

Forum:[Hack Forums](#)

Thread: [How to Spoof your MAC Address](#)

NoodleBot™ - October 28, 2013, 10:33 pm

[img]http://i.minus.com/ieq6viOQ6szdE.gif[/img]

I see a lot of threads about MAC addresses with no answers so I thought it was about time for a good MAC address help thread.

Here is a few ways that I like and have found that work fine to spoof your MAC.

Method 1: EtherChange

Download v1.1 (<http://ntsecurity.nu/downloads/etherchange.exe>) (for Windows 2000 / XP / 2003 / Vista / Windows 7 / Windows 8)

Introduction

EtherChange can change the Ethernet address of the network adapters in Windows.

Usage instructions

Download the exe file and run it from a Command Prompt. It will give you the instructions you need. EtherChange only works if your account is in the Administrators group.

Troubleshooting:

Q: When I double-click on the file a window comes up and disappears immediately. What's wrong?

A: You must run the file from a Command Prompt.

Method 2: SMAC

Introduction

SMAC is a powerful, yet an easy-to-use and intuitive Windows MAC Address Modifying Utility (MAC Address spoofing) which allows users to change MAC address for almost any Network Interface Cards (NIC) on the Windows VISTA, XP, 2003, and 2000 systems, regardless of whether the manufacturers allow this option or not.

SMAC does not change the hardware burned-in MAC addresses. SMAC changes the "software based" MAC addresses, and the new MAC addresses you change will sustain from reboots.

SMAC helps people to protect their privacy by hiding their real MAC Addresses in the widely available wifi Wireless Network. SMAC also helps Network and IT Security professionals to troubleshoot network problems, test Intrusion Detection / Prevention Systems (IDS/IPS,) test Incident Response plans, build high-availability solutions, recover (MAC Address based) software licenses, and etc...

SMAC is the first Windows MAC Address Modifying Utility (since 2002), and it is developed base on the extensive research of KLC Consulting, Inc. SMAC is continuous updated with the latest trend in the networking and security, as well as valuable customers' wishes and feedbacks.

SMAC is created and maintained by Certified Information Systems Security Professionals (CISSP), Certified Information Systems Auditors (CISA), and Microsoft Certified Systems Engineers (MCSE), and professional software engineers. With combined efforts, SMAC is well designed to be an user-friendly tool for both the technical and non-technical users.

Download: <http://www.klcconsulting.net/smac/#Download>

Features of SMAC

MAC Address Lookup

Automatically Activate new MAC Address right after changing it (you have the option to manually activate)

Show the manufacturer of the MAC Address

Show All or "Only Active" network adapters

Randomly Generate any New MAC Address or based on a selected manufacturer

Pre-load MAC Addresses List and choose the new MAC address from the list (Professional Edition)

"IPConfig" button - click to show network adapter (IPConfig) info to confirm changes

User-friendly GUI and easy-to-follow User Guide

Change MAC Address in 3 clicks:

Select a network adapter

Click "Random" to generate a MAC Address to spoof

Click "Update MAC" to change and activate new MAC Address

Protect your personal privacy by hiding the real MAC Address of your Network Adapters

Easy, intuitive, and user-friendly GUI for viewing and changing MAC addresses

Display detailed information of all available adapters, or ONLY the active network adapters

Displays the following information of your Network Interface Card (NIC)

- o Device ID
- o Active Status
- o NIC description
- o NIC Manufacturer
- o Spoofed status (Yes/No)
- o IP Address
- o Active MAC addresses
- o Spoofed MAC Address
- o NIC Hardware ID
- o NIC Configuration ID

View and select the 10 Most Recently Used (MRU) MAC Addresses directly from the MRU list to

spoof

Generate comprehensive reports on Network Adapter details (Professional Edition only)

Built-in logging capability allows users to track MAC address change activities (Professional Edition has the option to turn-on or turn-off this option)

Remove spoofed MAC Address to restore original MAC Address

Troubleshooting / Extra Information

Any additional information about SMAC product may be found here:

http://smactool.com/smac/help/smac20_userguide.pdf

Method 3: MadMACs

Description

I hope you enjoy this little MAC address and host name changer. When Glj12 told me about his host name randomizer, I told him about my desire to make a MAC address randomizer. We decided it would be cool to rap them both together, so I ported parts of his VBScript to Autoit3.

MadMACs was designed with the privacy paranoid in mind. The two main things a DHCP server records when you get an IP from it is your host name and the MAC address of the network card you are connecting from. This is identifying information that not all users want to leave behind. MadMACs allows you to randomize this information after it runs and reboots.

Configuring MACs to Spoof and Randomize

Quote: The first thing you should do is copy MadMACs.exe to what ever directory you plan to have it run from. If mac-config.txt does not exist in the same directory as the binary a wizard will come up and guide you through configuring which adapters get their MAC addresses randomized. The Wizard will ask you what prefix to use on the MAC address, keep the default 00 unless you want to use a specific vendor's MAC address range. For a list of vendor specific prefixes see:

<http://standards.ieee.org/regauth/oui/oui.txt>

This wizard also lets you set a registry entry to automatically run the randomizer on start up. There are two possible command line parameters:

config

Brings up the setup wizard

remove

Removes all of the registry entries.

If you run MadMAX without parameters you are asked "Do you wish to remove MadMACs from startup and clear the registry? Click No to configure MadMACs instead or Cancel to forget the whole matter." Make the logical choice to get the desired outcome.

If you want MadMACs to randomly set your host name make a text file called dic.txt in the same directory as the binary. This text file's format is one word after another separated by line feeds. If you are feeling lazy just rename the file "sample dic.txt" that comes with MadMACs to "dic.txt". MadMACs will randomly select a word from dic.txt and make that your host name. You may not want to use the host name randomizing functionality if you need to reach the host with the same name every time.

Most of the setting don't take effect until the computer reboots (sort of :) there are exceptions, like if you disable and enable the adapter). Basically, the current session randomizes the next session. If you have questions about the code, ask on the Binrev forums so I don't have to answer the same questions over and over again in email.

I take no liability for the misuse of this code. If you mess up your system or network with a bad MAC address or host name it's your fault. Use at your own risk. I've only tested it in Windows XP, and Vista so far. Consider this code GPLed.

Download the Download Newest MadMACs now at (<http://www.irongeek.com/downloads/MadMACs1.2.zip>)

Now for last we have the two manual methods.

Manually Spoofing your MAC Address Windows 2000/XP/Vista: The Hard Way

In XP you can use the regedit to edit the registry from a GUI or the reg command to edit it from the console, I'll be using regedit. Information on all your NICs can be found the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\ . Under this key you will find a bunch of sub keys labeled as 0000, 00001, 0002 and so forth. We can assume any MAC address we want by finding the key that controls the NIC we want to change, putting in a string value called "NetworkAddress" and setting it to the MAC address we want to use formatted as a twelve digit hex number (example: 001). To find out which key is which we can search through them for the value "DriverDesc" until we find the one that matches the NIC we wish to alter. After you set "NetworkAddress" to the address you want just restart the NIC by disabling it then enabling it (or in the case of PCMCIA cards, just eject and reinsert). You can confirm the MAC address change by using the "getmac" or "ipconfig /all" commands.

If all else fails with the manual way, try the automatic methods posted above. If you can't use the programs, try the manual method!

Please leave feedback if this was helpful to you! I would appreciate it greatly.

Excalvius - October 28, 2013, 10:43 pm

Very nice tutorial, except, some images would be nice though.

This would have been really nice when I was in the MapleStory times.

NoodleBot™ - October 28, 2013, 11:24 pm

I had to prune down the images for HackForums 15 image post count! I then ended up removing most of them whilst leaving the rest of the idea there.