DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP
PRUEBA DE HABILIDADES PRACTICA

EDINSON ALBERTO NÚÑEZ ZÚÑIGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
CARTAGENA
2023

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP
PRUEBA DE HABILIDADES PRACTICA

EDINSON ALBERTO NÚÑEZ ZÚÑIGA

Diplomado de opción de grado presentado para optar el
Título de INGENIERO ELECTRÓNICO

DIRECTOR:
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
CARTAGENA
2023

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Cartagena, 14 de mayo de 2023

CONTENIDO

Lista de tablas

Lista de figuras

RESUMEN

En este trabajo de grado se desarrollarán actividades que demuestran las habilidades practicas adquiridas durante la realización del diplomado de profundización CISCO CCNP, en donde se abordaran temas como estructuración de redes conmutadas mediante el uso del protocolo STP y la configuración de VLANs, implementar soluciones de redes jerárquicas convergentes, efectuando configuraciones básicas y avanzadas de protocolos de enrutamiento.

La actividad se desenvuelve en un entorno simulado por medio del software GNS3, en el cual se plantea un escenario practico, en donde se deben configurar dispositivos de red tales como routers, switches y computadores, para que de este modo se pueda configurar una red dividida en dos subredes. Por otra parte, se establecerán niveles de seguridad de diferentes tipos.

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

ABSTRACT

In this degree work, activities will be developed that demonstrate the practical skills acquired during the completion of the CISCO CCNP in-depth diploma, where topics such as structuring of switched networks will be addressed through the use of the STP protocol and the configuration of VLANs, implementing network solutions convergent hierarchical networks, carrying out basic and advanced configurations of routing protocols.

The activity is carried out in a simulated environment by means of the GNS3 software, in which a practical scenario is proposed, where network devices such as routers, switches and computers must be configured, so that in this way a divided network can be configured. in two subnets. On the other hand, security levels of different types will be established.

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

INTRODUCCIÓN

Para llevar a cabo la implementación de tanto de una red LAN como una red WAN, es necesario establecer ciertos protocolos de enrutamiento, para garantizar la comunicación efectiva entre los diferentes dispositivos.

Actualmente las redes informáticas usan el protocolo TCP/IP basado en el modelo OSI, el cual consta de 7 capas: Physical (layer 1), Data link (layer 2), Network (layer 3), Transport (layer 4), session (layer 5), Presentation (layer 6) y Aplication (layer 7). Cada una de ellas tiene una función dentro de la comunicación.

En las redes de computadores se usa un método para segmentar las redes en una organización, de acuerdo a una jerarquía, este método es mediante el uso de VLAN o LAN virtual, esta consiste en crear redes virtuales dentro de una red física y así establecer comunicaciones entre dispositivos específicos sin sobrecargar toda la red.

Otro elemento muy importante es el uso y definición de rutas de enlace, para esto se usa el protocolo STP (spanning tree protocol), con esto se garantiza una conexión más confiable, ya que se usan múltiples enlaces entre dispositivos y en caso de que falle una línea física, se envían los datos por otra ruta hacia el mismo receptor.

Para una mayor seguridad en la conexión se utiliza el enrutamiento estático, en donde se le asigna una dirección IP a cada dispositivo y al mismo tiempo con el uso de VRF (virtual routing forwarding), que garantiza que dentro de una red existan tablas de enrutamiento diferentes en una misma red, para evitar que una sección se comunique con otra, y así mantener la red seccionada.

DESARROLLO DE LA ACTIVIDAD
Escenario Propuesto

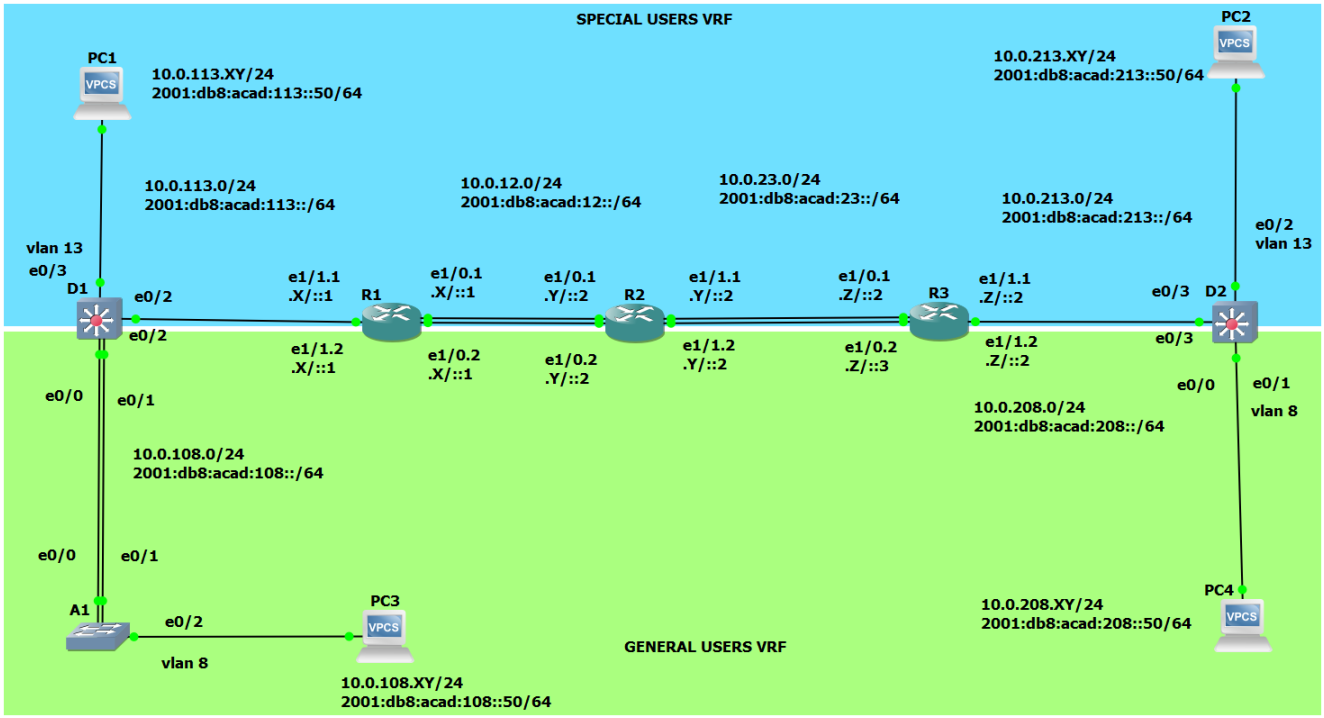

Figura 1. Topología de red ejemplo

Tabla 1. Direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.7/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.7/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.7/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.7/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.9/24	2001:db8:acad:12::2/64	fe80::1:1
	E1/0.2	10.0.12.9/24	2001:db8:acad:12::2/64	fe80::1:2
	E1/1.1	10.0.23.9/24	2001:db8:acad:23::2/64	fe80::1:3
	E1/1.2	10.0.23.9/24	2001:db8:acad:23::2/64	fe80::1:4
R3	E1/0.1	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::1:1

	E1/0.2	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::1:2
	E1/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::1:3
	E1/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::1:4
PC1	NIC	10.0.113.79/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.79/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.79/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.79/24	2001:db8:acad:208::50/64	EUI-64

Nota: las letras “X, Y, Z” corresponden a los últimos tres dígitos de su número de cédula. CC: 1129571791, entonces X representa 7, Y representa 9, Z representa 1

Recursos requeridos

• 3 Routers (Cisco 7200).

• 3 Switches (Cisco IOU L2).

• 4 PCs (Use the GNS3’s VPCS)

• Después de la configuración de los dispositivos en GNS, configurar los slots de la red de cada SW de la siguiente manera:

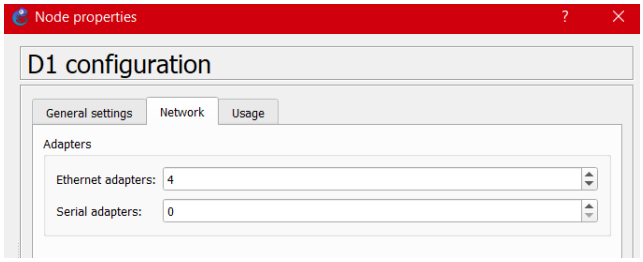

Figura 2. Configuración de D1

Y en los routers así:

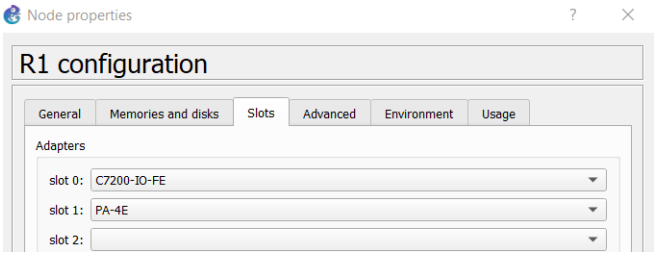

Figura 3. Configuración de R1

1. construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz. En esta Parte, configurará la topología de la red y configurará los ajustes básicos.

1.1 Cableado de la red

Se conectaron los dispositivos como se muestra en el diagrama de topología y se cablearon según fue necesario.

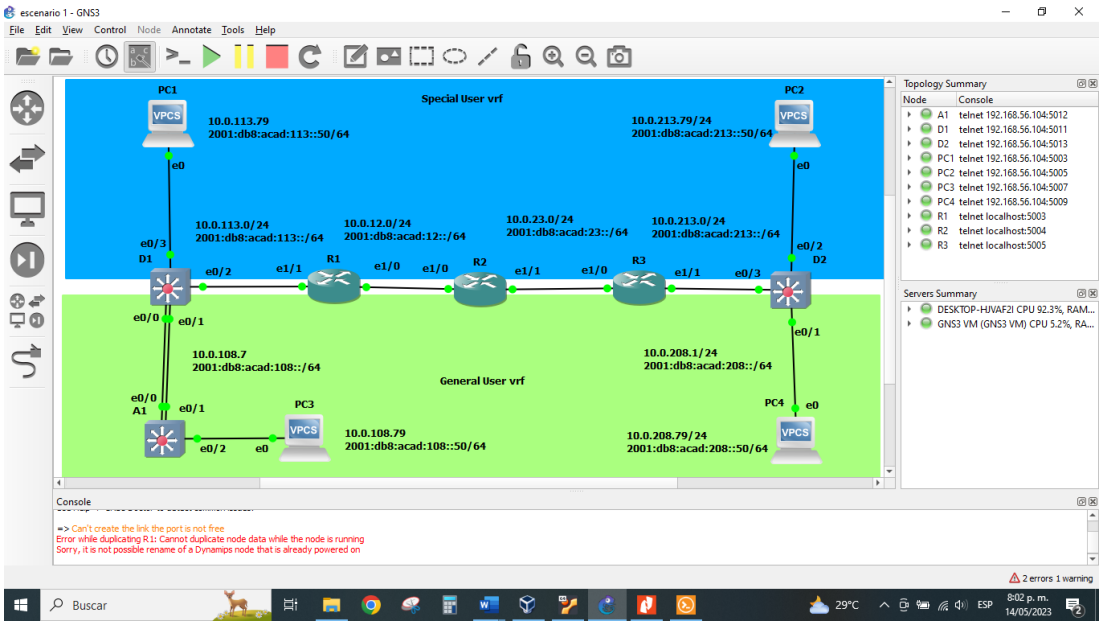

Figura 4. Topología realizada

1.2 Configure los ajustes básicos para cada dispositivo.

a. Se Ingreso al modo de configuración global en cada uno de los dispositivos y se aplicó la configuración básica. Las configuraciones se llevaron a cabo por medio de los comandos mostrados a continuación.

Router R1

```
Config t
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
exit
copy running-config startup-config

Router R2

Config t
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
exit
copy running-config startup-config

Router R3

Config t
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
exit
copy running-config startup-config

Switch D1

Enable
Config t
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
exit
copy running-config startup-config

Switch D2

Enable
Config t
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
exit
copy running-config startup-config

Switch A1

Enable
Config t
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
exit
copy running-config startup-config

b. Se guardo las configuraciones en cada uno de los dispositivos.
Se uso el comando:
“Copy running-config startup-config” en cada router y switch, para guardar dichas configuraciones.

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

Se llevo a cabo la configuración de los PCs con los siguientes comandos:

En PC1
set pcname pc1
ip 10.0.113.79/24 10.0.113.7
ip 2001:db8:acad:113::50/64
show

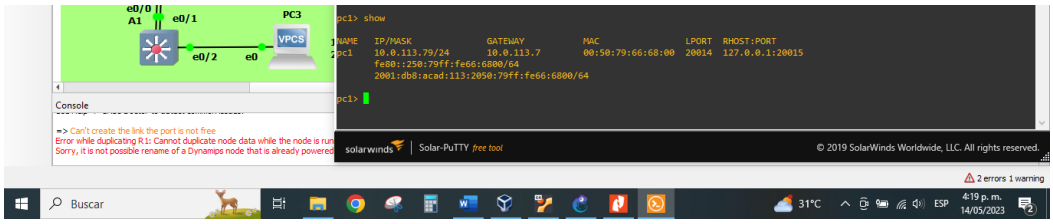

Figura 5. Configuración de PC1

En PC2
set pcname pc2
ip 10.0.213.79/24 10.0.213.1
ip 2001:db8:acad:213::50/64
show

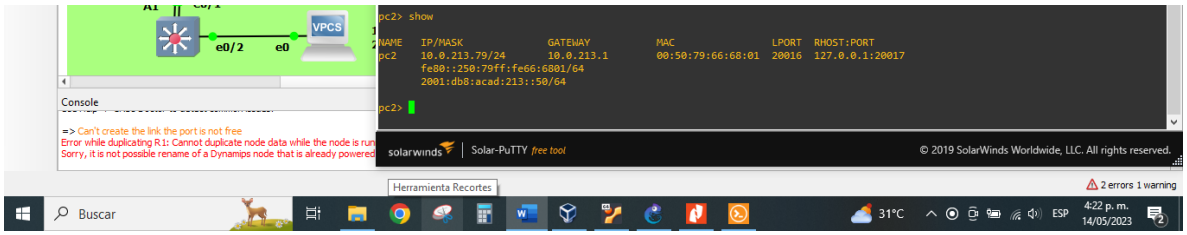

Figura 6. Configuración de PC2

En PC3

set pcname pc3
ip 10.0.108.79/24 10.0.108.7
ip 2001:db8:acad:108::50/64
show

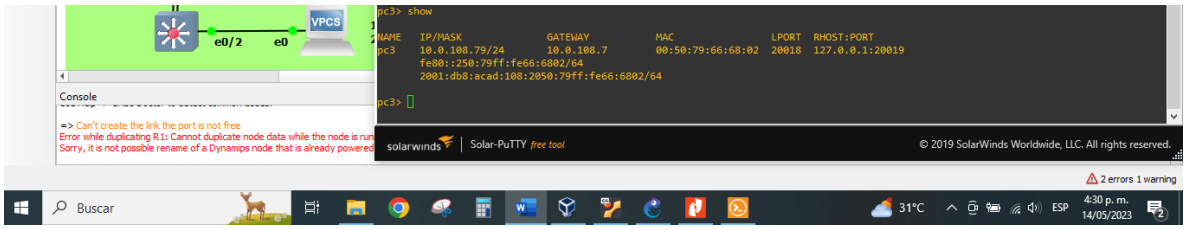

Figura 7. Configuración de PC3

En PC4

set pcname pc4
ip 10.0.208.79/24 10.0.208.1
ip 2001:db8:acad:208::50/64
show

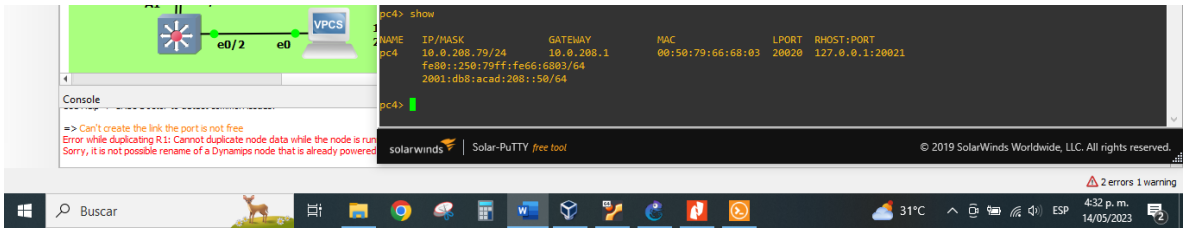

Figura 8. Configuración de PC4

En cada uno de los pc, se ejecuto el comando “save” para guardar la configuración.

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 ping a R3 en cada VRF. Sus tareas de configuración son las siguientes:

Tabla 2. Configuración vrf

Task#	Task	Specification
2.1	On R1, R2, and R3, configure VRF-Lite VRFs as shown in the topology diagram.	Configure two VRFs: • General-Users • Special-Users The VRFs must support IPv4 and IPv6.
2.2	On R1, R2, and R3, configure IPv4 and IPv6 interfaces on each VRF as detailed in the addressing table above.	All routers will use Router-On-A-Stick on their e1/1.x interfaces to support separation of the VRFs. Sub-interface 1: • In the Special Users VRF • Use dot1q encapsulation • IPv4 and IPv6 GUA and link-local addresses • Enable the interfaces Sub-interface 2: • In the General Users VRF • Use dot1q encapsulation • IPv4 and IPv6 GUA and link-local addresses • Enable the interfaces
2.3	On R1 and R3, configure default static routes pointing to R2.	Configure VRF static routes for both IPv4 and IPv6 in both VRFs.
2.4	Verify connectivity in each VRF.	From R1, verify connectivity to R3: • ping vrf General-Users 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

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

Siguiendo las tareas y especificaciones de la tabla anterior, se digitaron los siguientes comandos en cada uno de los diferentes dispositivos.

Router 1

```
config t
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
```

```
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
exit
exit
copy running-config startup-config
```

Router 2

```
config t
ipv6 unicast-routing
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
exit
copy running-config startup-config
```

Router 3

```
config t
ipv6 unicast-routing
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
exit
exit
copy running-config startup-config
```

en esta sección se llevó a cabo la configuración de VRF, en cada dispositivo, tanto para el direccionamiento IPV4 como para IPV6

2.2. En R1, R2, y R3 se configura IPv4 y Ipv6 en cada VRF, como lo solicita la tabla de enrutamiento.

Router 1

```
Config t
int E1/0
no shutdown
int E1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.12.7 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
ipv6 address fe80::1:1 link-local
no shutdown
exit
int E1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.12.7 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
ipv6 address fe80::1:2 link-local
no shutdown
exit
int E1/1
no shutdown
int E1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.113.7 255.255.255.0
ipv6 address 2001:db8:acad:113::1/64
ipv6 address fe80::1:3 link-local
no shutdown
exit
int E1/1.2
encapsulation dot1Q 8
vrf forward General-Users
ip address 10.0.108.7 255.255.255.0
ipv6 address 2001:db8:acad:108::1/64
ipv6 address fe80::1:4 link-local
no shutdown
exit
exit
copy running-config startup-config
```

luego verificamos la configuración de vrf por medio del siguiente comando

show ip vrf interfaces

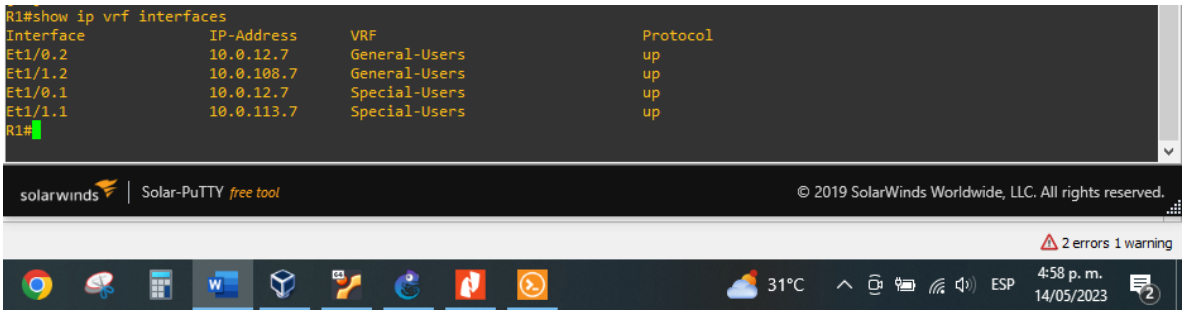

Figura 9. Verificación de vrf en R1

Router 2

Config t
int E1/0
no shutdown
int E1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.12.9 255.255.255.0
ipv6 address 2001:db8:acad:12::2/64
ipv6 address fe80::2:1 link-local
no shutdown
exit
int E1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.12.9 255.255.255.0
ipv6 address 2001:db8: acad:12::2/64
ipv6 address fe80::2:2 link-local
no shutdown
exit
int E1/1
no shutdown
int E1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.23.9 255.255.255.0
ipv6 address 2001:db8:acad:23::2/64
ipv6 address fe80::2:3 link-local
no shutdown

exit
int E1/1.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.23.9 255.255.255.0
ipv6 address 2001:db8:acad:23::2/64
ipv6 address fe80::2:4 link-local
no shutdown
exit
exit
copy running-config startup-config

luego verificamos la configuración de vrf por medio del siguiente comando

show ip vrf interfaces

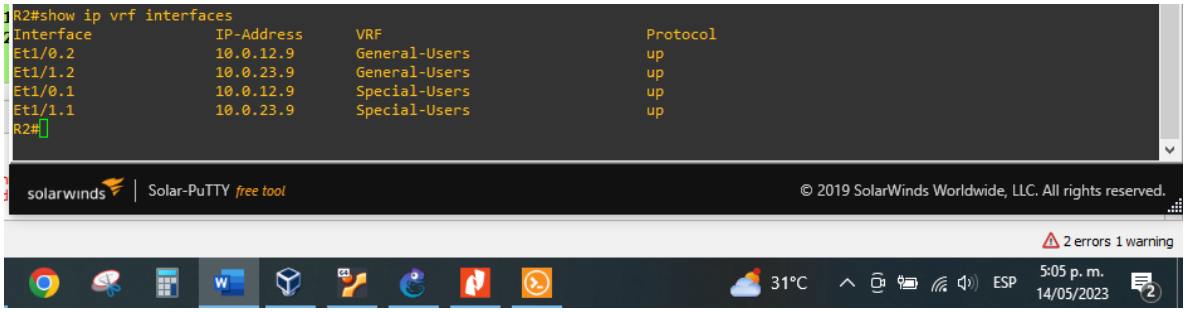

Figura 10. Verificación de vrf en R2

Router 3
Config t
int E1/0
no shutdown
int E1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.23.1 255.255.255.0
ipv6 address 2001:db8:acad:23::3/64
ipv6 address fe80::3:1 link-local
no shutdown
exit
int E1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.23.1 255.255.255.0

ipv6 address 2001:db8:acad:23::3/64
ipv6 address fe80::3:2 link-local
no shutdown
exit
int E1/1
no shutdown
interface E1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.213.1 255.255.255.0
ipv6 address 2001:db8:acad:213::1/64
ipv6 address fe80::3:3 link-local
no shutdown
exit
int E1/1.2
encapsulation dot1Q 8
vrf forward General-Users
ip address 10.0.208.1 255.255.255.0
ipv6 address 2001:db8:acad:208::1/64
ipv6 address fe80::3:4 link-local
no shutdown
exit
exit
copy running-config startup-config

luego verificamos la configuración de vrf por medio del siguiente comando
show ip vrf interfaces

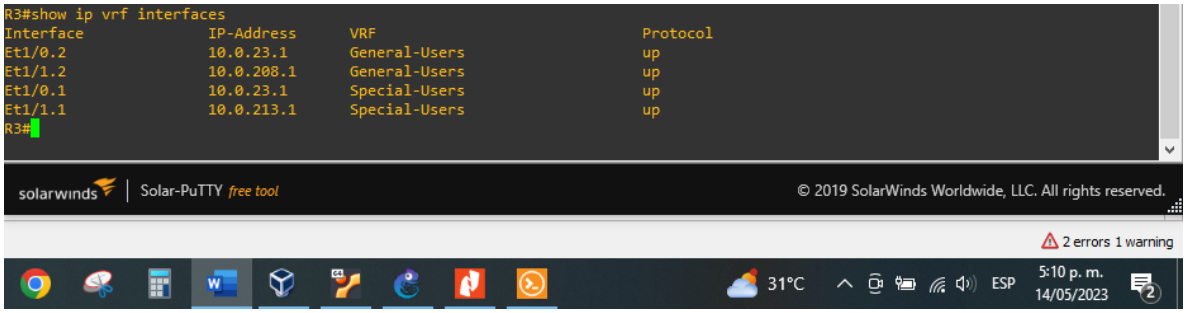

Figura 11. Verificación de vrf en R3

En este punto se realizó la creación de subredes dentro de los enlaces físicos existentes para cada dispositivo de red y se asignaron las direcciones IP correspondientes a cada VRF.

2.3. En R1 y R3, configure enrutamiento estático predeterminadas que apuntan a R2

Se digitaron los comandos correspondientes para configurar el enrutamiento estático.

Router 1
config t
ip route vrf Special-Users 10.0.23.0 255.255.255.0 10.0.12.9
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.12.9
ipv6 route vrf Special-Users 2001:db8:acad:23::2/64 2001:db8:acad:12::2
ipv6 route vrf Special-Users 2001:db8:acad:213::1/64 2001:db8:acad:12::2
ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.9
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.9
ipv6 route vrf General-Users 2001:db8:acad:23::2/64 2001:db8:acad:12::2
ipv6 route vrf General-Users 2001:db8: acad:208::1/64 2001:db8:acad:12::2
exit
copy running-config startup-config

para verificar la configuración del enrutamiento estático en R1, se digito el siguiente comando

show run | inc route

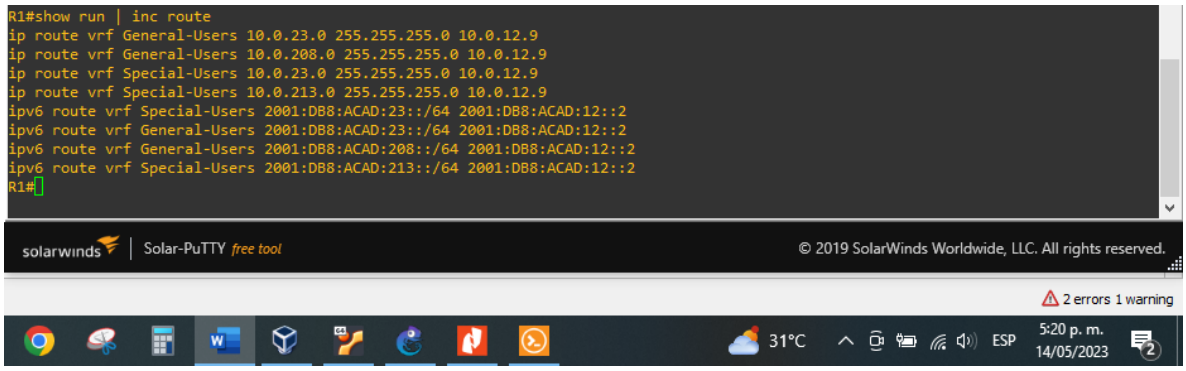

Figura 12. Enrutamiento estatico en R1

Router 2
config t
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.7
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.1
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.7
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.1
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
ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1

ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3
exit
copy running-config startup-config

para verificar la configuración del enrutamiento estatico en R2, se digito el siguiente comando

show run | inc route

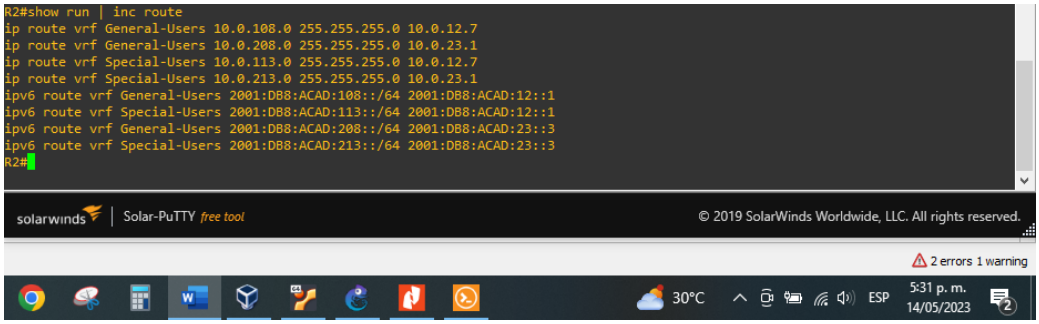

Figura 13. Enrutamiento estatico en R2

Router 3
config t
ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.9
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.9
ip route vrf Special-Users 10.0.12.0 255.255.255.0 10.0.23.9
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.23.9
ipv6 route vrf General-Users 2001:db8:acad:12::/64 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users 2001:db8:acad:12::/64 2001:DB8:ACAD:23::2
ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:DB8:ACAD:23::2
exit
copy running-config startup-config

para verificar la configuración del enrutamiento estatico en R2, se digito el siguiente comando

show run | inc route

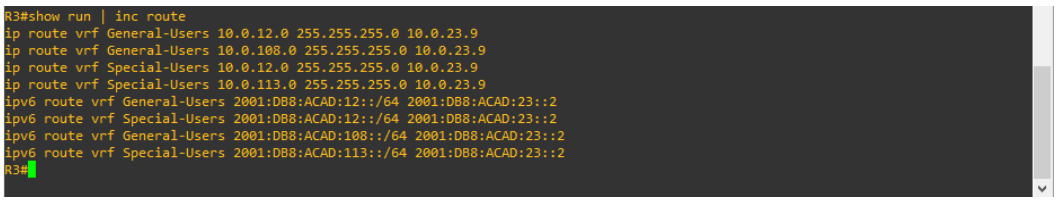

Figura 14. Enrutamiento estatico en R3

2.4. verificar conectividad en cada VRF

desde R1, se verifico la conectividad a R3, por medio de los siguientes comandos:

• 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

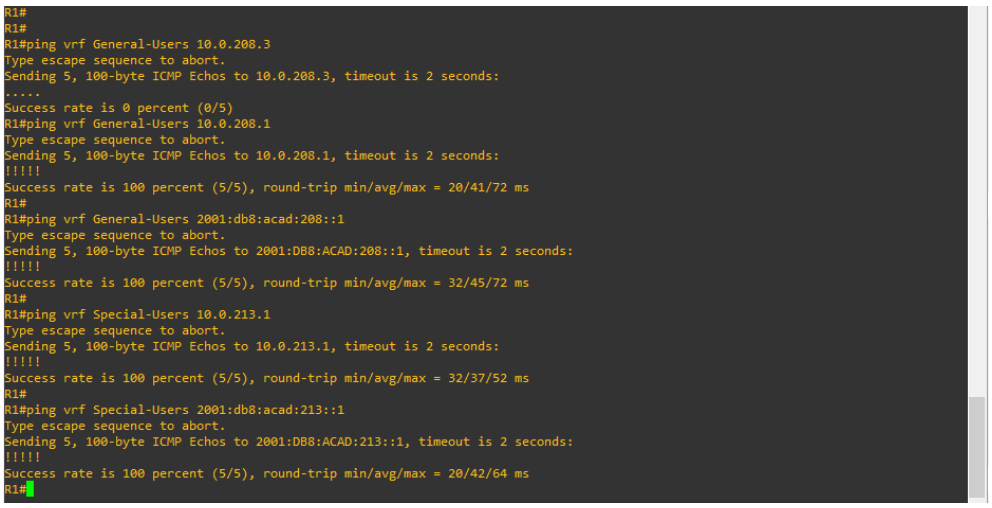

Figura 15. Conectividad en cada vrf

Obteniendo como resultado una comunicación exitosa en cada caso, tanto por ipv4 como por ipv6

Al realizar la prueba de comunicaciones entre los dispositivos, evidenciamos que el router 1 tiene restringida la comunicación con PC2 y PC4

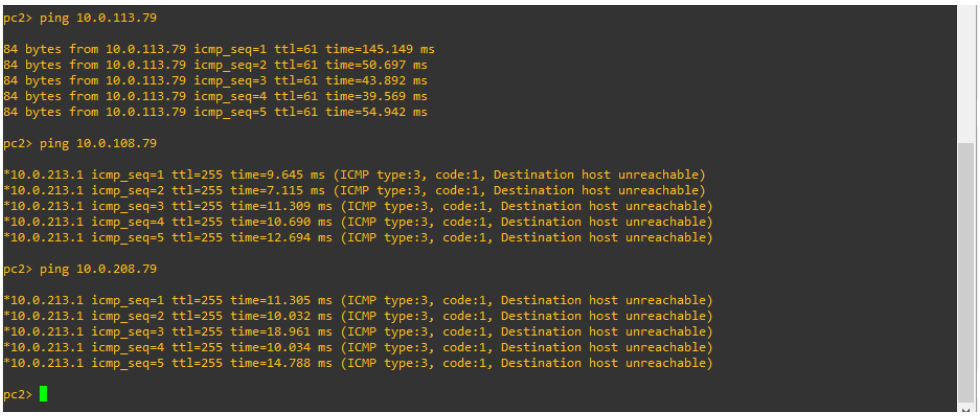

Figura 16. Comunicación entre R1 con PC3 y PC4

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 3. Configuración de 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.

3.1 En D1, D2 y A1 desactivar todas las interfaces

Procedemos a desactivar todas las interfaces de los switch D1, D2 y A1 con los siguientes comandos:

D1
enable
config ter
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
shutdown
exit
exit

D2
enable
config ter
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
shutdown
exit
exit

A1
enable
config ter
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
shutdown
exit
exit

3.2 En D1 y D2, configure el enlace troncal a R1 y R3

Se realizo la configuración del modo troncal para los switch D1 y S2 con los siguientes comandos

D1
config ter
interface e0/2
switchport trunk encapsulation dot1Q
switchport mode trunk
switchport trunk allowed Vlan 13,8
no shutdown
exit
exit
copy running-config startup-config

por medio del comando show interfaces trunk, podemos verificar el modo troncal en el switch D1

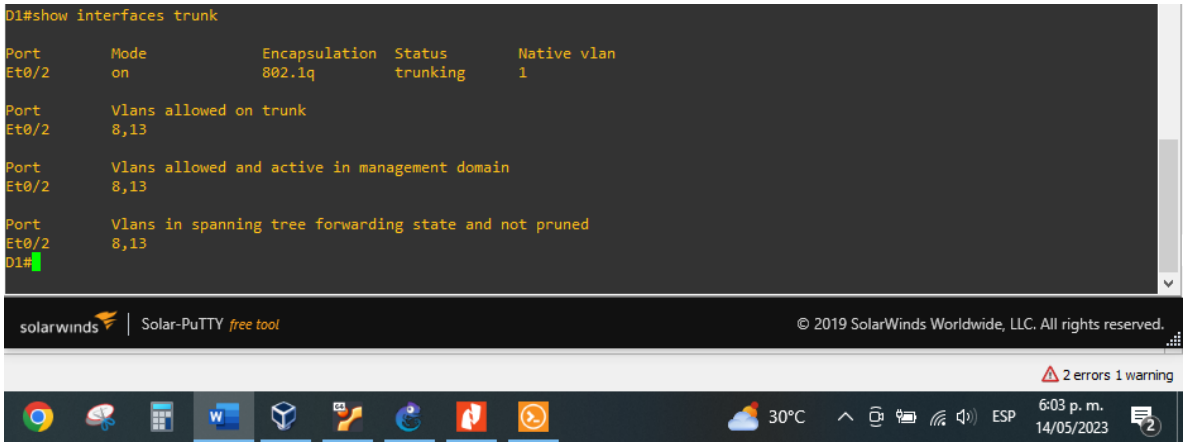

Figura 17. Interfaz troncal en D1

D2
config ter
interface e0/3
switchport trunk encapsulation dot1Q

switchport mode trunk
switchport trunk allowed Vlan 13,8
no shutdown
exit
exit
copy running-config startup-config

por medio del comando show interfaces trunk, podemos verificar el modo troncal en el switch D2

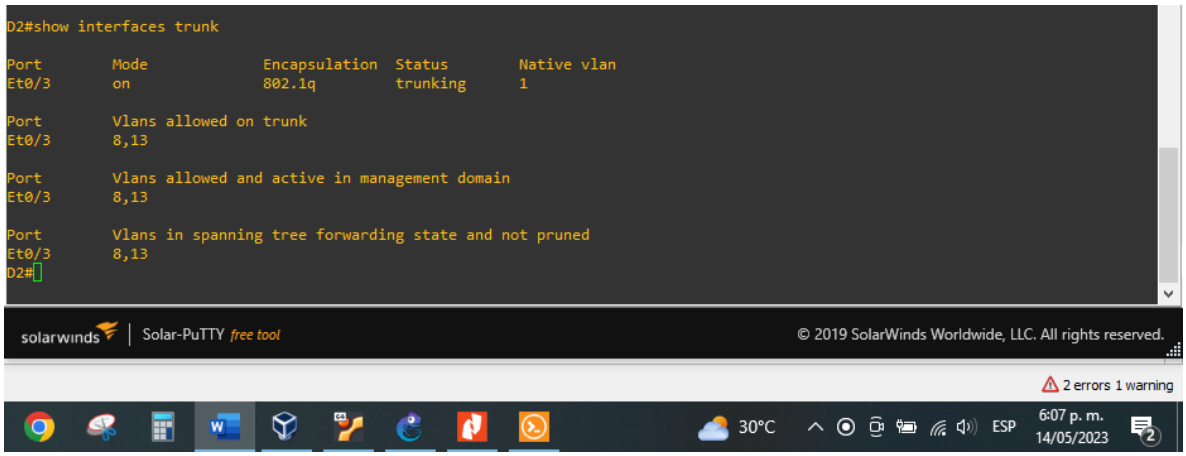

Figura 18. Intrefaz troncal en D2

3.3 en D1 y A1, configurar el EtherChannel

Se realizo la configuración de EtherChannel en los dispositivos D1 y A1, con los siguientes comandos:

D1
config ter
interface e0/0
switchport mode access
switchport Access vlan 8
channel-group 1 mode desirable
no shutdown
exit
interface e0/1
switchport mode access
switchport Access vlan 8
channel-group 1 mode desirable
no shutdown
exit
exit
copy running-config startup-config

comprobamos esta configuración con el siguiente comando

show EtherChannel summary

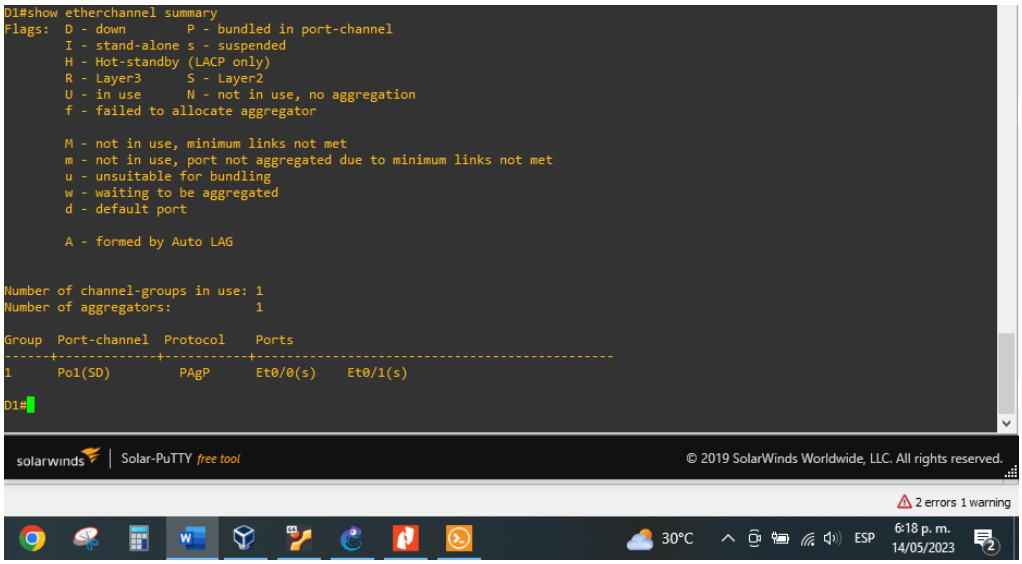

Figura 19. EtherChannel en D1

A1
config ter
interface e0/0
switchport mode access
switchport Access vlan 8
channel-group 1 mode desirable
no shutdown
exit
interface e0/1
switchport mode access
switchport Access vlan 8
channel-group 1 mode desirable
no shutdown
exit
exit
copy running-config startup-config
comprobamos esta configuración con el siguiente comando

show EtherChannel summary

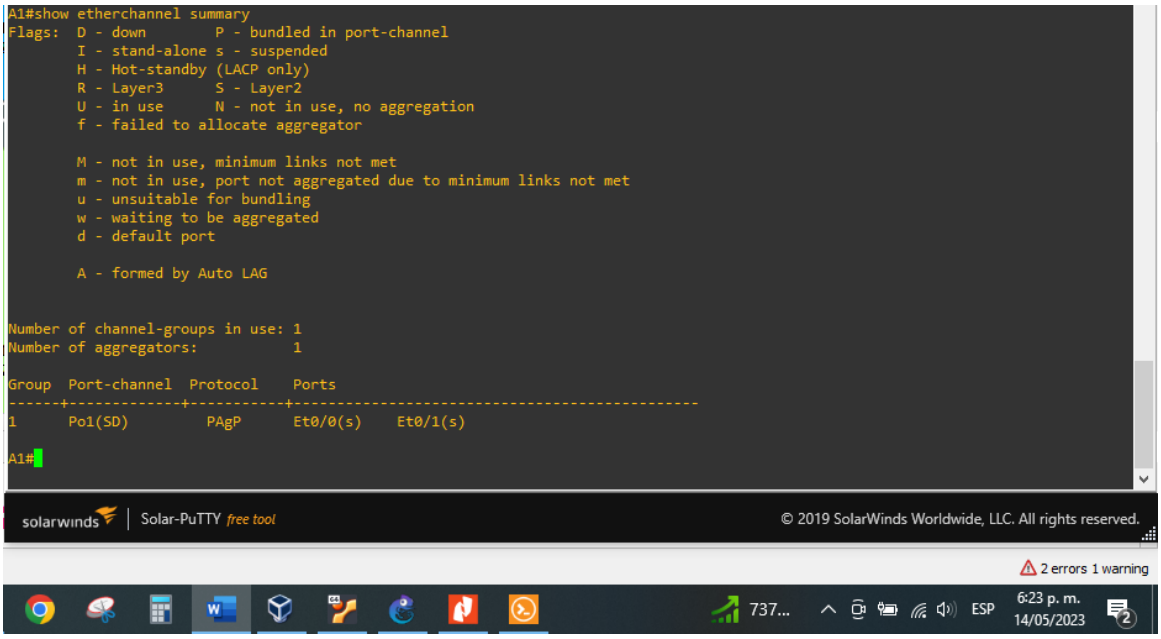

Figura 20. EtherChannel en A1

3.4 en D1, D2 y A1, configurar puertos de acceso para PC1, PC2, PC3 Y PC4

Para configurar los puertos de acceso en PC1, PC2, PC3 y PC4, se digitaron los siguientes comandos en D1, D2 y A1:

D1
config t
interface e0/3
switchport mode access
switchport access vlan 13
spanning-tree portfast
no shutdown
exit
exit
copy running-config startup-config

comprobamos esta configuración con el comando
show run interface e0/3

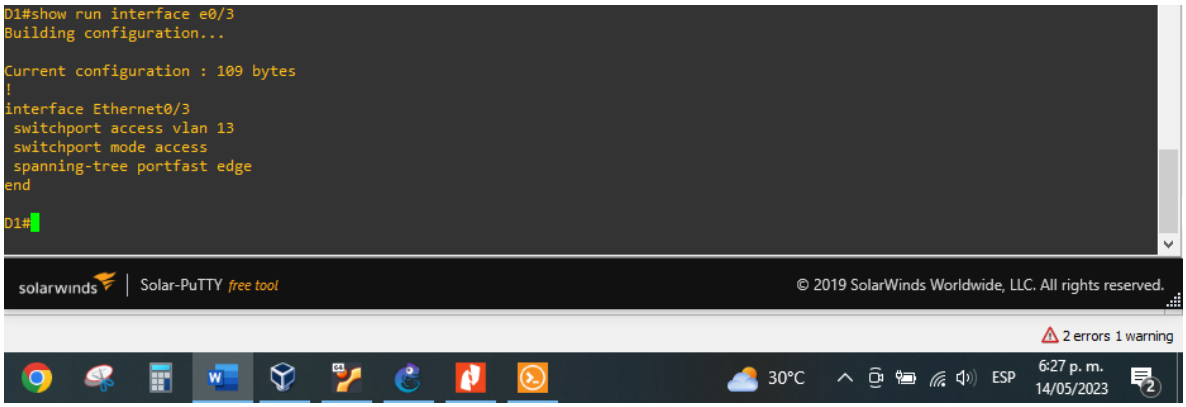

Figura 21. Ethernet 0/3 en D1

D2

config t
interface e0/2
switchport mode access
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
exit
copy running-config startup-config

comprobamos las dos interfaces con los siguientes comandos

show run interface e0/2

show run interface e0/1

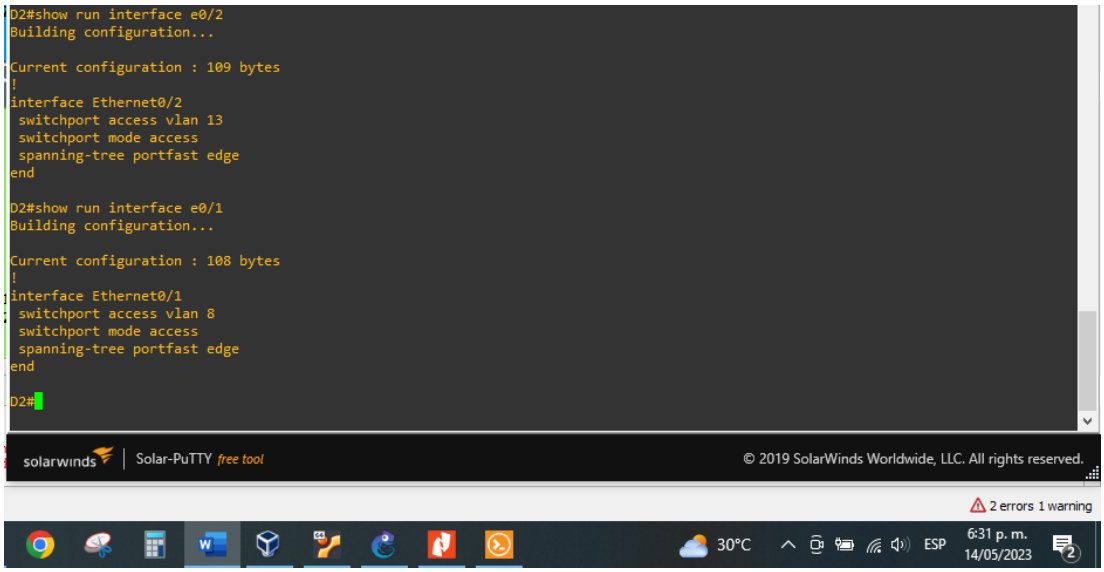

Figura 22. Ethernet 0/2 y 0/1 en D2

A1
Config t
interface e0/2
switchport mode access
switchport access vlan 8
spanning-tree portfast
no shutdown
exit
exit
copy running-config startup-config

comprobamos la interfaz con el siguiente comando

show run interface e0/2

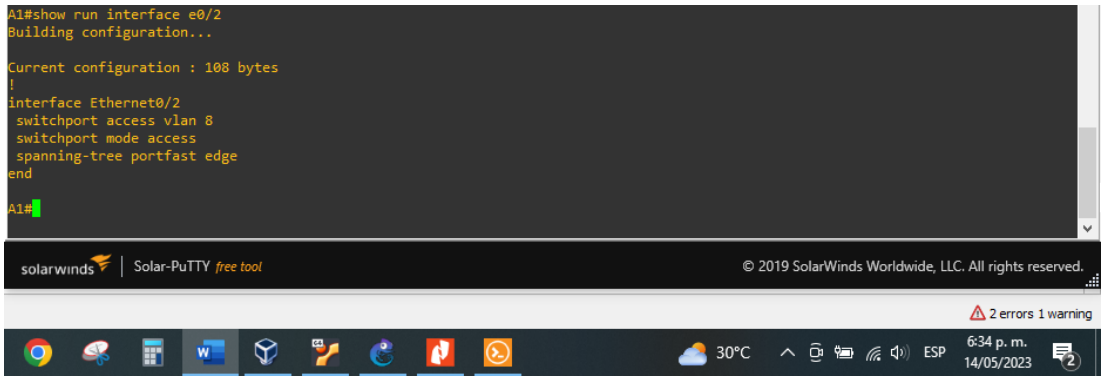

Figura 23. Ethernet 0/2 en A1

3.5 Verificación de la conectividad pc a pc

Para verificar la conectividad de pc a pc, primero se realizó ping desde el PC1 hacia el PC2 por ipv4 e ipv6

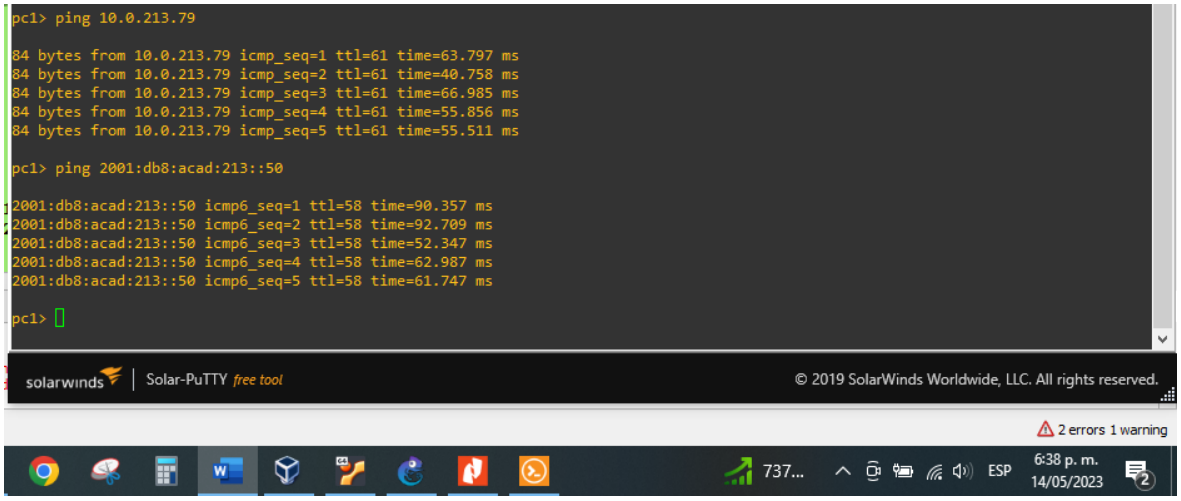

Figura 24. Conectividad de PC1 a PC2

Luego se realizó ping desde el PC1 hacia el PC3 y el PC4 por ipv4 e ipv6

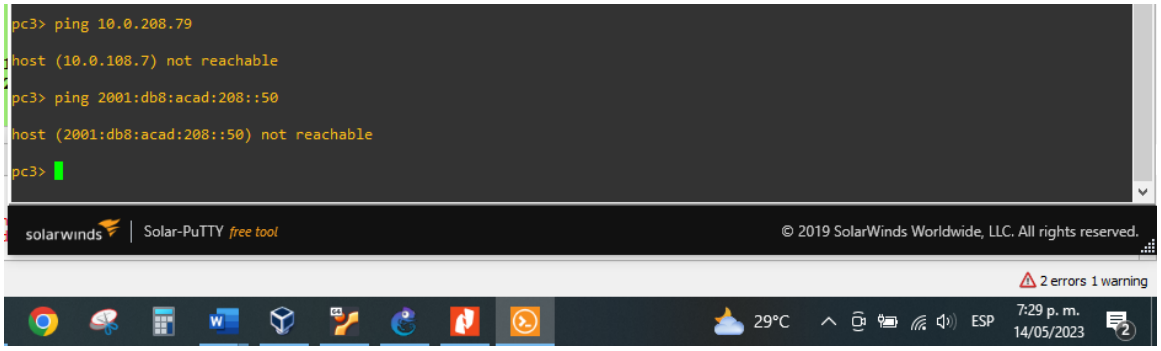

Figura 25. No Conectividad de PC1 a PC3 y PC4

4. Configuración de seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tabla 4. Configuración de 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.

4.1 en todos los dispositivos, modo de seguridad exec privilegiado

Iniciamos con el router R1 con los siguientes comandos

R1
Config t
Service password-encryption
Enable secret edinson791
Exit
copy running-config startup-config
R2
Config t
Service password-encryption
Enable secret edinson791
Exit
copy running-config startup-config
R3
Config t
Service password-encryption
Enable secret edinson791
Exit
copy running-config startup-config
D1
Config t
Service password-encryption
Enable secret edinson791
Exit

copy running-config startup-config
D2
Config t
Service password-encryption
Enable secret edinson791
Exit
copy running-config startup-config
A1
Config t
Service password-encryption
Enable secret edinson791
Exit
copy running-config startup-config

4.2 En todos los dispositivos, crear una cuanta local de usuario

R1
configure terminal
username admin secret 0 edinson791
username admin privilege 15 secret edinson791
exit
copy running-config startup-config
R2
configure terminal
username admin secret 0 edinson791
username admin privilege 15 secret edinson791
exit
copy running-config startup-config
R3
configure terminal
username admin secret 0 edinson791
username admin privilege 15 secret edinson791
exit
copy running-config startup-config
D1
configure terminal
username admin secret 0 edinson791
username admin privilege 15 secret edinson791
exit
copy running-config startup-config
D2
configure terminal
username admin secret 0 edinson791
username admin privilege 15 secret edinson791

exit
copy running-config startup-config
A1
configure terminal
username admin secret 0 edinson791
username admin privilege 15 secret edinson791
exit
copy running-config startup-config

4.3. En todos los dispositivos, activa el modelo AAA y activa AAA autenticación

R1
configure terminal
aaa new-model
aaa authentication login default local
exit
copy running-config startup-config
R2
configure terminal
aaa new - model
aaa authentication login default local
exit
copy running-config startup-config
R3
configure terminal
aaa new - model
aaa authentication login default local
exit
copy running-config startup-config
D1
configure terminal
aaa new - model
aaa authentication login default local
exit
copy running-config startup-config
D2
configure terminal
aaa new - model
aaa authentication login default local
exit
copy running-config startup-config
A1
configure terminal

aaa new - model
aaa authentication login default local
exit
copy running-config startup-config

por medio del comando “show run | include aaa | username”, comprobamos que quedaron configurados los parámetros de seguridad en todos los dispositivos.

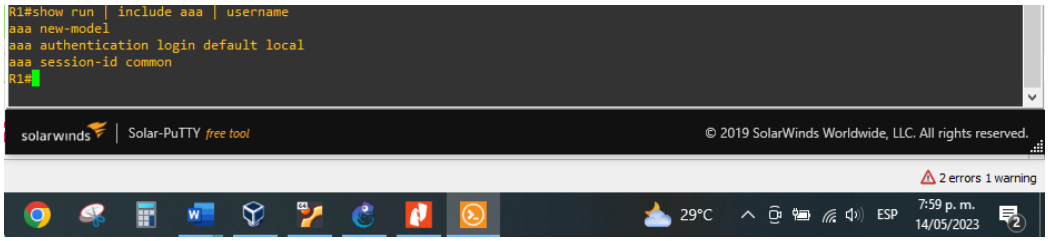

Figura 26. Configuración de seguridad en R1

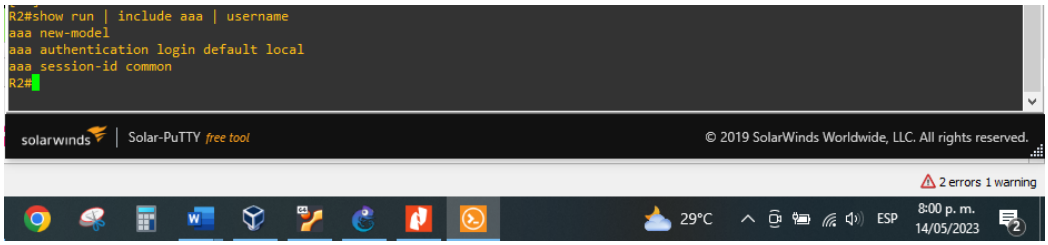

Figura 27. Configuración de seguridad en R2

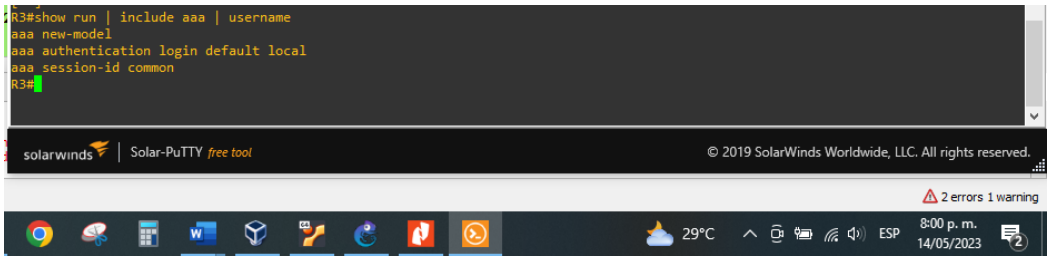

Figura 28. Configuración de seguridad en R3

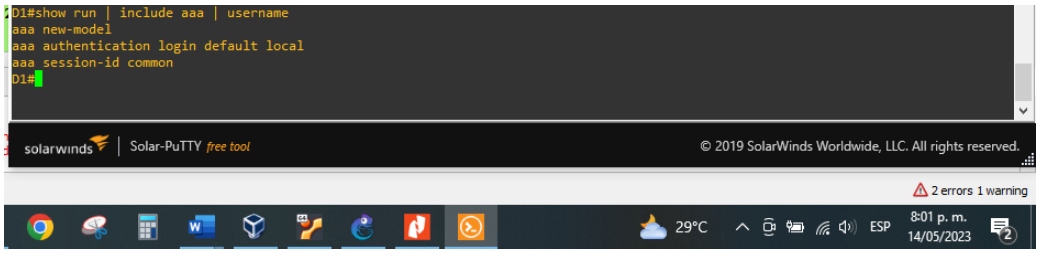

Figura 29. Configuración de seguridad en D1

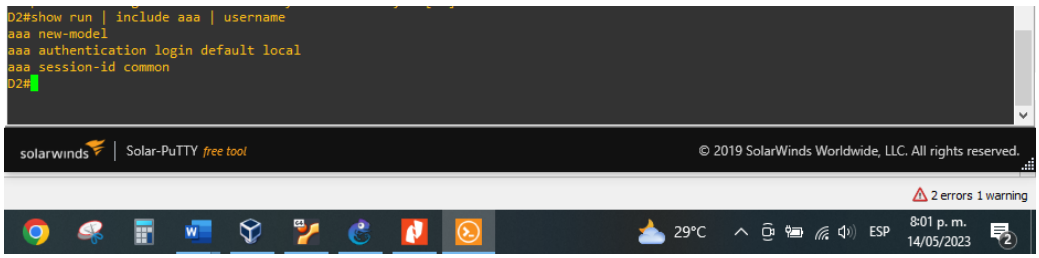

Figura 30. Configuración de seguridad en D2

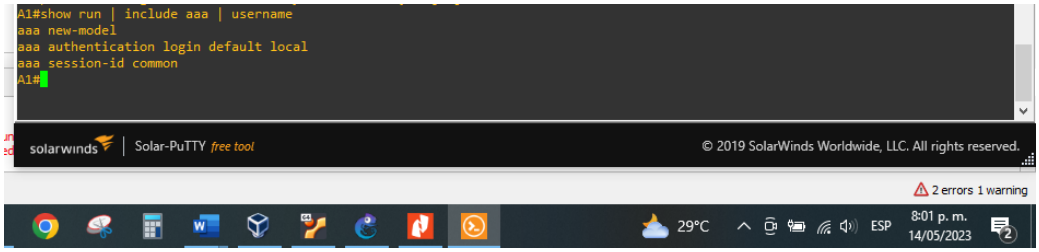

Figura 31. Configuración de seguridad en A1

Conclusión

Con la realización de esta actividad, se logró poner en práctica el enrutamiento estático entre dispositivos de una misma red, seccionándola en dos redes virtuales, haciendo uso de VRF (virtual routing forwarding), garantizando la comunicación de dispositivos pertenecientes a una misma VRF y restringiendo la comunicación entre dispositivos que pertenecen a VRF diferentes.

Por otra parte, se llevó a cabo la configuración de dispositivos capa 2, en donde se configuraron sus interfaces, rutas troncales y EtherChannel para que se puedan comunicar terminales pertenecientes a una vlan y al mismo tiempo impedir la comunicación con terminales que pertenecen a una vlan diferente.

Se establecieron niveles de seguridad, para impedir que personal no autorizado penetre la red, robe información y realice cambios perjudiciales a la organización.

Referencias Bibliográficas

- Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). CCNP and CCIE Enterprise Core ENCOR. https://1drv.ms/b/s!AAIGg5JUgUBthk8

- Vesga, J. (2019). *Introducción al Laboratorio Remoto SmartLab* [OVI]. http://hdl.handle.net/10596/24167

- Granados, G. (2019). Registro y acceso a la plataforma Cisco CCNP [OVI]. https://repository.unad.edu.co/handle/10596/24419

- Flor, P. (2022). Introducción al protocolo BGP [OVI]. https://repository.unad.edu.co/handle/10596/49573