A Novel Approach for Spoofing Media Access Control Address

G. Ram Sekhar, Dwarampudi Rajasekhar Reddy, R. Srinivas
Sri Sai Aditya Institute of Science & Technology,

Abstract: - **Every network adapter has a Media Access Control address. It is permanently embedded in the fireware of the adapter. We may also hear people refer to the Media access control address as MAC address, the physical address, the hardware address, or the adapter address. An attacker wishing to disrupt a wireless network has a wide arsenal available to them. Many of these tools rely on using a faked MAC address, masquerading as an authorized client. Using this spoofing of media access control address, an attacker can launch denial of service attacks, bypass access control mechanisms as a client.**

Keywords:-MAC Address, fireware, Network adapter, spoofing and Network address.

1. INTRODUCTION

MAC addresses have long been used as the singularly unique layer 2 network identifier in LANs. Through controlled, organizationally unique identifiers (OUI) allocated to hardware manufacturers, MAC addresses are globally unique for all LAN-based devices in use today. In many cases, the MAC address of a workstation is used as an authentication factor or as a unique identifier for granting varying levels of network or system privileges to a user.

This method of client tracking and authentication is also employed in 802.11 wireless networks. Attackers targeting wireless LANs utilize the ability to change their MAC address to circumvent network security measures: an attacker with minimal skill might alter their MAC address in an effort to masquerade or hide their presence, an attacker with minimally more skill might change their MAC address to one that is otherwise authorized to bypass access control lists or to escalate network privileges.

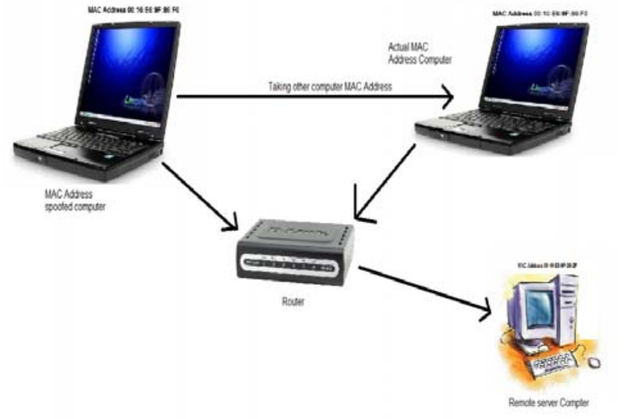

MAC Address 00 16 E6 9F 86 F6
MAC Address 00 10 E6 9F 86 F2
Actual MAC
Address Computer
Taking other computer MAC Address
MAC Address
spoofed computer
Router
Remote server Compter

Figure 1

2. NOTATIONAL CONVENTIONS

The standard IEEE.802 format for printing MAC-48 addresses in the form is six groups of two hexadecimal digits, these MAC Address are separated using colons (:) or hyphens (-), in transmission order, for example the order will be as ab:cd:ef:12:03:45 or ab-cd-ef-12-03-45. Another convention used by networking equipment uses three groups of four hexadecimal digits separated by dots (.) i.e., abcd.ef12.0345, these 4 bytes separated with dot make 2 octets each.

Address Details

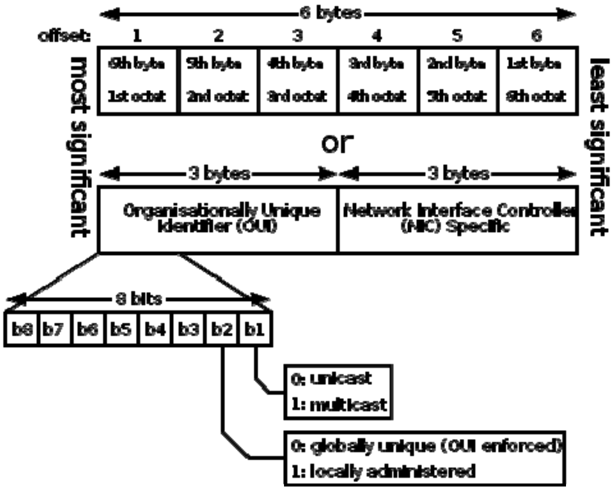


Figure 2

In the above Figure 2 we are showing that MAC Address details that is based on the least significant and most significant bits. Here the original IEEE 802 MAC Address comes from the original Xerox Ethernet Addressing schema and the address space contains potentially 2^{48} or 281,474,976,710,656 possible MAC Addresses. The division of a pair of numbers in the MAC address is called one octet so the original MAC Address will contain 6 octets. In the order of transmission ,the first three octets identify the organization that issued the identifier and are known as the Organizationally Unique Identifier, that is OUI.zd the following three (MAC-48 and EUI-48) or five (EUI-64) octets assigned by that organization to make constraint of uniqueness which are Network Interface Controller (NIC) Specific.

The IEEE experts the MAC-48 space to be exhausted no sooner than the year 2100. Addresses are distinguished by setting the universally administered and locally administered through the second least-significant bit of the most significant byte of the address. Here in this bit 0 will indicate the universally administered and 1 will indicate locally administered. By considering example address 12-34-56-AB-CD-EF the most significant byte is 12 (hex decimal number), and EF will indicate the least significant byte.

If the least significant bit of the most significant octet of an address is set to 0 (zero), the frame is meant to reach only one receiving NIC. This type of transmission is called unicast. A unicast frame is transmitted to all nodes within the collision domain, which typically ends at the nearest network switch or router. Only the node with the matching hardware MAC address will accept the frame; network frames with non-matching MAC-addresses are ignored, unless the device is in promiscuous mode.

If the least significant bit of the most significant address octet is set to 1, the frame will still be sent only once; however, NICs will choose to accept it based on different criteria than a matching MAC address: for example, based on a configurable list of accepted multicast MAC addresses. This is called multicast addressing.

The following technologies use the MAC-48 identifier format:

- Ethernet
- 802.11 wireless network
- IEEE 802.5 token ring
- ATM-switched virtual connections only
- Fiber channel and Serial attached SCSI

INDIVIDUAL ADDRESS BLOCK

An Individual_Address_Block is a 24-bit OUI managed by the IEEE Registration Authority, followed by 12 IEEE-provided bits (identifying the organization), and 12 bits for the owner to assign to individual devices. An IAB is ideal for organizations requiring fewer than 4097 unique 48-bit numbers (EUI-48).

USAGE IN HOSTS

Although intended to be a permanent and globally unique identification, it is possible to change the MAC address on most modern hardware. Changing MAC addresses is necessary in network_virtualization. It can also be used in the process of exploiting security vulnerabilities. This is called MAC_spoofing.

A host cannot determine from the MAC address of another host whether that host is on the same link (network_segment) as the sending host, or on a network segment bridged to that network segment.

In TCP/IP networks, the MAC address of an interface can be queried knowing the IP address using the Address Resolution Protocol (ARP) for Internet Protocol Version 4 (IPv4) or the Neighbor Discovery Protocol (NDP) for IPv6. On broadcast networks, such as Ethernet, the MAC address uniquely identifies each node on that segment and allows frames to be marked for specific hosts. It thus forms the basis of most of the Link layer (OSI Layer 2) networking upon which upper layer protocols rely to produce complex, functioning networks.

USAGE IN SWITCHES

Layer 2 switches use MAC addresses to restrict packet transmission to the intended recipient. However, the effect is not immediate (address learning).

Many higher-end switches currently in distribution are Layer 3 switches. Such a switch supports IP multicast and therefore uses the IP address for routing. The switch preserves the MAC address for compatibility but does not need to use it for routing.

BIT-REVERSED NOTATION

The standard notation, also called canonical format, for MAC addresses is written in transmission bit order with the least significant bit transmitted first, as seen in the output of the iproute2 /ipconfig command, for example.

However, since IEEE 802.3 (Ethernet) and IEEE 802.4 (Token Bus) send the bytes (octets) over the wire, left-to-right, with least significant bit in each byte first, while IEEE 802.5 (Token Ring) and IEEE 802.6 send the bytes over the wire with the most significant bit first, confusion may arise when an address in the latter scenario is represented with bits reversed from the canonical representation. For example, an address in canonical form 12-34-56-78-9A-BC would be transmitted over the wire as bits 00010010 00110100 01010110 01111000 10011010 10111100 in the standard transmission order (least significant bit first). But for Token Ring networks, it would be transmitted as bits 00111101 01011001 00011110 01101010 00101100 01001000 in most-significant-bit first order. The latter might be incorrectly displayed as CB-A9-87-65-43-21. This is referred to as bit-reversed order, non-canonical form, MSB format, IBM format, or Token Ring format, as explained in RFC 2469. Canonical form is generally preferred, and used by all modern implementations.

When the first switches supporting both Token Ring and Ethernet came out, some did not distinguish between canonical form and non-canonical form and so did not reverse MAC address bits as required. This led to cases of duplicate MAC addresses in the field.

3. FINDING MAC ADDRESS

3.1 FINDING YOUR MAC ADDRESS ON WINDOWS 95 AND UP

Method 1:-

1. Click the Windows (Start) button and type **cmd** in the search box. Hit Enter
2. In the black window that opens, type **getmac /v** then hit Enter. It show MAC Address look something like XX-XX-XX-XX-XX-XX
3. Register your MAC address accordingly

Method 2:-

1. Click the Windows (Start) button, select *Run* then type **cmd** then hit Enter

2. In the black window that opens, type **ipconfig /all**. A page of information will scroll past including the Physical Address or MAC address
3. Make the window larger then scroll back through the information to find your wired and wireless MAC Addresses will be labeled and will look something like XX-XX-XX-XX-XX-XX
4. Register your MAC address accordingly

Method 3:-

1. Click the Windows (Start) button, select *Run* then type **cmd** then hit Enter
2. In the black window that opens, type **arp –a** then hit Enter. Your wired and wireless MAC Addresses will be appear with Internet Addresses, Physical Addresses and Type of Addresses will be present in that we will find IP Addresses, MAC Address and Type will be labeled and will look something like 192.172.21.1, XX-XX-XX-XX-XX-XX and Static.
3. Register your MAC address accordingly

3.2 STANDARDS GROUP MAC PUBLIC LISTING

Table 3.1-IEEE Standards 802.1D and IEEE Standards 802.1Q Reserved Addresses

Group MAC address value	Organization using the value	Standard using the value	Notes
01-80-C2-00-00-00	IEEE 802	IEEE Std 802.1D IEEE Std 802.1Q	IEEE Std 802.1D Bridge Group Address
01-80-C2-00-00-01	IEEE 802	"	IEEE MAC-specific control protocols
01-80-C2-00-00-02	IEEE 802	"	IEEE Std 802.3 Slow Protocols multicast address
01-80-C2-00-00-03	IEEE 802	"	IEEE Std 802.1X PAE address
01-80-C2-00-00-04	IEEE 802	"	IEEE MAC-specific control protocols
01-80-C2-00-00-05	IEEE 802	"	Reserved for media access method specific use
01-80-C2-00-00-06	IEEE 802	"	Reserved for future standardization
01-80-C2-00-00-07	IEEE 802	"	Reserved for future standardization
01-80-C2-00-00-08	IEEE 802	"	Provider Bridge group address
01-80-C2-00-00-09	IEEE 802	"	Reserved for future standardization
01-80-C2-00-00-0A	IEEE 802	"	Reserved for future standardization
01-80-C2-00-00-0B	IEEE 802	"	Reserved for future standardization
01-80-C2-00-00-0C	IEEE 802	"	Reserved for future standardization
01-80-C2-00-00-0D	IEEE 802	"	Provider Bridge MVRP address
01-80-C2-00-00-0E	IEEE 802	"	Std 802.1AB Link Layer Discovery Protocol address
01-80-C2-00-00-0F	IEEE 802	"	Reserved for future standardization

Table 3.2-Standard Group MAC Addresses

Group MAC address value	Organization using the value	Standard using the value	Notes
01-80-C2-00-00-10	IEEE 802	IEEE Std 802.1D	All LANs Bridge Management Group Address (deprectated)
01-80-C2-00-00-11	IEEE 802	IEEE Std 802.1E	Load Server Generic Address
01-80-C2-00-00-12	IEEE 802	IEEE Std 802.1E	Loadable Device Generic Address
01-80-C2-00-00-13	IEEE 1905	IEEE Std 1905.1	Transmission of IEEE 1905.1 control packets
01-80-C2-00-00-14	ISO/IEC JTC1/SC6	ISO/IEC 10589	All Level 1 Intermediate Systems Address
01-80-C2-00-00-15	ISO/IEC JTC1/SC6	ISO/IEC 10589	All Level 2 Intermediate Systems Address
01-80-C2-00-00-16	ISO/IEC JTC1/SC6	ISO/IEC 10030	All CONS End Systems Address
01-80-C2-00-00-17	ISO/IEC JTC1/SC6	ISO/IEC 10030	All CONS SNARES Address
01-80-C2-00-00-18	IEEE 802	IEEE Std 802.1B	Generic Address for All Manager Stations
01-80-C2-00-00-19	unassigned		
01-80-C2-00-00-1A	IEEE 802	IEEE Std 802.1B	Generic Address for All Agent Stations
01-80-C2-00-00-1B	ISO/IEC JTC1/SC6	ISO/IEC 9542	All Multicast Capable End Systems Address
01-80-C2-00-00-1C	ISO/IEC JTC1/SC6	ISO/IEC 9542	All Multicast Announcements Address
01-80-C2-00-00-1D	ISO/IEC JTC1/SC6	ISO/IEC 9542	All Multicast Capable Intermediate Systems Address
01-80-C2-00-00-1E	ISO/IEC JTC1/SC6	ISO/IEC 8802-5	All DTR Concentrators MAC Group Address
01-80-C2-00-00-1F	unassigned		
01-80-C2-00-00-20 — 01-80-C2-00-00-2F	IEEE 802	IEEE Std 802.1Q	Reserved for use by Multiple Registration Protocol (MRP) applications

Group MAC address value	Organization using the value	Standard using the value	Notes
01-80-C2-00-00-30 — 01-80-C2-00-00-3F	IEEE 802	IEEE Std 802.1ag	Destination group MAC addresses for CCM and Link trace messages
01-80-C2-00-00-40 to 01-80-C2-00-00-4F	IETF	TRILL	Group MAC addresses used by the TRILL protocols
01-80-C2-00-00-40 — 01-80-C2-00-00-FF	unassigned		
01-80-C2-00-01-00		ISO/IEC 9314-6	Ring Management Directed Beacon Multicast Address
01-80-C2-00-01-01 — 01-80-C2-00-01-0F	ISO/IEC JTC1/SC25		Assigned to ISO/IEC JTC1/SC25 for future use
01-80-C2-00-01-10	ISO/IEC JTC1/SC25	ISO/IEC 9314-6	Status Report Frame Status Report Protocol Multicast Address
01-80-C2-00-01-11 — 01-80-C2-00-01-1F	ISO/IEC JTC1/SC25		Assigned to ISO/IEC JTC1/SC25 for future use
01-80-C2-00-01-20	ISO/IEC JTC1/SC25	ISO/IEC 9314-2	All FDDI Concentrator MACs
01-80-C2-00-01-21 — 01-80-C2-00-01-2F	ISO/IEC JTC1/SC25		Assigned to ISO/IEC JTC1/SC25 for future use
01-80-C2-00-01-30	ISO/IEC JTC1/SC25	ISO/IEC 9314-6	Synchronous Bandwidth Allocation Address
01-80-C2-00-01-31 — 01-80-C2-00-01-FF	ISO/IEC JTC1/SC25		Assigned to ISO/IEC JTC1/SC25 for future use
01-80-C2-00-02-00 — 01-80-C2-00-02-FF	ETSI		Assigned to ETSI for future use
01-80-C2-00-03-00 — 01-80-C2-FF-FF-FF	unassigned		

Table 3.3-Group MAC Addresses Used in ISO 9542 ES-IS Protocol

Group MAC address value	Organization using the value	Standard using the value	Notes
09-00-2B-00-00-04	ISO/IEC JTC1/SC6	ISO 9542	All End System Network Entities Address
09-00-2B-00-00-05	ISO/IEC JTC1/SC6	ISO 9542	All Intermediate System Network Entities Address

Table 3.4-Locally Administered Group MAC Addresses Used by IEEE Std 802.5 (IEEE Std 802.5 Functional Addresses)

Group MAC address value	Organization using the value	Standard using the value	Notes
03-00-00-00-00-08	IEEE 802	IEEE Std 802.5	Configuration Report Server (CRS) MAC Group Address
03-00-00-00-00-10	IEEE 802	IEEE Std 802.5	Ring Error Monitor (REM) MAC Group Address
03-00-00-00-00-40	IEEE 802	IEEE Std 802.5	Ring Parameter Server (RPS) MAC Group Address
03-00-00-00-01-00	IEEE 802	ISO 9542	All Intermediate System Network Entities Address
03-00-00-00-02-00	ISO/IEC JTC1/SC6, IEEE 802	ISO 9542, and IEEE Std 802.5	All End System Network Entities Address, and Lobe Media Test (LMT) MAC Group Address
03-00-00-00-04-00	IEEE 802	IEEE Std 802.1B	Generic Address for all Manager Stations
03-00-00-00-08-00	IEEE 802	ISO/IEC 10030	All CONs SNARES Address
03-00-00-00-10-00	IEEE 802	ISO/IEC 10030	All CONs End System Address
03-00-00-00-20-00	IEEE 802	IEEE Std 802.1E	Loadable Device Generic Address
03-00-00-00-40-00	IEEE 802	IEEE Std 802.1E	Load Server Generic Address
03-00-00-40-00-00	IEEE 802	IEEE Std 802.1B	Generic Address for all Agent Stations

After examining this trace more closely however, we see that the 802.11 sequence numbers for Vic’s MAC address (“00:02:2d:38:83:2c”) are not in sequence with the previously established baseline. Rather, the sequence number pattern more closely reflects that of Eve in the range 62-65. With this information, we can match the activity from the MAC address “00:02:2d:38:83:2c” as spoofed MAC activity from Eve. Problems with Sequence Number Analysis In order to identify out-of-order sequence numbers as having originated from a spoofed MAC address, we need to establish a baseline of monitored MAC addresses and the sequence numbers in use. With a fixed access point and fixed IDS appliance (or IDS code on an access point), we can reliably track sequence numbers for the access point by capturing all wireless traffic in the area. If we wish to monitor client MAC addresses and their sequence numbers however, we must be sensitive to roaming clients leaving the range of monitoring by the layer 2 wireless IDS. If the layer 2 anomaly-based intrusion detection system tracks the sequence number values for a particular client and the client then roams out of the range of the IDS, we are no longer able to monitor sequence number patterns. When the client returns within range of the IDS, the sequence numbers that follow will appear anomalous due to the large gap in sequence values. In order to avoid this potential false-positive detect, the IDS must be sensitive to time delays when establishing patterns in sequence numbers. If the IDS detect a delay of more than a few seconds between receiving frames for the activity of a client, it must assume the client has roamed out of range or has reset their card and therefore must invalidate the tracked sequence number pattern. It is also important to note that sequence numbers will sometimes skip values when changing the transmit/receive channel, or if the firmware should drop a malformed frame. A sequence number will also be reset to zero if the WLAN card is reinitialized by the PCMCIA bus or other controlling subsystem. For this reason, WLAN anomaly detection systems should not alert on a single missed sequence number or by a small gap in sequence numbers. In most cases, an attacker who is spoofing the MAC address of another client or access point will be significantly different than the legitimate source MAC. A rule of thumb for alerting might be a sequence number that appears out of order with a difference of plus or minus thirty sequence values. While testing the sequence analysis patterns presented in this paper, I discovered that Lucent 802.11b cards, using all firmware releases to the present 8.10, do not follow the 802.11 specification for sequence number gene ration. These cards will send frames with low-numbered sequence values in an initially incremental fashion and will sporadically jump from their initial values to the sequence numbers used by the wireless access point. The card will mirror the sequence numbers used by the wireless access point for a short period of time before returning to its initial sequence number pattern. Without alternate accommodation, this peculiar activity would generate a false positive detect for a spoofed MAC address when following the techniques detailed in this paper. A wireless intrusion analysis system needs to monitor the sequence numbers of the access point in the network as well as the monitored client sequence numbers for variations in the sequence number pattern; first comparing an anomalous sequence number value to the pattern presently in use by the wireless access point before generating an alert.

4. SPOOFING MAC ADDRESS

4.1 METHOD TO SPOOF MAC ADDRESS IN WINDOWS 2000 AND UP

1) Click on the windows Start Button on your desktop
2) Click on the “Run” Option
3) Type the word “Cmd” and press enter
4) Type in the command prompt “ipconfig /all”
5) There you will find the MAC address, 12-digit alpha-numeric #.

Method 1:

This is depending on the type of Network Interface Card (NIC) you have. If you have a card that doesn’t Supports Clone MAC addresses, and then you have to go to second method.

Step1:- Go to Windows Start button -> Settings -> Control Panel and double click on Network Connections.

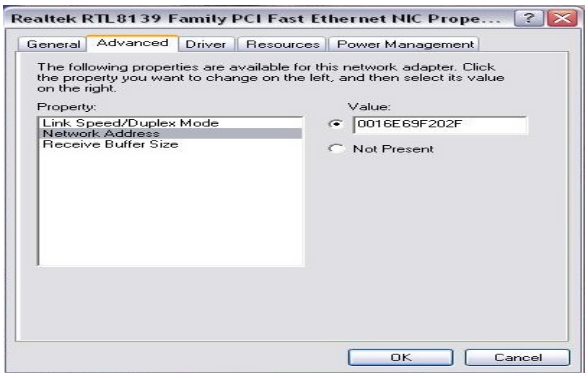
Step2:- Right click on the NIC you want to change the MAC address and click on properties.

Step3:- Under “General” tab, click on the “Configure” button

Step4:- Click on “Advanced” tab

Step5:- Under “Property section”, you should see an item called “Network Address” or "Locally Administered Address", click on it. (See figure below as an example)

Step6:- On the right side, under “Value”, type in the New MAC address you want to assign to your NIC. Usually this value is entered without the “-“between the MAC address numbers.


Realtek RTL8139 Family PCI Fast Ethernet NIC Prope...

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:
Link Speed/Duplex Mode
Network Address
Receive Buffer Size

Value:
● 0016E69F202F
○ Not Present

Figure 4.1

4.2 TO KNOW WHETHER THE MAC ADDRESS SPOOFS ARE NOT THESE ARE THE COMMANDS TO CHECK

Method 1:-

Step1. Go to command prompt and type in “ipconfig /all” or “net config rdr” or “getmac -v” to verify the changes. If the changes are not materialized, then use the second method.

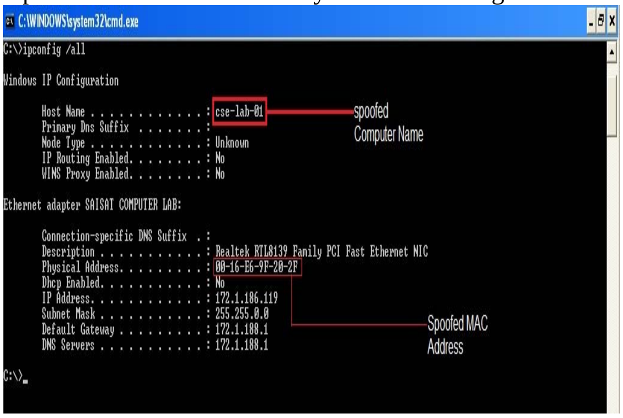
Step2. If successful, reboot your systems.

Method 2:-

This method requires some knowledge on the Windows Registry. If you are not familiar with Windows Registry, just use the simple-to-use **SMAC** MAC Address Changer to change the MAC addresses (the easiest and safest way,) or consult with a technical person before you attempt on the following steps. Also, make sure you have a good backup of your registry.

Step1. Go to command prompt and type “ipconfig /all”.

Step2. Note the MAC Address you want to change.

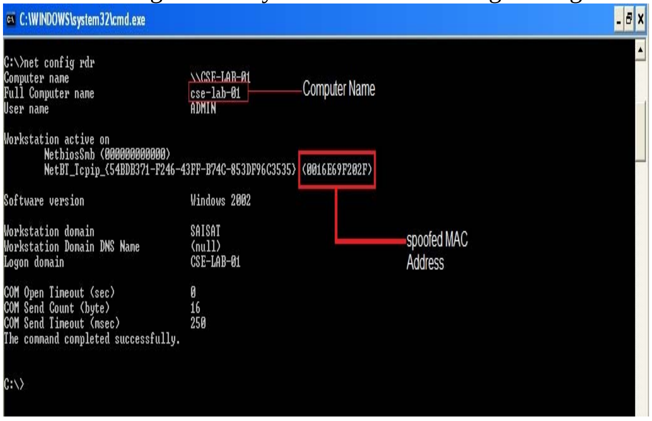

C:\WINDOWS\system32\cmd.exe

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : cse-lab-01
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter SAISAT COMPUTER LAB:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-16-E6-9F-20-2F
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.1.186.119
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.1.188.1
        DNS Servers . . . . . . . . . . . : 172.1.188.1

C:\>_
```

Figure 4.2

Other commands to get whether the MAC Address which we want to change is correct are not.

- Go to windows command prompt and type “net config rdr” and you will see something like figure 8



C:\WINDOWS\system32\cmd.exe

```
C:\>net config rdr
Computer name                        \\CSE-LAB-01
Full Computer name                   cse-lab-01
User name                            ADMIN

Workstation active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{54BDB371-F246-43FF-B74C-853DF96C3535} (0016E69F202F)

Software version                     Windows 2002

Workstation domain                   SAISAT
Workstation Domain DNS Name          (null)
Logon domain                         CSE-LAB-01

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.


C:\>
```

Figure 4.3

Step1:-Go to Start -> Run, type “regedt32” to start registry editor. Do not use “Regedit.”

Step2:-Double click on “HKEY_LOCAL_MACHINE”

Step3:-Double click on the root key “SYSTEM”.

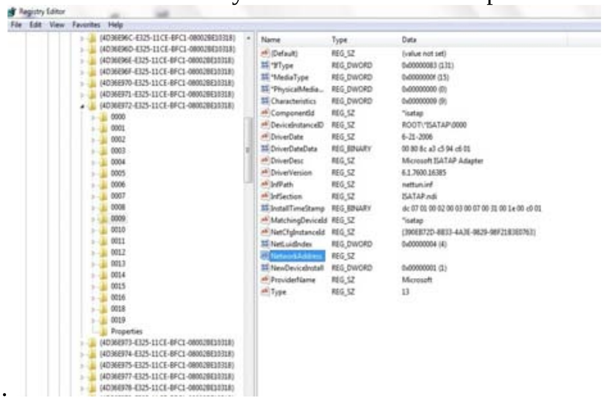
Step4:-Double click on the root key “CurrentControlSet”

Step5:-Double click on the “Control” and then click on “Class”

Step6:-Search for the root tree for {4D36E972-E325-11CE-BFC1-08002BE10318} and Double click on it to expand the tree. There you will find some sub keys of 4-digit numbers which represent particular network adapters like 0000, 0001, 0002 and so on. See the figure 10 to get clear cut of regedt32 editor.

Step7:- Go through each sub key starts with 0000. On Clicking 0000, check **Driver Desc** keyword on the right to see if that's the NIC you want to change the MAC address. If you are not 100% sure about the DriverDesc, then you can verify by checking if the **NetCfgInstanceID** or **Network Address** keyword value matches the GUID.

If there is no match, then try to find it on to 0001, 0002, 0003, and so on, until you find the one you want. Usually 0009 contains the first NIC you installed on the computer



```
{4D36E96C-E325-11CE-BFC1-08002BE10318}
{4D36E96D-E325-11CE-BFC1-08002BE10318}
{4D36E96E-E325-11CE-BFC1-08002BE10318}
{4D36E96F-E325-11CE-BFC1-08002BE10318}
{4D36E970-E325-11CE-BFC1-08002BE10318}
{4D36E971-E325-11CE-BFC1-08002BE10318}
{4D36E972-E325-11CE-BFC1-08002BE10318}
    0000
    0001
    0002
    0003
    0004
    0005
    0006
    0007
    0008
    0009
    0010
    0011
    0012
    0013
    0014
    0015
    0016
    0018
    0019
    Properties
{4D36E973-E325-11CE-BFC1-08002BE10318}
{4D36E974-E325-11CE-BFC1-08002BE10318}
{4D36E975-E325-11CE-BFC1-08002BE10318}
{4D36E977-E325-11CE-BFC1-08002BE10318}
{4D36E978-E325-11CE-BFC1-08002BE10318}
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
*IfType	REG_DWORD	0x00000083 (131)
*MediaType	REG_DWORD	0x0000000f (15)
*PhysicalMedia...	REG_DWORD	0x00000000 (0)
Characteristics	REG_DWORD	0x00000009 (9)
ComponentId	REG_SZ	*isatap
DeviceInstanceID	REG_SZ	ROOT*ISATAP\0000
DriverDate	REG_SZ	6-21-2006
DriverDateData	REG_BINARY	00 80 8c a3 c5 94 c6 01
DriverDesc	REG_SZ	Microsoft ISATAP Adapter
DriverVersion	REG_SZ	6.1.7600.16385
InfPath	REG_SZ	nettun.inf
InfSection	REG_SZ	ISATAP.ndi
InstallTimeStamp	REG_BINARY	dc 07 01 00 02 00 03 00 07 00 31 00 1e 00 c0 01
MatchingDeviceId	REG_SZ	*isatap
NetCfgInstanceId	REG_SZ	{390EB72D-8833-4A3E-9829-98F2183B0763}
NetLuidIndex	REG_DWORD	0x00000004 (4)
NetworkAddress	REG_SZ	
NewDeviceInstall	REG_DWORD	0x00000001 (1)
ProviderName	REG_SZ	Microsoft
Type	REG_SZ	13

.

Figure 4.4

Step8:- Once you selected the sub key (i.e. 0000), check if there is a keyword "NetCfgInstanceID or Network Address" exist in the right side of the window. (See figure 10)

I. If “**NetCfgInstanceID or Network Address**" keyword does not exist, and then create this new keyword:

i. Click on the drop down menu “Edit -> Add Value”.

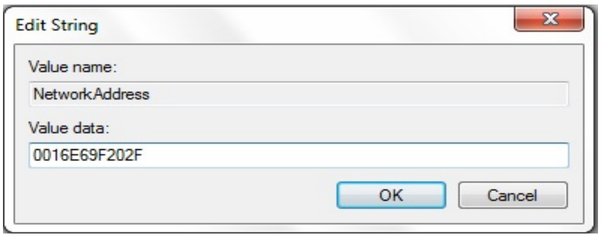
ii. In the Add Value window, enter the following value then click OK. (See figure 11.)

Value Name: = **NetCfgInstanceID** or **Network Address**

Data Type: = **REG_SZ**

iii. String Editor Window will pop up at this time.

iv. Enter the new MAC address you want to modify. Then click OK.



Edit String

Value name: NetworkAddress

Value data: 0016E69F202F

Figure 4.5

The Simple-to-Use **SMAC** MAC Address Changer (Spoof) is definitely a lot SAFER and EASIER for this type of process. Check out some SMAC screenshots.

Step9:- There are 2 ways to make the new MAC address active. Method I does not require a system reboot:

II. Go to Start->Setting->Control Panel, and double click on "Network Neighborhood".

NOTE: you will lose the network connection after completing step "ii." below, and

if you have a DHCP client, you will get a new IP address after completing step "iii."

i. Select the Network Adaptor you just changed the MAC address.

ii. Right click on the selected Network Adaptor and click "Disable.”

Verify the status column for this adaptor changes to "Disabled"

iii. Right click on the selected Network Adaptor and click "Enable."

Verify the status column for this adaptor changes to "Enabled"

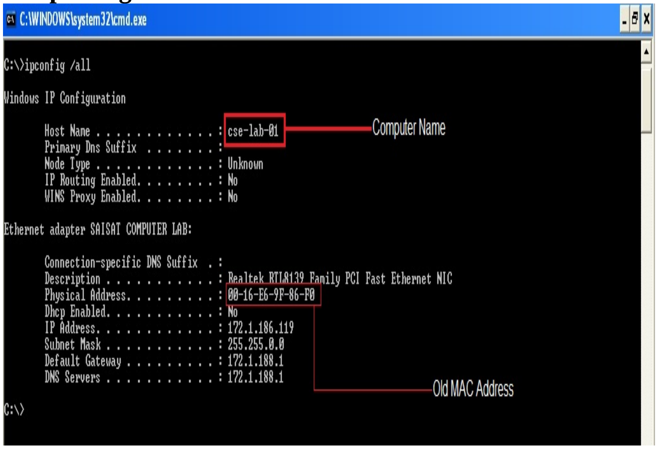
iv. If for any reason it cannot be disabled or re-enabled.

III. Reboot your Windows system.

Once completing step III (if rebooting the system, wait until the reboot is completed), go to command prompt, type “ipconfig /all” to confirm the new MAC address.

5. Results And Discussions Old Mac Address In System Named Cse-Lab-01 Displaying Mac Addresses Using Different Commands

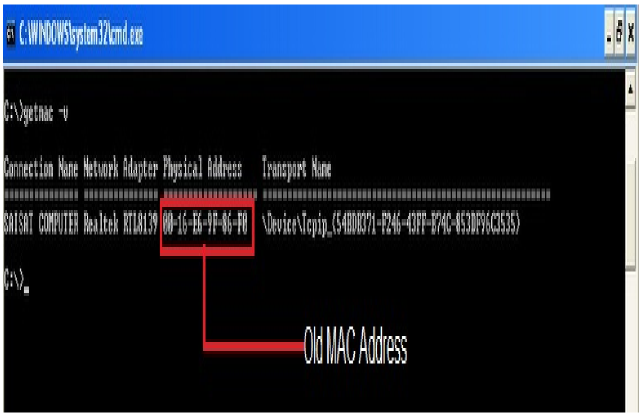
1. "ipconfig /all"



```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : cse-lab-01
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter SAISAT COMPUTER LAB:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-16-E6-9F-86-F0
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.1.186.119
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.1.188.1
        DNS Servers . . . . . . . . . . . : 172.1.188.1

C:\>
```

Figure 5.1

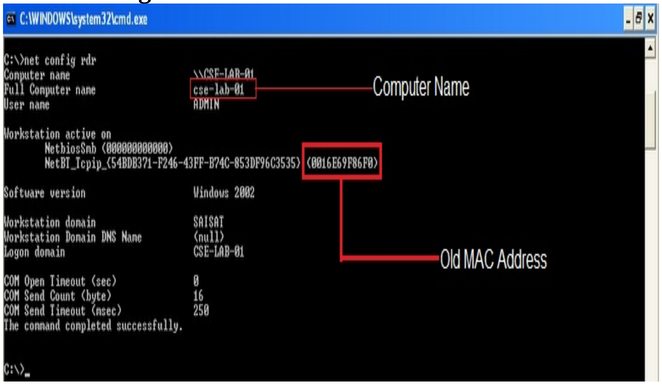
2. "getmac -v"



```
C:\>getmac -v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== =================== ==========================================================
SAISAT COMPUTER Realtek RTL8139 00-16-E6-9F-86-F0   \Device\Tcpip_{54BDB371-F246-43FF-B74C-853DF96C3535}

C:\>_
```

Figure 5.2

3. "net config rdr"

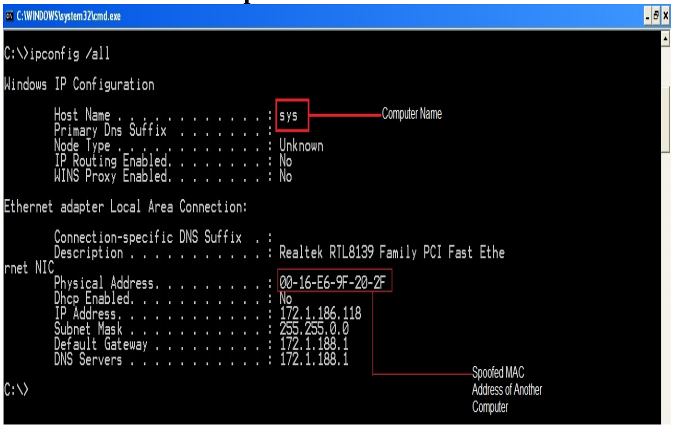


```
C:\>net config rdr
Computer name                        \\CSE-LAB-01
Full Computer name                   cse-lab-01
User name                            ADMIN

Workstation active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{54BDB371-F246-43FF-B74C-853DF96C3535} (0016E69F86F0)

Software version                     Windows 2002

Workstation domain                   SAISAT
Workstation Domain DNS Name          (null)
Logon domain                         CSE-LAB-01

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.

C:\>_
```

Figure 5.3

MAC ADDRESS OF OTHER COMPUTER WHICH WE ARE SPOOFING TO CSE-LAB-01 COMPUTER

MAC Address of computer named SYS

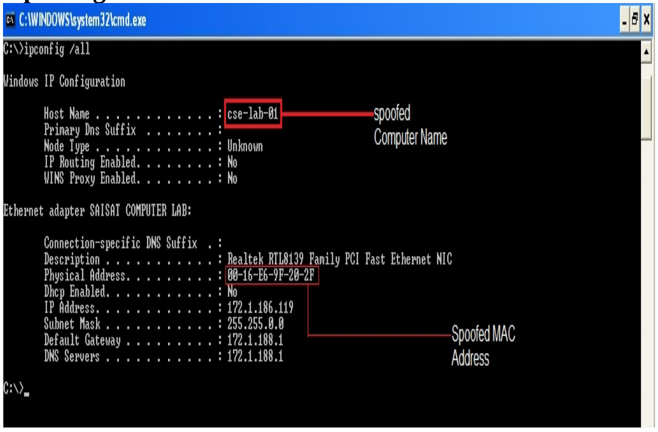

C:\WINDOWS\system32\cmd.exe
Computer Name
Spoofed MAC Address of Another Computer

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : sys
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
        Physical Address. . . . . . . . . : 00-16-E6-9F-20-2F
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.1.186.118
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.1.188.1
        DNS Servers . . . . . . . . . . . : 172.1.188.1

C:\>
```

Figure 5.4

SPOOFING COMPUTER CSE-LAB-01 MAC ADDRESS

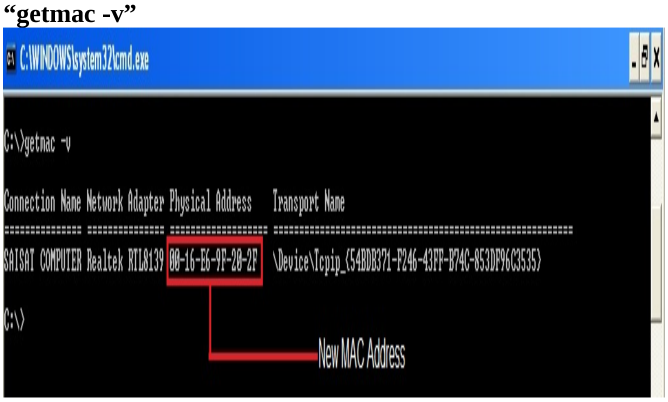
1. Command to get new MAC Address using command "ipconfig /all"



```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : cse-lab-01
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter SAISAT COMPUTER LAB:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-16-E6-9F-20-2F
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.1.186.119
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.1.188.1
        DNS Servers . . . . . . . . . . . : 172.1.188.1

C:\>_
```

Figure 5.5

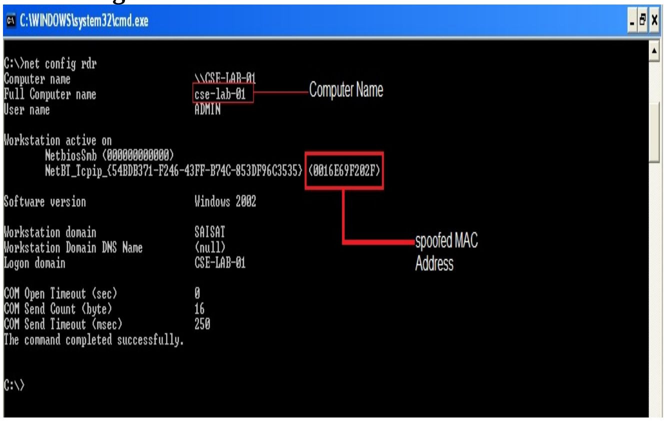
2. Command to get new MAC Address using command "getmac -v"



```
C:\>getmac -v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== =================== ==========================================================
SAISAT COMPUTER Realtek RTL8139 00-16-E6-9F-20-2F   \Device\Tcpip_{54BDB371-F246-43FF-B74C-853DF96C3535}

C:\>
```

Figure 5.6

3. Command to get new MAC Address using command "net config rdr"



```
C:\>net config rdr
Computer name                        \\CSE-LAB-01
Full Computer name                   cse-lab-01
User name                            ADMIN

Workstation active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{54BDB371-F246-43FF-B74C-853DF96C3535} (0016E69F202F)

Software version                     Windows 2002

Workstation domain                   SAISAT
Workstation Domain DNS Name          (null)
Logon domain                         CSE-LAB-01

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.


C:\>
```

Figure 5.7

6. COUNTER MEASURES

There are certain countermeasures to reduce the above-mentioned vulnerable affects of MAC spoofing.Our OS is static but it should be dynamic so that it provide a utility that check after few second if any entry found in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\0001 or 0005" with the name "network address" then the utility should delete it automatically [7],[8].

- Whenever ARP packets arrive it should not check the MAC address for the OS, it should retrieve it directly from LAN card or whenever ARP packets arrive it should compare the MAC address from OS to NIC and if it doesn't match it should delete the entry from OS or from registry[9].
  - MAC address is stored in OS. Whenever MAC address is required it is retrieved from operating system. If we want to prevent MAC address to be spoofed then whenever we require MAC address we must retrieve it directly from NIC.
- You can lock your MAC address by introducing the router which support the MAC filtering and IP reservation. This is where you associate a DHCP IP address with a particular MAC address. By this way only that MAC gets associated with particular IP address.
- To prevent MAC spoofing you would need to encrypt the communication between the wireless PC and access point. Higher end AP's support IPSEC.

7. CONCLUSION

Spoofing is possible because the IEEE 802.11 standard does not provide per-frame source authentication, but in future it can be effectively prevented if a proper authentication is added into the standard. There is plan for such standard modification to support link-layer source authentication that covers both management and control frames. The key idea of this project is to leverage the sequence number field in the link-layer header of IEEE 802.11 frames without modifying STAs, APs, or the MAC protocol. If an intrusion detection system keeps track of the latest sequence number of each wireless node, to impersonate a node an attacker needs to spoof the source address as well as its corresponding sequence number. If the sequence number of a spoofed frame is equal to or smaller than the corresponding node's current sequence number, the spoofed frame is considered a retransmitted frame and thus has to have the same content as the authentic frame with the same sequence number. This means that the spoofed frame cannot possibly do any harm as it is just a duplicate.

MAC spoofing attacks in 802.3 networks exploit a fundamental vulnerability of the 802.3 protocols. The MAC addresses of the Ethernet LAN card can be easily forged, imposing a serious security challenge. With this we conclude that the dangerous security hole is in our OS. Our OS is static but if it will be dynamic it will resolve our many spoofed based problem. If a MAC is spoofed its entry is made in registry, a dynamic OS may have the utility to check its registry after few second if there is any entry with name network address then it should delete it therefore MAC cannot be spoofed.

REFERENCES

[1]. MACspoofing : http://en.wikipedia.org/wiki/

[2]. E.D Cardenas. MAC Spoofing An Introduction. http://www.giac.org/practical/GSEC/Edgar Cardenas GSEC.pdf

[3]. http://wn.com/Gerador_de_chaves_pre- defenidas_wpa2-psk_para_redes_d- link_da_sapo_por_MAC_address

[4]. J.Wright. Detecting Wireless LAN MAC Address Spoofing. http://home.jwu.edu/ jwright/papers/wlan-mac-spoof.pdf

[5]. Y. Liu, K. Dong, L. Dong, B. Li, Research of the ARP Spoofing Principle and a Defensive Algorithm, International Journal of Communications.

[6]. D.C. Plummer, An Ethernet Address Resolution Protocol, RFC-826, Network Working Group, November 1982

[7]. T. Pusateri, IP Multicast over Token-Ring Local Area Networks, RFC-1469, Network Working Group, June 1993

[8]. M.D.Spivey, Practical Hacking techniques and countermeasures

[9]. M.k.Choi1, R.J. Robles1, C.Hong, T.Kim1, Wireless Network Security: Vulnerabilities, Threats and Countermeasures, International journal of Multimedia and Ubiquitous Engineering, Vol.3, No. 3, July, 2008.