1. a) What is Data link layer?
b) How to work Data link layer?
c) Write down functionality of Data link layer.

2. a) Why occur DCN error?
b) What types of error occur DCN?
c) How to detect error in DCN?
d) How to correct error in DCN?

3. a) What is flow control?
b) Write down the mechanism of flow control?
c) Write down the steps Data-link layer may deploy to control the errors by ARQ.
d) Write down the mechanism of error control.

4. a) What do you mean network layer?
b) Write down the layer-3 functionlity.
c) Write about network layer features.

5. a) what is network addressing?
b) write down the different types of network addressing.
c) write down the point where the routers take help of routing tables.

6. a) what is Broadcast routing?
b) write down the mechanussum the Broadcast routing
c) Routers how can make decision based on?

7. a) write down short notes:
i) Unicast routing ii) multicast routing
iii) Anycast routing
b) write about Routing Algorithms.

8. a) write about Address Resolution Protocol.
b) write a short note about Packet Fragmentation.

Answer to the Question no: 1 (a)

Data link layer is second layer of OSI layered model this layer is one of the most complicated layer 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 communi

Answer to the Question no: 1 (b)

Data link layer works between two hos which are directly connected in some sense. this direct connection could be point to point or broad cast. system 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 multipule hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the

underdying hardware. At the receiving end Data link layers picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format and hands over to uppers layers.

Answers to the Question no: 1 (c)

Data link layers does many tasks on behalf of uppers layers. These are:

framing:

Data-link layers takes packets from network layers and encapsulates them into frames. Then, it sends each frame bit-by-bit on the hardware.

Addressing:

Data-link layers 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 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.

Mult-Access:

When host on the shared link tries to transfer the data. It has a high probability of collision.

Answer to the Question no: 2 (a)

There are many reasons such as noise cross-talk etc. which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual Hardware data processing. The upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Answere to the Quation no: 2 (b)

There may be three types of errors.

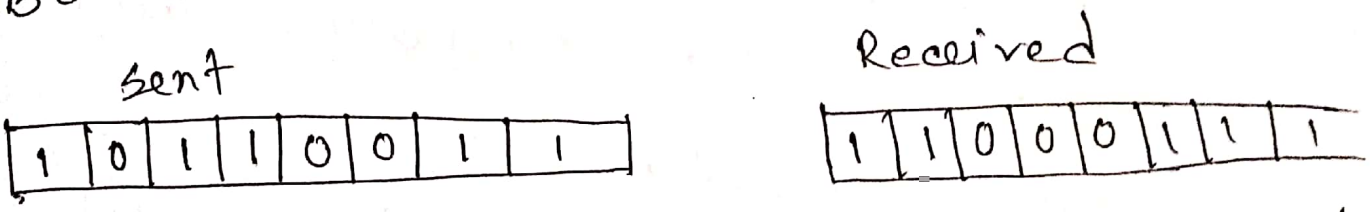
Single bit error:

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

Multipule bit error:

Frame is received with more than one bits in corrupted state

Burst error:



Frame contains more than 1 consecuti. bits corrupted.

Answer to the Question no: 2 (c)

Error control mechanism may involve two possible ways.

* Error detection
* Error correction

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:

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.

Data Bits

1	0	0	1	0	0	1

Even Parity

1	0	0	1	0	0	1	1

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. If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are error reous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy check (CRC)

Sender

```
101 ) 1100 1
      101
      ---
       110
       101
       ---
        111
        101
        ---
         10
```

Receiver

```
101 ) 1100110
      101
      ---
       110
       101
       ---
        111
        101
        ---
         101
         101
         ---
          000
```

Answere to the Question no: 2 (d)

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 transmit 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 fruist one, Backward Error correction is simple and can only be effficiently used where retransmitting is not expensive for example fiber optics. But in case of wireless tranmission retransmitting may cost too much. In the latter case, Forward Error correction is used.

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

Answere to the Question no: 3(a)

Flow control:

When a data frame 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 of the sender or receiver differs.

Answere to the Question no: 3 (b)

Two typer of mechanism forces the sender after transmitting a data frame to stop 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 untill the acknowledement 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.

Answere to the Question no: 3 (b)

The following transition may occure in stop-and-wait ARQ:

* the sendere maintains a timeout counter.
* when a frame is sent, the sendere starts the timeout counter.
* If acknowlegement of frame comes in time, the sendere transmits the next frame in queue.
* If acknowledgement does not come in time, the sendere assumes that either the frame or its acknowledgement is lost in transit. sendere retransmits the frame and starts the timeout counter.
* If a negative acknowledgement is received, the sendere retransmits the frame.

Answer to the Question no: 3(c)

In 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 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 correct 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.

Answer to the Question no: 4(a)

Network layer:

Network layer taker 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.

Answer to the Question no: 4(b)

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

- Addressing devices and networks.
- Populating routing tables in static routers.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraint

set for those packets.

- Internetworking between two different subnets.
- Delivering packs to destination with best efforts.
- Provider connection oriented and connection less mechanism.

Answer to the Question no: 4 (c)

Network Layer Features:

With its standard functionalities, layer 3 can provide various features are:

- Quality of service management
- load balancing and link management
- security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.

Internet protocol is widely respected and deployed Network layer protocol which helps to communicate end to end devices over the ~~the~~ internet. It comes in two flavors. IPv4 which has ruled the world for decades but now is running out of address space. IPv6 is created to replace IPv4 and hopefully mitigates limitations IPV4 too.

Answer to the Question no: 5 (a)

Network addressing:

A network address always points to host 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.

Answer to the Question no: 5 (b)

There are different kinds of network addresses in existence.

1. IP
2. IPX
3. AppleTalk

We are discussing IP here as It is the only one we use in practice these days.

IP addressing Provides mechanism to differentiate between hosts and network. Because IP address 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 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 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.

Answere to the Question no: 5 (c)

Routers take help of routing tables which have the following information. i-

⇒ Method to reach the network.

Routers upon receiving a forwarding request, forwards packet to its next hop to 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.

Unicast
Multicast
Broadcast
Anycast

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.

Answer to the Question no: 6(a)

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.

Answer to the Question no: 6(b)

Broadcast routing can be done in two ways (algorithm).

- A router creates a data 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 address. All packets are sent as unicast but because they are sent to all, it 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 broadcasted, It simply floods those packets out of all interfaces. All routers are configured in the same way.

This method is easy on router's CPU but may cause the problem of duplicate Packets recived from peer routers.

Reverse path forwarding is a technigu in which router knows in advice about its predcessor from where it should recived broadcast. This technique used to detect and discard duplicates.

Answer to the Question no: 6(c)

Routers can make decision based on the following information:

* Hop count
* Band width
* Metric
* Prefix-length
* Delay.

Answer to the Question no: 7(a)

Unicast routing:

Most of the traffic on the internet and intranets know as unicast data or unicast traffic is sent with a 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.

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 known 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 Path Forwarding technique to detect and discard duplicates and loops.

Anycast routing:

Anycast packet forwarding is a mechanism where multiple host 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 packets 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.

Answer to the Question no: 7 (c)

Routing Algorithms:

The routing Algorithms are as follows:

Flooding:

Flooding is simplest method Packet of 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 decision in networks are mostly taken on the basis of cost between source and destination. Hop count plays major role here. shortest path is a technique which uses various algorithms to decide a path with minimum number of hops.

common shortest path algorithms are:

* Dijkstra's Algorithm
* Bellman Foard algorithm
* Floyd warshall algorithm

Answer to the Question no: 8(a)

Address Resolution Protocol:

while communicating a host needs layer-2 address of the destination machine which belongs to the same broadcast domain network. A MAC address is physically burnt into the network Interface card of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed If the NIC is changed in case of some fault. MAC address also changes. this way, for layer-2 communication to take place, a mapping

between the two is required. To know the MAC address of remote

Answer to the Question no: 8(b)

If the data packet size is less than or equal to the size of packet the network can handle. It is processed neutrally. If the packet is larger. It is broken into smaller pieces and then forward. This is called 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 bit set to 1 comes to router which can not handle the packet because of its length, the packet is dropped.