UNIT 3

#) Network Layer

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

- Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- Logical Addressing: Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.
- Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

#) Network addressing :

- A network address always points to host / node / server or it can represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.
- Network Addressing is one of the major responsibilities of the network layer.
- Network addresses are always logical, i.e., software-based addresses.
- A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.

The most widely used network address is an IP address. It uniquely identifies a node in an IP network. An IP address is a 32-bit long numeric address represented in a form of dot-decimal notation where each byte is written in a decimal form separated by a period.

The first three bytes of an IP address represents the network and the last byte specifies the host in the network. An IP address is further divided into sub classes :

- Class A : An IP address is assigned to those networks that include large number of hosts.
- Class B : An IP address is assigned to networks range from small sized to large sized.
- Class C : An IP address is assigned to networks that are small sized.
- Class D : IP address are reserved for multicast address and does notpossess subnetting.
- Class E : An IP address is used for the future use and for the research and development purposes and does not possess any subnetting.

An IP address is divided into two parts:

1. Network ID : represents the number of networks.
2. Host ID : represents the number of hosts.

#) Subnetting

Subnetting is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.
IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.
It also helps you to reduce the size of the routing tables, which is stored in routers. This method also helps you to extend the existing IP address base & restructures the IP address.

Why Use Subnetting?

- It helps you to maximise IP addressing efficiency.
- Extend the life of IPV4.
- Public IPV4 Addresses are scarce.
- IPV4 Subnetting reduces network traffic by eliminating collision and broadcast traffic and thus improves overall performance.
- This method allows you to apply network security policies at the interconnection between subnets.
- Optimized IP network performance.
- Facilitates spanning of large geographical distances.
- Subnetting process helps to allocate IP addresses that prevent large numbers of IP network addresses from remaining unused.
- Subnets are usually set up geographically for specific offices or particular teams within a business that allows their network traffic to stay within the location.

Limitations of subnetting

While subnetting offers many advantages, it can also result in some disadvantages:

- Communication between one subnet to another subnet requires a router. A poorly configured or fatally failed router can significantly impact your organization's network.
- Since each subnet requires dedicated IP addresses as subnet ID and broadcast address, it wastes IP addresses.
- Creating too many subnets can create unnecessary complexity and impact the effectiveness of network administration.

What is Subnet Mask?

A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address. A subnet mask identifies which part of an IP address is the network address and the host address. They are not shown inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.

#) Routing

- 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.

#) Routing techniques

Routing can be classified into three categories:

- Static Routing
- Default Routing
- Dynamic Routing

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.

#) Routing Table:

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
default		Eth2

Entries of an IP Routing Table:

A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.

Each entry in the routing table consists of the following entries:

1. Network ID:

The network ID or destination corresponding to the route.

2. Subnet Mask:

The mask that is used to match a destination IP address to the network ID.

3. Next Hop:

The IP address to which the packet is forwarded

4. Outgoing Interface:

Outgoing interface the packet should go out to reach the destination network.

5. Metric:

A common use of the metric is to indicate the minimum number of hops (routers crossed) to the

network ID.

#) Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.
DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.
  DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

Benefits of DHCP

There are following benefits of DHCP:

- Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

- Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

- Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

- Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

#) 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 Routing Algorithms: The routing algorithms can be classified as follows:

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.

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.

#) Distance Vector Routing

- It is a dynamic routing algorithm in which each router computes a distance between itself and each possible destination i.e. its immediate neighbours.
- The router shares its knowledge about the whole network to its neighbours and accordingly updates the table based on its neighbours.
- The sharing of information with the neighbour's takes place at regular intervals.
- It makes use of Bellman-Ford Algorithm for making routing tables.
- The Distance vector algorithm is iterative, asynchronous and distributed.
    - Distributed: It is distributed in that each node receives information from one or more of its directly attached neighbours, performs calculation and then distributes the result back to its neighbours.
    - Iterative: It is iterative in that its process continues until no more information is available to be exchanged between neighbours.
    - Asynchronous: It does not require that all of its nodes operate in the lock step with each other.
- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as Vector.

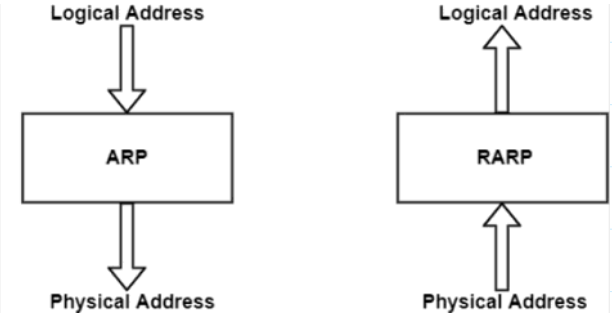
#) Link State Routing

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbours with every other router in the network.
- A router sends its information about its neighbours only to all the routers through flooding.
- Information sharing takes place only whenever there is a change.
- It makes use of Dijkstra's Algorithm for making routing tables.

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

#) ARP

Address Resolution Protocol (ARP) is a network-specific standard protocol. The Address Resolution Protocol is important for changing the higher-level protocol address (IP addresses) to physical network addresses. It is described in RFC 826.



ARP relates an IP address with the physical address. On a typical physical network such as LAN, each device on a link is identified by a physical address, usually printed on the network interface card (NIC). A physical address can be changed easily when NIC on a particular machine fails.

The IP Address cannot be changed. ARP can find the physical address of the node when its internet address is known. ARP provides a dynamic mapping from an IP address to the corresponding hardware address.

Types of ARP

There are four types of Address Resolution Protocol, which is given below:

- Proxy ARP
- Gratuitous ARP
- Reverse ARP
- Inverse ARP

Proxy ARP:

In the Proxy ARP method, Layer 3 devices can respond to ARP requests. This ARP type is configured router will respond to the target IP address and maps the router's MAC address with the target IP address and sender when it is reached to its destination.

Gratuitous ARP:

Gratuitous is another type of ARP request of the host. This type of ARP request helps the network to identify

the duplicate IP address. Therefore, when an ARP request is sent by a router or switch to get its IP address, no ARP responses are received so that no other nodes can use the IP address allocated to that switch or router.

Reverse ARP (RARP):
Reverse ARP, also now called RARP, is a type of ARP networking protocol which is used by the client system in a LAN to request its IPV4 address from the ARP router table. The network admin mostly creates a table in the gateway-router, which helps determine the MAC address to that specific IP address.

Inverse ARP (InARP):
Inverse ARP is also called InARP, is a type of ARP used to find the nodes' IP of addresses from the data link layer addresses. InARP is widely used for ATM networks frame relays where Layer 2 virtual circuit addressing acquired from Layer 2 signalling.

Advantages of ARP
Here are the pros/benefits of using ARP

- If you are using ARP, then MAC addresses can easily be known if you know the IP address of the same system.
- End nodes should not be configured to "know" MAC addresses. It can be found when needed.
- ARP's goal is to enable each host on a network that allows you to build up a mapping between IP addresses and physical addresses.
- The set of mappings or table stored in the host is called ARP table or ARP cache.

Disadvantages of using ARP

- ARP attacks such as ARP spoofing and ARP denial of service may occur.

#) Difference Between ARP and RARP

S.NO	ARP	RARP
1.	ARP stands for Address Resolution Protocol.	Whereas RARP stands for Reverse Address Resolution Protocol.
2.	Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.	Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.
3.	In ARP, broadcast MAC address is used.	While in RARP, broadcast IP address is used.
4.	In ARP, ARP table is managed or maintained by local host.	While in RARP, RARP table is managed or maintained by RARP server.
5.	In Address Resolution Protocol, Receiver's MAC address is fetched.	While in RARP, IP address is fetched.
6.	In ARP, ARP table uses ARP reply for its updation.	While in RARP, RARP table uses RARP reply for configuration of IP addresses .
7.	Hosts and routers uses ARP for knowing the MAC address of other hosts and routers in the networks.	While RARP is used by small users having less facilities.

#) ICMP

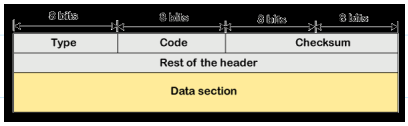
The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose

network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.
The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination.
A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP.

ICMP Message Format

The message format has two things; one is a category that tells us which type of message it is. If the message is of error type, the error message contains the type and the code. The type defines the type of message while the code defines the subtype of the message.

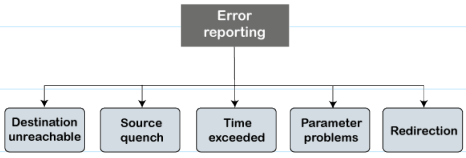
The ICMP message contains the following fields:



ICMP Protocol
Type: It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPV6, and the values from 128 to 255 are the informational messages.
Code: It is an 8-bit field that defines the subtype of the ICMP message
Checksum: It is a 16-bit field to detect whether the error exists in the message or not

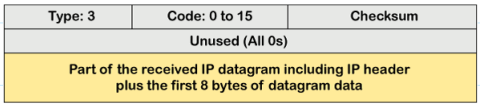
Types of Error Reporting messages

The error reporting messages are broadly classified into the following categories:



- Destination unreachable

The destination unreachable error occurs when the packet does not reach the destination. Suppose the sender sends the message, but the message does not reach the destination, then the intermediate router reports to the sender that the destination is unreachable.

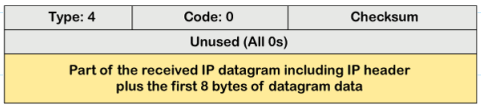


The above diagram shows the message format of the destination unreachable message. In the message format:
Type: It defines the type of message. The number 3 specifies that the destination is unreachable.
Code (0 to 15): It is a 4-bit number which identifies whether the message comes from some intermediate router or the destination itself.
Note: If the destination creates the destination unreachable message then the code could be either 2 or 3.

- Source quench

There is no flow control or congestion control mechanism in the network layer or the IP protocol. The sender is concerned with only sending the packets, and the sender does not think whether the receiver is ready to receive those packets or is there any congestion occurs in the network layer so that the sender can send a lesser

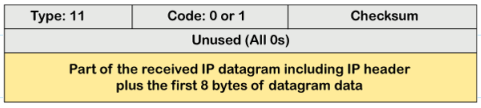
number of packets, so there is no flow control or congestion control mechanism. In this case, ICMP provides feedback, i.e., source quench. Suppose the sender resends the packet at a higher rate, and the router is not able to handle the high data rate. To overcome such a situation, the router sends a source quench message to tell the sender to send the packet at a lower rate.



Note: A source quench message informs the sender that the datagram has been discarded due to the congestion occurs in the network layer.
So, the sender must either stop or slow down the sending of datagrams until the congestion is reduced. The router sends one source-quench message for each datagram that is discarded due to the congestion in the network layer.

- Time exceeded

Sometimes the situation arises when there are many routers that exist between the sender and the receiver. When the sender sends the packet, then it moves in a routing loop. The time exceeded is based on the time-to-live value. When the packet traverses through the router, then each router decreases the value of TTL by one. Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source.



#) 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.

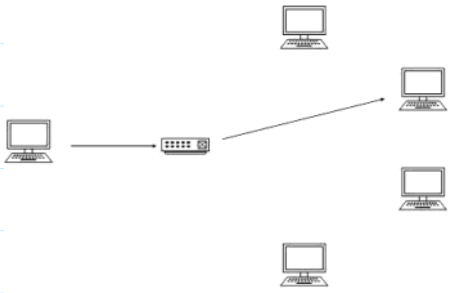
#) IPV6

IPV6 or Internet Protocol Version 6 is an upgrade of IPV4. IP version 6 is a network layer protocol that allows data communications to pass packets over a network. This involves sending and receiving data in the form of packets between 2 nodes in a network.

IPV6 offers several types of modes by which a single host can be addressed. More than one host can be addressed at once or the host at the closest distance can be addressed.

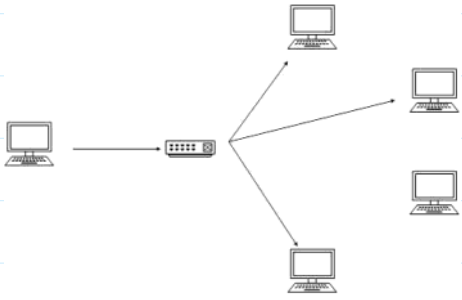
Unicast

In unicast mode of addressing, an IPV6 interface (host) is uniquely identified in a network segment. The IPV6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment. When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.



Multicast

The IPV6 multicast mode is same as that of IPV4. The packet destined to multiple hosts is sent on a special multicast address. All the hosts interested in that multicast information, need to join that multicast group first. All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.



Anycast

IPV6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.

Advantages of IPV6

- Reliability
- Faster Speeds: IPV6 supports multicast rather than broadcast in IPV4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- Stringer Security: IP Security, which provides confidentiality, and data integrity, is embedded into IPV6.
- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network.

Disadvantages of IPV6

- Conversion: Due to widespread present usage of IPV4 it will take a long period to completely shift to IPV6.
- Communication: IPV4 and IPV6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

#) Flooding :

flooding occurs when a router uses a nonadaptive routing algorithm to send an incoming packet to every outgoing link except the node on which the packet arrived.
Flooding is a way to distribute routing protocols updates quickly to every node in a large network. Examples of these protocols include the Open Shortest Path First and Distance Vector Multicast Routing Protocol.
Network flooding also has some other uses, including the following:

- multicasting data packets from one source node to many specific nodes in a real or virtual network;
- bridging;
- peer-to-peer file sharing; and
- and ad hoc wireless networks.

Types of Flooding

Flooding may be of three types —

- Uncontrolled flooding — Here, each router unconditionally transmits the incoming data packets to all its neighbours.
- Controlled flooding — They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF).
- Selective flooding — Here, the routers don't transmit the incoming packets only along those paths which are heading towards approximately in the right direction, instead of every available paths

Advantages of Flooding

- It is very simple to setup and implement, since a router may know only its neighbours.
- It is extremely robust.
- All nodes which are directly or indirectly connected are visited.
- The shortest path is always chosen by flooding.

Limitations of Flooding

- Flooding tends to create an infinite number of duplicate data packets, unless some measures are adopted to damp packet generation.
- It is wasteful if a single destination needs the packet, since it delivers the data packet to all nodes irrespective of the destination.
- The network may be clogged with unwanted and duplicate data packets. This may hamper delivery of other data packets.