

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES  
PRÁCTICAS CCNP

FRANCIS JAVIER MURILLO PEREA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
CCAV QUIBDÓ

2022

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FRANCIS JAVIER MURILLO PEREA

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

DIRECTOR:

MSc. HECTOR JULIAN PARRA MOGOLLON

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

CCAV QUIBDÓ

2022

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

QUIBDÓ, 26 de junio de 2022

## **AGRADECIMIENTOS**

En primer Lugar, quiero agradecer a mis padres por brindarme la oportunidad de estudiar una Carrera tan maravillosa y llena de sorpresas como lo es la ingeniería de telecomunicaciones, a tutores y compañeros quien con sus conocimientos y apoyo me orientaron a través de cada una de las etapas de este proyecto para alcanzar los resultados que se requerían para estas prácticas.

También quiero agradecer a la Universidad Nacional Abierta y a Distancia (UNAD) por brindarme todos los recursos y herramientas necesarias para llevar a cabo el proceso y el desarrollo de este curso y por último, quiero agradecer a todos mis compañeros y a mi familia, por todo el apoyo moral brindado.

## CONTENIDO

<b>NOTA DE ACEPTACIÓN</b> .....	3
<b>AGRADECIMIENTOS</b> .....	4
<b>CONTENIDO</b> .....	4
<b>LISTA DE TABLAS</b> .....	6
<b>TABLA DE FIGURAS</b> .....	7
<b>GLOSARIO</b> .....	8
<b>RESUMEN</b> .....	9
<b>ABSTRACT</b> .....	9
<b>INTRODUCCION</b> .....	10
<b>DESARROLLO</b> .....	11
<b>PARTE 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces</b> .....	12
<b>PARTE 2: Configurar vrf y rutas estáticas</b> .....	18
<b>2.1 Configuración vrf-lite y vrfs en r1, r2 y r3, como se muestra en la topología del diagrama</b> .....	19
<b>2.2 Configuración de las interfaces ipv4 y ipv6 en r1, r2 y r3 para cada vrf según la tabla de direccionamiento</b> .....	20
<b>2.3 Configuración de las rutas estáticas predeterminadas que apuntan a r2, en r1 y r3</b> .....	26
<b>2.4 Verificación de la conectividad en cada vrf</b> .....	28
<b>PARTE 3: Configurar capa 2</b> .....	29
<b>3.2 Configurar los enlaces troncales a r1 y r3 en d1 y d2</b> .....	31
<b>3.3 Configurar el etherchannel en d1 y a1</b> .....	31
<b>3.4 Configurar puertos de acceso para vpc1, vpc2, vpc3 y vpc4 en d1, d2 y a1</b> .....	32
<b>3.5 Verificación de la conectividad de pc a pc</b> .....	33
<b>PARTE 4: Configurar seguridad</b> .....	34
<b>4.2 En todos los dispositivos, cree una cuenta de usuario local</b> .....	35
<b>4.3 Habilite la autenticación aaa en todos los dispositivos</b> .....	36
<b>CONCLUSIONES</b> .....	39
<b>BIBLIOGRAFIA</b> .....	40

## LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento .....	12
Tabla 2. Código implementado para la configuración con la respectiva descripción.....	14
Tabla 3. Comando para guardar la configuración en los Routers y los Switches .....	16
Tabla 4. Configuración de los VPCs .....	16
Tabla 5. Validación de la configuración realizada en cada uno de los VPCs..	17
Tabla 6. Configurar VRF y rutas estáticas .....	18
Tabla 7. Crear estancias para VRF y rutas estáticas.....	19
Tabla 8. Configuración VRF-Lite y VRFs en R1, R2 y R3.....	20
Tabla 9. Configuración de las direcciones IP para las sub-interfaces para la separación de las VRFs.....	21
Tabla 10. Rutas estáticas predeterminadas.....	26
Tabla 11. Deshabilitar interfaces en los Switches.....	29
Tabla 12. Deshabilitar interfaces en los Switches.....	30
Tabla 13. Configuración de enlaces troncales .....	31
Tabla 14. Configuración de EtherChannel .....	31
Tabla 15. Configuración de puertos de acceso.....	32
Tabla 16. Configurar seguridad .....	34
Tabla 17. Configurar seguridad .....	35
Tabla 18. Configuración de usuario local.....	35
Tabla 19. Habilitar la autenticación AAA.....	36

## TABLA DE FIGURAS

Figura 1 - Escenario propuesto.....	11
Figura 2. Topología del escenario propuesto realizada en el software GNS3	12
Figura 3. Configuración ip VRF en R1 .....	27
Figura 4. Configuración ip VRF en R2 .....	27
Figura 5. Configuración ip VRF en R3 .....	27
Figura 6 . ping vrf General-Users 10.0.208.1 .....	28
Figura 7 . ping vrf General-Users 2001:db8:acad:208::1 .....	28
Figura 8. ping vrf Special-Users 10.0.213.1 .....	28
Figura 9. ping vrf Special-Users 2001:db8:acad:213::1 .....	29
Figura 10 . ping ipv4 ,ipv6 desde pc1 a pc2.....	33
Figura 11. ping ipv4 ,ipv6 desde pc3 a pc4.....	34
Figura 12. Nombre de usuario y la autenticación AAA en D1 .....	36
Figura 13. Nombre de usuario y la autenticación AAA en A1 .....	37
Figura 14. Nombre de usuario y la autenticación AAA en D2 .....	37
Figura 15. Nombre de usuario y la autenticación AAA en R1 .....	37
Figura 16. Nombre de usuario y la autenticación AAA en R2 .....	38
Figura 17. Nombre de usuario y la autenticación AAA en R3 .....	38

## GLOSARIO

**IPV6:** El Protocolo de Internet versión 6 o IPv6 (*Internet Protocol version 6*, en inglés) es una versión del Protocolo de Internet (IP). El Protocolo de Internet permite transmitir datos a través de una red a las direcciones IP (IPv4 o IPv6), que son las que identifican a los diferentes dispositivos conectados a Internet y permiten la comunicación entre ellos.

**IPV4:** IPv4 es el nombre del protocolo de Internet utilizado actualmente para las direcciones IP de los dominios. Estas direcciones IP se asignan automáticamente cuando se registra un dominio.

**ROUTER:** Un router es un dispositivo que ofrece una conexión Wi Fi, que normalmente está conectado a un módem y que envía información de Internet a tus dispositivos personales, como ordenadores, teléfonos o tablets. Los dispositivos que están conectados a Internet en tu casa conforman tu red de área local (LAN).

**VRF:** Las VRFs son principalmente utilizadas en la MPLS para aislar el tráfico de cada cliente, pero no se encuentra limitada a dicha tecnología. Cuando las VRFs son usadas en una red que no trabaja con MPLS, son llamadas VRF-Lite.

**VLAN :** Las **VLAN (Virtual LAN)**, o también conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física. El objetivo de usar VLAN en un entorno doméstico o profesional, es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN gracias a un dispositivo L3 como un router o un switch multicapa L3.

## **RESUMEN**

En el presente trabajo se desarrollaron habilidades y prácticas para comprender la importancia de las redes de telecomunicación con tecnología CISCO CCNP y está enfocado en la configuración correcta de sus dispositivos con el fin de establecer comunicación entre Routers y switches por medio de las aplicaciones como GNS3, SOLAR WINDS, imágenes de simulación IOS de los Router CISCO y diversos códigos fuentes de programación para generar el correcto funcionamiento de la topología.

Cabe destacar la importancia de la certificación CCNP Cisco en el día a día de una compañía que se centra en la formación y seguridad de su información. Nosotros como estudiantes al obtener esta certificación ampliamos nuestras habilidades, conocimientos y capacidad de diseño, implementación, configuración y solución de problemas de Cisco como también la colaboración y comunicaciones unificadas de aplicaciones, dispositivos y redes.

Palabras Clave: CISCO, CCNP, Comunicación, Seguridad, Enrutamiento, Redes, Router, CCNP Cisco.

## **ABSTRACT**

In the present work, skills and practices were developed to understand the importance of telecommunication networks with CISCO CCNP technology and is focused on the correct configuration of their devices in order to establish communication between routers and switches through applications such as GNS3, SOLAR. WINDS, IOS simulation images of CISCO Routers and various programming source codes to generate the correct operation of the topology.

It is worth noting the importance of the CCNP Cisco certification in the day-to-day of a company that focuses on the training and security of its information. As students, by obtaining this certification, we expand our skills, knowledge, and capacity for Cisco design, implementation, configuration, and troubleshooting, as well as collaboration and unified communications for applications, devices, and networks.

CISCO, CCNP, Communication, Security, Routing, Networks, Router, CCNP Cisco.

## **INTRODUCCION**

Este Diplomado nos permite comprender los criterios de selección de dispositivos de red y tecnologías WAN para el cumplimiento de los requisitos objetivo. Los estudiantes aprenderemos a configurar el equipamiento de red necesario y cómo solucionar incidencias relacionadas con los protocolos de la capa de enlace de datos.

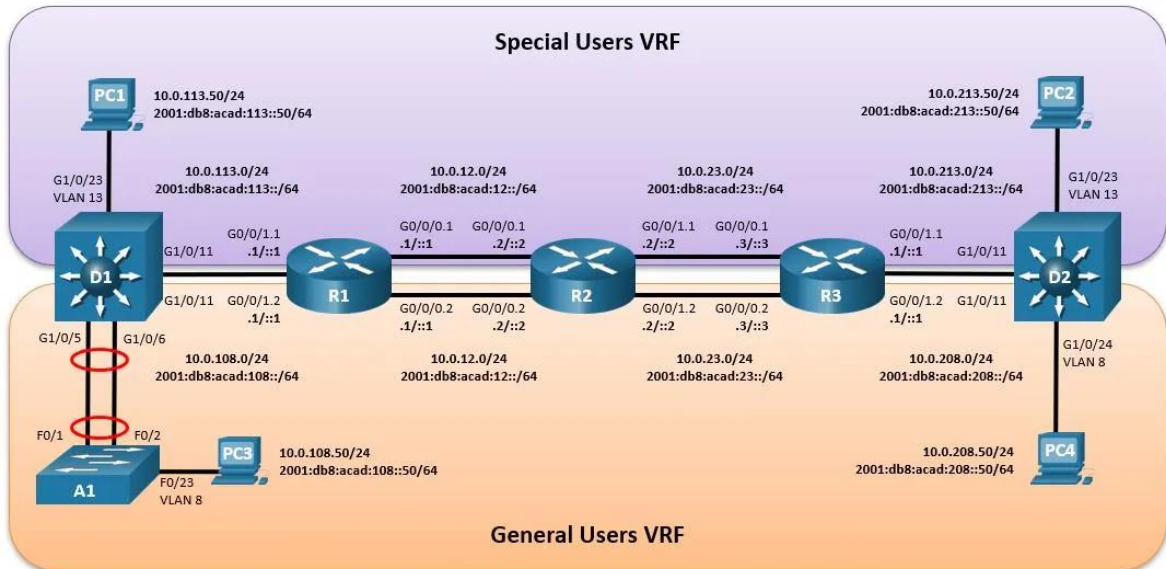
El presente trabajo se basa en la profundización de configuraciones de Routing and Switching de Cisco se centra en las tecnologías de switching y las operaciones de router que admiten redes empresariales pequeñas a medianas, incluidas las redes de área local y otros conceptos de seguridad.

En este diplomado veremos una serie programaciones de CCNA y se realizará la configuración básica de redes empresariales y a la solución de problemas que identificará y mitigará las amenazas de seguridad de telecomunicaciones pequeñas, medianas o grandes.

# DESARROLLO

## ESCENARIO PROPUESTO (Escenario2)

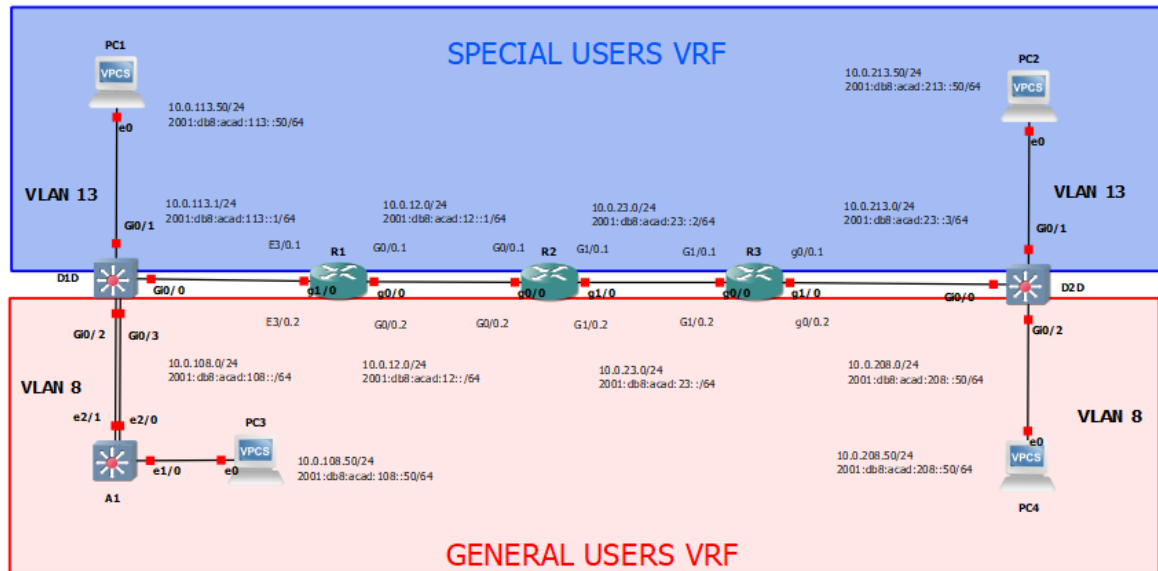
Figura 1 - escenario propuesto



Autoría- Guía avance documento final CCNP

**Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces.**

Figura 2. Topología del escenario propuesto realizada en el software GNS3



*Autoría- Propia*

Tabla 1. Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
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

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
	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	G1/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G1/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G0/0.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G0/0.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
vPC1	NIC	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
vPC2	NIC	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
vPC3	NIC	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
vPC4	NIC	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

*Fuente: Guía avance documento final CCNP*

Tabla 2. Código implementado para la configuración con la respectiva descripción

Configuración de R1	
Comando	Descripción
hostname R1 ipv6 unicast-routing no ip domain lookup banner motd # R1, ENCOR Skills Assessment, Scenario 2 #  line con 0 exec-timeout 0 0 logging synchronous exit	Nombre del host Habilita el routing IPv6. Desactiva la búsqueda DNS. Configuración del MOTD Banner.   Configuración de consola
Configuración de R2	
hostname R2 ipv6 unicast-routing no ip domain lookup banner motd # R2, ENCOR Skills Assessment, Scenario 2 #  line con 0 exec-timeout 0 0 logging synchronous exit	Nombre del host Habilita el routing IPv6. Desactiva la búsqueda DNS. Configuración del MOTD Banner.   Configuración de consola
Configuración de R3	
hostname R3 ipv6 unicast-routing no ip domain lookup banner motd # R3, ENCOR Skills Assessment, Scenario 2 #  line con 0 exec-timeout 0 0 logging synchronous exit	Nombre del host Habilita el routing IPv6. Desactiva la búsqueda DNS. Configuración del MOTD Banner.   Configuración de consola

Configuración de SWITCH – D1	
<pre>hostname D1 ip routing ipv6 unicast-routing no ip domain lookup  banner motd # D1, ENCOR Skills Assessment, Scenario 2 #  vlan 8 name General-Users exit  vlan 13 name Special-Users exit</pre>	<p>Se le asigna el nombre al dispositivo. Se habilita el routing IPv6. Se desactiva la búsqueda DNS.</p> <p>Configuración del MOTD Banner</p> <p>Se crea la VLAN 8 – General Users</p> <p>Se crea la VLAN 13 - Special Users</p>
Configuración de SWITCH – D2	
<pre>hostname D2 ip routing ipv6 unicast-routing no ip domain lookup  banner motd # D2, ENCOR Skills Assessment, Scenario 2 #  vlan 8 name General-Users exit  vlan 13 name Special-Users exit</pre>	<p>Se le asigna el nombre al dispositivo. Se habilita el routing IPv6. Se desactiva la búsqueda DNS.</p> <p>Configuración del MOTD Banner</p> <p>Se crea la VLAN 8 – General Users</p> <p>Se crea la VLAN 13 - Special Users</p>

Configuración de SWITCH – A1	
hostname A1 ip routing ipv6 unicast-routing no ip domain lookup	Se le asigna el nombre al dispositivo. Se habilita el routing IPv6. Se desactiva la búsqueda DNS.
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #	Configuración del MOTD Banner
vlan 8 name General-Users exit	Se crea la VLAN 8 – General Users

Tabla 3. Comando para guardar la configuración en los Routers y los Switches

R1,R2,R3,D1,D2,A1
Se puede utilizar el comando “copy running-config startup-config “ o se puede abreviar y usar “wr”

*Fuente: Autoría propia*

Tabla 4. Configuración de los VPCs

VPC1	
ip 10.0.113.50/24 10.0.113.1	Asigna la dirección IPv4 y la puerta de enlace.
ip 2001:db8:acad:113::50/64 auto	Se le asigna la dirección IPv6.
save	Salvar la configuración
VPC2	
ip 10.0.213.50/24 10.0.213.1	Asigna la dirección IPv4 y la puerta de enlace.
ip 2001:db8:acad:213::50/64 auto	Se le asigna la dirección IPv6.
save	Salvar la configuración

VPC3	
ip 10.0.108.50/24 10.0.108.1	Asigna la dirección IPv4 y la puerta de enlace.
ip 2001:db8:acad:108::50/64 auto	Se le asigna la dirección IPv6.
save	Salvar la configuración
VPC4	
ip 10.0.208.50/24 10.0.208.1	Asigna la dirección IPv4 y la puerta de enlace.
ip 2001:db8:acad:208::50/64 auto	Se le asigna la dirección IPv6.
save	Salvar la configuración

Fuente: Autoría propia

Tabla 5. Validación de la configuración realizada en cada uno de los VPCs.

Para realizar este paso debemos ejecutar la consola del VPC y digitamos el comando "show"	
VPC1	<pre>PC1&gt; PC1&gt; show  NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PO RT PC1      10.0.113.50/24      10.0.113.1      00:50:79:66:68:03      20000      127.0.0. 1:20001           fe80::250:79ff:fe66:6803/64           2001:db8:acad:113::50/64</pre>
VPC2	<pre>PC2&gt; show  NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PO RT PC2      10.0.213.50/24      10.0.213.1      00:50:79:66:68:00      20004      127.0.0. 1:20005           fe80::250:79ff:fe66:6800/64           2001:db8:acad:213::50/64</pre>
VPC3	<pre>PC3&gt; show  NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PO RT PC3      10.0.108.50/24      10.0.108.1      00:50:79:66:68:01      20002      127.0.0. 1:20003           fe80::250:79ff:fe66:6801/64           2001:db8:acad:108::50/64</pre>

VPC4	<pre> PC4&gt; show  NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO RT PC4      10.0.208.50/24  10.0.208.1   00:50:79:66:68:02  20006  127.0.0. 1:20007           fe80::250:79ff:fe66:6802/64           2001:db8:acad:208::50/64 </pre>
------	--

*Fuente: Autoría propia*

## Parte 2: Configurar VRF y rutas estáticas.

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

Sus tareas de configuración son las siguientes:

Tabla 6. Configurar VRF y rutas estáticas

Tarea#	Tarea	Especificación
2.1	En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.	Configure dos VRF: <ul style="list-style-type: none"> <li>• Usuarios generales</li> <li>• Usuarios especiales</li> </ul> Los VRF deben admitir IPv4 e IPv6.
2.2	En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.	Todos los enrutadores utilizarán Router-On-A-Stick en sus interfaces G0/0/1.x para admitir la separación de los VRF. Sub-interfaz 1: <ul style="list-style-type: none"> <li>• En el VRF de Usuarios Especiales</li> <li>• Usar encapsulamiento dot1q 13</li> <li>• IPv4 e IPv6 GUA y direcciones link-local</li> </ul> Sub-interfaz 2: <ul style="list-style-type: none"> <li>• Habilitar las interfaces</li> <li>• En el VRF de Usuarios Generales</li> </ul>

Tarea#	Tarea	Especificación
		<ul style="list-style-type: none"> <li>• Usar encapsulamiento dot1q 8</li> <li>• IPv4 e IPv6 GUA y direcciones locales de enlace</li> <li>• Habilite las interfaces</li> </ul>
2.3	En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.	Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.
2.4	Verifique la conectividad en cada VRF.	<p>Desde R1, verifique la conectividad con R3:</p> <ul style="list-style-type: none"> <li>• ping vrf General-Users 10.0.208.1</li> <li>• ping vrf General-Users 2001:db8:acad:208::1</li> <li>• ping vrf Special-Users 10.0.213.1</li> <li>• ping vrf Special-Users 2001:db8:acad:213::1</li> </ul>

Fuente: Guía avance documento final CCNP

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

Tabla 7. Crear estancias para VRF y rutas estáticas

Para crear la estancia debemos ejecutar el siguiente comando en cada uno de los routers.	
Comando	Descripción
Vrf definition General-Users address-family ipv4 address-family ipv6 exit	Definición dentro de RED la Vrf Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.

vrf definition Special-Users address-family ipv4 address-family ipv6 exit	Definición dentro de RED la Vrf Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.
--	---

Fuente: Autoría propia

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

Tabla 8. Configuración VRF-Lite y VRFs en R1, R2 y R3

Configuración R1	
Comando	Descripción
Vrf definition General-Users address-family ipv4 address-family ipv6 exit	Definición Vrf dentro de la RED Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.
vrf definition Special-Users address-family ipv4 address-family ipv6 exit	Definición Vrf dentro de la RED Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.
Configuración R2	
Vrf definition General-Users address-family ipv4 address-family ipv6 exit	Definición Vrf dentro de la RED Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.
vrf definition Special-Users address-family ipv4 address-family ipv6 exit	Definición Vrf dentro de la RED Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.
Configuración R3	
Vrf definition General-Users address-family ipv4 address-family ipv6 exit	Definición Vrf dentro de la RED Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.

<pre>vrf definition Special-Users address-family ipv4 address-family ipv6 exit</pre>	Definición Vrf dentro de la RED Habilitación para Ipv4 Habilitación para Ipv6 Salir de esta configuración.
--	---

*Fuente: Autoría propia*

Tabla 9. Configuración de las direcciones IP para las sub-interfaces para la separación de las VRFs

R1	
Comando	Descripción
<pre>interface GigabitEthernet0/0.1 encapsulation dot1Q 13  vrf forwarding Special-Users ip address 10.0.12.1 255.255.255.0  ipv6 address FE80::1:1 link-local  ipv6 address 2001:DB8:ACAD:12::1/64  no shut</pre>	Sub interface G0/0.1 Encapsulamiento en protocolo IEEE 802.1Q Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users. Asignación de la dirección IPv4. Asignación de la dirección IPv6. Activación de la interfaz (mode Up)
<pre>interface GigabitEthernet0/0.2 encapsulation dot1Q 8  vrf forwarding General-Users  ip address 10.0.12.1 255.255.255.0  ipv6 address FE80::1:2 link-local ipv6 address 2001:DB8:ACAD:12::1/64  no shut</pre>	Sub interface G0/0.2 Encapsulamiento en protocolo IEEE 802.1Q Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users. Asignación de la dirección IPv4. Asignación de la dirección IPv6. Activación de la interfaz (mode Up)
<pre>interface G0/0 no ip address no shutdown exit</pre>	Interface G0/0 Sin dirección IP Activa la interfaz física(mode Up) Salir de esta configuración.

<pre>interface GigabitEthernet1/0.1 encapsulation dot1Q 13  vrf forwarding Special-Users  ip address 10.0.113.1 255.255.255.0  ipv6 address FE80::1:3 link-local ipv6 address 2001:DB8:ACAD:113::1/64  no shut</pre>	<p>Sub interface G1/0.1 Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p> <p>Activación de la interfaz (mode Up)</p>
<pre>interface GigabitEthernet1/0.2 encapsulation dot1Q 8  vrf forwarding General-Users  ip address 10.0.108.1 255.255.255.0  ipv6 address FE80::1:4 link-local ipv6 address 2001:DB8:ACAD:108::1/64  no shut</pre>	<p>Sub interface G1/0.2 Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p> <p>Activación de la interfaz (mode Up)</p>
<pre>interface g1/0 no ip address no shut</pre>	<p>Interface G1/0 Sin dirección IP Activa la interfaz física(mode Up)</p>
<b>Configuración R2</b>	
<pre>interface GigabitEthernet0/0.1 encapsulation dot1Q 13  vrf forwarding Special-Users  ip address 10.0.12.2 255.255.255.0  ipv6 address FE80::2:1 link-local ipv6 address 2001:DB8:ACAD:12::2/64</pre>	<p>Sub interface G0/0.1 Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p>

no shut	Activación de la interfaz (mode Up)
interface GigabitEthernet0/0.2 encapsulation dot1Q 8  vrf forwarding General-Users  ip address 10.0.12.2 255.255.255.0  ipv6 address FE80::2:2 link-local ipv6 address 2001:DB8:ACAD:12::2/64  no shut	Sub interface G0/0.2 Encapsulamiento en protocolo IEEE 802.1Q  Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.  Asignación de la dirección IPv4.  Asignación de la dirección IPv6.  Activación de la interfaz (mode Up)
interface GigabitEthernet1/0.1 encapsulation dot1Q 13  vrf forwarding Special-Users  ip address 10.0.23.2 255.255.255.0  ipv6 address FE80::2:3 link-local ipv6 address 2001:DB8:ACAD:23::2/64  no shut	Sub interface G1/0.1 Encapsulamiento en protocolo IEEE 802.1Q  Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.  Asignación de la dirección IPv4.  Asignación de la dirección IPv6.  Activación de la interfaz (mode Up)
interface g1/0 no ip address no shutdown exit	Interface G1/0 Sin dirección IP Activa la interfaz física(mode Up)

<pre>interface GigabitEthernet1/0.2 encapsulation dot1Q 8  vrf forwarding General-Users  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 shut</pre>	<p>Sub interface G1/0.1 Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p> <p>Activación de la interfaz (mode Up)</p>
<pre>interface g0/0 no ip address no shutdown exit</pre>	<p>Interface física Sin dirección IP Activa la interfaz física(mode Up)</p>
<b>Configuración R3</b>	
<pre>interface GigabitEthernet0/0.1 encapsulation dot1Q 13  vrf forwarding Special-Users  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 shut</pre>	<p>Sub interface Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p> <p>Activación de la interfaz (mode Up)</p>
<pre>interface GigabitEthernet0/0.2 encapsulation dot1Q 8  vrf forwarding General-Users  ip address 10.0.23.3 255.255.255.0  ipv6 address FE80::3:2 link-local ipv6 address 2001:DB8:ACAD:23::3/64  no shut</pre>	<p>Sub interface Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p> <p>Activación de la interfaz (mode Up)</p>

<pre>interface g1/0 no ip address no shut</pre>	<p>Interface física Sin dirección IP Activa la interfaz física(mode Up)</p>
<pre>interface GigabitEthernet1/0.1 encapsulation dot1Q 13  vrf forwarding Special-Users  ip address 10.0.213.1 255.255.255.0  ipv6 address FE80::3:3 link-local ipv6 address 2001:DB8:ACAD:213::1/64 no shut</pre>	<p>Sub interface Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p> <p>Activación de la interfaz (mode Up)</p>
<pre>interface g0/0 no ip address no shutdown exit</pre>	<p>Interface física Sin dirección IP Activa la interfaz física(mode Up)</p>
<pre>interface GigabitEthernet1/0.2 encapsulation dot1Q 8  vrf forwarding General-Users  ip address 10.0.208.1 255.255.255.0  ipv6 address FE80::3:4 link-local ipv6 address 2001:DB8:ACAD:208::1/64  no shut</pre>	<p>Sub interface Encapsulamiento en protocolo IEEE 802.1Q</p> <p>Se crea la instancia para la tabla de enrutamiento de la VFR Special-Users.</p> <p>Asignación de la dirección IPv4.</p> <p>Asignación de la dirección IPv6.</p> <p>Activación de la interfaz (mode Up)</p>

*Fuente: Autoría propia*

### 2.3 Configuración de las rutas estáticas predeterminadas que apuntan a R2, en R1 y R3.

Tabla 10. Rutas estáticas predeterminadas

R1	<pre> R1#show run   inc route ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2 ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.2 ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.2 ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2 ip route vrf Special-Users 10.0.23.0 255.255.255.0 10.0.12.2 ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.12.2 ipv6 route vrf Special-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2 ipv6 route vrf General-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2 ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:12::2 ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:12::2 ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2 ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2 R1# </pre>
R2	<pre> R2# R2#show run   inc route 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 R2# </pre>
R3	<pre> R3#show run   inc route ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.2 ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.2 ip route vrf Special-Users 10.0.12.0 255.255.255.0 10.0.23.2 ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.23.2 ipv6 route vrf Special-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2 ipv6 route vrf General-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2 ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::2 ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::2 R3# </pre>

Fuente: Autoría propia

Verificación del direccionamiento IP de las interfaces VRF creadas en cada Router.

Para verificar el direccionamiento IP de las VRFs, se utiliza el comando `show ip vrf interfaces`.

Figura 3. Configuración ip VRF en R1

```
R1#show ip vrf interfaces
Interface          IP-Address      VRF              Protocol
Gi0/0.2           10.0.12.1      General-Users    up
Gi1/0.2           10.0.108.1     General-Users    up
Gi0/0.1           10.0.12.1      Special-Users    up
Gi1/0.1           10.0.113.1     Special-Users    up
R1#
```

Fuente: Autoría propia

Figura 4. Configuración ip VRF en R2

```
R2#show ip vrf interfaces
Interface          IP-Address      VRF              Protocol
Gi0/0.2           10.0.12.2      General-Users    up
Gi1/0.2           10.0.23.2      General-Users    up
Gi0/0.1           10.0.12.2      Special-Users    up
Gi1/0.1           10.0.23.2      Special-Users    up
R2#
```

Fuente: Autoría propia

Figura 5. Configuración ip VRF en R3

```
R3#show ip vrf interfaces
Interface          IP-Address      VRF              Protocol
Gi0/0.2           10.0.23.3      General-Users    up
Gi1/0.2           10.0.208.1     General-Users    up
Gi0/0.1           10.0.23.3      Special-Users    up
Gi1/0.1           10.0.213.1     Special-Users    up
R3#
```

Fuente: Autoría propia

## 2.4 Verificación de la conectividad en cada VRF.

Esto se realiza enviando ping desde R1 a R3.

Figura 6 . ping vrf General-Users 10.0.208.1

```
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 = 40/71/116 ms
R1#
```

*Fuente: Autoría propia*

Figura 7 . ping vrf General-Users 2001:db8:acad:208::1

```
R1#ping vrf General-Users 2001:db8:acad:208::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/68/160 ms
R1#
```

*Fuente: Autoría propia*

Figura 8. ping vrf Special-Users 10.0.213.1

```
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 = 20/40/60 ms
R1#
```

*Fuente: Autoría propia*

Figura 9. ping vrf Special-Users 2001:db8:acad:213::1

```
R1#ping vrf Special-Users 2001:db8:acad:213::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/36/60 ms
R1#
```

Fuente: Autoría propia

### Parte 3. Configurar capa 2

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

Tabla 11. Deshabilitar interfaces en los Switches

Tarea#	Tarea	Especificación
3.1	En D1, D2 y A1, deshabilite todas las interfaces.	En D1 y D2, apague G1/0/1 a G1/0/24. En A1, apague F0/1 – F0/24, G0/1 – G0/2.
3.2	En D1 y D2, configure los enlaces troncales a R1 y R3.	Configure y habilite el enlace G1/0/11 como enlace troncal.
3.3	En D1 y A1, configure el EtherChannel.	En D1, configure y habilite: • Interfaz G1/0/5 y G1/0/6 • Canal de puerto 1 mediante PAgP En A1, configure habilitar: • Interfaz F0/1 y F0/2 • Canal de puerto 1 usando PAgP
3.4	En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.	Configure y habilite los puertos de acceso de la siguiente manera: • En D1, configure la interfaz G1/0/23 como puerto de acceso en VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/23 como puerto de acceso en VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/24 como puerto de acceso en

Tarea#	Tarea	Especificación
		VLAN 8 y habilite Portfast. • En A1, configure la interfaz F0/23 como puerto de acceso en VLAN 8 y habilite Portfast.
3.5	Verifique la conectividad de PC a PC.	Desde la PC1, verifique la conectividad IPv4 e IPv6 a la PC2. Desde la PC3, verifique la conectividad IPv4 e IPv6 a la PC4.

Fuente: Guía avance documento final CCNP

Tabla 12. Deshabilitar interfaces en los Switches

Configuración Switch - D1	
Comando	Descripción
interface range g0/0-3, g1/0-3, g2/0-3, g3/0-3 shutdown exit	Rango de todas las interfaces que contiene el Switch D1. Deshabilita todas las interfaces contenidas en el rango.
Configuración Switch D2	
interface range g0/0-3, g1/0-3, g2/0-3, g3/0-3 shutdown exit	Rango de todas las interfaces que contiene el Switch D2. Deshabilita todas las interfaces contenidas en el rango.
Configuración Switch A1	
interface range e2/0-3, e1/0-3, e2/0-3, e3/0-3 shutdown exit	Rango de todas las interfaces que contiene el Switch D2. Deshabilita todas las interfaces contenidas en el rango.

Fuente: Autoría propia

### 3.2 Configurar los enlaces troncales a R1 y R3 en D1 y D2.

Tabla 13. Configuración de enlaces troncales

Configuración Switch - D1	
Comando	Descripción
interface g0/0 switchport trunk encapsulation dot1q switchport mode trunk no shutdown exit	interfaz E0/1. Establece el modo de encapsulación del enlace troncal al estándar 802.1Q. Configura la interfaz a modo de enlace troncal. Activa la interfaz.
Configuración Switch – D2	
interface g0/0 switchport trunk encapsulation dot1q switchport mode trunk no shutdown exit	Configuración de la interfaz E0/1. Establece el modo de encapsulación del enlace troncal al estándar 802.1Q. Configura la interfaz a modo de enlace troncal. Activa la interfaz.

*Fuente: Autoría propia*

### 3.3 Configurar el EtherChannel en D1 y A1.

Tabla 14. Configuración de EtherChannel

Configuración Switch D1	
Comando	Descripción
interface range g0/2, g0/3  switchport trunk encapsulation dot1q  switchport mode trunk  channel-group 1 mode desirable  no shutdown exit	Rango de las interfaces g0/2 y G0/3. Establece el modo de encapsulación de los enlaces troncales al estándar 802.1Q. Configura las interfaces a modo de enlace troncal. Establece los puertos agrupados en modo activo, negociará el estado cuando reciba paquetes PAgP. Activación de las interfaces.
Configuración Switch A1	
interface range e2/1-2	Configuración de las interfaces E2/1 y E2/0.

switchport trunk encapsulation dot1q	<p>Establece el modo de encapsulación de los enlaces troncales al estándar 802.1Q.</p> <p>Configura las interfaces a modo de enlace troncal.</p> <p>Establece los puertos agrupados en modo activo, negociará el estado cuando reciba paquetes PAgP.</p> <p>Activación de las interfaces.</p>
switchport mode trunk	
channel-group 1 mode desirable	
no shutdown	
exit	

Fuente: Autoría propia

### 3.4 Configurar puertos de acceso para vPC1, vPC2, vPC3 y vPC4 en D1, D2 y A1.

Tabla 15. Configuración de puertos de acceso

Configuración Switch D1	
Comando	Descripción
interface g0/0	<p>Configuración de la interfaz g0/0. Establece el puerto en modo de acceso.</p> <p>Asigna al puerto la VLAN 8 y13. Habilita la protección BPDU en el puerto</p> <p>Se habilita PortFast.</p> <p>Activación de la interfaz.</p>
switchport mode access	
switchport access vlan 8,13	
spanning-tree portfast	
no shutdown	
exit	
Configuración Switch D2	
interface g1/0	<p>Configuración de la interfaz g1/0. Establece el puerto en modo de acceso.</p> <p>Asigna al puerto la VLAN 13. Habilita la protección BPDU en el puerto</p> <p>Se habilita PortFast.</p> <p>Activación de la interfaz.</p>
switchport mode Access	
switchport access vlan 13	
spanning-tree portfast	
no shutdown	
exit	
interface g0/2	<p>Configuración de la interfaz g0/2.</p>
switchport mode access	

switchport access vlan 8 spanning-tree portfast no shutdown exit	Establece el puerto en modo de acceso. Asigna al puerto la VLAN 8. Habilita la protección BPDU en el puerto con PortFast habilitado. Activación de la interfaz.
Configuración Switch A1	
interface e1/0 switchport mode Access  switchport access vlan 8 spanning-tree portfast no shutdown exit	Configuración de la interfaz e1/0. Establece el puerto en modo de acceso. Asigna al puerto la VLAN 8. Habilita PortFast habilitado. Activación de la interfaz.

*Fuente: Autoría propia*

### 3.5 Verificación de la conectividad de PC a PC.

*Verifique la conectividad de PC a PC.*

Figura 10 . ping ipv4 ,ipv6 desde pc1 a pc2

```

PC1>
PC1> ping 10.0.213.50/24

84 bytes from 10.0.213.50 icmp_seq=1 ttl=61 time=92.708 ms
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=59.119 ms
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=51.491 ms
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=62.717 ms
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=60.223 ms

PC1> ping 2001:db8:acad:213::50/64

2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=100.252 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=71.473 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=69.830 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=63.491 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=65.011 ms

```

*Fuente: Autoría propia*

Figura 11. ping ipv4 ,ipv6 desde pc3 a pc4

```

PC3> ping 10.0.208.50/24

84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=73.116 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=58.466 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=51.350 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=60.922 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=44.812 ms

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

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=156.200 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=62.026 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=58.897 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=60.862 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=59.501 ms
    
```

Fuente: Autoría propia

#### Parte 4. Configurar seguridad

En esta parte, configurará varios mecanismos de seguridad en los dispositivos de la topología.

Tabla 16. Configurar seguridad

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, modo EXE privilegiado seguro.	Configure un secreto de habilitación de la siguiente manera: <ul style="list-style-type: none"> <li>• Tipo de algoritmo: SCRYPT</li> <li>• Clave:cisco12345cisco.</li> </ul>
5.2	En todos los dispositivos, cree una cuenta de usuario local.	Configure un usuario local: <ul style="list-style-type: none"> <li>• Nombre:admin</li> <li>• Nivel de privilegio:15</li> <li>• Tipo de algoritmo: SCRYPT</li> <li>• Clave:cisco12345cisco.</li> </ul>
5.3	En todos los dispositivos, habilite AAA y habilite la autenticación AAA.	Habilite la autenticación AAA usando la base de datos local en todas las líneas.

Fuente: Guía avance documento final CCNP

Tabla 17. Configurar seguridad

Configuración R1	
Comando	Descripción
enable algorithm-type SCRYPT secret cisco12345cisco	Habilita el algoritmo de encriptado SCRYPT y la contraseña cisco12345cisco.
Configuración R2	
enable algorithm-type SCRYPT secret cisco12345cisco	Habilita el algoritmo de encriptado SCRYPT y la contraseña cisco12345cisco.
Configuración R3	
enable algorithm-type SCRYPT secret cisco12345cisco	Habilita el algoritmo de encriptado SCRYPT y la contraseña cisco12345cisco.
Configuración Switch - D1	
enable algorithm-type SCRYPT secret cisco12345cisco	Habilita el algoritmo de encriptado SCRYPT y la contraseña cisco12345cisco.
Configuración Switch - D2	
enable algorithm-type SCRYPT secret cisco12345cisco	Habilita el algoritmo de encriptado SCRYPT y la contraseña cisco12345cisco.
Configuración Switch A1	
enable algorithm-type SCRYPT secret cisco12345cisco	Habilita el algoritmo de encriptado SCRYPT y la contraseña cisco12345cisco.

Fuente: Autoría propia

#### 4.2 En todos los dispositivos, cree una cuenta de usuario local.

*Nota: Se usa el siguiente comando para todos los dispositivos.*

Tabla 18. Configuración de usuario local

Configuración en R1,R2,R3,D1,D2,A1	
Comando	Descripción
username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Configuración del nombre de usuario, nivel de privilegio 15 y contraseña secreta encriptada cisco12345cisco.

Fuente: Autoría propia

### 4.3 Habilite la autenticación AAA en todos los dispositivos.

*Nota: Se usa el siguiente comando para todos los dispositivos.*

*“aaa new-model”*

*“aaa authentication login default local”*

*“end”*

Tabla 19. Habilitar la autenticación AAA

Configuración en R1,R2,R3,D1,D2,A1	
Comando	Descripción
aaa new-model aaa authentication login default local end	Habilita el uso de listas para los métodos de autenticación. Activación predeterminada de inicio de sesión de autenticación AAA.

*Fuente: Autoría propia*

Verificación del nombre de usuario y la autenticación AAA.

Para verificar el nombre de usuario y la autenticación AAA, usamos el siguiente comando *“show run | include aaa|username”*

Figura 12. Nombre de usuario y la autenticación AAA en D1

```
D1>  
D1>en  
Password:  
D1#show run | include aaa|username  
username admin privilege 15 secret 9 $9$zt3qrqWadPm40o$ycEioFxb4VOSc6DqELUNdEQPS  
QADzhcbIxFR.hjWfEY  
aaa new-model  
aaa authentication login default local  
aaa session-id common  
D1#
```

*Fuente: Autoría propia*

Figura 13. Nombre de usuario y la autenticación AAA en A1

```
Username: admin
Password:

A1#show run | include aaa|username
username admin privilege 15 secret 4 PxFnRQHeDp9u3TLc8.Sw7QZ8GORUJ3TKPHA71beGWQs
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```

*Fuente: Autoría propia*

Figura 14. Nombre de usuario y la autenticación AAA en D2

```
D2>en
Password:
D2#show run | include aaa|username
username admin privilege 15 secret 9 $9$PSrm2H05.ZR0jI$Vcyme0dzvor5i7d568iX1ZxA
zkyuJRlxAqmPg5tLBU
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```

*Fuente: Autoría propia*

Figura 15. Nombre de usuario y la autenticación AAA en R1

```
Username: admin
Password:

R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 4 PxFnRQHeDp9u3TLc8.Sw7QZ8GORUJ3TKPHA71beGWQs
R1#
```

*Fuente: Autoría propia*

Figura 16. Nombre de usuario y la autenticación AAA en R2

```
Username: admin
Password:

R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 4 PxFnRQHeDp9u3TLc8.Sw7QZ8G0RUJ3TKPHA71beGWQs
R2#
```

*Fuente: Autoría propia*

Figura 17. Nombre de usuario y la autenticación AAA en R3

```
Username: admin
Password:

R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 4 PxFnRQHeDp9u3TLc8.Sw7QZ8G0RUJ3TKPHA71beGWQs
R3#
```

*Fuente: Autoría propia*

## CONCLUSIONES

Durante el desarrollo y las prácticas de este diplomado cisco CCNP, se ha logrado los conocimientos adquiridos en el diplomado de profundización cisco CCNP, por lo anterior se establecen la funcionalidad de los comandos detallados pasa a paso, lo cual hemos desarrollado tales como el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, ping vrf Special-Users, show ip route y entre otros que se pueden utilizar en la herramienta GNS3 o CISCO Packet tracer.

Mediante el desarrollo de este escenarios, donde se utiliza el funcionamiento de las VLANs y las VRF como desarrollo de una red empresarial donde nos permite administrar los swiches para su importante administración de cada Swicht y llevar cada ip a su respectivo pc.

Cada proceso nos está brindando los conocimientos prácticos y teóricos, en la utilización de herramientas como el software GNS3 o CISCO Packet tracer, que permite entender mejor las redes y los protocolos de enrutamiento como futuros Ingenieros de telecomunicaciones.

## **BIBLIOGRAFIA**

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF v3. CCNP and CCIE Enterprise Core ENCORA 350-401.

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF. CCNP and CCIE Enterprise Core ENCORA 350-401.

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCORA 350-401.

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.