

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

JORGE IVAN MENDIETA MUÑOZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA
DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
2022**

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

JORGE IVAN MENDIETA MUÑOZ

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

**DIRECTOR:
MSc. HÉCTOR JULIÁN PARRA MOGOLLÓN**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA
DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2022**

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 26 de junio de 2022

AGRADECIMIENTOS

Agradezco a Dios por darme la oportunidad de haber cursado la carrera como Ingeniero de Telecomunicaciones, agradezco a mi familia por darme ánimo en todo momento, a mis hijas que fueron gran motivación y se me concedió a través de los estudios realizados brindarles ejemplo que si se puede hacer las cosas que uno se propone, un agradecimiento especial a mi esposa quien ha sido apoyo constante e incondicional, también a todos y cada uno de los docentes que aportaron sus conocimientos y realizaron acompañamiento durante los diferentes procesos, de igual manera retribuyo a la Universidad Nacional Abierta y a Distancia UNAD por poner a disposición los recursos necesarios para formar profesionales y por su modelo educativo el cual permite que más personas logremos tener acceso a la educación superior.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS.....	7
LISTA DE FIGURAS	8
GLOSARIO.....	9
RESUMEN.....	10
ABSTRAC	10
INTRODUCCIÓN.....	12
DESARROLLO.....	13
CONFIGURACION INICIAL EN ROUTER R1.....	14
CONFIGURACION INICIAL EN ROUTER R2.....	15
CONFIGURACION INICIAL EN ROUTER R3.....	15
CONFIGURACION INICIAL EN SWITCH D1.....	15
CONFIGURACION INICIAL EN SWITCH D2.....	16
CONFIGURACION INICIAL EN SWITCH A1.....	16
CONFIGURACION DE CAPA 2 EN SWITCH D1.....	27
CONFIGURACION DE CAPA 2 EN SWITCH D2.....	28
CONFIGURACION DE CAPA 2 EN SWITCH D3.....	29

CONFIGURACION BASICA DE SEGURIDAD EN A1 - D1 - D2 - R1 - R2 - R3...31

CONCLUSIONES32

BIBLIOGRAFIA33

LISTA DE TABLAS

<i>Tabla 1. Direccionamiento para los dispositivos</i>	<i>19</i>
--	-----------

LISTA DE FIGURAS

<i>Ilustración 1. Escenario propuesto.....</i>	<i>13</i>
<i>Ilustración 2. Simulación del escenario propuesto</i>	<i>14</i>
<i>Ilustración 3. Comando para guardar la configuración en los dispositivos.....</i>	<i>17</i>
<i>Ilustración 4. Configuración de PC1.....</i>	<i>17</i>
<i>Ilustración 5. Configuración de PC2.....</i>	<i>18</i>
<i>Ilustración 6. Configuración de PC3.....</i>	<i>18</i>
<i>Ilustración 7. Configuración de PC4.....</i>	<i>19</i>
<i>Ilustración 8. Prueba de ping VRF R1 a R3.....</i>	<i>27</i>
<i>Ilustración 9. Prueba de ping de PC1 a PC2.....</i>	<i>30</i>
<i>Ilustración 10. Prueba de ping de PC1 a PC2.....</i>	<i>30</i>

GLOSARIO

BGP: (Border Gateway Protocol) Es un protocolo de puerta de enlace utilizado para el intercambio de información entre routers de borde de los sistemas autónomos los cuales establecen una sesión de comunicación y logran conseguir la entrega confiables de la información.

MPLS: (Multiprotocol Label Switching) Se refiere a la técnica capaz de unificar diversos tipos de datos por medio de una misma red, es un estándar IP de conmutación de paquetes. Permite al router o switch asignar la etiqueta a la tabla de enrutamiento para comunicarla con sus nodos vecinos la etiqueta es transportada en el encabezado del paquete para identificar la clase de equivalencia que es el conjunto de paquetes reenviados sobre la misma ruta a través de la red, aun cuando los destinos finales sean diferentes.

OSPF: (Open Shortest Path First) Es un protocolo de estado de enlace el cual puede detectar cambios en la topología de un sistema autónomo y que evita bucles en la red, permite también escalabilidad e interacción con MPLS.

Router: Dispositivo encargado principalmente del enrutamiento y reenvío de paquetes de datos, también incluyen temas de QoS, seguridad y administración, adicionalmente mediante estos se corrigen diferentes errores que se puedan presentar en una red.

SWITCH: Dispositivo usado para conectar los elementos de una LAN como los son computadoras, servidores, AP e impresoras con el fin de compartir los recursos principalmente en oficinas y centros de datos.

VRF: (Virtual Routing and Forwarding) Tecnología que permite a varias instancias de una tabla de enrutamiento coexistir en un mismo router y trabajar simultáneamente.

RESUMEN

Hoy en día el mundo cada vez se mueve, se comunica y avanza principalmente con el uso de la tecnología y para lograr acceso a muchas de las tecnologías actuales son fundamentales las redes de electrónicas y de telecomunicaciones, es allí donde encontramos grandes proveedores de servicios de transporte, procesamiento y almacenamiento de datos, estos se comunican entre sí y cooperan para el constante desarrollo y optimización de los recursos de las redes mediante el uso de diferentes equipos y dispositivos como los routers y los switches que son los encargados de interconectar la mayoría de las redes haciendo uso de protocolos avanzados de comunicación que permiten el aprovechamiento de los recursos de red y por consiguiente empresariales.

Cisco System es una de las compañías encargada de desarrollar varios de los protocolos de comunicación los cuales también son compatibles con tecnologías de otros fabricantes y que brindan flexibilidad y mejoramiento en cuanto a enrutamiento y conmutación de las redes.

En este trabajo implementaremos una solución a modo de laboratorio haciendo uso de uno de los protocolos que usan los ISP (Proveedores de servicios de Internet) en la actualidad como lo es VRF (Enrutamiento virtual y reenvió) que permite la creación de redes privadas virtuales separadas en un mismo router y se pueden separar para brindar las necesidades de sus diferentes clientes.

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

ABSTRAC

Today the world moves, communicates and advances mainly with the use of technology and to gain access to many of the current technologies, electronic and telecommunications networks are essential., it is there where we find great providers of transport services, data processing and storage these communicate with each other and cooperate for the constant development and optimization of network resources through the use of different equipment and devices such as routers and switches which are responsible for interconnecting most networks using advanced communication protocols that allow the use of network resources and therefore business.

Cisco System is one of the companies in charge of developing several of the communication protocols which are also compatible with technologies from other manufacturers and that provide flexibility and improvement in terms of routing and

switching networks.

In this work we will implement a solution as a laboratory using one of the protocols used by ISPs (Internet Service Providers) currently as it is VRF (Virtual Routing and Forwarding) that allows the creation of separate virtual private networks in the same router and can be separated to provide the needs of its different clients.

Palabras clave: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

El diplomado CCNP busca que los estudiantes adquiramos competencias que nos ayuden a comprender modos de operación de las redes de gran escala y convergencia, así mismo que las podamos administrar para solución de fallas, y crecimiento de estas. Para ello se deben conocer y saber aplicar los diferentes protocolos usados principalmente en escenarios corporativos como lo son STP, OSPF EIGRP y BGP.

En el siguiente trabajo se realiza la implementación de VRF-Lite con base en un escenario que plantea el uso de dos VRF lo que nos permite tener ventajas en la red debido a que podemos separar y segmentar rutas haciendo uso de un mismo router y manteniendo el tráfico de diferentes clientes en el mismo dispositivo.

La implementación es realizada en el software GNS3 el cual es una potente herramienta para la practica y diseño de redes de gran escala.

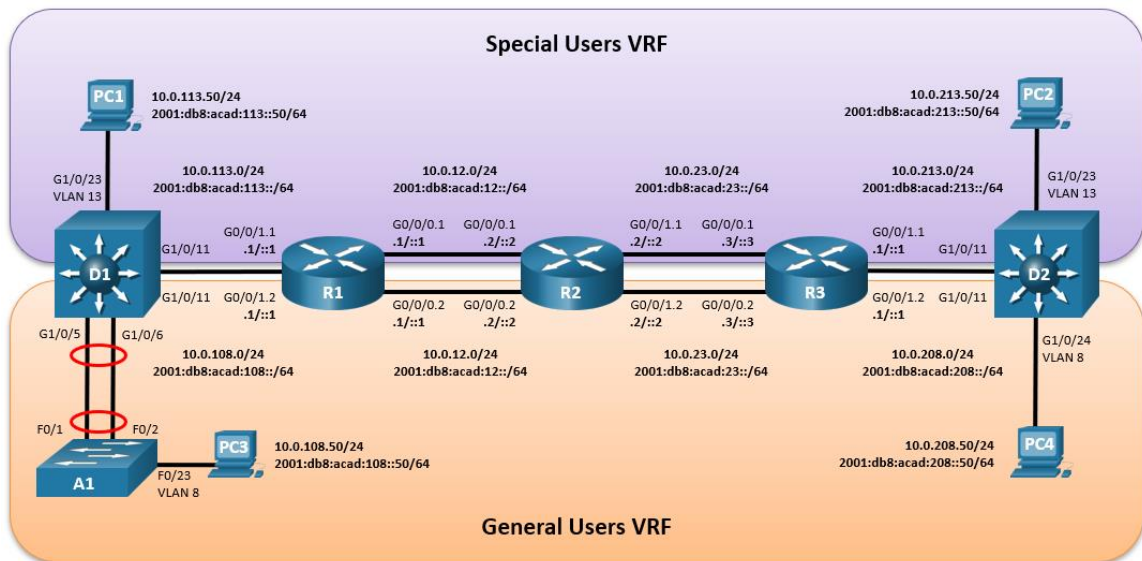
En la primera sección se construirá la topología del escenario propuesto, se realizarán las conexiones, se configuran los ajustes básicos en cada dispositivo y vrf-lite en los router confirmando su correcto funcionamiento, en la segunda sección se realizará la configuración de la capa 2 en los switch con su respectiva comprobacion y finalmente se realizan los ajustes de seguridad.

DESARROLLO

1. ESCENARIO 1

Se requiere 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.

Ilustración 1. Escenario propuesto



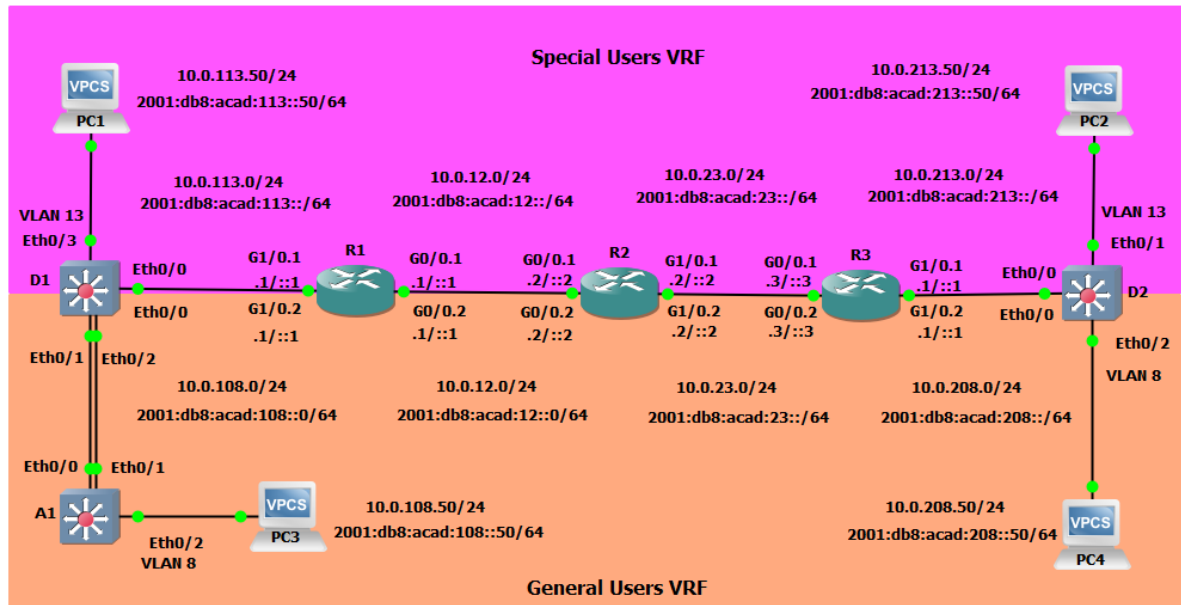
Fuente: Tomado de documento guía UNAD

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

Paso 1: Cablear la red como se muestra en la topología.

Conectar los dispositivos como se muestra en el diagrama de topología y cablee según sea necesario.

Ilustración 2. Simulación del escenario propuesto



Fuente: Elaboración propia en GNS3

Paso 2: Configure los ajustes básicos para cada dispositivo

- 1.1. Se aplican las configuraciones iniciales para los routers R1, R2, R3, los switch D1, D2, A1 según el diagrama.

CONFIGURACION INICIAL EN ROUTER R1

enable	//Ingresar en modo privilegiado
configure terminal	//Ingresar a modo de configuración
hostname R1	//Asignar nombre al router
ipv6 unicast-routing	//Habilitar el routing ipv6
no ip domain lookup	//Habilitar la traducción de nombre
line con 0	//Ingresar al modo de configuración de la línea de consola
exec-timeout 0 0	//Establecer el tiempo de espera inactivo de la sesión remota
logging synchronous	//Indicar si hay un mensaje de evento
exit	//Salir del modo actual
wr	//Guardar la configuración

CONFIGURACION INICIAL EN ROUTER R2

```
Enable //Ingresar a modo privilegiado
configure terminal //Ingresar a modo de configuración
hostname R1 //Asignar nombre al router
ipv6 unicast-routing //Habilitar el routing ipv6
no ip domain lookup //Habilitar la traducción de nombre
line con 0 //Ingresar al modo de configuración
de la linea de consola
exec-timeout 0 0 //Establecer el tiempo de espera
inactivo de la sesión remota
logging synchronous //Indicar si hay un mensaje de
evento
exit //Salir del modo actual
wr //Guardar la configuración
```

CONFIGURACION INICIAL EN ROUTER R3

```
enable //Ingresar en modo privilegiado
configure terminal //Ingresar a modo de configuración
hostname R1 //Asignar nombre al router
ipv6 unicast-routing //Habilitar el routing ipv6
no ip domain lookup //Habilitar la traducción de nombre
line con 0 //Ingresar al modo de configuración
de la linea de consola
exec-timeout 0 0 //Establecer el tiempo de espera
inactivo de la sesión remota
logging synchronous //Indicar si hay un mensaje
de evento
exit //Salir del modo actual
wr //Guardar la configuración
```

CONFIGURACION INICIAL EN SWITCH D1

```
Enable //Ingresar a modo privilegiado
configure terminal //Ingresar a modo de configuración
hostname R1 //Asignar nombre al switch
ipv6 unicast-routing //Habilitar el routing ipv6
no ip domain lookup //Habilitar la traducción de nombre
line con 0 //Ingresar al modo de
configuración de la linea de consola
exec-timeout 0 0 //Establecer el tiempo de espera
inactivo de la sesión remota
logging //Indicar si hay un mensaje de evento
synchronous
```

```

exit //Salir del modo actual
vlan 8 //Crear la vlan 8
name General-Users //Asignar nombre a la vlan
exit //Salir del modo actual
vlan 13 //Crear la vlan 13
name Special-Users //Asignar nombre a la vlan
exit //Salir del modo actual
wr //Guardar la configuración

```

CONFIGURACION INICIAL EN SWITCH D2

```

Enable //Ingresar a modo privilegiado
configure terminal //Ingresar a modo de configuración
hostname R1 //Asignar nombre al switch
ipv6 unicast-routing //Habilitar el routing ipv6
no ip domain lookup //Habilitar la traducción de nombre
line con 0 //Ingresar al modo de configuración
de la linea de consola
exec-timeout 0 0 //Establecer el tiempo de espera
inactivo de la sesión remota
logging synchronous //Indicar si hay un mensaje de
evento
exit //Salir del modo actual
vlan 8 //Crear la vlan 8
name General-Users //Asignar nombre a la vlan
exit //Salir del modo actual
vlan 13 //Crear la vlan 13
name Special-Users //Asignar nombre a la vlan
exit //Salir del modo actual
wr //Guardar la configuración

```

CONFIGURACION INICIAL EN SWITCH A1

```

Enable //Ingresar a modo privilegiado
configure terminal //Ingresar a modo de configuración
hostname R1 //Asignar nombre al switch
ipv6 unicast-routing //Habilitar el routing ipv6
no ip domain lookup //Habilitar la traducción de nombre
line con 0 //Ingresar al modo de configuración
de la linea de consola
exec-timeout 0 0 //Establecer el tiempo de espera
inactivo de la sesión remota
logging synchronous //Indicar si hay un mensaje de evento

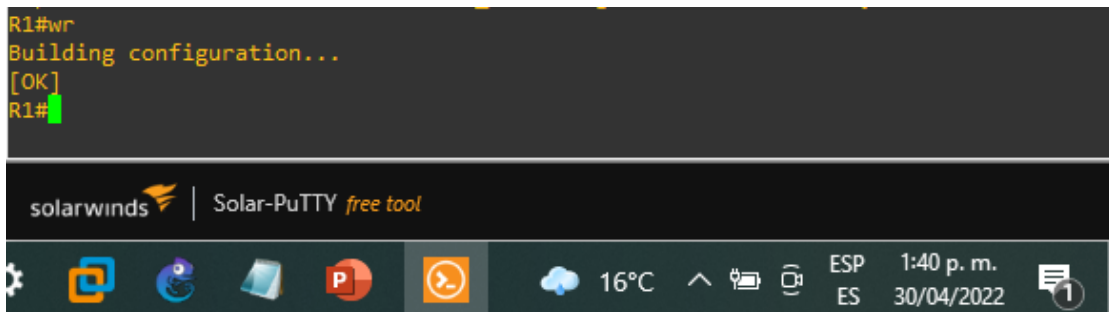
```

```

exit //Salir del modo actual
vlan 8 //Crear la vlan 8
name General-Users //Asignar nombre a la vlan
exit //Salir del modo actual
wr //Guardar la configuración

```

Ilustración 3. Comando para guardar la configuración en los dispositivos



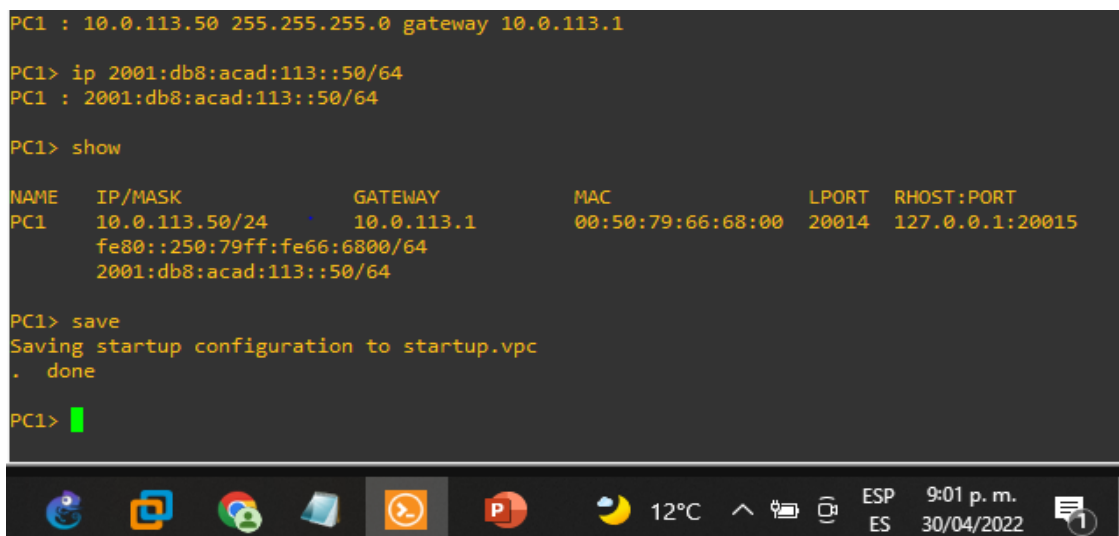
```

R1#wr
Building configuration...
[OK]
R1#

```

Fuente: Elaboración propia en GNS3

Ilustración 4. Configuración de PC1



```

PC1 : 10.0.113.50 255.255.255.0 gateway 10.0.113.1
PC1> ip 2001:db8:acad:113::50/64
PC1 : 2001:db8:acad:113::50/64
PC1> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.0.113.50/24 10.0.113.1 00:50:79:66:68:00 20014 127.0.0.1:20015
fe80::250:79ff:fe66:6800/64
2001:db8:acad:113::50/64
PC1> save
Saving startup configuration to startup.vpc
. done
PC1>

```

Fuente: Elaboración propia en GNS3

Ilustración 5. Configuración de PC2

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

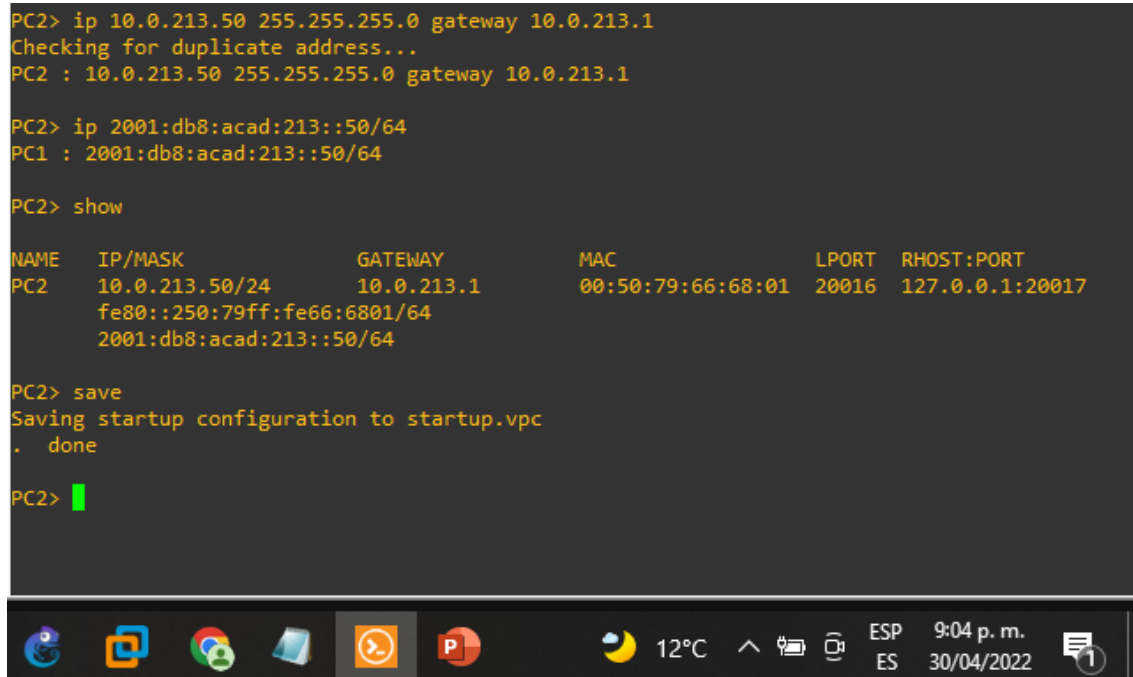
PC2> ip 2001:db8:acad:213::50/64
PC1 : 2001:db8:acad:213::50/64

PC2> show

NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC2       10.0.213.50/24   10.0.213.1       00:50:79:66:68:01 20016  127.0.0.1:20017
          fe80::250:79ff:fe66:6801/64
          2001:db8:acad:213::50/64

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

PC2> █
```



Fuente: Elaboración propia en GNS3

Ilustración 6. Configuración de PC3

```
PC3> ip 10.0.108.50/24 gateway 10.0.108.1
Checking for duplicate address...
PC3 : 10.0.108.50 255.255.255.0 gateway 10.0.108.1

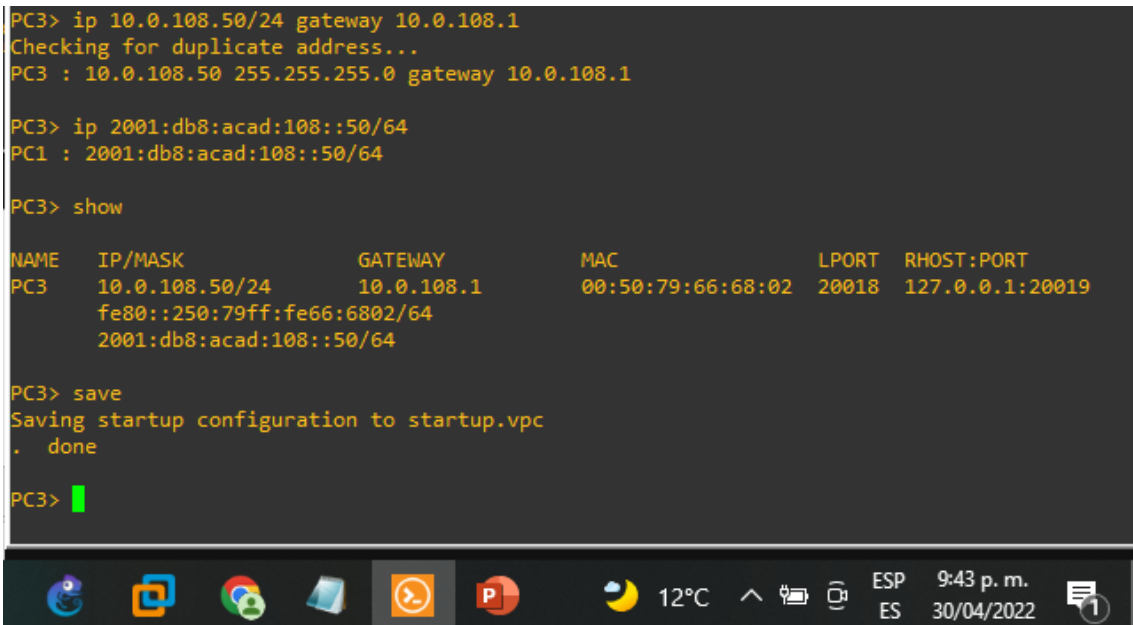
PC3> ip 2001:db8:acad:108::50/64
PC1 : 2001:db8:acad:108::50/64

PC3> show

NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC3       10.0.108.50/24   10.0.108.1       00:50:79:66:68:02 20018  127.0.0.1:20019
          fe80::250:79ff:fe66:6802/64
          2001:db8:acad:108::50/64

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

PC3> █
```



Fuente: Elaboración propia en GNS3

Ilustración 7. Configuración de PC4

```

PC4> ip 10.0.208.50/24 gateway 10.0.208.1
Checking for duplicate address...
PC4 : 10.0.208.50 255.255.255.0 gateway 10.0.208.1

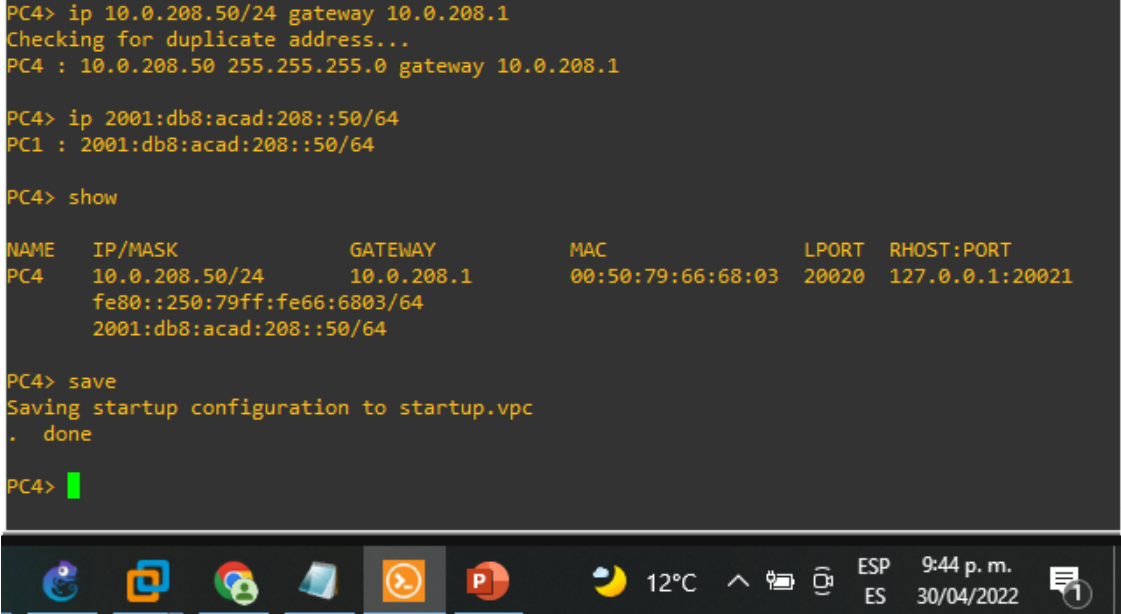
PC4> ip 2001:db8:acad:208::50/64
PC1 : 2001:db8:acad:208::50/64

PC4> show

NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC4      10.0.208.50/24   10.0.208.1       00:50:79:66:68:03  20020  127.0.0.1:20021
          fe80::250:79ff:fe66:6803/64
          2001:db8:acad:208::50/64

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

PC4> █
    
```



Fuente: Elaboración propia en GNS3

2. Se configura VRF-Lite de acuerdo a la topología de la figura se crean dos VRF General-Users y Special-Users los cuales admiten IPv4 e IPv6 de acuerdo a la siguiente tabla de direccionamiento

Tabla 1. Direccionamiento para los dispositivos

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace local IPv6
R1	G0/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G1/0.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G1/0.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G0/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G1/0.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3

	G1/0.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G0/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G0/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G1/0.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G1/0.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NADA	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NADA	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC3	NADA	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NADA	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

2.1 Se implementa el uso de Router-On-A-Stick en cada router de acuerdo a la tabla anterior, para la encapsulación de Special-Users aplicar dot1Q 13 y para General-Users dot1Q 8, adicionalmente se configuran las rutas estáticas para VRF IPv4 e IPv6

CONFIGURACION DE VRF EN R1

```

vrf definition Special-Users //Crear la VRF
address-family ipv4 //Asignar la vrf IPv4
address-family ipv6 //Asignar la vrf IPv6
exit //Salir del modo actual
interface g1/0 //Ingresar a la interfaz
ip dirección 10.0.113.1 255.255.255.0 //Asignar dirección IPv4
ipv6 address 2001:db8:acad:113::1/64 //Asignar dirección IPv6
no shutdown //Encender la interfaz
exit //Salir del modo actual
interface g1/0.1 //Crear subinterfaz
encapsulation dot1Q 13 //Permitir enlace troncal e
identificar la subinterfaz
vrf forwarding Special-Users //Permitir varias instancias de
enrutamiento
ip address 10.0.113.1 255.255.255.0 //Asignar dirección IPv4 a la
subinterfaz
ipv6 address 2001:db8:acad:113::1/64 //Asignar dirección IPv6 a la subinterfaz

```

```

no shutdown
exit
interface g0/0
ip dirección 10.0.12.1 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
no shutdown
exit
interface g0/0.1
encapsulation dot1Q 13
la subinterfaz
vrf forwarding Special-Users
enrutamiento
ip address 10.0.12.1 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
no shutdown
exit
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
interface g1/0
ip dirección 10.0.108.1 255.255.255.0
ipv6 address 2001:db8:acad:108::1/64
no shutdown
exit
interface g1/0.2
encapsulation dot1Q 8
la subinterfaz
vrf forwarding General-Users
enrutamiento
ip address 10.0.108.1 255.255.255.0
subinterface
ipv6 address 2001:db8:acad:108::1/64
subinterfaz
no shutdown
exit
interface g0/0
ip dirección 10.0.12.1 255.255.255.0
ipv6 dirección 2001:db8:acad:12::1/64
no shutdown
exit
interface g0/0.2
encapsulation dot1Q 8
identificar la subinterfaz
vrf forwarding General-Users

```

```

//Encender las subinterfaz
//Salir del modo actual
//Ingresar a la interfaz
//Asignar dirección IPv4 a la interfaz
//Asignar dirección IPv6 a la interfaz
//Encender la interfaz
//Salir del modo actual
//Crear la subinterfaz
//Permitir enlace troncal e identificar

//Permitir varias instancias de

//Asignar dirección IPv4 a la subinterfaz
//Asignar dirección IPv6 a la subinterfaz
//Encender la subinterfaz
//Salir del modo actual
//Crear la VRF
//Asignar la vrf a IPv4
//Asignar la vrf a IPv6
//Salir del modo actual
//Ingresar a la interfaz
//Asignar dirección IPv4 a la interfaz
//Asignar dirección IPv6 a la interfaz
//Encender la interface
//Salir del modo actual
//Crear la subinterfaz
//Permitir enlace troncal e identificar

//Permitir varias instancias de

//Asignar dirección IPv4 a la

//Asignar dirección a IPv6 a la

//Encender las subinterfaz
//Salir del modo actual
//Ingresar a la interfaz
//Asignar IPv4 a la interfaz
//Asignar IPv6 a la interfaz
//Encender la interfaz
//Salir del modo actual
//Crear la subinterfaz
//Permitir enlace troncal e

//Permitir varias instancias de

```

```

enrutamiento
ip address 10.0.12.1 255.255.255.0 //Asignar dirección IPv4 a la
subinterfaz
ipv6 address 2001:db8:acad:12::1/64 //Asignar dirección IPv6 a la
subinterfaz
no shutdown //Encender la subinterfaz

```

CONFIGURACION DE VRF EN R2

```

vrf definition Special-Users //Crear la VRF
address-family ipv4 //Asignar IPv4 a la VRF
address-family ipv6 //Asignar Ipv6 a la VRF
exit //Salir del modo actual
exit //Salir del modo actual
interface g0/0 //Ingreso a la interface
ip dirección 10.0.12.2 255.255.255.0 //Asignar dirección IPv4 a la
interfaz
ipv6 address 2001:db8:acad:12::2/64 //Asignar dirección IPv6 a la
interfaz
no shutdown //Encender la interfaz
exit //Salir del modo actual
interface g0/0.1 //Crear la subinterfaz
encapsulation dot1Q 13 //Permitir enlace troncal e
identificar la subinterfaz
vrf forwarding Special-Users //Permitir varias instancias de
enrutamiento
ip address 10.0.12.2 255.255.255.0 //Asignar dirección IPv4 a la
subinterface
ipv6 address 2001:db8:acad:12::2/64 //Asignar dirección IPv6 a la
subinterfaz
no shutdown //Encender la subinterfaz
exit //Salir de modo configuración
vrf definition General-Users //Crear la VRF
address-family ipv4 //Asignar IPv4 a la VRF
address-family ipv6 //Asignar IPv4 a la VRF
exit //Salir del modo actual
interface g0/0 //Ingresar a la interfaz
ip dirección 10.0.12.2 255.255.255.0 //Asigna dirección IPv4 a la
interfaz
ipv6 address 2001:db8:acad:12::2/64 //Asignar dirección IPv6 a la
interfaz
no shutdown //Encender la interfaz
exit //Salir del modo actual
interface g0/0.2 //Crear la subinterfaz
encapsulation dot1Q 8 //Permitir enlace troncal e

```

```

identificar la subinterfaz
vrf forwarding General-Users //Permitir varias instancias de
enrutamiento //Asignar dirección IPv4 a la
ip address 10.0.12.2 255.255.255.0 //Asignar dirección IPv6 a la
subinterfaz //Asignar dirección IPv6 a la
ipv6 address 2001:db8:acad:12::2/64 //Asignar dirección IPv6 a la
subinterfaz //Asignar dirección IPv6 a la
no shutdown //Encender la subinterfaz
exit //Salir del modo actual
interface g1/0 //Ingresar a la interfaz
ip dirección 10.0.23.2 255.255.255.0 //Asignar dirección
a la interfaz //Asignar dirección
ipv6 address 2001:db8:acad:23::2/64 //Asignar dirección a la interface
no shutdown //Encender la interface
exit //Salir del modo actual
interface g1/0.2 //Crear la subinterfaz
encapsulation dot1Q 8 //Permitir enlace troncal e
identificar la subinterfaz //Permitir varias instancias de
vrf forwarding General-Users //Permitir varias instancias de
enrutamiento //Permitir varias instancias de
ip address 10.0.23.2 255.255.255.0 //Asignar dirección IPv4 a la
subinterfaz //Asignar dirección IPv4 a la
ipv6 address 2001:db8:acad:23::2/64 //Asignar dirección IPv6 a la
subinterfaz //Asignar dirección IPv6 a la
no shutdown //Encender la subinterfaz
exit //Salir del modo actual

```

CONFIGURACION DE VRF EN R3

```

vrf definition Special-Users //Crear la VRF
address-family ipv4 //Asignar IPv4 a la VRF
address-family ipv6 //Asignar IPv6 a la VRF
exit //Salir del modo actual
exit //Salir del modo actual
interface g0/0 //Ingresar a la interfaz
ip dirección 10.0.23.3 255.255.255.0 //Asignar dirección IPv4 a la
interface //Asignar dirección IPv4 a la
ipv6 address 2001:db8:acad:23::3/64 //Asignar dirección IPv6 a la
interfaz //Asignar dirección IPv6 a la
no shutdown //Encender la interfaz
exit //Salir del modo actual
interface g0/0.1 //Crear la subinterfaz
encapsulation dot1Q 13 //Permitir enlace troncal e
identificar la subinterfaz //Permitir varias instancias de
vrf forwarding Special-Users //Permitir varias instancias de

```

```

enrutamiento
ip address 10.0.23.3 255.255.255.0 //Asignar dirección IPv4 a la
subinterfaz
ipv6 address 2001:db8:acad:23::3/64 //Asignar dirección IPv6 a la
subinterfaz
no shutdown //Encender la subinterfaz
exit //Salir del modo actual
interface g1/0 //Ingresar a la interfaz
ip dirección 10.0.213.1 255.255.255.0 //Asignar dirección Ipv4 a la
interfaz
ipv6 dirección 2001:db8:acad:213::1/64 //Asignar IPv6 a la interfaz
no shutdown //Encender la interfaz
exit //Salir del modo actual
interface g1/0.1 //Crear la subinterface
encapsulation dot1Q 13 //Permitir enlace troncal e
identificar la subinterfaz
vrf forwarding Special-Users //Permitir varias instancias de
enrutamiento
ip address 10.0.213.1 255.255.255.0 //Asignar dirección IPv4 a la
subinterfaz
ipv6 address 2001:db8:acad:213::1/64 //Asignar Ipv6 a la subinterfaz
no shutdown //Encender la subinterfaz
exit //Salir del modo actual
vrf definición General-Users //Crear la VRF
address-family ipv4 //Asignar IPv4 a la VRF
address-family ipv6 //Asignar IPv6 a la VRF
exit //Salir del modo actual
interface g0/0 //Ingresar a la interfaz
ip dirección 10.0.23.3 255.255.255.0 //Asignar dirección IPv4 a la
interfaz
ipv6 address 2001:db8:acad:23::3/64 //Asignar a dirección IPv6 a la
interfaz
no shutdown //Encender la interfaz
exit //Salir del modo actual
interface g0/0.2 //Crear la subinterfaz
encapsulation dot1Q 8 //Permitir enlace troncal e
identificar la subinterfaz
vrf forwarding General-Users //Permitir varias instancias de
enrutamiento
ip address 10.0.23.3 255.255.255.0 //Asignar dirección IPv4 a la
subinterfaz
ipv6 address 2001:db8:acad:23::3/64 //Asignar dirección IPv6 a la
subinterfaz
no shutdown //Encender la interfaz
exit //Salir del modo actual

```

```

interface g1/0 //Ingresar a la interface
ip dirección 10.0.208.1 255.255.255.0 //Asignar dirección IPv4 a la
interfaz
ipv6 address 2001:db8:acad:208::1/64 //Asignar dirección IPv6 a la
interfaz
no shutdown //Encender la interfaz
exit //Salir del modo actual
interface g1/0.2 //Crear la subinterface
encapsulation dot1Q 8 //Permitir enlace troncal e
identificar la subinterfaz
vrf forwarding General-Users //Permitir varias instancias
de enrutamiento
ip address 10.0.208.1 255.255.255.0 //Asignar dirección IPv4 a la
subinterfaz
ipv6 address 2001:db8:acad:208::1/64 //Asignar dirección IPv6 a la
subinterfaz
no shutdown //Encender la subinterfaz
exit //Salir del modo actual

```

CONFIGURACION RUTAS ESTATICAS VRF EN R1

```

ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.2
//Definir la red de destino mascara de la subred y dirección del próximo
salto
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.2
//Definir la red de destino mascara de la subred y dirección del próximo
salto
vrf General-Users 2001:db8:acad:23::/64 2001:db8:acad:12::2
//Definir la red de destino mascara de la subred y dirección del próximo
salto
vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:12::2
//Definir la red de destino mascara de la subred y dirección del próximo
salto

```

CONFIGURACION RUTAS ESTATICAS VRF EN R2

```

ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.1
//Definir la red de destino mascara de la subred y dirección del próximo
salto
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.3
//Definir la red de destino mascara de la subred y dirección del próximo
salto
vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1
//Definir la red de destino mascara de la subred y dirección del próximo
salto

```

```
salto
vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3
//Definir la red de destino mascara de la subred y dirección del próximo
salto
```

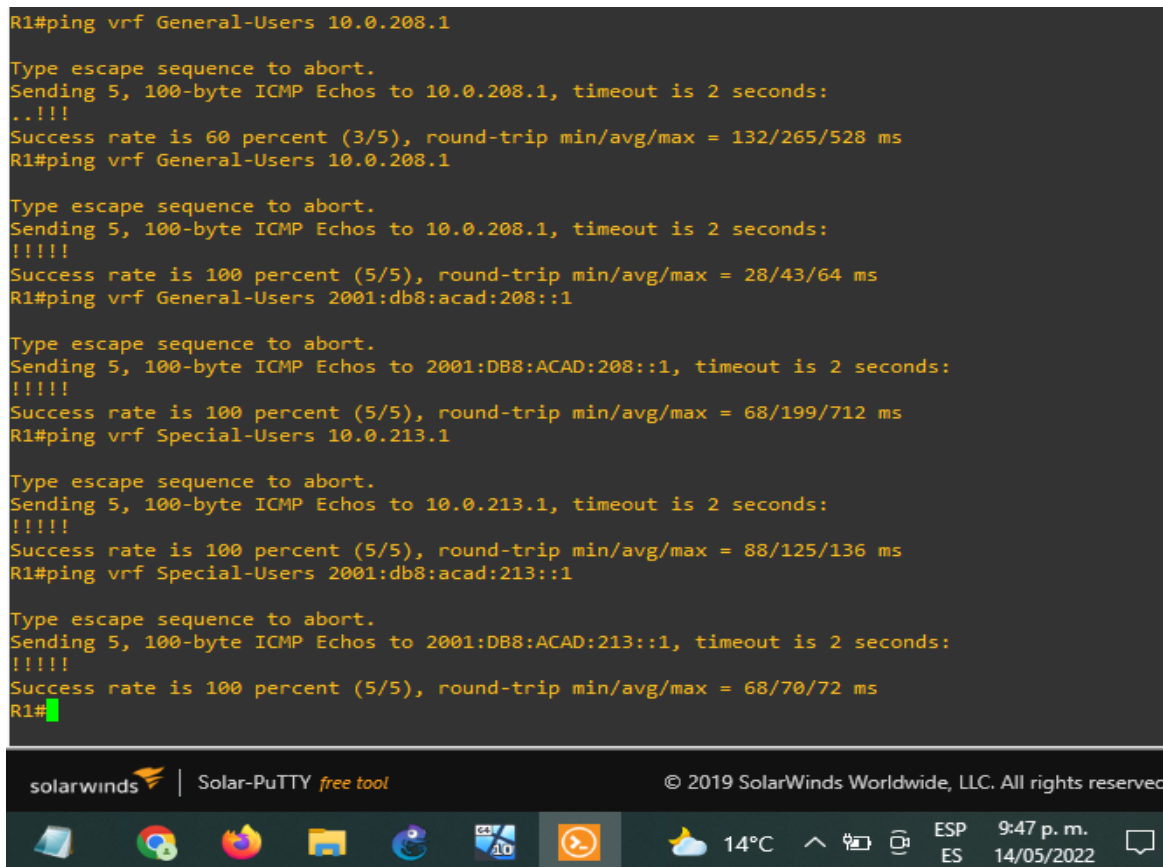
CONFIGURACION RUTAS ESTATICAS VRF EN R3

```
ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.2
//Definir la red de destino mascara de la subred y dirección del próximo
salto
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.2
//Definir la red de destino mascara de la subred y dirección del próximo
salto
vrf General-Users 2001:db8:acad:12::/64 2001:db8:acad:23::2
//Definir la red de destino mascara de la subred y dirección del próximo
salto
vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:23::2
//Definir la red de destino mascara de la subred y dirección del próximo
salto
```

2.2 Comprámbamos la conectividad de las dos VRF mediante ping entre R1 y R3

Ilustración 8. Prueba de ping VRF R1 a R3

```
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 60 percent (3/5), round-trip min/avg/max = 132/265/528 ms
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 = 28/43/64 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 = 68/199/712 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 = 88/125/136 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 = 68/70/72 ms
R1#
```



Fuente: Elaboración propia en GNS3

Parte 3. Configurar Capa 2, en esta parte, se configuran los Switches para soportar la conectividad con los dispositivos finales

CONFIGURACION DE CAPA 2 EN SWITCH D1

```
interface range ethernet 0/0-3,1/0-3, 2/0-3,3/0-3 //Definir rango de interfaces
shutdown //Apagar las interfaces
interface Ethernet0/0 //Ingresar a la interfaz
no shutdown //Encender la interfaz
switchport trunk encapsulation dot1q //Permitir enlace troncal
switchport trunk allowed vlan 8,13 //Agregar las vlan al enlace
truncal
switchport mode trunk //Permitir paso del tráfico de
las vlan
```

```

interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
troncal
interface range Eth0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode desirable
activo, negociará los paquetes PAgP
no shutdown
interface Ethernet0/3
switchport access vlan 13
acceso
switchport mode access
spanning-tree portfast
la capa 2

```

//Crear la interfaz portchannel
//Permitir enlace troncal
//Definir el puerto como enlace

//Definir un rango de interfaces
//Permitir enlace troncal
//Definir el puerto como
//Establece el puerto en modo

//Encender la interfaces
//Ingresar a la interfaz
//Asignar la vlan en modo

//Definir el puerto como acceso
//Obtener acceso inmediato a

CONFIGURACION DE CAPA 2 EN SWITCH D2

```

interface range ethernet 0/0-3,1/0-3, 2/0-3,3/0-3
shutdown
interface Ethernet0/0
no shutdown
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 8,13
troncal
switchport mode trunk
las vlan
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
enlace troncal
interface Ethernet0/1
no shutdown
switchport access vlan 13
acceso
switchport mode access
acceso
spanning-tree portfast
la capa 2
interface Ethernet0/2
no shutdown
switchport access vlan 13
acceso
switchport mode access

```

//Definir rango de interfaces
//Apagar las interfaces
//Ingresar a la interface
//Encender la interfaz
//Permitir enlace troncal
//Agregar las vlan al enlace

//Permitir paso del tráfico de

//Crear la interfaz portchannel
//Permitir enlace troncal
//Definir el puerto como

//Ingresar a la interfaz
//Encender la interfaz
//Asignar la vlan en modo

//Definir el puerto como

//Obtener acceso inmediato a

//Ingresar a la interfaz
//Encender la interfaz
//Asignar la vlan en modo

//Definir el puerto como

```
acceso
spanning-tree portfast //Obtener acceso inmediato a
la capa 2
```

CONFIGURACION DE CAPA 2 EN SWITCH D3

```
interface Port-channel1 //Crear la interfaz portchannel
switchport trunk encapsulation dot1q //Permitir enlace troncal
switchport mode trunk //Definir el puerto como enlace
troncal
interface range Eth0/0-1 //Definir un rango de interfaces
switchport trunk encapsulation dot1q //Permitir enlace troncal
switchport mode trunk //Definir el puerto como
channel-group 1 mode desirable //Establecer el puerto en modo
activo, negociará los paquetes PAgP
no shutdown //Encender la interfaces
interface Ethernet0/2 //Ingresar a la interfaz
switchport access vlan 8 //Asignar la vlan en modo acceso
switchport mode access //Definir el puerto como acceso
spanning-tree portfast //Obtener acceso inmediato a la
capa 2
```

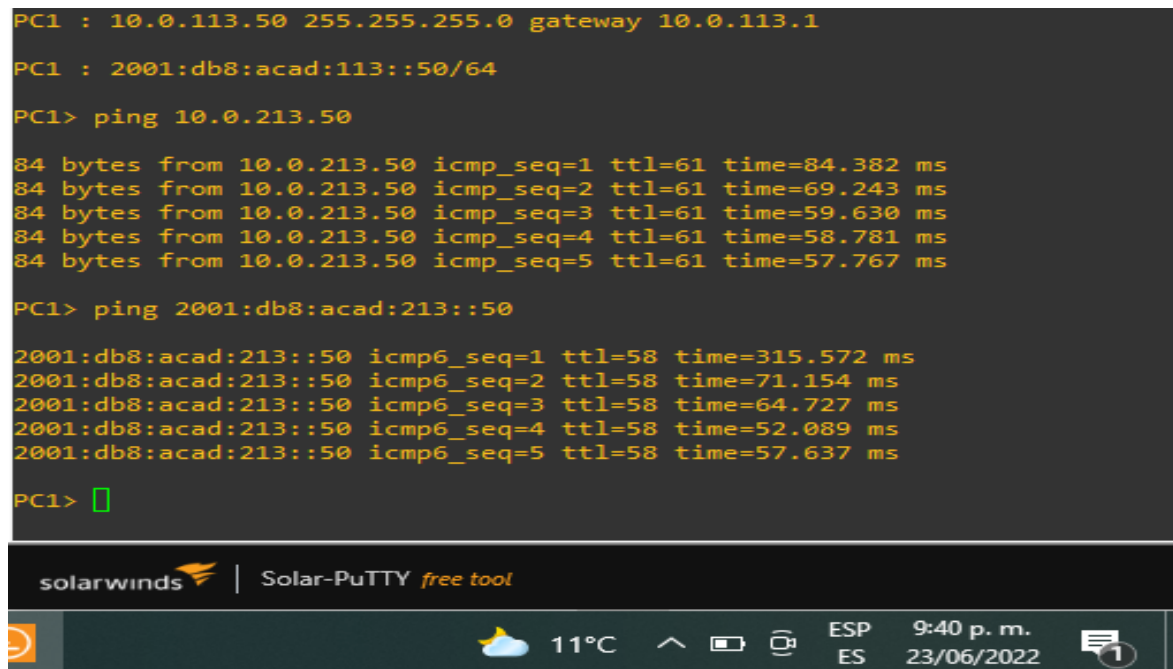
Parte 3.1 Verificamos la conectividad de capa 2, para eso se comprueba mediante ping entre PC1 y PC2 y Ping entre PC3 y PC4 en IPv4 e IPv6

Ilustración 9. Prueba de ping de PC1 a PC2

```
PC1 : 10.0.113.50 255.255.255.0 gateway 10.0.113.1
PC1 : 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=84.382 ms
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=69.243 ms
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=59.630 ms
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=58.781 ms
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=57.767 ms

PC1> ping 2001:db8:acad:213::50
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=315.572 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=71.154 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=64.727 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=52.089 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=57.637 ms

PC1> █
```



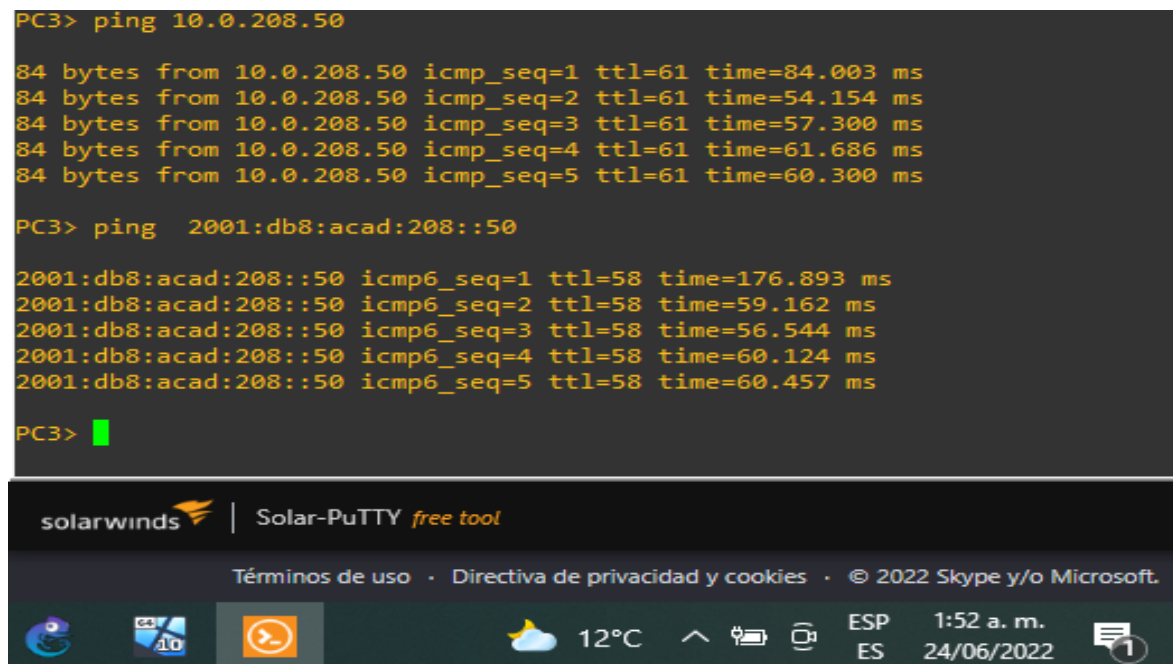
Fuente: Elaboración propia en GNS3

Ilustración 10. Prueba de ping de PC1 a PC2

```
PC3> ping 10.0.208.50
84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=84.003 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=54.154 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=57.300 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=61.686 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=60.300 ms

PC3> ping 2001:db8:acad:208::50
2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=176.893 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=59.162 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=56.544 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=60.124 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=60.457 ms

PC3> █
```



Fuente: Elaboración propia en GNS3

Parte 4. Configurar seguridad se debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Se muestran los comandos aplicados en cada uno de los dispositivos

CONFIGURACION BASICA DE SEGURIDAD EN A1 - D1 - D2 - R1 - R2 - R3

```
service password-encryption // Encriptar las contraseñas
del archivo de configuración
enable secret cisco12345cisco // Proteger el modo EXE con
privilegios
username admin secret 0 cisco12345cisco // Indicar nombre de usuario
y la contraseña encriptada
username admin privilege 15 secret cisco12345cisco //Crear cuenta de usuario
local
aaa new-model // Habilitar AAA
aaa authentication login default local //Autenticar AAA
```

CONCLUSIONES

Mediante el uso de herramientas de simulación de redes como Packet Tracer y GNS3 podemos suponer diversos escenarios LAN y WAN que hoy en día son implementados en entornos reales, es así que la academia Cisco Netacad coloca importantes recursos y programas con los cuales se pueden adquirir diferentes habilidades por medio de la práctica, para diseño, administración y solución de fallas.

Conocimos y aplicamos diferentes protocolos de comunicación que son usados en la actualidad en las redes de nivel corporativo como OSPF, EIGRP, BGP interpretando principios de enrutamiento y conmutación de paquetes, así mismo los modos de acción de protocolos como STP y creación de VLANs para lograr la conmutación de redes Switching y gestionar de mejor manera los dominios de broadcast independientes en las redes jerárquicas convergentes.

Evidenciamos que a través del uso e implementación de VRF se pueden crear varias VPN de manera separada lo que favorece el ahorro de infraestructura de las redes ya que se puede generar tráfico de diferentes clientes usando un mismo dispositivo, así mismo con el uso de VRF se acrecienta el tema de seguridad inclusive haciendo uso de la nube pública.

Durante la implementación del escenario propuesto se presentaron diversos problemas o fallas las cuales se debieron ir solucionando, pudimos evidenciar que es muy importante realizar las configuraciones paso a paso e ir chequeando con los comandos como `show running-config`, `show interfaces`, `show vlan brief` y otros comandos disponibles para la captura o visualización de información del estado de los equipos routers o switches, ya que si realizamos toda la configuración general lo más seguro cuando vayamos a probar se presente algún inconveniente y de ser así será más difícil identificar donde está el punto de falla, por el contrario si lo revisamos secuencialmente es más fácil identificar la falla y resolverla para continuar avanzando de forma segura y exitosa.

BIBLIOGRAFIA

GARZA RIOS, Edgeworth y HUCABY, Gooley. CCNP and CCIE Enterprise Core ENCOR. CISCO Press (Ed). Packet Forwarding. {En línea} {consultado junio de 2022} Disponible en <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

GARZA RIOS, Edgeworth y HUCABY, Gooley. CCNP and CCIE Enterprise Core ENCOR CISCO Press (Ed). Spanning Tree Protocol.). Packet Forwarding. {En línea} {consultado junio de 2022} Disponible en <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

GARZA RIOS, Edgeworth y HUCABY, Gooley. CCNP and CCIE Enterprise Core ENCOR. CISCO Press (Ed). Advanced Spanning Tree.). Packet Forwarding. {En línea} {consultado junio de 2022} Disponible en <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

GARZA RIOS, Edgeworth y HUCABY, Gooley. CCNP and CCIE Enterprise Core ENCOR. CISCO Press (Ed). Multiple Spanning Tree Protocol.). Packet Forwarding. {En línea} {consultado junio de 2022} Disponible en <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

GARZA RIOS, Edgeworth y HUCABY, Gooley. CCNP and CCIE Enterprise Core ENCOR. CISCO Press (Ed). Trunks and EtherChannel Bundles.). Packet Forwarding. {En línea} {consultado junio de 2022} Disponible en: <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

GARZA RIOS, Edgeworth y HUCABY, Gooley. CCNP and CCIE Enterprise Core ENCOR. CISCO Press (Ed). IP Routing Essentials.). Packet Forwarding. {En línea} {consultado junio de 2022} Disponible en: <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

GARZA RIOS, Edgeworth y HUCABY, Gooley. CCNP and CCIE Enterprise Core ENCOR. CISCO Press (Ed). EIGRP.). Packet Forwarding. {En línea} {consultado junio de 2022} Disponible en: <https://1drv.ms/b/s!AAIGg5JUgUBthk8>