1.

ⓐ Define data link layer. What are its sublayers? 3

ⓑ Explain the functionalities of data link layer. 5

ⓒ Which mechanism is responsible for Data link layer? Explain point-to-point flow control. 6

2.

ⓐ Briefly explain the error control mechanism. 4

ⓑ How many techniques are available in Data-link layer to control the errors by ARQ? 6

ⓒ How many ways may involve in error control mechanism? List the types of errors in data transmission. 4

3.

ⓐ Briefly explain how to control errors? 7

ⓑ List the network layer functionalities. 5

ⓒ How many different kinds of network addresses in existence? 2

4.

ⓐ Define Network Layer and its features. 6

ⓑ Briefly explain Network Addressing. 6

ⓒ Write down the protocols of network layer. 2

5.

ⓐ Define Network Routing. 2

ⓑ Explain different types of routing. 6

ⓒ Explain different routing protocols. 6

6.

ⓐ What is tunneling? 3

ⓑ Explain Packet Fragmentation. 5

ⓒ What does Internet Protocol Version 4 (IPv4) mean? Explain. 6

7.

ⓐ What are routing algorithms? 3

ⓑ What does Internet Control Message Protocol (ICMP) mean? Explain. 5

ⓒ What does Internet Protocol Version 6 (IPv6) mean? Explain. 6

8.

ⓐ Explain the TCP/IP model layer. 6

ⓑ How TCP/IP works? 5

ⓒ Write down the importance of TCP/IP. 3

1

@ Define data link layer. What are its sublayers?

Answer: 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 communication.

Data link layer has two sub-layers:

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

(b) Explain the functionalities of data link layer.

Answer: 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 frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

- **Addressing:** Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is ~~second~~ 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. It also provides error reporting mechanism to the sender.

• Flow Control: Stations 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.

Q Which mechanism is responsible for Data Link Layer? Explain point to point flow control.

Answer: Data link layer is responsible for converting data streaming to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer. Data-link layer is responsible for implementation of point-

to-point flow and error control mechanism.

Flow Control: When a data-frame (Layer-2 data) 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. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) 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

@ Briefly explain the error control mechanism.

Answer:

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

Requirements for error control mechanism:

- Error detection: The sender and receiver, either both or any, must ascertain that there is some error in the transit.

- Positive ACK : When the receiver receives a correct frame, it should acknowledge it.

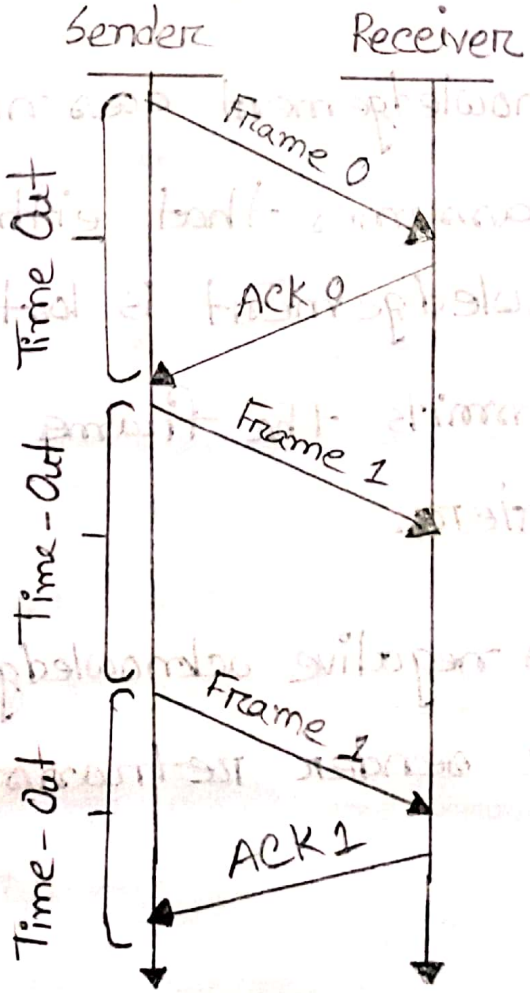
- Negative ACK: When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.

- Retransmission: The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

(2) How many techniques are available in Data-link layer to control the errors by ARQ?

Answer: There are three types of techniques available which Data-Link Layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

- Stop-and-wait ARQ:



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

i) The sender maintains a timeout counter.

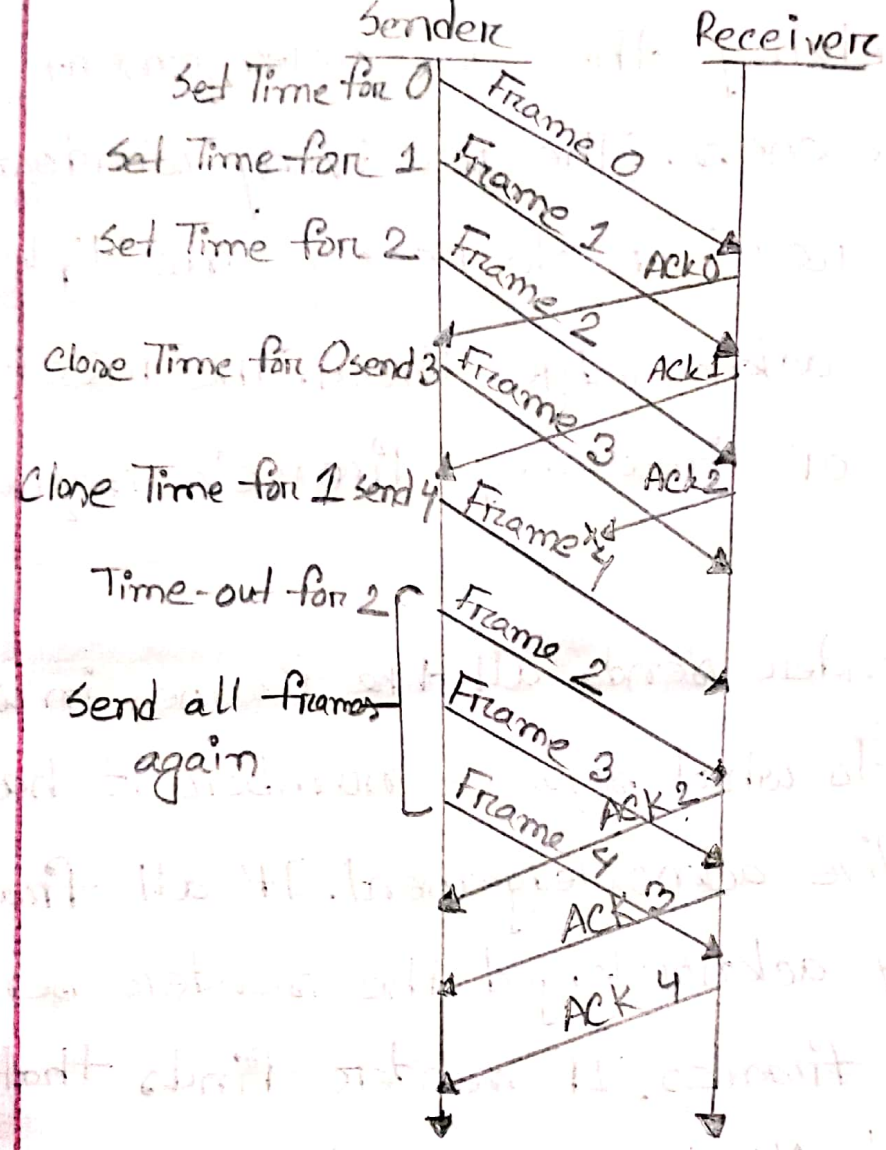
ii) When a frame is sent, the sender starts the timeout counter.

iii) If acknowledgement of frame comes in time, the sender transmits the next frame in queue.

iv) 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.

v) If a negative acknowledgement is received, the sender retransmits the frame.

• Go-Back-N ARQ:

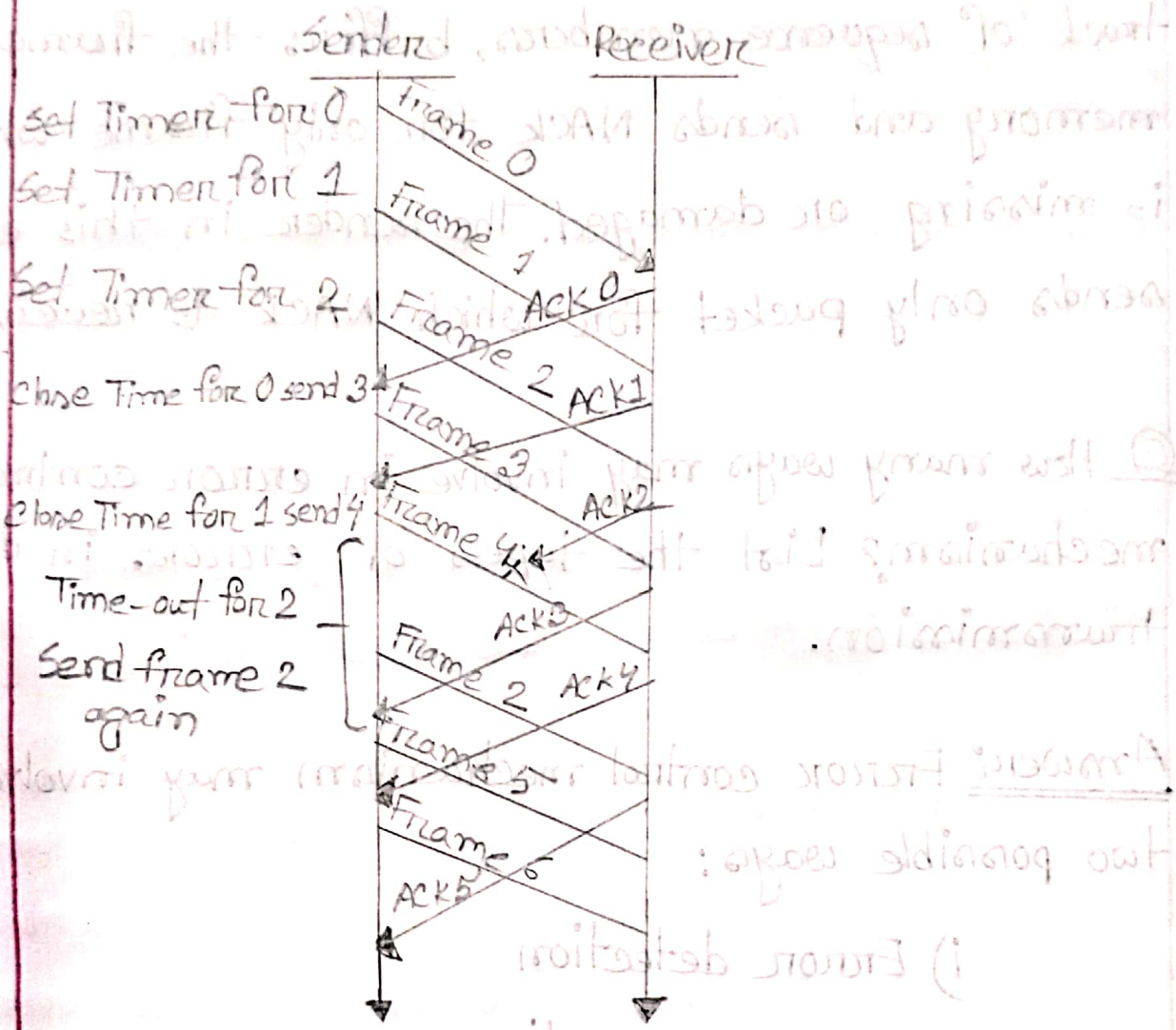


Stop-and-Wait ARQ mechanism does not utilize the resources at their best. When the acknowledgment is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window. The sending-window

size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

• Selective Repeat ARQ:



In Go-Back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.

In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged. The sender in this case, sends only packet for which NACK is received.

Q How many ways may involve in error control mechanism? List the types of errors in data transmission.

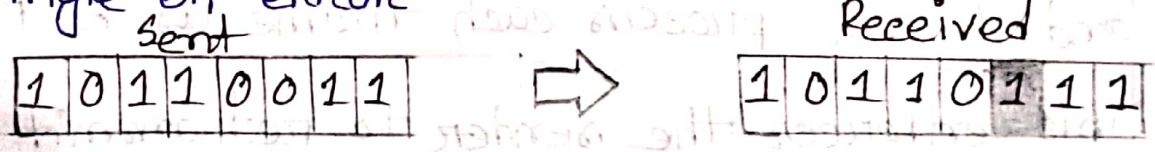
Answer: Error control mechanism may involve two possible ways:

i) Error detection

ii) Error correction

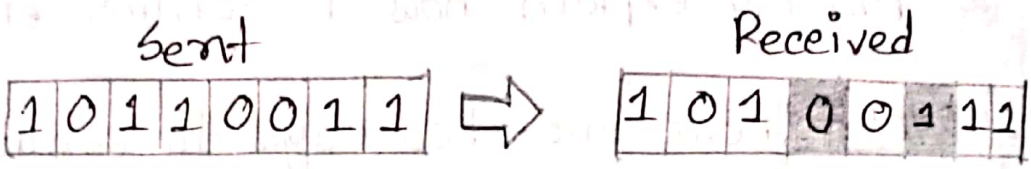
There may be three types of errors:

- 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

@ Briefly explain how to control errors?

Answer: There are two ways to control errors. They are explained below:

Error Detection:

Errors in the received frames are detected by means of Parity check and Cyclic Redundancy check (CRC). In both cases, few extra bits are sent ~~wrong~~ along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' and fails, the bits are considered corrupted.

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 number 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, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

Cyclic Redundancy Check (CRC): CRC is a different approach to detect if the received frame contains valid data. This 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 ~~using~~ 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 other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data ~~error~~ corruption occured in transit.

Error Correction:

In the digital word, 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 detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the letter case, Forward Error Correction is used.

~~(a) Define networ~~

(b) List the network layer functionalities.

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

These can be:

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

Q How many different kinds of network addresses in existence?

Ans: There are different kinds of network

addresses in existence:

- IP
- IPX
- AppleTalk

4 @ Define Network layer and its features.

Ans: 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.

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

- Quality of service management
- Load balancing and link management
- Security
- International 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.

⑥ Briefly explain Network Addressing.

Answer: 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 address 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 mapped by system with the MAC address of the machine for layer 2 communication.

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 acquires

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. Routers take help of routing tables, which has the following information:

- Method to reach the network Routers upon receiving a forwarding request, forwards packet to its next hop (adjacent router) towards the destination. The next router on the path follows the same thing and eventually the data packet reaches its destination.

Network address can be of one of the following:

- Musticast (destined to group)
- Broadcast (destined to all)

- Anycast (destined to nearest one)
- Unicast (destined to host)

A router never forwards broadcast traffic by default. Multicast traffic uses special treatment as it is most a video stream or audio with highest priority. Anycast is just similar to unicast, except that the packets are delivered to the nearest destination when multiple destinations are available.

Q. Write down the protocols of network layer.

Answer: The following are examples of protocols operating at the network layer;

- CLNS - Connectionless-mode Network Service
- DDP - Datagram Delivery Protocol
- EGP - Exterior Gateway Protocol
- ICMP - Internet Group Management Protocol
- IPV4/IPv6 - Internet Protocol

5

(a) Define Network Routing.

Answer: 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.

(b) Explain different types of routing.

Answer: Different types of routing is given below:

- 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 already

known. Hence, the routers he just has to look up the routing table and forward the packet to next hop.

• Broadcast Routing –

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers creat broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

• Multicast Routing –

Multicast Routing is special case of broadcast routing with significance difference and challenges. 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. The routers must know that there are nodes, which wish to

receive multicast packets then only it should forward. Multicast routing works spanning tree protocol to avoid looping. Multicast routing also uses reverse Forwarding technique, to detect and discard duplicates and loops.

- Anycast Routing -

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, 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 best IP address which is the nearest IP configured on it.

Q Explain Different routing protocols?

Answer:

•Unicast Routing Protocols:-

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

i) Distance Vector Routing Protocol -

Distance Vector Routing Protocol 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 set 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 (RIP).

ii) 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 routers build a common graph of the entire network. All routers then calculate their best path for routing purposes. For example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS).

Multicast Routing Protocols –

Unicast routing protocols use graphs while 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

Protocol Independent Multicast is commonly used now. It has two flavors:

- PIM Dense Mode – This mode uses source-

based trees. It is used in dense environment such as LAN.

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

6

@ What is tunneling?

Answer: If they 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. Tunnelling 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.

(b) Explain Packet Fragmentation.

Answer: 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 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 not handle the packet because of its length, the packet is dropped

If

When a packet is received by a router has its MF (more fragment) 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.

Q What does Internet Protocol Version 4 (IPv4) mean? Explain.

Answer: Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides the logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices - including manual and automatic configurations - depending on the network type.

IPv4 is based on the best-effort model. This model guarentees neither delivery nor avoidance of duplicate delivery; these aspects are handled by the upper layer transport. IPv4 is 32-bit addressing scheme

used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable. IPv4 provide hierarchical addressing scheme which enables it to divide the network into subnetworks, each with well-defined number of hosts. IP addresses are divided into many categories:

- Class A - it uses first octet for network addresses and last three octets for host addressing
- Class B - it uses first two octets for networ 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 in contrast to hierarchical structure for above three.

•Class E - It is used as experimental. IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet). Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

[X]

@ What are routing Algorithms?

Answer: 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 creats 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 network. In this method, the router does not flood out on all the interfaces, but selective ones.

Shortest Path-

Routing decisions 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

(b) What does Internet Control Message Protocol (ICMP) mean ? Explain.

Answer: ICMP is network ~~diagon~~ diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

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

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end 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 transmit network, the ICMP will report that problem.

Q. What does Internet Protocol Version 6 (IPv6) mean? Explain.

Answer: Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. Devices on the Internet are assigned a unique IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect devices than the IPv4 address space had available. 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 a 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 in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some

transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

i) Dual stack implementation

ii) Tunneling

iii) NAT-PT.

8 @ Explain the TCP/IP model layer.

Answer: TCP/IP functionality is divided into four layers, each of which include specific protocols:

i) The application layer - provides applications with standardized data exchange. Its protocols include the HTP, FTP, Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). At the application layer, the payload is the actual

application data.

ii) The transport layer - is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram protocol (UDP) which is sometimes used instead of TCP for special purposes.

iii) The network layer - also called the internet layer, deals with packets and connects independent networks to transport the packet across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

iv) The physical layer - also known as the network

interface layer or data link layer, consists of protocols that operate only on a link - the network component that interconnects nodes or hosts in the network. The protocol in this lowest layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).

(b) How TCP/IP works?

Answer: TCP/IP uses the client-server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network.

Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is under unrelated to previous requests. Being stateless frees up

network paths so they can be used continuously.

The transport layer itself, however, is stateful. It transmits a single message. and its connection remains in place until all the packets in a message have been received and reassembled at the destination.

The TCP/IP d model differs slightly from the seven-layer Open Systems Interconnection (OSI) networking model designed after it. The OSI reference model defines how applications can communicate over a network.

@ Write down the importance of TCP/IP.

Answer: Importance of TCP/IP

TCP/IP is nonproprietary and as a result is not controlled by any single company. Therefore, the Internet Protocol suite can be

modified easily. It is compatible with all operating systems, so it can communicate with any other system. The Internet Protocol suite is also compatible with all types of computer hardware and networks.

TCP/IP is highly scalable and as a routable protocol, can determine the most efficient path through the network. It is widely used in current internet architecture.