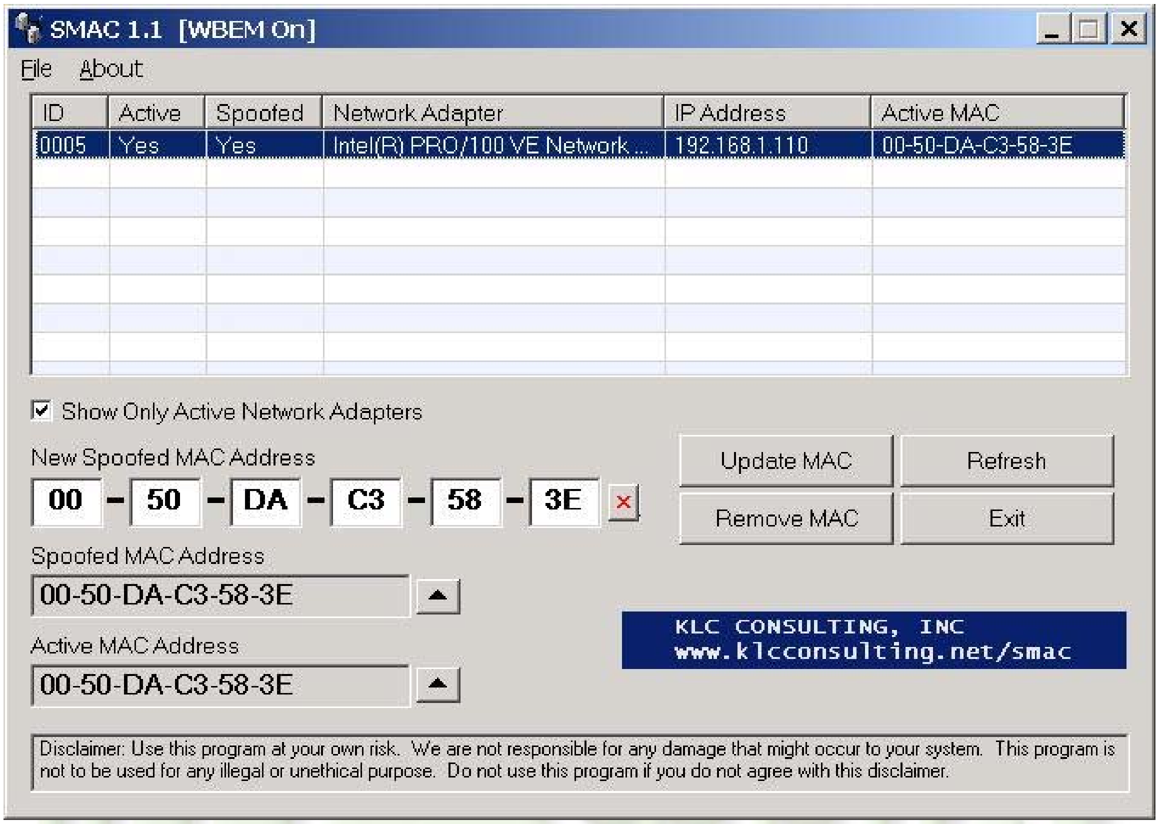
7.2.1

SPOOFING MAC ADDRESSES

(SMAC)



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0005	Yes	Yes	Intel(R) PRO/100 VE Network ...	192.168.1.110	00-50-DA-C3-58-3E

☑ Show Only Active Network Adapters

New Spoofed MAC Address

00 - 50 - DA - C3 - 58 - 3E

Spoofed MAC Address

00-50-DA-C3-58-3E

Active MAC Address

00-50-DA-C3-58-3E

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Laboratory Overview

Objective

At the end of this lab students will be able to alter the MAC address of their Windows 2000, XP, and 2003 systems. Students will become familiar with the operation of SMAC, a security tool which aids in the modification of the address.

Information for Laboratory

Students will use SMAC to alter the hardware address of their Network Adapters. The Instructor or lab aid will ensure the proper MAC address has been restored at the end of the lab.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Students will also need to install a copy of the SMAC application.

Estimated Completion Time

30 Minutes

What is a MAC Address?

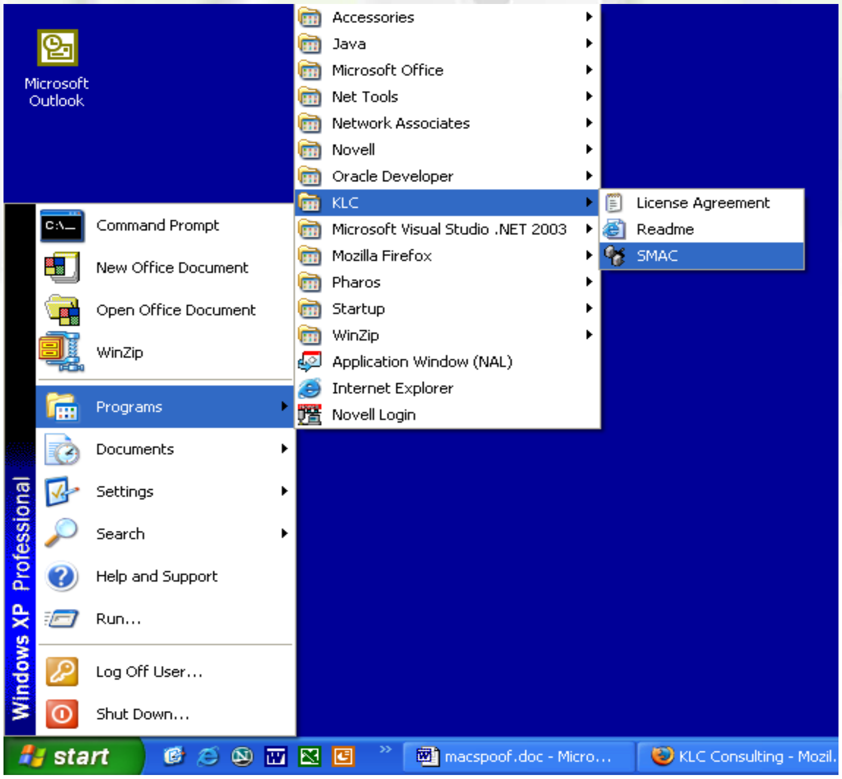
The Media Access Control (MAC) address, sometimes referred to as an Ethernet address, is the physical address for devices that are connected to your LAN. Each host connected to a network has a unique MAC address. This address is hard coded into the Network Interface Card (NIC) by the card’s manufacturer. This address is used to communicate with other devices on the same network.

SMAC

SMAC (Spoof Mac) is a utility that can be used to spoof the MAC address of a Network Interface Card on Windows 2000, XP, and 2003.

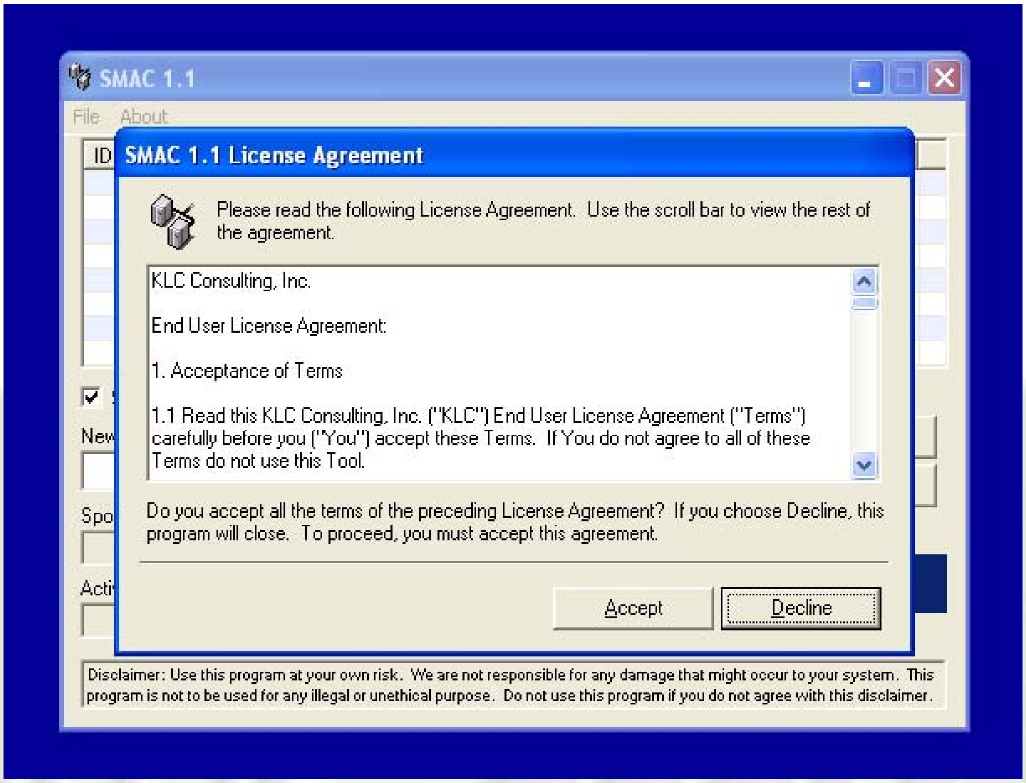
Step 1:

After you have installed the application, click on the **Start** Menu and maneuver your mouse to the **Programs** menu. Next, direct your mouse to the **KLC** application folder. Once you have done this, click on the **SMAC** icon.



Step 2:

If this is the first time you have run the application, you will be presented with a product License Agreement. Take a minute to read over it. When you are finished, click on Accept to continue.



Please read the following License Agreement. Use the scroll bar to view the rest of the agreement.

KLC Consulting, Inc.

End User License Agreement:

1. Acceptance of Terms

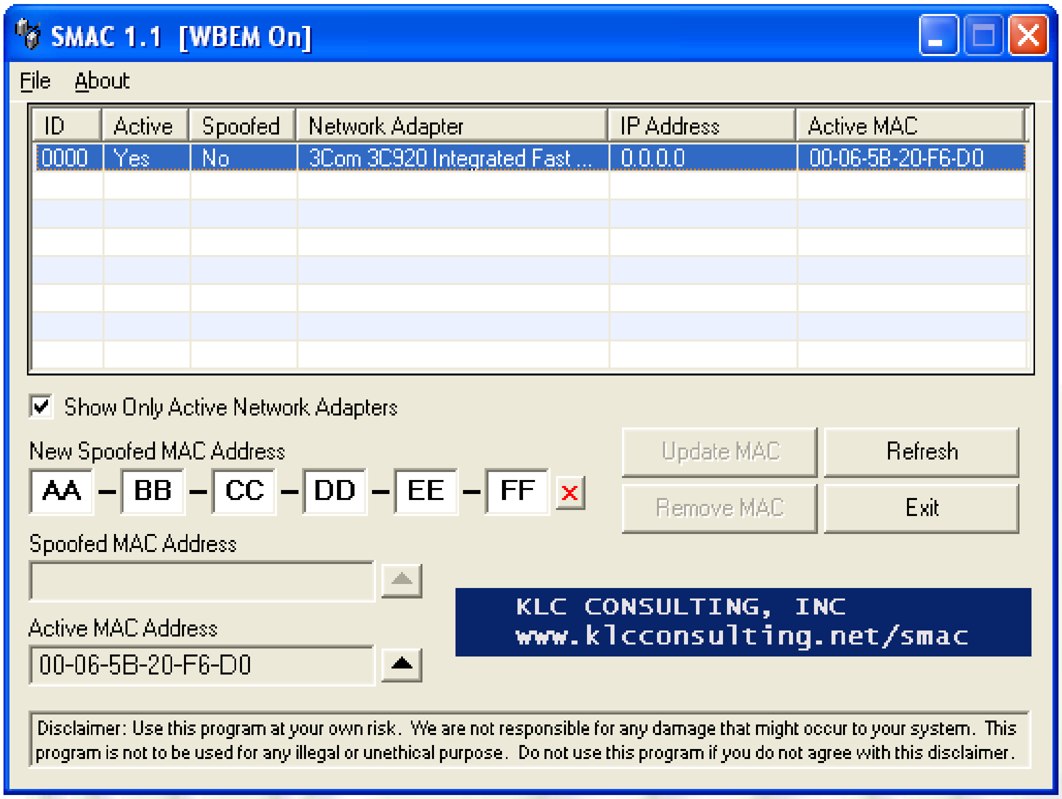
1.1 Read this KLC Consulting, Inc. ("KLC") End User License Agreement ("Terms") carefully before you ("You") accept these Terms. If You do not agree to all of these Terms do not use this Tool.

Do you accept all the terms of the preceding License Agreement? If you choose Decline, this program will close. To proceed, you must accept this agreement.

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Step 3:

You should see a screen resembling the following appear. Be sure to check the ‘Show Only Active Network Adapters’ box. Selecting this option will allow you to isolate and identify your own NIC.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	No	3Com 3C920 Integrated Fast ...	0.0.0.0	00-06-5B-20-F6-D0

☑ Show Only Active Network Adapters

New Spoofed MAC Address: AA – BB – CC – DD – EE – FF

Spoofed MAC Address:

Active MAC Address: 00-06-5B-20-F6-D0

KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

The **ID** Column represents your Network device ID.

The **Active** Column indicates whether a network adaptor is configured and available for use.

The **Spoofed** column indicates if the Windows Registry presently contains a spoofed MAC address entry.

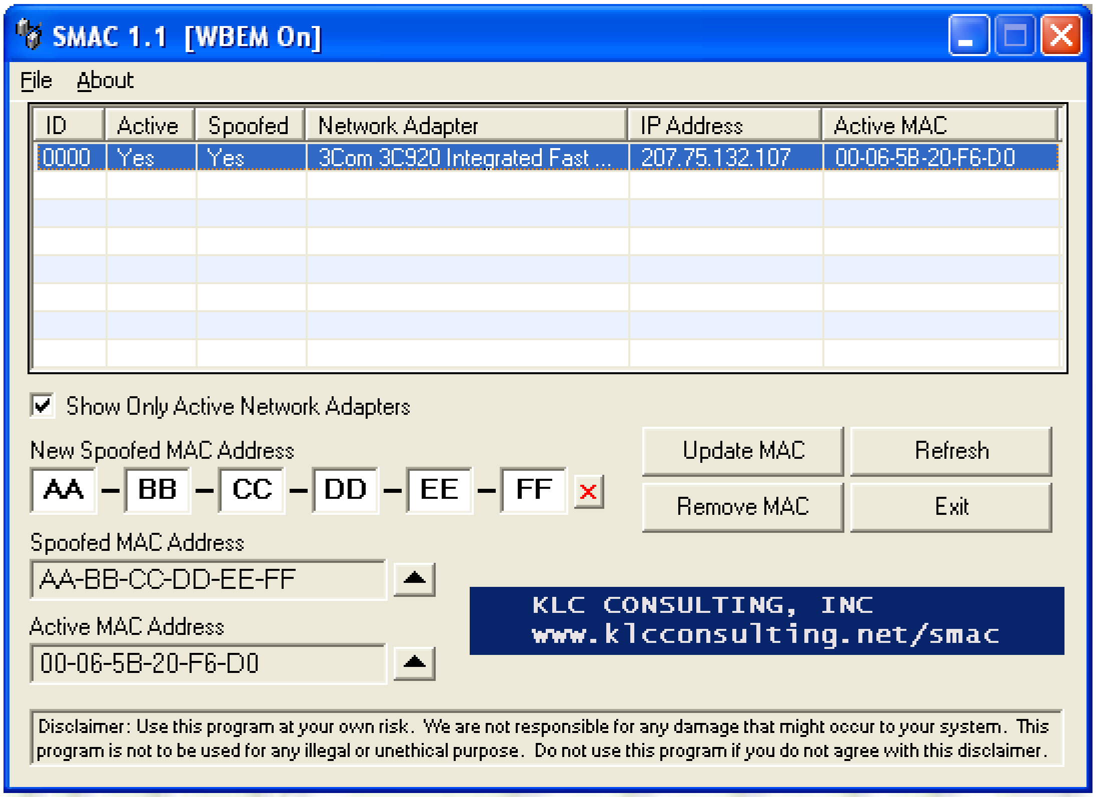
The **Network Adapter** column contains information about your NIC, including manufacturer and media compatibility type.

The **IP Address** column states your assigned IP address.

Active MAC displays the active MAC address for the network adapter.

Step 4:

Enter the value to be associated with your new MAC address in the New Spoofed MAC address field. Click on the Update MAC option. You will observe the Spoofed column has updated to indicate the registry entry now contains a counterfeit value.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	Yes	3Com 3C920 Integrated Fast ...	207.75.132.107	00-06-5B-20-F6-D0

☑ Show Only Active Network Adapters

New Spoofed MAC Address
AA – BB – CC – DD – EE – FF ×

Spoofed MAC Address
AA-BB-CC-DD-EE-FF

Active MAC Address
00-06-5B-20-F6-D0

KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

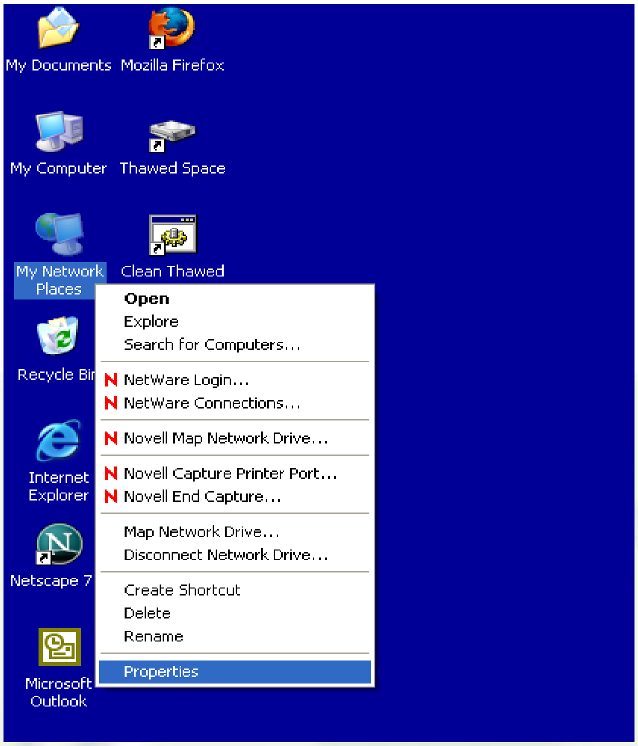
NOTE: When changing the MAC address, it is recommended that you assign the address according to the IANA Number Assignments database.

More information can be found at:
http://www.iana.org/assignments/ethernet-numbers

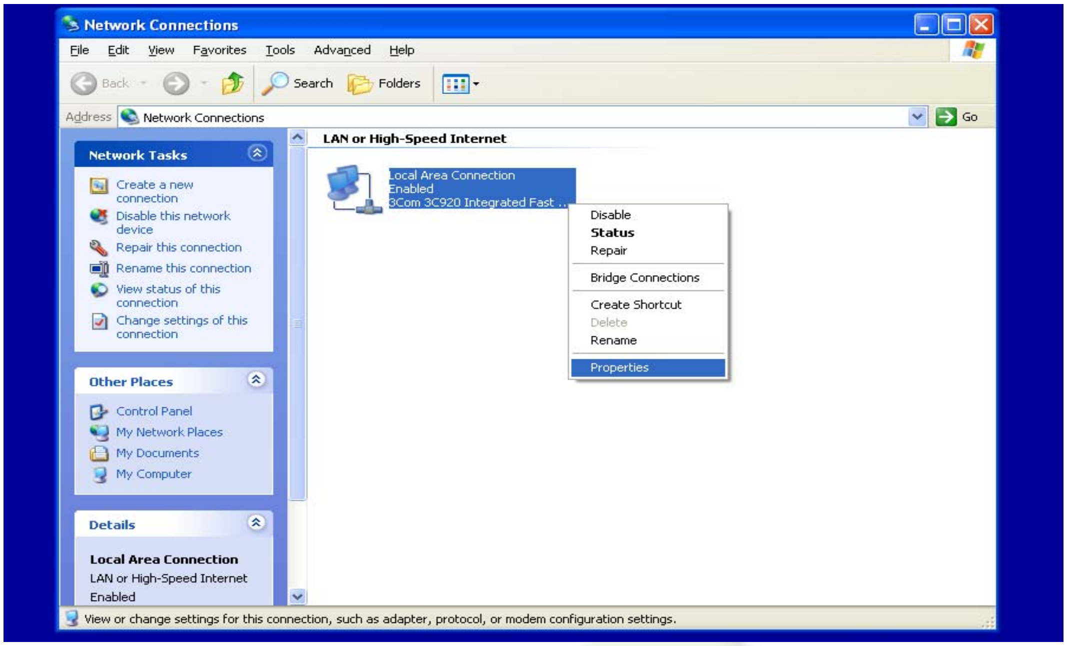
Step 5:

After you have clicked on the Update MAC option, you will need to disable and then re-enable your Network Adapter.

Right click My Network Places and select Properties.



The Network Connections window will open. Next, right click My Local Area Connection and select Properties.

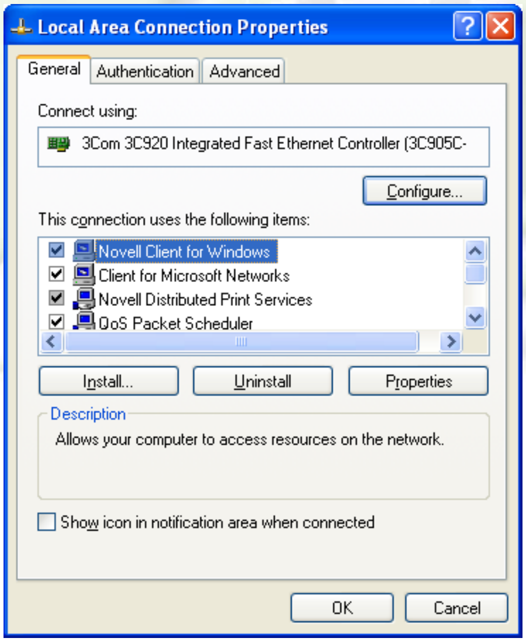


Local Area Connection
Enabled
3Com 3C920 Integrated Fast ...

Details: Local Area Connection
LAN or High-Speed Internet
Enabled

View or change settings for this connection, such as adapter, protocol, or modem configuration settings.

You will see a screen similar to the one below. Click on the Configure tab.



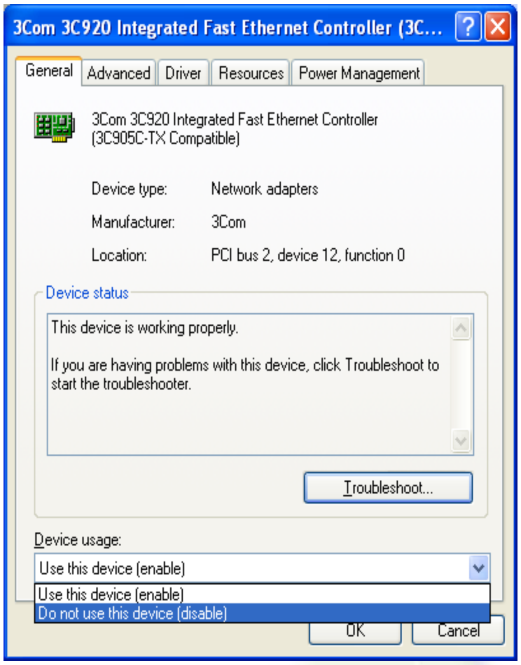
Connect using:
3Com 3C920 Integrated Fast Ethernet Controller (3C905C-

This connection uses the following items:
☑ Novell Client for Windows
☑ Client for Microsoft Networks
☑ Novell Distributed Print Services
☑ QoS Packet Scheduler

Description
Allows your computer to access resources on the network.

□ Show icon in notification area when connected

A window specific to your Network Adapter will open. Click the Device Usage arrow and select the option to disable this device. Click OK.



3Com 3C920 Integrated Fast Ethernet Controller
(3C905C-TX Compatible)

Device type: Network adapters

Manufacturer: 3Com

Location: PCI bus 2, device 12, function 0

Device status

This device is working properly.

If you are having problems with this device, click Troubleshoot to start the troubleshooter.

Device usage:

Use this device (enable)

Use this device (enable)

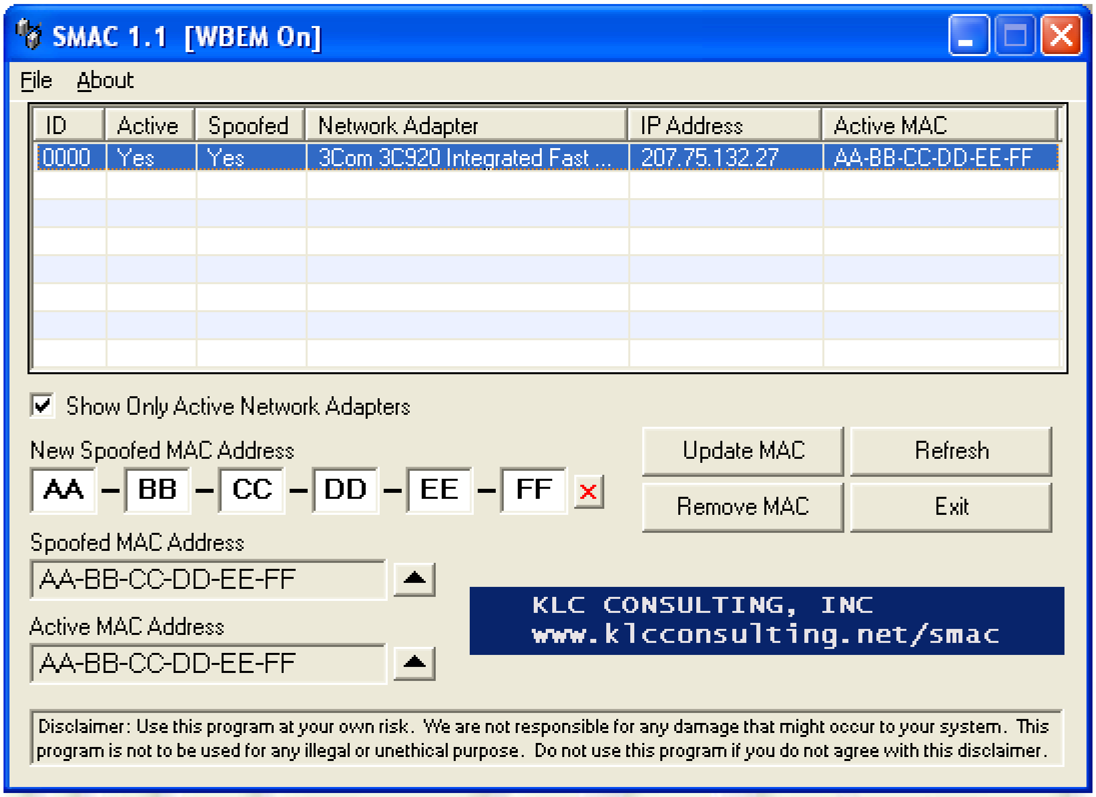
Do not use this device (disable)

Step 6:

Repeat the Step 5 from above. This time, choose to re-enable the device.

Step 7:

Click on the Refresh tab on the SMAC application. You will observe the Active MAC address has been updated with the value you specified.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	Yes	3Com 3C920 Integrated Fast ...	207.75.132.27	AA-BB-CC-DD-EE-FF

☑ Show Only Active Network Adapters

New Spoofed MAC Address: AA – BB – CC – DD – EE – FF

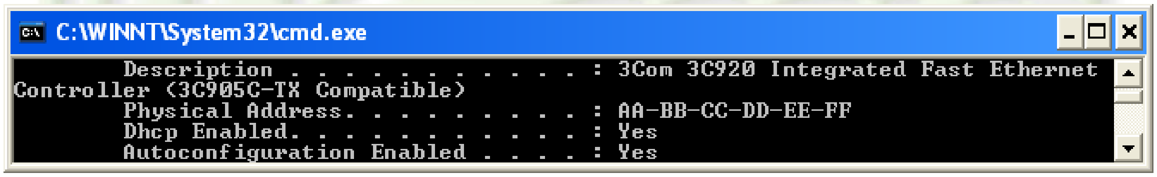
Spoofed MAC Address: AA-BB-CC-DD-EE-FF

Active MAC Address: AA-BB-CC-DD-EE-FF

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Step 8:

To verify the above, go to a command prompt and type ‘ipconfig /all’

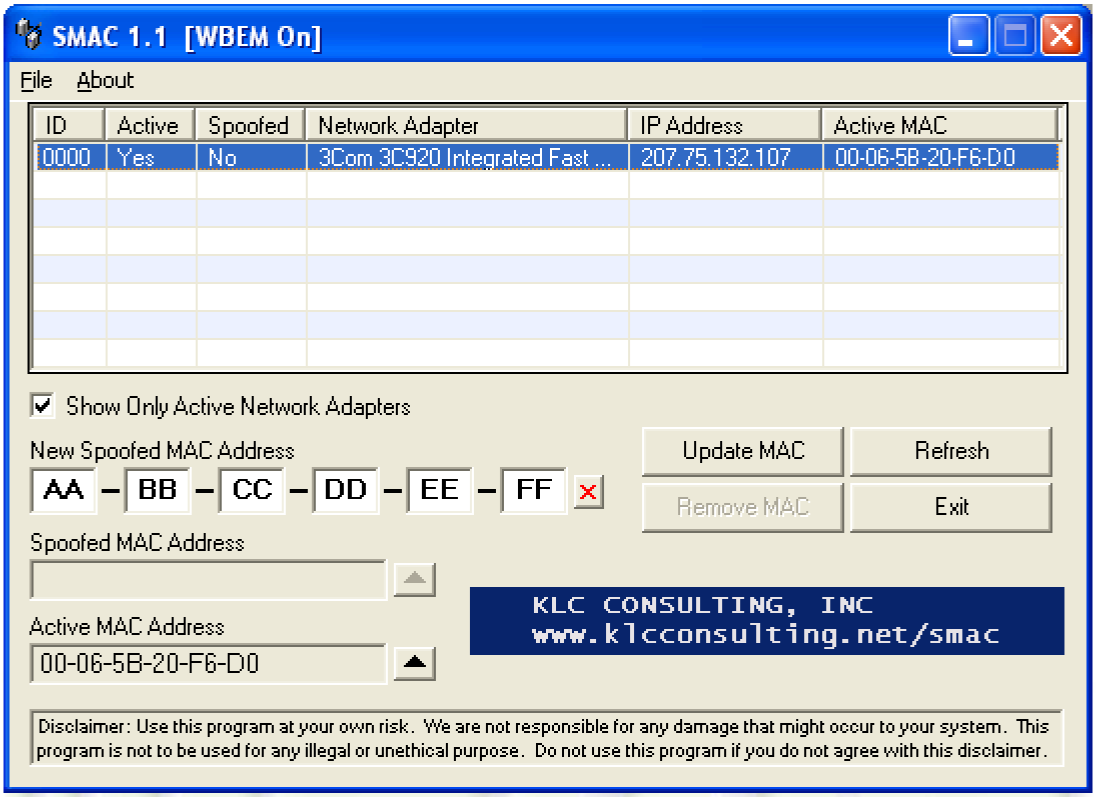


```
        Description . . . . . . . . . . . : 3Com 3C920 Integrated Fast Ethernet
Controller (3C905C-TX Compatible)
        Physical Address. . . . . . . . . : AA-BB-CC-DD-EE-FF
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
```

Notice the Physical Address has changed.

Step 9:

Once you have finished this lab, restore the true Ethernet address. To do this click on the Remove MAC option tab and repeat the steps above to disable, and then re-enable your Network Adapter.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	No	3Com 3C920 Integrated Fast ...	207.75.132.107	00-06-5B-20-F6-D0

☑ Show Only Active Network Adapters

New Spoofed MAC Address

AA – BB – CC – DD – EE – FF ✕

Spoofed MAC Address

Active MAC Address

00-06-5B-20-F6-D0

KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Analysis

1) Why does an attacker's ability to spoof their MAC address present a threat to your network's security?

2) What are some precautions you, as a Security Professional, can take to mitigate this threat?

3) How might you incorporate the above precautions into your organization's Security Policy?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Become familiar with the operation of the Data Link Layer, and the Open Systems Interconnect (OSI) model.

Appendix

This lab was designed using SMAC 1.1, which can be found at

http://www.klcconsulting.net/smac

SMAC 1.2 is now available.

The computer operating system was Windows XP Professional Service Pack 2