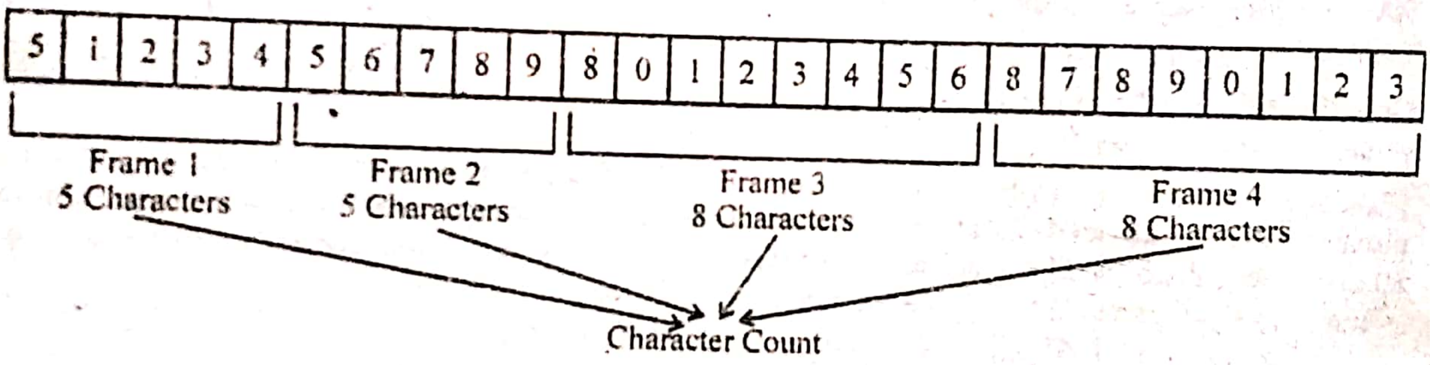
known as Dynamic IP address.

Q6(a). What is Framing ? Explain flow control.

Ans. Framing is the process of breaking the bit stream up into frames. It is done at Data Link layer. The usual approach is for the data link layer to break the bit stream up into discrete frames and compute the checksum for each frame when a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in frame, the data link layer known that an error has occurred and takes steps to deal with it.

We have Different Methods of Framing :

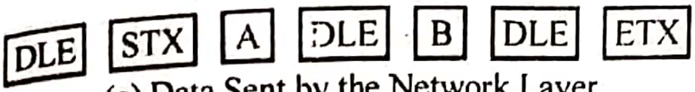
1. Character Count : It uses a field in header to specify the no. of characters in frame when the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of frame. **For example :**



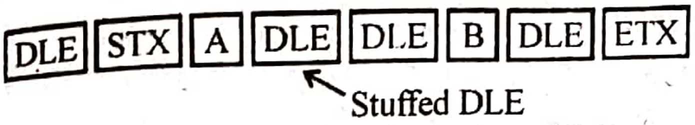
It has problem, for example if the character count of 5 in 2nd frame becomes 7, the destination will get out of synchronization and will be unable to locate the start of next frame.

2. Character Stuffing : The resynchronization problem can be eliminated by having each frame start with a special ASCII character sequence "DLE STX" and end with "DLE ETX" [DLE → Data Link Escape, STX → Start of Text, ETX → End of Text).

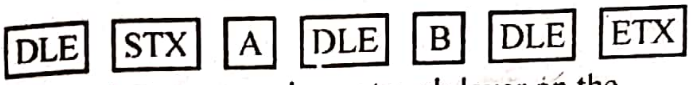
In this way, if the destination ever loses track of frame boundaries, all it has to do is look for DLE STX or DLE ETX characters to figure out where it is :



(a) Data Sent by the Network Layer



(b) Data after being character stuffed by the data link layer



(c) Data passed to network layer on the receiving side

3. Bit Stuffing : It allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. In this, each frame begins and ends with special bit pattern, 01111110, called a flag byte whenever the sender's data link layer encounters five consecutive ones in data, it automatically stuffs a 0-bit into outgoing bit stream. When the receiver sees five consecutive incoming 1 bits, followed by 0 bit, it automatically deletes 0 bit. If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in receiver's memory as 01111110.

For example :

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Fig : Original data

(b)0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

Stuffed Bits

Fig : Data as Appear Online

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

↑

Fig : The data as they are stored in receiver's memory after destuffing.

4. Physical Layer Coding Violations : It is applicable to networks in which encoding on physical medium contains some redundancy. If some LANs encode 1-bit of data by using 2 physical bits. Normally, a bit is high low pair and a 0-bit is low-high pair. The combinations high-high and low-low are not used for data.

Flow Control : Flow control is one of the key aspects of data link layer. Flow control is a set of procedures that tell the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

The flow of data must not be allowed to overwhelm the receiver. This situation happens when the sender is running on a fast computer and the receiver on a slow computer. Flow control mechanisms must be employed so that the sender sends as much frames as are able by the receiver to receive. For this reason, each receiving device has a block of memory, called a buffer, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again ready to receive.

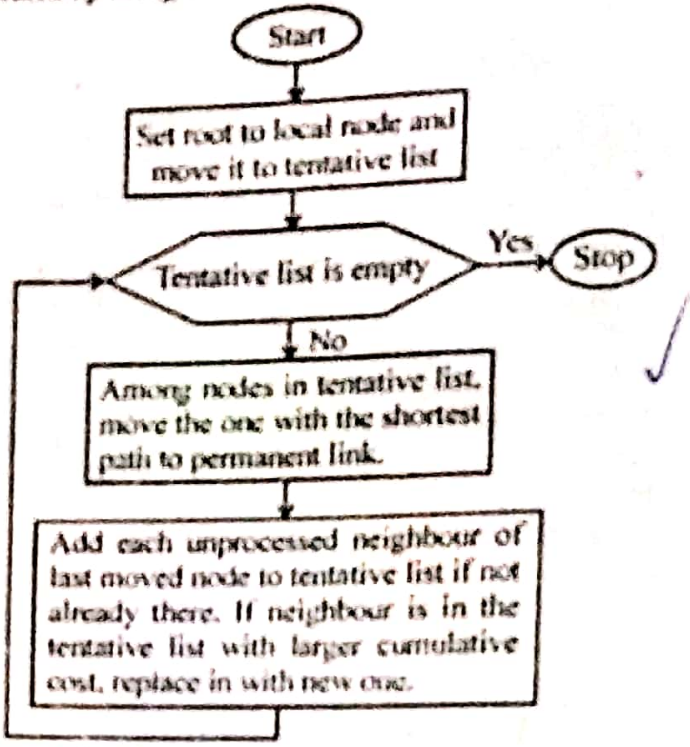
The simplest way of flow control is a stop and go protocol in which a sender waits for an acknowledgement by the receiver before sending another packet. Stop and go protocols utilize only 4% of the network bandwidth. To obtain high throughput rates, sliding window protocol is used. The sender and receiver are programmed to use a fixed window size, which is the maximum amount of data that can be sent before an acknowledgement arrives.

Q8(a). Describe shortest path algorithm for Routing.

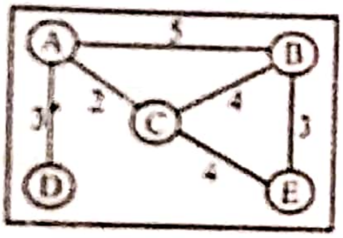
Ans. Formation of Shortest Path Tree : Dijkstra Algorithm after receiving all LSPs, (*Link State Packet*), each node will have a copy of the whole topology.

The Dijkstra Algorithm creates a shortest path tree from a graph. The algorithm divides the nodes into two sets : Tentative and Permanent. It finds the neighbours of a current node, makes them tentative, examines them and if they pass the criteria, makes them permanent.

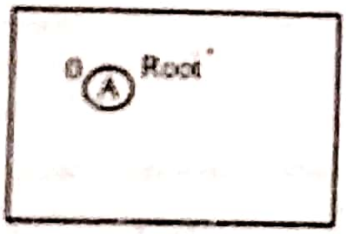
Dijkstra Algorithm can be defined by using a flow chard Dijkstra Algorithm :


Start
Set root to local node and move it to tentative list
Tentative list is empty
Yes
Stop
No
Among nodes in tentative list, move the one with the shortest path to permanent link.
Add each unprocessed neighbour of last moved node to tentative list if not already there. If neighbour is in the tentative list with larger cumulative cost, replace in with new one.

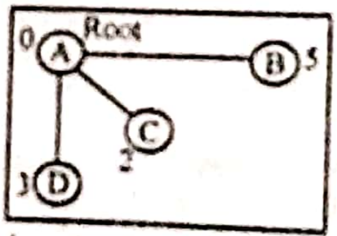
Examples of Formation of Shortest Path Tree



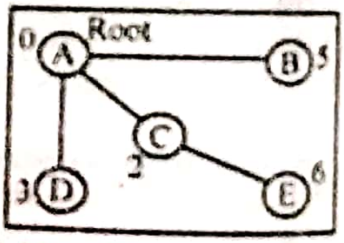
Topology



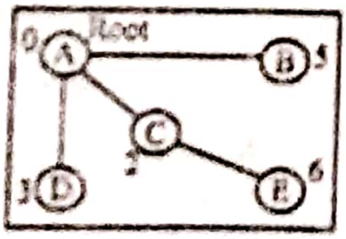
1. Set root to A and move A to tentative list



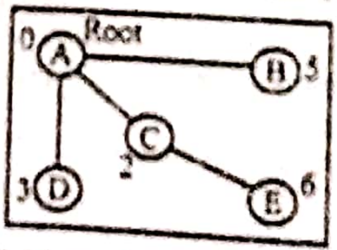
2. Move A to permanent list and add B, C and D to tentative list



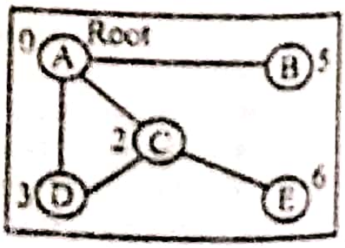
3. Move C to permanent and add E to tentative list



4. Move D to permanent list



5. Move B to permanent list



6. Move E to permanent list (tentative list is empty)

1. Permanent list : Empty
   Tentative list : A(0)
3. Permanent list : A(0), C(2)
   Tentative list : B(5), D(3), E(6)
5. Permanent list : A(0), B(5), C(2), D(3)
   Tentative list : E(6)

2. Permanent list : A(0)
   Tentative list : B(5), C(2), D(3)
4. Permanent list : A(0), C(2), D(3)
   Tentative list : B(5), E(6)
6. Permanent list : A(0), B(5), C(2), D(3), E(6),
   Tentative list : Empty

To find shortest path at each step, we need to cumulative cost from the root to each node, which is shown next to the node.

5

Q8(b). Write advantages of Flow-based routing over Flood routing.

Ans. The advantages of flow-based routing over flood routing are as follows :

1. The mean data flow between each pair of nodes is relatively stable and predictable.
2. If the capacity and average flow are known, it is possible to compute the mean packet delay on that line from queuing theory.
3. Flow-based routing, it is straight forward to calculate a flow-weighted average to get the mean packet delay for the whole subnet.
4. The routing problem then reduces to finding the routing algorithm that produces the minimum average delay for the subnet.
5. To use this technique, certain information must be known in advance.

5R

Q9(a). Define IP address. What are different classes of IP address? Describe.

Ans. IP address mean a logical address in the network layer of the TCP/IP protocol suite.

The Internet addresses are 32 bits in length, this gives a maximum of 2^{32} addresses.

These addresses are referred to as IPV4 i.e., (IP version 4) addresses or simply IP addresses if there is no confusion.

The need for more addresses, in addition to other concerns about the IP layer, motivated a new design of the IP layer called the new generation of IP or IPV6 (IP version 6). In this version, the internet uses 128-bit addresses that give much greater flexibility in address allocation. These address are referred to as IPV6 addresses.

The classes of IP addresses are further divided into 5 classes : A, B, C, D and E.

	First byte	Second byte	Third byte	Fourth byte
Class A	0 - 127			
Class B	128 - 191			
Class C	192 - 223			
Class D	224 - 239			
Class E	240 - 255			

Class A : Address were designed for large organisation with a large number of attached hosts or routers.

Class B : Addresses were designed for midsize organization with tens of thousands of attached hosts or routers.

Class C : Address were designed for small organizations with a small number of attached hosts or routers.

Class D : Addresses were designed for multicasting. Each address in this class is used to define one group of hosts on the internet. The Internet authorities wrongly predicted a need for 268, 435, 456 groups. This never happened and many addresses were wasted here too.

Class E : And lastly, the class E addresses were reserved for future use; only a few were used, resulting in another waste of addresses.

5

Q9(b). Compare subnetting and supernetting.

Ans. Subnetting :

During the era of classful addressing, subnetting was introduced. If an organization was granted a large block in A and B, it could divide the addresses into several contigous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbours subnetting increases the number of 1s in the most.