gradeup

Network Layers Part - 2

Prep Smart. Stay Safe. go Gradeup

gradeup.co

Network Layer Part-2

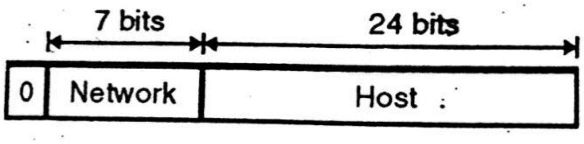
Content:

IP ADDRESSES CLASSES:

- The IP addresses are classified into 5 types as follows:
  1. Class A
  2. Class B
  3. Class C
  4. Class D
  5. Class E

CLASS 'A' ADDRESSES

- The format used for IP address are as shown in below figure. The IP address for class A networks is shown in below figure.

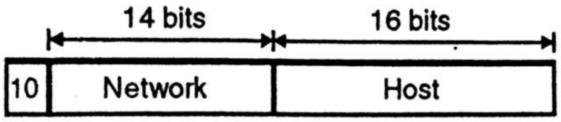


- The network field is 7 bit long as shown in above figure and the host field is of 24 bit length. So the network field can have numbers between 1 to 126.

- But the host numbers will range from 0.0.0.0 to 127.255.255.255
- Thus in class A, there can be 126 types of networks and 17 million hosts.
- The “0” in the first field identifies that it is a class A networks address.

CLASS ‘B’ FORMAT

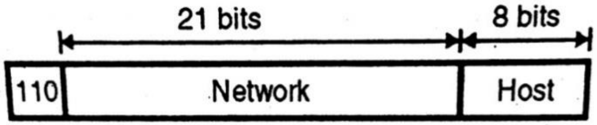
- The class B address format is shown in below figure.
- The first two fields identify the networks, and the number in the first field must be in the range 128 - 191.



- Class B networks are large. Host number 0.0 and 255.255 are reserved, so there can be upto 65.534 hosts in a class B network. Most of 16,382 class B addresses have been allocated. The first block covers address from 128.0.0.0 to 128.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255. **Example:** 128.89.0.26, for host 0.26 on net 128.89.

CLASS C FORMAT

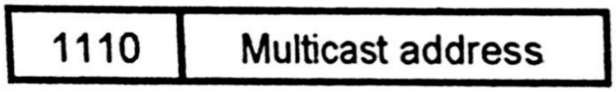
- The class C address format is shown in below figure.



- The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255

CLASS D FORMAT

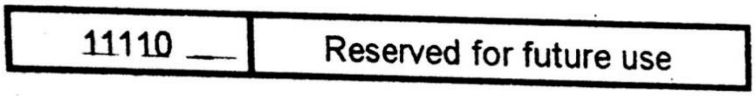
- The class D address format is shown in below figure.



- The class format allow for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

CLASS E ADDRESS FORMAT

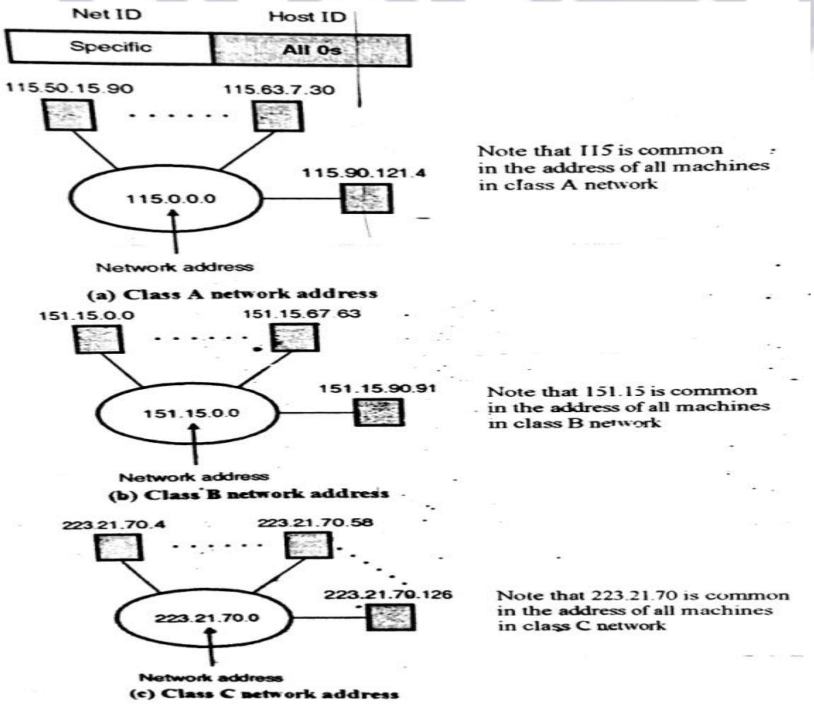
- Below figure shows the address format for a class E address. This address beings with 11110 which shows that it is reserved for the future use



- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4-bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IP address is 255.255.255.255.

NETWORKS ADDRESSES

- The network address is an address that defines the network itself. It cannot be assigned to a host. Below figure shows the example of network addresses for different classes



Note that 115 is common in the address of all machines in class A network

(a) Class A network address

Note that 151.15 is common in the address of all machines in class B network

(b) Class B network address

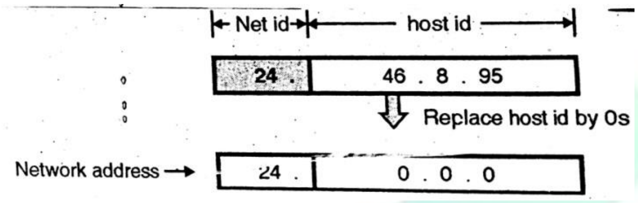
Note that 223.21.70 is common in the address of all machines in class C network

(c) Class C network address

EXAMPLE: For the address 24.48.8.95 identify the type of network and find the network address.

Solution:

- Examine the first byte. Its value is 24 i.e. it is between 0 and 127. So it is a class A network.
- So only the first byte defines the Net id. So we can find the network address by replacing the host id with 0's
- The process of obtaining the network address is shown in below figure.

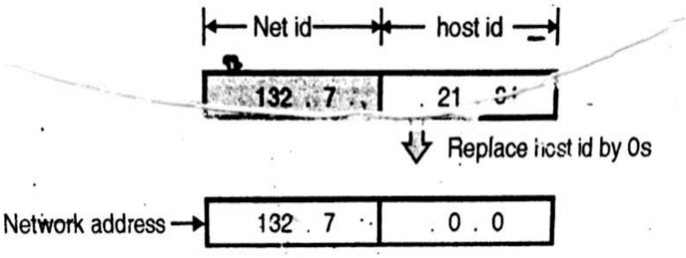


So the network address is 24.0.0.0

EXAMPLE: For the address 132.7.21.84 find the type of network and the network address.

Solution:

- Examine the first byte. It is 132 i.e. between 128 and 192. So it is a class B networks.
- So the first two bytes define the net id. Replace the host id with 0's to get the network address as shown in below figure.



So the network address is 132.7.0.0.

What is the difference between net id and network address?

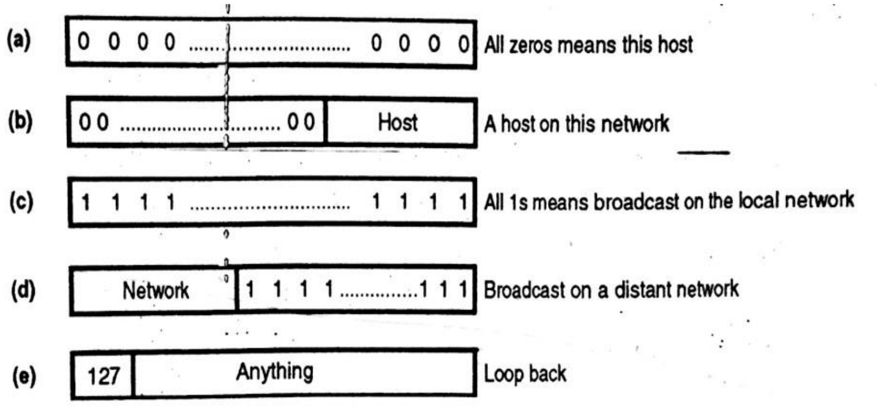
The network address is different from a net id. A network address has both net id and host id, with 0's for the host id.

Where to use the network address?

The network address is used to route the packets to the desired location.

SPECIAL IP ADDRESSES

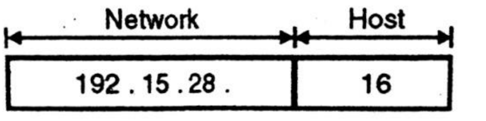
Below figure shows some special IP addresses.



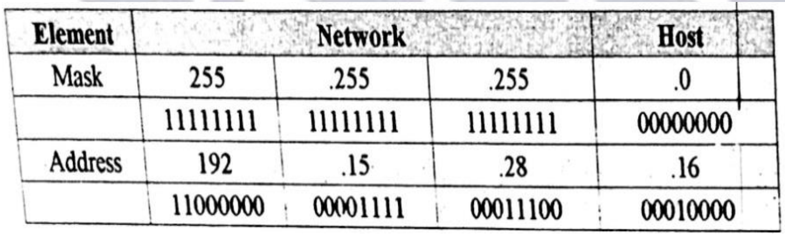
- ➢ All zeros means this host or this network and all 1s means broadcast address to all hosts on the indicated network.
- ➢ The IP address 0.0.0.0 is used by the hosts when they are being booted but not used afterward.
- ➢ The IP addresses with 0 as the network number refer to their own network without knowing its number as above figure.
- ➢ The address having all ones is used for broadcasting on the local network such as a LAN as shown in above figure.
- ➢ Refer above figure. This is an address with proper network number and all 1s in the host field. This address allow machines to send broadcast packets to distant LANs anywhere in the Internet.
- ➢ If the address is "127. Anything" as shown in above diagram then it is a reserved address loopback testing. This feature is also used for debugging network software.

ADDRESS MASKS (DEFAULT MASKS)

- An address mask determines which portion of an IP address identifies the network and which portion identifies the host.
- Like the IP address, the mask is represented by four octets. (An octet is an 8-bit binary number equivalent to a decimal number in the range 0 - 255).
- If a given bit of the mask is 1, the corresponding bit of the IP address is in the network portion of the address and if a given bit of the mask is 0, the corresponding bit of the IP address is in the host portion.
- For example consider a class C address 192.15.28.16. This is shown in below figure. Note that 192.15.28 corresponds to the network part and 16 corresponds to the host part.

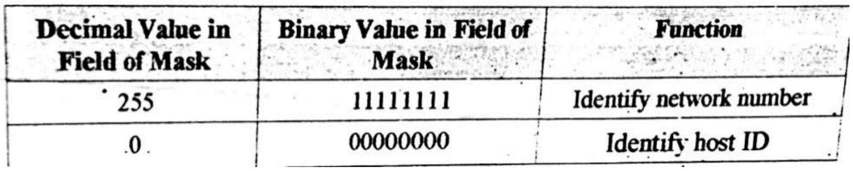


- So as to differentiate the network and host parts. We have to use a mask 255.255.255.0.
- Below table shows the mask 255.255.255.0 in both decimal and binary form, aligned with the class C address 192.15.28.16, also in both decimal and binary form:



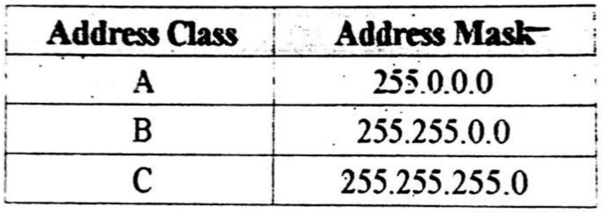
Element	Network			Host
Mask	255	.255	.255	.0
	11111111	11111111	11111111	00000000
Address	192	.15	.28	.16
	11000000	00001111	00011100	00010000

- If a field of the network address is entirely used for the network number, the corresponding field of the mask has the decimal value 255 (binary 11111111), and if a n address field is entirely used for the host ID, the corresponding field of the mask has the decimal value 0.



Decimal Value in Field of Mask	Binary Value in Field of Mask	Function
255	11111111	Identify network number
.0	00000000	Identify host ID

- Accordingly, the address masks for the three network classes described above are as shown in below table. These masks are also called as default masks.



Address Class	Address Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Which IP protocol version is being used currently?

- The network protocol in the Internet is currently IPv4. It was first introduced in 1970's
- After that the world of data communication has grown beyond imaginations. Even though IPv4 is a well designed protocol, it has some limitations.

LIMITATION OF IPv4

- The most obvious limitation of IPv4 is its address field. IP relies on network layer addresses to identify end-point on networks, and each networked device has a unique IP address.
- IPv4 uses a 32-bit addressing scheme, which gives it 4 billion possible addresses. With the proliferation of networked devices including PCs, cell phones, wireless devices, etc. unique IP addresses are becoming scarce, and the world could theoretically run out of IP addresses.
- If a network has slightly more number of hosts than a particular class, then it needs either two IP addresses of that class or the next class of IP address. For example, let us say a network has 300 hosts, this network needs either a signal class B IP address or two class C IP addresses. If class B address is allocated to this network, as the number hosts that can be defined in a class B network is (2 ^ 16 - 2), a large number of host IP addresses are wasted.
- If two class C IP addresses are allocated, as the number of networks that can be defined using a class C address is only (2 ^ 21), the number of available class C networks will quickly exhaust. Because of the above two reasons, a lot

of IP address are wasted and also the available IP address space is rapidly reduced.

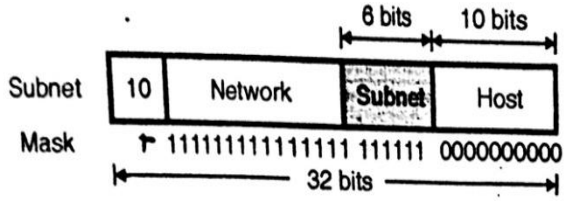
- Other identified limitations of the IPv4 prptocol are: complex host and router configuration, non-hierarchical addressing, difficult in re-numbering addresses, large routing tables, non-trival implementations in providing security, QoS (Quality of service), mobility and multi-homing, multicasting etc.
- To overcome these problems the internet protocol version 6 (IPv6) which is also known as internet protocol, next generation (IPng, was proposed)
- In IPv6 the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
- The format and length of the IP addresses has been changed and the packet format also is changed.

SUBNETTING IN IP

All hosts in a network must have same network number. But this property of IP addressing can be problematic as the network size increases.

- For example a company initially may have only one LAN but as the time passes by it might end up with many LANs each one having its own router and each one with its own class C network number.
- With everything in the number of distinct local networks, their management because a problem.
- Everything a new network gets installed, the system administration has to contact NIC to get a new network number and then this number is to be announced worldwide.
- Another problem is that if a machine is to be moved from one LAN to the other, then its IP address needs to be changed. This will require modification in its configuration files and its modified IP number needs to be announced to the world.
- The solution of this problem is that, the network is split into several smaller networks internally but it acts like a single network to the outside world.

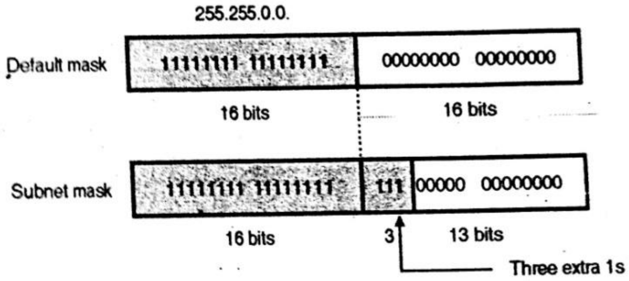
- The smaller parts of a network are called as subnet.
- Now continue with the same-example taken at the beginning of this subsection. The growing company should start up with class B address instead of class C address and it can number the hosts from 1 to 254.
- When a second LAN is to be installed it can split the 16 bit host number into a 6-bit subnet number and 10 bit host number as shown in below figure.



- Due to the split it is possible to connect 62 LANs (0 and - 1 are reserved) and each one can contain up to 1022 hosts.
- Outside the network, the sub netting is not visible. So even if a new subnet is created it is not necessary to contact NIC or change any database.

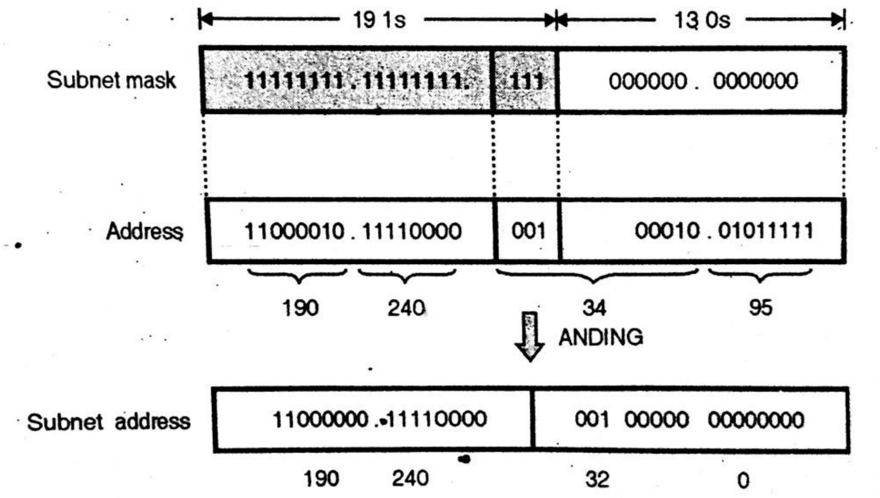
SUBNET MASK

- The number of 1's in the subnet mask is more than the number of 1s in the corresponding default mask.
- In subnet mask we change some of the leftmost 0s in the default mask to make a subnet mask.
- Below figure shows the difference between a class B default mask and subnet mask for the same block.



EXAMPLE: a router inside an, organization receives the same packet with a destination address 190.240.34.95. if the subnet mask is /19 (first 19 bit are 1s and following bit are 0s). Find the subnet address.

Solution: To find the subnet address, AND the destination address with the subnet mask as shown in below figure.



Thus the subnet address is 190.240.32.0

SUPERNETTING

- The class A and B addresses are almost depleted. But class C addresses are still available.
- But the size of class C address with a maximum number of 256 addresses does not satisfy the needs of an organization. More addresses will be required.
- The solution to this problem is supernetting.
- In super netting an organization is combines several class C blocks to create a large range of addresses i.e. several networks are combined to create supernetwork.
- By doing this organization can apply for a set of class C blocks instead of just one.

CLASSLESS ADDRESSING

- Even though the number of actual device connected to Internet is much less than 4 billion, the address depletion has taken place due to flows in the classful addressing scheme.

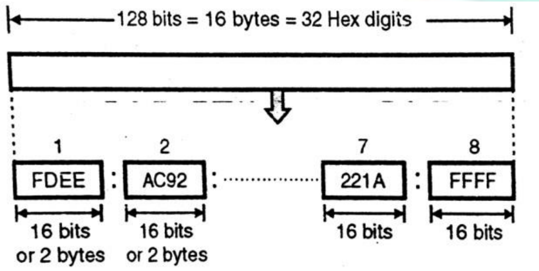
- We have run out of class A and B addresses. To overcome these problems, the classless addressing is now being tried out.
- In the classless addressing there are no classes but the addresses are still generated in blocks.

IPv6

It is the next generation Internet Protocol designed as a successor to the IPv4. IPv6 was designed to enable high-performance, scalable Internet. This was achieved by overcome marry of the weakness of IPv4 protocol and by adding several new features.

IPv6

An IPv6 address consists of 16 bytes (octets) i.e. it is 128 bits long as shown in below figure.

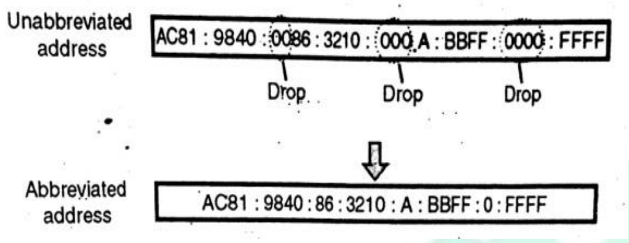


HEXADECIMAL COLON NOTATION

- IPv6 uses a special notation called hexadecimal colon notation. In this, the 128 bits are divided into 8 sections, each one is 2 bytes long.
- 2 bytes correspond 16 bits. So in hexadecimal notation will require four hexadecimal digits.
- Hence the IPv6 address consists of 32 hex digits and every group of 4 digits is separated by a colon as shown in above figure.
- IPv6 uses 128-bit addresses. Only about 15% of the address space is initially allocated, the remaining 85% being reserved for future use.
- This remainder may by used in the future for expanding the address spaces of existing address type or for totally new uses.

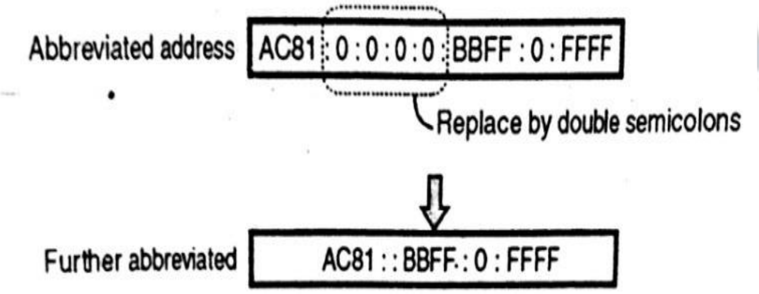
ABBREVIATION

- The IPv6 address, even in hexadecimal format is very long. But in this address there are many of the zero digits in it.
- In such a case, we can abbreviate the address.Leading zeros of a section (four digits between two colons) can be omitted.
- Note that only the leading zeros can be dropped but the trailing zeros cannot dropped. This is illustrated in below figure.


Unabbreviated address
AC81 : 9840 : 0086 : 3210 : 000A : BBFF : 0000 : FFFF
Drop
Drop
Drop
Abbreviated address
AC81 : 9840 : 86 : 3210 : A : BBFF : 0 : FFFF

FURTHER ABBREVIATION

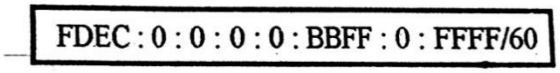
- Further abbreviation are possible if there are consecutive section consisting of only zeros.
- We can remove the zeros completely and replace them with double semicolon as shown in below figure.


Abbreviated address
AC81 : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF
Replace by double semicolons
Further abbreviated
AC81 : : BBFF : 0 : FFFF

- It is important to note that abbreviation is allowed only once per address. Also note that if there are two runs of zero sections, then only one of them can be abbreviated.

CIDR NOTATION

IPv6 protocol allows classless addressing and CDR notation. BDR.



FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF/60

CATEGORIES OF ADDRESS

IPv6 defines three different types of addresses

1. **UNICAST**

   A unicast address defines a signal computer. When a packet sent to a unicast address is delivered to that specific computer.

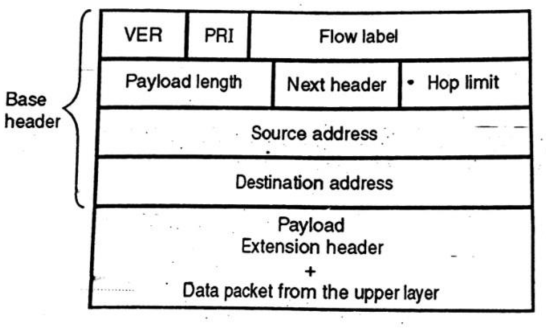
2. **MULTICAST ADDRESSES**

   - A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to the same physical network.
   - Packet sent to a multicast address must be delivered to each and every member of the set.
   - There are no broadcast addresses in IPv6, because multicast addresses can perform the same function. The type of address is determined by the leading bits.
   - Multicast addresses all start with FF (11111 11111) and all other addresses are unicast addresses.

IPv6 PACKET FOUND

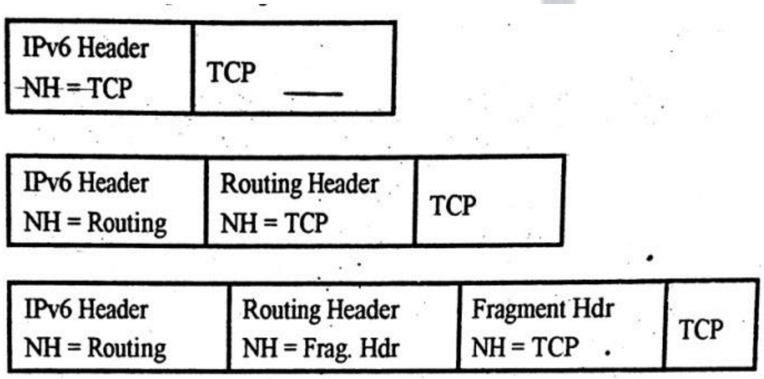
- ➢ The IPv6 packet is shown in below figure. Each packet consists of a base header which is mandatory followed by the payload.
- ➢ The pay load is made up of two parts.

  1. Optional extension headers 2. Data from an upper layer



EXTENSION HEADERS

- The length of the base header is fixed at 40 byte
- But in IPv6, the base header can be followed by upto six extension headers.
- This is to give more functionality to the IP datagram. Many of the extension header are options in IPv4.
- The IPv4 header has space for some optional fields requiring a particular processing of packets. These optional fields are not used often, and they can deteriorate router performance remarkably because their presence must be checked for each packet. IPv6 replaces optional fields by extension headers.
- In IPv6, optional Internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet (see in below figure).
- There are a small number of such extension headers, each identified by a distinct Next Header value. An IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the proceeding header. There are seven kinds of extension header.



- Therefore, extension header must be processed strictly in the order they appear in the packet; a receiver must not, for example, scan through a packet looking for a particular kind of extension header and process that header prior to processing all the preceding ones.
- When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:

1. IPv6 header

2. Hop-by-Hop Optional header
3. Destination Options header
4. Routing header
5. Fragment header
6. Authentication header
7. Encapsulating security payload header
8. Destination optional header
9. Upper-layer header

FRAGMENTATION

- Conceptually the fragmentation is same as that in IPv4 but the place where fragmentation takes place is different.
- In IPv4 the fragmentation is done by the source or router, but in IPv6 only the original source can fragment.

MIGRATING TO IPv6 (COMPATIBILITY TO IPv4)

- It was IPv4's success the made an upgraded necessary, which means that there is a significant installed base of users to upgrade.
- Keeping the transmission orderly was a major objective of the entire IPng program, and there are no plans for a cutover data when IPv6 would be turned on and IPv4 turned off.
- The strategy chosen for the upgrade is to deploy the IPv6 protocol stack in parallel with IPv4. In other words, hosts the upgrade to IPv6 will continue to exist as IPv4 hosts at the same time.
- An experimental IPv6 backbone, or 6 bone, has been set up to handle IPv6 Internet traffic in parallel with the regular Internet.
- Such hosts will continue to have 32-bit IPv4 addresses but will add 128-bit IPv6 addresses. By the year 1999, hundreds of networks were linked to the 6 bone.
- The transition can be achieved through two approaches: protocol tunnelling or IPv4/IPv6 dual stack.

COMPARISON BETWEEN IPv4 AND IPv6

IPv4	IPv6
In IPv4 there are only 2^{32} possible ways how to represent the address (about 4 billion possible addresses)	In Ipv6 there are 12^{128} possible way (about 3, $4*10^{38}$ possible addresses)
The IPv4 address is written by dotted-decimal	IPv6 is written in hexadecimal and consists of 8 group, containing 4 hexadecimal digits or 8 groups of 16 bits each, e.g. FABC: AC77: 7834:2222:FACB: AB98:5432:4567
The basic length of the IPv4 header comprises a minimum of 20 bytes (without option field). Maximum total length of the IPv4 header is 60 bytes (with option fields), and uses 13 fields to identify various control settings.	It has static header of 40 bytes in length, and has only 8 fields. Option information is carried by the extension header, which is placed after the IPv6 header.
It's header has a checksum, that must be computed by each router.	IPv6 has no header checksum because checksum are, for example, above the TCP/IP protocol suit, and above the Token Ring, Ethernet etc.
IPv4 contains an 8-bit fields called Service Type. Service Type field is composed of a procedure field and TOS (Type of Service) field	Header contains an 8-bit field called the Traffic Class Field. This field allows the traffic source to identify desired delivery priority of its packets.
The IPv4 node has only state full auto-configuration.	The IPv6 node has both a state full and a stateless address auto-configuration mechanism.
Security in IPv4 networks is limited to tunnelling between two networks	IPv6 has been designed to satisfy the growing and expanded need for a network security.
Both the source and destination addresses are 32 bits (4 bytes) in length.	Source and destination and addresses are 128 bits (16 bytes) in length.
IPsec support in optional.	IPsec support is required.
No identification of packet flow for QoS handling by router as present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label Field.
Address resolution Protocol (ARP) uses broadcast ARP request frames to resolve an IPv4 address to a link layer address	ARP Request frames are replaced with multicast Neighbour Solicitation messages
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
ICMP Router Discovery is used to determine the optional	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Options are included in header	All optional data is moved to IPv6 extension headers.

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

- The IP provides unreliable and connectionless datagram delivery.
- IP is a best-effort delivery service that delivery a datagram from its original source to its final destination. However, it has two deficiencies: lack of assistance mechanisms and lack of error control.
- The Internet Control Message Protocol (ICMP) reports error and sends control messages on behalf of IP.
- ICMP does not attempt to make IP a reliable protocol. It simply attempts to report error and provide feedback on specific conditions. These messages are carried as IP packets and are therefore unreliable.
- IP also lack a mechanism for host and management queries. A host sometimes needs to determine if a another host or a router is alive. And sometimes a network manager needs information from another router or host
- The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP. ICMP itself it is a network layer protocol.
- However, its messages are not passed directly to the data link layer as would be expected. Instead, the message are first encapsulated inside IP datagrams before going to the lower layer (The value of the protocol field in the IP datagram is 1 to indicate that the IP data are an ICMP message)