S.Y. B.Sc. (IT) : Sem. III

Computer Networks

Time : 2½ Hrs.] Prelim Question Paper Solution **[Marks : 75**

Q.1 Attempt the following (any THREE) [15]

Q.1(a) What do you mean by Transmission line impairments? Explain in detail. [5]

Ans.: The imperfection happening to the signal while transmitting through the medium are called transmission impairments.

Types :

➢ **Attenuation :**

- It means loss of energy
- When a signal, simple or composite while travelling through a medium loses some of its energy in overcoming the resistance of the medium.
- To overcome this, amplifiers are used.
- Decibel is negative if a signal is attenuated and positive if amplified.

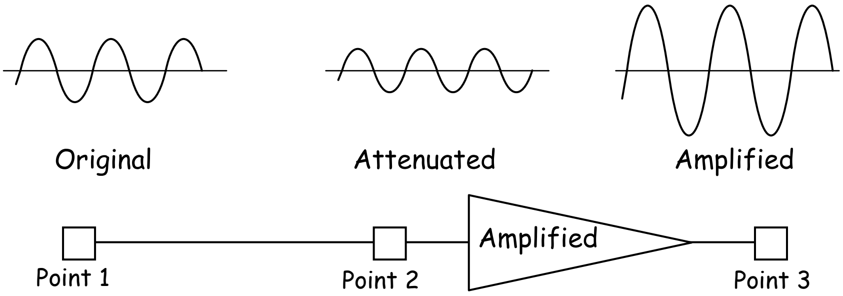


Fig. Attenuation

➢ **Distortion :**

- Means that the signal changes its form or shape.
- It occurs in a composite signal made of different frequencies.
- In this signal components at the receiver have phases different from what they had at the sender.

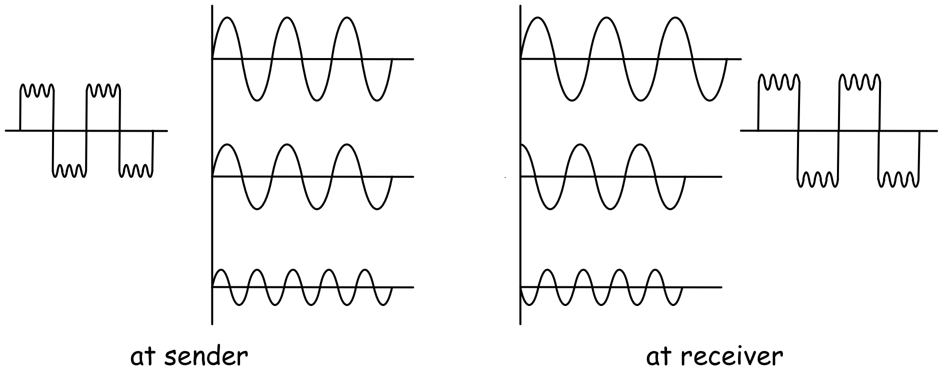


Fig.: Distortion

➢ **Noise :**

- Several types of noise, such as thermal noise, induced noise, crosstalk and impulse noise may corrupt the signal.
  example, Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.
- Noise is calculated as signal–to–noise ratio

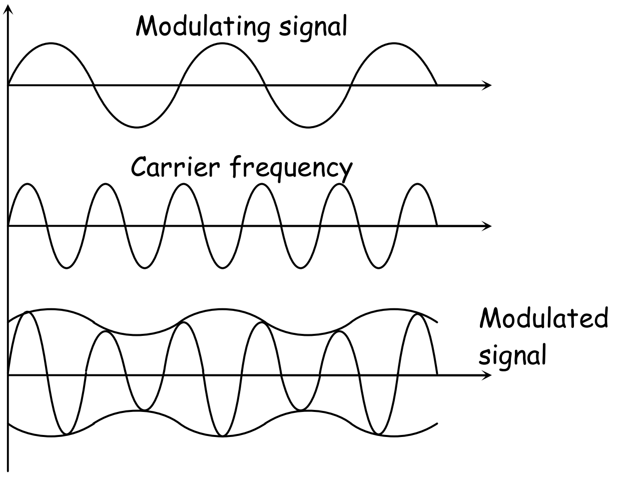
$$\text{SNR} = \frac{\text{wanted (Signal)}}{\text{not wanted (Singal)}} = \frac{\text{average signal power}}{\text{average noise power}}$$

Q.1(b) Define Modulation. Write a short note on Amplitude Modulation. [5]

Ans.: It is the technique by which the signal which is low–pass can be presented to transfer on bandpass channel.

Amplified Modulation :

- There the carrier signal is modulated so that its amplitude varies with the changing amplitude of the modulating signal.
- Then frequency and phase of the carrier remain the same, only the amplitude changes to follow variations in the information.
- Amplitude modulation is implemented by using a simple multiplier because the amplified of the carrier.
- Signal needs to be changed according to the amplitude of the modulating signal.

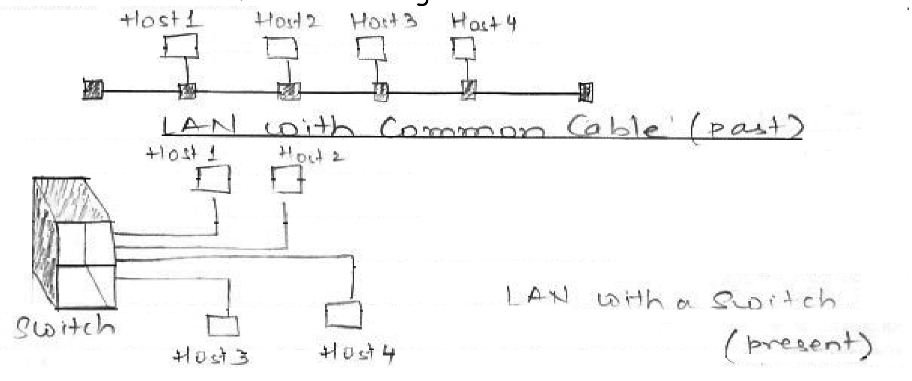


- Modulation creates a bandwidth that is twice the bandwidth of the modulating signal and covers a range centered on the carrier frequency.

Q.1(c) State and explain various types of networks. What are the different ways to access the Internet? [5]

Ans.: **(i) Local Area Network (LAN)**

- Usually privately owned and connects some hosts in a single office, building or campus.
- Each host in a LAN has an identifier, and address that uniquely defines the host in the LAN.
- A packet sent by a host to another host carries both the source's host and the destination hosts addresses.
- Most LANs use a smart connecting switch.

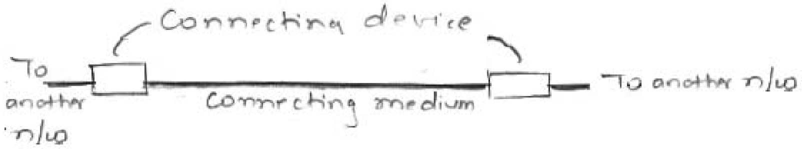


(ii) Wide Area Network (WAN)

- It has wider geographical span, spanning a town, state, country, world.
- Interconnects devices such as switcher, routers or modems.
- Run and created by communication companies and leased by an organization that uses it.

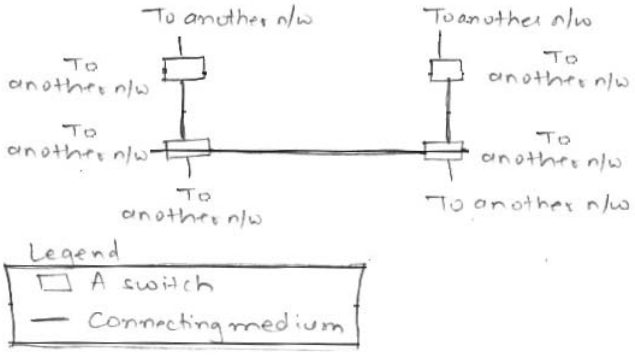
Point to point WAN

- Connects two communicating devices through a transmission media (cable or air)



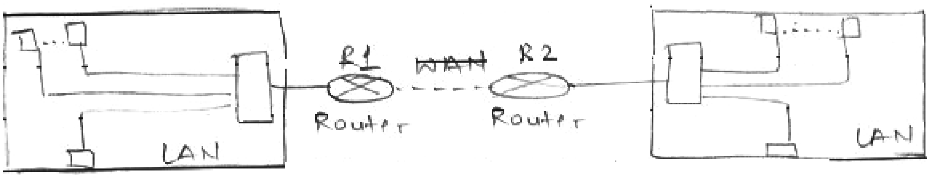
Switch WAN

- A network with more than two ends.
- A combination of several point to point WANs that are connected by switches.



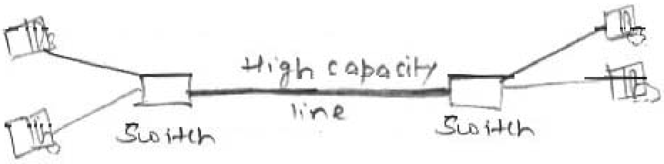
Internetwork

- When two or more networks are connected.



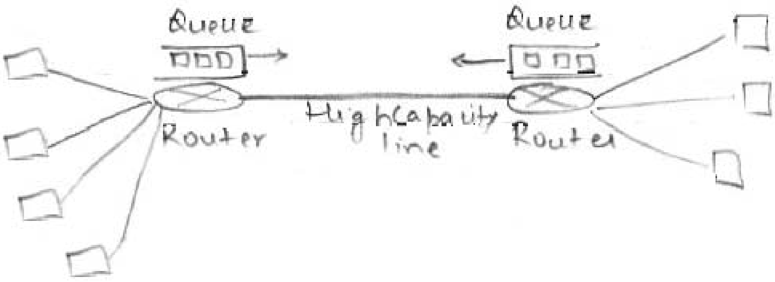
Circuit switched network

- A dedicated connection called a circuit is always available between the two end systems, the switch can only make it active or inactive.



Packet switched network

- Communication between the two ends is done in blocks of data called packets.



Different ways to access Internet

- Using Telephone Networks
  - Dial up service
    - Add to the telephone line a modern that converts data to voice.
    - Software installed dials ISP and imitates making a telephone connection.

- DSL Service
  - > Allows line to be used simultaneously for voice and data communication.
- Using Cable Network
  - Cable companies have upgraded their cable networks and connect to the Internet.
  - Provides higher speed connection.
- Using Wireless Networks
  - A household or small business can be connected to the Internet through a wireless LAN.
- Direct Connection to the Internet
  - A large organization can become a local ISP and be connected to the Internet.
  - Organisation leases a high speed WAN from a carrier provider and connects itself to a regional ISP.

Q.1(d) Define Data Communication. Explain its various components. **[5]**

Ans.: Data communication can be defined as exchange of data between a source and destination over some kind of transmission medium. This exchange of data has the following five components :

(a) Message : The information or data which is to be sent from sender to the receiver. A message can be in form of sound, text, number, pictures, video or combination of them.

(b) Sender : Sender is a device such as a host, video camera, telephone, workstation which sends the message over the medium.

(c) Medium : The message originating from the sender needs a path over which it can travel to the receiver, such a path is called as the medium. E.g. Co–axial cable, twisted pair wire.

(d) Receiver : It is the device, which receives the message and reproduces it. A receiver can be in the form of a workstation.

(e) Protocol : Protocol is defined as the set of rules agreed by the sender and the receiver. Protocols govern the exchange of data in true sense.

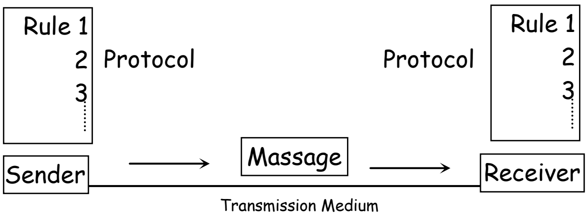
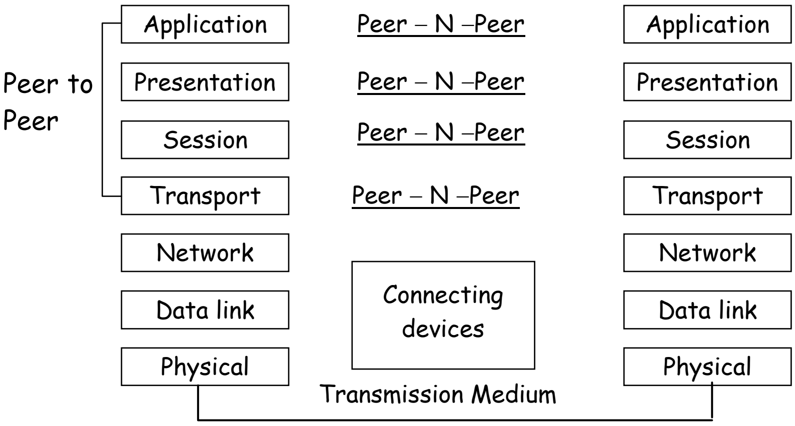


Fig. : Five Components of data communication.

Q.1(e) List and explain the functions of ISO's OSI Model Layers. **[5]**

Ans.: **ISO's OSI Model :**

The seven layers of OSI reference model are :



Physical Layer :

- To activate, maintain and deactivate the physical connection
- To convert the digital data bits into electrical signals.

- To decide whether the transmission is simplex half duplex or full duplex.
- To define voltages and data rates needed for transmission.

Data Link Layer :

- Synchronization and error control
- To enable error detection
- To assemble outgoing messages into frames.

Network layer :

- To route the signals through various channel to the other end.
- To act as the network controller by deciding which route data should be taken.
- To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher levels.

Transport layer :

- It decides if the data transmission should take place on parallel paths or single path.
- It does the functions such as multiplexing, splitting or segmenting on the data.
- Transport layer guarantees transmission of data from one end to the other.

Session layer :

- This layer manages and synchronizes conversation between two different applications. This is the level at which the user will establish system to system connection.
- It controls logging on and off, user identification, billing and session management.

Presentation layer :

- The presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.
- The form and syntax of the two communicating systems can be different.

Application layer :

- It provides different services such as manipulation of information in various ways, retransferring the files of information, distributing the results.
- The functions such as LOGIN or PASSWORD checking are also performed by the application layer.

Q.1(f) Explain the following terms of Data Transmission **[5]**
(i) Parallel Transmission **(ii) Serial Transmission**

Ans.: (i) Parallel Transmission :

- In this transmission groups of n bits are transferred from the sender to the receiver at the given clock pulse instead of 1 bit at the time.
- **Implementation :** Use n wires to send n bits at one time. So each bit has its own wire and all n bits of one group are transmitted with each clock tick from one device to another.
- **Advantage :** It increases the transfer speed by a factor of n over serial transmission.
- **Disadvantage :** Requires n communication lines, as this is expensive, parallel transmission is usually limited to short distances.

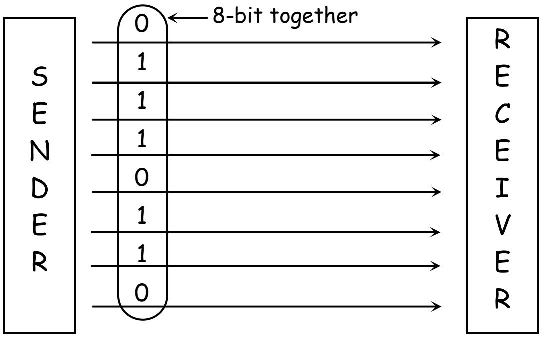


Fig.: Parallel Transmission

(ii) Serial Transmission :

- There one bit follows another, so we need only one communication channel than n to transmit data between two communicating devices.
- **Advantage** : One communication channel reduces the cost of transmission over parallel by roughly a factor of n.
- Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line and between the line and the receiver.
- Serial transmission occurs in one of the three ways.
  - **(i) Asynchronous** :Asynchronous at the byte level but the bits are still synchronized ; their durations are the same.
  - **(ii) Synchronous** : We send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to groip the bits.
  - **(iii) Isochronous** : There the entire stream of bits must be synchronized. It guarantees that the data arrives at a fixed rate.

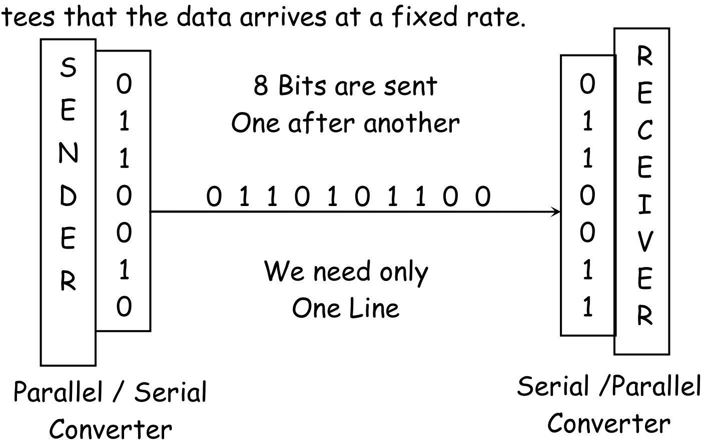


Fig.: Serial Transmission

Q.2 Attempt the following (any THREE) **[15]**

Q.2(a) Write a short note on Spread Spectrum Modulation (SSM) techniques along with its Application. **[5]**

Ans.: Applications of spread spectrum modulation :

1. To avoid the intentional interference.
2. To reject the unintentional interference from some other user.
3. To avoid the self-interference due to multipath propagation.
4. In low probability of intercept signals.
5. In obtaining the message privacy.

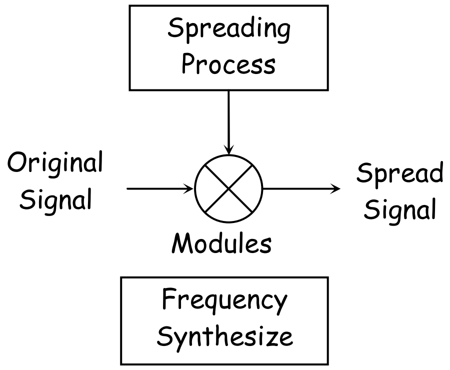
Spread Spectrum Modulation :

- In spread spectrum we combine signals from different sources to fit into a large bandwidth.
- It is designed to be used in wireless applications.
- In wireless applications, all stations use air as the medium for communication. Stations must be able to share this medium without interception by an eavesdropper and without being subject to jamming from a malicious intruder.
- To achieve these goals, spread spectrum techniques add redundancy; they spread the original spectrum needed for each station. If required bandwidth for each station in B, spread spectrum expands it to B_{ss}, such that B_{ss}, >> B.
- The expanded bandwidth allows the source to wrap its message in a protective envelope for a more secure transmission. An analogy is the sending of a delicate expensive gift.

Spread spectrum achieves its goals through two principles :

1) The bandwidth allocated to each station needs to be, by far large, than what is needed. This allows redundancy.

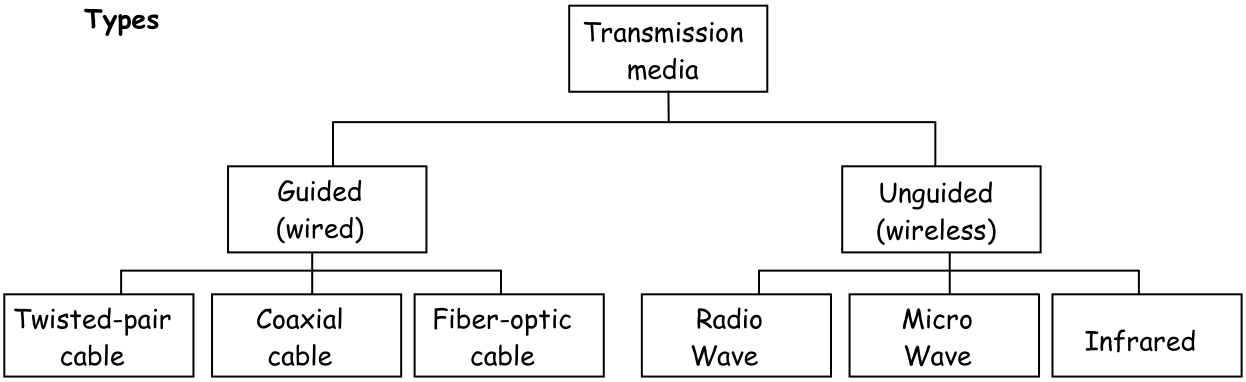
2) The expanding of the original bandwidth B to the bandwidth B_{ss} must be done by a process that is independent of the original signal. In other words, the spreading process occurs after the signal is created by the source.



Q.2(b) What are the different types of transmission media? Explain each type. [5]

Ans.: Transmission medium is anything that can carry information from a source to a destination.

Types



(i) Guided Media (Wired)

– Those that provide conduit from one device to another.

- Twisted pair cable
  – Consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
  – One wire carries signals to the receiver, other is used as ground reference.
  – Receiver uses the difference between the two.
- Co-axial cable
  – Categorized by their Radio Government (RG) ratings.
  – Carries signals of higher frequency ranges them those in twisted pair cable.
  – It has a central core conductor of solid or standed wire (usually copper) enclosed in an insulating sheath, which in turn is enlosed in an outer conductor of metal foil, braid or a combination of the two.
  – The outer metallic wrapping serves both as a shield against noise and as the second conductor which completes the circuit.
  – This outer conductor is also enclosed in an insulating sheath and the whole cable is protected by a plastic cover.
- Fiber-Optic cable
  – Made of glass or plastic and transmits signals in the form of light.
  – Use reflection to guide light through a channel.
  – Glass or plastic core is surrounded by a cladding of less dense glass or plastic.
  – Difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

(ii) Unguided media (Wireless)

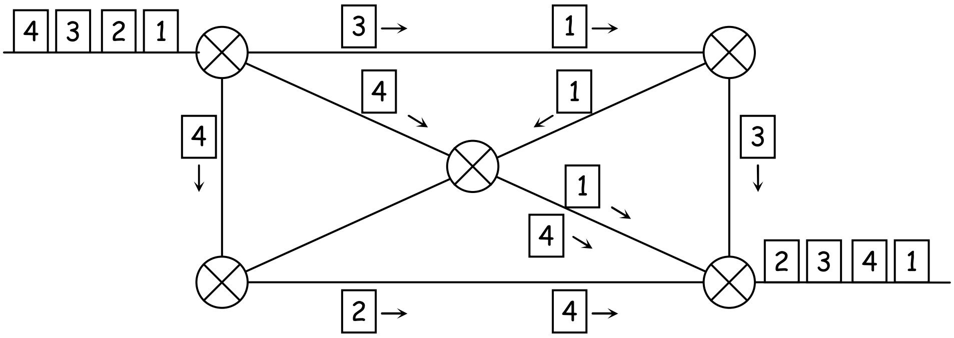
– Transport electromagnetic waves without using a physical conductor.

- Radio waves
  - Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are called radio waves.
  - Are omni directional.
  - In sky mode, can travel long distances.
  - Low and medium frequencies can penetrate walls.
  - Useful for multicasting.
- Microwaves
  - Electromagnetic waves ranging in frequencies between 1 and 300 GHz are called microwaves.
  - Are unidirectional.
  - Sending and receiving antennas have to be aligned.
  - Propagation is line-of-sight. Repeaters are often needed for long distance communication.
  - High frequency microwaves cannot penetrate walls.
  - High data rate is possible.
- Infrared
  - Waves with frequencies from 300 GHz to 400 THz (wavelength from 1 mm to 770 mm) can be used for short–range communication.
  - High frequencies can not penetrate walls.
  - Useless for long range communication.
  - Cannot be used outside a building.
  - Has excellent potential for data transmission.

Q.2(c) What is Packet Switching? Explain its methods of implementation. **[5]**

Ans.: Packet switching :

- In packet switching, messages are broken up into packets. Each packet has a header with source, destination and intermediate node address information.
- Each packet is treated independently of all others, though it's a multipacket transmission.
- Packets in this approach are referred as datagram :



Packet Switching

- The above datagram approach is used to deliver four packets from station A to Station X. The switches in a datagram network are referred to as routers. All four packets belong to the same message, but may travel different paths to reach their destination.
- This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all packets from A to X.
- Packets may be lost or dropped because of lack of resource allocation.
- It is also referred as connectionless network.
- There is not setup or teardown phase.
- The efficiency of datagram, network is better than that of circuit switched network as resources are allocated only when there are packets to be transferred.
- There may be delay product in packet switch as compared with virtual circuit network.

Q.2(d) Explain the following terms : [5]

(i) Forward Error Corrections (FEC)

(ii) Automatic request for Retransmission (ARQ)

Ans.: **(i) Forward Error Correction :**

- Retransmission of corrupted and last packets is not useful for real–time multimedia transmission because it creates an unacceptable delay in reproducing.
- So we need to correct the error or reproduce the packet immediately.
- This can be done by forward error correction.

- **Using hamming distance :** Here, to correct 10 bits in a packet, we need to have the minimum distance 21 bits which means a lot of redundant bits need to be sent with the data.
- **Using XOR :** If we divide a packet into N chunks, create the exclusive OR of all the chunks and send N + 1 chunks.
  If any chunk is lost or corrupted, it can be created at the receiver site. This will help to correct the data if only one out of four chunks is lost.
- **Chunk interleaving :** In this method some small chunks to be missing at the receiver.
  e.g. : If we divide each packet into 5 chunks we can then create data chunk by chunk but combine the chunk into packets vertically. In this case, each packet sent carries a chunk from several original packets.
- Hence, if the packet is lost, we miss only one chunk in each packet.
- Combining hamming distance and interleaving we create n–bit packets that can correct t–bit errors, then we interleave m rows and send the bits column by column.
- Compounding high and low resolution packets. Here we create a duplicate of each packet with a low resolution redundancy and combine the redundant version with the next packet.

(ii) Automatic Request for Retransmission (ARQ)

In this in case if error approached the data packets transmitted to the target network address are controlled continuously and when the error is discovered a service packet is sent to the transmitting computer containing the identification number of corrupted packet.

Since other packets are transmitted over communication channel after corrupted packet, until the error is detected, the problem with retransmission appears.

If the transmitting computer transmit again only the corrupted packet then there will be an inconsistent exceptional packet in sequence of packet sent to the receiver.

Q.2(e) List the different error correcting codes. Explain any two in detail with examples. [5]

Ans.: Four different error correcting codes.

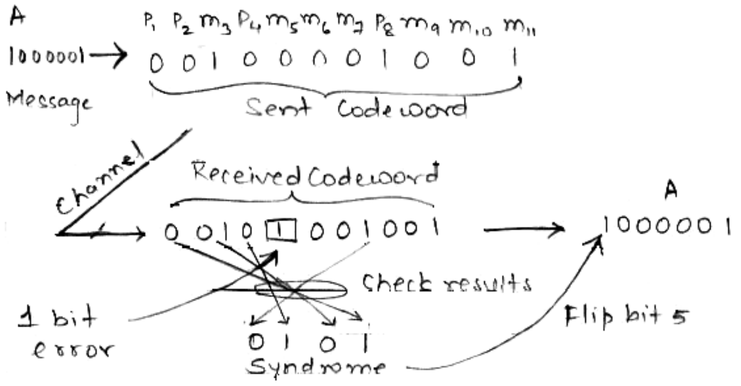
(i) Hamming codes
(ii) Binary convolutional codes
(iii) Reed-Solomon codes
(iv) Low Density Parity Check Codes

(i) Hamming codes

- Bits of codeword are numbered consecuvely, starting with bit 1 at the left end, bit 2 to its immediate right, and so on.
- Bits that are powers of 2(1, 2, 4, 8, 16 etc.) are check bits.
- The rest (3, 5, 6, 7, 9 etc.) are filled up with 'm' data bits.

Example

Below pattern is shown for an (11, 7) Hamming code with 7 data bits and 4 check bits. Each check bit forces the modulo 2 sum or parity of some collection of bits including itself to be even (or odd). A bit may be included in several check bit computations. To see which check bits the data bit in position 'k' contributes to, rewrite 'k' as a sum of lowers of 2. In the above example the check bits are computed for even parity, sums for a message that is ASCII letter 'A'.

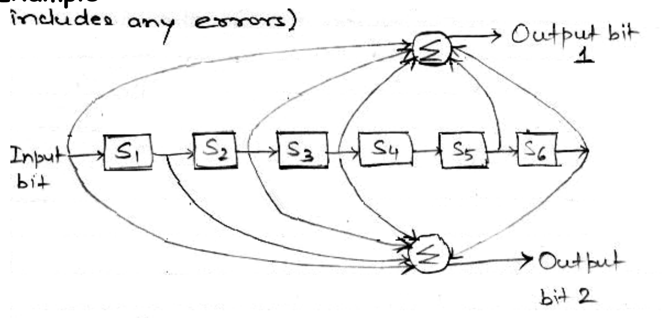


This construction gives a code with Hamming dist of 3, so it can correct single errors or detect double errors. When the code word arrives, receiver redoes the check bit computations including the values of the received check bits. These are called check results. It the check results are not all zero, an error has been detected. The set of check results forms the error syndrome that is used to pinpoint and correct the error. Flipping the incorrect bit (which might be a check or data bit) and discarding the check bits gives the correct message of ASCII letter 'A'.

(ii) Binary Convolutional Codes

- Not a block code.
- An encoder processes a sequence of input bits and generates a sequence of output bits.
- There is no natural message size or encoding boundary as in block code.
- Output depends on current and previous input bits i.e. the encoder has memory.
- No. of previous bits on which the output depends is called constraint length.
- Convolutional codes are specified in terms of their rate and constraint length.
- This code is decoded by finding the sequence of input bits that is most likely to have produced the observed sequence of output bits (which includes any errors).

Example



NASA Binary Convolutional Code used in 802.11

- The above code is known as the NASA convolutional code of r = ½ and k = 7.
- Each input bit on the left hand side produces two output bits on the right hand side that are XOR sums of the input and internal state.
- Since it deals with bits and performs linear operations, this is a binary linear convolutional code.
- Since 1 input bit produces 2 output bits, the code rate is ½.
- It is not systematic since none of the output bits is simply the input bit.
- The internal state is kept in six memory registers. Each time another bit is input the values in the registers are shifted to the right.

Example

If 111 is input and the initial state is all zeroes, internal state written left to right will become 100000, 110000, 111000 after the first, second, third bits have been input. The output will be 11, 10, then 01. It takes seven shifts to flush an input completely so that it doesn't affect output.

∴ the constraint length of this code is K = 7.

(iii) Reed-Solomon codes

- Linear block code.
- Often systematic.
- Operates on m-bit symbols.
- Based on the fact that every 'n' degree polynomial is uniquely determined by n + 1 points.

Example

A line having the form ax + b is determined by two points. Extra points on the same line are redundant, which is helpful for error correction. Suppose we have two data points that represent a line and we send those two data points plus two check points chosen to lie on the line. If one of the points is received in error, we can still recover the data points by fitting a line to the received points. Three of the points will lie on the line and one point, the one in error will not. By finding the line, we have corrected the error.

- Reed Solomon codes are actually defined as polynomials that operate over finite fields.
- For 'm' bit symbols, code words are $2^m - 1$ symbols long.
- Popular choice is to make m = 8 ∴ Code word is 255 bytes long. The (255, 233) code is widely used; it adds 32 redundant symbols to 233 data symbols. This can correct upto 16 symbol errors and an error burst of 128 bits can be corrected.

(iv) Low Density Parity Check Codes

- LDPC codes are linear block codes.
- In a LDPC code, each output bit is formed from only a fraction of the input bits.
- This leads to a matrix representation of the code that has a low density of 1s, hence the name for the code.
- The received code words are decoded with an approximation algorithm that iteratively improves on a best fit of the received data to a legal code word. This corrects errors.
- The codes are practical for large block sizes and have excellent error correction abilities that out perform many other codes.

Example

They are part of the standard for digital video broadcasting, 10 Gbps Ethernet, power-line networks, and the latest version of 802.11.

Q.2(f) What are the functions of data link layer? What is the relationship between packets and frames? Explain the different methods of framing. [5]

Ans.: The functions of data line layer are :

(i) Providing a well defined service interface to the network layer. (framing).

(ii) Dealing with transmission errors (Error control and Congestion Control)

(iii) Regulating the flow of data so that slow receivers are not swamped by fast senders (Flow control)

(i) Framing

- Data link layer at each node needs to encapsulate the datagram in a frame before sending it to the next node.

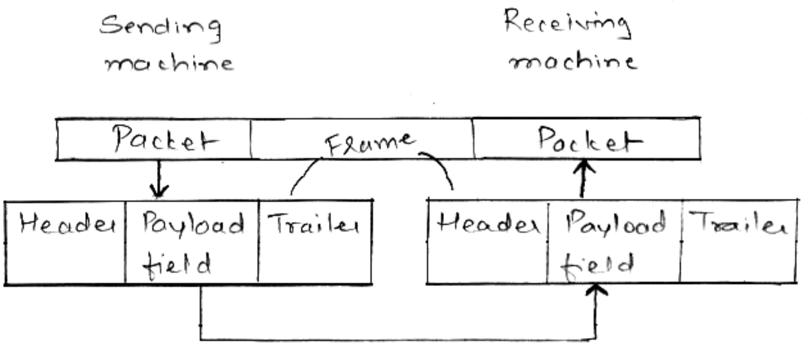
(ii) Error Control and Congestion Control

- Since electromagnetic signals are susceptible to error, a frame is susceptible to error.
- The error first needs to be detected, then it is either corrected at the receiver node or discarded and retransmitted by sending node.
- Although a link may be congested with frames which may result in frame loss, most data link layer protocol do not directly use congestion control.

(iii) Flow Control

- For controlling the control of frames sent/received, the first choice is to let the receiving data link layer to drop the frames it its buffer is full.
- The second choice is to let the receiving data link layer send a feedback to the sending data link layer to ask it to stop or slow down.

Relationship between packets and frames



Different methods of framing

(i) Byte Count

- Uses a field in the header to specify the number of bytes in the frame.
- When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the ends of the frame is.

(ii) Flag bytes with byte stuffing

- Gets around the problem of resynchronization after an error by having each frame start and end with special bytes.
- Often the same bye, called flag byte is used as both the starting and ending delimiter.
- Two consecutive flag bytes indicate the end of one frame and the start of the next.
- To distinguish the framing flag byte from one in the data, a special escape byte (ESC) is inserted just before each 'accidental' flag byte.
- The data link layer on the receiving end removes the escape bytes before giving the data to the network layer. This technique is called byte stuffing.
- If an escape byte occurs in the middle of the data, then that too is stuffed with an escape byte.
- At the receiver, the first escape byte is removed, leaving the data byte that follows it (which might be another escape byte or flag byte).

(iii) Flag bits with bit stuffing

- This method of delimiting the bit stream gets around the disadvantage of byte stuffing.
- Whenever the senders data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically dyestuffs/deletes the 0 bit.

Example

It uses data contain flag pattern 01111110 this flag is transmitted as 011111010 but stored in the receivers memory as 01111110.

- With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern.
- It receiver loses track of where it is, it just has to scan the input for flag sequences, since they can occur only at frame boundaries and never within the data.

(iv) Physical layer coding violations

- This method uses a shortcut from the physical layer.
- Encoding of bits as signals often includes redundancy to help the receiver. This redundancy means that some signals will not occur in regular data.
- We can use some reserved signals to indicate the start and end of frames.
- In effect coding violations are used to delimit frames.
- Biggest advantage is that because they are reserved signals, it is easy to find the start and end of frames and there is no need to stuff the data.

Q.3 Attempt the following (any THREE) [15]

Q.3(a) What is HDLC? What are the different types of frames in HDLC? Explain the different fields in HDLC frames. [5]

Ans.: HDLC

High-level Data Link Control is a bit oriented protocol for communication over point to point and multipoint links. It implements the stop and wait protocol.

Types of frames in HDLC

(i) Information frames (I-frames)

- Used to data-link user data and control information relating to user data (piggy backing).

(ii) Supervisory frames (S-frames)

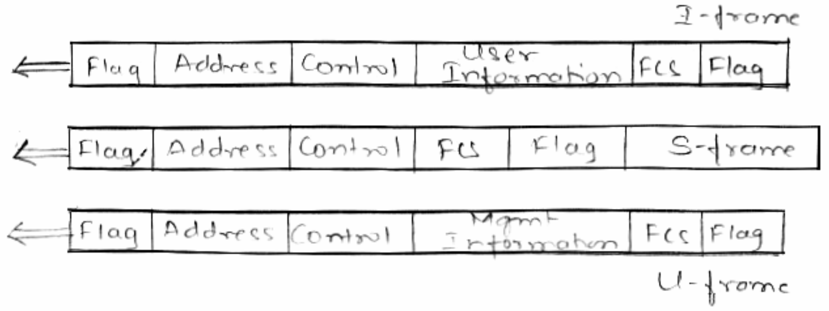
- Used only to transport control information.

(iii) Unnumbered frames (U-frames)

- Reserved for system management.
- Information carried is intended for managing the link itself.

Thus every type of frame serves as an envelope for the transmission of a different type of message.

Different fields in HDLC frames



(i) Flag field

- Contains synchronization pattern 011111110, which identifies both the beginning and the end of a frame.

(ii) Address field

- Contains address of the secondary station.
- If primary station created frame, it contains 'to' address.
- If secondary station creates frame, it contains 'from' address.
- Can be one byte or several bytes long.

(iii) Control field

- One or two bytes determines type of frame and defines its functionality.
- Used for flow and error control.

(iv) Information field

- Contains the users data from the network layer or management information.
- Length can vary from one network to another.

(v) FCS field

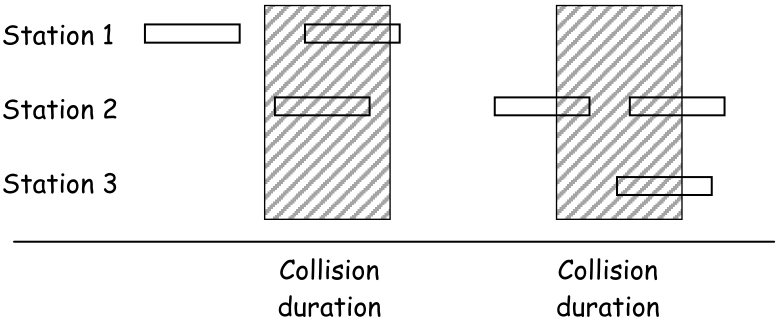
- Frame check sequence (FCS) is the HDLC error detection field.
- Can contain either a 2 or 4 byte CRC.

Q.3(b) Explain ALOHA system with its two versions. **[5]**

Ans.:
- ALOHA is a random access method, where no station is superior to another station and none is assigned control over medium.
- In this method the no of collisions are high as the medium is shared between the stations.

Types of ALOHA :

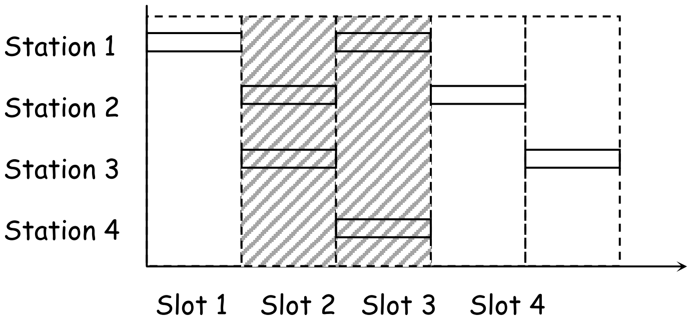
(i) Pure ALOHA



- In this each station sends a frame whenever it has a frame to send. Since there is only one channel to share, there is the possibility of collision between frames from different stations.
- The scheme relies on acknowledgements from the receiver. When station sends a frame, it expects the receiver to send an ACK, if ACK does not arrive after, a time out period, the station assumes that the frame is destroyed and resends the frame.
- As collision can occur after this, so this scheme says each station waits a random amount of time before resending it frame.

(ii) Slotted ALOHA :

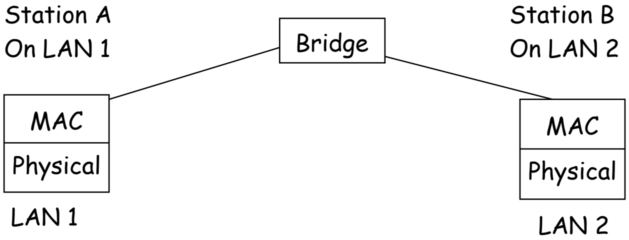
- Here we divide the time slot of T_{fr} seconds and force the station to send only of the beginning of the time slot.
- As the station is allowed to send only at the beginning of the synchronized time, slot, if a station misses this moment, it must wait until the beginning of the next Time slot.
- Through put is better than pure ALOHA by two times.



Q.3(c) Explain the following connecting devices in networking [5]
(i) Bridge (ii) Gateway

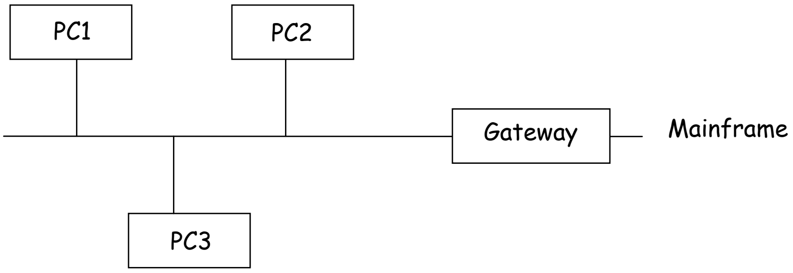
Ans.: (i) Bridge :

- A network bridge joins the otherwise separate computer networks to enable communication between them and allow them to work as a single network.. Bridges are used in local area network 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.
- Bridges work at data link layer and physical.
- **Working :**
  - checks the physical address of the destination when receives a frame, forward, the new copy only to the segment to which is the address belongs.
  - It has a table which contains the address with the mapping to parts.



(ii) Gateway :

- Operates in all five layers of the internet or seven layers of the OSI model.
- It takes an application message, read it and interrupts it.
- It is used as connecting devices between two internetwork that uses different models.
- It provides security by filtering unwanted application layer messages
- It is a link between two computers to connect to internet or another network is called gateway.

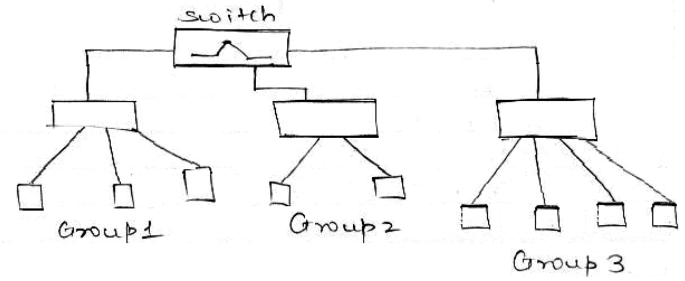


Q.3(d) What is Virtual LAN? How are stations grouped into different VLANs? Explain. [5]

Ans.: Virtual Local Area Network (VLAN) is a local area network configured by software and not by physical wiring.

Grouping stations into different VLANs
Examples

- The figure below shows a switched LAN in which nine stations are grouped into three LANs that are connected by a switch.



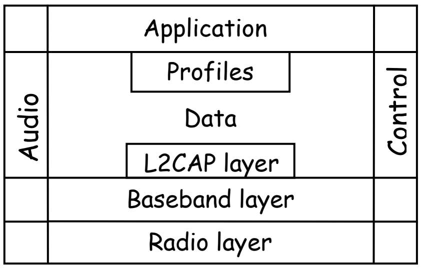
- It any of the computers have to moved from one group to another, the LAN configuration would need to be changed. The network technician must rewire. Thus in a switched LAN changes in the workgroup mean physical changes in the network configuration.

- The LAN can instead be divided into logical, instead of physical segments. These logical LANs are called VLANs. Each VLAN is a work group in the organization. It a person/computer moves from one group to another, there is no need to change the physical configuration.
- The group membership in VLANs is defined by software not hardware. Any station can be logically moved to another VLAN. All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN i.e. if a station moves from VLAN1 to VLAN2, it receives broadcast messages sent to VLAN2, but no longer receives broadcast messages sent to VLAN1.

Q.3(e) Explain Bluetooth Layered Architecture. **[5]**

Ans.: **Bluetooth Layered Architecture :**

Bluetooth uses several layers for the process of data transfer between systems :



L2CAP :

- Logical link control and Adaptation protocol is equivalent to LLC.
- It is used for data exchange on an ACL link SCO channels do not use L2CAP layer.
- It also performs the task of multiplexing, segmentation, reassembly, quality of service and group management.

Baseband Layer :

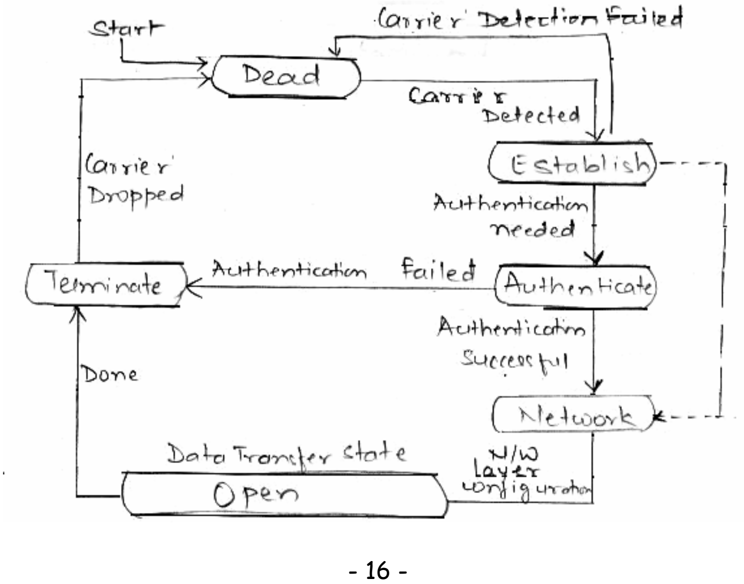
- It is equivalent to MAC sublayer. It uses TDMA for the process of communication between primary and secondary stations.
- It uses time division – duplex TDMA .

Radio Layer :

- It is equivalent to the physical layer. This devices are low–power and have range of 10 m.
- It uses 2.4 GHz ISM band divided into 79 channels of 1MHz each.
- It uses frequency hopping spread spectrum to avoid interference from other devices.
- It uses Gaussian bandwidth filtering as modulation technique.

Q.3(f) Explain the transition phases of point-to-point protocol. **[5]**

Ans.: A point to point protocol (PPP) goes through phases which can be shown in a transition phase diagram.

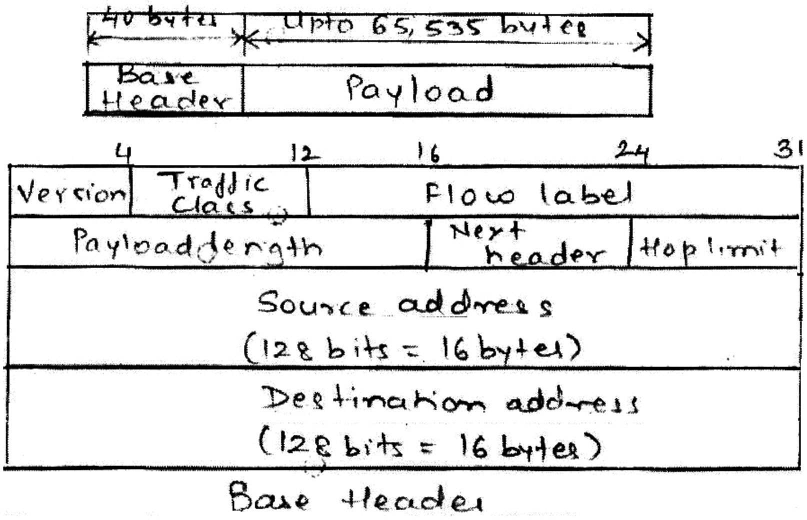


- The diagram starts with the 'Dead' state. In this state there is no active carrier (at the physical layer) and the line is quiet.
- When one of the two nodes starts the communication the connection goes to 'Establish' state. In this state, options are negotiated between the two parties. If the two parties agree that they need authentication then the system needs to do authentication (extra step); otherwise the parties can simply start communication. Several packets may be exchanged here.
- Data transfer takes place in 'Open' state. When a connection reaches this state exchange of data packets can be started. The connection remains in this state, until one of the end points wants to terminate the connection. In this case, system goes to 'terminate' state. The system remains in this state until the carrier is dropped, which moves the system to 'dead' state again.

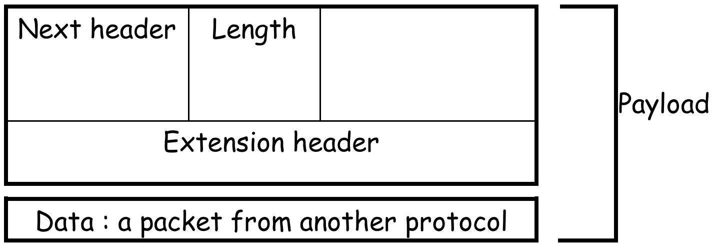
Q.4 Attempt the following (any THREE) [15]

Q.4(a) Draw and explain the IPv6 header format. [5]

Ans.:



- **Version** : The 4 bit version field defines the version number of the IP. For IPv6, the value is 6.
- **Traffic Class** : The 8 bit traffic class field is used to distinguish different payloads with different delivery requirements. Replaces the type–of–service field in IPv4.
- **Flow label** : 20 bit field that is designed to provide special handling for a particular flow of data.
- **Payload length** : 2 byte payload length field defines the length of the IP datagram the header. In IPv6, the length of the base header is fixed (40 bytes). Only the length of the payload needs to be defined.
- **Next header** : The next header is an 8 bit field defining the type of the first extension header (if prsent) or the type of the data that follows the base header in the datagram.
- **Hop Limit** : 8 bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source & destination addresses** : Source is a 16 byte Internet address that identifies the original source of the datagram. Destination address field is a 16 byte Internet address that identifies the destination of the datagram.
- **Payload** : Payload in IPv6 has a different meaning than in IPv4. It means a combination of zero or move extension headers (options) followed by the data from other protocols (UDP, TCP, etc.) Each extension header has two mandatory fields – next header & length, followed by into related to particular option. Each next header field value (code) defines the type of the next header (hope–by–hop option, source routing option.....) last next header field defines the protocol (4dp, TCP ....) that is carried by the datagram.



Next header codes

00	Hp by Hop option
02	ICMPv6
06	TCP
17	UDP
43	Source routing option
44	Fragmentation option
50	Encrypted security payload
51	Authentication header
59	Null (no next header)
60	Destination option

Q.4(b) What is routing information protocol? Explain the RIP algorithm. [5]

Ans.: Routing Information Protocol (RIP) is one of the most widely used intradomain routing protocols based on the distance vector routing algorithm.

RIP Algorithm

- Instead of sending only distance vectors, a router needs to send the whole contents of its forwarding table in a response msg.
- The receiver adds one hop to each cost and changes the next router field to the address of sending routes. Each route in the modified forwarding table. The received route & each route in the old forwarding table the old route. Received router selects the old routes as the new ones except in the following 3 cases.
  (i) If the received route does not exist in the old forwarding table, it should be added to the route.
  (ii) If the cost of the received route is lower than the cost of the old one, the received route should be selected as the new one.
  (iii) If the cost of the received route is higher than the cost of the old one, but the value of the next router is the same in both routes, the received route should be selected as the new one.
  This is the case where the route was actually advertised by the same router in the past, but the situation has now changed.
- The new forwarding table needs to be sorted according to the destination route (mostly using the longest prefix first)

Q.4(c) What is fragmentation? Explain its various strategies. [5]

Ans.: The wireless environment is very noisy, so frames are often corrupted. A corrupt frames has to be transmitted. The protocol therefore recommends fragmentation– division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.

Strategies :

A wireless LAN defined by IEEE 802.11 has three categories of frames :

- Management frame : It is used for the initial communication between station and access points.
- Control Frames : Used for accessing the channel and acknowledging frames. It has the subtype fields.

1011	Request to send
1100	Clear to send
1101	Acknowledgement

- Data Frame : Data frames are used for carrying data and control information.

FC	D	Add1	Add2	Add3	SC	Add4	Frame body	FCS

Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Poor Mgt.	More data	WEP	Rsvd

Fig.: Frame Format

FC	D	ADDRESS 1	ADDRESS2	FCS	RTS

Fig.: Control Frames

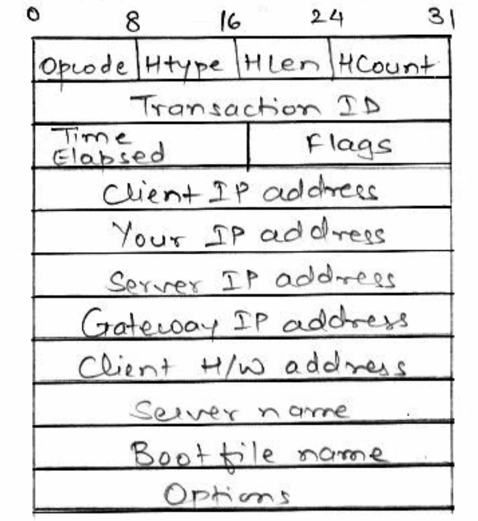
FC	D	ADDRESS 1	FCS	CTS or ACK

Q.4(d) What is dynamic host configuration protocol? Explain the DHCP message format. [5]

Ans.: **DHCP**

- Automatic address assignment in an organization.
- Application layer program, user client server paradigm.
- Can be configured to assign permanent IP address to the host and routers.
- Can also provide temporary IP address to hosts on demand.
- DHCP can also be used to provide the prefix, address of router and IP address of name server.

DHCP message format



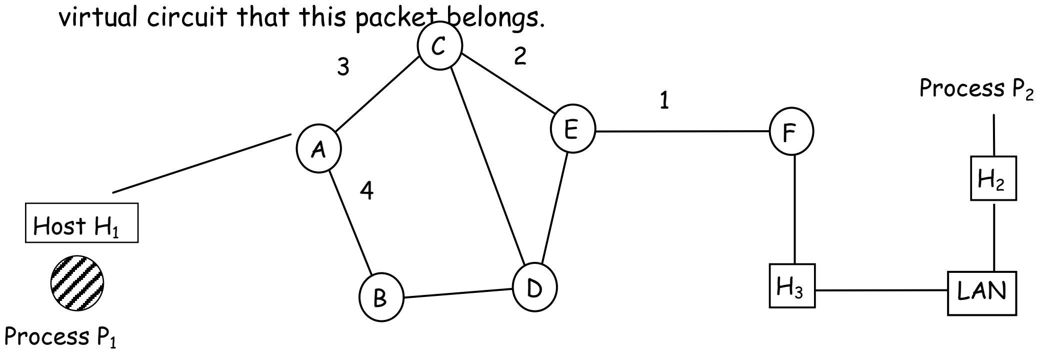
Fields

Opcode	Operation code, request (1), reply (2)
Htype	Hardware type (Ethernet…)
Hlen	Length of hardware address
HCount	Maximum no. of hops the packet can travel
TransactionID	An integer set by the client and repeated by the server
Time elapsed	No. of seconds since client started to boot
Flags	First bit defines unicast (0), multicast (1), other 15 bits not used
Client IP address	Set to 0 if client does not know it
Your IP address	Client IP addr sent by server
Gateway IP address	Address of default router

Q.4(e) Explain the terms : [5]
(i) Connection Oriented Network Services
(ii) Connectionless Network Services

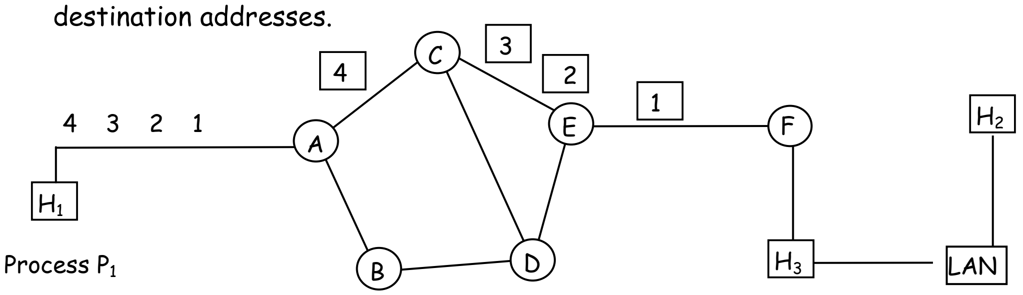
Ans.: (i) Connection Oriented Network Services :

- Connection Oriented Network Services is called virtual-circuit approach: There is a relationship between all packets belonging to a message.
- Here all the packets will follow the same path which was established before communication.
- When the connection is opened, the virtual circuit is also terminated. In connection oriented service, each packet carries an identifier. This identifier tell us about the virtual circuit that this packet belongs.



(ii) Connectionless Network Services :

- Here the packets from sending host H_1 are injected into the subnet individually and each packet is routed independently.
- No advance connection establishment is required. The packets are called as datagrams and the subnet is called as datagram subnet.
- The switches in this type of network are called routers.
- A packet may be followed by a packet coming from the same or from a different source.
- Each packet is routed bared on the information contained in header : source and destination addresses.



A's table

H_1	1		C	1
In			Out	

B's table

A	1		E	1
In			Out	

C's table

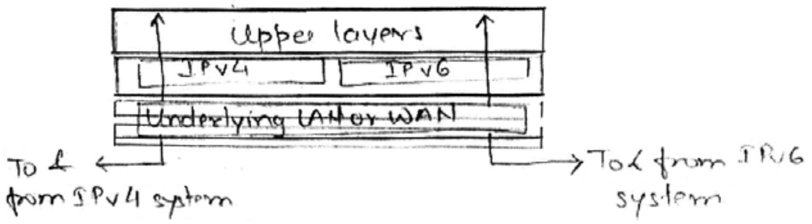
C	1		F	1

Q.4(f) What are the different transition strategies from IPv4 to IPv6? Explain. [5]

Ans.: 3 Strategies for transition

(i) Dual stack

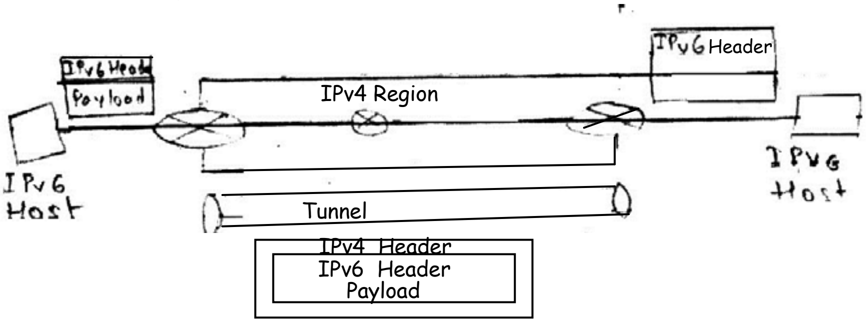
- A station must run IPv4 and IPv5 simultaneously until all the Internet use, IPv6.



- To determine which version to use when sending a packet to a destination, the source host queries the DNS.
- If the DNS returns an IPv4 address, source host sends an IPv4 packet.
- If DNS returns on IPv6 address, source host sends an IPv6 packet.

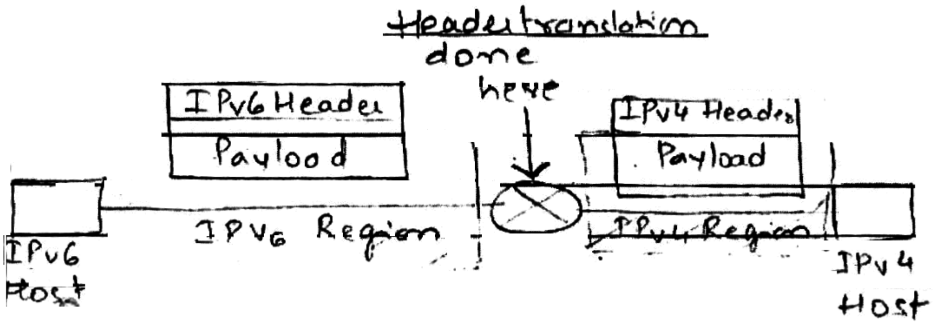
(ii) Tunneling

- Used when two computers using IPv6 want to communicate with each other and the packet must pass through this region, the packet must have an IPv4 address.
- To pass through this region, the packet must have an IPv4 address.
- So the IPV6 packet is encapsulated in an IPv4 packet when it enters the region & leaves its capsule when it exists the region.
- It seems as if the IPv6 packet enters the tunnel of one end & emerges at the other end.
- To make it dear that the IPv4 packet is carrying an IPv6 packet as data, protocol value is set to 41.



(iii) Header translation

- Necessary when the majority of the Internet has moved to IPv6 but some systems still use ϕ IPv4.
- Sender wants to use IPv6, but receiver understand only IPv4.
- In such case, header format must be totally changed through header translation.
- Header of IPv6 packet is converted to IPv4 packet.



Q.5 Attempt the following (any THREE) [15]

Q.5(a) Write a short note on TCP. [5]

Ans.: TCP :

- The internet has two main protocols in the transport layer.
- TCP (Transmission Control) is a connection oriented protocol.
- It provides reliable transmission of data in an IP environment. It corresponds to the transport layer of the OSI reference model.
- TCP provides stream data transfer, reliability efficient flow control, full –duplex operation and multiplexing.
- TCP delivers an unstructured stream of bytes identified by sequence numbers.
- Features of TCP :
  - It is process–to–process protocol
  - Uses port numbers
  - It is connection oriented protocol.
  - Uses flow and error control mechanism

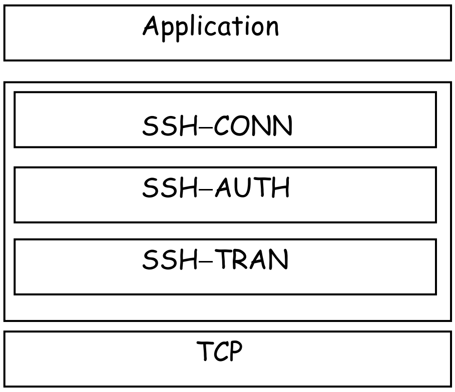
- Reliable protocol
- Efficient numbering system
- Byte numbers.
- Sequence numbers
- Flow control, Error, control and congestion control.

- Process–to–Process : TCP uses port numbers a transport layer address for communication of data.
- Full duplex service : Offers full duplex service where data can flow in both the directions.
- Stream delivery Service : The sending process delivers data in the form of a stream of bytes and the receiving process receives the same.
- Flow control : The receiver has a control over the amount of data to be send by the sender.
- Congestion control : Depending upon the network traffic the sender and the receiver is informed about the flow.

Q.5(b) What is secure shell? Explain the components of secure shell. **[5]**

Ans.: Secure Shell (SSH) is a secure application program that can be used today for several purposes such as remote logging & file transfer.

Components of SSH



SSH – TRANS

- As TCP is not a secured transport layer protocol, SSH first uses a protocol that creates a secured channel on top of the TCP. This new layer is an independent protocol called SSH–TRANS.

SSH AUTH

- After a secure channel is established between the client & the server & the server is authenticated for the client, SSH can call another procedure that can authenticate the client for the server.
- This process is similar to SSL.
- This Layer defines a no. of authentication tools similar to the ones used in SSH.
- Authentication starts with the client, which sends a request message to the server.
- Request includes user name, server name, method of authentication, & required data.
- Server responds with either a success message or failed message.

SSH-CONN

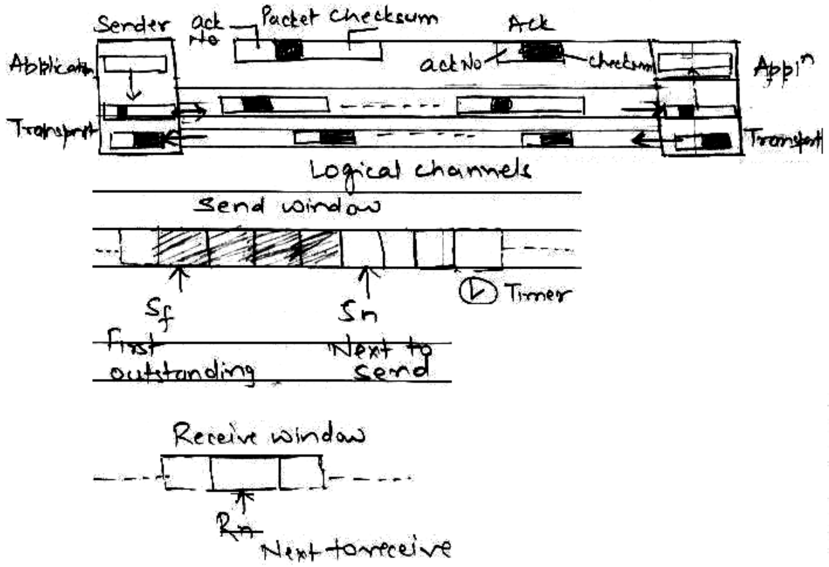
- After the secured channel is established & both server & client are authenticated for each other. SSH can call a piece of software that implements the third protocol SSH–CONN.
- It provides multiplexing.
- It takes the channel (secure) established by the two previous protocol & lets the client create multiple logical channels over it.
- Each channel can be used for a different purpose such as remote logging file transfer etc.

Q.5(c) Explain Simple Mail Transfer Protocol (SMTP). **[5]**

Ans.:
- The actual mail transfer is carried out through the message transfer agent. A system should have the client MTA in order to send a mail and it should have a server MTA in order to receive one.
- SMTP is the protocol which defines MTA client and server in the Internet.
- It is simple ASCII protocol.
- It uses a TCP connection between a sender and part 25 of the receiver, the sending machine operates as a client and the receiving machine acts a server.
- The client then waits for the server to take initiative in communication.
- The server sends line of text which declares its identity and announces its willingness or not to receive mail.
- But if the server is willing to accept e–mail, then the client announces the sender of email and its recipient.
- If such a recipient exists at the destination, then the server tells the client to send the message. The client, then sends the message and the server sends back its acknowledgement.
- No checksums are generally required because TCP provides a reliable byte stream.
- After exchanging all the emails, the connection is released.
- The components of E–mail system are :
  - User agent : The mail is created by a user agent program in response to user input. Each created message consists of a header which includes the recipient's E–mail address.
  - SMTP sender : Takes message from the queue and transmits them to the proper destination host.
  - SMTP receiver : Accepts each arriving message and stores it in the user mail box.

Q.5(d) With the help of a diagram, explain the Go-Back-N protocol. **[5]**

Ans.:

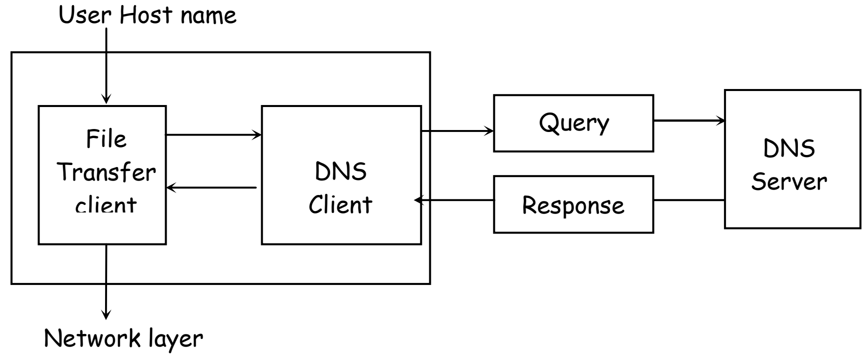


Goal of the protocol
- To improve efficiency of transmission multiple packet must be in transition while the sender is waiting for acknowledgement. Thus more than one packet is outstanding to keep the channel busy while the sender is waiting for ack.
- Key to GBN is that several packets can be sent before receiving ack, but the receiver can only buffer one packet.
- A copy of the sent packets is kept till the ack arrive.
- Sequence numbers are modulo 2^m, where m is the size of the seq. No. field in bits.
- Ack no. is cumulative & defines the seq. No. of the next packet expected to arrive.
- Send window is an imaginary box covering the seq. nos. of the data packets that can be in transit or can be sent. In each window position, some of these seq. nos. define the packets that have been sent, others define those that can be sent.

- Receive window makes sure that the correct data packets are received & that the correct ack are sent, the size of the receive window is always 1.
- Timers – Only one time is used. Timer for the first outstanding packet always expire first.
- All outstanding packets are resent when this timer expires [Resending packets]. Two local servers, the original resolver gets the final answer from the local server.

Q.5(f) What do you mean by Domain Name System? What is the use of the same? [5]

Ans.:



- The addressing in application program is different from that in the other layers. Each program will have its own address format.
- It is important to note there is an alias name for the address of remote host. The application program uses on alias name instead of an IP address.
- So the alias address has to be mapped to the IP address. For this an application program needs service of another entity.
- This entity is an application program called DNs.

Uses of DNS :

- The attacker may read the response of a DNS server to find the nature or names of sites the user mostly accesses. This type of information can be used to find the user's profile.
- The attacker may intercept the response of a DNS Server and change it or create a totally new bogus response to direct the user to the site or domain the attacker wishes the user to access. Helps to achieve authentication and message integrity.
- The attacker may flood the DNS server to overwhelm it or eventually crash it. This type of attack can be prevented using the provision against denial of service.

❑ ❑ ❑ ❑ ❑