Unit-7

TCP/IP Reference Model

Introduction

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.

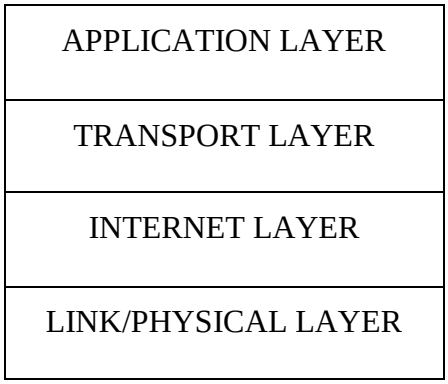
Overview of TCP/IP Reference Model:

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to (send data packets) another application running on different computer.



Layers of TCP/IP reference model

Application Layer (Layer 4)

The top layer of the protocol stack is the application layer. It refers to the programs that initiate communication in the first place. TCP/IP includes several application layer protocols for mail, file transfer, remote access, authentication and name resolution. These protocols are embodied in

programs that operate at the top layer just as any custom-made or packaged client/server application would.

There are many Application Layer protocols and new protocols are always being developed.

The most widely known Application Layer protocols are those used for the exchange of user information, some of them are:

- **The HyperText Transfer Protocol (HTTP)** is used to transfer files that make up the Web pages of the World Wide Web.
- **The File Transfer Protocol (FTP)** is used for interactive file transfer.
- **The Simple Mail Transfer Protocol (SMTP)** is used for the transfer of mail messages and attachments.
- **Telnet,** is a terminal emulation protocol, and, is used for remote login to network hosts.

Other Application Layer protocols that help in the management of TCP/IP networks are:

- **The Domain Name System (DNS),** which, is used to resolve a host name to an IP address.
- **The Simple Network Management Protocol (SNMP)** which is used between network management consoles and network devices (routers, bridges, and intelligent hubs) to collect and exchange network management information.

Examples of Application Layer interfaces for TCP/IP applications are Windows Sockets and NetBIOS. Windows Sockets provides a standard application programming interface (API) under the Microsoft Windows operating system. NetBIOS is an industry standard interface for accessing protocol services such as sessions, datagrams, and name resolution.

Transport Layer (Layer 3)

The Transport Layer (also known as the Host-to-Host Transport Layer) is responsible for providing the Application Layer with session and datagram communication services.

TCP/IP does not contain Presentation and Session layers, the services are performed if required, but they are not part of the formal TCP/IP stack. For example, Layer 6 (Presentation Layer) is where data conversion (ASCII to EBCDIC, floating point to binary, etc.) and encryption /decryption is performed. Layer 5 is the Session Layer, which is performed in layer 4 in TCP/IP. Thus, we jump from layer 7 of OSI down to layer 4 of TCP/IP.

From Application to Transport Layer, the application delivers its data to the communications system by passing a stream of data bytes to the transport layer along with the socket of the destination machine.

The core protocols of the Transport Layer are TCP and the User Datagram Protocol (UDP).

- **TCP:** TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- **UDP:** UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a

TCP connection is not desired, or when the applications or upper layer protocols provide reliable delivery.

The Transport Layer encompasses the responsibilities of the OSI Transport Layer and some of the responsibilities of the OSI Session Layer.

Internet Layer (Layer 2)

The Internet layer handles the transfer of information across multiple networks through the use of gateways and routers. The Internet layer corresponds to the part of the OSI network layer that is concerned with the transfer of packets between machines that are connected to different networks. It deals with the routing of packets across these networks as well as with the control of congestion. A key aspect of the Internet layer is the definition of globally unique addresses for machines that are attached to the Internet.

The Internet layer provides a single service namely, best-effort connectionless packet transfer. IP packets are exchanged between routers without a connection setup; the packets are routed independently and so they may traverse different paths. For this reason, IP packets are also called datagrams. The connectionless approach makes the system robust; that is, if failures occur in the network, the packets are routed around the points of failure; hence, there is no need to set up connections. The gateways that interconnect the intermediate networks may discard packets when congestion occurs. The responsibility for recovery from these losses is passed on to the Transport Layer.

The core protocols of the Internet Layer are IP, ARP, ICMP, and IGMP.

- **The Internet Protocol (IP)** is a routable protocol responsible for IP addressing and the fragmentation and reassembly of packets.
- **The Address Resolution Protocol (ARP)** is responsible for the resolution of the Internet Layer address to the Network Interface Layer address, such as a hardware address.
- **The Internet Control Message Protocol (ICMP)** is responsible for providing diagnostic functions and reporting errors or conditions regarding the delivery of IP packets.
- **The Internet Group Management Protocol (IGMP)** is responsible for the management of IP multicast groups.

Link/Physical Layer (Layer 1)

The Link/Physical Layer (also called the Network Access Layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets of the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. This includes LAN technologies such as Ethernet or Token Ring and WAN technologies such as X.25 or Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface Layer encompasses the Data Link and Physical layers of the OSI Model. **Note,** that the Internet Layer does not take advantage of sequencing and acknowledgement services that may be present in the Data Link Layer. An unreliable Network Interface Layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgement of packets is the responsibility of the Transport Layer.

Merits of TCP/IP model:

- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports a number of routing protocols.
- Can be used to establish a connection between two computers.

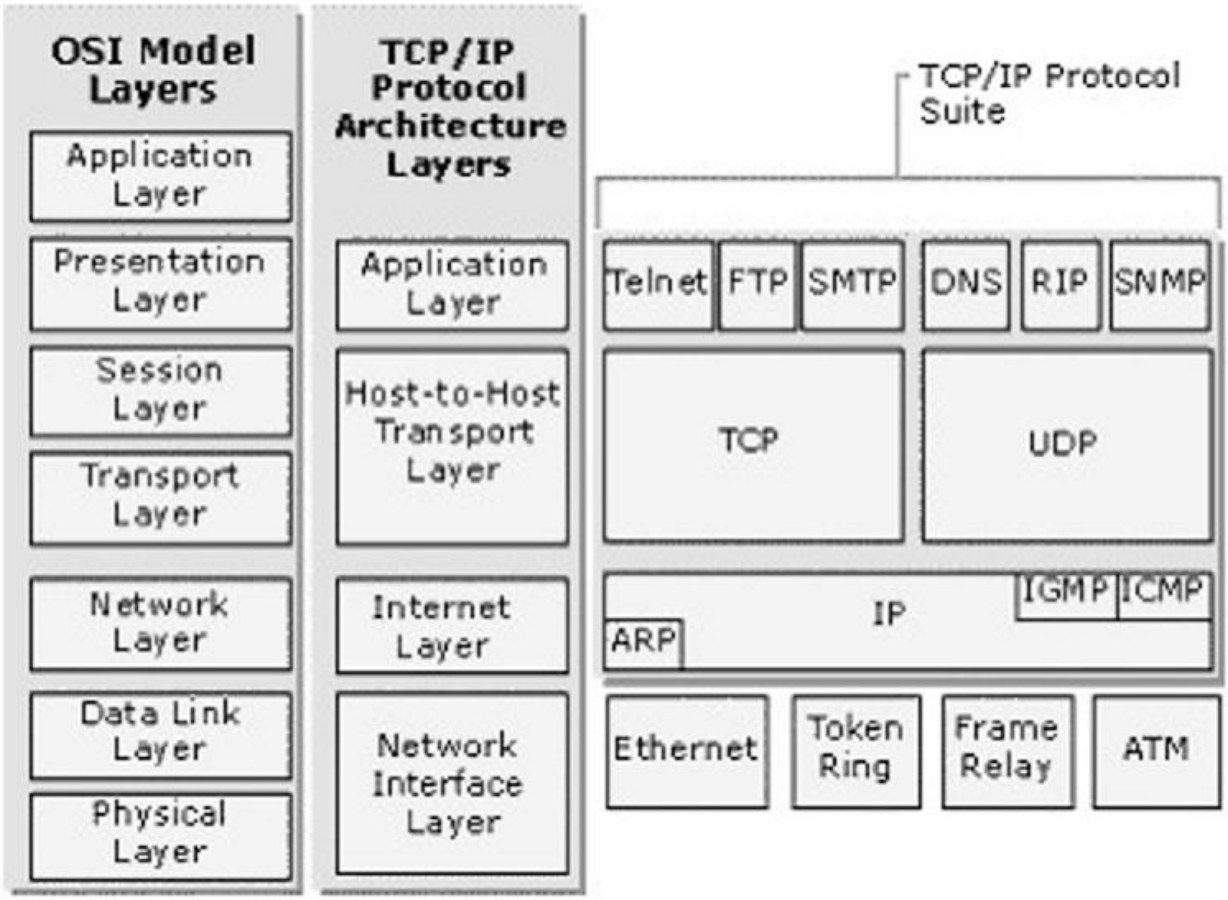
Demerits of TCP/IP

- In this, the transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference model

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol

8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

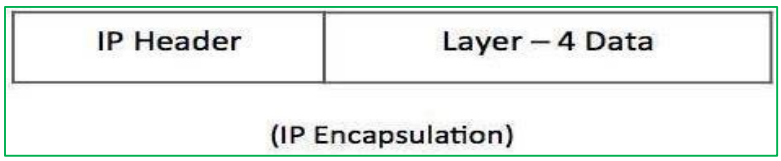


Internet Protocol Version 4 (IPv4)

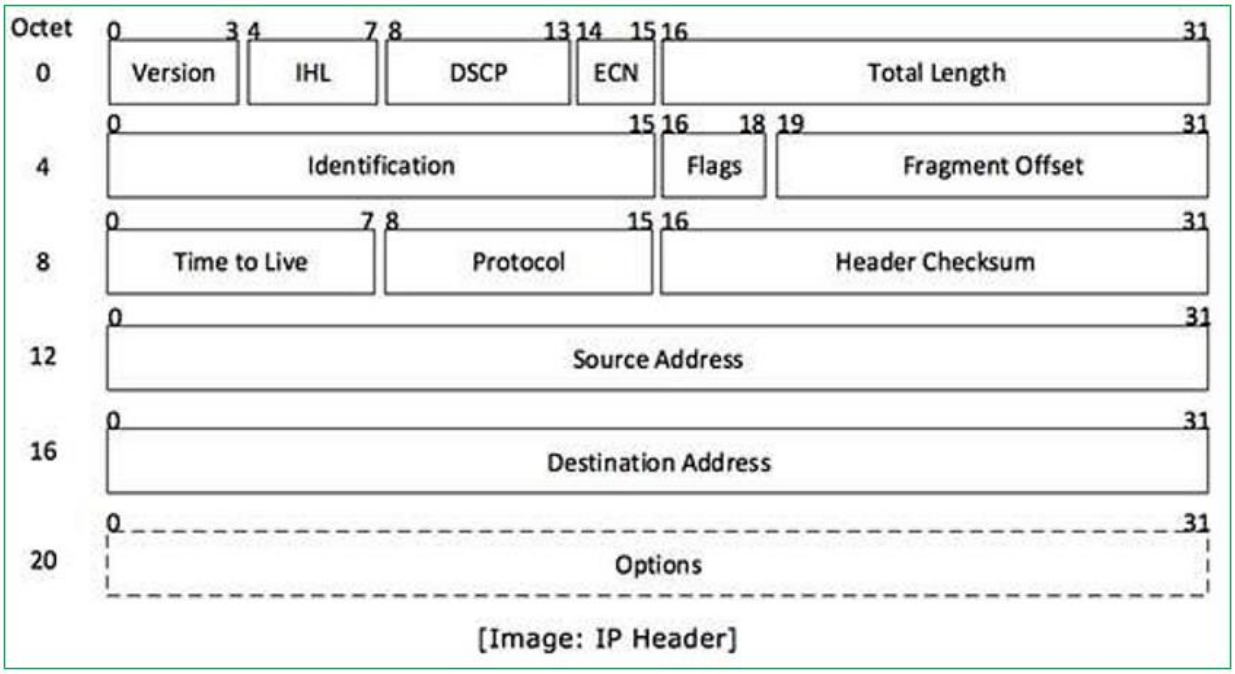
Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among 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.

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



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



IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).

- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. To identify original IP packet they belong to.
- **Flags:** As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address:** 32-bit address of the Sender (or source) of the packet.
- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPv4 - Addressing:

IPv4 supports three different types of addressing modes:

1. Unicast Addressing Mode:

Unicast is a type of communication where data is sent from one computer to another computer.

In Unicast type of communication, there is only one sender, and one receiver. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server.

Example:

- Browsing a website. (Webserver is the sender and your computer is the receiver.)
- Downloading a file from a FTP Server. (FTP Server is the sender and your computer is the receiver.)

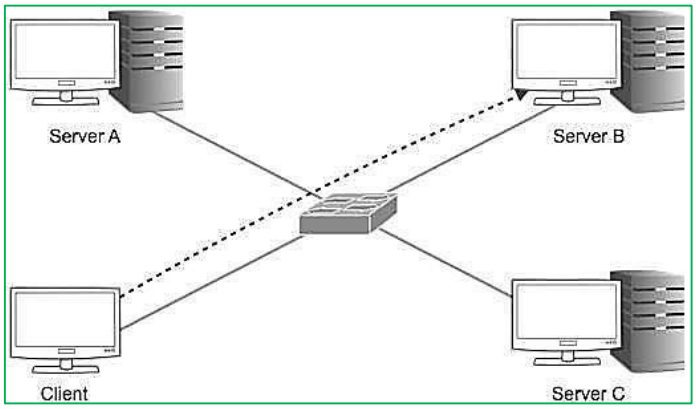


Fig: Unicast Addressing Mode

2. Broadcast Addressing Mode:

Broadcast is a type of communication where data is sent from one computer once and a copy of that data will be forwarded to all the devices. In Broadcast, there is only one sender and the data is sent only once. But the Broadcast data is delivered to all connected devices. Switches by design will forward the broadcast traffic and Routers by design will drop the broadcast traffic. In other words, Routers will not allow a broadcast from one LAN to cross the Router and reach another Network Segment. The primary function of a Router is to divide a big Broadcast domain to multiple smaller Broadcast domain.

Example:

- ARP Request message
- DHCP DISCOVER Message

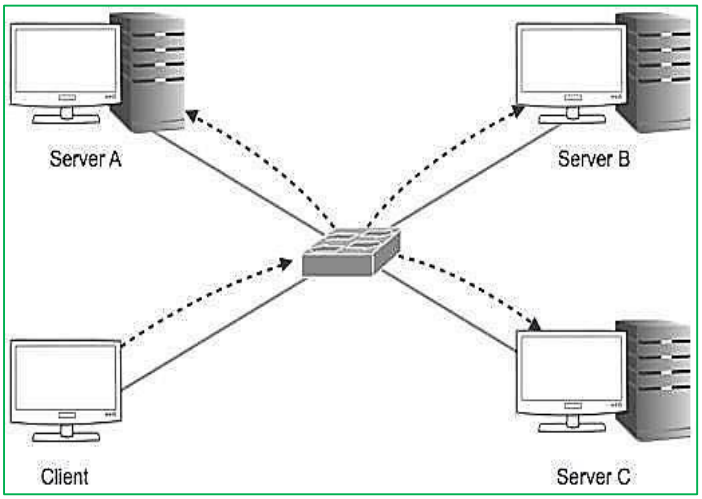


Fig: Broadcast Addressing Mode

3. Multicast Addressing Mode:

Multicast is a type of communication where multicast traffic addressed for a group of devices on the network. IP multicast traffic are sent to a group and only members of that group receive and/or process the Multicast traffic. Devices which are interested in a particular Multicast traffic must join to that Multicast group to receive the traffic. IP Multicast Groups are identified by Multicast IP Addresses (IPv4 Class D Addresses). In Multicast, the sender transmit only one copy of data and it is delivered and/or processed to many devices (Not as delivered and processed by all devices as in Broadcast) who are interested in that traffic.

Example:

- Multicast Windows Deployment Services (WDS) OS deployment traffic
- IP TV etc.

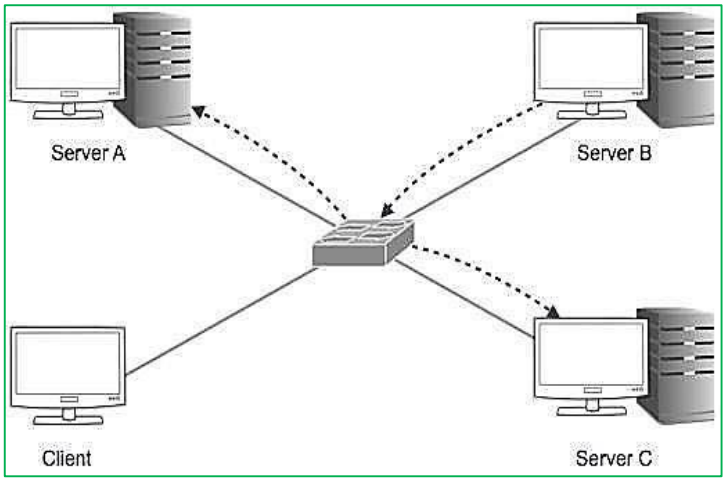


Fig: Multicast Addressing Mode

Hierarchical Addressing Scheme:

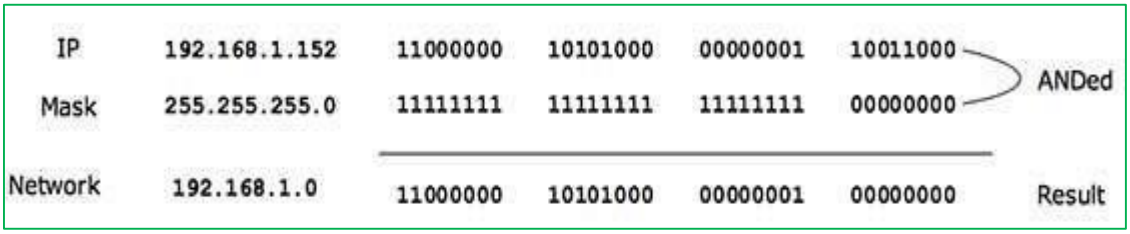
IPv4 uses hierarchical addressing scheme. An IP address, which is 32-bits in length, is divided into two or three parts as depicted:

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

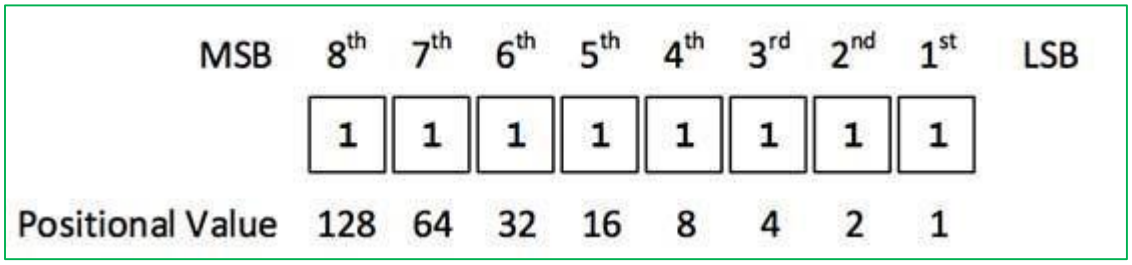
:



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:

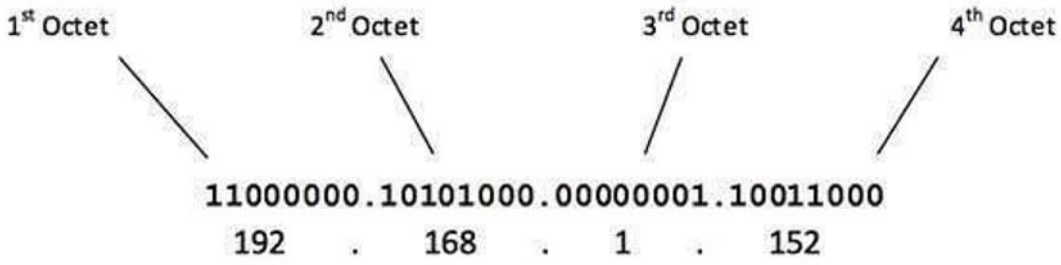
128	64	32	16	8	4	2	1	Value
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
0	0	0	0	0	1	1	1	7
0	0	0	0	1	0	0	0	8
0	0	0	0	1	0	0	1	9
0	0	0	0	1	0	1	0	10
0	0	0	1	0	0	0	0	16
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	1	0	0	100
0	1	1	1	1	1	1	1	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.

1. 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

2. 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

3. Class C Address:

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

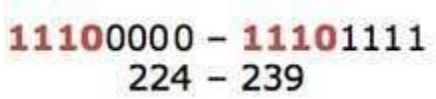
11000000 – 11011111
192 – 223

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

4. 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 rage 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.

5. 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.

1. 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 sub-netting. Given below is a list of all possible combination of Class A subnets: In case of sub-netting 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.

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

2. 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 sub-netted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B sub-netting:

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

3. 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 sub-netted 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

Variable Length Subnet Mask:

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 selfaddress, 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.

Introduction of IPv6:

Internet Protocol version 6, is a new addressing protocol designed to incorporate whole sort of requirement of future internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on Network Layer (Layer-3). Along with its offering of enormous amount of logical address space, this protocol has ample of features which addresses today's shortcoming of IPv4.

Why new IP version?

So far, IPv4 has proven itself as a robust routable addressing protocol and has served human being for decades on its best-effort-delivery mechanism. It was designed in early 80's and did not get any major change afterward. At the time of its birth, Internet was limited only to a few Universities for their research and to Department of Defense. IPv4 is 32 bits long which offers around

4,294,967,296 (2^{32}) addresses. This address space was considered more than enough that time. Given below are major points which played key role in birth of IPv6:

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement of protocol which can satisfy the need of future Internet addresses which are expected to grow in an unexpected manner.
- Using features such as NAT, has made the Internet discontiguous i.e. one part which belongs to intranet, primarily uses private IP addresses; which has to go through number of mechanism to reach the other part, the Internet, which is on public IP addresses.
- IPv4 on its own does not provide any security feature which is vulnerable as data on Internet, which is a public domain, is never safe. Data has to be encrypted with some other security application before being sent on Internet.
- Data prioritization in IPv4 is not up to date. Though IPv4 has few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. There exists no technique which can configure a device to have globally unique IP address.

Why not IPv5?

Till date, Internet Protocol has been recognized has IPv4 only. Version 0 to 3 were used while the protocol was itself under development and experimental process. So, we can assume lots of background activities remain active before putting a protocol into production. Similarly, protocol version 5 was used while experimenting with stream protocol for internet. It is known to us as Internet Stream Protocol which used Internet Protocol number 5 to encapsulate its datagram. Though it was never brought into public use, but it was already used.

Here is a table of IP version and their use:

Decimal	Keyword	Version
0-1		Reserved
2-3		Unassigned
4	IP	Internet Protocol
5	ST	ST Datagram mode
6	IPv6	Internet Protocol version 6
7	TP/IX	TP/IX: The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TUBA
10-14		Unassigned
15		Reserved

Brief History:

After IPv4's development in early 80s, the available IPv4 address pool begun to shrink rapidly as the demand of addresses exponentially increased with Internet. Taking pre-cognizance of situation

that might arise IETF, in 1994, initiated the development of an addressing protocol to replace IPv4. The progress of IPv6 can be tracked by means of RFC published:

- 1998 – RFC 2460 – Basic Protocol
- 2003 – RFC 2553 – Basic Socket API
- 2003 – RFC 3315 – DHCPv6
- 2004 – RFC 3775 – Mobile IPv6
- 2004 – RFC 3697 – Flow Label Specification
- 2006 – RFC 4291 – Address architecture (revision)
- 2006 – RFC 4294 – Node requirement

June 06, 2012 some of Internet giants chose to put their Servers on IPv6. Presently they are using Dual Stack mechanism to implement IPv6 parallel with IPv4.

IPv6 Header:

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

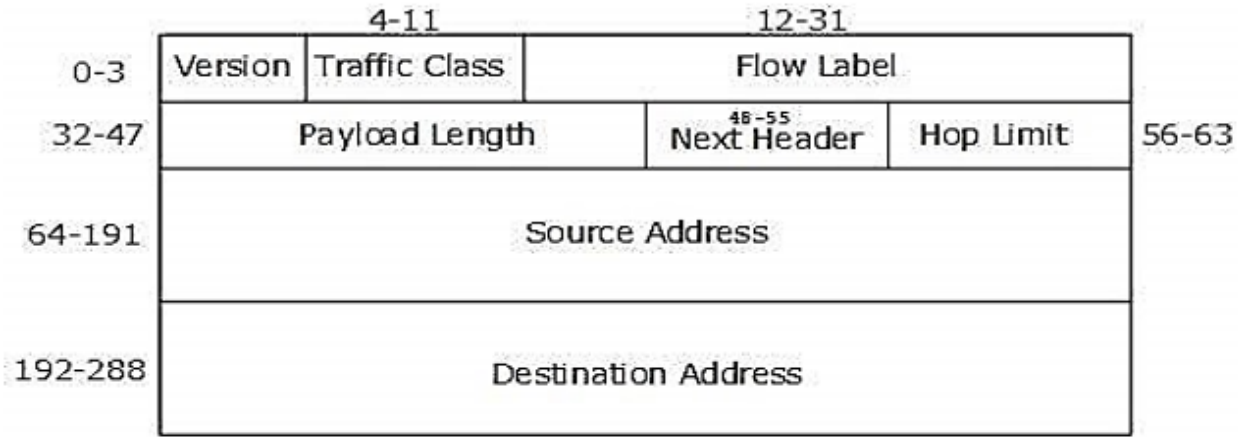


Fig: IPv6 Fixed Header

IPv6 fixed header is 40 bytes long and contains the following information.

S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.

2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

Features:

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

- **Larger Address Space:**

In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1038 different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

- **Simplified Header:**

IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 providing the fact the IPv6 address is four times longer.

- **End-to-end Connectivity:**

Every system now has unique IP address and can traverse through the internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other host on the Internet, with some limitations involved like Firewall, Organization's policies, etc.

- **Auto-configuration:**

IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way absence of a DHCP server does not put halt on inter segment communication.

- **Faster Forwarding/Routing:**

Simplified header puts all unnecessary information at the end of the header. All information in first part of the header are adequate for a Router to take routing decision thus making routing decision as quickly as looking at the mandatory header.

- **IPSec:**

Initially it was decided for IPv6 to must have IPSec security, making it more secure than IPv4. This feature has now been made optional.

- **No Broadcast:**

Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any Broadcast support anymore left with it. It uses multicast to communicate with multiple hosts.

- **Anycast Support:**

This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, sends the packet to the nearest destination.

- **Mobility:**

IPv6 was designed keeping mobility feature in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with same IP address. IPv6 mobility feature takes advantage of auto IP configuration and Extension headers.

- **Enhanced Priority support:**

Where IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it.

In IPv6, Traffic class and Flow label are used to tell underlying routers how to efficiently process the packet and route it.

- **Smooth Transition:**

Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This assures that mechanism to save IP addresses such as NAT is not required. So devices can send/receive data between each other, for example VoIP and/or any streaming media can be used much efficiently.

Other fact is, the header is less loaded so routers can make forwarding decision and forward them as quickly as they arrive.

- **Extensibility:**

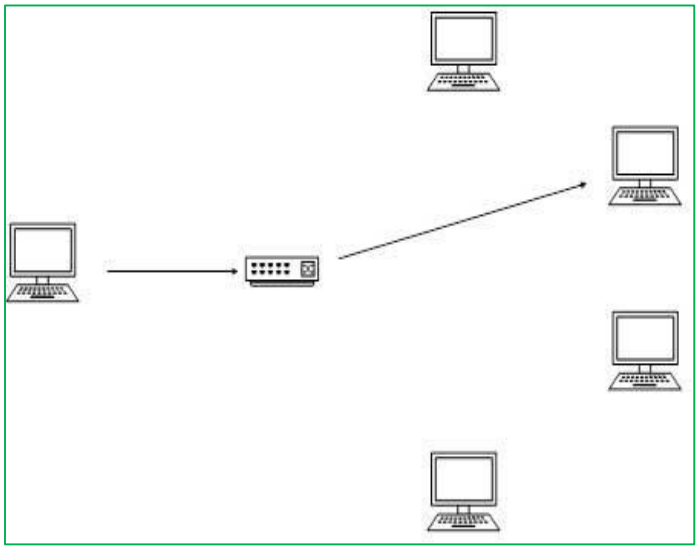
One of the major advantage of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options whereas options in IPv6 can be as much as the size of IPv6 packet itself.

Addressing Modes:

In computer networking, addressing mode refers to the mechanism how we address a host on the network. IPv6 offers several types of modes by which a single host can be addressed, more than one host can be addressed at once or the host at closest distance can be addressed.

1. Unicast:

In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment. A network switch or router when receives a unicast IP packet, destined to single host, sends out to one of its outgoing interface which connects to that particular host.



[*Image: Unicast Messaging*]

2. Multicast:

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All hosts interested in that multicast information, need to join that multicast group first. All interfaces which have joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.

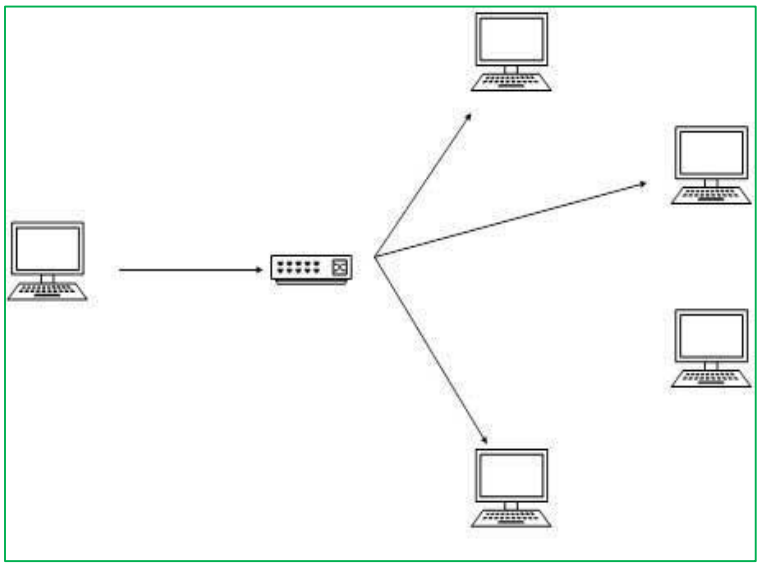


Image: Multicast Messaging

3. Anycast:

IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the

host closest to the Sender, in terms of Routing cost.

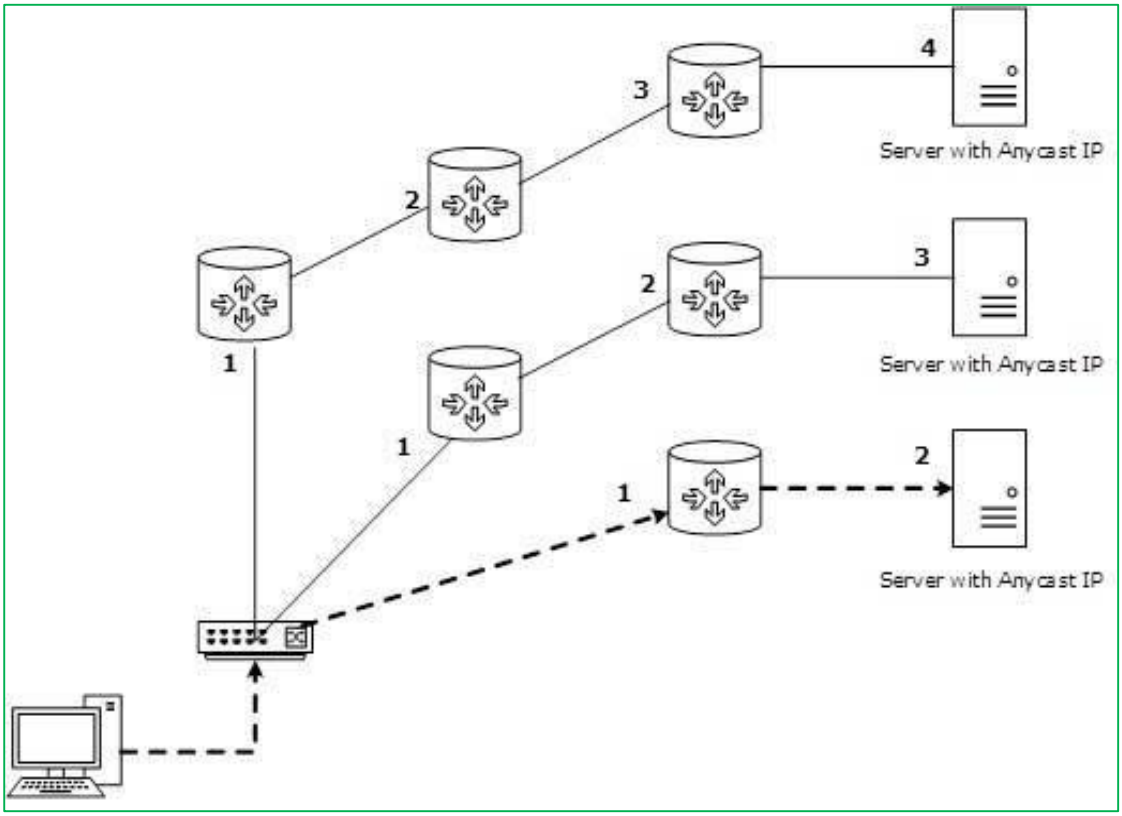


Image: Anycast Messaging

Let's take an example of TutorialPoints.com Web Servers, located in all continents. Assume that all Web Servers are assigned single IPv6 Anycast IP Address. Now when a user from Europe wants to reach TutorialsPoint.com the DNS points to the server which is physically located in

Europe itself. If a user from India tries to reach Tutorialspoint.com, the DNS will then point to Web Server physically located in Asia only. Nearest or Closest terms are used in terms of Routing Cost.

In the above picture, when a client computer tries to reach a Server, the request is forwarded to the Server with lowest Routing Cost.

Address Types:

Hexadecimal Number System:

Before introducing IPv6 Address format, we shall look into Hexadecimal Number System.

Hexadecimal is positional number system which uses radix (base) of 16. To represent the values in readable format, this system uses 0-9 symbols to represent values from zero to nine and A-F symbol to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.

Address Structure:

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbol.

For example, the below is 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000110100 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. These rules are:

Rule: 1 Discard leading Zero (es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule: 2 If two of more blocks contains consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

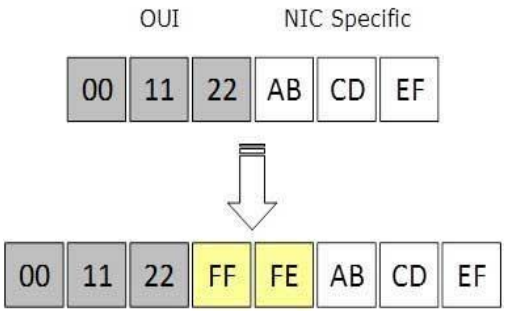
2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address they can be shrink down to single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

Interface ID:

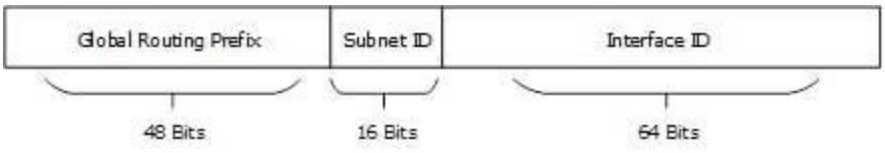
IPv6 has three different type of Unicast Address scheme. The second half of the address (last 64 bits) is always used for Interface ID. MAC address of a system is composed of 48-bits and represented in Hexadecimal. MAC address is considered to be uniquely assigned worldwide. Interface ID takes advantage of this uniqueness of MAC addresses. A host can auto-configure its Interface ID by using IEEE's Extended Unique Identifier (EUI-64) format. First, a Host divides its own MAC address into two 24-bits halves. Then 16-bit Hex value 0xFFFE is sandwiched into those two halves of MAC address, resulting in 64-bit Interface ID.



[*Image: EUI-64 Interface ID*]

Global Unicast Address:

This address type is equivalent to IPv4's public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.



[*Image: Global Unicast Address*]

Global Routing Prefix: The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific Autonomous System. Three most significant bits of Global Routing Prefix is always set to 001.

Link-Local Address:

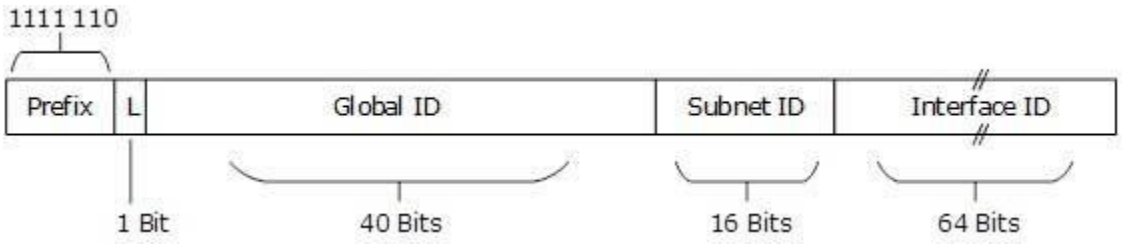
Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. First 16 bits of Link-Local address is always set to 1111 1110 1000 0000 (FE80). Next 48bits are set to 0, thus:

[*Image: Link-Local Address*]

Link-Local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable so a Router never forwards these addresses outside the link.

Unique-Local Address:

This type of IPv6 address which is though globally unique, but it should be used in local communication. This address has second half of Interface ID and first half is divided among Prefix, Local Bit, Global ID and Subnet ID.



[*Image: Unique-Local Address*]

Prefix is always set to 1111 110. L bit, which is set to 1 if the address is locally assigned. So far the meaning of L bit to 0 is not defined. Therefore, Unique Local IPv6 address always starts with 'FD'.

Difference between IPv4 and IPv6:

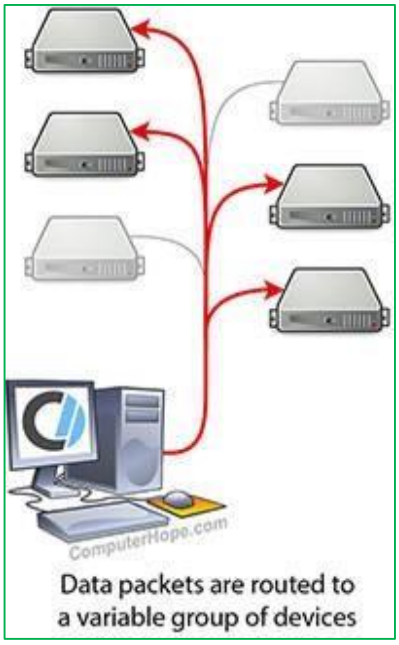
IPv4	IPv6
1. IPv4 addresses are 32 bit length.	1. IPv6 addresses are 128 bit length.
2. IPv4 addresses are binary numbers represented in decimals.	2. IPv6 addresses are binary numbers represented in hexadecimals.
3. IPSec support is only optional.	3. Inbuilt IPSec support.
4. Fragmentation is done by sender and forwarding routers.	4. Fragmentation is done only by sender.
5. No packet flow identification.	5. Packet flow identification is available within the IPv6 header using the Flow Label field.
6. Checksum field is available in IPv4 header	6. No checksum field in IPv6 header.
7. Options fields are available in IPv4 header.	7. No option fields, but IPv6 Extension headers are available.
8. Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	8. Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
9. Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	9. IGMP is replaced with Multicast Listener Discovery (MLD) messages.
10. Broadcast messages are available.	10. Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.

11. Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required configure IPv4 addresses.	11. Auto-configuration of addresses is available.

Internet Multicasting:

Multicasting is similar to broadcasting, but only transmits information to specific users. It is used to efficiently transmit streaming media and other types of data to multiple users at one time.

The simple way to send data to multiple users simultaneously is to transmit individual copies of the data to each user. However, this is highly inefficient, since multiple copies of the same data are sent from the source through one or more networks. Multicasting enables a single transmission to be split up among multiple users, significantly reducing the required bandwidth.



Multicasts that take place over the Internet are known as IP multicasts, since they use the Internet protocol (IP) to transmit data. IP multicasts create "multicast trees," which allow a single transmission to branch out to individual users. These branches are created at Internet routers wherever necessary. For example, if five users from five different countries requested access to the same stream, branches would be created close the original source. If five users from the same city requested access to the same stream, the branches would be created close to users.

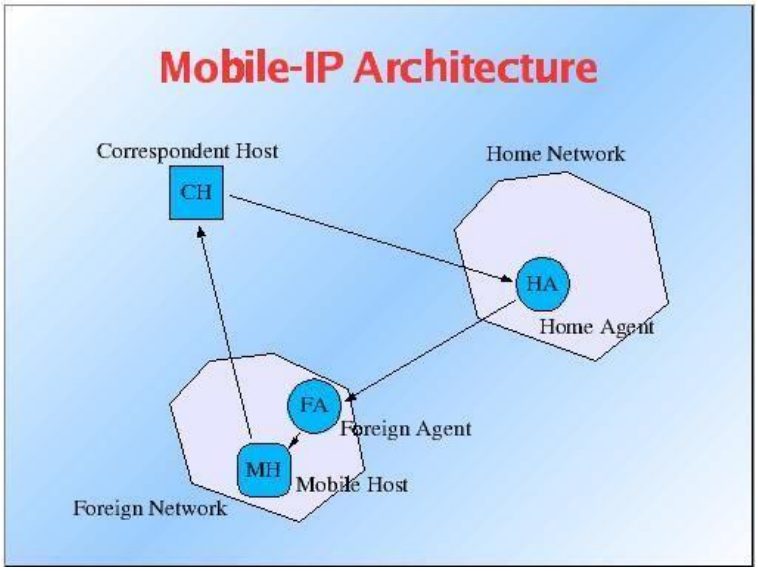
IP multicasting works by combining two other protocols with the Internet protocol. One is the Internet Group Management Protocol (IGMP), which allows users or client systems use to request access to a stream. The other is Protocol Independent Multicast (PIM), which is used by network routers to create multicast trees. When a router receives a request to join a stream via IGMP, it uses PIM to route the data stream to the appropriate system.

Multicasting has several different applications. It is commonly used for streaming media over the Internet, such as live TV and Internet radio. It also supports video conferencing and webcasts. Multicasting can also be used to send other types of data over the Internet, such as news, stock quotes, and even digital copies of software. Whatever the application, multicasting helps reduce Internet bandwidth usage by providing an efficient way of sending data to multiple users.

Mobile IP:

Mobile IP is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining their permanent IP address. Defined in Request for Comments (RFC) 2002, Mobile IP is an enhancement of the Internet Protocol (IP) that adds mechanisms for forwarding Internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

In traditional IP routing, IP addresses represent a topology. Routing mechanisms rely on the assumption that each network node will always have the same point of attachment to the Internet, and that each node's IP address identifies the network link where it is connected. Core Internet routers look at the IP address prefix, which identifies a device's network. At the network level, routers look at the next few bits to identify the appropriate subnet. Finally, at the subnet level, routers look at the bits identifying a particular device. In this routing scheme, if you disconnect a mobile device from the Internet and want to reconnect through a different subnet, you have to configure the device with a new IP address, and the appropriate netmask and default router. Otherwise, routing protocols have no means of delivering packets because the device's IP address doesn't contain the necessary information about the current point of attachment to the Internet.



All the variations of Mobile IP assign each mobile node a permanent home address on its home network and a care-of address that identifies the current location of the device within a network and its subnets. Each time a user moves the device to a different network, it acquires a new careof address. A mobility agent on the home network associates each permanent address with its care-of address. The mobile node sends the home agent a binding update each time it changes its care-of address using Internet Control Message Protocol (ICMP). In Mobile IPv4, traffic for the mobile node is sent to the home network but is intercepted by the home agent and forwarded via tunneling mechanisms to the appropriate care-of address. Foreign agents on the visited network help to forward datagrams. Mobile IPv6 was developed to minimize the necessity for tunneling and to include mechanisms that make foreign agents unnecessary.

Enhancements to the Mobile IP standard, such as Mobile IPv6 and Hierarchical Mobile IPv6 (HMIPv6), were developed to advance mobile communications by making the processes involved less cumbersome. Although the North American mobile trend is not moving as quickly as some other markets, the growing adoption of mobile communications elsewhere is likely to drive acceptance globally. According to a Gartner Group report, by 2004 40% of all business-to business (B2B) transactions outside of North America will be initiated by mobile devices.