Sub : _____

Day | | | | | | | |

Time : Date : / /

CT-2

Name : Moniruzzaman

ID : IT-18007

Sub : _____ Day | | | | | | | |

Time : Date : / /

1]

(a) Define data link layer. what are its sublayers? 3

b. Explain the functionalities of data link layer. 5

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

2]

(a) Briefly explain the error control mechanism. 4

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

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

3]

(a) Bitiefly explain how to control errors? 7

(b) List the network layer functionalities. 5

(c) How many different kinds of network address in existance? 2

Sub : _____ Day | | | | | | | |

Time : Date : / /

4]

(a) Define Network Layer and its features : 6

(b) Briefly explain Network Addressing. 6

(c) Write down the protocols of network layer. 2

5]

(a) Define Network Routing. 2

(b) Explain different types of routing. 6

(c) Explain different routing protocols. 6

6]

(a) What is tunneling ? 3

(b) Explain Packet Fragmentation. 5

(c) What does Internet Protocol version 4 (IPV4) means ? Explain. 6

7]

(a) What are routing algorithms? 3

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

Sub :

Day

Time : Date : / /

ⓒ 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

Sub :

Day

Time : Date : / /

Answer to the ques. no :- 1

(a)

Data link layer is second layer of OSI Layered Model. This layer is one of the most complicated layers ~~has~~ 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.

Sub : Day Time : Date : / /

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.

Answer to the quen no : 01

(b)

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

* Framing : Data link layer takes packet 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

Sub : _____ Day | | | | | | | |

Time : Date : / /

address is assumed to 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 synchonized 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

Sub : _____ Day | | | | | | | |

Time : Date : / /

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.

Answer to the ques. no: 01

(c)

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 layer picks up data from hardware which are in the ~~link~~ layer 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.

Time : Date : / /

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.

Sub : _____ Day | | | | | | | |

Time : Date : / /

* 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.

Answer to the ques no: 02

(a)

Error control :- When data frame is transmitted, there is probability that data frame may be lost in the transit or it is received corrupted. In both case, 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 equipped with some protocols wich helps them to detect transit errors such as

Sub: Day Time: Date: / /

loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may requient 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 reciver receives a correct frame, it should acknowledge it.

* Negative Ack: when the receiver receives a damage 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 acknowledge

Time : Date : / /

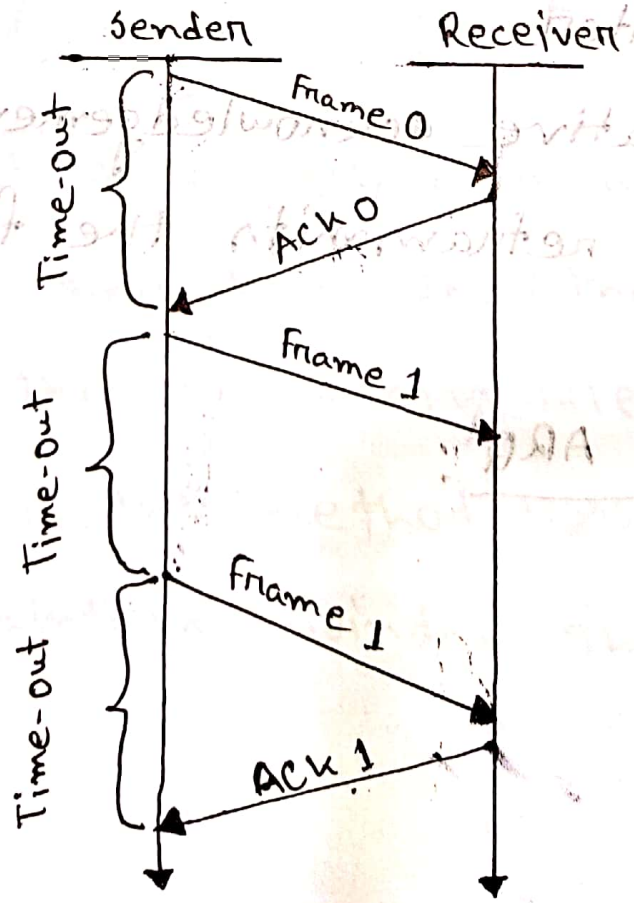
of a data frame previously transmitted doen not arrive before the timeout the sender transm the frame, thinking that the frame or its acknowledgement is lost in transmit.

Ans. to the ques no: 02.

(b)

There are three types of techniques avilable which Data-Link Layer may deploy to contr the errors by Automatic Repeat Requests (AR

* Stop-and-wait ARQ:



Sub: _____ Day | | | | | | | |

Time: Date: / /

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

i) The sender maintains a timeout counter.

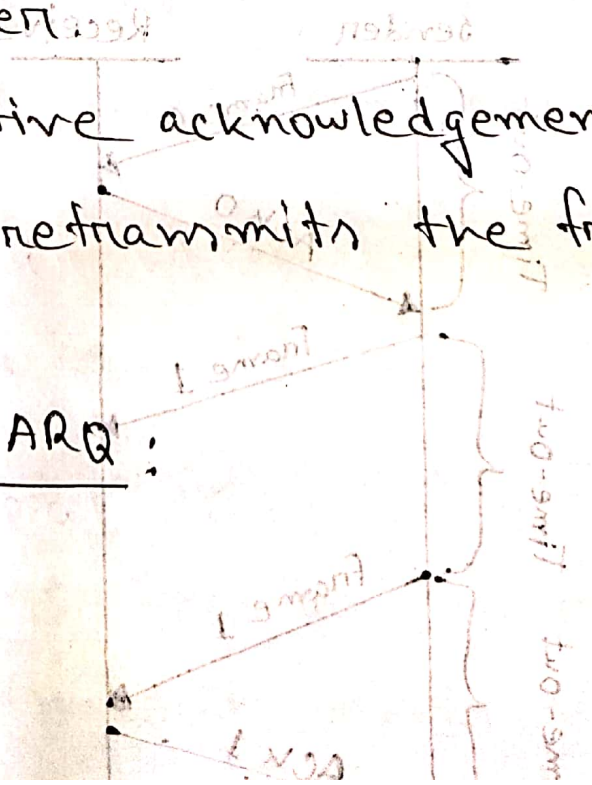
ii) When a frame is sent, the sender starts the timeout counter.

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.

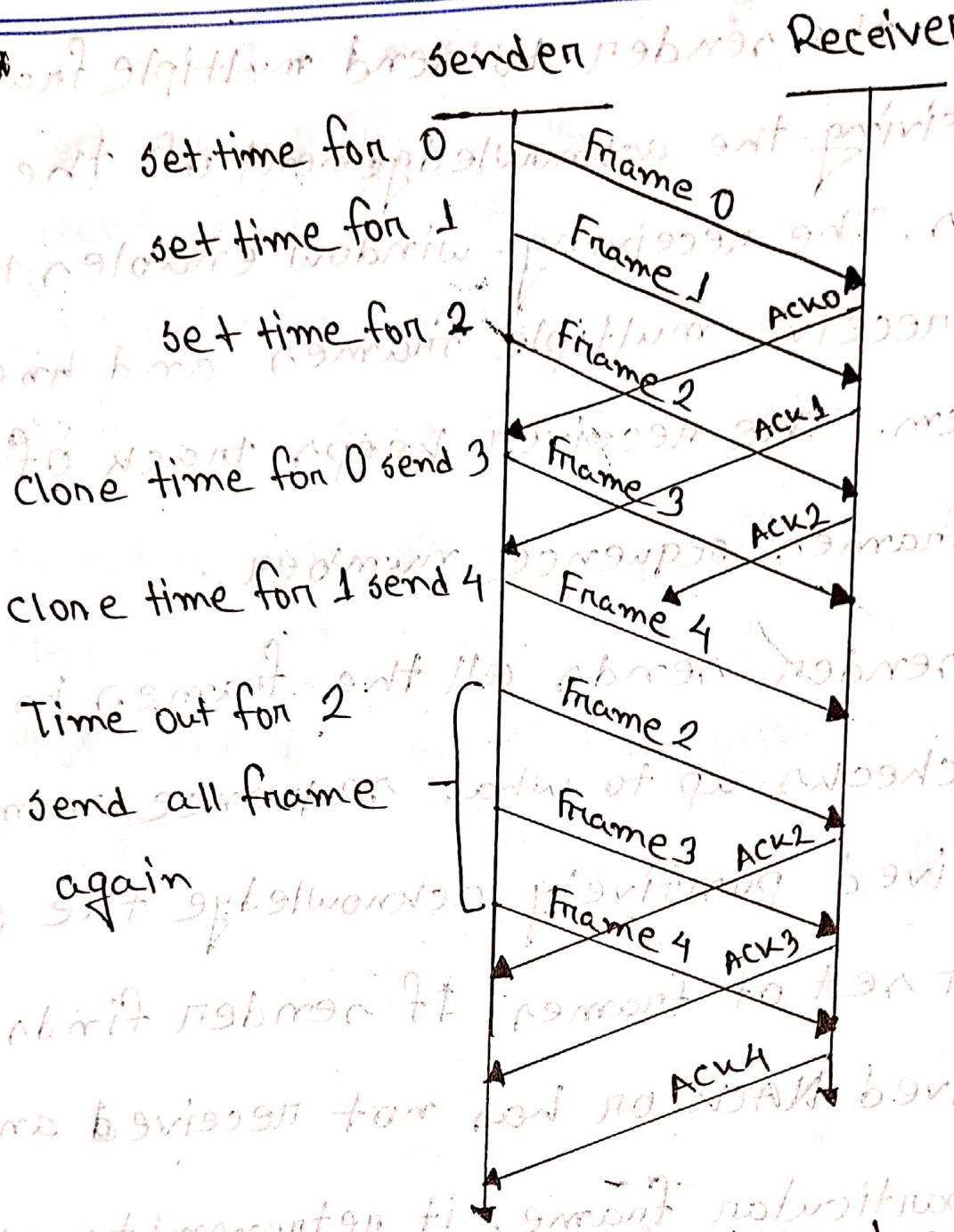
v) In a negative acknowledgement is received, the sender retransmits the frame.

* Go-Back-N ARQ:



Sub :

*



Stop and wait ARQ mechanism does not utilize resources at their best. When the acknowledgemer is received, the sender sits idle and does noth In go-Back-N ARQ method both sender and receiver maintain a window. The sending-win

Sub: Day Time: Date: / /

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 ~~to~~ acknowledge them. The receiver keeps track of incoming frames sequence number.

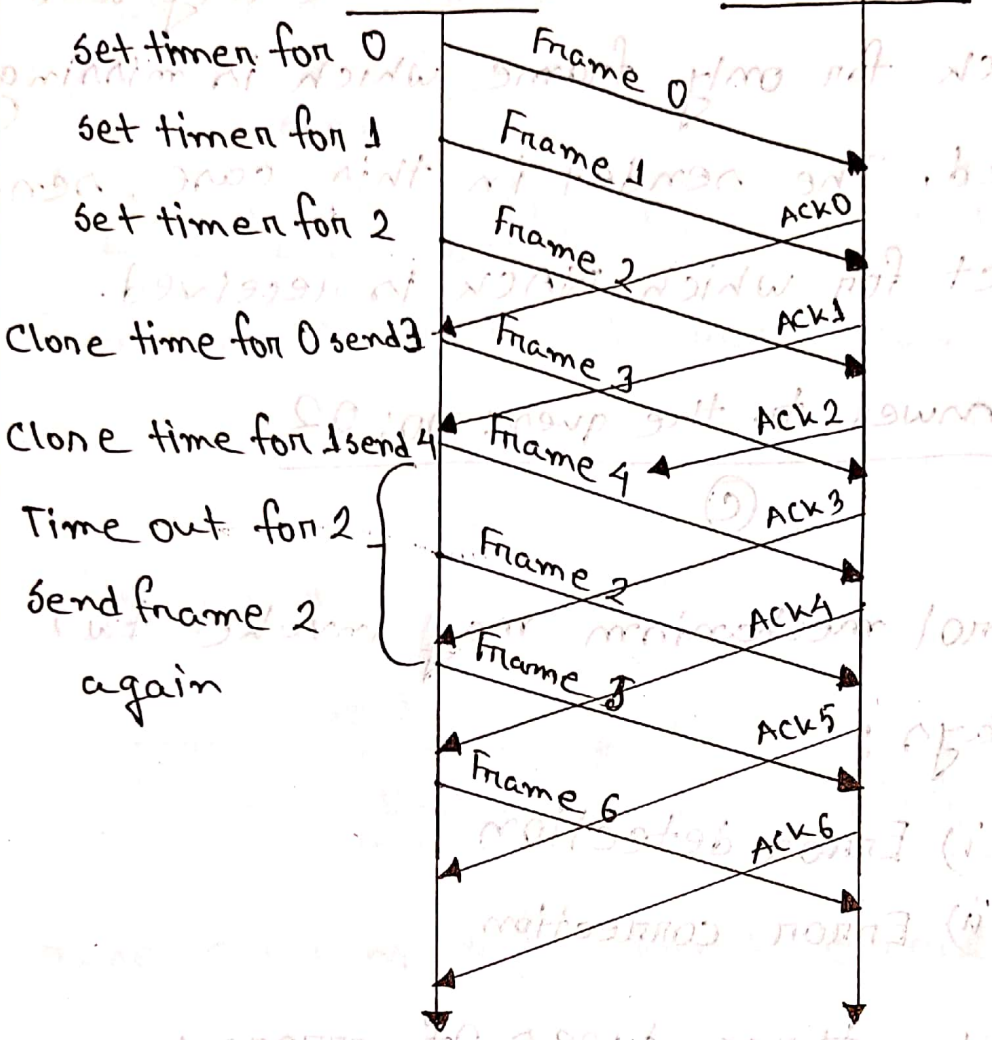
When the sender sends all the frames in window it checks up to what sequence number it has received positively acknowledge the sender sends next set of frames. If sender finds that it has received NACK or has not received any Ack for a particular frame, it retransmits all the frames after which it does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

* Selective Repeat ARQ:

Sub :

Day

Time : Date : / /



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 transmit all the frames which are not acknowledge. 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.

Answer to the ques: no: 02

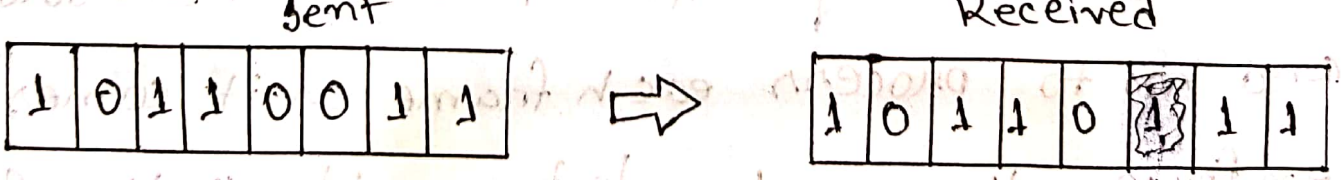
(c)

Error control mechanism may invoke two possible ways:

i) Error detection
ii) Error correction

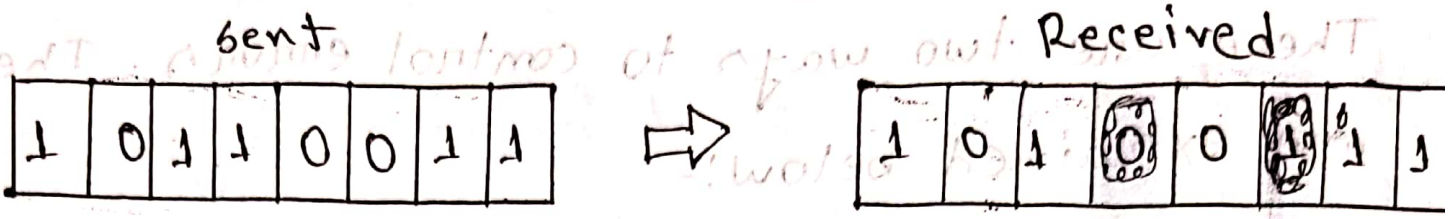
There may be three types of errors:

* Single bit error



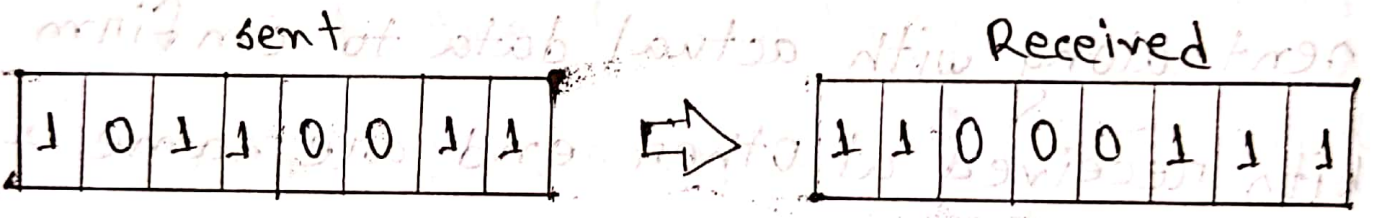
In a frame, there is only one bit, anywhere though, which is corrupt.

* Multiple bits error



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

* Burst error



Frame contains more then 1 consecutive bits corrupted.

Ans. to the ques no: 03

(a)

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 along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver end 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 add in case of odd parity. The sender while creating a frame counts the number of 1s in it

Time : Date : / /

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

Sub: Day Time: Date: / /

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 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 corruption occoured in transit.

Error Correction:

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

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

Sub : Day Time : Date : / /

• Forword Error Collection : when the receiver detects some error in the data received, it executes error-connecting code, which helps it to auto-recover and to connect some kinds of errors. The first one, Backword Error Connection is simple and can be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless tranmission retranmitting may cost too much. In the letter case Forword Error Connection is used.

Answer to the ques no: 03

(b)

Devices which work on Network layer mainly focus on routing. Routing may include various tasks aimed to achive a single goal.

Sub: Day Time: Date: / /

There can be:-

- Addressing devices and network.
- Populating routing tables on static routers.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism
- Queuing income and outgoing data and then forwarding them according to quality of service constrains set for those packets.

Answer to the ques. no: 03

(c)

There are different kinds of network address in existence:-

- IP
- IPX
- AppleTalk

Time : Date : / /

Ans: to the ques: no: 04

(a)

Network layer taken the responsiblity for routing packet 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 be provided various features as:-

- Quality of service management.

Sub: Day Time: Date: / /

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

Answer to the ques: no: 04

(b)

Layer 3 network addressing is one of the major task of Network layer. Network Addresses are always logical i.e there are software based addressing which can be changed by appropiate configurations. A network address always points to host / node / server or it can represent a whole network. Network address is always

Sub : _____ Day | | | | | | | |

Time : Date : / /

configured on network interfaced 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 distination network address, where the packet / data is to be sent. Host 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

Sub: Day Time: Date: / /

3 address (IP-address) of the remote host. it forwarded 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:-

- Multicast
- Broadcast

Sub :

Day

Time : Date : / /

- Anycast
- Onicast

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

Ans. to the ques no: 04

(c)

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 - Internal Group Management Protocol
- IPv4 / IPv6 - Internet Protocol

Answer to the ques: no: 05

(a)

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.

Answer to the ques. no: 05

(b)

Different types of routing is given bellow :-

- Unicast Routing -

Most of the traffic on the internet and internets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the

Sub :

Day

Time : Date : / /

internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence, the router just has to look up the routing table and forword 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 forword 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, packet data are sent to all node even if they do not want it.

Sub: Day Time: Date: / /

But in multicast routing, the data is sent to only nodes which wants to receive the packet. The router must know that there are nodes, which wish to receive multicast packet then only it should forwarded. 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

Sub : _____ Day | | | | | | | |

Time : Date : / /

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.

Ans: to the ques: no:05

(c)

- Unicast Routing Protocols :-

There are two kinds of routing protocols avilable to route unicast packet:

i) Distance Vector Routing Protocal -

Distance vector Routing Protocol is simple routing protocol which takes routing decision on the number of hops between source and destination. A router with less number of hops is considered as the best route. Every router advertises its net best routes to other routers. Ultimately,

Sub: Day Time: Date: / /

all routers build up their network topology based on the advertisements of their peer routers, For example Routing Information Protocol.

ii) Link State Routing Protocol :-

Link state protocol is slightly complicated protocol then Distance vector. It takes into account the states of links of all the vectors in a network. This technology helps routes build a common path 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 Intermediat system (ISIS)

Multicast Routing Protocol :-

Unicast routing protocols use graphs while Multicast Routing Protocols use trees, i.e

Sub: _____ Day | | | | | | | |

Time: Date: / /

spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

- DVMRP - Distance Vector Multicast Routing Protocol
- MOSPE - 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.

Answer to the question 06

(a)

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 complaxities. 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.

Sub: _____ Day | | | | | | | |

Time: Date: / /

Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modification.

Ans. to the ques: no:06

(b)

Most Ethernet segment have their maximum transmission unit (MTV) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transmit path also have their hardware and software capabilities which tell what amount of data device can handle and what ~~amount~~ 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 proccessed

Sub: Day Time: Date: / /

naturally. If the packet is ~~by~~ larger, it is broken into smaller pieces and then forwarded. This is packet fragmantation. Each fragmantation contain the same dentination 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.

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

If packet is fragmented too ~~much~~ small, the overhead is increase. If the packet is

Sub :

Day

Time : Date : / /

fragmented too large, intermediate router may not be able to process it and it might get dropped

Answer to the quen no: 06

©

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 indetification for each device. There are many ways to configure IPv4 with all kinds of devices including manual and autometic configurations depending on the network type. IPv4 is based

Sub: Day Time: Date: / /

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

Class A - it uses first octet for network addresses and host three octets for host addressing.

Sub : _____ Day | | | | | | | |

Time : Date : / /

- 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 it 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, and public addresses.

Though IP is not reliable one; it provides 'Best-Effort-Delivery mechanism.

Sub: _____ Day | Time: Date: / /

Answer to the ques: no:07

(a)

The routing algorithms are as follow:

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 ~~bort~~ 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

Sub : _____ Day | | | | | | | |

Time : Date : / /

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

Ans: to the ques: no: 07

(b)

ICMP is network 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.

Sub: Day Time: Date: / /

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 the problem.

Sub :

Day

Time : Date : / /

Ans. to the ques no:07

(c)

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 computer on networks and ~~location system for computers~~ routes traffic across the internet. Devices on the Internet are assigned a unique IP address for identification and location defination with the rapid growth of the Internet after commercialization in the 1990s. it becomes evident that far more addresses would be needed to connect devices than the IPv4 address space had avilable.

Exchange of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128 bit wide address providing.

Sub: Day Time: Date: / /

planty of address space for future to be used on entire planet on beyond. IPv6 has introduced Anycast addressing but has removed the concept of ~~dr~~broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto configured removes the dependability of Dyn Host configuration Protocol (DHCP) servers. This way, even if the DHCP server on the subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam arou without the need of changing their IP addres IPv6 is still in transition phase and is

Sub : _____ Day | | | | | | | |

Time : Date : / /

expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms avilable for IPv6 enabled networks to speak and roam around different networks easily on IPv4. There are :

i) Dual stack implementation
ii) Tunneling
iii) NAT-PT

Ans: to the ques: no: 08

(a)

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

i) The application Layer -

Provides applications with

Sub: Day Time: Date: / /

standardized data exchange. Its protocol include the HTP, FTP, Post office protocol 3 (POP 3), Simple Mail Tramfer Protocol (SMTP) and simple Network Management Protocol (SNMP). At the application layer, the payload in the actual application data.

ii) The transport layer -

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

Sub: Day Time: Date: / /

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

iv) The physical layer - also known as the network interface layer or data 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 Resulation Protoc (ARP)

Sub :

Day

Time : Date : / /

Answer to the ques no 08

(b)

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~~ stateless, which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continiously. The transport layer itself, however, is stateful. It transmits a single message and its connection remains in place untill all the packets in a message

Sub: _____ Day | | | | | | | |

Time: Date: / /

have been received and reassembled at the destination. The TCP/IP model differs slightly from the seven-layer Open System Interconnection (OSI) networking model designed after it. The OSI reference model defines how applications can communicate over a network.

Ans: to the ques: no: 08

(c)

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.

Sub: _____ Day | | | | | | | |

Time: Date: / /

The Internet Protocol suite is also compatible with all types of computer hardware and networks.

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