

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

SERGIO ALEXANDER PEREZ HENAO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
MEDELLÍN
2022**

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

SERGIO ALEXANDER PEREZ HENAO

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

**DIRECTOR:
Msc. HÉCTOR JULIAN PARRA MOGOLLÓN**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
MEDELLÍN
2022**

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Medellín, 26 de Junio de 2022

AGRADECIMIENTOS

Quiero agradecerle principalmente a Dios por bendecirme todos los días y darme vida y salud para seguir adelante, por guiarme por el camino correcto y cuidarme durante todo mi tiempo de vida estudiantil, por ser mi apoyo y fortaleza en esos momentos de debilidad en los cuales quise dejar todo, gracias Dios por nunca abandonarme y siempre estar ahí para darme nuevas fuerzas.

Agradecerles a mi padre y a mi madre, por ser los principales creyentes en mi sueño, por confiar y creer en que yo si sería capaz de lograrlo, gracias a esa inspiración era que podía seguir adelante cada día sin importar lo difícil de la situación, por los consejos que me dieron en momentos difíciles y por los principios que me enseñaron desde niño ya que gracias a eso, soy el hombre que soy y espero ser un gran profesional

CONTENIDO

	Pág.
INTRODUCCIÓN	10
DESARROLLO	11
1. ESCENARIO	11
1.1 PARTE 1: CONSTRUCCIÓN DE LA RED Y CONFIGURACIONES BÁSICAS.	12
1.1.1 PASO 1: LA RED SE ELABORA EN EL SIMULADOR GRAFICO GNS3	12
1.1.2 PASO 2: CONFIGURACIÓN BÁSICA	13
1.1.3 PASO 3: GUARDAR LAS CONFIGURACIONES	17
1.1.4 PASO 4: ASIGNACIÓN LAS DIRECCIONES A LOS PCs	17
1.2 PARTE 2: CONFIGURACIÓN VRF Y DEL ENRUTAMIENTO ESTÁTICO	19
1.2.1 PASO 1: CONFIGURACIÓN VRF	19
1.2.2 PASO 2: CONFIGURACIÓN DE LAS INTERFACES	20
1.2.3 PASO 3: CONFIGURACIÓN DE LAS RUTAS ESTÁTICAS	23
1.2.4 PASO 4: VERIFICACIÓN DE CONEXIÓN DESDE R1 A R3	24
1.3 PARTE 3: CONFIGURACIÓN DE CAPA 2	25
1.3.1 PASO 1: DES HABILITACIÓN DE LOS PUERTOS	25
1.3.2 PASO 2: CONFIGURACIÓN TRONCAL	26
1.3.1 PASO 3: CONFIGURACIÓN ETHERCHANNEL	26
1.3.2 PASO 4: CONFIGURACIÓN DE LOS PUERTOS DE ACCESO	27
1.3.3 PASO 5: VERIFICACIÓN DE CONEXIÓN DE PC A PC	29
1.4 PARTE 4: CONFIGURACIÓN DE SEGURIDAD	31
1.4.1 PASO 1: CONFIGURACIÓN Y HABILITACIÓN DE LA ARQUITECTURA AAA	31
CONCLUSIONES	33
REFERENCIAS	34

LISTA DE TABLAS

	Pág.
Tabla 1. Tabla de direccionamiento	11
Tabla 2. Configuración básica del Router R1	13
Tabla 3. Configuración básica del Router R2	13
Tabla 4. Configuración básica del Router R3	14
Tabla 5. Configuración básica del Switch D1	14
Tabla 6. Configuración básica del Switch D2	15
Tabla 7. Configuración básica del Switch A1	16
Tabla 8. Configuración VRF-Lite de los Router	19
Tabla 9. Configuración de las interfaces del Router R1	20
Tabla 10. Configuración de las interfaces del Router R2	21
Tabla 11. Configuración de las interfaces del Router R3	22
Tabla 12. Des habilitación de los puertos del Switch D1	25
Tabla 13. Des habilitación de los puertos del Switch D2	25
Tabla 14. Des habilitación de los puertos del Switch A1	25
Tabla 15. Configuración de enlace troncal del Switch D1 a R1	26
Tabla 16. Configuración de enlace troncal del Switch D2 a R3	26
Tabla 17. Configuración de EtherChannel en el Switch D1	26
Tabla 18. Configuración de EtherChannel en el Switch A1	27
Tabla 19. Configuración de puertos de acceso del Switch D1	27
Tabla 20. Configuración de puertos de acceso del Switch A1	28
Tabla 21. Configuración de puertos de acceso del Switch D2	28

LISTA DE FIGURAS

	Pág.
Figura 1. Topología del escenario.....	11
Figura 2. Elaboración de la topología en GNS3.....	12
Figura 3. Asignación de dirección IPv4 e IPv6 en PC1	18
Figura 4. Asignación de dirección IPv4 e IPv6 en PC2.....	18
Figura 5. Asignación de dirección IPv4 e IPv6 en PC3.....	18
Figura 6. Asignación de dirección IPv4 e IPv6 en PC4.....	19
Figura 7. Verificación de conexión desde R1 a R3	24
Figura 8. Verificación de conexión de PC1 a PC2	29
Figura 9. Verificación de conexión de PC2 a PC1	30
Figura 10. Verificación de conexión de PC3 a PC4	30
Figura 11. Verificación de conexión de PC4 a PC3	31

GLOSARIO

DIRECCION IP: Es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa “protocolo de Internet”, conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

ENRUTAMIENTO ESTÁTICO: Es aquel en el que se configura manualmente cada uno de los routers que forman la red. Hay que acceder a cada router, configurarlo individualmente y enseñarle cada una de las rutas existentes.

GATEWAY: Es el enlace que conecta dos ordenadores a Internet.

GNS3: Es un software utilizado para emular, configurar, probar y solucionar problemas de redes virtuales y reales.

INTERFAZ: La conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro.

PROTOCOLO: Un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

RED: Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información.

ROUTER: Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI.

SWITCH: Dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection).

VRF: (Virtual Routing and Forwarding, enrutamiento virtual y reenvío). Es una tecnología que permite que un enrutador ejecute más de una tabla de enrutamiento simultáneamente.

RESUMEN

El desarrollo del presente informe consiste en la construcción y configuración en tiempo real de una red. Inicialmente, se construye la red y se configuran los parámetros básicos de los dispositivos y el direccionamiento de las interfaces y de los host, se continúa con la configuración VRF y el enrutamiento estático. Posteriormente se configura la capa 2, en la cual los switches podrán soportar la conectividad con los dispositivos finales y así por último se procederá a configurar varios mecanismos de seguridad en los dispositivos de la topología junto con varias funciones de administración de red. De esta manera se hace posible ejecutar las acciones de control aprendidas sobre las redes de una forma más eficiente.

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

ABSTRACT

The development of this report consists of the construction and configuration in real time of a network. Initially, the network is built and the basic parameters of the devices and the addressing of the interfaces and hosts are configured, VRF configuration and static routing are continued. Layer 2 is then configured, in which the switches will be able to support connectivity with the end devices and so finally will proceed to configure several security mechanisms on devices in the topology along with various network management roles. In this way it becomes possible to execute the control actions learned on the networks in a more efficient way.

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

INTRODUCCIÓN

Nos encontramos en una era digital; donde pequeñas, medianas y grandes empresas se están actualizando implementando múltiples redes, y es entonces allí cuando es indispensable aprender a administrar, crear, diseñar y gestionar sistemas en tecnología de la información y las telecomunicaciones.

El presente documento está basado en el diseño y configuración de un escenario LAN/WAN manejando herramientas de simulación en el software GNS3, con el fin de realizar un análisis sobre el comportamiento de múltiples configuraciones, se evalúa el desempeño de los routers y de los switches con direccionamiento IPv4 e IPv6 mediante el uso de comandos de administración avanzados para protocolos de enrutamiento; asimismo se diseña e implementan soluciones de red escalables, mediante el uso de los principios y conmutación de paquetes en ambientes LAN y WAN.

Debido a que el método convencional de aprender de redes LAN/WAN puede resultar tedioso y riesgoso para el personal capacitado en la realización de esta labor, y a las circunstancias actuales del mundo entero, se ve en esto una oportunidad para aprender, diseñar y construir redes adquiriendo las habilidades y destrezas propias de un profesional en su labor cotidiana.

DESARROLLO

1. ESCENARIO

El presente escenario se fundamenta en completar la configuración Multi-VRF de la red, teniendo en cuenta que se divide en "Usuarios generales" y "Usuarios especiales". Una vez finalizada la configuración se procede a dar accesibilidad completa de un extremo a otro, considerando que los dos grupos previamente mencionados no se comunican entre sí. Por último se procede a verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según lo requerido para la red.

Figura 1. Topología del escenario. Fuente: Prueba de habilidades CCNP

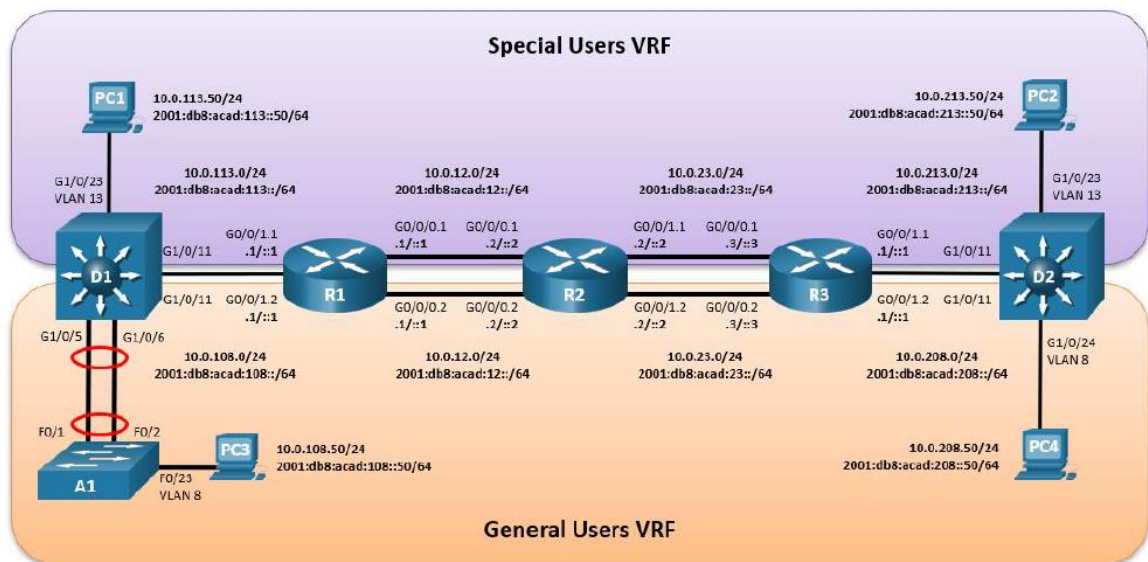


Tabla 1. Tabla de direccionamiento. Fuente: Prueba de habilidades CCNP

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	fe0/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	fe0/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	fe0/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	fe0/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4

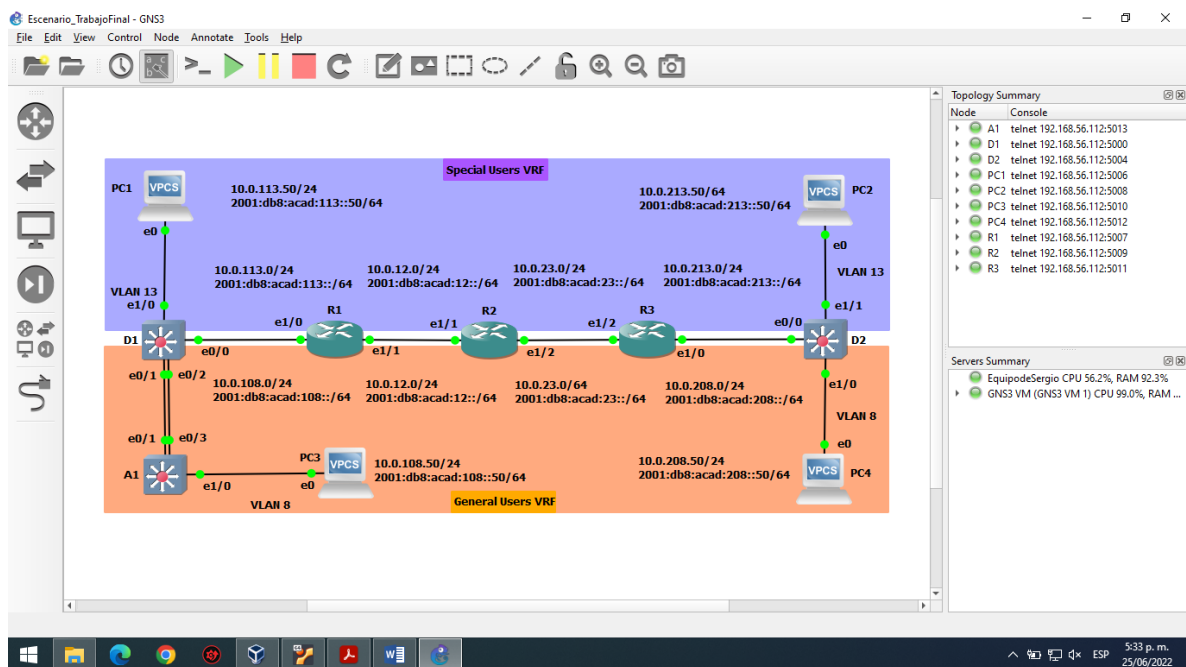
R2	fe0/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	fe0/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	fe0/1.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	fe0/1.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	fe0/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	fe0/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	fe0/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	fe0/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

1.1 PARTE 1: CONSTRUCCIÓN DE LA RED Y CONFIGURACIONES BÁSICAS.

1.1.1 PASO 1: LA RED SE ELABORA EN EL SIMULADOR GRAFICO GNS3

Como se observa en la Figura 2, está compuesta por: 3 Routers, 2 Switches, 1 Switch, y 4 PCs, además se tiene en cuenta que los dispositivos se conectan por medio de cables Ethernet.

Figura 2. Elaboración de la topología en GNS3. Fuente: Propia



1.1.2 PASO 2: CONFIGURACIÓN BÁSICA

Para cada dispositivo se realiza en el modo de configuración global de cada uno de ellos aplicando los comandos que se aprecian en las siguientes tablas.

Tabla 2. Configuración básica del Router R1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
hostname R1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración

Tabla 3. Configuración básica del Router R2. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
hostname R1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # R2, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router

line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración

Tabla 4. Configuración básica del Router R3. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
hostname R1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración

Tabla 5. Configuración básica del Switch D1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
hostname D1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router

no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración
vlan 8	#Crea una VLAN con un número de ID válido
name general-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado
vlan 13	#Crea una VLAN con un número de ID válido
name special-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado

Tabla 6. Configuración básica del Switch D2. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
hostname D1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola

exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración
vlan 8	#Crea una VLAN con un número de ID válido
name general-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado
vlan 13	#Crea una VLAN con un número de ID válido
name special-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado

Tabla 7. Configuración básica del Switch A1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
hostname D1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración
vlan 8	#Crea una VLAN con un número de ID válido

name general-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado
vlan 13	#Crea una VLAN con un número de ID válido
name special-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado

1.1.3 PASO 3: GUARDAR LAS CONFIGURACIONES

En cada uno de los dispositivos anteriores por último se coloca el comando running-config al archivo startup-config.

Router R1

R1#copy running-config startup-config

Router R2

R2#copy running-config startup-config

Router R3

R3#copy running-config startup-config

Switch D1

D1#copy running-config startup-config

Switch D2

D2#copy running-config startup-config

Switch A1

A1#copy running-config startup-config

1.1.4 PASO 4: ASIGNACIÓN LAS DIRECCIONES A LOS PCS

A los PC1, PC2, PC3 y PC4, de acuerdo a la Tabla 1 se les asigna la dirección IP.

PC1

ip 10.0.113.50/24 10.0.113.1

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

PC2

ip 10.0.213.50/24 10.0.213.1

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

PC3

ip 10.0.108.50/24 10.0.108.1

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

PC4

ip 10.0.208.50/24 10.0.208.1

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

Figura 3. Asignación de dirección IPv4 e IPv6 en PC1. Fuente: Propia

```
PC1> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.0.113.50/24 10.0.113.1 00:50:79:66:68:00 20020 127.0.0.1:20021
fe80::250:79ff:fe66:6800/64
2001:db8:acad:113::50/64
PC1>
```

Figura 4. Asignación de dirección IPv4 e IPv6 en PC2. Fuente: Propia

```
PC2> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.213.50/24 10.0.213.1 00:50:79:66:68:01 20022 127.0.0.1:20023
fe80::250:79ff:fe66:6801/64
2001:db8:acad:213::50/64
PC2>
```

Figura 5. Asignación de dirección IPv4 e IPv6 en PC3. Fuente: Propia

```
PC3> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.108.50/24 10.0.108.1 00:50:79:66:68:02 20026 127.0.0.1:20027
fe80::250:79ff:fe66:6802/64
2001:db8:acad:108::50/64
PC3>
```

Figura 6. Asignación de dirección IPv4 e IPv6 en PC4. Fuente: Propia

```

PC4> sh
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC4      10.0.208.50/24  10.0.208.1   00:50:79:66:68:03  20024  127.0.0.1:20025
          fe80::258:79ff:fe66:6803/64
          2001:db8:acad:208::50/64
PC4>

```

1.2 PARTE 2: CONFIGURACIÓN VRF Y DEL ENRUTAMIENTO ESTÁTICO

En esta parte se configura VRF-Lite (Virtual Routing and Forwarding) para realizar la segmentación del tráfico cuando tenemos diferentes clientes o cuando necesitamos que el tráfico de management quede aislado del resto, esta configuración se realiza en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro, para ello se aplican los pasos y comandos que se aprecian a continuación.

1.2.1 PASO 1: CONFIGURACIÓN VRF

En R1, R2 y R3, se configura VRF-Lite VRF como se muestra en el diagrama de topología de la Figura 1. La configuración de los parámetros básicos para cada dispositivo se realiza en el modo de configuración global de cada uno de ellos aplicando los comandos que se aprecian en las siguientes tablas.

Tabla 8. Configuración VRF-Lite de los Router. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
vrf definition special-users	#Crea instancia de enrutamiento
description special-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description special-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6
exit	#Sale del modo de configuración
vrf definition general-users	#Crea instancia de enrutamiento
description general-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description general-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6

1.2.2 PASO 2: CONFIGURACIÓN DE LAS INTERFACES

En R1, R2 y R3, se configuran las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento para así seguir las siguientes tablas.

Tabla 9. Configuración de las interfaces del Router R1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e1/0.1	#Ingresa a la interface Ethernet 1/0.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.113.1 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:3 link-local#	#Configura link-local
ipv6 address 2001:db8:acad:113::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0.2	#Ingresa a la interface Ethernet 1/0.2
encapsulation dot1q 8	#Se establece el tipo de encapsulación
vrf forward general-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.108.1 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:4 link-local	#Configura link-local
ipv6 address 2001:db8:acad:108::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0	#Ingresa a la interface Ethernet 1/0
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.1	#Ingresa a la interface Ethernet 1/1.1
encapsulation dot1q 13	#Se establece el tipo de encapsulación
vrf forward special-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.12.1 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:1 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.2	#Ingresa a la interface Ethernet 1/1.2
encapsulation dot1q 8	#Establece el tipo de encapsulación

vrf forward general-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.12.1 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:2 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1	#Ingresa a la interface Ethernet 1/1
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz

Tabla 10. Configuración de las interfaces del Router R2. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e1/1.1	#Ingresa a la interface Ethernet 1/1.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.12.2 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:1 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.2	#Ingresa a la interface Ethernet 1/1.2
encapsulation dot1q 8	#Se establece el tipo de encapsulación
vrf forward general-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.12.2 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:2 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1	#Ingresa a la interface Ethernet 1/1
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/2.1	#Ingresa a la interface Ethernet 1/2.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia interface a tabla de enrutamiento

ip address 10.0.23.2 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:3 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/2.2	#Ingresa a la interface Ethernet 1/2.2
encapsulation dot1q 8	#Establece el tipo de encapsulación
vrf forward general-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.23.2 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:4 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/2	#Ingresa a la interface Ethernet 1/2
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz

Tabla 11. Configuración de las interfaces del Router R3. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e1/2.1	#Ingresa a la interface Ethernet 1/2.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.23.3 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::3:1 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::3/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/2.2	#Ingresa a la interface Ethernet 1/2.2
encapsulation dot1q 8	#Se establece el tipo de encapsulación
vrf forward general-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.23.3 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::3:2 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::3/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/2	#Ingresa a la interface Ethernet 1/2

no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0.1	#Ingresa a interface Ethernet 1/0.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.213.1 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::3:3 link-local	#Configura link-local
ipv6 address 2001:db8:acad:213::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0.2	#Ingresa a la interface Ethernet 1/0.2
encapsulation dot1q 8	#Establece el tipo de encapsulación
vrf forward general-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.208.1 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::3:4 link-local	#Configura link-local
ipv6 address 2001:db8:acad:208::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0	#Ingresa a la interface Ethernet 1/0
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz

1.2.3 PASO 3: CONFIGURACIÓN DE LAS RUTAS ESTÁTICAS

En los dispositivos R1 y R3, se configuran las rutas estáticas predeterminadas que apuntan a R2, por medio de los comandos que se detallan a continuación conservando el orden:

Router R1

```
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.2
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.2
ipv6 route vrf special-users ::/0 2001:db8:acad:12::2
ipv6 route vrf general-users ::/0 2001:db8:acad:12::2
```

Router R2

```
ip route vrf general-users 10.0.108.0 255.255.255.0 10.0.12.1
ip route vrf general-users 10.0.208.0 255.255.255.0 10.0.23.3
ip route vrf special-users 10.0.113.0 255.255.255.0 10.0.12.1
ip route vrf special-users 10.0.213.0 255.255.255.0 10.0.23.3
```

```

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

```

Router R3

```

ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.23.2
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.23.2
ipv6 route vrf special-users ::/0 2001:db8:acad:23::2
ipv6 route vrf general-users ::/0 2001:db8:acad:23::2

```

1.2.4 PASO 4: VERIFICACIÓN DE CONEXIÓN DESDE R1 A R3

Se verifica la conectividad en cada VRF, desde R1 a R3, por medio del comando ping desde R1 como se muestra a continuación:

```

R1# ping vrf general-users 10.0.208.1
R1# ping vrf general-users 2001:db8:acad:208::1
R1# ping vrf special-users 10.0.213.1
R1# ping vrf special-users 2001:db8:acad:213::1

```

Figura 7.Verificación de conexión desde R1 a R3. Fuente: Propia

```

R1
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#int e1/1
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#
Building configuration...

*Jun 25 18:03:35.523: XSYS-5-CONFIG_I: Configured from console by console[OK]
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)#ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)#ipv6 route vrf special-users ::/0 2001:db8:acad:12::2
R1(config)#ipv6 route vrf general-users ::/0 2001:db8:acad:12::2
R1(config)#exit
R1#
*Jun 25 18:41:25.863: XSYS-5-CONFIG_I: Configured from console by console
R1#ping vrf general-users 10.0.208.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/18/64 ms
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 = 4/6/10 ms
R1#ping vrf special-users 10.0.213.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/11/14 ms
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 = 3/5/10 ms
R1#

```

1.3 PARTE 3: CONFIGURACIÓN DE CAPA 2

En esta parte, se configuran los Switches para soportar la conectividad con los dispositivos finales,

1.3.1 PASO 1: DES HABILITACIÓN DE LOS PUERTOS

En D1, D2 y A1, se deshabilitan todas las interfaces y se aplican los comandos que se aprecian en las siguientes tablas.

Tabla 12. Des habilitación de los puertos del Switch D1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
Interface range e0/0-3 , e1/0-3	#Ingresa al rango de interfaces de Ethernet de e0/0-3 , e1/0-3
shutdown	#Apaga la interfaz
exit	#Sale del modo de configuración

Tabla 13. Des habilitación de los puertos del Switch D2. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	#Ingresa al rango de interfaces de Ethernet de e0/0-3 , e1/0-3 , e2/0-3 , e3/0-3
shutdown	#Apaga la interfaz
exit	#Sale del modo de configuración

Tabla 14. Des habilitación de los puertos del Switch A1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface range e0/0-3, e1/0-3	#Ingresa al rango de interfaces de Ethernet de e0/0-3, e1/0-3
shutdown	#Apaga la interfaz
exit	#Sale del modo de configuración

1.3.2 PASO 2: CONFIGURACIÓN TRONCAL

Segundo en D1 y D2 se configuran los enlaces troncales a R1 y R3, por medio de los comandos que se muestran en las siguientes tablas:

Tabla 15. Configuración de enlace troncal del Switch D1 a R1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e0/0	#Ingresa a la interface de Ethernet 0/0
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport trunk allowed vlan 8,13	#Permite enlace troncal en la vlan 8 y 13
switchport mode trunk	#Modo de enlace troncal permanente
shutdown	#Apaga la interfaz
exit	#Sale del modo de configuración

Tabla 16. Configuración de enlace troncal del Switch D2 a R3. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e0/0	#Ingresa a la interface de Ethernet 0/0
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport trunk allowed vlan 8,13	#Permite enlace troncal en la vlan 8 y 13
switchport mode trunk	#Modo de enlace troncal permanente
Shutdown	#Apaga la interfaz
exit	#Sale del modo de configuración

1.3.1 PASO 3: CONFIGURACIÓN ETHERCHANNEL

Tercero en D1 y A1, se configura el EtherChannel con PAgP, por medio de los comandos que se muestran en las siguientes tablas:

Tabla 17. Configuración de EtherChannel en el Switch D1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado

configure terminal	#Cambia a modo Configuración
interface e0/1	#Ingresa a la interface de Ethernet 0/1
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e0/2	#Ingresa a la interface de Ethernet 0/2
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Tabla 18. Configuración de EtherChannel en el Switch A1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e0/1	#Ingresa a la interface de Ethernet 0/1
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e0/3	#Ingresa a la interface de Ethernet 0/3
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

1.3.2 PASO 4: CONFIGURACIÓN DE LOS PUERTOS DE ACCESO

En D1, D2 y A1 se configuran los puertos de acceso para PC1, PC2, PC3 y PC4, por medio de los comandos que se muestran en las siguientes tablas:

Tabla 19. Configuración de puertos de acceso del Switch D1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado

configure terminal	#Cambia a modo Configuración
interface e1/0	#Ingresa a la interface de Ethernet 0/1
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 13	#Asigna al puerto la VLAN 13
spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Tabla 20. Configuración de puertos de acceso del Switch A1. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e1/0	#Ingresa a la interface de Ethernet 0/1
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 13	#Asigna al puerto la VLAN 13
spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Tabla 21. Configuración de puertos de acceso del Switch D2. Fuente: Propia

Comando	Descripción
enable	#Cambia a modo privilegiado
configure terminal	#Cambia a modo Configuración
interface e1/0	#Ingresa a la interface de Ethernet 1/0
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 8	#Asigna al puerto la VLAN 8
spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1	#Ingresa a la interface de Ethernet 1/1
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 13	#Asigna al puerto la VLAN 13
spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

1.3.3 PASO 5: VERIFICACIÓN DE CONEXIÓN DE PC A PC

Se verifica la conectividad en toda la red de PC a PC, por medio del comando ping seguido de la dirección IP, como se muestra a continuación:

Verificación de conexión de PC1 a PC2

```
ping 10.0.213.50  
ping 2001:db8:acad:213::50/64
```

Verificación de conexión de PC2 a PC1

```
ping 10.0.113.50  
ping 2001:db8:acad:113::50/64
```

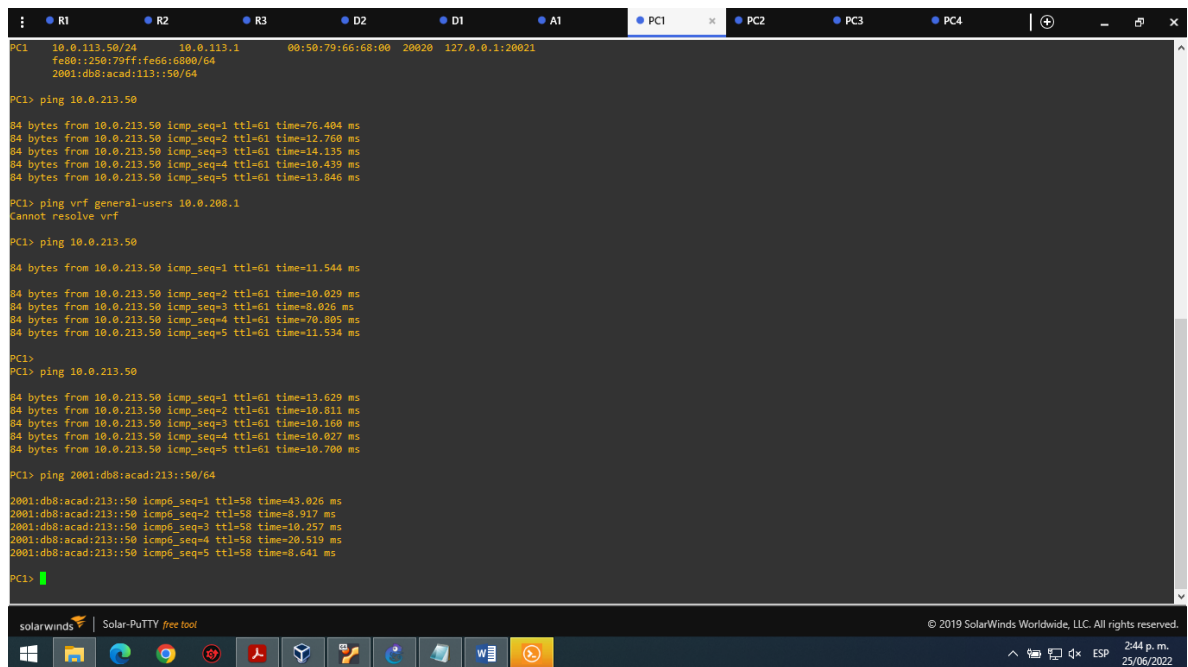
Verificación de conexión de PC3 a PC4

```
ping 10.0.208.50  
ping 2001:db8:acad:208::50/64
```

Verificación de conexión de PC4 a PC3

```
ping 10.0.108.50  
ping 2001:db8:acad:108::50/64
```

Figura 8. Verificación de conexión de PC1 a PC2. Fuente: Propia



```
PC1 10.0.113.50/24 10.0.113.1 00:50:79:66:68:00 20020 127.0.0.1:20021  
fe80::258:79ff:fe66:6800/64  
2001:db8:acad:113::50/64  
  
PC1> ping 10.0.213.50  
  
84 bytes from 10.0.213.50 icmp_seq=1 ttl=61 time=76.404 ms  
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=12.760 ms  
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=14.135 ms  
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=10.439 ms  
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=13.846 ms  
  
PC1> ping vrf general-users 10.0.208.1  
Cannot resolve vrf  
  
PC1> ping 10.0.213.50  
  
84 bytes from 10.0.213.50 icmp_seq=1 ttl=61 time=11.544 ms  
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=10.029 ms  
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=8.026 ms  
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=70.805 ms  
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=11.534 ms  
  
PC1>  
PC1> ping 10.0.213.50  
  
84 bytes from 10.0.213.50 icmp_seq=1 ttl=61 time=13.629 ms  
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=10.811 ms  
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=10.160 ms  
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=10.027 ms  
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=10.700 ms  
  
PC1> ping 2001:db8:acad:213::50/64  
  
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=43.026 ms  
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=8.917 ms  
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=10.257 ms  
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=20.519 ms  
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=8.641 ms  
  
PC1>
```

Figura 9. Verificación de conexión de PC2 a PC1. Fuente: Propia

```
Press '?' to get help.
Executing the startup fil
^

PC2> ip 10.0.213.50 255.255.255.0 10.0.213.1
Checking for duplicate address...
PC2 : 10.0.213.50 255.255.255.0 gateway 10.0.213.1

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

PC2> wr
Saving startup configuration to startup.vpc
. done

PC2> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.213.50/24 10.0.213.1 00:50:79:66:68:01 20024 127.0.0.1:20025
fe80::250:79ff:fe66:6801/64
2001:db8:acad:213::50/64

PC2> ping 10.0.113.50

84 bytes from 10.0.113.50 icmp_seq=1 ttl=61 time=89.847 ms
84 bytes from 10.0.113.50 icmp_seq=2 ttl=61 time=12.790 ms
84 bytes from 10.0.113.50 icmp_seq=3 ttl=61 time=12.023 ms
84 bytes from 10.0.113.50 icmp_seq=4 ttl=61 time=10.119 ms
84 bytes from 10.0.113.50 icmp_seq=5 ttl=61 time=15.849 ms

PC2> ping 2001:db8:acad:113::50/64

2001:db8:acad:113::50 icmp6_seq=1 ttl=58 time=13.151 ms
2001:db8:acad:113::50 icmp6_seq=2 ttl=58 time=12.698 ms
2001:db8:acad:113::50 icmp6_seq=3 ttl=58 time=17.258 ms
2001:db8:acad:113::50 icmp6_seq=4 ttl=58 time=10.784 ms
2001:db8:acad:113::50 icmp6_seq=5 ttl=58 time=12.505 ms

PC2>
```

Figura 10. Verificación de conexión de PC3 a PC4. Fuente: Propia

```
PC3> ip 10.0.108.50 255.255.255.0 10.0.108.1
Checking for duplicate address...
PC3 : 10.0.108.50 255.255.255.0 gateway 10.0.108.1

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

PC3> wr
Saving startup configuration to startup.vpc
. done

PC3> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.108.50/24 10.0.108.1 00:50:79:66:68:02 20022 127.0.0.1:20023
fe80::250:79ff:fe66:6802/64
2001:db8:acad:108::50/64

PC3> wr
Saving startup configuration to startup.vpc
. done

PC3> ping 10.0.208.50

84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=35.392 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=13.809 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=34.026 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=12.756 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=15.769 ms

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

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=111.429 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=14.459 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=12.667 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=10.299 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=21.343 ms

PC3>
```

Figura 11. Verificación de conexión de PC4 a PC3. Fuente: Propia

```
Executing the startup file
PC4> ip 10.0.208.50 255.255.255.0 10.0.208.1
Checking for duplicate address...
PC4 : 10.0.208.50 255.255.255.0 gateway 10.0.208.1

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

PC4> wr
Saving startup configuration to startup.vpc
. done

PC4> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.0.208.50/24 10.0.208.1 00:50:79:66:68:03 20026 127.0.0.1:20027
fe80::258:79ff:fe66:6803/64
2001:db8:acad:208::50/64

PC4> wr
Saving startup configuration to startup.vpc
. done

PC4> ping 10.0.108.50

84 bytes from 10.0.108.50 icmp_seq=1 ttl=61 time=15.633 ms
84 bytes from 10.0.108.50 icmp_seq=2 ttl=61 time=19.715 ms
84 bytes from 10.0.108.50 icmp_seq=3 ttl=61 time=65.507 ms
84 bytes from 10.0.108.50 icmp_seq=4 ttl=61 time=20.171 ms
84 bytes from 10.0.108.50 icmp_seq=5 ttl=61 time=51.512 ms

PC4> ping 2001:db8:acad:108::50/64

2001:db8:acad:108::50 icmp6_seq=1 ttl=58 time=28.072 ms
2001:db8:acad:108::50 icmp6_seq=2 ttl=58 time=19.901 ms
2001:db8:acad:108::50 icmp6_seq=3 ttl=58 time=18.351 ms
2001:db8:acad:108::50 icmp6_seq=4 ttl=58 time=9.551 ms
2001:db8:acad:108::50 icmp6_seq=5 ttl=58 time=10.806 ms

PC4>
```

1.4 PARTE 4: CONFIGURACIÓN DE SEGURIDAD

Esta configuración consiste en utilizar la arquitectura AAA que representa las siglas Authentication (Autenticación), Authorization (Autorización) y Accounting (Registro), esta arquitectura de seguridad aprueba la gestión de acceso al definir políticas de seguridad.

1.4.1 PASO 1: CONFIGURACIÓN Y HABILITACIÓN DE LA ARQUITECTURA AAA

En esta parte, se configuran varios mecanismos de seguridad en los dispositivos, en todos los dispositivos se configura y habilita el modo EXEC privilegiado seguro, para ello se aplican los comandos que se aprecian a continuación:

Switch D1

```
enable secret cisco12345cisco
username admin privilege 15 secret cisco12345cisco
aaa new-model
aaa authentication login default local
exit
```

Switch D2

```
enable secret cisco12345cisco
username admin privilege 15 secret cisco12345cisco
aaa new-model
aaa authentication login default local
exit
```

Switch A1

```
enable secret cisco12345cisco
username admin privilege 15 secret cisco12345cisco
aaa new-model
aaa authentication login default local
exit
```

Router R1

```
enable algorithm-type scrypt secret cisco12345cisco
username admin privilege 15 algorithm-type scrypt secret cisco12345cisco
aaa new-model
aaa authentication login default local
exit
```

Router R2

```
enable algorithm-type scrypt secret cisco12345cisco
username admin privilege 15 algorithm-type scrypt secret cisco12345cisco
aaa new-model
aaa authentication login default local
exit
```

Router R3

```
enable algorithm-type scrypt secret cisco12345cisco
username admin privilege 15 algorithm-type scrypt secret cisco12345cisco
aaa new-model
aaa authentication login default local
exit
```

CONCLUSIONES

A lo largo del desarrollo de este escenario a través del software GNS3, hemos afianzado los conocimientos y aprendido al mismo tiempo; por lo que el procedimiento y configuración de este tuvo como resultado el correcto funcionamiento y ejecución de la simulación, dando cumplimiento a lo solicitado en la guía, esto se ve reflejado en las verificaciones de conexión entre los dispositivos de la red por medio del comando ping; un comando importante para asegurar las configuraciones o detectar errores y fallas en la red a medida que se va configurando y no al final.

Asimismo la configuración inicial de cualquier dispositivo de la red tiene una importancia, ya que esta proporciona seguridad a los dispositivos y a la red. Tras el establecimiento de contraseñas, nombres y el mensaje de advertencia. Esto apoya a las configuraciones de seguridad realizadas por medio de la arquitectura AAA que permite la gestión de acceso definiendo políticas de seguridad en la red.

Además, mediante el desarrollo del escenario se logró realizar satisfactoriamente la configuración VRF; esta consiste primero en definir las distintas VRF, seguidamente asignar a cada VRF un identificador para indicar al router cómo separar las rutas y por último asociar las interfaces a las VRF y así asignar las direcciones IP, Por lo que podemos considerar que los pasos coleccionados en esta configuración pueden servir de utilidad para futuras configuraciones que aborden este tema.

Después de realizar las evaluaciones correspondientes y utilizar las configuraciones necesarias ya conocidas y mencionados con anterioridad, se concluye que la red es funcional y segura. Se sugiere apropiar más los conocimientos del uso de tecnología CISCO para estimular el funcionamiento, configuración y diseño ya que todavía queda mucho por aprender de las redes LAN/WAN.

REFERENCIAS

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). 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>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. 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). 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). 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). 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). 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>