DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SAMAEL JAVIER AMADO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
COROZAL - SUCRE
2023

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SAMAEL JAVIER AMADO HERNANDEZ

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

DIRECTOR:
GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
COROZAL - SUCRE
2023

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Sincelejo, 02 de abril 2023

AGRADECIMIENTOS

A Dios, por darme la sabiduría, salud y fortaleza para lograr este objetivo tan importante en mi formación personal y profesional.

A mi familia, por ser mi apoyo, esperar con paciencia y contribuir con su amor y compañía en este título tan anhelado.

Al cuerpo de docentes por ser orientadores y estar prestos a colaborar todo el tiempo, sin dejarnos decaer e impulsarnos a conquistar nuestras metas.

A mis amigos, quienes de una u otra manera contribuyeron con sus ideas, acompañamiento y apoyo en los diferentes momentos de esta etapa profesional.

INDICE PRINCIPAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

Ethernet-Channel: es una tecnología utilizada por equipos Cisco que permite la agrupación de varios enlaces físicos en un enlace lógico con un mayor ancho de canal.

IPV4: Protocolo de enrutamiento versión 4, es utilizado para identificar una interfaz de red. Este protocolo está compuesto por un numero de 32 bits que se divide en 4 campos de 8 bits separados.

IPV6: protocolo de enrutamiento versión 6, es utilizado para identificar una interfaz de la red. Este protocolo cuenta con 128 bits divididos en 8 grupos de 4 dígitos hexadecimales

Protocolo de enrutamiento: permite la comunicación entre los hosts de una red intercambiando información de enrutamiento.

Vlan: Redes de Área Local virtuales, son dominios de difusión lógica, este método permite crear varias redes lógicas independientes dentro de una red física.

VRF: Enrutamiento Virtual y Reenvío es una tecnología implementada por los Routers que permite mantener varias tablas de enrutamiento de forma simultánea.

RESUMEN

El presente trabajo nos muestra el desarrollo del escenario 1 propuesto para el diplomado de profundización CISCO prueba de habilidades prácticas CCNP, realizando la configuración de las VRF Virtual Routing and Forwarding, enrutamiento virtual y reenvío entre los diferentes routers, configuración administración de los Switch capa 2 y capa 3 e implementación de seguridad en los todos los dispositivos utilizados. Se rinde el informe desarrollando el enrutamiento utilizado, así como la configuración utilizada en cada dispositivo, refiriendo cada una de las líneas de códigos con el fin de presentar un trabajo bien constituido según los requerimientos establecidos.

En esta prueba de habilidades, somos los encargados de completar la configuración multi-VRF de la red que admite "Usuarios generales" y "Usuarios especiales", realizando la topología de la red en los softwares GNS3 Y VM VirtualBox configurando los ajustes básicos en todos los dispositivos utilizados como son tres routers, tres switchs y cuatro Pcs.

Del mismo modo conectando los dispositivos como se muestra en el diagrama de topología y cableando según sea necesario, a continuación, ingresamos al modo de configuración global en cada uno de los dispositivos y aplicamos la configuración básica. Las configuraciones de inicio para cada dispositivo, se configurará VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a extremo. Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF.

PALABRAS CLAVE: Telecomunicaciones, CISCO, CCNP, VRF, Enrutamiento, Redes.

ABSTRACT

The present work shows us the development of scenario 1 proposed for the CISCO in-depth diploma test of CCNP practical skills, configuring the VRF Virtual Routing and Forwarding, virtual routing and forwarding between the different routers, configuration administration of Layer 2 Switches and layer 3 and security implementation in all the devices used. The report is rendered developing the routing used, as well as the configuration used in each device, referring to each one of the code lines in order to present a well-constituted work according to the established requirements.

In this skills test, we are in charge of completing the multi-VRF configuration of the network that supports "General Users" and "Special Users", performing the network topology in the GNS3 and VM VirtualBox software configuring the basic settings in all the devices used are three routers, three switches and four PCs.

Similarly connecting the devices as shown in the topology diagram and wiring as needed, we then enter global configuration mode on each of the devices and apply the basic settings. Starting configurations for each device, VRF-Lite will be configured on all three routers and the appropriate static routes to support end-to-end reachability. By the end of this part, R1 should be able to ping R3 on each VRF.

KEY WORDS: CISCO, CCNP, VRF, Routing, Networks, Telecommunications.

INTRODUCCIÓN

El hombre es un ser tecnológico por naturaleza, siempre ha estado rodeado de ella para resolver situaciones cotidianas buscando siempre mejorar sus condiciones de vida y la de los demás. Desde ese momento hasta hoy, los avances han sido muchos, pero siempre han mantenido el mismo fin que es mejorar las condiciones de supervivencia del hombre. La evolución de la tecnología ha posibilitado ir mejorando el desempeño humano en las actividades u oficios que realiza; por ello cada día se busca perfeccionar las diferentes herramientas y las formas de uso de la tecnología.

En tal sentido, se hace necesario manejar, seleccionar y estar a la vanguardia de dichos avances que le permitan resolver los problemas de la cotidianidad e incorporarse tecnológicamente a un mundo más competitivo y cambiante que demanda de un cambio de pensamiento y transformación de la sociedad, teniendo en cuenta que las redes de telecomunicaciones se han transformado en una herramienta indispensable para transmitir información por medios electrónicos.

Como ingenieros de telecomunicaciones es indispensable el conocimiento destreza sobre el funcionamiento y configuración de estos equipos, los protocolos y topologías utilizadas, en los diferentes campos de las telecomunicaciones para un óptimo funcionamiento de la red.

El presente trabajo nos muestra el desarrollo del escenario 1 propuesto para el diplomado de profundización CISCO prueba de habilidades prácticas CCNP, realizando la configuración de las VRF Virtual Routing and Forwarding, enrutamiento virtual y reenvío en los diferentes routers, configuración administración de los Switch capa 2 y capa 3 e implementación de seguridad en los todos los dispositivos utilizados. Se rinde el informe desarrollando el enrutamiento utilizado, así como la configuración utilizada en cada dispositivo, refiriendo cada una de las líneas de códigos con el fin de presentar un trabajo bien constituido según los requerimientos establecidos.

DESARROLLO

Escenario Propuesto

Topología de la Red:

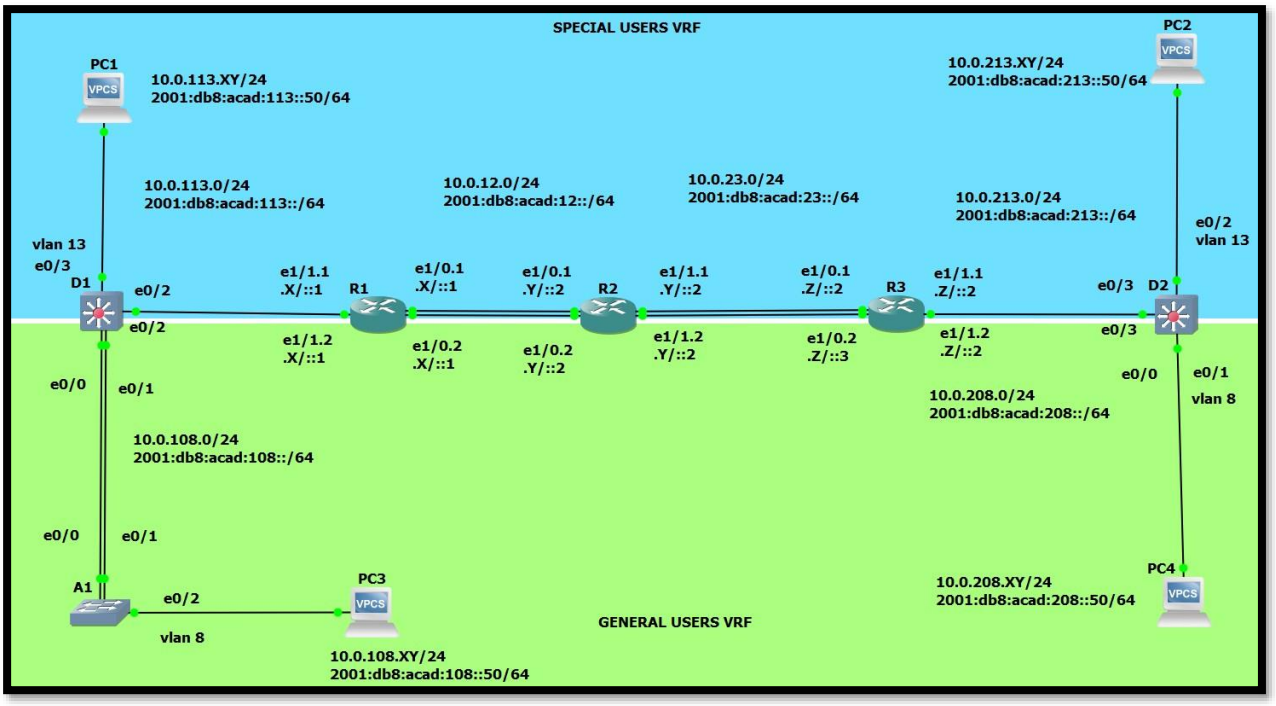

Figura 1. Escenario 1

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, configurará la topología de la red y configurará 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.

Paso 2: Configure los ajustes básicos para cada dispositivo.

a. 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.

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

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

Tabla 1. Tabla de direccionamiento Escenario 1

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.X/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.X/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.X/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.X/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.Y/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.Y/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.Y/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.Y/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.Z/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.Z/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.Z/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.Z/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.XY/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.XY/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.XY/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.XY/24	2001:db8:acad:208::50/64	EUI-64

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.
Sus tareas de configuración son las siguientes:

Tabla 2. Tabla de tareas y especificaciones

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 their e1/1.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 and IPv6 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

Nota: R1 no estará habilitado para realizar ping entre PC2 o PC4 con la configuración de las Partes 1 y 2.

DESARROLLO DE LA ACTIVIDAD

Configuración de la topología de la red de igual forma se configurará los ajustes básicos. Se elabora el montaje de la topología en el software GNS3.

Escenario elaborado en GNS3

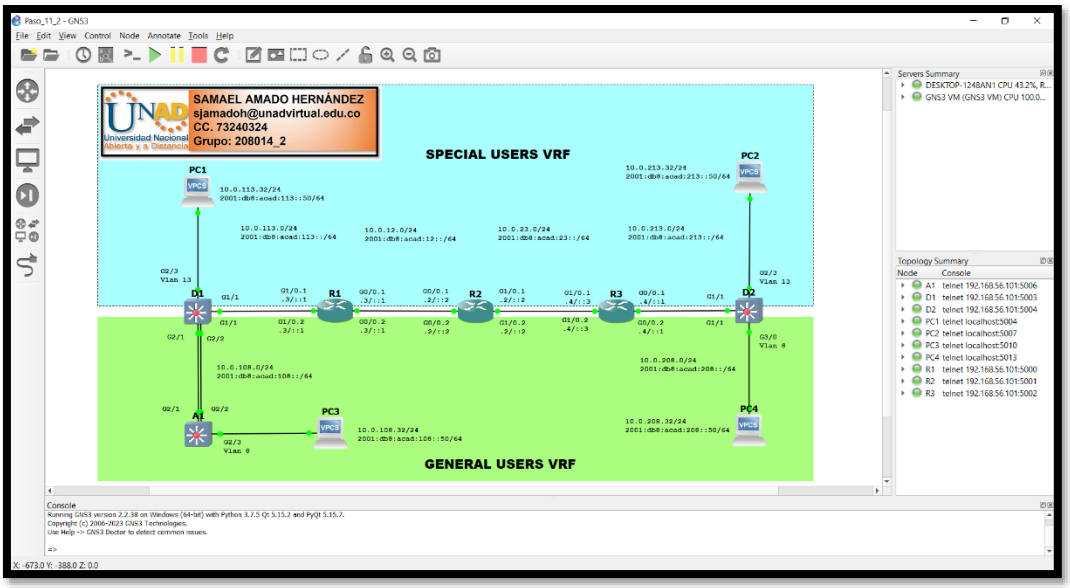

Figura 2. Escenario elaborado en GNS3

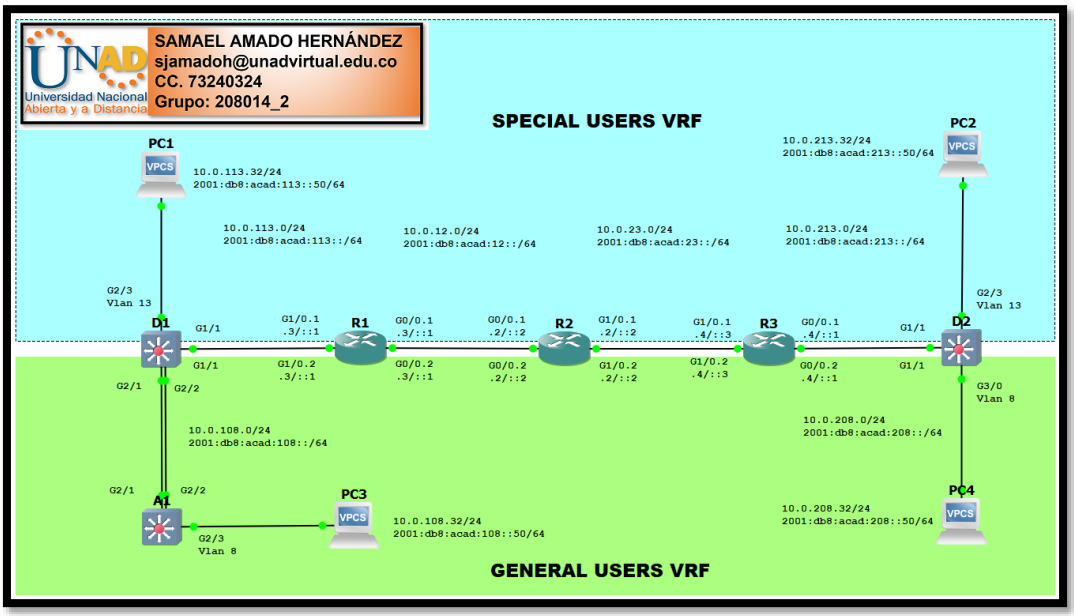

Figura 3. Figura 2. Escenario elaborado en GNS3

Tabla de direccionamiento elaborada y aplicada en GNS3

Se elabora la tabla de direccionamiento, donde se enuncian las interfaces utilizadas en la simulación GNS3 del escenario 1.

Tabla 3. Tabla de direccionamiento elaborada y aplicada en GNS3

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G0/0.1	10.0.12.3/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0.2	10.0.12.3/24	2001:db8:acad:12::1/64	fe80::1:2
	G1/0.1	10.0.113.3/24	2001:db8:acad:113::1/64	fe80::1:3
	G1/0.2	10.0.108.3/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G0/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G1/0.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	G1/0.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G1/0.1	10.0.23.4/24	2001:db8:acad:23::3/64	fe80::3:1
	G1/0.2	10.0.23.4/24	2001:db8:acad:23::3/64	fe80::3:2
	G0/0.1	10.0.213.4/24	2001:db8:acad:213::1/64	fe80::3:3
	G0/0.2	10.0.208.4/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.32/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.32/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.32/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.32/24	2001:db8:acad:208::50/64	EUI-64

Configuración de los ajustes básicos para cada dispositivo.

a. 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.

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global en cada uno de los dispositivos tales como Router 1, Router 2 y Router 3 aplicando las configuraciones de inicio para cada equipo de red.

Configuración Router R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 2 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1#
```

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global del Router 1 aplicando las configuraciones de inicio para el equipo de red.

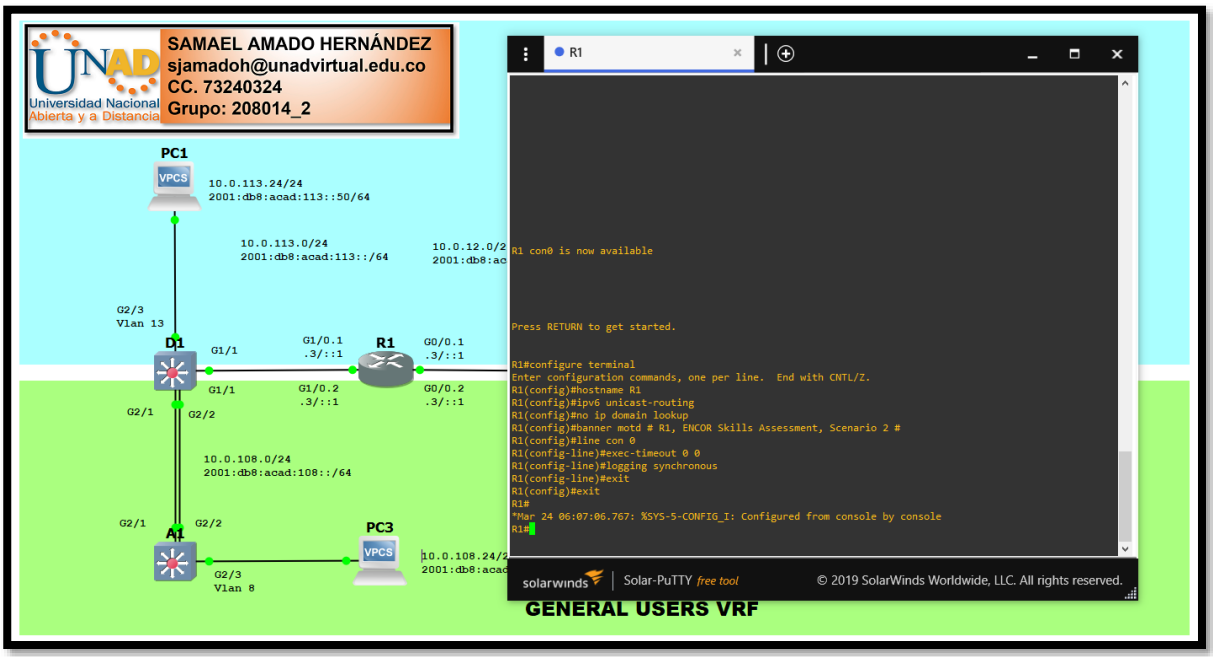

Figura 4. Configuración de inicio Router *R1 en Solar-PuTTY GNS3*

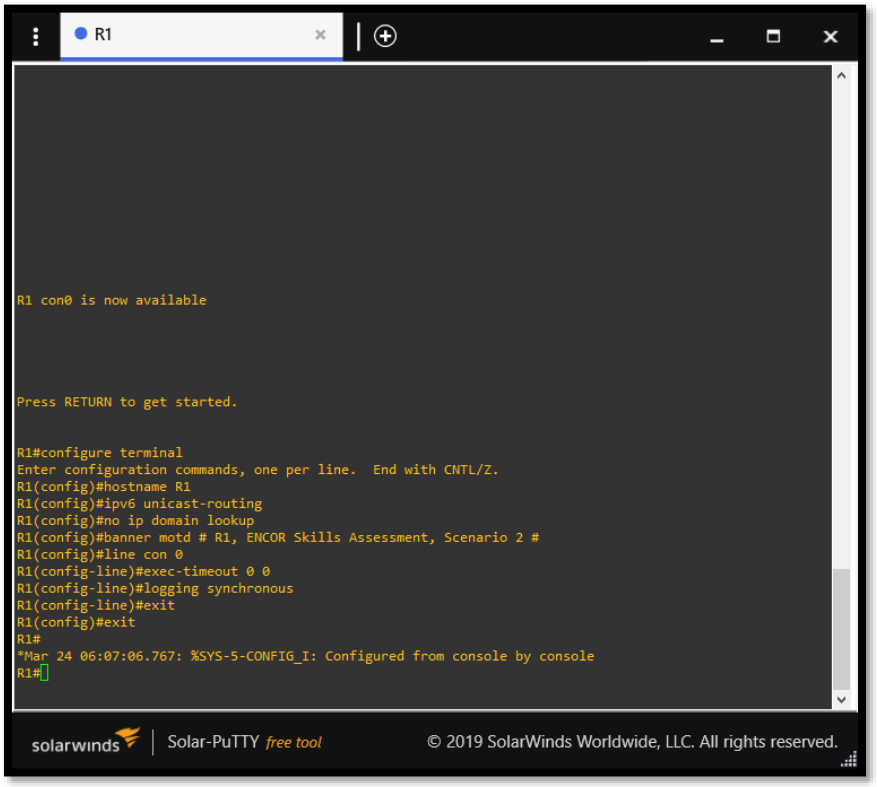

Figura 5. Configuración de inicio Router *R1 en Solar-PuTTY GNS3*

Configuración Router R2

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 2 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#exit
R2#
```

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global del Router 2 aplicando las configuraciones de inicio para el equipo de red.

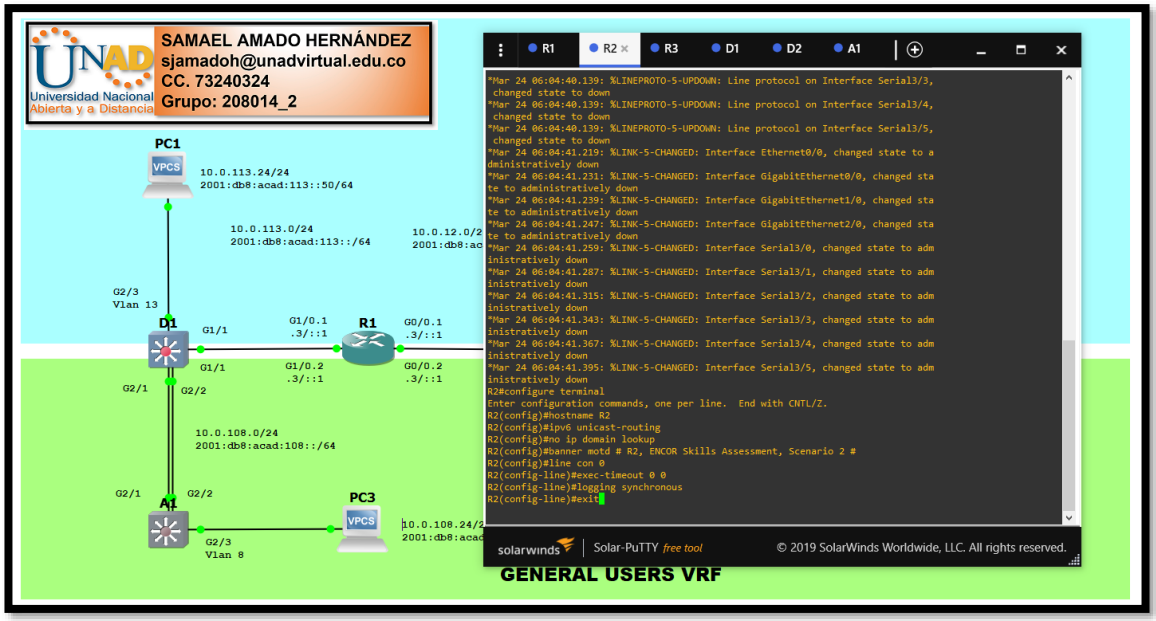

Figura 6. Configuración de inicio Router *R2 en Solar-PuTTY GNS3*

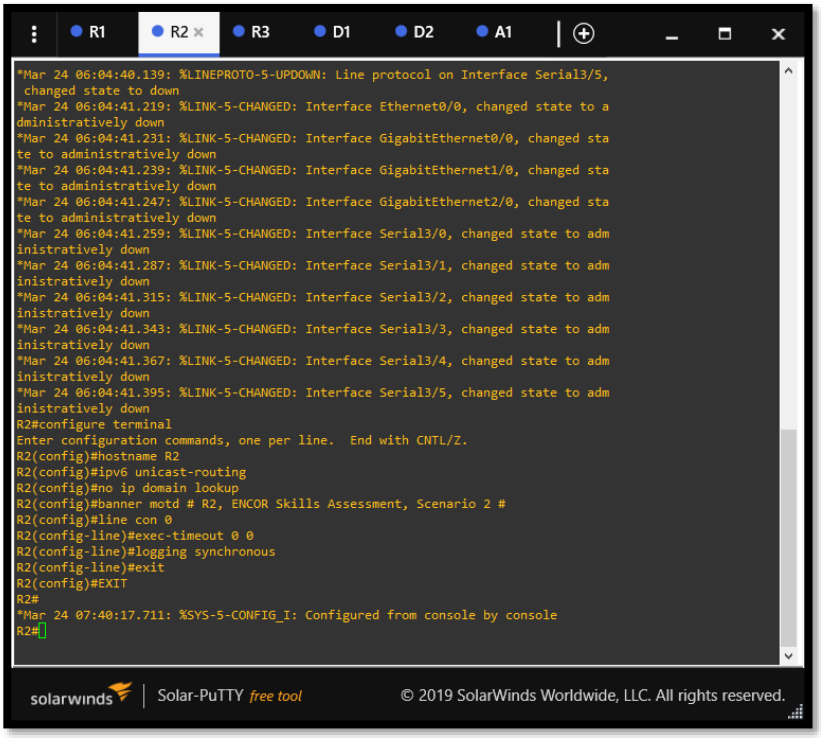

Figura 7. Configuración de inicio Router *R2 en Solar-PuTTY GNS3*

Configuración Router R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 2 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#exit
R3#
```

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global del Router 3 aplicando las configuraciones de inicio para el equipo de red.

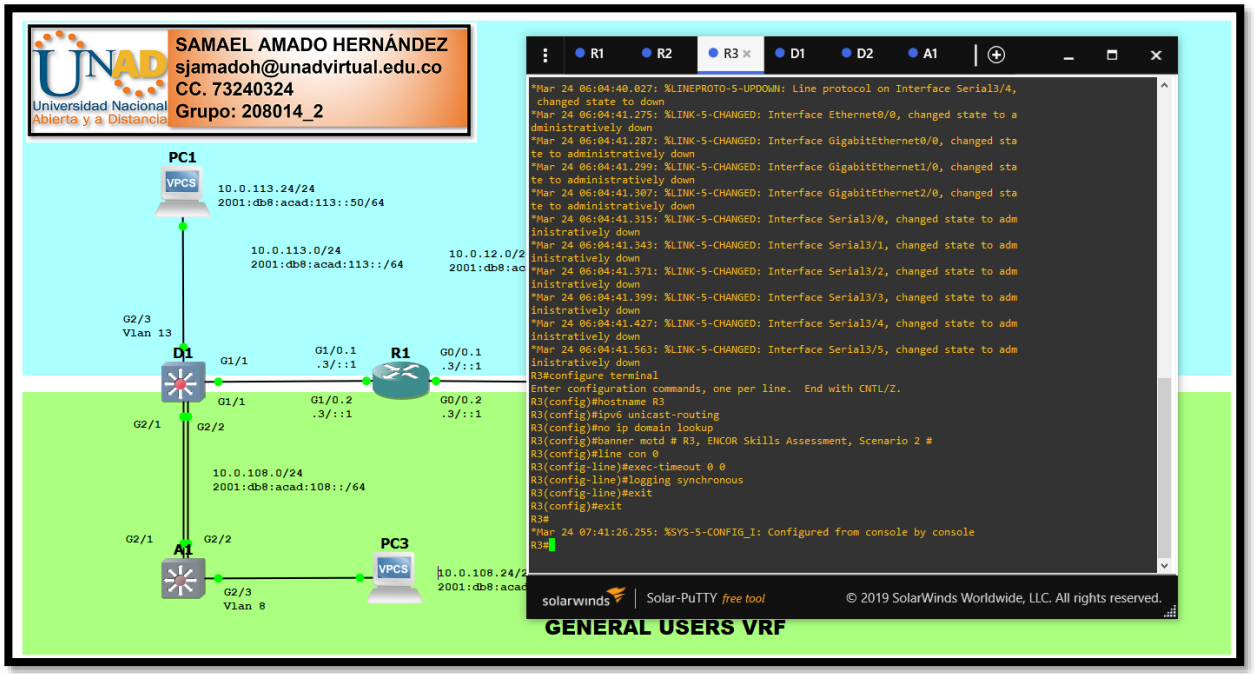

Figura 8. Configuración de inicio Router *R3 en Solar-PuTTY GNS3*

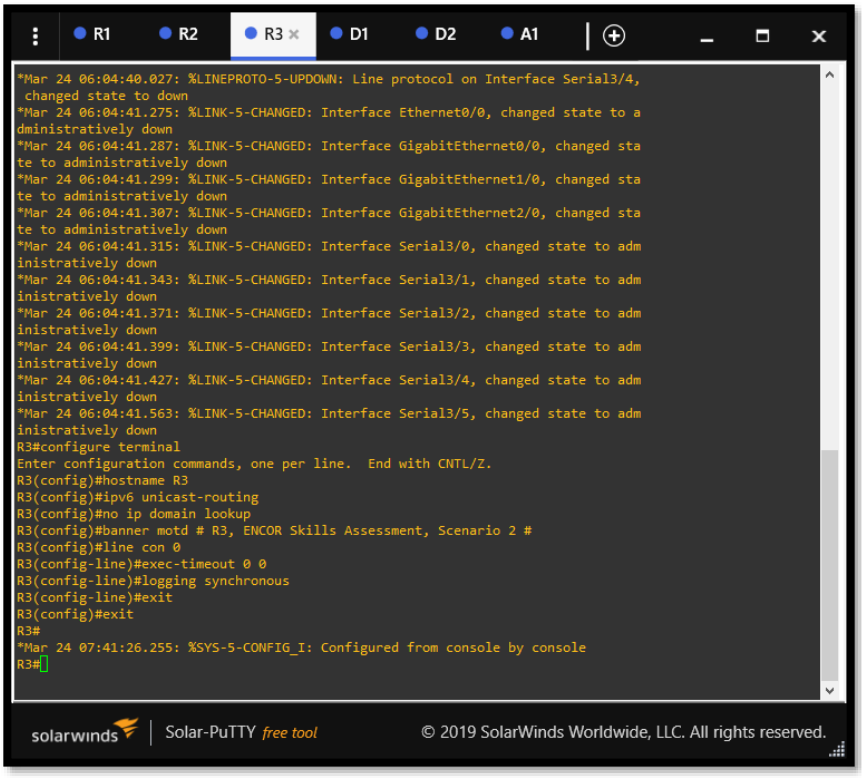

Figura 9. Configuración de inicio Router *R3 en Solar-PuTTY GNS3*

Configuración Switch D1

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 2 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 8
D1(config-vlan)#name General-Users
D1(config-vlan)#exit
D1(config)#vlan 13
D1(config-vlan)#name Special-Users
D1(config-vlan)#exit
D1(config)#exit
D1#
```

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global del Switch D1 aplicando las configuraciones de inicio para el equipo de red.

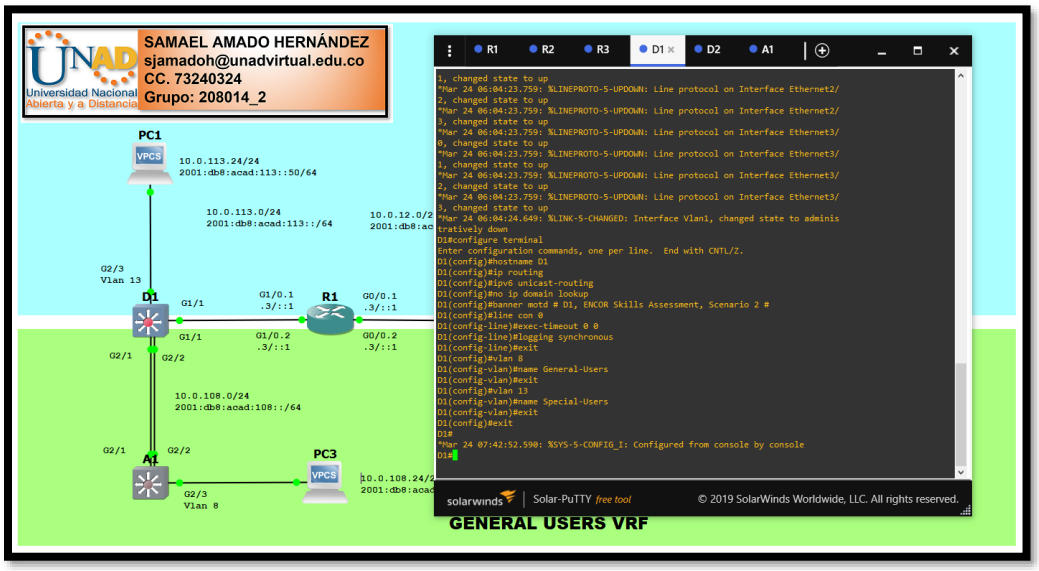

Figura 10. Configuración de inicio *Switch D1 en Solar-PuTTY GNS3*

Figura 11. Configuración de inicio *Switch D1 en Solar-PuTTY GNS3*

Configuración Switch D2

```
D2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 2 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 8
D2(config-vlan)#name General-Users
D2(config-vlan)#exit
D2(config)#vlan 13
D2(config-vlan)#name Special-Users
D2(config-vlan)#exit
D2(config)#exit
D2#
```

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global del Switch D2 aplicando las configuraciones de inicio para el equipo de red.

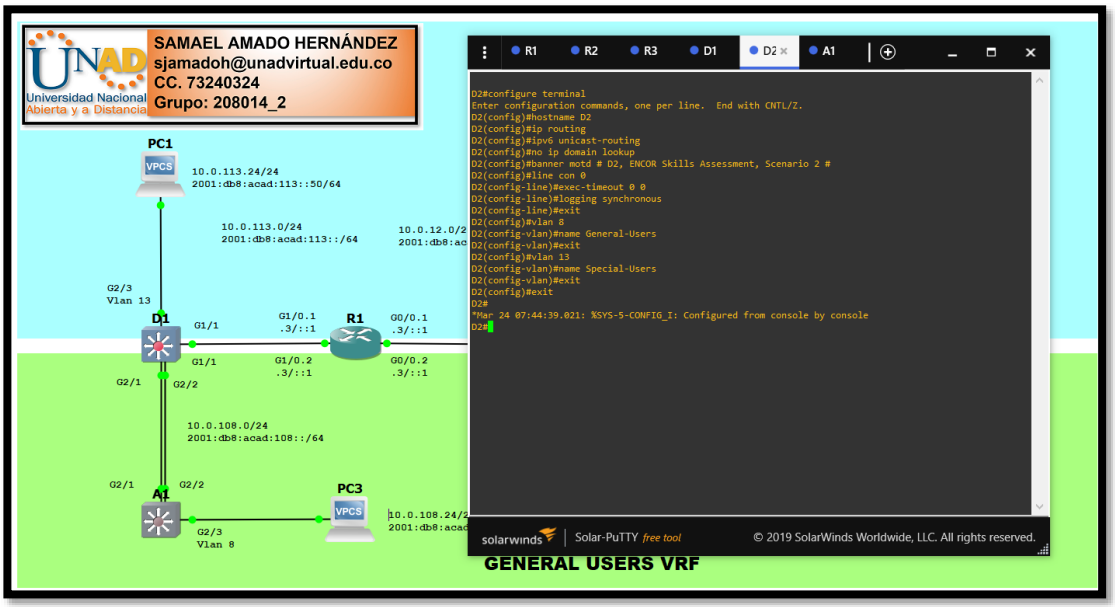

Figura 12. Configuración de inicio *Switch D2 en Solar-PuTTY GNS3*

Figura 13. Configuración de inicio *Switch D2 en Solar-PuTTY GNS3*

Configuración Switch A1

```
A1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#hostname A1
A1(config)#ipv6 unicast-routing
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 2 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 8
A1(config-vlan)#name General-Users
A1(config-vlan)#exit
A1(config)#exit
A1#
```

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global del Switch A1 aplicando las configuraciones de inicio para el equipo de red.

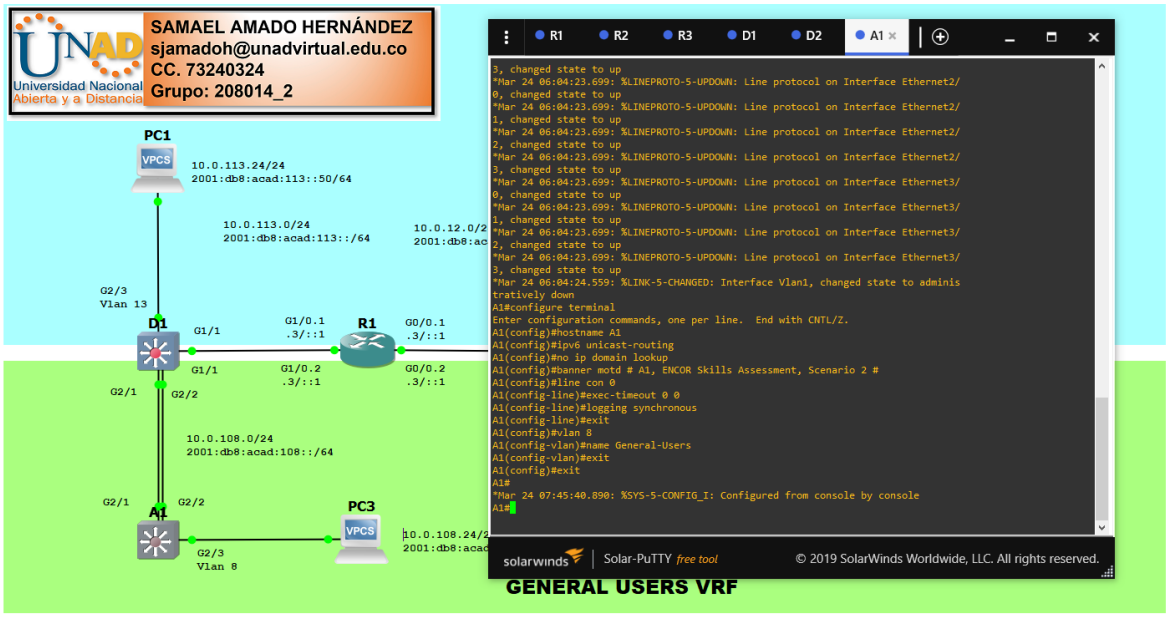

Figura 14. Configuración de inicio Switch A1 en Solar-PuTTY GNS3

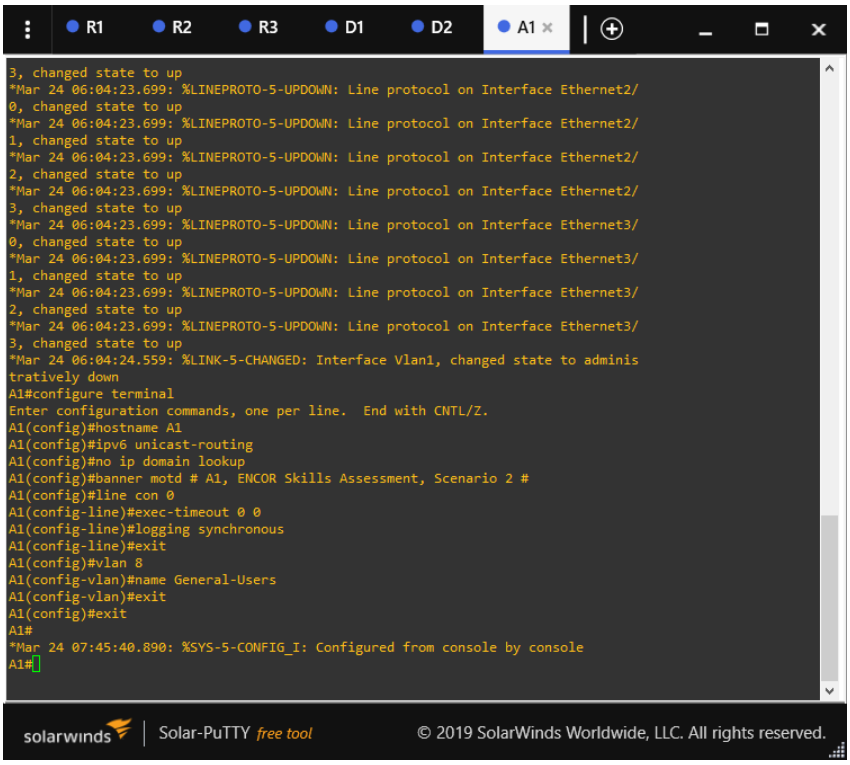

Figura 15. Configuración de inicio Switch A1 en Solar-PuTTY GNS3

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

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global en cada uno de los dispositivos tales como Router 1, Router 2, Router 3, Switch D1, Switch D2 y Switch A1 aplicando las configuraciones para cada equipo de red, de igual forma se guardan los cambios en la memoria de los dispositivos, utilizando el comando **"copy running-config startup-config"**

- ✓ Mediante la herramienta Solar-PuTTY se guardan los cambios en la memoria del dispositivo de red Router 1 y Router 2, utilizando el comando **"copy running-config startup-config"**

Figura 16. Guardado de la configuración Router 1 y Router 2

✓ Mediante la herramienta Solar-PuTTY se guardan los cambios en la memoria del dispositivo de red Router 3 y Switch D1, utilizando el comando **"copy running-config startup-config"**

Figura 17. Guardado de la configuración Router 3 y Switch D1

✓ Mediante la herramienta Solar-PuTTY se guardan los cambios en la memoria del dispositivo de red Switch D2 y Switch A1, utilizando el comando **"copy running-config startup-config"**

Figura 18. Guardado de la configuración Switch D2 y Switch A1

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

Mediante la herramienta Solar-PuTTY ingresamos al modo de configuración global en cada uno de los dispositivos tales como PC1, PC2, PC3 Y PC4 aplicando las configuraciones de IP estática en los PCs según lo dispuesto en la tabla de direccionamiento.

Configuración Pc1

```
PC1> ip 10.0.113.32/24
Checking for duplicate address...
PC1 : 10.0.113.32 255.255.255.0
PC1> ip 2001:db8:acad:113::50/64 fe80::1:3
PC1 : 2001:db8:acad:113::50/64
PC1>
```

Mediante la herramienta Solar-PuTTY asignamos la IP estática IPV4 10.0.113.32 255.255.255.0 e IVP6 2001:db8:acad:113::50/64 fe80::1:3 al Pc1.

Figura 19. Asignación de IP estática al PC1

Configuración Pc2

```
PC2> ip 10.0.213.32/24
Checking for duplicate address...
PC1 : 10.0.213.32 255.255.255.0
PC2> ip 2001:db8:acad:213::50/64 fe80::3:3
PC1 : 2001:db8:acad:213::50/64
PC2>
```

Mediante la herramienta Solar-PuTTY asignamos la IP estática IPV4 10.0.213.32 255.255.255.0 e IVP6 2001:db8:acad:213::50/64 fe80::3:3 al Pc2.

Figura 20. Asignación de IP estática al PC2

Configuración Pc3

```
PC3> ip 10.0.108.32/24
Checking for duplicate address...
PC1 : 10.0.108.32 255.255.255.0
PC3> ip 2001:db8:acad:108::50/64 fe80::1:4
PC1 : 2001:db8:acad:108::50/64
PC3>
```

Mediante la herramienta Solar-PuTTY asignamos la IP estática IPV4 10.0.108.32 255.255.255.0 e IVP6 2001:db8:acad:108::50/64 fe80::1:4 al Pc3.

Figura 21. Asignación de IP estática al PC3

Configuración Pc4

```
PC4> ip 10.0.208.32/24
Checking for duplicate address...
PC1 : 10.0.208.32 255.255.255.0
PC4> ip 2001:db8:acad:208::50/64 fe80::3:4
PC1 : 2001:db8:acad:208::50/64
PC4>
```

Mediante la herramienta Solar-PuTTY asignamos la IP estática IPV4 10.0.208.32 255.255.255.0 e IVP6 2001:db8:acad:208::50/64 fe80::3:4 al Pc4.

Figura 22. Asignación de IP estática al PC4

Parte 2: configurar VRF y enrutamiento estático

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

Se realiza la configuración en los Routers (R1,R2 y R3) para la creación de las VRFs (del inglés Virtual Routing and Forwarding, enrutamiento virtual y reenvío) denominadas (General-Users, Special-Users), y habilitación IPV4 e IPV6.

Configuración VRF en el Router R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#vrf definition General-Users
R1(config-vrf)#address-family ipv4
R1(config-vrf-af)#address-family ipv6
R1(config-vrf-af)#exit
R1(config-vrf)#vrf definition Special-Users
R1(config-vrf)#address-family ipv4
R1(config-vrf-af)#address-family ipv6
R1(config-vrf-af)#exit
R1(config-vrf)#exit
R1(config)#
```

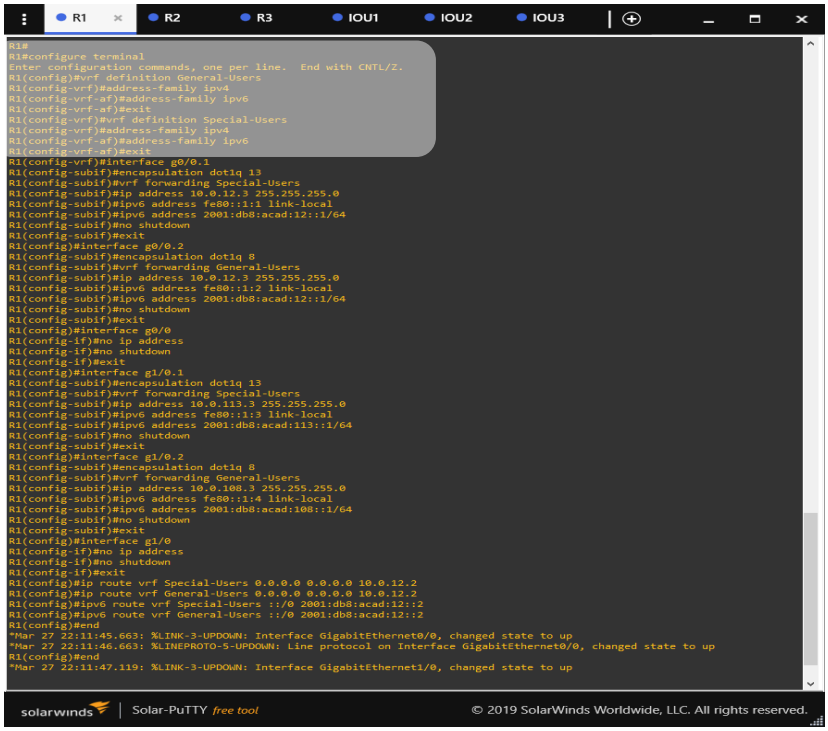

Figura 23. Configuración VRF en el Router R1

Configuración VRF en el Router R2

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#vrf definition General-Users
R2(config-vrf)#address-family ipv4
R2(config-vrf-af)#address-family ipv6
R2(config-vrf-af)#exit
R2(config-vrf)#vrf definition Special-Users
R2(config-vrf)#address-family ipv4
R2(config-vrf-af)#address-family ipv6
R2(config-vrf-af)#exit
R2(config-vrf)#
```

Figura 24. Configuración VRF en el Router R2

Configuración VRF en el Router R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#vrf definition General-Users
R3(config-vrf)#address-family ipv4
R3(config-vrf-af)#address-family ipv6
R3(config-vrf-af)#exit
R3(config-vrf)#vrf definition Special-Users
R3(config-vrf)#address-family ipv4
R3(config-vrf-af)#address-family ipv6
R3(config-vrf-af)#exit
R3(config-vrf)#
```

Figura 25. Configuración VRF en el Router R3

Se verifican de las VRF creadas mediante el comando **Show VRF Brief** verificamos que las VRFs se hayan creado de forma exitosa y se habilite IPV4 e IPV6. se crearon las VRFs *General-User* y *Special-User* habilitando los protocolos IPV4 e IPV6 para el direccionamiento.

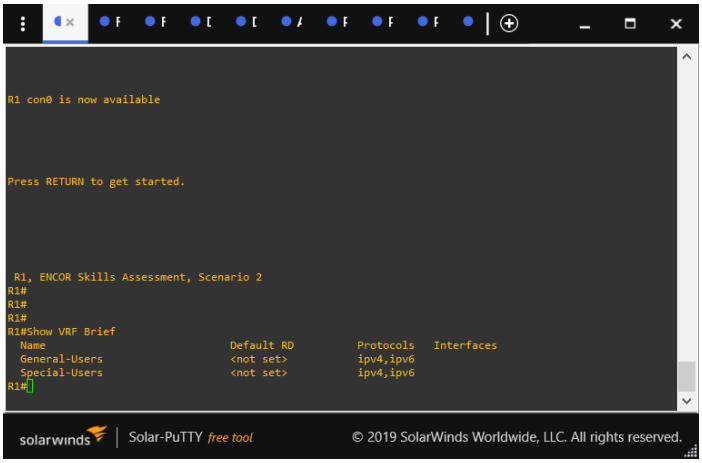

Figura 26. VRF creadas y protocolos IPV4 e IPV6 en R1

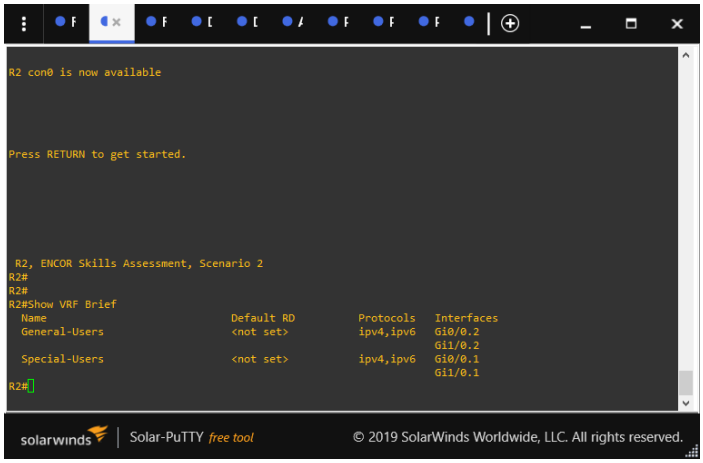

Figura 27. VRF creadas y protocolos IPV4 e IPV6 en R2

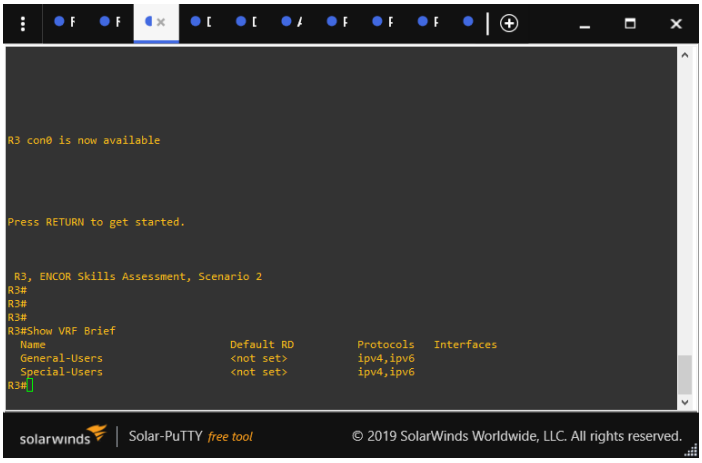

Figura 28. VRF creadas y protocolos IPV4 e IPV6 en R3

2.2. En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.

En esta parte se configuran las sub-interfaces VRF asignado direccionamiento IPV4 e IPV6 en cada Router.

Configuración sub-interfaces VRF en el Router R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/0.1
R1(config-subif)#encapsulation dot1q 13
R1(config-subif)#vrf forwarding Special-Users
R1(config-subif)#ip address 10.0.12.3 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:12::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g0/0.2
R1(config-subif)#encapsulation dot1q 8
R1(config-subif)#vrf forwarding General-Users
R1(config-subif)#ip address 10.0.12.3 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:2 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:12::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g0/0
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface g1/0.1
R1(config-subif)#encapsulation dot1q 13
R1(config-subif)#vrf forwarding Special-Users
R1(config-subif)#ip address 10.0.113.3 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:3 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:113::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g1/0.2
R1(config-subif)#encapsulation dot1q 8
R1(config-subif)#vrf forwarding General-Users
R1(config-subif)#ip address 10.0.108.3 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:4 link-local
```

```
R1(config-subif)#ipv6 address 2001:db8:acad:108::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g1/0
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

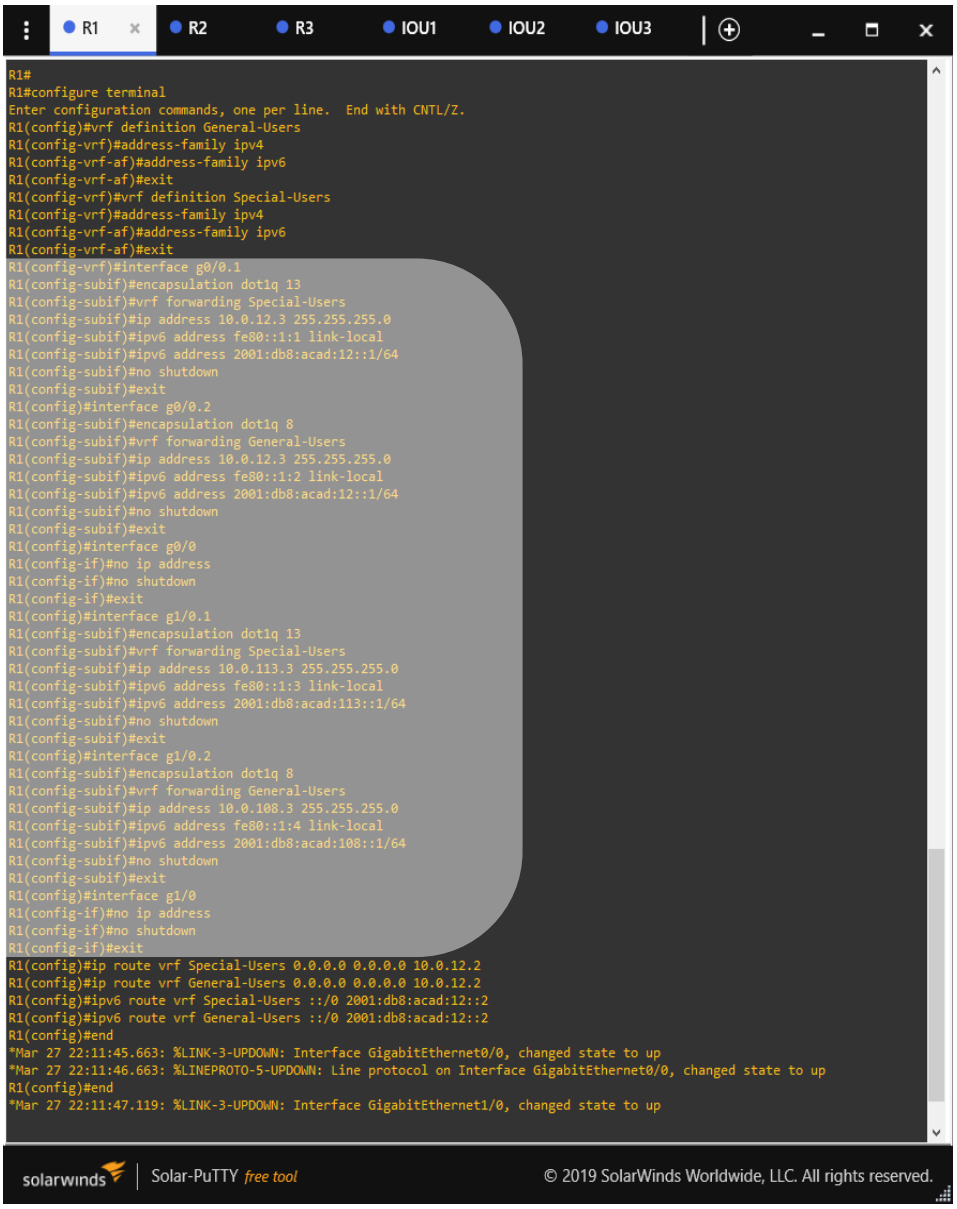

Figura 29. Configuración sub-interfaces VRF en el Router R1

Configuración sub-interfaces VRF en el Router R2

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface g0/0.1
R2(config-subif)#encapsulation dot1q 13
R2(config-subif)#vrf forwarding Special-Users
R2(config-subif)#ip address 10.0.12.2 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:1 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface g0/0.2
R2(config-subif)#encapsulation dot1q 8
R2(config-subif)#vrf forwarding General-Users
R2(config-subif)#ip address 10.0.12.2 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:2 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface g0/0
R2(config-if)#no ip address
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface g1/0.1
R2(config-subif)#encapsulation dot1q 13
R2(config-subif)#vrf forwarding Special-Users
R2(config-subif)#ip address 10.0.23.2 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:3 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:23::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface g1/0.2
R2(config-subif)#encapsulation dot1q 8
R2(config-subif)#vrf forwarding General-Users
R2(config-subif)#ip address 10.0.23.2 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:4 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:23::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface g1/0
R2(config-if)#no ip address
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Figura 30. Configuración sub-interfaces VRF en el Router R2

Configuración sub-interfaces VRF en el Router R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface g1/0.1
R3(config-subif)#encapsulation dot1q 13
R3(config-subif)#vrf forwarding Special-Users
R3(config-subif)#ip address 10.0.23.4 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:1 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#interface g1/0.2
R3(config-subif)#encapsulation dot1q 8
R3(config-subif)#vrf forwarding General-Users
R3(config-subif)#ip address 10.0.23.4 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:2 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#interface g1/0
R3(config-if)#no ip address
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface g0/0.1
R3(config-subif)#encapsulation dot1q 13
R3(config-subif)#vrf forwarding Special-Users
R3(config-subif)#ip address 10.0.213.4 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:3 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:213::1/64
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#interface g0/0.2
R3(config-subif)#encapsulation dot1q 8
R3(config-subif)#vrf forwarding General-Users
R3(config-subif)#ip address 10.0.208.4 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:4 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:208::1/64
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#interface g0/0
R3(config-if)#no ip address
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

Figura 31. Configuración sub-interfaces VRF en el Router R3

Se Verifica el direccionamiento IP configurado para cada VRF.

Se realiza la verificación en los Routers de las interfaces VRF creadas, mediante el comando **show ip vrf interfaces** confirmando direccionamiento IPV4 e IPV6.

*Figura 32. Comando show **ip vrf interfaces** en Router 1*

Se puede observar el direccionamiento VRF aplicado a las sub-interfaces de los Router 1 confirmando el direccionamiento IPV4 e IPV6.

*Figura 33. Comando show **ip vrf interfaces** en Router 2*

Se puede observar el direccionamiento VRF aplicado a las sub-interfaces de los Router 2 confirmando el direccionamiento IPV4 e IPV6.

*Figura 34. Comando show **ip vrf interfaces** en Router 3*

Se puede observar el direccionamiento VRF aplicado a las sub-interfaces de los Router 3 confirmando el direccionamiento IPV4 e IPV6.

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

En esta parte se configuran las IPs estáticas IPV4 e IPV6 que apuntaran al R2.se adjuntan pantallazos y código.

Configuración IPs estáticas R1.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)#ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)#ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2
R1(config)#ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2
R1(config)#end
R1#
```

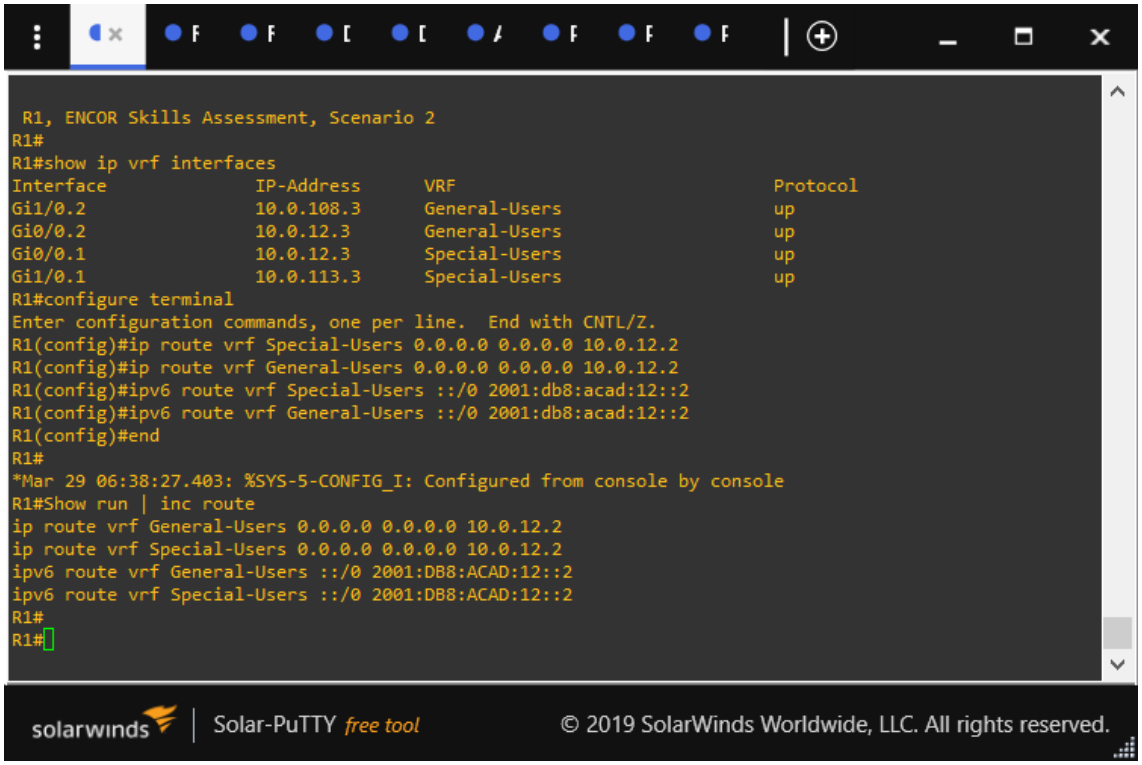

Figura 35. Configuración IPs estáticas IPV4 e IPV6 en R1

Configuración IPs estáticas R2.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.3
R2(config)#ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.4
R2(config)#$vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1
R2(config)#$vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3
R2(config)#ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.3
R2(config)#ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.4
R2(config)#$vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1
R2(config)#$vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3
R2(config)#end
R2#
```

Figura 36. Configuración IPs estáticas IPV4 e IPV6 en R2

Configuración IPs estáticas R3.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2
R3(config)#ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2
R3(config)#ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2
R3(config)#ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2
R3(config)#end
R3#
```

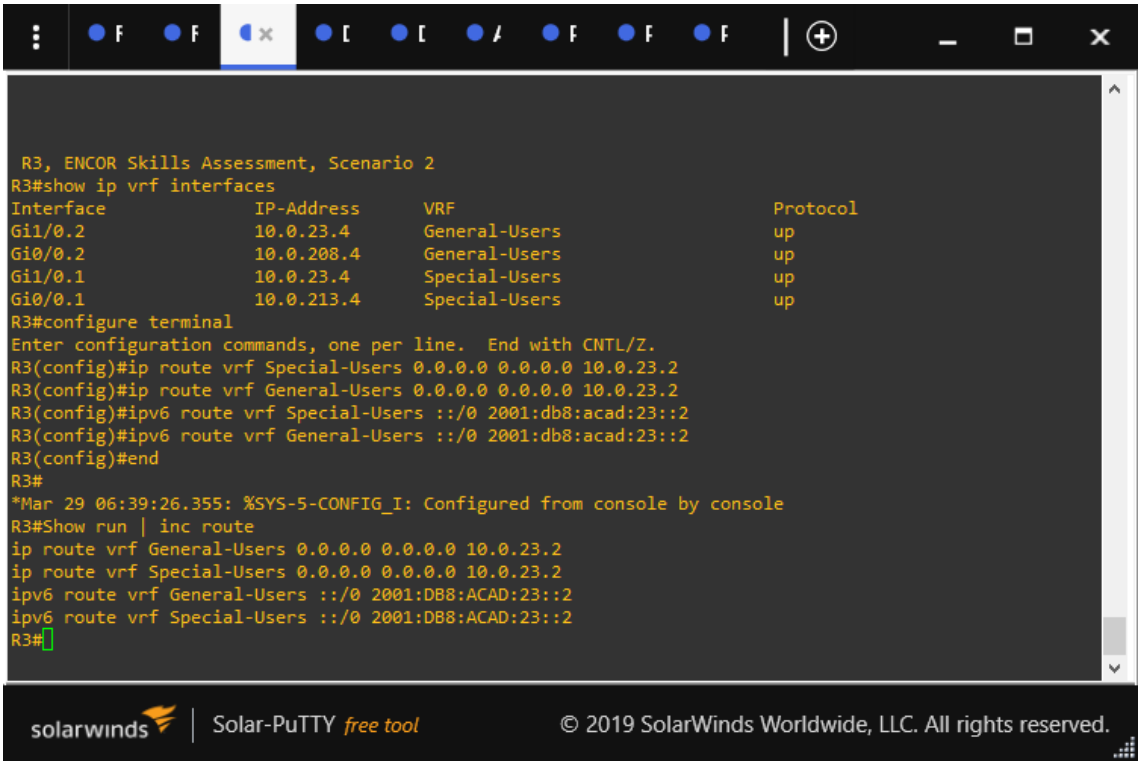

Figura 37. Configuración IPs estáticas IPV4 e IPV6 en R3

Se verifican las rutas estáticas en R1,R2 y R3.

Se ejecuta el comando **Show run | inc route**, para verificar la ruta estática VRF IPV4 e IPV6 configurada en cada Router, esto nos permite conocer las rutas asignadas en cada equipo, y verificar el direccionamiento VRF.

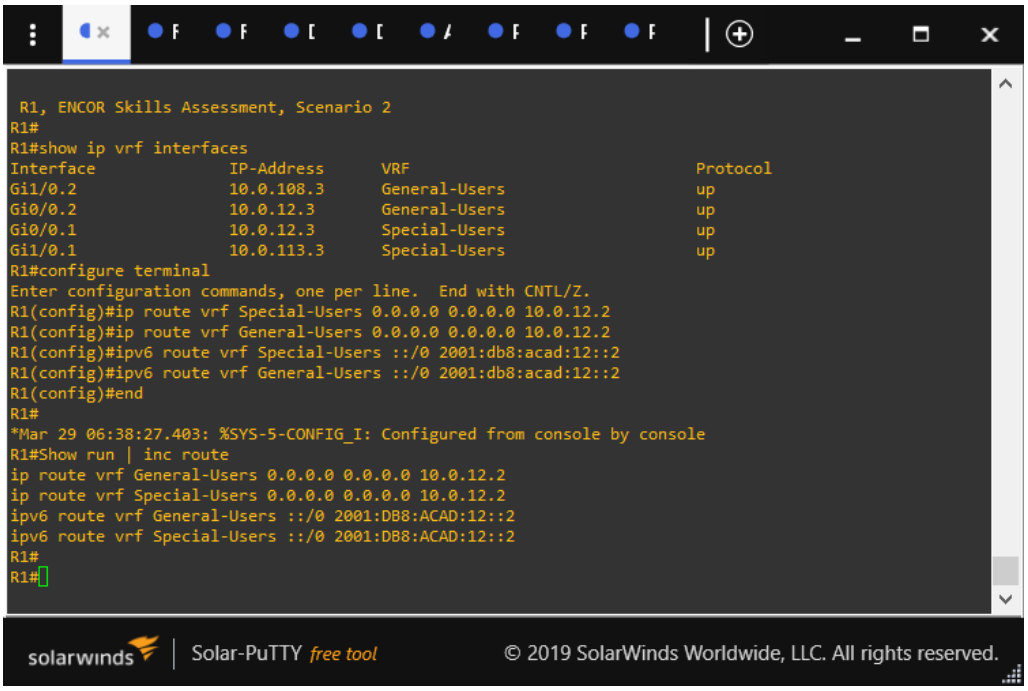

*Figura 38. Comando **Show run | inc route** en Router 1*

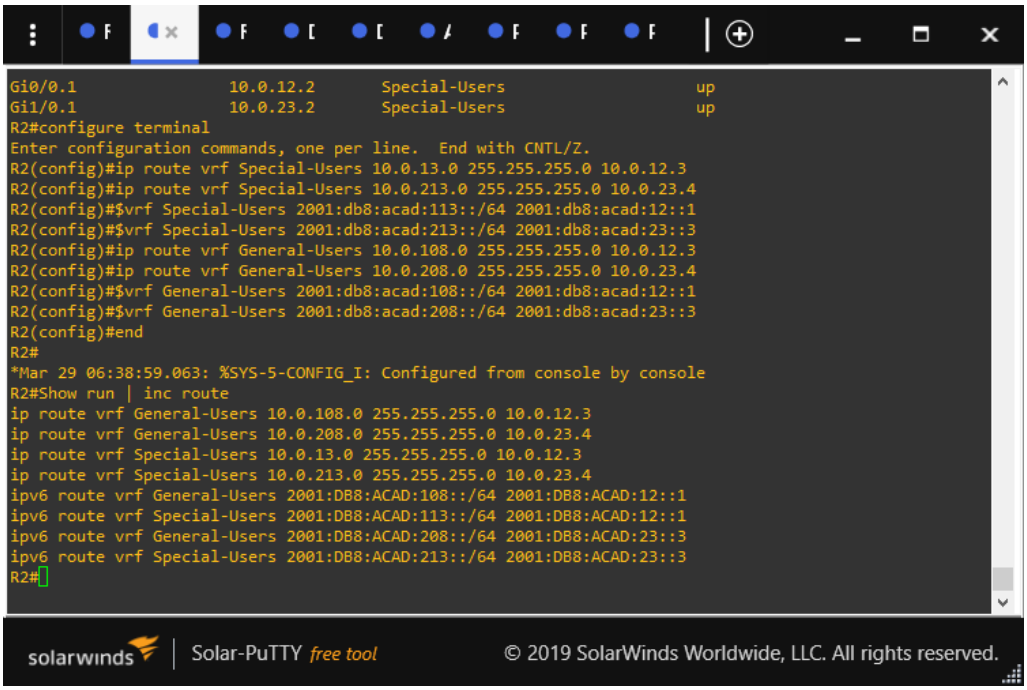

*Figura 39. Comando **Show run | inc route** en Router 2*

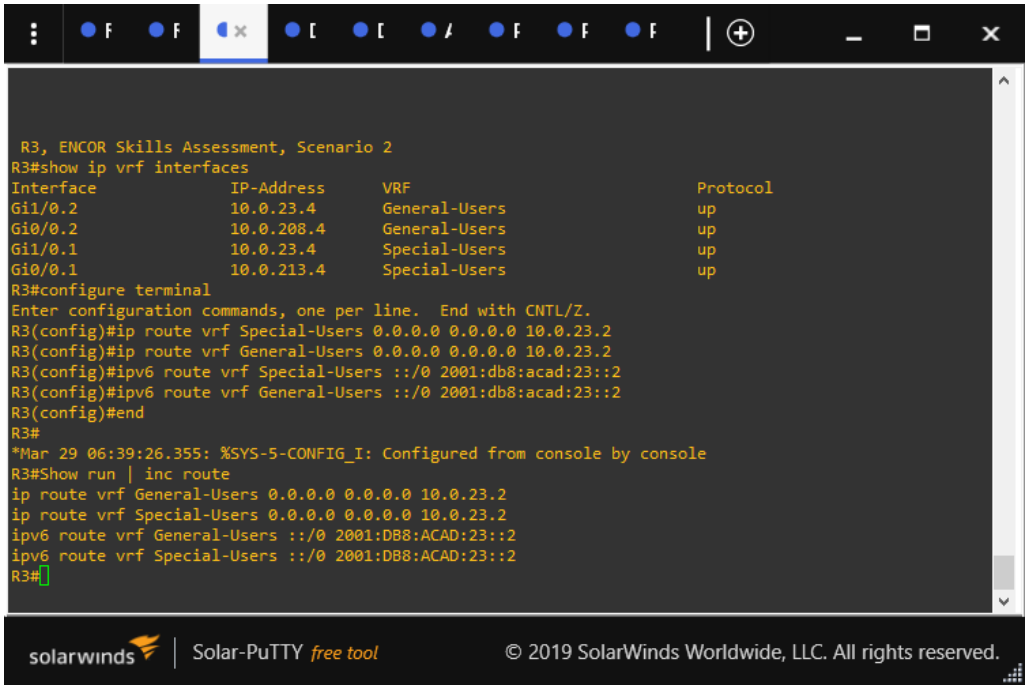

*Figura 40. Comando **Show run | inc route** en Router 3*

2.4 Verifique la conectividad en cada VRF.

2.4. Verifique la conectividad en cada VRF.

En esta parte del informe se realiza la verificación de conectividad de las distintas VRFs mediante el comando Ping vrf.

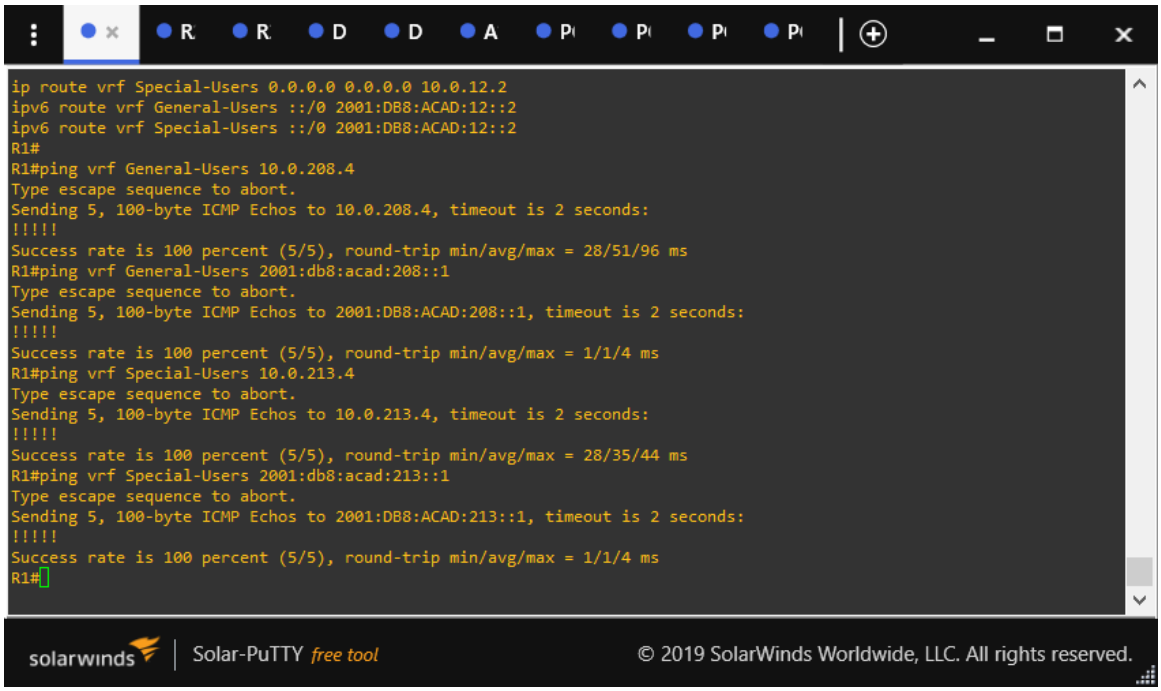

Figura 41. Ping VRF R1 a R3.

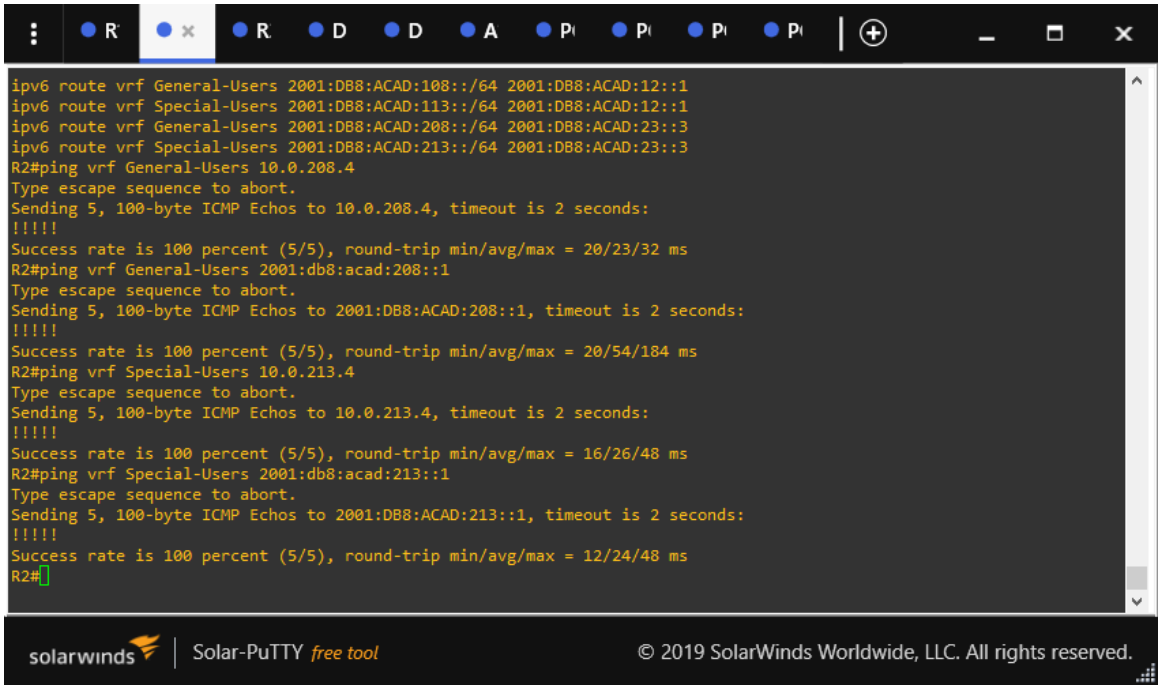

Figura 42. Ping VRF R2 a R3.

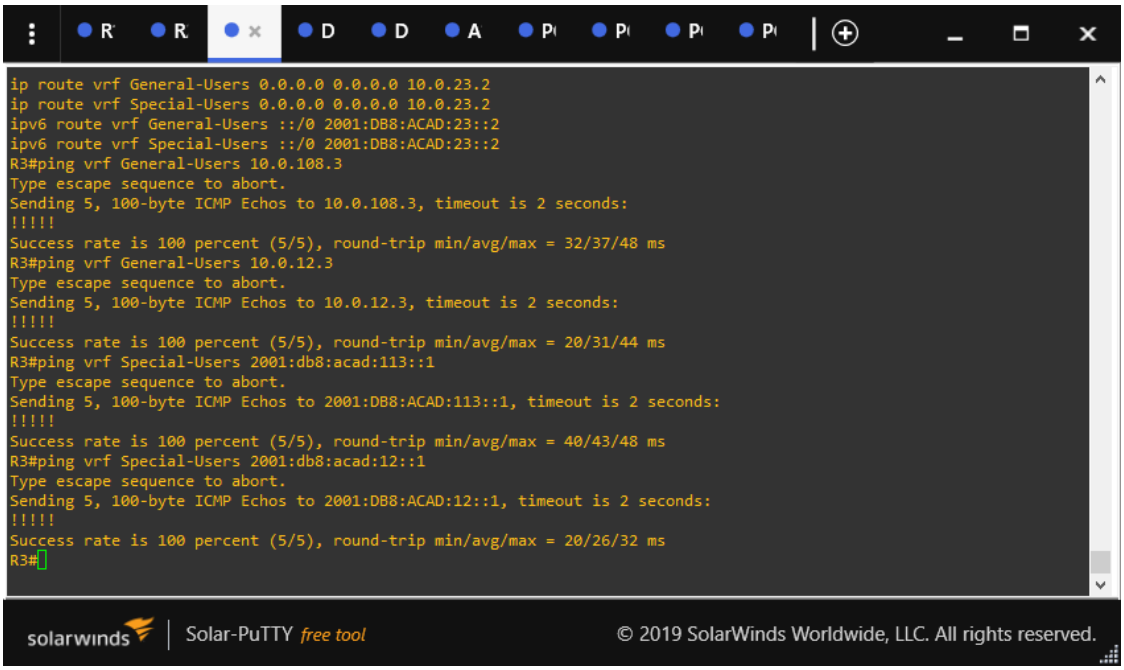

Figura 43. Ping VRF R3.a R1

DESARROLLO ESCENARIO 2 PARTE 3

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:

Tabla 4. Configurar Switch capa 2.

Task#	Task	Specification
3.1	On D1, D2, and A1, disable all interfaces.	On D1 and D2, shutdown G1/0/1 to G1/0/24. On A1, shutdown F0/1 – F0/24, G0/1 – G0/2.
3.2	On D1 and D2, configure the trunk links to R1 and R3.	Configure and enable the G1/0/11 link as a trunk link.
3.3	On D1 and A1, configure the EtherChannel.	On D1, configure and enable: • Interface G1/0/5 and G1/0/6 • Port Channel 1 using PAgP On A1, configure enable: • Interface F0/1 and F0/2 • 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 G1/0/23 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface G1/0/23 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface G1/0/24 as an access port in VLAN 8 and enable Portfast. • On A1, configure interface F0/23 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.

Escenario elaborado en GNS3

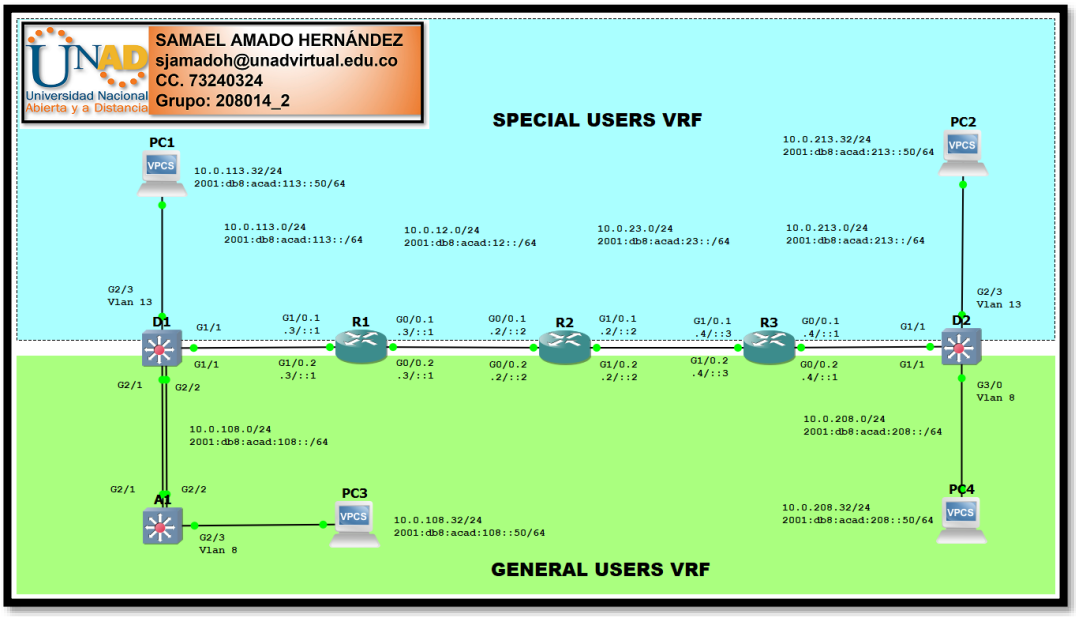

Figura 44. Escenario elaborado en GNS3 parte 3 y 4

Tabla 5. Tabla de direccionamiento elaborada y aplicada en GNS3

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G1/0.1	10.0.12.X/24	2001:db8:acad:12::1/64	fe80::1:1
	G1/0.2	10.0.12.X/24	2001:db8:acad:12::1/64	fe80::1:2
	G1/1.1	10.0.113.X/24	2001:db8:acad:113::1/64	fe80::1:3
	G1/1.2	10.0.108.X/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G1/0.1	10.0.12.Y/24	2001:db8:acad:12::2/64	fe80::2:1
	G1/0.2	10.0.12.Y/24	2001:db8:acad:12::2/64	fe80::2:2
	G1/1.1	10.0.23.Y/24	2001:db8:acad:23::2/64	fe80::2:3
	G1/1.2	10.0.23.Y/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G1/0.1	10.0.23.Z/24	2001:db8:acad:23::3/64	fe80::3:1
	G1/0.2	10.0.23.Z/24	2001:db8:acad:23::3/64	fe80::3:2
	G1/1.1	10.0.213.Z/24	2001:db8:acad:213::1/64	fe80::3:3
	G1/1.2	10.0.208.Z/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.XY/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.XY/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.XY/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.XY/24	2001:db8:acad:208::50/64	EUI-64

DESARROLLO DE LA ACTIVIDAD

3.1. Parte 3 paso 1. En este paso hay que deshabilitar todas las interfaces de los equipos activos de red D1, D2 y A1. Se realiza el procedimiento apagando las interfaces Ethernet de los Switchs D1, D2 y A1 mediante el comando Shutdown. De igual forma se anexa el código y pantallazos de GNS3.

Configuración Switch D1.

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 2 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 8
D1(config-vlan)#name General-Users
D1(config-vlan)#exit
D1(config)#vlan 13
D1(config-vlan)#name Special-Users
D1(config-vlan)#exit
D1(config)#interface range e0/0-3,e1/0-3,e2/0-3,e3/0-3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1(config)#exit
D1#
```

Figura 45. Apagado de interfaces D1

Configuración Switch D2.

```
D2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 2 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 8
D2(config-vlan)#name General-Users
D2(config-vlan)#exit
D2(config)#vlan 13
D2(config-vlan)#name Special-Users
D2(config-vlan)#exit
D2(config)#interface range e0/0-3,e1/0-3,e2/0-3,e3/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#exit
D2#
```

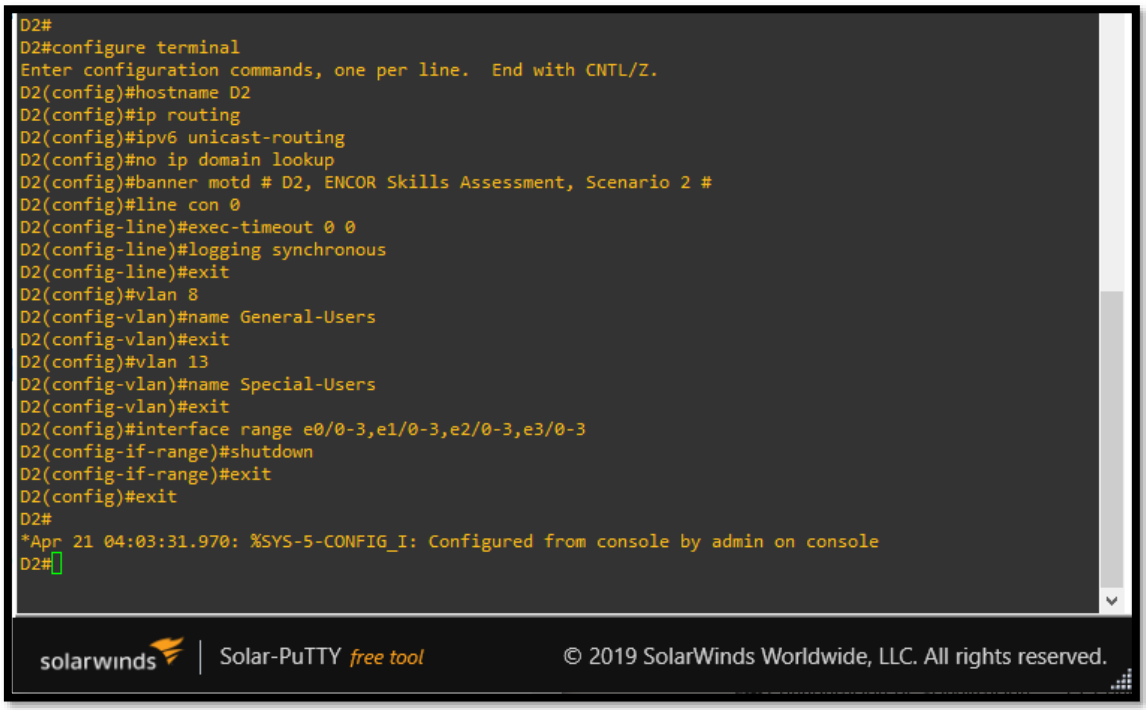

Figura 46. Apagado de interfaces D2

Configuración Switch A1.

```
A1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#hostname A1
A1(config)#ipv6 unicast-routing
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 2 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 8
A1(config-vlan)#name General-Users
A1(config-vlan)#exit
A1(config)#interface range e0/0-3,e1/0-3,e2/0-3,e3/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#exit
A1#
```

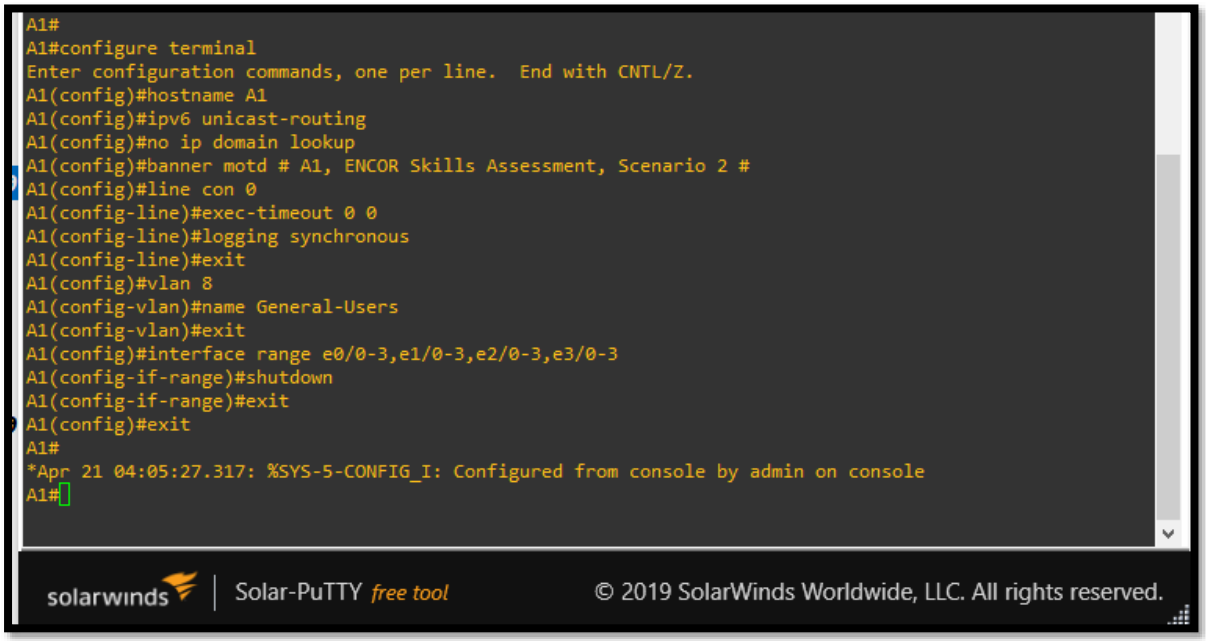

Figura 47. Apagado de interfaces A1

3.2. Parte 3 paso 2. En este paso hay que configurar los enlaces troncales que van D1 y D2, hacia R1 y R3.

Para realizar el procedimiento se configuran las interfaces Ethernet 1/1 de los Switch D1 y D2, utilizando los comandos **`switchport trunk encapsulation do1q`** el cual se utiliza para habilitar el encapsulamiento do1q y el comando **`switchport mode trunk`** el cual nos permite establecer los enlaces troncales que admitirán la salida de paquetes a R1 y R3. se anexa el código y pantallazos de GNS3.

Configuración Switch D1.

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#interface e1/1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#exit
D1#
```

Figura 48. Configuración enlace troncal en D1

Configuración Switch D2.

```
D2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#interface e1/1
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#exit
D2#
```

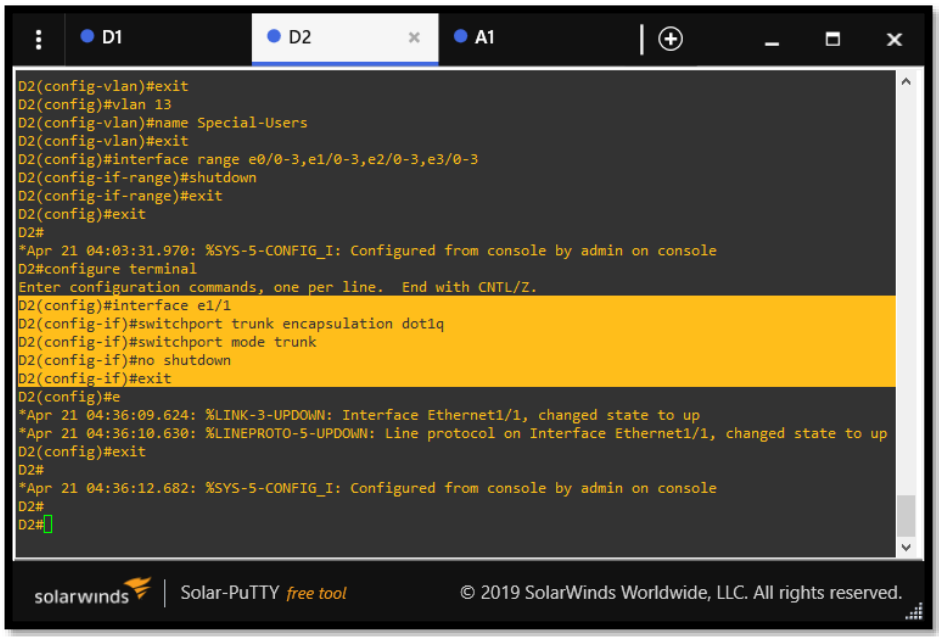

Figura 49. Configuración enlace troncal en D2.

Paso a seguir se verifican las interfaces troncales con el comando **`Show Interface Trunk`** constatando la configuración de los enlaces troncales en los Switchs D1 y D2 de la topología establecida en el escenario 2.

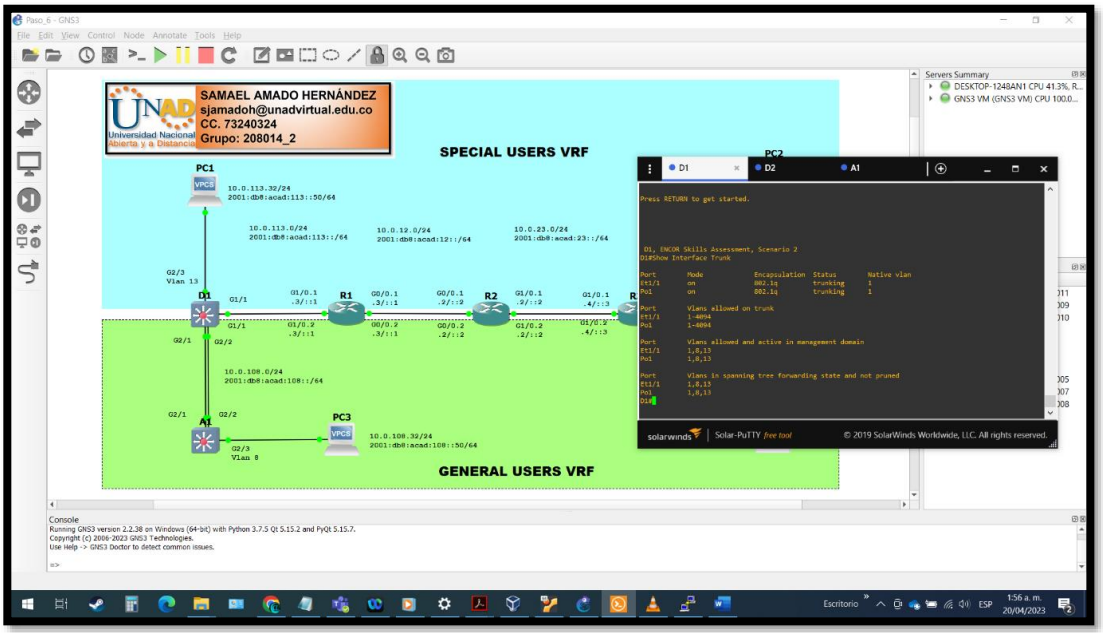

Figura 50. Show Interface Trunk D1.

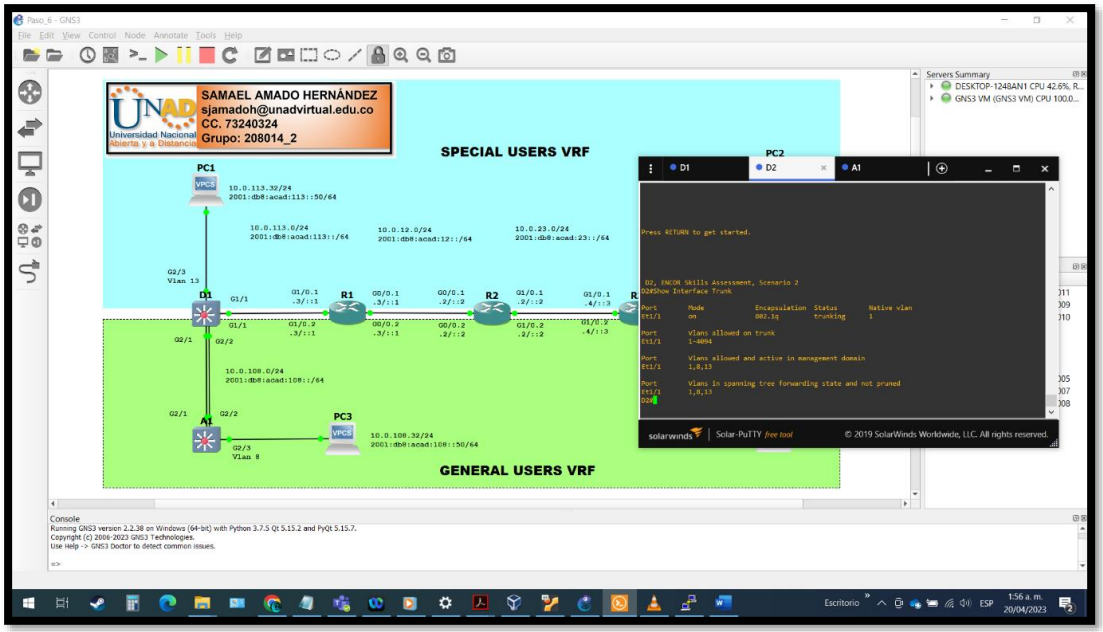

Figura 51. Show Interface Trunk D2.

3.3. Para esta parte configuramos EthernetChannel en los Switch D1 y A1 de forma que agrupamos los 2 enlaces físicos en un enlace lógico configurado en modo troncal, que admitirá la salida de las Vlans. se anexa el código y pantallazos de GNS3.

Configuración Switch D1.

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#interface range e2/1-2
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#channel-group 1 mode desirable
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#exit
D1#
```

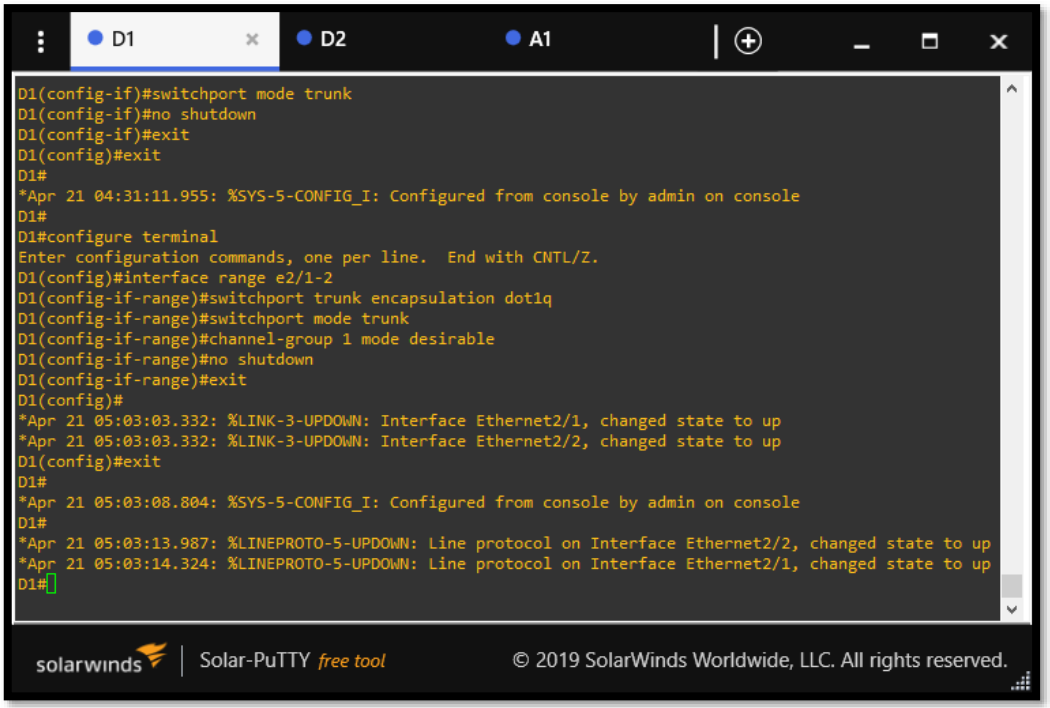

Figura 52. Configuración EtherChannel D1.

Configuración Switch A1.

```
A1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#interface range e2/1-2
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#channel-group 1 mode desirable
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#exit
A1#
```

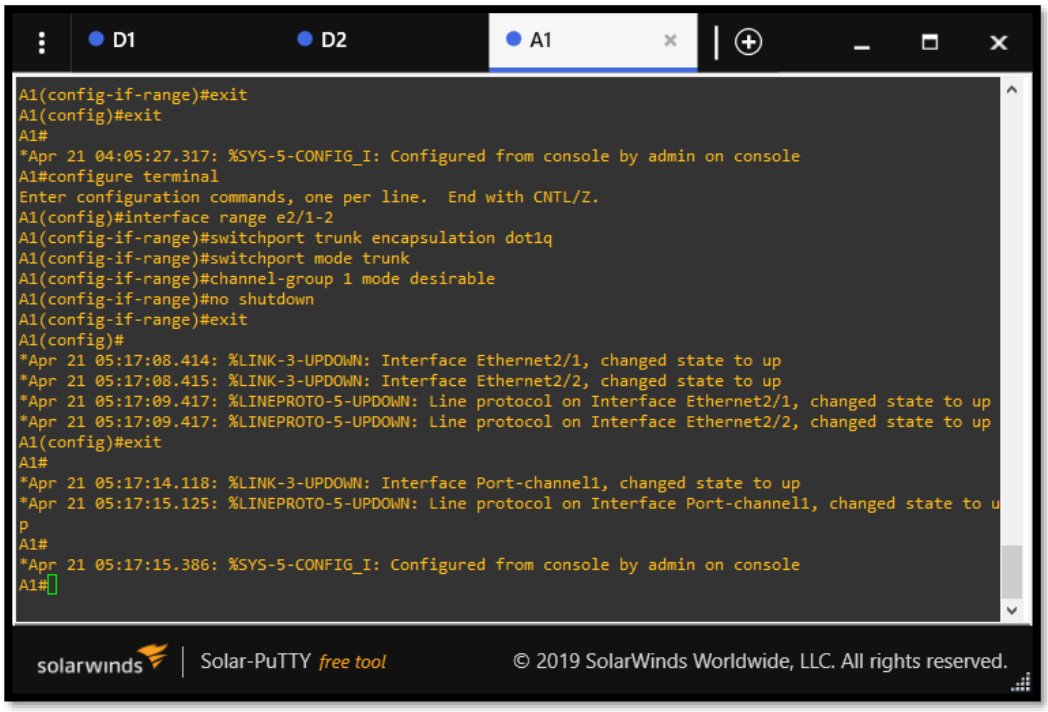

Figura 53. Configuración EtherChannel A1.

Mediante las líneas de comando de Solar-PuTTY se agruparon las interfaces Ethernet 2/1 y Ethernet 2/2 de los dispositivos Switch D1 y A1 mediante la configuración channel-group 1 que crea la interfaz PortChannel y el modo desirable que permite la transmisión de paquetes PAgP. De igual forma se habilita el enlace en modo troncal mediante el comando **`switchport mode trunk`** en los dos Switchs.

A continuación, verificaremos la configuración de Ethernet-Channel mediante el comando **`show etherchannel summary`** constatando que se encuentre creado el enlace Port-Channel1 y se habilite el tráfico PAgP.

Figura 54. Port-Channel en D1

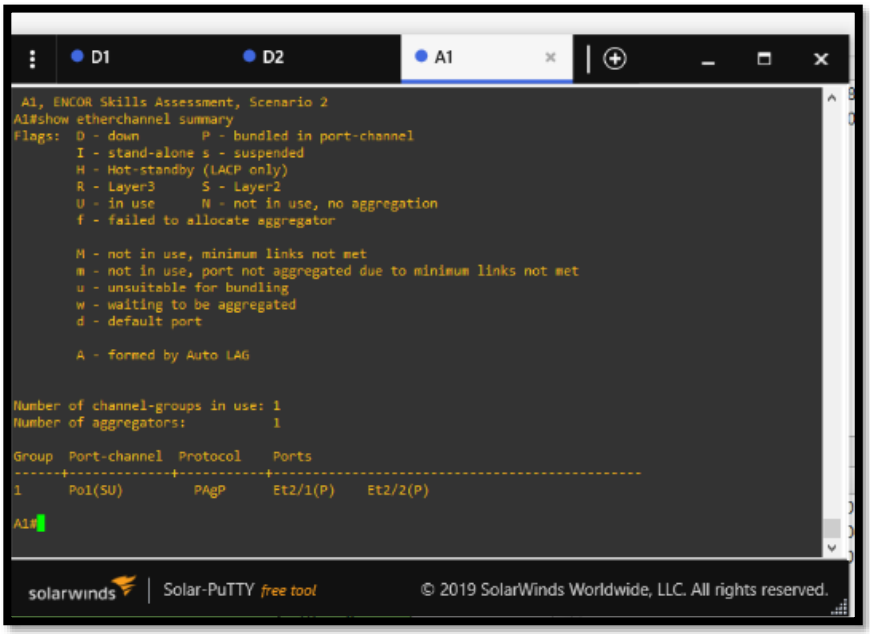

Figura 55. Port-Channel en A1.

3.4. Parte 3 paso 4. En este paso se configura los puertos de acceso en los dispositivos de red switch D1, D2 y A1 para los PC1, PC2, PC3 y PC4. Mediante los comandos **`switchport mode access`** que permiten que la interfaz cambie a modo acceso y **`switchport access vlan`** que permite el acceso a las Vlans. Y utiliza el comando **`spanning-tree portfast`** para habilitar el portfast en las interfaces según lo requerido. se anexa el código y pantallazos de GNS3.

Configuración D1

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#interface e2/3
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 13
D1(config-if)#spanning-tree portfast
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#exit
D1#
```

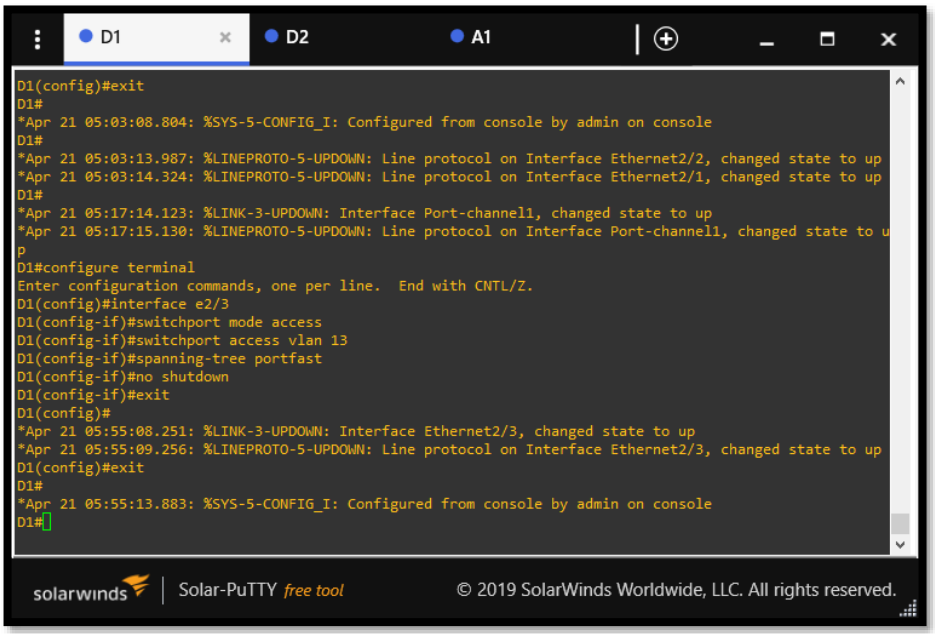

Figura 56. modo acceso en D1.

Configuración D2

```
D2(config)#interface e2/3
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 13
D2(config-if)#spanning-tree portfast
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface e3/0
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 8
D2(config-if)#spanning-tree portfast
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#exit
D2#
```

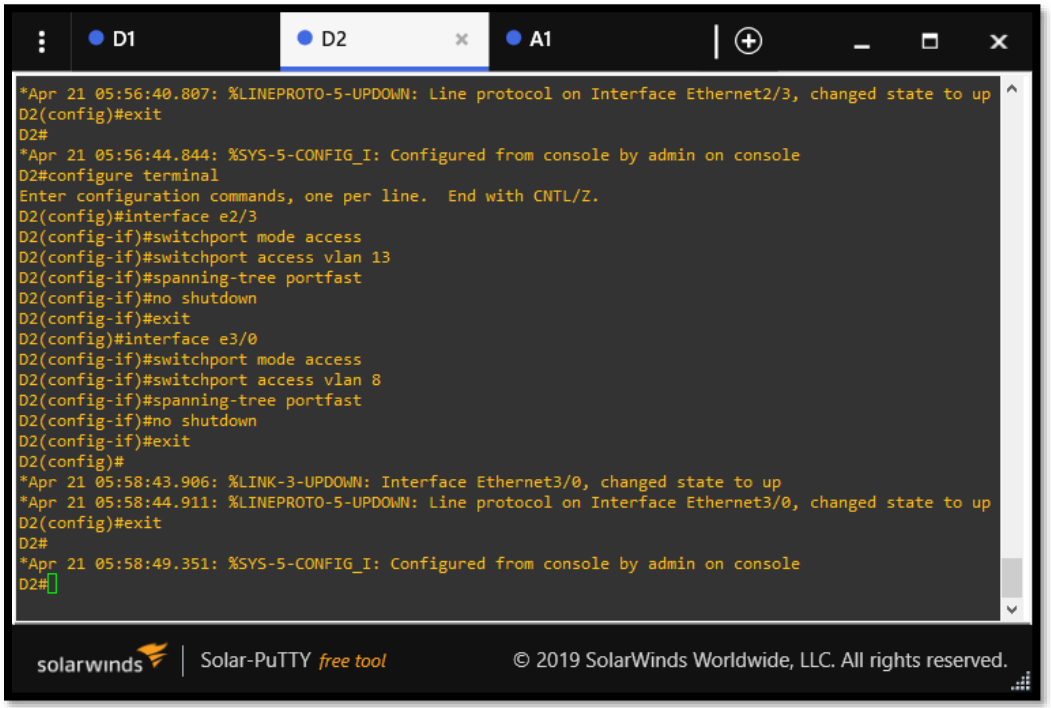

Figura 57. modo acceso en D2.

Configuración A1

```
A1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#interface e2/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 8
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#exit
A1#
```

Figura 58. modo acceso en A1.

Mediante el comando **`Show run interface`** se verifica la configuración en cada interface en los dispositivos de red switch D1, D2 y A1.

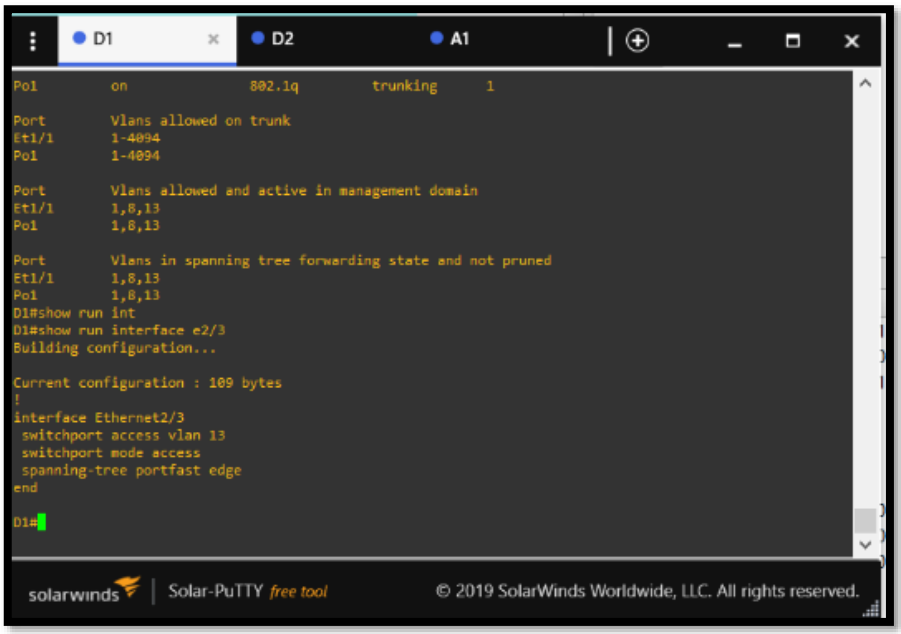

Figura 59. interfaces configuradas en D1

Figura 60. interfaces configuradas en D2

Figura 61. interfaces configuradas en A1

3.5. Parte 3 paso 5. Verifique la conectividad de PC a PC. Se realiza la verificación de conexión entre los PCs Desde la PC1, se verifica la conectividad IPv4 e IPv6 al PC2.

Y Desde la PC3, se verifica la conectividad IPv4 e IPv6 al PC4, mediante el comando Ping, validando comunicación en la red establecida. se anexa el código y pantallazos de GNS3.

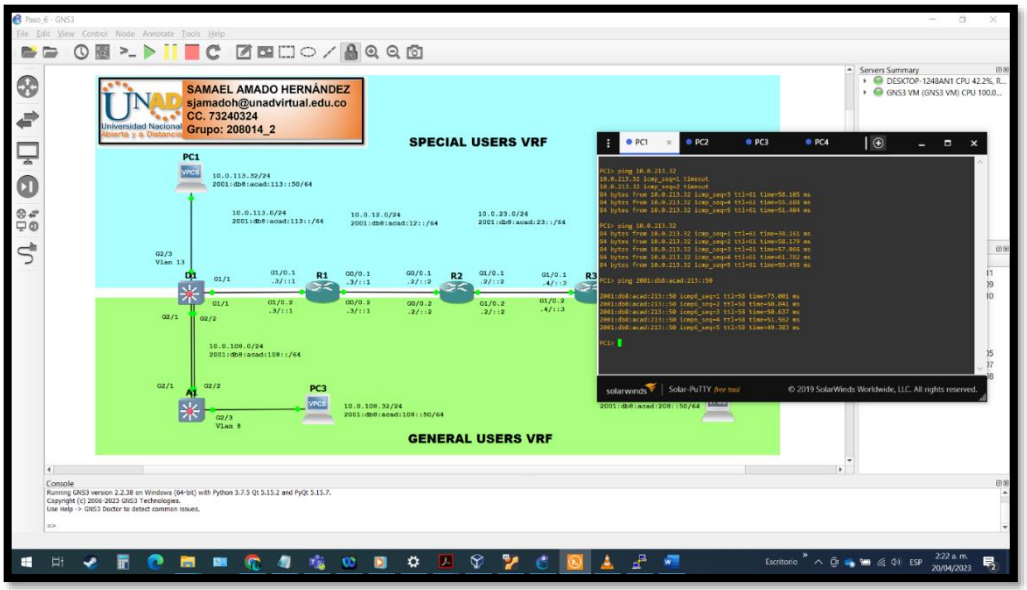

Figura 62. Ping de PC1 a PC2.

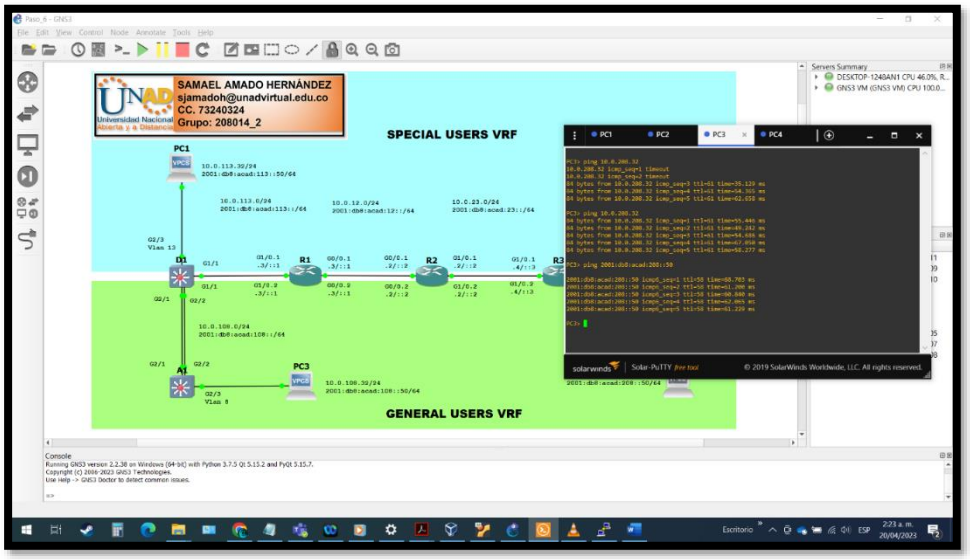

Figura 63. Ping de PC3 a PC4.

Figura 64. Ping de PC1 a PC2 y Ping de PC3 a PC4.

se evidencia comunicación exitosa entre los PCs, por lo cual podemos concluir que la configuración de la red fue satisfactoria.

DESARROLLO ESCENARIO 2 PARTE 4

Parte 4. Configurar seguridad.

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tabla 6. Configurar Switch capa 2.

Task#	Task	Specification
4.1	On all devices, secure privileged EXE mode.	Configure an enable secret as follows: • Algorithm type: **SCRYPT** • Password: **cisco12345cisco**.
4.2	On all devices, create a local user account.	Configure a local user: • Name: **admin** • Privilege level: **15** • Algorithm type: **SCRYPT** • Password: **cisco12345cisco**.
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

4.1. Parte 4 paso 1. En todos los dispositivos, modo EXE privilegiado seguro. Se configura un password secreto en todos los dispositivos utilizando un algoritmo tipo SCRYP. Mediante el comando **`enable algorithm-type scrypt secret`**. Es de tener en cuenta que al configurar el password secreto en los dispositivos nos solicitara una contraseña cuando queramos ingresar a la consola. se anexa el código y pantallazos de GNS3.

Configuración R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable algorithm-type scrypt secret cisco12345cisco
R1(config)#exit
R1#
```

Figura 65. Configuración de Password en R1.

Configuración R2

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#enable algorithm-type scrypt secret cisco12345cisco
R2(config)#exit
R2#
```

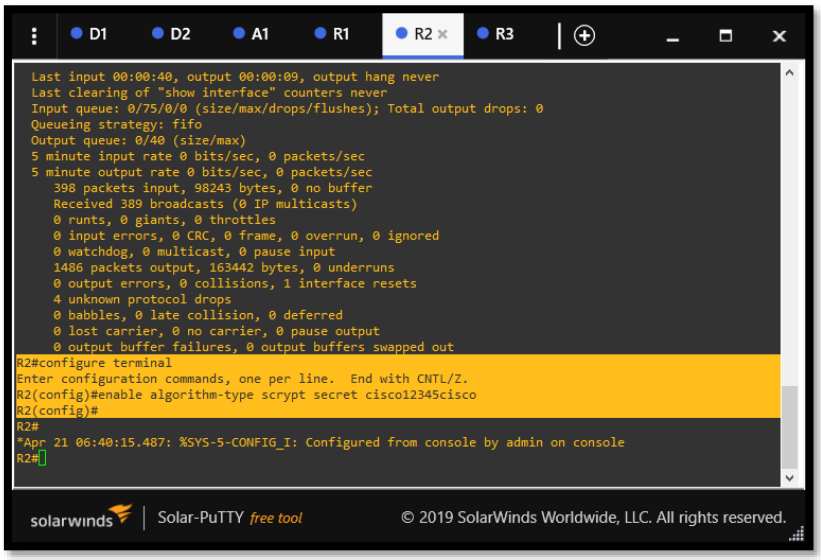

Figura 66. Configuración de Password en R2.

Configuración R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#enable algorithm-type scrypt secret cisco12345cisco
R3(config)#exit
R3#
```

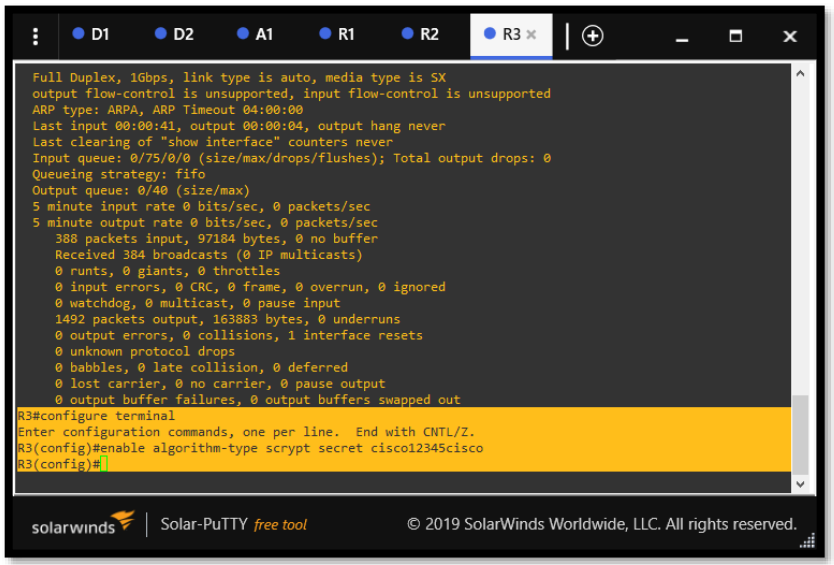

Figura 67. Configuración de Password en R3.

Configuración D1

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
D1(config)#exit
D1#
```

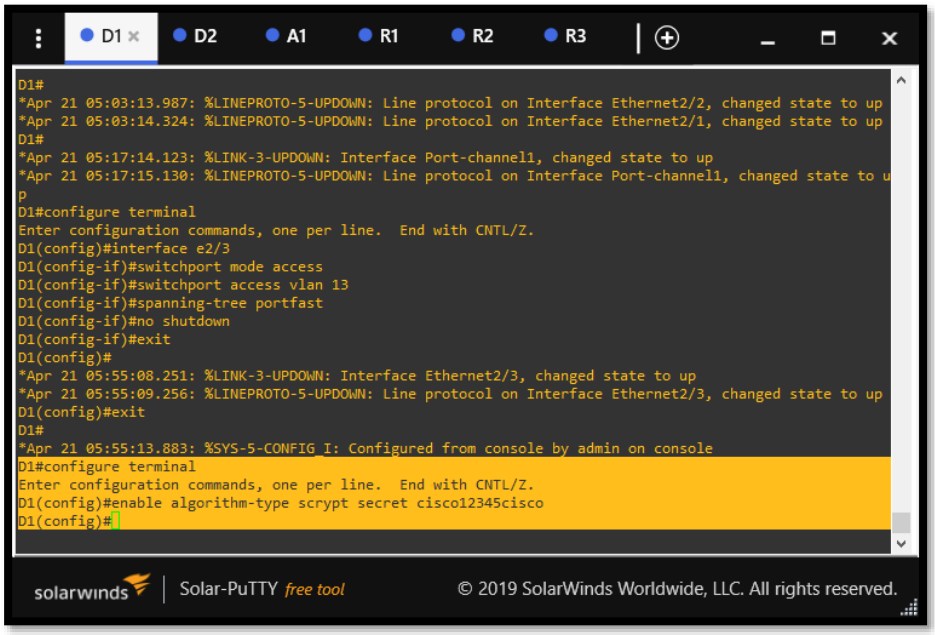

Figura 68. Configuración de Password en D1.

Configuración D2

```
D2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#enable algorithm-type scrypt secret cisco12345cisco
D2(config)#exit
D2#
```

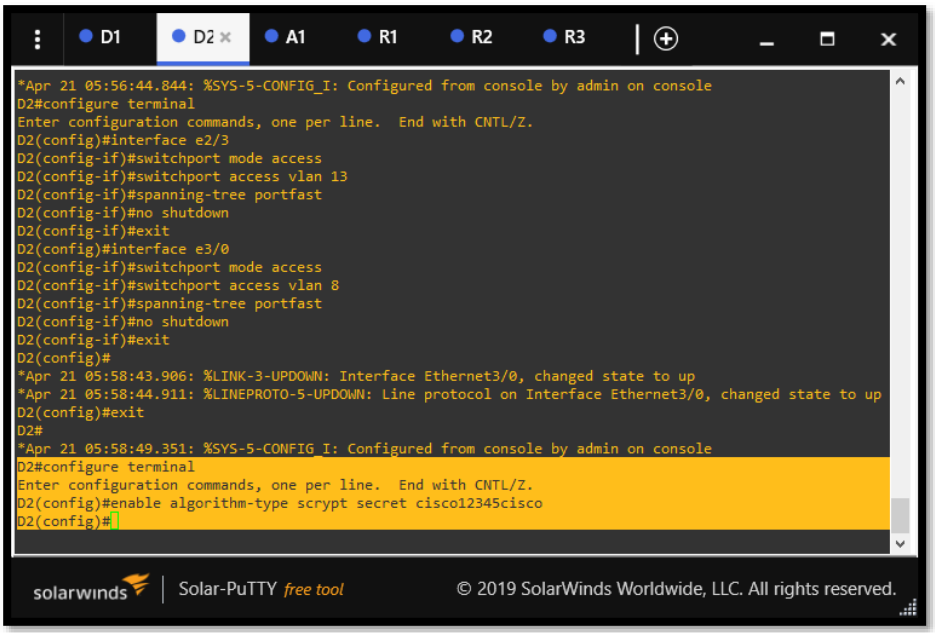

Figura 69. Configuración de Password en D2.

Configuración A1

```
A1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#enable algorithm-type scrypt secret cisco12345cisco
A1(config)#exit
A1#
```

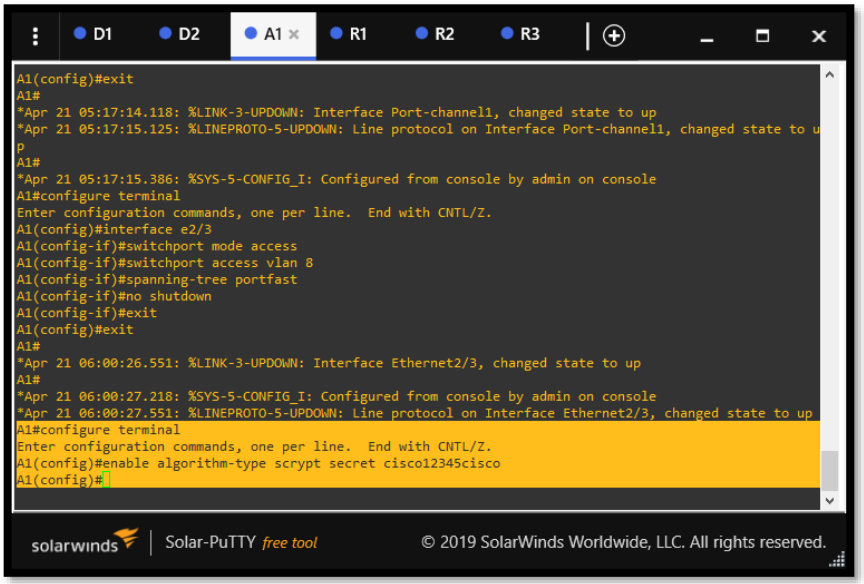

Figura 70. Configuración de Password en A1.

4.2. Parte 4 paso 2. En todos los dispositivos, cree una cuenta de usuario local. Se crea el usuario y se le otorgan los privilegios mediante el comando username admin privilege 15 algorithm-type scrypt secret cisco12345cisco. se anexa el código y pantallazos de GNS3.

Configuración R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username admin privilege 15 algorithm-type scrypt secret
cisco12345$
R1(config)#exit
R1#
```

Figura 71. Configuración de usuario en R1.

Configuración R2

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username admin privilege 15 algorithm-type scrypt secret
cisco12345$
R2(config)#exit
R2#
```

Figura 72. Configuración de usuario en R2.

Configuración R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username admin privilege 15 algorithm-type scrypt secret
cisco12345$
R3(config)#exit
R3#
```

Figura 73. Configuración de usuario en R3.

Configuración D1

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#username admin privilege 15 algorithm-type scrypt secret
cisco12345$
D1(config)#exit
D1#
```

Figura 74. Configuración de usuario en D1.

Configuración D2

```
D2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#username admin privilege 15 algorithm-type scrypt secret
cisco12345$
D2(config)#exit
D2#
```

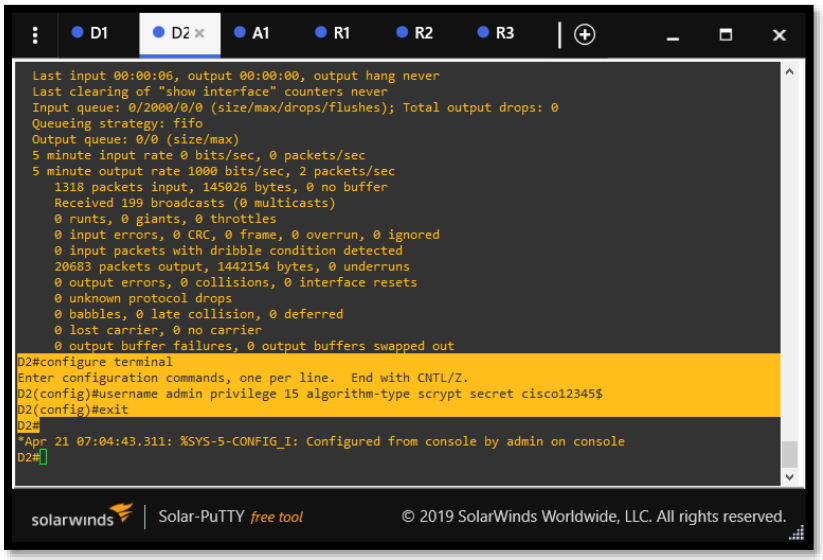

Figura 75. Configuración de usuario en D2.

Configuración A1

```
A1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#username admin privilege 15 algorithm-type scrypt secret
cisco12345$
A1(config)#exit
A1#
```

Figura 76. Configuración de usuario en A1.

4.3. Parte 4 paso 3. En todos los dispositivos, habilite AAA y habilite la autenticación AAA.

Se habilita la autenticación AAA mediante los comandos aaa new-model - aaa authentication login default local. Mediante este protocolo de autenticación, permitirá que solo los usuarios que tengan administración sobre los equipos tengan acceso a los mismos.

Configuración R1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#exit
R1#
```

Figura 77. Se habilita autenticación AAA en R1.

Configuración R2

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#aaa new-model
R2(config)#aaa authentication login default local
R2(config)#exit
R2#
```

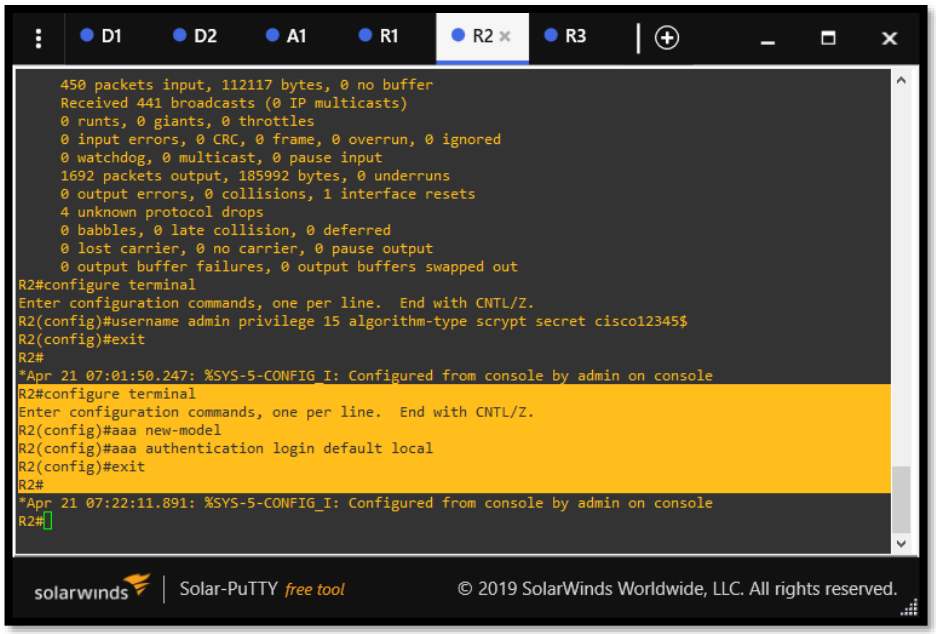

Figura 78. Se habilita autenticación AAA en R2.

Configuración R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#aaa new-model
R3(config)#aaa authentication login default local
R3(config)#exit
R3#
```

Figura 79. Se habilita autenticación AAA en R3.

Configuración D1

```
D1(config)#aaa new-model
D1(config)#aaa authentication login default local
D1(config)#exit
D1#
```

Figura 80. Se habilita autenticación AAA en D1.

Configuración D2

```
D2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#aaa new-model
D2(config)#aaa authentication login default local
D2(config)#exit
D2#
```

Figura 81. Se habilita autenticación AAA en D2.

Configuración A1

```
A1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#aaa new-model
A1(config)#aaa authentication login default local
A1(config)#exit
A1#
```

Figura 82. Se habilita autenticación AAA en A1.

Se verifica configuración de seguridad.

Se realiza la verificación de la configuración de seguridad aplicada mediante el comando **`show run | include aaa|username`**

De tal forma que constatar que los dispositivos tomaron la configuración de seguridad, por lo cual al ingresar requiriera usuario y clave de acceso, permitiendo solo ingreso a personal autorizado.

Figura 83. configuración de seguridad en R1

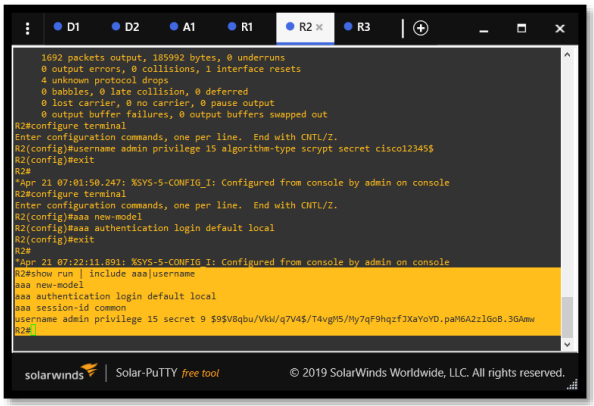

Figura 84. configuración de seguridad en R2

Figura 85. configuración de seguridad en R3

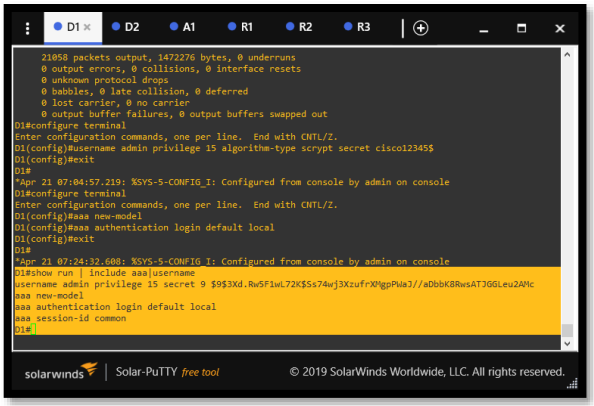

Figura 86. configuración de seguridad en D1

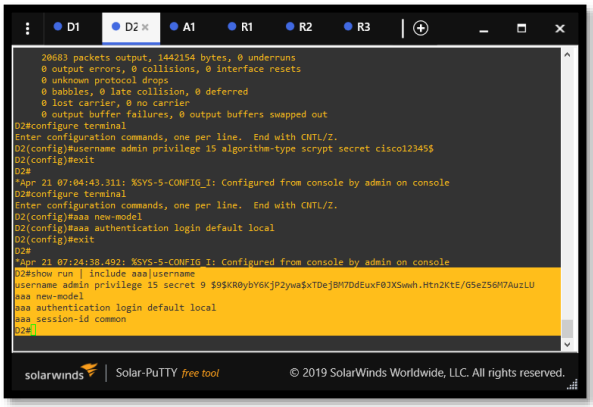

Figura 87. configuración de seguridad en D2

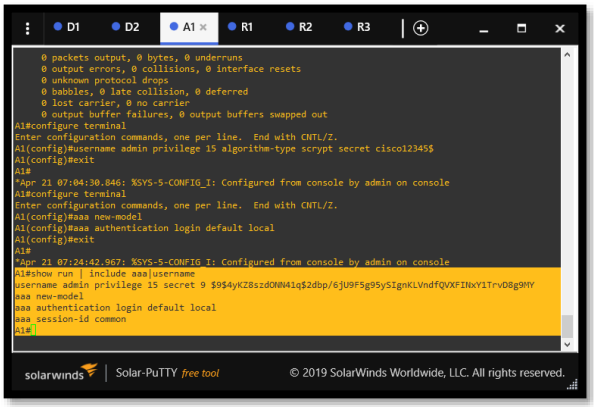

Figura 88. configuración de seguridad en A1

En esta parte podemos evidenciar que los dispositivos tomaron la configuración de seguridad, por lo cual al ingresar requiriera usuario y clave de acceso, permitiendo solo ingreso a personal autorizado.

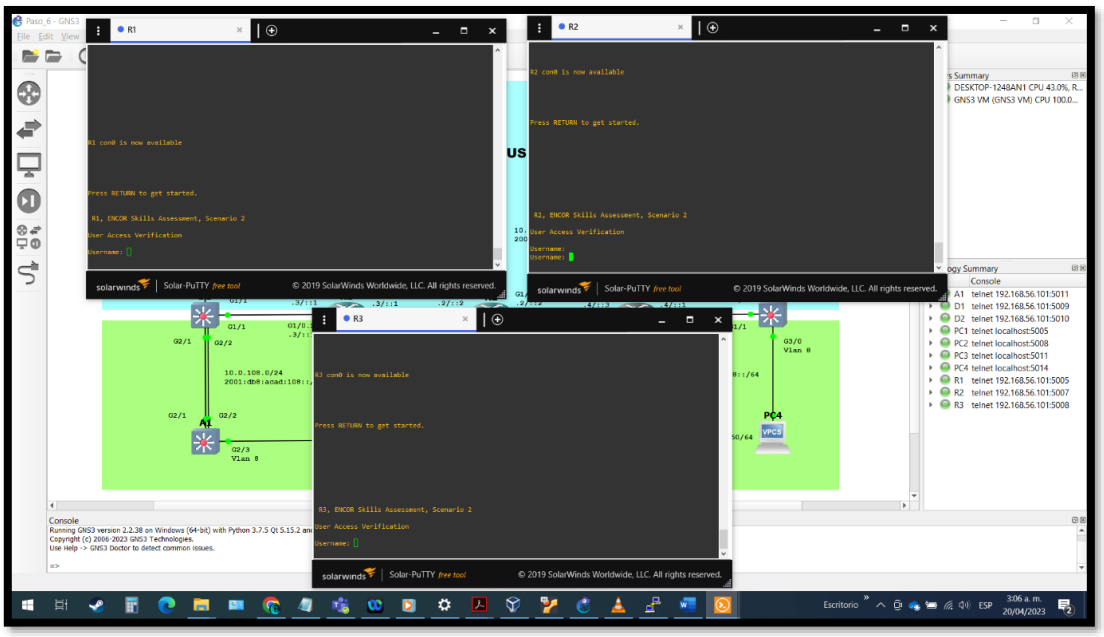

Figura 89. Prueba de seguridad en los dispositivos R1, R2 y R3.

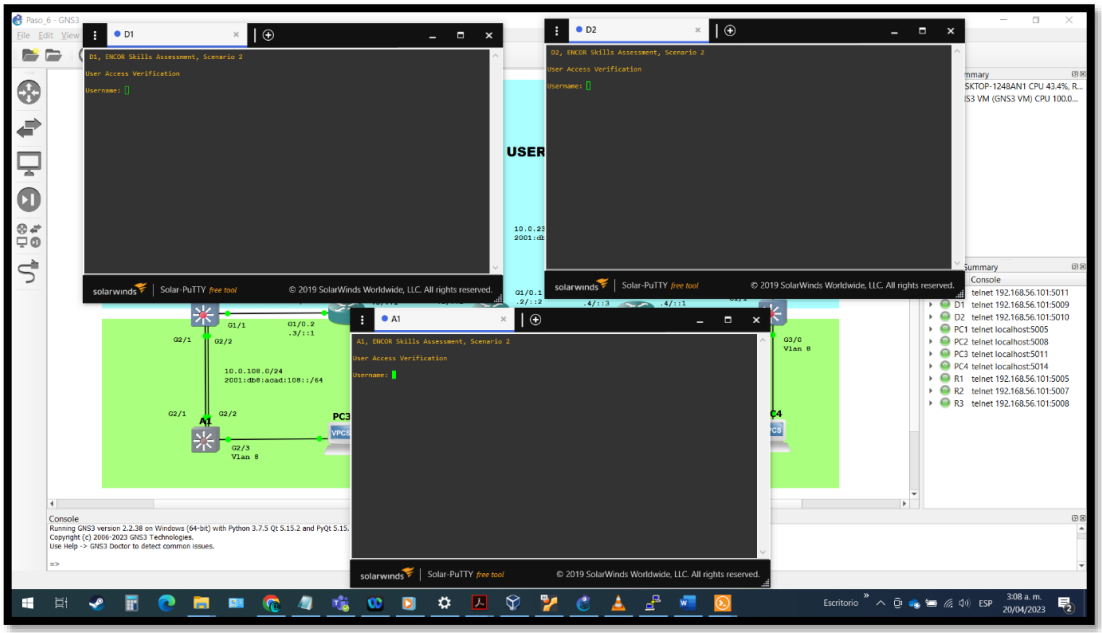

Figura 90. Prueba de seguridad en los dispositivos D1, D2 y A1.

CONCLUSIONES

En el desarrollo de esta práctica podemos que las VRF, que significa enrutamiento y reenvío virtuales, es una tecnología que permite que varias instancias de una tabla de enrutamiento coexistan dentro del mismo enrutador o conmutador de capa 3. El objetivo principal de VRF es crear una instancia de enrutamiento separada para diferentes clientes o aplicaciones, de modo que puedan operar de forma independiente sin interferir entre sí. En esencia, VRF permite a los administradores de red crear múltiples enrutadores virtuales en un solo dispositivo físico, y cada enrutador virtual funciona como si fuera un enrutador físico distinto con su propia tabla de enrutamiento, interfaces y políticas de reenvío.

Esta tecnología es particularmente útil en entornos de proveedores de servicios donde múltiples clientes necesitan compartir la misma infraestructura de red mientras mantienen un aislamiento y seguridad completos entre sus flujos de tráfico. Los VRF se implementan en una variedad de dispositivos de red, incluidos enrutadores, conmutadores y firewalls. Son ampliamente utilizados en redes empresariales, centros de datos y redes de proveedores de servicios. Mediante el uso de VRF, los administradores de red pueden lograr ahorros de costos significativos al reducir la cantidad de dispositivos físicos necesarios mientras mantienen el mismo nivel de segmentación y seguridad de la red.

Los enrutadores de Cisco son conocidos por su alta calidad y confiabilidad, lo que los convierte en una muy buena opción para muchas organizaciones. Estos enrutadores y productos de enrutamiento pueden transformar su red y brindar un servicio confiable y de alta seguridad a las redes de campus, centros de datos y sucursales.

BIBLIOGRAFÍA

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

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

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

Cibergrafía
Vaca, Pablo Andrés. (10 abr 2022). *instalación configuración GNS3 VM. (*Video YouTube)
https://www.youtube.com/watch?v=A6RRo6ioFFQ

Cibergrafía
Vaca, Pablo Andrés. (10 abr 2022). *Agregar dispositivos a GNS3*. *(*Video YouTube)
https://www.youtube.com/watch?v=2JvRu9v-Xlo