UNIT-4

VIRTUAL CIRCUIT:

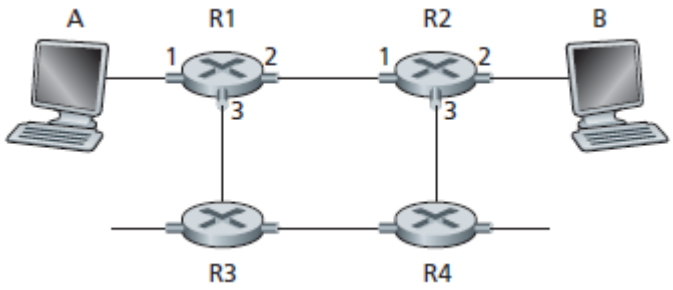
Virtual Circuit is the computer network providing connection-oriented service. It is a connection-oriented network. Virtual – circuit network is a category of packet switching network, where a virtual path is established between the source and the destination systems for data communication to occur. This path appears to the user as if it is a dedicated physical path, but actually is a logical circuit allocated from a managed pool of circuit resources as per traffic requirements. The network resources forming parts of this path can be shared by other communications, however, is not visible to this user.

A Virtual Circuit consists of:

1. A path (that is , a series of links and routers) between the source and destination hosts,
2. VC numbers, one number for each link along the path, and
3. Entries in the forwarding table n each router along the path.

A packet belonging to a virtual circuit will carry a VC number in its header. Because a virtual circuit may have a different VC number on each link, each intervening router must replace the VC number of each traversing packet with a new VC number. The new VC number is obtained from the forwarding table.

To illustrate the concept, consider the network shown in the figure below:



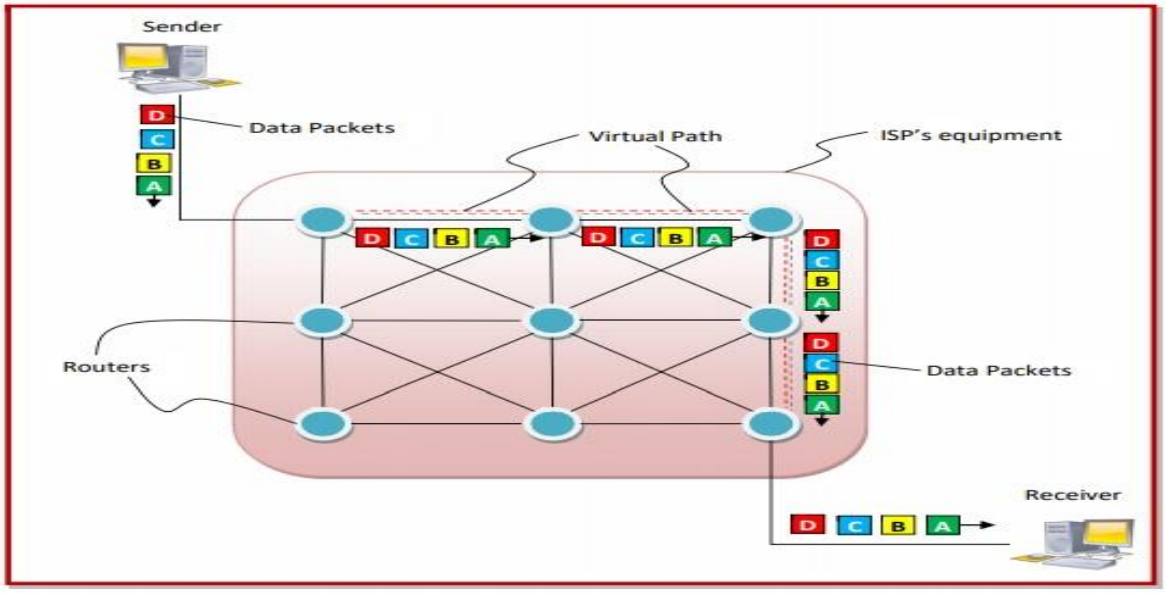
The numbers next to links of R1 in the above figure are the link interface numbers. Suppose now that Host A requests that the network establish a VC between itself and Host B. Suppose also that the network chooses the path A-R1-R2-B and assigns VC numbers 12, 22, and 32 to the three links in this path for this virtual circuit. In this case, when a packet in this VC leaves Host A, the value in the VC number filed in the packet header is 12; when it leaves R1, the value is 22; and when it leaves R2, the value is 32.

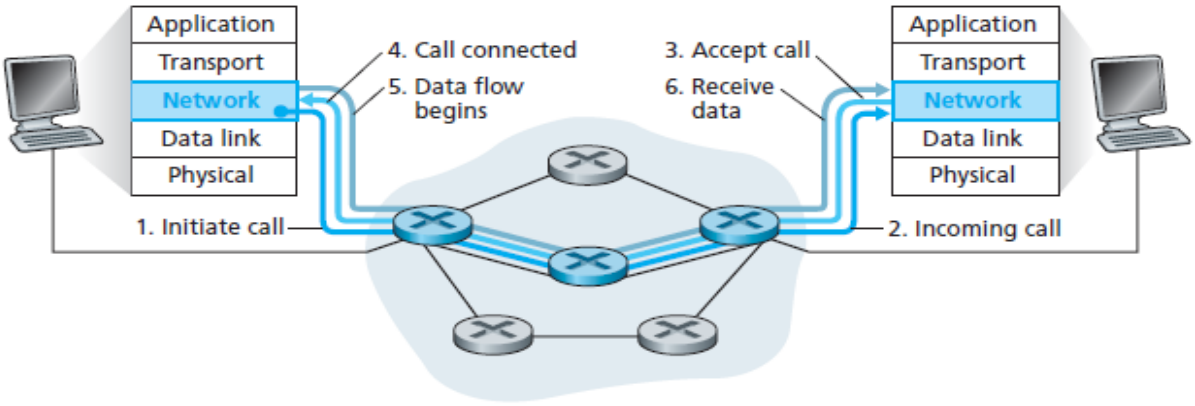
Phases of Virtual - Circuit Transmission:

There are three phases of transmission by virtual circuits, set up, data transfer and teardown.

- **Set up Phase** – In this phase, a virtual circuit or a route is established from the source to the destination through number of switches. The source and destination use global addresses using which the switches make routing table entries.
- **Data Transfer** – Once the virtual circuit is set up, all packets follow the route established during the set up phase adhering to the routing tables.
- **Teardown Phase** – When data transfer is complete, the source sends a teardown request. The destination responds using a teardown confirmation. The switches flush their routing table entries, thus relinquishing the circuit.

In the following diagram, we can that a virtual circuit is created, as denoted by the dotted lines, and all the packets from the sender to the receiver are being routed along this virtual circuit.





Advantages of Virtual Circuit:

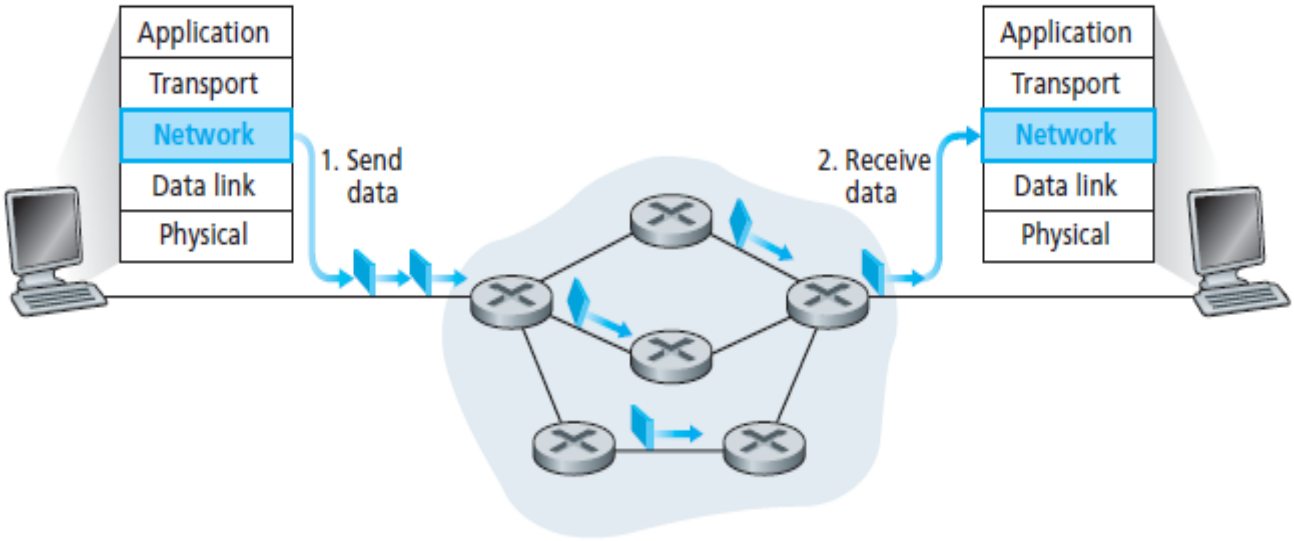
1. Packets are delivered to the receiver in the same order sent by the sender.
2. Virtual circuit is a reliable network circuit.
3. There is no need for overhead in each packet.
4. Single global packet overhead is used in virtual circuit.

Disadvantages of Virtual Circuit:

1. Virtual circuit is costly to implement.
2. It provides only connection-oriented service.
3. Always a new connection set up is required for transmission.

DATAGRAM NETWORKS:

In a datagram network, each time an end system wants to send a packet; it stamps the packet with the address of the destination end system and then pops the packet into the network. As shown in the figure below, there is no VC setup and routers do not maintain any VC state information (because there are no VCs).

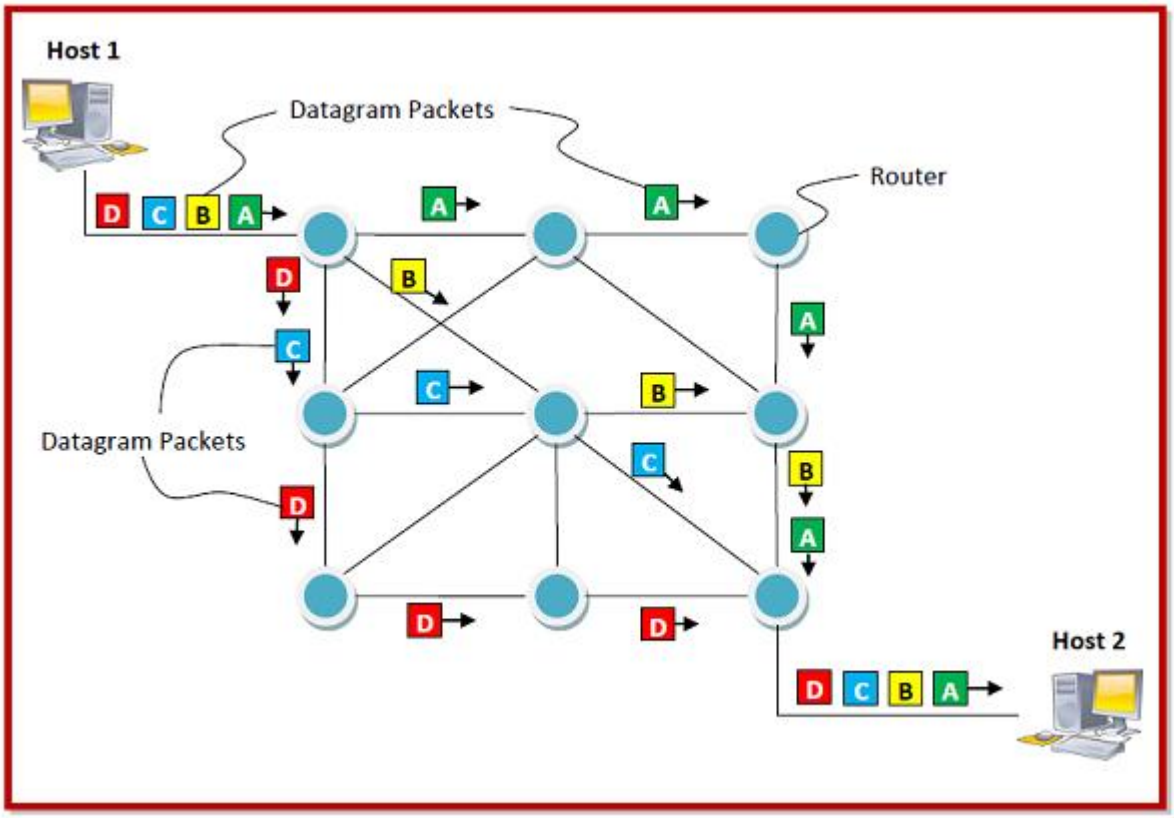


Features of Datagram Networks:

- Datagram switching is done at the network layer of the communication system.
- In datagram networks, each data packet or datagram is routed independently from the source to the destination even if they belong to the same message. The network treats the packet as if it exists alone.

- Since the datagram's are treated as independent units, no dedicated path is fixed for data transfer. Each datagram is routed by the intermediate routers using dynamically changing routing tables. So two successive packets from the source may follow completely separate routes to reach destination.
- In these networks, no prior resource allocation is done for the individual packets. This implies that no resources like buffers, processors, bandwidth, etc. are reserved before the communication commences.
- In datagram networks, resources are allocated on demand on a First−Come First−Serve (FCFS) basis. When a packet arrives at a router, the packet must wait if there are other packets being processed, irrespective of its source or destination.
- Datagram communication is generally guided by User Datagram Protocol or UDP.

The following diagram shows datagram packets being send by host H1 to host H2. The four datagram packets labeled as A, B, C and D, all belonging to same message are being routed separately via separate routes. The packets in the message arrive in the destination out of order. It is the responsibility of H2 to reorder the packets in order to retrieve the original message.



THE INTERNET PROTOCOL (IP):

IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.

The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.

IP Function:

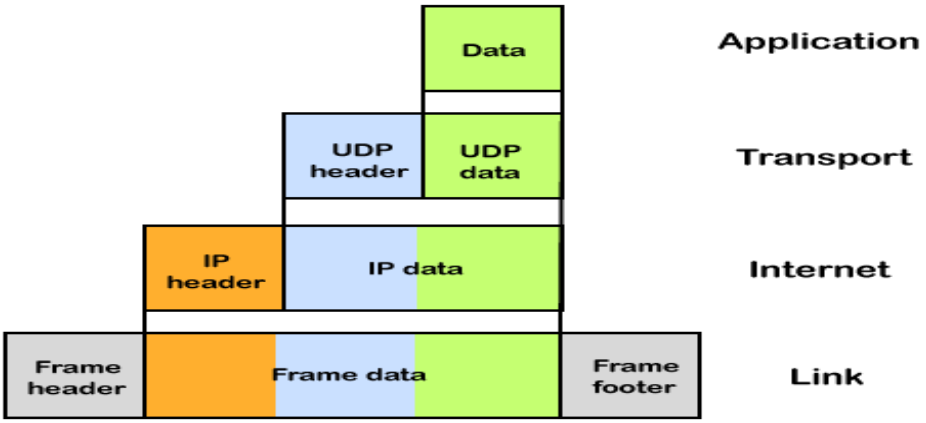
The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more IP networks. In order to achieve these functionalities, internet protocol provides two major things which are given below.

An internet protocol defines two things:

- Format of IP packet
- IP Addressing system

Format of IP packet:

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.



An IP header contains lots of information about the IP packet which includes:

- Source IP address: The source is the one who is sending the data.
- Destination IP address: The destination is a host that receives the data from the sender.
- Header length
- Packet length
- TTL (Time to Live): The number of hops occurs before the packet gets discarded.
- Transport protocol: The transport protocol used by the internet protocol, either it can be TCP or UDP.

Payload: Payload is the data that is to be transported.

IP Addressing:

An IP address is a unique identifier assigned to the computer which is connected to the internet. Each IP address consists of a series of characters like 192.168.1.2. Users cannot access the domain name of each website with the help of these characters, so DNS resolvers are used that convert the human-readable domain names into a series of characters. Each IP packet contains two addresses, i.e., the IP address of the device, which is sending the packet, and the IP address of the device which is receiving the packet.

Types of IP addresses

IPv4 addresses are divided into two categories:

- **Public address**
- **Private address**

Public Address:

The public address is also known as an external address as they are grouped under the WAN addresses. We can also define the public address as a way to communicate outside the network. This address is used to access the internet. The public address available on our computer provides the remote access to our computer. With the help of a public address, we can set up the home server to access the internet. This address is generally assigned by the ISP (Internet Service Provider).

Key points related to public address are:

- The scope of the public address is global, which means that we can communicate outside the network.
- This address is assigned by the ISP (Internet Service Provider).
- It is not available at free of cost.
- We can get the Public IP by typing on Google "What is my IP".

Private Address:

A private address is also known as an internal address, as it is grouped under the LAN addresses. It is used to communicate within the network. These addresses are not routed on the internet so that no traffic can come from the internet to this private address. The address space for the private address is allocated using **InterNIC** to create our own network. The private addresses are assigned to mainly those computers, printers, smart phones, which are kept inside the home or the computers that are kept within the organization. For example, a private address is assigned to the printer, which is kept inside our home, so that our family member can take out the print from the printer.

If the computer is assigned with a private address, then the devices available within the local network can view the computer through the private ip address. However, the devices available outside the local network cannot view the computer through the private IP address, but they can access the computer if they know the router's public address. To access the computer directly, NAT (Network Address Translator) is to be used.

Key points related to private address are:

- Its scope is local, as we can communicate within the network only.
- It is generally used for creating a local area network.
- It is available at free of cost.
- We can get to know the private IP address by simply typing the "ipconfig" on the command prompt.

FORWARDING:

Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination. However, this simple solution is impossible today in an internetwork such as the Internet because the number of entries needed in the routing table would make table lookups inefficient.

Forwarding Techniques: Several techniques can make the size of the routing table manageable and also handle issues such as security.

a. Next-Hop Method versus Route Method: One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.

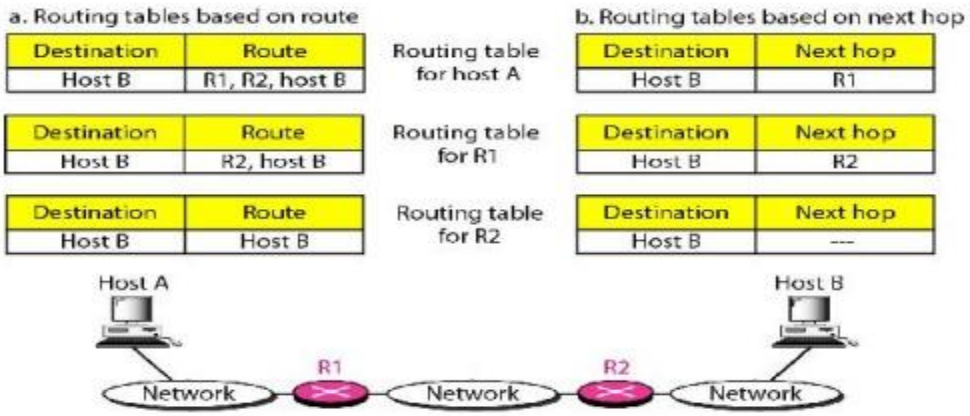


Figure 3.40 Route method versus next-hop method

b. Network-Specific Method versus Host-Specific Method: A second technique to reduce the routing table and simplify the searching process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself.

Host-specific routing is used for purposes such as checking the route or providing security measures

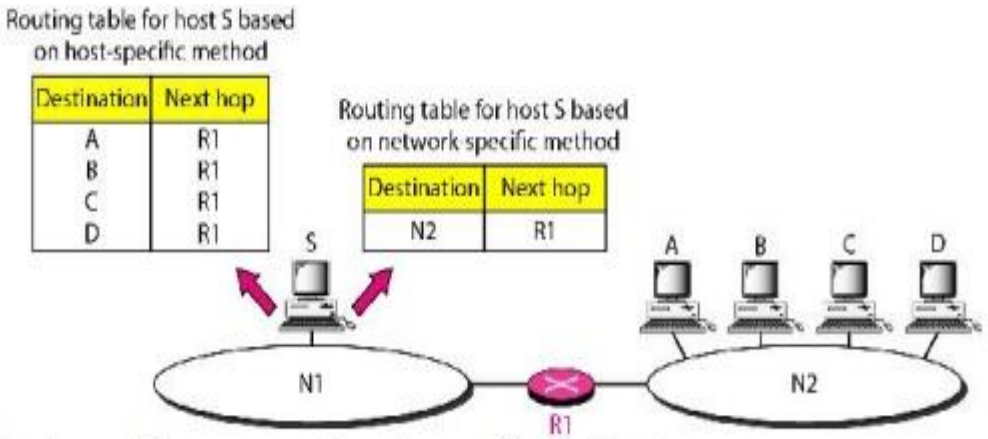


Figure 3.41 Host-specific versus network-specific method

c. Default Method: Another technique to simplify routing is called the default method. Host A is connected to a network with two routers. Router R1 routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default (normally defined as network address 0.0.0.0).

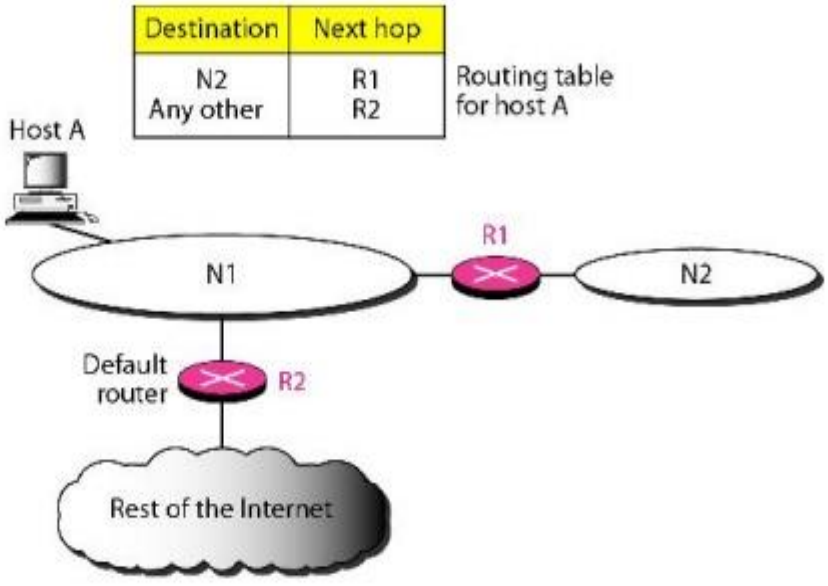


Figure 3.42 Default method

ADDRESSING IN THE INTERNET:

Addressing In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

Global Addressing: A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

Virtual-Circuit Identifier: The identifier that is actually used for data transfer is called the virtual-circuit identifier (Vel). A vel, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl. Figure 8.11 shows how the VCI in a data frame 44 changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCls.

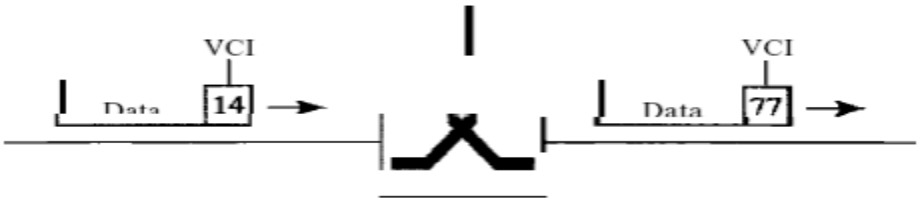


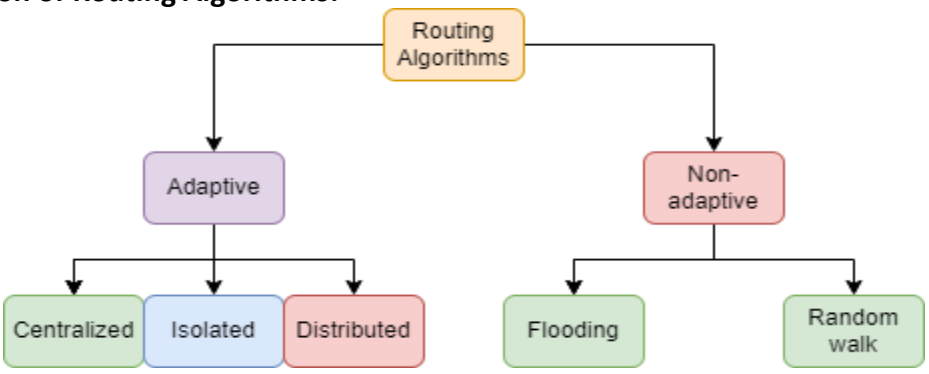
Figure 1 *Virtual-circuit identifier*

ROUTING ALGORITHMS:

A **routing algorithm** is a way to establish the path for data packets. The path is from the source to the destination. It helps in leading internet traffic.

When a data packet leaves its origin, it can take one of many different paths. It computes the best path (least-cost path) to send the data.

Classification of Routing Algorithms:



1. Adaptive Algorithms: These are the algorithms that change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as the traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops, and estimated transit time.

Further, these are classified as follows:

(a) Isolated – In this method each, node makes its routing decisions using the information it has without seeking information from other nodes. The sending nodes don't have information about the status of a particular link. The disadvantage is that packets may be sent through a congested network which may result in delay. Examples: Hot potato routing, backward learning.

(b) Centralized – In this method, a centralized node has entire information about the network and makes all the routing decisions. The advantage of this is only one node is required to keep the information of the entire network and the disadvantage is that if the central node goes down the entire network is done. The link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

(c) Distributed – In this method, the node receives information from its neighbors and then takes the decision about routing the packets. A disadvantage is that the packet may be delayed if there is a change in between intervals in which it receives information and sends packets. It is also known as a decentralized algorithm as it computes the least-cost path between source and destination

2. Non Adaptive Algorithms: These are the algorithms that do not change their routing decisions once they have been selected. This is also known as static routing as a route to be taken is computed in advance and downloaded to routers when a router is booted.

Further, these are classified as follows:

(a) Flooding – This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in a loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count, and spanning trees.

(b) Random walk – In this method, packets are sent host by host or node by node to one of its neighbors randomly. This is a highly robust method that is usually implemented by sending packets onto the link which is least queued.

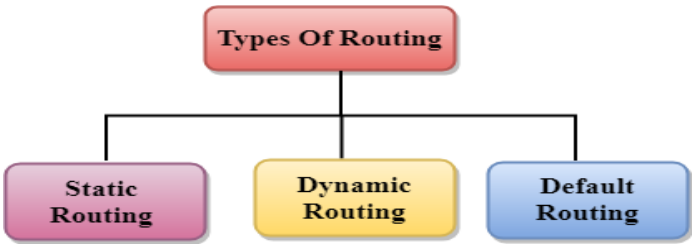
Routing v/s Flooding:

Routing	Flooding
--> Routing table is required.	--> No routing table is required.
--> May give shortest path.	--> Always gives shortest path.
--> Less reliable.	--> More reliable.
--> Traffic is less.	--> Traffic is high.
--> No duplicate packets.	--> Duplicate packets are present

ROUTING IN INTERNET:

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Types of Routing: Routing can be classified into three categories:



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 packets 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

Advantages of Static Routing:

Following are the advantages of Static Routing:

- **No Overhead:** It has ho 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.

Disadvantages of Static Routing:

Following are the disadvantages 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.

Default Routing:

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.

- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing:

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

The Dynamic protocol should have the following features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

Advantages of Dynamic Routing:

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing:

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

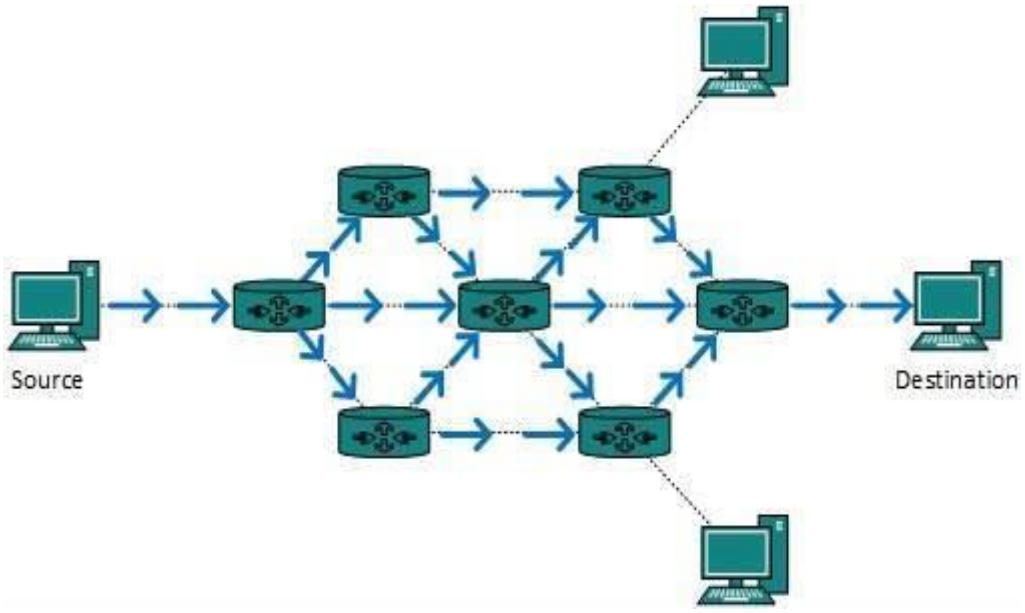
BROADCAST ROUTING:

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.

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 addresses. 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.

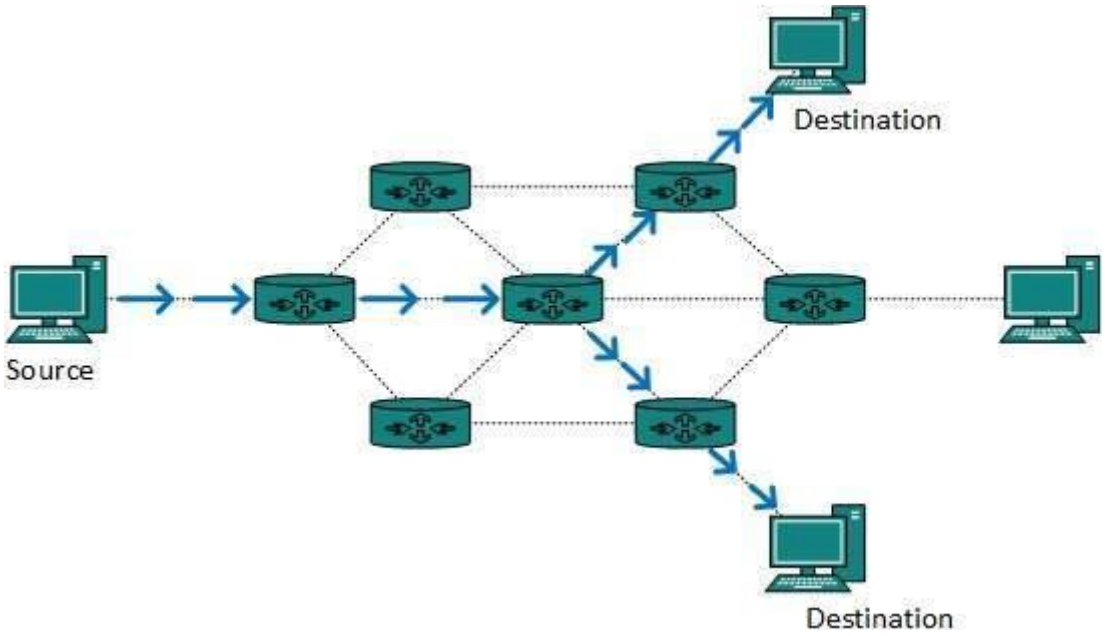


This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.

Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

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 router must know that there are nodes, which wish to receive multicast packets (or stream) 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.