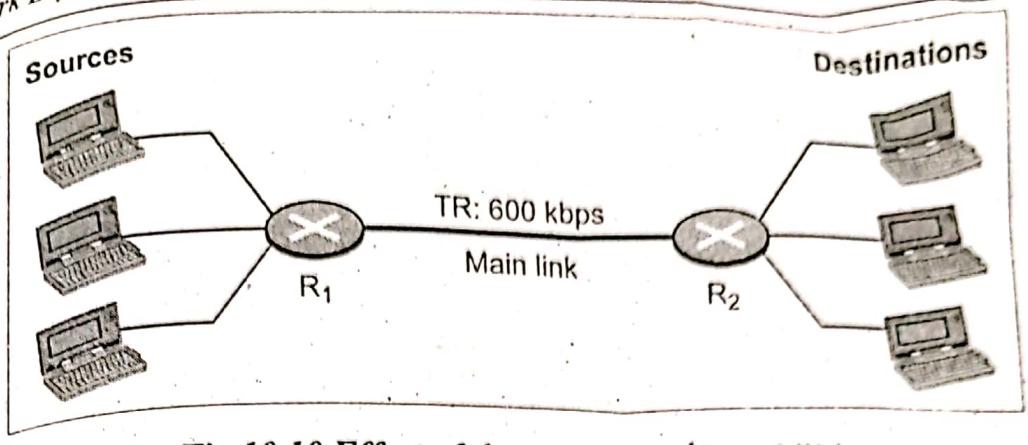

Fig 10.10 Effect of throughput in shared links

10.3.3 Packet Loss

- Packet loss during transmission is one of the main issue that severely affects the performance of communication.
- When a router receives a packet while processing another packet, then the received packet needs to be stored in the input buffer and waiting for its turn.
- But the input buffer is in limited size, when the buffer is full and the next packet needs to be dropped.
- The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss.

10.3.4 Congestion Control

- *When too many packets are present in (a part of) the subnet, the performance of the network will be degraded. This situation is called* ***congestion***.
- A network faces the problem of ***congestion*** *"if the users of the network send data at a rate that is greater than the network can handle (number of packets)".*
- ***Congestion control*** refers to the *techniques and mechanisms that can either prevents congestion, before it happens (or) removes congestion, after it has happened.* It keeps the load below the capacity of the network.

(1) Types of Congestion Control

- Two categories of congestion control are,
  - (i) *Open-loop congestion control (Prevention)*, and
  - (ii) *Closed-loop congestion control (Removal)*.

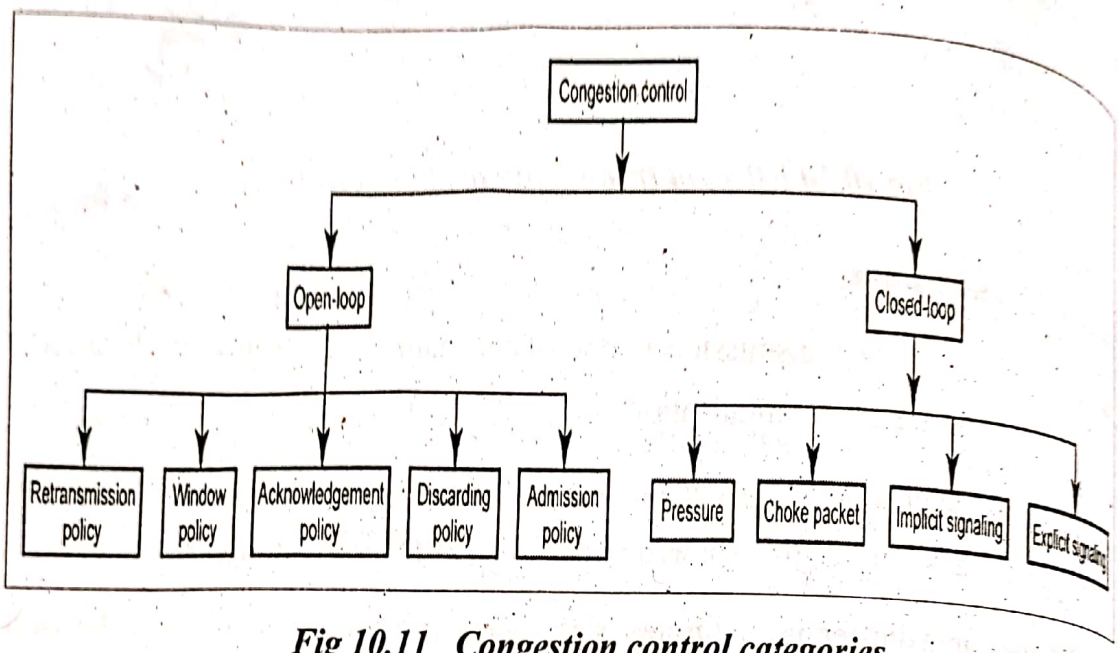

Fig 10.11 Congestion control categories

(2) Open-Loop Congestion Control

- In open-loop congestion control, ***techniques are applied to prevent congestion before it happens.*** Lists of policies that can prevent congestion are,

(i) Retransmission Policy

- If the sender packets are corrupted or lost, the packets should be retransmitted. This will increase congestion in the network.
- The retransmission policy and the retransmission timers must be designed to ***optimize efficiency*** and at the same time it ***prevents*** congestion.

(ii) Window Policy

- The type of window at the sender may also affects congestion. The ***selective repeat window*** is ***better than*** the ***Go-Back-N window*** for congestion control.

- In the Go-back-N window, when the timer for a packets gets time out, several packets may be resent. This may increase congestion.
- In a selective repeat window it tries to send the specific packets that have been lost or corrupted.

(iii) Acknowledgement Policy

- The acknowledgement policy also affects congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender but helps to prevent congestion.
- Sending fewer acknowledgments means imposing less load on the network. A receiver may decide to acknowledge only N packets at a time.

(iv) Discarding Policy

- A good discarding policy by the routers may prevent congestion.
- For example, in audio transmission, if the policy is to discard the less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented.

(v) Admission Policy

- It is a quality of service mechanism, can also prevent congestion in virtual circuit networks.
- Here, once congestion has been signaled, no more virtual circuits are set up until the problem has gone away.

(3) Closed Loop Congestion Control:

- *Closed-loop congestion control try to alleviate congestion after it happens.*

Some of the policies that can remove congestion are,

(i) Back Pressure:

- *Back pressure is a kind of node-to-node congestion control that starts with a node and propagates in the opposite direction of data flow towards the source.*

- This may cause the upstream node or nodes to become congested and reject data from their upstream node or nodes.
- Backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.

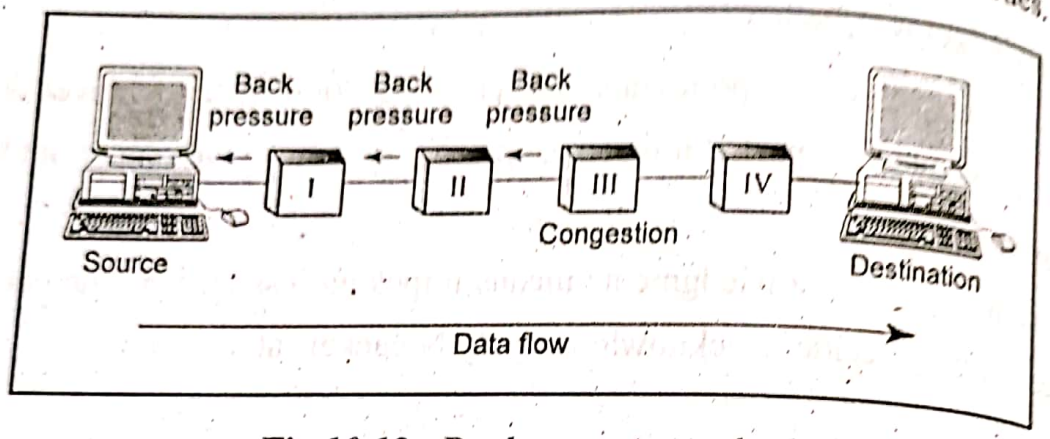

Fig 10.12 Backpressure method

(ii) Choke Packet:

- *The choke packet is a packet sent by a router to the source to inform it about congestion.*
- This choke packets will have the effect of stopping (or) slowing down the rate of transmission from the sources and hence limits the total number of packets in the networks.

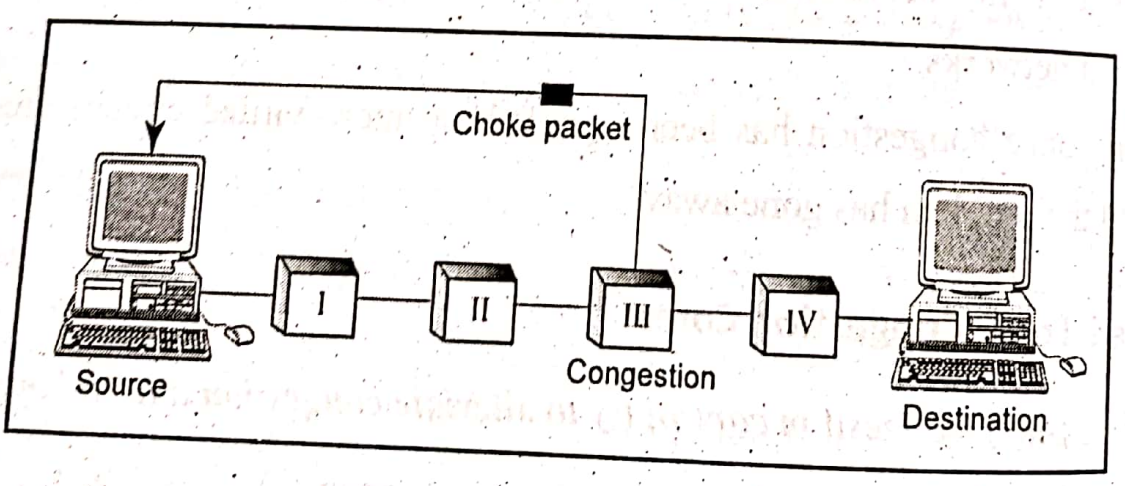

Fig 10.13 Choke packet

) Implicit Signaling

- In implicit signaling, there is no communication between the congested node to the source.

(iv) Quality of Service (QoS)

- Internet has allowed new applications such as multimedia communication, the QoS has become more important. The Internet provides better quality of service to support these applications.
- The network layer not taking any steps regarding this issues and these provisions are mostly implemented in the upper layer.

(v) Security

- Another issue related to communication at the network layer is security, but the network layer was designed with no security provision.
- To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service. This virtual layers are called as ***IP Security (IPSec).***

10.2 PACKET SWITCHING

10.2.1 Introduction

- Packet switching is generally ***more efficient*** than circuit switching for ***non-voice communication.***
- *In the packet-switched network, the* ***sending message*** *is divided into packets of* ***fixed*** *or* ***variable size****. Here, there* ***is no resource allocation*** *for packets. Resources are allocated based on demand.*
- Each ***packet*** contains not only ***data*** but also a ***header*** with control information such as the sender's address and destination's address. The ***packets*** are sent over the network from ***node to node.***

10.2.2 Approaches to Packet Switching

- There are two popular approaches to packet switching. They are
  - (i) Datagram Approach, and
  - (ii) Virtual Circuit Approach.

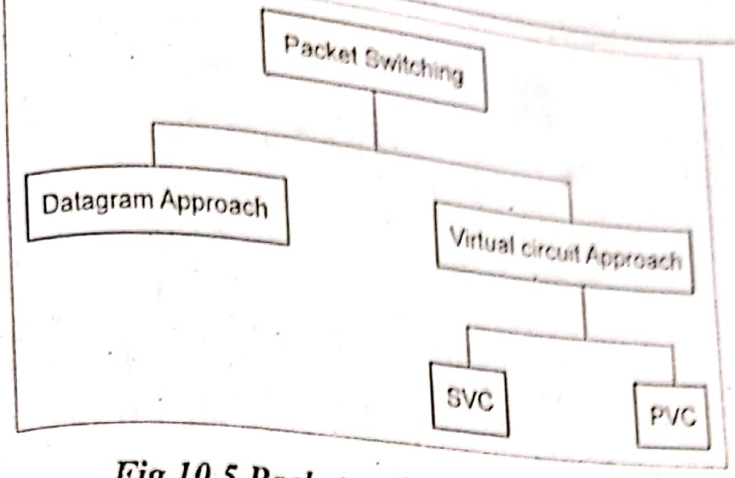

Fig 10.5 Packet switching approaches

- Virtual circuit is implemented in two formats:
  - → Switched Virtual Circuit (SVC), and
  - → Permanent virtual Circuit (PVC).

0.2.3 Datagram Approach: Connectionless Service

- *In the **datagram approach**, each packet is **treated independently** with no reference to packets that have gone before. Packets in this approach are referred to as **datagrams**. There are no setup (or) teardown phases.*
- As the network condition and congestion at different nodes/links differs every seconds, different packets may choose different routes based on the situation at that time.
- Fig.10.6, shows how the datagram approach can be used to deliver message from ***Station A*** to ***Station G***. All three packets belong to the ***same message*** but may choose ***different paths*** to reach their ***destination***.
- This approach makes the datagrams to arrive at their destination ***out of order***. Hence, it is responsible for the transport layer to ***reorder*** the datagrams before passing them on to the ***destination port***.

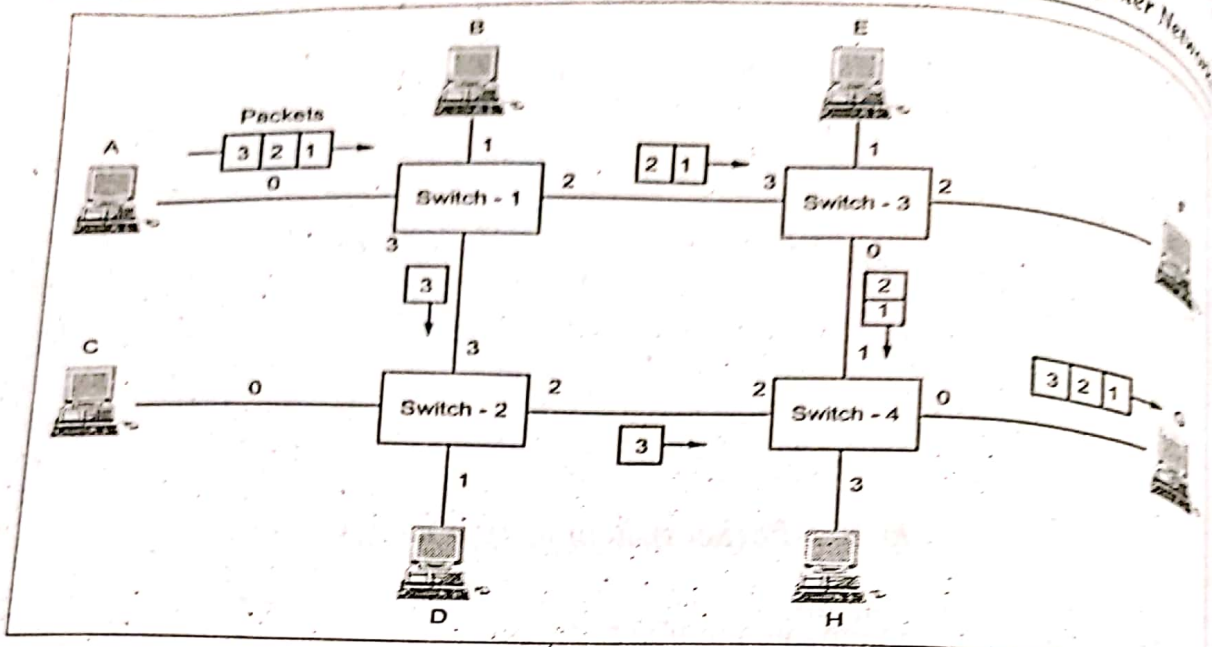

Fig 10.6 Datagram approach

- The link joining each ***pair of nodes*** can contain ***multiple channels***. Each of these channels is capable of carrying datagrams either from several ***different sources*** or ***from one source***. Multiplexing can be done using *TDM* or *FDM*.

(1) Forwarding Table:

- A switch in a datagram network uses a ***routing table*** decides how to forward a packet that is ***based on the destination address.*** The routing tables are ***updated periodically*** which is sometimes called as ***forwarding table.***

Destination	Port
A	0
B	1
C	3
D	3
E	2
F	2
G	2 & 3
H	2 & 3

Table 10.1 Forwarding table of switch-1 in Fig 10.6

- The destination addresses and the corresponding forwarding *output ports* are recorded in these tables.

(a) Efficiency, Applications and Advantages

Efficiency:

The efficiency of a datagram network is ***better*** than that of a circuit-switched network because the resources are allocated only when there are packets to be transferred.

Application:

Switching in the ***Internet*** is done by using the datagram approach to packet switching at the network layer.

Advantages

The advantages of datagram approach are given as follows:

(i) *No **call setup phase**. Thus, if a station wishes to send only one or a few packets, **datagram delivery** will be **quicker.***

(ii) *It is **more flexible** and **reliable**. For example, if the congestion develops in one part of the network, incoming datagrams can be routed away from congestion.*

(iii) *If a node fails, subsequent packets may find an alternate route that bypasses that node.*

10.2.4 Virtual-Circuit Approach: Connection-Oriented Service

- *A virtual-circuit network is a cross between a circuit-switched network and a datagram network.*
- *A preplanned **single virtual connection route** is chosen between the **sender** and the **receiver** before any data is sent. When data are sent, all packets travel one after another along this route. For this, it is also referred to as a **connection-oriented model.***

- A ***virtual-circuit*** network is normally implemented in the ***data-link layer***, a ***circuit-switched*** network is implemented at the ***physical layer*** and a ***datagram*** network in the ***network layer***.
- ***Switched WAN*** is normally implemented by using virtual-circuit techniques, is implemented in two formats:
  - → Switched Virtual Circuit (SVC).
  - → Permanent virtual Circuit (PVC).

SVC: *In this method, a **virtual circuit path** is created whenever it is needed and exists **only for the duration of the specific exchanges.***

PVC: *In this method, the same **virtual circuit** path is provided between two **users** on a **continuous basis**. The circuit is dedicated to the specific users.*

(1) Switched Virtual Circuit (SVC)

- In SVC based datagram approach for transferring the packets between two nodes, there may be a three-stage process (or) phases:

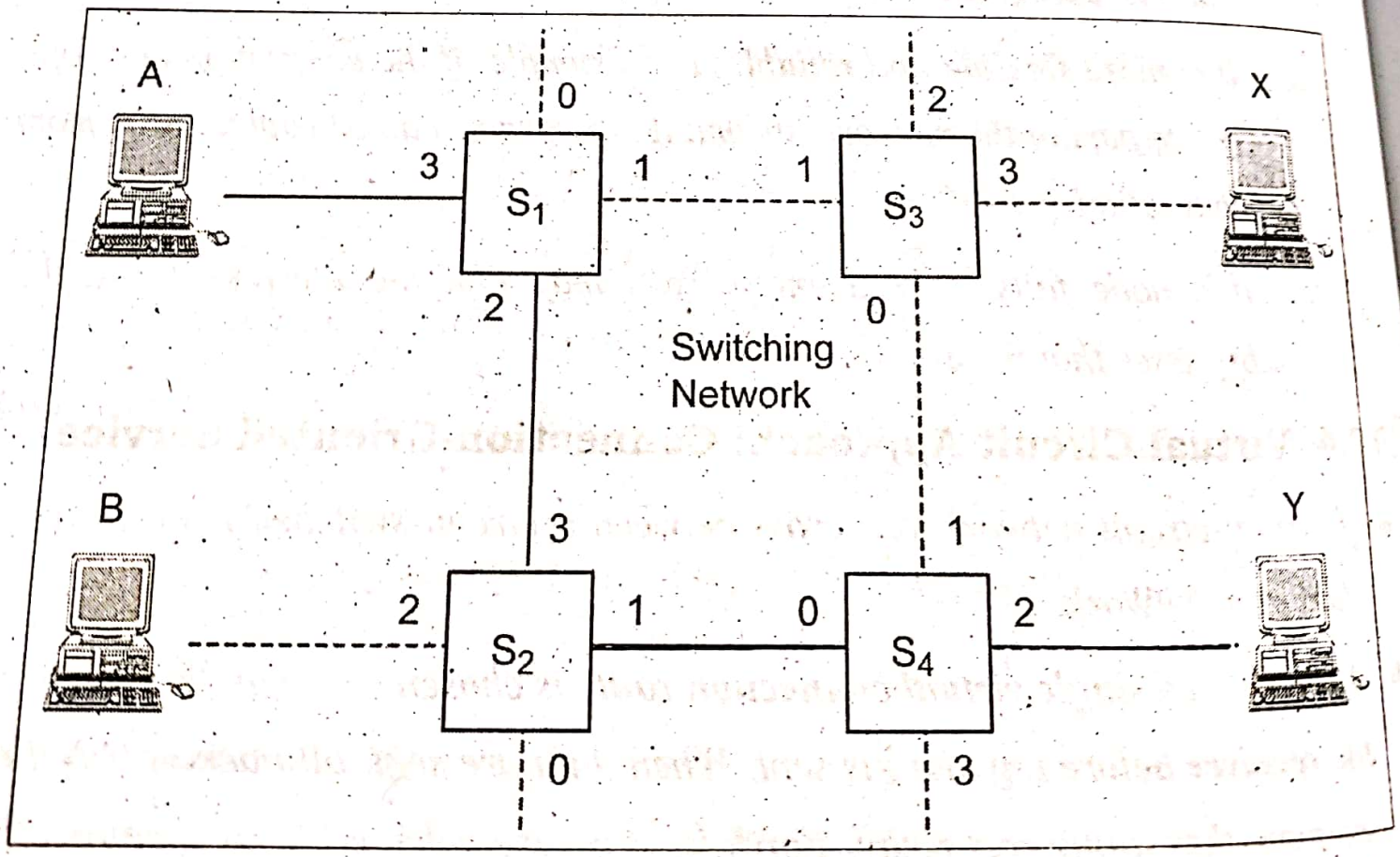

Fig 10.7 Virtual circuit connection

(i) Connection setup (or) establishment,
(ii) Data transfer, and
(iii) Connection release.

- In the Fig.10.7, shows that a virtual line formed between source A and destination Y for the data transfer.
- During the ***connection establishment phase***, one of the available paths is selected. This path is called as ***virtual circuit***, which is shown in thick lines; other available paths are shown with dashed lines.

(a) Virtual Circuit (VC) Table

The connection state for a single connection consists of an entry in a ***"VC table"***. One entry in the VC table on a single switch contains the following:

Incoming interface (port)	*Incoming VCI*	*Outgoing interface (port)*	*Outgoing VCI*

Table 10.2 VC table

(i) *Virtual Circuit Identifier (VCI)*

- This uniquely identifies the connection link at the switch and it is carried inside the header of the packets that belong to this connection.
- It is a small number in a data frame changes from one switch to another switch used for data transfer.

(ii) An ***incoming interface*** to the switch on which packets for this VCI arrive at the input port of the switch.

(iii) An ***outgoing interface*** from the switch on which packets for this VCI leaves from the output port of the switch.

(iv) ***Outgoing connection link VCI***, will be used for outgoing packets.

- If host A wants to send its packets to host Y, the administrator needs to identify a path from the switches 1, 2, 3 and 4. The administrator then picks a VC value that is currently unused on each link for the connection.

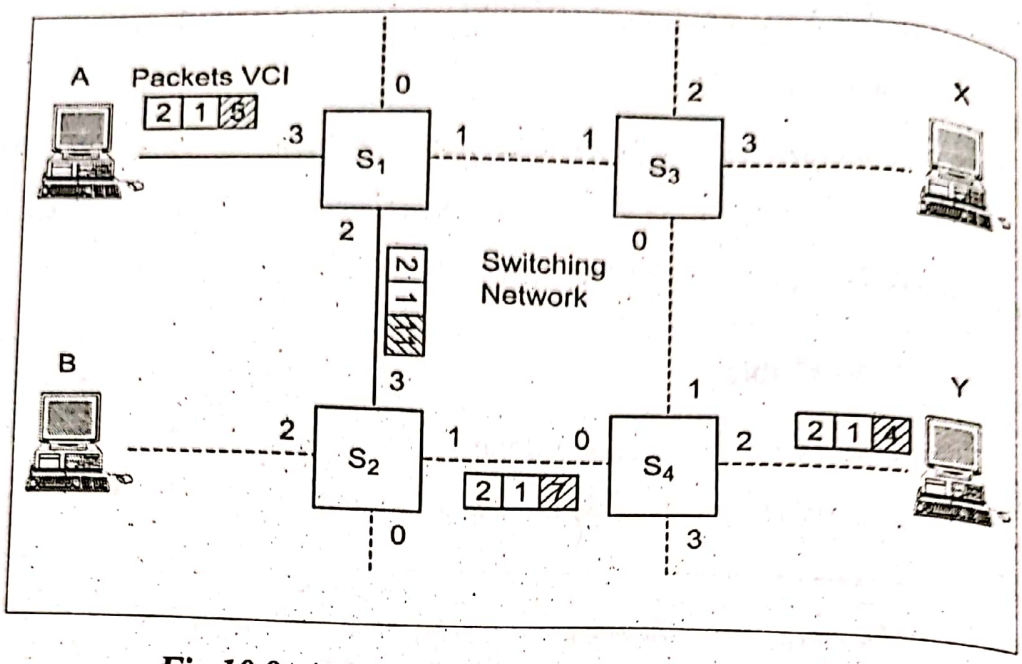

Fig 10.8 An example of a virtual circuit network

- Let's suppose that the VCI value 5 is chosen for the link from host A to switch 1, and then 11 is chosen for the link from switch 1 to switch 2. In that case switch 1 need to have an entry in its VC table and it is configured as shown Table 10.3.

Virtual circuit table entry for switch - 1			
Incoming interface	Incoming VCI	Outgoing interface	Outgoing VCI
3	5	2	11

Table 10.3 VC table for switch-1

- VCI of 7 is chosen to identify the connection on the link from switch 2 switch 3 and that a VCI of 4 is chosen for the link from switch 4 to host Y.

(i) Static Routing Table (or) Non-adaptive Routing Table:

A static routing table contains the ***information entered manually****. The administrator enters the route for each destination into the table. When the table is created, it cannot be updated automatically when there is a change in the Internet.*

Example: *Flooding*

(ii) Dynamic Routing Table (or) Adaptive Routing Table:

- The entries are updated ***automatically by dynamic routing*** protocols such as RIP, OSPF or BGP.
- It will change their routing decisions to reflect ***changes*** in the ***topology***, and usually the ***traffic*** as well.

Example: → Distance Vector Routing (DVR).
→ Link State Routing

- *The Internet preferred to use dynamic routing table, where the updation occurs as soon as there is a change.*

13.2 ROUTING ALGORITHMS

- Several routing algorithms, and the corresponding protocols, are developed to find the best route among them.
- The ***routing algorithm*** is that part of the network layer software responsible for ***deciding*** which ***output line*** an incoming packet should be transmitted on. In routing, the pathway with the ***lowest cost*** is considered the best.

In routing, the term ***shortest*** means the combination of many factors including,

→ Shortest,
→ Cheapest,
→ Fastest,
→ More reliable, and so on.

13.2.1 Network as a Graph

- Figure 13.2 shows a graph representing a network. The nodes of the graph, labeled A through E and all the nodes are connected using links.

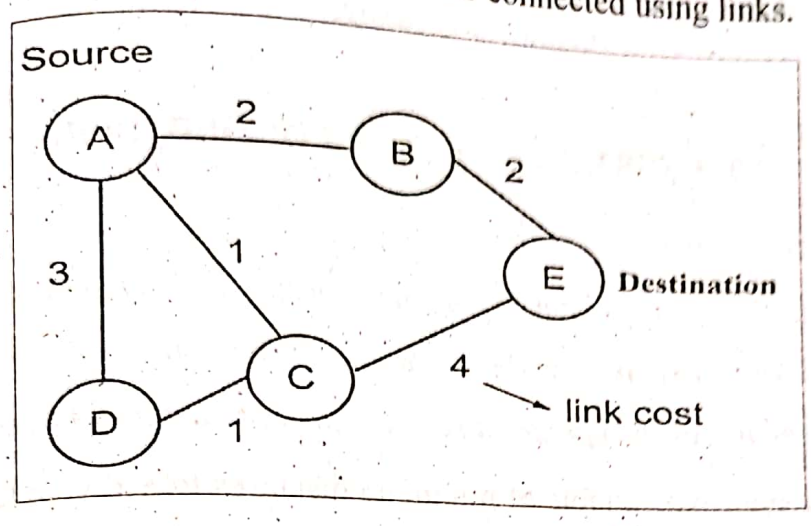

Fig 13.2 Network represented as graph

- Each link has an associated cost, which gives some indication of the desirability of sending traffic over that link.
- The basic problem of routing is to find the ***lowest-cost path*** between any two nodes. For example, consider A is a source and E is a destination, here possible paths are (A→B→E = 2+2 = 4 & A→C→E =1+4 = 5). The shortest path is A→B→E based on the low link cost value.

A Static (manual entry) Approach has Several Drawbacks:

(i) It does not deal with ***node or link failures***.

(ii) It does not consider the addition of new nodes or links.

(iii) It implies that link costs cannot change, eventhough we might reasonably wish to have links cost change over time.

- For these reasons, routing is achieved in most practical networks by using ***distributed, dynamic routing protocols*** among the nodes. It will address the problem of finding the lowest-cost path in the presence of link and node failures and changing an edge costs.

- Some of the important routing algorithms are
  - (i) Distance vector routing (DVR).
  - (ii) Link-state (LS) routing.
  - (iii) Path-vector (PV) routing.

13.3 DISTANCE VECTOR ROUTING (DVR)

13.3.1 Introduction

- *A lowest-cost path algorithm. Each router periodically shares its knowledge about its neighbors, a list of networks it can reach and the distance (cost) to them. network which uses the updates it receives to construct its forwarding table.*
- Each node maintains a table of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next hop in the route (next-hop routing).
- The protocol that implements distance vector routing is called ***Routing Information Protocol (RIP).***

13.3.2 Working Principle

- To understand the working principle of distance vector routing, consider the Fig 13.3 shown below, which contains the nodes of A, B, C, D, E, F and G.
- DVR simplifies the routing process by assuming a cost of one unit for every link. That is, the ***cost*** is based on the ***hop count***.

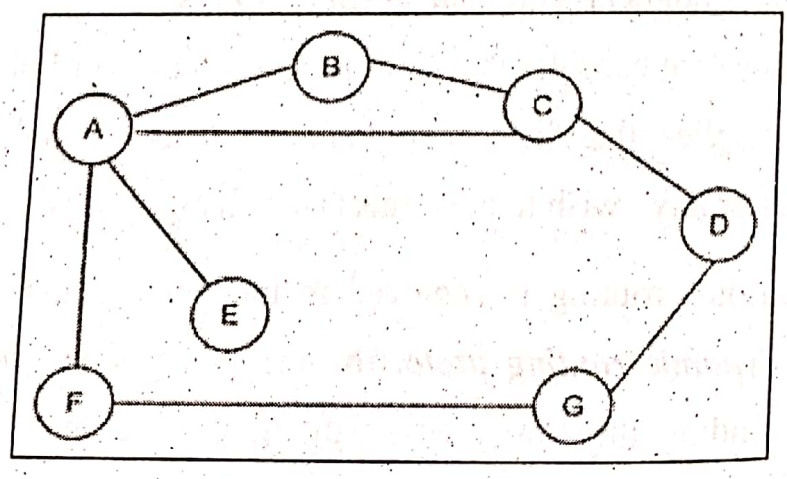

Fig 13.3 Network graph

- The destination addresses and the corresponding forwarding ***output ports*** are recorded in these tables.

(2) Efficiency, Applications and Advantages

Efficiency:

The efficiency of a datagram network is ***better*** than that of a circuit-switched network because the resources are allocated only when there are packets to be transferred.

Application:

Switching in the ***Internet*** is done by using the datagram approach to packet switching at the network layer.

Advantages

The advantages of datagram approach are given as follows:

(i) *No **call setup phase**. Thus, if a station wishes to send only one or a few packets, **datagram delivery** will be **quicker.***

(ii) *It is **more flexible** and **reliable**. For example, if the congestion develops in one part of the network, incoming datagrams can be routed away from congestion.*

(iii) *If a node fails, subsequent packets may find an alternate route that bypasses that node.*

10.2.4 Virtual-Circuit Approach: Connection-Oriented Service

- *A virtual-circuit network is a cross between a circuit-switched network and a datagram network.*
- *A preplanned **single virtual connection route** is chosen between the **sender** and the **receiver** before any data is sent. When data are sent, all packets travel one after another along this route. For this, it is also referred to as a **connection-oriented model**.*

- A *virtual-circuit* network is normally implemented in the *data-link layer*, while a *circuit-switched* network is implemented at the *physical layer* and a *datagram* network in the *network layer*.
- *Switched WAN* is normally implemented by using virtual-circuit techniques and is implemented in two formats:
  - → Switched Virtual Circuit (SVC).
  - → Permanent virtual Circuit (PVC).

SVC: *In this method, a* ***virtual circuit path*** *is created whenever it is needed and exists* ***only for the duration of the specific exchanges.***

PVC: *In this method, the same* ***virtual circuit*** *path is provided between two* ***users on a continuous basis****. The circuit is dedicated to the specific users.*

(1) Switched Virtual Circuit (SVC)

- In SVC based datagram approach for transferring the packets between two nodes, there may be a three-stage process (or) phases:

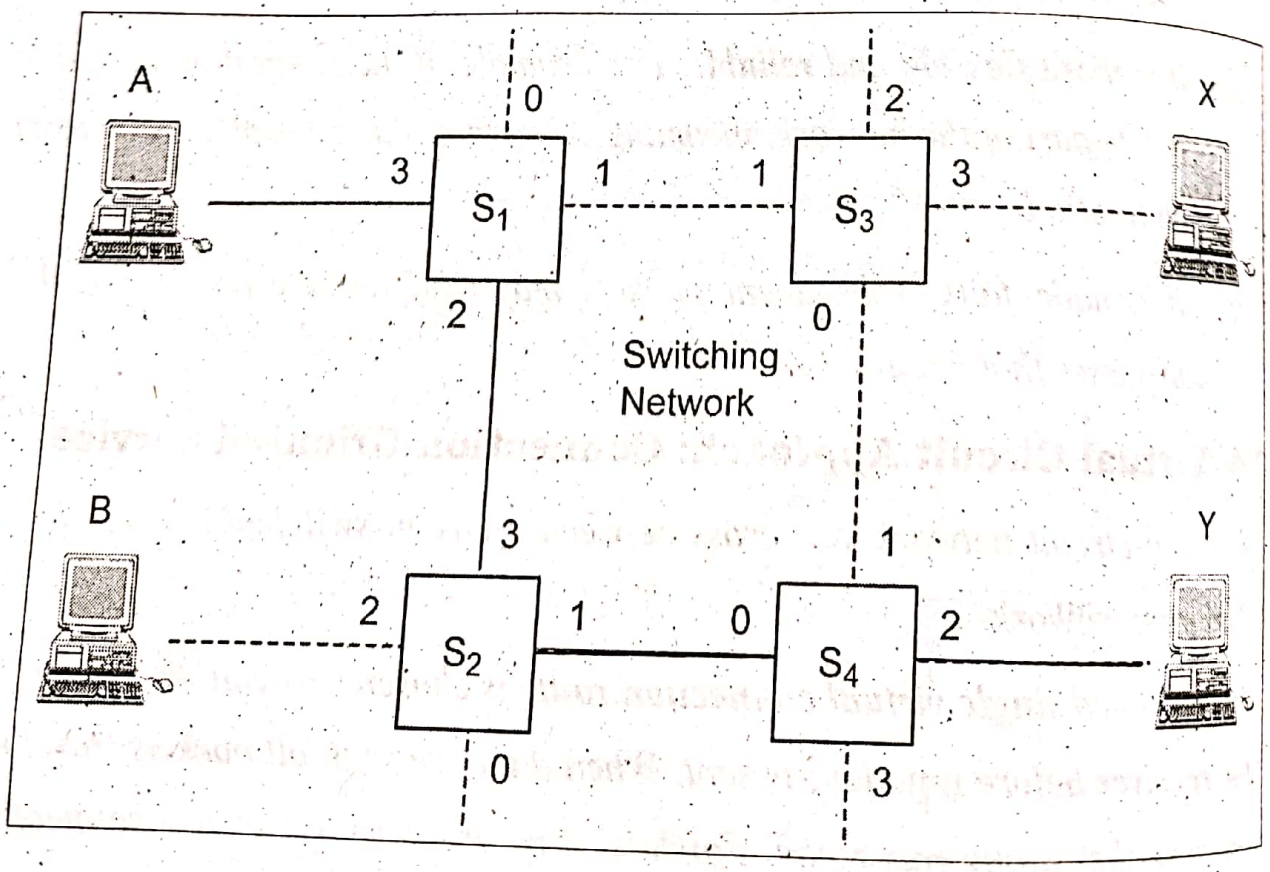

Fig 10.7 Virtual circuit connection

(i) Connection setup (or) establishment,
(ii) Data transfer, and
(iii) Connection release.

- In the Fig.10.7, shows that a virtual line formed between source A and destination Y for the data transfer.
- During the ***connection establishment phase***, one of the available paths is selected. This path is called as ***virtual circuit***, which is shown in thick lines; other available paths are shown with dashed lines.

(a) Virtual Circuit (VC) Table

The connection state for a single connection consists of an entry in a ***"VC table"***. One entry in the VC table on a single switch contains the following:

Incoming interface (port)	*Incoming VCI*	*Outgoing interface (port)*	*Outgoing VCI*

Table 10.2 VC table

(i) *Virtual Circuit Identifier (VCI)*

- This uniquely identifies the connection link at the switch and it is carried inside the header of the packets that belong to this connection.
- It is a small number in a data frame changes from one switch to another switch used for data transfer.

(ii) An ***incoming interface*** to the switch on which packets for this VCI arrive the input port of the switch.

(iii) An ***outgoing interface*** from the switch on which packets for this VCI leave from the output port of the switch.

(iv) ***Outgoing connection link VCI***, will be used for outgoing packets.

- If host A wants to send its packets to host Y, the administrator needs to identify a path from the switches 1, 2, 3 and 4. The administrator then picks a VCI value that is currently unused on each link for the connection.

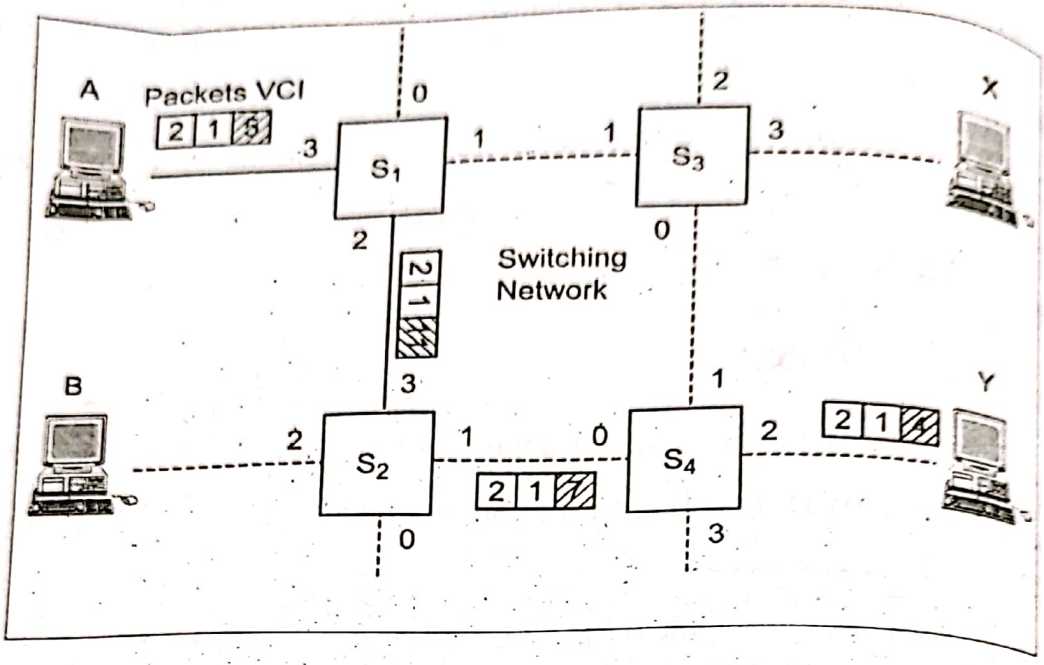

Fig 10.8 An example of a virtual circuit network

- Let's suppose that the VCI value 5 is chosen for the link from host A to switch 1, and then 11 is chosen for the link from switch 1 to switch 2. In that case, switch 1 need to have an entry in its VC table and it is configured as shown in Table 10.3.

Virtual circuit table entry for switch – 1			
Incoming interface	Incoming VCI	Outgoing interface	Outgoing VCI
3	5	2	11

Table 10.3 VC table for switch-1

- VCI of 7 is chosen to identify the connection on the link from switch 2 to switch 3 and that a VCI of 4 is chosen for the link from switch 4 to host Y.