Computer Network

Network Layer

Prof. Pooja Sisodiya

Assistant Professor CE & IT

Network Layer

- Network layer is majorly focused on getting packets from the source to the destination, routing, error handling and congestion control.
- Network layer design issues:

1. Store and Forward packet switching:

- The host sends the packet to the nearest router.
- This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination.
- This mechanism is called “Store and Forward packet switching.”

2. Services provided to Transport Layer:

- The network layer provides service its immediate upper layer, namely transport layer, through the network – transport layer interface.
- The two types of services provided are –
  - Connection – Oriented Service – In this service, a path is setup between the source and the destination, and all the data packets belonging to a message are routed along this path.

Network Layer

2. **Services provided to Transport Layer: Continue**
   - **Connectionless Service** – In this service, each packet of the message is considered as an independent entity and is individually routed from the source to the destination.
3. **Implementation of Connectionless Service:**

- Packet are termed as “datagrams” and corresponding subnet as “datagram subnets”.
- When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol.
- Each data packet has destination address and is routed independently irrespective of the packets.

4. **Implementation of Connection Oriented service:**
5. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.

Network Layer

4. Implementation of Connection Oriented service: Continue

- It can be done in either two ways :
  - **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
  - **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver.
  - A virtual path is established here. While, other connections may also be using the same path.

IPv4 classful and classless addressing

Classful Address:

•The first addressing system to be implemented as part of the Internet Protocol was Classful Addressing.

•In the year 1981, the Classful addressing network architecture was first used on the Internet.

•The Classful addressing system was superseded by a Classless addressing scheme with the introduction of Classless Inter-Domain Routing (CIDR) in 1993.

- The IP address comprises up of 32 bits and is split into four sections separated by dots: part 1, part 2, part 3, and part 4.
- The IP address is made up of four parts, each of which is eight bits long (1 byte).
- Further, the 4 parts of the IP address is divided into parts: a network ID and a Host ID.

IPv4 classful and classless addressing

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

IPv4 address is divided into two parts:

1.Network ID

2.Host ID

The class of IP address is used to:

•Determine the bits used for network ID?

•Determine the bits used for host ID?

1.Determine the number of total networks?

•Determine the hosts possible in that particular class?

IPv4 classful and classless addressing

Types of Classful Address:

- Classes A-C: unicast addresses
- Class D: multicast addresses
- Class E: reserved for future use

Class A :

•In a class A address, the first bit of the first octet is always ‘0’.

•Thus, class A addresses range from 0.0.0.0 to 127.255.255.255(as 01111111 in binary converts to 127 in decimal).

•The first 8 bits or the first octet denote the network portion and the rest 24 bits or the 3 octets belong to the host portion.

•Its Subnet mask is 255.0.0.0.

•Example: 10.1.1.1

•Exception –

- 127.X.X.X is reserved for loopback
- 0.X.X.X is reserved for default network

•Therefore, the actual range of class A addresses is: 1.0.0.0 to 126.255.255.255

IPv4 classful and classless addressing

Class A :

- The network ID is 8 bits long.
- The host ID is 24 bits long.
- Determine the number of total networks: 2^7-2(One for Network_ID and one for Brodcast_ID) =126
- Determine the number of total Host: 2^{24}-2=16,777,214

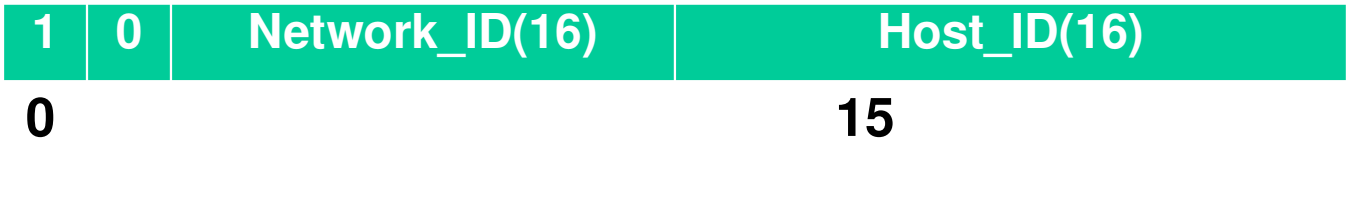
IPv4 classful and classless addressing

Class B :

- In a class B address, the first octet would always start with ’10’.
- Thus, class B addresses range from 128.0.0.0 to 191.255.255.255.
- The first 16 bits or the first two octets denote the network portion and the remaining 16 bits or two octets belong to the host portion.
- Its Subnet mask is 255.255.0.0.
- Example: 172.16.1.1

IPv4 classful and classless addressing

Class B :



- The network ID is 16 bits long.
- The host ID is 16 bits long.
- Determine the number of total networks Addresses: $2^{14}-2=16384$

- Determine the number of total Host Addresses: $2^{16}-2=65534$

IPv4 classful and classless addressing

Class C :

- In a class C address, the first octet would always start with '110'.
- Thus, class C addresses range from 192.0.0.0 to 223.255.255.255.
- The first 24 bits or the first three octets denote the network portion and the rest 8 bits or the remaining one octet belong to the host portion.
- Its Subnet mask is 255.255.255.0.
- Example: 192.168.1.1

- The network ID is 24 bits long.
- The host ID is 8 bits long.
- Determine the number of total networks Addresses: $2^{21}-2=2097152$
- Determine the number of total Host Addresses: $2^{8}-2=254$

IPv4 classful and classless addressing

Class D :

- Class D is used for multicast addressing and in a class D address the first octet would always start with ‘1110’.
- Thus, class D addresses range from 224.0.0.0 to 239.255.255.255.
- Its Subnet mask is not defined.
- Example: 239.2.2.2
- Class D addresses are used by routing protocols like OSPF, RIP, etc.

Class E :

- Class E addresses are reserved for research purposes and future use.
- The first octet in a class E address starts with ‘1111’.
- Thus, class E addresses range from 240.0.0.0 to 255.255.255.255.
- Its Subnet mask is not defined.

IPv4 classful and classless addressing

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

IPv4 classful and classless addressing

Classless Inter-Domain Routing (CIDR):

- CIDR or Class Inter-Domain Routing was introduced in 1993 to replace classful addressing.
- It allows the user to use VLSM or Variable Length Subnet Masks.

CIDR notation:

- In CIDR subnet masks are denoted by /X. For example a subnet of 255.255.255.0 would be denoted by /24.
- To work a subnet mask in CIDR, we have to first convert each octet into its respective binary value.
- For example, if the subnet is of 255.255.255.0. then :
- First Octet –
  - 255 has 8 binary 1's when converted to binary
- Second Octet –
  - 255 has 8 binary 1's when converted to binary
- Third Octet –
  - 255 has 8 binary 1's when converted to binary
- Fourth Octet –
  - 0 has 0 binary 1's when converted to binary
- Therefore, in total there are 24 binary 1’s, so the subnet mask is /24

What is Internet Protocol (IP)

- Here, IP stands for internet protocol.
- It is a protocol defined in the TCP/IP model used for sending the packets from source to destination.
- The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers.
- IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.
- The first version of IP (Internet Protocol) was IPv4.
- After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.

Function:

- The main function of the internet protocol is **to provide addressing to the hosts**, **encapsulating the data into a packet structure**, and **routing the data from source to the destination across one or more IP networks**.
- In order to achieve these functionalities, internet protocol provides two major things which are given below

What is Internet Protocol (IP)

Function: Continue...

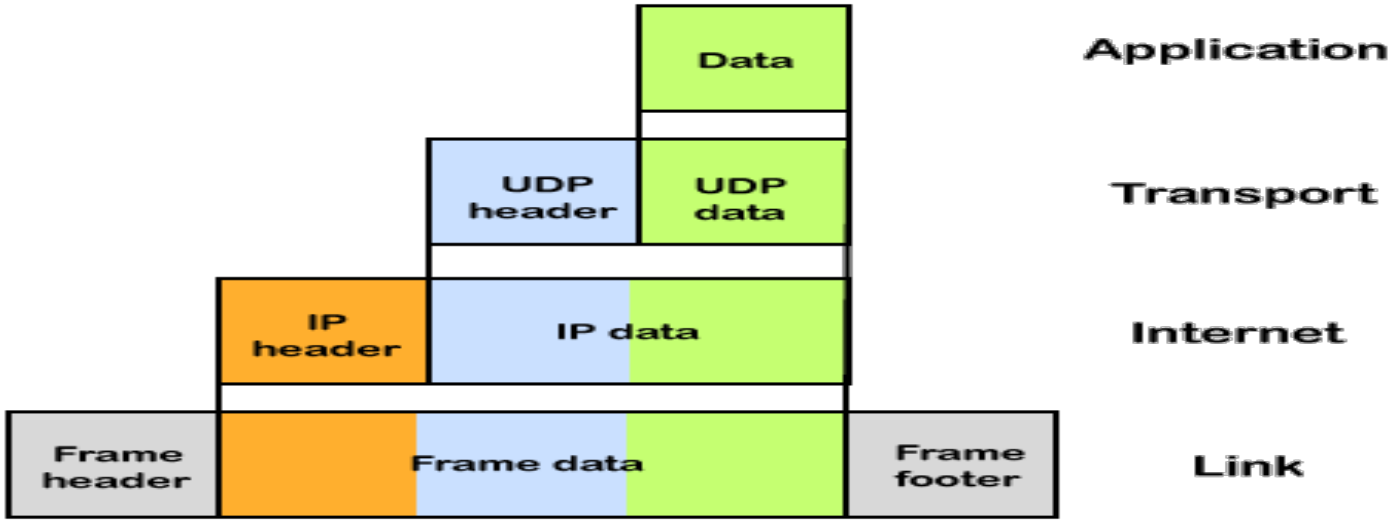
•An internet protocol defines two things:

1.Format of IP packet

2.IP Addressing system

What is an IP packet?:

•Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., header and a payload.



IPv4 - Packet Structure

- Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets.
- IP packet encapsulates data unit received from above layer and add to its own header information.

(IP Encapsulation)

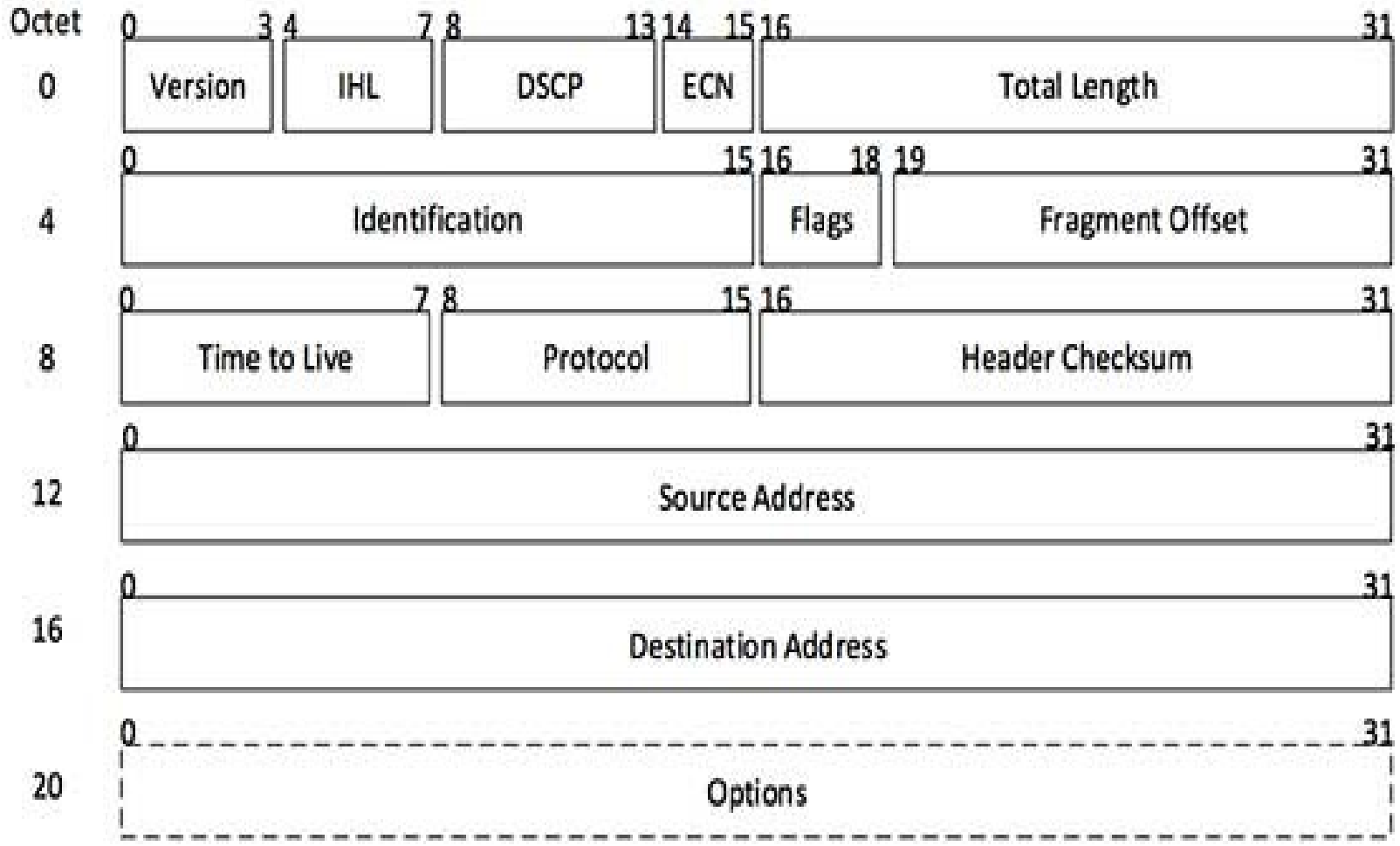
- The encapsulated data is referred to as IP Payload.
- IP header contains all the necessary information to deliver the packet at the other end.
- IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows –

Version – Version no. of Internet Protocol used (e.g. IPv4).

IHL – Internet Header Length; Length of entire IP header.

DSCP – Differentiated Services Code Point; this is Type of Service.

IPv4 - Packet Structure



[Image: IP Header]

IPv4 - Packet Structure

ECN – Explicit Congestion Notification; It carries information about the congestion seen in the route.

Total Length – Length of entire IP Packet (including IP header and IP Payload).

Identification – If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.

Flags – As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.

Fragment Offset – This offset tells the exact position of the fragment in the original IP Packet.

Time to Live – To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

Protocol – Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.

IPv4 - Packet Structure

Header Checksum – This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

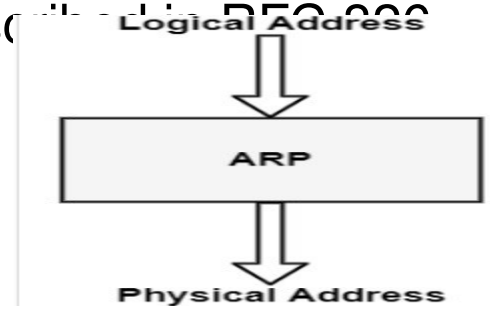
Source Address – 32-bit address of the Sender (or source) of the packet.

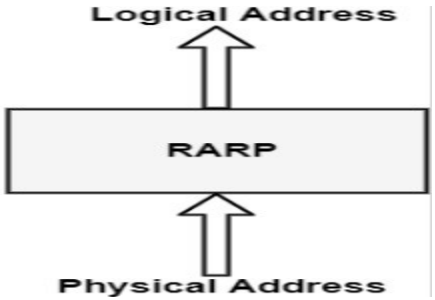
Destination Address – 32-bit address of the Receiver (or destination) of the packet.

Options – This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Address Resolution Protocol (ARP)

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





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

Address Resolution Protocol (ARP)

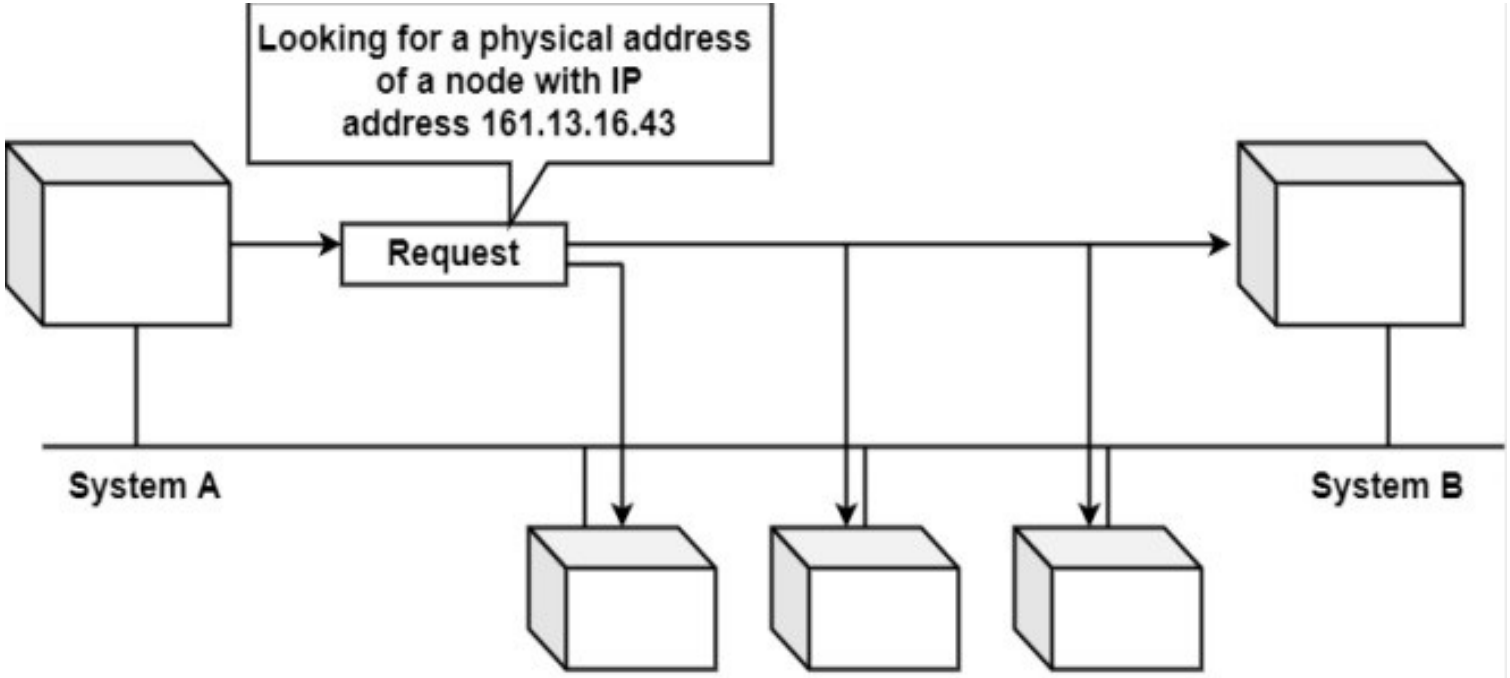
- The IP Address cannot be changed.
- ARP can find the physical address of the node when its internet address is known.
- ARP provides a dynamic mapping from an IP address to the corresponding hardware address.
- When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address.

This process is as follows–

- When a host tries to interact with another host, an ARP request is initiated. If the IP address is for the local network, the source host checks its ARP cache to find out the hardware address of the destination computer.
- If the correspondence hardware address is not found, ARP broadcasts the request to all the local hosts.
- All hosts receive the broadcast and check their own IP address. If no match is discovered, the request is ignored.

Address Resolution Protocol (ARP)

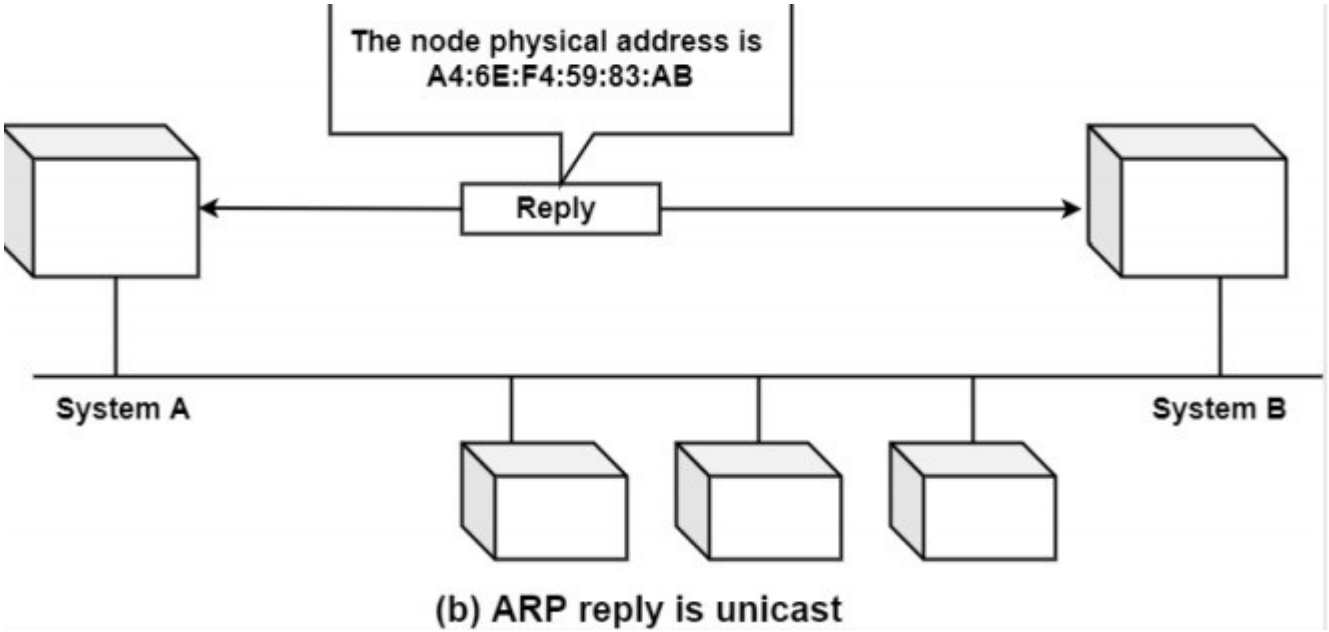
- The destination host that finds the matching IP address sends an ARP reply to the source host along with its hardware address, thus establishing the communication. The ARP cache is then updated with the hardware address of the destination host.



(a) ARP request is broadcast

Address Resolution Protocol (ARP)

- .

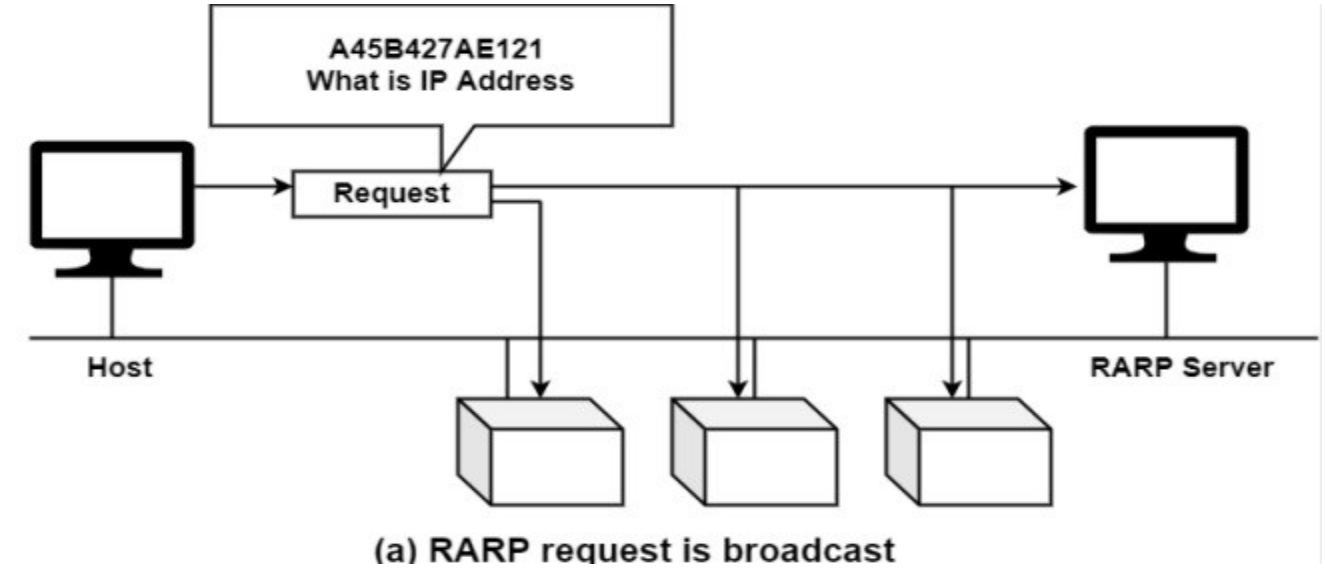


(b) ARP reply is unicast

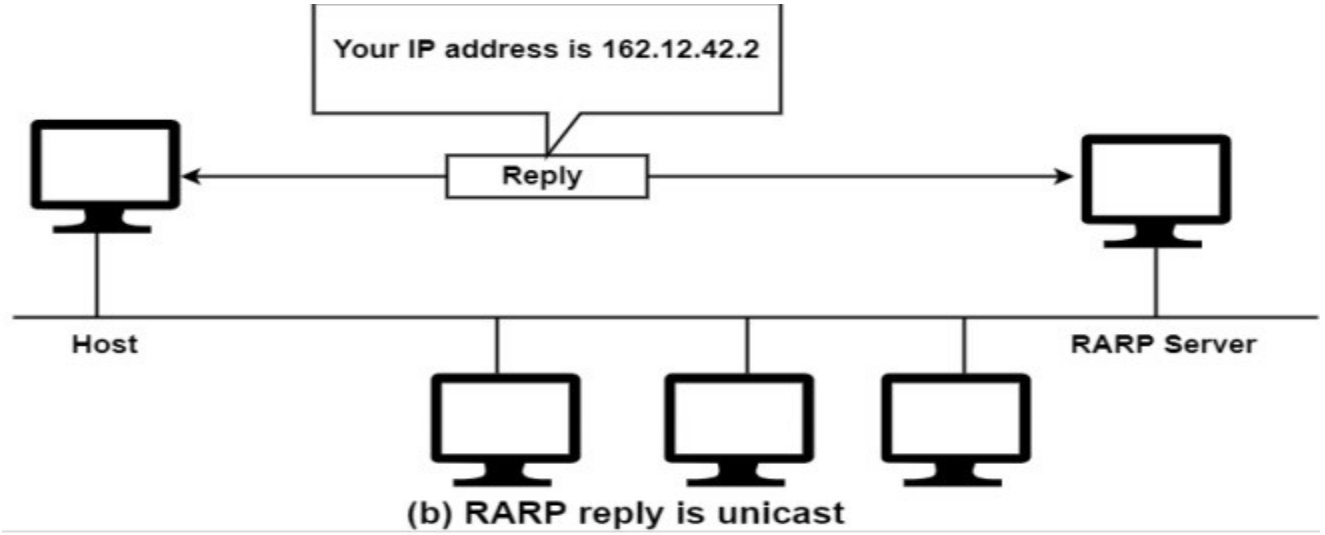
Reverse Address Resolution Protocol (RARP)

- Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol. It is described in RFC 903.
- Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted.
- To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.
- The reverse address resolution is performed the same way as the ARP address resolution.
- The same packet format is used for the ARP.
- An exception is the operation code field that now takes the following values–
  - 3 for RARP request
  - 4 for RARP reply
- The physical header of the frame will now indicate RARP as the higher-level protocol (8035 hex) instead of ARP (0806 hex) or IP-(0800 hex) in the Ether type field.

Address Resolution Protocol (ARP)



(a) RARP request is broadcast



(b) RARP reply is unicast

Internet Control Message Protocol (ICMP)

- Internet Control Message Protocol (ICMP) works in the network layer of the OSI model and the internet layer of the TCP/IP model.
- It is used to send control messages to network devices and hosts.
- Routers and other network devices monitor the operation of the network.
- When an error occurs, these devices send a message using ICMP.
- Messages that can be sent include "destination unreachable", "time exceeded", and "echo requests".
- ICMP is a network layer protocol.
- ICMP messages are not passed directly to the data link layer. The message is first encapsulated inside the IP datagram before going to the lower layer.

Types of ICMP messages:

Information Messages – In this message, the sender sends a query to the host or router and expects an answer. For example, A host wants to know if a router is alive or not.

Error-reporting message – This message report problems that a router or a host (destination) may encounter when it processes an IP packet

Internet Control Message Protocol (ICMP)

Query Message – It helps a router or a network manager to get specific information from a router or another host.

Category	Type	Message
Error-Reporting Messages	3	Destination unreachable
	4	Source quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Message	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router Solicitation or advertisement

Internet Control Message Protocol (ICMP)

Source Quench – It requests to decrease the traffic rate of message sending from source to destination.

Time Exceeded – When fragments are lost in a network the fragments hold by the router will be dropped and then ICMP will take the source IP from the discarded packet and inform the source, that datagram is discarded due to the time to live field reaches zero, by sending time exceeded message.

Fragmentation Required – When a router is unable to forward a datagram because it exceeds the MTU of the next-hop network and the DF (Don't Fragment) bit is set, the router is required to return an ICMP Destination Unreachable message to the source of the datagram, with the Code indicating fragmentation is needed and DF (Don't Fragment) set.

Destination Unreachable – This error message indicates that the destination host, network, or port number that is specified in the IP packet is unreachable. This may happen due to the destination host device is down, an intermediate router is unable to find a path to forward the packet, and a firewall is configured to block connections from the source of the packet.

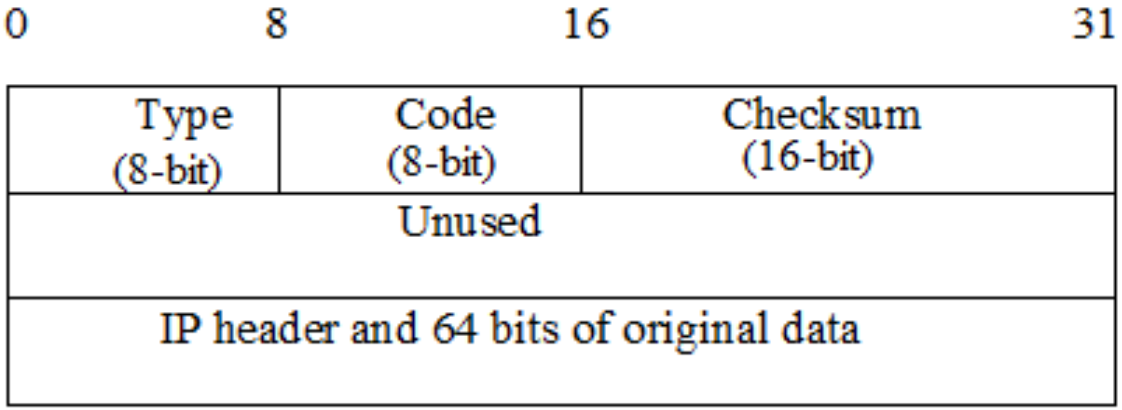
Internet Control Message Protocol (ICMP)

Redirect Message – A redirect error message is used when a router needs to tell a sender that it should use a different path for a specific destination. It occurs when the router knows a shorter path to the destination.

ICMP Basic Error Message Format:

A basic ICMP error message would have the following format –

- **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.



Routing Algorithms

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Distance Vector Routing Algorithm

- The Distance-Vector routing algorithm is known by other names. Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm are generally distributed after the researchers create it (Bellman 1957, and Ford and Fulkerson, 1962).
- The Distance vector algorithm is iterative, asynchronous and distributed.
  - **Distributed:** It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
  - **Iterative:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
  - **Asynchronous:** It does not require that all of its nodes operate in the lock step with each other.
- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as Vector.

Distance Vector Routing Algorithm

Three Keys to understand the working of Distance Vector Routing Algorithm:

Knowledge about the whole network: Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.

Routing only to neighbors: The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.

Information sharing at regular intervals: Within 30 seconds, the router sends the information to the neighboring routers.

Distance Vector Routing Algorithm

Distance Vector Routing Algorithm:

•Let dx(y) be the cost of the least-cost path from node x to node y. The least costs are related by Bellman-Ford equation,

$$dx(y) = \min_v\{c(x,v) + dv(y)\}$$

•Where the minv is the equation taken for all x neighbors. After traveling from x to v, if we consider the least-cost path from v to y, the path cost will be c(x,v)+dv(y). The least cost from x to y is the minimum of c(x,v)+dv(y) taken over all neighbors.

With the Distance Vector Routing algorithm, the node x contains the following routing information:

•For each neighbor v, the cost c(x,v) is the path cost from x to directly attached neighbor, v.

•The distance vector x, i.e., Dx = [Dx(y) : y in N], containing its cost to all destinations, y, in N.

•The distance vector of each of its neighbors, i.e., Dv = [Dv(y) : y in N] for each neighbor v of x.

Distance Vector Routing Algorithm

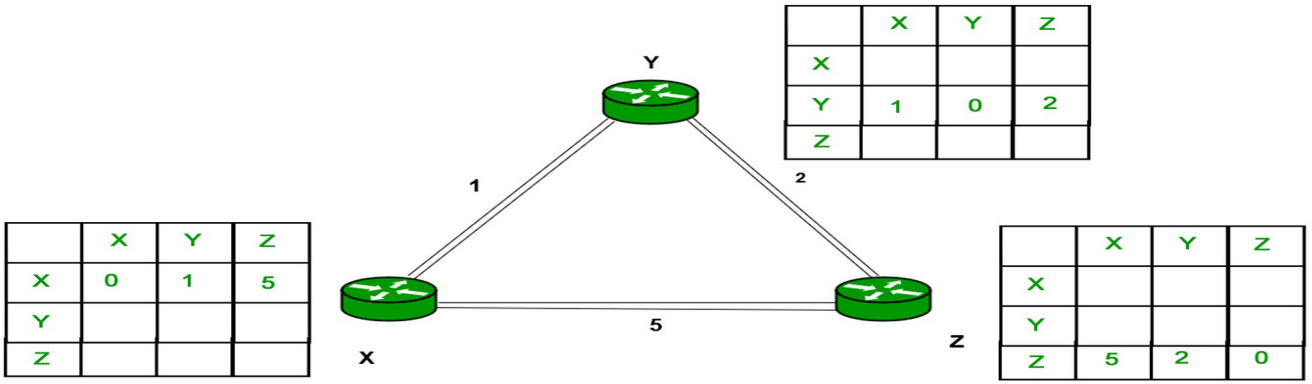
- Distance vector routing is an asynchronous algorithm in which node x sends the copy of its distance vector to all its neighbors.
- When node x receives the new distance vector from one of its neighboring vector, v, it saves the distance vector of v and uses the Bellman-Ford equation to update its own distance vector.
- The equation is given below:

  $d_x(y) = \min_v\{ c(x,v) + d_v(y)\}$ for each node y in N

- The node x has updated its own distance vector table by using the above equation and sends its updated table to all its neighbors so that they can update their own distance vectors.

Distance Vector Routing Algorithm

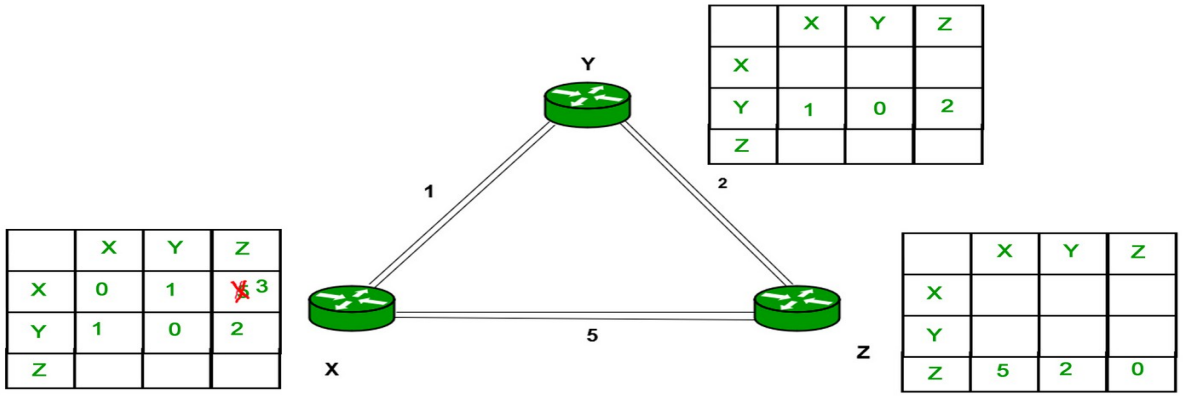
- Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



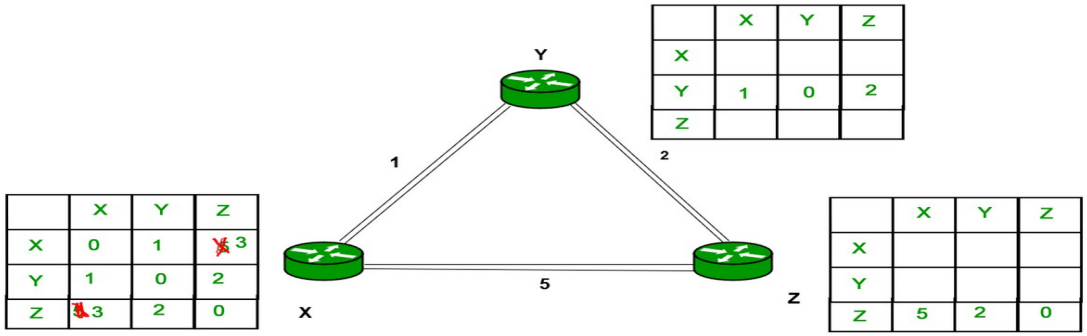
- Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.
- $Dx(y) = \min \{ C(x,v) + Dv(y)\}$ for each node $y \in N$

Distance Vector Routing Algorithm

- As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.

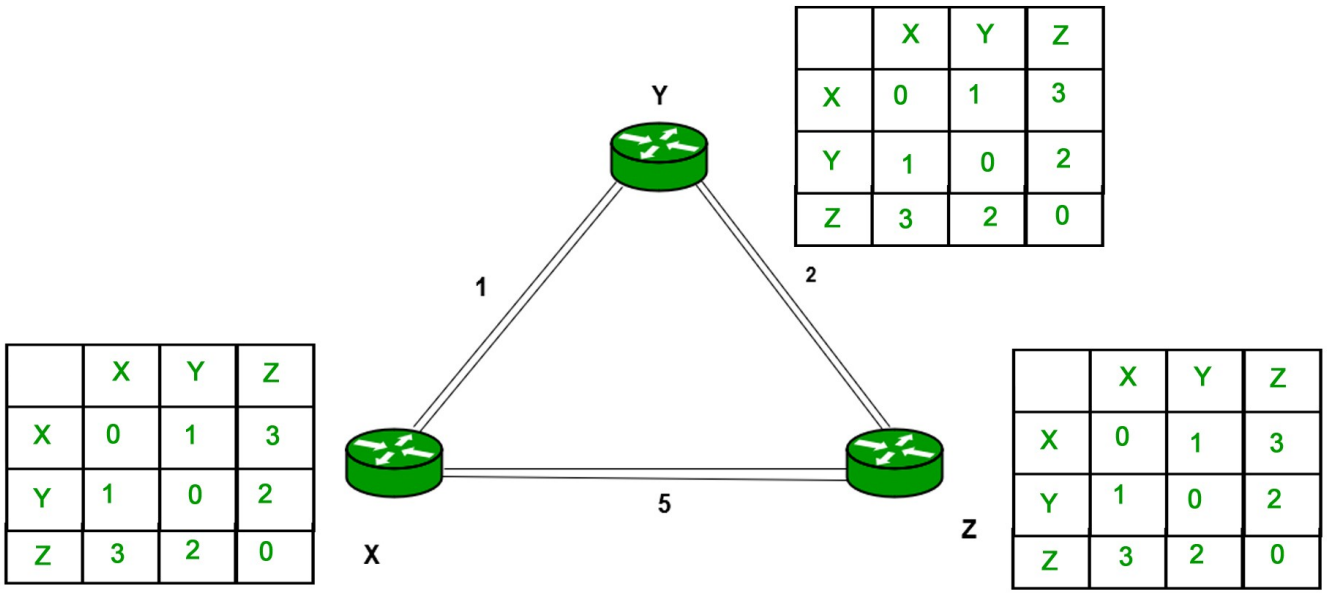


- Similar for Z also-



Distance Vector Routing Algorithm

- Finally the routing table for all –



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Distance Vector Routing Algorithm

Disadvantages of Distance Vector routing –

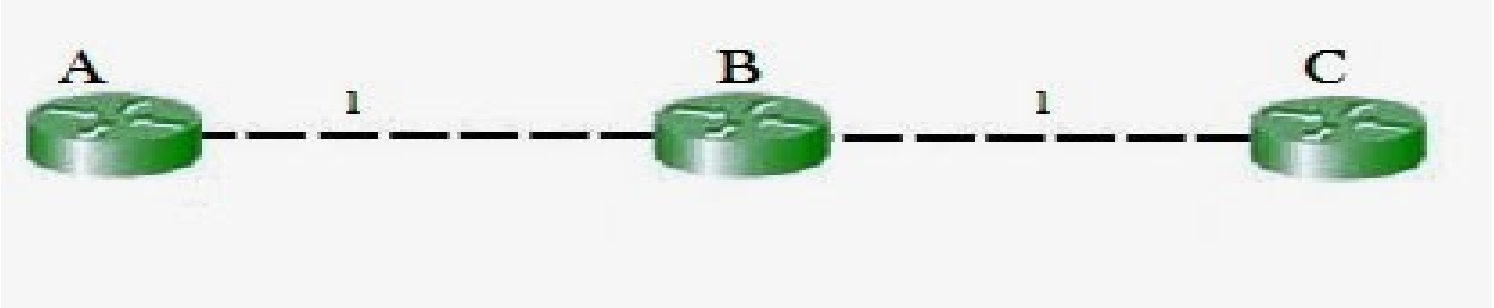
- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Distance Vector Routing Algorithm

The Count to Infinity Problem –

•The main issue with Distance Vector Routing (DVR) protocols is Routing Loops since Bellman-Ford Algorithm cannot prevent loops.

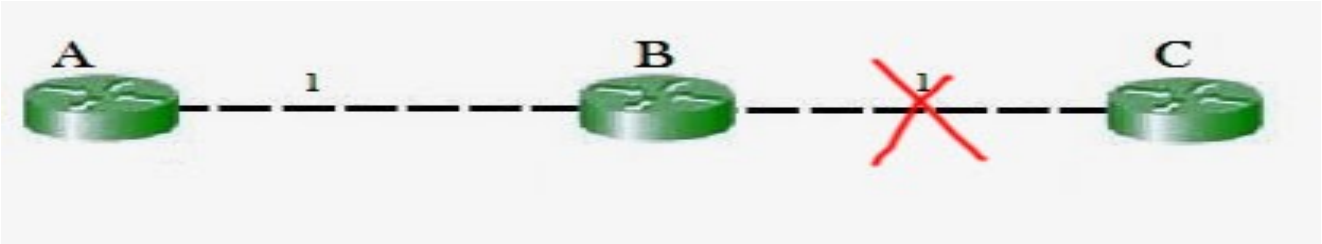
•This routing loop in the DVR network causes the Count to Infinity Problem. Routing loops usually occur when an interface goes down or two routers send updates at the same time.



•So in this example, the Bellman-Ford algorithm will converge for each router, they will have entries for each other. B will know that it can get to C at a cost of 1, and A will know that it can get to C via B at a cost of 2.

Distance Vector Routing Algorithm

The Count to Infinity Problem –



- If the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table.
- Before it can send any updates it's possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2.
- B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3.
- A will then receive updates from B later and update its cost to 4.
- They will then go on feeding each other bad information toward infinity which is called as **Count to Infinity problem.**

Link State Routing Algorithm

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

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Link State Routing Algorithm

Link State Routing has two phases:

1.Reliable Flooding:

- **Initial state:** Each node knows the cost of its neighbors.
- **Final state:** Each node knows the entire graph.

2.Route Calculation: Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

•The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

•The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

Link State Routing Algorithm

Let's describe some notations:

- **c(i , j):** Link cost from node i to node j. If i and j nodes are not directly linked, then c(i , j) = ∞.
- **D(v):** It defines the cost of the path from source code to destination v that has the least cost currently.
- **P(v):** It defines the previous node (neighbor of v) along with current least cost path from source to v.
- **N:** It is the total number of nodes available in the network.

Link State Routing Algorithm

- Initialization

  N = {A} // A is a root node.

  for all nodes v

  if v adjacent to A

  then D(v) = c(A,v)

  else D(v) = infinity

- loop

  find w not in N such that D(w) is a minimum.

  Add w to N

  Update D(v) for all v adjacent to w and not in N:

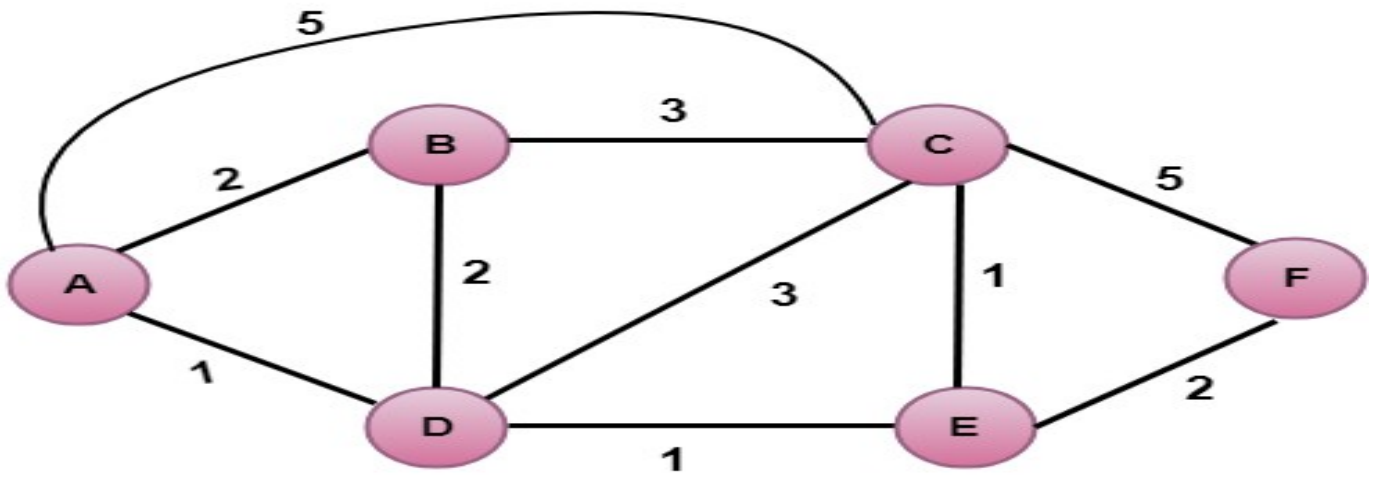
  D(v) = min(D(v) , D(w) + c(w,v))

  Until all nodes in N

- In the above algorithm, an initialization step is followed by the loop.
- The number of times the loop is executed is equal to the total number of nodes available in the network.

Link State Routing Algorithm

- **Let's understand through an example:**



- **In the above figure, source vertex is A.**
- **Step 1:**
- The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

Link State Routing Algorithm

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞

- **Step 2:**
- In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

a) Calculating shortest path from A to B

v = B, w = D

D(B) = min(D(B) , D(D) + c(D,B))

= min(2, 1+2)>

= min(2, 3)

- The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

Link State Routing Algorithm

b) Calculating shortest path from A to C:

v = C, w = D

D(B) = min(D(C) , D(D) + c(D,C))

= min(5, 1+3)

= min(5, 4)

• The minimum value is 4. Therefore, the currently shortest path from A to C is 4.

c) Calculating shortest path from A to E

v = E, w = D

D(B) = min(D(E) , D(D) + c(D,E))

= min(∞, 1+1)

= min(∞, 2)

•The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

•

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞

Link State Routing Algorithm

Step 3:

•In the above table, we observe that both E and B have the least cost path in step 2. Let's consider the E vertex. Now, we determine the least cost path of remaining vertices through E.

a) Calculating the shortest path from A to B.

v = B, w = E

D(B) = min(D(B) , D(E) + c(E,B))

= min(2 , 2+ ∞)

= min(2, ∞)

•The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating the shortest path from A to C.

v = C, w = E

D(B) = min(D(C) , D(E) + c(E,C))

= min(4 , 2+1)

= min(4,3)

- The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

Link State Routing Algorithm

c) Calculating the shortest path from A to F.

v = F, w = E

D(B) = min(D(F) , D(E) + c(E,F))

= min(∞ , 2+2)

= min(∞ ,4)

•The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E

Link State Routing Algorithm

Step 4:

•In the above table, we observe that B vertex has the least cost path in step 3. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through B.

a) Calculating the shortest path from A to C.

v = C, w = B

D(B) = min(D(C) , D(B) + c(B,C))

= min(3 , 2+3)

= min(3,5)

The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

b) Calculating the shortest path from A to F.

v = F, w = B

D(B) = min(D(F) , D(B) + c(B,F))

= min(4, ∞)

= min(4, ∞)

The minimum value is 4. Therefore, the currently shortest path from A to

Link State Routing Algorithm

Step 4:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E

Step 5:

In the above table, we observe that C vertex has the least cost path in step 4. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through C.

a) Calculating the shortest path from A to F.

v = F, w = C

D(B) = min(D(F) , D(C) + c(C,F))

= min(4, 3+5)

= min(4,8)

The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Link State Routing Algorithm

Step 5:

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E

Final tab

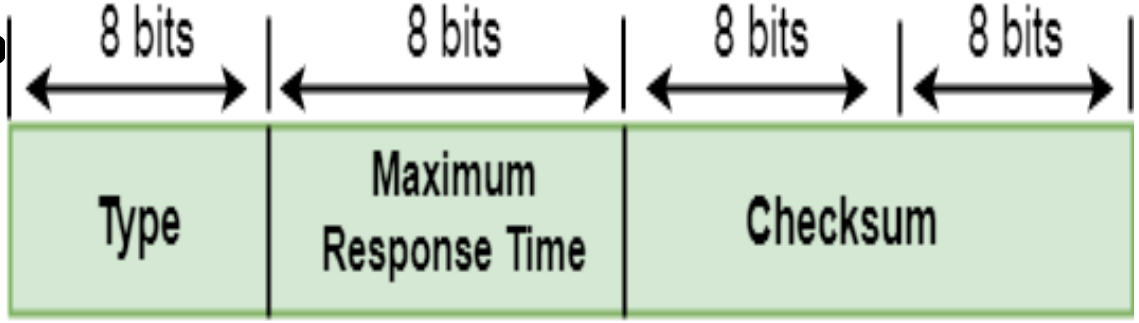
Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E
6	ADEBC					

Internet Group Management Protocol (IGMP)

- The Internet Group Management Protocol (IGMP) is one of the necessary, but

  not sufficient, protocols that is involved in multicasting.
- IGMP is a companion to the IP protocol.
- The IGMP protocol is used by the hosts and router to support multicasting.
- The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.
- IGMP is a part of the IP layer, and IGMP has a fixed-size message.
- The IGMP message is encapsulated within an IP datagram.

The Format o



Internet Group Management Protocol (IGMP)

Type: It determines the type of IGMP message. There are three types of IGMP message: Membership Query, Membership Report and Leave Report.

Maximum Response Time: This field is used only by the Membership Query message. It determines the maximum time the host can send the Membership Report message in response to the Membership Query message.

Checksum: It determines the entire payload of the IP datagram in which IGMP message is encapsulated.

Group Address: The behavior of this field depends on the type of the message sent.

- For Membership Query, the group address is set to zero for General Query and set to multicast group address for a specific query.
- For Membership Report, the group address is set to the multicast group address.
- For Leave Group, it is set to the multicast group address.

Internet Group Management Protocol (IGMP)

IGMP Messages:

Membership Query message:

•This message is sent by a router to all hosts on a local area network to determine the set of all the multicast groups that have been joined by the host.

•It also determines whether a specific multicast group has been joined by the hosts on a attached interface.

•The group address in the query is zero since the router expects one response from a host for every group that contains one or more members on that host.

Membership Report message :

- The host responds to the membership query message with a membership report message.
- Membership report messages can also be generated by the host when a host wants to join the multicast group without waiting for a membership query message from the router.
- Membership report messages are received by a router as well as all

Internet Group Management Protocol (IGMP)

Membership Report message: Continue...

- Each membership report message includes the multicast address of a single group that the host wants to join.
- IGMP protocol does not care which host has joined the group or how many hosts are present in a single group. It only cares whether one or more attached hosts belong to a single multicast group.

Leave Report:

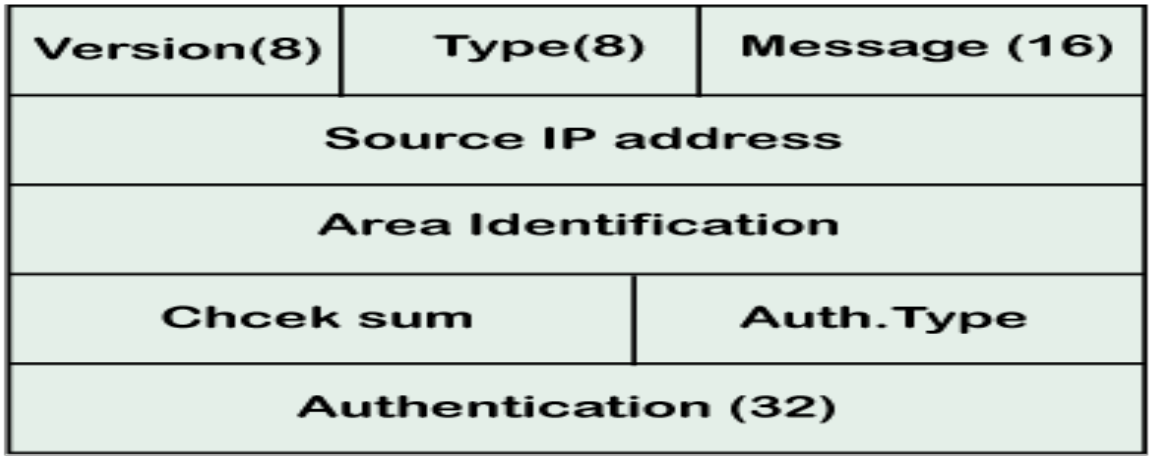
- When the host does not send the "Membership Report message", it means that the host has left the group.
- The host knows that there are no members in the group, so even when it receives the next query, it would not report the group.

Open Shortest Path First (OSPF) Protocol

- Open shortest path first (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm.
- A link-state routing protocol is a protocol that uses the concept of triggered updates, i.e., if there is a change observed in the learned routing table then the updates are triggered only, not like the distance-vector routing protocol where the routing table is exchanged at a period of time.
- It is a network layer protocol that works on protocol number 89.
- OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

Open Shortest Path First (OSPF) Protocol

OSPF Message Format: The following are the fields in an OSPF message format



Version: It is an 8-bit field that specifies the OSPF protocol version.

Type: It is an 8-bit field. It specifies the type of the OSPF packet.

Message: It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.

Source IP address: It defines the address from which the packets are sent. It is a sending routing IP address.

Open Shortest Path First (OSPF) Protocol

OSPF Message Format: Continue....

Area identification: It defines the area within which the routing takes place.

Checksum: It is used for error correction and error detection.

Authentication type: There are two types of authentication, i.e., 0 and 1.

•Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.

Authentication: It is a 32-bit field that contains the actual value of the authentication data.

Open Shortest Path First (OSPF) Protocol

OSPF terms:

1.Router I'd – It is the highest active IP address present on the router. First, the highest loopback address is considered.

- If no loopback is configured then the highest active IP address on the interface of the router is considered.

2.Router priority – It is an 8-bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.

3.Designated Router (DR) – It is elected to minimize the number of adjacencies formed. DR distributes the LSAs to all the other routers.

- DR is elected in a broadcast network to which all the other routers share their DBD.
- In a broadcast network, the router requests for an update to DR, and DR will respond to that request with an update.

4.Backup Designated Router (BDR) – BDR is a backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

Open Shortest Path First (OSPF) Protocol

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

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

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

1. **Down –** In this state, no hello packets have been received on the interface.
   5. Note – The Downstate doesn't mean that the interface is physically down. Here, it means that the OSPF adjacency process has not started yet.
- **INIT –** In this state, the hello packets have been received from the other router.
- **2WAY –** In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.

Open Shortest Path First (OSPF) Protocol

OSPF states – Continue...

4.Exstart – In this state, NULL DBD are exchanged.

- In this state, the master and slave elections take place.
- The router having the higher router I'd become the master while the other becomes the slave.
- This election decides Which router will send its DBD first (routers who have formed neighbourship will take part in this election).

5. Exchange – In this state, the actual DBDs are exchanged.

6.Loading – In this state, LSR, LSU, and LSA (Link State Acknowledgement) are exchanged.

Important – When a router receives DBD from other router, it compares its own DBD with the other router DBD.

7.If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed.

•The other router replies with the LSU containing the updates that are needed.

•In return to this, the router replies with the Link State Acknowledgement.

Open Shortest Path First (OSPF) Protocol

7. **Full –** In this state, synchronization of all the information takes place. OSPF routing can begin only after the Full state.

Criteria –

- To form neighbourship in OSPF, there is a criterion for both the routers:

1. It should be present in the same area.
2. The router I'd be unique.
3. The subnet mask should be the same.
4. Hello, and the dead timer should be the same.
7. The stub flag must match.
8. Authentication must match.

Open Shortest Path First (OSPF) Protocol

OSPF messages –

1. Hello message –

- These are keep-alive messages used for neighbor discovery /recovery.
- These are exchanged every 10 seconds.
- This includes the following information: Router I'd, Hello/dead interval, Area I'd, Router priority, DR and BDR IP address, authentication data.

2. Database Description (DBD) –

- It is the OSPF route of the router. This contains the topology of an AS or an area (routing domain).

3. Link state request (LSR) –

- When a router receives DBD, it compares it with its own DBD.
- If the DBD received has some more updates than its own DBD then LSR is being sent to its neighbor.

4. Link state update (LSU) –

- When a router receives LSR, it responds with an LSU message containing the details requested.

Open Shortest Path First (OSPF) Protocol

OSPF messages – Continue...

5. Link state acknowledgement –

- This provides reliability to the link-state exchange process. It is sent as the acknowledgement of LSU.

6. Link state advertisement (LSA) –

- It is an OSPF data packet that contains link-state routing information, shared only with the routers to which adjacency has been formed.

Timers –

1. Hello timer –

- The interval in which the OSPF router sends a hello message on an interface. It is 10 seconds by default.

2. Dead timer –

- The interval in which the neighbor will be declared dead if it is not able to send the hello packet.
- It is 40 seconds by default. It is usually 4 times the hello interval but can be configured manually according to need.

Routing Information Protocol (RIP)

- RIP stands for Routing Information Protocol.
- Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network
- RIP is an intra-domain routing protocol used within an autonomous system.
- Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area.
- To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

Before understanding the structure of the packet, we first look at the following points:

- RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
- In a routing table, the first column is the destination, or we can say that it is a network address.

Routing Information Protocol (RIP)

- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- The next column contains the address of the router to which the packet is to be sent to reach the destination.

How is hop count determined?

- 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 hops allowed in a path from source and destination.
- The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

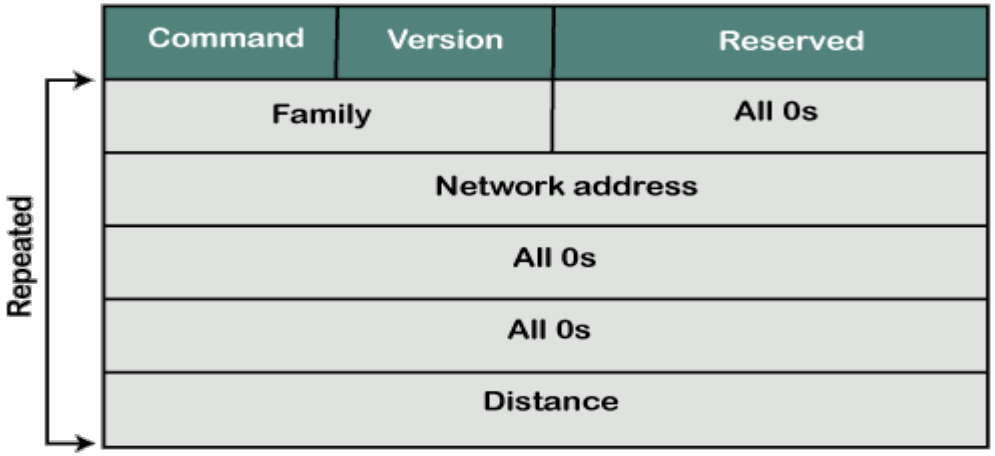
Routing Information Protocol (RIP)

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 routing information received from neighbor routers. This is also known as Routing on rumors.

RIP Message Format

•The message format is used to share information among different routers. The RIP contains the following fields in a message:



Routing Information Protocol (RIP)

Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.

Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.

Reserved: This is a reserved field, so it is filled with zeroes.

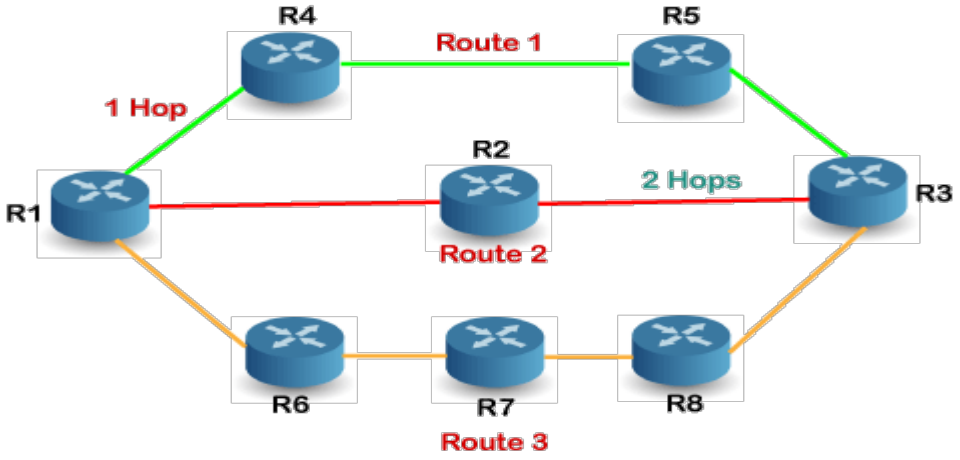
Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.

Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.

Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

Routing Information Protocol (RIP)

How does the RIP work?



- If there are 8 routers in a network where Router 1 wants to send the data to Router 3.
- If the network is configured with RIP, it will choose the route which has the least number of hops.
- There are three routes in the above network, i.e., Route 1, Route 2, and Route 3.
- The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

Border Gateway Protocol (BGP)

- It is an interdomain routing protocol, and it uses the path-vector routing.
- It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.
- An autonomous system is a collection of networks that comes under the single common administrative domain.
- Or we can say that it is a collection of routers under the single administrative domain.
- The protocol that is running on the internet or used to communicate between two different autonomous number systems is known as BGP (Border Gateway Protocol).
- The BGP is the only protocol that is running on the internet backbone or used to exchange the routes between two different autonomous number systems.
- Internet service providers use the BGP protocol to control all the routing information.

Border Gateway Protocol (BGP)

Characteristics of Border Gateway Protocol (BGP):

1.Inter-Autonomous System Configuration: The main role of BGP is to provide communication between two autonomous systems.

- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).

2.Path Information: BGP advertisement also include path information, along with the reachable destination and next destination pair.

3.Policy Support: BGP can implement policies that can be configured by the administrator.

- For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.

4.Runs Over TCP.

5.BGP conserve network Bandwidth.

6.BGP supports CIDR.

7.BGP also supports Security.

Border Gateway Protocol (BGP)

BGP Route Information Management Functions:

Route Storage: Each BGP stores information about how to reach other networks.

Route Update: In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.

Route Selection: Each BGP uses the information in its route databases to select good routes to each network on the internet network.

Route advertisement: Each BGP speaker regularly tells its peer what is knows about various networks and methods to reach them.

Border Gateway Protocol (BGP)

Membership

Border Gateway Protocol (BGP)

Membership

Question and Answer

1.