

**Name:** Bint e Fatima Niazi

**Date:** July 2025

**Contact:**

-Email: fatimabinte4@gmail.com

-LinkedIn: linkedin.com/in/bint-e-fatima-niazi

-GitHub: github.com/fatima-niazi

Project: MAC Address Spoofing using macchanger

# Introduction

This document covers the understanding and performing of MAC address spoofing. The project involves using the `macchanger` utility on a Linux system to change the MAC address of a network interface, understand the purpose behind doing so, and observe how MAC spoofing affects network identity.

This project was conducted in a safe lab environment for educational purposes only.

# Tools & Environment

- Kali Linux   
- Terminal  
- macchanger  
- ip / ifconfig commands

# What is a MAC Address?

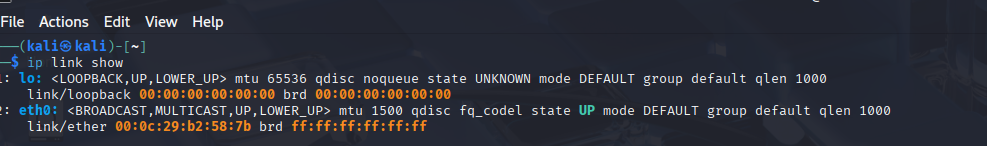
A MAC (Media Access Control) address is a unique identifier assigned to a device’s network interface. It operates at Layer 2 (Data Link Layer) of the OSI model and is used for device identification within a local network. MAC addresses look like: `b8:27:eb:45:12:89` and consist of a manufacturer prefix and a device-specific suffix.

MAC spoofing involves changing this address to a random or manually assigned value. This is commonly used for privacy, bypassing MAC-based restrictions, testing, or masking identity.

# Steps Performed

**1. Checked the available network interfaces:**

* Command: `ip link show`

****

**2. Identified the active interface: `eth0`**

A screen shot of a computer code

AI-generated content may be incorrect.

**3. Brought down the interface before spoofing:**

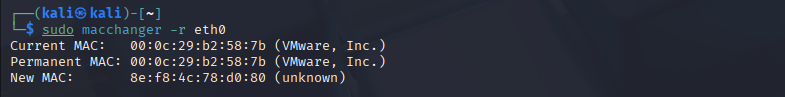
* Command: `sudo ip link set eth0 down`
* Reason: MAC addresses can only be changed when the interface is disabled to avoid system/network errors.

A close up of a word

AI-generated content may be incorrect.

**4. Spoofed MAC Address (random):**

* Command: `sudo macchanger -r eth0`



**5. Optionally set a manual MAC address:**

* Command: `sudo macchanger --mac=00:11:22:33:44:55 eth0`

A computer screen with white text

AI-generated content may be incorrect.

**6. Brought interface back up:**

* Command: `sudo ip link set eth0 up`



**7. Verified the spoofed MAC address:**

* Command: `macchanger -s eth0` or `ifconfig eth0`

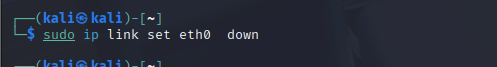
A close up of a computer screen

AI-generated content may be incorrect.

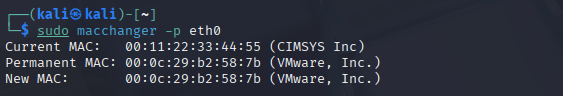
# Reverting to Original MAC

To restore the original hardware MAC address:

1. **Disable interface: `sudo ip link set eth0 down`**



1. **Restore MAC: `sudo macchanger -p eth0`**



1. **Enable interface: `sudo ip link set eth0 up`**



You can also simply reboot to revert temporary spoofing.

# Conclusion

This activity helped understand how network devices identify each other and how MAC spoofing can alter device behavior on a LAN. It also reinforced safe handling of interfaces and demonstrated how identity can be masked or restored using terminal tools.