before it starts transmitting. This effectively minimizes the possibility of collisions and makes more efficient use of the medium.

Another difference between CSMA CD and CSMA CA is where they are typically used. CSMA CD is used mostly

in wired installations because it is possible to detect whether a collision has occurred. With wireless installations, it is not possible for the transmitter to detect whether a collicion has occurred or not. That is why wireless installations often use CSMA CA instead of CSMA CD.

Most people do not really have to deal with access control protocols as they work behind the scenes in order for our devices to work together. CSMA CD has also fallen out of favor with modern wired networks as they were only necessary with hubs and not with modern switches that route the information instead of broadcasting it.

Summary :

(1) CSMA CD takes effect after a collision while CSMA CA takes effect before a collision.

(2) CSMA CA reduces the possibility of a collision while CSMA CD only minimizes the recovery time.

(3) CSMA CD is typically used in wired networks while CSMA CA is used in wireless networks.

15. ***Which of the following CRC generators guarantee the detection of a single bit error?*** **(2014-15)**

(1) $x + 1$

(2) $x^2 + 1$

Cyclic Redundancy Check (CRC) an error detection mechanism in which a special number is appended to a block of data in order to detect any changes introduced during storage (or transmission). The CRC is recalculated on retrieval (or reception) and compared to the value originally transmitted, which can reveal certain types of error. For example, a single corrupted bit in the data results in a one-bit change in the calculated CRC, but multiple corrupt bits may cancel each other out.

A CRC is derived using a more complex algorithm than the simple CHECKSUM involving MODULO ARITHMETIC (hence the 'cyclic' name) and treating each input word as a set of coefficients for a polynomial.

(1) CRC is more powerful than VRC and LRC in detecting errors.

(2) It is not based on binary addition like VRC and LRC. Rather it is based on binary division.

(3) At the sender side, the data unit to be transmitte divided by a predetermined divisor (binary num in order to obtain the remainder. This remainde called CRC.

(4) The CRC has one bit less than the divisor. It m that if CRC is of n bits, divisor is of $n + 1$ bit.

(5) The sender appends this CRC to the end of data such that the resulting data unit becomes ex divisible by predetermined divisor i.e. remai becomes zero.

(6) At the destination, the incoming data unit i.e. da CRC is divided by the same number (predetermi binary divisor).

(7) If the remainder after division is zero then there is error in the data unit & receiver accepts it.

(8) If remainder after division is not zero, it indica that the data unit has been damaged in transit a therefore it is rejected.

(9) This technique is more powerful than the pa check and checksum error detection.

(10) CRC is based on binary division. A sequen of redundant bits called CRC or CRC remainder appended at the end of a data unit such as byte.

Single Bit Error

It means only one bit of data unit is changed fro to 0 or from 0 to 1. Single bit error can happen in para transmission where all the data bits are transmitted us separate wires. Single bit errors are the least likely type error in serial transmission.

A single-bit error is $e(x) = x_i$, where i is the position the bit. If a single-bit error is caught, then x_i is divisible by $g(x)$. (Note that when we say not divisible, mean that there is a remainder.) If $g(x)$ has at least terms (which is normally the case) and the coefficient o is not zero (the rightmost bit is 1), then $e(x)$ cannot divided by $g(x)$. If the generator has more than o term and the coefficient of x_0 is 1, all single errors can caught.

(1) $x + 1$: No x_i can be divisible by $x + 1$. In other word $x_i/(e(x) + 1)$ always has a remainder. So the syndro is nonzero. Any single-bit error can be caught.

(2) $x^2 + 1$: To detect single bit errors, a CRC generator must have at least two terms and the coefficient of x_0 must be nonzero. It meets both criteria. Hence guarantee the detection of a single bit error

16. *Generate the CRC code for the data word of 1100 10101. The divisor is 10101.* (2013-14)

Generation of CRC Code

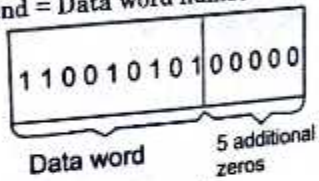
Given : Data word : 11001010₁

Divisor : 10101

The number of data bits = $m = 9$

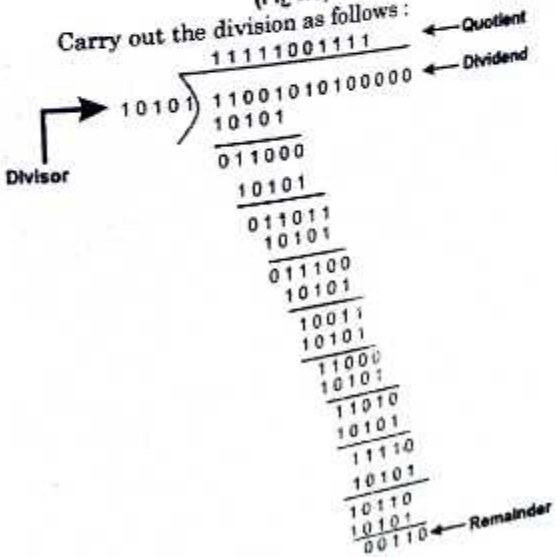
The number of bits in the codeword = N

Dividend = Data word number of zeros.



(Figure)

Carry out the division as follows :



(Figure)

17. *Compare two data link layer protocols : Go Back N and Selective repeat in terms of flow control, error recovery and packet loss.* (2013-14)

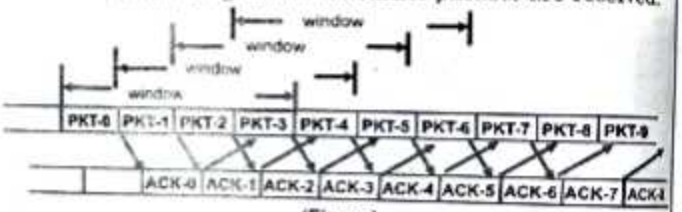
Go Back N ARQ (Sliding Window)

(1) Stop and Wait is inefficient when propagation delay is larger than the packet transmission time.

Can only send one packet per round-trip time.

(2) Go Back N allows the transmission of new packets before earlier ones are acknowledged.

(3) Go back N uses a window mechanism where the sender can send packets that are within a "window" (range) of packets. The window advances as acknowledgements for earlier packets are received.



(Figure)

Selective Repeat :

(1) In Selective Repeat the receiver accepts out of sequence I-frames

(2) Retransmission of out of sequence I-frames is requested by means of Selective Reject (SREJ) S-frames

The sender only retransmits the I-frame indicated by the N(r) field carried on each SREJ, thus reducing the number of retransmissions

(3) The receiver only acknowledges blocks of consecutive I- frames (as in Go-Back-N) and thus it has to wait for missing frames and fill the corresponding gaps before acknowledging the I-frames that had been received out of sequence and stored.

(4) This method is more complex than Go-Back-N but is advantageous in links with a high Delay • Bandwidth product (e.g., satellite links), for which large window sizes are recommended, or in links with high Bit Error Ratio (BER), even if small window sizes are acceptable.

(5) To allow the receiver to distinguish new out of sequence I-frames from duplicates originated by the retransmission of I-frames already acknowledged, the maximum sender window size has to be reduced to $W_{max} = M / 2 = 2^{k-1}$ (and the maximum receiver window size has the same value)

18. *If a bit string 01111110111111011111110 is subjected to bit stuffing, what would be the output string?* (2013-14)

If a bit string 01111110111111011111110 is subjected to bit stuffing, The output string is 01111101011111011111010.

19. *Differentiate between Token ring and Token bus LAN standards. Consider building a CSMA/CD network running at 1Gbps over a 1-km cable with no repeaters. The signal speed in the cable is 2,00,000 km/sec. What is the minimum frame size?* (2010-11)

Token Ring

(1) When a station wishes to transmit, it must wait for token to pass by and seize the token.

(2) **One Approach** : change one bit in token which transforms it into a "start-of-frame sequence" and appends frame for transmission.

(3) **Second Approach** : station claims token by removing it from the ring.

(4) Frame circles the ring and is removed by the transmitting station.

Each station interrogates passing frame, if destined for station, it copies the frame into local buffer.

Token Ring : Local area network (LAN) technology is a local area network protocol which resides at the data link layer (DLL) of the OSI model. It uses a special three-byte frame called a token that travels around the ring. Token-possession grants the possessor permission to transmit on the medium. Token ring frames travel completely around the loop.

Initially used only in IBM computers, it was eventually standardized with protocol IEEE 802.5.

Token Bus : Token bus is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable. A token is passed around the network nodes and only the node possessing the token may transmit. If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring. Each node must know the address of its neighbor in the ring, so a special protocol is needed to notify the other nodes of connections to, and disconnections from, the ring.

Token bus was standardized by IEEE standard 802.4. It is mainly used for industrial applications. Token bus was used by GM (General Motors) for their Manufacturing Automation Protocol (MAP) standardization effort. This is an application of the concepts used in token ring networks. The main difference is that the endpoints of the bus do not meet to form a physical ring. The IEEE 802.4 Working Group is disbanded. In order to guarantee the packet delay and transmission in Token bus protocol, a modified Token bus was proposed in Manufacturing Automation Systems and flexible manufacturing system.

Numerical Solution : Given

Bandwidth = I *Gbps*,

Distance = 1 *Km*.

Signal Speed = 200000 *km/sec*

Tp = Distance / Propagation Speed

= 1*km*/200000 *km/sec* = 5 × 10-6 *sec*.

$T_{fr} = 2 \times Tp = 2 \times 5 \times 10^{-6}$ *sec*. $= 10^{-5}$*sec*.

Therefore minimum Frame Size = Bandwidth × T_{fr}

$= 10^9 \times 10^{-5}$ *sec*. $= 10^4$ *bits* **(Ans.)**

20. *What are Medium Access Control (MAC) protocols? Discuss salient features of CSMA/CD protocol.*

Medium Access Control Protocols

(1) The protocols used to determine who goes next on a multi-access channel belong to a sub-layer of the data link layer called the MAC (Medium Access Control) sub layer.

(2) Multiple access control protocol is used in the MAC sub layer.

Different Protocols of MAC Sub-Layers :

ALOHA : The basic idea of ALOHA is that, it is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.

Pure ALOHA :

(a) If listening while transmission is not possible for some reason, acknowledgement is needed.

(b) If frames are destroyed the sender just waits random amount of time and sends it again.

Throughput :

$$S = be^{-2b}$$

Maximum throughput occurs at $b = 0.5$

$$S = 1/2e$$

$$S = 0.184$$

Slotted ALOHA : In it time is divided into discrete intervals each interval corresponding to one frame, have one special station emits a pipe at the S, each interval, like a clock.

Throughput :

$$S = be^{-b}$$

Maximum throughput :

$$S = 0.368$$

Carrier Sense Multiple Access Protocols : Protocols in which stations listen for a carrier and act accordingly are called carrier sense protocols.

Persistent :

(1) When a station has data to send, if first listens to the channel to see if anyone else is transmitting at that moment.

(2) If the channel is busy, the station waits until it becomes idle. It waits for random amount of time.

Non Persistent CSMA :

(a) The station does not continuously sense it.

(b) It waits for a random period of time and then repeated algorithms.

Persistent :

(a) When a station becomes ready to send, it senses the channel.

(b) If it is idle, it transmits with a probability P.

CSMA with Collision Detection (CSMA/CD) :

(a) If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.

(b) Rather than finish transmitting their frames, as soon as the collision is detected they will quickly terminate transmitting.

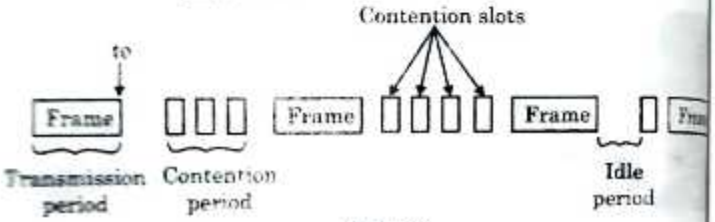
(c) Quickly terminating damaged frames saves time and bandwidth.

CSMA/CD can be in one of three States :

(i) Contention

(ii) Transmission

(iii) Idle



(Figure)

21. *Consider a CSMA/CD network running at 200 Mbps over a 1 km cable with no repeater. The signal speed is 2×10^8 m/sec. Compute the minimum frame size.*

Signal speed $= 2 \times 10^8$ *m/sec.*

For 1 km the propagation time $\tau = 5\,\mu$sec.

In 10^6 *μsec* network runs 200 *mb*

$= 200 \times 1024 \times 1024$ *bit*

$\tau = 5\,\mu$sec network runs $= \dfrac{200 \times 1024 \times 1024}{10^6} \times 5$

$= 1048\,576$ *bits*

NETWORK LAYER

1. ◆ ***What is switching? Briefly explain different Methods of Switching.*** (2017-18)
   ◆ ***Differentiate among circuit switching, packet switching and message switching.*** (2010-11)
   ◆ ***List all the routing schemes with their important features.***

Switching

Switching algorithms is relatively simple; it is the same for most routing protocols. In most cases, a host determines that it must send a packet to another host. Having acquired a router's address by some means, the source host sends a packet addressed specifically to a router's physical (Media Access Control [MAC]-layer) address, this time with the protocol (network layer) address of the destination host. As it examines the packet's destination protocol address, the router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it typically drops the packet. If the router knows how to forward the packet, however, it changes the destination physical address to that of the next hop and transmits the packet. The next hop may be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. As the packet moves through the internetwork, its physical address changes, but its protocol address remains constant. The preceding discussion describes switching between a source and a destination end system.

Different Method of Switching

Circuit Switching :

(1) Circuit switching was designed in 1878 in order to send telephone calls down a dedicated channel. This channel remained open and in use throughout the whole call and could not be used by any other data or phone calls.

(2) There are three phases in circuit switching :

(a) Establish
(b) Transfer
(c) Disconnect

(3) The telephone message is sent in one go, it is not broken up. The message arrives in the same order that it was originally sent.

(4) In modern circuit-switched networks, electronic signals pass through several switches before a connection is established.

(5) During a call, no other network traffic can use those switches.

(6) The resources remain dedicated to the circuit during the entire data transfer and the entire message follows the same path.

(7) Circuit switching can be analogue or digital.

(8) With the expanded use of the Internet for voice and video, analysts predict a gradual shift away from circuit-switched networks.

(9) A circuit-switched network is excellent for data that needs a constant link from end-to-end. For example real-time video.

(10) Security

(11) Bandwidth used to full potential

(12) Devices of different speeds can communicate

Packet Switching :

(1) In packet-based networks, the message gets broken into small data packets. These packets are sent out from the computer and they travel around the network seeking out the most efficient route to travel as circuits become available. This does not necessarily mean that they seek out the shortest route.

(2) Each packet may go a different route from the others.

(3) Each packet is sent with a 'header address'. This tells it where its final destination is, so it knows where to go.

(4) The header address also describes the sequence for reassembly at the destination computer so that the packets are put back into the correct order.

(5) One packet also contains details of how many packets should be arriving so that the recipient computer knows if one packet has failed to turn up.

(6) If a packet fails to arrive, the recipient computer sends a message back to the computer which originally sent the data, asking for the missing packet to be resent.

(7) Message is broken up into segments (packets).

(8) Each packet carries the identification of the intended recipient, data used to assist in data correction and the position of the packet in the sequence.

Message Switching :

(1) In telecommunications, message switching was the precursor of packet switching, where messages were routed in their entirety and one hop at a time. It was first introduced by Leonard Kleinrock in 1961. Message switching systems are now a day's mostly implemented over packet-switched or circuit-switched data network. Each message is treated as a separate entity.

(2) Each message contains addressing information, and at each switch this information is read and the transfer path to the next switch is decided. Depending on network conditions, a conversation of several messages may not be transferred over the same path. Each message is stored (usually on hard drive due to RAM limitations) before being transmitted to the next switch. Because of this it is also known as a 'store-and-forward' network. Email is a common application for Message Switching. A delay in delivering email is allowed unlike real time data transfer between two computers.

(3) Data channels are shared among communication devices improving the use of bandwidth.

(4) Messages can be stored temporarily at message switches, when network congestion becomes a problem.

(5) Priorities may be used to manage network traffic.

(6) Broadcast addressing uses bandwidth more efficiently because messages are delivered to multiple destinations.

Routing Basics : Here we introduce the underlying concepts widely used in routing protocols. Topics summarized here include routing protocol components and algorithms. In addition, the role of routing protocols is

briefly contrasted with the role of routed or network protocols.

Routing : Routing is the act of moving information across an internet work from a source to a destination. Along the way, at least one intermediate node typically is encountered. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways.

Routing Components : Routing involves two basic activities: Determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. In the context of the routing process, the latter of these is referred to as packet switching. Although packet switching is relatively straightforward, path determination can be very complex.

Path Determination : Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth, that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Destination/next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the "next hop" on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop. Routing tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes and these metrics differ

depending on the design of the routing algorithm used. Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table.

2. ◆ ***What is IP addressing? How would you design class A, Class B and Class C of IP addresses?*** **(2018-19)**

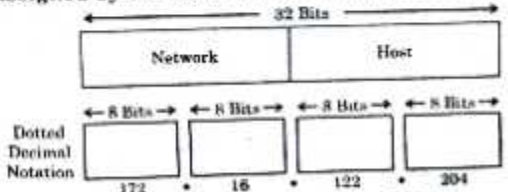
◆ ***Briefly explain about IP Addressing. Differentiate between classfull addressing and classless addressing.*** **(2017-18)**

◆ ***Give a classification of different IP addresses. Explain the concept of subnetting.*** **(2013-14)**

IP Addressing

As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a basic format.

Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts: The network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator.



(Figure : An IP Address Consists of 32 bits, Grouped into Four Octets)

IP Address Format : The 32-bit IP address is grouped eight bits at a time, separated by dots and represented in

decimal format (known as dotted decimal notation). Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1). The minimum value for an octet is 0 and the maximum value for an octet is 255.

IP Address Classes : IP addressing supports five different address classes: *A, B,C, D* and *E*. Only classes *A, B* and *C* are available for commercial use. The left-most (high-order) bits indicate the network class and provides reference information about the five IP address classes.

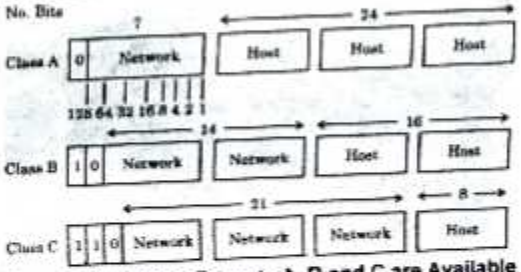
Table 1 : Reference Information about the Five IP Address Classes :

Purpose	High Order Bit(s)	Address Range	No. Bits Network / Host	Max. Hosts
Few Large Organizations	0	1.0.0.0 to 126.0.0.0	7/24	16,777,214 (2^{24}-2)
Medium-size organization	1, 0	128.1.0.0 to 191.254.0.0	14/16	65,543 (2^{16}-2)
Relatively small organizations	1, 1, 0	192.0.1.0 to 223.255.254.0	22/8	245 (2^{8}-2)
Multicast groups (RFC 1112)	1, 1, 1, 0	224.0.0.0 to 239.255.255.255	N/A (not for commerc	N/A
Experimental	1, 1, 1, 1	240.0.0.0 to 254.255.255.255	N/A	N/A

IP Address Classes	Format
A	N.H.H.H
B	N.N.H.H
C	N.N.N.H
D	N/A
E	N/A

N = Network number, H = Host number.

One address is reserved for the broadcast address and one address is reserved for the network.



(Figure : IP Address Formats A, B and C are Available for Commercial Use)

The class of address can be determined easily by examining the first octet of the address and mapping that value to a class range in the following table. In IP address of 172.31.1.2, for example, the first octet is 172. Because 172 fall between 128 and 191, 172.31.1.2 is a Class B address. Summarizes the range of possible values for the first octet of each address class :

Address Class	First Octet in Decimal	High Order Bits
Class A	1 D 126	0
Class B	128 D 191	10
Class C	192 D 223	110
Class D	224 D 239	1110
Class E	240 D 254	1111

(Figure : A Range of Possible Values Exists for the First Octet of Each Address Class)

IP Subnet Addressing : IP networks can be divided into smaller networks called sub-networks (or subnets). Sub

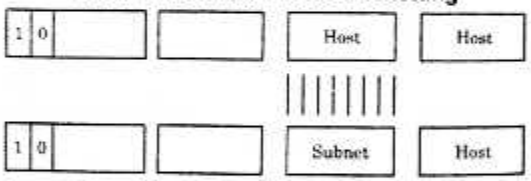
netting provides the network administrator with several benefits, including extra flexibility, more efficient use of network addresses and the capability to contain broadcast traffic.

Subnets are under local administration. As such, the outside world sees an organization as a single network and has no detailed knowledge of the organization's internal structure.

A given network address can be broken up into many sub networks. For example, 172.16.1.0, 172.16.2.0, 172.16.3.0 and 172.16.4.0 are all subnets within network 171.16.0.0.

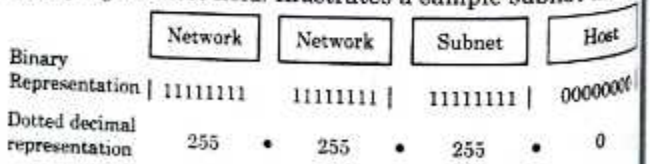
IP Subnet Mask : A subnet address is created by "borrowing" bits from the host field and designating them as the subnet field. The number of borrowed bits varies and is specified by the subnet mask. Shows how bits are borrowed from the host address field to create the subnet address field. Figure given below : Bits are borrowed from the host address field to create the subnet address field.

Class B Address : Before Subnetting



(Class B Address : After Subnetting)

Subnet masks use the same format and representation technique as IP addresses. The subnet mask, however, has binary 1s in all bits specifying the network and subnetwork fields and binary 0s in all bits specifying the host field. Illustrates a sample subnet mask.



(Figure : A Sample Subnet Mask Consists of All Binary 1s and 0s)

Subnet mask bits should come from the high-order (left-most) bits of the host field, as illustrates. Details of Class B and C subnet mask types follow :

128 ↓	64 ↓	32 ↓	16 ↓	8 ↓	4 ↓	2 ↓	1 ↓		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

(Figure : Subnet Mask Bits Come from the High-Order Bits of the Host Field)

Various types of subnet masks exist for Class B and C subnets :

The default subnet mask for a Class B address that has no subnetting is 255.255.0.0, while the subnet mask for a Class B address 171.16.0.0 that specifies eight bits of subnetting is 255.255.255.0. The reason for this is that eight bits of subnetting or $2^8 - 2$ (1 for the network address and 1 for the broadcast address) = 254 subnets possible, with $2^8 - 2 = 254$ hosts per subnet. The subnet mask for a Class C address 192.168.2.0 that specifies five bits of subnetting is 255.255.255.248 With five bits available for subnetting, $2^5 - 2 = 30$ subnets possible, with $2^3 - 2 = 6$ hosts per subnet.

Table - 2

Number of Bits	Subnet Mask	Number of Subnets	Number of Hosts
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30

12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

Chart

Number of Bits	Subnet Mask	Number of Subnets	Number of Hosts
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Table 3 : **Class C Subnetting Reference Chart**

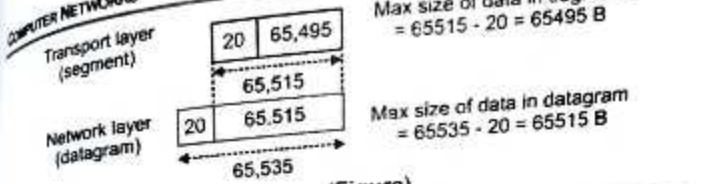
Difference Between Classfull Addressing and Classless Addressing :

As Applied To	Classfull Addressing	Classless Addressing
Addresses	Addresses have three parts : Network, subnet, and host.	Addresses have two parts . subnet or prefix and host.
Routing protocols	Routing protocol does not advertise masks nor support VLSM; RIP-1 and IGRP.	Routing protocol does advertise masks and support VLSM; RIP-2, EIGRP, OSPF.
Routing (forwarding)	IP forwarding process is restricted in how it uses the default route.	IP forwarding process has no restrictions on using the default route.

3. *Define Fragmentation.* **(2018-19)**

Fragmentation is phenomenon in which storage space is used inefficiently reducing capacity or performance and often both. The exact consequences of fragmentation depend on the specific system of storage allocation in use and the particular form of fragmentation. Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held a frame i.e., its Maximum Transmission Unit (MTU). The network layer divides the datagram received from transport layer into fragments so that data flow is not disrupted.

Since there are 16 bits for total length in IP header so, maximum size of IP datagram = $2^{16} - 1 = 65,535$ bytes.



(Figure)

4. *What problems of IPv4 are being addressed by IPv6?* **(2017-18)**

Problem of IPv4 are Beings Addressed by IPv6

(1) IPv4 has not enough addresses. In theory there are 232 total, but allocation isn't very sufficient. There are probably 108 (a factor of 10 or so) internet hosts today and growing exponentially.

(2) IPv4 has not enough networks. Even with CIDR addressing, allocating (and then routing) to an ever increasing number of addresses is hard.

(3) IPv4 simplifies header contents (make router's job easier)

(4) IPv4 makes host configuration easier (No need for DHCP servers in most cases).

(5) IPv4 needs address security, mobility, multicast and other application.

(6) IPv4 headers and IPv6 headers do not interoperate. IPv6 is not a superset of functionality that is backward compatible with IPv4 is not possible.

(7) Multicast, the ability to send a single packet to multiple destinations, is part of the base specification in IPv6. This is unlike IPv4, where it is optional (but usually implemented). Multicasting is delivering a data stream to multiple destinations at the same time, with no duplication unless called for. Those functionalities are not supported by IPv4.

(8) IPv4 limits packets to 64 *KB* of payload. IPv6 has optional support for packets over this limit, referred to as jumbo grams, which can be as large as 4 *GB*.

5. *A classless address is given as 167.199.170.82/27. Find the* **(2017-18)**

(1) *The number of addresses in the network*

(2) *First address*

(3) *Last address*

A classless address is given as 167.199.170.82/27.

(1) **Number of Addresses** $n = 27$

Therefore number of addresses is $2(32 - n) = 32$

(2) **First Address :** The prefix length is 27, which means that we must keep the first 27 bits as is and change the remaining bits (5) to 0s. The following shows the process :

Address in Binary : 10100111, 11000111, 10101010, 01010010.

Keep the Left 27 Bits : 10100111, 11000111, 10101010, 01000000

Result in CIDR Notation : 167. 199. 170. 64/27.

(3) **Last Address** = (any address) OR [NOT (network mask)].

167.199.170.95

6. *What do you mean by logical address?*

Address generated by CPU while a program is running is referred as Logical Address. The logical address is virtual as it does not exist physically. Hence, it is also called as Virtual Address. This address is used as a reference to access the physical memory location. The set of all logical addresses generated by a programs perspective is called Logical Address Space.

The logical address is mapped to its corresponding physical address by a hardware device called Memory Management Unit. The address-binding methods used by MMU generate identical logical and physical addresses during compile time and load time. However, while run time the address-binding methods generate different logical and physical address.

7. *Write short note on Address Mapping.*

Address Mapping

An internet is made of a combination of physical networks connected by internetworking devices such as routers. A packet starting from a source host may pass through several different physical networks before finally reaching the destination host. The hosts and routers are recognized at the network level by their logical addresses. However, packets pass through physical networks to reach these hosts and routers. At the physical level, the hosts and routers are recognized by their physical addresses.

A physical address is a local address. Its jurisdiction is a local network. It must be unique locally, but is not necessarily unique universally. It is called a physical address because it is usually (but not always) implemented in hardware. An example of a physical address is the 48-bit MAC address in the Ethernet protocol, which is imprinted on the NIC installed in the host or router.

The physical address and the logical address are two different identifiers. We need both because a physical network such as Ethernet can have two different protocols at the network layer such as IP and IPX (Novell) at the same time. Likewise, a packet at a network layer such as IP may pass through different physical networks such as Ethernet and Local Talk (Apple).

This means that delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. These can be done by using either static or dynamic mapping.

Static mapping involves in the creation of a table that associates a logical address with a physical address. This table is stored in each machine on the network. Each machine that knows, for example, the IP address of another machine but not its physical address can look it up in the table. This has some limitations because physical addresses may change in the following ways :

(1) A machine could change its NIC, resulting in a new physical address.

(2) In some LANs, such as Local Talk, the physical address changes every time the computer is turned on. 3. A mobile computer can move from one physical network to another, resulting in a change in its physical address.

8. *Explain the main performance comparison between IPv4 and IPv6.* **(2013-14)**

Comparison

IPv4	IPv6
This is internet protocol version 4	This is internet protocol version 6
IPv4 has 32 bit Address.	IPv6 is uses 128 bit (16 bytes) addresses.
It cannot accommodate larger number of users	IPv6 accommodates a larger number of users.
The service type field is in IPv4.	The service type field is eliminated in IPv6.
The total length field is available in IPV4.	The total length field is eliminated in IPv6 and replaced by the payload length field.
The identification, flag and offset are available in IPv4 Header format.	The identification, flag offset fields are eliminated from the base header and they are included in the fragmentation extension header.
The TTL field is available in the IPv4 header	The TTL field is called Hop limit in IPv6.
The header check sum is available in the IPV4 Header.	The header check sum is eliminated because check sum is provided by upper layer protocol it is therefore not needed at this level.

9. *Write a short note on ARP.* (2013-14)

ARP : Address Resolution Protocol

ARP converts an Internet Protocol (IP) address to its corresponding physical network address. ARP is a low-level network protocol, operating at Layer 2 of the OSI model.

ARP usually is implemented in the device drivers of network operating systems. It is most commonly seen on Ethernet networks, but ARP has also been implemented for ATM, Token Ring, and other physical networks. RFC 826 documented the initial design and implementation of ARP.

ARP works on Ethernet networks as follows. Ethernet network adapters are produced with a physical address embedded in the hardware called the Media Access Control (MAC) address. Manufacturers take care to ensure these 6-byte (48-bit) addresses are unique and Ethernet relies on these unique identifiers for message delivery.

When any device wishes to send data to another target device over Ethernet, it must first determine the MAC address of that target given its IP address. These IP-to-MAC address mappings are derived from an ARP cache maintained on each device. If the given IP address does not appear in a device's cache, that device cannot direct messages to that target until it obtains a new mapping. To do this, the initiating device first sends an ARP request broadcast message on the local subnet. The host with the given IP address sends an ARP reply in response to the broadcast, allowing the initiating device to update its cache and proceed to deliver messages directly to the target.

10. *The IP address of a host on class C network is 198.123.46.237. Four networks are allowed for this network. What will be the subnet mask?* (2013-14)

The IP address of a host on a Class C network is 198.123.46.237. Four subnets are allowed for this network.

11111111.	11111111.	11111111.	11000000
255.	255.	255.	192

11. *Write a short note on ICMP.* (2013-14)

ICMP (Internet Control Message Protocol)

(1) ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or disoperation.

(2) Since ICMP uses IP, ICMP packet delivery is unreliable, so hosts cannot count on receiving ICMP packets for any network problem.

ICMP is a network protocol useful in Internet Protocol (IP) network management and administration. ICMP is a required element of IP implementations. ICMP is a control protocol, meaning that it does not carry application data, but rather information about the status of the network itself. ICMP can be used to report :

(a) Errors in the underlying communications of network applications

(b) Availability of remote hosts

(c) Network congestion

Perhaps the best known example of ICMP in practice is the ping.

Utility, that uses ICMP to probe remote hosts for responsiveness and overall round-trip time of the probe messages. ICMP also supports trace route, that can identify intermediate "hops" between a given source and destination.

12. *Draw and explain IPv 4 header format. A router has just received the following new IP address : 57.6.96.0/21,57.6.104.0/21,57.6.112.0/21 and 57.6.120.0/21. If all of them use the same outgoing line, can they be aggregated? If so, to what? If not, why not?* **(2010-11)**

IPv 4 Header Format

Internet protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. IPv4 is still by far the most widely deployed Internet Layer protocol (As of 2011, IPv6 deployment is still in its infancy).

IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (example, Ethernet). It operates on a best effort delivery model; in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

Addressing : IPv4 uses 32-bit (four-byte) addresses, which limits the address space to 4294967296 (2^{32}) addresses. However, some address blocks are reserved for special purposes such as private networks (~18 million addresses) and multicast addresses (~270 million addresses). This reduces the number of addresses that may be allocated for routing on the public Internet. As addresses are assigned to end users, an IPv4 address shortage has been developing.

Address Representations : IPv4 addresses may be written in any notation expressing a 32-bit integer value, but for human convenience, they are most often written in dot-decimal notation, which consists of four octets of the address expressed individually in decimal and separated by periods.

Solution : Yes, if all of them use the same outgoing line, they can aggregated to enhance the outgoing line to avoid losing the packets.

They can aggregate at IP address 57.6.96.0/19.

Version	H.length	TOS	Total length
Identification			Flags / Fragment offset
Time to Live	Protocol		Header checksum
32 - bit source address			
32 - bit destination address			
Option			

Total length : 20 bytes + options Modified Deleted

(Figure : IPv4 Header Format)

13. *Write short notes on RARP, BOOTP and DHCP.*

RARP

RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Bootstrap Protocol (BOOTP)

A TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a bootstrap protocol (BOOTP) server. The network interface card (NIC) on these diskless workstations contains a programmable read-only memory (PROM) chip containing code necessary to initialize the client.

Routers may not always have a consistent view of the network topology, because of the time updates take to reach all routers. This inconsistent view of the network can lead to the formation of loops, which are temporary and disappear in the time it takes for all routers to have the same topological information.

Shortest Path First (SPF) is a link state protocol in which each node computes and broadcast the cost of its outgoing links periodically and applies Dijkstra's shortest path algorithm to determine the next hop, other routing protocols that work on the same link state approach are IS-IS and OSPF.

Distance-Vector Algorithms : Routing Information Protocol (RIP)

RIP (Routing Information Protocol) is a standard for exchange of routing information among gateways and hosts. It is a distance-vector protocol. RIP is most useful as an "interior gateway protocol". The network is organized as a collection of "autonomous systems". Each autonomous system has its own routing technology, which may well be different for different autonomous systems. The routing protocol used within an autonomous system is referred to as an interior gateway protocol, or "IGP". Routing Information Protocol (RIP) is designed to work with moderate-size networks using reasonably homogeneous technology. Thus, it is suitable as an Interior Gateway Protocol (IGP) for many campuses and for regional networks using serial lines whose speeds do not vary widely. It is not intended for use in more complex environments. RIP2 derives from RIP, which is an extension of the Routing Information Protocol (RIP) intended to expand the amount of useful information carried in the RIP messages and to add a measure of security. RIP2 is an UDP-based protocol.

The Protocol Structure for RIP & and RIP2 is shown in the figure below :

8 bits	16 bits	32 bits
Command	Version	Unused
Address Family Identifier		Route Tag (only for RIP2, 0 for RIP)

TRANSPORT LAYER

1. ***Distinguish between TCP and UDP.*** (2018-19)

Difference between TCP and UDP

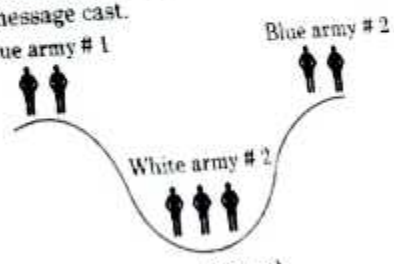
TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge sequencing	No acknowledgment

2. ◆ ***Describe in detail about the three way handshake protocol for connection establishment in TCP.*** (2018-19)
   ◆ ***What are two army problem and a three way handshake?***

Two Army Man Problem

A problem having two army units white army and blue army. Imagine that a white army is encamped in a valley. On both surrounding hillsides, blue army resides. The white army is larger than the individual blue army. But simultaneously blue army is larger in size.

How blue army wants to synchronize their attack. The only communication medium is to send messages on foot down into the valley, where they might be captured and the message cast.



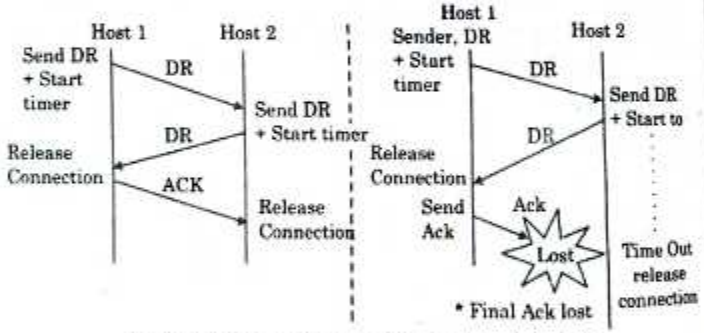
(Figure)

On, suppose commander of blue army #1 send message. 1 propose we attack, suppose messengers arrives the commander of blue army #2 agrees and his reply gets safely back to blue army one will attack happen? No because commander #2 (blue army) does not know if his reply got through.

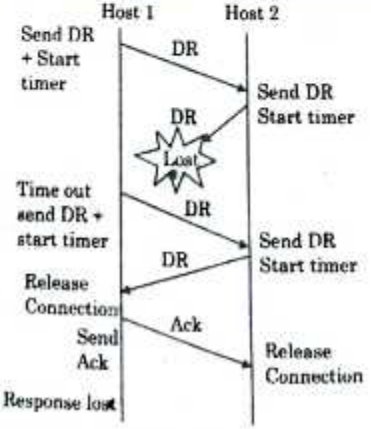
If did not blue army #1 will not attack. So, it will be foolish for him to attack. Here lack of acknowledgement results.

Three Way Hand-Shake

In normal case, user sends a DR (Disconnection request) TPDU to initiate the connection release. When it arrives the recipient sends back a DT TPDU, too and starts a timer just in case if DR is lost. When this DR arrives original sender sends back acknowledgement TPDU and release the connection. Finally when TPDU arrives, the receiver also releases the connection.



(Figure : Normal Case of 3-way Handshake)



(Figure)

3. ◆ ***How is congestion controlled? Explain in details the TCP congestion control.*** **(2018-19)**
   ◆ ***What is congestion? Define congestion control with a suitable example.*** **(2017-18)**
   ◆ ***What is the congestion in network layer? Differentiate and explain Leaky-Bucket algorithm and Token Bucket algorithm.***

Congestion in Network Layer

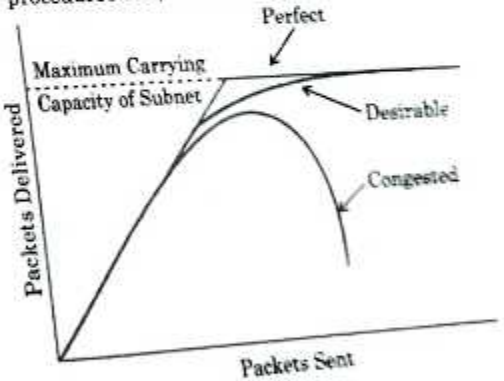
Network congestion characterized by presence of a large number of packets (load) being routed in all or portions of the subnet that exceeds its link and router capacities (resources) resulting in a performance slowdown.

Steps of Closed-loop Congestion Control :

(1) Congestion detection. Using system monitoring

(2) Transmit the information to parts of the network where corrective measures are possible.

(3) Adjust network operation parameters (routing procedures etc.) to correct the problem.



(Figure)

Congestion Detection can Utilize Two Techniques

(1) Notification from packet switches (routers)

(2) Infer congestion from packet loss.

(3) Sender can infer congestion from packet loss through missing acknowledgments.

(4) Rate or percentage of lost packets can be used to gauge degree of congestion.

Policies Affecting Network Congestion :

Layer	Policies
Transport	Re-transmission policy
	Out-of-order caching policy
	Acknowledgement policy
	Flow control policy
	Time out determination
Network	Virtual circuits versus datagram inside the subnet
	Packet queuing and service policy
	Packet discard policy
	Routing algorithm
	Packet lifetime management
Data Link	Re-transmission policy
	Out-of-order caching policy
	Acknowledgement policy
	Flow control policy

Difference between Leaky-Bucket and Token Bucket Algorithm

	Leaky-Bucket Algorithm	Token-Bucket Algorithm
Discard :	Packets	Tokens
		Packet management separate
Rate :	Fixed rate (perfect)	Average rate
		Burst allowed
Arriving Burst :	Waits in bucket	Can be sent immediately

The Leaky-Bucket Algorithm : This algorithm can be conceptually understood as follows :

(1) Consider a bucket with a hole in the bottom.

(2) If packets arrive, they are placed into the bucket. If the bucket is full, packets are discarded.

(3) Packets in the bucket are sent at a constant rate equivalent to the size of the hole in the bucket.

(4) The Leaky Bucket used to control rate in a network. It is implemented as a single-server queue with constant service time.

(5) If the bucket (buffer) overflows then packets are discarded.

(6) A traffic shaping method that aims at creating a uniform transmission rate at the hosts.

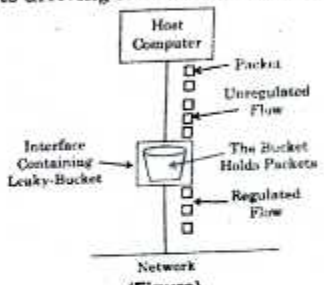
(7) Used in ATM networks.

(8) An output queue of finite length is connected between the sending host and the network.

(9) Either built into the network hardware interface or implemented by the operating system.

(10) One packet (for fixed-size packets) or a number of bytes (for variable-size packets) are allowed into the queue per clock cycle.

(11) Congestion control is accomplished by discarding packets arriving from the host when the queue is full.

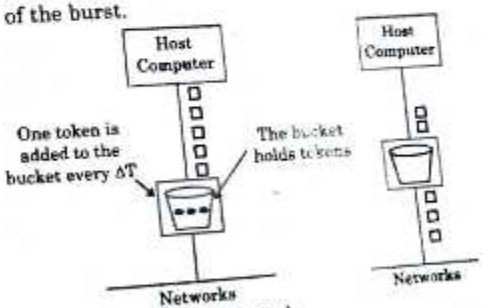


(Figure)

The Token-Bucket Algorithm : This algorithm can be conceptually understood as follows :

(1) The bucket holds tokens. To transmit a packet, we "use" one token.

(2) Allows the output rate to vary, depending on the size of the burst.



(Figure)

(3) An output queue is connected to the host where tokens are generated and a finite number is stored at the rate of DT.

(4) Packets from the host can be transmitted only if enough tokens exist.

(5) When the queue is full tokens are discarded not packets.

(6) Implemented using a variable that counts tokens.

Example of Congestion Control : Example of Congestion Control :

(1) **Choke Point :** A choke point is a packet sent by a router to the source to inform it of congestion. This type of control is similar to ICMP's source quench packet.

(2) **Back Pressure :** When a router is congested it can inform the previous upstream router to reduce the rate of outgoing packets. The action can be recursive all the way to the router before the source. This mechanism is called backpressure.

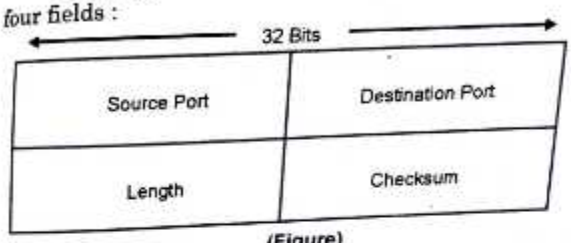
4. ◆ ***Explain UDP.*** **(2017-18)**
   ◆ ***Explain TCP.*** **(2017-18)**
   ◆ ***What do you mean by TCP and UDP? Explain some performance comparison of UDP and TCP.*** **(2013-14)**
   ◆ ***Describe Transmission control protocol and also describe TCP connection establishment.*** **(2008-09)**

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol (Layer 4) that belongs to the Internet protocol family. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another. Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control. UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol

(SNMP), Domain Name System (DNS) and Trivial File Transfer Protocol (TFTP). The UDP packet format contains four fields, as shown in. These include source and destination ports, length and checksum fields.

Figure given below shows A UDP packet consists of four fields :



(Figure)

Source and destination ports contain the 16-bit UDP protocol port numbers used to demultiplex data grams for receiving application-layer processes. A length field specifies the length of the UDP header and data. Checksum provides an (optional) integrity check on the UDP header and data.

(1) UDP support common communications session. It does not provide acknowledgement of transmitted data. UDP describe in RFC 768.

(2) UDP provides interface to the IP protocol with added feature of demultiplexing multiple processes using the ports.

(3) Useful in client server establishment and client send short request to the server expects a short reply back.

The main value of having UDP over just using raw IP is the addition of the source and destination port without the port field the transport layer would not know what to do with the packets, with them it send or delivers segments correctly.

Transmission Control Protocol (TCP)

The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation and multiplexing. With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service

benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery. TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission. TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers. Full-duplex operation means that TCP processes can both send and receive at the same time. Finally, TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

TCP Connection Establishment : To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a "three-way handshake" mechanism. A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well. This is necessary so that packets are not transmitted or retransmitted during session establishment or after session termination. Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the following manner :

The first host (Host *A*) initiates a connection by sending a packet with the initial sequence number (*X*) and SYN bit set to indicate a connection request. The second host (Host *B*) receives the SYN, records the sequence

number *X* and replies by acknowledging the SYN (with an ACK = *X* + 1). Host *B* includes its own initial sequence number (SEQ = *Y*). An ACK = 20 means the host has received bytes 0 through 19 and expects byte 20 next. This technique is called forward acknowledgment. Host *A* then acknowledges all bytes Host *B* sent with a forward acknowledgment indicating the next byte Host *A* expects to receive (ACK = *Y* + 1). Data transfer then can begin.

5. *Define controlled access and list three protocols in this category.* **(2018-19)**

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. Protocols in this category: reservation, polling, token passing.

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

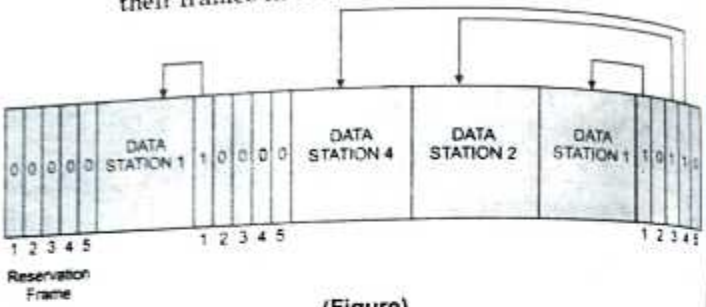
The three controlled-access methods are :

(1) Reservation
(2) Polling
(3) Token Passing

Reservation

(1) In the reservation method, a station needs to make a reservation before sending data.
(2) The time line has two kinds of periods :
  (a) Reservation interval of fixed time length
  (b) Data transmission period of variable frames.
(3) If there are *M* stations, the reservation interval is divided into *M* slots, and each station has one slot.
(4) Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
(5) In general, *i* th station may announce that it has a frame to send by inserting a 1 bit into *i* th slot. After all N slots have been checked, each station knows which stations wish to transmit.

(6) The stations which have reserved their slots transfer their frames in that order.



(Figure)

Polling

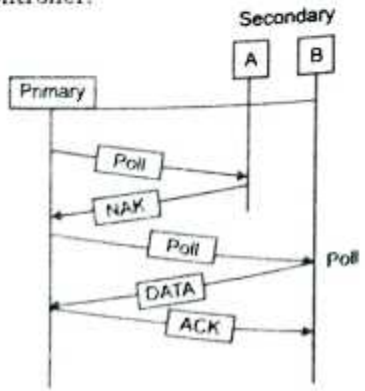
(1) Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.

(2) In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.

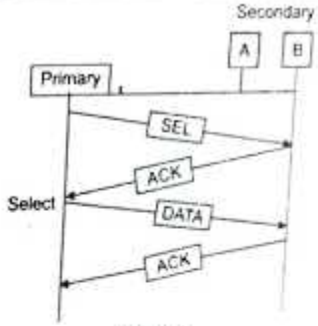
(3) The message sent by the controller contains the address of the node being selected for granting access.

(4) Although all nodes receive the message but the addressed one responds to it and sends data, if any. If there is no data, usually a "poll reject"(NAK) message is sent back.

(5) Problems include high overhead of the polling messages and high dependence on the reliability of the controller.



(Figure)



(Figure)

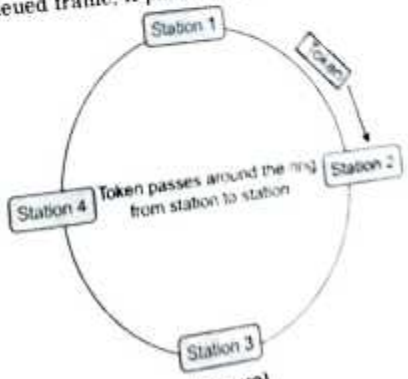
Token Passing :

(1) In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens.

(2) A token is a special bit pattern or a small message, which circulate from one station to the next in the some predefined order.

(3) In Token ring, token is passed from one station to another adjacent station in the ring whereas in case of Token bus, each station uses the bus to send the token to the next station in some predefined order.

(4) In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.



(Figure)

6. *CB84000D001C001C is the content of a UDP header*
(1) *What is the source port number?*
(2) *What is the destination port number?*
(3) *What is the length of the data?*
(4) *What is the total length of the user datagram?*
(2018-19)

(1) The source port number is the first four hexadecimal digits $(CB84)_{16}$ which means that the source port number is 52100.

(2) The destination port number is the second four hexadecimal digits $(000D)_{16}$, which means that the destination port number is 13.

(3) The length of the data is the length of the whole packet minus the length of the header, or 28 – 8 = 20 bytes.

(4) The third four hexadecimal digits $(001C)_{16}$ define the length of the whole UDP packet as 28 bytes.

7. *Explain SCTP.* **(2017-18)**

SCTP (Stream Control Transmission Protocol)

SCTP (Stream Control Transmission Protocol) is a protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network. Sometimes referred to as "next generation TCP" (Transmission Control Protocol) - or TCPng, SCTP is designed to make it easier to support a telephone connection over the Internet (and specifically to support the telephone system's Signaling System 7 - SS7 - on an Internet connection). A telephone connection requires that signaling information (which controls the connection) be sent along with voice and other data at the same time. SCTP also is intended to make it easier to manage connections over a wireless network and to manage the transmission of multimedia data.

Like TCP, SCTP manages "reliable transport" (ensuring the complete arrival of data units that are sent over the network) over the Internet's basically connectionless Internet Protocol (IP), the protocol responsible for moving the data but not for managing whether all the data arrives. Unlike TCP, SCTP ensures the complete concurrent transmission of several streams of data (in units called messages) between connected end points. SCTP also supports multihoming, which means that a connected end point can have alternate IP addresses associated with it in order to route around network failure or changing conditions.

8. *Define Connectionless and Connection-oriented Protocols.* **(2017-18)**

Connection Less Services

Connection Less Services is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

Connection Oriented Services

There is a sequence of operation to be followed by the users of connection oriented service. These are :

(1) Connection is established.
(2) Information is sent.
(3) Connection is released.

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection.

Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

9. *What is the maximum and minimum size of a UDP datagram? Also discuss the use of UDP.* **(2014-15)**

Maximum and Minimum Size of a UDP Datagram

User Datagram (UDP) packets, called user data grams, have a fixed-size header of 8 bytes. The fields are as follows :

(1) **Source Port Number :** This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535. If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.

(2) **Destination Port Number :** This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet.

(3) **Length :** This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be much less because a UDP user datagram is stored in an IP datagram with a total length of 65,535 bytes. The length field in a UDP user datagram is actually not necessary. A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram that defines the total length. There is another field in the IP datagram that defines the length of the header. So if we subtract the value of the second field from the first, we can deduce the length of a UDP datagram that is encapsulated in an IP datagram. However, the designers of the UDP protocol felt that it was more efficient for the destination UDP to calculate the length of the data from the information provided in the UDP user datagram rather than ask the IP

software to supply this information. We should remember that when the IP software delivers the UDP user datagram to the UDP layer, it has already dropped the IP header.

(4) **Checksum :** This field is used to detect errors over the entire user datagram (header plus data)

Use of UDP

The following lists some uses of the UDP protocol :

(1) UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as FrP that needs to send bulk data.

(2) UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.

(3) UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.

(4) UDP is used for management processes such as SNMP.

(5) UDP is used for some route updating protocols such as Routing Information Protocol (RIP).

10. *Discuss the Transport Layer Security.* **(2010-11)**

Transport Layer Security

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

TLS is Composed of Two Layers

The TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption.

The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is

exchanged. The TLS protocol is based on Netscape's SSL 3.0 protocol; however, TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0. The most recent browser versions support TLS.

11. *Draw TCP segment Header Format and explain its various fields.* **(2010-11)**

TCP Sliding Window

A TCP sliding window provides more efficient use of network bandwidth than PAR because it enables hosts to send multiple bytes or packets before waiting for an acknowledgment. In TCP, the receiver specifies the current window size in every packet. Because TCP provides a byte-stream connection, window sizes are expressed in bytes. This means that a window is the number of data bytes that the sender is allowed to send before waiting for an acknowledgment. Initial window sizes are indicated at connection setup but might vary throughout the data transfer to provide flow control. A window size of zero, for instance, means "Send no data." In a TCP sliding-window operation, for example, the sender might have a sequence of bytes to send (numbered 1 to 10) to a receiver who has a window size of five. The sender then would place a window around the first five bytes and transmit them together. It would then wait for an acknowledgment.

The receiver would respond with an ACK = 6, indicating that it has received bytes 1 to 5 and is expecting byte 6 next. In the same packet, the receiver would indicate that its window size is 5. The sender then would move the sliding window five bytes to the right and transmit bytes 6 to 10. The receiver would respond with an ACK = 11, indicating that it is expecting sequenced byte 11 next. In this packet, the receiver might indicate that its window size is 0 (because, for example, its internal buffers are full). At this point, the sender cannot send any more bytes until the receiver sends another packet with a window size greater than 0.

TCP Packet Format : The fields and overall format of a TCP packet. Figure given below shows twelve fields comprise a TCP packet.

Source Port			Destination Port
Sequence Number			
Acknowledgment Number			
Data Offset	Reserved	Flags	Window
Checksum			Urgent Pointer
Options (+ Padding)			
Data (Variable)			

(Figure)

TCP Packet Field Descriptions

The following descriptions summarize the TCP packet fields illustrated in

(1) Source Port and Destination Port : Identifies points at which upper-layer source and destination processes receive TCP services.

(2) Sequence Number : Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field also can be used to identify an initial sequence number to be used in an upcoming transmission.

(3) Acknowledgment Number : Contains the sequence number of the next byte of data the sender of the packet expects to receive.

(4) Data Offset : Indicates the number of 32-bit words in the TCP header.

(5) Reserved : Remains reserved for future use.

(6) Flags : Carries a variety of control information, including the SYN and ACK bits used for connection establishment and the FIN bit used for connection termination.

(7) Window : Specifies the size of the sender's receive window (that is, the buffer space available for incoming data).

(8) Checksum : Indicates whether the header was damaged in transit.

(9) Urgent Pointer : Points to the first urgent data byte in the packet.

(10) Options : Specifies various TCP options.

(11) Data : Contains upper-layer information.

12. *What do you mean by congestion control and QoS? What are the parameters of QoS? Explain.* (2013-14)

Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories : open-loop congestion control (prevention) and closed-loop congestion control (removal).

Quality of Service : Quality of service (QoS) is the overall performance of a telephony or computer network, particularly the performance seen by the users of the network.

To quantitatively measure quality of service, several related aspects of the network service are often considered, such as error rates, bandwidth, throughput, transmission delay, availability, jitter, etc.

Quality of service is particularly important for the transport of traffic with special requirements. In particular, much technology has been developed to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter service demands.

Parameters of Quality of Service

In packet-switched networks, quality of service is affected by various factors, which can be divided into "human" and "technical" factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, grade of service, etc.

Many things can happen to packets as they travel from origin to destination, resulting in the following problems as seen from the point of view of the sender and receiver :

(1) **Low Throughput :** Due to varying load from disparate users sharing the same network resources, the bit rate (the maximum throughput) that can be provided to a certain data stream may be too low for real time multimedia services if all data streams get the same scheduling priority.

(2) **Dropped Packets :** The routers might fail to deliver (drop) some packets if their data loads are corrupted, or the packets arrive when the router buffers are already full. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.

(3) **Errors :** Sometimes packets are corrupted due to bit errors caused by noise and interference, especially in wireless communications and long copper wires. The receiver has to detect this and, just as if the packet was dropped, may ask for this information to be retransmitted.

(4) **Latency :** It might take a long time for each packet to reach its destination, because it gets held up in long queues, or it takes a less direct route to avoid congestion. This is different from throughput, as the *delay* can build up over time, even if the throughput is almost normal. In some cases, excessive latency can render an application such as VoIP or online gaming unusable.

(5) **Jitter :** Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.

(6) **Out-of-order Delivery :** When a collection of related packets is routed through a network, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This is especially important for video and VoIP streams where quality is dramatically affected by both latency and lack of sequence.

13. *What is the difference between open-loop congestion control and closed-loop congestion control?* (2013-14)

Difference between Open-loop Congestion Control and Closed-loop Congestion Control

Closed-loop Control :

(1) Shows a closed-loop action (closed control loop).

(2) Can counteract against disturbances (negative feedback).

(3) Can become unstable, i.e. the controlled variable does not fade away, but grows (theoretically) to an infinite value.

Open-Loop Control :

(1) Shows an open-loop action (controlled chain).

(2) Can only counteract against disturbances, for which it has been designed; other disturbances cannot be removed.

(3) Cannot become unstable – as long as the controlled object is stable.

Summarizing These Properties We can Define : Systems in which the output quantity has no effect upon the process input quantity are called open-loop control systems.

Systems in which the output has an effect upon the process input quantity in such a manner as to maintain the desired output value are called closed-loop control systems.

14. *Describe Hop-by-hop choke packets algorithm to congestion handling.* (2010-11)

Hop-By-Hop Choke Packets

(1) A more direct way of telling the source to slow down.

(2) A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow.

(3) The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.

(4) An example of a choke packet is the ICMP Source Quench Packet.

(5) Over long distances or at high speeds choke packets are not very effective.

(6) A more efficient method is to send to choke packets hop-by-hop.

(7) This requires each hop to reduce its transmission even before the choke packet arrives at the source.

15. *Explain Process to Process delivery.*

Process to Process Delivery : UDP and TCP

(1) UDP and TCP are transport-layer protocols that create a process-to-process communication.

(2) UDP is an unreliable and connectionless protocol that requires little overhead and offers fast delivery.

(3) In the client-server paradigm, an application program on the local host, called the client, needs services from an application program on the remote host, called a server.

(4) Each application program has a unique port number that distinguishes it from other programs running at the same time on the same machine.

(5) The client program is assigned a random port number called the ephemeral port number.

(6) The server program is assigned a universal port number called a well-known port number.

(7) The combination of the IP address and the port number, called the socket address, uniquely defines a process and a host.

(8) The UDP packet is called a user datagram.

(9) UDP has no flow control mechanism.

(10) Transmission Control Protocol (TCP) is a connection-oriented, reliable, stream transport-layer protocol in the Internet model.

(11) The unit of data transfer between two devices using TCP software is called a segment; it has 20 to 60 bytes of header, followed by data from the application program.

(12) TCP uses a sliding window mechanism for flow control.

(13) Error detection is handled in TCP by the checksum, acknowledgment, and time-out.

(14) Corrupted and lost segments are retransmitted, and duplicate segments are discarded.

(15) TCP uses four timers—retransmission, persistence, keep-alive, and time-waited—in its operation.

(16) Connection establishment requires three steps; connection termination normally requires four steps.

(17) TCP software is implemented as a finite state machine.

(18) The TCP window size is determined by the receiver.

16.
- ***Write a short note on quality of service (QOS).***
- ***Explain the techniques of improve the quality of service.***
- ***Write the name and explain techniques for achieving good QOS.***

On the Internet and in other networks, QoS (Quality of Service) is the idea that transmission rate error rates, and other characteristics can be measure improved, and, to some extent, guaranteed in advance. Q is of particular concern for the continuous transmissio high-bandwidth video and multimedia informati Transmitting this kind of content dependably is difficul public networks using ordinary "best effort" protocols.

QoS can be improved with traffic shaping techniq such as packet prioritization, application classification queuing at congestion points. Using the Interne Resource Reservation Protocol (RSVP), packets pass through a gateway host can be expedited based on po and reservation criteria arranged in advance. Using AT which also lets a company or user preselect a level quality in terms of service, QoS can be measured a guaranteed in terms of the average delay at a gateway, th variation in delay in a group of cel (cells are 53-byte transmission units), cell losses, and th transmission error rate.

The Common Open Policy Service (COPS) is a protocol that allows router and layer 3 switches to get QoS policy information from the network policy server.

17.
- ***What is UDP? What is the maximum size of a UDP datagram?***
- ***Compare the TCP header and the UDP header. List the field in the TCP header that are missing from UDP header. Give the reason for their absence. What is the maximum and minimum size of TCP and UDP header?***

Comparison of TCP Header and The UDP Header

Characteristic / Description	UDP	TCP
General Description	Simple, high-speed, low-functionality "wrapper" that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues
Protocol Connection Setup	Connectionless; data is sent without setup.	Connection-oriented; connection must be established prior to transmission
Data Interface To Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure
Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged
Retransmissions	Not performed. Application must detect lost data and retransmit if needed	Delivery of all data is managed, and lost data is retransmitted automatically
Types of Applications That Use The Protocol	Applications where data delivery speed matters more than completeness, where small amounts of data are sent; or where multicast/broadcast are used	Most protocols and applications sending data that must be received reliably, including most file and message transfer protocols
Features Provided to Manage Flow of Data	None	Flow control using sliding windows, window size adjustment heuristics, congestion avoidance algorithms
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Well-Known Applications and	Multimedia applications, DNS	FTP, Telnet, SMTP, DNS, HTTP, POP

Protocols	BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions)	NNTP, IMAP, BGP, IRC, NFS (later versions)
Data Quantity Suitability	Small to moderate amounts of data (up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)

List the Field in the TCP Header that is Missing from UDP Header

The sequence number, acknowledge number, and window fields.

Absence Reason : In TCP header (32 *bits*) we have a field that is called options and padding that has variable in length and the header length shows the actual header size of 20 octets + size of options and padding field and in UDP we don't have any field like that and its header is fixed of 8 OCTETS (32 *bits* header size)

The Maximum and Minimum Size of TCP and UDP Header : For UDP, the head itself is 8 bytes, 2 of which are allocated for the payload size (in bytes). Since there are 8bits in a byte, that means the payload size can be a maximum of $2^{16} - 1$ bytes. The minimum size is just a header with no payload, and the maximum is the header size plus the maximum payload. Note that the header size is fixed.

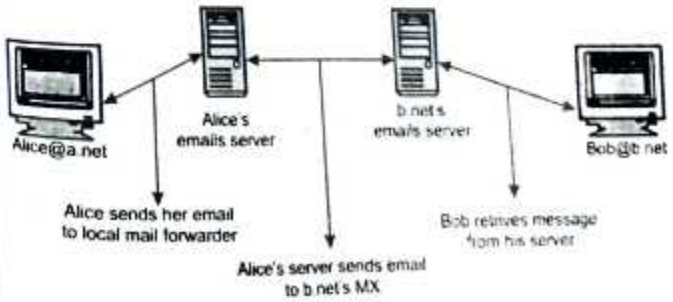
For TCP, it is slightly more complicated. The mandatory TCP header is 20 bytes (minimum size), with an optional variable amount of protocol options appended to the end of the header. The size of the header in 32bit words is defined by offset, which has 4 bits allocated to it. Therefore offset can have a max value of $2^4 - 1$, or 15. This means the maximum TCP header size is 60 bytes (15 * 4 bytes).

APPLICATION LAYER

1. ◆ ***Describe in detail about the following in Electronic mail.*** (2018-19)
   (1) ***Message format.***
   (2) ***Message transfer.***
   (3) ***Mail reader.***
   ◆ ***Briefly Explain Electronic mail system. Differentiate between POP 3 and IMAP protocol.*** (2017-18)
   ◆ ***Explain Email.***

Electronic mail, or email, is a very popular application in computer networks such as the Internet. Email appeared in the early 1970s and allows users to exchange text based messages. Initially, it was mainly used to exchange short messages, but over the years its usage has grown. It is now not only used to exchange small, but also long messages that can be composed of several parts as we will see later.

Before looking at the details of Internet email, let us consider a simple scenario illustrated in the figure below, where Alice sends an email to Bob. Alice prepares her email by using an email client and sends it to her email server. Alice's email server extracts Bob's address from the email and delivers the message to Bob's server. Bob retrieves Alice's message on his server and reads it by using his favourite email client or through his webmail interface.



Simplified Architecture of the Internet Email

The email system that we consider in this book is composed of four components :

(1) A message format, that defines how valid email messages are encoded

(2) Protocols, that allow hosts and servers to exchange email messages

(3) Client software, that allows users to easily create and read email messages

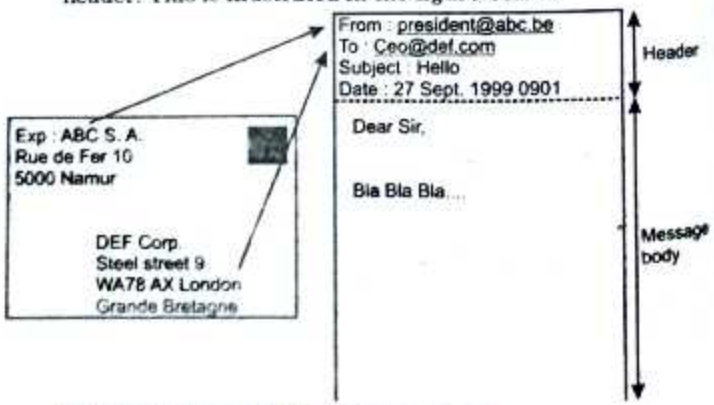
(4) Software, that allows servers to efficiently exchange email messages

Email messages, like postal mail, are composed of two parts :

(1) A header that plays the same role as the letterhead in regular mail. It contains metadata about the message.

(2) The body that contains the message itself.

Email messages are entirely composed of lines of ASCII characters. Each line can contain up to 998 characters and is terminated by the CR and LF control characters RFC 5322. The lines that compose the header appear before the message body. An empty line, containing only the CR and LF characters, marks the end of the header. This is illustrated in the figure below.



The Structure of Email Messages

The email header contains several lines that all begin with a keyword followed by a colon and additional information. The format of email messages and the

different types of header lines are defined in RFC 5322. Two of these header lines are mandatory and must appear in all email messages :

(1) **The Sender Address :** This header line starts with From:. This contains the (optional) name of the sender followed by its email address between < and >. Email addresses are always composed of a username followed by the @ sign and a domain name.

(2) **The Date :** This header line starts with Date . RFC 5322 precisely defines the format used to encode a date.

Other header lines appear in most email messages. The Subject: header line allows the sender to indicate the topic discussed in the email. Three types of header lines can be used to specify the recipients of a message :

(a) **The To :** Header line contains the email addresses of the primary recipients of the message. Several addresses can be separated by using commas.

(b) **The cc :** Header line is used by the sender to provide a list of email addresses that must receive a carbon copy of the message. Several addresses can be listed in this header line, separated by commas. All recipients of the email message receive the To : and cc : header lines.

(c) **The bcc :** Header line is used by the sender to provide a list of comma separated email addresses that must receive a blind carbon copy of the message. The bcc : header line is not delivered to the recipients of the email message.

Difference Between POP3 and IMAP Protocol :

Differences	POP3	IMAP
Name	Post Office Protocol is a client/server protocol in which e-mail is received and held for you by your Internet server.	Internet Messaging Access Protocol is a two way synchronization between the email client you use and access same account from multiple email clients.
Typical Use	Access mails from single machine	Access mails from multiple machines

Append	No	Yes
Folders	No	Yes
Protocol Granularity	Limited retrieve the entire mail	Retrieve any part of the mail
Complexity	Less complex to implement pop client and server	More complex to implement the client and server based on the demanding task

Message Transfer : A message transfer (MT) is a software application used within an Internet message handling system (MHS). It is responsible for transferring and routing an electronic mail message from the sender's computer to the recipient's computer. The basic platform for an MTA is an exchange system with client/server architecture.

A message transfer agent receives incoming emails and forwards the messages to individual clients/users. The main function of the MTA is forwarding the incoming message to the proper end-user or destination. Microsoft Exchange and UNIX sendmail are the best examples of MTAs.

MT is also known as mail relay.

Mail Reader : Email reader or more formally mail user agent (MUA) is a computer program used to access and manage a user's email.

A web application which provides message management, composition, and reception functions may act as an email client, and "email client" may also refer to a piece of computer hardware or software whose primary or most visible role is to work as an email client.

The most common arrangement is for an email user (the client) to make an arrangement with a remote Mail Transfer Agent (MTA) server for the receipt and storage of the client's emails. The MTA, using a suitable mail delivery agent (MDA), adds email messages to a client's storage as they arrive. The remote mail storage is referred to as the user's mailbox. The default setting on many Unix systems is for the mail server to store formatted messages in mbox, within the user's HOME directory. Of course, users of the system can log-in and run a mail client on the same computer that hosts their mailboxes; in

which case, the server is not actually remote, other than in a generic sense.

2. ◆ ***Write about digital signature.*** **(2018-19)**
   ◆ ***Define Cryptography. List four Cryptography Primitives.*** **(2017-18)**

Cryptography

There are two kinds of cryptosystems : symmetric and asymmetric. Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt a message and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Asymmetric cryptosystems are also called public key cryptosystems. Symmetric cryptosystems have a problem: How do you transport the secret key from the sender to the recipient securely and in a tamperproof fashion? If you could send the secret key securely, then, in theory, you wouldn't need the symmetric cryptosystem in the first place : because you would simply use that secure channel to send your message. Frequently, trusted couriers are used as a solution to this problem. Another, more efficient and reliable solution is a public key cryptosystem, such as RSA, which is used in the popular security tool PGP. Sci.crypt and sci.crypt.research are two USENET newsgroups that deal exclusively with cryptography. The latter is a moderated group.

This is an important part of any Internet Service. Some points we like to emphasize are :

(1) We examine/block traffic attempting to access our network for only approved access.

(2) Adaptive firewall software looks for unusual activity, automatically protects and alerts staff.

(3) Security fixes/patches are applied in a timely manner and we use the Red Hat Network to keep current.

(4) Internally we use best practices regarding your passwords. We also closely monitor subscriber activity to note any unusual command usage. Our web site control panel allows you to both check & set security permissions on your files.

Cryptography Primitives

These are following four cryptography primitives given below.

Encryption : In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher text that can be read only if decrypted.

MAC : A media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC) for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi.

Hash Function : A Hash function is any function that can be used to map data of arbitrary size to data of a fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

Digital Signature : A Digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

3. *Differentiate between Symmetric Key Encryption and Asymmetric Key Encryption.* (2017-18)

Difference Between Symmetric Key Encryption and Asymmetric Key Encryption

	Symmetric Encryption	Asymmetric Encryption
Functionality	Allows efficient communication between two parties in a closed environment.	Enables security in settings in which symmetric encryption simply does not work or is more difficult to implement.
Computational efficiency	Computes incredibly fast, since the relatively simple operations used are executed very efficiently.	Computes slowly, using computationally heavy and complex operations, based on the difficulty of solving number theoretic problems.
Key size	Uses 128-bit symmetric keys, which are considered very secure.	Employs key sizes of at least 1000 bits to achieve sufficient, lasting security.
Hardware	Performs simple algorithms requiring relatively inexpensive hardware.	Implements complex and time – consuming algorithms that need more powerful hardware.

4. *Define Application-Layer Paradigms.* (2017-18)

Application – Layer Paradigms

This is the scope within which applications create user data and communicate this data to other processes or applications on another or the same host. The communications partners are often called peers. This is where the "higher level" protocols such as SMTP, FTP, SSH, HTTP, etc. operate.

To use Internet, need two application programs to internet with each other :

(1) One running on a computer somewhere in world.

(2) Another running on computer somewhere else.

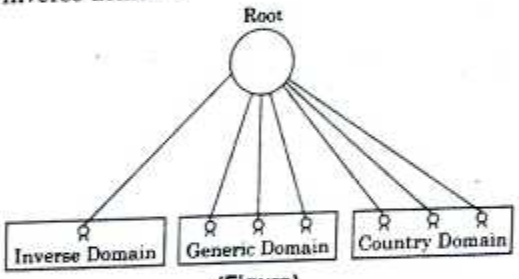
- (a) Need to send messages to each other through Internet infrastructure.
- (b) Two paradigms have been developed.
- (c) Client – server paradigm.
- (d) Peer – to – peer paradigm (discussed last week).

5. *What is the essence of DNS (Domain Name system)? How does it map to IP address?*

To identify an entity TCP/IP protocols use the IP address which uniquely identifies the connection of a host to the internet. However people prefer to use names instead of address. Therefore we need a system that can map a name to an address. This is the Domain Name System (DNS).

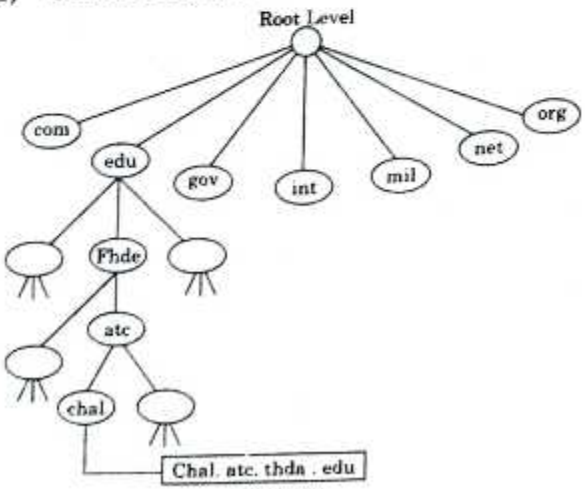
DNS in the Internet

DNS is a protocol that can be used in different platform. In the internet the domain name space is divided into three different section generic domain, country domains and inverse domain.



(Figure)

(1) Generic Domains :

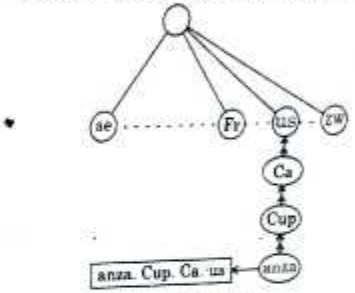


(Figure)

The generic domain define registered host according to their generic behaviour, each node in the tree defines a domain.

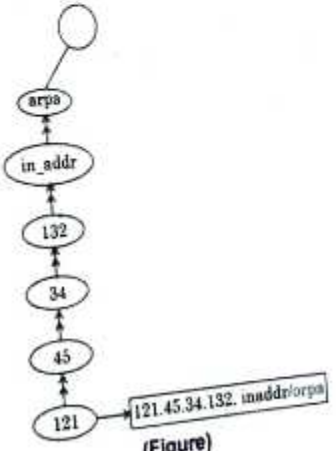
(2) Country Domains : The country domain section follows the same format as the generic domain but uses two-character country abbreviation (example, 'US' for United States) in place of three character organizational.

Figure shows the country domain section the address anza. cup.ca.us can be translated to be Anza College in Cupertino in California.



(Figure)

(3) Inverse Domain : The inverse domain is used to map an address to a name, this may happen for example when a server has received a request from a client to do a task.



(Figure)

In any network programs theoretically could refer to hosts, mailboxes and other resources by their network addresses, these addresses are hard for people to remember. Also sending e-mail to raj@172.28.23.100 means that if raj's ISP or organization moves the mail server to a different machine with a different IP address, her e-mail address has to change.

However, when thousands of minicomputers and PCs were connected to the net, everyone realized that this approach could not continue to work forever. For one thing, the size of the file would become too large. However, even more important, host name conflicts would occur constantly unless names were centrally managed, something unthinkable in a huge international network due to the load and latency. To solve these problems, DNS (Domain Name System) was invented. The essence of DNS is the invention of a hierarchical, domain-based naming scheme and a distributed database system for implementing this naming scheme. It is primarily used for mapping host names and e-mail destinations to IP addresses but can also be used for other purposes. DNS is defined in RFCs 1034 and 1035. Very briefly, the way DNS is as follows. To map a name onto an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter. We saw an example of a resolver, get host-by name, Fig given below. The resolver sends a UDP Packet to a local DNS Server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller. Armed with the IP Address, the program can then establish a TCP connection with the destination or send it UDP packets.

6. *Write a short note on FTP.*

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network.

FTP is built on client-server model architecture and uses separate control and data connections between the

client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.

FTP sessions work in passive or active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data. In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and Network Address Translation (NAT) gateways.

7. *What is World Wide Web? Illustrate history and growth of web.* (2013-14)

World Wide Web

The term WWW refers to the World Wide Web or simply the Web. The World Wide Web consists of all the public Web sites connected to the Internet worldwide, including the client devices (such as computers and cell phones) that access Web content. The WWW is just one of many applications of the Internet and computer networks.

The World Web is based on these technologies :

(1) **HTML** : Hypertext Markup Language

(2) **HTTP** : Hypertext Transfer Protocol

(3) Web servers and Web browsers

History and Growth of the Web

Tim Berners-Lee invented the World Wide Web in 1989, about 20 years after the first connection was established over what is today known as the Internet. At the time, Tim was a software engineer at CERN, the large particle physics laboratory near Geneva, Switzerland. Many scientists participated in experiments at CERN for extended periods of time and then returned to their laboratories around the world. These scientists were eager to exchange data and results, but had difficulties doing so. Tim understood this need, and understood the unrealized potential of millions of computers connected together through the Internet.

Tim documented what was to become the World Wide Web with the submission of a proposal to his management at CERN, in late 1989. This proposal specified a set of technologies that would make the Internet truly accessible and useful to people. Believe it or not, Tim's initial proposal was not immediately accepted. However, Tim persevered. By October of 1990, he had specified the three fundamental technologies that remain the foundation of today's Web (and which you may have seen appear on parts of your Web browser) :

(1) **HTML** : Hyper Text Markup Language. The publishing format for the Web, including the ability to format documents and link to other documents and resources.

(2) **URI** : Uniform Resource Identifier. A kind of "address" that is unique to each resource on the Web.

(3) **HTTP** : Hypertext Transfer Protocol. Allows for the retrieval of linked resources from across the Web.

Tim also wrote the first Web page editor/browser ("World Wide Web") and the first Web server ("httpd"). By the end of 1990, the first Web page was served. By 1991, people outside of CERN joined the new Web community. Very important to the growth of the Web, CERN announced in April 1993 that the World Wide W technology would be available for anyone to use on royalty-free basis.

Since that time, the Web has changed the world. I has arguably become the most powerful communication medium the world has ever known. Whereas only 25% of the people on the planet are currently using the Web (and the Web Foundation aims to accelerate this growth substantially), the Web has changed the way we teach and learn, buy and sell, inform and are informed, agree and disagree, share and collaborate, meet and love, and tackle problems ranging from putting food on our tables to curing cancer.

Tim Berners-Lee and others realized that for the Web to reach its full potential, the underlying technologies must become global standards, implemented in the same way around the world. Therefore, in 1994, Tim founded the World Wide Web Consortium (W3C) as a place for stakeholders to reach consensus around the specification and guidelines to ensure that the Web works for everyone and that it evolves in a responsible manner. W3C standards have enabled a single World Wide Web of information and people, and an increasingly-rich set of capabilities: Web 2.0 (personal and dynamic), Web 3.0 (a semantic Web of linked data), Web services, voice access, mobile access, accessibility for people with disabilities and for people speaking many languages, richer graphics and video, etc. The Web Foundation supports the work of W3C to ensure that the Web and the technologies that underpin it remain free and open to all.

8. ***What do you mean by following :***

(1) HTTP

(2) SNMP

(1) ***HTTP : (Hyper Text Transport Protocol)***

(a) Mainly used to access data on the World Wide Web. It transfers data in form of plain text, hyper-text, audio, video and so on.

(b) It is used an environment where there are rapid jumps from document to another.

(c) HTTP functions like a combination of

(i) FTP (File Transfer Protocol).
(ii) STP (Simple Mail Transfer Protocol)

(d) HTTP is like SMTP because the data transferred between client and server is similar to SMTP message.
(e) It is defined in RFC - 2616
(f) Support persistent connections.

(2) **SNMP (Simple Network Management Protocol)**

(a) The TCP/IP protocol specifies the process of management in the internet.
(b) Specify detail such as message format and the use of transport protocol.
(c) Its standard defines the set of operation and the meaning of each.
Example : Routers keep statistics on the status of LAN/WAN interface :
(d) Incoming, outgoing packet traffic.
(e) Dropped datagram.
(f) Error messages interfaces.
(g) Band rate.
(h) SNMP doesn't specify exactly which data can be accessed on which device.

9. *Write short notes on Telnet and Rlogin.* (2013-14)

Telnet and Rlogin

Telnet : Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

Rlogin : Rlogin (remote login) is a UNIX command that allows an authorized user to login to other UNIX machines (hosts) on a network and to interact as if the user were physically at the host computer. Once logged in to the host, the user can do anything that the host has given permission for, such as read, edit, or delete files.

Rlogin is similar to the better known Tel command. Rlogin is considered useful for simple log that don't require a lot of control over the client/ho interaction, but is thought to be less useful than Teln where a lot of customization is desired, for multip sessions, for connections between very distant terminals o to terminals that are not running UNIX, for that matter since rlogin can only connect to UNIX hosts. A benefit of rlogin is the ability to use a file called hosts that resides on the host machine and maintains a list of terminals allowed to login without a password.

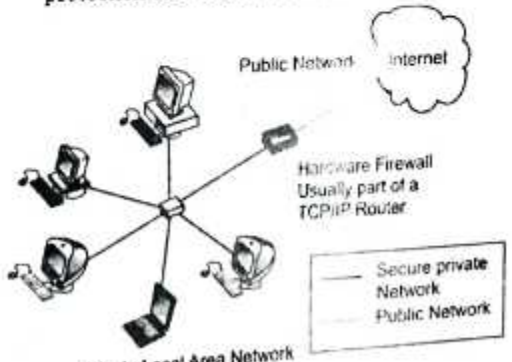
A secure version of rlogin (slogin) was combined with two other UNIX utility, ssh and scp, in the Secure Shell suite, an interface and protocol created to replace the earlier utilities.

10. *Write short note on Firewall.* (2013-14)

Firewall

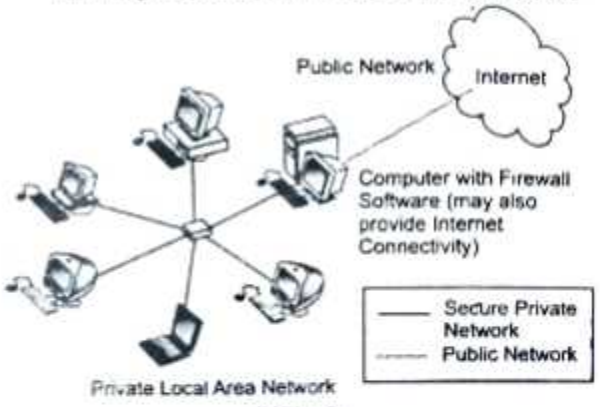
A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to.

(1) **Hardware Firewall** : Hardware firewall providing protection to a Local Network.



(Figure)

(2) **Computer with Firewall Software** : Computer running firewall software to provide protection



(Figure)

A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers. The term firewall comes from the fact that by segmenting a network into different physical subnet works, they limited the damage that could spread ,from one subnet to another just like fire doors or firewalls.

11. *What is MIME? Explain standard content-types of MIME in detail.* **(2010-11)**

MIME

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support :

(1) Text in character sets other than ASCII.
(2) Non-text attachments.
(3) Message bodies with multiple parts.
(4) Header information in non-ASCII character sets.

MIME's use, however, has grown beyond describing the content of email to describe content type in general, including for the web and as storage for rich content in some commercial products (example, IBM Lotus Domino and IBM Lotus Quickr).

Virtually all human-written Internet email and a fairly large proportion of automated email is transmitted via SMTP in MIME format. Internet email is so closely associated with the SMTP and MIME standards that it is sometimes called SMTP/MIME email.

The content types defined by MIME standards are also of importance outside of email, such as in communication protocols like HTTP for the World Wide Web. HTTP requires that data be transmitted in the context of email-like messages, although the data most often is not actually email.

Standard Content Types of MIME

This header indicates the Internet media type of the message content, consisting of a type and subtype, for example

Content Type : Text / plain

Through the use of the multipart type, MIME allows messages to have parts arranged in a tree structure where the leaf nodes are any non-multipart content type and the non-leaf nodes are any of a variety of multipart types. This mechanism supports :

(1) Simple text messages using text/plain (the default value for "Content-Type: ")
(2) Text plus attachments (multipart/mixed with a text/plain part and other non-text parts) A MIME message including an attached file generally indicates the file's original name with the "Content-disposition:" header, so the type of file is indicated both by the MIME content-type and the (usually OS-specific) filename extension.
(3) Reply with original attached (multipart/mixed with a text/plain part and the original message as a message/rfc822 part)
(4) Alternative content, such as a message sent in both plain text and another format such as HTML (multipart/alternative with the same content in text/plain and text/html forms)
(5) Image, audio, video and application (for example, image/ jpeg, audio/mp3, video/mp4 and a plication / MS word and so on)
(6) Many other message constructs

Following is a Table for **Content Types of MIME** :

Description of Data Content	Typical Filename Extensions	MIME type/subtype
Text and Text Related **Types** :		
HTML text data (RFC 1866)	html htm	text/html
Plain text documents program listings	txt c c++ pl cc h	text/plain
Richtext (obsolete replaced by text/enriched)		text/richtext
Structure enhanced text	(etx?)	text/x-setext
Image Types :		
GIF	gif	image/gif
X-Windows bitmap (b w)	xbm	image/x-xbitmap
X-Windows pixelmap (8-bit color)	xpm	image/x-xpixmap
Portable Network Graphics	png	image/x-png
Audio/Voice/Music Related Types :		
"basic" audio - 8-bit u-law PCM	au snd	audio/basic
Macintosh audio format (Alpple)	aif aiff aifc	audio/x-aiff
Microsoft audio	wav	audio/x-wav
Video Types :		
MPEG video	mpeg mpg mpe	video/mpeg
MPEG-2 video	mpv2 mp2v	video/mpeg 2
Macintosh QuickTime	qt mov	video/quicktime

12. ***What is the function of SMTP? Differentiate between a User Agent (UA) and a Mail Transfer Agent. How does MIME enhance SMTP?*** **(2013-14)**

Function of SMTP

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail transfer (SMTP). It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides mail exchange between users on the same or different computers.

Difference between a User Agent (UA) and a Mail Transfer Agent (MTA)

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.

MIME Enhance SMTP : MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender, site to NVT ASCII data and delivers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original data.

13. ◆ ***Discuss the attacks.*** **(2018-19)**
◆ ***What do you understand by Network Security attacks/ Describe active and passive security attacks.***

Network Security Attacks

Network security measures are needed to protect data during their transmission. An assault on system security that derives from an intelligent threat that is an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system. The use of networks and communication facilities for carrying data between terminal user and computer and between computer and computer.

Examples of security attacks are as follows :

(1) Gain unauthorized access to information.

(2) Impersonate another user either to shift responsibility or else to use the other's license for the purpose of :
- **(a)** Originating fraudulent information.
- **(b)** Modifying legimate information.
- **(c)** Using fraudulent identity to gain unauthorized access.
- **(d)** Fraudulently identity transaction or endorsing them.

(3) Disavow responsibility or liability for information the cheater did originate.

(4) Claim to have received from some other user information that the cheater created.
(5) Claim to have sent to a receiver information that was not sent.
(6) Either disavow receipt of information that was in far received, or claim a false time of receipt.
(7) Modify the license of others.
(8) Insert self into a communication link between other users an active relay point.
(9) Pervert the function of software, typically by adding to convert function.
(10) Undermine confidence in a proposal by causing apparent failure in the system.

Types of Attack

There are two types of network security attack.

Active Attacks : Active attacks involve some modification of the data stream or the certain of a false stream and can be subdivided into four categories : masquerade, replay, modification of message, and denial of service.

(1) **Masquerade :** It take place when one entity pretends to be a different entity. A masquerade attack usually included one of other forms of active attack.
(2) **Replay :** It involves the passive capture of data unit and its subsequent retransmission to produce an unauthorized effect.
(3) **Modification of Messages :** It simply means that some portion of a legitimate message is altered or that message delayed or recorded to produce an unauthorized effect.
(4) **Denial of Service :** It prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target.

Passive Attacks : Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmissions. Two types of passive attacks are release of message contents and traffic analysis.

(1) **Release of Message Contents :** It is easily understood. A telephone conversation, an electronic mail message, and a transferred file may certain services or confidential information. We would like to

prevent the opponent from learning the contents of these transmissions.

(2) **Traffic Analysis :** It is subtler. Suppose that we had a way of making the contents of message and other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common techniquc for making content is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communication hosts and observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

14. ◆ ***What is data confidentiality?*** (2018-19)
◆ ***Explain Data Integrity.*** (2018-19)
◆ ***Define the three security goals.***

Three primary goals of Network Security are

(1) Confidentiality
(2) Integrity
(3) Availability

These three pillars of Network Security are often represented as CIA Triangle, as shown below :

(Figure)

Confidentiality : The first goal of Network Security is "Confidentiality". The function of "Confidentiality" is in protecting precious business data (in storage or in motion) from unauthorized persons. Confidentiality part of Network Security makes sure that the data is available only to intended and authorized persons. Access to business data should be only for those individuals who are permitted to use that data.

Integrity : The second goal of Network Security is "Integrity". Integrity aims at maintaining and assuring the accuracy and consistency of data. The function of Integrity is to make sure that the date is accurate and reliable and is not changed by unauthorized persons or hackers. The data received by the recipient must be exactly same as the data sent from the sender, without change in even single bit of data.

Availability : The third goal of network security is "Availability". The function of "Availability" in Network Security is to make sure that the Data, Network Resources or Network Services are continuously available to the legitimate users, whenever they require it.

15. *What do you understand by Cryptography? Describe the basic types of cryptographic systems.*

Cryptography

A cryptographic system (or a cipher system) is a method of hiding data so that only certain people can view it. Cryptography is the practice of creating and using cryptographic systems. Cryptanalysis is the science of analyzing and reverse engineering cryptographic systems. The original data is called plaintext. The protected data is called cipher text. Encryption is a procedure to convert plaintext into cipher text. Decryption is a procedure to convert cipher text into plaintext. A cryptographic system typically consists of algorithms, keys, and key management facilities.

Types of Cryptographic Systems

There are two basic types of cryptographic systems : symmetric ("private key") and asymmetric ("public key") :

(1) Symmetric or Private Key Cryptography : Symmetric cryptography uses a single private key to both encrypt and decrypt data. Any party that has the key can use it to encrypt and decrypt data. They are also referred to as block ciphers. Symmetric cryptography algorithms are typically fast and are suitable for processing large streams of data.

Symmetric key systems require both the sender and the recipient to have the same key. This key is used by the sender to encrypt the data, and again by the recipient to decrypt the data. Key exchange is clearly a problem. How do you securely send a key that will enable you to send other data securely? If a private key is intercepted or stolen, the adversary can act as either party and view all data and communications. You can think of the symmetric crypto system as akin to the Chubb type of door locks. You must be in possession of a key to both open and lock the door.

The disadvantage of symmetric cryptography is that it presumes two parties have agreed on a key and been able to exchange that key in a secure manner prior to communication. This is a significant challenge. Symmetric algorithms are usually mixed with public key algorithms to obtain a blend of security and speed.

(2) Asymmetric or Public Key Cryptography : Public-key cryptography is also called asymmetric. It uses a secret key that must be kept from unauthorized users and a public key that can be made public to anyone. Both the public key and the private key are mathematically linked; data encrypted with the public key can be decrypted only by the private key, and data signed with the private key can only be verified with the public key.

The public key can be published to anyone. Both keys are unique to the communication session.

Public-key cryptographic algorithms use a fixed buffer size. Private-key cryptographic algorithms use a variable length buffer. Public-key algorithms cannot be used to chain data together into streams like private-key algorithms can. With private-key algorithms only a small block size can be processed, typically 8 or 16 bytes.

Asymmetric cryptographic systems are considered much more flexible. Each user has both a public key and a private key. Messages are encrypted with one key and can be decrypted only by the other key. The public key can be published widely while the private key is kept secret. If Alice wishes to send Bob a secret, she finds and verifies Bob's public key, encrypts her message with it, and mails it off to Bob.

When Bob gets the message, he uses his private key to decrypt it. Verification of public keys is an important step. Failure to verify that the public key really does belong to Bob leaves open the possibility that Alice is using a key whose associated private key is in the hands of an enemy. Public Key Infrastructures or PKI's deals with this problem by providing certification authorities that sign keys by a supposedly trusted party and make them available for download or verification. Asymmetric ciphers are much slower than their symmetric counterparts and key sizes are generally much larger. You can think of a public key system as akin to a Yale type door lock. Anyone can push the door locked, but you must be in possession of the correct key to open the door.

❑❑

MCA

(SEM. IV) THEORY EXAMINATION, 2017-18

RCA – 402 : COMPUTER NETWORK

Time : 3 Hours *Total Marks : 70*

Note : Attempt *all* Sections. If require any missing data; then choose suitably.

SECTION – A

1. **Attempt *all* questions in brief.** **(2 × 7 = 14)**
   (a) Define Radio wave.
   (b) Define Protocol. Give the need for Protocol Layering.
   (c) Explain Nyquist Bit Rate.
   (d) Write about CSMA/CD protocol.
   (e) Explain burst error.
   (f) Write about Socket.
   (g) Differentiate between Symmetric Key Encryption and Asymmetric Key Encryption.

SECTION – B

2. **Attempt *any three* of the following :** **(7 × 3 = 21)**
   (a) What is switching? Briefly explain different Methods of Switching.
   (b) Define Data Communication. Describe Fundamental characteristics of Data Communication.
   (c) Briefly explain about IP Addressing. Differentiate between classfull addressing and classless addressing.
   (d) What is congestion? Define congestion control with a suitable Example.
   (e) Briefly Explain Electronic mail system. Differentiate between POP 3 and IMAP protocol.

SECTION – C

3. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) What is Network topology. Explain different types of topologies.
   (b) Explain Transmission media. Differentiate guided media from unguided media.

4. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) Describe hamming code. How it is used for error detection and correction? Illustrate with the help of a suitable example.
   (b) A classless address is given as 167.199.170.82/27. Find the
      (i) The number of addresses in the network
      (ii) First address
      (iii) Last address

5. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) Explain any two connecting devices : hubs, link - layer switches, and routers.
   (b) What are the performance measure criteria of a Network? Explain.

6. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) Explain any two protocol.
   (i) UDP
   (ii) TCP
   (iii) SCTP
   (b) Define Connectionless and Connection-Oriented Protocols.

7. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) Define Cryptography. List four Cryptography Primitives.
   (b) Define Application-Layer Paradigms.

❑❑

MCA

(SEM. IV) THEORY EXAMINATION, 2018-19
RCA – 402 : COMPUTER NETWORKS

Time : 3 Hours *Total Marks* : 70

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

SECTION – A

1. **Attempt *all* questions in brief.** **(2 × 7 = 14)**
   (a) What are the applications of computer network?
   (b) What is Shannon capacity for Noisy Channel?
   (c) Differentiate between Baseband Transmission and Broadband Transmission.
   (d) Distinguish between TCP and UDP.
   (e) What is Gateway?
   (f) Define Fragmentation.
   (g) Write about digital signature.

SECTION – B

2. **Attempt *any three* of the following :** **(7 × 3 = 21)**
   (a) What is Network? Explain different types of Networks.
   (b) What is cyclic code and explain Cyclic Redundancy Check (CRC) code?
   (c) What is IP addressing? How would you design class A, Class B and Class C of IP addresses?
   (d) Explain the TCP/IP reference model with neat diagram.
   (e) Describe in detail about the three way handshake protocol for connection establishment in TCP.

SECTION – C

3. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) What is transmission medium? What are the different types of transmission medium?
   (b) What is multiplexing? Define all Categories of multiplexing.

4. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) Write short notes on (i) SONET (ii) ATM (iii) BLUETOOTH.
   (b) Discuss different standards of Ethernet.

5. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) Describe internetworking connecting devices in reference to layers.
   (b) Define controlled access and list three protocols in this category.

6. **Attempt *any one* part of the following :** **(7 × 1 = 7)**
   (a) How is congestion controlled? Explain in details the TCP congestion control.
   (b) CB84000D001C001C is the content of a UDP header

(i) What is the source port number?
(ii) What is the destination port number?
(iii) What is the length of the data?
(iv) What is the total length of the user datagram?

7. **Attempt *any one* part of the following :** (7 × 1 = 7)

(a) What is security goals? Explain different types of Networ Attacks.

(b) Describe in detail about the following in Electronic mail.
(i) Message format.
(ii) Message transfer.
(iii) Mail reader.

QQ