

MAC Address

Monika Asija

Assistant Professor of Computer Science
Department of Computer Science
Patel Memorial National College, Rajpura (Punjab)

ABSTRACT

Media Access Control (Mac) Address is 48-bit address which is permanently assigned to a network interface card (NIC) or wireless cards. This address is assigned by the manufacturer itself. Every host on a network has a mac address which helps those devices to communicate with other devices at layer-2 (Datalink Layer) of OSI- Model on the other hand IP address is a network address which allows a device to communicate with others on layer-3 of OSI- Model (Network Layer) on a network. A Mac Address is also named as physical address of an Interface.

Mac Address Spoofing is an activity which is performed to change the Mac Address of a machine. It may be done by authorised or unauthorised persons to access the network or resources. These kind of activities are performed by hackers also who changes the mac address of their pc/ laptop so that their machine can be treated as the authorised machine in that network.(Cardenas, 2003)(MAC address spoofing, 2012)

Keywords: MAC address, IP, Computers, IT, Computer Network

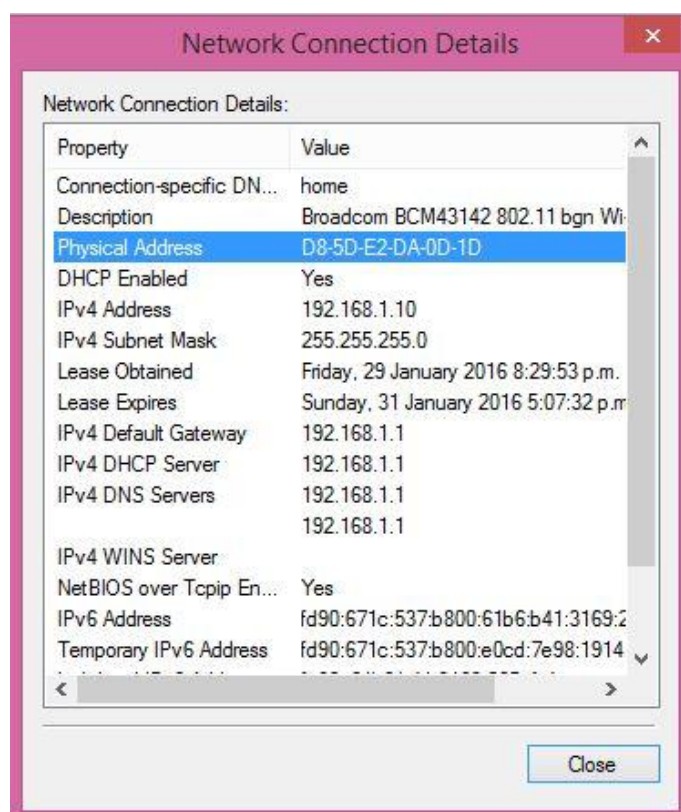
Mac Address

Mac Address is a unique hardware address assigned to a network interface by the manufacturer. This is unique for every network interface. A Network interface can be a

Network Interface Card (NIC) for wired network or it can be a wireless adaptor. There are various companies who manufactures network Interfaces and they burn in a unique hardware address in every network interface. This address uniquely identifies a network interface.(Mitchell, 2015)

Mac Address Format

Mac Address is a 48-bit address represented in hexadecimal. First 24-bits represent the company specific code which is assigned by IEEE to every manufacturing company. For example, 00:13:10 is the code (Organisational Unique Identifier) associated with Linksys. There can be more than one codes associated with a single company also. And the next 24-bits represent the interface specific number for every single network interface/adaptor.(MAC address/vendor lookup and search, n.d.)



In the above figure, it shows the Physical address/ Mac address of the Wi-Fi adaptor of my laptop. Which is D8-5D-E2-DA-0D-1D. First 24-bits D8-5D-E2 is the Organisation's unique identifier and this code is assigned to Hon Hai Precision Ind. Co., Ltd. which is a Taiwan based company. Rest of the bits DA-0D-1D are the interface specific.

By the advancements in technologies there are some upgradations done in Mac Address format also. Now 64-bit Mac Address is also used now a days with the development of IPv6.(Khanna, 2016)

How to find Mac Address of a network interface of a PC / Laptop?

Every device which is connected to the network has a network interface with uniquely identified physical address/ mac address. To find the mac address of network interfaces in a pc or a laptop I used "ipconfig /all" command.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\OEM>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN81
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : home

Wireless LAN adapter Local Area Connection* 15:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Hosted Network Virtual Adapter
Physical Address. . . . . : D8-5D-E2-DA-0D-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : DA-5D-E2-DA-0D-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . . . : home
Description . . . . . : Broadcom BCM43142 802.11 bgn Wi-Fi M.2 Ad
apter
Physical Address. . . . . : D8-5D-E2-DA-0D-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : fd90:671c:537:b800:61b6:b41:3169:265e<Pre
ferred>
Temporary IPv6 Address. . . . . : fd90:671c:537:b800:bda3:710a:4cc2:9bb4<Pr
eferred>
Link-local IPv6 Address . . . . . : fe80::61b6:b41:3169:265e%4<Preferred>
IPv4 Address. . . . . : 192.168.1.10<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, 1 February 2016 4:19:51 p.m.
Lease Expires . . . . . : Wednesday, 3 February 2016 2:01:15 p.m.
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 81288674
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-1B-46-50-58-20-B1-3E-5B-45

DNS Servers . . . . . : fe80::1%4
192.168.1.1
192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 58-20-B1-3E-5B-45
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

```

In the above figure, it shows the configurations of all the interfaces. The command used to show the configuration of the network interfaces is “ipconfig /all”. When we enter after typing this command prompt will show the current IP configuration along with the physical addresses / mac address of the particular interfaces.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\OEM>GETMAC

Physical Address      Transport Name
=====
58-20-B1-3E-5B-45    Media disconnected
D8-5D-E2-DA-0D-1D    \Device\Tcpip_{CD58C584-FE06-4D45-934C-DA45E18359AC}
0A-00-27-00-00-00    \Device\Tcpip_{662B3E4A-BCF4-49BF-B6F5-881C5BCDE675}

C:\Users\OEM>

```

In the above figure, there is another command used which is particularly used to retrieve the Mac Address of all the interfaces present on the Machine.

Under “Wireless adapter Wi-Fi” It shows the IP configuration of the wireless adapter of my laptop along with the Mac Address/ Physical Address of the interface. The Physical Address of the interface is D8-5D-E2-DA-0D-1D.

Under “Ethernet adapter Ethernet” It shows the configuration of the Network Interface Card. But it does not show any IP Configuration because it is not connected to any network. Instead it shows the Mac Address of the interface which is 58-20-B1-3E-5B-45.

Mac Address Spoofing

Mac Address Spoofing is the technique of changing the mac address of the particular network interface of a device for getting in to the network. This can be done for legal purpose or it can be done for any kind of malicious activity. In detail, we can say that to access a particular network which is only available to the authorised or registered clients, we have to change the Mac Address of our machine. This is called Mac Address Spoofing. Spoofed Mac Address can be randomly generated by the attacker or it can be a pre assigned address used by some other authorised machine. The new Mac address is

The journal is a scholarly peer reviewed and refereed publication and is a publisher member of PILA Inc., USA, (CrossRef).
 © Institute of Research Advances. Website: <http://www.research-advances.org/journal/>

named as the Spoofed Mac Address which is one of the authorised mac addresses in the network. Now, to get the list of the authorised Mac Addresses in a network there are various tools available like Nmap, Emco Mac Address Scanner, Advanced IP Scanner, Cain, Ethereal, Wireshark and there are many more. For Hackers, Mac Spoofing is the basic step to execute an attack on a network or on machines. Hackers usually steal data packets from the ongoing transmissions when they get in to the network with the help of spoofed mac address. Attackers use spoofed mac address to connect to the other client machines in the network as an authorised machine and the clients respond to the requests of the machines as they see that the requesting machine with the particular spoofed address is the authorised machine.

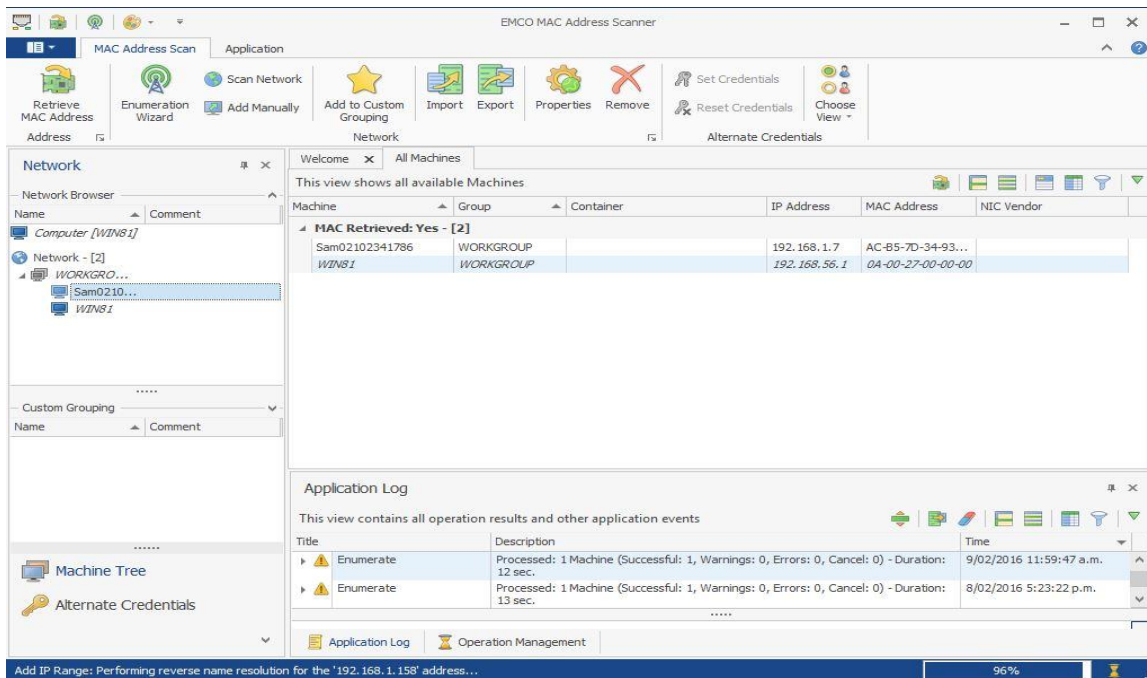
There are various methods/tools for Mac Address Spoofing in different operating systems. Changing a Mac Address is not illegal that is why all the operating systems support Mac Address Spoofing but this gives a platform to attackers to use this feature in the malicious way for their own benefits.(Cardenas, 2003)(RaymondCCBlog, n.d.)

Mac Address Scanner tools

There are various tools available which can provide us the information regarding each machine which is connected to the network. These tools provide us all the information regarding Mac Address, IP address etc. about a particular machine.

1. Emco Mac Address Scanner

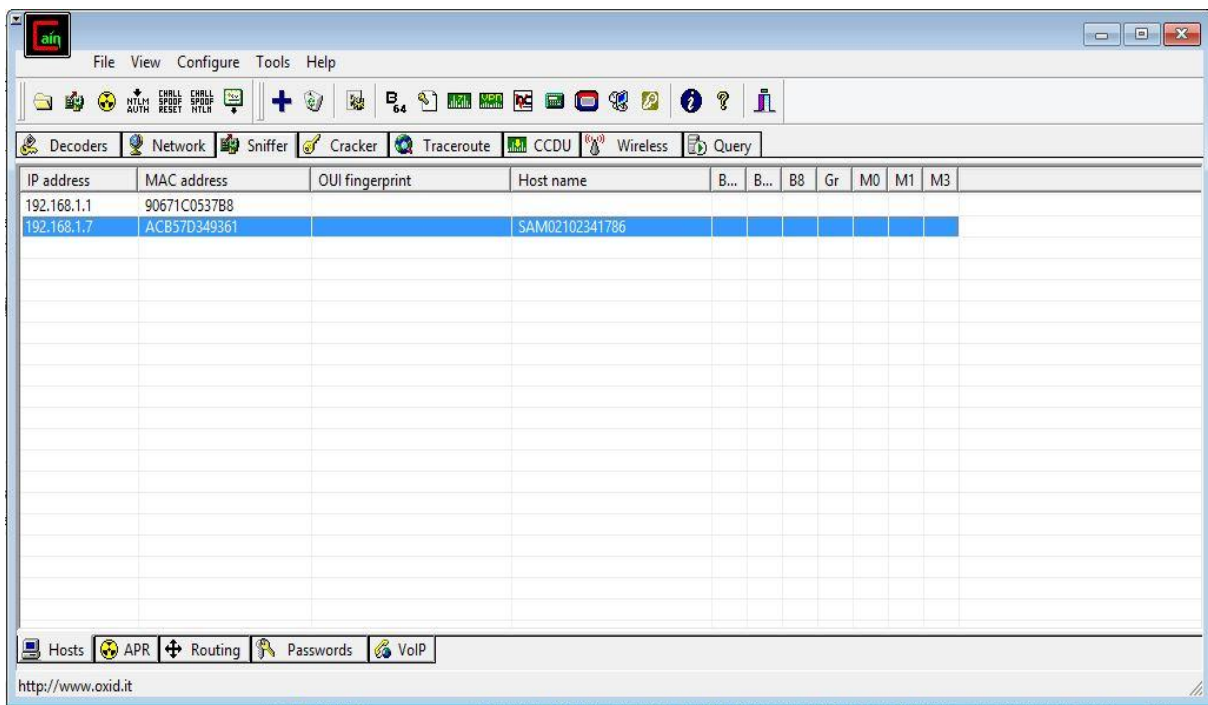
In the figure below, this tool scans the whole network and retrieves all the nodes connected to the network. As in this, figure there are two nodes represented as 192.168.56.1 with Mac Address 0A-00-27-00-00-00 and 192.168.1.7 with Mac Address AC-B5-7D-34-93-61. The machine with the IP address 192.168.56.1 is the virtual machine created in Oracle Virtual Box and the machine with IP address 192.168.1.7 is another machine which is connected to the home network. This is one of the common tools used for capturing the list of Mac Addresses of the machines connected to the network.



When we get a complete list of Mac addresses of the machines present on the network, then we can easily change Mac Address of our machine to get in to the authorised network.

2. Cain & Abel

Cain & Abel is a network monitoring tool which can be used for getting the list of all the devices which are connected to the network. It provides us the list of all the nodes connected to the network with their IP Addresses along with their Mac Addresses. In the figure below, it represents the list of nodes present on the network. The machine with 192.168.1.1 IP address is the gateway or the Modem in our home network. The machine with 192.168.1.7 IP address is the client machine which accesses the network and is currently connected to the network. We can see in this given figure that Cain & Abel can provide us the information of a machine like IP address, MAC address and Host name.



3. Nmap

Nmap is a network monitoring utility tool used by network administrators and Attackers to get list of all the nodes attached to the network. This tool can provide us the Mac Address of the machines and information regarding the Operating System of the machines in the network. This tool can also be used to monitor the Mac Address Spoofing. (Nmap 7 Release Notes, 2015) (Cane, 2013)

```

C:\soft\nmap-7.01-win32\nmap-7.01>nmap -sP 192.168.1.0/24
Starting Nmap 7.01 < https://nmap.org > at 2016-02-09 12:57 New Zealand Daylight
Time
Nmap scan report for 192.168.1.1
Host is up <0.047s latency>.
MAC Address: 90:67:1C:05:37:B8 <Huawei Technologies>
Nmap scan report for 192.168.1.7
Host is up <0.10s latency>.
MAC Address: AC:B5:7D:34:93:61 <Liteon Technology>
Nmap scan report for 192.168.1.10
Host is up.
Nmap done: 256 IP addresses <3 hosts up> scanned in 5.78 seconds

C:\soft\nmap-7.01-win32\nmap-7.01>nmap -O 192.168.1.7
Starting Nmap 7.01 < https://nmap.org > at 2016-02-09 12:58 New Zealand Daylight
Time
Nmap scan report for 192.168.1.7
Host is up <0.0043s latency>.
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdaapi
10243/tcp open  unknown
49156/tcp open  unknown
MAC Address: AC:B5:7D:34:93:61 <Liteon Technology>
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008!7!Phone!Uista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7::-:pr
ofessional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsof
t:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Windows Server 2008 R2, Microsoft Windows 7 Professional or Windows
8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Mi
crosoft Windows Uista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microso
ft Windows Uista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address <1 host up> scanned in 9.72 seconds

C:\soft\nmap-7.01-win32\nmap-7.01>

```

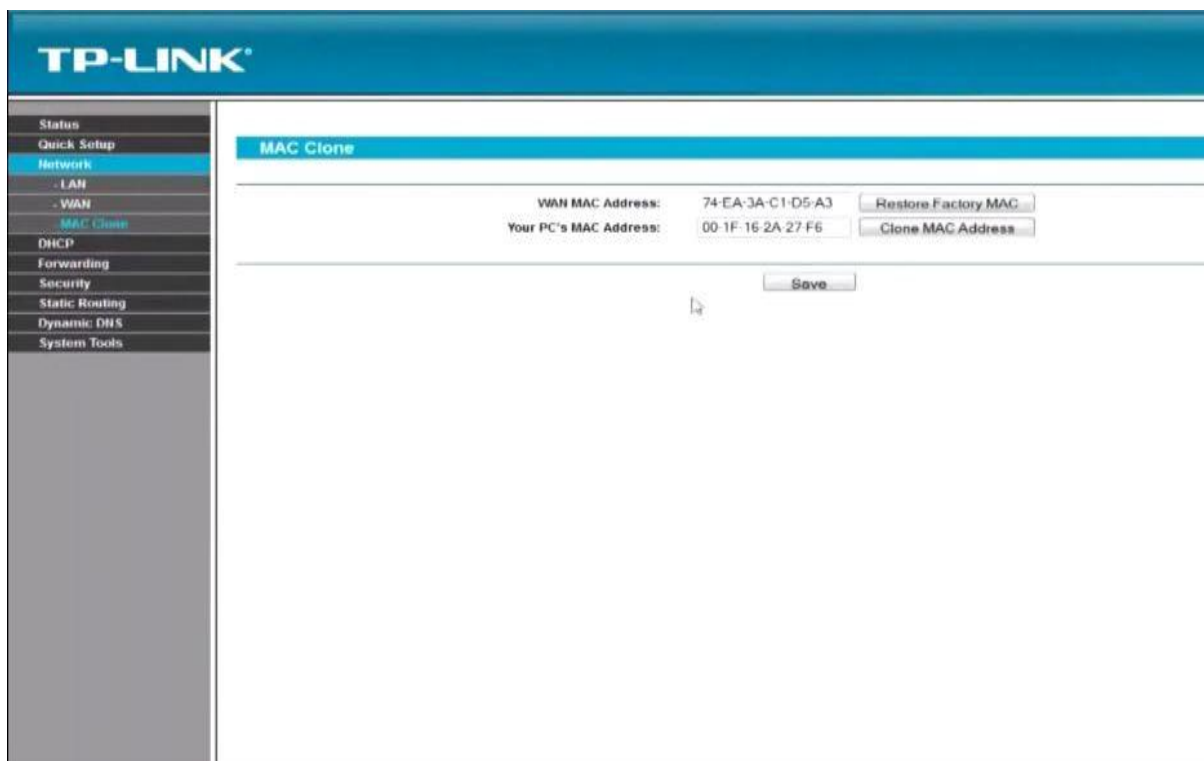
There are many more tools which can be used to capture the information regarding the machines which are connected to the network.

Why Mac Spoofing is needed?

Mac Spoofing is not illegal activity because there are some cases when it is needed to access some kind of services which are provided by the ISPs. But in most of the cases Hackers may use this feature for illegal purpose for their own benefits. There are some scenarios where Mac Spoofing is needed. These scenarios are discussed below:-

Scenario 1 (Legitimate Use of Mac Spoofing)

ISP decides to issue new modems to its customers which are more secure than the older one. And the old modems were registered with the ISP that means their Mac Address was mapped to the public IP Addresses assigned to the customer. While installation, the New Modem does not connect to the internet. In this case either ISP should map the new Mac Address of the new modem to the Public IP Address of the customer or the customer should change the Mac Address of the new modem to the Mac Address of the old Modem. This is called Mac Spoofing which is done for the legitimate purpose. In other words, we can say that we have changed our new modems' identity to the older one. To change Mac address of a modem access to the admin panel is needed. Instructions are always given to access admin panel of a modem. By following instructions, we can easily change the settings of a modem. We can change DNS settings, DHCP Server Settings, Mac Address Filtering, Mac Address Changing, Admin Panel Username and Password settings etc. In the figure below, it shows an example how we can change Mac Address of a modem.



Scenario 2 (Legitimate Use of Mac Spoofing)

Secure web servers have the ability to block devices by using their Mac Addresses. This type of situation occurs when an authorized user wants to access a web server but he/she forgets his/her login credentials, and after a certain number of attempts the Web Server blocks that Computer. This is usually done by recording Mac Address of that Computer in the blocked list of the Web Server. After that whenever that computer is used to login, Web server checks its block list and blocks it all the times. To overcome this kind of situations, User must change Mac Address of their computer to access that particular Web Server.

Scenario 3 (Illegitimate Use of Mac Spoofing)

In a Proxy monitored local Area Network, when Network Administrator finds some malicious activities from a particular machine. Then He/ She blocks Mac Address of that machine. After that machine cannot access the internet. To breach these kind of

securities users can change Mac Address of their machine to access the Internet again without even getting noticed by the Network Administrator. Some of the proxy packages available are Squid Proxy, CProxy, and Wingate Proxy. These are some of the proxy packages which are available for the Network administrators. To prevent this kind of malicious activities of Mac Spoofing a Network Administrator can use Mac filtering for providing Internet Access to only authorised Machines.

Figure below: Mac Address Block in Squid Proxy

```
acl badmac arp 00:16:17:4C:AA:50
```

```
http_access deny badmac
```

This is the command, which can be used to block a particular Mac Address

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed

acl badmac arp 00:16:17:4C:AA:50
http_access deny badmac

acl lab_network src 192.168.1.0/24
http_access allow lab_network

# And finally deny all other access to this proxy
http_access allow localhost
http_access deny all
```

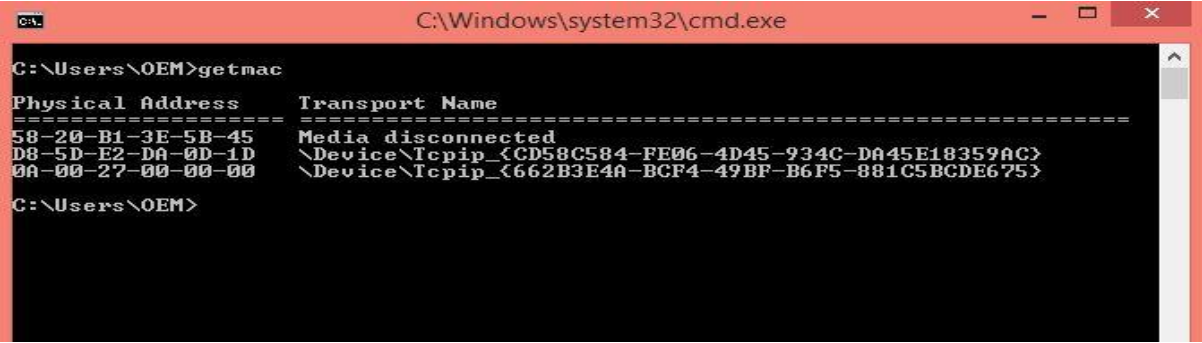
00:16:17:4C: AA: 50 in a squid proxy.

Scenario 4 (Illegitimate Use of Mac Spoofing)

An attacker can use Mac Spoofing to get access of the network depending upon the level of security. In some cases attacker can use an authorised Mac Address of some other authorised machine to get access of the network. After getting access of the network attacker can harm devices attached to the network. An attacker can sniff confidential information from the network and can use that information to harm an organisation in many possible ways. Changing a devices' Mac Address is not a difficult task for a normal computer user.

There are various steps in changing Mac Address of a machine. Changing of Mac Address is different in different Operating Systems. I have taken an example of Windows 8.1 as it is my own machine.

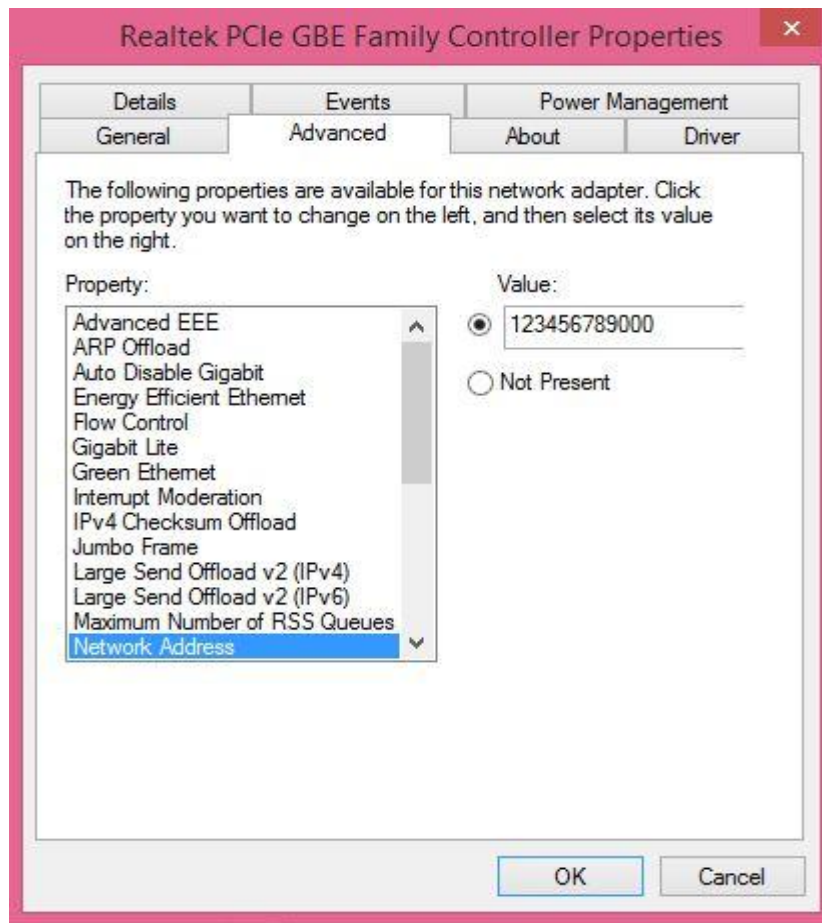
First step is to check the Mac Address of the Machine by typing the command “getmac”. This command lists all the Interfaces of the machine with their Mac Addresses.



```
C:\Windows\system32\cmd.exe
C:\Users\OEM>getmac
Physical Address      Transport Name
-----
58-20-B1-3E-5B-45    Media disconnected
D8-5D-E2-DA-0D-1D    \Device\NPF{CD58C584-FE06-4D45-934C-DA45E18359AC}
0A-00-27-00-00-00    \Device\NPF{662B3E4A-BCF4-49BF-B6F5-881C5BCDE675}
C:\Users\OEM>
```

I am going to change the Mac Address of the network Interface with Mac Address 58-20-B1-3E-5B-45. This is a Network Interface Card with RJ 45 connector.

Second step is to change the Mac Address of the Network Adaptor by following various



steps.

Network Address here means the Mac Address of the particular Network Interface. To change Mac Address of a network interface click on value and enter custom value. I have entered 12:34:56:78:90:00. Now to check whether the Mac Address changed or not type "getmac" command in command prompt. In the figure below, we can see that Mac Address of the network Interface has been changed.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\OEM>getmac

Physical Address      Transport Name
=====
12-34-56-78-90-00    Media disconnected
D8-5D-E2-DA-0D-1D    \Device\NPF{CD58C584-FE06-4D45-934C-DA45E18359AC}
0A-00-27-00-00-00    \Device\NPF{662B3E4A-BCF4-49BF-B6F5-881C5BCDE675}

C:\Users\OEM>
```

This is how we can change Mac Address of our machine to get into the network access. And the Mac Address which I have assigned to the network interface is called Spoofed Mac Address. If we want to revert back to the default Mac Address then we can click on “Not Present” which is a default configured Mac Address of the Network Interface Card.

I have discussed various scenarios of Mac Address Spoofing in this report. Legitimate use can be done to unlock access to the network. On the other hand, illegitimate use of Mac Address Spoofing is done by some unauthorised persons / attackers. Attackers can use this technique to get access to the authorised network. Attackers can use this technique to sniff information from the network for their own benefits. To prevent these kind of problems there are various countermeasures which can prevent Mac Address Spoofing.

Counter measures

As we all know that a network is a backbone of every industry now a days. Every company either small scale or large scale is using network and computers for its daily work. Without a network we cannot think of a good business. As network provides a great way to share information and resources in a company environment. With the advancements of technology there are various new technologies are used to design a

network. With the advancements in technology threat levels of information loss is also increasing. Because attackers can use their knowledge to sniff, destroy and manipulate the sensitive information. Attackers can use various techniques for malicious activities. Here are some of techniques which are used by attackers like Mac Address Spoofing, Denial of Services, and Sniffing etcetera. Mac Address Spoofing is one of the basic activity that is used by the attacker to launch an attack in a network to do some kind of malicious activity. For network security we need to prevent Mac Address Spoofing. There are various ways to prevent Mac Address Spoofing like to avoid Mac Address Spoofing using network security tools like Firewall etc., Detect Mac Address Spoofing in the network using various techniques like RARP, Hardening the network security using Mac Filtering along with the higher level of encryption like WPA2 security while configuring. (Detecting and Preventing MAC Spoofing, n.d.)

Tools to detect Mac Address Spoofing in the network

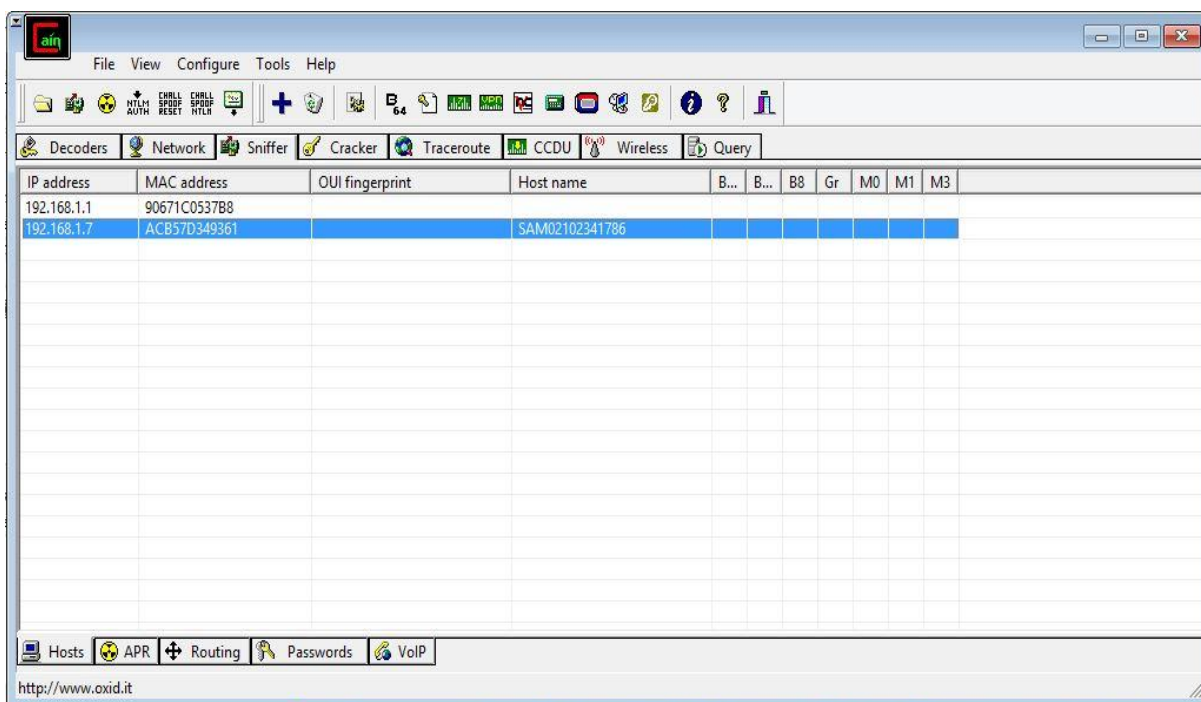
There are various tools to detect Mac Address Spoofing in a network. A Network Administrator has the responsibility of detecting Mac Address Spoofing in a network. Here is the list of tools and techniques to which are used by a Network Administrator.

RARP (Reverse Address Resolution Protocol)

First and the basic technique of detecting Mac Address Spoofing is to run RARP (Reverse Address Resolution Protocol) against the suspected MAC Address. As RARP is a protocol through which a Mac Address is inspected for its IP Address.

Cain & Abel

Cain & Abel is a tool which finds the information regarding all the nodes connected to the network. The information includes IP Address, MAC Address, and Hostname. By using this tool we can easily detect that which machines are using same Mac Address (Mac Address Spoofing). This also shows the IP Addresses associated with the Mac Address. If it shows two IP addresses associated with the single Mac Address then it needs to be prevented.



Also there are various other tools to detect the Mac Address Spoofing. But there working is different from these tools and techniques.

Tools for prevention of Mac Address Spoofing in the Network

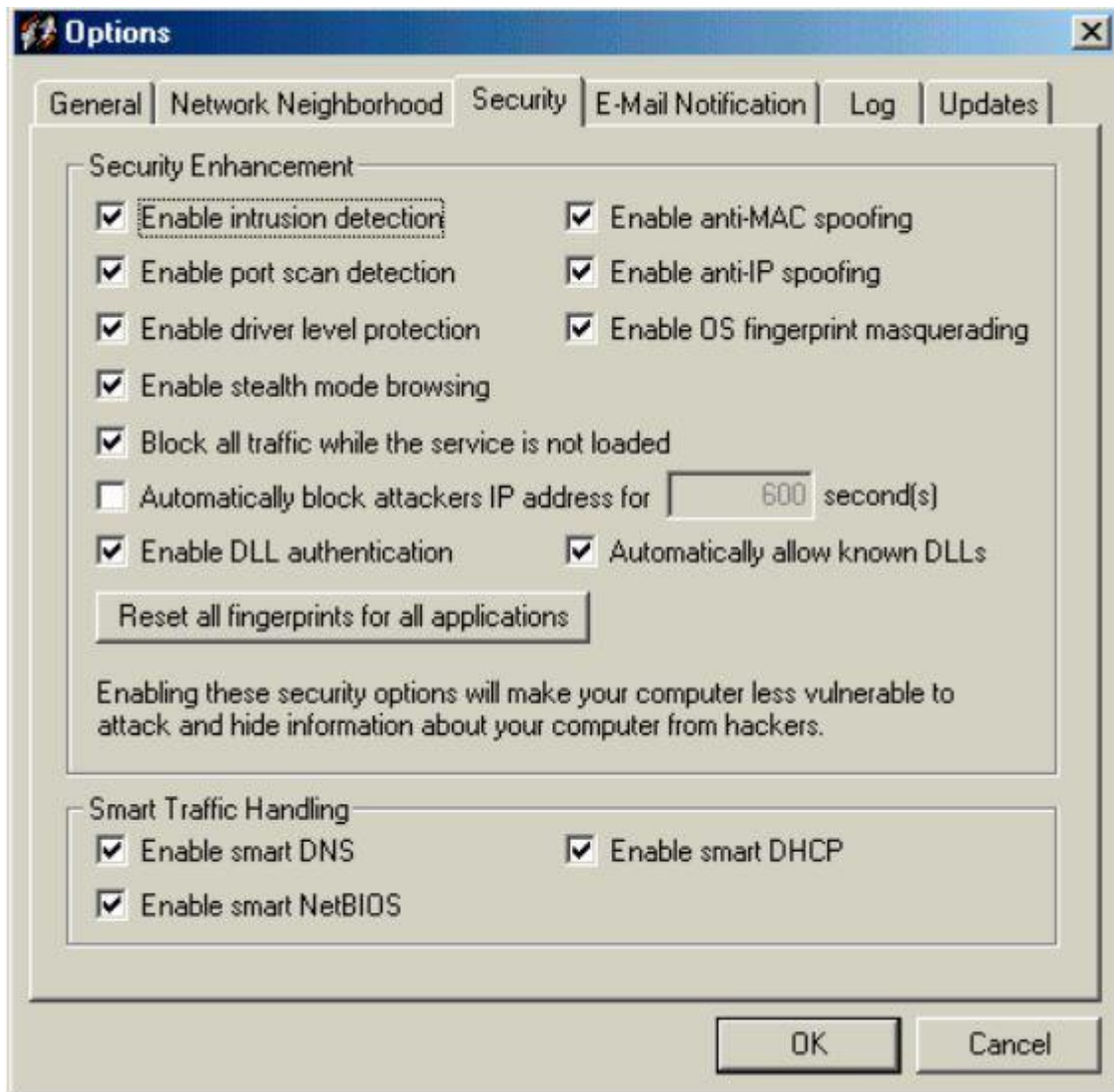
There are various tools (Hardware & Software) available to prevent Mac Address Spoofing in the network. Tools available to prevent Mac Address Spoofing.

Mac Locking

Mac Locking is the technique to bind Mac Address of a machine to a particular port of the Switch. Whenever an intruder tries to spoof a Mac Address the switch does not allow that machine to communicate with the rest of the network. Because switch does not have any information of that spoofed address for particular port to which that spoofed machine is attached.

Firewalls with Anti Mac Spoofing Ability

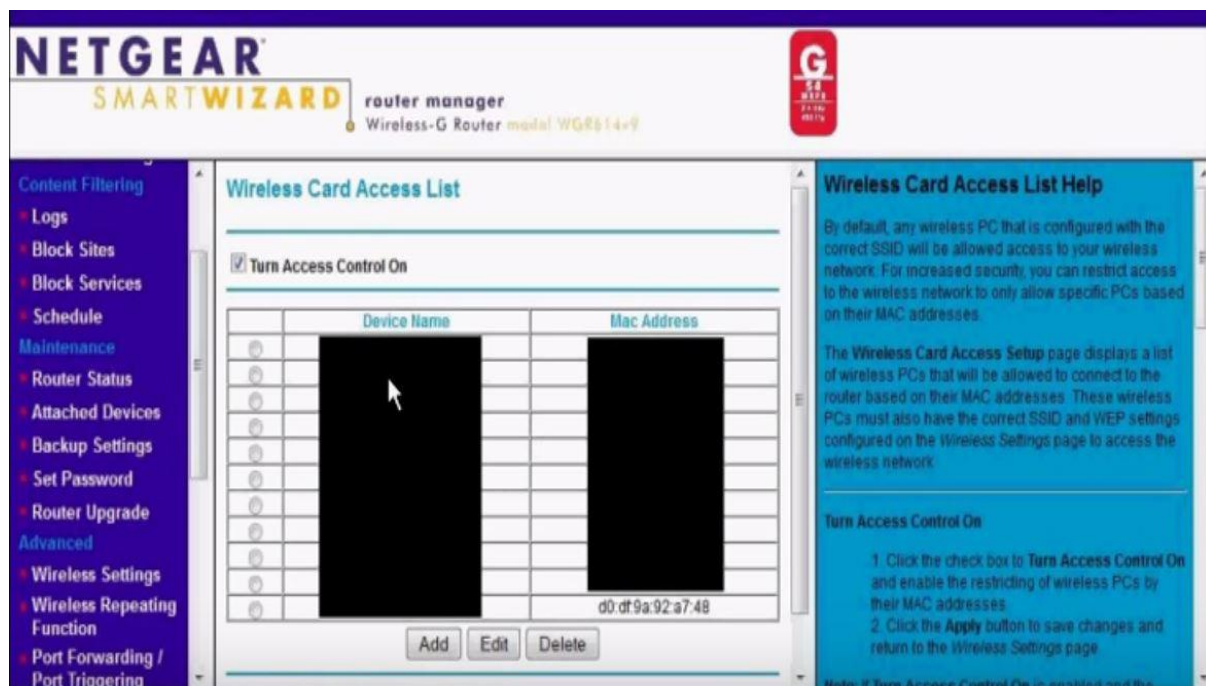
There are some firewalls also which offers Anti Mac Spoof ability. One of them is Sygate firewall. This is a Graphical User Interface application with the ability of Anti Mac Spoofing.



In figure above there is an option of Anti Mac Spoofing which does not allow intruder to change the Mac Address of their machine in the network.

Mac Filtering

Mac Filtering is the process of making an access list of Mac Addresses to which the access should be given in a router or a Wireless Access Point. This is one of the security measures to deny unauthorised access to the network. Mac filtering can be used in combination with the WPA2 wireless security. In the figure below, Access list of Mac Addresses is made and access of the internet is only allowed to the Mac Address which are there in the access list. (bwilds, 2006)



Conclusion

Mac Address Spoofing is a legal activity which can also be used by some intruders / attackers. Mac Address Spoofing can be done in almost all the operating systems very easily. Mac Address Spoofing is basic activity which can be used to launch a big attack on the network. Intruders may use this to get access of the network which is secure. Intruders can use this to gain access of the information from the network. Attacker can use that information in the malicious way. In this report, I have discussed about various tools which are used to detect Mac Address Spoofing in the network. To secure a network from Mac Address Spoofing a Network Administrator uses various tools to detect it. Tools used in this report are Cain & Abel, Nmap and Emco Mac Address

Scanner. Apart from the detection of Mac Address Spoofing, I have also discussed various tools and techniques to prevent Mac Spoofing in a network. These are Firewalls with Anti Mac Spoof, Mac Locking, and Mac Filtering with WPA2 wireless security. This report will help to learn more about the Mac Address, Mac Address Spoofing, Tools used for securing network from Mac Address Spoofing. (Mrs. Hatkar Archana A, 2012)

References:

bwilds. (2006, 11 21). *Wireless Network Security; MAC Address Spoofing*. Retrieved from <http://it.toolbox.com>: <http://it.toolbox.com/blogs/unwired/wireless-network-security-mac-address-spoofing-13077>

Cane, B. (2013, 02 25). *10 nmap Commands Every Sysadmin Should Know* . Retrieved from <http://bencane.com>: <http://bencane.com/2013/02/25/10-nmap-commands-every-sysadmin-should-know/>

Cardenas, E. D. (2003, 08 23). *MAC Spoofing--An Introduction - GIAC*. Retrieved from <https://www.giac.org/>: <https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315>

Detecting and Preventing MAC Spoofing. (n.d.). Retrieved from <https://infoexpress.com>: <https://infoexpress.com/content/practical/142>

Khanna, S. (2016, 04 01). *Understanding IPv6 EUI-64 Bit Address*. Retrieved from <https://supportforums.cisco.com>: <https://supportforums.cisco.com/document/100566/understanding-ipv6-eui-64-bit-address>

MAC address spoofing. (2012, 12 15). Retrieved from <http://www.axllent.org>: <http://www.axllent.org/docs/view/mac-address-spoofing/>

MAC address/vendor lookup and search. (n.d.). Retrieved from <https://www.adminsub.net>: <https://www.adminsub.net/mac-address-finder>

Mitchell, B. (2015, 09 25). *Introduction to MAC Addresses*. Retrieved from <http://compnetworking.about.com>: <http://compnetworking.about.com/od/networkprotocols/a/introduction-to-mac-addresses.htm>

Mrs. Hatkar Archana A, M. V. (2012). Media Access Control Spoofing Techniques and its Counter Measures. *International Journal of Scientific and Engineering Research*, Volume 3(Issue 6), 451-455. Retrieved from <http://www.ijser.org/>: http://www.ijser.org/onlineResearchPaperViewer.aspx?Media_Access_Control_Spoofing_Techniques_and_its_Counter_Measures.pdf

Nmap 7 Release Notes. (2015, 12 19). Retrieved from <https://nmap.org/>: <https://nmap.org/7/>

RaymondCCBlog. (n.d.). *Hacking Knowledge – The Power of Spoofing MAC Address*. Retrieved from <https://www.raymond.cc/>: <https://www.raymond.cc/blog/hacking-knowledge-importance-of-spoofing-your-mac-address/>