Name: Farhana Afrin Shikha
ID : IT-18038
CT : 02

1.(a) What do you mean by data link layer? Write down two sub-layers of data link layer.

(b) Describe the functionality of data link layer.

2.(a) Write about flow control.

(b) What is error control?

(c) Describe Stop-and-Wait ARQ.

3.(a) What do you mean by error detection and correct

(b) Write down 3 types of errors.

(c) What does cyclic redundancy check mean?

4.(a) Define network layer.

(b) Write about network layer functionalities.

(c) What are the features of network layer?

5. (a) What is network addressing?

(b) What do you mean by IP Addressing?

(c) Describe parity check. Write about two types of error correction.

6. (a) What do you mean by Routing?

(b) Describe different types of routing.

(c) Write about two types of routing.

7. (a) What do you mean by internetworking?

(b) Describe Shortly about tunneling.

(c) What does packet fragmentation mean?

8. (a) What is Internet Control Message Protocol (ICMP)?

(b) Describe IPv4 and write the catagories of IP addresses.

(c) Define Internet Protocol Version 6 (IPv6).

1.(a) What do you mean by data link layer? Write down the sub-layers of data link layer.

Ans: Data link layer is second layer of OSI layered model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the

underlying hardware. At the receiving end, Data link laye
picks up data from hardware which are in the form o
electrical signals, assembles them in a recognizable fram
format, and hands over to upper layer.

Data link layer has two sub-layers:

- Logical Link Control: It deals with protocols, flow-contro
  and error control.
- Media Access Control: It deals with actual control of medi

1.(b) Describe the functionality of data-link layer.

Ans: Data link layer does many tasks on behalf of upper layer. These are:

Framing: Data-link layer takes packets from Network Layer and encapsulates them into frames. Then, it sends each fram bit-by-bit on the hardware. At receiver' end, data link laye picks up signals from hardware and assembles them into fr

Addressing: Data link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed t

be unique on the link. It is encoded into hardware at the time of manufacturing:

Synchronization: When data frames are sent on the link both machines must be synchronized in order to transfer to take place.

Error control: Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits.

Flow Control: Stations are on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

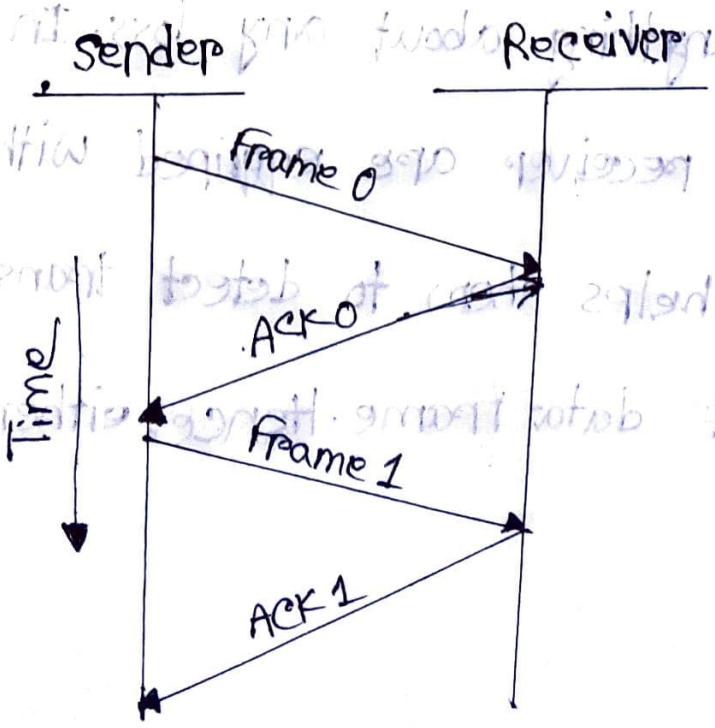
Multi-Access: When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple systems.

2.(a) Write about flow control.

Ans: When a data frame is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. If sender is sending too fast the receiver may be overloaded and data may be lost.

Two types of mechanisms can be deployed to control the flow

- Stop and Wait: This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



Sliding Window: In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, Stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

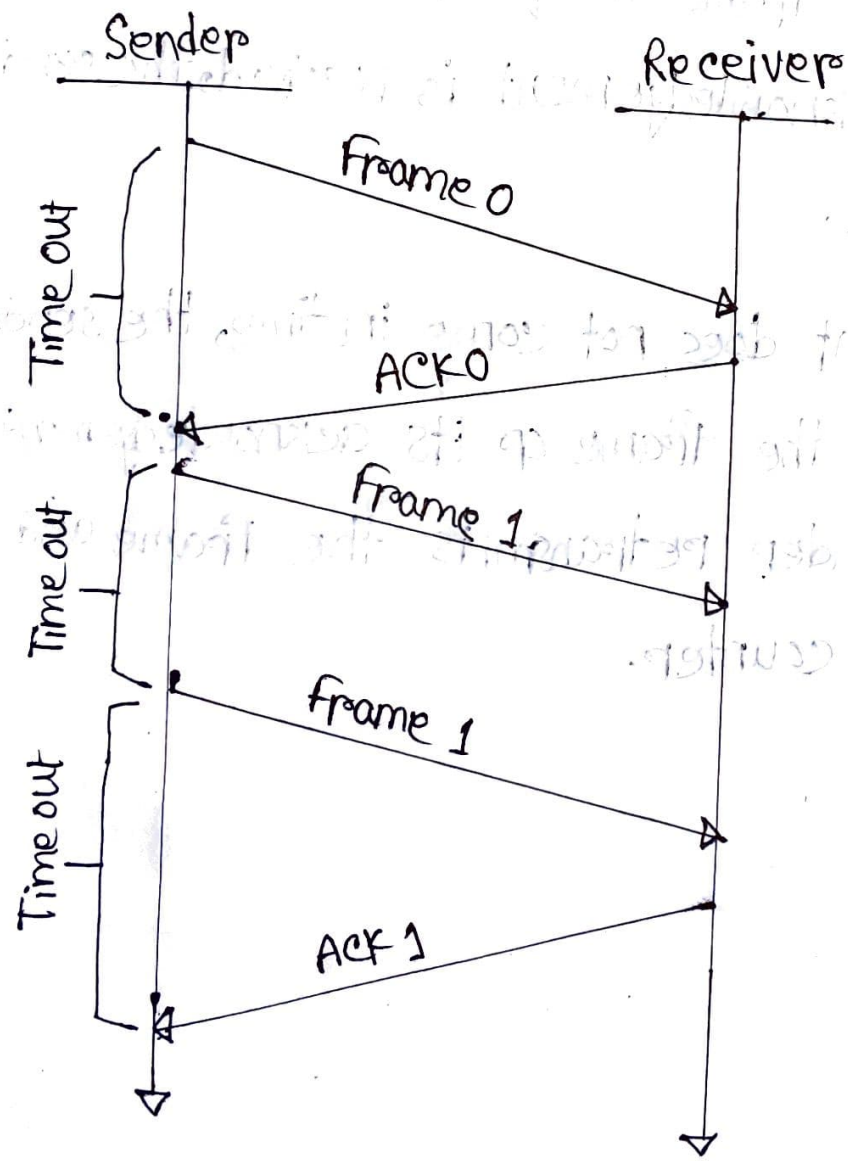
2.(b) What is error control ?

Ans: When data-frame is transmitted, there is a probability that data-frame may be lost in the trasit or it is received corrupted. In both cases, the receiver does not receive the correct data frame and sender does not know anything about any loss. In such case, both sender and receiver are equiped with some protocols which helps them to detect transit errors such as loss of data frame. Hence, either the

request to resend the previous data frame.

2.(c) Describe Stop and Wait ARQ.

Ans: Stop and Wait ARQ :



The following transition may occur in Stop-and-wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If a negative acknowledgement is received, the sender transmits the frame.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.

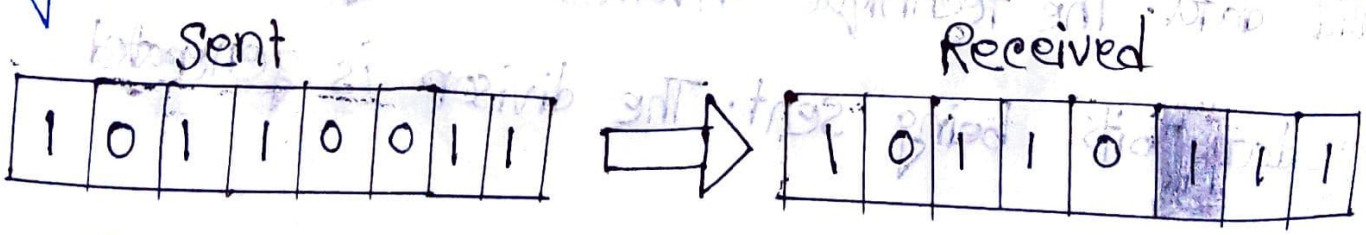
3.(a) What do you mean by error detection and correction?

Ans: In information theory and coding theory with application in computer science and telecommunication, error detection and correction or error control are techniques that enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables reconstruction of the original data in many cases.

3.(b) Write down 3 types of errors.

Ans: There may be three types of errors:

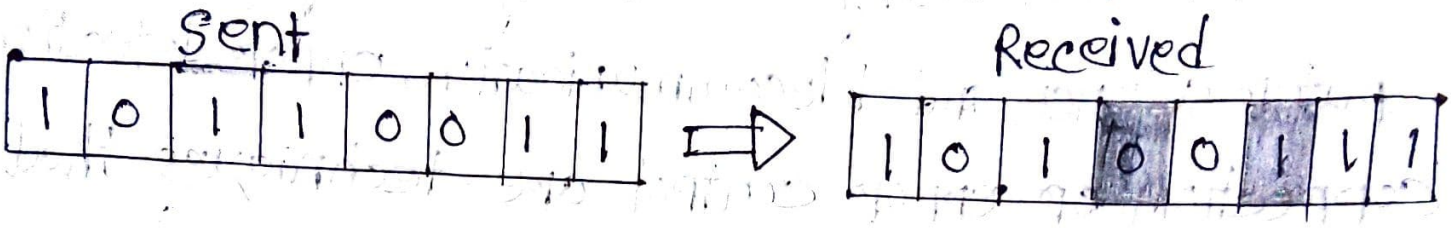
- Single bit error:



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

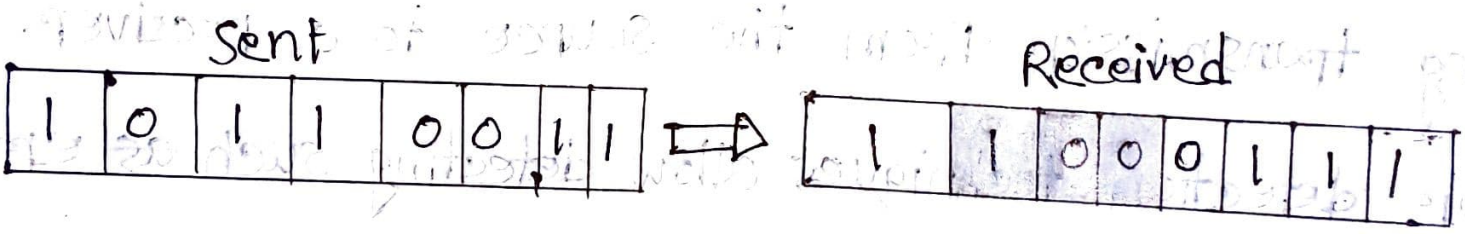
is corrupt.

Multiple bits error:



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

Burst error:

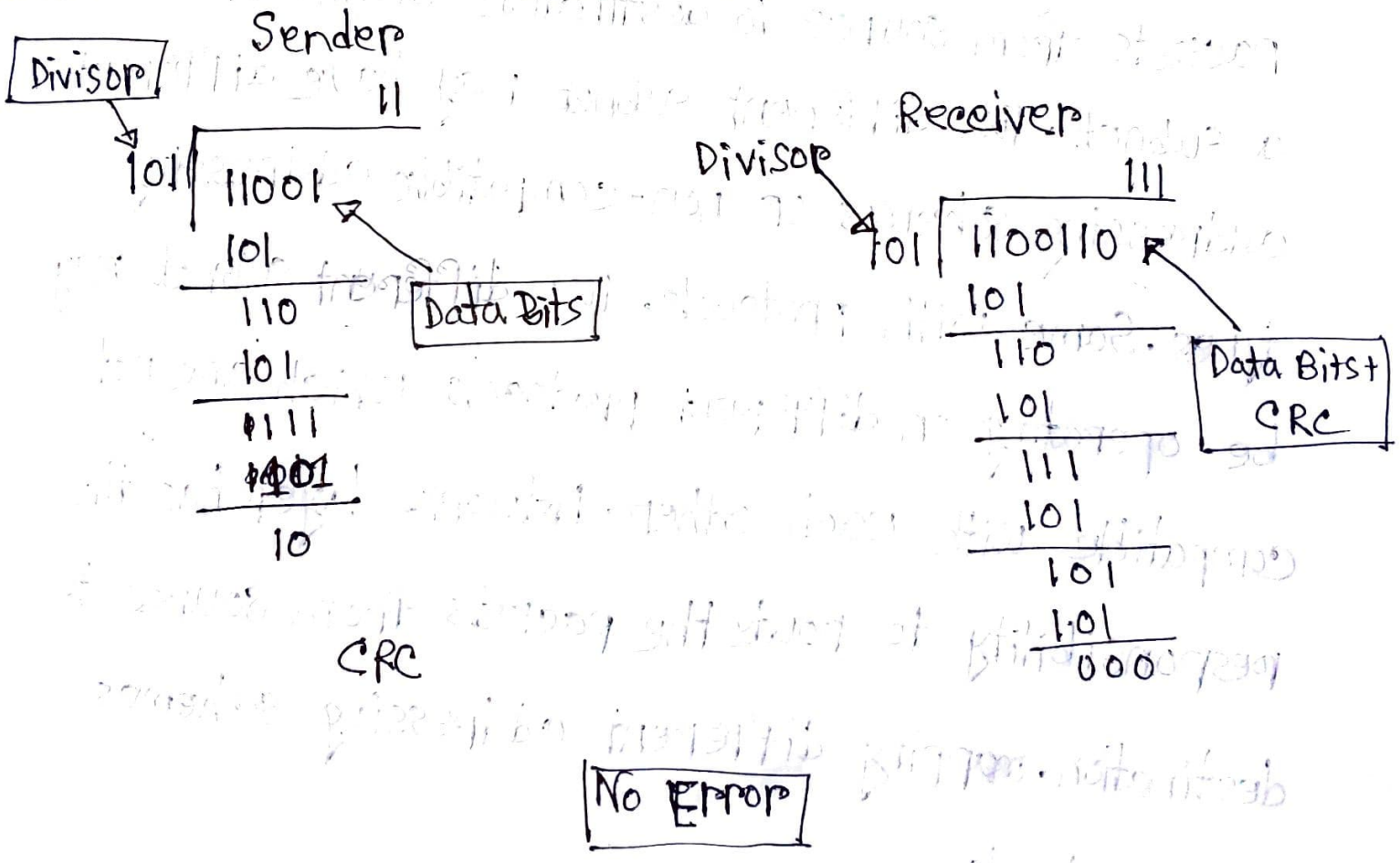


Frame contains more than 1 consecutive bits corrupted

3.(c) What does Cyclic Redundancy Check mean?

Ans: Cyclic Redundancy Check (CRC) is a different approach to detect if the received frame contains valid data. The technique involves binary division of the data bits being sent. The divisor is generated

using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other hand end, the receiver performs division operation on codewords using the same CRC divisor.

4.(a) Define network layer.

Ans: Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks and internetworking.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols. two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

4.(b) Write about network layer functionalities.

Ans: Device which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

- Addressing devices and networks.
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Interworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

4.(c) What are the features of network layer?

Ans: With its standard functionalities, layer 3 can provide various features as:

- Quality of service management.
- Load balancing and link management.
- Security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Internet protocol is widely respected and deployed Network Layer protocol which helps to communicate end to end devices over the internet. It comes in two flavors. IPv4 which has ruled the world for decades but now is running out of address space. IPv6 is created to replace IPv4 and hopefully mitigates limitations of IPv4 too.

5.(a) What is network addressing?

Ans: Layer 3 network addressing is one of the major tasks of Network Layer. Network Addresses are always logical i.e. these are software based addresses which can be changed by appropriate configurations.

A network addresses always points to host/node/server or it can represent a whole network. Network address is always configured on network interface card and is generally maped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.

There are different kinds of addresses in existence:

- IP
- IPX
- Apple Talk

What do you mean by IP addressing?

Ans: IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.

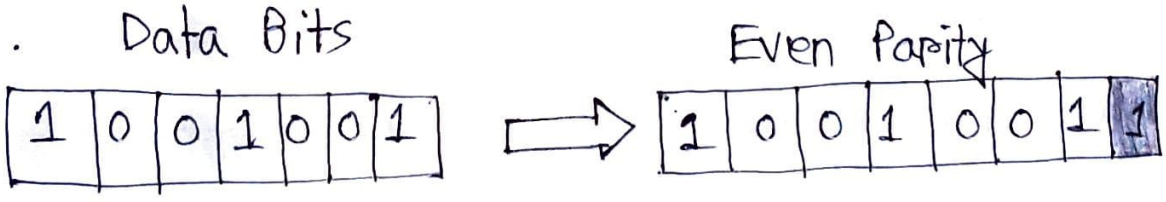
Hosts in different subnet need a mechanism to locate each other. This task can be done by DNS. DNS is a server which provides Layer-3 address of remote host mapped with its domain name or FQDN. When a host acquire the Layer-3 address (IP Address) of the remote host, it forwards all its packet to its gateway. A gateway is a router equipped with all the information which leads to route

packets to the destination host.

B.(c) Describe parity check. Write about two types of error correction.

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

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



The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used and ~~number of 1s~~ the frame is considered to be

not corrupted. and is accepted.

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

Backward Error Correction: When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

Forward Error Correction: When the receiver detect some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

6.(a) What do you mean by Routing ?

Ans: When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software based routers have limited functionality and limited scope.

A router is always configured with some default route. A default router tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

- Hop count
- Bandwidth
- Metric
- Prefix-length
- Delay

6.(b) Describe different types of routing.

Ans: Unicast Routing: Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is always known.

Broadcast Routing: By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases.

Multicast Routing: Multicast routing is special case of broadcast routing with significance difference and challanges. In broadcast routing, packets are sent to all nodes even if they do not want it.

But in multicast routing, the data is sent to only nodes which wants to receive the packets.

Anycast Routing: Anycast packet forwarding is a mechanis where multiple hosts can have some logical address. When a packet destined to this logical address is received it is sent to the host which is nearest in routing topology.

6.(c) Write about two types of routing algorithm.

Ans: The routing algorithms are as follows:

Flooding: Flooding is simplest method packet forwarding. When a packet is received, the routers send it to all the interfaces except the one on which it was received. This creates too much burden on the network and lots of duplicate packets wandering in the network.

Time to Live (TTL) can be used to avoid infinite looping of packets. There exists another approach for flooding,

which is called Selective Flooding to reduce the overhead on the method.

Shortest path: Routing decision in networks are mostly taken on the basis of cost between source and destination. Hop count plays major role here. Shortest path is a technique which uses various algorithms to decide a path with minimum number of hops.

Common shortest path algorithms are:

- Dijkstra's algorithm
- Bellman Ford algorithm
- Floyd warshall algorithm.

7.(a)-What do you mean by internetworking ?

Ans: In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking.

Networks can be considered different based on various parameters such as; Protocol, topology, Layer-2 network and addressing scheme.

In internetworking, routers have knowledge of each other's addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP.

7.(b) Describe shortly about tunneling.

Ans: If there are two geographically separate networks which want to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.

Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.

When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.

Both ends seem as if they are directly connected

and tagging makes data travel through transit network without any modifications.

7.(c) What does packet fragmentation mean?

Ans: Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily.

At the receiving end it is assembled again.

If a packet with DF (don't fragment) bit set to 1 comes to a router which can't handle the packet because of its length, the packet is dropped.

When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way.

If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

8.(a) What is Internet Control Message Protocol (ICMP)?

Ans: ICMP is network diagnostic and error reporting protoc
ICMP belongs to IP protocol suite and uses IP as carrie
protocol. After constructing ICMP packet, it is encapsulate
in IP packet. Because IP itself is a best-effort non-
reliable protocols, so is ICMP.

Any feedback about network is sent back to the original
host. If some error in the network occurs, it is reported
by means of ICMP. ICMP contains dozens of diagnostic
and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly
used ICMP messages to check the reachability of end-to-en
hosts. When a host receives an ICMP-echo request, it is
bound to send back an ICMP-echo-reply. If there is
any problem in the transit network, the ICMP will repor
that problem.

8.(b) Describe IPv4 and write the catagories of IP addresses.

Ans: IPv4 is 32-bit addressing scheme used as TCP/I host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiabl

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts.

IP addresses are divided into many catagories:

- Class A - it uses first octet for network addresses and last three octets for host addressing.
- Class B - it uses first two octets for network addresses and last two for host addressing.
- Class C - it uses first three octets for network addresses and last one for host addressing.
- Class D - it provides flat IP addressing scheme

hierarchical structure for above three. Class E - it is used as experimental.

8.(c) Define Internet Protocol Version 6 (IPv6).

Ans: Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6

equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still transition phase and is expected to replace IPv6 completely in coming years. At present there are few networks whichare running on IPv6.