

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CAMILO ANDRES BECERRA CORREDOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA ELECTRONICA
BOGOTA
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CAMILO ANDRES BECERRA CORREDOR

Diplomado de opción de grado presentado para optar el título de
INGENIERO ELECTRONICO

DIRECTOR:
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGNIERIA ELECTRONICA
BOGOTA
2023

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 28 abril 2023

AGRADECIMIENTOS

Agradezco primero a Dios por permitirme llegar a este punto de mi carrera profesional de manera satisfactoria y permitirme estar en un punto muy cercano a la obtención de mi título de Ingeniero electrónico.

Reconozco a cada uno de los tutores y directores de las diferentes áreas y materias y a la Universidad, los cuales con sus conocimientos y enseñanzas me guiaron a través del tiempo para hacer realidad uno de mis más grandes sueños y una de las metas con mayor importancia en mi formación académica.

A cada uno de los compañeros con los que compartí los escenarios de aprendizaje y que con su ética y profesionalismo logramos completar esta hermosa carrera.

CONTENIDO

	Pág.
AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	7
RESUMEN.....	10
ABSTRACT.....	11
INTRODUCCIÓN	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.	15
PARTE 2: Configurar vrf y enrutamiento estático	22
2.1 On R1, R2, and R3, configure VRF-Lite VRFs as shown in the topology diagram.	23
2.2 On R1, R2, and R3, configure IPv4 and IPv6 interfaces on each VRF as detailed in the addressing table above.	25
2.3 On R1 and R3, configure default static routes pointing to R2.....	30
2.4. Verify connectivity in each VRF.....	35
PARTE 3. Configurar Capa 2	37
3.1 On D1, D2, and A1, disable all interfaces.....	38
3.2 On D1 and D2, configure the trunk links to R1 and R3.....	38
3.3 On D1 and A1, configure the EtherChannel.	39
3.4 On D1, D2, and A1, configure access ports for PC1, PC2, PC3, and PC4.	40
3.5 Verify PC to PC connectivity.....	41
PARTE 4. Configurar Seguridad	44
4.1 On all devices, secure privileged EXE mode.....	44
4.2 On all devices, create a local user account.	46
4.3 On all devices, enable AAA and enable AAA authentication.	47

CONCLUSIONES51
BIBLIOGRAFÍA.....52

LISTA DE TABLAS

TABLA 1.TABLA DE DIRECCIONAMIENTO.	14
TABLA 2.CONFIGURACIÓN ROUTER 1	15
TABLA 3.CONFIGURACION ROUTER 2	16
TABLA 4.CONFIGURACIÓN ROUTER 3	17
TABLA 5. CONFIGURACIÓN SWITCH D1	17
TABLA 6. CONFIGURACIÓN SWITCH D2	18
TABLA 7.CONFIGURACIÓN SWITCH A1	19
TABLA 8.ALMACENAMIENTO DE CONFIGURACIONES	19
TABLA 9. TAREAS DE CONFIGURACIÓN.	22
TABLA 10. CONFIGURACIÓN VRF R1	23
TABLA 11. CONFIGURACIÓN VRF R2	24
TABLA 12. CONFIGURACIÓN VRF EN R3	24
TABLA 13. CONFIGURACIÓN DE INTERFACES Y VRF EN R1	25
TABLA 14. CONFIGURACIÓN DE INTERFACES Y VRF EN R2	27
TABLA 15. CONFIGURACIÓN DE INTERFACES Y VRF EN R3	28
TABLA 16. CONFIGURACIÓN DE RUTAS ESTÁTICAS EN R1	30
TABLA 17. CONFIGURACIÓN DE RUTAS ESTÁTICAS EN R2	30
TABLA 18. CONFIGURACIÓN DE RUTAS ESTÁTICAS EN R3	32
TABLA 19. CONFIGURACIÓN DE DISPOSITIVOS FINALES	37
TABLA 20. DESHABILITAR INTERFACES EN LOS SW	38
TABLA 21. CONFIGURACIÓN ENLACES TRONCALES EN D1 Y D2	38
TABLA 22. CONFIGURACIÓN DE ETHERCHANNEL	39
TABLA 23. CONFIGURACIÓN DE PUERTOS DE ACCESO EN D1, D2 Y A1	40
TABLA 24. TAREAS DE CONFIGURACIÓN DE SEGURIDAD.	44
TABLA 25. CONFIGURACIÓN ALGORITMO DE ENCRIPTADO	44
TABLA 26. CREACIÓN DE CUENTA DE USUARIO LOCAL	46
TABLA 27. CONFIGURACIÓN AAA Y SU AUTENTICACIÓN	47

LISTA DE FIGURAS

FIGURA 1. ESCENARIO 1.	13
FIGURA 2. CONEXIÓN DISPOSITIVOS EN GNS3	15
FIGURA 3. ALMACENAMIENTO CONFIGURACIONES EN EL DISPOSITIVO	20
FIGURA 4. CONFIGURACIÓN IPV4 E IPV6 PC1 Y PC2	21
FIGURA 5. CONFIGURACIÓN IPV4 E IPV6 PC3 Y PC4	21
FIGURA 6. VERIFICACIÓN CONFIGURACIÓN VRF EN R1	32
FIGURA 7. VERIFICACIÓN CONFIGURACIÓN VRF EN R2	33
FIGURA 8. VERIFICACIÓN CONFIGURACIÓN VRF EN R3	33
FIGURA 9. VERIFICACIÓN RUTAS ESTÁTICAS EN R1	33
FIGURA 10. VERIFICACIÓN RUTAS ESTÁTICAS EN R2	34
FIGURA 11. VERIFICACIÓN RUTAS ESTÁTICAS EN R3	34
FIGURA 12. VERIFICACIÓN DE CONEXIÓN A LA INTERFAZ E1/1.2 IPV4	35
FIGURA 13. VERIFICACIÓN DE CONEXIÓN A LA INTERFAZ E1/1.2 IPV6	35
FIGURA 14. VERIFICACIÓN DE CONEXIÓN A LA INTERFAZ E1/1.1 IPV4	35
FIGURA 15. FIGURA 25 VERIFICACIÓN CONEXIÓN INTERFAZ E1/1.1 IPV6	36
FIGURA 16. VERIFICACIÓN DE CONEXIÓN ENTRE PC2 Y PC4	36
FIGURA 17. PING PC1 - PC2 IPV4	41
FIGURA 18. PING PC1 - PC2 IPV6	41
FIGURA 19. PING PC3 - PC4 IPV4	41
FIGURA 20. PING PC3 - PC4 IPV6	42
FIGURA 21. COMANDO VERIFICACIÓN INTERFACES TRUNK EN D1	42
FIGURA 22. VERIFICACION INTERFACES TRUNK EN D2	42
FIGURA 23. VERIFICACIÓN ETHERCHANNEL EN D1	43
FIGURA 24. USERNAME Y AUTENTICACIÓN AAA EN R1	49
FIGURA 25. USERNAME Y AUTENTICACIÓN AAA EN R2	49
FIGURA 26. USERNAME Y AUTENTICACIÓN AAA EN R3	50
FIGURA 27. USERNAME Y AUTENTICACIÓN AAA EN D1	50
FIGURA 28. USERNAME Y AUTENTICACIÓN AAA EN A1	50
FIGURA 29. USERNAME Y AUTENTICACIÓN AAA EN D2	50

GLOSARIO

DIRECCIONAMIENTO: El direccionamiento se refiere a la configuración de una red para asignar una dirección única y exclusiva a cada dispositivo conectado a ella. Esto ayuda a prevenir errores en la transmisión y recepción de datos.

GNS3: Es una herramienta de simulación gráfica de redes que permite a los usuarios diseñar topologías de redes complejas y simular dispositivos tanto reales como virtuales.

INTERFAZ: Es la conexión física y funcional que se establece entre dos dispositivos o sistemas que funcionan de manera independiente entre sí.

IPV4: Es el protocolo de dirección IP más comúnmente utilizado en la actualidad, que utiliza un formato de 32 bits para identificar hosts en una red.

IPV6: Es el estándar más reciente de dirección IP, que utiliza direcciones de 128 bits.

RUTAS ESTÁTICAS: Son rutas definidas manual y administrativamente para que los paquetes se envíen de un puerto de origen a un puerto de destino específico.

VLAN: Una VLAN (Virtual Local Area Network) es una red de área local virtual que opera como una subdivisión lógica más pequeña dentro de una red física de mayor envergadura, conectada por cable.

VRF: Es una tecnología que permite que un enrutador ejecute múltiples tablas de enrutamiento simultáneamente.

RESUMEN

En este proyecto, se ha planteado un escenario que permitirá la conexión de dos usuarios de forma independiente mediante una topología de red. Para lograr esto, se utilizará la herramienta GNS3, la cual nos permitirá emular los dispositivos que se irán a usar y construir la topología de red entregada en el escenario. Posteriormente, se aplicarán los scripts para configurar los ajustes básicos, el direccionamiento IPv4 e IPv6, la creación de VRF correspondientes para los usuarios General-Users y Special-Users, la creación de las VLAN 8 y 13, la encriptación de seguridad, rutas troncales y estáticas para los clientes o usuarios específicos y finalmente la seguridad de acceso a las configuraciones de los dispositivos.

A medida que se avanza en el desarrollo y configuración de la red, se realiza una descripción de cada línea de comando usado, así como las evidencias que soportan el funcionamiento deseado de la red. Se explicará cada parte de la configuración con sumo cuidado, a fin de garantizar la completa comprensión de la configuración de la red por parte de los estudiantes y profesionales de redes.

Finalmente, ya con las configuraciones realizadas de manera exitosa, se podrá evidenciar que se cuenta con conectividad completa entre los host pertenecientes a cada uno de los usuarios y que no se permite conectividad entre host de diferentes grupos.

Palabras clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this project, a scenario has been proposed that will allow the connection of two users independently through a network topology. To achieve this, the GNS3 tool will be used, which will allow us to emulate the devices that will be used and build the network topology delivered in the scenario. Subsequently, the scripts will be applied to configure the basic settings, IPv4 and IPv6 addressing, the creation of corresponding VRFs for General-Users and Special-Users, the creation of VLANs 8 and 13, security encryption, trunk routes and static for specific customers or users and finally the security of access to device settings.

As progress is made in the development and configuration of the network, a description of each command line used is made, as well as the evidence that supports the desired operation of the network. Each part of the configuration will be explained carefully to ensure complete understanding of network configuration by students and network professionals.

Finally, once the configurations have been carried out successfully, it will be possible to show that there is complete connectivity between the hosts belonging to each of the users and that connectivity between hosts from different groups is not allowed.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

En la actualidad, la seguridad de las redes es esencial para garantizar la protección de la información y el acceso seguro a los dispositivos debido al aumento de los ataques cibernéticos. Por esta razón, es fundamental que los administradores tengan el conocimiento necesario para implementar los servicios y protocolos que se requieren en una red.

El propósito de este informe es diseñar, configurar y direccionar una red LAN utilizando GNS3 con el objetivo de mejorar la calidad de los servicios de la red y poner a prueba la capacidad de los administradores para identificar y solucionar problemas de acceso o conexión. Se presta especial atención a la seguridad en todas las etapas del proceso de configuración para asegurar el funcionamiento seguro de la red.

La configuración adecuada de los switches y router es un elemento crucial en cualquier red, ya que estos dispositivos son responsables de conectar los dispositivos finales y los servidores, permitiendo la comunicación y transferencia de datos en toda la red. Es importante destacar que la seguridad de la red es fundamental para garantizar la protección de los datos y la privacidad de los usuarios. Por esta razón, en el presente informe se analizarán los aspectos más relevantes relacionados con la configuración de switches, incluyendo la creación de VLANs, la configuración de protocolos de enrutamiento y la implementación de mecanismos de seguridad como el control de acceso.

ESCENARIO PROPUESTO

Figura 1. Escenario 1.

Topología de la Red:



Fuente: Guía de Actividades escenario CCNP

Escenario

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

Para el desarrollo de la actividad, en la tabla de direccionamiento se tomarán los valores.

X=4

Y=X+Z =6 (Solo en R2)

Y=0 Demás dispositivos

Z=2

Nota importante: Debido a que el numero indicado para el direccionamiento es 402, se reemplaza el 0 del valor de Y por la suma entre X y Z para poder realizar el correcto direccionamiento en el router R2

TABLA DE DIRECCIONAMIENTO

Tabla 1. Tabla de direccionamiento.

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.4/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.4/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.4/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.4/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.6/24	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	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.2/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.2/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.40/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.40/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.40/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.40/24	2001:db8:acad:208::50/64	EUI-64

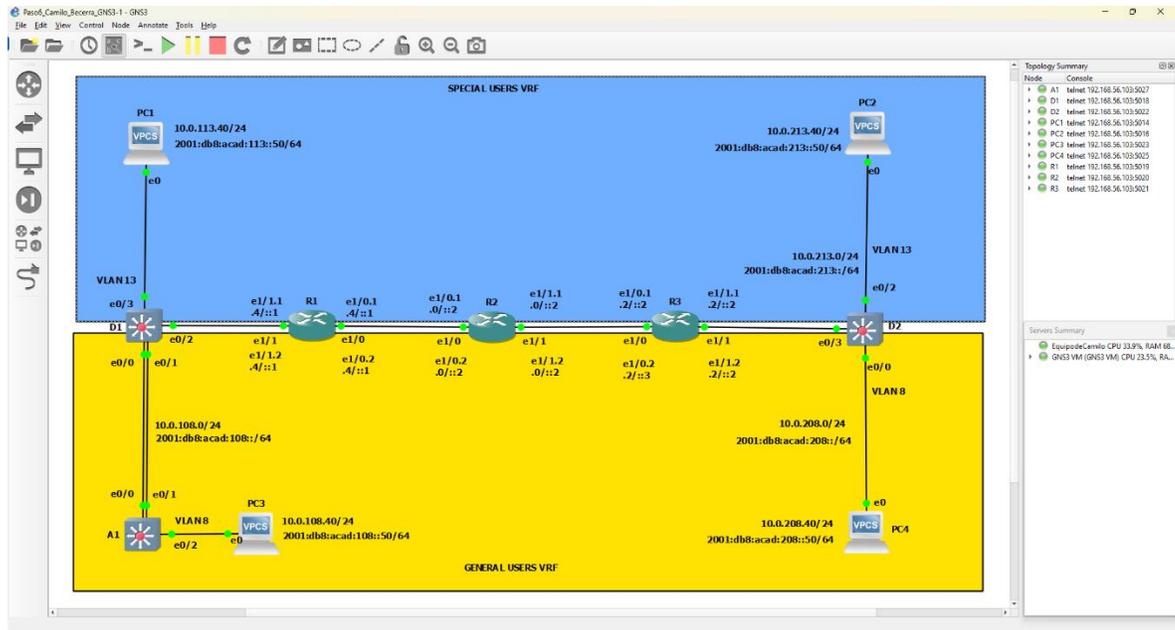
Fuente: Guía de Actividades escenario CCNP

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.

Figura 2. Conexión dispositivos en GNS3



Fuente: Escenario de Emulación GNS3

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.

Tabla 2. Configuración Router 1

DISPOSITIVO: ROUTER 1	
CODIGO	DESCRIPCION
Enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
hostname R1	Nombra el Dispositivo como R1
ipv6 unicast-routing	Habilitación del Routing IPV6
no ip domain lookup	Se deshabilita la búsqueda de dominio o

	DNS
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #	Configuración del MODBANNER con mensaje de Advertencia
line con 0	Línea 0
exec-timeout 0 0	Tiempo de espera
logging synchronous	Configuración de registro síncrono
exit	Salida

Fuente: Autoría Propia

Tabla 3. Configuración Router 2

DISPOSITIVO: ROUTER 2	
CODIGO	DESCRIPCION
Enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
hostname R2	Nombra el Dispositivo como R2
ipv6 unicast-routing	Habilitación del Routing IPV6
no ip domain lookup	Se deshabilita la búsqueda de dominio o DNS
banner motd # R2, ENCOR Skills Assessment, Scenario 2 #	Configuración del MODBANNER con mensaje de Advertencia
line con 0	Línea 0
exec-timeout 0 0	Tiempo de espera
logging synchronous	Configuración de registro síncrono
exit	Salida

Fuente: Autoría Propia

Tabla 4. Configuración Router 3

DISPOSITIVO: ROUTER 3	
CODIGO	DESCRIPCION
Enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
hostname R3	Nombra el Dispositivo como R2
ipv6 unicast-routing	Habilitación del Routing IPV6
no ip domain lookup	Se deshabilita la búsqueda de dominio o DNS
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #	Configuración del MODBANNER con mensaje de Advertencia
line con 0	Línea 0
exec-timeout 0 0	Tiempo de espera
logging synchronous	Configuración de registro síncrono
exit	Salida

Fuente: Autoría Propia

Tabla 5. Configuración Switch D1

DISPOSITIVO: SWITCH D1	
CODIGO	DESCRIPCION
Enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
hostname D1	Nombra el Dispositivo como D1
ipv6 unicast-routing	Habilitación del Routing IPV6
no ip domain lookup	Se deshabilita la búsqueda de dominio o DNS
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #	Configuración del MODBANNER con mensaje de Advertencia
line con 0	Línea 0
exec-timeout 0 0	Tiempo de espera
logging synchronous	Configuración de registro síncrono
exit	Salida
vlan 8	Se crea la Vlan 8
name General-Users	Se le asigna un nombre a la Vlan 8

exit	Salida
vlan 13	Se crea la Vlan 13
name Special-Users	Se le asigna nombre a la Vlan 13
exit	salida

Fuente: Autoría propia

Tabla 6. Configuración Switch D2

DISPOSITIVO: SWITCH D2	
CODIGO	DESCRIPCION
Enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
hostname D2	Nombra el Dispositivo como D2
ipv6 unicast-routing	Habilitación del Routing IPV6
no ip domain lookup	Se deshabilita la búsqueda de dominio o DNS
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #	Configuración del MODBANNER con mensaje de Advertencia
line con 0	Línea 0
exec-timeout 0 0	Tiempo de espera
logging synchronous	Configuración de registro síncrono
exit	Salida
vlan 8	Se crea la Vlan 8
name General-Users	Se le asigna un nombre a la Vlan 8
exit	Salida
vlan 13	Se crea la Vlan 13
name Special-Users	Se le asigna nombre a la Vlan 13
exit	salida

Fuente: Autoría Propia

Tabla 7. Configuración Switch A1

DISPOSITIVO: SWITCH A1	
CODIGO	DESCRIPCION
Enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
hostname A1	Nombra el Dispositivo como A1
ipv6 unicast-routing	Habilitación del Routing IPV6
no ip domain lookup	Se deshabilita la búsqueda de dominio o DNS
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #	Configuración del MODBANNER con mensaje de Advertencia
line con 0	Línea 0
exec-timeout 0 0	Tiempo de espera
logging synchronous	Configuración de registro síncrono
exit	Salida
vlan 8	Se crea la Vlan 8
name General-Users	Se le asigna un nombre a la Vlan 8
exit	Salida

Fuente: Autoría Propia

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

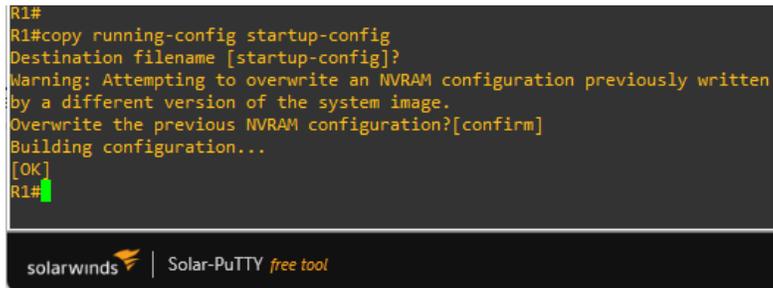
Tabla 8. Almacenamiento de configuraciones

DISPOSITIVO: R1, R2, R3, D1, D2, A1	
CODIGO	DESCRIPCION
copy running-config startup-config	Habilita el ingreso a la configuración del dispositivo.

Fuente: Autoría Propia

Figura 3. Almacenamiento configuraciones en el dispositivo

```
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#
```



Fuente: Escenario de Emulación GNS3

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

PC1

ip 10.0.113.40/24	10.0.113.4	Direccionamiento Ipv4 PC1
ip 2001:DB8:ACAD:113::50/64		Direccionamiento IPv6 PC1

PC2

ip 10.0.213.40/24	10.0.213.2	Direccionamiento IPv4 PC2
ip 2001:DB8:ACAD:213::50/64		Direccionamiento IPv6 PC2

PC3

ip 10.0.108.40/24	10.0.108.4	Direccionamiento IPv4 PC3
ip 2001:DB8:ACAD:108::50/64		Direccionamiento IPv6 PC3

PC4

ip 10.0.208.40/24	10.0.208.2	Direccionamiento IPv4 PC4
ip 2001:DB8:ACAD:208::50/64		Direccionamiento IPv6 PC4

Figura 4. Configuración IPv4 e IPv6 PC1 y PC2

```

PC1> ip 10.0.113.40/24 10.0.113.1
Checking for duplicate address...
PC1 : 10.0.113.40 255.255.255.0 gateway 10.0.113.1

PC1> ip 2001:db8:acad:113::50/64
PC1 : 2001:db8:acad:113::50/64

PC1> show ip

NAME          : PC1[1]
IP/MASK       : 10.0.113.40/24
GATEWAY       : 10.0.113.1
DNS           :
MAC           : 00:50:79:66:68:00
LPORT        : 20032
RHOST:PORT    : 127.0.0.1:20033
MTU           : 1500

PC1> show ipv6

NAME          : PC1[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6800/64
GLOBAL SCOPE    : 2001:db8:acad:113::50/64
DNS            :
ROUTER LINK-LAYER :
MAC           : 00:50:79:66:68:00
LPORT        : 20032
RHOST:PORT    : 127.0.0.1:20033
MTU           : 1500

PC2>
PC2> ip 10.0.213.40/24 10.0.213.1
Checking for duplicate address...
PC2 : 10.0.213.40 255.255.255.0 gateway 10.0.213.1

PC2> ip 2001:db8:acad:213::50/64 autosave
PC1 : 2001:db8:acad:213::50/64

PC2> show ipv4
Invalid arguments

PC2> show ip

NAME          : PC2[1]
IP/MASK       : 10.0.213.40/24
GATEWAY       : 10.0.213.1
DNS           :
MAC           : 00:50:79:66:68:01
LPORT        : 20030
RHOST:PORT    : 127.0.0.1:20031
MTU           : 1500

PC2> show ipv6

NAME          : PC2[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6801/64
GLOBAL SCOPE    : 2001:db8:acad:213::50/64
DNS            :
ROUTER LINK-LAYER :
MAC           : 00:50:79:66:68:01
LPORT        : 20030
RHOST:PORT    : 127.0.0.1:20031
MTU           : 1500
    
```

Fuente: Escenario de Emulación GNS3

Figura 5. Configuración IPv4 e IPv6 PC3 y PC4

```

PC3>
PC3> ip 10.0.108.40/24 10.0.108.1
Checking for duplicate address...
PC3 : 10.0.108.40 255.255.255.0 gateway 10.0.108.1

PC3> ip 2001:db8:acad:108::50/64 autosave
PC1 : 2001:db8:acad:108::50/64

PC3> show ip

NAME          : PC3[1]
IP/MASK       : 10.0.108.40/24
GATEWAY       : 10.0.108.1
DNS           :
MAC           : 00:50:79:66:68:02
LPORT        : 20034
RHOST:PORT    : 127.0.0.1:20035
MTU           : 1500

PC3> show ipv6

NAME          : PC3[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6802/64
GLOBAL SCOPE    : 2001:db8:acad:108::50/64
DNS            :
ROUTER LINK-LAYER :
MAC           : 00:50:79:66:68:02
LPORT        : 20034
RHOST:PORT    : 127.0.0.1:20035
MTU           : 1500

PC4>
PC4> ip 10.0.208.40/24 10.0.208.1
Checking for duplicate address...
PC4 : 10.0.208.40 255.255.255.0 gateway 10.0.208.1

PC4> ip 2001:db8:acad:208::50/64 autosave
PC1 : 2001:db8:acad:208::50/64

PC4> show ip

NAME          : PC4[1]
IP/MASK       : 10.0.208.40/24
GATEWAY       : 10.0.208.1
DNS           :
MAC           : 00:50:79:66:68:03
LPORT        : 20036
RHOST:PORT    : 127.0.0.1:20037
MTU           : 1500

PC4> show ipv6

NAME          : PC4[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6803/64
GLOBAL SCOPE    : 2001:db8:acad:208::50/64
DNS            :
ROUTER LINK-LAYER :
MAC           : 00:50:79:66:68:03
LPORT        : 20036
RHOST:PORT    : 127.0.0.1:20037
MTU           : 1500
    
```

Fuente: Escenario de Emulación GNS3

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 9. Tareas de Configuración.

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 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.Z · ping vrf General-Users 2001:db8:acad:208::1 · ping vrf Special-Users 10.0.213.Z · ping vrf Special-Users 2001:db8:acad:213::1

Fuente: Guía de Actividades escenario CCNP

2.1 On R1, R2, and R3, configure VRF-Lite VRFs as shown in the topology diagram.

Tabla 10. Configuración VRF R1

CONFIGURACION EN R1	
CODIGO	DESCRIPCION
enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
vrf definition Special-Users	Define la VRF como Special-Users.
description Special-Users	Describe la VRF como Special-Users
address-family ipv4	Habilita el direccionamiento IPV4
exit	Salida
description Special-Users	Describe la VRF como Special Users
address-family ipv6	Habilita el direccionamiento IPV6
exit	Salida
vrf definition General-Users	Define la VRF como General-Users.
description General-Users	Describe la VRF como General-Users
address-family ipv4	Habilita el direccionamiento IPV4
exit	Salida
description General-Users	Describe la VRF como General-Users
address-family ipv6	Habilita el direccionamiento IPV6
Exit	salida

Fuente: Autoría Propia

Tabla 11. Configuración VRF R2

CONFIGURACION EN R2	
CODIGO	DESCRIPCION
enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
vrf definition Special-Users	Define la VRF como Special-Users.
description Special-Users	Describe la VRF como Special-Users
address-family ipv4	Habilita el direccionamiento IPV4
exit	Salida
description Special-Users	Describe la VRF como Special Users
address-family ipv6	Habilita el direccionamiento IPV6
exit	Salida
vrf definition General-Users	Define la VRF como General-Users.
description General-Users	Describe la VRF como General-Users
address-family ipv4	Habilita el direccionamiento IPV4
exit	Salida
description General-Users	Describe la VRF como General-Users
address-family ipv6	Habilita el direccionamiento IPV6
Exit	salida

Fuente: Autoría Propia

Tabla 12. Configuración VRF en R3

CONFIGURACION EN R3	
CODIGO	DESCRIPCION
enable	Habilita el ingreso a la configuración del dispositivo.
Configure terminal	Ingresa al modo de configuración del dispositivo.
vrf definition Special-Users	Define la VRF como Special-Users.
description Special-Users	Describe la VRF como Special-Users
address-family ipv4	Habilita el direccionamiento IPV4
exit	Salida
description Special-Users	Describe la VRF como Special Users
address-family ipv6	Habilita el direccionamiento IPV6
exit	Salida
vrf definition General-Users	Define la VRF como General-Users.
description General-Users	Describe la VRF como General-Users
address-family ipv4	Habilita el direccionamiento IPV4
exit	Salida
description General-Users	Describe la VRF como General-Users
address-family ipv6	Habilita el direccionamiento IPV6
Exit	salida

Fuente: Autoría Propia

2.2 On R1, R2, and R3, configure IPv4 and IPv6 interfaces on each VRF as detailed in the addressing table above.

Se configuran las interfaces IPv4 e IPv6 en las dos VRF creadas; teniendo en cuenta que todos los enrutadores utilizan Router-On-A-Stick en sus interfaces e1/1.x para admitir la separación de los VRF. Por ende, el procedimiento consiste en crear dos sub-interfaces, usar el protocolo de encapsulación IEEE 802.1Q, asignar las direcciones IPv4 e IPv6, las direcciones locales de enlace y por último se activan las interfaces.

Tabla 13. Configuración de interfaces y VRF en R1

ROUTER R1	
Codigo	Descripción
Enable	Habilita el Dispositivo para configurar
Configure terminal	habilita la configuración en el dispositivo
interface e1/0.1	Selecciona la interfaz
encapsulation dot1q 13	encapsulación de la subinterfaz como 802.1Q para VLAN 13.
vrf forward Special-Users	Habilita el VRF en el Router para Special-Users
ip address 10.0.12.4 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::1:1 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:12::1/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/0.2	Selecciona la interfaz
encapsulation dot1q 8	encapsulación de la subinterfaz como 802.1Q para VLAN 8.
vrf forward General-Users	Habilita el VRF en el Router para General-Users
ip address 10.0.12.4 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::1:2 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:12::1/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida

interface e1/0	Selecciona la interfaz
no ip address	No se establece configuración IP v4.
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1.1	Selecciona la interfaz
encapsulation dot1q 13	encapsulación de la subinterfaz como 802.1Q para VLAN 13.
vrf forward Special-Users	Habilita el VRF en el Router para Special-Users
ip address 10.0.113.4 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::1:3 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:113::1/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1.2	Selecciona la interfaz
encapsulation dot1q 8	encapsulación de la subinterfaz como 802.1Q para VLAN 8.
vrf forward General-Users	Habilita el VRF en el Router para General-Users
ip address 10.0.108.4 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::1:4 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:108::1/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1	Selecciona la interfaz
no ip address	No se establece configuración IP v4.
no shutdown	Habilitación de la interfaz
exit	Salida

Fuente: Autoría Propia.

Tabla 14. Configuración de interfaces y VRF en R2

ROUTER R2	
Código	Descripción
Enable	Habilita el Dispositivo para configurar
Configure terminal	habilita la configuración en el dispositivo
interface e1/0.1	Selecciona la interfaz
encapsulation dot1q 13	encapsulación de la subinterfaz como 802.1Q para VLAN 13.
vrf forward Special-Users	Habilita el VRF en el Router para Special-Users
ip address 10.0.12.6 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::2:1 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:12::2/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/0.2	Selecciona la interfaz
encapsulation dot1q 8	encapsulación de la subinterfaz como 802.1Q para VLAN 8.
vrf forward General-Users	Habilita el VRF en el Router para General-Users
ip address 10.0.12.6 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::2:2 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:12::2/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/0	Selecciona la interfaz
no ip address	No se establece configuración IP v4.
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1.1	Selecciona la interfaz
encapsulation dot1q 13	encapsulación de la subinterfaz como 802.1Q para VLAN 13.
vrf forward Special-Users	Habilita el VRF en el Router para Special-Users
ip address 10.0.23.6 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::2:3 link- local	Configuración de IP v6 de enlace local

ipv6 address 2001:db8:acad:23::2/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1.2	Selecciona la interfaz
encapsulation dot1q 8	encapsulación de la subinterfaz como 802.1Q para VLAN 8.
vrf forward General-Users	Habilita el VRF en el Router para General-Users
ip address 10.0.23.6 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::2:4 link-local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:23::2/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1	Selecciona la interfaz
no ip address	No se establece configuración IP v4.
no shutdown	Habilitación de la interfaz
exit	Salida

Fuente: Autoría propia.

Tabla 15. Configuración de interfaces y VRF en R3

ROUTER R3	
Codigo	Descripción
Enable	Habilita el Dispositivo para configurar
Configure terminal	habilita la configuración en el dispositivo
interface e1/0.1	Selecciona la interfaz
encapsulation dot1q 13	encapsulación de la subinterfaz como 802.1Q para VLAN 13.
vrf forward Special-Users	Habilita el VRF en el Router para Special-Users
ip address 10.0.23.2 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::3:1 link-local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:23::3/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/0.2	Selecciona la interfaz
encapsulation dot1q 8	encapsulación de la subinterfaz como 802.1Q para VLAN 8.

vrf forward General-Users	Habilita el VRF en el Router para General-Users
ip address 10.0.23.2 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::3:2 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:23::3/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/0	Selecciona la interfaz
no ip address	No se establece configuración IP v4.
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1.1	Selecciona la interfaz
encapsulation dot1q 13	encapsulación de la subinterfaz como 802.1Q para VLAN 13.
vrf forward Special-Users	Habilita el VRF en el Router para Special-Users
ip address 10.0.213.2 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::3:3 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:213::1/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1.2	Selecciona la interfaz
encapsulation dot1q 8	encapsulación de la subinterfaz como 802.1Q para VLAN 8.
vrf forward General-Users	Habilita el VRF en el Router para General-Users
ip address 10.0.208.2 255.255.255.0	Configuración de IP v4 y mascara de subred
ipv6 address fe80::3:4 link- local	Configuración de IP v6 de enlace local
ipv6 address 2001:db8:acad:208::1/64	Configuración de IPv6 de enlace Global
no shutdown	Habilitación de la interfaz
exit	Salida
interface e1/1	Selecciona la interfaz
no ip address	No se establece configuración IP v4.
no shutdown	Habilitación de la interfaz
exit	Salida

Fuente: Autoría Propia.

2.3 On R1 and R3, configure default static routes pointing to R2.

Se realiza la configuración de las rutas estáticas predeterminadas Ipv4 e Ipv6 de acuerdo con los dos grupos creados para la red.

Tabla 16. Configuración de rutas estáticas en R1

ROUTER R1	
Código	Descripción
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.6	Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.6	Ruta estática predeterminada IPv4 para VRF General-Users.
ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2	Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2	Ruta estática predeterminada IPv6 para VRF General-Users.

Fuente: Autoría Propia

Tabla 17. Configuración de rutas estáticas en R2

ROUTER R2	
Código	Descripción
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.4	Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.2	Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.4	Ruta estática predeterminada IPv4 para VRF General-Users.

ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.2	Ruta estática predeterminada IPv4 para VRF General-Users.
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1	Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3	Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1	Ruta estática predeterminada IPv6 para VRF General-Users.
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3	Ruta estática predeterminada IPv6 para VRF General-Users.

Fuente: Autoría Propia.

Tabla 18. Configuración de rutas estáticas en R3

ROUTER R3	
Codigo	Descripción
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.6	Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.6	Ruta estática predeterminada IPv4 para VRF General-Users.
ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2	Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2	Ruta estática predeterminada IPv6 para VRF General-Users.

Fuente: Autoría Propia.

Después de configurar los routers con los comandos anteriores en el puerto de consola de cada dispositivo según corresponda, se realizan validaciones de que estén bien realizadas las configuraciones y la conexión VRF. Por lo tanto, se inicia verificando el direccionamiento IP de las VRFs, por medio de colocar el comando:

```
show ip vrf interfaces
```

Figura 6. Verificación configuración VRF en R1

```
R1#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.4       General-Users    up
Et1/1.2        10.0.108.4      General-Users    up
Et1/0.1        10.0.12.4       Special-Users    up
Et1/1.1        10.0.113.4      Special-Users    up
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Fuente: Escenario de Emulación GNS3

Figura 7.Verificación configuración VRF en R2

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

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Fuente: Escenario de Emulación GNS3

Figura 8.Verificación configuración VRF en R3

```
Interface          IP-Address      VRF              Protocol
Et1/0.2            10.0.23.2      General-Users    up
Et1/1.2            10.0.208.2     General-Users    up
Et1/0.1            10.0.23.2      Special-Users    up
Et1/1.1            10.0.213.2     Special-Users    up
R3#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Fuente: Escenario de Emulación GNS3

Verificación del direccionamiento estático en cada router usando el comando:
show run | inc route

Figura 9. Verificación Rutas estáticas en R1

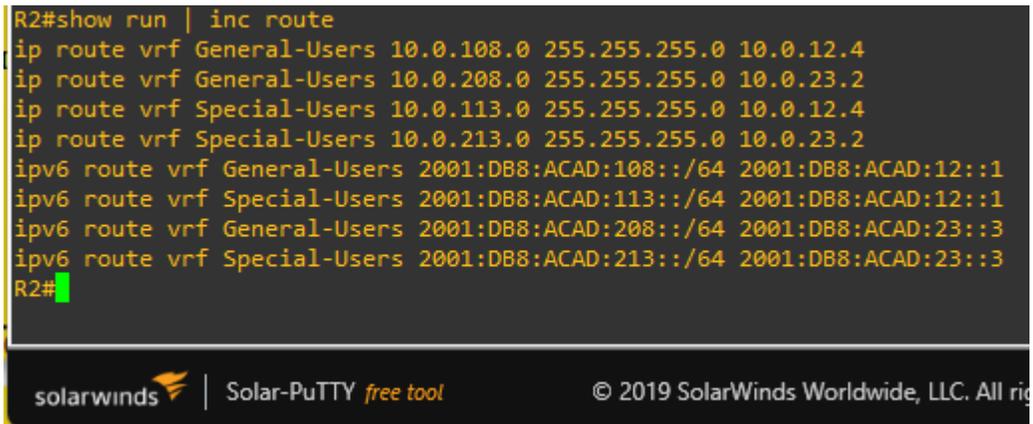
```
R1#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.6
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.6
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWind

Fuente: Escenario de Emulación GNS3

Figura 10. Verificación Rutas estáticas en R2

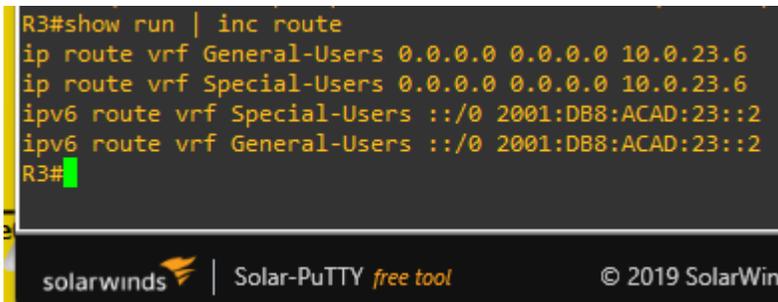
```
R2#show run | inc route
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.4
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.2
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.4
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.2
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3
R2#
```



Fuente: Escenario de Emulación GNS3

Figura 11. Verificación Rutas estáticas en R3

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



Fuente: Escenario de Emulación GNS3

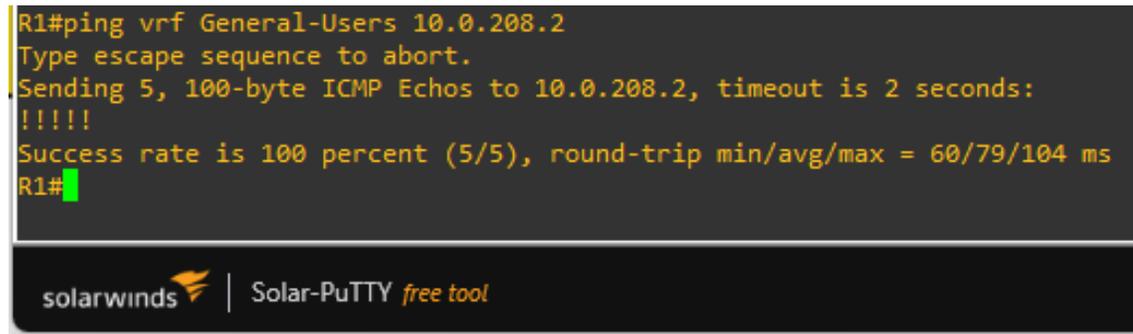
2.4. Verify connectivity in each VRF.

Desde R1, verificar conectividad con R3

- ping vrf General-Users 10.0.208.2

Figura 12. Verificación de conexión a la interfaz E1/1.2 Ipv4

```
R1#ping vrf General-Users 10.0.208.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/79/104 ms
R1#
```

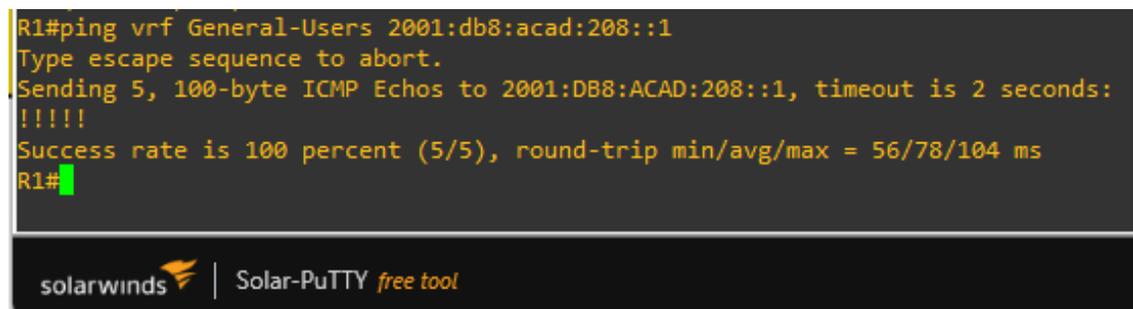


Fuente: Escenario de Emulación GNS3

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

Figura 13. Verificación de conexión a la interfaz E1/1.2 Ipv6

```
R1#ping vrf General-Users 2001:db8:acad:208::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/78/104 ms
R1#
```

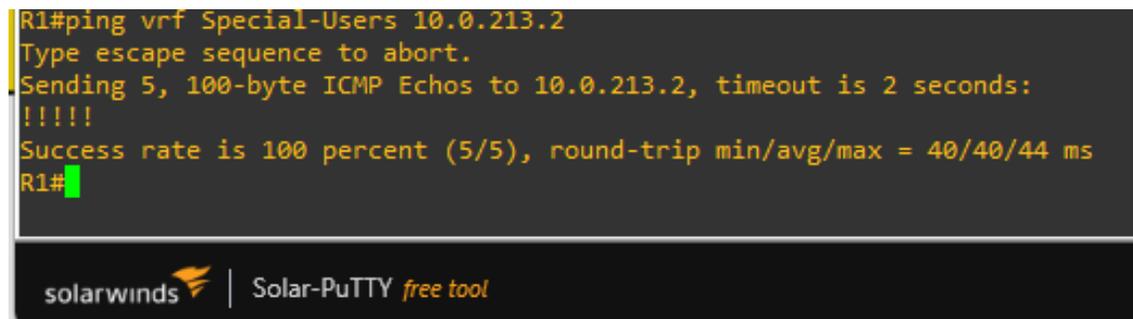


Fuente: Escenario de Emulación GNS3

- ping vrf Special-Users 10.0.213.2

Figura 14. Verificación de conexión a la interfaz E1/1.1 Ipv4

```
R1#ping vrf Special-Users 10.0.213.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms
R1#
```



Fuente: Escenario de Emulación GNS3

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

Figura 15. Figura 25 Verificación conexión interfaz E1/1.1 Ipv6

```
R1#ping vrf Special-Users 2001:db8:acad:213::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
R1#
```



Fuente: Escenario de Emulación GNS3

Con las configuraciones realizadas hasta el momento, se tiene que R1 no está habilitado para realizar ping entre PC2 o PC4. Por lo tanto, este deberá fallar.

Comando:

ping 10.0.208.40

Figura 16. Verificación de conexión entre PC2 y PC4

```
PC2> ping 10.0.208.40
host (10.0.213.1) not reachable
PC2>
```

Fuente: Escenario de Emulación GNS3.

PARTE 3. Configurar Capa 2

En esta parte, se tendrán que configurar los Switches para soportar la conectividad con los dispositivos finales.

Las tareas de configuración son las siguientes:

Tabla 19. Configuración de dispositivos finales

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. • 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.

Fuente: Guía de Actividades escenario CCNP

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

Tabla 20. Deshabilitar interfaces en los SW

SWITCH D1	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Selecciona el rango de las interfaces en el SW D1
shutdown	Deshabilita las interfaces seleccionadas
exit	Salida
SWITCH D2	
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Selecciona el rango de las interfaces en el SW D2
shutdown	Deshabilita las interfaces seleccionadas
exit	Salida
SWITCH A1	
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Selecciona el rango de las interfaces en el SW D1
shutdown	Deshabilita las interfaces seleccionadas
exit	Salida

Fuente: Autoría Propia

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

Tabla 21. Configuración Enlaces troncales en D1 y D2

SWITCH D1	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface e0/2	Configuración de la interfaz e0/2
switchport trunk encapsulation dot1q	Configura el enlace troncal con encapsulación 802.1Q.
switchport mode trunk	Establece el modo troncal en la interfaz
no shutdown	habilita la interfaz seleccionada
Exit	salida

SWITCH D2	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface e0/3	Configuración de la interfaz e0/3
switchport trunk encapsulation dot1q	Configura el enlace troncal con encapsulación 802.1Q.
switchport mode trunk	Establece el modo troncal en la interfaz
no shutdown	habilita la interfaz seleccionada
Exit	salida

Fuente: Autoría Propia.

3.3 On D1 and A1, configure the EtherChannel.

Tabla 22. Configuración de EtherChannel

SWITCH D1	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface range e0/0, e0/1	Selecciona las interfaces e0/0 y e0/1
switchport trunk encapsulation dot1q	Configura el enlace troncal con encapsulación 802.1Q.
switchport mode trunk	Establece el modo troncal en la interfaz
channel-group 1 mode desirable	Configura los puertos en modo activo para negociar los paquetes PAgP
no shutdown	Habilita las interfaces.
exit	salida
SWITCH A1	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface range e0/0, e0/1	Selecciona las interfaces e0/0 y e0/1
switchport trunk encapsulation dot1q	Configura el enlace troncal con encapsulación 802.1Q.
switchport mode trunk	Establece el modo troncal en la interfaz
channel-group 1 mode desirable	Configura los puertos en modo activo para negociar los paquetes PAgP
no shutdown	Habilita las interfaces.
exit	salida

Fuente: Autoría Propia.

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

Tabla 23. Configuración de puertos de acceso en D1, D2 y A1

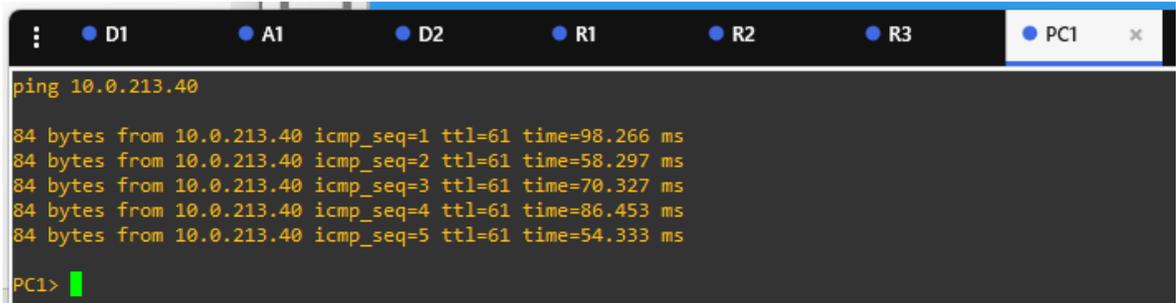
SWITCH D1	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface e0/3	Configuración de la interface e0/3
switchport mode access	Establece el modo de acceso en el puerto
switchport access vlan 13	Asigna la vlan 13 al puerto
spanning-tree portfast	Habilita el puerto con PortFast y protección BPDU
no shutdown	Habilita la Interfaz
exit	salida
SWITCH D2	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface e0/2	Configuración de la interface e0/2
switchport mode access	Establece el modo de acceso en el puerto
switchport access vlan 13	Asigna la vlan 13 al puerto
spanning-tree portfast	Habilita el puerto con PortFast y protección BPDU
no shutdown	Habilita la Interfaz
exit	salida
interface e0/0	Configuración de la interface e0/0
switchport mode access	Establece el modo de acceso en el puerto
switchport access vlan 8	Asigna la vlan 8 al puerto
spanning-tree portfast	Habilita el puerto con PortFast y protección BPDU
no shutdown	Habilita la Interfaz
exit	salida
SWITCH A1	
CODIGO	DESCRIPCION
Enable	Habilita el dispositivo a configurar
Configure terminal	Habilita la configuración en el dispositivo
interface e0/2	Configuración de la interface e0/2
switchport mode access	Establece el modo de acceso en el puerto
switchport access vlan 8	Asigna la vlan 8 al puerto
spanning-tree portfast	Habilita el puerto con PortFast y protección BPDU
no shutdown	Habilita la Interfaz
exit	salida

Fuente: Autoría Propia.

3.5 Verify PC to PC connectivity.

From PC1, verify IPv4 and IPv6 connectivity to PC2.

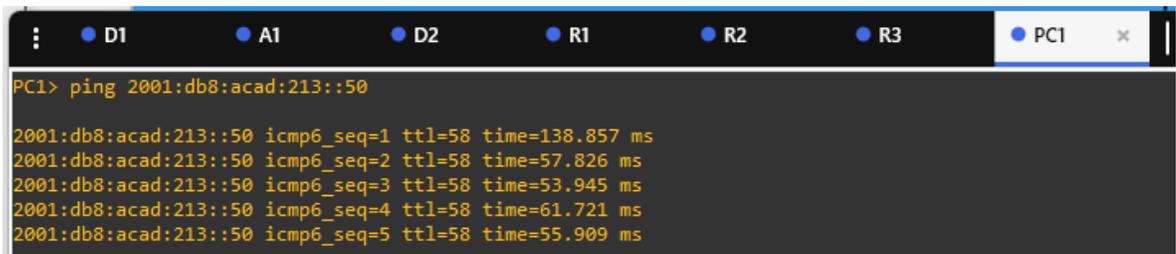
Figura 17. Ping PC1 - PC2 IPv4



```
ping 10.0.213.40
84 bytes from 10.0.213.40 icmp_seq=1 ttl=61 time=98.266 ms
84 bytes from 10.0.213.40 icmp_seq=2 ttl=61 time=58.297 ms
84 bytes from 10.0.213.40 icmp_seq=3 ttl=61 time=70.327 ms
84 bytes from 10.0.213.40 icmp_seq=4 ttl=61 time=86.453 ms
84 bytes from 10.0.213.40 icmp_seq=5 ttl=61 time=54.333 ms
PC1>
```

Fuente: Escenario de Emulación GNS3.

Figura 18. Ping PC1 - PC2 IPv6

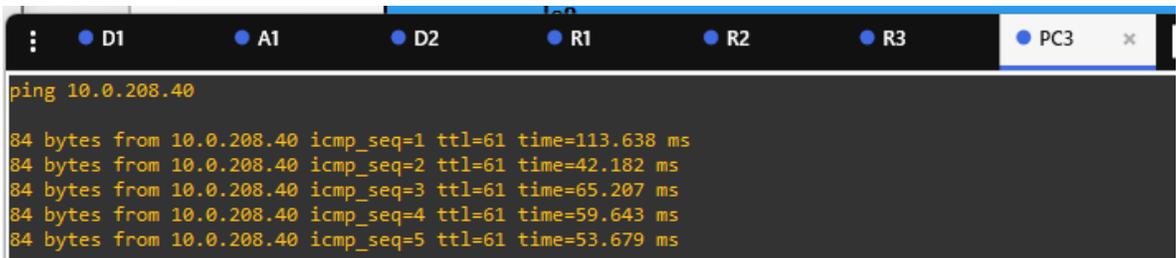


```
PC1> ping 2001:db8:acad:213::50
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=138.857 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=57.826 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=53.945 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=61.721 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=55.909 ms
```

Fuente: Escenario de Emulación GNS3.

From PC3, verify IPv4 and IPv6 connectivity to PC4.

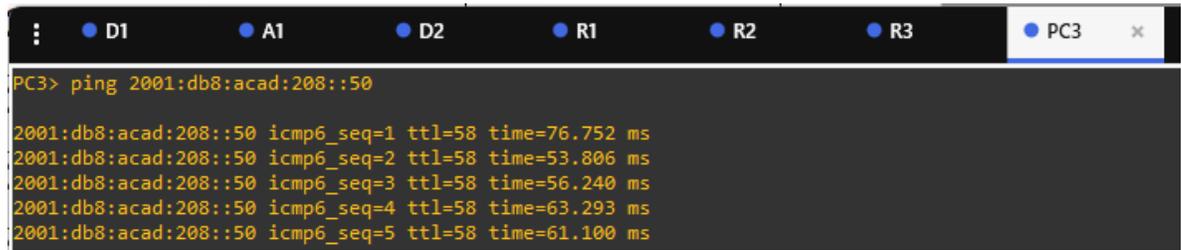
Figura 19. Ping PC3 - PC4 IPv4



```
ping 10.0.208.40
84 bytes from 10.0.208.40 icmp_seq=1 ttl=61 time=113.638 ms
84 bytes from 10.0.208.40 icmp_seq=2 ttl=61 time=42.182 ms
84 bytes from 10.0.208.40 icmp_seq=3 ttl=61 time=65.207 ms
84 bytes from 10.0.208.40 icmp_seq=4 ttl=61 time=59.643 ms
84 bytes from 10.0.208.40 icmp_seq=5 ttl=61 time=53.679 ms
```

Fuente: Escenario de Emulación GNS3.

Figura 20. Ping PC3 - PC4 IPv6



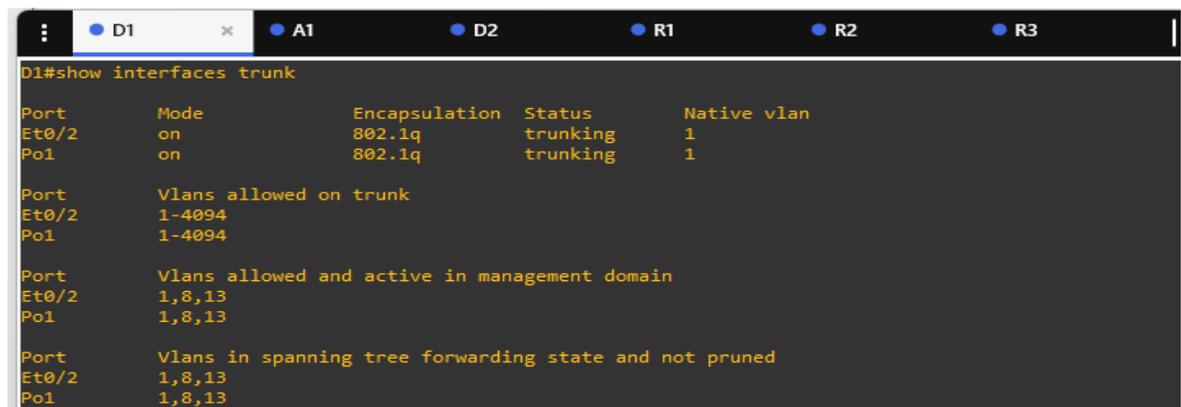
```
PC3> ping 2001:db8:acad:208::50
2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=76.752 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=53.806 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=56.240 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=63.293 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=61.100 ms
```

Fuente: Escenario de Emulación GNS3

Comandos de verificación L2 Network:

D1# show interfaces trunk:

Figura 21. Comando Verificación Interfaces Trunk en D1



```
D1#show interfaces trunk

Port      Mode           Encapsulation  Status        Native vlan
Et0/2     on             802.1q         trunking      1
Po1       on             802.1q         trunking      1

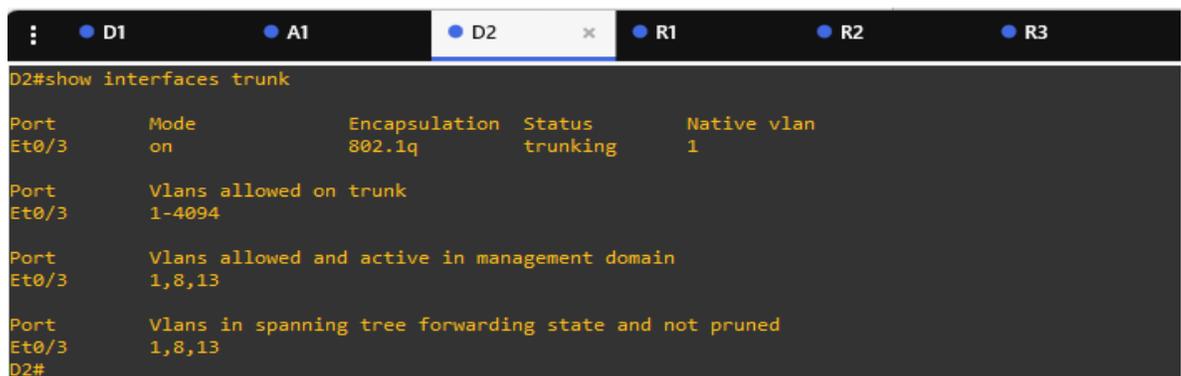
Port      Vlans allowed on trunk
Et0/2     1-4094
Po1       1-4094

Port      Vlans allowed and active in management domain
Et0/2     1,8,13
Po1       1,8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/2     1,8,13
Po1       1,8,13
```

Fuente: Escenario de Emulacion GNS3

Figura 22. Verificacion Interfaces Trunk en D2



```
D2#show interfaces trunk

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

Port      Vlans allowed on trunk
Et0/3     1-4094

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

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

Fuente: Escenario de Emulación GNS3

Figura 23. Verificación Etherchannel en D1

```
D1#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  S - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

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

       A - formed by Auto LAG

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

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

Fuente: Escenario de Emulación GNS3

PARTE 4. Configurar Seguridad

En esta parte se realizará la configuración de varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tabla 24. Tareas de configuración de seguridad.

Task#	Task	Specification
4.1	On all devices, secure privileged EXE mode.	Configure an enable secret as follows: <ul style="list-style-type: none"> • Algorithm type: SCRYPT • Password: camilobecerra402
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: camilobecerra402
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

Fuente: Guía de Actividades escenario CCNP

4.1 On all devices, secure privileged EXE mode.

Tabla 25. Configuración Algoritmo de encriptado

SWITCH D1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
enable algorithm-type SCRYPT secret camilobecerra402	Habilita el cifrado Scrypt y la contraseña
exit	salida

SWITCH D2	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
enable algorithm-type SCRYPT secret camilobecerra402	Habilita el cifrado Scrypt y la contraseña
exit	salida
SWITCH A1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
enable algorithm-type SCRYPT secret camilobecerra402	Habilita el cifrado Scrypt y la contraseña
exit	salida
Debido a la compatibilidad de los componentes en R1, R2 y R3 se realiza la siguiente configuración con el comando Service Password-Encryption.	
ROUTER R1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
Service password-encryption	Habilita el cifrado de contraseñas
Enable secret camilobecerra402	proporciona Mayor Nivel de seguridad
exit	salida
ROUTER R2	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
Service password-encryption	Habilita el cifrado de contraseñas
Enable secret camilobecerra402	proporciona Mayor Nivel de seguridad
exit	salida
ROUTER R3	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
Service password-encryption	Habilita el cifrado de contraseñas

Enable secret camilobecerra402	proporciona Mayor Nivel de seguridad
exit	salida

Fuente: autoría Propia

4.2 On all devices, create a local user account.

Tabla 26. Creación de cuenta de Usuario Local

ROUTER R1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
Username admin secret 0 camilobecerra402	Indica el nombre de usuario
Username admin privilege 15 secret camilobecerra402	Usuario nivel Privilegio
exit	salida
ROUTER R2	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
Username admin secret 0 camilobecerra402	Indica el nombre de usuario
Username admin privilege 15 secret camilobecerra402	Usuario nivel Privilegio
exit	salida
ROUTER R3	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
Username admin secret 0 camilobecerra402	Indica el nombre de usuario
Username admin privilege 15 secret camilobecerra402	Usuario nivel Privilegio
exit	salida
SWITCH D1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar

configure terminal	Habilita la configuración en el dispositivo
username admin privilege 15 algorithm-type SCRYPT secret camilobecerra402	Indica el nombre de usuario, el nivel de privilegios 15 y la encriptación de la contraseña camilobecerra402
exit	Salida
SWITCH D2	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
username admin privilege 15 algorithm-type SCRYPT secret camilobecerra402	Indica el nombre de usuario, el nivel de privilegios 15 y la encriptación de la contraseña camilobecerra402
exit	salida
SWITCH A1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
username admin privilege 15 algorithm-type SCRYPT secret camilobecerra402	Indica el nombre de usuario, el nivel de privilegios 15 y la encriptación de la contraseña camilobecerra402
exit	salida

Fuente: autoría Propia

4.3 On all devices, enable AAA and enable AAA authentication.

Tabla 27. configuración AAA y su autenticación

ROUTER R1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
aaa new-model	habilita las listas para métodos de autenticación
aaa authentication login default local	autenticación predeterminada AAA para inicio de sesión

username admin password camilobecerra402	Usuario Admin y contraseña camilobecerra402
end	final
ROUTER R2	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
aaa new-model	habilita las listas para métodos de autenticación
aaa authentication login default local	autenticación predeterminada AAA para inicio de sesión
username admin password camilobecerra402	Usuario Admin y contraseña camilobecerra402
end	final
ROUTER R3	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
aaa new-model	habilita las listas para métodos de autenticación
aaa authentication login default local	autenticación predeterminada AAA para inicio de sesión
username admin password camilobecerra402	Usuario Admin y contraseña camilobecerra402
end	final
SWITCH D1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
aaa new-model	habilita las listas para métodos de autenticación
aaa authentication login default local	autenticación predeterminada AAA para inicio de sesión
username admin password camilobecerra402	Usuario Admin y contraseña camilobecerra402
end	final
SWITCH D2	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
aaa new-model	habilita las listas para métodos de autenticación

aaa authentication login default local	autenticación predeterminada AAA para inicio de sesión
username admin password camilobecerra402	Usuario Admin y contraseña camilobecerra402
end	final
SWITCH A1	
CODIGO	DESCRIPCION
enable	Habilita el dispositivo a configurar
configure terminal	Habilita la configuración en el dispositivo
aaa new-model	habilita las listas para métodos de autenticación
aaa authentication login default local	autenticación predeterminada AAA para inicio de sesión
username admin password camilobecerra402	Usuario Admin y contraseña camilobecerra402
end	final

Fuente: autoría Propia.

Verificación de configuración username y AAA

Comando: show run | include aaa|username

Figura 24. Username y autenticación AAA en R1

```

R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$ZJmF$Akn9rWXXUo4nf8orH7zhA.
R1#

```

Fuente: Escenario de emulación GNS3

Figura 25. Username y autenticación AAA en R2

```

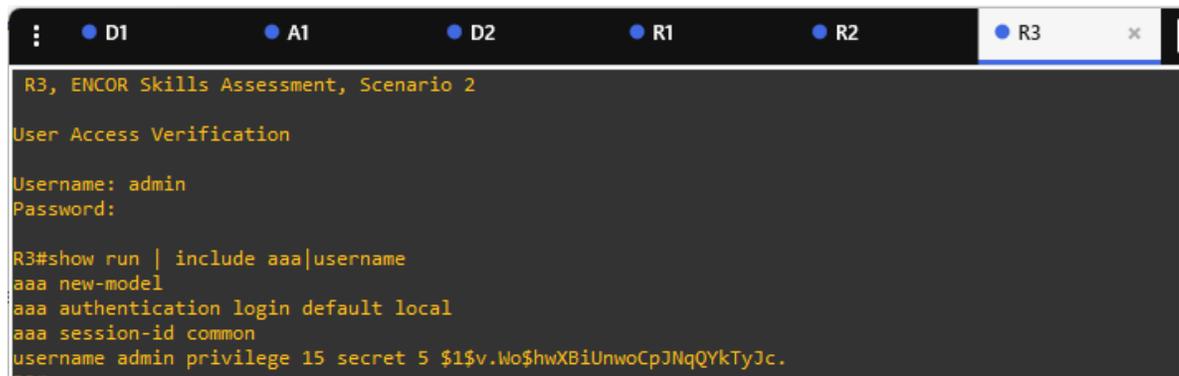
Username: admin
Password:

R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$HE1r$jHtN78HogGBs1UIJdzT/1.
R2#

```

Fuente: Escenario de emulación GNS3

Figura 26. Username y autenticación AAA en R3



```
R3, ENCOR Skills Assessment, Scenario 2
User Access Verification
Username: admin
Password:

R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$v.Wo$hWXBiUnwoCpJNqQYkTyJc.
```

Fuente: Escenario de emulación GNS3

Figura 27. Username y autenticación AAA en D1



```
*Apr 22 15:50:44.539: %SYS-5-CONFIG_I: Configured from console by admin on console
D1#show run | include aaa|username
username admin privilege 15 secret 9 $9$a993TyeXSiNBa4$0mcRfdE9Q5aKTmwlhQT2THgjSdw8iqQ0jxm0MMGBZ7U
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
```

Fuente: Escenario de emulación GNS3

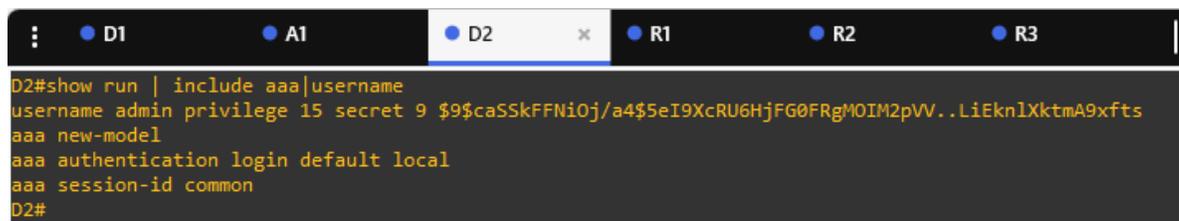
Figura 28. Username y autenticación AAA en A1



```
A1#show run | include aaa|username
username admin privilege 15 secret 9 $9$updwDTCUQKqGqiq$uZ6vnbY8xbDHKwinP1D/R9C1XKEfGPHpo90/kYhvR7c
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```

Fuente: Escenario de emulación GNS3

Figura 29. Username y autenticación AAA en D2



```
D2#show run | include aaa|username
username admin privilege 15 secret 9 $9$caSSkFFNi0j/a4$5eI9XcRU6HjFG0FRgMOIM2pVW..LiEkn1XktmA9xfts
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```

Fuente: Escenario de emulación GNS3

CONCLUSIONES

El entorno presentado posibilita el crecimiento y manejo de capacidades en la implementación de la estructura de la red, y también en la aplicación de los comandos precisos para la configuración de cada aparato con el objetivo de conseguir el apropiado desempeño de la red, siguiendo los requerimientos establecidos. Para ello, se utilizarán configuraciones multi-VRF, lo que permitirá la creación de dos redes separadas completamente, conocidas como “Usuarios Especiales” y “Usuarios Generales”.

Durante la configuración de la red, se pudo comprobar que la topología de la red y las configuraciones fueron exitosas sin ningún problema. Este es un aspecto positivo ya que los dos grupos creados ahora son completamente independientes y no hay comunicación entre ellos, tal como se esperaba.

La segmentación de la red demostró la importancia de las VLAN, ya que permitieron dividir la red sin necesidad de crear subredes. Además, se evidenció que es esencial realizar el proceso de encapsulamiento dot1q para garantizar que la información no pase de una VLAN a otra y mantener la independencia entre los grupos Especiales y Generales.

Durante la configuración, se utilizó la herramienta GNS3, que resultó ser adecuada debido a su utilidad, eficacia y entorno interactivo y completo para ingresar los comandos en cada dispositivo y realizar las verificaciones de conexión correspondientes. Los resultados fueron satisfactorios y permitieron poner en práctica los conocimientos adquiridos.

BIBLIOGRAFÍA

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

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

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

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

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

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

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

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

UNAD (2020). Configuración de Switches y Routers [OVA]. <https://1drv.ms/u/s!AmIJYei-NT1lhqL9QChD1m9EuGqC>