

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SANTIAGO RAFAEL PALACIO GALVAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
SOLEDAD, ATLANTICO  
2023

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SANTIAGO RAFAEL PALACIO GALVAN

DIPLOMADO O DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL  
TÍTULO DE INGENIERO ELECTRÓNICO

Tutor

GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
SOLEDAD, ATLANTICO  
2023

Nota de aceptación:

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Soledad, 08 de mayo de 2023

## CONTENIDO

|   |    |
|---|----|
| CONTENIDO .....   | 4  |
| LISTA DE TABLAS .....   | 5  |
| LISTA DE FIGURAS .....  | 5  |
| GLOSARIO .....  | 8  |
| RESUMEN.....  | 9  |
| ABSTRACT.....   | 9  |
| INTRODUCCIÓN.....   | 10 |
| DESARROLLO .....  | 12 |
| 1 Tabla de direccionamiento .....   | 12 |
| 1.1 Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces ..... | 13 |
| 1.2 Configuración básica de los dispositivos .....  | 13 |
| 1.3 Configurar los pc1, pc2, pc3 y pc4 de acuerdo con la tabla de direccionamiento. ....                                | 23 |
| 1.4 Configurar vrf y enrutamiento estatico. ....  | 26 |
| CONCLUSIONES .....  | 61 |
| BIBLIOGRAFIA.....   | 62 |

## LISTA DE TABLAS

|  |    |
|--|----|
| Tabla 1. Direccionamiento de la Red..... | 12 |
|--|----|

## LISTA DE FIGURAS

|   |    |
|---|----|
| Figura 1. Escenario de la red.....  | 13 |
| Figura 2. Aplicando código R1.....  | 19 |
| Figura 3. Aplicando código R2.....  | 20 |
| Figura 4. Aplicando código R3.....  | 20 |
| Figura 5. Aplicando código D1.....  | 21 |
| Figura 6. Aplicando código D2.....  | 21 |
| Figura 7. Aplicando código A1.....  | 22 |
| Figura 8. Configuración PC1.....  | 24 |
| Figura 9. Configuración PC2.....  | 25 |
| Figura 10. Configuración PC3.....   | 25 |
| Figura 11. Configuración PC4.....   | 26 |
| Figura 12. Configuración VRF en R1.....                                       | 29 |
| Figura 13. Configuración VRF en R2.....                                       | 30 |
| Figura 14. Configuración VRF en R3.....                                       | 30 |
| Figura 15. Permite la comunicación entre las diferentes interfaces en R1..... | 38 |
| Figura 16. Permite la comunicación entre las diferentes interfaces en R2..... | 38 |
| Figura 17. Permite la comunicación entre las diferentes interfaces en R3..... | 39 |
| Figura 18. Verificación conectividad de R1 y R3.....                          | 42 |
| Figura 19. Desactivación del puerto D1.....                                   | 43 |
| Figura 20. Desactivación del puerto D2.....                                   | 44 |
| Figura 21. Desactivación del puerto A1.....                                   | 45 |
| Figura 22. Configuración troncal en D1.....                                   | 46 |
| Figura 23. Configuración troncal en D2.....                                   | 47 |
| Figura 24. Enlace troncal D1.....   | 48 |
| Figura 25. Enlace troncal A1.....   | 49 |
| Figura 26. Configuración puerto de acceso D1.....                             | 50 |
| Figura 27. Configuración puerto de acceso D2.....                             | 52 |
| Figura 28. Configuración puerto de acceso A1.....                             | 53 |

|   |    |
|---|----|
| Figura 29. Conectividad PC1-PC2.....                    | 54 |
| Figura 30. Conectividad PC3-PC4.....                    | 54 |
| Figura 31. Encriptación en D1, D2, A1.....              | 55 |
| Figura 32. Encriptación R1, R2, R3. ....                | 56 |
| Figura 33. Configurar contraseña en D1, D2 y A1. ....   | 57 |
| Figura 34. Configurar contraseña en R1, R2 y R3. ....   | 57 |
| Figura 35. Habilitación modelo AAA en D1, D2 y A1. .... | 58 |
| Figura 36. Habilitación modelo AAA en R1, R2 y R3. .... | 59 |
| Figura 37. Configuración actual D1, D2 y A1.....        | 59 |
| Figura 38. Configuración actual R1, R2 y R3.....        | 60 |

## GLOSARIO

OSPF (Open Shortest Path First): Protocolo de enrutamiento dinámico utilizado en redes IP para calcular la ruta más corta y confiable entre dos nodos. OSPF es un protocolo de enrutamiento de estado de enlace que selecciona la ruta óptima en función de los costos de los enlaces.

VLAN (Virtual Local Area Network): Una red lógica separada dentro de una red física en la que los dispositivos pueden comunicarse entre sí como si estuvieran conectados a un mismo segmento físico de la red. Las VLAN se utilizan para mejorar la eficiencia y la seguridad de las redes empresariales.

QoS (Quality of Service): La capacidad de priorizar el tráfico de red y asignar ancho de banda en función de las necesidades de los diferentes tipos de datos y aplicaciones. La implementación de QoS es importante para garantizar un rendimiento óptimo de los servicios críticos y evitar la congestión de la red.

ACL (Access Control List): Una lista de reglas que se utiliza para controlar el acceso a una red o dispositivo. Las ACL se utilizan para permitir o denegar el acceso a la red en función de ciertas condiciones, como la dirección IP de origen o destino, el protocolo utilizado, el puerto, etc.

VPN (Virtual Private Network): Una red privada que se extiende a través de una red pública como Internet. Las VPN se utilizan para conectar de forma segura redes remotas o usuarios individuales a una red corporativa. La información transmitida a través de una VPN está protegida por cifrado para garantizar la privacidad y la seguridad de los datos.

## **RESUMEN**

El diseño de soluciones de red escalables implica la selección de protocolos de enrutamiento adecuados para la red, la configuración básica y avanzada de estos protocolos, la configuración de calidad de servicio (QoS) para garantizar el rendimiento de los servicios críticos, y la configuración de redes WAN para asegurar la conectividad entre las oficinas remotas y la sede central.

El uso del protocolo STP permite evitar bucles de red, lo que mejora la fiabilidad de la red y evita la congestión. Por otro lado, la configuración de VLANs permite dividir la red en grupos lógicos, lo que mejora la seguridad y el rendimiento. En conjunto, el uso de STP y VLANs permite diseñar una infraestructura de red jerárquica convergente que mejora la eficiencia y la seguridad de la red.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

Designing scalable network solutions involves selecting appropriate routing protocols for the network, basic and advanced configuration of these protocols, configuring quality of service (QoS) to ensure performance of critical services, and configuring WAN networks to ensure connectivity between remote offices and the central headquarters.

The use of STP protocol helps avoid network loops, improves network reliability and prevents congestion. Additionally, configuring VLANs allows for the division of the network into logical groups, which improves security and performance. Together, the use of STP and VLANs allows for the design of a convergent hierarchical network infrastructure that improves network efficiency and security.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

## INTRODUCCIÓN

La complejidad de las redes empresariales modernas requiere un diseño cuidadoso que incluya elementos como el protocolo Spanning Tree (STP) y la configuración de Virtual LANs (VLANs) para crear una infraestructura de red jerárquica convergente que garantice la eficiencia y la seguridad de la red. Además, es necesario diseñar soluciones escalables que puedan manejar grandes volúmenes de tráfico y asegurar un alto rendimiento para los servicios críticos de la organización, lo que se puede lograr mediante la configuración básica y avanzada de protocolos de enrutamiento y la implementación de servicios IP con calidad de servicio en ambientes de red empresariales LAN y WAN. En resumen, el diseño de una red empresarial eficiente y escalable es fundamental para garantizar el éxito de una organización y la satisfacción del usuario.

Para diseñar una red empresarial escalable, se deben considerar varios factores, incluyendo el tamaño y la complejidad de la organización, el tipo de aplicaciones y servicios que se van a utilizar, y la cantidad de tráfico que se espera en la red. Una red empresarial bien diseñada debe tener una estructura jerárquica que permita una fácil gestión y escalabilidad. Además, es importante seleccionar cuidadosamente los protocolos de enrutamiento adecuados para la red y configurarlos correctamente para evitar congestiones y retrasos en el tráfico de la red.

La implementación de servicios de calidad de servicio (QoS) es también una parte importante del diseño de redes empresariales escalables. Los servicios de QoS permiten priorizar el tráfico de la red, lo que asegura que los servicios críticos de la organización tengan el ancho de banda necesario y una latencia baja para su correcto funcionamiento. Finalmente, la configuración de redes WAN debe ser cuidadosamente planificada para garantizar la conectividad entre las oficinas remotas y la sede central, y para asegurar que los datos se transmitan de manera

segura y eficiente. En conjunto, todos estos factores son esenciales para diseñar una red empresarial escalable y eficiente que pueda satisfacer las necesidades de una organización en crecimiento.

## DESARROLLO

### 1 TABLA DE DIRECCIONAMIENTO

Tabla 1. Direccionamiento de la Red.

| Device | Interface | IPv4 Address   | IPv6 Address             | IPv6 Link-Local |
|--------|-----------|----------------|--------------------------|-----------------|
| R1     | E1/0.1    | 10.0.12.9/24   | 2001:dby:acad:12::1/64   | fe0::1:1        |
|        | E1/0.2    | 10.0.12.9/24   | 2001:dby:acad:12::1/64   | fe0::1:2        |
|        | E1/1.1    | 10.0.113.9/24  | 2001:dby:acad:113::1/64  | fe0::1:3        |
|        | E1/1.2    | 10.0.10y.9/24  | 2001:dby:acad:10y::1/64  | fe0::1:4        |
| R2     | E1/0.1    | 10.0.12.7/24   | 2001:dby:acad:12::2/64   | fe0::2:1        |
|        | E1/0.2    | 10.0.12.7/24   | 2001:dby:acad:12::2/64   | fe0::2:2        |
|        | E1/1.1    | 10.0.23.7/24   | 2001:dby:acad:23::2/64   | fe0::2:3        |
|        | E1/1.2    | 10.0.23.7/24   | 2001:dby:acad:23::2/64   | fe0::2:4        |
| R3     | E1/0.1    | 10.0.23.4/24   | 2001:dby:acad:23::3/64   | fe0::3:1        |
|        | E1/0.2    | 10.0.23.4/24   | 2001:dby:acad:23::3/64   | fe0::3:2        |
|        | E1/1.1    | 10.0.213.4/24  | 2001:dby:acad:213::1/64  | fe0::3:3        |
|        | E1/1.2    | 10.0.20y.4/24  | 2001:dby:acad:20y::1/64  | fe0::3:4        |
| PC1    | NIC       | 10.0.113.97/24 | 2001:dby:acad:113::50/64 | EUI-64          |
| PC2    | NIC       | 10.0.213.97/24 | 2001:dby:acad:213::50/64 | EUI-64          |
| PC3    | NIC       | 10.0.10y.97/24 | 2001:dby:acad:10y::50/64 | EUI-64          |
| PC4    | NIC       | 10.0.20y.97/24 | 2001:dby:acad:20y::50/64 | EUI-64          |

Nota: las letras "X, Y, Z" corresponden a los últimos tres dígitos de su número de cédula

CC: 1100543974

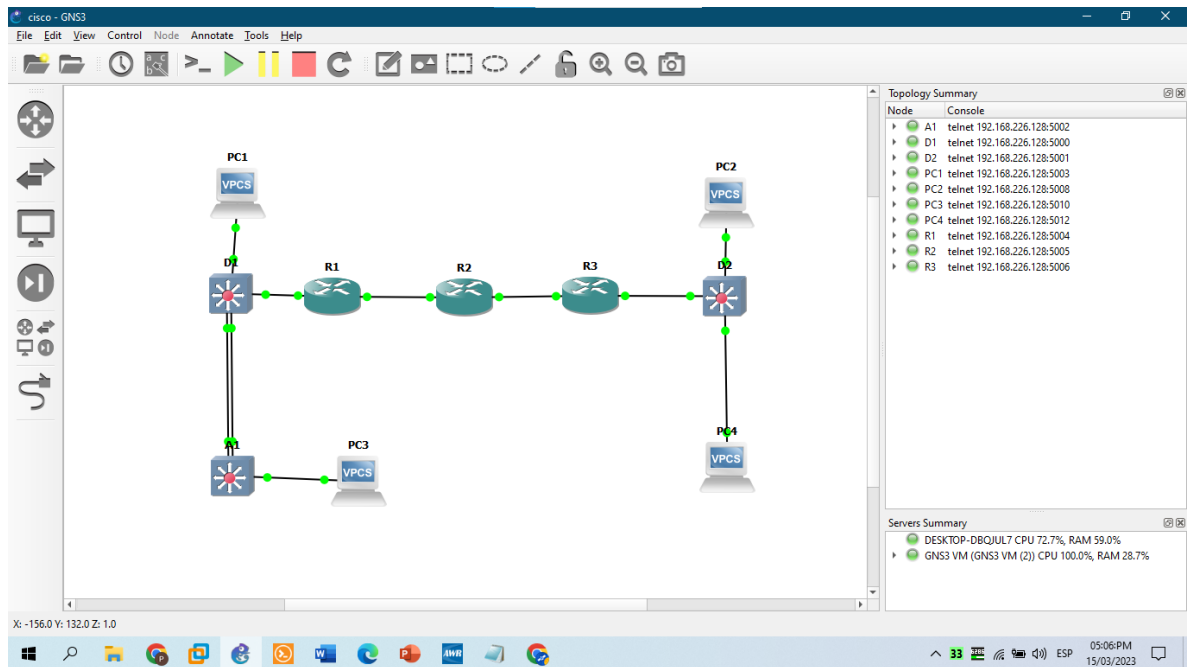
X: 9

Y: 7

Z: 4

## 1.1 Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

Figura 1. Escenario de la red.



Fuente: Autoría propia

## 1.2 Configuración básica de los dispositivos

En este proceso se accede al modo de configuración de cada dispositivo y se aplican las configuraciones básicas correspondientes, las cuales son implementadas mediante códigos específicos en cada uno de ellos.

router 1

hostname r1

ipv6 unicast-routing

```
no ip domain lookup
banner motd # r1, encor skills assessment, scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

Este código configura un router llamado r1, se realiza también con el router r2 y r3, se habilitan el enrutamiento ipv6 unicast y deshabilita la búsqueda de dominio ip. también configura un banner de mensaje de bienvenida para la autenticación y seguridad de acceso, y modifica las líneas de consola para evitar que se cierre la sesión automáticamente y para sincronizar los mensajes de registro.

```
router 2
hostname r2
ipv6 unicast-routing
no ip domain lookup
banner motd # r2, encor skills assessment, scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

El código proporcionado configura algunas características básicas del router 2 (R2) en el escenario 2 del examen de habilidades de ENCOR. A continuación se explica cada una de las líneas del código:

- `hostname R2`: Esto establece el nombre del host para el router 2 como "R2". El nombre del host se utiliza para identificar de manera única el dispositivo en la red.
- `ipv6 unicast-routing`: Esta línea permite que el router enrutamiento unicast IPv6. El enrutamiento es la función principal de los routers, y permite que los paquetes de datos se envíen de una red a otra.
- `no ip domain lookup`: Esta línea desactiva la función de búsqueda de nombres de dominio. Esto significa que si el usuario ingresa una dirección que no es una dirección IP, el router no intentará resolverla en un nombre de dominio.
- `banner motd # R2, ENCOR Skills Assessment, Scenario 2 #`: Esta línea configura un mensaje de banner para ser mostrado en la pantalla de inicio de sesión. El mensaje indica el nombre del router y el escenario del examen.
- `line con 0`: Esta línea configura la conexión a la consola del router.
- `exec-timeout 0 0`: Esta línea establece el tiempo de espera de inactividad en la consola en cero, lo que significa que la sesión no se desconectará automáticamente por inactividad.
- `logging synchronous`: Esta línea configura el registro del router para que sea sincrónico con la entrada de comandos en la consola. Esto significa que los mensajes de registro no se imprimirán mientras se ingresan comandos.
- `exit`: Esta línea sale del modo de configuración de línea de consola.

En general, este código es útil para establecer la configuración básica del router y garantizar que la consola esté configurada adecuadamente para la administración del dispositivo.

```
router 3
```

```
hostname R3
```

```
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

El código presentado corresponde a la configuración del Router 3 en una red, en la que se establecen ciertas directrices para su correcto funcionamiento. Al definir el hostname, se identifica el nombre del dispositivo en la red; al activar el ipv6 unicast-routing, se permite la comunicación entre redes utilizando IPv6; al desactivar el ip domain lookup, se evita la resolución de nombres de dominio DNS que puede afectar el rendimiento de la red; al configurar un banner motd se establece un mensaje de bienvenida o aviso a los usuarios que intenten acceder al dispositivo; finalmente, al configurar la línea de consola, se establecen parámetros como el tiempo de espera de inactividad y el registro sincrónico de eventos de registro para la sesión de consola.

```
switch d1
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
```

```
logging synchronous
exit
vlan 8
name General-Users
exit
vlan 13
name Special-Users
exit
```

Este código establece la configuración inicial de un switch con el nombre D1, aplicado también en el switch D2 y A1, donde se activa el enrutamiento IP y IPv6 unicast, se deshabilita la búsqueda de dominios IP y se agrega un mensaje de bienvenida para fines de autenticación y seguridad de acceso. Además, se ajusta la configuración de la línea de consola para evitar el cierre automático de la sesión y sincronizar los mensajes de registro.

También se configuran dos VLAN en el switch: la VLAN 8 se denomina "General-Users" y la VLAN 13 se denomina "Special-Users". Esta segmentación de red permite clasificar a los usuarios en dos grupos diferentes, lo que puede mejorar la eficiencia y seguridad de la red.

```
switch d2
hostname d2
ip routing
ipv6 unicast-routing
no ip domain lookup
```

```
banner motd # d2, encor skills assessment, scenario 2 #  
line con 0  
exec-timeout 0 0  
logging synchronous  
exit  
vlan 8  
name General-Users  
exit  
vlan 13  
name Special-Users  
exit
```

Este código es utilizado para configurar un switch llamado D2 en el escenario 2 del examen de habilidades ENCOR. Al definir el nombre del host como D2, se identifica claramente en la red. La configuración de "ip routing" y "ipv6 unicast-routing" indica que el switch actúa como un enrutador y puede enrutar paquetes de red entre diferentes subredes. Al definir dos VLANs diferentes (8 y 13), se pueden separar los usuarios generales y especiales en diferentes grupos para la gestión de red y seguridad. También se establece un banner de mensaje de bienvenida para el acceso a la consola y se configura una sesión de consola para que se cierre automáticamente después de un período inactivo.

```
switch a1  
hostname a1  
ipv6 unicast-routing  
no ip domain lookup  
banner motd # a1, encor skills assessment, scenario 2 #
```

line con 0

exec-timeout 0 0

logging synchronous

exit

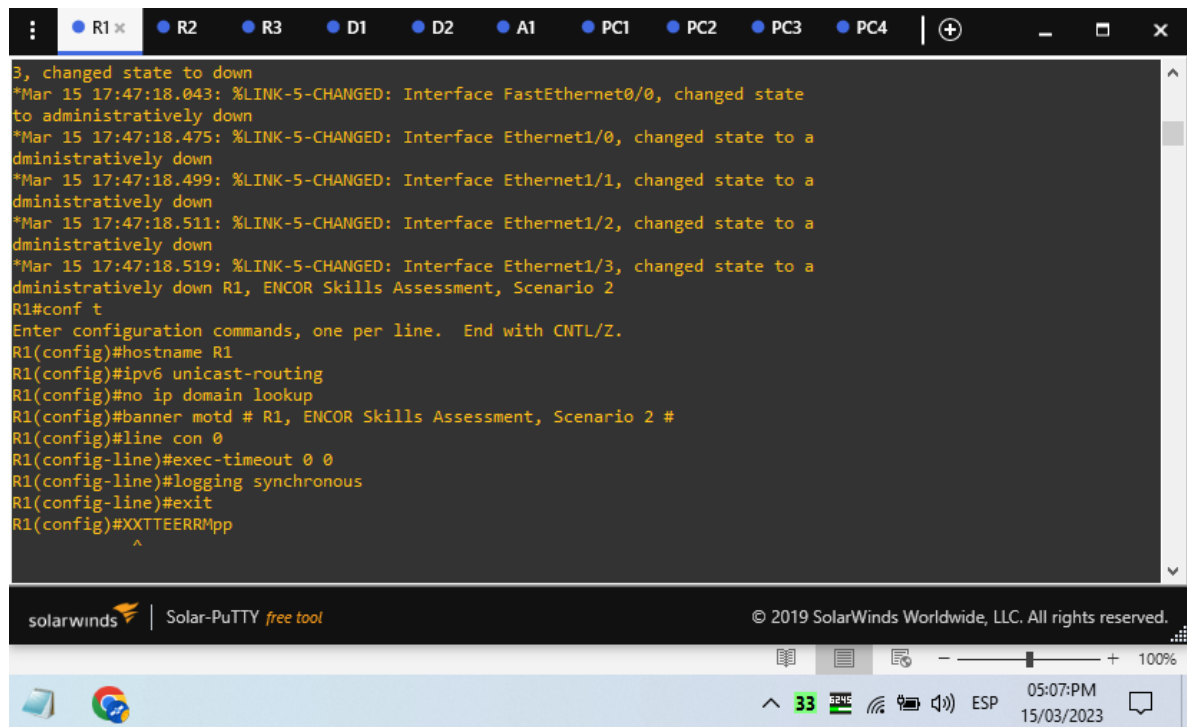
vlan 8

name General-Users

exit

El código configurado en el switch A1 establece el nombre del host del switch, habilita el enrutamiento ipv6 y deshabilita la búsqueda de nombres de dominio en el dispositivo. Además, se establece un mensaje del día (motd) para identificar el switch y se configura un tiempo de espera de inactividad y un registro de eventos en la consola. Finalmente, se crea una vlan llamada "general-users" que puede ser utilizada para separar y segmentar el tráfico de red de diferentes usuarios o dispositivos.

Figura 2. Aplicando código R1.



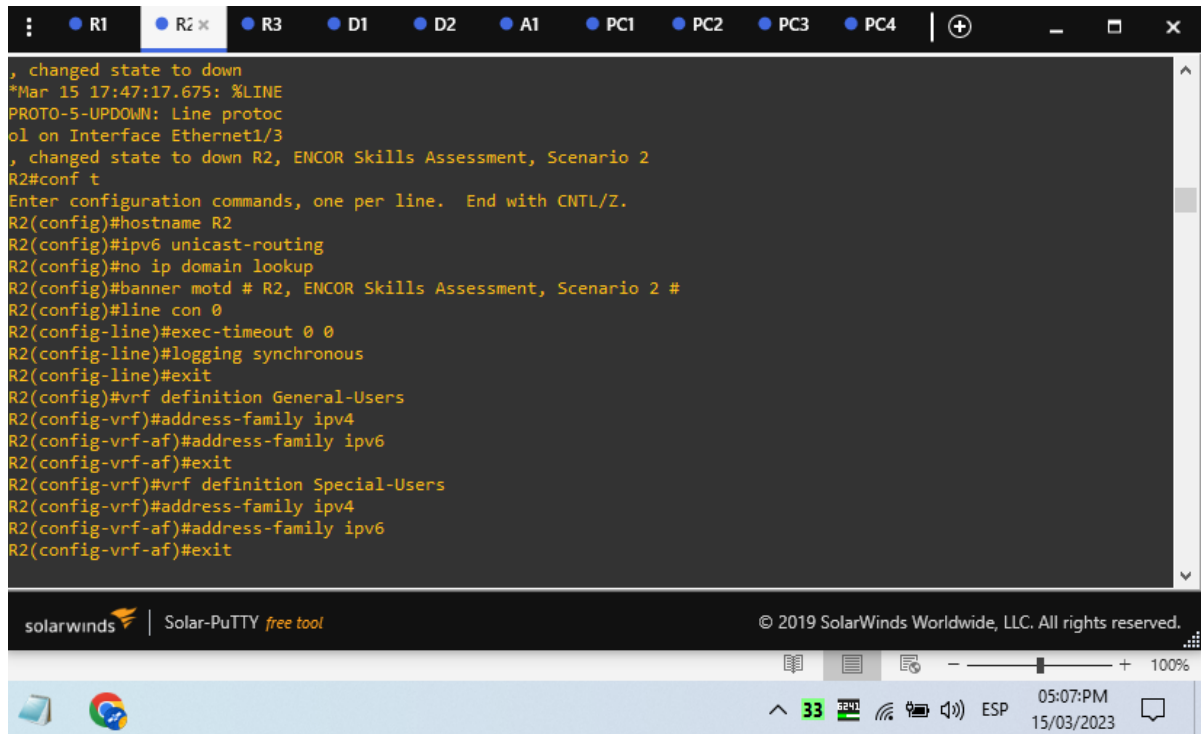
```
R1 x R2 R3 D1 D2 A1 PC1 PC2 PC3 PC4 | + - □ ×
3, changed state to down
*Mar 15 17:47:18.043: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Mar 15 17:47:18.475: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to a
dministratively down
*Mar 15 17:47:18.499: %LINK-5-CHANGED: Interface Ethernet1/1, changed state to a
dministratively down
*Mar 15 17:47:18.511: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to a
dministratively down
*Mar 15 17:47:18.519: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to a
dministratively down R1, ENCOR Skills Assessment, Scenario 2
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 2 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#XXTTEERRMpp
^
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

33 ESP 05:07:PM 15/03/2023

Fuente: Autoría propia

Figura 3. Aplicando código R2.



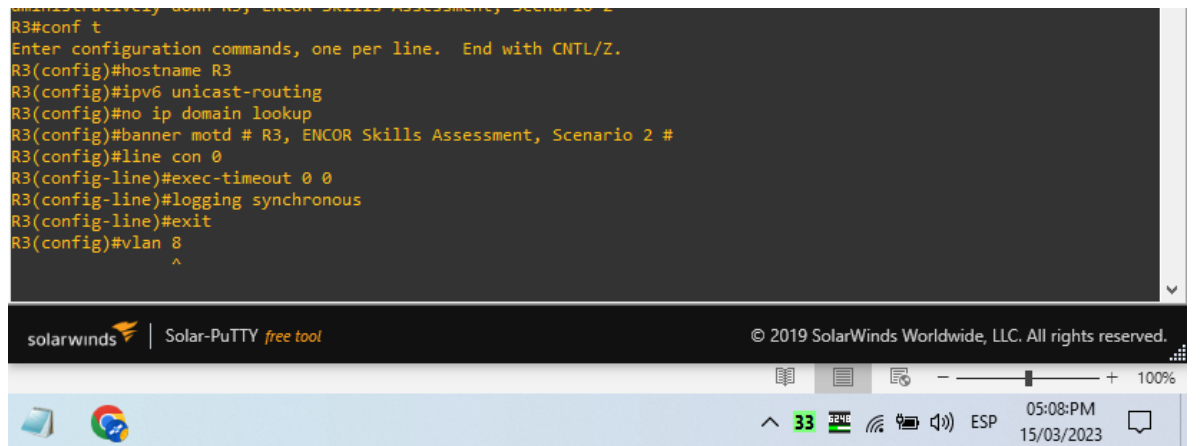
```

, changed state to down
*Mar 15 17:47:17.675: %LINE
PROTO-5-UPDOWN: Line protoc
ol on Interface Ethernet1/3
, changed state to down R2, ENCOR Skills Assessment, Scenario 2
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 2 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#vrf definition General-Users
R2(config-vrf)#address-family ipv4
R2(config-vrf-af)#address-family ipv6
R2(config-vrf-af)#exit
R2(config-vrf)#vrf definition Special-Users
R2(config-vrf)#address-family ipv4
R2(config-vrf-af)#address-family ipv6
R2(config-vrf-af)#exit

```

Fuente: Autoría propia

Figura 4. Aplicando código R3.



```

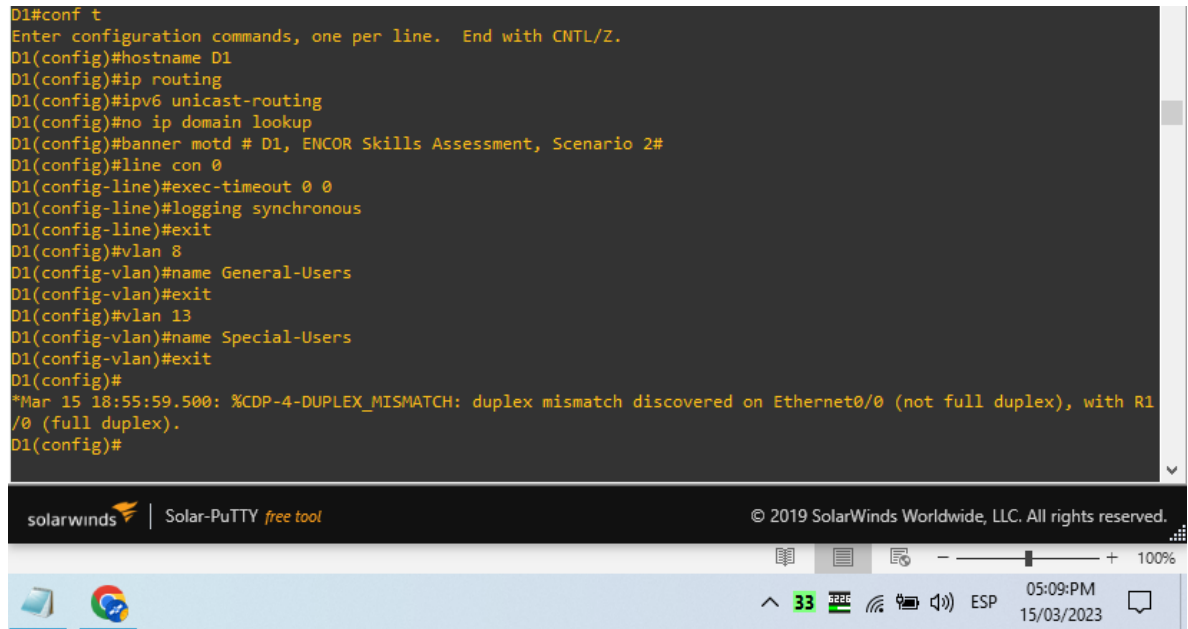
, changed state to down R3, ENCOR Skills Assessment, Scenario 2 #
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 2 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#vlan 8
^

```

Fuente: Autoría propia

Figura 5. Aplicando código D1.

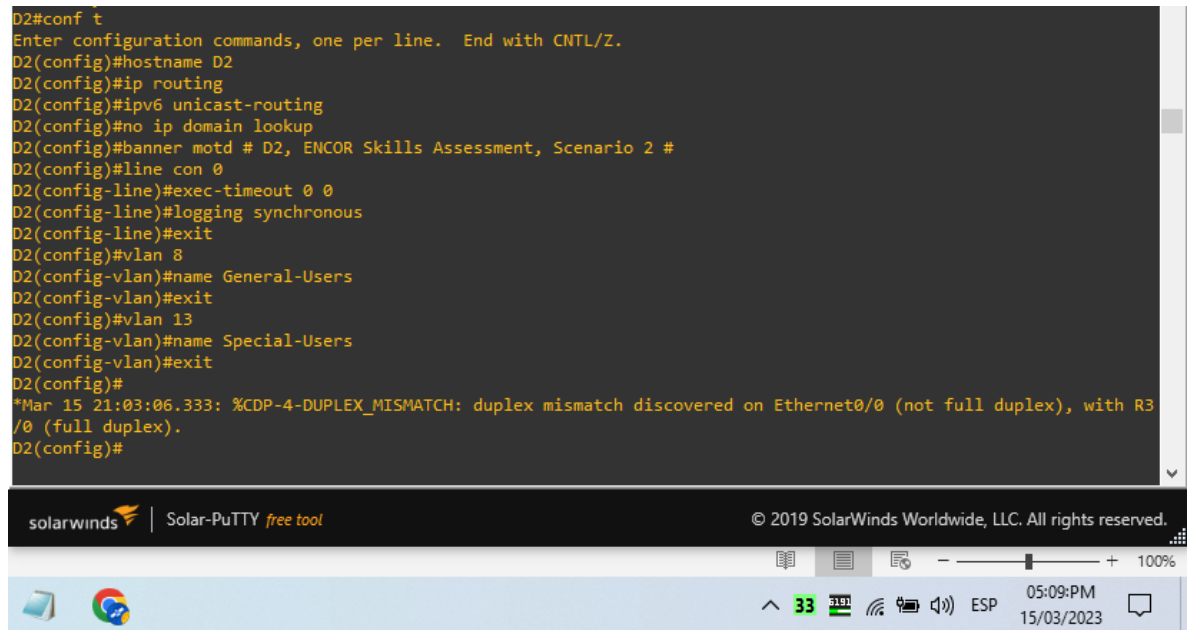
```
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 2#
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 8
D1(config-vlan)#name General-Users
D1(config-vlan)#exit
D1(config)#vlan 13
D1(config-vlan)#name Special-Users
D1(config-vlan)#exit
D1(config)#
*Mar 15 18:55:59.500: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R1
/0 (full duplex).
D1(config)#
```



Fuente: Autoría propia

Figura 6. Aplicando código D2.

```
D2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 2 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 8
D2(config-vlan)#name General-Users
D2(config-vlan)#exit
D2(config)#vlan 13
D2(config-vlan)#name Special-Users
D2(config-vlan)#exit
D2(config)#
*Mar 15 21:03:06.333: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R3
/0 (full duplex).
D2(config)#
```

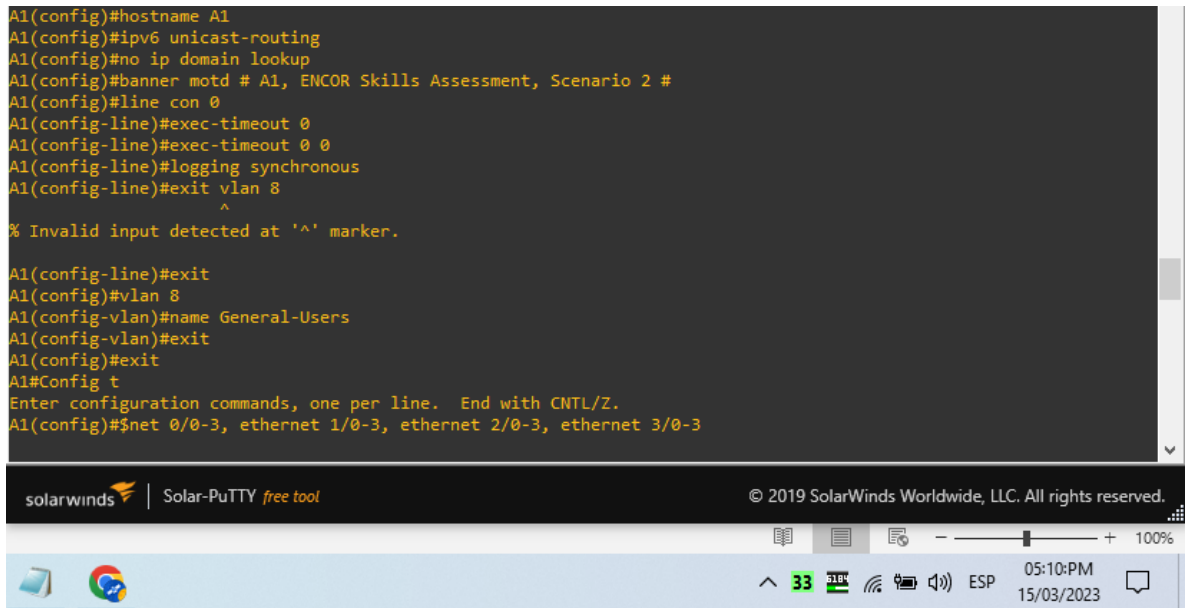


Fuente: Autoría propia

Figura 7. Aplicando código A1.

```
A1(config)#hostname A1
A1(config)#ipv6 unicast-routing
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 2 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit vlan 8
      ^
% Invalid input detected at '^' marker.

A1(config-line)#exit
A1(config)#vlan 8
A1(config-vlan)#name General-Users
A1(config-vlan)#exit
A1(config)#exit
A1#Config t
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#$net 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
```



Fuente: Autoría propia

### 1.3 Configurar los pc1, pc2, pc3 y pc4 de acuerdo con la tabla de direccionamiento.

Para configurar adecuadamente los dispositivos de red y permitir la conectividad entre ellos, se debe realizar la configuración de cada PC de acuerdo con la tabla de direccionamiento proporcionada.

En el caso de PC1, se establece la dirección IP como 10.0.113.97 y la máscara de subred como 255.255.255.0. Se configura también la dirección IP del gateway predeterminado como 10.0.113.1 para permitir la conexión con otros dispositivos de la red. Además, se configura la dirección IPv6 como 2001:DB8:ACAD:113::50 y se especifica la máscara de subred IPv6 como /64.

Es importante recordar que cada dispositivo debe ser configurado de acuerdo con la tabla de direccionamiento para asegurar la correcta conectividad en la red.

PC1 : ip 10.0.113.97 10.0.113.1

PC1 : ip 2001:DB8:ACAD:113::50/64

PC2 : ip 10.0.213.97 10.0.213.1

PC2 : ip 2001:DB8:ACAD:213::50/64

PC3 : ip 10.0.108.97 10.0.108.1

PC3 : ip 2001:DB8:ACAD:108::50/64

PC4 : ip 10.0.208.97 10.0.208.1

PC4 : ip 2001:DB8:ACAD:208::50/64

Los cuatro equipos (PC1, PC2, PC3 y PC4) tienen asignadas dos direcciones IP cada uno: una dirección IPv4 y una dirección IPv6.

Para la dirección IPv4, se utiliza el esquema de direccionamiento privado de clase A, con la dirección base 10.0.0.0 y una máscara de subred de 255.255.255.0, que permite hasta 254 direcciones IP por subred. A cada PC se le asigna una dirección IP única dentro de su subred, donde el último octeto (97) es el número de host.

Para la dirección IPv6, se utiliza el prefijo global unicast 2001:DB8:ACAD, que es un prefijo reservado para fines de documentación y ejemplos. Los siguientes dos octetos (113, 213, 108, 208) se utilizan para identificar la subred a la que pertenece cada PC. El último octeto (::50) es la dirección de host única para cada PC. La longitud de la máscara de subred se especifica como /64, lo que significa que los primeros 64 bits de la dirección son el prefijo de red y los últimos 64 bits son el identificador de interfaz del host.

Figura 8. Configuración PC1.

```
PC1> ip 10.0.113.97/24 10.0.113.1
Checking for duplicate address...
PC1 : 10.0.113.97 255.255.255.0 gateway 10.0.113.1

PC1> 2001:db8:acad:113::50/64
Bad command: "2001:db8:acad:113::50/64". Use ? for help.

PC1> ip 2001:db8:acad:113::50/64
PC1 : 2001:db8:acad:113::50/64

PC1> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC1       10.0.113.97/24  10.0.113.1   00:50:79:66:68:00  20034  127.0.0.1:20035
          fe80::250:79ff:fe66:6800/64
          2001:db8:acad:113::50/64

PC1>
```

Fuente: Autoría propia

Figura 9. Configuración PC2.

```
PC2> ip 10.0.213.97/24
Checking for duplicate address...
PC2 : 10.0.213.97 255.255.255.0

PC2> ip 10.0.213.97/24 10.0.213.1
Checking for duplicate address...
PC2 : 10.0.213.97 255.255.255.0 gateway 10.0.213.1

PC2> ip 2001:db8:acad:213::50/64
PC1 : 2001:db8:acad:213::50/64

PC2> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC2       10.0.213.97/24  10.0.213.1   00:50:79:66:68:01  20036  127.0.0.1:20037
          fe80::250:79ff:fe66:6801/64
          2001:db8:acad:213::50/64

PC2> █
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

file 11:28:AM 15/03/2023

Fuente: Autoría propia

Figura 10. Configuración PC3.

```
PC3> ip 10.0.108.97/24 10.0.108.1
Checking for duplicate address...
PC3 : 10.0.108.97 255.255.255.0 gateway 10.0.108.1

PC3> ip 2001:db8:acad:208::50/64
PC1 : 2001:db8:acad:208::50/64

PC3> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC3       10.0.108.97/24  10.0.108.1   00:50:79:66:68:02  20038  127.0.0.1:20039
          fe80::250:79ff:fe66:6802/64
          2001:db8:acad:208::50/64

PC3> █
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

1 error 2 warnings 11:30:AM 15/03/2023

Fuente: Autoría propia

Figura 11. Configuración PC4.

```
PC4> ip 10.0.208.97/24 10.0.208.1
Checking for duplicate address...
PC4 : 10.0.208.97 255.255.255.0 gateway 10.0.208.1

PC4> ip 2001:db8:acad:208::50/64
PC1 : 2001:db8:acad:208::50/64

PC4> show

NAME      IP/MASK      GATEWAY      MAC              LPORT  RHOST:PORT
PC4      10.0.208.97/24  10.0.208.1   00:50:79:66:68:03 20032  127.0.0.1:20033
          fe80::250:79ff:fe66:6803/64
          2001:db8:acad:208::50/64

PC4> █
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

W P 33 11:32:AM 15/03/2023

Fuente: Autoría propia

#### 1.4 Configurar vrf y enrutamiento estatico.

Para configurar adecuadamente el R1, R2 y R3, se pueden seguir los siguientes pasos:

- Acceder al modo de configuración global utilizando el comando "config t".
- Crear una definición de VRF (Virtual Routing and Forwarding) llamada "Special-Users" para la VLAN 13 que se configuró anteriormente en el Switch D1. Esto se puede hacer mediante el comando "vrf definition Special-Users" y configurando las dos address-families de IPv4 e IPv6 utilizando el comando correspondiente para cada una.

- Crear una definición de VRF llamada "General-Users" para la VLAN 8. De manera similar, se debe crear primero la definición utilizando el comando "vrf definition General-Users" y luego configurar las dos address-families para IPv4 e IPv6.
- Salir del modo de configuración VRF utilizando el comando "exit".
- Guardar la configuración utilizando el comando "wr" para asegurarse de que los cambios se guarden y no se pierdan después de reiniciar el dispositivo.

R1

```
config t
```

```
vrf definition Special-Users
```

```
address-family ipv4
```

```
address-family ipv6
```

```
exit
```

```
vrf definition General-Users
```

```
address-family ipv4
```

```
address-family ipv6
```

```
exit
```

```
wr
```

Este código de configuración está creando dos VRF (Virtual Routing and Forwarding) en el router R1: "Special-Users" y "General-Users". Las VRF son como instancias virtuales de routing, que permiten que diferentes redes tengan sus propias tablas de routing separadas, lo que significa que pueden tener diferentes rutas, políticas de routing y topologías.

En este caso, se está creando una VRF para cada una de las redes VLAN creadas en los switches D2 y A1 (General-Users y Special-Users), lo que permitirá mantener estas redes separadas y con políticas de routing específicas.

Después de crear las VRF, se utiliza el comando "wr" para guardar la configuración en la memoria no volátil del router.

```
R2
config t
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
wr
```

Este código configura dos VRF (Virtual Routing and Forwarding) en el router R2: Special-Users y General-Users. Una VRF es una forma de separar las redes lógicas dentro de un router compartiendo un único conjunto de interfaces físicas. En este caso, cada VRF tendrá sus propias tablas de enrutamiento y políticas de seguridad, lo que permitirá una mayor seguridad y separación de tráfico entre los usuarios generales y los usuarios especiales. La sección "address-family" define el protocolo

de red utilizado por cada VRF, en este caso IPv4 e IPv6. Finalmente, el comando "wr" se utiliza para guardar la configuración en la memoria no volátil del router.

R3

config t

vrf definition Special-Users

address-family ipv4

address-family ipv6

exit

vrf definition General-Users

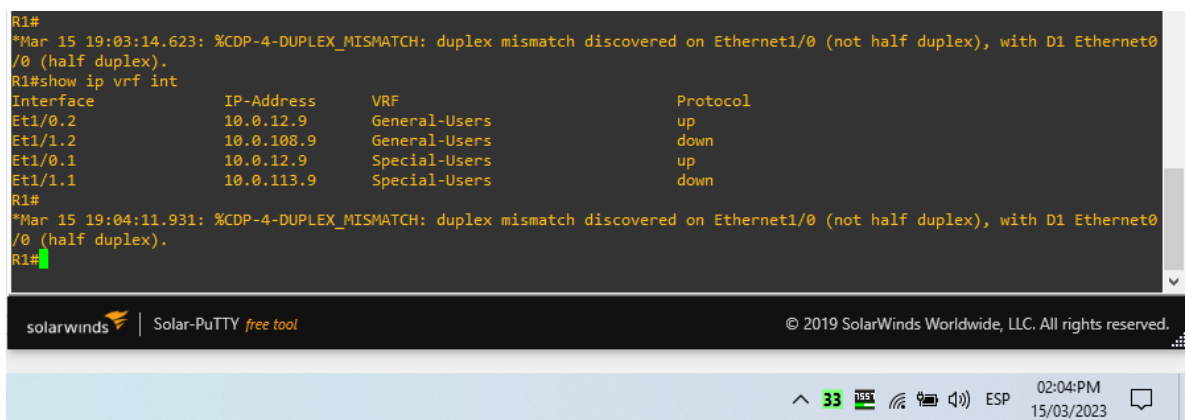
address-family ipv4

address-family ipv6

exit

wr

Figura 12. Configuración VRF en R1



```
R1#
*Mar 15 19:03:14.623: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with D1 Ethernet0/0 (half duplex).
R1#show ip vrf int
Interface          IP-Address      VRF              Protocol
Et1/0.2            10.0.12.9       General-Users     up
Et1/1.2            10.0.108.9      General-Users     down
Et1/0.1            10.0.12.9       Special-Users     up
Et1/1.1            10.0.113.9      Special-Users     down
R1#
*Mar 15 19:04:11.931: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with D1 Ethernet0/0 (half duplex).
R1#
```

Fuente: Autoría propia

Figura 13. Configuración VRF en R2.

```
R2#show ip vrf int
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.7       General-Users    up
Et1/1.2        10.0.23.7       General-Users    up
Et1/0.1        10.0.12.7       Special-Users    up
Et1/1.1        10.0.23.7       Special-Users    up
R2#
```

Fuente: Autoría propia

Figura 14. Configuración VRF en R3.

```
R3#show ip vrf int
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.23.4       General-Users    up
Et1/1.2        10.0.208.4      General-Users    up
Et1/0.1        10.0.23.4       Special-Users    up
Et1/1.1        10.0.213.4      Special-Users    up
R3#
*Mar 15 21:03:31.723: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with D2 Ethernet0
/0 (half duplex).
R3#
```

Fuente: Autoría propia

Para la configuración en el router R1, R2 y R3 se realiza en la interfaz E1/0 y E1/1 para crear subinterfases para las VLANs 8 y 13, que corresponden a los grupos de usuarios generales y especiales, respectivamente.

Para la subinterfaz E1/0.1, se establece la encapsulación dot1Q 13, se asigna la VRF Special-Users y se configuran las direcciones IP e IPv6 correspondientes. La subinterfaz E1/0.2 se configura de manera similar, con la encapsulación dot1Q 8, la VRF General-Users y las direcciones IP e IPv6 correspondientes.

En la interfaz E1/1, se configura la subinterfaz E1/1.1 con la encapsulación dot1Q 13, la VRF Special-Users y las direcciones IP e IPv6 correspondientes. La subinterfaz E1/1.2 se configura con la encapsulación dot1Q 8, la VRF General-Users y las direcciones IP e IPv6 correspondientes.

Todas las interfaces se habilitan con el comando "no shutdown".

```
R1
int E1/0
no shutdown
int E1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.12.9 255.255.255.0
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:acad:12::1/64
no shutdown
exit
int E1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.12.9 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
ipv6 address fe80::1:2 link-local
no shutdown
```

```
exit
int E1/1
no shutdown
int E1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.113.9 255.255.255.0
ipv6 address 2001:db8:acad:113::1/64
ipv6 address fe80::1:3 link-local
no shutdown
exit
int E1/1.2
encapsulation dot1Q 8
vrf forward General-Users
ip address 10.0.108.9 255.255.255.0
ipv6 address 2001:db8:acad:108::1/64
ipv6 address fe80::1:4 link-local
no shutdown
exit
```

Este código configura las interfaces del router R1 para permitir la comunicación entre las diferentes VLANs y VRFs en la topología de red. La configuración utiliza la tecnología de etiquetado de VLANs (dot1Q) para separar el tráfico en diferentes dominios de broadcast, y la tecnología de VRFs para crear diferentes instancias virtuales de red para mantener la separación lógica entre los usuarios generales y los usuarios especiales.

Además, se asignan direcciones IP y direcciones IPv6 a las interfaces para permitir la comunicación de los dispositivos conectados a las diferentes VLANs y VRFs. La configuración también habilita las interfaces con el comando "no shutdown" para activar la conexión en las interfaces correspondientes. En resumen, este código configura las interfaces del router R1 para permitir la comunicación de los dispositivos en diferentes redes y asegurar la separación lógica de diferentes tipos de usuarios.

```
R2
int E1/0
no shutdown
int E1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.12.7 255.255.255.0
ipv6 address 2001:db8:acad:12::2/64
ipv6 address fe80::2:1 link-local
no shutdown
exit
int E1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.12.7 255.255.255.0
ipv6 address 2001:db8:acad:12::2/64
ipv6 address fe80::2:2 link-local
```

```
no shutdown
exit
int E1/1
no shutdown
int E1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.23.7 255.255.255.0
ipv6 address 2001:db8:acad:23::2/64
ipv6 address fe80::2:3 link-local
no shutdown
exit

int E1/1.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.23.7 255.255.255.0
ipv6 address 2001:db8:acad:23::2/64
ipv6 address fe80::2:4 link-local
no shutdown
exit
```

Este código configura las interfaces del router R2 para que puedan comunicarse con el resto de la red.

Primero, se activan las interfaces E1/0 y E1/1 con el comando "no shutdown". Luego, se configuran las subinterfaces para permitir el etiquetado VLAN.

En la subinterface E1/0.1 se configura la VLAN 13 y se especifica que se usará el VRF "Special-Users". Se asigna una dirección IP IPv4 e IPv6 y se activa la interfaz con "no shutdown".

En la subinterface E1/0.2 se configura la VLAN 8 y se especifica que se usará el VRF "General-Users". Se asigna una dirección IP IPv4 e IPv6 y se activa la interfaz con "no shutdown".

En la subinterface E1/1.1 se configura la VLAN 13 y se especifica que se usará el VRF "Special-Users". Se asigna una dirección IP IPv4 e IPv6 y se activa la interfaz con "no shutdown".

Finalmente, en la subinterface E1/1.2 se configura la VLAN 8 y se especifica que se usará el VRF "General-Users". Se asigna una dirección IP IPv4 e IPv6 y se activa la interfaz con "no shutdown".

Con esta configuración, R2 podrá enrutar el tráfico entre los distintos VRF y VLAN de la red.

R3

```
int E1/0
```

```
no shutdown
```

```
int E1/0.1
```

```
encapsulation dot1Q 13
```

```
vrf forwarding Special-Users
ip address 10.0.23.4 255.255.255.0
ipv6 address fe80::3:1 link-local
ipv6 address 2001:db8:acad:23::3/64
no shutdown
exit
int E1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.23.4 255.255.255.0
ipv6 address 2001:db8:acad:23::3/64
ipv6 address fe80::3:2 link-local
no shutdown
exit
int E1/1
no shutdown
interface E1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.213.4 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:acad:213::1/64
no shutdown
exit
int E1/1.2
```

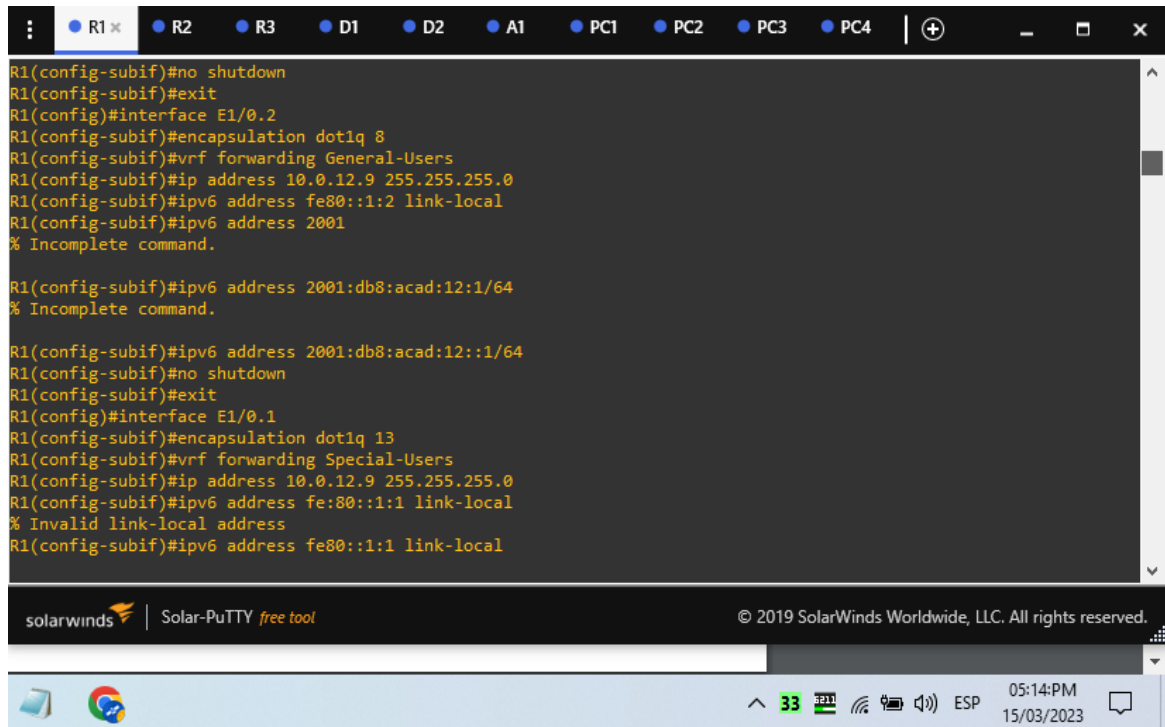
```
encapsulation dot1Q 8
vrf forward General-Users
ip address 10.0.208.4 255.255.255.0
ipv6 address fe80::3:4 link-local
ipv6 address 2001:db8:acad:208::1/64
no shutdown
exit
```

Este es un fragmento de configuración para el router R3. Aquí se están configurando cuatro interfaces:

- La interfaz E1/0, que se activa con el comando "no shutdown". Se configuran dos subinterfaces, E1/0.1 y E1/0.2, con la etiqueta VLAN 13 y 8 respectivamente. Cada subinterfaz tiene una dirección IPv4, una dirección IPv6 y una dirección de enlace local IPv6 configuradas. También se especifica la asignación de VRF para cada subinterfaz.
- La interfaz E1/1, que también se activa con el comando "no shutdown". Se configuran dos subinterfaces, E1/1.1 y E1/1.2, con la etiqueta VLAN 13 y 8 respectivamente. Cada subinterfaz tiene una dirección IPv4, una dirección IPv6 y una dirección de enlace local IPv6 configuradas. También se especifica la asignación de VRF para cada subinterfaz.

En resumen, esta configuración está estableciendo conexiones de red virtuales (VLAN) y asignando diferentes VRF a cada VLAN en el router R3.

Figura 15. Permite la comunicación entre las diferentes interfaces en R1.



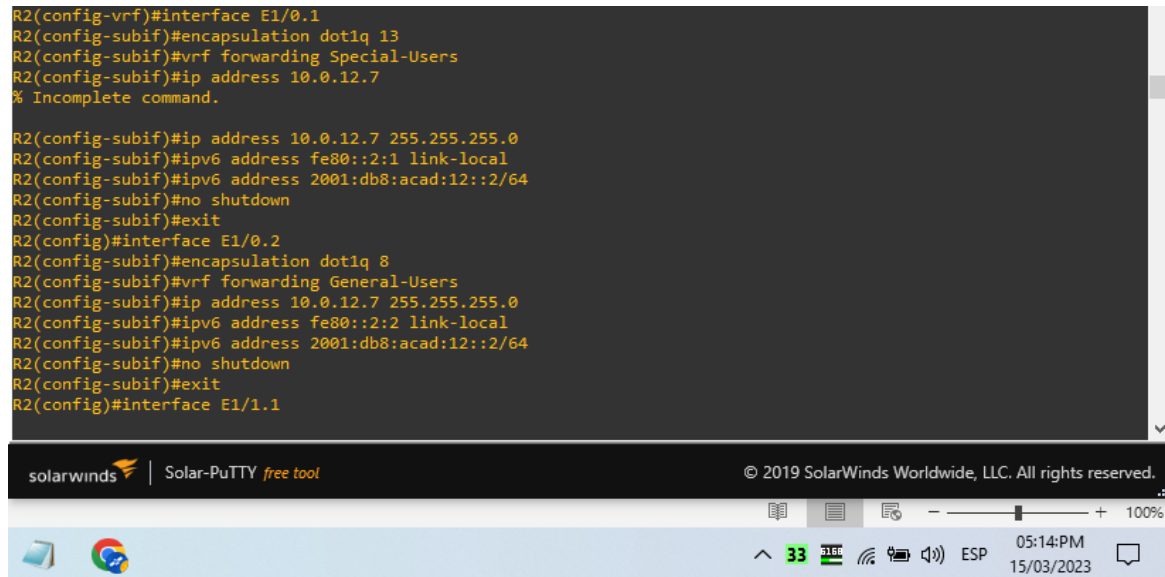
```
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface E1/0.2
R1(config-subif)#encapsulation dot1q 8
R1(config-subif)#vrf forwarding General-Users
R1(config-subif)#ip address 10.0.12.9 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:2 link-local
R1(config-subif)#ipv6 address 2001
% Incomplete command.

R1(config-subif)#ipv6 address 2001:db8:acad:12:1/64
% Incomplete command.

R1(config-subif)#ipv6 address 2001:db8:acad:12::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface E1/0.1
R1(config-subif)#encapsulation dot1q 13
R1(config-subif)#vrf forwarding Special-Users
R1(config-subif)#ip address 10.0.12.9 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:1 link-local
% Invalid link-local address
R1(config-subif)#ipv6 address fe80::1:1 link-local
```

Fuente: Autoría propia

Figura 16. Permite la comunicación entre las diferentes interfaces en R2.



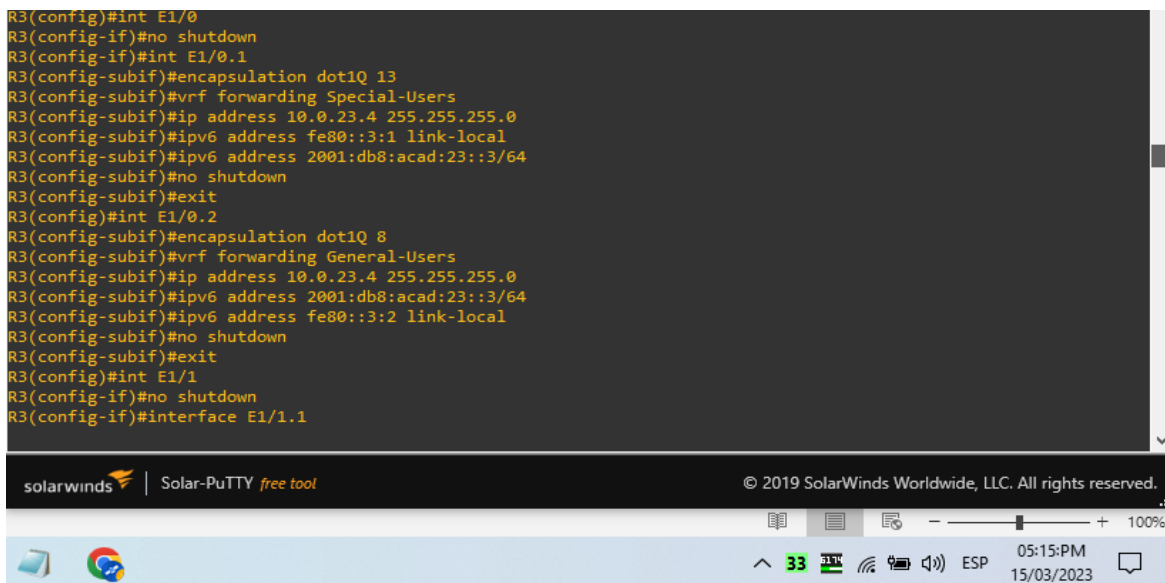
```
R2(config-vrf)#interface E1/0.1
R2(config-subif)#encapsulation dot1q 13
R2(config-subif)#vrf forwarding Special-Users
R2(config-subif)#ip address 10.0.12.7
% Incomplete command.

R2(config-subif)#ip address 10.0.12.7 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:1 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface E1/0.2
R2(config-subif)#encapsulation dot1q 8
R2(config-subif)#vrf forwarding General-Users
R2(config-subif)#ip address 10.0.12.7 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:2 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface E1/1.1
```

Fuente: Autoría propia

Figura 17. Permite la comunicación entre las diferentes interfaces en R3.

```
R3(config)#int E1/0
R3(config-if)#no shutdown
R3(config-if)#int E1/0.1
R3(config-subif)#encapsulation dot1Q 13
R3(config-subif)#vrf forwarding Special-Users
R3(config-subif)#ip address 10.0.23.4 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:1 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#int E1/0.2
R3(config-subif)#encapsulation dot1Q 8
R3(config-subif)#vrf forwarding General-Users
R3(config-subif)#ip address 10.0.23.4 255.255.255.0
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64
R3(config-subif)#ipv6 address fe80::3:2 link-local
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#int E1/1
R3(config-if)#no shutdown
R3(config-if)#interface E1/1.1
```



Fuente: Autoría propia

Se agregan rutas estáticas predeterminadas para las tres VRFs configuradas en el router R1, R2 y R3. La dirección IP del siguiente salto es 10.0.12.7 para las VRFs General-Users y Special-Users, mientras que la dirección IPv6 del siguiente salto es 2001:DB8:ACAD:12::2 para ambas VRFs.

R1

config t

```
ip route 0.0.0.0 0.0.0.0 10.0.12.7
```

```
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.7
```

```
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.7
```

```
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2
```

```
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2
```

exit

wr

Este código se utiliza para configurar las rutas predeterminadas (también conocidas como rutas por defecto) en R1 para que cualquier tráfico que no tenga una ruta específica hacia su destino se envíe a la dirección 10.0.12.7, que se supone que es el siguiente salto en la ruta hacia el destino final.

Además, este código configura las rutas predeterminadas para las dos VRFs (General-Users y Special-Users) que se han definido previamente en el router. Esto significa que el tráfico que ingresa en R1 en una interfaz asignada a una de estas VRFs y que no tiene una ruta específica hacia su destino, se envía a la dirección 10.0.12.7 dentro de la VRF correspondiente.

También se están configurando rutas predeterminadas IPv6 para ambas VRFs, lo que significa que cualquier tráfico IPv6 que ingrese en R1 en una interfaz asignada a una de estas VRFs y que no tenga una ruta específica hacia su destino, se enviará a la dirección IPv6 2001:DB8:ACAD:12::2 dentro de la VRF correspondiente.

R2

config t

```
ip route vrf General-User 10.0.113.0 255.255.255.0 10.0.12.9
```

```
ip route vrf General-User 10.0.208.0 255.255.255.0 10.0.23.4
```

```
ip route vrf Special-User 10.0.113.0 255.255.255.0 10.0.12.9
```

```
ip route vrf Special-User 10.0.213.0 255.255.255.0 10.0.23.4
```

```
ipv6 route vrf General-User 2001:db8:acad:108::/64 2001:db8:acad:12::1
```

```
ipv6 route vrf General-User 2001:db8:acad:208::/64 2001:db8:acad:23::3
```

```
ipv6 route vrf Special-User 2001:db8:acad:113::/64 2001:db8:acad:12::1
```

```
ipv6 route vrf Special-User 2001:db8:acad:213::/64 2001:db8:acad:23::3
```

```
exit
```

```
wr
```

Este código configura las rutas de IP y IPv6 en R2 para las VRF General-User y Special-User. Para la VRF General-User, se agrega una ruta hacia la red 10.0.113.0/24 a través del próximo salto 10.0.12.9 y otra ruta hacia la red 10.0.208.0/24 a través del próximo salto 10.0.23.4. Para la VRF Special-User, se agrega una ruta hacia la red 10.0.113.0/24 a través del próximo salto 10.0.12.9 y otra ruta hacia la red 10.0.213.0/24 a través del próximo salto 10.0.23.4.

Además, se agregan rutas IPv6 correspondientes para las VRF General-User y Special-User, especificando los prefijos de red y los próximos saltos correspondientes.

Por último, se ejecuta el comando "wr" para guardar la configuración en la memoria persistente del dispositivo.

```
R3
```

```
config t
```

```
ip route vrf General-User 0.0.0.0 0.0.0.0 10.0.23.7
```

```
ip route vrf Special-User 0.0.0.0 0.0.0.0 10.0.23.7
```

```
ipv6 route vrf General-User ::/0 2001:DB8:ACAD:23::3
```

```
ipv6 route vrf Special-User ::/0 2001:DB8:ACAD:23::3
```

```
exit
```

```
wr
```

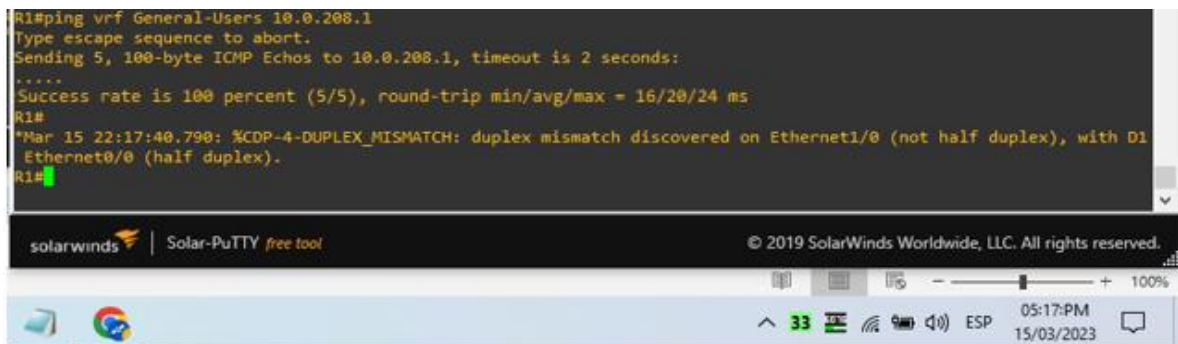
Este código está configurando las rutas por defecto en las VRF General-User y Special-User en el router R3. Estas rutas indican que cualquier tráfico destinado a

una red que no está incluida en la tabla de enrutamiento de la VRF será enviado a través del siguiente salto 10.0.23.7. Además, se está configurando una ruta por defecto IPv6 en ambas VRF para que el tráfico IPv6 que no pertenezca a ninguna red conocida se envíe a través del siguiente salto 2001:DB8:ACAD:23::3.

La configuración de estas rutas por defecto es importante para asegurar que cualquier tráfico que no pueda ser enrutado de forma directa se envíe correctamente. También ayuda a garantizar que el tráfico de diferentes VRF no se mezcle entre sí. La opción "wr" al final del código es un comando para guardar la configuración en la memoria no volátil del router para que sobreviva a un reinicio.

Y por último verificar las conexiones desde R1 con su conectividad con R3

Figura 18. Verificación conectividad de R1 y R3.



```
R1#ping vrf General-Users 10.0.208.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/24 ms
R1#
*Mar 15 22:17:40.798: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with D1
Ethernet0/0 (half duplex).
R1#
```

Fuente: Autoría propia

Otorgando una buena conexión R1 con R3, cumpliendo con el objetivo del trabajo.

## CONFIGURAR CAPA 2

On D1, D2, and A1, disable all interfaces

D1

en

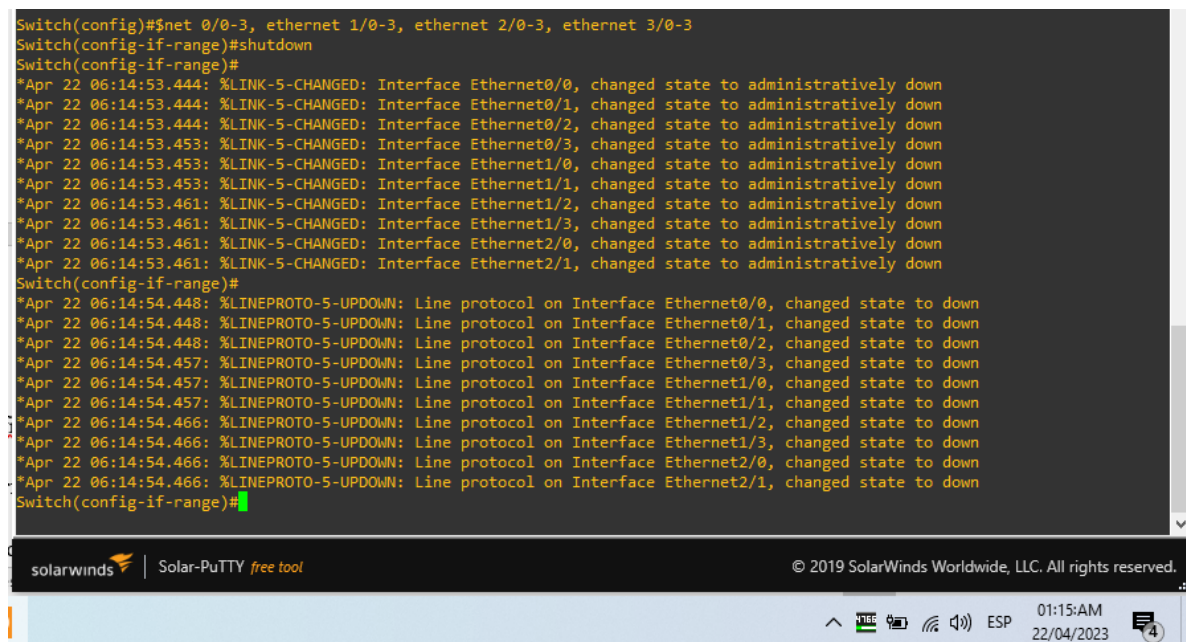
config t

```
interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
```

```
shutdown
```

Este código se utiliza para desactivar todos los puertos de los dispositivos D1, D2 y A1. Se hace esto para asegurarse de que no haya interferencias en la red durante la configuración de los otros dispositivos de la red. Desactivar los puertos garantiza que no haya ningún tipo de tráfico en la red y que la red se pueda configurar de manera segura y sin interrupciones.

Figura 19. Desactivación del puerto D1.



```
Switch(config)#$net 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#
*Apr 22 06:14:53.444: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Apr 22 06:14:53.444: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Apr 22 06:14:53.444: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*Apr 22 06:14:53.453: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
*Apr 22 06:14:53.453: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
*Apr 22 06:14:53.453: %LINK-5-CHANGED: Interface Ethernet1/1, changed state to administratively down
*Apr 22 06:14:53.461: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to administratively down
*Apr 22 06:14:53.461: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to administratively down
*Apr 22 06:14:53.461: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to administratively down
*Apr 22 06:14:53.461: %LINK-5-CHANGED: Interface Ethernet2/1, changed state to administratively down
Switch(config-if-range)#
*Apr 22 06:14:54.448: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Apr 22 06:14:54.448: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Apr 22 06:14:54.448: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
*Apr 22 06:14:54.457: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
*Apr 22 06:14:54.457: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
*Apr 22 06:14:54.457: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down
*Apr 22 06:14:54.466: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down
*Apr 22 06:14:54.466: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down
*Apr 22 06:14:54.466: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/0, changed state to down
*Apr 22 06:14:54.466: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/1, changed state to down
Switch(config-if-range)#
```

Fuente: Autoría propia

D2

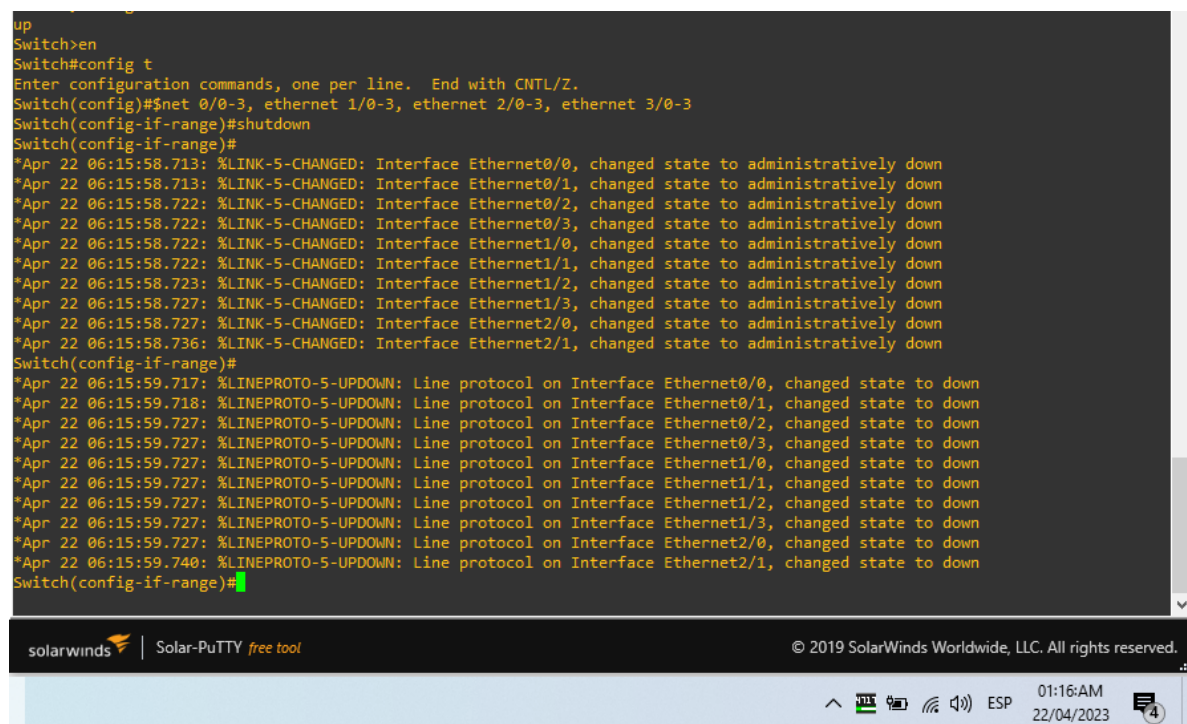
en

config t

```
interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
shutdown
```

Este código es utilizado para deshabilitar todas las interfaces en el dispositivo D2. Es posible que esto sea necesario durante el desarrollo o la configuración de una red, por ejemplo, para evitar que se produzcan errores o conflictos de red mientras se realizan cambios en la configuración. Después de que se hayan realizado los cambios necesarios, las interfaces pueden volver a habilitarse para permitir la conectividad de red.

Figura 20. Desactivación del puerto D2.



```
up
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#net 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#
*Apr 22 06:15:58.713: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Apr 22 06:15:58.713: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Apr 22 06:15:58.722: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*Apr 22 06:15:58.722: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
*Apr 22 06:15:58.722: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
*Apr 22 06:15:58.722: %LINK-5-CHANGED: Interface Ethernet1/1, changed state to administratively down
*Apr 22 06:15:58.723: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to administratively down
*Apr 22 06:15:58.727: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to administratively down
*Apr 22 06:15:58.727: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to administratively down
*Apr 22 06:15:58.736: %LINK-5-CHANGED: Interface Ethernet2/1, changed state to administratively down
Switch(config-if-range)#
*Apr 22 06:15:59.717: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Apr 22 06:15:59.718: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Apr 22 06:15:59.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
*Apr 22 06:15:59.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
*Apr 22 06:15:59.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
*Apr 22 06:15:59.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down
*Apr 22 06:15:59.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down
*Apr 22 06:15:59.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down
*Apr 22 06:15:59.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/0, changed state to down
*Apr 22 06:15:59.740: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/1, changed state to down
Switch(config-if-range)#
```

Fuente: Autoría propia

A1

en

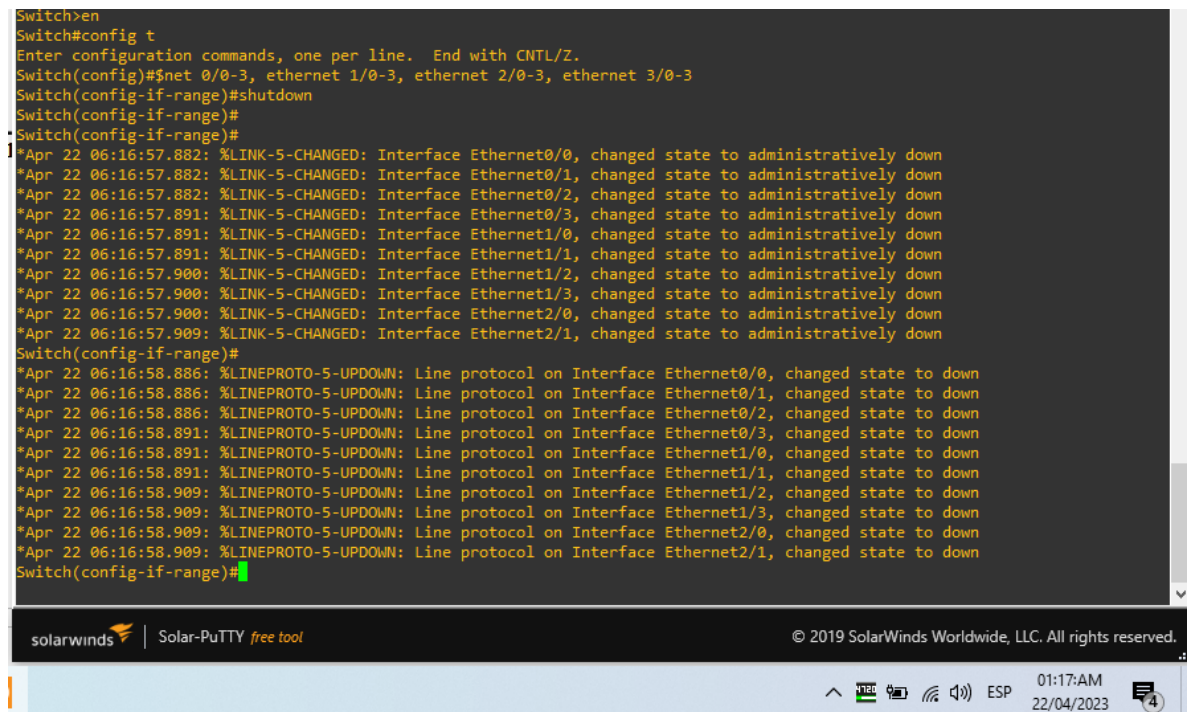
config t

interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3

shutdown

Este código es utilizado para deshabilitar todas las interfaces de los switches A1. Esto se puede hacer por varias razones, como por ejemplo para realizar una actualización de firmware o configuraciones en los switches sin que haya interrupciones en la red, o para realizar pruebas en la topología de red. La función de este código es detener el tráfico de datos a través de los switches A1.

Figura 21. Desactivación del puerto A1.



```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#$net 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#
Switch(config-if-range)#
*Apr 22 06:16:57.882: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Apr 22 06:16:57.882: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Apr 22 06:16:57.882: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*Apr 22 06:16:57.891: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
*Apr 22 06:16:57.891: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
*Apr 22 06:16:57.891: %LINK-5-CHANGED: Interface Ethernet1/1, changed state to administratively down
*Apr 22 06:16:57.900: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to administratively down
*Apr 22 06:16:57.900: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to administratively down
*Apr 22 06:16:57.900: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to administratively down
*Apr 22 06:16:57.909: %LINK-5-CHANGED: Interface Ethernet2/1, changed state to administratively down
Switch(config-if-range)#
*Apr 22 06:16:58.886: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Apr 22 06:16:58.886: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Apr 22 06:16:58.886: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
*Apr 22 06:16:58.891: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
*Apr 22 06:16:58.891: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
*Apr 22 06:16:58.891: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down
*Apr 22 06:16:58.909: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down
*Apr 22 06:16:58.909: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down
*Apr 22 06:16:58.909: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/0, changed state to down
*Apr 22 06:16:58.909: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/1, changed state to down
Switch(config-if-range)#
```

Fuente: Autoría propia

On D1 and D2, configure the trunk links to R1 and R3.

D1

```
inter ether 0/0
```

```
switchport trunk encapsulation dot1Q
```

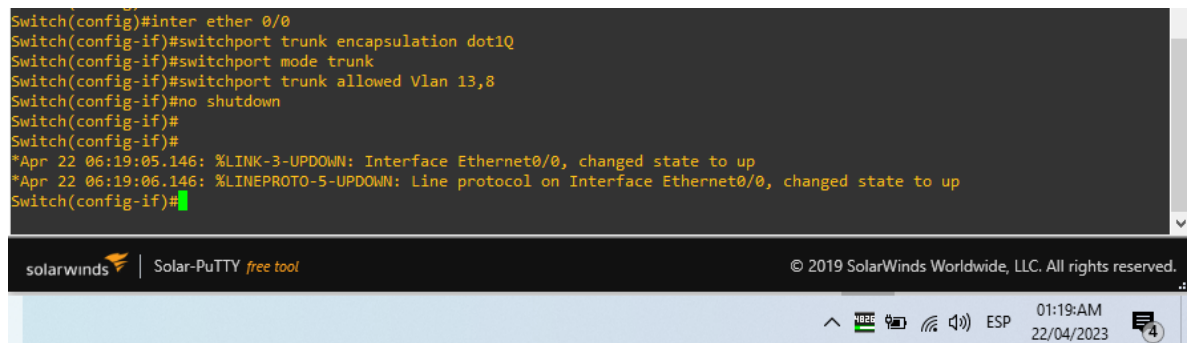
```
switchport mode trunk
```

```
switchport trunk allowed Vlan 13,8
```

```
no shutdown
```

La configuración anterior configura el enlace troncal en el puerto Ethernet 0/0 de D1 hacia R1 y R3. Se especifica el encapsulamiento dot1Q para el troncal y se permite el tráfico de las VLAN 13 y 8 a través del enlace. También se asegura de que el puerto no esté en estado de apagado.

Figura 22. Configuración troncal en D1.



```
Switch(config)#inter ether 0/0
Switch(config-if)#switchport trunk encapsulation dot1Q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed Vlan 13,8
Switch(config-if)#no shutdown
Switch(config-if)#
Switch(config-if)#
*Apr 22 06:19:05.146: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Apr 22 06:19:06.146: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Switch(config-if)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

01:19:AM 22/04/2023

Fuente: Autoría propia

D2

```
inter ether 0/0
```

```
switchport trunk encapsulation dot1Q
```

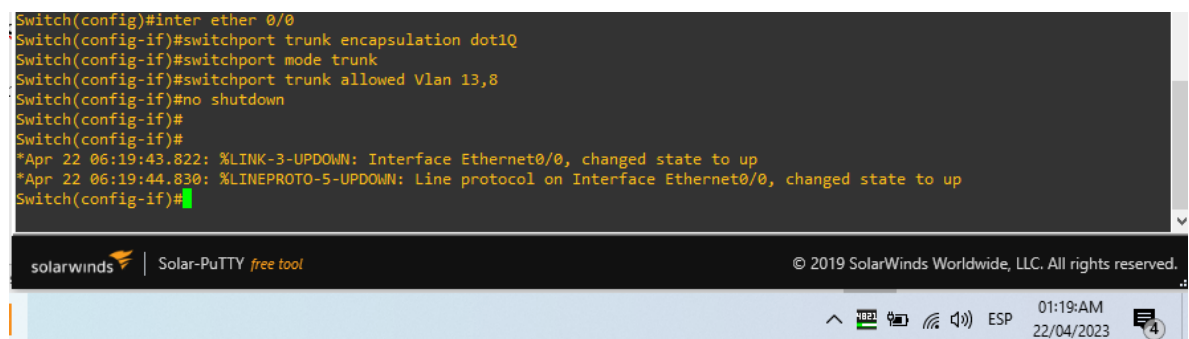
```
switchport mode trunk
```

```
switchport trunk allowed Vlan 13,8
```

```
no shutdown
```

ste código configura el enlace troncal en el puerto Ethernet 0/0 de D2 hacia R1 y R3. La línea "switchport trunk encapsulation dot1Q" establece la encapsulación del troncal como dot1Q, que es el estándar actual para enlaces troncales. La línea "switchport mode trunk" indica que el puerto se configura como troncal. La línea "switchport trunk allowed Vlan 13,8" especifica qué VLANs están permitidas en el enlace troncal, en este caso las VLAN 13 y 8. Finalmente, la línea "no shutdown" activa el puerto Ethernet 0/0.

Figura 23. Configuración troncal en D2.



```
Switch(config)#inter ether 0/0
Switch(config-if)#switchport trunk encapsulation dot1Q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed Vlan 13,8
Switch(config-if)#no shutdown
Switch(config-if)#
Switch(config-if)#
*Apr 22 06:19:43.822: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Apr 22 06:19:44.830: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Switch(config-if)#
```

Fuente: Autoría propia

On D1 and A1, configure the EtherChannel.

D1

```
inter range e1/0-1
```

```
switchport trunk encapsulation dot1Q
```

```
switchport mode trunk
```

```
channel-group 1 mode desirable
```

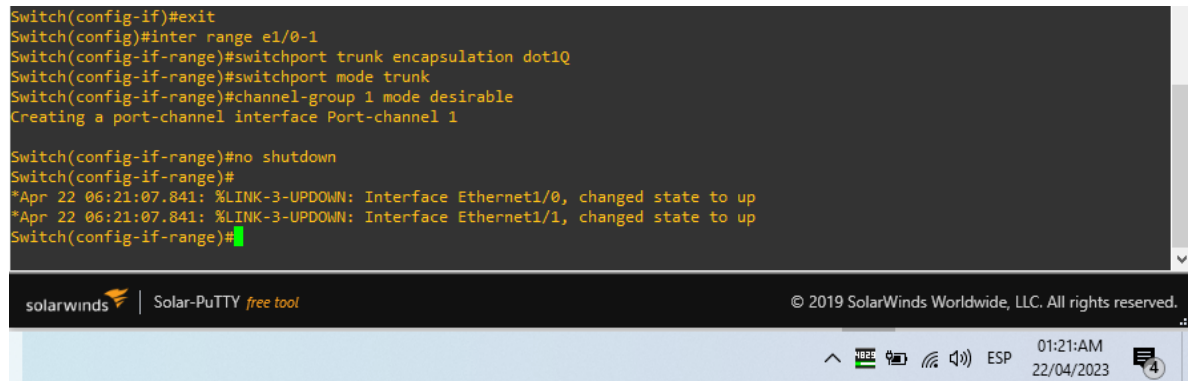
```
no shutdown
```

Este código está configurando las interfaces Ethernet 1/0 y 1/1 de D1 como trunk ports, utilizando el protocolo de encapsulación dot1Q. Además, se está agregando la interfaz al channel-group 1 en modo "desirable" para configurar un enlace troncal LACP. Finalmente, se activa la interfaz con el comando "no shutdown". Esto permitirá la comunicación entre D1 y R1 a través de un enlace troncal.

Figura 24. Enlace troncal D1.

```
Switch(config-if)#exit
Switch(config)#inter range e1/0-1
Switch(config-if-range)#switchport trunk encapsulation dot1Q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

Switch(config-if-range)#no shutdown
Switch(config-if-range)#
*Apr 22 06:21:07.841: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Apr 22 06:21:07.841: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
Switch(config-if-range)#
```



Fuente: Autoría propia

A1

inter range e1/0-1

switchport trunk encapsulation dot1Q

switchport mode trunk

channel-group 1 mode desirable

no shutdown

En este código, se están configurando los enlaces de troncales entre A1 y D1, y entre A1 y D2, para que utilicen el protocolo LACP para formar un grupo de enlaces EtherChannel.

Primero, se selecciona el rango de interfaces con el comando "interface range", y luego se configura cada una de ellas como troncal, especificando el encapsulamiento dot1Q y el modo troncal.

Luego, se configura el grupo de canales EtherChannel con el comando "channel-group", especificando el número del grupo y el modo deseado (en este caso, "desirable"). Finalmente, se habilita la interfaz con el comando "no shutdown".

Figura 25. Enlace troncal A1.

```
Switch(config-if-range)#exit
Switch(config)#inter range e1/0-1
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

Switch(config-if-range)#no shutdown
Switch(config-if-range)#
*Apr 22 06:21:40.616: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Apr 22 06:21:40.616: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
Switch(config-if-range)#
Switch(config-if-range)#
```

Fuente: Autoría propia

On D1, D2, and A1, configure access ports for PC1, PC2, PC3, and PC4.

D1

```
inter e0/0
```

```
switchport mode Access
```

```
switchport access vlan 13
```

```
spanning-tree portfast
```

```
no shutdown
```

```
exit
```

```
do wr
```

Este código de configuración se utiliza para configurar el puerto de acceso del switch D1 conectado al host de la VLAN 13.

Los comandos switchport mode access y switchport access vlan 13 configuran el puerto como un puerto de acceso y lo asignan a la VLAN 13, respectivamente.

El comando spanning-tree portfast activa el modo PortFast en el puerto, lo que permite que el puerto se ponga en estado de reenvío inmediatamente después de la conexión del host, en lugar de esperar el tiempo de convergencia del protocolo STP.

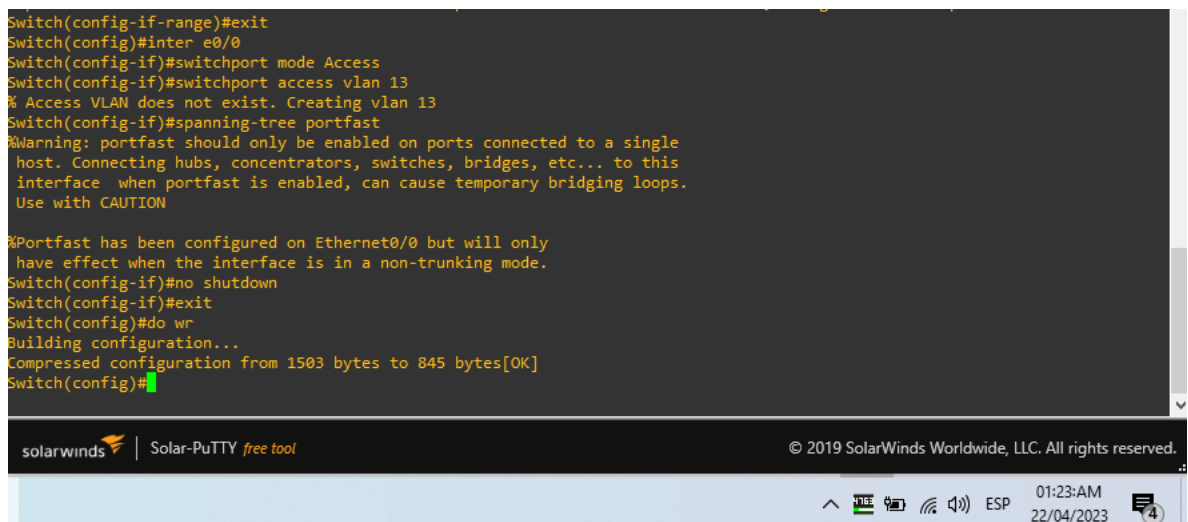
El comando no shutdown activa el puerto y lo pone en línea.

Por último, el comando do wr guarda la configuración en la memoria persistente del switch

Figura 26. Configuración puerto de acceso D1.

```
Switch(config-if-range)#exit
Switch(config)#inter e0/0
Switch(config-if)#switchport mode Access
Switch(config-if)#switchport access vlan 13
% Access VLAN does not exist. Creating vlan 13
Switch(config-if)#spanning-tree portfast
Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

Portfast has been configured on Ethernet0/0 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
Compressed configuration from 1503 bytes to 845 bytes[OK]
Switch(config)#
```



Fuente: Autoría propia

```
D2
inter e0/0
switchport mode Access
switchport access vlan 13
spanning-tree portfast
no shutdown
exit
inter e1/0
switchport mode Access
switchport access vlan 8
spanning-tree portfast
no shutdown
exit
do wr
```

Estos comandos configuran los puertos Ethernet 0/0 y Ethernet 1/0 de D2 como puertos de acceso, asignando a cada uno una VLAN diferente.

En el primer bloque de comandos, se configura el puerto Ethernet 0/0 para la VLAN 13, se habilita el portfast (para que el puerto pase directamente al estado forwarding sin pasar por el estado blocking del protocolo STP), se cambia el modo de switchport a access y finalmente se activa el puerto.

En el segundo bloque de comandos, se configura el puerto Ethernet 1/0 para la VLAN 8, se habilita el portfast, se cambia el modo de switchport a access y finalmente se activa el puerto.

Figura 27. Configuración puerto de acceso D2.

```
Switch(config-if)#exit
Switch(config)#inter e0/0
Switch(config-if)#switchport mode Access
Switch(config-if)#switchport access vlan 13
% Access VLAN does not exist. Creating vlan 13
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/0 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#inter e1/0
Switch(config-if)#switchport mode Access
Switch(config-if)#switchport access vlan 8
% Access VLAN does not exist. Creating vlan 8
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet1/0 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
Compressed configuration from 1380 bytes to 783 bytes[OK]
Switch(config)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 01:24:AM 22/04/2023

Fuente: Autoría propia

A1

inter e0/0

switchport mode Access

switchport access vlan 8

spanning-tree portfast

no shutdown

exit

Este conjunto de comandos configura el puerto Ethernet 0/0 en el switch A1 como un puerto de acceso. Se establece la VLAN de acceso en 8 y se habilita el Spanning

Tree PortFast para mejorar el tiempo de convergencia del protocolo STP. Finalmente, se habilita el puerto con el comando "no shutdown".

Figura 28. Configuración puerto de acceso A1.

```
Switch(config-if-range)#exit
Switch(config)#inter range e1/0-1
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

Switch(config-if-range)#no shutdown
Switch(config-if-range)#
*Apr 22 06:21:40.616: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Apr 22 06:21:40.616: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
Switch(config-if-range)#
Switch(config-if-range)#
*Apr 22 06:21:51.289: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to up
Switch(config-if-range)#
*Apr 22 06:21:52.395: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up
Switch(config-if-range)#exit
Switch(config)#inter e0/0
Switch(config-if)#switchport mode Access
Switch(config-if)#switchport access vlan 8
% Access VLAN does not exist. Creating vlan 8
Switch(config-if)#spanning-tree portfast
%%Warning: portfast should only be enabled on ports connected to a single
  host. Connecting hubs, concentrators, switches, bridges, etc... to this
  interface when portfast is enabled, can cause temporary bridging loops.
  Use with CAUTION

%Portfast has been configured on Ethernet0/0 but will only
  have effect when the interface is in a non-trunking mode.
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
*Apr 22 06:24:36.775: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Apr 22 06:24:37.780: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Switch(config)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

01:24:AM 22/04/2023

Fuente: Autoría propia

Verify PC to PC connectivity.

PC1-PC2

Figura 29. Conectividad PC1-PC2

```
VPCS> ping 10.0.208.97

10.0.208.97 icmp_seq=1 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=2 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=3 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=4 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=5 ttl=64 time=0.001 ms

VPCS>
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

01:29:AM 22/04/2023

Fuente: Autoría propia

### PC3-PC4

Figura 30. Conectividad PC3-PC4.

```
VPCS>
VPCS> ping 10.0.208.97

10.0.208.97 icmp_seq=1 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=2 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=3 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=4 ttl=64 time=0.001 ms
10.0.208.97 icmp_seq=5 ttl=64 time=0.001 ms

VPCS> ping 2001:db8:acad:208::50

2001:db8:acad:208::50 icmp_seq=1 ttl=64 time=0.001 ms
2001:db8:acad:208::50 icmp_seq=2 ttl=64 time=0.001 ms
2001:db8:acad:208::50 icmp_seq=3 ttl=64 time=0.001 ms
2001:db8:acad:208::50 icmp_seq=4 ttl=64 time=0.001 ms
2001:db8:acad:208::50 icmp_seq=5 ttl=64 time=0.001 ms
```

01:39:AM 22/04/2023

Fuente: Autoría propia

#### Parte 4. Configure Security

On all devices, secure privileged EXE mode

Configure an enable secret as follows:

Algorithm type: SCRYPT

Password: santiagorafael974.

R1, R2, R3, D1, D2, A1

en

config ter

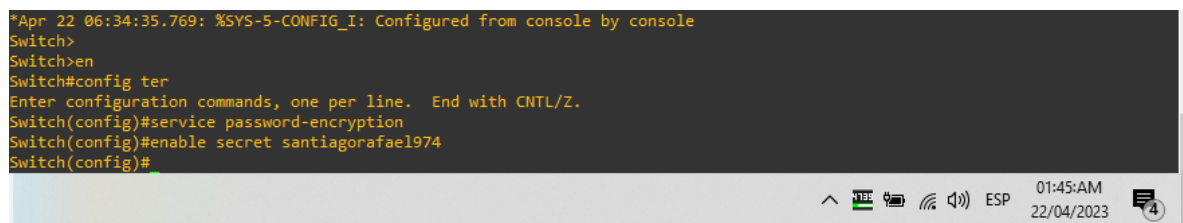
service password-encryption

enable secret santiagorafael974

Este conjunto de comandos habilita la encriptación de contraseñas de servicio y establece una contraseña encriptada para el modo privilegiado de cada dispositivo. La encriptación de contraseñas de servicio hace que sea más difícil para alguien que obtenga acceso no autorizado a los dispositivos obtener las contraseñas almacenadas en texto plano. La contraseña establecida para el modo privilegiado ayuda a proteger el acceso a los comandos de configuración y administración de cada dispositivo.

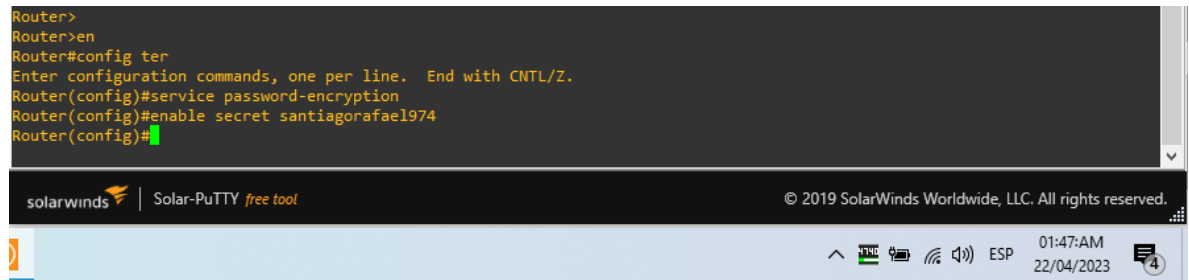
Figura 31. Encriptación en D1, D2, A1.

```
*Apr 22 06:34:35.769: %SYS-5-CONFIG_I: Configured from console by console
Switch>
Switch>en
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#service password-encryption
Switch(config)#enable secret santiagorafael974
Switch(config)#
```



Fuente: Autoría propia

Figura 32. Encriptación R1, R2, R3.



```
Router>
Router>en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#enable secret santiagorafael974
Router(config)#
```

The screenshot shows a terminal window with the SolarWinds Solar-PuTTY interface. The terminal displays the following commands and output: Router>, Router>en, Router#config ter, Enter configuration commands, one per line. End with CNTL/Z., Router(config)#service password-encryption, Router(config)#enable secret santiagorafael974, and Router(config)#. The terminal window includes a status bar at the bottom with the SolarWinds logo, the text 'Solar-PuTTY free tool', and a copyright notice '© 2019 SolarWinds Worldwide, LLC. All rights reserved.'. The system tray at the bottom right shows the time '01:47:AM' and date '22/04/2023'.

Fuente: Autoría propia

On all devices, create a local user account

Configure a local user:

Name: admin

Privilege level: 15

Algorithm type: SCRYPT

Password: santiagorafael974

R1, R2, R3, D1, D2, A1

en

config ter

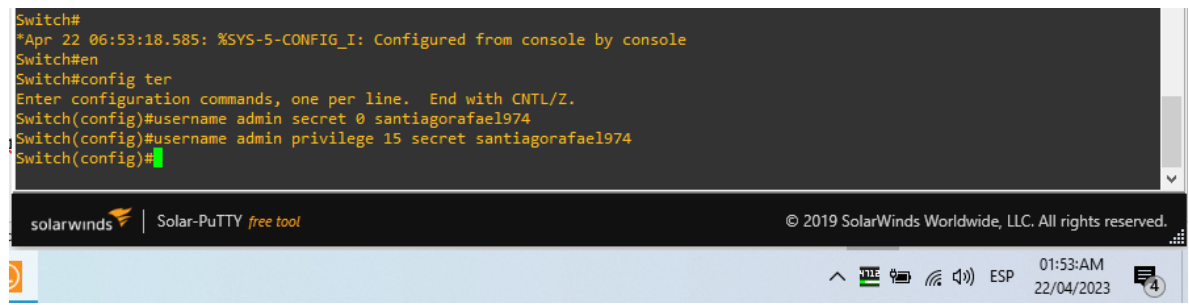
username admin secret 0 santiagorafael974

username admin privilege 15 secret santiagorafael974

Los comandos escritos son para configurar una contraseña segura para el acceso a la configuración de los dispositivos de red (R1, R2, R3, D1, D2 y A1) y crear un usuario con privilegios de administrador y su respectiva contraseña encriptada. Esto

ayuda a garantizar la seguridad de la red y evitar accesos no autorizados a la configuración de los dispositivos.

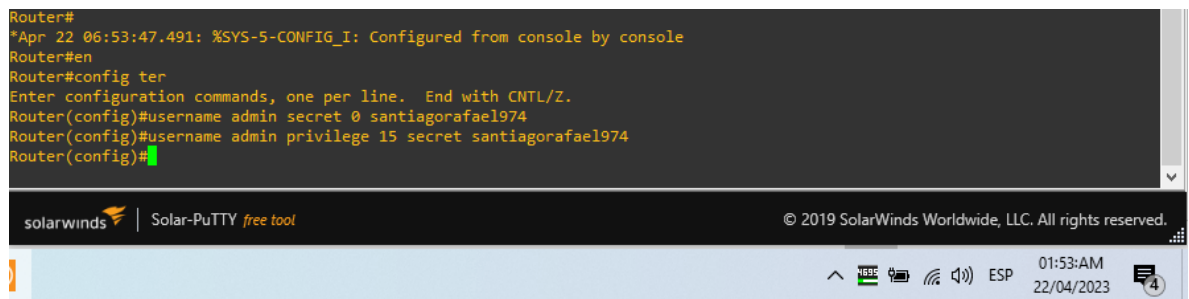
Figura 33. Configurar contraseña en D1, D2 y A1.



```
Switch#
*Apr 22 06:53:18.585: %SYS-5-CONFIG_I: Configured from console by console
Switch#en
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#username admin secret 0 santiagorafael974
Switch(config)#username admin privilege 15 secret santiagorafael974
Switch(config)#
```

Fuente: Autoría propia

Figura 34. Configurar contraseña en R1, R2 y R3.



```
Router#
*Apr 22 06:53:47.491: %SYS-5-CONFIG_I: Configured from console by console
Router#en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#username admin secret 0 santiagorafael974
Router(config)#username admin privilege 15 secret santiagorafael974
Router(config)#
```

Fuente: Autoría propia

On all devices, enable AAA and enable AAA authentication.

R1, R2, R3, D1, D2, A1

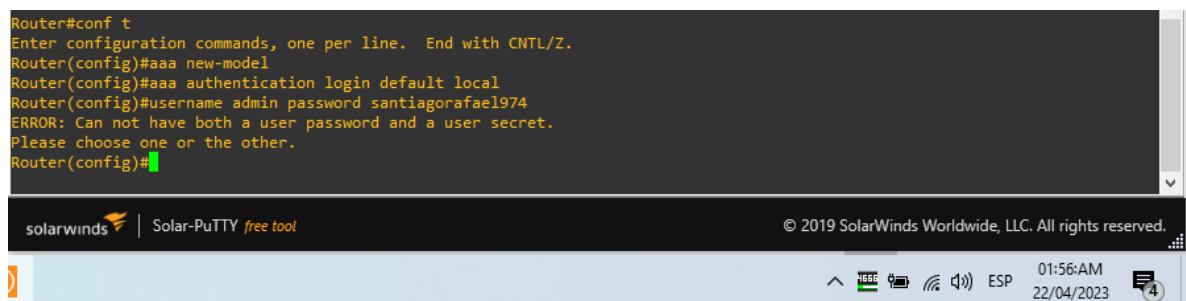
aaa new-model

aaa authentication login default local

username admin password santiagorafael974

- `aaa new-model`: Este comando habilita el modelo AAA (Autenticación, Autorización y Contabilidad) en el dispositivo. Es una práctica recomendada para una gestión de seguridad más efectiva.
- `aaa authentication login default local`: Con este comando se establece la autenticación predeterminada para el inicio de sesión a través del modo de consola o Telnet, utilizando la base de datos local del dispositivo. Esto significa que cualquier usuario que desee iniciar sesión en el dispositivo a través de la consola o Telnet deberá proporcionar las credenciales de autenticación locales configuradas en el dispositivo.
- `username admin password santiagorafael974`: Este comando crea un nuevo usuario con el nombre de 'admin' y le asigna una contraseña de 'santiagorafael974'. Este usuario solo se puede utilizar para iniciar sesión a través de Telnet o la interfaz de línea de comando (CLI) en el dispositivo.

Figura 35. Habilitación modelo AAA en D1, D2 y A1.

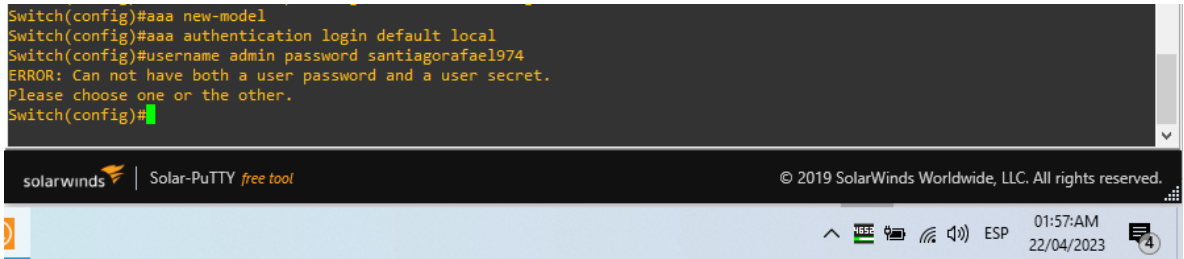


```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#aaa authentication login default local
Router(config)#username admin password santiagorafael974
ERROR: Can not have both a user password and a user secret.
Please choose one or the other.
Router(config)#
```

Fuente: Autoría propia

Figura 36. Habilitación modelo AAA en R1, R2 y R3.

```
Switch(config)#aaa new-model
Switch(config)#aaa authentication login default local
Switch(config)#username admin password santiagorafael1974
ERROR: Can not have both a user password and a user secret.
Please choose one or the other.
Switch(config)#
```



Fuente: Autoría propia

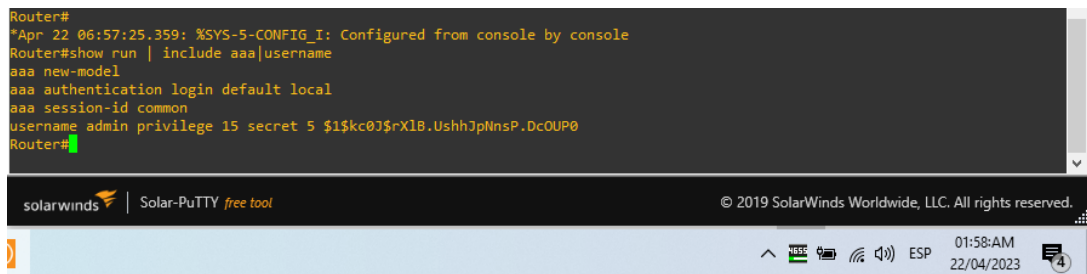
R1, R2, R3, D1, D2, A1

show run | include aaa|username

Este comando muestra la configuración actual de los dispositivos que incluye las líneas que contienen las palabras clave "aaa" o "username".

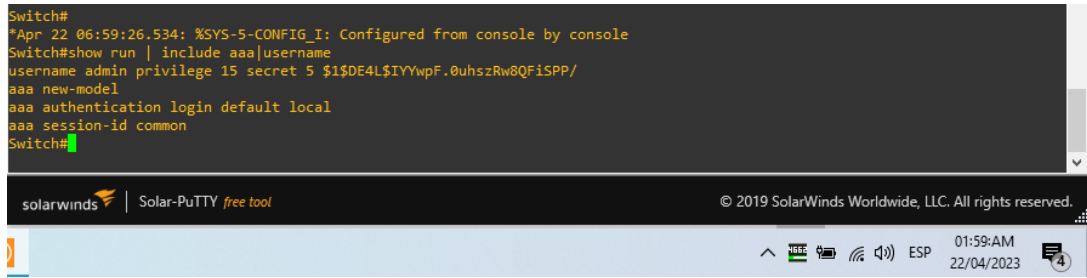
Figura 37. Configuración actual D1, D2 y A1.

```
Router#
*Apr 22 06:57:25.359: %SYS-5-CONFIG_I: Configured from console by console
Router#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$kc0J$rX1B.UshhJpNnsP.Dc0UP0
Router#
```



Fuente: Autoría propia

Figura 38. Configuración actual R1, R2 y R3.



```
Switch#
*Apr 22 06:59:26.534: %SYS-5-CONFIG_I: Configured from console by console
Switch#show run | include aaa|username
username admin privilege 15 secret 5 $1$DE4L$IYYwpF.0uhszRw8QF1SPP/
aaa new-model
aaa authentication login default local
aaa session-id common
Switch#
```

The screenshot shows a terminal window titled "Solar-PuTTY free tool" with a copyright notice for SolarWinds Worldwide, LLC. The terminal output displays the configuration for the 'aaa' service on a switch, including the creation of a local user 'admin' and the configuration of authentication and session parameters.

Fuente: Autoría propia

## CONCLUSIONES

El diseño de redes conmutadas utilizando STP y VLANs es una práctica esencial para garantizar una infraestructura de red jerárquica convergente que mejore la eficiencia y seguridad de la red. La utilización de estas herramientas permite evitar problemas de congestión y bucles de red, al mismo tiempo que se mejora la eficiencia y se garantiza la seguridad de la red. Al separar la red en grupos lógicos con VLANs, se pueden controlar de manera efectiva el flujo de tráfico y las políticas de seguridad, lo que mejora el rendimiento y la protección de la red.

El diseño de soluciones de red escalables es esencial para garantizar que las empresas puedan manejar grandes volúmenes de tráfico y mantener un alto rendimiento para los servicios críticos. La selección adecuada de protocolos de enrutamiento, la configuración básica y avanzada, la implementación de QoS y la configuración de redes WAN son elementos clave para lograr una solución de red escalable y eficiente. Una red escalable y eficiente no solo se asegura de que los usuarios puedan acceder a los servicios críticos de manera confiable, sino que también puede reducir el costo total de propiedad al minimizar la cantidad de hardware y software necesarios para soportar la infraestructura de red.

El diseño de redes empresariales eficientes y escalables es fundamental para garantizar el éxito de una organización y la satisfacción del usuario. Al utilizar herramientas como STP y VLANs, se puede crear una infraestructura de red jerárquica convergente que mejora la eficiencia y la seguridad de la red. Además, al diseñar soluciones de red escalables, se pueden manejar grandes volúmenes de tráfico y asegurar un alto rendimiento para los servicios críticos. La combinación de estos elementos esenciales permite diseñar soluciones de red empresariales que son capaces de enfrentar los desafíos de la actualidad y el futuro.

## BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Wireless Signals and Modulation. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Foundational Network Programmability Concepts. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Configure stp settings on a switch through the cli. (2022, 1 mayo). cisco. <https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5760-configure-stp-settings-on-a-switch-through-the-cli.html>