1. a) What is data link layer? What are the sub-layers of data link layer?

b) Describe the functionality of data link layer.

c) Draw the Data link layer of OSI reference model

2. a) Describe the flow control techniques in data link layer.

b) Write the phases in error control mechanism.

c) What are the protocols of data link layer?

3. a) Describe the types of errors in data link layer

b) How data link layer can be used to control error?

c) Write the error correction techniques.

4. a) What is network layer? Draw the network layer of OSI model.

b) Write the functionalities of network layer.

c) What are the features of network layer?

5. a) What is network addressing? Give the example of network addressing.

b) How are IP addresses managed and distributed?

c) What are the differences between IPv4 and IPv6?

6. a) What is Routing? Describe the types of routing.

b) Difference the unicast, Broadcast and Multicast routing.

c) Write the multicast routing protocols.

7. a) Describe the routing algorithms.

b) What kinds of routing protocols available to route unicast packets?

c) What is Anycast? How does Anycast work?

8. a) What is tunneling? How does cloudflare use tunneling?

b) How does packet encapsulation work?

c) Why is encapsulation useful?

Ques - 1 :

Q) What is data link layer? What are the sublayers of data link layer?

Ans : Data link layer is the second layer of OSI layered Model. This layer is the protocol layer that transfers data between nodes on a network segment across the physical layer. The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly corrects error that may occur in the physical layer. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate. This layer is one of the most complicated layers and has complex functionabilities.

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 has two sub-layers:

1. Logical Link Control: It deals with protocols, flow control and error control.

2. Media Access Control: It deals with actual control of media.

b) Describe the functionality of data link layer.

Ans: Functionality of Data-link layer:

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

1) Framing: Data link layer takes packets from network layer and encapsulates them into frames. Then, it sends each frame bit-by-bit on the hardware. At receiver's end data link layer picks up signals from hardware and assembles them into frames.

2) Addressing: Data link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

3) 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 different speed or capacity, encountered problem in transition and the bits are flipped. These errors are detected and attempted to recovere actual data bits.

Flow control: Sations 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.

9) Draw the data link layer of OSI reference model.

Ans:

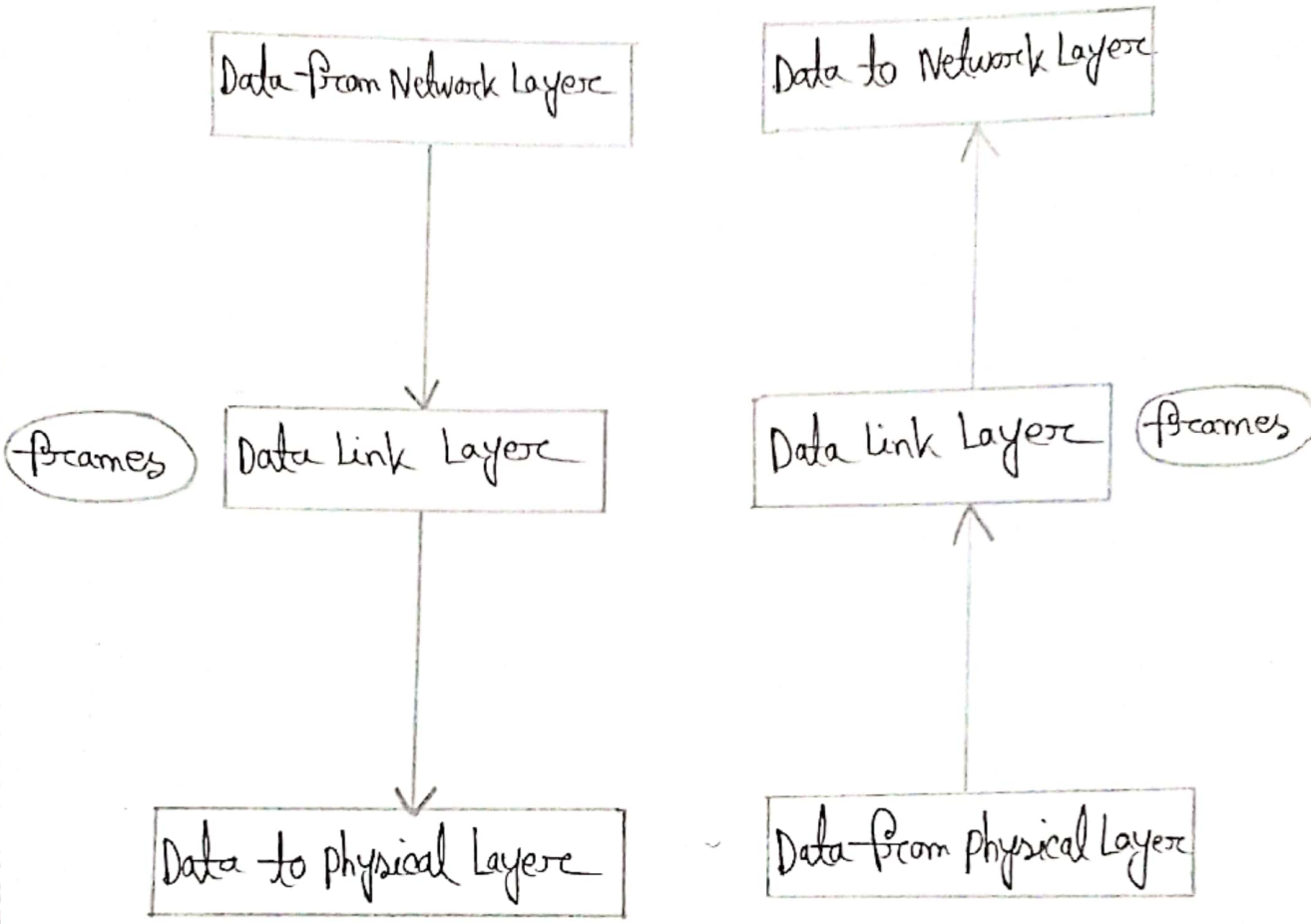


Fig: Data Link Layer of OSI Reference Model

Ques-2:

a) Describe the flow control techniques in data link layer.

Ans: Flow control techniques in Data Link Layer:

Data Link Layer uses feedback based flow control mechanisms. There are two main techniques-

1. Stop and wait: This protocol involves the following transitions:

i) the sender sends a frame and waits for acknowledgements.

ii) once the receiver receives the frame, it sends an acknowledgement frame back to the sender.

iii) on receiving the acknowledgement frame the sender understands that the receiver

is ready to accept the next frame. So, it sends the next frame in queue.

2. Siding window: The working principle of this protocol can be described as follows-

i) Both the sender and the receiver has finite sized buffers called windows. The sender and the receivers agrees upon the number of frames to be sent based upon the buffer size.

ii) The sender sends multiple frames in a sequence, without waiting for acknowledgement. On receiving acknowledgement, it advances the window and transmits the next frames, according to the number of acknowledgements received.

b) Write the phases in error control mechanism.

Ans: The error control mechanism in data link layer involves the following phases—

1) Defection of error - Transmission error, if any, is detected by either the sender or the receiver.

2) Acknowledgement - Acknowledgement may be positive or negative

→ positive ACK - On receiving a correct frame, the receiver sends a positive acknowledge.

→ Negative ACK - On receiving a damaged frame or a duplicate frame, the receiver sends a negative acknowledgement back to the sender

3) Retransmission – The sender maintains a clock and sets a timeout period. If an acknowledgment of a data-frame previously transmitted does not arrive before the timeout or a negative acknowledgement is received, the sender transmits the frame.

Q) What are the protocols of Data link layer?

Ans: Data link protocols:

- SDLC
- HDLC
- SLIP
- PPP
- LCP
- LAP
- NCP

SDLC: Synchronous Data Link protocol

HDLC: High-Level Data Link control

SLIP: Serial Line Interface protocol

PPP: Point to point protocol

LCP: Link control protocol

LAP: Link Access procedure

NCP: Network control protocol

Four protocols have been defined for the data link layer to deal with flow and error control:

① Simple

② Stop-and-wait

③ Go-Back-N

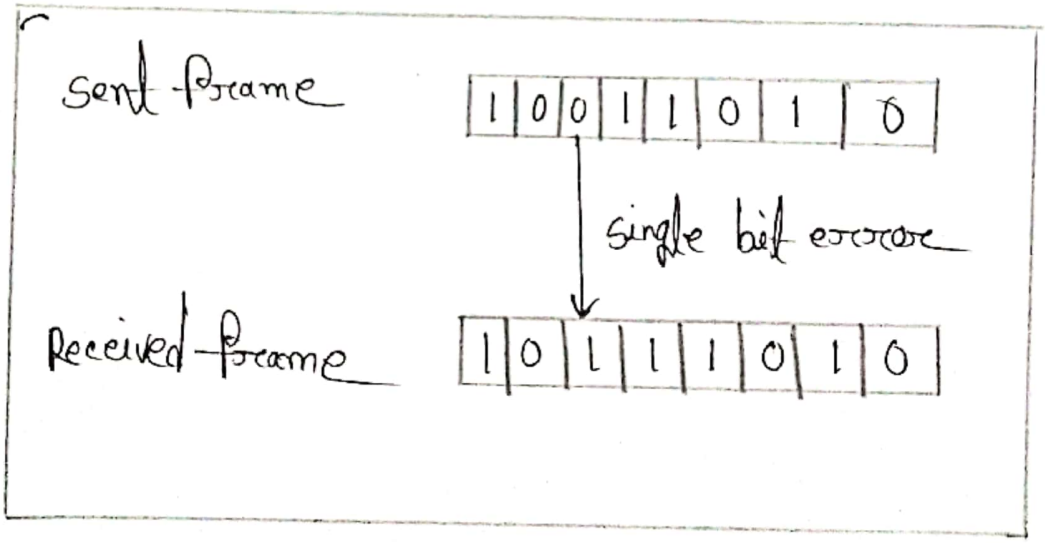
④ Selective-Repeat

Ques - 2 :

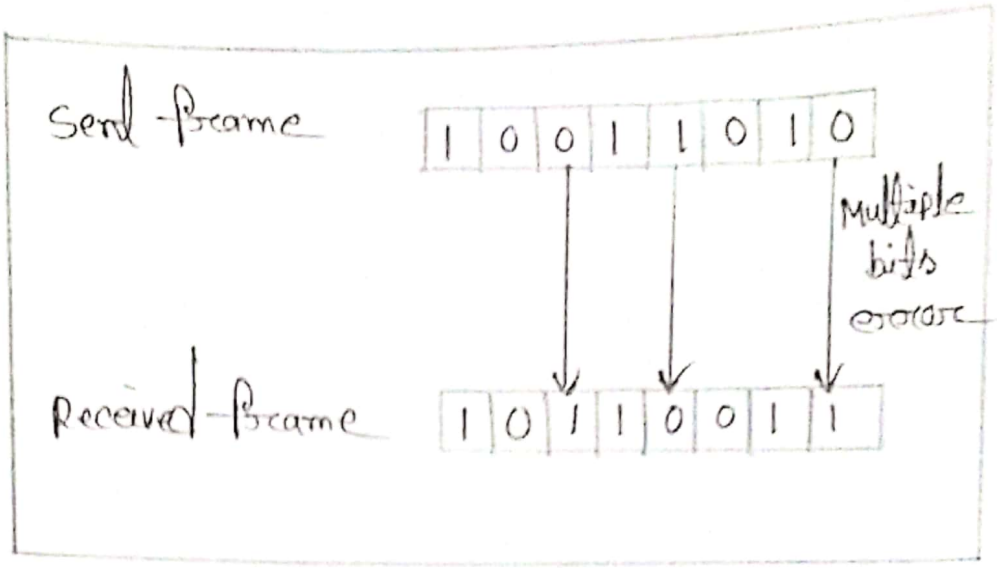
a) Describe the types of errors in Data Link Layer.

Ans : Errors can be of three types. namely Single bit errors, multiple bit errors and burst errors.

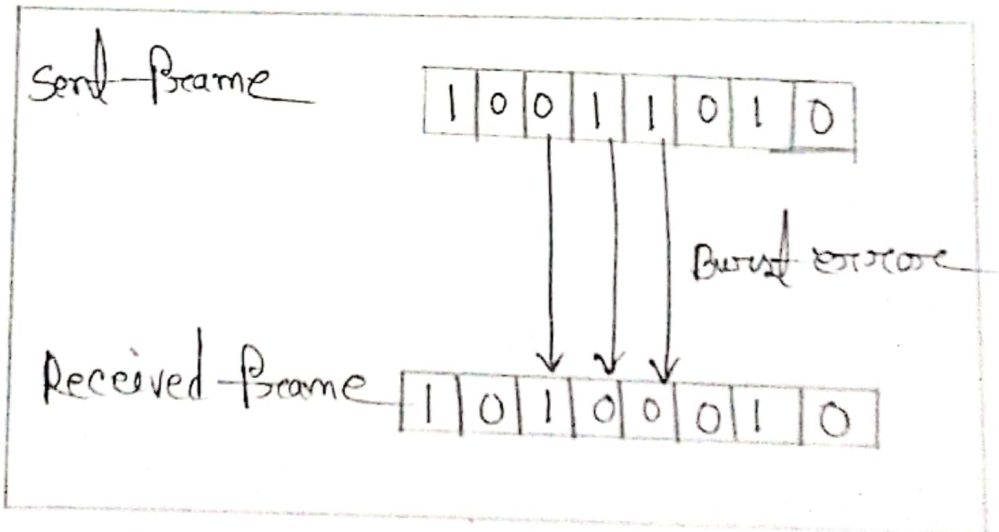
1) Single bit error - In the received frame, only one bit has been corrupted, ie. either changed from 0 to 1 or from 1 to 0.



2) Multiple bits error - In the received frame, more than one bits are corrupted



3) Burst Error: In the received frame, more than one consecutive bits are corrupted



b) How data link layer can be used to control error?

Ans: Error control can be done in two ways.

1. Error detection - Error detection involves checking whether any error has occured or not. The number of error bits and the type of error does not matter.

2 Error correction - Error correction involves ascertaining the exact number of bits that has been corrupted and the location of the corrupted bits.

For both error detection and error correction, the sender needs to send some additional bits along with the data bits. The receiver performs necessary checks

based upon the additional redundant bits.

c) Write the error correction techniques.

Ans: There are two principle ways.

1. Backward Error Correction: If the receiver detects an error in the incoming frame, it requests the sender to retransmit the frame. It is a relatively simple technique. But it can be efficiently used only where retransmitting is not expensive as in fiber optics and the time for retransmission is low.

2. Forward Error Correction: If the receiver detects some error in the incoming frame, it executes error-correcting code that generates the actual frame. This saves bandwidth required for retransmission. It is inevitable in real-time systems. However, if there are

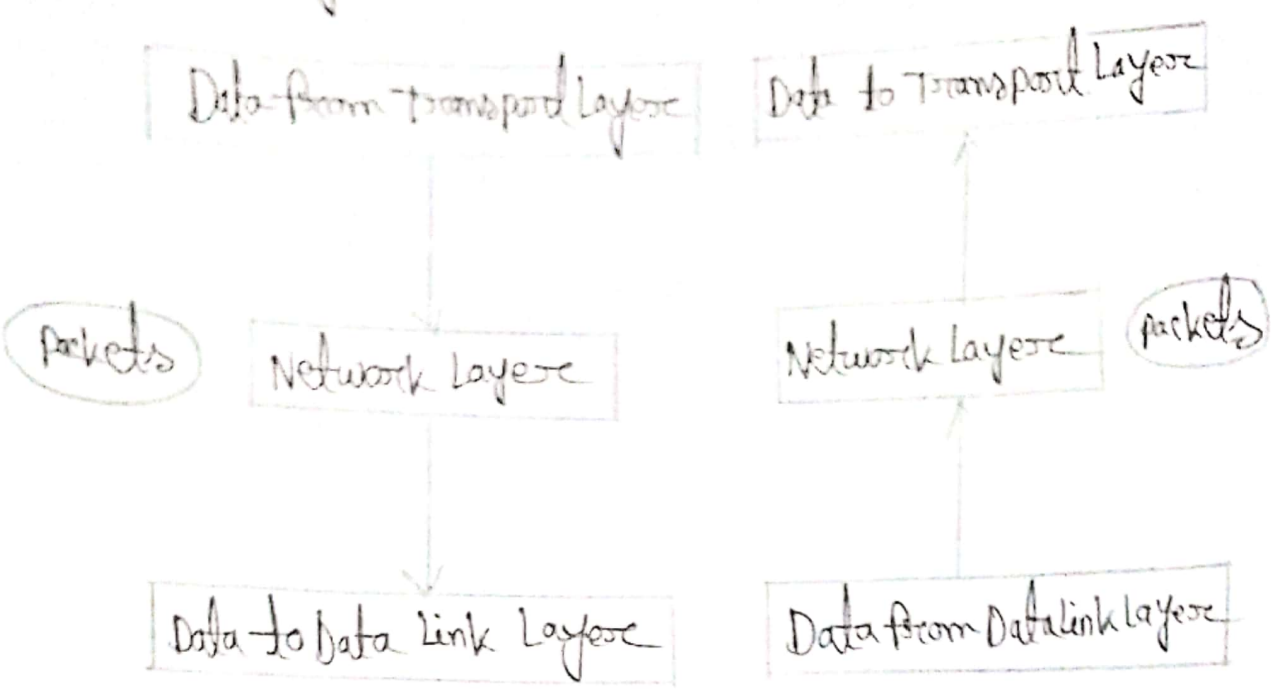
too many errors, the frames need to be retransmitted

Ques-4:

a) What is Network Layer? Draw the network layers of OSI model

Ans: The Network Layer is a portion of online communications that allows for the connection and transfer of data packets between different devices or networks. The network layer is the third level of the OSI model and the layer that provides data routing paths for network communication. Data is transferred to the receiving device in form of packets via logical network paths in an ordered format controlled by the network layer.

Network Layer of OSI model:



b) Write the functionalities of Network layer.

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

1) Addressing devices and networks.

2) populating routing tables or

static routes.

3) Queing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.

4) Internetworking between two different subnets.

5) Delivering packets to destination with best efforts.

6) Provides connection oriented and connection less mechanism.

c) What are the features of network layer?

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

1) Quality of service management
2) Load balancing and link management
3) Security
4) Interrelation of different protocols and subnets with different schema.
5) Different logical network design over the physical network design.
6) 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.

5. a) What is network addressing? Give the example of network addressing.

Ans:

A network address is an identifier for a node or host on a telecommunications network. Network addreses are designed to be unique identifiers across the network, although some networks allow for local, private addresses or locally administered addresses that may not be unique. Special network addresses are allocated as broadcast or multicast addresses. These two are not unique. In some cases, network hosts may have more than one network address. For example each network interface may be uniquely identified. Further, because protocols are

frequently layered, more than one protocol's network address can occur in any particular work interface or node and more than one type of network address may be used in any one network.

Examples of network addresses include:

1. Telephone number in the public switched telephone network.
2. IP address in IP networks including the internet.
3. IP address in Netware
4. X.25 or X.21 address in a circuit switched data network.
5. MAC address, in Ethernet and other related IEEE 802 network technologies.

b) How are IP addresses managed and distributed?

Ans:

IP addresses are managed by the Internet Assigned numbers Authority (IANA), which has overall responsibility for the Internet Protocol (IP) address pool, and by the Regional Internet registries (RIRs) to which IANA distributes large blocks of addresses.

The RIRs manage, distribute, and publicly register IP addresses and related internet number resources such as Autonomous System Numbers (ASN) and reverse Domain Name System (DNS) delegations within their respective regions. They do this according

to policies which are developed with their respective regional communities through open and bottop-up processes.

c) What are the differences between IPV4 and IPV6?

Ans:

Difference between IPv4 and IPv6

Basis	IPv4	IPV6
1. Size of IP address	1. IPv4 is a 32-bit Address	1. IPV6 is 128 bit IP address
2. Addressing method	2. IPv4 is a numeric address and its binary bits are separated by a dot(.)	2. IPv6 is an alphanumeric address whose binary bits are separated by a colon(:). It also contains hexa-decimal.

Basis	IPv4	IPv6
3. Number of header files	12	8
4. Length of header file	20	40
5. Checksum	Has checksum fields	Doesnot have checksum fields
6. Type of address	Unicast, Broadcast and Multicast	Unicast, Multicast and Anycast
7. Number of classes	IPv4 offers five different classes of IP address	IPv6 allows storing an unlimited number of Ip address.
8. VLSM support	IPv4 support VLSM	IPv6 doesnot offer support for VLSM
9. Fragmentation	Fragmentation is done by sending and forwarding routes.	Fragmentation is done by the sender.

Ques-6: a) What is Routing? Describe the types of routing.

Ans:

Routing is the process of finding a path to a destination host and of moving information across an internetwork from a source to a destination. There are two types:

1. Static routing: This type is the optimal path between all possible pairs of success and destinations in the given network is pre-defined and fed into the routing table of the routers of the network.

Advantages:

1) There is no CPU overhead for the

routers to decide the next step for the packet as the paths are predefined.

2). Between the routers, no bandwidth would be used.

Disadvantages:

1) For a larger network topology, it will be difficult for the administrator to identify and pre-define an optimal path from all possible combinations of source and destination.

2. Dynamic routing: This type gives the router the ability to discover the network by protocols like OSPF and RIP, updates the routing table by itself and effectively decides upon the path that the incoming packet must follow to reach its destination

Advantages:

1. This is easy to configure
2. It would be efficient in order to discover some remote network and execute route here.

Disadvantages:

1. Consuming a higher amount of bandwidth than static.
2. It is relative less secure

b) Difference the unicast, Broadcast and Multicast

Unicast	Broadcast	Multicast
1. It has only one sender and one reciever	1. It has one or multiple senders and multiple receivers	1. It has one sender and multiple receivers.
2. Sends data from one device to single device	2. Data can be sent from one device to multiple device.	2. Data sent from one device to all the other devices.

3. Works on single Node topology	3. Works on star, mesh, tree and hybrid topology	3. Works on bus and star topology.
4. Two devices are connected to each other with a single cable.	4. The switch is an example of a multicast device.	4. Hub is an example of a broadcast device
5. The ip addresses which are not used for multicast and broadcast are used for unicast transmission.	5. IANA controls assignment of multicast addresses. Addresses in range from 224.0.0.0 to 239.255.255.255 are used as ip multicast addresses.	5. The IPv4 address 255.255.255.25 is used as broadcast address. It uses multicast assignment of addresses.

9) Write the Multicast Routing protocols:

Ans:

Multicast Routing protocols use trees, i.e. spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

DVMRP – Distance Vector Multicast routing Protocol

MOSPF – Multicast Open shortest path first

CBT – Core Based Tree

PIM – protocol independent Multicast

Protol Independent Multicast has two flavours:

1. PIM Dense Mode: This mode uses source based trees. It is used in dense environment such as LAN.

2. PIM Sparse Mode: This mode uses shared trees. It is used in sparse environment such as WAN.

Ques-7

a) Describe the Routing algorithms.

Ans: The routing algorithms are as follows:

Flooding: Flooding is simplest algorithm 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 border 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 network. In this method the routers does not flood out on all the interfaces, but selective ones.

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:

1) Dijkstra's algorithm
2) Bellman Ford algorithm
3) Floyd Warshall algorithm

b) What kinds of routing protocols available to route unicast packets?

Ans:

There are two kinds of routing protocols available to route unicast packets.

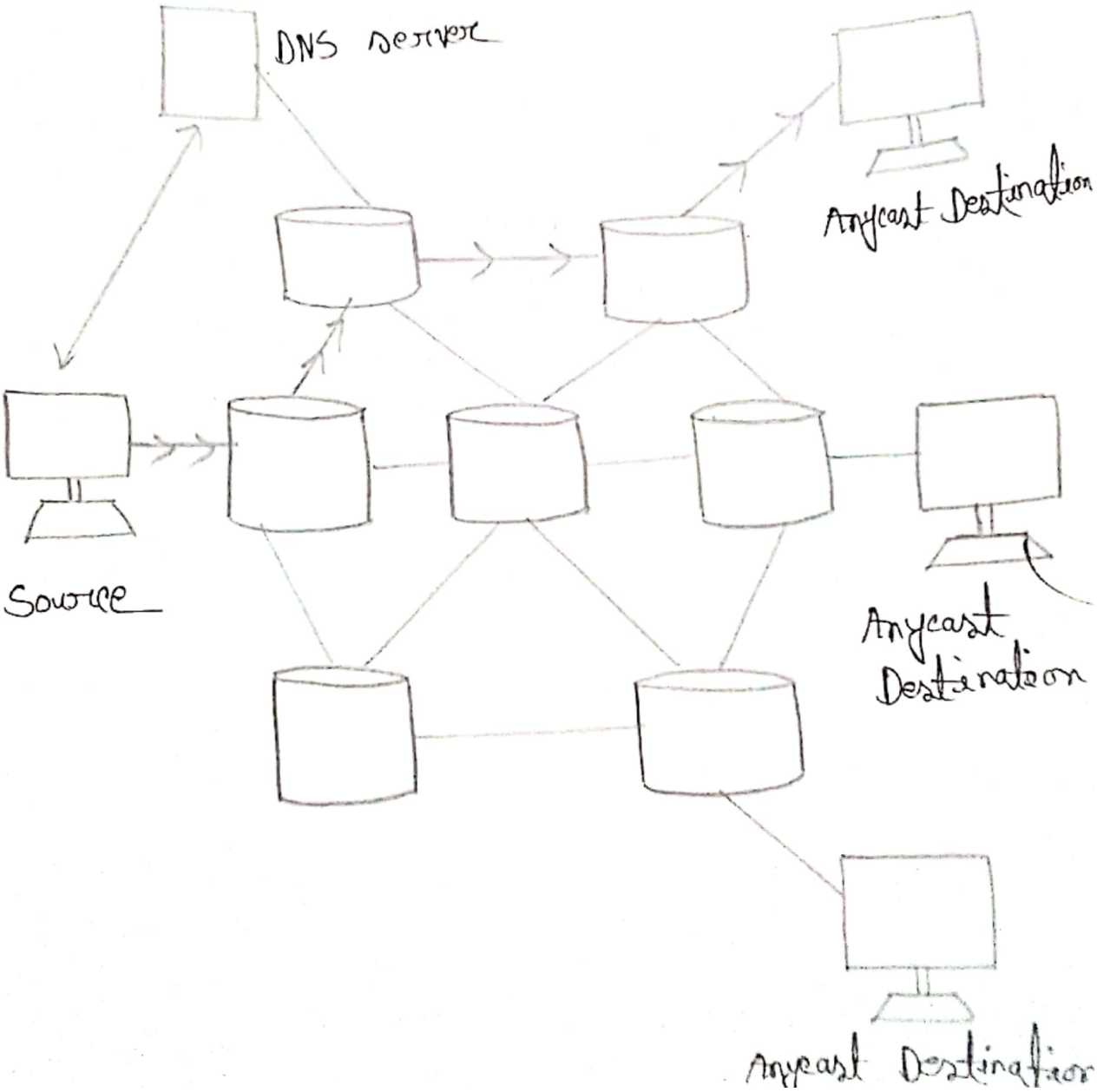
1) Distance vector Routing protocol:

Distance vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its best routes to other routers. ultimately, all routers build up their network topology based on the advertisements of their peer routers. For example Routing Information protocol

2) Link state Routing protocol: Link state protocol is slightly complicated protocol than distance vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network. For example, open shortest path first (OSPF).

3) What is Anycast? How does Anycast work?
Anycast packet forwarding is a mechanism where multiple hosts can have some logical address. When a packet destined to this logical address is receive, it is sent to the host which is nearest in routing topology. Anycast routing is done with help

of DNS server. Whenever an Anycast Packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.



Ques-8 :

a) What is tunneling? How does cloudflare use tunneling?

Ans : Tunneling is a way to cross terrain or boundaries that could not normally be crossed. Similarly in networking tunnels are a method for transporting data across a network using protocols that are not supported by that network. Tunneling works by encapsulating packets: wrapping packets inside of other packets. Tunneling is often used in Virtual private networks (VPNs). It can also set up efficient and secure connections between networks

enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

Cloudflare Magic Transit protects on-premise, cloud and hybrid network infrastructure from DDoS attacks and other threats.

In order for Magic Transit to work, the cloudflare network has to be securely connected to the customer's internal network. cloudflare uses GRE tunneling to form these connections with GRE tunneling, Magic Transit is able to connect directly to cloudflare customers networks securely over the public Internet.

b) How does packet encapsulation work?

Ans:

Data traveling over a network is divided into packets. A typical packet has two parts: the header, which indicates the packet's destination and which protocol it uses, and the payload, which is the packet's actual contents.

An encapsulated packet is essentially a packet inside another packet. In an encapsulated packet, the header and payload of the first packet goes inside the payload section of the surrounding packet. The original packet itself becomes the payload.

Q) Why is encapsulation useful?

Ans:

All packets use networking protocols - standardized ways of formatting data to get to their destinations. However, not all networks support all protocols. Imagine a company wants to set up a Wide Area Network (WAN) connecting office A and office B. The company uses the IPv6 protocol, which is the latest version of the Internet protocol (IP), but there is a network between office A and office B that only supports IPv4. By encapsulating their IPv6 packets inside IPv4 packets, the company can continue to use IPv6 while still sending data directly between the offices.

Encapsulation is also useful for encrypted network connections. Encryption is the process of scrambling data in such a way that it can only be unscrambled using a secret encryption key. The process of undoing encryption is called decryption. If a packet is completely encrypted, including the header, then network routers will not be able to forward the packet to its destination since they do not have the key and cannot see its header. By wrapping the encrypted packet inside another unencrypted packet, the packet can travel across networks like normal