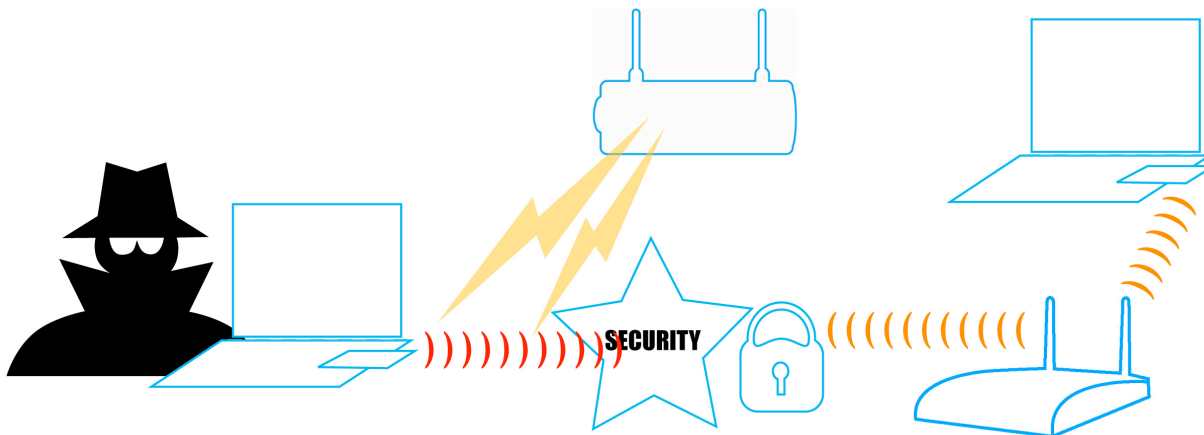


# Section 7

## Using a Wireless IPS/IDS

We've been playing with the 'bad-guy' side of Wireless LANs for awhile. In this section we'll be taking the other side. Trying to detect and protect against the hackers.

We'll show you Hardware and Software solutions in this category. Some are included, and some will be just an Instructor Demo, but either way you'll have fun seeing what we can 'see'.



## Lab 7.1 Airtight Sensor

**Instructor will now demonstrate Airtight Sensor.**

## LAB 7.2: Using a Software Wireless IPS- AirDefense Mobile



You will learn how to use a Wireless Intrusion Prevention System (WIPS) to detect, identify and mitigate wireless attacks. You will learn the benefits of a software based WIPS using a Laptop based version of AirDefense Mobile software.

### Product Information

#### Source

AirDefense Mobile

Free

[www.AirDefense.net](http://www.AirDefense.net)

#### Where, When, Why

AirDefense Mobile is free software based IPS for wireless PC's. Software based IPS is good for troubleshooting, analyzing, or walking the network to scan for devices. Software IPS's are more mobile and give you more flexibility in location.

#### Requirements / Dependencies

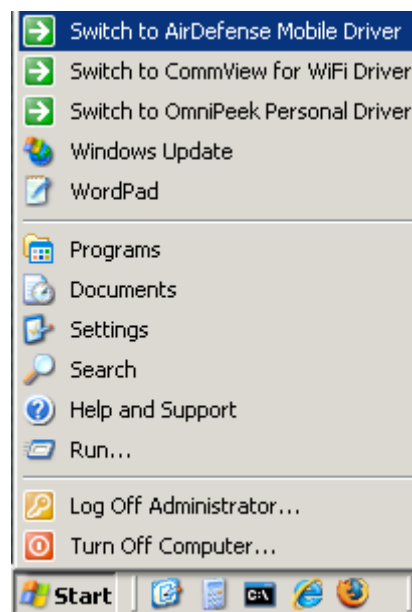
This lab requires the classroom AP and your WLSAT AP to be up and running. The Intel internal adapter in your WLSAT laptop will act as the client station on the wireless network. The Ubiquiti pen testing adapted will be used as the adapter for AirDefense Mobile software WIPS.

- AirDefense Mobile Laptop based IPS Software
- Cat 5 Crossover Network Cable
- WLSAT Dell Laptop
- Ubiquiti Wireless NIC and antenna

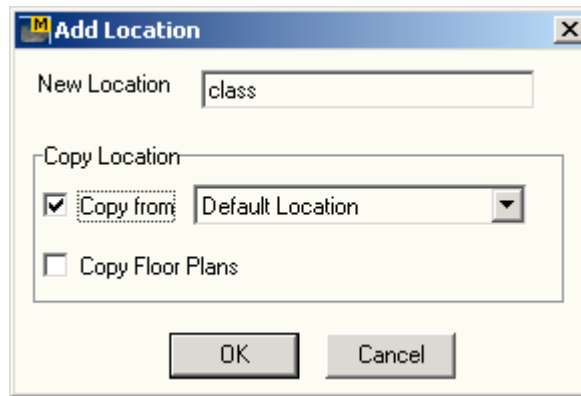
- Step 1. Insert the Ubiquiti Card in the PCMCIA Slot on the side of your WLSAT Laptop. (you can use either the small 2.2dBi or the 5dBi antennas - note the arrow on the bottom pointing to the antenna jack to use)



- Step 2. Go to **Start** → **'Switch to AirDefense Mobile Driver'**.



- Step 3. Open **AirDefense** – **Start** → **Wireless Tools** → **AirDefense Mobile**.
- Step 4. Click **Add Location** button.
- Step 5. Type **class** for the new location name.
- Step 6. Choose the checkbox **copy from default location**.
- Step 7. Click OK.



- Step 8. Select the new *class* location and click **OK**.
- Step 9. Click **Yes** to start scan now.
- Step 10. Click **Threats** to view vulnerabilities for your network.

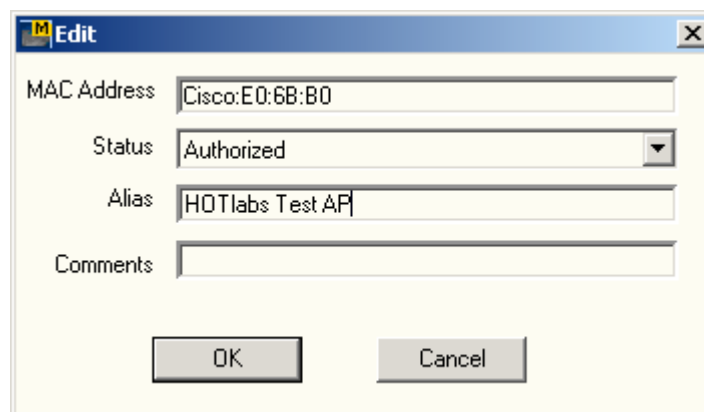


AirDefense is now monitoring the RF environment with default alarm settings. Next you will add classifications to your Station, your wireless security auditor AP, and the classroom AP.

- Step 11. Click the **Access Pts button** on the toolbar.

Access Point Summary View									
Last Seen	AP MAC	Alias	Protocol	SSID	Channel	Signal Strength	Noise	Encryption	Association count
05/11/07 04:21:4...	The Link:75:EC:A1		g	hedgehog	11	-71	-92	Unknown	0
05/11/07 04:21:4...	Cisco-Li:02:E8:B1		g	wirelessvoip	6	-74	-90	On	0
05/11/07 04:21:3...	Cisco:E0:6B:B0		g	inp_bg	1	-75	-90	Off	2
05/11/07 04:21:3...	Cisco:02:78:30		a	inp_a	149	-76	-95	On	0
05/11/07 04:21:4...	Netgear :58:1E:85		g	NETGEAR	11	-82	-92	Off	0
05/11/07 04:21:4...	00:1A:70:5A:63:FD		g	dd-wrt	6	-58	-90	Off	0

- Step 12. **Right click** on *your access point* then **Edit**.
- Step 13. Change the status to **Authorized** you can also add an *Alias* so it will be easier to find in the future.



- Step 14. Click **OK** to confirm the change.

- Step 15. **Right click** on the **classroom AP**.
- Step 16. Change the status to **Authorized** you can also add an **Alias** so it will be easier to find in the future.
- Step 17. Click **OK** to confirm the change.
- Step 18. Choose **Locate** and walk around the room.

Live View  
Packet Decodes - (Last 1000 Packets)

Time	Src Addr	Dest Addr	Type	Sub Type	Length	Channel	R
16:25:17	Cisco:E0:6B:B0	FF:FF:FF:FF:FF:FF	Mgmt	BEACON	156	1	
16:25:17	Cisco:E0:6B:B0	FF:FF:FF:FF:FF:FF	Mgmt	BEACON	156	1	
16:25:17	Cisco:E0:6B:B0	FF:FF:FF:FF:FF:FF	Mgmt	BEACON	156	1	
16:25:17	Cisco:E0:6B:B0	ASKEY CO:34:08:2C	Ctrl	CTS	14	1	
16:25:17	ASKEY CO:34:08:2C	Cisco:E0:6B:B0	Data	NULL	28	1	
16:25:17	Cisco:E0:6B:B0	FF:FF:FF:FF:FF:FF	Mgmt	BEACON	156	1	

Beep on Locate  Lock on Channel    Auto Scroll

Step 19. Where is the Access Point located? \_\_\_\_\_

Step 20. Click on **Stations**.

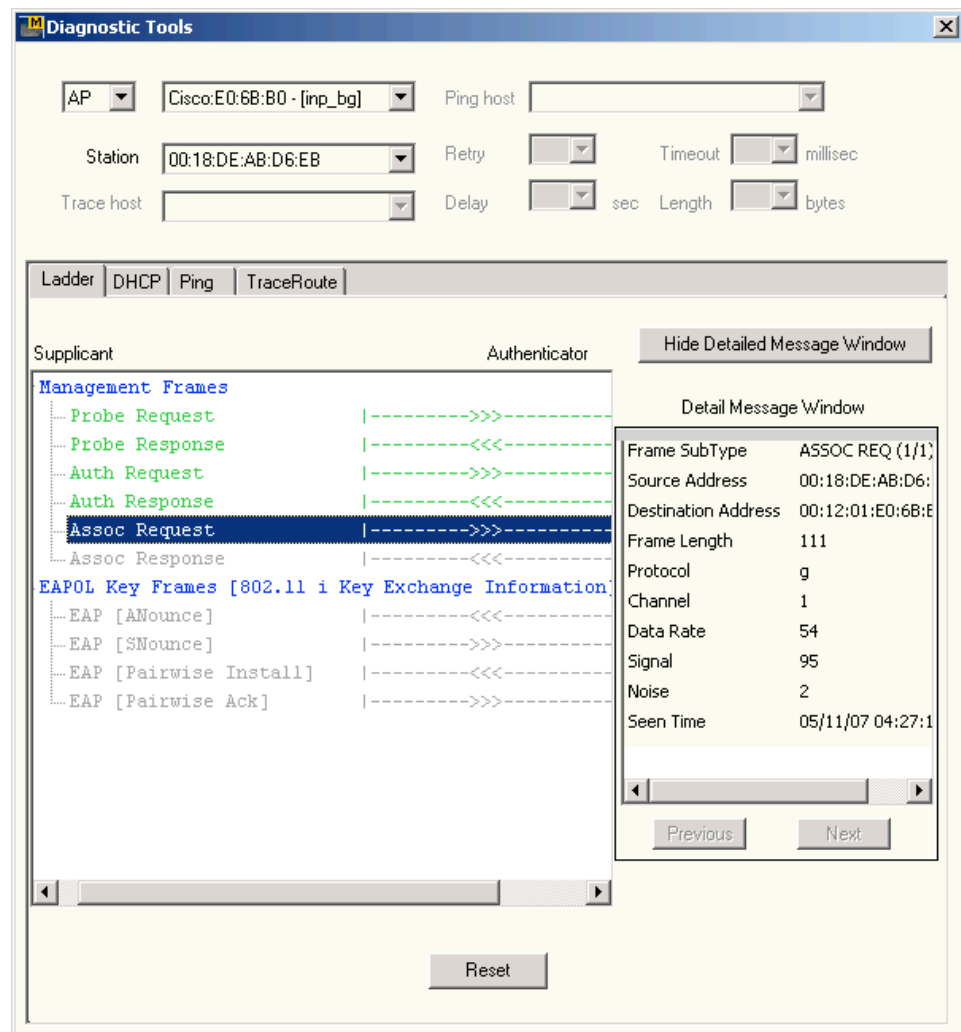
Station Summary View											
Last Seen	Probing Status	Strn MAC	Alias	Protocol	SSID	Channel	Signal Strength	Noise	Encryption	Authentication	IP
35/11/07 04:24:2...	✗	Agere Sy:3A:...	b	inp...	inp...	1	-59	-90	Off	Unknown	10
35/11/07 04:25:3...	✗	ASKEY CO:34:...	g	inp...	inp...	1	-66	-90	Off	Unknown	10
35/11/07 04:24:5...	✗	Apple Co:84:...	g	he...	he...	11	-100	-100	Unknown	Unknown	Un
35/11/07 04:25:2...	✗	Intel Co:10:4...	g	inp...	inp...	1	-60	-91	Off	Unknown	Un
35/11/07 04:25:4...	✗	Global D:22:9...	b	hp...	hp...	10	-77	-91	Off	Unknown	Un
35/11/07 04:25:3...	✓	00:18:DE:AB:...	b	Pro...	Unknown		-26	-91	Unknown	Unknown	Un
35/11/07 04:24:4...	✓	00:18:DE:AB:...	a	Pro...	Unknown		-23	-91	Unknown	Unknown	Un
35/11/07 04:25:3...	✗	00:18:DE:AB:...	g	inp...	inp...	1	-49	-92	Off	Unknown	Un
35/11/07 04:25:3...	✗	GemTek T:5E:...	g	inp...	inp...	1	-74	-89	Off	Unknown	Un
35/11/07 04:23:1...	✗	ASKEY CO:C6:...	a	Un...	Unknown		-61	-90	Unknown	Unknown	Un
35/11/07 04:25:2...	✗	ASKEY CO:C6:...	g	inp...	inp...	1	-64	-90	Off	Unknown	Un

Step 21. **Right click** your station MAC address and **change status to Authorized**. Type **DELL Internal** in the Alias field.

**NOTE:** AirDefense has now categorized devices as Authorized or unauthorized and created an alias for a station. Notice the change in the icons on the left hand side of the screen. Next you will look at troubleshooting a station connecting to an AP.

- Step 22. Click **Diagnostics Tools**.
- Step 23. Choose **your AP** and **your STA** from the drop down list.
- Step 24. Click **Start** and reconnect your STA to your AP and monitor the communications.

You might need to stop/start your wireless NIC to force a re-association.



You should see the station discover the network using probe frames, Authentication to the network, and Associate to the AP.

- Step 25. Extra bonus: Click on the **frame** to see details in the box on the right hand side of the screen.

AirDefense Mobile is a full-function professional tool. There are many other functions that are available to a WLAN professional. We recommend you print out and review the User Guide as well as watch a little training video we've included on your WLSAT Student DVD.

## LAB 7.3: Sniffing and Capturing Data on Open Wireless Networks

The purpose of this lab is to learn how to capture information on open Wi-Fi Networks. Wireless sniffers can capture data on unencrypted networks and display everything from an email or web page to FTP or telnet logins. Many applications used to send data on a wireless network including HTTP, FTP, Telnet, SMTP, POP3 and VoIP are unencrypted and as such can be captured by a wireless pen tester during a wireless security assessment.

### Product Information

#### Requirements / Dependencies

- POP3 server
- SMTP server
- FTP server
- NetResident
- Driftnet
- Aircap USB adapter
- Wireshark
- Nokia N800 Internet Tablet

Step 1. Plug the Ethernet cable into the back of the Linksys AP.



Step 2. Connect to the interface of the Linksys AP using a web browser.

Step 3. **Login to the AP** using *username admin* and *password admin*.

Step 4. **Configure** on the configuration menu and select **use MAC filters** and type the *MAC address of your Nokia N800 wireless station*.

Step 5. Click **Apply**.

Step 6. Verify connectivity with the Nokia N800 and Linksys AP.



- Step 7. Attempt to connect to the AP with the Dell Internal adapter. The Dell internal adapter should not connect.



- Step 8. Open *Omnipeek* and identify the MAC address of your Nokia N800.
- Step 9. **Right click on the Dell Internal adapter** and choose **properties**.
- Step 10. Click the **configure button**.
- Step 11. Click the **advanced tab**.
- Step 12. Select **Locally administered MAC** and type the **MAC address of the Nokia N800** discovered by using Omnipeek.
- Step 13. Click **OK**.
- Step 14. Click **OK** again.
- Step 15. Attempt to connect to the AP with the Dell Internal adapter. This time it should be successful.

## Lab 7.4: Technitium MAC Address Changer



Technitium MAC Address Changer allows you to change Media Access Control (MAC) Address of your Network Interface Card (NIC) irrespective to your NIC manufacturer or its driver. It has a very simple user interface and provides ample of information regarding each NIC in the machine.

### Product Information

#### Source

Technitium.com

Freeware

[www.technitium.com](http://www.technitium.com)

#### Where, When, Why

##### Computer Forensics—MAC Address Spoofing

You have just setup MAC address filtering for one of your company's wireless Access Points. For testing purposes, you've set it to block everything but your own MAC address. You'd like to test it without having to borrow someone else's computer for a unique MAC address. You take out your USB stick, load SMAC, assign yourself a new software MAC address, and attempt to access the internet through the AP, which you now cannot.

In order to 'Spoof' a MAC Address you need a tool to make the changes. For Windows OS you can use this tool to not only make changes to any NIC's MAC Address, but do resets to IP and DNS configurations as well.

#### Usage and Features

- Helps people to protect their privacy by hiding their real MAC Addresses in the widely available Wi-Fi Wireless Network
- Helps Network and IT Security professionals to troubleshoot network problems
- Test Intrusion Detection / Prevention Systems (IDS/IPS)
- recover (MAC Address based) software licenses

Every NIC has an MAC address hard coded in its circuit by its manufacturer. This hard coded MAC address is used by Windows drivers to access Ethernet Networks (LAN). This tool can set a new MAC address to your NIC, bypassing the original hard coded MAC address. Technitium MAC Address Changer is a must have tool in every security professionals tool box.

- Changes MAC address of Network Interface Card (NIC) including Wireless LAN Cards, irrespective of its manufacturer or its drivers.
- Has list of all known manufacturers (with corporate addresses) to choose from. You can also enter any MAC address and know which manufacturer it belongs to.
- Allows you to select random MAC address from the list of manufacturers by just clicking a button.

- Restarts your NIC automatically to apply MAC address changes instantaneously.
  - Allows you to create Configuration Presets, which saves all your NIC settings and makes it very simple to switch between many settings in just a click and hence saves lot of time.
  - Displays all information you would ever need about your NIC in one view like Device Name, Configuration ID, Hardware ID, Connection Status, Link Speed, DHCP details, TCP/IP details etc.
  - Displays total bytes sent and received through the NIC.
  - Displays current data transfer speed per second.
  - Allows you to configure IP Address, Gateway and DNS Server for your NIC quickly and instantaneously.
  - Allows you to enable/disable DHCP instantaneously.
  - Allows you to Release/Renew DHCP IP address instantaneously.
  - Displays DHCP lease obtained and lease expires time.
  - Allows you to configure Interface Metric instantaneously.
- 

### Requirements / Dependencies

- Supports all Microsoft(R) Windows(TM) NT based versions in all languages
- 

### Where to Go for More Information

[www.technitium.com](http://www.technitium.com)

---

### What you will do in this lab:

- Check your existing MAC address
- Use TMAC to spoof a different MAC address
- Prove your machine now has a different MAC address
- Restore your physical MAC address
- Try out some of the other features of TMAC

## Lab Part 1 - Change the MAC Address of a NIC

### Misconceptions

Many people believe MAC address, which is hard coded in the NIC card, cannot be changed. Yes, it's hard coded, but it can be changed only by removing the flash chip from the NIC card, re-programming it with new MAC address, and putting it back on the card. But this software does not change the hard coded MAC address. Technitium MAC Address Changer instructs Windows(TM) to use MAC address it has specified in windows registry. If no MAC address is specified to Windows(TM), it uses the hard coded one in the NIC to construct Ethernet or IEEE network frames (or simply packets), which are used at OSI layer 2. Also Windows(TM) changes MAC address of your NIC when Windows(TM) Network Bridge is enabled. The first number in the MAC address of the NIC added in the Network Bridge is set to 0x02. Changing MAC address of Network Bridge is not possible in Windows(TM) using this software.

### How Does It Work?

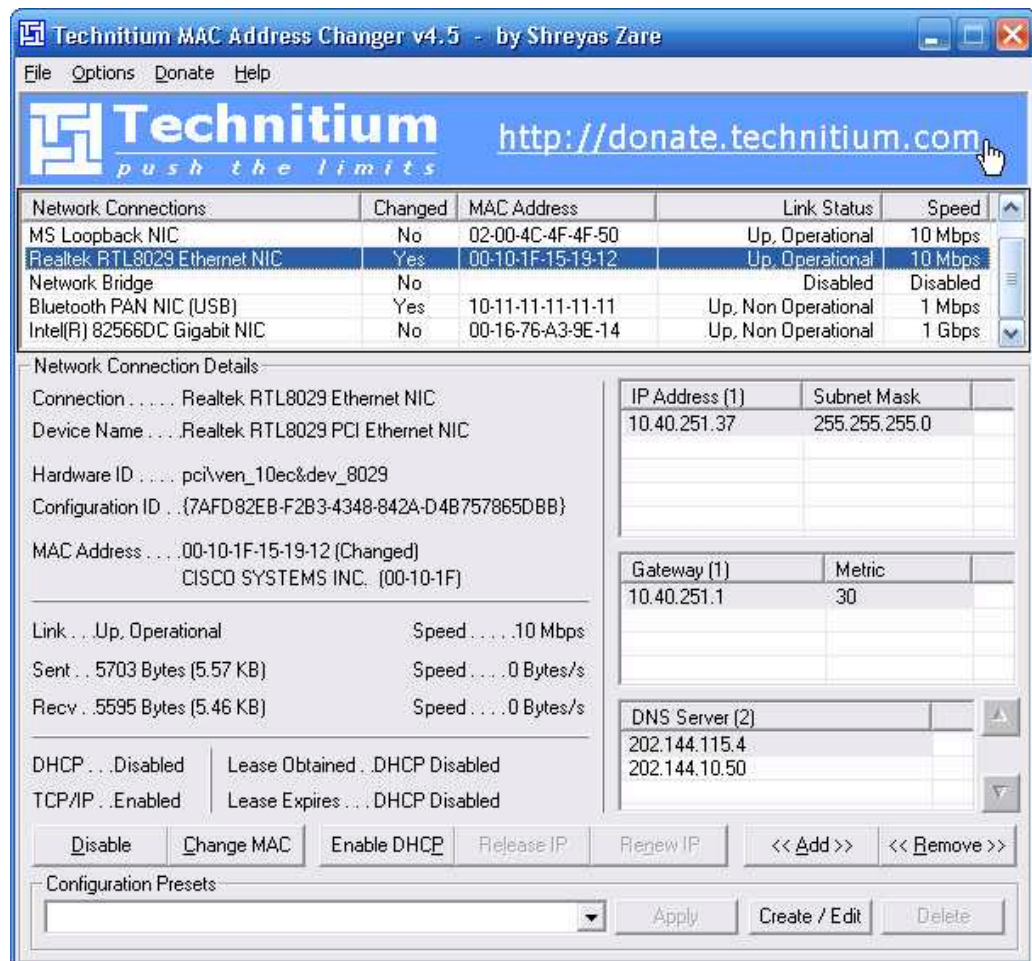
This software just writes a value into the windows registry. When the Network Adapter Device is enabled, windows searches for the registry value 'NetworkAddress' in the key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\[ID of NIC e.g. 0001]. If a value is present, windows will use it as MAC address. If not, windows will use the hard coded manufacturer provided MAC address. Simple? Some Network Adapter drivers have this facility built-in. It can be found in the Advance settings tab in the Network Interface Configuration tab.

- Step 1. **Launch Technitium MAC Address Changer (TMAC).**
- Step 2. Starting MAC address changer will list all available network adapters.
- Step 3. Select the **adapter** you want to change the MAC address. You will get the details of your selection below.
- |                     |    |                   |                 |         |
|---------------------|----|-------------------|-----------------|---------|
| Intel 3945 Wireless | No | 00-18-DE-AB-D6-EB | Up, Operational | 54 Mbps |
|---------------------|----|-------------------|-----------------|---------|
- Step 4. Click **change MAC button**, enter **new MAC address** and click **change Now** button and **confirm changes** you made when prompted.

- Step 5. To restore the original MAC address of the network adapter, select the **adapter**, click **Change MAC button** and then click **Original MAC button** and **confirm changes** you made when prompted.

**NOTE:** This tool cannot change MAC address of Microsoft Network Bridge. Network Bridge will automatically use the original MAC address of the first NIC added into bridge with the first octet of MAC address set to 0x02.

- Step 6. Now try out a few of the other options included in this substantial professional software in controlling your network interface cards.



## What you learned in this Lab:

In this Lab you learned to use Product to:

1. Checked your existing MAC address
2. Used TMAC to spoof a different MAC address
3. Proved your machine now has a different MAC address
4. Restored your physical MAC address

---

## Additional things you can do with this software

### Change MAC address of an Network Interface Card (NIC)

First, select the Network Connection for which you want to change the MAC address and click on Change MAC button. Now enter a new MAC address in hexadecimal format in the six blank text boxes provided for each hexadecimal number. You may click the Random MAC Address button to generate a random MAC address from the available list of manufacturers. You may also select a particular Vendor/Manufacturer from the drop down list to get a random MAC address for the selected vendor.

After entering a MAC address select the Automatically Restart Network Connection To Apply Changes check box if you want to restart the network connection. Now click the Change Now ! button and confirm changes you made when prompted.

### Change MAC address back to the original MAC address of NIC

To change MAC address back to the original MAC address of the NIC, just click the Change MAC button and then click the Original MAC button and confirm the changes you made when prompted.

### Enable/Disable a Network Connection

Select the Network Connection for which you want to perform the required operation and click the Enable/Disable button to enable/disable the network connection. After you click TMAC will not respond for 5 seconds. A message window will appear after the operation is completed.

### Refresh the Network Connection list

To refresh the Network Connection list, Click Options menu and click the Refresh menu item. You can also do this task by pressing F5 key.

### Add/Remove an IP address

To add an IP address, click on the << Add >> button, a menu will appear. Click on the IP Address menu item, an editor window will appear inside the main window (see screen shots). Enter IP address and enter the subnet mask. You can enter the subnet mask directly or enter a CIDR style notation for example /24 for 255.255.255.0 subnet mask. Select the checkbox below if you want to make the IP address persistent. A persistent IP address will be saved in registry and will persist across system reboots. A non persistent IP address will be flushed when the Network Connection is disabled or system rebooted. Now click Add IP button to instantaneously add IP address to the NIC.

If you click on the IP address list and start typing a new IP address, the IP address editor window will appear automatically saving time.

To remove an IP address, select the IP address from the list and press Delete key on your keyboard or you can click the << Remove >> button, a menu will appear, select the IP Address menu item to remove the selected IP.

### Add/Remove a Gateway

To add a Gateway, click on the << Add >> button, a menu will appear. Click on the Gateway menu item, an editor window will appear inside the main window. Enter IP address of the Gateway and enter the metric or check the Auto Metric checkbox. If metric is not specified, it assumed to be automatic metric. Select the Persistent Gateway checkbox below if you want to make the Gateway persistent. A persistent Gateway IP address will be saved in registry and will persist across system reboots. A non persistent Gateway IP address will be flushed when the Network Connection is disabled or system rebooted. Now click Add Gateway button to instantaneously add Gateway IP address to the NIC.

If you click on the Gateway list and start typing a new Gateway IP address, the Gateway IP address editor window will appear automatically saving time.

To remove an Gateway, select the Gateway IP address from the list and press Delete key on your keyboard or you can click the << Remove >> button a menu will appear, select the Gateway menu item to remove the selected Gateway.

### **Add/Remove a DNS Server IP Address**

To add a DNS Server, click on the << Add >> button, a menu will appear. Click on the DNS Server menu item, an editor window will appear inside the main window. Enter IP address of the DNS Server and click Add DNS button to instantaneously add DNS Server IP address to the NIC.

If you click on the DNS Server list and start typing a new DNS Server IP address, the DNS Server IP address editor window will appear automatically saving time.

To remove a DNS Server IP, select the DNS Server IP address from the list and press Delete key on your keyboard or you can click the << Remove >> button a menu will appear, select the DNS Server menu item to remove the selected DNS Server.

### **Change DNS Servers priority**

To change the DNS Server priority, select the DNS Server IP Address from the list and click the Up and Down arrow buttons, situated on the right side of the list, to move the priority either up or down. The top most DNS Server IP address has highest priority while the bottom most has the least.

You can even hold the ALT key on your keyboard in combination with the UP and DOWN navigation keys to perform the above operations.

### Enable/Disable DHCP on a Network Connection

Select the Network Connection on which you want to enable/disable DHCP and click the Enable DHCP/Disable DHCP button to perform the operation. You will be prompted to restart the selected connection in order to apply changes.

Note, all the previous IP and Gateway settings will be deleted when DHCP is enabled/disabled. Hence you are recommended to create Configuration Preset for the connection before performing the operation as in case you wish to revert changes.

### Release IP and Renew IP lease for selected connection

Select the Network Connection on which you want to Release IP/Renew IP lease and click the Release IP/Renew IP button to perform the operation.

Note, TMAC will not respond till the operation selected is finished or it has timed out.

### Set Interface Metric

Select the Network Connection on which you need to change the Interface Metric, click on the Options menu and click the Interface Metric menu item. You will be prompted to enter a metric value in a new window. The existing value in the prompt is the current value. Zero value indicated automatic metric. Enter a value and click OK to set a new Interface Metric value.

### Use the command line interface

Command line parameters are as given below with their description

```
tmac -n network_connection_name [-m mac_address / -r] [-h] [-i
ip_address_1 [, ip_address_2 ...] : subnet_mask_1 [, subnet_mask_2 ...] ] [-g
gateway_1 [, gateway_2 ...] : metric_1 [, metric_2 ...] ] [-d
dns_server_1 [, dns_server_2 ...] ] [-p preset_name] [-s] [-re] [-di] [-rn] [-rl] [-sv] [-ro]
```

#### Parameter Description -

- n Specifies name of the network connection/adaptor (NIC). Name may be complete or partial or just a part of it.
- m Specifies a MAC address. Blank MAC address implies original MAC address of the NIC.
- r Specifies to use a random MAC address from manufacturers list.
- h Enables DHCP and removes previous IP addresses and Gateways.
- rl Releases DHCP server assigned IP address.
- Rn Renews IP address lease from DHCP server.
- i Changes IP address. IP address list is comma separated, subnet masks list is comma separated. Both IP addresses and subnet masks lists are separated using a colon ':'
- g Changes Gateway address. Gateway addresses list is comma separated, metrics list is comma separated Both Gateway addresses and metric lists are

separated using a colon ':'

**-d** Changes DNS server address. DNS server address list is comma separated

**-s** Silent mode. Do not show any message window.

**-re** Restarts network connection/adapter.

**-di** Disable network connection/adapter.

**-p** Specifies name of a configuration preset saved earlier to be used. Preset name may be complete or partial or just a part of it. This parameter over powers all other network settings.

**-sv** Loads short vendor list which makes TMAC load faster. This parameter over powers all other parameters.

**-ro** Resets the original MAC address info saved in registry by TMAC. Use this only if original MAC address saved is wrong. This parameter over powers all other parameters.

**-help** Displays command line interface parameters list.