DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LEIDY ROCÍO RAMÍREZ SANCHEZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LEIDY ROCIO RAMIREZ SANCHEZ

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

DIRECTOR:
JUAN ESTEBAN TAPIAS

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 23 DE ABRIL DE 2023

AGRADECIMIENTOS

Reitero mis agradecimientos, primeramente, a Dios, a mis padres, esposo y familiares que brindaron un granito de arena para el cumplimiento de mis logros académicos , a profesores y compañeros que me apoyaron con su conocimiento y me alentaron a continuar con el proceso de formación académica,

Contenido

INDICE DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Network,
O red, es un conjunto de ordenadores que están conectados entre ellos y comparten información, siendo un enrutamiento de una misma dirección ipv4 o ipv6, las redes pueden estar conectadas de diferentes formas, en forma de estrella, en circulo, en forma de malla, o red mixta. Están conectados por medio de cableado estructurado, disminuyendo gastos y licencias en sistemas operativos corporativos.

CCNP,
Es la certificación profesional ofrecida por cisco Certified, Network Professional, que avala al profesional en redes en la capacidad de crear, implementar, diseñar redes WAN y LAN que den soluciones de redes de datos en la industria, la aeronáutica, aviación, el sector público, sector educativo y todo lo que se necesite conectar una red. Siendo un experto, es indispensable aprobar el examen de la academia cisco.

Redes VRF,
Permite la tecnología en el diseño de redes aplicando varios enrutamientos independientes dentro del mismo Reuter, enrutamiento virtual y reenvío, sus siglas en ingles es Virtual Routing and Forwarding, ejecuta la tabla de enrutamiento a las interfaces usando la misma dirección IP. cada VRF es independiente, con una misma subred se puede aplicar en dos VRF creada, segmentando la red con una tabla de enrutamiento virtualizada separada.

VLANS,
Red lógica, red de área virtual, que permiten una difusión mayor en la subred, y dividiéndolas en pequeñas estaciones de trabajo, agiliza el tráfico en la red, los switches son los encargados de dividir la red, mediante los puertos de acceso, que pueden ser de 8, 12, 24, 36 puertos y más.

Reuters
O enrutador es el dispositivo encargado de dirigir la red, ya que en este se configura el direccionamiento estático, se divide las subinterfaces y se implementan protocolos de configuración como DHCP, DNS, OSPF entre otros.

RESUMEN

El presente informe corresponde a la prueba final Prueba de Habilidades Practicas del Diplomado de profundización CCNP, que se realiza en el simulador GNS3 que permite crear e implementar una red, se utilizan dispositivos cisco y se da solución a un escenario propuesto quien tiene una implementación de redes VRF, una red VRF el Reuter está configurado en un direccionamiento que utiliza la misma dirección IP que se asigna a dos interfaces distintas, este Reuter conecta con otros Reuters y a un switch que esta segmentado en vlans diferentes. Las subinterfaces creadas extienden la red, siendo una red escalable.

El escenario propuesto exige una solución, la redes VRF al implementarse en un escenario donde hay dos usuarios, Special Users y General Users que comparte la misma IP, el tráfico de red es independiente uno del otro, la seguridad de la red es autenticada con protocolo de seguridad de contraseña secreta y esquema de autenticación y autorización AAA.
El control de acceso como Radius (Cisco) permite el acceso solo a usuarios autorizados

Palabras Clave: Redes, Switch, vlan, Router, CCNP,

SUMMARY

This report corresponds to the final test Practical Skills Test of the CCNP Deepening Diploma, which is carried out in the GNS3 simulator that allows the creation and implementation of a network, Cisco devices are used and a solution is given to a proposed scenario who has an implementation of VRF networks, a VRF network the Router is configured in an address that uses the same IP address that is assigned to two different interfaces, this Router connects with other Reuters and to a switch that is segmented into different vlans. The created sub interfaces extend the network, being a scalable network.

The proposed scenario requires a solution, the vrf networks when implemented in a scenario where there are two users, Special Users and General Users who share the same IP, the network traffic is independent of each other, the network security is authenticated with protocol secret password security and AAA authentication and authorization scheme.
Access control such as Radius (Cisco) allows access only to authorized users

Keywords: Networks, Switch, vlan, Router, CCNP,

INTRODUCCIÓN

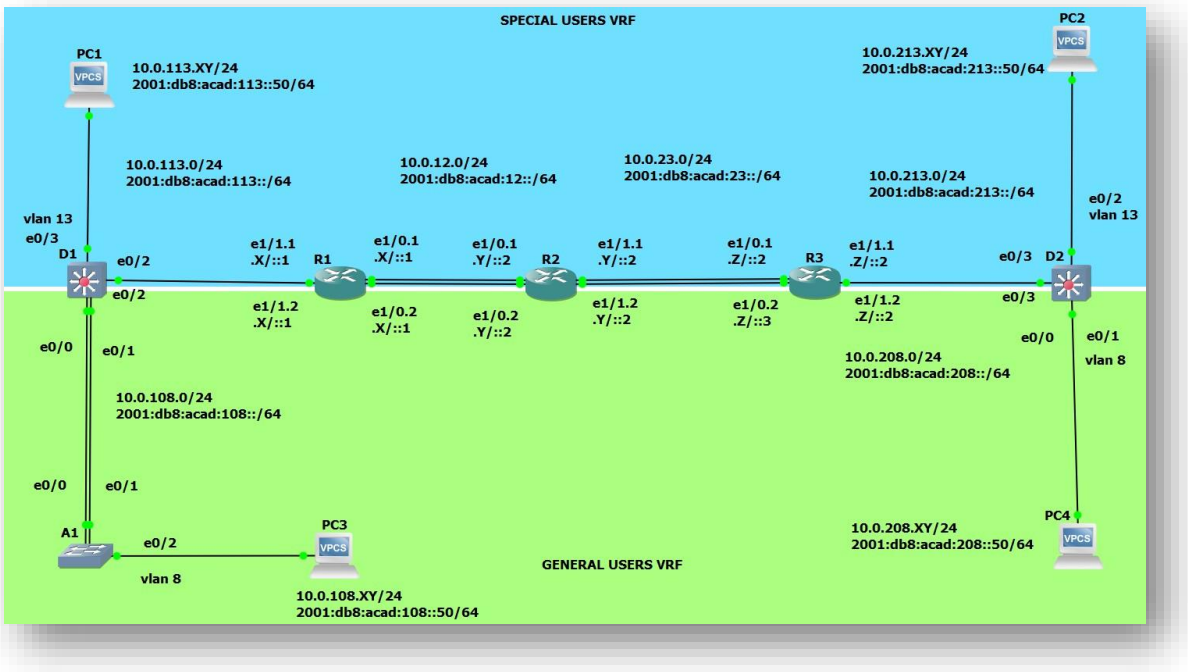
El trabajo presentado Prueba de Habilidades Practicas donde se da una solución a un problema implementando una red que cumpla con las especificaciones de un escenario propuestos, el documento desarrolla una serie de pasos, se divide en cuatro partes, configuración básica en los Reuters, direccionamiento, configuración de capa dos (switch)y seguridad en la red.

La implementación de la red está compuesta por dispositivos de enrutamiento (Reuters), dispositivos de capa dos (switch) y host finales (Pc), conectado por medio de cable de red, la configuración es de redes VRF, con dos usuarios, uno para usuarios generales y el otro para usuarios especiales y con una tabla de direccionamiento que especifica las direcciones de red a cada una de las subinterfaces.

PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE CADA DISPOSITIVO Y EL DIRECCIONAMIENTO DELAS INTERFACES

En la Parte 1, configurará la topología de la red y configurará los ajustes básicos.

Figura 1. Escenario Propuesto



Fuente: guía prueba final

Escenario

En esta evaluación de habilidades, usted es responsable de completar la configuración multi-VRF de 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.

Asegúrese de verificar que sus configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según lo requerido.

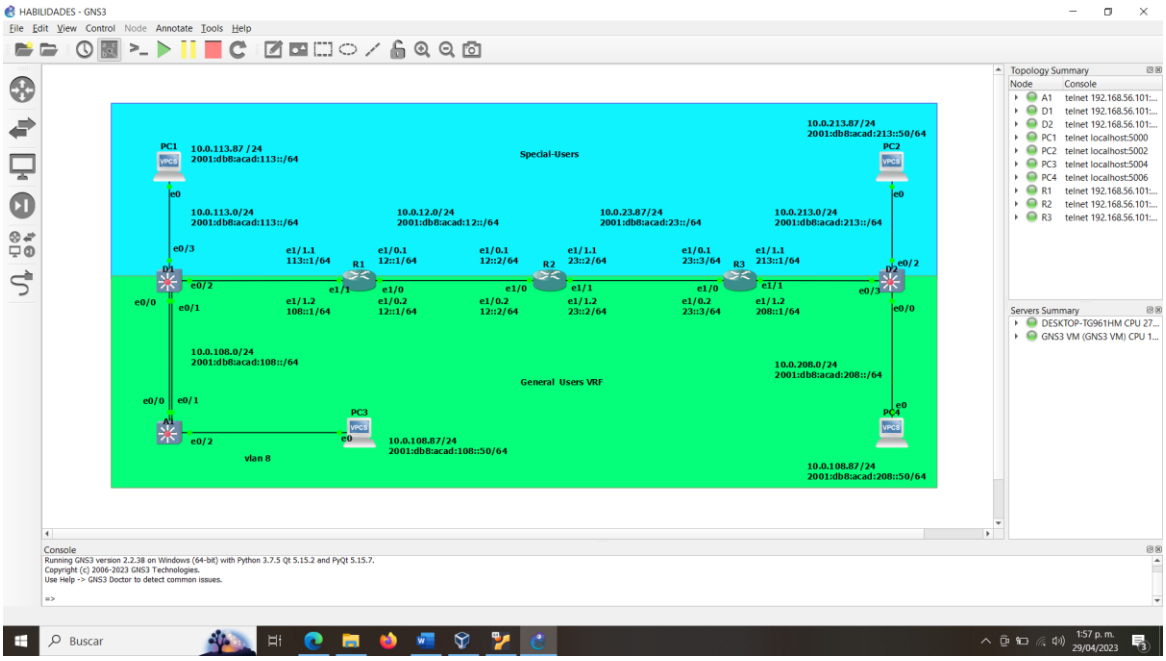
Paso 1: Cablee la red como se muestra en la topología.

En la Parte 1, configurará la topología de la red y configurará los ajustes básicos.

Cablee la red como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y cablee según sea necesario.

Figura 2 Simulador escenario propuesto



Fuente: Elaboración propia

Por medio del simulador GNS3 se realiza el escenario propuesto. Compuesto por los dispositivos de red (Reuter, switch, pc) y conectado según la figura 1 escenario propuesto.

Tabla de direccionamiento

La Tabla de Direccionamiento muestras las direcciones ip con protocolo IPV4 e IPV6, dirección IPv6 Link-Local, las subinterfaces, los dispositivos Reuters, Switches, Computadores PCs, y el nombre dl dispositivos.

Tabla 1 Direccionamiento de la Red

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.8/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.8/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.8/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.8/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.7/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.7/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.7/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.7/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.87/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.87/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.87/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.87/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Documento tabla 1 prueba de habilidades
1XXXX68710 X=8 Y=7 Z=1

Paso 2: Configure los ajustes básicos para cada dispositivo.

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

Configuración Básica de la red.

En Router R1
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

En 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

En 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

En 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

En 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

En 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

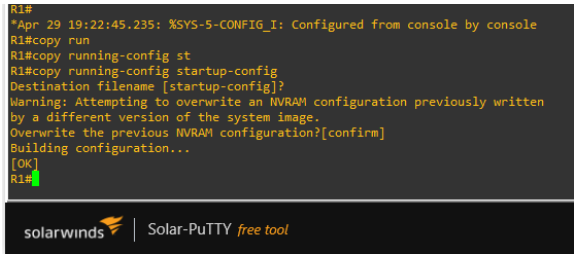
b. Guarde las configuraciones en cada uno de los dispositivos.

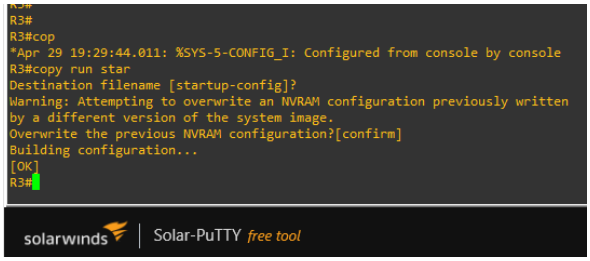
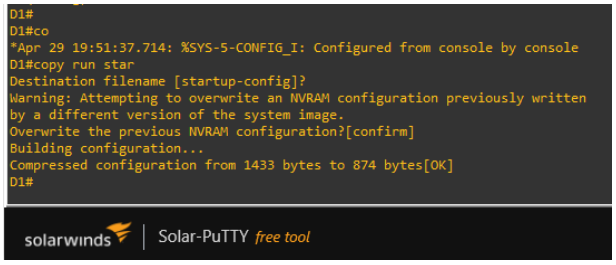
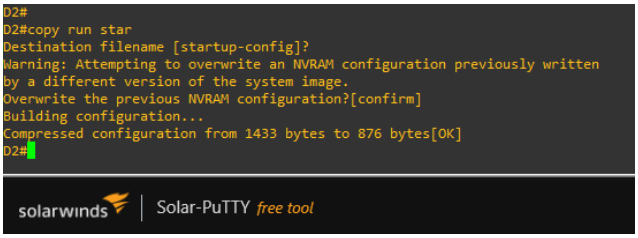
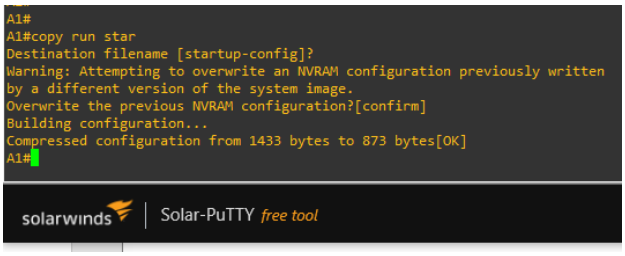
En modo usuario, se guarda la configuración con el comando copy running startup config en el dispositivo

copy running-config startup-config
en forma abreviada
copy running startup config
y la configuración se guarda en la Nvram del dispositivo, al momento de apagar y encender de nuevo la configuración sigue disponible en el dispositivo.

Guardar la configuración en los dispositivos R1, R2, R3, D1, D2 y A1

Tabla 2 Guardar la configuración en los dispositivos

comando copy running startup config en R1 	R1#copy run star Destination filename [startup-config]? Building configuration... [OK] R1#
comando copy running startup config en R2 	R2#copy run star Destination filename [startup-config]? Building configuration... [OK] R2#
comando copy running startup config en R3,	R3#copy run star

	Destination filename [startup- config]? Building configuration... [OK] R3#
comando copy running startup config en D1 	*D1#copy run star* *Destination filename [startup-config]?* *Building configuration...* *[OK]* *D1#*
comando copy running startup config en D2 	*D2#copy run star* *Destination filename [startup-config]?* *Building configuration...* *[OK]* *D2#*
comando copy running startup config en A1 	*A1#copy run star* *Destination filename [startup-config]?* *Building configuration...* *[OK]* *A1#*

Fuente: Elaboración propia

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

PC1

PC1> ip 10.0.113.87/24 10.0.113.1
Checking for duplicate address...
PC1 : 10.0.113.87 255.255.255.0 gateway 10.0.113.1
PC1> ip 2001:db8:acad:113::50/64
PC1 : 2001:db8:acad:113::50/64

PC2,

PC2> ip 10.0.213.87/24 10.0.213.1
Checking for duplicate address...
PC2 : 10.0.213.87 255.255.255.0 gateway 10.0.213.1
PC2> ip 201:db8:acad:213::50/64
PC2 : 201:db8:acad:213::50/64

PC3

PC3> ip 10.0.108.87/24 10.0.108.1
Checking for duplicate address...
PC3 : 10.0.108.87 255.255.255.0 gateway 10.0.108.1
PC3> ip 2001:db8:acad:108::50/64
PC1 : 2001:db8:acad:108::50/64

PC4

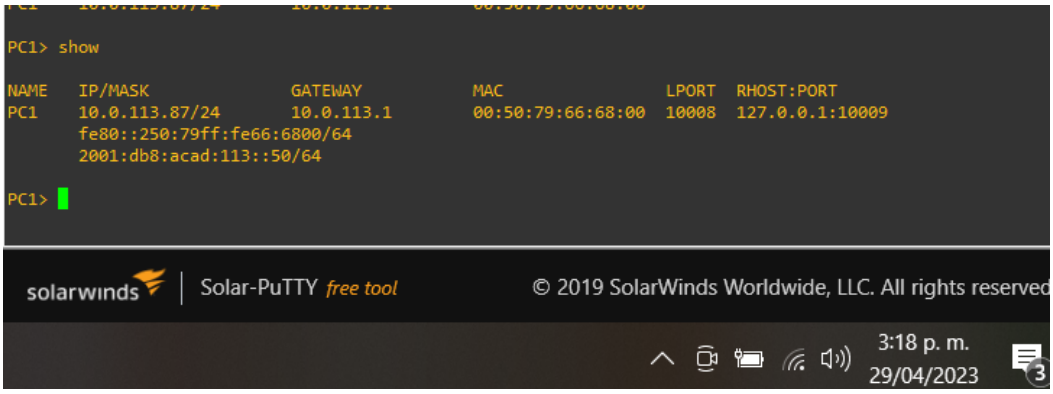
PC4> ip 10.0.208.87/24 10.0.208.1
Checking for duplicate address...
PC4 : 10.0.208.87 255.255.255.0 gateway 10.0.208.1
PC4> ip 2001:db8:acad:208::50/64
PC4 : 2001:db8:acad:208::50/64

Se recomienda guardar la configuracion de los PCs ingresando el commando “Save” en cada uno de ellos.

Verificar el direccionamiento de los PCs

En GNS3 permite revisar la dirección del PC1 usando el comando Show solamente, también se puede mostrar información con otros comandos como “Show ipv4 details”, “Show ipv6 details”, “Show Version” son los más utilizados.

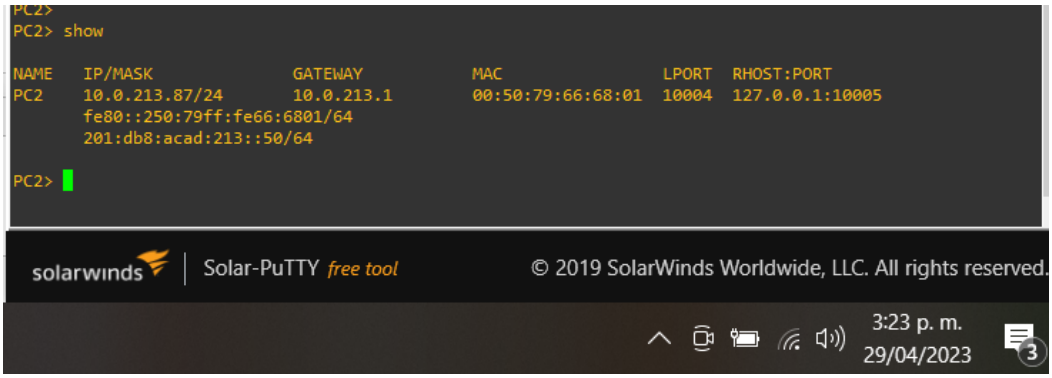
Figura 3. show en PC1



Fuente: Elaboración propia

Al verificar la configuración de enrutamiento en PC1 se identifica el nombre, la máscara de subred, la puerta de enlace, la identificación MAC del dispositivo. El puerto y la dirección IPv4 e IPv6.

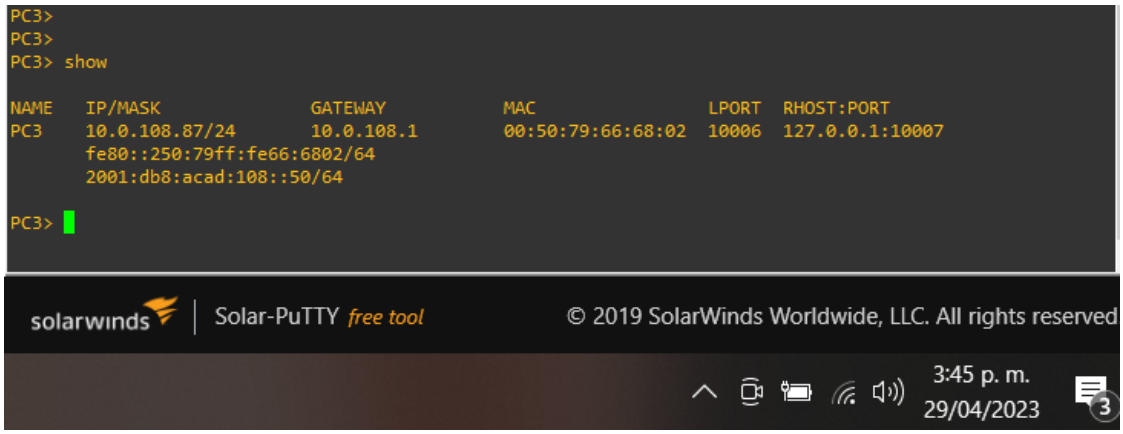
Figura 4. show en PC2



Fuente: Elaboración propia

Es igual en la configuración de enrutamiento en PC2 se identifica el nombre, la máscara de subred, la puerta de enlace, la identificación MAC del dispositivo. El puerto y la dirección IPv4 e IPv6.

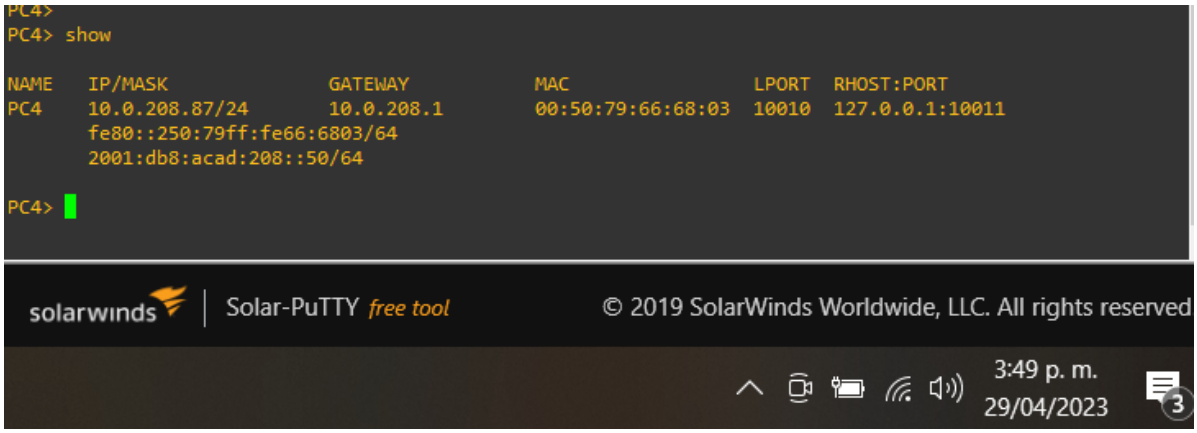
Figura 5. show en PC3



Fuente: Elaboración propia

en la configuración de enrutamiento en PC3 se identifica el nombre, la máscara de subred, la puerta de enlace, la identificación MAC del dispositivo. El puerto y la dirección IPv4 e IPv6.

Figura 6 show en PC4



Fuente: Elaboración propia

en PC4 se identifica el nombre, la máscara de subred, la puerta de enlace, la identificación MAC del dispositivo. El puerto y la dirección IPv4 e IPv6.

PARTE 2: CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO

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

Sus tareas de configuración son las siguientes:
Tabla 3 parte dos configurar VRF y enrutamiento estático

Tarea #	Tarea	Especificación
2.1	En R1, R2 y R3, configure VRF VRF-Lite como se muestra en el diagrama de topología.	Configure dos VRF: Usuarios generales Usuarios especiales Los VRF deben admitir IPv4 e IPv6.
2.2	En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.	Todos los Reuters utilizarán Reuter-En-A-Stick en sus interfaces G0/0/1.x para admitir la separación de los VRF. Subinterfaz 1: En el VRF de usuarios especiales Usar encapsulación dot1q 13 IPv4 e IPv6 GUA y direcciones locales de enlace Habilitar las interfaces Subinterfaz 2: En el VRF de usuarios generales Usar encapsulación dot1q 8 IPv4 e IPv6 GUA y direcciones locales de enlace Habilitar las interfaces
2.3	En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.	Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.
2.4	Verifique la conectividad en cada VRF.	Desde R1, verifique la conectividad con R3: ping VRF General-Usuarios

		10.0.208.Z ping VRF General-Users 2001:db8:acad:208::1 ping VRF Special-Users 10.0.213.Z ping VRF Special-Users 2001:db8:acad:213::1

Fuente: Elaboración propia

Nota: R1 no estará habilitado para realizar ping entre PC2 o PC4 con la configuración de las Partes 1 y 2.

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

Se configura dos VRF, Usuarios generales, Usuarios especiales,
Los VRF deben admitir IPv4 e IPv6

Configuración R 1

```
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#vrf definition General-Users
R1(config-vrf)#address-family ipv4
R1(config-vrf-af)#address-family ipv6
R1(config-vrf-af)#exit
R1(config-vrf)#vrf definition Special-Users
R1(config-vrf)#address-family ipv4
R1(config-vrf-af)#address-family ipv6
R1(config-vrf-af)#exit
```

Configuración R 2

```
R2#enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#vrf definition General-Users
R2(config-vrf)#address-family ipv4
```

R2(config-vrf-af)#address-family ipv6
R2(config-vrf-af)#exit
R2(config-vrf)#vrf definition Special-Users
R2(config-vrf)#address-family ipv4
R2(config-vrf-af)#address-family ipv6
R2(config-vrf-af)#exit

Configuración R3
R3#enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#vrf definition General-Users
R3(config-vrf)#address-family ipv4
R3(config-vrf-af)#address-family ipv6
R3(config-vrf-af)#exit
R3(config-vrf)#vrf definition Special-Users
R3(config-vrf)#address-family ipv4
R3(config-vrf-af)#address-family ipv6
R3(config-vrf-af)#exit

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

Se debe revisar la tabla de direccionamiento y aplicar la siguiente configuracion. segun las especificaciones anteriores a los router R1, R2 y R3.

Habilitar las interfaces

Todos los Reuters utilizarán Reuter-En-A-Stick en sus interfaces G0/0/1.x para admitir la separación de los VRF.
Subinterfaz 1:
En el VRF de usuarios especiales
Usar encapsulación dot1q 13
IPv4 e IPv6 GUA y direcciones locales de enlace
Habilitar las interfaces
Subinterfaz 2:
En el VRF de usuarios generales
Usar encapsulación dot1q 8
IPv4 e IPv6 GUA y direcciones locales de enlace

VRF en R 1

R1#confi term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface E1/0.1
R1(config-subif)#encapsulation dot1q 13
R1(config-subif)#vrf forwarding Special-Users
R1(config-subif)#ip address 10.0.12.8 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:12::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit

R1(config)#interface E1/0.2
R1(config-subif)#encapsulation dot1q 8
R1(config-subif)#vrf forwarding General-Users
R1(config-subif)#ip address 10.0.12.8 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:2 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:12::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit

R1(config)#interface E1/1.1
R1(config-subif)#encapsulation dot1q 13
R1(config-subif)#vrf forwarding Special-Users
R1(config-subif)#ip address 10.0.113.8 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:3 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:113::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit

R1(config)#interface E1/1.2
R1(config-subif)#encapsulation dot1q 8
R1(config-subif)#vrf forwarding General-Users
R1(config-subif)#ip address 10.0.108.8 255.255.255.0
R1(config-subif)#ipv6 address fe80::1:4 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:108::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#

Encender la interface

R1(config)#interface E1/0
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface E1/1
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#exit

VRF en R 2

R2(config)#interface E1/0.1
R2(config-subif)#encapsulation dot1q 13
R2(config-subif)#vrf forwarding Special-Users
R2(config-subif)#ip address 10.0.12.7 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:1 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface E1/0.2
R2(config-subif)#encapsulation dot1q 8
R2(config-subif)#vrf forwarding General-Users
R2(config-subif)#ip address 10.0.12.7 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:2 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit

R2(config)#interface E1/1.1
R2(config-subif)#encapsulation dot1q 13
R2(config-subif)#vrf forwarding Special-Users
R2(config-subif)#ip address 10.0.23.7 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:3 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:23::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface E1/1.2

R2(config-subif)#encapsulation dot1q 8
R2(config-subif)#vrf forwarding General-Users
R2(config-subif)#ip address 10.0.23.7 255.255.255.0
R2(config-subif)#ipv6 address fe80::2:4 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:23::2/64
R2(config-subif)#no shutdown
R2(config-subif)#exit

Encender la interface
R2(config)#interface E1/0
R2(config-if)#no ip address
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface E1/1
R2(config-if)#no ip address
R2(config-if)#no shutdown
R2(config-if)#exit

VRF en R 3
R3(config)#interface E1/0.1
R3(config-subif)#encapsulation dot1q 13
R3(config-subif)#vrf forwarding Special-Users
R3(config-subif)#ip address 10.0.23.1 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:1 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64
R3(config-subif)#no shutdown
R3(config-subif)#exit

R3(config)#interface E1/0.2
R3(config-subif)#encapsulation dot1q 8
R3(config-subif)#vrf forwarding General-Users
R3(config-subif)#ip address 10.0.23.1 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:2 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64
R3(config-subif)#no shutdown
R3(config-subif)#exit

R3(config)#interface E1/1.1
R3(config-subif)#encapsulation dot1q 13

R3(config-subif)#vrf forwarding Special-Users
R3(config-subif)#ip address 10.0.213.1 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:3 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:213::1/64
R3(config-subif)#no shutdown
R3(config-subif)#exit

R3(config)#interface E1/1.2
R3(config-subif)#encapsulation dot1q 8
R3(config-subif)#vrf forward General-Users
R3(config-subif)#ip address 10.0.208.1 255.255.255.0
R3(config-subif)#ipv6 address fe80::3:4 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:208::1/64
R3(config-subif)#no shutdown
R3(config-subif)#exit

Encender la interface
R3(config)#interface E1/0
R3(config-if)#no ip address
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface E1/1
R3(config-if)#no ip address
R3(config-if)#no shutdown
R3(config-if)#exit

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

Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF. Special-Users y General-Users.
Para la comunicación entre Reuter se configura el protocolo IP Route, implementando una ruta estática que gestione el tráfico de red de R1 y R3 hacia R2,

Ruta estatica R 1
R1(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.7
R1(config)#ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.7
R1(config)#ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2
R1(config)#ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2

Ruta estatica *R 2*

R2(config)#ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.8
R2(config)#ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.1
R2(config)#Ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1
R2(config)#ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3
R2(config)#ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.8
R2(config)#ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.1
R2(config)#ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1
R2(config)#ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3
R2(config)#exit

Ruta estatica R 3

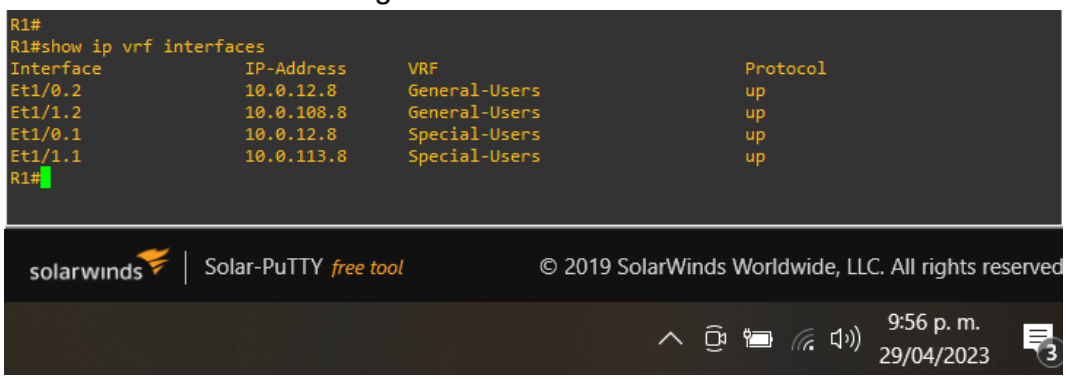
R3(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.7
R3(config)#ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.7
R3(config)#ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2
R3(config)#ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2
R3(config)#exit
R3#

2.4 Verifique la conectividad en cada VRF.

Verificación de las interfaces vrf

Desde R1 El comando *show ip VRF interfaces hacia R2*

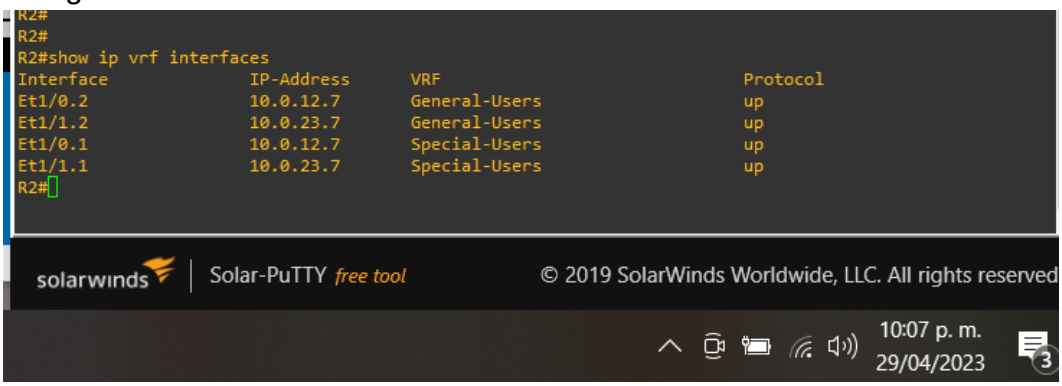
Figura 7 VRF Interface R1



Fuente: Elaboración propia

El comando *show ip VRF interfaces* en R1, muestra las subinterfaces, la ip address, y el nombre de las VRF.

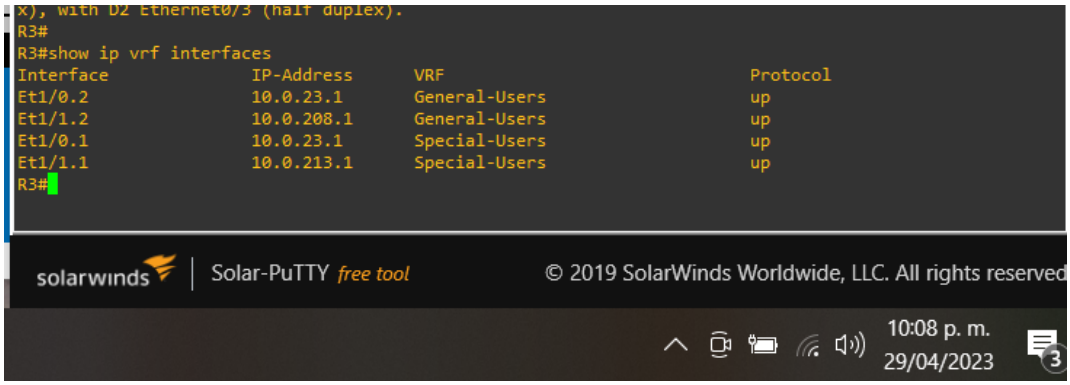
Figura 8 VRF Interface R2



Fuente: Elaboración propia

El comando *show ip VRF interfaces* en R2, muestra las subinterfaces, la ip address, y el nombre de las VRF.

Figura 9 VRF Interface R3



Fuente: Elaboración propia

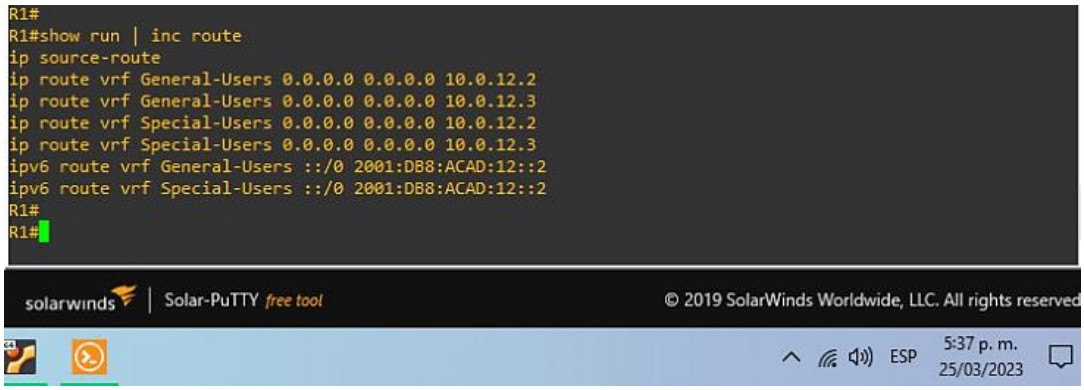
El comando *show ip VRF interfaces* en R3, muestra las subinterfaces, la ip address, y el nombre de las VRF.

Verificación del direccionamiento estático en todos los R1, R2 y R3
Verificar el direccionamiento estático en R1

Para visualizar la configuración de enrutamiento se utiliza el comando Show ip route

R1#show ip route

Figura 10 ruta estática en R1

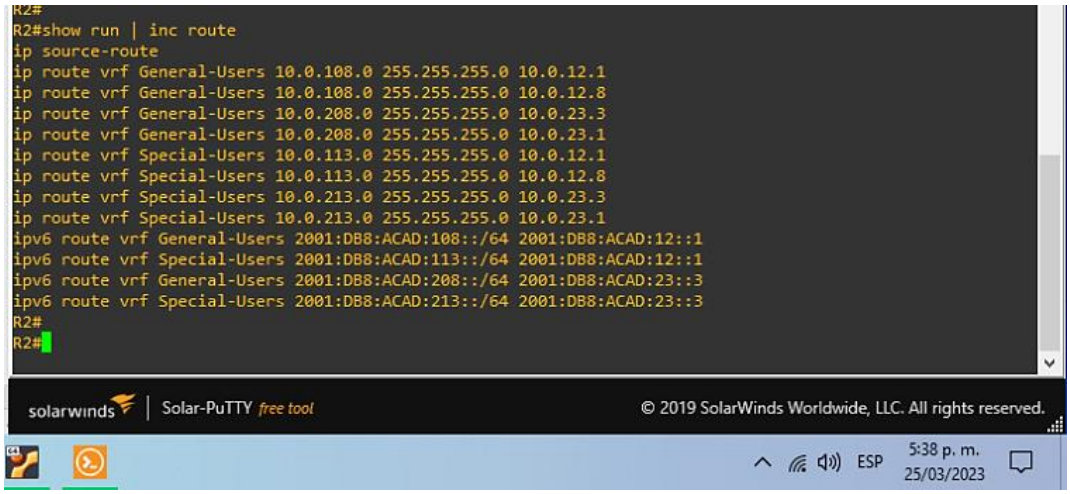


Fuente: Elaboración propia

El comando Show ip route muestra las vrf del Reuter, con una dirección ip de entrada y una dirección ip de salida

Verificación de la ruta estática en R2
R2#show ip route

Figura 11. Verificación de la ruta estático en R2



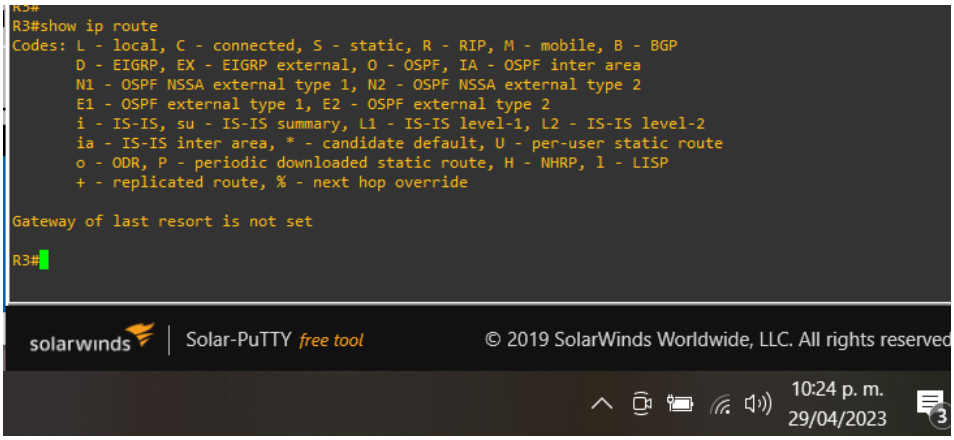
Fuente; Elaboración propia

El comando Show ip route muestra las vrf del Reuter, con una dirección ip de entrada y una dirección ip de salida, R2 muestra más interfaces al tener de vecinos al R1 y al R2.

Verificación de la ruta estática en R3

R3#show ip route

Figura 12. Verificación ruta estático en R3



Fuente: Elaboración propia

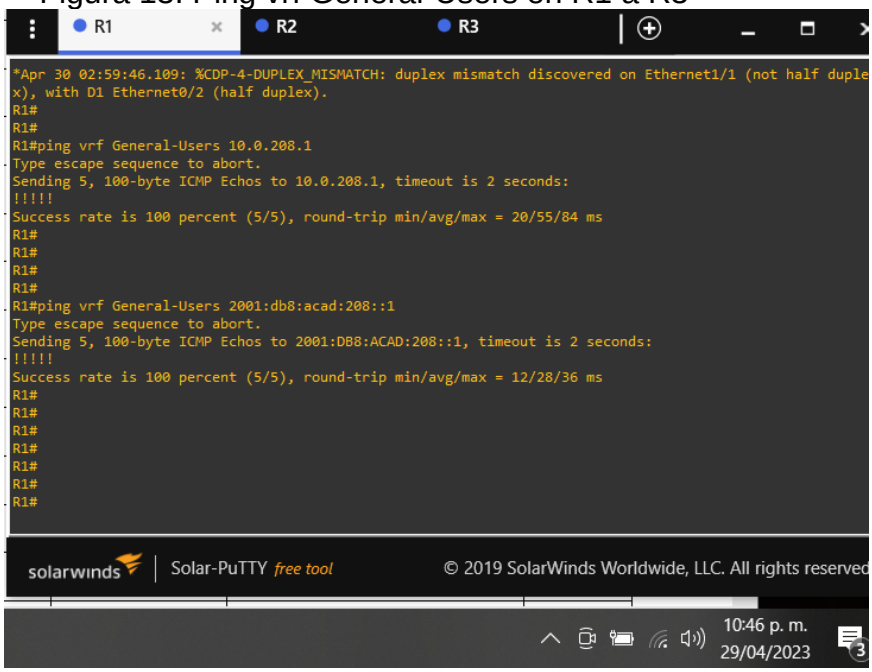
El comando Show ip route muestra las vrf del Reuter, con una dirección ip de entrada y una dirección ip de salida, tiene de vecino al R2 y a D2

Conectividad vrf General Users en R1 a R3

Ping vrf General-Users 10.0.208.1

Ping vrf General-Users 2001:db8:acad:208::1

Figura 13. Ping vrf General-Users en R1 a R3

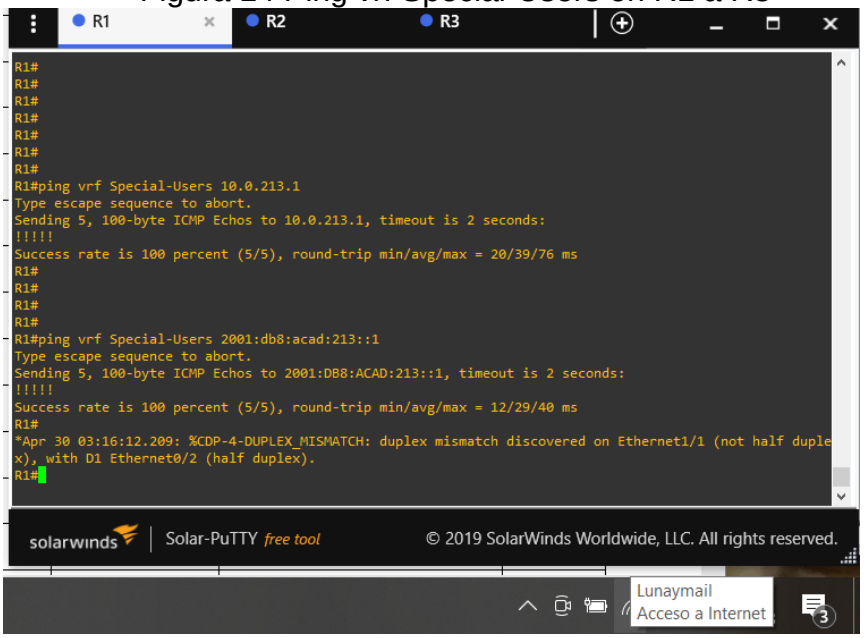


Fuente: Elaboración propia

Conectividad vrf Special-Users en R1 a R3

- Ping vrf Special-Users 10.0.213.1
- ping vrf Special-Users 2001:db8:acad:213::1

Figura 14 Ping vrf Special-Users en R1 a R3



Fuente: Elaboración propia

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 4. Tareas de configuración Capa 2

Task#	Task	Specification
3.1	On D1, D2, and A1, disable all interfaces.	**On D1 and D2, shutdown G1/0/1 to G1/0/24.On A1, shutdown F0/1 – F0/24, G0/1 – G0/2.**
3.2	On D1 and D2, configure the trunk links to R1 and R3.	**Configure and enable the G1/0/11 link as a trunklink.**
3.3	On D1 and A1, configure the EtherChannel.	**On D1, configure and enable:** • **Interface G1/0/5 and G1/0/6** • **Port Channel 1 using** **PAgPOn A1, configure** **enable:** • **Interface F0/1 and F0/2** • **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 G1/0/23 as an access port in VLAN 13 and enable Portfast.** • **On D2, configure interface G1/0/23 as an access port in VLAN 13 and enable Portfast.** • **On D2, configure interface G1/0/24 as an access port in VLAN 8 and enable Portfast.** • **On A1, configure interface F0/23 as an accessport in VLAN 8 and enable Portfast.**
3.5	**Verify PC to PC connectivity.**	**From PC1, verify IPv4 and IPv6 connectivity toPC2.** **From PC3, verify IPv4 and IPv6 connectivity toPC4.**

Fuente: Documento Prueba de Habilidades Practicas CCNP

Paso uno Tareas de configuración switches D1, D2, y A1,

Tabla 5 Configuracion en switch D1

Configuración Switch D1 Deshabilitar interface	
	Descripción
interface range e0/0-3, e1/0-3, e2/0-3,e3/0-3 shutdown exit	Selecciona el rango de Switch D1. Apaga las interfaces Se devuelve a un punto anterior.
Configura lo enlaces troncales	
interface e0/2	*Ingresa a la interfaz E0/2*
switchport trunk encapsulation dot1q *switchport mode trunk* *no shutdown* *exit*	*Activa el modo de encapsulación* *Configura puerto troncal encapsulación 802-1q* *Activa la interface* *se devuelve a un punto anterior,*
Configure EtherChannel	
interface range e0/0, e0/1 *switchport trunk encapsulation dot1q* *switchport mode trunk* *channel-group 1 mode desirableno* *shutdown* *exit*	*Ingresa a la interfaz seleccionada.* *Activa el modo trocal con encapsulación estándar 802.1Q.* *Activar interfaz modo troncal.* *Agrupa las interfaces modo activo ,* *Negociación de paquetes 802-1q.* *Se devuelve a un punto anterior*
Configuracion de puertos de acceso PC1 y PC2	
interface e0/3	*Ingresa a la interfaz E0/03*
switchport mode access *switchport access vlan 13* *spanning-tree portfast* *no shutdown*	*Activa el puerto de acceso.* *Asigna el puerto a la vlan 13* *Habilito puerto PortFast protección BPDU* *Habilita la interface*
exit	*Sale de la interface*

Fuente: Elaboración propia

Tabla 6 configuracion en switch D2

Configuración Switch D2	
Deshabilitar interface	
	Descripción
interface range e0/0-3, e1/0-3, e2/0-3,e3/0-3	Selecciona el rango de Switch D2.
shutdown	Apaga las interfaces
exit	Se devuelve a un punto anterior.
Configura lo enlaces troncales	
interface e0/3	*Ingresa a la interfaz E0/3*
switchport trunk encapsulation dot1q	*Activa el modo de encapsulación*
switchport mode trunk	*Configura puerto troncal encapsulación 802-1q*
no shutdown	*Activa la interface*
exit	*se devuelve a un punto anterior,*
Configuracion de puertos de acceso PC3 y PC4	
interface e0/2	*Ingresa a la interfaz E0/2.*
switchport mode access	*Activa el puerto de acceso.*
switchport access vlan 13	*Asigna el puerto a la vlan 13*
spanning-tree portfast	*Habilito puerto PortFast protección BPDU*
no shutdown	*Habilita la interface*
exit	*Sale de la interface*
interface e0/0	*Ingresa a la interfaz E0/0*
switchport mode access	*Activa el puerto de acceso.*
switchport access vlan 8	*Asigna el puerto a la vlan 8*
spanning-tree portfast	*Habilito puerto PortFast protección BPDU*
no shutdown	*Habilita la interface*
exit	*Sale de la interface*

Fuente: Elaboración propia

Tabla 7 configuracion en switch A1

Configuración Switch A1 Deshabilitar interface	
	Descripción
interface range e0/0-3, e1/0-3, e2/0-3,e3/0-3 shutdown exit	Selecciona el rango de Switch D1. Apaga las interfaces Se devuelve a un punto anterior.
interface e0/2	*Ingresa a la interfaz E0/2*
Configure EtherChannel	
interface range e0/0, e0/1 *switchport trunk encapsulation dot1q* *switchport mode trunk* *channel-group 1 mode desirableno* *shutdown* *exit*	*Ingresa a la interfaz seleccionada.* *Activa el modo trocal con encapsulación estándar 802.1Q.* *Activar interfaz modo troncal.* *Agrupa las interfaces modo activo , Negociación de paquetes 802-1q.* *Se devuelve a un punto anterior*
Configuracion de puertos de acceso PC1 y PC2	
interface e0/2	*Ingresa a la interfaz E0/0.*
switchport mode access *switchport access vlan 8* *spanning-tree portfast* *no shutdown*	*Activa el puerto de acceso.* *Asigna el puerto a la vlan 8* *Habilito puerto PortFast protección BPDU* *Habilita la interface*
exit	*Sale de la interface*

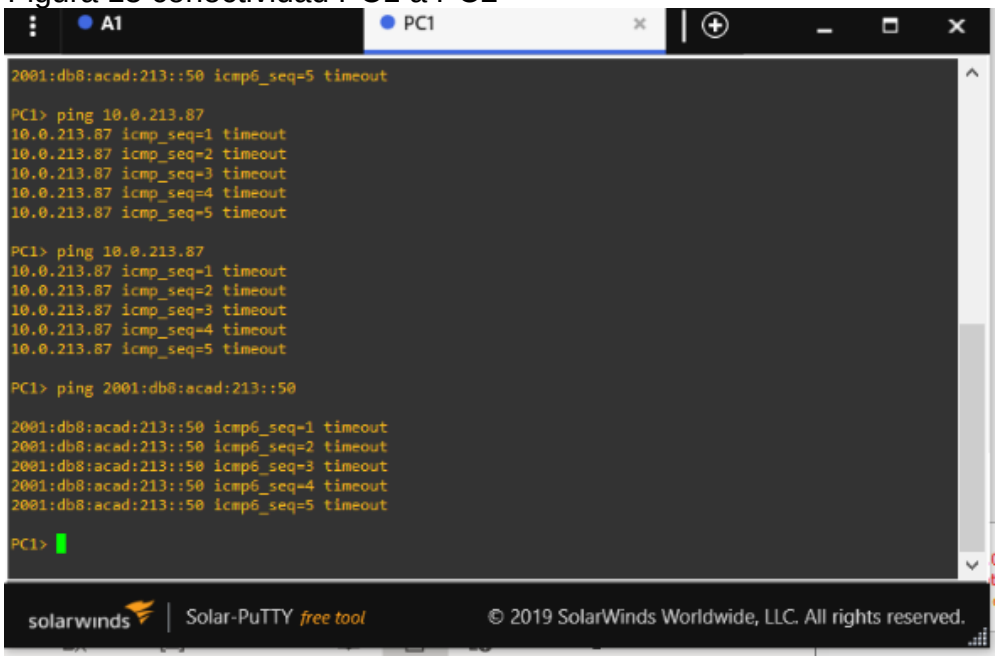
Fuente: Elaboración propia

Paso dos Verifique la conectividad de PC a PC

Para verificar la conectividad punto a punto se puede verificar por el commando ping seguido de la dirección ip.

De PC1, verifique la conectividad en IPv4 y IPv6 hacia PC2

Figura 15 conectividad PC1 a PC2



Fuente: Elaboración propia

De PC3, verifique la conectividad en IPv4 y IPv6 hacia PC4

El PC1 presenta una conectividad hacia el PC 2 con el commando ping 10.0.213.87 protocolo IPV4 y conecta al PC2 con el commando ping 2001:db8:acad:213::50 protocolo IPV6 conectando con el PC2

Figura 16 conectividad PC3 a PC4

Fuente: Elaboración propia

El PC3 se conecta con el PC4 por medio del comando ping 10.0.208.87 con una conectividad exitosa, y con el comando ping 201:db8:acad:208::50 direccionamiento IPV6 con una conectividad exitosa.

verificación de interfase trunk

para verificar las interfaces en modo trunk en el switch se utiliza el comando show interface trunk

mode trunk en D1

Figura 17 mode trunk en D1

Fuente: Elaboración propia

mode trunk en D2

Figura 18 mode trunk en D2

Fuente: Elaboración propia

mode trunk en A1

Figura 19 mode trunk en A1

Fuente: Elaboración propia

PARTE 4 CONFIGURE SECURITY

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

Tabla 8 configuración de Seguridad

Tarea #	Tarea	Especificación
4.1	En todos los dispositivos, proteja el modo EXE privilegiado.	Configure un secreto de habilitación de la siguiente manera: Tipo de algoritmo: SCRYPT Contraseña: nombreestudianteXYZ.
4.2	En todos los dispositivos, cree una cuenta de usuario local.	Configurar un usuario local: Nombre: admin Nivel de privilegio: 15 Tipo de algoritmo: SCRYPT Contraseña: nombrestudianteXYZ.
4.3	En todos los dispositivos, habilite AAA y habilite la autenticación AAA.	Habilite la autenticación AAA mediante la base de datos local en todas las líneas.

Fuente: Documento Prueba de Habilidades Practicas

4.1 Protección de todos los dispositivos

Configure una contraseña secretea
Algorithm type: SCRYPT
Password: Leidy871

Tabla 9 configuración de Seguridad en Switches y Reuters

Configuración de seguridad en SWITCH D1	
configure terminal	Ingresa al modo de configuración
enable algorithm-type SCRYPTsecret leidy871	Activa el cifrado Scrypt y activa una contraseña secreta
exit	Se devuelve a un estado anterior
Configuración de seguridad en SWITCH D2	
configure terminal	Ingresa al modo de configuración
enable algorithm-type SCRYPTsecret	Activa el cifrado Scrypt y activa una

leidy871	contraseña secreta
exit	Se devuelve a un estado anterior
Configuración de seguridad en SWITCH A1	
configure terminal	Ingresa al modo de configuración
enable algorithm-type SCRYPTsecret leidy871	Activa el cifrado Scrypt y activa una contraseña secreta
exit	Se devuelve a un estado anterior
Configuración de seguridad en ROUTER R1	
configure terminal	Ingresa al modo de configuración
enable secret leidy871	Activa una contraseña secreta
Service password-encryption	Activa el cifrado de contraseñas
exit	Se devuelve a un estado anterior
Configuración de seguridad en ROUTER R2	
configure terminal	Ingresa al modo de configuración
enable secret leidy871	Activa una contraseña secreta
Service password-encryption	Activa el cifrado de contraseñas
exit	Se devuelve a un estado anterior
Configuración de seguridad en ROUTER R2	
configure terminal	Ingresa al modo de configuración
enable secret leidy871	Activa una contraseña secreta
Service password-encryption	Activa el cifrado de contraseñas
exit	Se devuelve a un estado anterior

Fuente: Elaboración propia

4.2 Configurar un usuario local admin en todos los dispositivos

Configurar un usuario local:

- Nombre: admin
- Nivel de privilegio: 15
- Tipo de algoritmo: SCRYPT
- Contraseña: leidy871

Tabla 10 configuración de usuario local en Switches y Reuters

Creación de usuario y contraseña secreta en Router R1	
configure terminal	Ingresa al modo de configuración
Username admin privilege 15 secret leidy871secret leidy871	crea un usuario admin con ingreso de contraseña secreta
Username admin privilege 15 secret	Establece un nivel de privilegio 15

leidy871	
exit	Se devuelve a un estado anterior
Configuración de seguridad en ROUTER R2	
configure terminal	Ingresa al modo de configuración
Username admin privilege 15 secret leidy871secret leidy871	crea un usuario admin con ingreso de contraseña secreta
Username admin privilege 15 secret leidy871	Establece un nivel de privilegio 15
exit	Se devuelve a un estado anterior
Configuración de seguridad en ROUTER R3	
configure terminal	Ingresa al modo de configuración
Username admin privilege 15 secret leidy871secret leidy871	crea un usuario admin con ingreso de contraseña secreta
Username admin privilege 15 secret leidy871	Establece un nivel de privilegio 15
exit	Se devuelve a un estado anterior
Configuración de seguridad en SWITCH D1	
configure terminal	Ingresa al modo de configuración
Username admin privilege 15 secret leidy871	Establece un nivel de privilegio 15 encripta la contraseña secreta
exit	Se devuelve a un estado anterior
Configuración de seguridad en SWITCHC D2	
configure terminal	Ingresa al modo de configuración
Username admin privilege 15 secret leidy871	Establece un nivel de privilegio 15 encripta la contraseña secreta
exit	Se devuelve a un estado anterior
Configuración de seguridad en SWITCHC A1	
configure terminal	Ingresa al modo de configuración
Username admin privilege 15 secret leidy871	Establece un nivel de privilegio 15 encripta la contraseña secreta
exit	Se devuelve a un estado anterior

Fuente: Elaboración propia

4.3 habilite AAA y habilite la autenticación AAA en todos los dispositivos

Se configura Habilitando la autenticación AAA por medio de la base de datos local en cada dispositivo

De la siguiente manera

Tabla 11 Habilitación de AAA en Reuters y Switches

Creación de usuario y contraseña secreta en Router R1	
configure terminal	Ingresa al modo de configuración
aaa new-model	Activa seguridad protocolo de autenticación aaa
aaa authentication login default local	Activa autenticación de usuario local para inicio de sesión.
username admin password leidy871	Le proporciona una contraseña a usuario local
exit	Se devuelve a un estado anterior
Configuración AAA en ROUTER R2	
configure terminal	Ingresa al modo de configuración
aaa new-model	Activa seguridad protocolo de autenticación aaa
aaa authentication login default local	Activa autenticación de usuario local para inicio de sesión.
username admin password leidy871	Le proporciona una contraseña a usuario local
exit	Se devuelve a un estado anterior
Configuración AAA en ROUTER R3	
configure terminal	Ingresa al modo de configuración
aaa new-model	Activa seguridad protocolo de autenticación aaa
aaa authentication login default local	Activa autenticación de usuario local para inicio de sesión.
username admin password leidy871	Le proporciona una contraseña a usuario local
exit	Se devuelve a un estado anterior
Configuración AAA en Switch D1	
configure terminal	Ingresa al modo de configuración
aaa new-model	Activa seguridad protocolo de autenticación aaa
aaa authentication login default local	Activa autenticación de usuario local

	para inicio de sesión.
username admin password leidy871	Le proporciona una contraseña a usuario local
exit	Se devuelve a un estado anterior
Configuración AAA en Switch D2	
configure terminal	Ingresa al modo de configuración
aaa new-model	Activa seguridad protocolo de autenticación aaa
aaa authentication login default local	Activa autenticación de usuario local para inicio de sesión.
username admin password leidy871	Le proporciona una contraseña a usuario local
exit	Se devuelve a un estado anterior
Configuración AAA en SwitchA1	
configure terminal	Ingresa al modo de configuración
aaa new-model	Activa seguridad protocolo de autenticación aaa
aaa authentication login default local	Activa autenticación de usuario local para inicio de sesión.
username admin password leidy871	Le proporciona una contraseña a usuario local
exit	Se devuelve a un estado anterior

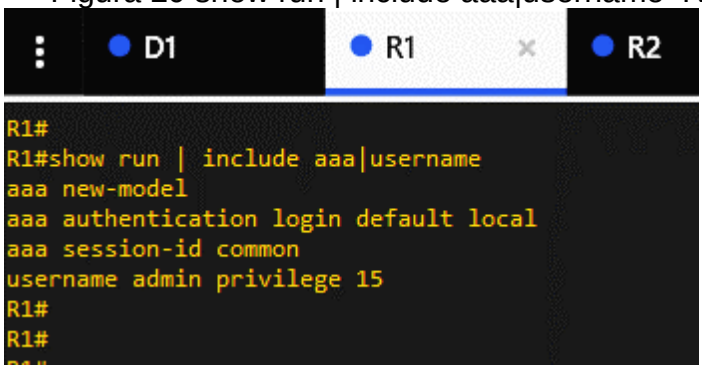
Fuente: Elaboración propia

4.2 verificación de usuario local y configuración de seguridad AAA

En seguridad de dispositivo Reuter R1 el protocolo AAA corresponde a sus iniciales de authentication, authorization y accouting.

Verificar show run | include aaa|username en R1

Figura 20 show run | include aaa|username R1



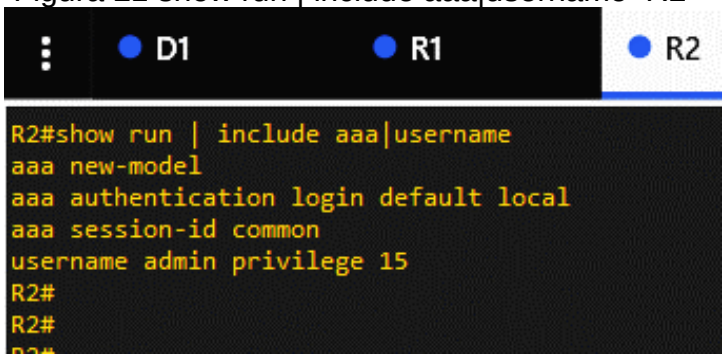
Fuente: Elaboración propia

El comando show run | include aaa|username, en R1 permite visualizar el protocolo de autenticación aaa y el usuario local, admin con un privilegio 15 que significa que le da un acceso a modo privilegiado completo

Verificación de configuración de seguridad aaa en R2,

Verificar la configuración de seguridad con el comando show run | include aaa|username.

Figura 21 show run | include aaa|username R2



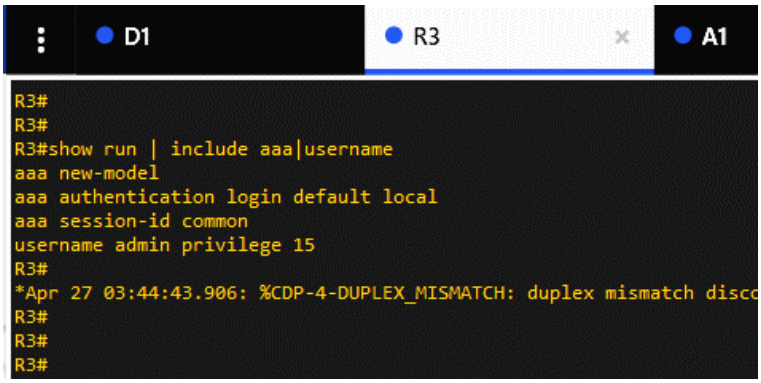
Fuente: Elaboración propia

El comando show run | include aaa|username, en R2 permite visualizar el protocolo de autenticación aaa y el usuario local, admin con un privilegio 15 que significa que le da un acceso a modo privilegiado completo

Verificación de configuración de seguridad aaa en R3

Verificar la configuración de seguridad con el comando show run | include aaa|username.

Figura 22 show run | include aaa|username R3



Fuente: Elaboración propia

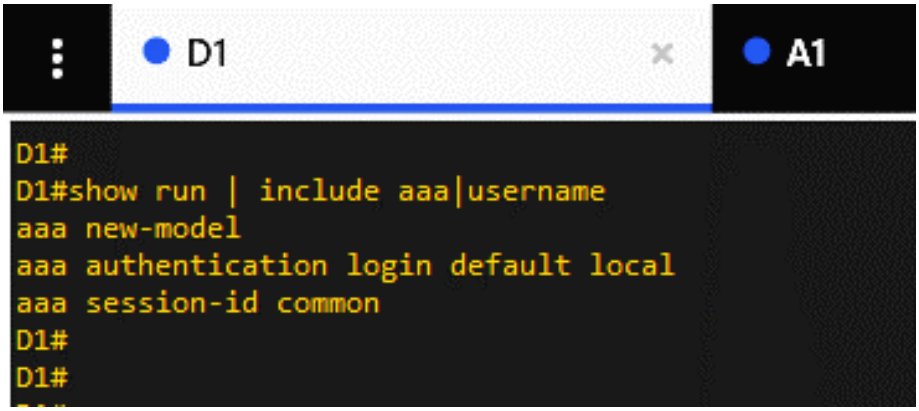
El comando show run | include aaa|username, en R3 permite visualizar el

protocolo de autenticación aaa y el usuario local, admin con un privilegio 15 que significa que le da un acceso a modo privilegiado completo

Verificación de configuración de seguridad aaa en D1

Verificar la configuración de seguridad con el comando show run | include aaa|username.

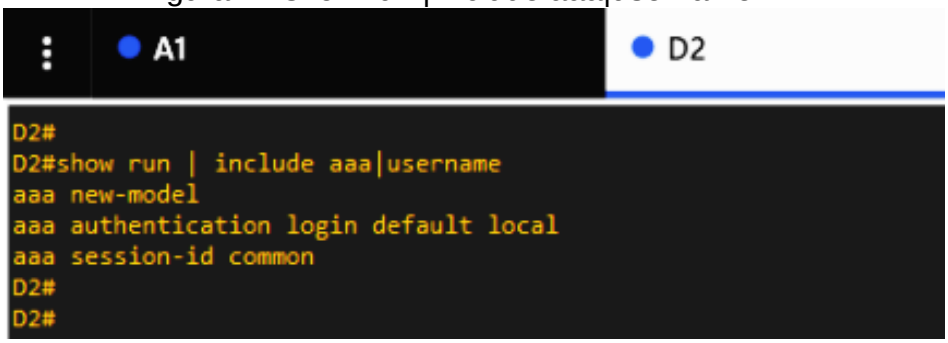
Figura 23 show run | include aaa|username D1



Verificación de configuración de seguridad aaa en D2

Verificar la configuración de seguridad con el comando show run | include aaa|username.

Figura 24 show run | include aaa|username D2



Fuente: Elaboración propia

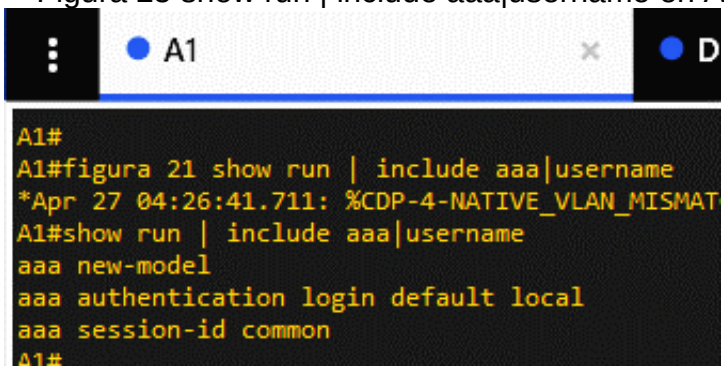
El comando show run | include aaa|username, en D2 permite visualizar el protocolo de autenticación aaa y el usuario local, admin con un privilegio 15 que significa que le da un acceso a modo privilegiado completo

Verificación de configuración de seguridad aaa en A1

Para verificar el nombre de usuario y la autenticación AAA, se utiliza el comando

show run | include aaa|username.

Figura 25 show run | include aaa|username en A1



Fuente: Elaboración propia

El comando show run | include aaa|username, en A1 permite visualizar el protocolo de autenticación aaa y el usuario local

CONCLUSIONES

La prueba de habilidades es la evaluación final donde se aplican los conocimientos adquiridos en el periodo de formación académica donde se da solución a un escenario propuesto, el diplomado de profundización CCNP explora las capacidades y competencias de un profesional en el área de las telecomunicaciones y la electrónica, y en la solución de problemas en redes de datos.

En la desarrollo de la configuración de cada uno de los pasos de es fundamental en ir verificando la correcta configuración de cada dispositivo y de cada paso, en las documentación de CISCO dispone de una gran cantidad de librerías en donde exponen comandos como ping, show ip vrf interfaces, Show run | include aaa|username, son algunas líneas de comando que son útiles para verificar la configuración de un dispositivo, en este trabajo se visualizan las imágenes con el uso de estos comandos para una mejor comprensión en la aplicación de la configuración en la implementación de la red.

El escenario propuesto documenta la solución paso a paso de las cuatro partes en que está dividido la implementación de la red, configuración básica de los dispositivos, creación de VRF de General-Users y Special-Users, configuración de capa dos y por último aplicación de seguridad en la red.

REFERENCIAS BIBLIOGRAFICAS

EDGEWORTH, Bladley., GARZA RIOS Ramiro, B., GOOLEY, J., HUCABY, David. CISCO Press (Ed). Enterprise Network Architecture. CCNP and CCIE Enterprise Core ENCOR 350-401 [En línea]. 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bladley., GARZA RIOS Ramiro, B., GOOLEY Jasson., HUCABY, David., Hucaby, D. CISCO Press (Ed). Foundational Network Programmability Concepts**.** CCNP and CCIE Enterprise Core ENCOR 350-401. [En línea]. 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bladley., GARZA RIOS Ramiro, B., GOOLEY, J., HUCABY, David CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401. [En línea]. 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bladley., GARZA RIOS Ramiro, B., GOOLEY, J., HUCABY, David CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. [En línea]. 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bladley., GARZA RIOS Ramiro, B., GOOLEY, J., HUCABY, David CISCO Press (Ed). Virtualization. CCNP and CCIE Enterprise Core ENCOR 350-401[En línea]. 2020. Disponible en . https://1drv.ms/b/s!AAIGg5JUgUBthk8