THE NETWORK LAYER

The network layer is concerned with getting packets from the source all the way to the destination. Getting to the destination may require making many hops at intermediate routers along the way. This function clearly contrasts with that of the data link layer, which has the more modest goal of just moving frames from one end of a wire to the other. Thus, the network layer is the lowest layer that deals with end-to-end transmission. To achieve its goals, the network layer must know about the topology of the network (i.e., the set of all routers and links) and choose appropriate paths through it, even for large networks. It must also take care when choosing routes to avoid overloading some of the communication lines and routers while leaving others idle. Finally, when the source and destination are in different networks, new problems occur. It is up to the network layer to deal with them. In this chapter we will study all these issues and illustrate them, primarily using the Internet and its network layer protocol, IP.

Network layer design issues:

The network layer comes with some design issues they are described as follows:

1. Store and Forward packet switching:

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

2. Services provided to Transport Layer:

Through the network/transport layer interface, the network layer transfers it’s services to the transport layer. These services are described below.
But before providing these services to the transfer layer following goals must be kept in mind :-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided :

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service:

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

4. Implementation of Connection Oriented service:

To use a connection-oriented service, first we establish a connection, use it and then release

it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.
It can be done in either two ways:

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

Routing is the process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes that data packets follow. Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

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.

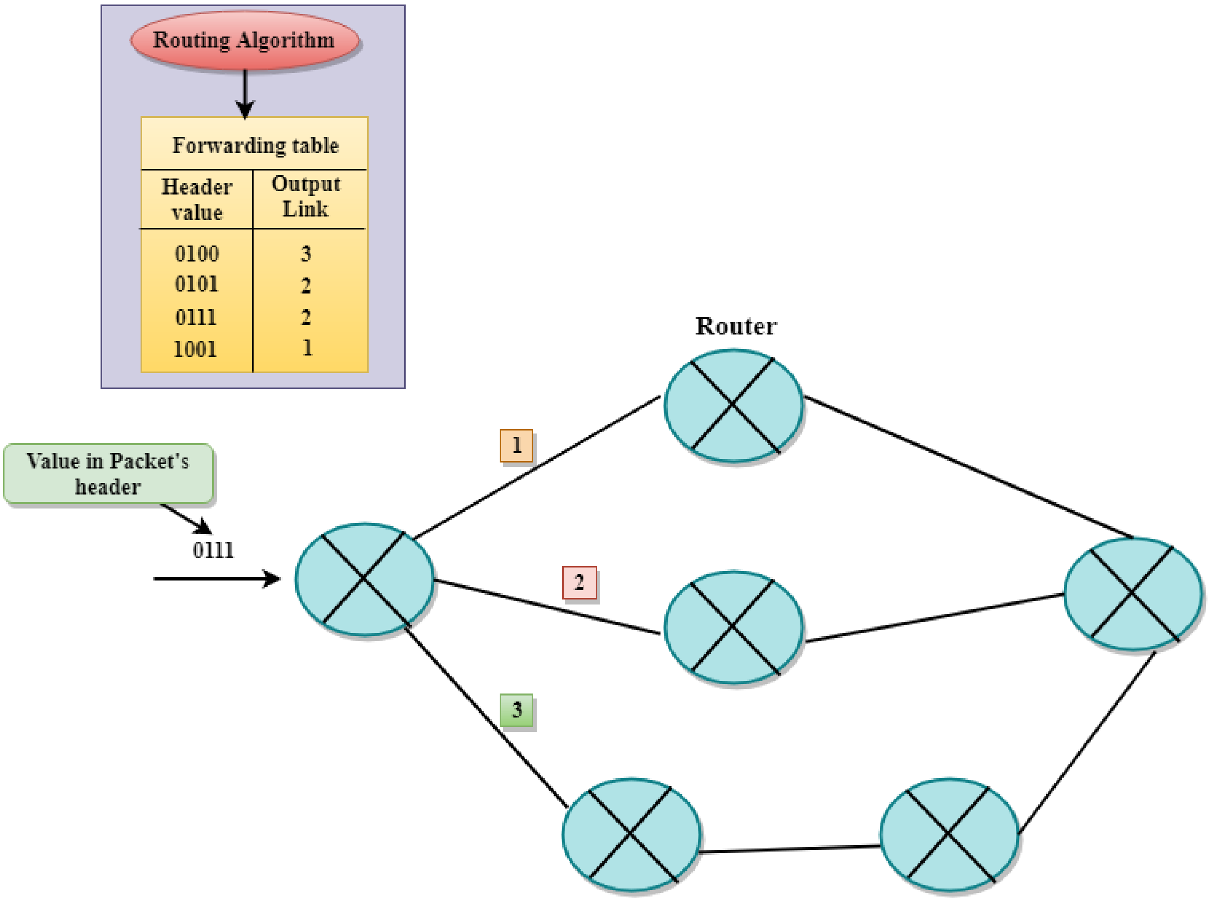
Forwarding & Routing

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 2. 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.



Forwarding table

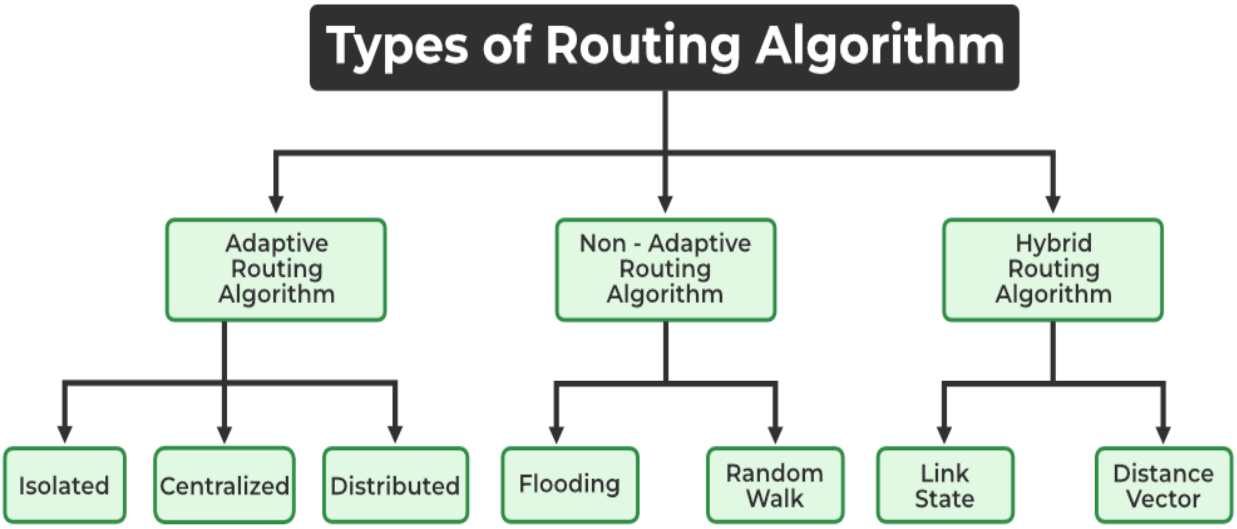
Header value	Output Link
0100	3
0101	2
0111	2
1001	1

Routing algorithms determine the values in forwarding table

Classification of Routing Algorithms

The routing algorithms can be classified as follows:

1. Adaptive Algorithms
2. Non-Adaptive Algorithms
3. Hybrid Algorithms



Types of Routing Algorithm

1. Adaptive Algorithms

These are the algorithms that change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as the traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops, and estimated transit time.
Further, these are classified as follows:

- **Isolated:** In this method each, node makes its routing decisions using the information it has without seeking information from other nodes. The sending nodes don't have information about the status of a particular link. The disadvantage is that packets may be sent through a congested network which may result in delay.
  Examples: Hot potato routing, and backward learning.

- **Centralized:** In this method, a centralized node has entire information about the network and makes all the routing decisions. The advantage of this is only one node is required to keep the information of the entire network and the disadvantage is that if the central node goes down the entire network is done. The link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

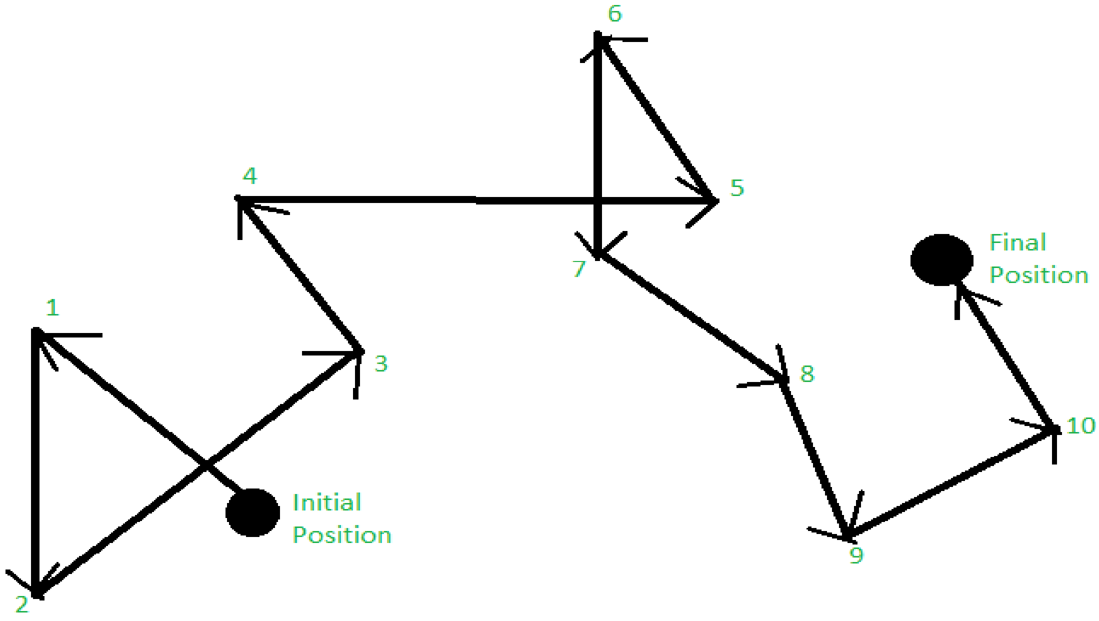
- **Distributed:** In this method, the node receives information from its neighbors and then takes the decision about routing the packets. A disadvantage is that the packet may be delayed if there is a change in between intervals in which it receives information and sends packets. It is also known as a decentralized algorithm as it computes the least-cost path between source and destination.

2. Non-Adaptive Algorithms

These are the algorithms that do not change their routing decisions once they have been selected. This is also known as static routing as a route to be taken is computed in advance and downloaded to routers when a router is booted.

Further, these are classified as follows:

- **Flooding:** This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in a loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count, and spanning trees.
- **Random walk:** In this method, packets are sent host by host or node by node to one of its neighbors randomly. This is a highly robust method that is usually implemented by sending packets onto the link which is least queued.



Random Walk

3. Hybrid Algorithms

As the name suggests, these algorithms are a combination of both adaptive and non-adaptive algorithms. In this approach, the network is divided into several regions, and each region uses a different algorithm. Further, these are classified as follows:

- Link-state: In this method, each router creates a detailed and complete map of the network which is then shared with all other routers. This allows for more accurate and efficient routing decisions to be made.
- Distance vector: In this method, each router maintains a table that contains information about the distance and direction to every other node in the network. This table is then shared with other routers in the network. The disadvantage of this method is that it may lead to routing loops.

Difference between Adaptive and Non-Adaptive Routing Algorithms

The main difference between Adaptive and Non-Adaptive Algorithms is:

Adaptive Algorithms are the algorithms that change their routing decisions whenever network topology or traffic load changes. It is called Dynamic Routing. Adaptive Algorithm is used in a large amount of data, highly complex network, and rerouting of data.

Non-Adaptive Algorithms are algorithms that do not change their routing decisions once they have been selected. It is also called static Routing. Non-Adaptive Algorithm is used in case of a small amount of data and a less complex network.

For more differences, you can refer to Differences between Adaptive and Non-Adaptive Routing Algorithms.

Difference between Routing and Flooding:

Routing	**Flooding**
A routing table is required.	No Routing table is required.
May give the shortest path.	Always gives the shortest path.
Less Reliable.	More Reliable.
Traffic is less.	Traffic is high.
No duplicate packets.	Duplicate packets are present.

IPv4:

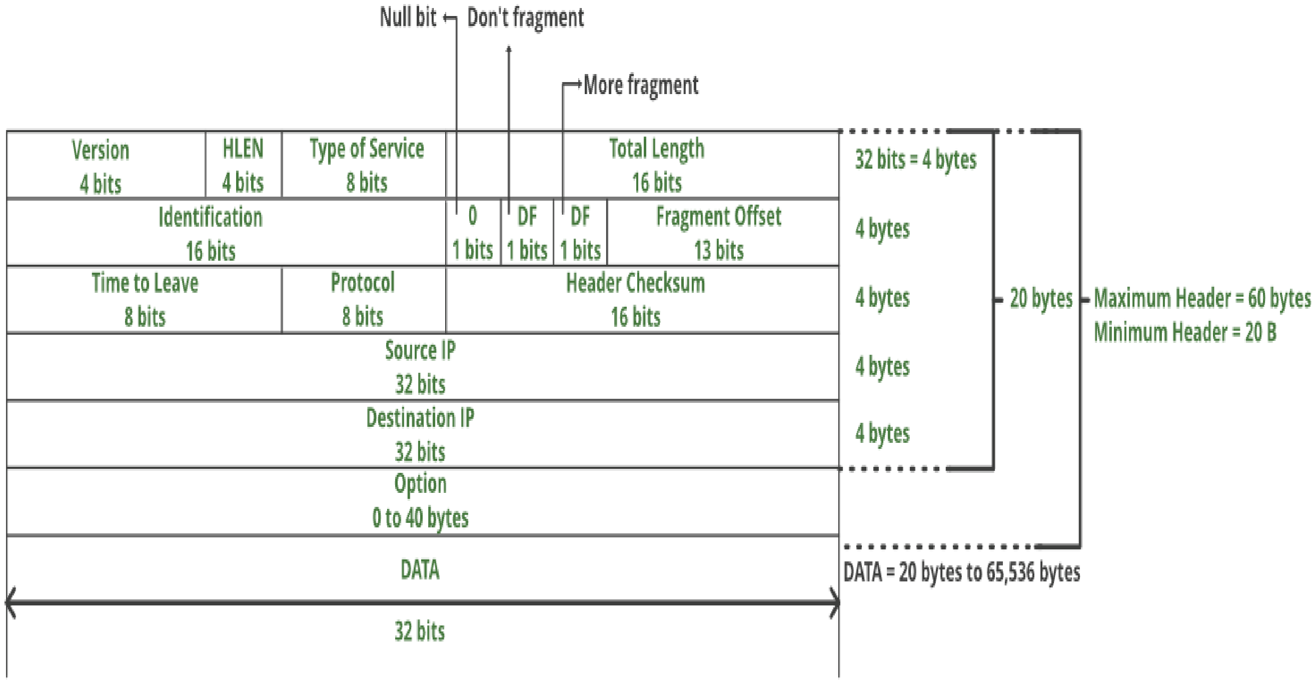
IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.

IPv4 is defined and specified in IETF publication RFC 791.

IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use.

IPv4 uses 32-bit (4 byte) addressing, which gives 2^{32} addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

IPv4 Datagram Header: Size of the header is 20 to 60 bytes.



VERSION: *Version of the IP protocol (4 bits), which is 4 for IPv4*
HLEN: *IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*
Type of service: *Low Delay, High Throughput, Reliability (8 bits)*
Total Length: *Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.*
Identification: *Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)*
Flags: *3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)*
Fragment Offset: *Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.*
Time to live: *Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*
Protocol: *Name of the protocol to which the data is to be passed (8 bits)*
Header Checksum: *16 bits header checksum for checking errors in the datagram header*
Source IP address: *32 bits IP address of the sender*
Destination IP address: *32 bits IP address of the receiver*
Option: *Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
- Data communication across the network becomes a lot of specific in multicast organizations.
    - Limits net growth for existing users and hinders the use of the net for brand new users.
    - Internet Routing is inefficient in IPv4.
    - IPv4 has high System Management prices and it’s labor-intensive, complex, slow & frequent to errors.
    - Security features are nonobligatory.
    - Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

Limitations of IPv4

- IP relies on network layer addresses to identify end-points on network, and each network has a unique IP address.
- The world’s supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
- If there are multiple host, we need IP addresses of next class.
- Complex host and routing configuration, non-hierarchical addressing, difficult to re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc. are the big limitation of IPv4 so that’s why IPv6 came into the picture.

IP address is your digital identity. It’s a network address for your computer so the Internet knows where to send you emails, data, etc.

IP address determines who and where you are in the network of billions of digital devices that are connected to the Internet.

IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

IPv4 vs IPv6
The common type of IP address (is known as IPv4, for “version 4”). Here’s an example of what an IP address might look like:

25.59.209.224

An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. Each of the four numbers can range from 0 to 255. This group of separated numbers creates the addresses that let you and everyone around the globe to send and retrieve data over our Internet connections. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic. Initially, it was assumed it would never run out of addresses but the present situation paves a new way to IPv6, let’s see why? An IPv6 address consists of eight groups of four hexadecimal digits. Here’s an example IPv6 address:

3001:0da8:75a3:0000:0000:8a2e:0370:7334

This new IP address version is being deployed to fulfil the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 also called IPng (Internet Protocol next generation).

IPv6 support a theoretical maximum of 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456. To keep it straightforward, we will never run out of IP addresses again.

Types of IPv6 Address
Now that we know about what is IPv6 address let’s take a look at its different types.

- **Unicast addresses** It identifies a unique node on a network and usually refers to a single sender or a single receiver.
- **Multicast addresses** It represents a group of IP devices and can only be used as the destination of a datagram.
- **Anycast addresses** It is assigned to a set of interfaces that typically belong to different nodes.

Advantages of IPv6

- Reliability
- **Faster Speeds:** IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- **Stronger Security:** IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network.

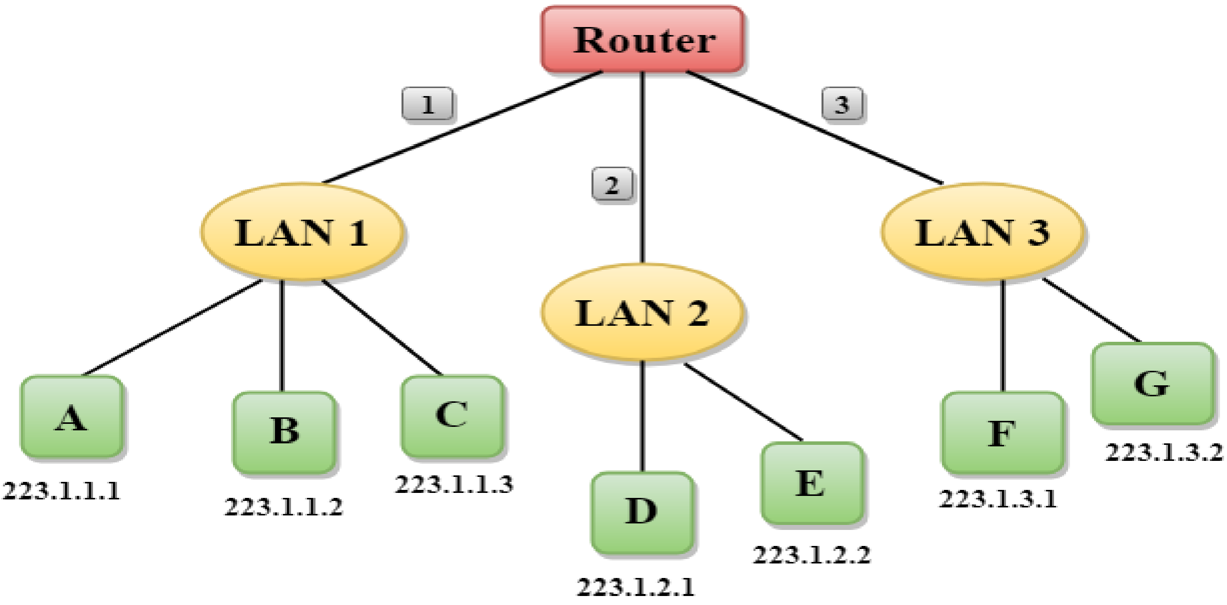
Disadvantages of IPv6

- **Conversion:** Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- **Communication:** IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

Network Addressing

- Network Addressing is one of the major responsibilities of the network layer.
- Network addresses are always logical, i.e., software-based addresses.
- A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

Let's understand through a simple example.



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

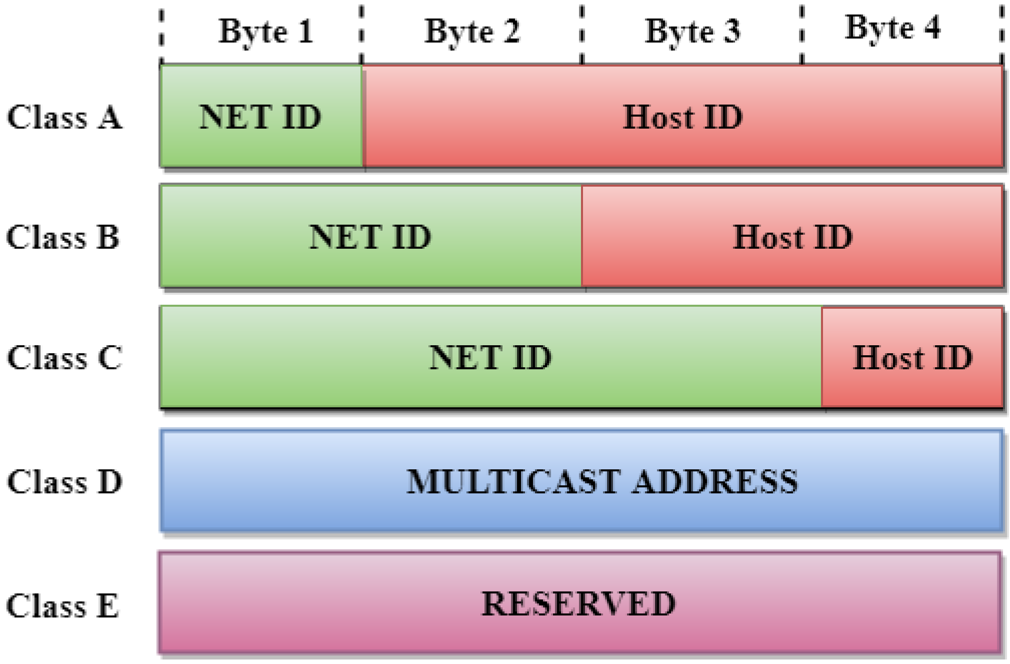
Classful Addressing

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

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

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



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

Class A

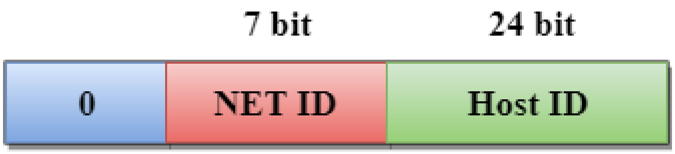
In Class A, an IP address is assigned to those networks that contain a large number of hosts.

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

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

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address



Class B

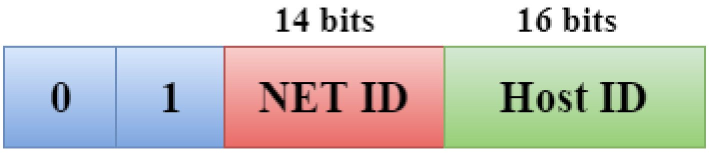
In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

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

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

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address



Class C

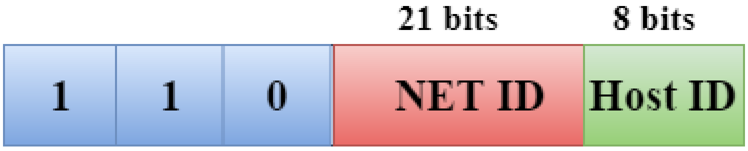
In Class C, an IP address is assigned to only small-sized networks.

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

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

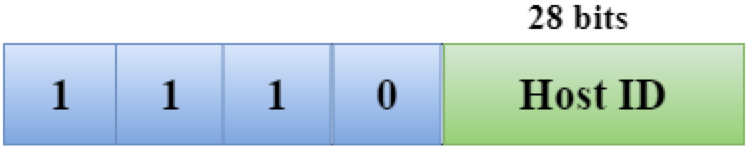
The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^{8} - 2 = 254 host address



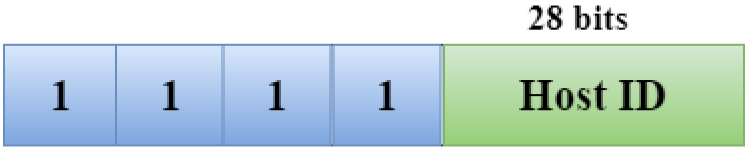
Class D

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



Class E

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



Rules for assigning Host ID:

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

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

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

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

Classful Network Architecture

Class	**Higher bits**	**NET ID bits**	**HOST ID bits**	**No.of networks**	**No.of hosts per network**	**Range**
A	0	8	24	2^{7}	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^{8}	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

Subnetting

Subnetting is the process of dividing a large IP network into smaller sub-networks, known as subnets. This is done by borrowing bits from the host portion of the IP address and using them to create a network ID for the subnet. Subnetting allows network administrators to better manage their IP address space and improve network performance and security.

For example, consider the IP address 192.168.1.0/24. This means that the network has 256 IP addresses (0-255), with 192.168.1.0 being the network address and 192.168.1.255 being the broadcast address. By subnetting this network, we can create smaller sub-networks with their own network ID and broadcast address.

Let's say we want to create 4 subnets from this network. To do this, we need to borrow 2 bits from the host portion of the IP address. This gives us 4 possible combinations of those 2 bits, which we can use as the network ID for each subnet.

So, we would end up with the following subnets:

- Subnet 1: 192.168.1.0/26 (64 hosts)
- Subnet 2: 192.168.1.64/26 (64 hosts)
- Subnet 3: 192.168.1.128/26 (64 hosts)
- Subnet 4: 192.168.1.192/26 (64 hosts)

Each of these subnets has its own network ID and broadcast address, and can be used to manage separate departments or groups within the organization.

Supernetting

Supernetting, also known as route aggregation or CIDR (Classless Inter-Domain Routing), is the opposite of subnetting. It involves combining multiple smaller networks into a larger network, which can be advertised as a single route. This reduces the size of routing tables and improves network performance.

For example, let's say an organization has the following networks:

- 192.168.1.0/26 (64 hosts)
- 192.168.1.64/26 (64 hosts)
- 192.168.1.128/26 (64 hosts)
- 192.168.1.192/26 (64 hosts)

Instead of advertising each of these networks separately, we can combine them into a single supernet using CIDR notation. The prefix length of the supernet is determined by the number of common bits in the network portion of the IP addresses.

In this case, all of the networks have the same first 24 bits (192.168.1), so we can represent them as a single supernet with a prefix length of /24:

- 192.168.1.0/24 (256 hosts)

This means that any traffic destined for any of the original networks will be sent to the supernet, which will then route the traffic to the appropriate subnet based on the network ID.

Supernetting is commonly used by Internet Service Providers (ISPs) to reduce the size of their routing tables and improve network efficiency.

Question:

You have been assigned the IP address block 192.168.10.0/24 for your organization's network. You want to create four subnets, each with at least 30 hosts. Design the subnets and provide the following information for each subnet:

- Network ID
- First usable IP address
- Last usable IP address
- Broadcast address

Also, assume that you have been allocated the IP address blocks 192.168.10.0/25, 192.168.10.128/26, and 192.168.10.192/26 from your ISP. Design a supernet for these blocks and provide the following information:

- Network ID
- First usable IP address
- Last usable IP address
- Broadcast address
- Prefix length in CIDR notation

Solution:

Subnetting:

We want to create four subnets with at least 30 hosts each, which means we need to reserve at least 5 bits for the host portion of the IP address (2^5 = 32). Since the original network has a prefix length of 24 bits, we have 8 bits available for the host portion.

To create four subnets, we need to borrow 2 bits from the host portion of the IP address. This leaves us with 6 bits for the host portion, which gives us 2^6 - 2 = 62 usable hosts per subnet (the -2 is for the network and broadcast addresses).

The subnet mask for each subnet will be /26 (24 + 2 = 26). The four subnets can be designed as follows:

- Subnet 1:
    - Network ID: 192.168.10.0/26
    - First usable IP address: 192.168.10.1
    - Last usable IP address: 192.168.10.62
    - Broadcast address: 192.168.10.63
- Subnet 2:
    - Network ID: 192.168.10.64/26
    - First usable IP address: 192.168.10.65
    - Last usable IP address: 192.168.10.126
    - Broadcast address: 192.168.10.127
- Subnet 3:

    - Network ID: 192.168.10.128/26
    - First usable IP address: 192.168.10.129
    - Last usable IP address: 192.168.10.190
    - Broadcast address: 192.168.10.191
- Subnet 4:
    - Network ID: 192.168.10.192/26
    - First usable IP address: 192.168.10.193
    - Last usable IP address: 192.168.10.254
    - Broadcast address: 192.168.10.255

Supernetting:

We have been allocated the IP address blocks 192.168.10.0/25, 192.168.10.128/26, and 192.168.10.192/26 from our ISP. To create a supernet, we need to find the common prefix between these blocks.

- 192.168.10.0/25: 192.168.10.0 - 192.168.10.127
- 192.168.10.128/26: 192.168.10.128 - 192.168.10.191
- 192.168.10.192/26: 192.168.10.192 - 192.168.10.255

From these blocks, we can see that the first 25 bits are common among all of them. Therefore, we can create a supernet with a prefix length of /25 (the first 25 bits are common). The network ID for the supernet will be 192.168.10.0/25, and the first and last usable IP addresses will be the same as the first and last IP addresses of the original /25 block. The broadcast address for the supernet will be the same as the broadcast address of the original /25 block.

- Supernet:
- Network ID: 192.168.10.0/25
- First usable IP address: 192.168.10.1
- Last usable IP address: 192.168.10.126
- Broadcast address: 192.168.10.127
- Prefix length: /25