Distance Vector Routing

The Distance Vector Routing algorithm (DVR) operate by having each router maintain a table giving the best-known distance to each destination and which path to use to get there.

These tables are updated by exchanging information with the neighbours.

Bellman Ford Basics: The distance vector routing algorithm is also known as the distributed Bellman-Ford routing algorithm & the Ford-Fulkerson algorithm, which Bellman developed in 1957 and Ford-Fulkerson in 1962.

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

Network Information: Every node in the network should have information about its neighbouring node. Each node in the network is designed to share information with all the nodes in the network.

Routing pattern: In DVR the data shared by the node are transmitted only to that node i.e., linked directly to one or more nodes in the network.

Distance Vector Routing Algorithm

It is used in CN to choose optimal path for data travel blw nodes. ie

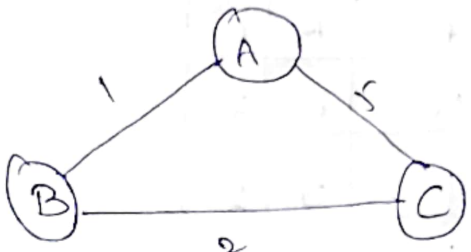
i) It works by exchanging data with its nearby nodes that are directly linked in order to compile a table of the most direct paths to every other node in the network.

(ii) Every node in the network keeps a routing table that details the distance to each target node as well as the subsequent hop node on the way there.

(iii) Normally, the distance is expressed in terms of the no of hops or the travel duration to destination

(iv) Bellman-Ford algorithm used by DVR algorithm to update the routing database. Each node sends its routing table to its neighbours on a regular basis, and they use the data they receive to update their own tables. Until every node has access to the most recent routing information, this procedure is repeated

Example.



Step1: Each router shares its routing table with every neighbor in this distance vector routing network. As A will share its routing table with B & C, neighbors B and C will share their routing table with A

Routing table A: From A

A	0
B	1
C	5

Routing table B: From B

A	1
B	0
C	2

Routing table C: From C

A	5
B	2
C	0

Step2: If path via neighbor has lowest cost, the router updates it local table to forward packets to the neighbor.

updated routing table A from A

A	0
B	1
C	3

updated routing table B

A	1
B	0
C	2

updated routing table C

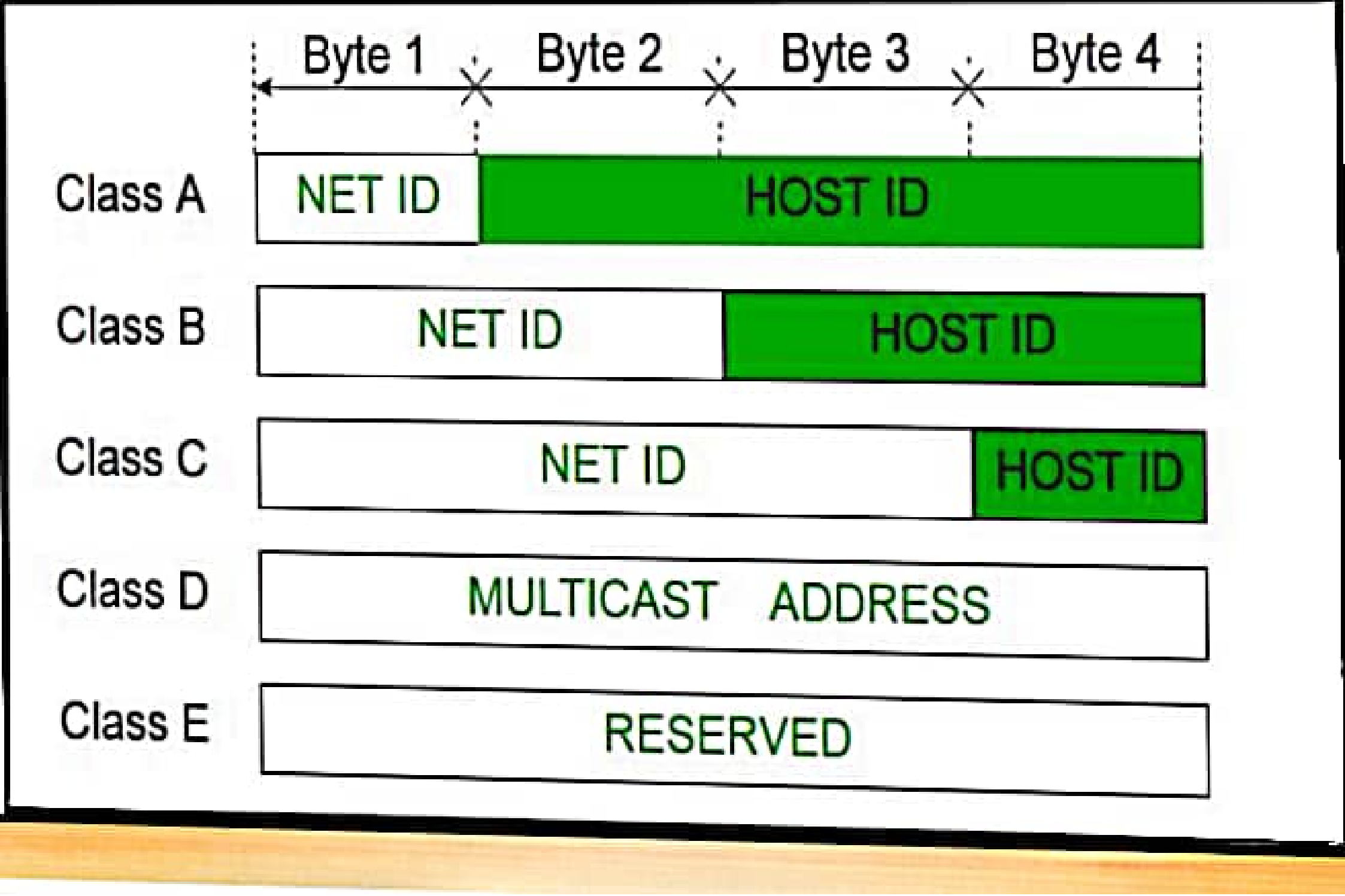
A	3
B	2
C	0

Step 3:

The following are the final routing table for all the routers A, B & C with lower cost distance vector routing protocol

updated table

X	A	B	C
A	0	1	3
B	1	0	2
C	3	2	0



Class A

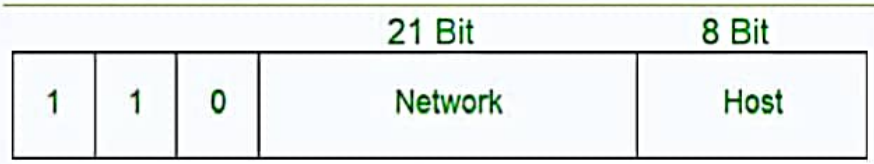
Class B:

- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.
  - The network ID is 16 bits long.
  - The host ID is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to 10.
- The remaining 14 bits are used to determine network ID.
- The 16 bits of host ID is used to determine the host in any network.
- The default sub-net mask for class B is 255.255.x.x.
- Class B has a total of:
  - 2^14 = 16384 network address
  - 2^16 – 2 = 65534 host address
- IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

Class B

Class C:

- IP address belonging to class C are assigned to small-sized networks.
  - The network ID is 24 bits long.
  - The host ID is 8 bits long.
- The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:
  - 2^21 = 2097152 network address
  - 2^8 – 2 = 254 host address
- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.



Class C

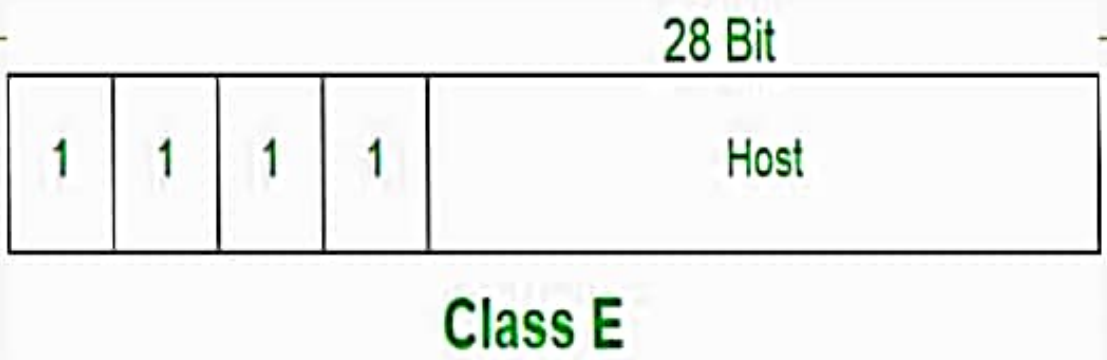
Class D:

- IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.

Class D

Class E:

- IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Class E

QoS is an overall performance measure of the computer network.

Important flow characteristics of the QoS are given below:

1. Reliability
If a packet gets lost or acknowledgement is not received (at sender), the re-transmission of data will be needed. This decreases the reliability.
The importance of the reliability can differ according to the application.
For example:
E- mail and file transfer need to have a reliable transmission as compared to that of an audio conferencing

2. Delay
Delay of a message from source to destination is a very important characteristic. However, delay can be tolerated differently by the different applications.
For example:
The time delay cannot be tolerated in audio conferencing (needs a minimum time delay), while the time delay in the e-mail or file transfer has less importance.

3. Jitter

The jitter is the variation in the packet delay.
If the difference between delays is large, then it is called as **high jitter.** On the contrary, if the difference between delays is small, it is known as **low jitter.**

Example:

Case1: If 3 packets are sent at times 0, 1, 2 and received at 10, 11, 12. Here, the delay is same for all packets and it is acceptable for the telephonic conversation.
Case2: If 3 packets 0, 1, 2 are sent and received at 31, 34, 39, so the delay is different for all packets. In this case, the time delay is not acceptable for the telephonic conversation.

4. Bandwidth

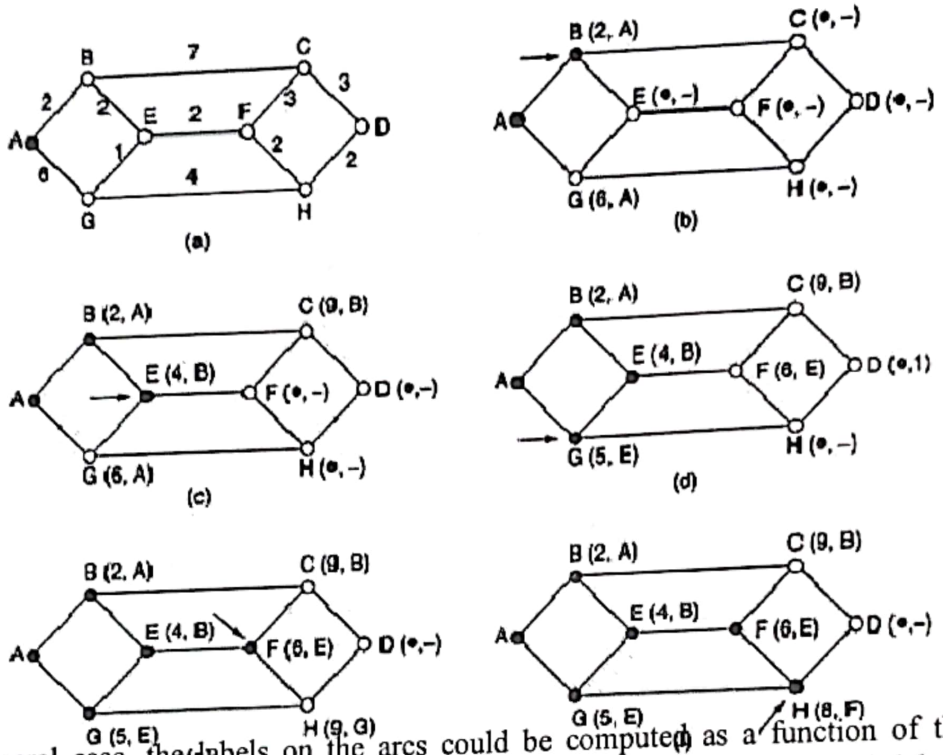
Different applications need the different bandwidth.
For example:
Video conferencing needs more bandwidth in comparison to that of sending an e-mail.

Shortest Path Routing

Let us begin our study of feasible routing algorithms with a technique that is widely used in many forms because it is simple and easy to understand. The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line (often called a link). To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

The concept of a **shortest path** deserves some explanation. One way of measuring path length is the number of hops. Using this metric, the paths ABC and ABE in the following figure are equally long. Another metric is the geographic distance in kilometers, in which case ABC is clearly much longer than ABE (assuming the figure is drawn to scale).

re : The first five steps used in computing the shortest path from A to D. The arrows indicate the working node.



In the general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, and other factors. By changing the weighting function, the algorithm would then compute the "shortest" path measured according to any one of a number of criteria or to a combination of criteria.

Several algorithms for computing the shortest path between two nodes of a graph are known. This one is due to Dijkstra (1959). Each node is labeled (in parentheses) with its distance from the source node along the best known path. Initially, no paths are known, so all nodes are labeled with infinity. As the algorithm proceeds and paths are found, the labels may change, reflecting better paths. A label may be either tentative or permanent. Initially, all labels are tentative. When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed thereafter.

To illustrate how the labeling algorithm works, look at the weighted, undirected graph of Fig. 5-7(a), where the weights represent, for example, distance. We want to find the shortest path from A to D. We start out by marking node A as permanent, indicated by a filled-in circle. Then we examine, in turn, each of the nodes adjacent to A (the working node), relabeling each one with the distance to A. Whenever a node is relabeled, we also label it with the node from which the probe was made so that we can reconstruct the final path later. Having examined each of the nodes adjacent to A, we examine all the tentatively labeled nodes in the whole graph and make

the one with the smallest label permanent, as shown in Fig. 5-7(b). This one becomes the new working node.

We now start at B and examine all nodes adjacent to it. If the sum of the label on B and the distance from B to the node being considered is less than the label on that node, we have a shorter path, so the node is relabeled.

After all the nodes adjacent to the working node have been inspected and the tentative labels changed if possible, the entire graph is searched for the tentatively-labeled node with the smallest value. This node is made permanent and becomes the working node for the next round. Figure 5-7 shows the first five steps of the algorithm.

To see why the algorithm works, look at Fig. 5-7(c). At that point we have just made E permanent. Suppose that there were a shorter path than ABE, say AXYZE. There are two possibilities: either node Z has already been made permanent, or it has not been. If it has, then E has already been probed (on the round following the one when Z was made permanent), so the AXYZE path has not escaped our attention and thus cannot be a shorter path.

Now consider the case where Z is still tentatively labeled. Either the label at Z is greater than or equal to that at E, in which case AXYZE cannot be a shorter path than ABE, or it is less than that of E, in which case Z and not E will become permanent first, allowing E to be probed from Z.

This algorithm is given in Fig. 5-8. The global variables n and dist describe the graph and are initialized before shortest_path is called. The only difference between the program and the algorithm described above is that in Fig. 5-8, we compute the shortest path starting at the terminal node, t, rather than at the source node, s. Since the shortest path from t to s in an undirected graph is the same as the shortest path from s to t, it does not matter at which end we begin (unless there are several shortest paths, in which case reversing the search might discover a different one). The reason for searching backward is that each node is labeled with its predecessor rather than its successor. When the final path is copied into the output variable, path, the path is thus reversed. By reversing the search, the two effects cancel, and the answer is produced in the correct order.

Link State Routing Protocols

Link state routing protocol is a type of network routing protocol. It maps the entire network, including the routers and the links between them. This map is called the link state database or topology table. The LSDB(Link State Database) is a very important component of a Link State Routing Protocol. It is a data structure that stores the topology of a network as known by a specific router running a Link State Routing Protocol.

Link state routing protocols exchange LSAs(Link State Advertisements) between routers. It contains information about the state of the links connected to each router. The LSAs are used to build and maintain a complete and up-to-date network map. It enables routers to calculate the shortest path to a destination.

Phases of Link State Routing

There are two primary phases in link state routing:

Phases of Link State Routing

There are two primary phases in link state routing:

Flooding Phase

In this phase, each router floods its own LSA to all other routers in the network. The LSA contains information about the router's own links. It also contains the state of its neighboring routers. Routers use the LSA to build their own LSDB and to update the database as changes occur in the network.

Calculation Phase

Once each router has received all LSAs from its neighbors and has built its own LSDB, it performs a shortest-path-first (SPF) calculation. It performs SPF to determine the best path to each destination in the network.

The SPF calculation considers the cost of each link. It also considers the state of each router in the LSDB. The result of the SPF calculation is used to build the forwarding table. This table contains the best path to each destination. This table is used to forward packets to their intended destination.

Algorithm for Link State Routing

The algorithm for Link State Routing involves the following steps:

1. **Discovery phase:** Each router sends out Hello packets to discover its neighbors and to establish a neighbor adjacency. Once a neighbor adjacency is established, routers exchange LSAs for learning about the state of the network.

2. **LSA flooding:** Each router floods its own LSA to all other routers in the network. The LSA consists of information about the router's own links and the state of its neighboring routers. Routers use the LSA to build their own LSDB and to update the database as changes occur in the network.

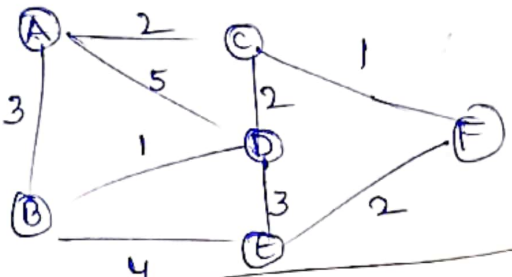
3. **Shortest Path First (SPF) calculation:** Once each router has received all LSAs from its neighbors and has built its own LSDB, it performs an SPF calculation which determines the best path to each destination in the network.
The SPF calculation considers the cost of each link and the state of each router in the LSDB. The result of the SPF calculation is used to build the forwarding table. This table contains the best path to each destination. This table is used to forward packets to their intended destination.

4. **Updating LSAs:** When a change occurs in the network, such as a link failure or adding a new router, the affected router floods a new LSA to all other routers in the network. This triggers a recalculation of the SPF algorithm, and the forwarding table is updated to reflect the new best path to each destination.

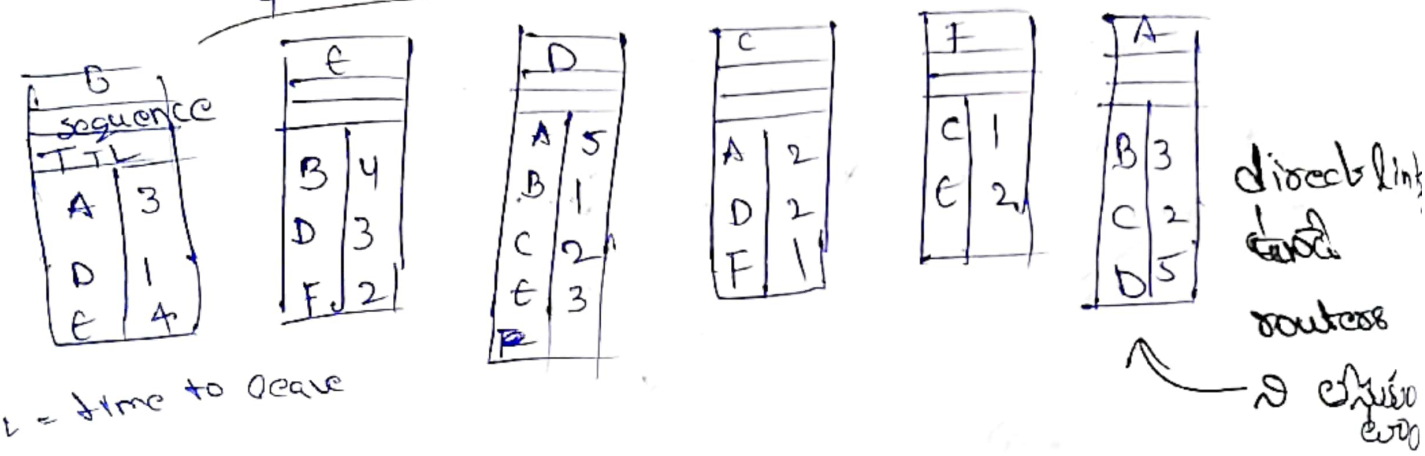
5. **Aging LSAs:** To prevent outdated LSAs from remaining in the LSDB, each router assigns a time-to-live (TTL) value to each LSA. When the TTL value expires, the router removes the LSA from its LSDB.

③ Link state routing algorithm

IMP



Link state routing packets



TTL = time to leave

Iteration	Destination	B	C	D	E	F
Initially	{A}	3	(2)	5	∞	∞
1	{A, C}	(3)	—	4	∞	3
2	{A, C, B}	—	—	4	7	(3)
3	{A, C, B, F}	—	—	(4)	5	—
4	{A, C, B, F, D}	—	—	—	5	—
5	{A, C, B, F, D, E}	—	—	—	—	—

4.4.10 Internet Control Protocols:

In addition to IP, which is used for data transfer, the Internet has several companion control protocols that are used in the network layer. They include ICMP, ARP, and DHCP.

3. IMCP—The Internet Control Message Protocol

The operation of the Internet is monitored closely by the routers. When something unexpected occurs during packet processing at a router, the event is reported to the sender by the **ICMP (Internet Control Message Protocol)**. ICMP is also used to test the Internet. About a dozen types of ICMP messages are defined. Each ICMP message type is carried encapsulated in an IP packet. The most important ones are listed in Fig. 5-60.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

Figure 5-60. The principal ICMP message types.

The DESTINATION UNREACHABLE message is used when the router cannot locate the destination or when a packet with the *DF* bit cannot be delivered because a ``small-packet'' network stands in the way.

The TIME EXCEEDED message is sent when a packet is dropped because it's *TTL (Time to live)* counter has reached zero. This event is a symptom that packets are looping, or that thecounter values are being set too low.

The PARAMETER PROBLEM message indicates that an illegal value has been detected in a header field. This problem indicates a bug in the sending host's IP software or possibly in the software of a router transited.

The SOURCE QUENCH message was long ago used to throttle hosts that were sending too many packets. When a host received this message, it was expected to slow down. It is rarely used anymore because when congestion occurs, these packets tend to add more fuel to the fire and it is unclear how to respond to them.

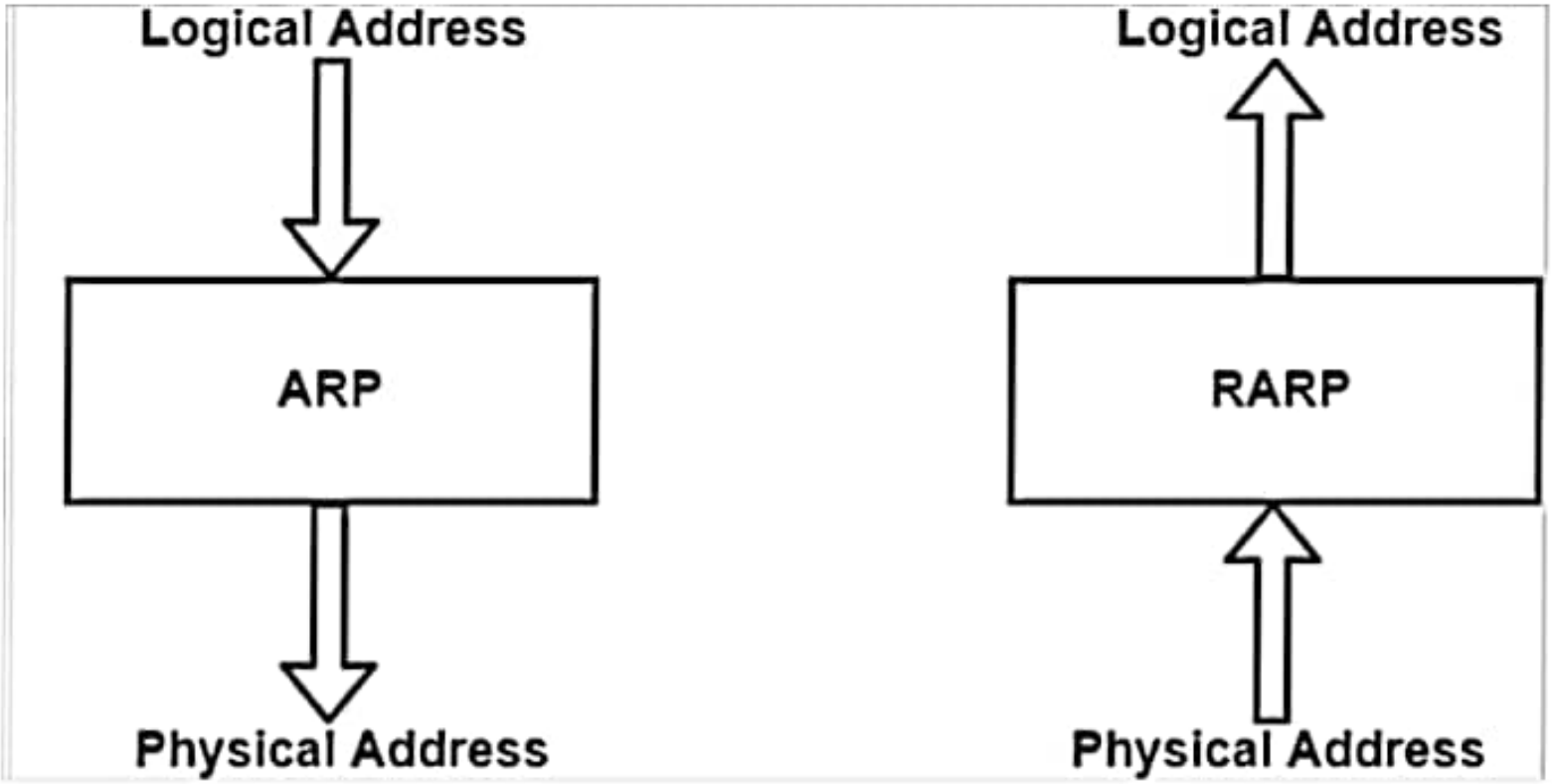
The REDIRECT message is used when a router notices that a packet seems to be routed incorrectly. It is used by the router to tell the sending host to update to a better route.

The ECHO and ECHO REPLY messages are sent by hosts to see if a given destination is reachable and currently alive. Upon receiving the ECHO message, the destination is expected to send back an ECHO REPLY message. These messages are used in the **ping** utility that checks if a host is up and on the Internet.

The TIMESTAMP REQUEST and TIMESTAMP REPLY messages are similar, except that the arrival time of the message and the departure time of the reply are recorded in the reply. This facility can be used to measure network performance.

The ROUTER ADVERTISEMENT and ROUTER SOLICITATION messages are used to let hosts find nearby routers. A host needs to learn the IP address of at least one router to be able to send packets off the local network.

Address Resolution Protocol (ARP) is a network-specific standard protocol. The Address Resolution Protocol is important for changing the higher-level protocol address (IP addresses) to physical network addresses. It is described in RFC 826.



ARP relates an IP address with the physical address. On a typical physical network such as LAN, each device on a link is identified by a physical address, usually printed on the network interface card (NIC). A physical address can be changed easily when NIC on a particular machine fails.

The IP Address cannot be changed. ARP can find the physical address of the node when its internet address is known. ARP provides a dynamic mapping from an IP address to the corresponding hardware address.

When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address.

5. DHCP—The Dynamic Host Configuration Protocol

With DHCP, every network must have a DHCP server that is responsible for configuration. When a computer is started, it has a built-in Ethernet or other link layer address embedded in the NIC, but no IP address. Much like ARP, the computer broadcasts a request for an IP address on its network. It does this by using a DHCP DISCOVER packet. This packet must reach the DHCP server. If that server is not directly attached to the network, the router will be configured to receive DHCP broadcasts and relay them to the DHCP server, wherever it is located.

When the server receives the request, it allocates a free IP address and sends it to the host in a DHCP OFFER packet (which again may be relayed via the router). To be able to do this work even when hosts do not have IP addresses, the server identifies a host using its Ethernet address (which is carried in the DHCP DISCOVER packet)

An issue that arises with automatic assignment of IP addresses from a pool is for how long an IP address should be allocated. If a host leaves the network and does not return its IP address to the DHCP server, that address will be permanently lost. After a period of time, many addresses may be lost. To prevent that from happening, IP address assignment may be for a fixed period of time, a technique called **leasing**. Just before the lease expires, the host must ask for a DHCP renewal. If it fails to make a request or the request is denied, the host may no longer use the IP address it was given earlier.