

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JAIRO HUMBERTO ZAMBRANO SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA DE TELECOMUNICACIONES
SAN JUAN DE PASTO
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JAIRO HUMBERTO ZAMBRANO SALAZAR

Diplomado de opción de grado presentado para optar el
título de INGENIERO DE TELECOMUNICACIONES

TUTOR:
MARITZA FARLEY MONDRAGON GUZMAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA DE TELECOMUNICACIONES
SAN JUAN DE PASTO
2023

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

San Juan de Pasto, 17 de abril de 2023

AGRADECIMIENTOS

En primer lugar, quiero agradecer a DIOS y a todas las personas que me han apoyado en mi formación académica llegando a obtener el título de INGENIERO EN TELECOMUNICACIONES, quiero agradecer a mi pareja Sandra Fajardo quien ha seguido de cerca este proceso apoyándome y no permitiendo que abandone mis sueños; a mi Padre Jairo Zambrano quien incondicionalmente siempre está pendiente de las metas que me propongo alcanzar; a mi Madre que ya no está presente en este mundo pero siento que nunca nos abandona y nos da la fuerza para continuar luchando; a mis hermanos que son una parte demasiado importante en mi vida; quiero agradecer a mis tutores y directores de curso quienes en este proceso compartieron con migo su conocimiento y me hicieron amar aún mas esta hermosa profesión.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTAS DE TABLAS.....	7
LISTA DE FIGURAS	8
GLOSARIO	10
RESUMEN.....	11
ABSTRACT.....	11
INTRODUCCIÓN	12
DESARROLLO	13
1. ESCENARIO 1	13
Parte 1:	13
Paso 1: se realiza la conexión o cableado de cada uno de los dispositivos para la interconexión total de la topología	13
Paso 2: Configure los ajustes básicos para cada dispositivo.....	13
Parte 2: configurar VRF y enrutamiento estático	23
2.1 En R1, R2, y R3, configure VRF-Lite VRFs Como se muestra en el diagrama de topología.....	23
2.2 En R1, R2 y R3 configure interfaces ipv4 y ipv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.....	24
2.3 En R1 y R3, configuran rutas estáticas predeterminadas que apuntan a R2. 28	
2.4 Verifique la conectividad en cada VRF.	32
2. Escenario 2	34
Parte 3. Configurar Capa 2	34
3.1 Deshabilitar todas las interfaces en D1, D2 y A1	34
3.2 Configurar los enlaces troncales.....	34
3.3 Configurar el EtherChannel en D1 y A1	36
3.4 Configurar puertos de acceso para PC1, PC2, PC3 y PC4 en D1, D2 y A1.....	37
3.5 Verificación de la conectividad de PC a PC	38

Parte 4. Configure seguridad	39
4.1 Configuración de seguridad privilegiada en modo EXE en todos los dispositivos	39
4.2 Crear una cuenta de usuario local en todos los dispositivos.....	40
4.3 Habilite la autenticación AAA en todos los dispositivos	40
CONCLUSIONES	42
BIBLIOGRAFÍA.....	43

LISTAS DE TABLAS

Tabla 1. Tabla de direccionamiento

14

LISTA DE FIGURAS

Figura 1. Topología de la red	13
Figura 2. Comando guardar del Router 1.	18
Figura 3. Comando Guardar del Router 2	19
Figura 4. Comando Guardar del Router 3	19
Figura 5. Comando guardar del Switch D1.	20
Figura 6. Comando guardar del Switch D2.	20
Figura 7. Comando guardar del Switch A1.	20
Figura 8. Configuración ip PC1	21
Figura 9. Configuración ip PC2	22
Figura 10. Configuración ip PC3	22
Figura 11. Configuración ip PC4	22
Figura 12. Comando “Show ip vrf interface” en Router 1.	25
Figura 13. Comando “Show ip vrf interface” en Router 2.	27
Figura 14. Comando “Show ip vrf interface” en Router 3.	28
Figura 15. Tabla de enrutamiento Router 1	29
Figura 16. Tabla de enrutamiento Router 2	30
Figura 17. Tabla de enrutamiento Router 3	32
Figura 18. Conectividad entre R1 y R3 por VRF General-users ipv4	32
Figura 19. Conectividad entre R1 y R3 por VRF General-users ipv6	33
Figura 20. Conectividad entre R1 y R3 por VRF Special-users ipv4	33
Figura 21. Conectividad entre R1 y R3 por VRF Special-users ipv6	33
Figura 22. Interface Troncal Ethernet 0/2	35
Figura 23. Interface Troncal Ethernet 0/3	35
Figura 24. Interface port-channel 1	36
Figura 25. Interface port-channel 1	37
Figura 26. ping exitoso entre PC1 y PC2 con ipv4 e ipv6	38
Figura 27. ping exitoso entre PC3 y PC4 con ipv4 e ipv6	39
Figura 28. Verificación de seguridad en R1	40

Figura 29. Verificación de seguridad en R2	40
Figura 30. Verificación de seguridad en R3	41
Figura 31. Verificación de seguridad en D1	41
Figura 32. Verificación de seguridad en D2	41
Figura 33. Verificación de seguridad en A1	41

GLOSARIO

LINK AGREGATION: Nos permite combinar dos o más enlaces físicos (ya sea Fast-Ethernet, Gigabit Ethernet e incluso 10Gigabit) de manera que podamos ampliar el ancho de banda de la conexión.

ROUTER: Un rúter, enrutador o encaminador es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP.

SUB-INTERFAZ: Se utilizan en el enrutamiento no tradicional. Sobre una misma interfaz física se realizan varias subinterfaces virtuales sobre enlaces troncales. Cada subinterfaz se configura con su dirección IP, máscara de subred y VLAN

SWITCH: Dispositivo de interconexión que sirve para conectar todos los equipos en una red; incluidos los computadores, las consolas, las impresoras y los servidores.

TABLA DE ENRUTAMIENTO: En esta tabla es donde almacenamos las rutas a los diferentes dispositivos conectados a una red informática

VLAN: (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

VRF: El Enrutamiento Virtual y Reenvío (VRF) es una tecnología incluida en routers de red IP (Internet Protocol) que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar al simultáneamente.

RESUMEN

En el siguiente informe presentamos un proyecto para el diplomado CISCO CCNP en el que aplicamos nuestros conocimientos en electrónica y redes, con los protocolos de enrutamiento aplicamos las habilidades prácticas adquiridas durante los cursos CCNA de CISCO, en una topología de red realizada en GNS3 configuramos varios routers y switches en los que debemos realizar una conmutación para transmitir información entre los usuarios de la red creando VLANs, VRFs (Tablas de enrutamiento virtuales por cada VLAN), rutas estáticas, encapsulamiento de datos, configuración de capa 2 como rutas troncales, puertos de acceso y seguridad entre otros.

En el presente informe encontraremos los comandos utilizados para realizar la configuración en cada equipo de forma detallada de tal manera que cada comando utilizado está debidamente explicado.

Palabras clave: CISCO, CCNP, conmutación, enrutamiento, redes, electrónica

ABSTRACT

In the following report we present a project for the CISCO CCNP diploma in which we apply our knowledge in electronics and networks, with the routing protocols we apply the practical skills acquired during the CISCO CCNA courses, in a network topology made in GNS3 we configure several routers and switches in which we must perform a switch to transmit information between network users creating VLANs, VRFs (Virtual Routing Tables for each VLAN), static routes, data encapsulation, layer 2 configuration such as trunk routes, ports of access and security among others.

In this report we will find the commands used to configure each computer in detail in such a way that each command used is properly explained.

Keywords: CISCO CCNP routing, switching, networking, electronics

INTRODUCCIÓN

Los cursos de certificación CCNA (Cisco Certified Network Associate) son una parte importante para el campo de las redes y telecomunicaciones. Estos cursos proporcionan a los profesionales un conocimiento práctico y exhaustivo de las tecnologías de red, como el enrutamiento y la conmutación, los protocolos de red y los servicios de seguridad.

Presentamos el desarrollo de un escenario propuesto el cual nos permite desarrollar y practicar los conocimientos adquiridos durante la carrera, teniendo que desarrollar una topología en la que se pide configurar en los equipos que la conforman unas rutas para transportar datos de un dispositivo a otro implementando algunos protocolos como VRFs, VLANs, enlaces troncales y seguridad a los mismos.

El escenario propuesto se compone de tres routers, tres switches y cuatro PCs en los que debemos configurar diferentes protocolos para dar solución a lo que la guía solicita. En los routers crearemos dos VRFs: Special-users y General-users, también debemos crear en cada router subinterfaces a las que les asignaremos IPv4 e IPv6, cada VRF tendrá una VLAN asignada, entre dos switches crearemos un link aggregation el cual nos permite combinar dos enlaces físicos ethernet en un único enlace lógico para ampliar el ancho de banda en la conexión. En los routers hemos creado unas rutas estáticas por cada VLAN de capa 2, las cuales nos permiten aumentar la seguridad y tener el control de las rutas por las que se transmiten los datos entre los PCs de la topología.

En los switches debemos habilitar las interfaces y crear enlaces troncales para conectarnos a los routers y permitir el paso del tráfico de las VLANs configuradas, también tenemos interfaces en modo acceso. En los dispositivos configuramos contraseñas para aumentar la seguridad de estos mismos.

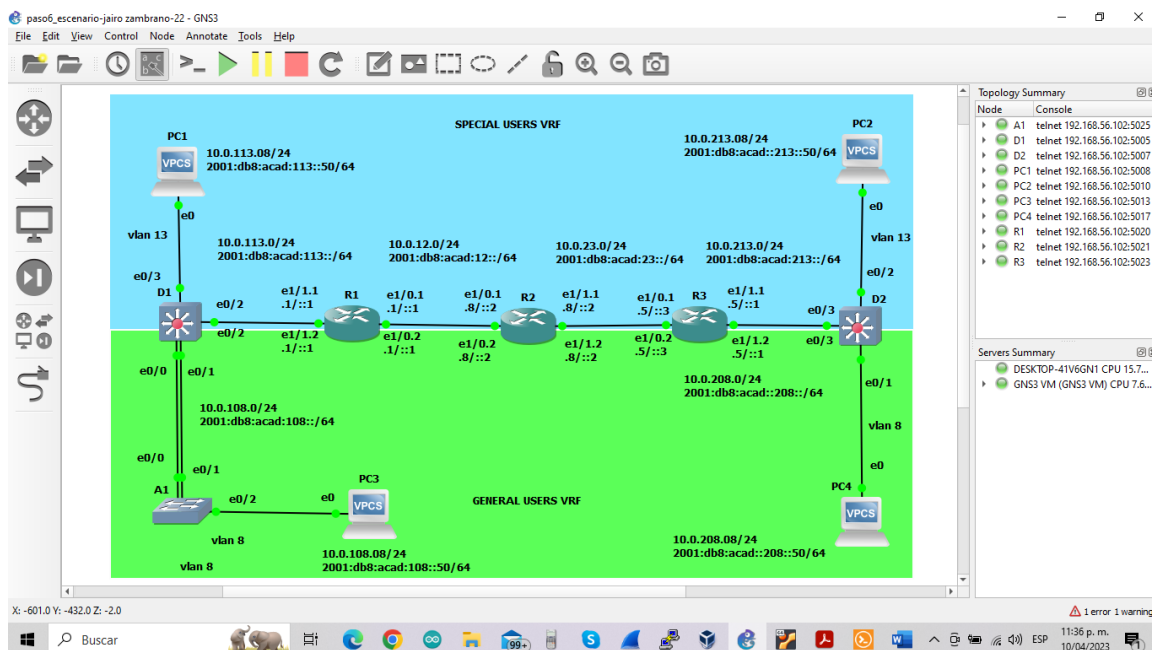
DESARROLLO

1. ESCENARIO 1

Parte 1: Para el desarrollo del escenario o topología de red a implementar, primero se construyó el diseño de red, organizo y se realizó las configuraciones básicas de los dispositivos, además de configurar el direccionamiento IP y encender cada una de las interfaces de los equipos. Posteriormente se realizó la conexión o cableado de cada uno de los dispositivos para la interconexión total de la topología.

Paso 1: se realiza la conexión o cableado de cada uno de los dispositivos para la interconexión total de la topología

Figura 1. Topología de la red



Fuente: Autoría propia

Paso 2: Configure los ajustes básicos para cada dispositivo

- a. En este paso, se ingresa a los dispositivos y se realizó la configuración básica inicial del dispositivo donde se configuro elementos como la asignación del direccionamiento IPV4 e IPV6, teniendo claro de acuerdo a los lineamientos del trabajo en el espacio que corresponde a la letra X se debe reemplazar por el

digito de mi cedula, que en mi caso es 085 la X corresponde al cero y en mi caso la IP 10.0.113.0 no la puedo utilizar en E1/1.1 por que esta es la IP de red y así que se optó por utilizar la dirección IP 10.0.113.1 que corresponde a mi asignación de IPs como se puede observar a continuación:

X=1
Y=8
Z=5

De esta forma, se construyo la siguiente tabla de direccionamiento IP utilizada en la implementación de la topología del escenario propuesto.

Tabla 1. Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.8/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.8/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.8/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.8/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.5/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.5/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.5/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.5/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.08/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.08/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.08/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.08/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Autoría propia

Router R1

Comandos ejecutados

Configure terminal Acceder a modo configuración global
Ipv6 unicast-routing Habilitar enrutamiento ipv6
No Ip domain lookup.....Desactiva la traducción de nombres a dirección del dispositivo
Banner motd # R1, ENCOR Skills Assessment, Scenario 2#..... Configurar un texto como mensaje del día
Line con 0.....Ingresar al modo de configuración de línea de la consola.
Exec-timeout 0 0.....Establece el tiempo de espera inactivo de la sesión remota

Logging synchronous..... Evita que los mensajes inesperados que aparecen en pantalla nos desplacen los comandos que estamos escribiendo en el momento.
Exit..... Salir del modo configuración global
Configure terminal..... Acceder a modo configuración global
Ipv6 unicast-routing Habilitar enrutamiento ipv6
No Ip domain lookup..... Desactiva la traducción de nombres a dirección del dispositivo

Router R2

Comandos ejecutados

Configure terminal Acceder a modo configuración global
Ipv6 unicast-routing Habilitar enrutamiento ipv6
No ip domain lookup.....desactiva la traducción de nombres a dirección del dispositivo
Banner motd # r2, encor skills assessment, scenario 2#..... Configurar un texto como mensaje del día
Line con 0.....Ingresar al modo de configuración de línea de la consola.
Exec-timeout 0 0.....Establece el tiempo de espera inactivo de la sesión remota
Logging synchronous..... evita que los mensajes inesperados que aparecen en pantalla nos desplacen los comandos que estamos escribiendo en el momento.

Exit..... Salir del modo configuración global
Configure terminal..... acceder a modo configuración global
Ipv6 unicast-routing Habilitar enrutamiento ipv6
No Ip domain lookup..... Desactiva la traducción de nombres a dirección del dispositivo

Router R3

Comandos ejecutados

Configure terminal Acceder a modo configuración global
Ipv6 unicast-routing Habilitar enrutamiento ipv6
No Ip domain lookup.....Desactiva la traducción de nombres a dirección del dispositivo
Banner motd # R3, ENCOR Skills Assessment, Scenario 2#..... Configurar un texto como mensaje del día
Line con 0.....Ingresar al modo de configuración de línea de la consola.
Exec-timeout 0 0.....Establece el tiempo de espera inactivo de la sesión remota
Logging synchronous.....Evita que los mensajes inesperados que aparecen en pantalla nos desplacen los comandos que estamos escribiendo en el momento.
Exit..... Salir del modo configuración global
Configure terminal..... Acceder a modo configuración global
Ipv6 unicast-routing Habilitar enrutamiento ipv6
No Ip domain lookup..... Desactiva la traducción de nombres a dirección del dispositivo

A continuación, se presente la configuración básica realizada en cada uno de los switches de la topología implementada.

Switch D1

Comandos ejecutados

Ipv6 unicast-routing.....Habilitar el enrutamiento ipv6
No ip domain lookup.....Desactiva la traducción de nombres a dirección del dispositivo
Banner motd # D1, ENCOR Skills Assessment, Scenario 2 #..... Configurar un texto como mensaje del día
Line con 0.....Ingresar al modo configuración de línea de la consola

Exec-timeout 0 0.....Establecer el tiempo de espera inactivo de la sesión remota
 Logging synchronous.....Evita que los mensajes que escribimos se desplacen por mensajes inesperados en pantalla
 Exit.....Salir
 Vlan 8.....Crear Vlan 8
 Name General-users.....Asignamos nombre a la Vlan 8
 Exit.....Salir
 Vlan 13.....Creamos la Vlan 13
 Name Special-users.....Asignamos nombre a la Vlan 13
 Exit.....Salimos

Switch D2

Comandos ejecutados

Ipv6 unicast-routing.....Habilitar el enrutamiento ipv6
 No ip domain lookup.....Desactiva la traducción de nombres a dirección del dispositivo
 Banner motd # D1, ENCOR Skills Assessment, Scenario 2 #..... Configurar un texto como mensaje del día
 Line con 0.....Ingresar al modo configuración de línea de la consola
 Exec-timeout 0 0.....Establecer el tiempo de espera inactivo de la sesión remota
 Logging synchronous.....Evita que los mensajes que escribimos se desplacen por mensajes inesperados en pantalla
 Exit.....Salir
 Vlan 8.....Crear Vlan 8
 Name General-users..... Asignamos nombre a la Vlan 8
 Exit.....Salir
 Vlan 13.....Creamos la Vlan 13
 Name Special-users.....Asignamos nombre a la Vlan 13
 Exit.....Salimos

Switch A1

Comandos ejecutados

Ipv6 unicast-routing.....Habilitar el enrutamiento ipv6
 No ip domain lookup.....Desactiva la traducción de nombres a dirección del dispositivo

Banner motd # A1, ENCOR Skills Assessment, Scenario 2 #..... Configurar un texto como mensaje del día

Line con 0.....Ingresar al modo configuración de línea de la consola

Exec-timeout 0 0.....Establecer el tiempo de espera inactivo de la sesión remota

Logging synchronous.....Evita que los mensajes que escribimos se desplacen por mensajes inesperados en pantalla

Exit.....Salir

Vlan 8..... Crear Vlan 8

Name General-users..... Asignamos nombre a la Vlan 8

Exit..... Salir

b. Guarde las configuraciones en cada uno de los dispositivos.

Figura 2. Comando guardar del Router 1.

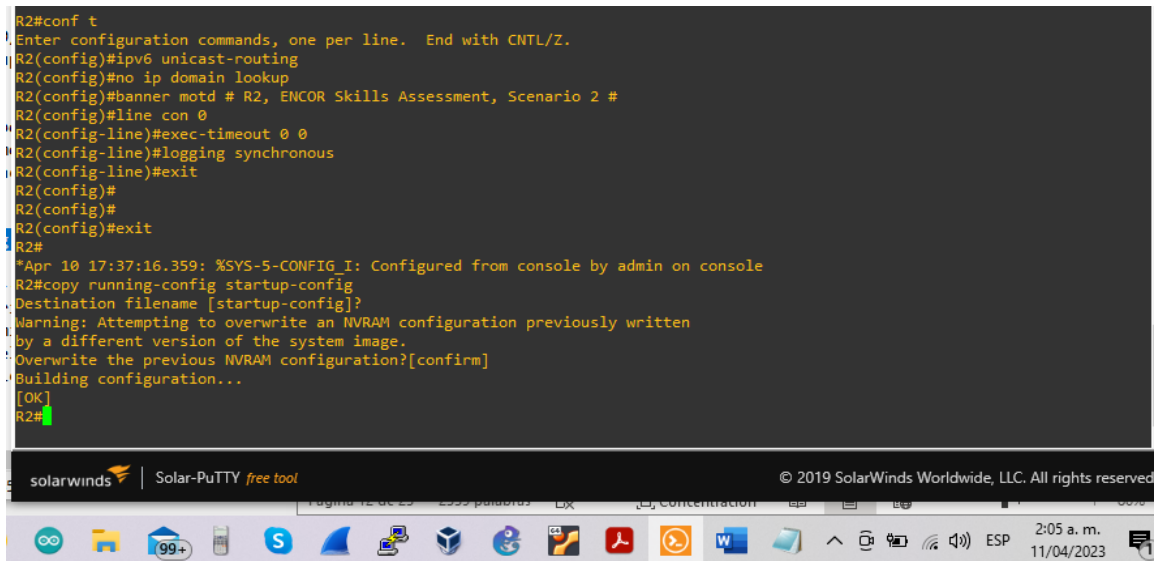
```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 2 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#copy running-config startup-config
^
% Invalid input detected at '^' marker.

R1(config)#exit
R1#
*Apr 10 20:13:33.254: %SYS-5-CONFIG_I: Configured from console by admin on console
R1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#
```

Fuente: Autoría propia

Figura 3. Comando Guardar del Router 2

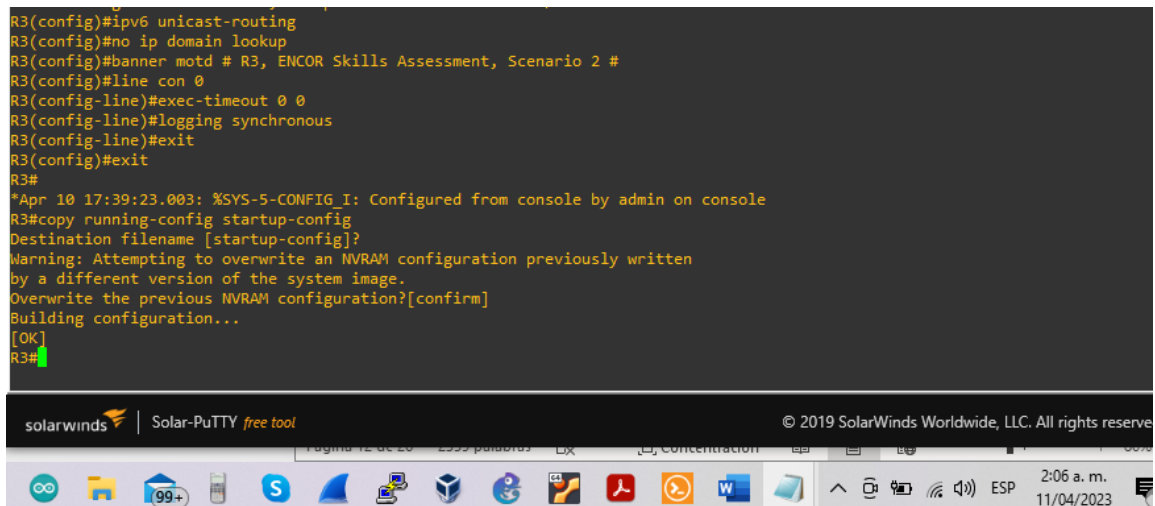
```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 2 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#
R2(config)#
R2(config)#exit
R2#
*Apr 10 17:37:16.359: %SYS-5-CONFIG_I: Configured from console by admin on console
R2#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#
```



Fuente: Autoría propia

Figura 4. Comando Guardar del Router 3

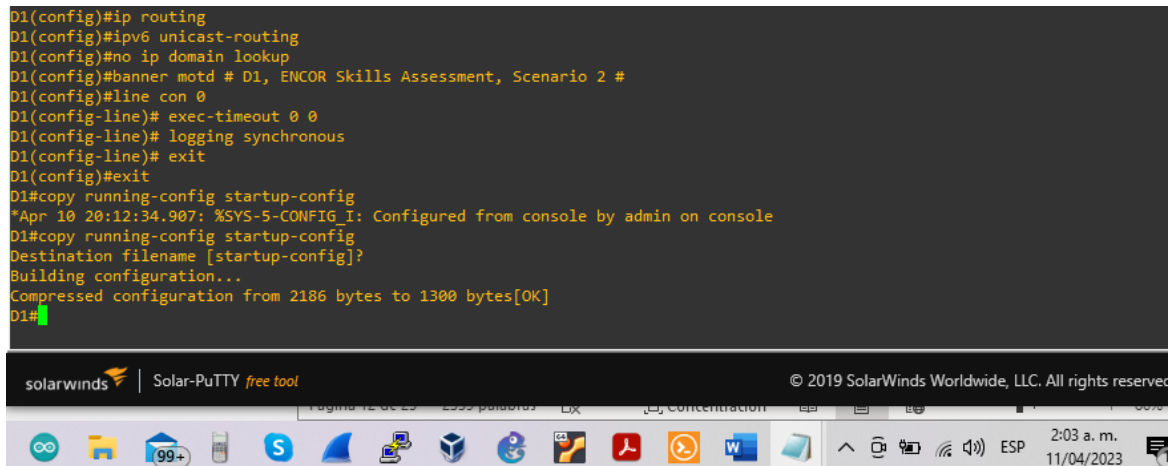
```
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 2 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#exit
R3#
*Apr 10 17:39:23.003: %SYS-5-CONFIG_I: Configured from console by admin on console
R3#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#
```



Fuente: Autoría propia

Figura 5. Comando guardar del Switch D1.

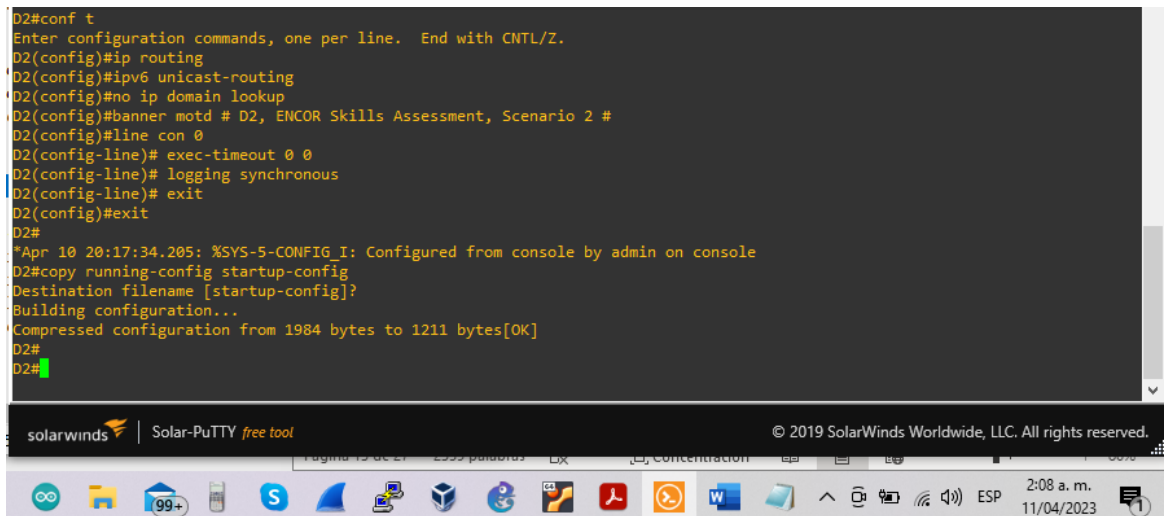
```
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 2 #
D1(config)#line con 0
D1(config-line)# exec-timeout 0 0
D1(config-line)# logging synchronous
D1(config-line)# exit
D1(config)#exit
D1#copy running-config startup-config
*Apr 10 20:12:34.907: %SYS-5-CONFIG_I: Configured from console by admin on console
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2186 bytes to 1300 bytes[OK]
D1#
```



Fuente: Autoría propia

Figura 6. Comando guardar del Switch D2.

```
D2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#exit
D2#
*Apr 10 20:17:34.205: %SYS-5-CONFIG_I: Configured from console by admin on console
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 1984 bytes to 1211 bytes[OK]
D2#
D2#
```



Fuente: Autoría propia

Figura 7. Comando guardar del Switch A1.

```
A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 0
A1(config-line)# logging synchronous
A1(config-line)# exit
A1(config)#exit
A1#copy running-config startup-config
*Apr 10 20:16:39.894: %SYS-5-CONFIG_I: Configured from console by admin on console
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2124 bytes to 1266 bytes[OK]
A1#
```

Fuente: Autoría propia

c. Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento

PC1

ip 10.0.113.8/24 10.0.113.1.....Ingresar ipv4 con mascara y puerta de enlace
ip 2001:db8:acad:113::50/64.....Ingresar la ipv6 con la mascara de red

Figura 8. Configuración ip PC1

```
PC1> sh

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC1       10.0.113.8/24  10.0.113.1   00:50:79:66:68:00  20032  127.0.0.1:20033
          fe80::250:79ff:fe66:6800/64
          2001:db8:acad:113::50/64

PC1>
```

Fuente: Autoría propia

PC2

ip 10.0.213.8/24 10.0.213.1.....Ingresar ipv4 con mascara y puerta de enlace
ip 2001:db8:acad:213::50/64.....Ingresar la ipv6 con la mascara de red

Figura 9. Configuración ip PC2

```
PC2> sh
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC2       10.0.213.8/24  10.0.213.5   00:50:79:66:68:01  20034  127.0.0.1:20035
          fe80::250:79ff:fe66:6801/64
          2001:db8:acad:213::50/64
PC2> █
```

Fuente: Autoría propia

PC3

ip 10.0.108.8/24 10.0.108.1.....Ingresar ipv4 con mascara y puerta de enlace
ip 2001:db8:acad:108::50/64.....Ingresar la ipv6 con la mascara de red

Figura 10. Configuración ip PC3

```
PC3> sh
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC3       10.0.108.8/24  10.0.108.1   00:50:79:66:68:02  20036  127.0.0.1:20037
          fe80::250:79ff:fe66:6802/64
          2001:db8:acad:108::50/64
PC3> █
```

Fuente: Autoría propia

PC4

ip 10.0.208.8/24 10.0.208.1.....Ingresar ipv4 con mascara y puerta de enlace
ip 2001:db8:acad:208::50/64.....Ingresar la ipv6 con la mascara de red

Figura 11. Configuración ip PC4

```
PC4> sh
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC4       10.0.208.8/24  10.0.208.5   00:50:79:66:68:03  20038  127.0.0.1:20039
          fe80::250:79ff:fe66:6803/64
          2001:db8:acad:208::50/64
PC4> █
```

Fuente: Autoría propia

Parte 2: configurar VRF y enrutamiento estático

En la evaluación de habilidades hemos configurado en cada uno de los enrutadores las rutas estáticas correspondientes para que de esta manera podamos comunicar el router 1 con el router 3 por medio de un ping de extremo a extremo en cada VR.

2.1 A cada uno de los router de la topología le configuramos dos VRFs, General-users y Special-users las cuales admiten IPV4 e IPV6.

2.2 A cada router le configuramos las interfaces IPV4 e IPV6 para cada VRF, esto lo hicimos habilitando subinterfaces y encapsulándolas en la VLAN que corresponde, le asignamos la VRF al igual que las direcciones IPV4, IPV6 y Link local.

2.3 En los router de los extremos R1 y R3 configuramos las rutas estáticas VRF para IPV4 IPV6 en General-users y Special-users que se comunican con el router 2.

2.4 Para verificar que las configuraciones están correctas, verificamos que R1 y R3 se puedan comunicar, esto lo hicimos haciendo ping a las direcciones de las VRF, en Special-users IPV4 10.0.213.5 e IPV6 2001:db8:acad:213::1 y General-users IPV4 10.0.208.5 e IPV6 2001:db8:acad:208::1.

Solución

2.1 En R1, R2, y R3, configure VRF-Lite VRFs Como se muestra en el diagrama de topología.

R1

Configuración de las vrf's

```
Vrf definition General-users.....se crea la vrf General-users
Address-family ipv4.....se habilita la ipv4
Address-family ipv6.....se habilita la ipv6
Exit.....salir
Vrf definition Special-users.....se crea la vrf Special-users
Address-family ipv4.....se habilita la ipv4
Address-family ipv6.....se habilita la ipv6
Exit.....salir
```

R2

Configuración de las vrfs

Vrf definition General-users.....se crea la vrf General-users
Address-family ipv4.....se habilita la ipv4
Address-family ipv6.....se habilita la ipv6
Exit..... salir
Vrf definition Special-users.....se crea la vrf Special-users
Address-family ipv4.....Se habilita la ipv4
Address-family ipv6.....Se habilita la ipv6
Exit.....salir

R3

Configuración de las vrfs

Vrf definition General-users.....se crea la vrf General-users
Address-family ipv4.....se habilita la ipv4
Address-family ipv6.....se habilita la ipv6
Exit.....Salir
Vrf definition Special-users.....se crea la vrf Special-users
Address-family ipv4.....Se habilita la ipv4
Address-family ipv6.....Se habilita la ipv6
Exit.....salir

2.2 En R1, R2 y R3 configure interfaces ipv4 y ipv6 en cada VRF como se detalla en la tabla de direccionamiento anterior

- Router R1

int e 1/0.1..... Habilitamos la sub-interface
encapsulation dot1Q 13..... La encapsulamos en la vlan 13
vrf forwarding Special-users..... Asignamos la vrf
ip address 10.0.12.1 255.255.255.0..... Asignamos ipv4
ipv6 address fe80::1:1 link-local..... Asignamos el link local
ipv6 address 2021:db8:acad:12::1/64..... Asignamos ipv6
no shutdown..... Encendemos la interface
exit..... Salimos
int e 1/0.2..... Habilitamos la sub-interface
encapsulation dot1Q 8..... La encapsulamos en la vlan 8
vrf forwarding General-users..... Asignamos la vrf
ip address 10.0.12.1 255.255.255.0..... Asignamos ipv4
ipv6 address fe80::1:2 link-local..... Asignamos el link local
ipv6 address 2021:db8:acad:12::1/64..... Asignamos ipv6

no shutdown Encendemos la interface
 exit Salimos
 interface e1/0..... Habilitamos la sub-interface
 no ip address..... Deshabilitamos ip
 no shutdown..... Habilitamos interface física Salimos
 exit.....salir
 int e 1/1.1..... Habilitamos la sub-interface
 encapsulation dot1Q 13..... La encapsulamos en la vlan 13
 vrf forwarding Special-users..... Asignamos la vrf
 ip address 10.0.113.1 255.255.255.0..... Asignamos ipv4
 ipv6 address fe80::1:3 link-local..... Asignamos el link local
 ipv6 address 2021:db8:acad:113::1/64..... Asignamos ipv6
 no shutdown..... Encendemos la interface
 exit..... Salimos
 int e 1/1.2..... Habilitamos la sub-interface
 encapsulation dot1Q 8..... La encapsulamos en la vlan 8
 vrf forwarding General-users..... Asignamos la vrf
 ip address 10.0.108.1 255.255.255.0..... Asignamos ipv4
 ipv6 address fe80::1:4 link-local..... Asignamos el link local
 ipv6 address 2021:db8:acad:108::1/64..... Asignamos ipv6
 no shutdown..... Encendemos la interface
 exit..... Salimos
 interface e1/1.....Habilitamos la sub-interface
 no ip address.....Deshabilitamos ip
 no shutdown.....Habilitamos interface física
 exit..... Salimos

A continuación, se presenta el resultado de configuración de las VRFs, donde observamos que se encuentran creadas y activas en R1

Figura 12. Comando “Show ip vrf interface” en Router 1.

```

R1#
R1#show ip vrf interface
Interface          IP-Address      VRF              Protocol
Et1/0.2            10.0.12.1       General-users     up
Et1/1.2            10.0.108.1      General-users     up
Et1/0.1            10.0.12.1       Special-users     up
Et1/1.1            10.0.113.1      Special-users     up
R1#
R1#
R1#

```

Fuente: Autoría propia

- **Router R2**

```
Int e 1/0.1..... Habilitamos la sub-interface
Encapsulation dot1q 13..... La encapsulamos en la vlan 13
Vrf forwarding special-users..... Asignamos la vrf
Ip address 10.0.12.8 255.255.255.0..... asignamos ipv4
Ipv6 address fe80::2:1 link-local..... Asignamos el link local
Ipv6 address 2021:db8:acad:12::2/64..... Asignamos ipv6
No shutdown..... encendemos la interface
Exit..... Salimos
Int e 1/0.2..... habilitamos la sub-interface
Encapsulation dot1q 8..... La encapsulamos en la vlan 8
Vrf forwarding general-users..... Asignamos la vrf
Ip address 10.0.12.8 255.255.255.0..... Asignamos ipv4
Ipv6 address fe80::2:2 link-local..... asignamos el link local
Ipv6 address 2021:db8:acad:12::2/64..... Asignamos ipv6
No shutdown ..... encendemos la interface
Exit ..... salimos
Interface e1/0..... habilitamos la sub-interface
No ip address..... deshabilitamos ip
No shutdown..... Habilitamos interface física salimos
Exit.....salir
Int e 1/1.1..... Habilitamos la sub-interface
Encapsulation dot1q 13..... La encapsulamos en la vlan 13
Vrf forwarding special-users..... Asignamos la vrf
Ip address 10.0.23.8 255.255.255.0..... asignamos ipv4
Ipv6 address fe80::2:3 link-local..... Asignamos el link local
Ipv6 address 2021:db8:acad:23::2/64..... Asignamos ipv6
No shutdown..... encendemos la interface
Exit..... Salimos
Int e 1/1.2..... Habilitamos la sub-interface
Encapsulation dot1q 8..... La encapsulamos en la vlan 8
Vrf forwarding general-users..... Asignamos la vrf
Ip address 10.0.23.8 255.255.255.0..... asignamos ipv4
Ipv6 address fe80::2:4 link-local..... Asignamos el link local
Ipv6 address 2021:db8:acad:23::2/64..... Asignamos ipv6
No shutdown..... encendemos la interface
Exit..... Salimos
Interface e1/1..... habilitamos la sub-interface
No ip address..... deshabilitamos ip
No shutdown.....habilitamos interface física
Exit..... salimos
```

A continuación, se presenta el resultado de configuración de las VRFs, donde observamos que se encuentran creadas y activas en R2

Figura 13. Comando “Show ip vrf interface” en Router 2.

```

R2#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.8       General-users     up
Et1/1.2        10.0.23.8       General-users     up
Et1/0.1        10.0.12.8       Special-users     up
Et1/1.1        10.0.23.8       Special-users     up
R2#
  
```

Fuente: Autoría propia

- **Router R3**

```

Int e 1/0.1..... Habilitamos la sub-interface
Encapsulation dot1q 13..... La encapsulamos en la vlan 13
Vrf forwarding Special-users..... Asignamos la vrf
Ip address 10.0.23.5 255.255.255.0..... Asignamos ipv4
Ipv6 address fe80::3:1 link-local..... Asignamos el link local
Ipv6 address 2021:db8:acad:23::3/64..... Asignamos ipv6
No shutdown..... Encendemos la interface
Exit..... Salimos
Int e 1/0.2..... Habilitamos la sub-interface
Encapsulation dot1q 8..... La encapsulamos en la vlan 8
Vrf forwarding General-users..... Asignamos la vrf
Ip address 10.0.23.5 255.255.255.0..... Asignamos ipv4
Ipv6 address fe80::3:2 link-local..... Asignamos el link local
Ipv6 address 2021:db8:acad:23::3/64..... Asignamos ipv6
No shutdown ..... Encendemos la interface
Exit ..... Salimos
Interface e1/0..... Habilitamos la sub-interface
No ip address..... Deshabilitamos ip
No shutdown..... Habilitamos interface física Salimos
Exit.....salir
Int e 1/1.1..... Habilitamos la sub-interface
Encapsulation dot1q 13..... La encapsulamos en la vlan 13
Vrf forwarding Special-users..... Asignamos la vrf
Ip address 10.0.213.5 255.255.255.0..... Asignamos ipv4
Ipv6 address fe80::3:3 link-local..... Asignamos el link local
Ipv6 address 2021:db8:acad:213::1/64..... Asignamos ipv6
  
```

No shutdown..... Encendemos la interface
Exit..... Salimos
Int e 1/1.2..... Habilitamos la sub-interface
Encapsulation dot1q 8..... La encapsulamos en la vlan 8
Vrf forwarding General-users..... Asignamos la vrf
Ip address 10.0.208.5 255.255.255.0..... Asignamos ipv4
Ipv6 address fe80::3:4 link-local..... Asignamos el link local
Ipv6 address 2021:db8:acad:208::1/64..... Asignamos ipv6
No shutdown..... Encendemos la interface
Exit..... Salimos
Interface e1/1.....Habilitamos la sub-interface
No ip address.....Deshabilitamos ip
No shutdown.....Habilitamos interface física
Exit..... Salimos

A continuación, se presenta el resultado de configuración de las VRFs, donde observamos que se encuentran creadas y activas en R3

Figura 14. Comando “Show ip vrf interface” en Router 3.

```
R3#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.23.5       General-users    up
Et1/1.2        10.0.208.5     General-users    up
Et1/0.1        10.0.23.5       Special-users    up
Et1/1.1        10.0.213.5     Special-users    up
R3#
```

Fuente: Autoría propia

2.3 En R1 y R3, configuran rutas estáticas predeterminadas que apuntan a R2.

Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.

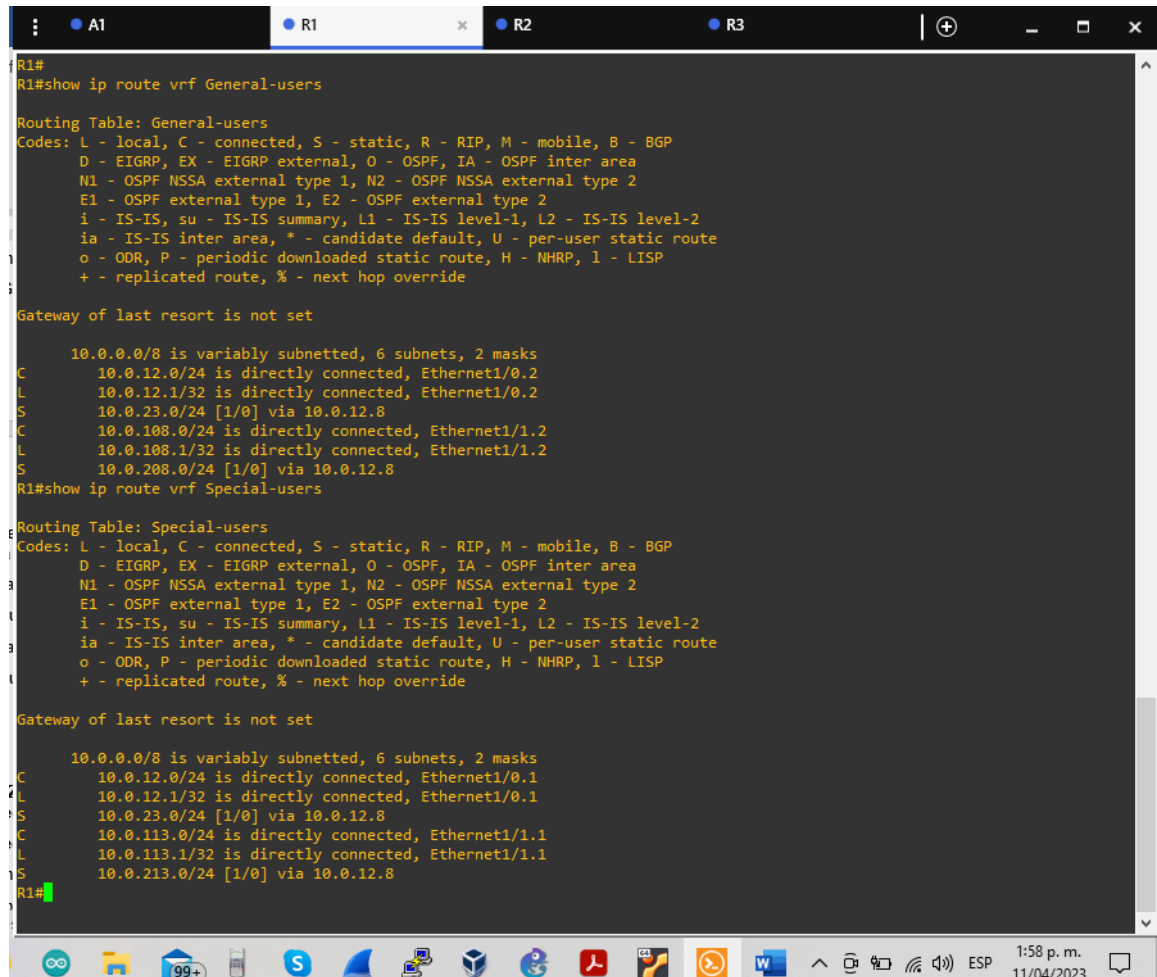
- **Router 1**

Configure terminal..... Entramos en la configuración terminal
ip route vrf Special-users 0.0.0.0 0.0.0.0 10.0.12.8..... Asignamos ruta ipv4
pv6 route vrf Special-users ::/0 2001:db8:acad:12::2..... Asignamos la ruta ipv6
ip route vrf General-users 0.0.0.0 0.0.0.0 10.0.12.8..... Asignamos ruta ipv4

ip route vrf General-users ::/0 2001:db8:acad:12::2..... Asignamos la ruta ipv6
exit..... Salimos

A continuación, se presenta el resultado de configuración de rutas estáticas en las VRFs.

Figura 15. Tabla de enrutamiento Router 1



```
R1#
R1#show ip route vrf General-users

Routing Table: General-users
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
+ - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, Ethernet1/0.2
L    10.0.12.1/32 is directly connected, Ethernet1/0.2
S    10.0.23.0/24 [1/0] via 10.0.12.8
C    10.0.108.0/24 is directly connected, Ethernet1/1.2
L    10.0.108.1/32 is directly connected, Ethernet1/1.2
S    10.0.208.0/24 [1/0] via 10.0.12.8
R1#show ip route vrf Special-users

Routing Table: Special-users
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
+ - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, Ethernet1/0.1
L    10.0.12.1/32 is directly connected, Ethernet1/0.1
S    10.0.23.0/24 [1/0] via 10.0.12.8
C    10.0.113.0/24 is directly connected, Ethernet1/1.1
L    10.0.113.1/32 is directly connected, Ethernet1/1.1
S    10.0.213.0/24 [1/0] via 10.0.12.8
R1#
```

Fuente: Autoría propia

- Router 2

ip route vrf Special-users 10.0.113.0 255.255.255.0 10.0.23.5.....Asignamos
ruta ipv4 a vrf Special-users

ip route vrf Special-users 10.0.12.0 255.255.255.0 10.0.23.5.....Asignamos
ruta ipv4 a vrf Special-users

ip route vrf General-users 10.0.108.0 255.255.255.0 10.0.23.5.....Asignamos
ruta ipv4 a vrf General-users

ip route vrf General-users 10.0.208.0 255.255.255.0 10.0.12.1.....Asignamos
ruta ipv4 a vrf General-users

ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1Asigno
la ruta ipv6 para sacar trafico

ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3....Asigno
la ruta ipv6 para sacar trafico

ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1 ...Asigno
la ruta ipv6 para sacar trafico

ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3...Asigno
la ruta ipv6 para sacar trafico

A continuación, se presenta el resultado de configuración de rutas estáticas en las
VRFs.

Figura 16. Tabla de enrutamiento Router 2

```

Et1/1.1          10.0.23.8      Special-users    up
R2#show ip route vrf General-users

Routing Table: General-users
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
       + - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, Ethernet1/0.2
L    10.0.12.8/32 is directly connected, Ethernet1/0.2
C    10.0.23.0/24 is directly connected, Ethernet1/1.2
L    10.0.23.8/32 is directly connected, Ethernet1/1.2
S    10.0.108.0/24 [1/0] via 10.0.12.1
S    10.0.208.0/24 [1/0] via 10.0.23.5
R2#show ip route vrf Special-users

Routing Table: Special-users
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
       + - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, Ethernet1/0.1
L    10.0.12.8/32 is directly connected, Ethernet1/0.1
C    10.0.23.0/24 is directly connected, Ethernet1/1.1
L    10.0.23.8/32 is directly connected, Ethernet1/1.1
S    10.0.113.0/24 [1/0] via 10.0.12.1
S    10.0.213.0/24 [1/0] via 10.0.23.5
R2#
  
```

Fuente: Autoría propia

- Router 3

- ip route vrf Special-users 0.0.0.0 0.0.0.0 10.0.23.8..... Asignamos ruta ipv4
- ip route vrf General-users 0.0.0.0 0.0.0.0 10.0.23.8..... Asignamos ruta ipv4
- ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2..... Asignamos ruta ipv6
- ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2..... Asignamos ruta ipv6

A continuación, se presenta el resultado de configuración de rutas estáticas en las VRFs.

Figura 17. Tabla de enrutamiento Router 3

```
R3#show ip route vrf Special-users
Routing Table: Special-users
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
+ - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
S   10.0.12.0/24 [1/0] via 10.0.23.8
C   10.0.23.0/24 is directly connected, Ethernet1/0.1
L   10.0.23.5/32 is directly connected, Ethernet1/0.1
S   10.0.113.0/24 [1/0] via 10.0.23.8
C   10.0.213.0/24 is directly connected, Ethernet1/1.1
L   10.0.213.5/32 is directly connected, Ethernet1/1.1
R3#show ip route vrf Genera}l-users
% IP routing table vrf Genera}l-users does not exist
R3#show ip route vrf General-users
Routing Table: General-users
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
+ - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
S   10.0.12.0/24 [1/0] via 10.0.23.8
C   10.0.23.0/24 is directly connected, Ethernet1/0.2
L   10.0.23.5/32 is directly connected, Ethernet1/0.2
S   10.0.108.0/24 [1/0] via 10.0.23.8
C   10.0.208.0/24 is directly connected, Ethernet1/1.2
L   10.0.208.5/32 is directly connected, Ethernet1/1.2
```

Fuente: Autoría propia

2.4 Verifique la conectividad en cada VRF.

Desde R1, verifique la conectividad con R3:

- ping vrf General-users 10.0.208.5

Figura 18. Conectividad entre R1 y R3 por VRF General-users ipv4

```
R1#
R1#ping vrf General-users 10.0.208.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/50/100 ms
R1#
R1#
```

Fuente: Autoría propia

- ping vrf General-users 2001:db8:acad:208::1

Figura 19. Conectividad entre R1 y R3 por VRF General-users ipv6

```
R1#
R1#ping vrf General-users 2001:db8:acad:208::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/24/32 ms
R1#
```

Fuente: Autoría propia

- ping vrf Special-users 10.0.213.5

Figura 20. Conectividad entre R1 y R3 por VRF Special-users ipv4

```
R1#
R1#ping vrf Special-users 10.0.213.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/24/32 ms
R1#
R1#
R1#
```

Fuente: Autoría propia

- ping vrf Special-users 2001:db8:acad:213::1

Figura 21. Conectividad entre R1 y R3 por VRF Special-users ipv6

```
R1#
R1#ping vrf Special-users 2001:db8:acad:213::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/32/52 ms
R1#
```

Fuente: Autoría propia

2. Escenario 2

Parte 3. Configurar Capa 2

En esta parte configuraremos los switches para soportar la conectividad con los dispositivos finales.

- 3.1 Deshabilitamos las interfaces en los switches D1, D2 y A1.
- 3.2 Configuramos enlaces troncales en D1 y D2 para los router R1 y R3.
- 3.3 Configuramos un EtherChannel entre los switches D1 y A1, creamos la interfaz port-channel 1 e ingresamos al rango de interfaces entre e0/0 hasta la e0/1, administramos la interface por link aggregation 1, habilitamos el puerto en modo de acceso y habilitamos también el acceso a la VLAN 8.
- 3.4 En este paso hemos configurado interfaces como puertos de acceso para las 4 PCs en los 3 switches, en D1 habilite un puerto de acceso en la VLAN13, en D2 habilite dos puertos de acceso uno en la VLAN 13 y otro en la VLAN 8 y en A1 habilite un puerto de acceso en la VLAN 8.
- 3.5 En este paso lo que hicimos fue verificar la conectividad IPV4 e IPV6 entre PC1 a PC2 y PC3 a PC4.

Solución

3.1 Deshabilitar todas las interfaces en D1, D2 y A1.

Para todas los Switches utilizamos el siguiente comando:

```
conf t -----entrar en modo configuración global
Interface range e0/0-24-----rango de interfaces de 0-24
shutdown -----apagamos las interfaces seleccionadas
```

3.2 Configurar los enlaces troncales.

D1

```
interface range e0/2
switchport trunk encapsulation dot1q-----habilitar encapsulamiento de vlan
switchport mode trunk-----lo habilitamos en modo troncal
switchport trunk allowed vlan add 8,13-----permitir vlans en el puerto troncal
no shutdown----- encendemos interface de red
exit-----salir
```

A continuación, se presenta el resultado de configurar enlaces troncales

Figura 22. Interface Troncal Ethernet 0/2

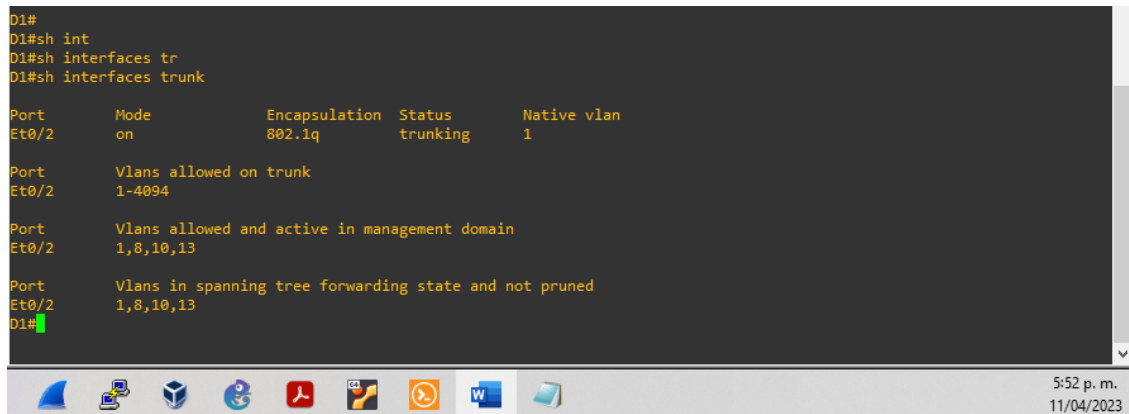
```
D1#
D1#sh int
D1#sh interfaces tr
D1#sh interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
Et0/2     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Et0/2     1-4094

Port      Vlans allowed and active in management domain
Et0/2     1,8,10,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/2     1,8,10,13
D1#
```



Fuente: Autoría propia.

D2

interface e0/3

switchport trunk encapsulation dot1q-----habilitar encapsulamiento de vlan

switchport mode trunk-----lo habilitamos en modo troncal

switchport trunk allowed vlan add 8,13-----permitir vlans en el puerto troncal

no shutdown-----encendemos interface de red

exit-----salir

A continuación, se presenta el resultado de configurar enlaces troncales

Figura 23. Interface Troncal Ethernet 0/3

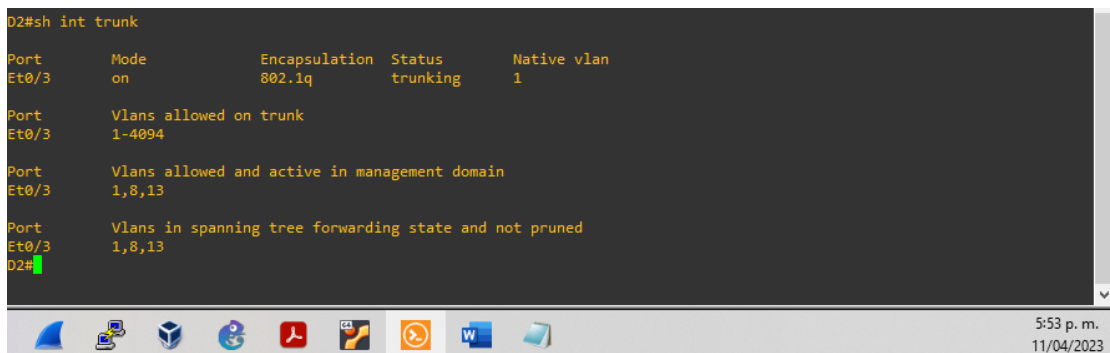
```
D2#sh int trunk

Port      Mode      Encapsulation  Status      Native vlan
Et0/3     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Et0/3     1-4094

Port      Vlans allowed and active in management domain
Et0/3     1,8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/3     1,8,13
D2#
```



Fuente: Autoría propia.

3.3 Configurar el EtherChannel en D1 y A1

D1

Interface port-channel 1-----creamos la interfaz port-channel 1
Exit-----salimos
Int range e0/0-1-----ingresamos al rango de interfaces
Channel-group 1 mode desirable -----administración de la interfaz por link
agregation 1
Exit-----salir
Interface port-channel 1-----creamos la interfaz port-channel 1
Switchport mode access-----habilita el puerto en modo de acceso
Switchport access vlan 8-----hailitamos el acceso a la vlan 8
Exit

A continuación, se presenta el resultado de configurar EtherChannel en D1

Figura 24. Interface port-channel 1

```
D1#sh etherchannel s
D1#sh etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----+-----
1      Po1(SU)        PAgP        Et0/0(P)  Et0/1(P)
D1#
```

Fuente: Autoría propia.

A1

Interface port-channel 1----- creamos la interfaz port-channel 1
Switchport mode access----- habilita el puerto en modo de acceso
Switchport access vlan 8----- habilitamos el acceso a la vlan 8

Exit-----salir
 Interface range e0/0-1----- ingresamos al rango de interfaces
 Channel-group 1 mode desirable----- administración de la interfaz por link
 aggregation 1
 Interface range e0/2 ----- ingresamos al rango de interfaces
 Switchport mode access----- habilita el puerto en modo de acceso
 Switchport access vlan 8----- habilitamos el acceso a la vlan 8
 No shutdown-----encendemos la interface
 Exit-----salir

A continuación, se presenta el resultado de configurar EtherChannel en A1.

Figura 25. Interface port-channel 1

```
A1#sh et
A1#sh etherc
A1#sh etherchannel s
A1#sh etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----+-----
1      Po1(SU)        PAgP        Et0/0(P)  Et0/1(P)

A1#
```

Fuente: Autoría propia.

3.4 Configurar puertos de acceso para PC1, PC2, PC3 y PC4 en D1, D2 y A1.

D1

interface e0/3 -----interface en la que se encuentra PC1
 switchport mode access-----configurar el puerto en modo de acceso
 switchport access vlan 13-----agregamos la vlan 13 modo de acceso
 no shutdown-----habilitamos la interfaz
 exit-----salimos

D2

```
interface e0/2-----interface donde esta PC2
switchport mode access----- configurar el puerto en modo acceso
switchport access vlan 13----- asignamos la vlan 13 en acceso para el pc 2
no shutdown-----habilitamos la interfaz
exit-----salimos
interface e0/1-----ingresamos a la interfaz ethernet 0/1
switchport mode access-----configurar el puerto en modo acceso
switchport access vlan 8-----asignamos la vlan 8 en acceso para el pc 4
no shutdown-----encendemos la interface
exit-----salir
```

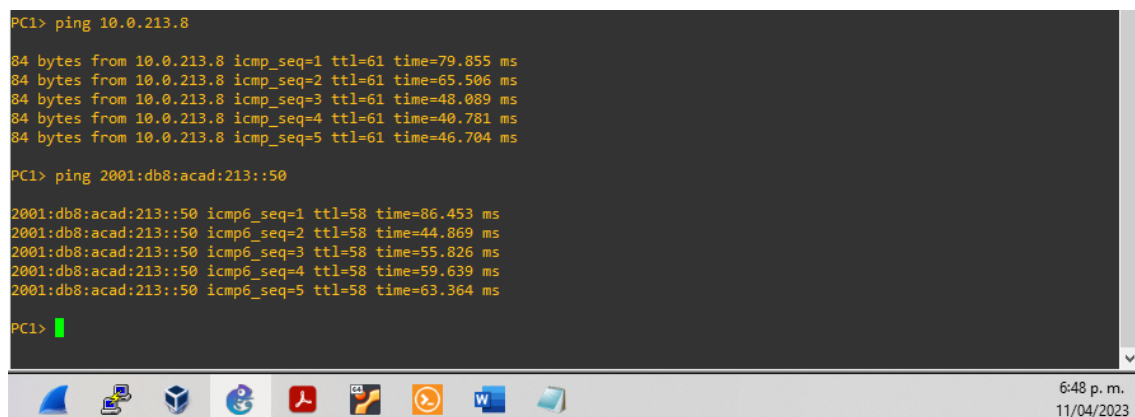
A1

```
interface e0/2 -----ingresamos a la interfaz ethernet 0/2
switchport mode access-----configuramos el puerto en modo de acceso
switchport access vlan 8-----asignamos la vlan 8 en acceso para la PC3
no shutdown-----encendemos la interfaz
exit-----salir
```

3.5 Verificación de la conectividad de PC a PC

A continuación, se presenta el resultado de conectividad de PC1 a PC2 ipv4 e ipv6.

Figura 26. ping exitoso entre PC1 y PC2 con ipv4 e ipv6



```
PC1> ping 10.0.213.8

84 bytes from 10.0.213.8 icmp_seq=1 ttl=61 time=79.855 ms
84 bytes from 10.0.213.8 icmp_seq=2 ttl=61 time=65.506 ms
84 bytes from 10.0.213.8 icmp_seq=3 ttl=61 time=48.089 ms
84 bytes from 10.0.213.8 icmp_seq=4 ttl=61 time=40.781 ms
84 bytes from 10.0.213.8 icmp_seq=5 ttl=61 time=46.704 ms

PC1> ping 2001:db8:acad:213::50

2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=86.453 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=44.869 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=55.826 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=59.639 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=63.364 ms

PC1> █
```

Fuente: Autoría propia.

A continuación, se presenta el resultado de conectividad de PC3 a PC4 ipv4 e ipv6.

Figura 27. ping exitoso entre PC3 y PC4 con ipv4 e ipv6

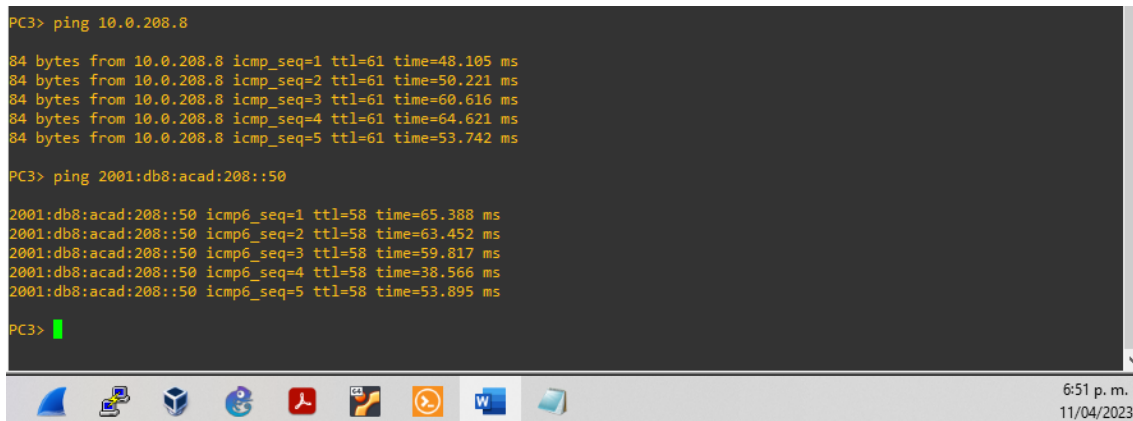
```
PC3> ping 10.0.208.8

84 bytes from 10.0.208.8 icmp_seq=1 ttl=61 time=48.105 ms
84 bytes from 10.0.208.8 icmp_seq=2 ttl=61 time=50.221 ms
84 bytes from 10.0.208.8 icmp_seq=3 ttl=61 time=60.616 ms
84 bytes from 10.0.208.8 icmp_seq=4 ttl=61 time=64.621 ms
84 bytes from 10.0.208.8 icmp_seq=5 ttl=61 time=53.742 ms

PC3> ping 2001:db8:acad:208::50

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=65.388 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=63.452 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=59.817 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=38.566 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=53.895 ms

PC3> █
```



Fuente: Autoría propia.

Parte 4. Configure seguridad

En esta parte configuramos varios mecanismos de seguridad en cada uno de los dispositivos de la topología.

Las tareas de configuración son las siguientes:

- 4.1 Configuramos en cada dispositivo de la topología el modo EXE privilegiado seguro, con un tipo de algoritmo SCRYPT, y contraseña jairozambrano085.
- 4.2 Creamos una cuenta de usuario local en cada dispositivo.
- 4.3 En cada uno de los dispositivos se habilito la autenticación AAA usando la base de datos local en todas las líneas

Solución

4.1 Configuración de seguridad privilegiada en modo EXE en todos los dispositivos.

Para todos los dispositivos utilizamos los mismos comandos.

configure terminal-----ingreso modo global

service password-encryption-----habilitar el cifrado de la contraseña al revisar la configuración
enable secret jairozambrano085-----habilitar la contraseña encriptada

4.2 Crear una cuenta de usuario local en todos los dispositivos

Para todos los dispositivos utilizamos los mismos comandos.

username admin secret 0 jairozambrano085-----ingreso de usuario y contraseña
username admin privilege 15 secret jairozambrano085-----habilitar el usuario y contraseña

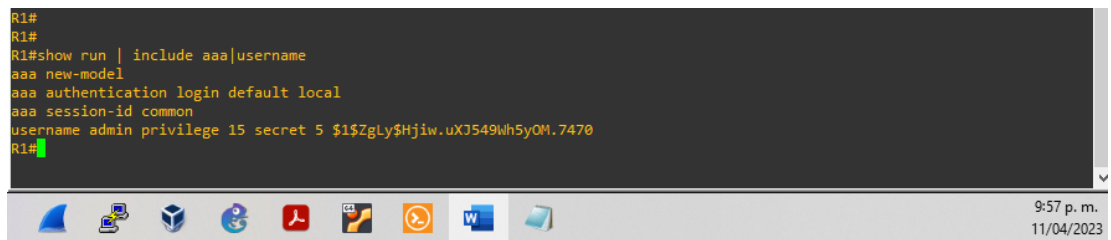
4.3 Habilite la autenticación AAA en todos los dispositivos

Para todos los dispositivos utilizamos los mismos comandos.

Aaa new-model-----habilita la configuración AAA
Aaa authentication login default local-----habilita la autenticación AAA

A continuación, se presenta la verificación de seguridad en cada uno de los dispositivos de la topología.

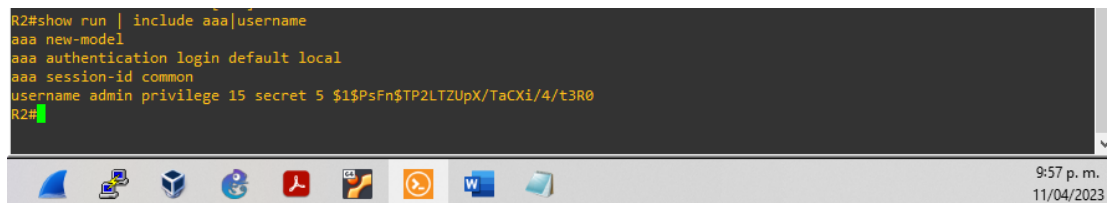
Figura 28. Verificación de seguridad en R1



```
R1#
R1#
R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$ZgLy$Hjiw.uXJ549Wh5y0M.7470
R1#
```

Fuente: Autoría propia.

Figura 29. Verificación de seguridad en R2

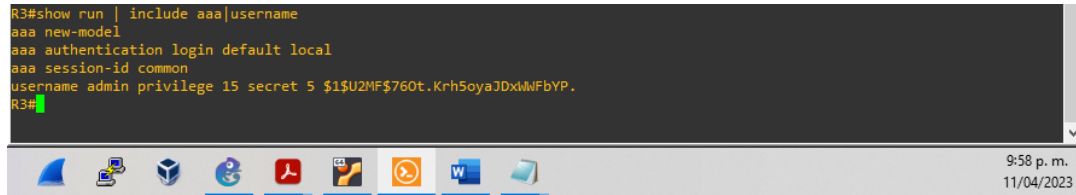


```
R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$PsFn$TP2LTZUpX/TaCXi/4/t3R0
R2#
```

Fuente: Autoría propia.

Figura 30. Verificación de seguridad en R3

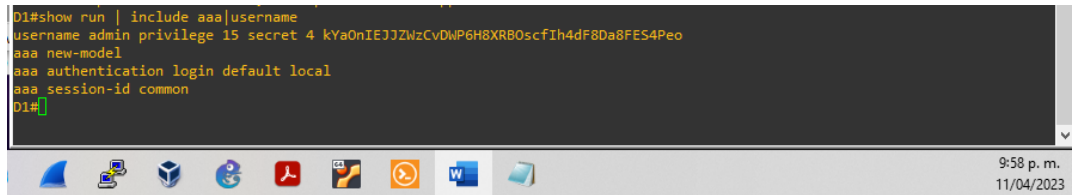
```
R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$U2MF$760t.Krh5oyaJDxMWFbYP.
R3#
```



Fuente: Autoría propia.

Figura 31. Verificación de seguridad en D1

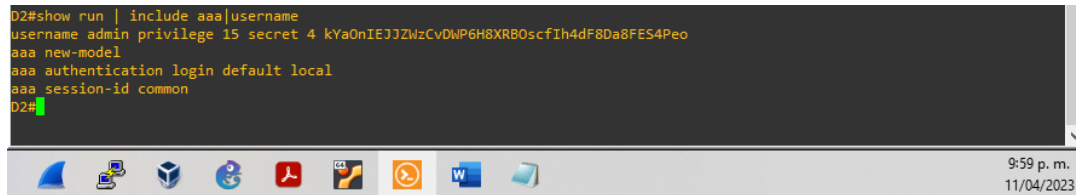
```
D1#show run | include aaa|username
username admin privilege 15 secret 4 kYaOnIEJJZwzCvDWP6H8XR80scfIh4dF8Da8FES4Peo
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
```



Fuente: Autoría propia.

Figura 32. Verificación de seguridad en D2

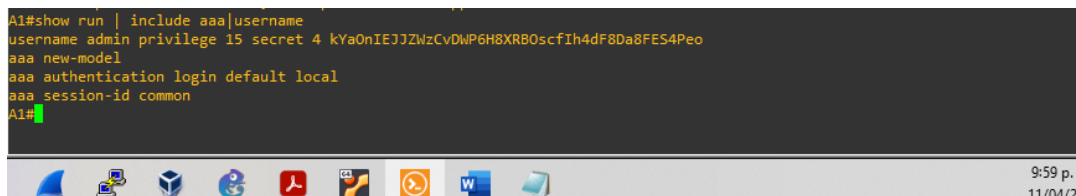
```
D2#show run | include aaa|username
username admin privilege 15 secret 4 kYaOnIEJJZwzCvDWP6H8XR80scfIh4dF8Da8FES4Peo
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```



Fuente: Autoría propia.

Figura 33. Verificación de seguridad en A1

```
A1#show run | include aaa|username
username admin privilege 15 secret 4 kYaOnIEJJZwzCvDWP6H8XR80scfIh4dF8Da8FES4Peo
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```



Fuente: Autoría propia.

CONCLUSIONES

La configuración de VRFs permite en los dispositivos de capa tres como son los routers ejecutar de forma simultanea varias tablas de enrutamiento virtual, las cuales permiten asignar la misma dirección IP a dos interfaces al mismo tiempo

La configuración de un EtherChannel en dos switches nos permite combinar dos enlaces físicos para convertirlos en uno solo enlace lógico, esto lo que nos permite es aumentar el ancho de banda para de esta manera tener un mejor tráfico entre los mismos.

Al utilizar el protocolo de autenticación AAA creamos niveles privilegiados para restringir el acceso a los equipos, sea utilizando el rol de usuario o de administrador para proteger la información que transmitimos en nuestra red.

El desarrollo de este trabajo final nos permitió practicar algunas habilidades y conocimientos que adquirimos con anterioridad durante el transcurso de esta carrera de ingeniería en telecomunicaciones, lo cual nos hizo ampliar y fortalecer conocimientos y habilidades en redes.

BIBLIOGRAFÍA

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

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

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

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

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

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

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

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