DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAMES MORA MOSQUERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

SOACHA, CUNDINAMARCA

2023

DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NOMBRE

JAMES MORA MOSQUERA

DIRECTOR

JUAN ESTEBAN TAPIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

SOACHA, CUNDINAMARCA

2023

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Soacha, 9 de mayo de 2023

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

Protocolo de enrutado: Es un conjunto de reglas y procedimientos que se utilizan en redes de computadoras para determinar la ruta óptima que deben seguir los paquetes de datos desde su origen hasta su destino. El protocolo de enrutado es responsable de tomar decisiones en tiempo real para seleccionar la mejor ruta disponible y garantizar una entrega eficiente de los datos.

Conmutador: Es un dispositivo de red que se utiliza para conectar varios dispositivos en una red local. El conmutador funciona como un interruptor de circuito para la red y puede enrutar los datos entre dispositivos de manera inteligente, asegurando que los datos lleguen a su destino de manera rápida y confiable.

Redes de computadoras: Es un campo de la informática que se ocupa del diseño, implementación y mantenimiento de sistemas de interconexión de dispositivos de hardware y software para permitir la comunicación y el intercambio de datos. Las redes de computadoras son fundamentales en la era de la información y se utilizan en una amplia variedad de aplicaciones, desde redes de área local hasta redes de internet globales.

Protocolo de puerta de enlace de borde: Border Gateway Protocol (BGP) es un protocolo de enrutado utilizado en internet para intercambiar información de enrutado entre diferentes sistemas autónomos. El protocolo de puerta de enlace de borde es esencial para garantizar la conectividad y la redundancia en la red de internet, y es utilizado por proveedores de servicios de internet y grandes empresas de redes.

Protocolo de tiempo de red: Network Time Protocol (NTP) es un protocolo utilizado para sincronizar el reloj de los dispositivos en una red. El protocolo de tiempo de red es esencial para garantizar que los dispositivos estén sincronizados con una hora de referencia común y precisa, lo que es crítico para muchas aplicaciones de red.

RESUMEN

En esta evaluación de habilidades, se lleva a cabo la configuración multi-VRF (Virtual Routing and Forwarding) en GNS3, siendo esta una técnica avanzada de enrutamiento que permite a una red virtualizar el plano de control y de datos, creando múltiples tablas de enrutamiento y aislamiento de tráfico entre ellas. La configuración multi-VRF en GNS3 se puede utilizar en diferentes escenarios, como redes corporativas con múltiples departamentos, servicios de proveedores de servicios de Internet (ISP) o redes de centros de datos.

Al utilizar la técnica multi-VRF, se pueden lograr beneficios como un mejor rendimiento, una mayor seguridad y una mayor eficiencia en el uso de los recursos de la red. Además, GNS3 es una herramienta útil para simular y probar configuraciones de red, permitiendo a los administradores de redes experimentar y validar diferentes configuraciones antes de implementarlas en una red real.

Palabras clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Multi-VRF.

ABSTRACT

In this skills assessment, multi-VRF (Virtual Routing and Forwarding) configuration is carried out in GNS3, this being an advanced routing technique that allows a network to virtualize the control and data plane, creating multiple routing tables. and traffic isolation between them. The multi-VRF configuration in GNS3 can be used in different scenarios, such as corporate networks with multiple departments, Internet Service Provider (ISP) services, or data center networks.

By using the multi-VRF technique, benefits such as better performance, higher security, and greater efficiency in the use of network resources can be achieved. Furthermore, GNS3 is a useful tool for simulating and testing network configurations, allowing network administrators to experiment and validate different configurations before implementing them in a real network.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Multi-VRF.

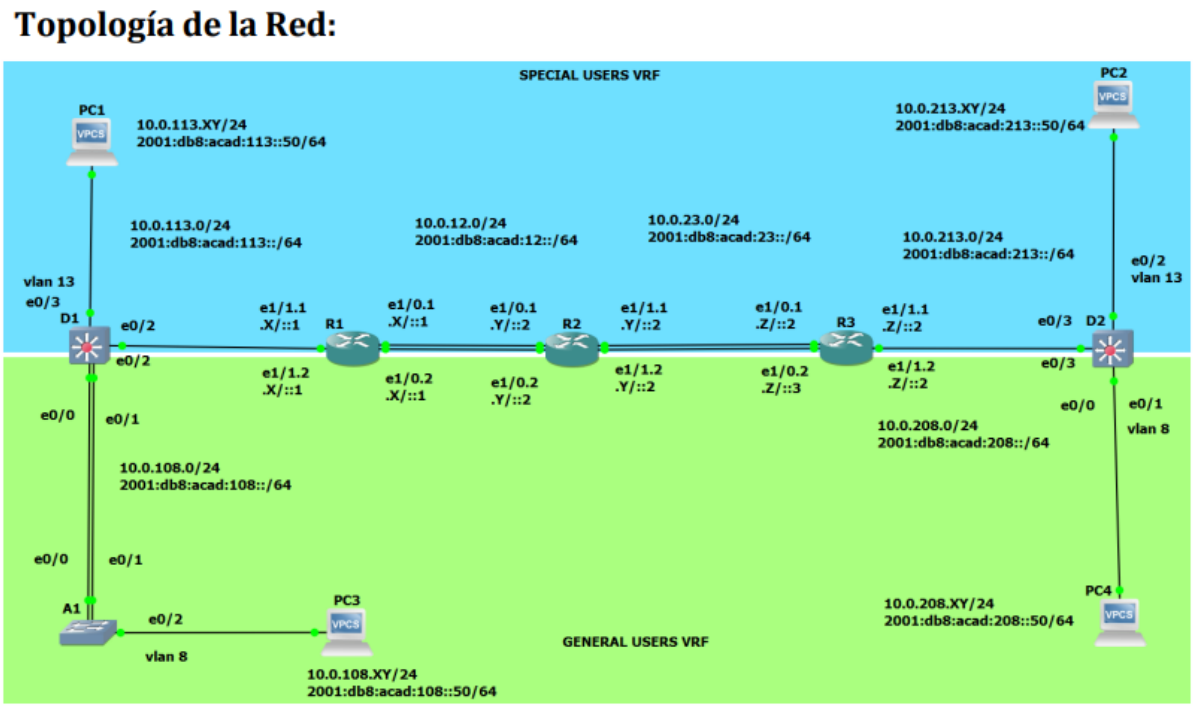
INTRODUCCION

En la evaluación de habilidades presente, se aborda un reto en la configuración de redes de comunicaciones, específicamente la implementación de una configuración multi-VRF para separar dos grupos de usuarios, "Usuarios Generales" y "Usuarios Especiales", mediante el uso de VLANs. Para ello, se realizan ajustes en la configuración básica de los dispositivos de red, incluyendo la asignación de direccionamiento IP a las interfaces que conectan los segmentos de red. Luego, se configuran VRF-Lite en los tres enrutadores de la red y se asignan rutas estáticas apropiadas para permitir la conectividad de extremo a extremo, verificando la accesibilidad mediante comandos de ping desde R3 a cada VRF. El objetivo final es asegurar la accesibilidad completa de un extremo a otro en la red, mientras que los dos grupos de usuarios permanecen aislados entre sí sin comunicación posible. Para ello, se realiza una verificación exhaustiva de las configuraciones para garantizar que cumplan con las especificaciones requeridas y que los dispositivos funcionen correctamente para resolver el problema. En resumen, la evaluación de habilidades de configuración multi-VRF es un proceso desafiante que requiere un alto nivel de conocimientos y habilidades en redes de comunicaciones. Es esencial comprender en profundidad los conceptos de enrutamiento, conmutación, VLANs, VRFs, direccionamiento IP y seguridad de red, y aplicarlos adecuadamente en la configuración de dispositivos de red para lograr una red de comunicaciones segura, escalable y eficiente.

DESARROLLO DEL TRABAJO

Topología de la red

Figura 1. Escenario 1



Fuente: Guía avance documento final CCNP

Escenario

En esta evaluación de habilidades, usted es responsable de completar la configuración multi-VRF de la red que admite "Usuarios generales" y "Usuarios especiales". Una vez finalizado, debería haber accesibilidad completa de un extremo a otro y los dos grupos no deberían poder comunicarse entre sí. Asegúrese de verificar que sus configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según lo requerido.

Tabla de direccionamiento

Tabla 1.Direccionamiento de la Red

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.4/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.4/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.4/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.4/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.5/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.5/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.5/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.5/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.6/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.6/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.6/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.6/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.45/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.45/24	2001:db8:acad:213::50/64	EUI-64

Fuente: Autoría Propia

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

CC: 93020455

X: 4

Y: 5

Z: 5, se asume como 6 en casos debido a que se repiten las IP’s

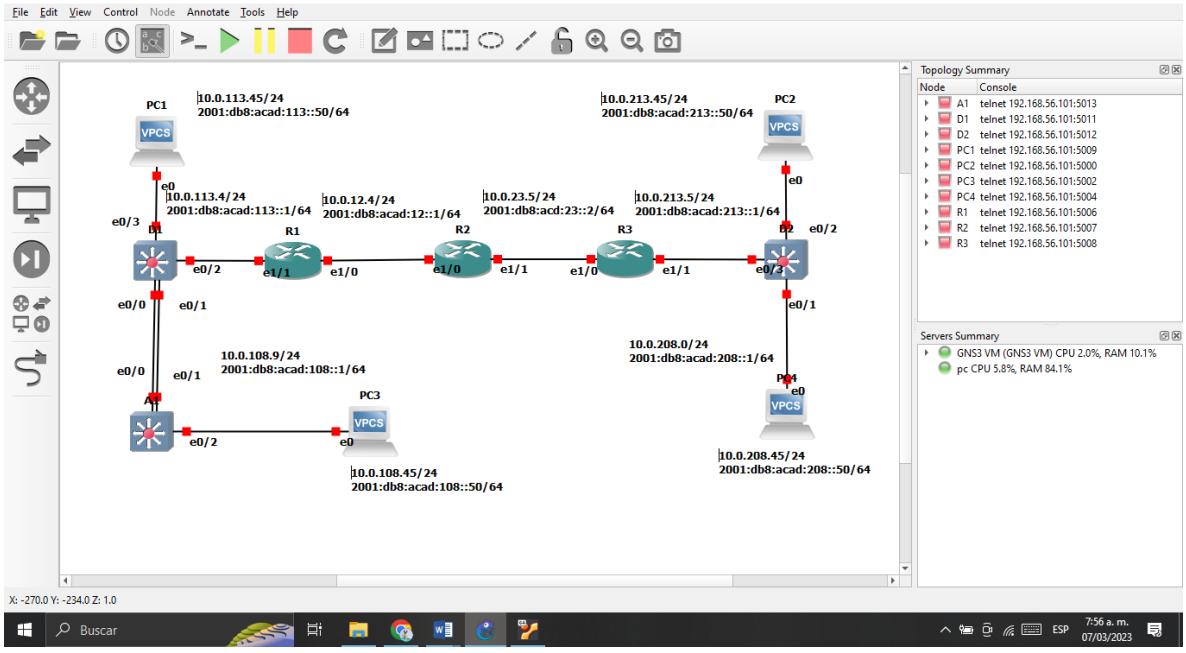
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz

En la Parte 1, se configura la topología de la red y se configura los ajustes básicos.

Paso 1. Cablee la red como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y cablee según sea necesario.

Figura 2 Simulación escenario GNS3



Fuente: Autoría Propia

Paso 2: Configure los ajustes básicos para cada dispositivo.

Ingrese al modo de configuración global en cada uno de los dispositivos y aplique la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.

a. Ingrese al modo de configuración global en cada uno de los dispositivos y aplique la configuración básica.

Router R1

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

se asigna un nombre único de identificación para el router con el comando hostname , para luego habilitar el enrutamiento unicast IPv6 en el. Esto permite que el router enrute paquetes IPv6 en la red.

Router R2

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

Router R3

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

Para R1, R2 y R3:

1. **hostname** : Este comando establece el nombre del router. El nombre se utiliza para identificar el dispositivo en la red.
2. **ipv6 unicast-routing**: Este comando habilita el enrutamiento unicast IPv6 en el router. Esto permite que el router enrute paquetes IPv6 en la red.
3. **no ip domain lookup**: Este comando desactiva la resolución de nombres DNS en el router. Esto ayuda a evitar retrasos en la entrada de comandos en la línea de comando.
4. **banner motd # R1, ENCOR Skills Assessment, Scenario 2 #**: Este comando establece un mensaje del día (MOTD) en el router. El mensaje es "# R1, ENCOR Skills Assessment, Scenario 2 #". El MOTD se muestra en la pantalla cuando un usuario se conecta al router.
5. **line con 0**: Este comando configura la línea de consola del router para su configuración.
6. **exec-timeout 0 0**: Este comando establece el tiempo de espera de la sesión de consola en cero. Esto significa que la sesión de consola no se cerrará automáticamente.
7. **logging synchronous**: Este comando hace que los mensajes de registro se muestren en la pantalla del usuario sin interrumpir la entrada de comandos en la línea de comando.

1.1. Configuración y ajustes básicos en los switches

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

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

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

Para D1, D2 y A1

1. **hostname**: Este comando establece el nombre del switch . El nombre se utiliza para identificar el dispositivo en la red.
2. **ipv6 unicast-routing**: Este comando habilita el enrutamiento unicast IPv6 en el switch. Esto permite que el switch enrute paquetes IPv6 en la red.

3. **no ip domain lookup**: Este comando desactiva la resolución de nombres DNS en el switch. Esto ayuda a evitar retrasos en la entrada de comandos en la línea de comando.
4. **banner motd # A1, ENCOR Skills Assessment, Scenario 2 #**: Este comando establece un mensaje del día (MOTD) en el switch. El mensaje es "# A1, ENCOR Skills Assessment, Scenario 2 #". El MOTD se muestra en la pantalla cuando un usuario se conecta al switch.
5. **line con 0**: Este comando configura la línea de consola del switch para su configuración.
6. **exec-timeout 0 0**: Este comando establece el tiempo de espera de la sesión de consola en cero. Esto significa que la sesión de consola no se cerrará automáticamente.
7. **logging synchronous**: Este comando hace que los mensajes de registro se muestren en la pantalla del usuario sin interrumpir la entrada de comandos en la línea de comando.
8. **exit**: Este comando sale del modo de configuración de línea y vuelve al modo de usuario normal del switch.
9. **vlan 8**: Este comando crea una nueva VLAN con el identificador numérico 8.
10. **name General-Users**: Este comando establece el nombre "General-Users" para la VLAN recién creada. Esto ayuda a identificar el propósito de la VLAN en la red.
11. **exit**: Este comando sale del modo de configuración VLAN y vuelve al modo de configuración normal del switch.

- Guarde las configuraciones en cada uno de los dispositivos.

  Comando abreviado

  Copy run st

  R1#copy run st

  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#

R2#copy run st

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#

R3#copy run st

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#

D1#copy run st

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...

Compressed configuration from 1432 bytes to 868 bytes[OK]

D1#

D2#copy run st

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...

Compressed configuration from 1432 bytes to 873 bytes[OK]

A1#copy run st

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...

Compressed configuration from 1432 bytes to 868 bytes[OK]

El comando "copy run st" , "copy running-config startup-config" o simplemente "wr" (abreviatura de "write memory"), son comandos equivalentes para guardar la configuración actual en la memoria no volátil del dispositivo. Estos comandos son importantes para guardar cualquier cambio de configuración que se haya realizado en el dispositivo y asegurarse de que se mantenga después de un reinicio.

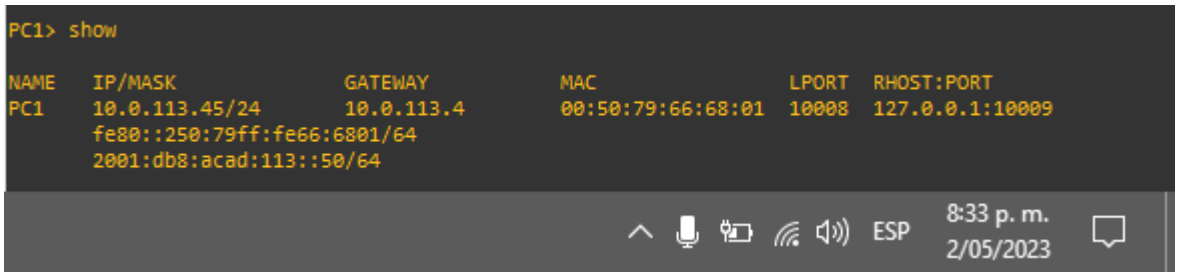
- Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento

PC1

ip 10.0.113.45/24 10.0.113.4

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

Figura 3 Configuracion IP en PC1



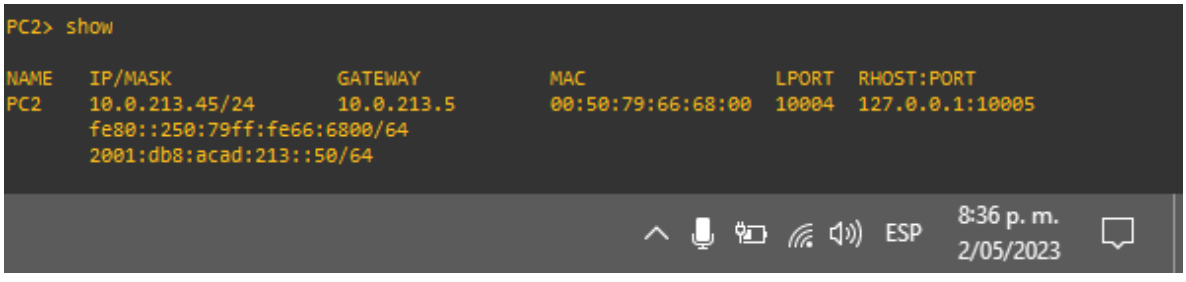
Fuente. Autoria propia

PC2

ip 10.0.213.45/24 10.0.213.5

ip 2001:db8:acad:213::50/64

Figura 4 Configuracion IP en PC2



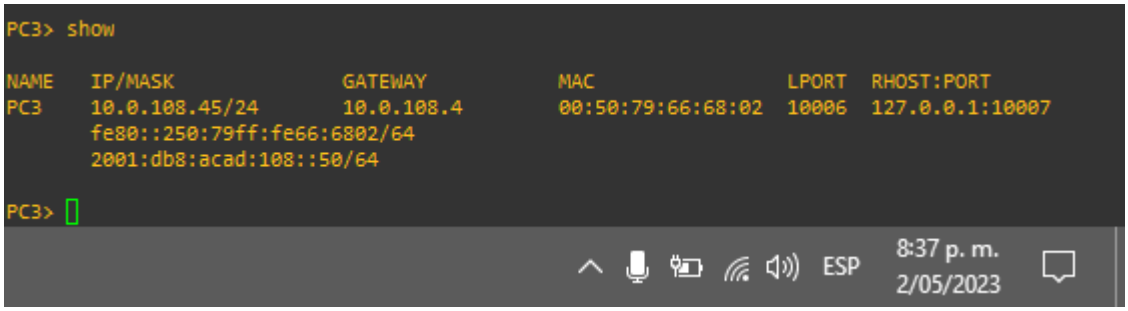
Fuente. Autoria propia

PC3

ip 10.0.108.45/24 10.0.108.4

ip 2001:db8:acad:108::50/64

Figura 5 Configuracion IP en PC3



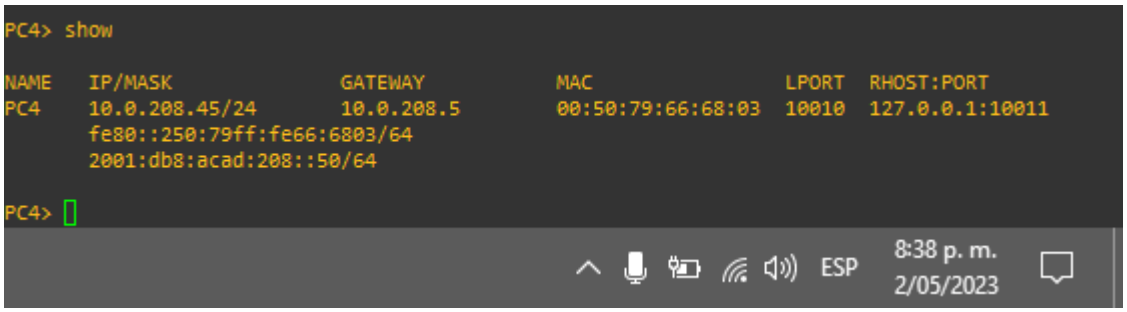
Fuente. Autoria propia

PC4

ip 10.0.208.45/24 10.0.208.5

ip 2001:db8:acad:208::50/64

Figura 6 Configuracion IP en PC4



Fuente. Autoria propia

Parte 2: configurar VRF y enrutamiento estático.

En esta parte de la evaluación de habilidades, configurará VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF.

Tabla 2.Evaluación de habilidades

Task#	Task	Specification
2.1	On R1, R2, and R3, configure VRF-Lite VRFs as shown in the topology diagram.	Configure two VRFs: • General-Users • Special-Users The VRFs must support IPv4 and IPv6.
2.2	On R1, R2, and R3, configure IPv4 and IPv6 interfaces on each VRF as detailed in the addressing table above.	All routers will use Router-On-A-Stick on theire1/1.x interfaces to support separation of the VRFs. Sub-interface 1: • In the Special Users VRF • Use dot1q encapsulation • IPv4 and IPv6 GUA and link-local addresses • Enable the interfaces Sub-interface 2: • In the General Users VRF • Use dot1q encapsulation • IPv4 and IPv6 GUA and link-local addresses • Enable the interfaces
2.3	On R1 and R3, configure default static routes pointing to R2.	Configure VRF static routes for both IPv4 andIPv6 in both VRFs.
2.4	Verify connectivity in each VRF.	From R1, verify connectivity to R3: • ping vrf General-Users 10.0.208.Z • ping vrf General-Users 2001:db8:acad:208::1 • ping vrf Special-Users 10.0.213.Z • ping vrf Special-Users 2001:db8:acad:213::1

Fuente. Autoria.

2.1 Configuración VRF-Lite y VRFs en R1, R2 y R3, como se muestra en la topología del diagrama.

Configuración Router R1

```
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
```

Configuración Router R2

```
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
```

Configuración Router R3

vrf definition General-Users

address-family ipv4

address-family ipv6

exit

vrf definition Special-Users

address-family ipv4

address-family ipv6

exit

Para los router R1, R2 y R3.

1. **vrf definition General-Users**: Este comando crea una instancia de VRF llamada "General-Users". Una instancia de VRF es una versión virtual de un enrutador que permite a varias instancias de VRF compartir el mismo hardware físico pero mantener rutas de enrutamiento separadas.
2. **address-family ipv4**: Este comando especifica que la instancia de VRF "General-Users" usará el protocolo IPv4. Esto permite que los dispositivos en la VRF se comuniquen entre sí utilizando IPv4.
3. **address-family ipv6**: Este comando especifica que la instancia de VRF "General-Users" usará el protocolo IPv6. Esto permite que los dispositivos en la VRF se comuniquen entre sí utilizando IPv6.
4. **exit**: Este comando sale del modo de configuración de la instancia de VRF "General-Users" y vuelve al modo de configuración global.
5. **vrf definition Special-Users**: Este comando crea otra instancia de VRF llamada "Special-Users".
6. **address-family ipv4**: Este comando especifica que la instancia de VRF "Special-Users" usará el protocolo IPv4.
7. **address-family ipv6**: Este comando especifica que la instancia de VRF "Special-Users" usará el protocolo IPv6.

8. **exit**: Este comando sale del modo de configuración de la instancia de VRF "Special-Users" y vuelve al modo de configuración global.

2.2 Configuración de las interfaces IPv4 e IPv6 en R1, R2 y R3 para cada

Tabla 3.Direccionamiento.

Configuración Router R1	**Descripcion**
interface e1/0.1	Configuración de la sub-interface e1/0.1
encapsulation dot1q 13	Encapsulamiento en protocolo IEEE 802.1Q
vrf forwarding Special-Users	Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.
ip address 10.0.12.4	Asignación de la dirección IPv4.
255.255.255.0	Asignación de la dirección IPv6.
ipv6 address fe80::1:1 link-local	Activación de la interfaz.
ipv6 address 2001:db8:acad:12::1/64	
no shutdown	
exit	
interface e1/0.2	Configuración de la sub-interface e1/0.2
encapsulation dot1q 8	Encapsulamiento en protocolo IEEE 802.1Q
vrf forwarding General-Users	Se crea la instancia para la tabla de enrutamiento de la VFR General-Users.
ip address 10.0.12.4	Asignación de la dirección IPv4.
255.255.255.0	Asignación de la dirección IPv6.
ipv6 address fe80::1:2 link-local	Activación de la interfaz
ipv6 address 2001:db8:acad:12::1/64	
no shutdown	
exit	
interface e1/1.1	Configuración de la sub-interface e1/1.1
encapsulation dot1q 13	Encapsulamiento en protocolo IEEE 802.1Q
vrf forwarding Special-Users	Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.
ip address 10.0.113.4	Asignación de la dirección IPv4.
255.255.255.0	Asignación de la dirección IPv6.
ipv6 address fe80::1:3 link-local	Activación de la interfaz.

ipv6 address 2001:db8:acad:113::1/64 no shutdown exit	
interface e1/1.2 encapsulation dot1q 8 vrf forward General-Users ip address 10.0.108.4 255.255.255.0 ipv6 address fe80::1:4 link-local ipv6 address 2001:db8:acad:108::1/64 no shutdown exit	Configuración de la sub-interface e1/1.2 Encapsulamiento en protocolo IEEE 802.1Q Se crea la instancia para la tabla de enrutamiento de la VFR General-Users. Asignación de la dirección IPv4. Asignación de la dirección IPv6. Activación de la interfaz.

Configuración Router R2	**Descripción**
interface e1/0.1 encapsulation dot1q 13 vrf forwarding Special-Users ip address 10.0.12.5 255.255.255.0 ipv6 address fe80::2:1 link-local ipv6 address 2001:db8:acad:12::2/64 no shutdown exit	Configuración de la sub-interface e1/0.1 Encapsulamiento en protocolo IEEE 802.1Q Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users. Asignación de la dirección IPv4. Asignación de la dirección IPv6. Activación de la interfaz.
interface e1/0.2 encapsulation dot1q 8 vrf forwarding General-Users ip address 10.0.12.5 255.255.255.0 ipv6 address fe80::2:2 link-local	Configuración de la sub-interface e1/0.2 Encapsulamiento en protocolo IEEE 802.1Q Se crea la instancia para la tabla de enrutamiento de la VFR General-Users. Asignación de la dirección IPv4. Asignación de la dirección IPv6. Activación de la interfaz

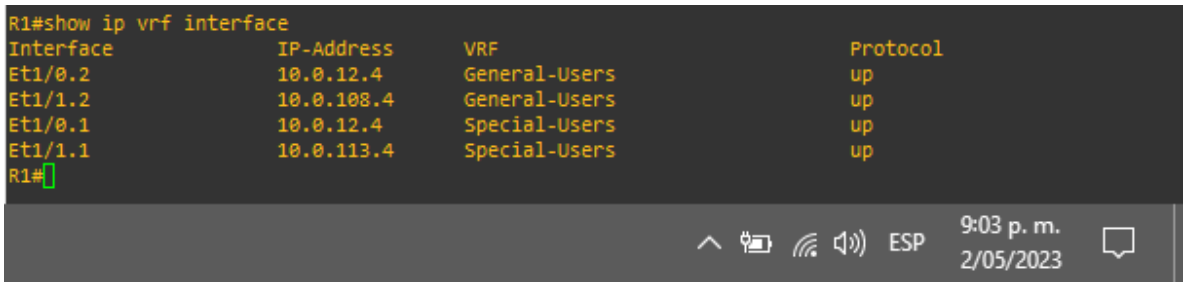
ipv6 address 2001:db8:acad:12::2/64	
no shutdown	
exit	
	Configuración de la sub-interface e1/1.1
interface e1/1.1	Encapsulamiento en protocolo IEEE 802.1Q
encapsulation dot1q 13	Se crea la instancia para la tabla de enrutamiento
vrf forwarding Special-Users	de la VFR Special-Users.
	Asignación de la dirección IPv4.
ip address 10.0.23.5 255.255.255.0	Asignación de la dirección IPv6.
	Activación de la interfaz.
ipv6 address fe80::2:3 link-local	
ipv6 address 2001:db8:acad:23::2/64	
no shutdown	
exit	
	Configuración de la sub-interface e1/1.2
interface e1/1.2	Encapsulamiento en protocolo IEEE 802.1Q
encapsulation dot1q 8	Se crea la instancia para la tabla de enrutamiento
vrf forwarding General-Users	de la VFR General-Users.
	Asignación de la dirección IPv4.
ip address 10.0.23.5 255.255.255.0	Asignación de la dirección IPv6.
	Activación de la interfaz.
ipv6 address fe80::2:4 link-local	
ipv6 address 2001:db8:acad:23::2/64	
no shutdown	
exit	

Configuración Router R3	**Descripción**
Interface e1/0.1	Configuración de la sub-interface e1/0.1
encapsulation dot1q 13	Encapsulamiento en protocolo IEEE 802.1Q
vrf forwarding Special-Users	Se crea la instancia para la tabla de enrutamiento
	de la VFR Special-Users.
ip address 10.0.23.6 255.255.255.0	Asignación de la dirección IPv4.
	Asignación de la dirección IPv6.
ipv6 address fe80::3:1 link-local	Activación de la interfaz.
ipv6 address 2001:db8:acad:23::3/64	

no shutdown	
exit	
interface e1/0.2	
encapsulation dot1q 8	Configuración de la sub-interface e1/0.2
vrf forwarding General-Users	Encapsulamiento en protocolo IEEE 802.1Q Se crea la instancia para la tabla de enrutamiento de la VFR General-Users.
ip address 10.0.23.6 255.255.255.0	Asignación de la dirección IPv4.
ipv6 address fe80::3:2 link-local	Asignación de la dirección IPv6.
ipv6 address 2001:db8:acad:23::3/64	Activación de la interfaz
no shutdown	
exit	
interface e1/1.1	
encapsulation dot1q 13	Configuración de la sub-interface e1/1.1
vrf forwarding Special-Users	Encapsulamiento en protocolo IEEE 802.1Q Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.
ip address 10.0.213.5 255.255.255.0	Asignación de la dirección IPv4.
ipv6 address fe80::3:3 link-local	Asignación de la dirección IPv6.
ipv6 address 2001:db8:acad:213::1/64	Activación de la interfaz.
no shutdown	
exit	
interface e1/1.2	
encapsulation dot1q 8	Configuración de la sub-interface e1/1.2
vrf forward General-Users	Encapsulamiento en protocolo IEEE 802.1Q
ip address 10.0.208.5 255.255.255.0	Se crea la instancia para la tabla de enrutamiento de la VFR General-Users.
ipv6 address fe80::3:4 link-local	Asignación de la dirección IPv4.
ipv6 address 2001:db8:acad:208::1/64	Asignación de la dirección IPv6. Activación de la interfaz.
no shutdown	
exit	

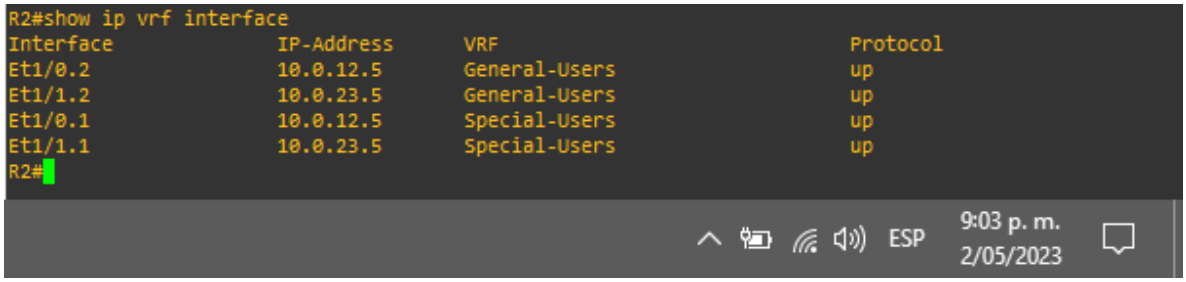
Fuente: Autoría Propia

Figura 7 Visualización de las subinterfaces en R1



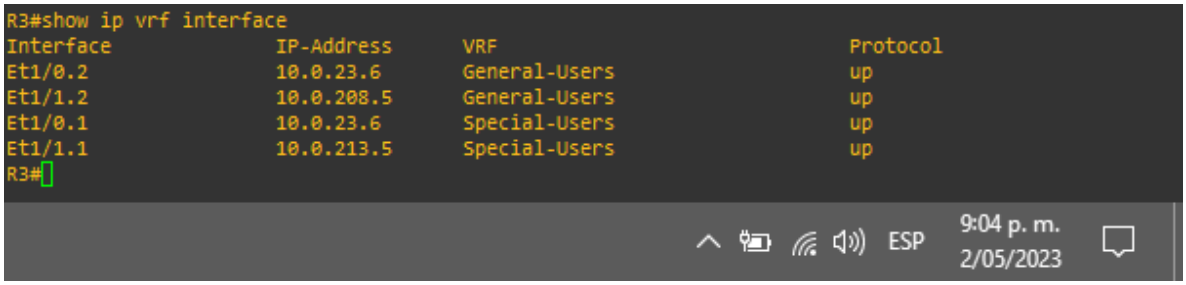
Fuente. Autoria propia

Figura 8 Visualización de las subinterfaces en R2



Fuente. Autoria propia

Figura 9 Visualización de las subinterfaces en R3



Fuente. Autoria propia

2.3 Configuración de las rutas estáticas predeterminadas que apuntan a R2, en R1 y R3.

R1

ip route vrf Special-Users 10.0.23.0 255.255.255.0 10.0.12.5

ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.12.5

ipv6 route vrf Special-Users 2001:db8:acad:23::1/64 2001:db8:acad:12::2

ipv6 route vrf Special-Users 2001:db8:acad:213::1/64 2001:db8:acad:12::2

ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.5

ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.5

ipv6 route vrf General-Users 2001:db8:acad:23::2/64 2001:db8:acad:12::2

ipv6 route vrf General-Users 2001:db8:acad:208::2/64 2001:db8:acad:12::2

end

R2

ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.4

ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.6

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

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

ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.4

ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.6

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

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

exit

R3

ip route vrf Special-Users 10.0.12.0 255.255.255.0 10.0.23.5

ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.23.5

ipv6 route vrf Special-Users 2001:db8:acad:12::1/64 2001:db8:acad:23::2

ipv6 route vrf Special-Users 2001:db8:acad:113::1/64 2001:db8:acad:23::2

ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.5

ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.5

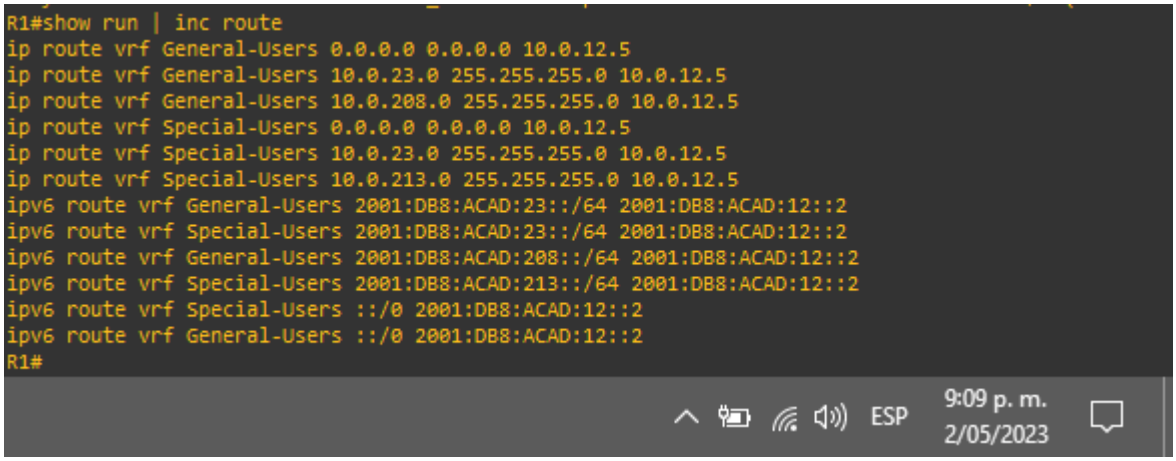
ipv6 route vrf General-Users 2001:db8:acad:12::1/64 2001:db8:acad:23::2

ipv6 route vrf General-Users 2001:db8:acad:108::1/64 2001:db8:acad:23::2

exit

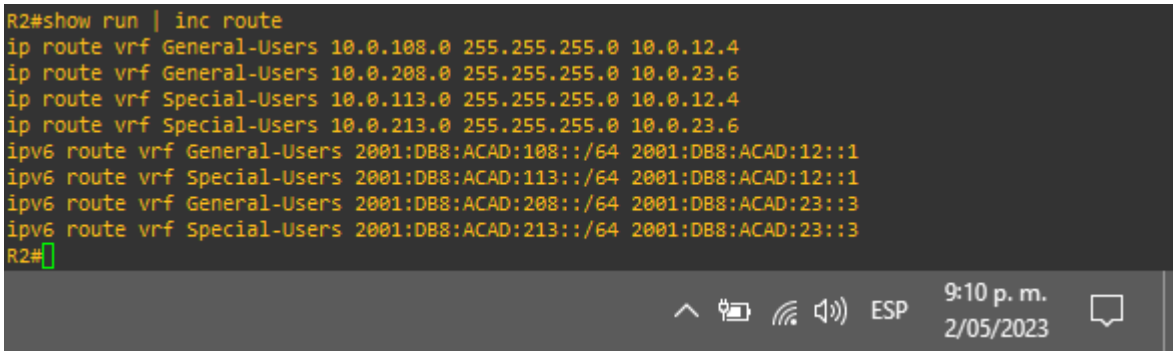
La visualización de configuración de dichas rutas se observa a continuación:

Figura 10 Visualización de rutas configuradas en R1



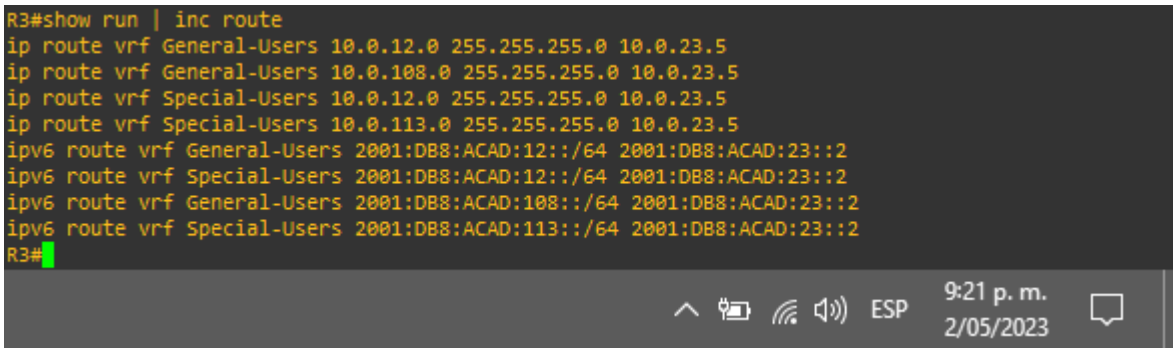
Fuente. Autoria propia

Figura 11 Visualización de rutas configuradas en R2



Fuente. Autoria propia

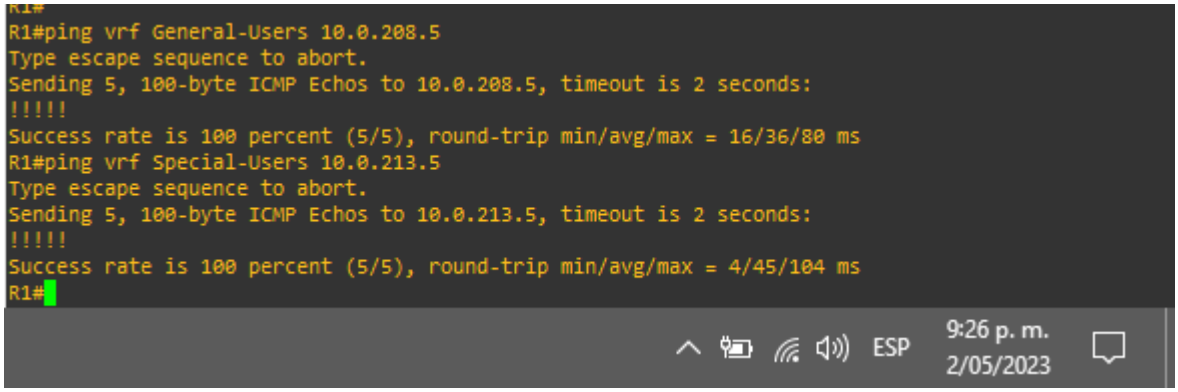
Figura 12 Visualización de rutas configuradas en R3



Fuente. Autoria propia

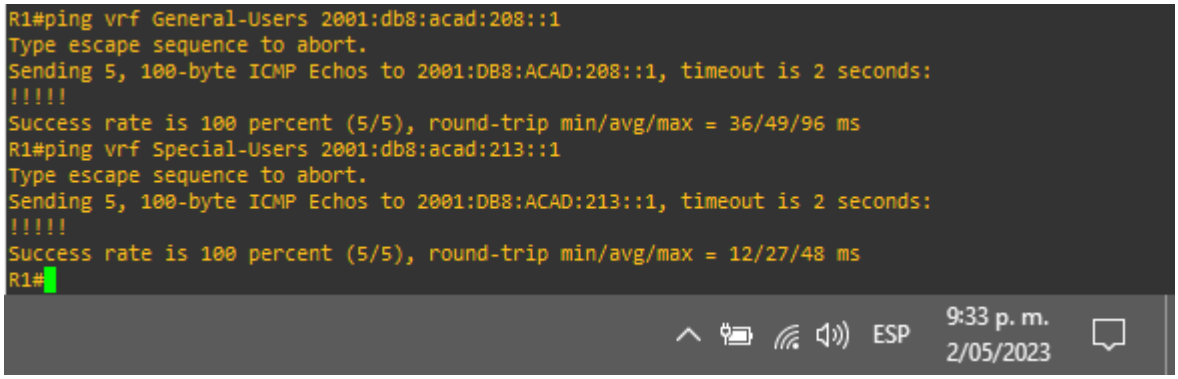
2.4 Verificar la conectividad en VRF

Figura 13 Prueba de ping IPv4 de R1 a R3



Fuente. Autoria propia.

Figura 14 Prueba de ping IPv6 de R1 a R3



Fuente. Autoria propia.

Parte 3: Configurar capa 2.

En esta parte de la evaluación de habilidades, se configurará los switches para que tengan soporte de conectividad con los dispositivos finales o hosts, las tareas a realizar son:

Tabla 4. Evaluación de habilidades para configurar la capa 2.

Task#	Task	Specification
3.1	On D1, D2, and A1, disable all interfaces.	
3.2	On D1 and D2, configure the trunk links to R1 and R3.	Configure and enable the e0/3 link as a trunk link.
3.3	On D1 and A1, configure the EtherChannel.	On D1, configure and enable: • Interface e0/0 and e0/1 • Port Channel 1 using PAgP On A1, configure enable: • Interface E0/0 and E0/1 • Port Channel 1 using PAgP
3.4	On D1, D2, and A1, configure access ports for PC1, PC2, PC3, and PC4.	Configure and enable the access ports as follows: • On D1, configure interface E0/3 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface E0/2 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface E0/1 as an access port in VLAN 8 and enable Portfast. • On A1, configure interface E0/2 as an access port in VLAN 8 and enable Portfast.
3.5	Verify PC to PC connectivity.	From PC1, verify IPv4 and IPv6 connectivity to PC2. From PC3, verify IPv4 and IPv6 connectivity to PC4.

Fuente. Autoria

3.1 Desactivar las interfaces en los switches D1, D2 y A1.

Como se observa en la tabla 4, se requiere desactivar las interfaces de dichos switches que, en este caso, según el diagrama de guía son interfaces ethernet y no giga, con esto claro se emplea las configuraciones.

Configuración Switch D1

conf t

interface range e1/0-3,e2/0-3,e3/0-3

shutdown

exit

Configuración Switch D2

conf t

interface range e1/0-3,e2/0-3,e3/0-3

shutdown

exit

Configuración Switch A1

conf t

interface range e1/0-3,e2/0-3,e3/0-3

shutdown

exit

Para los switches D1, D2 y A1.

1. **conf t**: Este comando accede a la configuración del dispositivo
2. **interface range**: Este comando especifica las interfaces que se deben apagar

3. **shutdown**: Apaga la interfaz donde se encuentra actualmente
4. **exit**: Este comando sale del modo de configuración o interfaz

3.2 En D1 y D2 configure los enlaces troncales para R1 y R3

Configuración Switch D1

conf t

interface range e0/2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

Configuración Switch D2

conf t

interface range e0/3

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

Para los switches D1 y D2.

1. **conf t**: Este comando accede a la configuración del dispositivo
2. **interface**: Este comando especifica la interfaz necesaria
3. **switchport trunk encapsulation dot1q**: Este comando especifica el tipo de encapsulación para el modo troncal
4. **switchport mode trunk**: Este comando activa la interfaz en modo troncal

5. **no shutdown**: Activa la interfaz donde se encuentra actualmente
6. **exit**: Este comando sale del modo de configuración o interfaz

3.3 En D1 y A1 configure EtherChannel

En la configuración de los switches mencionados, se configura mediante sus enlaces EtherChannel empleando PAgP usando el puerto de canal 1. Las configuraciones son:

Configuración Switch D1

conf t

interface range e0/0-1

switchport trunk encapsulation dot1q

switchport mode trunk

channel-group 1 mode desirable

no shutdown

exit

Configuración Switch A1

conf t

interface range e0/0-1

switchport trunk encapsulation dot1q

switchport mode trunk

channel-group 1 mode desirable

no shutdown

exit

Para los switches D1 y A1.

1. **conf t**: Este comando accede a la configuración del dispositivo
2. **interface range**: Este comando especifica el rango de interfaces necesarias
3. **switchport trunk encapsulation dot1q**: Este comando especifica el tipo de encapsulación para el modo troncal
4. **switchport mode trunk**: Este comando activa la interfaz en modo troncal
5. **channel-group 1 mode desirable**: Este comando establece los puertos agrupados para modo activo, negocia cuando se reciban paquetes PAgP
6. **no shutdown**: Activa la interfaz donde se encuentra actualmente
7. **exit**: Este comando sale del modo de configuración o interfaz

3.4 En D1, D2 y A1 configure los puertos de acceso para PC1, PC2, PC3 y PC4.

Se configura ahora los puertos de acceso en los switches con base a las VLAN configuradas anteriormente habilitando como puertos rápidos.

Configuración Switch D1

conf t

interface range e0/3

switchport mode access

switchport access vlan 13

spanning-tree portfast

no shutdown

exit

Configuración Switch D2

conf t

interface range e0/2

switchport mode access

switchport access vlan 13

spanning-tree portfast

no shutdown

exit

interface range e0/1

switchport mode access

switchport access vlan 8

spanning-tree portfast

no shutdown

exit

Configuración Switch A1

conf t

interface range e0/2

switchport mode access

switchport access vlan 8

spanning-tree portfast

no shutdown

exit

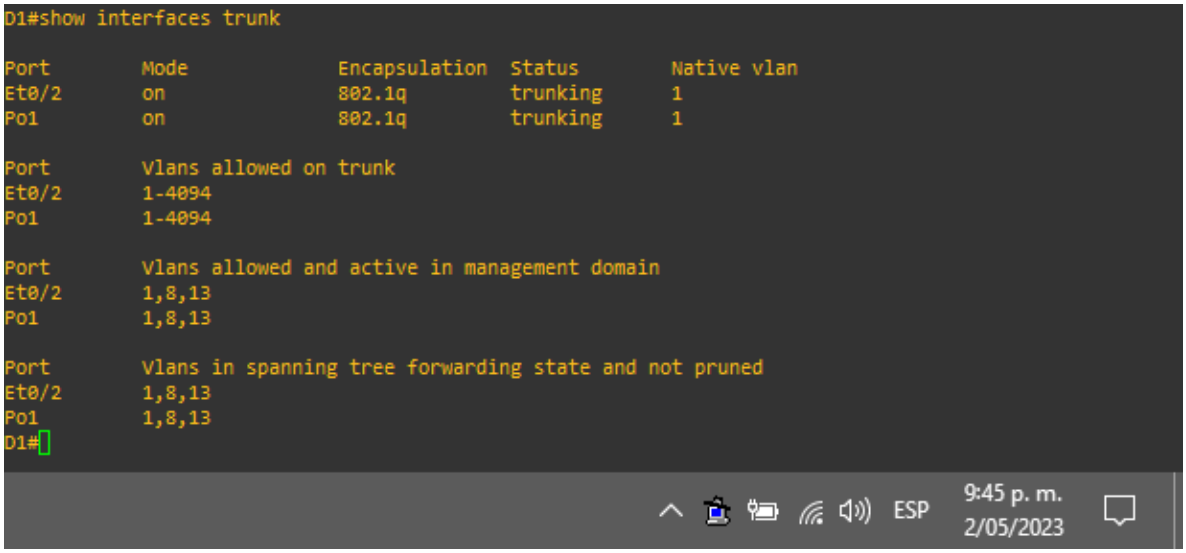
Para los switches D1, D2 y A1.

1. **conf t**: Este comando accede a la configuración del dispositivo
2. **interface range**: Este comando especifica el rango de interfaces necesarias
3. **switchport mode access**: Este comando establece el puerto en modo acceso.

4. **switchport access vlan** #: Este comando establece la vlan mencionada al puerto
5. **spanning-tree portfast**: Este comando establece protección por BPDU y modo portfast o puerto rapido.
6. **no shutdown**: Activa la interfaz donde se encuentra actualmente
7. **exit**: Este comando sale del modo de configuración o interfaz

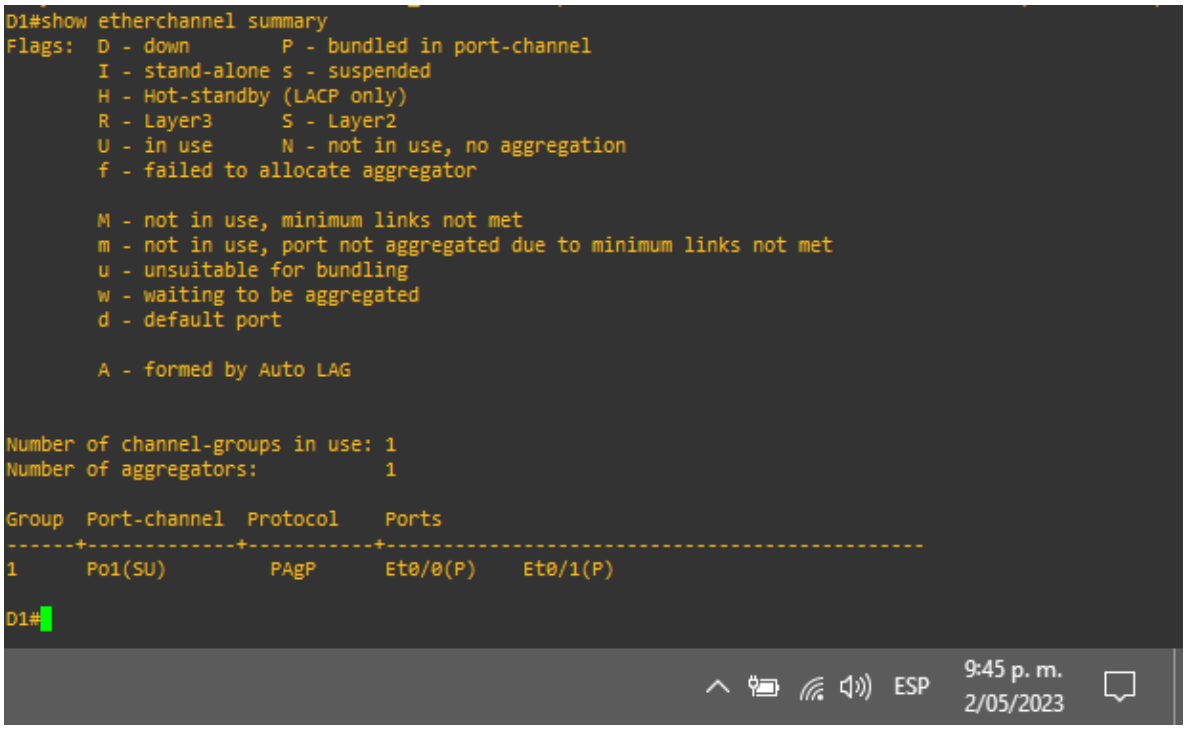
A partir de estas configuraciones se procede a observar los registros mediante el comando show:

Figura 15 Visualización de interfaz troncal en D1



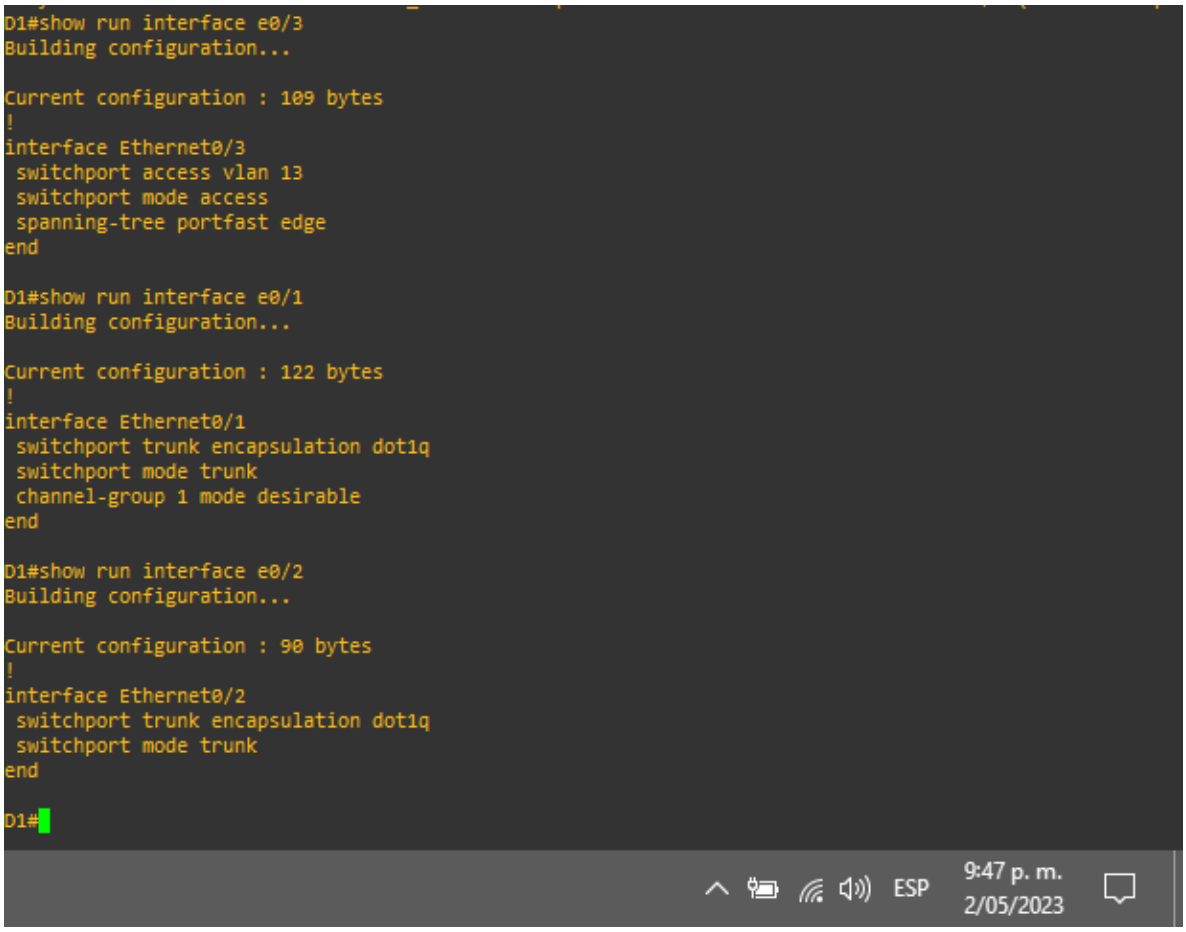
Fuente. Autoria propia.

Figura 16 Visualización de etherchannel en D1



Fuente. Autoria propia.

Figura 17 Visualización de interfaces de D1

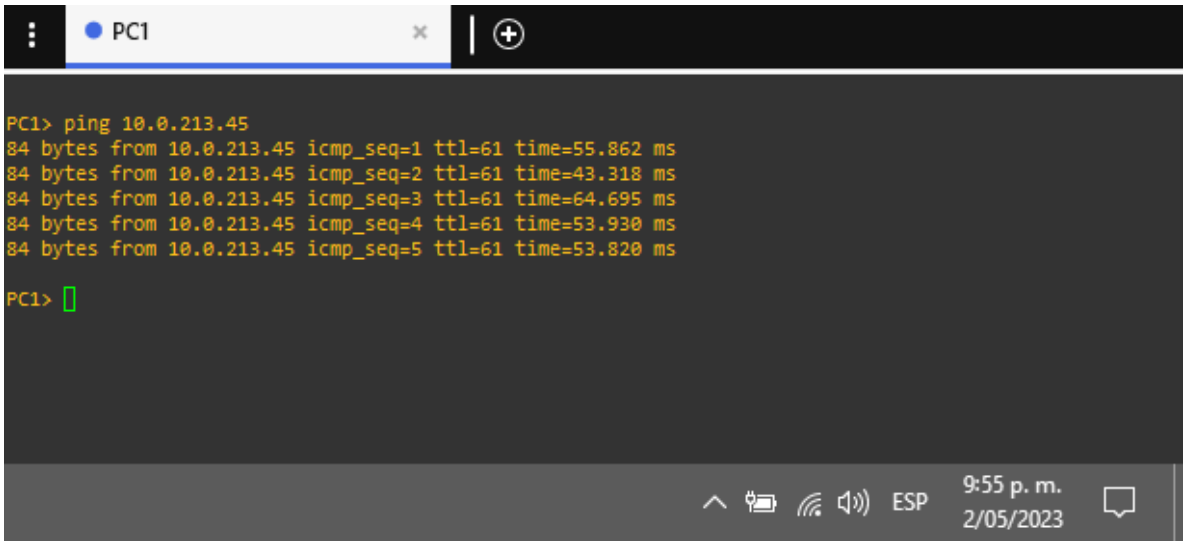


Fuente. Autoria propia

3.5 Verificar la conectividad de PC a PC.

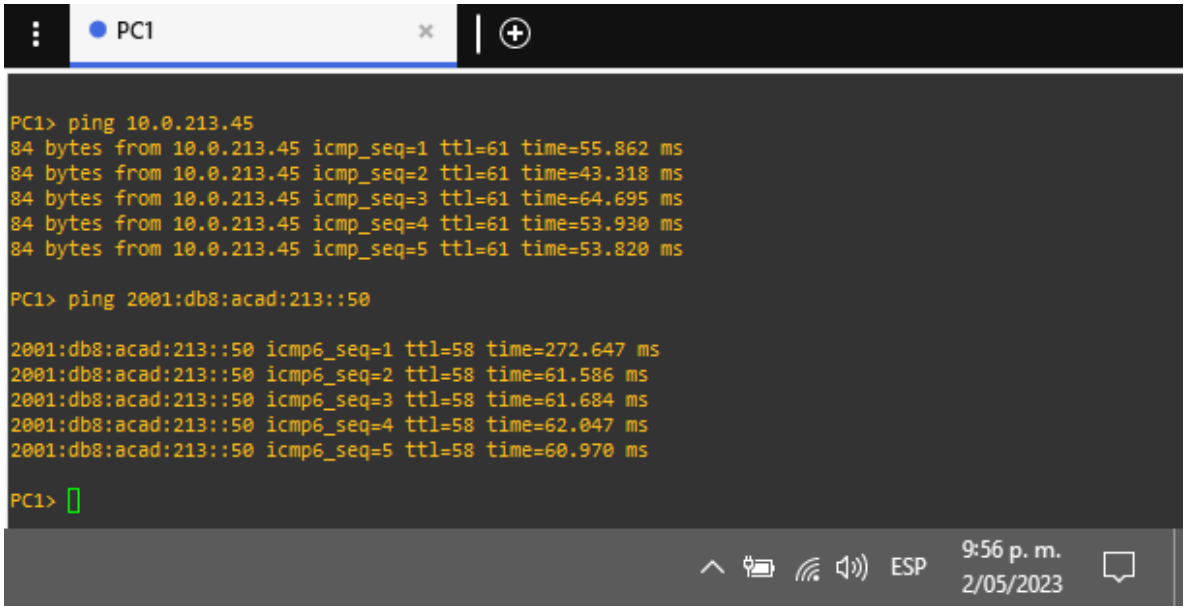
Luego de las configuraciones anteriores, se procede a comprobar que exista conexión o conectividad entre los equipos con pruebas de ping para IPv4 e IPv6.

Figura 18 Prueba de ping IPv4 desde PC1 a PC2



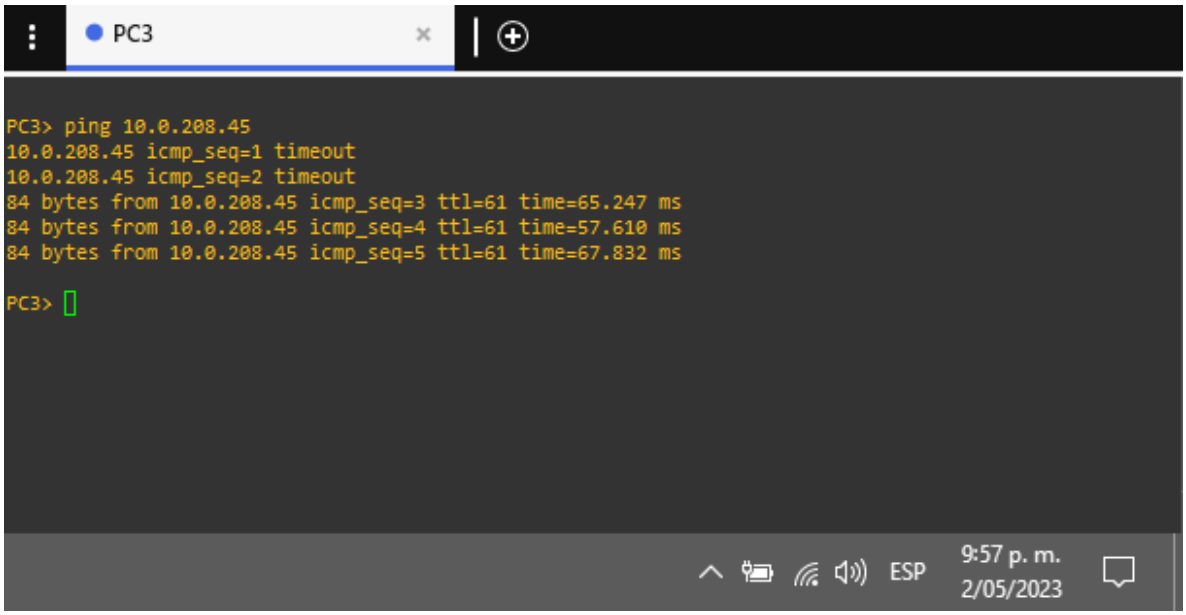
Fuente. Autoria propia.

Figura 19 Prueba de ping IPv6 desde PC1 a PC2



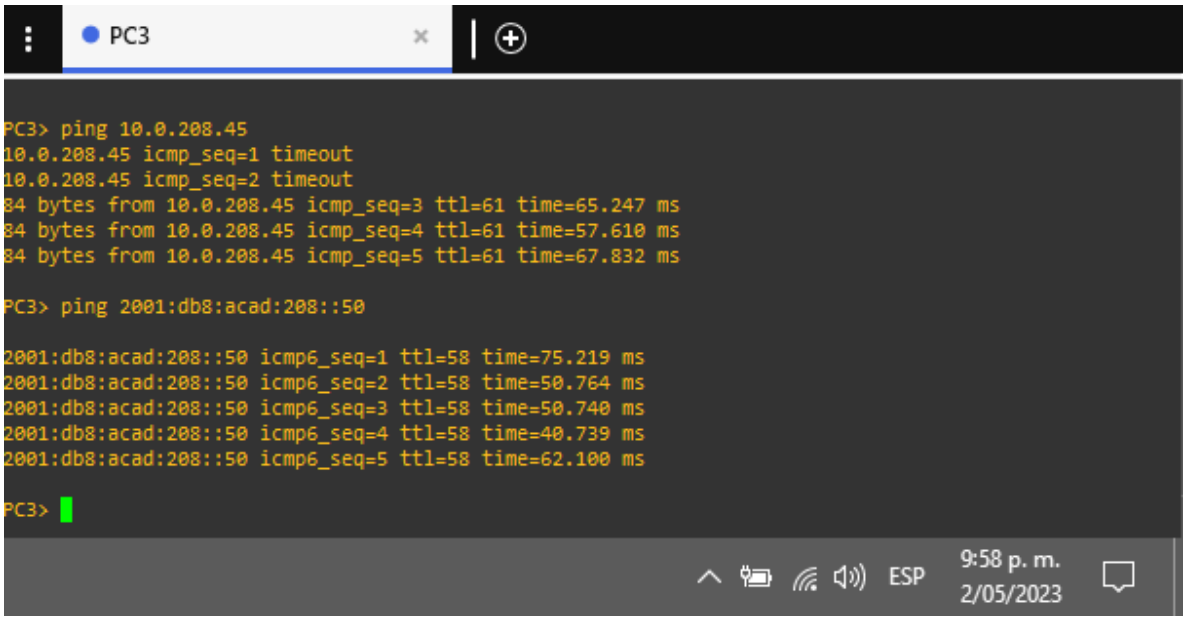
Fuente. Autoria propia.

Figura 20 Prueba de ping IPv4 desde PC3 a PC4



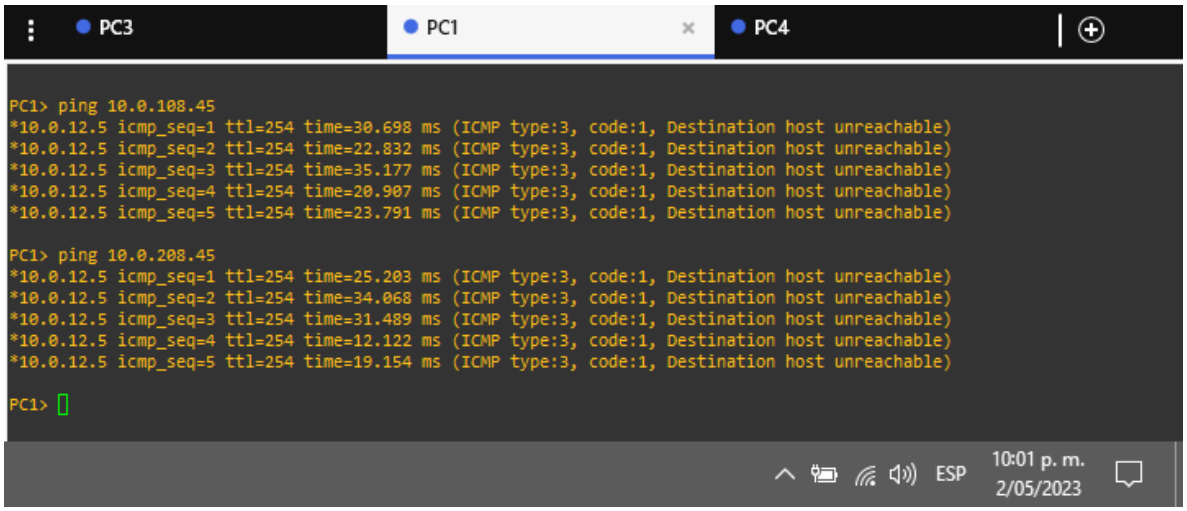
Fuente. Autoria

Figura 21 Prueba de ping IPv6 desde PC3 a PC4



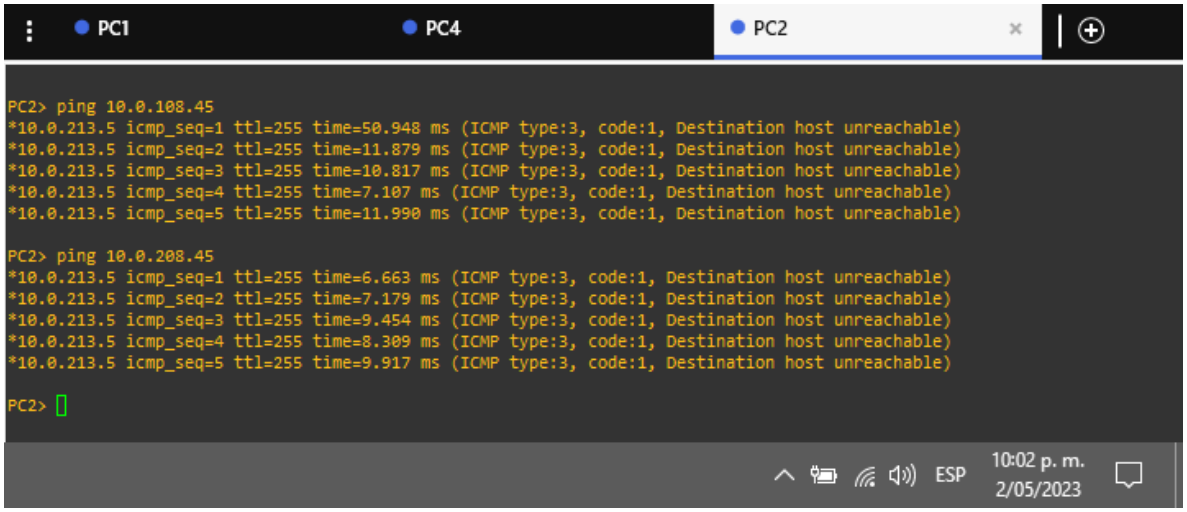
Fuente. Autoria

Figura 22 Prueba de ping IPv4 desde PC1 a PC3 y PC4



Fuente. Autoria propia

Figura 23 Prueba de ping IPv6 desde PC2 a PC3 y PC4



Fuente. Autoria propia

Parte 4: Configurar seguridad

Finalmente, para la cuarta parte de la evaluación de habilidades, se configurará varios mecanismos de seguridad en cada uno de los dispositivos de la topología de la red, dichas tareas se presentan a continuación.

Tabla 5.Evaluación de habilidades para configurar seguridad.

Task#	Task	Specification
4.1	On all devices, secure privileged EXE mode.	Configure an enable secret as follows: • Algorithm type: **SCRYPT** • Password: **nombreestudianteXYZ**.
4.2	On all devices, create a local user account.	Configure a local user: • Name: **admin** • Privilege level: **15** • Algorithm type: **SCRYPT** • Password: **nombrestudianteXYZ**.
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the localdatabase on all lines.

4.1 En todos los dispositivos, configurar modo EXEC privilegiado.

Como se observa en la tabla 5, para todos los dispositivos se emplea la encriptación por algoritmo CRYPT con una contraseña en específico.

Configuración router R1

conf t

enable algorithm-type scrypt secret jamesmora455

exit

Configuración router R2

conf t

enable algorithm-type scrypt secret jamesmora455

exit

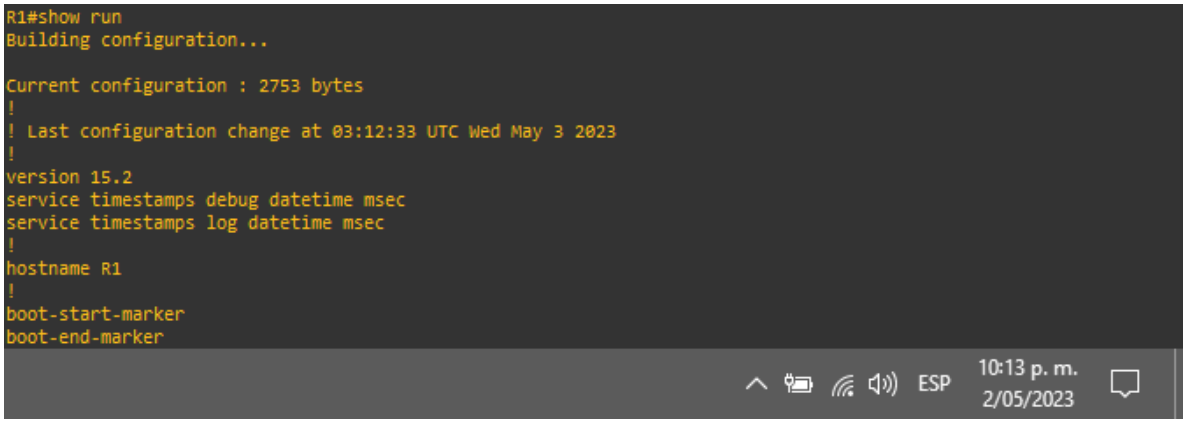
Configuración router R3

conf t

enable algorithm-type scrypt secret jamesmora455

exit

Figura 24 Versión IOS de los routers empleados



Fuente. Autoria propia

Figura 25 Ingreso del comando presentando error

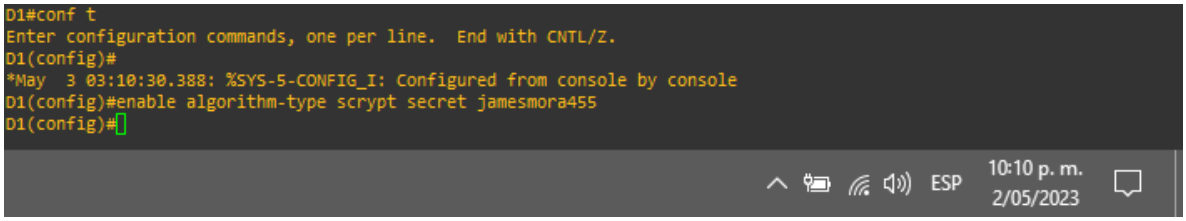
Fuente. Autoria propia

Figura 26 Explicación de introducción del encriptado SCRYPT desde versión 15.3

Therefore, look at the figure above again, you see ***type 8 or type 9 passwords,*** they are the recommended method of configuring all secret passwords (using either) . But both were introduced in Cisco IOS 15.3(3)M and later. They also use SHA encryption and type 9 is slightly stronger than type 8.

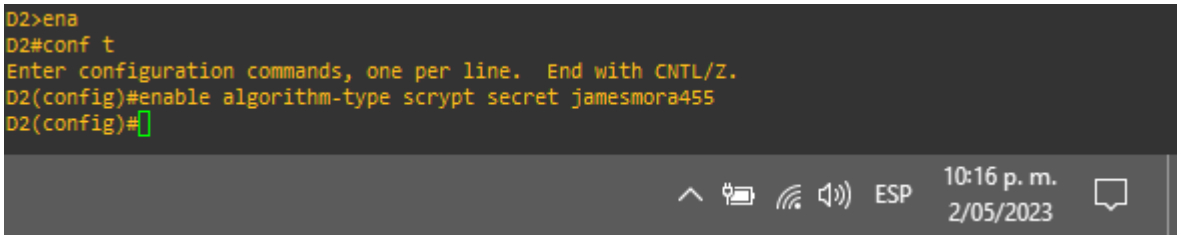
Fuente: https://www.linkedin.com/pulse/enable-secret-password-algorithms-md5-sha256-scrypt-michael-akintola/

Figura 27 Ingreso del comando en el router D1



Fuente. Autoria propia.

Figura 28 Ingreso del comando en el router D2



Fuente. Autoria propia.

Para los routers R1, R2,R3, D1 y D2.

1. **conf t**: Este comando accede a la configuración del dispositivo
2. **enable algorithm-type scrypt secret #**: Este comando especifica el algoritmo de encriptado scrypt y la contraseña en cuestión.
3. **exit**: Este comando sale del modo de configuración o interfaz

4.2 En todos los dispositivos, crear una cuenta de usuario local

Como se observa en la tabla 5, se configura un usuario local con nombre “admin” un valor de privilegio de 15, algoritmo de encriptación scrypt y contraseña jamesmora455.

Configuración router R1

conf t

username admin privilege 15 algorithm-type SCRYPT secret jamesmora455

exit

Configuración router R2

conf t

username admin privilege 15 algorithm-type SCRYPT secret jamesmora455

exit

Configuración router R3

conf t

username admin privilege 15 algorithm-type SCRYPT secret jamesmora455

exit

Para los routers R1, R2 y R3.

1. **conf t**: Este comando accede a la configuración del dispositivo
2. **username admin privilege 15 algorithm-type SCRYPT secret** #: Este comando especifica el nombre de usuario, privilegio, algoritmo de encriptado scrypt y la contraseña en cuestión.
3. **exit**: Este comando sale del modo de configuración o interfaz

Al igual que los comandos de la sección 4.1, estos no son compatibles debido a la versión de los routers empleados en la topología.

4.3 En todos los dispositivos, habilite AAA y habilitar autentificación por AAA.

Como se observa en la tabla 5, se habilita la autentificación por AAA usando las bases de datos locales en todas las líneas

Configuración router R1

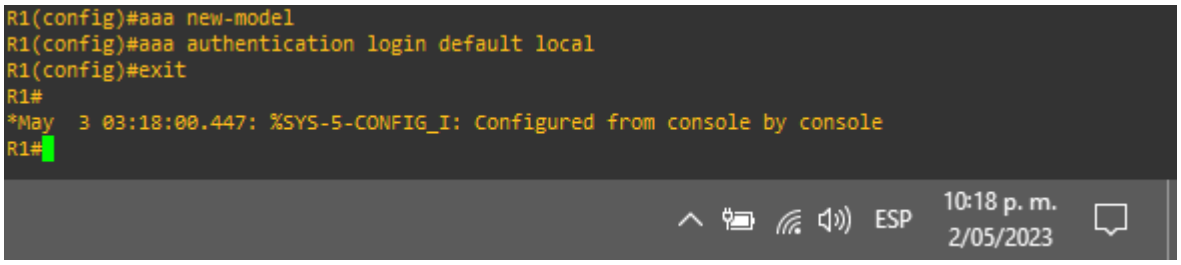
conf t

aaa new-model

aaa authentication login default local

exit

Figura 29 Configuracion de AAA y autentificación en R1



Fuente. Autoria propia

Configuración router R2

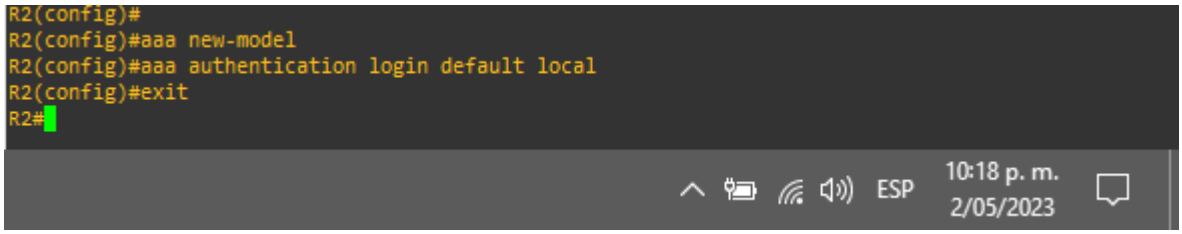
conf t

aaa new-model

aaa authentication login default local

exit

Figura 30 Configuracion de AAA y autentificación en R2



Fuente. Autoria propia

Configuración router R3

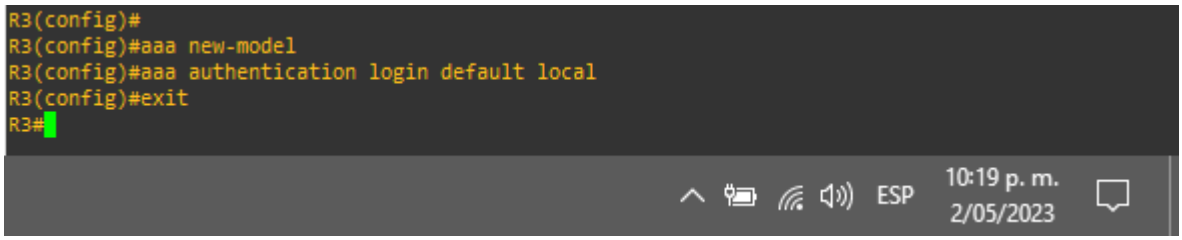
conf t

aaa new-model

aaa authentication login default local

exit

Figura 31 Configuracion de AAA y autentificación en R3

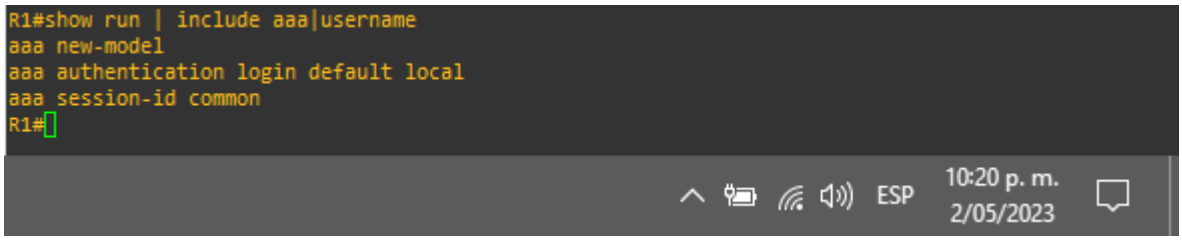


Fuente. Autoria propia

Para los routers R1, R2 y R3.

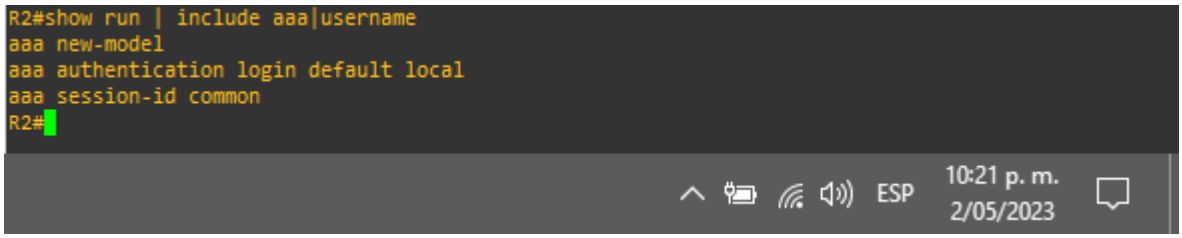
1. **conf t**: Este comando accede a la configuración del dispositivo
2. **aaa new-model**: Este comando habilita el uso de listas para el método de autentificación.
3. **aaa authentication login default local**: Este comando habilita la autentificación por AAA al iniciar sesión
4. **exit**: Este comando sale del modo de configuración o interfaz

Figura 32 Visualización de las configuraciones realizadas en R1



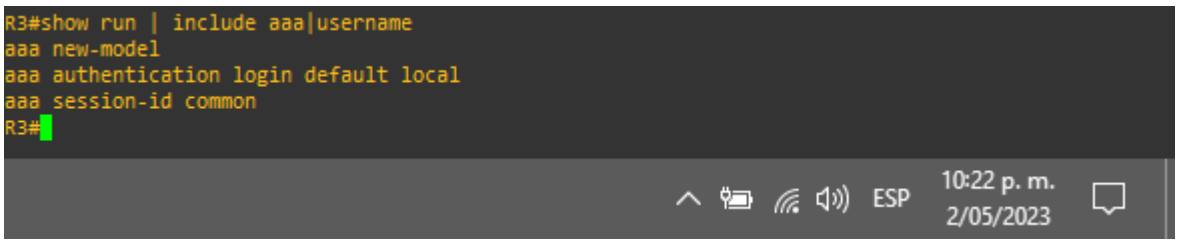
Fuente. Autoria propia

Figura 33 Visualización de las configuraciones realizadas en R2



Fuente. Autoria propia

Figura 34 Visualización de las configuraciones realizadas en R3



Fuente. Autoria propia

CONCLUSIONES

En conclusión, la configuración multi-VRF en GNS3 es una técnica avanzada de enrutamiento que permite la virtualización del plano de control y datos, creando múltiples tablas de enrutamiento y aislamiento de tráfico entre ellas. La configuración multi-VRF se utiliza en diferentes escenarios, como redes corporativas, proveedores de servicios de Internet o redes de centros de datos. Al utilizar la técnica multi-VRF, se pueden lograr beneficios como un mejor rendimiento, una mayor seguridad y una mayor eficiencia en el uso de los recursos de la red.

Se puede detallar como GNS3 es una herramienta útil para simular y probar configuraciones de red, permitiendo a los administradores de redes experimentar y validar diferentes configuraciones antes de implementarlas en una red real. La configuración multi-VRF en GNS3 implica la creación de instancias VRF, la configuración de interfaces, la configuración de las tablas de enrutamiento para cada instancia VRF, y la configuración de las rutas de enrutamiento entre las distintas instancias VRF.

Las configuraciones en la capa de red 2 permite detallar como nos permite asignar direccionamientos, asignación de protocolos y posteriormente garantizar conexión entre varios dispositivos de una topología de red. De igual manera, la autenticación AAA es un proceso crucial de seguridad para cualquier sistema de red o aplicación que maneja información confidencial. Se concluye que a partir de estos se logra garantizar la identidad del usuario y su acceso autorizado a recursos específicos, al tiempo que registra y supervisa las actividades de seguridad importantes.

REFERENCIAS BIBLIOGRAFICAS

SUÁREZ, M. (2017). Redes de área amplia: configuración avanzada en GNS3. México: Ediciones ENI.

LEÓN, R. (2018). Guía de práctica: Implementación de VRFs en routers Cisco. España: Editorial Alfaomega.

HIDALGO, J. (2017). Configuración avanzada de redes: VRF en GNS3. Madrid: Ediciones RA-MA.

HERNÁNDEZ, L. (2019). Redes de comunicaciones: Configuración de VRF en GNS3. México: Universidad Nacional Autónoma de México.

GONZÁLEZ, P. (2020). Configuración avanzada de VRF en GNS3 para redes empresariales. Chile: Editorial Universitaria de la Universidad de Chile.

PEÑA, L. (2018). VRF (Virtual Routing and Forwarding) [Sitio web]. [Consultado: 17 de abril de 2023]. Disponible en: https://community.cisco.com/t5/documentos-routing-y-switching/vrf-virtual-routing-and-forwarding/ta-p/3406835

ZUÑIGA, C. (2020). AAA - AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO [Sitio web]. [Consultado: 16 de abril de 2023]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/