MAC ADDRESS

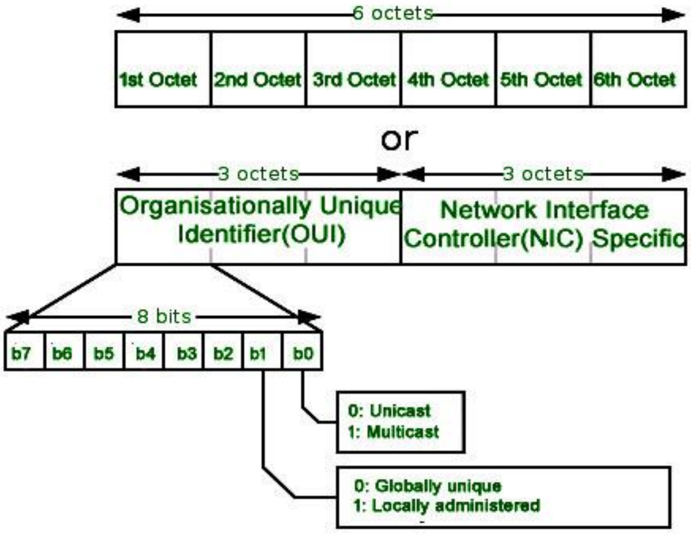
In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer. In this article, we will discuss about addressing in DLL, which is MAC Address.

MEDIA ACCESS CONTROL (MAC) ADDRESS –

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.



FORMAT OF MAC ADDRESS –

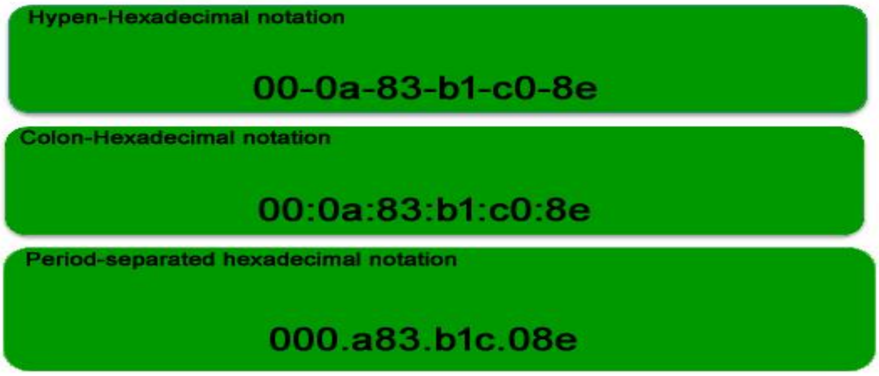
MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique Identifier**). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

Here are some OUI of well known manufacturers :

CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc.
3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

The rightmost six digits represents **Network Interface Controller**, which is assigned by manufacturer.

As discussed above, MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats –



Hypen-Hexadecimal notation
00-0a-83-b1-c0-8e

Colon-Hexadecimal notation
00:0a:83:b1:c0:8e

Period-separated hexadecimal notation
000.a83.b1c.08e

Note: Colon-Hexadecimal notation is used by LINUX OS and Period-separated Hexadecimal notation is used by CISCO SYSTEMS.

HOW TO FIND MAC ADDRESS –

Command for UNIX/Linux - IFCONFIG -A
IP LINK LIST
IP ADDRESS SHOW

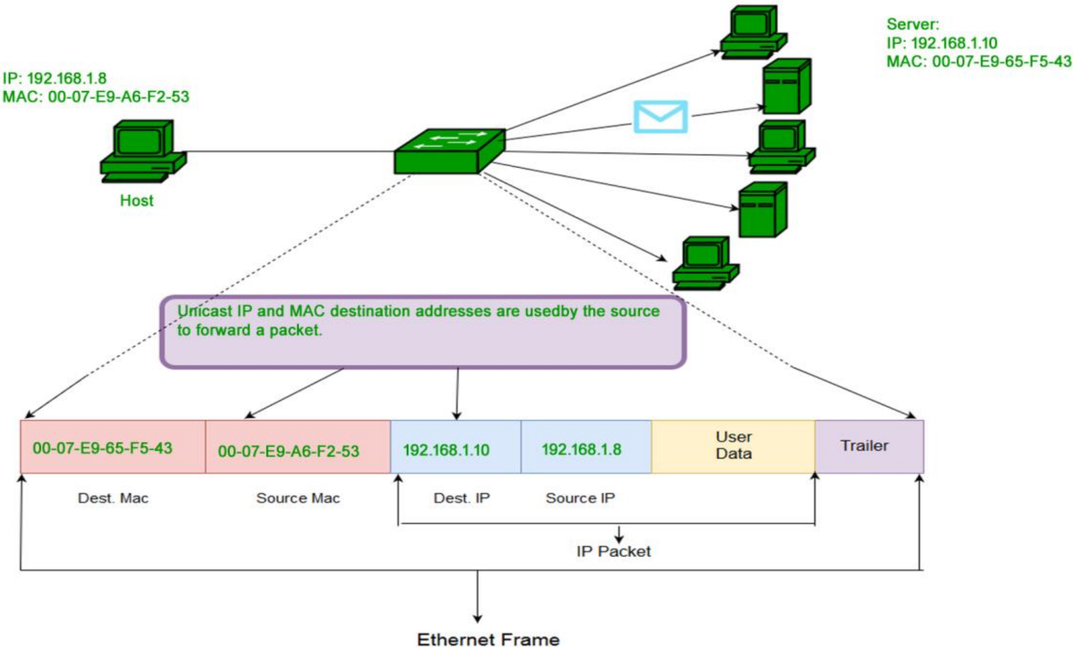
Command forWindows OS - IPCONFIG /ALL

MacOS - TCP/IP CONTROL PANEL

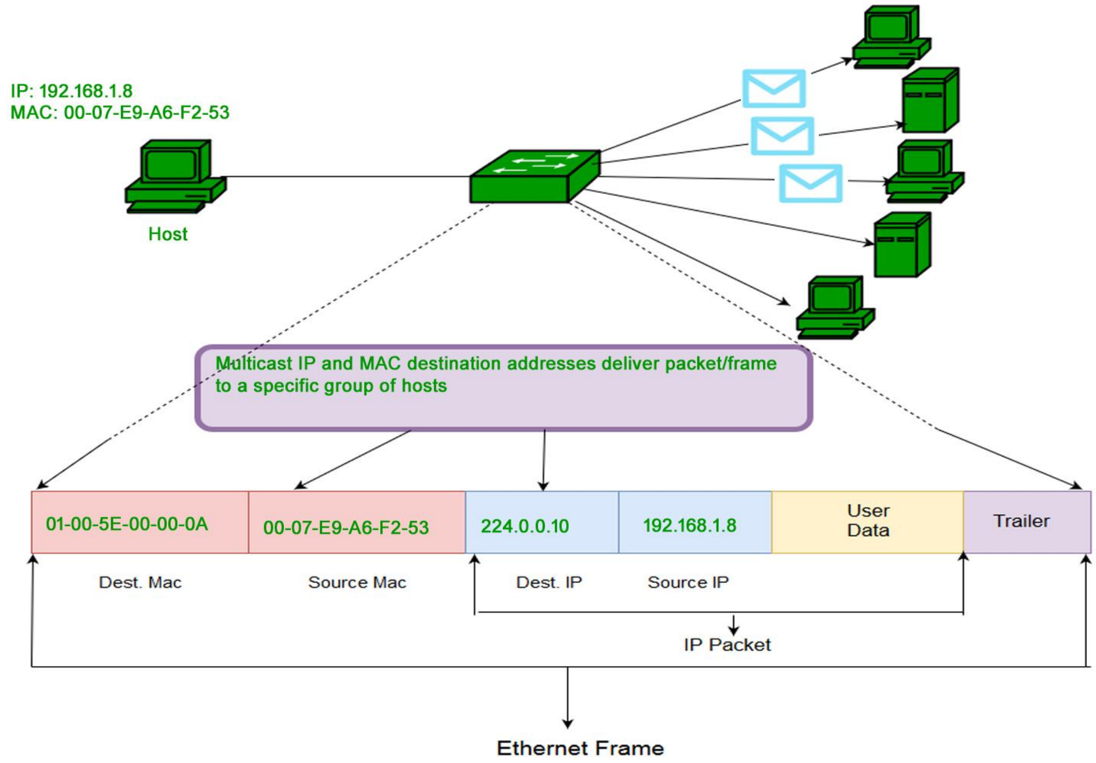
Note – LAN technologies like Token Ring, Ethernet use MAC Address as their Physical address but there are some networks (AppleTalk) which does not use MAC address.

TYPES OF MAC ADDRESS –

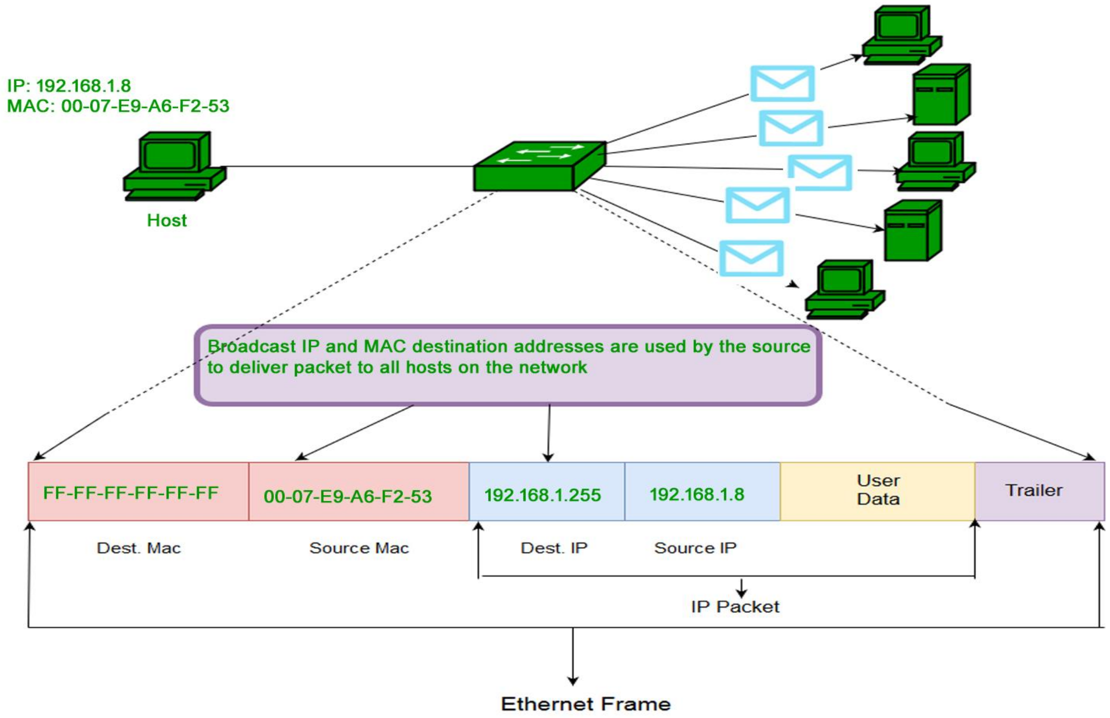
1. **Unicast –** A Unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB (least significant bit) of first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.



2. **Multicast –** Multicast address allow the source to send a frame to group of devices. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) of first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.



3. **Broadcast –** Similar to Network Layer, Broadcast is also possible on underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred as broadcast address. Frames which are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belong to that LAN segment.



WHAT IS MAC CLONING –

Some ISPs use MAC address inorder to assign IP address to gateway device. When device connects to the ISP, DHCP server records the MAC address and then assign IP address. Now the system will be identified through MAC address. When the device gets disconnected, it looses the IP address. If user wants to reconnect, DHCP server checks if the device is connected before. If so, then server tries to assign same IP address (in case lease period not expired). In case user changed the router, user has to inform the ISP about new MAC address because new MAC address is unknown to ISP, so connection cannot be established.

Or the other option is **Cloning**, user can simply clone the registered MAC address with ISP. Now router keeps reporting old MAC address to ISP and there will be no connection issue.

IPADDRESSING

WHAT IS IP ADDRESS?

An IP address is a numeric identity of an interface. Just like a postal address provides a unique identity to a house, an IP address provides a unique identity to an interface.

WHY AN INTERFACE NEEDS UNIQUE IP ADDRESS?

IP network uses IP address to find the destination interface and delivers the IP packets. In order to receive IP packets, an interface needs a unique IP address. If multiple interfaces have same IP address, IP network will not work.

Let’s understand it with an example. In a city all houses have same house number, suppose 195. If there is mail for house number 195, how mailman will delivery that mail? To deliver the mail at correct house, postal system needs unique address of that house. Exactly same way, to deliver an IP packet at correct interface, IP network needs a unique IP address of that interface.

IP ADDRESS FORMAT

An IP address is 32 bits in length. These bits are divided in four parts. Each part is known as octets and contains and 8 bits.

An IP address can be written in three notations; dotted-decimal, binary and hexadecimal. Among these types, dotted-decimal is the most popular and frequently used method for writing an IP address.

In dotted-decimal notation, each byte (8 bits) of the 32 bits IP address is written in decimal equivalent. The four resulting decimal numbers are separated by a dot and written in a sequence. 10.10.10.10, 172.168.10.1, 192.168.1.1 and 200.0.0.1 are some examples of IP address in dotted-decimal notation.

SUBNET MASK

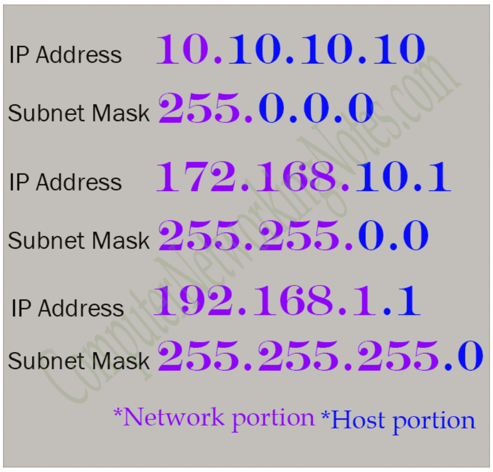
Subnet mask is used to separate the network address from the host address in IP address. As we discussed earlier an IP address is the combination of network address and host address, subnet mask helps us and programs which use IP address in identifying the network portion and the host portion.

Just like IP address, subnet mask is also 32 bits in length and uses same notations which IP address uses to present itself.

Subnet mask assigns an individual bit for each bit of IP address. If IP bit belongs to network portion, assigned subnet mask bit will be turned on. If IP bit belongs to host portion, assigned subnet mask bit will be turned off.

In binary notation, 1 (one) represents a turned on bit while 0 (zero) represents a turned off bit. In dotted-decimal notation, a value range 1 to 255 represents a turned on bit while a value 0 (zero) represents a turned off bit.

An IP address is always used with subnet mask. Without subnet mask, an IP address is an ambiguous address in IP network.



IP Address 10.10.10.10
Subnet Mask 255.0.0.0

IP Address 172.168.10.1
Subnet Mask 255.255.0.0

IP Address 192.168.1.1
Subnet Mask 255.255.255.0

*Network portion *Host portion

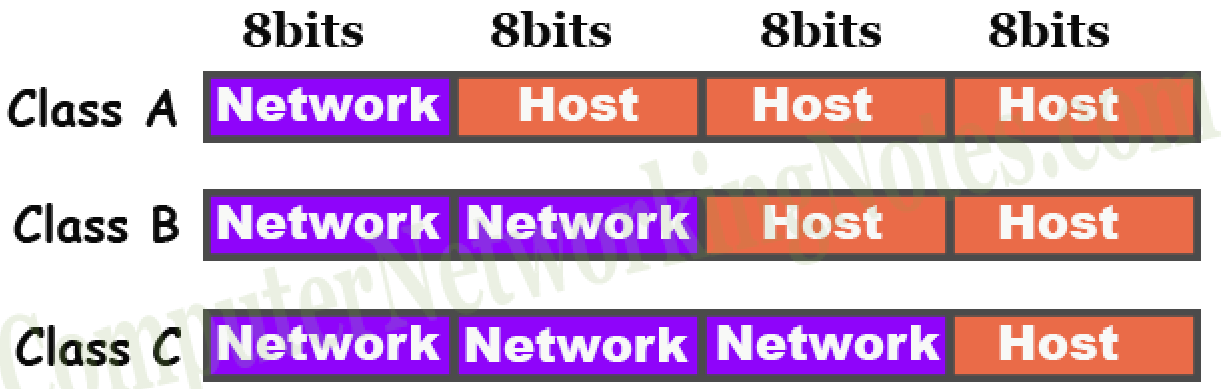
IP ADDRESS CLASSES

There are 4,294,967,296 IP addresses. Managing all these addresses without any scheme are next to impossible. Let's understand it with a simple example. If you have to find out a word from a language dictionary, how long will you take? Usually you will take less than five minutes to find out that word. You are able to do this because words in dictionary are organized in alphabetic order. If you have to find out the same word from the dictionary which does not use any sequence or order to organize the words, how long will you take this time? It may take up to one week to find out that specific word from all words. If an unorganized dictionary which roughly contains 1 billion words can turn a five minutes task in a one week task than suppose how nearly 4.3 billion addresses will make a search task complicated if they are unorganized.

For easier management, IP addresses are organized in numeric order and divided in following five classes.

Class	Starting Address	Ending Address	Subnet mask
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	255.255.255.255
E	240.0.0.0	255.255.255.255	255.255.255.255

As we discussed earlier, an IP address is the combination of network address and host address. In each IP address, few bits are reserved for network address. In class A, B and C first 8, 16 and 24 bits are reserved respectively for network addresses.



HOW TO FIND THE CLASS OF AN IP ADDRESS?

To find the class of an IP address, simply pay attention on the first octet.

If the value of first octet is in **range 1 to 127**, it's a class A IP address. Examples of class A IP address are:

- **1**.2.3.4, **10**.20.30.45, **125**.234.123.23, **126**.100.200.45, etc.

If the value of first octet is **in range 128 to 191**, it's a **class B** IP address. Examples of class B IP address are:

- **128**.200.100.50, **191**.200.100.1, **172**.168.0.1, **175**.45.48.14, etc.

If the value of first octet is in **range 192 to 223**, it's a **class C** IP address. Examples of class C IP address are:

- **192**.168.1.1, **200**.0.0.1, **223**.224.127.1, **212**.14.15.56, etc.

PRIVATE IP ADDRESS AND PUBLIC IP ADDRESS

Based on accessibility, IP addresses are mainly divided in two categories; private IP addresses and public IP addresses. Differences between private IP addresses and public IP addresses are following.

PRIVATE IP ADDRESSES

Private IP addresses are the IP addresses which are reserved for local networks and cannot be accessed from a public network such as Internet. Vice versa a public network cannot be accessed from a private IP address.

Following IP ranges are reserved for private IP addresses.

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

PUBLIC IP ADDRESSES

Public IP addresses are the IP addresses which are publicly accessible from any public network such as Internet. In order to access a public IP address, we must have to use a public IP address.

Except private IP addresses, all IP addresses of class A, B and C are public IP addresses.

SPECIAL IP ADDRESSES

Special IP addresses are the IP addresses which are reserved for network testing and troubleshooting. These IP addresses cannot be assigned to an end device or an interface. Following addresses are reserved for special purpose: -

0.0.0.0:- This is the first IP address of IP addresses. It represents all networks.

127.0.0.0 to 127.255.255.255: - Reserved for IP protocol testing and troubleshooting. Virtual interfaces such as loopback adaptor use this IP range for addressing.

224.0.0.0 to 239.255.255.255 (*Class D*): - Reserved for multicast addresses. A multicast address is an address which has multiple recipients.

240.0.0.0 to 255.255.255.255 (*Class E*): - Reserved for future use. These addresses are not used currently for any purpose.

255.255.255.255:- This is the last IP address of IP addresses. It represents all hosts.

IPv6

Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on the Network Layer (Layer-3). Along with its offering of an enormous amount of logical address space, this protocol has ample features to which address the shortcoming of IPv4.

WHY NEW IP VERSION?

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 3.4×10^{38} 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 provided the fact that 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 hosts on the Internet, with some limitations involved like Firewall, organization 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 a halt on inter segment communication.
- **Faster Forwarding/Routing**
  Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.
- **IPSec**
  Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.
- **No Broadcast**

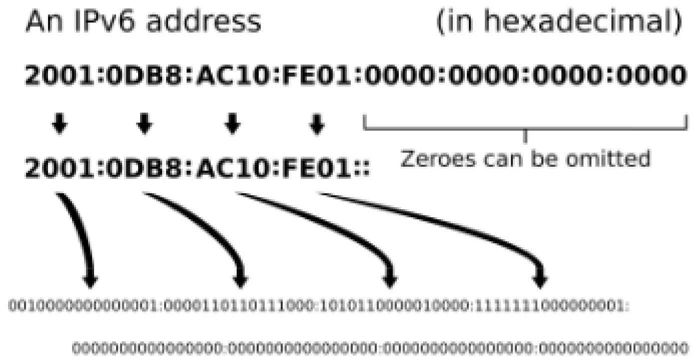
Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

- **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, send the packet to the nearest destination.
- **Mobility**
  IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.
- **Extensibility**
  One of the major advantages 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.

THE STRUCTURE

In IPv4, the standard IP address would be formatted as such: 192.168.1.1, but it is entirely different with IPv6. There are 128 bits **(binary digits)** in IPv6, which gets converted into a **hexadecimal** format so that it can be used in networking. That large set of 0's and 1's once converted will look like this IPv6 example format: **6e3d:e161:de2a:eb9e:28af:86bc:55a3:e5ce**.

This will be the new format of IP addresses going forward once IPv4 addresses run out, and they are quite a bit longer than most people are used to seeing.



How IPv6 gets translated from 128 bits to usable hexadecimal code.

DIFFERENCES BETWEEN IPV4 AND IPV6

IPv4 and IPv6 are internet protocol version 4 and internet protocol version 6, IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency.

Difference Between IPv4 and IPv6:

IPV4	IPV6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
In IPv4 Packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In IPv4 checksumfield is available	In IPv6 checksumfield is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed