DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MAYLEBIS CASTELLAR NIZ

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MAYLEBIS CASTELLAR NIZ

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

DIRECTOR:
JUAN ESTEBAN TAPIAS BAENA

Universidad nacional abierta y a distancia - UNAD
Escuela de ciencias básicas, tecnología e ingeniería - ECBTI
Ingeniería Telecomunicaciones
Bogotá – Distrito Capital
2023

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTÁ – DISTRITO CAPITAL, 04 mayo de 2023

AGRADECIMIENTOS

Primero gracias a Dios por ser mi guía y luz en este camino que no ha sido fácil y darme fuerzas en los momentos más vulnerables para poder seguir adelante con mis estudios. A mis padres que siempre han luchado con mucho esfuerzo para poder apoyarme siempre en todas las decisiones de mi vida. A mi esposo quien me motivo, que no era tarde para poder seguir adelante con mis estudios y coloco su granito de arena para poder empezar esta profesión, a mis hijos José Manuel e Isabella que son mi impulso y motivación para poder lograr una estabilidad económica para ellos, para aquellas personas especiales que se fueron antes que terminara mi título, a mi tía Carmenza quien siempre me insistió que terminara mis estudios y me alentaba y mi suegro José Manuel quien se alegró demasiado con solo contarle que me inscribí en esta profesión cada oportunidad me preguntaba en que semestre iba cursando, con su frase bella que “con dos manos nos lavamos la cara” para ser un apoyo en mi hogar. A mis primos que son hermanos de la vida y mis hermanos que con sus palabras que faltaba poco, para que siguiera adelante ellos que son mis mejores amigos y se alegran con mis logros, Gracias a mí que, a pesar del cansancio, de momentos difíciles seguí persistiendo, logrando terminar todas mis materias para estar a un paso de tan anhelado sueño. Para mi virgencita de Siracusa que para ella nada imposible, la fe mueve mi vida y con perseverancia todo se logra.

TABLA DE CONTENIDO

TABLA DE FIGURAS.....**¡Error! Marcador no definido.**

AGRADECIMIENTOS..... 4

GLOSARIO..... 8

RESUMEN..... 9

ABSTRACT..... 10

INTRODUCCIÓN..... 11

DESARROLLO..... 12

1. Escenario 1..... 12

2. Escenario 2..... 24

CONCLUSIONES..... 36

BIBLIOGRAFIAS..... 37

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento. 16
Tabla 3. Configuración Capa 2 24
Tabla 4. Direcciones IPV4 e IPV6 para las estaciones de trabajo 32
Tabla 5. Configurar la seguridad 32

TABLA DE FIGURAS

Figura 1. Topología de la Red 12
Figura 2.Simulación de Escenario en GNS3 13
Figura 3. Configuración IPV4 Y IPV6 - PC1 17
Figura 4. Configuración IPV4 Y IPV6 - PC2 18
Figura 5.Configuración IPV4 Y IPV6 - PC3 18
Figura 6. Configuración IPV4 Y IPV6 - PC4 19
Figura 7. Configuración de vrf en R1 19
Figura 8. Configuración de Vrf en R2. 20
Figura 9. Configuración de Vrf en R3 20
Figura 10. Verificación de rutas estáticas mediante show run en R1. 21
Figura 11. Verificación de rutas estáticas mediante show run en R2. 21
Figura 12. Verificación de rutas estáticas mediante show run en R3. 22
Figura 13. Verificación de conectividad 23
Figura 14. Estado Interfaces D1 y D2 25
Figura 15. Interfaces A1 26
Figura 16. Configuración en D1 y D2 de los enlaces troncales hacia R1 y R3 27
Figura 17. Configuración Ethernetchannel D1 y A1 29
Figura 18. Configuración en D1,D2 and A1 puertos de acceso para PC1, PC2, PC3, y PC4 30
Figura 19. Verificación conectividad IPV4 Y IPV6 31
Figura 20. Verificación usuario, contraseña y sh AAA sesión para D1, D2 y A1 34
Figura 21. Verificación usuario, contraseña y sh AAA sesión para R1, R2 y R3 34

GLOSARIO

Router: dispositivo de red utilizado para conectar diferentes redes y dirigir el tráfico de red.
Switch: dispositivo de red que se utiliza para conectar múltiples dispositivos en una red y enviar datos a través de la red.
VLAN: red de área local virtual, que se utiliza para separar dispositivos en una red.
DHCP: protocolo de configuración dinámica de host, que se utiliza para asignar direcciones IP a dispositivos en una red.
DNS: sistema de nombres de dominio, que se utiliza para resolver nombres de host en direcciones IP.
IP: protocolo de Internet, que se utiliza para enviar y recibir datos a través de la red.
OSPF: protocolo de enrutamiento de estado de enlace abierto, utilizado para enrutar datos a través de una red.
NAT: traducción de dirección de red, que se utiliza para permitir que dispositivos en una red privada se comuniquen con dispositivos en una red pública.
ACL: lista de control de acceso, que se utiliza para controlar el tráfico de red y proteger la red contra ataques maliciosos.
VPN: red privada virtual, que se utiliza para establecer una conexión segura a través de una red pública.
WAN: red de área amplia, que se utiliza para conectar dispositivos en diferentes ubicaciones geográficas.
LAN: red de área local, que se utiliza para conectar dispositivos en un área geográfica limitada.
SNMP: protocolo simple de administración de red, que se utiliza para administrar y supervisar dispositivos de red.
STP: protocolo de árbol de expansión, que se utiliza para evitar bucles de red en una red de switches.
VLAN Trunking: técnica utilizada para transportar múltiples VLAN a través de un único enlace de red físico.
VTP: protocolo de trama de VLAN, que se utiliza para distribuir información de configuración de VLAN en una red.

RESUMEN

El presente trabajo donde profundización en Cisco que busca formar a los estudiantes en el uso avanzado de tecnologías de redes y comunicaciones de la marca Cisco. Este diplomado proporciona a los estudiantes una comprensión más profunda de los conceptos teóricos y prácticos relacionados con el diseño, Conmutación, Enrutamiento, Electrónica, la implementación y el mantenimiento de redes basadas en tecnologías de Cisco.

Los participantes en este diplomado aprenderán a utilizar herramientas de redes y software de Cisco CCNP, como los sistemas operativos IOS y NX-OS, así como a configurar y administrar dispositivos de redes, como router y switches. Además, el programa cubre temas como la seguridad de redes, la gestión de redes y la virtualización de redes.

Este diplomado está dirigido a profesionales de TI, ingenieros de redes, administradores de sistemas y cualquier persona interesada en adquirir habilidades avanzadas en tecnologías de redes de Cisco. Al completar el programa, los graduados tendrán un conocimiento sólido y práctico en el uso de tecnologías de redes y comunicaciones de Cisco para diseñar, implementar y mantener redes empresariales.

Palabras claves: CISCO, CCNP, Conmutación, Enrutamiento, Electrónica

ABSTRACT

The present work where deepening in Cisco that seeks to train students in the advanced use of network and communication technologies of the Cisco brand. This diploma provides students with a deeper understanding of theoretical and practical concepts related to the design, Switching, Routing, Electronics, implementation and maintenance of networks based on Cisco technologies.

Participants in this diploma course will learn to use Cisco CCNP software and networking tools, such as the IOS and NX-OS operating systems, as well as configure and manage network devices, such as routers and switches. Additionally, the program covers topics such as network security, network management, and network virtualization.

This diploma is for IT professionals, network engineers, system administrators, and anyone interested in gaining advanced skills in Cisco networking technologies. Upon completion of the program, graduates will have a solid, practical understanding of using Cisco networking and communications technologies to design, implement, and maintain enterprise networks.

Keywords: CISCO, CCNP, Switching, Routing, Electronics

INTRODUCCIÓN

En la época actual el avance tecnológico en cada aspecto de la sociedad ha sido grande llevándonos a una conocida transformación digital, de la cual hacen parte las redes de datos, las cuales resultan ser fundamentales para las comunicaciones, entre dispositivos. En el presente informe se desarrolla las actividades correspondientes a la evaluación final de habilidades prácticas del Cisco CCNP en el que se plantean un escenario conformado por una topología de red dada. En este se procede a la configuración de subinterfaces VRF y rutas estáticas. Se configuran protocolos de enrutamientos donde explica con detalle cada respectiva línea de comando utilizada en la configuración de los dispositivos correspondientes a la solución.

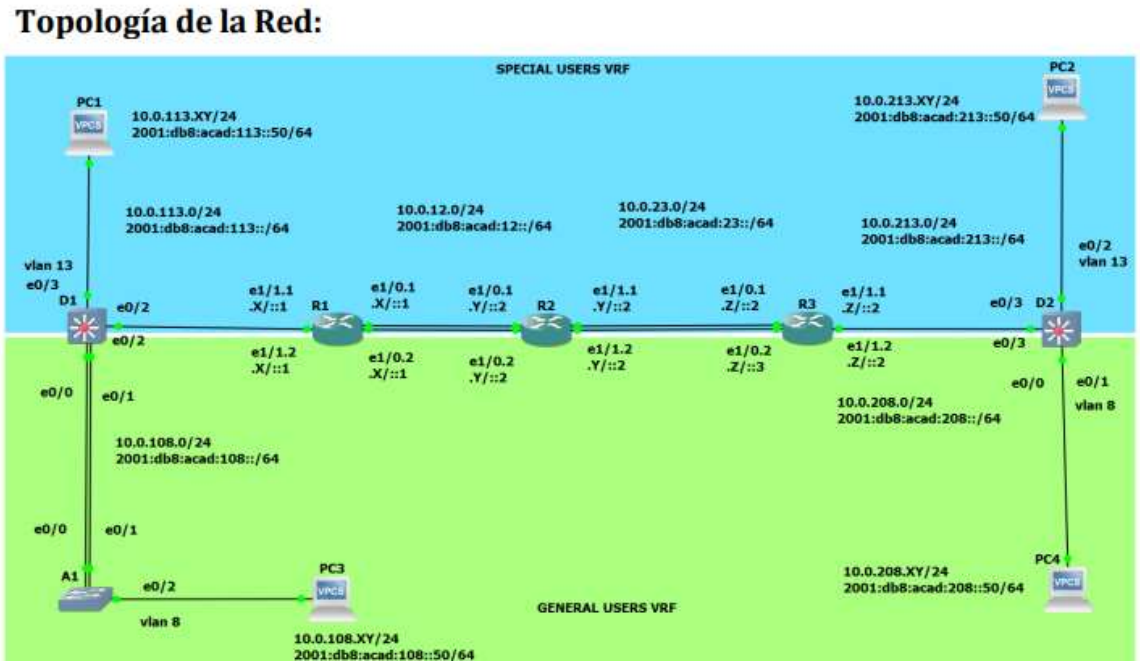
DESARROLLO

1. Escenario 1

Para la elaboración de este de este trabajo se utilizó el software GNS3, para realizar la topología y el desarrollo del escenario teniendo en cuenta las recomendaciones dadas por el tutor, se debe completar la configuración multi-VRFde la red que admite "Usuarios generales" y "Usuarios especiales". Una vez finalizado debería haber accesibilidad completa de un extremo a otro y los dos grupos no deberían poder comunicarse entre sí.

TOPOLOGIA INTERFACES

Figura 1. Topología de la Red



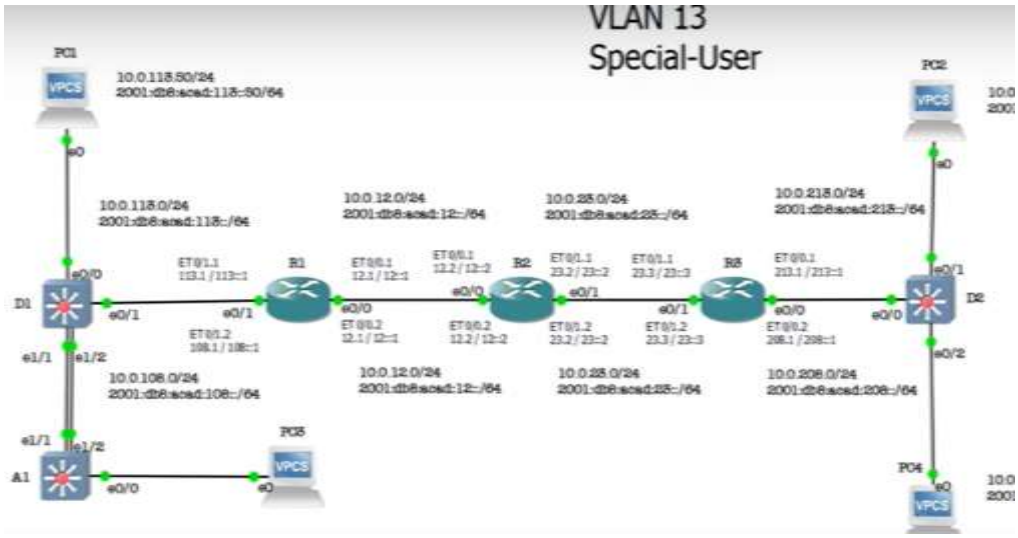
Fuente: Elaboración propia a través de software GNS3

Cablear La Red Como Se Muestra En La Topología.

Para poder realizar la topología que se muestra en la Imagen 1. Fue necesario instalar el programa GNS3 y la máquina virtual VM, de igual manera fue necesario instalar los módems y router necesarios para poder cargar la configuración de la topología, esto se realizó por sugerencia del tutor en la videoconferencia, seguido a esto procedemos a realizar el cableado de todos los componentes que se observan en la imagen 2.

Después de tener todo el cableado de los componentes procedemos a copiar los códigos de configuración de cada uno de los router y switches para iniciar de esta manera con la comprobación de la conectividad.

Figura 2.Simulación de Escenario en GNS3



Fuente: Autoría propia.

Se realiza la configuración multi VRF de la red que admite Usuarios generales y Usuarios especiales. Donde se pueda acceder de un extremo a otro y los dos grupos se puedan comunicar entre si verificando que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funciones según lo requerido.

Se desarrolla en el simulador GNS3 armando la configuración establecida, con el fin de construir el escenario se realiza la distribución de los elementos que realizaran la función, enrutadores, switches y los ultimo los PC que son los empleados en el posteriormente realizamos la conexión que enlaza cada dispositivo permitiendo así que se procesa a la configuración inicial. Para organizar en el escenario GNS3.

Los switches pueden usarse como router al mismo tiempo admite múltiples puertos de Ethernet y con función de conmutación inspeccionando sus direcciones IP que se requieren en el desarrollo de la guía con todas las funciones de conmutación. También Switch de capa 2 es un paquete de datos de un puerto determinado primero realiza la lectura MAC de origen en el paquete luego lee la dirección MAC de destino en el paquete y busca el puerto correspondiente en la tabla de direcciones.

Teniendo la guía de desarrollo se realiza la configuración inicial para cada elemento en el

cual router, switches, Pc y en su conjunto las VLANS se establecen detalladamente comando para cada dispositivo utilizados en cada uno de los elementos que conforman el escenario.

Configurar los ajustes básicos para cada dispositivo

Se Ingresa al modo de configuración global en cada uno de los dispositivos y aplica la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.

Router R1
hostname R1 ¡Se asigna el nombre!
ipv6 unicast-routing ¡Se habilita ipv6 en el router!
no ip domain lookup ¡Desactivamos la búsqueda DNS!
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #
line con 0 ¡Se ingresa a la configuración de la consola!
exec-timeout 0 0 ¡Se establece en 0 el tiempo de inactividad!
logging synchronous ¡Se evita el desplazamiento del comando!
exit

Router R2
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit

Router R3
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
Switch D1
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

Switch D2
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

Switch A1
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

Para guardar las configuraciones de cada dispositivo se finaliza cada configuración con el comando wr.

Configurar Los PC1, PC2, PC3 Y PC4

PC1 ip 10.0.113.50/24, **PC2** Ip 10.0.213.50/24, **PC3** Ip 10.0.108.50/24, **PC4** Ip 10.0.208.50/24

Tabla 1. Tabla de direccionamiento.

Device	Interface	IPv4 Address	IPv6 Address	IPV6 LinkLocal
R1	E1/0.1	10.0.12.5/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.5/24	2001:db8:acad:12::1/64	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	10.0.12.2/24	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	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.2/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.2/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.52/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.52/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.52/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.52/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Elaboración Propia

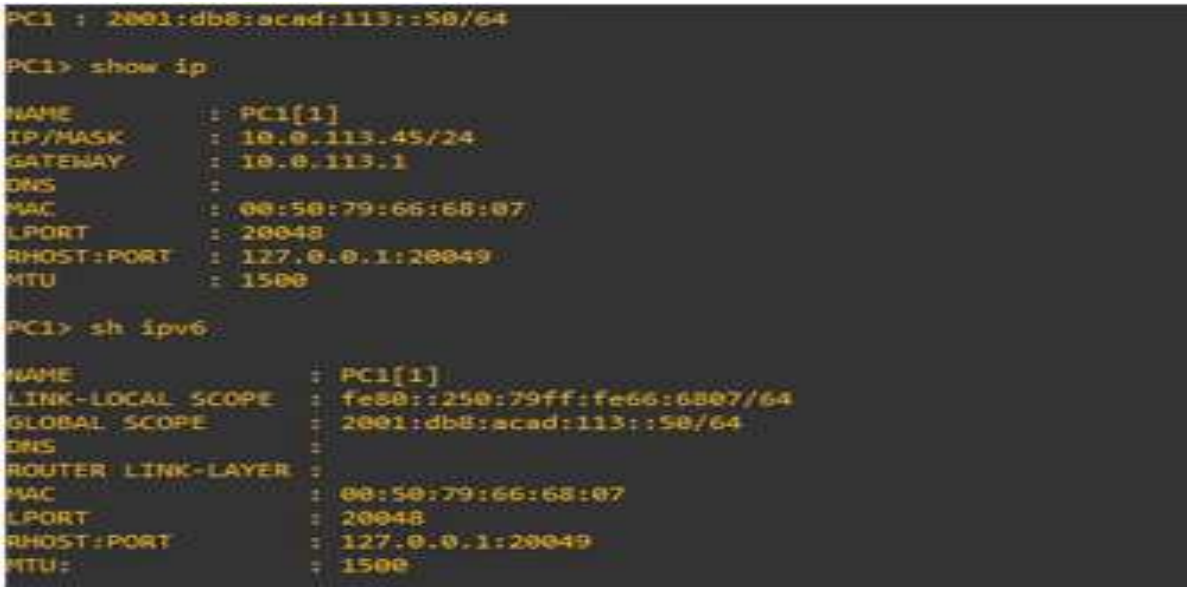
Configuración de ipv4 y ipv6

Se configuran las interfaces ipv4 y ipv6 en R1, R2 y R3 utilizando router-on-A-stick para poder admitir la separación de los vrfs.

Mirar en las siguientes imágenes la creación de cada vrf con sus interfaces y las rutas estáticas que se utilizaron.

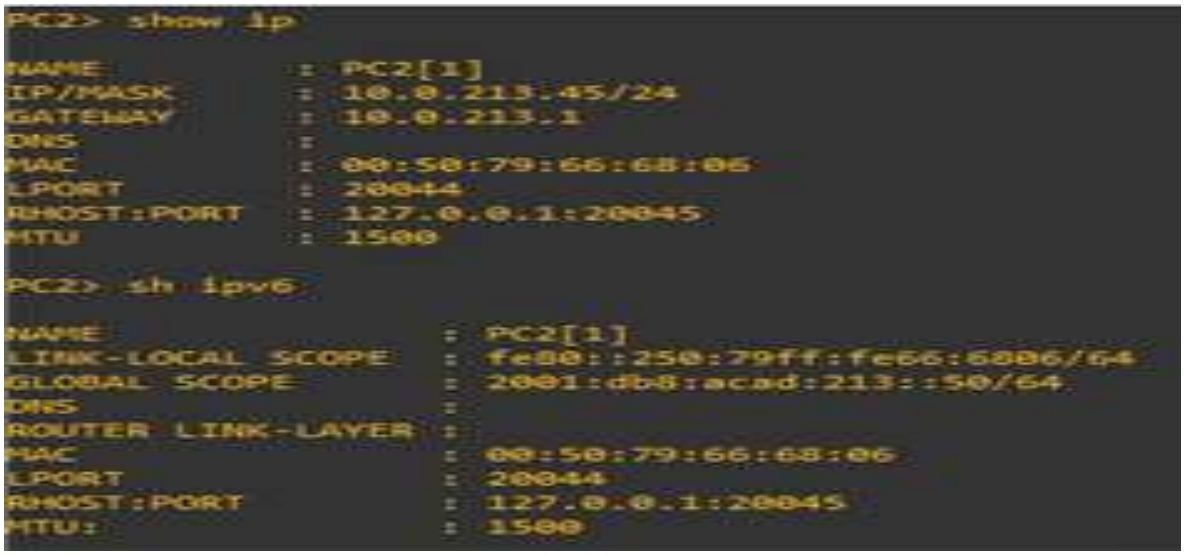
En esta parte se puede evidenciar mediante el comando show run en cadauno de los router las rutas estáticas que se configuraron en R1, R2 y R3.

Figura 3. Configuración IPV4 Y IPV6 - PC1



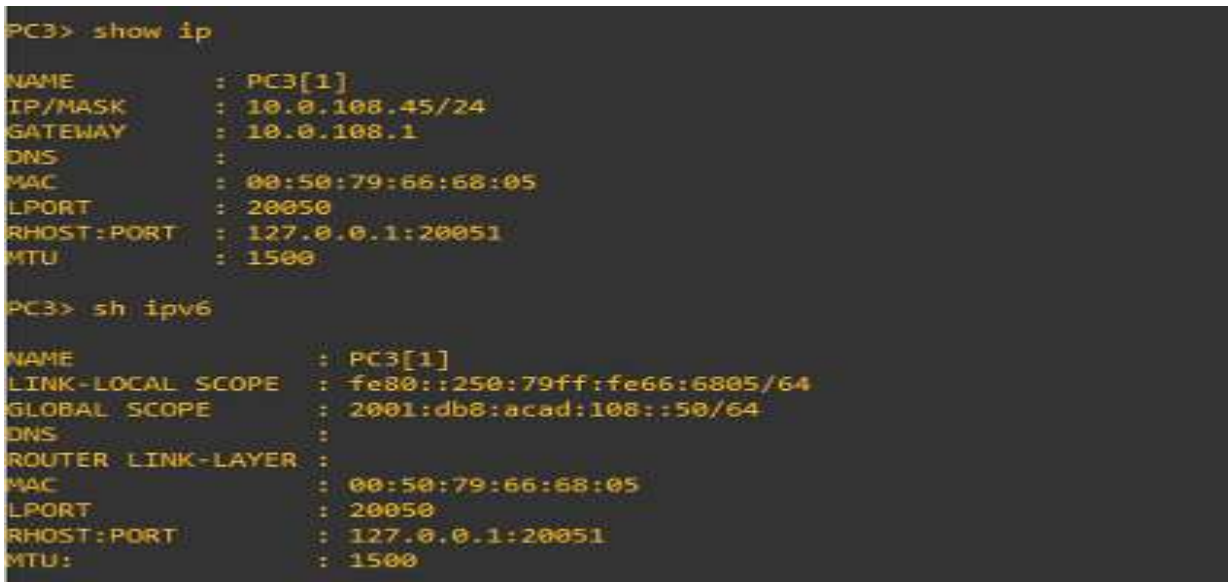
Fuente. elaboración propia

Figura 4. Configuración IPV4 Y IPV6 - PC2



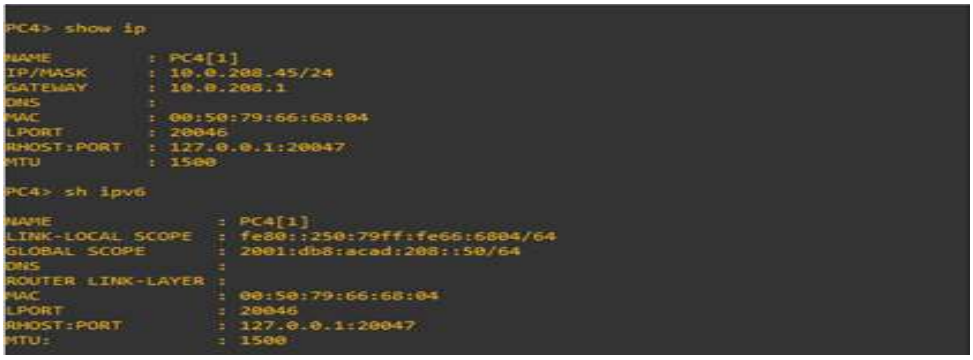
Fuente. elaboración propia

Figura 5.Configuración IPV4 Y IPV6 - PC3



Fuente. elaboración propia

Figura 6. Configuración IPV4 Y IPV6 - PC4



Fuente. elaboración propia

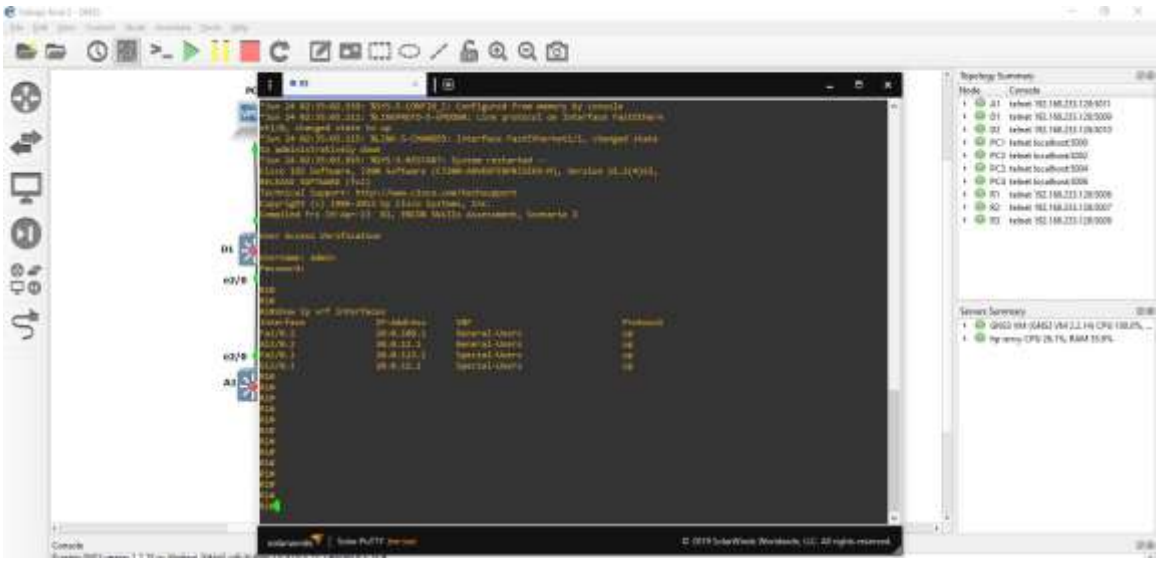
CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO

En esta parte de la evaluación de habilidades, se configuran VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro.

Configuración de VRF

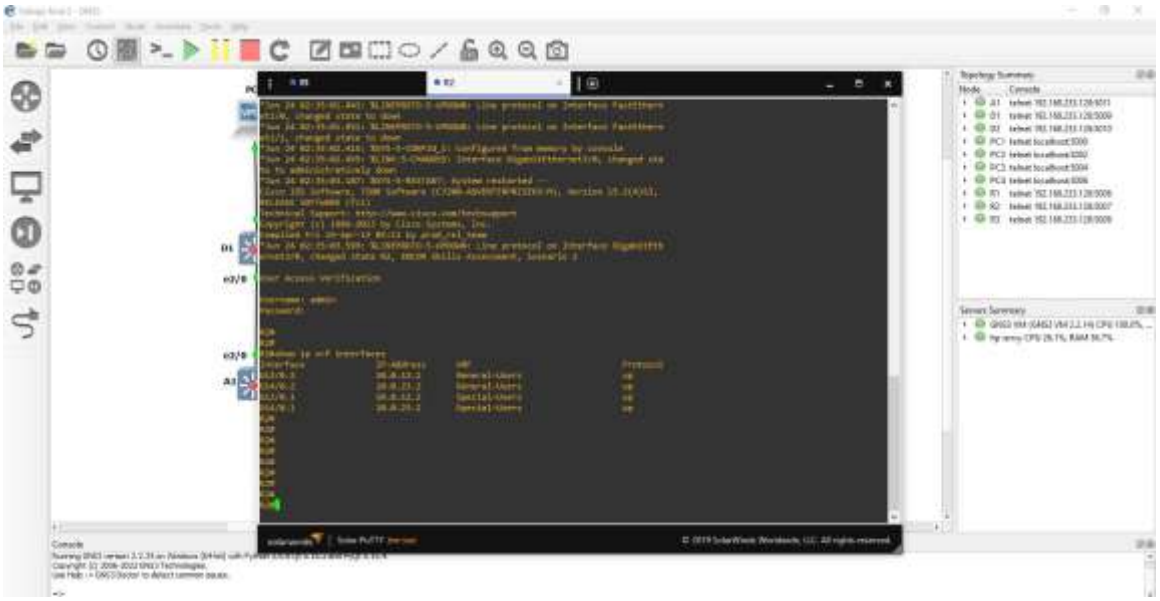
A continuación, se observa en las imágenes la configuración de las VRFs mediante el comando show ip vrf interfaces en R1, R2 y R3, se crean dos vrfs General- Users y Special-Users las cuales admiten ipv4 y ipv6.

Figura 7. Configuración de vrf en R1



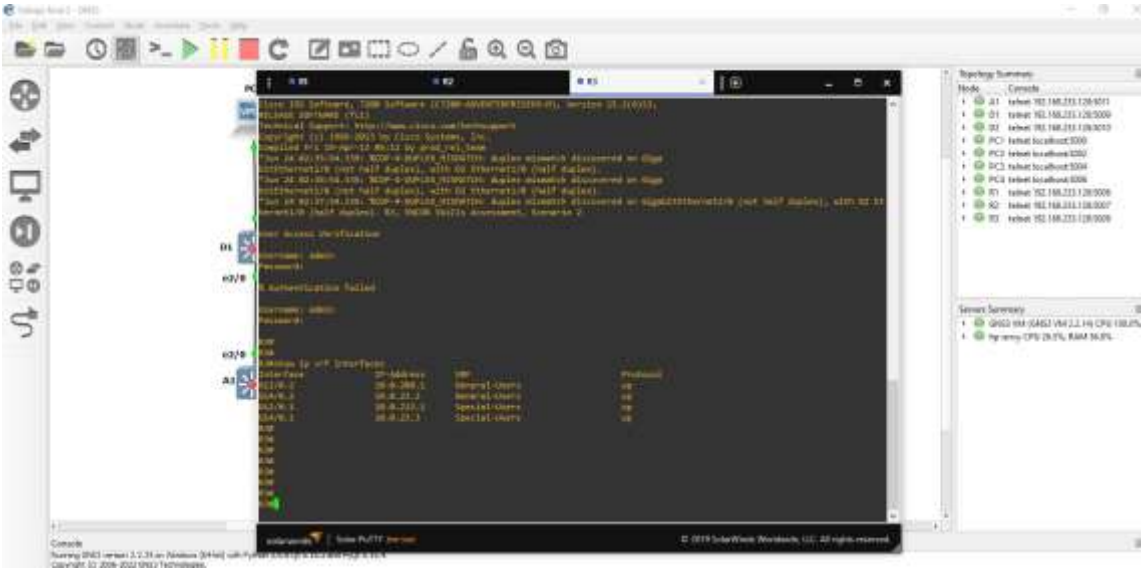
Fuente: Autoría propia.

Figura 8. Configuración de Vrf en R2.



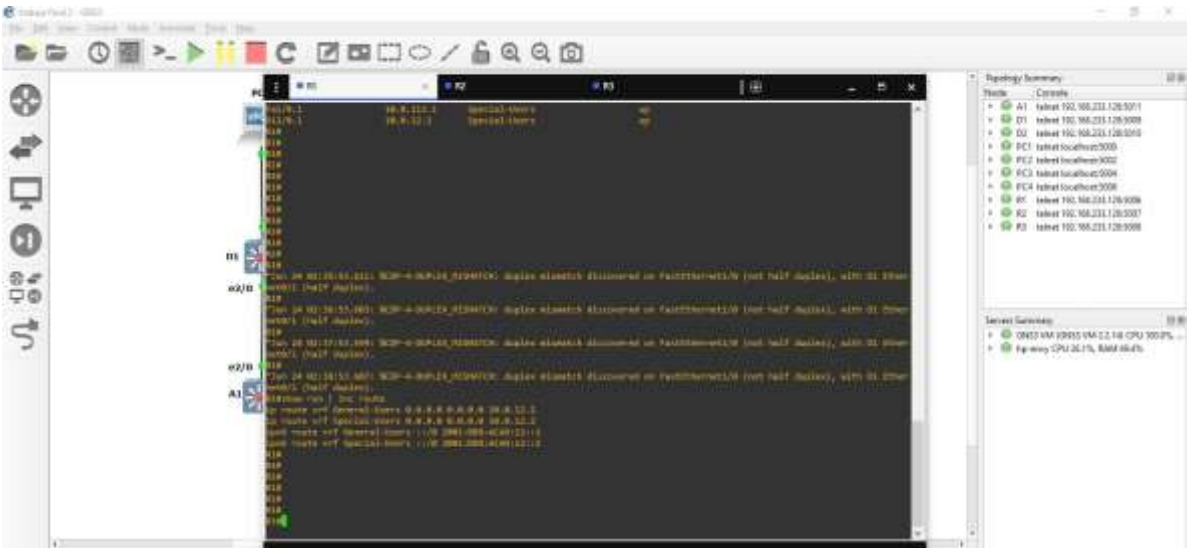
Fuente: Autoría propia.

Figura 9. Configuración de Vrf en R3



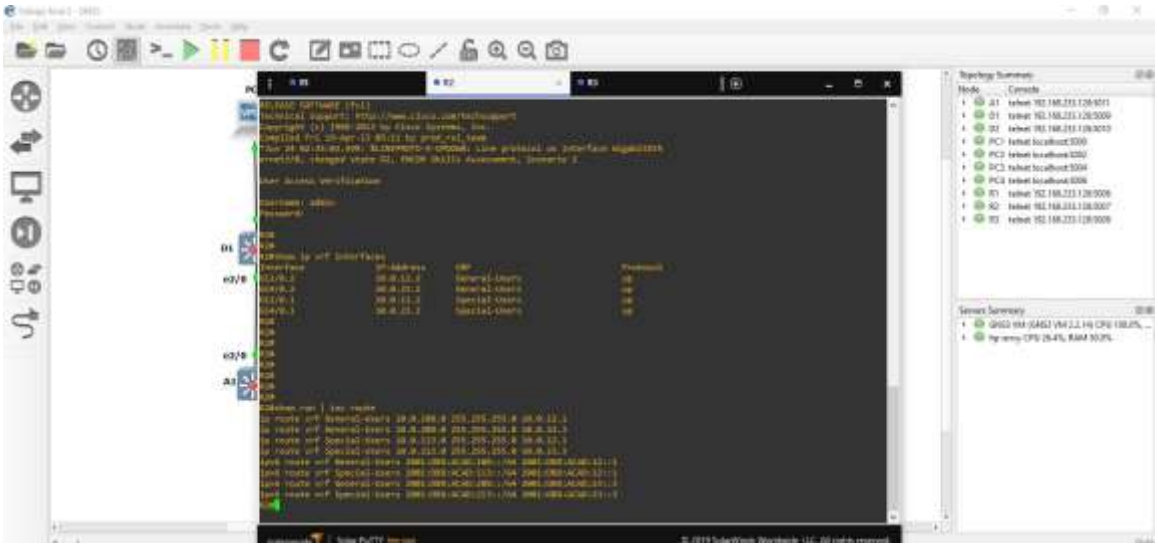
Fuente: Autoría propia.

Figura 10. Verificación de rutas estáticas mediante show run en R1.



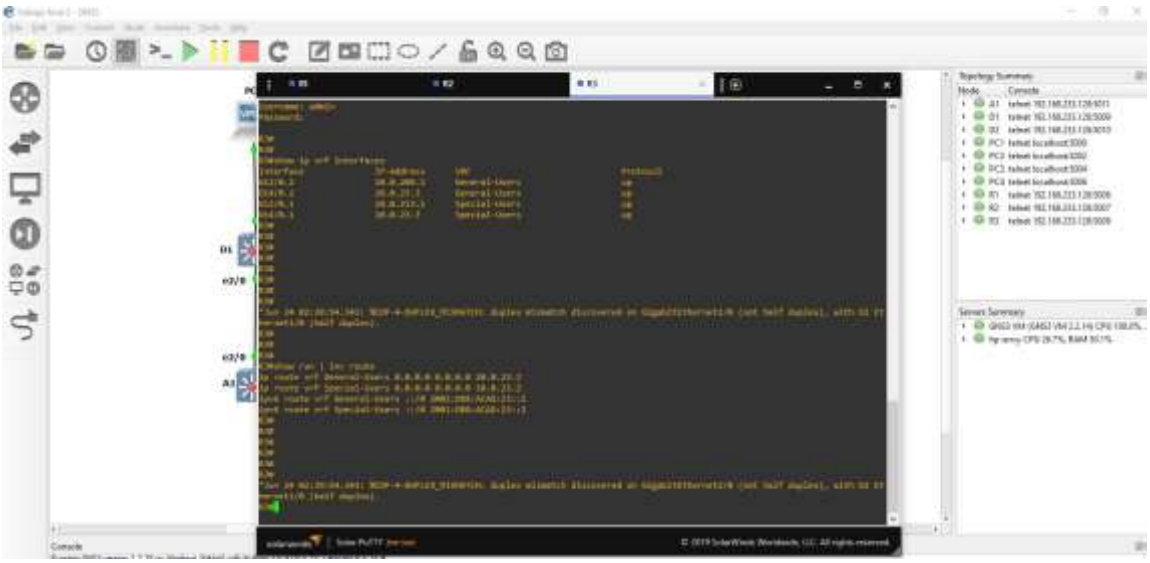
Fuente: Autoría propia.

Figura 11. Verificación de rutas estáticas mediante show run en R2.



Fuente: Autoría propia.

Figura 12. Verificación de rutas estáticas mediante show run en R3.



Fuente: Autoría propia.

Verificación de conectividad

Se puede verificar mediante ping desde el router R1 la conectividad con R3 y como se puede evidenciar en las imágenes 9. los pings son satisfactorios.

ping vrf General-Users 10.0.208.1
ping vrf General-Users 2001:db8:acad:208::1
ping vrf Special-Users 10.0.213.1
ping vrf Special-Users 2001:db8:acad:213::1

Figura 13. Verificación de conectividad

Fuente: Autoría propia.

2. Escenario 2

Parte 3. Configurar Capa 2

En esta parte, tendrá que configurar los Switches para soportar la conectividad con los dispositivos finales. Las tareas de configuración son las siguientes

Tabla 2. Configuración Capa 2

Task#	Task	Specification
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 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.

Fuente: Elaboración Propia

Para esta red existe la agregación del link switch D1 y el switch A1 el cual tiene como función incluir tarjetas de red con dos puertos a los servidores NAS que disponen dos o más puertos Gigabit Ethernet, link agregación nos permite combinar dos o más enlaces físicos ya sea Fast-Ethernet , Gigabit Ethernet e incluso 10 Gigabit de manera que podamos ampliar el ancho de banda de la conexión .

3.1 en D1, D2 y A1 desactive todas las interfaces.

Configuración en D1

Interface range e0/0-3 //ingreso a interfaces desde ethernet 0/0 a ethernet 0/3

Shutdown //apaga las interfaces
Interface range e1/0-3 //ingreso a interfaces desde ethernet 1/0 ethernet 1/3

Shutdown //apaga las interfaces

Configuración en A1

Interface range e0/0-3 //ingreso a interfaces desde ethernet 0/0 a ethernet 0/3

Shutdown //apaga las interfaces
Interface range e1/0-3 //ingreso a interfaces desde ethernet 1/0 ethernet 1/3

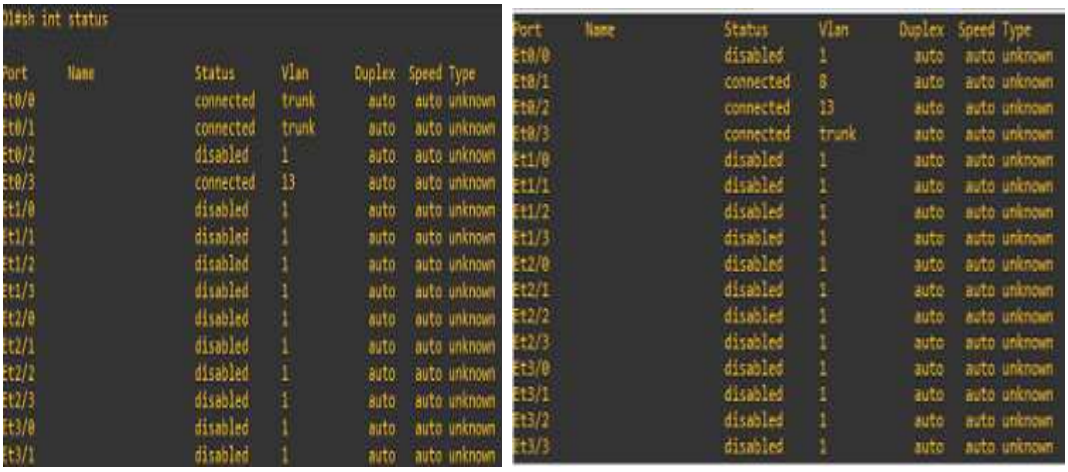
Shutdown //apaga las interfaces

Configuración en D2

Interface range e0/0-3 //ingreso a interfaces desde ethernet 0/0 a ethernet 0/3

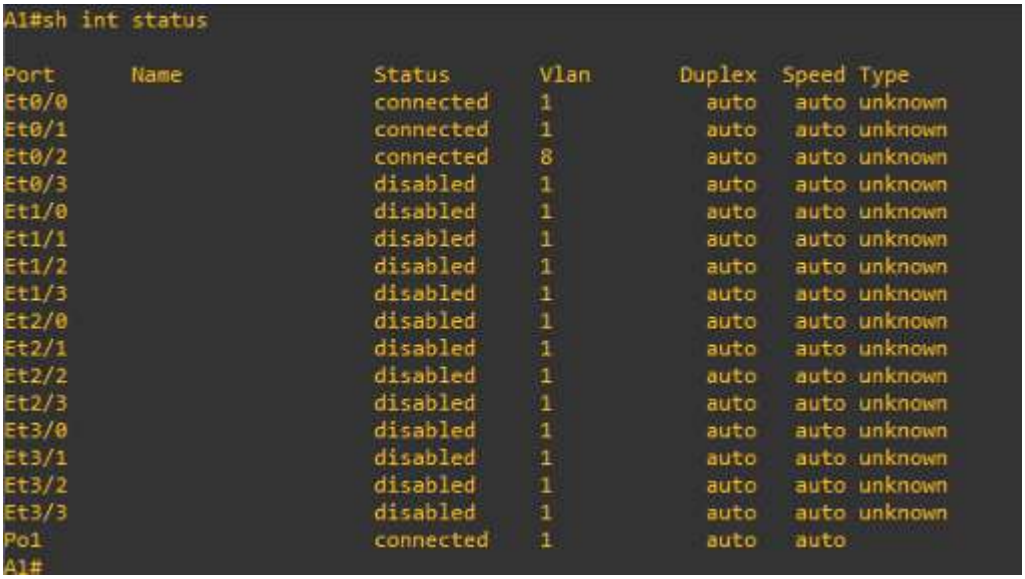
Shutdown //apaga las interfaces

Figura 14. Estado Interfaces D1 y D2



Fuente: Autoría propia.

Figura 15. Interfaces A1



```
A1#sh int status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    1            auto   auto unknown
Et0/1                        connected    1            auto   auto unknown
Et0/2                        connected    8            auto   auto unknown
Et0/3                        disabled     1            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    1            auto   auto
A1#
```

Fuente: Autoría propia.

3.2 En D1 y D2 configure los enlaces troncales a R1 y R3

Configuración enlace troncal Switch D1

Vlan 13 //Determina la vlan
Name Special -User //asigna nombre a la vlan
Exit //Salir

Vlan 8 //Determina la vlan
Name General-User //asigna nombre a la vlan
Exit //salir
Interface ethernet 0/1 //selecciona la interface
Switchport trunk encapsulation dot1q //aplica el modo troncal con encapsulación fot1q

Switchport mode trunk //actica el modo troncal
Switchport trunk allowed vlan 13 //garantiza el modo troncal para la vlan 13
Switchport trunk allowed vlan add 8 //garantiza el modo troncal para la vlan 8

Configuración enlace troncal Switch D2

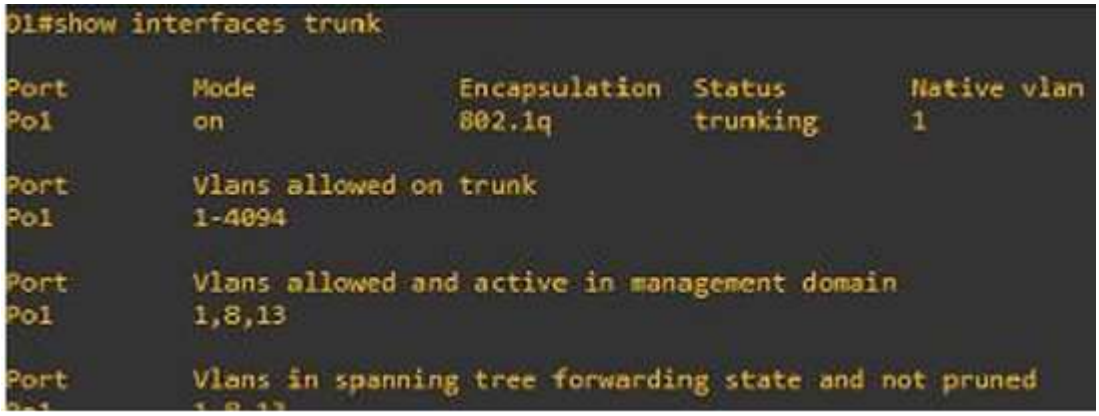
Vlan 13 //Determina la vlan
Name Special -User //asigna nombre a la vlan
Exit //Salir

Vlan 8 //Determina la vlan

Name General-User //asigna nombre a la vlan
Exit //salir
Interface ethernet 0/1 //selecciona la interface
Switchport trunk encapsulation dot1q //aplica el modo troncal con encapsulación fot1q

Switchport mode trunk //activa el modo troncal
Switchport trunk allowed vlan 13 //garantiza el modo troncal para la vlan 13
Switchport trunk allowed vlan add 8 //garantiza el modo troncal para la vlan 8

Figura 16. Configuración en D1 y D2 de los enlaces troncales hacia R1 y R3



Fuente: Autoría propia.

3.3 En D1 y A1 configure EtherChannel

Configuración D1

Interface port-channel 1 //Crea la interfaz port-channel 1
Switchport //la interfaz se comporta como capa 2
Switchport mode Access //se pone en modo acceso
Switchport Access vlan 8 //el trafico solo se admite de la Vlan 8
Exit //salir de la configuración
Interface e1/1 //ingreso a la interface ethernet 1/1
Switchport //ingreso a la interface ethernet 1/1 en modo negación
Channel-group 1 mode desirable //se agrega el puerto al port-channel 1 en modo negación
Switchport mode Access //se pone en modo acceso
Switchport Access vlan 8 //el trafico solo se admite de la Vlan 8
No shutdown //se enciende la interfaz
Exit //salir de la configuración
Interface e1/2 //ingreso a la interface ethernet ½
Switchport //la interfaz se comporta como capa 2
Channel-group 1 mode desirable //se agrega el puerto al port-channel 1 en modo de negociación

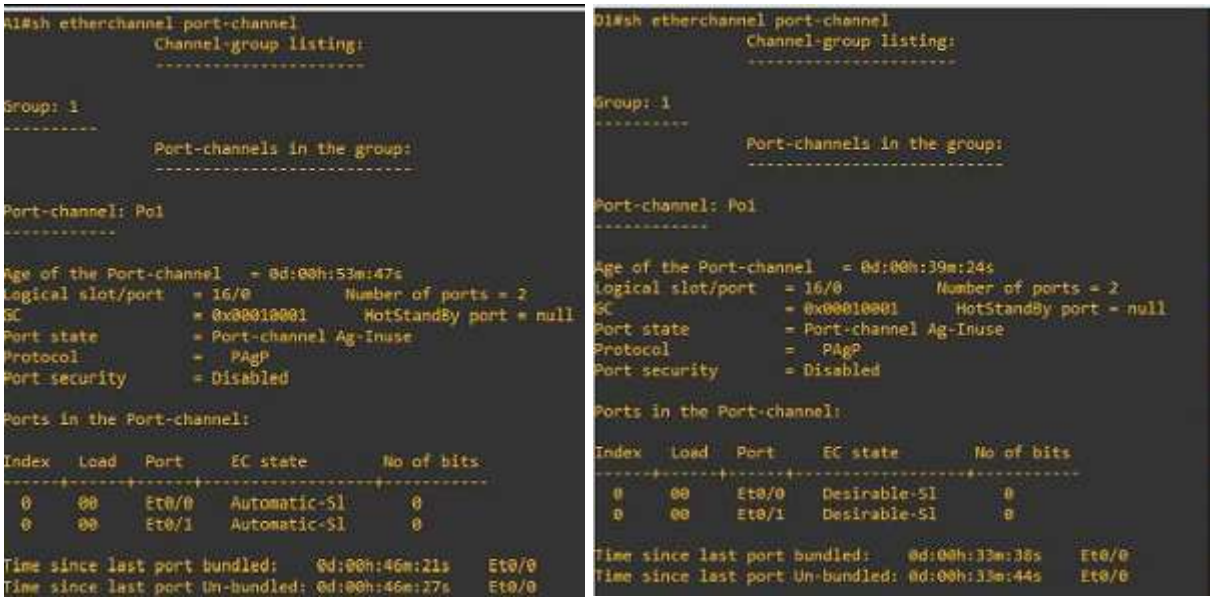
Switchport mode Access //se pone en modo acceso
Switchport Access vlan 8 //el trafico solo admite de la Vlan 8
No shutdown // Se enciende la interfaz
Exit //salir de la configuración

Configuración A1

Interface port-channel 1 //Crea la interfaz port-channel 1
Switchport //la interfaz se comporta como capa 2
Switchport mode Access //se pone en modo acceso
Switchport Access vlan 8 //el tráfico solo se admite de la Vlan 8
Exit //salir de la configuración
Interface e1/1 //ingreso a la interface ethernet 1/1
Switchport //ingreso a la interfaz ethernet capa 2
Channel-group 1 mode desirable //se agrega el puerto al port-channel 1 en modo negación

Switchport mode Access //se pone en modo acceso
Switchport Access vlan 8 //el tráfico solo se admite de la Vlan 8
No shutdown //se enciende la interfaz
Exit //salir de la configuración
Interface e1/2 //ingreso a la interface ethernet 1/2
Switchport //la interfaz se comporta como capa 2
Channel-group 1 mode desirable //se agrega el puerto al port-channel 1 en modo de negociación
Switchport mode Access //se pone en modo acceso
Switchport Access vlan 8 //el tráfico solo admite de la Vlan 8
No shutdown // Se enciende la interfaz
Exit //salir de la configuración

Figura 17. Configuración Ethernetchannel D1 y A1



Fuente: Autoría propia.

En primer switch D1 y el Switch D3 se configura como modo troncal, debido a que por ambos switch se lleva acabo el paso de la informacion de las dos zonas que se han configurado en la red.

Vlan 13 y Vlan 8 denominados Special-User y General-User respectivamente. En el switch D1 mediante la orden show interfaces trunk es posible evidenciar que el modo troncal esta activo y de igual manera se vinculan las vlans 8 y 13 para el acceso de cada zona y el reenvio de paquetes.

Mediante el comando show etherchannel summary, podemos comprobar la linea de informacion por canal de cada puerto.

La configuracion que se lleva a cabo en el lnk agregation se realiza en los dos puertos del Switch D1 como en los dos puertos del Switch A1. Primero es necesario crear la interface que controlara el link agregation.

3.4 En D1, D2 y A1 configure los puertos de acceso de PC1, PC2, PC3 Y PC4

Configuracion puertos de acceso para PC1 en D1

```
Interface e0/0                    //ingreso a interfaz ethernet 0/0
Switchport mode Access            //se pone en modo acceso
Switchport Access vlan 8          //solo se permite acceso a la vlan 8
Spanning-tree portfast            //se habilita el PortFast
No shutdown                       //se enciende la interfaz
```

Configuracion uertos de acceso para PC3 en A1

Interface e0/0 //ingreso a interfaz ethernet 0/0
Switchport mode Access //se pone en modo acceso
Switchport Access vlan 8 //solo se permite acceso a la vlan 8
Spanning-tree portfast //se habilita el PortFast
No shutdown //se enciende la interfaz

Configuracion puertos de acceso para PC2 Y PC4 en D2

Interface e0/1 //ingreso a interfaz ethernet 0/1
Switchport mode Access //se pone en modo acceso
Switchport Access vlan 13 //solo se permite acceso a la vlan 13
Spanning-tree portfast //se habilita el PortFast
No shutdown //se enciende la interfaz

Interface e0/2 //ingreso a interfaz ethernet 0/2
Switchport mode Access //se pone en modo acceso
Switchport Access vlan //solo se permite acceso a la vlan 8
Spanning-tree portfast //se habilita el PortFast
No shutdown //se enciende la interfaz

Figura 18. Configuración en D1,D2 and A1 puertos de acceso para PC1, PC2, PC3, y PC4

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 1 mode desirable
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 1 mode desirable
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 switchport access vlan 13
 switchport trunk encapsulation dot1q
 switchport mode access
 spanning-tree portfast edge
```

```
interface Ethernet0/0
 shutdown
!
interface Ethernet0/1
 switchport access vlan 8
 switchport mode access
 spanning-tree portfast edge
!
interface Ethernet0/2
 switchport access vlan 13
 switchport mode access
 spanning-tree portfast edge
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

```
interface Port-channel1
 switchport trunk encapsulation dot1q
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 channel-protocol pagp
 channel-group 1 mode auto
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 channel-protocol pagp
 channel-group 1 mode auto
!
interface Ethernet0/2
 switchport access vlan 8
 switchport mode access
 spanning-tree portfast edge
```

Fuente: Autoría propia.

3.5 verifique la conectividad de PC a PC

Desde PC1 has PC2

PC1>PING 10.0.213.50

Desde PC3 hasta PC4
PC3>PING 10.0.208.50

Conectividad entre PC1 y PC2 en Vlan 13 Special-User
Conectividad entre PC3 y PC4 en Vlan 8 Special-User
Entre las dos Vlan, no debe hacer comunicación

Figura 19. Verificación conectividad IPV4 Y IPV6

```
PC3> ping 10.0.213.45

10.0.213.45 icmp_seq=1 ttl=64 time=0.001 ms
10.0.213.45 icmp_seq=2 ttl=64 time=0.001 ms
10.0.213.45 icmp_seq=3 ttl=64 time=0.001 ms
10.0.213.45 icmp_seq=4 ttl=64 time=0.001 ms
10.0.213.45 icmp_seq=5 ttl=64 time=0.001 ms
```

```
PC3> ping 10.0.208.45

10.0.208.45 icmp_seq=1 ttl=64 time=0.001 ms
10.0.208.45 icmp_seq=2 ttl=64 time=0.001 ms
10.0.208.45 icmp_seq=3 ttl=64 time=0.001 ms
10.0.208.45 icmp_seq=4 ttl=64 time=0.001 ms
10.0.208.45 icmp_seq=5 ttl=64 time=0.001 ms
```

Fuente: Autoría propia.

En la figura anterior se evidencia que no existe concetividad entre PC1 Y PC3 ya que pertenecen a VRF distintas por tanto laconfiguracin obedece a lo solicitado. Los PC deben configurarse tal como se indica en el escenario.

Tabla 3. Direcciones IPV4 e IPV6 para las estaciones de trabajo

EQUIPO	DIRECCION IPV4	DIRECCION IPV6	GATEWAY
PC1	**10.0.113.50/24**	**2001:db8:acad:113::50/64**	**10.0.113.1**
PC2	**10.0.213.50/24**	**2001:db8:acad:213::50/64**	**10.0.213.1**
PC3	**10.0.108.50/24**	**2001:db8:acad:108::50/64**	**10.0.108.1**
PC4	**10.0.208.50/24**	**2001:db8:acad:208::50/64**	**10.0.208.1**

Fuente: documento de escenario propuesto

Cada uno de los equipos tiene asignada una direccion ipv4 y tambien una direccion IPV6 es necesario que a los equipos se les determine una direccion de gateway ya que es la que orienta en el primer salto al equipo para que pueda hacer el primer enlace de la conexión.

Parte 4: Configurar la seguridad

En todos los dispositivos que se encuentran dentro una red, es necesario la adicion de seguridad y para la configuracion del escenario del presente trabajo se da aplicación con privilegio de categoria 15 y seguridad triple A a cada uno de los componenetes que conforman la red tanto routers como switchs.

Tabla 4. Configurar la seguridad

Task#	Task	Specification
4.1	On all devices, secure privileged EXE mode.	Configure an enable secret as follows: • Algorithm type: **SCRYPT** • Password: **nombreestudianteXYZ**.
4.2	On all devices, create a local user account.	Configure a local user: • Name: **admin** • Privilege level: **15** • Algorithm type: **SCRYPT** • Password: **nombrestudianteXYZ**.
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

Fuente: Elaboración Propia

Router R1:

Enable algorithm-type scrypt secret MaylebiscastellarnizXYZ //habilita el modo de contraseña // en privilegio 15 se asigna nombre de usuario y contraseña
Username admin privilige 15 Algoritthm-type scrypt secret MaylebiscastellarnizXYZ
aaa new-model //se habilita la seguridad triple A para la aaa
authentication login default local autenticacion loca

Router R2:

Enable algorithm-type scrypt secret MaylebiscastellarnizXYZ //habilita el modo de contraseña // en privilegio 15 se asigna nombre de usuario y contraseña
Username admin privilige 15 Algoritthm-type scrypt secret MaylebiscastellarnizXYZ
aaa new-model //se habilita la seguridad triple A para la aaa
authentication login default local autenticacion loca

Router 3

Enable algorithm-type scrypt secret MaylebiscastellarnizXYZ //habilita el modo de contraseña // en privilegio 15 se asigna nombre de usuario y contraseña
Username admin privilige 15 Algoritthm-type scrypt secret MaylebiscastellarnizXYZ
aaa new-model //se habilita la seguridad triple A para la aaa
authentication login default local autenticacion loca

Switch D1:

Service password-encryption //Modo de encryptacion
Enable secret MaylebiscastellarnizXYZ // habilita la contraseña
Username admin secret 0 //determian el usuario y contraseña MaylebiscastellarnizXYZ
aaa new-model //se habilita la seguridad triple A para la authentication aaa authentication login default local autenticacion loca

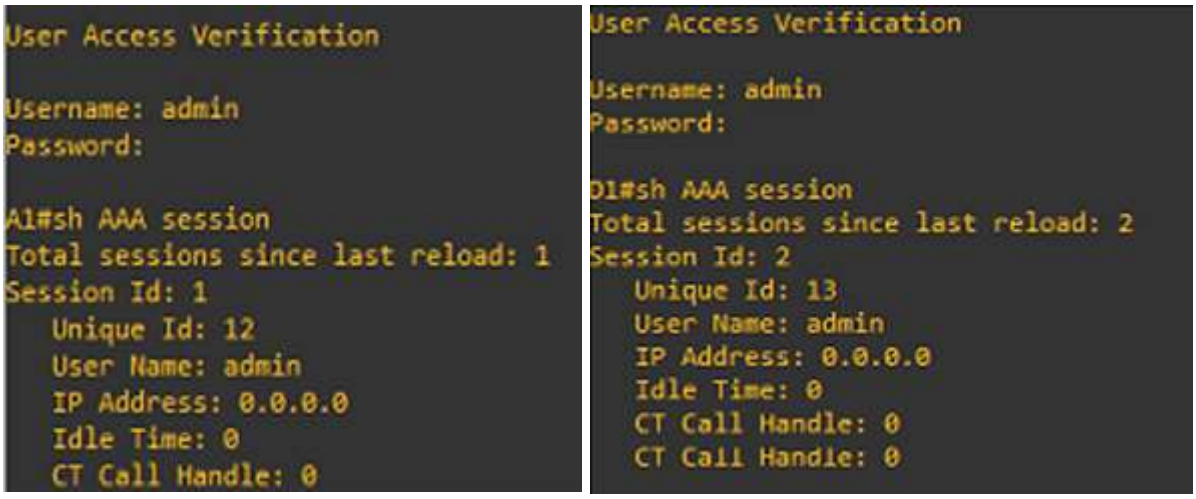
Switch D2

Service password-encryption //Modo de encryptacion
Enable secret MaylebiscastellarnizXYZ // habilita la contraseña
Username admin secret 0 //determian el usuario y contraseña MaylebiscastellarnizXYZ
aaa new-model //se habilita la seguridad triple A para la authentication aaa authentication login default local autenticacion loca

Switch A1

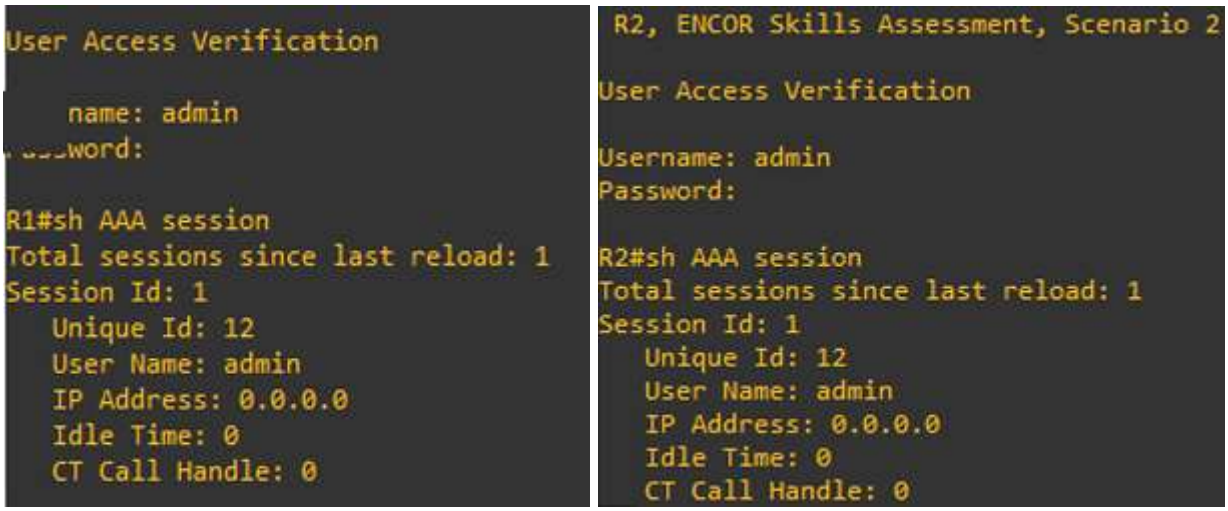
Service password-encryption //Modo de encryptacion
Enable secret MaylebiscastellarnizXYZ // habilita la contraseña
Username admin secret 0 //determian el usuario y contraseña MaylebiscastellarnizXYZ
aaa new-model //se habilita la seguridad triple A para la authentication aaa authentication login default local autenticacion loca

Figura 20. Verificación usuario, contraseña y sh AAA sesión para D1, D2 y A1



Fuente: Autoría propia.

Figura 21. Verificación usuario, contraseña y sh AAA sesión para R1, R2 y R3




User Access Verification
Username: admin
Password:
R3#sh AAA session
Total sessions since last reload: 2
Session Id: 2
Unique Id: 13
User Name: admin
IP Address: 0.0.0.0
Idle Time: 0

CONCLUSIONES

Se logra comprender y así mismo se destaca los programas como el GNS3 (Graphic Network Simulation o Simulación Grafica de Redes) donde este simulador grafico de red permite diseñar topología de una red compleja, así como diversos protocolos y métricas de enrutamiento, con la capacidad de simulación de dispositivos reales. Mediante el uso de VRF (Enrutamiento virtual) se logra la configuración de las tablas de enrutamiento propuestas para la actividad, así logrando una separación de tipo lógico para las redes dentro del enrutamiento, permitiendo así la capacidad de manejar más de un esquema de enrutamiento mediante los mismos dispositivos. Se destaca acerca del uso de VRF, que permite utilizar la misma dirección IP en diferentes interfaces de este router, sin entrar en conflicto entre ellas. Concluimos así que la tecnología VRF, es clave en la escalabilidad de redes ya que permite el ahorro de la cantidad de router que se utilizan para el desarrollo de las redes, también aportando a la seguridad de la red.

BIBLIOGRAFIAS

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). Multicast. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). QoS. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). IP Services. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). Enterprise Network Architecture. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). Fabric Technologies. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). Press (Ed). Network Assurance. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8