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:

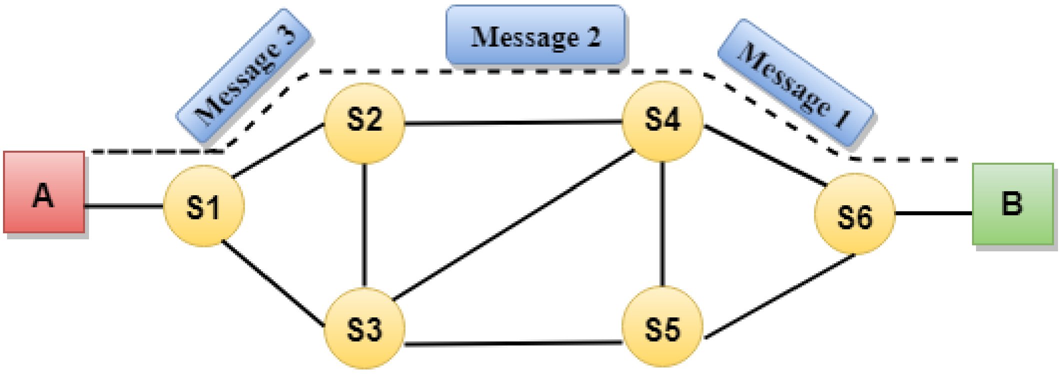
- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the 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.

Switching

In large networks, there can be multiple paths from sender to receiver. The switching technique will
decide the best route for data transmission.
Switching technique is used to connect the systems for making one-to-one communication.

Circuit Switching:

o Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
o In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
o Circuit switching in a network operates in a similar way as the telephone works.
o A complete end-to-end path must exist before the communication takes place.
o In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability
of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
o Circuit switching is used in public telephone network. It is used for voice transmission.
o Fixed data can be transferred at a time in circuit switching technology.



Advantages of Circuit Switching:

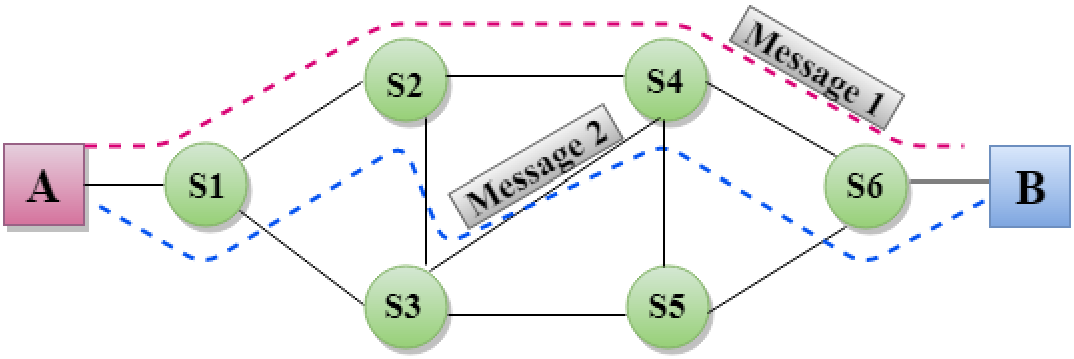
o In the case of Circuit Switching technique, the communication channel is dedicated.
o It has fixed bandwidth.

Disadvantages of Circuit Switching:

o Once the dedicated path is established, the only delay occurs in the speed of data transmission.
o It takes a long time to establish a connection approx. 10 seconds during which no data can be transmitted.
o It is more expensive than other switching techniques as a dedicated path is required for each connection.
o It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
o In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching:

o Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
o In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
o The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
o Message switches are programmed in such a way so that they can provide the most efficient routes.
o Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network.
o Message switching treats each message as an independent entity.



Advantages of Message Switching

o Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
o Traffic congestion can be reduced because the message is temporarily stored in the nodes.
o Message priority can be used to manage the network.
o The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

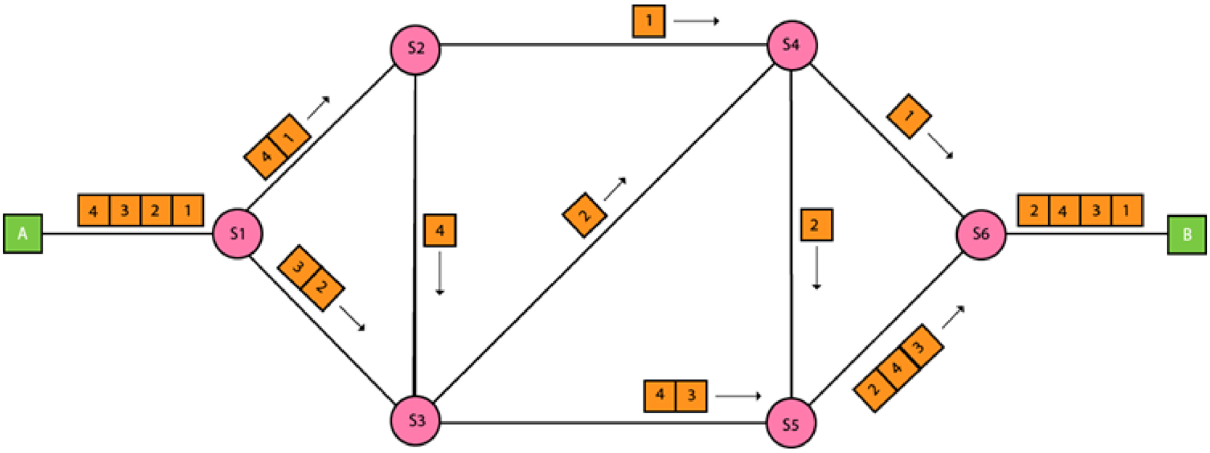
Disadvantages of Message Switching

o The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
o The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching:

o The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
o The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
o Every packet contains some information in its headers such as source address, destination address and sequence number.
o Packets will travel across the network, taking the shortest path as possible.
o All the packets are reassembled at the receiving end in correct order.
o If any packet is missing or corrupted, then the message will be sent to resend the message.

o If the correct order of the packets is reached, then the acknowledgment message will be sent.



Advantages of Packet Switching:

o Cost-effective: In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.

o Reliable: If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.

o Efficient: Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages of Packet Switching:

o Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.

o The protocols used in a packet switching technique are very complex and requires high implementation cost.

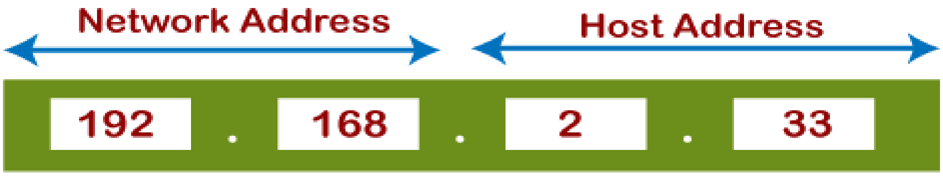
o If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Internet Protocol (IP)

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

IP Address Format

Originally IP addresses were divided into five different categories called **classes**. These divided IP classes are class A, class B, class C, class D, and class E. Out of these, classes A, B, and C are most important. Each address class defines a different number of bits for its **network prefix (network address)** and **host number (host address)**. The starting address bits decide from which class an address belongs.

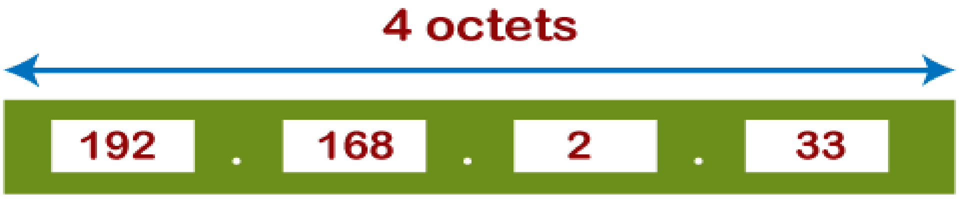


Network Address: The network address specifies the unique number which is assigned to your network. In the above figure, the network address takes two bytes of IP address.

Host Address: A host address is a specific address number assigned to each host machine. With the help of the host address, each machine is identified in your network. The network address will be the same for each host in a network, but they must vary in host address.

Address Format IPv4

The address format of IPv4 is represented into **4-octets** (32-bit), which is divided into three different classes, namely class A, class B, and class C.



The above diagram shows the address format of IPv4. An IPv4 is a 32-bit decimal address. It contains four octets or fields separated by 'dot,' and each field is 8-bit in size. The number that each field contains should be in the range of 0-255.

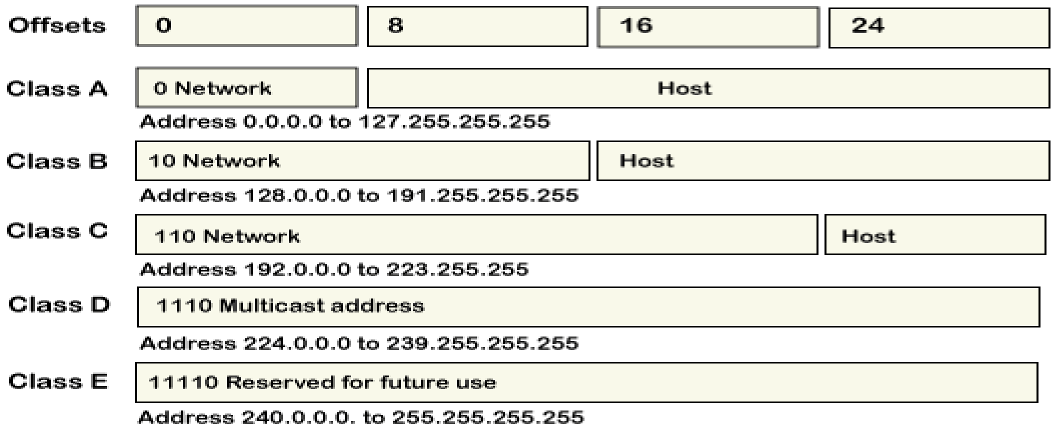
Class A address uses only first higher order octet (byte) to identify the network prefix, and remaining three octets (bytes) are used to define the individual host addresses. The class A address ranges between 0.0.0.0 to 127.255.255.255. The first bit of the first octet is always set to 0 (zero), and next 7 bits determine network address, and the remaining 24 bits determine host address. So, the first octet ranges from 0 to 127 (00000000 to 01111111).

Class B addresses use the initial two octets (two bytes) to identify the network prefix, and the remaining two octets (two bytes) define host addresses. The class B addresses are range between 128.0.0.0 to 191.255.255.255. The first two bits of the first higher octet is always set to 10 (one and zero bit), and next 14 bits determines the network address and remaining 16 bits determines the host address. So the first octet ranges from 128 to 191 (10000000 to 10111111).

Class C addresses use the first three octets (three bytes) to identify the network prefix, and the remaining last octet (one byte) defines the host address. The class C address ranges between 192.0.0.0 to 223.255.255.255. The first three bit of the first octet is always set to 110, and next 21 bits specify network address and remaining 8 bits specify the host address. Its first octet ranges from 192 to 223 (11000000 to 11011111).

Class D IP address is reserved for multicast addresses. Its first four bits of the first octet are always set to 1110, and the remaining bits determine the host address in any IP address. The first higher octet bits are always set to 1110, and the remaining bits specify the host address. The class D address ranges between 224.0.0.0 to 239.255.255.255. In multicasting, data is not assigned to any particular host machine, so it is not require to find the host address from the IP address, and also, there is no subnet mask present in class D.

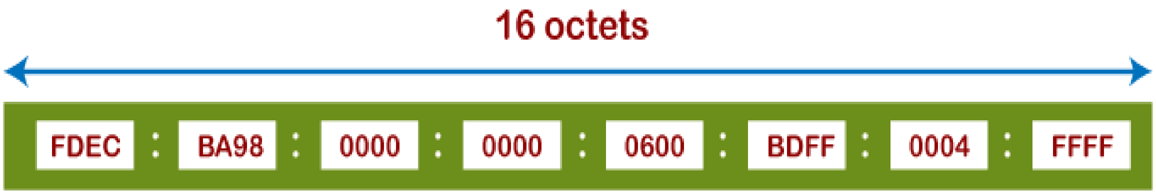
Class E IP address is reserved for experimental purposes and future use. It does not contain any subnet mask in it. The first higher octet bits are always set to 1111, and next remaining bits specify the host address. Class E address ranges between 240.0.0.0 to 255.255.255.255.


Offsets
0
8
16
24
Class A
0 Network
Host
Address 0.0.0.0 to 127.255.255.255
Class B
10 Network
Host
Address 128.0.0.0 to 191.255.255.255
Class C
110 Network
Host
Address 192.0.0.0 to 223.255.255
Class D
1110 Multicast address
Address 224.0.0.0 to 239.255.255.255
Class E
11110 Reserved for future use
Address 240.0.0.0. to 255.255.255.255

In every IP address class, all host-number bits are specified by a power of 2 that indicates the total numbers of the host's address that can create for a particular network address. Class A address can contain the maximum number of 2^{24} (16,777,216) host numbers. Class B addresses contain the maximum number of 2^{16} (65, 536) host numbers. And class C contains a maximum number of 2^{8} (256) host numbers.

IP Address Format IPv6

All IPv6 addresses are 128-bit hexadecimal addresses, written in 8 separate sections having each of them have 16 bits. As the IPv6 addresses are represented in a hexadecimal format, their sections range from 0 to FFFF. Each section is separated by colons (:). It also allows to removes the starting zeros (0) of each 16-bit section. If two or more consecutive sections 16-bit contains all zeros (0 : 0), they can be compressed using double colons (::).



IPv6 addresses are consist of 8 different sections, each section has a 16-bit hexadecimal values separated by colon (:). IPv6 addresses are represented as following format:

```
xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx
```

Each "xxxx" group contains a 16-bit hexadecimal value, and each "x" is a 4-bit hexadecimal value. For example:

```
FDEC : BA98 : 0000 : 0000 : 0600 : BDFF : 0004 : FFFF
```

IP Address Table

On the basis of ranges, IP addresses are categorized into five address classes which are given below.

Class	Higher bits	Network address bits	Host address bits	No. of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 125.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	224.0.0.0 to 239.255.255.255
E	1111	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	Not defined and reserved for future	240.0.0.0 to 255.255.255.255

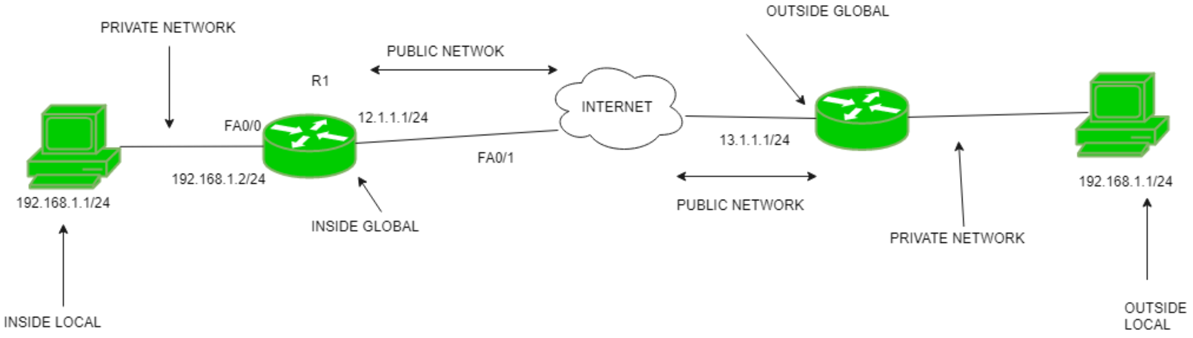
Network Address Translation (NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.



- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.
- **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address –** This is the actual IP address of the destination host in the local network after translation.
- **Outside global address –** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

- Advantages of NAT –
- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunnelling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

Subnetting

Subnetting is a method of dividing a single physical network into numerous smaller logical sub-networks. These subnetworks are referred to as subnets. An IP address is formed by combining a network and host segments. A subnet is created by accepting bits from the IP address host part and is used to split the original network into smaller subnetworks.

The process of subnetting involves turning host bits into network bits. Its approach was originally intended to slow the depletion of IP addresses. It permits the administrator to split a single class A, class B, or class C network into smaller sections. ***VLSM (Variable Length Subnet Mask)*** divides IP address space into subnets of varying sizes while preventing memory waste. Furthermore, ***FLSM (Fixed Length Subnet Mask)*** occurs when the number of hosts in subnets is the same.

Advantages

1. Subnetting reduces broadcast volume and hence reduces network traffic.
2. The permitted host numbers in the local area network are increased by subnetting.
3. Subnetworks are simple to handle and maintain.
4. The network security may easily be utilized amongst sub-networks instead of using it on the entire network.
5. It increases the flexibility of address.

Disadvantages

1. You require a qualified administrator to perform the subnetting process.
2. The subnetting process is quite expensive.

CIDR

Classless Inter-Domain Routing (CIDR) is a network routing method that is utilized to route network traffic over the internet. CIDR is a supernetting technology in which many subnets are joined for network routing. To put it another way, CIDR allows IP addresses to be organized in subnetworks regardless of their value.

Advantages

1. The router memory table size is reduced by condensing numerous routing data entries into a single entry.
2. It also minimizes network traffic.
3. It also speeds up the lookup of routing tables.
4. It allows the router to isolate topology changes from other routers.

Disadvantages

1. The supernet's networks must all use the same IP address class.
2. The block combination should be constructed in power 2; if three blocks are required, then four blocks must be assigned.
3. The entire network should be in the same class.

ARP

- ARP stands for Address Resolution Protocol.
- It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

RARP

- RARP stands for **Reverse Address Resolution Protocol**.
- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

ICMP

- ICMP stands for Internet Control Message Protocol.
- The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- ICMP uses echo test/reply to check whether the destination is reachable and responding.
- ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ICMP messages are transmitted within IP datagram.

IGMP

- IGMP stands for **Internet Group Message Protocol**.
- The IP protocol supports two types of communication:
  - **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.

    - **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
- The IGMP protocol is used by the hosts and router to support multicasting.
- The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.
- IGMP is a part of the IP layer, and IGMP has a fixed-size message.
- The IGMP message is encapsulated within an IP datagram.

Network 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.

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

- **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:

- 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.

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.

Distance Vector Routing:

The distance vector (DV) protocol is the oldest routing protocol in practice. With distance vector routes are advertised based upon the following **characteristics**:

- **Distance** - How far the destination network is based upon a metric such as hop count.
- **Vector** - The direction (next-hop router or egress interface) required to get to the destination.

This routing information is **exchanged between directly connected neighbours**.[2] Therefore when a node receives a routing update, it has no knowledge of where the neighbour learned it from. In other words, the node has no visibility of the network past its own neighbour. This part of distance vector is also known as "**routing by rumour**".

Furthermore, routing updates are sent in full (rather than delta-based updates) and at regular intervals, resulting in extremely **slow convergence times** - one of the key downfalls to distance vector protocols. In addition, due to the slow convergence times and "routing by rumour", distance vector protocols are prone to **routing loops**.

Link-state Routing:

In contrast to distance vector routing, link state routing (OSPF, ISIS) relies on each node advertising/**flooding** the **state** (i.e. delay, bandwidth etc) of their **links** to every node within the link state domain. This results in each node building a complete map of the network (**shortest path tree**), with itself as the root using the shortest path first algorithm, also known as the Dijkstra algorithm.

Unlike distance vector link-state neighbours only sends **incremental routing updates** (LSAs) rather than a full routing update. Also, these updates are only sent at the point a change in the **network topology occurs**, rather than at regular intervals.

Link-state protocols provide extremely low convergence times and, due to each router having a complete view of the network, aren't prone to the same routing loops seen with DV-based protocols.

However, due to the computation required for the algorithms to run across the shortest path trees upon each node, greater resources are consumed compared to that of distance vector, however, this really isn't a concern with the systems of today.

Path Vector Routing:

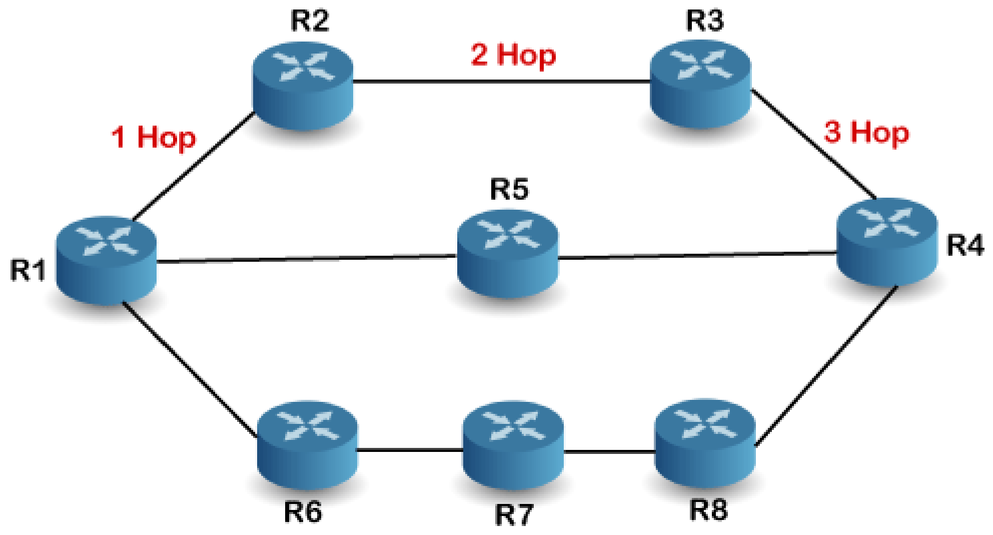
Path vector (PV) protocols, such as BGP, are used **across domains** aka autonomous systems. In a path vector protocol, a router does not just receive the distance vector for a particular destination from its neighbour; instead, a node receives the distance *as well* as **path information** (aka BGP path attributes), that the node can use to calculate (via the BGP path selection process) how traffic is routed to the destination AS

Routing Protocols:

RIP Protocol

RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

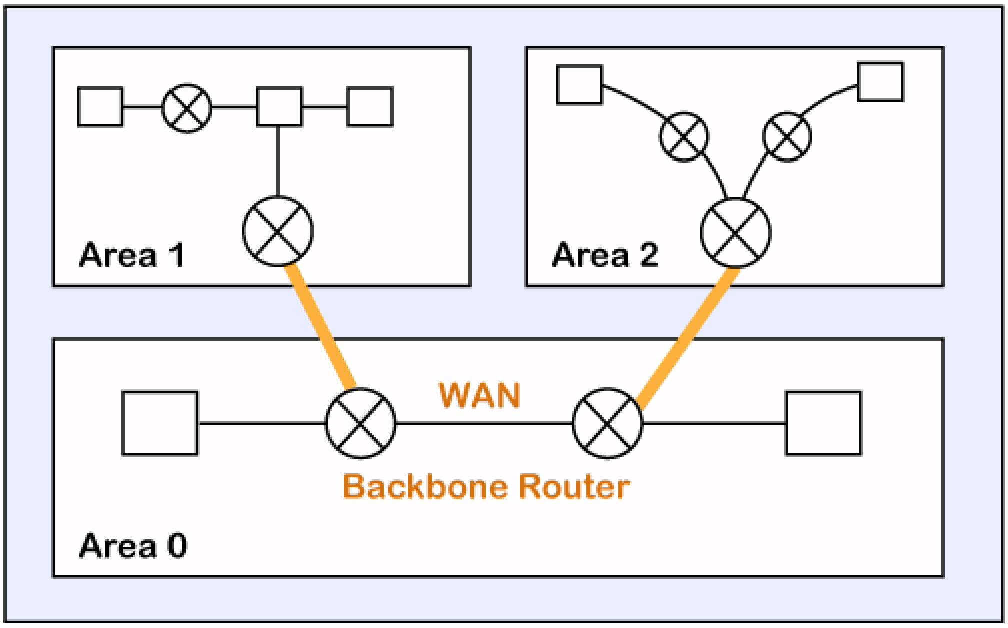
- RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
- In a routing table, the first column is the destination, or we can say that it is a network address.
- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- The next column contains the address of the router to which the packet is to be sent to reach the destination.



In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, RIP can support maximum up to 15 hops, which means that the 16 routers can be configured in a RIP.

OSPF Protocol

The OSPF stands for **Open Shortest Path First**. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network. It is an interior gateway protocol that has been designed within a single autonomous system. It is based on a link-state routing algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to learn routes. The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network. The way the router learns this information by sending LSA (Link State Advertisements). These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB. The main goal is to have the same information about every router in an LSDBs.



OSPF divides the autonomous systems into areas where the area is a collection of networks, hosts, and routers. Like internet service providers divide the internet into a different autonomous system for easy management and OSPF further divides the autonomous systems into Areas.

Routers that exist inside the area flood the area with routing information

In Area, the special router also exists. The special routers are those that are present at the border of an area, and these special routers are known as Area Border Routers. This router summarizes the information about an area and shares the information with other areas.

Border Gateway Protocol

It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes.

The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router. BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers.

Characteristics of Border Gateway Protocol (BGP):

- Inter-Autonomous System Configuration: The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- Path Information: BGP advertisement also include path information, along with the reachable destination and next destination pair.
- Policy Support: BGP can implement policies that can be configured by the administrator. For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.
- Runs Over TCP.
- BGP conserve network Bandwidth.
- BGP supports CIDR.
- BGP also supports Security.

MPLS Protocol:

Multiprotocol Label Switching, or MPLS, is a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide area networks. As a scalable and protocol-independent solution, MPLS assigns labels to each data packet, controlling the path the packet follows. MPLS greatly improves the speed of traffic, so users don't experience downtime when connected to the network.

Routing in MANET:

Ad-hoc On-demand Distance Vector (AODV):

AODV is a kind of reactive protocols. Its methodology is hop-to-hop routing. The node establishes the Route Request (RREQ) if it wants to know the route to a particular destination. Then the intermediate nodes forward the route request and at the same time, these intermediate nodes create a reverse route to the destination.

When the node receives the request that has the route to the destination, it establishes a Route Reply (RREP) which includes numeral of hops which are required to arrive the destination. Each node that cooperates in sending this reply to the source node, it creates a forward route to the destination.

Figure shows the routing of RREQ and RREP in AODV protocol. This route that has been established from source to destination is a hop-by-hop case.

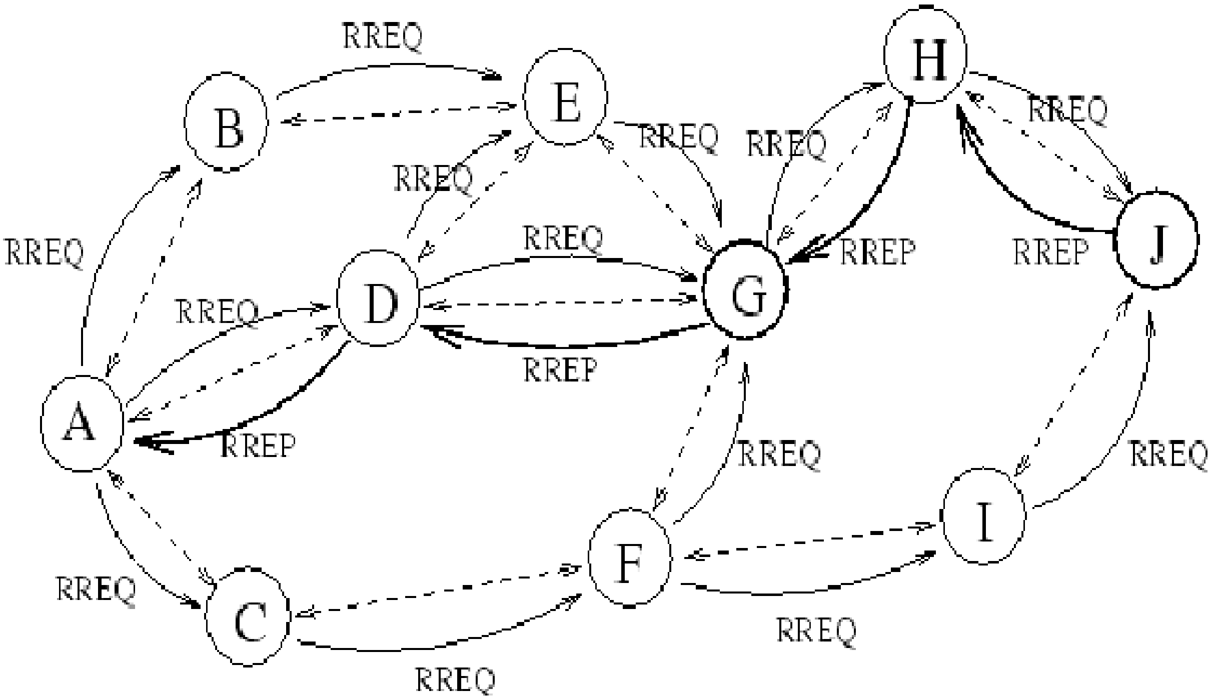


Fig.: RREQ and RREP in AODV

Dynamic Source Routing (DSR):

DSR is a reactive or on-demand routing protocol. This protocol has been designed to reduce the bandwidth wasted via the control packets in wireless networks and that via deleting the periodic table-update messages required in the table-driven approach.

In DSR protocol, there is no need for network infrastructure or administration, due to these networks fully self-configured and organized. The source routing is a method which the source packet defines the complete sequence of nodes through which to forward the data packets. The source routing does not need to keep the routing information via the intermediate hops.

Mobile IP

This is an **IETF (Internet Engineering Task Force)** standard communications protocol designed to allow mobile devices' (such as laptop, PDA, mobile phone, etc.) users to move from one network to another while maintaining their permanent IP (Internet Protocol) address.

Defined in RFC (Request for Comments) 2002, mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

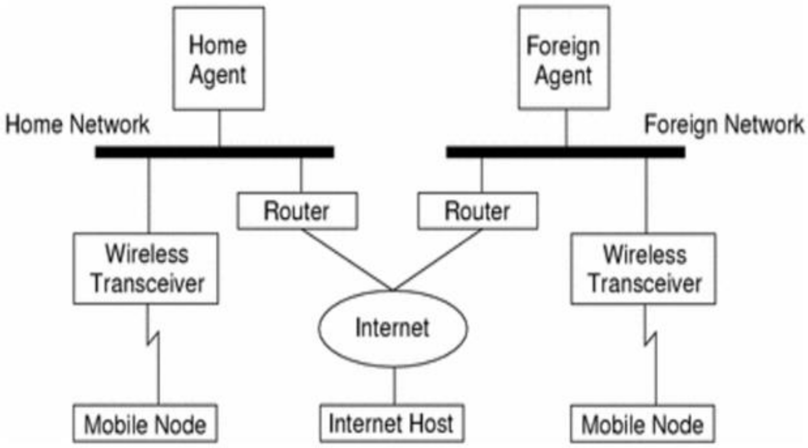


Fig: Mobile IP topology

- First of all, the internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
- If the mobile node (MN) is on its home network, the datagram is delivered through the normal IP (Internet Protocol) process to the mobile node. Otherwise the home agent picks up the datagram.
- If the mobile node (MN) is on foreign network, the home agent (HA) forwards the datagram to the foreign agent.
- The foreign agent (FA) delivers the datagram to the mobile node.
- Datagrams from the MN to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The FA forwards the datagram to the Internet host.

In the case of wireless communications, the above illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the MN use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address (COA) is used only for communication with mobility agents and is never seen by the Internet host.