

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBAS DE HABILIDADES PRACTICAS CCNP

JULIAN ANDRES TORO ESCOBAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA ELECTRÓNICA  
TULUA – VALLE  
2022

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBAS DE HABILIDADES PRACTICAS CCNP

JULIAN ANDRES TORO

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

Director

MSc. HECTOR JULIAN PARRA MOGOLLON

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

TULUA – VALLE

2022

NOTA DE ACEPTACIÓN:

---

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

TULUA, (26 de junio, 2022)

## **AGRADECIMIENTO**

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

## CONTENIDO

AGRADECIMIENTO .....	4
LISTA DE FIGURAS.....	8
GLOSARIO.....	9
RESUMEN.....	10
ABSTRACT .....	10
INTRODUCCION.....	11
DESARROLLO DEL ESCENARIO .....	12
1. CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DEL INTERFAZ .....	12
1.1 Topología a desarrollar .....	12
1.2 Cablear la red como se muestra en la topología.....	13
1.3 Configurar los parámetros básicos para cada dispositivo de interconexión.....	13
1.4 Configurar los parámetros básicos para cada dispositivo final.....	16
2. CONFIGURAR VRF Y RUTAS ESTÁTICAS .....	19
2.1. Configurar las dos VRF's y que soporten IPv4 e IPv6 .....	19
2.2. En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF según la tabla de direccionamiento.....	20
2.3. Verificación del direccionamiento IPv4 e IPv6 de las interfaces.....	25
2.4. Configuración de rutas estáticas.....	26
2.4. Verificar conectividad en cada VRF .....	28
3. CONFIGURACIÓN DE LOS DISPOSITIVOS DE CAPA 2.....	29
3.1. Desactivar todas las interfaces en D1, D2, y A1 .....	29
3.2. En D1 y D2, configurar los enlaces troncales a R1 y R3.....	29

3.3. En D1 y A1, configurar el EtherChannel.....	30
3.4. En D1, D2, y A1, Se configuran las interfaces de acceso para PC1, PC2, PC3, y PC4.....	31
3.5. Verificar la conectividad PC a PC.....	32
4. CONFIGURAR SEGURIDAD .....	34
4.1. En todos los equipos configurar, el modo EXEC privilegiado .....	34
4.2. En todos los equipos, se crea una cuenta para un usuario local .....	34
4.3. En todos los equipos, activar AAA y activar la autenticación AAA .....	34
CONCLUSIONES .....	35
BIBLIOGRAFIA.....	36

## LISTA DE TABLAS

TABLA 1. HOST PC 1 .....	16
TABLA 2. HOST PC 2 .....	17
TABLA 3. HOST PC 3 .....	17
TABLA 4. HOST PC 4 .....	18

## LISTA DE FIGURAS

Figura 1. Topología Propuesta.....	12
Figura 2. Topología de red del escenario propuesto .....	13
Figura 3. Verificación VRF R1 comando show ip vrf Interface .....	25
Figura 4. Verificación VRF R2 comando show ip vrf Interface .....	25
Figura 5. Verificación VRF R3 comando show ip vrf Interface .....	26
Figura 6. Verificar conectividad.....	28
Figura 7. Ping PC1 a PC2.....	33
Figura 8. Ping PC3 a PC4.....	33

## GLOSARIO

**AAA** : Son los tres pasos fundamentales en la seguridad de datos en informática: Autenticación, Autorización y Auditoria

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

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

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

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

## RESUMEN

En el siguiente Informe se desarrolla el escenario correspondiente propuesto en la prueba de habilidades prácticas del diplomado de profundización cisco CCNP, este consiste en una red propuesta la cual busca de evaluar en el estudiante competencias y habilidades en el manejo de configuración y administración de protocolos de conmutación y enrutamiento en enrutadores y switches en un entorno basado en solución de problemas mediante tres escenarios diferentes, utilizando la herramienta de packet tracer.

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

## ABSTRACT

The following Report develops the corresponding scenario proposed in the practical skills test of the cisco CCNP deepening diploma course, this consists of a proposed network which seeks to evaluate in the student competencies and skills in the management of configuration and administration of communication protocols switching and routing in routers and switches in an environment based on troubleshooting through three different scenarios, using the packet tracer tool.

**Keywords :** CISCO, CCNP, Switching, Routing, Networks, Electronics.

## INTRODUCCION

El diplomado de profundización CCNP de cisco (Cisco Certified Network Professional) abarca temáticas avanzadas respecto a temas de instalación, configuración y operación de redes de área local y área amplia, cuyo objetivo tiene como fin la implementación de redes escalables que vayan desde campus hasta instalación de intranets y la solución de problemas presentados en dichos entornos, motivo por el cual su alcance aborda conceptos fundamentales de protocolos de enrutamiento, mediante uso de protocolos como STP, configuración VLANs, configuración de subinterfaces VRF y rutas estáticas en escenarios de red corporativas.

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

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

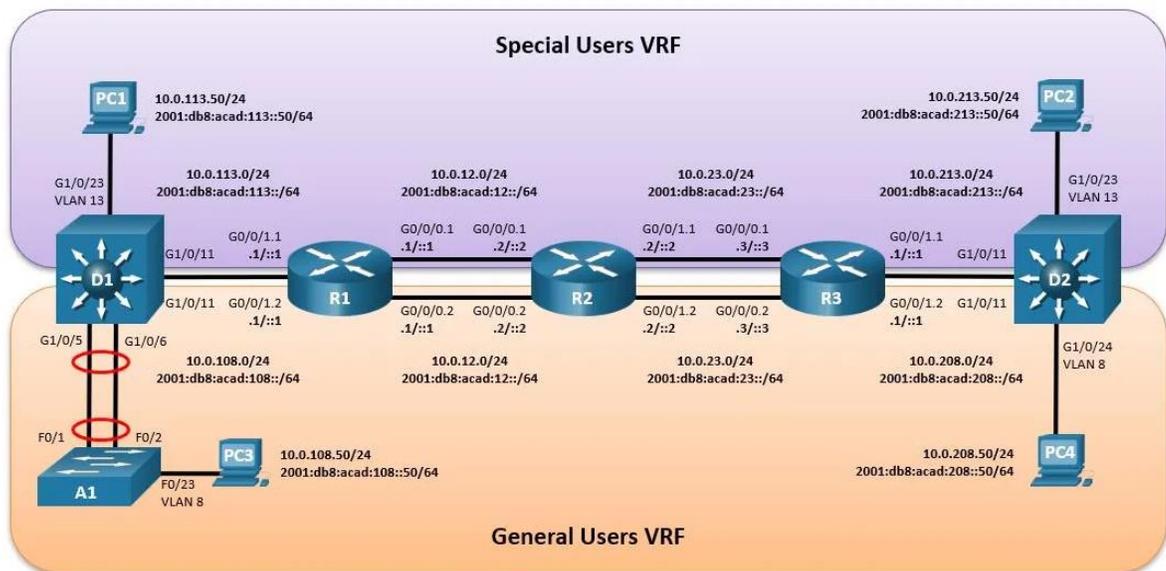
## DESARROLLO DEL ESCENARIO

### 1. CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DEL INTERFAZ

#### 1.1 Topología a desarrollar

Para el desarrollo de este trabajo de grado el escenario propone desarrollar la siguiente topología.

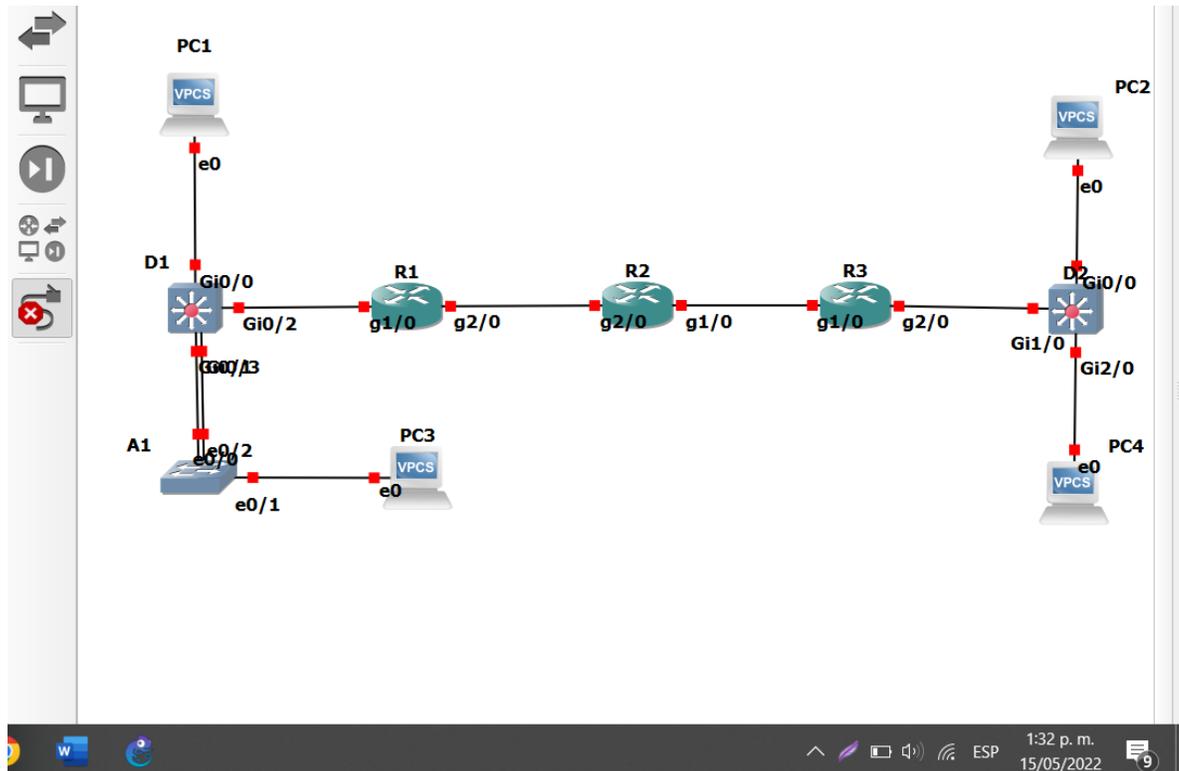
Figura 1. Topología Propuesta



Fuente: Prueba de habilidades practica CCNP

## 1.2 Cablear la red como se muestra en la topología.

Figura 2. Topología de red del escenario propuesto.



Fuente: Autoría Propia

## 1.3 Configurar los parámetros básicos para cada dispositivo de interconexión

A continuación, se presentan los comandos ejecutados en cada uno de los dispositivos de la red en la configuración inicial.

### Enrutador R1

```
hostname R1 #Asigna nombre al enrutador 1
ipv6 unicast-routing # Habilita el enrutamiento ipv6
no ip domain lookup # Deshabilita la traducción de nombre a dirección basada en DNS

banner motd # R1, ENCOR Skills Assessment, Scenario 2 # #Habilita un mensaje de bienvenida
line con 0 # se ingresa al modo de consola de la línea 0
exec-timeout 0 0 #Establece el tiempo de espera inactivo de la sesión remota
```

```

logging synchronous          # Evita los mensajes inesperados que
                              aparecen en pantalla
exit                          #Salimos del modo consola de la línea 0

```

Se ejecutan los mismos comandos en los enrutadores restantes, identificándolos como R2 y R3 respectivamente.

## Enrutador R2

```

hostname R2                  #Asigna nombre al enrutador 2
ipv6 unicast-routing        # Habilita el enrutamiento ipv6
no ip domain lookup         # Deshabilita la traducción de nombre a
                              dirección basado en DNS
banner motd # R2, ENCOR Skills Assessment, Scenario 2 # #Habilita un mensaje de bienvenida
line con 0                  # se ingresa al modo de consola en línea 0
exec-timeout 0 0           #Establece el tiempo de espera inactivo de la
                              sesión remota
logging synchronous        # Evita los mensajes inesperados que
                              aparecen en pantalla
exit                          #Salimos del modo consola de la línea 0

```

## Enrutador R3

```

hostname R3                  #Asigna nombre al enrutador 3
ipv6 unicast-routing        # Habilita el enrutamiento ipv6
no ip domain lookup         # Deshabilita la traducción de nombre a
                              dirección basado en DNS
banner motd # R3, ENCOR Skills Assessment, Scenario 2 # #Habilita un mensaje de bienvenida
line con 0                  # se ingresa al modo de consola en línea 0
exec-timeout 0 0           #Establece el tiempo de espera inactivo de la
                              sesión remota
logging synchronous        # Evita los mensajes inesperados que
                              aparecen en pantalla
exit                          #Salimos del modo consola de la línea 0

```

## Switch D1

```

hostname D1                  # asigna nombre el nombre correspondiente al
                              Switch D1
ip routing                   # permite configurar la table de enrutamiento

```

ipv6 unicast-routing	principal
no ip domain lookup	# Habilita el enrutamiento ipv6
	# Deshabilita la traducción de nombre a dirección basado en DNS
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #	#Establece mensaje de bienvenida
line con 0	# se ingresa al modo de consola en línea 0
exec-timeout 0 0	# Establece el tiempo de espera inactivo de la sesión remota
	# Evita los mensajes inesperados que aparecen en pantalla
logging synchronous	#Salimos del modo consola de la línea 0
exit	# Se configura la Vlan 8
vlan 8	# Se asigna al nombre a la Vlan según las VRF
name General-Users	# Salimos de la configuración de Vlan 8
exit	# Se configura la Vlan 13
vlan 13	# Se asigna al nombre a la Vlan según las VRF
name Special-Users	# Salimos de la configuración de la Vlan 13
exit	

Se configura de la misma manera el switch D2 y en el caso del switch A1 solo se configura la Vlan 8 de General-Users ya que este dispositivo solo pertenece a esta red.

## Switch D2

hostname D2	# asigna nombre el nombre correspondiente al Switch D2
ip routing	# permite configurar la tabla de enrutamiento principal
ipv6 unicast-routing	# Habilita el enrutamiento ipv6
no ip domain lookup	# Deshabilita la traducción de nombre a dirección basado en DNS
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #	# Establece mensaje de bienvenida
line con 0	# se ingresa al modo de consola en línea 0
exec-timeout 0 0	# Establece el tiempo de espera inactivo de la sesión remota
	# Evita los mensajes inesperados que aparecen en pantalla
logging synchronous	# Salimos del modo consola de la línea 0
exit	# Se configura la Vlan 8
vlan 8	

```

name General-Users # Se asigna al nombre a la Vlan según las VRF
exit # Salimos de la configuración de Vlan 8
vlan 13 # Se configura la Vlan 13
name Special-Users # Se asigna al nombre a la Vlan según las VRF
exit # Salimos de la configuración de la Vlan 13

```

## Switch A1

```

hostname A1 # asigna nombre el nombre correspondiente al
Switch A1

ipv6 unicast-routing # Habilita el enrutamiento ipv6
no ip domain lookup # Deshabilita la traducción de nombre a
dirección basada en DNS

banner motd # A1, ENCOR Skills Assessment, Scenario 2 #
line con 0 # se ingresa al modo de consola en línea 0
exec-timeout 0 0 # Establece el tiempo de espera inactivo de la
sesión remota

logging synchronous # Evita los mensajes inesperados que
aparecen en pantalla

exit # Salimos del modo consola de la línea 0
vlan 8 # Se configura la Vlan 8
name General-Users # Se asigna al nombre a la Vlan según las VRF
exit # Salimos de la configuración de Vlan 8

```

## 1.4 Configurar los parámetros básicos para cada dispositivo final

Ahora se procede a realizar la configuración inicial de cada una de las Pc, la cual corresponde a la asignación de las direcciones IP.

Tabla 1. Host PC 1

PC1	
IPV4	10.0.113.50
Mascara	255.255.255.0

<b>Default Gateway</b>	10.0.113.1
<b>IPV6</b>	2001:db8:acad:113::50/64

## PC 1

```

set pncname PC1 # Se asigna el nombre a la PC virtual
ip 10.0.113.50/24 10.0.113.1 # Se asigna la dirección Ipv4 y su default
                             gateway
ip 2001:db8:acad:113::50/64 # se asigna la dirección en Ipv6

```

Tabla 2. Host PC 2

<b>PC2</b>	
<b>IPv4</b>	10.0.213.50
<b>Mascara</b>	255.255.255.0
<b>Default Gateway</b>	10.0.213.1
<b>IPv6</b>	2001:db8:acad:213::50/64

## PC 2

```

set pncname PC2 # Se asigna el nombre a la PC virtual
ip 10.0.213.50/24 10.0.213.1 # Se asigna la dirección Ipv4 y su default
                             gateway
ip 2001:db8:acad:213::50/64 # se asigna la dirección en Ipv6

```

Tabla 3. Host PC 3

<b>PC3</b>	
<b>IPv4</b>	10.0.108.50

<b>Mascara</b>	255.255.255.0
<b>Default Gateway</b>	10.0.108.1
<b>IPv6</b>	2001:db8:acad:108::50/64

### PC 3

```

set pncname PC3 # Se asigna el nombre a la PC virtual
ip 10.0.108.50/24 10.0.108.1 # Se asigna la dirección Ipv4 y su default
                             gateway
ip 2001:db8:acad:108::50/64 # se asigna la dirección en Ipv6

```

Tabla 4. Host PC 4

PC4	
<b>IPv4</b>	10.0.208.50
<b>Mascara</b>	255.255.255.0
<b>Default Gateway</b>	10.0.208.1
<b>IPv6</b>	2001:db8:acad:208::50/64

### PC 4

```

set pncname PC4 # Se asigna el nombre a la PC virtual
ip 10.0.208.50/24 10.0.208.1 # Se asigna la dirección Ipv4 y su default
                             gateway
ip 2001:db8:acad:208::50/64 # se asigna la dirección en Ipv6

```

## 2. CONFIGURAR VRF Y RUTAS ESTÁTICAS

En esta parte de la evaluación de habilidades se procede a configurar VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF.

### 2.1. Configurar las dos VRF's y que soporten IPv4 e IPv6

Definimos las VRF's en cada uno de los enrutadores ejecutando los siguientes comandos en cada uno de los dispositivos.

#### Enrutadores R1, R2 y R3

```
vrf definition GeneralUsers          # Definimos la Vrf con el nombre
                                     GeneralUsers
address-family ipv4                  # Habilita Ipv4 en la Vrf General
                                     Users en el enrutador
address-family ipv6                  # Habilita Ipv6 en la Vrf General
                                     Users en el enrutador
exit                                  # Salimos de la configuración de
                                     la Vrf GeneralUsers
vrf definition SpecialUsers          # Definimos la Vrf con el nombre
                                     SpecialUsers
address-family ipv4                  # Habilita Ipv4 en la Vrf
                                     SpecialUsers en el enrutador
address-family ipv6                  # Habilita Ipv6 en la Vrf
                                     SpecialUsers en el enrutador
exit                                  # Salimos de la configuración de
                                     la Vrf SpecialUsers
```

## 2.2. En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF según la tabla de direccionamiento

A continuación, se procede a realizar la asignación según el direccionamiento propuesto en la topología de las direcciones IPv4 e IPv6 en las interfaces respectivas para cada dirección.

- Configuramos las subinterfaces que conectan R1 y R2

### Enrutador R1

```
interface g2/0.1                                     # Se configura la subinterfaz indicada
encapsulation dot1q 13                               # permite que el enrutador tenga enlace troncal
                                                       por la vlan 13
vrf forwarding SpecialUsers                          # asocia la tabla de enrutamiento de
                                                       specialusers
ip address 10.0.12.1 255.255.255.0                  # configure la ipv4
ipv6 address fe80::1:1 link-local                    # configure link local
ipv6 address 2001:db8:acad:12::1/64                 # configure la ipv6
no shutdown                                          # levantamos a la interfaz
exit                                                 # Salimos de la subinterfaz
interface g2/0.2                                     # Se configura la subinterfaz indicada
encapsulation dot1q 8                               # permite que el enrutador tenga enlace
                                                       troncal por la vlan 8
vrf forwarding GeneralUsers                          # asocia la tabla de enrutamiento de
                                                       Generalusers
ip address 10.0.12.1 255.255.255.0                  # configure la ipv4
ipv6 address fe80::1:2 link-local                    # configure link local
ipv6 address 2001:db8:acad:12::1/64                 # configure la ipv6
no shutdown                                          # levantamos la interfaz
exit                                                 # Salimos de la subinterfaz
```

- Encendemos la interfaz G2/0, en R1

```
interface g2/0                                       # Entrar en el modo de configuración interface
no ip address                                        # se le dice que no va tener un ip
```

```
no shutdown # levantamos la interfaz
exit # salimos de la interfaz
```

- Configuramos las subinterfaces que conectan R1 y D1

```
interface g1/0.1 # Se configura la subinterfaz indicada
encapsulation dot1q 13 # permite que el enrutador tenga enlace troncal
                    # por la vlan 13
vrf forwarding SpecialUsers # asocia la tabla de enrutamiento de
                             # specialusers
ip address 10.0.113.1 255.255.255.0 # configure la ipv4
ipv6 address fe80::1:3 link-local # configure link local
ipv6 address 2001:db8:acad:113::1/64 # configure la ipv6
no shutdown # levantamos a la interfaz
exit # Salimos de la subinterfaz
interface g1/0.2 # Se configura la subinterfaz indicada
encapsulation dot1q 8 # permite que el enrutador tenga enlace troncal
                    # por la vlan 8
vrf forward GeneralUsers # asocia la tabla de enrutamiento de
                           # Generalusers
ip address 10.0.108.1 255.255.255.0 # configure la ipv4
ipv6 address fe80::1:4 link-local # configure link local
ipv6 address 2001:db8:acad:108::1/64 # configure la ipv6
no shutdown # levantamos la interfaz
exit # Salimos de la subinterfaz
```

- Encendemos la interfaz G1/0, en R1

```
interface g1/0 # Entrar en el modo de configuración interface
no ip address # se le dice que no va tener un ip
no shutdown # levantamos la interfaz
exit # salimos de la interfaz
```

## Enrutador R2

- Configuramos las subinterfaces que conectan R1 y R2

```
interface g2/0.1 # Se configura la subinterfaz indicada
```

```

encapsulation dot1q 13                                # permite que el enrutador tenga enlace troncal
                                                       por la vlan 13

vrf forwarding SpecialUsers                            # asocia la tabla de enrutamiento de
                                                       specialusers

ip address 10.0.12.2 255.255.255.0                   # configure la ipv4
ipv6 address fe80::2:1 link-local                     # configure link local
ipv6 address 2001:db8:acad:12::2/64                  # configure la ipv6
no shutdown                                           # levantamos a la interfaz
exit                                                  # Salimos de la subinterfaz

interface g2/0.2                                       # Se configura la subinterfaz indicada
encapsulation dot1q 8                                 # permite que el enrutador tenga enlace troncal
                                                       por la vlan 8

vrf forwarding GeneralUsers                            # asocia la tabla de enrutamiento de
                                                       Generalusers

ip address 10.0.12.2 255.255.255.0                   # configure la ipv4
ipv6 address fe80::2:2 link-local                     # configure link local
ipv6 address 2001:db8:acad:12::2/64                  # configure la ipv6
no shutdown                                           # levantamos la interfaz
exit                                                  # Salimos de la subinterfaz

```

- Encendemos la interfaz G2/0 en R2

```

interface g2/0                                        # Entrar en el modo de configuración interface
no ip address                                         # se le dice que no va tener un ip
no shutdown                                           # levantamos la interfaz
exit                                                  # salimos de la interfaz

```

- Configuramos las subinterfaces que conectan R2 y R3

```

interface g1/0.1                                       # Se configura la subinterfaz indicada
encapsulation dot1q 13                                 # permite que el enrutador tenga enlace troncal
                                                       por la vlan 13

vrf forwarding SpecialUsers                            # asocia la tabla de enrutamiento de
                                                       specialusers

ip address 10.0.23.2 255.255.255.0                   # configure la ipv4
ipv6 address fe80::2:3 link-local                     # configure link local
ipv6 address 2001:db8:acad:23::2/64                  # configure la ipv6
no shutdown                                           # levantamos a la interfaz
exit                                                  # Salimos de la subinterfaz

```

```

interface g1/0.2
encapsulation dot1q 8

vrf forwarding GeneralUsers

ip address 10.0.23.2 255.255.255.0
ipv6 address fe80::2:4 link-local
ipv6 address 2001:db8:acad:23::2/64
no shutdown
exit

```

# Se configura la subinterfaz indicada  
# permite que el enrutador tenga enlace troncal por la vlan 8  
# asocia la tabla de enrutamiento de Generalusers  
# configure la ipv4  
# configure link local  
# configure la ipv6  
# levantamos la interfaz  
# Salimos de la subinterfaz

- Encendemos la interfaz G1/0 en R2

```

interface g1/0
no ip address
no shutdown
exit

```

# Entrar en el modo de configuración interface  
# se le dice que no va tener un ip  
# levantamos la interfaz

## Enrutador R3

- Configuramos las subinterfaces que conectan R2 y R3

```

interface g1/0.1
encapsulation dot1q 13
por

vrf forwarding SpecialUsers

ip address 10.0.23.3 255.255.255.0
ipv6 address fe80::3:1 link-local
ipv6 address 2001:db8:acad:23::3/64
no shutdown
exit

interface g1/0.2
encapsulation dot1q 8

vrf forwarding GeneralUsers

ip address 10.0.23.3 255.255.255.0

```

# Se configura la subinterfaz indicada  
# permite que el enrutador tenga enlace troncal la vlan 13  
# asocia la tabla de enrutamiento de specialusers  
# configure la ipv4  
# configure link local  
# configure la ipv6  
# levantamos a la interfaz  
# Salimos de la subinterfaz

# Se configura la subinterfaz indicada  
# permite que el enrutador tenga enlace troncal por la vlan 8  
# asocia la tabla de enrutamiento de Generalusers  
# configure la ipv4

```

ipv6 address fe80::3:2 link-local          # configure link local
ipv6 address 2001:db8:acad:23::3/64      # configure la ipv6
no shutdown                               # levantamos la interfaz
exit                                      # Salimos de la subinterfaz

```

- Encendemos la interfaz G1/0 en R1

```

interface g1/0                            # Entrar en el modo de configuración interface
no ip address                             # se le dice que no va tener un ip
no shutdown                               # levantamos la interfaz
exit                                      # salimos de la subinterfaz

```

- Configuramos las subinterfaces que conectan R3 y D2

```

interface g2/0.1                          # Se configura la subinterfaz indicada
encapsulation dot1q 13                   # permite que el enrutador tenga enlace troncal
                                          # por la vlan 13
vrf forwarding SpecialUsers              # asocia la tabla de enrutamiento de
                                          # specialusers
ip address 10.0.213.1 255.255.255.0      # configure la ipv4
ipv6 address fe80::3:3 link-local        # configure link local
ipv6 address 2001:db8:acad:213::1/64     # configure la ipv6
no shutdown                              # levantamos a la interfaz
exit                                      # Salimos de la subinterfaz
interface g2/0.2                          # Se configura la subinterfaz indicada
encapsulation dot1q 8                   # permite que el enrutador tenga enlace troncal
                                          # por la vlan 8
vrf forward GeneralUsers                 # asocia la tabla de enrutamiento de
                                          # Generalusers
ip address 10.0.208.1 255.255.255.0     # configure la ipv4
ipv6 address fe80::3:4 link-local        # configure link local
ipv6 address 2001:db8:acad:208::1/64     # configure la ipv6
no shutdown                              # levantamos la interfaz
exit                                      # Salimos de la subinterfaz

```

- Encendemos la interfaz G2/0 en R2

```

interface g2/0                                # Entrar en el modo de configuración interface
no ip address                                  # se le dice que no va tener un ip
no shutdown                                    # levantamos la interfaz
exit                                            # salimos de la interfaz

```

### 2.3. Verificación del direccionamiento IPv4 e IPv6 de las interfaces

Figura 3. Verificación VRF R1 comando show ip vrf Interface

```

R1#sh ip vrf int
Interface      IP-Address      VRF              Protocol
Gi1/0.2        10.0.108.1      GeneralUsers      up
Gi2/0.2        10.0.12.1       GeneralUsers      up
Gi1/0.1        10.0.113.1     SpecialUsers      up
Gi2/0.1        10.0.12.1       SpecialUsers      up
R1#

```

Fuente: Autoría Propia

Figura 4. Verificación VRF R2 comando show ip vrf Interface

```

R2#sh ip vrf int
Interface      IP-Address      VRF              Protocol
Gi2/0.2        10.0.12.2       GeneralUsers      up
Gi1/0.2        10.0.23.2       GeneralUsers      up
Gi2/0.1        10.0.12.2       SpecialUsers      up
Gi1/0.1        10.0.23.2       SpecialUsers      up
R2#

```

Fuente: Autoría Propia

Figura 5. Verificación VRF R3 comando show ip vrf Interface

```
R3#sh ip vrf int
Interface      IP-Address      VRF              Protocol
Gi1/0.2       10.0.23.3       GeneralUsers      up
Gi2/0.2       10.0.208.1     GeneralUsers      up
Gi1/0.1       10.0.23.3       SpecialUsers      up
Gi2/0.1       10.0.213.1     SpecialUsers      up
R3#
```

Fuente: Autoría Propia

## 2.4. Configuración de rutas estáticas

A continuación, se procede a realizar la configuración del enrutamiento estático en cada uno de los enrutadores indicando los saltos que se deben dar de acuerdo al destino que se quiere llegar, en los Routers 1 y 2 configuramos rutas estáticas de último recurso cuando no se encuentre entrada en la tabla de enrutamiento.

### Enrutador R1

```
ip route vrf SpecialUsers 0.0.0.0 0.0.0.0 10.0.12.2      #Se define la dirección ipv4 como último
                                                         recurso para SpecialUsers
ip route vrf GeneralUsers 0.0.0.0 0.0.0.0 10.0.12.2      #Se define la dirección ipv4 como último
                                                         recurso para GeneralUsers
ipv6 route vrf SpecialUsers ::/0 2001:db8:acad:12::2     #Se define la dirección ipv6 como último
                                                         recurso para SpecialUsers
ipv6 route vrf GeneralUsers ::/0 2001:db8:acad:12::2     #Se define la dirección ipv6 como último
                                                         recurso para GeneralUsers
end                                                         #Salimos de la configuración del enrutador R1
```

### Enrutador R3

```
ip route vrf SpecialUsers 0.0.0.0 0.0.0.0 10.0.23.2     #Se define la dirección ipv4 como último
                                                         recurso para SpecialUsers
```

```

ip route vrf GeneralUsers 0.0.0.0 0.0.0.0 10.0.23.2      #Se define la dirección ipv4 como último
                                                         recurso para GeneralUsers

ipv6 route vrf SpecialUsers ::/0 2001:db8:acad:23::2    #Se define la dirección ipv6 como último
                                                         recurso para SpecialUsers

ipv6 route vrf GeneralUsers ::/0 2001:db8:acad:23::2    #Se define la dirección ipv6 como último
                                                         recurso para GeneralUsers

end                                                       #Salimos de la configuración del enrutador

```

Configuramos el enrutamiento estático para el enrutador R2, especificando el siguiente salto para el destino especificado.

## Enrutador R2

```

ip route vrf SpecialUsers 10.0.113.0 255.255.255.0 10.0.12.1 # Los paquetes con destino a la red
                                                         10.0.113.0 se envían por 10.0.12.1

ip route vrf SpecialUsers 10.0.213.0 255.255.255.0 10.0.23.3 #Los paquetes con destino a la red
                                                         10.0.213.0 se envían por 10.0.23.3

ipv6 route vrf SpecialUsers 2001:db8:acad:113::/64 2001:db8:acad:12::1 # Los paquetes con destino a la red
                                                         2001:db8:acad:113::/ se envían por
                                                         2001:db8:acad:12::1

ipv6 route vrf SpecialUsers 2001:db8:acad:213::/64 2001:db8:acad:23::3 # Los paquetes con destino a la red
                                                         2001:db8:acad:213::/ se envían por
                                                         2001:db8:acad:23::3

ip route vrf GeneralUsers 10.0.108.0 255.255.255.0 10.0.12.1 # Los paquetes con destino a la red
                                                         10.0.108.0 se envían por 10.0.12.1

ip route vrf GeneralUsers 10.0.208.0 255.255.255.0 10.0.23.3 # Los paquetes con destino a la red
                                                         10.0.208.0 se envían por 10.0.23.3

ipv6 route vrf GeneralUsers 2001:db8:acad:108::/64 2001:db8:acad:12::1 # Los paquetes con destino a la red
                                                         2001:db8:acad:108::/ se envían por
                                                         2001:db8:acad:12::1

ipv6 route vrf GeneralUsers 2001:db8:acad:208::/64 2001:db8:acad:23::3 # Los paquetes con destino a la red
                                                         2001:db8:acad:208::/ se envían por
                                                         2001:db8:acad:23::3

end                                                       # Salimos de la configuración del
                                                         router

```

## 2.4. Verificar conectividad en cada VRF

Se ejecutan los siguientes comandos desde enrutador R1 para verificar conectividad por IPV4 y IPV6 hasta el enrutador R3.

```
ping vrf GeneralUsers 10.0.208.1
```

```
ping vrf GeneralUsers 2001:db8:acad:208::1
```

```
ping vrf SpecialUsers 10.0.213.1
```

```
ping vrf SpecialUsers 2001:db8:acad:213::1
```

Figura 6. Verificar conectividad

```
R1#ping vrf GeneralUsers 10.0.208.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/62/72 ms
R1#ping vrf GeneralUsers 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 = 48/61/104 ms
R1#ping vrf SpecialUsers 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 = 68/71/72 ms
R1#ping vrf SpecialUsers 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 = 48/62/104 ms
```

Fuente: Autoría Propia

### 3. CONFIGURACIÓN DE LOS DISPOSITIVOS DE CAPA 2

Una vez se realiza la configuración de los dispositivos de enrutamiento procedemos a realizar la configuración de los dispositivos correspondientes a capa 2, los cuales se encargarán de dirigir los paquetes de acuerdo a la MAC del dispositivo al cual están conectados.

#### 3.1. Desactivar todas las interfaces en D1, D2, y A1

Antes de comenzar con la configuración de las interfaces de los dispositivos empezamos apagando todas las interfaces de cada dispositivo.

##### Switch D1

```
int r g0/0-3, g1/0-3, g2/0-3, g3/0-3      # Accedemos a las interfaces
shutdown                                  # Apagamos las interfaces
exit
```

##### Switch D2

```
int r g0/0-3, g1/0-3, g2/0-3, g3/0-3      # Accedemos a las interfaces
shutdown                                  # Apagamos las interfaces
exit
```

##### Switch A1

```
int r e0/0-3, e1/0-3, e2/0-3, e3/0-3      # Accedemos a las interfaces
shutdown                                  # Apagamos las interfaces
exit
```

#### 3.2. En D1 y D2, configurar los enlaces troncales a R1 y R3

Configuraremos la conexión de los dispositivos de Capa 2, con los respectivos enrutadores con los que tienen conexión dado que estamos utilizando VLAN y es

necesario la creación de los enlaces troncales para que estos puedan funcionar correctamente, para ello estaremos utilizando los siguientes comandos.

### Switch D1

```
interface g0/2                                #Accedemos a la interfaz
switchport trunk encapsulation dot1q         #Debemos establecer la encapsulación
switchport mode trunk                         #Establecemos el modo del enlace
no shutdown                                   #Levantamos la interfaz
exit                                           #Salimos de la configuración de la interfaz
```

### Switch D2

```
interface g1/0                                #Accedemos a la interfaz
switchport trunk encapsulation dot1q         #Debemos establecer la encapsulación
switchport mode trunk                         #Establecemos el modo del enlace
no shutdown                                   #Levantamos la interfaz
exit                                           #Salimos de la configuración de la interfaz
```

### 3.3. En D1 y A1, configurar el EtherChannel

Procedemos a configurar el EtherChannel entre los switches D1 y A1 en las interfaces respectivas en los equipos, así de esta manera se proporciona para estos un mayor ancho de banda de comunicación lo cual permite que aunque alguno de los enlaces físicos falle este funcione mientras al menos uno se encuentre conectado.

### Switch D1

```
interface range g0/1, g0/3                    #Accedemos a las interfaces respectivas
switchport trunk encapsulation dot1q         #Establecemos la encapsulación
switchport mode trunk                         #Establecemos el modo de Acceso
channel-group 1 mode desirable                #Establecemos el modo de comunicación del
                                              EtherChannel
no shutdown                                   #Encendemos la interfaz
exit                                           #Salimos de la configuración de la interfaz
```

## Switch A1

```
interface range e0/0, e0/2          #Accedemos a las interfaces respectivas
switchport trunk encapsulation dot1q #Establecemos la encapsulación
switchport mode trunk              #Establecemos el modo de Acceso
channel-group 1 mode desirable      #Establecemos el modo de comunicación del
                                    EtherChannel
no shutdown                          #Encendemos la interfaz
exit                                  #Salimos de la configuración de la interfaz
```

### 3.4. En D1, D2, y A1, Se configuran las interfaces de acceso para PC1, PC2, PC3, y PC4

Ahora se realizará la configuración de los interfaces correspondientes conectados a los dispositivos finales y en la Vlan correspondiente, en nuestro escenario corresponden a las Virtual PC.

## Switch D1

```
interface g0/0                      #Accedemos a la interfaz requerida
switchport mode access              #Establecemos el modo de acceso
switchport access vlan 13           #Establecemos la Vlan
spanning-tree portfast              #Configuramos el modo de reenvío
no shutdown                          #Levantamos la interfaz
exit                                  #Salimos de la configuración
```

## Switch D2

```
interface g0/0                      #Accedemos a la interfaz requerida
switchport mode access              #Establecemos el modo de acceso
switchport access vlan 13           #Establecemos la Vlan
spanning-tree portfast              #Configuramos el modo de reenvío
no shutdown                          #Levantamos la interfaz
exit                                  #Salimos de la configuración
```

```
interface g2/0                      #Accedemos a la interfaz requerida
switchport mode access              #Establecemos el modo de acceso
switchport access vlan 8            #Establecemos la Vlan
```

```
spanning-tree portfast
no shutdown
exit
```

```
#Configuramos el modo de reenvío
#Levantamos la interfaz
#Salimos de la configuración
```

## Switch A1

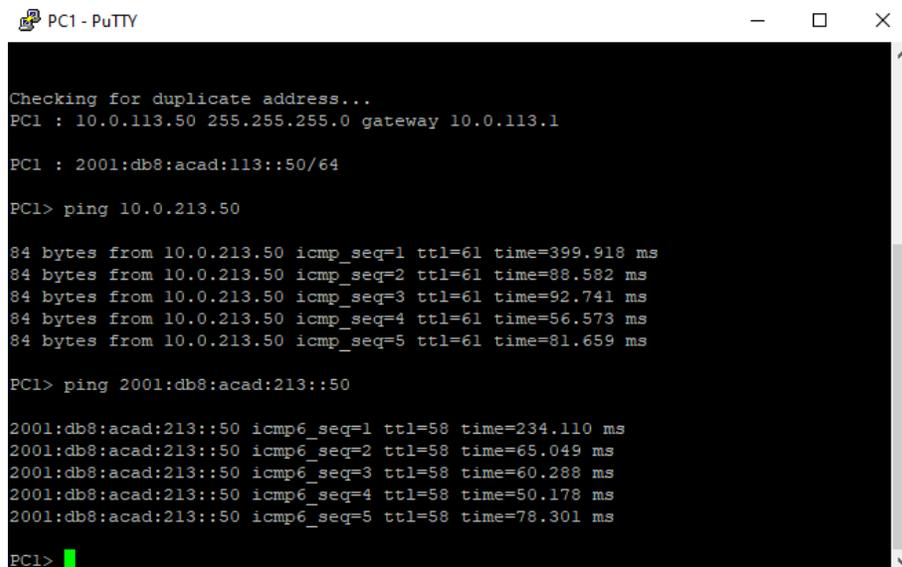
```
interface e0/1
switchport mode access
switchport access vlan 8
spanning-tree portfast
no shutdown
exit
```

```
#Accedemos a la interfaz requerida
#Establecemos el modo de acceso
#Establecemos la Vlan
#Configuramos el modo de reenvío
#Levantamos la interfaz
#Salimos de la configuración
```

### 3.5. Verificar la conectividad PC a PC

Ahora para verificar que nuestra configuración se realizó correctamente procedemos a comprobar la conectividad entre los dispositivos finales correspondientes a cada Vlan y grupo de usuarios, a continuación, se realiza la prueba entre a PC1 y PC2 correspondientes al grupo de “SpecialUsers” en la Vlan 13.

Figura 7. Ping PC1 a PC2



```
PC1 - PuTTY
Checking for duplicate address...
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=399.918 ms
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=88.582 ms
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=92.741 ms
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=56.573 ms
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=81.659 ms

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

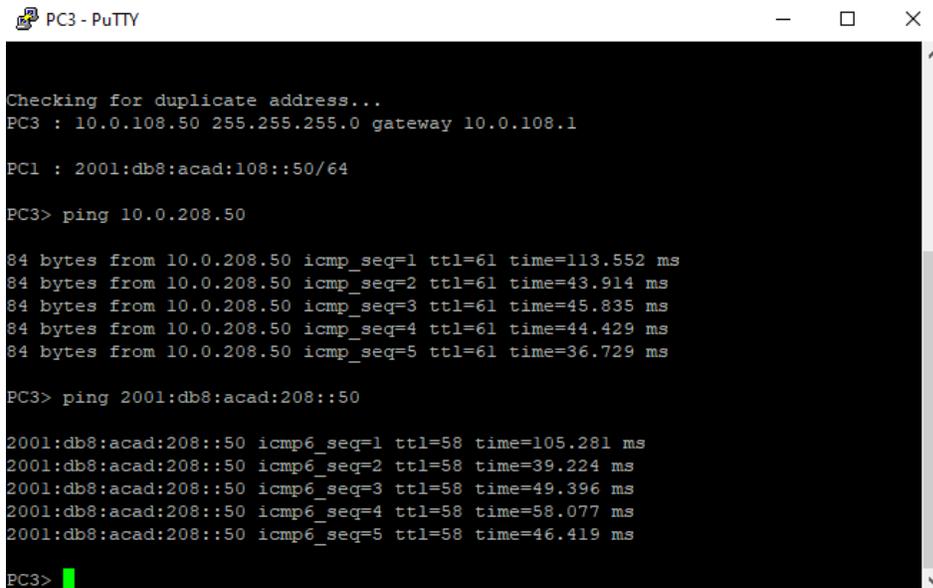
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=234.110 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=65.049 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=60.288 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=50.178 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=78.301 ms

PC1>
```

Fuente: Autoría Propia

Ahora procedemos a realizar la prueba de conectividad entre la PC3 a PC4 correspondiente al grupo de “GeneralUsers” en la Vlan 8.

Figura 8. Ping PC3 a PC4



```
PC3 - PuTTY
Checking for duplicate address...
PC3 : 10.0.108.50 255.255.255.0 gateway 10.0.108.1

PC1 : 2001:db8:acad:108::50/64

PC3> ping 10.0.208.50

84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=113.552 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=43.914 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=45.835 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=44.429 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=36.729 ms

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

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=105.281 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=39.224 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=49.396 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=58.077 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=46.419 ms

PC3>
```

Fuente: Autoría Propia

## 4. CONFIGURAR SEGURIDAD

Para finalizar la configuración del escenario se procede a culminar con la configuración de seguridad para restringir el acceso a la configuración de los dispositivos, esto se realiza con la finalidad de proteger el acceso no deseado a la configuración de los dispositivos.

### 4.1. En todos los equipos configurar, el modo EXEC privilegiado

```
enable algorithm-type scrypt secret cisco12345cisco # Se establece la contraseña para la configuración
```

### 4.2. En todos los equipos, se crea una cuenta para un usuario local

```
username admin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

#Creamos un usuario local junto con su contraseña

### 4.3. En todos los equipos, activar AAA y activar la autenticación AAA

```
aaa new-model
```

#Creamos el modelo

```
aaa authentication login default local
```

#Establecemos la autenticación

## CONCLUSIONES

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

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

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

Se configura correctamente cada uno de los dispositivos planteados en la prueba de habilidades específicas, cumpliendo así con cada uno de los objetivos propuestos en el escenario planteado, quedando en evidencia que se logro adquirir la capacidad adecuada para el desarrollo de una red.

## BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.  
<https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101.  
<https://1drv.ms/b/s!AmIJYeiNT1InMfy2rhPZHwEoWx>

UNAD (2015). Switch CISCO -Procedimientos de instalación y configuración del IOS [OVA]. <https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dq>