Name: Maskur Al Shal Sabil

ID : IT18021

Topic: Data Link Layer and Network

Course Code: ICT3207

Course Code: Computer Network

## Question NO 1

1(a) What is data link layer? Write down the sublayer of data link layer.

Ans 1(a) Data link layer is the second layer of OSI layered model after physical layer. When a packet or message reaches to a network, it is the responsibility of Data Link layer to transmit it to the Host using its MAC Address.

sublayers of Data Link layer are as follows:

(i) Logical Link control (LLC)

This is the uppermost sub-layer LLC consist of protocols running at the top of the data link layer. and also provides flow control, acknowledgement. and error notification. The LLC provides addressing and data link control. It specifies which methods are to be used for addressing channel over the transmission medium and for controlling the data exchanged between the generator of packet and recipent of the message.

(2) Media Access Control (MAC):
Who can access the media at any one time, determines by MAC sublayer.

Q 1 b What are the functionalities of data link layer?

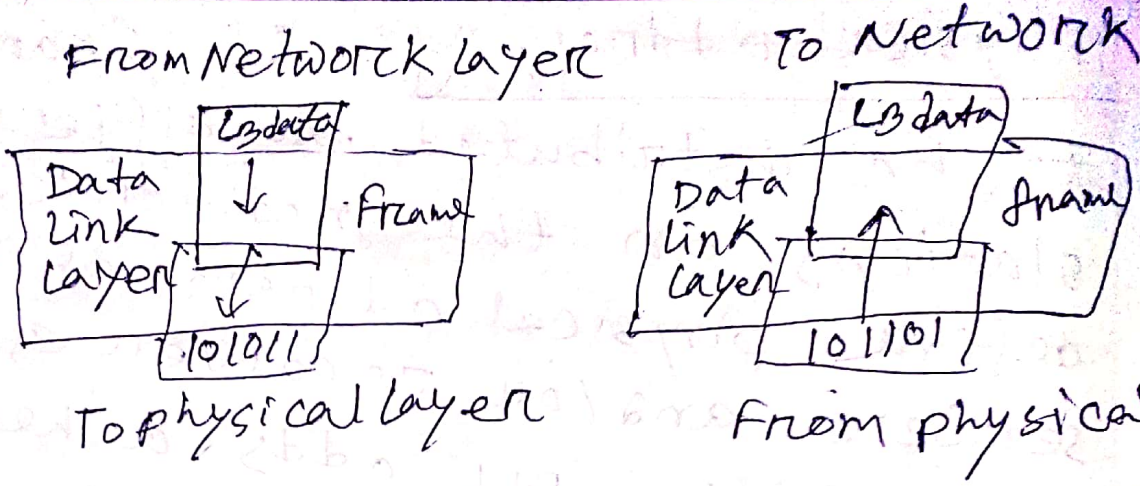
Ans 1b

The functionalites of Data link layer are given below:

Framing: The data link layer receives the stream of bits from the network layer divides into manageable data units called frame.

**Physical addressing:** If frames are to be distributed to different stations on the network, to define physical address of the sender and/or receiver of the frame, the DLL adds a header to the frame. If the frame is to be sent for a system outside the sender's network. The receiver address means the address of the device that connects one network to another.

The figure shows the relationship of the data link layer to the Network and physical layer:




Flow Control: If the rate at which the data are consumed by the receiver is less than the rate produced by the sender, the data link layer deals with a flow control mechanism to prevent overrun the receiver.

Error Control: The data link layer also deals with damaged or lost frames. By adding mechanisms to detect and retransmit lost frames increases reliability.

A trailer added to the end of the frame to achieve error control.

Access control: When more than two or two devices are connected to the common link, data link layer protocols are necessary to determine which device has control over the link at any point of time.

Q1c) How the flow control in data link layer handle?

Ans: There are basically two types of techniques being developed to control the flow of data.

(1) Stop and wait flow Control:

This Method is the easiest and simplest form of flow Control. In this method basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data. When acknowledgment is received, then only sender will send or transfer the next frame. This process is continued until sender transmits EOT (End of transmission) frame. In this method only one of frames can be in

transmission at a time. It leads to inefficiently. inefficiency. less productivity if propagation delay is very much longer than the transmission delay.

(2) Sliding Window flow Control:

This method is required where reliable in order delivery of packets or frames is very much need like in data link layer. It is point to point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer gets completed. In this method, sender transmits or sends various frames or packets before

receiving any acknowledgement. In this method both the sender and receiver agree upon total number of data frames after which acknowledgement is needed to be transmitted. Data link layer requires and uses this method that simply allows sender to have more than one unacknowledged packet in-flight at a time. This increases and improves network throughput.

Question 2

2 (a) What are the layer #2 devices? Write down the Data link layer protocol.

Ans: A layer 2 network device is a multiport device that uses hardware addresses, MAC address. to process and forward data at the data link layer 2. A switch operating as a network bridge may interconnect devices in a home or office. The bridge learns the MAC address of each connected device.

Some common Data link protocols are:

(i) Synchronous Data link protocol (SDLC): It is basically a Communication protocol of Computer.

(ii) High level data link protocol; HDLC is bassically a protocol

that is now assumed to be an umbrella under which many wide area protol sit.

(3) Serial line Interface protocol:
SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet.

(4) Point to point Protocol (PPP)-
PPP is protocol that is basically used to provide same functionality as SLIP.

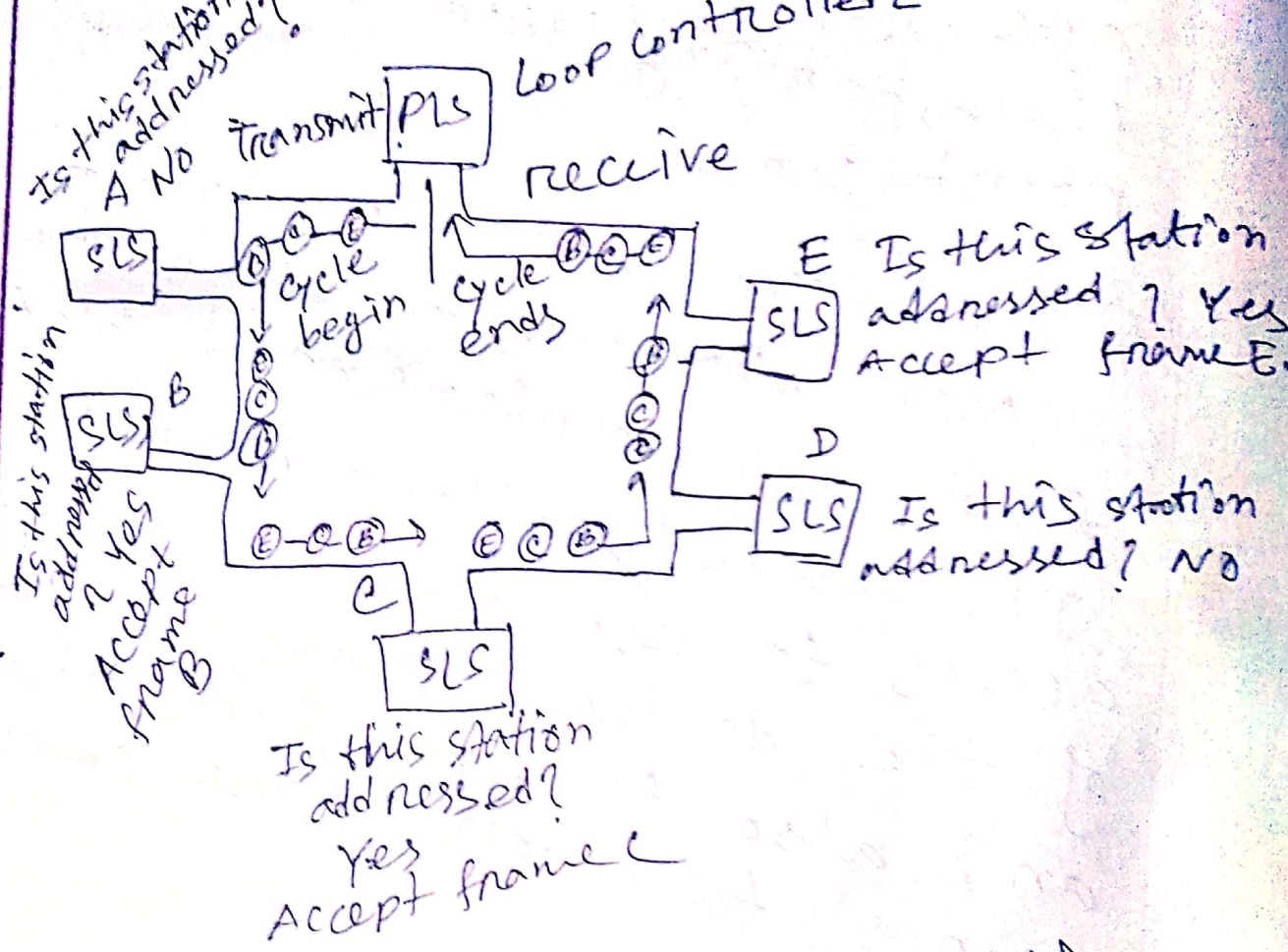
(5) Link Control Protocol - It was originally developed and created by IEEE 802.2. It is also used to provide HDLC style services on LAN (Local Area network)

(6) Link Access Procedure (LAP) -
LAP Protocols are basically a data link layer protocols that are required for framing and transferring data across point to point links.

(7) Network Control protocol -
NCP was also an older protocol that was implemented by ARPANET It basically allows user to have access to use computers and some of the devices at remote locations and also to transfer files among two or more computer.

2(b) Design and Demonstrate primary station transmitting in SDLC loop operation.

Ans




Here, PLS → Primary link station

SLS → Secondary link station.

Primary station basically transfer data frames or packets to one or more

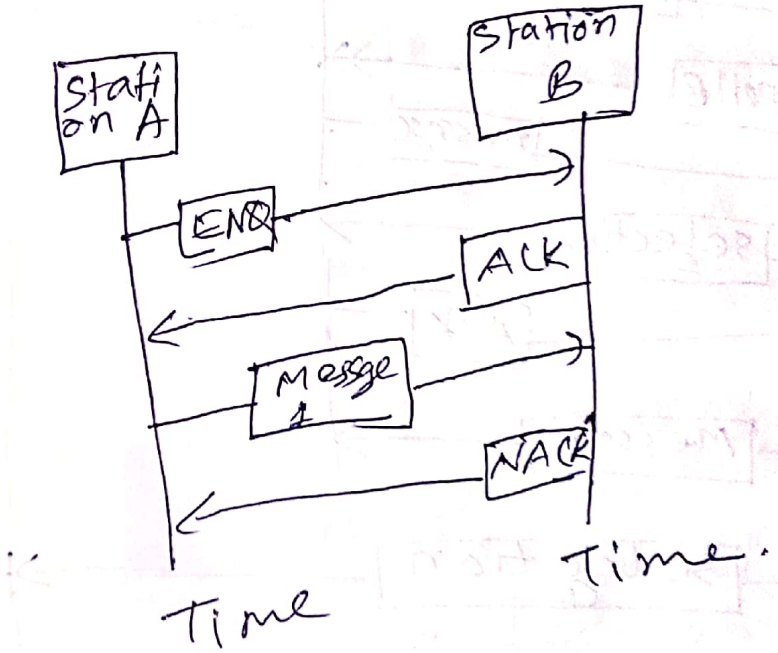
secondary stations, Each of the frames that is transmitted or transferred contains address of station to which the frame is directed. secondary station. When data frames get transmitted successfully by the primary station, it then follows the last flag of the last frame along with total eight consecutive logic 0's, known as turnaround sequence. and then followed by continuous logic 1. (01111)

2(c) How to achieve Line Discipline?

Ans: Line discipline is a function of Data Link layer. It simply identifies and determines the direction of communication.
There are basically two ways of doing line discipline as given below:

(1) ENQ/ACK (Enquiry/Acknowledgement)
ENQ/ACK is a procedure of line disciplining that is used to determine that which of device on network is capable of initiating or starting transmission of data or message and weather the receiver is ready and is capable to receive the data or not.

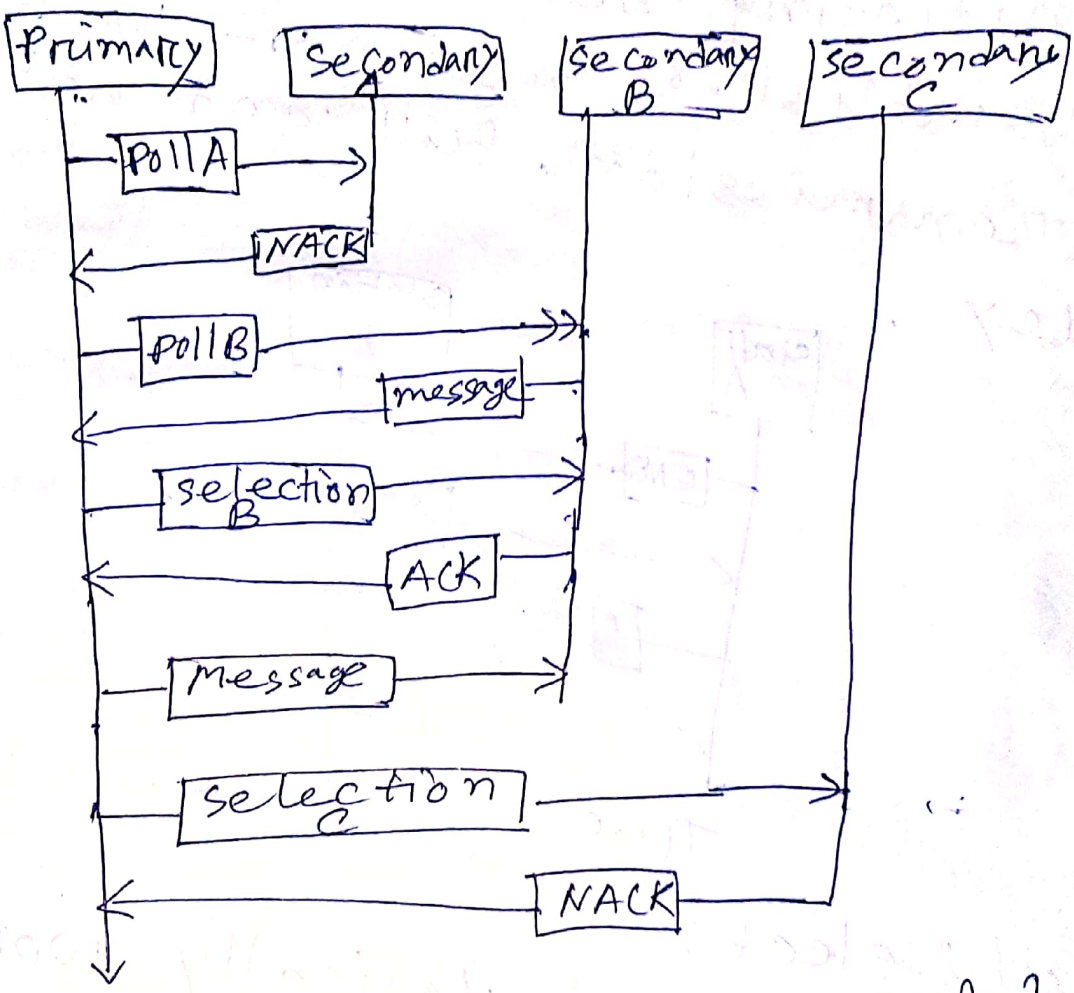
If the hosts have similar and equal ranks, then either of hosts or stations can initiate process of transmission. The initiating device generally establishes session in both transmission, full and half duplex.




(2) Poll/select:

The poll/select basically works with some topologies where one of device is considered as primary station and other devices are

considered as secondary station multipoint connection can be seen rather than two.




When primary station wants to transmit something to secondary station, downstream

then select mode is used. To solicit transmission from secondary to primary (upstream) then pull mode is used. The primary device basically controls and handles link or connection and on the other hand, secondary device simply follows its instruction.

## Question No 3

3(a) What is ARP?

Ans: Address Resolution Protocol (ARP) is a procedure for mapping a dynamic internet protocol address to a permanent physical machine address in a local area network ~~lan~~ LAN. The physical machine address is also known as a media Access control or MAC

address. The job of the ARP is essentially to translate 32 bit addresses to 48 bit addresses and vice versa. This is necessary because in IP version 4 (IPV4) the most common level of Internet protocol in use today, an IP address is 32 bits long but MAC addresses are 48 bits long. ARP works between network layers 2 and 3 of the open systems Interconnection model (OSI model). The MAC address exist on layer 2 of the OSI model, the data link layer while the IP address exists on layer 3, the network layer. IPV6 which uses 128 bit addresses

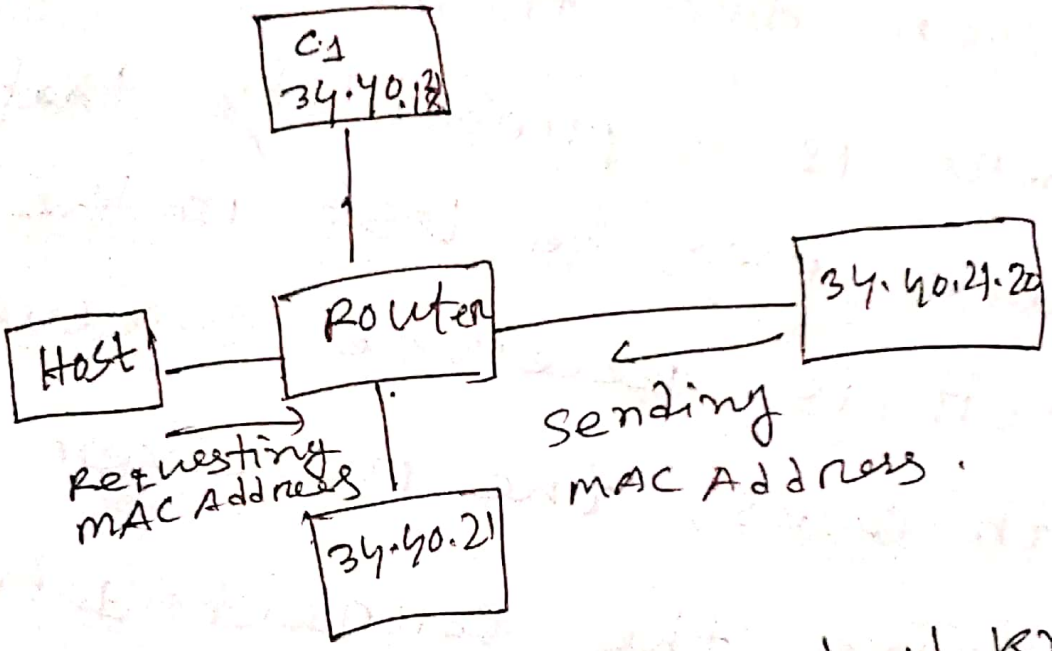
ARP has been replaced by the Neighbor Discovery protocol.

3(b) How ARP works?

Ans: When a new Computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. All operating systems in an IPV4 Ethernet network keep an ARP cache. Every time a host requests a MAC address

in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does then a new ARP request is unnecessary. If the translation does not already exist, then the request for network address is sent and ARP is performed. ARP broadcast a request packet to all the machine on the LAN and asks if any of the machine knows they are using that particular IP address. When a machine recognizes the IP address as its own, it sends reply so ARP can update the cache for future

reference and ~~future~~ proceed with the communication.




Host machine that don't know their own IP address can use the Reverse ARP. protocol for discovery.

3(c) Explain the Error control with one of its technique.

Ans: 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 doesn't 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.

Requirements for error control

mechanism:

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

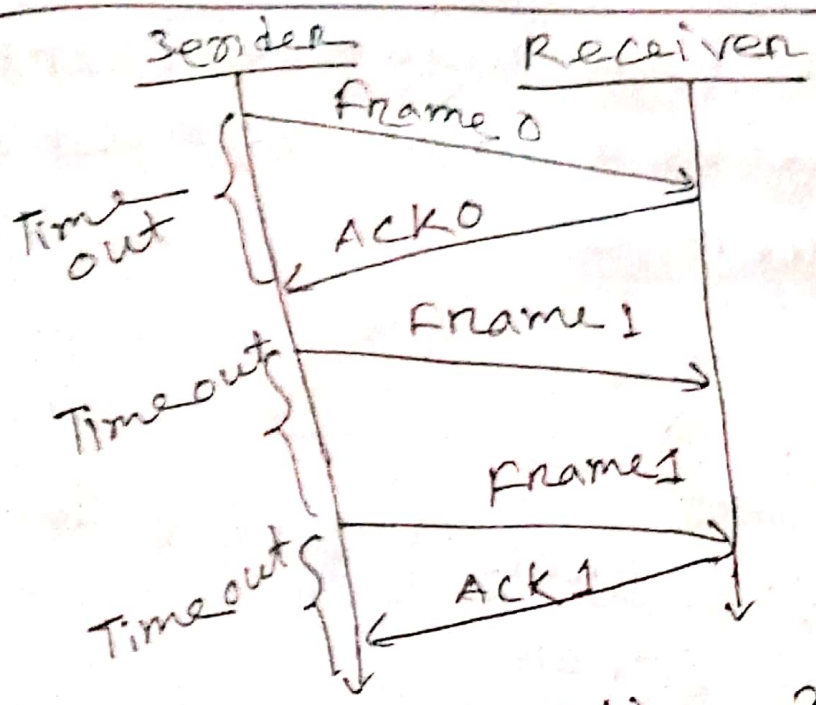
(2) Positive ACK - When the receiver receives a correct frame, it should acknowledge it.

(3) 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 correct frame.

(4) Retransmission: The sender maintains a clock and sets a time out period. If an

acknowledgement of a data previously transmitted does not arrive before the timeout the sender retransmits the frame thinking that the frame or its acknowledgement is lost in transit.

There are three types of techniques available which Data link layer may deploy to control the errors by Automatic Repeat Requests (ARQ: Here the stop and wait ARQ is given below:




The above transition may occour in stop and wait ARQ:

(1) The sender maintains a timeout counter.

(2) When a frame is sent the sender starts the time out counter.

(3) If acknowledgement of frame comes in time the sender assumes that the frame or its acknowledgement is lost in transit. sender retransmit the frame and starts the timeout counter.

(c) If a negative acknowledg is received, the sender retra the frame.

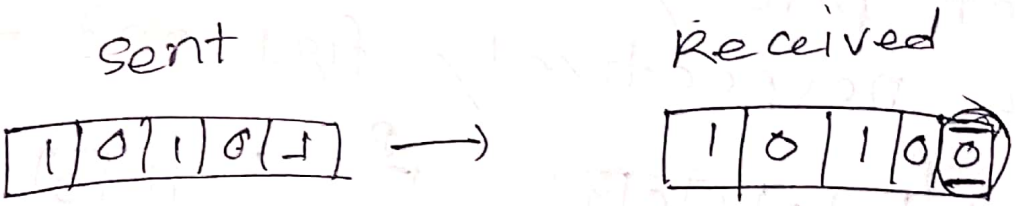
## Question 4

(4 a) What is ERROR? Write down the types of error.

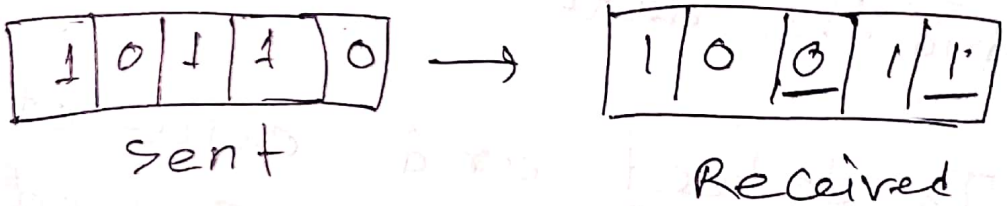
Ans: Error is a condition when the output information does not matc with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0. there may be three types of

errors :

(1) single bit error

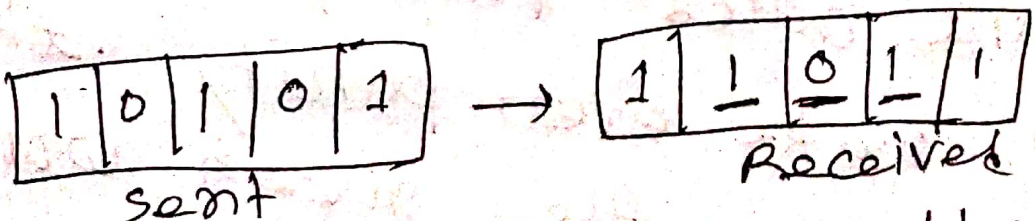



(2) Multiple error:




Frame received with more than one bits in corrupted state.

(3) Burst error.




Frame contains more than 1 consecutive bits corrupted.

4(b) Define parity bits. Construct even parity and odd parity for respectively fig1 and fig2.

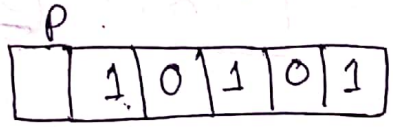



fig 1

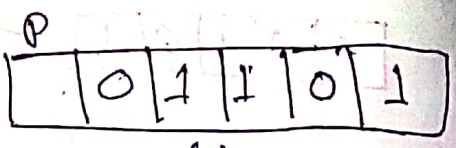


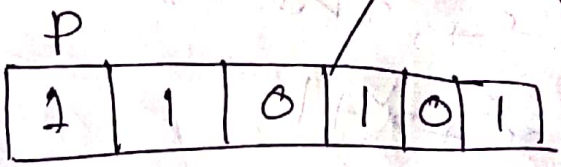

fig2

find the data bits from the above fig.

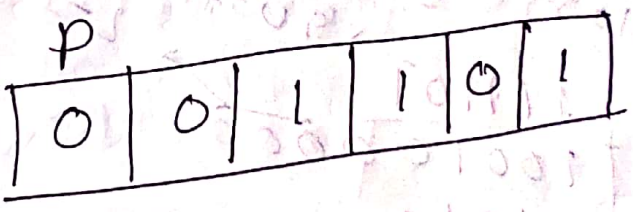
Ans: To detect and correct errors additional bits are added to the data bits at the time of of transmission. The additional bits are called parity bits.

To make even parity the number of 1's in the given word including the parity bit should be even. so for figure-1 there are three 1 which is ~~even~~ odd so to make even parity we must put 1

as the parity bit.




To make odd parity the number of total 1 in the word must be odd. So here the number of 1 is already odd. So we dont need to set 1 as parity bit. In this case parity bit will be 0.




4(c) Find the CRC for the data blocks 100100 with $x^3+x^2+1$ ?

Any; CRC generation at sender side.

1. Find the length of the divisor i.e. L.
2. Append L-1 0's bit to the original message.

3. So here the Divisor is

$$x^3+x^2+1$$

$$x^3+x^2+x+1$$

1 1 0 1

Divisor : 1101 and length is 4

(3) Now perform binary division operation.

(4) Finally the Reminder of the division = CRC

Now start,

```
          11101   → quotient
1101 | 100100000  → 4-1 bits added
       1101
       ----
        1000
        1101
        ----
         1010
         1101
         ----
          1110
          1101
          ----
           0110
           0000
           ----
            1100
            1101
            ----
             001  → CRC
```

so the reminder is 001 which is the CRC.

## Question 5

5(a) What is Error Correction? Differentiate between Layer2 and Layer3 switch:

Ans: Error correction is the process of detecting errors in transmitted message and reconstructing the original error free data. Error correction ensures that corrected and error free message are obtained at the receiver side.

The difference between Layer2 and Layer3 switches are as follows:

| Layer 2 switch | Layer 3 switch |
| --- | --- |
| Operate on Data link layer of OSI | Operate on Network layer of OSI |
| Send frames on the basis of MAC address | Route packet with help of IP address |
| Work with MAC address only | Can perform functioning of both 2 layer and 3 layer switch |
| It has single broadcast domain | It has multiple broadcast domain |
| Can communicate within a network only | Can communicate within or outside network |

4(b) How many way's error can be corrected. Check weather the message 1100110 is corrupted or not when Divisor is 101.

Ans: Error Correction can be done in two ways:

(1) Backward error correction: when the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

(2) forward error Correction: when the receiver detects same error in the data received, it executes error correcting ~~coding~~ code, which helps it to auto-recover and to correct some kinds of errors.

So to check the correctness of the word we use cyclic Redundancy check..

```
        1111
    ---------
101 | 1100110
      101
    ---------
       110
       101
    ---------
        110
        101
    ---------
         101
         101
    ---------
           000
```

Hence the reminder is zero the word is correct.

5(c) Why do we need ARQ?

Ans Automatic Repeat Request is a group of error-control protocol for transmission of data over noisy or unreliable communication network. These protocols reside in the data link layer and in

the transport layer of the OSI (Open System Interconnection) reference model. They are named so because they provide for automatic retransmission of frames that are corrupted or lost during transmission. ARQ is also called positive acknowledgement with Retransmission (PAR). ARQs are used to provide reliable transmission over unreliable upper layer services. They are often used in Global System for Mobile Communication. (GSM). So that ARQ's is an important part in computer Network.

## Question NO: 6

6(a) What is the main function of the Network layer?

Ans: The role of the Network layer is to enable any two open system anywhere to exchange data with one another, irrespective of the types of network the two system are attached to and of the means of interconnecting two networks. With this basic communications facility it achieves half of the dream of OSI; the other half using that communications faciulty in an appropriate way to support distributed processing.

is the task of the transport and higher layers of OSI. The Devices which work on Network layer mainly focus on routing. And routing may include various task aimed to achieve a single goal. These can be:

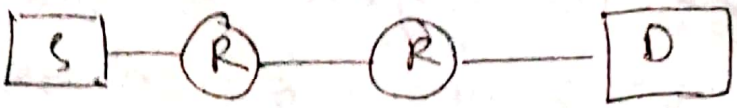
(1) Addressing devices and Networks.

(2) Populating routing or static routes.

(3) Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packet.

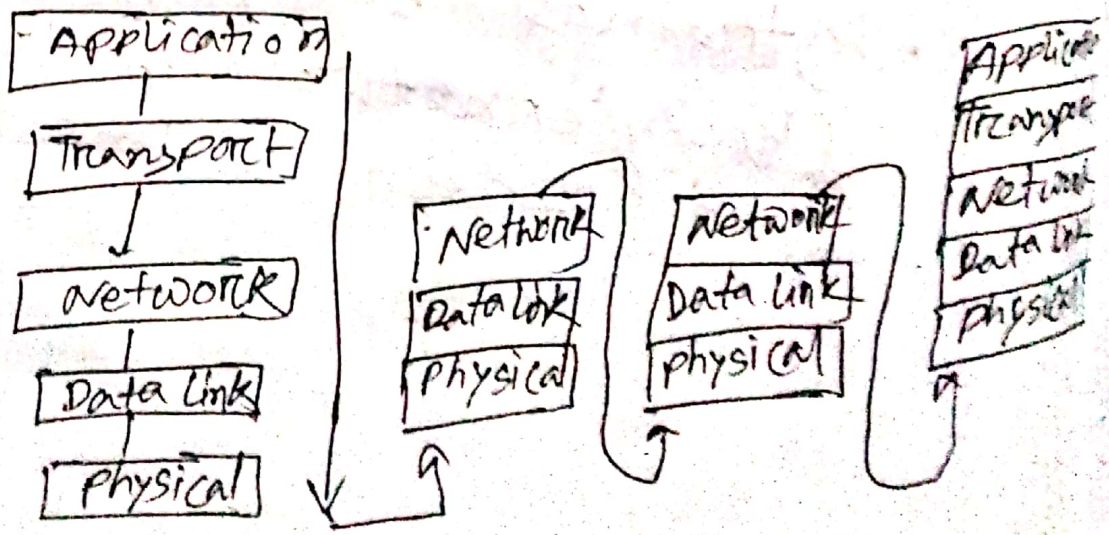
(4) Internetworking between two different subnets.

6(b) Consider the figure below:




Assume that source S and destination D are connected through two intermediate routers labled R. Determine how many times each packet has to visit the network layer and the data link layer during transmission from S to D.

Ans: Router is a Network layer device. So the packet send will be:



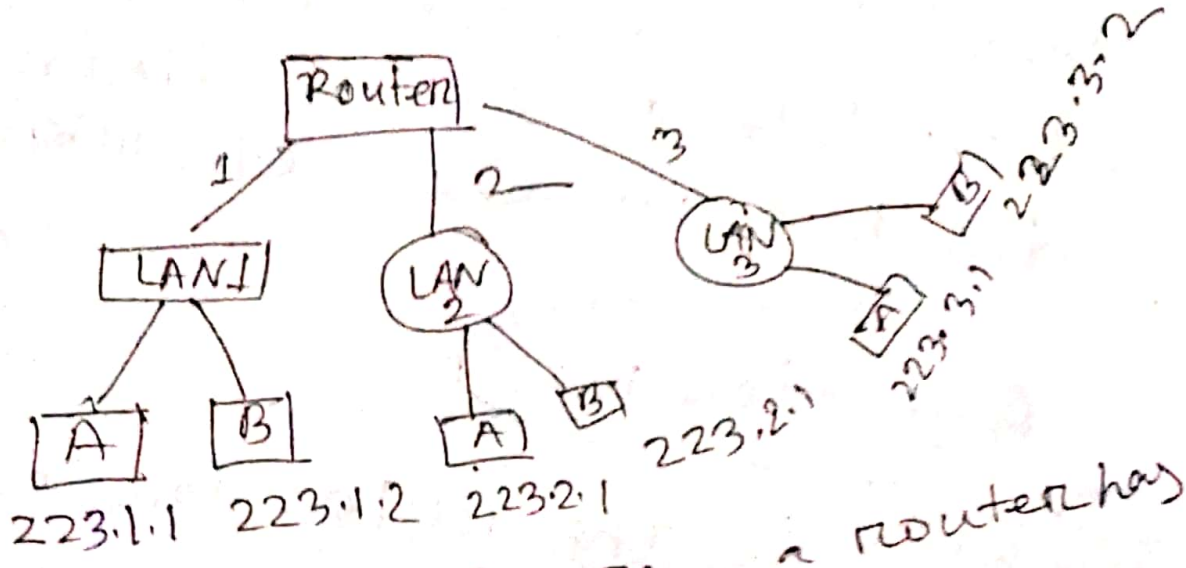
So here every packet passes twice through data link layer of every intermediate router. So it has to visit Network layer 4 times and ~~Data~~ link layer 6 times.

6(c) Explain Network Address in details.

Ans: Network Addressing is one of the major responsibilities of the network layer. Network addresses are always logical, software based addresses. A host is also known as end system that has one link to the network. The boundary between the host and link is known as interface. Therefore

the host can only have one interface. A router is different from the host in that it has two or more links that connect to it. When a routers forward a datagram it forwards the packet to one of the links. Each Interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address. Each IP address is 32 bit long, and they are represented in the form of a dot-decimal notation where each byte is written in decimal form. An IP address look like 193.32.216.9

lets take an example.




In the above figure, a router has three interfaces labled as 1, 2 & 3 each router & contains its own IP address. Each host contains its own interface and IP address.

All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xx Each IP address consists of two parts

The first part (first three bytes) specifies the network and second part (last byte of an IP address) specifies the host in the network.

## Question No 7

7(a) What is the rules for assigning Host ID and Network ID?

Ans The Host ID is determine the host within any network. The Host ID is assigned based on the following rules

(1) The Host ID must be unique within any network.

(2) The Host ID in which all the bits are set to 0 can not be assigned as it is used to represent the network ID of the IP address

(3) The host ID in which all the bits are set to 1 can not be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:
If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning network ID:

(1) The network ID can not start with 127 as 127 is used by class A.

(2) The network ID in which all the bits are set to 0 can not be assigned as it is used to specify a particular host on the local network.

(3) The network ID in which all the bits are set to 1 can not

be assigned as it is reserved for the multicast address.

7(b) Explain classful Addressing in details

Ans: An IP address is a 32 bit unique address having an address space of $2^{32}$. The IPv4 addressing system ~~System~~ is divided into five classes of IP address. The dotted decimal notation of IP Address-

1st octet 2nd octet 3rd octet 4th octet

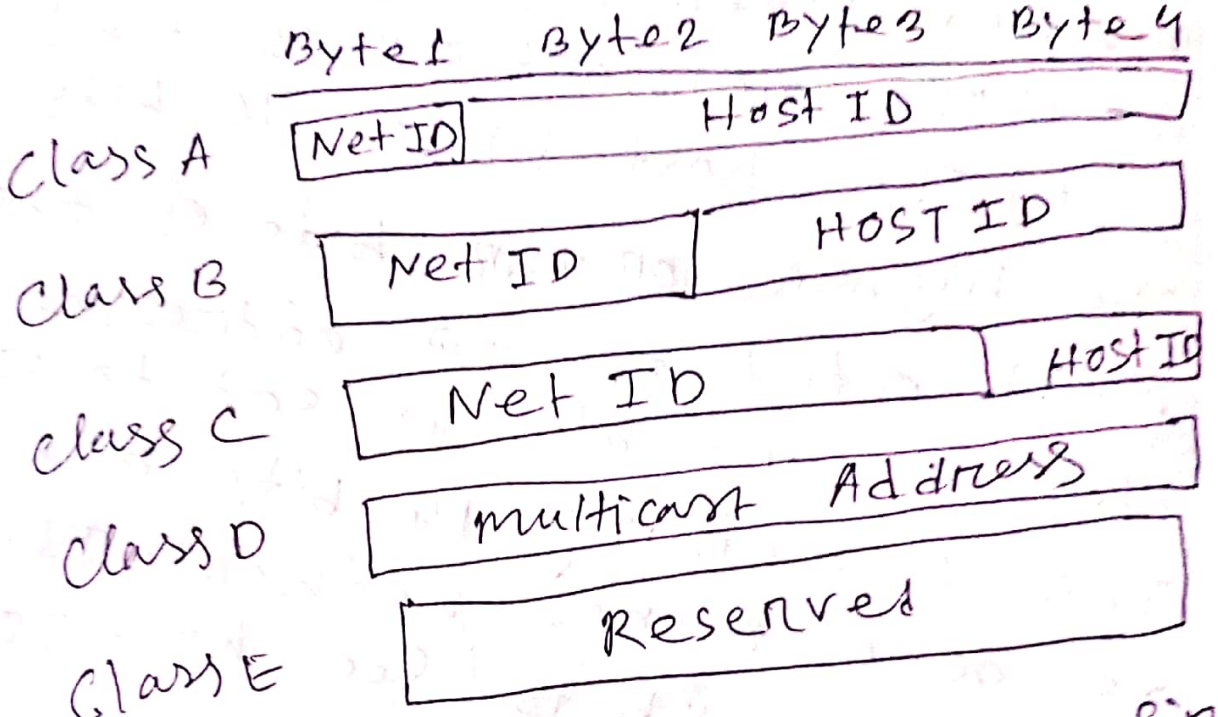
11000000. 10101000. 10011000. 10011000

192 168 152

All the five classes are identified by the 1st octet. The number of networks and number of hosts per class can be derived by this formula-

Number of networks = $2^{\text{network bits}}$

Number of Hosts/Network = $2^{\text{Host\_bits}} - 2$




Class A: The first bit of the first octet set to be 0. Thus the remaining 7 bits used to determine network ID. Class A has total of: $2^7 - 2 = 126$ network ID (Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address)

$2^{24} - 2 = 16,777,214$ Host ID.

Class B : Class B are assigned to the networks that ranges from medium-sized to large sized networ

(1) The network ID is 16 bits long

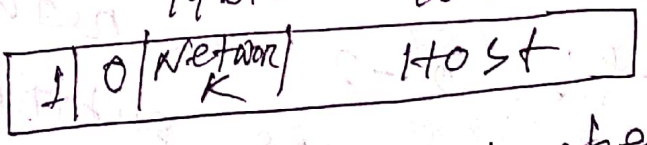
(2) The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. and remaining 16 bits for host ID. Class B has total of :

$2^{14} = 16384$ network address.

$2^{16} - 2 = 65534$ host address.

14 bit 16 bit




Class C : IP address belonging to ClassC are assigned to small sized networks. the network ID is 24 bits long. The host ID is 8 bits long.

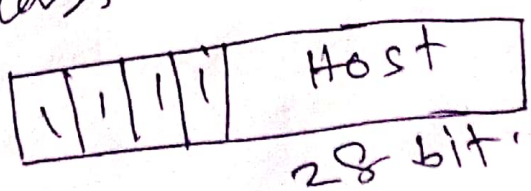
The higher order bits of the first octet of IP addresses of Class C are always set to 110. Remaining 21 bits are used to determine network id. Class C has total of: $2^{21}$ network ID and $2^8 - 2$ Host ID.

Class D: Class D's MSB set to 1110.

~~So the class D has total of $2^{20}$ network ID and~~

Class D are reserved for multicasting the remaing bits are for the address that interested to recognize. host.

Class E: IP address belonging to class E are reserved for experimental and research purpose. The higher order bits of first octet of class E are always set to 1111.



(XC) If a class B network on the internet has a subnet mask of 255.255.248.0, What is the maximum number of hosts per subnet?

Ans: The binary representation of subnet mask is 11111111.11111111.11111000.00000000
There are 21 bits set in subnet.
So left bit 32-21 = 11 bits for host id. Now total possible values of Host ID is $2^n - 2$

$$= 2^{11} - 2$$
$$= 2048 - 2$$
$$= 2046$$

## Question NO: 8

8(a) What is routing? Differentiate between Adaptive and Non-Adaptive Routing algorithm.

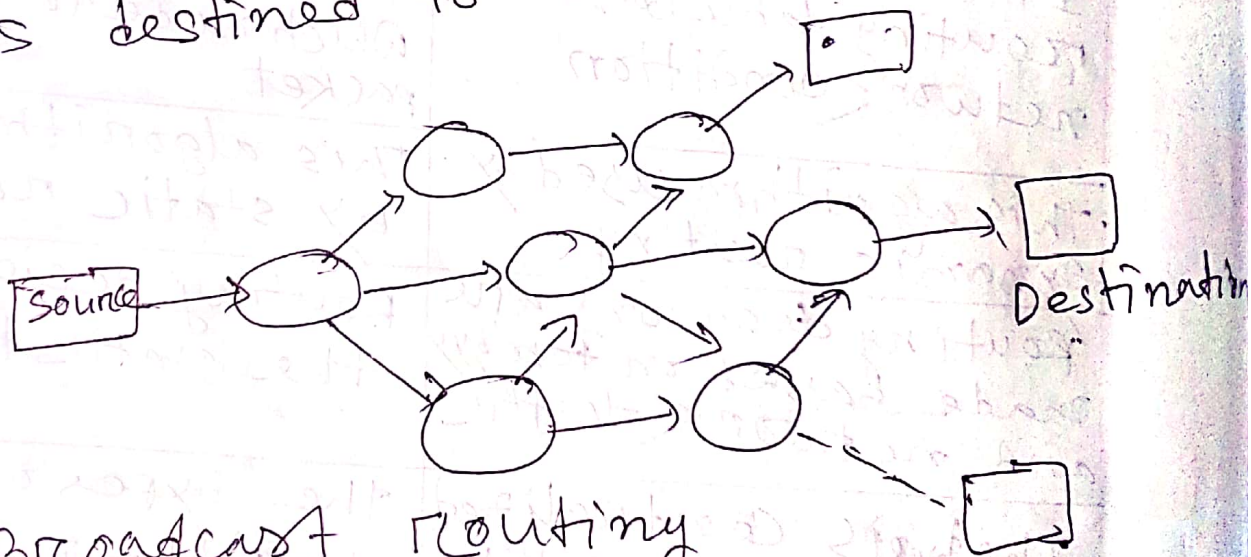
Ans: Routing is a process of selecting path along which data can be transferred from source to destination.

Difference between Adaptive and non Adaptive algorithm are as follows:

| Adaptive Routing algorithm | Non-Adaptive routing |
|---|---|
| It Constructs the routing table based on network condition | It Constructs static table to determine which node to send the packet |
| This algorithm used by dynamic routing | This algorithm used by static routing |
| Routing decisions are made based on topology and network traffic | Routing decisions are the static table. |
| The types is centralized, isolation and distributed. | The types of this algorithm is flooding and random walks |
| Adaptive algorithm are more complex | Non adaptive algorithm are simple |

8(b) Explain Broadcast Routing in details.

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




Broadcast routing can be done in two ways -

(1) A router creates a packet and then sends it to each host

one by one. In this case the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it ~~sti~~ simulates as if router is broadcasting. This method consumes lots of bandwidth and router must destination address of each node.

Secondly, when router receives a packet that is to be broadcast, it simply floods those packets out of all interfaces. All routers are configured in the same way.

8(c) What is static Routing? Write down the pros and cons of static Routing.

Ans: Static Routing: Static Routing is also known as Nonadaptive Routing. It is a technique in which the administrator manually adds the routes in a routing table. A router can send the packet for the destination along the route defined by the administrator. In this technique, routing decisions are not made based on the condition or topology of the networks.

Advantage of Static Routing:

* (1) No overhead: It has no overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain

Static routing.

Bandwidth: It has not bandwidth usage between the routers.

Security: It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantage of static routing:

for a large network, it becomes a very difficult task to add each route manually to the routing table.

The system administrator should have a good knowledge of a topology as he has to add each route manually.