...2...
Routing Protocols

Learning Outcomes...

- Explain the mechanism of routing.
- Differentiate - Intra and Inter domain routing.
- Explain message structure of ICMP.

2.0 INTRODUCTION

- An Internet is a combination of networks connected by routers. Communication in the Internet today is not only unicasting; multicasting communication is growing fast.
- When a datagram goes from a source to a destination, it will probably pass through many routers until it reaches the router attached to the destination network.
- In unicasting, there is one source and one destination network. The relationship between the source and the destination network is one to one. Each router in the path of the datagram tries to forward the packet to one and only one of its interfaces.
- In multicasting, there is one source and a group of destinations. The relationship is one to many. In this type of communication, the source address is a unicast address, but the destination address is a group address, a group of one or more destination networks in which there, is at least one member of the group that is interested in receiving the multicast datagram.
- When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing.
- Routing is deciding the routes that packets travel in the network. Routing unicast data over the internet is called unicast routing. In multicast routing, the data is sent to only nodes which wants to receive the packets.
- Routing is done by special network devices called routers or it can be done by means of software processes.
- Routing is process of establishing the routes that data packets must follow to reach the destination. Effective routing ensures that data is transferred across networks in an efficient, reliable, and timely manner.
- There are two main forms of routing namely static and dynamic. Static routing uses manually configured routes, while dynamic routing uses algorithms and protocols to automatically adjust routes based on network conditions. **[S-22]**
- Static routing or non-adaptive routing follows user-defined routing. Dynamic routing or adaptive routing allows routers to choose paths based on changes in the logical network layout in real-time.
- A router receives a packet from a network and passes it to another network. In routing a routing table is created which contains information regarding routes which data packets follow. **[W-22]**
- A routing table can be either static routing table or dynamic routing table. A static routing table is one with manual entries while a dynamic routing table 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 example, they need to be updated when a link is down, and they need to be updated whenever a better route has been found.
- Routing protocols have been created in response to the demand for dynamic routing tables.
- A routing protocol is a combination of rules and procedures that lets routers in the internet inform each other of changes.
- A unicast routing protocol is optimized for processing unicast network information and provides routing intelligence for forwarding IP packets to unicast destination addresses.
- Multicast forwarding is conceptually different and requires special routing applications to support forwarding of multicast packets.
- Example of unicast routing protocol are Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (ISIS), Border Gateway Protocol (BGP), and so on.
- Multicast routing protocols are functionally different from unicast routing protocols, in that they build multicast forwarding state in the multicast-enabled routers by using a concept known as Reverse Path Forwarding (RPF).
- RPF is used to ensure that a multicast packet is received from the interface leading to the expected location of the multicast source, as dictated by the routing table in place.
- Examples of multicast routing protocol includes Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), Protocol independent Multicast (PIM), and so on.
- Routing protocols are the rules and procedures that routers use to communicate with each other and determine the best path for forwarding data across networks.

2.1 ROUTER ARCHITECTURE

- A router is a networking device that forwards data packets between computer networks. It performs two main functions namely, switching and queuing to ensure efficient packet delivery.
- One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.
- Following are the major uses of a router:
  1. **Multiple Network Connection:** It connects multiple networks and forwards data packets that are destined for direct or remotely attached networks.
  2. **Managing Congestion:** It manages traffic between networks by forwarding data packets to the destination address. It also allows multiple addresses to use the same internet connection.
  3. **Providing Connectivity:** Large routers interconnect several Internet Service Providers (ISPs). Small routers provide connectivity for homes and office networks.
  4. **Connecting Subnets:** Routers are used for connecting multiple logical groups of computer devices called subnets with the different network prefixes.
  5. **Port Forwarding:** They are also used for port forwarding among private ISPs.
  6. **Traffic Classification:** A router with the help of QoS, takes the decision on which data packet should be first processed.
- Router architecture refers to the design and organization of routers, which are responsible for forwarding packets in a network.
- Router architecture is designed in a way that the routers are equipped to perform two main functions. These functions are as follows:
  1. Process routable protocols.
  2. Use routing protocols to determine the best path.

- A router has four components namely, input ports, output ports, the routing processor, and the switching fabric, as shown in Fig. 2.1.

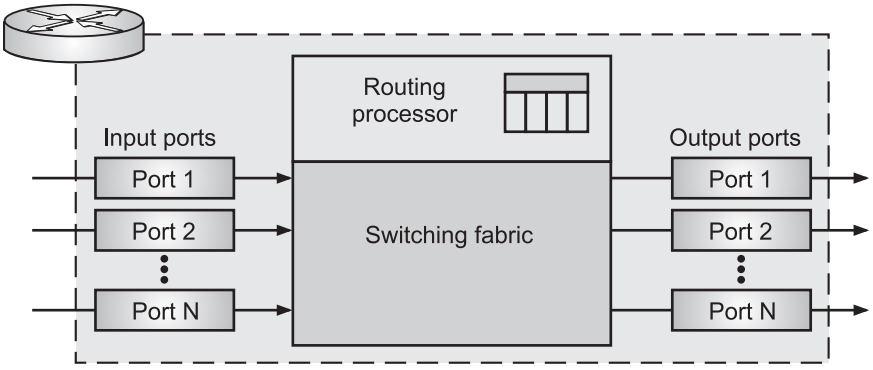


Fig. 2.1: Router Architectural Components

- Let us discuss components of router in detail:

Input port:

- It performs the physical and data link layer functions of the router. The bits are constructed from the received signal. The packet is decapsulated from the frame.
- Errors are detected and corrected. The packet is ready to be forwarded by the network layer.
- In addition to a physical layer processor and a data link processor, the input port has buffers (queues) to hold the packets before they are directed to the switching fabric.
- Fig. 2.2 shows the functioning of an input port in a router.

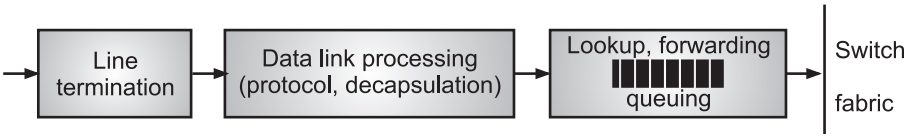


Fig. 2.2: Input Port

Output Ports:

- It performs the same functions as the input port, but in the reverse order.
- First the outgoing packets are queued, then the packet is encapsulated in a frame, and finally the physical layer functions are applied to the frame to create the signal to be sent on the line.
- Fig. 2.3 shows the functioning of an output port in a router.

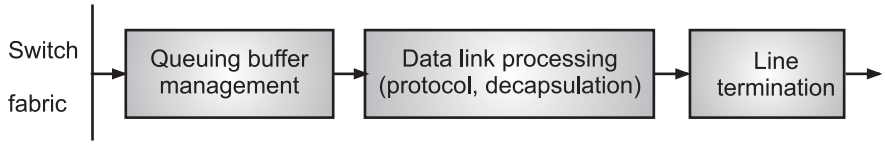


Fig. 2.3: Output Port

Routing Processor:

- It executes routing protocols. It maintains routing information and forwarding tables.
- It also performs network management functions within the router.

Switching Fabric:

- The switching fabric connects the router's input ports to its output ports.
- Switching fabric is the combination of hardware and software which moves data coming in to a network node out by the correct port to the next node in the network.
- Today, routers use a variety of switching fabrics such as crossbar switch, banyan switch and so on.

Types of Routers:

- The following are different types of routers that are used by individuals as well as enterprises:
  1. **Edge Router:**
     - Also known as a gateway router, it is a specialized router that acts as an intermediary between different networks. It resides at the edge of a network.
     - Edge ensures connectivity of its network with wide area network (WAN), internet or external networks. For connectivity with remote networks, Edge uses the network protocol External Border Gateway.
     - Edge routers have ethernet ports as inputs to connect with the internet and have multiple outputs for connecting additional routers.
  2. **Wireless Router:**
     - It is a device that acts as a router as well as a wireless access point. Such routers provide access to private computer networks or the internet.
     - Based on the model, it can function in either a wired local area network, wireless-only LAN or a mix of the wired and wireless network.
     - In functionality, they are a combination of edge and distribution routers. These routers have one or two USB ports that can be connected to a device and used as a shared resource on the network.
  3. **Virtual Router:**
     - It is a software-based framework with the same function as physical routers.
     - These routers run on commodity servers and are packaged either alone or with other network functions. However, they increase the reliability of a network through virtual redundancy protocol.
  4. **Distribution Router:**
     - It is a router in the local area network of a single organization.
     - Also known as an interior router, it receives data from Edge router via a wired connection and it sends this to the end user. This is usually done through Wi-Fi.
  5. **Core Router:**
     - It is a computer communication device that operates at the core of the internet. It links all network devices to provide multiple fast data communication interfaces.
     - Usually, service or cloud providers use core routers. This router provides maximum bandwidth to connect additional routers.
     - It supports multiple telecommunication interfaces of the highest speed and should be able to forward IP packets at full speed.

2.1.1 Routing Table

- A routing table is a set of rules that helps network devices decide the best path for data packets as they move from their source to a destination.
- 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 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.
- 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.

Destination	Subnet Mask	Interface
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 0.0.0.0.

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 of the following entries:
  - **Network ID:** The network ID or destination corresponding to the route.
  - **Subnet Mask:** The mask that is used to match a destination IP address to the network ID.
  - **Next Hop:** The IP address to which the packet is forwarded
  - **Outgoing Interface:** Outgoing interface the packet should go out to reach the destination network.
  - **Metric:** A common use of the metric is to indicate the *minimum number of hops* (routers crossed) to the network ID.
- A routing table can be either static or dynamic. A static table is one with manual entries. A dynamic table 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 example, they need to be updated when a link is down, and they need to be updated whenever a better route has been found.

2.1.2 Queueing and Switching

- Queuing and switching are crucial components of router architecture. **Switching** determines how packets move through the router, while **queuing** ensures proper packet scheduling and congestion control.
- Efficient queuing and switching mechanisms are essential for high-speed networks and Quality of Service (QoS).
- In routers queuing and switching are essential for managing network traffic. Queuing stores packets temporarily when the network is congested, while switching determines the path packets take to their destination.

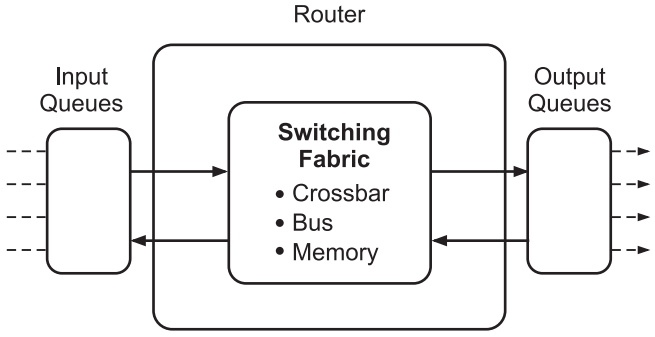


Fig. 2.4: Queuing and Switching in Router Architecture

Queuing in Router:

- The purpose of Queuing is to store packets temporarily when the arrival rate exceeds the departure rate, preventing packet loss due to congestion.
- Queuing is the process of storing packets in buffers before forwarding them. It helps manage congestion and ensures fair packet transmission.
- Types of Queuing in Routers are explained below:
  1. **FIFO (First-In-First-Out):**
     - The simplest form of queuing.
     - Packets are processed in the order they arrive.
     - No priority mechanism (can cause delays for important packets).
  2. **Priority Queuing (PQ):**
     - Assigns priority levels to packets.
     - Higher-priority packets are transmitted first.
     - Risk: Lower-priority packets might starve.
  3. **Weighted Fair Queuing (WFQ):**
     - Ensures fair distribution of bandwidth among different flows.
     - Packets are classified based on traffic type and assigned weights.
     - Efficient for multimedia applications.
  4. **Round Robin Queuing:**
     - Each queue gets an equal opportunity to send a packet.
     - Useful for ensuring fairness in resource allocation.

Switching in Router:

- Switching is the process of moving packets from the input interface to the appropriate output interface. The router follows a switching fabric to interconnect input and output ports efficiently.
- Types of Switching Fabrics in a router are given below:
  1. **Memory-Based Switching:**
     - The router stores incoming packets in memory before forwarding them.
     - Works like a CPU-based operation (older routers).
     - Slow and limited by memory speed.
  2. **Bus-Based Switching:**
     - A shared bus connects input and output ports.
     - Packets wait for their turn to be transmitted over the bus.
     - Faster than memory switching but suffers from congestion.
  3. **Crossbar-Based Switching:**
     - Uses a matrix to directly connect input ports to output ports.
     - Allows multiple packets to be switched simultaneously.
     - High-performance but expensive.

2.2 ROUTING PROTOCOLS [S-22]

- The Internet, nowadays is becoming more and more complex. Its size/growth as well as its technical and economical complexity both contribute to this phenomenon.
- Today, 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 the networks and the routers, which are operated under the authority of a single administration.

- In other words, the Internet consist of number of domains and each domain is called as Autonomous System managed independently.
- Routing inside an autonomous system is referred to as intra-domain routing. Each AS can choose its own intra-domain routing protocol. Distance vector and link state routing are the examples of Intra-domain routing.
- Routing between two or more autonomous systems can be referred to as inter-domain routing. Only one inter-domain routing protocol is usually used between ASs. Path vector is an example of an inter-domain routing.

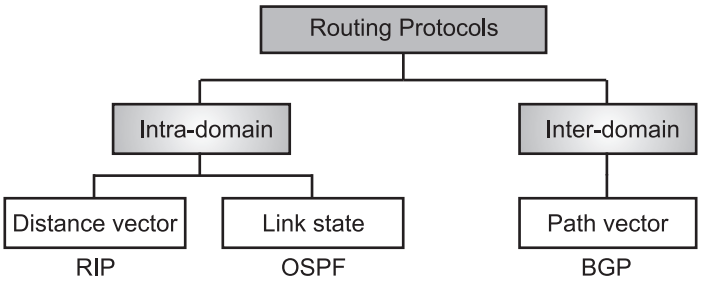


Fig. 2.5: Popular Routing Protocols

- Intra-domain routing algorithms route data packets within the same domain only while inter-domain routing algorithms route data packets between domains. Within a domain or AS, system administrators can select their own routing policy.
- Routing inside an Autonomous System (AS) is referred to as interior routing. RIP and OSPF are popular interior routing protocols used to update routing tables in an AS.
- Routing between autonomous systems is referred to as exterior routing. BGP is a popular protocol used in exterior routing.

Difference between Intra-Domain and Inter-Domain Routing:

Sr. No.	Intra-Domain Routing	Inter-Domain Routing
1.	Routing takes place within an autonomous network.	Routing takes place between the two autonomous networks.
2.	This protocol ignores the internet outside the autonomous system.	This protocol assumes that internet consists of a collection of interconnected autonomous systems.
3.	Protocols for Intra-domain routing are called as interior gateway protocols.	Protocol for Inter-domain routing are also called as exterior gateway protocols.
4.	For a packet that enters a domain, intra-domain routing will determine the route via which the packet will travel through to the border router connected to the next domain.	Inter-domain routing is the top-level routing. It determines the AS path each packet will travel through to its destination.
5.	Intra-domain multicast routing protocols, by which packets are multicast within a domain.	Inter-domain routing protocols, by which packets multicast among domains.
6.	In Interdomain Routing, Interior-gateway protocols such as RIP (resource information protocol) and OSPF (open shortest path first) are being used.	In Intradomain Routing, additional exterior-gateway protocols such as BGP (Border Gateway Protocol) are used.
7.	Interdomain Routing, as name suggests, is the protocol in which the Routing algorithm works within and in between the domains.	Intradomain Routing is a protocol in which the Routing algorithm works only within the domains.

- Routing protocols are sets of rules that routers use to exchange information and determine the best path for forwarding data packets across a network.
- They enable efficient and reliable communication by allowing routers to discover network destinations, maintain up-to-date routing tables, and make routing decisions.

Purpose of Routing Protocols:

- Routing protocols are essential for enabling data packets to travel efficiently and reliably across interconnected networks, ensuring they reach their intended destinations through the most optimal paths.

Function of Routing Protocols:

- They determine how routers communicate with each other to share information about network topology, allowing routers to dynamically adapt to changes like link failures or network congestion.

2.2.1 Intra-Domain Routing [W-22, S-24]

- Intra-domain routing protocols are used by routers within a network to determine the best path for forwarding packets to destinations within that same network.
- When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.
- Different routing algorithms use different methods to determine the best path. Routing is process of establishing the routes that data packets must follow to reach the destination.
- A routing algorithm specifies how packets choose the path to their destinations. There are two types of routing algorithms namely, deterministic and adaptive.
- In deterministic routing only one path is determined through source to destination, while adaptive routing algorithms allow multiple paths.
- Although deterministic routing is generally simple and fast, but it cannot tolerate even single node or link failure. Since adaptive routing algorithms can use multiple paths from source to destination.
- Adaptive routing usually requires additional network resources. To avoid using extra physical channels, a physical channel can be shared by several virtual channels.
- The routing algorithm can be classified into following two types: [W-23]

1. **Static (Non-Adaptive) Routing Algorithms:**

- In this type of algorithms, the network topology determines the final path. All the possible paths which are already calculated are loaded into the routing table.
- Static routing is suitable for small networks. The disadvantage of static routing is, inability to respond quickly in case of network failure.

2. **Dynamic (Adaptive) Routing Algorithms:** [W-23]

- The dynamic routing algorithms can change their routing decision on the basis of some changes made in the topology.
- Each router can check the network status by communicating with the neighbors. So, the changes in the topology are reflected to all routers.
- Finally, the router can calculate the suitable path to the final destination. The disadvantage of this type is, its complexity in the router.
- The "Distance Vector" and "Link State" are terms used to describe routing protocols which are used by routers to forward packets between networks.
- The purpose of any routing protocol is to dynamically communicate information about all network paths used to reach a destination and to select the from those paths, the best path to reach a destination network.

- The terms distance vector and link state are used to group routing protocols into two broad categories based on whether the routing protocol selects the best routing path based on a distance metric (the distance) and an interface (the vector), or selects the best routing path by calculating the state of each link in a path and finding the path that has the lowest total metric to reach the destination.

2.2.1.1 Distance Vector Routing [S-22, W-22, S-23, W-23, S-24, W-24]

- Distance vector routing algorithm is the dynamic routing algorithm in computer networks. Distance vector routing algorithm also known as Bellman-Ford routing algorithm (also called Ford-Fulkerson algorithm) to find the shortest path between nodes in a graph given the distance between nodes.
- It was designed for small network topologies. Distance Vector Routing (DVR) method sees an AS, with all routers and networks, as a graph, a set of nodes and lines (edges) connecting the nodes.
- A router can normally be represented by a node and a network by a link connecting two nodes, although other representations are also possible.
- In distance vector routing algorithm, node router constructs a table containing the distance (total cost of path) to all other nodes and distributes that vector to its immediate neighbors.
- For distance vector routing, it is assumed that each node knows the cost of the link to each of its directly connected neighbors.
- A link, which is 'down' (which is not working) is assigned as an infinite cost. Every node sends a message to its directly connected neighbors.
- For example: A sends its information to B and F.
- After communicating to each directly connected node the shortest path can be easy to compute (See Fig. 2.6).
- The shortest path can be computed as:

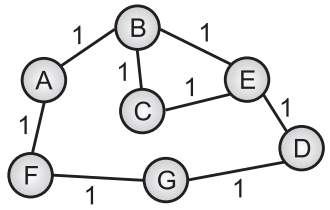


Fig. 2.6: Distance Vector Routing

Information at Node	Cost to Reach Node						
	A	B	C	D	E	F	G
A	0	1	2	2	2	1	2
B	1	0	1	2	1	2	2
C	2	1	0	2	1	2	2
D	2	2	2	0	1	2	2
E	2	1	1	1	0	2	2
F	1	2	2	2	2	0	1
G	2	2	2	1	2	1	0

- Distance vector routing protocols are like road signs because routers must make preferred path decisions based on a distance or metric to a network.
- Just as travelers trust a road sign to accurately state the distance to the next town, a distance vector router trusts that another router is advertising the true distance to the destination network.
- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance (mi).
- 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 in Fig. 2.7 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.

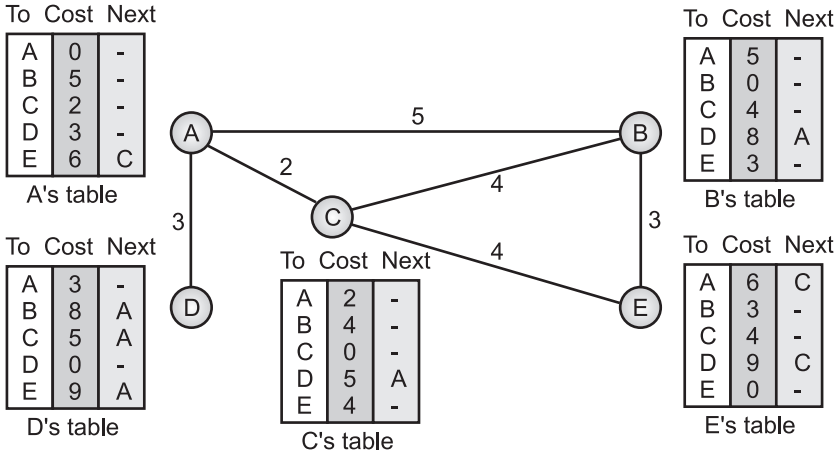


Fig. 2.7: Distance Vector Routing Tables

- **Initialization:** The tables in Fig. 2.7 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.

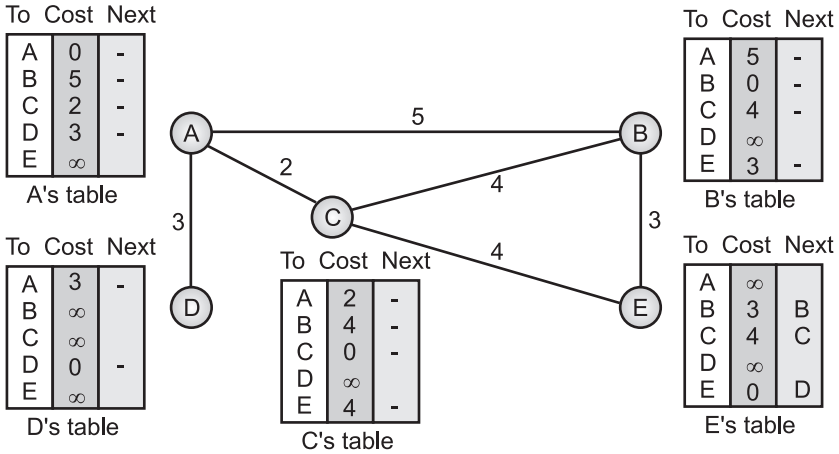


Fig. 2.8 (a): Initialization of Tables in Distance Vector Routing (DVR)

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

  Step 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.

  Step 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.

Step 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.

(i) 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.

(ii) 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 2.

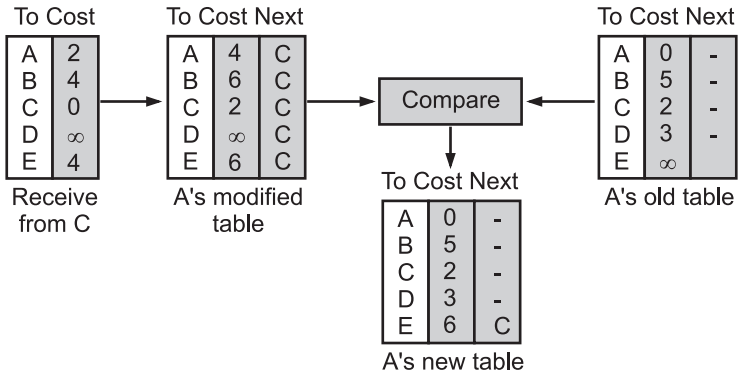


Fig. 2.8 (b): Updating Distance Vector Routing

Bellman-Ford Algorithm:

- The Bellman–Ford algorithm is an algorithm that computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph.
- Bellman-Ford algorithm solves single shortest path problem in which edge weight may be negative but no negative cycle exists.
- The Bellman–Ford algorithm works correctly when some of the edges of the directed graph G may have negative weight. When there are no cycles of negative weight, then we can find out the shortest path between source and destination.
- It is slower than Dijkstra's Algorithm but more versatile, as it capable of handling some of the negative weight edges. This algorithm detects the negative cycle in a graph and reports their existence.
- Based on the "Principle of Relaxation" in which more accurate values gradually recovered an approximation to the proper distance by until eventually reaching the optimum solution.
- Given a weighted directed graph G = (V, E) with source s and weight function w: E $\rightarrow$R, the Bellman-Ford algorithm returns a Boolean value indicating whether or not there is a negative weight cycle that is attainable from the source.
- If there is such a cycle, the algorithm produces the shortest paths and their weights. The algorithm returns TRUE if and only if a graph contains no negative - weight cycles that are reachable from the source.

Recurrence Relation:

distk [u] = [min[distk-1 [u],min[distk-1 [i]+cost [i,u]]] as i except u.

k $\rightarrow$ k is the source vertex

u $\rightarrow$ u is the destination vertex

i $\rightarrow$ no of edges to be scanned concerning a vertex.

- Bellman-Ford algorithm can be used in many applications in graph theory. Given a graph and a source vertex src in graph, find shortest paths from src to all vertices in the given graph. The graph may contain negative weight edges. Time complexity of this algorithm is O(VE) which is more than Dijkstra's algorithm O(VlogV) with the use of Fibonacci heap.

Input: Graph with source vertex src.

Output: Shortest distance to all vertices from src. If there is a negative weight cycle, then shortest distance are not calculated, negative weight cycle is reported.

Step 1: This step initializes distances from source to all vertices as infinite and distance to source itself is 0. Array dis[ ] of size v will keep these values.

Step 2: This step calculates shortest distances. Do following |v|-1 times.

Do following for each edge u-v

If dist[v] > dist[u] + weight of u-v then

dist[v]=dist[u] + weight of u-v

Step 3: This step reports if there is negative weight cycle in graph

Do the following for each edge u-v

If dist[v]>dist[u] + weight of edge u-v then

"Graph contains negative weight cycle"

- The sequence of steps in Bellmamm-Ford algorithm are given below:

BELLMAN-FORD(G, w, s)

1. INITIALIZE-SINGLE-SOURCE(G, s)
2. for i ← 1 to |V[G]| - 1
3. do for each edge (u, v) E[G]
4. do RELAX(u, v, w)
5. for each edge (u, v) E[G]
6. do if d[v] > d[u] + w(u, v)
7. then return FALSE
8. return TRUE

Examples:

Example 1: Fig. 2.9 shows a map with nodes and lines and the cost of each line is given over the line. Find the least cost between the nodes.

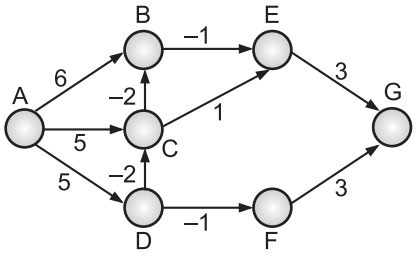


Fig. 2.9

Solution: List of edges: (a, b), (a, c), (a, d), (b, e), (c, b), (c, e), (d, c), (d, f), (e, g), (f, g).

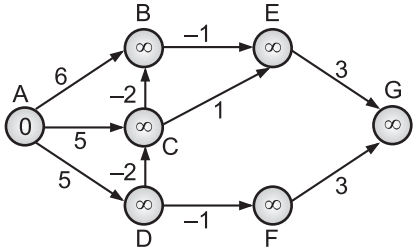


Fig. 2.10

Initially:

Node	A	B	C	D	E	F	G
Distance	0	.	.	.	.	.	.
Distance From							

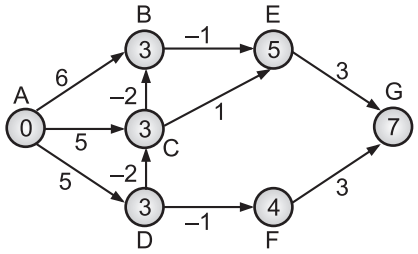


Fig. 2.11

Iteration 1:

Node	A	B	C	D	E	F	G
Distance	0	2	2	5	5	4	7
Distance From	0	C	D	A	B	D	F

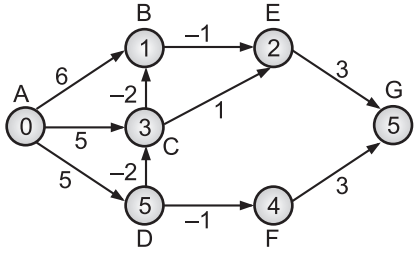


Fig. 2.12

Iteration 2:

Node	A	B	C	D	E	F	G
Distance	0	1	2	5	2	4	5
Distance From	0	C	D	A	B	D	E

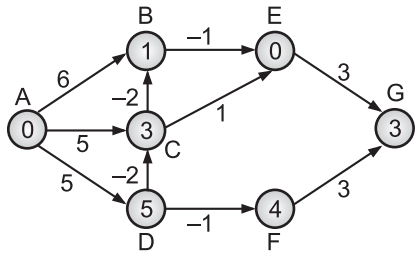


Fig. 2.13

Iteration 2:

Node	A	B	C	D	E	F	G
Distance	0	1	2	5	0	4	2
Distance From	0	C	D	A	B	D	E

Example 2: Fig. 2.14 shows a map with nodes and lines and the cost of each line is given over the line. Find the least cost between the nodes.

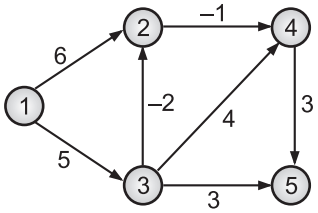


Fig. 2.14

Solution: Here, first we list all the edges and their weights.

Vertices →

No. of edges traversed ↑

	1	2	2	4	5
1	0	6	5	∞	∞
2	0	2	5	5	8
2	0	2	5	2	8
4	0	2	5	2	5

Example 3: Fig. 2.15 shows a map with nodes and lines and the cost of each line is given over the line. Find the least cost between the nodes.

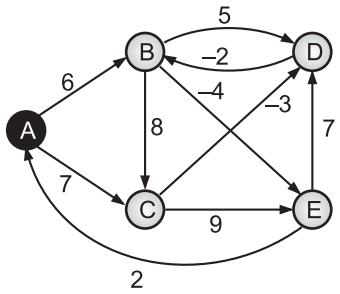


Fig. 2.15

Solution:

Step 1: Consider A as source index.

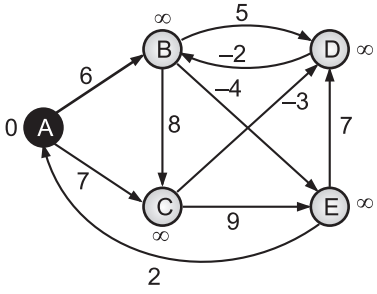


Fig. 2.16

No. of Nodes	A	B	C	D	E
Distance	0	6	7	∞	∞
Distance From	A	A	A		

Step 2: Consider Vertex B.

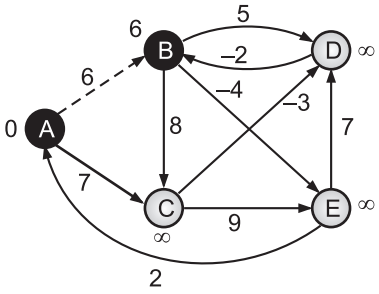


Fig. 2.17

No. of Nodes	A	B	C	D	E
Distance	0	6	7	11	2
Distance From	A	A	A	B	B

Step 3: Consider Vertex E.

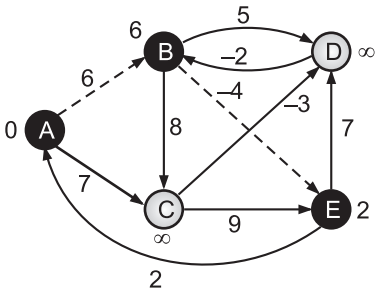


Fig. 2.18

No. of Nodes	A	B	C	D	E
Distance	0	6	7	9	2
Distance From	A	A	A	E	B

Step 4: Consider Vertex C.

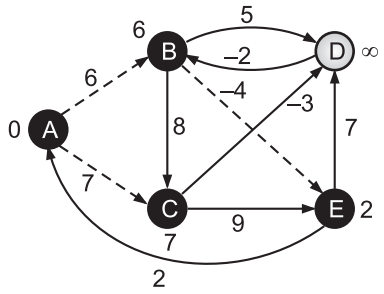


Fig. 2.19

No. of Nodes	A	B	C	D	E
Distance	0	6	7	4	2
Distance From	A	A	A	C	B

Step 5: Consider Vertex D.

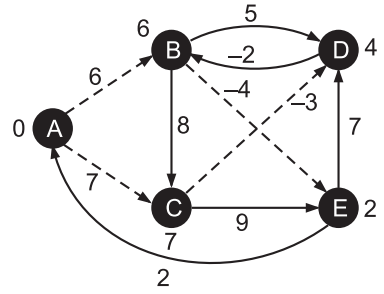


Fig. 2.20

No. of Nodes	A	B	C	D	E
Distance	0	2	7	4	2
Distance From	A	D	A	C	B

Step 6: Consider Vertex B.

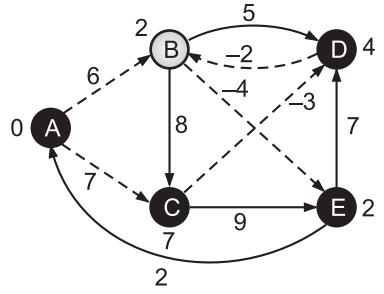


Fig. 2.21

No. of Nodes	A	B	C	D	E
Distance	0	2	7	4	–2
Distance From	A	D	A	C	B

Step 7: Consider Vertex E.

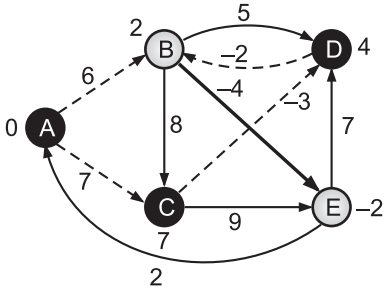


Fig. 2.22

No. of Nodes	A	B	C	D	E
Distance	0	2	7	4	–2
Distance From	A	D	A	C	B

Result:

Vertex	Distance From A
A	0
B	2
C	7
D	4
E	–2

2.2.1.2 Routing Information Protocol (RIPv2) [S-22, W-22, W-23, W-24]

- The Routing Information Protocol (RIP) is an intra-domain (interior) routing protocol used inside an autonomous system.
- The RIP is a protocol used to propagate routing information inside an autonomous system. Today, the Internet is so large that one routing protocol cannot handle the task of updating the routing tables of all routers.
- RIP is a distance vector routing protocol which uses Bellman-Ford algorithm for calculating routing tables and works on the application layer of OSI model. RIP uses port number 520.
- Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.

Concept of Hop Count:

- A hop is one portion of the path between source and destination. Data packets pass through bridges, routers and gateways as they travel between source and destination. Each time packets are passed to the next network device, a hop occurs.
- Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table.
- RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.
- In other words, the hop count refers to the number of intermediate devices through which data must pass between source and destination.
- Fig. 2.23 shows hops in a network. The hop count between the computers in this case is 2.

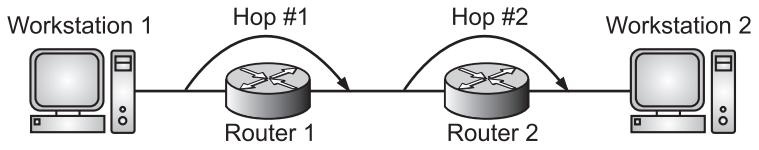


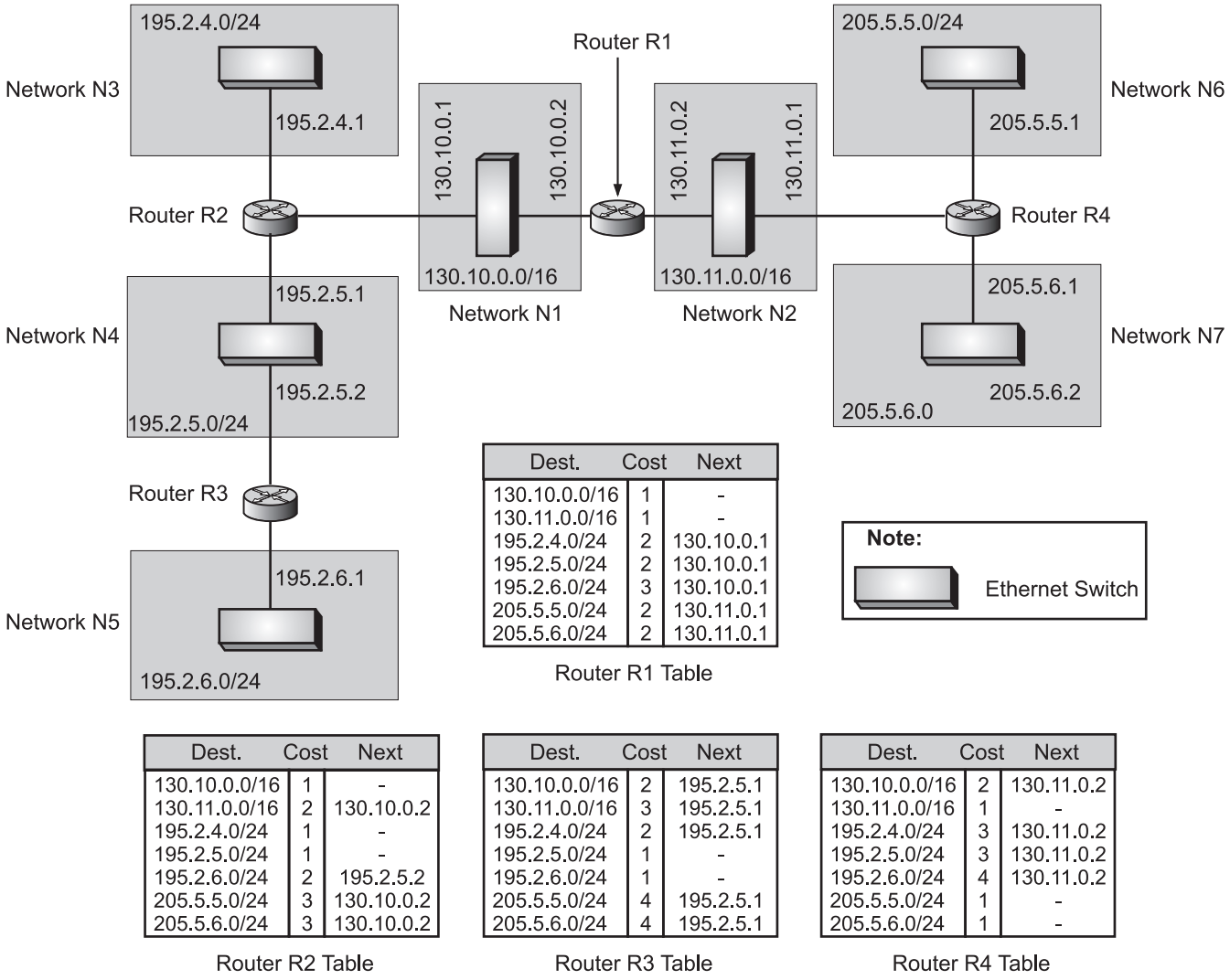
Fig. 2.23

Features of RIP:

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

Working Example of RIP:

- Fig. 2.24 shows an autonomous system with seven networks and four routers. The routing table for R1 has seven entries to show how to reach each network in the autonomous system.
- Router R1 is directly connected to networks 120.10.0.0 and 120.11.0.0, which means that there are no next hop entries for these two networks.
- To send a packet to one of the three networks at the far left, router R1 needs to deliver the packet to R2. The next node entry for these three networks is the interface of router R2 with IP address 120.10.0.1.
- To send a packet to the two networks at the far right, router R1 needs to send the packet to the interface of router R4 with IP address 120.11.0.1. The other tables can be explained similarly.



Dest.	Cost	Next
130.10.0.0/16	1	-
130.11.0.0/16	1	-
195.2.4.0/24	2	130.10.0.1
195.2.5.0/24	2	130.10.0.1
195.2.6.0/24	3	130.10.0.1
205.5.5.0/24	2	130.11.0.1
205.5.6.0/24	2	130.11.0.1

Router R1 Table

Dest.	Cost	Next
130.10.0.0/16	1	-
130.11.0.0/16	2	130.10.0.2
195.2.4.0/24	1	-
195.2.5.0/24	1	-
195.2.6.0/24	2	195.2.5.2
205.5.5.0/24	3	130.10.0.2
205.5.6.0/24	3	130.10.0.2

Router R2 Table

Dest.	Cost	Next
130.10.0.0/16	2	195.2.5.1
130.11.0.0/16	3	195.2.5.1
195.2.4.0/24	2	195.2.5.1
195.2.5.0/24	1	-
195.2.6.0/24	1	-
205.5.5.0/24	4	195.2.5.1
205.5.6.0/24	4	195.2.5.1

Router R3 Table

Dest.	Cost	Next
130.10.0.0/16	2	130.11.0.2
130.11.0.0/16	1	-
195.2.4.0/24	3	130.11.0.2
195.2.5.0/24	3	130.11.0.2
195.2.6.0/24	4	130.11.0.2
205.5.5.0/24	1	-
205.5.6.0/24	1	-

Router R4 Table

Fig. 2.24: Example of Domain using RIP

RIP Message Format of RIP: **[W-23]**

- Fig. 2.25 shows message format of RIP.

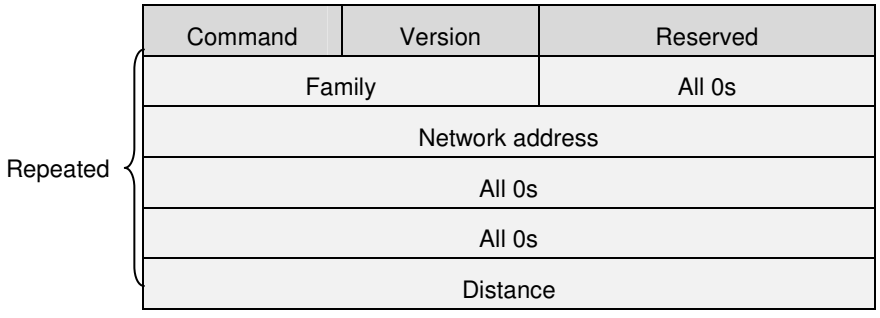


Fig. 2.25: RIP Message Format

- Various fields in message format of RIP are explained below:
  1. **Command:** This 8-bit field specifies the type of message i.e., request (1) or response (2).
  2. **Version:** This 8-bit field defines the version.
  3. **Family:** This 16-bit field defines the family of the protocol used. For TCP/IP the value is 2.
  4. **Network Address:** The address field defines the address of the destination network. RIP has allocated 14 bytes for this field to be applicable to any protocol. However, IP currently uses only 4 bytes. The rest of the address is filled with 0s.

5. **Distance:** This 22-bit field defines the hop count (cost) from the advertising router to the destination network.

- RIP has two types of messages namely, request and response as explained below:
  1. **Request:** A request message is sent by a router that has just come up or by a router that has some time-out entries. A request can ask about specific entries or all entries.
  2. **Response**: A response can be either solicited or unsolicited. A solicited response is sent only in answer to a request. It contains information about the destination specified in the corresponding request. An unsolicited response, is sent periodically, every 20 seconds or when there is a change in the routing table. The response is sometimes called an update packet.

RIP Version 2:

- RIP version 2 was designed to overcome some of the shortcomings of RIP version 1. The designers of version 2 have not augmented the length of the message for each entry.
- They have only replaced those fields in version 1 that were filled with 0s for the TCP/IP protocol with some new fields.

Message Format of RIP Version 2:

- Fig. 2.26 shows message format of RIP version 2.

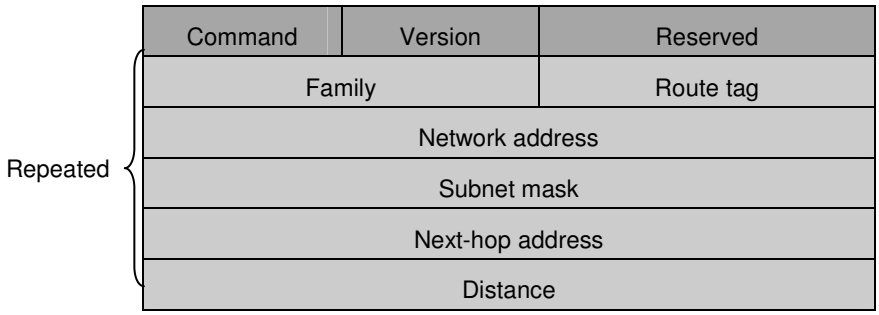


Fig. 2.26: RIP Version 2 Format

- The new fields of RIP version 2 message are as follows:
  1. **Route Tag**: This field carries information such as the autonomous system number. It can be used to enable RIP to receive information from an inter-domain routing protocol.
  2. **Subnet Mask:** This is a 4-byte field that carries the subnet mask (or prefix). This means that RIP version 2 supports classless addressing and CIDR.
  3. **Next-hop Address**: This field shows the address of the next hop. This is particularly useful if two autonomous systems share a network (a backbone, for example). Then the message can define the router, in the same autonomous system or another autonomous system, to which the packet next goes.

Difference between RIPv1 and RIPv2:

Sr. No.	RIPv1	RIPv2
1.	It uses broadcast for routing update.	It uses multicast for routing update.
2.	It sends broadcast on 255.255.255.255 destination.	It sends multicast on 224.0.0.9 destination.
3.	It does not support VLSM (Variable Length Subnet Masking).	It supports VLSM.
4.	It does not support any authentication.	It supports MD5 authentication.
5.	It only supports classful routing.	It supports both classful and classless routing.

Contd...

6.	It does not support discontinuous network.	It supports discontinuous network.
7.	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.
8.	RIPv1 routing updates are broadcasted.	RIP v2 routing updates are multicasted.
9.	RIP v1 does not carry mask in updates.	RIP v2 does carry mask in updates, so it supports for VLSM.
10.	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 usag.e

2.2.1.3 Link State Routing [W-22, W-23, S-24]

- Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork. 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.

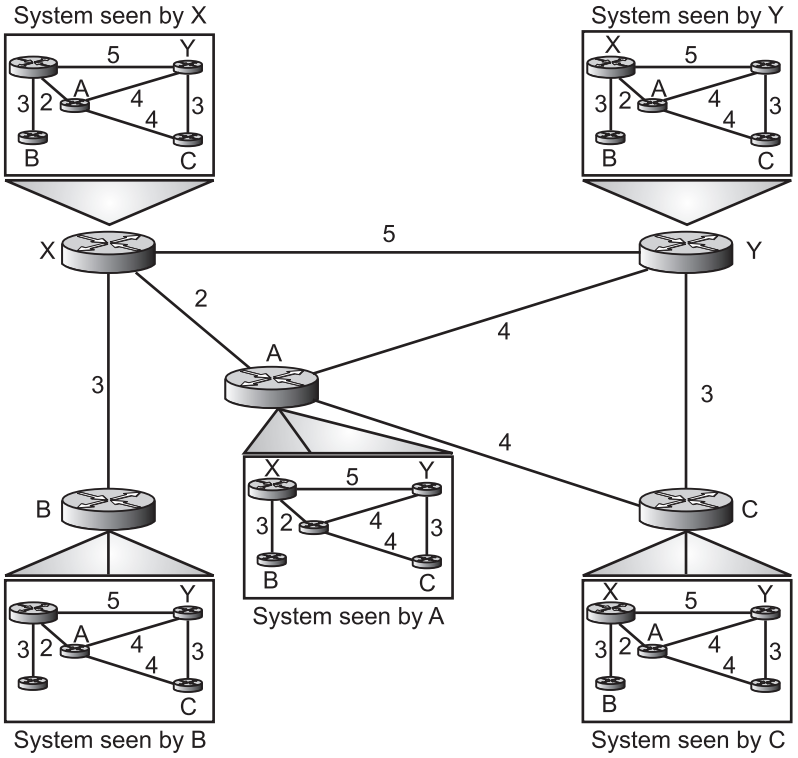


Fig. 2.27: Concept of Link State Routing (LSR)

- Link state routing protocols are more like a road map because they create a topological map of the network and each router uses this map to determine the shortest path to each network.
- Just as you refer to a map to find the route to another town, link-state routers use a map to determine the preferred path to reach another destination.
- Routers running a link state routing protocol send information about the state of its links to other routers in the routing domain.

- The state of those links refers to its directly connected networks and includes information about the type of network and any neighboring routers on those networks-hence the name link state routing protocol.

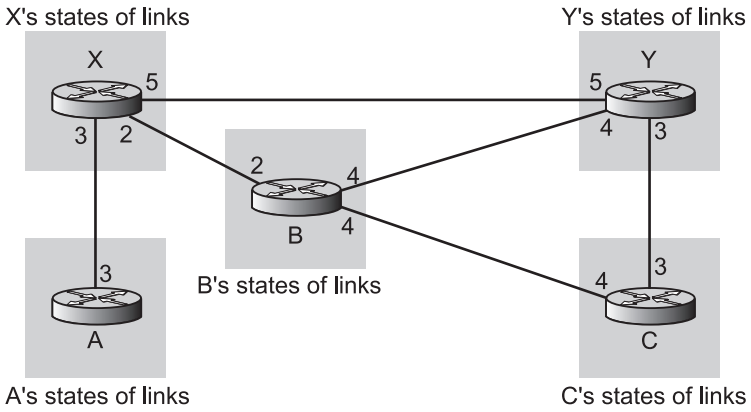


Fig. 2.28: Link State Knowledge

- The Fig. 2.28 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 the routing table showing the least-cost node to every other node.
- Creation of the states of the links by each node, called the link state packet or LSP.
- Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
- Formation of a shortest path tree for each node.
- Calculation of a routing table based on the shortest path tree.

Formation of Shortest Path Tree: Dijkstra Algorithm:

- A tree is a graph of nodes and links; one node is called the root. All other nodes can be reached from the root through only one single route.
- A shortest path tree is a tree in which the path between the root and every other node is the shortest. What we need for each node is a shortest path tree with that node as the root.
- The Dijkstra algorithm is used to create a shortest path tree from a given graph. The algorithm uses the following steps:
  - **Initialization:** Select the node as the root of the tree and add it to the path. Set the shortest distances for all the root's neighbors to the cost between the root and those neighbors. Set the shortest distance of the root to zero.
  - **Iteration:** Repeat the following two steps until all nodes are added to the path:
    1. **Adding the next node to the path:** Search the nodes not in the path. Select the one with minimum shortest distance and add it to the path.
    2. **Updating:** Update the shortest distance for all remaining nodes using the shortest distance of the node just moved to the path in step 2.
  - Dj = minimum (Dj, Di + cij) for all remaining nodes

Dijkstra Algorithm:

```
Dijkstra ( )
{
// Initialization
```

```
Path = {s}              // s means self
for (i = 1 to N)
{
if(i is a neighbor of s and I≠ s)   Di= csi
if (i is not a neighbor of s)       Di=∞
}
Ds = 0
} // Dijkstra
// Iteration
Repeat
{
// Finding the next node to be added
Path = Path ∪ i if Di is minimum among all remaining nodes
// Update the shortest distance for the rest
for (j = 1 to M)              // M number of remaining nodes
{
Dj = minimum (Dj , Dj + cij)
}
} until (all nodes included in the path, M = 0)
```

Examples:

Example 1: Fig. 2.29 shows the formation of the shortest path tree for the graph of seven nodes. In the initialization step, node A selects itself as the root. It then assigns shortest path distances to each node on the topology. The nodes that are not neighbors of A receive a shortest path distance value of infinity.

Solution: In each iteration, the next node with minimum distance is selected and added to the path. Then all shortest distances are updated with respect to the last node selected. For example, in the first iteration, node B is selected and added to the path and the shortest distances are updated with respect to node B (The shortest distances for C and E are changed, but for the others remain the same). After six iterations, the shortest path tree is found for node A. Note that in iteration 4, the shortest path to G is found via C, but in iteration 5, a new shortest route is discovered (via G); the previous path is erased and the new one is added.

Calculation of Routing Table from Shortest Path Tree (SPT):

Each node uses the shortest path tree found in the previous discussion to construct its routing table. The routing table shows the cost of reaching each node from the root. Routing table for node A using the shortest path tree found in above Fig. 2.29.

Destination	Cost	Next Router
A	0	–
B	2	–
C	7	B
D	2	–
E	6	B
F	8	B
G	9	B

Fig. 2.29: Routing Table for Node A

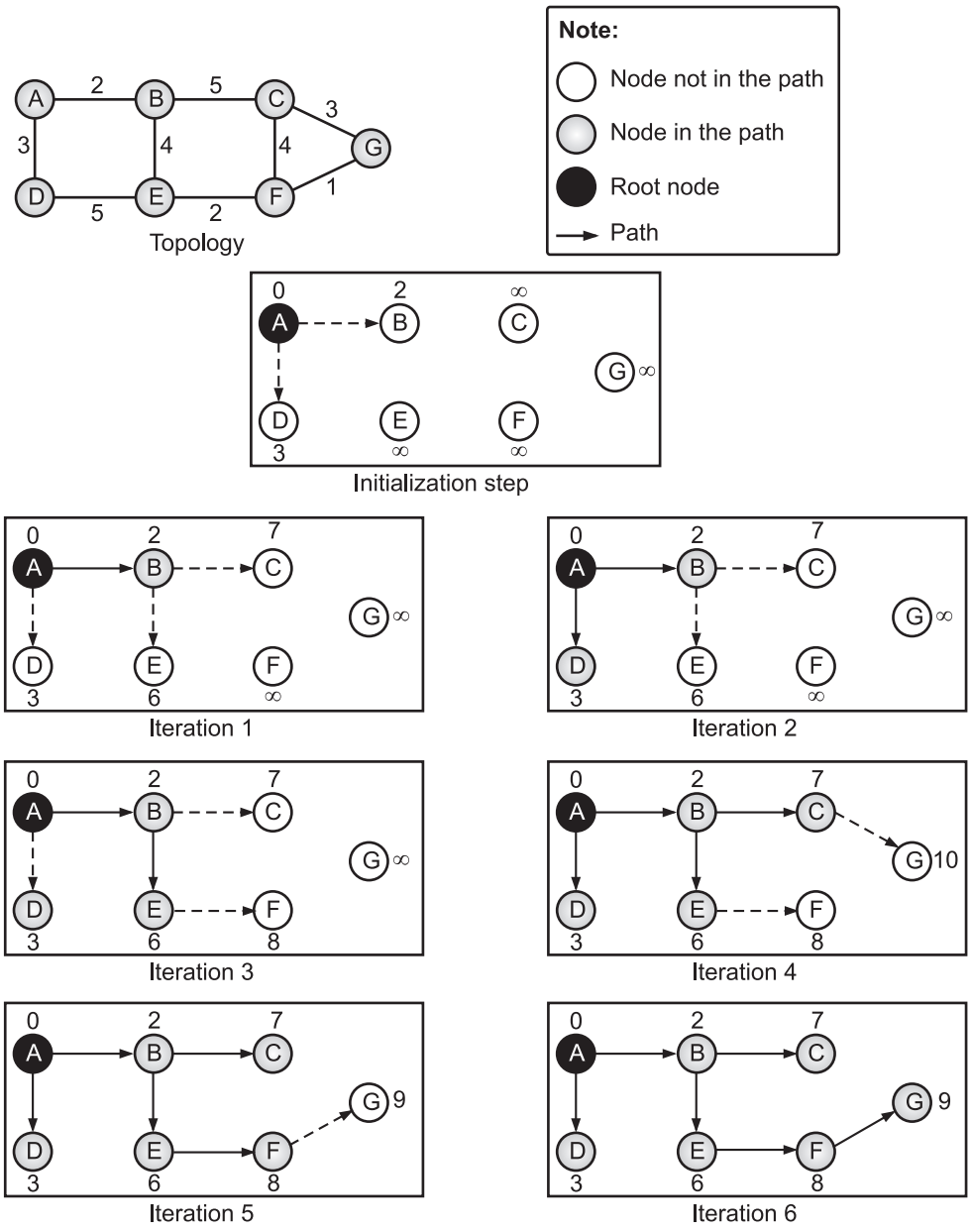


Fig. 2.30

Example 2: Consider Fig. 2.31. Find the shortest path.

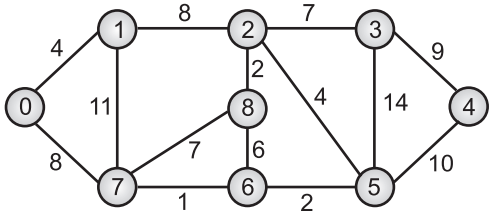


Fig. 2.31

Solution:

The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with minimum distance value. The vertex 0 is picked, include it in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update distance values of its adjacent vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8. The vertices included in SPT are shown in black colour, (See Fig. 2.32).

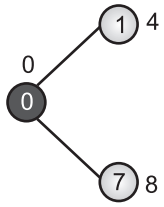


Fig. 2.32

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12, (See Fig. 2.33).

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7. The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively), (See Fig. 2.34).

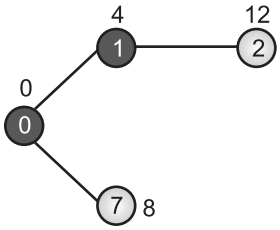


Fig. 2.33

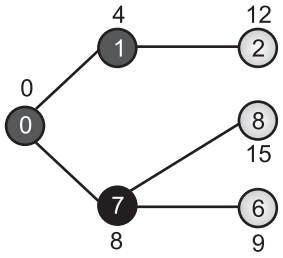


Fig. 2.34

Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6, (See Fig. 2.35). The distance value of vertex 5 and 8 are updated.

We repeat the above steps until sptSet doesn't include all vertices of given graph. Finally, we get the Shortest Path Tree (SPT) as shown in Fig. 2.36.

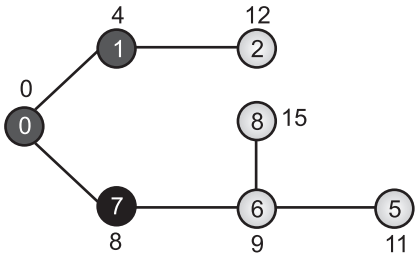


Fig. 2.35

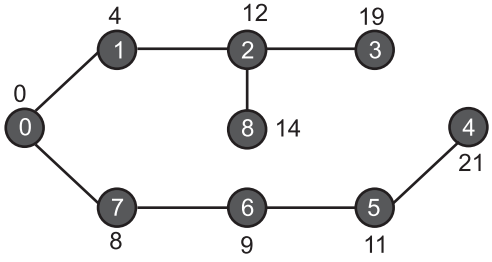


Fig. 2.36

Difference between Distance Vector Routing and Link State Routing:

Sr. No.	Distance Vector Routing	Link State Routing
1.	The distance vector routing determines the direction (vector) and distance (such as link cost or number of hops) to any link in the network.	The link state routing uses the Shortest Path First (SPF) algorithm to create an abstract of the exact topology of the entire network.
2.	Distance vector routing protocols do not have an actual map of the network topology.	A link state routing protocol is like having a complete map of the network topology.
3.	The distance vector routing algorithm is a type of routing algorithm that is based on the number of hops in a route between a source and destination computer.	The link state routing algorithm broadcasts information about the cost of reaching each of its neighbors to all other routers in the network.
4.	Uses Bellman-Ford algorithm.	Uses Dijkstra's algorithm.

Contd...

5.	The name 'distance vector' is used because the routers exchange vectors containing distance and direction information.	In link state routing, each routing node makes a connectivity graph for the nodes in the network and independently calculates its shortest path to every other destination in the network.
6.	Less bandwidth is required.	High bandwidth is required.
7.	Distance vector routing updates full routing table.	Link state routing updates only the link state.
8.	Example of distance vector routing protocols is RIP.	Example of link state routing protocols is OSPF.
9.	The utilization of CPU and memory in distance vector routing is lower than the link state routing.	Higher utilization of CPU and memory.
10.	Distance vector routing does not have any hierarchical design.	Link state routing works best for hierarchical routing design and in networks where fast convergence is crucial.

2.2.1.4 Open Shortest Path First (OSPF) [W-22, W-24]

- The Open Shortest Path First (OSPF) is a new alternative to RIP as an interior routing protocol. It overcomes all the limitations of RIP.
- OSPF uses link state routing to update the routing tables in an area, as opposed to RIP which is a distance vector protocol.
- The OSPF protocol is an intra domain routing protocol based on link state routing. Its domain is also an autonomous system.
- OSPF is a routing protocol used to determine the best route for delivering the packets within an IP networks. OSPF is a link state routing protocol, whereas RIP is distance vector routing protocols.
- OSPF use the Dijkstra algorithm to initially construct a shortest path tree and follows that by populating the routing table with the resulting best route.
- In 1998, the current version of OSPF for IPv4 is OSPFv2 introduced in RFC 1247 and updated in RFC 2228 by John Moy. In 1999, OSPFv2 for IPv6 was published in RFC 2740.
- OSPF divides an autonomous system into areas. An area is defined as, a collection of networks, hosts, and routers all contained within an autonomous system.
- Routers inside an area flood the area with routing information. At the border of an area, special routers called area border routers summarize the information about the area and send it to other areas.

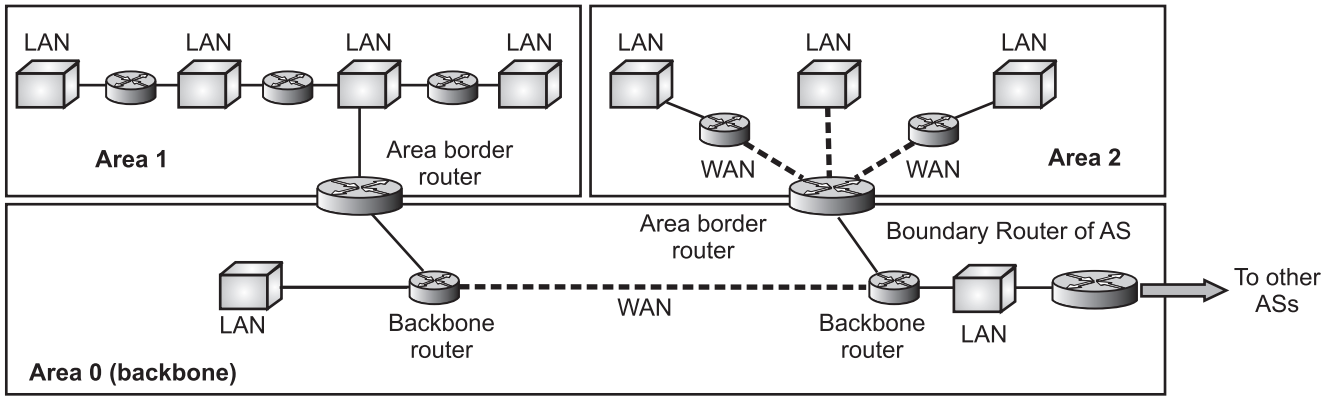


Fig. 2.37

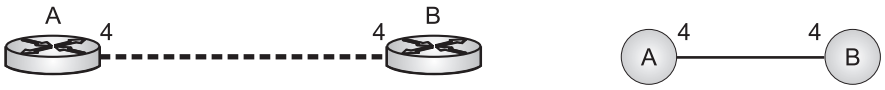
- Among the areas inside an autonomous system is a special area called the backbone; all of the areas inside an autonomous system must be connected to the backbone.
- In other words, the backbone serves as a primary area and the other areas as secondary areas. The routers inside the backbone are called the backbone routers.
- The connectivity between a backbone and an area is broken, a virtual link between routers must be created by the administration to allow continuity of the functions of the backbone as the primary area.
- Each area in OSPF has an area identification. The area identification of the backbone is zero. Fig. 2.37 shows an autonomous system and its areas.

2.2.1.4.1 Types of Links

- In OSPF terminology, a connection is called a link. OSPF defines four types of links namely, point-to-point, transient, stub and virtual.

1. Point-to-point Link:

- 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.
- Point-to-point links between routers do not need an IP address at each end. Unnumbered links can save IP addresses.



(a) Point-to-point Network **(b) Representation**

Fig. 2.38: Point-to-point links

2. Transient Link:

- A transient link is a network with several routers attached to it. A stub link is a network that is connected to only one router. A transient link is a network with several routers attached to it.
- The data can enter through any of the routers and leave through any router. All LANs and some WANs with two or more routers are of this type.

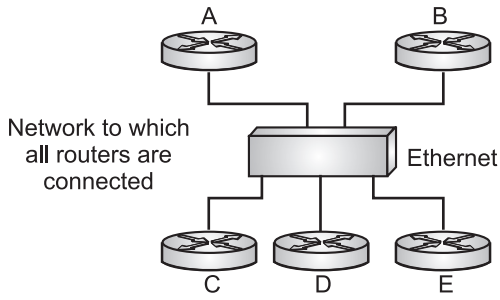


Fig. 2.39: Transient Link

3. Stub Link:

- A stub link is a network that is connected to only one router. The data packets enter the network through this single router and leave the network through this same router. This is a special case of the transient network.
- We can show this situation using the router as a node and using the designated router for the network. However, the link is only one directional, from the router to the network

(a) Stub Network **(b) Representation**

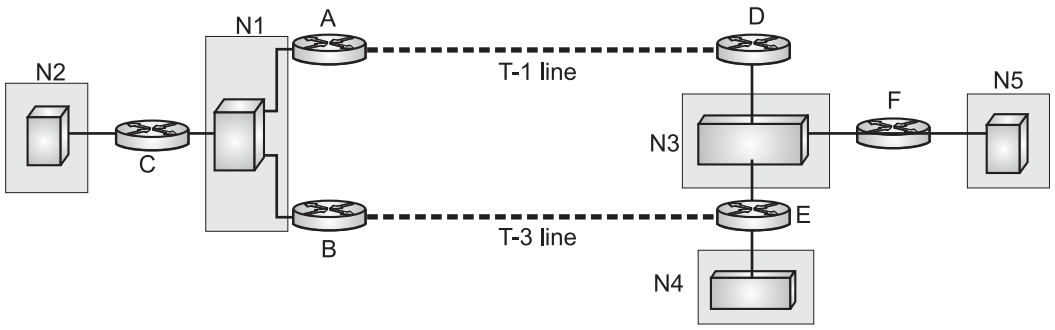
Fig. 2.40: Stub Link

4. Virtual Link:

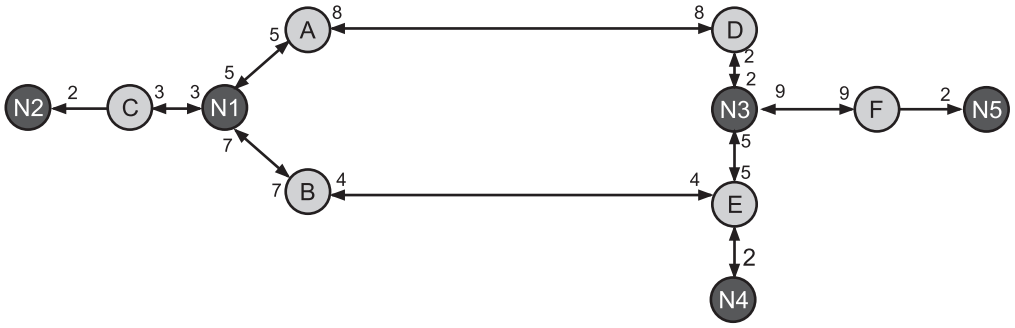
- When the link between two routers is broken, the administration may create a virtual link between them using a longer path that probably goes through several routers.

2.2.1.4.2 Graphical Representation

- Now we examine how an AS can be represented graphically. Fig. 2.41 shows a small AS with seven networks and six routers. Two of the networks are point-to-point networks.
- We use symbols such as N1 and N2 for transient and stub networks. There is no need to assign an identity to a point-to-point network.
- The Fig. 2.41 also shows the graphical representation of the AS as seen by OSPF.
- We have used color nodes for the routers and shaded nodes for the networks (represented by designated routers). However, OSPF sees both as nodes. Note that we have three stub networks.



(a) Autonomous System



(b) Graphical Representation

Fig. 2.41: Example of an AS and its Graphical Representation in OSPF

2.2.1.4.3 OSPF Packets

- OSPF uses five different types of packets such as hello, database description, link state request, link state update, and link state acknowledgment.

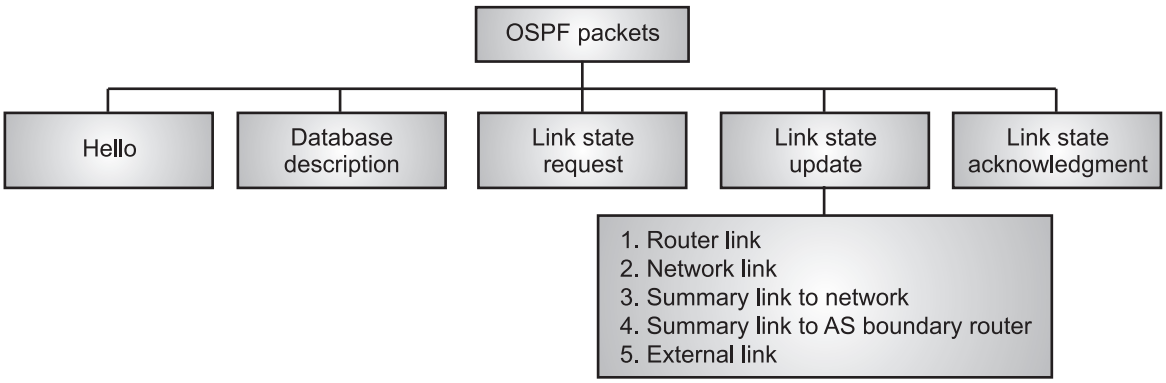


Fig. 2.42: Types of OSPF Packet

- Various types of OSPF packets in Fig. 2.42 are explained below:
  1. **Hello:** Establishes and maintains neighbor relationships.
  2. **Database Description:** Describes the contents of the topological database. These messages are exchanged when an adjacency is initialized.
  3. **Link State Request:** Requests pieces of the topological database from neighbor routers. These messages are exchanged after a router discovers, (by examining database-description packets) that parts of its topological database are out of date.
  4. **Link State Update:** Responds to a link state request packet. These messages also are used for the regular dispersal of Link State Acknowledgments (LSA). Several LSAs can be included within a single link-state update packet.
  5. **Link State Acknowledgment:** Acknowledges link state update packets.

2.2.1.4.4 OSPF Common Header

- Fig. 2.43 shows common header of OSPF.

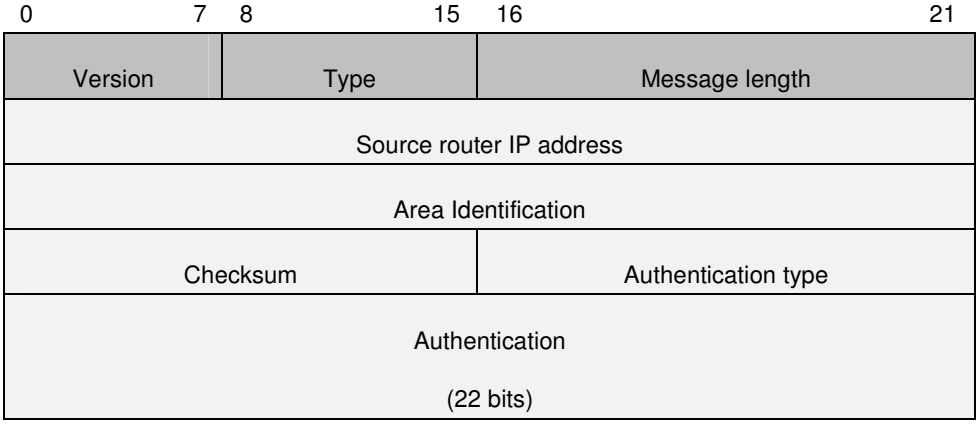


Fig. 2.43: OSPF Common Header

- All OSPF packets have the same common header. The various fields in OSPF common header are explained below:
  1. **Version**: This 8-bit field defines the version of the OSPF protocol. It is currently version 2.
  2. **Type**: This 8-bit field defines the type of the packet. As we said before, we have five types, with values 1 to 5 defining the types.
  3. **Message Length:** This 16-bit field defines the length of the total message including the header.
  4. **Source Router IP Address:** This 22-bit field defines the IP address of the router that sends the packet.

5. **Area Identification**: This 22-bit field defines the area within which the routing takes place.
6. **Checksum**: This field is used for error detection on the entire packet excluding the authentication type and authentication data field.
7. **Authentication Type**: This 16-bit field defines the authentication protocol used in this area. At this time, two types of authentication are defined: 0 for none and 1 for password.
8. **Authentication**: This 64-bit field is the actual value of the authentication data. In the future, when more authentication types are defined, this field will contain the result of the authentication calculation. For now, if the authentication type is 0, this field is filled with 0s. If the type is 1, this field carries an eight-character password.

OSPF Tables:

- The OSPF uses different kinds of tables to keep track of the routers and maintain a set of the databases. Various OSPF tables are explained below:
  1. **Neighbor Tables:** Neighbor tables contain the routers directly connected to different interfaces of a router. It is also known as the adjacency table. Neighbor table is often used in troubleshooting if there is no communication between two routers. Neighbor table of a router is checked at first hand to see if two routers make neighbors at all.
  2. **Database Table:** Database table also refers to LSDB (Link State Database). It contains all the possible routes to different routers in the network.
  3. **Routing Table:** The routing table is used to find the best possible path to any router in the network.

OSPF Processes:

- There are following seven stages in which OSPF works:
  1. **Down State:** Initially, all the routers will be in the down state. That means all the routers are oblivious to all the routers in an autonomous system.
  2. **Initialization State:** Once a router is powered up, it begins advertising by sending hello packets to the adjacent routers. In the hello packet, it also sends the IP address of the interface through which it sends the hello packet. The hello packet is sent to a multicast address at 224.0.0.5 and is delivered to all the routers.
  3. **Two Way State:** Once all the routers receive the hello packet. The routers open the hello packet and look at the IP address. After processing the hello packet, routers conclude that if the received packet is from the same network or not. If the received packet is from the same network, then they look at the interface from where the packet was received.

     Once the interface has been identified, the other router receiving the packet replies to the first router by unicasting its own hello packet along with its IP address. This way, both the routers can know they are neighbors. This is called two-way state because Router A becomes the neighbor of Router B and vice versa.
  4. **ExStart State:** ExStart state is dependent on another concept used in the OSPF called Router ID. The Router ID is the name of the router.
  5. **Router ID:** Router ID is the highest physical interface of the router. Sometimes, a router might have a logical interface configured as well, in that case, the router Id will be the highest IP address of the logical interface. Coming back to the ExStart State, it is not about exchanging the information between two routers, but it's more about deciding which router shares the information first. So, both the routers compare their router IDs. The router with the higher router ID will get the privilege to start sharing information first.

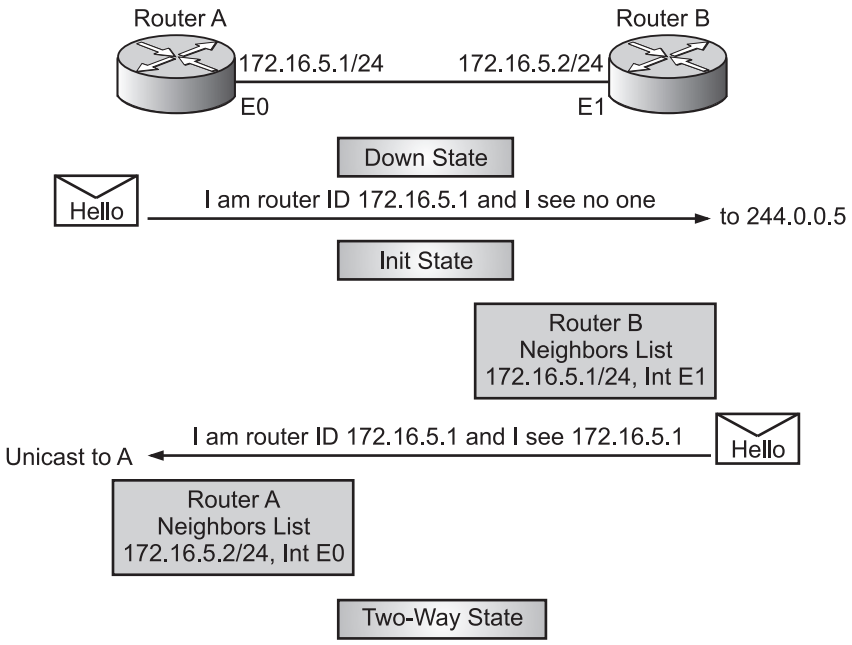


Fig. 2.44

6. **Exchange State:** After the ExStart state, the real exchange happens in the exchange state only. The routers share summaries of the database that they have. The database is called LSDB (Link State Database).
7. **Loading State:** In the loading state, the router compares its database against the database it receives from the neighbors. That is because OSPF relies on the fact that all the routers in the network should have the same network database and topology.
   - **(i) LSR (Link State Request):** In case there is a discrepancy in the link state database, the router sends the link state request, also known as LSR, to its neighbor requesting for more information about a particular network which is mismatched.
   - **(ii) Link State Update (LSU):** Once, a router receives the LSR, it replies with LSU which contains the updated information.
   - **(iii) LSAck (Link State Acknowledgement):** Once, the router receives the LSU, it sends the LSAck.
8. **Full State:** When all the routers have the same database, the network is in the final stage of the OSPF we call full state. Now when a router receives a packet, based on the maintained databases, it calculates the best path and sends the packet.

Advantages of OSPF:

1. OSPF is an open standard, not related to any particular vendor.
2. OSPF is hierarchical routing protocol, using area 0 (Autonomous System) at the top of the hierarchy.
3. OSPF uses Link State Algorithm, and an OSPF network diameter can be much larger than that of RIP.
4. OSPF supports Variable Length Subnet Masks (VLSM), resulting in efficient use of networking resources.
5. OSPF uses multicasting within areas.
6. After initialization, OSPF only sends updates on routing table sections which have changed, it does not send the entire routing table, which in turn conserves network bandwidth.
7. Using areas, OSPF networks can be logically segmented to improve administration, and decrease the size of routing tables.

Disadvantages of OSPF:

1. OSPF is very processor intensive due to implementation of SPF algorithm. OSPF maintains multiple copies of routing information, increasing the amount of memory needed.
2. OSPF is a more complex protocol to implement compared to RIP.

Comparison between RIP and OSPF:

Sr. No.	RIP	OSPF
1.	RIP is a distance vector routing protocol that has two versions namely, RIPv1 and RIPv2.	OSPF is a link state routing protocol.
2.	RIP is easy to configure.	OSPF is complicated to configure and Requires network design and planning.
3.	RIP networks cannot grow larger than 15 hops.	OSPF networks are technically unlimited in size.
4.	An end system (a system with only one network interface) can run RIP in passive mode to listen for routing information.	OSPF does not have a passive mode.
5.	RIP uses much more bandwidth because of its distance vector behavior.	OSPF requires lower bandwidth than RIP.
6.	In RIP, the networks are classified as areas and tables.	In OSPF, the networks are classified as areas, sub areas, autonomous systems and backbone areas.
7.	RIP may be slow to adjust for link failures.	OSPF is quick to adjust for link failures.
8.	The RIP routing protocol uses the distance vector algorithm.	OSPF uses the shortest path algorithm Dijkstra to determine the transmission routes.
9.	RIP generates more protocol traffic than OSPF.	OSPF generates less protocol traffic than RIP.
10.	RIP is simpler routing protocol.	OSPF is much more complex protocol.
11.	RIP is not well suited to large networks, because RIP packet size increases as the number of networks increases.	OSPF works well in large networks.

2.2.2 Inter-Domain Routing [S-22, S-23, S-24]

- Routing between autonomous systems is referred to as inter-domain routing. Inter-domain routing directs network traffic between different Autonomous Systems (AS) on the internet.
- Interdomain routing refers to the process of directing network traffic between different autonomous systems on the Internet.
- It involves the use of protocols such as BGP to determine the most efficient path for data transmission.
- An interdomain routing protocol's goal is to distribute routing information between domains.

2.2.2.1 Path Vector Routing [S-22]

- A path vector routing is a more recent concept compared to both a distance vector routing and the link state routing.

- The path vector routing approach not only exchanges information about the existence of destination networks but also exchanges the path on how to reach the destination.
- Path information is used to determine the best paths and to prevent routing loops. The only widely used path vector protocol is BGP.
- Distance vector routing and link state routing are both intra-domain routing protocols. They can be used inside an autonomous system, but not between autonomous systems.
- These two protocols are not suitable for inter-domain 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 is used for inter-domain routing with low computational overhead and support of heterogeneous policies and securities advantages.
- Path vector routing proved to be useful for inter-domain 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.

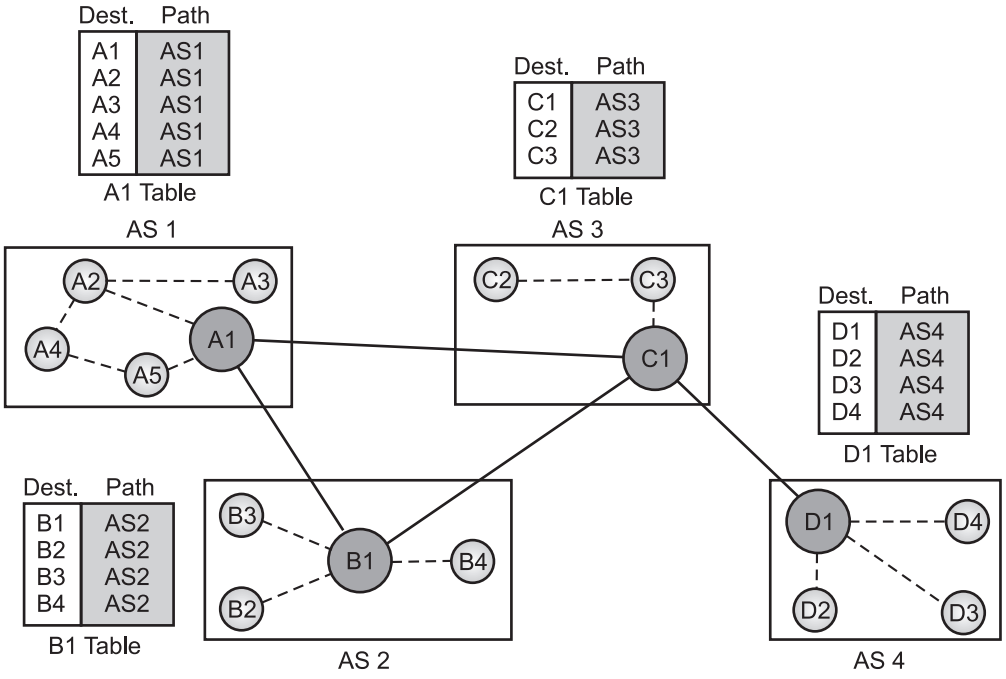


Fig. 2.45: Initial Routing Table in Path Vector Routing

- In Fig. 2.45 Node A1 is the speaker node for AS1, B1 for AS2, C1 for AS2, and D1 for AS4.
- Node A1 creates an initial table that shows A1 to A5 are located in ASI and can be reached through it. Node B1 advertises that B1 to B4 are located in AS2 and can be reached through B1 and so on.
- A path vector protocol is a network routing protocol which maintains the path information that gets updated dynamically.
- Updates which have looped through the network and returned to the same node are easily detected and discarded. Border Gateway Protocol (BGP) is an example of a path vector protocol.

Disadvantages of Path Vector Routing:

1. **Lack of Congestion Control:** In path vector routing, the routing policies may be heterogeneous across the ASs. The network traffic or the link congestion may not be the criterion for path selection in the policies of any AS. Moreover, the path vector routing protocol converges very quickly and stabilizes. Thus, it may not be suitable for handling network congestion efficiently.
2. **Complex:** Path vector routing can be very complex to configure in the network.
3. **Load Balancing:** Load balancing between the source and destination can be done by disseminating packets through each of the alternative paths, multiple paths for packet dissemination are not selected to support load balancing.
4. **Inefficient Load Balancing:** The basic path vector routing protocol does not support load balancing. The path vector table may contain alternative paths to a destination, but an alternative path is selected generally on the failure of an existing path.

2.2.2.2 Border Gateway Protocol (BGPv4) [S-22]

- BGP is an exterior gateway protocol for communication between routers in different autonomous systems. BGP is based on a routing method called path vector routing.
- Border Gateway Protocol (BGP) is an inter-domain routing protocol using path vector routing. The current version of BGP is version 4 (BGP4).
- The BGP4 is an external gateway protocol. It allows two routers in different routing domains, known as Autonomous Systems, to exchange routing information to facilitate the forwarding of data across the borders of the routing domains.

BGP Session:

- In BGP, the exchange of routing information between two routers takes place in a session. A session is a connection that is established between two BGP routers only for the sake of exchanging routing information. To create a reliable environment, BGP uses the services of TCP.
- In other words, a session at the BGP level, as an application program is a connection at the TCP level. However, there is a subtle difference between a connection in TCP made for BGP and other application programs.
- When a TCP connection is created for BGP, it can last for a long time, until something unusual happens. For this reason, BGP sessions are sometimes referred to as semi-permanent connections.

External and Internal BGP:

- BGP can have two types of sessions namely, external BGP (E-BGP) and internal BGP (I-BGP) sessions.
- The E-BGP session in BGP is used to exchange information between two speaker nodes belonging to two different autonomous systems.
- The I-BGP session in BGP is used to exchange routing information between two routers inside an autonomous system.
- The session established between AS1 and AS2 is an E-BGP session. The two speaker routers exchange information they know about networks in the Internet.

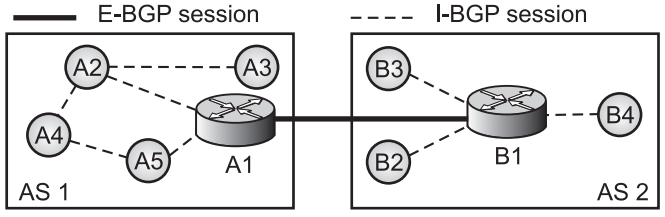


Fig. 2.46: Internal and External BGP Sessions

- However, these two routers need to collect information from other routers in the autonomous systems. This is done using I-BGP sessions.

BGP Packet Format:

- Fig. 2.47 shows packet header format of BGP. All BGP packets share the same common header.

- The size of BGP message format is 22 bit long. They encode with different type of message from the five types of messages function used to establish, maintain and update the neighbour relationship, notify and formatting errors about the peer router of BGP.
- All of these messages have a common header that is sent to their BGP neighbour or also called a BGP peers.

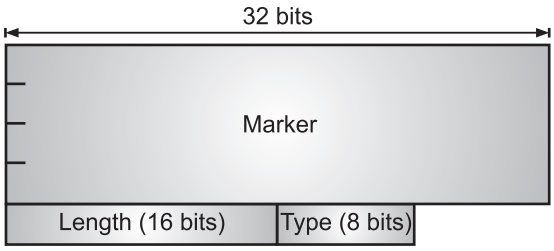


Fig. 2.47: BGP Packet Header

- The most common fields that will be found in a BGP message header are explained below:
  1. **Type:** This field is 8-bit long and it states what type of packet this is and what type of information it contained in the packet. There are five different type of message code defined by the Internet Engineering Task Force to standardize BPG so that all vendors can them. The five type of message type codes are 1-Open, 2-Update, 2-Notification, 4-Keepalive and the last and the only one code message type defined in RFC2918 is 5-Route-Refresh whereas the others are defined in the RFC 1771.
  2. **Length:** This filed message on the header is normally 2-byes long. This shows the total length of the BPG Message including the BGP headers. The value will always be between 19 and the maximum message allowed in any BGP message is 4096 byes.
  3. **Marker:** The remaining 16-bytes of the BGP Header is the Marker field this used to authentication BGP. If no authentication information is assigned or contained in this field then the marker is set to all ones or if the message is an open message.

Types of BGP Messages:

- BGP uses four different types of messages namely, open, update, keepalive and notification as shown in Fig. 2.48.

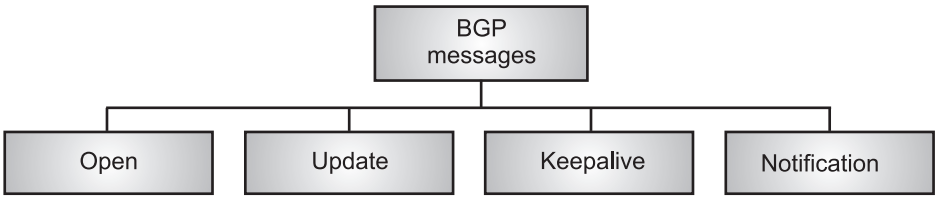


Fig. 2.48: Types of BGP Messages

- The messages of BGP in Fig. 2.48 are explained below:

Open Message:

- One of the five type of message that BGP send first is an Open message. An open message is sent after a TCP connection has been established with its peer router.
- Once, an Open message has been sent and been accept by the neighboring router a keep alive message is sent to acknowledge the open message, after the router that sent an open message receives a keep alive message in return the BGP connect is in the established state and then update, keep alive and notification messages are to send.

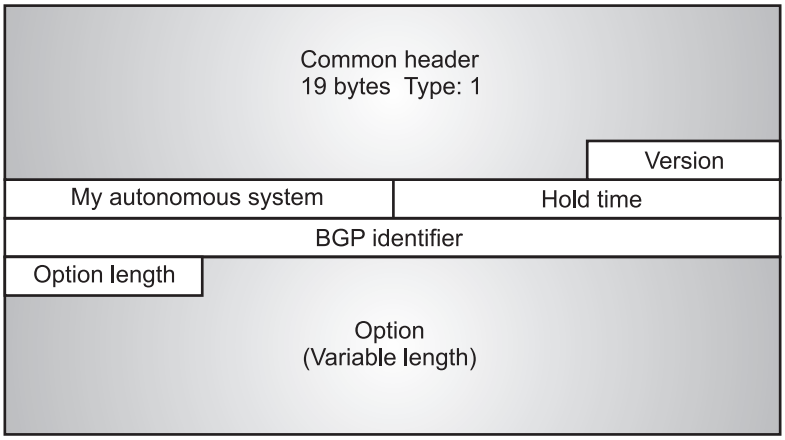


Fig. 2.49: Open Message

- Fig. 2.49 is an open message format again the fields can be up to 22 bits message.
- Various fields in open message are explained below:
  1. **Version:** This 8 bit field contain the BGP Version that the originator is running. The most common BGP version used around the word is BGP 4.
  2. **My Autonomous System:** This is a 2 byte field which content one of the most important message, which is the AS number of the originator router of the packet.
  3. **Hold Time:** This field is 16 bits long and it states the number of seconds the sender purposes for the hold time. The receiving peer will compare the value in the hold time field with it own configuration setting of hold time and give the value is same or smaller value it will accept the connection or reject the connection if any other difference. The hold time value must be within 0 or at least 2 seconds.
  4. **BGP Identifier:** This field can contain up to 22 bit value. The BGP Identifier is the routers ID of the senders peer. In Cisco vendors the highest IP address of the loopback interface on the router is BGP Identifier, if not loopback interface are configured than any highest IP address physical interface is selected as the value for the BGP Identifier.
  5. **Option Length:** The open message may contain some option parameters. In this case, this 1-byte field defines the length of the total option parameters. If there are no option parameters, the value of this field is zero.
  6. **Option Parameters:** If the value of the option parameter length is not zero, it means that there are some option parameters. Each option parameter itself has two subfields: the length of the parameter and the parameter value. The only option parameter defined so far is authentication.

Update Message:

- The Update message that gets sent to all the BGP router's including the peer, contains one of the most important information in any BGP message.
- The update message is responsible for exchanging routing information and possible route path to other networks between BGP neighbors.
- Fig. 2.50 shows the format of the update message of BGP.

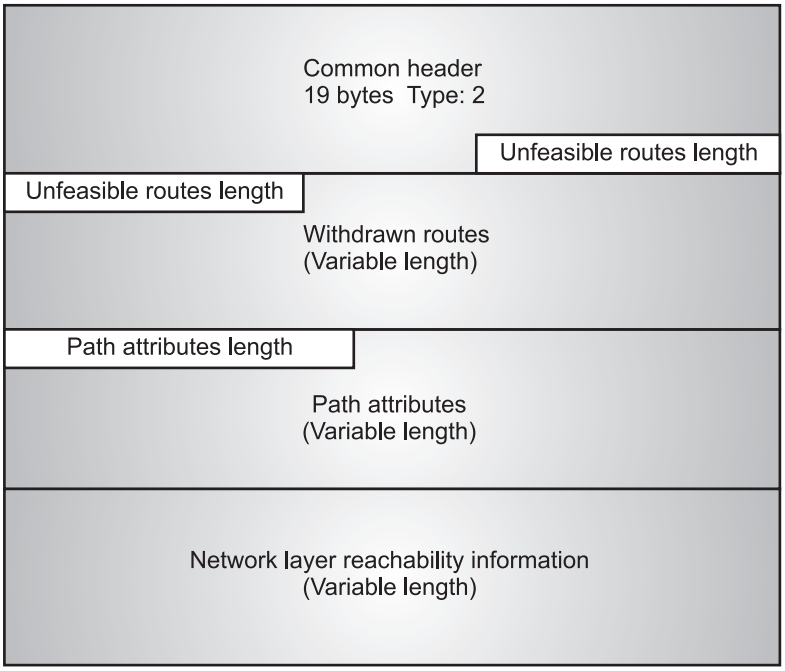


Fig. 2.50: Update Message

- Various fields in update message are explained below:
  1. **Unfeasible Routes Length:** This field in the message is a 2 Octets, this field indicated the receiving BGP router the total number of Withdrawn Routes has been withdrawn for the BGP route. When the length is 0 it means that no routes has been withdrawn from the BGP exchange information.
  2. **Withdrawn Routes:** This field in the message can be variable length in the message. In this part of the packet is the list of all the IP address of all the route/ip address that need to be withdrawn from the receiving BGP router.
  3. **Total Path Attribute Length:** In this part of the packet, the total number of length of the path attributes field in the byte. If the value is set to 0 then that will mean Network Layer Reachability information field is present in this packet.
  4. **Path Attributes:** In this field of the packet, will be help the list of path attribute that are related to the Network Layer Reachability information. In this section each path attribute has the following: attribute type, attribute length, and attribute value.
  5. **Network Layer Reachability Information (NLRI):** This field defines the network that is actually advertised by this message. It has a length field and an IP address prefix. The length defines the number of bits in the prefix. The prefix defines the common part of the network address. For example, if the network is 152.18.7.0/24, the length of the prefix is 24 and the prefix is 152.18.7. BGP4 supports classless addressing and CIDR.

Keepalive Message:

- The keepalive message consists of only the common header shown in Fig. 2.51.
- The routers (called peers in BGP parlance) running the BGP protocols exchange keepalive messages regularly (before their hold time expires) to tell each other that they are alive.

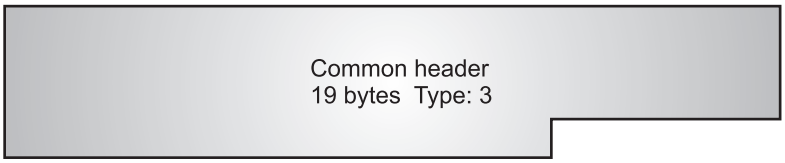


Fig. 2.51: Keepalive Message

Notification Message:

- The format of the notification message is shown in Fig. 2.52. A notification message is sent by a router whenever an error condition is detected or a router wants to close the connection.
- Notification message is used when an error is detected than BGP will send a notification message and then the BGP connection will be closed immediately after sending.
- This type of packet message only contains three different type of information as shown in Fig. 2.52.

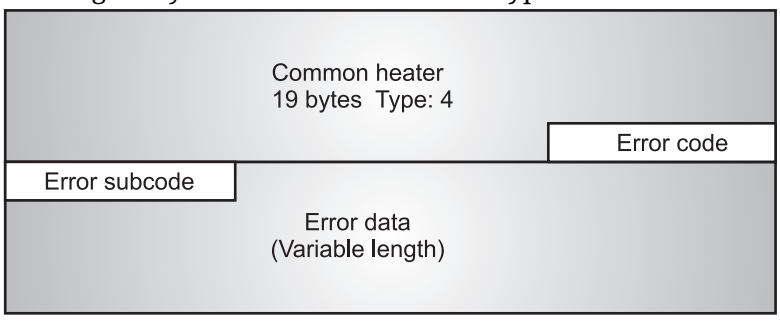


Fig. 2.52: Notification Message

- The fields making up the notification message are as follow:
  1. **Error Code:** The error code of the notification. This 1-byte field defines the category of the error.
  2. **Error Sub code:** Specifics the information about the nature of the problem that it has reported.
  3. **Data:** This contains depend upon the error code and the error sub code, it is normally used to diagnose the reason of the notification.

Error Codes:

Error Code	Error Code Description	Error Subcode Description
1.	Message header error	Three different sub codes are defined for this type of error: synchronization problem (1), bad message length (2), and bad message type (2).
2.	Open message error	Six different sub codes are defined for this type of error: unsupported version number (1), bad peer AS (2), bad BGP identifier (2), unsupported optional parameter (4), authentication failure (5), and unacceptable hold time (6).
3.	Update message error	Eleven different sub codes are defined for this type of error: malformed attribute list (1), unrecognized well-known attribute (2), missing well-known attribute (2), attribute flag error (4), attribute length error (5), invalid origin attribute (6), AS routing loop (7), invalid next hop attribute (8), optional attribute error (9), invalid network field (10), malformed AS_PATH (11).
4.	Hold timer	No sub code defined.
5.	Finite state	This defines the procedural error. No sub code defined.
6.	Cease	No sub code defined.

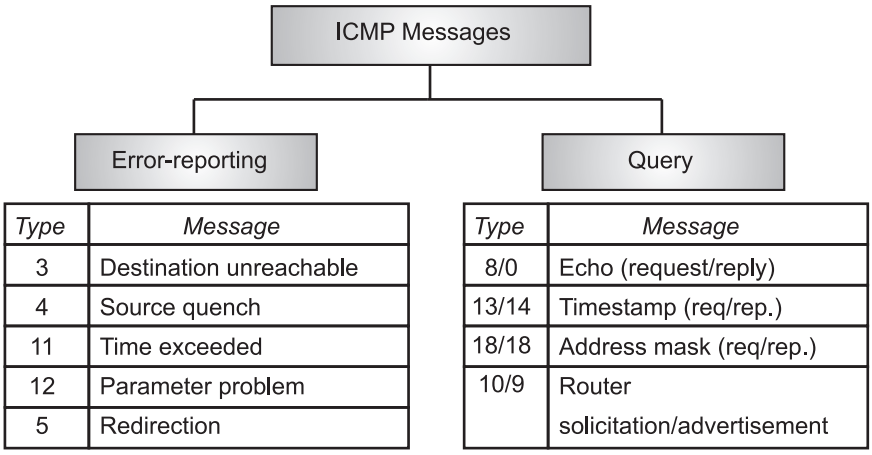
2.3 INTERNET CONTROL MESSAGE PROTOCOL (ICMP) [S-23, S-24]

- ICMP is one of the simplest protocols in the TCP/IP protocol suite. Most protocols implement a particular type of functionality to either facilitate basic operation of a part of the network stack or an application.
- ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information.
- For example, the requested service is not available or a host or router could not be reached. Since, the IP protocol lacks an error-reporting or error-correcting mechanism, information is communicated via a message.
- For instance, when a message is sent to its intended recipient, it may be intercepted along the route from the sender.
- The sender may believe that the communication has reached its destination if no one reports the problem. If a middleman reports the mistake, ICMP helps in notifying the sender about the issue.
- For example, if a message can't reach its destination, if there's network congestion, or if packets are lost, ICMP sends back feedback about these issues. This feedback is essential for diagnosing and fixing network problems, making sure that communication can be adjusted or rerouted to keep everything running smoothly.

2.3.1 Types of ICMP Messages [S-23, S-24]

- Various message types are defined in ICMP that allow different types of information to be exchanged. These are usually either generated for the purpose of reporting errors.
- ICMP messages are used to allow the communication of different types of information between IP devices on an internetwork.
- The messages themselves are used for a wide variety of purposes and they are organized into general categories as well as numerous specific types and subtypes.
- ICMP was originally designed with the idea that most messages would be sent by routers, but they can be sent by both routers and by regular hosts as well, depending on the message type.

- ICMP messages are divided into:
  - **Error Messages:** These messages are used to provide feedback to a source device about an error that has occurred. They are typically generated specifically in response to some sort of action, usually the transmission of a datagram. These are messages which are sent when an error is reported by ICMP protocol. Some of common messages under this category are Destination Unreachable message and Redirect message.
  - **Informational (or Query) Messages:** These are messages that are used to let devices exchange information, implement certain IP-related features and perform testing. They do not indicate errors and are typically not sent in response to a regular datagram transmission. They are generated either when directed by an application or on a regular basis to provide information to other devices. An informational ICMP message may also be sent in reply to another informational ICMP message. Query messages are messages which are sent when ICMP queries about the status of the host. Some of common messages under this category are Echo Request and Echo Reply, Time-stamp Request and Time stamp Reply.



Type	*Message*
3	Destination unreachable
4	Source quench
11	Time exceeded
12	Parameter problem
5	Redirection

Type	*Message*
8/0	Echo (request/reply)
13/14	Timestamp (req/rep.)
18/18	Address mask (req/rep.)
10/9	Router solicitation/advertisement

Types of ICMP Messages:

Category	Type	Message Name	Description
Error-Reporting Messages	3	Destination Unreachable	Indicates that a datagram could not be delivered to its destination. The Code value provides more information on the nature of the error.
	4	Source Quench	Lets a congested IP device tell a device that is sending it datagrams to slow down the rate at which it is sending them.
	11	Time Exceeded	Sent when a datagram has been discarded prior to delivery due to expiration of its Time to Live field.
	12	Parameter Problem	Indicates a miscellaneous problem (specified by the Code value) in delivering a datagram.
	5	Redirect	Allows a router to inform a host of a better route to use for sending datagrams.
	0	Echo Reply	Sent in reply to an Echo (Request) message; used for testing connectivity.
	8	Echo Request	Sent by a device to test connectivity to another device on the internetwork. The word Request sometimes appears in the message name.

	13	Timestamp Request	Sent by a device to request that another send it a timestamp value for propagation time calculation and clock synchronization. The word Request sometimes appears in the message name.
Query Message	14	Timestamp Reply	Sent in response to a Timestamp (Request) to provide time calculation and clock synchronization information.
	17	Address Mask Request	Used to request that a device send a subnet mask.
	18	Address Mask Reply	Contains a subnet mask sent in reply to an Address Mask Request.
	9	Router Advertisement	Used by routers to tell hosts of their existence and capabilities.
	10	Router Solicitation	Used by hosts to prompt any listening routers to send a Router Advertisement.

2.3.2 ICMP Packet Format [S-23, S-24]

- ICMP header comes after IPv4 and IPv6 packet header. Fig. 2.53 shows ICMPv4 packet format.

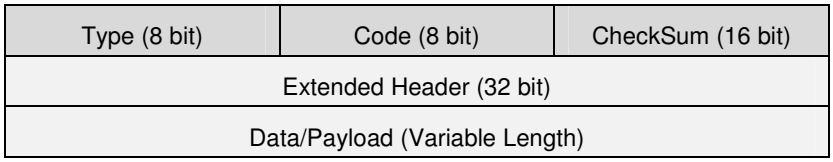


Fig. 2.53: ICMPv4 Packet Format

- In the ICMP packet format, the first 32 bits of the packet contain three fields:

  Type (8-bit): The initial 8-bit of the packet is for message type, it provides a brief description of the message so that receiving network would know what kind of message it is receiving and how to respond to it. Some common message types are as follows:
  - Type 0 – Echo Reply
  - Type 3 – Destination Unreachable
  - Type 5 – Redirect Message
  - Type 8 – Echo Request
  - Type 11 – Time Exceeded
  - Type 12 – Parameter Problem

  Code (8-bit): Code is the next 8 bits of the ICMP packet format, this field carries some additional information about the error message and type.

  Checksum (16-bit): Last 16 bits are for the checksum field in the ICMP packet header. The checksum is used to check the number of bits of the complete message and enable the ICMP tool to ensure that complete data is delivered.

  Extended Header: The next 32 bits of the ICMP Header are Extended Header which has the work of pointing out the problem in IP Message. Byte locations are identified by the pointer which causes the problem message and receiving device looks here for pointing to the problem.

  Data or Payload: The last part of the ICMP packet is Data or Payload of variable length.

2.3.3 ICMP Basic Error Message Format

- Error-reporting message report problems that a router or a host (destination) may encounter when it processes an IP packet.
- A basic ICMP error message would have the following format, (See Fig. 2.54).

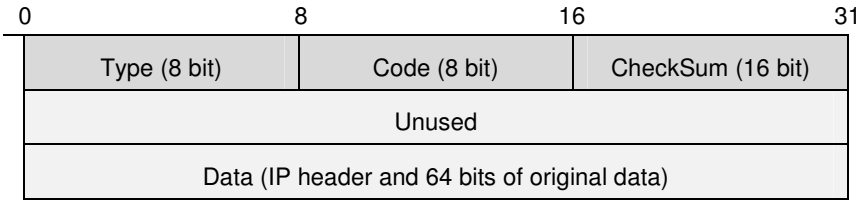


Fig. 2.54: ICMP Basic Error Message Format

- Fields in Fig. 2.54 are explained below:
  - **Type:** The type field identifies the type of the message.
  - **Code:** The code field in ICMP describes the purpose of the message.
  - **Checksum:** The checksum field is used to validate ICMP messages.
  - **Unused:** Reserved for future use and is set to zero. The computer that receives an ICMP message must not use the value in this field.
  - **Data:** Includes the IP header of the datagram that was received and also the first eight bytes of data in the IP datagram. This will be used by the sender to get more details about the error that has occurred.

Practice Questions

1. What is routing? Define it.
2. Explain inter-domain and intra-domain in detail.
3. Describe distance vector routing protocol with example.
4. What is link state routing?
5. With the help of example explain Bellman-ford routing algorithm.
6. What is RIPv2?
7. Describe OSPF in detail.
8. What is BGP? Describe in detail.
9. What is internet? Define it.
10. Explain routing table.
11. What is inter-domain protocol and intra-domain protocol? Enlist them.
12. Describe path vector routing with example.
13. Explain RIP in detail.
14. Explain RIP messages with diagram.
15. With the help of diagram describe OSPF frame format.
16. Describe BGP packet format.
17. Explain types of messages of ICMP.
18. Explain message format of ICMP.
19. Explain message format of ICMP-error reporting message.

MSBTE Questions with Answers

Summer 2023

1. Define Inter domain routing. **[2 M]**

Ans. Refer to Section 2.2.2.

2. List types of ICMPv4 messages. **[2 M]**

Ans. Refer to Section 2.3.2.

3. Explain distance vector routing with suitable example. **[4 M]**

Ans. Refer to Section 2.2.1.1.

Winter 2023

1. List all four routing algorithms. **[2 M]**

Ans. Refer to Section 2.2.1.

2. Differentiate between distance vector routing and link state routing. **[4 M]**

Ans. Refer to Sections 2.2.1.1 and 2.2.1.3.

3. Describe RIP message format in detail. **[4 M]**

Ans. Refer to Section 2.2.1.2.

4. Explain distance vector routing and open shortest path first routing protocol in detail. **[6 M]**

Ans. Refer to Section 2.2.1.1.

Summer 2024

1. Define Inter-domain and Intra-domain routing. **[2 M]**

Ans. Refer to Section 2.2.2.

2. Explain ICMP protocol with its header format. **[4 M]**

Ans. Refer to Sections 2.3 and 2.3.2.

3. Compare between link state routing and distance vector routing. **[4 M]**

Ans. Refer to Sections 2.2.1.3 and 2.2.1.1.

4. Compare dynamic routing and static routing. **[4 M]**

Ans. The following table differentiate between Static Routing and Dynamic Routing.

Sr. No.	Parameters	Static Routing	Dynamic Routing
1.	Routing	In static routing, user-defined routes are used in the routing table.	In dynamic routing, routes are updated as per the changes in network.
2.	Scalability	Limited.	High.
3.	Protocols used	Static routing may not follow any specific protocol. Static routing involves manually configuring routes on network devices.	Dynamic routing uses protocols (like OSPF, RIP, EIGRP) that enable routers to communicate and automatically adjust routes in response to network changes.
4.	Security	Higher security	Less security.
5.	Automation	Static routing is a manual process.	Dynamic routing is an automatic process.

5. Explain any three Intra-domain routing protocols. **[6 M]**

Ans. Refer to Section 2.2.1.

Winter 2024

1. Describe Routing Information Protocol (RIP). **[4 M]**

Ans. Refer to Section 2.2.1.2.

2. Enlist any four features of OSPF. Explain any two OSPF features in brief. **[4 M]**

Ans. Refer to Section 2.2.1.4.

3. Compare distance vector routing and link state routing w.r.t. (i) Concept (ii) Information sharing (iii) Algorithm used (iv) Convergence (v) Problem in Protocol (vi) Example Protocol. **[6 M]**

Ans. Refer to Section 2.2.1.1.

❖❖❖