UNIT : 3

# Internet Address

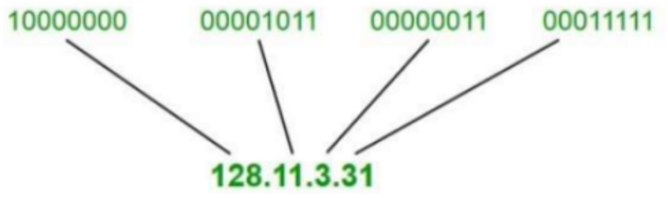
An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. Computers that communicate over the internet or via local networks share information to a specific location using IP addresses.

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 232.

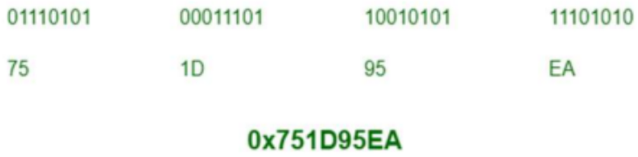
Every device with an internet connection has an IP address, whether it's a computer, laptop, IoT device, or even toys. The IP addresses allow for the efficient transfer of data between two connected devices, allowing machines on different networks to talk to each other.

Generally, there are two notations in which an IP address is written:

Dotted Decimal Notation:



Hexadecimal Notation:



01110101	00011101	10010101	11101010
75	1D	95	EA

0x751D95EA

Working of IP addresses

- Your device directly requests your Internet Service Provider which then grants your device access to the web.
- And an IP Address is assigned to your device from the given range available.
- Your internet activity goes through your service provider, and they route it back to you, using your IP address.
- Your IP address can change. For example, turning your router on or off can change your IP Address.
- When you are out of your home location your home IP address doesn't accompany you. It changes as you change the network of your device.

Types of IP Address

1. IPv4 (Internet Protocol version 4)

It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices can be assigned with IPv4.

IPv4 can be written as: 189.123.123.90

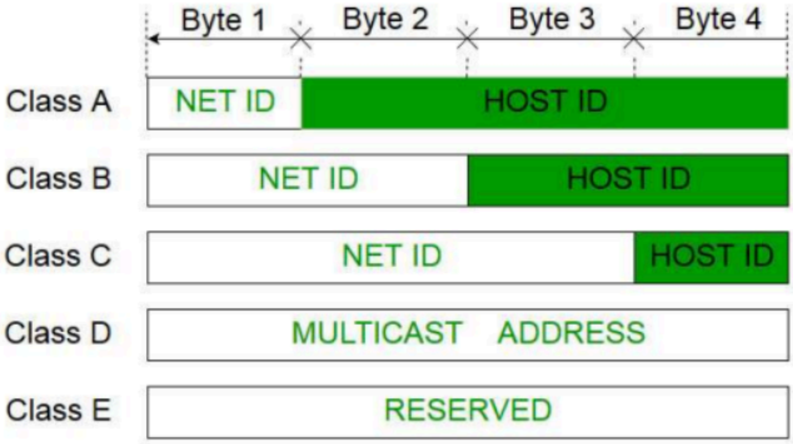
2. IPv6 (Internet Protocol version 6)

There is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to IPv6 Address which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons(:). But in the computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^128) devices can be assigned with unique addresses which are actually more than enough for upcoming future generations.

IPv6 can be written as: 2011:0bd9:75c5:0000:0000:6b3e:0170:8394

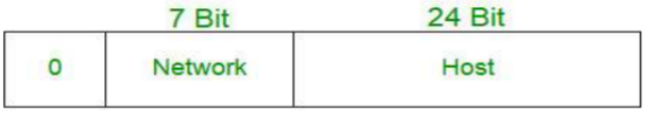
Classful Addressing

The 32 bit IP address is divided into five subclasses. These are: Class A, class B, Class C, Class D, Class E. Each of these classes has a valid range of IP addresses. The order of bits in the first octet determines the classes of IP addresses.



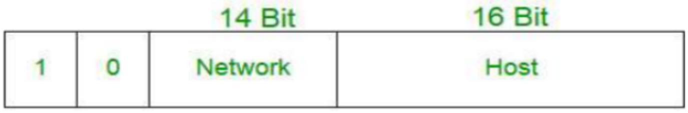
Class A:

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts. The network ID is 8 bits long. The host ID is 24 bits long.



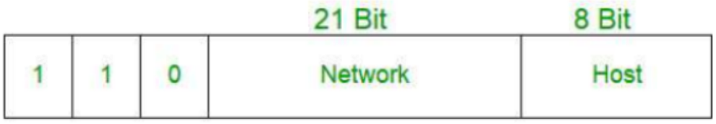
Class B:

IP addresses belonging to class B are assigned to the networks that range from medium-sized to large-sized networks. The network ID is 16 bits long. The host ID is 16 bits long.



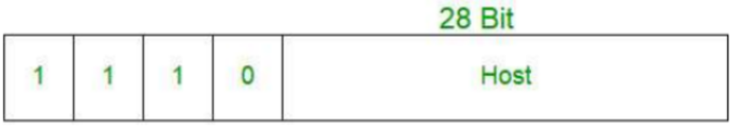
Class C:

IP addresses belonging to class C are assigned to small-sized networks. The network ID is 24 bits long. The host ID is 8 bits long.



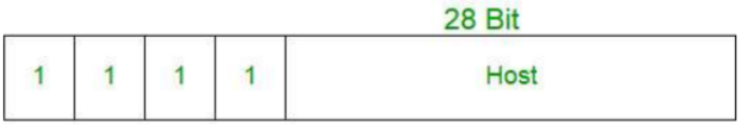
Class D:

IP addresses belonging to class D are reserved for multicasting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.



Class E:

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



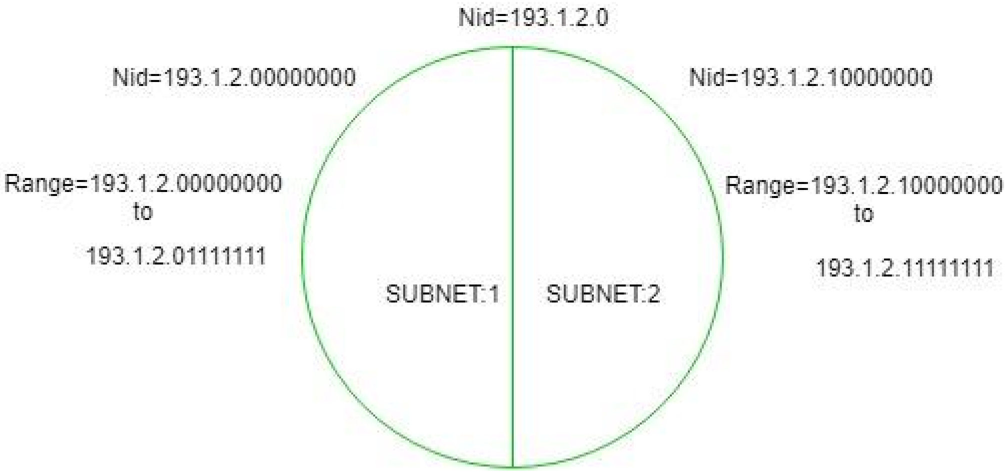
# Subnetting

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, 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

- Subnetting helps in organising the network in an efficient way.
- Subnetting is used for specific staffing structures to reduce traffic.
- Subnetting is used in increasing 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.



How Does Subnetting Work?

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

In class C the first 3 octets are network bits so it remains as it is.

For Subnet-1: The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part. Thus, the range of subnet 1 is: 193.1.2.0 to 193.1.2.127 Subnet id of Subnet-1 is : 193.1.2.0 The total number of hosts possible is: 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)

For Subnet-2: The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111). Thus, the range of subnet-2 is: 193.1.2.128 to 193.1.2.255 Subnet id of Subnet-2 is : 193.1.2.128 The total number of hosts possible is: 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)

Finally, after using the subnetting the total number of usable hosts is reduced from 254 to 252.

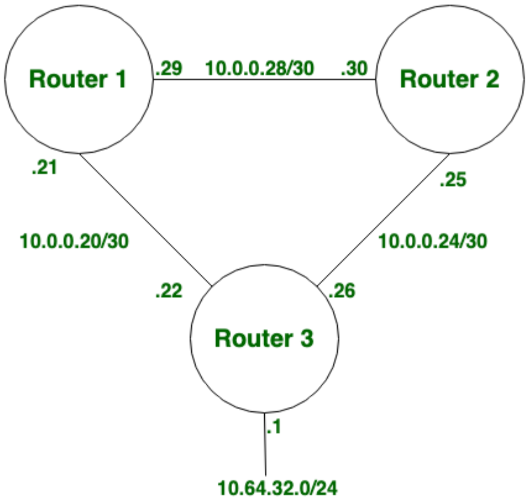
# Routing

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

Static Routing:

Static Routing is also known as non-adaptive routing which doesn't change the routing table unless the network administrator changes or modifies them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing.

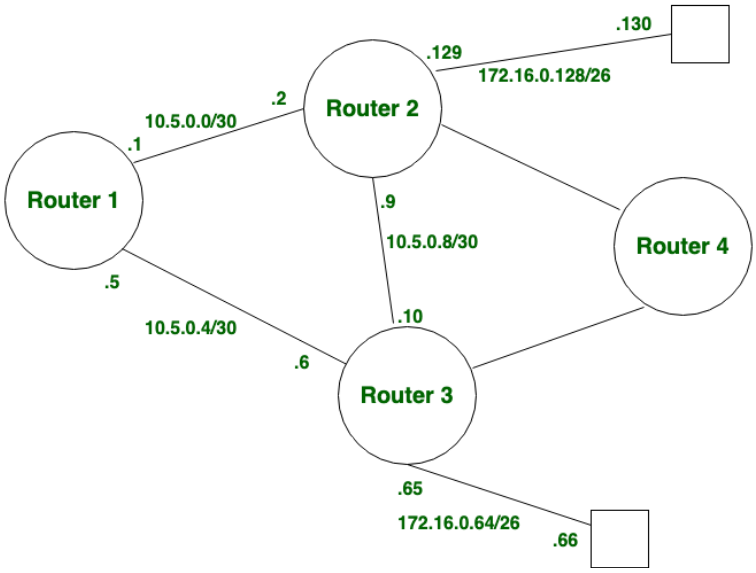
Configuration:



Dynamic Routing:

Dynamic routing is also known as adaptive routing which changes the routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide high security like static routing. When the network change(topology) occurs, it sends the message to the router to ensure that changes then the routes are recalculated for sending updated routing information.

Configuration:



S.No.	Static Routing	Dynamic Routing
1	In static routing, routes are user-defined	In dynamic routing, routes are updated according to the topology
2	It does not use complex routing algorithms	It uses complex routing algorithms
3	It provides high security	It provides less security
4	It is manual	It is automated
5	It is implemented in small networks	It is implemented in large networks
6	Additional resources are not required	Additional resources are required
7	Failure of link disrupts the rerouting	Failure of link does not interrupt the rerouting
8	Less bandwidth is required	More bandwidth is required
9	It is difficult to configure	It is easy to configure
10	It is non-adaptive routing	It is adaptive routing

# Routing Table

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets travelling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
default		Eth2

The entry corresponding to the default gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of default route is always 255.255.255.255 .

Entries of an IP Routing Table:

- **Destination:** This is the IP address of the packet's final destination.
- **Subnet mask:** Also known as the netmask, this is a 32-bit network address that identifies whether a host belongs to the local or remote network. To enhance routing efficiency and reduce the size of the broadcast domain, administrators can apply a custom subnet mask through the process of subnetting, which can divide a network into two or smaller connected networks.
- **Gateway:** This is the next hop, or the neighbouring device's IP address to which the packet is forwarded.
- **Interface:** Routers typically use Ethernet interfaces to connect to other devices on the same network, such as eth0 or eth1, and serial interfaces to connect to outside wide area networks (WANs). The routing table lists the inbound network interface, also known as the outgoing interface, that the device should use when forwarding the packet to the next hop.
- **Metric:** This entry assigns a value to each available route to a specific network. The value ensures that the router can choose the most effective path. In some cases, the metric is the number of routers that a data packet must cross before it gets to the destination address. If multiple routes exist to the same destination network, the path with the lowest metric is given precedence.

- **Routes:** This includes directly attached subnets, indirect subnets that aren't attached to the device but can be accessed through one or more hops, and default routes to use for certain types of traffic or when information is lacking.

When a router receives a packet, it examines the destination IP address, and looks up into its Routing Table to figure out which interface packet will be sent out.

There are ways to maintain Routing Table:

- Directly connected networks are added automatically.
- Using Static Routing.
- Using Dynamic Routing.

Routing table working:

The main purpose of a routing table is to help routers make effective routing decisions. Whenever a packet is sent through a router to be forwarded to a host on another network, the router consults the routing table to find the IP address of the destination device and the best path to reach it. The packet is then directed to a neighbouring router -- or the next hop listed in the table -- until it reaches its final destination

# DHCP

Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

- Subnet Mask (Option 1 – e.g., 255.255.255.0)
- Router Address (Option 3 – e.g., 192.168.1.1)
- DNS Address (Option 6 – e.g., 8.8.8.8)
- Vendor Class Identifier (Option 43 – e.g., ‘unifi’ = 192.168.1.9 ##where unifi = controller)

Working of DHCP

DHCP works on the Application layer of the TCP/IP Protocol. The main task of DHCP is to dynamically assign IP Addresses to the Clients and allocate information on TCP/IP configuration to Clients. For more, you can refer to the Article Working of DHCP.

The DHCP port number for the server is 67 and for the client is 68. It is a client-server protocol that uses UDP services. An IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called the DORA process, but there are 8 DHCP messages in the process.

The 8 DHCP Messages:

1. DHCP discover message: This is the first message generated in the communication process between the server and the client. This message is generated by the Client host in order to discover if there is any DHCP server/servers present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long

2. DHCP offers a message: The server will respond to the host in this message specifying the unleashed IP address and other TCP configuration information. This message is broadcasted by the server. The size of the message is 342 bytes. If there is more than one DHCP server present in the network then the client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.

3. DHCP request message: When a client receives an offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with the same IP address. If there is no reply from another host, then there is no host with the same TCP configuration in the network and the message is broadcasted to the server showing the acceptance of the IP address. A Client ID is also added to this message.

4. DHCP acknowledgment message: In response to the request message received, the server will make an entry with a specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by the server.

5. DHCP negative acknowledgment message: Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that are configured, it sends a DHCP Nak message to the client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to the client.

6. DHCP decline: If the DHCP client determines the offered configuration parameters are different or invalid, it sends a DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends a DHCP decline message to the server showing the offered IP address is already in use.

7. DHCP release: A DHCP client sends a DHCP release packet to the server to release the IP address and cancel any remaining lease time.

8. DHCP inform: If a client address has obtained an IP address manually then the client uses DHCP information to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, the DHCP server generates a DHCP ack message with a local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Advantages of DHCP

- Centralised management of IP addresses.
- Centralised and automated TCP/IP configuration.
- Ease of adding new clients to a network.
- Reuse of IP addresses reduces the total number of IP addresses that are required.

Disadvantages of DHCP

- IP conflict can occur.
- The client is not able to access the network in absence of a DHCP Server.

# IEEE Standards 802.x

The IEEE 802 Standard comprises a family of networking standards that cover the physical layer specifications of technologies from Ethernet to wireless.

IEEE 802 is subdivided into 22 parts that cover the physical and data-link aspects of networking.

The better known specifications (bold in table below) include 802.3 Ethernet, 802.11 Wi-Fi, 802.15 Bluetooth/ZigBee, and 802.16

Working:

- Initiation : The authenticator (typically a switch) or supplicant (client device) sends a session initiation request. A supplicant sends an EAP-response message to the authenticator, which encapsulates the message and forwards it to the authentication server.

- Authentication : Messages pass between the authentication server and the supplicant via the authenticator to validate several pieces of information.

- Authorization : If the credentials are valid, the authentication server notifies the authenticator to give the supplicant access to the port.

- Accounting : RADIUS accounting keeps session records including user and device details, session types, and service details.

- Termination : Sessions are terminated by disconnecting the endpoint device, or by using management software.

IEEE standards in CN	Description
IEEE 802	It is used for the overview and architecture of LAN/MAN.
IEEE 802.1	It is used for bridging and management of LAN/MAN.
IEEE 802.1s	It is used in multiple spanning trees.
IEEE 802.1w	It is used for rapid reconfiguration of spanning trees.
IEEE 802.1x	It is used for network access control of ports.
IEEE 802.2	It is used in Logical Link Control (LLC).
IEEE 802.3	It is used in Ethernet.
IEEE 802.4	It is used for token passing bus access methods.
IEEE 802.5	It is used for token ring access methods.
IEEE 802.6	It is used for the physical layer specifications (MAN).
IEEE 802.7	It is used in broadband LAN.
IEEE 802.8	It is used in fibre optics.

# Shortest Path Algorithm

In computer networks, the shortest path algorithms aim to find the optimal paths between the network nodes so that routing cost is minimised. They are direct applications of the shortest path algorithms proposed in graph theory.

Explanation

Consider that a network comprises N vertices (nodes) that are connected by M edges. Each edge is associated with a weight. The target of shortest path algorithms is to find a route between any pair of vertices along the edges, so the sum of weights of edges is minimum. If the edges are of equal weights, the shortest path algorithm aims to find a route having a minimum number of hops.

Common Shortest Path Algorithms:

- Bellman Ford’s Algorithm
- Dijkstra’s Algorithm
- Floyd Warshall’s Algorithm

i) Bellman Ford Algorithm

Input : A graph representing the network; and a source node, s

Output : Shortest path from s to all other nodes.

Initialize distances from s to all nodes as infinite (∞); distance to itself as 0; an array dist[ ] of size |V| (number of nodes) with all values as ∞ except dist[s].

Calculate the shortest distances iteratively. Repeat |V|- 1 times for each node except s

Repeat for each edge connecting vertices u and v

If dist[v] > (dist[u] + weight of edge u-v), Then

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

The array dist[ ] contains the shortest path from s to every other node.

ii) Dijkstra's Algorithm

Input : A graph representing the network; and a source node, s

Output : A shortest path tree, spt[], with s as the root node.

Initializations :

An array of distances dist[ ] of size |V| (number of nodes), where dist[s] = 0 and dist[u] = ∞ (infinite), where u represents a node in the graph except s.

An array, Q, containing all nodes in the graph. When the algorithm runs into completion, Q will become empty.

An empty set, S, to which the visited nodes will be added. When the algorithm runs into completion, S will contain all the nodes in the graph.

Repeat while Q is not empty −

Remove from Q, the node, u having the smallest dist[u] and which is not in S. In the first run, dist[s] is removed.

Add u to S, marking u as visited.

For each node v which is adjacent to u, update dist[v] as −

If (dist[u] + weight of edge u-v) < dist[v], Then

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

The array dist[ ] contains the shortest path from s to every other node.

iii) Floyd Warshall Algorithm

Input − A cost adjacency matrix, adj[][], representing the paths between the nodes in the network.

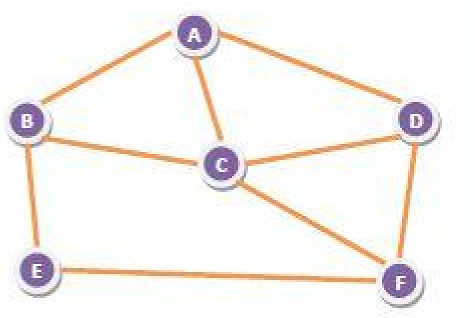
Output − A shortest path cost matrix, cost[][], showing the shortest paths in terms of cost between each pair of nodes in the graph.

```
Populate cost[ ][ ] as follows:
If adj[ ][ ] is empty Then cost[ ][ ] = ∞ (infinite)
Else cost[ ][ ] = adj[ ][ ]
N = |V|, where V represents the set of nodes in the network.
Repeat for k = 1 to N −
    Repeat for i = 1 to N −
        Repeat for j = 1 to N −
            If cost[i][k] + cost[k][j] < cost[i][j], Then
                Update cost[i][j] := cost[i][k] + cost[k][j]
The matrix cost[ ][ ] contains the shortest cost from each node, i , to every other node, j.
```

# Flooding

Flooding is a non-adaptive routing technique following this simple method: when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on.

For example, let us consider the network in the figure, having six routers that are connected through transmission lines.



Using flooding technique −

An incoming packet to A, will be sent to B, C and D.
B will send the packet to C and E.
C will send the packet to B, D and F.
D will send the packet to C and F.
E will send the packet to F.
F will send the packet to C and E.

Types of Flooding

Uncontrolled flooding : Here, each router unconditionally transmits the incoming data packets to all its neighbours.

Controlled flooding : They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF).

Selective flooding : The routers don't transmit the incoming packets only along those paths which are heading approximately in the right direction, instead of every available path.

Advantages of Flooding

- It is very simple to set up and implement, since a router may know only its neighbours.
- It is extremely robust. Even in case of malfunctioning of a large number routers, the packets find a way to reach the destination.
- All nodes which are directly or indirectly connected are visited. So, there are no chances for any node to be left out. This is a main criteria in case of broadcast messages.
- The shortest path is always chosen by flooding.

Limitations of Flooding

- Flooding tends to create an infinite number of duplicate data packets, unless some measures are adopted to damp packet generation.
- It is wasteful if a single destination needs the packet, since it delivers the data packet to all nodes irrespective of the destination.
- The network may be clogged with unwanted and duplicate data packets. This may hamper delivery of other data packets.

# Distance Vector Algorithm

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

The DV calculation is based on minimising the cost to each destination

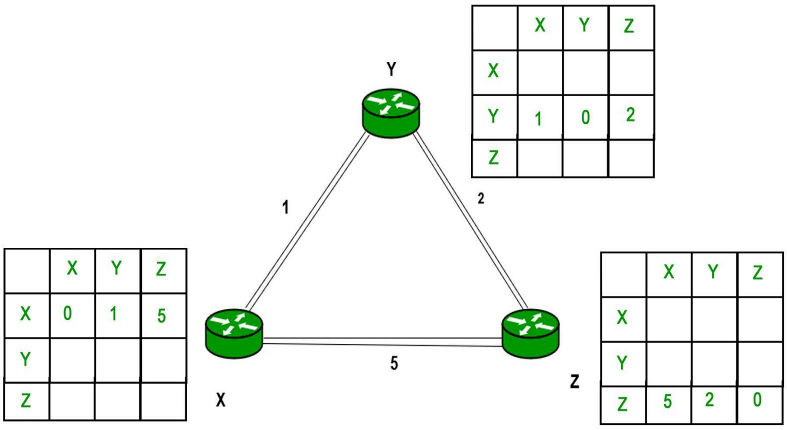
Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbour v

Dx = [Dx(y): y ? N] = Node x maintains distance vector

Node x also maintains its neighbours' distance vectors: For each neighbour v, x maintains Dv = [Dv(y): y ? N]

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



	X	Y	Z
X			
Y	1	0	2
Z			

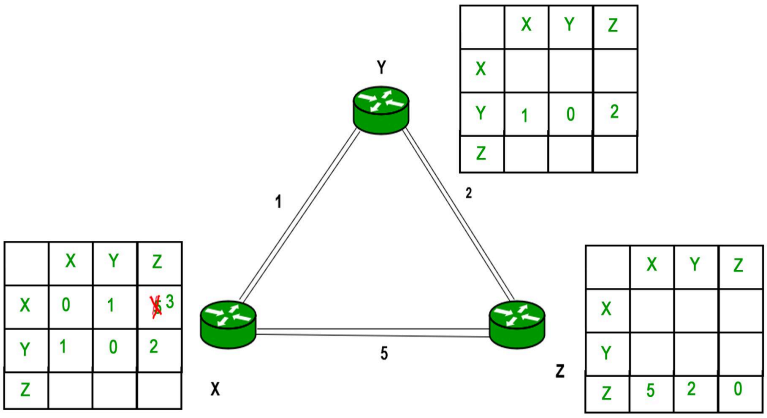
	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Consider router X , X will share its routing table to neighbours and neighbours will share it routing table to it to X and distance from node X to destination will be calculated using bellman- ford equation.

Dx(y) = min { C(x,v) + Dv(y)} for each node y ? N

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

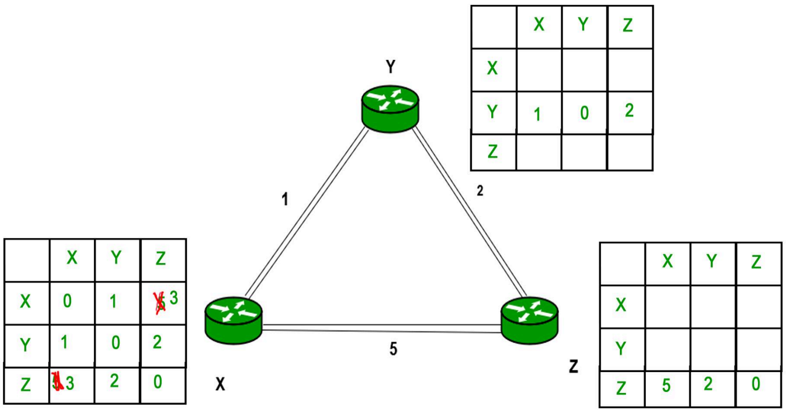


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Similarly for Z also –

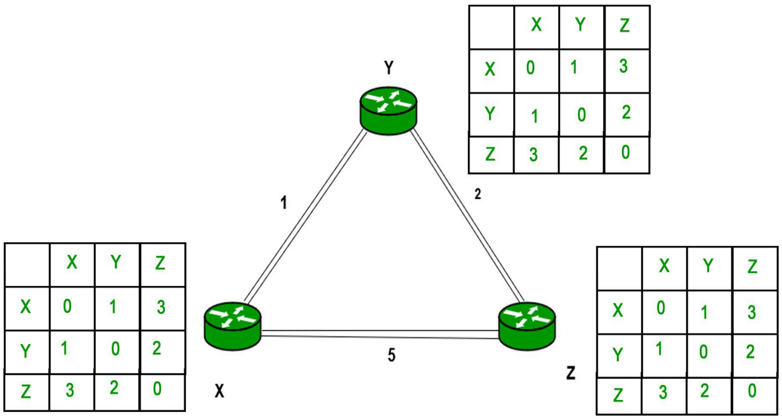


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z	~~5~~ 3	2	0

	X	Y	Z
X			
Y			
Z	5	2	0

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

Advantage : It is simpler to configure and maintain than link state routing.

Disadvantages :

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- 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.

# Link State Routing Algorithm

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 a shortest path computation.

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 has two phases:

i) Reliable Flooding

- ○ Initial state: Each node knows the cost of its neighbours.
- ○ Final state: Each node knows the entire graph.

ii) Route Calculation

To find the shortest path, each node needs to run the famous Dijkstra algorithm. This famous algorithm uses the following steps:

Step-1: The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database

Step-2: Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree.The shape of the tree gets changed .

Step-3: After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.

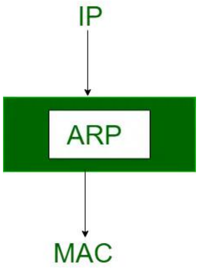
Step-4: The node repeats Step 2. and Step 3. until all the nodes are added in the tree

Features of Link State Routing Protocols

- Link State Packet: A small packet that contains routing information.
- Link-State Database: A collection of information gathered from the link-state packet.
- Shortest Path First Algorithm (Dijkstra algorithm): A calculation performed on the database results in the shortest path
- Routing Table: A list of known paths and interfaces.

# ARP

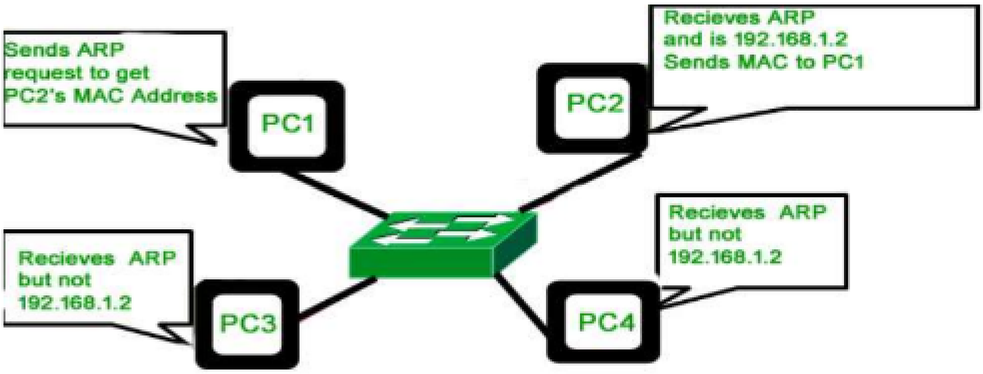
The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Data link layer in the OSI model. It is responsible to find the hardware address of a host from a known IP address.



Most of the computer applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address). So, our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical address.

ARP working

Before sending the IP packet, the MAC address of the destination must be known. If not so, then the sender broadcasts the ARP-discovery packet requesting the MAC address of the intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP- reply) to the sender of ARP-discovery packet. After the original sender receives the ARP- reply, it updates ARP-cache and starts sending a unicast message to the destination.


Sends ARP request to get PC2's MAC Address
PC1
Recieves ARP and is 192.168.1.2 Sends MAC to PC1
PC2
Recieves ARP but not 192.168.1.2
PC3
Recieves ARP but not 192.168.1.2
PC4

The important terms associated with ARP are :

ARP Cache: After resolving MAC address, the ARP sends it to the source where it stores in a table for future reference. The subsequent communications can use the MAC address from the table

ARP Cache Timeout: It indicates the time for which the MAC address in the ARP cache can reside

ARP request: This is nothing but broadcasting a packet over the network to validate whether we came across a destination MAC address or not.

Cases when ARP is used:

CASE 1: The sender is a host and wants to send a packet to another host on the same network. Use ARP to find another host's physical address

CASE 2: The sender is a host and wants to send a packet to another host on another network. Sender looks at its routing table. Find the IP address of the next hop (router) for this destination. Use ARP to find the router's physical address

CASE 3: the sender is a router and received a datagram destined for a host on another network. Router checks its routing table. Find the IP address of the next router. Use ARP to find the next router's physical address.

CASE 4: The sender is a router that has received a datagram destined for a host in the same network. Use ARP to find this host's physical address.

# RARP

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. It is the reverse of the more commonly used Address Resolution Protocol (ARP), which maps an IP address to a MAC address.

RARP was developed in the early days of computer networking as a way to provide IP addresses to the devices that could not store their own IP addresses. With RARP, the device would broadcast its MAC address and request an IP address, and a RARP server on the network would respond with the corresponding IP address.

While RARP was widely used in the past, it has largely been replaced by newer protocols such as DHCP, which provides more flexibility and functionality in assigning IP addresses dynamically.

Working of RARP :

The RARP is on the Network Access Layer and is employed to send data between two points in a network. The IP address gets assigned by software and after that the MAC address is constructed into the hardware.

The RARP server that responds to RARP requests, can even be any normal computer within the network. However, it must hold the data of all the MAC addresses with their assigned IP addresses. If a RARP request is received by the network, only these RARP servers can reply to it. The info packet needs to be sent on very cheap layers of the network. This implies that the packet is transferred to all the participants at the identical time.

The client broadcasts a RARP request with an Ethernet broadcast address and with its own physical address. The server responds by informing the client its IP address.

Uses of RARP :

RARP is used to convert the Ethernet address to an IP address. It is available for the LAN technologies like FDDI, token ring LANs, etc.

RARP VS ARP

RARP	ARP
RARP stands for Reverse Address Resolution Protocol	ARP stands for Address Resolution Protocol
A protocol used to map a physical (MAC) address to an IP address	A protocol used to map an IP address to a physical (MAC) address
To obtain the IP address of a network device when only its MAC address is known	To obtain the MAC address of a network device when only its IP address is known
Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address	Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address
Rarely used in modern networks as most devices have a pre-assigned IP address	Widely used in modern networks to resolve IP addresses to MAC addresses
RFC 903 Standardization	RFC 826 Standardization
In RARP, we find our own IP address	In ARP, we find the IP address of a remote machine
The MAC address is known and the IP address is requested	The IP address is known, and the MAC address is being requested
It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses

IP

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.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.

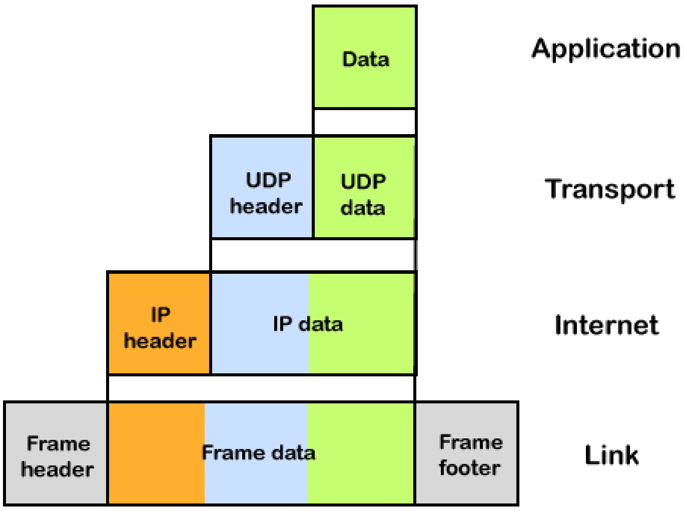
The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.

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:

○ Format of IP packet

○ IP Addressing system



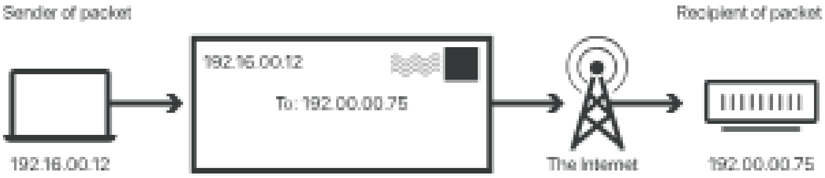
An IP header contains lots of information about the IP packet which includes:

- Source IP address: The source is the one who is sending the data.
- Destination IP address: The destination is a host that receives the data from the sender.
- Header length

- Packet length
- TTL (Time to Live): The number of hops occurs before the packet gets discarded.
- Transport protocol: either it can be TCP or UDP.

Working of Internet Protocol

The internet and many other data networks work by organising data into small pieces called packets. Each large data sent between two network devices is divided into smaller packets by the underlying hardware and software. Each network protocol defines the rules for how its data packets must be organised in specific ways according to the protocols the network supports.



IPv4 vs. IPv6

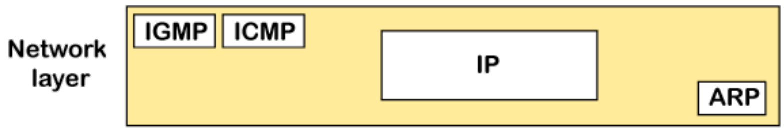
The fourth version of IP (IPv4 for short) was introduced in 1983. However, just as there are only so many possible permutations for automobile licence plate numbers and they have to be reformatted periodically, the supply of available IPv4 addresses has become depleted. IPv6 addresses have many more characters and thus more permutations; however, IPv6 is not yet completely adopted, and most domains and devices still have IPv4 addresses.

# ICMP

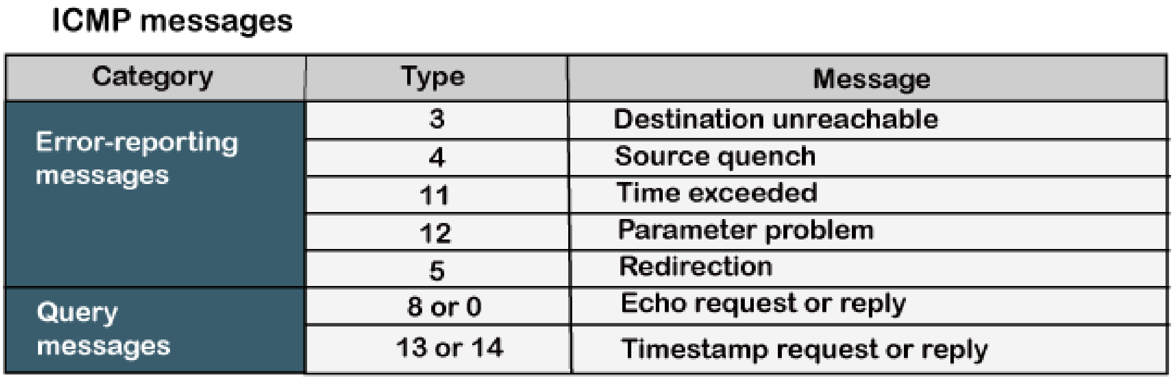
The ICMP stands for Internet Control Message Protocol. It is a network layer protocol. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, ICMP can be used to report these errors and to debug those errors. For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.

The IP protocol does not have any error-reporting or error-correcting mechanism, so it uses a message to convey the information. For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination. If no one reports the error, then the sender might think that the message has reached the destination. If someone in-between reports the error, then the sender will resend the message very quickly.

Position of ICMP in the network layer



The ICMP messages are usually divided into two categories:



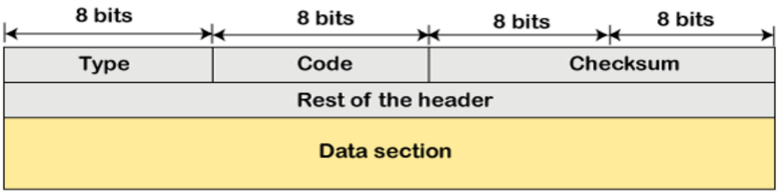
ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

- Error-reporting messages: The error-reporting message means that the router encounters a problem when it processes an IP packet then it reports a message.
- Query messages: The query messages are those messages that help the host to get the specific information of another host. For example, suppose there is a client and a server, and the client wants to know whether the server is live or not, then it sends the ICMP message to the server.

ICMP Message Format: The message format has two things; one is a category that tells us which type of message it is. The type defines the type of message while the code defines the subtype of the message.

The ICMP message contains the following fields:



- Type: It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.

- Code: It is an 8-bit field that defines the subtype of the ICMP message
- Checksum: It is a 16-bit field to detect whether the error exists in the message or not.

# IGMP

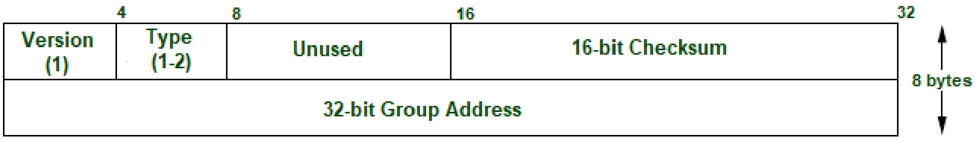
IGMP is an acronym for Internet Group Management Protocol. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on the network layer.

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.

Types:

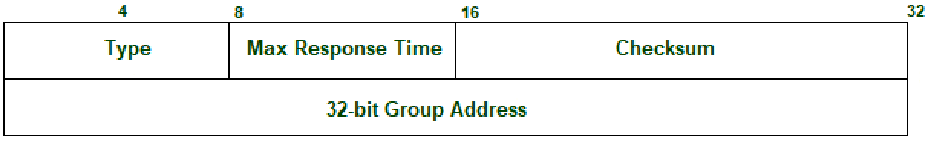
There are 3 versions of IGMP. These versions are backward compatible.

1. IGMPv1 : The version of IGMP communication protocol allows all the supporting hosts to join the multicast groups using membership requests and include some basic features. But, the host cannot leave the group on their own and have to wait for a timeout to leave the group.



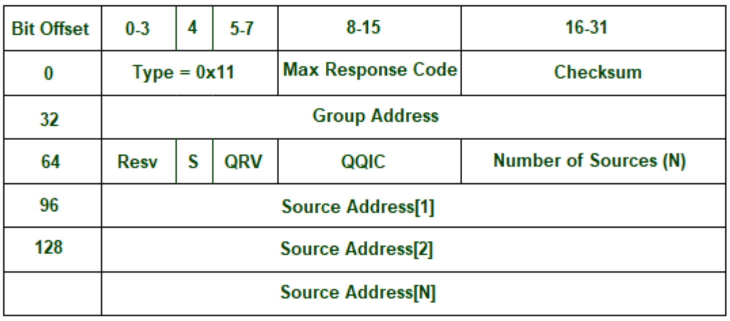
4	8	16	32
Version (1)	Type (1-2)	Unused	16-bit Checksum
32-bit Group Address			

2. IGMPv2 : IGMPv2 is the revised version of IGMPv1 communication protocol. It has added functionality of leaving the multicast group using group membership.



4	8	16	32
Type	Max Response Time	Checksum	
32-bit Group Address			

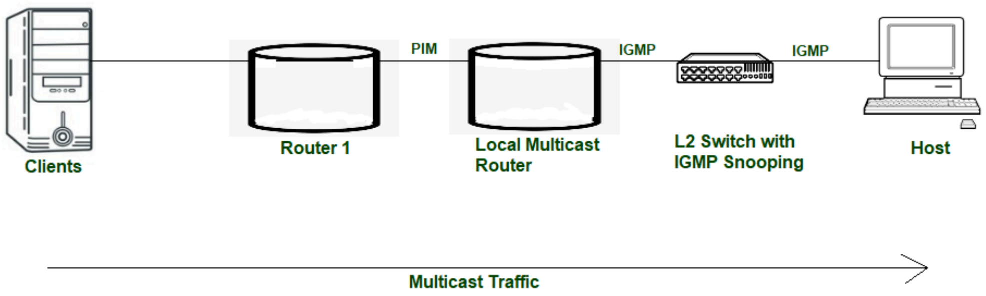
3. IGMPv3 : IGMPv2 was revised to IGMPv3 and added source-specific multicast and membership report aggregation. These reports are sent to 224.0.0.22.



Bit Offset	0-3	4	5-7	8-15	16-31
0	Type = 0x11			Max Response Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address[1]				
128	Source Address[2]				
	Source Address[N]				

Working: IGMP works on devices that are capable of handling multicast groups and dynamic multicasting. These devices allow the host to join or leave the membership in the multicast group. These devices also allow clients to add and remove clients from the group. This communication protocol is operated between host and local multicast router. When a multicast group is created, the multicast group address is in range of class D (224-239) IP addresses and is forwarded as destination IP address in the packet.

Working of IGMP

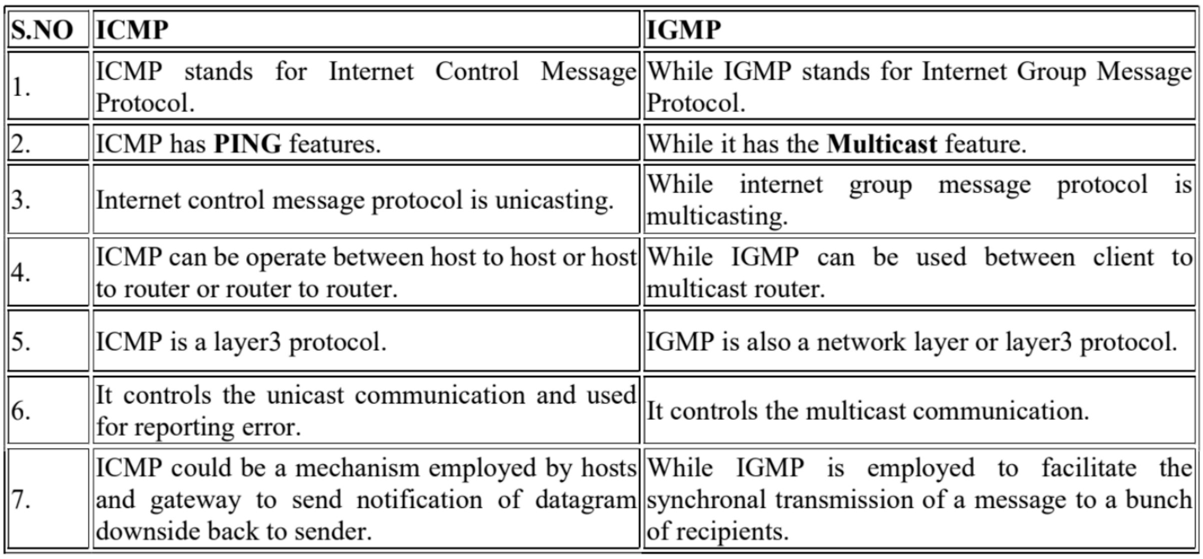


Advantages:

- IGMP communication protocol efficiently transmits the multicast data to the receivers and so, no junk packets are transmitted to the host which shows optimised performance.
- Bandwidth is consumed totally as all the shared links are connected.
- Hosts can leave a multicast group and join another.

Disadvantages:

- It does not provide good efficiency in filtering and security.
- Due to lack of TCP, network congestion can occur.
- IGMP is vulnerable to some attacks such as DOS attack (Denial-Of-Service).



S.NO	ICMP	IGMP
1.	ICMP stands for Internet Control Message Protocol.	While IGMP stands for Internet Group Message Protocol.
2.	ICMP has **PING** features.	While it has the **Multicast** feature.
3.	Internet control message protocol is unicasting.	While internet group message protocol is multicasting.
4.	ICMP can be operate between host to host or host to router or router to router.	While IGMP can be used between client to multicast router.
5.	ICMP is a layer3 protocol.	IGMP is also a network layer or layer3 protocol.
6.	It controls the unicast communication and used for reporting error.	It controls the multicast communication.
7.	ICMP could be a mechanism employed by hosts and gateway to send notification of datagram downside back to sender.	While IGMP is employed to facilitate the synchronal transmission of a message to a bunch of recipients.

# IPv6

Internet Protocol version 6 (IPV 6) is the replacement for version 4 (IPV 4). The phenomenal development of the Internet has begun to push IP to its limits. It provides a large address space, and it contains a simple header as compared to IPv4.

Features of IPV6

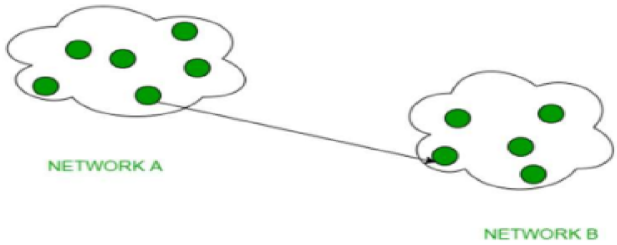
- Larger address space: An IPV6 address is 128 bits long. It is compared with the 32-bit address of IPV4. It will allow for unique IP-addresses up to 3.4 x 10^{38} whereas IPV4 allows up to 4.3 x 10^{8} unique addresses.
- Better Header format: New header form has been designed to reduce overhead. It is done by moving both non-essential fields and optional fields to extension field header that are placed after the IPV6 header.
- More Functionality: It is designed with more options like priority of packet for control of congestion, Authentication etc.
- Allowance for Extension: It is designed to allow the extension of the protocol if required by new technologies.
- Support of resource allocation: In IPV6, the type of service fields has been removed, but a new mechanism has been added to support traffic control or flow labels like real-time audio and video.

Types of IPv6 Address

Unicast, Broadcast and Multicast Routing Protocols. The cast term here signifies some data (stream of packets) is being transmitted to the recipient(s) from client(s) side over the communication channel that help them to communicate.

1. Unicast :

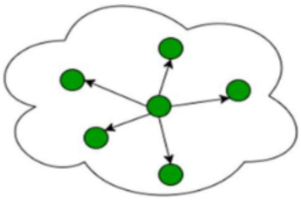
This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network,then unicast comes into picture. This is the most common form of data transfer over the networks.



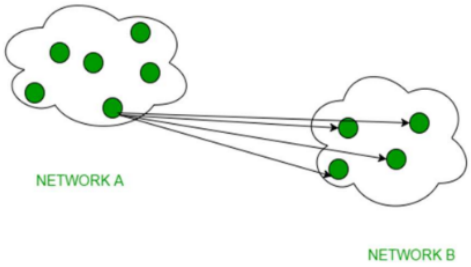
2. Broadcast :

Broadcasting transfer (one-to-all) techniques can be classified into two types :

i) Limited Broadcasting :Suppose you have to send stream of packets to all the devices over the network that you reside, this broadcasting comes handy. For this to achieve,it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as Limited Broadcast Address in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.



ii) Direct Broadcasting : This is useful when a device in one network wants to transfer packet stream to all the devices over the other network.This is achieved by translating all the Host ID part bits of the destination address to 1,referred as Direct Broadcast Address in the datagram header for information transfer.



This mode is mainly utilised by television networks for video and audio distribution. One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) that is used for resolving IP address into physical address which is necessary for underlying communication.

3. Multicast :

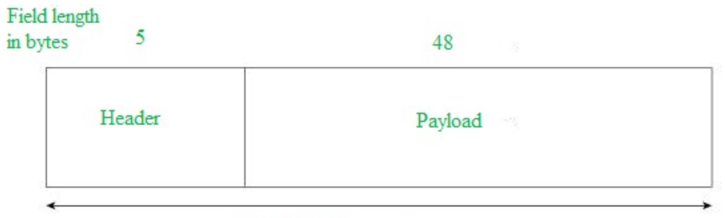
In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server’s direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also in Classful IP addressing Class D is reserved for multicast groups.

# ATM

Asynchronous Transfer Mode (ATM) is an International Telecommunication Union-Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

ATM Cell Format :

As information is transmitted in the ATM in the form of fixed-size units called cells. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



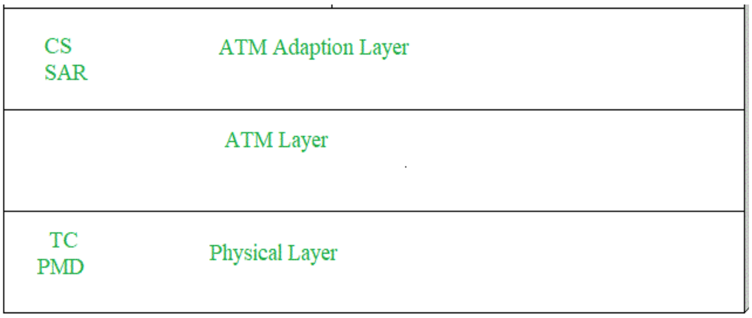
ATM Cell Format

Working of ATM:

ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not route the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

ATM Layers:



CS SAR	ATM Adaption Layer
	ATM Layer
TC PMD	Physical Layer

1. ATM Adaptation Layer (AAL) –

It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol accepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

2. Physical Layer –

It manages the medium-dependent transmission and is divided into two parts: physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:

- It converts cells into a bitstream.
- It controls the transmission and receipt of bits in the physical medium.
- It can track the ATM cell boundaries.
- Look for the packaging of cells into the appropriate type of frames.

3. ATM Layer –

It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.