Unit-3 : Unicast Routing

❖ Introduction – Routing :

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes.The software based routers have limited functionality and limited scope.

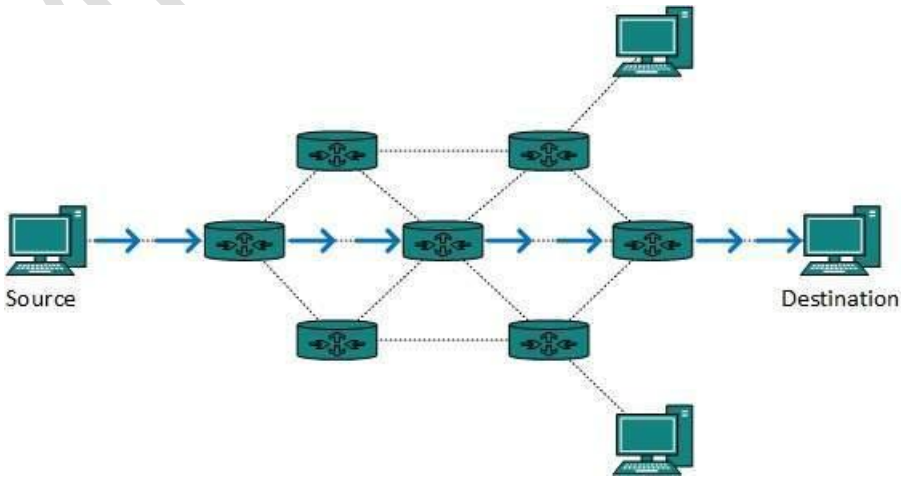
A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

- Hop Count
- Bandwidth
- Metric
- Prefix-length
- Delay

Routes can be statically configured or dynamically learnt. One route can be configured to be preferred over others.

Unicast routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.



❖ Intra- and Inter-domain Routing

An internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems. An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as intra domain routing. Routing between autonomous systems is referred to as inter domain routing.

Several intradomain and interdomain routing protocols are in use.

Two intradomain routing protocols: **Distance vector and link state**.

One interdomain routing protocol: **path vector**.

Routing Information Protocol (RIP) is an implementation of the distance vector protocol. Open Shortest Path First (OSPF) is an implementation of the link state protocol. Border Gateway Protocol (BGP) is an implementation of the path vector protocol.

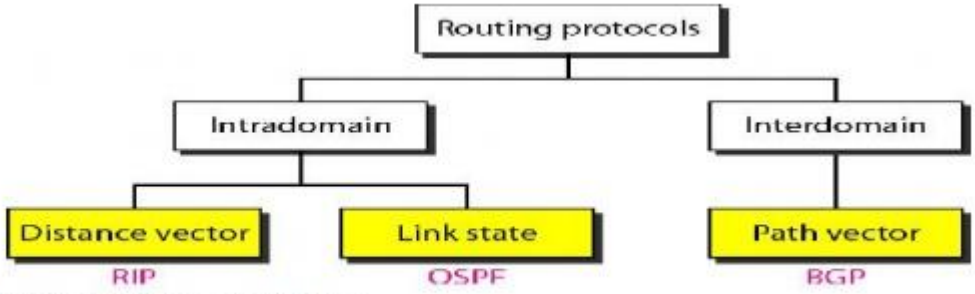


Figure 3.44 Popular routing protocols

Intra-domain Routing is different from Inter-domain Routing.

Intra domain is any protocol in which Routing algorithm works only within domains on the other hand Inter domain is any protocol in which Routing algorithm works within and between domains.

Let us see the differences between Intradomain and Interdomain:

S.No	Intradomain Routing	Interdomain Routing
1.	Routing algorithm works only within domains.	Routing algorithm works within and between domains.
2.	It need to know only about other routers within their domain.	It need to know only about other routers within and between their domain.
3.	Protocols used in intradomain routing are known as Interior-gateway protocols.	Protocols used in interdomain routing are known as Exterior-gateway protocols.
4.	In this Routing, routing takes place within an autonomous network.	In this Routing, routing takes place between the autonomous networks.
5.	Intradomain routing protocols ignores the internet outside the AS(autonomous system).	Interdomain routing protocol assumes that the internet contains the collection of interconnected AS(autonomous systems).
6.	Some Popular Protocols of this routing are RIP(routing information protocol) and OSPF(open shortest path first).	Popular Protocols of this routing is BGP(Border Gateway Protocol) used to connect two or more AS(autonomous system).

❖ Routing Algorithms

(1) Distance Vector Routing

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

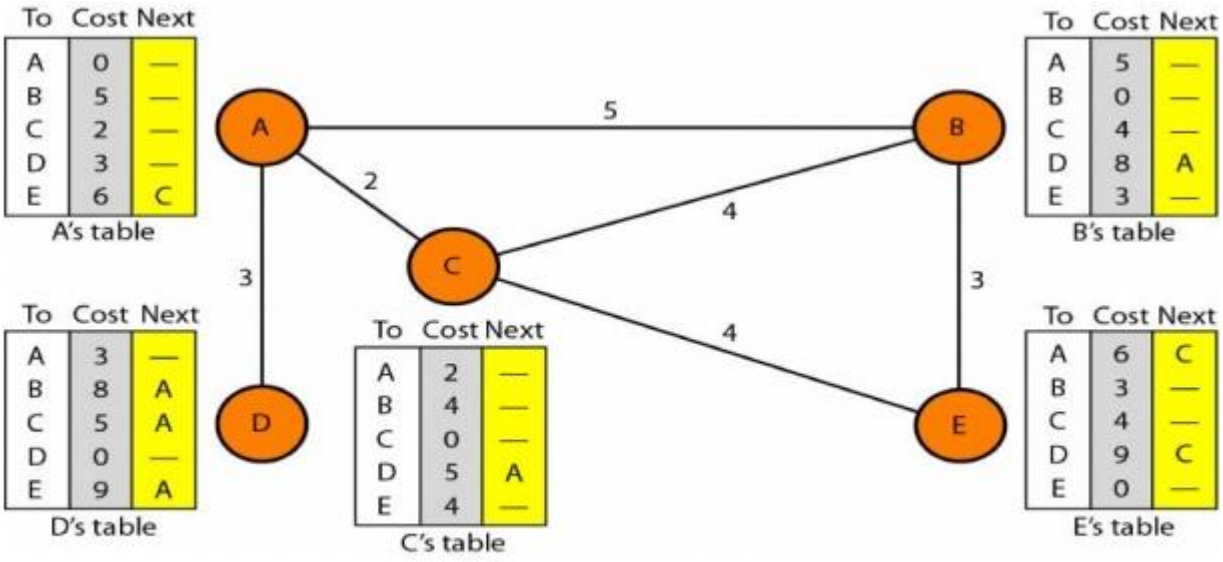


Figure 3.45 Distance vector routing tables

The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

Initialization

The tables in Figure 3.45 are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. The distance for any entry that is not a neighbor is marked as infinite (unreachable).

Sharing

The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

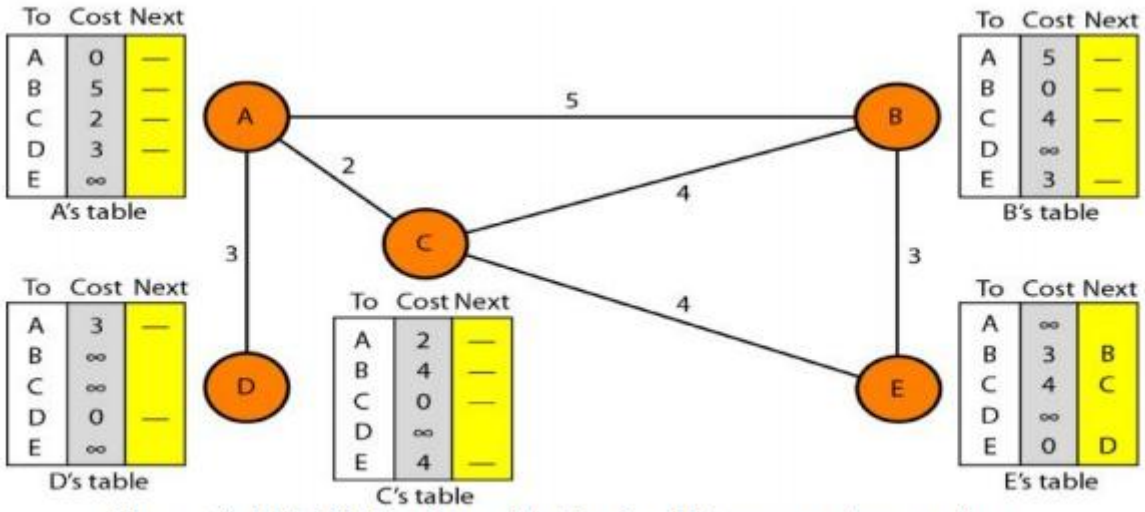


Figure 3.46 Initialization of tables in distance vector routing

Updating

When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is *x* mi, and the distance between A and C is *y* mi, then the distance between A and that destination, via C, is $x + y$ mi.

2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

a) If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.

b) If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3.

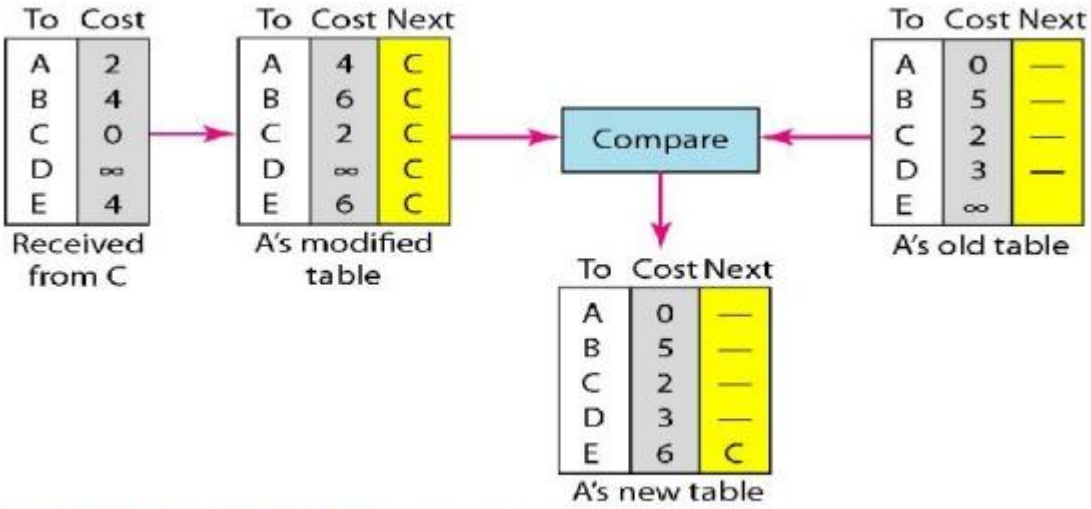


Figure 3.47 Updating in distance vector routing

Two-Node Loop Instability

A problem with distance vector routing is instability, which means that a network using this protocol can become unstable. To understand the problem, let us look at the scenario depicted.

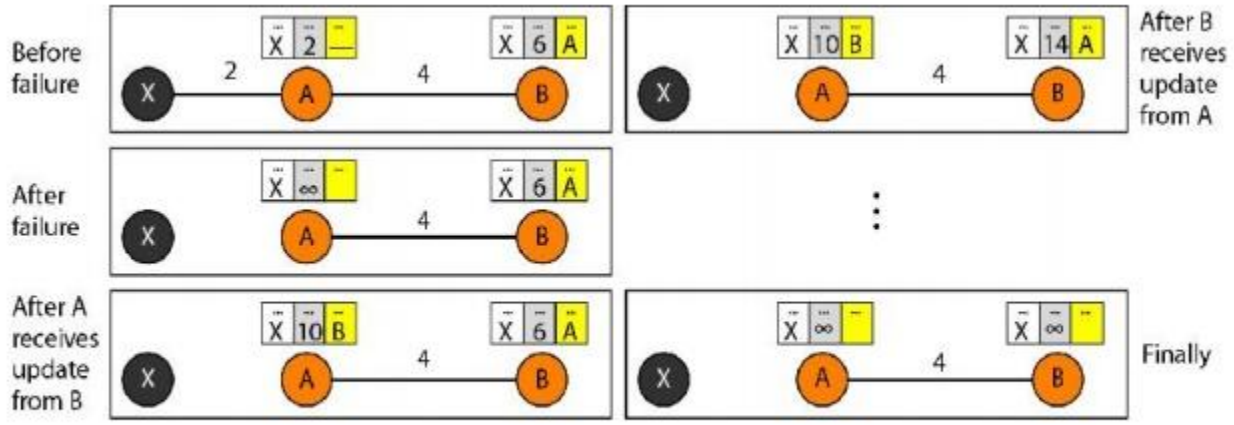


Figure 3.48 Two-node instability

Defining Infinity The first obvious solution is to redefine infinity to a smaller number, such as100. For our previous scenario, the system will be stable in less than 20 update s. As a matter of fact, most implementations of the distance vector protocol define the distance between each node to be I and define 16 as infinity. However, this means that the distance

vector routing cannot be used in large systems. The size of the network, in each direction, cannot exceed 15 hops.

Split Horizon Another solution is called split horizon. In this strategy, instead of flooding thetable through each interface, each node sends only part of its table through each interface. If, according to its table, node B thinks that the optimum route to reach X is via A, it does not need to advertise this piece of information to A; the information has corne from A (A already knows). Taking information from node A, modifying it, and sending it back to node A creates the confusion. In our scenario, node B eliminates the last line of its routing table before it sends it to A. In this case, node A keeps the value of infinity as the distance to X.

(2) Link State Routing

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

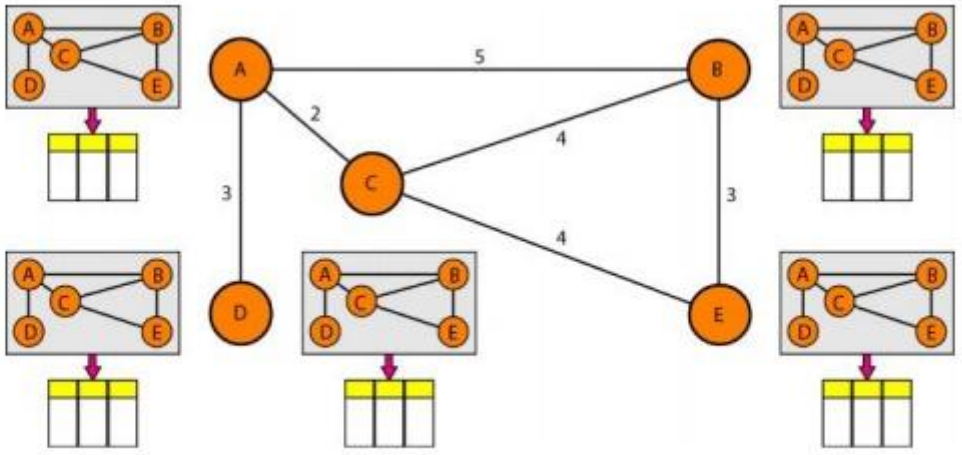


Figure 3.50 Concept of link state routing

The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination

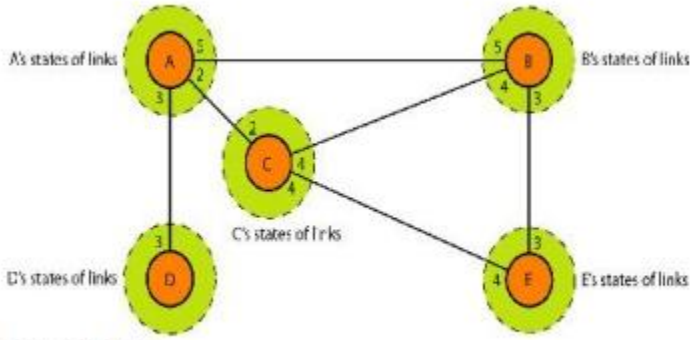


Figure 3.51 Link state knowledge

Building Routing Tables:

In link state routing, four sets of actions are required to ensure that each node has therouting table showing the least-cost node to every other node.

a) Creation of the states of the links by each node, called the link state packet (LSP).

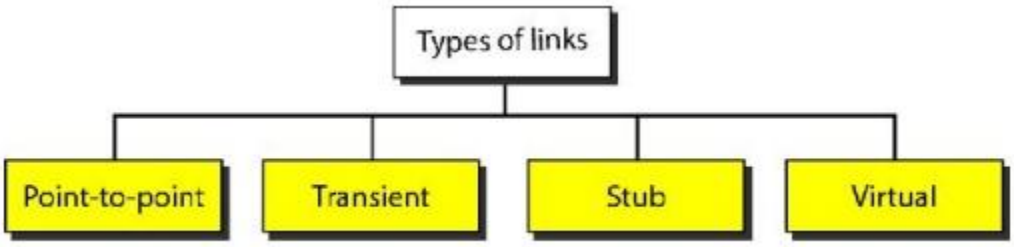
b)Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.

c) Formation of a shortest path tree for each node.

d)Calculation of a routing table based on the shortest path tree.

Types of Links

In OSPF terminology, a connection is called a *link.* Four types of links have been defined: point-to-point, transient, stub, and virtual.



A point-to-point link connects two routers without any other host or router in between. In other words, the purpose of the link (network) is just to connect the two routers. An example of this type of link is two routers connected by a telephone line or a T line. There is no need to assign a network address to this type of link. Graphically, the routers are represented by nodes, and the link is represented by a bidirectional edge connecting the nodes. The metrics, which are usually the same, are shown at the two ends, one for each direction. In other words, each router has only one neighbor at the other side of the link.

(3) Path Vector Routing

Distance vector and link state routing are both intradomain routing protocols. They can be used inside an autonomous system, but not between autonomous systems. These two protocols are not suitable for interdomain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there are more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.

Path vector routing proved to be useful for interdomain routing. The principle of path vector routing is similar to that of distance vector routing. In path vector routing, we assume that there is one node in each autonomous system that acts on behalf of the entire autonomous system.

Initialization

At the beginning, each speaker node can know only the reach ability of nodes inside its autonomous system

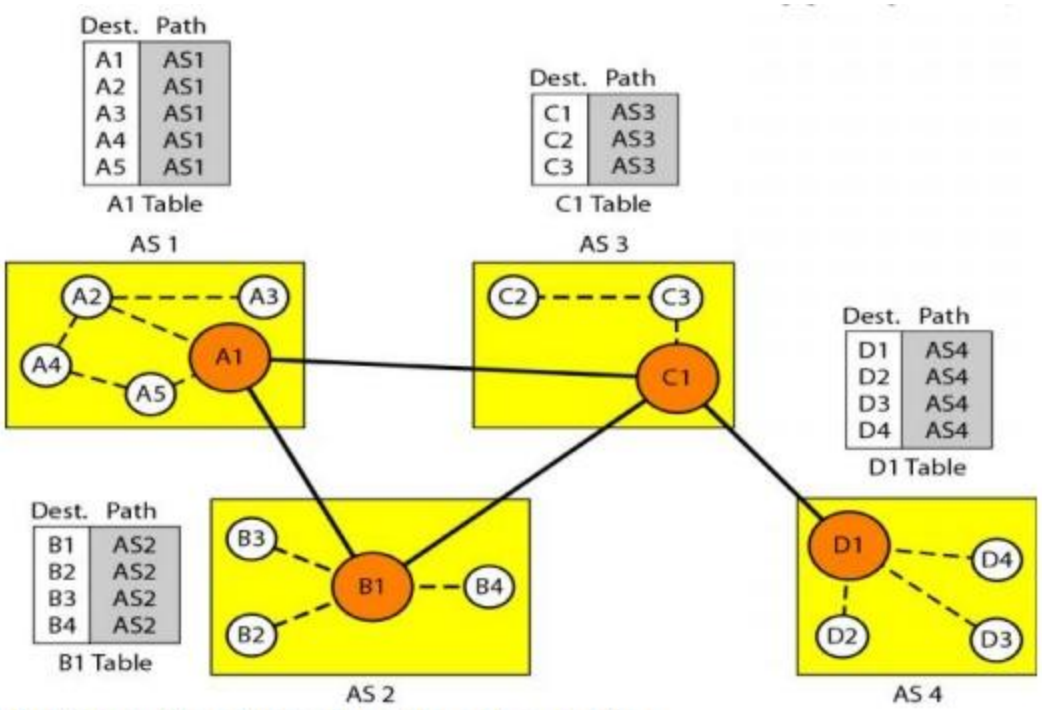
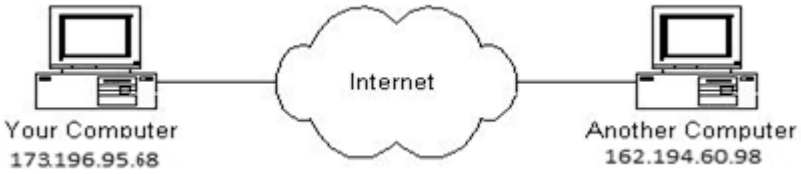


Figure 3.53 Initial routing tables in path vector routing

Node Al is the speaker node for AS1, B1 for AS2, C1 for AS3, and Dl for AS4. Node Al creates an initial table that shows Al to A5 are located in ASI and can be reached through it. Node B1 advertises that Bl to B4 are located in AS2 and can be reached through Bl. And so on.

❖ Internet structure:

Computers connected to the internet means that the systems are connected to computers' worldwide network. Therefore, each machine/device has its own or unique address. Addresses of the internet are in the form **"kkk.kkk.kkk.kkk,"** where each **"kkk"** ranges from 0-256. This structure of the internet address is known as an IP address (Internet Protocol). Fig. 1 describes the connection between two computers using the internet. Both systems have unique IP addresses. However, the internet is a unique object between both systems.

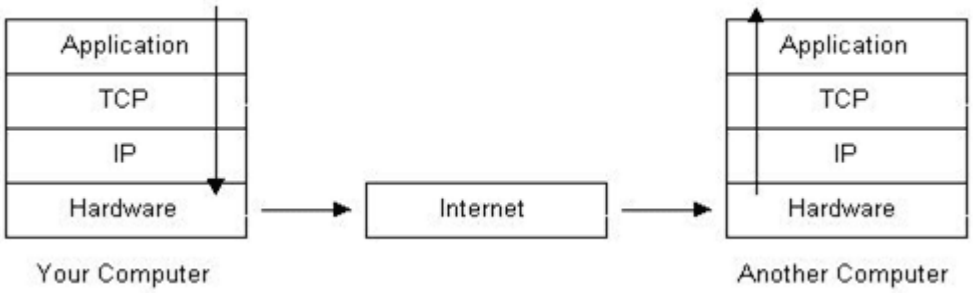


If a client connects the computer with the internet using Internet Service Provider (ISP), the client's system is allocated a temporary internet protocol address till the session client is operating. However, if someone becomes part of the internet using a local area network (LAN), the client is probably assigned to a permanent internet protocol. At the time of connection, the system will have a unique internet protocol address. A handy program is named "Ping" to ensure the internet connection on the system; this provision is available on all the Microsoft Windows operating systems and sometimes on a flavour of Unix OS.

Protocol Stacks and Packets

As the device is connected to the internet and retains a unique address. What is the procedure to communicate the device with the system at another end? For the sake of understanding, we are considering an example. As we discussed in Figure 1, one system retains an IP address, i.e., 173.196.95.98, and the second system contains an IP address, i.e., 162.194.60.98. Suppose you want to send a message "Hello Friend" to another computer via "Your computer". The medium of communication will be the wire that connects "Your computer" to the internet. Suppose you are using ISP facilities, then the message will be communicated via the phone line of ISP. In such a case, the first message will be encrypted in digital form. All the alphanumeric characters will be converted into an electronic signal. The electronic signal will be delivered to the other computer and then again decrypted into the original form as received on the second IP system. The convergence of messages from alphanumeric form to a digital signal and vice versa is performed employing Protocol Stack that is part of each operating system, i.e., Windows, Unix, Android, etc. The protocol stack applied in the domain of the internet is known as TCP/IP, as it is the primary protocol used for communication.

Figure briefly describes the path framework related to that message from "Your computer" to another computer.



The message that needs to be sent is written in an application on "Your computer" it starts from the top using the protocol stack and moves downward.

1. If the message is large, the stack layer breaks the message into smaller chunks so that data management remains stable. The chunks of data are known as **Packets.**
2. The data from the application layer move towards the TCP/IP layer. The packet of the data is assigned with a port number. In computers, various types of message applications are working at a time. Therefore, it is essential to know which application is sending the message so that it needs to be synced at the reception level (another computer) with the same application. Hence, the message will listen on the same port.
3. After necessary processing at the TCP level, the packets move towards the IP layer. The IP layer provides the destination layer where the message should be received. At this level, message packets retain port number as well as IP address.
4. The hardware layer is responsible for converting alpha/numeric messages into a digital signal and sending the message through the telephone's path.
5. Internet services provider (ISP) is also attached to the internet, where the ISP router examines the recipient's address. The next stop of the packet is another router.
6. Eventually, the packets reach another computer. This time packets start from the bottom.
7. As the packets move upwards, the packets' unnecessary data is removed that was helping to reach the destination; this includes IP address and port number.
8. On reaching the stack's top, all the packets are reassembled to form the original message sent by "Your computer".

❖ RIP Protocol

RIP stands for Routing Information Protocol.

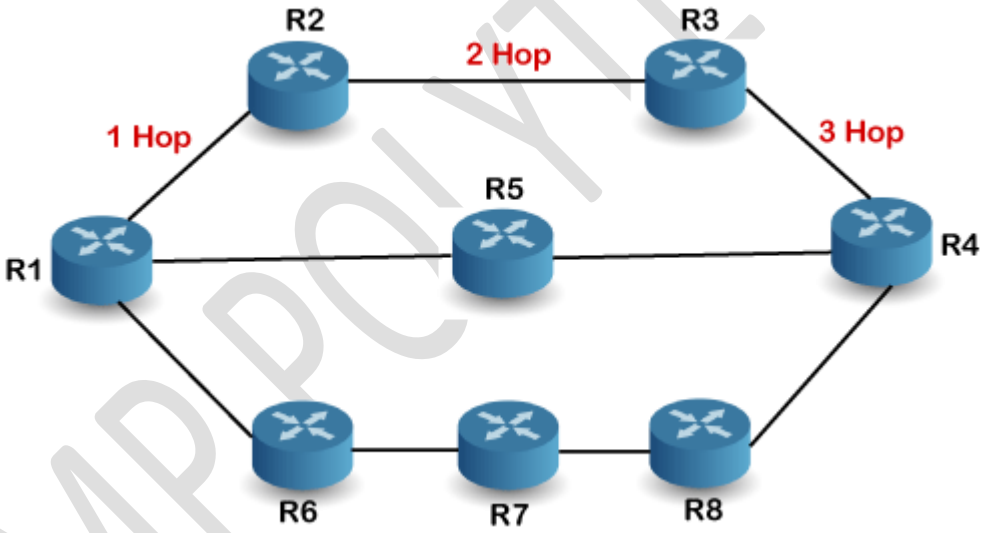
RIP is an intra-domain routing protocol used within an autonomous system.

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.

How is hop count determined?

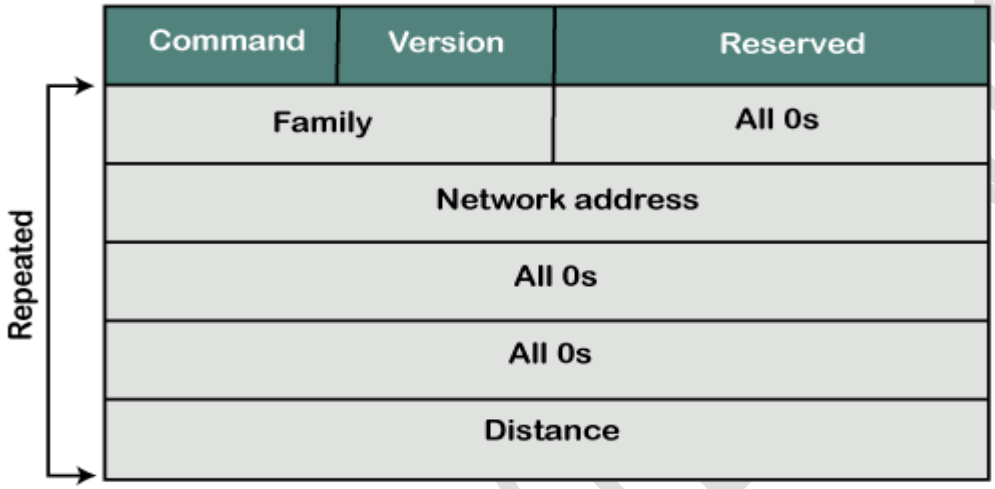
When the router sends the packet to the network segment, then it is counted as a single hop.



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.

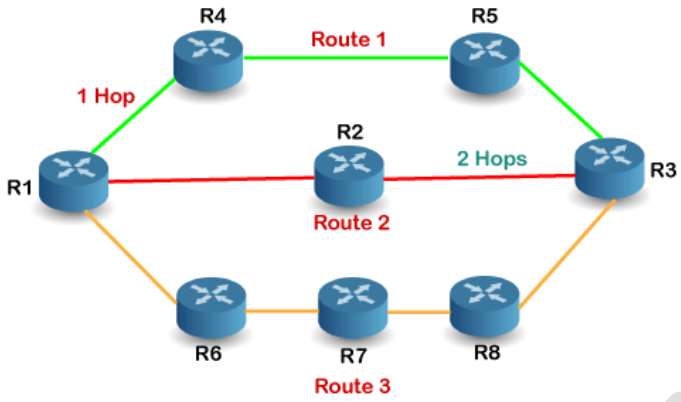
RIP Message Format

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.

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.
- 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.
- RIP supports maximum 15 hops which means that the maximum 16 hops can be configured in a RIP

Advantages of RIP

- 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.

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.

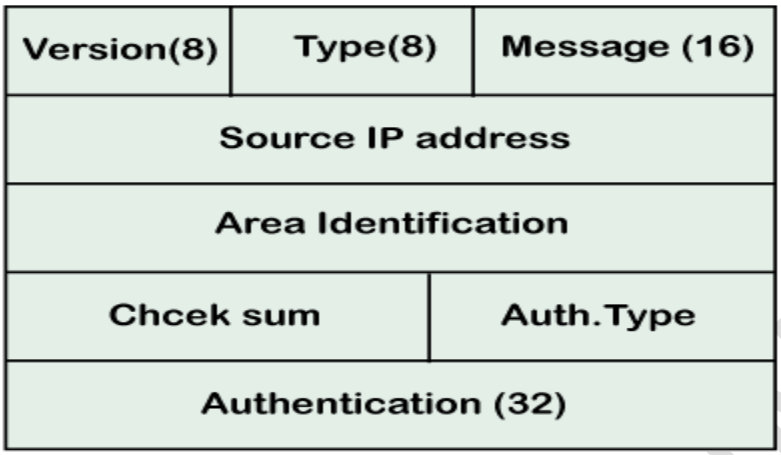
How a router forms a neighbor relationship?

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.

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.

There are five different types of packets in OSPF:

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.

❖ 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.

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.

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.

Inter AS-domain routing

It is specially designed for inter-domain routing, where inter AS-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.

Types of packets

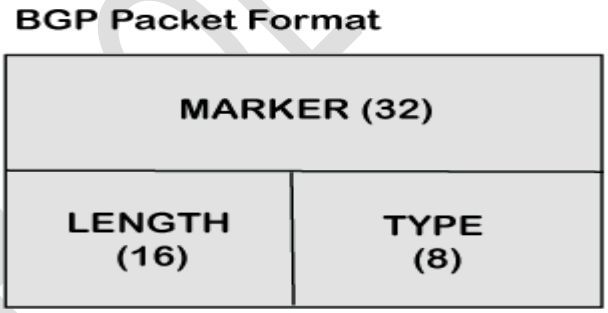
There are four different types of packets exist in BGP:

- **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



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.