

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBAS DE HABILIDADES PRACTICAS CCNP

HUGO MAURICIO MERA YARPAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES

PASTO

2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBAS DE HABILIDADES PRACTICAS CCNP

HUGO MAURICIO MERA YARPAZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO
DE INGENIERÍA DE TELECOMUNICACIONES

TUTOR

ING. MARITZA MONDRAGÓN GUZMÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES

PASTO

2023

NOTA DE ACEPTACIÓN:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

PASTO, (mayo 14, 2023)

AGRADECIMIENTO

Un agradecimiento especial a mi familia, que me brindó su apoyo incondicional durante mi formación profesional como ingeniero de electrónico. Así mismo, agradezco a todos mis compañeros que a pesar de que pasamos duros momentos por cuestiones laborales se notó la entrega, compromiso y apoyo oportuno de cada uno de nosotros para el cumplimiento de las actividades durante el curso. Estoy muy agradecido al personal de la Universidad UNAD por brindarme pacientemente todos estos años de esfuerzo, sacrificios, dedicación y su apoyo con herramientas necesarias para que pueda capacitarme para convertirme en un ingeniero electrónico con capacidades y valores al servicio de la sociedad. Y agradecer a mi esposa, hija e hijo por brindarme su apoyo y dejarme cumplir con este objetivo donde me comprometí a cumplir con todos los requisitos académicos al inicio de este proyecto académico.

CONTENIDO

AGRADECIMIENTO	4
INDICE DE TABLAS	7
INDICE DE FIGURAS	8
GLOSARIO	9
RESUMEN	10
ABSTRACT	11
INTRODUCCION	12
ESCENARIO PROPUESTO	13
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz	15
Paso 1: Cablee la red como se muestra en la topología.....	15
Paso 2: Configure los ajustes básicos para cada dispositivo.....	16
Parte 2: configurar VRF y enrutamiento estático	25
2.1 En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.	26
2.2 Configuración de las interfaces IPv4 y IPv6 en R1, R2 y R3 para cada VRF como esta detallada en la tabla 1 de direccionamiento.	28
2.3 Configuración de las rutas estáticas predeterminadas que apuntan a R2, en R1 y R3.	35
2.4 Verificación de la conectividad en cada VRF.	37
Parte 3. Configurar Capa 2	39
3.1 Desactivar las interfaces en los switches D1, D2 y A1.	40
3.2 Configurar los enlaces troncales a R1 y R3 en D1 y D2.	41

3.3 Configurar el EtherChannel en D1 y A1	42
3.4 Configurar puertos de acceso para PC1, PC2, PC3 y PC4 en D1, D2 y A1. ...	43
3.5 Verificación de la conectividad de PC a PC.....	47
Parte 4. Configurar seguridad	49
4.1 En todos los dispositivos, configurar modo EXEC privilegiado.	49
4.2 Crear una cuenta de usuario local en todos los dispositivos.....	51
4.3 Habilite la autenticación AAA en todos los dispositivos.	52
CONCLUSIONES	55
BIBLIOGRAFIA	56

INDICE DE TABLAS

Tabla 1 Tabla de direccionamiento	14
Tabla 2 Código implementado para la configuración con la respectiva descripción	25
Tabla 3 Tareas de configuración.....	39
Tabla 4 tareas de configuración.....	49

INDICE DE FIGURAS

Figura 1 Topología de red escenario 1	13
Figura 2 Topología realizada en Gsn3.....	15
Figura 3 Configuración PC1.....	23
Figura 4 Configuración PC2.....	23
Figura 5 Configuración PC3.....	24
Figura 6 Configuración PC4.....	24
Figura 7 Verificación de las subinterfaces en R1	34
Figura 8 Verificación de las subinterfaces en R2	34
Figura 9 Verificación de las subinterfaces en R3.....	34
Figura 10 Verificación de rutas configuradas en R1	36
Figura 11 Verificación de rutas configuradas en R2	37
Figura 12 Verificación de rutas configuradas en R3	37
Figura 13 ping interfaces vrf Genera-Special – IPV4-IPV6	38
Figura 14 Verificación de Comandos en Switch D1	45
Figura 15 Verificación de Comandos en Switch D2	46
Figura 16 Verificación de Comandos en Switch A1	47
Figura 17 Ping IPv4 e IPv6 desde PC1 a PC2.....	48
Figura 18 Ping IPv4 e IPv6 desde PC3 a PC4.....	48
Figura 19 Nombre de usuario y autenticación AAA en R1	53
Figura 20 Nombre de usuario y autenticación AAA en R2.....	53
Figura 21 Nombre de usuario y autenticación AAA en R3.....	53
Figura 22 Nombre de usuario y autenticación AAA en D1	54
Figura 23 Nombre de usuario y autenticación AAA en D2.....	54
Figura 24 Nombre de usuario y autenticación AAA en A1	54

GLOSARIO

Dirección IP: Una dirección de red se asigna a la interfaz de un nodo de red y se utiliza para identificar (identificar) de forma única un nodo en Internet. Actualmente se están implementando dos versiones: IPv4 e IPv6.

Enrutamiento: se refiere al proceso en el que los enrutadores aprenden sobre redes remotas, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas (las más rápidas) para intercambiar datos entre las mismas.

LAN (Local Área Network): Son redes constituidas por dispositivos como Routers, Switchs, Host, Servidores los cuales se encargan de intercambiar datos y compartir recursos entre los usuarios de la red, estas redes pueden ser empresariales y domésticas

Red: Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

ROUTER: permite interconectar computadoras que funcionan en el marco de una red, se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática.

Switch: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

VRF: Es una tecnología utilizada en redes de computadoras que permite la coexistencia de múltiples instancias las tablas de ruteo de un mismo enrutador

RESUMEN

A continuación, se presenta la prueba de habilidades prácticas, que es la actividad del diplomado CISCO CCNP, que tiene como objetivo que los estudiantes puedan organizar y dominar de manera efectiva los conocimientos y habilidades necesarios para enfrentar situaciones complejas a través de la implementación y la configuración, en el protocolo de enrutamiento y en la conmutación para mejorar el pensamiento crítico y las habilidades de análisis activo en la plataforma de red.

Esto se puede demostrar implementando un protocolo de VLAN para una interfaz de red específica en cada conmutador, como parte básica de la interconexión de computadoras y dispositivos periféricos. Aplicar comandos de configuración a diferentes tipos de dispositivos activos para restaurar el conocimiento previo.

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

ABSTRACT

The following is the practical skills test, which is the CISCO CCNP diploma activity that aims to enable students to effectively organize and master the knowledge and skills needed to deal with complex situations through implementation and configuration, in routing protocol and switching to enhance critical thinking and active analysis skills on the network platform.

This can be demonstrated by implementing a VLAN mapping protocol for a specific network interface on each switch as a basic part of interconnecting computers and peripheral devices. Apply configuration commands to different types of active devices to restore prior knowledge.

Keywords: CISCO, CCNP, Routing, Switching, Networking, Electronics

INTRODUCCION

Con el paso del tiempo, la tecnología se ha convertido en una parte importante de nuestras vidas, ayudándonos a comprender y afrontar todas las incógnitas que se nos presentan, pues sin duda, internet ha cambiado el mundo y su constante desarrollo cambiará radicalmente este mundo.

Con la ayuda de la plataforma Cisco Networking Academy, se ha adquirido el contenido clave para desarrollar un diplomado CCNP. Esto es muy importante porque contribuye mucho al crecimiento laboral, lo que mejorará nuestro desempeño profesional al participar en el mundo online.

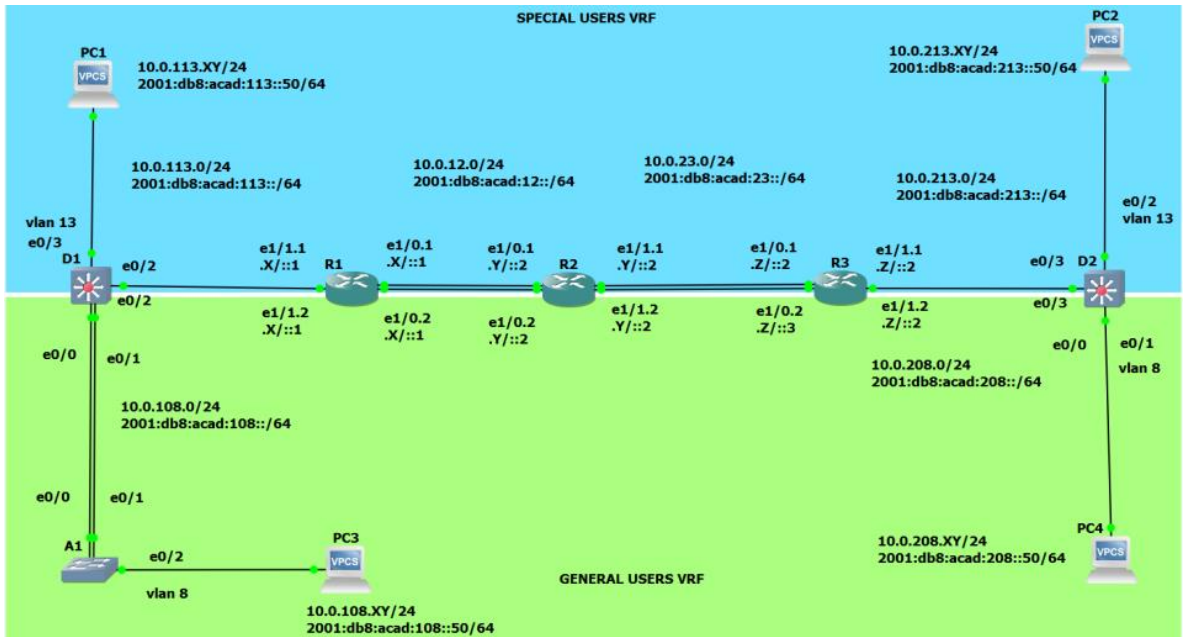
En el siguiente documento se presenta el desarrollo de un escenario propuesto como prueba de habilidades practica de CCNP, el cual abarcara de manera amplia las temáticas apropiadas durante la realización del diplomado.

Para el desarrollo del escenario se utilizará el software de simulación GNS3 para el diseño de topología y configuración de cada dispositivo, y el protocolo se configurará en el enrutador.

ESCENARIO PROPUESTO

Topología de la Red:

Figura 1 Topología de red escenario 1



Fuente: tomado de Prueba de habilidades Ccnp 2023, Cisco Academy

Tabla 1 Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 link-local
R1	E1/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.6/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.6/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.6/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.6/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.16/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.16/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.16/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.16/24	2001:db8:acad:208::50/64	EUI-64

Fuente: propia

Objetivos

Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

Parte 2: Configurar VRF y rutas estáticas.

Parte 3: Configurar Capa 2 (se entrega finalizado el paso 6)

Parte 4: Configurar seguridad

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.

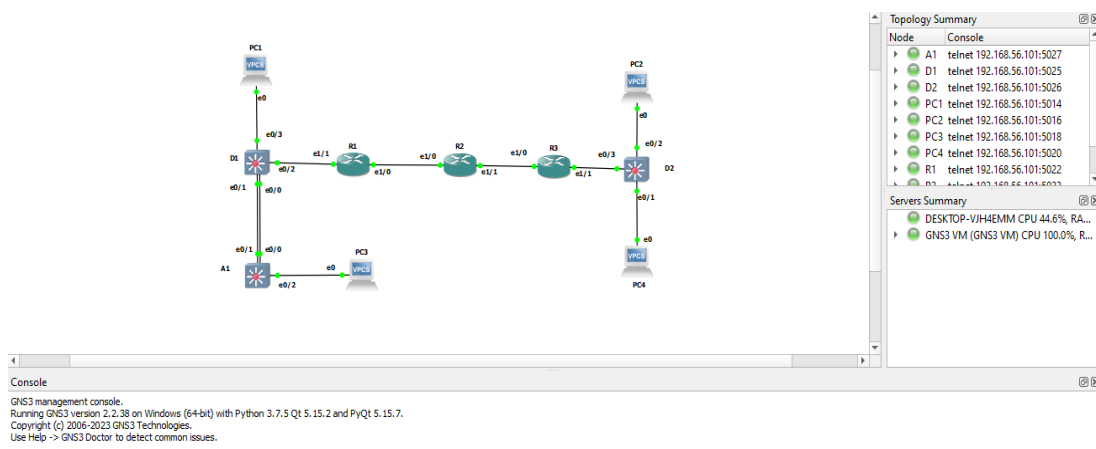
Instrucciones

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

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 Topología realizada en Gsn3



Fuente: propia

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.

Router R1

```
Hostname R1 ## Asigna el nombre del router R1
ipv6 unicast-routing ## Habilitamos IPV6 en el dispositivo.
no ip domain lookup ## Desactivamos la traducción de nombres
banner motd # R1, ENCOR Skills Assessment, Scenario 2 # ## mensaje de
advertencia

line con 0 ## Ingresa en configuración de la consola
exec-timeout 0 0 ## Se establece un tiempo de espera para salir de la
sesión
logging synchronous ## Se deniegan mensajes inesperados o de alertas en
pantalla

exit ## sale de configuración de la consola
```

Router R2

```
hostname R2 ## Asigna el nombre del router R2
ipv6 unicast-routing ## Habilitamos IPV6 en el dispositivo
no ip domain lookup ## Desactivamos la traducción de nombres
banner motd # R2, ENCOR Skills Assessment, Scenario 2 # ## mensaje de
advertencia

line con 0 ## Ingresa en configuración de la consola
```

exec-timeout 0 0 ## Se establece un tiempo de espera para salir de la sesión

logging synchronous ## Se deniegan mensajes inesperados o de alertas en pantalla

exit ## sale de configuración de la consola

Router R3

hostname R3 ## Asigna el nombre del router R3

ipv6 unicast-routing ## Habilitamos IPV6 en el dispositivo

no ip domain lookup ## Desactivamos la traducción de nombres

banner motd # R3, ENCOR Skills Assessment, Scenario 2 # ## mensaje de advertencia

line con 0 ## Ingresamos en configuración de la consola

exec-timeout 0 0 ## Se establece un tiempo de espera para salir de la sesión

logging synchronous ## Se deniegan mensajes inesperados o de alertas en pantalla

exit ## sale de configuración de la consola

Switch D1

hostname D1 ## Asigna el nombre del switch D1

ip routing ## habilita el protocolo de enrutamiento

ipv6 unicast-routing ## Habilitamos IPV6 en el dispositivo

no ip domain lookup ## Desactivamos la traducción de nombres

banner motd # D1, ENCOR Skills Assessment, Scenario 2 # ## mensaje de advertencia

line con 0 ## Ingresa en configuración de la consola

exec-timeout 0 0 ## Se establece un tiempo de espera para salir de la session

logging synchronous ## Se deniegan mensajes inesperados o de alertas en pantalla

exit ## sale de configuración de la consola

vlan 8 ## Se crea la VLAN

name General-Users ## Asignacion de nombre

exit ## sale de configuración de la consola

vlan 13 ## Se crea la VLAN

name Special-Users ## Asignacion de nombre

exit ## sale de configuración de la consola

Switch D2

hostname D2 ## Asigna el nombre del switch D2

ip routing ## habilita el protocolo de enrutamiento

ipv6 unicast-routing ## Habilitamos IPV6 en el dispositivo

no ip domain lookup ## Desactivamos la traducción de nombres

banner motd # D2, ENCOR Skills Assessment, Scenario 2 # ## mensaje de advertencia

line con 0 ## Ingresa en configuración de la consola

exec-timeout 0 0 ## Se establece un tiempo de espera para salir de la session

logging synchronous ## Se deniegan mensajes inesperados o de alertas en pantalla

exit ## sale de configuración de la consola

vlan 8 ## Se crea la VLAN

name General-Users ## Asignacion de nombre

exit ## sale de configuración de la consola

vlan 13 ## Se crea la VLAN

name Special-Users ## Asignacion de nombre

exit ## sale de configuración de la consola

Switch A1

hostname A1 ## Asigna el nombre del switch A1

ipv6 unicast-routing ## Habilitamos IPV6 en el dispositivo

no ip domain lookup ## Desactivamos la traducción de nombres

banner motd # A1, ENCOR Skills Assessment, Scenario 2 # ## mensaje de advertencia

line con 0 ## Ingresa en configuración de la consola

exec-timeout 0 0 ## Se establece un tiempo de espera para salir de la session

logging synchronous ## Se deniegan mensajes inesperados o de alertas en pantalla

```
exit ## sale de configuración de la consola  
vlan 8 ## Se crea la VLAN  
name General-Users ## Asignacion de nombre  
exit ## sale de configuración de la consola
```

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

Una vez ingresadas cada una de las instrucciones sugeridas por la guía para la configuración inicial se procede a escribir el siguiente comando:

Router R1

```
R1#copy running-config startup-config  
Destination filename [startup-config]?  
Warning: Attempting to overwrite an NVRAM configuration previously written  
by a different version of the system image.  
Overwrite the previous NVRAM configuration?[confirm]  
Building configuration...  
[OK]  
R1#
```

Router R2

```
R2#copy running-config startup-config  
Destination filename [startup-config]?  
Warning: Attempting to overwrite an NVRAM configuration previously written
```

by a different version of the system image.

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

[OK]

R2#

Router R3

R3#copy running-config startup-config

Destination filename [startup-config]?

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

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

[OK]

R3#

Switch D1

D1# copy running-config startup-config

Destination filename [startup-config]?

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

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

Compressed configuration from 1433 bytes to 873 bytes[OK]

D1#

Switch D2

D2#copy running-config startup-config

Destination filename [startup-config]?

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

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

Compressed configuration from 1433 bytes to 876 bytes[OK]

D2#

Switch A1

A1#copy running-config startup-config

Destination filename [startup-config]?

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

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

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

La configuración de los host finales de la red se realiza de manera muy sencilla, simplemente ingresando las direcciones IP y al final mediante el comando “save”, se guarda la información ingresada en cada host.

PC1

```
ip 10.0.113.16/24 10.0.113.1    ##asignacion de ip y mascara de subred
ip 2001:db8:acad:113::50/64 auto ##Asignacion de ipv6
save ## Guardar configuracion
```

Figura 3 Configuración PC1

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC1	10.0.113.16/24	10.0.113.1	00:50:79:66:68:00	10004	127.0.0.1:10005
	fe80::250:79ff:fe66:6800/64				
	2001:db8:acad:113::50/64				

PC1> █

Fuente: propia

PC2

```
ip 10.0.213.16/24 10.0.213.1 ##asignacion de ip y mascara de subred
ip 2001:db8:acad:213::50/64 auto ##Asignacion de ipv6
save ## Guardar configuración
```

Figura 4 Configuración PC2

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC2	10.0.213.16/24	10.0.213.1	00:50:79:66:68:01	10002	127.0.0.1:10003
	fe80::250:79ff:fe66:6801/64				
	2001:db8:acad:213::50/64				

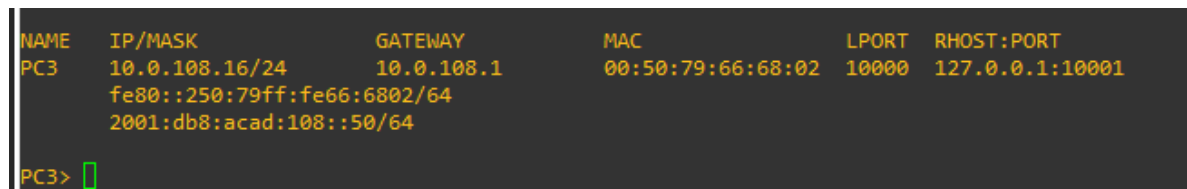
PC2> █

Fuente: propia

PC3

```
ip 10.0.108.16/24 10.0.108.1 ##asignacion de ip y mascara de subred  
ip 2001:db8:acad:108::50/64 auto ##Asignacion de ipv6  
save ## Guardar configuración
```

Figura 5 Configuración PC3

A screenshot of a network configuration table for PC3. The table has six columns: NAME, IP/MASK, GATEWAY, MAC, LPORT, and RHOST:PORT. The data row shows PC3 with IP/MASK 10.0.108.16/24, GATEWAY 10.0.108.1, MAC 00:50:79:66:68:02, LPORT 10000, and RHOST:PORT 127.0.0.1:10001. Below the table, the IPv6 address 2001:db8:acad:108::50/64 is listed. The prompt PC3> is visible at the bottom left.

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC3	10.0.108.16/24	10.0.108.1	00:50:79:66:68:02	10000	127.0.0.1:10001

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

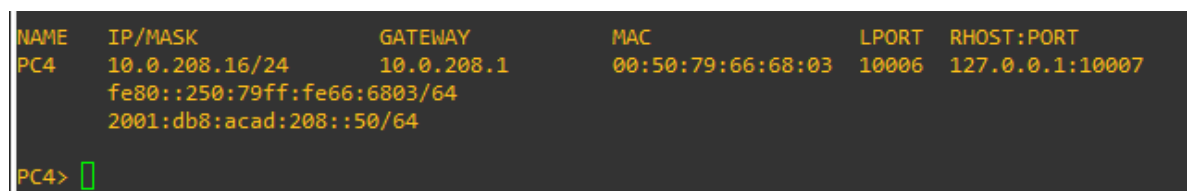
PC3>

Fuente: propia

PC4

```
ip 10.0.208.16/24 10.0.208.1 ##asignacion de ip y mascara de subred  
ip 2001:db8:acad:208::50/64 auto ##Asignacion de ipv6  
save ## Guardar configuración
```

Figura 6 Configuración PC4

A screenshot of a network configuration table for PC4. The table has six columns: NAME, IP/MASK, GATEWAY, MAC, LPORT, and RHOST:PORT. The data row shows PC4 with IP/MASK 10.0.208.16/24, GATEWAY 10.0.208.1, MAC 00:50:79:66:68:03, LPORT 10006, and RHOST:PORT 127.0.0.1:10007. Below the table, the IPv6 address 2001:db8:acad:208::50/64 is listed. The prompt PC4> is visible at the bottom left.

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC4	10.0.208.16/24	10.0.208.1	00:50:79:66:68:03	10006	127.0.0.1:10007

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

PC4>

Fuente: 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.

Sus tareas de configuración son las siguientes:

Tabla 2 Código implementado para la configuración con la respectiva descripción

Task#	Task	Specification
2.1	On R1, R2, and R3, configure VRF-Lite VRFs as shown in the topology diagram	Configure two VRFs: <ul style="list-style-type: none">• 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 G0/0/1.x interfaces to support separation of the VRFs. Sub-interface 1: <ul style="list-style-type: none">• In the Special Users VRF• Use dot1q encapsulation 13• IPv4 and IPv6 GUA and link-local addresses• Enable the interfaces Sub-interface 2: <ul style="list-style-type: none">• In the General Users VRF• Use dot1q encapsulation 8• 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: <ul style="list-style-type: none"> • ping vrf General-Users 10.0.208.1 • ping vrf General-Users 2001:db8:acad:208::1 • ping vrf Special-Users 10.0.213.1 • ping vrf Special-Users 2001:db8:acad:213::1

Fuente: propia

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

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

R1

configuración VRF-Router 1

Configuración de las subinterfaces VRF

config term ## entramos a la configuración global

vrf definition Special-User ## definimos nombre del VRF virtual vlan 13

address-family ipv4 ## agregamos la familia del protocolo ipv4

address-family ipv6 ## agregamos la familia del protocolo ipv6

```
exit ## salida de la configuración  
vrf definition General-User ## definimos nombre del VRF virtual vlan 8  
address-family ipv4 ## agregamos la familia del protocolo ipv4  
address-family ipv6 ## agregamos la familia del protocolo ipv6  
exit ## salida del modo interface
```

R2

configuración VRF-Router 2

```
config term ## entramos a la configuración global  
vrf definition Special-User ## definimos nombre del VRF virtual vlan 13  
address-family ipv4 ## agregamos la familia del protocolo ipv4  
address-family ipv6 ## agregamos la familia del protocolo ipv6  
exit ## salida de configuración  
vrf definition General-User ## definimos nombre VRF virtual vlan 8  
address-family ipv4 ## agregamos familia del protocolo ipv4  
address-family ipv6 ## agregamos familia del protocolo ipv6  
exit ## salida del modo interface  
Configuración VRF para General – Special
```

R3

configuración VRF-Router 1

```
config term ## ingresamos a la configuración global
```

```
vrf definition Special-User ## definimos nombre del VRF virtual
address-family ipv4 ## agregamos la familia del protocolo ipv4
address-family ipv6 ## agregamos la familia del protocolo ipv6
exit ## salida de la configuración
```

```
vrf definition General-User ## definimos nombre del VRF virtual
address-family ipv4 ## agregamos la familia del protocolo ipv4
address-family ipv6 ## agregamos la familia del protocolo ipv6
exit ## salida de la configuración
```

2.2 Configuración de las interfaces IPv4 y IPv6 en R1, R2 y R3 para cada VRF como esta detallada en la tabla 1 de direccionamiento.

Configuración Router R1

```
Config term ## ingresamos al modo configuración global
interface g1/0 ## ingresamos a la interface del Router 1 g1/0
no shutdown ## habilitamos la interface g1/0
interface g1/0.1 ## ingresamos a las subinterfaces
encapsulation dot1Q 13 ## protocolo permite un enlace troncal Vlan 13
vrf forwarding Special-User ## agregamos el VRF configurado
ip address 10.0.12.1 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:12::1/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::1:1 link-local ## agregamos su link local
```

```
no shutdown ## habilitamos la interface

exit ## salida del modo interface

interface g1/0.2 ## ingresamos a las subinterfaces

encapsulation dot1Q 8 ## protocolo permite un enlace troncal Vlan 8

vrf forwarding General-User ## agregamos el VRF configurado

ip address 10.0.12.1 255.255.255.0 ## agregamos su ip y mascara ipv4

ipv6 address 2001:db8:acad:12::1/64 ## agregamos su ip y mascara ipv6

ipv6 address fe80::1:2 link-local ## agregamos su link local

no shutdown ## habilitamos la interface

exit ## salida del modo interface
```

```
interface g2/0.1 ## ingresamos a las subinterfaces

encapsulation dot1Q 13 ## protocolo permite un enlace troncal Vlan 13

vrf forwarding Special-User ## agregamos el VRF configurado

ip address 10.0.113.1 255.255.255.0 ## agregamos su ip y mascara ipv4

ipv6 address 2001:db8:acad:108::1/64 ## agregamos su ip y mascara ipv6

ipv6 address fe80::1:3 link-local ## agregamos su link local.

no shutdown ## habilitamos la interface

exit ## salida de la configuración
```

```
interface g2/0.2 ## ingresamos a las subinterfaces

encapsulation dot1Q 8 ## protocolo permite un enlace troncal Vlan 8

vrf forwarding General-User ## agregamos el VRF configurado
```

```
ip address 10.0.108.1 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:108::1/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::1:4 link-local ## agregamos su link local
no shutdown ## habilitamos la interface

exit ## salida del modo interface

wr ## guardamos configuración
```

Configuración Router R2

```
Config term ## ingresamos al modo configuración global
interface g1/0 ## ingresamos a la interface del Router 2 g1/0
no shutdown ## habilitamos la interface g1/0
interface g1/0.1 ## ingresamos a las subinterfaces
encapsulation dot1Q 13 ## protocolo permite un enlace troncal Vlan 13
vrf forwarding Special-User ## agregamos el VRF configurado
ip address 10.0.12.6 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:12::2/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::2:1 link-local ## agregamos su link local
no shutdown ## habilitamos la interface
exit ## salida del modo interface

interface g1/0.2 ## ingresamos a las subinterfaces
encapsulation dot1Q 8 ## protocolo permite un enlace troncal Vlan 8
vrf forwarding General-User ## agregamos el VRF configurado
```

```
ip address 10.0.12.6 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:12::2/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::2:2 link-local ## agregamos su link local
no shutdown ## habilitamos la interface

exit ## salida del modo interface

interface g2/0.1 ## ingresamos a las subinterfaces

encapsulation dot1Q 13 ## protocolo permite un enlace troncal Vlan 13
vrf forwarding Special-User ## agregamos el VRF configurado
ip address 10.0.23.6 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:23::2/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::2:3 link-local ## agregamos su link local
no shutdown ## habilitamos la interface

exit ## salida de la configuración

interface g2/0.2 ## ingresamos a las subinterfaces

encapsulation dot1Q 8 ## protocolo permite un enlace troncal Vlan 8
vrf forwarding General-User ## agregamos el VRF configurado
ip address 10.0.23.6 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:23::2/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::2:4 link-local ## agregamos su link local
no shutdown ## habilitamos la interface

exit ## salida del modo interface
```

wr ## guardamos configuración

Configuración Router R3

Config term ## ingresamos al modo configuración global

interface g1/0 ## ingresamos a la interface física del Router 3 g1/0

no shutdown ## habilitamos la interface

interface g1/0.1 ## ingresamos a las subinterfaces virtual

encapsulation dot1Q 13 ## protocolo permite un enlace troncal Vlan 13

vrf forwarding Special-User ## agregamos el VRF configurado

ip address 10.0.23.1 255.255.255.0 ## agregamos su ip y mascara ipv4

ipv6 address 2001:db8:acad:23::3/64 ## agregamos su ip y mascara ipv6

ipv6 address fe80::3:1 link-local ## agregamos su link local

no shutdown ## habilitamos la subinterfaz virtual

exit ## salida del modo interface

interface g1/0.2 ## ingresamos a las subinterfaces virtual

encapsulation dot1Q 8 ## protocolo que permite un enlace troncal vlan8

vrf forwarding General-User ## agregamos el VRF configurado

ip address 10.0.23.1 255.255.255.0 ## agregamos su ip y mascara ipv4

ipv6 address 2001:db8:acad:23::3/64 ## agregamos su ip y mascara ipv6

ipv6 address fe80::3:2 link-local ## agregamos su link local

no shutdown ## habilitamos la subinterfaz virtual

exit ## salida del modo interface

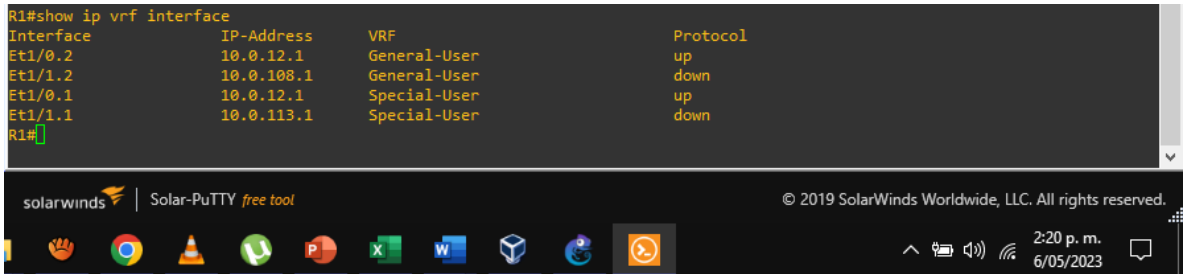
```
interface g2/0 ## ingresamos a la interface física del Router 3 g2/0
no shutdown ## habilitamos la interface

interface g2/0.1 ## ingresamos a las subinterfaces virtual
encapsulation dot1Q 13 ## protocolo que permite un enlace troncal vlan 13
vrf forwarding Special-User ## agregamos el VRF configurado
ip address 10.0.213.1 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:208::1/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::3:3 link-local ## agregamos su link local
no shutdown ## habilitamos la subinterfaz virtual
exit ## salida del modo interface
```

```
interface g2/0.2 ## ingresamos a las subinterfaces virtual
encapsulation dot1Q 8 ## protocolo que permite un enlace troncal vlan13
vrf forwarding General-User ## agregamos el VRF configurado
ip address 10.0.208.1 255.255.255.0 ## agregamos su ip y mascara ipv4
ipv6 address 2001:db8:acad:208::1/64 ## agregamos su ip y mascara ipv6
ipv6 address fe80::3:4 link-local ## agregamos su link local
no shutdown ## habilitamos la interface virtual
exit ## salida del modo interface
```

Figura 7 Verificación de las subinterfaces en R1

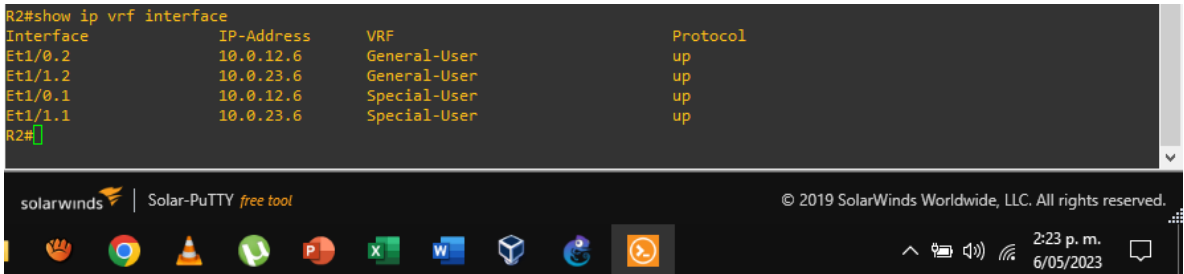
```
R1#show ip vrf interface
Interface      IP-Address    VRF           Protocol
Et1/0.2       10.0.12.1    General-User  up
Et1/1.2       10.0.108.1   General-User  down
Et1/0.1       10.0.12.1    Special-User  up
Et1/1.1       10.0.113.1   Special-User  down
R1#
```



Fuente: propia

Figura 8 Verificación de las subinterfaces en R2

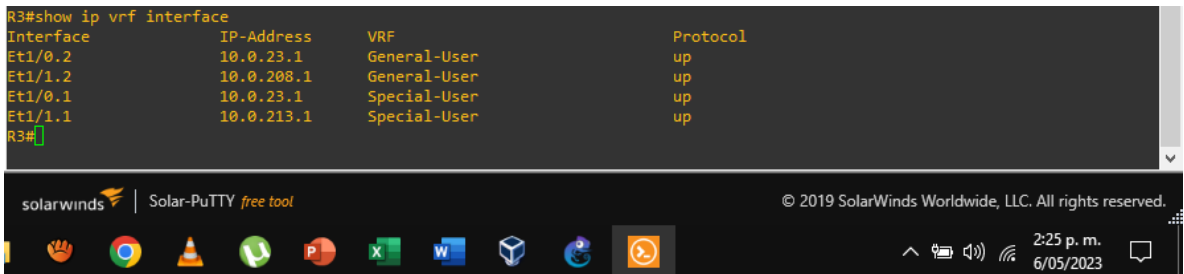
```
R2#show ip vrf interface
Interface      IP-Address    VRF           Protocol
Et1/0.2       10.0.12.6    General-User  up
Et1/1.2       10.0.23.6    General-User  up
Et1/0.1       10.0.12.6    Special-User  up
Et1/1.1       10.0.23.6    Special-User  up
R2#
```



Fuente: propia

Figura 9 Verificación de las subinterfaces en R3

```
R3#show ip vrf interface
Interface      IP-Address    VRF           Protocol
Et1/0.2       10.0.23.1    General-User  up
Et1/1.2       10.0.208.1   General-User  up
Et1/0.1       10.0.23.1    Special-User  up
Et1/1.1       10.0.213.1   Special-User  up
R3#
```



Fuente: propia

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

Configuración rutas estáticas para Router 1 protocolo ipv4 y ipv6

Configuración Router R1

Protocolo ipv4

```
ip route 0.0.0.0 0.0.0.0 10.0.12.6 ## rutas estáticas para llegar a R3
```

```
ip route vrf General-User 0.0.0.0 0.0.0.0 10.0.12.6 ## ruta ipv4
```

```
ip route vrf Special-User 0.0.0.0 0.0.0.0 10.0.12.6 ## ruta ipv4
```

protocolos ipv6

```
ipv6 route vrf General-User::/0 2001:DB8:ACAD:12::2 ## rutas ipv6
```

```
ipv6 route vrf Special-User::/0 2001:DB8:ACAD:12::2 ## rutas
```

Configuración rutas estáticas Router 2 protocolo ipv4 y ipv6

Configuración Router R2

protocolos ipv4

```
ip route vrf General-User 10.0.108.0 255.255.255.0 10.0.12.1
```

```
ip route vrf General-User 10.0.208.0 255.255.255.0 10.0.23.1
```

```
ip route vrf Special-User 10.0.113.0 255.255.255.0 10.0.12.1
```

```
ip route vrf Special-User 10.0.213.0 255.255.255.0 10.0.23.1
```

protocolos ipv6

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

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

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

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

Configuración Router R3

Protocolo ipv4

```
ip route vrf General-User 0.0.0.0 0.0.0.0 10.0.23.6 ## ruta ipv4
```

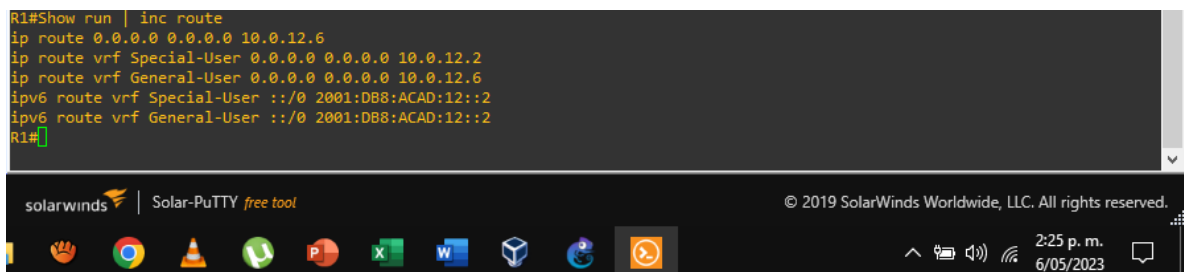
```
ip route vrf Special-User 0.0.0.0 0.0.0.0 10.0.23.6 ## ruta ipv4
```

protocolo ipv6

```
ipv6 route vrf General-User ::/0 2001:DB8:ACAD:23::2 ## ruta ipv6
```

```
ipv6 route vrf Special-User ::/0 2001:DB8:ACAD:23::2 ## ruta ipv6
```

Figura 10 Verificación de rutas configuradas en R1

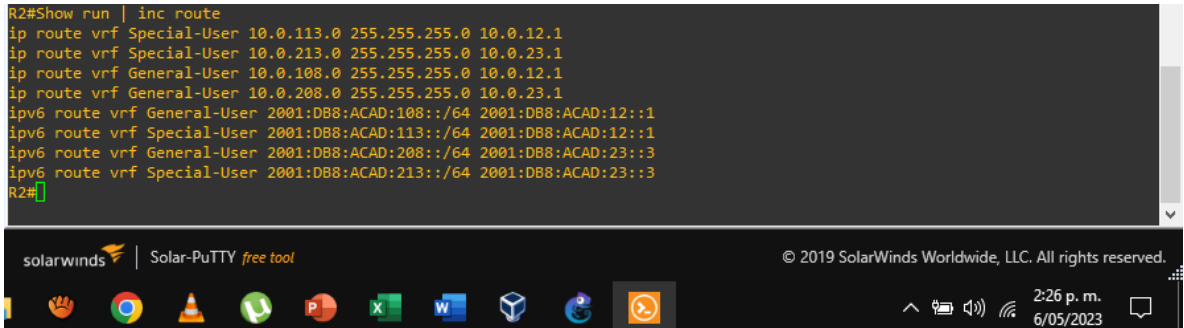


```
R1#Show run | inc route
ip route 0.0.0.0 0.0.0.0 10.0.12.6
ip route vrf Special-User 0.0.0.0 0.0.0.0 10.0.12.2
ip route vrf General-User 0.0.0.0 0.0.0.0 10.0.12.6
ipv6 route vrf Special-User ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf General-User ::/0 2001:DB8:ACAD:12::2
R1#
```

Fuente: propia

Figura 11 Verificación de rutas configuradas en R2

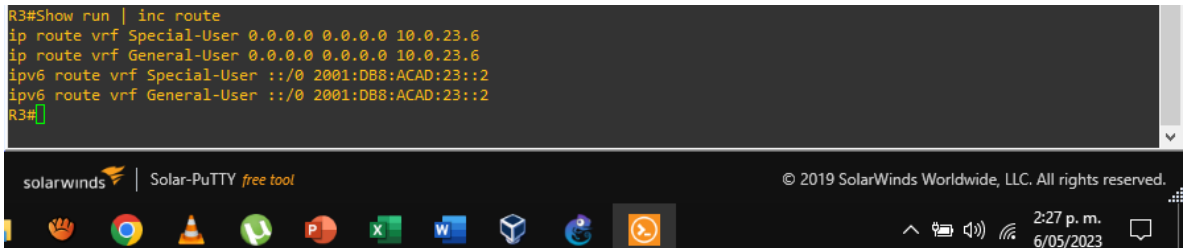
```
R2#Show run | inc route
ip route vrf Special-User 10.0.113.0 255.255.255.0 10.0.12.1
ip route vrf Special-User 10.0.213.0 255.255.255.0 10.0.23.1
ip route vrf General-User 10.0.108.0 255.255.255.0 10.0.12.1
ip route vrf General-User 10.0.208.0 255.255.255.0 10.0.23.1
ipv6 route vrf General-User 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1
ipv6 route vrf Special-User 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1
ipv6 route vrf General-User 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3
ipv6 route vrf Special-User 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3
R2#
```



Fuente: propia

Figura 12 Verificación de rutas configuradas en R3

```
R3#Show run | inc route
ip route vrf Special-User 0.0.0.0 0.0.0.0 10.0.23.6
ip route vrf General-User 0.0.0.0 0.0.0.0 10.0.23.6
ipv6 route vrf Special-User ::/0 2001:DB8:ACAD:23::2
ipv6 route vrf General-User ::/0 2001:DB8:ACAD:23::2
R3#
```



Fuente: propia

2.4 Verificación de la conectividad en cada VRF.

Se realiza la verificación de la conectividad VRF, enviando ping desde R1 a R3.

Ping vrf General-User 10.0.208.1

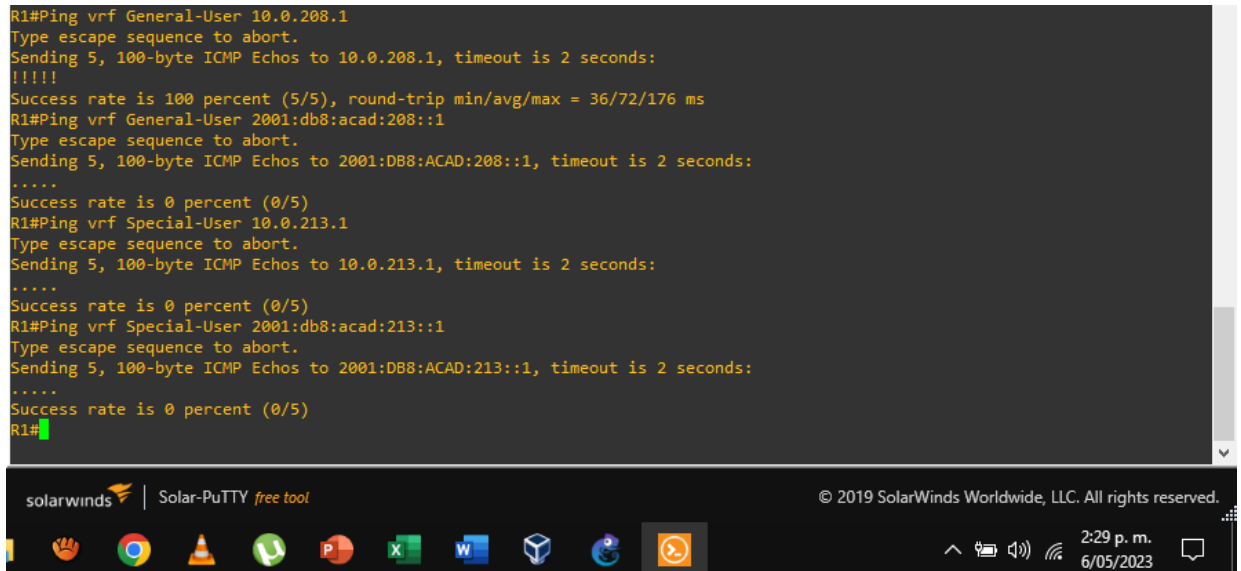
Ping vrf General-User 2001:db8:acad:208::1

Ping vrf Special-User 10.0.213.1

Ping vrf Special-User 2001:db8:acad:213::1

Figura 13 ping interfaces vrf Genera-Special – IPV4-IPV6

```
R1#Ping vrf General-User 10.0.208.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/72/176 ms
R1#Ping vrf General-User 2001:db8:acad:208::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#Ping vrf Special-User 10.0.213.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#Ping vrf Special-User 2001:db8:acad:213::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```



Fuente: 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:

Tabla 3 Tareas de configuración

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: <ul style="list-style-type: none">• Interface G1/0/5 and G1/0/6• Port Channel 1 using PAgP On A1, configure enable: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• On D1, configure interface G1/0/23 as an access port in VLAN 13 and enable Portfast.

		<ul style="list-style-type: none"> • 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.	<p>From PC1, verify IPv4 and IPv6 connectivity to PC2.</p> <p>From PC3, verify IPv4 and IPv6 connectivity to PC4.</p>

Fuente: propia

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

Configuración del Switch D1

Config term ## ingresar al modo configuración global

interface range g0/4-15, rango de interface de 4 a 15

shutdown ## comando para apagar las interfaces seleccionadas

Configuración Switch D2

Config term ## ingresar al modo configuración global

interface range g0/4-15, rango de interface de 4 a 15

shutdown ## comando para apagar las interfaces seleccionadas

Configuración Switch A1

Config term ## ingresar al modo configuración global
interface range g0/4-15, rango de interface de 4 a 15
shutdown ## comando para apagar las interfaces seleccionadas

3.2 Configurar los enlaces troncales a R1 y R3 en D1 y D2.

Configuración Switch D1

Config term ## ingresar al modo configuración global
inter ether 2/0 ## enlace troncal del Router 1
switchport trunk encapsulation dot1Q ## especifica el tipo encapsulación
switchport mode trunk ## habilita modo enlace troncal
switchport trunk allowed Vlan 13,8 ## se asocia a vlan 13,8
no shutdown ## habilitamos la interface

Configuración Switch D2

Config term ## ingresar al modo configuración global
inter ether 2/0 ## interface del enlace troncal del Router 3
switchport trunk encapsulation dot1Q ## especifica el tipo encapsulación
switchport mode trunk ## habilita modo enlace troncal
switchport trunk allowed Vlan 13,8 ## se asocia a vlan 13,8

no shutdown ## habilitamos la interface

3.3 Configurar el EtherChannel en D1 y A1

Configuración Switch D1

```
Config term ## ingresar al modo configuración global
inter range e1/0-1 ## ingresamos las interfaces del EtherChannel
switchport trunk encapsulation dot1Q ## especifica el tipo encapsulación
switchport mode trunk ## habilita modo enlace troncal
channel-group 1 mode desirable ## la interface será administrada grupo 1
no shutdown ## habilitar la interface
```

Configuración Switch A1

```
Config term ## ingresar al modo configuración global
inter range e1/0-1 ## ingresamos las interfaces del EtherChannel
switchport trunk encapsulation dot1Q ## especifica el tipo encapsulación
switchport mode trunk ## habilita modo enlace troncal
channel-group 1 mode desirable ## la interface será administrada grupo 1
no shutdown ## habilitamos la interface
```

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

Configure y habilite los puertos de acceso de la siguiente manera:

Configuración Switch D1

```
inter e0/0 ## interface donde está conectada la pc1  
switchport mode Access ## colocar en puerto en modo acceso  
switchport access vlan 13 ## agréguese en vlan 13 modo acceso  
spanning-tree portfast ## establecer automáticamente el valor de prioridad  
no shutdown ## habilitar la interface  
exit ## salida del modo interface
```

Configuración Switch D2

```
inter e0/0 ## interface donde está conectada la pc2  
switchport mode Access ## colocar en puerto en modo acceso  
switchport access vlan 13 ## agréguese en vlan 13 modo acceso  
spanning-tree portfast ## establecer automáticamente el valor de prioridad  
no shutdown ## habilitar la interface  
exit ## salida del modo interface
```

```
inter e0/0 ## interface donde está conectada la pc4  
switchport mode Access ## colocar en puerto en modo acceso  
switchport access vlan 8 ## agréguese en vlan 8 modo acceso
```

```
spanning-tree portfast ## establecer automáticamente el valor de prioridad  
no shutdown ## habilitar la interface  
exit ## salida del modo interface
```

Configuración Switch A1

```
inter e0/0 ## interface donde está conectada la pc3  
switchport mode Access ## colocar en puerto en modo acceso  
switchport access vlan 8 ## agréguese en vlan 8 modo acceso  
spanning-tree portfast ## establecer automáticamente el valor de prioridad  
no shutdown ## habilitar la interface  
exit ## salida del modo interface  
wr ## guardamos la configuración
```

Se valida la configuración de cada Switch, Mediante el comando Show run interface.

Switch D1

```
D1#show interface trunk  
D1#show run interface e0/0
```

Figura 14 Verificación de Comandos en Switch D1

```
D1#show interface trunk

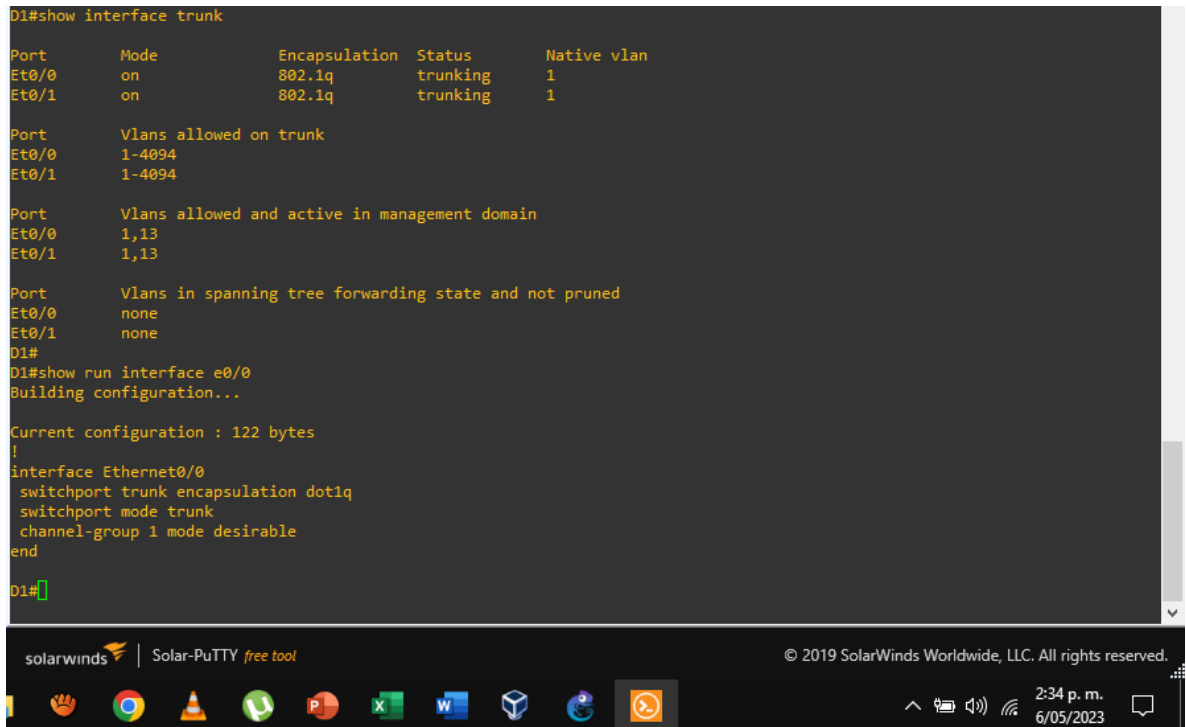
Port      Mode           Encapsulation  Status        Native vlan
Et0/0     on             802.1q         trunking      1
Et0/1     on             802.1q         trunking      1

Port      Vlans allowed on trunk
Et0/0     1-4094
Et0/1     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1,13
Et0/1     1,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     none
Et0/1     none
D1#
D1#show run interface e0/0
Building configuration...

Current configuration : 122 bytes
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
end
D1#
```



Fuente: propia

Switch D2

D2#show interface trunk

D2#show run interface e0/2

Figura 15 Verificación de Comandos en Switch D2

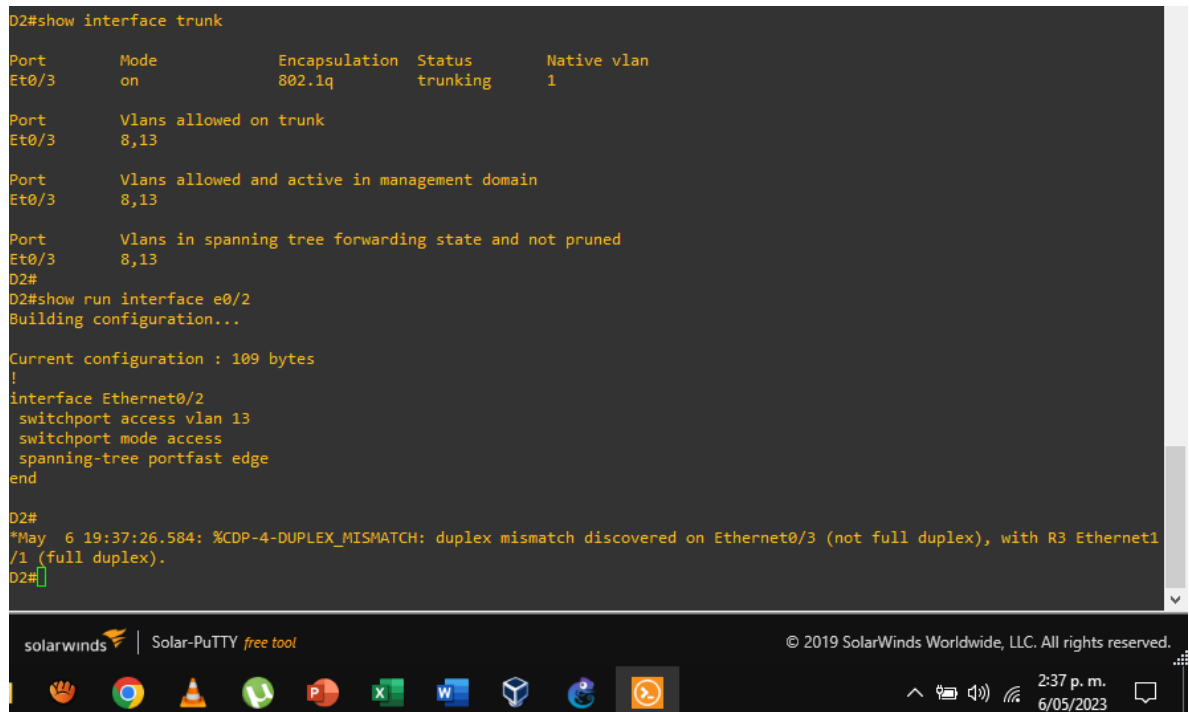
```
D2#show interface trunk
Port      Mode          Encapsulation  Status        Native vlan
Et0/3     on            802.1q         trunking      1

Port      Vlans allowed on trunk
Et0/3     8,13

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

Port      Vlans in spanning tree forwarding state and not pruned
Et0/3     8,13
D2#
D2#show run interface e0/2
Building configuration...

Current configuration : 109 bytes
!
interface Ethernet0/2
 switchport access vlan 13
 switchport mode access
 spanning-tree portfast edge
end
D2#
*May  6 19:37:26.584: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/3 (not full duplex), with R3 Ethernet1/1 (full duplex).
D2#
```



Fuente: propia

Switch A1

A1#show interface trunk

A1#show run interface e0/0

Figura 16 Verificación de Comandos en Switch A1

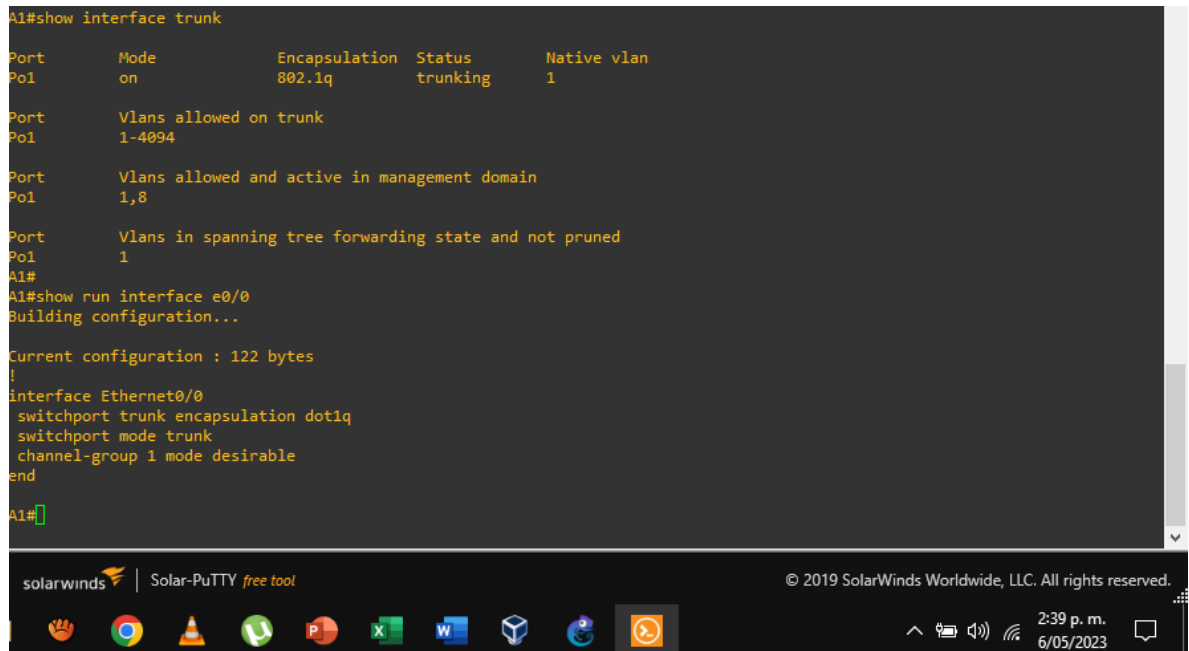
```
A1#show interface trunk
Port      Mode          Encapsulation  Status        Native vlan
Po1       on            802.1q         trunking      1

Port      Vlans allowed on trunk
Po1       1-4094

Port      Vlans allowed and active in management domain
Po1       1,8

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1
A1#
A1#show run interface e0/0
Building configuration...

Current configuration : 122 bytes
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
end
A1#
```



Fuente: propia

3.5 Verificación de la conectividad de PC a PC.

Se realiza verificación de la conectividad IPv4 e IPv6 entre los PCs que pertenecen a la VRF de Usuarios Especiales.

Figura 17 Ping IPv4 e IPv6 desde PC1 a PC2

```
PC1> ping 10.0.213.16
84 bytes from 10.0.213.16 icmp_seq=1 ttl=61 time=55.862 ms
84 bytes from 10.0.213.16 icmp_seq=2 ttl=61 time=43.318 ms
84 bytes from 10.0.213.16 icmp_seq=3 ttl=61 time=64.695 ms
84 bytes from 10.0.213.16 icmp_seq=4 ttl=61 time=53.930 ms
84 bytes from 10.0.213.16 icmp_seq=5 ttl=61 time=53.820 ms

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

2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=272.647 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=61.586 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=61.684 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=62.047 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=60.970 ms

PC1> █
```

Fuente: propia

Figura 18 Ping IPv4 e IPv6 desde PC3 a PC4

```
PC3> ping 10.0.208.16
84 bytes from 10.0.208.16 icmp_seq=1 ttl=61 time=63.965 ms
84 bytes from 10.0.208.16 icmp_seq=2 ttl=61 time=54.688 ms
84 bytes from 10.0.208.16 icmp_seq=3 ttl=61 time=63.928 ms
84 bytes from 10.0.208.16 icmp_seq=4 ttl=61 time=82.710 ms
84 bytes from 10.0.208.16 icmp_seq=5 ttl=61 time=57.642 ms

PC3>
PC3>
PC3> ping 2001:db8:acad:208::50/64

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=309.894 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=65.964 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=62.954 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=56.128 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=62.851 ms
```

Fuente: propia

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 4 tareas de configuración

Task#	Task	Specification
4.1	On all devices, secure privileged EXEC mode.	Configure an enable secret as follows: <ul style="list-style-type: none">• Algorithm type: SCRYPT• Password: hmmmeray161.
4.2	On all devices, create a local user account.	Configure a local user: <ul style="list-style-type: none">• Name: admin• Privilege level: 15• Algorithm type: SCRYPT• Password: hmmmeray161.
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

Fuente: propia

4.1 En todos los dispositivos, configurar modo EXEC privilegiado.

Configuración Router R1

config ter ## ingresamos al modo configuración global

Enable secret hmmeray161 ## proporciona mayor seguridad

Configuración Router R2

config ter ## ingresamos al modo configuración global

Enable secret n hmmeray161 ## proporciona mayor seguridad

Configuración Router R3

config ter ## ingresamos al modo configuración global

Enable secret hmmeray161 ## proporciona mayor seguridad

Configuración Switch D1

config ter ## ingresamos al modo configuración global

Enable secret hmmeray161 ## proporciona mayor seguridad

Configuración Switch D2

config ter ## ingresamos al modo configuración global

Enable secret hmmeray161 ## proporciona mayor seguridad

Configuración Switch A1

config ter ## ingresamos al modo configuración global

Enable secret hmmeray161 ## proporciona mayor seguridad

4.2 Crear una cuenta de usuario local en todos los dispositivos

Configuración Router R1

config ter ## ingresamos al modo configuración global

Username admin privilege 15 secret hmmeray161 ## usuario nivel privileg

Configuración Router R2

config ter ## ingresamos al modo configuración global

Username admin privilege 15 secret hmmeray161 ## usuario nivel privileg

Configuración Router R3

config ter ## ingresamos al modo configuración global

Username admin privilege 15 secret hmmeray161 ## usuario nivel privileg

Configuración Switch D1

config ter ## ingresamos al modo configuración global

Username admin privilege 15 secret hmmeray161 ## usuario nivel privileg

Configuración Switch D2

config ter ## ingresamos al modo configuración global

Username admin privilege 15 secret hmmeray161 ## usuario nivel privileg

Configuración Switch A1

config ter ## ingresamos al modo configuración global

Username admin privilege 15 secret hmmeray161 ## usuario nivel privileg

4.3 Habilite la autenticación AAA en todos los dispositivos.

Configuración Router R1

aaa new-model ## aplica la autenticación local a la interface

aaa authentication login default local ## autenticación de dispositivos

Configuración Router R2

aaa new-model ## aplica la autenticación local a la interface

aaa authentication login default local ## autenticación de dispositivos

Configuración Router R3

aaa new-model ## aplica la autenticación local a la interface

aaa authentication login default local ## autenticación de dispositivos

Configuración Switch D1

aaa new-model ## aplica la autenticación local a la interface

aaa authentication login default local ## autenticación de dispositivos

Configuración Switch D2

aaa new-model ## aplica la autenticación local a la interface

aaa authentication login default local ## autenticación de dispositivos

Configuración Switch A1

aaa new-model ## aplica la autenticación local a la interface

aaa authentication login default local ## autenticación de dispositivos

Verificación del nombre de usuario y la autenticación AAA

Figura 19 Nombre de usuario y autenticación AAA en R1

```
R1# config ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#Service password-encryption
R1(config)#Enable secret hmmeray161
R1(config)#Username admin secret 0 hmmeray161
R1(config)#Username admin privilege 15 secret hmmeray161
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
```

Fuente: propia

Figura 20 Nombre de usuario y autenticación AAA en R2

```
R2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#Service password-encryption
R2(config)#Enable secret hmmeray161
R2(config)#Username admin secret 0 hmmeray161
R2(config)#Username admin privilege 15 secret hmmeray161
R2(config)#aaa new-model
R2(config)#aaa authentication login default local
```

Fuente: propia

Figura 21 Nombre de usuario y autenticación AAA en R3

```
R3(config)#Service password-encryption
R3(config)#Enable secret hmmeray161
R3(config)#Username admin secret 0 hmmeray161
R3(config)#Username admin privilege 15 secret hmmeray161
R3(config)#aaa new-model
R3(config)#aaa authentication login default local
```

Fuente: propia

Figura 22 Nombre de usuario y autenticación AAA en D1

```
D1#config ter
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#Enable secret hmmeray161
D1(config)#Username admin privilege 15 secret hmmeray161
D1(config)#aaa new-model
D1(config)#aaa authentication login default local
```

Fuente: propia

Figura 23 Nombre de usuario y autenticación AAA en D2

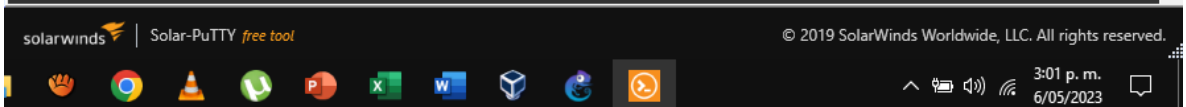
```
D2(config)#Enable secret hmmeray161
D2(config)#Username admin privilege 15 secret hmmeray161
D2(config)#aaa new-model
D2(config)#aaa authentication login default local
D2(config)#do wr
Building configuration...
Compressed configuration from 1458 bytes to 890 bytes[OK]
D2(config)#
```



Fuente: propia

Figura 24 Nombre de usuario y autenticación AAA en A1

```
A1#config ter
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#Service password-encryption
A1(config)#Enable secret hmmeray161
A1(config)#Username admin secret 0 hmmeray161
A1(config)#Username admin privilege 15 secret hmmeray161
A1(config)#aaa new-model
A1(config)#aaa authentication login default local
A1(config)#do wr
Building configuration...
Compressed configuration from 1554 bytes to 931 bytes[OK]
A1(config)#
```



Fuente: propia

CONCLUSIONES

Con el desarrollo de las pruebas de habilidades prácticas de CCNP, es posible adquirir las capacidades necesarias para administrar equipos de red (como enrutadores y conmutadores), utilizar recursos y herramientas para establecer conexiones de red y resolver problemas que surjan.

Se describen adecuadamente las etapas de desarrollo del curso donde se logra comprender y evidenciar la configuración de los equipos de redes, mediante el escenario tratado el cual refleja situaciones problema y cotidianas en la dinámica de labores profesionales en entornos laborales, lo que implica no solo un componente evaluativo para el diplomado sino una preparación académica para el entorno laboral.

Se logra extraer, elaborar, plantear y conocer programas durante nuestro aprendizaje de habilidades prácticas como el GNS3 la cual es una herramienta muy poderosa que permite no solo entender mejor las redes y sus protocolos de enrutamiento, sino también la construcción lógica para la posterior implementación de cualquier sistema de redes en el ámbito laboral.

BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

<https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

<https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

<https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101.

<https://1drv.ms/b/s!AmIJYeiNT1InMfy2rhPZHwEoWx>