Difference between MAC and IP Address

IP Address: The term IP address stands for "INTERNET PROTOCOL ADDRESS". An IP address is a 32 bit decimal number that is normally written as four numbers between 1 and 255, each separated from the other by a decimal point. An example of IP address is

128.11.3.31

The above form of representing the IP address is called "dotted decimal notation."

Deep understanding of IP Address concepts

An internet is made up of combination of physical networks (LAN or WAN) connected by routers. When a host communicates with another host, the packets may travel from one physical network to another using these routers. This suggests that communication at this level also needs some global identification system. A host must be able to communicate with any other host without worrying about which physical network must be passed through. This means that the hosts must be identified uniquely and globally at this layer also. N addition, for efficient and optimum routing, each router must also be identified uniquely and globally at this layer.

The identifier that is used in the IP layer of the TCP/IP protocol is called the INTERNET PROTOCOL ADDRESS OR THE IP ADDRESS.

It is a 32-bit binary address implemented in software that uniquely and universally defines a host or a router on the internet.

The IP addresses are unique. They are unique in the sense that each address defines one, and only one, device (host or router) on the internet. Two devices on the internet can never have the same IP address.

Each IP address consists of four bytes(32 bits), defining two parts: netid and host id
Where net id : Identifies a network
Host id :. Identifies host on that network.

For example in the IP address 127.255.255.255 (class b address), the first 2 bytes 127.255 defies the netid and the last 2 bytes 255.255 defines the host id.

MAC ADDRESS:

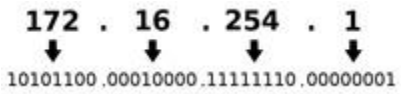
The hosts and routers are recognized at the network level by their logical address. Every protocol that deals with interconnecting networks requires logical address (i. e. IP address).

However , packets must pass through physical networks to reach these hosts and routers. At the physical level, the hosts and routers are recognized by their physical address. A physical address is a local address. Its jurisdiction is a local network. It should be unique locally, but not necessary universally. It is called physical address because it is usually (not always) implemented in hardware. Examples of

physical address are 48 bit MAC address in Ethernet and token ring protocols, which are implemented on the NIC installed in the host or router.

The physical and logical addresses are two different identifiers. We need both of them because a physical network, such as Ethernet can be used by two different protocols at the network layer such as IP and IPX(Novell) at the same time. Likewise , a packet at the network layer such as IP may pass through different physical networks such as Ethernet and Local talk.

Therefore, in order to deliver a packet to a host or router we need 2 kinds of addressing, one is logical and the other one is physical.. The logical address is IP address and the physical addresss is MAC address.



MAC (Media Access Control) and IP (Internet Protocol) are the two addresses that identifies your computer in a network. It is usually used to track data packets to ensure that they get to where it was intended. An IP address is usually assigned by the network administrator or internet service provider, you are either provided a static one at the beginning or given a dynamic one every time you connect to the network. This is not true with MAC addresses as it is already embedded on the device or the network card during manufacturing. It is supposed to be permanent and could not be changed by anyone as it was meant to identify a specific network interface card no matter where it is in the world.

Experienced IT people can deduce from an IP address to which network that computer is connected to and consequently its approximate location. Certain addresses should only be from certain regions or countries and are thus a little bit easier to track. With a MAC address, this is not possible as the address itself does not contain information that lets you identify its location. For this reason, it is more comparable to a name than an address.

One of the uses of a MAC address which people are most likely to encounter is in MAC filtering, used by wireless routers to allow or disallow certain computer from accessing the network. This is a quick and easy method if you only want a handful of computers or laptops to connect. A MAC address can also be used to assign an IP address to a certain computer. The server queries the MAC address of the network card, looks it up in a list, and assigns the corresponding IP address,

Despite all the security measures put in place. MAC and IP address spoofing is still easy for those who knows how to do it. It is therefore still possible to gain access to a WiFI network by monitoring it and intercepting the MAC address of an authorized computer. IP address spoofing is also possible, a common practice for people who do not want to be found.

References:

http://webupon.com/web-talk/difference-between-ip-address-and-mac-address/
http://www.differencebetween.net/technology/difference-between-mac-and-ip-address/