**** THESE ANSWER KEYS ARE JUST A GUIDELINE.**

1 Attempt *any three* of the following: **15**

a Define Data Communication and Explain Components of Data Communication.

Ans: **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.

Components of Data Communication:

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.

b List and Explain the functions of ISO’s OSI Model Layers.

Ans: Functions of Different Layers :

Layer 1: The Physical Layer :

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

Layer 2: Data Link Layer :

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer :

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

Layer 4: Transport Layer :

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer :

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

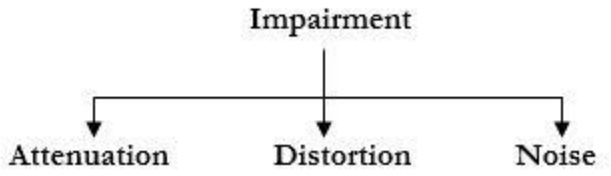
Layer 6: The Presentation Layer :

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It perfroms Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer :

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

c What do you mean by Transmission Impairments? Give the reasons of the same.



Attenuation:

The strength of a signal decrease with the increase in distance travelled over a medium. Attenuation means loss of energy. When any signal travels over a medium or channel, it loses some of its energy in the form of heat in the resistance of the medium. Attenuation decides the signal to noise ratio hence the quality of received signal.

Attenuation is given in decibels as:

Attenuation (dB) = 10log10 (Pout/Pin)

Where, Pin= Power at the sending end

Pout= Power at the receiving end

Distortion (Harmonic):

Another meaning of distortion is change in shape of the signal. This type of distortion is observed for the composite signals made by different frequencies. If the medium is not perfect, then all the frequency components present at the input will not only be equally attenuated and will not be proportionally delayed.

Noise:

When the data travels over a transmission medium, noise gets added to it. Noise is a major limiting factor in communication system performance. Noise can be categorized into four types as follows:

(i) Thermal noise (ii) Intermodulation noise (iii) Crosstalk (iv) Impulse noise

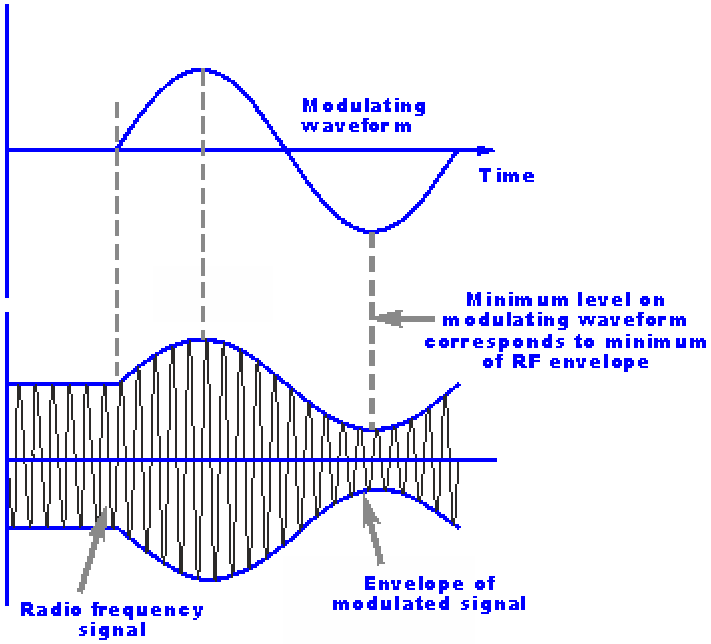
d Explain the following terms in relation with Data Communication

1. Half Duplex System.
   Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time. For example, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Like full-duplex transmission, half-duplex transmission implies a bidirectional line (one that can carry data in both directions).

2. Full Duplex System
   Full-duplex data transmission means that data can be transmitted in both directions on a signal carrier at the same time. For example, on a local area network with a technology that has full-duplex transmission, one workstation can be sending data on the line while another workstation is receiving data. Full-duplex transmission necessarily implies a bidirectional line (one that can move data in both directions).

e Write a short note on Amplitude Modulation.

When an amplitude modulated signal is created, the amplitude of the signal is varied in line with the variations in intensity of the sound wave. In this way the overall amplitude or envelope of the carrier is modulated to carry the audio signal. Here the envelope of the carrier can be seen to change in line with the modulating signal.


Modulating waveform
Time
Minimum level on modulating waveform corresponds to minimum of RF envelope
Radio frequency signal
Envelope of modulated signal

Amplitude Modulation

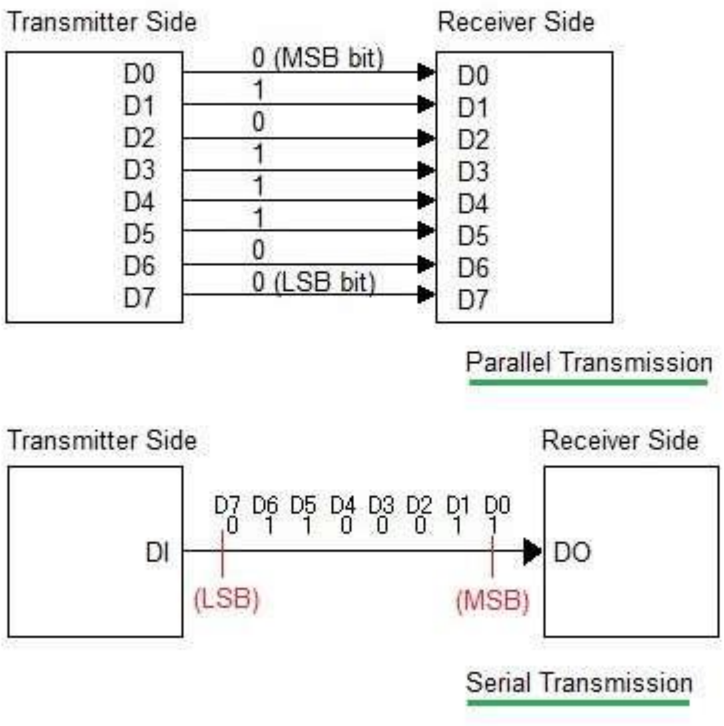
Amplitude modulation, AM is the most straightforward way of modulating a signal. Demodulation, or the process where the radio frequency signal is converted into an audio frequency signal is also very simple. An amplitude modulation signal only requires a simple diode detector circuit. The circuit that is commonly used has a diode that rectifies the signal, only allowing the one half of the alternating radio frequency waveform through. A capacitor is used to remove the radio frequency parts of the signal, leaving the audio waveform. This can be fed into an amplifier after which it can be used to drive a loudspeaker. As the circuit used for demodulating AM is very cheap, it enables the cost of radio receivers for AM to be kept low.

f. Explain the following terms of Data Transmission

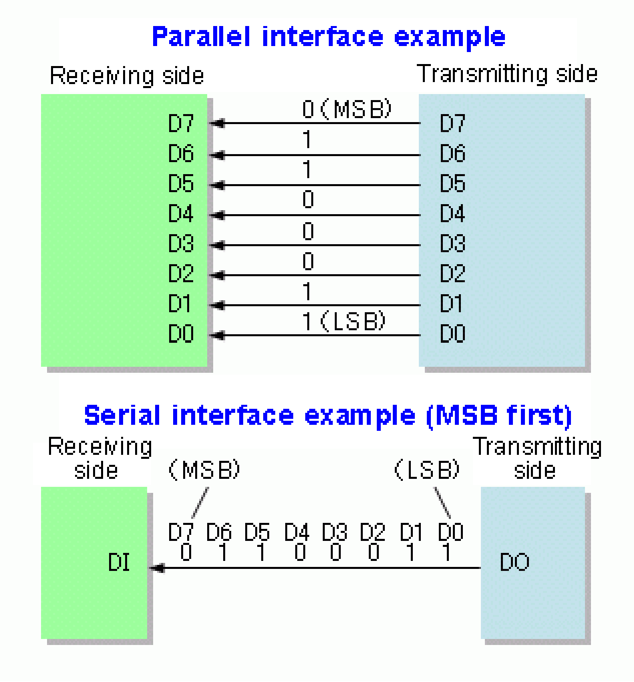
1. Parallel Transmission.

parallel transmission

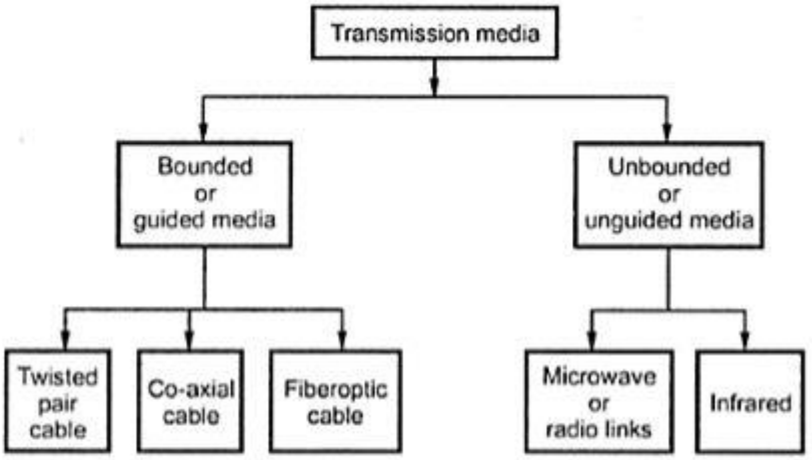
Transmitting several bits of data simultaneously using multiple lines (8, 16, 32, 64). The pathways between the CPU and memory are parallel, and they used to be parallel between the CPU and peripheral devices. For example, parallel ATA (PATA) was replaced with serial ATA (SATA); parallel PCI was replaced with serial PCIe. See SATA, PATA, PCI and PCIE.

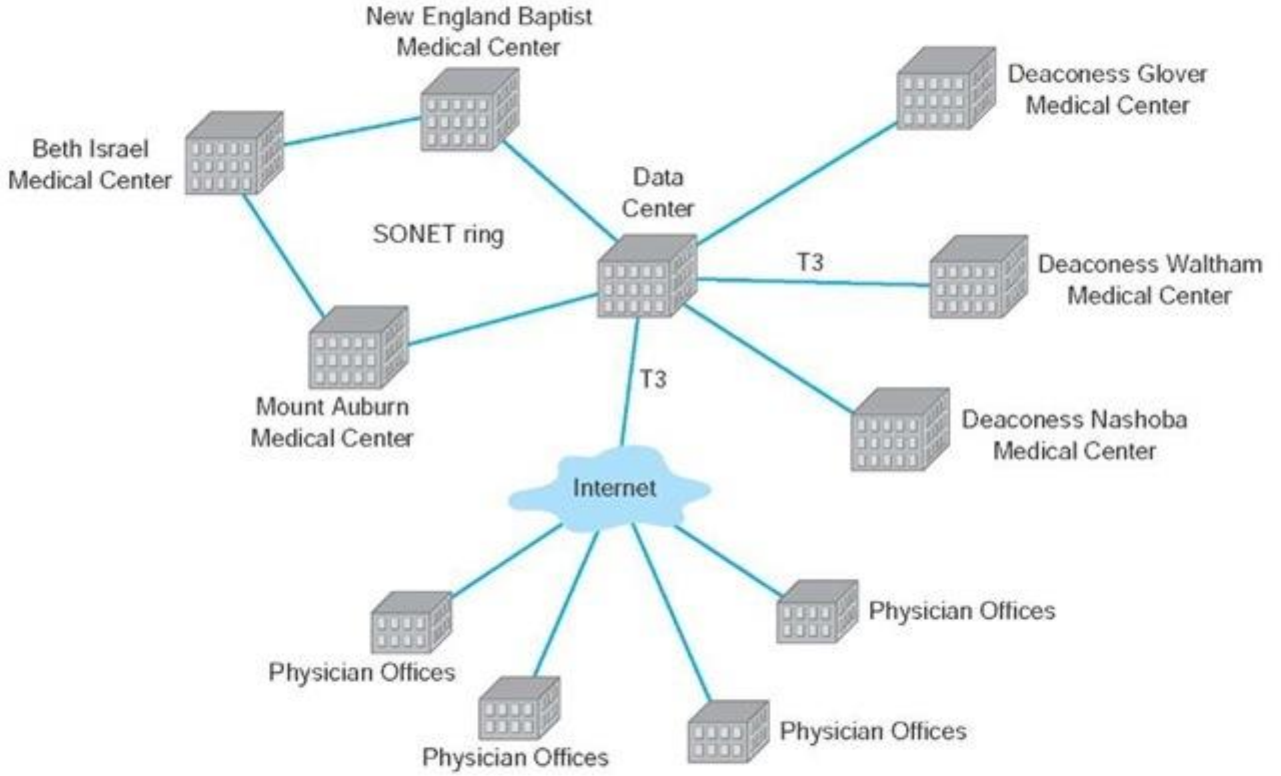


2. Serial Transmission.
   In telecommunication and data **transmission**, **serial communication** is the process of sending data one bit at a time, sequentially, over a **communication** channel or computer bus. This is in contrast to parallel **communication**, where several bits are sent as a whole, on a link with several parallel channels



1	**Attempt *any three* of the following:**	**15**
a	Differentiate between Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM). DM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing) are two methods of multiplexing multiple signals into a single carrier. Multiplexing is the process of combining multiple signals into one, in such a manner that each individual signal can be retrieved at the destination. Since multiple signals are occupying the channel, they need to share the resource in some manner. The primary difference between FDM and TDM is how they divide the channel. FDM divides the channel into two or more frequency ranges that do not overlap, while TDM divides and allocates certain time periods to each channel in an alternating manner. Due to this fact, we can say that for TDM, each signal uses all of the bandwidth some of the time, while for FDM, each signal uses a small portion of the bandwidth all of the time. TDM provides greater flexibility and efficiency, by dynamically allocating more time periods to the signals that need more of the bandwidth, while reducing the time periods to those signals that do not need it. FDM lacks this type of flexibility, as it cannot dynamically change the width of the allocated frequency. The advantage of FDM over TDM is in latency. Latency is the time it takes for the data to reach its destination. As TDM allocates time periods, only one channel can transmit at a given time, and some data would often be delayed, though it's often only in milliseconds. Since channels in FDM can transmit at any time, their latencies would be much lower compared to TDM. FDM is often used in applications where latency is of utmost priority, such as those that require real-time information.	
b	Write a short note on Spread Spectrum Modulation with its Application. This is a technique in which a telecommunication signal is transmitted on a bandwidth considerably larger than the frequency content of the original information. Frequency hopping is a basic modulation technique used in spread spectrum signal transmission. Spread-spectrum telecommunications is a signal structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases the potential interference to other receivers while achieving privacy. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies. The receiver correlates the received signals to retrieve the original information signal. Originally there were two motivations: either to resist enemy efforts to jam the communications (anti-jam, or AJ), or to hide the fact that communication was even taking place, sometimes called low probability of intercept (LPI) or low probability of detection (LPD). Although spread spectrum methods have been used for many years to establish LPD communication, the fundamental limits of covert communications were only recently studied[1] and extended for many scenarios, such as artificial noise generation[2]. Frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), time-hopping spread spectrum (THSS), chirp spread spectrum (CSS), and combinations of these techniques are forms of spread spectrum	

c	Discuss the major classification of transmission media.  Transmission media Bounded or guided media Unbounded or unguided media Twisted pair cable Co-axial cable Fiberoptic cable Microwave or radio links Infrared Fig1: Classification of Transmission Media	
d	What is Packet Switching? Explain its methods of implementation. **Packet switching** is a method of grouping data transmitted over a digital network into *packets* which are composed of a header and a payload. Data in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software. Packet switching is the primary basis for data communications in computer networks worldwide. In the early 1960s, American computer scientist Paul Baran developed the concept *Distributed Adaptive Message Block Switching* with the goal to provide a fault-tolerant, efficient routing method for telecommunication messages as part of a research program at the RAND Corporation, funded by the US Department of Defense.[1] This concept contrasted and contradicted then-established principles of pre-allocation of network bandwidth, largely fortified by the development of telecommunications in the Bell System. The new concept found little resonance among network implementers until the independent work of British computer scientist Donald Davies at the National Physical Laboratory (United Kingdom) in 1965. Davies is credited with coining the modern name *packet switching* and inspiring numerous packet switching networks in the decade following, including the incorporation of the concept in the early ARPANET in the United States.	


New England Baptist Medical Center
Deaconess Glover Medical Center
Beth Israel Medical Center
Data Center
SONET ring
T3
Deaconess Waltham Medical Center
T3
Mount Auburn Medical Center
Deaconess Nashoba Medical Center
Internet
Physician Offices
Physician Offices
Physician Offices
Physician Offices

e Define Error under scope of Networking and Explain its types.

Types of Errors Single Bit **Error** : Only one bit of **data** unit is changed from either 0 to 1 or 1 to 0. Burst **Error** : Two or more bits in the **data** is changed. Packet **error** are errors like Packet loose/ Duplication/ Re-ordering. **Error** Detection Process of detecting errors between sender and receiver.

f. Explain the following terms

1. Forward Error Correction (FEC).

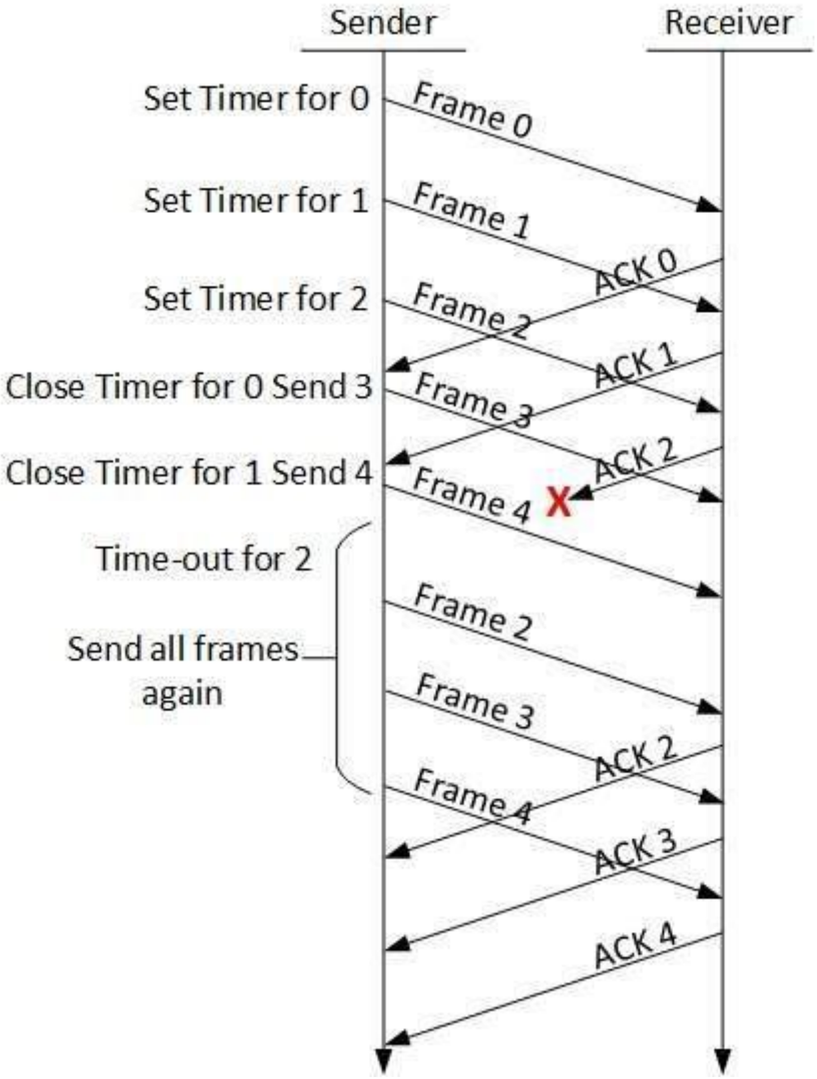
   Forward error correction (FEC) is a method of obtaining error control in data transmission in which the source (transmitter) sends redundant data and the destination (receiver) recognizes only the portion of the data that contains no apparent errors. Because FEC does not require handshaking between the source and the destination, it can be used for broadcasting of data to many destinations simultaneously from a single source.

2. Automatic request for Retransmission (ARQ).

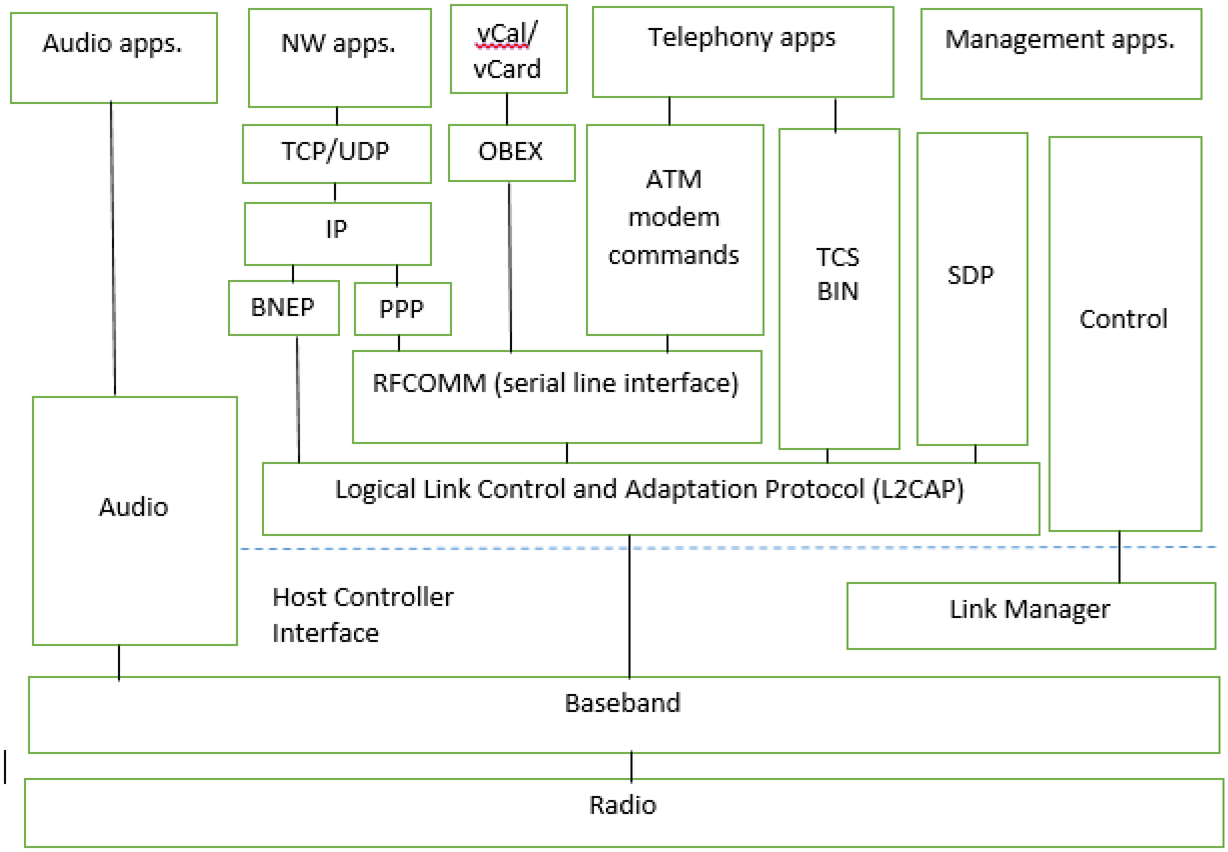
Automatic Repeat reQuest (**ARQ**), also known as **Automatic Repeat Query**, is an error-control method for data transmission that uses acknowledgements (messages sent by the receiver indicating that it has correctly received a data frame or packet) and timeouts (specified periods of time allowed to elapse before an acknowledgment is to be received) to achieve reliable data transmission over an unreliable service. If the sender does not receive an acknowledgment before the timeout, it usually re-transmits the frame/packet until the sender receives an acknowledgment or exceeds a predefined number of re-transmissions .

The types of ARQ protocols include Stop-and-wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ / Selective Reject.

	All three protocols usually use some form of sliding window protocol to tell the transmitter to determine which (if any) packets need to be retransmitted.	
2	**Attempt *any three* of the following:**	**15**
a	Explain ALOHA system with its two versions. Aloha, also called the *Aloha method*, refers toa simple communications scheme in which each source (transmitter) in a network sends data wheneverthere is a frame to send. If the framesuccessfully reaches the destination (receiver), the next frame is sent. If theframe fails to be received at the destination, it is sent again. This protocol wasoriginally developed at the University of Hawaii for use with satellite communication systems in the Pacific. n a wireless broadcast systemor a half-duplex two-way link, Aloha works perfectly. But as networks become morecomplex, for example in an Ethernet systeminvolving multiple sources and destinations that share a common data path,trouble occurs because data frames collide (conflict). The heavier thecommunications volume, the worse the collision problems become. The result isdegradation of system efficiency, because when two frames collide, the data contained inboth frames is lost. To minimize the number of collisions, thereby optimizing networkefficiency and increasing the number of subscribers that can use a given network, a schemecalled *slotted Aloha* was developed. This system employs signals called beacons that are sentat precise intervals and tell each source when the channel is clear to send aframe. Further improvement can be realized by a more sophisticated protocol called Carrier Sense Multiple Access withCollision Detection (CSMA/CD).	
b	Discuss**GO BACK N ARQ** in detail. Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.	

	 Sender Receiver Set Timer for 0 Frame 0 Set Timer for 1 Frame 1 ACK 0 Set Timer for 2 Frame 2 ACK 1 Close Timer for 0 Send 3 Frame 3 ACK 2 Close Timer for 1 Send 4 Frame 4 X Time-out for 2 Frame 2 Send all frames again Frame 3 ACK 2 Frame 4 ACK 3 ACK 4 The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number. When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK	
c		

Explain Bluetooth Layered Architecture.



- AT: Attention sequence
- OBEX: Object Exchange
- TCS BIN: Telephony control protocol specification – binary
- BNEP: Bluetooth network encapsulation protocol
- SDP: Service discovery protocol
- RFCOMM: Radio frequency comm.

Radio Layer

- Radio layer defined the carrier frequencies and output power
- Bluetooth uses 2.4 GHZ license free band.

• Frequency hopping and TDD (time division duplex) is used for transmission with fast hopping rate of 1600 hops/s.

• It uses 79 hop carriers equally spaced with 1 MHz.

• Gaussian FSK used for modulation.

Baseband Layer

• Baseband layer performs frequency hopping to avoid interference and to access the medium.

• Defines physical links and many packet formats.

• It controls:

o Device Addressing

o Channel control through paging and inquiry methods

o Power saving operations

o Flow control and synchronization among Bluetooth devices.

Link Manager Protocol (LMP)

• The Link Manager protocol manages various aspects of the radio link between master and slave.

• The following functions are covered by LMP:

o Authentication, pairing and encryption

o Synchronization

o Capability negotiation

o QoS negotiation

o Power control

o Link Supervision

o State and transmission mode change

Logical Link Control and Adaptation Layer Protocol (L2CAP)

• L2CAP is layered over the Baseband Protocol and resides in the data link layer.

• L2CAP provides:

o Connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability.

o Segmentation and reassembly operation.

o Group abstractions.

• L2CAP provides three different types of logical channels that are transported via ACL link between master and slave, these are:

o Connectionless used for broadcast

o Connection-oriented for data transfer with QoS flow specification.

o Signaling used to exchange signaling messages between L2CAP entities.

Host Controller Interface (HCI)

• The HCI provides a command interface to the baseband controller and link manager.

• It provides access to hardware status and control registers.

• Essentially this interface provides a uniform method of accessing the Bluetooth baseband capabilities.

• The HCI exists across 3 sections, The Host, Transport Layer, and Host Controller. Each of the sections has a different role to play in HCI system.

• HCI defines the set of functions of a Bluetooth module that are accessible to the host and its application.

• HCI can be seen as a software/hardware boundary.

RFCOMM

• The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol.

• It is a cable replacement protocol that provides a serial line interface to all the applications.

• The protocol is based on the ETSI standard TS 07.10.

• It supports multiple serial ports over a single physical channel.

Service Discovery Protocol (SDP)

- The service discovery protocol helps the applications to discover which services are available and to determine the characteristics of those available services.

- SDP defines only the discovery of services, not about their usage.

- New service is discovered as follows:

  - Client sends a request to search for an interested service.

  - Then the server responds to the client with the list of available services that match to the client’s criteria.

  - The client uses the list to retrieve additional service attribute for the service of interest.

Profiles

- Profiles are specifications which describe how Bluetooth should be used in a specific application and thus ensures that all devices from different manufacturers can seamlessly work with one another.

- There are about a dozen profiles:

Generic Access, Serial Port, Dial up Networking, FAX, Headset, LAN, Access Point, Generic Object Exchange (OBEX), File Transfer, Object Push, Synchronization, Cordless Telephony, and Intercom.

- The profile concept is used to decrease the risk of interoperability problems between different manufacturers’ products.

Telephony Control Protocol Specification Binary (TCS-BIN)

- To define call control signaling for the establishment of voice and data calls between Bluetooth devices TCS-BIN describes a binary, packet-based, bit-oriented protocol

d Differentiate between Satellite Communication and Optical Communication.

1- Optical Fiber is quicker but Satellite is slow in communication.
2- Optical Fiber higher bandwidth but Satellite Lower Bandwidth.
3- In case of any fault we can easily repair Fiber Optics but Satellite can not be repair.
4- Fiber Optics initial Cast is low but Satellite is very High.
5- Many People want to communication during jogging, driving, sailing and flying these all possible in Satellite Communication But Fiber Optics not use for them.
6- Satellite cost low for long range communication, while optical fiber is very costly for long range communication.
7-Minimum three or four satellite can cover the whole world, Fiber optics can also do that but cost considerations are to be worked out (possible with solition communications only).

8-Satellite provide global mobile communication, for example, GPS. For optical fiber, there is no possibility of mobile terminals since cable is to be laid physically.
9-Satellite is more suitable to the rough terrain and remote areas where fiber optics and microwave can't be used.
10-Satellite suffers from propagation delay. For optical fiber, no such delays.

e Explain the following Connecting devices in networking

1. Bridge

   A network bridge joins two otherwise separate computer networks to enable communication between them and allow them to work as a single network. Bridges are used with local area networks (LANs) to extend their reach to cover larger physical areas than the LAN can otherwise reach. Bridges are similar to—but more intelligent than—simple repeaters, which also extend signal range.

2. Gateway

A gateway is a node (router) in a computer network, a key *stopping point* for data on its way to or from other networks. Thanks to gateways, we are able to communicate and send data back and forth. The Internet wouldn't be any use to us without gateways (as well as a lot of other hardware and software).

In a workplace, the gateway is the computer that routes traffic from a workstation to the outside network that is serving up the Web pages. For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet.

f. Explain CSMA with Collision Detection.

Carrier-sense multiple access with collision detection (**CSMA/CD**) is a media access control method used most notably in early Ethernet technology for local area networking. It uses a carrier-sensing scheme in which a transmitting station detects collisions by sensing transmissions from other stations while transmitting a frame. When this collision condition is detected, the station stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.[1]

CSMA/CD is a modification of pure carrier-sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

3 Attempt *any three* of the following: 15

a Explain the terms

1. Connection Oriented Network Services.

Connection-oriented communication is a network communication mode in telecommunications and computer networking, where a communication session or a semi-permanent connection is established before any useful data can be transferred, and where a stream of data is delivered in the same order as it was sent. The alternative to connection-oriented transmission is connectionless communication, for example the datagram mode communication used by the IP and UDP protocols, where data may be delivered out of order, since different packets are routed independently, and may be delivered over different paths.

Connection-oriented communication may be a circuit switched connection, or a packet-mode virtual circuit connection. In the latter case, it may use either a transport layer virtual circuit protocol such as the TCP protocol, allowing data to be delivered in order although the lower layer switching is connectionless, or it may be a data link layer or network layer switching mode, where all data packets belonging to the same traffic stream are delivered over the same path, and traffic flows are identified by some *connection identifier* rather than by complete routing information, allowing fast hardware based switching.

2. Connectionless Network Services.

Connectionless communication, often referred to as **CL-mode** communication,[1] is a data transmission method used in packet switching networks in which each data unit is individually addressed and routed based on information carried in each unit, rather than in the setup information of a prearranged, fixed data channel as in connection-oriented communication.

Under connectionless communication between two network end points, a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. Some protocols allow for error correction by requested retransmission. Internet Protocol (IP) and User Datagram Protocol (UDP) are connectionless protocols.

A packet transmitted in a connectionless mode is frequently called a datagram.

Connectionless protocols are usually described as stateless protocols because the end points have no protocol-defined way to remember where they are in a "conversation" of message exchanges.

b Write a short note on Static Algorithm explain any two.

Static routing manually sets up optimal paths between the source and destination computers.

Routers that use static routing do not have any controlling mechanism if they come across any faults in the routing paths. These routers do not sense faulty computers encountered while finding the path between two computers or routers in a network.

Static routing is suitable for very small networks; they cannot be used in large networks.

Static routing is the simplest way of routing data packets from a source to a destination in a network

1. Shortest Path Routing
2.

c What is fragmentation? Explain various strategies of the same.

IP fragmentation is an Internet Protocol (**IP**) process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size. The fragments are reassembled by the receiving host.

Internal fragmentation

Due to the rules governing memory allocation, more computer memory is sometimes allocated than is needed. For example, memory can only be provided to programs in chunks divisible by 4, 8 or 16, and as a result if a program requests perhaps 23 bytes, it will actually get a chunk of 32 bytes. When this happens, the excess memory goes to waste. In this scenario, the unusable memory is contained within an allocated region. This arrangement, termed fixed partitions, suffers from inefficient memory use - any process, no matter how small, occupies an entire partition. This waste is called **internal fragmentation**.[1][2]

Unlike other types of fragmentation, internal fragmentation is difficult to reclaim; usually the best way to remove it is with a design change. For example, in dynamic memory allocation, memory pools drastically cut internal fragmentation by spreading the space overhead over a larger number of objects.

External fragmentation

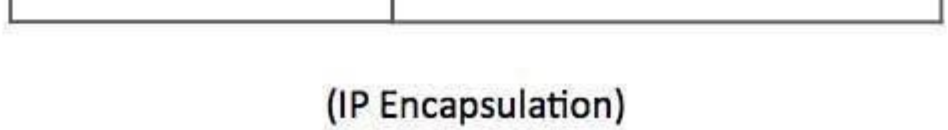
External fragmentation arises when free memory is separated into small blocks and is interspersed by allocated memory. It is a weakness of certain storage allocation algorithms, when they fail to order memory used by programs efficiently. The result is that, although free storage is available, it is effectively unusable because it is divided into pieces that are too small individually to satisfy the demands of the application. The term "external" refers to the fact that the unusable storage is outside the allocated regions.

For example, consider a situation wherein a program allocates 3 continuous blocks of memory and then frees the middle block. The memory allocator can use this free block of memory for future allocations. However, it cannot use this block if the memory to be allocated is larger in size than this free block.

External fragmentation also occurs in file systems as many files of different sizes are created, change size, and are deleted. The effect is even worse if a file which is divided into many small pieces is deleted, because this leaves similarly small regions of free spaces.

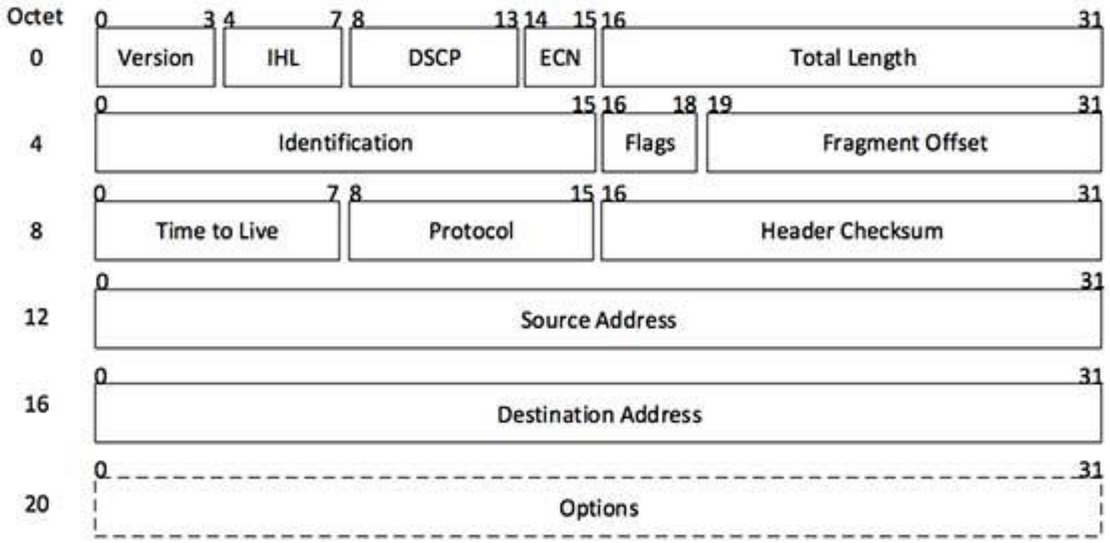
d Draw and Explain IPv4 header structure.

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

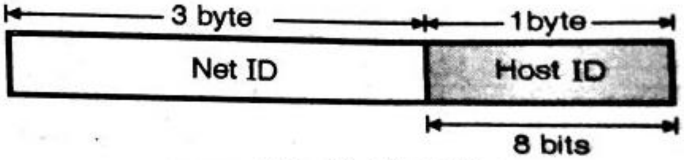
IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).
- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- **Flags:** As required by the network resources, if IP Packet is too large to handle, these ‘flags’ tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to ‘0’.
- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address:** 32-bit address of the Sender (or source) of the packet.
- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

e For a given class ‘C’ network 195.188.65.0 design equal subnets in a such a way that each subnet has atleast 60 nodes.

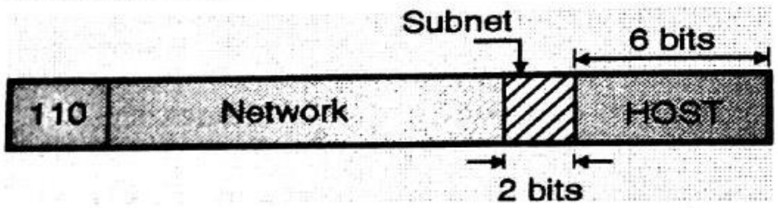
soln. :

- Fig. P. 14.6.5(a) shows the structure of a class C address in which 3-bytes are reserved for net ID and 1-byte for host ID.



(G-558) **Fig. P. 14.6.5(a)**

- We are expected to design equal subnets such that each subnet has atleast 60 nodes (i.e. 60 users).
- In order to identify at least 60 users we need 6-bits in the host ID.
- The remaining 2-bits are assigned for subnetting as shown in Fig. P. 14.6.5(b).



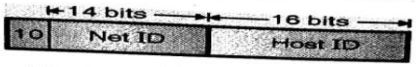
(G-559) **Fig. P. 14.6.5(b)**

- **This shows that there will be four equal subnets each one having at least 60 nodes.**

f. A class ‘B’ network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per sub networks?

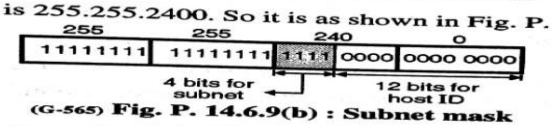
soln. :

The structure of class B address is as shown in Fig. P. 14.6.9(a).



(G-564) **Fig. P. 14.6.9(a) : Class B address**

The given subnet mask is 255.255.2400. So it is as shown in Fig. P. 14.6.9(b)



(G-565) **Fig. P. 14.6.9(b) : Subnet mask**

Thus there are 4 extra 1s as shown in Fig. P. 14.6.9(b). So there will be 16 subnets and each subnet can have $2^{12} = 4096$ hosts.

4 Attempt *any three* of the following: **15**

a Write a short note on TCP.

TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet. TCP is defined by the Internet Engineering Task Force (IETF) in the Request for Comment (RFC) standards document number 793.

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and—because it is meant to provide error-free data transmission—handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. In the Open Systems Interconnection (OSI) communication model, TCP covers parts of Layer 4, the Transport Layer, and parts of Layer 5, the Session Layer.

For example, when a Web server sends an HTML file to a client, it uses the HTTP protocol to do so. The HTTP program layer asks the TCP layer to set up the connection and send the file. The TCP stack divides the file into packets, numbers them and then forwards them individually to the IP layer for delivery. Although each packet in the transmission will have the same source and destination IP addresses, packets may be sent along multiple routes. The TCP program layer in the client computer waits until all of the packets have arrived, then acknowledges those it receives and asks for the retransmission on any it does not (based on missing packet numbers), then assembles them into a file and delivers the file to the receiving application.

b Explain Addressing Issues of transport Protocol.

- **Induced traffic**: Unlike wired networks, ad hoc wireless networks utilize multi-hop radio relaying. A link-level transmission affects the neighbor nodes of both the sender and receiver of the link. In a path having multiple links, transmission at a particular link affects one upstream link and one downstream link. This traffic at any given link (or path) due to the traffic through neighboring links (or paths) is referred to as induced traffic. This is due to the broadcast nature of the channel and the location-dependent contention on the channel. This induced traffic affects the throughput achieved by the transport layer protocol.
- **Induced throughput unfairness**: This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layers such as the network and *MAC* layers. For example, an ad hoc wireless network that uses *IEEE* 802.11 *DCF* as the *MAC* protocol may experience throughput unfairness at the transport layer as well. A transport layer protocol should consider these in order to provide a fair share of throughput across contending flows.
- **Separation of congestion control, reliability, and flow control**: **A** transport layer protocol can provide better performance if end-to-end reliability, flow control, and congestion control are handled separately. Reliability and flow control are end-to-end activities, whereas congestion can at times be a local activity. The transport layer flow can experience congestion with just one intermediate link under congestion. Hence, in networks such as ad hoc wireless networks, the performance of the transport layer may be improved if these are separately handled. While separating these, the most important objective to be considered is the minimization of the additional control overhead generated by them.
- **Power and bandwidth constraints**: Nodes in ad hoc wireless networks face resource constraints including the two most important resources: (i) power source and (ii) bandwidth. The performance of a transport layer protocol is significantly affected by these constraints.
- **Misinterpretation of congestion**: Traditional mechanisms of detecting congestion in networks, such as packet loss and retransmission timeout, are not suitable for detecting the network congestion in ad hoc

wireless networks. This is because the high error rates of wireless channel, location-dependent contention, hidden terminal problem, packet collisions in the network, path breaks due to the mobility of nodes, and node failure due to a drained battery can also lead to packet loss in ad hoc wireless networks. Hence, interpretation of network congestion as used in traditional networks is not appropriate in ad hoc wireless networks.

- **Completely decoupled transport layer**: Another challenge faced by a transport layer protocol is the interaction with the lower layers. Wired network transport layer protocols are almost completely decoupled from the lower layers. In ad hoc wireless networks, the cross-layer interaction between the transport layer and lower layers such as the network layer and the *MAC* layer is important for the transport layer to adapt to the changing network environment.
- **Dynamic topology**: Some of the deployment scenarios of ad hoc wireless networks experience rapidly changing network topology due to the mobility of nodes. This can lead to frequent path breaks, partitioning and remerging of networks, and high delay in reestablishment of paths. Hence, the performance of a transport layer protocol is significantly affected by the rapid changes in the network topology.

c What do you mean by Domain Name System? What is the use of the same?

The Domain Name System (DNS) translates Internet domain and host names to IP addresses and vice versa.

On the Internet, DNS automatically converts between the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites. Larger corporations also use DNS to manage their own company intranet. Home networks use DNS when accessing the Internet but do not use it for managing the names of home computers.

d Explain Simple Mail Transfer Protocol (SMTP).

SMTP (Simple Mail Transfer Protocol) is a TCP/IPprotocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, sendmail is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

e Write a short note on following

1. TELNET

   Telnet is a user command and an underlying TCP/IPprotocol 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.
2. FTP

The **File Transfer Protocol** (**FTP**) is the standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1] 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; it is technologically different.

The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems.[2][3] Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as web page editors.

f. Differentiate between TCP and UDP.

TCP	**UDP**	
Acronym for	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Use by other protocols	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because error recovery is not attempted. It is a "best effort" protocol.
Reliability	There is absolute guarantee that the data transferred remains intact	There is no guarantee that the messages or packets sent would reach

	and arrives in the same order in which it was sent.	at all.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.
Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control
Error Checking	TCP does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination.	UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.
Fields	1. Sequence Number, 2. AcK number, 3. Data offset, 4. Reserved, 5. Control bit, 6. Window, 7. Urgent Pointer 8. Options, 9. Padding, 10. Check Sum, 11. Source port, 12. Destination port	1. Length, 2. Source port, 3. Destination port, 4. Check Sum
Acknowledgement	Acknowledgement segments	No Acknowledgment
Handshake	SYN, SYN-ACK, ACK	No handshake (connectionless protocol)