UNIT-3

NETWORK LAYER

Switching concepts – Circuit switching – Packet switching –IPV4, IPV6 ––IP address

Hierarchy – ICMP – Routing Protocols – Distance Vector – Link State.

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. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **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.

Forwarding & Routing

In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field

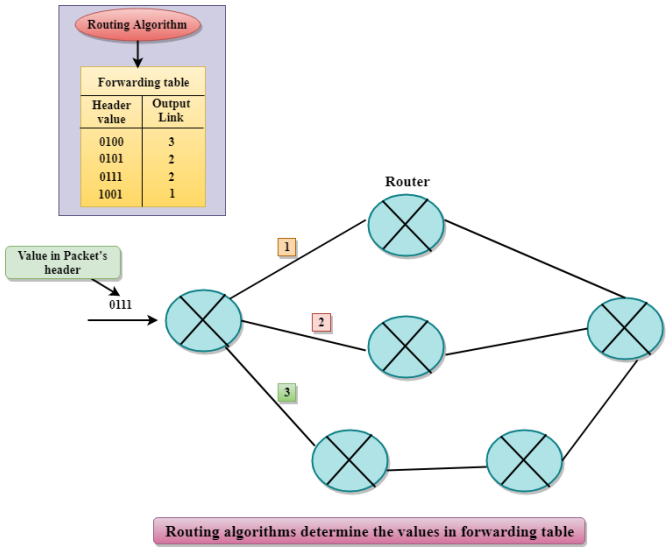
and then using the header field value to index into the forwarding table.

The value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

For example, the router with a header field value of 0111 arrives at a router, and then router indexes this header value into the forwarding table that determines the output link interface is

1.The router forwards the packet to the interface

2. The routing algorithm determines the values that are inserted in the forwarding table. The routing algorithm can be centralized or decentralized.



Services Provided by the Network Layer

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host.

The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Why is Switching Concept required?

Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

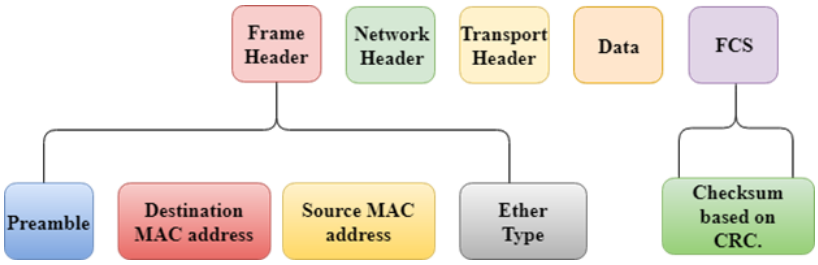
- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

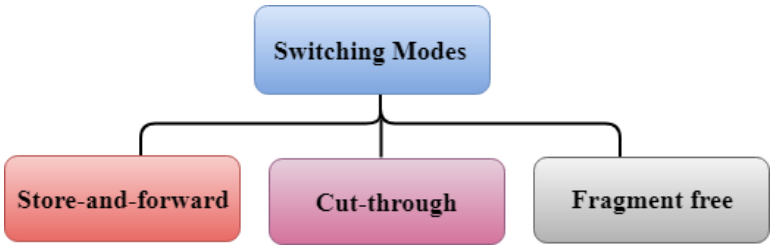
Switching Modes

- The layer 2 switches are used for transmitting the data on the data link layer, and it also performs error checking on transmitted and received frames.
- The layer 2 switches forward the packets with the help of MAC address.
- Different modes are used for forwarding the packets known as **Switching modes**.
- In **switching mode**, Different parts of a frame are recognized. The frame consists of several parts such as preamble, destination MAC address, source MAC address, user's data, FCS.

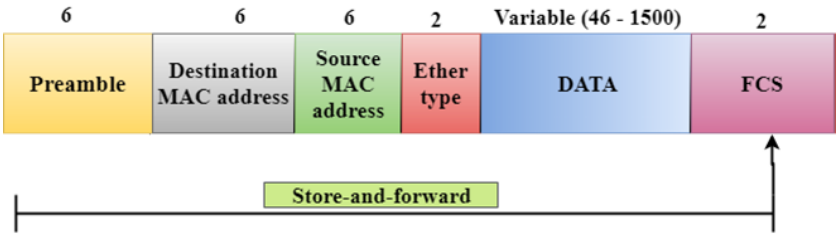


There are three types of switching modes:

- Store-and-forward
- Cut-through
- Fragment-free

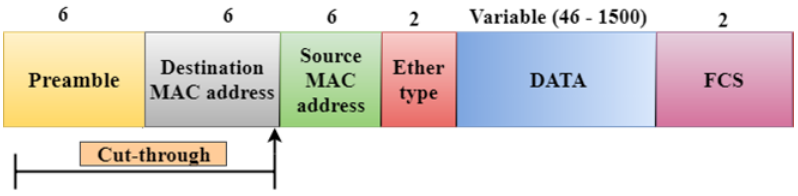


Store-and-forward



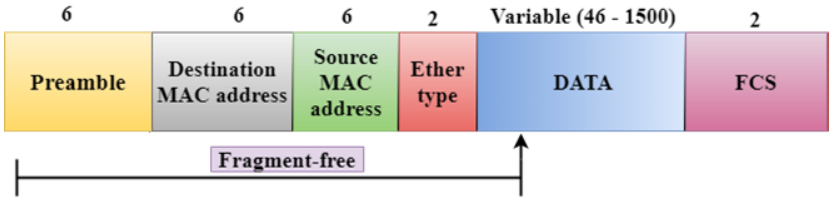
- Store-and-forward is a technique in which the intermediate nodes store the received frame and then check for errors before forwarding the packets to the next node.
- The layer 2 switch waits until the entire frame has received. On receiving the entire frame, switch store the frame into the switch buffer memory. This process is known as **storing the frame**.
- When the frame is stored, then the frame is checked for the errors. If any error found, the message is discarded otherwise the message is forwarded to the next node. This process is known as **forwarding the frame**.
- CRC (Cyclic Redundancy Check) technique is implemented that uses a number of bits to check for the errors on the received frame.
- The store-and-forward technique ensures a high level of security as the destination network will not be affected by the corrupted frames.
- Store-and-forward switches are highly reliable as it does not forward the collided frames.

Cut-through Switching



- Cut-through switching is a technique in which the switch forwards the packets after the destination address has been identified without waiting for the entire frame to be received.
- Once the frame is received, it checks the first six bytes of the frame following the preamble, the switch checks the destination in the switching table to determine the outgoing interface port, and forwards the frame to the destination.
- It has **low latency** rate as the switch does not wait for the entire frame to be received before sending the packets to the destination.
- It has no **error checking technique**. Therefore, the errors can be sent with or without errors to the receiver.
- A Cut-through switching technique has **low wait time** as it forwards the packets as soon as it identifies the destination MAC address.
- In this technique, collision is not detected, if frames have collided will also be forwarded.

Fragment-free Switching



- A Fragment-free switching is an advanced technique of the Cut-through Switching.
- A Fragment-free switching is a technique that reads atleast 64 bytes of a frame before forwarding to the next node to provide the error-free transmission.
- It combines the speed of Cut-through Switching with the error checking functionality.
- This technique checks the 64 bytes of the ethernet frame where addressing information is available.
- A collision is detected within 64 bytes of the frame, the frames which are collided will not be forwarded further.

Differences b/w Store-and-forward and Cut-through Switching.

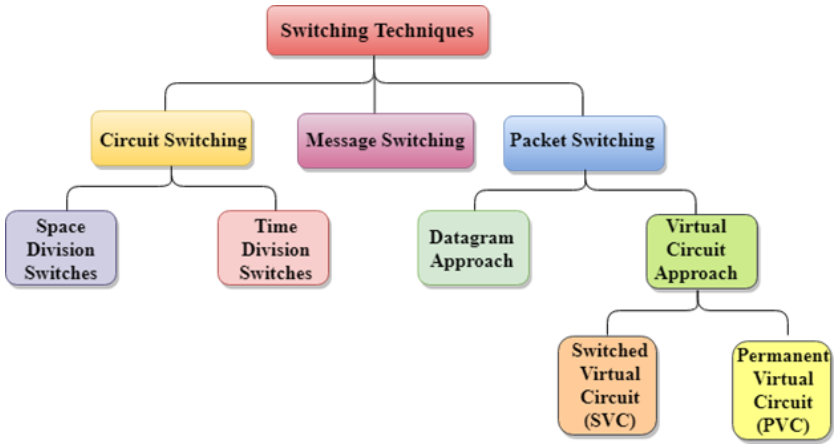
Store-and-forward Switching	Cut-through Switching
Store-and-forward Switching is a technique that waits until the entire frame is received.	Cut-through Switching is a technique that checks the first 6 bytes following the preamble to identify the destination address.
It performs error checking functionality. If any error is found in the frame, the frame will be discarded otherwise forwarded to the next node.	It does not perform any error checking. The frame with or without errors will be forwarded.
It has high latency rate as it waits for the entire frame to be received before forwarding to the next node.	It has low latency rate as it checks only six bytes of the frame to determine the destination address.
It is highly reliable as it forwards only error-free packets.	It is less reliable as compared to Store-and-forward technique as it forwards error prone packets as well.
It has a high wait time as it waits for the entire frame to be received before taking any forwarding decisions.	It has low wait time as cut-through switches do not store the whole frame or packets.

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques



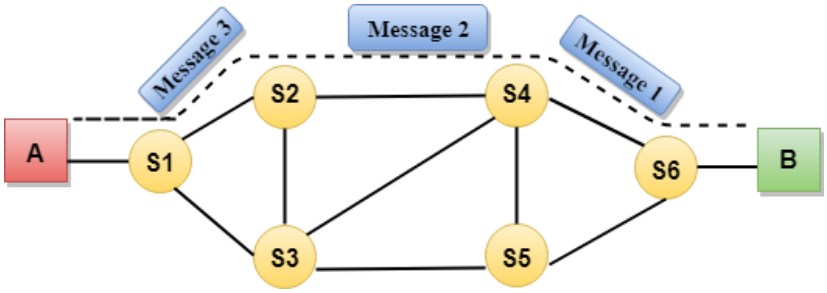
Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

Where to interact with an IO Operative's Computer in Fortnite Chapter 2 Season 7

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be

enabled or disabled by a control unit.

- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**
- **Multistage Switch**

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages Of Circuit Switching:

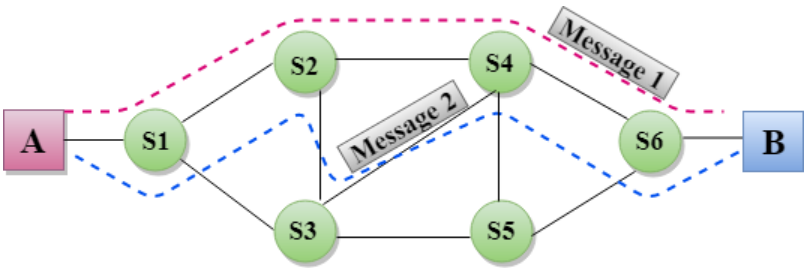
- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which

no data can be transmitted.

- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.

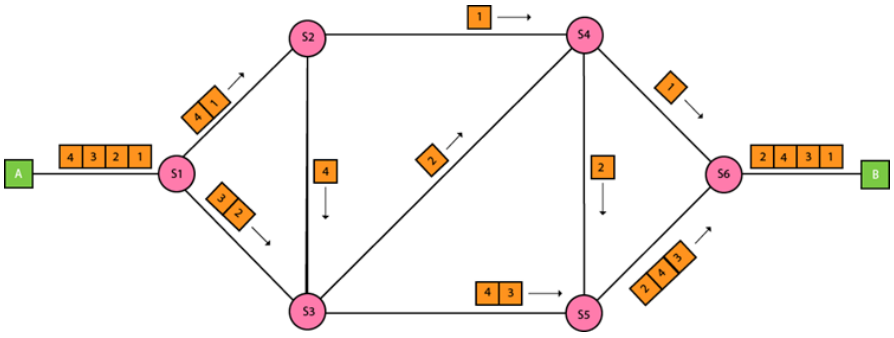
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

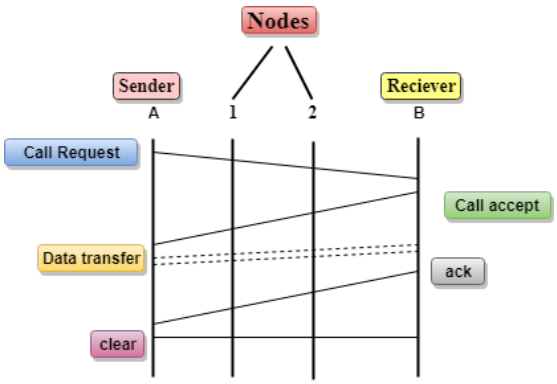
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

IPv4 vs IPv6

What is IP?

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network.

It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP . It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely.

To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

There are two types of IP addresses:

- **IPv4**
- **IPv6**

What is IPv4?

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, 66.94.29.13

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Representation of 8 Bit Octet

128	64	32	16	8	4	2	1

The above representation shows the structure of 8- bit octet.

Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

Step 1: First, we find the binary number of 66.

128	64	32	16	8	4	2	1
0	1	0	0	0	0	1	0

To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

Step 2: Now, we calculate the binary number of 94.

128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

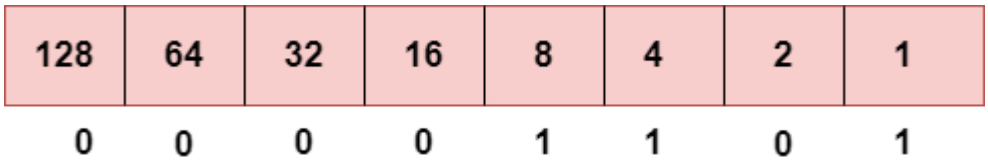
To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

Step 3: The next number is 29.

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13.



To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet.

As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet.

Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet.

But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

What is IPv6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses.

The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address.

IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

- **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.

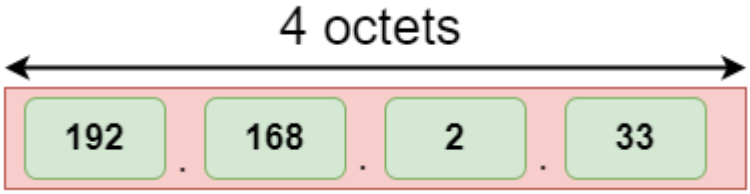
- **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion ($3.4*10^{38}$) addresses.

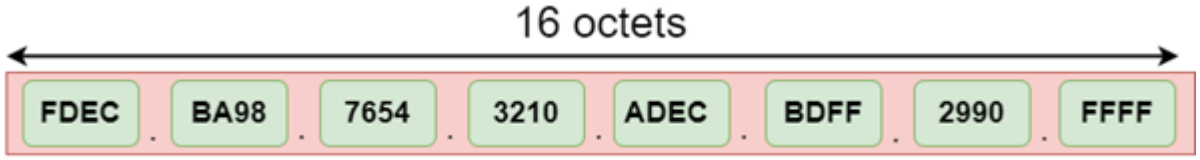
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

The address format of IPv4:



The address format of IPv6:



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Internet Protocol Version 4 (IPv4)

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model.

Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

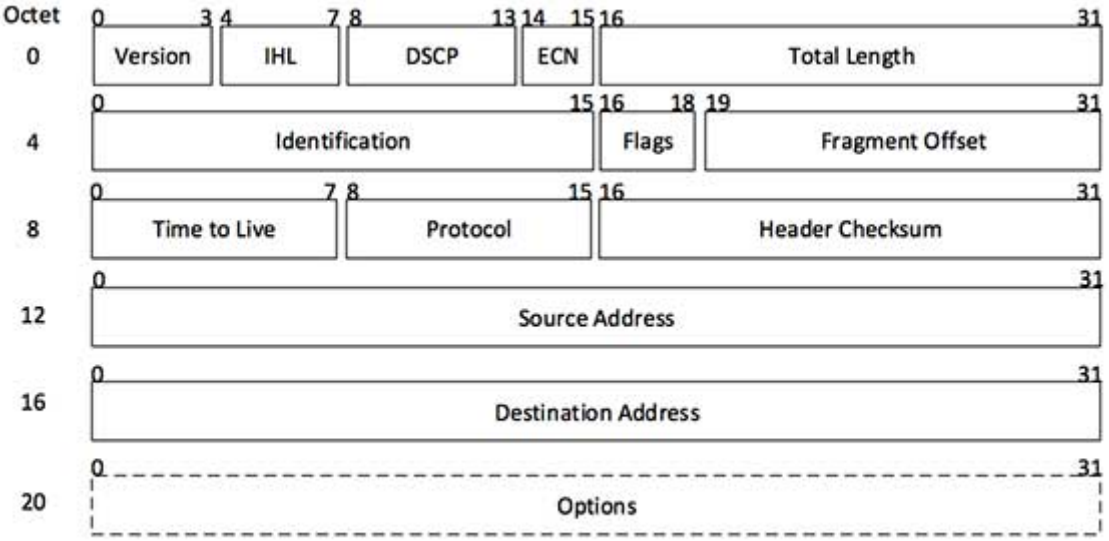
IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.

IPv4 - Packet Structure

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

(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

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’.

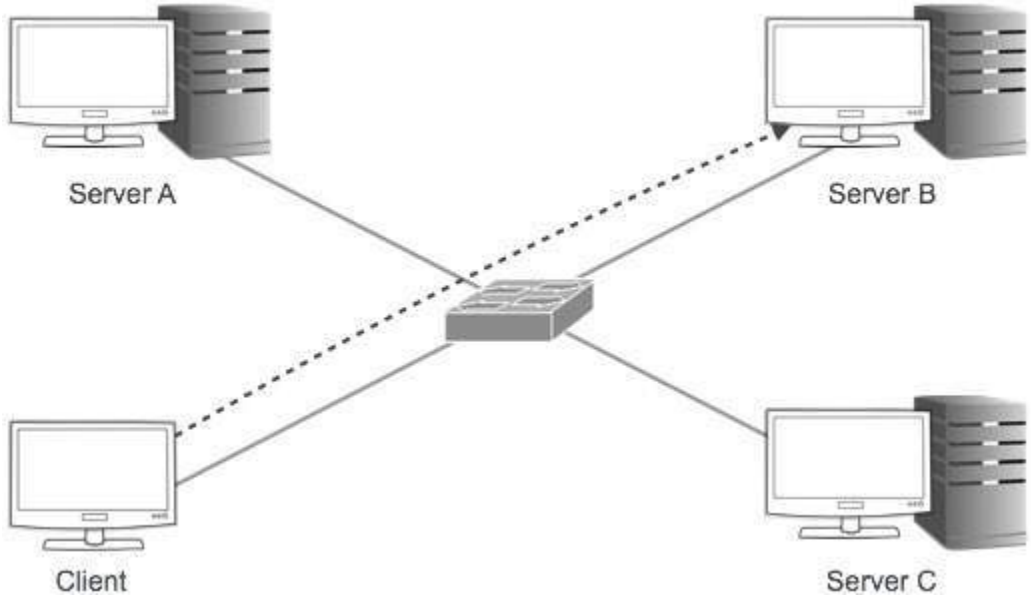
- **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is 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.

IPv4 - Addressing

IPv4 supports three different types of addressing modes. −

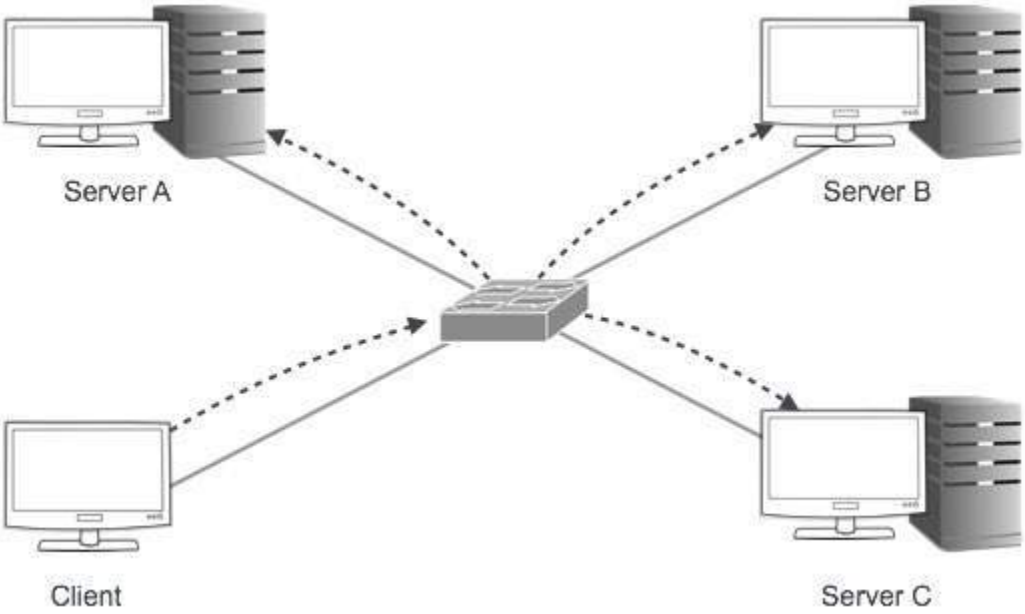
Unicast Addressing Mode

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server −



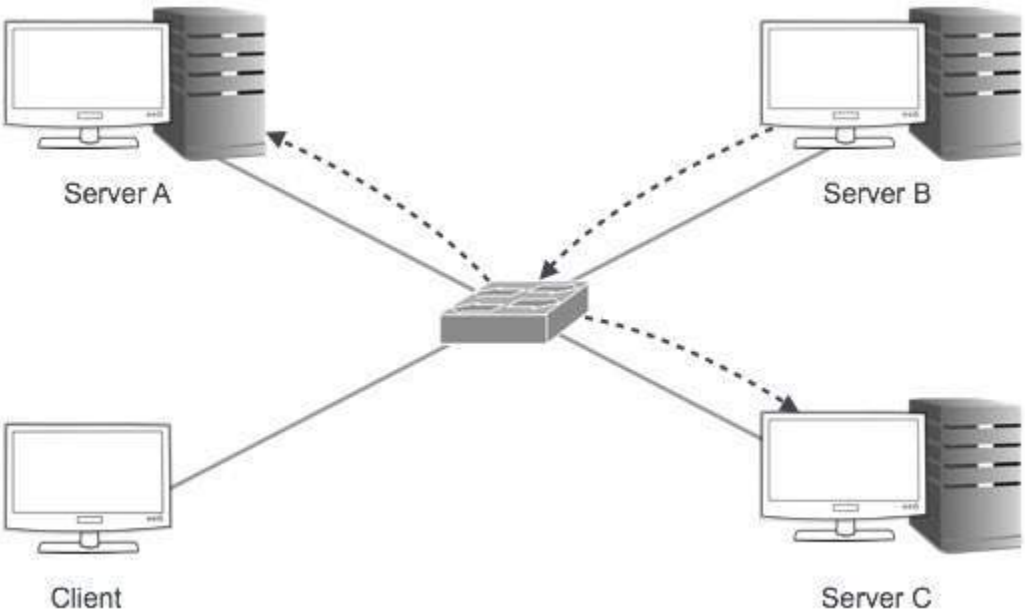
Broadcast Addressing Mode

In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers –



Multicast Addressing Mode

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents

all the hosts in that network.

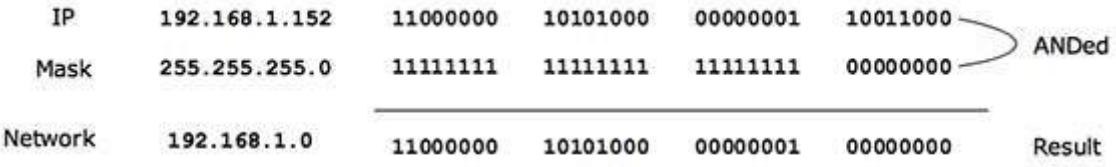
Hierarchical Addressing Scheme

IPv4 uses hierarchical addressing scheme. An IP address, which is 32-bits in length, is divided into two or three parts as depicted −

A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables the IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

Subnet Mask

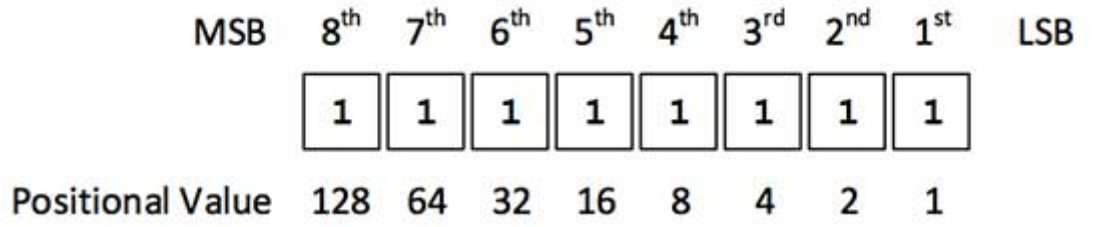
The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then −



This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

Binary Representation

The positional value method is the simplest form of converting binary from decimal value. IP address is 32 bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of each bit can be determined by the position of bit value '1' in the octet.



Positional value of bits is determined by 2 raised to power (position – 1), that is the value of a bit 1 at position 6 is 2^(6-1) that is 2^5 that is 32. The total value of the

octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below –

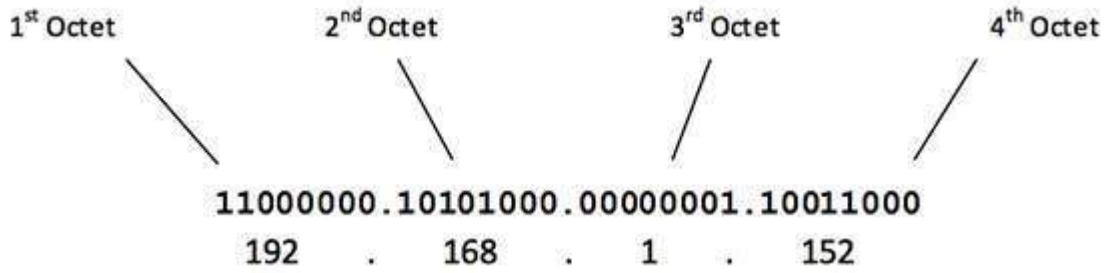
128	64	32	16	8	4	2	1	Value
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
0	0	0	0	0	1	1	1	7
0	0	0	0	1	0	0	0	8
0	0	0	0	1	0	0	1	9
0	0	0	0	1	0	1	0	10
0	0	0	1	0	0	0	0	16
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	1	0	0	100
0	1	1	1	1	1	1	1	127
1	0	0	0	0	0	0	0	128
1	0	1	0	1	0	0	0	168
1	1	0	0	0	0	0	0	192
1	1	1	1	1	1	1	1	255

IPv4 - Address Classes

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address –



The number of networks and the number of hosts per class can be derived by this formula –

Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits – 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

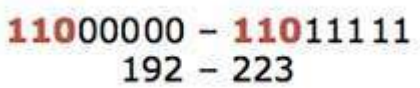
Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format

is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is −



Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of −

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

IPv4 - Subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet

mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^1=2) with (2^{23} -2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits

providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

IPv4 - VLSM

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs.

For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum

wastage of IP addresses.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size.

Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step - 1

Make a list of Subnets possible.

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step - 2

Sort the requirements of IPs in descending order (Highest to Lowest).

- Sales 100
- Purchase 50
- Accounts 25
- Management 5

Step - 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step - 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step - 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step - 6

Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used CIDR.

IPv4 - Reserved Addresses

There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.

Private IP Addresses

Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.

Class A IP Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

In order to communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.

The sole purpose to create a separate range of private addresses is to control

assignment of already-limited IPv4 address pool. By using a private address range within LAN, the requirement of IPv4 addresses has globally decreased significantly. It has also helped delaying the IPv4 address exhaustion.

IP class, while using private address range, can be chosen as per the size and requirement of the organization. Larger organizations may choose class A private IP address range where smaller organizations may opt for class C. These IP addresses can be further sub-netted and assigned to departments within an organization.

Loopback IP Addresses

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address. This loopback IP address is managed entirely by and within the operating system.

Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine.

Other than that, if a host machine can successfully ping 127.0.0.1 or any IP from loopback range, implies that the TCP/IP software stack on the machine is successfully loaded and working.

Link-local Addresses

In case a host is not able to acquire an IP address from the DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses. Link local address ranges from 169.254.0.0 -- 169.254.255.255.

Assume a network segment where all systems are configured to acquire IP addresses from a DHCP server connected to the same network segment. If the DHCP server is not available, no host on the segment will be able to communicate to any other.

Windows (98 or later), and Mac OS (8.0 or later) supports this functionality of self-configuration of Link-local IP address. In absence of DHCP server, every host machine randomly chooses an IP address from the above mentioned range and then checks to ascertain by means of ARP, if some other host also has not configured itself with the same IP address.

Once all hosts are using link local addresses of same range, they can communicate with each other.

These IP addresses cannot help system to communicate when they do not belong to the same physical or logical segment. These IPs are also not routable.

IPv4 - Example

Packet Flow in Network

All the hosts in IPv4 environment are assigned unique logical IP addresses. When a host wants to send some data to another host on the network, it needs the physical (MAC) address of the destination host.

To get the MAC address, the host an broadcasts ARP message and asks to give the MAC address whoever is the owner of destination IP address. All the hosts on that segment receive the ARP packet, but only the host having its IP matching with the one in the ARP message, replies with its MAC address.

Once the sender receives the MAC address of the receiving station, data is sent on the physical media.

In case the IP does not belong to the local subnet, the data is sent to the destination by means of Gateway of the subnet. To understand the packet flow, we must first understand the following components −

- **MAC Address** − Media Access Control Address is 48-bit factory hard coded physical address of network device which can uniquely be identified. This address is assigned by device manufacturers.
- **Address Resolution Protocol** − Address Resolution Protocol is used to acquire the MAC address of a host whose IP address is known. ARP is a Broadcast packet which is received by all the host in the network segment. But only the host whose IP is mentioned in ARP responds to it providing its MAC address.
- **Proxy Server** − To access the Internet, networks use a Proxy Server which has a public IP assigned. All the PCs request the Proxy Server for a Server on the Internet. The Proxy Server on behalf of the PCS sends the request to the server and when it receives a response from the Server, the Proxy Server forwards it to the client PC. This is a way to control Internet access in computer networks and it helps to implement web based policies.
- **Dynamic Host Control Protocol** − DHCP is a service by which a host is assigned IP address from a pre-defined address pool. DHCP server also provides necessary information such as Gateway IP, DNS Server Address, lease assigned with the IP, etc. By using DHCP services, a network administrator can manage assignment of IP addresses at ease.
- **Domain Name System** − It is very likely that a user does not know the IP address of a remote Server he wants to connect to. But he knows the name assigned to it, for example, tutorialpoints.com. When the user types the name of a remote server he wants to connect to, the localhost behind the screens sends a DNS query. Domain Name System is a method to acquire the IP address of the host whose Domain Name is known.
- **Network Address Translation** − Almost all PCs in a computer network are assigned private IP addresses which are not routable on the Internet. As soon as a router receives an IP packet with a private IP address, it drops it. In order to access servers on public private address, computer networks use an address translation service, which translates between public and private addresses, called Network Address Translation. When a PC sends an IP

packet out of a private network, NAT changes the private IP address with public IP address and vice versa.

We can now describe the packet flow. Assume that a user wants to access www.TutorialsPoint.com from her personal computer. She has internet connection from her ISP. The following steps will be taken by the system to help her reach the destination website.

Step 1 – Acquiring an IP Address (DHCP)

When the user's PC boots up, it searches for a DHCP server to acquire an IP address. For the same, the PC sends a DHCPDISCOVER broadcast which is received by one or more DHCP servers on the subnet and they all respond with DHCPOFFER which includes all the necessary details such as IP, subnet, Gateway, DNS, etc. The PC sends DHCPREQUEST packet in order to request the offered IP address.

Finally, the DHCP sends DHCPACK packet to tell the PC that it can keep the IP for some given amount of time that is known as IP lease.

Alternatively, a PC can be assigned an IP address manually without taking any help from DHCP server. When a PC is well configured with IP address details, it can communicate other computers all over the IP enabled network.

Step 2 – DNS Query

When a user opens a web browser and types www.tutorialpoints.com which is a domain name and a PC does not understand how to communicate with the server using domain names, then the PC sends a DNS query out on the network in order to obtain the IP address pertaining to the domain name. The pre-configured DNS server responds to the query with IP address of the domain name specified.

Step 3 – ARP Request

The PC finds that the destination IP address does not belong to his own IP address range and it has to forward the request to the Gateway. The Gateway in this scenario can be a router or a Proxy Server.

Though the Gateway's IP address is known to the client machine but computers do not exchange data on IP addresses, rather they need the machine's hardware address which is Layer-2 factory coded MAC address.

To obtain the MAC address of the Gateway, the client PC broadcasts an ARP request saying "Who owns this IP address?" The Gateway in response to the ARP query sends its MAC address. Upon receiving the MAC address, the PC sends the packets to the Gateway.

An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data. It is important that source and destination MAC addresses change as they travel across the Internet (segment by segment) but source and destination IP addresses never change.

Internet Protocol v6 (IPv6)

IETF (Internet Engineering Task Force) has redesigned IP addresses to mitigate the drawbacks of IPv4. The new IP address is version 6 which is 128-bit address, by which every single inch of the earth can be given millions of IP addresses.

Today majority of devices running on Internet are using IPv4 and it is not possible to shift them to IPv6 in the coming days. There are mechanisms provided by IPv6, by which IPv4 and IPv6 can co-exist unless the Internet entirely shifts to IPv6 −

- Dual IP Stack
- Tunneling (6to4 and 4to6)
- NAT Protocol Translation

IPv6

- The IPv4 provides host to host communication systems, which are connected through the Internet.
- The **IPv6 (Internetworking Protocol, version 6)** is designed to overcome the shortfalls of the IPv4.

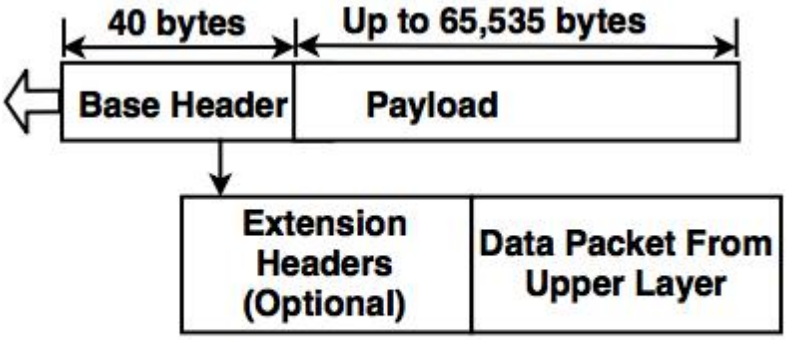
Advantages of IPv6

Some advantages of IPv6 over IPv4 are mentioned below:

1. Address Space : IPv6 has a 128 bit long address, which is larger than IPv4.
2. Header format : IPv6 has a new header format, in which options are separated from the base header and inserted between the base header and the upper layer data.
3. Extension : IPv6 is designed to allow the extension of the protocol, if required for new applications.
4. Security : Encryption and authentication mechanism provides confidentiality and integrity to the packets in IPv6.

Packet Format of IPv6

The IPv6 packet is shown in the diagram. Each packet is composed of base header and the payload. The payload consists of two fields, optional extension headers and the data from upper layer.



IPv6 Datagram Header and Payload

The Base header consists of eight fields:

1. Version : This is 4 bit field, which defines the version number of an IP and its value is 6 for IPv6.
2. Priority : This is 4 bit field, which defines the priority of the packet with respect to the traffic congestion.
3. Flow label : This is 24 bit field, which is designed to provide facility of specially handling the specific flow of the data.
4. Payload length : This is 16 bit field, which defines the length of an IP datagram excluding the base header.
5. Next header : This is 8 bit field, which defines the header that follows the base header in the datagram.
6. Hop limit : This is 8 bit field, which serves the same purpose as the TTL(Time to Live field in IPv4) field. It is a mechanism that limits the life span of the data in computer networks.
7. Source address : This is 128 bit source address field, which identifies the original source of the datagram.
8. Destination address : It is 128 bit destination address field, which identifies the original destination of the datagram.

Priority field of IPv6

Defines the priority of each packet with respect to other packets from the same source.

The IPv6 divides the traffic into two categories:

- **Congestion-Controlled Traffic :** If source can adjust itself with traffic slowdown due to congestion, the traffic is referred to as congestion controlled traffic.
- **Non Congestion-Controlled Traffic :** Non-Congestion - Controlled Traffic is a type of traffic which can accept a minimum delay.

Extension Headers

The length of the base header is 40 bytes and to provide greater functionality to the IP datagram.

It can be extended upto six extension headers.

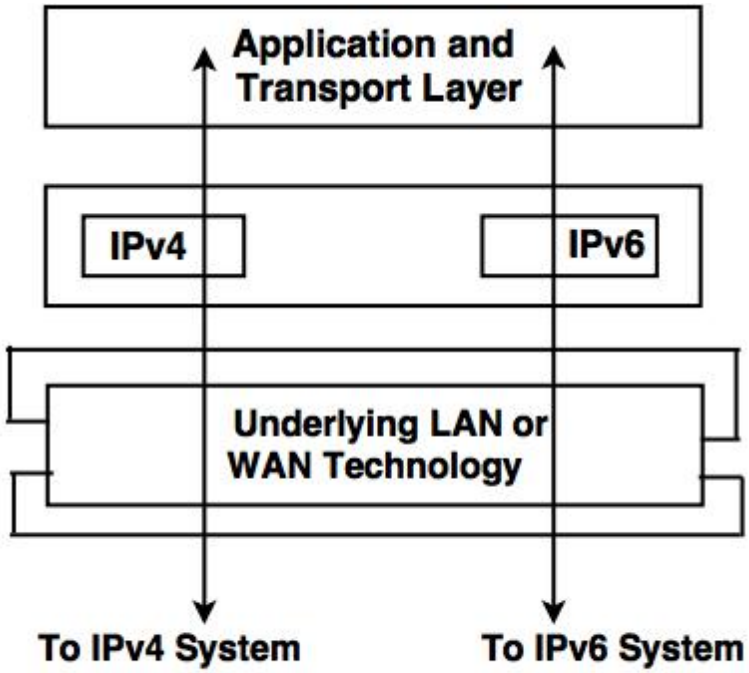
1. Hop by hop option : It is used when the source needs to pass the information to all routers visited by the datagram.
2. Source routing : It combines the concepts of the strict source route and the loose source route options of IPv4.
3. Fragmentation : The data travels through the different networks, each router first decapsulates the IPv6 datagram from the received frame, then processes it and again encapsulates in another frame.
4. Authentication : Authentication validates the message sender and ensures the integrity of the data.
5. Encrypted Security Payload (ESP) : It is an extension that provides confidentiality and protects against eavesdropping .
6. Destination option : It is used when the source needs to forward information to the destination only and not to intermediate routers.

Transition from IPv4 to IPv6

Three strategies have been invented by the IETF (Internet Engineering Task Force) to help the transition:

1. Dual stack

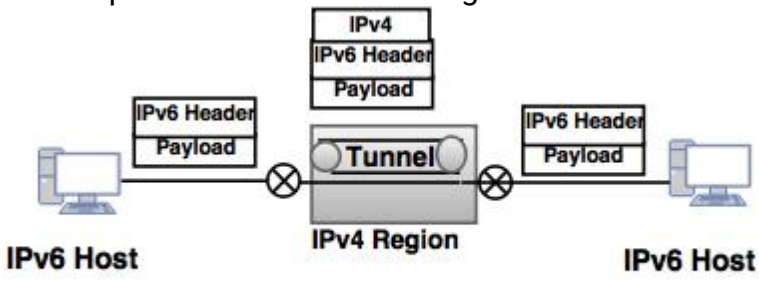
- The host should run IPv4 and IPv6 simultaneously until the entire internet uses IPv6.
- The source host queries the DNS, to determine which version can be used at the time of sending a packet to the destination.
- If the DNS returns an IPv6 address, the source host sends an IPv6 packet.



Dual Stack

2. Tunneling

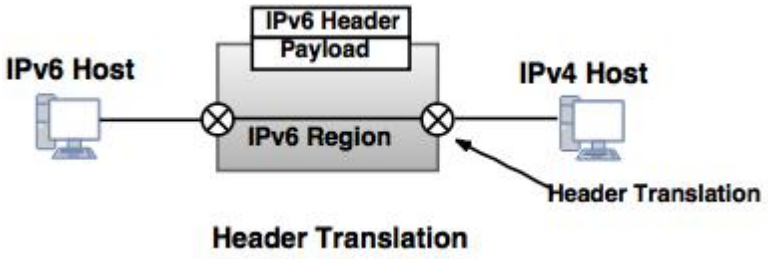
- When two computers use IPv6 and want to communicate with each other and the packet passes through a region that uses IPv4, it is called tunneling.
- The IPv6 packet is encapsulated in an IPv4 packet, when it enters the region. It leaves the capsule when it exits the region.



Tunneling

3. Header Translation

- It is used when some of the systems use the IPv4 and the sender wants to use IPv6, but the receiver does not understand IPv6.
- The header format should be totally changed through header translation.
- The header of the IPv6 packet is converted to an IPv4 header.



Header translation procedure

1. Change the IPv6 mapped address to an IPv4 address by extracting the rightmost 32 bits.
2. Discard the value of IPv6 priority field.
3. Set the type of service field in IPv4 to be zero.
4. Calculate the checksum for IPv4 and insert in the corresponding field.
5. Ignore the Ipv6 flow label.
6. Convert the compatible extension headers to options and insert them in the IPv4 header.
7. Calculate the length of IPV4 header and insert it into the corresponding field.
8. Eventually, compute the total length of the IPv4 packet and insert it into the corresponding field.

Differences between IPv4 and IPv6

	IPV4	IPV6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and

		renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

An IP address is the identifier that enables your device to send or receive data packets across the internet. It holds information related to your location and therefore making devices available for two-way communication.

The internet requires a process to distinguish between different networks, routers, and websites. Therefore, IP addresses provide the mechanism of doing so,

and it forms an indispensable part in the working of the internet. You will notice that most of the IP addresses are essentially numerical. Still, as the world is witnessing a colossal growth of network users, the network developers had to add letters and some addresses as internet usage grows.

An IP address is represented by a series of numbers segregated by periods(.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255.

IP addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN.

ICANN stands for Internet Corporation for Assigned Names and Numbers. It is a non-profit corporation founded in the US back in 1998 with an aim to manage Internet security and enable it to be available by all.

How do IP addresses work?

Sometimes your device doesn't connect to your network the way you expect it to be, or you wish to troubleshoot why your network is not operating correctly. To answer the above questions, it is vital to learn the process with which IP addresses work.

Internet Protocol or IP runs the same manner as other languages, i.e., applying the set guidelines to communicate the information. All devices obtain, send, and pass information with other associated devices with the help of this protocol only. By using the same language, the computers placed anywhere can communicate with one another.

The process of IP address works in the following way:

1. Your computer, smartphone, or any other Wi-Fi-enabled device firstly connects to a network that is further connected to the internet. The network is responsible for giving your device access to the internet.
2. While working from home, your device would be probably using that network provided by your Internet Service Provider (ISP). In a professional environment, your device uses your company network.
3. Your ISP is responsible to generate the IP address for your device.
4. Your internet request penetrates through the ISP, and they place the requested data back to your device using your IP address. Since they provide you access to the internet, ISP's are responsible for allocating an IP address to your computer or respective device.
5. Your IP address is never consistent and can change if there occurs any

changes in its internal environment. For instance, if you turn your modem or router on or off, it will change your IP address. Or the user can also connect the ISP to change their IP address.

6. When you are out of your home or office, mainly if you travel and carry your device with you, your computer won't be accessing your home IP address anymore. This is because you will be accessing the different networks (your phone hotspot, Wi-Fi at a cafe, resort, or airport, etc.) to connect the device with the internet. Therefore, your device will be allocated a different (temporary) IP address by the ISP of the hotel or cafe.

Types of IP addresses

There are various classifications of IP addresses, and each category further contains some types.

Consumer IP addresses

Every individual or firm with an active internet service system pursues two types of IP addresses, i.e., Private IP (Internet Protocol) addresses and public IP (Internet Protocol) addresses.

The public and private correlate to the network area. Therefore, a private IP address is practiced inside a network, whereas the other (public IP address) is practiced outside a network.

1. Private IP addresses

All the devices that are linked with your internet network are allocated a private IP address. It holds computers, desktops, laptops, smartphones, tablets, or even Wi-Fi-enabled gadgets such as speakers, printers, or smart Televisions. With the expansion of IoT (internet of things), the demand for private IP addresses at individual homes is also seemingly growing.

However, the router requires a method to identify these things distinctly. Therefore, your router produces unique private IP addresses that act as an identifier for every device using your internet network. Thus, differentiating them from one another on the network.

2. Public IP addresses

A public IP address or primary address represents the whole network of devices associated with it. Every device included within with your primary address contains their own private IP address.

ISP is responsible to provide your public IP address to your router. Typically, ISPs contains the bulk stock of IP addresses that they dispense to their clients. Your

public IP address is practiced by every device to identify your network that is residing outside your internet network.

Public IP addresses are further classified into two categories- dynamic and static.

- **Dynamic IP addresses**

  As the name suggests, Dynamic IP addresses change automatically and frequently. With this types of IP address, ISPs already purchase a bulk stock of IP addresses and allocate them in some order to their customers. Periodically, they re-allocate the IP addresses and place the used ones back into the IP addresses pool so they can be used later for another client. The foundation for this method is to make cost savings profits for the ISP.

- **Static IP addresses**

  In comparison to dynamic IP addresses, static addresses are constant in nature. The network assigns the IP address to the device only once and, it remains consistent. Though most firms or individuals do not prefer to have a static IP address, it is essential to have a static IP address for an organization that wants to host its network server. It protects websites and email addresses linked with it with a constant IP address.

Types of website IP addresses

The following classification is segregated into the two types of website IP addresses i.e., shared and dedicated.

1. Shared IP addresses

Many startups or individual website makers or various SME websites who don't want to invest initially in dedicated IP addresses can opt for shared hosting plans.

Various web hosting providers are there in the market providing shared hosting services where two or more websites are hosted on the same server.

Shared hosting is only feasible for websites that receive average traffic, the volumes are manageable, and the websites themselves are confined in terms of the webpages, etc.

2. Dedicated IP addresses

Web hosting providers also provide the option to acquire a dedicated IP address. Undoubtedly dedicated IP addresses are more secure, and they permit the

users to run their File Transfer Protocol (FTP) server.

Therefore, it is easier to share and transfer data with many people within a business, and it also provides the option of anonymous FTP sharing. Another advantage of a dedicated IP addresses it the user can easily access the website using the IP address rather than typing the full domain name.

How to search for IP addresses

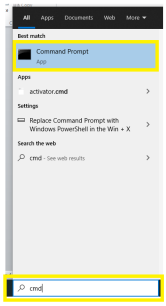
The easiest method to find the public IP address of your router is to type "What is my IP address?" on Google.com. Google will immediately display the results on the screen.

There are some third-party websites available on the internet that also provides the same information. Those websites can access your public IP address because your router has requested to access their information by visiting their website.

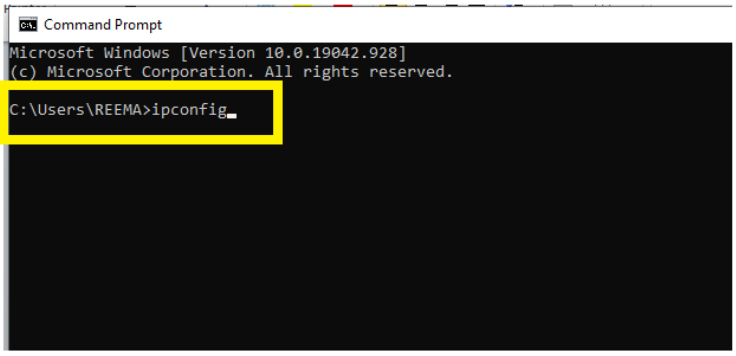
Below are the steps to find your private IP address in two commonly used platforms:

In Windows:

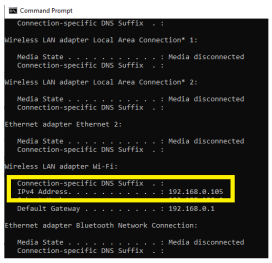
1. Open the command prompt by typing the term 'cmd' (no quote marks) in the Windows search panel.



2. The following window will appear. Type "ipconfig" (without the quotes) to access the private IP address information.



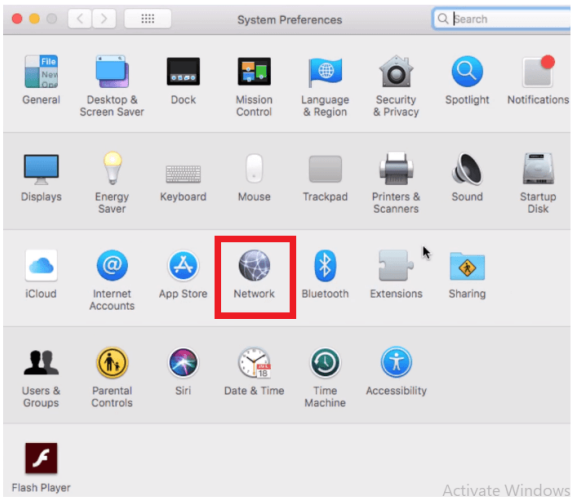
3. It will display the following information.



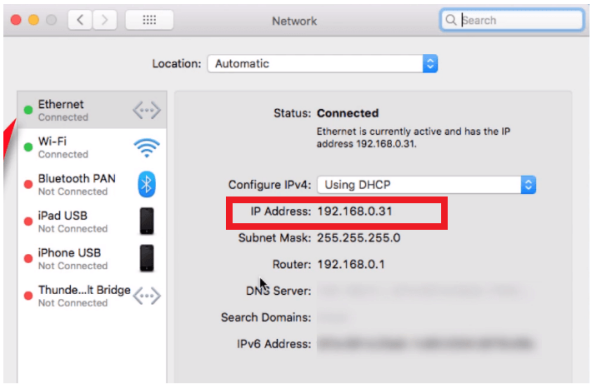
On a Mac:

1. Go to System Preferences

2.Click on the network option.



3.It will display the information regarding your private IP address.



IP address security threats

Cybercriminals or digital crackers various ways to hack your IP address. The two commonly used techniques include social engineering and online stalking.

Social engineering

Hackers can practice social engineering techniques to trick you into disclosing your device's IP address. For example, they will connect you through email, Skype, or a similar instantaneous messaging app, that accepts IP addresses to communicate and pass information.

If you chat with these anonymous people using these messaging applications, it is essential to note that they can get your IP address. Cybercriminals can use a third-party tool named Skype Resolver, with the help of which they can locate your IP address using your username.

Online stalking

Attackers can get crack your IP address by simply tracking your online activities. Any online activity can disclose your IP address, i.e., from using an instant messaging app to playing online games to discussing a topic on any digital websites and forums. Once they gain access to your IP address, criminals can visit an IP address tracking website (whatismyipaddress.com), they will enter your IP address there, and in no seconds, they can track your current location.

They won't stop till this; they can further cross-check it with other available information to verify whether the IP address is connected with you particularly. Social networking sites such as instagram, LinkedIn, facebook are used to verify the information of your location gathered by the attacker.

ICMP Protocol

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, so 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.

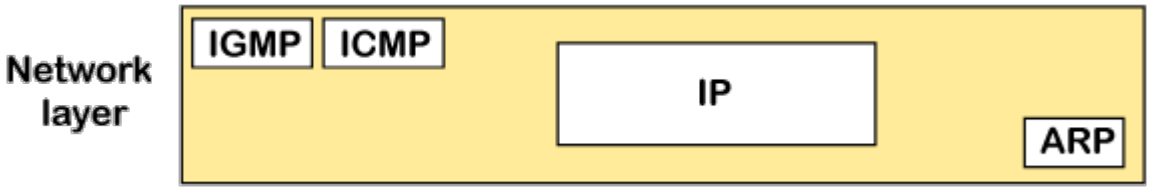
For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination. If no one reports the error, then the sender might think that the message has reached the destination. If

someone in-between reports the error, then the sender will resend the message very quickly.

Position of ICMP in the network layer

The ICMP resides in the IP layer, as shown in the below diagram.

Features of Java - Javatpoint



Messages

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**

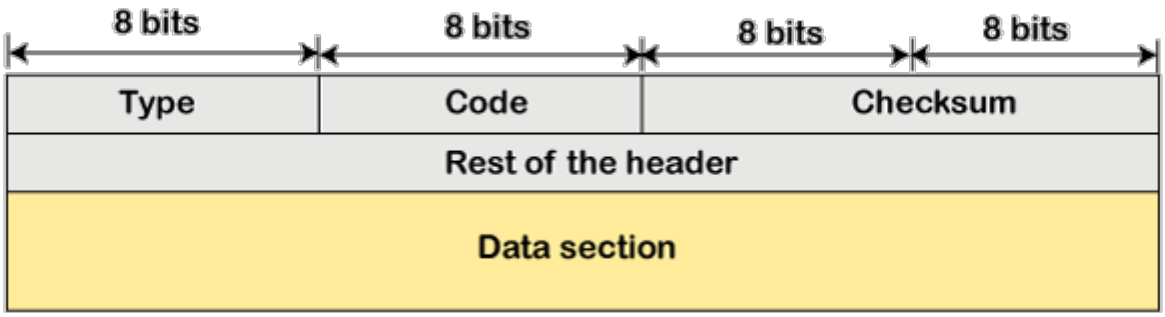
The query messages are those messages that help the host to get the specific information of another host. For example, suppose there are a client and a server, and the client wants to know whether the server is live or not, then it sends the ICMP message to the server.

ICMP Message Format

The message format has two things; one is a category that tells us which type of message it is. If the message is of error type, the error message contains the type

and the code. The type defines the type of message while the code defines the subtype of the message.

The ICMP message contains the following fields:

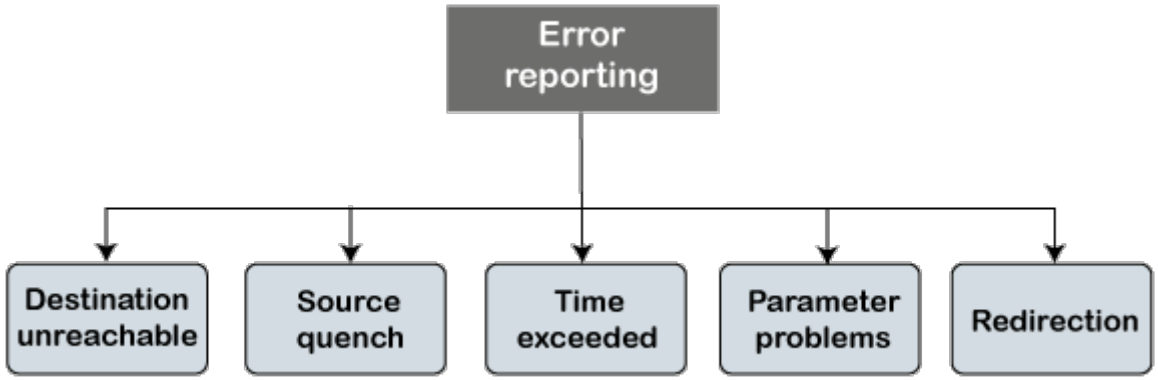


- **Type:** It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
- **Code:** It is an 8-bit field that defines the subtype of the ICMP message
- **Checksum:** It is a 16-bit field to detect whether the error exists in the message or not.

> ***Note:** The ICMP protocol always reports the error messages to the original source. For example, when the sender sends the message, if any error occurs in the message then the router reports to the sender rather than the receiver as the sender is sending the message.*

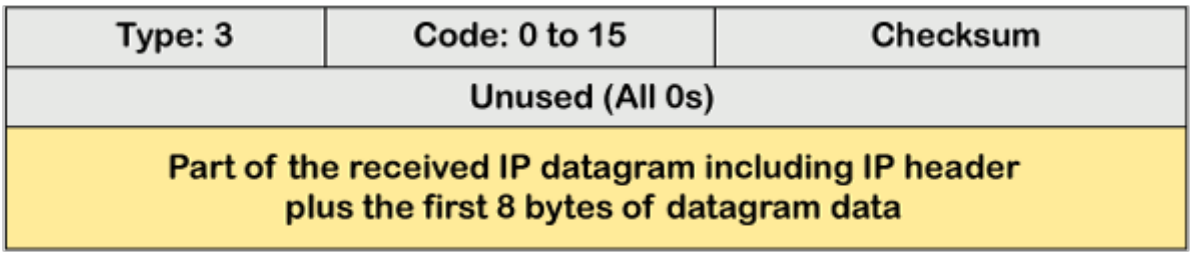
Types of Error Reporting messages

The error reporting messages are broadly classified into the following categories:



- **Destination unreachable**

The destination unreachable error occurs when the packet does not reach the destination. Suppose the sender sends the message, but the message does not reach the destination, then the intermediate router reports to the sender that the destination is unreachable.



The above diagram shows the message format of the destination unreachable message. In the message format:

Type: It defines the type of message. The number 3 specifies that the destination is unreachable.

Code (0 to 15): It is a 4-bit number which identifies whether the message comes from some intermediate router or the destination itself.

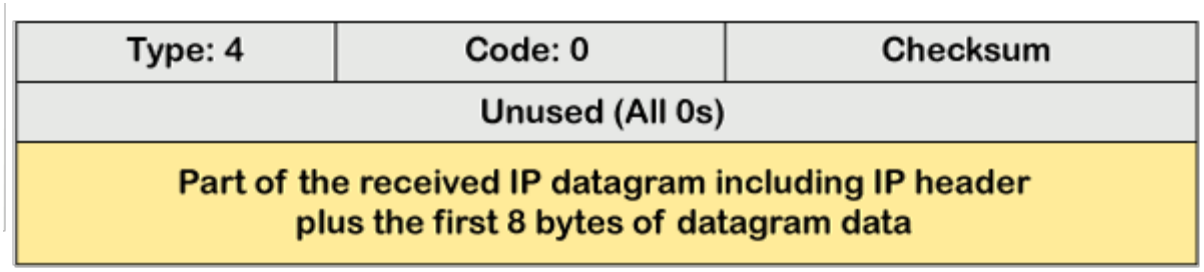
Note: If the destination creates the destination unreachable message then the code could be either 2 or 3.

Sometimes the destination does not want to process the request, so it sends the destination unreachable message to the source. A router does not detect all the problems that prevent the delivery of a packet.

- **Source quench**

There is no flow control or congestion control mechanism in the network layer or the IP protocol. The sender is concerned with only sending the packets, and the sender does not think whether the receiver is ready to receive those packets or is there any congestion occurs in the network layer so that the sender can send a lesser number of packets, so there is no flow control or congestion control mechanism.

In this case, ICMP provides feedback, i.e., source quench. Suppose the sender resends the packet at a higher rate, and the router is not able to handle the high data rate. To overcome such a situation, the router sends a source quench message to tell the sender to send the packet at a lower rate.



The above diagram shows the message format of the source quench message. It is a type 4 message, and code is zero.

Note: A source quench message informs the sender that the datagram has been discarded due to the congestion occurs in the network layer.

So, the sender must either stop or slow down the sending of datagrams until the congestion is reduced. The router sends one source-quench message for each datagram that is discarded due to the congestion in the network layer.

- **Time exceeded**

Sometimes the situation arises when there are many routers that exist between the sender and the receiver. When the sender sends the packet, then it moves in a routing loop.

The time exceeded is based on the time-to-live value. When the packet traverses through the router, then each router decreases the value of TTL by one. Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source.

Each of the MAC layers has different data units. For example, some layers can handle upto 1500 data units, and some can handle upto 300 units. When the packet is sent from a layer having 1500 units to the layer having 300 units, then the packet is divided into fragments; this process is known as fragmentation.

These 1500 units are divided into 5 fragments, i.e., f1, f2, f3, f4, f5, and these fragments reach the destination in a sequence. If all the fragments are not reached to the destination in a set time, they discard all the received fragments and send a time-exceeded message to the original source.

In the case of fragmentation, the code will be different as compared to TTL. Let's observe the message format of time exceeded.

Type: 11	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

The above message format shows that the type of time-exceeded is 11, and the code can be either 0 or 1. The code 0 represents TTL, while code 1 represents fragmentation. In a time-exceeded message, the code 0 is used by the routers to show that the time-to-live value is reached to zero.

The code 1 is used by the destination to show that all the fragments do not reach within a set time.

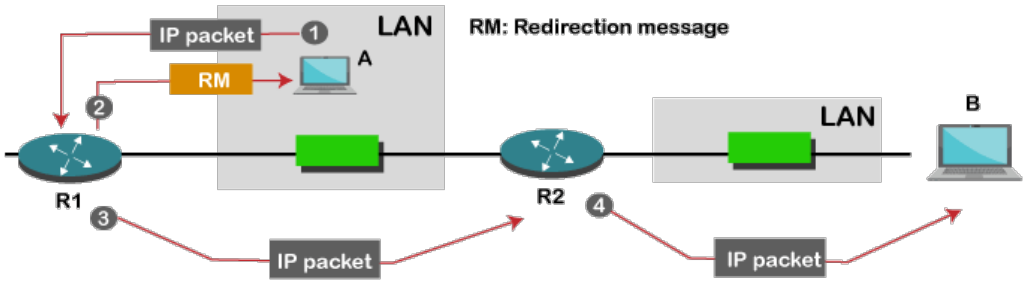
Parameter problems

The router and the destination host can send a parameter problem message. This message conveys that some parameters are not properly set.

Type: 12	Code: 0 or 1	Checksum
Pointer	Unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

The above diagram shows the message format of the parameter problem. The type of message is 12, and the code can be 0 or 1.

Redirection



When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message. For example, A wants to send the packet to B, and there are two routers exist between A and B. First, A sends the data to the router 1. The router 1 sends the IP packet to router 2 and

redirection message to A so that A can update its routing table.

ICMP Query Messages

The ICMP Query message is used for error handling or debugging the internet. This message is commonly used to ping a message.

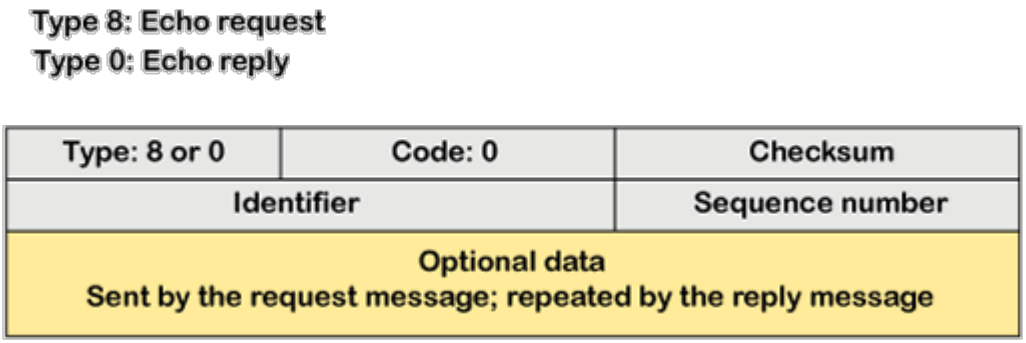
Echo-request and echo-reply message

A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive". If the other host is alive, then it sends the echo-reply message. An echo-reply message is sent by the router or the host that receives an echo-request message.

Key points of Query messages

1. The echo-request message and echo-reply message can be used by the network managers to check the operation of the IP protocol. Suppose two hosts, i.e., A and B, exist, and A wants to communicate with host B. The A host can communicate to host B if the link is not broken between A and B, and B is still alive.
2. The echo-request message and echo-reply message check the host's reachability, and it can be done by invoking the ping command.

The message format of echo-request and echo-reply message



The above diagram shows the message format of the echo-request and echo-reply message. The type of echo-request is 8, and the request of echo-reply is 0. The code of this message is 0.

Timestamp-request and timestamp-reply message

The timestamp-request and timestamp-reply messages are also a type of query messages. Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B. The computer B responds with a timestamp-reply message.

Message format of timestamp-request and timestamp-reply

Type 13: request
Type 14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence number
Original timestamp		
Receive timestamp		
Transmit timestamp		

The type of timestamp-request is 13, and the type of timestamp-reply is 14. The code of this type of message is 0.

Key points related to timestamp-request and timestamp-reply message

- It can be used to calculate the round-trip time between the source and the destination, even if the clocks are not synchronized.
- It can also be used to synchronize the clocks in two different machines if the exact transit time is known.

If the sender knows the exact transit time, then it can synchronize the clock. The sender asks the time on the receiver's clock, and then it adds the time and propagation delay. Suppose the time is 1:00 clock and propagation delay is 100 ms, then time would be 1:00 clock plus 100 ms.

Debugging tools

There are several tools used for debugging. In this topic, we will learn two tools that use ICMP for debugging. The two tools are **ping** and **traceroute**. We have learned about ping in echo-request and echo-reply messages that check whether the host or a router is alive or running.

Now we will take a look at the traceroute.

Traceroute is a tool that tracks the route taken by a packet on an IP network from source to destination. It records the time taken by the packet on each hop during its route from source to destination. Traceroute uses ICMP messages and TTL values.

The TTL value is calculated; if the TTL value reaches zero, the packet gets discarded. Traceroute uses small TTL values as they get quickly expired. If the TTL value is 1 then the message is produced by router 1; if the TTL value is 2 then the message is produced by router 2, and so on.

Let's understand the traceroute through an example.

Suppose A and B are two different hosts, and A wants to send the packet to the host B. Between A and B, 3 routers exist. To determine the location of the routers, we use the traceroute tool.

TTL value =1: First, host A sends the packet to router 1 with TTL value 1, and when the packet reaches to router 1 then router reduces the value of TTL by one and TTL values becomes 0. In this case, router 1 generates the time-exceeded message and host A gets to know that router 1 is the first router in a path.

TTL value=2: When host A sends the packet to router 1 with TTL value 2, and when the packet reaches to router 1 then the TTL value gets decremented by 1 and the TTL value becomes 1. Then router 1 sends the packet to router 2, and the TTL value becomes 0, so the router generates a time-exceeded message. The host A gets to know that router 2 is the second router on the path.

TTL value=3: When host A sends the packet to router 1 with TTL value 3, then the router decrements its value by one, and the TTL value becomes 2. Then, router 1 sends the packet to router 2, and the TTL value becomes 1. Then, router 2 sends the packet to router 3, and the TTL value becomes 0. As TTL value becomes 0, router 3 generates a time-exceeded message. In this way, host A is the third router on a path.

What is Routing Protocols?

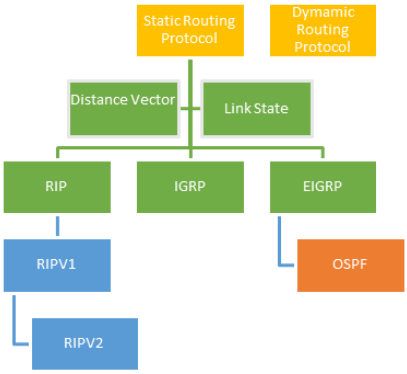
Routing Protocols are the set of defined rules used by the routers to communicate between source & destination. They do not move the information to the source to a destination, but only update the routing table that contains the information.

Network Router protocols helps you to specify way routers communicate with each other. It allows the network to select routes between any two nodes on a computer network.

Types of Routing Protocols

There are mainly two types of Network Routing Protocols

- Static
- Dynamic



Routing Protocols

Static Routing Protocols

Static routing protocols are used when an administrator manually assigns the path from source to the destination network. It offers more security to the network.

Advantages

- No overhead on router CPU.
- No unused bandwidth between links.
- Only the administrator is able to add routes

Disadvantages

- The administrator must know how each router is connected.
- Not an ideal option for large networks as it is time intensive.
- Whenever link fails all the network goes down which is not feasible in small networks.

Dynamic Routing Protocols

Dynamic routing protocols are another important type of routing protocol. It helps routers to add information to their routing tables from connected routers automatically. These types of protocols also send out topology updates whenever the network changes' topological structure.

Advantage:

- Easier to configure even on larger networks.
- It will be dynamically able to choose a different route in case if a link goes down.
- It helps you to do load balancing between multiple links.

Disadvantage:

- Updates are shared between routers, so it consumes bandwidth.
- Routing protocols put an additional load on router CPU or RAM.

Distance Vector Routing Protocol (DVR)

Distance Vector Protocols advertise their routing table to every directly connected neighbor at specific time intervals using lots of bandwidths and slow converge.

In the Distance Vector routing protocol, when a route becomes unavailable, all routing tables need to be updated with new information.

Advantages:

- Updates of the network are exchanged periodically, and it is always broadcast.
- This protocol always trusts route on routing information received from neighbor routers.

Disadvantages:

- As the routing information are exchanged periodically, unnecessary traffic is generated, which consumes available bandwidth.

Internet Routing Protocols:

The following are types of protocols which help data packets find their way across the Internet:

Routing Information Protocol (RIP)

RIP is used in both LAN and WAN Networks. It also runs on the Application layer of the OSI model. The full form of RIP is the Routing Information Protocol. Two versions of RIP are

1. RIPv1
2. RIPv2

The original version or RIPv1 helps you determine network paths based on the IP destination and the hop count journey. RIPv1 also interacts with the network by broadcasting its IP table to all routers connected with the network.

RIPv2 is a little more sophisticated as it sends its routing table on to a multicast address.

Interior Gateway Protocol (IGP)

IGRP is a subtype of the distance-vector interior gateway protocol developed by CISCO. It is introduced to overcome RIP limitations. The metrics used are load, bandwidth, delay, MTU, and reliability. It is widely used by routers to exchange routing data within an autonomous system.

This type of routing protocol is the best for larger network size as it broadcasts after every 90 seconds, and it has a maximum hop count of 255. It helps you to sustain larger networks compared to RIP.

IGRP is also widely used as it is resistant to routing loop because it updates itself automatically when route changes occur within the specific network. It is also given an option to load balance traffic across equal or unequal metric cost paths.

Link State Routing Protocol

Link State Protocols take a unique approach to search the best routing path. In this protocol, the route is calculated based on the speed of the path to the destination and the cost of resources.

Routing protocol tables:

Link state routing protocol maintains below given three tables:

- **Neighbor table:** This table contains information about the neighbors of the router only. For example, adjacency has been formed.
- **Topology table:** This table stores information about the whole topology. For example, it contains both the best and backup routes to a particular advertised network.
- **Routing table:** This type of table contains all the best routes to the advertised network.

Advantages:

- This protocol maintains separate tables for both the best route and the backup routes, so it has more knowledge of the inter-network than any other distance vector routing protocol.
- Concept of triggered updates are used, so it does not consume any unnecessary bandwidth.
- Partial updates will be triggered when there is a topology change, so it does not need to update where the whole routing table is exchanged.

Exterior Gateway Protocol (EGP)

EGP is a protocol used to exchange data between gateway hosts that are neighbors with each other within autonomous systems. This routing protocol offers a forum for routers to share information across different domains. The full form for EGP is the Exterior Gateway Protocol. EGP protocol includes known routers, network addresses, route costs, or neighboring devices.

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a hybrid routing protocol that provides routing protocols, distance vector, and link-state routing protocols. The full form routing protocol EIGRP is

Enhanced Interior Gateway Routing Protocol. It will route the same protocols that IGRP routes using the same composite metrics as IGRP, which helps the network select the best path destination.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) protocol is a link-state IGP tailor-made for IP networks using the Shortest Path First (SPF) method.

OSPF routing allows you to maintain databases detailing information about the surrounding topology of the network. It also uses the Dijkstra algorithm (Shortest path algorithm) to recalculate network paths when its topology changes. This protocol is also very secure, as it can authenticate protocol changes to keep data secure.

Here are some main difference between these Distance Vector and Link State routing protocols:

Distance Vector	Link State
Distance Vector protocol sends the entire routing table.	Link State protocol sends only link-state information.
It is susceptible to routing loops.	It is less susceptible to routing loops.
Updates are sometimes sent using broadcast.	Uses only multicast method for routing updates.
It is simple to configure.	It is hard to configure this routing protocol.
Does not know network topology.	Know the entire topology.
Example RIP, IGRP.	Examples: OSPF IS-IS.

Intermediate System-to-Intermediate System (IS-IS)

ISIS CISCO routing protocol is used on the Internet to send IP routing information. It consists of a range of components, including end systems, intermediate systems, areas, and domains.

The full form of ISIS is Intermediate System-to-Intermediate System. Under the IS-IS protocol, routers are organized into groups called areas. Multiple areas are grouped to make form a domain.

Border Gateway Protocol (BGP)

BGP is the last routing protocol of the Internet, which is classified as a DPVP (distance path vector protocol). The full form of BGP is the Border Gateway Protocol.

This type of routing protocol sends updated router table data when changes are made. Therefore, there is no auto-discovery of topology changes, which means that the user needs to configure BGP manually.

What is the purpose of Routing Protocols?

Routing protocols are required for the following reasons:

- Allows optimal path selection
- Offers loop-free routing
- Fast convergence
- Minimize update traffic
- Easy to configure
- Adapts to changes
- Scales to a large size
- Compatible with existing hosts and routers
- Supports variable length

Classful Vs. Classless Routing Protocols

Here are some main difference between these routing protocols:

Classful Routing Protocols	Classless Routing Protocols
Classful routing protocols never send subnet mask detail during routing updates.	Classless routing protocols can send IP subnet mask information while doing routing updates.
RIPv1 and IGRP are classful protocols. These two are classful protocols as they do not include subnet mask information.	RIPv2, OSPF, EIGRP, and IS-IS are all types of class routing protocols which has subnet mask information within updates.

Distance Vector Routing Algorithm

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

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

- **Knowledge about the whole network:** Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.
- **Routing only to neighbors:** The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.
- **Information sharing at regular intervals:** Within 30 seconds, the router sends the information to the neighboring routers.

Distance Vector Routing Algorithm

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

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

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

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

- For each neighbor v, the cost c(x,v) is the path cost from x to directly attached neighbor, v.
- The distance vector x, i.e., $D_x = [\ D_x(y) : y \text{ in } N\ ]$, containing its cost to all destinations, y, in N.
- The distance vector of each of its neighbors, i.e., $D_v = [\ D_v(y) : y \text{ in } N\ ]$ for each neighbor v of x.

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

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

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

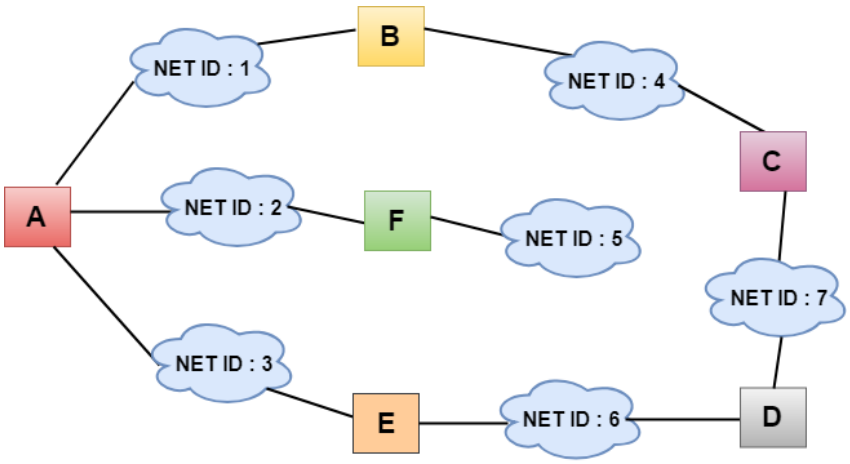
Algorithm

At each node x,

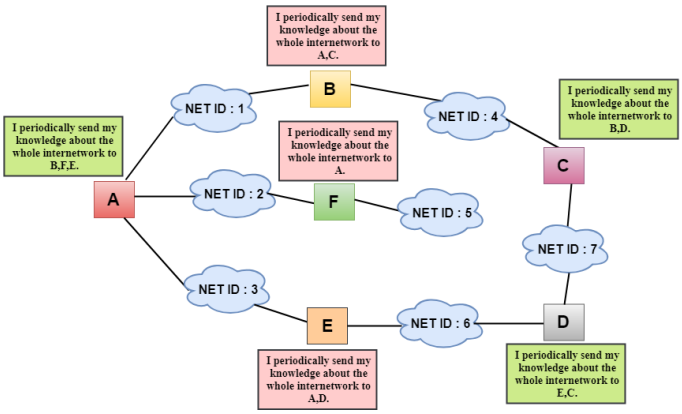
Initialization

for all destinations y in N:
$D_x(y) = c(x,y)$ // If y is not a neighbor then $c(x,y) = \infty$
for each neighbor w
$D_w(y) = ?$ for all destination y in N.
for each neighbor w
send distance vector $D_x = [D_x(y) : y \text{ in } N]$ to w
loop
wait(until I receive any distance vector from some neighbor w)
for each y in N:
$D_x(y) = \min_v\{c(x,v)+D_v(y)\}$
If $D_x(y)$ is changed for any destination y
Send distance vector $D_x = [D_x(y) : y \text{ in } N]$ to all neighbors
forever

Sharing Information



- In the above figure, each cloud represents the network, and the number inside the cloud represents the network ID.
- All the LANs are connected by routers, and they are represented in boxes labeled as A, B, C, D, E, F.
- Distance vector routing algorithm simplifies the routing process by assuming the cost of every link is one unit. Therefore, the efficiency of transmission can be measured by the number of links to reach the destination.
- In Distance vector routing, the cost is based on hop count.



In the above figure, we observe that the router sends the knowledge to the immediate neighbors. The neighbors add this knowledge to their own knowledge and sends the updated table to their own neighbors. In this way, routers get its own information plus the new information about the neighbors.

Routing Table

Two process occurs:

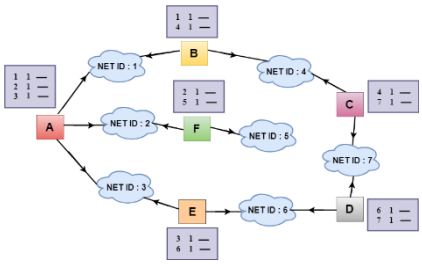
- **Creating the Table**
- **Updating the Table**

Creating the Table

Initially, the routing table is created for each router that contains at least three types of information such as Network ID, the cost and the next hop.

NET ID	Cost	Next Hop

- **NET ID:** The Network ID defines the final destination of the packet.
- **Cost:** The cost is the number of hops that packet must take to get there.
- **Next hop:** It is the router to which the packet must be delivered.



- In the above figure, the original routing tables are shown of all the routers. In a routing table, the first column represents the network ID, the second column represents the cost of the link, and the third column is empty.
- These routing tables are sent to all the neighbors.

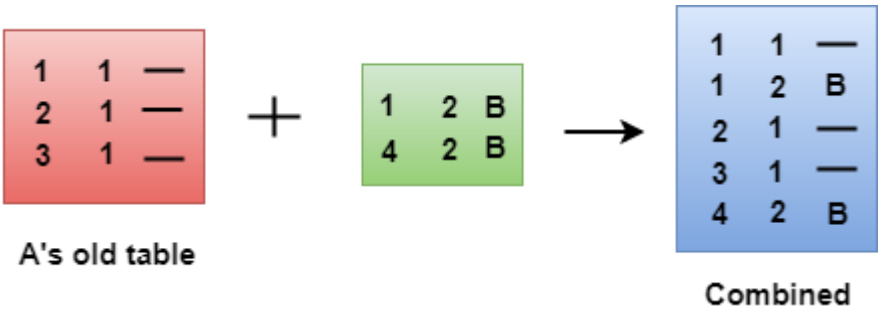
For Example:

1. A sends its routing table to B, F & E.
2. B sends its routing table to A & C.
3. C sends its routing table to B & D.
4. D sends its routing table to E & C.
5. E sends its routing table to A & D.
6. F sends its routing table to A.

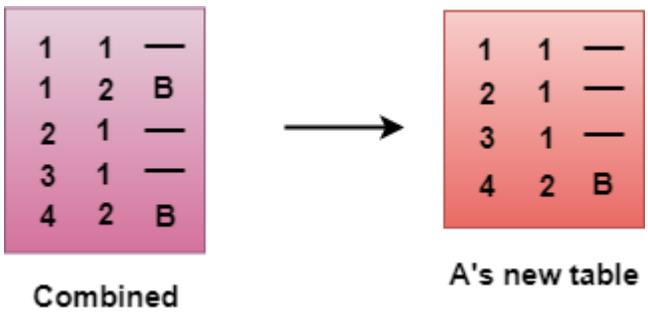
Updating the Table

- When A receives a routing table from B, then it uses its information to update the table.
- The routing table of B shows how the packets can move to the networks 1 and 4.
- The B is a neighbor to the A router, the packets from A to B can reach in one hop. So, 1 is added to all the costs given in the B's table and the sum will be the cost to reach a particular network.

- After adjustment, A then combines this table with its own table to create a combined table.

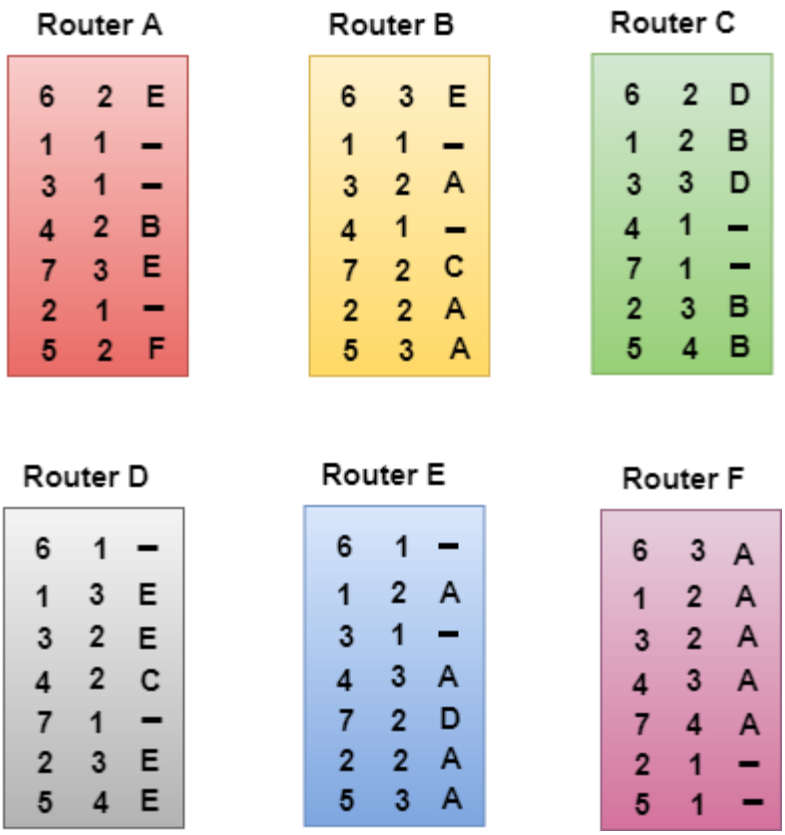


- The combined table may contain some duplicate data. In the above figure, the combined table of router A contains the duplicate data, so it keeps only those data which has the lowest cost. For example, A can send the data to network 1 in two ways. The first, which uses no next router, so it costs one hop. The second requires two hops (A to B, then B to Network 1). The first option has the lowest cost, therefore it is kept and the second one is dropped.



- The process of creating the routing table continues for all routers. Every router receives the information from the neighbors, and update the routing table.

Final routing tables of all the routers are given below:



Link State Routing

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

The three keys to understand the Link State Routing algorithm:

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

Link State Routing has two phases:

Reliable Flooding

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

- **Final state:** Each node knows the entire graph.

Route Calculation

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

- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

Let's describe some notations:

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

Algorithm

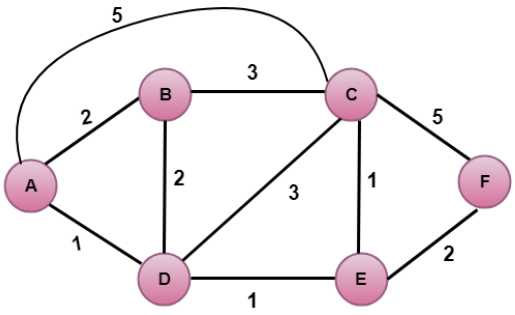
Initialization
N = {A} // **A is a root node**.
for all nodes v
if v adjacent to A
then D(v) = c(A,v)
else D(v) = infinity
loop
find w not in N such that D(w) is a minimum.
Add w to N
Update D(v) for all v adjacent to w and not in N:
D(v) = min(D(v) , D(w) + c(w,v))
Until all nodes in N

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

network.

Triggers in SQL (Hindi)

Let's understand through an example:



In the above figure, source vertex is A.

Step 1:

The first step is an initialization step. The currently known least cost path from A to its directly attached neighbors, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

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

Step 2:

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

a) Calculating shortest path from A to B

1. v = B, w = D
2. D(B) = min(D(B) , D(D) + c(D,B))
3. = min(2, 1+2)>
4. = min(2, 3)
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating shortest path from A to C

1. v = C, w = D
2. D(B) = min(D(C) , D(D) + c(D,C))
3. = min(5, 1+3)
4. = min(5, 4)
5. The minimum value is 4. Therefore, the currently shortest path from A to C is 4.</p>

c) Calculating shortest path from A to E

1. v = E, w = D
2. D(B) = min(D(E) , D(D) + c(D,E))
3. = min(∞, 1+1)
4. = min(∞, 2)
5. The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

Note: The vertex D has no direct link to vertex E. Therefore, the value of D(F) is infinity.

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

Step 3:

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

a) Calculating the shortest path from A to B.

1. v = B, w = E
2. D(B) = min(D(B) , D(E) + c(E,B))
3. = min(2 , 2+ ∞)
4. = min(2, ∞)
5. The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating the shortest path from A to C.

1. v = C, w = E
2. D(B) = min(D(C) , D(E) + c(E,C))
3. = min(4 , 2+1)
4. = min(4,3)
5. The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

c) Calculating the shortest path from A to F.

1. v = F, w = E
2. D(B) = min(D(F) , D(E) + c(E,F))
3. = min(∞ , 2+2)
4. = min(∞ ,4)
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

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

Step 4:

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

a) Calculating the shortest path from A to C.

1. v = C, w = B
2. D(B) = min(D(C) , D(B) + c(B,C))
3. = min(3 , 2+3)
4. = min(3,5)
5. The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

b) Calculating the shortest path from A to F.

1. v = F, w = B
2. D(B) = min(D(F) , D(B) + c(B,F))
3. = min(4, ∞)
4. = min(4, ∞)
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

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

Step 5:

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

a) Calculating the shortest path from A to F.

1. v = F, w = C
2. D(B) = min(D(F) , D(C) + c(C,F))
3. = min(4, 3+5)
4. = min(4,8)
5. The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

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

Final table:

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

Disadvantage:

Heavy traffic is created in Line state routing due to Flooding. Flooding can cause an infinite looping, this problem can be solved by using Time-to-leave field.