**MAC Address Spoofing**

**Description 1**

MAC spoofing attacks are attacks launched by clients on a Layer 2 network. Attackers spoof their MAC address **to perform a man-in-the-middle (MiTM) attack.** In one common attack, the attacker pretends to be the default gateway and sends out a gratuitous Address Resolution Protocol (ARP) to the network **so that users send their traffic through the attacker** rather than the default gateway. The attacker then forwards user traffic to the real default gateway. An attacker on a fast enough host can capture and forward packets so that victims do not notice any change in their network access. [1]

**Description 2**

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. Unlike IP spoofing, **MAC spoofing involves actually invading a network, and taking over a machine within that network. [2]** (therefore MAC spoofing can lead to all of consequences of IP spoofing )

**Description 3**

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has the MAC address of a user’s choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer’s identity, for any reason, and it is relatively easy.

MAC spoofing attacks involve **the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker. By sending a single frame with the source Ethernet address of the other host, the network attacker overwrites the MAC Table entry so that the switch forwards packets destined for the host to the network attacker**. Until the host sends traffic, it will not receive any traffic. When the host sends out traffic, the MAC Table entry is rewritten once more so that it moves back to the original port.

**Reference**

**[1]** [**http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=4**](http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=4)

**[2]** [**https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315**](https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315)

**[3]** [**http://itsecurity.telelink.com/mac-address-spoofing/**](http://itsecurity.telelink.com/mac-address-spoofing/)