

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN SEBASTIÁN SOTO BALLESTEROS

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

BOGOTÁ

2023

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN SEBASTIÁN SOTO BALLESTEROS

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

DIRECTOR:
JOHN HAROLD PÉREZ CALDERÓN

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 18 de abril de 2023

AGRADECIMIENTOS

En este proceso de mi vida, doy mis más grandes agradecimientos a Dios, por permitirme haber alcanzado este logro en mi carrera, por regalarme cada día vida y salud para superar los desafíos que un estudiante de ingeniería afronta a lo largo del proceso formativo. Por otra parte, agradezco a mis padres quienes constantemente han estado en mi proceso de formación, a mi familia, a mis amigos y allegados.

Al grupo de docentes de la universidad también agradezco, por cada enseñanza y por el seguimiento que realizaron a mi proceso de formación en cada uno de los cursos que contiene la ingeniería de Telecomunicaciones.

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	6
LISTA DE FIGURAS.....	7
GLOSARIO	9
RESUMEN	10
<i>ABSTRACT</i>	10
INTRODUCCIÓN.....	11
1. PRIMER ESCENARIO.....	12
1.1. Construir y Cablear la red	12
1.2. Configurar los ajustes básicos para cada dispositivo.....	14
1.3. Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento.....	19
1.4. Configurar VRF.....	21
1.5. Configure IPv4 and IPv6 en las interfaces	24
1.6. Configurar rutas estáticas que apuntan a R2	30
1.7. Verificar la conectividad en cada VRF.....	33
2. SEGUNDO ESCENARIO	35
2.1. Desactivar todas las interfaces En D1, D2, y A1	35
2.2. Configurar el enlace troncal hacia R1 y R3	36
2.3. Configurar EtherChannel en D1 y A1.....	38
2.4. Configure los puertos de acceso para los computadores en D1, D2 y A1	40
2.5. Verificar la conectividad de PC a PC	42
2.6. Modo privilegiado en todos los dispositivos	44
2.7. Cuenta de Usuario local en todos los dispositivos	46
2.8. Autenticación AAA en todos los dispositivos	47
CONCLUSIONES	52
BIBLIOGRAFÍA.....	53

LISTA DE TABLAS

Tabla 1. Direccionamiento IP.....	13
Tabla 2. Script Configuración Inicial Routers	14
Tabla 3. Script Configuración Inicial Switch.....	15
Tabla 4. Script Configuración IP de Computadores	19
Tabla 5. Script Configuración VRF Routers.....	22
Tabla 6. Script Configuración Interfaces Router 1.....	24
Tabla 7 Script Configuración Interfaces Router 2.....	25
Tabla 8 Script Configuración Interfaces Router 3.....	26
Tabla 9. Script Enrutamiento Router 1	30
Tabla 10. Script Enrutamiento Router 2.....	30
Tabla 11. Script Enrutamiento Router 3	31
Tabla 12. Script para desactivar Interfaces Switch	35
Tabla 13. Script Configuración Enlace Troncal	36
Tabla 14. Script Configuración EtherChannel.....	38
Tabla 15. Script Asignación Vlan a Puertos.....	40
Tabla 16. Script Configuración Modo Privilegiado.....	45
Tabla 17. Script Configuración Cuentas de Usuario	46
Tabla 18. Script Autenticación AAA.....	47

LISTA DE FIGURAS

Figura 1. Escenario Por Construir.....	12
Figura 2. Escenario Construido y Cableado	13
Figura 3. Show running-config Configuración Básica Router 1	16
Figura 4. Show running-config Configuración Básica Router 2	17
Figura 5. Show running-config Configuración Básica Router 3	17
Figura 6. Show running-config Configuración Básica Switch D1.....	18
Figura 7. Show running-config Configuración Básica Switch D2.....	18
Figura 8. Show running-config Configuración Básica Switch A1	19
Figura 9. Configuración IP Computador 1	20
Figura 10. Configuración IP Computador 2.....	20
Figura 11. Configuración IP Computador 3	21
Figura 12. Configuración IP Computador 4.....	21
Figura 13. Configuración VRF Lite Router 1	23
Figura 14. Configuración VRF Lite Router 2.....	23
Figura 15. Configuración VRF Lite Router 3.....	23
Figura 16. Configuración Interfaces Router 1	27
Figura 17. Configuración Interfaces R2	28
Figura 18. Configuración Interfaces R3	29
Figura 19. Configuración Rutas Estáticas R1	32
Figura 20. Configuración Rutas Estáticas R2.....	32
Figura 21. Configuración Rutas Estáticas R3.....	32
Figura 22. Ping vrf General-Users 10.0.208.9	33
Figura 23. Ping vrf General-Users 2001:db8:acad:208::1	33
Figura 24. Ping vrf Special-Users 10.0.213.9	34
Figura 25. Ping vrf Special-Users 2001:db8:acad:213::1.....	34
Figura 26. Estado de las Interfaces Switch D1.....	37
Figura 27. Estado de las Interfaces Switch D2.....	37
Figura 28. Estado de las Interfaces Switch A1	38
Figura 29. Configuración EtherChannel Switch D1.....	39
Figura 30. Configuración EtherChannel Switch D1.....	40

Figura 31. Vlans Asociadas a Puertos Switch D1	41
Figura 32. Vlans Asociadas a Puertos Switch D2	42
Figura 33. Vlans Asociadas a Puertos Switch A1	42
Figura 34. Ping IPV4 PC1 a PC2.....	43
Figura 35. Ping IPV6 PC1 a PC2.....	43
Figura 36. Ping IPV4 PC3 a PC4.....	44
Figura 37. Ping IPV4 PC3 a PC4.....	44
Figura 38. Autenticación AAA Router 1	48
Figura 39. Autenticación AAA Router 2.....	48
Figura 40. Autenticación AAA Router 3.....	48
Figura 41. Autenticación AAA Switch D1	49
Figura 42. Autenticación AAA Switch D2	49
Figura 43. Autenticación AAA Switch A1.....	49
Figura 44. Mensaje de Credenciales Router 1	50
Figura 45. Mensaje de Credenciales Router 2	50
Figura 46. Mensaje de Credenciales Router 3	50
Figura 47. Mensaje de Credenciales Switch D1.....	51
Figura 48. Mensaje de Credenciales Switch D2.....	51
Figura 49. Mensaje de Credenciales Switch A1	51

GLOSARIO

ENLACE TRONCAL: Es un enlace punto a punto que funciona para poder transmitir varias *Vlans* por medio de una misma interfaz entre dispositivos de capa 2 y capa 3. Dichas interfaces en las cuales se aplica un enlace troncal deben contener subinterfaces lógicas las cuales trabajan por medio del estándar *IEEE 802.1Q*.

ETHERCHANNEL: Corresponde a una tecnología basada en los estándares *802.3 full-dúplex Fast Ethernet* la cual permite agrupar varios enlaces físicos de tipo *Ethernet* en enlaces lógicos. Dentro de esta tecnología se trabajan ciertos protocolos, como son *PAgP, Auto, Desirable, LACP*

ROUTER: Consiste en un dispositivo que tiene como función principal enviar y recibir tráfico informático, con el objetivo que mejorar el acceso a internet, también se conoce como enrutador y esto se debe a que, en el proceso de enviar y recibir tráfico, el dispositivo elige la mejor ruta para llegar a los dispositivos de destino.

SWITCH: También es llamado conmutador, y es un dispositivo que está enfocado en la escalabilidad de las redes porque está diseñado para interconectar dispositivos y de esta manera conformar una red de área local. Un switch está diseñado para soportar conectividades entre impresoras, computadores, o cualquier dispositivo final en una red.

VLAN: Son redes de área local, pero que tienen las características de tener virtualización, y sirven para segmentar las redes físicas. Las vlan dentro de una red tienen bastante importancia porque contribuyen a mejorar la seguridad, flexibilidad, mejorar costos, administrar de mejor manera aplicaciones y en general optimizar la calidad del tráfico de datos.

VRF: Hace referencia a una tecnología que permite a los *Routers* poder manejar varios protocolos de enrutamiento de forma simultánea e independiente, es muy utilizado en redes en las cuales se requieren tener dos puertas de enlace con la misma dirección IP. Esta tecnología contribuye a mejorar la funcionalidad de una red, mantener el tráfico separado, aumentar la seguridad, y permite extenderse a múltiples dispositivos.

RESUMEN

Las redes de Cisco juegan un papel muy importante en el sector de telecomunicaciones, sistemas y electrónica y es por este motivo que el correcto manejo de equipos, lenguajes y protocolos pertenecientes a Cisco, contribuyen a fortalecer la formación de los ingenieros porque genera que se abran los caminos en los entornos de tecnología para obtener mejores oportunidades de empleo.

Este trabajo está enfocado en desarrollar habilidades de *CCNP*, por lo cual se ejecutan configuraciones para la conmutación y enrutamiento de paquetes por medio de *VRF* tanto en *IPV4* como en *IPV6*, utilizando la plataforma *GNS3* en equipos de 3 y multicapa.

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

ABSTRACT

Cisco networks play a very important role in the telecommunications, systems and electronics sector and it is for this reason that the correct handling of equipment, languages and protocols belonging to Cisco contributes to strengthening the training of engineers because it generates pathways in technology environments for better employment opportunities.

This work is focused on developing CCNP skills, for which configurations for packet switching and routing are executed through VRF in both IPV4 and IPV6, using the GNS3 platform in 3 and multilayer equipment.

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

INTRODUCCIÓN

A continuación, se desarrolla un ejercicio denominado prueba de habilidades prácticas correspondientes al Diplomado de Profundización *CISCO CCNP*. El presente documento tiene gran importancia, puesto que corresponde al trabajo escrito que evidencia la apropiación de las temáticas enseñadas dentro del curso, con el objetivo de culminar satisfactoriamente el proceso formativo como Ingeniero de Telecomunicaciones y de esta manera obtener el título profesional.

La ejecución de esta prueba de habilidades comienza desde la asignación de una topología de red suministrada los docentes del curso, la cual debe ser cableada y configurada mediante el emulador GNS3. Esta tarea se desarrolla en dos partes, la primera consiste en la configuración de los equipos de capa 3, en las cuales se establece el direccionamiento IP tanto en versión 4 como en versión 6, creación de *VRF*, y enrutamiento

Una vez culminada la primera parte, se procede a continuar con la segunda la cual consiste en la configuración de los equipos de capa 2, por lo tanto, se establecen enlaces troncales, EtherChannel, administración de puertos en los switches, y se finaliza con las configuraciones de seguridad, y aplicación de estándares AAA. Para cada una de las prácticas contenidas en la primera y segunda parte, se presentan los Scripts de configuración, pantallazos de la interfaz de consola correspondiente a cada equipo para evidenciar la correcta configuración, y finalmente se muestran las pruebas de conectividad entre equipos finales.

1. PRIMER ESCENARIO

El desarrollo de este trabajo comienza con la entrega de una topología de red por parte de los docentes del Diplomado de Profundización *Cisco CCNP*, la cual debe construirse, cablearse y configurarse para al final del ejercicio conseguir comunicación entre las sub-interfaces de los equipos de capa 3.

Figura 1. Escenario Por Construir

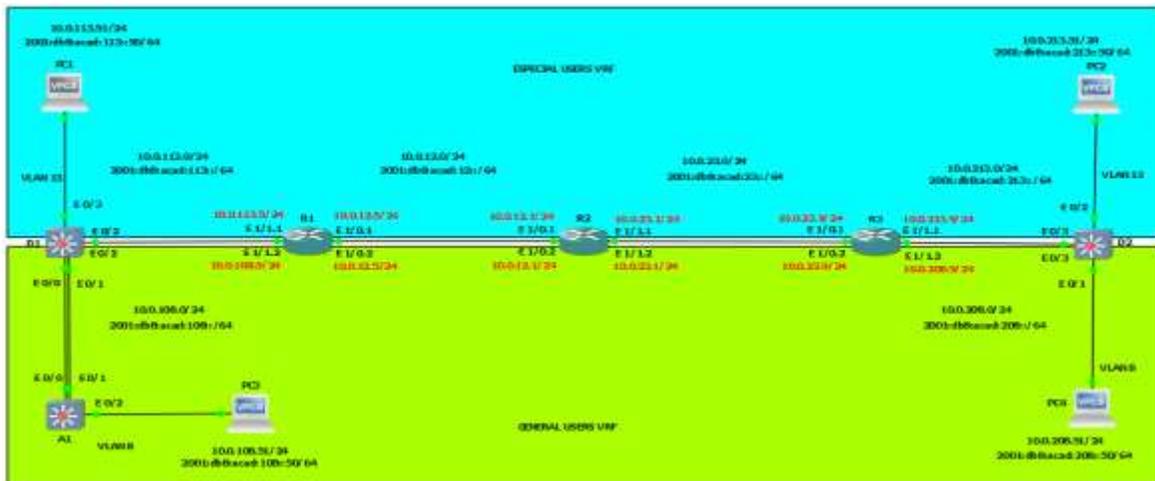


Fuente: Prueba de habilidades Cisco CCNP

1.1. Construir y Cablear la red

Se realiza la instalación de la máquina virtual y de *GNS*, posteriormente se requiere descargar los archivos de imágenes de cada uno de los dispositivos que conforman la red. Una vez se encuentren descargadas las imágenes, es necesario cargarlas al entorno de *GNS* para comenzar a cablear.

Figura 2. Escenario Construido y Cableado



Fuente: elaboración propia.

El objetivo de la práctica es configurar el escenario construido en GNS3 con base al direccionamiento ip contemplado en la Tabla 1.

Tabla 1. Direccionamiento IP

Dispositivo	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.5/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.1/24	2001:db8:acad:12::2/64	fe80::1:2
	E1/1.1	10.0.113.5/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.5/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.1/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.1/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.1/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.9/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.9/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.9/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.9/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.51/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.51/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.51/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.51/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Prueba de habilidades Cisco CCNP

1.2. Configurar los ajustes básicos para cada dispositivo

Para cada uno de los dispositivos es necesario configurar aspectos básicos tales como nombre, habilitación de *routing* para ipv6, configuración del banner y consola. A continuación, se describe el Script empleado para cada dispositivo y de esa forma obtener la configuración requerida.

Tabla 2. Script Configuración Inicial Routers

Configuración Router 1	Descripción
<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>Asigna nombre al Router Permite routing en IPV6 Bloquea Búsqueda DNS Configura Mensaje de Inicio</p> <p>Configura la consola</p> <p>Salir de la Configuración</p>
Configuración Router 2	Descripción
<pre>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</pre>	<p>Asigna nombre al Router Permite routing en IPV6 Bloquea Búsqueda DNS Configura Mensaje de Inicio</p> <p>Configura la consola</p> <p>Salir de la Configuración</p>
Configuración Router 3	Descripción
<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>Asigna nombre al Router Permite routing en IPV6 Bloquea Búsqueda DNS Configura Mensaje de Inicio</p> <p>Configura la consola</p> <p>Salir de la Configuración</p>

Fuente: elaboración propia.

Para el caso de los Switch se realiza la misma configuración básica de los Routers, pero adicionalmente se crean 2 *Vlans* con sus respectivos nombres.

Tabla 3. Script Configuración Inicial Switch

Configuración Switch D1	Descripción
<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>Asigna nombre al Switch</p> <p>Permite routing en IPV6 Bloquea Búsqueda DNS Configura Mensaje de Inicio</p> <p>Configura la consola</p> <p>Creación del número de Vlan Creación del nombre de la Vlan</p> <p>Creación del número de Vlan Creación del nombre de la Vlan</p>
Configuración Switch D2	Descripción
<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>	<p>Asigna nombre al Switch</p> <p>Permite routing en IPV6 Bloquea Búsqueda DNS Configura Mensaje de Inicio</p> <p>Configura la consola</p> <p>Creación del número de Vlan Creación del nombre de la Vlan</p> <p>Creación del número de Vlan Creación del nombre de la Vlan</p>

Configuración Switch A1	Descripción
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	Asigna nombre al Switch Permite routing en IPV6 Bloquea Búsqueda DNS Configura Mensaje de Inicio Configura la consola Creación del número de Vlan

Fuente: elaboración propia.

Una vez ejecutado el script para cada dispositivo, se requiere realizar una validación para corroborar la correcta configuración, para lo cual se emplea el comando *Show running-config* en cada Router y Switch. Por lo tanto, se evidencia el registro fotográfico del comando anteriormente mencionado aplicándose en cada uno de los dispositivos

Figura 3. *Show running-config* Configuración Básica Router 1

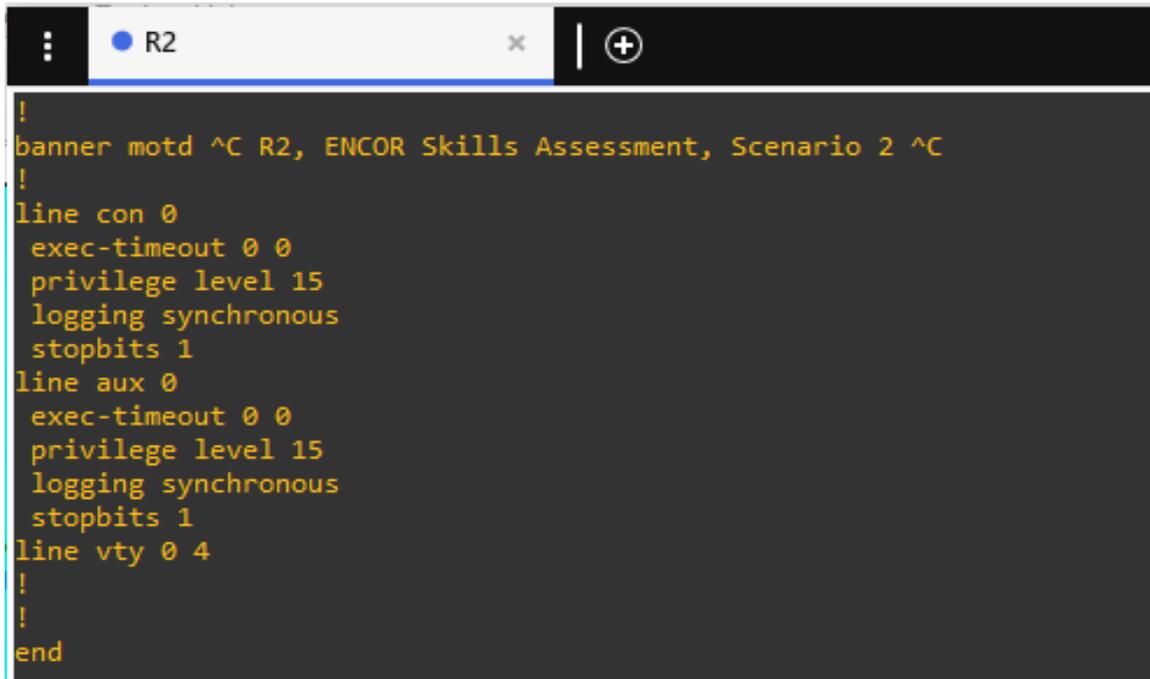
```

!
control-plane
!
banner motd ^C R1, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
!
!
end

```

Fuente: elaboración propia.

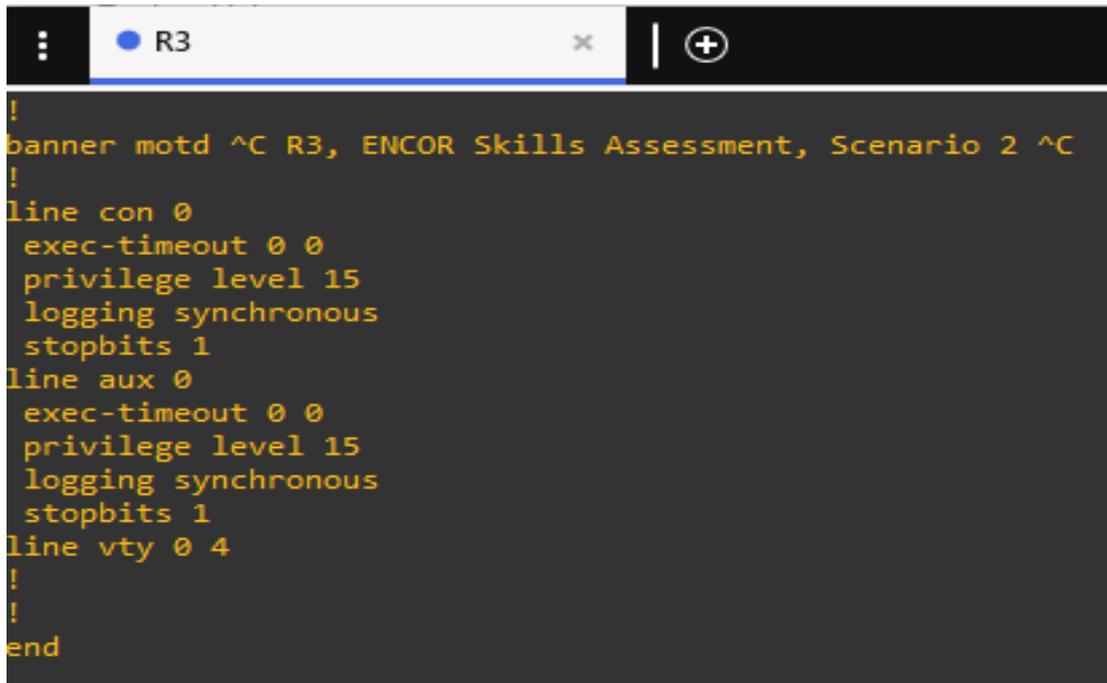
Figura 4. *Show running-config* Configuración Básica Router 2



```
!
banner motd ^C R2, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
!
!
end
```

Fuente: elaboración propia.

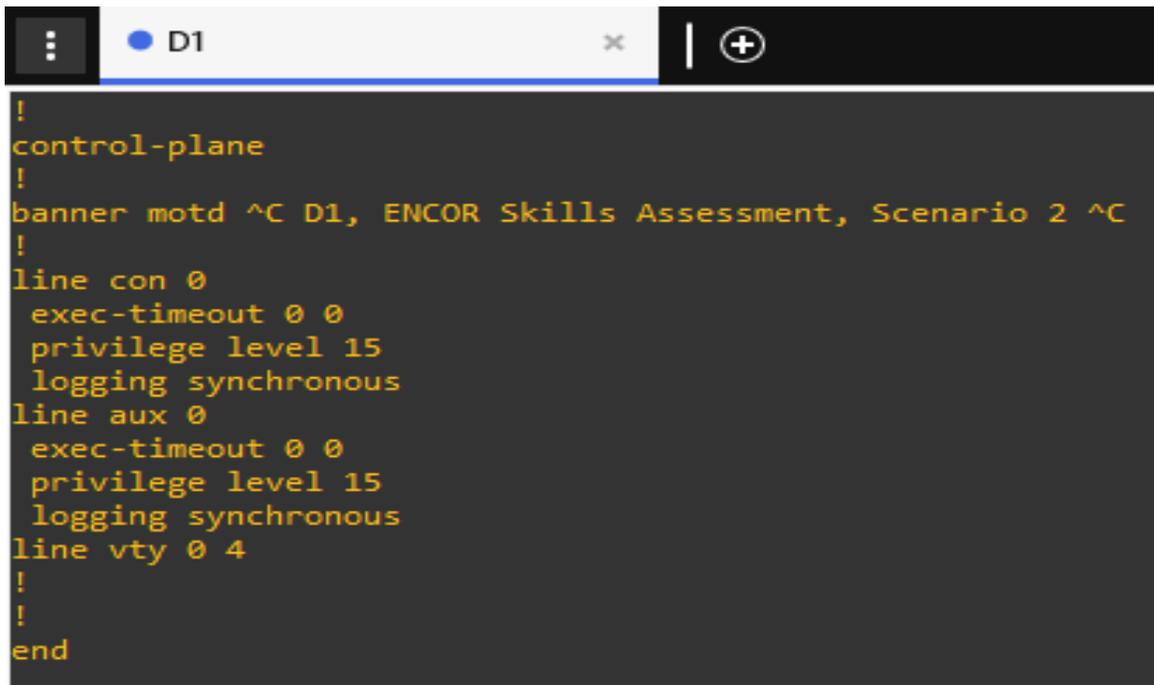
Figura 5. *Show running-config* Configuración Básica Router 3



```
!
banner motd ^C R3, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
!
!
end
```

Fuente: elaboración propia.

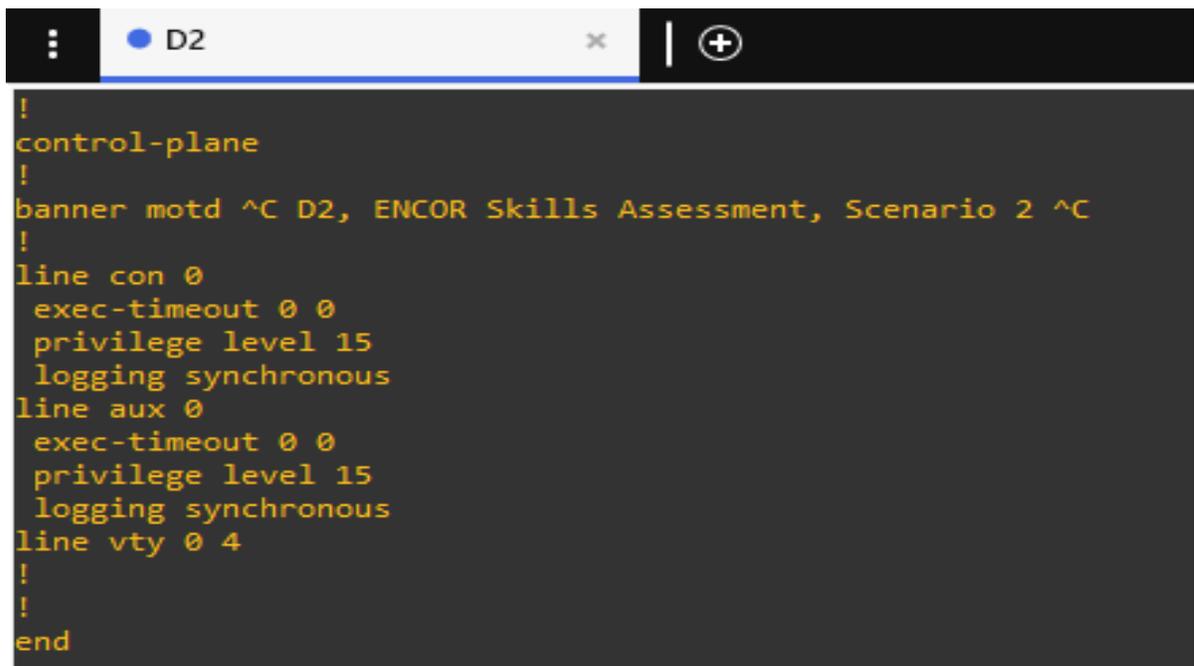
Figura 6. *Show running-config* Configuración Básica Switch D1



```
!
control-plane
!
banner motd ^C D1, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
!
!
end
```

Fuente: elaboración propia.

Figura 7. *Show running-config* Configuración Básica Switch D2



```
!
control-plane
!
banner motd ^C D2, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
!
!
end
```

Fuente: elaboración propia.

Figura 8. *Show running-config* Configuración Básica Switch A1

```

!
control-plane
!
banner motd ^C A1, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
!
!
end

```

Fuente: elaboración propia.

- 1.3. Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento.

Para realizar la configuración de dirección IPV4 e IPV6, se debe ingresar a cada uno de los computadores por medio del acceso de consola y digitar cada uno de los Scripts que se contemplan en la tabla 4.

Es de suma importancia escribir `save` en cada configuración de consola porque de esta forma se garantiza que los cambios queden guardados y no se pierdan cuando se cierre el emulador GNS3

Tabla 4. Script Configuración IP de Computadores

Configuración Computador 1	Descripción
ip 10.0.113.51/24 10.0.113.5	Configuración Ipv4 y puerta de enlace
ip 2001:db8:acad:113::50/64	Configuración Ipv6
save	Guardar
Configuración Computador 2	Descripción
ip 10.0.213.51/24 10.0.213.9/24	Configuración Ipv4 y puerta de enlace
ip 2001:db8:acad:213::50/64	Configuración Ipv6
save	Guardar

Configuración Computador 3	Descripción
ip 10.0.108.51/24 10.0.108.5/24 ip 2001:db8:acad:108::50/64 save	Configuración Ipv4 y puerta de enlace Configuración Ipv6 Guardar
Configuración Computador 4	Descripción
ip 10.0.208.51/24 10.0.208.9/24 ip 2001:db8:acad:208::50/64 save	Configuración Ipv4 y puerta de enlace Configuración Ipv6 Guardar

Fuente: elaboración propia.

Luego de efectuar la configuración en cada computador, se procede a verificar el direccionamiento IP, para lo cual se ejecuta el comando *sh* desde la consola de cada computador.

Figura 9. Configuración IP Computador 1

```

PC1>
PC1> sh

NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC1       10.0.113.51/24   10.0.113.5      00:50:79:66:68:00 10008  127.0.0.1:10009
          fe80::250:79ff:fe66:6800/64
          2001:db8:acad:113::50/64

PC1>

```

Fuente: elaboración propia.

Figura 10. Configuración IP Computador 2

```

PC2>
PC2>
PC2> sh

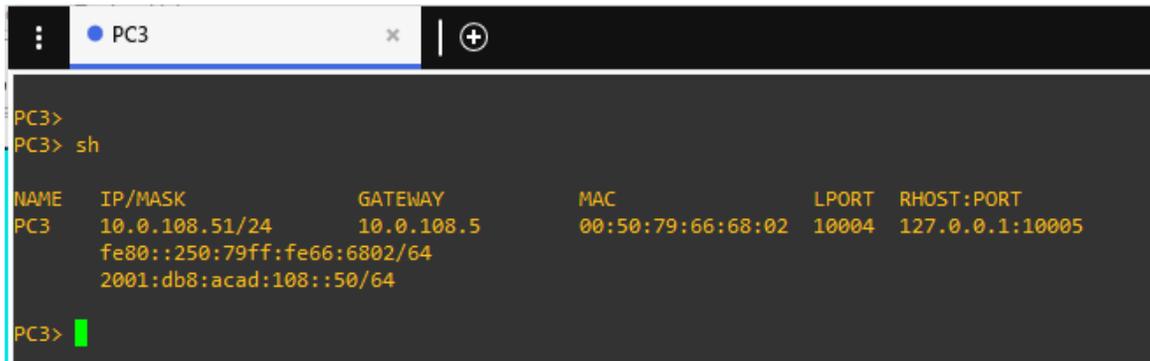
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC2       10.0.213.51/24   10.0.213.9      00:50:79:66:68:01 10006  127.0.0.1:10007
          fe80::250:79ff:fe66:6801/64
          2001:db8:acad:213::50/64

PC2>

```

Fuente: elaboración propia.

Figura 11. Configuración IP Computador 3



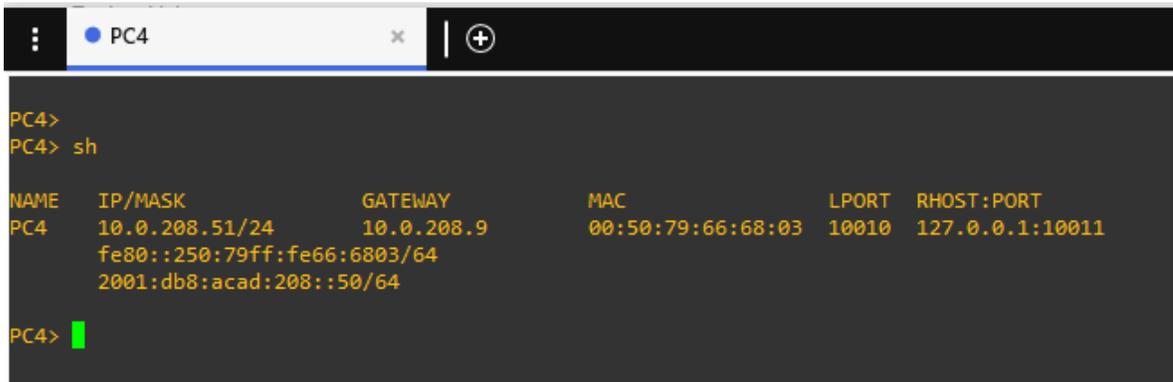
```
PC3>
PC3> sh

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC3      10.0.108.51/24  10.0.108.5   00:50:79:66:68:02  10004  127.0.0.1:10005
         fe80::250:79ff:fe66:6802/64
         2001:db8:acad:108::50/64

PC3>
```

Fuente: elaboración propia.

Figura 12. Configuración IP Computador 4



```
PC4>
PC4> sh

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC4      10.0.208.51/24  10.0.208.9   00:50:79:66:68:03  10010  127.0.0.1:10011
         fe80::250:79ff:fe66:6803/64
         2001:db8:acad:208::50/64

PC4>
```

Fuente: elaboración propia.

1.4. Configurar VRF

En esta parte se establece la configuración de VRF la cual se lleva a cabo en los equipos de capa 3, el objetivo de esta configuración es establecer 2 vrf, la primera denominada *General-Users* y la segunda *Special-Users*.

Cada una de las VRF deben soportar trabajar con *IPV4* e *IPV6*. Para esto se aplica el Script contemplado en la tabla 5, para cada Router.

Tabla 5. Script Configuración VRF Routers

Configuración VRF Lite R1	Descripcion
<pre>vrf definition General-Users address-family ipv4 address-family ipv6 exit</pre>	<p>Creación y Definición de vrf Se habilita para ipv4 Se habilita para ipv6</p>
<pre>vrf definition Special-Users address-family ipv4 address-family ipv6 exit</pre>	<p>Creación y Definición de vrf Se habilita para ipv4 Se habilita para ipv6</p>
Configuración VRF Lite R2	Descripcion
<pre>vrf definition General-Users address-family ipv4 address-family ipv6 exit</pre>	<p>Creación y Definición de vrf Se habilita para ipv4 Se habilita para ipv6</p>
<pre>vrf definition Special-Users address-family ipv4 address-family ipv6 exit</pre>	<p>Creación y Definición de vrf Se habilita para ipv4 Se habilita para ipv6</p>
Configuración VRF Lite R3	Descripcion
<pre>vrf definition General-Users address-family ipv4 address-family ipv6 exit</pre>	<p>Creación y Definición de vrf Se habilita para ipv4 Se habilita para ipv6</p>
<pre>vrf definition Special-Users address-family ipv4 address-family ipv6 exit</pre>	<p>Creación y Definición de vrf Se habilita para ipv4 Se habilita para ipv6</p>

Fuente: elaboración propia.

Luego de digitar cada Script se procede a validar la correcta configuración en cada Router por medio del comando *show vrf brief*

Figura 13. Configuración VRF Lite Router 1

```
R1#
R1#
R1#show vrf lis
*Apr 11 01:32:23.539: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ether
/2 (half duplex).
R1#show vrf br
R1#show vrf brief
  Name                Default RD          Protocols           Interfaces
  General-Users        <not set>           ipv4,ipv6           Et1/0.2
                                                              Et1/1.2
  Special-Users        <not set>           ipv4,ipv6           Et1/0.1
                                                              Et1/1.1
```

Fuente: elaboración propia.

Figura 14. Configuración VRF Lite Router 2

```
R2#sh
R2#sh vr
R2#sh vrf
R2#sh vrf br
R2#sh vrf brief
  Name                Default RD          Protocols           Interfaces
  General-Users        <not set>           ipv4,ipv6           Et1/0.2
                                                              Et1/1.2
  Special-Users        <not set>           ipv4,ipv6           Et1/0.1
                                                              Et1/1.1
```

Fuente: elaboración propia.

Figura 15. Configuración VRF Lite Router 3

```
R3#show vrf
R3#show vrf br
R3#show vrf brief
  Name                Default RD          Protocols           Interfaces
  General-Users        <not set>           ipv4,ipv6           Et1/0.2
                                                              Et1/1.2
  Special-Users        <not set>           ipv4,ipv6           Et1/0.1
                                                              Et1/1.1
```

Fuente: elaboración propia.

1.5. Configure IPv4 and IPv6 en las interfaces

Se configuran las interfaces de los equipos de capa 3 de acuerdo con la tabla de direccionamiento IP. Y según la topología del escenario propuesto es necesario configurar sub-interfaces, es decir interfaces lógicas que se encuentran dentro de las interfaces físicas.

Por este motivo en las sub-interfaces de los Routers se debe activar el encapsulamiento *dot1Q*, adicionalmente se debe aplicar cada uno de los VRF configurados previamente. Por último, se asocia la dirección IPV4 e IPV5 y se encienden las interfaces.

Tabla 6. Script Configuración Interfaces Router 1

Configuración Interfaces R1	Descripción
<pre>interface ethernet 1/1 no ip address no shutdown exit</pre>	<p>Se configura interfaz No se le asigna IP Se enciende la interfaz</p>
<pre>interface ethernet 1/1.1 encapsulation dot1Q 13 vrf forwarding Special-Users ip address 10.0.113.5 255.255.255.0 ipv6 address fe80::1:3 link-local ipv6 address 2001:db8:acad:113::1/64 no shutdown exit</pre>	<p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
<pre>interface ethernet 1/1.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.108.5 255.255.255.0 ipv6 address fe80::1:4 link-local ipv6 address 2001:db8:acad:108::1/64 no shutdown exit</pre>	<p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
<pre>interface ethernet 1/0 no ip address no shutdown exit</pre>	<p>Se configura interfaz No se le asigna IP Se enciende la interfaz</p>
<pre>interface ethernet 1/0.1 encapsulation dot1Q 13 vrf forwarding Special-Users ip address 10.0.12.5 255.255.255.0</pre>	<p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4</p>

<pre> ipv6 address fe80::1:1 link-local ipv6 address 2001:db8:acad:12::1/64 no shutdown exit interface ethernet 1/0.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.12.5 255.255.255.0 ipv6 address fe80::1:2 link-local ipv6 address 2001:db8:acad:12::1/64 no shutdown exit </pre>	<p>Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p> <p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
--	--

Fuente: elaboración propia.

Tabla 7 Script Configuración Interfaces Router 2

Configuración Interfaces R2	Descripción
<pre> interface ethernet 1/0 no ip address no shutdown exi </pre>	<p>Se configura interfaz No se le asigna IP Se enciende la interfaz</p>
<pre> interface ethernet 1/0.1 encapsulation dot1Q 13 vrf forwarding Special-Users ip address 10.0.12.1 255.255.255.0 ipv6 address fe80::2:1 link-local ipv6 address 2001:db8:acad:12::2/64 no shutdown exit </pre>	<p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
<pre> interface ethernet 1/0.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.12.1 255.255.255.0 ipv6 address fe80::2:2 link-local ipv6 address 2001:db8:acad:12::2/64 no shutdown exit </pre>	<p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
<pre> interface ethernet 1/1 no ip address no shutdown exi </pre>	<p>Se configura interfaz No se le asigna IP Se enciende la interfaz</p>
<pre> interface ethernet 1/1.1 encapsulation dot1Q 13 </pre>	<p>Se configura subinterfaz Se asigna encapsulamiento</p>

<pre>vrf forwarding Special-Users ip address 10.0.23.1 255.255.255.0 ipv6 address fe80::2:3 link-local ipv6 address 2001:db8:acad:23::2/64 no shutdown exit interface ethernet 1/1.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.23.1 255.255.255.0 ipv6 address fe80::2:4 link-local ipv6 address 2001:db8:acad:23::2/64 no shutdown exit</pre>	<p>Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p> <p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
--	--

Fuente: elaboración propia.

Tabla 8 Script Configuración Interfaces Router 3

Configuración Interfaces R3	Descripción
<pre>interface ethernet 1/0 no ip address no shutdown interface ethernet 1/0.1 encapsulation dot1Q 13 vrf forwarding Special-Users ip address 10.0.23.9 255.255.255.0 ipv6 address fe80::3:1 link-local ipv6 address 2001:db8:acad:23::3/64 no shutdown exit interface ethernet 1/0.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.23.9 255.255.255.0 ipv6 address fe80::3:2 link-local ipv6 address 2001:db8:acad:23::3/64 no shutdown exit</pre>	<p>Se configura interfaz No se le asigna IP Se enciende la interfaz</p> <p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p> <p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
<pre>interface ethernet 1/1 no ip address no shutdown</pre>	<p>Se configura interfaz No se le asigna IP Se enciende la interfaz</p>

<pre>interface ethernet 1/1.1 encapsulation dot1Q 13 vrf forwarding Special-Users ip address 10.0.213.9 255.255.255.0 ipv6 address fe80::3:3 link-local ipv6 address 2001:db8:acad:213::1/64 no shutdown exit</pre>	<p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>
<pre>interface ethernet 1/1.2 encapsulation dot1Q 8 vrf forwarding General-Users ip address 10.0.208.9 255.255.255.0 ipv6 address fe80::3:4 link-local ipv6 address 2001:db8:acad:208::1/64 no shutdown exit</pre>	<p>Se configura subinterfaz Se asigna encapsulamiento Se le asocia el vrf creado Se asigna dirección Ipv4 Permite comunicación entre equipos Se asigna dirección Ipv6 Se activa la subinterfaz</p>

Fuente: elaboración propia.

Después de configurar cada uno de los Routers, se valida con el *comando show running-config*. Para observar que la configuración haya quedado correctamente.

Figura 16. Configuración Interfaces Router 1

```

R1
interface Ethernet1/0
no ip address
duplex full

interface Ethernet1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.12.5 255.255.255.0
ipv6 address FE80::1:1 link-local
ipv6 address 2001:DB8:ACAD:12::1/64

interface Ethernet1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.12.5 255.255.255.0
ipv6 address FE80::1:2 link-local
ipv6 address 2001:DB8:ACAD:12::1/64

interface Ethernet1/1
no ip address
duplex full

interface Ethernet1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.113.5 255.255.255.0
ipv6 address FE80::1:3 link-local
ipv6 address 2001:DB8:ACAD:113::1/64

interface Ethernet1/1.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.108.5 255.255.255.0
ipv6 address FE80::1:4 link-local
ipv6 address 2001:DB8:ACAD:108::1/64

```

Fuente: elaboración propia.

Figura 17. Configuración Interfaces R2

```
interface Ethernet1/0
  no ip address
  duplex full
!
interface Ethernet1/0.1
  encapsulation dot1Q 13
  vrf forwarding Special-Users
  ip address 10.0.12.1 255.255.255.0
  ipv6 address FE80::2:1 link-local
  ipv6 address 2001:DB8:ACAD:12::2/64
!
interface Ethernet1/0.2
  encapsulation dot1Q 8
  vrf forwarding General-Users
  ip address 10.0.12.1 255.255.255.0
  ipv6 address FE80::2:2 link-local
  ipv6 address 2001:DB8:ACAD:12::2/64
!
interface Ethernet1/1
  no ip address
  duplex full
!
interface Ethernet1/1.1
  encapsulation dot1Q 13
  vrf forwarding Special-Users
  ip address 10.0.23.1 255.255.255.0
  ipv6 address FE80::2:3 link-local
  ipv6 address 2001:DB8:ACAD:23::2/64
!
interface Ethernet1/1.2
  encapsulation dot1Q 8
  vrf forwarding General-Users
  ip address 10.0.23.1 255.255.255.0
  ipv6 address FE80::2:4 link-local
  ipv6 address 2001:DB8:ACAD:23::2/64
!
```

Fuente: elaboración propia.

Figura 18. Configuración Interfaces R3

```
interface Ethernet1/0
no ip address
duplex full
!
interface Ethernet1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.23.9 255.255.255.0
ipv6 address FE80::3:1 link-local
ipv6 address 2001:DB8:ACAD:23::3/64
!
interface Ethernet1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.23.9 255.255.255.0
ipv6 address FE80::3:2 link-local
ipv6 address 2001:DB8:ACAD:23::3/64
!
interface Ethernet1/1
no ip address
duplex full
!
interface Ethernet1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.213.9 255.255.255.0
ipv6 address FE80::3:3 link-local
ipv6 address 2001:DB8:ACAD:213::1/64
!
interface Ethernet1/1.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.208.9 255.255.255.0
ipv6 address FE80::3:4 link-local
ipv6 address 2001:DB8:ACAD:208::1/64
!
```

Fuente: elaboración propia.

1.6. Configurar rutas estáticas que apuntan a R2

En este paso se requiere configurar en cada equipo de capa 3, el enrutamiento necesario para que exista comunicación de las interfaces correspondientes a cada VRF, es decir que, el objetivo es que las interfaces que pertenezcan al *vrf Special-Users* se comuniquen únicamente entre ellas, y de igual manera con las interfaces que pertenezcan a *vrf General-Users*.

Tabla 9. Script Enrutamiento Router 1

Rutas Estáticas R1	descripción
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.1	Ruta estática ipv4 para vrf Special
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.1	Ruta estática ipv4 para vrf General
ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2	Ruta estática ipv6 para vrf Special
ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2	Ruta estática ipv6 para vrf General
end	

Fuente: elaboración propia.

Tabla 10. Script Enrutamiento Router 2

Rutas Estáticas R2	descripción
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.5	Ruta estática ipv4 para vrf Special
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.9	
ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1	Ruta estática ipv6 para vrf Special
ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3	
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.5	Ruta estática ipv4 para vrf General

<pre> ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.9 ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1 ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3 end </pre>	Ruta estática ipv6 para vrf General
---	-------------------------------------

Fuente: elaboración propia.

Tabla 11. Script Enrutamiento Router 3

Rutas Estáticas R3	descripción
<pre> ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.1 </pre>	Ruta estática ipv4 para vrf Special
<pre> ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.1 </pre>	Ruta estática ipv4 para vrf General
<pre> ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2 </pre>	Ruta estática ipv6 para vrf General
<pre> ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2 end </pre>	Ruta estática ipv6 para vrf General

Fuente: elaboración propia.

Mediante el comando *show run | inc route* se valida en cada Router que la configuración de los Scripts para el enrutamiento haya quedado realizada de manera correcta.

Figura 19. Configuración Rutas Estáticas R1

```
R1#  
R1#  
R1#show run | inc route  
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.1  
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.1  
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2  
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2  
R1#
```

Fuente: elaboración propia.

Figura 20. Configuración Rutas Estáticas R2

```
R2#  
R2#show run | inc route  
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.5  
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.9  
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.5  
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.9  
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#
```

Fuente: elaboración propia.

Figura 21. Configuración Rutas Estáticas R3

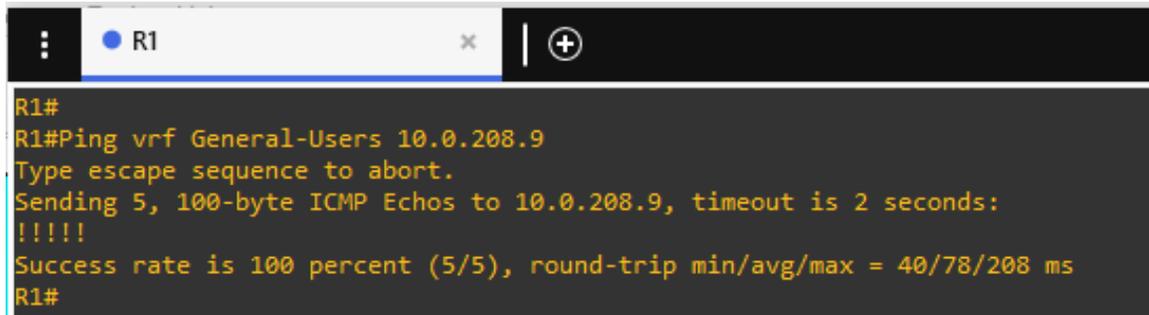
```
R3#  
R3#show run | inc route  
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.1  
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.1  
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:23::2  
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:23::2  
R3#
```

Fuente: elaboración propia.

1.7. Verificar la conectividad en cada VRF

Una vez configurado en enrutamiento entre cada vrf, se procede a validar si la comunicación entre interfaces se ejecuta con normalidad, para esto desde el Router 1 se digita el *Script Ping vrf General-Users* y *Ping vrf Special-Users* seguido de la dirección *IPV4 e IPV6* de cada *Gateway* según el caso.

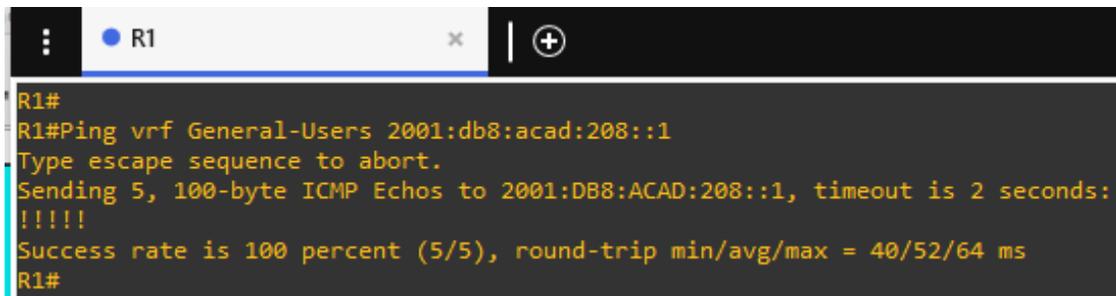
Figura 22. Ping vrf General-Users 10.0.208.9



```
R1#
R1#Ping vrf General-Users 10.0.208.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.9, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/78/208 ms
R1#
```

Fuente: elaboración propia.

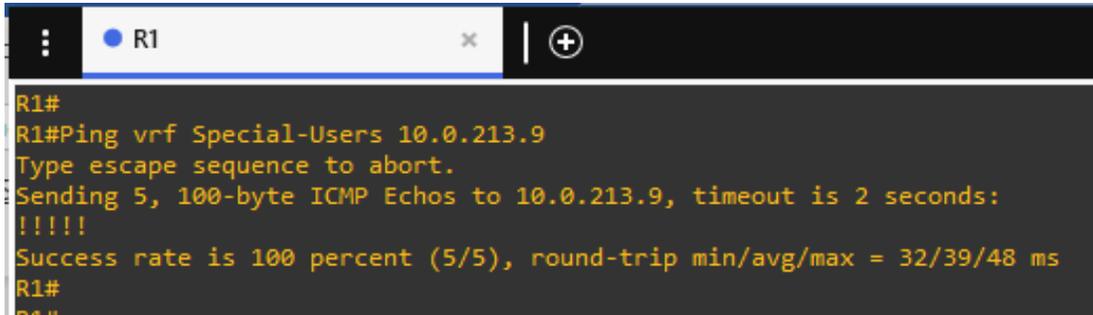
Figura 23. Ping vrf General-Users 2001:db8:acad:208::1



```
R1#
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 = 40/52/64 ms
R1#
```

Fuente: elaboración propia.

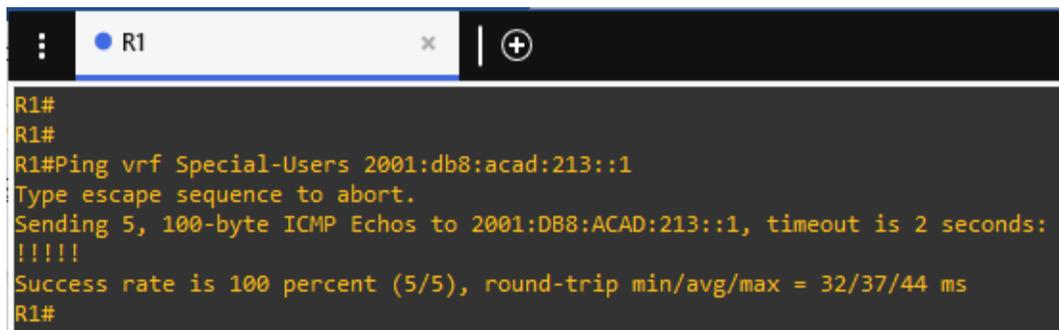
Figura 24. Ping vrf Special-Users 10.0.213.9



```
R1#  
R1#Ping vrf Special-Users 10.0.213.9  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.213.9, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/39/48 ms  
R1#
```

Fuente: elaboración propia.

Figura 25. Ping vrf Special-Users 2001:db8:acad:213::1



```
R1#  
R1#  
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 = 32/37/44 ms  
R1#
```

Fuente: elaboración propia.

2. SEGUNDO ESCENARIO

Luego de haber realizado la configuración del escenario 1, en la cual se obtuvo comunicación entre las sub-interfaces de los equipos de capa 3. Se requiere dar continuidad al trabajo y en esta ocasión se deben configurar los equipos de capa 2.

Una vez concluida la configuración de estos equipos, se continúa con la creación de usuarios y cifrados de contraseñas para acceder a los equipos que se encuentran dentro de la red, y finalmente se debe garantizar comunicación entre los equipos finales dependiendo de la Vlan a la que se encuentren asociados.

2.1. Desactivar todas las interfaces En D1, D2, y A1

Uno de los aspectos más importantes que se deben tener en cuenta al momento de interactuar con redes de comunicaciones en equipos de capa 2, es mitigar el tema de ataques a la red, por tal motivo siempre que se configuren cualquier tipo de Switches es necesario apagar las interfaces que no se encuentren conectadas a nada, y dejar únicamente encendidas las que si se encuentren ocupadas.

Lo anterior es la razón por la cual, en este escenario de práctica se debe efectuar una configuración para apagar las interfaces que se encuentren libres.

Tabla 12. Script para desactivar Interfaces Switch

Configuración Switch D1	Descripción
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 shutdown exit	Se establece rango de interfaces Se apaga la interfaz
Configuración Switch D2	Descripción
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 shutdown exit	Se establece rango de interfaces Se apaga la interfaz
Configuración Switch A1	Descripción
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 shutdown exit	Se establece rango de interfaces Se apaga la interfaz

Fuente: elaboración propia.

2.2. Configurar el enlace troncal hacia R1 y R3

Se debe configurar un enlace troncal en las sub-interfaces que conectan el Switch D1 hacia el Router 1, y el Switch D2 hacia el Router 3. Y esto se debe a que dentro de los Routers se configuran sub-interfaces y en los Switch se crean 2 Vlans. Entonces, el enlace troncal va a servir para que el trafico de cada una de las Vlans pueda transportarse por medio de la misma interfaz física, y el Router pueda conmutar paquetes. A este tipo de practica también se le denomina *Routing Inter- Vlan*.

Tabla 13. Script Configuración Enlace Troncal

Configuración Switch D1	Descripción
interface e0/2 switchport trunk encapsulation dot1q switchport mode trunk no shutdown exit	Se configura interfaz Se asigna encapsulación 802.1Q Se configura como modo troncal Se enciende interfaz
Configuración Switch D2	Descripción
interface e0/3 switchport trunk encapsulation dot1q switchport mode trunk no shutdown exit	Se configura interfaz Se asigna encapsulación 802.1Q Se configura como modo troncal Se enciende interfaz

Fuente: elaboración propia.

Una vez apagadas las interfaces de los Switch que no se encuentran ocupadas y la creación de los enlaces troncales, se procede a verificar el estado de las interfaces mediante el comando *show interfaces status*. Este comando muestra en cada Switch cuantos puertos están activos, cuantos, apagados, y de ellos cuáles están en modo troncal.

Figura 26. Estado de las Interfaces Switch D1

```
D1#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	trunk	auto	auto	unknown
Et0/1		connected	trunk	auto	auto	unknown
Et0/2		connected	trunk	auto	auto	unknown
Et0/3		connected	13	auto	auto	unknown
Et1/0		disabled	1	auto	auto	unknown
Et1/1		disabled	1	auto	auto	unknown
Et1/2		disabled	1	auto	auto	unknown
Et1/3		disabled	1	auto	auto	unknown
Et2/0		disabled	1	auto	auto	unknown
Et2/1		disabled	1	auto	auto	unknown
Et2/2		disabled	1	auto	auto	unknown
Et2/3		disabled	1	auto	auto	unknown
Et3/0		disabled	1	auto	auto	unknown
Et3/1		disabled	1	auto	auto	unknown
Et3/2		disabled	1	auto	auto	unknown
Et3/3		disabled	1	auto	auto	unknown
Po1		connected	trunk	auto	auto	

```
D1#
```

Fuente: elaboración propia.

Figura 27. Estado de las Interfaces Switch D2

```
D2#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		disabled	1	auto	auto	unknown
Et0/1		connected	8	auto	auto	unknown
Et0/2		connected	13	auto	auto	unknown
Et0/3		connected	trunk	auto	auto	unknown
Et1/0		disabled	1	auto	auto	unknown
Et1/1		disabled	1	auto	auto	unknown
Et1/2		disabled	1	auto	auto	unknown
Et1/3		disabled	1	auto	auto	unknown
Et2/0		disabled	1	auto	auto	unknown
Et2/1		disabled	1	auto	auto	unknown
Et2/2		disabled	1	auto	auto	unknown
Et2/3		disabled	1	auto	auto	unknown
Et3/0		disabled	1	auto	auto	unknown
Et3/1		disabled	1	auto	auto	unknown
Et3/2		disabled	1	auto	auto	unknown
Et3/3		disabled	1	auto	auto	unknown

```
D2#
```

Fuente: elaboración propia.

Figura 28. Estado de las Interfaces Switch A1

```

A1#show interfaces status

Port      Name          Status      Vlan      Duplex  Speed  Type
Et0/0     Et0/0         connected   trunk     auto    auto   unknown
Et0/1     Et0/1         connected   trunk     auto    auto   unknown
Et0/2     Et0/2         connected   8         auto    auto   unknown
Et0/3     Et0/3         disabled    1         auto    auto   unknown
Et1/0     Et1/0         disabled    1         auto    auto   unknown
Et1/1     Et1/1         disabled    1         auto    auto   unknown
Et1/2     Et1/2         disabled    1         auto    auto   unknown
Et1/3     Et1/3         disabled    1         auto    auto   unknown
Et2/0     Et2/0         disabled    1         auto    auto   unknown
Et2/1     Et2/1         disabled    1         auto    auto   unknown
Et2/2     Et2/2         disabled    1         auto    auto   unknown
Et2/3     Et2/3         disabled    1         auto    auto   unknown
Et3/0     Et3/0         disabled    1         auto    auto   unknown
Et3/1     Et3/1         disabled    1         auto    auto   unknown
Et3/2     Et3/2         disabled    1         auto    auto   unknown
Et3/3     Et3/3         disabled    1         auto    auto   unknown
Po1       Po1           connected   trunk     auto    auto
A1#
A1#

```

Fuente: elaboración propia.

2.3. Configurar EtherChannel en D1 y A1

Entre los Switch D1 y Switch A1 se encuentran cableadas 2 interfaces, a las cuales se les debe configurar la tecnología de Cisco denominada EtherChannel, y eso se realiza con el fin de agrupar esas 2 interfaces físicas en 1 única interfaz lógica para generar un único enlace con mejores velocidades.

En la tabla 14, se contempla el Script requerido para configurar en cada uno de los Switches el EtherChannel.

Tabla 14. Script Configuración EtherChannel

Configuración Switch D1	Descripción
interface range e0/0, e0/1 switchport trunk encapsulation dot1q switchport mode trunk channel-group 1 mode desirable no shutdown exit	Se configuran interfaces Se asigna encapsulación 802.1Q Se configura como modo troncal Activa las interfaces como negociadora Activación de la interfaz
Configuración Switch A1	Descripción
interface range e0/0, e0/1 switchport trunk encapsulation dot1q	Se configuran interfaces Se asigna encapsulación 802.1Q

<pre>switchport mode trunk channel-group 1 mode desirable no shutdown exit</pre>	<p>Se configura como modo troncal Activa las interfaces como negociadora Activación de la interfaz</p>
--	--

Fuente: elaboración propia.

Para verificar la correcta configuración de EtherChannel, se utiliza el comando *show etherchannel port-channel* en el Switch D1 y A1

Figura 29. Configuración EtherChannel Switch D1

```
D1#
D1#
D1#show etherchannel port-channel
Channel-group listing:
-----

Group: 1
-----

Port-channels in the group:
-----

Port-channel: Po1
-----

Age of the Port-channel    = 0d:00h:59m:07s
Logical slot/port         = 16/0           Number of ports = 2
GC                        = 0x00010001     HotStandBy port = null
Port state                 = Port-channel Ag-Inuse
Protocol                   = PAgP
Port security              = Disabled

Ports in the Port-channel:

Index  Load  Port    EC state      No of bits
-----+-----+-----+-----+-----
  0     00    Et0/0   Desirable-S1    0
  0     00    Et0/1   Desirable-S1    0

Time since last port bundled:  0d:00h:59m:02s  Et0/0
```

Fuente: elaboración propia.

Figura 30. Configuración EtherChannel Switch D1

```

A1#show etherchannel port-channel
Channel-group listing:
-----
Group: 1
-----
Port-channels in the group:
-----
Port-channel: Po1
-----
Age of the Port-channel   = 0d:01h:00m:18s
Logical slot/port        = 16/0           Number of ports = 2
GC                       = 0x00010001   HotStandBy port = null
Port state               = Port-channel Ag-Inuse
Protocol                 = PAgP
Port security            = Disabled

Ports in the Port-channel:

Index  Load  Port    EC state      No of bits
-----+-----+-----+-----+-----
  0     00    Et0/0   Desirable-S1    0
  0     00    Et0/1   Desirable-S1    0

Time since last port bundled:  0d:01h:00m:13s  Et0/0

```

Fuente: elaboración propia.

2.4. Configure los puertos de acceso para los computadores en D1, D2 y A1

En el Escenario 1, se realizó la creación de las *Vlans* en cada uno de los Switches, pero ahora es necesario asignar a cada puerto a los que se encuentra conectado cada dispositivo final, el número de la *Vlan* que corresponda según la topología construida. Esto se debe hacer para lograr la comunicación entre los computadores y que solo los equipos finales que pertenezcan a la *vlan* 8 se comuniquen entre sí, y de igual forma con los que hagan parte de la *vlan* 13. En la tabla 15 se contemplan los Scripts utilizados para las configuraciones.

Tabla 15. Script Asignación Vlan a Puertos

Configuración Switch D1	Descripción
interface e0/3 switchport mode access switchport access vlan 13 spanning-tree portfast no shutdown exit	Se configura la interfaz Establece la interfaz en modo acceso Asigna el puerto a la <i>vlan</i> Activa la protección BPDU Se enciende la interfaz
Configuración Switch D2	Descripción
interface e0/2 switchport mode access	Se configura la interfaz Establece la interfaz en modo acceso

<pre>switchport access vlan 13 spanning-tree portfast no shutdown exit interface e0/1 switchport mode access switchport access vlan 8 spanning-tree portfast no shutdown exit</pre>	<p>Asigna el puerto a la vlan Activa la protección BPDU Se enciende la interfaz</p> <p>Se configura la interfaz Establece la interfaz en modo acceso Asigna el puerto a la vlan Activa la protección BPDU Se enciende la interfaz</p>
Configuración Switch A1	Descripción
<pre>interface e0/2 switchport mode access switchport access vlan 8 spanning-tree portfast no shutdown exit</pre>	<p>Se configura la interfaz Establece la interfaz en modo acceso Asigna el puerto a la vlan Activa la protección BPDU Se enciende la interfaz</p>

Fuente: elaboración propia.

Para verificar en cada uno de los Switches la correcta configuración, se emplea el comando *show Vlan*. En el cual se muestra cuales puertos se encuentran asociados a cada Vlan, y cuales puertos pertenecen por defecto a la *VLAN1* la cual es propia de los equipos Cisco por naturaleza.

Figura 31. Vlans Asociadas a Puertos Switch D1

```
D1#SHoW VL
D1#SHoW VLan

VLAN Name                Status    Ports
-----
1    default                 active    Et1/0, Et1/1, Et1/2, Et1/3
                    Et2/0, Et2/1, Et2/2, Et2/3
                    Et3/0, Et3/1, Et3/2, Et3/3
8    General-Users           active
13   Special-Users           active    Et0/3
1002 fddi-default           act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

Fuente: elaboración propia.

Figura 32. Vlans Asociadas a Puertos Switch D2

```
D2#show vl
D2#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Et0/0, Et1/0, Et1/1, Et1/2
                    Et1/3, Et2/0, Et2/1, Et2/2
                    Et2/3, Et3/0, Et3/1, Et3/2
                    Et3/3
8    General-Users          active    Et0/1
13   Special-Users          active    Et0/2
1002 fddi-default          act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

Fuente: elaboración propia.

Figura 33. Vlans Asociadas a Puertos Switch A1

```
A1#show vlan

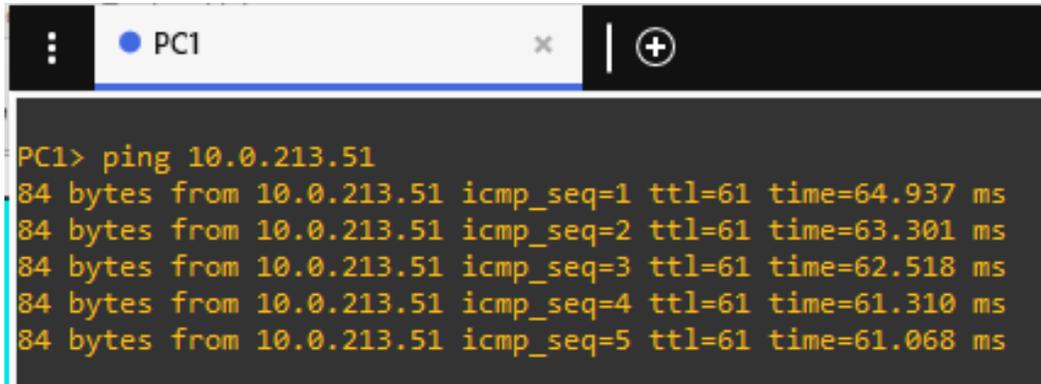
VLAN Name                Status    Ports
-----
1    default                active    Et0/3, Et1/0, Et1/1, Et1/2
                    Et1/3, Et2/0, Et2/1, Et2/2
                    Et2/3, Et3/0, Et3/1, Et3/2
                    Et3/3
8    General-Users          active    Et0/2
1002 fddi-default          act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

Fuente: elaboración propia.

2.5. Verificar la conectividad de PC a PC

Para corroborar que toda la configuración del Escenario 1 y del Escenario 2 fue efectiva, se debe validar si existe comunicación entre los dispositivos finales, para lo cual desde los computadores se ejecuta el comando *Ping* seguido de la dirección *IPV4* e *IPV6* del computador de destino al cual se le desee verificar la comunicación.

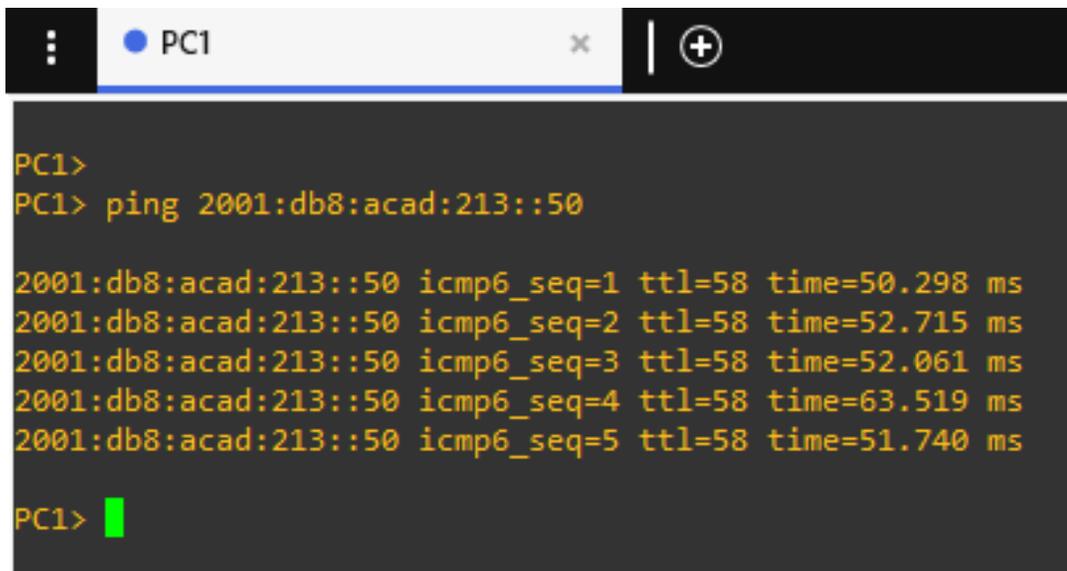
Figura 34. Ping IPV4 PC1 a PC2



```
PC1> ping 10.0.213.51
84 bytes from 10.0.213.51 icmp_seq=1 ttl=61 time=64.937 ms
84 bytes from 10.0.213.51 icmp_seq=2 ttl=61 time=63.301 ms
84 bytes from 10.0.213.51 icmp_seq=3 ttl=61 time=62.518 ms
84 bytes from 10.0.213.51 icmp_seq=4 ttl=61 time=61.310 ms
84 bytes from 10.0.213.51 icmp_seq=5 ttl=61 time=61.068 ms
```

Fuente: elaboración propia.

Figura 35. Ping IPV6 PC1 a PC2



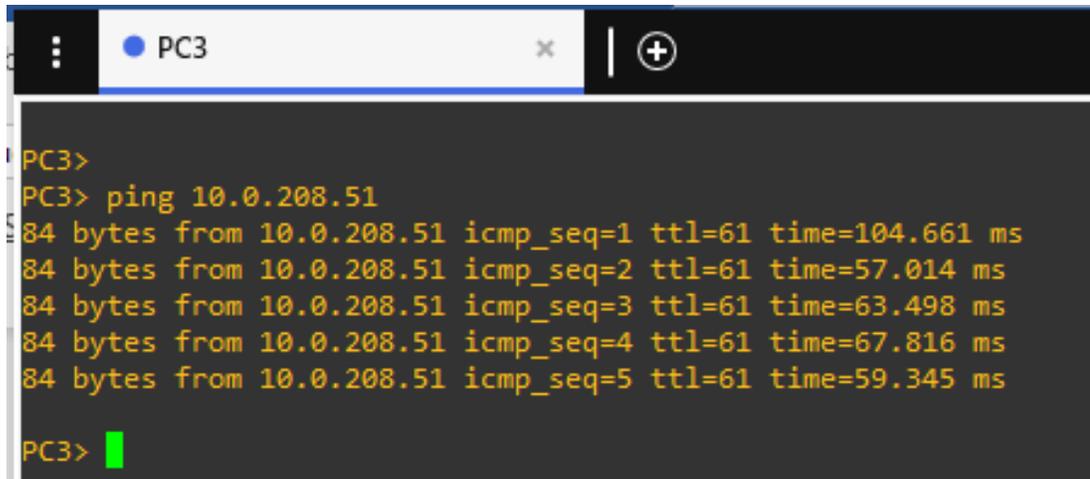
```
PC1>
PC1> ping 2001:db8:acad:213::50

2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=50.298 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=52.715 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=52.061 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=63.519 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=51.740 ms

PC1> █
```

Fuente: elaboración propia.

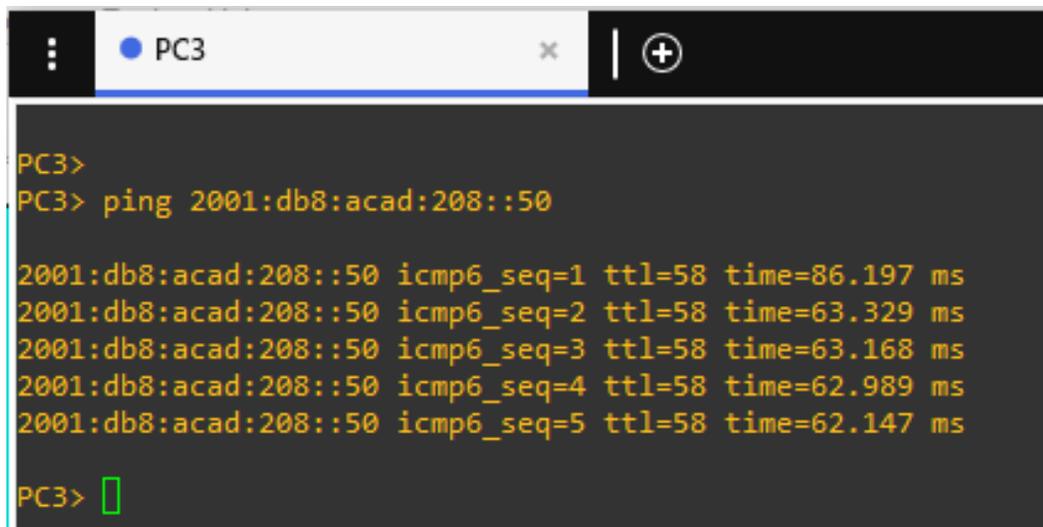
Figura 36. Ping IPV4 PC3 a PC4



```
PC3>
PC3> ping 10.0.208.51
84 bytes from 10.0.208.51 icmp_seq=1 ttl=61 time=104.661 ms
84 bytes from 10.0.208.51 icmp_seq=2 ttl=61 time=57.014 ms
84 bytes from 10.0.208.51 icmp_seq=3 ttl=61 time=63.498 ms
84 bytes from 10.0.208.51 icmp_seq=4 ttl=61 time=67.816 ms
84 bytes from 10.0.208.51 icmp_seq=5 ttl=61 time=59.345 ms
PC3>
```

Fuente: elaboración propia.

Figura 37. Ping IPV4 PC3 a PC4



```
PC3>
PC3> ping 2001:db8:acad:208::50
2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=86.197 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=63.329 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=63.168 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=62.989 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=62.147 ms
PC3>
```

Fuente: elaboración propia.

Finalmente, se procede a configurar los temas de seguridad y acceso a los dispositivos

2.6. Modo privilegiado en todos los dispositivos

Todos los Routers y Switches en un entorno real, deben tener una configuración especial, para que cuando alguna persona quiera acceder a configurar estos dispositivos, el sistema operativo de cada uno de ellos le solicite al usuario alguna clave. De esta forma se logran mitigar ataques a los equipos capa 3 y capa 2. Generalmente, el administrador

de equipos cisco mediante las configuraciones contempladas en la tabla 16, puede establecer la clave que los equipos van a solicitar cuando alguien quiera acceder al modo privilegiado a efectuar determinada configuración.

El Script para los Routers es distinto al de los Switches, pero esto se debe a que las imágenes cargadas en el emulador GNS3 para los Routers, no están diseñadas para aceptar el comando *algorithm-type SCRYPT*

Tabla 16. Script Configuración Modo Privilegiado

Configuración Router 1	Descripcion
enable secret juan519	Crea la contraseña juan519
Configuración Router 2	Descripcion
enable secret juan519	Crea la contraseña juan519
Configuración Router 3	Descripcion
enable secret juan519	Crea la contraseña juan519
Configuración Switch D1	Descripcion
enable algorithm-type SCRYPT secret juan519	Crea la contraseña juan519 y habilita el algoritmo de tipo SCRYPT
Configuración Switch D2	Descripcion
enable algorithm-type SCRYPT secret juan519	Crea la contraseña juan519 y habilita el algoritmo de tipo SCRYPT
Configuración Switch A1	Descripcion
enable algorithm-type SCRYPT secret juan519	Crea la contraseña juan519 y habilita el algoritmo de tipo SCRYPT

Fuente: elaboración propia.

2.7. Cuenta de Usuario local en todos los dispositivos

Se recomienda que los equipos de capa 2 y capa 3 también tengan una configuración especial para que las personas que deseen acceder a ellos, de manera general o global, deban ingresar un usuario y una contraseña

En la tabla 17, se observa el Script utilizado para ejecutar esta configuración.

Tabla 17. Script Configuración Cuentas de Usuario

Configuración Router 1	Descripcion
username admin privilege 15 secret juan519	Configura nombre de usuario y contraseña
Configuración Router 2	Descripcion
username admin privilege 15 secret juan519	Configura nombre de usuario y contraseña
Configuración Router 3	Descripcion
username admin privilege 15 secret juan519	Configura nombre de usuario y contraseña
Configuración Switch D1	Descripcion
username admin privilege 15 algorithm-type SCRYPT secret juan519	Configura nombre de usuario y contraseña
Configuración Switch D2	Descripcion
username admin privilege 15 algorithm-type SCRYPT secret juan519	Configura nombre de usuario y contraseña
Configuración Switch A1	Descripcion
username admin privilege 15 algorithm-type SCRYPT secret juan519	Configura nombre de usuario y contraseña

Fuente: elaboración propia.

2.8. Autenticación AAA en todos los dispositivos

Finalmente, se configura la autenticación AAA en cada uno de los Routers y Switches. El protocolo AAA debe implementarse para garantizar en cada dispositivo la funcionalidad de, autenticación, autorización y responsabilidad.

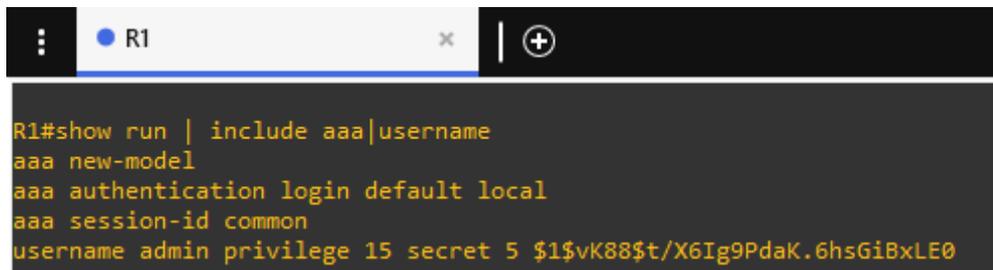
Tabla 18. Script Autenticación AAA

Configuración Router 1	Descripcion
aaa new-model aaa authentication login default local end	Permite el uso de modelos de autenticación AAA y activa el modelo predeterminado
Configuración Router 2	Descripcion
aaa new-model aaa authentication login default local end	Permite el uso de modelos de autenticación AAA y activa el modelo predeterminado
Configuración Router 3	Descripcion
aaa new-model aaa authentication login default local end	Permite el uso de modelos de autenticación AAA y activa el modelo predeterminado
Configuración Switch D1	Descripcion
aaa new-model aaa authentication login default local end	Permite el uso de modelos de autenticación AAA y activa el modelo predeterminado
Configuración Switch D2	Descripcion
aaa new-model aaa authentication login default local end	Permite el uso de modelos de autenticación AAA y activa el modelo predeterminado
Configuración Switch A1	Descripcion
aaa new-model aaa authentication login default local end	Permite el uso de modelos de autenticación AAA y activa el modelo predeterminado

Fuente: elaboración propia.

Una vez configurados los accesos de seguridad para el modo privilegiado, creación de usuarios, contraseñas e implementación de la autenticación AAA. Por medio del comando `show run | include aaa|username`, se puede observar si un dispositivo queda configurado con el protocolo de autenticación, adicionalmente se puede verificar el nombre del usuario para el acceso a cada dispositivo, junto con la clave, pero esta se va a encontrar encriptada.

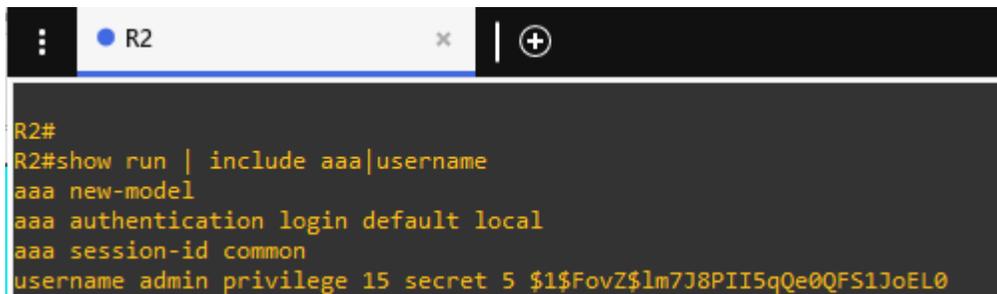
Figura 38. Autenticación AAA Router 1



```
R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$vK88$t/X6Ig9PdaK.6hsGiBxLE0
```

Fuente: elaboración propia.

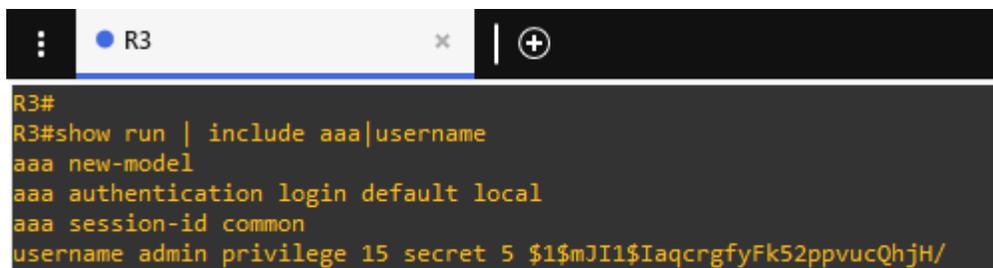
Figura 39. Autenticación AAA Router 2



```
R2#
R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$FovZ$l7J8PII5qQe0QFS1JoEL0
```

Fuente: elaboración propia.

Figura 40. Autenticación AAA Router 3



```
R3#
R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$mJI1$IaqcrgfyFk52ppvucQhjH/
```

Fuente: elaboración propia.

Figura 41. Autenticación AAA Switch D1

```
D1#  
D1#  
D1#show run | include aaa|username  
username admin privilege 15 secret 9 $9$FMkuUUGwf7stLK$1IPwZ/BGsTF4vZF2KbnjQv5bkeNDVEkDDNp2fX8du2k  
aaa new-model  
aaa authentication login default local  
aaa session-id common  
D1#
```

Fuente: elaboración propia.

Figura 42. Autenticación AAA Switch D2

```
D2#  
D2#show run | include aaa|username  
username admin privilege 15 secret 9 $9$at61t1qwwYaXaK$WQ20QQ.p.2yhIDDUPBZ5hLY2K4FCUYIBtVhYIXHtLbE  
aaa new-model  
aaa authentication login default local  
aaa session-id common  
D2#
```

Fuente: elaboración propia.

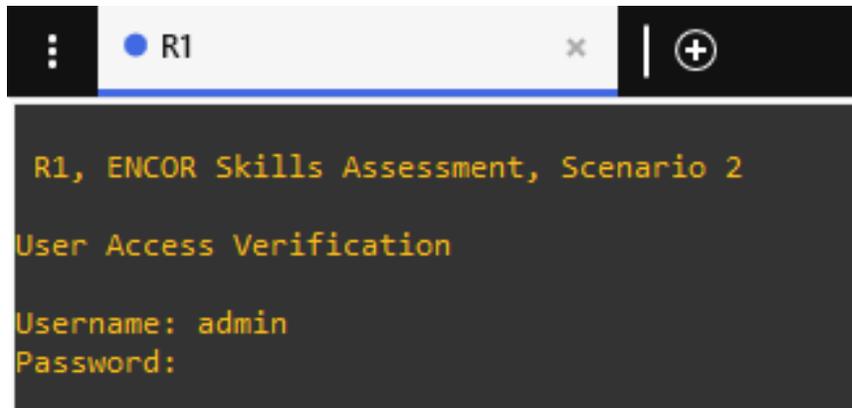
Figura 43. Autenticación AAA Switch A1

```
A1#  
A1#show run | include aaa|username  
username admin privilege 15 secret 9 $9$kWd5SDYiqwXB2q$NrNis96h95C9TU0Fy7YxnBou/rDnZf46T2NZ97u15jk  
aaa new-model  
aaa authentication login default local  
aaa session-id common  
A1#
```

Fuente: elaboración propia.

La última verificación que se deben realizar para concluir con éxito el desarrollo de esta práctica es ingresar a cada Router y Switch, y verificar si los dispositivos solicitan usuario y contraseña para ingresar.

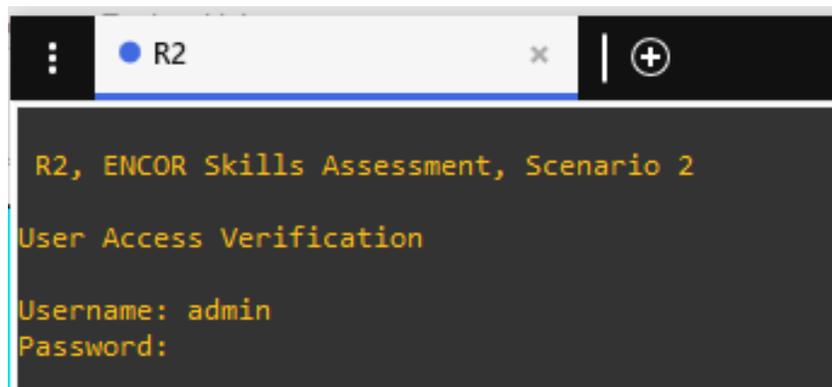
Figura 44. Mensaje de Credenciales Router 1



```
R1, ENCOR Skills Assessment, Scenario 2
User Access Verification
Username: admin
Password:
```

Fuente: elaboración propia.

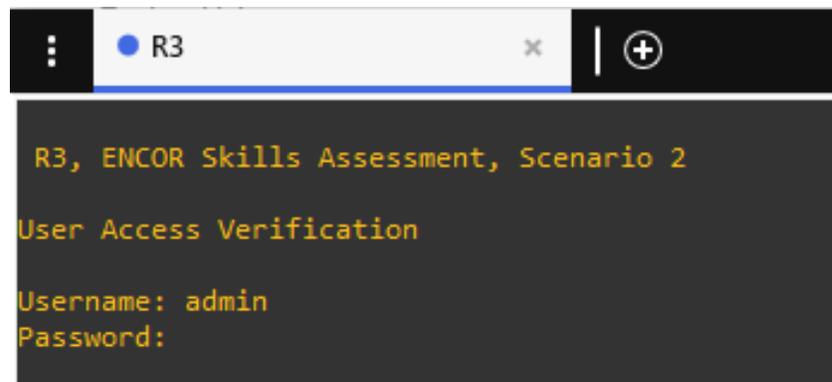
Figura 45. Mensaje de Credenciales Router 2



```
R2, ENCOR Skills Assessment, Scenario 2
User Access Verification
Username: admin
Password:
```

Fuente: elaboración propia.

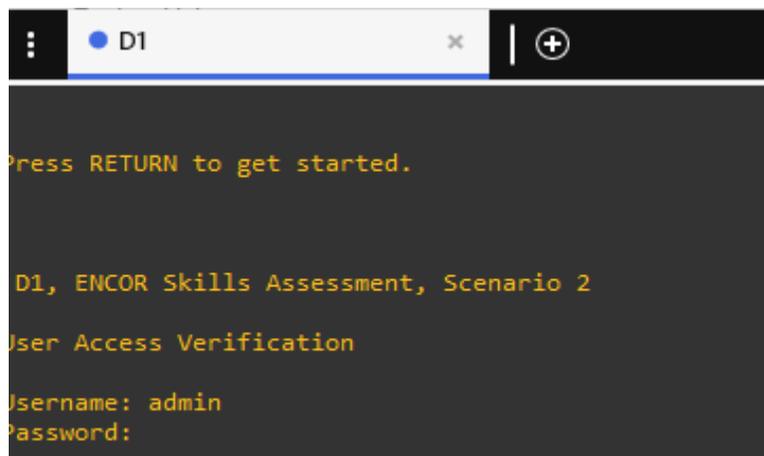
Figura 46. Mensaje de Credenciales Router 3



```
R3, ENCOR Skills Assessment, Scenario 2
User Access Verification
Username: admin
Password:
```

Fuente: elaboración propia.

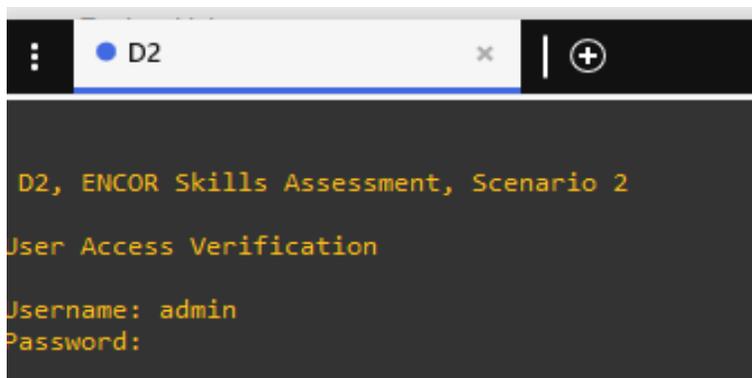
Figura 47. Mensaje de Credenciales Switch D1



```
Press RETURN to get started.  
  
D1, ENCOR Skills Assessment, Scenario 2  
User Access Verification  
Username: admin  
Password:
```

Fuente: elaboración propia.

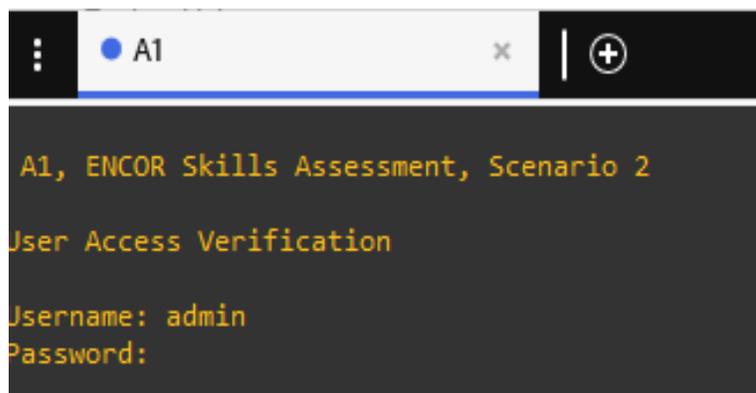
Figura 48. Mensaje de Credenciales Switch D2



```
D2, ENCOR Skills Assessment, Scenario 2  
User Access Verification  
Username: admin  
Password:
```

Fuente: elaboración propia.

Figura 49. Mensaje de Credenciales Switch A1



```
A1, ENCOR Skills Assessment, Scenario 2  
User Access Verification  
Username: admin  
Password:
```

Fuente: elaboración propia.

CONCLUSIONES

Con el desarrollo de la actividad se comprende que existen varias tecnologías avanzadas que los ingenieros de telecomunicaciones y carreras afines, deben manejar para adquirir mejores oportunidades en el campo laboral y de esa forma aportar al crecimiento y conectividad de redes alrededor del mundo, una de tantas tecnologías es VRF, y gracias a la configuración de la topología contemplada en este documento, se aprende que un equipo de capa 3, puede configurarse para contener varios enrutamientos de manera lógica mediante una interfaz física, que internamente contengan dos direcciones ip idénticas.

Después de configurar las subinterfaces de los Routers, se concluye que una interfaz física tiene la capacidad de configurarse para contener dos direcciones ip o dos Gateway. La importancia de configurar subinterfaces radica en que es una de las mejores alternativas para economizar puertos en los equipos y ahorrar cableado cuando una red necesita trabajar mediante distintas Vlans.

Luego de ejecutar las configuraciones en los equipos de capa dos, se logra comprender la importancia de apagar los puertos que no se encuentren conectados a nada, ya que en un entorno de la vida real una red de comunicaciones puede ser vulnerable a ataques si todos los puertos de un switch que no estén cableados se encuentran encendidos. Adicionalmente, se aprende que, al momento de configurar subinterfaces, la interfaz física que se encuentre interconectando el equipo de capa 2 al equipo de capa 3, debe configurarse en modo troncal, para que los Routers puedan leer que se está transmitiendo información convergente por medio de un mismo puerto y que esa información proviene de distintas Vlans, para así lograr enrutar estos paquetes a otros Routers.

Al finalizar las configuraciones de la última parte del segundo escenario, se comprende que en una red de telecomunicaciones el tema de seguridad va más allá de crear un usuario y contraseña para acceder a los equipos. Cuando se habla de una red segura, se debe enfocar en garantizar que la encriptación de las contraseñas sea adecuada, y que la seguridad se encuentre orientada a la autenticación, autorización y contabilización propia de los protocolos AAA para generar eficacia en la ciberseguridad.

BIBLIOGRAFÍA

EDGEWORTH, Bradley, et al. VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

EDGEWORTH, Bradley, et al. Virtual Routing and Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en <https://1drv.ms/b/s!AAIGg5JUqUBthk8>