MAC and Logical addressing (A Review Study)

Umang Garg[1], Pushpneel Verma[2], Yudhveer Singh Moudgil[3], Sanjeev Sharma[4],

Department of Computer Science & Engineering
[1,3,4] Uttaranchal Institute of Technology, Arcadia Grant, P.O. Chandanwari
PremNagar,Dehradun,Uttarakhand.
[2] Bhagwant Institute of Technology, Bhagwantpuram, Muzaffarnagar

ABSTRACT

Networking is the vast growing technology in our culture today. One of the technologies is Internet Protocol. It is the main network protocol in the Internet model (TCP/IP). The success of TCP/IP as the network protocol of the Internet is largely because of its ability to connect together networks of different sizes and systems of different types. These networks are arbitrarily defined into three main classes (along with a few others) that have predefined sizes, each of which can be divided into smaller subnet works by system administrators. A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs.

In this paper we analysis that when MAC address is unique for all machines although we are using IP address for networking purpose. We studied and analyzed various attributes related to IP address scheme and MAC address. A detailed review study is discussed in this paper.

Keywords: Internet Protocol (IP), IPv4, IPv6, Mask, Classless Addressing, Classful Addressing, Subnet Mask, Default gateway.

1. INTRODUCTION

IP was first developed in the early 1980s. Its intent was to interconnect few nodes and was never expected to grow to the size of the Internet has become today. IPv4 was initially designed for best-effort service and only scaled to today's Internet size because of its state-less design. In the early 1990s, it became pretty evident that if the Internet will continue to grow at the exponential rate of doubling every eighteen months, the IPv4 address space would be depleted by the turn of the millennium. However work began on a new Internet Protocol, which was first called IPnG from IP Next Generation, but later became known as IPv6. The most evident reason for a new version of an IP was to increase the address space. Even in the most pessimistic scenario of inefficient allocation of addresses there would still be well over 1000 unique IP addresses per square meter of the earth.

2. IP addresses: Networks and hosts

An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

IP addresses are normally expressed in dotted-decimal format, with four numbers separated by dotes, such as 192.168.123.132. To understand how subnet masks are used to distinguish between hosts, networks, and subnetworks, examine an IP address in binary notation. For example, the dotted-decimal IP address 192.168.123.130 is (in binary notation) the 32 bit number 1100000000101000111101110000010. This number may be hard to make sense of, so divide it into four parts of eight binary digits. These eight bit sections are known as octets. The example IP address, then, becomes 1000000.10101000.01111011.10000010. For a TCP/IP wide area network (WAN) to work efficiently as a collection of networks, the routers that pass packets of data between networks do not know the exact location of a host for which a packet of information is destined. Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host.

For this process to work, an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address.(fig:1)

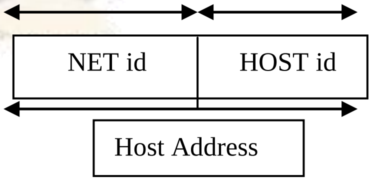

Fig: 1

2.1 Subnet mask

The second item, which is required for TCP/IP to work, is the subnet mask. The subnet mask is used by the

TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

In TCP/IP, the parts of the IP address that are used as the network and host addresses are not fixed. This information is supplied in another 32-bit number called a subnet mask. In this example, the subnet mask is 255.255.255.0.

Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the Network Address or Number.

For example, after applying logical AND b/w our test IP address and the default Class B subnet mask, we get:

```
10001100.10110011.11110000.11001000
11111111.11111111.00000000.00000000
-------------------------------------------------------
10001100.10110011.00000000.00000000
```

That indicates the Network address.

Default subnet masks for:
Class A - 11111111.00000000.00000000.00000000(/8 CIDR)
Class B - 11111111.11111111.00000000.00000000(/16 CIDR)
Class C - 11111111.11111111.11111111.00000000(/24 CIDR)

2.2 Network classes

Internet addresses are allocated by the InterNIC the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

- Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
- Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

In some situations, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions. So network can be divided into subnet masks.

2.3 Subnetting

A subnetwork, or subnet, is a logically visible subdivision of an IP network. The practice of dividing a single network into two or more networks is called subnetting and the networks created are called subnetworks or subnets. A Class A, B, or C TCP/IP network can be further divided, or subnetted, by a system administrator.

A system administrator who is allocated a block of IP addresses may be administering networks that are not organized in a way that easily fits these addresses. For example, you have a wide area network with 150 hosts on three networks that are connected by a TCP/IP router. Each of these three networks has 50 hosts. You are allocated the class C network 192.168.123.0. (For example.) This means that you can use the addresses 192.168.123.1 to 192.168.123.254 for your 150 hosts.

Two addresses that cannot be used in this example are 192.168.123.0 and 192.168.123.255 because binary addresses with a host portion of all ones and all zeros are invalid. The zero address is invalid because it is used to specify a network without specifying a host. The 255 address (in binary notation, a host address of all ones) is used to broadcast a message to every host on a network. So these addresses are not assigned to any individual host.

Instead of requesting more address blocks for each network, you divide your network into subnets that enable you to use one block of addresses on multiple physical networks.

In this case, you divide your network into four subnets by using a subnet mask that makes the network address larger and the possible range of host addresses smaller. In other words, you are 'borrowing' some of the bits usually used for the host address, and using them for the network portion of the address. The subnet mask 255.255.255.192 gives you four networks of 62 hosts each. This works because in binary notation, 255.255.255.192 is the same as 1111111.11111111.1111111.11000000. The first two digits of the last octet become network addresses, so you get the additional networks 00000000 (0), 01000000 (64), 10000000 (128) and 11000000 (192). (Some administrators will only use two of the subnetworks using 255.255.255.192 as a subnet mask. (Fig: 2) In these four networks, the last 6 binary digits can be used for host addresses.

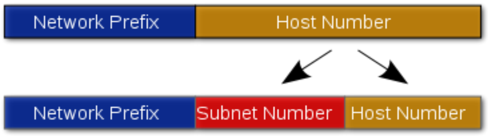

Fig: 2

2.4 Default gateways

If a TCP/IP computer needs to communicate with a host on another network, it will usually communicate through a device called a router. In TCP/IP terms, a router that is specified on a host, which links the host's subnet to other networks, is called a default gateway.

When a host attempts to communicate with another device using TCP/IP, it performs a comparison process using the defined subnet mask and the destination IP address versus the subnet mask and its own IP address. The result of this comparison tells the computer whether the destination is a local host or a remote host.

If the result of this process determines the destination to be a local host, then the computer will simply send the packet on the local subnet. If the result of the comparison determines the destination to be a remote host, then the computer will forward the packet to the default gateway defined in its TCP/IP properties. It is then the responsibility of the router to forward the packet to the correct subnet.

3. MAC ADDRESS

A Physical address or MAC address is a 12-digit hexadecimal numbers (48-bits) flat address burned into the ROM of the NIC card which is a Layer1 device of the OSI model. This is divided into 24-bit vendor code and 24-bit serial address. This is unique for each system and cannot be changed. In computing, a physical address, also real address, is the memory address that is represented in the form of a binary number on the address bus circuitry in order to enable the data bus to access a particular storage cell of main memory. A MAC address usually encodes the manufacturer's registered identification number. It may also be known as an Ethernet Hardware Address (EHA), hardware address, adapter address, or physical address. The MAC protocol encapsulates a SDU (payload data) by adding a 14 byte header (Protocol Control Information (PCI)) before the data and appending a 4-byte (32-bit) Cyclic Redundancy Check (CRC) after the data. The entire frame is preceded by a small idle period (the minimum inter-frame gap, 9.6 microseconds (µS)) and a 8 byte preamble (including the start of frame delimiter).
Three numbering spaces, managed by the Institute of Electrical and Electronics Engineers (IEEE), are in common use for formulating a MAC address: MAC-48, EUI-48, and EUI-64. Where "EUI" stands for Extended Unique Identifier.

3.1 MAC Address Notations

Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits which specify the interface serial number for that interface vendor.
The Standard (IEEE 802) format for printing MAC-48 addresses is six groups of two hexadecimal digits separated by hyphens (-) or colon (:) in transmission order e.g. 01-23-45-56-67-AB, 01-12-23-34-56-AB. This form is also commonly used for EUI-64.Other convention use three groups of four hexadecimal digits separated by dots (.) e.g. 0123.4567.89AB; again in transmission order.

3.2 MAC Address Representation

The Original IEEE 802 MAC Address comes from the original Xerox Ethernet Addressing Scheme. The 48 bit Address space contains potentially 248 or 281,474,976,710,656 possible MAC address (Fig: 3).

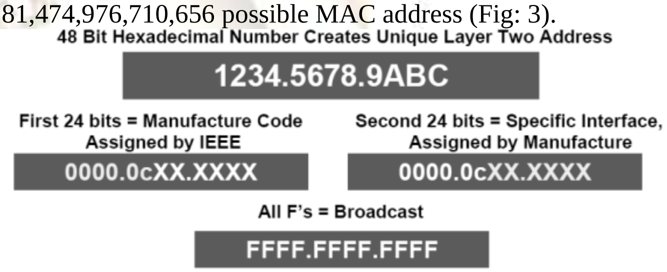
48 Bit Hexadecimal Number Creates Unique Layer Two Address
1234.5678.9ABC
First 24 bits = Manufacture Code Assigned by IEEE
0000.0cXX.XXXX
Second 24 bits = Specific Interface, Assigned by Manufacture
0000.0cXX.XXXX
All F's = Broadcast
FFFF.FFFF.FFFF

Fig: 3

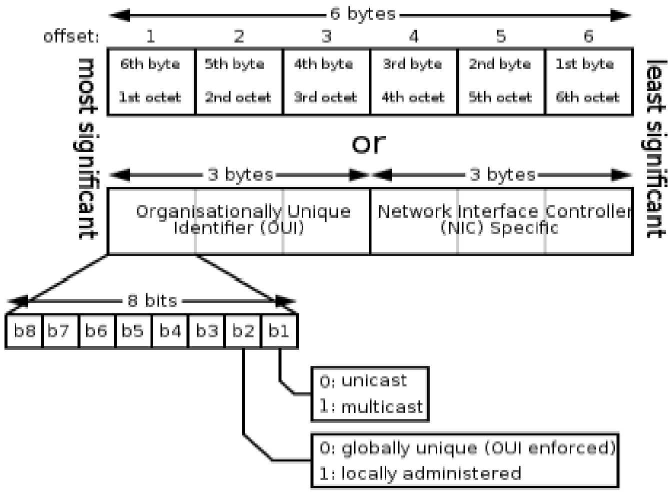

Fig: 4

Address can either be universally administered address or locally administered address. A universally administered address is uniquely assigned to a device by its manufacturer these are sometimes also called burned in address (BIA). The First three octets identify the organization that issued the identifier (OUI) (Fig: 4). The following three octets are assigned by the organization in nearly any manner they please Subject to the constraint of uniqueness. The locally administered address is assigned by to a device by a networks administrator address do not contain OUIs. Universally administered and locally administered address are distinguishing by setting the second least significant bit of the most significant byte of the address. If the bit is 0 the address is universally admit if it is of the address is locally administered.

4. TECHNOLOGY AND WORKING MECHANISM OF IPV4

The Internet protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols. IPv4 is an unreliable and connectionless datagram protocol— a best-effort delivery service. The term best-effort means that IPv4 provides no error control or flow control. IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. If reliability is important, IPv4 must be paired with a reliable protocol such as TCP. IPv4 is also a connectionless protocol for a packet-switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transmission.

4.1 Packet Structure, Header & Version

An IP packet consists of a header section and a data section. Packet is called datagrams. It is customary to show the header in 4-byte sections. The IPv4 packet header consists of 13 fields, of which 12 are required. The 13th field is optional (red background in table) and aptly named: options. The fields in the header are packed with the most significant byte first (big endian) and for the diagram and discussion, the most significant bits are considered to come first. The most significant bit is numbered 0, so the version field is actually found in the four most significant bits of the first byte. The first header field in an IP packet is the four-bit version field.

4.2 IPv4 Addresses

IPv4 uses 32-bit (four-byte) addresses, which limits the address space to 4,294,967,296 (2^{32}) possible unique addresses. However, some are reserved for special purposes such as private networks (~18 million addresses) or multicast addresses (~270 million addresses). As addresses are being incrementally delegated to end users, an IPv4 address shortage has been developing, however network addressing architecture redesign via classful network design, Classless Inter-Domain Routing, and network address translation (NAT) has significantly delayed the inevitable exhaustion. IPv4 addresses are usually represented in dot-decimal notation (four numbers, each ranging from 0 to 255, separated by dots, e.g. 208.77.188.166). Each part represents 8 bits of the address, and is therefore called an octet.

4.3 Classful & Classless IP addressing

IPv4 addressing at its inception used the concept of classes. This architecture is called classful addressing. Although this scheme is becoming obsolete, we briefly discuss it here to show the rational behind classless addressing. In classful addressing, the space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space. To overcome address depletion and give more organizations access to the Internet classless addressing was designed and implemented. The different schemes of classless addressing are briefly described below. Around 1987 Variable Length Subnet mask (VLSM) was introduced. VLSM is used to implement subnets of different sizes. This allows efficient use of subnets and avoids wasting IP addresses. An address in CIDR notation is written with a suffix indicating the number of bits in the prefix, such as 192.168.0.0/16, where /16 is the suffix, and 192.168.0.0 is the prefix.

4.4 Mask

Although the length of the netid and hostid (in bits) is predetermined in classful addressing. We can also use a mask (also called the default mask) a 32-bit number made of contiguous 1s followed by contiguous 0s. The mask can help us to find the netid and the hostid. For example, the mask for a class A address has eight 1s, which means the first 8 bit of any address in class A define the net id; the next 24 bits defined the hostid. And the complete address is specify to the host address.

4.5 Applications

In the IPv4 mobile network and via the IPv4 mobile LAN any application can be run. A Web-based application will be utilized that take real time GPS data and sends it to a site on the Internet. A Web-based application will be utilized to show real-time flight weather and other information useful to the aeronautics community, government organizations, and the military. Instant Messaging is a nice application to run as it is readily available and used very little bandwidth.

4.6 IPv4 Limitations

The first limit of IPv4 lies in the exhaustion of available public IPv4 addresses. The development of such mobile and home services will lead to a more rapid consumption of IPv4 addresses even if ISPs assign only one static public IP address to each home network. The customers will more and more use permanent connections, based on digital subscriber line (DSL) or 3G accesses. In practice, for all IP devices in mobile and home network to be addressable from outside, the network will need a lot of public IP addresses.

5. TECHNOLOGY AND WORKING MECHANISM OF IPV6

The IPv6 packet is composed of a mandatory base header followed by the payload. The payload consists of two parts: optional extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information.

5.1 IPV6 ADDRESS AND STRUCTURE

An IPv6 address is 128 bit (16 byte) value, with a logical structure, which can be assigned on a network interface, making the host reachable over IPv6 on that interface on that address. An IPv6 address can be assigned on an interface that has an IPv4 address assigned also. IPv6 addresses are part of the IPv6 header where they indicate origin and destination of the IPv6 datagram. Source IPv6 addresses are always unicast addresses, uniquely identifying the originating interface. Destination IPv6 addresses are unicast, anycast, or multicast addresses.

Addresses are 128 bits long and have several distinct structural definitions, except for the loopback address and the "unspecified" address, which have no specific structure. Unicast addresses are typically composed of two logical parts: a 64-bit (sub) network prefix used for routing, and a 64-bit host part used to identify a host within the network. A network prefix consists of an ISP-assigned value in the most significant 48 bits of the address. This value can be self-assigned in case of a unique local address. The 16 bits of the *subnet* field are available to the network administrator to define subnets within the given network. The 64-bits interface identifier is automatically generated from the interface's MAC address (using modified EUI-64 format), obtained from a DHCPv6 server, or assigned manually.

5.2 Notation

Single addresses can be written as eight groups of four hexadecimal digits (each group representing 16 bits, or two octets), and each group is separated by a colon (:). For e.g.: 3001:0db8:85a3:0000:0000:8a2e:0370:7334. Leading zeroes in a group may be omitted (but at least one digit per group must be left). The address above could be written as: 3001:db8:85a3:0:0:8a2e:370:7334. A string of consecutive all-zero groups may be replaced by two colons. In order to avoid ambiguity, this simplification may only be applied once. The address above would typically be written as: 3001:db8:85a3::8a2e:370:7334. The localhost (loopback) address (0:0:0:0:0:0:0:1) and the IPv6 undetermined address (0:0:0:0:0:0:0:0) can thus be reduced to:: 1 and :: respectively

5.3 Unspecified address

There are a number of addresses with special meaning in IPv6: Unspecified address: ::/128 — the address with all zero bits is called the unspecified address (In IPv4 it can be represented as 0.0.0.0). Default Route: ::/0 is the default unicast route address (corresponding to 0.0.0.0 with netmask 0.0.0.0 in IPv4). Local addresses: ::1/128 — the loopback address is a unicast localhost address. fe80::/10 — Addresses in the link-local prefix are only valid on a single link. Unique local addresses fc00::/7 — Unique local addresses (ULA's) are intended for local communication.

5.4 Applications

With the development of IPv6 the application areas are growing. It will be possible for many handheld and mobile devices to be connected. Some examples of IPv6 application are: Multi-user network games, Ad-hoc networking, Collaborative working, Home networking, Peer-to-Peer networking, Ambient Intelligence, Medical Applications, In-Car Communications.

5.5 Advantages

The IPv6 has some advantages over IPv4 that can be summarized as follows: The main advantage of IPv6 over IPv4 is address space. It was design to support +340 undecillion IP addresses compared with 4.3 billion IPv4 addresses. This is the main reason why we should migrate to IPv6 rather than maintaining IPv4 that will be exhausted. The IPv6 specification mandates that IPv6-enabled nodes must support the IP Security Protocol (IPSec), therefore IPv6 nodes more secure than IPv4 nodes. It is also includes security features, such as payload encryption and authentication of the source of the communication, in its specifications. Enhance QoS support to provide better support for real-time traffic (e.g. Voice over IP). IPv6 includes ―labeled flows in its specifications.

5.6 Disadvantages

Ipv6 has no such disadvantages. The only disadvantage is that its network bit is quite longer. This gives rise to complexity and hinders the clear understanding of its technology. For this reason spreading of IPv6 is being slow.

6. COMPARISON BETWEEN IPV4 AND IPV6

Address features is the main changes between IPv4 and IPv6. 128bits addressing space in IPv6 was built to overcome the address space shortage in IPv4. From this table (Table: 1) we are showing some differences between IPv4 and IPv6 -

Features	IPv4	IPv6
No of Addresses	32 bits	128 bits
Checksum in header	Included	No checksum
Header includes options	Required	Moved to IPv6 extension headers
Quality of Services (QoS)	Differentiated Services	Use traffic classes & flow labels
IPSec support	Optional	Required
IP configuration	Manually or DHCP	Auto-configuration or DHCP
Address Resolution Protocol (ARP)	Use to resolve an IPv4 address	Replaced by Neighbor Discovery
IGMP	Use to manage local subnet group	Replaced with Multicast Listener Discovery (MLD)
Mobility	Use Mobile IPv4 (MIPv4)	MIPv6 with faster handover, routing
Domain Name System	Use host address (A) resource records	Use host address (AAAA) resource records

Table: 1

7. CONCLUSION

MAC address is the basis on which communication occurs. However we need IP address to be able to create a routing table, which enables faster communication. Lots of communication algorithms take use of IP addresses (Network address +Subnet masks) to be able to route packages faster.

We need IP address because when we work on LAN we can communicate without IP address with the help of NETBIOS and WINS but in WAN we work on network layer and data frame becomes packet and packet need IP address for routing.

IP address (network address) is just use for transferring information from one network to another. Travelling of information among networks uses IP addresses. While Mac addresses (physical addresses) are actually uses for distribution of information in following ways:

1) Carring of information from one network to another.
2) Distribution of information (resources) is based upon MAC address.

For example:-Network A, Network B and Network C are three networks. All networks are having 5 nodes (client). If network A's node 1 want to send information to node 3 for network B. Then: -

1) Information to the network is sent with the help of IP address of that network (Network B). IP addresses are unique on network layer.
2) Then it will send information to node 3 of network B with the help of MAC address which is unique at layer 2(DLL).

IP address (network address) is just used for transferring information from one network to another network. Travelling of information among networks uses IP addresses. It is used to identify the network and host.

A MAC address (physical addresses) is used for distribution of information within the network segment.

The Ethernet uses MAC address to transfer data between hosts. When it is used with IP network, the IP address is resolved using ARP protocol to find the MAC address of the end device and the data is transmitted.

Port numbers are used by the TCP/UDP protocol to isolate the traffic which is multiplexed and sent by the user application. For example, the user device can open multiple applications at the same time like, multiple web browsers, email and FTP. To identify the data individually the port number are used.

REFERENCES

[1] Y. Rekhter, R. Moskowitz, D. Karrenberg, G. de Groot, E. Lear, , "Address Allocation for Private Internets", 02/29/1996. (Pages=9) (Obsoletes RFC1627).

[2] L.Venkatraman, D.P. Agrawal: A novel authentication in ad hoc networks. In Proceedings of the second IEEE Wireless Communications and Networking Conference, Chicago, September 2009

[3] Mousam Dagar,Priyanka Sangwan "Spoofing Media Access Control (MAC) & Its Counter Measures" IJMAN 2011, www.ifrsa.org

[4] "Comperative study of IPv4 and IPv6" by Rashed Mazumder, Mohammad Badrul Alam Miah, Md. Ahsan Habib from IJMAN -2011 page no. 334 to 337.

[5] Forouzan, B. A., 2006: ―Data Communications and Networking‖, McGraw-Hill Forouzan Networking Series.

[6] IPv6 Ready Logo Program Website, 2009: http://www.ipv6ready.org/.

[7] IPv6_Wikipedia, 2010: IPv6, http://en.wikipedia.org/wiki/IPv6.

[8] IPv4_Wikipedia, 2010: http://en.wikipedia.org/wiki/IPv4.