MAC table flooding attack (of the switch)

Design Report

Sadia Tasnim

Student Id. : 1505076

Section: B Group: 6

July 30, 2019

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology
(BUET)
Dhaka - 1000

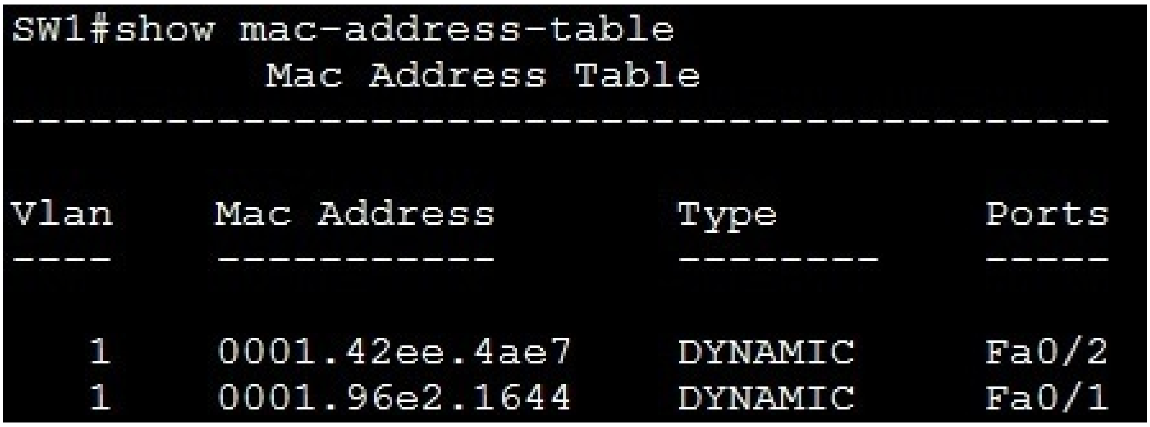
Contents

1 Introduction

MAC Flooding is one of the most common network attacks. Unlike other web attacks, MAC Flooding is not a method of attacking any host machine in the network, but it is the method of attacking the network switches. However, the victim of the attack is a host computer in the network.

2 How switches work

A switch is a device in a computer network that connects other devices together.Switches manage the flow of data across a network by transmitting a received network frame only to the one or more devices for which the frame is intended. Each networked device connected to a switch can be identified by its **MAC(Media Access Control)** address, allowing the switch to make accurate forwarding and filtering decision.
The switch maintains an address table called MAC address table in order to efficiently switch frames between interfaces. When the switch receives a frame, it associates the MAC address of the sending device with the switch port on which it was received. In this way, a switch dynamically builds an address table by using the source MAC address of the frames received.
If we use **show mac address-table** command on Cisco switch CLI, we will see the mac address table of the switch. (Shown is figure 1)



```
SW1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.42ee.4ae7    DYNAMIC     Fa0/2
   1    0001.96e2.1644    DYNAMIC     Fa0/1
```

Figure 1: Mac address table of a CLI switch

3 Mac Table Flooding Attack

The MAC Flooding is an attacking method intended to compromise the security of the network switches.This goal is achieved by the use of MAC tables The aim of the MAC Flooding is to take down this MAC Table. In a typical

MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.
If the attacker keeps sending Ethernet frames MAC Address Table will stay full and the switch will be unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting.
As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine. So that the attacker will be able to steal sensitive data from the communication of the victim and other computers.

4 Strategy to perform the attack

The strategy of this attack is pretty simple.Steps are given below:

1. Attacker needs to be on the same LAN network on which he plans to attack.**His goal can be getting all the packets from all the devices connected to the network or from a specific device.**

2. Attacker can do the job just by sending normal packet to the switch with a little change in the header.Header contains a field called source address.Attacker needs to create a huge number of packets with different source address.

3. Switch will get the packets with different source address coming from same port number.So it will keep populating mac table for different source mac address with the same port number.As the address is removed When the aging time for a MAC address in the table expires, valid mac addresses get removed from the mac table and get filled up with bogus entries.

4. When a valid source tries to send packet to a destination mac table cannot find the port number for the destination mac, so it broadcasts to all.And as the switch cannot learn the mac of the sending device because of the memory shortage, it will broadcast packets meant for it too.

5. Thus the attacker gets the desired packets.

5 Timing Diagrams

Two timing diagrams will be shown to discuss the attack further. They are given below:

5.1 Normal Timing Diagram:

It shows how switch normally works.

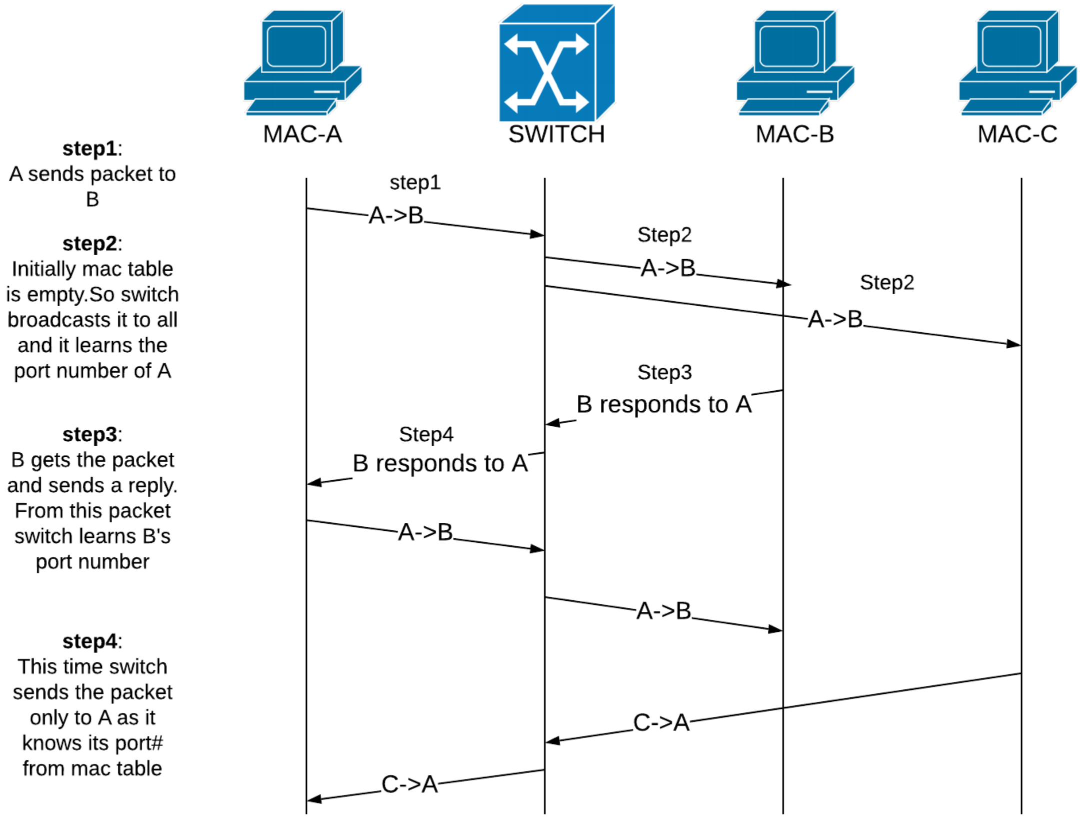
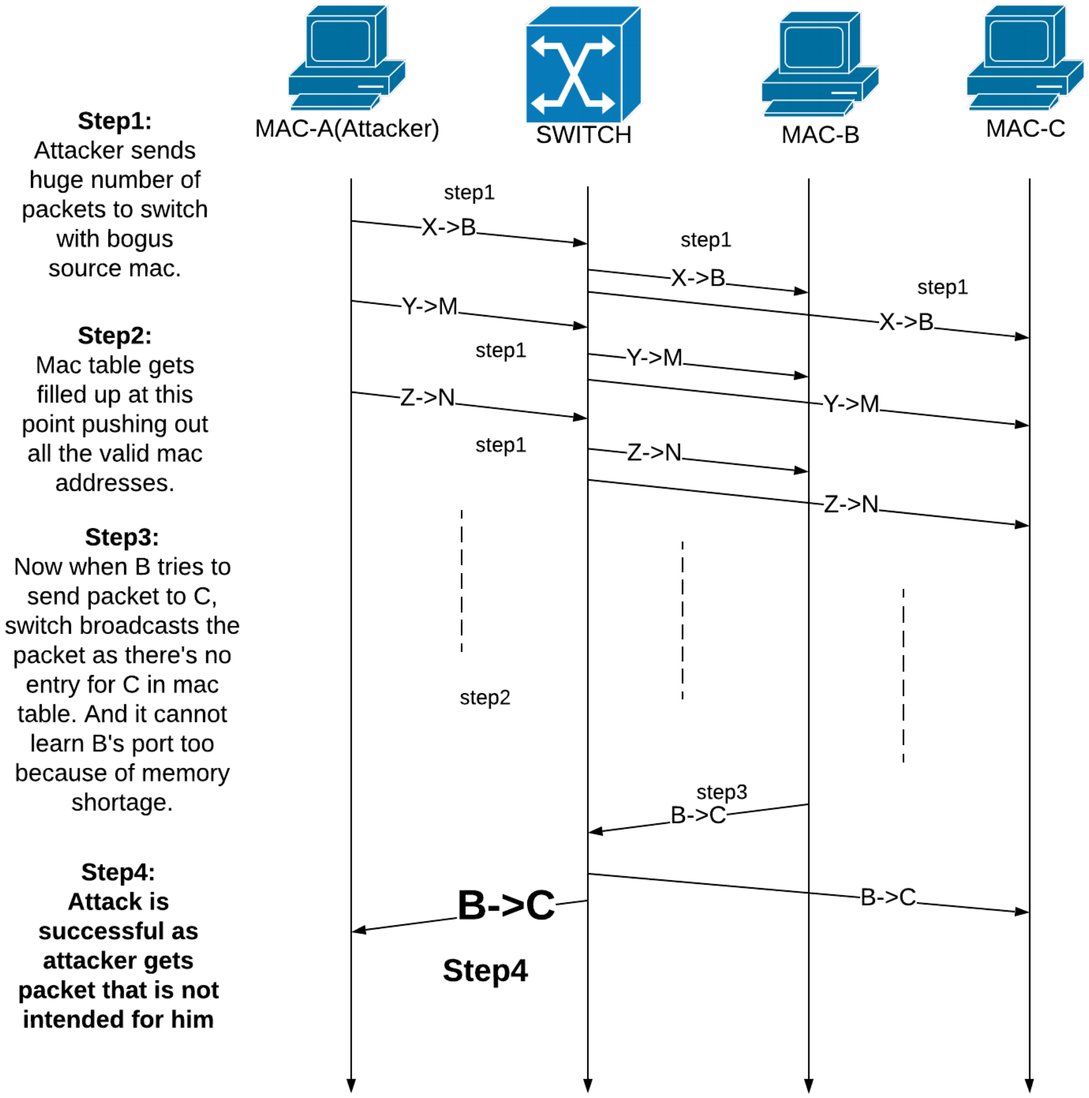

MAC-A
SWITCH
MAC-B
MAC-C
step1: A sends packet to B
step2: Initially mac table is empty.So switch broadcasts it to all and it learns the port number of A
step3: B gets the packet and sends a reply. From this packet switch learns B's port number
step4: This time switch sends the packet only to A as it knows its port# from mac table
step1
A->B
Step2
A->B
Step2
A->B
Step3
B responds to A
Step4
B responds to A
A->B
A->B
C->A
C->A

Figure 2: Typical Timing diagram of a Switch

5.2 Attacking timing diagram:

This timing diagram shows how an attacker perform the mac table flooding attack.



Step1: Attacker sends huge number of packets to switch with bogus source mac.

Step2: Mac table gets filled up at this point pushing out all the valid mac addresses.

Step3: Now when B tries to send packet to C, switch broadcasts the packet as there's no entry for C in mac table. And it cannot learn B's port too because of memory shortage.

Step4: Attack is successful as attacker gets packet that is not intended for him

Figure 3: Attacking Timing diagram of a Switch

6 Ethernet MAC data frame format

The basic frame consists of seven elements split between three main areas:

1. **Header**
   (a) Preamble / SFD
   (b) Destination Address (DA)
   (c) Source Address (SA)
   (d) Length / Type
2. **Payload**

   (a) Data

3. **Trailer**

   (a) FCS(frame check sequence) or CRC(cyclic redundancy check)

Ethernet data frame is shown in 4

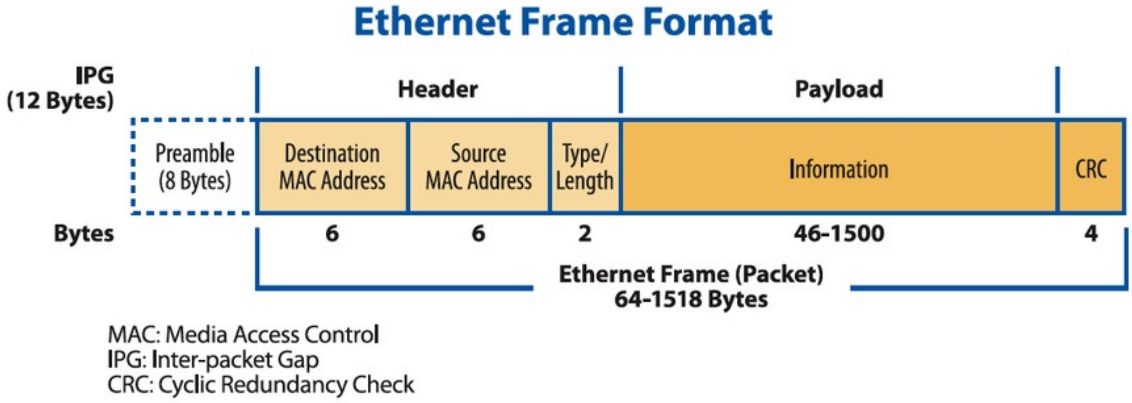


Figure 4: Ethernet Frame Format

So, we will generate huge number of frame with randomly generated source mac addresses following this data frame format. Then we will send the frames to perform the mac table flooding attack.

7 Target Network Topology

We have to use one Switch and at least 3 end devices to demonstrate the mac table flooding attack.
The target network topology is given below:

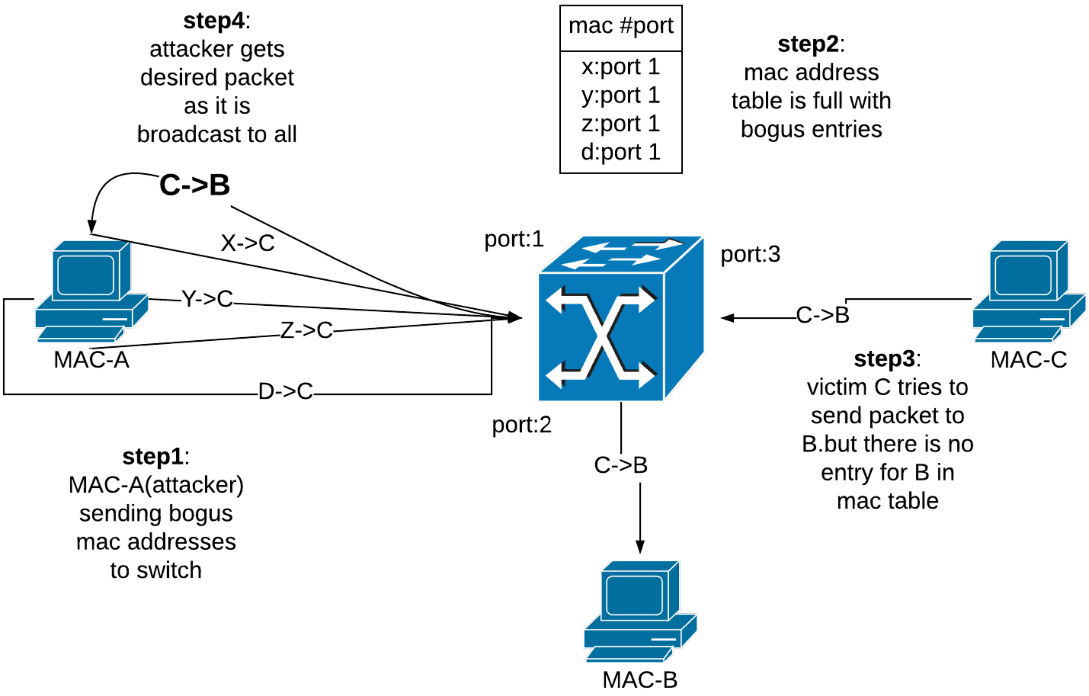


Figure 5: Target Network Topology

8 Justification

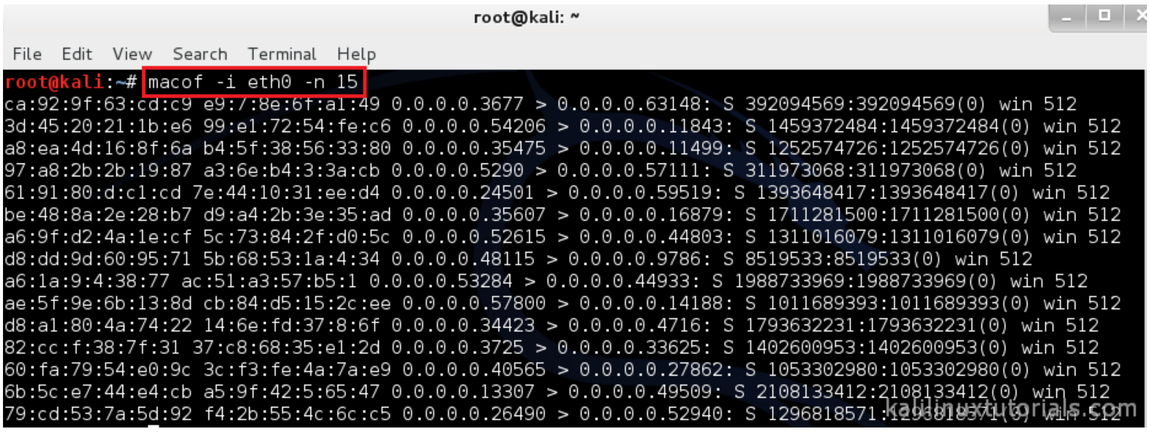
Mac table flooding is just sending numerous packets to the switch to consume its memory so that when any valid device sends any packet to another valid device, it gets broadcast to all.We know when any switch sees a packet from a certain port with certain source mac address it creates an entry for that source mac with its port where the switch thinks it is connected in the mac address table.
So if we send numerous packets with different source mac address from the same port, the mac table will dynamically get populated with the entries corresponding the source addresses and the attack will be successful.

9 Available Tools

The most available tool for this attack is **MACOF**. Macof is a member of the Dsniff suit toolset and mainly used to flood the switch on a local network with MAC addresses
In kali linux we can use this tool by using some commands.

1. **Simple Flooding:**

    ```
    command: macof -i eth1 -n 10
    ```

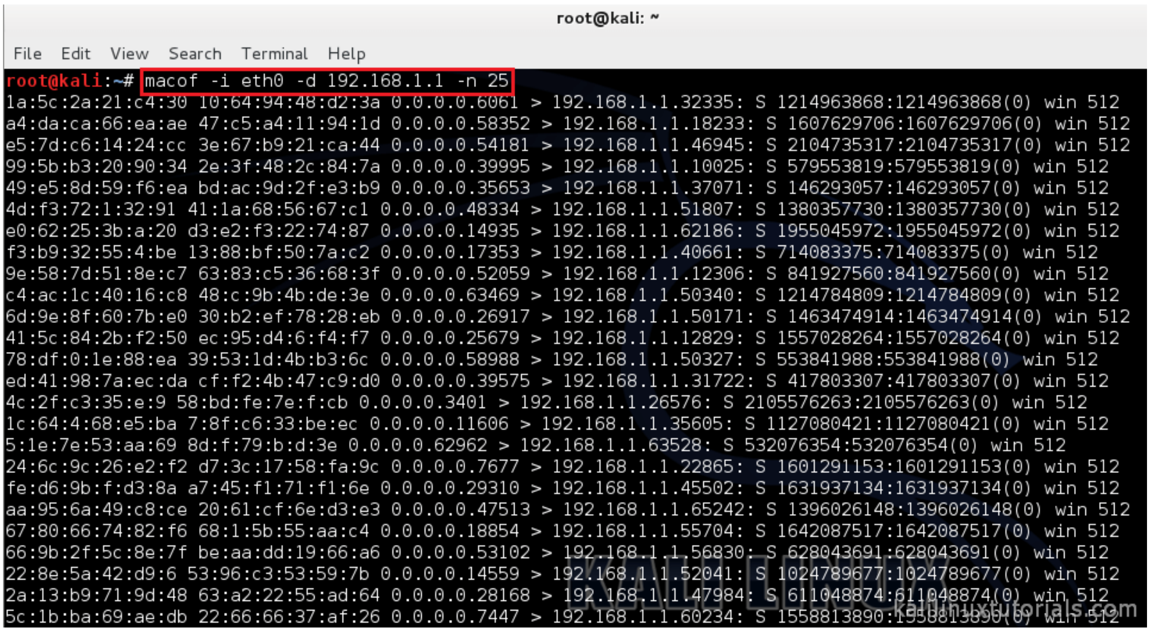


```
root@kali:~# macof -i eth0 -n 15
ca:92:9f:63:cd:c9 e9:7:8e:6f:a1:49 0.0.0.0.3677 > 0.0.0.0.63148: S 392094569:392094569(0) win 512
3d:45:20:21:1b:e6 99:e1:72:54:fe:c6 0.0.0.0.54206 > 0.0.0.0.11843: S 1459372484:1459372484(0) win 512
a8:ea:4d:16:8f:6a b4:5f:38:56:33:80 0.0.0.0.35475 > 0.0.0.0.11499: S 1252574726:1252574726(0) win 512
97:a8:2b:2b:19:87 a3:6e:b4:3:3a:cb 0.0.0.0.5290 > 0.0.0.0.57111: S 311973068:311973068(0) win 512
61:91:80:d:c1:cd 7e:44:10:31:ee:d4 0.0.0.0.24501 > 0.0.0.0.59519: S 1393648417:1393648417(0) win 512
be:48:8a:2e:28:b7 d9:a4:2b:3e:35:ad 0.0.0.0.35607 > 0.0.0.0.16879: S 1711281500:1711281500(0) win 512
a6:9f:d2:4a:1e:cf 5c:73:84:2f:d0:5c 0.0.0.0.52615 > 0.0.0.0.44803: S 1311016079:1311016079(0) win 512
d8:dd:9d:60:95:71 5b:68:53:1a:4:34 0.0.0.0.48115 > 0.0.0.0.9786: S 8519533:8519533(0) win 512
a6:1a:9:4:38:77 ac:51:a3:57:b5:1 0.0.0.0.53284 > 0.0.0.0.44933: S 1988733969:1988733969(0) win 512
ae:5f:9e:6b:13:8d cb:84:d5:15:2c:ee 0.0.0.0.57800 > 0.0.0.0.14188: S 1011689393:1011689393(0) win 512
d8:a1:80:4a:74:22 14:6e:fd:37:8:6f 0.0.0.0.34423 > 0.0.0.0.4716: S 1793632231:1793632231(0) win 512
82:cc:f:38:7f:31 37:c8:68:35:e1:2d 0.0.0.0.3725 > 0.0.0.0.33625: S 1402600953:1402600953(0) win 512
60:fa:79:54:e0:9c 3c:f3:fe:4a:7a:e9 0.0.0.0.40565 > 0.0.0.0.27862: S 1053302980:1053302980(0) win 512
6b:5c:e7:44:e4:cb a5:9f:42:5:65:47 0.0.0.0.13307 > 0.0.0.0.49509: S 2108133412:2108133412(0) win 512
79:cd:53:7a:5d:92 f4:2b:55:4c:6c:c5 0.0.0.0.26490 > 0.0.0.0.52940: S 1296818571:1296818571(0) win 512
```

Figure 6: Macof to cause simple flooding

2. **Trageted Flooding:** Macof can flood a switch with random MAC addresses destinated to 192.168.1.1.

    ```
    command: macof -i eth1 -d 192.168.1.1
    ```

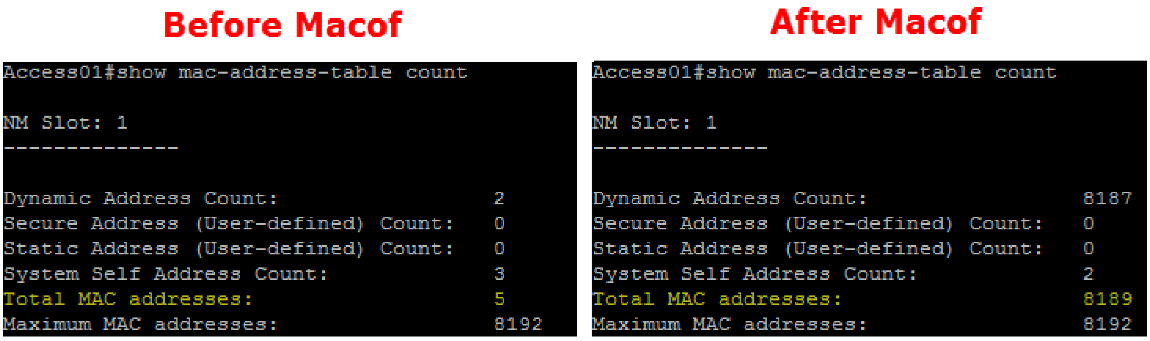


```
root@kali:~# macof -i eth0 -d 192.168.1.1 -n 25
1a:5c:2a:21:c4:30 10:64:94:48:d2:3a 0.0.0.0.6061 > 192.168.1.1.32335: S 1214963868:1214963868(0) win 512
a4:da:ca:66:ea:ae 47:c5:a4:11:94:1d 0.0.0.0.58352 > 192.168.1.1.18233: S 1607629706:1607629706(0) win 512
e5:7d:c6:14:24:cc 3e:67:b9:21:ca:44 0.0.0.0.54181 > 192.168.1.1.46945: S 2104735317:2104735317(0) win 512
99:5b:b3:20:90:34 2e:3f:48:2c:84:7a 0.0.0.0.39995 > 192.168.1.1.10025: S 579553819:579553819(0) win 512
49:e5:8d:59:f6:ea bd:ac:9d:2f:e3:b9 0.0.0.0.35653 > 192.168.1.1.37071: S 146293057:146293057(0) win 512
4d:f3:72:1:32:91 41:1a:68:56:67:c1 0.0.0.0.48334 > 192.168.1.1.51807: S 1380357730:1380357730(0) win 512
e0:62:25:3b:a:20 d3:e2:f3:22:74:87 0.0.0.0.14935 > 192.168.1.1.62186: S 1955045972:1955045972(0) win 512
f3:b9:32:55:4:be 13:88:bf:50:7a:c2 0.0.0.0.17353 > 192.168.1.1.40661: S 714083375:714083375(0) win 512
9e:58:7d:51:8e:c7 63:83:c5:36:68:3f 0.0.0.0.52059 > 192.168.1.1.12306: S 841927560:841927560(0) win 512
c4:ac:1c:40:16:c8 48:c:9b:4b:de:3e 0.0.0.0.63469 > 192.168.1.1.50340: S 1214784809:1214784809(0) win 512
6d:9e:8f:60:7b:e0 30:b2:ef:78:28:eb 0.0.0.0.26917 > 192.168.1.1.50171: S 1463474914:1463474914(0) win 512
41:5c:84:2b:f2:50 ec:95:d4:6:f4:f7 0.0.0.0.25679 > 192.168.1.1.12829: S 1557028264:1557028264(0) win 512
78:df:0:1e:88:ea 39:53:1d:4b:b3:6c 0.0.0.0.58988 > 192.168.1.1.50327: S 553841988:553841988(0) win 512
ed:41:98:7a:ec:da cf:f2:4b:47:c9:d0 0.0.0.0.39575 > 192.168.1.1.31722: S 417803307:417803307(0) win 512
4c:2f:c3:35:e:9 58:bd:fe:7e:f:cb 0.0.0.0.3401 > 192.168.1.1.26576: S 2105576263:2105576263(0) win 512
1c:64:4:68:e5:ba 7:8f:c6:33:be:ec 0.0.0.0.11606 > 192.168.1.1.35605: S 1127080421:1127080421(0) win 512
5:1e:7e:53:aa:69 8d:f:79:b:d:3e 0.0.0.0.62962 > 192.168.1.1.63528: S 532076354:532076354(0) win 512
24:6c:9c:26:e2:f2 d7:3c:17:58:fa:9c 0.0.0.0.7677 > 192.168.1.1.22865: S 1601291153:1601291153(0) win 512
fe:d6:9b:f:d3:8a a7:45:f1:71:f1:6e 0.0.0.0.29310 > 192.168.1.1.45502: S 1631937134:1631937134(0) win 512
aa:95:6a:49:c8:ce 20:61:cf:6e:d3:e3 0.0.0.0.47513 > 192.168.1.1.65242: S 1396026148:1396026148(0) win 512
67:80:66:74:82:f6 68:1:5b:55:aa:c4 0.0.0.0.18854 > 192.168.1.1.55704: S 1642087517:1642087517(0) win 512
66:9b:2f:5c:8e:7f be:aa:dd:19:66:a6 0.0.0.0.53102 > 192.168.1.1.56830: S 628043691:628043691(0) win 512
22:8e:5a:42:d9:6 53:96:c3:53:59:7b 0.0.0.0.14559 > 192.168.1.1.52041: S 1024789677:1024789677(0) win 512
2a:13:b9:71:9d:48 63:a2:22:55:ad:64 0.0.0.0.28168 > 192.168.1.1.47984: S 611048874:611048874(0) win 512
5c:1b:ba:69:ae:db 22:66:66:37:af:26 0.0.0.0.7447 > 192.168.1.1.60234: S 1558813890:1558813890(0) win 512
```

Figure 7: Macof to cause targeted flooding

If we use the following command before and after running macof we get figure 8

```
show mac-address-table count
```



Before Macof

```
Access01#show mac-address-table count

NM Slot: 1
--------------

Dynamic Address Count:                 2
Secure Address (User-defined) Count:   0
Static Address (User-defined) Count:   0
System Self Address Count:             3
Total MAC addresses:                   5
Maximum MAC addresses:                 8192
```

After Macof

```
Access01#show mac-address-table count

NM Slot: 1
--------------

Dynamic Address Count:                 8187
Secure Address (User-defined) Count:   0
Static Address (User-defined) Count:   0
System Self Address Count:             2
Total MAC addresses:                   8189
Maximum MAC addresses:                 8192
```

Figure 8: Before and after MACOf

10 Defense Mechanism

We can prevent the MAC Flooding attack with various methods. The following are some of these methods.

1. Port Security
2. Authentication with AAA server
3. Security measures to prevent ARP Spoofing or IP Spoofing
4. Implement IEEE 802.1X suites

Port Security
The port security is often used as a counter measure for MAC Flooding attack. The switches are configured to limit the number of MAC addresses that can be learned on ports connected to the end stations. Also a small table of 'secure' MAC addresses is maintained with the traditional MAC address table. This table also acts as a subset of the MAC address table. Cisco switches are available with in-built port security system.

Authentication with AAA server
In this method, the discovered MAC addresses are authenticated against an authentication, authorization and accounting server (AAA Server) and these addresses are subsequently filtered

Security measures to prevent ARP Spoofing or IP Spoofing
Security measures to prevent ARP Spoofing or IP Spoofing in some cases may also perform additional MAC address filtering on unicast packets.

Implement IEEE 802.1X suites
Implementing IEEE 802.1X suites will allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.

These are the methods often used to prevent the MAC Flooding attack.

11 Conclusion

We have seen what is mac table flooding and how it works.W e have also seen how one can perform this attack or defend from it.Mac table flooding is a very common attack and its important to take sufficient measure to defend from it.