



Redes Seguras Prácticas Bloque II

Aarón Cela Riveiro
Sergio Vila Riveira
Samuel Fernández Vázquez
Lennart Thiele

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

En este laboratorio se desplegará un sistema de autenticación y autorización tolerante a fallos y se configurarán los dispositivos de red para utilizar dicho sistema de autenticación y autorización.

1.1 FreeRadius

El servidor de control de acceso elegido fue FreeRadius, instalado y configurado directamente en la máquina mirtual con dirección IP 10.1.239.100. Este actuará como el "single entry point" de nuestra red, que para tener conectividad con los dispositivos de clase se configuró la interfaz ens192 con una IP de la red de administración.

```
1 network:
2   ethernets:
3     ens192:
4       addresses:
5         - 10.1.239.100/24
6   version: 2
```

Listing 1: Archivo de configuración de red

1.1.1 Configuración de FreeRadius

El fichero /etc/freeradius/3.0/clients.conf define los clientes, en nuestro caso, los dispositivos que se autenticarán contra el servidor.

```
1 # IPv4 Clients
2 # /etc/freeradius/3.0/clients.conf
3
4 client vlan239{
5   ipaddr = 10.1.239.100
6   secret = Bayern_2025
7   require_message_authenticator = true
8 }
9
10
11 client AL-SW1 {
12   ipaddr = 10.1.239.1
13   secret = Bayern_2025
14   require_message_authenticator = no
15   limit_proxy_state = no
16 }
17
18 client DL-SW1 {
19   ipaddr = 10.1.239.2
20   secret = Bayern_2025
21   require_message_authenticator = no
22   limit_proxy_state = no
23 }
24
25 client FW {
26   ipaddr = 10.1.239.3
27   secret = Bayern_2025
28   require_message_authenticator = no
29   limit_proxy_state = no
30 }
31
32
33
34
```

```

35 client CPE {
36     ipaddr = 10.1.239.4
37     secret = Bayern_2025
38     require_message_authenticator = no
39     limit_proxy_state = no
40 }
41
42
43 client ISP {
44     ipaddr = 10.1.239.5
45     secret = Bayern_2025
46     require_message_authenticator = no
47     limit_proxy_state = no
48 }
```

Listing 2: Archivo de configuración de Radius

Además definimos los usuarios que se podrán autenticar en el servidor

```

1 # /etc/freeradius/3.0/users
2
3 munics Cleartext-Password := "Bayern_2025"
4     Service-Type = NAS-Prompt-User
5
6 superMunics Cleartext-Password := "Bayern_2025"
7     Service-Type = NAS-Prompt-User ,
8     Cisco-AVPair = "shell:priv-lvl=15"
```

Listing 3: Usuarios definidos en Radius

1.2 Configuración de dispositivos

A continuación se configurarán los dispositivos para implementar el sistema de autenticación AAA.

1.2.1 Base de datos de usuarios locales

Se crean los siguientes usuarios en local, para autenticarse en caso de que el servidor Radius falle.

```

1 username juniorAdmin secret Bayern_2025
2 username admin privilege 15 secret Bayern_2025
```

Listing 4: Usuarios de la base de datos local

1.2.2 Autenticación AAA

Se configura el servidor Radius previamente creado

```

1 radius server RAD1
2 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
3 key Bayern_2025
```

Listing 5: Configuración de servidor Radius en dispositivo

A continuación creamos el método de autenticación AAA-LOGIN que funciona contra el servidor radius, y en caso de que este no esté funcional, funcionará con la base de datos local que acabamos de crear.

```

1 aaa new-model
2 aaa authentication login default group radius local
3 aaa authentication login AAA-LOGIN group radius local
4 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
```

Listing 6: Definimos el modelo AAA

1.2.3 SSH

Creamos una clave de SSH y activamos el protocolo en todos los dispositivos

```
1 crypto key generate rsa general-keys modulus 1024
2 ip ssh version 2
```

Listing 7: Generar clave SSH

A mayores se configuró una ACL para solo permitir el SSH desde nuestra máquina virtual

```
1 ip access-list standard SSH-FROM-VM
2 remark ACL SSH from VM
3 permit 10.1.239.100
4 deny any log
5 logging esm config
6 !
```

Listing 8: Limitar acceso SSH

Por último hacemos que estos cambios sean efectivos activando el login por SSH con la ACL y con autorización

```
1 line vty 0 4
2 access-class SSH-FROM-VM in
3 password munics
4 authorization exec AAA-AUTHZ
5 login authentication AAA-LOGIN
6 transport input ssh
7
8 !
```

Listing 9: Limitar acceso SSH

1.3 Demostraciones Lab 6

Para acceder por SSH, cada máquina necesitas un conjunto de claves diferentes:

```
1 # Para AL, DL x=(1,2)
2 ssh -oHostKeyAlgorithms=+ssh-rsa      -oKexAlgorithms=+diffie-hellman-group1-
     sha1      -oCiphers=+aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
     superMunics@10.1.239.x
3
4 # Para CPE, FW, ISP y=(3,4,5)
5 ssh -oHostKeyAlgorithms=+ssh-rsa -oKexAlgorithms=+diffie-hellman-group14-sha1
     superMunics@10.1.239.y
```

Listing 10: Limitar acceso SSH

Acceso desde la VM, con ambos usuarios:

```
munics@municsPOD:~$ ssh -oHostKeyAlgorithms=+ssh-rsa      -oKexAlgorithms=+diffie-hellman-group1-sha1
     -oCiphers=+aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc      munics@10.1.239.1
(munics@10.1.239.1) Password:

AL-SW1>exit
Connection to 10.1.239.1 closed.
munics@municsPOD:~$ ssh -oHostKeyAlgorithms=+ssh-rsa      -oKexAlgorithms=+diffie-hellman-group1-sha1
     -oCiphers=+aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc      superMunics@10.1.239.1
(superMunics@10.1.239.1) Password:

AL-SW1#
```

Tiramos el servidor Radius y accedemos a través de la base de datos local:

```
munics@municsPOD:~$ sudo systemctl stop freeradius
munics@municsPOD:~$ ssh -oHostKeyAlgorithms=+ssh-rsa -oKexAlgorithms=+diffie-hel
lman-group14-sha1 superMunics@10.1.239.3
(superMunics@10.1.239.3) Password:
(superMunics@10.1.239.3) Password:

munics@municsPOD:~$ ssh -oHostKeyAlgorithms=+ssh-rsa -oKexAlgorithms=+diffie-hel
lman-group14-sha1 admin@10.1.239.3
(admin@10.1.239.3) Password:
FW#
```

Figure 1: Login contra la base de datos local

2 Laboratorio 7 - Fortificación de la capa de acceso Ethernet

2.1 Servidor DHCP

Primero que nada lo que se hará es configurar un servidor DHCP para la asignación de IPs a los usuarios de forma dinámica para que se puedan conectar al switch de acceso. Para ello también lo configuraremos en el switch multicapa (DL-SW1).

La configuración del servidor DHCP en la máquina virtual es la siguiente:

```
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [ "ens192" ]
    },
    "lease-database": {
      "type": "memfile",
      "lfc-interval": 3600
    },
    "subnet4": [
      {
        "subnet": "10.1.16.0/24",
        "pools": [ { "pool": "10.1.16.50 - 10.1.16.150" } ],
        "option-data": [
          { "name": "routers", "data": "10.1.16.1" },
          { "name": "subnet-mask", "data": "255.255.255.0" },
          { "name": "domain-name-servers", "data": "8.8.8.8" }
        ]
      },
      {
        "subnet": "10.1.17.0/24",
        "pools": [ { "pool": "10.1.17.50 - 10.1.17.150" } ],
        "option-data": [
          { "name": "routers", "data": "10.1.17.1" },
          { "name": "subnet-mask", "data": "255.255.255.0" },
          { "name": "domain-name-servers", "data": "8.8.8.8" }
        ]
      },
      {
        "subnet": "10.1.18.0/24",
        "pools": [ { "pool": "10.1.18.50 - 10.1.18.150" } ],
        "option-data": [
          { "name": "routers", "data": "10.1.18.1" },
          { "name": "subnet-mask", "data": "255.255.255.0" },
          { "name": "domain-name-servers", "data": "8.8.8.8" }
        ]
      }
    ],
    "valid-lifetime": 600,
    "renew-timer": 300,
    "rebind-timer": 400
  }
```

Figure 2: Configuración DHCP

Lo configuraremos para las VLANs 16,17 y 18. Mostramos la configuración para las VLANs:

```
interface Vlan16
  ip address 10.1.16.1 255.255.255.0
  ip helper-address 10.1.239.100
  ip ospf 1 area 0
!
interface Vlan17
  ip address 10.1.17.1 255.255.255.0
  ip helper-address 10.1.239.100
  ip ospf 1 area 0
!
interface Vlan18
  ip address 10.1.18.1 255.255.255.0
  ip helper-address 10.1.239.100
  ip ospf 1 area 0
!
```

Figure 3: Ip Helper Address

2.2 Ataques

En esta parte de la memoria mostraremos los ataques que se han utilizado.

2.2.1 Saturación de la tabla de envío de AL-SW1

El ataque de MAC Flooding consiste en sobrecargar la tabla CAM (Content Addressable Memory) del switch AL-SW1 enviando una gran cantidad de direcciones MAC de origen falsas. Estas tablas tienen un tamaño limitado, por lo que si el atacante introduce miles de MACs inventadas, el switch ya no puede aprender las direcciones MAC reales asociadas a cada puerto.

Cuando la tabla CAM se llena y el switch no conoce la MAC de destino de un paquete, comienza a reenviar el tráfico por todos los puertos (excepto por el de entrada).

Para probar el ataque, se utilizará **macof**. El ataque se lanzará a la interfaz conectada al switch de acceso AL_SW1:

```
1 sudo macof
```

Desde el switch se puede ver como la tabla CAM se ha llenado, en este caso las entradas de la VLAN 16, para verlo el comando que se usa es el siguiente:

```
1 show mac address-table count
```

```
AL-SW1#show mac address-table count

Mac Entries for Vlan 739:
-----
Dynamic Address Count : 1
Static Address Count : 0
Total Mac Addresses   : 1

Mac Entries for Vlan 16:
-----
Dynamic Address Count : 7989
Static Address Count : 0
Total Mac Addresses   : 7989

Mac Entries for Vlan 17:
-----
Dynamic Address Count : 1
Static Address Count : 0
Total Mac Addresses   : 1

Mac Entries for Vlan 18:
-----
Dynamic Address Count : 1
Static Address Count : 0
Total Mac Addresses   : 1

Total Mac Address Space Available: 48
```

Figure 4: Address-table AL-SW1

Desde la herramienta **Wireshark**, se puede ver los paquetes que se están enviando:

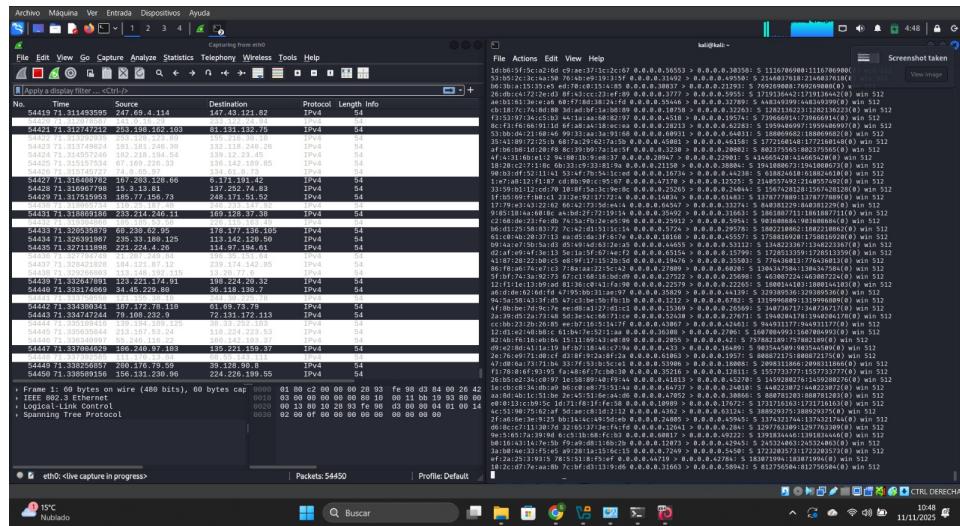


Figure 5: Ejecución macof y paquetes mostrados en Wireshark

2.2.2 STP, BPDUs de configuración, DoS

Este ataque consiste en enviar una gran cantidad de tramas BPDU de configuración falsificadas hacia el switch. El protocolo STP (Spanning Tree Protocol) utiliza estas BPDUs para evitar bucles de red y es procesado directamente por la CPU del switch, no por hardware.

Si un atacante envía muchas BPDUs por segundo, el switch debe procesarlas una a una. Provocando saturación de la CPU del switch, degradación del rendimiento general del dispositivo, etc.

Para realizar este ataque se utilizará la herramienta **Yersinia** con esta configuración:

```
1 yersinia stp -attack 2 -interface eth0
```

Para comprobar que el ataque está siendo efectivo se puede comprobar desde el switch con el siguiente comando:

```
1 show proc cpu | incl CPU
```

```
CPU utilization for five seconds: 7%/0%; one minute: 5%; five minutes: 5%
AL-SW1#show processes cpu | incl CPU
CPU utilization for five seconds: 7%/0%; one minute: 5%; five minutes: 5%
AL-SW1#show processes cpu | incl CPU
CPU utilization for five seconds: 89%/14%; one minute: 12%; five minutes: 7%
AL-SW1#show processes cpu | incl CPU
CPU utilization for five seconds: 89%/14%; one minute: 12%; five minutes: 7%
```

Figure 6: CPU en uso después del ataque.

Y con Wireshark también se puede ver los paquetes enviados:

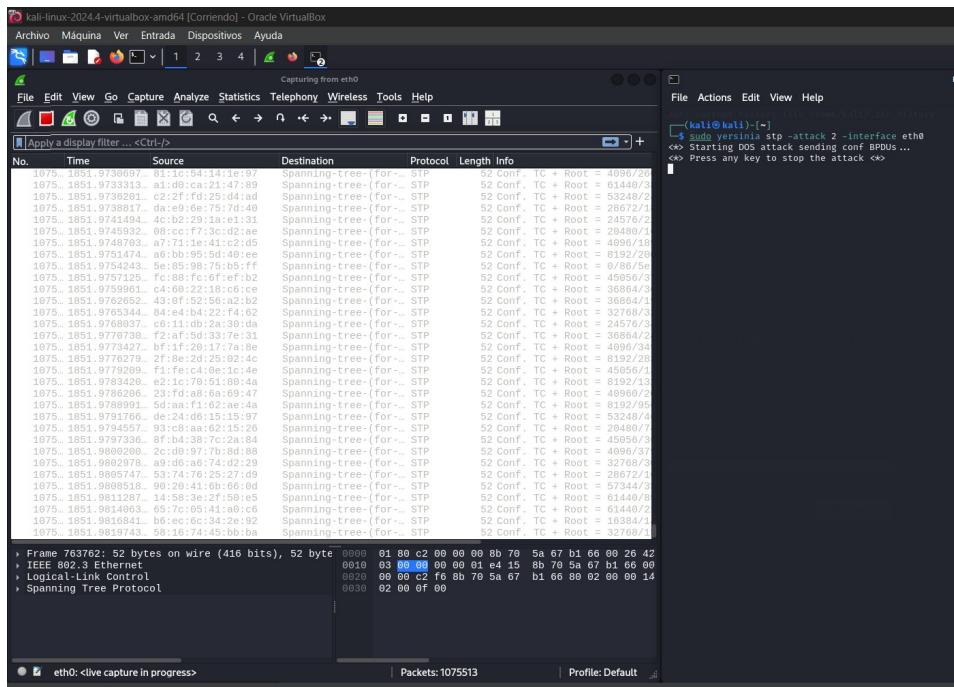


Figure 7: Wireshark Bpdus.

2.2.3 CDP Flooding

Cisco Discovery Protocol (CDP) es un protocolo de capa 2 utilizado por los dispositivos Cisco para anunciar información como modelo, versión o interfaces, y es procesado directamente por la CPU del switch, no por hardware.

El ataque de CDP Flooding consiste en enviar al switch una gran cantidad de paquetes CDP falsos buscando una denegación de servicio.

Cuando un atacante genera cientos o miles de paquetes CDP por segundo, el switch debe procesarlos individualmente, provocando aumento del uso del CPU de una forma similar al ataque anterior.

Para este ataque también utilizamos Yersinia, con el siguiente comando:

```
1 yersinia cdp -attack 1 -interface eth0
```

De la misma manera que antes se comprueba el uso de la CPU desde el switch:

```
AL-SW1#show processes cpu | incl CPU
CPU utilization for five seconds: 8%/0%; one minute: 35%; five minutes: 21%
AL-SW1#show processes cpu | incl CPU
CPU utilization for five seconds: 7%/0%; one minute: 33%; five minutes: 21%
AL-SW1#show processes cpu | incl CPU
CPU utilization for five seconds: 98%/10%; one minute: 34%; five minutes: 22%
AL-SW1#show processes cpu | incl CPU
CPU utilization for five seconds: 98%/10%; one minute: 34%; five minutes: 22%
AL-SW1#
```

Figure 8: CPU en uso después del ataque CPD flooding.

Los paquetes enviados capturados en Wireshark son los siguientes:

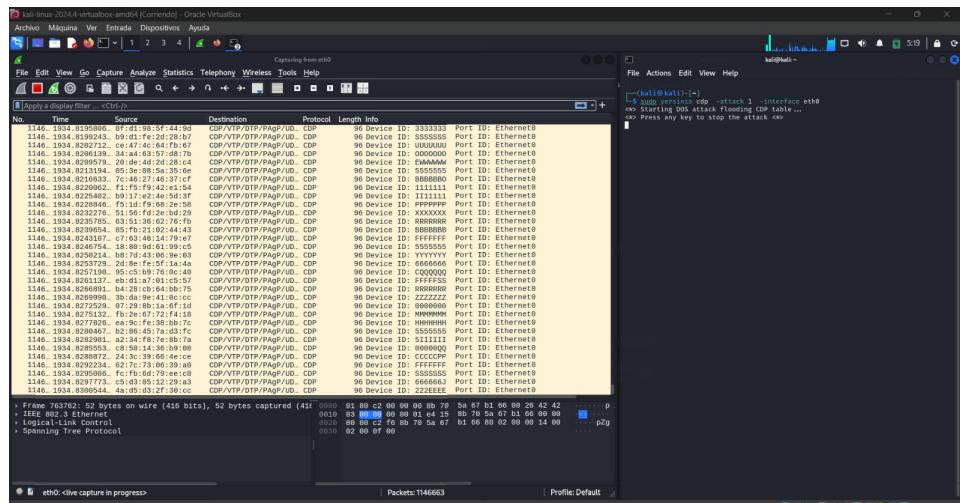


Figure 9: CDP flooding visto desde Wireshark.

2.2.4 DTP trunking

El ataque de DTP Trunking aprovecha el comportamiento por defecto del protocolo Dynamic Trunking Protocol (DTP), que permite que dos interfaces negocien automáticamente si el enlace será access o trunk. Si un puerto del switch está en modo dynamic auto o dynamic desirable, un atacante puede enviar tramas DTP falsificadas para forzar al switch a convertir su puerto en un trunk.

LA vulnerabilidad que da acceso a este ataque se aprovecha de las configuraciones de las interfaces que están en dynamic auto. En nuestro caso se prueba con la interfaz g0/4:

```
1 int g0/4
2 switchport mode dynamic auto
```

Una vez hecho esto, ya se podrá probar el ataque. Para demostrar que funciona, primero se muestra el estado de todas las interfaces antes del ataque:

AL-SW1#show interfaces status							
Port	Name	Status	Vlan	Duplex	Speed	Type	
Gi0/1		notconnect	739	auto	auto	10/100/1000BaseTX	
Gi0/2		notconnect	16	auto	auto	10/100/1000BaseTX	
Gi0/3		connected	16	a-full	a-1000	10/100/1000BaseTX	
Gi0/4		connected	16	a-full	a-1000	10/100/1000BaseTX	
Gi0/5		notconnect	17	auto	auto	10/100/1000BaseTX	
Gi0/6		notconnect	17	auto	auto	10/100/1000BaseTX	
Gi0/7		notconnect	17	auto	auto	10/100/1000BaseTX	
Gi0/8		notconnect	18	auto	auto	10/100/1000BaseTX	
Gi0/9		notconnect	18	auto	auto	10/100/1000BaseTX	
Gi0/10		notconnect	18	auto	auto	10/100/1000BaseTX	
Gi0/11		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/12		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/13		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/14		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/15		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/16		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/17		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/18		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/19		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/20		connected	trunk	a-full	a-100	10/100/1000BaseTX	
Gi0/21		notconnect	1	auto	auto	Not Present	
Gi0/22		notconnect	1	auto	auto	Not Present	
Gi0/23		notconnect	1	auto	auto	Not Present	
Gi0/24		notconnect	1	auto	auto	Not Present	

Figure 10: Interfaces Status Pre Attack

Para el ataque se utiliza Yersinia, con el siguiente comando:

```
1 yersinia dtp -attack 1 -interface eth0
```

Y comprobamos que el ataque ha tenido éxito:

AL-SW1#show interfaces status							
Port	Name	Status	Vlan	Duplex	Speed	Type	
Gi0/1		notconnect	739	auto	auto	10/100/1000BaseTX	
Gi0/2		notconnect	16	auto	auto	10/100/1000BaseTX	
Gi0/3		connected	16	a-full	a-1000	10/100/1000BaseTX	
Gi0/4		connected	trunk	a-full	a-1000	10/100/1000BaseTX	
Gi0/5		notconnect	17	auto	auto	10/100/1000BaseTX	
Gi0/6		notconnect	17	auto	auto	10/100/1000BaseTX	
Gi0/7		notconnect	17	auto	auto	10/100/1000BaseTX	
Gi0/8		notconnect	18	auto	auto	10/100/1000BaseTX	
Gi0/9		notconnect	18	auto	auto	10/100/1000BaseTX	
Gi0/10		notconnect	18	auto	auto	10/100/1000BaseTX	
Gi0/11		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/12		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/13		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/14		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/15		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/16		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/17		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/18		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/19		notconnect	1	auto	auto	10/100/1000BaseTX	
Gi0/20		connected	trunk	a-full	a-100	10/100/1000BaseTX	
Gi0/21		notconnect	1	auto	auto	Not Present	
Gi0/22		notconnect	1	auto	auto	Not Present	
Gi0/23		notconnect	1	auto	auto	Not Present	
Gi0/24		notconnect	1	auto	auto	Not Present	

Figure 11: Interfaces Status Post Attack

Los paquetes capturados con Wireshark son los siguientes:

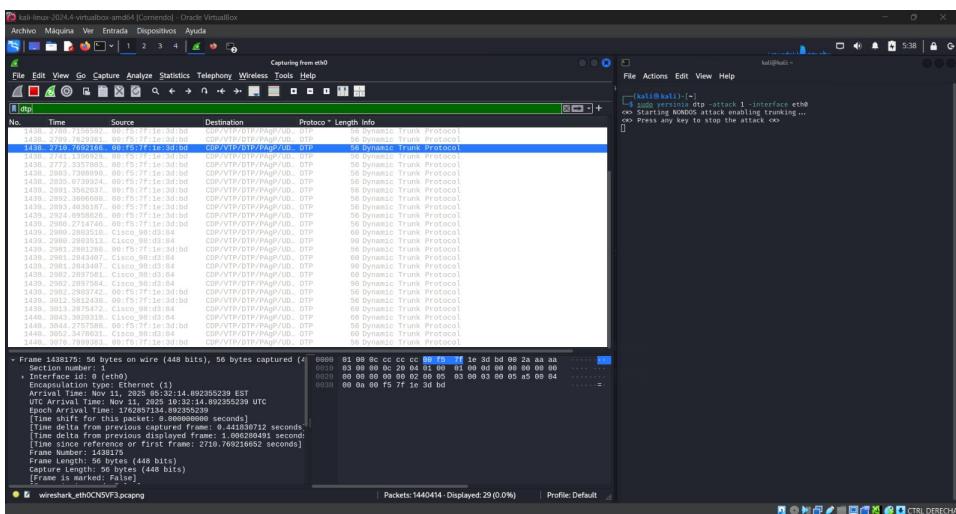


Figure 12: DTP trunking visto con Wireshark

2.2.5 ARP spoofing attack

El ataque de ARP Spoofing consiste en enviar respuestas ARP falsificadas dentro de la red local para asociar la dirección IP de otro equipo con la MAC del atacante. Como ARP no tiene autenticación y los dispositivos confían en cualquier respuesta ARP recibida, el atacante puede hacer que otros hosts actualicen su tabla ARP con información incorrecta. De esta forma el atacante se posiciona como **Man-in-the-Middle (MitM)**, de esta forma todo el tráfico que el usuario envía al switch, o a cualquier otro host, pasa primero por el atacante.

Para realizar el ataque, en este caso, se usará Ettercap.

En Ettercap se añadirá al usuario como nuestro Target 1 y al switch como nuestro Target 2 y aparte veremos que los paquetes desde la víctima pasan por el atacante, usaremos Wireshark para capturar esos paquetes:

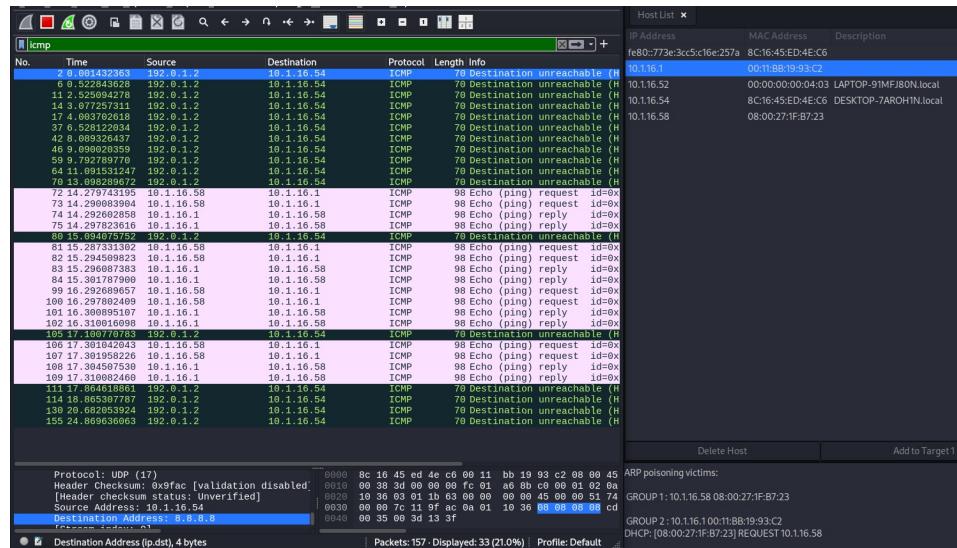


Figure 13: Ettercap y MitM

Para ver que el ataque ha sido exitoso, comprobaremos en nuestra víctima que dentro de su tabla de direcciones MAC hay dos MACs idénticas.

```
(r0n3z@Kali)-[~]
$ ip neigh show
10.1.16.41 dev eth0 lladdr 8c:16:45:ed:4e:c6 STALE
10.1.16.42 dev eth0 lladdr 08:00:27:7a:c5:e4 STALE
10.1.16.25 dev eth0 lladdr 00:00:00:00:04:03 STALE
10.1.16.1 dev eth0 lladdr 08:00:27:7a:c5:e4 REACHABLE
fe80::21b9:999f:3e45:10d4 dev eth0 lladdr 00:00:00:00:04:03 STALE
```

Figure 14: Direcciones MAC idénticas

Si se desactiva Ettercap, automáticamente el tráfico dejará de pasar por el atacante.

2.2.6 DHCP Spoofing y DHCP Rogue Server

Lo primero que tenemos que hacer para realizar el ataque sería agotar las direcciones IP que el servidor DHCP oferta, generando e inundando de peticiones DHCP con direcciones MAC falsas.

Este ataque es el siguiente:

```
1 yersinia dhcp -attack 1 -interface eth0
```

Esto acabará con el pool de direcciones del servidor DHCP:

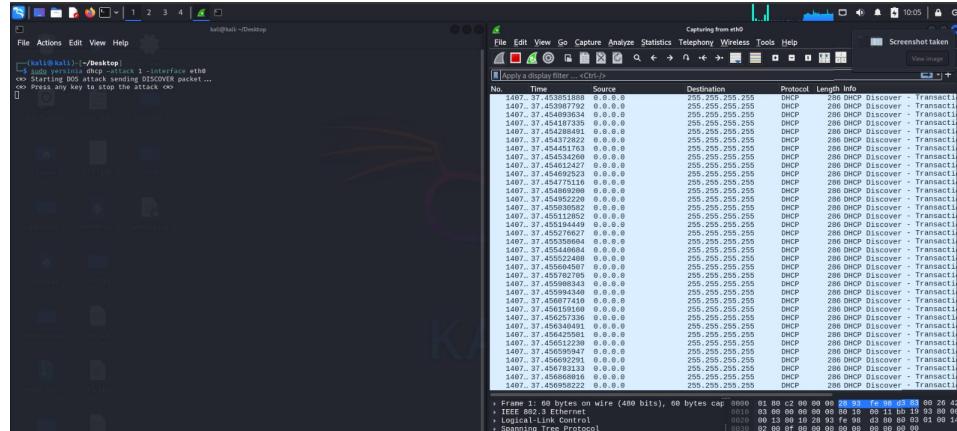


Figure 15: DHCP spoofing

Los usuarios al intentarse conectar no podrán obtener una IP del servidor DHCP legítimo, dejando al cliente sin conexión.

Como el servidor DHCP está inutilizado, desplegaremos un servidor Rogue DHCP para realizar nuestro segundo ataque y que, de esta forma los usuarios se conecten a nosotros en vez de al servidor DHCP original. Ya que nos haremos pasar por el servidor DHCP legítimo enviándoles una IP disponible de la pool y a mayores nuestra MAC como puerta de enlace, haciendo que pase por nosotros todo el tráfico.

Despliegue del servidor con yersinia:

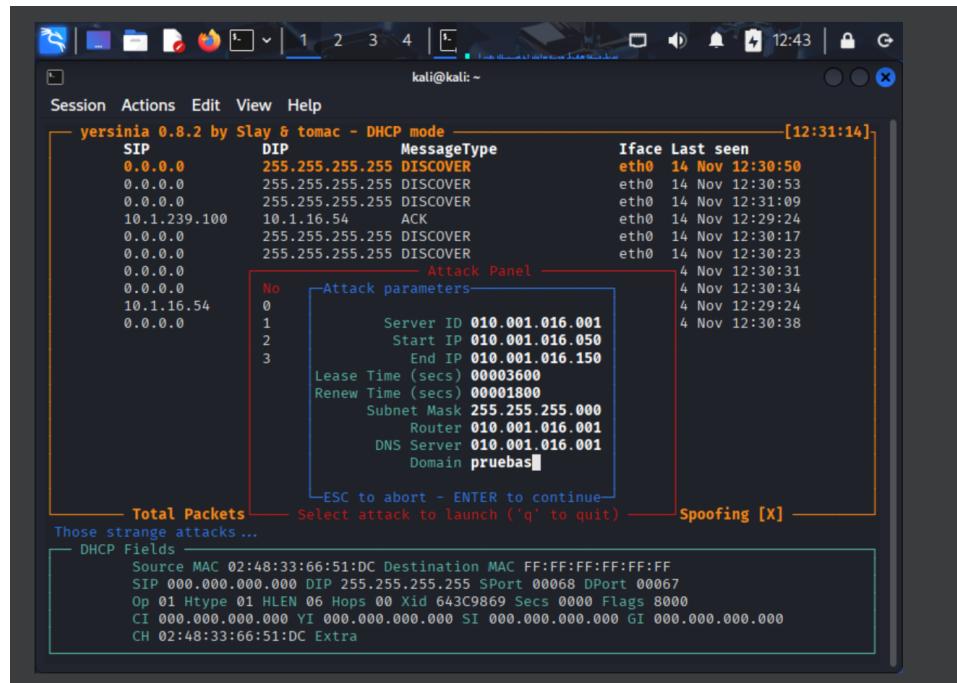


Figure 16: Configurar Rogue de prueba desde Yersinia

2.3 Fortificación de los dispositivos de red en capa 2

A continuación mostraremos como mitigar las vulnerabilidades que han sido explotadas en los ataques realizados.

2.3.1 Limitar número de MACs

Limitaremos el máximo número de MACs a 10 por interfaz para evitar que la tabla CAM se sature.

Para ello la configuraremos las interfaces g0/2-10 con port security de esta manera:

```
1 interface range g0/2-10
2 switchport mode access
3 switchport port-security
4 switchport port-security maximum 10
5 switchport port-security violation protect
```

Secure Port Action	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security
Gi0/2 utdown	10	0	0	Sh
Gi0/3 utdown	10	2	0	Sh
Gi0/4 utdown	10	0	1	Sh
Gi0/5 utdown	10	0	0	Sh
Gi0/6 utdown	10	0	0	Sh
Gi0/7 utdown	10	0	0	Sh
Gi0/8 utdown	10	0	0	Sh
Gi0/9 utdown	10	0	0	Sh
Gi0/10 utdown	10	0	0	Sh

Total Addresses in System (excluding one mac per port) : 1				
Max Addresses limit in System (excluding one mac per port) : 8192				

Figure 17: Verificación port-security

Si volvemos a lanzar el ataque como antes, veremos que no ha tenido éxito:

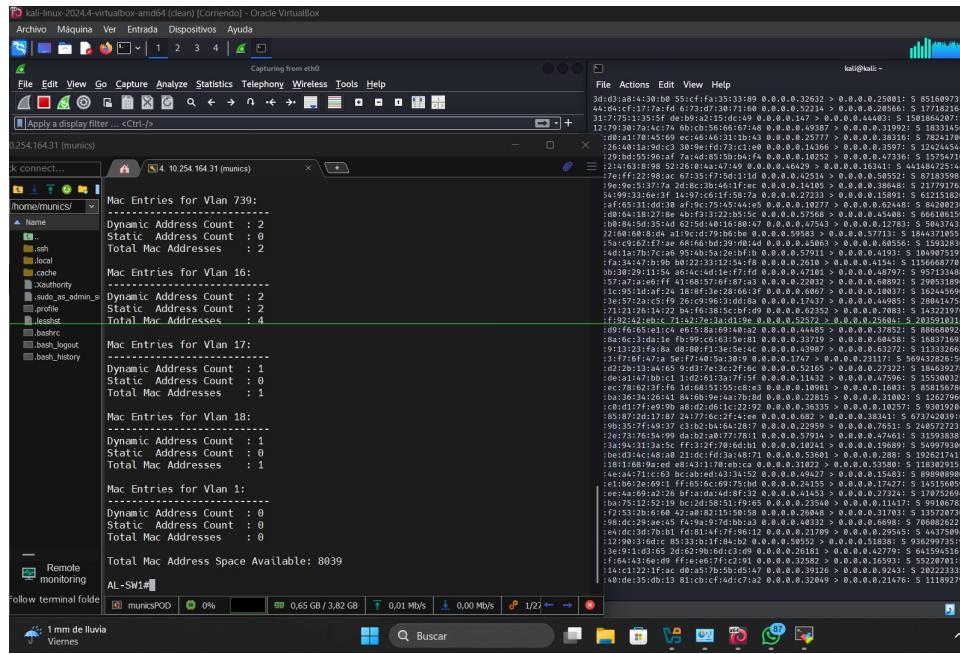


Figure 18: Ataque con Macof Mitigado

2.3.2 Mitigar STP, Bpdus

En AL-SW1 activamos portfast y bpduguard en los puertos de acceso para proteger el switch frente a BPDUs maliciosas. En DL-SW1 lo configuramos como root bridge de las VLAN 16, 17, 18 y 739 para estabilizar y controlar la topología STP.

```

1 AL-SW1#conf t
2 Enter configuration commands, one per line. End with CNTL/Z.
3 AL-SW1(config)#spanning-tree portfast bpduguard default
4 AL-SW1(config)#int range g0/2-10
5 AL-SW1(config-if-range)#spanning-tree portfast
6 AL-SW1(config-if-range)#exit
7 AL-SW1(config)#
8
9 DL-SW1#
10 DL-SW1#conf t
11 Enter configuration commands, one per line. End with CNTL/Z.
12 DL-SW1(config)#spanning-tree vlan 16,17,18,739 root primary
13 DL-SW1(config)#end
14 DL-SW1#

```

Si lanzamos el ataque con la nueva configuración, comprobamos que se ha mitigado el problema:

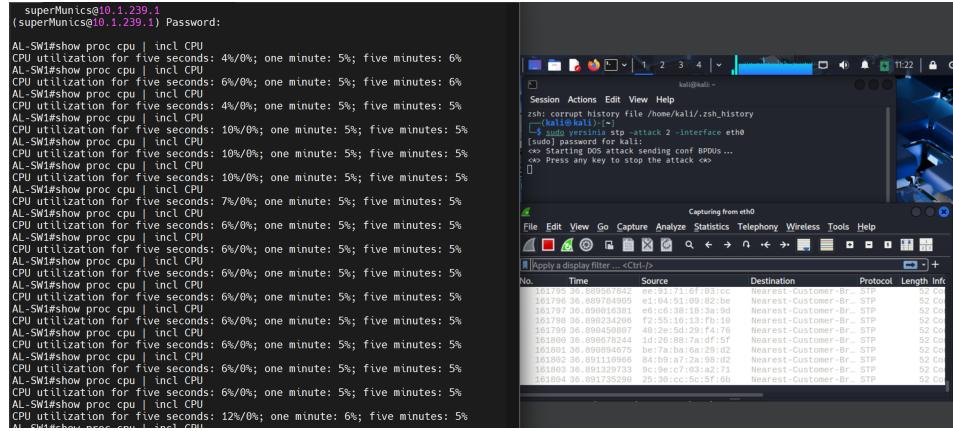


Figure 19: Ataque con stp Mitigado

2.3.3 Mitigar CDP Flooding

Para solucionarlo desactivaremos en las interfaces cdp con el siguiente comando:

```
1 interface range Gi0/2 - 10
2   no cdp enable
```

Una vez configurado, veremos que el ataque ya no tiene efecto:

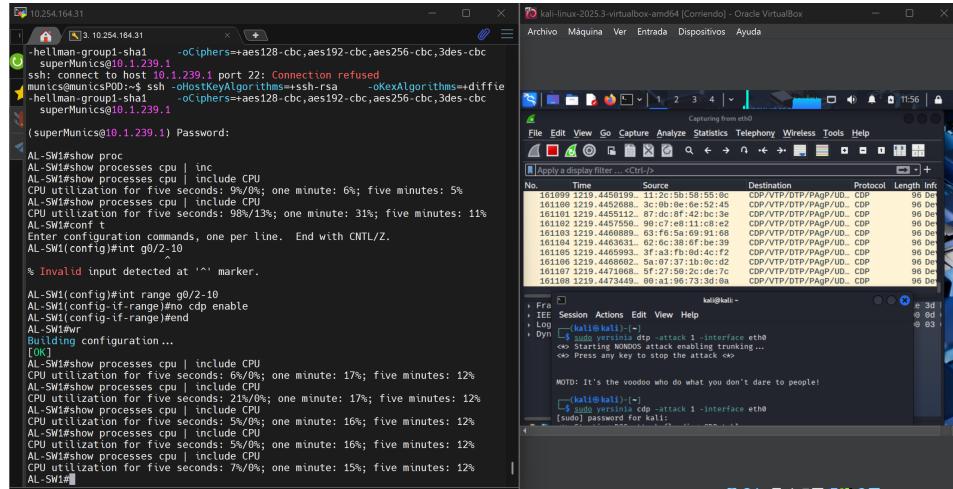


Figure 20: CDP mitigado

2.3.4 Mitigar DTP trunking

Para mitigar este ataque, los puertos de acceso tienen que estar en mode access (que no esté en modo dynamic auto) y para los puertos troncales deberemos de añadirles lo siguiente en la configuración:

```
1 AL-SW1(config-if)#int g0/20
2 AL-SW1(config-if)#switchport nonegotiate
```

Demostración del ataque sin éxito:

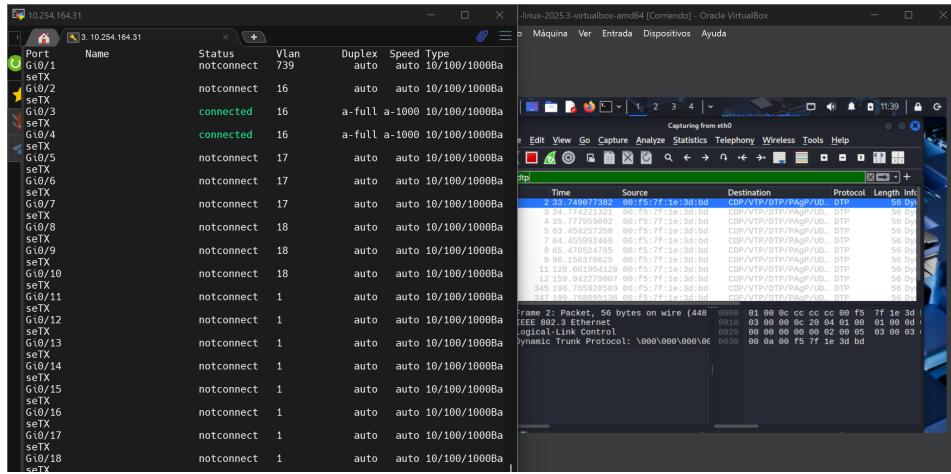


Figure 21: DTP trunking mitigado

2.3.5 Mitigar salto VLAN

Para evitar el salto de VLAN, se configuran todos los puertos no utilizados como puertos de acceso, asignándolos a una VLAN inactiva (en este caso la VLAN 88) y dejándolos en estado shutdown. De este modo se impide que negocien un enlace troncal.

```
1 vlan 88
2 interface range g0/11-19
3   switchport mode access
4   switchport access vlan 88
5   shutdown
6
7 interface range g0/21-24
8   switchport mode access
9   switchport access vlan 88
10  shutdown
```

2.3.6 Mitigar ARP Spoofing

Para ello activaremos la funcionalidad Dynamic ARP para mitigar los ataques de ARP spoofing. De esta forma el switch se asegura que solamente se enviarán respuestas ARP válidas.

```
1 ip arp inspection vlan 16,17,18
2 int g0/20
3 ip arp inspection trust
```

2.3.7 Mitigar los ataques DHCP

Para evitar este tipo de ataques, se utilizará DHCP snooping, con la siguiente configuración:

```
1 ip dhcp snooping
2 no ip dhcp snooping information option
3 ip dhcp snooping vlan 16,17,18
4
5 int g0/20
6 ip dhcp snooping trust
7 exit
8
9 int range g0/2-10
10 ip dhcp snooping limit rate 10
11
12 end
```

Con el snooping activado, si el ataque se intenta de nuevo, no funcionará.

3 Configuración de los dispositivos

3.1 AL-SW1

```
1  AL-SW1#show running-config
2  Building configuration...
3
4  Current configuration : 6865 bytes
5  !
6  ! Last configuration change at 00:30:21 UTC Mon Mar 1 1993 by superMunics
7  !
8  version 12.2
9  no service pad
10 service timestamps debug datetime msec
11 service timestamps log datetime msec
12 no service password-encryption
13 !
14 hostname AL-SW1
15 !
16 boot-start-marker
17 boot-end-marker
18 !
19 enable secret 5 $1$4ggR$iNwcR8H.ugsTaXxgbLjRE0
20 enable password munics
21 !
22 username juniorAdmin secret 5 $1$d7AC$tqsCDMtxIT2qtcTB6Q1e60
23 username admin privilege 15 secret 5 $1$4JQN$abPigzcy1C8p.ZxNfzcKI.
24 aaa new-model
25 !
26 !
27 aaa authentication login default group radius local
28 aaa authentication login AAA-LGIN group radius local
29 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
30 !
31 !
32 !
33 !
34 !
35 aaa session-id common
36 system mtu routing 1500
37 ip arp inspection vlan 16-18
38 !
39 !
40 ip dhcp snooping vlan 16-18
41 no ip dhcp snooping information option
42 ip dhcp snooping
43 ip domain-name munics.pri
44 !
45 !
46 crypto pki trustpoint TP-self-signed-4271428480
47 enrollment selfsigned
48 subject-name cn=IOS-Self-Signed-Certificate-4271428480
49 revocation-check none
50 rsakeypair TP-self-signed-4271428480
51 !
52 !
53 crypto pki certificate chain TP-self-signed-4271428480
54 certificate self-signed 01
55     30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
56     31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
57     69666963 6174652D 34323731 34323834 3830301E 170D3933 30333031 30303031
58     30395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
```

```

59  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 32373134
60  32383438 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
61  810085E1 0E0FF69D 55BAA4B8 3242956C 88BA4A20 007F0BAE 7C775218 787A4D1E
62  6A592433 AC88CA8D F2E44FA1 8B8061E1 0640595E AB331A30 7231D400 87C14740
63  12109636 B239C3DE AB88408E 9479B0AF OFE5CCBD 29B2AA25 3092B8C2 4953E0E1
64  D0A43208 26766077 ADB9F855 EC64E3EA BE46ACC2 C1683A25 5A016AF6 A6C90A66
65  EA FD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
66  551D1104 15301382 11414C2D 5357312E 6D756E69 63732E70 7269301F 0603551D
67  23041830 16801424 61E8C2FF 22D3F0BC 988C64AA 5150C191 90078430 1D060355
68  1D0E0416 04142461 E8C2FF22 D3F0BC98 8C64AA51 50C19190 0784300D 06092A86
69  4886F70D 01010405 00038181 003C7B6B BD62DE1F 846CB7BC 2DD4AC14 18346E36
70  94077A12 17788E9F 779BDC53 EC20C9E8 76522AF6 3BCB2F13 29B0536B CBDDB47A
71  92923AE7 A68A5C1D 240F8583 88A15EE8 336A4BFC 7F51A462 BBDC05DB 4966E706
72  3128FD1E 3A7293C8 8E2EF904 05DE8ED6 914029F8 57EC6202 A6C8F86E D18F5A8B
73  FF5A5A6A 686C2158 574E7941 F1
    quit
74 !
75 !
76 !
77 !
78 spanning-tree mode pvst
79 spanning-tree portfast bpduguard default
80 spanning-tree extend system-id
81 !
82 vlan internal allocation policy ascending
83 !
84 ip ssh time-out 60
85 ip ssh version 2
86 !
87 !
88 !
89 !
90 !
91 interface GigabitEthernet0/1
92   switchport access vlan 739
93   switchport mode access
94   spanning-tree portfast
95 !
96 interface GigabitEthernet0/2
97   switchport access vlan 16
98   switchport mode access
99   switchport port-security maximum 10
100  switchport port-security violation protect
101  no cdp enable
102  spanning-tree portfast
103  ip dhcp snooping limit rate 10
104 !
105 interface GigabitEthernet0/3
106  switchport access vlan 16
107  switchport mode access
108  switchport port-security maximum 10
109  switchport port-security violation protect
110  no cdp enable
111  spanning-tree portfast
112  ip dhcp snooping limit rate 10
113 !
114 interface GigabitEthernet0/4
115  switchport access vlan 16
116  switchport mode access
117  switchport port-security maximum 10
118  switchport port-security violation protect
119  no cdp enable
120  spanning-tree portfast

```

```

121 ip dhcp snooping limit rate 10
122 !
123 interface GigabitEthernet0/5
124   switchport access vlan 17
125   switchport mode access
126   switchport port-security maximum 10
127   switchport port-security violation protect
128   no cdp enable
129   spanning-tree portfast
130   ip dhcp snooping limit rate 10
131 !
132 interface GigabitEthernet0/6
133   switchport access vlan 17
134   switchport mode access
135   switchport port-security maximum 10
136   switchport port-security violation protect
137   no cdp enable
138   spanning-tree portfast
139   ip dhcp snooping limit rate 10
140 !
141 interface GigabitEthernet0/7
142   switchport access vlan 17
143   switchport mode access
144   switchport port-security maximum 10
145   switchport port-security violation protect
146   no cdp enable
147   spanning-tree portfast
148   ip dhcp snooping limit rate 10
149 !
150 interface GigabitEthernet0/8
151   switchport access vlan 18
152   switchport mode access
153   switchport port-security maximum 10
154   switchport port-security violation protect
155   no cdp enable
156   spanning-tree portfast
157   ip dhcp snooping limit rate 10
158 !
159 interface GigabitEthernet0/9
160   switchport access vlan 18
161   switchport mode access
162   switchport port-security maximum 10
163   switchport port-security violation protect
164   no cdp enable
165   spanning-tree portfast
166   ip dhcp snooping limit rate 10
167 !
168 interface GigabitEthernet0/10
169   switchport access vlan 18
170   switchport mode access
171   switchport port-security maximum 10
172   switchport port-security violation protect
173   no cdp enable
174   spanning-tree portfast
175   ip dhcp snooping limit rate 10
176 !
177 interface GigabitEthernet0/11
178   switchport access vlan 88
179   switchport mode access
180   shutdown
181 !
182 interface GigabitEthernet0/12

```

```

183  switchport access vlan 88
184  switchport mode access
185  shutdown
186 !
187 interface GigabitEthernet0/13
188  switchport access vlan 88
189  switchport mode access
190  shutdown
191 !
192 interface GigabitEthernet0/14
193  switchport access vlan 88
194  switchport mode access
195  shutdown
196 !
197 interface GigabitEthernet0/15
198  switchport access vlan 88
199  switchport mode access
200  shutdown
201 !
202 interface GigabitEthernet0/16
203  switchport access vlan 88
204  switchport mode access
205  shutdown
206 !
207 interface GigabitEthernet0/17
208  switchport access vlan 88
209  switchport mode access
210  shutdown
211 !
212 interface GigabitEthernet0/18
213  switchport access vlan 88
214  switchport mode access
215  shutdown
216 !
217 interface GigabitEthernet0/19
218  switchport access vlan 88
219  switchport mode access
220  shutdown
221 !
222 interface GigabitEthernet0/20
223  switchport trunk allowed vlan 16-18,739
224  switchport mode trunk
225  switchport nonegotiate
226  ip arp inspection trust
227  ip dhcp snooping trust
228 !
229 interface GigabitEthernet0/21
230  switchport access vlan 88
231  switchport mode access
232  shutdown
233 !
234 interface GigabitEthernet0/22
235  switchport access vlan 88
236  switchport mode access
237  shutdown
238 !
239 interface GigabitEthernet0/23
240  switchport access vlan 88
241  switchport mode access
242  shutdown
243 !
244 interface GigabitEthernet0/24

```

```

245 switchport access vlan 88
246 switchport mode access
247 shutdown
248 !
249 interface Vlan1
250 no ip address
251 shutdown
252 !
253 interface Vlan739
254 ip address 10.1.239.1 255.255.255.0
255 !
256 ip http server
257 ip http secure-server
258 !
259 ip access-list standard ACL-MGMT
260 remark Solo gestion desde VLAN Pod1-adm
261 permit 10.1.239.0 0.0.0.255
262 deny any log
263 logging esm config
264 !
265 radius server RAD1
266 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
267 key Bayern_2025
268 !
269 !
270 !
271 line con 0
272 password munics
273 line vty 0 4
274 password munics
275 authorization exec AAA-AUTHZ
276 login authentication AAA-LOGIN
277 transport input telnet ssh
278 line vty 5 15
279 !
280 end

```

3.2 DL-SW1

```
1  DL-SW1#show running-config
2  Building configuration...
3
4  Current configuration : 4913 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 $1$zKX1$6XtnZqAyzRsANPWZbyDWH.
18 enable password munics
19 !
20 !
21 !
22 aaa new-model
23 !
24 !
25 aaa authentication login AAA-LOGIN group radius local
26 aaa authentication login CONSOLE group radius local
27 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
28 aaa authorization exec CONSOLE group radius local
29 !
30 !
31 !
32 aaa session-id common
33 system mtu routing 1500
34 ip routing
35 ip domain-name munics.pri
36 !
37 !
38 !
39 !
40 crypto pki trustpoint TP-self-signed-3139015552
41 enrollment selfsigned
42 subject-name cn=IOS-Self-Signed-Certificate-3139015552
43 revocation-check none
44 rsakeypair TP-self-signed-3139015552
45 !
46 !
47 crypto pki certificate chain TP-self-signed-3139015552
48 certificate self-signed 01
49     30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
50     31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
51     69666963 6174652D 33313339 30313535 3532301E 170D3933 30333031 30303030
52     35365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
53     4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31333930
54     31353535 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
55     8100EEFO 77B70D39 C077512A 5E183579 2E051087 D4B06526 22A76CB5 11FCC6EC
56     A3F2516A DFBE4837 104CF317 B63576B7 7FE48A7B 2F3F8F01 C095FB6A F3F9A15C
57     F3E052FB F2B60124 6A6BF8DD B2C6DD7A 175F496A 3228903B B6288596 B7F15493
58     4BFF2578 D16AB815 F61B3253 F8E5B0C9 EC236C7B DBD2802D 5CF30BAB 806A39E8
59     54E50203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
60     551D1104 15301382 11444C2D 5357312E 6D756E69 63732E70 7269301F 0603551D
```

```

61  23041830 168014EB 2849A1D4 49DFF386 2F8F4A87 7DA4977D 18848B30 1D060355
62  1D0E0416 0414EB28 49A1D449 DFF3862F 8F4A877D A4977D18 848B300D 06092A86
63  4886F70D 01010405 00038181 00307FFD AB23E244 74634FD5 44EB45CC C0211344
64  3C00652E 97E7E5CE EA8C42D9 FE518876 D5172237 6090DABE 211B3531 38A323B1
65  D3C37783 BF1CDC40 CFB0AD25 AD830DB0 4B30792F BC6F3D7C E9EC5056 03153280
66  6D2B31A0 6DC1BEC7 24691E7D 095F8D2E 98384A30 3DD6DBDD 5E3771FE 454907D6
67  C72687DF FB681141 C5E6CD8A FF
68  quit
69 !
70 !
71 !
72 !
73 spanning-tree mode pvst
74 spanning-tree extend system-id
75 spanning-tree vlan 16-18,739,745 priority 24576
76 !
77 vlan internal allocation policy ascending
78 !
79 ip ssh time-out 60
80 ip ssh version 2
81 !
82 !
83 !
84 interface FastEthernet0/1
85 !
86 interface FastEthernet0/2
87 !
88 interface FastEthernet0/3
89 !
90 interface FastEthernet0/4
91 !
92 interface FastEthernet0/5
93 !
94 interface FastEthernet0/6
95 !
96 interface FastEthernet0/7
97 !
98 interface FastEthernet0/8
99 !
100 interface FastEthernet0/9
101 !
102 interface FastEthernet0/10
103 !
104 interface FastEthernet0/11
105 !
106 interface FastEthernet0/12
107   switchport trunk encapsulation dot1q
108   switchport trunk allowed vlan 16-18,739
109   switchport mode trunk
110   switchport nonegotiate
111 !
112 interface FastEthernet0/13
113   switchport trunk encapsulation dot1q
114   switchport trunk allowed vlan 2,739,740
115   switchport mode trunk
116 !
117 interface FastEthernet0/14
118   switchport access vlan 3
119   switchport mode access
120 !
121 interface FastEthernet0/15
122   switchport trunk encapsulation dot1q

```

```

123  switchport trunk allowed vlan 3,739
124  switchport mode trunk
125 !
126 interface FastEthernet0/16
127  switchport access vlan 4
128  switchport mode access
129 !
130 interface FastEthernet0/17
131  switchport trunk encapsulation dot1q
132  switchport trunk allowed vlan 4,739
133  switchport mode trunk
134 !
135 interface FastEthernet0/18
136 !
137 interface FastEthernet0/19
138 !
139 interface FastEthernet0/20
140 !
141 interface FastEthernet0/21
142 !
143 interface FastEthernet0/22
144 !
145 interface FastEthernet0/23
146 !
147 interface FastEthernet0/24
148  switchport trunk encapsulation dot1q
149  switchport trunk allowed vlan 739,740
150  switchport mode trunk
151 !
152 interface GigabitEthernet0/1
153 !
154 interface GigabitEthernet0/2
155 !
156 interface Vlan1
157  no ip address
158  shutdown
159 !
160 interface Vlan2
161  ip address 10.1.0.1 255.255.255.252
162  ip ospf 1 area 0
163 !
164 interface Vlan16
165  ip address 10.1.16.1 255.255.255.0
166  ip helper-address 10.1.239.100
167  ip ospf 1 area 0
168 !
169 interface Vlan17
170  ip address 10.1.17.1 255.255.255.0
171  ip helper-address 10.1.239.100
172  ip ospf 1 area 0
173 !
174 interface Vlan18
175  ip address 10.1.18.1 255.255.255.0
176  ip helper-address 10.1.239.100
177  ip ospf 1 area 0
178 !
179 interface Vlan739
180  ip address 10.1.239.2 255.255.255.0
181 !
182 router ospf 1
183  log-adjacency-changes
184  passive-interface default

```

```

185 no passive-interface Vlan2
186 !
187 ip classless
188 ip http server
189 ip http secure-server
190 !
191 !
192 ip access-list standard ACL-MGMT
193 remark Solo gestion desde VLAN Pod1-adm
194 permit 10.1.239.0 0.0.0.255
195 deny   any log
196 !
197 ip sla enable reaction-alerts
198 !
199 radius-server host 10.1.239.100 auth-port 1812 acct-port 1813 key Bayern_2025
200 !
201 !
202 line con 0
203 password munics
204 line vty 0 4
205 access-class ACL-MGMT in
206 password munics
207 authorization exec AAA-AUTHZ
208 login authentication AAA-LOGIN
209 transport input ssh
210 line vty 5 15
211 !
212 end

```

3.3 FW

```
1 FW#show running-config
2 Building configuration...
3
4 Current configuration : 2842 bytes
!
6 ! Last configuration change at 13:39:38 UTC Fri Nov 7 2025 by superMunics
7 !
8 version 15.4
9 service timestamps debug datetime msec
10 service timestamps log datetime msec
11 no service password-encryption
12 !
13 hostname FW
14 !
15 boot-start-marker
16 boot-end-marker
17 !
18 !
19 enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
20 enable password munics
21 !
22 aaa new-model
23 !
24 !
25 aaa authentication login AAA-LGIN group radius local
26 aaa authentication login SSH-LGIN group radius local
27 aaa authentication login CONSOLE group radius local
28 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
29 aaa authorization exec SSH-LGIN group radius local
30 aaa authorization exec CONSOLE group radius local
31 !
32 !
33 !
34 !
35 !
36 aaa session-id common
37 memory-size iomem 15
38 !
39 !
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 !
49 !
50 !
51 !
52 !
53 ip domain name munics.pri
54 ip cef
55 no ipv6 cef
56 !
57 multilink bundle-name authenticated
58 !
59 !
60 !
```

```

61 license udi pid CISCO1941/K9 sn FCZ1731609A
62 license boot c1900 technology-package securityk9
63 license boot c1900 technology-package datak9
64 !
65 !
66 username juniorAdmin secret 5 $1$7V/v$HXT2XqfZZ1yakmQIW/YxH1
67 username admin privilege 15 secret 5 $1$XJKK$2EQITMry7Lf7R0hltEAcL.
68 !
69 redundancy
70 !
71 !
72 !
73 !
74 !
75 ip ssh time-out 60
76 ip ssh version 2
77 !
78 !
79 !
80 !
81 !
82 !
83 !
84 !
85 !
86 !
87 interface Embedded-Service-Engine0/0
88   no ip address
89   shutdown
90 !
91 interface GigabitEthernet0/0
92   description Trunk to DL-SW1 F0/13
93   no ip address
94   duplex auto
95   speed auto
96 !
97 interface GigabitEthernet0/0.2
98   encapsulation dot1Q 2
99   ip address 10.1.0.2 255.255.255.252
100 !
101 interface GigabitEthernet0/0.739
102   description ADM (Pod1)
103   encapsulation dot1Q 739
104   ip address 10.1.239.3 255.255.255.0
105 !
106 interface GigabitEthernet0/0.740
107   encapsulation dot1Q 740
108   ip address 10.1.240.1 255.255.255.0
109 !
110 interface GigabitEthernet0/1
111   ip address 10.1.0.5 255.255.255.252
112   duplex auto
113   speed auto
114 !
115 interface Serial0/0/0
116   no ip address
117   shutdown
118   clock rate 2000000
119 !
120 interface Serial0/0/1
121   no ip address
122   shutdown

```

```

123  clock rate 2000000
124 !
125 router ospf 1
126   passive-interface default
127   no passive-interface GigabitEthernet0/0.2
128   no passive-interface GigabitEthernet0/1
129   network 10.1.0.0 0.0.255.255 area 0
130 !
131 ip forward-protocol nd
132 !
133 no ip http server
134 no ip http secure-server
135 !
136 !
137 ip access-list standard ACL-MGMT
138   remark Solo gestion desde VALN Pod1_adm
139   permit 10.1.239.0 0.0.0.255
140   deny   any log
141 !
142 ip radius source-interface GigabitEthernet0/0.739
143 !
144 !
145 !
146 radius server RAD1
147   address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
148   key Bayern_2025
149 !
150 !
151 !
152 control-plane
153 !
154 !
155 !
156 line con 0
157   password munics
158   login authentication CONSOLE
159 line aux 0
160 line 2
161   no activation-character
162   no exec
163   transport preferred none
164   transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
165   stopbits 1
166 line vty 0 4
167   access-class ACL-MGMT in
168   password munics
169   authorization exec AAA-AUTHZ
170   login authentication AAA-LOGIN
171   transport input ssh
172 !
173 scheduler allocate 20000 1000
174 !
175 end

```

3.4 CPE

```
1   CPE#show running-config
2 Building configuration...
3
4
5 Current configuration : 2276 bytes
6 !
7 ! Last configuration change at 17:55:37 UTC Fri Nov 7 2025 by superMunics
8 !
9 version 15.7
10 service timestamps debug datetime msec
11 service timestamps log datetime msec
12 no service password-encryption
13 !
14 hostname CPE
15 !
16 boot-start-marker
17 boot-end-marker
18 !
19 !
20 enable secret 5 $1$3FPY$n.Qd8MGjf/Gdju/Fd6Ai2.
21 enable password munics
22 !
23 aaa new-model
24 !
25 !
26 aaa authentication login AAA-LIST group radius local
27 aaa authentication login CONSOLE group radius local
28 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
29 aaa authorization exec CONSOLE group radius local
30 !
31 !
32 !
33 !
34 !
35 !
36 aaa session-id common
37 !
38 !
39 !
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 !
49 ip domain name munics.pri
50 ip cef
51 no ipv6 cef
52 !
53 multilink bundle-name authenticated
54 !
55 !
56 !
57 license udi pid CISCO1941/K9 sn FHK14287AAC
58 !
59 !
60 username admin privilege 15 secret 5 $1$C97z$JGvHtFWUCPaWk9XVeYx310
```

```

61 username juniorAdmin secret 5 $1$Jm7P$ZdkceIBDI6WeyrwRy2DXt1
62 !
63 redundancy
64 !
65 !
66 !
67 !
68 !
69 !
70 !
71 !
72 !
73 !
74 !
75 !
76 !
77 !
78 !
79 interface Embedded-Service-Engine0/0
80   no ip address
81   shutdown
82 !
83 interface GigabitEthernet0/0
84   no ip address
85   duplex auto
86   speed auto
87 !
88 interface GigabitEthernet0/0.3
89   encapsulation dot1Q 3
90   ip address 10.1.0.6 255.255.255.252
91 !
92 interface GigabitEthernet0/0.739
93   encapsulation dot1Q 739
94   ip address 10.1.239.4 255.255.255.0
95 !
96 interface GigabitEthernet0/1
97   ip address 192.0.1.1 255.255.255.0
98   duplex auto
99   speed auto
100 !
101 router ospf 1
102   passive-interface default
103   no passive-interface GigabitEthernet0/0.3
104   network 10.1.0.4 0.0.0.3 area 0
105   default-information originate
106 !
107 ip forward-protocol nd
108 !
109 no ip http server
110 no ip http secure-server
111 !
112 ip route 0.0.0.0 0.0.0.0 192.0.1.2
113 ip ssh time-out 60
114 ip ssh version 2
115 !
116 ip access-list standard ACL-MGMT
117   permit 10.1.239.0 0.0.0.255
118   deny   any log
119 !
120 !
121 !
122 !

```

```
123 radius server RAD1
124 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
125 key Bayern_2025
126 !
127 !
128 !
129 control-plane
130 !
131 !
132 line con 0
133 password munics
134 login authentication CONSOLE
135 line aux 0
136 line 2
137 no activation-character
138 no exec
139 transport preferred none
140 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
141 stopbits 1
142 line vty 0 4
143 access-class ACL-MGMT in
144 password munics
145 authorization exec AAA-AUTHZ
146 login authentication AAA-LOGIN
147 transport input ssh
148 !
149 scheduler allocate 20000 1000
150 !
151 end
```

3.5 ISP

```
1  ISP#show running-config
2  Building configuration...
3
4  Current configuration : 2380 bytes
5  !
6  ! Last configuration change at 15:12:15 UTC Fri Nov 7 2025 by superMunics
7  !
8  version 15.4
9  service timestamps debug datetime msec
10 service timestamps log datetime msec
11 no service password-encryption
12 !
13 hostname ISP
14 !
15 boot-start-marker
16 boot-end-marker
17 !
18 !
19 no logging console
20 enable secret 5 $1$Pyez$rusV3Zwb.xaThFtrZJgsP/
21 enable password munics
22 !
23 aaa new-model
24 !
25 !
26 aaa authentication login SSH-LOGIN group radius local
27 aaa authentication login CONSOLE group radius local
28 aaa authorization exec SSH-LOGIN group radius local
29 aaa authorization exec CONSOLE group radius local
30 !
31 !
32 !
33 !
34 !
35 aaa session-id common
36 memory-size iomem 15
37 !
38 !
39 !
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 !
49 !
50 !
51 !
52 ip domain name munics.pri
53 ip cef
54 no ipv6 cef
55 !
56 multilink bundle-name authenticated
57 !
58 !
59 !
60 license udi pid CISCO1941/K9 sn FCZ1626901Y
```

```

61 license boot c1900 technology-package datak9
62 !
63 !
64 username juniorAdmin secret 5 $1$1n22$4rNzB0PvcUyeIGzyU1h7R0
65 username admin privilege 15 secret 5 $1$AgDE$8L9VyE7FY3JaKLgNZMtad.
66 !
67 redundancy
68 !
69 !
70 !
71 !
72 !
73 ip ssh version 2
74 !
75 !
76 !
77 !
78 !
79 !
80 !
81 !
82 !
83 !
84 interface Embedded-Service-Engine0/0
85   no ip address
86   shutdown
87 !
88 interface GigabitEthernet0/0
89   description TRUNK link to DL-SW1 F0/17
90   no ip address
91   duplex auto
92   speed auto
93 !
94 interface GigabitEthernet0/0.4
95   encapsulation dot1Q 4
96   ip address 192.0.1.2 255.255.255.0
97 !
98 interface GigabitEthernet0/0.739
99   description ADM (VLAN 739)
100  encapsulation dot1Q 739
101  ip address 10.1.239.5 255.255.255.0
102 !
103 interface GigabitEthernet0/1
104  ip address 192.0.0.1 255.255.255.0
105  duplex auto
106  speed auto
107 !
108 interface Serial0/0/0
109  no ip address
110  shutdown
111  clock rate 2000000
112 !
113 interface Serial0/0/1
114  no ip address
115  shutdown
116  clock rate 2000000
117 !
118 ip forward-protocol nd
119 !
120 no ip http server
121 no ip http secure-server
122 !

```

```

123 ip route 10.1.0.0 255.255.0.0 192.0.1.1
124 !
125 ip access-list standard MGMT-ONLY
126   permit 10.1.239.0 0.0.0.255
127   deny   any log
128 !
129 ip radius source-interface GigabitEthernet0/0.739
130 !
131 !
132 radius-server host 10.1.239.100 auth-port 1812 acct-port 1813 key Bayern_2025
133 !
134 !
135 !
136 control-plane
137 !
138 !
139 !
140 line con 0
141   logging synchronous
142   login authentication CONSOLE
143 line aux 0
144 line 2
145   no activation-character
146   no exec
147   transport preferred none
148   transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
149   stopbits 1
150 line vty 0 4
151   access-class MGMT-ONLY in
152   authorization exec SSH-LGIN
153   login authentication SSH-LGIN
154   transport input ssh
155 !
156 scheduler allocate 20000 1000
157 !
158 end

```