Unit-1

Routing Algorithms: Introduction

A routing algorithm is a procedure that lays down the route or path to transfer data packets from source to the destination. They help in directing Internet traffic efficiently. After a data packet leaves its source, it can choose among the many different paths to reach its destination. Routing algorithm mathematically computes the best path, i.e., “least – cost path” that the packet can be routed through.

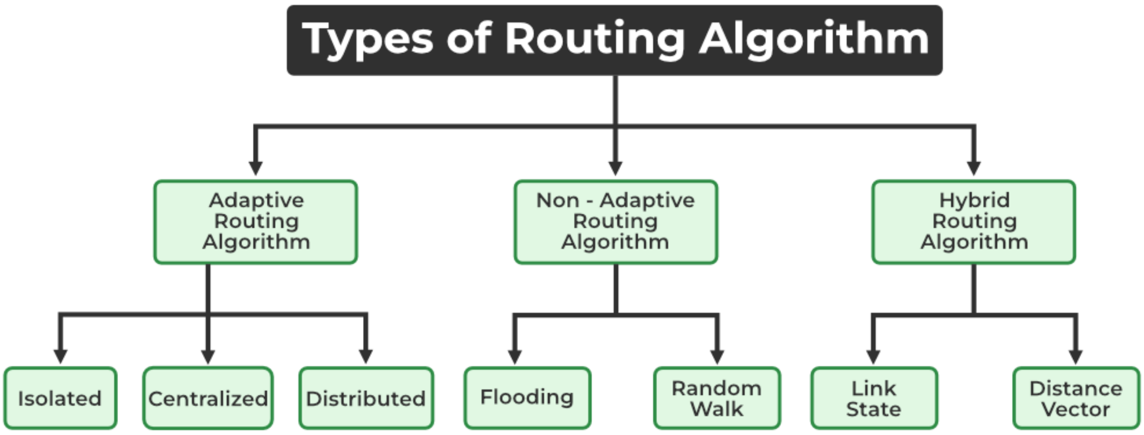
- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.

Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of Routing Algorithms

The routing algorithms can be classified as follows:

1. Adaptive Algorithms
2. Non-Adaptive Algorithms
3. Hybrid Algorithms



Adaptive Routing Algorithms

Adaptive routing algorithms, also known as dynamic routing algorithms, makes routing decisions dynamically depending on the network conditions. It constructs the routing table depending upon the network traffic and topology. They try to compute the optimized route depending upon the hop count, transit time and distance.

These are the algorithms that change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as the traffic of the network. Also known as **dynamic routing**, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops, and estimated transit time.

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 Algorithms

Non-adaptive Routing algorithms, also known as static routing algorithms, construct a static routing table to determine the path through which packets are to be sent. The static routing table is constructed based upon the routing information stored in the routers when the network is booted up.

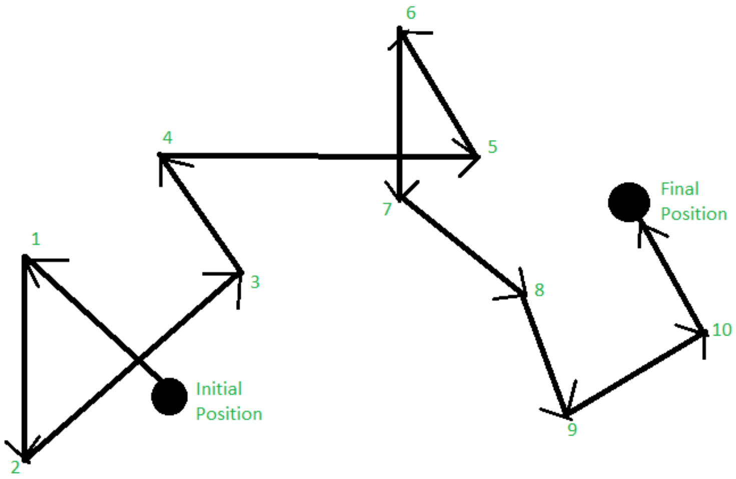
These are the algorithms that do not change their routing decisions once they have been selected. This is also known as **static routing** as a route to be taken is computed in advance and downloaded to routers when a router is booted.

The two types of non – adaptive routing algorithms are −

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.

This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in a loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count, and spanning trees.

Random walk: In this method, packets are sent host by host or node by node to one of its neighbours randomly. This is a highly robust method that is usually implemented by sending packets onto the link which is least queued.



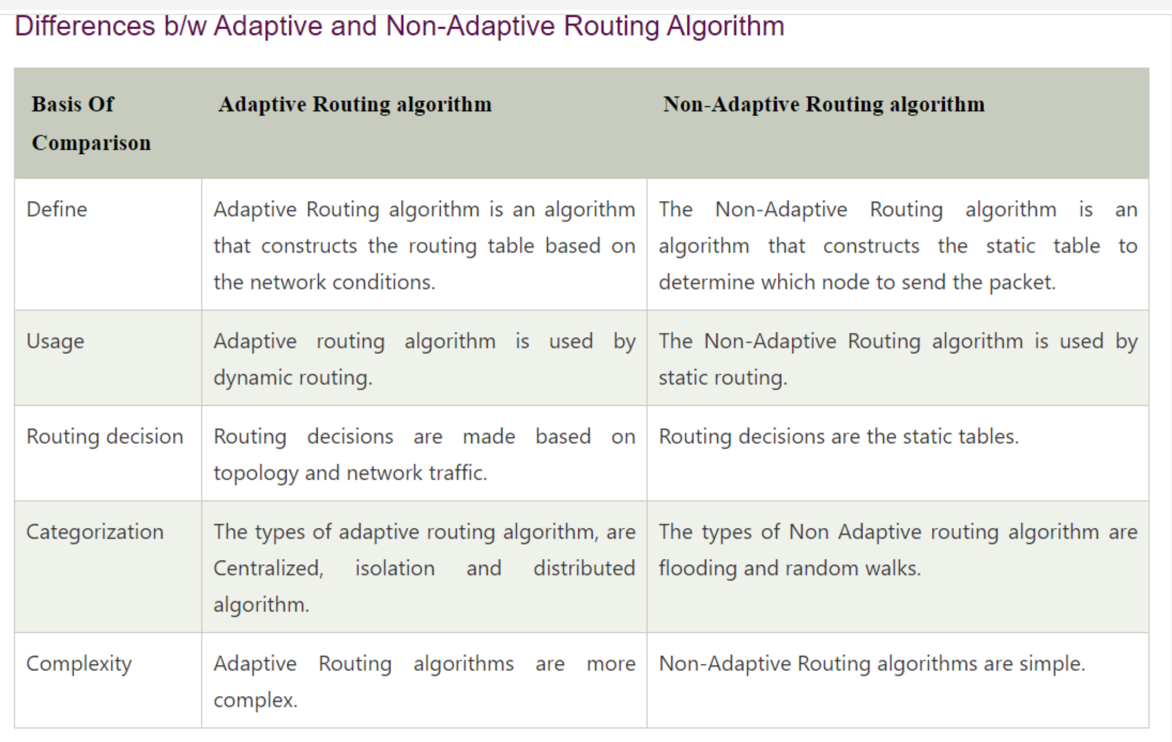
Random Walk

3. Hybrid Algorithms

As the name suggests, these algorithms are a combination of both adaptive and non-adaptive algorithms. In this approach, the network is divided into several regions, and each region uses a different algorithm.
Further, these are classified as follows:

Link-state: In this method, each router creates a detailed and complete map of the network which is then shared with all other routers. This allows for more accurate and efficient routing decisions to be made.

Distance vector: In this method, each router maintains a table that contains information about the distance and direction to every other node in the network. This table is then shared with other routers in the network. The disadvantage of this method is that it may lead to routing loops.



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.

Global vs Decentralized Routing

A **global routing algorithm** computes the least-cost path between a source and destination using complete, global knowledge about the network. That is, the algorithm takes the connectivity between all nodes and all link costs as inputs. This then requires that the algorithm somehow obtain this information before actually performing the calculation. The calculation itself can be run at one site (a centralized global routing algorithm) or replicated at multiple sites. The key distinguishing feature here, however, is that a global algorithm has complete information about connectivity and link costs. In practice, algorithms with global state information are often referred to as **link-state (LS) algorithms**, since the algorithm must be aware of the cost of each link in the network.

In a **decentralized routing algorithm**, the calculation of the least-cost path is carried out in an iterative, distributed manner. No node has complete information about the costs of all network links. Instead, each node begins with only the knowledge of the costs of its own directly attached links. Then, through an iterative process of calculation and exchange of information with its neighbouring nodes (that is, nodes that are at the other end of links to which it itself is attached), a node gradually calculates the least-cost path to a destination or set of destinations. The example is **distance-vector (DV) algorithm**, because each node maintains a vector of estimates of the costs (distances) to all other nodes in the network.

Link-State (LS) algorithm

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 neighbourhood with every other router i.e., the internet work. The three keys to understand the link state routing algorithm.

Knowledge about the neighbourhood: Instead of sending its routing table, a router sends the information about its neighbourhood 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 neighbours. This process is known as flooding. Every router that receives the packet sends the copies to all the neighbours. Finally, each and every router receives a copy of the same information.

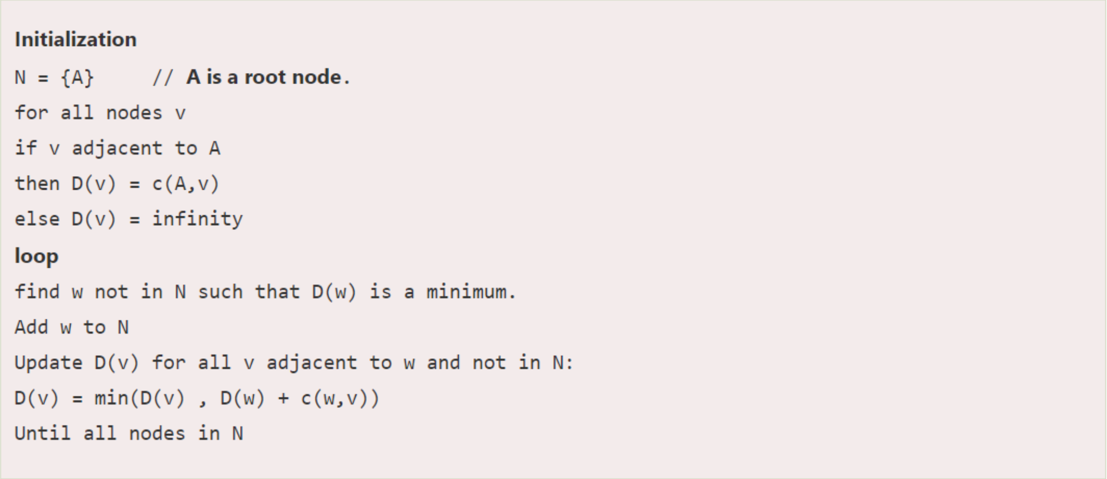
Information Sharing: A router send the information to every other router only when the change occurs in the information.

Link state routing has two phases:

Reliable Flooding: Initial state– Each node knows the cost of its neighbours. 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.

Algorithm



```
Initialization
N = {A}     // A is a root node.
for all nodes v
if v adjacent to A
then D(v) = c(A,v)
else D(v) = infinity
loop
find w not in N such that D(w) is a minimum.
Add w to N
Update D(v) for all v adjacent to w and not in N:
D(v) = min(D(v) , D(w) + c(w,v))
Until all nodes in N
```

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.

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.

Protocols of Link State Routing

- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)

Problems in Link State Routing –

- Heavy traffic due to flooding of packets.
- Flooding can result in infinite looping which can be solved by using the Time to live (TTL) field.

Distance-Vector (DV) algorithm

The Distance-Vector routing algorithm is known by other names. Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm are generally distributed after the researchers create it (Bellman 1957, and Ford and Fulkerson, 1962).

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

The Distance vector algorithm is iterative, asynchronous and distributed.

Distributed: It is distributed in that each node receives information from one or more of its directly attached neighbours, performs calculation and then distributes the result back to its neighbours.

Iterative: It is iterative in that its process continues until no more information is available to be exchanged between neighbours.

Asynchronous: It does not require that all of its nodes operate in the lock step with each other.

- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as Vector.

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

- Knowledge about the whole network: Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbours.
- Routing only to neighbours: The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.
- Information sharing at regular intervals: Within 30 seconds, the router sends the information to the neighbouring routers.

Procedure

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

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

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

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

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

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

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

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

Algorithm

```
At each node x,

Initialization


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

Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing –

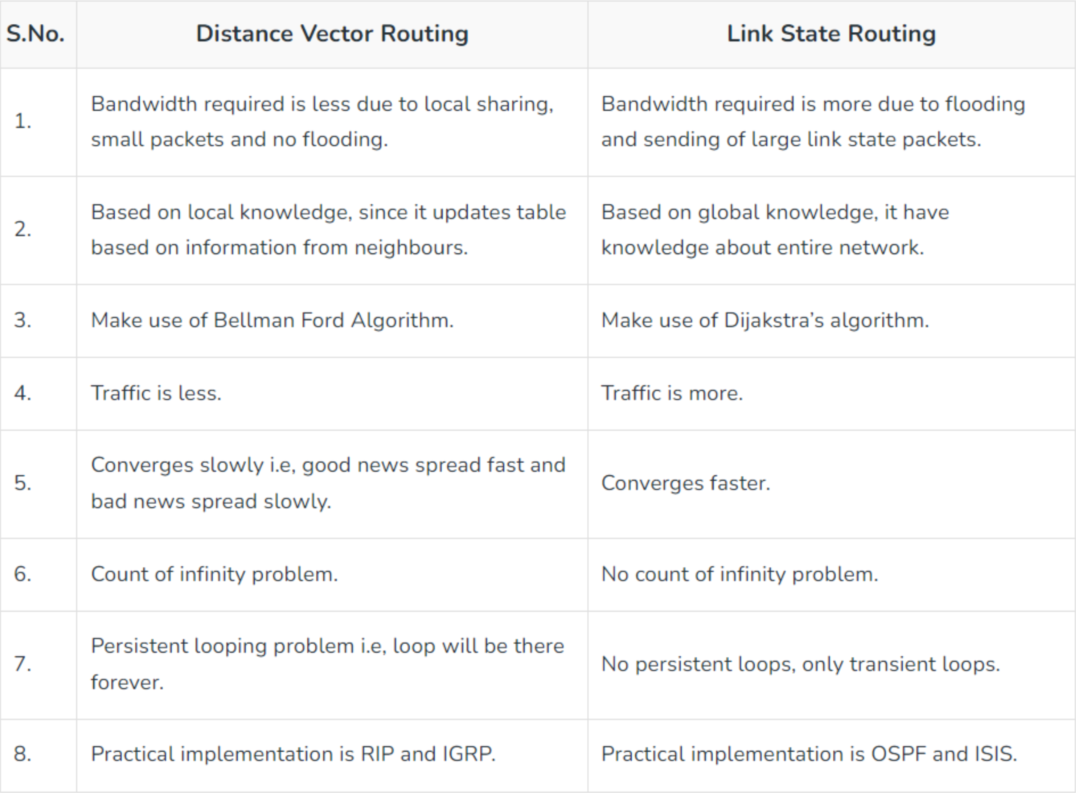
- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Note – Distance Vector routing uses UDP (User datagram protocol) for transportation.

Problems in Distance Vector Routing:

- Count to infinity problem which can be solved by splitting horizon.
- Good news spread fast and bad news spread slowly.
- Persistent looping problem i.e., loop will be there forever.

Difference between Distance vector routing and Link State routing



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

Hierarchical Routing

In hierarchical routing, the routers are divided into regions. Each router has complete details about how to route packets to destinations within its own region. But it does not have any idea about the internal structure of other regions.

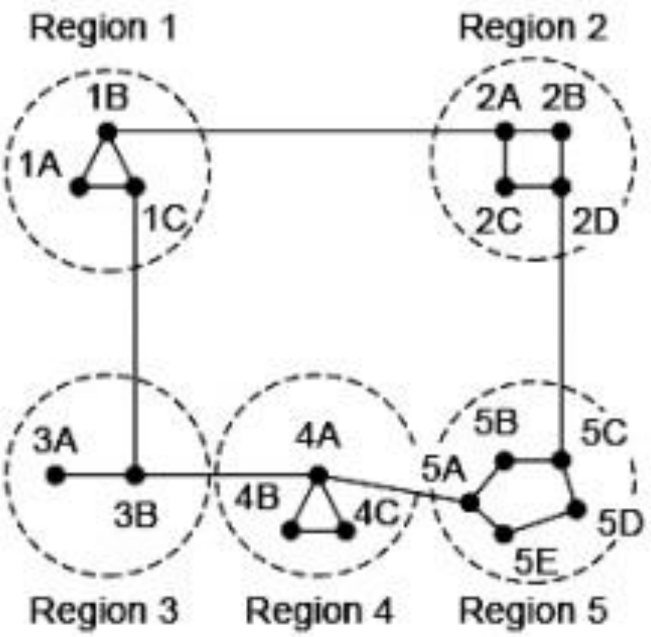
As we know, in both LS and DV algorithms, every router needs to save some information about other routers. When network size is growing, the number of routers in the network will increase. Therefore, the size of routing table increases, then routers cannot handle network traffic as efficiently. To overcome this problem, we are using hierarchical routing.

In hierarchical routing, routers are classified in groups called regions. Each router has information about the routers in its own region and it has no information about routers in other regions. So, routers save one record in their table for every other region.

For huge networks, a two-level hierarchy may be insufficient hence, it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups and so on.

Example

Consider an example of two-level hierarchy with five regions as shown in figure –



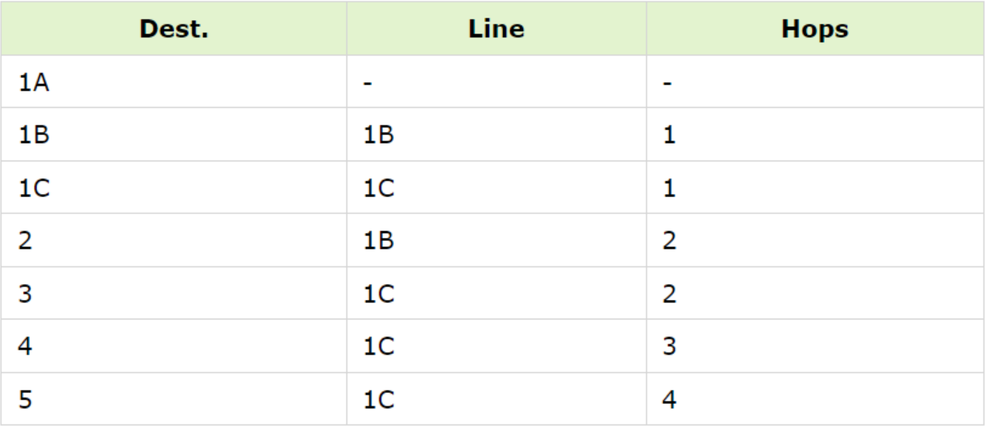
Let see the full routing table for router 1A which has 17 entries, as shown below –

Full Table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

When routing is done hierarchically then there will be only 7 entries as shown below –

Hierarchical Table for 1A



Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Unfortunately, this reduction in table space comes with the increased path length.

Explanation

Step 1 – For example, the best path from 1A to 5C is via region 2, but hierarchical routing of all traffic to region 5 goes via region 3 as it is better for most of the other destinations of region 5.

Step 2 – Consider a subnet of 720 routers. If no hierarchy is used, each router will have 720 entries in its routing table.

Step 3 – Now if the subnet is partitioned into 24 regions of 30 routers each, then each router will require 30 local entries and 23 remote entries for a total of 53 entries.

Routing in the Internet: RIP

RIP is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

Hop Count

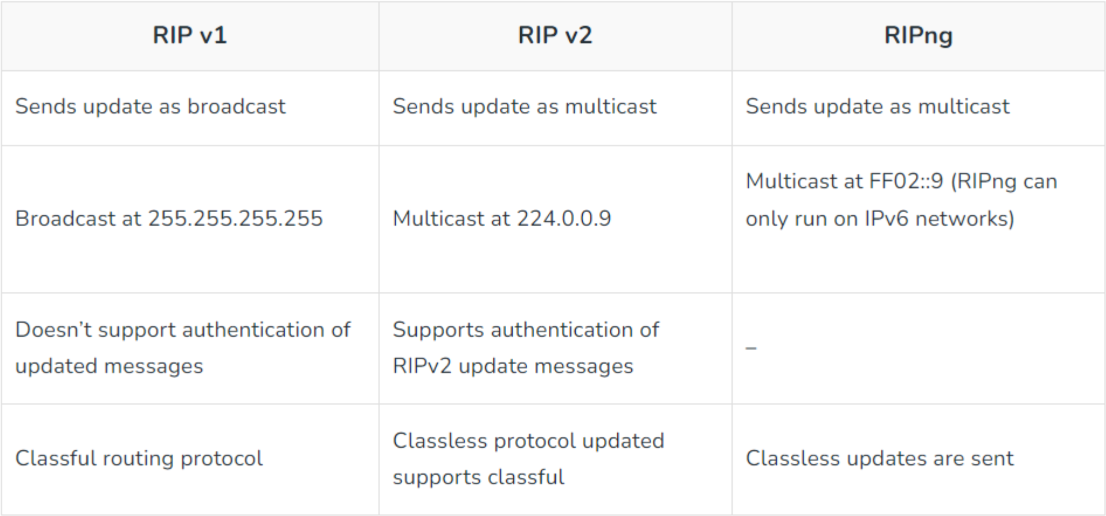
Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Features of RIP

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust routing information received from neighbor routers. This is also known as Routing on rumors.

RIP versions:

There are three versions of routing information protocol – RIP Version1, RIP Version2, and RIPng.

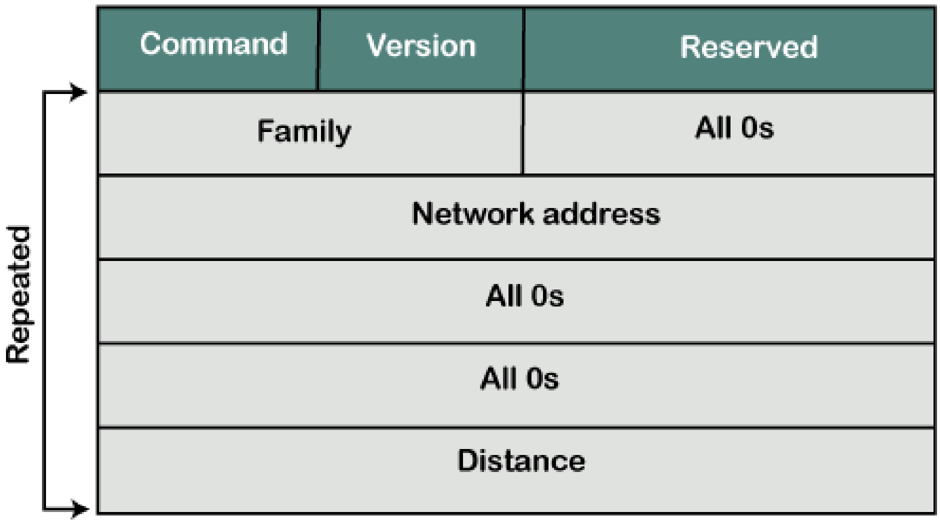


RIP v1	RIP v2	RIPng
Sends update as broadcast	Sends update as multicast	Sends update as multicast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Multicast at FF02::9 (RIPng can only run on IPv6 networks)
Doesn't support authentication of updated messages	Supports authentication of RIPv2 update messages	–
Classful routing protocol	Classless protocol updated supports classful	Classless updates are sent

RIP v1 is known as Classful Routing Protocol because it doesn't send information of subnet mask in its routing update.
RIP v2 is known as Classless Routing Protocol because it sends information of subnet mask in its routing update.

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.

Normal utilization of RIP:

Small to medium-sized networks: RIP is normally utilized in little to medium-sized networks that have moderately basic directing prerequisites. It is not difficult to design and requires little support, which goes with it a famous decision for little organizations.

Legacy organizations: RIP is as yet utilized in some heritage networks that were set up before further developed steering conventions were created. These organizations may not merit the expense and exertion of overhauling, so they keep on involving RIP as their directing convention.

Lab conditions: RIP is much of the time utilized in lab conditions for testing and learning purposes. A basic convention is not difficult to set up, which pursues it a decent decision for instructive purposes.

Backup or repetitive steering: In certain organizations, RIP might be utilized as a reinforcement or excess directing convention, on the off chance that the essential steering convention falls flat or encounters issues. RIP isn't generally so productive as other directing conventions, however, it very well may be helpful as a reinforcement if there should be an occurrence of crisis.

Advantages of RIP :

- Simplicity: RIP is a relatively simple protocol to configure and manage, making it an ideal choice for small to medium-sized networks with limited resources.
- Easy implementation: RIP is easy to implement, as it does not require much technical expertise to set up and maintain.
- Convergence: RIP is known for its fast convergence time, meaning that it can quickly adapt to changes in network topology and route packets efficiently.
- Automatic updates: RIP automatically updates routing tables at regular intervals, ensuring that the most up-to-date information is being used to route packets.
- Low bandwidth overhead: RIP uses a relatively low amount of bandwidth to exchange routing information, making it an ideal choice for networks with limited bandwidth.
- Compatibility: RIP is compatible with many different types of routers and network devices, making it easy to integrate into existing networks.

Disadvantages of RIP :

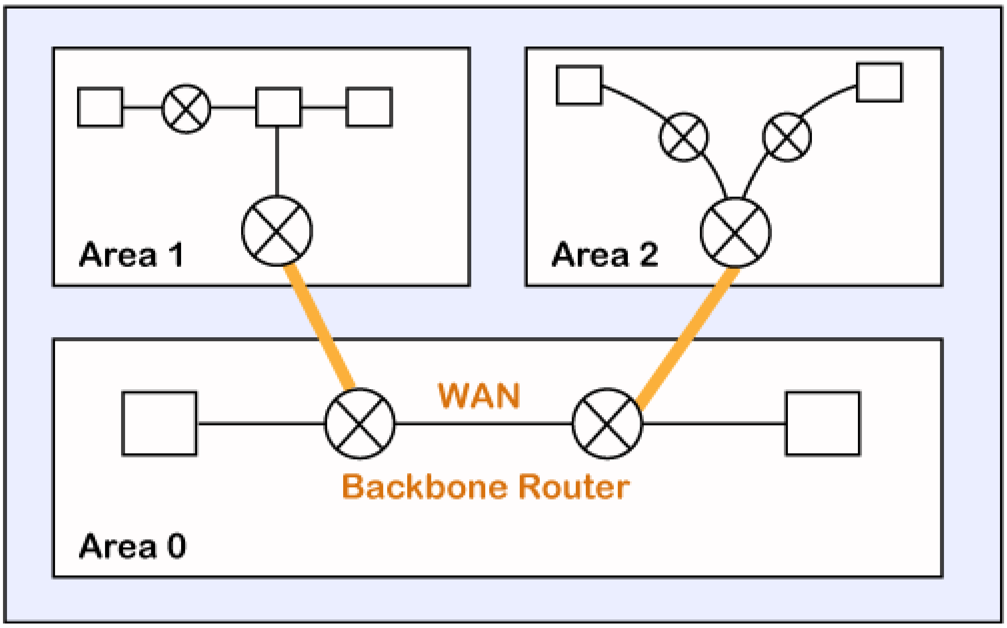
- Limited scalability: RIP has limited scalability, and it may not be the best choice for larger networks with complex topologies. RIP can only support up to 15 hops, which may not be sufficient for larger networks.
- Slow convergence: While RIP is known for its fast convergence time, it can be slower to converge than other routing protocols. This can lead to delays and inefficiencies in network performance.
- Routing loops: RIP can sometimes create routing loops, which can cause network congestion and reduce overall network performance.
- Limited support for load balancing: RIP does not support sophisticated load balancing, which can result in suboptimal routing paths and uneven network traffic distribution.
- Security vulnerabilities: RIP does not provide any native security features, making it vulnerable to attacks such as spoofing and tampering.

- Inefficient use of bandwidth: RIP uses a lot of bandwidth for periodic updates, which can be inefficient in networks with limited bandwidth.

Routing in the Internet: OSPF

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 neighbour 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:

Point-to-point link: The point-to-point link directly connects the two routers without any host or router in between.

Transient link: When several routers are attached in a network, they are known as a transient link. The transient link has two different implementations:

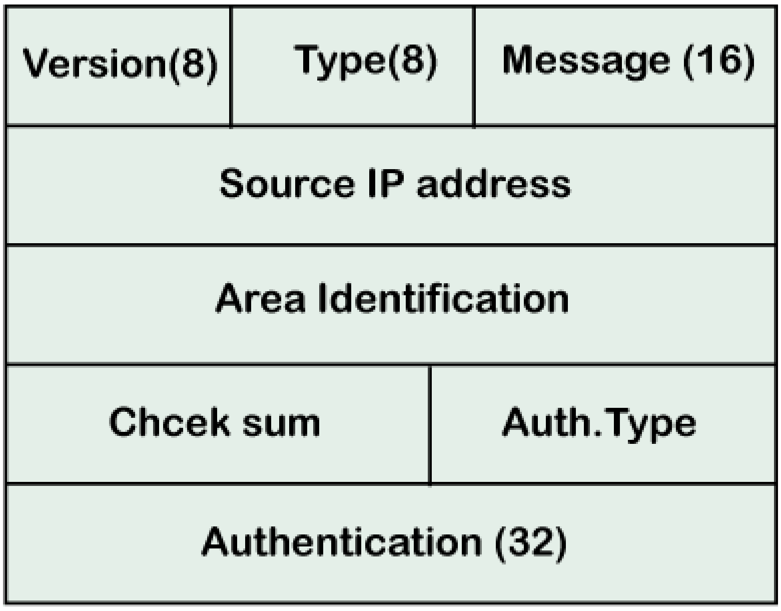
- Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.
- Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.

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.

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:



<table>
<tr><td>Version(8)</td><td>Type(8)</td><td colspan="2">Message (16)</td></tr>
<tr><td colspan="4">Source IP address</td></tr>
<tr><td colspan="4">Area Identification</td></tr>
<tr><td colspan="2">Chcek sum</td><td colspan="2">Auth.Type</td></tr>
<tr><td colspan="4">Authentication (32)</td></tr>
</table>

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:

1. Hello
2. Database Description

3. Link state request
4. Link state update
5. 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.

Routing in the Internet: BGP

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.

History of BGP

The first network was ARPANET, which the department of defense developed, and the Advanced Research Project Agency designed it. In Arpanet, only one network exists, which was handled by the single administrator. All the routers were the part of the single network, and the routing was performed with the help of the GGP (Gateway to Gateway Routing Protocol). The GGP was the first protocol among all the routing protocols. The autonomous system numbers were not used in the GGP protocol.

When the internet came into the market, then GGP started creating the problem. As the internet backbone became large due to which the routing table was also large, which led to the maintenance issue. To resolve this issue, the ARPANET was divided into multiple domains, known as autonomous systems. Each autonomous system can be handled individually, and each system has its own routing policy, and the autonomous system contains the small routing database. When the autonomous system concept was implemented, then the first routing protocol came known as RIP that runs on the single autonomous system. To connect the one autonomous system with another autonomous system, EGP (Exterior Gateway Protocol) protocol was developed. The EGP protocol was launched in 1984, defined in RFC 904. The EGP protocol was used for five years, but it had certain flaws due to which the new protocol known as Border Gateway Protocol (BGP) was developed in 1989, defined in RFC 1105.

There are many versions of BGP, such as:

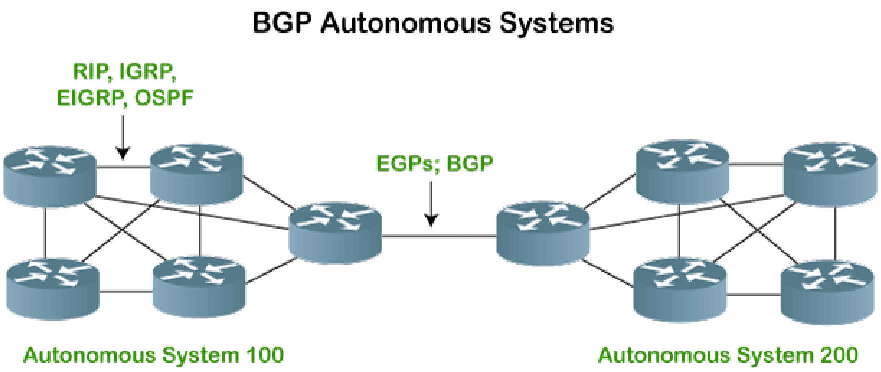
BGP version 1: This version was released in 1989 and is defined in RFC 1105.

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.

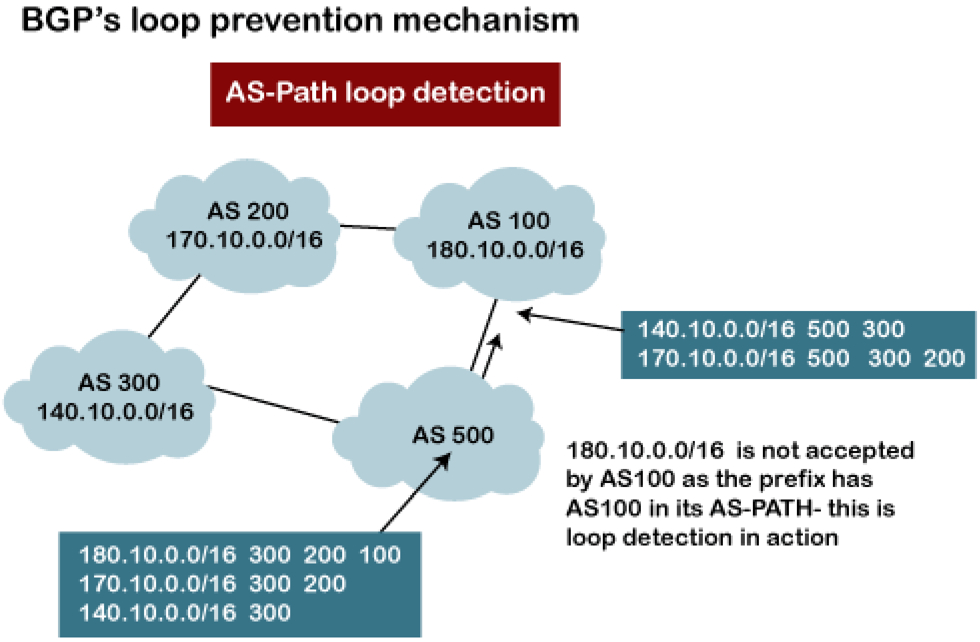
Metric

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

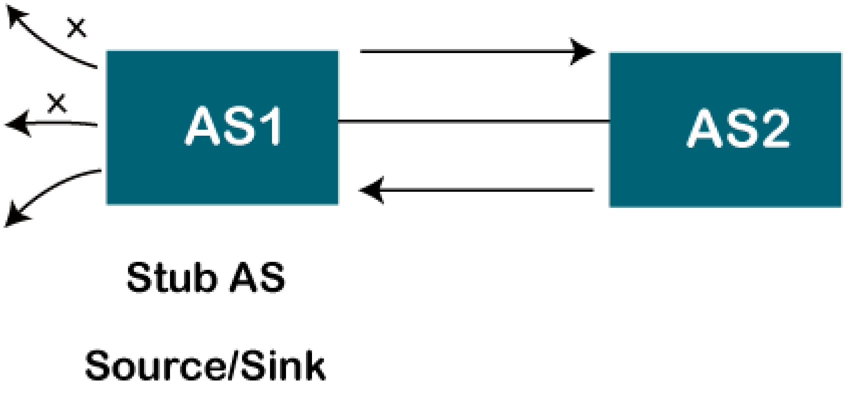


There is a possibility that when you are connecting to the internet, then you may be advertising route 10.0.0.0 to some autonomous system, then it is advertised to some other autonomous system. Then there is a possibility that the same route is coming back again. This creates a loop. But, in BGP, there 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

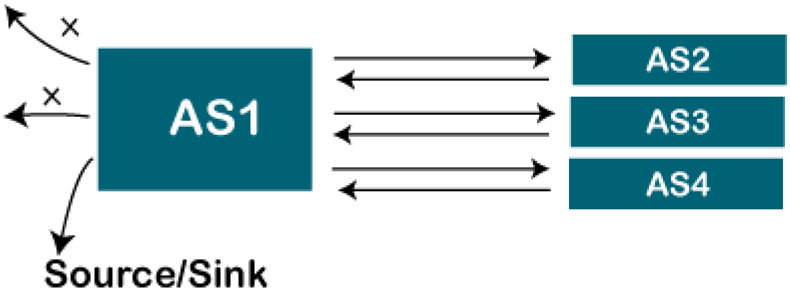
The following are the types of autonomous systems:

Stub autonomous system



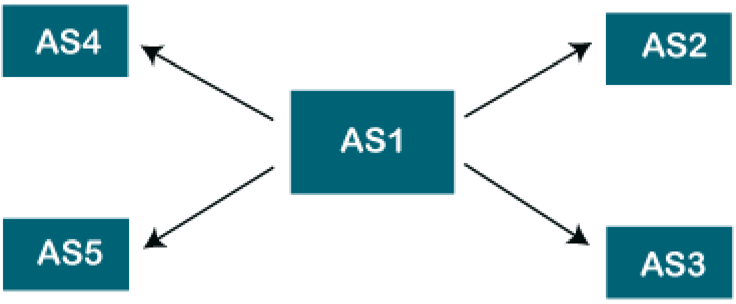
It is a system that contains only one connection from one autonomous system to another autonomous system. The data traffic cannot be passed through the stub autonomous system. The Stub AS can be either a source or a sink. If we have one autonomous system, i.e., AS1, then it will have a single connection 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

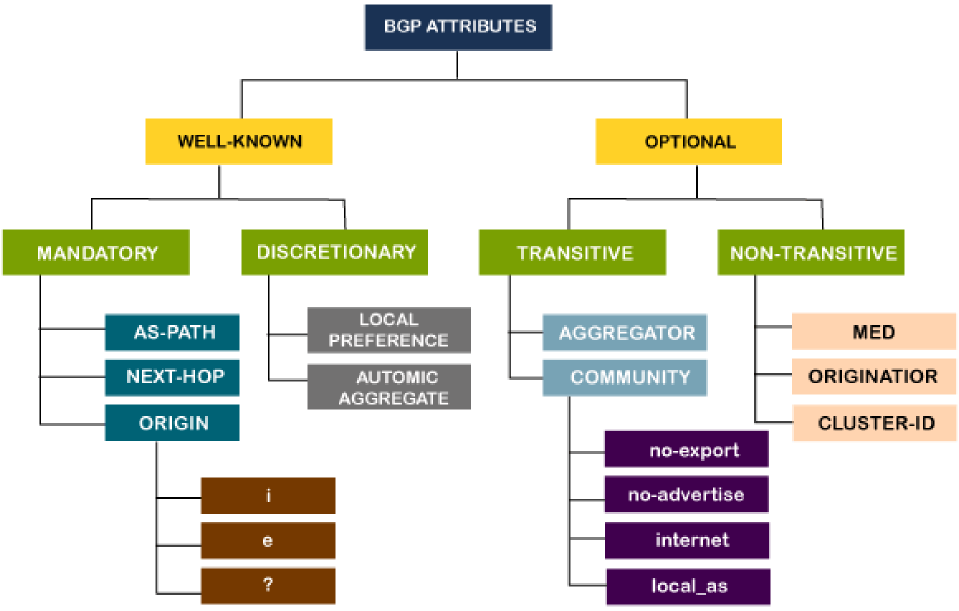


The transient autonomous system is a multihomed autonomous system, but it also provides transient traffic flow.

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 neighbours. 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.

Introduction to Broadcast and Multicast Routing

Broadcast routing

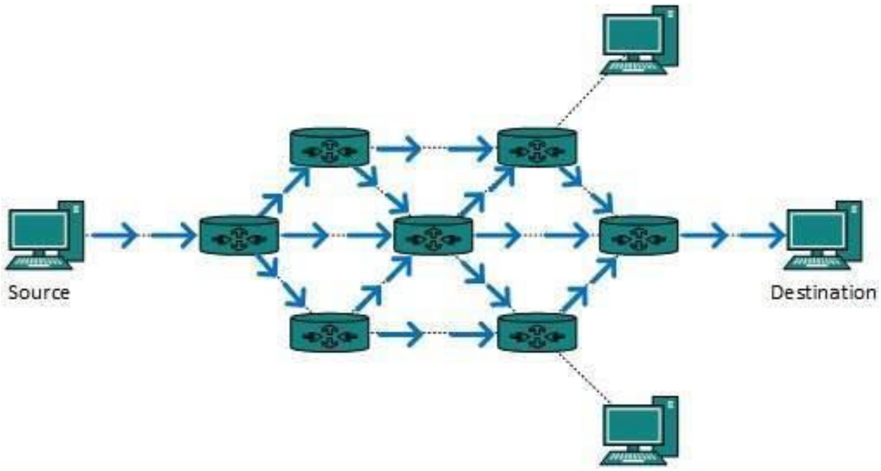
By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.

This method consumes lots of bandwidth and router must destination address of each node.

Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.

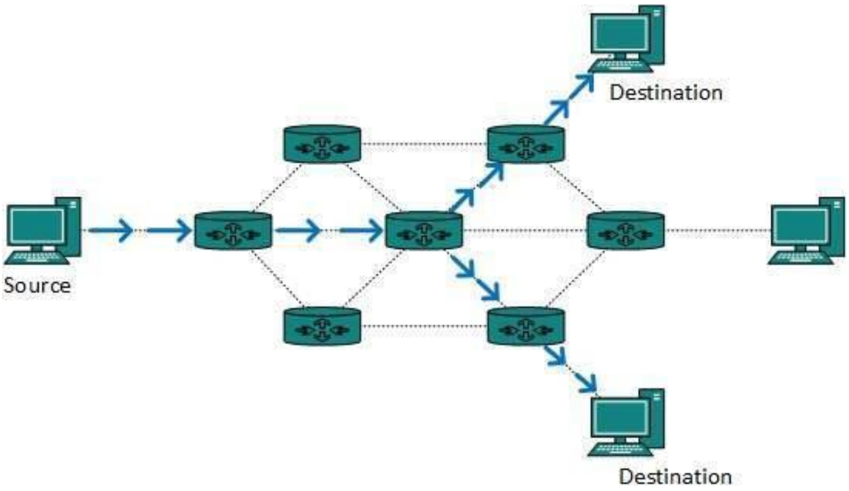


This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.

Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.



The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

Types of Multicast Routing Protocols

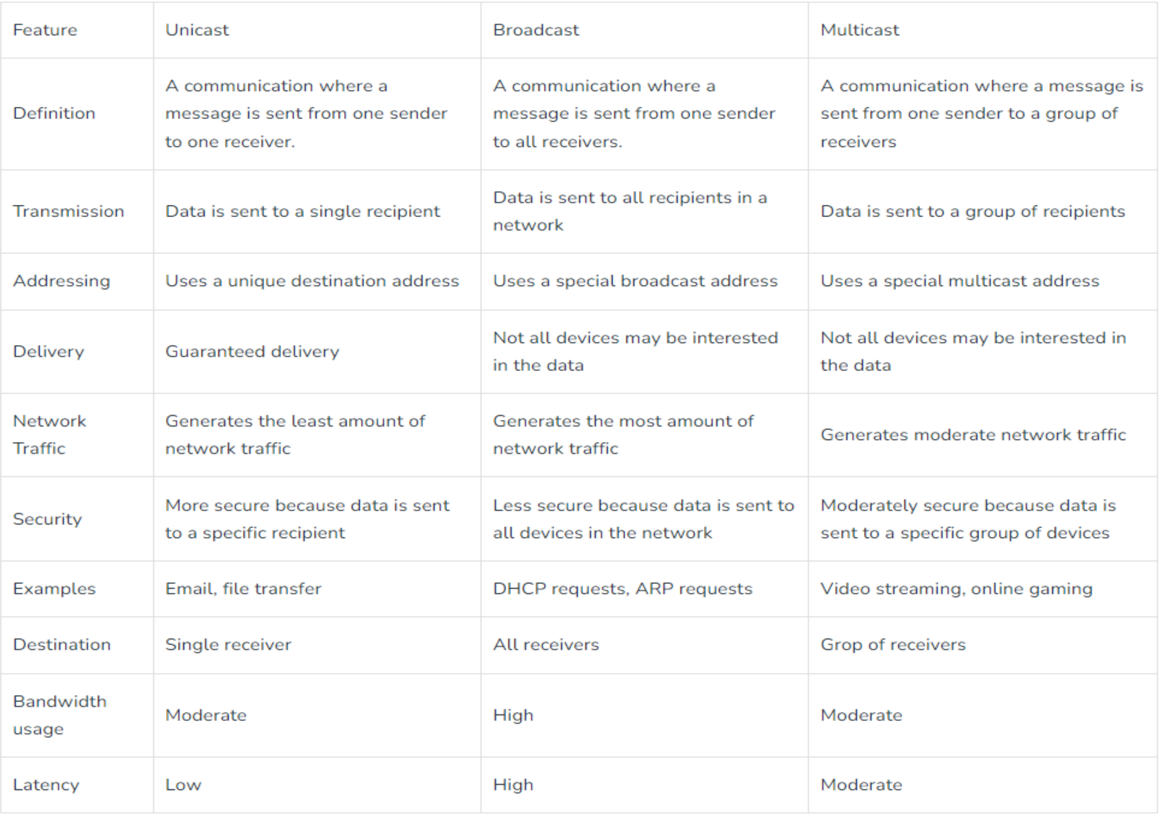
Unicast routing protocols use graphs while Multicast routing protocols use trees, i.e. spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

DVMRP - Distance Vector Multicast Routing Protocol

MOSPF - Multicast Open Shortest Path First

CBT - Core Based Tree

PIM - Protocol independent Multicast



Feature	Unicast	Broadcast	Multicast
Definition	A communication where a message is sent from one sender to one receiver.	A communication where a message is sent from one sender to all receivers.	A communication where a message is sent from one sender to a group of receivers
Transmission	Data is sent to a single recipient	Data is sent to all recipients in a network	Data is sent to a group of recipients
Addressing	Uses a unique destination address	Uses a special broadcast address	Uses a special multicast address
Delivery	Guaranteed delivery	Not all devices may be interested in the data	Not all devices may be interested in the data
Network Traffic	Generates the least amount of network traffic	Generates the most amount of network traffic	Generates moderate network traffic
Security	More secure because data is sent to a specific recipient	Less secure because data is sent to all devices in the network	Moderately secure because data is sent to a specific group of devices
Examples	Email, file transfer	DHCP requests, ARP requests	Video streaming, online gaming
Destination	Single receiver	All receivers	Grop of receivers
Bandwidth usage	Moderate	High	Moderate
Latency	Low	High	Moderate

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

ACADEMIC SESSION: ODD SEMESTER (2023-24)

Assignment No. 1 (Unit-1)

Name of Subject: Computer Networks-II (TCS 703) **Course: B.Tech.**

Branch: CSE **Semester: VII**

Date of Issue: **Date of Submission:**

Instructions:

1. Use A-4 sized blank pages.

2. Submit the hard-copy to the subject-teacher. Create the PDF of the assignment submitted and keep it with you for knowledge.

3. Attempt all questions. Each question carries equal marks.

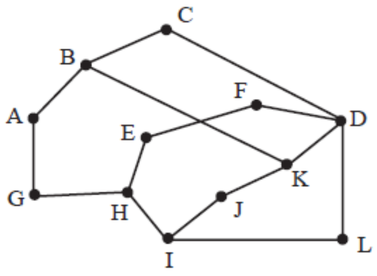
Questions:

1. Discuss the following in brief.

   i) Routing Information Protocol.

   ii) Open Shortest Path First Protocol.

2. What is Multicast Routing? Discuss Multicast Routing Protocols.
3. Discuss the problem of count to infinity associated with Distance Vector Routing Protocol.
4. What is Unicast Routing? Discuss Unicast Routing Protocols.
5. Compute a Multicast Spanning Tree for router C in the following subnet for a group with members at routers A, B, C, D, E, F, I and K.


C
B
F
A
E
D
K
G
J
H
L
I