<u>**UNIT-1**</u>

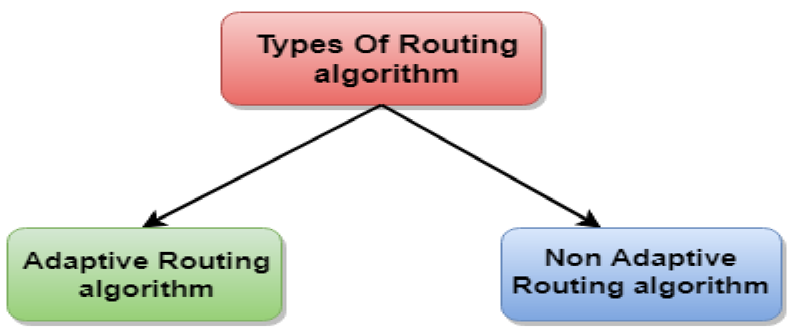
Routing algorithm

- 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-

Distance Vector Routing is a dynamic routing algorithm.

It works in the following steps-

Step-01:

Each router prepares its routing table. By their local knowledge. each router knows about-

- All the routers present in the network
- Distance to its neighboring routers

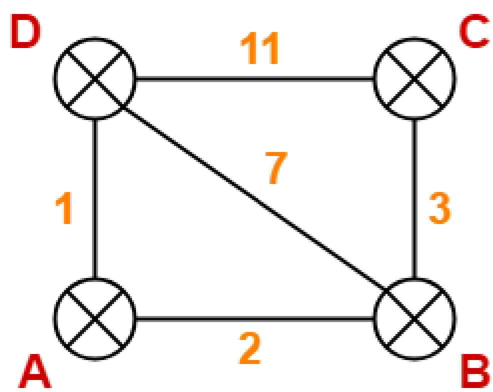
Step-02:

- Each router exchanges its distance vector with its neighboring routers.
- Each router prepares a new routing table using the distance vectors it has obtained from its neighbors.
- This step is repeated for (n-2) times if there are n routers in the network.
- After this, routing tables converge / become stable.

Distance Vector Routing Example-

Consider-

- There is a network consisting of 4 routers.
- The weights are mentioned on the edges.
- Weights could be distances or costs or delays.



Step-01:

Each router prepares its routing table using its local knowledge.

Routing table prepared by each router is shown below-

At Router A-

Destination	Distance	Next Hop
A	0	A
B	2	B
C	∞	–
D	1	D

At Router B-

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	7	D

At Router C-

Destination	Distance	Next Hop
A	∞	–
B	3	B
C	0	C
D	11	D

At Router D-

Destination	Distance	Next Hop
A	1	A
B	7	B
C	11	C
D	0	D

Step-02:

- Each router exchanges its distance vector obtained in Step-01 with its neighbors.
- After exchanging the distance vectors, each router prepares a new routing table.

This is shown below-

At Router A-

- Router A receives distance vectors from its neighbors B and D.
- Router A prepares a new routing table as-

From B

2
0
3
7

Cost(A→B) = 2

From D

1
7
11
0

Cost(A→D) = 1

Destination	Distance	Next hop
A	0	A
B		
C		
D		

New Routing Table at Router A

- Cost of reaching destination B from router A = min { 2+0 , 1+7 } = 2 via B.
- Cost of reaching destination C from router A = min { 2+3 , 1+11 } = 5 via B.
- Cost of reaching destination D from router A = min { 2+7 , 1+0 } = 1 via D.

Explanation For Destination B

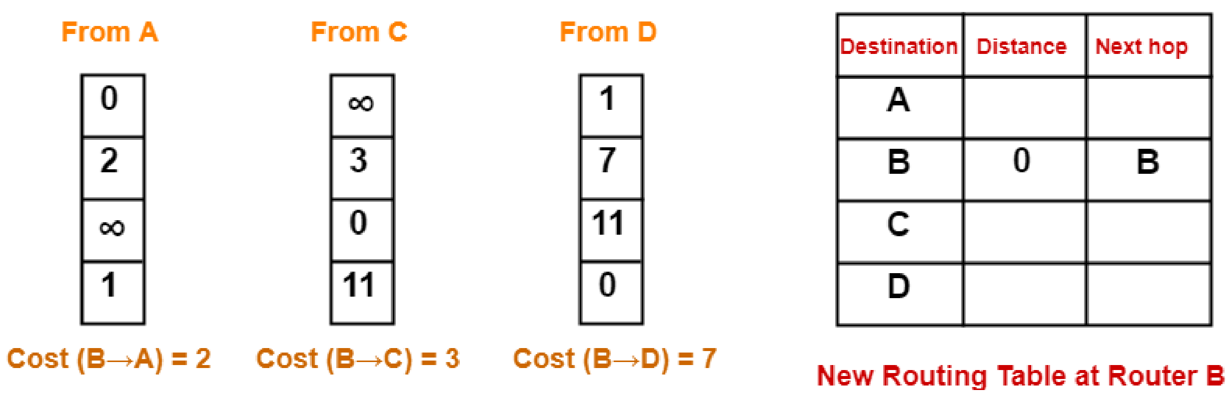
- Router A can reach the destination router B via its neighbor B or neighbor D.
- It chooses the path which gives the minimum cost.
- Cost of reaching router B from router A via neighbor B = Cost (A→B) + Cost (B→B)= **2 + 0** = 2
- Cost of reaching router B from router A via neighbor D = Cost (A→D) + Cost (D→B) = **1 + 7** = 8
- Since the cost is minimum via neighbor B, so router A chooses the path via B.
- It creates an entry (2, B) for destination B in its new routing table.
- Similarly, we calculate the shortest path distance to each destination router at every router.

Thus, the new routing table at router A is-

Destination	Distance	Next Hop
A	0	A
B	2	B
C	5	B
D	1	D

<u>At Router B-</u>

- Router B receives distance vectors from its neighbors A, C and D.
- Router B prepares a new routing table as-



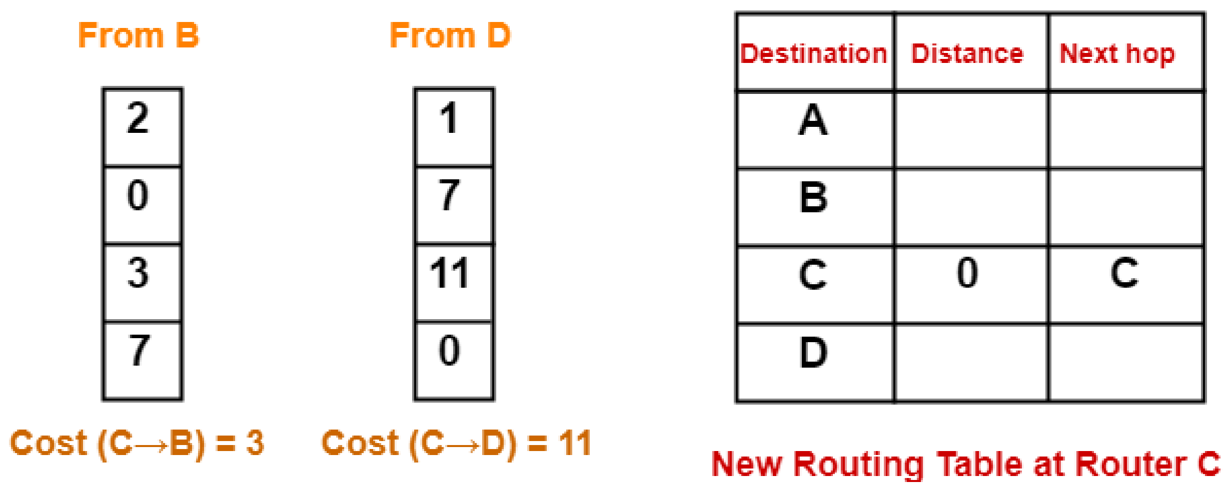
- Cost of reaching destination A from router B = min { 2+0 , 3+∞ , 7+1 } = 2 via A.
- Cost of reaching destination C from router B = min { 2+∞ , 3+0 , 7+11 } = 3 via C.
- Cost of reaching destination D from router B = min { 2+1 , 3+11 , 7+0 } = 3 via A.

Thus, the new routing table at router B is-

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	3	A

<u>At Router C-</u>

- Router C receives distance vectors from its neighbors B and D.
- Router C prepares a new routing table as-



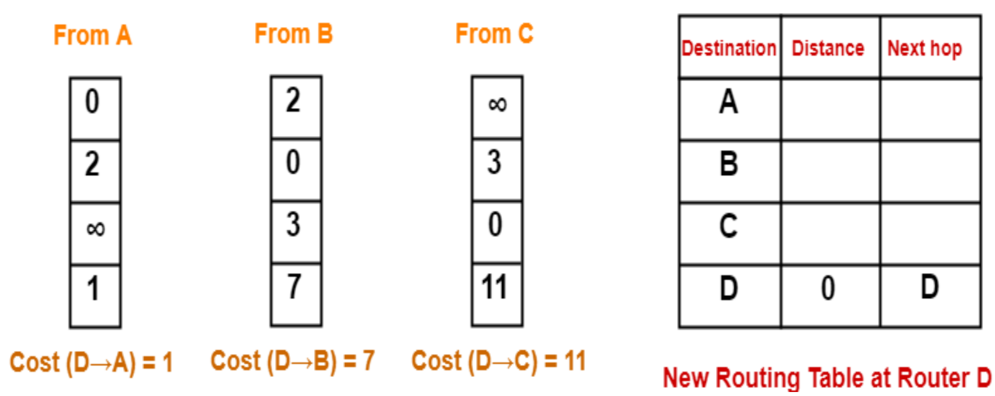
- Cost of reaching destination A from router C = min { 3+2 , 11+1 } = 5 via B.
- Cost of reaching destination B from router C = min { 3+0 , 11+7 } = 3 via B.
- Cost of reaching destination D from router C = min { 3+7 , 11+0 } = 10 via B.

Thus, the new routing table at router C is-

Destination	Distance	Next Hop
A	5	B
B	3	B
C	0	C
D	10	B

At Router D-

- Router D receives distance vectors from its neighbors A, B and C.
- Router D prepares a new routing table as-



- Cost of reaching destination A from router D = min { 1+0 , 7+2 , 11+∞ } = 1 via A.
- Cost of reaching destination B from router D = min { 1+2 , 7+0 , 11+3 } = 3 via A.
- Cost of reaching destination C from router D = min { 1+∞ , 7+3 , 11+0 } = 10 via B.

Thus, the new routing table at router D is-

Destination	Distance	Next Hop
A	1	A
B	3	A
C	10	B
D	0	D

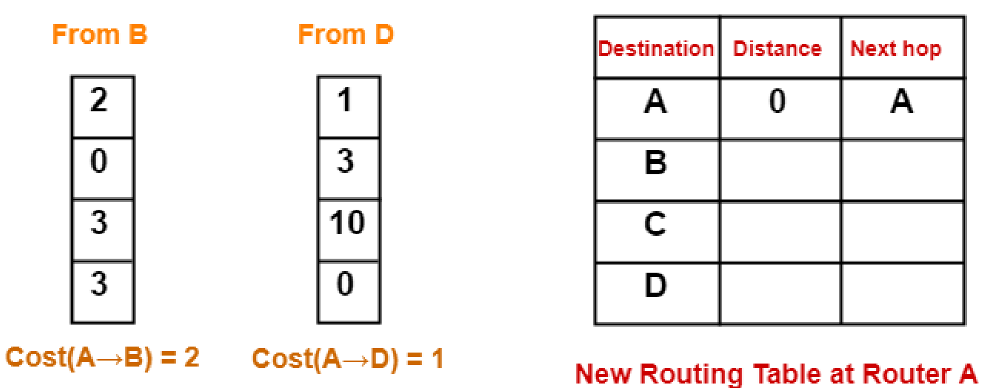
Step-03:

- Each router exchanges its distance vector obtained in Step-02 with its neighboring routers.
- After exchanging the distance vectors, each router prepares a new routing table.

This is shown below-

At Router A-

- Router A receives distance vectors from its neighbors B and D.
- Router A prepares a new routing table as-



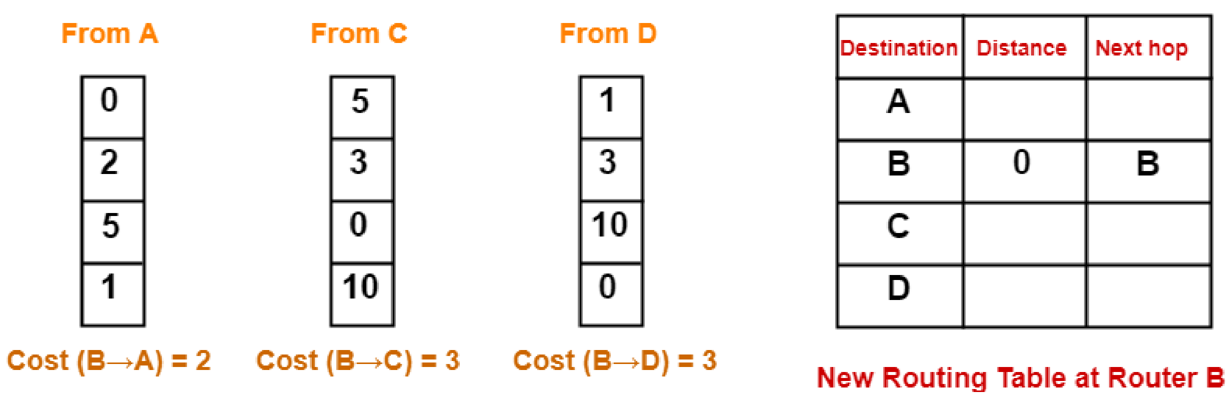
- Cost of reaching destination B from router A = min { 2+0 , 1+3 } = 2 via B.
- Cost of reaching destination C from router A = min { 2+3 , 1+10 } = 5 via B.
- Cost of reaching destination D from router A = min { 2+3 , 1+0 } = 1 via D.

Thus, the new routing table at router A is-

Destination	Distance	Next Hop
A	0	A
B	2	B
C	5	B
D	1	D

<u>At Router B-</u>

- Router B receives distance vectors from its neighbors A, C and D.
- Router B prepares a new routing table as-



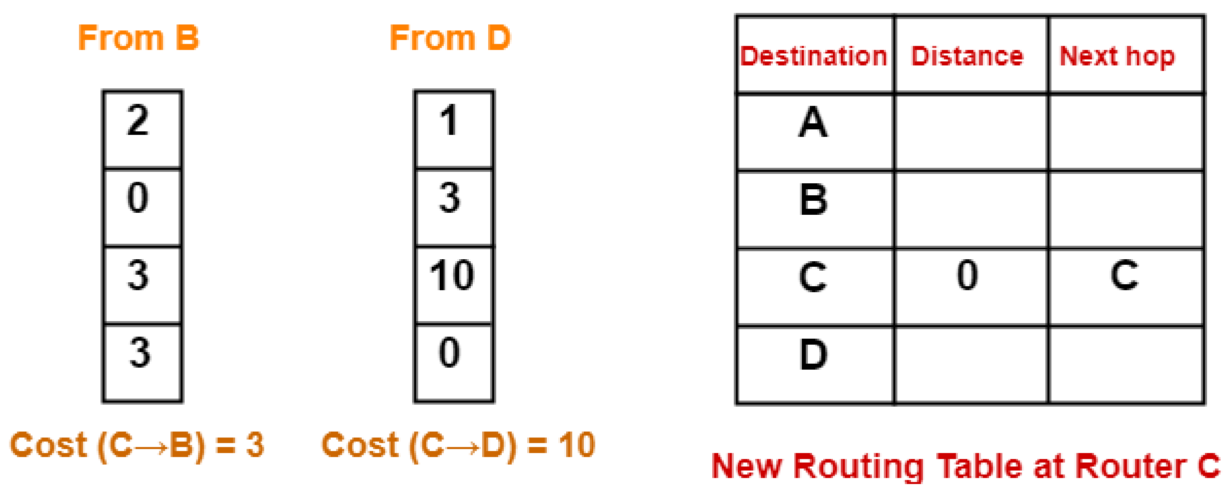
- Cost of reaching destination A from router B = min { 2+0 , 3+5 , 3+1 } = 2 via A.
- Cost of reaching destination C from router B = min { 2+5 , 3+0 , 3+10 } = 3 via C.
- Cost of reaching destination D from router B = min { 2+1 , 3+10 , 3+0 } = 3 via A.

Thus, the new routing table at router B is-

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	3	A

<u>At Router C-</u>

- Router C receives distance vectors from its neighbors B and D.
- Router C prepares a new routing table as-



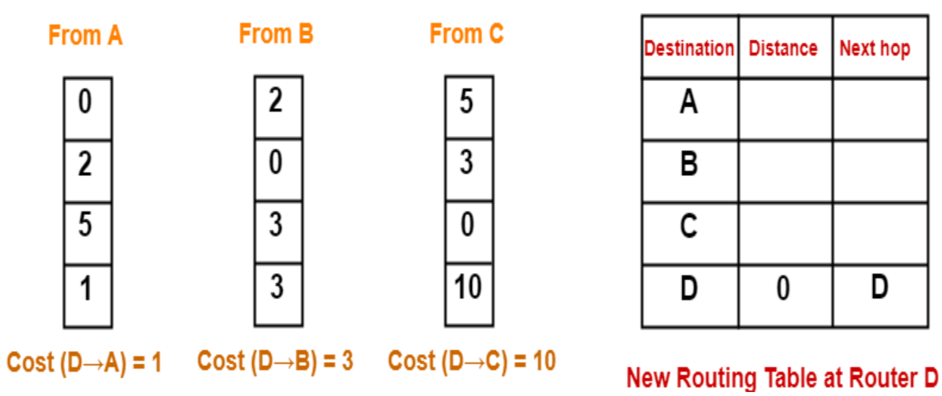
- Cost of reaching destination A from router C = min { 3+2 , 10+1 } = 5 via B.
- Cost of reaching destination B from router C = min { 3+0 , 10+3 } = 3 via B.
- Cost of reaching destination D from router C = min { 3+3 , 10+0 } = 6 via B.

Thus, the new routing table at router C is-

Destination	Distance	Next Hop
A	5	B
B	3	B
C	0	C
D	6	B

At Router D-

- Router D receives distance vectors from its neighbors A, B and C.
- Router D prepares a new routing table as-



- Cost of reaching destination A from router D = min { 1+0 , 3+2 , 10+5 } = 1 via A.
- Cost of reaching destination B from router D = min { 1+2 , 3+0 , 10+3 } = 3 via A.
- Cost of reaching destination C from router D = min { 1+5 , 3+3 , 10+0 } = 6 via A.

Thus, the new routing table at router D is-

Destination	Distance	Next Hop
A	1	A
B	3	A
C	6	A
D	0	D

These will be the final routing tables at each router.

Identifying Unused Links-

After routing tables converge (becomes stable),

- Some of the links connecting the routers may never be used.
- In the above example, we can identify the unused links as-

We have-

- The value of next hop in the final routing table of router A suggests that only edges AB and AD are used.
- The value of next hop in the final routing table of router B suggests that only edges BA and BC are used.
- The value of next hop in the final routing table of router C suggests that only edge CB is used.
- The value of next hop in the final routing table of router D suggests that only edge DA is used.

Thus, edges BD and CD are never used.

Important Notes-

Note-01:

In Distance Vector Routing,

- Only distance vectors are exchanged.
- “Next hop”values are not exchanged.
- This is because it results in exchanging the large amount of data which consumes more bandwidth.

Note-02:

While preparing a new routing table-

- A router takes into consideration only the distance vectors it has obtained from its neighboring routers.
- It does not take into consideration its old routing table.

Note-03:

The algorithm is called so because-

- It involves exchanging of distance vectors between the routers.
- Distance vector is nothing but an array of distances.

Note-04:

- The algorithm keeps on repeating periodically and never stops.
- This is to update the shortest path in case any link goes down or topology changes.

Note-05:

- Routing tables are prepared total (n-1) times if there are n routers in the given network.
- This is because shortest path between any 2 nodes contains at most n-1 edges if there are n nodes in the graph.

Note-06:

- Distance Vector Routing suffers from count to infinity problem.
- Distance Vector Routing uses UDP at transport layer.

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.

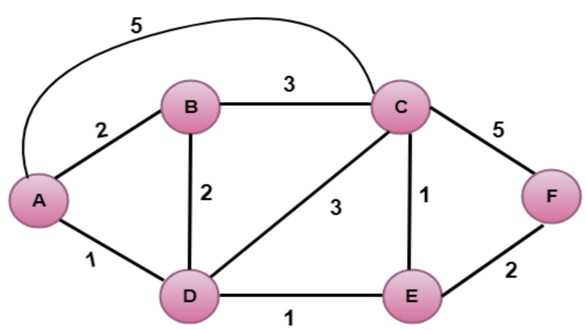
- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are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

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

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(B) = 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.</p>

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(∞, 1+1)
4.   = min(∞, 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+ ∞)
4. = min(2, ∞)
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(∞ , 2+2)
4. = min(∞ ,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, ∞)
4. = min(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
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-leave field

RIP PROTOCOL:

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

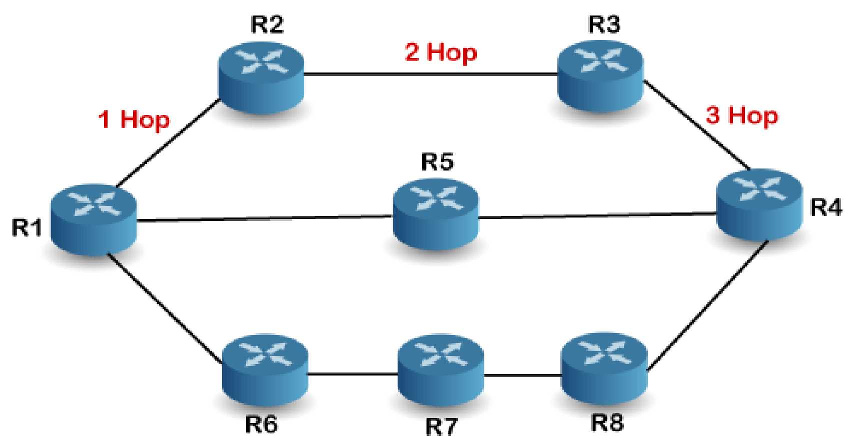
Before understanding the structure of the packet, we first look at the following points:

- RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
- In a routing table, the first column is the destination, or we can say that it is a network address.
- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.

- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- The next column contains the address of the router to which the packet is to be sent to reach the destination.

How is hop count determined?

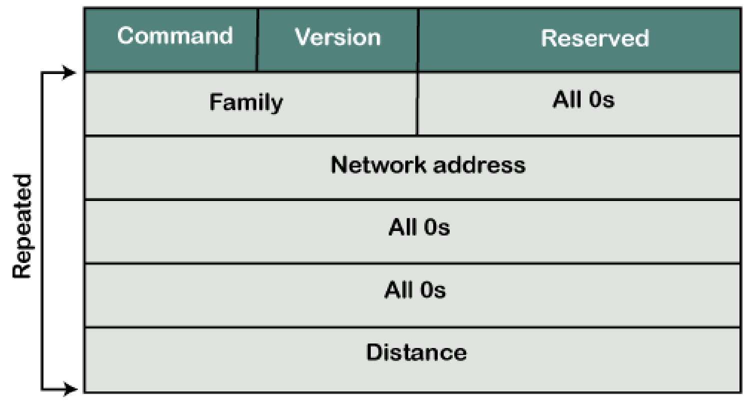
When the router sends the packet to the network segment, then it is counted as a single hop.



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

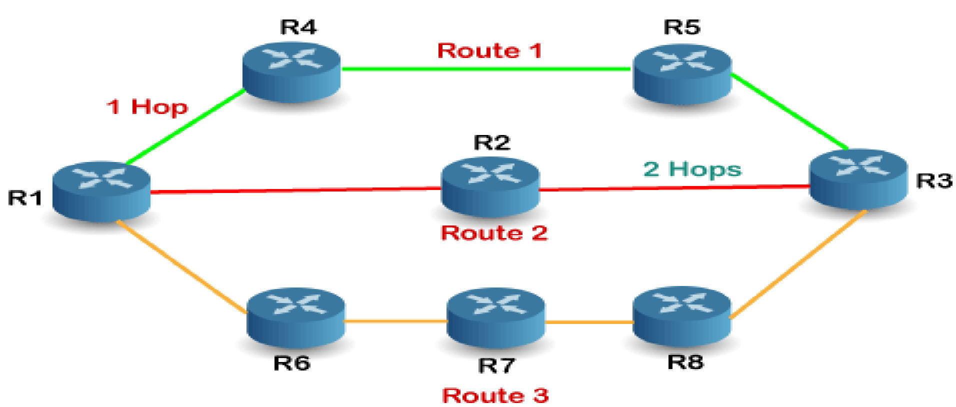
RIP Message Format

Now, we look at the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message:



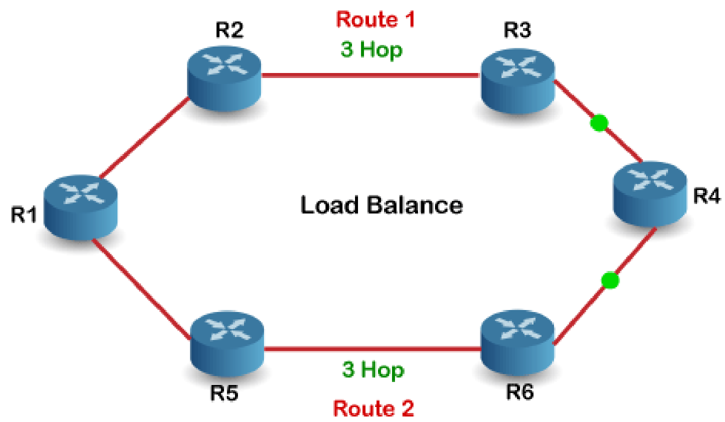
- Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.
- Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.
- Reserved: This is a reserved field, so it is filled with zeroes.
- Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
- Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
- Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

How does the RIP work?



If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

Let's look at another example.

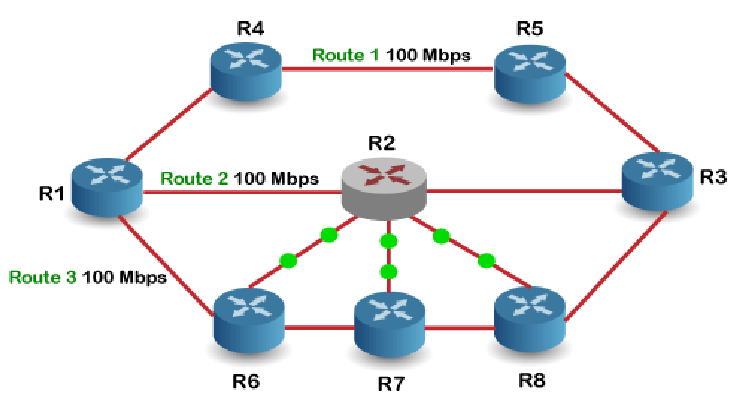


Suppose R1 wants to send the data to R4. There are two possible routes to send data from r1 to r2. As both the routes contain the same number of hops, i.e., 3, so RIP will send the data to both the routes simultaneously. This way, it manages the load balancing, and data reach the destination a bit faster.

Disadvantages of RIP

The following are the disadvantages of RIP:

- In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen. Let's understand this scenario through an example.



We can observe that Route 2 is chosen in the above figure as it has the least hop count. The Route 1 is free and data can be reached more faster; instead of this, data is sent to the Route 2 that makes the Route 2 slower due to the heavy traffic. This is one of the biggest disadvantages of RIP.

- The RIP is a classful routing protocol, so it does not support the VLSM (Variable Length Subnet Mask). The classful routing protocol is a protocol that does not include the subnet mask information in the routing updates.
- It broadcasts the routing updates to the entire network that creates a lot of traffic. In RIP, the routing table updates every 30 seconds. Whenever the updates occur, it sends the copy of the update to all the neighbors except the one that has caused the update. The sending of updates to all the neighbors creates a lot of traffic. This rule is known as a split-horizon rule.
- It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence.
- RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP
- The Administrative distance value is 120 (Ad value). If the Ad value is less, then the protocol is more reliable than the protocol with more Ad value.
- The RIP protocol has the highest Ad value, so it is not as reliable as the other routing protocols.

HOW RIP UPDATES ITS ROUTING TABLE?

The following timers are used to update the routing table:

- **RIP update timer : 30 sec**

The routers configured with RIP send their updates to all the neighboring routers every 30 seconds.

- **RIP Invalid timer : 180 sec**

The RIP invalid timer is 180 seconds, which means that if the router is disconnected from the network or some link goes down, then the neighbor router will wait for 180 seconds to take the update. If it does not receive the update within 180 seconds, then it will mark the particular route as not reachable.

- **RIP Flush timer : 240 sec**

The RIP flush timer is 240 second which is almost equal to 4 min means that if the router does not receive the update within 240 seconds then the neighbor route will remove that particular route from the routing table which is a very slow process as 4 minutes is a long time to wait.

Advantages of RIP

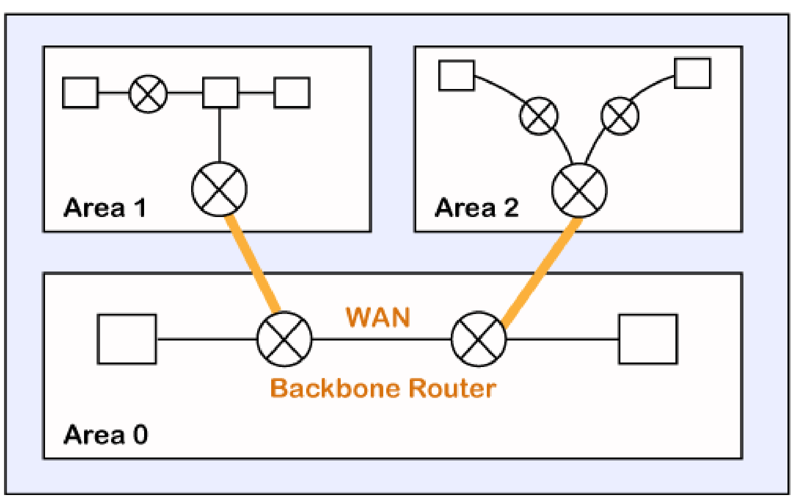
The following are the advantages of a RIP protocol:

- It is easy to configure
- It has less complexity
- The CPU utilization is less.

OSPF PROTOCOL:

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

OSPF Areas



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

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

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

All the areas inside an autonomous system are connected to the backbone routers, and these backbone routers are part of a primary area. The role of a primary area is to provide communication between different areas.

HOW DOES OSPF WORK?

There are three steps that can explain the working of OSPF:

Step 1: The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.

Step 2: The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.

Step 3: The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

How a router forms a neighbor relationship?

The first thing is happened before the relationship is formed is that each router chooses the router ID.

Router ID (RID): The router ID is a number that uniquely identifies each router on a network. The router ID is in the format of the IPv4 address. There are few ways to set the router ID, the first way is to set the router ID manually and the other way is to let the router decides itself.

The following is the logic that the router chooses to set the router ID:

- Manually assigned: The router checks whether the router ID is manually set or not. If it manually set, then it is a router ID. If it is not manually set, then it will choose the highest 'up' status loopback interface IP address. If there are no loopback interfaces, then it will choose the highest 'up' status non-loopback interface IP address.

Two routers connected to each other through point to point or multiple routers are connected can communicate with each other through an OSPF protocol. The two routers are adjacent only when both the routers send the HELLO packet to each other. When both the routers receive the acknowledgment of the HELLO packet, then they come in a two-way state. As OSPF is a link state routing protocol, so it allows to create the neighbor relationship between the routers. The two routers can be neighbors only when they belong to the same subnet, share the same area id, subnet mask, timers, and authentication. The OSPF relationship is a relationship formed between the routers so that they can know each other. The two routers can be neighbors if atleast one of them is designated router or backup designated router in a network, or connected through a point-to-point link.

Types of links in OSPF

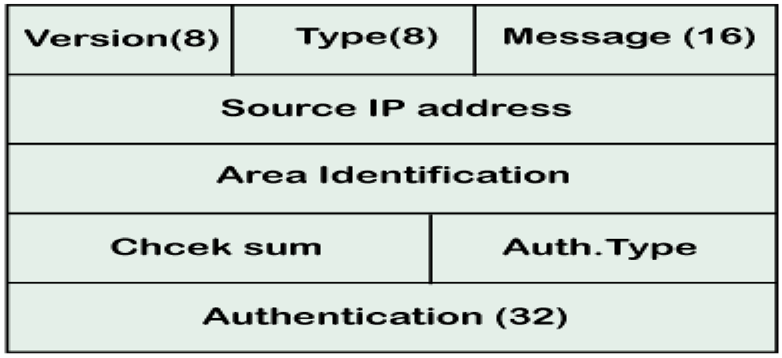
A link is basically a connection, so the connection between two routers is known as a link.

There are four types of links in OSPF:

1. **Point-to-point link:** The point-to-point link directly connects the two routers without any host or router in between.
2. **Transient link:** When several routers are attached in a network, they are known as a transient link.
   The transient link has two different implementations:
   Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.
   Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.
3. **Stub link:** It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.
4. **Virtual link:** If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

OSPF Message Format

The following are the fields in an OSPF message format:



- **Version:** It is an 8-bit field that specifies the OSPF protocol version.
- **Type:** It is an 8-bit field. It specifies the type of the OSPF packet.
- **Message:** It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.
- **Source IP address:** It defines the address from which the packets are sent. It is a sending routing IP address.
- **Area identification:** It defines the area within which the routing takes place.
- **Checksum:** It is used for error correction and error detection.
- **Authentication type:** There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.
- **Authentication:** It is a 32-bit field that contains the actual value of the authentication data.

OSPF Packets

There are five different types of packets in OSPF:

- Hello
- Database Description
- Link state request
- Link state update
- Link state Acknowledgment

Let's discuss each packet in detail.

1. Hello packet

The Hello packet is used to create a neighborhood relationship and check the neighbor's reachability. Therefore, the Hello packet is used when the connection between the routers need to be established.

2. Database Description

After establishing a connection, if the neighbor router is communicating with the system first time, it sends the database information about the network topology to the system so that the system can update or modify accordingly.

3. Link state request

The link-state request is sent by the router to obtain the information of a specified route. Suppose there are two routers, i.e., router 1 and router 2, and router 1 wants to know the information about the router 2, so router 1 sends the link state request to the router 2. When router 2 receives the link state request, then it sends the link-state information to router 1.

4. Link state update

The link-state update is used by the router to advertise the state of its links. If any router wants to broadcast the state of its links, it uses the link-state update.

5. Link state acknowledgment

The link-state acknowledgment makes the routing more reliable by forcing each router to send the acknowledgment on each link state update. For example, router A sends the link state update to the router B and router C, then in return, the router B and C sends the link- state acknowledgment to the router A, so that the router A gets to know that both the routers have received the link-state update.

OSPF States

The device running the OSPF protocol undergoes the following states:

- **Down:** If the device is in a down state, it has not received the HELLO packet. Here, down does not mean that the device is physically down; it means that the OSPF process has not been started yet.
- **Init:** If the device comes in an init state, it means that the device has received the HELLO packet from the other router.
- **2WAY:** If the device is in a 2WAY state, which means that both the routers have received the HELLO packet from the other router, and the connection gets established between the routers.

- **Exstart:** Once the exchange between the routers get started, both the routers move to the Exstart state. In this state, master and slave are selected based on the router's id. The master controls the sequence of numbers, and starts the exchange process.
- **Exchange:** In the exchange state, both the routers send a list of LSAs to each other that contain a database description.
- **Loading:** On the loading state, the LSR, LSU, and LSA are exchanged.
- **Full:** Once the exchange of the LSAs is completed, the routers move to the full state.

Router attributes

Before going to the Extract state, OSPF chooses one router as a Designated router and another router as a backup designated router. These routers are not the type, but they are the attributes of a router. In the case of broadcast networks, the router selects one router as a designated router and another router as a backup designated router. The election of designated and the backup designated router is done to avoid the flooding in a network and to minimize the number of adjacencies. They serve as a central point for exchanging the routing information among all the routers. Since point-to-point links are directly connected, so DR and BDR are not elected.

If DR and BDR are not elected, the router will send the update to all the adjacent neighbors, leading to the flooding in a network. To avoid this problem, DR and BDR are elected. Each non-DR and non-BDR send the update only to the DR and BDR instead of exchanging it with other routers in a network segment. DR then distributes the network topology information to other routers in the same area whereas the BDR serves a substitute for the DR. The BDR also receives the routing information from all the router but it does not distribute the information. It distributes the information only when the DR fails.

The multicast address 224.0.0.6 is used by the non-DR and non-BDR to send the routing information to the DR and BDR. The DR and BDR send the routing information to the multicast address 224.0.0.5.

Based on the following rules, the DR and BDR are elected:

- The router with the highest OSPF priority is chosen as the DR. By default, the highest priority is set as 1.
- If there is no highest priority, then the router with the highest router Id is chosen as the DR, and the router with the second-highest priority is chosen as the BDR.

BORDER GATEWAY PROTOCOL:

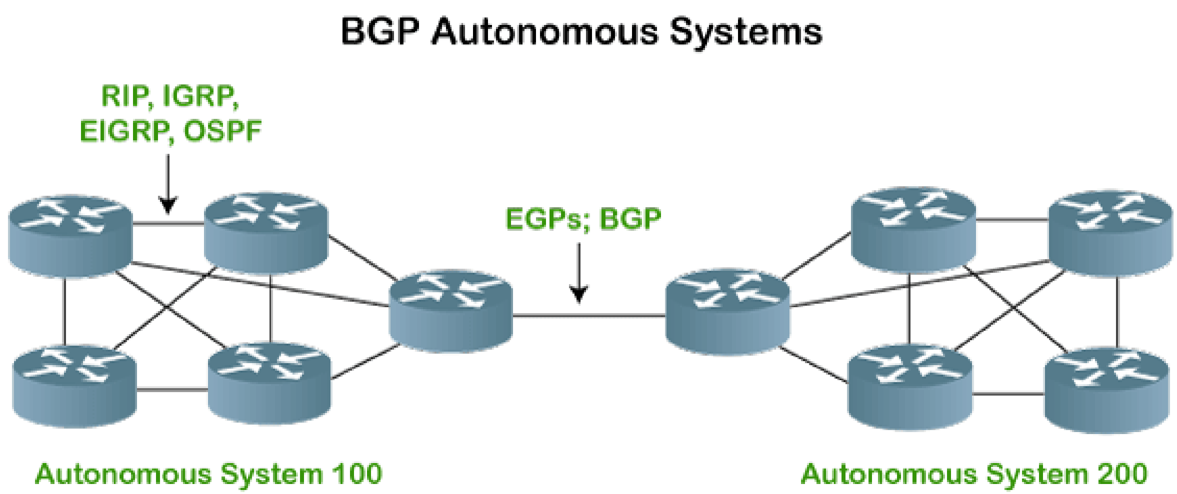
It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

As we know that Border Gateway Protocol works on different autonomous systems, so we should know the history of BGP, types of autonomous systems, etc.

There are many versions of BGP, such as:

- BGP version 1: This version was released in 1989 and is defined in RFC 1105.
- BGP version 2: It was defined in RFC 1163.
- BGP version 3: It was defined in RFC 1267.
- BGP version 4: It is the current version of BGP defined in RFC 1771.

BGP Autonomous Systems



An autonomous system is a collection of networks that comes under the single common administrative domain. Or we can say that it is a collection of routers under the single administrative domain. For example, an organization can contain multiple routers having different locations, but the single autonomous number system will recognize them. Within the same autonomous system or same organization, we generally use IGP (Interior Gateway Protocol) protocols like RIP, IGRP, EIGRP, OSPF. Suppose we want to communicate between two autonomous systems. In that case, we use EGP (Exterior Gateway Protocols). The protocol that is running on the internet or used to communicate between two different autonomous number systems is known as BGP (Border Gateway Protocol). The BGP is the only protocol that is running on the internet backbone or used to exchange the routes between two different autonomous number systems. Internet service providers use the BGP protocol to control all the routing information.

BGP Features

The following are the features of a BGP protocol:

- **Open standard**

It is a standard protocol which can run on any window device.

- **Exterior Gateway Protocol**

It is an exterior gateway protocol that is used to exchange the routing information between two or more autonomous system numbers.

- **InterAS-domain routing**

It is specially designed for inter-domain routing, where interAS-domain routing means exchanging the routing information between two or more autonomous number system.

- **Supports internet**

It is the only protocol that operates on the internet backbone.

- **Classless**

It is a classless protocol.

- **Incremental and trigger updates**

Like IGP, BGP also supports incremental and trigger updates.

- **Path vector protocol**

The BGP is a path vector protocol. Here, path vector is a method of sending the routes along with routing information.

- **Configure neighborhood relationship**

It sends updates to configure the neighborhood relationship manually. Suppose there are two routers R1 and R2. Then, R1 has to send the configure command saying that you are my neighbor. On the other side, R2 also has to send the configure command to R1, saying that R1 is a neighbor of R1. If both the configure commands match, then the neighborhood relationship will get developed between these two routers.

- **Application layer protocol**

It is an application layer protocol and uses TCP protocol for reliability.

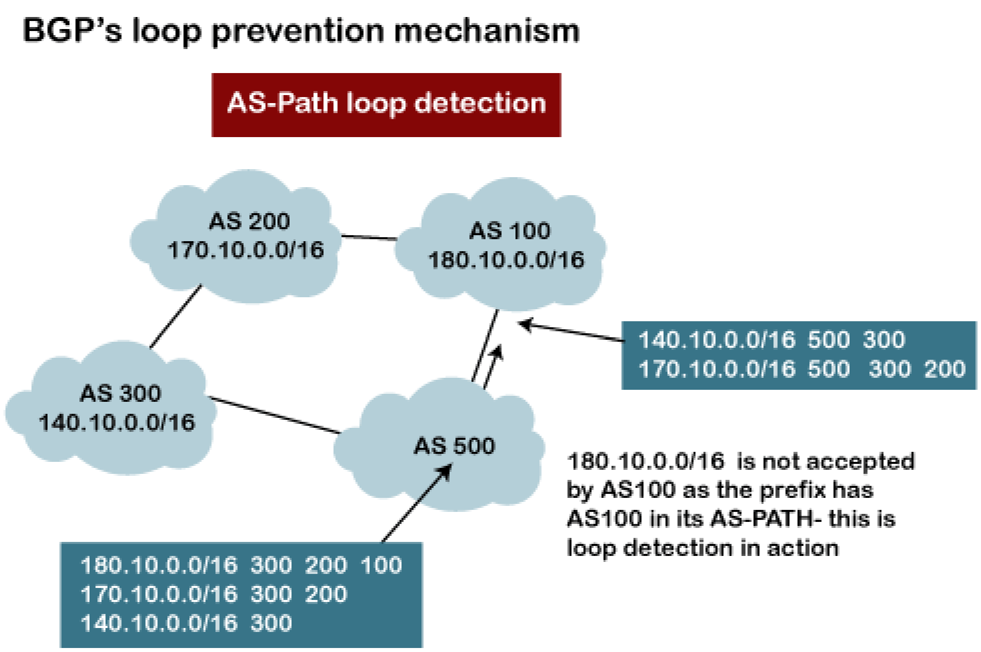
- **Metric**

It has lots of attributes like weight attribute, origin, etc. BGP supports a very rich number of attributes that can affect the path manipulation process.

- **Administrative distance**

If the information is coming from the external autonomous system, then it uses 20 administrative distance. If the information is coming from the same autonomous system, then it uses 200 administrative distance.

BGP's Loop prevention mechanism



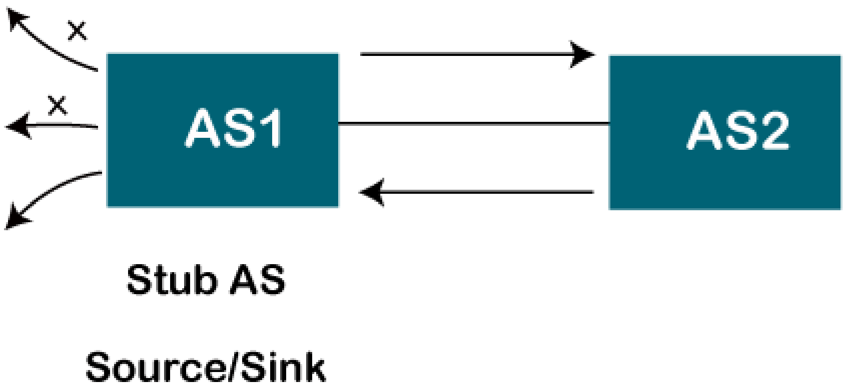
There is a possibility that when you are connecting to the internet, then you may be advertising route 10.0.0.0 to some autonomous system, then it is advertised to some other autonomous system. Then there is a possibility that the same route is coming back again. This creates a loop. But, in BGP, there is a rule that when the router sees its own AS number for example, as shown in the above figure, the network 180.10.0.0/16 is originating from the AS 100, and when it sends to the AS 200, it is going to carry its path information, i.e., 180.10.0.0/16 and AS 100. When AS 200 sends to the AS 300, AS 200 will send its path information 180.10.0.0/16 and AS path is 100 and then 200, which means that the route originates from AS 100, then reaches 200 and finally reaches to 300. When AS 300 sends to the AS 500, it will send the network information 180.10.0.0/16, and

AS path is 100, 200, and then 300. If AS 500 sends to the AS 100, and AS 100 sees its own autonomous number inside the update, it will not accept it. In this way, BGP prevents the loop creation.

Types of Autonomous systems

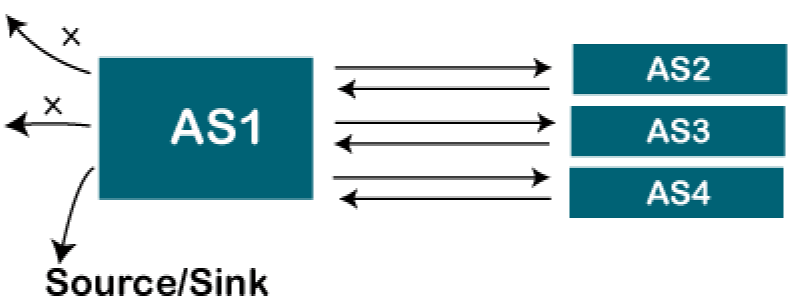
The following are the types of autonomous systems:

- **Stub autonomous system**



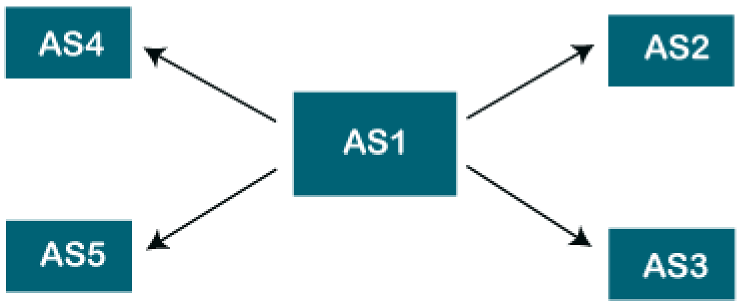
It is a system that contains only one connection from one autonomous system to another autonomous system. The data traffic cannot be passed through the stub autonomous system. The Stub AS can be either a source or a sink. If we have one autonomous system, i.e., AS1, then it will have a single connection to another autonomous system, AS2. The AS1 can act either as a source or a sink. If it acts as a source, then the data moves from AS1 to AS2. If AS1 acts as a sink, means that the data gets consumed in AS1 which is coming from AS2, but the data will not move forward from AS1.

- **Multihomed autonomous system**



It is an autonomous system that can have more than one connection to another autonomous system, but it can still be either a source or a sink for data traffic. There is no transient data traffic flow, which means that the data can be passed from one autonomous system.

- **Transient Autonomous System**

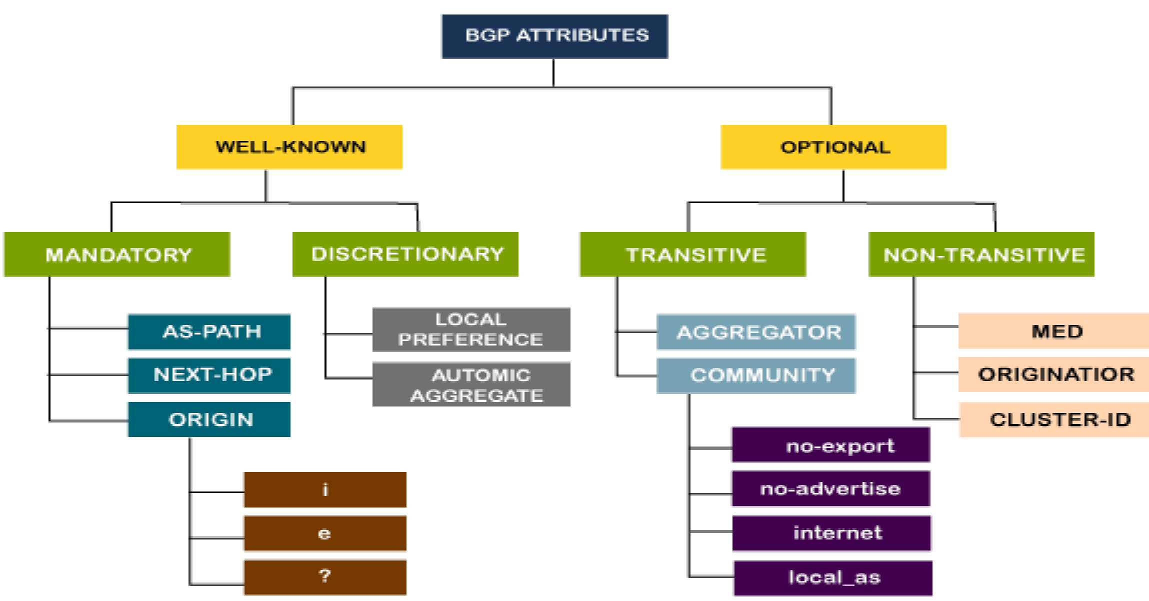


The transient autonomous system is a multihomed autonomous system, but it also provides transient traffic flow.

Path attributes

The BGP chooses the best route based on the attributes of the path.

As we know that path-vector routing is used in the border gateway routing protocol, which contains the routing table that shows the path information. The path attributes provide the path information. The attributes that show or store the path information are known as path attributes. This list of attributes helps the receiving router to make a better decision while applying any policy. Let's see the different types of attributes. The path attribute is broadly classified into two categories:



1. Well-known attribute: It is an attribute that should be recognized by every BGP router.

The well-known attribute is further classified into two categories:

- **Well-known mandatory:** When BGP is going to advertise any network, but it also advertises extra information, and that information with path attributes information. The information includes AS path information, origin information, next-hop information. Here, mandatory means that it has to be present in all the BGP routing updates.
- **Well-known discretionary:** It is recognized by all the BGP routers and passed on to other BGP routers, but it is not mandatory to be present in an update.

2. Optional attribute: It is an attribute that is not necessarily to be recognized by every BGP router. In short, we can say that it is not a mandatory attribute.

The optional attribute is further classified into two categories:

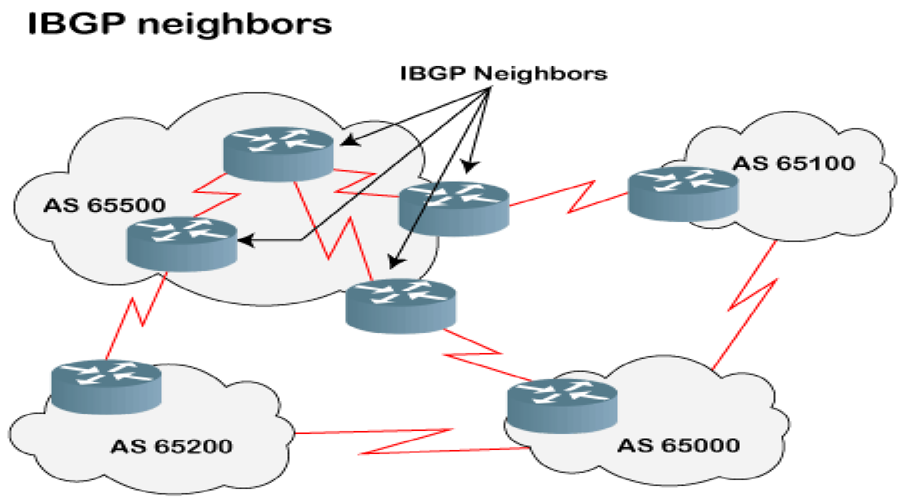
- **Optional transitive:** BGP may or may not recognize this attribute, but it is passed on to the other BGP neighbors. Here, transitive means that if the attribute is not recognized, then it is marked as a partial.
- **Optional non-transitive:** If the BGP cannot recognize the attribute, it ignores the update and does not advertise to another BGP router.

BGP Neighbors

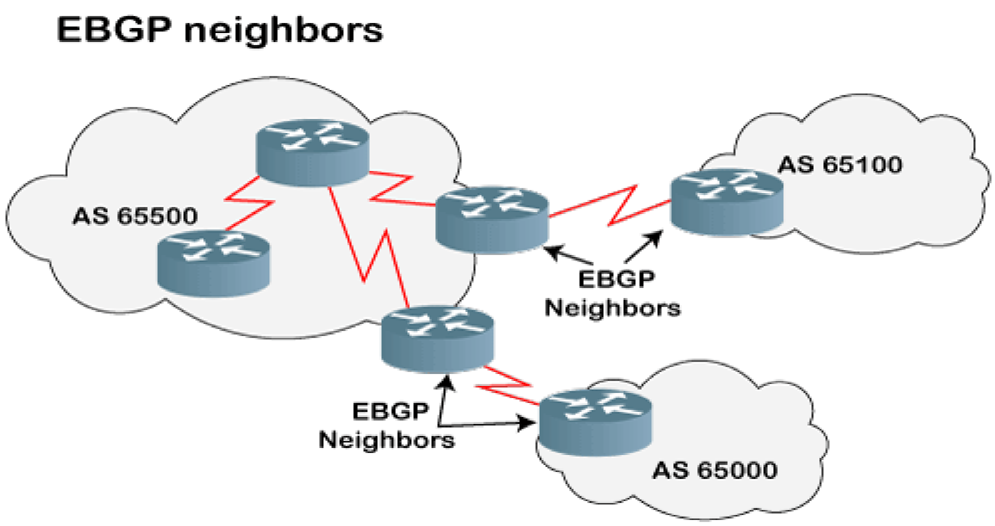
BGP neighborship is similar to the OSPF neighborship, but there are few differences. BGP forms the neighboring relationship with the help of the TCP connection on port number 179 and then exchanges the BGP updates. They exchange the updates after forming the neighbor relationship. In BGP, the neighbor relationship is configured manually. BGP neighbors are also known as BGP peers or BGP speakers.

There are two types of neighbor relationship:

- IBGP (Internal BGP): If all the routers are neighbors of each other and belong to the same autonomous number system, the routers are referred to as an IBGP.



- EBGP (External BGP): If all the routers are neighbors of each other and they belong to the different autonomous number systems, then the routers are referred to as an EBGP.



BGP Tables

There are three types of BGP tables:

- **Neighbor table:** It contains the neighbors who are configured by the administrator manually. The neighbor relationship has to be manually configured by using the neighbor command.

For the verification, the following commands are used:

1. #show ip bgp summary

2. # show ip bgp neighbors

The above commands are very useful to verify whether the neighbor relationship is up or not.

- **BGP forwarding table:** It contains all the routes advertised in BGP and can be verified using the following command:

1. # show ip bgp

- **IP routing table:** The IP routing table contains the best path routes required to reach the destination. The following command shows the best routing path:

1. #SH ip route

BGP Sessions

When we talk about the BGP, which means that the communication between the autonomous systems. Let's consider two autonomous systems having five nodes each.

BGP sessions are classified into two categories:

1. Internal BGP session

The internal BGP session is used to exchange information between the routers inside an autonomous system. In short, we can say that the routing information is exchanged between the routers of the same autonomous system.

2. External BGP session

The external BGP session is a session in which nodes or routers of different autonomous systems communicate with each other.

Types of packets

There are four different types of packets exist in BGP:

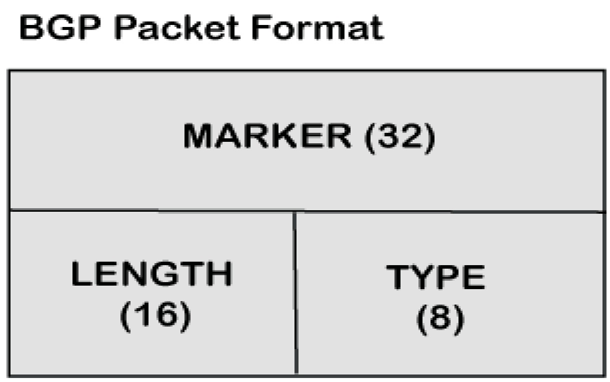
- **Open:** When the router wants to create a neighborhood relation with another router, it sends the Open packet.
- **Update:** The update packet can be used in either of the two cases:

1. It can be used to withdraw the destination, which has been advertised previously.
2. It can also be used to announce the route to the new destination.

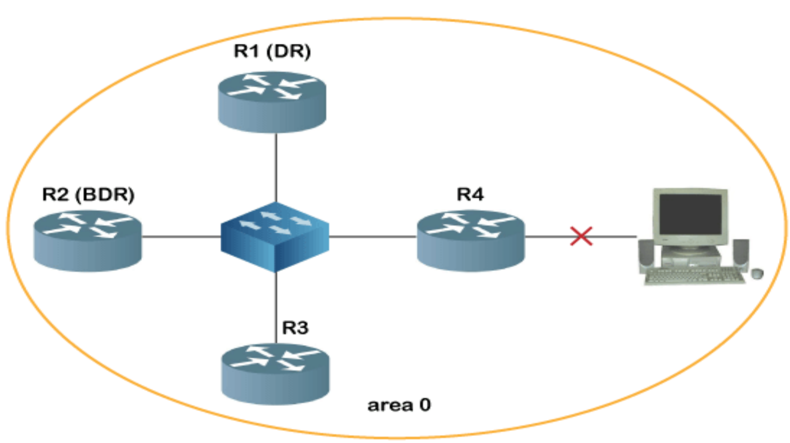
- **Keep Alive:** The keep alive packet is exchanged regularly to tell other routers whether they are alive or not. For example, there are two routers, i.e., R1 and R2. The R1 sends the keep alive packet to R2 while R2 sends the keep alive packet to R1 so that R1 can get to know that R2 is alive, and R2 can get to know that R1 is alive.
- **Notification:** The notification packet is sent when the router detects the error condition or close the connection.

BGP Packet Format

Now we will see the format in which the packet travels. The following are the fields in a BGP packet format:



1. **Marker:** It is a 32-bit field which is used for the authentication purpose.
2. **Length:** It is a 16-bit field that defines the total length of the message, including the header.
3. **Type:** It is an 8-bit field that defines the type of the packet.

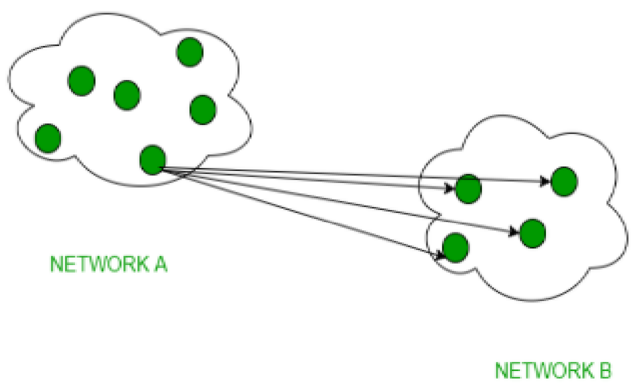


In the above figure, R1 is chosen as the DR, while R2 is chosen as the BDR as R1 has the highest router ID, whereas the R2 has the second-highest router ID. If the link fails between R4 and the system, then R4 updates only R1 and R4 about its link failure. Then, DR updates all the non-DR and non-BDR about the change, and in this case, except R4, only R3 is available as a non-DR and non-BDR.

DIFFERENCE BETWEEN BROADCAST AND MULTICAST

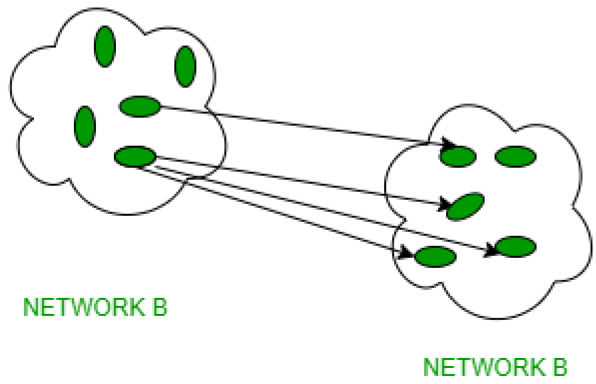
1.Broadcast:

Broadcast transfer (one-to-all) techniques and can be classified into two types : Limited Broadcasting, Direct Broadcasting. In broadcasting mode, transmission happens from one host to all the other hosts connected on the LAN. The devices such as bridge uses this. The protocol like ARP implement this, in order to know MAC address for the corresponding IP address of the host machine. ARP does ip address to mac address translation. RARP does the reverse.



2. Multicasting **:**

Multicasting has one/more senders and one/more recipients participate in data transfer traffic. In multicasting traffic recline between the boundaries of unicast and broadcast. It server's direct single copies of data streams and that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols such as IGMP (Internet Group Management Protocol), Multicast routing for its working. And also in Classful IP addressing Class D is reserved for multicast groups.



Difference between Broadcast and Multicast :

S.No.	Broadcast	Multicast
1.	It has one sender and multiple receivers.	It has one or more senders and multiple receivers.
2.	It sent data from one device to all the other devices in a network.	It sent data from one device to multiple devices.
3.	It works on star and bus topology.	It works on star, mesh, tree and hybrid topology.
4.	It scale well across large networks.	It does not scale well across large networks.
5.	Its bandwidth is wasted.	It utilizes bandwidth efficiently.
6.	It has one-to-all mapping.	It has one-to-many mapping.
7.	Hub is an example of a broadcast device.	Switch is an example of a multicast device.

RIP Protocol

RIP stands for Routing Information Protocol.

RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area.

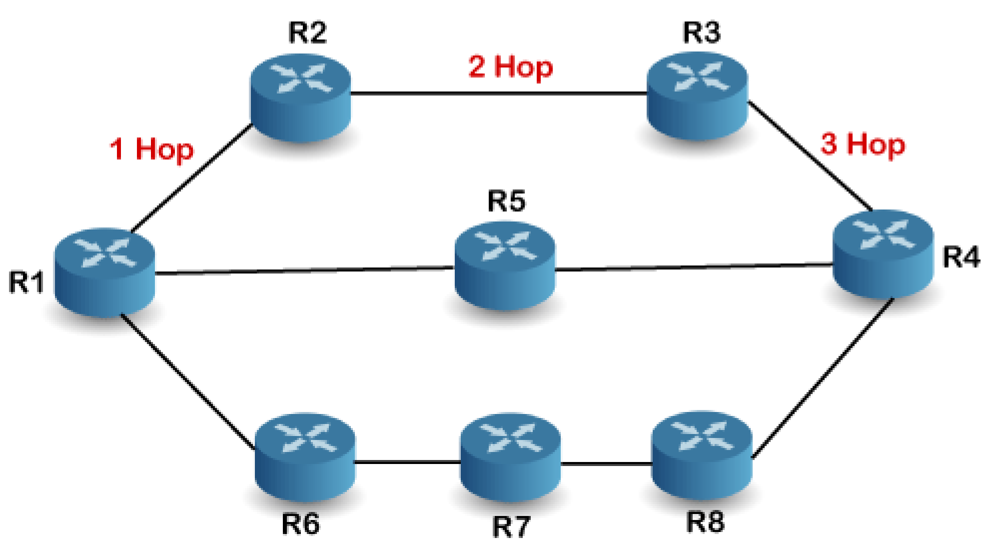
To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

Before understanding the structure of the packet, we first look at the following points:

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

How is hop count determined?

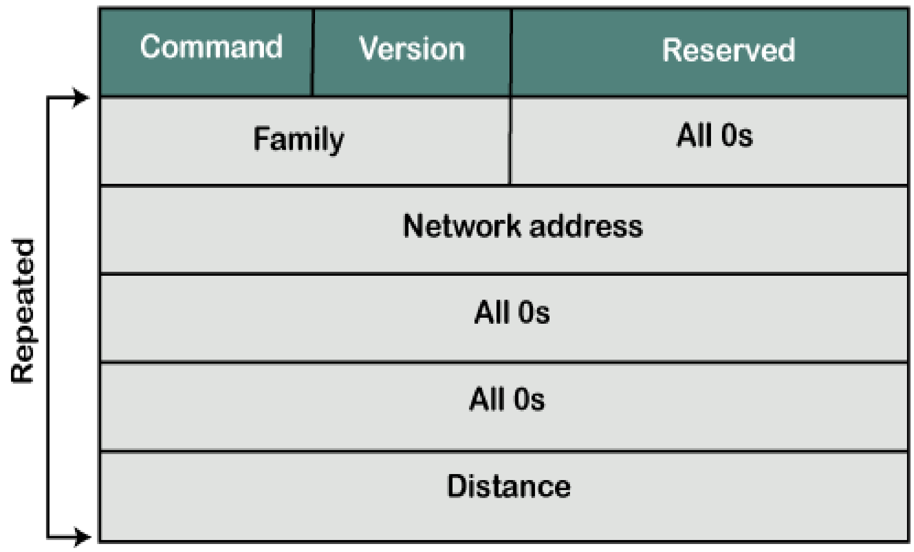
When the router sends the packet to the network segment, then it is counted as a single hop.



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

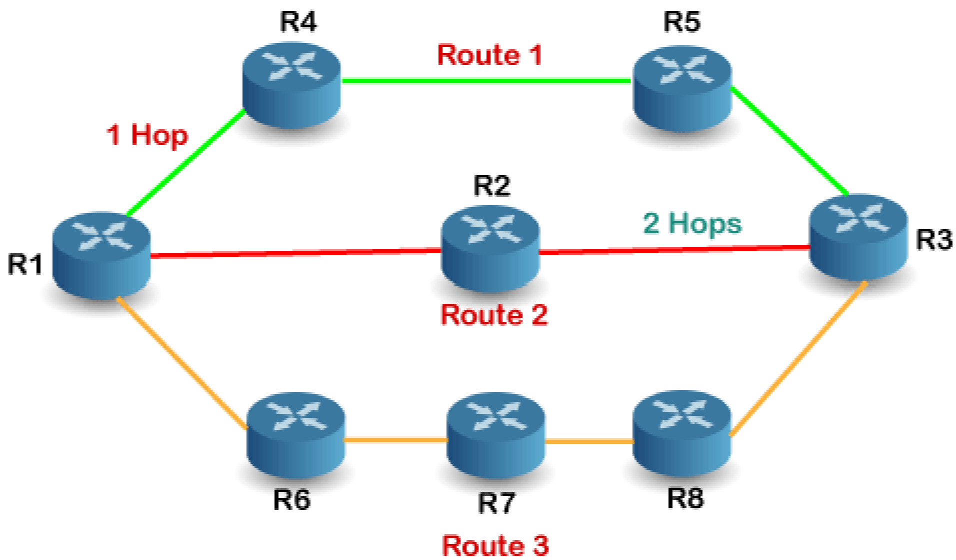
RIP Message Format

Now, we look at the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message:



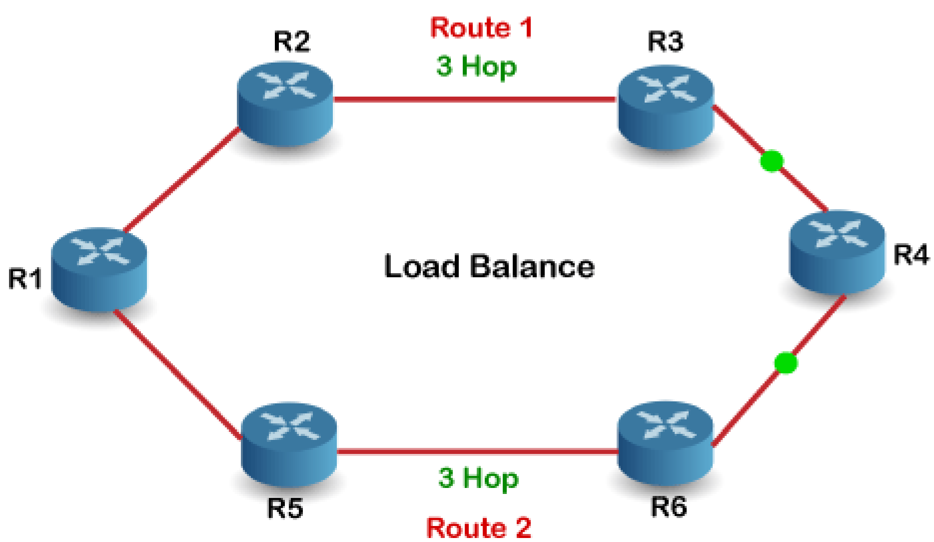
- Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.
- Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.
- Reserved: This is a reserved field, so it is filled with zeroes.
- Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
- Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
- Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

How does the RIP work?



If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

Let's look at another example.

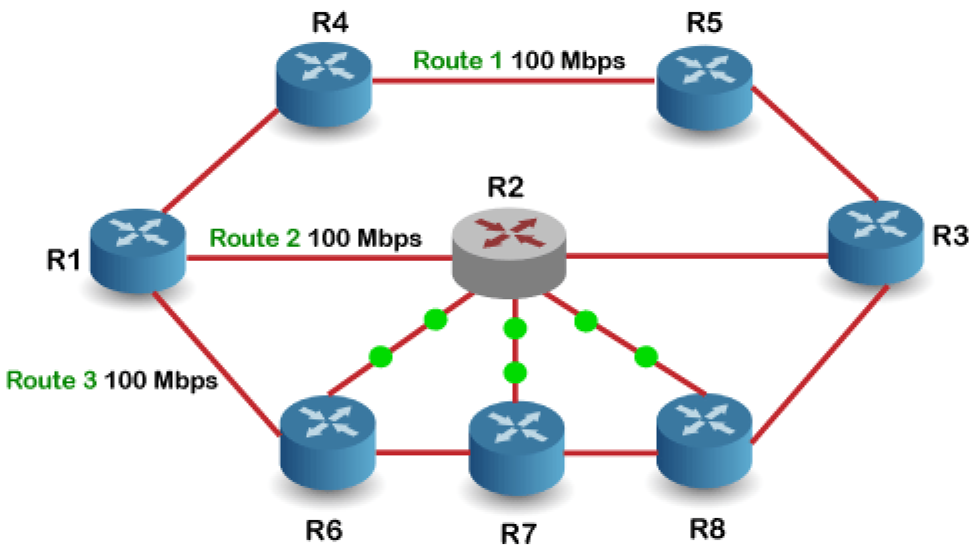


Suppose R1 wants to send the data to R4. There are two possible routes to send data from r1 to r2. As both the routes contain the same number of hops, i.e., 3, so RIP will send the data to both the routes simultaneously. This way, it manages the load balancing, and data reach the destination a bit faster.

Disadvantages of RIP

The following are the disadvantages of RIP:

- In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen. Let's understand this scenario through an example.



We can observe that Route 2 is chosen in the above figure as it has the least hop count. The Route 1 is free and data can be reached more faster; instead of this, data is sent to the Route 2 that makes the Route 2 slower due to the heavy traffic. This is one of the biggest disadvantages of RIP.

- The RIP is a classful routing protocol, so it does not support the VLSM (Variable Length Subnet Mask). The classful routing protocol is a protocol that does not include the subnet mask information in the routing updates.
- It broadcasts the routing updates to the entire network that creates a lot of traffic. In RIP, the routing table updates every 30 seconds. Whenever the updates occur, it sends the copy of the update to all the neighbors except the one that has caused the update. The sending of updates to all the neighbors creates a lot of traffic. This rule is known as a split-horizon rule.
- It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence.

- RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP
- The Administrative distance value is 120 (Ad value). If the Ad value is less, then the protocol is more reliable than the protocol with more Ad value.
- The RIP protocol has the highest Ad value, so it is not as reliable as the other routing protocols.

How RIP updates its Routing table

The following timers are used to update the routing table:

- **RIP update timer : 30 sec**

The routers configured with RIP send their updates to all the neighboring routers every 30 seconds.

- **RIP Invalid timer : 180 sec**

The RIP invalid timer is 180 seconds, which means that if the router is disconnected from the network or some link goes down, then the neighbor router will wait for 180 seconds to take the update. If it does not receive the update within 180 seconds, then it will mark the particular route as not reachable.

- **RIP Flush timer : 240 sec**

The RIP flush timer is 240 second which is almost equal to 4 min means that if the router does not receive the update within 240 seconds then the neighbor route will remove that particular route from the routing table which is a very slow process as 4 minutes is a long time to wait.

Advantages of RIP

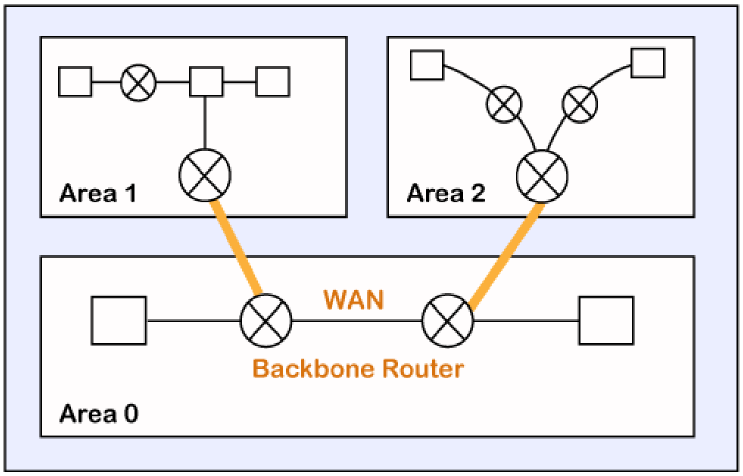
The following are the advantages of a RIP protocol:

- It is easy to configure
- It has less complexity
- The CPU utilization is less.

OSPF Protocol

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

OSPF Areas



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

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

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

All the areas inside an autonomous system are connected to the backbone routers, and these backbone routers are part of a primary area. The role of a primary area is to provide communication between different areas.

How does OSPF work?

There are three steps that can explain the working of OSPF:

Step 1: The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.

Step 2: The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.

Step 3: The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

How a router forms a neighbor relationship?

The first thing is happened before the relationship is formed is that each router chooses the router ID.

Router ID (RID): The router ID is a number that uniquely identifies each router on a network. The router ID is in the format of the IPv4 address. There are few ways to set the router ID, the first way is to set the router ID manually and the other way is to let the router decides itself.

The following is the logic that the router chooses to set the router ID:

- Manually assigned: The router checks whether the router ID is manually set or not. If it manually set, then it is a router ID. If it is not manually set, then it will choose the highest 'up' status loopback interface IP address. If there are no loopback interfaces, then it will choose the highest 'up' status non-loopback interface IP address.

Two routers connected to each other through point to point or multiple routers are connected can communicate with each other through an OSPF protocol. The two routers are adjacent only when both the routers send the HELLO packet to each other. When both the routers receive the acknowledgment of the HELLO packet, then they come in a two-way state. As OSPF is a link state routing protocol, so it allows to create the neighbor relationship between the routers. The two routers can be neighbors only when they belong to the same subnet, share the same area id, subnet mask, timers, and authentication. The OSPF relationship is a relationship formed between the routers so that they can know each other. The two routers can be neighbors if atleast one of them is designated router or backup designated router in a network, or connected through a point-to-point link.

Types of links in OSPF

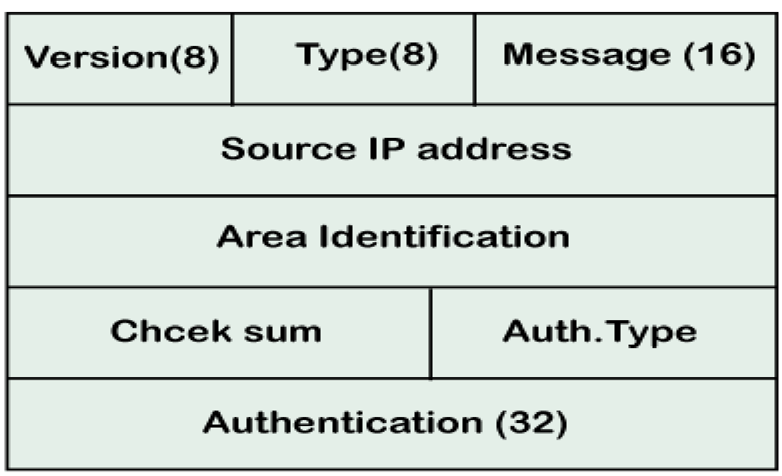
A link is basically a connection, so the connection between two routers is known as a link.

There are four types of links in OSPF:

1. **Point-to-point link:** The point-to-point link directly connects the two routers without any host or router in between.
2. **Transient link:** When several routers are attached in a network, they are known as a transient link.
   The transient link has two different implementations:
   Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.
   Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.
3. **Stub link:** It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.
4. **Virtual link:** If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

OSPF Message Format

The following are the fields in an OSPF message format:



- **Version:** It is an 8-bit field that specifies the OSPF protocol version.
- **Type:** It is an 8-bit field. It specifies the type of the OSPF packet.

- **Message:** It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.
- **Source IP address:** It defines the address from which the packets are sent. It is a sending routing IP address.
- **Area identification:** It defines the area within which the routing takes place.
- **Checksum:** It is used for error correction and error detection.
- **Authentication type:** There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.
- **Authentication:** It is a 32-bit field that contains the actual value of the authentication data.

OSPF Packets

There are five different types of packets in OSPF:

- Hello
- Database Description
- Link state request
- Link state update
- Link state Acknowledgment

Let's discuss each packet in detail.

1. Hello packet

The Hello packet is used to create a neighborhood relationship and check the neighbor's reachability. Therefore, the Hello packet is used when the connection between the routers need to be established.

2. Database Description

After establishing a connection, if the neighbor router is communicating with the system first time, it sends the database information about the network topology to the system so that the system can update or modify accordingly.

3. Link state request

The link-state request is sent by the router to obtain the information of a specified route. Suppose there are two routers, i.e., router 1 and router 2, and router 1 wants to know the information about the router 2, so router 1 sends the link state request to the router 2. When router 2 receives the link state request, then it sends the link-state information to router 1.

4. Link state update

The link-state update is used by the router to advertise the state of its links. If any router wants to broadcast the state of its links, it uses the link-state update.

5. Link state acknowledgment

The link-state acknowledgment makes the routing more reliable by forcing each router to send the acknowledgment on each link state update. For example, router A sends the link state update to the router B and router C, then in return, the router B and C sends the link- state acknowledgment to the router A, so that the router A gets to know that both the routers have received the link-state update.

OSPF States

The device running the OSPF protocol undergoes the following states:

- **Down:** If the device is in a down state, it has not received the HELLO packet. Here, down does not mean that the device is physically down; it means that the OSPF process has not been started yet.
- **Init:** If the device comes in an init state, it means that the device has received the HELLO packet from the other router.
- **2WAY:** If the device is in a 2WAY state, which means that both the routers have received the HELLO packet from the other router, and the connection gets established between the routers.
- **Exstart:** Once the exchange between the routers get started, both the routers move to the Exstart state. In this state, master and slave are selected based on the router's id. The master controls the sequence of numbers, and starts the exchange process.
- **Exchange:** In the exchange state, both the routers send a list of LSAs to each other that contain a database description.
- **Loading:** On the loading state, the LSR, LSU, and LSA are exchanged.
- **Full:** Once the exchange of the LSAs is completed, the routers move to the full state.