Name: Iqbal Hossen ID: IT-18041

1. (a) Briefly describe the Data link layer. 5

(b) Describe Functionality of Data-link layer. 9

2. (a) What is Data-link control? 2

(b) Explain Briefly Flow control and Error control mechanism. 8

(c) Service of Data-link Layer. 4

3. (a) Describe Simply Types of Errors. 4

(b) Explain the Error detection and Error correction. 10

4. (a) What do you mean by routeing and forwarding? 3

(b) What are the differences between multicast and Broadcast? 5

(c) Describe the functionalities and layer feature of network layer. 6

5. (a) what is DNS and IP address? 3

(b) why network addressing is important in Networking? 5

(c) Describe the following network Address. 6

(i) Unicast
(ii) multicast
(iii) Broadcast

6. (a) What do you mean by tunnelling? 3

(b) Different between IPV4 and IPV6. 5

(c) Why packet fragmentation is important in DCN 6

7. (a) What is Internetworking? 2

(b) What is classless addressing? 5
Given an example of classless IP Address

(c) What is the different between ARP and ICMP? 7

## Ans: to the qus. No: 01

(a)

**Question:**

Briefly describe Data link layer.

**Answer:**

- In the OSI model, the data link layer is a 4th layer form the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram, the datagram must be moved across an individual link.
- The main responsibility of the Data link layer is to transfer the datagram across an individual link.

☐ The Data link layer protocols are Ethernet token ring, FDDI and PPP.

☐ An important characteristic of a Data link layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by ethernet on the first link, ppp on the second link.

(b)

Question: Functionality 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 form 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 encoded into hardware at the time of manufacturing.

* Synchronization: When data frames are send 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 share.

Ans: to the qus: No: 02

(a)

Question: What is Data-link control?

Answer: Data link control is the service provided by the Data link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one devices can only transmit the data at a time. If both the devices at the end to the links transmit the data simultaneously, they will collide and leads to the loss of the information.

(b)

Question: Explain Briefly Flow control and error control mechanism.

Ans: Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

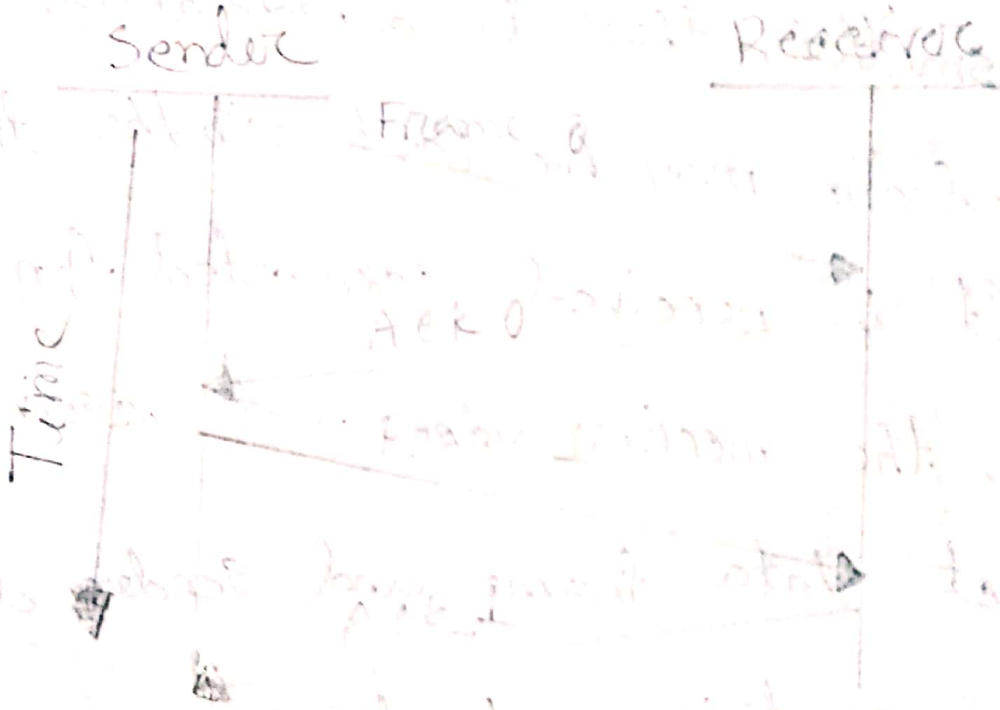
Flow control

When a data frame (layer-2 data) is sent from on host to another over a single medium, it is required that the sender and 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:

1. 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.




2. Sliding window:

In this flow control mechanism, both sender and receiver agree on the number

of data-frames after which the acknaledgement 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.

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 the cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.

## Requirment 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 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.

(c)

**Question:** Services of Data Link layer.

**Answer:** Services of Data Link layer are:-

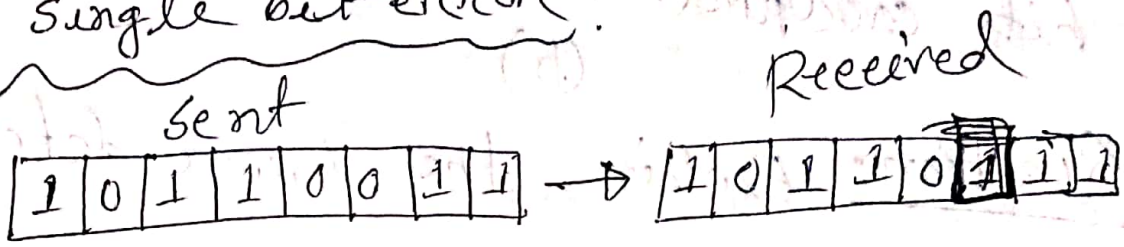
1) Framing and link access
2) Reliable Delivery
3) Flow control
4) Error detection
5) Error correction
6) Half-Duplex and full-Duplex

Ans. to the qus: No: 03 (a)

**Question:** Describe simply Types of Errors.

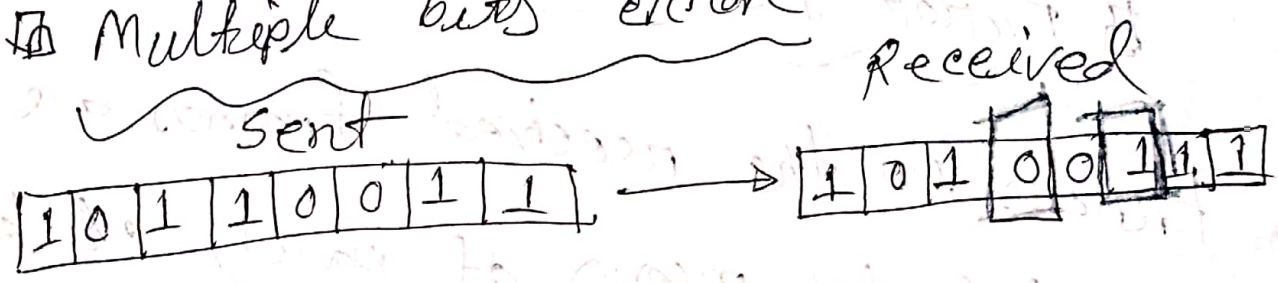
**Answer:** There may be three types of errors:

- **Single bit error:**



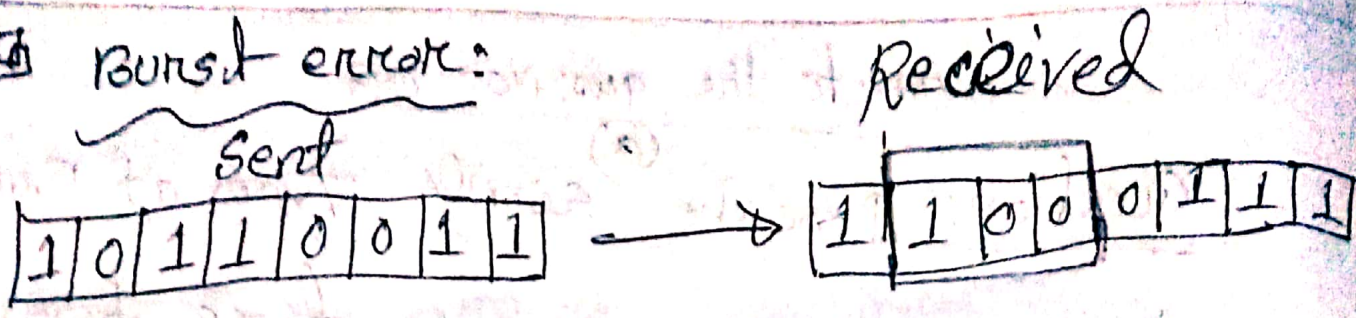

In a frame, there is only one bit anywhere though, which is corrupt

- **Multiple bits error**




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

Burst error:




Frame contains more than 1 consecutive bits corrupted.

(b)

Question: Explain the Error-detection and Error correction.

Answer:

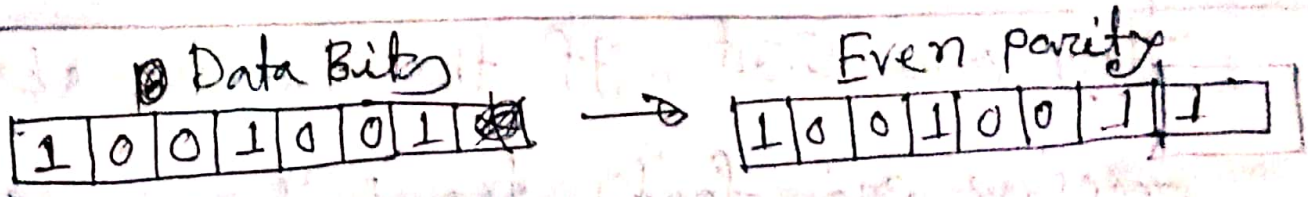
Error Detection

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 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 is odd, to make it even a bit with value 1 is added.

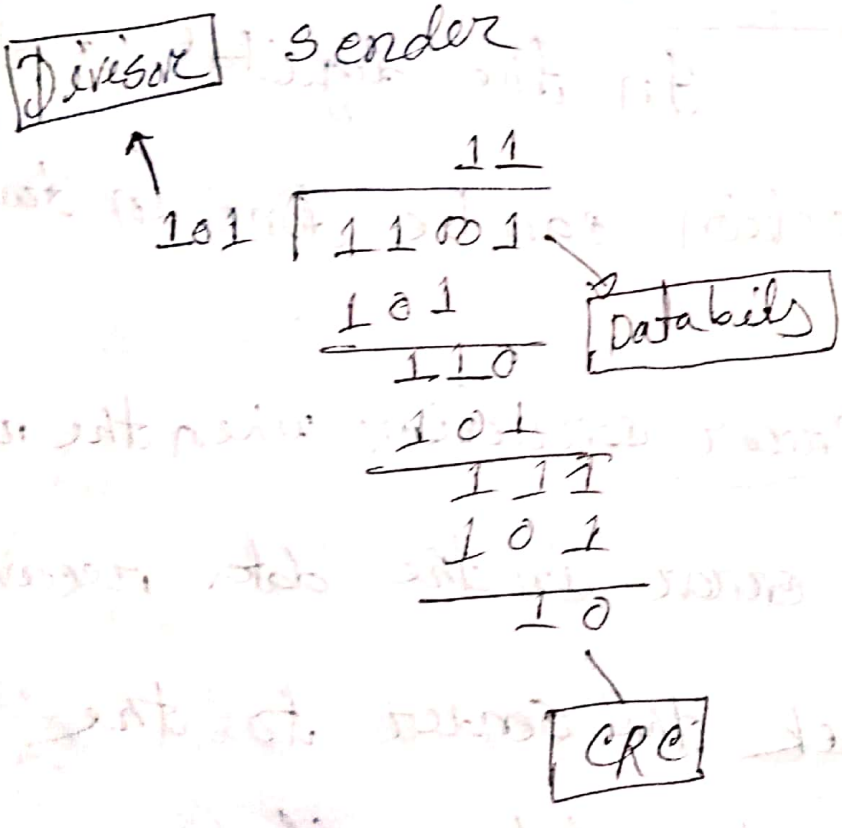


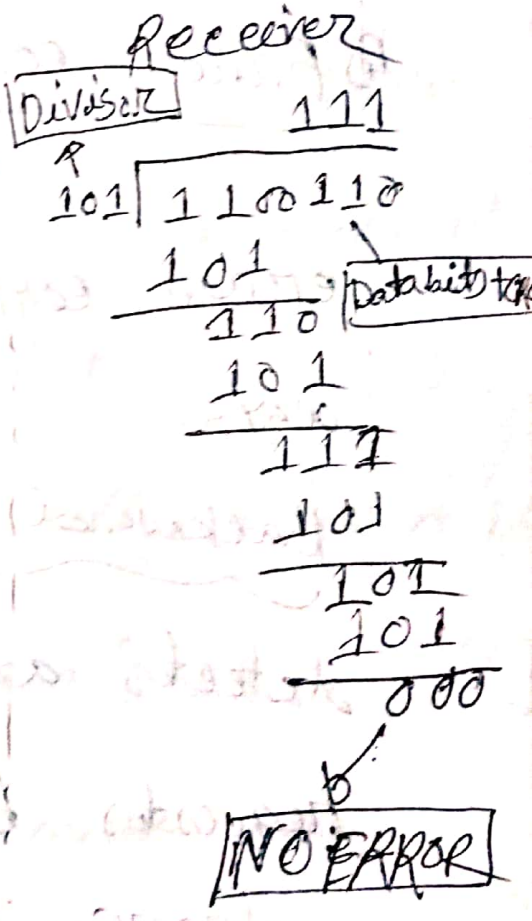

The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

## 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 sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bit plus the remainder is called a codeword. The sender transmits data bits as codeword



At the 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 occurred in transit.

4) Error correction:

In the 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 the 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 latter case, Forward Error correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in

error, redundant bits are used as parity bits for error detection.

For m data bits, r redundant bits are used. r bits can provided 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information i.e: m+r+1

$$2^r >= m+r+1$$

## Ans. to the qus. No: 04

(a)

**Question:** What do you mean by routing and forwarding.

**Answer:** Forwarding refers to the router-local action of transferring the packet from an input link interface to the appropriate output link interface.

Routing refers to the network-wide process that determines end-to-end paths that packets take from source to destination.

Using driving analogy, consider a trip from San Francisco to los Angeles. To differentiate between the two. Routing is the process of planning the whole trip from San

Francisco to los Angeles. i.e. the set route from San Francisco to Los Angeles. Forwarding on the other hand, can be considered as a process of getting through a single intersection. A car enters the interchange from one road and determines which road it should take to leave the interchange

(b)

Question: what are the different between multicast and Broadcast?

Answer: The different between multicast and broadcast are given below:

~~Ans to the question~~

| multicast | Broadcast |
|---|---|
| 1) The packet is transmitted only to intended recipients in the network. | 1) The packet is transmitted to all the hosts connected to the network. |
| 2) Transmission process is one-to-many | 3) Transmission process is one-to-all. |
| 3) Bandwidth is utilized efficiently. | 3) Bandwidth is wasted |
| 4) Traffic is under control | 4) Unnecessarily huge amount traffic is generated in the network |
| 5) Transmission speed is fast. | 5) Transmission speed is slow. |

(c)

Question: Describe the functionalities and layer features of network layer.

Answer: Devices which work on network layer mainly focus on routing. The functionalities of network are:

1) Addressing devices and network.
2) populating routing tables or static routes.
3) Queuing 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.

The layer features of network layer are:

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.

## Ans. to the que No. 05

(a)

Question: what is DNS and Ip address?

Answer: The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain

names, like nytimes.com or espn.com. 'IP' stands for Internet protocol which is the set of rules that makes it possible for devices to communicate over the Internet. With billions of people accessing the Internet every day, unique identifiers are necessary to keep track of who is doing what. The internet protocol solves this by assigning IP numbers to every device accessing the Internet.

(b)

Question: Network addressing is ~~one of the~~ important in networking?

Answer: 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 point 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 MAC address (hardware address or layer-2 address) of the machine for layer 2 communication.

(c)

Q: Describe the following Network Address.

1) Unicast
2) multicast
3) Broadcast

Answer:

(1) 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 router just has to look up the routing table and forward the packet to next hop.

(2) 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 ~~rece~~ receive the packets.

(3) 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. A broadcast

message is destined to all network devices.

## Ans: to the qus: No: 06

(a)

Q: What do you mean by tunnelling?

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

(b)

Question: Different between IPV4 and IPV6

Answer: The different between IPV4 and IPV6 are given below:

| IPv4 | IPv6 |
| --- | --- |
| 1) IPv4 has 32 bit address length | 1) IPv6 has 128-bit address length |
| 2) It supports manual and DHcp address configuration | 2) It supports Auto and renumbering address configuration |
| 3) In IPv4 end to end connection integrity is Unachievable. | 3) In IPv6 end to end connection integrity is Achievable |
| 4) It can generate 4.29x10 Address Space | 4) Address space of IPv6 is quite large it can produce 3.4x1038 address space |
| 5) security feature is dependent on application | 5) IPSEC is inbuilt security feature in the IPv6 protocol. |

(9)

Question: why packet fragmentation is important in DCN?

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 then or equal to the size of packet it can process. If the data packet

~~size~~ the transit network can handle. it is processed ~~not~~ neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contain 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 01 comes to a router the knows that is a fragmented packet and parts of the original packet is on the way. If packet is fragemented too small, the overhead is increases.

## Ans: to the qus: no: 07

(a)

**Question:** What is internetworking?

**Answer:** Internetworking is the practice of interconnecting multiple computer networks, such that any pair of hosts in the connected networks can exchange messages irrespective of their hardware-level-networking technology. The resulting system of interconnected networks are called an internetwork, or simply an internet.

(b)

Question: What is classless addressing? Given an example of classless IP Address.

Answer: To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, Subnet mask is found by putting the given number of bits out of 32 as 1, like

in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be ~~255.255.255~~ 255.255.255.240.

(c)

Question: what are the difference between ARP and ICMP

Answer: The difference between ARP and ICMP are given below:-

| ARP | Icmp |
| --- | --- |
| 1) ARP is a protocol used in a LAN to resolve the MAC address of the next or final destination IP | 1) An Icmp redirect message is typically used to notify routers of a better route |
| 2) An ARP MITM attack works by spoofing a MAC address within a LAN in response to victim's ARP request | 2) An ICMP MITM attack on the other hand is accomplished by spoofing an Icmp redirect message to any router that is in the path between |
| 3) If the MAC of the intended machine is successfully spoofed with the attackers machine, then the victim will send traffic to the | 3) It can be abused to effectively route the victim's traffic through an attacker controlled router. |