## 1. Differentiate between Link State routing and Distance vector routing algorithms.

BASIS FOR COMPARISON	DISTANCE VECTOR ROUTING	LINK STATE ROUTING
Algorithm	Bellman ford	Dijsktra
Network view	Topology information from the neighbour point of view	Complete information on the network topology
Best path calculation	Based on the least number of hops or delay.	network topology
Updates	Full routing table	Link state updates
Updates frequency	Periodic updates	Triggered updates
Simplicity	High simplicity	Requires a trained network administrator
Convergence time	Moderate	Fast
Updates done on	On broadcast	On multicast
Application	RIP, IGRP	OSPF, ISIS
Count to infinity problem	Yes	No
Flooding	No, so less bandwidth required comparatively.	Yes, so more bandwidth required

Distance vector Routing-
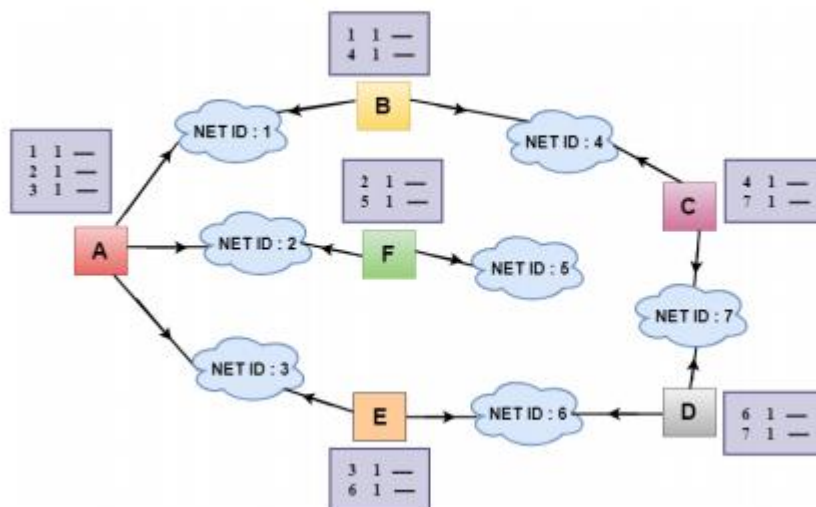
Link State Routing-
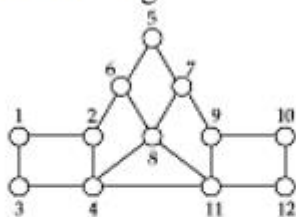
ROUTING TABLE AT 1

Destination	Next hop	Destination	Next hop
1	—	7	2
2	2□	8□	2□
3	3□	9□	2□
4	3□	10□	2□
5	2□	11□	3□
6	2	12	3

<mark>**2 Explain connection-oriented and connectionless services with the help of a suitable example.**</mark>

Connection Oriented Service

Theory and Working-

The following sequence of operation to be followed by the users of connection-oriented service-

Connection is established.

Information is sent.

Connection is released.

In connection-oriented service we have to establish a connection before starting the communication, that is, path from source router to destination router has to be established before any data packets can be sent. This connection is called a VC (Virtual Circuit) and subnet is called Virtual-Circuit Subnet.

When connection is established, we send the message or the information and then we release the connection. The idea is to avoid having to choose a new route for every packet sent. Instead when a connection is established, a route from source to destination is chosen as a part of connection setup and stored in tables inside the routers. The route is used for all the traffic for that particular connection. When the connection is released virtual circuit is terminated.

Example of Working-

1.   Host 1 Operation

a.   Host H1 has established connection 1 with host H2

b.   The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1.

c.   Similarly, the first entry at C routes the packet to E, also with connection identifier 1.

2.   If H3 wants to establish connection with H2 and it chooses connection identifier 1, it will create second entry in table which will lead to conflict because A can distinguish this conflict but C cannot. So instead we go to point 3.

3.   Host 3 Operation

d.   So, before A will change identifier of H3 to 2 before forwarding packet. This is known as label switching.

e.   Now normal routing and forwarding will take place to send data to Host 2 as shown in Figure below.

4.   After Host 2 receives the data, The connection is terminated
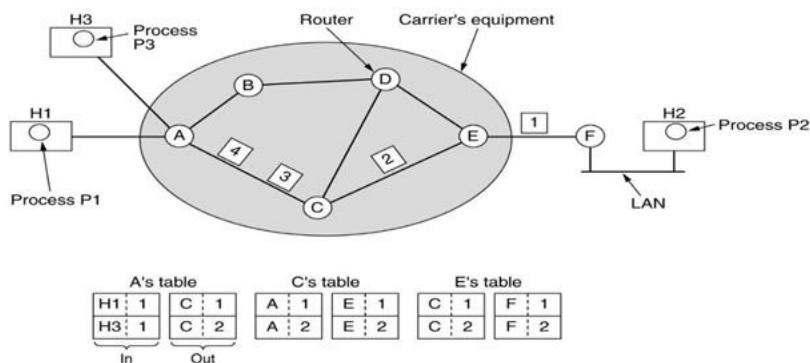
Connection oriented service is more reliable than connectionless service. We can send the message in connection-oriented service if there is an error at the receiver's end.

Quality of Service and convergence is easier comparatively here. Connection-oriented service is related to the telephone system. Example of connection oriented is TCP (Transmission Control Protocol) protocol.
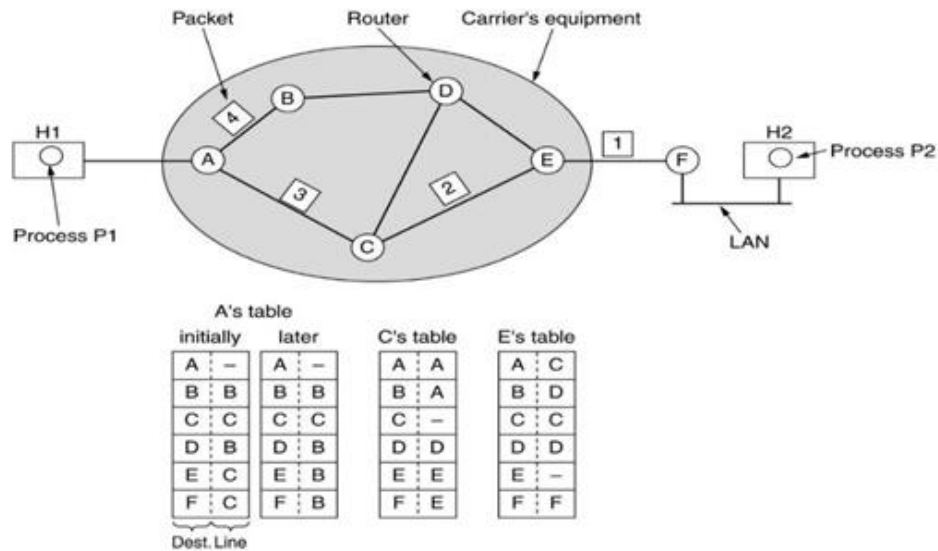
Connectionless Service

Theory and Working-

Connection-less service is related to the postal system. It does not include any connection establishment and connection termination. Connection-less Service does not give the guarantee of reliability. In this, packets do not follow same path to reach destination, that is, packets are injected into the subnet individually and routed independently of each other and no advance setup is needed. In this context packets are frequently called **datagrams** and the subnet is called a **datagram subnet**.

Example of Working-

1 Process p1 at host H1 has a long message for p2 at host H2.

2 It hands the message to transport layer with instructions to deliver it to process p2 on host h2.

3 Transport layer will add it's own header and will pass it to network layer.

4 Assuming that the message is 4 times longer than the maximum packet size.

5 Thus network layer has to break it into four packets 1,2,3 and 4.

6 It sends each of them to router A using some point to point protocol like ppp.

7 Every router has table, telling it where to send packets for each possible destination. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination.

8 Only directly connected lines can be used. A has only two outgoing lines to B and C as shown in figure. So every incoming packet must be sent to one of these routers, even if the destination is some other router.

9 When packet arrives at A, packets 1, 2, 3 stored briefly to check checksum

10 Then each was forwarded to C according to A's routing table

11 Packet 1,2 and 3 on same path, packet 4 on different path may be due to congestion this will update routing table. That shows that packets can go to any possible paths and routed independently of each other and no advance setup is needed and packet gets delivered to H2 where process P2 can use or infer it.

Figure showing H1/Process P1, network with routers A, B, C, D, E, F, H2/Process P2, LAN, and routing tables (A's table initially/later, C's table, E's table).

Application

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried.

Example of Connectionless service is UDP (User Datagram Protocol) protocol.

> **3 For each class of IP Address, determine the number of networks and hosts possible. Also explain why lot of Class A and B addresses are wasted.**
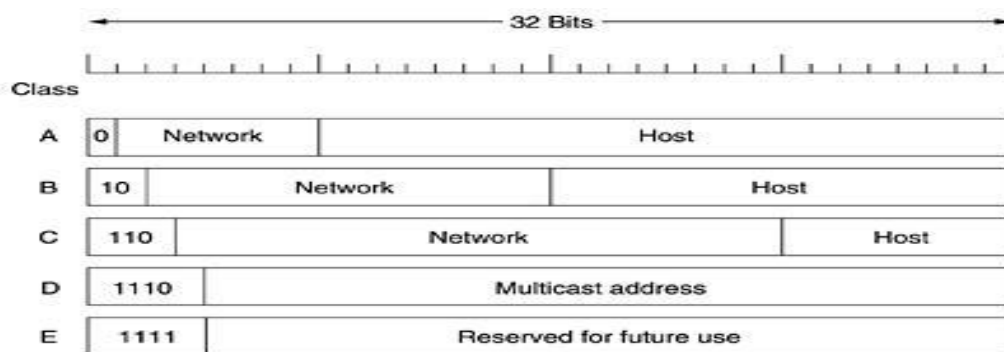
The 32-bit IP address is divided into five sub-classes. These are:

Class A Class B Class C Class D Class E

IPv4 address is divided into two parts:

➢ Network ID

➢ Host ID

Class			
A	0	Network	Host
B	10	Network	Host
C	110	Network	Host
D	1110	Multicast address	
E	1111	Reserved for future use	

Note- While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because

- the first IP address of any network is the network number and

- the last IP address is reserved for broadcast IP.

Class A

- o Total
  - 2^7= 128 network ID

    2^{24} = 16,777,216 host ID

- p Revised (Usable) Class A
  2^7-2= 126 network ID

  Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special addresses.

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

Class B

- Total
  - o 2^14 = 16384 network address
  - o 2^16= 65,536 host address

- Revised (Usable) Class B

  - o 2^14 = 16384 network address

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

Class C

- Total

  - 2^{21} = 2097152 network
    address o 2^8 = 256 host address

- Revised (Usable) Class C
    - 2^14 = 16384 network address o
    2^16 − 2 = 65534 host address

Class D

- Class D addresses are used for multicasting. There is only one block in this class.

Class E

1. Class E addresses are reserved for special purposes. Most of the block is wasted.

If we consider class A, the number of addresses in each block is more than enough for almost any organization. A class A subnet has 24 bits worth of addressing, which is enough for almost 17 million individual devices. So, it results in wastage of addresses.

Same is the case with class B, probably an organization receiving block from class B would not require that much of addresses. So, it also results in wastage of addresses. Also, the special blocks contribute to the wastage in Class A and B.

**4   Discuss the design issues of LAN and WAN.**

Ans.

Following are the problems with LAN in MAC sub-layer:

1. Each of the LANs uses different frame format

   For example, duration field is there in 802.11 due to MACAW protocol and make no sense in Ethernet.

   As a result, any copying between different LAN will require reformatting, which takes CPU time, requires a new checksum calculation, and introduces possibility of undetected errors due to bad bits in bridges memory.
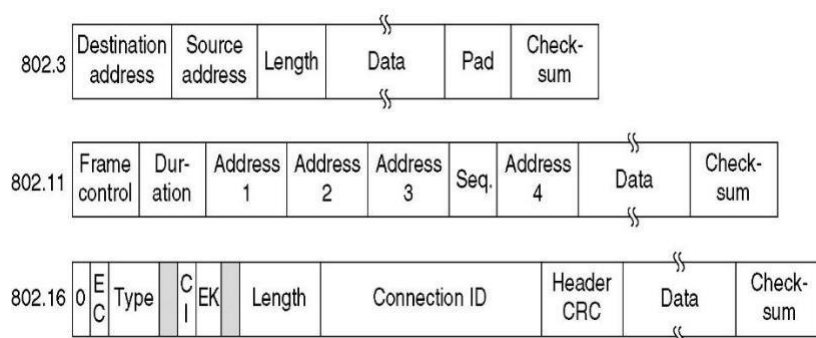
2. Interconnected LANs that do not run at same data rate

When forwarding many long frames from a fast LAN to slow one, the bridge will not be able to get rid of the frame as fast as they come in.

Bridge will have to buffer them.

Bridges that connect two or more LANS need to buffer frames from many LANs without running out of buffer memory.

3. Each 802 LANs have different maximum frame lengths

Problem arises when a long frame is forwarded to a LAN which cannot accept frame of that length. Splitting the frame out into pieces is not possible as DLL do not provide facility of reassembling pieces of frame.

Frames that are too large to be forwarded must be discarded.

4. Security

Both 802.11 and 802.16 supports encryption while ethernet do not support encryption.

This means various encryption services provided to the wireless networks are lost when that frame pass through Ethernet network or even when that frame arrive at Ethernet network there will be no way to decrypt it as Ethernet is not supporting encryption and decryption.

Following are the problems with WAN:

1. WAN Connections Fail as Load Increases

Users continually complain about lost connections at peak periods. One example of this problem is in an environment that features bridged DEC local-area transport (LAT) traffic and multiple routed protocols. Data entry input from users (or other application requests) might be getting buffered at the end of an already long input queue; eventually one end of the connection times out.

2. WAN Users Cannot Connect to Resources over a New Frame Relay Link or New X.25 WAN Link
Traffic does not pass through a newly installed router interconnecting broadcast networks via a Frame Relay WAN or an an X.25 WAN. So we look for problems associated with the new installation, especially when LANs previously interconnected via the WAN continue to communicate with no disruption of service.

3. Given a situation, the following problems are the best candidates for WAN interconnection failure: o Cabling problem to the switch or to the LAN

   o Wrong applique (must be data terminal equipment [DTE] for CSU/DSU connectivity) o Router hardware problem

   o Disabled port on the
   X.25 switch o Bad T1
   digital link

   o Mismatched Ethernet version
   configurations o Misconfigured hosts

   o Misconfigured router