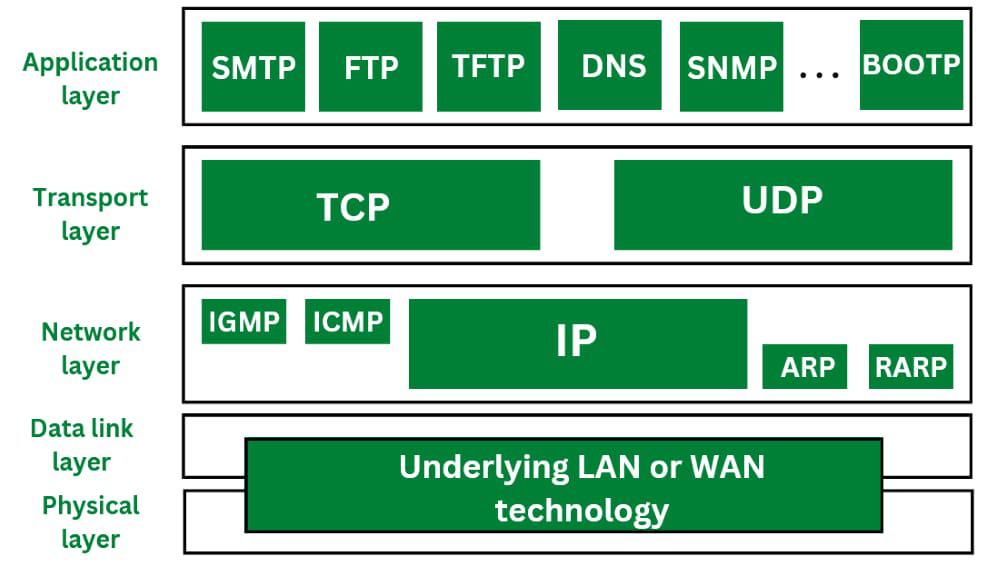
**Chapter 3** : Functions, Design Issues, Internetworks: Principle, Protocols and Operations, IP Protocol: IPv4 Header, Addresses, Operation, Subnetting, Classless, Network Address Translation, Internet Control Protocol - **ARP, RARP**, BOOTP, DHCP,**IGMP**; Problems of IPv4, IPv6, **Routing Algorithms, Interdomain Routing., OSPF, BGP.**

**Network Layer**

* The Network Layer is the third layer of the OSI model.
* It handles the service requests from the transport layer and further forwards the service request to the data link layer.
* The network layer translates the logical addresses into physical addresses
* It determines the route from the **source to the destination** and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
* The main role of the network layer is to move the packets from sending host to the receiving host.



**The main functions performed by the network layer are:**

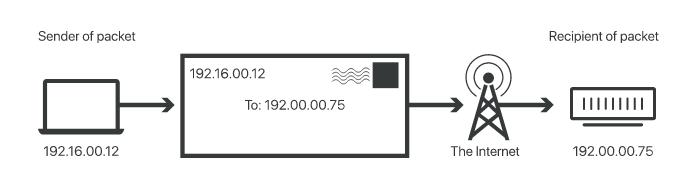
* **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link.
* **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
* **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
* **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

**Topic: IP**

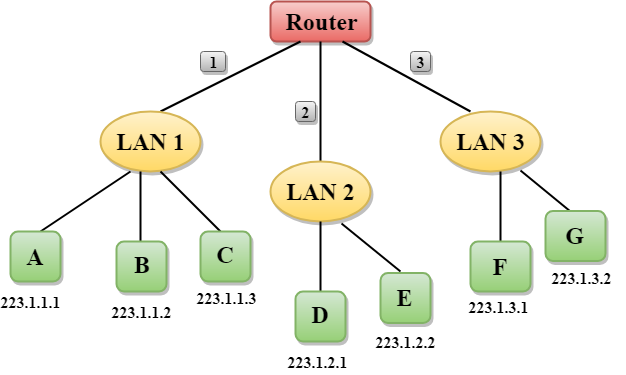
The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called [packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/). IP information is attached to each packet, and this information helps [routers](https://www.cloudflare.com/learning/network-layer/what-is-a-router/) to send packets to the right place. Every device or [domain](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) that connects to the Internet is assigned an [IP address](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and as packets are directed to the IP address attached to them, data arrives where it is needed.

## What is an IP address? How does IP addressing work?

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via [DNS](https://www.cloudflare.com/learning/dns/what-is-dns/) resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters. Each IP packet will contain both the IP address of the device or domain sending the packet and the IP address of the intended recipient, much like how both the destination address and the return address are included on a piece of mail.



**How do we setup LAN**

**Let's understand through a simple example.** 

* In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
* Each host contains its own interface and IP address.
* All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
* Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

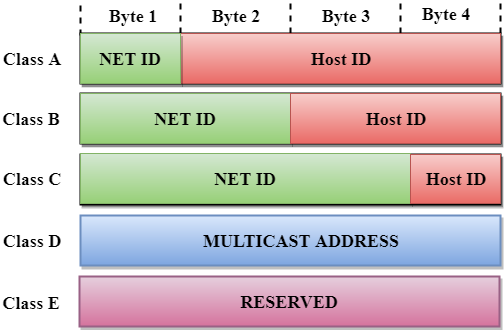
**Topic: Classful IP Addressing**

An IP address is 32-bit long. An IP address is divided into sub-classes:

* Class A
* Class B
* Class C
* Class D
* Class E

**An ip address is divided into two parts:**

* **Network ID:** It represents the number of networks.
* **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

## Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

* The network ID is 8 bits long.
* The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 27 = 128 network address

The total number of hosts in Class A = 224 - 2 = 16,777,214 host address



## Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

* The Network ID is 16 bits long.
* The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 214 = 16384 network address

The total number of hosts in Class B = 216 - 2 = 65534 host address

## Class C

In Class C, an IP address is assigned to only small-sized networks.

* The Network ID is 24 bits long.
* The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 221 = 2097152 network address

The total number of hosts = 28 - 2 = 254 host address



## Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



## Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



## Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

* The Host ID must be unique within any network.
* The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
* The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

## Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

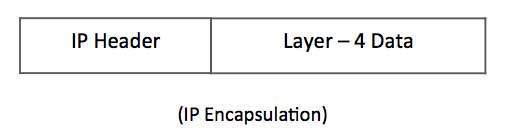
* The network ID cannot start with 127 as 127 is used by Class A.
* The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
* The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

## Classful Network Architecture

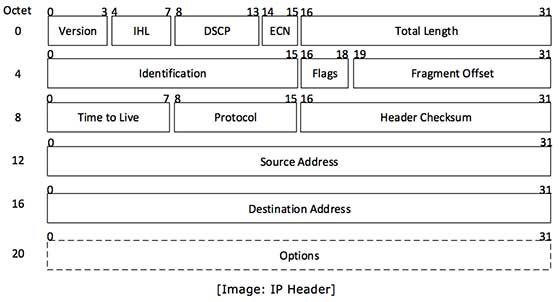
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Class** | **Higher bits** | **NET ID bits** | **HOST ID bits** | **No.of networks** | **No.of hosts per network** | **Range** |
| A | 0 | 8 | 24 | 27 | 224 | 0.0.0.0 to 127.255.255.255 |
| B | 10 | 16 | 16 | 214 | 216 | 128.0.0.0 to 191.255.255.255 |
| C | 110 | 24 | 8 | 221 | 28 | 192.0.0.0 to 223.255.255.255 |
| D | 1110 | Not Defined | Not Defined | Not Defined | Not Defined | 224.0.0.0 to 239.255.255.255 |
| E | 1111 | Not Defined | Not Defined | Not Defined | Not Defined | 240.0.0.0 to 255.255.255.255 |

**Topic: ipv4 header**

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.



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.
* **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.
* **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.

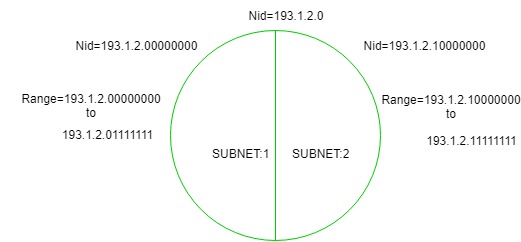
**Topic: subnetting**

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a [class A address](https://www.geeksforgeeks.org/introduction-of-classful-ip-addressing/), the possible number of hosts is 224 for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

## Uses of Subnetting

1. Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
2. Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
3. Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
4. Subnetting is used in increasing [network security](https://www.geeksforgeeks.org/network-security/).

The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

**Topic: ROUTING**

* A Routing is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
* A Router works at the network layer in the OSI model and internet layer in TCP/IP model
* A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
* The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
* The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
* The routing algorithm initializes and maintains the routing table for the process of path determination.

A routing table can be either static or dynamic. A *static table* is one with manual entries.

A *dynamic table,* on the other hand, is one that is updated automatically when there is a

change somewhere in the internet.

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

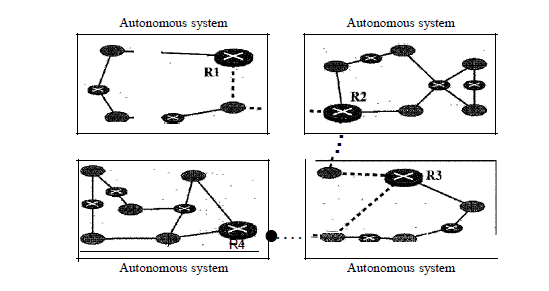
the internet inform each other of changes.

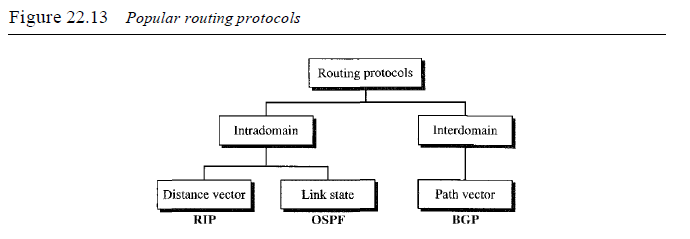
**Intra- and Interdomain Routing**

An autonomous system (AS) is a group of networks and routers under the authority of a single administration.

Routing inside an autonomous system is referred to as **intradomain routing.**

Routing between autonomous systems is referred to as **interdomain routing.**





Several intradomain and interdomain routing protocols are in use.

* Routing Information Protocol (RIP) is an implementation of the distance vector protocol.
* Open Shortest Path First (OSPF) is an implementation of the link state protocol.
* Border Gateway Protocol (BGP) is an implementation of the path vector protocol.

**Distance Vector Routing**

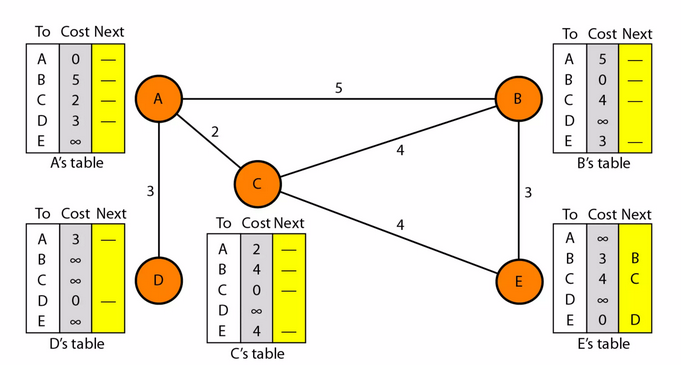
A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

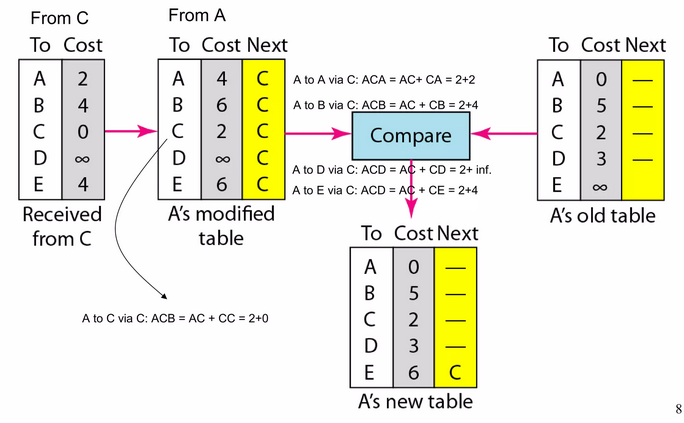
**Bellman Ford Basics –** Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors’ distance vectors.

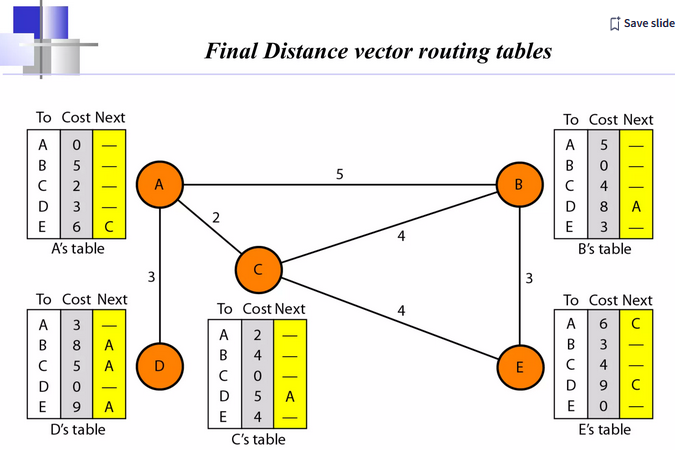
**Distance Vector Algorithm –**

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   * It receives a distance vector from a neighbor containing different information than before.
   * It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination.







**LINK STATE ROUTING**

## Link State Routing

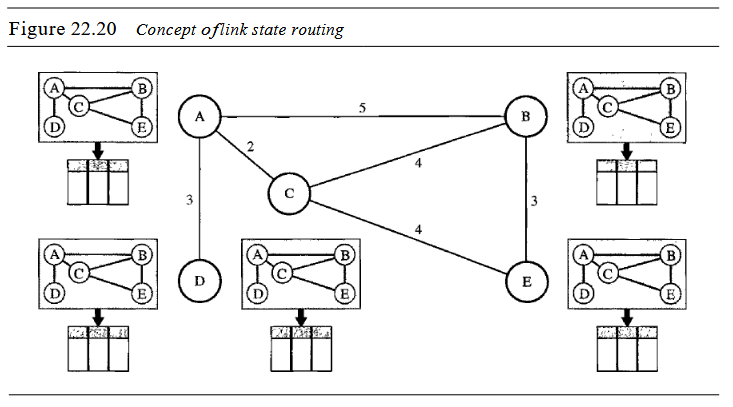
Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

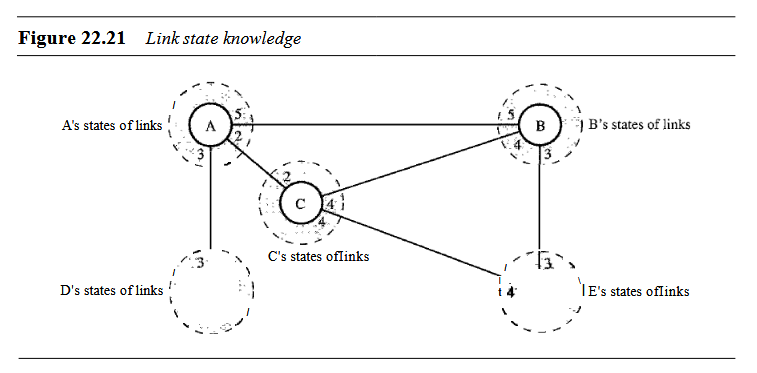
Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router i.e. the internet work. The three keys to understand the link state routing algorithm.

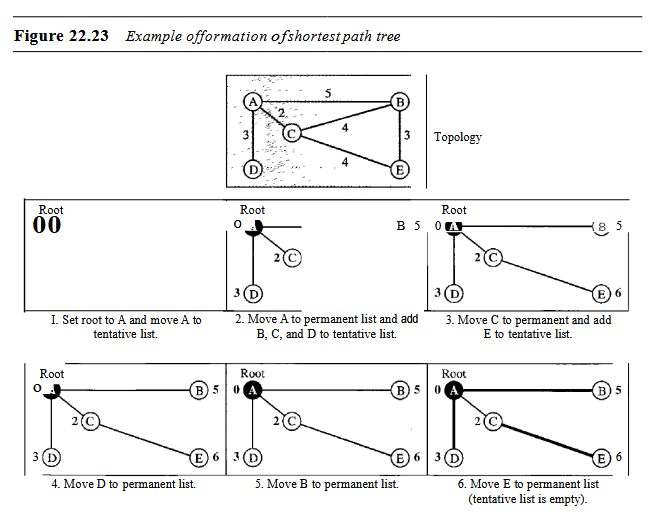
1. **Knowledge about the neighborhood**: Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
2. **Flooding:** Each router sends the information to every other router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

**Link state routing has two phase:**

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.



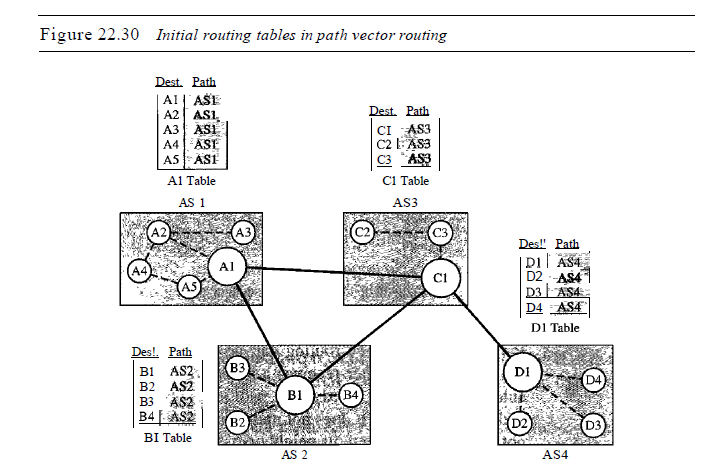




| **S.No.** | **Distance Vector Routing** | **Link State Routing** |
| --- | --- | --- |
| 1. | Bandwidth required is less due to local sharing, small packets and no flooding. | Bandwidth required is more due to flooding and sending of large link state packets. |
| 2. | Based on local knowledge, since it updates table based on information from neighbours. | Based on global knowledge, it have knowledge about entire network. |
| 3. | Make use of Bellman Ford Algorithm. | Make use of Dijakstra’s algorithm. |
| 4. | Traffic is less. | Traffic is more. |
| 5. | Converges slowly i.e, good news spread fast and bad news spread slowly. | Converges faster. |
| 6. | Count of infinity problem. | No count of infinity problem. |
| 7. | Persistent looping problem i.e, loop will be there forever. | No persistent loops, only transient loops. |
| 8. | Practical implementation is RIP and IGRP. | Practical implementation is **OSPF** and ISIS. |

**TOPIC 3: PATH VECTOR**

Path vector routing proved to be useful for interdomain routing. The principle of path vector routing is similar to that of distance vector routing. In path vector routing, we assume that there is one node (there can be more, but one is enough for our conceptual discussion) in each autonomous system that acts on behalf of the entire autonomous system. Let us call it the speaker node. The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs. The idea is the same as for distance vector routing except that only speaker nodes in each AS can communicate with each other. However, what is advertised is different. A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems.



**TOPIC: RIP, OSPF, BGP**

**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. It is a **distance-vector routing protocol** that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

#### **Hop Count**

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.

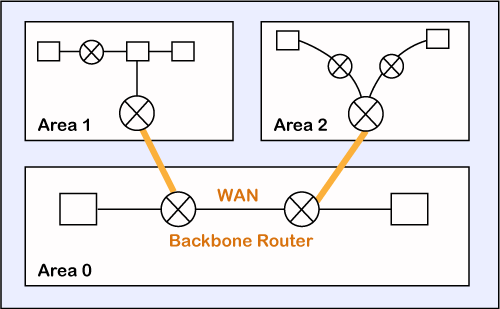
### ****Features of RIP****

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.

**OSPF**

The OSPF stands for **Open Shortest Path First**. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network. It is an interior gateway protocol that has been designed within a single autonomous system. It is based on a **link-state routing** algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to learn routes. The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network. The way the router learns this information by sending LSA (Link State Advertisements). These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB. The main goal is to have the same information about every router in an LSDBs.

### OSPF Areas



OSPF divides the autonomous systems into areas where the area is a collection of networks, hosts, and routers. Like internet service providers divide the internet into a different autonomous system for easy management and OSPF further divides the autonomous systems into Areas.

Routers that exist inside the area flood the area with routing information

In Area, the special router also exists. The special routers are those that are present at the border of an area, and these special routers are known as Area Border Routers. This router summarizes the information about an area and shares the information with other areas.

All the areas inside an autonomous system are connected to the backbone routers, and these backbone routers are part of a primary area. The role of a primary area is to provide communication between different areas.

### How does OSPF work?

**There are three steps that can explain the working of OSPF:**

**Step 1:** The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.

**Step 2:** The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.

**Step 3:** The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

**BGP**

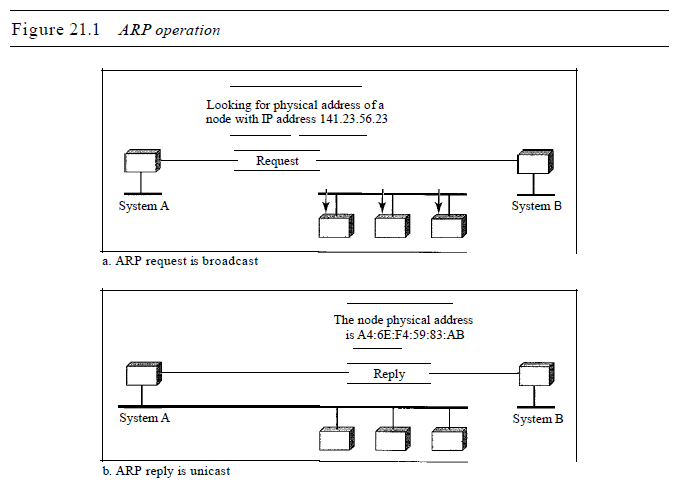
Border Gateway Protocol (BGP) refers to a gateway protocol that enables the internet to exchange routing information between autonomous systems (AS). As networks interact with each other, they need a way to communicate. This is accomplished through peering. BGP makes peering possible. Without it, networks would not be able to send and receive information with each other.

## How Does BGP Work?

When you have a network router that connects to other networks, it does not know which network is the best one to send its data to. BGP takes into consideration all the different peering options a router has and chooses the one closest to where the router is. Each potential peer communicates the routing information it has and that gets stored within a routing information base (RIB). BGP can access this information and use it to choose the best peering option.

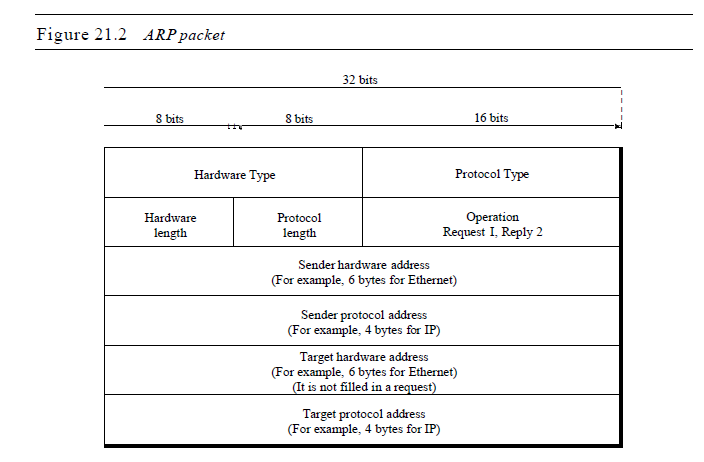
**Topic: ARP**

ARP stands for **Address Resolution Protocol**, which is **used to find the MAC address of the device from its known IP address.** This means, the source device already knows the IP address but not the MAC address of the destination device. The MAC address of the device is required because you cannot communicate with a device in a local area network (Ethernet) without knowing its MAC address. So, the Address Resolution Protocol helps to obtain the MAC address of the destination device.



The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network (see Figure 21.1).

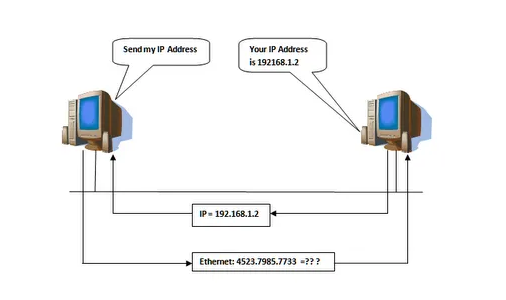
Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packet.



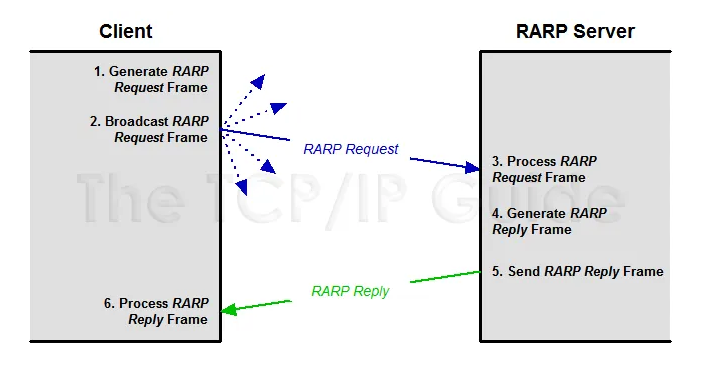
**TOPIC: RARP PROTOCOL**

The Reverse Address Resolution Protocol (RARP) is a networking protocol that is used to map a physical (MAC) address to an Internet Protocol (IP) address.

* Each network participant has two unique addresses more or less: a logical address (the IP address) and a physical address (the MAC address).
* While the IP address is assigned by software, the MAC address is built into the hardware.
* You have already been assigned a **Media Access Control address (MAC address)** by the manufacturer of your network card.
* There can be cases where the device could not save the IP address because there of insufficient memory available. In such cases, the **Reverse ARP** is used.
* This protocol can use the known **MAC address** to retrieve its IP address.
* Therefore, its function is the complete opposite of the **ARP.**
* The **ARP** uses the known IP address to determine the **MAC address** of the hardware.



* RARP is used by device A to say **“I am device A and I am sending this broadcast using my hardware address, can someone please tell me my IP address?”**
* It provides its own hardware address and asks for an IP address it can use.
* The response to a request returns the protocol address of the requesting station, not the address of the station receiving the request.
* Hosts like diskless workstations only have their hardware interface addresses or MAC address, but not their IP addresses.
* They must discover their **IP addresses** from an external source, usually via **RARP** protocol.
* **RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses.**
* MAC addresses need to be individually configured on the servers by an administrator.
* **RARP** is limited to serving only IP addresses.

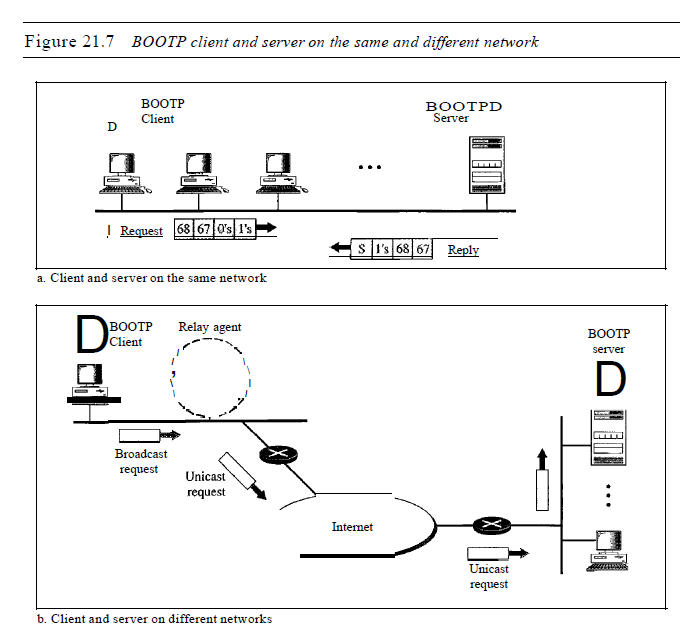


The Reverse Address Resolution Protocol has some disadvantages which eventually led to it being replaced by newer ones. To be able to use the protocol successfully, the RARP server has to be located in the **same physical network**.

The computer sends the RARP request on the lowest layer of the network. As a result, it is not possible for a router to forward the packet. **In addition, the RARP cannot handle subnetting because no subnet masks are sent.** If the network has been divided into multiple subnets, a RARP server must be available in each one. In addition, the network participant **only receives their own IP address** through the request. As previously mentioned, a subnet mask is not included and information about the gateway cannot be retrieved via Reverse ARP. Therefore, it is not possible to configure the computer in a modern network. These drawbacks led to the development of BOOTP and DHCP.

**Topic: BOOTP**

The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping. BOOTP is an application layer protocol. The administrator may put the client and the server on the same network or on different networks, as shown in Figure 21.7. BOOTP messages are encapsulated in a UDP packet, and the UDP packet itself is encapsulated in an IP packet.



One of the advantages of BOOTP over RARP is that **the client and server are application-layer processes.** As in other application-layer processes, a client can be in one network and the server in another, separated by several other networks. However, there is one problem that must be solved.

The BOOTP request is broadcast because the client does not know the IP address of the server. **A broadcast IP datagram cannot pass through any router.** To solve the problem, there is a need for an intermediary. One of the hosts (or a router that can be configured to operate at the application layer) can be used as a relay. The host in this case is called a **relay agent.** The relay agent knows the unicast address of a BOOTP server. When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the BOOTP server. The packet, carrying a unicast destination address, is routed by any router and reaches the BOOTP server. The BOOTP server knows the message comes from a relay agent because one of the fields in the request message defines the IP address of the relay agent. The relay agent, after receiving the reply, sends it to the BOOTP client.

**TOPIC: DHCP**

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

**DHCP does the following:**

* DHCP manages the provision of all the nodes or devices added or dropped from the network.
* DHCP maintains the unique IP address of the host using a DHCP server.
* It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

## Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

* **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
* **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
* **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
* **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
* **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
* **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

## Benefits of DHCP

There are following benefits of DHCP:

**Centralized administration of IP configuration:** DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

**Dynamic host configuration:** DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

**Seamless IP host configuration:** The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

**Flexibility and scalability:** Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

**TOPIC: IGMP**

IGMP is an abbreviated form of Internet Group Management Protocol(IGMP). Mainly the Internet Protocol can be involved in the two types of communication i.e, Unicasting and multicasting. IGMP is one of the necessary but not the efficient protocol that is involved in Multicasting.

IGMP is basically a companion of Internet Protocol(IP).

IGMP is not a multicasting routing protocol but it is a protocol that manages the group membership. This protocol mainly helps the multicast routers in order to create and update a list of loyal members that are related to each router interface.

This protocol is used in streaming videos, gaming, or web conferencing tools.

## IGMP Messages

There are two versions of IGMP: IGMPv1 and IGMPv2.

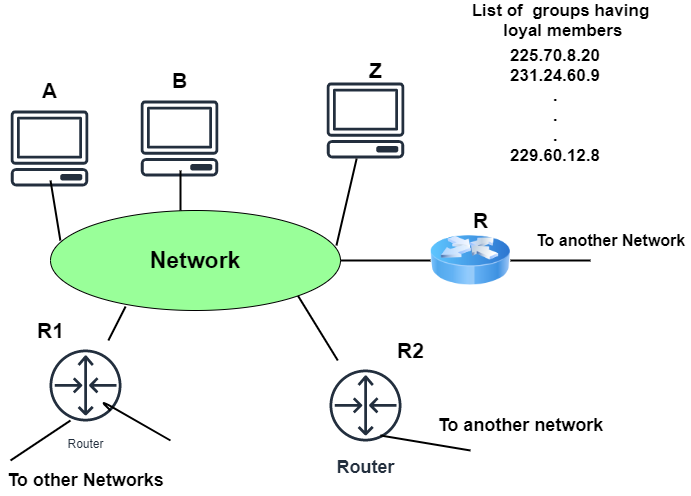
The version IGMPv2 has three types of messages:

* The Query
* The Membership report
* The Leave report.

## IGMP Operation

The Internet Group Management Protocol operates locally. The Multicast router that is connected to the network mainly has a list of multicast addresses of the group with at least one loyal member in that network. And for each group, there is mainly one router that has the duty of distributing the multicast packets destined for that group.

This simply indicates that in the case if there are three multicast routers connected to a network then their list of **groupids** are **mutually exclusive.**



Given below are the operations of IGMP:

* **Joining a Group**
  + In this operation, both the host and the router can join a group. Whenever a process on the host wants to join a group then it simply sends the request to the host. After that, the host then adds the name of the process and the name of the group to its list.
  + In case, if this is the first entry of that particular group, then the host sends the membership report message to the multicast router of the group.
  + And if the entry is not the first entry then there is no need of sending such a message.
* **Leaving a group**
  + Whenever the host finds that there is no process that is interested in the group then it mainly leaves a report message.
  + The membership is not disinfected by the multicast router of the group, rather than it immediately transmits the query packets repeatedly to see if anyone is still interested or not.
  + And in case if it gets the response in the form of a membership report message then the membership of the host or network is preserved.
* **Monitoring Membership**  
  Mainly the general query message does not define a particular group.
* **Delayed Response**  
  In order to prevent unnecessary traffic, the IGMP mainly makes use of a delayed response strategy.

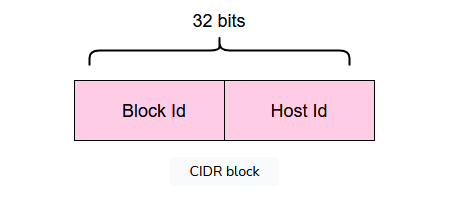
TOPIC: CLASSLESS ADDRESSING

**Classless addressing**, also called **Classless Inter-Domain Routing (CIDR)**,is an improved IP addressing system. It increases the effectiveness of IP address allocation because of the absence of class distribution.

**Structure**

The CIDR block comprises two parts. These are as follows:

* **Block id** is used for the network identification, but the number of bits is not pre-defined as it is in the classful IP addressing scheme.
* **Host id** is used to identify the host part of the network.



**Notation**

CIDR IP addresses look as follows:

w.x.y.z/n

In the example above,w,x,y,z each defines an 8-bit binary number, while n tells us about the number of bits used to identify the network and is called an **IP network prefix** or **mask**.

**Rules**

Requirements for CIDR are defined below:

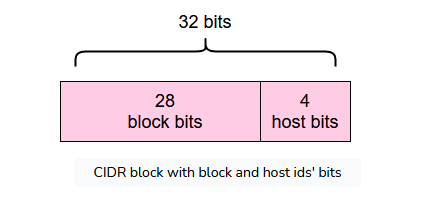
* Addresses should be contiguous.
* The number of addresses in the block must be in the power of 2.
* The first address of every block must be divisible by the size of the block.

**Block information**

Given the following IP address, let's find the network and host bits.

200.56.23.41/28

The following illustration gives a clear understanding of the aforementioned IP address scheme:



**Benefits**

Following are the benefits of classless IP addressing:

* Efficient IP address allocations.
* More balanced use of IP address ranges.
* More efficient routing.

TOPIC: IPV6 ADDRESSING

IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bits address having an address space of 2128, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:) .

### Components in Address format :

1. There are 8 groups and each group represents 2 Bytes (16-bits).
2. Each Hex-Digit is of 4 bits (1 nibble)
3. Delimiter used – colon (:)



## Need for IPv6:

The Main reason of IPv6 was the address depletion as the need for electronic devices rose quickly when [Internet Of Things (IOT)](https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/) came into picture after the 1980s & other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security.

IPv6 protocol responds to the above issues using the following main changes in the protocol:

#### **1. Large address space**

An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.

#### **2. Better header format**

IPv6 uses a new  header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data . This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

#### **3. New options**

IPv6 has new options to allow for additional functionalities.

#### **4. Allowance for extension**

IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

#### **5. Support for resource allocation**

In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

#### **6. Support for more security**

The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

In IPv6 representation, we have three addressing methods :

* Unicast
* Multicast
* Anycast