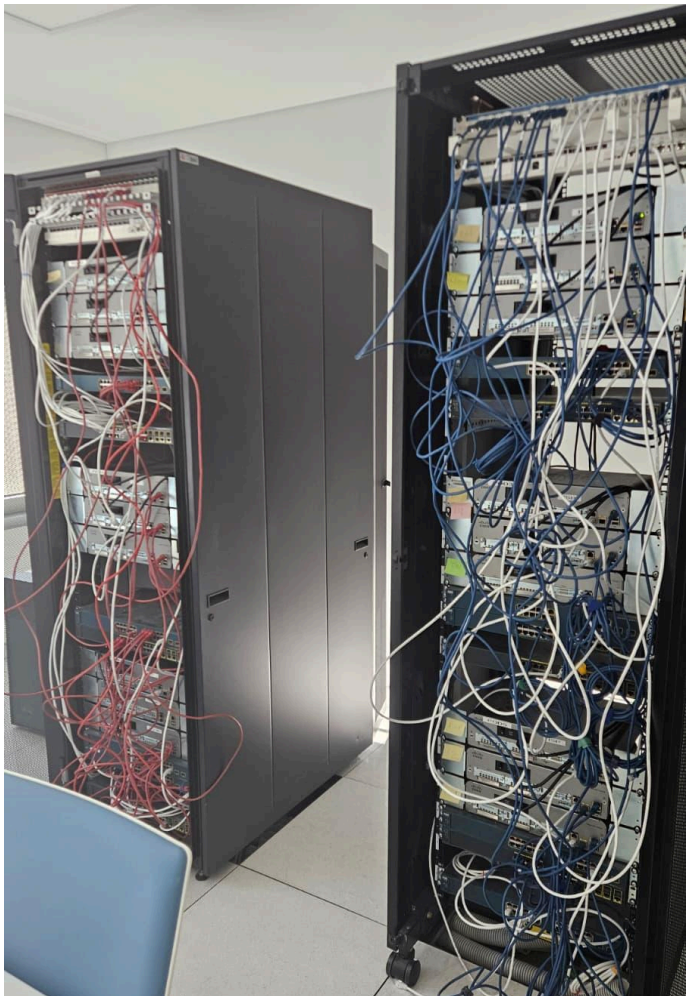
Redes Seguras - Práctica 1



Lennart Thiele
Aarón Cela Riveiro
Samuel Vázquez Fernández
Sergio Vila Riveira
A Coruña a 10 de Octubre de 2025

Índice

Lab 0

Cuestiones del Laboratorio 0

¿Por qué es necesario borrar la configuración de inicio (startup-config) antes de volver a cargar el router?

Se borra para garantizar que el dispositivo arranque sin configuraciones previas y se pueda trabajar desde cero.

Después de guardar la *running-config* como *startup-config*, encuentras un par de problemas de configuración, por lo que realizas los cambios necesarios para solucionar esos problemas. Si ahora se quisiera reiniciar el dispositivo, ¿qué configuración se aplicaría después del reinicio?

Si reinicias sin volver a guardar, el dispositivo perderá los cambios de la **running-config** y cargará de nuevo la **startup-config** (con la configuración de antes de borrar).

Por tanto, después del reinicio se aplicaría la configuración incorrecta (la guardada en **startup-config**), no la corregida.

Para que los cambios buenos persistan, habría que hacer:

```
copy running-config startup-config
```

Lab 1

Cuestiones del Laboratorio 1

Preguntas paso 5:

a) Revisa la configuración en ejecución mediante el comando:

```
Router# show running-config
```

¿Qué problema ves en la salida de este comando?

Podemos ver el texto en claro de la contraseña que acabamos de configurar.

b) Revisa ahora la configuración de inicio mediante el comando:

```
Router# show startup-config
```

¿Qué problema ves en la salida de este comando?

Este comando nos muestra una salida vacía, ya que los cambios que se han efectuado y aparecen en la running-config, no los hemos consolidado en la startup-config, por lo que si el router llega a reiniciarse perderíamos la configuración.

Preguntas paso 6:

a) ¿Qué contraseña debes usar para acceder al modo privilegiado? ¿Qué puedes concluir acerca de la prevalencia de contraseñas? Revisa la configuración en ejecución mediante el comando:

```
Router# show running-config
```

La contraseña que debemos utilizar para acceder al modo privilegiado es **bayern.**
La conclusión es que prevalece la contraseña creada con **enable secret.**

b) ¿Qué conclusiones puedes sacar con respecto a los comandos enable password y enable secret?

Si utilizamos el comando **enable password** la contraseña aparece en claro en la running-config, en cambio, con el comando **enable secret** se almacena usando un algoritmo de hashing unidireccional.

Con esto concluimos que con **enable password** la seguridad es prácticamente nula y **enable secret** es mucho más seguro, por lo que para almacenar la contraseña para acceder al modo privilegiado usaremos el segundo comando.

Así se ven ambas contraseñas en la running-config:

```
enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
enable password munics
```

c) ¿Qué sucedería si en este momento reiniciases el equipo con el comando reload?

Tras **reload**, si no se guarda la running-config, se perderán los cambios.

d) ¿Al rearrancar el router, qué sucedería si no recordases la contraseña de acceso a través de consola o la contraseña de acceso al modo privilegiado? ¿Qué se te ocurriría para intentar solucionar el problema?

Realizamos el proceso de recuperación de clave, los routers y switches tienen un método de recuperación de contraseñas. De hecho en los siguientes laboratorios (2 y 3) trabajaremos con ello.

```
Router>ena
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#login
% Login disabled on line 0, until 'password' is set
Router(config-line)#password munics
Router(config-line)#end
Router#
*Sep 29 10:52:50.239: %SYS-5-CONFIG_I: Configured from console by console
```

```
Router>ena
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password munics
Router(config)#end
Router#
*Sep 29 10:54:39.451: %SYS-5-CONFIG_I: Configured from console by console
```

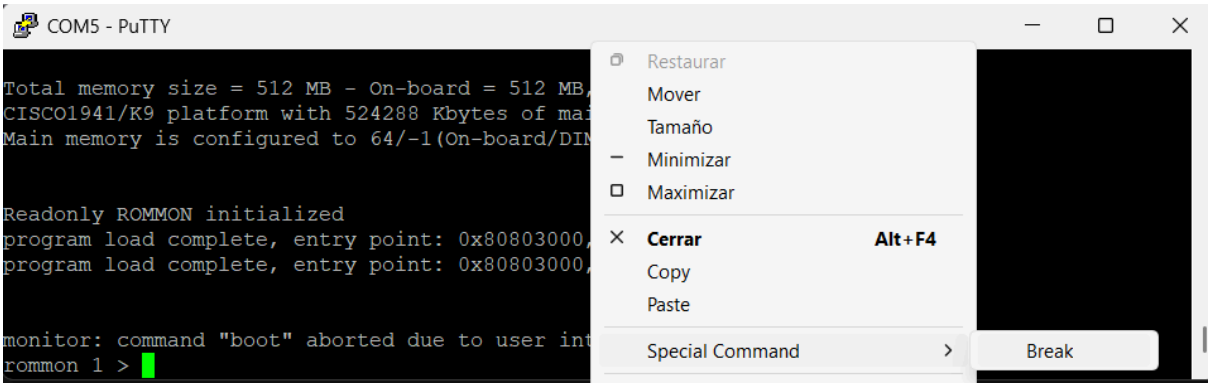
```
User Access Verification

Password:
Router>ena
Password:
Router#show running-config
Building configuration...

Current configuration : 1317 bytes
!
! Last configuration change at 10:54:39 UTC Mon Sep 29 2025
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
enable password munics
```

```
Router#show startup-config
startup-config is not present
```

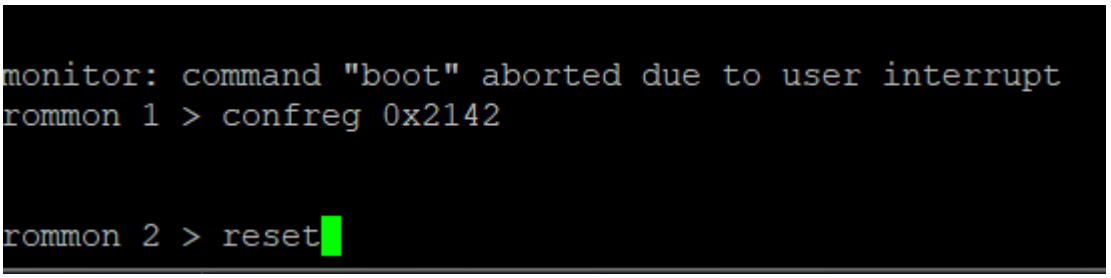
```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret bayern
Router(config)#end
Router#
*Sep 29 11:02:49.267: %SYS-5-CONFIG_I: Configured from console by console
```

Lab 2

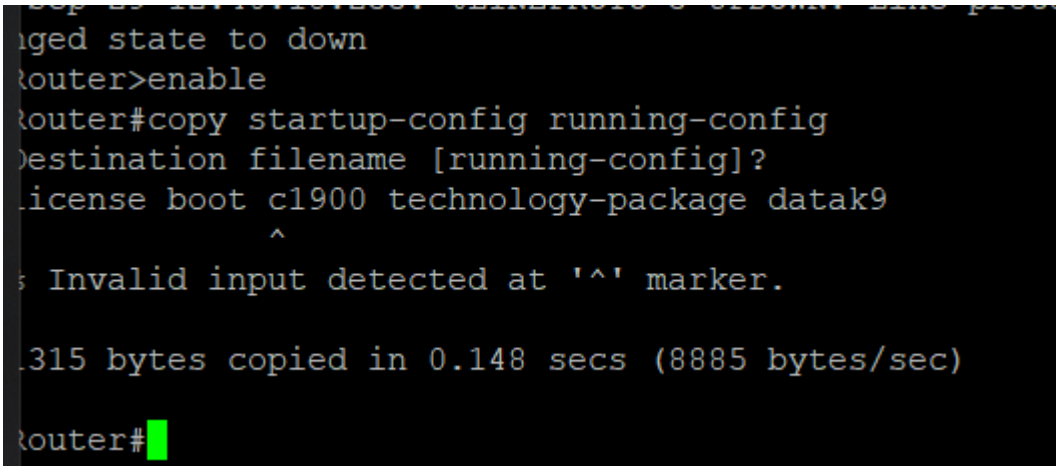
1. Para acceder al modo de recuperación de contraseñas en el router, primero tendremos que apagar y encender el router manualmente.
Justo después debemos de pulsar Break en la secuencia de encendido varias veces.
A continuación veremos que el router arranca en modo ROMMON.



2. Dentro del modo ROMMON, debemos establecer el valor del registro de configuración a **0x2142**, como se puede ver en la siguiente imagen. De esta forma estaremos omitiendo la configuración de inicio donde se almacenan las contraseñas.



3. En **startup-config** podremos ver la configuración anterior del router, la que en un principio hemos ignorado. Seguiremos copiando la **startup-config** a la **running-config**, para pasar a la configuración anterior.



4. Como el router ya está en modo privilegiado, aprovecharemos para editar la contraseña de acceso y la del modo privilegiado, y de esta forma recuperar el acceso a ambas. Y para continuar guardaremos la running-config (con las contraseñas nuevas) en la startup-config mediante el comando **wr.**

```
Router#
Router#
Router#
*Sep 30 09:26:25.823: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret bayern
Router(config)#line console 0
Router(config-line)#password munics
Router(config-line)#end
Router#
*Sep 30 09:26:59.675: %SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
Router#
```

5. Para finalizar, debemos editar de nuevo el valor del registro a su valor por defecto para que la startup-config se cargue cuando se arranca el router.

```
Router#
Router#ena
Router#show version | include Configuration
Configuration register is 0x2142
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#config-register 0x2102
Router(config)#show version | include register
                ^
% Invalid input detected at '^' marker.

Router(config)#end
Router#configure terminal
*Sep 30 09:28:30.955: %SYS-5-CONFIG_I: Configured from show version | include Configuration
Configuration register is 0x2142 (will be 0x2102 at next reload)
Router#reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
```

Lab 3

1. Primero observamos cómo aparece cuando no podemos acceder.

```
User Access Verification

Password:
Password:
Password:
% Bad passwords
```

2. Para poder acceder al modo de recuperación de contraseñas, primero debemos apagar y encender el switch de forma manual.

Después de eso, mantenemos presionado el botón **Mode,** más o menos 15 segundos, mientras el LED parpadea en verde, hasta que cambia a ámbar parpadeando y luego a verde continuo. Cuando esto suceda, aparecerá por pantalla lo siguiente

```
The system has been interrupted prior to initializing the
flash filesystem.  The following commands will initialize
the flash filesystem, and finish loading the operating
system software:

    flash_init
    boot
```

3. Escribimos **flash_init** para iniciar el sistema de archivo de la memoria flash.

```
switch: flash_init
Initializing Flash...
flashfs[0]: 550 files, 19 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 15497216
flashfs[0]: Bytes available: 17016832
flashfs[0]: flashfs fsck took 11 seconds.
...done Initializing Flash.
```

4. Al probar a cargar los comandos de ayuda, el dispositivo no reconoce el comando.

```
switch: load_helper
Unknown cmd: load_helper
```

5. Continuamos cargando el contenido de la memoria con **dir flash:** que nos muestra archivos de configuración. Entre ellos **config.text**, que es el que nos interesa.

```
switch: dir flash:
Directory of flash:/

    2  -rwx  156       <date>              express_setup.debug
    5  -rwx  1801      <date>              AL-SW1.base.G1
    3  -rwx  1919      <date>              private-config.text.renamed
    4  -rwx  5725      <date>              AL-conf
    7  -rwx  1919      <date>              private-config.text
  549  drwx  192       <date>              c2960-lanbasek9-mz.122-58.SE2
    8  -rwx  3096      <date>              multiple-fs
    9  -rwx  1664      <date>              config.text

17016832 bytes available (15497216 bytes used)
```

6. Cambiamos el nombre del archivo que contiene el **startup-config** (**config.text**)para que al iniciar no se cargue y ejecutamos el comando **boot** para iniciar.

```
switch: rename flash:config.text flash:config.text.old

switch: boot
Loading "flash:/c2960-lanbasek9-mz.122-58.SE2/c2960-lanbasek9-mz.122-58.SE2.b
in"...@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

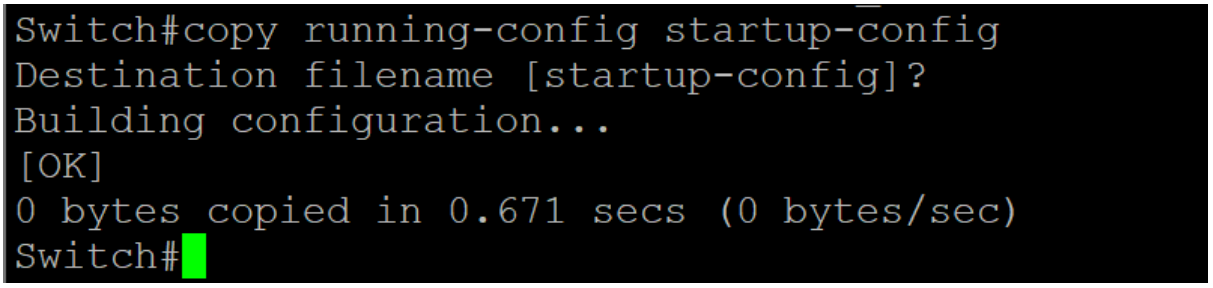
7, Ahora, a parte de ver que nos deja entrar en el switch sin pedir contraseñas (incluso al modo privilegiado), hacemos lo mismo que antes pero a la inversa para renombrar el archivo y poder cargar la configuración en memoria.

```
Switch#rename flash:config.text.old flash:config.text
Destination filename [config.text]?
Switch#copy flash:config.text system:running-config
Destination filename [running-config]?
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)
```

8. Volvemos a configurar las contraseñas como las queremos.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable secret bayern
Switch(config)#line console 0
Switch(config-line)#password munics
Switch(config-line)#login
Switch(config-line)#end
Switch#
```

9. Y copiamos la **running-config** en la **startup-config** para poder entrar con las nuevas contraseñas.



Registro de configuración de routers CISCO

El registro de configuración es un valor de 16 bits en formato hexadecimal que se almacena en el hardware del equipo y controla distintos comportamientos de arranque y diagnóstico del router.
Los tres aspectos principales que gestiona son: el comportamiento de arranque del router, las opciones de carga del sistema y la velocidad de la línea de consola.

Su funcionamiento es sencillo, cuando el router se inicia, revisa su software y los archivos de configuración. Para determinar qué archivos utilizar durante el proceso de arranque, consulta el valor del registro de configuración. Según ese valor, el router decide cómo proceder en el arranque.
Estos valores se representan en la siguiente tabla:

Configuration Register	Router Behavior
0x102	Ignores break 9600 console baud
0x1202	1200 baud rate
0x2101	Boots into bootstrap Ignores break Boots into ROM if initial boot fails 9600 console baud rate
0x2102	Ignores break Boots into ROM if initial boot fails 9600 console baud rate default value for most platforms
0x2120	Boots into ROMmon 19200 console speed
0x2122	Ignores break Boots into ROM if initial boot fails 19200 console baud rate
0x2124	NetBoot Ignores break Boots into ROM if initial boot fails 19200 console speed
0x2142	Ignores break Boots into ROM if initial boot fails 9600 console baud rate Ignores the contents of Non-Volatile RAM (NVRAM) (ignores configuration)
0x2902	Ignores break Boots into ROM if initial boot fails 4800 console baud rate
0x2922	Ignores break Boots into ROM if initial boot fails 38400 console baud rate
0x3122	Ignores break Boots into ROM if initial boot fails 57600 console baud rate
0x3902	Ignores break Boots into ROM if initial boot fails 2400 console baud rate
0x3922	Ignores break Boots into ROM if initial boot fails 115200 console baud rate

Por defecto, el registro de configuración tiene el valor 0x2102. Con este valor, el router realiza un arranque normal y aplica la startup-config almacenada en la NVRAM.
Si se desea modificar este comportamiento, existen dos formas, desde el modo ROMMON (como se ha visto en la práctica) o mediante el comando “config-register”.

Comparación de la NVRAM en routers CISCO y switches CISCO Catalyst

En la arquitectura Cisco, tanto routers como switches heredados de Catalyst utilizan un esquema en el que la startup-config, que se almacena en la NVRAM, es lo mismo a nivel lógico.

Sin embargo, a nivel de implementación física hay una variación clave: los routers Cisco tienen una memoria física NVRAM dedicada, mientras que en los switches Catalyst la startup-config se guarda en la flash.
En otras palabras, la NVRAM no existe físicamente y va "integrada" en la memoria flash. Aun así, el sistema lo implementa igualmente como nvram a nivel de comandos y línea de consola.

Por lo tanto, la diferencia fundamental es que en routers se mantiene una NVRAM dedicada, mientras que en los switches Catalyst esta se ha eliminado y su función es totalmente asumida por la flash.

Lab 4 y Lab 5

AL-SW1

Para el switch volvemos a configurar el hostname y la ip del nombre del dominio

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

Current configuration : 3987 bytes
!
! Last configuration change at 01:00:35 UTC Mon Mar 1 1993
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname AL-SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$4ggR$iNwcR8H.ugsTaXxgbLjRE0
enable password munics
!
no aaa new-model
system mtu routing 1500
!
!
ip domain-name munics.pri
!
!
crypto pki trustpoint TP-self-signed-4271428480
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4271428480
 revocation-check none
 rsakeypair TP-self-signed-4271428480
!
!
crypto pki certificate chain TP-self-signed-4271428480
```

Se crearon diferentes VLANs y se distribuyeron por los puertos GigabitEthernet según correspondía, como puertos de acceso:

-VLAN 739: administración (Pod1-adm)

-VLAN 16: alumnos

-VLAN 17: PDI

-VLAN 18: PAS

A mayores se activó spanning-tree portfast para permitir que los dispositivos se conecten sin esperar el proceso de convergencia STP.

```
interface GigabitEthernet0/1
 switchport access vlan 739
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/2
 switchport access vlan 16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/3
 switchport access vlan 16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/4
 switchport access vlan 16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/5
 switchport access vlan 17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/6
 switchport access vlan 17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/7
 switchport access vlan 17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/8
 switchport access vlan 18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/9
 switchport access vlan 18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/10
 switchport access vlan 18
 switchport mode access
 spanning-tree portfast
!
```

Además el puerto GigabitEthernet 0/20 se estableció como troncal, ya que va a ser el encargado de transportar las distintas VLANs al dispositivo DL-SW1.

Se creó una interfaz virtual VLAN 739 (Pod1-adm) para darle al switch una dirección IP de gestión dentro de la propia red administrativa, para dar acceso remoto y control.

```
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
 switchport trunk allowed vlan 16-18,739
 switchport mode trunk
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan739
 ip address 10.1.239.1 255.255.255.0
!
```

Aquí se listan todas las VLAN configuradas y sus puertos.

```
AL-SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/11, Gi0/12, Gi0/13, Gi0/14
                                                Gi0/15, Gi0/16, Gi0/17, Gi0/18
                                                Gi0/19, Gi0/21, Gi0/22, Gi0/23
                                                Gi0/24
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
739  Pod1-adm                         active    Gi0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
AL-SW1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/20      on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/20      16-18,739

Port        Vlans allowed and active in management domain
Gi0/20      16-18,739

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/20      16-18,739
AL-SW1#
```

Se vuelve a habilitar acceso por telnet remoto al switch.

```
ip http server
ip http secure-server
logging esm config
!
line con 0
 password munics
 login
line vty 0 4
 password munics
 login
line vty 5 15
 login
!
end
```

DL-SW1

Se vuelve a configurar el hostname y el dominio correspondiente

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

Current configuration : 4131 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname DL-SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zKX1$6XtnZqAyzRsANPWZbyDWH.
enable password munics
!
!
!
no aaa new-model
system mtu routing 1500
ip routing
ip domain-name munics.pri
!
!
```

Se listan los siguientes puertos, configurados,

Puertos troncales:

-F0/12: Troncal con AL-SW1 para las VLAN (16-18, 739)

-F0/13: Troncal con FW para las VLAN (2,739,740)

-F0/15: Troncal con CPE para las VLAN (3, 739)

-F0/17: Troncal hacia ISP para las VLAN (4,739)

Puertos de acceso:

-F0/14 y F0/16: usados como puntos de conexión directas.

```
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 16-18,739
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,739,740
 switchport mode trunk
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3,739
 switchport mode trunk
!
interface FastEthernet0/16
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 4,739
 switchport mode trunk
!
```

A mayores el puerto F0/24 utilizado como enlace troncal para las VLAN 739 y 740 (administración y servicios)

```
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 739,740
 switchport mode trunk
!
```

VLANs con direcciones IP asociadas para garantizar la conectividad de capa 3 entre las distintas VLANs del laboratorio

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.1.0.1 255.255.255.252
 ip ospf 1 area 0
!
interface Vlan16
 ip address 10.1.16.1 255.255.255.0
 ip ospf 1 area 0
!
interface Vlan17
 ip address 10.1.17.1 255.255.255.0
 ip ospf 1 area 0
!
interface Vlan18
 ip address 10.1.18.1 255.255.255.0
 ip ospf 1 area 0
!
interface Vlan739
 ip address 10.1.239.2 255.255.255.0
!
```

Se configura el protocolo de enrutamiento OSPF solo para la VLAN 2, que es el enlace de capa 3 entre DL-SW1 y FW.

```
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan2
!
```

Líneas de terminal activadas para conectividad.

```
line con 0
 password munics
 login
line vty 0 4
 password munics
 login
line vty 5 15
 login
!
end
```

ISP

Configuración del hostname y dominio correspondiente, en este caso acme.pri

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$Pyez$rusV3Zwb.xaThFtrZJgsP/
enable password munics
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
!
!


!
!
!
!
ip domain name ascme.pri
ip cef
no ipv6 cef
```

Interfaces:
El router se conecta con el cliente mediante el enlace troncal configurado sobre la interfaz GigabitEthernet0/0.4:

- GigabitEthernet0/0.4: Subinterfaz para la VLAN 4. Representa la red de tránsito entre el ISP y el switch de distribución (DL-SW1)
- GigabitEthernet0/0.739: Subinterfaz para la VLAN de administración, para permitir la gestión remota del equipo dentro del laboratorio.

```
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description TRUNK link to DL-SW1 F0/17
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.0.1.2 255.255.255.0
!
interface GigabitEthernet0/0.739
 description ADM (VLAN 739)
 encapsulation dot1Q 739
 ip address 10.1.239.5 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
```

Configuramos una única ruta IP estática que se corresponde con el switch DL-SW1, de forma que cualquier tráfico destinado a redes internas se enviará a través de la interfaz.

```
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 10.1.0.0 255.255.0.0 192.0.1.1
!
!
!
!
control-plane
```

Se habilita el acceso a consola mediante telnet y línea de comandos.

```
line con 0
 password munics
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password munics
 login
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

Tabla de ip routing del ISP

```
ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
S        10.1.0.0/16 [1/0] via 192.0.1.1
C        10.1.239.0/24 is directly connected, GigabitEthernet0/0.739
L        10.1.239.5/32 is directly connected, GigabitEthernet0/0.739
      192.0.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.1.0/24 is directly connected, GigabitEthernet0/0.4
L        192.0.1.2/32 is directly connected, GigabitEthernet0/0.4
```

CPE

Este es un router de borde externo que hace de pasarela entre la red corporativa (que nos llega desde el FW por la red interna) y el ISP.

```
CPE#show run
Building configuration...

Current configuration : 1547 bytes
!
! Last configuration change at 14:05:35 UTC Thu Oct 9 2025
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CPE
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$3FPY$n.Qd8MGjf/Gdju/Fd6Ai2.
enable password munics
!
```

Se han configurado las siguientes interfaces y las siguientes VLANS:

GigabitEthernet0/0 (troncal 802.1Q hacia DL-SW1): soporte de subinterfaces para separar gestión y tránsito.

- **GigabitEthernet0/0.739** (VLAN de administración): dir 10.1.239.4/24. Uso para gestión remota.
- **GigabitEthernet0/0.3** (VLAN de tránsito con FW): dir 10.1.0.6/30. Enlace punto a punto con el firewall.

GigabitEthernet0/1 (salida a ISP): interfaz de Capa 3 en la red 192.0.1.0/24 con 192.0.1.1. la ruta por defecto hacia 192.0.1.2 y la anuncia al interior, proporcionando salida al exterior al resto del escenario.

```
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 3
 ip address 10.1.0.6 255.255.255.252
!
interface GigabitEthernet0/0.739
 encapsulation dot1Q 739
 ip address 10.1.239.4 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
```

Se configuró el enrutamiento con OSPF, en el que:

- Solo se habilita OSPF en la interfaz G0/0.3, que conecta con el firewall.
- Se anuncia la red 10.1.0.4/30 y se redistribuye la ruta por defecto que el CPE tiene hacia el ISP.

```
!
router ospf 1
 redistribute static subnets
 passive-interface default
 no passive-interface GigabitEthernet0/0.3
 network 10.1.0.4 0.0.0.3 area 0
 default-information originate
!
```

Se configuró la ruta por defecto en el CPE apuntando al ISP como puerta de enlace.

```
!
ip route 0.0.0.0 0.0.0.0 192.0.1.2
!
```

Por último, se vuelve a habilitar el acceso a consola mediante telnet y línea de comandos.

```
!
line con 0
 password munics
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password munics
 login
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

FW

Se establece el nombre del host a FW y el dominio del laboratorio (munics.pri)

```
!
hostname FW
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
enable password munics
!
no aaa new-model
memory-size iomem 15
!
!

!
ip domain name munics.pri
ip cef
no ipv6 cef
!
```

La interfaz física G0/0 la conectamos al switch de distribución (DL-SW1) y transporta varias VLANs mediante subinterfaces. Cada subinterfaz representa:

-VLAN 2: enlace de capa 3 con el switch DL-SW1

-VLAN 739: red de administración (Pod1-adm)

- VLAN 740: red de servicios

La interfaz G0/1 se conecta con el CPE, simulando la frontera entre la red corporativa y el exterior.

```
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Trunk to DL-SW1 F0/13
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 10.1.0.2 255.255.255.252
!
interface GigabitEthernet0/0.739
 description ADM (Pod1)
 encapsulation dot1Q 739
 ip address 10.1.239.3 255.255.255.0
!
interface GigabitEthernet0/0.740
 encapsulation dot1Q 740
 ip address 10.1.240.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 10.1.0.5 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
```

Se activa el protocolo OSPF para el intercambio automático de rutas con los otros dispositivos de red (DL-SW1 y CPE).
Las interfaces que conectan con ellos participan en OSPF, mientras que las demás permanecen pasivas.

```
router ospf 1
 passive-interface default
 no passive-interface GigabitEthernet0/0.2
 no passive-interface GigabitEthernet0/1
 network 10.1.0.0 0.0.255.255 area 0
!
```

Además se habilitó el acceso mediante Telnet por consola virtual, con la contraseña munics.

```
line con 0
 password munics
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password munics
 login
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

A continuación se muestra la tabla de rutas aprendidas y configuradas en el router, donde:

-C: representan las redes locales configuradas directamente en las interfaces del FW

-L: representan las direcciones IP asignadas a las interfaces del propio FW.

-O: son las rutas que obtenemos gracias a aplicar OSPF.

```
FW#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.0.6 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.1.0.6, 00:09:45, GigabitEthernet0/1
      10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
C        10.1.0.0/30 is directly connected, GigabitEthernet0/0.2
L        10.1.0.2/32 is directly connected, GigabitEthernet0/0.2
C        10.1.0.4/30 is directly connected, GigabitEthernet0/1
L        10.1.0.5/32 is directly connected, GigabitEthernet0/1
O        10.1.16.0/24 [110/2] via 10.1.0.1, 00:50:45, GigabitEthernet0/0.2
O        10.1.17.0/24 [110/2] via 10.1.0.1, 00:50:35, GigabitEthernet0/0.2
O        10.1.18.0/24 [110/2] via 10.1.0.1, 00:50:25, GigabitEthernet0/0.2
C        10.1.239.0/24 is directly connected, GigabitEthernet0/0.739
L        10.1.239.3/32 is directly connected, GigabitEthernet0/0.739
C        10.1.240.0/24 is directly connected, GigabitEthernet0/0.740
L        10.1.240.1/32 is directly connected, GigabitEthernet0/0.740
```

Pruebas de Conectividad

AL-SW1

Pings hacia DL-SW1, FW, CPE, ISP

```
AL-SW1#ping 10.1.239.2 source 10.1.239.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
AL-SW1#ping 10.1.239.3 source 10.1.239.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.3, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
AL-SW1#ping 10.1.239.4 source 10.1.239.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.4, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
AL-SW1#ping 10.1.239.5 source 10.1.239.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.5, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

DL-SW1

Pings a la VLAN de gestión 739 (AL-SW1, FW, CPE, ISP)

```
DL-SW1#ping 10.1.239.1 source 10.1.239.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
DL-SW1#ping 10.1.239.3 source 10.1.239.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.3, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
DL-SW1#ping 10.1.239.4 source 10.1.239.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.4, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
DL-SW1#ping 10.1.239.5 source 10.1.239.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.5, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
```

Enlace L3 con FW (VLAN 2)

```
DL-SW1#ping 10.1.0.2 source 10.1.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
```

ISP

Prueba de conexión entre ISP y CPE mediante la VLAN 4

```
ISP#ping 192.0.1.1 source 192.0.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.0.1.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Prueba de alcance de conectividad desde la red de gestión (VLAN 739) a los equipos del segmento 10.1.239.x.

```
ISP#ping 10.1.239.1 source 10.1.239.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
ISP#ping 10.1.239.2 source 10.1.239.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
ISP#ping 10.1.239.3 source 10.1.239.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.3, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms
ISP#ping 10.1.239.4 source 10.1.239.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.4, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Prueba de alcance de conectividad de las VLANs 16,17 y 18.

```
ISP#ping 10.1.16.1 source 192.0.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.16.1, timeout is 2 seconds:
Packet sent with a source address of 192.0.1.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
ISP#ping 10.1.17.1 source 192.0.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.17.1, timeout is 2 seconds:
Packet sent with a source address of 192.0.1.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
ISP#ping 10.1.18.1 source 192.0.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.18.1, timeout is 2 seconds:
Packet sent with a source address of 192.0.1.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

CPE

Ping a 10.1.0.5 (FW) desde la IP de la subinterfaz `10.1.0.6` (G0/0.3): confirma conectividad entre el CPE y el FW en la red VLAN 3.

```
CPE#ping 10.1.0.5 source 10.1.0.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.5, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
CPE#
```

Ping a 192.0.1.2 (ISP) desde `192.0.1.1`

```
CPE#
CPE#ping 192.0.1.2 source 192.0.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.1.2, timeout is 2 seconds:
Packet sent with a source address of 192.0.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
CPE#
```

Pings a 10.1.16.1, 10.1.17.1 y 10.1.18.1 desde 10.1.0.6: conectividad hacia las interfaces de de DL-SW1 en las VLANs de alumnos, PDI y PAS, respectivamente.

```
CPE#
CPE#ping 10.1.16.1 source 10.1.0.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.16.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
CPE#
CPE#ping 10.1.17.1 source 10.1.0.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.17.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
CPE#
CPE#ping 10.1.18.1 source 10.1.0.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.18.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
CPE#
```

FW

Pings de:

- Enlace L3 con DL-SW1
- Enlace L3 con CPE
- De FW por CPE a ISP

```
FW#
FW#ping 10.1.0.1 source 10.1.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
FW#
FW#ping 10.1.0.6 source 10.1.0.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.6, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
FW#
FW#ping 192.0.1.2 source 10.1.0.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
FW#
FW#
```

Vlan de gestión 739 (AL-SW1, DL-SW, CPE e ISP)

```
FW#
FW#ping 10.1.239.1 source 10.1.239.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
FW#
FW#ping 10.1.239.2 source 10.1.239.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
FW#
FW#ping 10.1.239.4 source 10.1.239.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.4, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
FW#
FW#ping 10.1.239.5 source 10.1.239.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.239.5, timeout is 2 seconds:
Packet sent with a source address of 10.1.239.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
FW#
```

Gateways de usuarios en DL-SW1

```
FW#ping 10.1.16.1 source 10.1.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.16.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
FW#
FW#ping 10.1.17.1 source 10.1.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.17.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
FW#
FW#ping 10.1.18.1 source 10.1.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.18.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
FW#
```

Uso de Telnet

Prueba de conectividad mediante telnet desde ISP a AL-SW1 y luego desde AL-SW1 a FW

```
ISP#telnet 10.1.239.1
Trying 10.1.239.1 ... Open


User Access Verification

Password:
AL-SW1>enable
Password:
AL-SW1#telnet 10.1.239.3
Trying 10.1.239.3 ... Open


User Access Verification

Password:
FW>
```

Anexos

Running-configs de todos los equipos

ISP

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

Current configuration : 1654 bytes
!
! Last configuration change at 13:52:39 UTC Fri Oct 10 2025
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$Pyez$rusV3Zwb.xaThFtrZJgsP/
enable password munics
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
!
!


!
!
!
!
ip domain name ascme.pri
```

```
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FCZ1626901Y
license boot c1900 technology-package datak9
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description TRUNK link to DL-SW1 F0/17
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.0.1.2 255.255.255.0
!
interface GigabitEthernet0/0.739
 description ADM (VLAN 739)
 encapsulation dot1Q 739
 ip address 10.1.239.5 255.255.255.0
```

```
!
interface GigabitEthernet0/1
 ip address 192.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 10.1.0.0 255.255.0.0 192.0.1.1
!
!
!
!
control-plane
!
!
!
line con 0
 password munics
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password munics
 login
 transport input telnet
!
scheduler allocate 20000 1000
```

```
!
end
```

FW

```
FW#show startup-config
Using 1916 out of 262136 bytes
!
! Last configuration change at 09:57:19 UTC Thu Oct 9 2025
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FW
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
enable password munics
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
!
!


!
!
!
!
ip domain name munics.pri
ip cef
```

```
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FCZ1731609A
license boot c1900 technology-package securityk9
license boot c1900 technology-package datak9
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Trunk to DL-SW1 F0/13
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 10.1.0.2 255.255.255.252
!
interface GigabitEthernet0/0.739
 description ADM (Pod1)
 encapsulation dot1Q 739
 ip address 10.1.239.3 255.255.255.0
```

```
!
interface GigabitEthernet0/0.740
 encapsulation dot1Q 740
 ip address 10.1.240.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 10.1.0.5 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 passive-interface default
 no passive-interface GigabitEthernet0/0.2
 no passive-interface GigabitEthernet0/1
 network 10.1.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
 password munics
 login
line aux 0
line 2
 no activation-character
 no exec
```

```
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password munics
 login
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

CPE

```
CPE#show run
Building configuration...

Current configuration : 1547 bytes
!
! Last configuration change at 14:05:35 UTC Thu Oct 9 2025
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CPE
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$3FPY$n.Qd8MGjf/Gdju/Fd6Ai2.
enable password munics
!
no aaa new-model
!
!
!
!
!
!
!
!
```

```
!
!
!
!
ip domain name munics.pri
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FHK14287AAC
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 3
 ip address 10.1.0.6 255.255.255.252
!
interface GigabitEthernet0/0.739
```

```
 encapsulation dot1Q 739
 ip address 10.1.239.4 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 redistribute static subnets
 passive-interface default
 no passive-interface GigabitEthernet0/0.3
 network 10.1.0.4 0.0.0.3 area 0
 default-information originate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.0.1.2
!
!
!
!
control-plane
!
!
line con 0
 password munics
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password munics
 login
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

AL-SW1

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

Current configuration : 3987 bytes
!
! Last configuration change at 01:00:35 UTC Mon Mar 1 1993
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname AL-SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$4ggR$iNwcR8H.ugsTaXxgbLjRE0
enable password munics
!
no aaa new-model
system mtu routing 1500
!
!
ip domain-name munics.pri
!
!
crypto pki trustpoint TP-self-signed-4271428480
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4271428480
 revocation-check none
 rsakeypair TP-self-signed-4271428480
!
!
crypto pki certificate chain TP-self-signed-4271428480
 certificate self-signed 01
  3082023E 308201A7 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 34323731 34323834 3830301E 170D3933 30333031
```

```
30303031
  31305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34
32373134
  32383438 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  810085E1 0E0FF69D 55BAA4B8 3242956C 88BA4A20 007F0BAE 7C775218
787A4D1E
  6A592433 AC88CA8D F2E44FA1 8B8061E1 0640595E AB331A30 7231D400
87C14740
  12109636 B239C3DE AB88408E 9479B0AF 0FE5CCBD 29B2AA25 3092B8C2
4953E0E1
  D0A43208 26766077 ADB9F855 EC64E3EA BE46ACC2 C1683A25 5A016AF6
A6C90A66
  EAFD0203 010001A3 66306430 0F060355 1D130101 FF040530 030101FF
30110603
  551D1104 0A300882 06414C2D 53573130 1F060355 1D230418 30168014
2461E8C2
  FF22D3F0 BC988C64 AA5150C1 91900784 301D0603 551D0E04 16041424
61E8C2FF
  22D3F0BC 988C64AA 5150C191 90078430 0D06092A 864886F7 0D010104
05000381
  81001976 F5E919EF 401EF9C9 4E5F1E22 5D43689C AB4DA34C 5115EA1A
EA328AEA
  959211C5 24D74CAE 63B612AA 1A441A29 53AAECAA DDA1E327 E1875D10
9BB45546
  6383FBD2 91CF0913 5F416AA0 3F3AF9CE F2A1F624 09C2BE26 38440BAE
50A154FA
  1F1A65D9 692F3C91 23064A92 7FB6D8B3 1E2E5039 B00C3D60 DFF81C44
BBEFCF41 2EEE
        quit
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface GigabitEthernet0/1
```

```
 switchport access vlan 739
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/2
 switchport access vlan 16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/3
 switchport access vlan 16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/4
 switchport access vlan 16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/5
 switchport access vlan 17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/6
 switchport access vlan 17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/7
 switchport access vlan 17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/8
 switchport access vlan 18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/9
 switchport access vlan 18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/10
 switchport access vlan 18
```

```
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
 switchport trunk allowed vlan 16-18,739
 switchport mode trunk
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan739
 ip address 10.1.239.1 255.255.255.0
!
ip http server
ip http secure-server
logging esm config
!
line con 0
 password munics
```

```
 login
line vty 0 4
 password munics
 login
line vty 5 15
 login
!
end
```

DL-SW1

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

Current configuration : 4131 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname DL-SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zKX1$6XtnZqAyzRsANPWZbyDWH.
enable password munics
!
!
!
no aaa new-model
system mtu routing 1500
ip routing
ip domain-name munics.pri
!
!
!
!
crypto pki trustpoint TP-self-signed-3139015552
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3139015552
```

```
 revocation-check none
 rsakeypair TP-self-signed-3139015552
!
!
crypto pki certificate chain TP-self-signed-3139015552
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 33313339 30313535 3532301E 170D3933 30333031
30303030
  35365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33
31333930
  31353535 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100EEF0 77B70D39 C077512A 5E183579 2E051087 D4B06526 22A76CB5
11FCC6EC
  A3F2516A DFBE4837 104CF317 B63576B7 7FE48A7B 2F3F8F01 C095FB6A
F3F9A15C
  F3E052FB F2B60124 6A6BF8DD B2C6DD7A 175F496A 3228903B B6288596
B7F15493
  4BFF2578 D16AB815 F61B3253 F8E5B0C9 EC236C7B DBD2802D 5CF30BAB
806A39E8
  54E50203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF
30120603
  551D1104 0B300982 07444C2D 5357312E 301F0603 551D2304 18301680
14EB2849
  A1D449DF F3862F8F 4A877DA4 977D1884 8B301D06 03551D0E 04160414
EB2849A1
  D449DFF3 862F8F4A 877DA497 7D18848B 300D0609 2A864886 F70D0101
04050003
  818100C0 F6726ADB BCB9F6FC DEC2AAAF CF6F4622 41A4D0DD 545D7528
B3FDD889
  F724E978 A6AD4AB7 DA203547 4C92D2D6 EA7F23E9 CC48B7B4 200D5333
E2BA4B72
  C43ACD03 6941AC19 D98673B8 D3DDF480 BF8B8462 A0CD4200 C1598031
09819217
  72EAA325 03D1A4AD E0CED5EB 9532BA98 D5BB7F32 35B84289 6183A8C6
8BB25507 401386
  quit
!
!
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 16-18,739
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,739,740
 switchport mode trunk
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 3,739
 switchport mode trunk
!
interface FastEthernet0/16
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 4,739
 switchport mode trunk
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 739,740
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.1.0.1 255.255.255.252
 ip ospf 1 area 0
!
interface Vlan16
 ip address 10.1.16.1 255.255.255.0
 ip ospf 1 area 0
!
interface Vlan17
```

```
 ip address 10.1.17.1 255.255.255.0
 ip ospf 1 area 0
!
interface Vlan18
 ip address 10.1.18.1 255.255.255.0
 ip ospf 1 area 0
!
interface Vlan739
 ip address 10.1.239.2 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan2
!
ip classless
ip http server
ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
 password munics
 login
line vty 0 4
 password munics
 login
line vty 5 15
 login
!
end
```