**COMPUTER COMMUNICATIONh**

**UNIT 5**

***Forwarding:***

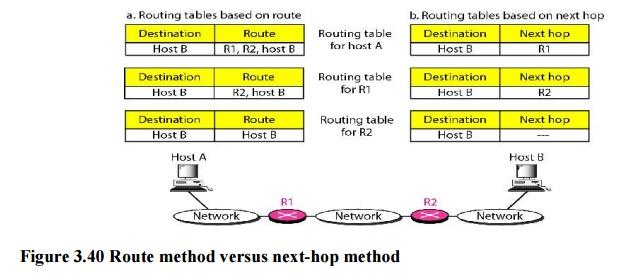
Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination. However, this simple solution is impossible today in an internetwork such as the Internet because the number of entries needed in the routing table would make table lookups inefficient.

***Forwarding Techniques:***

Several techniques can make the size of the routing table manageable and also handle issues such as security.

**a. Next-Hop Method versus Route Method**

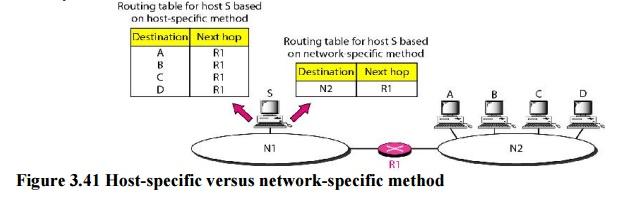
One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.



**b. Network-Specific Method versus Host-Specific Method**

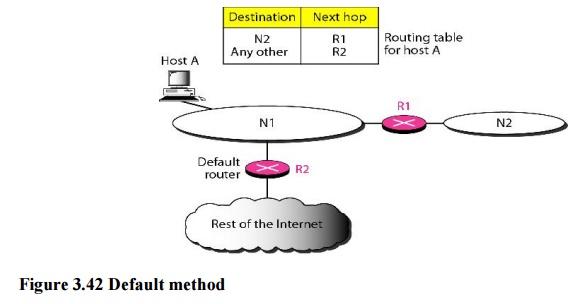
A second technique to reduce the routing table and simplify the searching process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself.

Host-specific routing is used for purposes such as checking the route or providing security measures



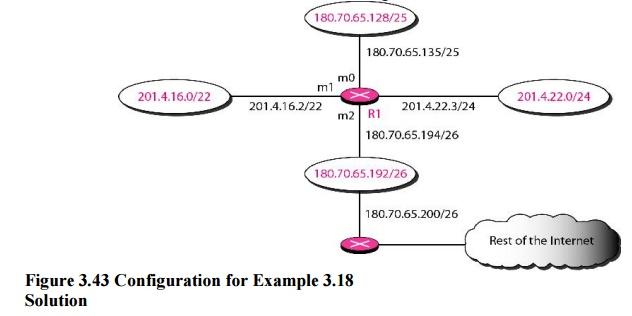
**c. Default Method**

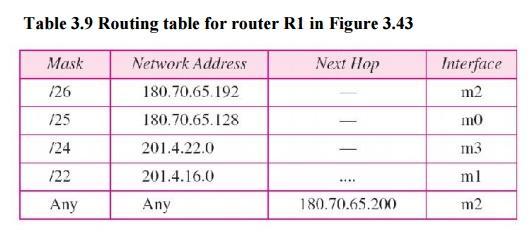
Another technique to simplify routing is called the default method. Host A is connected to a network with two routers. Router R1 routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default (normally defined as network address 0.0.0.0).



**Example 3.18**

Make a routing table for router R1, using the configuration in Figure 3.43





**Example 3.19**

Show the forwarding process if a packet arrives at R1 with the destination address 180.70.65.140.

**Solution**

The router performs the following steps:

1. The first mask (/26) is applied to the destination address. The result is 180.70.65.128, which does not match the corresponding network address.

2.  The second mask (/25) is applied to the destination address. The result is 180.70.65.128, which matches the corresponding network address. The next-hop address (the destination address of the packet in this case) and the interface number m0 are passed to ARP for further processing.

**Example 3.20**

Show the forwarding process if a packet arrives at R1 with the destination address 201.4.22.35.

**Solution**

The router performs the following steps:

* The first mask (/26) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 1).
* The second mask (/25) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 2).
* The third mask (/24) is applied to the destination address. The result is 201.4.22.0, which matches the corresponding network address. The destination address of the packet and the interface number m3 are passed to ARP.

**Example 3.21**

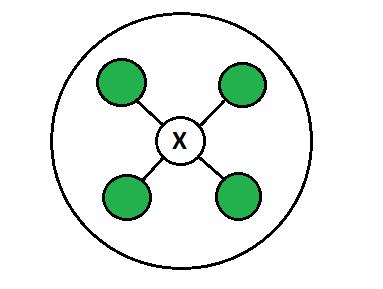
Show the forwarding process if a packet arrives at R1 with the destination address 18.24.32.78.

**Solution**

This time all masks are applied, one by one, to the destination address, but no matching network address is found. When it reaches the end of the table, the module gives the next-hop address 180.70.65.200 and interface number m2 to ARP. This is probably an outgoing package that needs to be sent, via the default router, to someplace else in the Internet.

***Routing Tables***

[***Routers***](https://www.geeksforgeeks.org/introduction-of-a-router/)***:***  
A Router is a networking device that forwards data packets between computer network. This device is usually connected to two or more different networks. When a data packet comes to a router port, the router reads address information in packet to determine out which port the packet will be sent. For example, a router provides you with the internet access by connecting your LAN with the Internet.



When a packet arrives at a Router, it examines destination IP address of a received packet and make routing decisions accordingly. Routers use *Routing Tables* to determine out which interface the packet will be sent. A routing table lists all networks for which routes are known. Each router’s routing table is unique and stored in the RAM of the device.

**Routing Table:**  
A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

**DestinationSubnet maskInterface**

128.75.43.0 255.255.255.0 Eth0

128.75.43.0 255.255.255.128 Eth1

192.12.17.5 255.255.255.255 Eth3

default Eth2

The entry corresponding to the *default* gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of default route is always 255.255.255.255 .

**Entries of an IP Routing Table:**

A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.

Each entry in the routing table consists o f the following entries:

1. **Network ID:**  
   The network ID or destination corresponding to the route.
2. **Subnet Mask:**  
   The mask that is used to match a destination IP address to the network ID.
3. **Next Hop:**  
   The IP address to which the packet is forwarded
4. **Outgoing Interface:**  
   Outgoing interface the packet should go out to reach the destination network.
5. **Metric:**  
   A common use of the metric is to indicate the *minimum number of hops* (routers crossed) to the network ID.

Routing table entries can be used to store the following types of routes:

* Directly Attached Network IDs
* Remote Network IDs
* Host Routes
* Default Route
* Destination

*When a router receives a packet, it examines the destination IP address, and looks up into its****Routing Table****to figure out which interface packet will be sent out.*

**How are Routing Tables populated?**  
There are ways to maintain Routing Table:

* Directly connected networks are added automatically.
* Using [Static Routing](https://www.geeksforgeeks.org/difference-between-static-and-dynamic-routing/).
* Using [Dynamic Routing](https://www.geeksforgeeks.org/difference-between-static-and-dynamic-routing/).

These Routing tables can be maintained manually or dynamically. In *dynamic routing*, devices build and maintain their routing tables automatically by using routing protocols to exchange information about the surrounding network topology. Dynamic routing tables allow devices to “listen” to the network and respond to occurrences like device failures and network congestion. Tables for *static network devices* do not change unless a network administrator manually changes them.

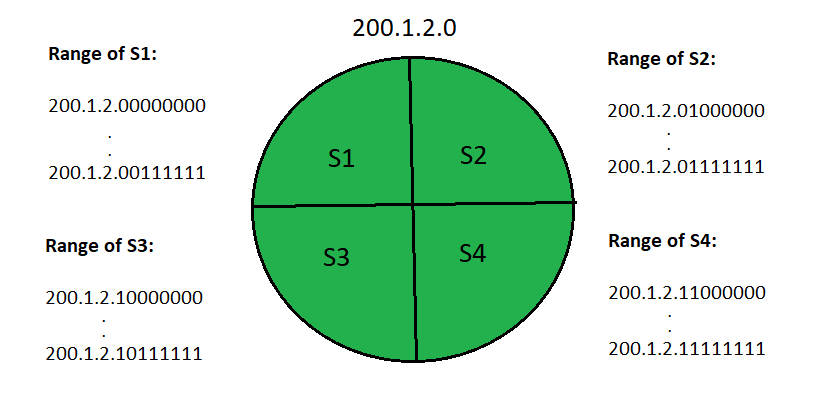
**Route Determination Process (finding Subnet ID using Routing Table):**  
Consider a network is [subnetted into 4 subnets](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-subnetting/) as shown in the above picture. The IP Address of the 4 subnets are:

200.1.2.0 (Subnet a)

200.1.2.64 (Subnet b)

200.1.2.128 (Subnet c)

200.1.2.192 (Subnet d)



Then, **routing table** maintained by the internal router looks like:

| **DESTINATION** | **SUBNET MASK** | **INTERFACE** |
| --- | --- | --- |
| 200.1.2.0 | 255.255.255.192 | a |
| 200.1.2.64 | 255.255.255.192 | b |
| 200.1.2.128 | 255.255.255.192 | c |
| 200.1.2.192 | 255.255.255.192 | d |
| Default | 0.0.0.0 | e |

To find its right [subnet](https://www.geeksforgeeks.org/introduction-to-subnetting/) (subnet ID), router performs the bitwise ANDing of destination IP Address mentioned on the data packet and all the subnet masks one by one.

* If there occurs only one match, router forwards the data packet on the corresponding interface.
* If there occurs more than one match, router forwards the data packet on the interface corresponding to the longest subnet mask.
* If there occurs no match, router forwards the data packet on the interface corresponding to the default entry.

***Unicast Routing Protocols***

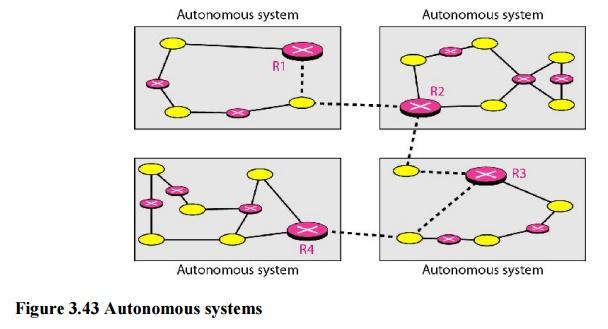
A routing table can be either static or dynamic. A static table is one with manual entries. A dynamic table*,* on the other hand, is one that is updated automatically when there is a change somewhere in the internet. Today, an internet needs dynamic routing tables. The tables need to be updated as soon as there is a change in the internet. For instance, they need to be updated when a router is down, and they need to be updated whenever a better route has been found.

***Optimization***

A router receives a packet from a network and passes it to another network. A router is usually attached to several networks. One approach is to assign a cost for passing through a network. We call this cost a metric. However, the metric assigned to each network depends on the type of protocol. Some simple protocols, such as the Routing Information Protocol (RIP), treat all networks as equals. The cost of passing through a network is the same; it is one hopcount. So if a packet passes through 10 networks to reach the destination, the total cost is 10 hop counts.

***Intra- and Inter-domain Routing***

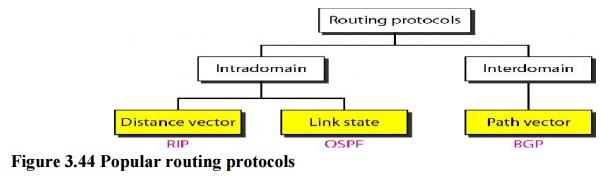
An internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems. An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing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



# Differences between Intradomain and Interdomain Routing

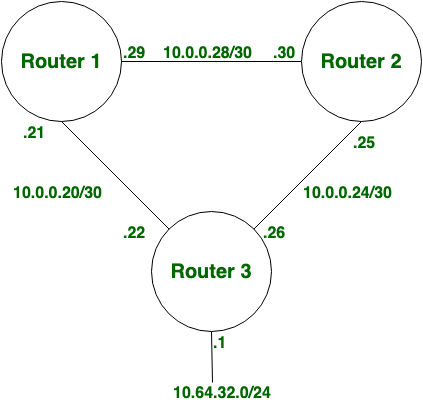
In this section, we shall discuss how **Intra-domain Routing** is different from **Inter-domain Routing**. Intra domain is any protocol in which Routing algorithm works only within domains on the other hand Inter domain is any protocol in which Routing algorithm works within and between domains.

Let us see the differences between Intradomain and Interdomain:

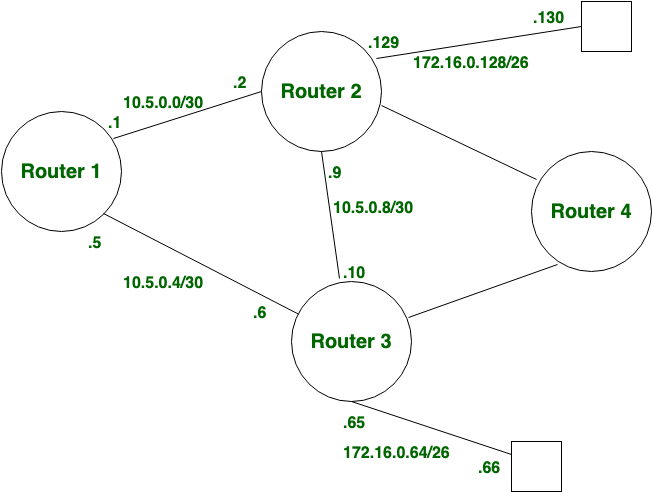
| **S.NO** | **INTRADOMAIN ROUTING** | **INTERDOMAIN ROUTING** |
| --- | --- | --- |
| 1. | Routing algorithm works only within domains. | Routing algorithm works within and between domains. |
| 2. | It need to know only about other routers within their domain. | It need to know only about other routers 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(resource 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). |

***Static and Dynamic Routing***

Both Static routing and dynamic routing are the [Types of Routing](https://www.geeksforgeeks.org/computer-network-types-routing/).  
*Static Routing:*  
Static Routing is also known as **non-adaptive** routing which doesn’t change routing table unless the network administrator changes or modify them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing.



*Dynamic Routing:*  
Dynamic routing is also known as **adaptive** routing which change routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide high security like static routing. When the network change(topology) occurs, it sends the message to router to ensure that changes then the routes are recalculated for sending updated routing information.

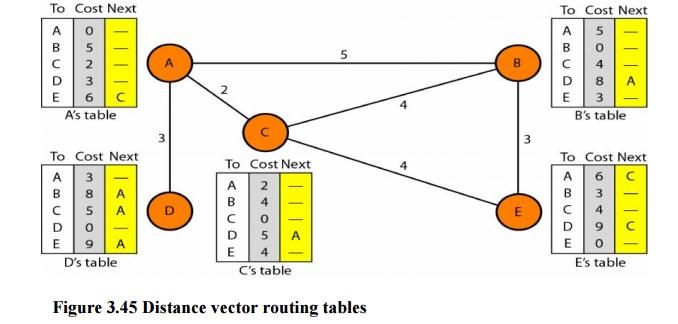


**Difference between Static and Dynamic Routing:**

| **S.NO** | **STATIC ROUTING** | **DYNAMIC ROUTING** |
| --- | --- | --- |
| 1. | In static routing routes are user defined. | In dynamic routing, routes are updated according to topology. |
| 2. | Static routing does not use complex routing algorithms. | Dynamic routing uses complex routing algorithms. |
| 3. | Static routing provides high or more security. | Dynamic routing provides less security. |
| 4. | Static routing is manual. | Dynamic routing is automated. |
| 5. | Static routing is implemented in small networks. | Dynamic routing is implemented in large networks. |
| 6. | In static routing, additional resources are not required. | In dynamic routing, additional resources are required. |

**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).



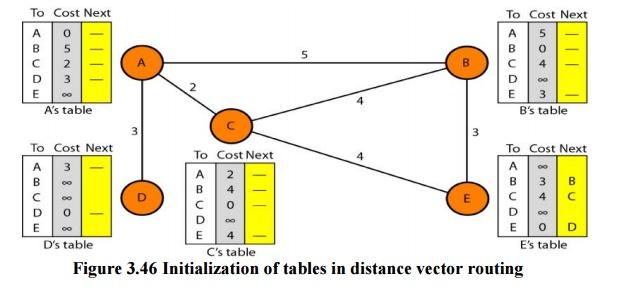
The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

**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.



**Updating**

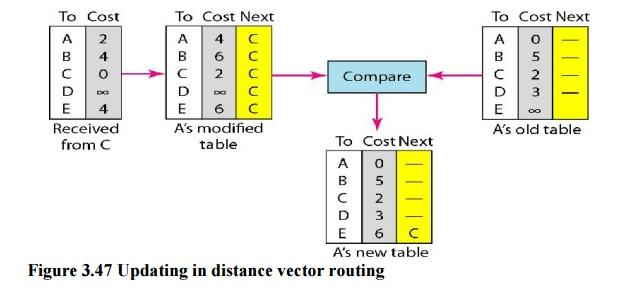
When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

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.

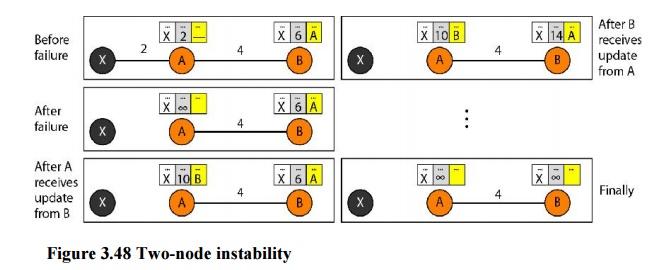
3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

1. 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.
2. 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.



**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.

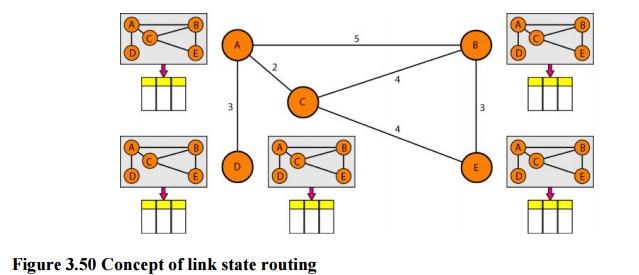


**Defining Infinity**The first obvious solution is to redefine infinity to a smaller number, such as100. For our previous scenario, the system will be stable in less than 20 update s. As a matter of fact, most implementations of the distance vector protocol define the distance between each node to be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

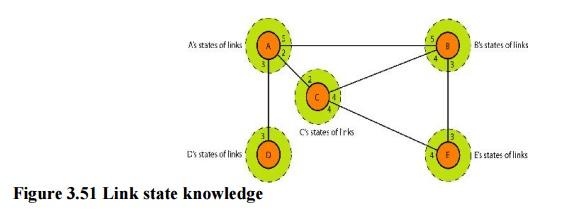
***Link State Routing***

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



**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).

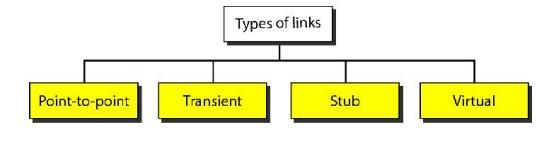
b)Dissemination of LSPs to every other router, called **flooding,** in an efficient and  reliable way.

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.



**Figure 3.52 Types of links**

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.

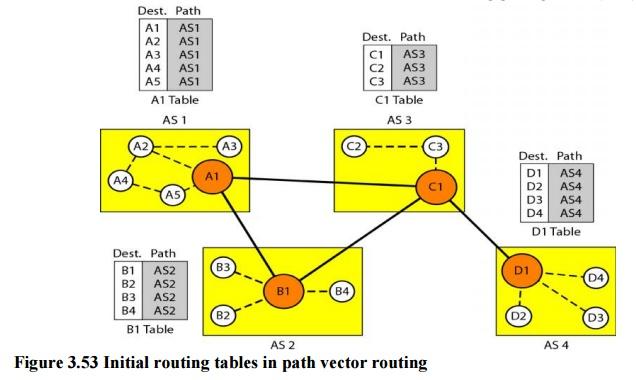
***Path Vector Routing***

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.

Difference between Distance vector routing and Link State routing

[**Distance Vector Routing**](https://www.geeksforgeeks.org/computer-network-routing-protocols-set-1-distance-vector-routing/)**–**

* It is a dynamic routing algorithm in which each router computes distance between itself and each possible destination i.e. its immediate neighbors.
* The router share its knowledge about the whole network to its neighbors and accordingly updates table based on its neighbors.
* The sharing of information with the neighbors takes place at regular intervals.
* It makes use of **Bellman Ford Algorithm** for making routing tables.
* **Problems –**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.

[**Link State Routing**](https://practice.geeksforgeeks.org/problems/what-is-link-state-routing-protocol)**–**

* It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
* A router sends its information about its neighbors only to all the routers through flooding.
* Information sharing takes place only whenever there is a change.
* It makes use of **Dijkastra’s Algorithm** for making routing tables.
* **Problems –**Heavy traffic due to flooding of packets.  
  **–**Flooding can result in infinite looping which can be solved by using **Time to leave (TTL)** field.

https://media.geeksforgeeks.org/wp-content/uploads/po-1.png

# *Routing Information Protocol (RIP) V1 & V2*

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

#### RIP Version-1:

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

**Advantages of RIP ver1 –**

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

**Disadvantage of RIP ver1 –**

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

#### RIP Version-2:

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

**Advantages of RIP ver2 –**

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

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

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

#### RIP ver1 versus RIP ver2:

| **RIP VER1** | **RIP VER2** |
| --- | --- |
| RIP v1 uses what is known as classful routing | RIP v2 is a classless protocol and it supports variable-length subnet masking (VLSM), CIDR, and route summarization |
| RIPv1 routing updates are broadcasted | RIP v2 routing updates are multicasted |
| RIPv1 has no authentication | RIP v2 supports authentication |
| RIP v1 does not carry mask in updates | RIP v2 does carry mask in updates, so it supports for VLSM |
| RIP v1 is an older, no longer much used routing protocol | IP v2 can be useful in small, flat networks or at the edge of larger networks because of its simplicity in configuration and usage |

***Open Shortest Path First (OSPF) protocol States:***

Open Shortest Path First (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

**OSPF terms –**

1. **Router I’d –**It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. **Router priority –** It is a 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. **Designated Router (DR) –** It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. **Backup Designated Router (BDR) –** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

**DR and BDR election –** DR and BDR election takes place in broadcast network or multi access network. Here is the criteria for the election:

1. Router having the highest router priority will be declared as DR.
2. If there is a tie in router priority then highest router I’d will be considered. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

**OSPF states –** The device operating OSPF goes through certain states. These states are:

1. **Down –** In this state, no hello packet have been received on the interface.  
   **Note –** The Down state doesn’t mean that the interface is physically down. Her, it means that OSPF adjacency process has not started yet.
2. **INIT –** In this state, hello packet have been received from the other router.
3. **2WAY –** In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.  
   **Note –** In between the 2WAY state and Exstart state, the DR and BDR election takes place.
4. **Exstart –** In this state, NULL DBD are exchanged.In this state, master and slave election take place. The router having the higher router I’d becomes the master while other becomes the slave. This election decides Which router will send it’s DBD first (routers who have formed neighbourship will take part in this election).
5. **Exchange –** In this state, the actual DBDs are exchanged.
6. **Loading –** In this sate, LSR, LSU and LSA (Link State Acknowledgement) are exchanged.  
   **Important –** When a router receives DBD from other router, it compares it’s own DBD with the other router DBD. If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed. The other router replies with the LSU containing the updates that are needed. In return to this, the router replies with the Link State Acknowledgement.
7. **Full –** In this state, synchronization of all the information takes place. OSPF routing can begin only after the Full state.

**Open Shortest Path First (OSPF) Protocol fundamentals**

Open shortest path first (OSPF) is a **link-state routing protocol** which is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm. A link-state routing protocol is a protocol which uses the concept of triggered updates, i.e., if there is a change observed in the learned routing table then the updates are triggered only, not like the distance-vector routing protocol where the routing table are exchanged at a period of time.

Open shortest path first (OSPF) is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a **network layer protocol** which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

**Criteria –**  
To form neighbourship in OSPF, there is a criteria for both the routers:

1. It should be present in same area
2. Router I’d must be unique
3. Subnet mask should be same
4. Hello and dead timer should be same
5. Stub flag must match
6. Authentication must match

OSPF supports NULL, plain text, MD5 authentication.

**Note –** Both the routers (neighbors) should have same type of authentication enabled. e.g- if one neighbor has MD5 authentication enabled then other should also have MD5 authentication enabled.

**OSPF messages–**

OSPF uses certain messages for the communication between the routers operating OSPF.

* **Hello message –** These are keep alive messages used for neighbor discovery /recovery. These are exchanged in every 10 seconds. This include following information : Router I’d, Hello/dead interval, Area I’d, Router priority, DR and BDR IP address, authentication data.
* **Database Description (DBD) –** It is the OSPF routes of the router. This contains topology of an AS or an area (routing domain).
* **Link state request (LSR) –** When a router receive DBD, it compares it with its own DBD. If the DBD received has some more updates than its own DBD then LSR is being sent to its neighbor.
* **Link state update (LSU) –** When a router receives LSR, it responds with LSU message containing the details requested.
* **Link state acknowledgement –** This provides reliability to the link state exchange process. It is sent as the acknowledgement of LSU.
* **Link state advertisement (LSA) –** It is an OSPF data packet that contains link-state routing information, shared only with the routers to which adjacency has been formed.

**Note –** Link State Advertisement and Link State Acknowledgement both are different messages.

**Timers –**

* **Hello timer –** The interval in which OSPF router sends a hello message on an interface. It is 10 seconds by default.
* **Dead timer –** The interval in which the neighbor will be declared dead if it is not able to send the hello packet . It is 40 seconds by default.It is usually 4 times the hello interval but can be configured manually according to need.

**OSPF supports/provides/advantages –**

* Both IPv4 and IPv6 routed protocols
* Load balancing with equal cost routes for same destination
* VLSM and route summarization
* Unlimited hop counts
* Trigger updates for fast convergence
* A loop free topology using SPF algorithm
* Run on most routers
* Classless protocol

There are some disadvantages of OSPF like, it requires extra CPU process to run SPF algorithm, requires more RAM to store adjacency topology and more complex to setup and hard to troubleshoot

***Features of Enhanced Interior Gateway Routing Protocol (EIGRP)***

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco-proprietary hybrid routing protocol that contains features of distance-vector and link-state routing protocols. It is a network layer protocol which works on the protocol number 88.

Some of its features are:

1. **Rapid convergence –** EIGRP uses DUAL algorithm to support rapid convergence. If a route to a network goes down then another route(feasible successor) can be used. If there is no route present to that network in the topology table also then a query message is multicast to find out the alternative route to that network.
2. **Reduced bandwidth usage –** EIGRP doesn’t send periodic updates like other distance vector routing protocol does.Distance Vector Routing protocol like RIP sends full routing table over a period of time therefore consumes the available bandwidth needlessly but EIGRP uses partial updates if there is any change in the topology occurs i.e updates are triggered only if any event occurs therfore consuming the bandwidth when needed. Also, EIGRP updates are propagated to the routers only who requires it.
3. **Support all LAN and WAN data link protocols and typologies –** EIGRP supports multi-access network like fddi, token ring etc and all WAN topologies like leased line, point-to-point links. EIGRP doesn’t require any additional configuration across layer 2 protocols like frame relay.
4. **Supports auto-summary –** In EIGRP, auto-summarization is enabled by default. Auto summarization is a feature which allows Routing Protocols to summarize its routes to their classful networks automatically i.e routers will receive summarised routes automatically. EIGRP. e.g-1.1.1.1 /24 will be automatically summarised to the classful 1.1.1.1/8
5. **Supports unequal cost load balancing –** Unequal cost load balancing is possible in EIGRP by changing the value of variance. By default, variance is 1 therfore supports equal cost load balancing but if we want to use unequal cost load balancing then we can change the value of variance according to the amount of traffic we want to divide across different paths. Feasible distance is multiplied in such a way that it becomes greater than the value of feasible distance of successor.
6. **Communication via Reliable Transfer Protocol (RTP) –** EIGRP depends upon proprietary protocol RTP to mange the communication between EIGRP speaking routers. EIGRP uses 224.0.0.10 as it’s multicast address. For each multicast it sends, the router prepares and maintains a list of routers (speaking EIGRP). If no acknowledgement of multicast is received then same data is transmitted through 16 unicast messages. If no acknowledgement is received even after 16 unicast attempt then it is declared dead. This process is known as reliable multicast.
7. **Best path selection using DUAL –** EIGRP uses Diffusing Update Algorithm (DUAL) to find out the best path available to a network. EIGRP speaking routers maintains a topology table in which all the routes to the network are maintained. If the best path (successor) goes down, then second best path (feasible successor) is used from the topology table. If there is no path available in topology table then it sends a query message to resolve the query.  
     
   It maintains 3 different tables mainly:  
   **(a) Neighbor table:** It contains information about the routers with which neighbourship has been formed. It contains the SRTT, RTP. It also contains queue count value for the hello messages that are not being acknowledged.  
   **(b) Topology table:** It contains all the routes available to a network (both feasible successor and successor).  
   **(c) Routing table:** It contains all the routes which are being used to make current routing decisions. The routes in this table are considered as successor (best path) route

*EIGRP fundamentals*

Dynamic routing Protocol performs the same function as static routing Protocol does. In dynamic routing Protocol, if the destination is unreachable then an another entry, in the routing table, to the same destination can be used. One of the routing Protocol is EIGRP.  
**EIGRP:**  
[Enhanced Interior Gateway Routing Protocol (EIGRP)](https://www.geeksforgeeks.org/computer-network-features-enhanced-interior-gateway-routing-protocol-eigrp/) is a dynamic routing Protocol which is used to find the best path between any two layer 3 device to deliver the packet. EIGRP works on network layer Protocol of osi model and uses the protocol number 88.It uses metric to find out best path between two layer 3 device (router or layer 3 switch) operating EIGRP. Administrative Distance for EIGRP are:-

| **EIGRP ROUTES** | **AD VALUES** |
| --- | --- |
| Summary Routes | 5 |
| Internal Routes | 90 |
| external routes | 170 |

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

1. **Hello message-**These messages are keep alive messages which are exchanged between two devices operating EIGRP. These messages are used for neighbour discovery/recovery, if there is any device operating EIGRP or if any device(operating EIGRP) coming up again.  
   These messages are used for neighbor discovery if multicast at 224.0.0.10. It contains values like AS number, k values etc.  
   These messages are used as acknowledgment when unicast. A hello with no data is used as the acknowledgment.
2. **NULL update-**It is used to calculate SRTT(Smooth Round Trip Timer) and RTO(Retransmission Time Out).  
   *SRTT:*The time is taken by a packet to reach neighboring router and the acknowledgment of the packet to reach to the local router.

*RTO:*If a multicast fails then unicast are being sent to that router. RTO is the time for which the local router waits for an acknowledgment of the packet.

1. **Full Update –**After exchanging hello messages or after the neighbourship is formed, these messages are exchanged. This message contains all the best routes.
2. **Partial update-**These messages are exchanged when there is a topology change and new links are added. It contains only the new routes, not all the routes. These messages are multicast.
3. **Query message-**These messages are multicast when the device is declared dead and it has no routes to it in its topology table.
4. **Reply message –**These messages are the acknowledgment of the query message sent to the originator of the query message stating the route to the network which has been asked in the query message.
5. **Acknowledgement message**  
   It is used to acknowledge EIGRP update, queries, and replies. Acks are hello packets that contain no data.

**Note:-**Hello, and acknowledgment packets do not require any acknowledgment.  
Reply, query, update messages are reliable messages i.e requires acknowledgement.

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

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

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

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

**Timers:-**  
**Hello timer-** The interval in which EIGRP sends a hello message on an interface. It is 5 seconds by default.  
**Dead timer-** The interval in which the neighbor will be declared dead if it is not able to send the hello packet. It is 15 seconds by default.

**Border Gateway Protocol (BGP)**

[Border Gateway Protocol (BGP)](https://practice.geeksforgeeks.org/problems/bgpborder-gateway-protocol) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes.

The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS’s BGP router. BGP’s main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems’ graph based on the information exchanged between BGP routers.

**Characteristics of Border Gateway Protocol (BGP):**

* **Inter-Autonomous System Configuration:** The main role of BGP is to provide communication between two autonomous systems.
* BGP supports Next-Hop Paradigm.
* Coordination among multiple BGP speakers within the AS (Autonomous System).
* **Path Information:** BGP advertisement also include path information, along with the reachable destination and next destination pair.
* **Policy Support:** BGP can implement policies that can be configured by the administrator. For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.
* Runs Over TCP.
* BGP conserve network Bandwidth.
* BGP supports CIDR.
* BGP also supports Security.

**Functionality of Border Gateway Protocol (BGP):**  
BGP peers performs 3 functions, which are given below.

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

**BGP Route Information Management Functions:**

* **Route Storage:**  
  Each BGP stores information about how to reach other networks.
* **Route Update:**  
  In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.
* **Route Selection:**  
  Each BGP uses the information in its route databases to select good routes to each network on the internet network.
* **Route advertisement:**  
  Each BGP speaker regularly tells its peer what is knows about various networks and methods to reach them