Unit-4: Network Layer

- **Introduction**

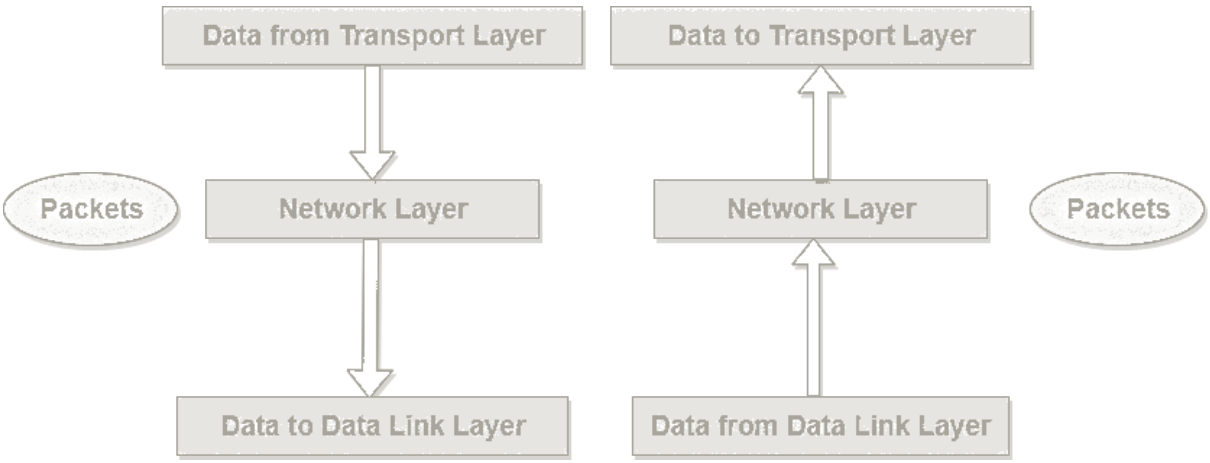
The network Layer controls the operation of the subnet. The main aim of this layer is to deliver packets from source to destination across multiple links (networks). If two computers (system) are connected on the same link, then there is no need for a network layer. It routes the signal through different channels to the other end and acts as a network controller.

It also divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

In broadcast networks, the routing problem is simple, so the network layer is often thin or even non-existent.

Functions of Network Layer

1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.



- **Virtual and Datagram Network**

In the network layer, these services are host-to-host services provided by the network layer for the transport layer. In the transport layer these services are process-to-process services provided by the transport layer for the application layer.

In all major computer network architectures to date (Internet, ATM, frame relay and so on), the network layer provides either host-to-host connectionless service or host-to-host connection service, but not both.

- Computer networks that provide only a connection service at the network layer are called virtual circuit (VC) networks
- Computer networks that provide only a connectionless service at the network layer are called datagram networks.

The implementations of connection oriented service in the transport layer and the connection service in the network layer are fundamentally different. We already know that the transport-layer connection-oriented service is implemented at the edge of the network in the end systems; we'll see shortly that the network-layer connection service is implemented in the routers in the network core as well as in the end systems.

Virtual circuit and datagram networks are two fundamental classes of computer networks. They use very different information in making their forwarding decision. Let's now take a closer look at their implementations.

Virtual Circuit Networks

While the internet is a datagram network, many alternative network architectures – including those of ATM (Asynchronous Transfer Mode) and frame relay – are virtual circuit networks and, therefore, use connections at the network layer. These network layer connections are called virtual circuits (VCs). Let's now consider how a VC service can be implemented in a computer network.

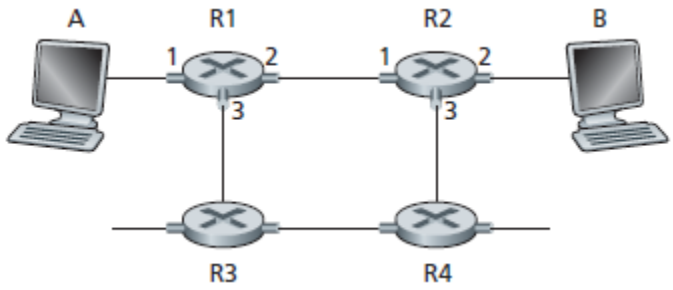
A VC consists of :

a path (that is , a series of links and routers) between the source and destination hosts,

VC numbers, one number for each link along the path, andentries 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.

How does the router determine the replacement VC number for a packet traversing the router? For a VC network, each router's forwarding table includes VC number translation; for example the forwarding table in R1 might look something like the table below

Whenever a new VC is established across a router, an entry is added to the forwarding table. Similarly, whenever a VC terminates, the appropriate entries in each table along its path are removed.

You might be wondering why a packet doesn't just keep the same VC number on each of the links along its route. The answer is twofold. First, replacing the number from the link reduces the length of the VC field in the packet header. Second, and more importantly, VC setup is considerably simplified by permitting a different VC number at each link along the path of the VC. Specifically, with multiple VC numbers, each link in the path can choose a VC number independently of the VC numbers chosen at other links along the path. If a common VC number were required for all links along the path, the routers would have to exchange and process a substantial number of messages to agree on a common VC number (e.g. one that is not being used by any other existing VC at these routers) to be used for a connection.

In a VC network, the network's routers must maintain connection state information for the ongoing connections. Specifically, each time a new connection is established across a router, a new connection entry must be added to the router's forwarding table; and each time a connection is released an entry must be removed from the table. Note that even if there is no VC number translation, it is still necessary to maintain connection state information that associates VC numbers with output interface numbers. The issue of whether or not a router maintains connection state information for each ongoing connection is a crucial one.

- **IP Protocol & Addressing**

If a device wants to communicate using TCP/IP, it needs an IP address. When the device has an IP address and the appropriate software and hardware, it can send and receive IP packets. Any device that can send and receive IP packets is called an IP host.

IP addresses consist of a 32-bit number, usually written in dotted-decimal notation. Each decimal number in an IP address is called an octet. The term octet is just a vendor- neutral term for byte . Finally, note that each network interface uses a unique IP address. Most people tend to think that their computer has an IP address, but actually their computer's network card has an IP address. If you put two Ethernet cards in a PC to forward IP packets through both cards, they both would need unique IP addresses.

RFC 791 defines the IP protocol, including several different classes of networks. IP defines three different network classes for addresses used by individual hosts—addresses called unicast Ip addresses. These three network classes are called A, B,

and C. TCP/IP defines Class D (multicast) addresses and Class E (experimental) addresses as well.
Class A, B, or C network have the same numeric value network portion of the addresses. The rest of the address is called the host portion of the address.
IP Add. 0.0.0.0 is reserved for the default network.
IP Add. 255.255.255.255 is Used for Broadcast.
Class A – Network. Host. Host. Host
Subnet mask - 255.0.0.0
Range - 1 to 126
1.0.0.0 to 126.0.0.0
Loop back Address- 127.0.0.1
That is designated for the Software loop back interface of a machine. The loop back interface has no hardware associated with it & it is not physically connected to network.
Class B – Network. Network . Host. Host
Subnet mask - 255.255.0.0
Range – 128 to 191
128.1.0.0 191.254.0.0
Class C – Network. Network . Network . Host
Subnet mask - 255.255.255.0
Range – 192 to 223
192.0.1.0 223.255.254.0
Class D – Multicast Addressing
Range- 224 to 239
224.0.0.5 & 224.0.0.6 OSPF Protocol.
224.0.0.9 RIPv2 Protocol.
224.0.0.10 EIGRP Protocol.
Other valid IP address using for Video Confer sing.
Class E- Experimental Address Range- 240 to 255.

Private IP Address Range –
In that IP address uniquely assign to particular computer. This address provide for (ISP). In the Internet addressing architecture, a private network is a network that uses private IP address space, These addresses are commonly used for home, office, and enterprise local area networks (LANs), These addresses are characterized as private because they are not globally delegated, meaning they are not allocated to any specific organization, and IP packets addressed by them cannot be transmitted onto the public Internet.

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks.
Class A - 10.0.0.0 – 10.255.255.255
Class B - 172.16.0.0 – 172.31.255.255
Class C - 192.168.0.0 – 192.168.255.255

Class	Starting Address	Ending Address	Subnet mask
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	255.255.255.255
E	240.0.0.0	255.255.255.255	255.255.255.255

- ## Router

Like bridges, *routers* are devices whose primary purpose is to connect two or more networks and to filter network signals so that only desired information travels between them. For
example, routers are often used to regulate the flow of information between school networks and the Internet. However, routers can inspect a good deal more information than bridges, and they
therefore can regulate network traffic more precisely. They also have another important capability: they are aware of many possible paths across the network and can choose the best one for each data packet to travel.
Features of Router :-
1) Multiple Active Paths
2) Identify address
3) Traffic Management
4) Sharing information
5) Filtering bad data
6) Performance
1) Multiple Active Paths:
Routers are able to keep track of multiple active paths between any given source and
destination network.
This makes it more flexible and active towards faults than bridge.
This is because in a bridge multiple online active paths are not allowed.
2) Identify address:

Routers work on Network layer and can access more information from packet than bridge.
Router can identify source and destination network addresses within packet.

3) Traffic Management:

Router provides excellent traffic management using intelligent path selection.
Router select the best route, which is based on traffic loads, line speeds, number of one
attached to another router.

4) Sharing information:

Router can share status and routing information with other routers. Routers can communicate
with each other by doing this they can listen to network and identify which connections are
busy and which are not.

5)Filtering bad data:

Routers do not forward any information that does not have a correct network address. This is
the reason they don't forward bad data.

6)Performance:

Routers perform complex task and it is continuously busy to execute network data. This means they are slower than bridge because they keep processing data intensively.

Types of Routing :-

There are two types of routers 1.Static Router 2.Dynamic Router

1) Static Router :-

Each router has its own software called 'Routing Table'. Administrator is a person who configures and maintains whole network as well as networking devices. Administrators have to manually configure routes between each network when the routers do
not communicate amongst themselves that type of routers are called static routers. Its advantage is that complete control remains with the network administrator.

2) Dynamic Router :-

Dynamic routers are those routers, which automatically find their own routes by communicating with each other.
These routers are self configured. This is because their routing tables are built and modified through these communications and these changes are quickly reflected. e.g. router failure PR broken links.

- **Routing algorithm**

In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.

Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.

The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.

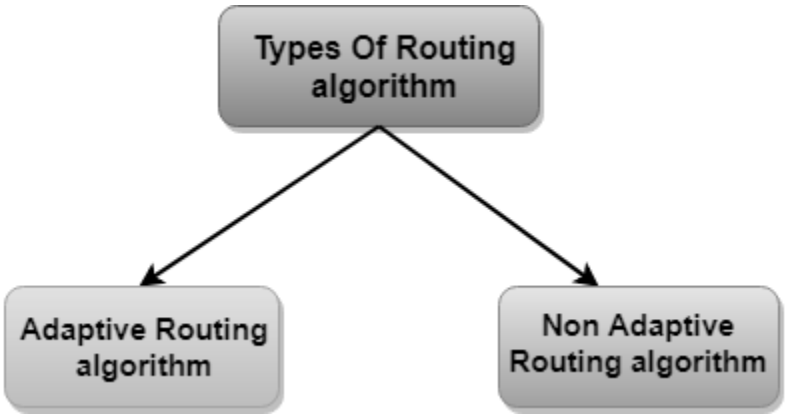
Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

Adaptive Routing algorithm

Non-adaptive Routing algorithm



Adaptive Routing algorithm

An adaptive routing algorithm is also known as dynamic routing algorithm.

This algorithm makes the routing decisions based on the topology and network traffic.

The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

Centralized algorithm: It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. Link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

Isolation algorithm: It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.

Distributed algorithm: It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm

Non Adaptive routing algorithm is also known as a static routing algorithm.

When booting up the network, the routing information stores to the routers.

Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Broadcast and Multicast Routing

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software based routers have limited functionality and limited scope.

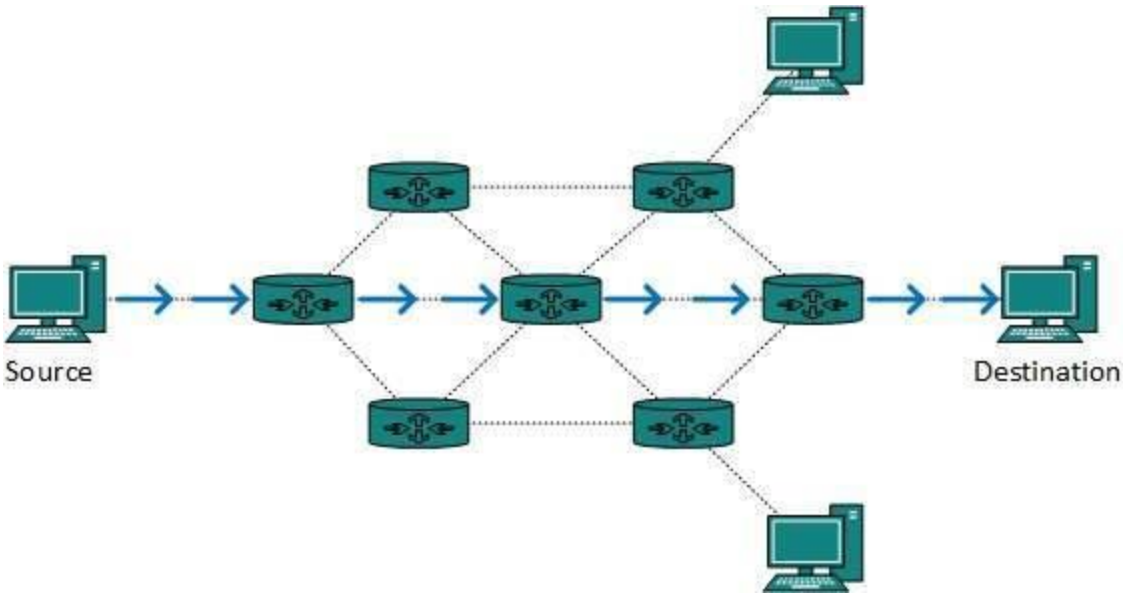
A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

- Hop Count
- Bandwidth
- Metric
- Prefix-length
- Delay

Routes can be statically configured or dynamically learnt. One route can be configured to be preferred over others.

Unicast routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with 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. Hence the router just has to look up the routing table and forward the packet to next hop.



Broadcast routing

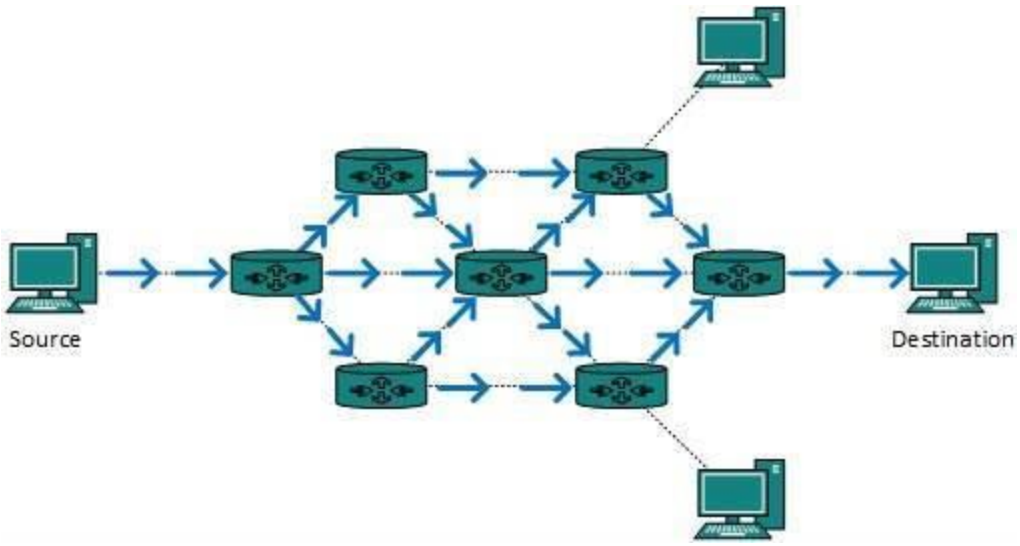
By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

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.

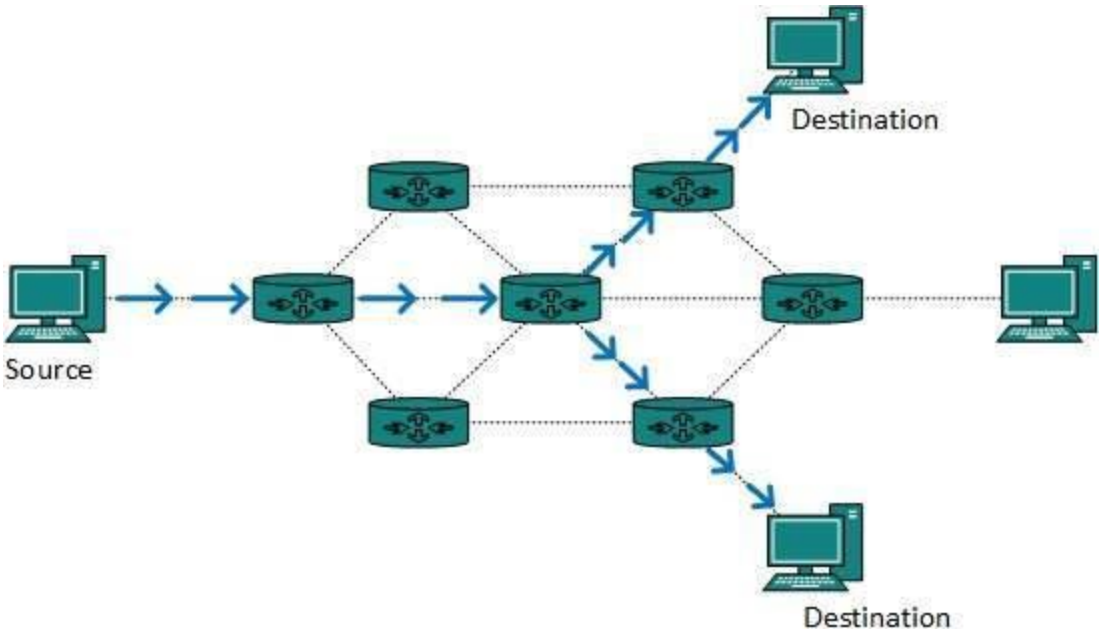


This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.

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.