

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LEONARDO MENDEZ ACOSTA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LEONARDO MENDEZ ACOSTA

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

DIRECTOR:

JUAN ESTEBAN TAPIAS

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del jurado

Firma del jurado

Bogotá, 04 de mayo de 2023

AGRADECIMIENTOS

Me dirijo a ustedes para expresar mi más sincero agradecimiento por la oportunidad que me brindaron al permitirme participar en el Diplomado De Profundización Cisco. Ha sido una experiencia enriquecedora en todos los sentidos, y estoy muy agradecido por todo el conocimiento que he adquirido durante el tiempo de formación.

A la Universidad Nacional Abierta y a Distancia Quiero destacar la profesionalidad y dedicación de los instructores, quienes con paciencia y claridad explicaron cada uno de los temas, haciendo que el aprendizaje fuera sencillo y ameno. Además, quiero agradecer al equipo organizador por su excelente trabajo en la logística del curso, lo que permitió que todo se desarrollara de manera fluida y sin contratiempos.

CONTENIDO

	Pág.
AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE FIGURAS	7
LISTA DE TABLA.....	8
GLOSARIO	9
RESUMEN.....	10
ABSTRACT.....	10
INTRODUCCIÓN	11
ESCENARIO 1	12
PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DEL DISPOSITIVO Y EL DIRECCIONAMIENTO DE LA INTERFAZ	12
paso 1: cablee la red como se muestra en la topología.....	12
Paso 2: Configure los ajustes básicos para cada dispositivo.....	14
PARTE 2: CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO	19
2.1 En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.	20
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.....	22
2.3 En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.	26
2.4 Verifique la conectividad en cada VRF.	28
ESCENARIO 2.....	30
PARTE 3. CONFIGURAR CAPA 2	30
3.1 En D1, D2 y A1, deshabilite todas las interfaces.	31
3.2 En D1 y D2, configure los enlaces troncales a R1 y R3.	32
3.3 En D1 y A1, configure el EtherChannel.	33
3.4 En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4. 36	
3.5 Verifique la conectividad de PC a PC.....	38

PARTE 4. CONFIGURE SEGURIDAD39
CONCLUSIONES44
BIBLIOGRAFÍA.....45

LISTA DE FIGURAS

	Pág.
Figura 1. Topología de Red	12
Figura 2. Configuración IP en PC1	17
Figura 3. Configuración IP en PC2	18
Figura 4. Configuración IP en PC3	18
Figura 5. Configuración IP en PC4	19
Figura 6. Verificación VRF en ROUTER R1	20
Figura 7. Verificación VRF en ROUTER R2	21
Figura 8. Verificación VRF en ROUTER R3	21
Figura 9. Verificación ip en interfaces en ROUTER R1	23
Figura 10. Verificación ip en interfaces en ROUTER R2	24
Figura 11. Verificación ip en interfaces en ROUTER R3	25
Figura 12. Verificación ip en interface R1	26
Figura 13. Verificación ip en interface R2	27
Figura 14. Verificación ip en interface R3	27
Figura 15. Verificación conectividad en la IP 10.0208.1	28
Figura 16. Verificación conectividad en la IP 2001:db8:acad:208::1	28
Figura 17. Verificación conectividad en la IP 10.0.213.1	29
Figura 18. Verificación conectividad en la IP 2001:db8:acad:2013::1	29
Figura 19. Verificación modo troncal SWITCH D1	32
Figura 20. Verificación modo troncal SWITCH D2	33
Figura 21. Verificación modo troncal SWITCH A1	34
Figura 22. Verificación modo troncal SWITCH D1	35
Figura 23. Verificación modo de acceso SWITCH D1	36
Figura 24. Verificación modo de acceso SWITCH A1.....	37
Figura 25. Verificación modo de acceso SWITCH D2	37
Figura 26. Verificación modo de acceso SWITCH D2	38
Figura 27. Ping de conectividad PC1 a PC2	38
Figura 28. Ping de conectividad PC3 a PC4	39
Figura 29. Configuración de Seguridad en ROUTER R1	40
Figura 30. Configuración de Seguridad en ROUTER R2	41
Figura 31. Configuración de Seguridad en ROUTER R3	41
Figura 32. Configuración de Seguridad en SWITCH D1	42
Figura 33. Configuración de Seguridad en SWITCH D2	43
Figura 34. Configuración de Seguridad en SWITCH A1	43

LISTA DE TABLA

	Pág.
Tabla 1. Direccionamiento IP	13
Tabla 2. Configuración Capa 2	30
Tabla 3. Configuración De Seguridad.....	39

GLOSARIO

DHCP: Protocolo de configuración dinámica de host, que se utiliza para asignar direcciones IP a dispositivos de una red.

Enrutador: Dispositivo que se utiliza para conectar múltiples redes y dirigir el tráfico de información entre ellas.

Firewall: Dispositivo de seguridad que se encarga de proteger una red contra accesos no autorizados.

PROTOCOLO: Conjunto de reglas y procedimientos que permiten la comunicación entre dispositivos de una red.

Router: Dispositivo que permite conectar múltiples dispositivos en una red y gestionar el tráfico de información.

VLAN: Red de área local virtual que permite segmentar una red física en varias subredes lógicas.

RESUMEN

El trabajo final del Diplomado De Profundización Cisco es una oportunidad para que los participantes muestren sus habilidades y conocimientos en la implementación de soluciones de red de alta tecnología utilizando equipos virtuales mediante el software GN3, creando vlans, configuración de servidor DHCP, la implementación de switch, router y firewall.

Consiguiendo diseñar, y simular redes escalables con la implementación de protocolos de comunicaciones entre equipos, protocolos de enrutamiento, logrando la solución a posibles fallas que se puedan presentar en el campo laboral

Palabras Clave: Cisco, Ccnp, Conmutación, Enrutamiento, Redes, Telecomunicaciones

ABSTRACT

The final work of the Cisco Deepening Diploma is an opportunity for participants to show their skills and knowledge in the implementation of high-tech network solutions using virtual teams using GN3 software, creating vlans, DHCP server configuration, switch implementation , router and firewall.

Getting to design, and simulate scalable networks with the implementation of communication protocols between teams, routing protocols, achieving the solution to possible failures that may occur in the workplace

Keywords: Cisco, Ccnp, Switching, Routing, Networks, Telecommunications

INTRODUCCIÓN

El Diplomado de Profundización Cisco es un programa de formación en redes de datos y comunicaciones de dispositivos activos, que brinda profundizar sus conocimientos en redes y aumentar sus habilidades en la implementación y gestión de soluciones de red utilizando los equipos y tecnologías de última generación.

Logrando que el estudiante cuente con las capacidades de diseñar, planificar y realizar redes con escalabilidad con los protocolos de comunicación IPV4 y IPV6, en base a los protocolos de seguridad necesarios para brindar a la red seguridad, disponibilidad y escalabilidad, de igual forma el diplomado es desarrollado en dos fases, por una lado se encuentra la parte teoría, en donde se refuerzan los conocimiento básicos con respecto a dispositivos activos de red y por otro lado tenemos la configuración de redes en entornos virtuales controlados que permitan la configuración de diferentes parámetros para practicar la ejecución de comando dentro de cada dispositivos que integra la red.

En el desarrollo del diplomado se aborda la temática desde los conceptos básicos en dispositivos hasta el punto de determinar las diferentes fallas que se puedan presentar en una red de una organización o empresa, llevando al ingeniero a poner en práctica todos los conocimientos adquiridos a lo largo de la carrera.

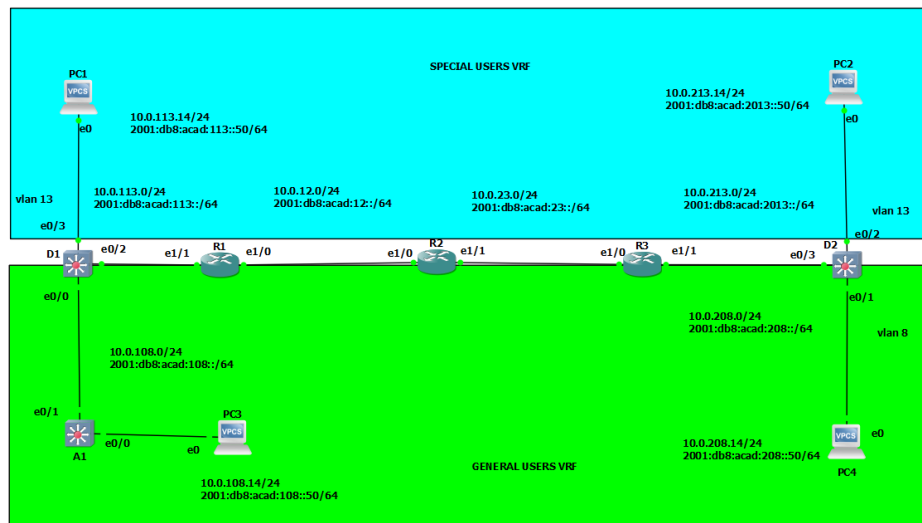
ESCENARIO 1

PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DEL DISPOSITIVO Y EL DIRECCIONAMIENTO DE LA INTERFAZ

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.

Figura 1. Topología de Red



Fuente: propia

Tabla 1. Direccionamiento IP

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
R1	E1/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.4/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.4/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.4/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.4/24	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	10.0.113.14/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.14/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.14/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.14/24	2001:db8:acad:208::50/64	EUI-64

Fuente: propia

Nota: las letras “X, Y, Z” corresponden a los últimos tres dígitos de su número de cédula. Leonardo Mendez Acosta, cc: 1054093040, se procede a remplazar el número de cero (0) por el número (1), quedando el número cc: 1054093141

PASO 2: CONFIGURE LOS AJUSTES BÁSICOS PARA CADA DISPOSITIVO.

a. 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.

ROUTER R1

```
Enable // Activa el modo privilegiado
configure terminal // Accede al modo de configuración
hostname R1 // nombre del equipo
ipv6 unicast-routing // habilita el routing IPv6 en el router.
no ip domain lookup // Habilita la traducción de nombre a dirección
basado en DNS del host
banner motd # R1, ENCOR SKills Assessment, Scenario 2 # // mensaje
emergente hay iniciar el dispositivo
line console 0 // Entra en la configuración de la consola.
exec-time 0 0 // establece el tiempo de espera inactivo
de la sesión remota
logging synchronous. // Sincroniza los mensajes no solicitados y el
resultado de la depuración
Exit // cierra la sesión del usuario actual
```

ROUTER R2

```
Enable // Activa el modo privilegiado
configure terminal // Accede al modo de configuración
hostname R2 // nombre del equipo
ipv6 unicast-routing // habilita el routing IPv6 en el router.
no ip domain lookup // Habilita la traducción de nombre a dirección
basado en DNS del host
banner motd # R2, ENCOR SKills Assessment, Scenario 2 # //mensaje emergente
hay iniciar el dispositivo
line console 0 // Entra en la configuración de la consola.
exec-time 0 0 // establece el tiempo de espera inactivo de la
sesión remota
logging synchronous. // Sincroniza los mensajes no solicitados y el
resultado de la depuración
Exit // cierra la sesión del usuario actual
```

ROUTER R3

```
Enable // Activa el modo privilegiado
configure terminal // Accede al modo de configuración
hostname R3 // nombre del equipo
ipv6 unicast-routing // habilita el routing IPv6 en el router.
no ip domain lookup // Habilita la traducción de nombre a dirección
basado en DNS del host
banner motd # R3, ENCOR Skills Assessment, Scenario 2 # //mensaje emergente
hay iniciar el dispositivo
line console 0 // Entra en la configuración de la consola.
exec-time 0 0 // establece el tiempo de espera inactivo
de la sesión remota
logging synchronous. // Sincroniza los mensajes no solicitados y
el resultado de la depuración
Exit // cierra la sesión del usuario actual
```

SWITCH D1

```
Enable // Activa el modo privilegiado
configure terminal // Accede al modo de configuración
hostname D1 // nombre del equipo
ip routing // gestiona rutas estáticas en la tabla de
direccionamiento
ipv6 unicast-routing // habilita el routing IPv6 en el router
no ip domain lookup //Habilita la traducción de nombre a dirección
basado en DNS del host
banner motd # D1, ENCOR Skills Assessment, Scenario 2 # //mensaje emergente
hay iniciar el dispositivo
line con 0 // Entra en la configuración de la consola.
exec-timeout 0 0 // establece el tiempo de espera inactivo
logging synchronous // Sincroniza los mensajes no solicitados y
el resultado de la depuración
exit // cierra la sesión del usuario actual
vlan 8 //se nombre y crea una vlan
name general-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual
vlan 13 //se nombre y crea una vlan
name special-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual
```

SWITCH D2

```
Enable // Activa el modo privilegiado
configure terminal // Accede al modo de configuración
hostname D2 // nombre del equipo
ip routing // gestiona rutas estáticas en la tabla de
direccionamiento
ipv6 unicast-routing // habilita el routing IPv6 en el router
no ip domain lookup //Habilita la traducción de nombre a
dirección basado en DNS del host
banner motd # D2, ENCOR Skills Assessment, Scenario 2# //mensaje emergente
hay iniciar el dispositivo
line con 0 // Entra en la configuración de la consola.
exec-timeout 0 0 // establece el tiempo de espera inactivo
logging synchronous // Sincroniza los mensajes no solicitados y
el resultado de la depuración
exit // cierra la sesión del usuario actual
vlan 8 //se nombre y crea una vlan
name general-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual
vlan 13 //se nombre y crea una vlan
name special-users // se asigna nombre a la vlan
```

SWITCH A1

```
Enable // Activa el modo privilegiado
configure terminal // Accede al modo de configuración
hostname D1 // nombre del equipo
ip routing // gestiona rutas estáticas en la tabla de
direccionamiento
ipv6 unicast-routing // habilita el routing IPv6 en el router
no ip domain lookup //Habilita la traducción de nombre a dirección
basado en DNS del host
banner motd # D1, ENCOR Skills Assessment, Scenario 2 # //mensaje emergente
hay iniciar el dispositivo
line con 0 // Entra en la configuración de la consola.
exec-timeout 0 0 // establece el tiempo de espera inactivo
logging synchronous // Sincroniza los mensajes no solicitados y
el resultado de la depuración
exit // cierra la sesión del usuario actual
vlan 8 //se nombre y crea una vlan
name general-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual
vlan 13 //se nombre y crea una vlan
name special-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual
```

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

ROUTER R1

```
Copy running-config startup-config
configuración inicial
```

// Guarda la configuración actual como

ROUTER R2

```
Copy running-config startup-config
configuración inicial
```

// Guarda la configuración actual como

ROUTER R3

```
Copy running-config startup-config
configuración inicial
```

// Guarda la configuración actual como

SWITCH D1

```
Copy running-config startup-config
configuración inicial
```

// Guarda la configuración actual como

SWITCH D2

```
Copy running-config startup-config
configuración inicial
```

// Guarda la configuración actual como

SWITCH A1

```
Copy running-config startup-config
configuración inicial
```

// Guarda la configuración actual como

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

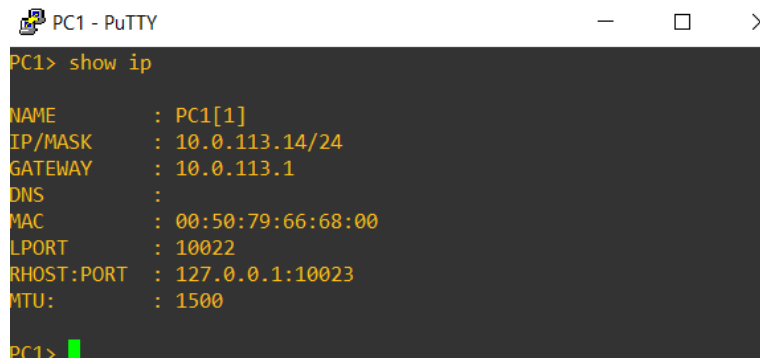
COMPUTADOR PC1

```
Ip 10.0.113.14/24 10.0.113.1
Ip 2001:db8:acad:113::50/64
save
```

// asignación de dirección IPV4

// asignación de dirección IPV6

Figura 2. Configuración IP en PC1



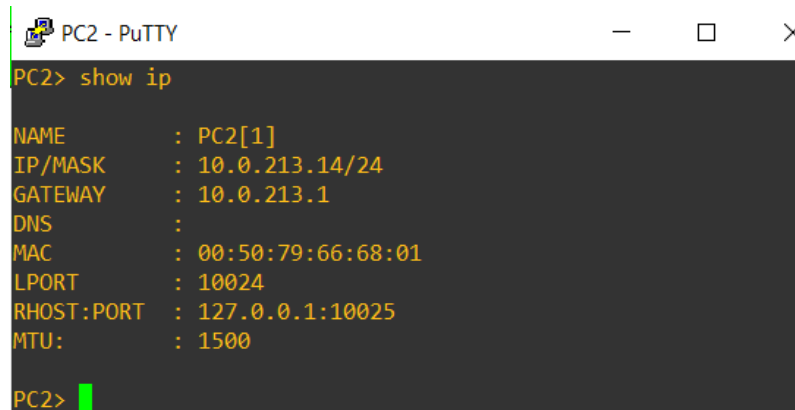
```
PC1 - PuTTY
PC1> show ip
NAME       : PC1[1]
IP/MASK    : 10.0.113.14/24
GATEWAY    : 10.0.113.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 10022
RHOST:PORT : 127.0.0.1:10023
MTU        : 1500
PC1>
```

Fuente: propia

COMPUTADOR PC2

```
Ip 10.0.213.14/24 10.0.213.1 // asignación de dirección IPV4  
Ip 2001:db8:acad:213::50/64 // asignación de dirección IPV6  
save
```

Figura 3. Configuración IP en PC2

A screenshot of a PuTTY terminal window titled "PC2 - PuTTY". The terminal shows the output of the "show ip" command. The output is as follows:

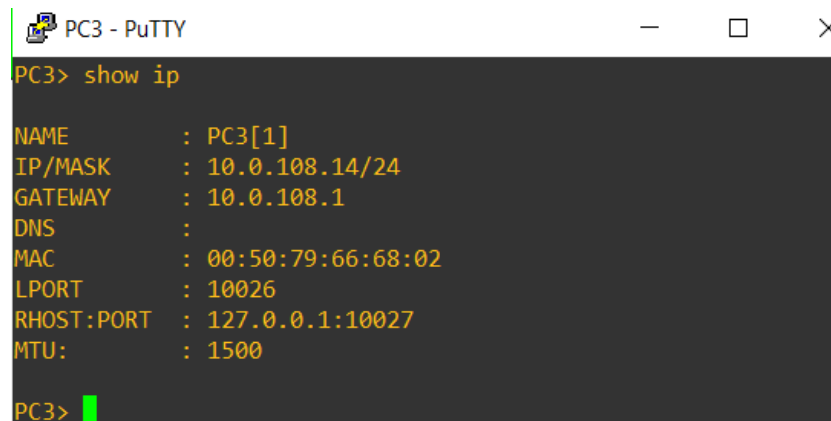
```
PC2> show ip  
  
NAME       : PC2[1]  
IP/MASK    : 10.0.213.14/24  
GATEWAY    : 10.0.213.1  
DNS        :  
MAC        : 00:50:79:66:68:01  
LPORT     : 10024  
RHOST:PORT : 127.0.0.1:10025  
MTU       : 1500  
  
PC2>
```

Fuente: propia

COMPUTADOR PC3

```
IP 10.0.108.14/24 10.0.108.1 // asignación de dirección IPV4  
IP 2001:db8:acad:108::50/64 // asignación de dirección IPV6  
Sabe
```

Figura 4. Configuración IP en PC3

A screenshot of a PuTTY terminal window titled "PC3 - PuTTY". The terminal shows the output of the "show ip" command. The output is as follows:

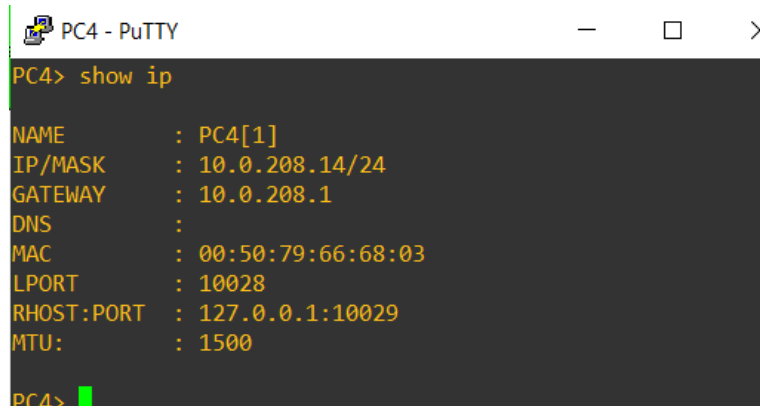
```
PC3> show ip  
  
NAME       : PC3[1]  
IP/MASK    : 10.0.108.14/24  
GATEWAY    : 10.0.108.1  
DNS        :  
MAC        : 00:50:79:66:68:02  
LPORT     : 10026  
RHOST:PORT : 127.0.0.1:10027  
MTU       : 1500  
  
PC3>
```

Fuente: propia

COMPUTADOR PC4

```
IP 10.0.208.14/24 10.0.208.1 // asignación de dirección IPV4
IP 2001:db8:acad:208::50/64 //asignación de dirección IPV6
save
```

Figura 5. Configuración IP en PC4



```
PC4 - PuTTY
PC4> show ip
NAME       : PC4[1]
IP/MASK    : 10.0.208.14/24
GATEWAY    : 10.0.208.1
DNS        :
MAC        : 00:50:79:66:68:03
LPORT      : 10028
RHOST:PORT : 127.0.0.1:10029
MTU        : 1500
PC4>
```

Fuente: propia

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.

Sus tareas de configuración son las siguientes:

Tarea	Tarea	Especificación
2.1	En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología	Configure dos VRF: <ul style="list-style-type: none">• Usuarios generales• Usuarios especiales Los VRF deben soportar 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 enrutadores utilizarán Router-On-A-Stick en sus interfaces e1/1.x para admitir la separación de los VRF. Sub-interfaz 1: <ul style="list-style-type: none">• En el VRF de Usuarios Especiales• Encapsulación Use dot1q• IPv4 e IPv6 GUA y direcciones locales de enlace• Habilitar las interfaces Subinterfaz 2: <ul style="list-style-type: none">• En el VRF de Usuarios Generales• Encapsulación Usedot1q

Tarea	Tarea	Especificación
		<ul style="list-style-type: none"> • 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 a R3: <ul style="list-style-type: none"> • ping vrf Usuarios generales 10.0.208.Z • ping vrf Usuarios generales 2001:db8:acad:208::1 • ping vrf Usuarios especiales 10.0.213.Z • ping vrf Usuarios especiales 2001:db8:acad:213::1

Fuente: propia

2.1 EN R1, R2 Y R3, CONFIGURE VRF-LITE VRF COMO SE MUESTRA EN EL DIAGRAMA DE TOPOLOGÍA.

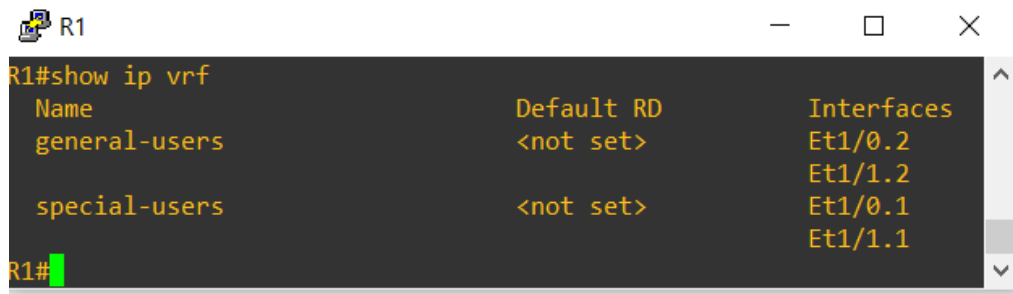
ROUTER R1

```

vrf definition general-users           // crea una vrf
description general-users             // describe la vrf creada
address-family ipv4                   // permite habilitar vrf con ipv4
address-family ipv6                   // permite habilitar vrf con ipv6
exit                                   // cierra la sesión del usuario actual
vrf definition special-users          // crea una vrf
address-family ipv4                   // permite habilitar vrf con ipv4
address-family ipv6                   // permite habilitar vrf con ipv6
exit                                   // cierra la sesión del usuario actual
do show vrf                           // muestra las vrf creadas

```

Figura 6. Verificación VRF en ROUTER R1



```

R1#show ip vrf
Name                Default RD          Interfaces
-----                -
general-users       <not set>          Et1/0.2
                   <not set>          Et1/1.2
special-users       <not set>          Et1/0.1
                   <not set>          Et1/1.1
R1#

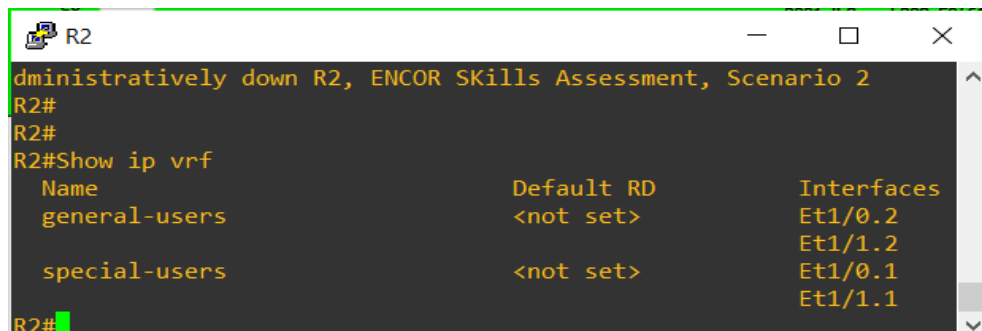
```

Fuente: propia

ROUTER R2

```
vrf definition general-users // crea una vrf
address-family ipv4 // permite habilitar vrf con ipv4
address-family ipv6 // permite habilitar vrf con ipv6
exit // cierra la sesión del usuario
vrf definition special-users // crea una vrf
address-family ipv4 // permite habilitar vrf con ipv4
address-family ipv6 // permite habilitar vrf con ipv6
exit // cierra la sesión del usuario
do show vrf // muestra las vrf creadas
```

Figura 7. Verificación VRF en ROUTER R2



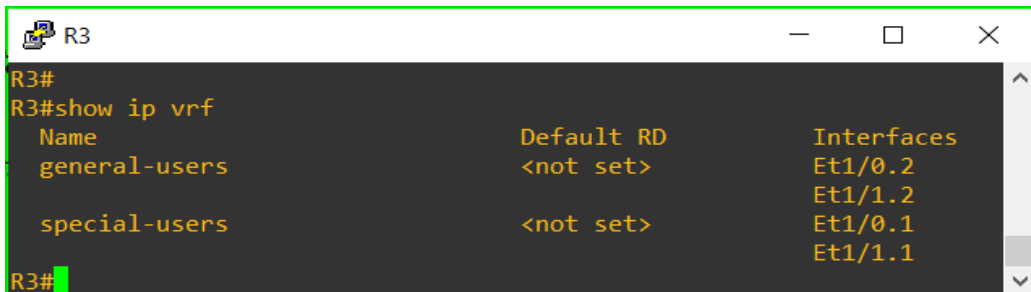
```
R2
R2#
R2#
R2#Show ip vrf
Name                Default RD          Interfaces
general-users       <not set>          Et1/0.2
                    <not set>          Et1/1.2
special-users       <not set>          Et1/0.1
                    <not set>          Et1/1.1
R2#
```

Fuente: propia

ROUTER R3

```
vrf definition general-users // crea una vrf
address-family ipv4 // permite habilitar vrf con ipv4
address-family ipv6 // permite habilitar vrf con ipv6
exit // cierra la sesión del usuario
vrf definition special-users // crea una vrf
address-family ipv4 // permite habilitar vrf con ipv4
address-family ipv6 // permite habilitar vrf con ipv6
exit // cierra la sesión del usuario
do show vrf // muestra las vrf creadas
```

Figura 8. Verificación VRF en ROUTER R3



```
R3
R3#
R3#show ip vrf
Name                Default RD          Interfaces
general-users       <not set>          Et1/0.2
                    <not set>          Et1/1.2
special-users       <not set>          Et1/0.1
                    <not set>          Et1/1.1
R3#
```

Fuente: propia

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.

ROUTER R1

```
interface ethernet 1/0 // ingresa a la interfaz
no shutdown // enciende la interfaz
interface ethernet 1/0.1 // ingresa a la subinterfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 13 // se encapsula los mensajes
vrf forwarding special-users // reenvía a la VRF special-users
ip address 10.0.12.1 255.255.255.0 // asigna dirección IPV4
ipv6 address 2001:db8:acad:12::1/64 // asigna dirección IPV6
ipv6 address fe80::1:1 link-local // asigna dirección IPV6
exit // cierra la sesión del usuario actual
interface Ethernet 1/0.2 // ingresa a la interfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 8 // se encapsula los mensajes
vrf forwarding general-users // reenvía a la VRF general-users
Ip address 10.0.12.1 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:12::1/64 // asigna dirección IPV6
Ipv6 address fe80::1:2 link-local // asigna dirección IPV6
Exit // cierra la sesión del usuario actual

interface Ethernet 1/1 // ingresa a la interfaz
no shutdown // enciende la interfaz
interface Ethernet 1/1.1 // ingresa a la subinterfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 13 // se encapsula los mensajes
vrf forwarding special-users // reenvía a la VRF general-users
Ip address 10.0.113.1 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:113::1/64 // asigna dirección IPV6
Ipv6 address fe80::1:3 link-local // asigna dirección IPV6
Exit // cierra la sesión del usuario actual
interface Ethernet 1/1.2 // ingresa a la interfaz
no shutdown // enciende la interfaz
Encapsulation dot1q 8 // se encapsula los mensajes
Vrf forwarding general-users // reenvía a la VRF general-users
Ip address 10.0.108.1 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:108::1/64 // asigna dirección IPV6
Ipv6 address fe80::1:4 link-local // asigna dirección IPV6
Exit // cierra la sesión del usuario
show ip vrf int //muestra las vrf activas
```

Figura 9. Verificación ip en interfaces en ROUTER R1

```

R1#show ip vrf interfaces
Interface      IP-Address      VRF              Protoco
-----
Et1/0.2        10.0.12.1       general-users     up
Et1/1.2        10.0.108.1     general-users     up
Et1/0.1        10.0.12.1       special-users     up
Et1/1.1        10.0.113.1     special-users     up
  
```

Fuente: propia

ROUTER R2

```

interface ethernet 1/0                // ingresa a la interfaz
no shutdown                          // enciende la interfaz
interface ethernet 1/0.1              // ingresa a la subinterfaz
no shutdown                          // enciende la interfaz
encapsulation dot1Q 13                // se encapsula los mensajes
vrf forwarding special-users          // reenvía a la VRF general-users
Ip address 10.0.12.4 255.255.255.0    // asigna dirección IPV4
Ipv6 address 2001:db8:acad:12::2/64   // asigna dirección IPV6
Ipv6 address fe80::2:1 link-local     // asigna dirección IPV6
Exit                                  // cierra la sesión del usuario actual
  
```

```

interface Ethernet1/0.2              // ingresa a la interfaz
no shutdown                          // enciende la interfaz
encapsulation dot1Q 8                // se encapsula los mensajes
vrf forwarding general-users          // reenvía a la VRF general-users
Ip address 10.0.12.4 255.255.255.0    // asigna dirección IPV4
Ipv6 address 2001:db8:acad:12::2/64   // asigna dirección IPV6
Ipv6 address fe80::2:2 link-local     // asigna dirección IPV6
Exit
  
```

```

interface ethernet 1/1                // ingresa a la interfaz
no shutdown                          // enciende la interfaz
interface Ethernet1/1.1              // ingresa a la subinterfaz
no shutdown                          // enciende la interfaz
encapsulation dot1Q 13                // se encapsula los mensajes
vrf forwarding special-users          // reenvía a la VRF general-users
Ip address 10.0.23.4 255.255.255.0    // asigna dirección IPV4
Ipv6 address 2001:db8:acad:23::2/64   // asigna dirección IPV6
Ipv6 address fe80::2:3 link-local     // asigna dirección IPV6
Exit                                  // cierra la sesión del usuario actual
  
```

```

interface Ethernet1/1.2 // ingresa a la interfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 8 // se encapsula los mensajes
vrf forwarding general-users // reenvía a la VRF general-users
Ip address 10.0.23.4 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:23::2/64 // asigna dirección IPV6
Ipv6 address fe80::2:4 link-local // asigna dirección IPV6
Exit // cierra la sesión del usuario
show ip vrf int // muestra las vrf activas

```

Figura 10. Verificación ip en interfaces en ROUTER R2



```

R2#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.4       general-users     up
Et1/1.2        10.0.23.4       general-users     up
Et1/0.1        10.0.12.4       special-users     up
Et1/1.1        10.0.23.4       special-users     up
R2#

```

Fuente: propia

ROUTER R3

```

interface ethernet 1/0 // ingresa a la interfaz
no shutdown // enciende la interfaz
interface ethernet 1/0.1 // ingresa a la subinterfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 13 // se encapsula los mensajes
vrf forwarding special-users // reenvía a la VRF general-users
Ip address 10.0.23.1 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:23::3/64 // asigna dirección IPV6
Ipv6 address fe80::3:1 link-local // asigna dirección IPV6
Exit // cierra la sesión del usuario

```

```

interface Ethernet1/0.2 // ingresa a la subinterfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 8 // se encapsula los mensajes
vrf forwarding general-users // reenvía a la VRF general-users
Ip address 10.0.23.1 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:23::3/64 // asigna dirección IPV6
Ipv6 address fe80::3:2 link-local // asigna dirección IPV6
Exit // cierra la sesión del usuario

```

```

interface Ethernet1/1 // ingresa a la interfaz
no shutdown // enciende la interfaz
interface Ethernet1/1.1 // ingresa a la subinterfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 13 // se encapsula los mensajes
vrf forwarding special-users // reenvía a la VRF general-users
Ip address 10.0.213.1 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:213::1/64 // asigna dirección IPV6
Ipv6 address fe80::3:3 link-local // asigna dirección IPV6
Exit // cierra la sesión del usuario

interface Ethernet1/1.2 // ingresa a la subinterfaz
no shutdown // enciende la interfaz
encapsulation dot1Q 8 // se encapsula los mensajes
vrf forwarding general-users // reenvía a la VRF general
Ip address 10.0.208.1 255.255.255.0 // asigna dirección IPV4
Ipv6 address 2001:db8:acad:208::1/64 // asigna dirección IPV6
Ipv6 address fe80::3:4 link-local // asigna dirección IPV6
End // cierra la sesión del usuario
show ip vrf int // muestra las vrf activas

```

Figura 11. Verificación ip en interfaces en ROUTER R3

```

R3#
R3#show ip vrf interface
Interface          IP-Address      VRF
-----
Et1/0.2            10.0.23.1      general-users
  up
Et1/1.2            10.0.208.1     general-users
  up
Et1/0.1            10.0.23.1      special-users
  up
Et1/1.1            10.0.213.1     special-users
  up
R3#

```

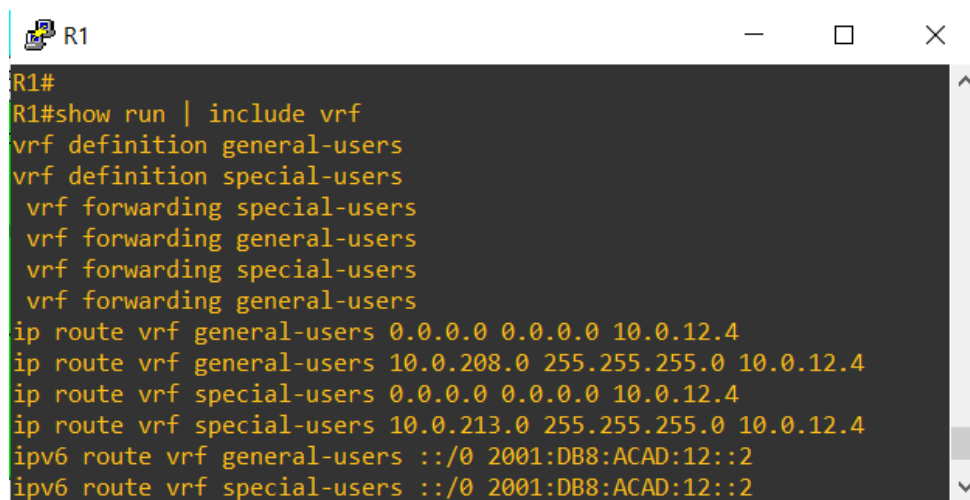
Fuente: propia

2.3 EN R1 Y R3, CONFIGURE LAS RUTAS ESTÁTICAS PREDETERMINADAS QUE APUNTAN A R2.

ROUTER R1

```
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.4 // se configura ruta
estatica es special-users en IPV4
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.4 // se configura ruta
estatica es general-users en IPV4
ipv6 route vrf special-users ::/0 2001:db8:acad:12::2 // se configura ruta
estatica es general-users en IPV6
ipv6 route vrf general-users ::/0 2001:db8:acad:12::2 // se configura ruta
estatica es general-users en IPV6
```

Figura 12. Verificación ip en interface R1



```
R1#
R1#show run | include vrf
vrf definition general-users
vrf definition special-users
 vrf forwarding special-users
 vrf forwarding general-users
vrf forwarding special-users
vrf forwarding general-users
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.4
ip route vrf general-users 10.0.208.0 255.255.255.0 10.0.12.4
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.4
ip route vrf special-users 10.0.213.0 255.255.255.0 10.0.12.4
ipv6 route vrf general-users ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf special-users ::/0 2001:DB8:ACAD:12::2
```

Fuente: propia

ROUTER R2

```
ip route vrf special-users 10.0.113.0 255.255.255.0 10.0.12.1 // se configura
ruta estatica es special-users en IPV4
ip route vrf special-users 10.0.213.0 255.255.255.0 10.0.23.1 // se configura
ruta estatica es special-users en IPV4
ip route vrf general-users 10.0.108.0 255.255.255.0 10.0.12.1 // se configura
ruta estatica es general-users en IPV4
ip route vrf general-users 10.0.208.0 255.255.255.0 10.0.23.1 // se configura
ruta estatica es general-users en IPV4
ipv6 route vrf special-users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1 //
se configura ruta estatica es special-users en IPV6
ipv6 route vrf special-users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3 //
se configura ruta estatica es special-users en IPV6
```

```

ipv6 route vrf general-users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1 //
se configura ruta estatica es general-users en IPV6
ipv6 route vrf general-users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3 //
se configura ruta estatica es general-users en IPV6

```

Figura 13. Verificación ip en interface R2

```

R2#show run | include vrf
vrf definition general-users
vrf definition special-users
vrf forwarding special-users
vrf forwarding general-users
vrf forwarding special-users
vrf forwarding general-users
ip route vrf general-users 10.0.108.0 255.255.255.0 10.0.12.1
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 10.0.12.1
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 special-users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:
12::1
ipv6 route vrf general-users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:
23::3
ipv6 route vrf special-users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:
23::3

```

Fuente: propia

ROUTER R3

```

ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.23.4 // se configura ruta
estatica es special-users en IPV4
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.23.4 // se configura ruta
estatica es general-users en IPV4
ipv6 route vrf special-users ::/0 2001:DB8:ACAD:23::2 // se
configura ruta estatica es special-users en IPV6
ipv6 route vrf general-users ::/0 2011:DB8:ACAD:23::2 // se
configura ruta estatica es general-users en IPV6

```

Figura 14. Verificación ip en interface R3

```

R3#show run | include vrf
vrf definition general-users
vrf definition special-users
vrf forwarding special-users
vrf forwarding general-users
vrf forwarding special-users
vrf forwarding general-users
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.23.4
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.23.4
ipv6 route vrf general-users ::/0 2011:DB8:ACAD:23::2
ipv6 route vrf special-users ::/0 2001:DB8:ACAD:23::2
R3#

```

Fuente: propia

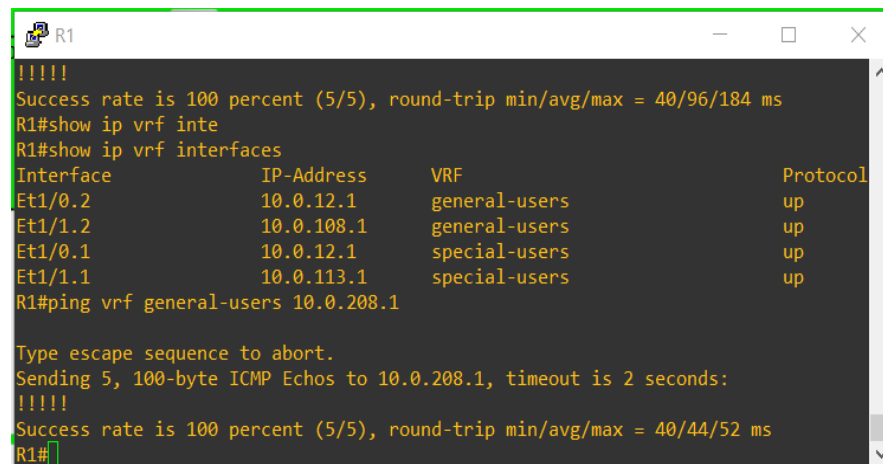
2.4 VERIFIQUE LA CONECTIVIDAD EN CADA VRF.

Desde R1, verifique la conectividad a R3:

- **ping vrf Usuarios generales 10.0.208.Z**

ping vrf general-users 10.0.208.1 // ping de conectividad en IPV4

Figura 15. Verificación conectividad en la IP 10.0208.1



```
R1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/96/184 ms
R1#show ip vrf inte
R1#show ip vrf interfaces
Interface          IP-Address      VRF              Protocol
Et1/0.2            10.0.12.1       general-users     up
Et1/1.2            10.0.108.1      general-users     up
Et1/0.1            10.0.12.1       special-users     up
Et1/1.1            10.0.113.1      special-users     up
R1#ping vrf general-users 10.0.208.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/44/52 ms
R1#
```

Fuente: propia

- **ping vrf Usuarios generales 2001:db8:acad:208::1**

ping vrf general-users 2001:db8:acad:208::1 // ping de conectividad en IPV6

Figura 16. Verificación conectividad en la IP 2001:db8:acad:208::1



```
R1
^208::1
% Invalid input detected at '^' marker.
R1#
R1#
R1#ping vrf general-users 2001:db8:acad:208::1

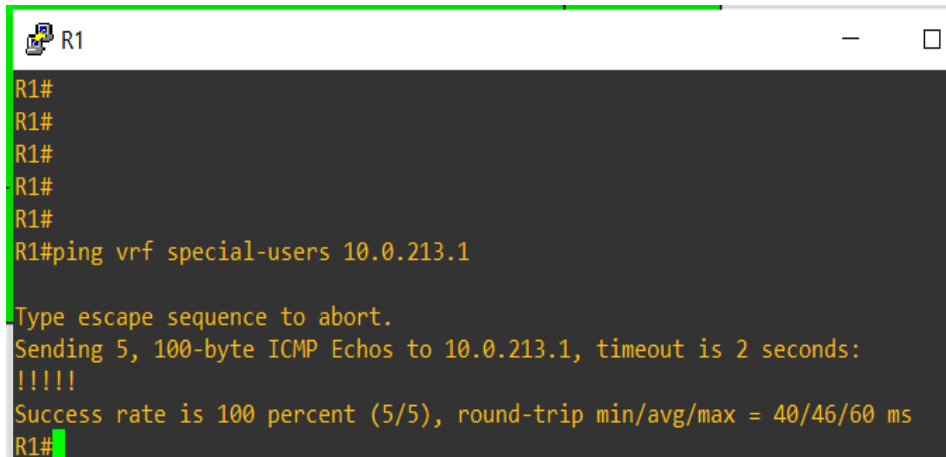
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
.....
Success rate is 0 percent (5/5)
R1#
```

Fuente: propia

- ping vrf Usuarios especiales 10.0.213.Z

```
ping vrf special-users 10.0.213.1 // ping de conectividad en IPV4
```

Figura 17. Verificación conectividad en la IP 10.0.213.1



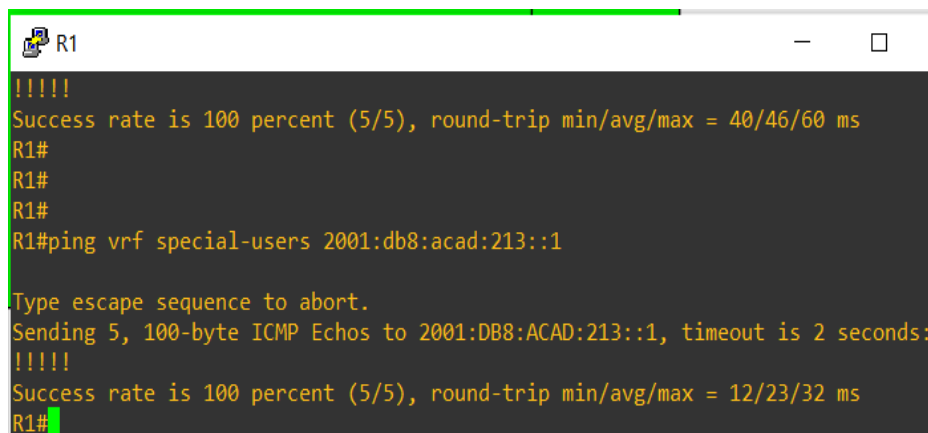
```
R1#  
R1#  
R1#  
R1#  
R1#  
R1#ping vrf special-users 10.0.213.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.213.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/46/60 ms  
R1#
```

Fuente: propia

- ping vrf Usuarios especiales 2001:db8:acad:213::1

```
ping vrf special-users 2001:db8:acad:213::1 // ping de conectividad en IPV6
```

Figura 18. Verificación conectividad en la IP 2001:db8:acad:213::1



```
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/46/60 ms  
R1#  
R1#  
R1#  
R1#ping vrf special-users 2001:db8:acad:213::1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/23/32 ms  
R1#
```

Fuente: propia

ESCENARIO 2

PARTE 3. CONFIGURAR CAPA 2

Tabla 2. Configuración Capa 2

Tarea	Tarea	Especificación
3.1	En D1, D2 y A1, deshabilite todas las interfaces.	En D1 y D2, apague G1/0/1 a G1/0/24. En A1, apague F0/1 – F0/24, G0/1 – G0/2.
3.2	En D1 y D2, configure los enlaces troncales a R1 y R3.	Configure y habilite el enlace G1/0/11 como enlace troncal.
3.3	En D1 y A1, configure el EtherChannel.	En D1, configure y habilite: <ul style="list-style-type: none">• Interfaz G1/0/5 y G1/0/6• Canal de puerto 1 usando PAgP En A1, configure habilitar: <ul style="list-style-type: none">• Interfaz F0/1 y F0/2• Canal de puerto 1 usando PAgP
3.4	En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.	Configure and enable the access ports as follows: <ul style="list-style-type: none">• 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 access port in VLAN 8 and enable Portfast.
3.5	Verifique la conectividad de PC a PC.	Desde la PC1, verifique la conectividad IPv4 e IPv6 a la PC2. Desde la PC3, verifique la conectividad IPv4 e IPv6 a la PC4.

Fuente: propia

3.1 EN D1, D2 Y A1, DESHABILITE TODAS LAS INTERFACES.

SWITCH D1

```
Configure terminal // Accede al modo de configuración
interface range e1/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
interface range e2/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
interface range e3/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
```

SWITCH D2

```
Configure terminal // Accede al modo de configuración
Interface e0/0 // ingresa a la interfaz
Shutdown // apaga la interfaz
Exit // cierra la sesión del usuario actual
interface range e1/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
interface range e2/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
interface range e3/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
```

SWITCH A1

```
Configure terminal // Accede al modo de configuración
interface e0/3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
interface range e1/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
interface range e2/0-3 // ingresa a un rango de interfaces
shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual
interface range e3/0-3 // ingresa a un rango de interfaces
```

```

shutdown // apaga la interfaz
exit // cierra la sesión del usuario actual

```

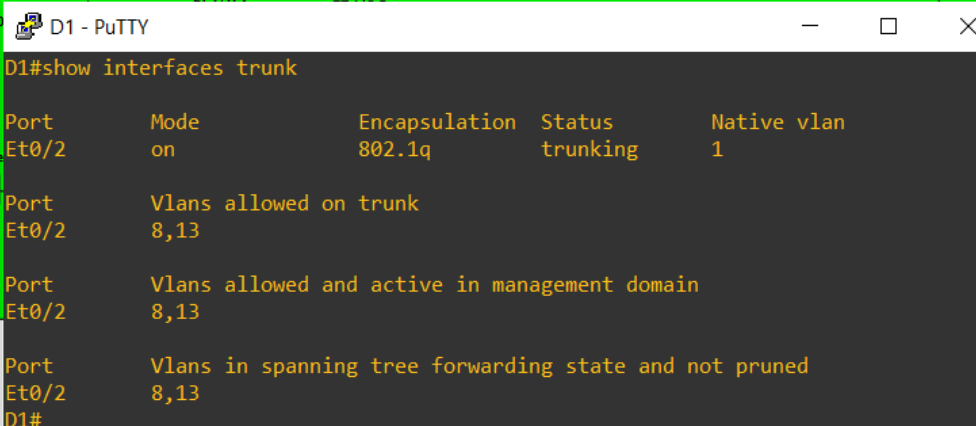
3.2 EN D1 Y D2, CONFIGURE LOS ENLACES TRONCALES A R1 Y R3. SWITCH D1

```

Configure terminal // Accede al modo de configuración
Vlan 13 // crea la VLAN 13
Name Special-Users // nombre de la VLAN creada
Exit // cierra la sesión del usuario actual
Vlan 8 // crea la VLAN 8
name General-Users // nombre de la VLAN creada
exit // cierra la sesión del usuario actual
interface ethernet 0/2 // ingresa a la interfaz
switchport trunk encapsulation dot1q // se encapsula los mensajes
switchport mode trunk // se activa el modo troncal
switchport trunk allowed vlan 13 // activa el modo para el paso de la
VLAN 13
switchport trunk allowed vlan add 8 // activa el modo para el paso de la VLAN
8

```

Figura 19. Verificación modo troncal SWITCH D1



```

D1#show interfaces trunk

Port      Mode           Encapsulation  Status        Native vlan
Et0/2     on             802.1q         trunking      1

Port      Vlans allowed on trunk
Et0/2     8,13

Port      Vlans allowed and active in management domain
Et0/2     8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/2     8,13
D1#

```

Fuente: propia

SWITCH D2

```

Configure terminal // Accede al modo de configuración
Vlan 13 // crea la VLAN 13
Name Special-Users // nombre de la VLAN creada
Exit // cierra la sesión del usuario actual
Vlan 8 // crea la VLAN 8

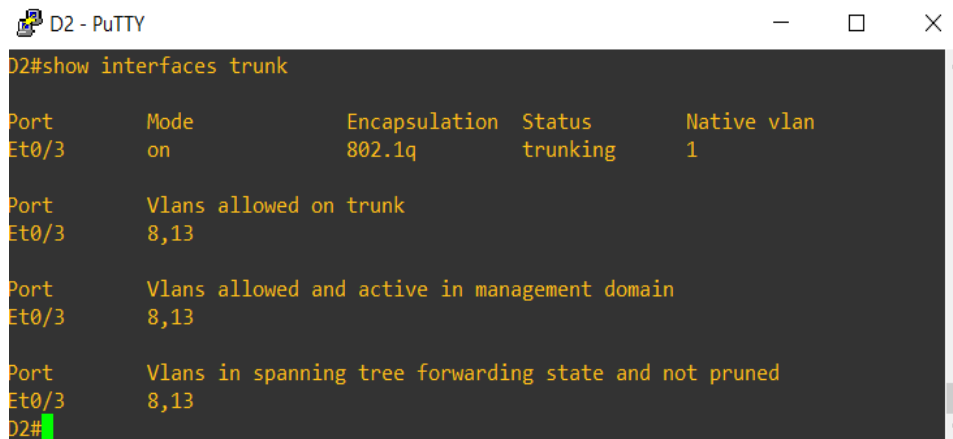
```

```

name General-Users // nombre de la VLAN creada
exit // cierra la sesión del usuario actual
interface ethernet 0/3 // ingresa a la interfaz
switchport trunk encapsulation dot1q // se encapsula los mensajes
switchport mode trunk // se activa el modo troncal
switchport trunk allowed vlan 13 // activa el modo para el paso de la
VLAN 13
switchport trunk allowed vlan add 8 // activa el modo para el paso de la VLAN
8

```

Figura 20. Verificación modo troncal SWITCH D2



```

D2 - PuTTY
D2#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Et0/3     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Et0/3     8,13

Port      Vlans allowed and active in management domain
Et0/3     8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/3     8,13
D2#

```

Fuente: propia

3.3 EN D1 Y A1, CONFIGURE EL ETHERCHANNEL. SWITCH D1

SWITCH D1

```

Configure terminal // Accede al modo de configuración
Interface port-channel 1 // ingresa al port-channel 1
Switchport mode Access // establezca el puerto en modo de
acceso.
Switchport Access vlan 8 // establezca el puerto en modo de
acceso a la VLAN 8
Exit // cierra la sesión del usuario actual
Interface e0/0 // ingrese a la interfaz
Channel-group 1 mode desirable // crea canal en modo grupo 1
Switchport mode Access // establece el modo acceso
Switchport Access vlan 8 // establezca el puerto en modo de
acceso vlan 8
No shutdown // enciende la interfaz
Exit // cierra la sesión del usuario

```

```

Interface e0/1 // ingresa a la interfaz
Channel-group 1 mode desirable // crea canal en modo grupo 1
Switchport mode Access // establezca el puerto en modo de
acceso.
Switchport Access vlan 8 // establezca el puerto en modo de
acceso a la VLAN 8

```

Figura 21. Verificación modo troncal SWITCH A1

```

A1#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)         PAgP        Et0/1(P)  Et0/2(P)
A1#

```

Fuente: propia

SWITCH A1

```

Configure terminal // Accede al modo de configuración
Interface port-channel 1 // ingresa al port-channel 1
Switchport mode Access // establezca el puerto en modo de
acceso.
Switchport Access vlan 8 // establezca el puerto en modo de
acceso vlan 8
Exit // cierra la sesión del usuario
Interface e0/1 // ingresa a la interfaz
Channel-group 1 mode desirable // crea canal en modo grupo 1

```

```

Switchport mode Access           // establece el modo acceso
Switchport Access vlan 8         // establezca el puerto en modo de
acceso vlan 8

No shutdown                       // enciende la interfaz
Exit                               // cierra la sesión del usuario
Interface e0/2                    // ingresa a la interfaz
Channel-group 1 mode desirable    // crea canal en modo grupo 1
Switchport mode Access           // establece el modo acceso
Switchport Access vlan 8         // establezca el puerto en modo de acceso
vlan 8
No shutdown                       // enciende la interfaz

```

Figura 22. Verificación modo troncal SWITCH D1

```

D1 - PuTTY
D1#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links
not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)          PAgP        Et0/0(P)   Et0/1(P)
D1#

```

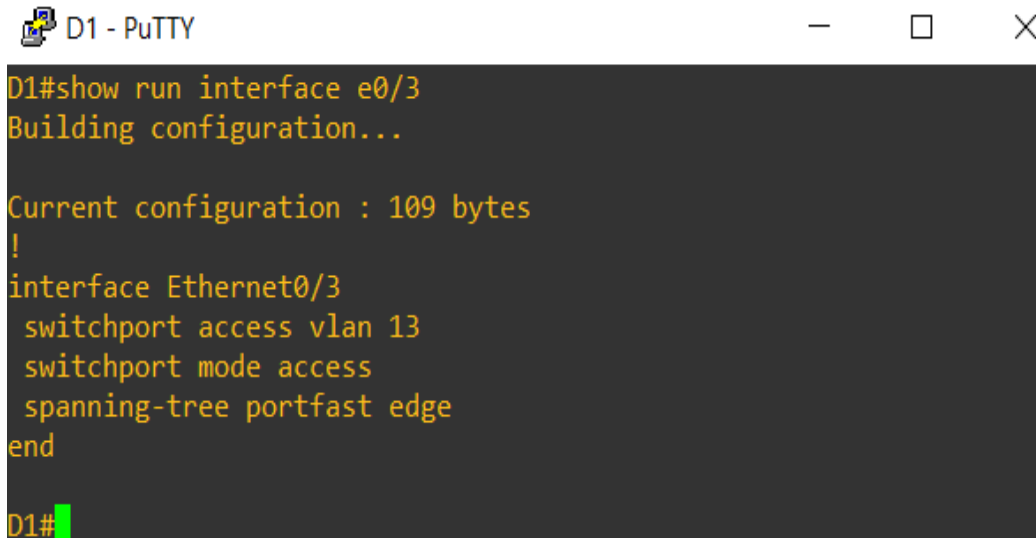
Fuente: propia

3.4 EN D1, D2 Y A1, CONFIGURE LOS PUERTOS DE ACCESO PARA PC1, PC2, PC3 Y PC4.

Configuración puertos de acceso para PC1 en SWITCH D1

```
Configure terminal // Accede al modo de configuración
Interface e0/3 // ingresa a la interfaz
Switchport mode Access // establece el modo acceso
Switchport Access vlan 13 // establezca el puerto en modo de acceso
vlan 13
Spanning-tree portfast // habilita la protección BPDU en todos los
puertos
No shutdown // enciende la interfaz
```

Figura 23. Verificación modo de acceso SWITCH D1



```
D1 - PuTTY
D1#show run interface e0/3
Building configuration...

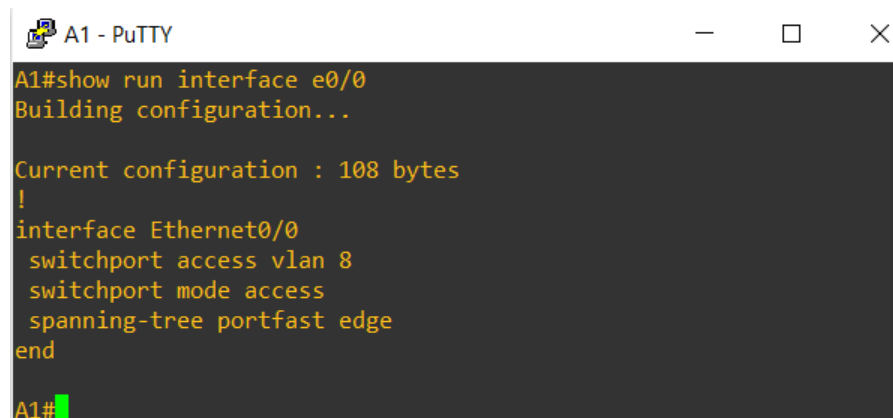
Current configuration : 109 bytes
!
interface Ethernet0/3
  switchport access vlan 13
  switchport mode access
  spanning-tree portfast edge
end
D1#
```

Fuente: propia

Configuración puertos de acceso para PC3 en SWITCH A1

```
Configure terminal // Accede al modo de configuración
Interface e0/0 // ingresa a la interfaz
Switchport mode Access // establece el modo acceso
Switchport Access vlan 8 // establezca el puerto en modo de acceso
vlan 8
Spanning-tree portfast // habilita la protección BPDU en todos los
puertos
No shutdown // enciende la interfaz
```

Figura 24. Verificación modo de acceso SWITCH A1



```
A1#show run interface e0/0
Building configuration...

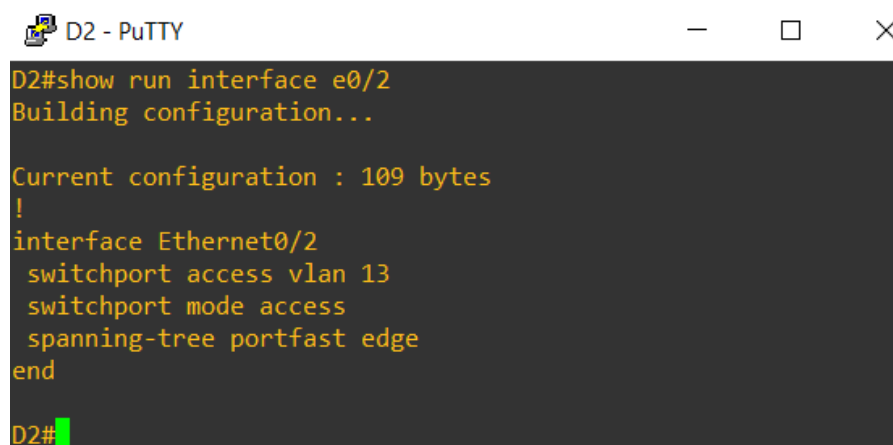
Current configuration : 108 bytes
!
interface Ethernet0/0
  switchport access vlan 8
  switchport mode access
  spanning-tree portfast edge
end
A1#
```

Fuente: propia

Configuración puertos de acceso para PC2 en SWITCH D2

Configure terminal	// Accede al modo de configuración
Interface e0/2	// ingresa a la interfaz
Switchport mode Access	// establece el modo acceso
Switchport Access vlan 13	// establezca el puerto en modo de acceso
vlan 13	
Spaning-tree portfast	// habilita la protección BPDU en todos los puertos
No shutdown	// enciende la interfaz

Figura 25. Verificación modo de acceso SWITCH D2



```
D2#show run interface e0/2
Building configuration...

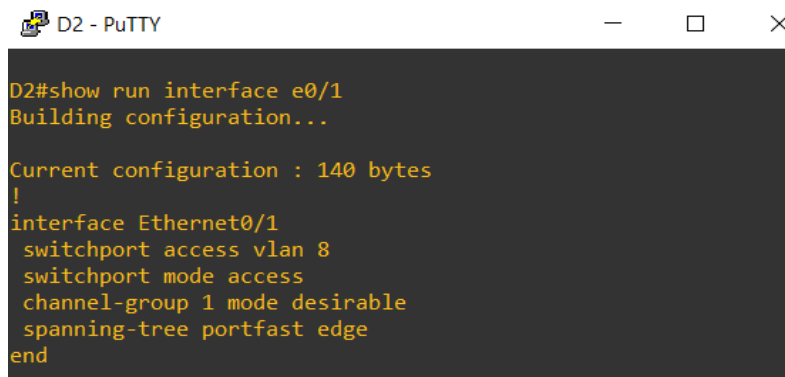
Current configuration : 109 bytes
!
interface Ethernet0/2
  switchport access vlan 13
  switchport mode access
  spanning-tree portfast edge
end
D2#
```

Fuente: propia

Configuración puertos de acceso para PC4 en SWITCH D2

```
Configure terminal           // Accede al modo de configuración
Interface e0/1              // ingresa a la interfaz
Switchport mode Access     // establece el modo acceso
Switchport Access vlan 8   // establezca el puerto en modo de acceso
vlan 8
Spanning-tree portfast     // habilita la protección BPDU en todos los
puertos
No shutdown                // enciende la interfaz
```

Figura 26. Verificación modo de acceso SWITCH D2



```
D2#show run interface e0/1
Building configuration...

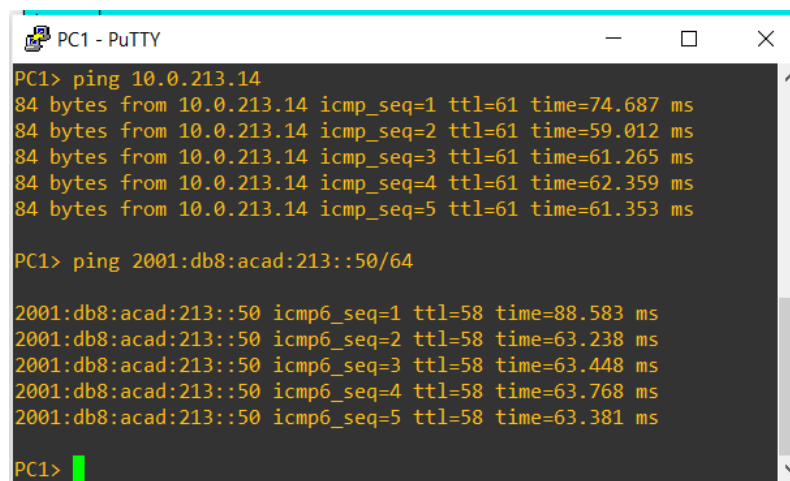
Current configuration : 140 bytes
!
interface Ethernet0/1
  switchport access vlan 8
  switchport mode access
  channel-group 1 mode desirable
  spanning-tree portfast edge
end
```

Fuente: propia

3.5 VERIFIQUE LA CONECTIVIDAD DE PC A PC.

Desde la pc1, verifique la conectividad ipv4 e ipv6 a la pc2.

Figura 27. Ping de conectividad PC1 a PC2



```
PC1> ping 10.0.213.14
84 bytes from 10.0.213.14 icmp_seq=1 ttl=61 time=74.687 ms
84 bytes from 10.0.213.14 icmp_seq=2 ttl=61 time=59.012 ms
84 bytes from 10.0.213.14 icmp_seq=3 ttl=61 time=61.265 ms
84 bytes from 10.0.213.14 icmp_seq=4 ttl=61 time=62.359 ms
84 bytes from 10.0.213.14 icmp_seq=5 ttl=61 time=61.353 ms

PC1> ping 2001:db8:acad:213::50/64

2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=88.583 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=63.238 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=63.448 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=63.768 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=63.381 ms

PC1>
```

Fuente: propia

Desde la pc3, verifique la conectividad ipv4 e ipv6 a la pc4.

Figura 28. Ping de conectividad PC3 a PC4

```

PC3> ping 10.0208.14
84 bytes from 10.0.213.14 icmp_seq=1 ttl=61 time=74.687 ms
84 bytes from 10.0.213.14 icmp_seq=2 ttl=61 time=59.012 ms
84 bytes from 10.0.213.14 icmp_seq=3 ttl=61 time=61.265 ms
84 bytes from 10.0.213.14 icmp_seq=4 ttl=61 time=62.359 ms
84 bytes from 10.0.213.14 icmp_seq=5 ttl=61 time=61.353 ms

PC3> ping 2001:db8:acad:213::50/64
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=88.58 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=63.238 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=63.448 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=63.768 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=63.381 ms
  
```

Fuente: propia

PARTE 4. CONFIGURE SEGURIDAD

Tabla 3. Configuración De Seguridad.

Tarea	Tarea	Especificación
4.1	En todos los dispositivos, modo EXE privilegiado seguro.	Configure un secreto de habilitación de la siguiente manera: <ul style="list-style-type: none"> • Tipo de algoritmo: SCRYPT • Contraseña: nombrestudianteXYZ.
4.2	En todos los dispositivos, cree una cuenta de usuario local.	Configurar un usuario local: <ul style="list-style-type: none"> • Nombre: administrador • 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 utilizando la base de datos local en todas las líneas.

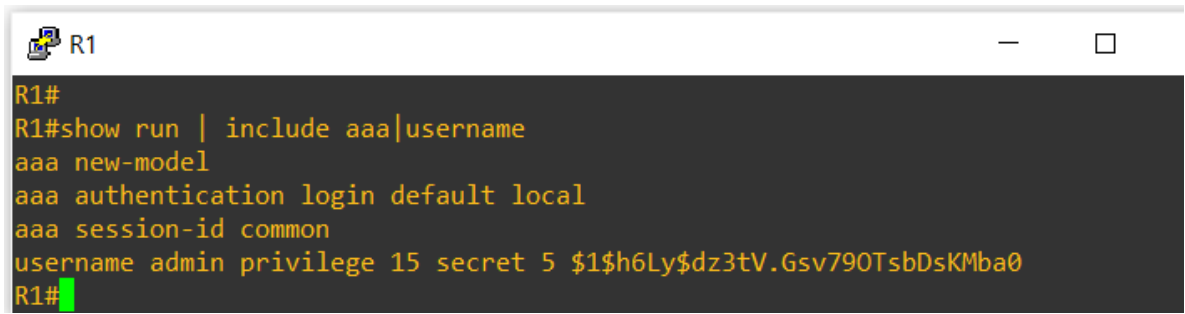
Fuente: propia

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

ROUTER R1

```
Configure terminal // Accede al modo de configuración
Service password-encryption // aplica un cifrado débil a todas las
contraseñas sin cifrar
Enable secret leonardo141 // establece la contraseña
Username admin secret 0 leonardo141 // crea usuario local admin
Username admin privilege 15 secret leonardo141 // crea usuario para nivel 15
aaa new-model // activa nuevo modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
exit // cierra la sesión del usuario actual
```

Figura 29. Configuración de Seguridad en ROUTER R1



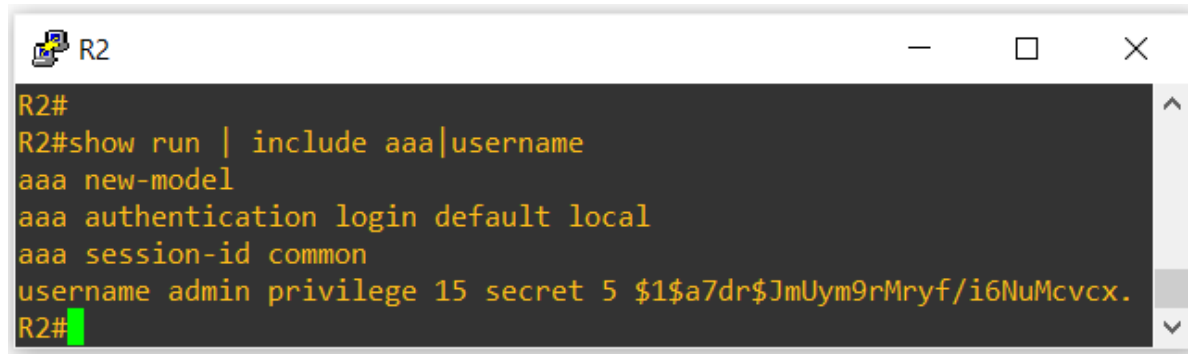
```
R1#
R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$h6Ly$dz3tV.Gsv790TsbDsKMba0
R1#
```

Fuente: propia

ROUTER R2

```
Configure terminal // Accede al modo de configuración
Service password-encryption // aplica un cifrado débil a todas las
contraseñas sin cifrar
Enable secret leonardo141 // establece la contraseña
Username admin secret 0 leonardo141 // crea usuario local admin
Username admin privilege 15 secret leonardo141 // crea usuario para nivel 15
aaa new-model // activa nuevo modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
exit // cierra la sesión del usuario actual
```

Figura 30. Configuración de Seguridad en ROUTER R2



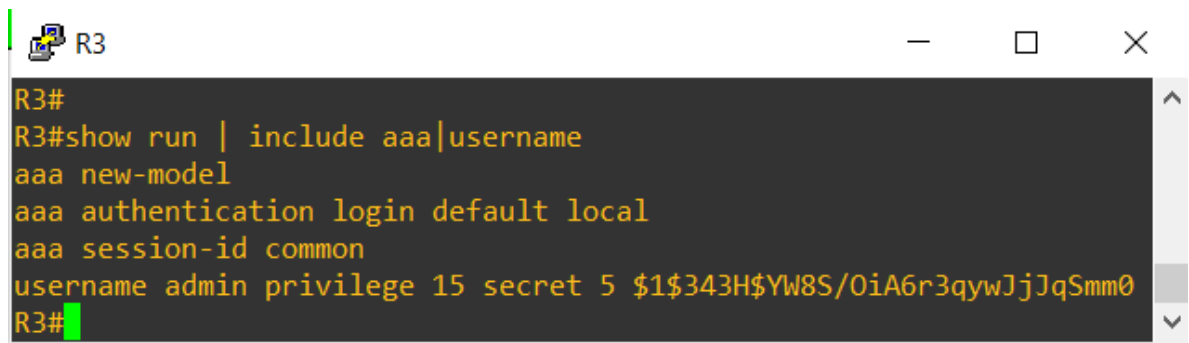
```
R2#
R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$a7dr$JmUym9rMryf/i6NuMcvcx.
R2#
```

Fuente: propia

ROUTER R3

Configure terminal	// Accede al modo de configuración
Service password-encryption	// aplica un cifrado débil a todas las contraseñas sin cifrar
Enable secret leonardo141	// establece la contraseña
Username admin secret 0 leonardo141	// crea usuario local admin
Username admin privilege 15 secret leonardo141	// crea usuario para nivel 15
aaa new-model	// activa nuevo modo de seguridad
aaa authentication login default local	// activa autenticación en el equipo
exit	// cierra la sesión del usuario actual

Figura 31. Configuración de Seguridad en ROUTER R3



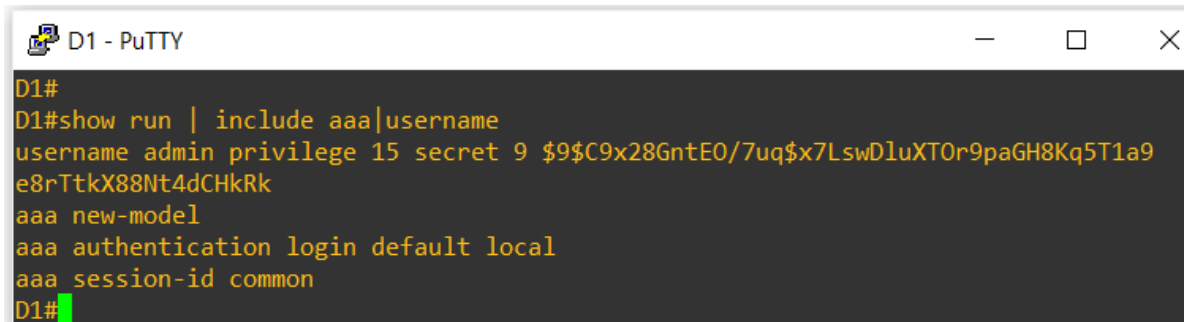
```
R3#
R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$343H$YW8S/OiA6r3qywJjJqSmm0
R3#
```

Fuente: propia

SWITCH D1

```
Configure terminal // Accede al modo de configuración
Service password-encryption // aplica un cifrado débil a todas las
contraseñas sin cifrar
Enable secret leonardo141 // establece la contraseña
Username admin secret 0 leonardo141 // crea usuario local admin
Username admin privilege 15 secret leonardo141 // crea usuario para nivel 15
aaa new-model // activa nuevo modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
end // cierra la sesión del usuario actual
```

Figura 32. Configuración de Seguridad en SWITCH D1



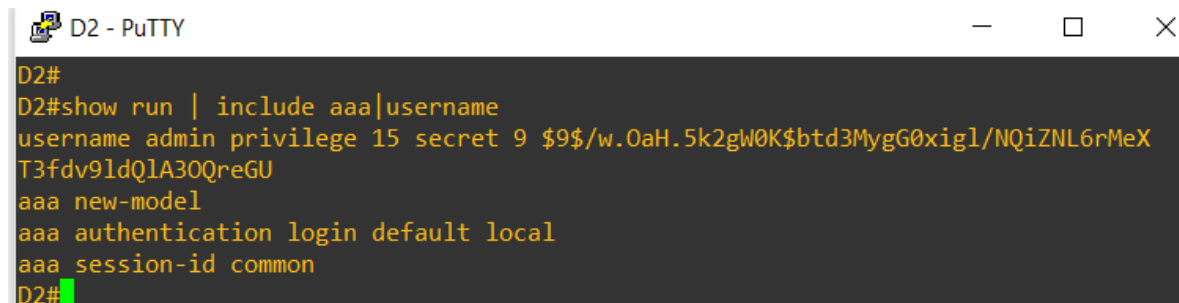
```
D1#
D1#show run | include aaa|username
username admin privilege 15 secret 9 $9$C9x28GntE0/7uq$x7LswDluXTOr9paGH8Kq5T1a9
e8rTtkX88Nt4dCHkRk
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
```

Fuente: propia

SWITCH D2

```
Configure terminal // Accede al modo de configuración
Service password-encryption // aplica un cifrado débil a todas las
contraseñas sin cifrar
Enable secret leonardo141 // establece la contraseña
Username admin secret 0 leonardo141 // crea usuario local admin
Username admin privilege 15 secret leonardo141 // crea usuario para nivel 15
aaa new-model // activa nuevo modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
end // cierra la sesión del usuario actual
```

Figura 33. Configuración de Seguridad en SWITCH D2



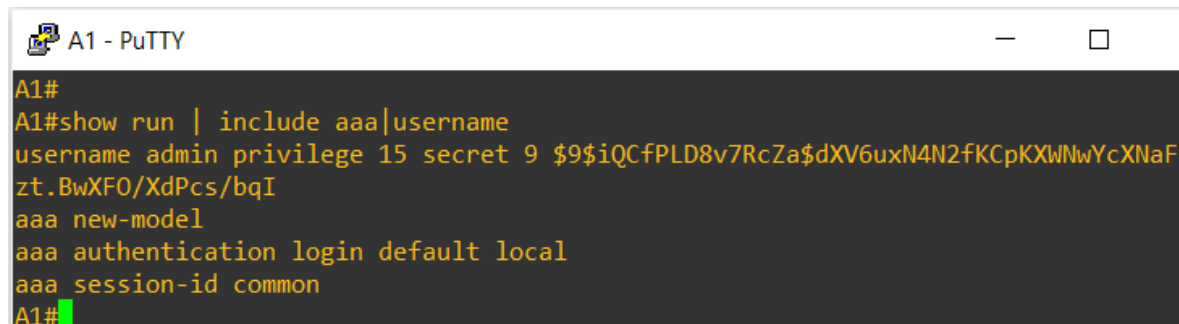
```
D2#
D2#show run | include aaa|username
username admin privilege 15 secret 9 $9$/w.OaH.5k2gW0K$btd3MygG0xigl/NQiZNL6rMeX
T3fdv9ldQlA30QreGU
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```

Fuente: propia

SWITCH A1

```
Configure terminal // Accede al modo de configuración
Service password-encryption // aplica un cifrado débil a todas las
contraseñas sin cifrar
Enable secret leonardo141 // establece la contraseña
Username admin secret 0 leonardo141 // crea usuario para nivel 15
Username admin privilege 15 secret leonardo141 // activa nuevo modo de
seguridad
aaa new-model // activa nuevo modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
end
```

Figura 34. Configuración de Seguridad en SWITCH A1



```
A1#
A1#show run | include aaa|username
username admin privilege 15 secret 9 $9$iQCfPLD8v7RcZa$dXV6uxN4N2fKcPcKXWNwYcXNaF
zt.BwXF0/XdPcs/bqI
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```

Fuente: propia

CONCLUSIONES

Con el desarrollo del Diplomado De Profundización Cisco CCNP, se logra desarrollar habilidades y competencias sobre la planificación, diseño e implementación de redes empresariales y áreas de escalabilidad constante en el sector de las telecomunicaciones, permitiendo obtener desde las habilidades básicas en la configuración de los equipos activos en red, como la seguridad, escalabilidad y disponibilidad de grandes redes empresariales.

Se logra contextualizar los conceptos teóricos aprendidos a lo largo de la carrera de telecomunicaciones con las fases del curso, de igual manera mediante herramientas digitales como software en este caso GN3, permitió la simulación virtual de redes con su configuración para la operatividad entre los dispositivos.

A partir del desarrollo de los escenarios propuestos, se alcanzaron la solución de los problemas que se presentaban en la red, debido al software implementado para la simulación, debido a la variación de configuración dependiendo de las imágenes que se carguen para simular los dispositivos.

Para concluir, se logra simular la planificación y diseño de una red, utilizando los protocolos de comunicación IPV4 y IPV6, logrando obtener seguridad, disponibilidad y confiabilidad en la red simulada.

BIBLIOGRAFÍA

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. "CCNP and CCIE Enterprise Core ENCOR 350-401". {En línea}. {25 de enero 2020}. Disponible en: <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. Multicast. "CCNP and CCIE Enterprise Core ENCOR 350-401". {En línea}. {25 de enero 2020}. Disponible en: <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. QoS. "CCNP and CCIE Enterprise Core ENCOR 350-401". {En línea}. {25 de enero 2020}. Disponible en: <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. IP Services. "CCNP and CCIE Enterprise Core ENCOR 350-401". {En línea}. {25 de enero 2020}. Disponible en: <https://1drv.ms/b/s!AAIGg5JUqUBthk8>