

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP  
PRUEBA DE HABILIDADES PRACTICAS

Diego Edinson Paredes Aguirre

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
SANTIAGO DE CALI  
2023

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP  
PRUEBA DE HABILIDADES PRACTICAS

Diego Edinson Paredes Aguirre

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

TUTORA  
MARITZA EARLEY MONDRAGON GUZMAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
SANTIAGO DE CALI  
2023

NOTA DE ACEPTACION

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

SANTIAGO DE CALI, 04 de mayo de 2023

## **AGRADECIMIENTOS**

Han sido casi 8 años desde que me inscribí en UNAD y nunca pensé que llegaría esta instancia, transcurrieron muchos obstáculos personales, emocionales de los cuales se me hacían frente y no me ayudaban a terminar mis estudios profesionales. Sin embargo, el rodearme con buenas personas, amigos y familiares han ayudado a seguir luchando para alcanzar los objetivos. Agradezco a mi padre y madre por su amor incondicional, su apoyo emocional, y por su paciencia y comprensión en los momentos en los que mi dedicación flaqueaba. Su confianza en mí fue siempre un motor que me impulsó a seguir adelante. También agradezco a mis amigos por su apoyo y motivación durante todo este proceso. Sus ánimos y palabras de aliento me ayudaron a superar los momentos de estrés y de duda. Por último, quiero agradecer a mis profesores y compañeros de carrera por su dedicación y enseñanzas, que me han permitido adquirir los conocimientos necesarios para convertirme en un Ingeniero. Sin su orientación y guía, no habría sido posible alcanzar este logro. A todos ellos, les estoy profundamente agradecido. Este logro no solo es mío, sino también de aquellos que me han apoyado y acompañado en el camino hacia la meta.

## CONTENIDO

<b>AGRADECIMIENTOS</b> .....	4
<b>LISTA DE TABLAS</b> .....	6
<b>LISTA DE FIGURAS</b> .....	7
<b>GLOSARIO</b> .....	9
<b>RESUMEN</b> .....	10
<b>ABSTRACT</b> .....	11
<b>INTRODUCCIÓN</b> .....	12
<b>CONTENIDO DE LA ACTIVIDAD</b> .....	13
<b>Objetivos</b> .....	14
<b>Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces</b> .....	15
<b>Paso1: Montaje de la topología de red.</b> .....	15
<b>Paso 2: Configuración de los ajustes básicos para cada dispositivo.</b> .....	16
<b>Parte 2: Configurar VRF y enrutamiento estático</b> .....	20
<b>Parte 3: Configurar la red L2</b> .....	27
<b>3.1 Deshabilitamos las interfaces:</b> .....	28
<b>3.2 Sobre D1 y D2, configurar los trunk links para R1 y R3</b> .....	29
<b>3.3 Sobre D1 y A1, configurar los EtherneChanel</b> .....	30
<b>3.4 Sobre D1, D2, and A1, configurar los puertos de acceso para PC1, PC2, PC3, and PC4</b> .....	30
<b>3.5 Verificar PC to PC conectividad</b> .....	32
<b>Parte 4 Configurar la Seguridad</b> .....	35
<b>4.1 En todos los dispositivos, configurar el modo privilegiado EXE</b> .....	35
<b>4.2 En todos los dispositivos, cree un usuario de cuenta local.</b> .....	36
<b>4.3 En todos los dispositivos, habilite AAA y habilitar la autenticación AAA</b> .....	38
<b>CONCLUSION</b> .....	40
<b>BIBLIOGRAFIA</b> .....	41

## LISTA DE TABLAS

<i>Tabla 1. R1 no alcanza PC2 y PC4.....</i>	<i>14</i>
<i>Tabla 2. Configuración R1 ajustes básicos.....</i>	<i>16</i>
<i>Tabla 3. Configuración R2 y R3 ajustes básicos .....</i>	<i>16</i>
<i>Tabla 4. Configuración D1 ajustes básicos.....</i>	<i>17</i>
<i>Tabla 5. Configuración D2 y A3 ajustes básicos.....</i>	<i>17</i>
<i>Tabla 6. Creación de VRF .....</i>	<i>20</i>
<i>Tabla 7. Configuración de interfaces de R1.....</i>	<i>21</i>
<i>Tabla 8. Configuración de interfaces de R2.....</i>	<i>22</i>
<i>Tabla 9. Configuración de interfaces de R3.....</i>	<i>23</i>
<i>Tabla 10. Configuración de ruta estática de R1.....</i>	<i>23</i>
<i>Tabla 11. Configuración de ruta estática de R1.....</i>	<i>24</i>
<i>Tabla 12. Configuración de ruta estática de R3.....</i>	<i>24</i>
<i>Tabla 13 Tareas a realizar parte 3 .....</i>	<i>27</i>
<i>Tabla 14 Deshabilitar Puertos .....</i>	<i>28</i>
<i>Tabla 15 Configurar puertos modo Trunk .....</i>	<i>29</i>
<i>Tabla 16 Configurar EthernetChannel.....</i>	<i>30</i>
<i>Tabla 17 Configurar puertos en acceso.....</i>	<i>31</i>
<i>Tabla 18 Configurar la seguridad .....</i>	<i>35</i>
<i>Tabla 19 Configuración EXE modo privilegiado.....</i>	<i>35</i>
<i>Tabla 20 Creación de cuenta Local.....</i>	<i>36</i>
<i>Tabla 21 Configuración de autenticación AAA.....</i>	<i>38</i>

## LISTA DE FIGURAS

<i>Ilustración 1. Topología de red.....</i>	<i>13</i>
<i>Ilustración 2. Topología de red implementada .....</i>	<i>15</i>
<i>Ilustración 3. R1 copia de configuración .....</i>	<i>17</i>
<i>Ilustración 4. R2 copia de configuración .....</i>	<i>17</i>
<i>Ilustración 5. R3 copia de configuración .....</i>	<i>17</i>
<i>Ilustración 6. D1 copia de configuración .....</i>	<i>18</i>
<i>Ilustración 7. D2 copia de configuración .....</i>	<i>18</i>
<i>Ilustración 8. Configuraciones IP de PC1 .....</i>	<i>18</i>
<i>Ilustración 9. Configuraciones IP de PC2.....</i>	<i>18</i>
<i>Ilustración 10. Configuraciones IP de PC3.....</i>	<i>19</i>
<i>Ilustración 11. Configuraciones IP de PC4 .....</i>	<i>19</i>
<i>Ilustración 12. Rutas estáticas R1 .....</i>	<i>24</i>
<i>Ilustración 13. Rutas estáticas R1.....</i>	<i>24</i>
<i>Ilustración 14. Rutas estáticas R1.....</i>	<i>25</i>
<i>Ilustración 15. ping vrf General-Users 10.0.208.8.....</i>	<i>25</i>
<i>Ilustración 16. ping vrf General-Users 2001:db8:acad:208::1.....</i>	<i>25</i>
<i>Ilustración 17. ping vrf Special-Users 10.0.213.8.....</i>	<i>25</i>
<i>Ilustración 18. ping vrf Special-Users 2001:db8:acad:213::1.....</i>	<i>25</i>
<i>Ilustración 19. R1 no alcanza PC2 y PC4.....</i>	<i>26</i>
<i>Ilustración 20. Deshabilitar puertos D1.....</i>	<i>28</i>
<i>Ilustración 21. Deshabilitar puertos D2.....</i>	<i>28</i>
<i>Ilustración 22. Deshabilitar puertos A1.....</i>	<i>29</i>
<i>Ilustración 23. Trunk Link D1 a R1 .....</i>	<i>29</i>
<i>Ilustración 24. Trunk Link D2 a R1 .....</i>	<i>29</i>
<i>Ilustración 25. Configuración EtherneChannel D1.....</i>	<i>30</i>
<i>Ilustración 26. Configuración EthernetChannel A1.....</i>	<i>30</i>
<i>Ilustración 27. Configuración puerto acceso D1.....</i>	<i>31</i>
<i>Ilustración 28. Configuración puerto acceso D2 a PC2 .....</i>	<i>31</i>
<i>Ilustración 29. Configuración puerto acceso D2 a PC4.....</i>	<i>32</i>
<i>Ilustración 30. Configuración puerto acceso A1.....</i>	<i>32</i>
<i>Ilustración 31. Conectividad PC1 a PC2.....</i>	<i>33</i>
<i>Ilustración 32. Conectividad PC3 a PC4.....</i>	<i>33</i>
<i>Ilustración 33. PC1 no alcanza PC3 y PC4.....</i>	<i>34</i>
<i>Ilustración 34. PC3 no alcanza PC1 y PC2.....</i>	<i>34</i>
<i>Ilustración 35. Enable Secret R1 .....</i>	<i>36</i>
<i>Ilustración 36. Enable Secret R2 .....</i>	<i>36</i>
<i>Ilustración 37. Enable Secret R3.....</i>	<i>36</i>
<i>Ilustración 38. Enable Secret D1 .....</i>	<i>36</i>

<i>Ilustración 39 Enable Secret D2 .....</i>	<i>36</i>
<i>Ilustración 40 Enable Secret A1.....</i>	<i>36</i>
<i>Ilustración 41 Creación cuenta local R1 .....</i>	<i>36</i>
<i>Ilustración 42 Creación cuenta local R2.....</i>	<i>37</i>
<i>Ilustración 43 Creación cuenta local R3.....</i>	<i>37</i>
<i>Ilustración 44 Creación cuenta local D1 .....</i>	<i>37</i>
<i>Ilustración 45 Creación cuenta local D2.....</i>	<i>37</i>
<i>Ilustración 46 Creación cuenta local A1 .....</i>	<i>37</i>
<i>Ilustración 47 Autenticación AAA R1 .....</i>	<i>38</i>
<i>Ilustración 48 Autenticación AAA R2 .....</i>	<i>38</i>
<i>Ilustración 49 Autenticación AAA R3 .....</i>	<i>38</i>
<i>Ilustración 50 Autenticación AAA D1 .....</i>	<i>38</i>
<i>Ilustración 51 Autenticación AAA D2 .....</i>	<i>39</i>
<i>Ilustración 52 Autenticación AAA A1.....</i>	<i>39</i>

## GLOSARIO

**Autenticación AAA:** AAA (Autenticación, Autorización y Contabilidad) es un método de autenticación de usuarios en la red y control de acceso a los recursos de la red en dispositivos Cisco. AAA se utiliza para verificar la identidad del usuario, determinar si el usuario tiene permiso para acceder a un recurso específico y registrar el acceso para fines de auditoría.

**PortChannel:** PortChannel es una tecnología de agrupación de puertos en dispositivos Cisco que permite combinar múltiples enlaces físicos en un solo enlace lógico. Esto proporciona un mayor ancho de banda y una mayor redundancia en la red.

**Subinterfaces de red en router:** Una subinterfaz es una interfaz virtual que se crea a partir de una única interfaz física en un router Cisco. Se utilizan para dividir el tráfico en diferentes redes o VLANs y permiten que un solo puerto del router se utilice para múltiples redes. Las subinterfaces se configuran con una etiqueta VLAN y una dirección IP única.

**Trunk:** Un trunk es un enlace de red que se utiliza para transportar múltiples VLANs entre dispositivos de red. Los troncales se utilizan comúnmente en redes VLAN para permitir que los dispositivos en diferentes redes se comuniquen entre sí. En un enlace trunk, las VLANs se etiquetan con una etiqueta VLAN específica para permitir que el tráfico se enrute correctamente.

**VLAN:** Una VLAN (Virtual Local Area Network) es una red virtual que se crea mediante la segmentación lógica de una red física. Las VLAN permiten que los dispositivos se agrupen en diferentes redes lógicas, independientemente de su ubicación física en la red. Esto puede mejorar la eficiencia de la red, la seguridad y el rendimiento.

**VRF:** Virtual Routing and Forwarding (VRF) es una tecnología de enrutamiento que permite tener múltiples instancias virtuales de enrutamiento en una sola red física. Cada instancia de VRF tiene su propia tabla de enrutamiento, lo que permite la separación y el aislamiento de tráfico entre diferentes dominios de enrutamiento.

## RESUMEN

En el trabajo de redes implementado en el entorno de simulación de GNS3 se utilizaron tecnologías como VRF, VLAN y subinterfaces para crear una red virtualizada. La red se construyó utilizando routers virtuales, que se conectaron entre sí mediante enlaces virtuales Ethernet. Para separar el tráfico de diferentes clientes, se crearon múltiples VRFs, cada una con su propia tabla de enrutamiento. Cada VRF se asignó a una VLAN específica, lo que permitió separar el tráfico de diferentes clientes en diferentes segmentos de red. Además, se crearon subinterfaces para permitir la conexión de múltiples redes a través de una única interfaz física. Durante la implementación, se configuraron las VLANs y subinterfaces en los routers virtuales, y se realizó una prueba de conectividad para verificar que el tráfico se estuviera transmitiendo correctamente entre las diferentes redes. Además, se configuraron las políticas de enrutamiento adecuadas para garantizar que el tráfico se enrute correctamente a través de la red.

La implementación de VRF, VLAN y subinterfaces permitió crear una red virtualizada segura y escalable que permitió separar el tráfico de diferentes clientes y proporcionar conectividad de red confiable. El uso de un entorno de simulación como GNS3 permitió probar la configuración de red antes de su implementación en una red real, lo que ayudó a evitar posibles problemas y errores de configuración.

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

## **ABSTRACT**

In the network work implemented in the GNS3 simulation environment, technologies such as VRF, VLAN and subinterfaces were used to create a virtualized network. The network was built using virtual routers, which were connected to each other via Ethernet virtual links. To separate traffic from different clients, multiple VRFs were created, each with its own routing table. Each VRF was assigned to a specific VLAN, which allowed traffic from different clients to be separated on different network segments. Additionally, subinterfaces were created to allow multiple networks to connect through a single physical interface. During the implementation, the VLANs and subinterfaces on the virtual routers were configured, and a connectivity test was performed to verify that the traffic was being transmitted correctly between the different networks. In addition, the proper routing policies have been configured to ensure that traffic is correctly routed through the network.

The implementation of VRF, VLANs and subinterfaces allowed to create a secure and scalable virtualized network that allowed to separate the traffic of different clients and to provide reliable network connectivity. The use of a simulation environment such as GNS3 allowed the network configuration to be tested before its implementation in a real network, which helped to avoid potential problems and configuration errors.

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

## INTRODUCCIÓN

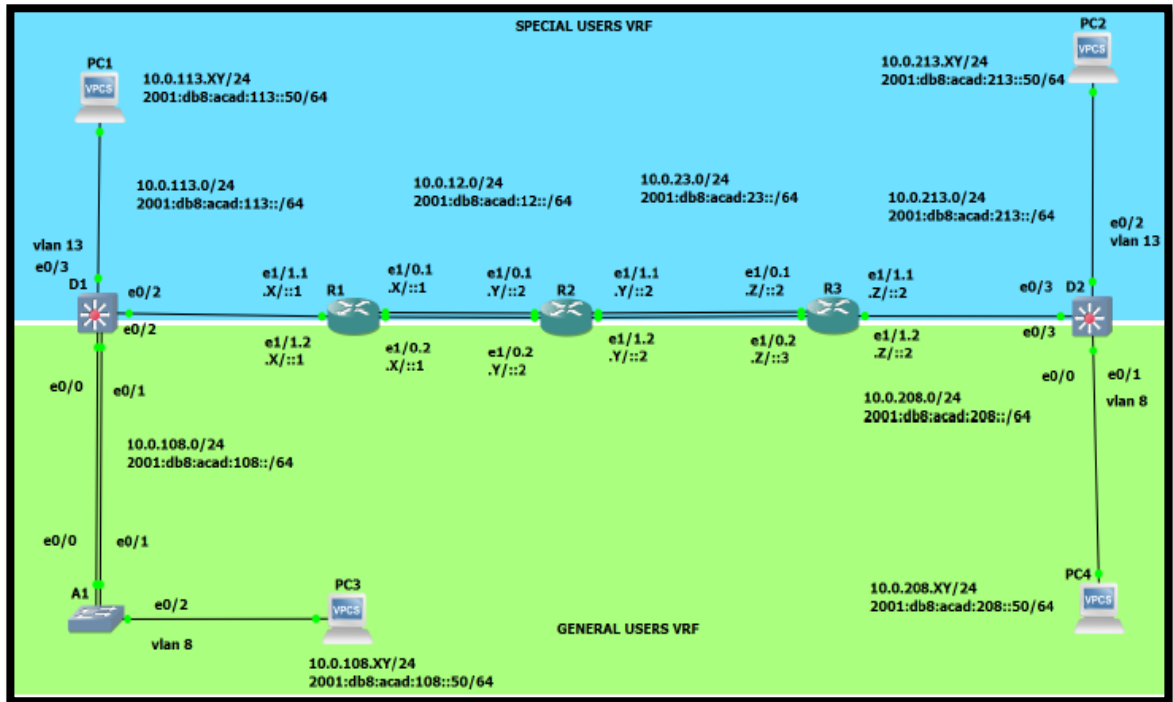
En el mundo de la informática y las comunicaciones, la implementación de redes es un tema esencial para garantizar el correcto funcionamiento de los sistemas y la transferencia de datos. En este sentido, el uso de tecnologías como Virtual Routing and Forwarding (VRF), Virtual LAN (VLAN) y cuentas de usuario locales son herramientas indispensables para lograr una gestión eficiente y segura de la red. En este trabajo, se presenta la implementación de VRF, VLAN y cuentas de usuario locales en tres switches con sus respectivas claves y encriptación, así como la configuración de enrutamiento estático de dos sedes y tres routers. La implementación de estas tecnologías y configuraciones permitirá una gestión más eficiente y segura de la red, al mismo tiempo que se garantiza la privacidad y protección de los datos.

La configuración de VRF permitirá la segmentación de la red en distintos dominios virtuales, lo que mejorará la seguridad y eficiencia en el tráfico de datos. Por su parte, la implementación de VLAN permitirá la creación de redes virtuales independientes dentro de la red física, permitiendo una mejor gestión del tráfico y la administración de los recursos. Por otro lado, la configuración de cuentas de usuario locales, junto con sus claves y encriptación, proporcionará una capa adicional de seguridad para la red. De esta manera, se garantiza que solo los usuarios autorizados puedan acceder a los recursos de la red.

Finalmente, la configuración de enrutamiento estático entre las dos sedes y los tres routers permitirá una comunicación eficiente y segura entre los distintos dispositivos de la red. Esta configuración se realiza estableciendo rutas de forma manual, lo que asegura que el tráfico de datos se dirija de manera óptima y segura entre los distintos dispositivos.

## CONTENIDO DE LA ACTIVIDAD

### Topología de la red:



*Ilustración 1. Topología de red*

### Tabla de direccionamiento:

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	LinkLocal IPV6
R1	E1/0.1	10.0.12.7/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.7/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.7/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.7/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.4/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.4/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.4/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.4/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.8/24	2001:db8:acad:23::3/64	fe80::3:1

	E1/0.2	10.0.23.8/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.8/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.8/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.74/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.74/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.74/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.74/24	2001:db8:acad:208::50/64	EUI-64

*Tabla 1. R1 no alcanza PC2 y PC4*

### **Objetivos**

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

Parte 2: Configurar VRF y rutas estáticas.

Parte 3: Configurar Capa 2(se entrega finalizado el paso 6)

Parte 4: Configurar seguridad (se entrega finalizado el paso 6)

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

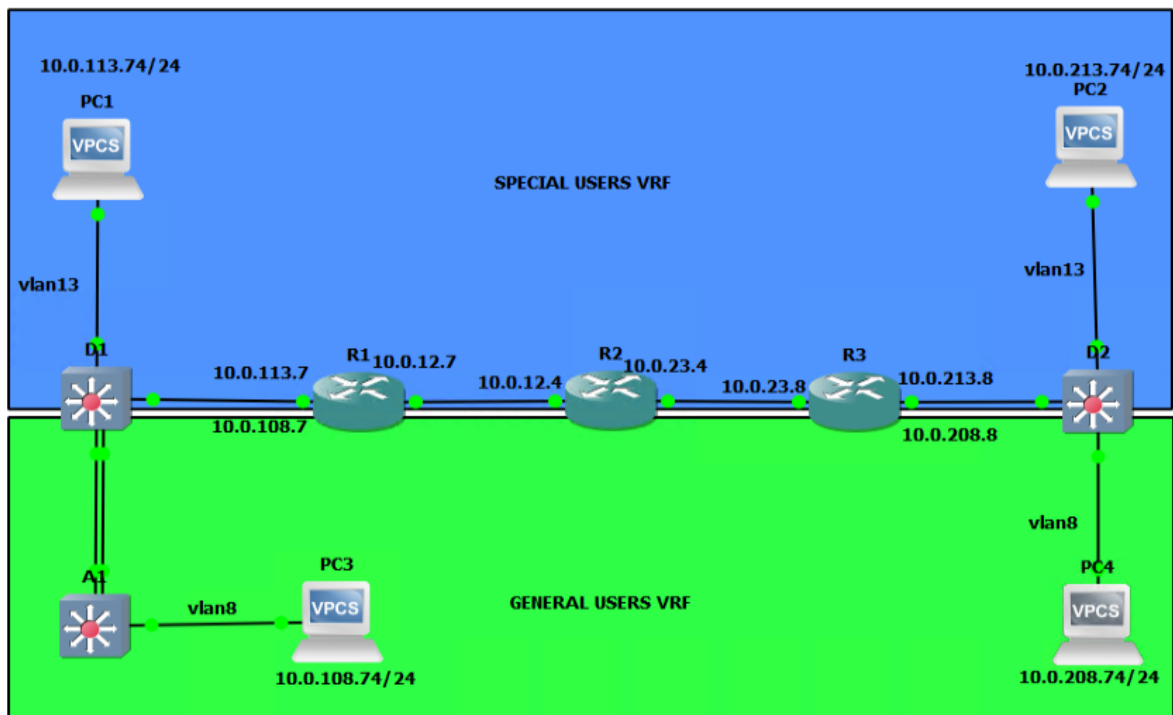
**Observación:** Para el desarrollo del laboratorio se debe tomar como datos los últimos dígitos del código, sin embargo, para el desarrollo de la actividad he tomado los anteriores números a los 3 últimos, debido a que los dígitos terminan en **0** y presenta inconsistencia a la hora de configurar las interfaces

Código: **1061748040**

Dígitos a utilizar: **748**

**Paso1:** Montaje de la topología de red.

### Montaje de topología sobre GNS3:



*Ilustración 2. Topología de red implementada*

**Nota:** En el laboratorio para la implementación del **Switch A1** se implementó el modelo Cisco IOU L2, debido a que en GNS3 el tipo de switch que ofrece no permite consola.

**Paso 2:** Configuración de los ajustes básicos para cada dispositivo.

- a) Ingresamos al modo de configuración de los equipos y aplicamos las configuraciones básicas.

**Router1:**

<pre>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</pre>	<p>Configuración del nombre de host</p> <p>Se habilita enrutamiento sobre ipv6</p> <p>Se deshabilita la búsqueda dominio</p> <p>Se asigna un mensaje de bienvenida cuando inicia el equipo</p> <p>Configuración de línea de consola en 0</p> <p>Se deshabilita el timeout</p> <p>Se habilita mensajes de log</p> <p>Se sale del menú</p>
--	--

*Tabla 2. Configuración R1 ajustes básicos*

Se omitirá la explicación de los comandos de los siguientes equipos debido a que es lo mismo del primer R1.

<p><b>Router2</b></p> <pre>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</pre>	<p><b>Router3</b></p> <pre>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</pre>
--	--

*Tabla 3. Configuración R2 y R3 ajustes básicos*

**Switch D1:**

<pre>hostname D1 ip routing ipv6 unicast-routing no ip domain lookup banner motd # D1, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit vlan 8 name General-Users exit vlan 13 name Special-Users exit</pre>	<p>Configuración del nombre de host</p> <p>Se habilita enrutamiento ipv4</p> <p>Se habilita enrutamiento sobre ipv6</p> <p>Se deshabilita la búsqueda dominio</p> <p>Se asigna un mensaje de bienvenida cuando inicia el equipo</p> <p>Configuración de línea de consola en 0</p> <p>Se deshabilita el timeout</p> <p>Se habilita mensajes de log</p> <p>Se sale del menu</p> <p>Se crea la vlan 8</p> <p>Se asigna un nombre a la vlan</p> <p>Se crea la vlan 13</p> <p>Se asigna un nombre a la vlan</p>
--	--

Tabla 4. Configuración D1 ajustes básicos

Se omitirá la explicación de los comandos de los siguientes equipos debido a que es lo mismo del primer D2 y A1.

**Switch D2 y A1:**

<pre>hostname D2 ip routing ipv6 unicast-routing no ip domain lookup banner motd # D2, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit vlan 8 name General-Users exit vlan 13 name Special-Users exit</pre>	<pre>hostname A1 ipv6 unicast-routing no ip domain lookup banner motd # A1, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit vlan 8 name General-Users exit</pre>
--	---

Tabla 5. Configuración D2 y A3 ajustes básicos

**b.** Realizamos copia o guardamos las configuraciones de cada uno de los dispositivos.

Comando utilizado:

**copy running-config startup-config / se utiliza para guardar la configuración en la memoria.**

```
R1#copy run
R1#copy running-config st
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Ilustración 3. R1 copia de configuración

```
R2#copy run
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Ilustración 4. R2 copia de configuración

```
R3#copy run
R3#copy running-config st
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Ilustración 5. R3 copia de configuración

```
D1#copy run
D1#copy running-config st
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 1952 bytes to 1121 bytes[OK]
D1#
```

*Ilustración 6. D1 copia de configuración*

```
D2#copy run
D2#copy running-config st
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 1733 bytes to 1024 bytes[OK]
D2#
```

*Ilustración 7. D2 copia de configuración*

c. Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de enrutamiento.

Comando utilizado en consola:

***Ip address mask / Se define la dirección IP para el equipo.***

### Configuración PC1

```
PC1> show
```

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC1	10.0.113.74/24	10.0.113.7	00:50:79:66:68:00	20009	127.0.0.1:20010
	fe80::250:79ff:fe66:6800/64				
	2001:db8:acad:113:2050:79ff:fe66:6800/64 eui-64				

*Ilustración 8. Configuraciones IP de PC1*

### Configuración PC2

```
PC2> show
```

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC2	10.0.213.74/24	10.0.213.8	00:50:79:66:68:01	20015	127.0.0.1:20021
	fe80::250:79ff:fe66:6801/64				
	2001:db8:acad:213:2050:79ff:fe66:6801/64 eui-64				

*Ilustración 9. Configuraciones IP de PC2*

## Configuración

PC3

```
PC3> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC3      10.0.108.74/24   10.0.108.7       00:50:79:66:68:02 20011  127.0.0.1:20012
fe80::250:79ff:fe66:6802/64
2001:db8:acad:108:2050:79ff:fe66:6802/64 eui-64
```

*Ilustración 10. Configuraciones IP de PC3*

## Configuración PC4

```
PC4> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC4      10.0.208.74/24   10.0.208.8       00:50:79:66:68:03 20013  127.0.0.1:20014
fe80::250:79ff:fe66:6803/64
2001:db8:acad:208:2050:79ff:fe66:6803/64 eui-64
```

*Ilustración 11. Configuraciones IP de PC4*

## Parte 2: Configurar VRF y enrutamiento estático

A continuación, se presenta la configuración VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. De tal manera, R1 pueda comunicarse mediante ping a R3 en cada VRF.

- a. En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.

### Comandos utilizados para la configuración de R1, R2 y R3:

<pre>vrf definition General-Users address-family ipv4 address-family ipv6 exit vrf definition Special-Users address-family ipv4 address-family ipv6 exit</pre>	<p>Creación de VRF y se asigna nombre</p> <p>Versión ipv4</p> <p>Versión ipv6</p> <p>Creación de VRF y se asigna nombre</p> <p>Versión ipv4</p> <p>Versión ipv6</p>
--	---

*Tabla 6. Creación de VRF*

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

### Configuración R1 de interfaces:

<pre>interface Ethernet1/0.1 encapsulation dot1Q 13 vrf forwarding Special-Users ip address 10.0.12.7 255.255.255.0 ipv6 address FE80::1:1 link- local ipv6 address 2001:DB8:ACAD:12::1/64 No shutdown ! interface Ethernet1/0.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.12.7 255.255.255.0 ipv6 address FE80::1:2 link- local ipv6 address 2001:DB8:ACAD:12::1/64 No shutdown ! interface Ethernet1/1 no ip address duplex full</pre>	<p>Selección de interfaz a configurar</p> <p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p> <p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p> <p>Selección de interfaz a configurar</p> <p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p> <p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p> <p>Selección de interfaz a configurar</p> <p>Se indica que no tendrá IP</p> <p>Se define tipo de conexión</p>
---	---

<pre> ! interface Ethernet1/1.1  encapsulation dot1Q 13  vrf forwarding Special-Users  ip address 10.0.113.7  255.255.255.0  ipv6 address FE80::1:3 link-  local  ipv6 address  2001:DB8:ACAD:113::1/64  No shutdown ! interface Ethernet1/1.2  encapsulation dot1Q 8  vrf forwarding General-Users  ip address 10.0.108.7  255.255.255.0  ipv6 address FE80::1:4 link-  local  ipv6 address  2001:DB8:ACAD:108::1/64  No shutdown </pre>	<p>Selección de interfaz a configurar Configuración para trabajar con vlan Se asigna el VRF a trabajar Se configura dirección IP y mascara IPv4 Se configura dirección Link-Local Se configura dirección IP y mascara IPv6 Habilitar interfaz</p> <p>Selección de interfaz a configurar Configuración para trabajar con vlan Se asigna el VRF a trabajar Se configura dirección IP y mascara IPv4 Se configura dirección Link-Local Se configura dirección IP y mascara IPv6 Habilitar interfaz</p>
---	---

*Tabla 7. Configuración de interfaces de R1.*

### Configuración R2 de interfaces:

<pre> interface Ethernet1/0.1  encapsulation dot1Q 13  vrf forwarding Special-Users  ip address 10.0.12.4  255.255.255.0  ipv6 address FE80::2:1 link-  local  ipv6 address  2001:DB8:ACAD:12::2/64  No shutdown ! interface Ethernet1/0.2  encapsulation dot1Q 8  vrf forwarding General-Users  ip address 10.0.12.4  255.255.255.0  ipv6 address FE80::2:2 link-  local  ipv6 address  2001:DB8:ACAD:12::2/64  No shutdown ! interface Ethernet1/1  no ip address  duplex full ! interface Ethernet1/1.1  encapsulation dot1Q 13 </pre>	<p>Selección de interfaz a configurar Configuración para trabajar con vlan Se asigna el VRF a trabajar Se configura dirección IP y mascara IPv4 Se configura dirección Link-Local Se configura dirección IP y mascara IPv6 Habilitar interfaz</p> <p>Selección de interfaz a configurar Configuración para trabajar con vlan Se asigna el VRF a trabajar Se configura dirección IP y mascara IPv4 Se configura dirección Link-Local Se configura dirección IP y mascara IPv6 Habilitar interfaz</p> <p>Selección de interfaz a configurar Se indica que no tendrá IP Se define tipo de conexión</p> <p>Selección de interfaz a configurar</p>
---	---

<pre> vrf forwarding Special-Users ip address 10.0.23.4 255.255.255.0 ipv6 address FE80::2:3 link- local ipv6 address 2001:DB8:ACAD:23::2/64 No shutdown ! interface Ethernet1/1.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.23.4 255.255.255.0 ipv6 address FE80::2:4 link- local ipv6 address 2001:DB8:ACAD:23::2/64 No shutdown </pre>	<p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p> <p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p> <p>Selección de interfaz a configurar</p> <p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p> <p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p>
--	---

*Tabla 8. Configuración de interfaces de R2.*

### Configuración R3 de interfaces:

<pre> interface Ethernet1/0.1 encapsulation dot1Q 13 vrf forwarding Special-Users ip address 10.0.23.8 255.255.255.0 ipv6 address FE80::3:1 link- local ipv6 address 2001:DB8:ACAD:23::3/64 no shutdown ! interface Ethernet1/0.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.23.8 255.255.255.0 ipv6 address FE80::3:2 link- local ipv6 address 2001:DB8:ACAD:23::3/64 no shutdown ! interface Ethernet1/1 no ip address duplex half ! interface Ethernet1/1.1 encapsulation dot1Q 13 vrf forwarding Special-Users </pre>	<p>Selección de interfaz a configurar</p> <p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p> <p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p> <p>Selección de interfaz a configurar</p> <p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p> <p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p> <p>Selección de interfaz a configurar</p> <p>Se indica que no tendrá IP</p> <p>Se define tipo de conexión</p> <p>Selección de interfaz a configurar</p> <p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p>
---	--

<pre> ip address 10.0.213.8 255.255.255.0 ipv6 address FE80::3:3 link- local ipv6 address 2001:DB8:ACAD:213::1/64 no shutdown ! interface Ethernet1/1.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.208.8 255.255.255.0 ipv6 address FE80::3:4 link- local ipv6 address 2001:DB8:ACAD:208::1/64 no shutdown </pre>	<p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p> <p>Selección de interfaz a configurar</p> <p>Configuración para trabajar con vlan</p> <p>Se asigna el VRF a trabajar</p> <p>Se configura dirección IP y mascara IPv4</p> <p>Se configura dirección Link-Local</p> <p>Se configura dirección IP y mascara IPv6</p> <p>Habilitar interfaz</p>
---	--

*Tabla 9. Configuración de interfaces de R3.*

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

**Configuración R1 rutas estáticas:**

<pre> ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.4 ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.4 ! ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2 ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2 </pre>	<p>Configuración de ruta ipv4 por defecto para VRF General-Users</p> <p>Configuración de ruta ipv4 por defecto para VRF Special-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF General-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF Special-Users</p>
--	---

*Tabla 10. Configuración de ruta estática de R1.*

**Configuración R2 rutas estáticas:**

<pre> ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.7 ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.8 ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.7 ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.8 ! 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 </pre>	<p>Configuración de ruta ipv4 por defecto para VRF General-Users</p> <p>Configuración de ruta ipv4 por defecto para VRF Special-Users</p> <p>Configuración de ruta ipv4 por defecto para VRF Special-Users</p> <p>Configuración de ruta ipv4 por defecto para VRF Special-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF General-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF Special-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF General-Users</p>
--	--

<pre> 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 </pre>	<p>Configuración de ruta ipv6 por defecto para VRF Special-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF General-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF Special-Users</p>
--	--

*Tabla 11. Configuración de ruta estática de R1*

### Configuración R3 rutas estáticas:

<pre> ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.4 ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.4 ! ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:23::2 ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:23::2 </pre>	<p>Configuración de ruta ipv4 por defecto para VRF General-Users</p> <p>Configuración de ruta ipv4 por defecto para VRF Special-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF General-Users</p> <p>Configuración de ruta ipv6 por defecto para VRF Special-Users</p>
--	---

*Tabla 12. Configuración de ruta estática de R3.*

Validación de las rutas estáticas en R1, R2 y R3:

```

R1#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.4
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.4
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2
R1#

```

*Ilustración 12. Rutas estáticas R1*

```

R2#show run | inc route
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.7
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.8
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.7
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.8
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#

```

*Ilustración 13. Rutas estáticas R1*

```

R3#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.4
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.4
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:23::2
R3#

```

*Ilustración 14. Rutas estáticas R1*

- b.** Verifique la conectividad en cada VRF.

Desde R1, verifique la conectividad a R3:

```

R1#ping vrf General-Users 10.0.208.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/48/64 ms

```

*Ilustración 15. ping vrf General-Users 10.0.208.8*

```

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 = 40/66/160 ms

```

*Ilustración 16. ping vrf General-Users 2001:db8:acad:208::1*

```

R1#ping vrf Special-Users 10.0.213.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/34/44 ms
R1#

```

*Ilustración 17. ping vrf Special-Users 10.0.213.8*

```

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 = 40/63/144 ms
R1#

```

*Ilustración 18. ping vrf Special-Users 2001:db8:acad:213::1*

Luego de las configuraciones se valida que desde R1 no puede conectarse a nivel de red a PC2 y PC4

```
R1#ping 10.0.213.74
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.74, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#ping 10.0.208.74
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.74, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

*Ilustración 19. R1 no alcanza PC2 y PC4*

### Parte 3: Configurar la red L2

En esta parte, la idea es poder configurar los switches para soportar la conectividad de host.

Se deberá realizar las siguientes configuraciones:

Tabla 13 Tareas a realizar parte 3

Tarea	Tarea	Especificación
3.1	On D1, D2, and A1, disable all interfaces	
3.2	On D1 and D2, configure the trunk links to R1 and R3.	Configure and enable the e0/3 link as a trunk link.
3.3	On D1 and A1, configure the EtherChannel.	On D1, configure and enable: • Interface e0/0 and e0/1 • Port Channel 1 using PAgP On A1, configure and enable: • Interface E0/0 and E0/1 • Port Channel 1 using PAgP
3.4	On D1, D2, and A1, configure access ports for PC1, PC2, PC3, and PC4.	Configure and enable the access ports as follows:  • On D1, configure interface E0/3 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface E0/2 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface E0/1 as an access port in VLAN 8 and enable Portfast. • On A1, configure interface E0/2 as an access port in VLAN 8 and enable Portfast.
3.5	Verify PC to PC connectivity	From PC1, verify IPv4 and IPv6 connectivity to PC2. From PC3, verify IPv4 and IPv6 connectivity to PC4.

### 3.1 Deshabilitamos las interfaces:

Procedemos a deshabilitar las interfaces en los SW D1, D2 y A1

#### Deshabilitar interfaces SW D1, D2 y A1

Tabla 14 Deshabilitar Puertos

Interface range et0/0-3	Selección de interfaces
Shutdown	Comando para apagar interfaces
exit	Salir

```
D1(config)#interface range et0/0-3/3
      ^
% Invalid input detected at '^' marker.
D1(config)#interface range et0/0-3
D1(config-if-range)#shutdo
D1(config-if-range)#shutdown
D1(config-if-range)#
*May 4 16:21:03.681: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*May 4 16:21:03.682: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*May 4 16:21:03.682: %LINK-3-UPDOWN: Interface Port-channell1, changed state to down
D1(config-if-range)#
*May 4 16:21:03.682: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*May 4 16:21:03.694: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
*May 4 16:21:04.682: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*May 4 16:21:04.682: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*May 4 16:21:04.682: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channell1, changed state to down
*May 4 16:21:04.683: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
*May 4 16:21:04.695: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
D1(config-if-range)#
```

Ilustración 20 Deshabilitar puertos D1

```
D2(config)#interface range et0/0-3
D2(config-if-range)#shutd
D2(config-if-range)#shutdown
D2(config-if-range)#en
*May 4 16:25:25.588: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*May 4 16:25:25.589: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*May 4 16:25:25.597: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*May 4 16:25:25.597: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
*May 4 16:25:26.588: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*May 4 16:25:26.589: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
D2(config-if-range)#end
D2#
*May 4 16:25:26.601: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
*May 4 16:25:26.601: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
*May 4 16:25:27.593: %SYS-5-CONFIG_I: Configured from console by console
D2#
```

Ilustración 21 Deshabilitar puertos D2

```

A1(config)#interface range et0/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#end
A1#
*May 4 16:27:26.975: %EC-5-CANNOT_BUNDLE2: Et0/2 is not compatible with Po1 and will be suspended (dtp mode of Et0/2 is off
, Po1 is on)
*May 4 16:27:26.978: %EC-5-CANNOT_BUNDLE2: Et0/2 is not compatible with Po1 and will be suspended (dtp mode of Et0/2 is off
, Po1 is on)
A1#
*May 4 16:27:28.004: %SYS-5-CONFIG_I: Configured from console by console
*May 4 16:27:28.977: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*May 4 16:27:28.977: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*May 4 16:27:28.986: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*May 4 16:27:28.986: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to administratively down
A1#
*May 4 16:27:29.977: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*May 4 16:27:29.977: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*May 4 16:27:29.990: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down

```

Ilustración 22 Deshabilitar puertos A1

### 3.2 Sobre D1 y D2, configurar los trunk links para R1 y R3 Configurar trunk links en D1 y D2

Tabla 15 Configurar puertos modo Trunk

Interface et0/3	Selección de interfaces
Switchport mode trunk	Configura modo trunk la interfaz
No shutdown	Habilitar el puerto
exit	Salir

Nota: En el montaje quedaron puertos diferentes respecto a la etapa 1 y 2. Es por ende que las configuraciones de puertos se ven reflejados de manera diferente.

```

D1(config)#interface et0/2
D1(config-if)#swi
D1(config-if)#switchport mode tru
D1(config-if)#switchport mode trunk
D1(config-if)#no shut
D1(config-if)#no shutdown
D1(config-if)#ei
*May 4 16:33:09.696: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*May 4 16:33:10.701: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
D1(config-if)#exit

```

Ilustración 23 Trunk Link D1 a R1

```

D2(config)#interface et0/3
D2(config-if)#swit
D2(config-if)#switchport mode
D2(config-if)#switchport mode tru
D2(config-if)#switchport mode trunk
D2(config-if)#no shu
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
*May 4 16:36:49.456: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
D2(config)#
*May 4 16:36:51.464: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to up
D2(config)#

```

Ilustración 24 Trunk Link D2 a R1

### 3.3 Sobre D1 y A1, configurar los EtherneChanel

#### Configurar Ethernetchannel en D1 y D2

Tabla 16 Configurar EthernetChannel

Interface range et0/0-1	Selección de interfaces
Switchport mode trunk	Configura modo trunk la interfaz
Channel-group 1 mode desirable	Ingresa al puerto al grupo
No shutdown	Habilitar el puerto
exit	Salir

```
D1(config-if-range)#swi
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#chan
D1(config-if-range)#channel-group 1 mode des
D1(config-if-range)#channel-group 1 mode desirable
D1(config-if-range)#no shut
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#
*May  4 16:47:54.947: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*May  4 16:47:54.947: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
D1(config)#
```

Ilustración 25 Configuración EtherneChannel D1

```
A1(config)#interface range et0/0-1
A1(config-if-range)#swit
A1(config-if-range)#switchport mo
A1(config-if-range)#switchport mode tru
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#chan
A1(config-if-range)#channel-group 1 mode des
A1(config-if-range)#channel-group 1 mode desirable
A1(config-if-range)#no shu
A1(config-if-range)#no shutdown
A1(config-if-range)#ex
A1(config-if-range)#exit
A1(config)#
*May  4 16:50:30.544: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*May  4 16:50:30.544: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*May  4 16:50:31.544: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
*May  4 16:50:31.544: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
A1(config)#
*May  4 16:50:36.293: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*May  4 16:50:37.298: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
A1(config)#
```

Ilustración 26 Configuración EthernetChannel A1

### 3.4 Sobre D1, D2, and A1, configurar los puertos de acceso para PC1, PC2, PC3, and PC4.

## Configurar Puertos en acceso en D1 y D2

Tabla 17 Configurar puertos en acceso

<pre>Interface range et0/3 Switchport mode access Switchport access vlan 13 Spanning-tree portfast No shutdown Exit</pre>	<p>Selección de interfaz Configura modo acceso la interfaz Ingresar al puerto a la vlan Habilitar protocolo spt Habilitar interfaz Salir</p>
<pre>Interface range et0/  Switchport mode access Switchport access vlan 8 Spanning-tree portfast No shutdown Exit</pre>	

```
D1(config)#interface et0/3
D1(config-if)#swi
D1(config-if)#sw
D1(config-if)#switchport mode ac
D1(config-if)#switchport mode access
D1(config-if)#swi
D1(config-if)#switchport ac
D1(config-if)#switchport access vl
D1(config-if)#switchport access vlan 13
D1(config-if)#sp
D1(config-if)#spanning-tree por
D1(config-if)#spanning-tree portf
D1(config-if)#spanning-tree portfast
D1(config-if)#no shu
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#
*May 4 16:43:50.619: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*May 4 16:43:51.620: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to up
D1(config)#inter
```

Ilustración 27 Configuración puerto acceso D1

```
D2(config)#interface et0/2
D2(config-if)#swi
D2(config-if)#switchport mode ac
D2(config-if)#switchport mode access
D2(config-if)#swit
D2(config-if)#switchport acc
D2(config-if)#switchport access vl
D2(config-if)#switchport access vlan 13
D2(config-if)#sppa
D2(config-if)#spanin
D2(config-if)#spannin
D2(config-if)#spanning-tree portfg
D2(config-if)#spanning-tree portfa
D2(config-if)#spanning-tree portfast
D2(config-if)#no shut
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
*May 4 18:42:18.843: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*May 4 18:42:19.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
D2(config)#
```

Ilustración 28 Configuración puerto acceso D2 a PC2

```

D2(config)#inter
D2(config)#interface et0/1
D2(config-if)#swi
D2(config-if)#switchport mod
D2(config-if)#switchport mode ac
D2(config-if)#switchport mode access
D2(config-if)#swi
D2(config-if)#switchport acc
D2(config-if)#switchport access vl
D2(config-if)#switchport access vlan 8
D2(config-if)#spann
D2(config-if)#spanning-tree portfa
D2(config-if)#spanning-tree portfast
D2(config-if)#no shu
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
*May  4 18:44:38.797: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*May  4 18:44:39.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
D2(config)#

```

*Ilustración 29 Configuración puerto acceso D2 a PC4*

```

A1(config)#inter
A1(config)#interface et0/2
A1(config-if)#swi
A1(config-if)#switchport mode
A1(config-if)#switchport mode ac
A1(config-if)#switchport mode access
A1(config-if)#swi
A1(config-if)#switchport ac
A1(config-if)#switchport access vl
A1(config-if)#switchport access vlan 8
A1(config-if)#sp
A1(config-if)#spanning-tree por
A1(config-if)#spanning-tree portf
A1(config-if)#spanning-tree portfast
A1(config-if)#no shu
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#
*May  4 18:56:43.897: %EC-5-CANNOT_BUNDLE2: Et0/2 is not compatible with Et0/0 and will be suspended (dtp mode of Et0/2 is o
ff, Et0/0 is on)
A1(config)#
*May  4 18:56:45.898: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
A1(config)#

```

*Ilustración 30 Configuración puerto acceso A1*

### 3.5 Verificar PC to PC conectividad

Probaremos la conectividad entre los diferentes equipos PC1, PC2 y PC3 y PC4

```

PC1> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC1      10.0.113.74/24   10.0.113.7       00:50:79:66:68:00 20014  127.0.0.1:20015
          fe80::250:79ff:fe66:6800/64
          2001:db8:acad:113:2050:79ff:fe66:6800/64

PC1> ping 10.0.213.74

84 bytes from 10.0.213.74 icmp_seq=1 ttl=61 time=56.993 ms
84 bytes from 10.0.213.74 icmp_seq=2 ttl=61 time=57.148 ms
84 bytes from 10.0.213.74 icmp_seq=3 ttl=61 time=62.079 ms
84 bytes from 10.0.213.74 icmp_seq=4 ttl=61 time=61.988 ms
84 bytes from 10.0.213.74 icmp_seq=5 ttl=61 time=62.801 ms

PC1> ping 2001:db8:acad:213:2050:79ff:fe66:6801/64

2001:db8:acad:213:2050:79ff:fe66:6801 icmp6_seq=1 ttl=58 time=73.143 ms
2001:db8:acad:213:2050:79ff:fe66:6801 icmp6_seq=2 ttl=58 time=57.497 ms
2001:db8:acad:213:2050:79ff:fe66:6801 icmp6_seq=3 ttl=58 time=62.135 ms
2001:db8:acad:213:2050:79ff:fe66:6801 icmp6_seq=4 ttl=58 time=62.826 ms
2001:db8:acad:213:2050:79ff:fe66:6801 icmp6_seq=5 ttl=58 time=56.872 ms

```

*Ilustración 31 Conectividad PC1 a PC2*

```

PC3> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC3      10.0.108.74/24   10.0.108.7       00:50:79:66:68:02 20018  127.0.0.1:20019
          fe80::250:79ff:fe66:6802/64
          2001:db8:acad:108:2050:79ff:fe66:6802/64

PC3> ping 10.0.208.74

84 bytes from 10.0.208.74 icmp_seq=1 ttl=61 time=65.834 ms
84 bytes from 10.0.208.74 icmp_seq=2 ttl=61 time=63.063 ms
84 bytes from 10.0.208.74 icmp_seq=3 ttl=61 time=62.436 ms
84 bytes from 10.0.208.74 icmp_seq=4 ttl=61 time=62.631 ms
84 bytes from 10.0.208.74 icmp_seq=5 ttl=61 time=56.988 ms

PC3> ping 2001:db8:acad:208:2050:79ff:fe66:6803/64

2001:db8:acad:208:2050:79ff:fe66:6803 icmp6_seq=1 ttl=58 time=123.929 ms
2001:db8:acad:208:2050:79ff:fe66:6803 icmp6_seq=2 ttl=58 time=41.331 ms
2001:db8:acad:208:2050:79ff:fe66:6803 icmp6_seq=3 ttl=58 time=55.643 ms
2001:db8:acad:208:2050:79ff:fe66:6803 icmp6_seq=4 ttl=58 time=61.728 ms
2001:db8:acad:208:2050:79ff:fe66:6803 icmp6_seq=5 ttl=58 time=61.732 ms

```

*Ilustración 32 Conectividad PC3 a PC4*

Se validará que PC1 no alcanza ni a PC3 ni a PC4, como también se puede validar la configuración de modo contrario, dando resultado que las configuraciones de los VRF quedaron bien implementadas.

```
PC1> ping 10.0.108.74
*10.0.12.4 icmp_seq=1 ttl=254 time=30.493 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=2 ttl=254 time=30.470 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=3 ttl=254 time=30.389 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=4 ttl=254 time=30.951 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=5 ttl=254 time=23.593 ms (ICMP type:3, code:1, Destination host unreachable)

PC1> ping 10.0.208.74
*10.0.12.4 icmp_seq=1 ttl=254 time=28.299 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=2 ttl=254 time=29.804 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=3 ttl=254 time=30.156 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=4 ttl=254 time=24.794 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=5 ttl=254 time=30.448 ms (ICMP type:3, code:1, Destination host unreachable)
```

*Ilustración 33 PC1 no alcanza PC3 y PC4*

```
PC3> ping 10.0.113.74
*10.0.12.4 icmp_seq=1 ttl=254 time=32.080 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=2 ttl=254 time=29.411 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=3 ttl=254 time=24.894 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=4 ttl=254 time=30.058 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=5 ttl=254 time=33.852 ms (ICMP type:3, code:1, Destination host unreachable)

PC3> ping 10.0.213.74
*10.0.12.4 icmp_seq=1 ttl=254 time=28.419 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=2 ttl=254 time=24.507 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=3 ttl=254 time=30.754 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=4 ttl=254 time=30.129 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.4 icmp_seq=5 ttl=254 time=30.655 ms (ICMP type:3, code:1, Destination host unreachable)
```

*Ilustración 34 PC3 no alcanza PC1 y PC2*

Como se mencionó anteriormente, los VRF nos permiten segmentar en capa 3 y ayuda a crear subredes la cuales benefician a las empresas el poder dividir ciertos servicios. Como en este caso PC1 y PC2 pertenecen a un mismo VRF y es por eso que permite su comunicación a nivel de capa 3, lo mismo pasa entre PC3 y PC4. Pero estos PC's no pueden verse entre sí, es decir, PC3 y PC1 no pueden verse debido a que se encuentran en VRF distintos, lo mismo pasa con PC2 y PC4.

## Parte 4 Configurar la Seguridad

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

*Tabla 18 Configurar la seguridad*

Tarea	Tarea	Especificación
4.1	En todos los dispositivos, EXE privilegiado seguro modo.	Configure un secreto de habilitación de la siguiente manera: <ul style="list-style-type: none"> <li>• Tipo de algoritmo: SCRYPT</li> <li>• Contraseña: nombrestudianteXYZ</li> </ul>
4.2	En todos los dispositivos, cree un usuario de cuenta local.	Configurar un usuario local: <ul style="list-style-type: none"> <li>• Nombre: administrador</li> <li>• Nivel de privilegio: 15</li> <li>• Tipo de algoritmo: SCRYPT</li> <li>• Contraseña: nombrestudianteXYZ.</li> </ul>
4.3	En todos los dispositivos, habilite AAA y habilite la autenticación AAA	Habilite la autenticación AAA usando el local base de datos en todas las líneas.

Empezaremos con las configuraciones referente al modo privilegiado:

### 4.1 En todos los dispositivos, configurar el modo privilegiado EXE

*Tabla 19 Configuración EXE modo privilegiado*

<b>R1, R2 y R3:</b> enable secret diegoparedes748  <b>D1, D2 y A1:</b> enable algorithm-type scrypt secret diegoparedes748	En modo privilegiado, digitamos el comando en cada uno de los dispositivos
--	--

<pre>R1(config)#enable sec R1(config)#enable secret ? 0 Specifies an UNENCRYPTED password will follow 5 Specifies a MD5 HASHED secret will follow LINE The UNENCRYPTED (cleartext) 'enable' secret level Set exec level password  R1(config)#enable secret diegoparedes748</pre> <p><i>Ilustración 35 Enable Secret R1</i></p>	<pre>R2(config)#en R2(config)#en R2(config)#ena R2(config)#enable se R2(config)#enable secret diegoparedes748 R2(config)#</pre> <p><i>Ilustración 36 Enable Secret R2</i></p>
<pre>R3(config)#en R3(config)#ena R3(config)#enable secre R3(config)#enable secret diegoparedes748 R3(config)#</pre> <p><i>Ilustración 37 Enable Secret R3</i></p>	<pre>D1(config)#en D1(config)#enab D1(config)#enable al D1(config)#enable algorithm-type s D1(config)#enable algorithm-type sc D1(config)#enable algorithm-type scrypt sec D1(config)#enable algorithm-type scrypt secret diegoparedes748 D1(config)#</pre> <p><i>Ilustración 38 Enable Secret D1</i></p>
<pre>D2(config)#en D2(config)#ena D2(config)#enable alg D2(config)#enable algorithm-type sc D2(config)#enable algorithm-type scrypt se D2(config)#enable algorithm-type scrypt secret diegoparedes748 D2(config)#</pre> <p><i>Ilustración 39 Enable Secret D2</i></p>	<pre>A1(config)#en A1(config)#ena A1(config)#enable al A1(config)#enable algorithm-type sc A1(config)#enable algorithm-type scrypt sec A1(config)#enable algorithm-type scrypt secret diegoparedes748 A1(config)#</pre> <p><i>Ilustración 40 Enable Secret A1</i></p>

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

*Tabla 20 Creación de cuenta Local*

<pre>username admin privilege 15 algorithm-type scrypt secret diegoparedes748</pre>	<p>En modo privilegiado, digitamos el comando en cada uno de los dispositivos el cual crea una cuenta local con su respectiva contraseña</p>
---	--

```
R1(config)#user
R1(config)#username admin pri
R1(config)#username admin privilege 15 al
R1(config)#username admin privilege 15 algo
R1(config)#username admin privilege 15 algor
R1(config)#username admin privilege 15 algori
R1(config)#username admin privilege 15 se
R1(config)#username admin privilege 15 secret diegoparedes748
R1(config)#
```

*Ilustración 41 Creación cuenta local R1*

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user
R2(config)#username admin privilege 15 secret diegoparedes748
R2(config)#
```

*Ilustración 42 Creación cuenta local R2*

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#user
R3(config)#username admin privilege 15 secret diegoparedes748
R3(config)#
```

*Ilustración 43 Creación cuenta local R3*

```
D1#config t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#usern
D1(config)#usern
D1(config)#username admin
D1(config)#$min privilege 15 algorithm-type scrypt secret diegoparedes748
D1(config)#
```

*Ilustración 44 Creación cuenta local D1*

```
D2#config t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#usern
D2(config)#$min privilege 15 algorithm-type scrypt secret diegoparedes748
D2(config)#end
```

*Ilustración 45 Creación cuenta local D2*

```
A1#config t
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#userna
A1(config)#$min privilege 15 algorithm-type scrypt secret diegoparedes748
A1(config)#end
A1#
```

*Ilustración 46 Creación cuenta local A1*

### 4.3 En todos los dispositivos, habilite AAA y habilite la autenticación AAA

*Tabla 21 Configuración de autenticación AAA*

<pre>aaa new-model  aaa authentication login default local</pre>	En modo privilegiado, digitamos el comando en cada uno de los dispositivos para habilitar la autenticación AAA.
--	---

```
R1(config)#aaa ne  
R1(config)#aaa new-model  
R1(config)#aaa aut  
R1(config)#aaa authen  
R1(config)#aaa authentication login default lo  
R1(config)#aaa authentication login default local  
R1(config)#end
```

*Ilustración 47 Autenticación AAA R1*

```
R2(config)#aaa ne  
R2(config)#aaa new-model  
R2(config)#aaa aut  
R2(config)#aaa authe  
R2(config)#aaa authentication login default lo  
R2(config)#aaa authentication login default local  
R2(config)#end
```

*Ilustración 48 Autenticación AAA R2*

```
R3(config)#aaa ne  
R3(config)#aaa new-model  
R3(config)#aaa aut  
R3(config)#aaa authe  
R3(config)#aaa authentication login default lo  
R3(config)#aaa authentication login default local
```

*Ilustración 49 Autenticación AAA R3*

```
D1(config)#aaa ne  
D1(config)#aaa new-model  
D1(config)#aaa auth  
D1(config)#aaa authe  
D1(config)#aaa authentication login default lo  
D1(config)#aaa authentication login default local  
D1(config)#end
```

*Ilustración 50 Autenticación AAA D1*

```
D2(config)#aaa ne
D2(config)#aaa new-model
D2(config)#aaa authe
D2(config)#aaa authentication login default lo
D2(config)#aaa authentication login default local
D2(config)#end
```

*Ilustración 51 Autenticación AAA D2*

```
A1(config)#aaa ne
A1(config)#aaa new-model
A1(config)#aaa aut
A1(config)#aaa authe
A1(config)#aaa authentication login default lo
A1(config)#aaa authentication login default local
A1(config)#end
```

*Ilustración 52 Autenticación AAA A1*

La autenticación AAA en Cisco se utiliza para controlar y gestionar el acceso de usuarios a dispositivos de red, como switches y routers. AAA significa Autenticación, Autorización y Contabilidad, y estas tres funciones son esenciales para garantizar la seguridad y la integridad de los sistemas de red. La autenticación AAA permite verificar la identidad de los usuarios que intentan acceder al dispositivo de red. Esto se logra a través de un proceso de autenticación que requiere que los usuarios proporcionen credenciales de autenticación, como un nombre de usuario y una contraseña. El proceso de autenticación verifica las credenciales proporcionadas por el usuario y autoriza o deniega el acceso en consecuencia. Tener una cuenta local en el switch es importante para la autenticación AAA ya que los usuarios necesitan un nombre de usuario y una contraseña para iniciar sesión en el dispositivo de red. La cuenta local proporciona un nivel adicional de seguridad, ya que los usuarios deben tener una cuenta en el dispositivo para acceder a él. Habilitar la clave EXE es otra medida de seguridad importante en la autenticación AAA en Cisco. La clave EXE es una contraseña que se utiliza para acceder a ciertos comandos en el switch. Al habilitar la clave EXE, se limita el acceso a ciertos comandos a usuarios autorizados, lo que ayuda a prevenir cambios no autorizados en la configuración del switch.

## CONCLUSION

En conclusión, el presente trabajo de grado de ingeniería ha permitido la implementación de tecnologías avanzadas en redes de comunicaciones utilizando equipamiento Cisco. En particular, se ha llevado a cabo la implementación de VRF, VLAN, enrutamiento estático, y la creación de cuentas con autenticación AAA. La implementación de VRF ha permitido la creación de múltiples instancias de enrutamiento virtual para la separación y aislamiento de tráfico en la red. La implementación de VLAN ha permitido la segmentación de la red en dominios de broadcast separados, lo que mejora la seguridad y la eficiencia en la transmisión de datos. La configuración de enrutamiento estático ha proporcionado una forma sencilla y segura de configurar las rutas de red necesarias para el correcto funcionamiento de la infraestructura de red. Además, la creación de cuentas con autenticación AAA ha proporcionado una capa adicional de seguridad en la red, ya que sólo los usuarios autorizados pueden acceder a los dispositivos de red. La implementación de estas tecnologías ha permitido la creación de una red de comunicaciones robusta y segura, lo que contribuye al buen funcionamiento de la organización. Se espera que este trabajo sirva como una referencia útil para futuras implementaciones de redes de comunicaciones.

## **BIBLIOGRAFIA**

FROOM, R., FRAHIM, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. <https://1drv.ms/b/s!AmIJYeINT1InWR0hoMxgBNv1CJ>

TEARE, D., VACHON B., GRAZIANI, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. <https://1drv.ms/b/s!AmIJYeINT1InMfy2rhPZHwEoWx>