

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

JOSE ELVER LOPEZ RODRIGUEZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
TUNJA
2023**

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

JOSE ELVER LOPEZ RODRIGUEZ

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

DIRECTOR:

JUAN ESTEBAN TAPIAS BAENA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES**

TUNJA

2023

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma de Jurado

Firma de Jurado

TUNJA, 04 de abril de 2023

AGRADECIMIENTOS

Como prioridad primero que todo a Dios por haberme guiado en los momentos difíciles, también darme mucha fortaleza de seguir siempre con la certeza de superarme y ser un ser útil para la sociedad, también de agradecerle que siempre estuvo en mis tropiezos y no dejarme renunciar al objetivo trazado que era culminar mis estudios.

También agradecerle a mi esposa Yuli que fue la persona que desde que tome la decisión de superarme fue la primera que me apoyo; también agradecerle a José

Mi padre, a Estrella mi madre, ellos personas incondicionales que a pesar de mi edad me impulsaban en esos momentos de debilidad.

Por último, agradecer a cada uno de esos profesionales de la universidad Nacional Abierta y a Distancia por su dedicación, paciencia, compromiso de guiar y enseñar y de esta forma culminar lo que era imposible por tantas dificultades

TABLA DE CONTENIDO

AGRADECIMIENTOS	4
LISTA DE FIGURAS	7
LISTA DE TABLAS	8
GLOSARIO	9
RESUMEN	10
ABSTRACT	10
INTRODUCCION	11
DESARROLLO DEL TRABAJO	12
Topología de la red	12
Escenario	12
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz	13
Paso 1. Cablee la red como se muestra en la topología.....	13
Paso 2: Configure los ajustes básicos para cada dispositivo.....	13
Configuración y ajustes básicos en los switches	16
Parte 2: configurar VRF y enrutamiento estático.	29
2.1 Configuración VRF-Lite y VRFs en R1, R2 y R3, como se muestra en la topología del diagrama.	29
2.2 Configuración de las interfaces IPv4 e IPv6 en R1, R2 y R3 para cada una. ..	33
2.3 Configuración de las rutas estáticas predeterminadas que apuntan a R2, en R1 y R3.	37
2.4 verificar la conectividad en VRF.....	40
Parte 3. Configurar Capa 2	41
3.1 On D1, D2, and A1, disable all interfaces.	41
3.2 On D1 and D2, configure the trunk links to R1 and R3	42
3.3 On D1 and A1, configure the EtherChannel.....	43
3.4 On D1, D2, and A1, configure access ports for PC1, PC2, PC3, and PC4.	45

Parte 4 configure Security.....47

4.1 On all devices, secure privileged EXE mode.47

4.2 On all devices, create a local user account.....48

4.3 On all devices, enable AAA and enable AAA authentication49

CONCLUSIONES51

REFERENCIAS BIBLIOGRAFICAS.....52

LISTA DE FIGURAS

Figura 1. Escenario 1	12
Figura 2.Simulación escenario GNS3	13
Figura 3.Configuración básica en R1	14
Figura 4.Configuración básica en R2.....	15
Figura 5.Configuración básica en R3.....	16
Figura 6.Configuración básica en D1	17
Figura 7.Configuración básica en D2.....	18
Figura 8.Configuración básica en A1	19
Figura 9.Configuración basica R1	20
Figura 10.Configuración básica R2.....	21
Figura 11.Configuración básica R3.....	22
Figura 12.Configuración básica D1	23
Figura 13.Configuración básica D2.....	23
Figura 14.Configuración básica A1	25
Figura 15.PC1	26
Figura 16.PC2.....	26
Figura 17.PC3.....	27
Figura 18.PC4.....	28
Figura 19.Router R1	30
Figura 20.Router R2	31
Figura 21.Router R3	32
Figura 22.Configuración Router R1	36
Figura 23.Configuración Router R2	36
Figura 24.Configuración Router R3	37
Figura 25.rutas estáticas R1	38
Figura 26.rutas estáticas R2	39
Figura 27.rutas estáticas R3	40
Figura 28.conectividad en VRF.....	40
Figura 29.conectividad en VRF	50

LISTA DE TABLAS

Tabla 1. Direccionamiento R1.....	33
Tabla 2. Direccionamiento R2.....	34
Tabla 3. Direccionamiento R3.....	35
Tabla 4. Configuración de ruta estática R1	37
Tabla 5. Configuración ruta estática R2	38
Tabla 6. Configuración ruta estática R3.....	39
Tabla 7. Configuración de interfaces.	41
Tabla 8. Configuración R1 y R3.....	42
Tabla 9. Configuración EtherChannel.....	43
Tabla 10. Configuración de acceso.....	45
Tabla 11. Conectividad.	46
Tabla 12. Modo privilegiado.	47
Tabla 13. Usuario local	48
Tabla 14. Habilitación y autenticación.....	49

GLOSARIO

SERVIDOR: Un servidor es un programa o dispositivo de computadora que proporciona servicios a otros dispositivos o programas llamados clientes en una red de computadoras. Los servidores pueden proporcionar una variedad de servicios, como almacenamiento de archivos, correo electrónico, servicios web y bases de datos.

DIRECCIÓN IP: Una dirección IP es un número que identifica de manera única un dispositivo conectado a una red de computadoras. Las direcciones IP se utilizan para enrutar el tráfico de red a través de Internet y otras redes.

FIREWALL: Un firewall es un software o dispositivo de hardware que se utiliza para proteger una red de computadoras contra amenazas externas. Los firewalls se utilizan para bloquear el tráfico no autorizado y permitir el tráfico autorizado a través de la red.

PROTOCOLO DE ENRUTADO: Un protocolo de enrutado es un conjunto de reglas que se utilizan para determinar la ruta que deben seguir los datos a través de una red de computadoras para llegar a su destino final. Los protocolos de enrutamiento se utilizan en redes IP para dirigir el tráfico de datos entre redes y subredes.

CONMUTADOR: Un conmutador es un dispositivo de red que se utiliza para conectar varios dispositivos de red juntos en una red local (LAN). Los conmutadores se utilizan para dirigir el tráfico de datos entre los dispositivos conectados, lo que permite una comunicación rápida y eficiente entre los dispositivos.

RESUMEN

En esta evaluación de habilidades se realiza la configuración de multi-VRF (Virtual Routing and Forwarding) en GNS3, que es una técnica avanzada de enrutamiento que permite la virtualización del plano de control y datos de una red, lo que genera múltiples tablas de enrutamiento y aísla el tráfico entre ellas. Esta configuración puede aplicarse a distintos escenarios, tales como redes corporativas con varios departamentos, servicios de proveedores de Internet (ISP) y redes de centros de datos. El uso de la técnica multi-VRF puede brindar beneficios como un mejor desempeño, mayor seguridad y eficiencia en la utilización de los recursos de red. GNS3, por su parte, es una herramienta valiosa para simular y probar configuraciones de red, lo que permite a los administradores experimentar y validar diferentes configuraciones antes de su implementación en una red real.

Palabras clave: CISCO, CCNP, conmutación, enrutamiento, GNS3, multi-VRF.

ABSTRACT

In this skills assessment, the configuration of multi-VRF (Virtual Routing and Forwarding) in GNS3 is performed, which is an advanced routing technique that allows the virtualization of the control plane and data of a network, which generates multiple routing tables. and isolates the traffic between them. This configuration can be applied to a variety of scenarios, such as corporate networks with multiple departments, Internet Service Providers (ISPs), and data center networks. The use of the multi-VRF technique can provide benefits such as better performance, greater security and efficiency in the use of network resources. GNS3, for its part, is a valuable tool for simulating and testing network configurations, allowing administrators to experiment and validate different configurations before their implementation on a real network.

Keywords: CISCO, CCNP, switching, routing, GNS3, multi-VRF.

INTRODUCCION

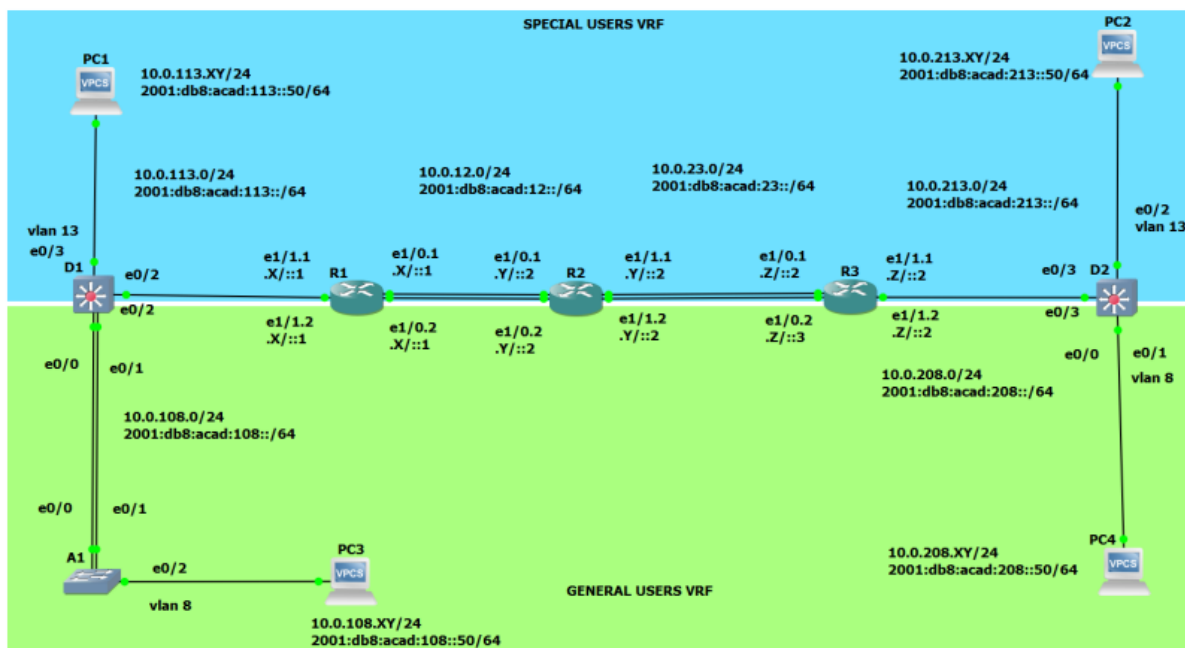
Durante la evaluación de habilidades actuales, se enfrenta un desafío en la configuración de redes de comunicaciones, específicamente en la implementación de una configuración multi-VRF para separar a dos grupos de usuarios, "Usuarios Generales" y "Usuarios Especiales", mediante el uso de VLANs. Se realizan ajustes en la configuración básica de los dispositivos de red para asignar direccionamiento IP a las interfaces que conectan los segmentos de red, seguido por la configuración de VRF-Lite en los tres enrutadores de la red y la asignación de rutas estáticas adecuadas para permitir la conectividad de extremo a extremo. Luego, se verifica la accesibilidad mediante comandos de ping desde R3 a cada VRF. El objetivo final es garantizar la accesibilidad completa de un extremo a otro en la red, mientras se mantiene el aislamiento entre los dos grupos de usuarios sin comunicación posible. Para lograr esto, se lleva a cabo una verificación detallada de las configuraciones para asegurarse de que cumplan con las especificaciones requeridas y que los dispositivos funcionen correctamente para resolver el problema. En resumen, la evaluación de habilidades en la configuración multi-VRF es un proceso desafiante que requiere un alto nivel de conocimientos y habilidades en redes de comunicaciones. Es fundamental comprender a fondo 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

Topología de la Red:



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.

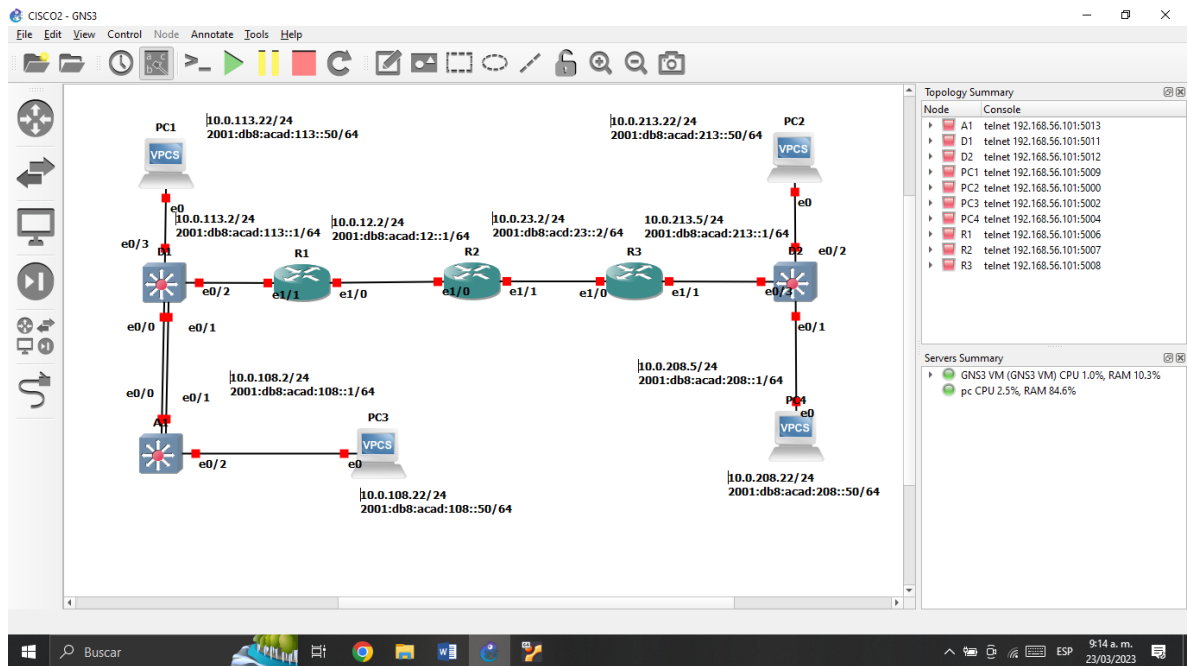
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz

En la Parte 1, se configura la topología de la red y se configuran 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 #

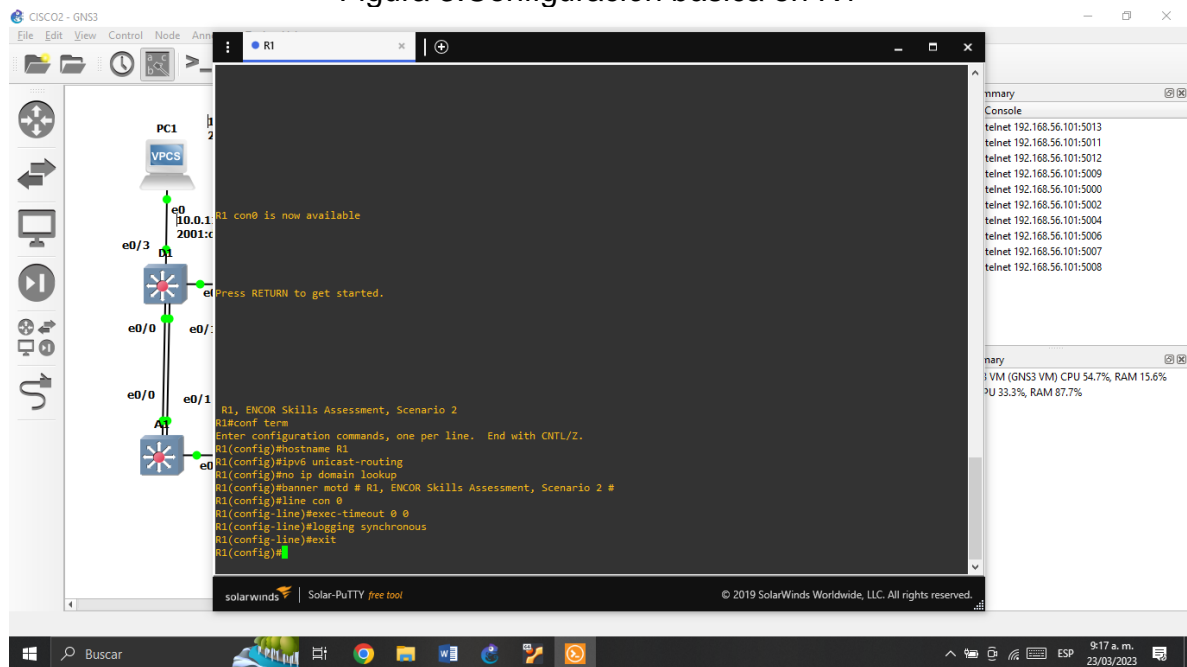
line con 0

exec-timeout 0 0

logging synchronous

exit

Figura 3. Configuración básica en R1



Fuente: Autoría Propia

Router R2

hostname R2

ipv6 unicast-routing

no ip domain lookup

banner motd # R2, ENCOR Skills Assessment, Scenario 2 #

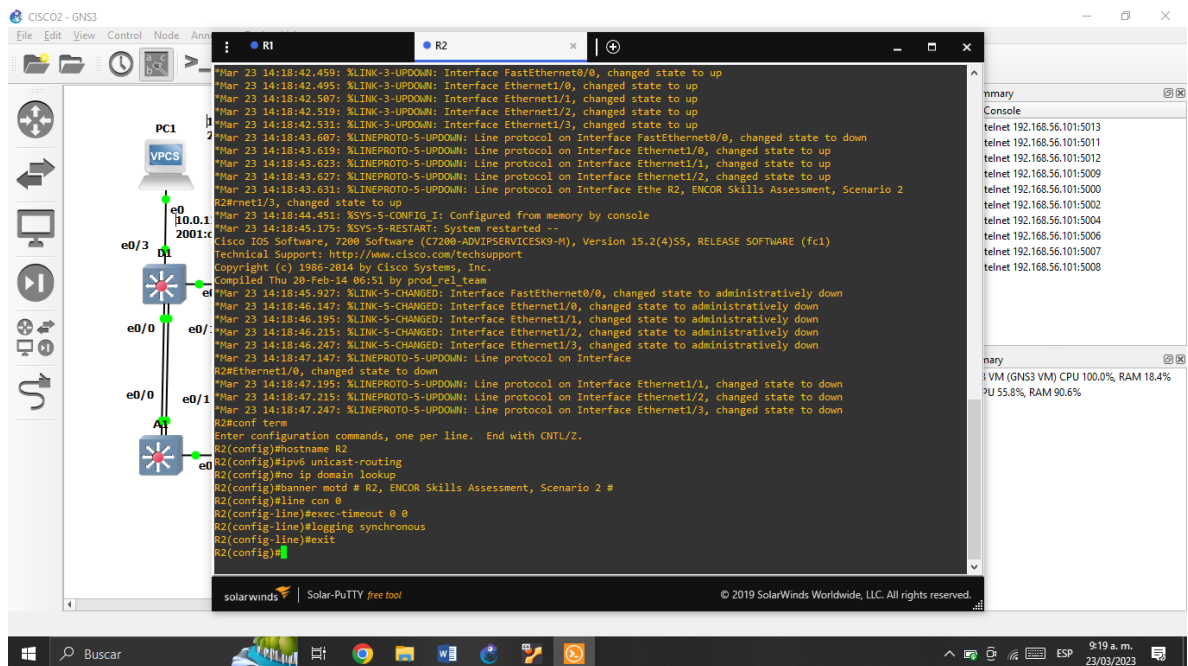
line con 0

exec-timeout 0 0

logging synchronous

exit

Figura 4. Configuración básica en R2



Fuente: Autoría Propia

Router R3

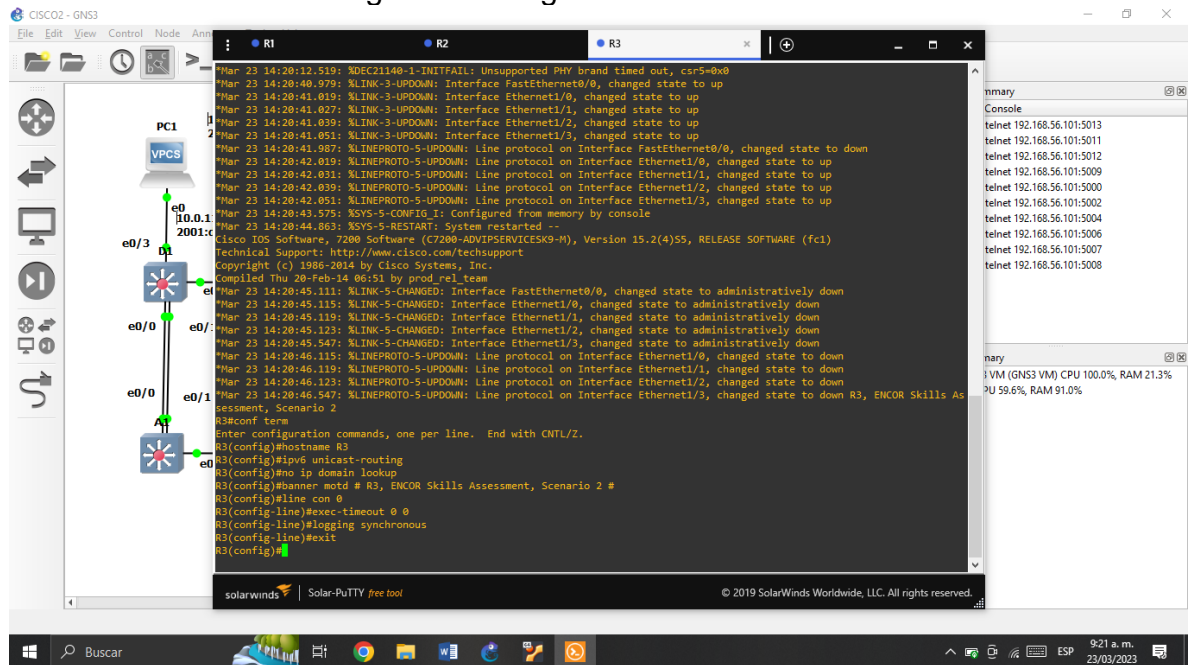
hostname R3

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

Figura 5. Configuración básica en R3



Fuente: Autoría Propia

Configuración y ajustes básicos en los switches

Switch D1

hostname D1

ip routing

ipv6 unicast-routing

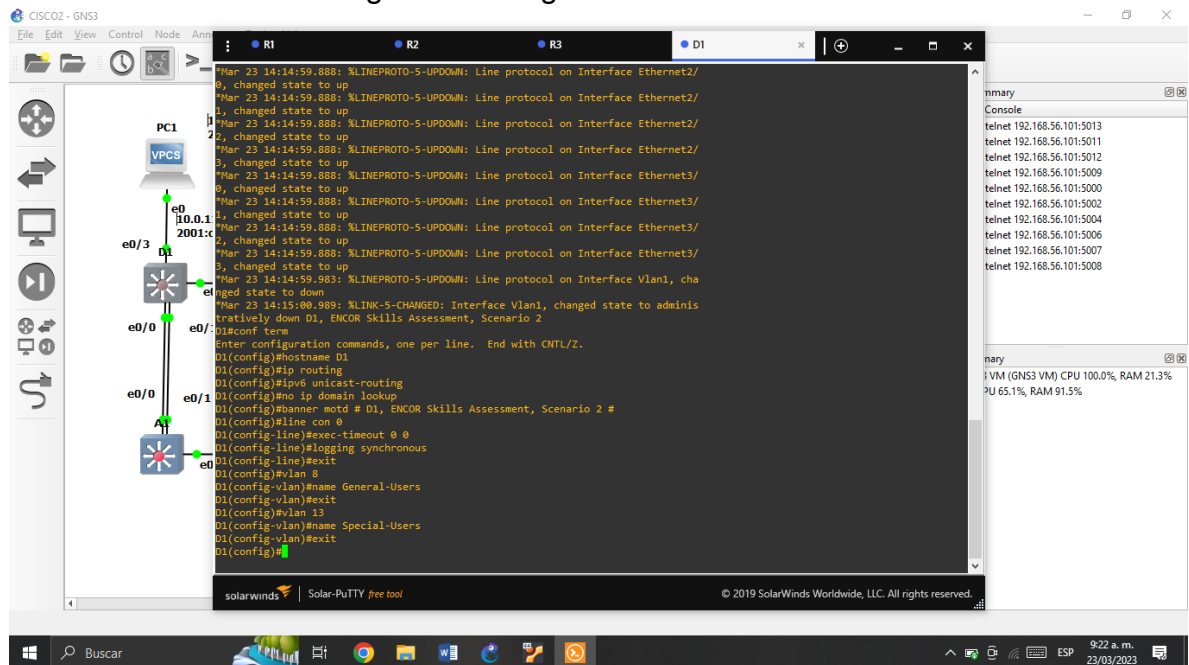
no ip domain lookup

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
```

Figura 6. Configuración básica en D1



Fuente: Autoría Propia

Switch D2

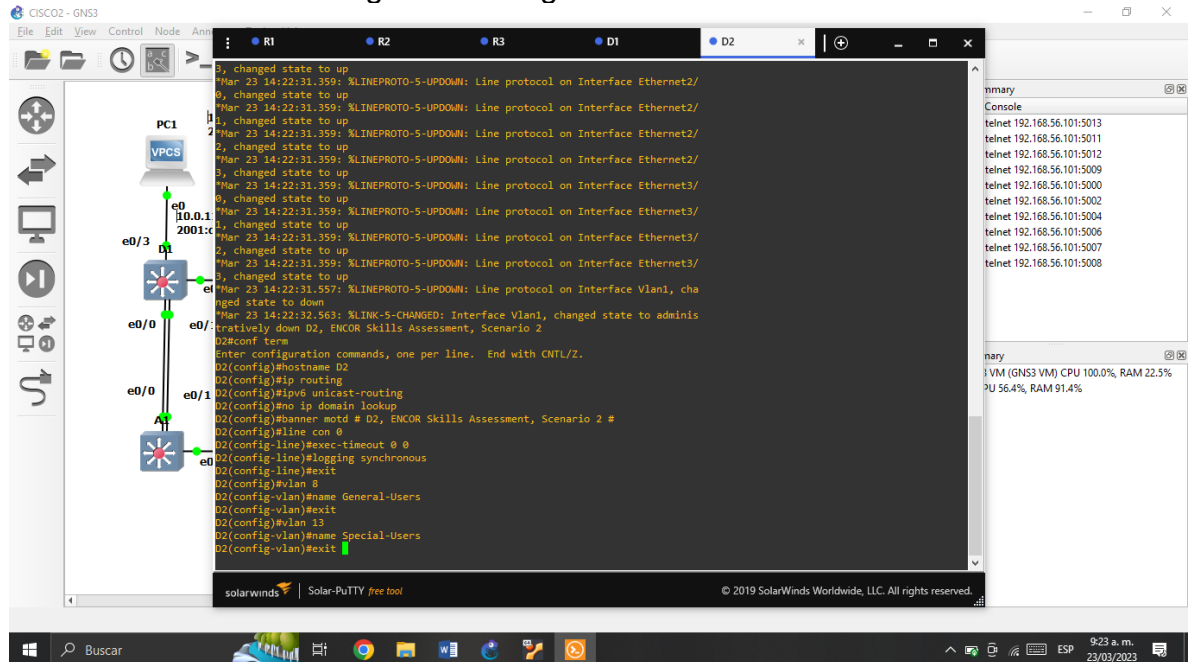
```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
```

```

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

```

Figura 7. Configuración básica en D2



Fuente: Autoría Propia

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

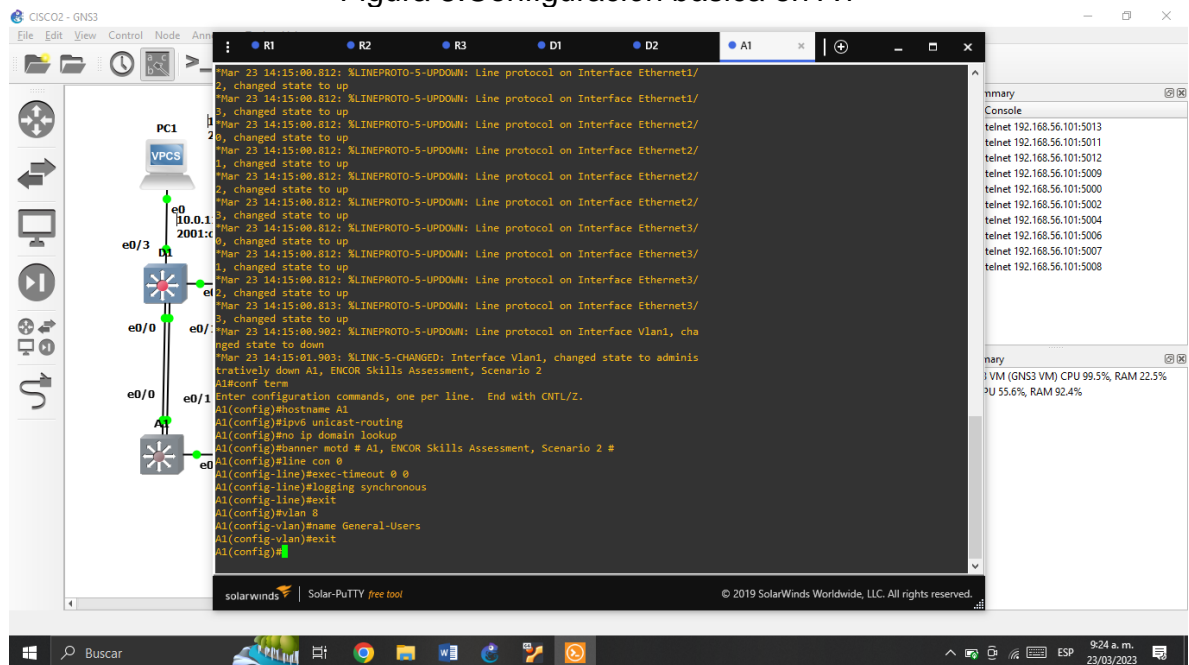
exit

vlan 8

name General-Users

exit

Figura 8. Configuración básica en A1



Fuente: Autoría Propia.

- 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.

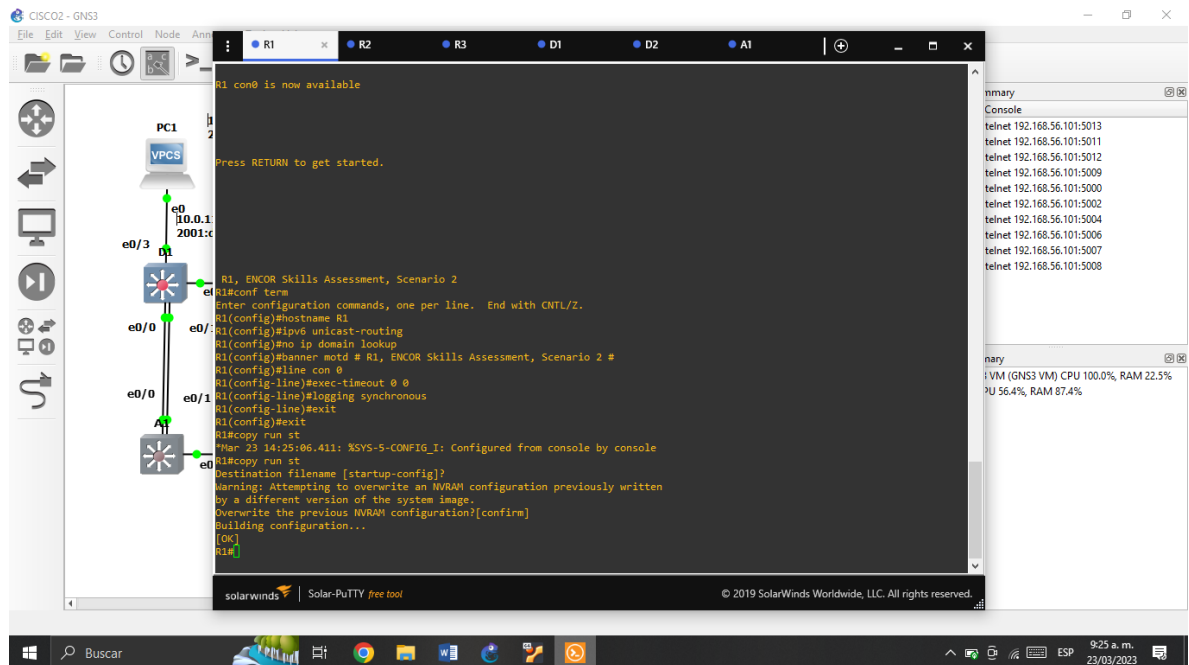
Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

[OK]

R1#

Figura 9. Configuración básica R1



Fuente: Autoria propia

```
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.
```

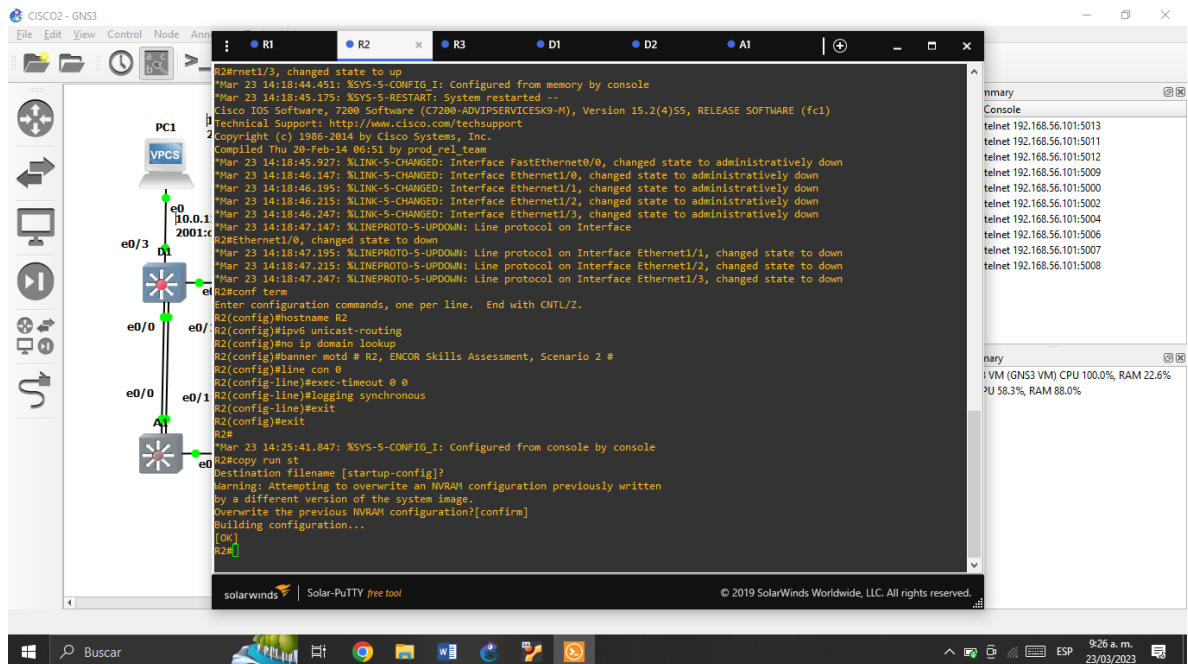
```
Overwrite the previous NVRAM configuration?[confirm]
```

```
Building configuration...
```

```
[OK]
```

```
R2#
```

Figura 10. Configuración básica R2



Fuente: Autoria propia

```
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.
```

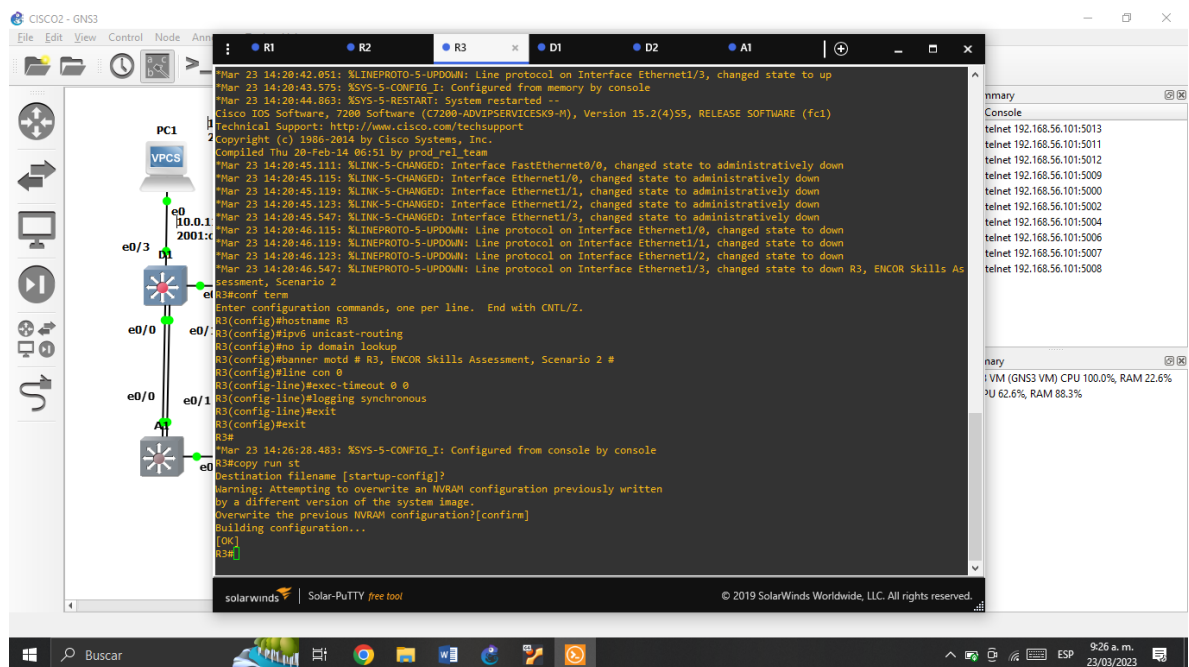
```
Overwrite the previous NVRAM configuration?[confirm]
```

Building configuration...

[OK]

R3#

Figura 11. Configuración básica R3



Fuente: Autoria propia

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.

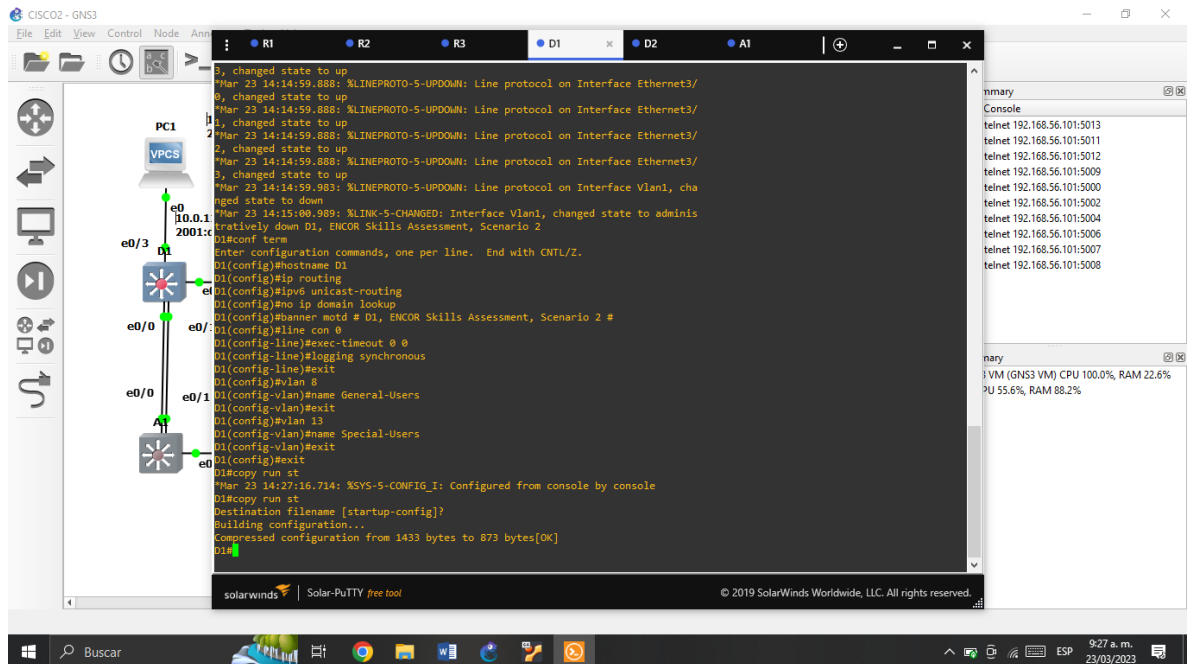
Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

Compressed configuration from 1432 bytes to 868 bytes[OK]

D1#

Figura 12. Configuración básica D1



Fuente: Autoria propia

D2#copy run st

Destination filename [startup-config]?

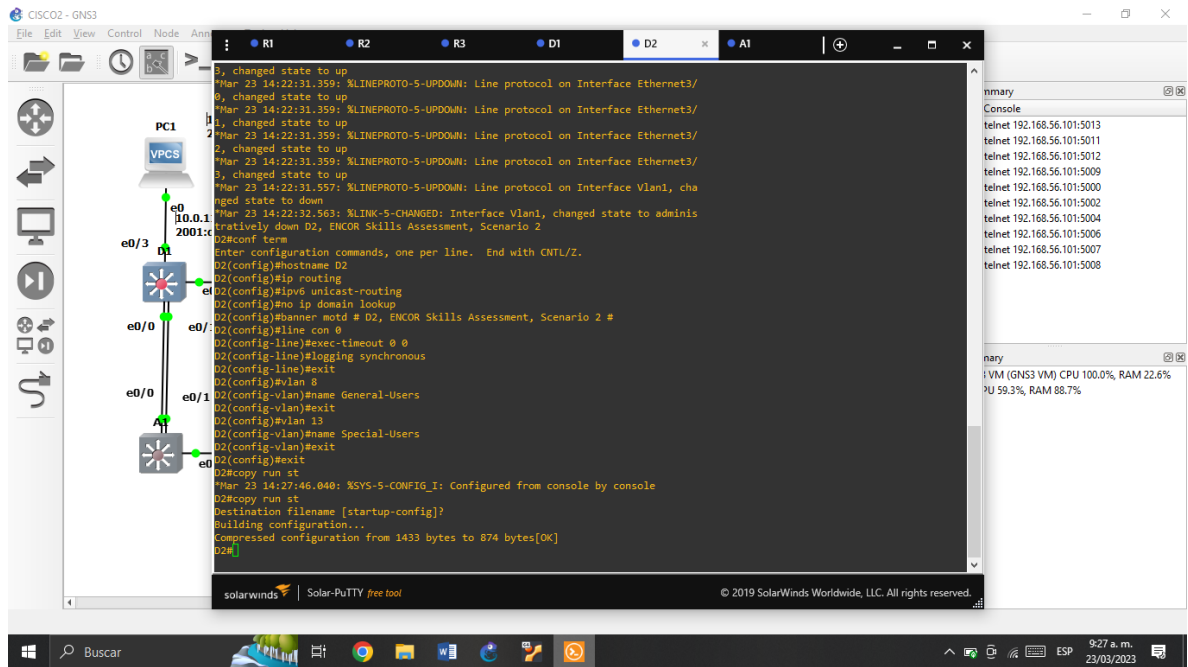
Warning: Attempting to overwrite an NVRAM configuration previously written by a different version of the system image.

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

Compressed configuration from 1432 bytes to 873 bytes[OK]

Figura 13. Configuración básica D2



Fuente: Autoria propia

A1#copy run st

Destination filename [startup-config]?

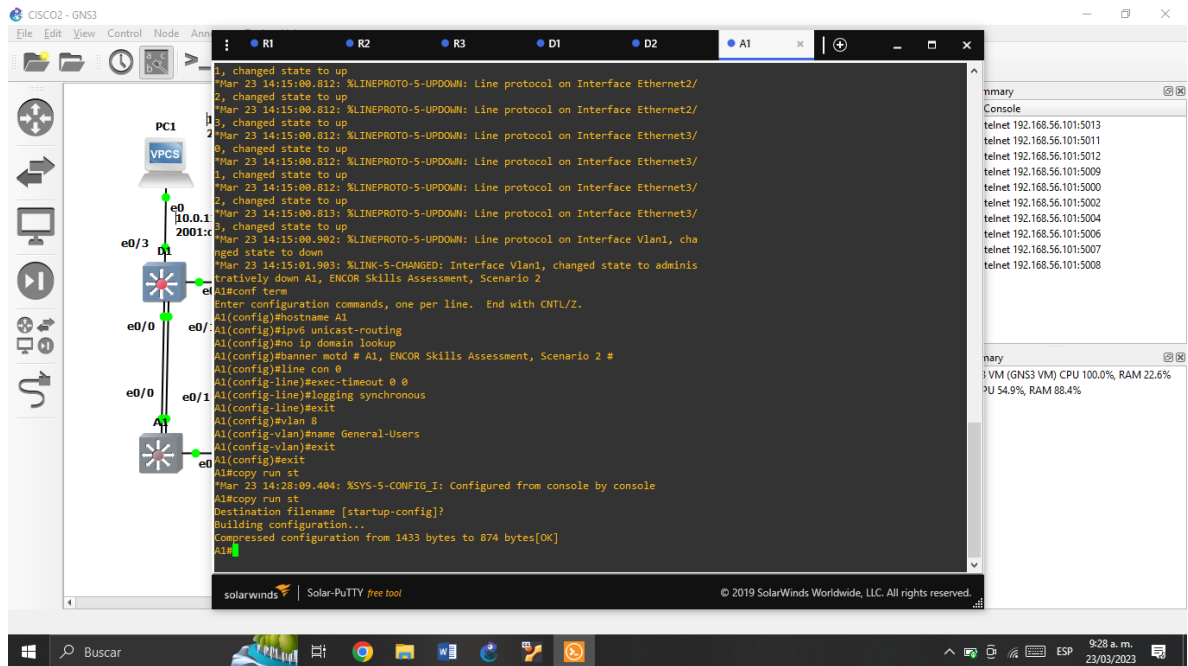
Warning: Attempting to overwrite an NVRAM configuration previously written by a different version of the system image.

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

Compressed configuration from 1432 bytes to 868 bytes[OK]

Figura 14. Configuración básica A1



Fuente: Autoria propia

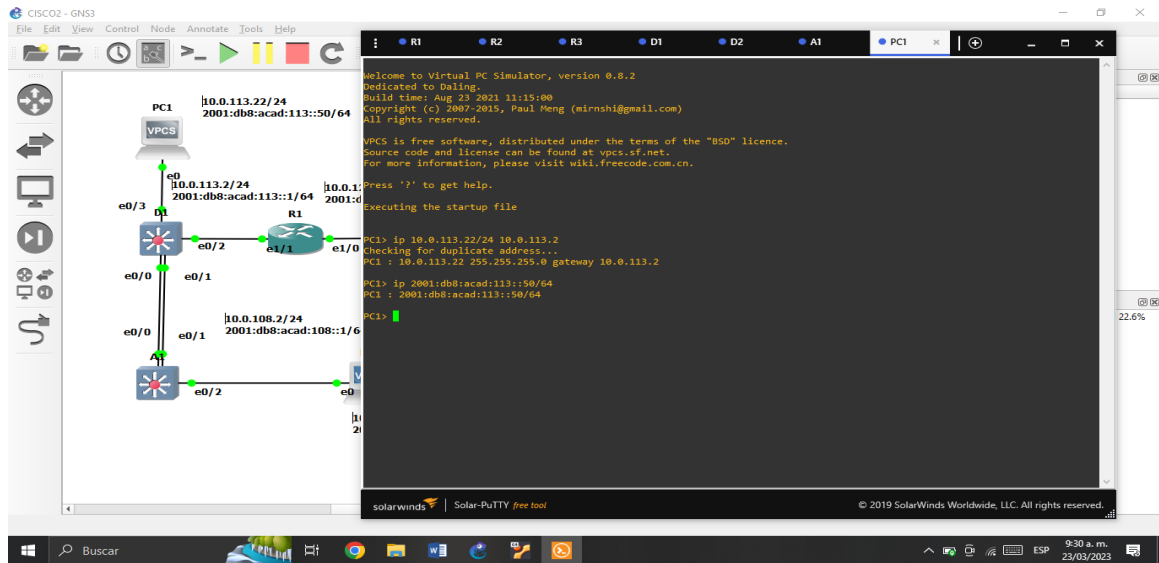
- Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento

PC1

ip 10.0.113.22/24 10.0.113.2

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

Figura 15.PC1



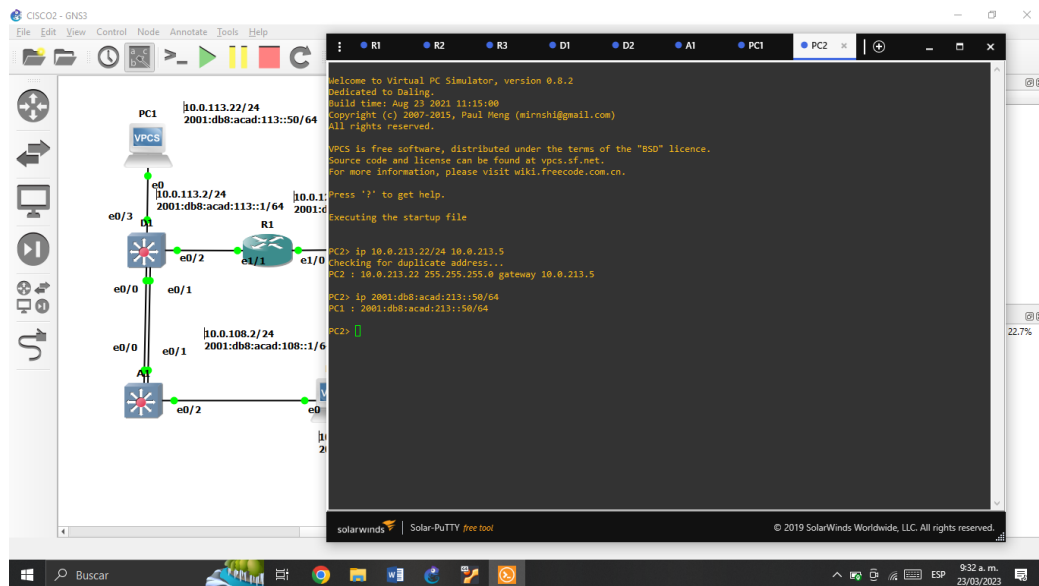
Fuente: Autoría propia

PC2

ip 10.0.213.22/24 10.0.213.5

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

Figura 16.PC2



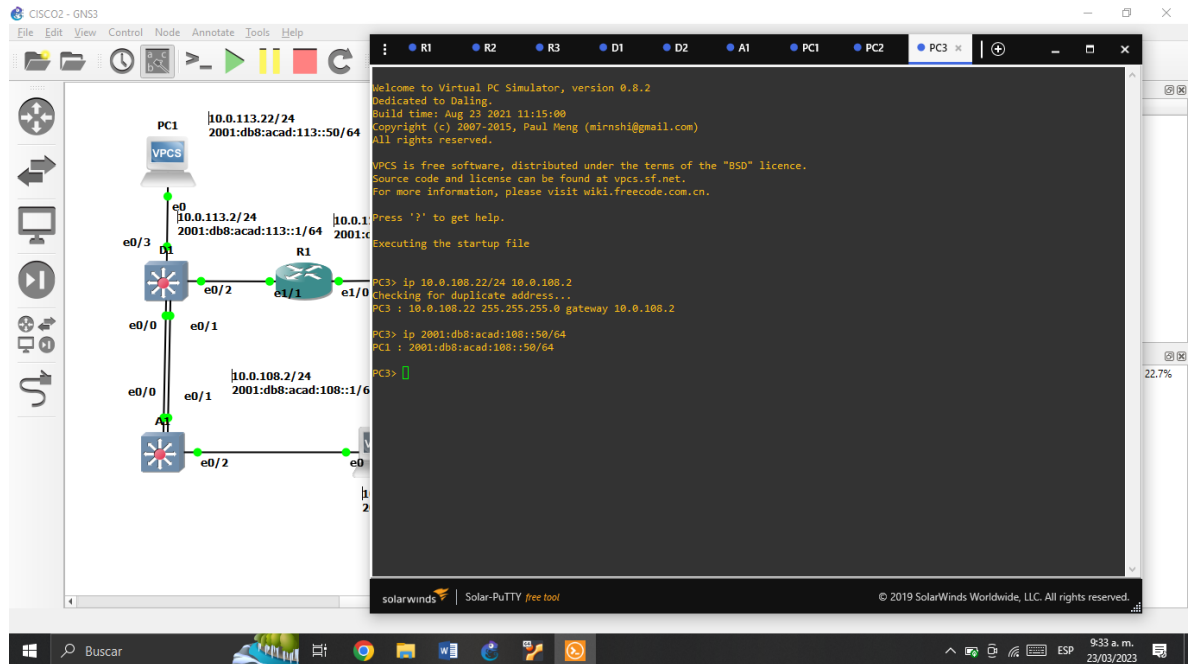
Fuente: Autoría propia.

PC3

ip 10.0.108.22/24 10.0.108.2

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

Figura 17.PC3



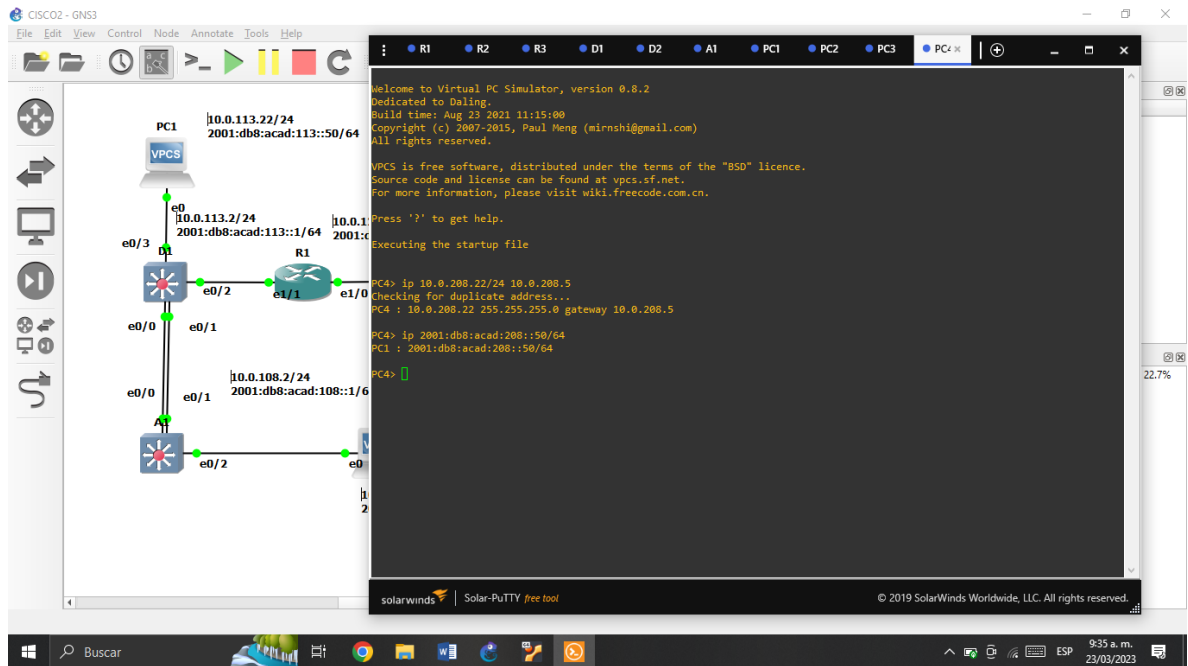
Fuente: Autoría propia

PC4

ip 10.0.208.22/24 10.0.208.5

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

Figura 18.PC4



Fuente: Autoría propia

Parte 2: configurar VRF y enrutamiento estático.

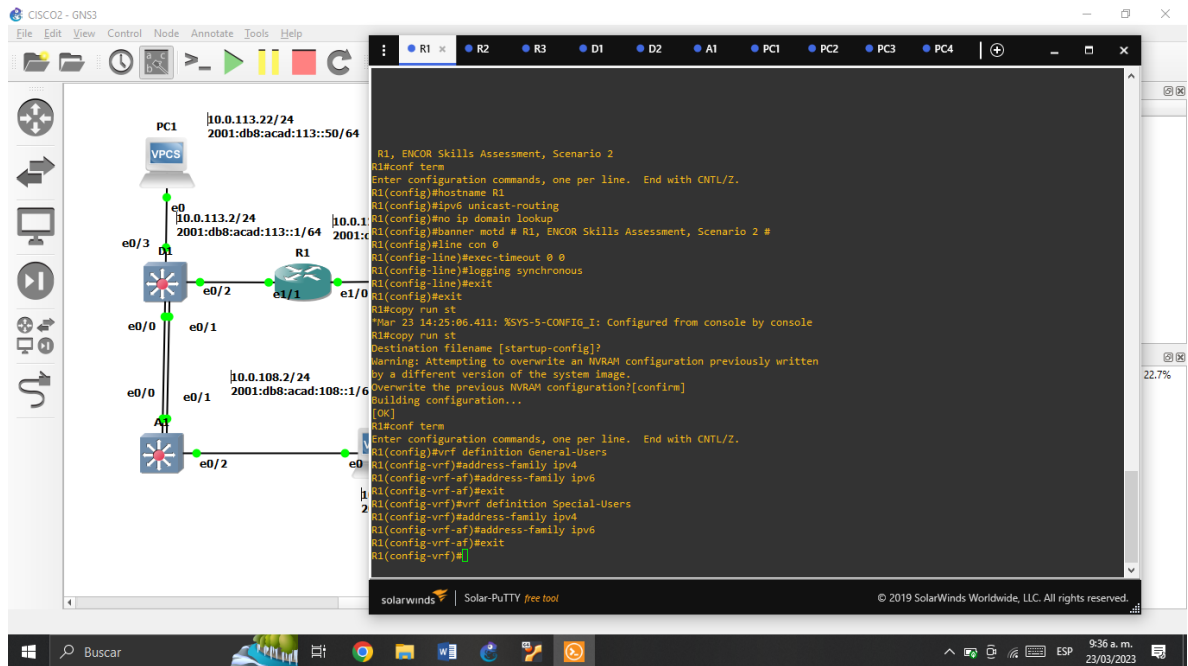
En esta parte de la evaluación de habilidades, configurará VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF.

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
```

Figura 19.Router R1



Fuente: Autoría propia

Configuración Router R2

vrf definition General-Users

address-family ipv4

address-family ipv6

exit

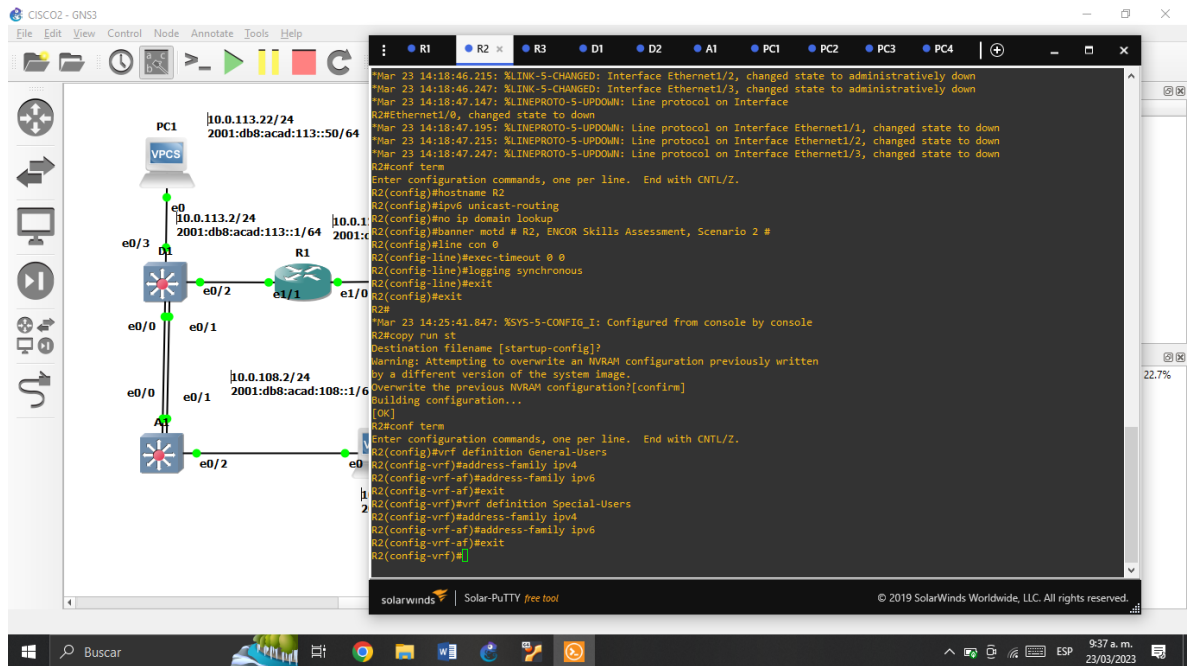
vrf definition Special-Users

address-family ipv4

address-family ipv6

exit

Figura 20.Router R2

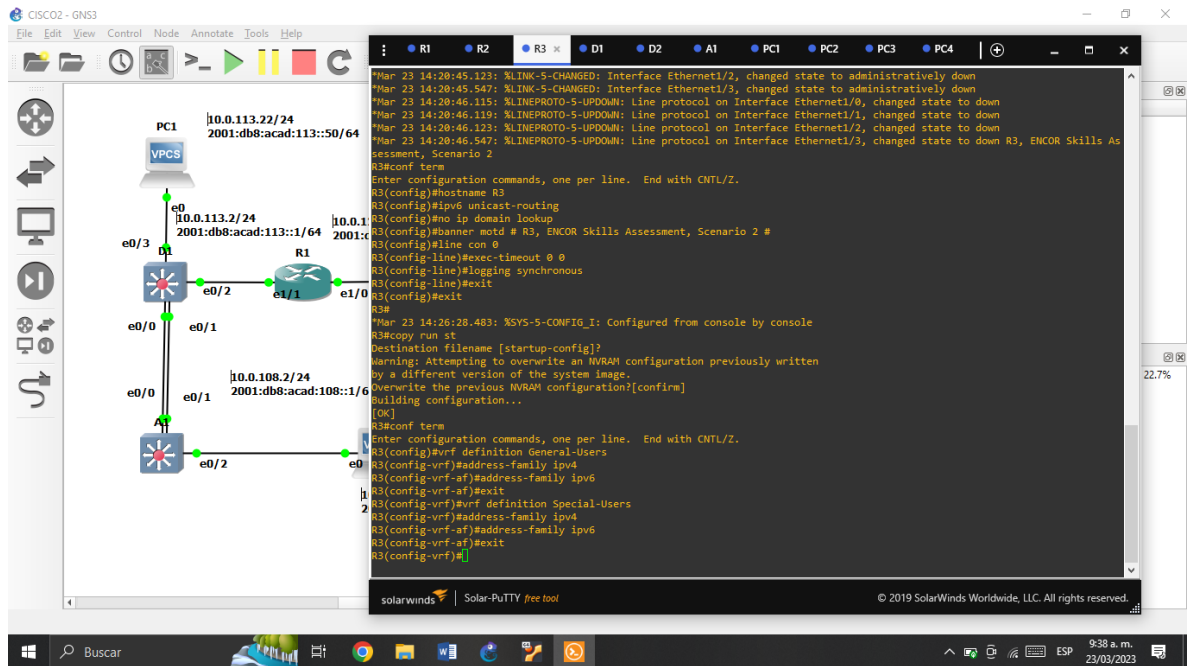


Fuente: Autoría propia

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
```

Figura 21.Router R3



Fuente: Autoría propia

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

Tabla 1. Direccionamiento R1.

Direccionamiento de Router R1

```
interface e1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:acad:12::1/64
no shutdown
exit
interface e1/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:acad:12::1/64
no shutdown
exit
interface e1/0
no ip address
no shutdown
exit
interface e1/1.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.113.2 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:acad:113::1/64
no shutdown
exit
interface e1/1.2
encapsulation dot1q 8
vrf forward General-Users
ip address 10.0.108.2 255.255.255.0
ipv6 address fe80::1:4 link-local
ipv6 address 2001:db8:acad:108::1/64
no shutdown
exit
```

Fuente: Autoría Propia

Tabla 2.Direccionamiento R2.

Direccionamiento de Router R2

```
interface e1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:acad:12::2/64
no shutdown
exit
interface e1/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address fe80::2:2 link-local
ipv6 address 2001:db8:acad:12::2/64
no shutdown
exit
interface e1/0
no ip address
no shutdown
exit
interface e1/1.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:acad:23::2/64
no shutdown
exit
interface e1/1.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address fe80::2:4 link-local
ipv6 address 2001:db8:acad:23::2/64
no shutdown
exit
interface e1/1
no ip address
no shutdown
```

Fuente: Autoría Propia

Tabla 3.Direccionamiento R3.

Direccionamiento de Router R3

```
Interface e1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address fe80::3:1 link-local
ipv6 address 2001:db8:acad:23::3/64
no shutdown
exit
interface e1/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:acad:23::3/64
no shutdown
exit
interface e1/0
no ip address
no shutdown
exit
interface e1/1.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.213.5 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:acad:213::1/64
no shutdown
exit
interface e1/1.2
encapsulation dot1q 8
vrf forward General-Users
ip address 10.0.208.5 255.255.255.0
ipv6 address fe80::3:4 link-local
ipv6 address 2001:db8:acad:208::1/64
no shutdown
exit
interface e1/1
no ip address
no shutdown
```

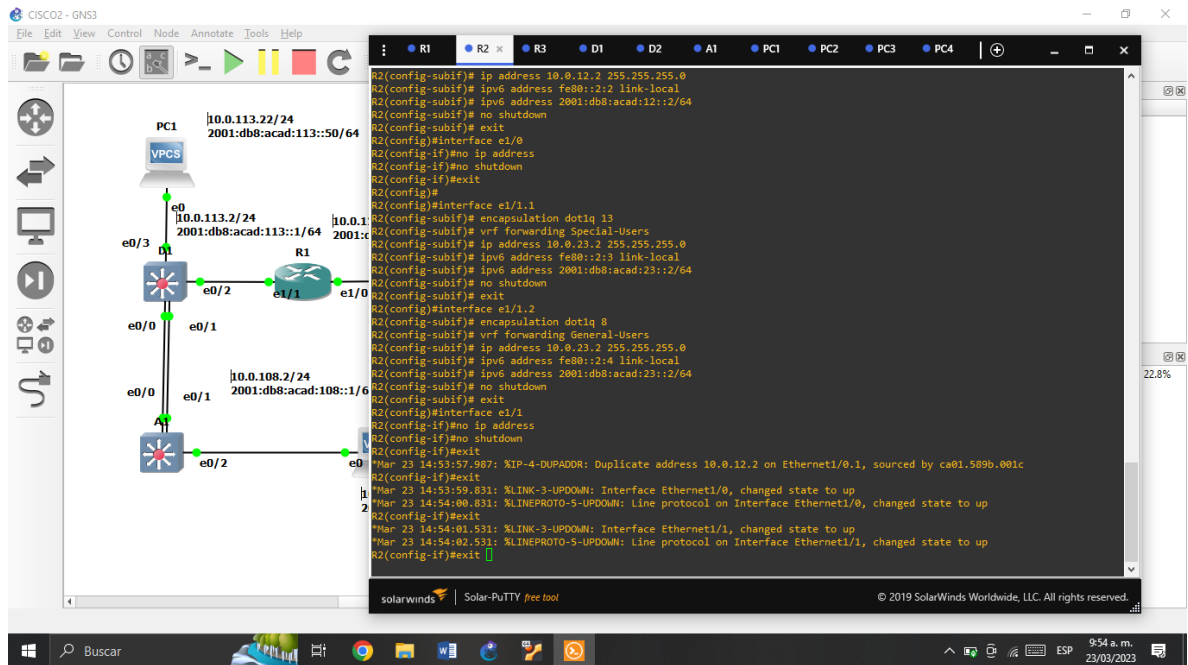
Fuente: Autoría Propia

Figura 22. Configuración Router R1



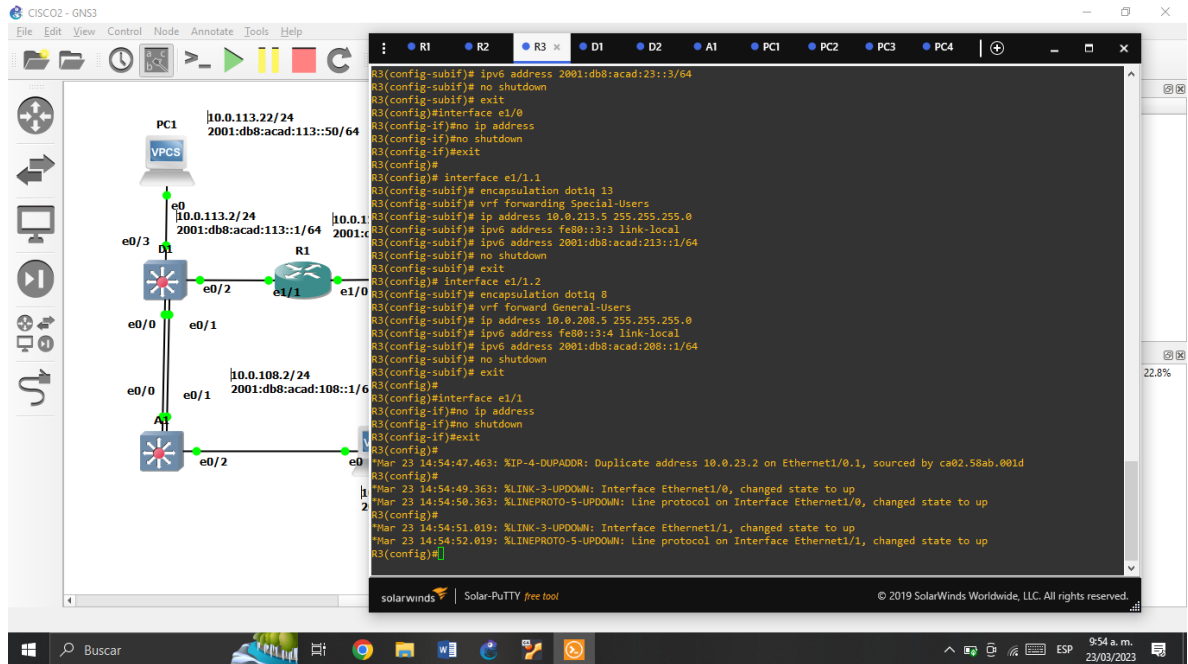
Fuente: Autoría propia

Figura 23. Configuración Router R2



Fuente: Autoría propia

Figura 24. Configuración Router R3



Fuente: Autoría propia

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

Tabla 4. Configuración de ruta estática R1

R1
<pre>ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.0 ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.0 ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2 ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2 end</pre>

Fuente: Autoría propia

Parte 3. Configurar Capa 2

En esta parte, tendrá que configurar los Switches para soportar la conectividad con los dispositivos finales. Las tareas de configuración, son las siguientes:

3.1 On D1, D2, and A1, disable all interfaces.

Tabla 7. Configuración de interfaces.

On D1, D2, and A1, disable all interfaces.
D1
Config t
interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
shutdown
exit
D2
Config t
interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
shutdown
exit
A1
Config t
interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
shutdown
exit

Fuente: Autoría propia.

Estos códigos se refieren a la configuración de interfaces en el software de simulación de redes Cisco Packet Tracer. La tarea que se especifica es "desactivar todas las interfaces" en los dispositivos D1, D2 y A1. Los comandos en la tabla 5

indican que se está accediendo a la configuración (config t) y luego se apaga (shutdown) todas las interfaces en un rango específico de interfaces Ethernet en cada uno de los dispositivos (D1, D2 y A1). Una vez que se completa la tarea, se sale del modo de configuración (exit).

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

Tabla 8. Configuración R1 y R3

On D1 and D2, configure the trunk links to R1 and R3
D1
inter ether 0/0
switchport trunk encapsulation dot1Q
switchport mode trunk
switchport trunk allowed Vlan 13,8
no shutdown
exit
D2
inter ether 0/0
switchport trunk encapsulation dot1Q
switchport mode trunk
switchport trunk allowed Vlan 13,8
no shutdown
exit

Fuente: Autoría propia.

Este conjunto de comandos de configuración se utiliza para configurar los enlaces troncales (trunk links) en los dispositivos D1 y D2 para conectarse con R1 y R3 en el software de simulación de redes Cisco Packet Tracer.

Los comandos específicos incluyen:

- Acceder a la interfaz ethernet 0/0 en el dispositivo D1 y D2 con los comandos "inter ether 0/0"
- Configurar la encapsulación del troncal como dot1Q con "switchport trunk encapsulation dot1Q"
- Configurar el modo de la interfaz como troncal con "switchport mode trunk"
- Especificar los VLAN permitidos a través del troncal con "switchport trunk allowed VLAN 13,8"
- Activar la interfaz troncal con "no shutdown"
- Salir del modo de configuración con "exit"
-

3.3 On D1 and A1, configure the EtherChannel.

Tabla 9. Configuración EtherChannel

On D1 and A1, configure the EtherChannel.

D1

```
inter range e1/0-1
switchport trunk encapsulation dot1Q
switchport mode trunk
channel-group 1 mode desirable
no shutdown
```

A1

```
inter range e1/0-1
switchport trunk encapsulation dot1Q
switchport mode trunk
channel-group 1 mode desirable
no shutdown
```

Fuente: Autoría propia.

Los comandos de configuración en la tabla 9 se utilizan para configurar el EtherChannel entre los dispositivos D1 y A1 en el software de simulación de redes Cisco Packet Tracer.

Los comandos específicos incluyen:

- Acceder a un rango de interfaces Ethernet en el dispositivo D1 y A1 con los comandos "inter range e1/0-1".
- Configurar la encapsulación del troncal como dot1Q con "switchport trunk encapsulation dot1Q".
- Configurar el modo de la interfaz como troncal con "switchport mode trunk".
- Configurar el EtherChannel en el grupo 1 como modo "desirable" con "channel-group 1 mode desirable".
- Activar la interfaz EtherChannel con "no shutdown".

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

Tabla 10. Configuración de acceso

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

D1

```
inter e0/0
switchport mode Access
switchport access vlan 13
spanning-tree portfast
no shutdown
```

exit

wr

D2

```
inter e0/0
switchport mode Access
switchport access vlan 13
spanning-tree portfast
no shutdown
```

exit

```
inter e1/0
```

```
switchport mode Access
switchport access vlan 8
spanning-tree portfast
no shutdown
```

exit

wr

A1

```
inter e0/0
switchport mode Access
switchport access vlan 8
spanning-tree portfast
```

Fuente: Autoría propia.

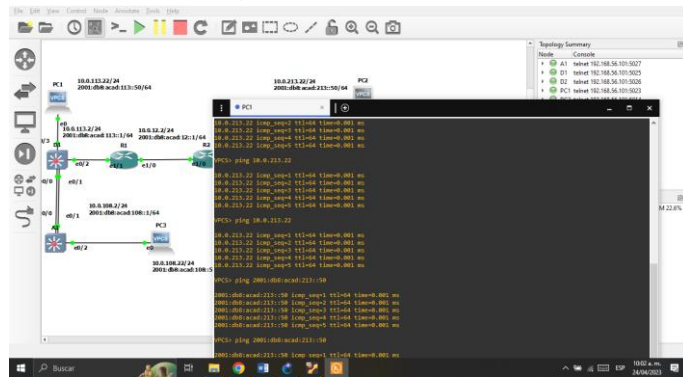
Estos comandos de configuración en la Tabla 10 se utilizan para configurar puertos de acceso en los dispositivos D1, D2 y A1 en el software de simulación de redes Cisco Packet Tracer para conectar los PCs1, PC2, PC3 y PC4.

3.5 Verify PC to PC connectivity.

Tabla 11. Conectividad.

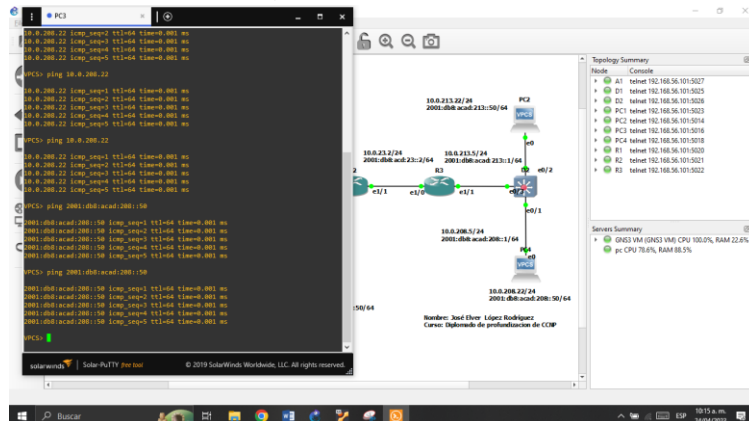
From PC1, verify IPv4 and IPv6 connectivity to PC2.
From PC3, verify IPv4 and IPv6 connectivity to PC4.

Figura 29. PC1-PC2



Fuente: Autoría propia.

Figura 30. PC3-PC4



Fuente: Autoría propia.

Fuente: Autoría propia.

Parte 4 configure Security

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

4.1 On all devices, secure privileged EXE mode.

Tabla 12. Modo privilegiado.

Privileged EXE mode.
R1, R2, R3 D1, D2, A1 config t service password-encryption enable secret cisco12345cisco exit

Fuente: Autoría propia.

La tabla 12 muestra una tarea que debe realizarse en todos los dispositivos de la red para asegurar el modo privilegiado. El modo privilegiado es un nivel de acceso más alto en los dispositivos Cisco, que permite al usuario realizar configuraciones y comandos avanzados. Es importante asegurarse de que el modo privilegiado esté protegido con una contraseña segura y que la información de la contraseña esté cifrada para evitar accesos no autorizados a la red.

El comando "config t" permite al usuario ingresar al modo de configuración global en el dispositivo. Luego, el comando "service password-encryption" activa el cifrado de la contraseña de todos los usuarios en el dispositivo, lo que ayuda a proteger la información de la contraseña de los ataques de ingeniería social o el acceso no autorizado a los archivos de configuración. El comando "enable secret" establece una contraseña segura para el modo privilegiado en el dispositivo, que se cifra automáticamente debido a la configuración anterior. El texto "cisco12345cisco" es un ejemplo de una contraseña que debe ser reemplazada por una contraseña segura y compleja que cumpla con las políticas de seguridad de la organización.

4.2 On all devices, create a local user account.

Tabla 13. Usuario local

```
On all devices, create a local user account.
```

```
R1, R2, R3 D1, D2, A1
config t
username admin secret 0 cisco12345cisco
username admin privilege 15 secret cisco12345cisco
exit
```

Fuente: Autoría propia.

La tabla 13 muestra una tarea que debe realizarse en todos los dispositivos de la red para crear una cuenta de usuario local. Esto es importante para la administración y el acceso seguro a los dispositivos de la red. El comando "config t" permite al usuario ingresar al modo de configuración global en el dispositivo. Luego, el comando "username" se utiliza para crear un nombre de usuario y establecer una contraseña. En este caso, se ha creado un usuario llamado "admin" y se ha establecido la contraseña "cisco12345cisco".

El comando "secret 0" indica que la contraseña se guardará en texto plano en la configuración del dispositivo. Sin embargo, no es recomendable utilizar este método ya que la contraseña sería visible para cualquier persona que tenga acceso a la configuración del dispositivo. Lo ideal es utilizar el comando "secret" seguido de un número de cifrado, que cifrará la contraseña y la protegerá contra accesos no autorizados. Además, el comando "username" se utiliza de nuevo para establecer el nivel de privilegio del usuario. En este caso, se ha establecido un nivel de privilegio de 15, que es el nivel más alto y permite al usuario realizar todas las tareas de configuración en el dispositivo.

4.3 On all devices, enable AAA and enable AAA authentication

Tabla 14. Habilitación y autenticación

On all devices, enable AAA and enable AAA authentication
R1, R2, R3 D1, D2, A1
Enable
algorithm-type SCRYPT secret cisco12345cisco username admin privilege 15
algorithm-type SCRYPT secret cisco12345cisco aaa new-model aaa
authentication login default local exit

Fuente: Autoría propia.

La tabla 14 muestra una tarea que debe realizarse en todos los dispositivos de la red para habilitar la autenticación AAA (Authentication, Authorization, and Accounting) y configurar la autenticación AAA.

El comando "enable" permite al usuario entrar al modo EXEC privilegiado en el dispositivo. Luego, se utiliza el comando "aaa new-model" para habilitar la autenticación AAA en el dispositivo. El comando "algorithm-type SCRYPT" establece el algoritmo de cifrado utilizado para proteger las contraseñas de los usuarios en el dispositivo. En este caso, se ha utilizado el algoritmo de cifrado SCRYPT, que es más seguro que el algoritmo de cifrado predeterminado en algunos dispositivos. El comando "secret" se utiliza para establecer la contraseña de administrador en el dispositivo. En este caso, se ha establecido la contraseña "cisco12345cisco" para el usuario "admin". El comando "username" se utiliza para crear la cuenta de usuario local en el dispositivo y establecer el nivel de privilegio en 15. Finalmente, el comando "aaa authentication login default local" se utiliza para configurar la autenticación AAA en el dispositivo. Este comando indica que se utilizará la autenticación local para permitir que los usuarios ingresen al dispositivo.

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.

La configuración multi-VRF en GNS3 requiere un alto nivel de conocimiento y habilidad en redes de comunicaciones, y la capacidad de aplicar estos conocimientos en la configuración de dispositivos de red. En general, la configuración multi-VRF en GNS3 es una técnica.

El uso de la técnica multi-VRF puede brindar beneficios como un mejor desempeño, mayor seguridad y eficiencia en la utilización de los recursos de red. GNS3, por su parte, es una herramienta valiosa para simular y probar configuraciones de red, lo que permite a los administradores experimentar y validar diferentes configuraciones antes de su implementación en una red real.

REFERENCIAS BIBLIOGRAFICAS

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

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

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