

MAC Spoofing Detection Via Wireshark

Ms. Konika Abid , Mr. Ajay Kumar Singh

Abstract—When computers are, connect on any network a network card is used, known as NIC card which is having a MAC address. This address is use to distinguish one system from another we may say that it is the physical address given by the manufacturer to provide a unique identity to equipment. We have studied that MAC address is permanent and cannot be changed but there are different ways in which MAC address of equipments could be changed whether it is a pc/laptop or mobile. We could use wire shark to know the changed MAC address of any system for which the packet is been send or received. The change in MAC is called MAC spoofing, which is having advantages as well as disadvantages.

Index Terms— MAC, NIC, ARP, LAN, IP, OS.

I. INTRODUCTION

Media access control (MAC) stands for media access control. MAC addresses [1] are permanent addresses, which are assigned to every network connected devices. MAC address also is known as physical address, which is unique and cannot be changed. Computer network uses two types of addresses to deliver network data. The transmission control address or node address is use to differentiate between different nodes connected to transport medium segment. The transport protocol known as Ethernet uses a MAC 48-bit address (12- digit hexadecimal number) for this purpose. A MAC address usually encodes the manufacturer's registered identification number. It is also known as Ethernet hardware address (EHA), hardware address, adapter address, or physical address. The MAC protocol encapsulates a payload data by adding a 14- byte header protocol control information (PCI) before the data and appending a 4-byte cyclic redundancy check (CRC) after the data. The entire frame proceeds by a small idle period (the minimum inter-frame gap, 9.6 μ s and an 8-byte preamble including the start of frame delimiter. The MAC address is the physical address of the machine, the physical identifier of the host on a segment. It needs to be unique only on a given segment. Theoretically two host could have same transport layer address provided they were not connected to the same network segment but both transport address and network address are two different things.

Konika abid , and M.Tech Student, CSE Deptt.from Meerut Institute of Engineering and Technology, Meerut, U.P, India.

Dr, Ajay Kumar., Professor (CSE),Meerut Institute of Engineering & Technology, Meerut, U.P, India.

In other words, we call network address as IP address, which is used as the unique identifier throughout the complete network, and it is statically defined 32-bit address. These network protocols are use to exchange data between different networks. MAC is assigned by the manufacturer and is burned into the ROM of the NIC card [2], which is a layer2 device of the OSI model [3]. This is divided into 24-bit vendor code and 24-bit serial address. These addresses are used as a network addresses for most IEEE 802 [4] network technologies, including Ethernet and Wi-Fi [5].

II. RULES FOR WRITING MAC ADDRESS

Institute of Electrical And Electronics Engineers (IEEE) manages MAC addressing rules. Three numbering spaces, managed by, are in common use for managing a MAC address: MAC-48, EUI-48, and EUI-64. Where, "EUI" stands for Extended Unique Identifier.

A. Notations for MAC Address

MAC address represented, in hexadecimal form. In these 12 hexa digits, starting 6 digits are Ethernet [6] interface given by IEEE and the last/right 6 digits which specify the interface serial number provided by the manufacturer. The Standard IEEE 802 format for printing MAC-48 addresses [7] is six groups of two hexadecimal digits separated by hyphens (-) or colon (:). in transmission order e.g. 01-12-23-34-56-AB.

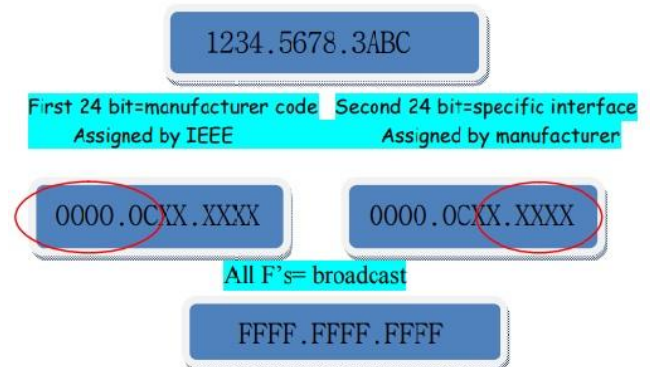


Fig. 1 Notation of MAC address.

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. Address either can be universally administered address or locally administered address. A universally administered address is uniquely assign to a device by its manufacturer, which is sometimes known as burned in address (BIA). The 48-bit address space contains potentially 248, 281, 474, 976, 710 or 656 possible MAC address.

III. TYPES OF MAC ADDRESSES

MAC addresses are mainly of two types:

- A. Universal
- B. Local

The manufacturer assigns the universally administrated address. The first three octets in transmission order identify the organization and is known as Organizationally Unique Identifier (OUI) the remaining octets are assigned by the manufacturer in any manner subject to the constraint of uniqueness. A network administrator, overriding the burned-in address, assigns a locally administered address to a device.

IV. . VULNERABILITIES WITH MAC ADDRESS

Even if the network is secure, enough then also the MAC address is send over the network regularly and some applications uses these to hack the network.

V. MAC SPOOFING

We have studied that MAC address are physical address, which cannot be change but there is a possibility to change the MAC address of almost every hardware. This process of changing the MAC address is known as MAC spoofing [8] which is different from that of IP spoofing [9] as in it the sender spoofs the receivers address as a request where as in this spoofing party gets the response

A. Advantages of MAC Spoofing

Some licenses are also hook up to specific MAC addresses so reverting the MAC address physical storage may help in using the software in simple words it can estimate the use of re-register the software. Perform security vulnerability testing, penetration testing on MAC address based authentication and authorization systems, i.e. wireless Access Points. It also helps in checking network management tools [10] and troubleshooting the system problems. Some Cable Modem Internet Service Provider assign IP addresses based on the device MAC addresses. For whatever reason, if you need to swap two systems regularly to connect to the cable modem, it would be a lot easier to change the MAC addresses rather than to change Network Interface Card (NIC). Test Intrusion Detection Systems (IDS) [11], whether they are Host and Network Based IDS.

B. Disadvantages of Spoofing MAC Address

Now a day it is pretty simple to find the different wireless networks using our phones or laptops, so any unauthorized user could use MAC spoofing easily to get access to these networks depending on the level of security. It is possible to track illegal internet traffic to a specific IP and to retrieve the name and address of the IP's registrant. MAC spoofing allows unauthorized access to someone else's network; therefore, responsibility for any illegal activity will fall on the authentic user. As a result, the real offender may go undetected by law enforcement.

VI. METHOD TO CHECK YOUR MAC ADDRESS

A. Checking of MAC address for the laptop or PC is shown in figure 2.

B. Checking of MAC address for the mobile is shown in figure 3.

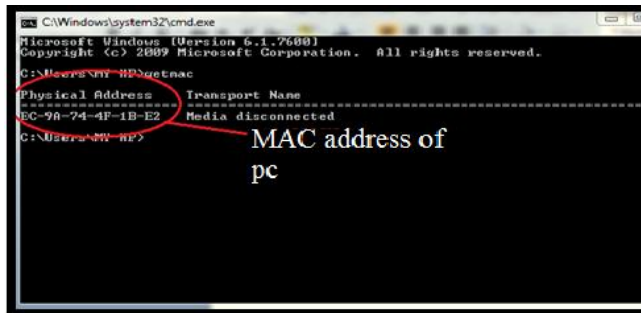


Fig. 2 Checking MAC address of laptop.



Fig. 3 Checking MAC address of mobile.

A. Checking of MAC address in pc.

- Go to start and type cmd in search bar .
- Write getmac and press enter. and colons.

B. Steps for checking MAC of mobile.

Go to setting. Click about phone in system column.Now go to Status. In status, you will see Wi-Fi MAC address or the MAC address of the mobile as shown in figure 3.

VII. SPOOFING/CHANGING MAC ADDRESS OF PC FOR WINDOWS

Following is the method by which MAC address of pc could be changed.

- 1) Open run dialog box and write REGEDIT.

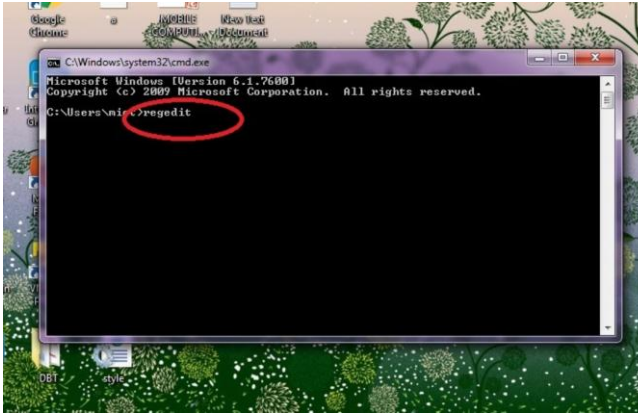


FIG. 4 OPEN REGEDIT.

2) Open registry editor as shown in the figure 4 which allow changing the network cards settings.

- 3) Navigate the registry key, shown in figure 5:
 - i. HKEY_LOCAL_MACHINESYSTEM
 - ii. CurrentControlSet
 - iii. Control
 - iv. Class
 - v. 4D36E972-E325-11CE-BFC1-08002BE10318

4) Open each folder one by one and check NetCfgInstanceID field and match it with the MAC address of your pc refer to figure 2 in above pages.

5) Right click on the folder that matches your device and then Select New → String Value. Name the new value “Network Address” as shown in figure 6.

6) Double-click the new Network Address entry. In the “Value data” field, enter your new MAC address. Note: MAC addresses should be of 12-digit and should be entered without any dashes or colons. For example, you would enter “2A1B4C3D6E5F” as given in figure 7.

7) Ensure that MAC should be formatted properly otherwise it is not accepted. DEXXXXXXXXXX

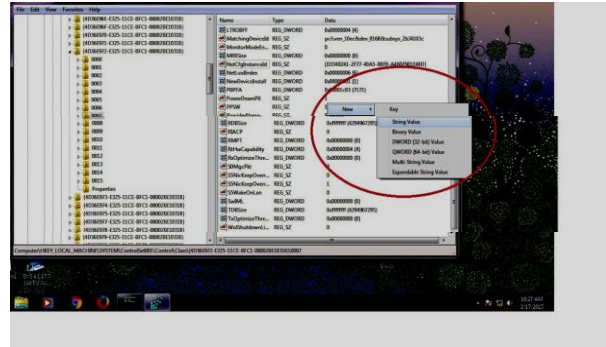


Fig. 6 Opening string value

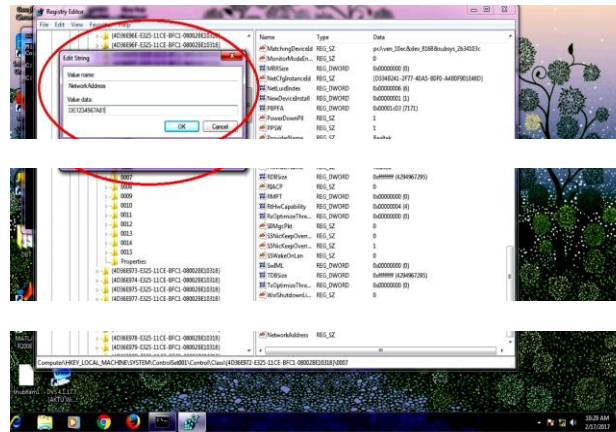


Fig. 7 Assigning MAC value

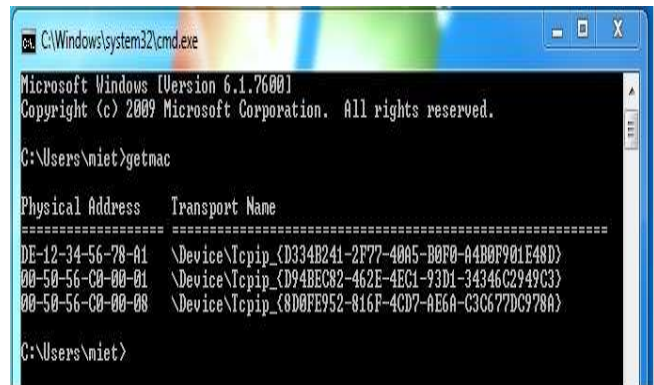


Fig. 8

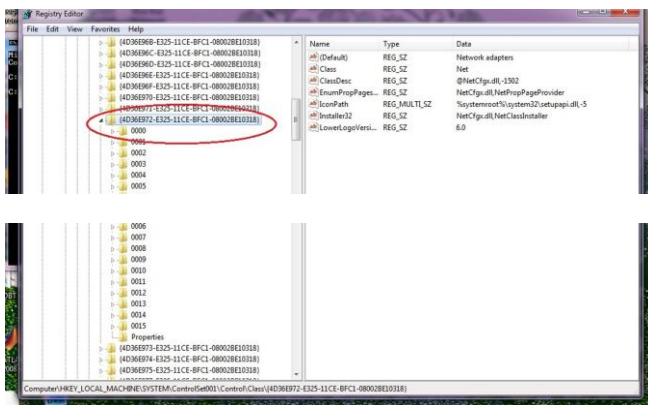


Fig. 5 Navigating registry key.

VIII. MAPPING MAC ADDRESS WITH THE HELP OF WIRESHARK

To check our MAC address using WIRESHARK, we follow the following steps: Firstly Start capturing the packets. Then Stop capturing the packets. Apply ARP filter shown in figure 9.

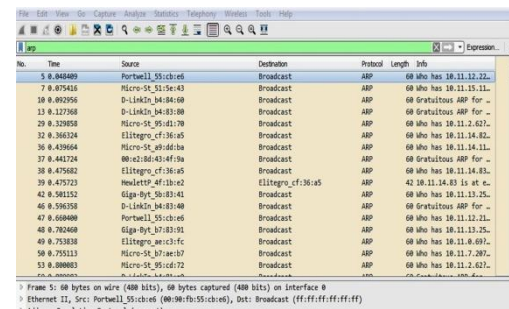


Fig. 9 ARP filters applied on packets.

You will receive all the ARP packets as the output. Now select any of the packets. You will see its destination and source details in the address resolution column. There you will see the MAC address of the source as well as of the target. For example, see figure 10 for understanding this concept.

A. Before Spoofing

- 1) We have already checked our MAC address and have changed it. We can analyse our MAC as well as the IP address with the help of wireshark. To perform this we ping our system from example, you would enter “2A1B4C3D6E5F” as given in figure 7.
- 2) Ensure that MAC should be formatted properly otherwise it is not accepted.
 DEXXXXXXXXXX
 another system and analyse these packets in wireshark. We simplified our work by applying filter ICMP as shown in figure 11. Once we apply this filter we find all the ICMP packets at once and can easily search our ping request packet.

B. After spoofing

We see that when we again ping our system from another system and repeats the same process. Our IP address remains the same where as the MAC changes as shown in figure 12.

```

Frame 39: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: HewlettP_4f:1b:a2 (ec:9a:74:4f:1b:a2), Dst: Elliot
Address Resolution Protocol (reply)
Hardware type: Ethernet (I)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HewlettP_4f:1b:a2 (ec:9a:74:4f:1b:a2)
Sender IP address: 10.11.11.83
Target MAC address: Ellitagr_cf:36:a9 (10:70:42:cf:36:a9)
Target IP address: 10.11.11.75
    
```

Fig. 10 Address resolution column with MAC address.

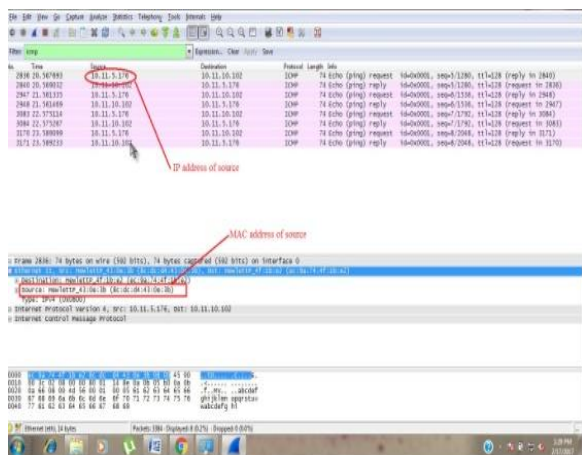


Fig. 11 ICMP packets with both IP and MAC addresses.

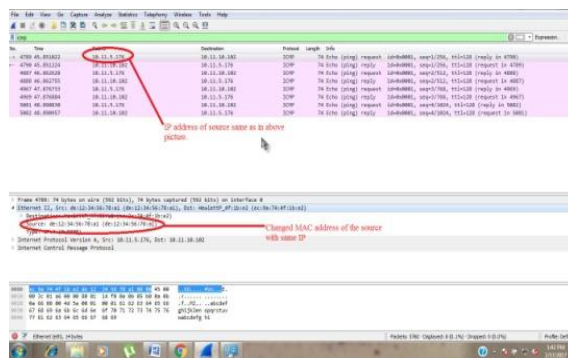


Fig. 12 Same IP addresses with change MAC address.

IX. CONCLUSION

In this paper, we have discussed about the MAC address also known as physical address, which is permanent, but it can be altered virtually. By following the methods discussed above we can we can compare both the MAC and could generate the beep or alert message.

This spoofed address could be detected by the WIRESHARK easily. We can detect the changes done in MAC address and accordingly we can take preventive steps.

X. ACKNOWLEDGMENT

We are thankful to our management and Chairman for his kind support and motivation.

REFERENCES

- [1]. Deepak gupta, Gaurav tiwari, Yachin Kapoor and Praveen kumar, “media access control (mac) mac spoofing and is countermeasure”, International Journal of Recent Trends in Engineering, Vol. 2, No. 4, pp.17-21, November 2009.
- [2]. W. Feng., “Network interface cards as first-class citizens”, Invited Talk, The Ohio State University, 1999.
- [3]. Sumit Kumar, Sumit Dalal and Vivek Dixit, “The OSI Model: Overview On The Seven Layers Of Computer Networks”, International Journal of Computer Science and Information Technology Research Vol. 2, Issue 3, pp. 461-466, July -September 2014.
- [4]. Jasleen Kaur and Shakti Nagpal, “Review Paper on Comparative Study of IEEE Protocols Suite”, International Journal of Advanced Research in Computer Science and Software Engineering, 2014, Vol. 4, pp. 1490-1500, 5 May 2014.
- [5]. Mathieu Cunche, “I know your MAC Address: Targeted tracking of individual using Wi-Fi”, HAL Id: hal-00858324 <https://hal.inria.fr/hal-00858324>, 3 October 2013.
- [6]. Bruce Lowekamp, David R. O'Hallaron and Thomas R. Gross. “Topology Discovery for Large Ethernet Networks”, In Proceedings of ACM SIGCOMM, August 2001.
- [7]. Umang Garg, Pushpneel Verma ,Yudhveer Singh Moudgil and Sanjeev Sharma, “MAC and Logical addressing (A Review Study)”, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 474-480.
- [8]. Mrs. Hatkar Archana A., Ms. Varade Gauri A. and Mr. Hatkar Arvind P, “Media Access Control Spoofing Techniques and its Counter Measures”, International Journal of Scientific & Engineering Research, Vol. 2, pp.1-5, 6 June 2012.
- [9]. Sharmin Rashid and Subhra Prosun Paul, “Proposed Methods of IP Spoofing Detection & Prevention”, International Journal of Science and Research (IJSR), Vol. 2, Issue 8, pp. 438-443, August 2013.
- [10]. G.S. Nagaraja, Ranjana R.Chittal, Kamod Kumar, “Study of Network Performance Monitoring Tools-SNMP”, IJCSNS International Journal of Computer Science and Network Security, Vol.7, No.7, pp. 1-5, July 2007.

- [11]. Nicholas, J.Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee and Ronald A.Olsson, "A Methodology for Testing Intrusion Detection System", National Security Agency INFOSEC University Research Program, 17th National Computer Security Conference in Baltimore, MD, pp. 1-25, October 1994.
- [12]. <http://www.wikihow.com/Change-a-Computer's-Mac-Address-in-Windows>



KONIKA ABID: She have done b.tech from Subharti University and M.Tech Student, CSE Deptt. from Meerut Institute of Engineering and Technology, Meerut, U.P, India.



Dr. Ajay Kumar Singh: Born in 1974 at Dhanbad (Jharkhand), India. He had done B.E (Computer Science & Engg.) from Kumaon Engineering College, M. Tech (I.T) Allahabad, Ph. D (Computer Science & Engg.) Jaypee University of Information Technology. **Work Experience:** He had been in different institution / university like Radha Govind Engineering College, Meerut, (U.P) here he worked as HoD, Sir Padampat Singhania University, Bhatewar, Udaipur, Rajasthan, Jaypee University of Information Technology, Wagnaghat, Solan

(H.P), Mody College of Engineering and Technology, Lakshmanagarh, Sikar, Rajasthan, Regional Engineering College (Now N.I.T.) Kurukshetra (Haryana), Software Solution Integrated Ltd. (Delhi). Now he is working with MIET, Meerut, U. P. He has published many papers in international Journals like PIER, Asia Magazine EFY Elsevier, many papers in international Conference out of which 4 of them in IEEE, He has chaired two IEEE conference at ABES Engg. College and Galgotia University. Published paper in Electronic For You, Springer LNCS and presented his papers at several places like Bangalore, Pune, IT B.H.U, USA (Washington DC).