Module 7

Routing and Congestion Control

Lesson 7

Basics of Routing

Specific Instructional Objectives

On completion of this lesson, the students will be able to:

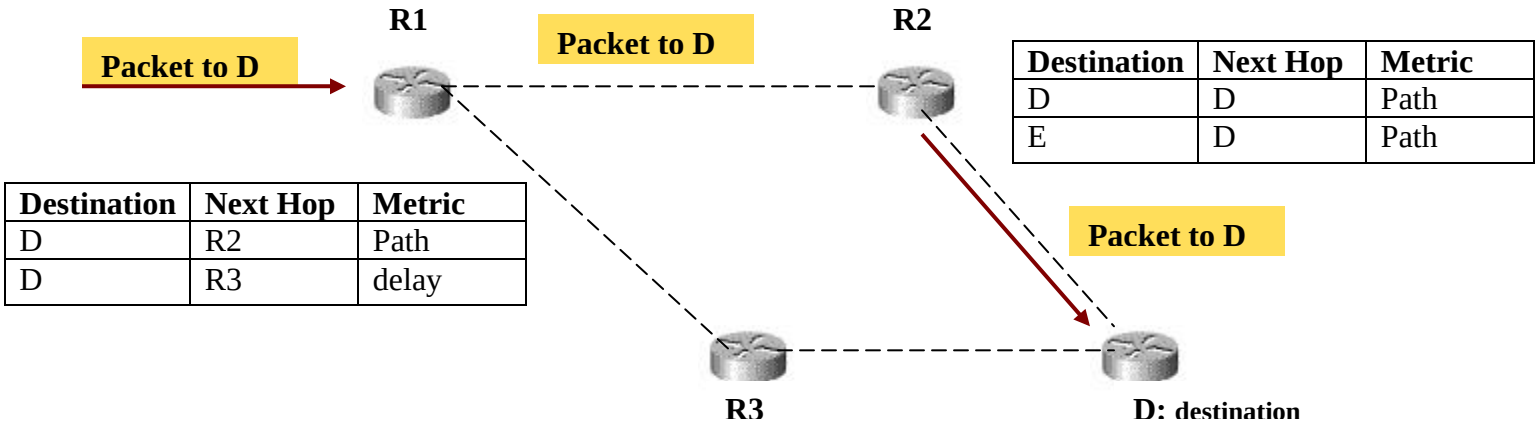
- Understand the need for routing
- Understand desirable properties of routing
- Understand various Routing algorithms
- Fixed (Static) routing
- Understand Flooding

7.1.1 Introduction

Routing is the act of moving information across an inter-network from a source to a destination. Along the way, at least one intermediate node typically is encountered. It's also referred to as the process of choosing a path over which to send the packets. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the data link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways. The routing algorithm is the part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on, i.e. what should be the next intermediate node for the packet.

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A *metric* is a standard of measurement; such as path bandwidth, reliability, delay, current load on that path etc; that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Mainly Destination/Next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular node representing the "next hop" on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop. Some of the routing algorithm allows a router to have multiple "next hop" for a single destination depending upon best with regard to different metrics. For example, let's say router R2 is be best next hop for destination "D", if path length is considered as the metric; while Router R3 is the best for the same destination if delay is considered as the metric for making the routing decision.



Destination	Next Hop	Metric
D	R2	Path
D	R3	delay

Destination	Next Hop	Metric
D	D	Path
E	D	Path

Figure 7.1.1 Typical routing in a small network

Figure 7.1.1 shows a small part of a network where packet destined for node "D", arrives at router R1, and based on the path metric i.e. the shortest path to destination is forwarded to router R2 which forward it to the final destination. Routing tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used. Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing *update message* is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A *link-state advertisement*, another example of a message sent between routers, informs other routers of the state of the sender's links. Link information also can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

Desirable properties of a router are as follows:

- **Correctness and simplicity:** The packets are to be correctly delivered. Simpler the routing algorithm, it is better.
- **Robustness:** Ability of the network to deliver packets via some route even in the face of failures.
- **Stability:** The algorithm should converge to equilibrium fast in the face of changing conditions in the network.
- **Fairness and optimality:** obvious requirements, but conflicting.
- **Efficiency:** Minimum overhead

While designing a routing protocol it is necessary to take into account the following design parameters:

- **Performance Criteria:** Number of hops, Cost, Delay, Throughput, etc
- **Decision Time:** Per packet basis (Datagram) or per session (Virtual-circuit) basis

- **Decision Place:** Each node (distributed), Central node (centralized), Originated node (source)
- **Network Information Source:** None, Local, Adjacent node, Nodes along route, All nodes
- **Network Information Update Timing:** Continuous, Periodic, Major load change, Topology change

7.1.2 Classification of Routers

Routing algorithms can be classified based on the following criteria:

- Static versus Adaptive
- Single-path versus multi-path
- Intra-domain versus inter-domain
- Flat versus hierarchical
- Link-state versus distance vector
- Host-intelligent versus router-intelligent

Static versus Adaptive

This category is based on how and when the routing tables are set-up and how they can be modified, if at all. Adaptive routing is also referred as **dynamic routing** and Non-adaptive is also known as **static routing** algorithms. *Static routing algorithms* are hardly algorithms at all; the table mappings are established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple. Routing decisions in these algorithms are in no way based on current topology or traffic.

Because static routing systems cannot react to network changes, they generally are considered unsuitable for today's large, constantly changing networks. Most of the dominant routing algorithms today are *dynamic routing algorithms*, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly. Dynamic routing algorithms can be supplemented with static routes where appropriate.

Single-Path versus Multi-path

This division is based upon the number of paths a router stores for a single destination.

Single path algorithms are where only a single path (or rather single next hop) is stored in the routing table. Some sophisticated routing protocols support multiple paths to the same

destination; these are known as multi-path algorithms. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines. The advantages of multipath algorithms are obvious: They can provide substantially better throughput and reliability. This is generally called load sharing.

Intradomain versus Interdomain

Some routing algorithms work only within domains; others work within and between domains. The nature of these two algorithm types is different. It stands to reason, therefore, that an optimal intra-domain-routing algorithm would not necessarily be an optimal inter-domain-routing algorithm.

Flat Versus Hierarchical

Some routing algorithms operate in a flat space, while others use routing hierarchies. In a *flat routing system*, the routers are peers of all others. In a hierarchical routing system, some routers form what amounts to a routing backbone. Packets from non-backbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone router through one or more non-backbone routers to the final destination.

Routing systems often designate logical groups of nodes, called domains, autonomous systems, or areas. In *hierarchical systems*, some routers in a domain can communicate with routers in other domains, while others can communicate only with routers within their domain. In very large networks, additional hierarchical levels may exist, with routers at the highest hierarchical level forming the routing backbone.

The primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns well. Most network communication occurs within small company groups (domains). Because intradomain routers need to know only about other routers within their domain, their routing algorithms can be simplified, and, depending on the routing algorithm being used, routing update traffic can be reduced accordingly.

Link-State versus Distance Vector

This category is based on the way the routing tables are updated.

Distance vector algorithms (also known as Bellman-Ford algorithms): Key features of the distance vector routing are as follows:

- The routers share the knowledge of the entire autonomous system
- Sharing of information takes place only with the neighbors
- Sharing of information takes place at fixed regular intervals, say every 30 seconds.

Link-state algorithms (also known as shortest path first algorithms) have the following key feature

- The routers share the knowledge only about their neighbors compared to all the routers in the autonomous system
- Sharing of information takes place only with all the routers in the internet, by sending small updates using flooding compared to sending larger updates to their neighbors
- Sharing of information takes place only when there is a change, which leads to lesser internet traffic compared to distance vector routing

Because convergence takes place more quickly in link-state algorithms, these are somewhat less prone to routing loops than distance vector algorithms. On the other hand, link-state algorithms require more processing power and memory than distance vector algorithms. Link-state algorithms, therefore, can be more expensive to implement and support. Link-state protocols are generally more scalable than distance vector protocols.

Host-Intelligent Versus Router-Intelligent

This division is on the basis of whether the source knows about the entire route or just about the next-hop where to forward the packet. Some routing algorithms assume that the source end node will determine the entire route. This is usually referred to as **source routing**. In source-routing systems, routers merely act as store-and-forward devices, mindlessly sending the packet to the next stop. These algorithms are also referred to as **Host-Intelligent Routing,** as entire route is specified by the source node.

Other algorithms assume that hosts know nothing about routes. In these algorithms, routers determine the path through the internet based on their own own strategy. In the first system, the hosts have the routing intelligence. In the latter system, routers have the routing intelligence.

7.1.3 Routing Algorithm Metrics

Routing tables contain information used by switching software to select the best route. In this section we will discuss the different nature of information they contain, and the way they determine that one route is preferable to others?

Routing algorithms have used many different metrics to determine the best route. Sophisticated routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric. All the following metrics have been used:

- Path length
- Delay
- Bandwidth
- Load

- Communication cost
- Reliability

Path length is the most common routing metric. Some routing protocols allow network administrators to assign arbitrary costs to each network link. In this case, path length is the sum of the costs associated with each link traversed. Other routing protocols define **hop count**, a metric that specifies the number of passes through internetworking products, such as routers, that a packet must pass through in a route from a source to a destination.

Routing delay refers to the length of time required to move a packet from source to destination through the internet. Delay depends on many factors, including the bandwidth of intermediate network links, the port queues (receive and transmit queues that are there in the routers) at each router along the way, network congestion on all intermediate network links, and the physical distance to be traveled. Because delay is a conglomeration of several important variables, it is a common and useful metric.

Bandwidth refers to the available traffic capacity of a link. All other things being equal, a 10-Mbps Ethernet link would be preferable to a 64-kbps leased line. Although bandwidth is a rating of the maximum attainable throughput on a link, routes through links with greater bandwidth do not necessarily provide better routes than routes through slower links. For example, if a faster link is busier, the actual time required to send a packet to the destination could be greater.

Load refers to the degree to which a network resource, such as a router, is busy. Load can be calculated in a variety of ways, including CPU utilization and packets processed per second. Monitoring these parameters on a continual basis can be resource-intensive itself.

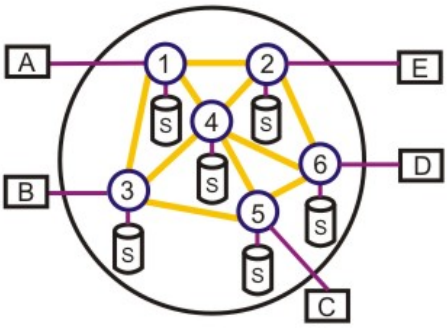
Communication cost is another important metric, especially because some companies may not care about performance as much as they care about operating expenditures. Although line delay may be longer, they will send packets over their own lines rather than through the public lines that cost money for usage time.

Reliability, in the context of routing algorithms, refers to the dependability (usually described in terms of the bit-error rate) of each network link. Some network links might go down more often than others. After a network fails, certain network links might be repaired more easily or more quickly than other links. Any reliability factor can be taken into account in the assignment of the reliability ratings, which are arbitrary numeric values, usually assigned to network links by network administrators.

7.1.4 Fixed or Static Routing

In fixed routing a route is selected for each source-destination pair of nodes in the network. The routes are fixed; they may only change if there is a change in the topology of the network. A central routing matrix is created based on least-cost path, which is stored at a network control center. The matrix shows, for each source-destination pair of

nodes, the identity of the next node on the route. Figure 7.1.2(a) shows a simple packet switching network with six nodes (routers), and Fig. 7.1.2 (b) shows the central routing table created based on least-cost path algorithm. Figure 7.1.3 shows the routing tables that can be distributed in different nodes of the network.



Central Routing Directory

From node	To node 1	2	3	4	5	6
1	-	2	3	2	2	2
2	1	-	1	6	6	6
3	1	1	-	4	5	1
4	6	6	3	-	5	6
5	4	4	3	4	-	4
6	2	2	2	4	4	-

Figures 7.1.2 (a) A simple packet switching network with six nodes (routers), (b) The central routing table created based on least-cost path

Node 1 Directory

Destination	Next Node
2	2
3	3
4	2
5	2
6	2

Node 2 Directory

Destination	Next Node
1	1
3	1
4	6
5	6
6	6

Node 3 Directory

Destination	Next Node
1	1
2	1
4	4
5	5
6	1

Node 4 Directory

Destination	Next Node
1	6
2	6
3	3
5	5
6	6

Node 5 Directory

Destination	Next Node
1	4
2	4
3	3
4	4
6	4

Node 6 Directory

Destination	Next Node
1	2
2	2
3	2
4	4
5	4

Figures 7.1.3 Routing tables that can be stored in different nodes of the network.

7.1.5 Flooding

Flooding requires no network information whatsoever. Every incoming packet to a node is sent out on every outgoing line except the one it arrived on. All possible routes between source and destination are tried. A packet will always get through if a path

exists. As all routes are tried, at least one packet will pass through the shortest route. All nodes, directly or indirectly connected, are visited. Main limitation flooding is that it generates vast number of duplicate packets. It is necessary to use suitable damping mechanism to overcome this limitation. One simple is to use *hop-count*; a hop counter may be contained in the packet header, which is decremented at each hop, with the packet being discarded when the counter becomes zero. The sender initializes the hop counter. If no estimate is known, it is set to the full diameter of the subnet. Another approach is keep track of packets, which are responsible for flooding using a sequence number and avoid sending them out a second time. A variation, which is slightly more practical, is *selective flooding*. The routers do not send every incoming packet out on every line, only on those lines that go in approximately in the direction of destination. Some of the important utilities of flooding are:

- Flooding is highly robust, and could be used to send emergency messages (e.g., military applications).
- It may be used to initially set up the route in a virtual circuit.
- Flooding always chooses the shortest path, since it explores every possible path in parallel.
- Can be useful for the dissemination of important information to all nodes (e.g., routing information).

7.1.6 Intradomain versus Interdomain

In this section we shall discuss the difference between inter-domain and intra-domain routing algorithms or as they are commonly known as Exterior-gateway protocols and Interior gateway protocols respectively. Before going into the details of each of these routing algorithms, let's discuss the concept of Autonomous systems, which is the major differentiator between the two.

Autonomous Systems

As internet is a network of network that spans the entire world and because it's not under the control of a single organization or body, one cannot think of forcing a single policy for routing over it. Thus, comes the concept of autonomous system.

An **Autonomous System (AS)** is a connected segment of a network topology that consists of a collection of subnetworks (with hosts attached) interconnected by a set of routes. The subnetworks and the routers are expected to be under the control of a single operations and maintenance (O&M) organization i.e., an AS is under the same administrative authority. These ASs share a common routing strategy. An AS has a single "interior" routing protocol and policy. Internal routing information is shared among routers within the AS, but not with systems outside the AS. However, an AS announces the network addresses of its internal networks to other ASs that it is linked to. An AS is identified by an Autonomous System number.

Border gateway protocols: To make the network that is hidden behind the autonomous systems reachable throughout the internet each autonomous system agrees to advertise network reachability information to other Autonomous systems. An autonomous system shares routing information with other autonomous systems using the *Border Gateway Protocol* (BGP). Previously, the Exterior Gateway Protocol (EGP) was used. When two routers exchange network reachability information, the message carry the AS identifier (AS number) that router represents.

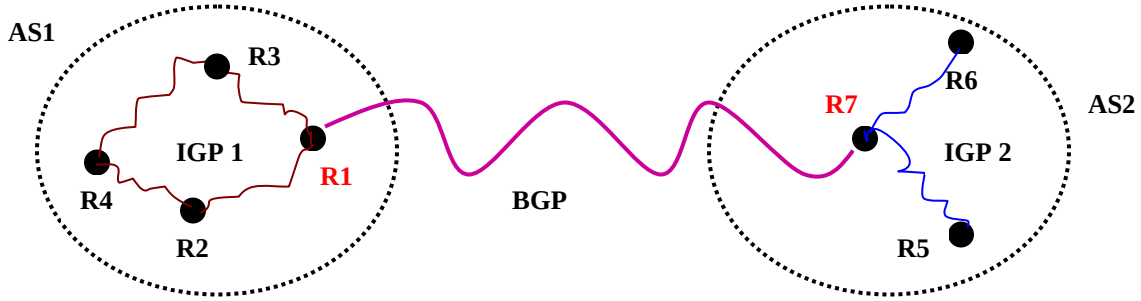


Figure 7.1.4 Two AS, each of which are using different IGPs internally and one BGP to communicate between each other

Figure 7.1.4 shows a conceptual view of two Autonomous systems (AS1 and AS2), each of which is using a different Interior gateway protocol (IGP1 and IGP2) as a routing protocol internally to the respective AS, while one router from each of the autonomous systems (R1 and R7) communicate among themselves to exchange the information of their respective Autonomous systems using a Border Gateway protocol, BGP. These two routers (R1 and R7) understands both interior and border gateway protocols.

Interior gateway protocols: In small and slowly changing network the network administrator can establish or modify routes by hand i.e. manually. Administrator keeps a table of networks and updates the table whenever a network is added or deleted from the autonomous system. The disadvantage of the manual system is obvious; such systems are neither scalable nor adaptable to changes. Automated methods must be used to improve reliability and response to failure. To automate the task this task, interior router (within a autonomous system) usually communicate with one another, exchanging network routing information from which reachability can be deduced. These routing methods are known as Interior gateway Protocols (IGP).

In the following lessons we shall discuss two Interior gateway protocols namely, routing Information Protocol (RIP) and Open Shortest path first (OSPF) and a border gateway protocol, for the better understanding of Routing.

Fill in the blanks

1. Routing is the act of _____ information across an inter-network from a source to a destination.
2. Bridging occurs at _____ layer of the OSI reference model, whereas routing occurs at _____ layer.
3. **IP** is an example of _____ protocol.
4. The entire process of routing can be divided into two main activities namely, _____ and _____.
5. Path bandwidth, reliability, delay, current load on that path are examples of _____.
6. Network devices without the capability to forward packets between subnetworks are called _____, whereas network devices with these capabilities are called _____ **.**
7. ISs are further divided into those that can communicate within routing domains _____ and those that communicate both within and between routing domains.
8. Adaptive routing is also referred as _____ **routing** and Non-adaptive is also known as _____ **routing** algorithms.
9. Some routing algorithms assume that the source end node will determine the entire route. Such algorithms are referred to as _____

Ans:

1. moving
2. Data Link Layer, Network layer
3. routed
4. Path Determination, switching
5. path metric
6. end systems (ESs), *intermediate systems (ISs)*
7. intradomain ISs, interdomain ISs
8. dynamic, static
9. source routing

1. What routing is important in a computer network?

Ans : In a packet switched network, there are number of nodes and different stations are communicating through these nodes. A packet is introduced in the network, which has to be delivered at a destination station. The path to be followed by the packet is decided by the routing algorithm. Routing tries to find out the least-cost or the optimized path between the source and the destination stations. If routing is not done properly, congestion may take place.

2. What are the primary conditions that affect routing?

Ans : The primary conditions that affect routing are

- Failure (Link / Node failure)
- Network congestion

3. Distinguish between virtual circuit and datagram type of routing?

Ans : In case of virtual circuit, a session is established between source and destination. At the beginning of the session, route is decided for all the packets to be sent for that session. In datagram type of routing, each packet is independently routed.

4. List out the advantages and disadvantages of fixed routing.

Ans : The advantages of fixed routing are as follows.

- The routes are always fixed and hence the routing overhead is minimum.
- The routing is dependent on network topology, i.e., static in nature.
- Routing is same for datagram and virtual circuit type of services.

The major disadvantages are:

- Lack of flexibility.
- The system is not robust. In case of link failure or node failure, the system cannot recover.
- Congestion may occur on a particular route.

5. What is flooding? Why flooding technique is not commonly used for routing?

Ans : Flooding is one type of non-adaptive routing technique where no network information is used. In case of flooding as each node receives a packet, it is re-transmitted or forwarded to all the links connected to the node (except the link through which the packet has arrived).

Flooding is not commonly used for routing for the following reasons:

- Flooding leads to unbounded number of packets
- May lead to congestion in the network
- A number of copies of the same packet is delivered at the destination node

6. In what situation flooding is most appropriate? How the drawbacks of flooding can be minimized?

Ans : Flooding is most appropriate in some critical operations, like military network, because of its robustness. In flooding routing technique the packet delivery is guaranteed if a path exists.

The drawbacks of flooding can be minimized by the following two ways:

- While forwarding a packet each node should find whether the particular packet has been already transmitted. If so, the second transmission of the packet should be stopped.
- Hop-count information should be maintained at each node. A packet is not forwarded, if hop-count is more than the specified limit.

7. Why adaptive routing is preferred over fixed routing?

Ans : The major problem of fixed routing is that in case of link/node failure, the system cannot recover. This problem is taken care in adaptive routing. The popularity of adaptive routing is mainly due to the following reasons:

- Adaptive routing improves performance of the network.
- It aids in avoiding congestion.

8. What kind of routing algorithm is used in Arpanet?

Ans : Arpanet uses network information supplied by adjacent nodes for routing rather than local information. Arpanet routing techniques have gone through three generations. Successive generations tried to improve the shortcomings of the previous ones. In the first generation (1969) and second generation (1979) techniques, the main metric was delay. Finally, in the third generation (1987) routing technique, the shortcomings are overcome by the following ways:

- Instead of using best route at each node, average path (under heavy load) is considered.
- The cost function is revised and it is keyed to the network utilization rather than delay.

Finally, it can be concluded that Apranet uses following routing technique:

- Delay based metric when load is light.
- Capacity based metric when the load is heavy.

9. Define Autonomous Systems.

Ans: A routing domain generally is considered a portion of an internet under common administrative authority that is regulated by a particular set of administrative guidelines. Routing domains are also called **autonomous systems**.

10. Differentiate between Single path and Multi-path routing algorithms.

Ans: Single path algorithms are where only a single path (or rather single next hop) is stored in the routing table. Some sophisticated routing protocols support multiple paths to the same destination; these are known as multi-path algorithms. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines.

11. Differentiate between Link State and Distance Vector routing algorithms.

Ans: Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. Each router, however, sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables.

Distance vector algorithms (also known as Bellman-Ford algorithms) call for each router to send all or some portion of its routing table, but only to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. *Distance vector* algorithms know only about their neighbors.

12. State few of the Routing metrics.

Ans: Routing algorithms have used many different metrics to determine the best route. Sophisticated routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric. All the following metrics have been used:

- **Path length :** Path length is the sum of the costs associated with each link traversed. It is also defined as **hop count**, a metric that specifies the number of internetworking devices between source and destination.
- **Delay :** It is the length of time required to move a packet from source to destination through the internetwork.
- **Bandwidth :** It refers to the available traffic capacity of a link.
- **Load :** Load refers to the degree to which a network resource, such as a router, is busy.
- **Reliability :** In the context of routing algorithms, refers to the dependability (usually described in terms of the bit-error rate) of each network link. Some network links might go down more often than others. After a network fails, certain network links might be repaired more easily or more quickly than other links.