

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:

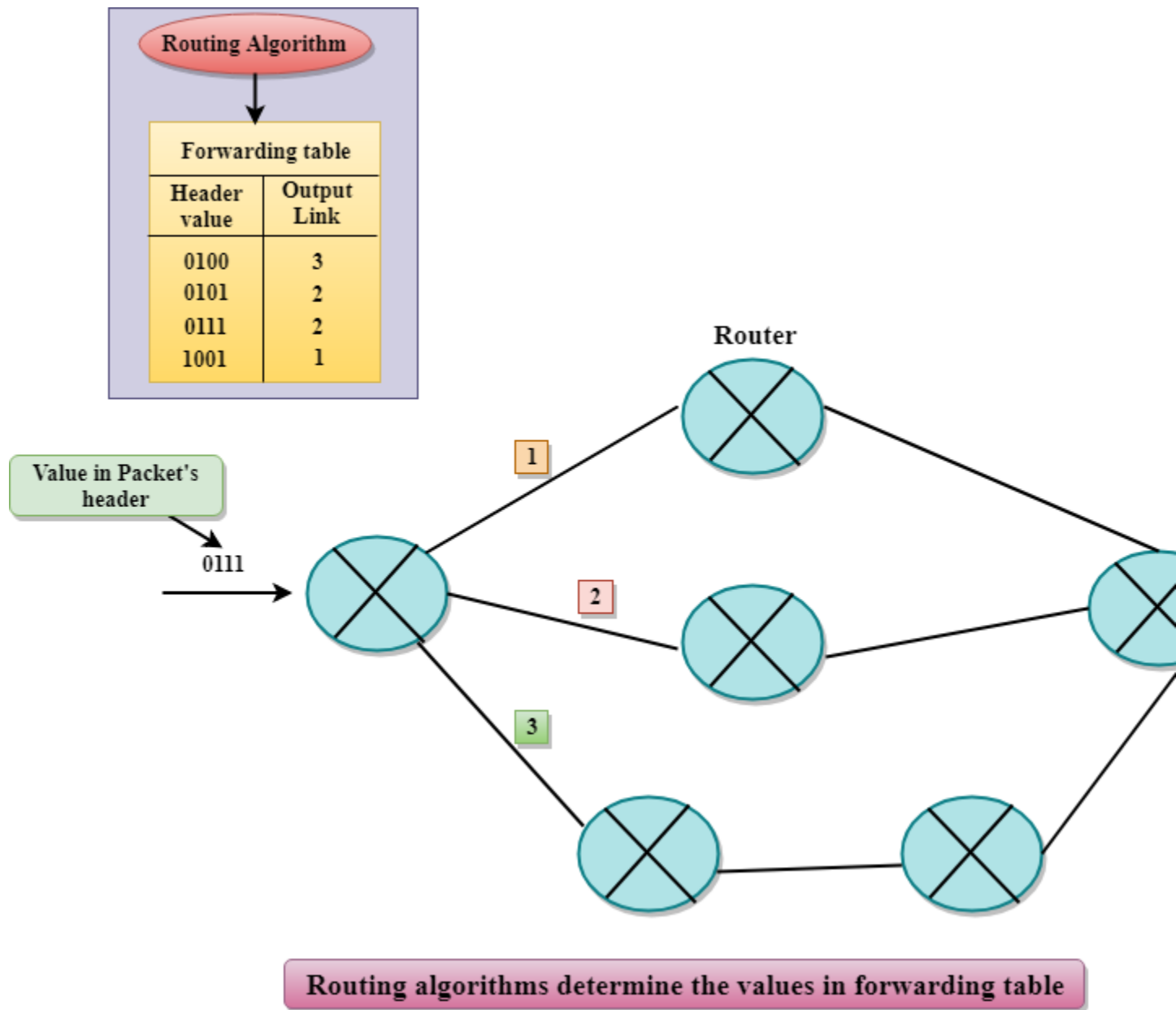
- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2. ✓
- **Logical Addressing:** The data link layer implements the physical addressing and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

Forwarding & Routing

In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field and then using the header field value to index into the forwarding table. The value stored in the forwarding

table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

For example, the router with a header field value of 0111 arrives at a router, and then router indexes this header value into the forwarding table that determines the output link interface is 2. The router forwards the packet to the interface 2. The routing algorithm determines the values that are inserted in the forwarding table. The routing algorithm can be centralized or decentralized.



Services Provided by the Network Layer

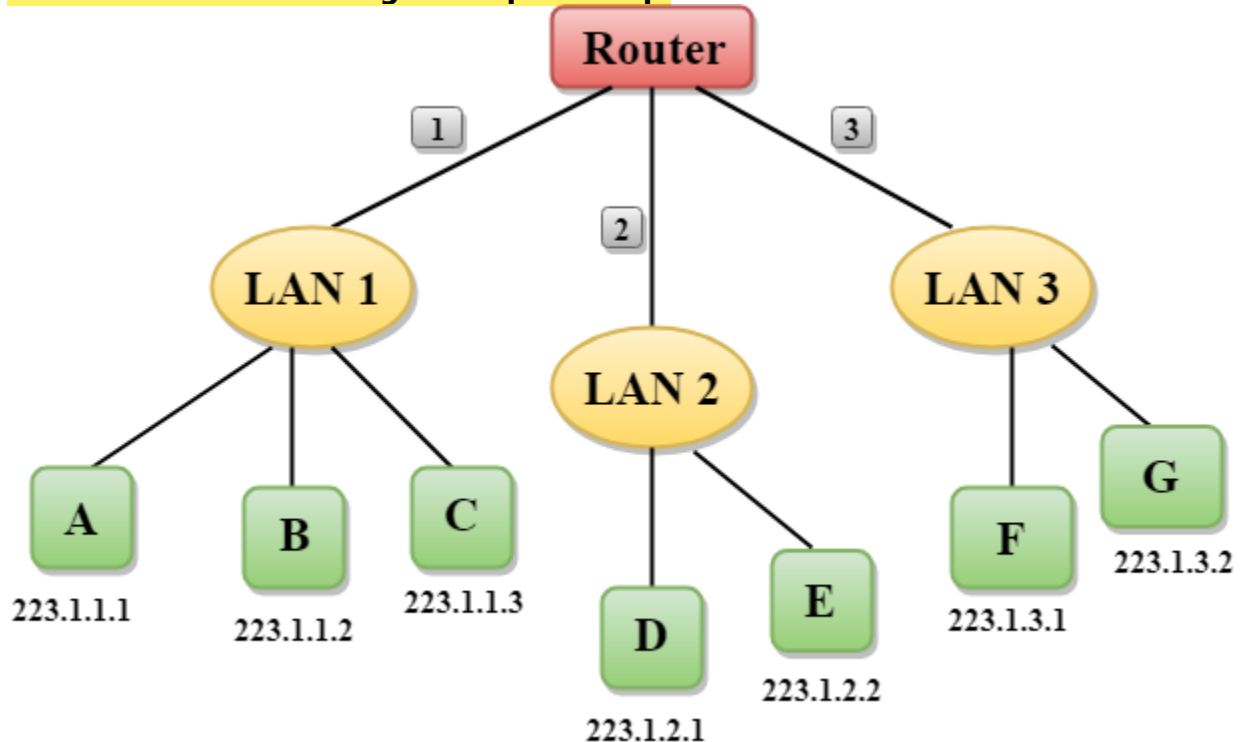
- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Network Addressing

- 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.
- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193

represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

- **Let's understand through a simple example.**



- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
- Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

Classful Addressing

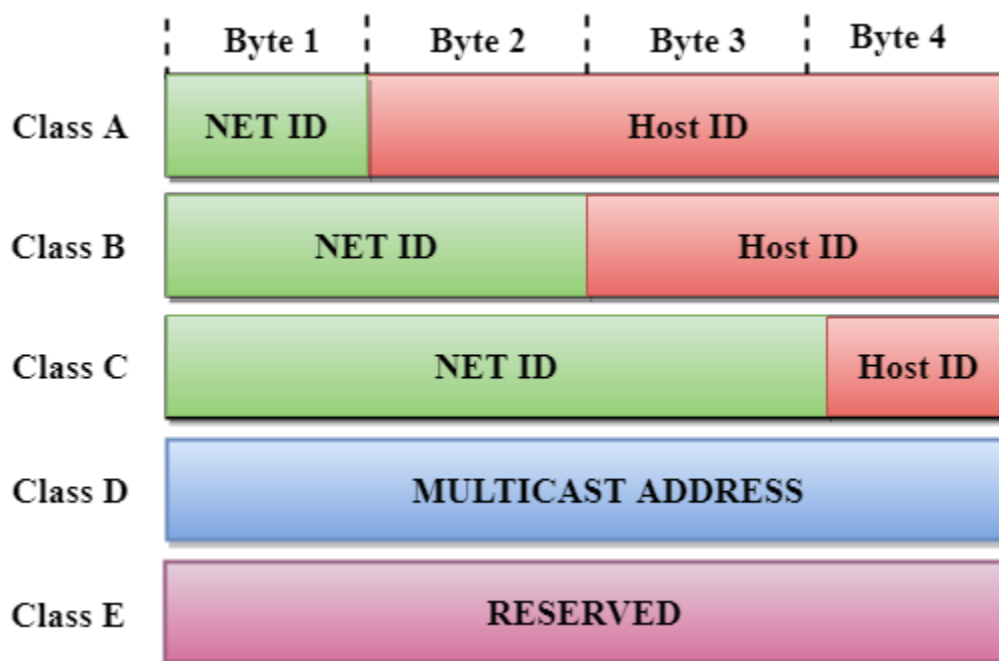
An IP address is 32-bit long. An IP address is divided into sub-classes:

- **Class A**

- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = $2^7 = 128$ network address

The total number of hosts in Class A = $2^{24} - 2 = 16,777,214$ host address



Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining 14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = $2^{14} = 16384$ network address

The total number of hosts in Class B = $2^{16} - 2 = 65534$ host address



Class C

In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = $2^{21} = 2097152$ network address

The total number of hosts = $2^8 - 2 = 254$ host address



Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- The Host ID must be unique within any network.

- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

- The network ID cannot start with 127 as 127 is used by Class A.
- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Classful Network Architecture

Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
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	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255

E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255
---	------	-------------	-------------	-------------	-------------	------------------------------

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.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Routing Metrics and Costs

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.

Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value cannot be changed and for

some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator.

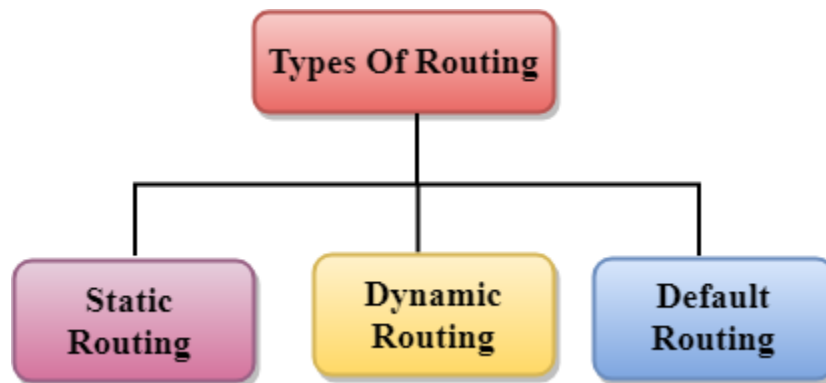
The most common metric values are given below:

- **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.
- **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.
- **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

Types of Routing

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 no 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.

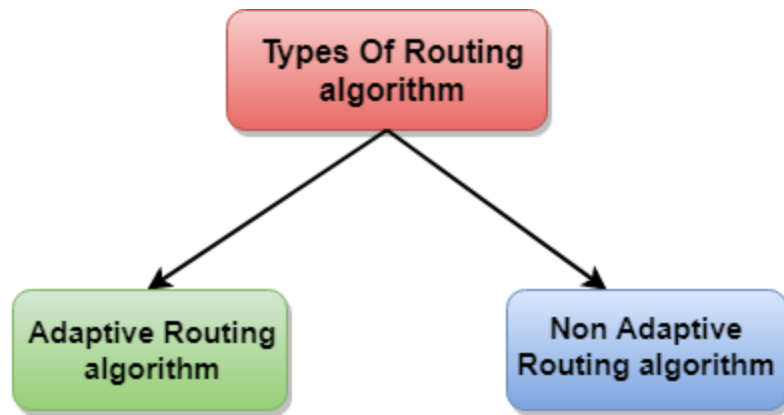
Routing algorithm

- 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.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.

Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

Distance Vector Routing Algorithm

- **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 neighbors, performs calculation and then distributes the result back to its neighbors.
 - **Iterative:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
 - **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**.

Three Keys to understand the working of Distance Vector Routing Algorithm:

- **Knowledge about the whole network:** Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.
- **Routing only to neighbors:** The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.

- **Information sharing at regular intervals:** Within 30 seconds, the router sends the information to the neighboring routers.

Distance Vector Routing Algorithm

Let $d_x(y)$ be the cost of the least-cost path from node x to node y . The least costs are related by Bellman-Ford equation,

$$d_x(y) = \min_v \{ c(x, v) + d_v(y) \}$$

Where the \min_v is the equation taken for all x neighbors. After traveling from x to v , if we consider the least-cost path from v to y , the path cost will be $c(x, v) + d_v(y)$. The least cost from x to y is the minimum of $c(x, v) + d_v(y)$ taken over all neighbors.

With the Distance Vector Routing algorithm, the node x contains the following routing information:

- For each neighbor v , the cost $c(x, v)$ is the path cost from x to directly attached neighbor, v .
- The distance vector x , i.e., $D_x = [D_x(y) : y \text{ in } N]$, containing its cost to all destinations, y , in N .
- The distance vector of each of its neighbors, i.e., $D_v = [D_v(y) : y \text{ in } N]$ for each neighbor v of x .

Distance vector routing is an asynchronous algorithm in which node x sends the copy of its distance vector to all its neighbors. When node x receives the new distance vector from one of its neighboring vector, v , it saves the distance vector of v and uses the Bellman-Ford equation to update its own distance vector. The equation is given below:

$$d_x(y) = \min_v \{ c(x, v) + d_v(y) \} \quad \text{for each node } y \text{ in } N$$

The node x has updated its own distance vector table by using the above equation and sends its updated table to all its neighbors so that they can update their own distance vectors.

Algorithm

At each node x ,

Initialization

```

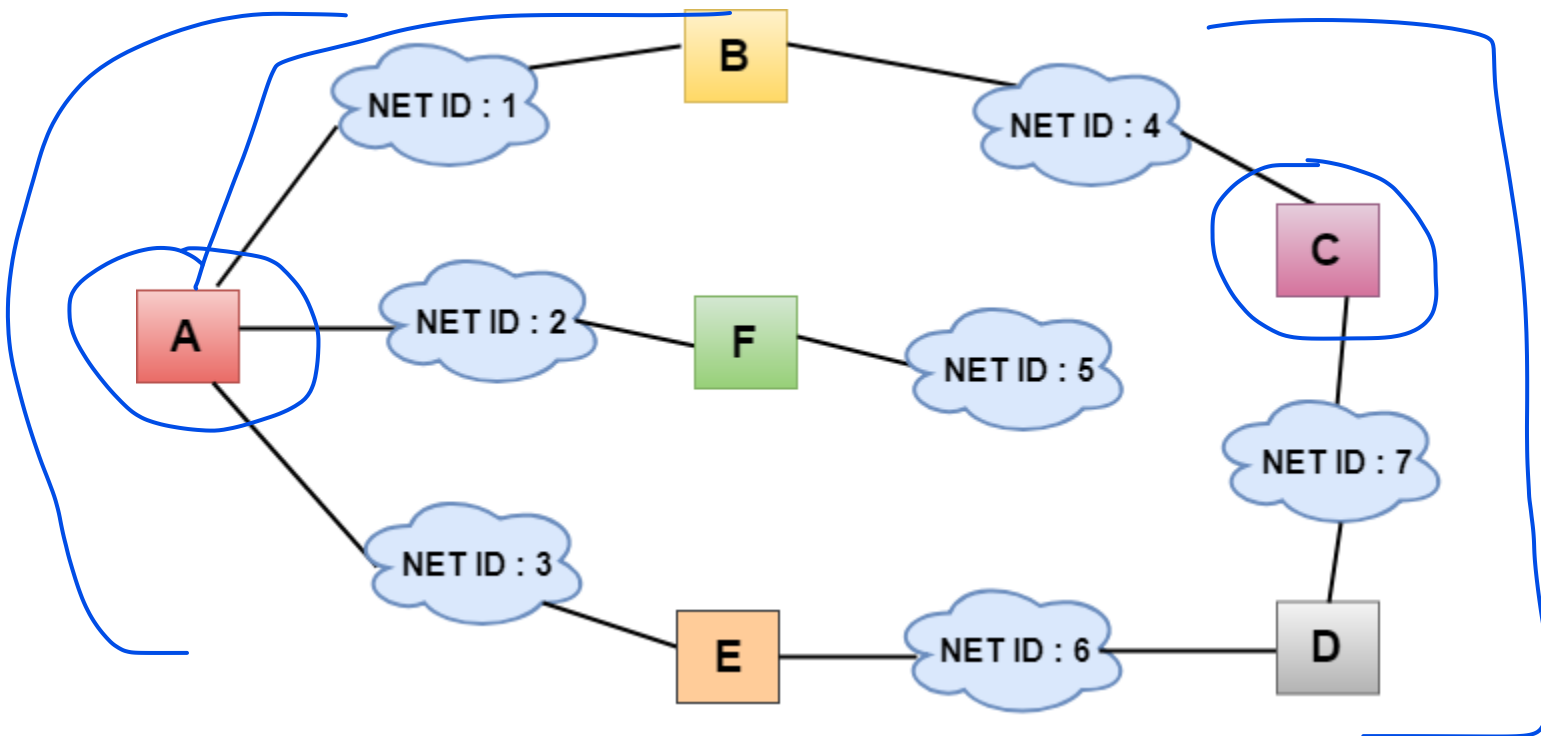
for all destinations y in N:
  Dx(y) = c(x,y)      // If y is not a neighbor then c(x,y) = ∞
for each neighbor w
  Dw(y) = ?          for all destination y in N.
for each neighbor w
  send distance vector Dx = [ Dx(y) : y in N ] to w
loop
  wait(until I receive any distance vector from some neighbor w)
  for each y in N:
    Dx(y) = minv{c(x,v)+Dv(y)}
  If Dx(y) is changed for any destination y
  Send distance vector Dx = [ Dx(y) : y in N ] to all neighbors
forever

```

Note: In Distance vector algorithm, node x update its table when it either see any cost change in one directly linked nodes or receives any vector update from some neighbor.

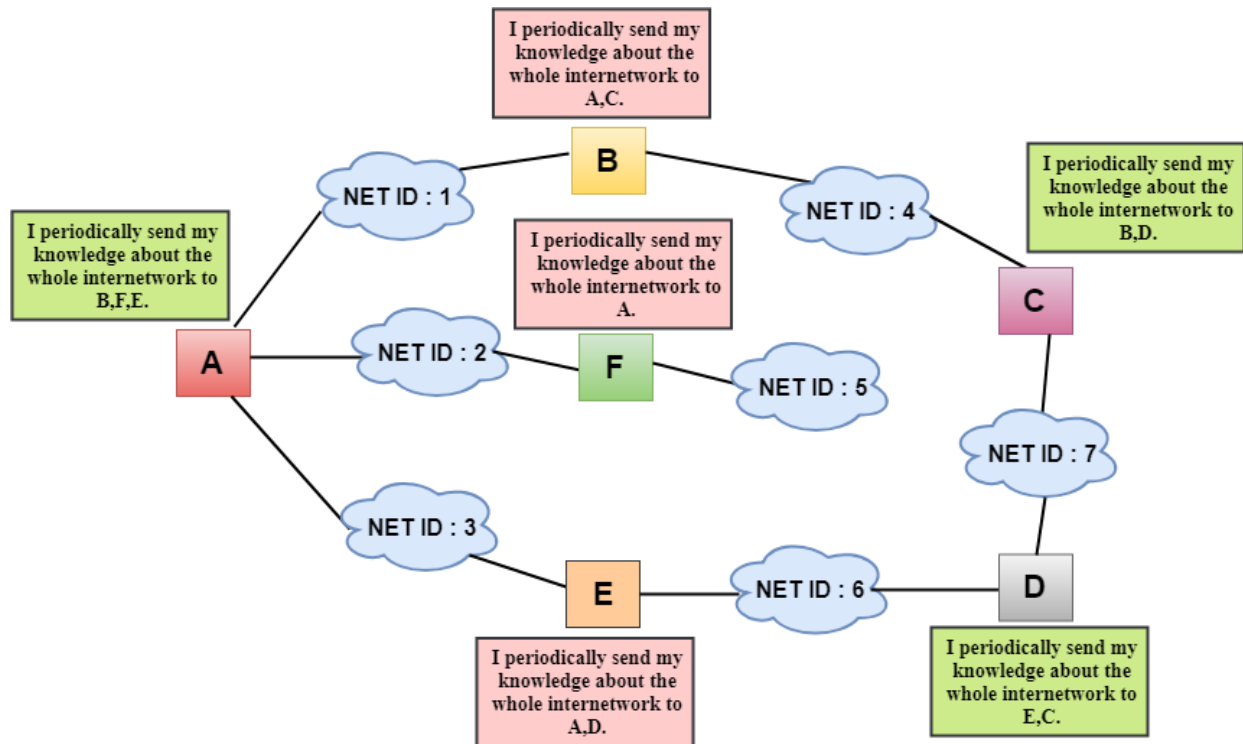
Let's understand through an example:

Sharing Information



- In the above figure, each cloud represents the network, and the number inside the cloud represents the network ID.
- All the LANs are connected by routers, and they are represented in boxes labeled as A, B, C, D, E, F.

- Distance vector routing algorithm simplifies the routing process by assuming the cost of every link is one unit. Therefore, the efficiency of transmission can be measured by the number of links to reach the destination.
- In Distance vector routing, the cost is based on hop count.



In the above figure, we observe that the router sends the knowledge to the immediate neighbors. The neighbors add this knowledge to their own knowledge and sends the updated table to their own neighbors. In this way, routers get its own information plus the new information about the neighbors.

Routing Table

Two process occurs:

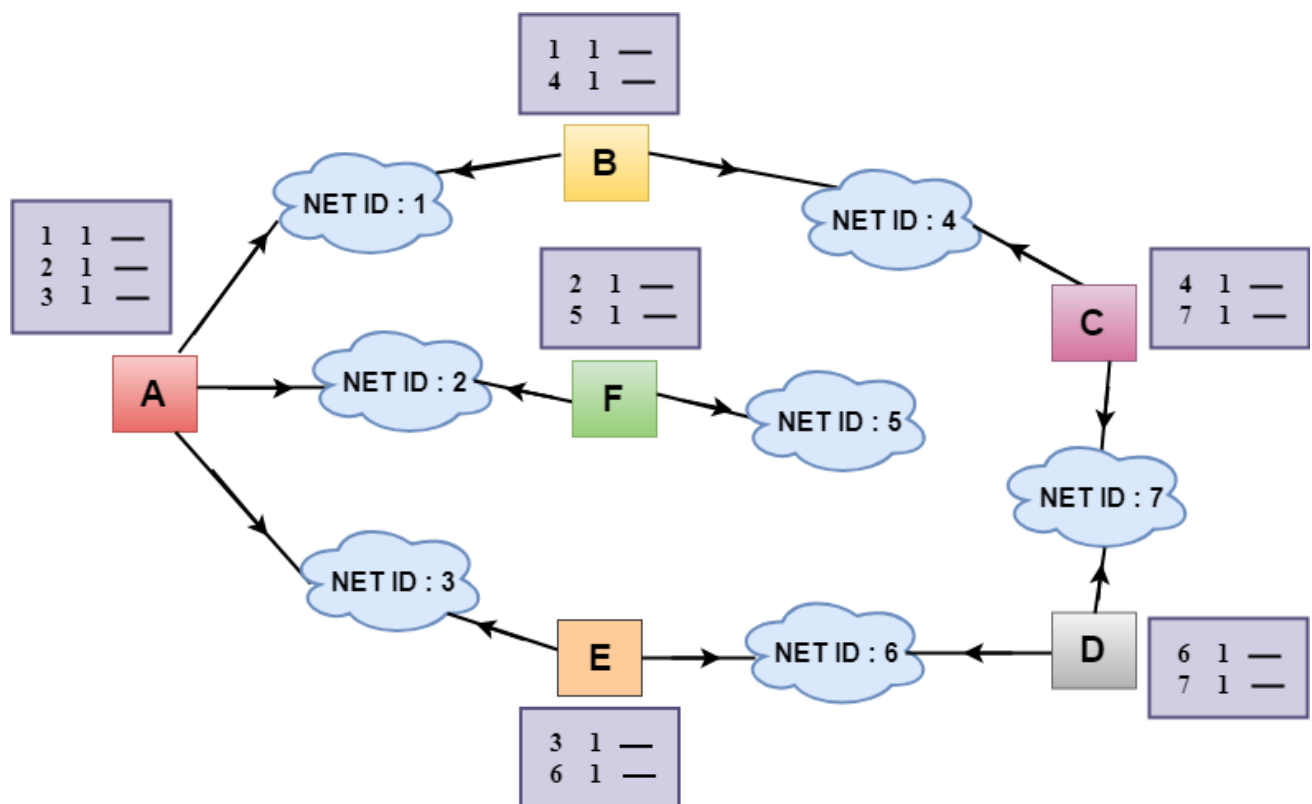
- Creating the Table
- Updating the Table

Creating the Table

Initially, the routing table is created for each router that contains atleast three types of information such as Network ID, the cost and the next hop.

NET ID	Cost	Next Hop

- **NET ID:** The Network ID defines the final destination of the packet.
- **Cost:** The cost is the number of hops that packet must take to get there.
- **Next hop:** It is the router to which the packet must be delivered.



- In the above figure, the original routing tables are shown of all the routers. In a routing table, the first column represents the network ID, the second column represents the cost of the link, and the third column is empty.
- These routing tables are sent to all the neighbors.

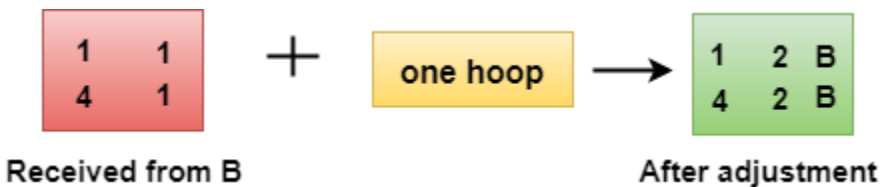
For Example:

1. A sends its routing table to B, F & E.

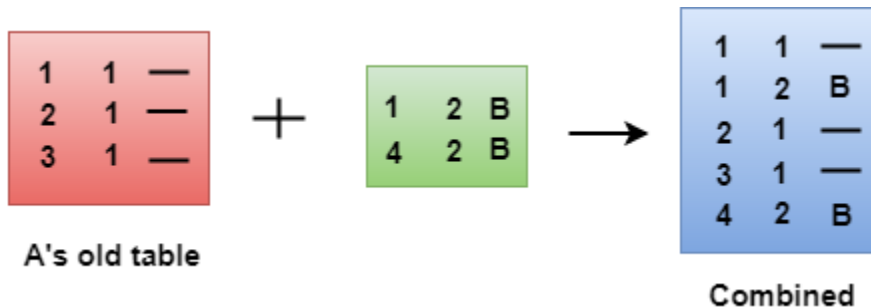
2. B sends its routing table to A & C.
3. C sends its routing table to B & D.
4. D sends its routing table to E & C.
5. E sends its routing table to A & D.
6. F sends its routing table to A.

Updating the Table

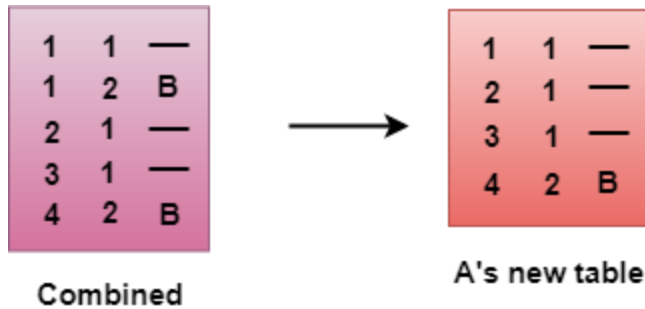
- When A receives a routing table from B, then it uses its information to update the table.
- The routing table of B shows how the packets can move to the networks 1 and 4.
- The B is a neighbor to the A router, the packets from A to B can reach in one hop. So, 1 is added to all the costs given in the B's table and the sum will be the cost to reach a particular network.



- After adjustment, A then combines this table with its own table to create a combined table.



- The combined table may contain some duplicate data. In the above figure, the combined table of router A contains the duplicate data, so it keeps only those data which has the lowest cost. For example, A can send the data to network 1 in two ways. The first, which uses no next router, so it costs one hop. The second requires two hops (A to B, then B to Network 1). The first option has the lowest cost, therefore it is kept and the second one is dropped.



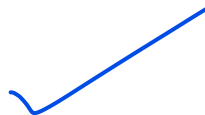
- The process of creating the routing table continues for all routers. Every router receives the information from the neighbors, and update the routing table.

Final routing tables of all the routers are given below:

Router A	Router B	Router C
6 2 E	6 3 E	6 2 D
1 1 —	1 1 —	1 2 B
3 1 —	3 2 A	3 3 D
4 2 B	4 1 —	4 1 —
7 3 E	7 2 C	7 1 —
2 1 —	2 2 A	2 3 B
5 2 F	5 3 A	5 4 B

Router D	Router E	Router F
6 1 —	6 1 —	6 3 A
1 3 E	1 2 A	1 2 A
3 2 E	3 1 —	3 2 A
4 2 C	4 3 A	4 3 A
7 1 —	7 2 D	7 4 A
2 3 E	2 2 A	2 1 —
5 4 E	5 3 A	5 1 —

Link State Routing



Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- ✓ ○ **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- ✓ ○ **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Link State Routing has two phases:

Reliable Flooding

- **Initial state:** Each node knows the cost of its neighbors.
- **Final state:** Each node knows the entire graph.

Route Calculation

Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

Let's describe some notations:

- $c(i, j)$: Link cost from node i to node j . If i and j nodes are not directly linked, then $c(i, j) = \infty$.
- $D(v)$: It defines the cost of the path from source code to destination v that has the least cost currently.

- **P(v):** It defines the previous node (neighbor of v) along with current least cost path from source to v.
- **N:** It is the total number of nodes available in the network.

Algorithm

Initialization

$N = \{A\}$ // **A is a root node .**

for all nodes v

if v adjacent to A

then $D(v) = c(A, v)$

else $D(v) = \text{infinity}$

loop

find w not in N such that $D(w)$ is a minimum.

Add w to N

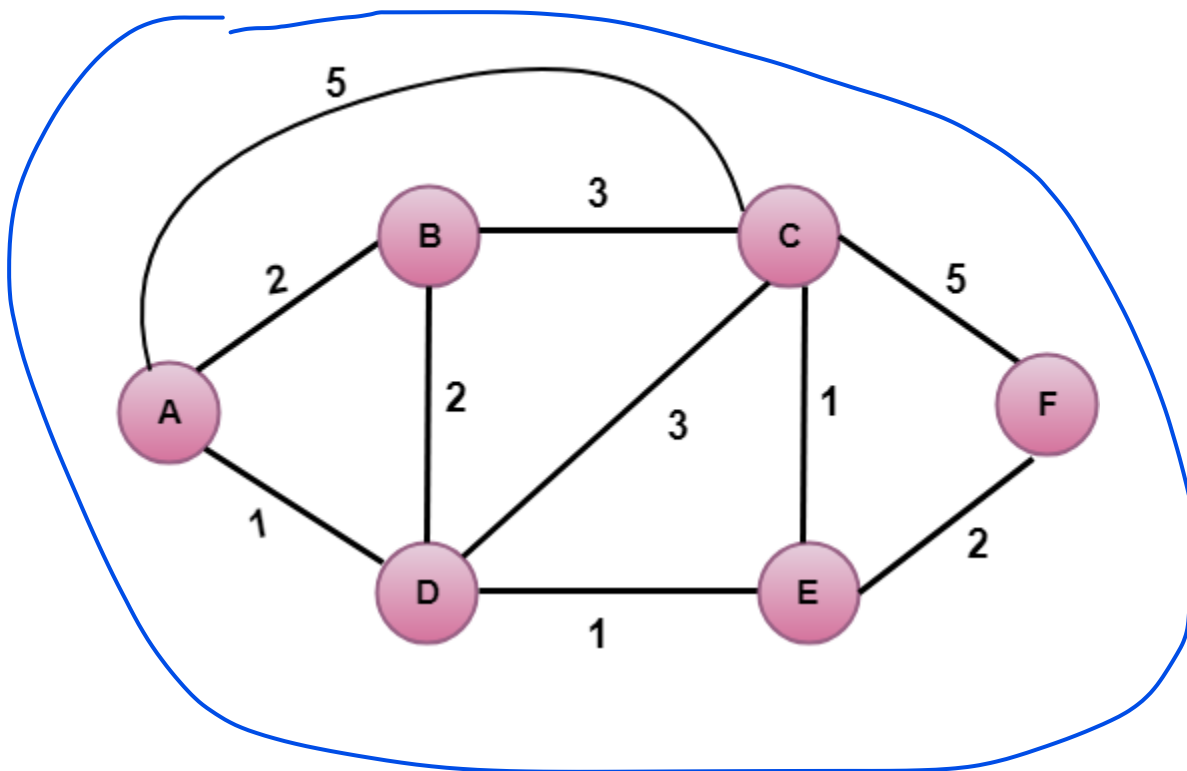
Update $D(v)$ for all v adjacent to w and not in N:

$D(v) = \min(D(v), D(w) + c(w, v))$

Until all nodes in N

In the above algorithm, an initialization step is followed by the loop. The number of times the loop is executed is equal to the total number of nodes available in the network.

Let's understand through an example:



In the above figure, source vertex is A.

Step 1:

The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞

Step 2:

In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

a) Calculating shortest path from A to B

1. $v = B, w = D$
2. $D(B) = \min(D(B) , D(D) + c(D,B))$
3. $= \min(2, 1+2)$
4. $= \min(2, 3)$
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating shortest path from A to C

1. $v = C, w = D$
 2. $D(C) = \min(D(C) , D(D) + c(D,C))$
 3. $= \min(5, 1+3)$
 4. $= \min(5, 4)$
 5. The minimum value is 4. Therefore, the currently shortest path from A to C is 4.
-

c) Calculating shortest path from A to E

1. $v = E, w = D$
2. $D(B) = \min(D(E) , D(D) + c(D,E))$
3. $= \min(\infty, 1+1)$
4. $= \min(\infty, 2)$
5. The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

Note: The vertex D has no direct link to vertex E. Therefore, the value of $D(F)$ is infinity.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞

Step 3:

In the above table, we observe that both E and B have the least cost path in step 2. Let's consider the E vertex. Now, we determine the least cost path of remaining vertices through E.

a) Calculating the shortest path from A to B.

1. $v = B, w = E$
2. $D(B) = \min(D(B) , D(E) + c(E,B))$
3. $= \min(2, 2 + \infty)$
4. $= \min(2, \infty)$
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating the shortest path from A to C.

1. $v = C, w = E$
2. $D(B) = \min(D(C) , D(E) + c(E,C))$
3. $= \min(4, 2+1)$
4. $= \min(4, 3)$
5. The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

c) Calculating the shortest path from A to F.

1. $v = F, w = E$
2. $D(B) = \min(D(F) , D(E) + c(E,F))$
3. $= \min(\infty , 2+2)$
4. $= \min(\infty , 4)$
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E

Step 4:

In the above table, we observe that B vertex has the least cost path in step 3. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through B.

a) Calculating the shortest path from A to C.

1. $v = C, w = B$
2. $D(B) = \min(D(C) , D(B) + c(B,C))$
3. $= \min(3 , 2+3)$
4. $= \min(3,5)$
5. The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

b) Calculating the shortest path from A to F.

1. $v = F, w = B$
2. $D(B) = \min(D(F) , D(B) + c(B,F))$
3. $= \min(4, \infty)$
4. $= \min(4, \infty)$
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E

Step 5:

In the above table, we observe that C vertex has the least cost path in step 4. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through C.

a) Calculating the shortest path from A to F.

1. $v = F, w = C$
2. $D(B) = \min(D(F) , D(C) + c(C,F))$
3. $= \min(4, 3+5)$
4. $= \min(4, 8)$
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E

5	ADEBC					4,E
---	-------	--	--	--	--	-----

Final table:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E
6	ADEBCF					

Disadvantage:

Heavy traffic is created in Line state routing due to Flooding. Flooding can cause an infinite looping, this problem can be solved by using Time-to-live field

Network Layer Protocols

TCP/IP supports the following protocols:

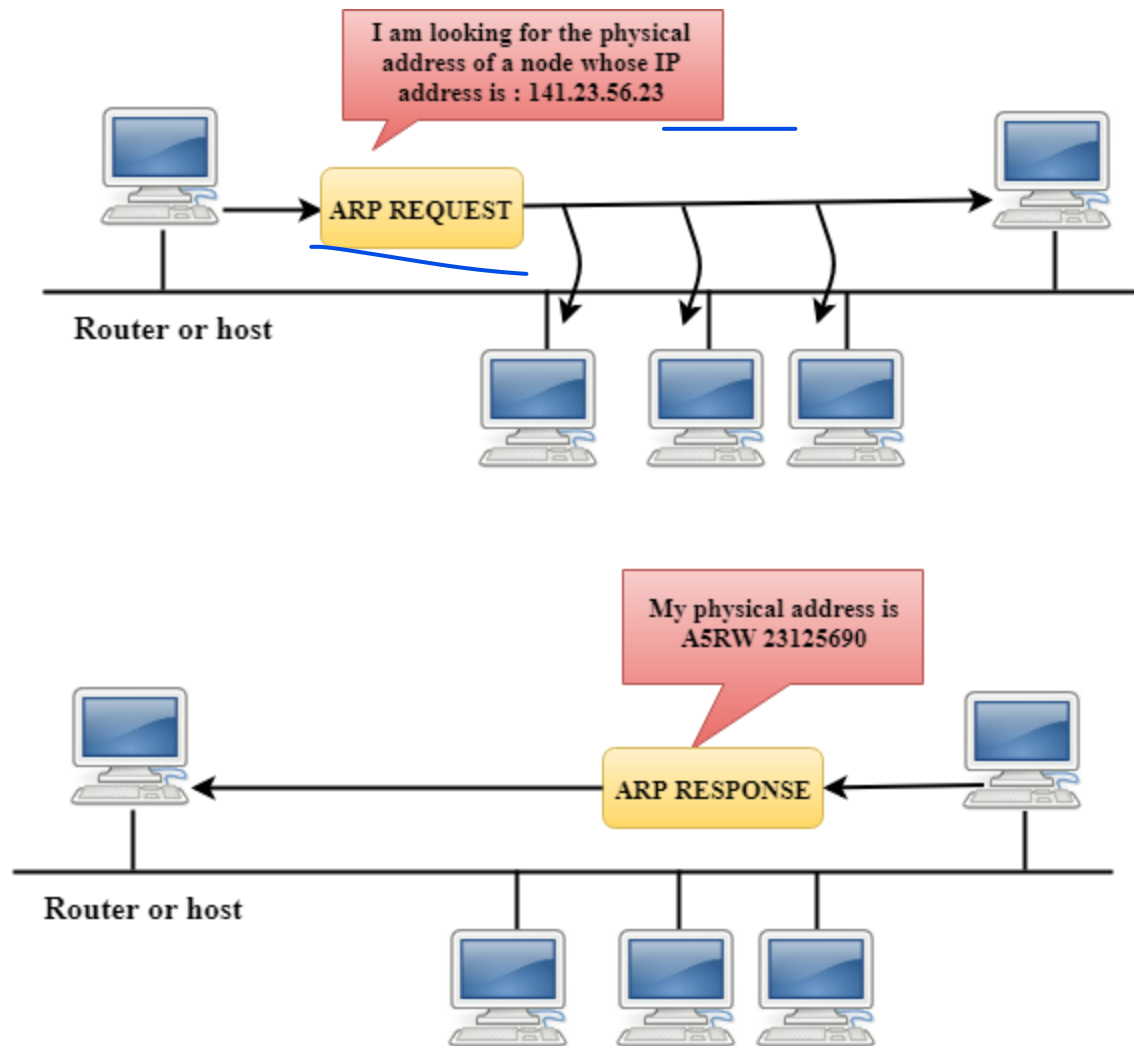
ARP

- 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.

*Note: MAC address: The MAC address is used to identify the actual device.
IP address: It is an address used to locate a device on the network.*

How ARP works

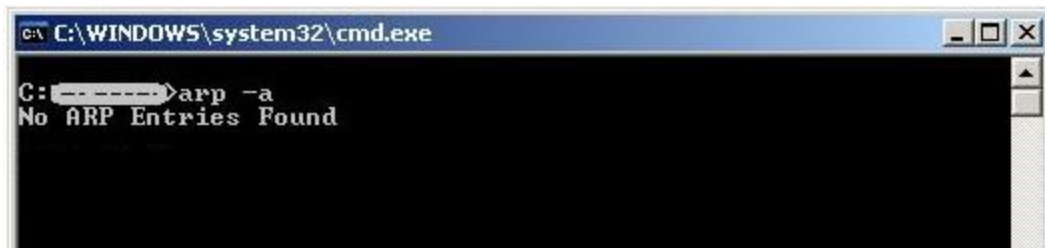
If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.



Steps taken by ARP protocol

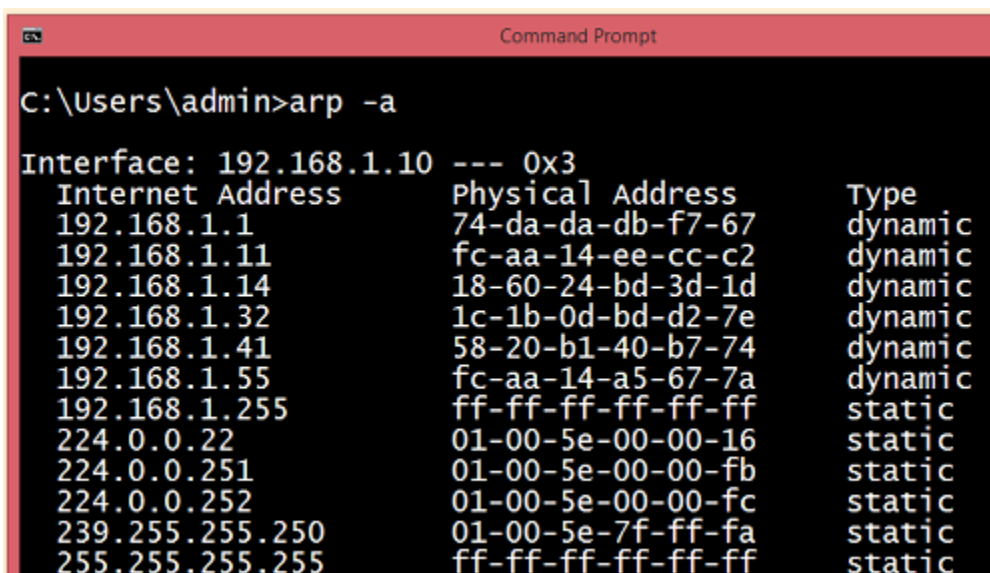
If a device wants to communicate with another device, the following steps are taken by the device:

- The device will first look at its internet list, called the ARP cache to check whether an IP address contains a matching MAC address or not. It will check the ARP cache in command prompt by using a command **arp-a**.



```
C:\WINDOWS\system32\cmd.exe
C:\>arp -a
No ARP Entries Found
```

- If ARP cache is empty, then device broadcast the message to the entire network asking each device for a matching MAC address.
- The device that has the matching IP address will then respond back to the sender with its MAC address
- Once the MAC address is received by the device, then the communication can take place between two devices.
- If the device receives the MAC address, then the MAC address gets stored in the ARP cache. We can check the ARP cache in command prompt by using a command arp -a.



```
Command Prompt
C:\Users\admin>arp -a
Interface: 192.168.1.10 --- 0x3
Internet Address      Physical Address      Type
192.168.1.1           74-da-da-db-f7-67    dynamic
192.168.1.11          fc-aa-14-ee-cc-c2    dynamic
192.168.1.14          18-60-24-bd-3d-1d    dynamic
192.168.1.32          1c-1b-0d-bd-d2-7e    dynamic
192.168.1.41          58-20-b1-40-b7-74    dynamic
192.168.1.55          fc-aa-14-a5-67-7a    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Note: ARP cache is used to make a network more efficient.

In the above screenshot, we observe the association of IP address to the MAC address.

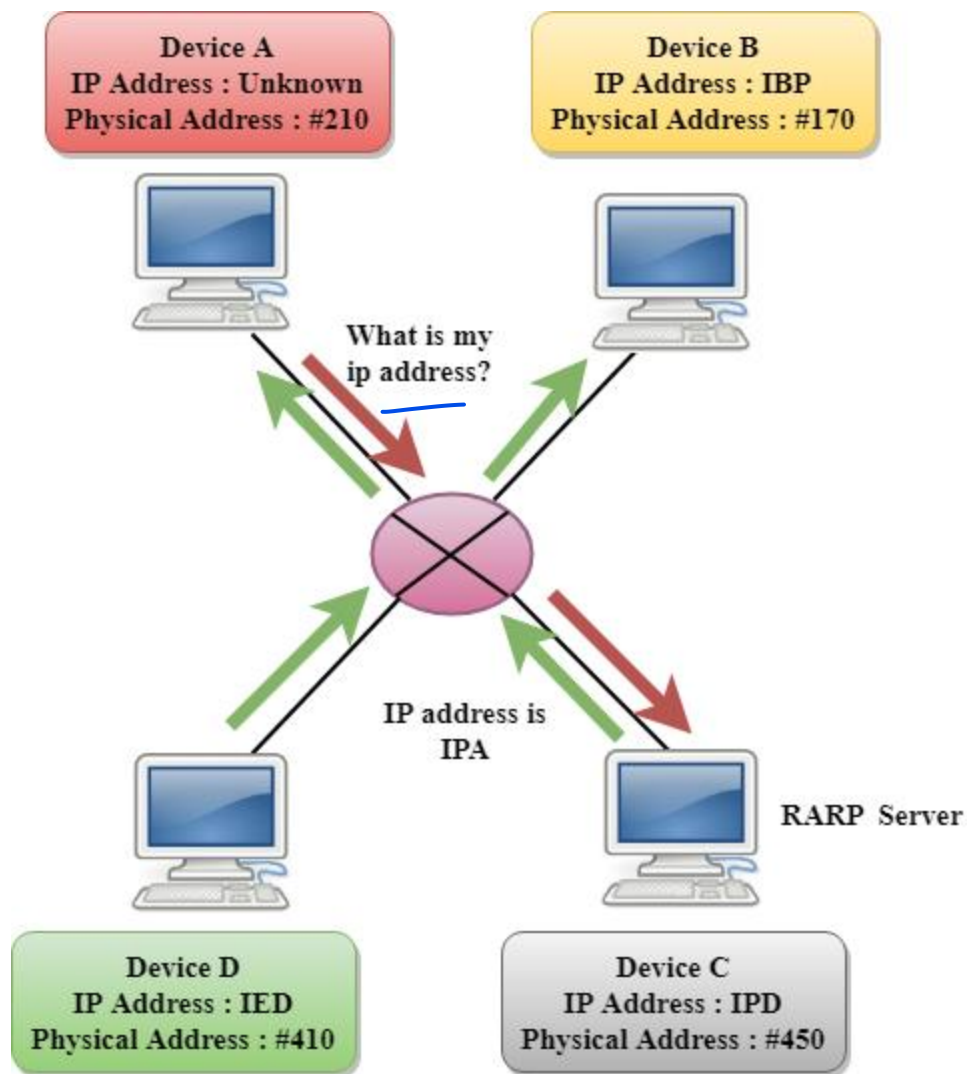
There are two types of ARP entries:

- **Dynamic entry:** It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.

- **Static entry:** It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility.
-

RARP

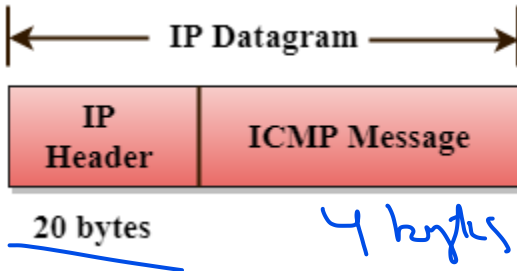
- RARP stands for **Reverse Address Resolution Protocol**.
- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- 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.



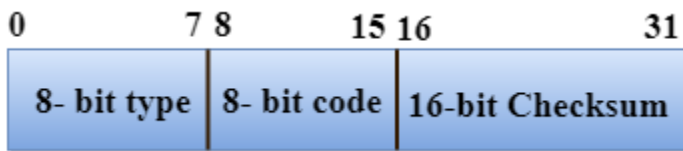
ICMP

- 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.



The Format of an ICMP message



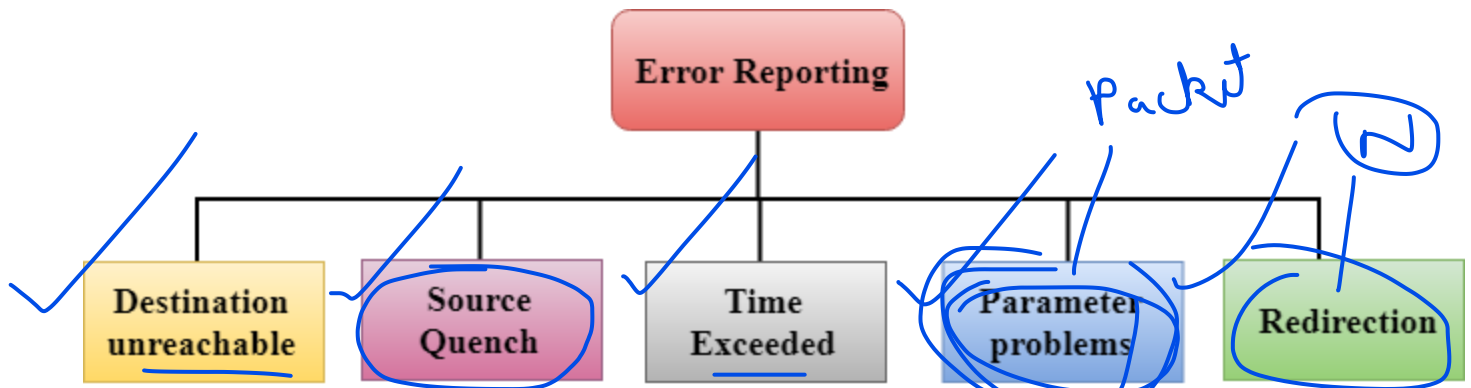
- The first field specifies the type of the message.
- The second field specifies the reason for a particular message type.
- The checksum field covers the entire ICMP message.

Error Reporting

ICMP protocol reports the error messages to the sender.

Five types of errors are handled by the ICMP protocol:

- Destination unreachable
- Source Quench
- Time Exceeded
- Parameter problems
- Redirection



- **Destination unreachable:** The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.
- **Source Quench:** The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.
- **Time Exceeded:** Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.

There are two ways when Time Exceeded message can be generated:

Sometimes packet discarded due to some bad routing implementation, and this causes the looping issue and network congestion. Due to the looping issue, the value of TTL keeps on decrementing, and when it reaches zero, the router discards the datagram. However, when the datagram is discarded by the router, the time exceeded message will be sent by the router to the source host.

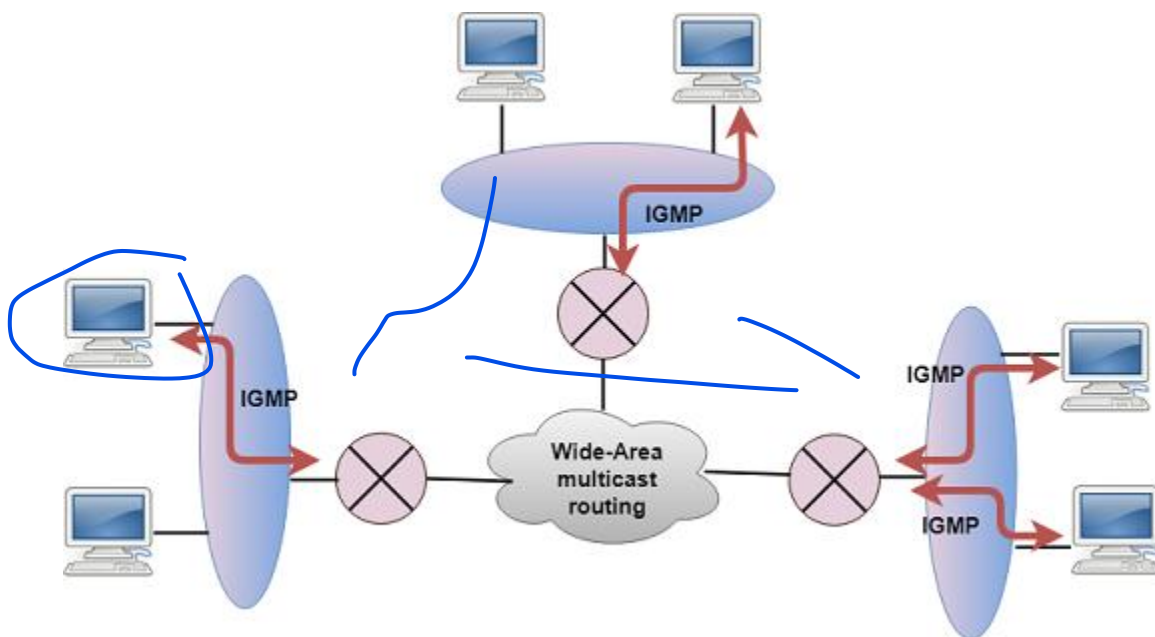
When destination host does not receive all the fragments in a certain time limit, then the received fragments are also discarded, and the destination host sends time Exceeded message to the source host.

- **Parameter problems:** When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.
-

- **Redirection:** Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table.

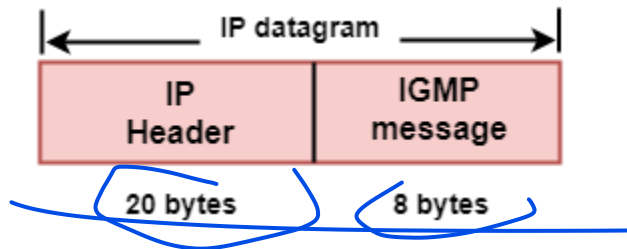
IGMP

- 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.

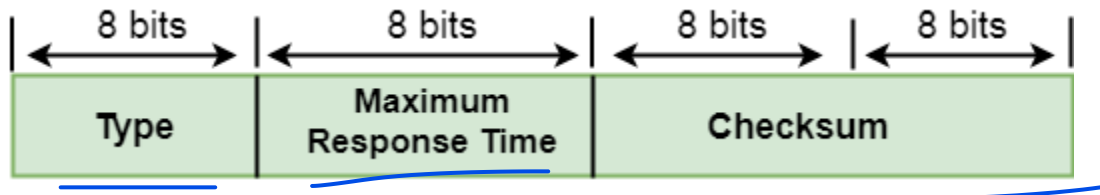


- IGMP is a part of the IP layer, and IGMP has a fixed-size message.

- The IGMP message is encapsulated within an IP datagram.



The Format of IGMP message



Where,

Type: It determines the type of IGMP message. There are three types of IGMP message: Membership Query, Membership Report and Leave Report.

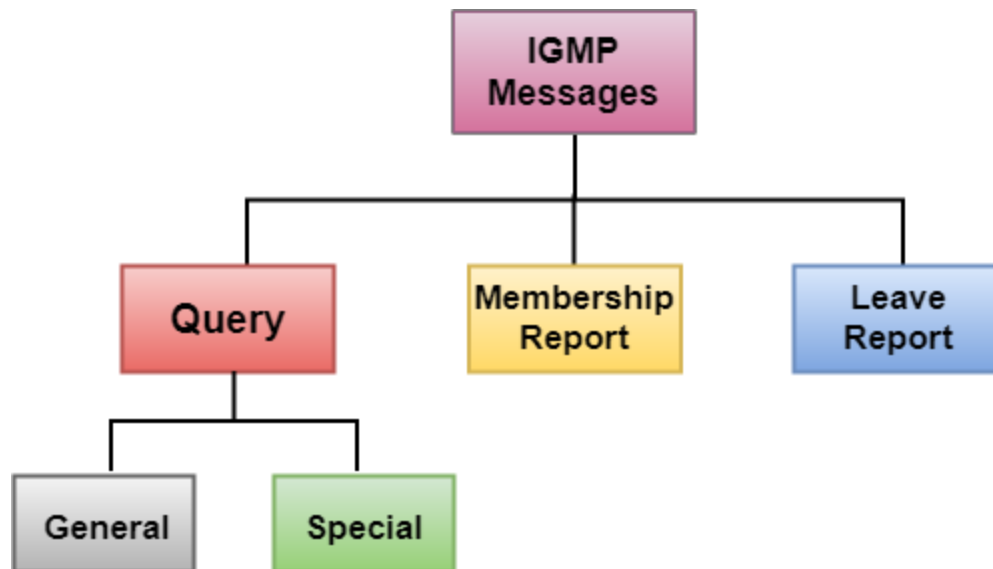
Maximum Response Time: This field is used only by the Membership Query message. It determines the maximum time the host can send the Membership Report message in response to the Membership Query message.

Checksum: It determines the entire payload of the IP datagram in which IGMP message is encapsulated.

Group Address: The behavior of this field depends on the type of the message sent.

- **For Membership Query**, the group address is set to zero for General Query and set to multicast group address for a specific query.
- **For Membership Report**, the group address is set to the multicast group address.
- **For Leave Group**, it is set to the multicast group address.

IGMP Messages



- **Membership Query message**

- This message is sent by a router to all hosts on a local area network to determine the set of all the multicast groups that have been joined by the host.
- It also determines whether a specific multicast group has been joined by the hosts on a attached interface.
- The group address in the query is zero since the router expects one response from a host for every group that contains one or more members on that host.

- **Membership Report message**

- The host responds to the membership query message with a membership report message.
- Membership report messages can also be generated by the host when a host wants to join the multicast group without waiting for a membership query message from the router.
- Membership report messages are received by a router as well as all the hosts on an attached interface.
- Each membership report message includes the multicast address of a single group that the host wants to join.
- IGMP protocol does not care which host has joined the group or how many hosts are present in a single group. It only cares whether one or more attached hosts belong to a single multicast group.

- The membership Query message sent by a router also includes a "**Maximum Response time**". After receiving a membership query message and before sending the membership report message, the host waits for the random amount of time from 0 to the maximum response time. If a host observes that some other attached host has sent the "**Maximum Report message**", then it discards its "**Maximum Report message**" as it knows that the attached router already knows that one or more hosts have joined a single multicast group. This process is known as feedback suppression. It provides the performance optimization, thus avoiding the unnecessary transmission of a "**Membership Report message**".
- **Leave Report**
When the host does not send the "Membership Report message", it means that the host has left the group. The host knows that there are no members in the group, so even when it receives the next query, it would not report the group.

Congestion Control Algorithm

What is **congestion**?

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Congestion control algorithms

- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.
- There are two congestion control algorithm which are as follows:

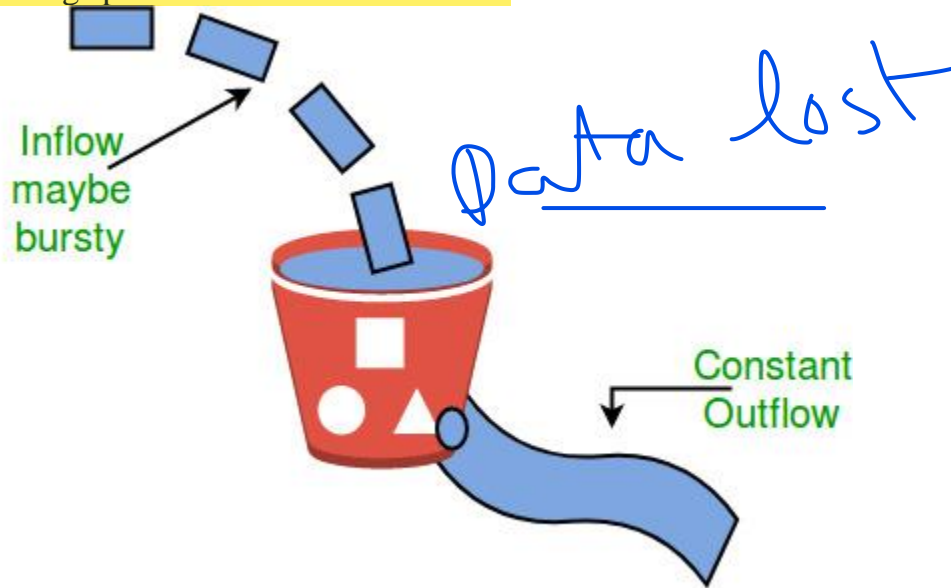
Leaky Bucket Algorithm

- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
-

- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the bursty traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

Token bucket Algorithm

- The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
- In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information.

Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.

- It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
- The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
- When tokens are shown, a flow to transmit traffic appears in the display of tokens.
- No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

Need of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

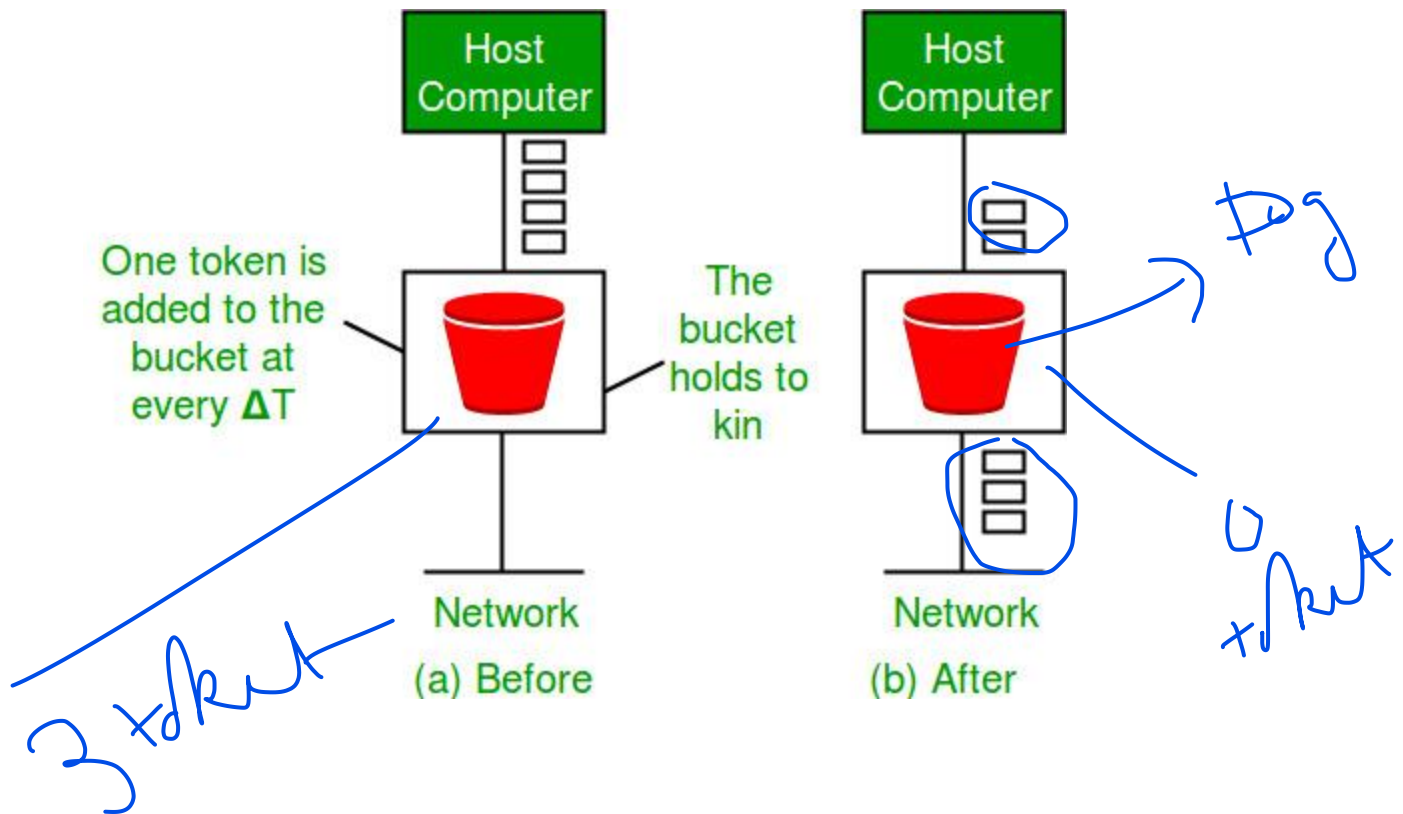
1. In regular intervals tokens are thrown into the bucket. f
2. The bucket has a maximum capacity. f
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

Let's understand with an example,

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Ways in which token bucket is superior to leaky bucket: The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busy packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

Formula: $M * s = C + \rho * s$ where S – is time taken M – Maximum output rate ρ – Token arrival rate C – Capacity of the token bucket in byte
Let's understand with an example,



Classful vs Classless addressing

IPv4 Addresses, Classful Addressing, Classless Addressing, and the difference between Classful and Classless addressing are discussed in this article.

Let's first discuss about IPv4 addresses

IPv4 ADDRESSES

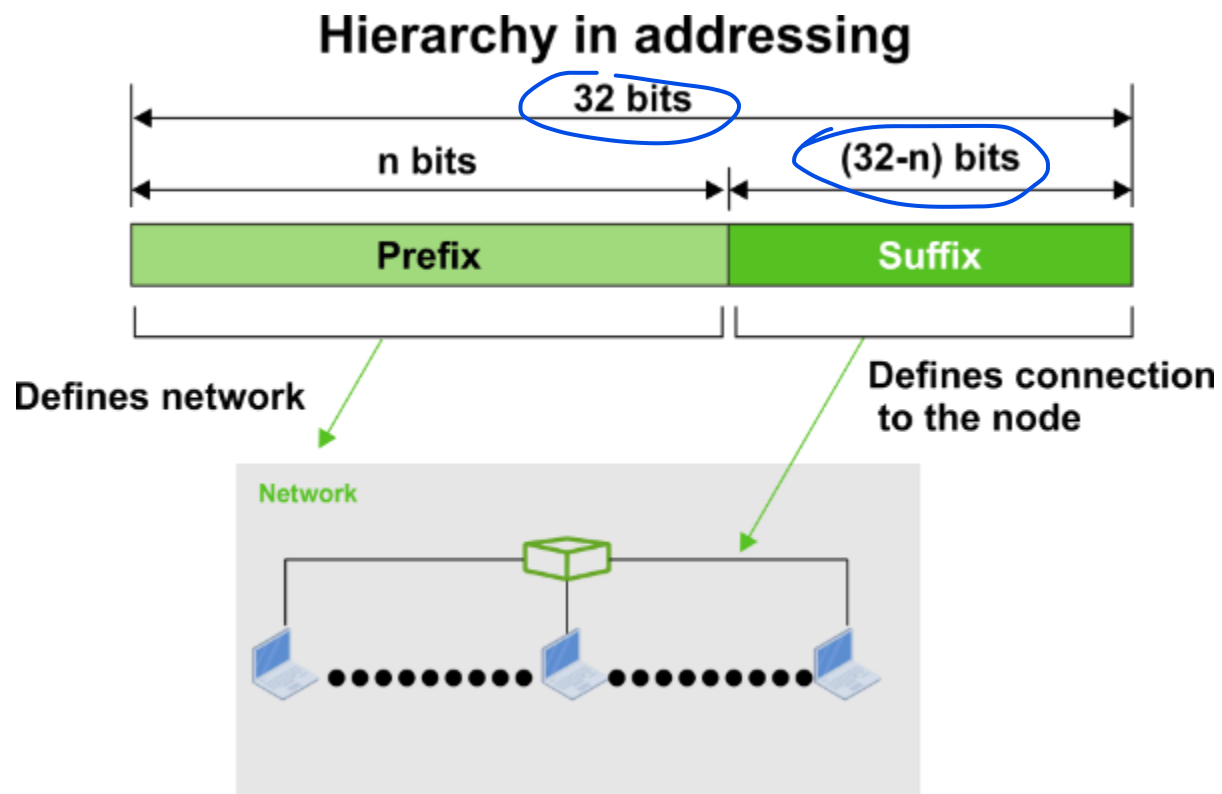
The IP address, often known as the Internet address, is the unique identifier used in the IP layer of the TCP/IP protocol suite to identify each device's connection to the Internet. A host's or router's connection to the Internet is defined by its 32-bit IPv4 address, which is unique and used worldwide. The IP address, not the host or router, is what identifies the connection because it could change if the device is relocated to a different network.

Since each address specifies a single and exclusive connection to the Internet, IPv4 addresses are distinctive. A device has two IPv4 addresses if it has two networks connecting to the Internet through it. Because every host that wishes to connect to the Internet must use the IPv4 addressing scheme, IPv4 addresses are considered universal.

Hierarchy in Addressing

The addressing system is hierarchical in every type of communication network that requires delivery, including phone and postal networks.

Although it is separated into two parts, a 32-bit IPv4 address is also hierarchical. The network is defined by the first component of the address, known as the **prefix**, and the node is defined by the second component, known as the **suffix** (connection of a device to the Internet). A 32-bit IPv4 address's prefix and suffix are shown in the given figure. The lengths of the prefix and suffix are n bits and $(32 - n)$ bits, respectively.



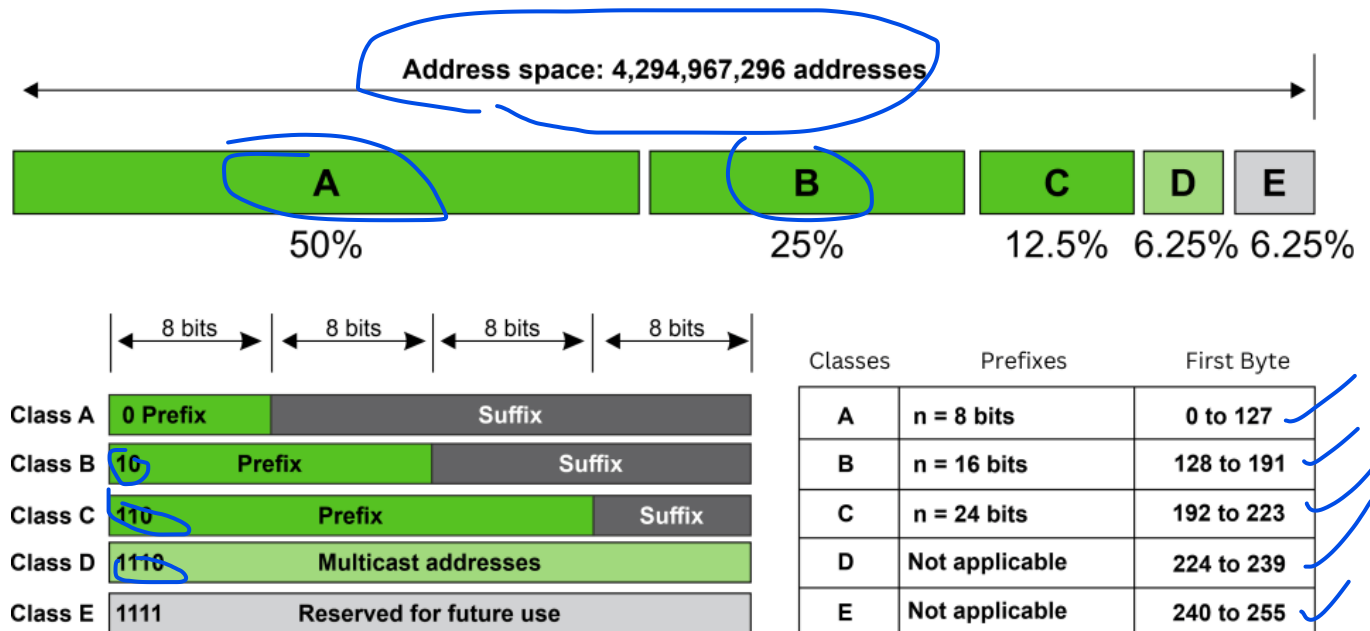
Prefixes can have variable or fixed lengths. The IPv4 network identification was initially intended to be a fixed-length prefix. **Classful addressing** is the term used to describe this outmoded system. **The brand-new addressing method, known as classless addressing, makes use of a variable-length network prefix.** Prior to focusing on classless addressing, we briefly explore classful addressing.

1. CLASSFUL ADDRESSING

An IPv4 address originally had a fixed-length prefix, but three fixed-length prefixes ($n = 8$, $n = 16$, and $n = 24$) were created in order to support both small and big networks. As

shown in the figure below, the entire address space was partitioned into five classes (classes A, B, C, D, and E). Classful addressing is the term used to describe this system. Despite being a thing of the past, classful addressing aids in the comprehension of classless addressing, which is covered in the later section.

Occupation of the address space in classful addressing



CLASS A - Despite the fact that the network length is 8 bits, we can only use seven bits for the network identifier since the first bit, which is 0 and determines the class, is part of the length. This indicates that only $2^7 = 128$ networks can have a class A address globally.

- Net ID = 8bits long and Host ID = 24 bits long
- Method to identify class A addresses:
 - The first bit is reserved to 0 in binary
 - Range of the first octet is [0, 127] in dotted decimal
- Total number of connections in Class A = 2^{31} (2, 14, 74, 83, 648)
- There are $2^7 - 2 = 126$ networks in the Class A network.
 - There are 2 fewer networks available overall since IP Address 0.0.0.0 is set aside for broadcasting needs. For usage as a loopback address while testing software, the IP address 127.0.0.1 is set aside.
 - Hence, the range of the first octet becomes [1, 126]
- Total number of Host IDs in Class A = $2^{24} - 2$ [1, 67, 77, 214]

- There are 2 fewer hosts that can be established across all classes due to the two reserved IP addresses, where all of the host ID bits are either zero or one.
- The Network ID for the network is represented when all of the Host ID bits are set to 0.
- The Broadcast Address is represented when all of the Host ID bits are set to 1.
- Organizations needing very large networks, like Indian Railways, employ class A.

CLASS B - Despite the fact that the first two bits of class B's network, which are 10 in binary or we can write it as $(10)_2$, determine the class, we can only use 14 bits as the network identification, as class B's network length is 16 bits. As a result, only $2^{14} = 16,384$ networks in the entire world are capable of using a class B address.

- Length of Net Id = 16 bits and length of Host ID 16 bits.
- Method to identify Class B networks:
 - First two bits are reserved to 10 in binary notation
 - The Range of the first octet is [128, 191] in dotted decimal notation
- Total number of connections in the class B network is $2^{30} = 1, 07, 37, 41, 824$
- Total number of networks available in class B is $2^{14} = 16, 384$
- Total number of hosts that can be configured in Class B = $2^{16} - 2 = 165, 534$
- Organizations needing medium-sized networks typically utilize class B.

CLASS C - All addresses that begin with the number $(110)_2$ fall under class C. Class C networks are 24 bits long, but since the class is defined by three bits, the network identifier can only be 21 bits long. As a result, $2^{21} = 2, 097, 152$ networks worldwide are capable of using a class C address.

- The length of the Net Id and the Host Id = 24 bits and 16 bits respectively.
- Method to identify Class C networks:
 - First three bits are reserved for 110 in binary notation or $(110)_2$.
 - The range of the first octet is [192, 223] in dotted decimal notation.
- Total number of connections in Class C = $2^{29} = 53, 68, 70, 912$.
- Total number of networks available in Class C = $2^{24} = 20, 97, 152$.

- Total number of hosts that can be configured in every network in Class C = $2^8 - 2 = 254$.
- Organizations needing small to medium-sized networks typically choose class C.

Quick Quiz - The maximum number of networks that can use Class C addresses in the IPv4 addressing format is _____

1. 2^{14}
2. 2^7
3. 2^{21}
4. 2^{24}

Ans. (c)

CLASS D - Prefix and suffix categories do not exist for Class D. It is employed for multicast addresses.

- There is no concept of Host ID and Net ID
- Method to identify Class D network:
 - The first four bits are reserved to 1110 in binary notation or $(1110)_2$
 - The range of the first octet is [224, 239] in dotted decimal notation
- Total number of IP addresses available is $2^{28} = 26, 84, 35, 456$
- Because data is not intended for a specific host, Class D is set aside for multicasting, which eliminates the requirement to extract the host address from the IP address.

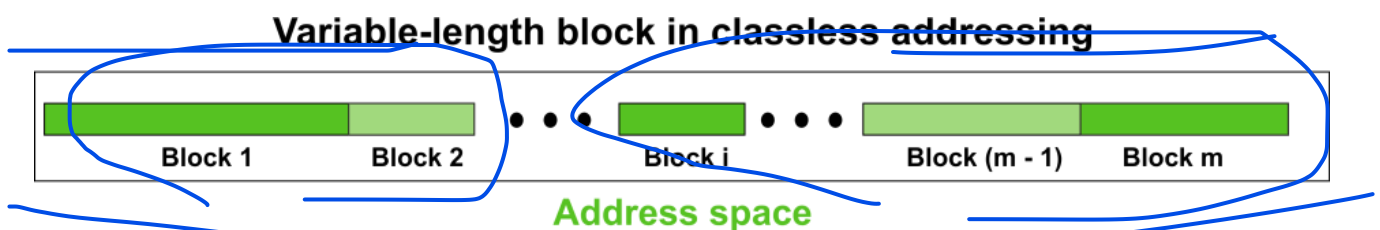
CLASS E - All binary addresses with the prefix 1111 fall under class E. Class E, like Class D, does not have a prefix or a suffix and is used as a reserve.

- Like in Class D, there is also no concept of Host ID and Net ID.
- Method to identify Class E networks:
 - The first four bits are reserved to 1111 in binary notation or (1111)
 - The range of the first octet is [240, 255] in dotted decimal notation.
- Total number of IP addresses available is $2^{28} = 26,84,35,456$.
- Class E is set aside for hypothetical or experimental uses.

2. CLASSLESS ADDRESSING

The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques. As the Internet expanded, it became obvious that a bigger address space was required as a long-term fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax. The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. ***Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses.*** In order to make up for address depletion, the class privilege was taken out of the distribution.

The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device). We are capable of having a block of 20, 21, 22, ..., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses. One address block may be given to an organization. The given figure demonstrates the non-overlapping block segmentation of the entire address space.



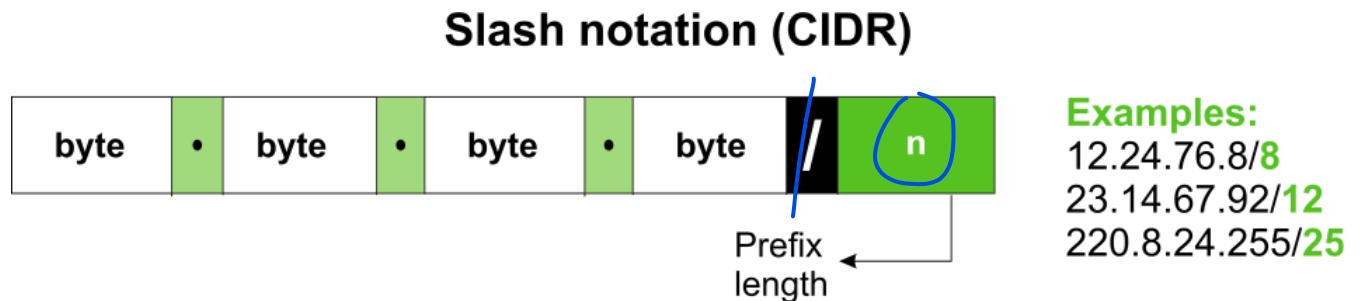
In contrast to classful addressing, classless addressing allows for varying prefix lengths. Prefix lengths that vary from 0 to 32 are possible. The length of the prefix has an inverse relationship with network size. A smaller network has a large prefix; a larger one has a small prefix.

We must stress that classful addressing is just as easily adaptable to the concept of classless addressing. Consider an address in class A as a classless address with a prefix length of 8. Class B addresses can be viewed as classless addresses with the prefix 16 and so on. Putting it another way, ***classless addressing is a specific instance of classful addressing.***

Prefix Length - Slash Notation

In classless addressing, the first issue that needs to be resolved is how to determine the prefix length if an address is provided. We must individually provide the prefix length

because it is not a property of the address. The address is inserted in this scenario, followed by a slash, and the prefix length, n . Slash notation is the colloquial name for the notation, while classless interdomain routing, or CIDR (pronounced cider) method, is the official name. An address in classless addressing can thus be expressed as illustrated in the figure below.



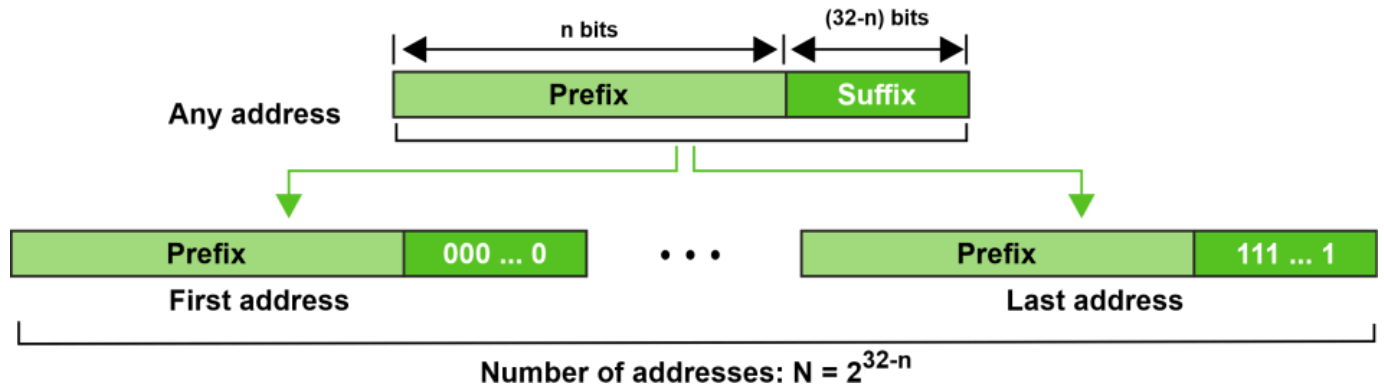
To put it another way, we must also provide the prefix length in classless addressing because an address does not automatically define the block or network to which it belongs.

Extracting Information from an Address

With respect to any given address in the block, we typically like to know three things: the number of addresses in the block, the start address in the block, and the last address. These three pieces of information, which are depicted in the picture below, are simple to locate because the prefix length, n , is known.

- The block has $N = 2^{32-n}$ addresses, according to the calculation.
- The n leftmost bits are kept, and the $(32 - n)$ rightmost bits are all set to zeroes to determine the first address.
- The n leftmost bits are kept, while the $(32 - n)$ rightmost bits are all set to 1s to determine the last address.

Information extraction in classless addressing



For Example - The address 167.199.170.82/27 is a classless address. The following is where we can find the aforementioned three pieces of data. In the network, there are $2^{32-n} = 2^5 = 32$ addresses in all.

The first 27 bits are kept while the remaining bits are converted to 0s to determine the first address.

Address: 167.199.170.82/27

10101010 01010010

10100111 11000111

First address: 167.199.170.64/27

10101010 01000000

10100111 11000111

Keeping the first 27 bits and turning the remaining bits to 1s will allow you to determine the last address.

Address: 167.199.170.82/27

10101010 01011111

10100111 11000111

Last address: 167.199.170.95/27

10101010 01011111

10100111 11000111

Quick Quiz - In the network 200.10.11.144/27, the fourth octet (in decimal) of the last IP address of the network, which can be assigned to a host is ____ (GATE 2015, 2 Marks)

Ans.

Address: 200.10.11.144/**27**
00001011 10010000

11010000 00001010

Last Address: 200.10.11.159/**27**
00001011 100**11111**

11010000 00001010

Here, the maximum possible value of the last octet is 159 in decimal. Hence, the fourth octet of the last IP address, which can be assigned to a host is 10011110 in binary or 158 in decimal. Hence, ***the answer to the question is 158.***

Difference Between Classful and Classless Addressing

1. IP addresses are divided into five groups using the classful addressing approach when they are assigned. In order to prevent the depletion of IP addresses, classless addressing is used. It is a method of IP address allocation that will eventually replace classful addressing.
2. A further distinction is the usefulness of classful and classless addressing. Comparatively speaking, classless addressing is more beneficial and useful than classful addressing.
3. In classful addressing, the network ID and host ID are adjusted according to the classes. However, the distinction between network ID and host ID does not exist with classless addressing. This opens up the possibility of making yet another contrast between both addressing.

CONCLUSION

IP addressing includes two types: classful and classless. Classless addressing offers a more effective method of allocating IP addresses than classful addressing, which is the main difference between the two. To put it briefly, classless addressing prevents the issue of IP address exhaustion that can occur with classful addressing.

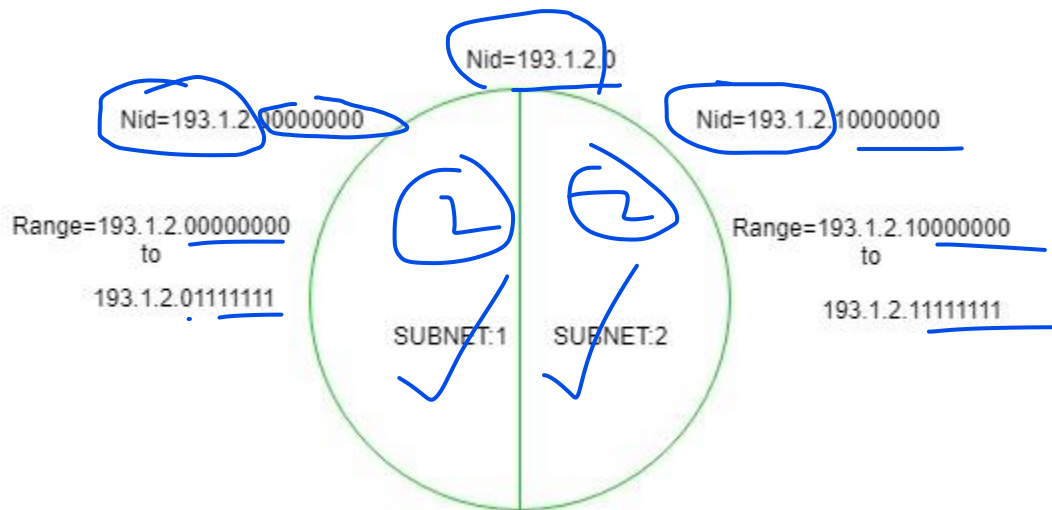
Introduction To Subnetting

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 2^{24} for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

Uses of Subnetting

1. Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
2. Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
3. Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
4. Subnetting is used in increasing network security.

The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

How Does Subnetting Work?

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its

linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

In [class C](#) the first 3 octets are network bits so it remains as it is.

- **For Subnet-1:** The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

Thus, the range of subnet 1 is: **193.1.2.0 to 193.1.2.127**

Subnet id of Subnet-1 is : 193.1.2.0

The direct Broadcast id of Subnet-1 is: 193.1.2.127

The total number of hosts possible is: 126 (Out of 128,

2 id's are used for Subnet id & Direct Broadcast id)

The subnet mask of Subnet- 1 is: 255.255.255.128

- **For Subnet-2:** The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).

Thus, the range of subnet-2 is: **193.1.2.128 to 193.1.2.255**

Subnet id of Subnet-2 is : 193.1.2.128

The direct Broadcast id of Subnet-2 is: 193.1.2.255

The total number of hosts possible is: 126 (Out of 128,

2 id's are used for Subnet id & Direct Broadcast id)

The subnet mask of Subnet- 2 is: 255.255.255.128

The best way to find out the subnet mask of a subnet

is to set the fixed bit of host-id to 1 and the rest to 0.

Finally, after using the subnetting the total number of usable hosts is reduced from 254 to 252.

Note:

1. To divide a network into four (2^2) parts you need to choose two bits from the host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (2^3) parts you need to choose three bits from the host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.
3. We can say that if the total number of subnets in a network increases the total number of usable hosts decreases.

Along with the advantage, there is a small disadvantage to subnetting that is, before subnetting to find the IP address first the network id is found then the host id followed by the process id, but after subnetting first network id is found then the subnet id then host id and finally process id by this the computation increases.

Example 1: An organization is assigned a [class C network address](#) of 201.35.2.0. It uses a netmask of 255.255.255.192 to divide this into sub-networks. Which of the following is/are valid host IP addresses?

1. 201.35.2.129
2. 201.35.2.191
3. 201.35.2.255
4. Both (A) and (C)

Solution:

Converting the last octet of the

netmask into the binary form: 255.255.255.**11000000**

Converting the last octet of option 1

into the binary form: 201.35.2.**10000001**

Converting the last octet of option 2

into the binary form: 201.35.2.**10111111**

Converting the last octet of option 3

into the binary form: 201.35.2.**11111111**

From the above, we see that Options 2 and 3 are not valid host IP addresses (as they are broadcast addresses of a subnetwork), and **OPTION 1** is not a broadcast address and it can be assigned to a host IP.

Example 2: An organization has a class C network address of 201.32.64.0. It uses a subnet mask of 255.255.255.248. Which of the following is NOT a valid broadcast address for any subnetworks?

1. 201.32.64.135
2. 201.32.64.240
3. 201.32.64.207
4. 201.32.64.231

Solution:

Converting the last octet of the netmask

into the binary form: 255.255.255.**11111000**

Converting the last octet of option 1

into the binary form: 201.32.64.**10000111**

Converting the last octet of option 2

into the binary form: 201.32.64.**11110000**

Converting the last octet of option 3

into the binary form: 201.32.64.**11001111**

Converting the last octet of option 4

into the binary form: 201.32.64.**11100111**

From the above, we can see that in OPTION 1, 3, and 4, all the host bits are 1 and give the valid broadcast address of subnetworks.

and **OPTION 2**, the last three bits of the Host address are not 1 therefore it's not a valid broadcast address.

Advantages of Subnetting

The advantages of Subnetting are mentioned below:

1. It provides security to one network from another network. eg) In an Organisation, the code of the Developer department must not be accessed by another department.
2. It may be possible that a particular subnet might need higher network priority than others. For example, a Sales department needs to host webcasts or video conferences.
3. In the case of Small networks, maintenance is easy.

Disadvantages of Subnetting

The disadvantages of Subnetting are mentioned below:

1. In the case of a single network, only three steps are required to reach a Process i.e Source Host to Destination Network, Destination Network to Destination Host, and then Destination Host to Process.
2. In the case of a Single Network only two IP addresses are wasted to represent Network Id and Broadcast address but in the case of Subnetting two IP addresses are wasted for each Subnet.
3. The cost of the overall Network also increases. Subnetting requires internal routers, Switches, Hubs, Bridges, etc. which are very costly.

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for host addressing
- **Class B** - it uses first two octets for network addresses and last two for host addressing
- **Class C** - it uses first three octets for network addresses and last one for host addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

ICMPv6

The Internet protocol (IP) moves data from one node to another; however, for IP to perform this task successfully, there are other functions that need to be performed: error reporting, router discovery, diagnostics, and others. In IPv6, all these tasks are carried out by the Internet Control Message Protocol (ICMPv6).

In addition, ICMPv6 provides a framework for Multicast Listener Discovery (MLD) and Neighbor Discovery (ND), which carry out the tasks of conveying multicast group membership information (the equivalent of the IGMP protocol in IPv4) and address resolution (performed by ARP in IPv4).

The types of ICMPv6 messages include error messages and informational messages:

Error

Report errors in the forwarding or delivery of IPv6 packets.

Informational

Provide diagnostic functions and additional host functionality such as MLD and ND.

The following ICMPv6 messages are supported:

- Destination unreachable
- Packet too big
- Time exceeded (hop limit exceeded)
- Echo request/reply
- Parameter problem
- Multicast listener discovery:
 - Group membership query
 - Report
 - Done
- Neighbor discovery:
 - Router solicitation and advertisement
 - Neighbor solicitation and advertisement
 - Redirect

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

✓ IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

- Dual stack implementation
- Tunneling
- NAT-PT

IPv6