

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DIEGO ZAMIR LIBERATO TAFUR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIRIA - ECBTI
INGENIERA ELECTRÓNICA
IBAGUE
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DIEGO ZAMIR LIBERATO TAFUR

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

TUTORA:
ING. MARITZA FARLEY MONDRAGON GUZMAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIRIA - ECBTI
INGENIERA ELECTRÓNICA
IBAGUE
2023

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado

Ibagué 12 de mayo de 2023

Especial dedicatoria a mi madre
y hermanos (una familia llena de
ingenio).

AGRADECIMIENTOS

Agradezco a la Universidad y a todo su cuerpo de tutores por el acompañamiento brindado durante toda mi formación académica, por otra parte, quiero agradecer a mis familiares, amigos y allegados que me acompañaron durante el proceso formativo. Agradecimiento especial al semillero de investigación SIART por permitirme formar parte de esta familia dándome conocimiento aplicado. Es un orgullo formarme en esta institución como un profesional íntegro y capacitado para el mercado laboral.

CONTENIDO

	Pág.
AGRADECIMIENTOS.....	5
CONTENIDO	6
LISTA DE TABLAS	8
LISTA DE FIGURAS	9
GLOSARIO	10
RESUMEN.....	11
ABSTRACT.....	12
1. INTRODUCCIÓN	13
2. ESCENARIO PROPUESTO Y TOPOLOGIA DE RED.....	14
3. PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE CADA DISPOSITIVO Y EL DIRECCIONAMIENTO DE LAS INTERFACES....	15
3.1. Paso 1: Cablee la red como se muestra en la topología.....	16
3.2. Paso 2: Configure los ajustes básicos para cada dispositivo.	16
4. PARTE 2: CONFIGURAR VRF Y RUTAS ESTÁTICAS.	22
4.1.Tarea 2.1 Configuración VRF-Lite y VRFs en R1, R2 y R3, como se muestra en la topología del diagrama.....	23
4.2.Tarea 2.2. En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior	24
4.3.Tarea 2.3. En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.	30
4.4.Tarea 2.4. Verificación de la conectividad en cada VRF	33
5. PARTE 3: CONFIGURAR CAPA 2.	34
5.1.Tarea 3.1. Deshabilitar todas las interfaces en D1, D2 y A1.....	35
5.2. Tarea 3.2. Configuración en D1 y D2 para los enlaces troncales a R1 y R3.	35
5.3.Tarea 3.3. Configuración de EtherChannel En D1 y A1	36
5.4.Tarea 3.4. Configuración de puertos de acceso para PC1, PC2, PC3 y PC4 en D1, D2 y A1	37
5.5.Tarea 3.5. Verificación de la conectividad de PC a PC.	39
6. PARTE 4: CONFIGURAR SEGURIDAD	41

6.1. Tarea 4.1. Configuración de seguridad privilegiada en modo EXE en todos los dispositivos.	41
6.2.Tarea 4.2. Crear una cuenta de usuario local en todos los dispositivos.	42
CONCLUSIONES	45
BIBLIOGRAFÍA.....	46

LISTA DE TABLAS

	Pag.
Tabla 1. Tabla de direccionamiento	15
Tabla 2. Lista de tareas Parte 2	22
Tabla 3. Lista de tareas Parte 3	34
Tabla 4. Lista de tareas Parte 4	41

LISTA DE FIGURAS

	Pág.
Figura 1. Escenario 1	14
Figura 2. Cableado de la topología de red en GNS3	16
Figura 3. Comando Show vlan brief en D1, D2 y A1	19
Figura 4. Comando show en PC1, PC2, PC3 y PC4	21
Figura 5. Comando show run vrf en R1, R2 y R3	24
Figura 6. Comando show ip vrf interface en R1, R2 y R3	32
Figura 7. Comando show run inc route en R1, R2 y R3	32
Figura 8. Ping IPV4 desde R1 a vrf General-Users 10.0.208.7	33
Figura 9. Ping IPV6 desde R1 a vrf General-Users 2001:db8:acad:208::1	33
Figura 10. Ping desde R1 a vrf Special-Users 10.0.213.7	33
Figura 11. Ping desde R1 a vrf Special-Users 2001:db8:acad:213::1	33
Figura 12. Comando show interface trunk en D1	38
Figura 13. Comando show etherchannel summary en D1	38
Figura 14. Comando show run interface en las interfaces configuradas en D1	39
Figura 15. Ping IPV4 e IPV6 de PC3 a PC4	39
Figura 16. Ping IPV4 e IPV6 de PC3 a PC4	40
Figura 17. Ping de PC1 a PC3 y ping de PC2 a PC4	40
Figura 18. Comando show run include aaa username en todos los dispositivos	44

GLOSARIO

ENLACE TRONCAL: Un enlace troncal es un enlace físico y lógico de punto a punto entre dos dispositivos que permite facilitar la intercomunicación entre VLANs ya que solo utiliza un solo enlace.

GATEWAY: la puerta de enlace es un nodo de comunicación que permite la comunicación de dos redes que trabajan con protocolos diferentes.

HOST: Un host es un dispositivo conectado a una red el cual puede ser un punto de inicio, nodo de comunicación o dispositivo final, su función es brindar y consumir datos además de permitir comunicación entre otros dispositivos en la red.

ROUTER: Un enrutador es un dispositivo que permite la comunicación entre varias redes, ya que, gestiona el tráfico de información recibiendo los paquetes y reenviándolos de manera ordenada a una red específica de destino.

SWITCH: Un conmutador es un dispositivo que permite la comunicación entre varios dispositivos creando redes locales (LAN)

VRF: (Virtual Routing and Forwarding) es un tipo de tecnología para los Routers IP la cual segmenta lógicamente el dispositivo, esto permite que múltiples tablas de enrutamiento existan en el mismo router y trabajen de manera simultánea.

VLAN: Una red de área local virtual es un segmento lógico dentro de una red que permite agrupar dispositivos y segmentar el flujo de datos por medio de subredes.

RESUMEN

La prueba de habilidades prácticas CCNP se divide en cuatro partes. Estas partes se desarrollaron mediante el entorno de simulación GNS3 donde se aplicaron varias técnicas de enrutamiento, direccionamiento y configuración de dispositivos CISCO. El principal objetivo de esta prueba fue realizar la configuración adecuada de tres Routers, tres Switchs y cuatro PCs haciendo uso de diferentes enlaces, VRFs, VLANs, interfaces y sub-interfaces para lograr segmentar la comunicación de manera oportuna entre los dispositivos. Por otra parte, se aplicaron protocolos de encriptación a los dispositivos lo cual permite una seguridad en las redes configuradas. Gracias a esta prueba práctica y al uso de este simulador se logró tener un gran acercamiento a un entorno real dando solución a problemas de comunicación recurrentes en la industria.

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

ABSTRACT

The CCNP practical skills test is divided into four parts. These parts were developed using the GNS3 simulation environment where various CISCO device routing, addressing and configuration techniques were applied. The main objective of this test was to carry out the proper configuration of three Routers, three Switches and four PCs using different links, VRFs, VLANs, interfaces and sub-interfaces in order to segment the communication in a timely manner between the devices. On the other hand, encryption protocols were applied to the devices, which allows security in the configured networks. Thanks to this practical test and the use of this simulator, it was possible to have a great approach to a real environment, solving recurring communication problems in the industry.

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

1. INTRODUCCIÓN

Actualmente las redes de comunicación son muy importantes debido a que el mundo se encuentra cada vez más conectado, en la cotidianidad se puede observar que las redes tienen aplicaciones en muchos lugares como lo son centros de salud, universidades, hoteles, empresas etc. Por este motivo esta rama de la ingeniería es actualmente muy demanda por el mercado laboral mundial.

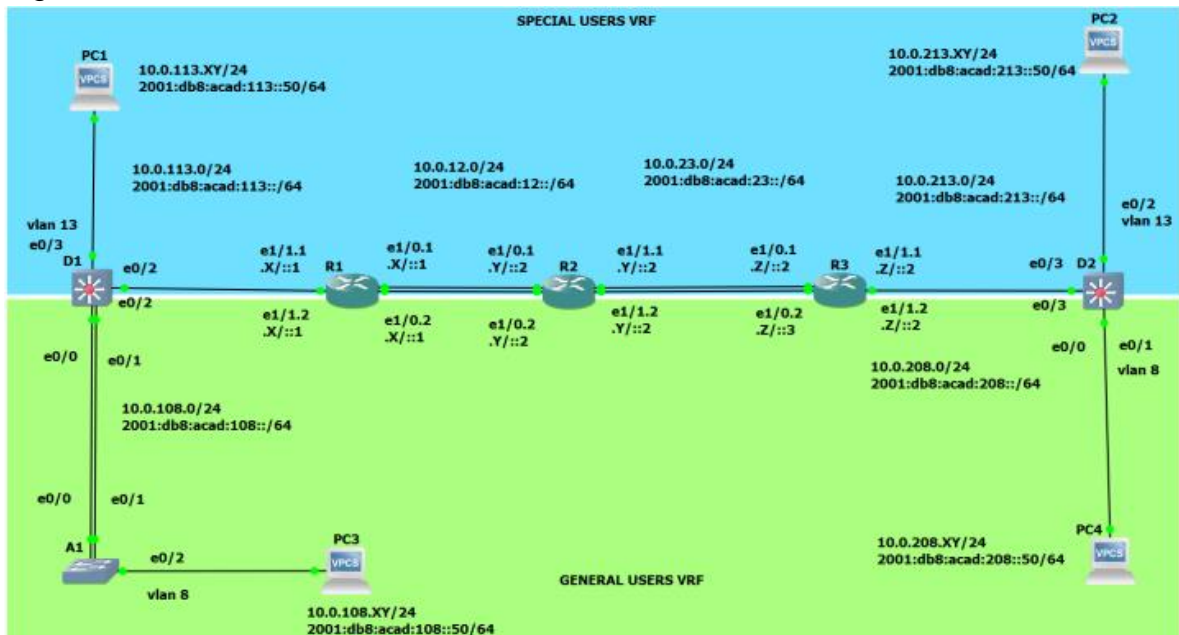
En este documento se encuentra el desarrollo de la prueba de habilidades prácticas CCNP del diplomado de profundización CCNP de la universidad nacional abierta y a distancia UNAD. En esta práctica se realizó haciendo uso del simulador GNS3 junto con una máquina virtual en virtual box con el objetivo de simular los dispositivos y tener un acercamiento detallado a los dispositivos. La práctica se divide en 4 partes. La parte numero 1 consiste en construir la red en el simulador, configurar los ajustes básicos de cada dispositivo, activar los protocolos de IPV4 e IPV6, crear las VLAN y el direccionamiento de las interfaces. La parte número 2 consiste en configurar las VRFs y rutas estáticas donde se enfoca en la configuración de los Routers. La parte número 3 consiste en la configuración de la capa 2 donde se enfoca en la configuración de los Switchs, los enlaces troncales y las VLANs. Para finalizar la parte 4 consiste en establecer parámetros de seguridad en todos los dispositivos configurados.

Esta configuración se realiza con la finalidad de crear dos grupos de usuarios (usuarios generales y usuarios especiales) cada grupo es asignado a una VRF la cual permite la comunicación exclusiva entre los dispositivos de un grupo en específico e impide la comunicación entre dispositivos de VRF diferente. A lo largo del desarrollo de la práctica se verifica las configuraciones mediante comandos como ping, traceroute, show ip route, entre otros. Realizar este tipo de configuración es de gran ayuda ya que permite que se usen menos dispositivos y la red sea más eficiente.

2. ESCENARIO PROPUESTO Y TOPOLOGIA DE RED

En esta evaluación de habilidades, se pretende 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.

Figura 1. Escenario 1



Fuente. Prueba de habilidades CISCO CCNP

3. PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE CADA DISPOSITIVO Y EL DIRECCIONAMIENTO DE LAS INTERFACES

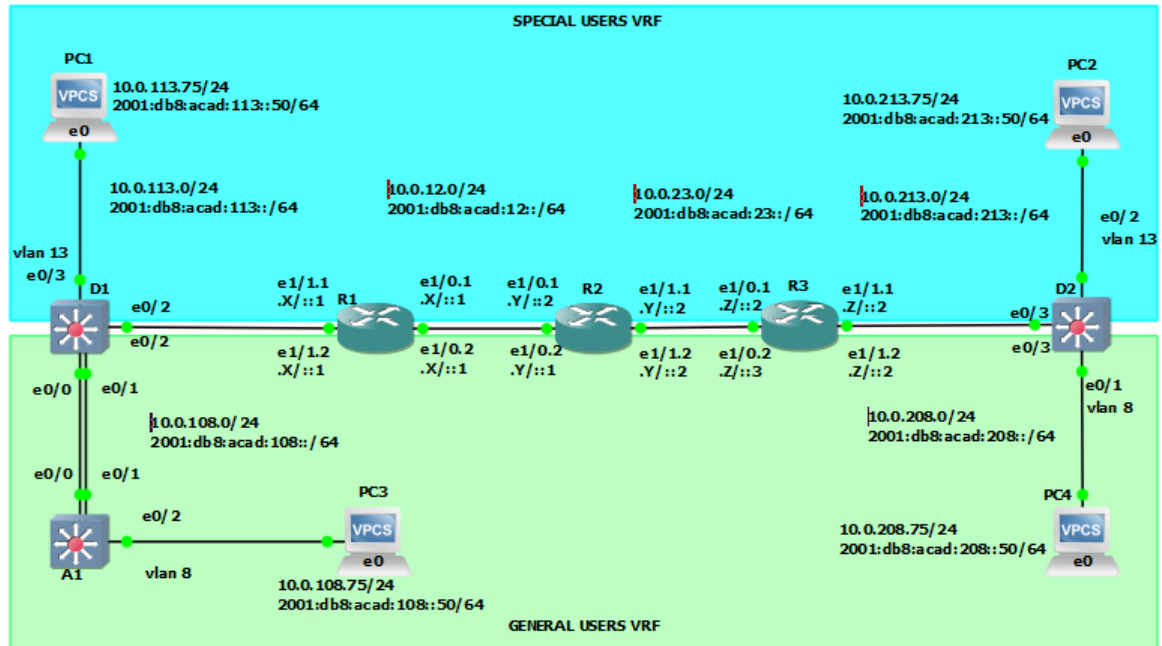
Tabla 1. Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.7/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.7/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.7/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.7/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.5/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.5/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.5/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.5/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.7/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.7/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.7/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.7/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.75/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.75/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.75/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.75/24	2001:db8:acad:208::50/64	EUI-64

Fuente. Prueba de habilidades CISCO CCNP

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

Figura 2. Cableado de la topología de red en GNS3



Fuente. Autoría Propia simulador GNS3.

3.2. Paso 2: Configure los ajustes básicos para cada dispositivo.

Se aplicó la siguiente configuración a cada dispositivo de la red

Router R1

Enable	Ingreso al modo privilegiado
Config terminal	Ingreso al modo de configuración del router
hostname R1	Asignación del nombre al dispositivo
ipv6 unicast-routing	Habilitación del routing en IPV6
no ip domain lookup	Desactivación de la búsqueda DNS
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #	Configuración de banner MOTD
line con 0	Configuración de consola 0
exec-timeout 0 0	Tiempo de espera inactivo de 0 min VTU
logging synchronous	Sincronización de la salida de información
exit	Salir de la configuración línea de consola 0

Enable
Config terminal
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills
Assessment, Scenario 2 #
line con 0
exec-timeout 0 0

logging synchronous

exit

Router R2

Ingreso al modo privilegiado
Ingreso al modo de configuración del router
Asignación del nombre al dispositivo
Habilitación del routing en IPV6
Desactivación de la búsqueda DNS

Configuración de banner MOTD

Configuración de consola 0
Tiempo de espera inactivo de 0 min
VTY
Sincronización de la salida de información
Salir de la configuración línea de consola 0

Enable
Config terminal
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills
Assessment, Scenario 2 #
line con 0
exec-timeout 0 0

logging synchronous

exit

Router R3

Ingreso al modo privilegiado
Ingreso al modo de configuración del router
Asignación del nombre al dispositivo
Habilitación del routing en IPV6
Desactivación de la búsqueda DNS

Configuración de banner MOTD

Configuración de consola 0
Tiempo de espera inactivo de 0 min
VTY
Sincronización de la salida de información
Salir de la configuración línea de consola 0

Enable
Config terminal
hostname D1
ipv6 unicast-routing
no ip domain lookup

Switch D1

Ingreso al modo privilegiado
Ingreso al modo de configuración del router
Asignación del nombre al dispositivo
Habilitación del routing en IPV6
Desactivación de la búsqueda DNS

```
banner motd # D1, ENCOR Skills
Assessment, Scenario 2 #
line con 0
exec-timeout 0 0

logging synchronous

exit

vlan 8
name General-Users
exit
vlan 13
name Special-Users
exit
```

Configuración de banner MOTD

Configuración de consola 0
Tiempo de espera inactivo de 0 min
VTY

Sincronización de la salida de información

Salir de la configuración línea de consola 0

Configuración de la VLAN 8
Asignación de nombre a VLAN

Salir de la configuración de la VLAN 8

Configuración de la VLAN 13
Asignación de nombre a VLAN

Salir de la configuración de la VLAN 13

```
Enable

Config terminal

hostname D2
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills
Assessment, Scenario 2 #
line con 0
exec-timeout 0 0

logging synchronous

exit

vlan 8
name General-Users
exit
vlan 13
name Special-Users
exit
```

Switch D2

Ingreso al modo privilegiado

Ingreso al modo de configuración del router

Asignación del nombre al dispositivo

Habilitación del routing en IPV6

Desactivación de la búsqueda DNS

Configuración de banner MOTD

Configuración de consola 0
Tiempo de espera inactivo de 0 min
VTY

Sincronización de la salida de información

Salir de la configuración línea de consola 0

Configuración de la VLAN 8
Asignación de nombre a VLAN

Salir de la configuración de la VLAN 8

Configuración de la VLAN 13
Asignación de nombre a VLAN

Salir de la configuración de la VLAN 13

```
Enable

Config terminal
```

Switch A1

Ingreso al modo privilegiado

Ingreso al modo de configuración del router

```

hostname A1
ipv6 unicast-routing
no ip domain lookup
banner motd # A1, ENCOR Skills
Assessment, Scenario 2 #
line con 0
exec-timeout 0 0

logging synchronous

exit

vlan 8
name General-Users
exit

```

Asignación del nombre al dispositivo
Habilitación del routing en IPV6
Desactivación de la búsqueda DNS
Configuración de banner MOTD
Configuración de consola 0
Tiempo de espera inactivo de 0 min
VTY
Sincronización de la salida de información
Salir de la configuración línea de consola 0
Configuración de la VLAN 8
Asignación de nombre a VLAN 8
Salir de la configuración de la VLAN 8

Figura 3. Comando Show vlan brief en D1, D2 y A1

```

D1# show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Et0/2, Et0/3, Et1/0, Et1/1
                                           Et1/2, Et1/3, Et2/0, Et2/1
                                           Et2/2, Et2/3, Et3/0, Et3/1
                                           Et3/2, Et3/3
8    General-Users          active
13   Special-Users          active
1002 fddi-default            act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default        act/unsup
D1#
6:38 p. m.
9/04/2023

D2#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Et0/0, Et0/1, Et0/2, Et0/3
                                           Et1/0, Et1/1, Et1/2, Et1/3
                                           Et2/0, Et2/1, Et2/2, Et2/3
                                           Et3/0, Et3/1, Et3/2, Et3/3
8    General-Users          active
13   Special-Users          active
1002 fddi-default            act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default        act/unsup
D2#
6:39 p. m.
9/04/2023

A1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Et0/2, Et0/3, Et1/0, Et1/1
                                           Et1/2, Et1/3, Et2/0, Et2/1
                                           Et2/2, Et2/3, Et3/0, Et3/1
                                           Et3/2, Et3/3
8    General-Users          active
1002 fddi-default            act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default        act/unsup
A1#
6:40 p. m.
9/04/2023

```

Fuente. Autoría Propia simulador GNS3.

Se guardan las configuraciones de cada dispositivo con las siguientes configuraciones en cada dispositivo R1, R2, R3, D1, D2 y A1

erase nvram:	Borrado del archivo de configuración de la NVRAM
copy running-config startup-config	Guarda la configuración de los dispositivos en la NVRAM

Se configura los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento.

Se utilizan los siguientes comandos en las terminales de cada PC

	<u>PC1</u>
ip 10.0.113.75/24 10.0.113.7	Configuración de la IPV4 y de la puerta de enlace
Ip 2001:db8:acad:113::50/64	Configuración de la IPV6
Save	Guardado de las configuraciones

	<u>PC2</u>
ip 10.0.213.75/24 10.0.213.7	Configuración de la IPV4 y de la puerta de enlace
Ip 2001:db8:acad:213::50/64	Configuración de la IPV6
Save	Guardado de las configuraciones

	<u>PC3</u>
ip 10.0.108.75/24 10.0.108.7	Configuración de la IPV4 y de la puerta de enlace
Ip 2001:db8:acad:108::50/64	Configuración de la IPV6
Save	Guardado de las configuraciones

	<u>PC4</u>
ip 10.0.208.75/24 10.0.208.7	Configuración de la IPV4 y de la puerta de enlace
Ip 2001:db8:acad:208::50/64	Configuración de la IPV6
Save	Guardado de las configuraciones

Se ejecuta el comando show en cada uno de los PC para validar la configuración.

Figura 4. Comando show en PC1, PC2, PC3 y PC4

```
PC1> show
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC1      10.0.113.75/24  10.0.113.7   00:50:79:66:68:00  10004  127.0.0.1:10005
          fe80::250:79ff:fe66:6800/64
          2001:db8:acad:113::50/64

PC2> show
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC2      10.0.213.75/24  10.0.213.7   00:50:79:66:68:01  10006  127.0.0.1:10007
          fe80::250:79ff:fe66:6801/64
          2001:db8:acad:213::50/64

PC3> show
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC3      10.0.108.75/24  10.0.108.7   00:50:79:66:68:03  10010  127.0.0.1:10011
          fe80::250:79ff:fe66:6803/64
          2001:db8:acad:108::50/64

PC4> show
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC4      10.0.208.75/24  10.0.208.7   00:50:79:66:68:02  10008  127.0.0.1:10009
          fe80::250:79ff:fe66:6802/64
          2001:db8:acad:208::50/64
```

Fuente. Autoría Propia simulador GNS3.

4. PARTE 2: CONFIGURAR VRF Y RUTAS ESTÁTICAS.

En esta parte se configura 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 debe de hacer ping a R3 en cada VRF.

Tabla 2. Lista de tareas Parte 2

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 10.0.208.7 • ping vrf General-Users 2001:db8:acad:208::1 • ping vrf Special-Users 10.0.213.7 • ping vrf Special-Users 2001:db8:acad:213::1

Fuente. Prueba de habilidades CISCO CCNP

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

Se configuran en cada Router las dos VRF con los protocolos IPV4 e IPV6 activados.

	<u>R1</u>
Enable	Ingreso al modo privilegiado
Config terminal	Ingreso al modo de configuración del router
vrf definition General-Users	Crea una nueva VRF con nombre General-Users
address-family ipv4	Activa el protocolo IPV4 para esta VRF
address-family ipv6	Activa el protocolo IPV6 para esta VRF
Exit	Salida de la configuración de la VRF
vrf definition Special-Users	Crea una nueva VRF con nombre Special-Users
address-family ipv4	Activa el protocolo IPV4 para esta VRF
address-family ipv6	Activa el protocolo IPV6 para esta VRF
End	Salida del modo de configuración del router

	<u>R2</u>
Enable	Ingreso al modo privilegiado
Config terminal	Ingreso al modo de configuración del router
vrf definition General-Users	Crea una nueva VRF con nombre General-Users
address-family ipv4	Activa el protocolo IPV4 para esta VRF
address-family ipv6	Activa el protocolo IPV6 para esta VRF
Exit	Salida de la configuración de la VRF
vrf definition Special-Users	Crea una nueva VRF con nombre Special-Users
address-family ipv4	Activa el protocolo IPV4 para esta VRF
address-family ipv6	Activa el protocolo IPV6 para esta VRF
End	Salida del modo de configuración del router

	<u>R3</u>
Enable	Ingreso al modo privilegiado
Config terminal	Ingreso al modo de configuración del router
vrf definition General-Users	Crea una nueva VRF con nombre

address-family ipv4	General-Users
address-family ipv6	Activa el protocolo IPV4 para esta VRF
Exit	Activa el protocolo IPV6 para esta VRF
vrf definition Special-Users	Salde de la configuración de la VRF
address-family ipv4	Crea una nueva VRF con nombre
address-family ipv6	Special-Users
End	Activa el protocolo IPV4 para esta VRF
	Activa el protocolo IPV6 para esta VRF
	Salde del modo de configuración del
	router

A continuación, se ejecuta el comando show run vrf en cada Router para verificar la configuración realizada.

Figura 5. Comando show run vrf en R1, R2 y R3

Fuente. Autoría Propia simulador GNS3.

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

Se realizan las siguientes configuraciones en los Routers R1, R2 y R3

Configuración en el Router R1

R1 configuración interfaz E1/0.1

Enable	Ingreso al modo privilegiado
Config terminal	Ingreso al modo de configuración del router

interface e1/0.1	Modo de configuración del sub interfaz E1/0.1
encapsulation dot1q 13	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 13 de la VLAN
vrf forwarding Special-Users	Asigna la sub interfaz al VRF Special-Users
ip address 10.0.12.7 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::1:1 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:12::1/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
exit	Salida de la configuración de la sub-interfaz

R1 configuración interfaz E1/0.2

interface e1/0.2	Modo de configuración del sub interfaz E1/0.2
encapsulation dot1q 8	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 8 de la VLAN
vrf forwarding General-Users	Asigna la sub interfaz al VRF General-Users
ip address 10.0.12.7 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::1:2 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:12::1/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
exit	Salida de la configuración de la sub-interfaz
Interface e1/0	Configuración del interfaz físico e1/0
No ip address	No se le asigna ninguna dirección ip dejando el interfaz de manera dinámica
No shutdown	Activación de la interfaz.

R1 configuración interfaz E1/1.1

interface e1/1.1	Modo de configuración del sub interfaz E1/1.1
encapsulation dot1q 13	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 13 de la VLAN
vrf forwarding Special-Users	Asigna la sub interfaz al VRF Special-Users
ip address 10.0.113.7 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::1:3 link-local	Asignación de link-local addresses para

	IPV6
ipv6 address 2001:db8:acad:113::1/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
exit	Salida de la configuración de la sub-interfaz
<u>R1 configuración interfaz E1/1.2</u>	
interface e1/1.2	Modo de configuración del sub interfaz E1/1.2
encapsulation dot1q 8	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 8 de la VLAN
vrf forwarding General-Users	Asigna la sub interfaz al VRF General-Users
ip address 10.0.108.7 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::1:4 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:108::1/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
exit	Salida de la configuración de la sub-interfaz
End	Salida del modo de configuración del router
Interface e1/0	Configuración del interfaz físico e1/1
No ip address	No se le asigna ninguna dirección ip dejando el interfaz de manera dinámica
No shutdown	Activación de la interfaz.

Configuración en el Router R2

R2 configuración interfaz E1/0.1

Enable	Ingreso al modo privilegiado
Config terminal	Ingreso al modo de configuración del router
interface e1/0.1	Modo de configuración del sub interfaz E1/0.1
encapsulation dot1q 13	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 13 de la VLAN
vrf forwarding Special-Users	Asigna la sub interfaz al VRF Special-Users
ip address 10.0.12.5 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::2:1 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:12::2/64	Asignación de la IPV6

no shutdown	Activación de la interfaz
exit	Salida de la configuración de la sub-interfaz
<u>R2 configuración interfaz E1/0.2</u>	
interface e1/0.2	Modo de configuración del sub interfaz E1/0.2
encapsulation dot1q 8	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 8 de la VLAN
vrf forwarding General-Users	Asigna la sub interfaz al VRF General-Users
ip address 10.0.12.5 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::2:2 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:12::2/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
Exit	Salida de la configuración de la sub-interfaz
Interface e1/0	Configuración del interfaz físico e1/0
No ip address	No se le asigna ninguna dirección ip dejando el interfaz de manera dinámica
No shutdown	Activación de la interfaz.
<u>R2 configuración interfaz E1/1.1</u>	
interface e1/1.1	Modo de configuración del sub interfaz E1/1.1
encapsulation dot1q 13	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 13 de la VLAN
vrf forwarding Special-Users	Asigna la sub interfaz al VRF Special-Users
ip address 10.0.23.5 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::2:3 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:23::2/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
Exit	Salida de la configuración de la sub-interfaz
<u>R2 configuración interfaz E1/1.2</u>	
interface e1/1.2	Modo de configuración del sub interfaz E1/1.2
encapsulation dot1q 8	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 8 de la VLAN

vrf forwarding General-Users	Asigna la sub interfaz al VRF General-Users
ip address 10.0.23.5 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::2:4 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:23::2/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
Exit	Salida de la configuración de la sub-interfaz
Interface e1/1	Configuración del interfaz físico e1/1
No ip address	No se le asigna ninguna dirección ip dejando el interfaz de manera dinámica
No shutdown	Activación de la interfaz.
End	Salida del modo de configuración del router

Configuración en el Router R3

R3 configuración interfaz E1/0.1

Enable	Ingreso al modo privilegiado
Config terminal	Ingreso al modo de configuración del router
interface e1/0.1	Modo de configuración del sub interfaz E1/0.1
encapsulation dot1q 13	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 13 de la VLAN
vrf forwarding Special-Users	Asigna la sub interfaz al VRF Special-Users
ip address 10.0.23.7 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::3:1 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:23::3/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
Exit	Salida de la configuración de la sub-interfaz

R3 configuración interfaz E1/0.2

interface e1/0.2	Modo de configuración del sub interfaz E1/0.2
encapsulation dot1q 8	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 8 de la VLAN
vrf forwarding General-Users	Asigna la sub interfaz al VRF General-

ip address 10.0.23.7 255.255.255.0	Users Asignación de la IPV4
ipv6 address fe80::3:2 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:23::3/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
Exit	Salida de la configuración de la sub-interfaz
Interface e1/0	Configuración del interfaz físico e1/0
No ip address	No se le asigna ninguna dirección ip dejando el interfaz de manera dinámica
No shutdown	Activación de la interfaz.

R3 configuración interfaz E1/1.1

interface e1/1.1	Modo de configuración del sub interfaz E1/1.1
encapsulation dot1q 13	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 13 de la VLAN
vrf forwarding Special-Users	Asigna la sub interfaz al VRF Special-Users
ip address 10.0.213.7 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::3:3 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:213::1/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
Exit	Salida de la configuración de la sub-interfaz

R3 configuración interfaz E1/1.2

interface e1/1.2	Modo de configuración del sub interfaz E1/1.2
encapsulation dot1q 8	Se usa el encapsulamiento IEEE802.1Q para la sub interfaz seleccionada con el id 8 de la VLAN
vrf forwarding General-Users	Asigna la sub interfaz al VRF General-Users
ip address 10.0.208.7 255.255.255.0	Asignación de la IPV4
ipv6 address fe80::3:4 link-local	Asignación de link-local addresses para IPV6
ipv6 address 2001:db8:acad:208::1/64	Asignación de la IPV6
no shutdown	Activación de la interfaz
Exit	Salida de la configuración de la sub-interfaz
Interface e1/1	Configuración del interfaz físico e1/1

No ip address	No se le asigna ninguna dirección ip dejando el interfaz de manera dinámica
No shutdown	Activación de la interfaz.
End	Salida del modo de configuración del router

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

Se ejecutan los siguientes comandos en cada uno de los Routers

	<u>R1</u>
Config terminal	Ingreso al modo de configuración
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.5	Configuración Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.5	Configuración Ruta estática predeterminada IPv4 para VRF General-Users
ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2	Configuración Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2	Configuración Ruta estática predeterminada IPv6 para VRF General-Users
End	Salida del modo de configuración del router
	<u>R2</u>
Config terminal	Ingreso al modo de configuración
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.7	Configuración Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.7	Configuración Ruta estática predeterminada IPv4 para VRF Special-Users.
ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1	Configuración Ruta estática predeterminada IPv6 para VRF Special-Users
ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3	Configuración Ruta estática predeterminada IPv6 para VRF Special-Users
ip route vrf General-Users 10.0.108.0	Configuración Ruta estática

255.255.255.0 10.0.12.7	predeterminada IPv4 para VRF General-Users.
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.7	Configuración Ruta estática predeterminada IPv4 para VRF General-Users.
ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1	Configuración Ruta estática predeterminada IPv6 para VRF General-Users
ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3	Configuración Ruta estática predeterminada IPv6 para VRF General-Users
End	Salida del modo de configuración del router

R3

Config terminal	Ingreso al modo de configuración
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.5	Configuración Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.5	Configuración Ruta estática predeterminada IPv4 para VRF General-Users
ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2	Configuración Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2	Configuración Ruta estática predeterminada IPv6 para VRF General-Users
End	Salida del modo de configuración del router

Verificación del direccionamiento IP Realizado en cada Router

Se usa el comando show ip vrf interface en cada router para verificar el direccionamiento ip de las VRFs

Figura 6. Comando show ip vrf interface en R1, R2 y R3

```
R1#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.7       General-Users     up
Et1/1.2        10.0.108.7      General-Users     up
Et1/0.1        10.0.12.7       Special-Users     up
Et1/1.1        10.0.113.7      Special-Users     up
R1#

R2#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.5       General-Users     up
Et1/1.2        10.0.23.5       General-Users     up
Et1/0.1        10.0.12.5       Special-Users     up
Et1/1.1        10.0.23.5       Special-Users     up
R2#

R3#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.23.7       General-Users     up
Et1/1.2        10.0.208.7      General-Users     up
Et1/0.1        10.0.23.7       Special-Users     up
Et1/1.1        10.0.213.7      Special-Users     up
R3#
```

Fuente. Autoría Propia simulador GNS3.

Verificación de las rutas estáticas en cada Router

Se usa el comando show run | inc route en cada router para verificar el direccionamiento estático.

Figura 7. Comando show run | inc route en R1, R2 y R3

```
R1#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.5
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.5
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2
R1#

R2#show run | inc route
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.7
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.7
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.7
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.7
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#

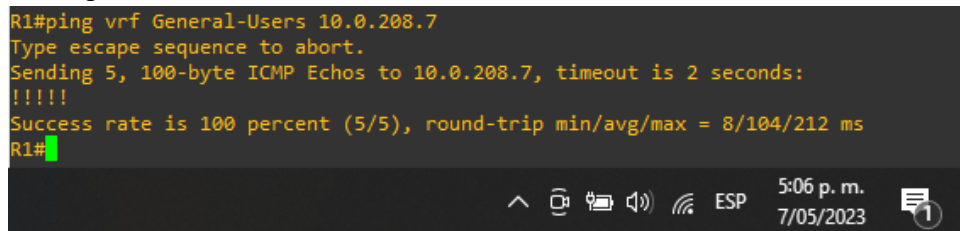
R3#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.5
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.5
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:23::2
R3#
```

Fuente. Autoría Propia simulador GNS3

4.4. Tarea 2.4. Verificación de la conectividad en cada VRF

Figura 8. Ping IPV4 desde R1 a vrf General-Users 10.0.208.7

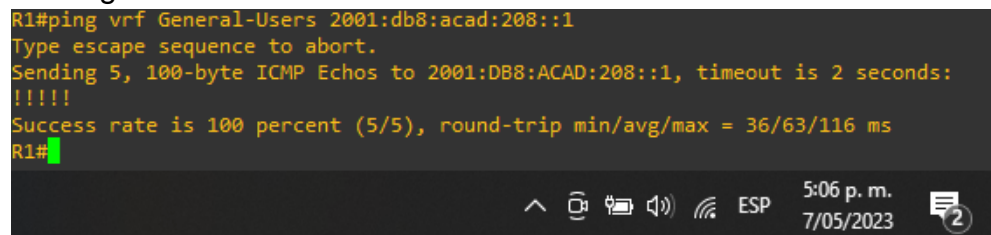
```
R1#ping vrf General-Users 10.0.208.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.7, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/104/212 ms
R1#
```



Fuente. Autoría Propia simulador GNS3.

Figura 9. Ping IPV6 desde R1 a vrf General-Users 2001:db8:acad:208::1

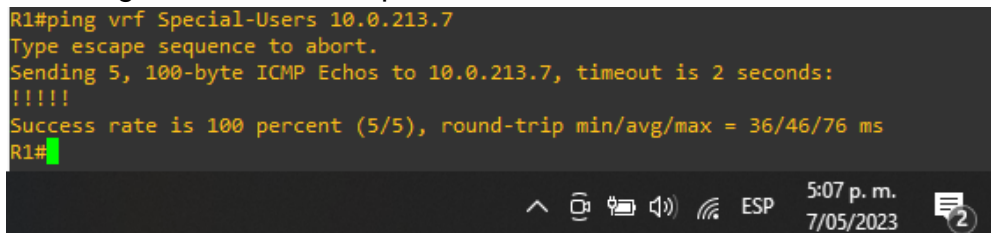
```
R1#ping vrf General-Users 2001:db8:acad:208::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/63/116 ms
R1#
```



Fuente. Autoría Propia simulador GNS3.

Figura 10. Ping desde R1 a vrf Special-Users 10.0.213.7

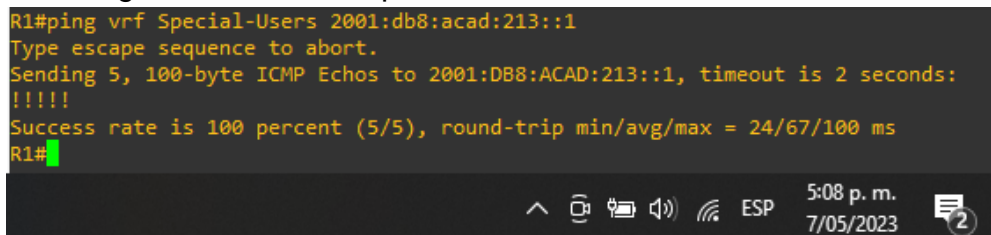
```
R1#ping vrf Special-Users 10.0.213.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.7, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/46/76 ms
R1#
```



Fuente. Autoría Propia simulador GNS3.

Figura 11. Ping desde R1 a vrf Special-Users 2001:db8:acad:213::1

```
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 = 24/67/100 ms
R1#
```



Fuente. Autoría Propia simulador GNS3.

5. PARTE 3: CONFIGURAR CAPA 2

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

Tabla 3. Lista de tareas Parte 3

Task #	Task	Specification
3.1	On D1, D2, and A1, disable all interfaces.	
3.2	On D1 and D2, configure the trunklinks to R1 and R3.	Configure and enable the e0/3 link as a trunk link.
3.3	On D1 and A1, configure the EtherChannel.	On D1, configure and enable: <ul style="list-style-type: none"> • Interface e0/0 and e0/1 • Port Channel 1 using PAgP On A1, configure enable: <ul style="list-style-type: none"> • Interface E0/0 and E0/1 • Port Channel 1 using PAgP
3.4	On D1, D2, and A1, configure accessports for PC1, PC2, PC3, and PC4.	Configure and enable the access ports as follows: <ul style="list-style-type: none"> • On D1, configure interface E0/3 as an accessport in VLAN 13 and enable Portfast. • On D2, configure interface E0/2 as an accessport in VLAN 13 and enable Portfast. • On D2, configure interface E0/1 as an accessport in VLAN 8 and enable Portfast. • On A1, configure interface E0/2 as an accessport 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. Prueba de habilidades CISCO CCNP

5.1. Tarea 3.1. Deshabilitar todas las interfaces en D1, D2 y A1.

Se ejecuta el comando shutdown en todos los interfaces de cada dispositivo para deshabilitarlos

	<u>D1</u>
Config terminal	Ingreso al modo de configuración
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Ingreso de configuración de todas las interfaces del Switch D1
shutdown	Deshabilita todas las interfaces
End	Sale del modo de configuración del router

	<u>D2</u>
Config terminal	Ingreso al modo de configuración
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Ingreso de configuración de todas las interfaces del Switch D2
shutdown	Deshabilita todas las interfaces
End	Sale del modo de configuración del router

	<u>A1</u>
Config terminal	Ingreso al modo de configuración
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Ingreso de configuración de todas las interfaces del Switch A1
shutdown	Deshabilita todas las interfaces
End	Sale del modo de configuración del router

5.2. Tarea 3.2. Configuración en D1 y D2 para los enlaces troncales a R1 y R3.

Como se observa en la *Figura 2. Cableado de la topología de red en GNS3*, los enlaces troncales se deben de realizar en D1 a través del interfaz e0/2 y en D1 a través del interfaz e0/3.

Se ejecutan los siguientes comandos en D1 y D2 para los interfaces e0/2 y e0/3 respectivamente.

	<u>D1</u>
Config terminal	Ingreso al modo de configuración
Interface e0/2	Ingreso de configuración del interfaz e0/2
Switchport trunk encapsulation dot1q	Se activa el modo de encapsulación IEEE 802.1Q para el enlace troncal.
switchport mode trunk	Configura el interfaz a modo troncal

no shutdown	Activación de la interfaz.
End	Salida del modo de configuración del router.

	<u>D2</u>
Config terminal	Ingreso al modo de configuración.
Interface e0/3	Ingreso de configuración del interfaz e0/3.
Switchport trunk encapsulation dot1q	Se activa el modo de encapsulación IEEE 802.1Q para el enlace troncal.
switchport mode trunk	Configura el interfaz a modo troncal.
no shutdown	Activación de la interfaz.
End	Salida del modo de configuración del router.

5.3. Tarea 3.3. Configuración de EtherChannel En D1 y A1

Se ejecutan los siguientes comandos en el switch D1 y A1 para configurar los EtherChannel

	<u>D1</u>
Config terminal	Ingreso al modo de configuración
Interface range e0/0-1	Ingreso de configuración del interfaz e0/0 y del interfaz e0/1.
Switchport trunk encapsulation dot1q	Se activa el modo de encapsulación IEEE 802.1Q para el enlace troncal.
switchport mode trunk	Configura el interfaz a modo troncal
channel-group 1 mode desirable	Configura los puertos agrupados en modo activo además activa el protocolo PApP para la negociación de paquetes
no shutdown	Activación de la interfaz.
End	Salida del modo de configuración del router

	<u>A1</u>
Config terminal	Ingreso al modo de configuración
Interface range e0/0-1	Ingreso de configuración del interfaz e0/0 y del interfaz e0/1.
Switchport trunk encapsulation dot1q	Se activa el modo de encapsulación IEEE 802.1Q para el enlace troncal.
switchport mode trunk	Configura el interfaz a modo troncal
channel-group 1 mode desirable	Configura los puertos agrupados en modo activo además activa el protocolo

no shutdown	PApP para la negociación de paquetes
End	Activación de la interfaz.
	Sale del modo de configuración del router

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

Se ejecutan los siguientes comandos de configuración en los switch D1 D2 y A1 para configurar los puertos correspondientes para los PCs.

	<u>D1</u>
Config terminal	Ingreso al modo de configuración
Interface e0/3	Ingreso de configuración del interfaz e0/3
switchport mode access	Configura el puerto en modo acceso
switchport access vlan 13	Asigna a la interfaz la VLAN 13
spanning-tree portfast	Habilita la protección del protocolo BPDU
no shutdown	Activación de la interfaz.
End	Sale del modo de configuración del router

	<u>D2</u>
Config terminal	Ingreso al modo de configuración
Interface e0/2	Ingreso de configuración del interfaz e0/2
switchport mode access	Configura el puerto en modo acceso
switchport access vlan 13	Asigna a la interfaz la VLAN 13
spanning-tree portfast	Habilita la protección del protocolo BPDU
no shutdown	Activación de la interfaz.
Interface e0/1	Ingreso de configuración del interfaz e0/1
switchport mode access	Configura el puerto en modo acceso
switchport access vlan 8	Asigna a la interfaz la VLAN 8
spanning-tree portfast	Habilita la protección del protocolo BPDU
no shutdown	Activación de la interfaz.
End	Sale del modo de configuración del router

A1

Config terminal

Interface e0/2

switchport mode access

switchport access vlan 8

spanning-tree portfast

no shutdown

End

Ingreso al modo de configuración
Ingreso de configuración del interfaz e0/2.

Configura el puerto en modo acceso
Asigna a la interfaz la VLAN 8
Habilita la protección del protocolo BPDU

Activación de la interfaz.

Sale del modo de configuración del router

Se ejecuta el comando show interface trunk para validar los enlaces troncales en D1

Figura 12. Comando show interface trunk en D1

```
D1#show interface 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
D1#
```

Fuente. Autoría Propia simulador GNS3.

Se ejecuta el comando show etherchannel summary para validar la configuración de los etherchannel que se conectan desde D1 a A1

Figura 13. Comando show etherchannel summary 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      f - failed to allocate aggregator

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

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

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)       PAGP        Et0/0(P)  Et0/1(P)
D1#
```

Fuente. Autoría Propia simulador GNS3.

Se ejecuta el comando show run interface seguido de cada interfaz configurada en D1 para validar las configuraciones realizadas.

Figura 14. Comando show run interface en las interfaces configuradas en D1

```
D1#show run interface e0/0
Building configuration...

Current configuration : 135 bytes
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
 channel-group 1 mode desirable
end
D1#

D1#show run interface e0/1
Building configuration...

Current configuration : 135 bytes
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
 channel-group 1 mode desirable
end
D1#

D1#show run interface e0/2
Building configuration...

Current configuration : 103 bytes
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
end
D1#

D1#show run interface e0/3
Building configuration...

Current configuration : 117 bytes
!
interface Ethernet0/3
 switchport access vlan 13
 switchport mode access
 duplex auto
 spanning-tree portfast
end
D1#
```

Fuente. Autoría Propia simulador GNS3.

5.5. Tarea 3.5. Verificación de la conectividad de PC a PC.

Se realiza el ping para de PC a PC teniendo en cuenta las direcciones IP asignadas en la tabla de direccionamiento.

Figura 15. Ping IPV4 e IPV6 de PC3 a PC4

```
PC1> ping 10.0.213.75
84 bytes from 10.0.213.75 icmp_seq=1 ttl=61 time=60.086 ms
84 bytes from 10.0.213.75 icmp_seq=2 ttl=61 time=58.648 ms
84 bytes from 10.0.213.75 icmp_seq=3 ttl=61 time=62.602 ms
84 bytes from 10.0.213.75 icmp_seq=4 ttl=61 time=46.844 ms
84 bytes from 10.0.213.75 icmp_seq=5 ttl=61 time=49.596 ms

PC1> ping 2001:db8:acad:213::50
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=104.107 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=64.148 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=64.466 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=62.220 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=63.960 ms
```

Fuente. Autoría Propia simulador GNS3.

Figura 16. Ping IPV4 e IPV6 de PC3 a PC4

```
PC3> ping 10.0.208.75
84 bytes from 10.0.208.75 icmp_seq=1 ttl=61 time=55.470 ms
84 bytes from 10.0.208.75 icmp_seq=2 ttl=61 time=59.547 ms
84 bytes from 10.0.208.75 icmp_seq=3 ttl=61 time=67.849 ms
84 bytes from 10.0.208.75 icmp_seq=4 ttl=61 time=65.679 ms
84 bytes from 10.0.208.75 icmp_seq=5 ttl=61 time=67.738 ms

PC3> ping 2001:db8:acad:208::50
2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=72.181 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=64.344 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=64.167 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=64.475 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=64.713 ms
```

Fuente. Autoría Propia simulador GNS3.

Se realiza ping de la PC1 a la PC3 y de la PC2 a la PC4

Figura 17. Ping de PC1 a PC3 y ping de PC2 a PC4

```
PC1> ping 10.0.108.75
*10.0.12.5 icmp_seq=1 ttl=254 time=31.905 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.5 icmp_seq=2 ttl=254 time=28.308 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.5 icmp_seq=3 ttl=254 time=46.111 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.5 icmp_seq=4 ttl=254 time=36.734 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.5 icmp_seq=5 ttl=254 time=49.828 ms (ICMP type:3, code:1, Destination host unreachable)

PC2> ping 10.0.208.75
*10.0.23.5 icmp_seq=1 ttl=254 time=42.400 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.23.5 icmp_seq=2 ttl=254 time=42.791 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.23.5 icmp_seq=3 ttl=254 time=28.386 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.23.5 icmp_seq=4 ttl=254 time=29.112 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.23.5 icmp_seq=5 ttl=254 time=63.035 ms (ICMP type:3, code:1, Destination host unreachable)
```

Fuente. Autoría Propia simulador GNS3.

Como se puede observar no se realiza el ping adecuadamente ya que los equipos se encuentran en redes diferentes, por ese motivo el dispositivo da el mensaje de “Host de destino inalcanzable”.

6. PARTE 4: CONFIGURAR SEGURIDAD

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

Tabla 4. Lista de tareas Parte 4

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: diegoliberato757.
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: diegoliberato757.
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

Fuente. Prueba de habilidades CISCO CCNP

6.1. Tarea 4.1. Configuración de seguridad privilegiada en modo EXEC en todos los dispositivos.

Teniendo en cuenta las imágenes montadas en los dispositivos se evidencia que el comando `algorithm-type SCRYPT` no es compatible por este motivo no se usó el tipo de algoritmo SCRYPT

Config terminal	<u>R1</u>
<code>enable secret diegoliberato757</code>	Ingreso al modo de configuración Configuración de la contraseña en el dispositivo
End	Salida del modo de configuración del router
Config terminal	<u>R2</u>
<code>enable secret diegoliberato757</code>	Ingreso al modo de configuración Configuración de la contraseña en el dispositivo
End	Salida del modo de configuración del router
Config terminal	<u>R3</u>
	Ingreso al modo de configuración

enable secret diegoliberato757	Configuración de la contraseña en el dispositivo
End	Sale del modo de configuración del router
Config terminal	<u>D1</u>
enable secret diegoliberato757	Ingreso al modo de configuración
End	Configuración de la contraseña en el dispositivo
Config terminal	Sale del modo de configuración del router
enable secret diegoliberato757	<u>D2</u>
End	Ingreso al modo de configuración
Config terminal	Configuración de la contraseña en el dispositivo
enable secret diegoliberato757	Sale del modo de configuración del router
End	<u>A1</u>
Config terminal	Ingreso al modo de configuración
enable secret diegoliberato757	Configuración de la contraseña en el dispositivo
End	Sale del modo de configuración del router

6.2. Tarea 4.2. Crear una cuenta de usuario local en todos los dispositivos.

Config terminal	<u>R1</u>
username admin privilege 15	Ingreso al modo de configuración
secret diegoliberato757	Configuración del nombre de usuario
End	nivel de privilegio 15 y contraseña.
Config terminal	Sale del modo de configuración del router
username admin privilege 15	<u>R2</u>
secret diegoliberato757	Ingreso al modo de configuración
End	Configuración del nombre de usuario
Config terminal	nivel de privilegio 15 y contraseña.
username admin privilege 15	Sale del modo de configuración del router
secret diegoliberato757	<u>R3</u>
End	Ingreso al modo de configuración
Config terminal	Configuración del nombre de usuario
username admin privilege 15	nivel de privilegio 15 y contraseña.
secret diegoliberato757	Sale del modo de configuración del router
End	

Config terminal
username admin privilege 15
secret diegoliberato757
End

D1

Ingreso al modo de configuración
Configuración del nombre de usuario
nivel de privilegio 15 y contraseña.
Sale del modo de configuración del
router

Config terminal
username admin privilege 15
secret diegoliberato757
End

D2

Ingreso al modo de configuración
Configuración del nombre de usuario
nivel de privilegio 15 y contraseña.
Sale del modo de configuración del
router

Config terminal
username admin privilege 15
secret diegoliberato757
End

A1

Ingreso al modo de configuración
Configuración del nombre de usuario
nivel de privilegio 15 y contraseña.
Sale del modo de configuración del
router

6.3. Tarea 4.3. Habilite la autenticación AAA en todos los dispositivos.

Config terminal
aaa new-model
aaa authentication login default local
End

R1

Ingreso al modo de configuración
Crea una lista de autenticación local con
el sistema AAA aplicada a todas las
líneas e interfaces.
Se Activa la autenticación por default
con la base de datos local
Sale del modo de configuración del
router

Config terminal
aaa new-model
aaa authentication login default local
End

R2

Ingreso al modo de configuración
Crea una lista de autenticación local con
el sistema AAA
Se Activa la autenticación por default
con la base de datos local
Sale del modo de configuración del
router

Config terminal
aaa new-model
aaa authentication login default local

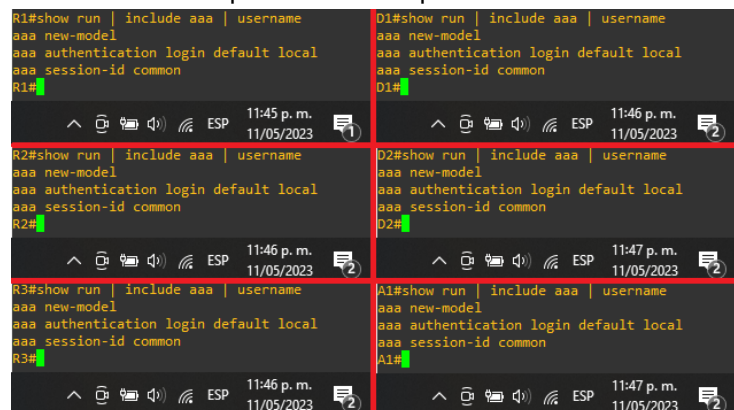
R3

Ingreso al modo de configuración
Crea una lista de autenticación local con
el sistema AAA
Se Activa la autenticación por default
con la base de datos local

End	Sale del modo de configuración del router
	<u>D1</u>
Config terminal	Ingreso al modo de configuración
aaa new-model	Crea una lista de autenticación local con el sistema AAA
aaa authentication login default local	Se Activa la autenticación por default con la base de datos local
End	Sale del modo de configuración del router
	<u>D2</u>
Config terminal	Ingreso al modo de configuración
aaa new-model	Crea una lista de autenticación local con el sistema AAA
aaa authentication login default local	Se Activa la autenticación por default con la base de datos local
End	Sale del modo de configuración del router
	<u>A1</u>
Config terminal	Ingreso al modo de configuración
aaa new-model	Crea una lista de autenticación local con el sistema AAA
aaa authentication login default local	Se Activa la autenticación por default con la base de datos local
End	Sale del modo de configuración del router

Se ejecuta el comando show run | include aaa | username en cada dispositivo para verificar la configuración de seguridad.

Figura 18. Comando show run | include aaa | username en todos los dispositivos



Fuente. Autoría Propia simulador GNS3

CONCLUSIONES

Las configuraciones iniciales en los dispositivos como router y/o switch, son fundamentales ya que en estas configuraciones se determinan los parámetros con los que la red va a trabajar, además se puede evidenciar que estos dispositivos tienen un archivo de configuración inicial por defecto en la NVRAM, ese archivo se debe de reemplazar, ya que, si no se realiza este procedimiento, los dispositivos no conservan las configuraciones cuando se enciendan nuevamente.

El uso de VRFs, VLANs y Enlaces troncales es muy eficiente en un entorno real, ya que evitan el uso de más dispositivos y por lo tanto de más enlaces punto a punto, lo cual se traduce a un menor costo en la implementación de un proyecto. Gracias a el uso de esta tecnología, con menos dispositivos se puede realizar un direccionamiento complejo, permitiendo seccionar el flujo de datos a los dispositivos finales (Host).

Al finalizar la práctica se puede observar la importancia de la seguridad informática en este entorno, si no se aplica una adecuada configuración de protocolos de seguridad la red sería vulnerable a ataques o a des-configuración por personal no autorizado. Por este motivo en la práctica se activa el protocolo AAA (Autenticación, Autorización, Contabilidad) para poder ingresar a realizar cambios en los dispositivos.

BIBLIOGRAFÍA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. 2020

TEARE, D., VACHON B., GRAZIANI, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101.
<https://1drv.ms/b/s!AmIJYeiNT1InMfy2rhPZHwEoW>