Unit III

ROUTING

Packet Forwarding

The process of packet forwarding simply implies the forwarding of incoming packets to their intended destination.

- Internet is made up of generally two terms- Interconnection and Network. So, it is a connection to a large collection of networks. A packet that is to be forwarded may be associated with the same network as the source host or may belong to a destination host in a different network. Thus, it depends on the destination how much a packet may need to travel before arriving at its destination.
- The router is responsible for the process of packet forwarding. It accepts the packet from the origin host or another router in the packet's path and places it on the route leading to the target host.
- The routing table is maintained by the router which is used for deciding the packet forwarding.

Packet Forwarding in Router:

Routers are used on the network for forwarding a packet from the local network to the remote network. So, the process of routing involves the packet forwarding from an entry interface out to an exit interface.

Working:

The following steps are included in the packet forwarding in the router-

- The router takes the arriving packet from an entry interface and then forwards that packet to another interface.
- The router needs to select the best possible interface for the packet to reach the intended destination as there exist multiple interfaces in the router.
- The forwarding decision is made by the router based on routing table entries. The entries in the routing table comprise destination networks and exit interfaces to which the packet is to be forwarded.
- The selection of exit interface relies on- firstly, the interface must lead to the target network to which the packet is intended to send, and secondly, it must be the best possible path leading to the destination network.

Packet Forwarding Techniques:

Following are the packet forwarding techniques based on the destination host:

- Next-Hop Method: By only maintaining the details of the next hop or next router in the packet's path, the next-hop approach reduces the size of the routing table. The routing table maintained using this method does not have the information regarding the whole route that the packet must take.
- Network-Specific Method: In this method, the entries are not made for all of the destination hosts in the router's network. Rather, the entry is made of the destination networks that are connected to the router.
- Host-Specific Method: In this method, the routing table has the entries for all of the destination hosts in the destination network. With the increase in the size of the routing table, the efficiency of the routing table decreases. It finds its application in the process of verification of route and security purposes.
- Default Method: Let's assume- A host in network N1 is connected to two routers, one of which (router R1) is connected to network N2 and the other router R2 to the rest of the internet. As a result, the routing table only has one default entry for the router R2.

Static and Default Routing

Routing is the technique of determining the optimal path to transmit the data from one location to another. The router may assist in completing this task. It is a device that operates on the network layer of the OSI model and the internet layer of the TCP and IP model. The routing algorithm enables the router to select the best route between the source and the destination. Furthermore, it stores path data in a table known as the routing table. Static and dynamic routing are the two forms of routing. Static routes are configured before any network interactions. In contrast, dynamic routing needs routers to communicate information with other routers to learn about network paths.

Static Routing

It is also known as *"non-adaptive routing"*. The network administrator contains the routes in the routing table while using this routing. As a result, the router transfers data from the source to the destination using the administrator-defined route. Routing decisions don't depend on factors like network traffic or topology. Furthermore, static routing doesn't need much bandwidth between routers. The network is also more secure because the network administrator conducts the necessary routing activities. Furthermore, the overall cost of static routing is less. Static routing is also unsuitable for big networks with significant traffic due to the difficulties of manually adding routes to routing tables.

Advantages and Disadvantages of Static Routing

There are various advantages and disadvantages of *static routing*. Some main advantages and disadvantages of static routing are as follows:

Advantages

1. It can easily implement in small networks.
2. It doesn't need bandwidth usage between the routers.
3. It doesn't need additional resources as update mechanisms are not required.
4. It is a more secure routing.
5. It is more predictable because the route is specified to the destination.

Disadvantages

1. It is not helpful for complicated topologies and large networks.
2. When the link is failed, it may affect the traffic rerouting.
3. The administrator must use extreme caution when configuring the routes.

Dynamic Routing

Dynamic routing is also known as *"adaptive routing"*, and it is a method of automatic routing. In other words, when new routers are introduced to the network, the routing tables change. When a router fails, the routing table automatically modifies to get the destination. As a result, dynamic routing responds to network and traffic changes. This routing method employs dynamic routing algorithms to find new routes to the destination. As a result, all network routers should use dynamic routing protocols that are consistent. Dynamic routing needs fewer routes. Moreover, it offers more accurate results in determining the optimum path based on network changes. However, this routing method needs more bandwidth and offers less security.

Advantages and Disadvantages of Dynamic Routing

There are various advantages and disadvantages of *dynamic routing*. Some main advantages and disadvantages of dynamic routing are as follows:

Advantages

1. It is very helpful to all the topologies.
2. Topologies automatically support traffic rerouting.
3. The activities of the router are unaffected by network size.

Disadvantages

1. Dynamic routes depend on the current topologies.
2. It needs extra resources like CPU, memory, and link bandwidth.
3. It may be complex to implement.
4. It is less secure as routing updates are broadcast and multicast.

Some main differences between Static and Dynamic Routing are as follows:

1. Static routing happens when a router utilizes a manually specified routing entry rather than information from dynamic routing traffic. In contrast, dynamic routing is a method in which a router may transmit data via a different route or to a specific destination based on the current state of the network's communication circuits.
2. Routing tables are manually updated in static routing. In contrast, tables are automatically updated in dynamic routing.
3. Complex algorithms are not used in static routing. In contrast, dynamic routing utilizes a complicated algorithm to determine the shortest path or route.
4. Dynamic routing is less secure due to message broadcast and multicast. In contrast, static routing doesn't require advertisement, which makes it more secure.
5. Static routing requires no additional resources. In contrast, dynamic routing needs resources like memory, bandwidth, etc.
6. Link failure may interrupt the rerouting in static routing. In contrast, link failure doesn't affect rerouting in dynamic routing.
7. The routes in static routing are user-defined. In contrast, the routes are updated as topology changes in dynamic routing.
8. RIP, BGP, EIGRP, and other protocols are used in dynamic routing. In contrast, static routing doesn't need such protocols.
9. The network architecture is minimal in static routing. In contrast, dynamic routing highly depends on network infrastructure.

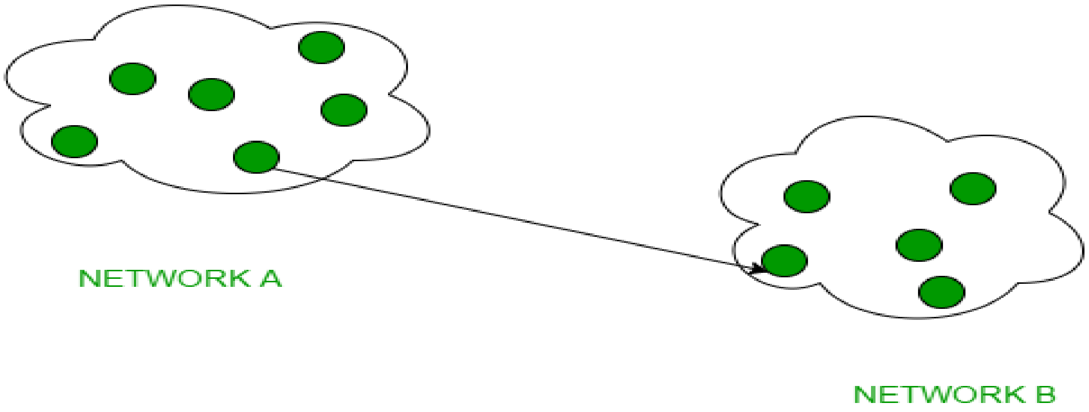
Features	**Static Routing**	**Dynamic Routing**

Definition	It happens when a router utilizes a manually specified routing entry rather than information from dynamic routing traffic.	It is a method in which a router may transmit data via a different route or to a specific destination based on the current state of the network's communication circuits.
Configuration Technique	The routing tables are manually updated in static routing.	The tables are automatically updated in dynamic routing.
Routes	Routes are specified by the administrative.	The routes are updated according to the modifications in the network.
Routing Algorithms	It doesn't utilize any complicated routing algorithms.	It utilizes complicated routing algorithms.
Link Affect	When a link fails in static routing, it interrupts the other routing path.	The link failure doesn't affect rerouting in dynamic routing.
Bandwidth	It needs less bandwidth.	It needs more bandwidth.
Security	It offers high security.	It offers less security.
Network Infrastructure	Its network infrastructure is minimal.	Its network infrastructure is large.
Routing Protocols	It doesn't utilize any protocol.	It employs protocols such as eigrp, arp, and others to calculate the routing process.
Additional Resources	It doesn't need any extra resources.	It needs extra resources to hold the information.
Implementation	It is implemented in small networks.	It is implemented in large networks.
Routing table building	Routing locations are hand-typed in static routing.	In dynamic routing, locations are dynamically filled in the table.

Unicast Routing Algorithms

Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between the sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP is the most commonly used unicast protocol. It is a connection-oriented protocol that relies on acknowledgment from the receiver side.
- HTTP stands for HyperText Transfer Protocol. It is an object-oriented protocol for communication.



UNICAST EXAMPLE

Major Protocols of Unicast Routing

1. **Distance Vector Routing:** Distance-Vector routers use a distributed algorithm to compute their routing tables.
2. **Link-State Routing:** Link-State routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.
3. **Path-Vector Routing:** It is a routing protocol that maintains the path that is updated dynamically.

Link State Routing

Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router i.e. the internet work. The three keys to understand the link state routing algorithm.

1. **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.
2. **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 the neighbors. Finally each and every router receives a copy of the same information.

3. **Information Sharing**: A router send the information to every other router only when the change occurs in the information.

Link state routing has two phase:

1. **Reliable Flooding: Initial state**– Each node knows the cost of its neighbors. Final state- Each node knows the entire graph.
2. **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.

Features of Link State Routing Protocols

- **Link State Packet:** A small packet that contains routing information.
- **Link-State Database:** A collection of information gathered from the link-state packet.
- **Shortest Path First Algorithm (Dijkstra algorithm):** A calculation performed on the database results in the shortest path
- **Routing Table:** A list of known paths and interfaces.

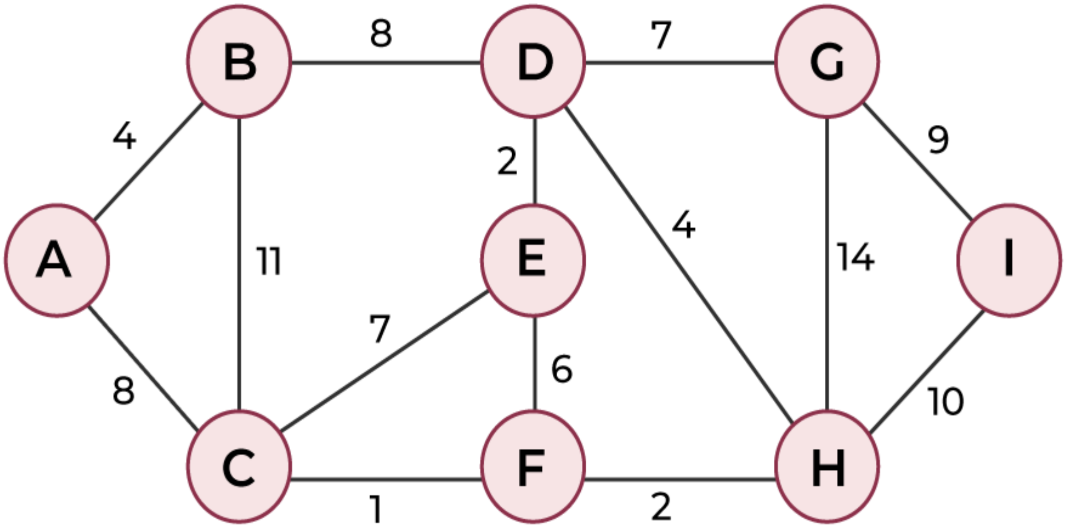
Calculation of Shortest Path

To find the shortest path, each node needs to run the famous Dijkstra algorithm. Let us understand how can we find the shortest path using an example.

Illustration

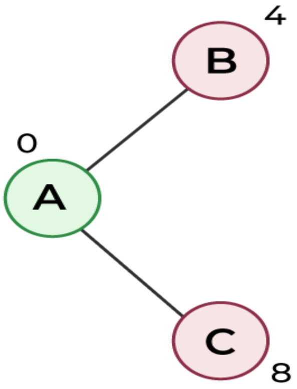
To understand the Dijkstra Algorithm, let's take a graph and find the shortest path from the source to all nodes.

Note: We use a boolean array **sptSet[]** to represent the set of vertices included in SPT.
If a value **sptSet[v]** is true, then vertex v is included in SPT, otherwise not.
Array **dist[]** is used to store the shortest distance values of all vertices.
Consider the below graph and src = 0.



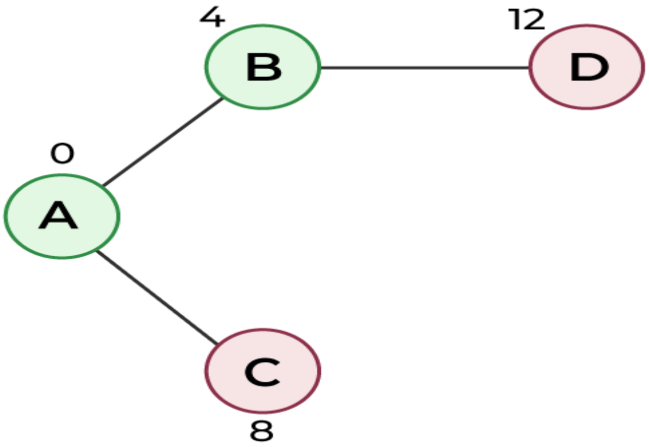
Shortest Path Calculation – Step 1

STEP 1: The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with a minimum distance value. The vertex 0 is picked and included in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update the distance values of its adjacent vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8.
The following subgraph shows vertices and their distance values. Vertices included in SPT are included in GREEN color.



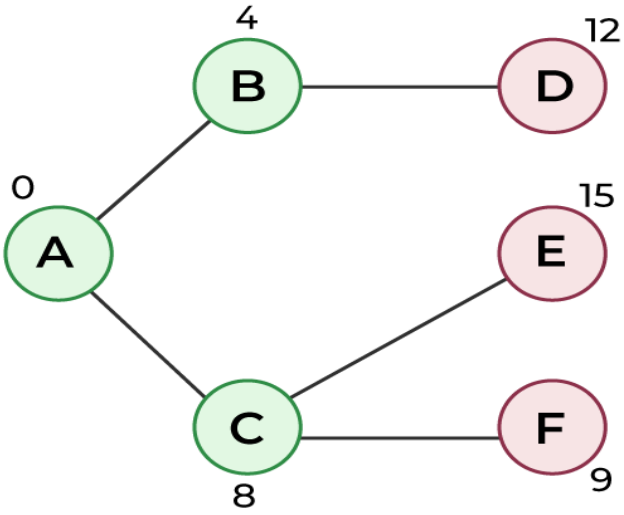
Shortest Path Calculation – Step 2

STEP 2: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12.



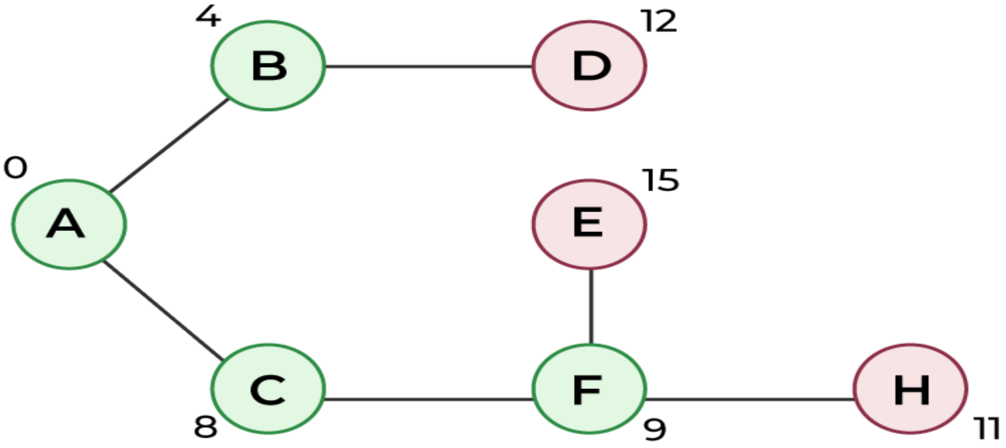
Shortest Path Calculation – Step 3

STEP 3: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7. The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively).



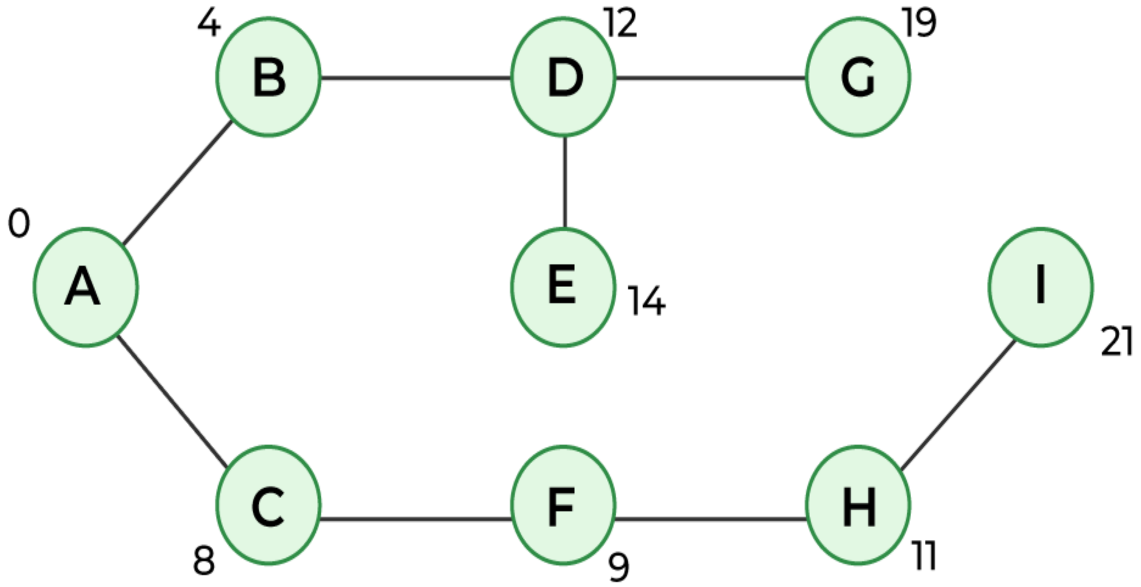
Shortest Path Calculation – Step 4

STEP 4: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6. The distance value of vertex 5 and 8 are updated.



Shortest Path Calculation – Step 5

We repeat the above steps until sptSet includes all vertices of the given graph. Finally, we get the following Shortest Path Tree (SPT).



Shortest Path Calculation – Step 6

Characteristics of Link State Protocol

- It requires a large amount of memory.
- Shortest path computations require many CPU circles.
- If a network uses little bandwidth; it quickly reacts to topology changes
- All items in the database must be sent to neighbors to form link-state packets.
- All neighbors must be trusted in the topology.
- Authentication mechanisms can be used to avoid undesired adjacency and problems.
- No split horizon techniques are possible in the link-state routing.
- OSPF Protocol

Distance Vector Routing

A distance-vector routing (DVR) protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances, based on a chosen metric, are computed using information from the neighbors' distance vectors.

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

```
Distance Vector Table Initialization -
•  Distance to itself = 0
•  Distance to ALL other routers = infinity number.
```

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbor containing different information than before.
   - It discovers that a link to a neighbor has gone down.

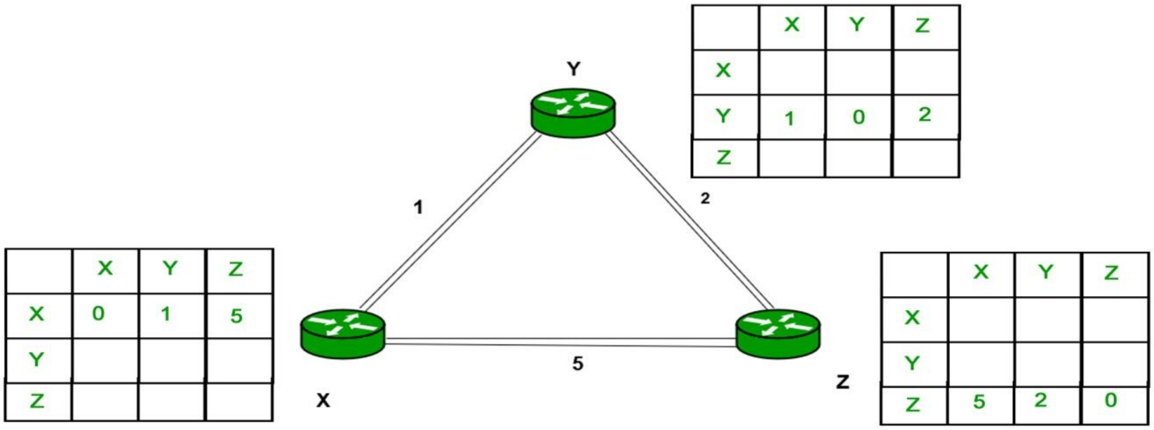
The DV calculation is based on minimizing the cost to each destination

```
Dx(y) = Estimate of least cost from x to y

C(x,v) =  Node x knows cost to each neighbor v

Dx   =  [Dx(y): y ? N ] = Node x maintains distance vector

Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ? N ]
```

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v’s distance vector and it updates its own DV using B-F equation:

```
Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ? N
```

Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



	X	Y	Z
X			
Y	1	0	2
Z			

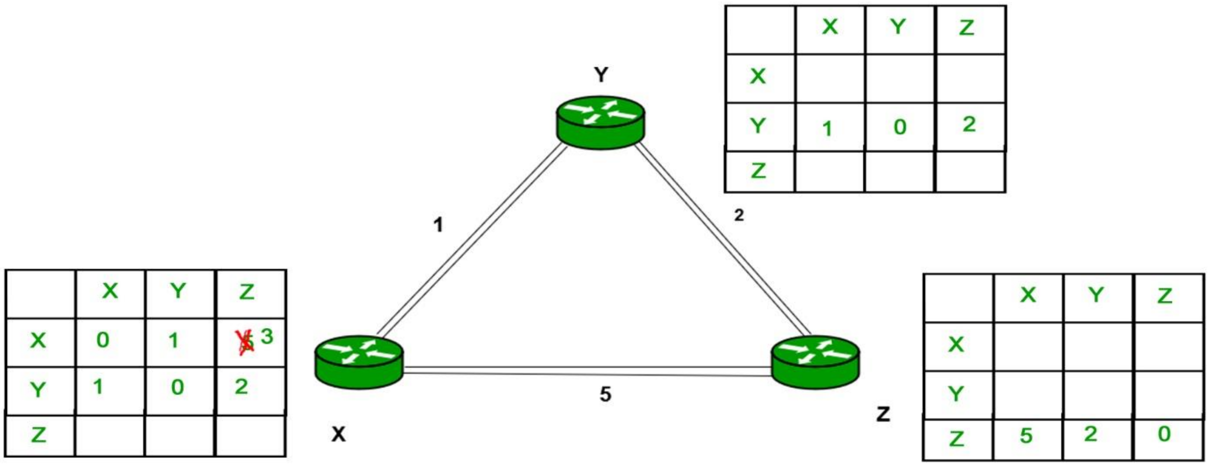
	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

```
Dx(y) = min { C(x,v) + Dv(y)} for each node y ? N
```

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.

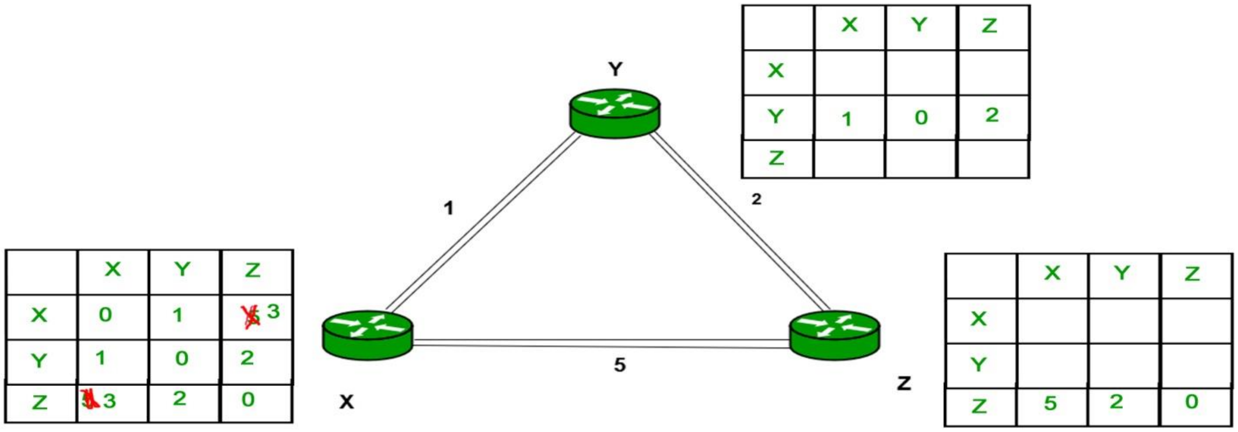


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Similarly for Z also –

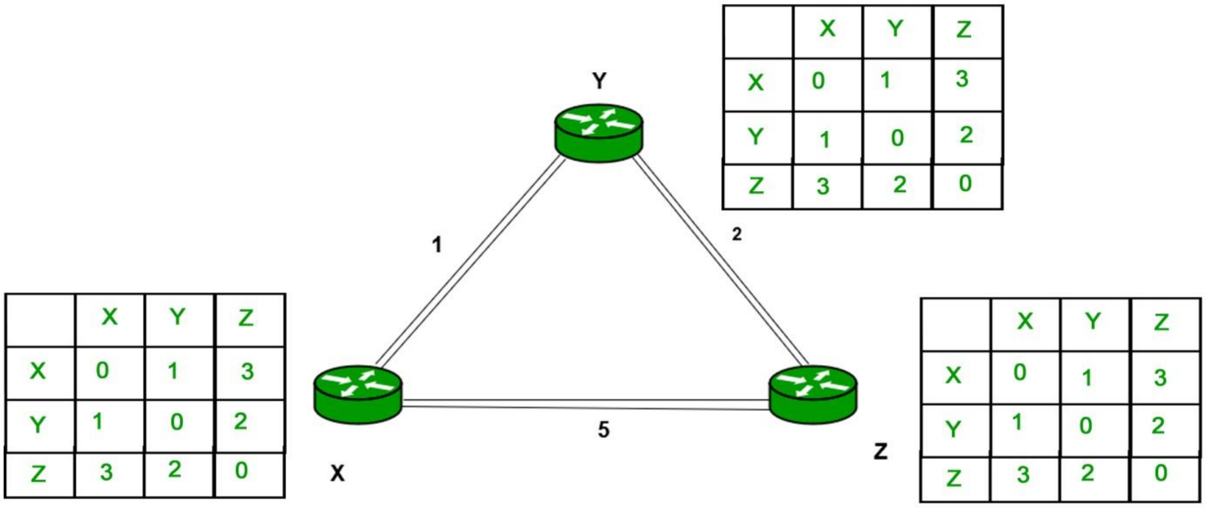


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z	~~5~~ 3	2	0

	X	Y	Z
X			
Y			
Z	5	2	0

Finally the routing table for all –



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

<u>Path Vector Routing Algorithm</u>

A **path vector protocol** is a computer network routing protocol which maintains the path information that gets updated dynamically. Updates which have looped through the network and returned to the same node are easily detected and discarded. This algorithm is sometimes used in Bellman–Ford routing algorithms to avoid "Count to Infinity" problems.

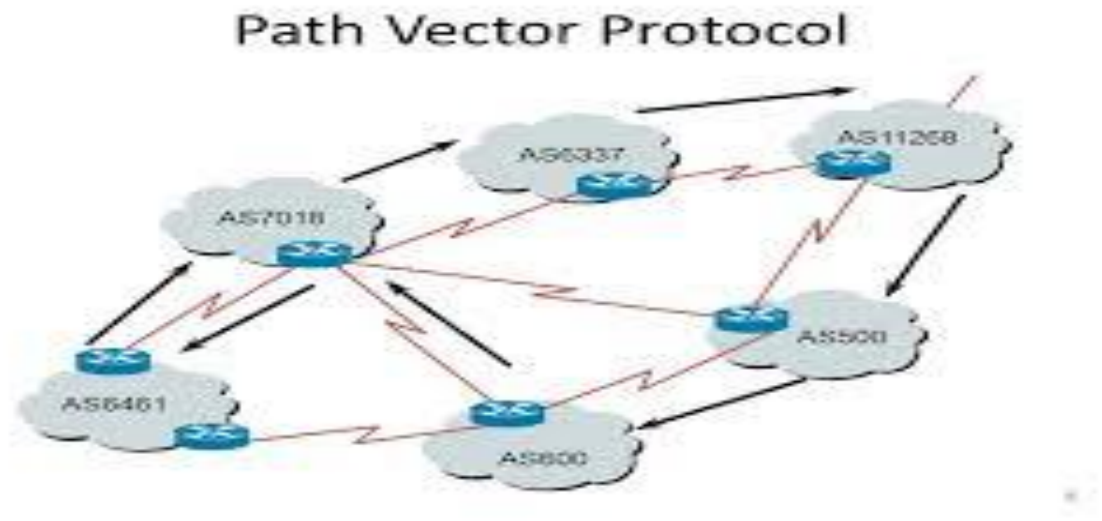
It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router and the path to reach the destination.

Path Vector Messages in BGP: The autonomous system boundary routers (ASBR), which participate in path vector routing, advertise the reachability of networks. Each router that receives a path vector message must verify that the advertised path is according to its policy. If the messages comply with the policy, the ASBR modifies its routing table and the message before sending it to the next neighbor. In the modified message it sends its own AS number and replaces the next router entry with its own identification.

BGP is an example of a path vector protocol. In BGP the routing table maintains the autonomous systems that are traversed in order to reach the destination system. Exterior Gateway Protocol (EGP) does not use path vectors.

It has three phases:

```
1.)   Initiation 2.)Sharing 3.)Updating
```



RIP V1

Routing Information Protocol (RIP) protocol are the intradomain (interior) routing protocol which is based on distance vector routing and it is used inside an autonomous system. Routers and network links are called node. The first column of routing table is destination address. The cost of metric in this protocol is hop count which is number of networks which need to be passed to reach destination. Here infinity is defined by a fixed number which is 16 it means that using a Rip, network cannot have more than 15 hops.

RIP Version-1:

It is an open standard protocol means it works on the various vendor's routers. It works on most of the routers, it is classful routing protocol. Updates are broadcasted. Its administrative distance value is 120, it means it is not reliable. The lesser the administrative distance value the reliability is much more. Its metric is hop count and max hop count is 15. There will be a total of 16 routers in the network. When there will be the same number of hop to reach the destination, Rip starts to perform load balancing. Load balancing means if there are three ways to reach the destination and each way has same number of routers then packets will be sent to each path to reach the destination. This reduces traffic and also the load is balanced. It is used in small companies, in this protocol routing tables are updated in each 30 sec. Whenever link breaks rip trace out another path to reach the destination. It is one of the slowest protocol.

Advantages of RIP ver1 –

1. Easy to configure, static router are complex.
2. Less overhead
3. No complexity.

Disadvantage of RIP ver1 –

1. Bandwidth utilization is very high as broadcast for every 30 seconds.
2. It works only on hop count.
3. It is not scalable as hop count is only 15. If there will be requirement of more routers in the network it would be a problem.
4. Convergence is very slow, wastes a lot of time in finding alternate path.

RIP Version-2:

Due to some deficiencies in the original RIP specification, RIP version 2 was developed in 1993. It supports classless Inter-Domain Routing (CIDR) and has the ability to carry subnet information, its metric is also hop count, and max hop count 15 is same as rip version 1. It supports authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

Advantages of RIP ver2 –

1. It's a standardized protocol.
2. It's VLSM compliant.
3. Provides fast convergence.
4. It sends triggered updates when the network changes.
5. Works with snapshot routing – making it ideal for dial networks.

Disadvantage of RIP ver2 – There lies some disadvantages as well:

1. Max hopcount of 15, due to the 'count-to-infinity' vulnerability.
2. No concept of neighbours.
3. Exchanges entire table with all neighbours every 30 seconds (except in the case of a triggered update).

RIP ver1 versus RIP ver2:

RIP Ver1	RIP Ver2
RIP v1 uses what is known as classful routing	RIP v2 is a classless protocol and it supports variable-length subnet masking (VLSM), CIDR, and route summarization
RIPv1 routing updates are broadcasted	RIP v2 routing updates are multicasted
RIPv1 has no authentication	RIP v2 supports authentication
RIP v1 does not carry mask in updates	RIP v2 does carry mask in updates, so it supports for VLSM

RIP Ver1	RIP Ver2
RIP v1 is an older, no longer much used routing protocol	IP v2 can be useful in small, flat networks or at the edge of larger networks because of its simplicity in configuration and usage

OSPF :-

Open Shortest Path First (OSPF) is an IP routing protocol that uses a mathematical algorithm to calculate the most efficient path to direct traffic on IP networks. OSPF is an open standard and designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs) within the family of TCP/IP protocols.

Based on link-state or shortest path first (SPF) technology, OSPF distributes routing information between routers in a single autonomous system (AS). This capability differentiates OSPF from older TCP/IP routing protocols, which were designed for less complex networks than those used today.

Using Dijkstra's shortest path algorithm, OSPF calculates the shortest path for all routers in an area of the AS to efficiently use network bandwidth and ensure scalability. The AS may be divided into multiple interconnected networks, such as a wide area network (WAN). The topology is visible only to the routers in the same area.

As a dynamic routing protocol, OSPF not only routes IP packets based on the destination IP address (given in the packet header), but it also detects topological changes in the AS. After detecting changes, OSPF calculates new, loop-free routes after a short period (known as convergence time) in which routing traffic is kept to a minimum.

All the routers in the same area of the OSPF network maintain the same link-state database that describes the area topology. Each router receives link-state advertisement (LSA) messages containing information about neighboring routers and path costs from the other routers in that area. Using these LSAs, each router generates the link-state database and uses the SPF algorithm to calculate a shortest-path spanning tree.

OSPF was designed and developed by the IETF for TCP/IP environments, mainly large enterprise networks. OSPF version 2 is defined in RFC 2328 of the IETF Network Working Group. This protocol is broadly implemented in enterprise routers. IPv6 revisions to this standard are captured in OSPF version 3 and defined in IETF RFC 5340.

Border Gateway Protocol (BGP)

The protocol can connect any internetwork of the autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that can run BGP and that is the router connected to at least one other AS's BGP router. BGP's main function is to exchange network reachability 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 the Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- **Path Information:** BGP advertisements 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 conserves network Bandwidth.
- BGP supports CIDR.
- BGP also supports Security.

Functionality of Border Gateway Protocol (BGP)

BGP peers perform 3 functions, which are given below.

- The first function consists of initial peer acquisition and authentication. both the peers established a TCP connection and performed message exchange that guarantees both sides have agreed to communicate.
- The second function mainly focuses on sending negative or positive reach-ability information.
- The third function verifies that the peers and the network connection between them are functioning correctly.

Importance of Border Gateway Protocol(BGP)

- **Security:** BGP is highly secure because it authenticates messages between routers using preconfigured passwords through which unauthorized traffic is filtered out.
- **Scalability:** BGP is more scalable because it manages a vast number of routes and networks present on the internet.

- **Supports Multihoming:** BGP allows multihoming means an organization can connect to multiple networks simultaneously.
- **Calculate the Best Path:** As we know data packets is traveled across the internet from source to destination every system in between the source and destination has to decide where the data packet should go next
- **TCP/IP Model:** BGP is based on the TCP/IP model and it is used to control the network layer by using transport layer protocol.

Types of Border Gateway Protocol

- **External BGP:** It is used to interchange routing information between the routers in different autonomous systems, it is also known as eBGP(External Border Gateway Protocol). The below image shows how eBGP interchange routing information.
    - Internal BGP: It is used to interchange routing information between the routers in the same autonomous system, it is also known as iBGP(Internal Border Gateway Protocol). Internal routers also ensure consistency among routers for sharing routing information. The below image shows how iBGP interchange routing information.

Difference Between BGP and OSPF

Here below are some key differences between BGP and OSPF:

BGP	OSPF
It follows the Path Vector Routing Algorithm	It follows the Link State Routing Algorithm
The speed of convergence is very slow in BGP	The speed of convergence is fast in the case of OSPF
BGP is also called inter-domain routing protocol	OSPF is also called intra-domain routing protocol
In BGP routing operation is performed between two AS	In OSPF routing operation is performed inside an AS
In BGP, TCP protocol is used	In OSPF, IP protocol is used

EIGRP Enhanced Interior Gateway Routing Protocol (EIGRP)

It is a dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet. EIGRP works on network layer Protocol of OSI model and uses protocol number 88. It uses metrics to find out the best path between two layer 3 devices (router or layer 3 switches) operating EIGRP. Administrative Distance for EIGRP are:-

EIGRP routes	AD values

Summary Routes	5
Internal Routes	90
external routes	170

It uses some messages to communicate with the neighbour devices that operate EIGRP. These are:-

1. Hello message-These messages are kept alive messages which are exchanged between two devices operating EIGRP. These messages are used for neighbour discovery/recovery, if there is any device operating EIGRP or if any device(operating EIGRP) coming up again. These messages are used for neighbor discovery if multicast at 224.0.0.10. It contains values like AS number, k values, etc.

   These messages are used as acknowledgement when unicast. A hello with no data is used as the acknowledgement.
2. NULL update-It is used to calculate SRTT(Smooth Round Trip Timer) and RTO(Retransmission Time Out).

   SRTT: The time is taken by a packet to reach the neighboring router and the acknowledgement of the packet to reach the local router.

   RTO: If a multicast fails then unicast is being sent to that router. RTO is the time for which the local router waits for an acknowledgement of the packet.
3. Full Update – After exchanging hello messages or after the neighbourship is formed, these messages are exchanged. This message contains all the best routes.
4. Partial update-These messages are exchanged when there is a topology change and new links are added. It contains only the new routes, not all the routes. These messages are multicast.
5. Query message-These messages are multicast when the device is declared dead and it has no routes to it in its topology table.
6. Reply message – These messages are the acknowledgment of the query message sent to the originator of the query message stating the route to the network which has been asked in the query message.
7. Acknowledgement message

   It is used to acknowledge EIGRP updates, queries, and replies. Acks are hello packets that contain no data.

   Note:-Hello and acknowledgment packets do not require any acknowledgment.

   Reply, query, update messages are reliable messages i.e require acknowledgement.

Composite matrix-The EIGRP composite metric calculation can use up to 5 variables, but only 2 are used by default (K1 and K3). The composite metric values are :

K1 (bandwidth)
K2 (load)
K3 (delay)
K4 (reliability)
K5 (MTU)

The lowest bandwidth, load, delay, reliability, MTU along the path between the source and the destination is considered in the composite matrix in order to calculate the cost. Note:- Generally, only k1 and k3 values are used for metric calculation by EIGRP. The values are 10100 for k1, k2, k3, k4, k5 respectively. criteria To form EIGRP neighbourship, these criteria should be fulfilled:-

1. k values should match.
2. Autonomous system number should match. (AS is a group of networks running under a single administrative control) .
3. authentication should match (if applied). EIGRP supports MD5 authentication only.
4. subnet mask should be the same.

Timers:-

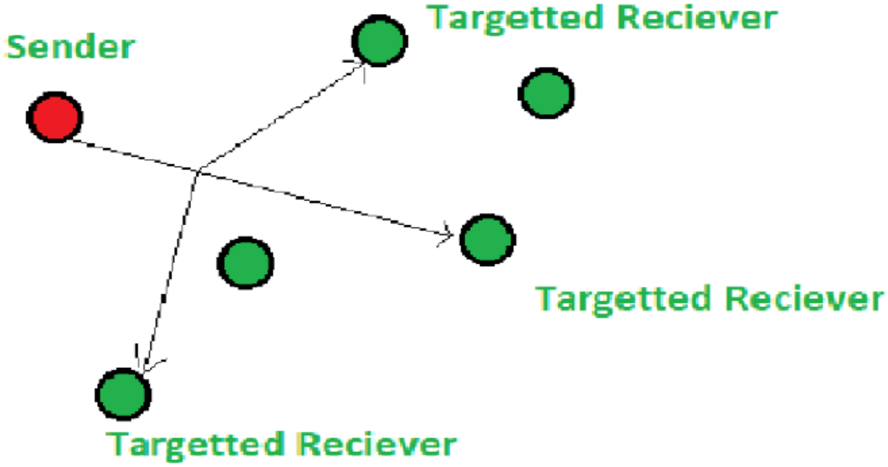
Hello timer- The interval in which EIGRP sends a hello message on an interface. It is 5 seconds by default.

5. Dead timer- The interval in which the neighbor will be declared dead if it is not able to send the hello packet. It is 15 seconds by default.

Multicasting Basics

Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network because at once the data can be received by multiple nodes.

Multicasting is considered as the special case of broadcasting as it works in similar to Broadcasting, but in Multicasting, the information is sent to the targeted or specific members of the network. This task can be accomplished by transmitting individual copies to each user or node present in the network, but sending individual copies to each user is inefficient and might increase the network latency. To overcome these shortcomings, multicasting allows a single transmission that can be split up among the multiple users, consequently, this reduces the bandwidth of the signal.



.

Applications : Multicasting is used in many areas like:

1. Internet protocol (IP)
2. Streaming Media
3. It also supports video conferencing applications and webcasts.

– Multicasting use classful addressing of IP address of class – D which ranges from 224.0.0.0 to 239.255.255.255

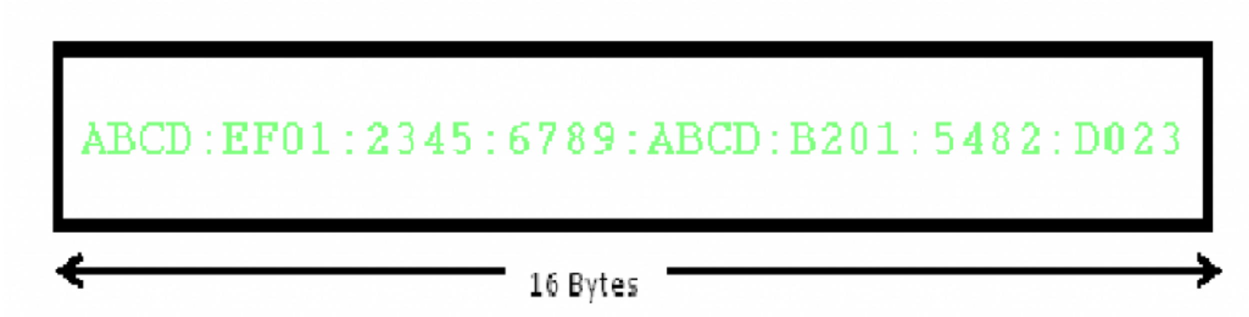
IP Multicast : Multicasting that takes place over the Internet is known as IP Multicasting. These multicast follow the internet protocol(IP) to transmit data. IP multicasting uses a mechanism known as ‘Multicast trees’ to transmit to information among the users of the network. Multicast trees; allows a single transmission to branch out to the desired receivers. The branches are created at the Internet routers, the branches are created such that the length of the transmission will be minimum.

IPV6 Address

IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bits address having an address space of 2128, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:).

Components in Address format :

1. There are 8 groups and each group represents 2 Bytes (16-bits).
2. Each Hex-Digit is of 4 bits (1 nibble)
3. Delimiter used – colon (:)



The Main reason of IPv6 was the address depletion as the need for electronic devices rose quickly when Internet Of Things (IOT) came into picture after the 1980s & other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security. IPv6 protocol responds to the above issues using the following main changes in the protocol:

1. Large address space

An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.

Better header format

IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data . This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

3. New options

IPv6 has new options to allow for additional functionalities.

4. Allowance for extension

IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

5. Support for resource allocation

In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

6. Support for more security

The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

In IPv6 representation, we have three addressing methods :

- Unicast
- Multicast
- Anycast

Addressing methods

1. Unicast Address

Unicast Address identifies a single network interface. A packet sent to a unicast address is delivered to the interface identified by that address.

2. Multicast Address

Multicast Address is used by multiple hosts, called as **groups**, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address. And every node is configured in the same way. In simple words, one data packet is sent to multiple destinations simultaneously.

3. Anycast Address

Anycast Address is assigned to a group of interfaces. Any packet sent to an anycast address will be delivered to only one member interface (mostly nearest host possible).

Note: Broadcast is not defined in IPv6.

Types of IPv6 address:

We have 128 bits in IPv6 address but by looking at the first few bits we can identify what type of address it is.

Prefix	**Allocation**	**Fraction of Address Space**
0000 0000	Reserved	1/256
0000 0001	Unassigned (UA)	1/256

Prefix	Allocation	Fraction of Address Space
0000 001	Reserved for NSAP	1/128
0000 01	UA	1/64
0000 1	UA	1/32
0001	UA	1/16
001	Global Unicast	1/8
010	UA	1/8
011	UA	1/8
100	UA	1/8
101	UA	1/8
110	UA	1/8
1110	UA	1/16
1111 0	UA	1/32

Prefix	Allocation	Fraction of Address Space
1111 10	UA	1/64
1111 110	UA	1/128
1111 1110 0	UA	1/512
1111 1110 10	Link-Local Unicast Addresses	1/1024
1111 1110 11	Site-Local Unicast Addresses	1/1024
1111 1111	Multicast Address	1/256