

MAC Addresses – The Future of Intra-organization Communication

Akhil Kaushik

Assistant Professor, CSE Department
T.I.T.&S Bhiwani
Haryana, India
akhil.kaushik@yahoo.com

Satvika

Assistant Professor, IT Department
T.I.T.&S Bhiwani
Haryana, India
satvika16@yahoo.com

Manoj Barnela

Assistant Professor, Electronics Department
T.I.T.&S Bhiwani
Haryana, India
m.barnela@gmail.com

Loveleen Girdhar

Student, B. Tech Final Year
T.I.T.&S Bhiwani
Haryana, India
loveleen1611@gmail.com

Abstract—The communication era of modern world requires speedy and efficient ways to offer quick and accurate delivery of information within an organization. However, the over dependency of communiqué over logical addressing has caused a mayhem in the intra-organization communication. IP addressing is slow and incompetent whenever compared to MAC addressing. The earlier quandaries of MAC addresses are no longer significant as there are technologies developed over the timeline, which may prove momentous while communication inside a LAN. This paper discusses new developments in the area of Ethernet addressing in correspondence to different operating systems as well as address resolution. The proposed approach also provides a brilliant approach of using the MAC addresses for intra-organization transfer of information.

Keywords— IP address, MAC address, address resolution, ARP cache, Dynamic MAC and Spoofing.

I. INTRODUCTION

The revolutionizing invention of past few decades is definitely the Internet. The internet has changed not only the communication technology, but also the way we think. Now the world has become a small supermarket, where distant product and services can be easily accessed. Innovative inventions like emails, videoconferencing, blogging, social networking, files sharing and ultra fast communication has brought the world at our doorstep. The Internet started with just four nodes at University of California at Los Angeles, University of California at Berkeley, University of Utah and Stanford Institute as an academic & Research sharing network. But now it has totally evolved into commercial entity and the new internet age is the known as the “Information age”. The

information age has turned time into real money, where the correct and timely information is the biggest need and asset. Information is now considered as the creative capital and every organization needs.

The accurate and well-timed information is the key to take the quick and best decision for gaining an edge over the potential competitors. The market sustainability and business stability fully depends on the information capital.

In infancy of Internet, MAC addresses played a wonderful role, but they became problematic with growing nodes in Internet. The new concept of logical (IP) addressing resolved that addressing issue. IP addresses have definitely revolutionized the world and there are uncountable advantages of using the logical addresses. The primary advantage of IP addressing is their dynamic nature i.e. they can be changed according to the user's or as per organizational need. Apparently, the MAC addresses or physical addresses were fixed and hence seem unimaginably solution. Due to this crucial concern and simplicity in usage, IP addresses superseded MAC addresses and the whole research was carried out keeping in mind[3]. The communication protocols and standards were developed for IP addresses rather than ethernet addresses. The over-dependant on IP addressing brought so many quandaries like depletion of IPv4 addresses and subsequent solutions like private addressing, NAT/ PAT, subnetting and supernetting, etc[1][7]. The advent of logical addressing over MAC addressing also requires special protocols like ARP, RARP, DHCP, BOOTP, etc to do the conversion from one to another[3]. Another reason for popularity of logical over physical addresses is the format. The IPv4 addresses are represented in dotted decimal form, while

the MAC addresses are usually characterized by the hexadecimal format, which is infact a bit hard to understand and employ. The MAC address details are described in the following diagram:

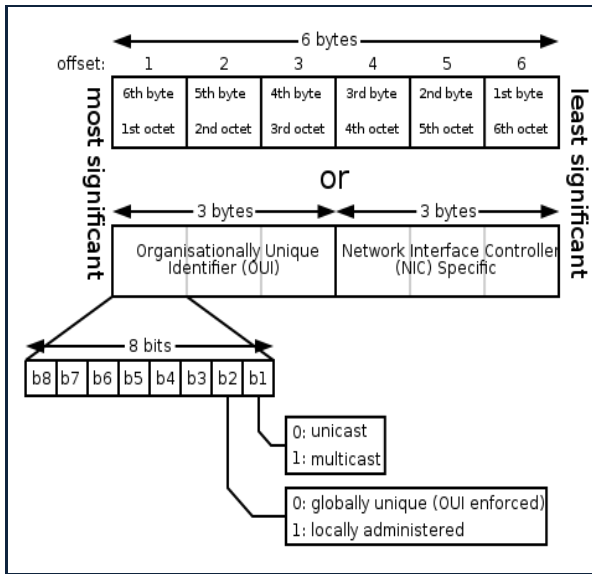


Fig 1. MAC address details

Apparently the format of next version of logical addressing i.e IPv6 or IPng is also hexadecimal. Moreover, the internet users don't need to know the Ethernet or IP address to the computer that they want to communicate. The whole communication from user's perspective just depends on the Domain Name System(DNS). Moreover, the jinx of fixed MAC address is over due to new features like MAC spoofing and dynamic MACs[7]. Some of the major hardware manufacturers and software giants like Apple have collaborated to revolutionize this concept.

II. DYNAMIC MAC & SPOOFING

The most pleasing development that took place in the addressing domain is the invention of "dynamic MAC addresses". There are softwares available in the market like SMAC to change the physical address of a machine. However, there are alternative ways of doing the same in different operating system, which will be discussed in the next section.

A. Windows Operating System

In case of Windows operating system like 7, XP, Server 2003, etc., the physical address can be modified with the help of windows registry[2]. The steps involved are as follows:

1. Go to Start -> Run, type "regedt32" to start registry editor.
2. Create a backup of the registry, in case the original physical address is needed. Click on "HKEY_LOCAL_MACHINE on Local Machine" sub-window. Then Click on the root key "HKEY_LOCAL_MACHINE". Finally, click on the drop-down menu "Registry -> Save Subtree As" and save the backup registry in to a file. Make sure that this file is kept in a safe place.

3. Go to "HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Control\ Class\ {4D36E972-E325-11CE-BFC1-08002BE10318}". Double click on it to expand the tree. The subkeys are 4-digit numbers, which represent particular network adapters. The subkeys starts with 0000, then 0001, 0002, 0003 and so on. Usually, most computers have only one NIC, so only 0000 subkey needs to be checked.
4. Once you selected the subkey (i.e. 0000), check if there is a keyword "NetworkAddress" exist in the right side of the window.
5. If "NetworkAddress" keyword exists, make sure it shows the keyword type is REG_SZ, and it should show as NetworkAddress:REG_SZ. Double click on the keyword NetworkAddress and the String Editor window will pop up. Enter the new MAC address you want to modify. Then click OK.
6. If "NetworkAddress" keyword does not exist, then create this new keyword by clicking on drop down menu "Edit -> Add Value". In the Add Value window, enter the value -> "Name: = NetworkAddress Data Type: = REG_SZ".
7. Reboot the system.

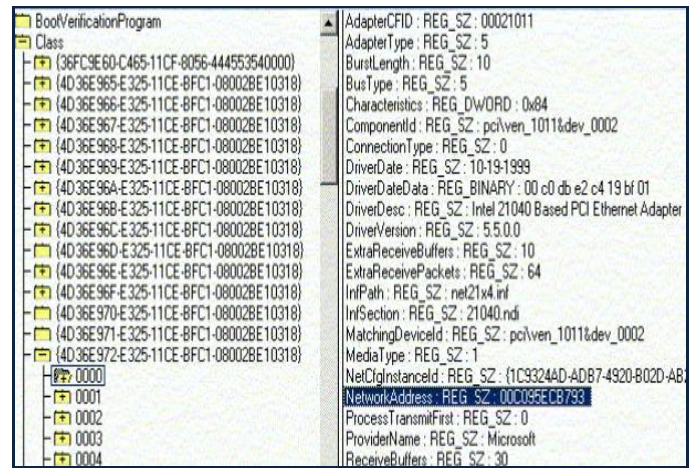


Fig 2: HKEY_LOCAL_MACHINE on Local Machine

B. Windows Operating System (NIC Dependant)

Another way of changing Ethernet address is dependant on the Network Interface Card(NIC). It is only applicable when a NIC supports Clone MAC address. The process id described as follows:

1. Go to Start->Settings->Control Panel and double click on Network and Dial-up Connections.
2. Right click on the NIC you want to change the MAC address and click on properties.
3. Under "General" tab, click on the "Configure" button.
4. Click on "Advanced" tab.

- Under "Property section", you should see an item called "Network Address" or "Locally Administered Address", click on it.
- On the right side, under "Value", type in the New MAC address that needs to be assigned to NIC. Usually this value is entered without the "-" between the MAC address numbers.
- Goto command prompt and type in "ipconfig /all" or "net config rdr" to verify the changes. If the changes are not materialized, then use the second method.
- If successful, reboot the system.

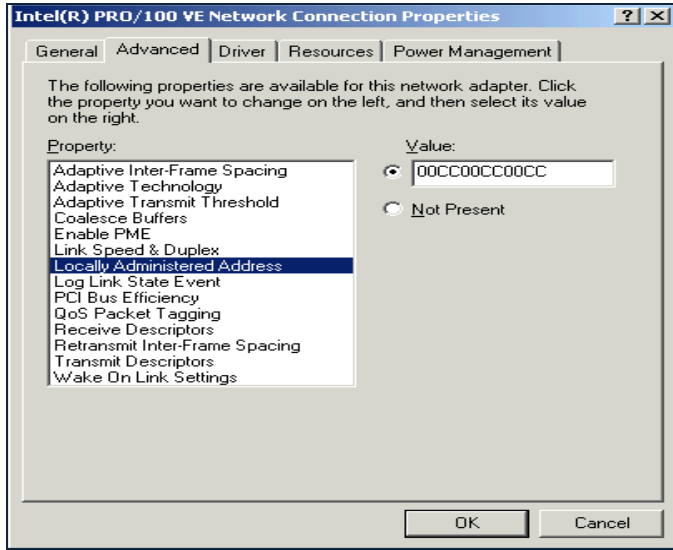


Fig 3: MAC Cloning in Windows OS

C. Linux Operating System

The MAC address changing can be pretty easy in Linux compared to Windows. The steps involved are as follow:

- The current Ethernet configuration can be viewed by issuing the "ifconfig" command.
- The physical address of the machine is specified as "HWaddr 00:A0:C9:29:3C:68".
- The MAC address can be altered by the command, "ifconfig hw ether".

```
[root]# ifconfig eth0 hw ether 01:02:03:04:05:06
[root]# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 01:02:03:04:05:06
inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:4 dropped:0 overruns:0 carrier:4
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:168 (168.0 b)
Interrupt:11 Base address:0xdf00 Memory:df9ff000-df9ff038
```

Fig 3: MAC Address Change Process in Linux

D. Appletalk Network

This network has an implicit competence to work on the principle of dynamic MAC addresses. Whenever a user requests to connect the computer to internet, the user is assigned a new MAC address dynamically. The provided MAC address is given randomly and it is not necessary that the user will get the same MAC address every time, the user connects to the internet. The need to spoof the MAC address by any tools or commands is not required. The users simply reconnect it to the network to obtain a new MAC address. These kinds of devices are made to provide high security to the users so that these cannot be easily traced by the hackers.

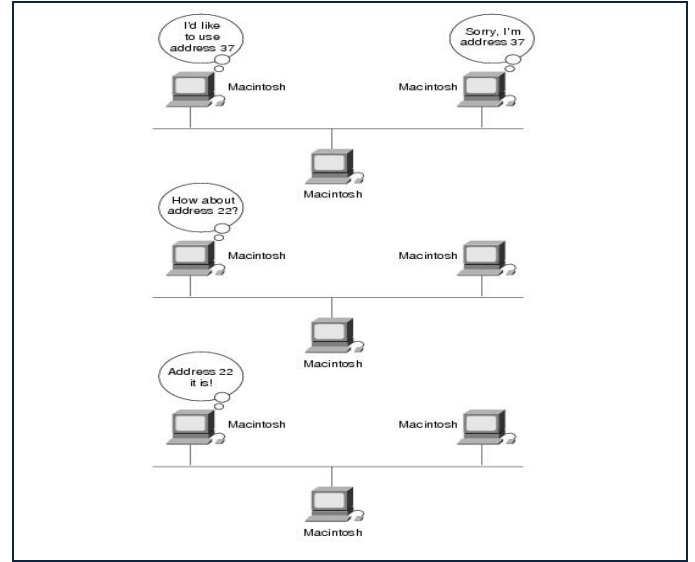


Fig 4: Appletalk Network in Macintosh OS

III. ELIMINATION OF ADDRESS RESOLUTION PROTOCOLS

The ARP and RARP protocols are usually implemented in most of the networks to resolve the mapping between logical addresses and physical addresses. The details of ARP and RARP are given as below:

A. Logical to physical address resolution

The Address Resolution Protocol(ARP) is primarily used to convert the IP addresses into MAC addresses. To do the address translation, there is a need of an ARP server, which holds the key to generate the link-local address from a corresponding logical address[4]. This is done with the help of ARP cache table. The ARP cache table can be displayed as:

State	Queue	Attempt	Time Out	Protocol Address	Hardware Address
R	5		900	180.3.6.1	ACAE32457342
F					
P	14	5		201.11.56.7	

R = resolved, P = pending, F = free (time to leave has expired)

Fig 5: Working of ARP Cache Table

The ARP cache table upholds the most recent mappings, hence increasing the efficiency of address translation. To maintain the network dynamics, each entry of ARP cache table has a timeout value. This helps in deleting the aged entries and keeping only current list in the table. The ARP cache is needed for basically two routing scenarios:

- i. To connect between two local hosts.
- ii. To connect between a router and a host.

B. Physical to logical address translation

There may arise some situation, where the Ethernet address needs to be converted into logical address. To compensate this particular need, mainly three protocols have been designed namely Reverse Address Resolution Protocol(RARP), Boot Protocol(BOOTP) and Dynamic Host Configuration Protocol(DHCP). With slight variations, all three protocols work in the same way i.e. they request the configured server to provide an IP address in correspondence to their MAC address[6]. Whenever, a machine is booted or rebooted, it sends IP address request to the preconfigured server. The server holds the data and replies back with all necessary details like IP address of the machine, IP address of name server, subnet mask and default gateway. This extra bit of information is usually provided by BOOTP and DHCP, which is typically required for diskless machines[5].

C. Advantage of using MAC addresses

The usage of MAC addresses in internal of the organization will eliminate the need for converting IP addresses to physical addresses and vice-versa. Moreover, the intra-organization communication will be more efficient when the need for address translation is eradicated. Some chief advantages of using MAC addresses in intra-organization communication are discussed as follows:

1. First of all, there will no need of configuring the ARP cache table on a dedicated server or maintaining a DHCP server[8].
2. The lookup time in ARP cache, resolution time and the total transfer time for sending packet between two internal hosts will be decreased to a great extent.
3. The requirement of maintaining the recent mappings and deleting old mappings is no longer needed.
4. The mapping between link-local and logical addressing can take long if number of host requesting for same are more than the server can handle. The increased number of pending requests may yield to the

denial of service by the resolution server. This seize of resolution server is also purged by use of MAC addresses.

5. The machines will be ready to communicate as soon as they are turned on. They need not wait for address resolution process to start commune.
6. Ultimately, the network bandwidth will be saved as a superfluous communication for address resolution is not involved.

IV. CONCLUSION

The paper discusses a novel approach of using the physical addressing only, instead of both logical and physical addressing while communicating within an organization. The paper highlights the drawbacks of logical addressing like maintaining the ARP cache table and time needed to lookup and resolve addressing. Some great technological changes in MAC addressing that have taken place in past few years have also been discussed. This paper compares the MAC addressing with the IP addressing, and explains why the need to use IP addresses for intra-organization communication can be overridden. The proposed MAC based routing approach is superior, proficient and swift, which can definitely pave the way for new age of communication between devices within same LAN.

REFERENCES

- [1] P.P Charles & P.L. Shari, "Security in Computing: 4th edition", Prentice-Hall Inc., 2008.
- [2] K. Lai, "Spoofing MAC address on Windows", CISSP, CISA, KLC Consulting Inc., article available online at http://www.klcconsulting.net/change_mac_w2k.htm
- [3] A.S. Tanenbaum, "Computer Networks", Fourth Edition, Prentice hall, 2004.
- [4] M. Oh, Y. Kim, S. Hong & S. Cha., "Agent-based secure cache management", IET Communications, Vol. 6, No. 7, pp. 685–693, May 2012.
- [5] S. Nam, D. Kim, and J. Kim, "Enhanced arp: preventing arp poisoning based man-in-the-middle attacks," Communications Letters, IEEE, vol. 14, no. 2, pp. 187–189, 2010.
- [6] B. Issac and L. Mohammed, "Secure unicast address resolution protocol (s-uarp) by extending dhcp," in Networks, Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on, vol. 1. IEEE, pp. 6., 2005.
- [7] I. Teterin, "Antidote," 2002, article available online at <http://online.securityfocus.com/archive/1/299929>
- [8] E.C. Sasu, O.Prostean, "Using Constant Traffic to Specific IP Destinations for Detecting Spoofed MAC Addresses in Local Area networks", ICC-CONTI Timisoara, Romania, ISBN 978-1-4244-7432-5, May 27-29, 2010