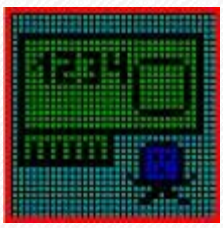
Tools from www.gorlani.com/portal:
Netboar: free and effective network analysis tool. Similar to iftop
Mac Makeup: change (spoof) your mac address
TurnItOn: enable disabled controls
Peks: checksum verification and modification tool for PE executables
Evtbak: batch backup your local/remote Windows NT event log
MyGears: gear/speed calculator
CTI: calculate rally times
Pinta: free simple customizable Mailenable antispam plugin

gorlani.com news

Vendesi appartamenti
Rally and fun
Setting up a mail server with FreeBSD
NetBoar is out!
Affitto casa
Back to school - building your dictionary
Configurare Asterisk con una BRI ISDN (italiano)
Antivirus results
MacMakeup 2.0
Gorlani.eu

Server time is 1/27/2008 7:14:57 PM

Versione in italiano
If you want to translate this page in your language, contact the author.



Mac MakeUp 1.95d

NEW!!! Go to this page and find vendor codes (ethernet OIDs) online!

Current release is 1.95 (20060116). You can download it here
MD5 Hash of the zip file is: **53822A94F78C92E76463541A8E69ABBF**
You can also find the BartPE Plugin version here

Jump to the end of page for release history

If you find it useful, you can donate 1 to 5 euros with PayPal. See Q0.

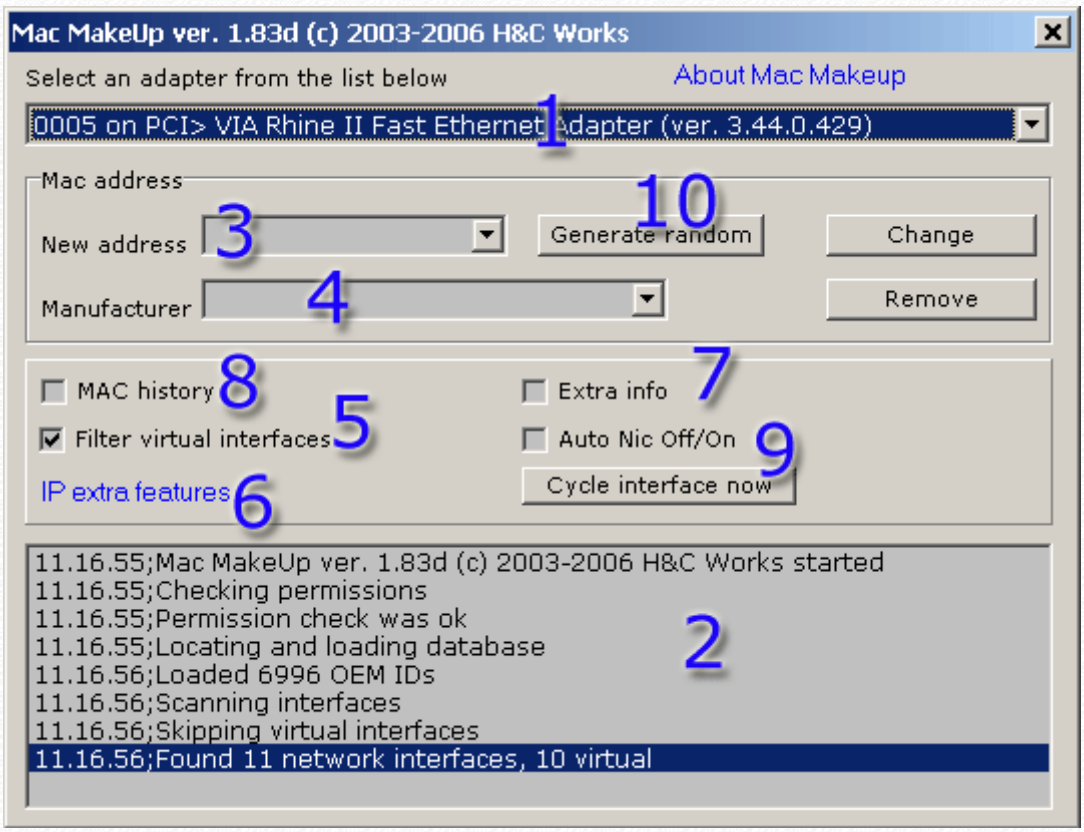
I need feedback from you! Jump to the forum and vote the poll. This will help in developing next version of Mac Makeup. Also note that on my home page there are others tools and forums to discuss!

What's this?

Did you ever get bored with your old MAC address? If you did, this is the solution! Mac MakeUp let's you change the MAC address of any of the interfaces present on your Windows 2000/XP/2003/Vista box.
Sometimes this is referred as MAC address spoofing.
You can choose a new address of your choice, or get the new one with the help of the tool, which sets the OID part according to your preference.

Well, how can I get it up and running?

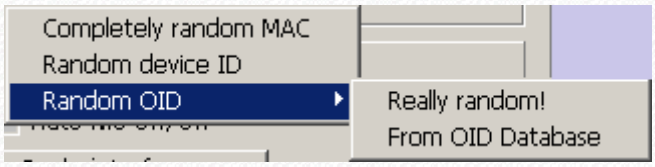
First of all, unzip the program into your preferred directory and start the program with administrative privileges. You should get a box like this:



Combo number (1) contains the list of the adapters you can select. The total number is shown in the last line of the log window (2). The adapter selected is the first PCI adapter in your system; the numbers after the name tell you the driver version.
If there is a "new" (spoofed) MAC for the adapter, it is shown in box number (3), and if it has a known OID the corrisponding manufacturer is show in box (4).
You can go back to your original MAC address by pressing Remove at this moment.
You can spoof the address by typing the new one into the box (3), or selecting a manufacturer from box (4). This creates a new MAC with the chosen OID and "123456" as device ID. Of course, you can change the device ID as you like.
Now just press Change and check the log for any errors. After disabling/enabling the adapter, your new MAC is in place.

That's all!
Also, if you start typing an OID into the box (3), there is an automatic lookup function that tells you what manufacturer you are referring to. Starting from version 1.91d Mac Makeup look for an installation of Wireshark: if you have it, the program will use tha OID database that ships with that tool. Authors of Wireshark made a great job with the sniffer and continuously update their manufacturers signature database. Also if you don't know Wireshark you're missing a very good network analyzer.
New from version 1.23d is the ability to filter out virtual interfaces. The filter is on by default, but you can disable it by clearing the check (5). Virtual interfaces are referread as the ones not being physical. From version 1.83d the filtering engine was revised to be more accurate and support different types of cards. Also the bus to which they are attached to is displayed.
If you check MAC History (8) the program looks for a file named *mmkup.ini*. This file contains the history of MAC addresses used on a per interface basis: this way you can use the combo box (3) to cycle through spoofed addresses. The file is located into the same directory of the main executable.
If you need to save the log window or clear it, just right-click on (2) and select the proper action from the popup menu.

Auto nic off/on (9) is new from version 1.83d and lets you disable and then reenable the network interface when you spoof its address. This way the change is immediate, no more need to open network connections applet or use external tools. The 'Cycle interface now' just disables/reenables the interface when you press it.

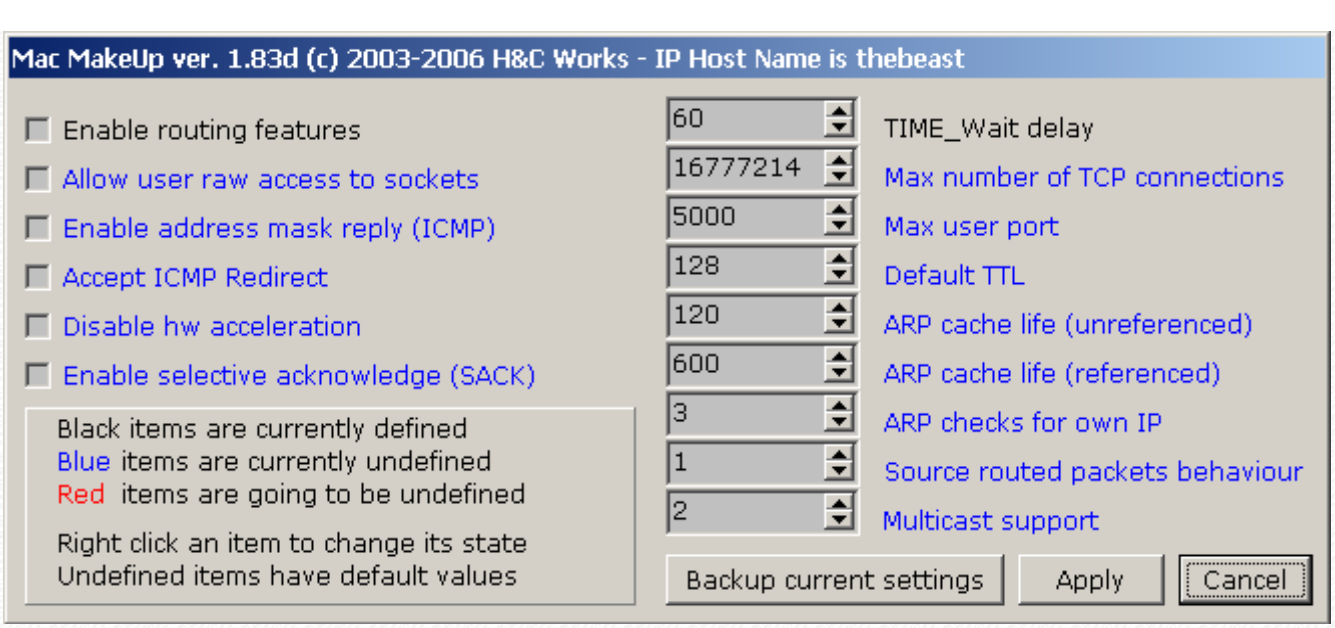
If you press (10) you have this 

menu that lets you generate a completely random mac address, a random device ID (mantaining the OID), or a new OID (mantaining device ID) taken from the database or autogenerated.

The log window now contains extra infos for any interface selected. Not all of these info are available all the times, dependig on the system settings, version and nic driver interfaces (it is fully functional with Windows XP SP2 and Broadcom 57x drivers for example).
These infos contain the *real* MAC address of your network interface (PermanentAddress), speed, IPs and so on.
Since it requires some seconds to load these infos, by default the Extra info checkbox (7) is disabled since it contains beta code and needs further testing.

IP Extra features

IP Extra features are available by clicking "IP estra features" (6). These options let you enable, disable or configure several aspect of Windows NT IP networking.
Figure below shows the options you can set:



Options can have three colors: red, black and blue.
Blue options are the ones not defined on your computer, meaning that Microsoft's default values will be used. The great part of IP Extra features are not defined by default, and this may vary depending on the software you've installed.
Black options are set, and their values will be used as shown.
Red options are the ones you are going to undefine (remove).
You can change the status of each parameter by right-clicking on the description and cycling though colors. Only defined (black) values are set pressing the "Apply" button. Undefined (blue) parameters are ignored. Undefined values are shown with their Microsoft default, so setting them without modifying the value **should** lead to no changes.
Please note there's a difference between undefined and defined but unchecked (for example).

The first thing you should do before experimenting, is taking a backup snapshot of your current configuration by pressing the "backup current settings button". This will ask you for a location to store a .reg (windows registry) file; double click on it at any time to revert to the starting situation.

Here is a very brief discussion about these parameters. Refer to Microsoft Technet documentation for any doubt. Please note that some of these directly impact your station's security.

Enable routing features	Makes your PC act as a router, forwarding packets from one interface to the other. Useful if you intend to use your laptop to route between wireless and wired networks
Allow user raw access to sockets	By default only admins can access raw sockets. This lets you override this setting
Enable address mask reply (ICMP)	Lets your station respond to subnet mask ICMP requests
Accept ICMP Redirect	Lets your station accept ICMP redirections
Disable hw acceleration	Disables task offloading to your network adapter (IP, IPSEC, ...)
Enable selective acknowledge (SACK)	See RFC 2018
TIME_Wait delay	The time a connection stays in Time wait state
Max number of TCP connections	Maximum number of TCP connections
Max user port	This controls the maximum port number used when an application requests any available user port from the system

Default TTL	This controls the maximum port number used when an application requests any available user port from the system
ARP cache life (unreferenced)	ARP cache life in seconds for unreferenced entries
ARP cache life (referenced)	ARP cache life in seconds for referenced entries
ARP checks for own IP	This controls the number of times that the computer sends a gratuitous ARP for its own IP address(es) while initializing
Source routed packets behaviour	0: Route All - 1 Do not route - 2 Drop incoming
Multicast support	0: No multicast support - 1: Send multicast - 2: Send and receive multicast

The command line mode

Mac Makeup has a command line mode since version 1.83d. This lets you script maniacs to include it into batches and set the new MAC addresses without intervention. You can disable/enable your interfaces with the ***devcon*** tool, you can find for free on Microsoft web site.

Command line usage:
`macmakeup.exe <count | <set | SET> <interface> <new_mac | random> | clear <interface> [quiet]`

enum: get a list of all the interfaces present, even virtual ones

set <interface> <mac>: sets <mac> on interface number <interface>
Just like: `macmakeup.exe set 4 010203040506`

If you use 'random' (without quotes) Mac Makeup will generate a random mac address for you.
Example: `macmakeup.exe set 4 random`
If you use '**SET**' (with capital letters) the interface will be disabled and reenabled to make the mac change effective.

clear <interface>: reset back to original mac address interface number <interface>
Example: `macmakeup clear 4`

quiet: optional parameter that sets the output mode to quiet, so that you have no kind of output.

If you don't use "quiet", the output of the program goes to a console. If the operations complete ok, then the console is closed. If there is some kind of error, the console is kept open and you're asked for confirmation before closing.

I have some questions...

Look at these FAQs.

Q0	How much does the program cost?
A0	The program is absolutely FREE. You must get it for free and freely distribute it. The program is NOT ad-supported nor it contains viruses or backdoors. To redistribute it, **please link this page**: it will always contain the last up to date version. If you mirror it, again put a link on this page. If you review it, please send me a link to the review

	 If you find it useful, you're encouraged to donate a little money with paypal. Sending 1 to 5 Euro will help in developing this and other tools. If you don't donate, you can still use the program without limitations and get assistance by the forum.
Q1	My list contains a lot of adapters, why?
A1	Because there are different adapters in your system, even some you don't suspect to exist, like dialup adapters. Also you can find adapters removed from your system without having them uninstalled first (so they are hidden, not removed).
Q2	I have to start the program after every reboot?
A2	No, you shouldn't. Changes are permanent until you decide to remove the new address.
Q3	Does the program installs its own device driver, DLLs, ActiveX controls or registry keys?
A3	No. The program just runs and does its job. You do not need to install the program. If you are bored with it, just delete the folder where you put it.
Q4	My adapter as an option to change the MAC address, so what?
A4	I'm happy you have such an adapter. There are a lot of adapters that do not allow you to change the MAC. This is especially true for wireless adapters.
Q5	You said wireless... What about the MAC address authentication based access points?
A5	They could have some problems, in that you can be authenticated as a regular user while you are not. I discourage the use of the tool as an intrusion one. You should only test it with your own access point.
Q6	Please, tell me more about Q5.
A6	A lot of access points let you get into the wireless network based on the MAC address. If yours is listed into the ACL of the AP, you can get in, else you cannot communicate. By changing your wireless adapter's MAC with a valid one, you can enter the network. This is a good starting point for studying and testing, but remember to use only your own access point.
Q7	Wow, the program breaks crypto based authentication systems?
A7	No, it doesn't. In fact I recommend you to use WEP, TKIP or WPA to protect your networks. Never rely only on MAC addresses to authenticate your clients.
Q8	I cannot find the combo to select an OID. Where is it?
A8	If the control is not shown, the database file failed to load. The log window should report this. Check that **oidb.hcw** is in the same directory where the program resides or install Wireshark
Q9	You said this is free, but I cannot find the source code.
A9	This is free, not open source.
Q10	The icon is absolutely ugly...
A10	Create a new one and send it to me. Maybe you can contribute to the next release.
Q11	Why did you wrote this tool and say not to use it for hacking into other's AP?
A11	This tool is useful for debugging and research. Other uses are discouraged, as I said before.
Q12	I have a question not listed in this page, what should I do?

A12	Send your comments, suggestions or usage reports to the forums at www.gorlani.com/portal
Q13	What do you mean with "virtual" adapters?
A13	I mean adapters that you do not see as "hardware" ones, like dialup adapters.
Q14	How do you consider interfaces into virtual machines?
A14	These are considered to be physical interfaces. This is a change from version 1.83d on. Mac Makeup was tested on all Windows from 2000 to Vista Beta 2 CTP in Microsoft Virtual PC 2004, VMWare Workstation 5.5 and GSX Server 2.5.
Q15	How can I stay up to date with new releases?
A15	Just click **?** on the main screen, and then click "check for updates". You can also register for free at http://www.gorlani.com/portal and get automatically notified by mail as new versions come out. Be aware that **you'll never receive** an email containing the new executable, but only the link to this page. Also remember to check the MD5 hash! See also Q19
Q16	I tried to download an older version, but the last one was retrieved...
A16	As new versions come out, older ones are removed from the site.
Q17	I cannot find the OID I'm looking for...
A17	I'm sorry, the included database obviously is not complete nor always up to date. If you find an OID that is missing, please contact me.
Q18	How can I use the router feature?
A18	Take a dual homed PC, connect each adapter to a network and set the default gateway for these network to each adapter IP address. Enable the router feature and reboot. There is **no need** to keep Mac Makeup running to have the router work.
Q19	What do you mean with "semi-automatic" updates?
A19	When you start the program, you have a 1/10 chance the program will ask you to go to its home page and lets you check for an update version. This is a compromise between asking you each time the program starts and never asking. There is no "don ask me anymore" checkbox because the program by design does not alter your registry at all nor it always need configuration files around, so it can't remember anything. If you contact me about it, maybe next version will be different
Q20	Is it the same to enable routing and starting "routing and remote access" service?
A20	No, it isn't. On Windows 2000 Pro and XP Pro/Home the RRAS service does not route traffic between networks. It can be done by properly configuring RRAS service on Windows 2000 Server and Windows Server 2003
Q21	I would like to discuss about Mac Makeup usage, problems, success stories and desiderata.
A21	Good. Just register to the portal and jump to the right forum! We need intelligent people to discuss about this and other projects that will be released in the near future
Q22	There are some MAC that your program is not compatible with?
A22	Really, no. MacMakeup can set almost any MAC address, but some network adapters cannot set their address due to driver/firmware limitations. This is true of course for **000000000000** that is not a valid MAC address, **FFFFFFFFFFFF** (broadcast), and some adapters complain when you try to set them to multicast.
Q23	Yeah! Now I'm ready to be an hacker!
A23	Mmmm, I think this is not enough :-))

Q24	You said you included Wireshark OID database into your program, but I find the same old **oidb.hcw**
A24	Wireshark database is NOT included with Mac Makeup, since this is the work of the people who made Wireshark. If you want it (trust me, this is the best choice) download Wireshark and install it.

Usage License

Don't worry, the program is always FREE software, just a couple of details...

By using this application, **you agree** to the terms below:
- You are granted to use this program for FREE, as it is FREE software
- You are allowed to use this program on one or more machines at a time
- You are allowed to distribute this program as long as you do it without profit and without modifications to this license (See note at the end)
- You may not modify or reverse engineer this program
- You may redistribute this program included as a support tool for your programs, as long you notify me by mail, get a positive reply and insert a note into tour software indicating the presence of Mac Makeup(*)
- The author has no obligation to provide assistance, defect correction or any kind of maintenance for this program
- Your are allowed to use it in any government environment. In this case an email notification to the author is appreciated

You **CANNOT** use this program if
- you intend to break into other people's networks
- you use it to access information you are not entitled to view
- you are a terrorist of any kind
- you don't know what you're doing, as you can disrupt network operations

If you don't agree, you MUST delete all the copies of this program.

(*) Really there is no reason to get a negative reply, only want to get stats and usage examples

BartPE Plugin

You can use Mac Makeup from 1.97d as a BartPE Plugin.
Just download this file (MD5 hash is **5CA65821EF6A744507E5FBFD71A7AF70**) and extract it into the Plugins directory of your BartPE installation.
Read the enclosed mmkup.htm file to get more info on using Mac Makeup on BartPE.

Release history

(20060116) 1.95d, MD5 hash **53822A94F78C92E76463541A8E69ABBF**
- Fixed a bug not powercycling an interface when removing spoofed mac
- Fixed a bug that prevented spoofed address from being removed
- Fixed a bug that sometimes showed the wrong interface being shut down in the log
= Changed the format of oidb.hcw file
+ Added support for Wireshark OID Database
+ Added hidden interfaces highlight

(20060103) 1.85d, MD5 hash **8A9C1880913AA9F31F26E62B586C91F3**

= Republished 1.83d that contained 2 buggy debug code lines

(20060103) 1.83d, MD5 hash **4B95F7733D27700D17C3F5A8C0F815C8**
+ Better handling of Extra (WMI) Info. This is still in beta.
+ Windows Vista Beta 2 CTP compatible
+ rewritten the filtering engine. Now more accurate recognition of virtual and external interfaces and detection for bus type
+ GUI: added ability to generate (partially) random addresses
+ command line: distinguish between 'set' and 'SET' commands. See help for details.
+ command line: added 'random' as a mac address option so generate a random mac address
- command line: corrected index of interface to be changed being subtracted by 1

(20040826) 1.71d, MD5 hash **BA159B4A98B97990C8F8EA81D43DD5A7**

+ Added extra info (Real MAC, IPs, Speed, ...)
+ Added log clear/save functions
+ Added MAC address history
+ Added command line mode
+ More friendly error messages
- Fixed a bug that could lead to "Cannot remove address" address error

(20040228) 1.53d, MD5 hash **C7A82BBA2EABA8D986A58E9855FB386D**

+ Added IP Extra features
+ Added semi-automatic updates check
+ OID lookup while you type
+ OS version checking to ensure proper operation

(20040122) 1.23d, MD5 hash **0FEDF03BE0A0D803993165E1702814E0**

- minor fix for Windows 2003 platform
- fixed problem on some Windows XP boxes that lead to "Must run with admin privileges" message
+ added ability to filter out virtual interfaces
+ added shortcut to check for last version
+ updated OID database
+ added debug messages to help individuate problems

(20031221) 1.11d

+ first public release

If you run Mac OSX, Mac Makeup inspired MacDaddy. You can find it here
Mac Makeup IS NOT related to MacDaddy, it is from another author

---

Current release is 1.95 (20060116). You can download it here
MD5 Hash of the zip file is: **53822A94F78C92E76463541A8E69ABBF**

Click here to send this link to a friend!

Tools from www.gorlani.com/portal:
Netboar: free and effective network analysis tool. Similar to iftop
Mac Makeup: change (spoof) your mac address
TurnItOn: enable disabled controls
Peks: checksum verification and modification tool for PE executables
Evtbak: batch backup your local/remote Windows NT event log
MyGears: gear/speed calculator

CTI: calculate rally times
Pinta: free simple customizable Mailenable antispam plugin

gorlani.com news

Vendesi appartamenti
Rally and fun
Setting up a mail server with FreeBSD
NetBoar is out!
Affitto casa
Back to school - building your dictionary
Configurare Asterisk con una BRI ISDN (italiano)
Antivirus results
MacMakeup 2.0
Gorlani.eu

Versione in italiano