Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b--Option 1

MAC Spoofing--An Introduction

Edgar D Cardenas
23 August 2003

Abstract
This paper covers what MAC spoofing is; why people use it; how it is accomplished; how to prevent it; and, what advantages MAC spoofing provides in penetration testing. MAC spoofing does not receive the same publicity as IP spoofing, but it is a more powerful and versatile tool in regards to breaking into a network, or for penetration testing. This practical paper also points out there are also some innocuous, "authorized" uses of MAC spoofing.

Every network interface controller (NIC) has a unique MAC (media access control) address "burned" into it. On a local area network, computers exchange their MAC addresses to identify each other. What is the difference, or commonality, between a MAC address and an IP address? They both identify where a frame came from, and where it is heading. However, an IP address can be easily assigned, and frequently are, to other machines. A MAC address is a hardware address, and it supposed to be permanent, following the NIC card wherever it goes. It is like the MAC address is the address for a house, to receive the postal service mail, and the IP address is like the telephone number. The "street address" (MAC address) and the "telephone number" (IP address) are both bound to the same house (computer on the network), but the telephone can be switched to another home, but the street address will remain the same. Every computer hooked up to a network uses a NIC card, and is used for identifying itself on the network.

Mac spoofing is computer identity theft, for good or for bad reasons, and it is relatively easy. MAC spoofing refers to altering the MAC address on a NIC (network interface controller) card. The MAC address is "burned in" at the factory. Therefore, each network card is shipped from the factory with a unique MAC address

MAC spoofing is done both for non-legitimate reasons--taking over another computer's identity—and for legitimate ones—like creating wireless connections to a network. Another example of a legitimate use of MAC spoofing is changing the function of a single computer from a router to computer and back to router through sharing a single MAC address. An example of an illegitimate use is when an intruder changes the MAC address of his station to enter a target network as an authorized user.

To prevent MAC address spoofing, or computer identity theft, one needs knowledge of the two schemes involved in preventing MAC spoofing attacks. One scheme is to detect MAC spoofing, the other is to harden the system, access points, or individual machines.
A quick way to detect if a suspected MAC address is being compromised is to run RARP (Reverse Address Resolution Protocol) against it. RARP maps a MAC address to an IP Address. As one MAC address should map to a single IP Address, Reverse ARP should return one IP address for one network device, so if multiple IP addresses return, one has evidence to pursue further investigation.

Since an intruder is trying to identify and duplicate existing MAC addresses on a LAN, defense involves searching for signs of MAC address guessing, detecting duplicate MAC addresses, and checking for multiple MAC addresses responding to a given address

We mentioned earlier that there are advantages of MAC spoofing in penetration testing. An essential component of penetration testing is the ability to specify arbitrary MAC addresses. An important feature of MAC spoofing in penetration testing is that it allows absolutely untraceable scans, because both source IP and MAC addresses are spoofed.
MAC spoofing can be used to test redirection of network traffic, and for testing access points. By allowing the impersonation of different MAC addresses within a network, MAC spoofing provides the facility for penetration tests to test firewalls, and to acquire information from a remote host.

MAC spoofing is the more sophisticated cousin of IP spoofing. By assuming the identity of another machine authorized to be on a network, it is a powerful tool for unauthorized entry into networks, the attack not drawing attention because it appears the invader is really a trusted user of the network. On the other hand, duplicating a MAC address can have positive effects. For example, impersonating a valid MAC address is also useful for authorized duplication of a NIC card. A good example where this can be seen when it is used to facilitate creating true hot fail over systems that require the use of the same MAC address of the primary system.

We will answer questions about how people use MAC spoofing to reroute network traffic, for legitimate, and non-legitimate purposes. We will answer how MAC spoofing can be accomplished through hardware or software modifications. How MAC spoofing attacks can be identified and defended against. How it is necessary for redirecting network traffic in penetration testing. And we will shine the light on how high-security networks should not use wireless devices due to the relative ease in using MAC spoofing to invade access points.

What is MAC spoofing?

Every network interface controller (NIC) has a unique MAC (media access control) address.

Ethernet Frame Format

Per IEEE-802.3: MAC header (14 Bytes) and trailer (4 bytes):

Destination address (DA) (48 bits)	Source address (SA) (48 bits)	Type/Length (16 bits)	Data (...)	Frame Checksum (FCS) (32 bits)

Type interpretation:

DA	Destination MAC Address	(6 bytes)
SA	Source MAC Address	(6 bytes)
Type	Protocol Type	(2 bytes)
Data	Protocol Data	(46 - 1500 bytes)
FCS	Frame Checksum	(4 bytes)

(Adapted from http://netcert.tripod.com/ccna/internetworking/eframes.html.)

On a local area network, computers exchange their MAC addresses to identify each other. Computers exchange their MAC addresses by the Address Resolution Protocol (ARP, see example at http://www.koot.biz/docs/tech/Obtaining%20passwords.htm.) before the IP connection is established. These ARP packets contain the MAC address of the sender. MAC addresses are hardware addresses that identify computers, servers, routers, etc.

The Hyperdictionary defines MAC as:

"(MAC) The lower sublayer of the OSI data link layer. The interface between a node's Logical Link Control and the network's physical layer. The MAC differs for various physical media." (See definition at http://www.hyperdictionary.com/dictionary/Media+Access+Control.)

MAC Addresses

"The Ethernet numbers include the 48-bit media access control (MAC) address assigned to each Ethernet interface, and the 16-bit value used in the Type field of the Ethernet frame….
Each Ethernet interface is assigned a unique MAC address at the time of manufacture. The first 24 bits of the MAC address consist of an Organizationally Unique Identifier (OUI) assigned to a vendor by the IEEE, which is why they are also called vendor codes. The Ethernet vendor combines their 24-bit OUI with a unique 24-bit value that they generate to create a unique 48-bit address for each Ethernet interface they build." (Spurgeon, first two paragraphs at http://www.ethermanage.com/ethernet/descript-troubleshoot.html)

MAC Address Examples

MAC Address	Manufacturer Code	Serial Number
DD34.2344.13FD	DD34.23	44.13FD
13CC.7800.34FF	13CC.78	00.34FF
110D.CC60.1388	110D.CC	60.1388

(Adapted from http://netcert.tripod.com/ccna/internetworking/eframes.html, scrolling 3/5 down the page)

Mac spoofing is computer identity theft, for good or for bad reasons, and it is relatively easy. MAC spoofing refers to altering the MAC address on a NIC (network interface controller) card. The MAC address is "burned in" at the factory. Therefore each network card is shipped from the factory with a unique MAC address. Every computer hooked up to a network uses a NIC.

Computers on the LAN (Local Area Network) send ARP (Address Resolution Protocol) packets to each other before the IP connection is established. ARP packets identify the sender by carrying the one's MAC and IP addresses.
Like IP spoofing, some hackers use MAC spoofing as a Layer 2 attack to attempt hijacking a communication session between two computers with the purpose of hacking one of the machines.
A MAC-spoofing attacker attempts to break into a LAN by assuming the MAC identity of an authorized computer station on the LAN. MAC address spoofing in this context relates to an attacker altering the manufacturer-assigned MAC address to a value that facilitates invading a LAN. This is opposed to the traditional notion of IP address spoofing where an attacker sends data from an arbitrary source address and does not expect to see a response to their actual source IP address.

So, how does this method of attack compare to the more familiar, more common, IP spoofing?
IP spoofing is a process used by hackers to hijack a communication session between two computers, which we will call Computers A and B. A hacker can send a data packet that causes Computer A to drop the communication. Then, pretending to be Computer A, the hacker can communicate with Computer B, thus hijacking a communication session and attempting to attack Computer B.
An IP spoof attack can direct response packets traffic at a target. For instance, if I want Joe.com server to go down, I can send packets to Steve.com, and other servers, with crafted data frames with Joe.com's IP address. The Steve.com server does not know any better that the IP source address is spoofed, so it starts sending messages to Joe.com. Escalate this scenario with multiple Steve.com servers, and Joe.com server will likely fail, providing an opening under this denial-of-service attack.

Malevolent MAC spoofing involves actually invading a network, and taking over a machine within that network.
A typical attack involves using two tools. The first tool, a sniffer, picks up LAN traffic to pull out authorized MAC addresses. The second tool, a MAC address generator. constructs and packages network packets with the “stolen” authorized MAC address.

Why is MAC Spoofing Done?

MAC spoofing is done both for non-legitimate reasons--taking over another computer’s identity -and for legitimate ones—like creating wireless connections to a network. Another example of a legitimate use of MAC spoofing is changing the function of a single computer from a router to computer and back to router through sharing a single MAC address. An example of an illegitimate use is when an intruder changes the MAC address of his station to enter a target network as an authorized user.

Non-Legitimate uses of MAC spoofing

An example of an illegitimate use is when an attacker changes the MAC address of his station to enter a target network as an authorized user-taking over a computer’s identity that is authorized to function on the network. With this new identity, an attacker can wreak havoc: for example to launch denial of service attacks, or to bypass access control mechanisms to advance more intrusion. An attacker might choose to change one’s MAC address in an attempt to evade network intrusion detection systems, to become invisible to security measures, allowing more time to act without detection.

Legitimate uses of MAC spoofing

An example of a legitimate use of MAC spoofing is changing the function of a single computer from a router to computer and back to router through MAC spoofing. If you only have a single public IP, you can only hook up one unit directly (PC or router). If one has two WAN IPs, the MAC address of the two devices must be different.
For whatever reason, if one needs to swap 2 PC's regularly to connect to the cable modem, it would be a lot easier to change the MAC addresses rather than to change the Network Interface Card (NIC). Many cable modem routers have a "Clone MAC Address" feature built-in for this. (In reality, the easiest way to enable two machines to access the same ISP from the same location is to use a cable modem router like LinkSys, which allows multiple MACs to use a single ISP connection.)

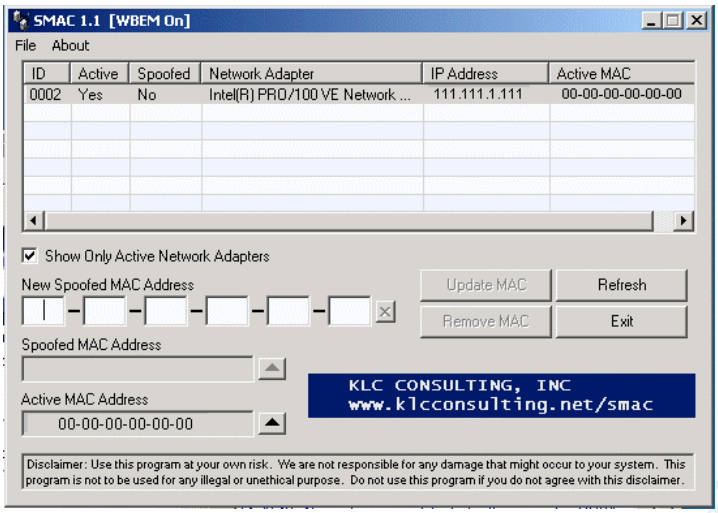
SMAC (See http://www.klcconsulting.net/smac.) advertises that its Windows tool can be used “for a hot back up system…” The idea is that one can set up a back up system with the same computer name, IP, and MAC addresses as the primary system. In case of fail over, there would be time savings as no ARP table refresh would be needed, making the back up system immediately available.

SMAC can also be used for troubleshooting network issues, system problems, for testing network management tools, and for testing intrusion detection systems.
MAC spoofing is also advantageous in wireless testing. The point is that a user may need and want to spoof one's own machine MAC address, with no malevolence involved.

How is MAC spoofing done?

There are MAC spoofing products, like SMAC, and utilities, like libnet (See http://www.packetfactory.net/papers/Libnet-primer/.), that allow MAC spoofing on UNIX and Windows systems. (For free Libnet download, go to http://gps.sourceforge.net/libs/libnet-1.0.2a.tar.gz.)
With MAC spoofing tools one has to choose addresses that are not already present on the network. Otherwise, the presence of two identical MAC addresses on the same Layer-2 LAN can cause switch convergence problems.
There are two methods to spoof a MAC address, through hardware or software
The hardware solution involves changing the EEPROM settings on the network interface card, Once one has the target MAC address, one can reprogram the EEPROM on the NIC card, but it involves a lot more technical knowledge than a software solution. Most MAC spoofing involving hardware changes are done by "authorized users," for their networking needs, not by hackers.
SMAC is sold as a MAC spoofing software product. (Free download for personal use is available at http://home.attbi.com/~rbourret/download/smac_1.1.zip.).
It works on Windows, and is referred to as a MAC Address Modifying Utility. It allows users to change quickly and easily their MAC addresses on their NICs. Instructions are included, and little network knowledge is needed.
The SMAC tool works locally, not on the LAN. It uses a Windows function, . NdisReadNetworkAddress, to look in the local registry for the current local MAC address. Then, the network adaptor driver overrides the factory set MAC address with changes to the MAC address on its hardware registers. The MAC address chosen must always be within IANA address-assignment guidelines. A non-IANA-compliant address, like 00:00:00:00:00:00, simply will not work.

Below is a screen capture of the SMAC GUI, with IP and MAC addresses changed (to protect the innocent). Notice how easy it is to change, spoof, on your own Windows OS PC.



How are target MAC addresses identified? In conjunction with a network sniffing tool, dsniff, one can pull real MAC addresses off the network traffic. One can then input one of those addresses into a MAC address modifying utility, like SMAC, converting one's MAC address into a network-authorized one.

MAC Changer (http://www.alobbs.com/modules.php?op=modload&name=macc&file=index) is an equivalent freeware software tool for spoofing MAC address on GNU/Linux. One can download version 1.3 at http://savannah.nongnu.org/download/macc/macchanger.pkg/1.3.0/macchanger-1.3.0.tar.gz

Libnet, on the other hand, is a high-level API (toolkit) which also does not reprogram the hardware. Designed and maintained primarily by Mike D. Schiffman (mike at infonexus.com).
"Libnet is a reasonably small programming library, written mainly in C, providing a high-level,
standard portable interface to low-level network packet shaping, handling and injection primitives." (Shiffman page 2)

It works by providing spoofing directly on the LAN by construction and packaging of network packets with the spoofed MAC address.

Cain, an all around intrusion device, is also used as a MAC spoofing tool. Its default MAC spoof address is simply 00:11:22:33:44:55, mostly because this address is not supposed to exist in a network.

To reprogram wireless network devices, vendors package drivers to allow creating different MAC addresses.
Let's look at Dell TrueMobile 1150 on Windows XP.

The procedure on Windows is:

1. Open Network Connections,
2. Click on the specific wireless net icon.
3. Select Change settings for this network.
4. Look at the General tab, there is Dell TrueMobile 1150.
5. Choose Configure
6. Select the Advanced tab, and select the appropriate parameter
7. Fill in a new value.

Alternatively, one can also navigate to the card configuration Windows dialog through Control Panel, System, Hardware, Device Manager. Right click the line for the card and choose Properties, then input a new value.

How does one stop MAC Spoofing?

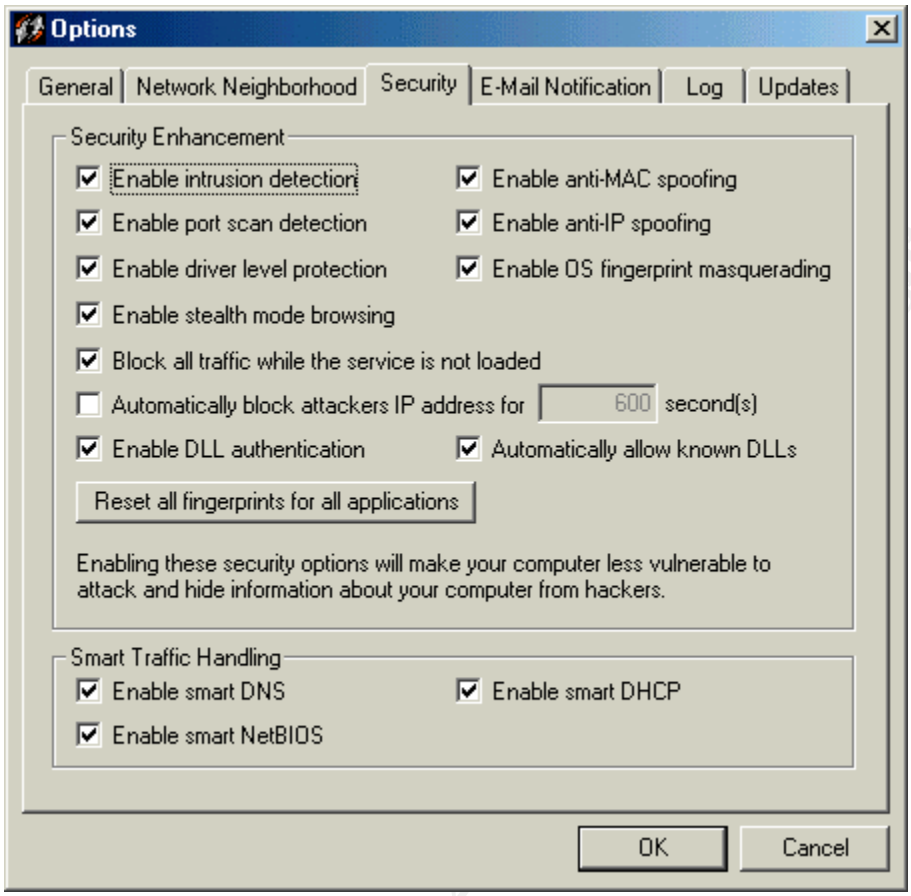
Two schemes are involved in preventing MAC spoofing attacks. One scheme is to detect MAC spoofing, the other is to harden the system, access points, or individual machines.
A quick way to detect if a suspected MAC address is being compromised is to run RARP against it. If multiple IP addresses return, one has evidence to pursue further investigation.
By having a firewall, like Sygate, (See Sygate Firewall Help Site at http://bellsouthpwp.net/i/k/ikpe/SygateBasics.html#GUI.), or running a service/daemon like echolot, configured specifically for MAC SPOOFING, one raises protection against MAC spoofing. Time wise, it is relatively easy and fast to set up, as we shall see later.
Configuration methods to harden systems to prevent MAC spoofing attacks include:

- Enabling "sticky" ARP.
- ARP table-based MAC/IP filtering
- MAC locking (For more information, go to http://www.xs4all.nl/~rmeijer/wayback.html.)
- Implicit MAC/IP filtering

Since an intruder is trying to identify and duplicate existing MAC addresses on a LAN, defense involves searching for signs of MAC address guessing, detecting duplicate MAC addresses, and checking for multiple MAC addresses responding to a given address.

The Sygate firewall is user-friendly, and involves little/no technical knowledge to set the anti-spoofing feature, as shown below. The graphical user interface makes choosing the “Enable anti-MAC spoofing” feature simply a matter of selecting a checkbox.

Below are the security options on the Sygate GUI. Notice the enable anti-MAC spoofing option on the top right column.



(Screen shot is from http://bellsouthpwp.net/i/k/ikpe/images/options%20Security.png.)

The echolot utility

The utility called echolot (http://echolot.sourceforge.net/), download available at http://echolot.sourceforge.net/echolot-download.html, reports if a computer gives a different MAC address in the ARP packet than its Ethernet frame indicates. It does not take countermeasure, but logs evidence of intrusion attempts. If someone claims a different IP address on one's LAN, echolot will report this. If echolot is run in daemon mode, it will log all information to syslog and one can see which host had a IP at a particular time.
One would know the date, time, and IP address of which host was used in an attack by auditing echolot's syslog output. Detecting MAC spoofing attempts are the first step in preventing and taking action in defense.

Sticky ARP

Tools, like firewalls or services, may enable "sticky" ARP (See page 11 Private VLANs on Catalyst 6000, at http://www.informit.com/isapi/product_id~%7BDBBECCF4-42A3-46D3-A337-

685E29F3CAFC%7D/content/images/1587050250/samplechapter/1587050250CH05.pdf.). The goal is to keep end stations from being able to change their MAC address. The down side is that "sticky" ARP is high maintenance.

It is highly recommended to implement ARP table-based MAC/IP filtering solution to better secure otherwise insecure shared-segment networks. The use of these filters unfortunately is not possible in the majority of operating systems,

MAC locking

MAC spoofing can be big problems on shared-segment networks. However, the current generations of Ethernet switches are offering us a basis for defeating this kind of intrusion by offering us MAC locking. It is possible to lock a MAC address to a specific physical port on the switch. When MAC-locking locks a MAC/port combination, it prevents the MAC address from being used from any other port on the segment.
This combined with static ARP and MAC/IP filters could totally eradicate the spoofing possibilities on a shared-segment network.
Expensive, managed switches allow port locking, but the disadvantage is the overhead cost is typically out of reach.

ARP table-based MAC/IP filtering in shared-segment networks

The use of the (static) ARP table in combination with the routing table could prevent most of the shared-segment spoofing possibilities.
Most operating systems do not by default check if a received IP datagram originated from a local MAC address matches the MAC addresses in the static ARP table, or if the external datagram matches the MAC address of one of the known network routers that has a valid route entry in the routing table.
Unauthorized MAC addresses are therefore exposed, and the decision to take defensive action can then take place.

New-IP ARP lookups and time gaps

By using non-promiscuous sniffing of the interface, the system can find any new IP address on the network that tries to communicate with, or through, the system it is on.
The system will need to send an ARP request to the originating IP address in order to validate the MAC/IP pair for further communications. This reveals inappropriate use (spoofing, for example) of MAC addresses on the network.

Special note on MAC-Spoofing prevention on high-security wireless networks

In the wireless LAN world, due to the lack of maturity in the wireless security model, high security environments should simply not allow wireless connectivity. The wireless cryptographic protocol, WEP (Wired Equivalency Privacy), and MAC ACLs are not foolproof, and are soft targets.
Known 802.11b vulnerabilities include ease of spoofing of a MAC address when MAC-level access control is in use (See http://www.bitshift.org/wardriving.shtml.).

Rogue access points are another vulnerability. Many wireless network cards support configurable MAC addresses. Using a sniffer, an intruder can capture wireless network data frames, pull out an authorized MAC address, and use it without conflict when the legitimate card goes offline.
MAC-spoof proofing a wireless network is possible, but involves throwing a security blanket over the whole wireless system, hardening access points, checking for IP addresses against tables, and using port locking, among other events.
At this time, wireless networks are just too vulnerable, with too many points of vulnerability.

What are the advantages of MAC spoofing in penetration testing?

An essential component of penetration testing is the ability to specify arbitrary MAC addresses. MAC spoofing can be used to test redirection of network traffic, and for testing access points. By allowing the impersonation of different MAC addresses within a network, MAC spoofing provides the facility for penetration tests to test firewalls, and to acquire information from a remote host.
MAC spoofing allows untraceable scans, because both source IP and MAC addresses are spoofed.

Spoofing MAC addresses is also required for the implementation of proxy ARP.

Let us take a look at the product GPS (Ghost Port Scan), download available at http://gps.sourceforge.net/en/download.html, is ideal for penetration testing. GPS is an advanced port scanner and a firewall rules disclosure software, which uses IP and MAC spoofing, among other features, to perform stealth and untraceable collections of a network and firewall information. GPS is valuable in LAN penetration testing due to its ability to disclose the firewall settings of a host.

Conclusion

MAC spoofing is the more sophisticated cousin of IP spoofing. By assuming the identity of another machine authorized to be on a network, it is a powerful tool for unauthorized entry into networks, the attack not drawing attention because it appears the invader is really a trusted user of the network.
On the other hand, duplicating a MAC address can have positive effects. For example, impersonating a valid MAC address is also useful for authorized duplication of a NIC card. A good example where this can be seen is when it is used to facilitate creating true hot fail over systems that require the use of the same MAC address of the primary system.

What conclusions can we draw about MAC spoofing? It can be another weapon against securing systems, or, ironically, it can be a tool for securing the same systems.

- People use MAC spoofing to reroute network traffic, for good and bad reasons.
- It can be accomplished through hardware or software modifications.

- MAC spoofing attacks can be identified and defended against.
- It is necessary for redirecting network traffic in penetration testing.
- High-security networks should not use wireless devices due to the relative ease in using MAC spoofing to invade access points. (For further information, see Conclusion, page 15, of Joshua Wright's Detecting Wireless LAN MAC Address Spoofing, http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf.)

References

Ethernet Frames, URL:
http://netcert.tripod.com/ccna/internetworking/eframes.html (1 Sep. 2003)

ARP (Address Resolution Protocol), URL:
http://www.koot.biz/docs/tech/Obtaining%20passwords.htm (22 Aug. 2003)

Hyperdictionary, URL:
http://www.hyperdictionary.com/dictionary/Media+Access+Control (1 Sep. 2003)

Charles Spurgeon, URL:
http://www.ethermanage.com/ethernet/descript-troubleshoot.html (1 Sep. 2003)

SMAC FAQs, URL:
http://www.klcconsulting.net/smac/ (1 Sep. 2003)

Mike Schiffman, Libnet 1.0.x Primer, URL:
http://www.packetfactory.net/papers/Libnet-primer/ (6 Sep. 2003)

Michael D. Schiffman, Libnet 101, Part 1: The Primer, June 19, 2000, URL:
http://www.packetfactory.net/papers/Libnet-primer/libnet-primer.pdf (1 Sep. 2003)

Free Libnet download, URL:
http://gps.sourceforge.net/libs/libnet-1.0.2a.tar.gz (1 Sep. 2003)

SMAC-MAC spoofing Windows product (free download for personal use), URL:
http://home.attbi.com/~rbourret/download/smac_1.1.zip

MAC Changer, URL:
http://www.alobbs.com/modules.php?op=modload&name=macc&file=index (6 Sep. 2003)

Free MAC Changer download for Linux systems, URL:
http://savannah.nongnu.org/download/macc/macchanger.pkg/1.3.0/macchanger-1.3.0.tar.gz

Sygate Firewall Help Site, URL:
http://bellsouthpwp.net/i/k/ikpe/SygateBasics.html#GUI (10 Jun. 2003)

Sygate Firewall screen shot -- Security options, URL:
http://bellsouthpwp.net/i/k/ikpe/images/options%20Security.png (10 Jun. 2003)

MAC locking, URL:
http://www.xs4all.nl/~rmeijer/wayback.html (23 Jul. 2003)

Wright, Joshua, Detecting Wireless LAN MAC Address Spoofing, page 15, URL:
http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf (26 Jul. 2003)

Private VLANs on Catalyst 6000, October 22, 2002, page 11 URL:
http://www.informit.com/isapi/product_id~%7BDBBECCF4-42A3-46D3-A337-685E29F3CAFC%7D/content/images/1587050250/samplechapter/1587050250CH05.pdf (6 Sep. 2003)

Gps Ghost Port Scan penet tool, URL:
http://www.ozetechnology.com/goodies/Security.shtml (22 Jul. 2003)

Ghost Port Scan, URL:
http://gps.sourceforge.net/en/download.html (21 Aug. 2003)

Mark C. Langston, WarDriving v2.0, Known 802.11b vulnerabilities, URL:
http://www.bitshift.org/wardriving.shtml (22 Aug. 2003)