DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Jessica Montoya Mendez

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Jessica Montoya Mendez

Diplomado de opción de grado presentado para optar por el
Título de INGENIERA DE TELECOMUNICACIONES

TUTORA
MARITZA FARLEY MONDRAGON GUZMAN

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

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

SANTIAGO DE CALI, 04 de mayo de 2023

AGRADECIMIENTOS

Agradezco principalmente a Dios por haberme dado la fortaleza para no desfallecer y lograr llegar a este momento de mi carrera, a mi madre por ser mi apoyo incondicional, ya que hizo carrera conmigo y estuvo siempre dispuesta y pasó horas buscando información académica que complementara mi formación, a mi padre y mi hermana por su palabras de aliento y la velar por mi desarrallo profesional. A mis amigos y compañeros de estudio por su disposición, ayuda, paciencia y colaboración que trazó el camino que hoy me ha permitido llegar hasta aquí. A todos los docentes que me acompañaron en este camino, por tranferir su conocimiento y hacer que la educación llegue a nosotros y estar dispuestos a participar en la construcción de un mejor país. A la universidad, mi universidad UNAD por crear modalidades de educación que permiten formarnos y cumplir nuestros sueños. A todos muchas gracias.

CONTENIDO

AGRADECIMIENTOS....4
CONTENIDO....5
LISTA DE TABLAS....7
LISTA DE FIGURAS....8
GLOSARIO....9
RESUMEN....10
ABSTRACT....10
INTRODUCCION....11
ESCENARIO....12
1. ESCENARIO PROPUESTO....12
2. PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE CADA DISPOSITIVO Y EL DIRECCIONAMIENTO DE LAS INTERFACES....14
2.1 Paso 1: Cablee la red como se muestra en la topología. 14
2.2 Paso 2: Configure los ajustes básicos para cada dispositivo. 14
3. PARTE 2: CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO 21
3.1 En R1, R2, y R3, configure VRF-LITE VRF como se muestra en el diagrama de la topología. 21
3.2 En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior. 22
3.3 En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2. 27
3.4 verifique la conectividad en cada VRF 30
4. PARTE 3. CONFIGURAR CAPA 2. 31
4.1 En D1, D2, y A1, deshabilite todas las interfaces. 31
4.2 En D1 y D2, configure los enlaces troncales a R1 y R3. 32
4.3 En D1 y A1, configure EtherChannel. 33

4.4 En D1, D2, y A1, configure los puertos de acceso para PC1, PC2, PC3, y PC4. 34
4.5 verifique la conectividad de PC a PC. 36
5. PARTE 4. CONFIGURE SECURITY.....38
CONCLUSIONES 42
BIBLIOGRAFIA 43

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento. 12
Tabla 2. Configuración básica R1. 15
Tabla 3. Configuración básica R2. 15
Tabla 4. Configuración básica R3. 16
Tabla 5. Configuración básica D1. 16
Tabla 6. Configuración básica D2. 18
Tabla 7. Configuración básica A1. 18
Tabla 8. Configuración VRF-Lite en R1, R2, R3. 21
Tabla 9. Configuración de interfaces para cada VRF en R1. 22
Tabla 10. Configuración de interfaces para cada VRF en R2. 24
Tabla 11. Configuración de interfaces para cada VRF en R3. 25
Tabla 12. configuración en R1 de rutas estáticas que apuntan a R2. 27
Tabla 13. Configuración en R3 de rutas estáticas que apuntan a R2. 28
Tabla 14. Deshabilitar interfaces en D1. 31
Tabla 15. Deshabilitar interfaces en D2 y A1. 31
Tabla 16. configuración enlace troncal en D1 y D2. 32
Tabla 17. configuración de EtherChannel en D1. 33
Tabla 18. Configuración de EtherChannel en A1. 33
Tabla 19. Configuración puertos de acceso a PC1 y PC2, en D1 y D2. 34
Tabla 20. Configuración puertos de acceso a PC4 en D2. 34
Tabla 21. Configuración puertos de acceso a PC3 en A1. 35
Tabla 22. Configuración de seguridad para D1, D2, A1. 38
Tabla 23. Configuración de seguridad para R1, R2, R3. 38

LISTA DE FIGURAS

Figura 1. Escenario propuesto 12
Figura 2. Simulación escenario 1 en GNS3. 14
Figura 3. Verificación de la creación de VLANs en D1. 17
Figura 4. Verificación de la creación de VLANs en A1. 19
Figura 5. Configuración de ip en PC1. 20
Figura 6. Verificación de creación de VRF en R1. 23
Figura 7. Verificación de IP y VRF en R1. 26
Figura 8. Verificación de IP y VRF en R2. 27
Figura 9. Verificación de IP y VRF en R3. 27
Figura 10. Verificación tabla de enrutamiento VRF General-Users en R1. 28
Figura 11. Verificación de rutas estáticas en R1. 29
Figura 12. Verificación de rutas estáticas en R2. 29
Figura 13. Verificación de rutas estáticas en R3. 29
Figura 14. Verificación de conectividad VRF General-Users entre R1 y R3. 30
Figura 15. Verificación de conectividad VRF Special-Users entre R1 y R3. 30
Figura 16. Verificación de enlace troncal en D1. 32
Figura 17. Verificación de EtherChannel en D1. 34
Figura 18. Verificación de configuración interfaz e0/0 en D1. 35
Figura 19. Verificación de comunicación entre PC2 y PC1. 36
Figura 20. Verificación de ping de PC3 a PC4. 36
Figura 21. Verificación de no comunicación entre VLANS. 37
Figura 22. Verificación de seguridad en D1. 39
Figura 23. Verificación de seguridad en D2. 39
Figura 24. Verificación de seguridad en A1. 40
Figura 25. Verificación de seguridad en R1. 40
Figura 26. Verificación de seguridad en R2. 40
Figura 27. Verificación de seguridad en R3. 41
Figura 28. Comprobación de solicitud de usuario y clave en R1. 41

GLOSARIO

Direccionamiento: en redes este concepto corresponde a la configuración que se realiza en los dispositivos de una red de datos, para lograr que a cada uno de los equipos que pertenecen a esta, se les asigne una dirección IP única y exclusiva para lograr una correcta transmisión y recepción de datos.

Enrutamiento estático: se refiere a la configuración que se predetermina en un dispositivo por parte del administrador de este, estableciendo tablas estáticas para así configurar y seleccionar manualmente las rutas que han de seguir los equipos en la red.

Protocolo de enrutamiento: se compone de un conjunto de reglas para especificar la manera de comunicación entre hosts para que logren reenviar e identificar paquetes y así mantener la información de las rutas conocidas a las redes más remotas.

Router-On-A-Stick: este método es usado para conectar varias subredes a una misma interfaz física, creando sobre estas interfaces virtuales, anexando al nombre de la interfaz física, un identificador asignado a la interfaz virtual. Ej. La interfaz física G0/0/1 quedaría como G0/0/1.1 al convertirse en una interfaz virtual.

VLAN: redes de área local virtual, permiten crear diferentes redes lógicas independientes en una misma red, segmentándola y facilitando su administración, ya que entre otras cosas permite asignar usuarios de manera lógica ya sea usando la dirección MAC, puertos del switch o etiquetas, a una misma VLAN sin necesidad que estén cerca físicamente.

VRF: tecnología de enrutamiento virtual y reenvío, por sus siglas en inglés virtual routing and forwarding, esta permite que un router cree más de una tabla de enrutamiento simultáneamente y así poder tener una misma dirección IP asignada a dos interfaces en el mismo router.

RESUMEN

Con el desarrollo de esta actividad se pone en práctica los conocimientos que se han ido adquiriendo a lo largo de este diplomado de profundización. Se tiene un escenario a desarrollar que consta de la configuración de diferentes dispositivos propios de una red de telecomunicaciones, para lograr tener una red segura e intercomunicada de acuerdo con las condiciones de la actividad.

La emulación de la actividad se realiza por medio del software GNS3, que permite tener de maneta simulada un escenario real, dado que los comandos y equipos que se emulan son representación de equipos existentes. En este escenario se segmenta la red por medio de creación de VLANs, ser realiza enrutamiento por medio de VRF, se configuran las direcciones estáticas de cada interfaz, se configura la seguridad de los dispositivos de la topología y se verifica que todas las configuraciones y la comunicación funcionen correctamente.

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

ABSTRACT

With the development of this activity, the knowledge that has been acquired throughout this in-depth diploma course is put into practice. There is a scenario to develop that consists of the configuration of different devices typical of a telecommunications network, in order to have a secure and intercommunicated network according to the conditions of the activity.

The emulation of the activity is carried out by means of the GNS3 software, which allows to simulate a real scenario, since the commands and equipment that are emulated are representations of existing equipment. In this scenario, the network is segmented through the creation of VLANs, routing is performed through VRF, the static addresses of each interface are configured, the security of the topology devices is configured, and it is verified that all the configurations and the communication work properly.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCION

En el desarrollo de esta actividad se plantea resolver un escenario establecido en la guía de actividades del presente diplomado, en el cual se debe separar una topología de red por medio de dos VLAN denominadas General Users, que será la VLAN 8 y Especial Users VLAN 13. Se deben implementar las configuraciones de cada dispositivo de red, de manera que se logre obtener una comunicación entre los equipos que estén en la misma VLAN y no deberá existir comunicación entre equipos que pertenecen a VLANs diferentes. Este escenario se desarrolará haciendo la emulación de la red, usando el software GNS3.

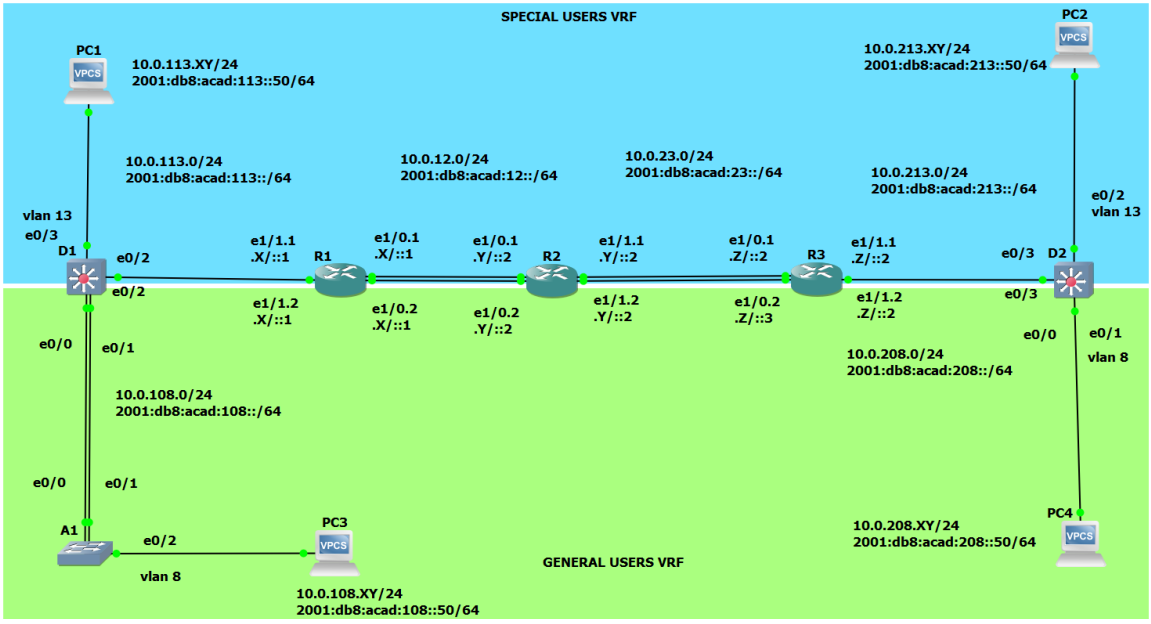
La actividad está divida en dos partes, para la primera parte, se harán configuraciones básicas de los dispositivos, entre los que encontramos switches, routers y equipos de cómputo. Se asignará nombre a cada dispositivo, en los routers se configuran las rutas estáticas, se habilitará direccionamiento IPv6 y se configurará las VRFs. También se configurará direccionamiento estático a cada equipo de cómputo.

En la segunda parte se realizará la configuración sobre los switches, se habilitarán opciones de seguridad, se crearán enlaces troncales, se configurará EtherChannel, se habilitará el acceso de los puertos de los PC a las VLANs correspondientes y se realizará la verficación de comunicación entre todos los PC, la cual debe ser exitosa entre los equipos de la misma VLAN y no debe haber comunicación entre las VLANs.

ESCENARIO

1. ESCENARIO PROPUESTO

Figura 1. Escenario propuesto



Fuente: guía de actividades.

Tabla 1. Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E1/0.1	10.0.12.2/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.2/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.2/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.2/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.3/24	2001:db8:acad:12::2/64	fe80::2:1

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
	E1/0.2	10.0.12.3/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.3/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.3/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.4/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.4/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.4/27	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.4/28	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.23/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.23/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.23/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.23/24	2001:db8:acad:208::50/64	EUI-64

Fuente: guía de actividades.

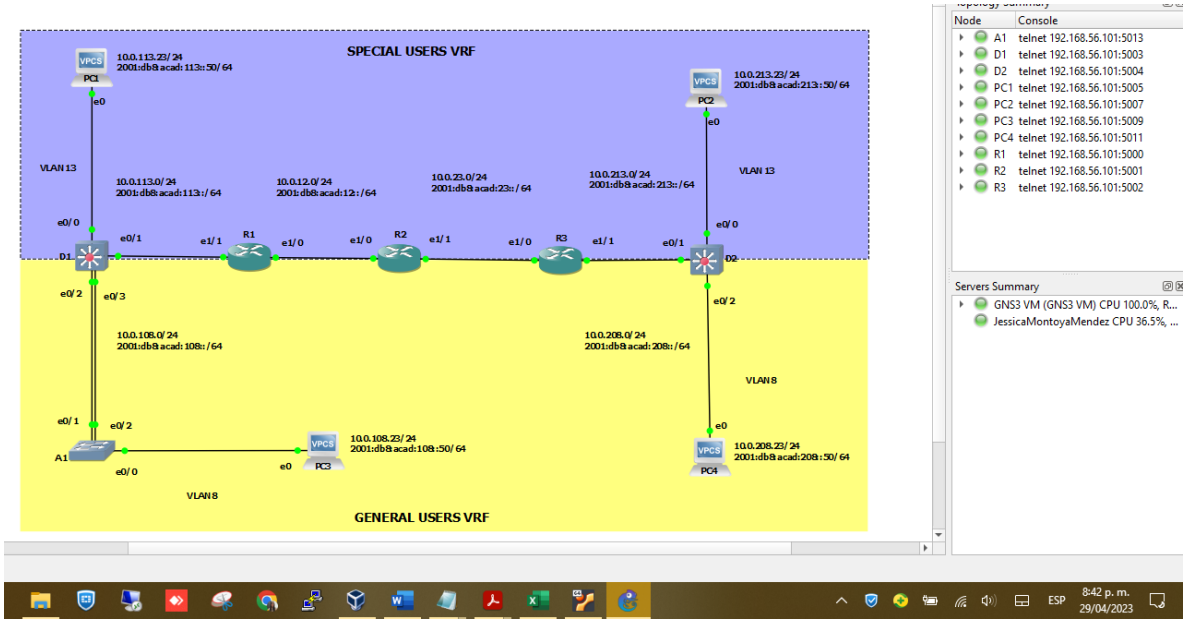
2. PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE CADA DISPOSITIVO Y EL DIRECCIONAMIENTO DE LAS INTERFACES

2.1 Paso 1: 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.

En este paso se realiza la instalación y configuración de los dispositivos de red necesarios para dar desarrollo al escenario propuesto y se realizan las conexiones necesarias que dan como resultado la ilustración siguiente:

Figura 2. Simulación escenario 1 en GNS3.



Fuente: autoría propia.

2.2 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.
- Guarde las configuraciones en cada uno de los dispositivos.
- Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento.

Se realiza configuración en cada dispositivo de red , asignando los nombres correspondientes, habilitando enrutamiento IPv6 y asignando el mensaje que se desea mostar al ingresar a cada uno.

Se relacionan los comando usados en cada dispositivo:

Router 1

Tabla 2. Configuración básica R1.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
hostname R1	Asignación de nombre al router
ipv6 unicast-routing	Habilitación el direccionamiento ipv6
no ip domain lookup	Se deshabilita el DNS
banner motd #R1, ENCOR Skills Assessment, Scenario 2#	Se asigna mensaje de inicio
line con 0	Se accede a modo configuración de consola
exec-timeout 0 0	Se establece el tiempo de espera inactivo en 0 minutos
logging synchronous	Se establece la sincronización de mensajes de salida hacia la consola
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Router 2

Tabla 3. Configuración básica R2.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
hostname R2	Asignación de nombre al router
ipv6 unicast-routing	Habilitación el direccionamiento ipv6
no ip domain lookup	Se deshabilita el DNS
banner motd #R2, ENCOR Skills Assessment, Scenario 2#	Se asigna mensaje de inicio

Comandos	Detalle
line con 0	Se accede a modo configuración de consola
exec-timeout 0 0	Se establece el tiempo de espera inactivo en 0 minutos
logging synchronous	Se establece la sincronización de mensajes de salida hacia la consola
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Router 3

Tabla 4. Configuración básica R3.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
hostname R3	Asignación de nombre al router
ipv6 unicast-routing	Habilitación el direccionamiento ipv6
no ip domain lookup	Se deshabilita el DNS
banner motd #R3, ENCOR Skills Assessment, Scenario 2#	Se asigna mensaje de inicio
line con 0	Se accede a modo configuración de consola
exec-timeout 0 0	Se establece el tiempo de espera inactivo en 0 minutos
logging synchronous	Se establece la sincronización de mensajes de salida hacia la consola
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

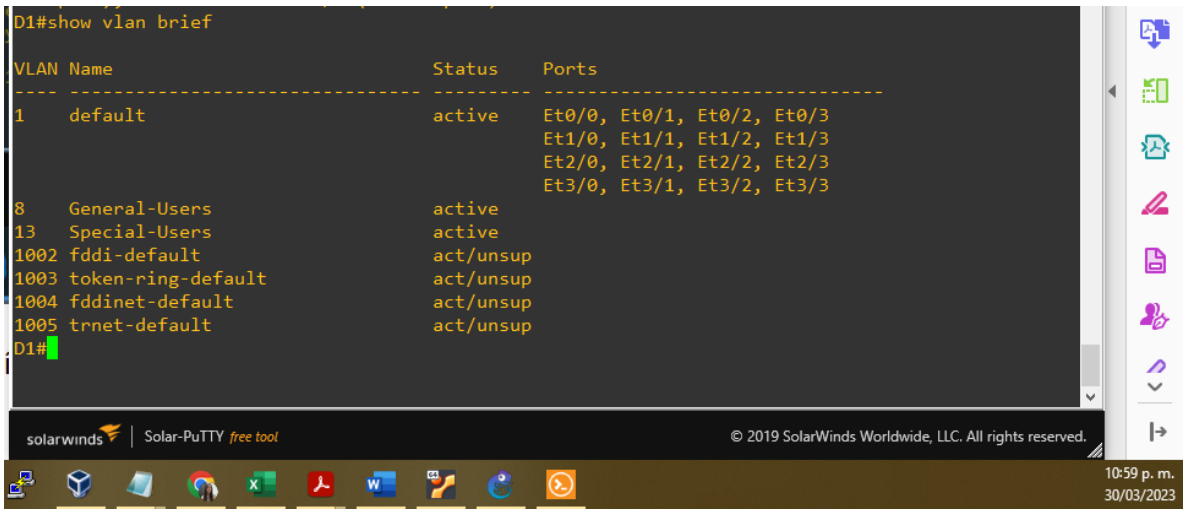
Switch D1

Tabla 5. Configuración básica D1.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global

Comandos	Detalle
hostname D1	Asignación de nombre al switch
ip routing	Habilitación IPv4
ipv6 unicast-routing	Habilitación el direccionamiento ipv6
no ip domain lookup	Se deshabilita el DNS
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #	Se asigna mensaje de inicio
line con 0	Se accede a modo configuración de consola
exec-timeout 0 0	Se establece el tiempo de espera inactivo en 0 minutos
logging synchronous	Se establece la sincronización de mensajes de salida hacia la consola
exit	Se regresa al modo privilegiado
vlan 8	Se crea VLAN
name General-Users	Se asigna nombre a la VLAN
exit	salir
vlan 13	Se crea VLAN
name Special-Users	Se asigna nombre a la VLAN
exit	salir
copy running-config startup-config	Se guarda la configuración

Figura 3. Verificación de la creación de VLANs en D1.



Fuente: autoría propia.

Switch D2

Tabla 6. Configuración básica D2.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
hostname D2	Asignación de nombre al switch
ip routing	Habilitación IPv4
ipv6 unicast-routing	Habilitación el direccionamiento ipv6
no ip domain lookup	Se deshabilita el DNS
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #	Se asigna mensaje de inicio
line con 0	Se accede a modo configuración de consola
exec-timeout 0 0	Se establece el tiempo de espera inactivo en 0 minutos
logging synchronous	Se establece la sincronización de mensajes de salida hacia la consola
exit	Se regresa al modo privilegiado
vlan 8	Se crea VLAN
name General-Users	Se asigna nombre a la VLAN
exit	salir
vlan 13	Se crea VLAN
name Special-Users	Se asigna nombre a la VLAN
exit	salir
copy running-config startup-config	Se guarda la configuración

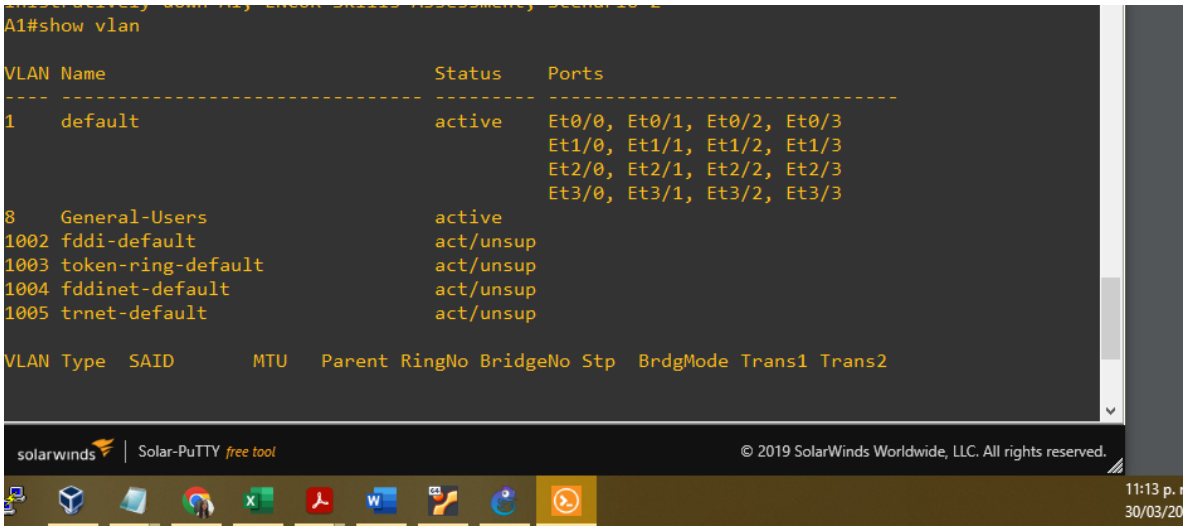
Switch A1

Tabla 7. Configuración básica A1.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
hostname A1	Asignación de nombre al switch
ipv6 unicast-routing	Habilitación el direccionamiento ipv6

Comandos	Detalle
no ip domain lookup	Se deshabilita el DNS
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #	Se asigna mensaje de inicio
line con 0	Se accede a modo configuración de consola
exec-timeout 0 0	Se establece el tiempo de espera inactivo en 0 minutos
logging synchronous	Se establece la sincronización de mensajes de salida hacia la consola
exit	Se regresa al modo privilegiado
vlan 8	Se crea VLAN
name General-Users	Se asigna nombre a la VLAN
exit	salir
copy running-config startup-config	Se guarda la configuración

Figura 4. Verificación de la creación de VLANs en A1.



Fuente: autoría propia.

Se procede ahora a configurar cada uno de los PCs, según la tabla de direccionamiento. A continuación se muestra la configuración de PC1, la cual se repite para cada uno de los otros equipos, con sus respectivas IP.

PC1

Figura 5. Configuración de IP en PC1.

Fuente: autoría propia.

3. 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 ping a R3 en cada VRF.

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

Sus tareas de configuración son las siguientes:

3.1 En R1, R2, y R3, configure VRF-LITE VRF como se muestra en el diagrama de la topología.

Configure two VRFs:

- General-Users
- Special-Users

The VRFs must support IPv4 and IPv6.

Se procede a realizar la configuración solicitada en el item 3.1, los mismos comandos relacionados en la tabla 9, se realizan en el Router 1, 2 y 3.

Tabla 8. Configuración VRF-Lite en R1, R2, R3.

Comandos	Detalle
vrf definition Special-Users	Se crea la VRF llamada Special-Users
address-family ipv6	Se indica la habilitación de IPv6
address-family ipv4	Se indica la habilitación de IPv4
Exit	Se regresa al modo de configuración global
vrf definition General-Users	Se crea la VRF llamada General-Users
address-family ipv6	Se indica la habilitación de IPv6
address-family ipv4	Se indica la habilitación de IPv4
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

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

All routers will use Router-On-A-Stick on their G0/0/1.x interfaces to support separation of the VRFs.

Sub-interface 1:

- In the Special Users VRF
- Use dot1q encapsulation 13
- IPv4 and IPv6 GUA and link-local addresses
- Enable the interfaces

Sub-interface 2:

- In the General Users VRF
- Use dot1q encapsulation 8
- IPv4 and IPv6 GUA and link-local addresses
- Enable the interfaces

Configuración requerida en el item 3.2 para R1:

Tabla 9. Configuración de interfaces para cada VRF en R1.

Comandos	Detalle
configure terminal	Se inicia en modo de configuración global
interface E1/0.1	Se habilita subinterfaz virtual
encapsulation dot1q 13	Se encapsula en la vlan 13
vrf forward Special-Users	Se asigna VRF
ip address 10.0.12.2 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:12::1/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::1:1 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/0.2	Se habilita subinterfaz virtual
encapsulation dot1q 8	Se encapsula en la vlan 8
vrf forward General-Users	Se asigna VRF
ip address 10.0.12.2 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:12::1/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::1:2 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz

Comandos	Detalle
exit	Salir
interface E1/0	Se ingresa a la interfaz física
no ip address	Se deshabilita configuración de IP
no shutdown	Se habilita interfaz física
exit	Salir
interface E1/1.1	Se habilita subinterfaz virtual
encapsulation dot1q 13	Se encapsula en la vlan 13
vrf forward Special-Users	Se asigna VRF
ip address 10.0.113.2 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:113::1/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::1:3 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/1.2	Se habilita subinterfaz virtual
encapsulation dot1q 8	Se encapsula en la vlan 8
vrf forward General-Users	Se asigna VRF
ip address 10.0.108.2 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:108::1/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::1:4 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/1	Se ingresa a la interfaz física
no ip address	Se deshabilita configuración de IP
no shutdown	Se habilita interfaz física
end	Se regresa al modo privilegiado

Figura 6. Verificación de creación de VRF en R1.

Fuente: autoría propia.

Configuración requerida en el item 3.2 para R2:

Tabla 10. Configuración de interfaces para cada VRF en R2.

Comandos	Detalle
configure terminal	Se inicia en modo de configuración global
interface E1/0.1	Se habilita subinterfaz virtual
encapsulation dot1q 13	Se encapsula en la vlan 13
vrf forward Special-Users	Se asigna VRF
ip address 10.0.12.3 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:12::2/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::2:1 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/0.2	Se habilita subinterfaz virtual
encapsulation dot1q 8	Se encapsula en la vlan 8
vrf forward General-Users	Se asigna VRF
ip address 10.0.12.3 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:12::2/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::2:2 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/0	Se ingresa a la interfaz física
no ip address	Se deshabilita configuración de IP
no shutdown	Se habilita interfaz física
exit	Salir
interface E1/1.1	Se habilita subinterfaz virtual
encapsulation dot1q 13	Se encapsula en la vlan 13
vrf forward Special-Users	Se asigna VRF
ip address 10.0.23.3 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:23::2/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::2:3 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/1.2	Se habilita subinterfaz virtual
encapsulation dot1q 8	Se encapsula en la vlan 8
vrf forward General-Users	Se asigna VRF

Comandos	Detalle
ip address 10.0.23.3 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:23::2/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::2:4 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/1	Se ingresa a la interfaz física
no ip address	Se deshabilita configuración de IP
no shutdown	Se habilita interfaz física
end	Se regresa al modo privilegiado

Configuración requerida en el item 3.2 para R3:

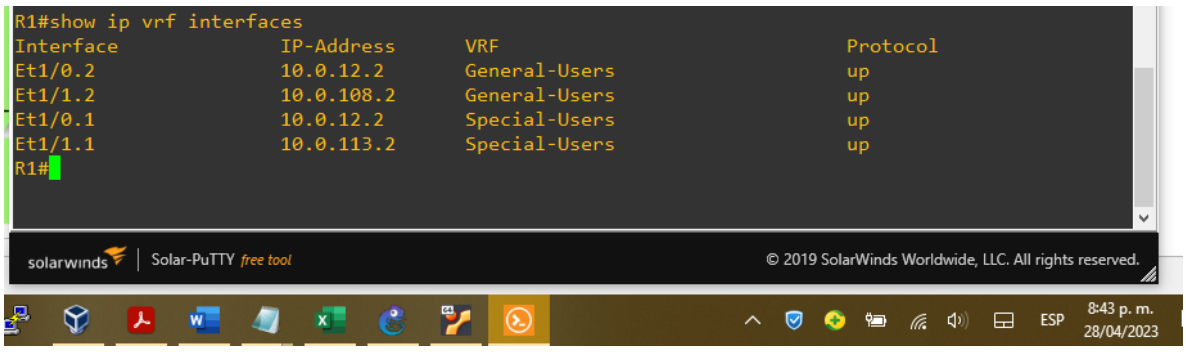
Tabla 11. Configuración de interfaces para cada VRF en R3.

Comandos	Detalle
configure terminal	Se inicia en modo de configuración global
interface E1/0.1	Se habilita subinterfaz virtual
encapsulation dot1q 13	Se encapsula en la vlan 13
vrf forward Special-Users	Se asigna VRF
ip address 10.0.23.4 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:23::3/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::3:1 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/0.2	Se habilita subinterfaz virtual
encapsulation dot1q 8	Se encapsula en la vlan 8
vrf forward General-Users	Se asigna VRF
ip address 10.0.23.4 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:23::3/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::3:2 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/0	Se ingresa a la interfaz física
no ip address	Se deshabilita configuración de IP
no shutdown	Se habilita interfaz física

Comandos	Detalle
exit	Salir
interface E1/1.1	Se habilita subinterfaz virtual
encapsulation dot1q 13	Se encapsula en la vlan 13
vrf forward Special-Users	Se asigna VRF
ip address 10.0.213.4 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:213::1/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::3:3 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/1.2	Se habilita subinterfaz virtual
encapsulation dot1q 8	Se encapsula en la vlan 8
vrf forward General-Users	Se asigna VRF
ip address 10.0.208.4 255.255.255.0	Se asigna la IPv4 correspondiente
ipv6 address 2001:db8:acad:208::1/64	Se asigna Ipv6 correspondiente
ipv6 address fe80::3:4 link-local	Se asigna link-local
no shutdown	Se habilita la subinterfaz
exit	Salir
interface E1/1	Se ingresa a la interfaz física
no ip address	Se deshabilita configuración de IP
no shutdown	Se habilita interfaz física
end	Se regresa al modo privilegiado

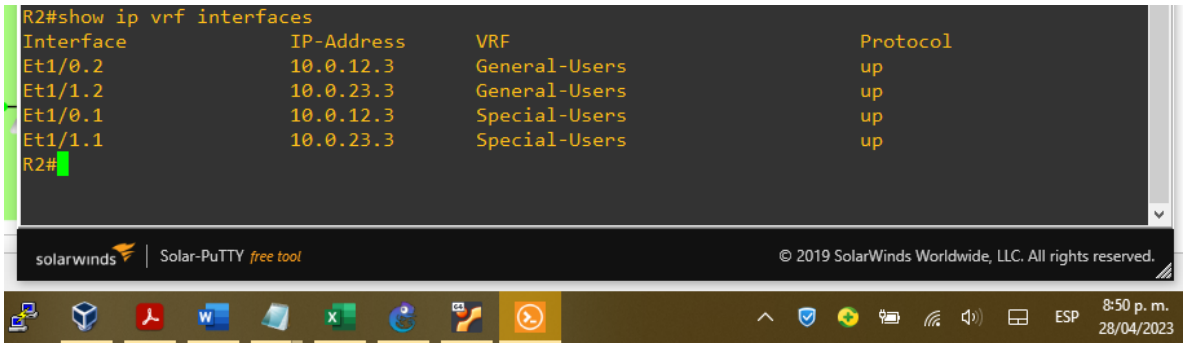
Para la verificación se usa el comando *show ip vrf interfaces*

Figura 7. Verificación de IP y VRF en R1.



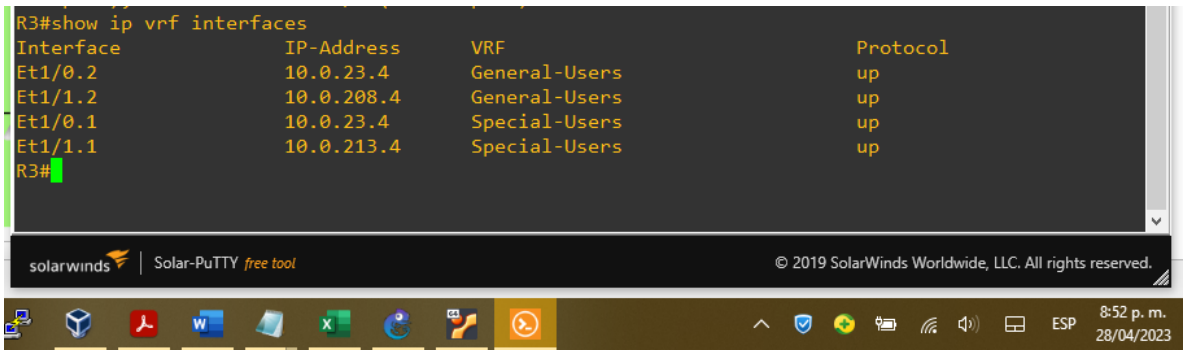
Fuente: autoría propia.

Figura 8. Verificación de IP y VRF en R2.



Fuente: autoría propia.

Figura 9. Verificación de IP y VRF en R3.



Fuente: autoría propia.

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

- Configure VRF static routes for both IPv4 and IPv6 in both VRFs.

Tabla 12. configuración en R1 de rutas estáticas que apuntan a R2.

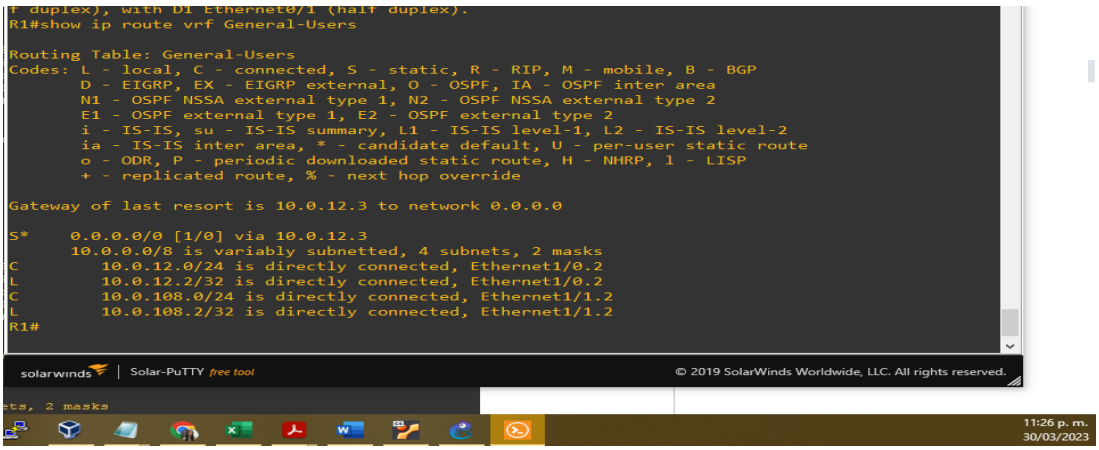
Comandos	Detalle
configure terminal	Ingreso al modo de configuración global
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.3	se realiza asignación de ruta IPv4 estática VRF General-Users

Comandos	Detalle
ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2	se realiza asignación de ruta IPv6 estática VRF General-Users
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.3	se realiza asignación de ruta IPv4 estática VRF Special-Users
ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2	se realiza asignación de ruta IPv6 estática VRF Special-Users
exit	salir de modo configuración VRF

Tabla 13. Configuración en R3 de rutas estáticas que apuntan a R2.

Comandos	Detalle
configure terminal	Ingreso al modo de configuración global
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.3	se realiza asignación de ruta IPv4 estática VRF General-Users
ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2	se realiza asignación de ruta IPv6 estática VRF General-Users
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.3	se realiza asignación de ruta IPv4 estática VRF Special-Users
ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2	se realiza asignación de ruta IPv6 estática VRF Special-Users
exit	salir de modo configuración VRF

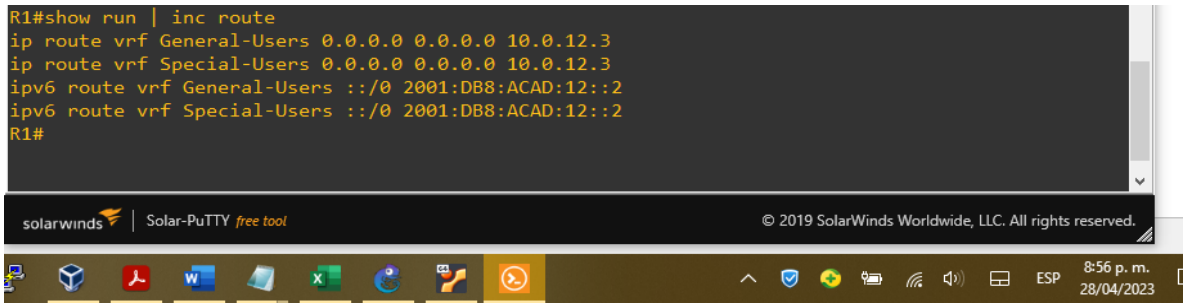
Figura 10. Verificación tabla de enrutamiento VRF General-Users en R1.



Fuente: autoría propia.

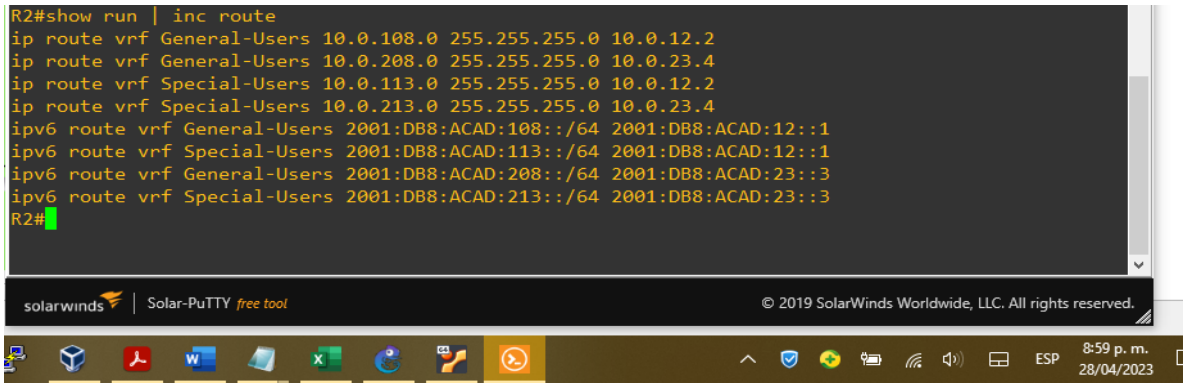
Para la verificación se usa el comando *show run* | *inc route*

Figura 11. Verificación de rutas estáticas en R1.



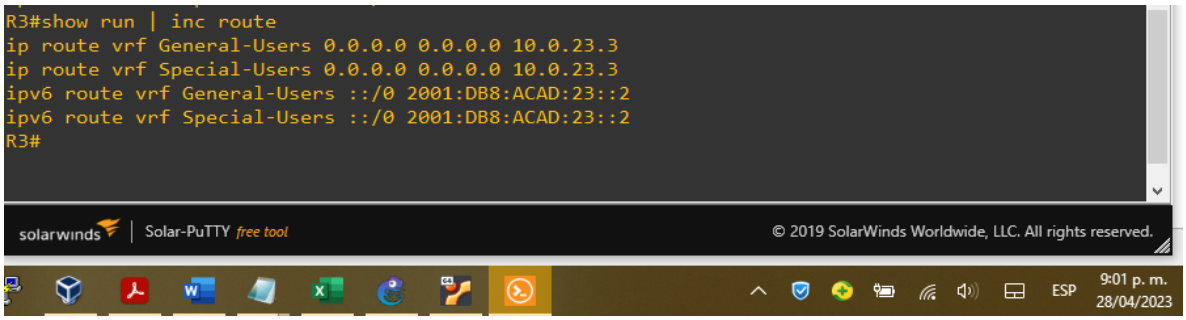
Fuente: autoría propia.

Figura 12. Verificación de rutas estáticas en R2.



Fuente: autoría propia.

Figura 13. Verificación de rutas estáticas en R3.



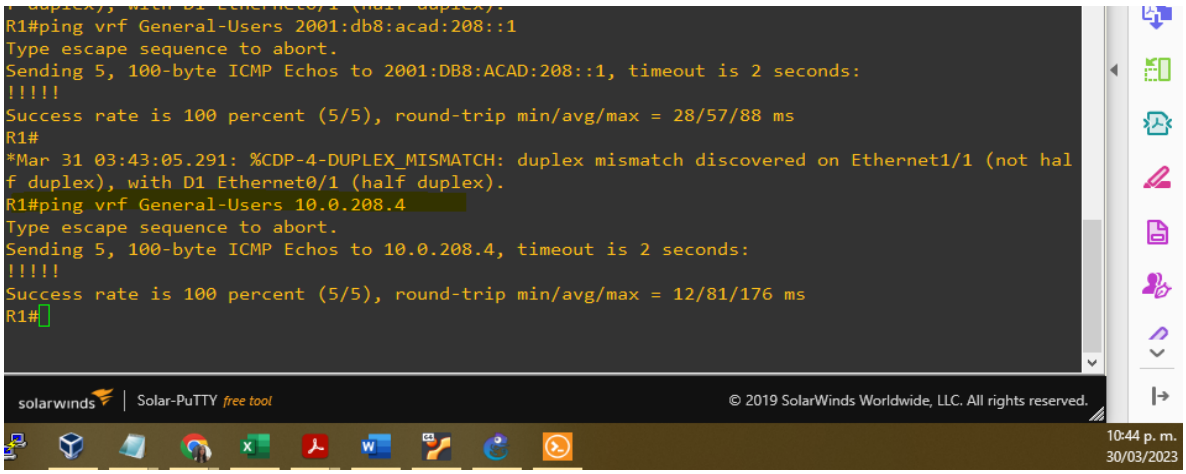
Fuente: autoría propia.

3.4 verifique la conectividad en cada VRF

From R1, verify connectivity to R3:

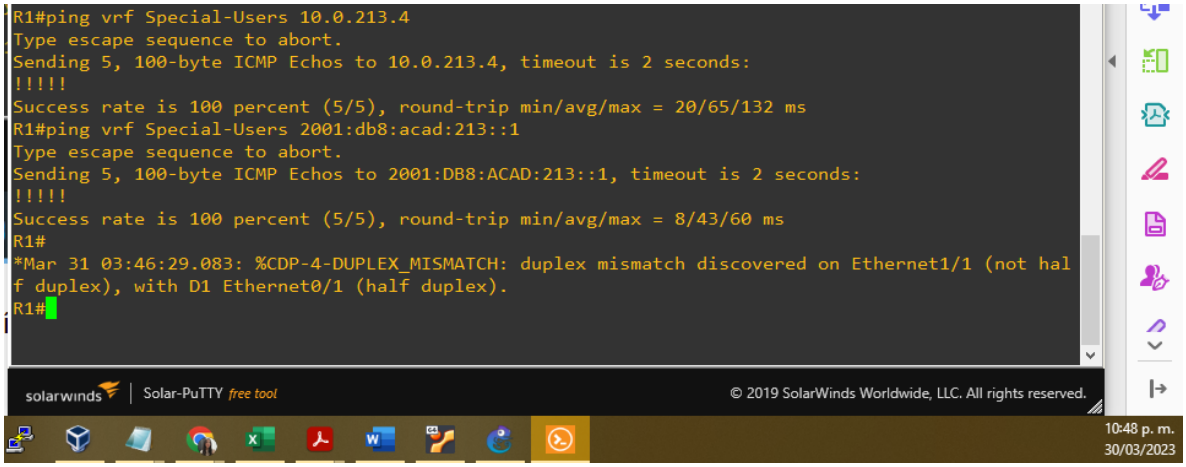
- ping vrf General-Users 10.0.208.4
- ping vrf General-Users 2001:db8:acad:208::1
- ping vrf Special-Users 10.0.213.4
- ping vrf Special-Users 2001:db8:acad:213::1

Figura 14. Verificación de conectividad VRF General-Users entre R1 y R3.



Fuente: autoría propia.

Figura 15. Verificación de conectividad VRF Special-Users entre R1 y R3.



Fuente: autoría propia.

4. PARTE 3. CONFIGURAR CAPA 2.

En esta parte se realiza la configuración de capa 2, realizando los siguientes pasos:

4.1 En D1, D2, y A1, deshabilite todas las interfaces.

Tabla 14. Deshabilitar interfaces en D1.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
interface range e1/0-3	se ingresa a un rango de interfaces
shutdown	se apagan las interfaces
exit	salir
interface range e2/0-3	se ingresa a un rango de interfaces
shutdown	se apagan las interfaces
exit	salir
interface range e3/0-3	se ingresa a un rango de interfaces
shutdown	se apagan las interfaces
exit	salir

Tabla 15. Deshabilitar interfaces en D2 y A1.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
interface e0/3	se ingresa a la interfaz
shutdown	se apagan la interfaz
exit	salir
interface range e1/0-3	se ingresa a un rango de interfaces
shutdown	se apagan las interfaces
exit	salir
interface range e2/0-3	se ingresa a un rango de interfaces
shutdown	se apagan las interfaces
exit	salir
interface range e3/0-3	se ingresa a un rango de interfaces
shutdown	se apagan las interfaces
exit	salir

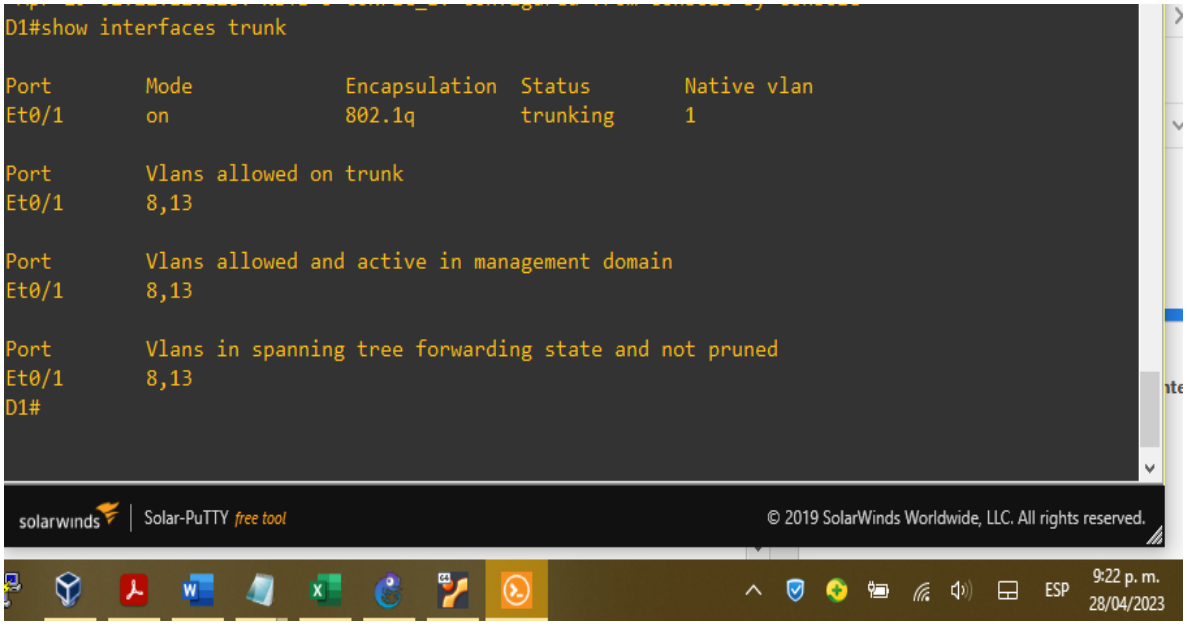
4.2 En D1 y D2, configure los enlaces troncales a R1 y R3.

Tabla 16. configuración enlace troncal en D1 y D2.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
interface e0/1	se ingresa a la interfaz
switchport trunk encapsulation dot1q	se configura el enlace al estándar 802.1Q
switchport mode trunk	se configura en modo troncal
switchport trunk allowed vlan 13,8	lista de VLAN permitidas en el enlace troncal
exit	salir
copy running-config startup-config	Se guarda la configuración

Para la verificación se usa el comando *show interfaces trunk*

Figura 16. Verificación de enlace troncal en D1.



Fuente: autoría propia.

4.3 En D1 y A1, configure EtherChannel.

Tabla 17. configuración de EtherChannel en D1.

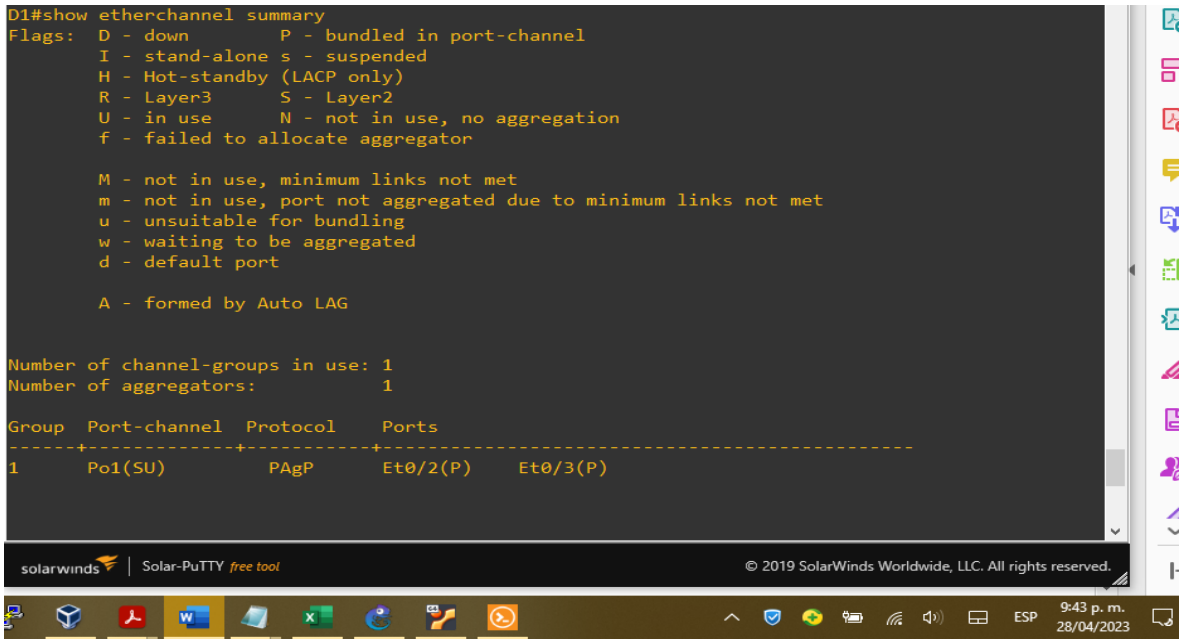
Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
interface range e0/2-3	se ingresa al rango de interfaces
switchport trunk encapsulation dot1q	se configura el enlace al estándar 802.1Q
switchport mode trunk	Se configura interfaces como troncales
channel-group 1 mode desirable	se asigna grupo -canal
no shutdown	Se levanta las interfaces
end	Se regresa al modo privilegiado

Tabla 18. Configuración de EtherChannel en A1.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
interface range e0/1-2	se ingresa al rango de interfaces
switchport trunk encapsulation dot1q	se configura el enlace al estándar 802.1Q
switchport mode trunk	Se configura interfaces como troncales
channel-group 1 mode desirable	se asigna grupo -canal
no shutdown	Se levanta las interfaces
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Para la verificación de la creación de etherChannel se usa el comando: *show etherchannel summary*

Figura 17. Verificación de EtherChannel en D1.



Fuente: autoría propia.

4.4 En D1, D2, y A1, configure los puertos de acceso para PC1, PC2, PC3, y PC4.

Tabla 19. Configuración puertos de acceso a PC1 y PC2, en D1 y D2.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
interface e0/0	se ingresa a la interfaz
switchport mode access	se activa modo de acceso
switchport access vlan 13	se habilita el acceso a la VLAN 13
spanning-tree portfast	se habilita el acceso rápido del puerto
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Tabla 20. Configuración puertos de acceso a PC4 en D2.

Comandos	Detalle
enable	Ingreso al modo privilegiado

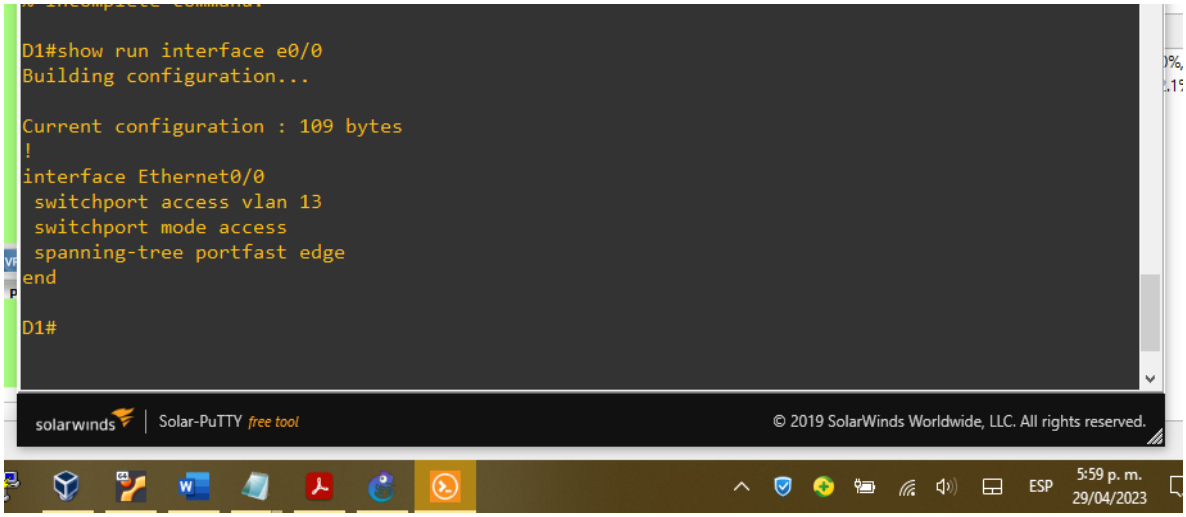
Comandos	Detalle
configure terminal	Ingreso al modo de configuración global
interface e0/2	se ingresa a la interfaz
switchport mode access	se activa modo de acceso
switchport access vlan 8	se habilita el acceso a la VLAN 8
spanning-tree portfast	se habilita el acceso rápido del puerto
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Tabla 21. Configuración puertos de acceso a PC3 en A1.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
interface e0/0	se ingresa a la interfaz
switchport mode access	se activa modo de acceso
switchport access vlan 8	se habilita el acceso a la VLAN 8
spanning-tree portfast	se habilita el acceso rápido del puerto
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Para la verificación de la configuración del puerto se usa el comando: *show run interface e0/0*

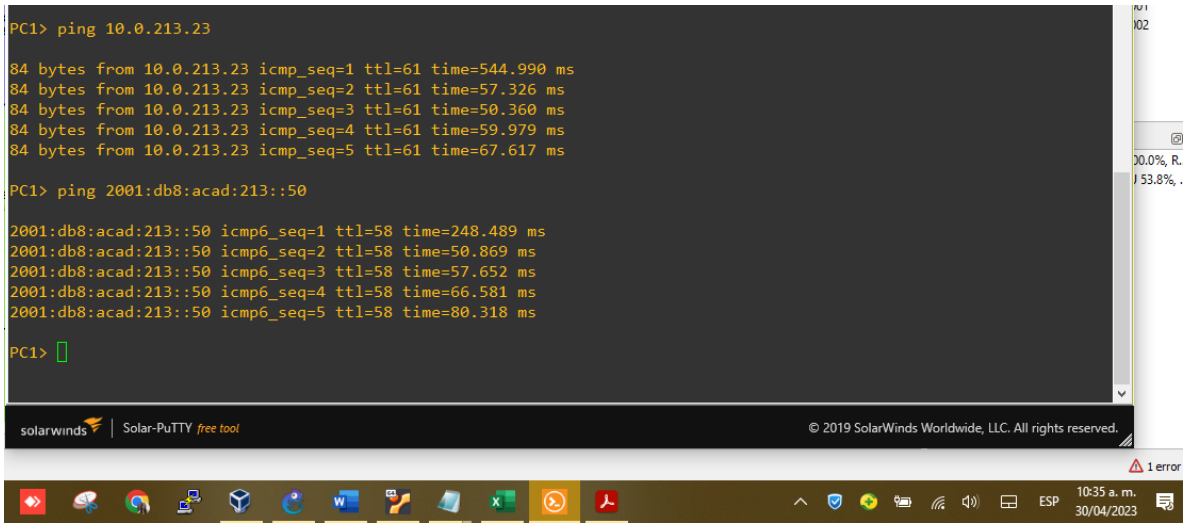
Figura 18. Verificación de configuración interfaz e0/0 en D1.



Fuente: autoría propia.

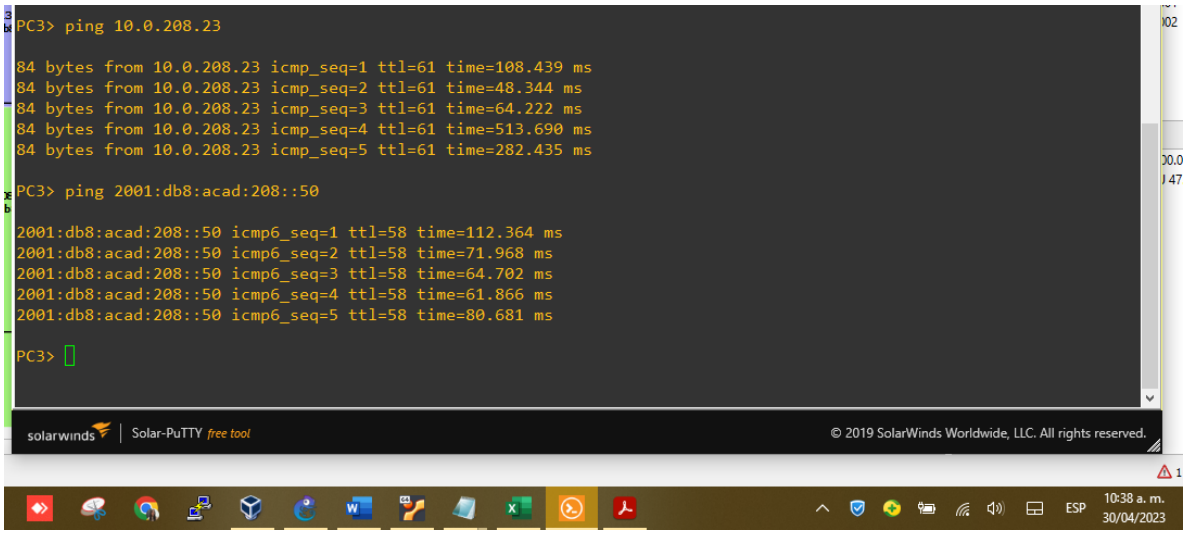
4.5 verifique la conectividad de PC a PC.

Figura 19. Verificación de comunicación entre PC2 y PC1.



Fuente: autoría propia.

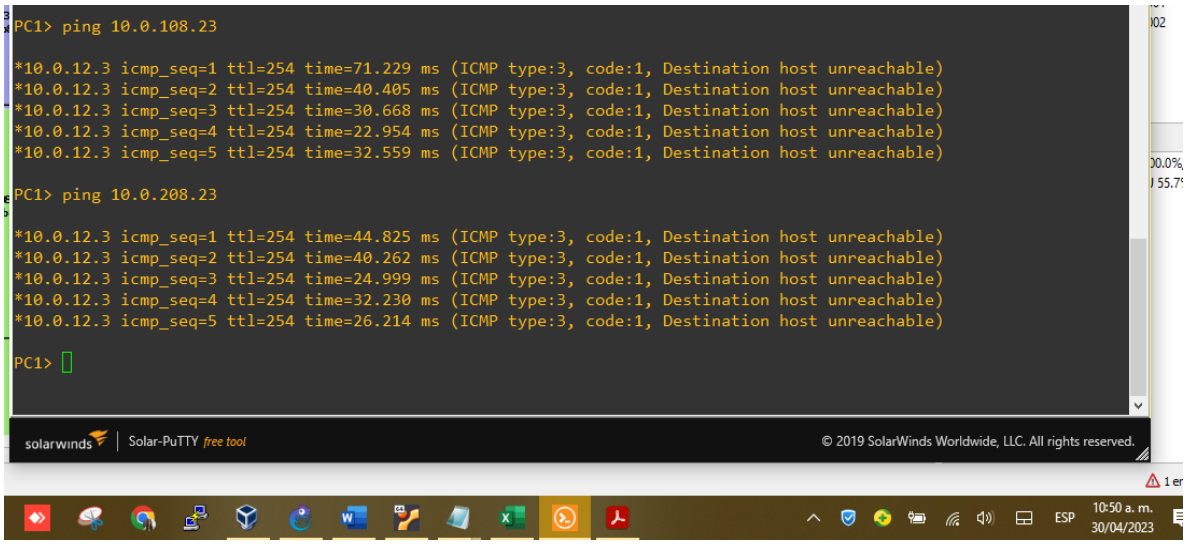
Figura 20. Verificación de ping de PC3 a PC4.



Fuente: autoría propia.

Se verifica que no hay conexión desde la VLAN 13, a los PC que están en la VLAN 8 General Users, haciendo ping desde el PC1 hacia el PC3 y PC4.

Figura 21. Verificación de no comunicación entre VLANS.



Fuente: autoría propia.

5. PARTE 4. CONFIGURE SECURITY

- En todos los dispositivos, habilite modo EXE privilegiado seguro.
- En todos los dispositivos cree una cuenta de usuario local
- En todos los dispositivos habilite AAA y habilite la autenticación AAA

Se realiza la configuración de seguridad para todos los dispositivos de la red.

Tabla 22. Configuración de seguridad para D1, D2, A1.

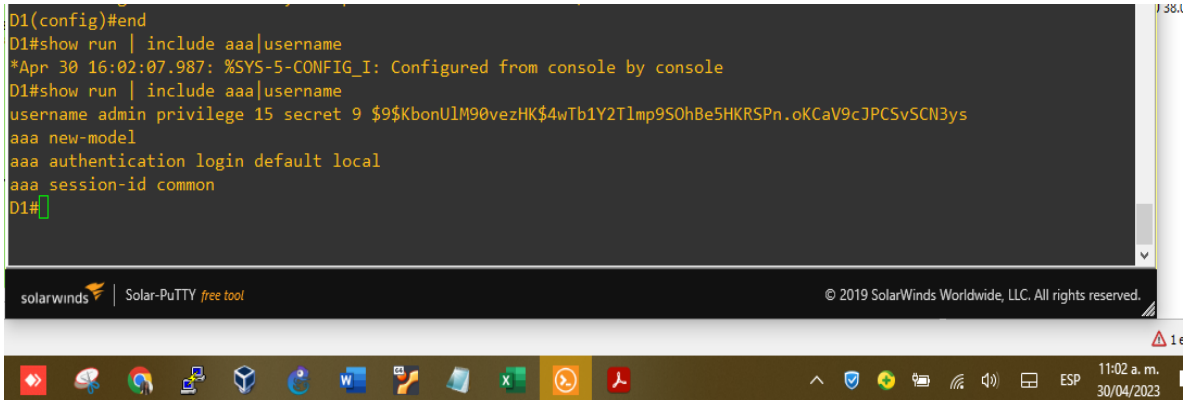
Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
enable algorithm-type scrypt secret cisco12345cisco	se habilita clave secreta
username admin privilege 15 algorithm-type scrypt secret cisco12345cisco	se habilita usuario y asocia clave secreta
aaa new-model	se habilita método de autenticación
aaa authentication login default local	se habilita autenticación usando la base de datos local
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Tabla 23. Configuración de seguridad para R1, R2, R3.

Comandos	Detalle
enable	Ingreso al modo privilegiado
configure terminal	Ingreso al modo de configuración global
service password-encryption	se habilita clave secreta
enable secret cisco12345cisco	se habilita usuario y asocia clave secreta
username admin secret 0 cisco12345cisco	se habilita usuario y asocia clave secreta
username admin privilege 15 secret cisco12345cisco	Se configura acceso a modo privilegiado completo.
aaa new-model	se habilita método de autenticación

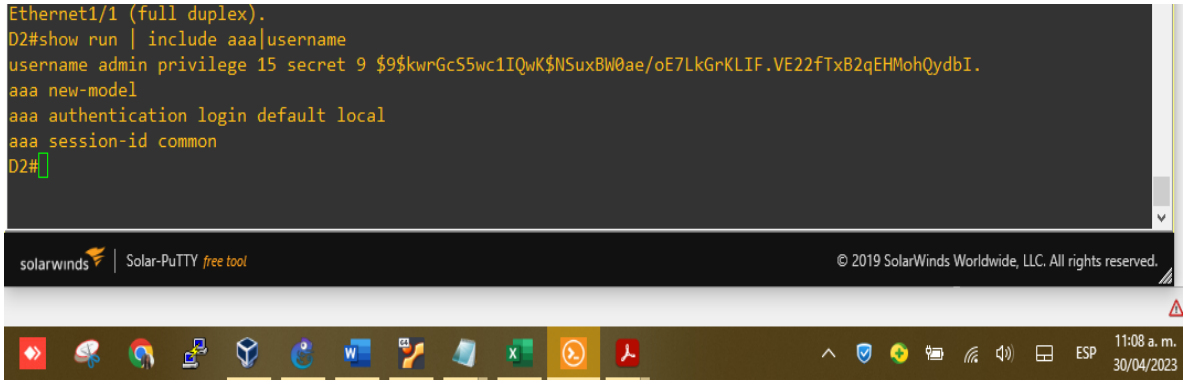
Comandos	Detalle
aaa authentication login default local	se habilita autenticación usando la base de datos local
end	Se regresa al modo privilegiado
copy running-config startup-config	Se guarda la configuración

Figura 22. Verificación de seguridad en D1.



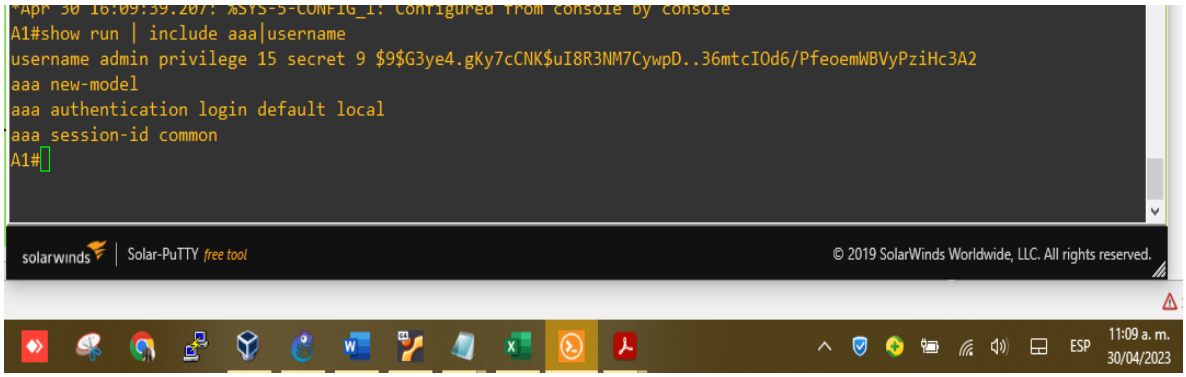
Fuente: autoría propia.

Figura 23. Verificación de seguridad en D2.



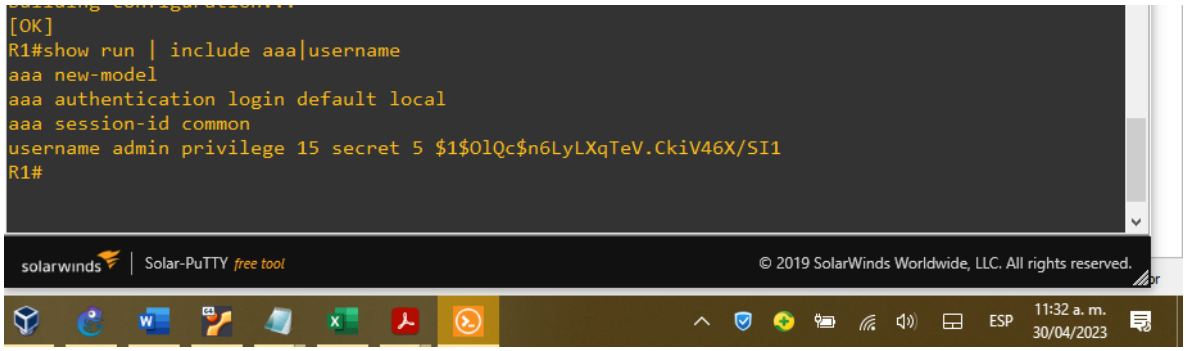
Fuente: autoría propia.

Figura 24. Verificación de seguridad en A1.



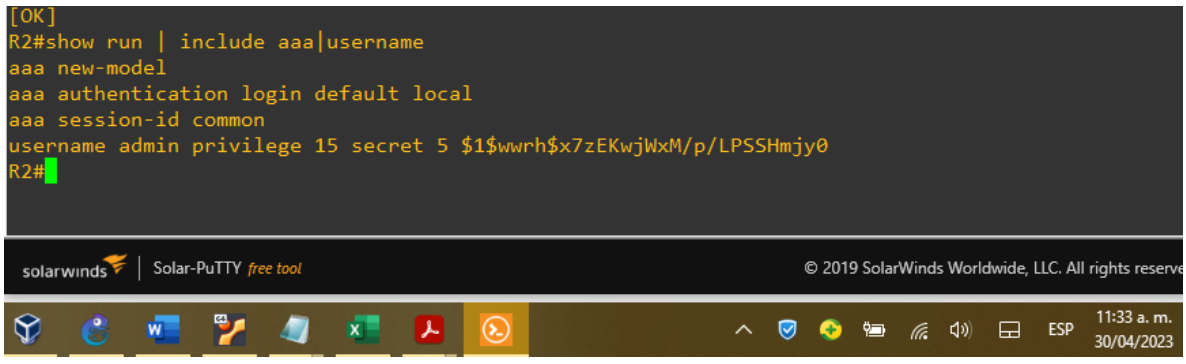
Fuente: autoría propia.

Figura 25. Verificación de seguridad en R1.



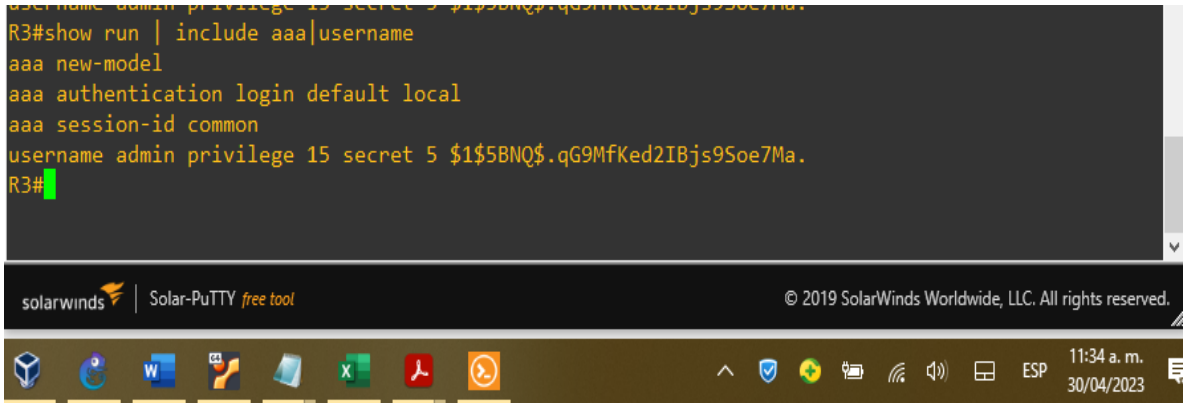
Fuente: autoría propia.

Figura 26. Verificación de seguridad en R2.



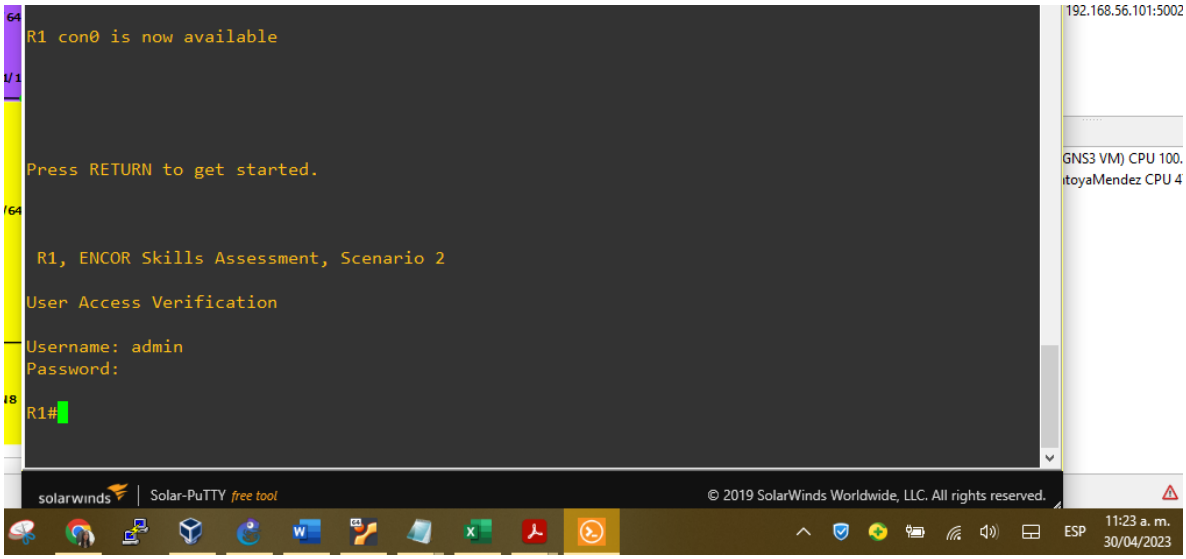
Fuente: autoría propia.

Figura 27. Verificación de seguridad en R3.



Fuente: autoría propia.

Figura 28. Comprobación de solicitud de usuario y clave en R1.



Fuente: autoría propia.

CONCLUSIONES

En el desarrollo de esta actividad del diplomado de profundización CCNP, se logra conocer más a fondo la herramienta de emulación de un entorno de red real, como lo es GNS3 que permite hacer configuraciones muy similares a las un escenario real, esto es importante cuando se realizan las configuraciones, pues cuando se presenta algún error se logra implementar los conocimientos adquiridos para comprender y dar solución a estos.

Se logra aprender el concepto de configuración usando redes multi-VRF, todas las configuraciones que deben hacerse en los dispositivos de capa 3 para que se habilite el direccionamiento entre las subredes tanto IPv4 como IPv6, los comandos que permiten realizar la creacion de las VRFs, asignar el direccionamiento estático, encapsular cada interfaz en la VLAN correspondiente y lograr tener una comunicación exitosa entre las VRF.

De igual manera se logra afianzar conocimientso ya adquiridos, impementando en los dispositivos de capa 2 en la topología, opciones de seguridad tales como, deshabilitar interfaces sin uso, crear enlaces troncales, configurar los puertos para que tengan acceso a la VLAN que corresponde en la topología y que sean de acceso rápido.

También la actividad ayuda a conocer más ampliamente el uso de varias tecnologías, como el caso de EtherChannel, que permite que se agrupen varios puertos en un solo canal lógico y de esta manera los enlaces tienen más robustez y el tráfico que circula por la está será más fluido. Para mi caso, en este paso logré tener una oportunidad de entender mejor su funcionamiento puesto que tuve inconvenientes en esta parte y no lograba habilitar el enlace en uno de los switches, por lo que la comunicación en la VLAN 8 no era posible. Investigando y realizando de nuevo los comandos, configurando en orden cada extremo de las interfaces en cada switch, logré la habilitación del canal y así la comunicación entre los equipos.

BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAlGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAlGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAlGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Virtual Routing and Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAlGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAlGg5JUgUBthk8