

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

EDWIN REYNEL MEDINA CORREA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
PALMIRA
2022

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

EDWIN REYNEL MEDINA CORREA

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

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
PALMIRA
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

PALMIRA, 26 de junio de 2022

AGRADECIMIENTOS

Lo primero es agradecer a Dios, así como a cada una de las personas que me han brindado su apoyo incondicional como lo son mis padres, mi pareja y mis hermanos, de los cuales solo he recibido enseñanzas y aliento para salir adelante. A mis tutores y profesores que han estado pendientes de mi proceso formativo, con paciencia y constancia siempre buscando la excelencia. A la Universidad Nacional Abierta y a Distancia por haberme permitido alcanzar este objetivo, siempre con seres éticos y profesionales.

CONTENIDO

AGRADECIMIENTOS.....	4
GLOSARIO.....	9
RESUMEN.....	10
ABSTRACT.....	10
INTRODUCCIÓN.....	11
DESARROLLO.....	12
ESCENARIO.....	12
Tabla de direccionamiento.....	13
Parte 1: Construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz.....	14
Paso 1.1: Cablear la red de acuerdo con la topología existente y la tabla de direccionamiento.....	14
Paso 1.2: Configurar los ajustes básicos de Routers, Switches y equipos de cómputo.....	15
Parte 2: Configurar VRF y enrutamiento estático.....	25
Paso 2.1: Configuración VRF.....	26
Paso 2.2: Configuración interfaz IPv4 e IPv6 de VRF.....	29
Paso 2.3: Configuración rutas estáticas.....	40
Paso 2.4: Verificación conexión de VRF.....	43
Parte 3: Configuración Switches.....	45
Paso 3.1: Deshabilitar interfaces.....	45
Paso 3.2: Configuración enlace troncal.....	47
Paso 3.3: Configuración EtherChannel.....	49
Paso 3.4: Configurar puertos de acceso.....	51
Paso 3.5: Conectividad entre equipos de cómputo.....	53
Parte 4: Configurar seguridad de los dispositivos.....	55
Paso 4.1: Configuración seguridad en modo EXEC.....	55
Paso 4.2: Configuración seguridad con usuario local.....	57
Paso 4.3: Configuración y autenticación AAA.....	59

SIMULACIÓN65
CONCLUSIONES66
BIBLIOGRAFÍA.....67

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento IP.....	13
Tabla 2. IOS implementadas en dispositivos	14
Tabla 3. Tareas y especificaciones de configuración en la Parte 2.	26
Tabla 4. Tareas y especificaciones de configuración en la Parte 3.	45
Tabla 5. Tareas y especificaciones de configuración en la Parte 4.	55

LISTA DE FIGURAS

Figura 1. Topología de red propuesta.....	12
Figura 2. Topología realizada en Software GNS3.....	14
Figura 3. Visualización dirección IP de PC1	23
Figura 4. Visualización dirección IP de PC2	24
Figura 5. Visualización dirección IP de PC3	24
Figura 6. Visualización dirección IP de PC4	25
Figura 7. Verificación VRF en R1.....	38
Figura 8. Verificación VRF en R2.....	39
Figura 9. Verificación VRF en R3.....	39
Figura 10. Visualización configuración, donde se incluyen las rutas en R1	40
Figura 11. Visualización configuración, donde se incluyen las rutas en R2.....	42
Figura 12. Visualización configuración, donde se incluyen las rutas en R3.....	43
Figura 13. Visualización conectividad entre R1 y R3 con cada VRF y familia.	44
Figura 14. Visualización configuración enlaces troncales en D1	48
Figura 15. Visualización configuración enlaces troncales en D2	49
Figura 16. Visualización del canal de puertos en D1	51
Figura 17. Visualización conectividad entre PC1 y PC2.	54
Figura 18. Visualización conectividad entre PC3 y PC4.	54
Figura 19. Verificación de configuración AAA y usuario en Router R1	62
Figura 20. Verificación de configuración AAA y usuario en Router R2	62
Figura 21. Verificación de configuración AAA y usuario en Router R3	63
Figura 22. Verificación de configuración AAA y usuario en Switch A1.....	63
Figura 23. Verificación de configuración AAA y usuario en Switch D1	64
Figura 24. Verificación de configuración AAA y usuario en Switch D2	64

GLOSARIO

AAA (Authentication, Authorization, Accounting): Es un conjunto de herramientas y protocolos que ofrecen un tratamiento en la autenticación, autorización y registro de la actividad.

BGP (Border Gateway Protocol): Es un protocolo de enrutamiento capa 4 en el modelo OSI, en el cual se intercambia información de ruteo que se basa en políticas de enrutamiento entre sistemas autónomos,

OSPF (Open Shortest Path First): Es un protocolo tipo enlace-estado, basado en el algoritmo de la ruta más corta, teniendo como ventaja que este no posee limitaciones en el número de saltos y, además, un menor tiempo de convergencia, ya que este se basa en el algoritmo Dijkstra

STP (Spanning Tree Protocol): El STP es un protocolo de capa 2 en el modelo OSI que permite controlar loops en las redes con el fin de asegurar el rendimiento de la red, esto lo hace por medio de un algoritmo que reconfigura los switches para evitar una pérdida de la conectividad.

VLAN (Virtual Local Area Network): Las VLAN o LAN Virtuales, es una tecnología que permite crear redes lógicas independientes dentro de una misma red física, esto se hace con la finalidad de segmentar, mejorar seguridad y controlar el tráfico de la red.

VRF (Virtual Routing and Forwarding): El VRF es una tecnología que funciona en la capa 3 del modelo OSI que se encuentra en los routers, que permite diferentes tablas de enrutamiento en un mismo router.

RESUMEN

El presente trabajo desarrolla el escenario planteado en el Diplomado de Profundización Cisco - Prueba de habilidades prácticas CCNP de la carrera de Ingeniería Electrónica, el cual se basa en la solución por medio de configuración de dispositivos de conexión (Routers y Switches), así como dispositivos finales (Computadores), con el propósito de realizar diferentes configuraciones multi-VRF, en donde se admitan diferentes grupos de usuarios pero que estos no tengan comunicación entre sí. Tanto el planteamiento del problema como su solución se basa en la implementación de forma correcta de VRF y VLANs, y es que lo que se busca llevar a cabo es utilizar diferentes grupos de usuarios (Special Users y General Users), cada uno asignado a una VLAN, con comunicación entre dispositivos finales en su misma VRF.

PALABRAS CLAVE: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

The present work develops the scenario proposed in the Cisco Deepening Diploma - CCNP practical skills test of the Electronic Engineering career, which is based on the solution through the configuration of connection devices (Routers and Switches), as well as devices terminals (Computers), with the purpose of carrying out different multi-VRF configurations, where different groups of users are admitted but they do not have communication with each other. Both the approach to the problem and its solution are based on the correct implementation of VRF and VLANs, and what is sought is to use different groups of users (Special Users and General Users), each one assigned to a VLAN, with communication between end devices in the same VRF.

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

INTRODUCCIÓN

A lo largo del desarrollo del escenario propuesto se observan diferentes configuraciones de dispositivos que basados en protocolos de red que permiten comprender tanto teóricamente como de forma práctica las principales ventajas de cada configuración, y es que con la implementación del paso 1 “Construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz” se observan diferentes comandos como lo son el habilitar el direccionamiento IPV6, desactivar la traducción de nombres a direcciones, crear VLANs y asignar los nombres a estas, entre otros; así como la configuración de los dispositivos finales tanto en IPV4 e IPV6.

La configuración de VRF y enrutamiento estático, se lleva a cabo en la parte 2 del trabajo, donde en los 3 Routers (C7200) se configuran dos VRF (Usuarios Generales y Usuarios Específicos), estos configurados para que admitan direccionamiento IPV4 e IPV6 según lo asignado en la tabla de direccionamiento encontrada en el contenido del trabajo; al igual que la asignación de VRF a las interfaces correspondientes, implementación de protocolos para que los diferentes Routers tengan enlace troncal en cada una de las VLANs creadas (VLAN 8 para PC3 y PC4, VLAN 13 para PC1 y PC2) , y por último, la visualización de la correcta configuración por medio de los comandos “show ip vrf interfaces”, “show run | inc route” y “ping vrf”.

En la configuración de los 3 Switches se configuran los enlaces troncales que van de los switches D1 y D2 a R1 y R3 respectivamente, se habilitan solamente las interfaces necesarias, se balancea el tráfico de la red aumentando el ancho de banda y aumentando la redundancia, y por último en esta etapa se configura el PortFast, permitiendo obtener información al instante de la capa 2, a los diferentes dispositivos finales; para finalizar se mejora la seguridad de todos los dispositivos con la implementación de contraseñas y algoritmos de encriptación de las mismas, creación de cuenta de usuario local y habilitación AAA (Autenticación, Autorización y Contabilización o Registro).

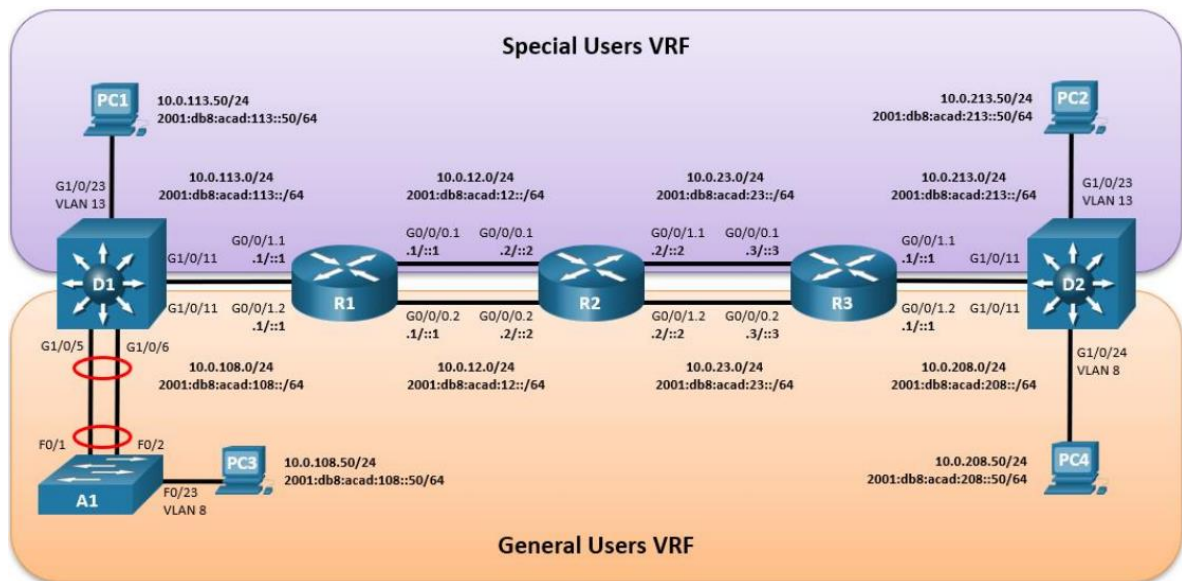
DESARROLLO

ESCENARIO

Configurar de forma que dos redes VRF coexistan, admitiendo “Usuarios Generales” y “Usuarios Especiales”, por medio de la configuración de 3 Routers, 3 Switches y 4 Equipos de cómputo, con conexión física entre ellos, e implementando subinterfaces a cada VRF para que al final del escenario se pueda comunicar el PC1 al PC2 y el PC3 al PC4, sin tener conexión entre los diferentes grupos de VRF.

Topología de red

Figura 1. Topología de red propuesta



Fuente: Diplomado de profundización Cisco CCNP

Tabla de direccionamiento

Construcción de tabla de direccionamiento IPv4 e IPv6 de Routers e interfaz de equipos PC, con ajuste en las interfaces disponibles en software GNS3.

Tabla 1. Tabla de direccionamiento IP

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Link-Local IPv6
R1	G1/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G1/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G2/0.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G2/0.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G1/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G1/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G2/0.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	G2/0.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G1/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G1/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G2/0.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G2/0.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC - e0	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC - e0	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC - e0	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC - e0	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

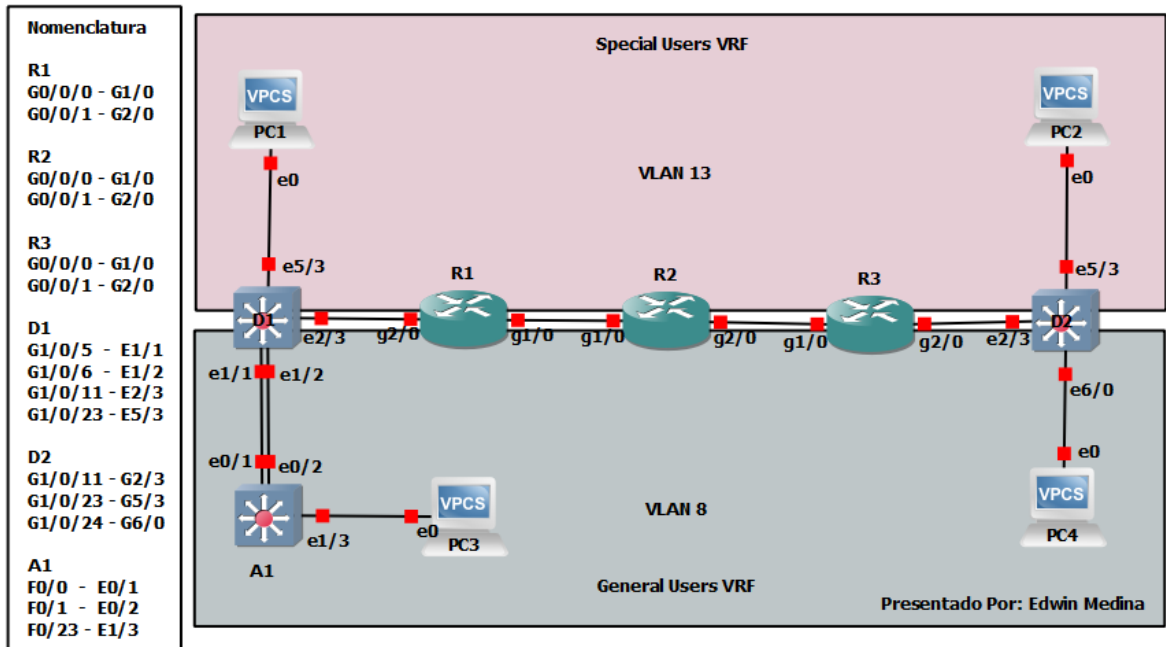
Fuente: Autoría propia

Parte 1: Construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz

Paso 1.1: Cablear la red de acuerdo con la topología existente y la tabla de direccionamiento

Conexión de los dispositivos en software GNS3 de acuerdo con el listado de interfaz, donde se modifica la nomenclatura del escenario propuesto debido a IOS disponibles en el momento del montaje.

Figura 2. Topología realizada en Software GNS3



Fuente: Autoría propia

Tabla 2. IOS implementadas en dispositivos

Dispositivo	IOS
R1	c7200-adventerprisek9-mz.152-4.M7bin
R2	c7200-adventerprisek9-mz.152-4.M7bin
R3	c7200-adventerprisek9-mz.152-4.M7bin
D1	i86bi-linux-l2-adventerprisek9-15.2d.bin
D2	i86bi-linux-l2-adventerprisek9-15.2d.bin
A1	i86bi-linux-l2-adventerprisek9-15.2d.bin

Fuente: Autoría propia

Paso 1.2: Configurar los ajustes básicos de Routers, Switches y equipos de cómputo.

Configurar los ajustes básicos en los dispositivos de red, así como su descripción en cada comando utilizado, guardar la configuración en la memoria NVRAM y configurar correctamente los equipos de cómputo, tanto en IPv4 como IPv6.

1. Configurar los dispositivos de red, con ajustes básicos.

Estructurar los ajustes básicos a cada uno de los dispositivos de red (3 Routers y 3 Switches).

- **Router R1**

```
enable
configure terminal
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo privilegiado
# Ingresa a modo de configuración global
# Cambiar el nombre al Router por R1
# Habilitar el routing ipv6
# Desactivar la traducción de nombres
# Configurar un mensaje de aviso al iniciar R1
# Ingresa a la configuración de la consola
# Establecer un tiempo de espera inactivo de la sesión remota
# Sincroniza los mensajes no solicitados
# Regresa al modo de configuración global
```

- **Router R2**

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

- **Descripción de cada comando utilizado**

```
# Ingresa a modo privilegiado
# Ingresa a modo de configuración global
# Cambiar el nombre al Router por R2
# Habilitar el routing ipv6
# Desactivar la traducción de nombres
# Configurar un mensaje de aviso al iniciar R2
# Ingresa a la configuración de la consola
# Establecer un tiempo de espera inactivo de la sesión remota
# Sincroniza los mensajes no solicitados
# Regresa al modo de configuración global
```

- **Router R3**

```
enable
configure terminal
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo privilegiado
# Ingresa a modo de configuración global
# Cambiar el nombre al Router por R3
# Habilitar el routing ipv6
# Desactivar la traducción de nombres
# Configurar un mensaje de aviso al iniciar R3
# Ingresa a la configuración de la consola
# Establecer un tiempo de espera inactivo de la sesión remota
# Sincroniza los mensajes no solicitados
# Regresa al modo de configuración global
```

- **Switch Capa 2 D1**

```
enable
configure terminal
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo privilegiado
# Ingresa a modo de configuración global
# Cambiar el nombre al Switch por D1
# Habilitar el routing
# Habilitar el routing ipv6
# Desactivar la traducción de nombres
# Configurar un mensaje de aviso al iniciar D1
# Ingresa a la configuración de la consola
# Establecer un tiempo de espera inactivo de la sesión remota
# Sincroniza los mensajes no solicitados
```

Regresa al modo de configuración global

- **Switch Capa 2 D1**

```
vlan 8
name General-Users
exit
vlan 13
name Special-Users
end
```

- **Descripción de cada comando utilizado**

```
# Crear la VLAN 8 e ingresar a ella
# Establecer General-Users como el nombre de la VLAN
# Regresa al modo de configuración global
# Crear la VLAN 13 e ingresar a ella
# Establecer Special-Users como el nombre de la VLAN
# Regresa al modo privilegiado
```

- **Switch Capa 2 D2**

```
enable
configure terminal
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo privilegiado
# Ingresa a modo de configuración global
# Cambiar el nombre al Switch por D2
```

```
# Habilitar el routing
# Habilitar el routing ipv6
# Desactivar la traducción de nombres
# Configurar un mensaje de aviso al iniciar D2
# Ingresa a la configuración de la consola
# Establecer un tiempo de espera inactivo de la sesión remota
# Sincroniza los mensajes no solicitados
# Regresa al modo de configuración global
```

- **Switch Capa 2 D2**

```
vlan 8
name General-Users
exit
vlan 13
name Special-Users
end
```

- **Descripción de cada comando utilizado**

```
# Crear la VLAN 8 e ingresar a ella
# Establecer General-Users como el nombre de la VLAN
# Regresa al modo de configuración global
# Crear la VLAN 13 e ingresar a ella
# Establecer Special-Users como el nombre de la VLAN
# Regresa al modo privilegiado
```

- **Switch Capa 3 A1**

```
enable
configure terminal
hostname A1
ipv6 unicast-routing
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo privilegiado
# Ingresa a modo de configuración global
# Cambiar el nombre al Switch por A1
# Habilitar el routing ipv6
# Desactivar la traducción de nombres
# Configurar un mensaje de aviso al iniciar D2
# Ingresa a la configuración de la consola
# Establecer un tiempo de espera inactivo de la sesión remota
# Sincroniza los mensajes no solicitados
# Regresa al modo de configuración global
```

2. Guardar las configuraciones en cada uno de los dispositivos.

Asegurar la configuración realizada, de todos los dispositivos de red que intervienen en la topología (3 Routers, 3 Switches), con la intención de que se guarde la información de la RAM en la memoria NVRAM.

- **Router R1**

```
copy running-config startup-config
```

- **Descripción de cada comando utilizado**

```
# Guarda la configuración actual como configuración inicial
```

- **Router R2**

```
copy running-config startup-config
```

- **Descripción de cada comando utilizado**

```
# Guarda la configuración actual como configuración inicial
```

- **Router R3**

```
copy running-config startup-config
```

- **Descripción de cada comando utilizado**

Guarda la configuración actual como configuración inicial

- **Switch Capa 2 D1**

copy running-config startup-config

- **Descripción de cada comando utilizado**

Guarda la configuración actual como configuración inicial

- **Switch Capa 2 D2**

copy running-config startup-config

- **Descripción de cada comando utilizado**

Guarda la configuración actual como configuración inicial

- **Switch Capa 3 A1**

copy running-config startup-config

- **Descripción de cada comando utilizado**

Guarda la configuración actual como configuración inicial

- 3. Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento.**

Configurar direccionamiento IPv4 e IPv6 en equipos de cómputo, adicionalmente configurar el proceso eui64 (4 Equipos de cómputo).

- **Equipo PC1**

```
ip 10.0.113.50/24 10.0.113.1  
ip 2001:db8:acad:113::50/64 eui-64  
copy running-config startup-config
```

- **Descripción de cada comando utilizado**

```
# Asignar dirección ipv4, máscara de subred y puerta de enlace  
# Asignar dirección ipv6, máscara de subred y proceso eui-64  
# Guarda la configuración actual como configuración inicial
```

- **Equipo PC2**

```
ip 10.0.213.50/24 10.0.213.1  
ip 2001:db8:acad:213::50/64 eui-64  
copy running-config startup-config
```

- **Descripción de cada comando utilizado**

```
# Asignar dirección ipv4, máscara de subred y puerta de enlace  
# Asignar dirección ipv6, máscara de subred y proceso eui-64  
# Guarda la configuración actual como configuración inicial
```

- **Equipo PC3**

```
ip 10.0.108.50/24 10.0.108.1  
ip 2001:db8:acad:108::50/64 eui-64  
copy running-config startup-config
```

- **Descripción de cada comando utilizado**

```
# Asignar dirección ipv4, máscara de subred y puerta de enlace  
# Asignar dirección ipv6, máscara de subred y proceso eui-64  
# Guarda la configuración actual como configuración inicial
```

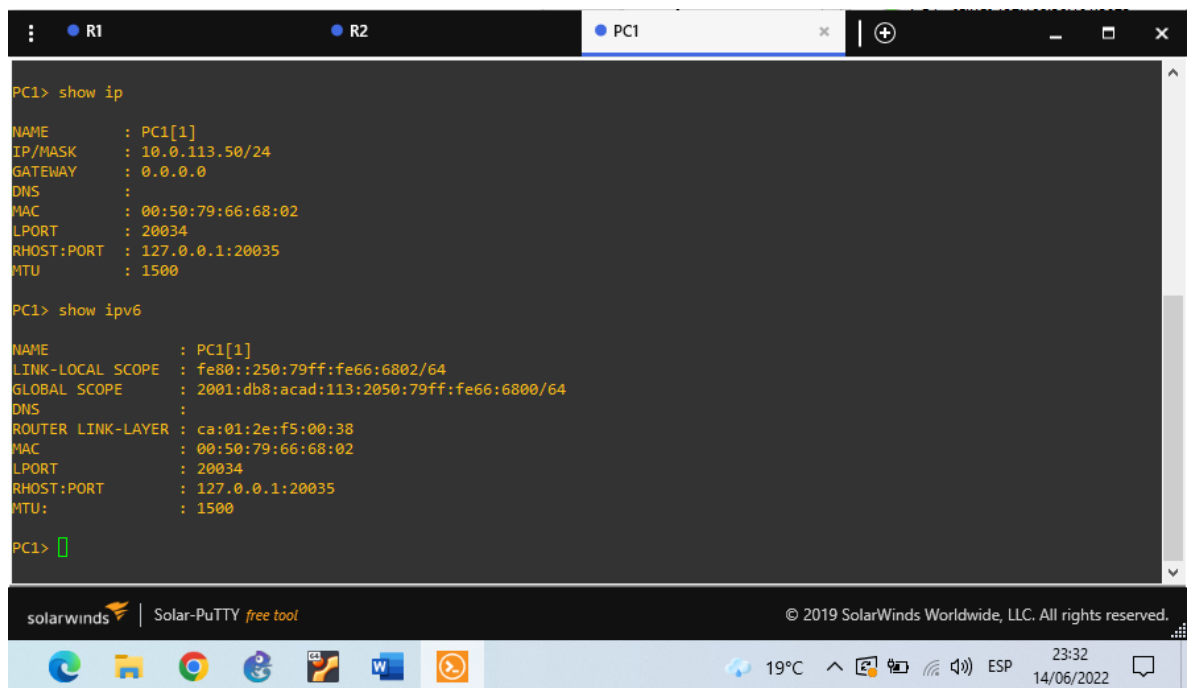
- **Equipo PC4**

```
ip 10.0.208.50/24 10.0.208.1  
ip 2001:db8:acad:208::50/64 eui-64  
copy running-config startup-config
```

- **Descripción de cada comando utilizado**

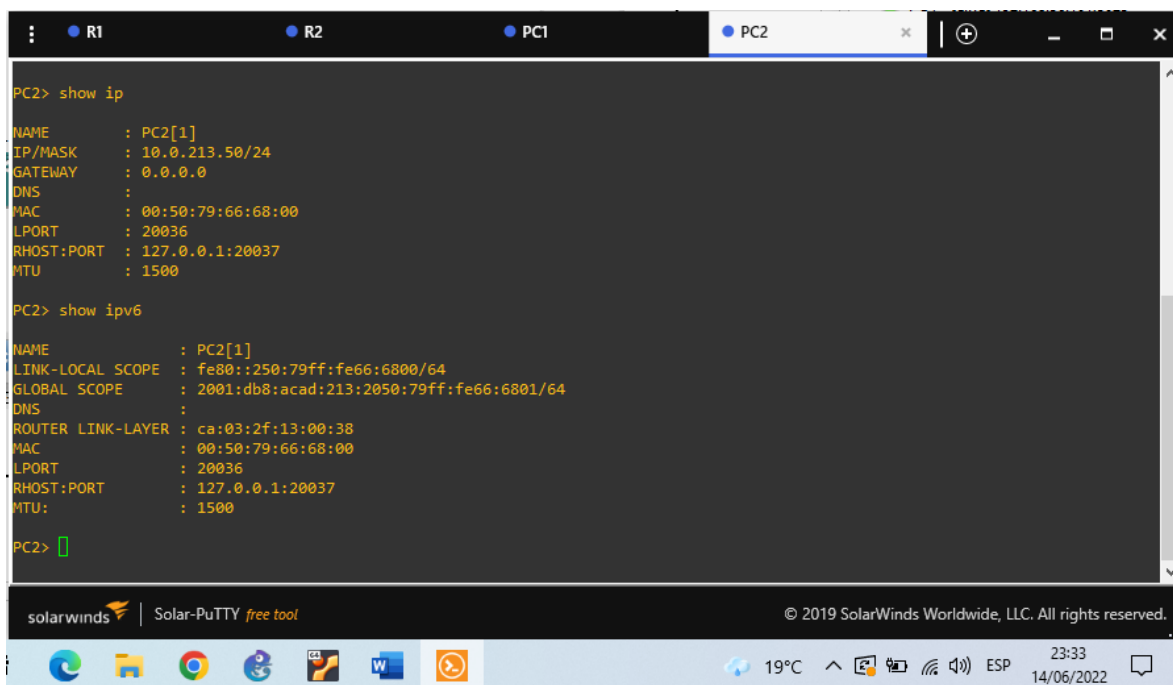
```
# Asignar dirección ipv4, máscara de subred y puerta de enlace  
# Asignar dirección ipv6, máscara de subred y proceso eui-64  
# Guarda la configuración actual como configuración inicial
```

Figura 3. Visualización dirección IP de PC1



Fuente: Autoría propia

Figura 4. Visualización dirección IP de PC2



The screenshot shows a SolarWinds Solar-PuTTY terminal window with tabs for R1, R2, PC1, and PC2. The PC2 tab is active, displaying the output of two commands: 'show ip' and 'show ipv6'. The 'show ip' command shows the following configuration: NAME: PC2[1], IP/MASK: 10.0.213.50/24, GATEWAY: 0.0.0.0, DNS: (empty), MAC: 00:50:79:66:68:00, LPORT: 20036, RHOST:PORT: 127.0.0.1:20037, and MTU: 1500. The 'show ipv6' command shows: NAME: PC2[1], LINK-LOCAL SCOPE: fe80::250:79ff:fe66:6800/64, GLOBAL SCOPE: 2001:db8:acad:213:2050:79ff:fe66:6801/64, DNS: (empty), ROUTER LINK-LAYER: ca:03:2f:13:00:38, MAC: 00:50:79:66:68:00, LPORT: 20036, RHOST:PORT: 127.0.0.1:20037, and MTU: 1500. The terminal interface includes a taskbar at the bottom with various application icons and system tray information such as temperature (19°C), time (23:33), and date (14/06/2022).

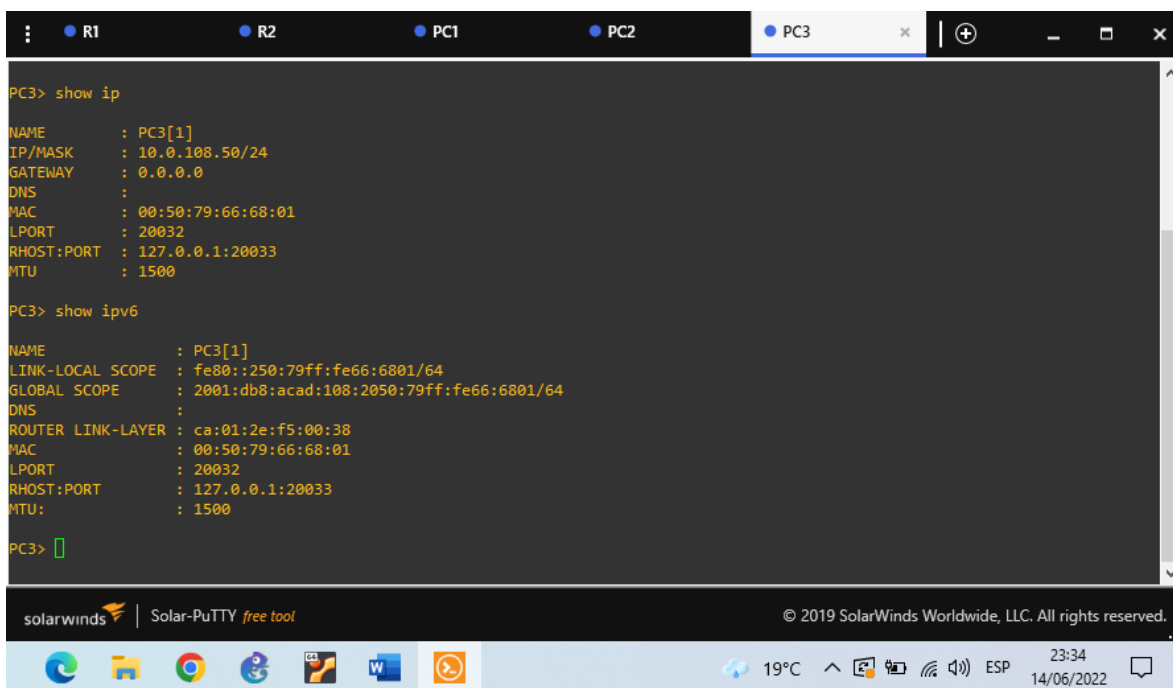
```
PC2> show ip
NAME       : PC2[1]
IP/MASK    : 10.0.213.50/24
GATEWAY    : 0.0.0.0
DNS        :
MAC       : 00:50:79:66:68:00
LPORT     : 20036
RHOST:PORT : 127.0.0.1:20037
MTU       : 1500

PC2> show ipv6
NAME       : PC2[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6800/64
GLOBAL SCOPE   : 2001:db8:acad:213:2050:79ff:fe66:6801/64
DNS           :
ROUTER LINK-LAYER : ca:03:2f:13:00:38
MAC          : 00:50:79:66:68:00
LPORT       : 20036
RHOST:PORT  : 127.0.0.1:20037
MTU        : 1500

PC2> 
```

Fuente: Autoría propia

Figura 5. Visualización dirección IP de PC3



The screenshot shows a SolarWinds Solar-PuTTY terminal window with tabs for R1, R2, PC1, PC2, and PC3. The PC3 tab is active, displaying the output of two commands: 'show ip' and 'show ipv6'. The 'show ip' command shows the following configuration: NAME: PC3[1], IP/MASK: 10.0.108.50/24, GATEWAY: 0.0.0.0, DNS: (empty), MAC: 00:50:79:66:68:01, LPORT: 20032, RHOST:PORT: 127.0.0.1:20033, and MTU: 1500. The 'show ipv6' command shows: NAME: PC3[1], LINK-LOCAL SCOPE: fe80::250:79ff:fe66:6801/64, GLOBAL SCOPE: 2001:db8:acad:108:2050:79ff:fe66:6801/64, DNS: (empty), ROUTER LINK-LAYER: ca:01:2e:f5:00:38, MAC: 00:50:79:66:68:01, LPORT: 20032, RHOST:PORT: 127.0.0.1:20033, and MTU: 1500. The terminal interface includes a taskbar at the bottom with various application icons and system tray information such as temperature (19°C), time (23:34), and date (14/06/2022).

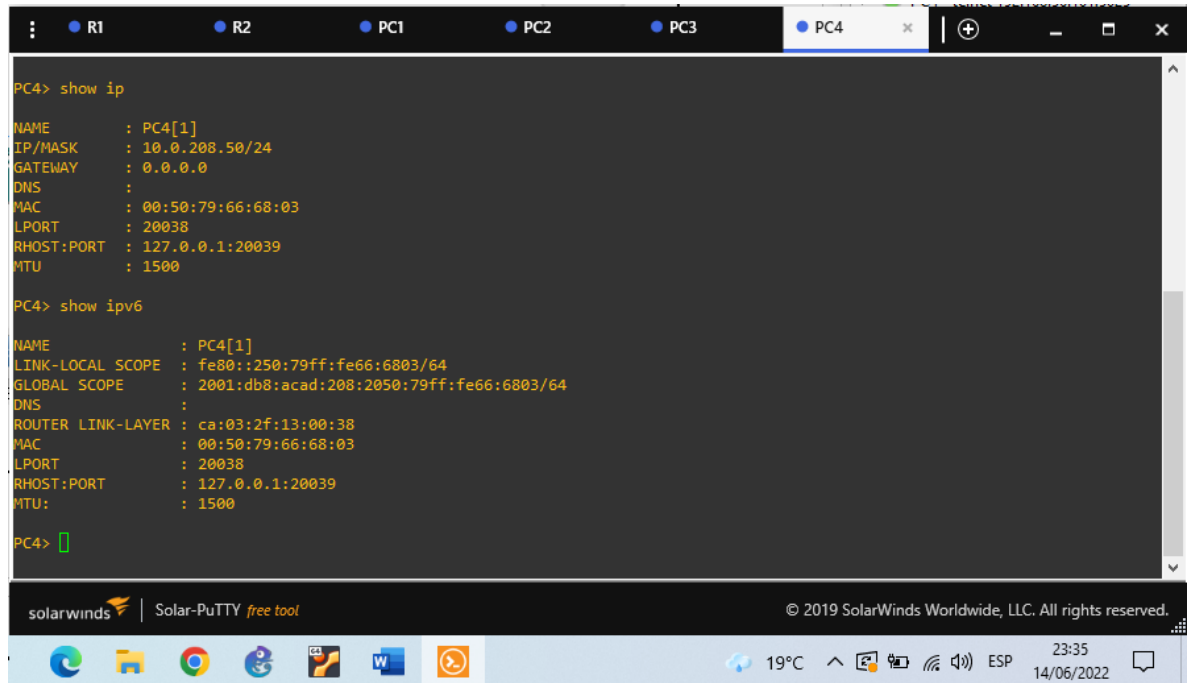
```
PC3> show ip
NAME       : PC3[1]
IP/MASK    : 10.0.108.50/24
GATEWAY    : 0.0.0.0
DNS        :
MAC       : 00:50:79:66:68:01
LPORT     : 20032
RHOST:PORT : 127.0.0.1:20033
MTU       : 1500

PC3> show ipv6
NAME       : PC3[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6801/64
GLOBAL SCOPE   : 2001:db8:acad:108:2050:79ff:fe66:6801/64
DNS           :
ROUTER LINK-LAYER : ca:01:2e:f5:00:38
MAC          : 00:50:79:66:68:01
LPORT       : 20032
RHOST:PORT  : 127.0.0.1:20033
MTU        : 1500

PC3> 
```

Fuente: Autoría propia

Figura 6. Visualización dirección IP de PC4



```
PC4> show ip
NAME          : PC4[1]
IP/MASK       : 10.0.208.50/24
GATEWAY       : 0.0.0.0
DNS           :
MAC           : 00:50:79:66:68:03
LPORT         : 20038
RHOST:PORT    : 127.0.0.1:20039
MTU           : 1500

PC4> show ipv6
NAME          : PC4[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6803/64
GLOBAL SCOPE    : 2001:db8:acad:208:2050:79ff:fe66:6803/64
DNS           :
ROUTER LINK-LAYER : ca:03:2f:13:00:38
MAC           : 00:50:79:66:68:03
LPORT         : 20038
RHOST:PORT    : 127.0.0.1:20039
MTU           : 1500

PC4> █
```

The screenshot shows a Solar-PuTTY terminal window with tabs for R1, R2, PC1, PC2, PC3, and PC4. The PC4 tab is active. The terminal displays the output of 'show ip' and 'show ipv6' commands. The 'show ip' command shows PC4[1] with IP 10.0.208.50/24, gateway 0.0.0.0, MAC 00:50:79:66:68:03, LPORT 20038, RHOST:PORT 127.0.0.1:20039, and MTU 1500. The 'show ipv6' command shows PC4[1] with Link-Local Scope fe80::250:79ff:fe66:6803/64, Global Scope 2001:db8:acad:208:2050:79ff:fe66:6803/64, Router Link-Layer ca:03:2f:13:00:38, MAC 00:50:79:66:68:03, LPORT 20038, RHOST:PORT 127.0.0.1:20039, and MTU 1500. The terminal window has a Windows taskbar at the bottom with icons for Edge, File Explorer, Chrome, Word, and PuTTY. The system tray shows 19°C, ESP, and the date 14/06/2022.

Fuente: Autoría propia

En las figuras 3, 4, 5 y 6 se observan las evidencias de direccionamiento IPv4 e IPv6 de los Equipos PC1, PC2, PC3 y PC4 respectivamente, se constata información como IP, mascara de subred, dirección MAC, Link-Local, Link-Layer, entre otros parámetros.

Parte 2: Configurar VRF y enrutamiento estático

Configurar las VRF-Lite en los tres (3) Routers, además de las rutas estáticas pertinentes que garantizarán la conectividad entre los extremos (R1 a R3). Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF, tanto IPv4 como IPv6.

Tabla 3. Tareas y especificaciones de configuración en la Parte 2.

Paso	Tarea
2.1	Configurar las VRF “General-Users” y “Special-Users”, soportando IPv4 e IPv6, de acuerdo con la topología y tabla de direccionamiento.
2.2	Configurar las interfaces IPv4 e IPv6 a ambas VRF, crear las subinterfaces y utilizar encapsulación dot1q.
2.3	Configurar las rutas estáticas desde R1 a R2 y desde R3 a R2, ambas configuradas tanto en IPv4 e IPv6, en ambas VRF.
2.4	Verificar la conexión entre VRF, realizando una prueba de "PING" desde R1 hacia R3, en ambas VRF y dirección IPv4 e IPv6.

Fuente: Autoría propia

Paso 2.1: Configuración VRF

Configurar las VRF “General-Users” y “Special-Users”, soportando IPv4 e IPv6, de acuerdo con la topología y tabla de direccionamiento.

- **Router R1**

```
configure terminal
vrf definition Special-Users
address-family ipv4
address-family ipv6
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Define y nombra la VRF e ingresa a configuración, en este caso Special-Users
# Define la familia o protocolo a utilizar, en este caso ipv4
# Define la familia o protocolo a utilizar, en este caso ipv6
# Regresa al modo privilegiado
```

- **Router R1**

```
configure terminal
vrf definition General-Users
address-family ipv4
address-family ipv6
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Define y nombra la VRF e ingresa a configuración, en este caso General-Users
# Define la familia o protocolo a utilizar, en este caso ipv4
# Define la familia o protocolo a utilizar, en este caso ipv6
# Regresa al modo privilegiado
```

- **Router R2**

```
configure terminal
vrf definition Special-Users
address-family ipv4
address-family ipv6
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Define y nombra la VRF e ingresa a configuración, en este caso Special-Users
# Define la familia o protocolo a utilizar, en este caso ipv4
# Define la familia o protocolo a utilizar, en este caso ipv6
# Regresa al modo privilegiado
```

- **Router R2**

```
configure terminal
vrf definition General-Users
address-family ipv4
address-family ipv6
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Define y nombra la VRF e ingresa a configuración, en este caso General-Users
# Define la familia o protocolo a utilizar, en este caso ipv4
# Define la familia o protocolo a utilizar, en este caso ipv6
# Regresa al modo privilegiado
```

- **Router R3**

```
configure terminal
vrf definition Special-Users
address-family ipv4
address-family ipv6
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Define y nombra la VRF e ingresa a configuración, en este caso Special-Users
# Define la familia o protocolo a utilizar, en este caso ipv4
# Define la familia o protocolo a utilizar, en este caso ipv6
# Regresa al modo privilegiado
```

- **Router R3**

```
configure terminal
vrf definition General-Users
address-family ipv4
address-family ipv6
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Define y nombra la VRF e ingresa a configuración, en este caso General-Users
# Define la familia o protocolo a utilizar, en este caso ipv4
# Define la familia o protocolo a utilizar, en este caso ipv6
# Regresa al modo privilegiado
```

Paso 2.2: Configuración interfaz IPv4 e IPv6 de VRF

Configurar las interfaces IPv4 e IPv6 a ambas VRF, crear las subinterfaces y utilizar encapsulación dot1q.

- **Router R1 – Interface Gigabitethernet 2/0.1**

```
configure terminal
interface Gigabitethernet 2/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.113.1 255.255.255.0
ipv6 address 2001:db8:acad:113::1/64
ipv6 address fe80::1:3 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Ingresa a la subinterfaz de Gigabitethernet 2/0.1
# Habilitar 802.1Q y asociar VLAN 13 a la subinterfaz
# Asocia la VRF Special-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 2/0.1
# Regresa al modo de configuración global
```

- **Router R1 – Interface Gigabitethernet 2/0.2**

```
interface Gigabitethernet 2/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.108.1 255.255.255.0
ipv6 address 2001:db8:acad:108::1/64
ipv6 address fe80::1:4 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 2/0.2
# Habilitar 802.1Q y asociar VLAN 8 a la subinterfaz
# Asocia la VRF General-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 2/0.2
# Regresa al modo de configuración global
```

- **Router R1 – Interface Gigabitethernet 2/0**

```
interface GigabitEthernet 2/0
no ip address
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la interfaz Gigabitethernet 2/0
# Se notifica que no se va a ingresar dirección ip
# Se habilita la interfaz
# Regresa al modo de configuración global
```

- **Router R1 – Interface Gigabitethernet 1/0.1**

```
interface Gigabitethernet 1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.12.1 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
ipv6 address fe80::1:1 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 1/0.1
# Habilitar 802.1Q y asociar VLAN 13 a la subinterfaz
# Asocia la VRF Special-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 1/0.1
# Regresa al modo de configuración global
```

- **Router R1 – Interface Gigabitethernet 1/0.2**

```
interface Gigabitethernet 1/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.12.1 255.255.255.0
ipv6 address 2001:db8:acad:12::1/64
ipv6 address fe80::1:2 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 1/0.2
# Habilitar 802.1Q y asociar VLAN 8 a la subinterfaz
# Asocia la VRF General-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 1/0.2
# Regresa al modo de configuración global
```

- **Router R1 – Interface Gigabitethernet 1/0**

```
interface Gigabitethernet 1/0
no ip address
no shutdown
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la interfaz Gigabitethernet 1/0
# Se notifica que no se va a ingresar dirección ip
# Se habilita la interfaz
# Regresa al modo privilegiado
```

- **Router R2 – Interface Gigabitethernet 1/0.1**

```
configure terminal
interface Gigabitethernet 1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address 2001:db8:acad:12::2/64
ipv6 address fe80::2:1 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Ingresa a la subinterfaz de Gigabitethernet 1/0.1
# Habilitar 802.1Q y asociar VLAN 13 a la subinterfaz
# Asocia la VRF Special-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 1/0.1
# Regresa al modo de configuración global
```

- **Router R2 – Interface Gigabitethernet 1/0.2**

```
interface Gigabitethernet 1/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address 2001:db8:acad:12::2/64
ipv6 address fe80::2:2 link-local
```

```
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 1/0.2
# Habilitar 802.1Q y asociar VLAN 8 a la subinterfaz
# Asocia la VRF General-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 1/0.2
# Regresa al modo de configuración global
```

- **Router R2 – Interface Gigabitethernet 1/0**

```
interface gigabitethernet 1/0
no ip address
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la interfaz Gigabitethernet 1/0
# Se notifica que no se va a ingresar dirección ip
# Se habilita la interfaz
# Regresa al modo de configuración global
```

- **Router R2 – Interface Gigabitethernet 2/0.1**

```
interface Gigabitethernet 2/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address 2001:db8:acad:23::2/64
ipv6 address fe80::2:3 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 2/0.1
# Habilitar 802.1Q y asociar VLAN 13 a la subinterfaz
# Asocia la VRF Special-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 2/0.1
# Regresa al modo de configuración global
```

- **Router R2 – Interface Gigabitethernet 2/0.2**

```
interface Gigabitethernet 2/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address 2001:db8:acad:23::2/64
ipv6 address fe80::2:4 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 2/0.2
# Habilitar 802.1Q y asociar VLAN 8 a la subinterfaz
# Asocia la VRF General-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 2/0.2
# Regresa al modo de configuración global
```

- **Router R2 – Interface Gigabitethernet 2/0**

```
interface gigabitethernet 2/0
no ip address
no shutdown
end
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la interfaz Gigabitethernet 2/0
# Se notifica que no se va a ingresar dirección ip
# Se habilita la interfaz
# Regresa al modo privilegiado
```

- **Router R3 – Interface Gigabitethernet 1/0.1**

```
configure terminal
interface Gigabitethernet 1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.23.3 255.255.255.0
ipv6 address 2001:db8:acad:23::3/64
ipv6 address fe80::3:1 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa al modo de configuración global
# Ingresa a la subinterfaz de Gigabitethernet 1/0.1
# Habilitar 802.1Q y asociar VLAN 13 a la subinterfaz
# Asocia la VRF Special-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 1/0.1
# Regresa al modo de configuración global
```

- **Router R3 – Interface Gigabitethernet 1/0.2**

```
interface Gigabitethernet 1/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.23.3 255.255.255.0
ipv6 address 2001:db8:acad:23::3/64
```

```
ipv6 address fe80::3:2 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 1/0.2
# Habilitar 802.1Q y asociar VLAN 8 a la subinterfaz
# Asocia la VRF General-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 1/0.2
# Regresa al modo de configuración global
```

- **Router R3 – Interface Gigabitethernet 1/0**

```
interface gigabitethernet 1/0
no ip address
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la interfaz Gigabitethernet 1/0
# Se notifica que no se va a ingresar dirección ip
# Se habilita la interfaz
# Regresa al modo de configuración global
```

- **Router R3 – Interface Gigabitethernet 2/0.1**

```
interface Gigabitethernet 2/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.213.1 255.255.255.0
ipv6 address 2001:db8:acad:213::1/64
ipv6 address fe80::3:3 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 2/0.1
# Habilitar 802.1Q y asociar VLAN 13 a la subinterfaz
# Asocia la VRF Special-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 2/0.1
# Regresa al modo de configuración global
```

- **Router R3 – Interface Gigabitethernet 2/0.2**

```
interface Gigabitethernet 2/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.208.1 255.255.255.0
ipv6 address 2001:db8:acad:208::1/64
ipv6 address fe80::3:4 link-local
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la subinterfaz de Gigabitethernet 2/0.2
# Habilitar 802.1Q y asociar VLAN 8 a la subinterfaz
# Asocia la VRF General-Users con la interfaz de capa 3
# Se asigna la dirección ipv4 de la subinterfaz y su máscara de subred
# Se asigna la dirección ipv6 de la subinterfaz y su máscara de subred
# Se asigna la dirección de link local
# Se habilita la subinterfaz Gigabitethernet 2/0.2
# Regresa al modo de configuración global
```

- **Router R3 – Interface Gigabitethernet 2/0**

```
interface gigabitethernet 2/0
no ip address
no shutdown
end
```

- Descripción de cada comando utilizado

```
# Ingresa a la interfaz Gigabitethernet 2/0
# Se notifica que no se va a ingresar dirección ip
# Se habilita la interfaz
# Regresa al modo privilegiado
```

Verificación VRF en Routers

En las Figuras 7, 8 y 9, se observan los resúmenes de las VRF en el Router R1, R2 y R3 respectivamente, donde se detalla la interfaz, la dirección IP, la VRF a la cual esta asignada y si se encuentra habilitada.

Figura 7. Verificación VRF en R1

```
*Jun 18 02:25:54.671: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Jun 18 02:25:54.679: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
*Jun 18 02:25:55.763: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Jun 18 02:25:55.767: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
*Jun 18 02:25:55.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
*Jun 18 02:25:56.859: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to down
*Jun 18 02:25:59.603: %LINK-5-CHANGED: Interface FastEtherne R1, ENCOR Skills Assessment, Scenario 2
R1#t0/0, changed state to administratively down
*Jun 18 02:26:01.867: %SYS-5-CONFIG_I: Configured from memory by console
*Jun 18 02:26:02.755: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)M7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 25-Sep-14 10:36 by prod_rel_team
*Jun 18 02:26:02.863: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Jun 18 02:26:03.739: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 18 02:26:03.739: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
R1#
R1#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Gi1/0.2        10.0.12.1       General-Users    up
Gi2/0.2        10.0.108.1     General-Users    up
Gi1/0.1        10.0.12.1       Special-Users    up
Gi2/0.1        10.0.113.1     Special-Users    up
R1#
```

Fuente: Autoría propia

Figura 8. Verificación VRF en R2

```

*Jun 18 02:27:29.959: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Jun 18 02:27:29.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
*Jun 18 02:27:29.967: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
*Jun 18 02:27:30.963: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to down
*Jun 18 02:27:35.651: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively R2, ENCOR Skills Assessm
R2# down
*Jun 18 02:27:39.803: %SYS-5-CONFIG_I: Configured from memory by console
*Jun 18 02:27:43.295: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)M7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 25-Sep-14 10:36 by prod_rel_team
*Jun 18 02:27:43.423: %SNMP-5-COLDSTART: SNMP agent on host R2 is undergoing a cold start
*Jun 18 02:27:43.831: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 18 02:27:43.835: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
R2#
R2#
R2#
R2#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Gi1/0.2        10.0.12.2       General-Users    up
Gi2/0.2        10.0.23.2       General-Users    up
Gi1/0.1        10.0.12.2       Special-Users    up
Gi2/0.1        10.0.23.2       Special-Users    up
R2#

```

Fuente: Autoría propia

Figura 9. Verificación VRF en R3

```

*Jun 18 02:30:01.791: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o down
*Jun 18 02:30:08.643: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Jun 18 02:30:13.711: %SYS-5-CONFIG_I: Configured from memory by console
*Jun 18 02:30:21.371: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)M7,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 25-Sep-14 10:36 by prod_rel_team
*Jun 18 02:30:21.523: %SNMP-5-COLDSTART: SNMP agent on host R3 is undergoing a c
old start
*Jun 18 02:30:22.035: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 18 02:30:22.039: % R3, ENCOR Skills Assessment, Scenario 2
R3#
R3#
R3#
R3#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Gi1/0.2        10.0.23.3       General-Users    up
Gi2/0.2        10.0.208.1     General-Users    up
Gi1/0.1        10.0.23.3       Special-Users    up
Gi2/0.1        10.0.213.1     Special-Users    up
R3#

```

Fuente: Autoría propia

Paso 2.3: Configuración rutas estáticas

Configurar las rutas estáticas desde R1 y R3 hacia R2, ambas configuradas tanto en IPv4 e IPv6, en ambas VRF.

- **Router R1**

configure terminal

```
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2
```

```
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2
```

```
ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2
```

```
ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2
```

```
end
```

- **Descripción de cada comando utilizado**

Ingresa al modo de configuración global

Configuración de ruta estática en ipv4 para VRF Special-Users a través de R2

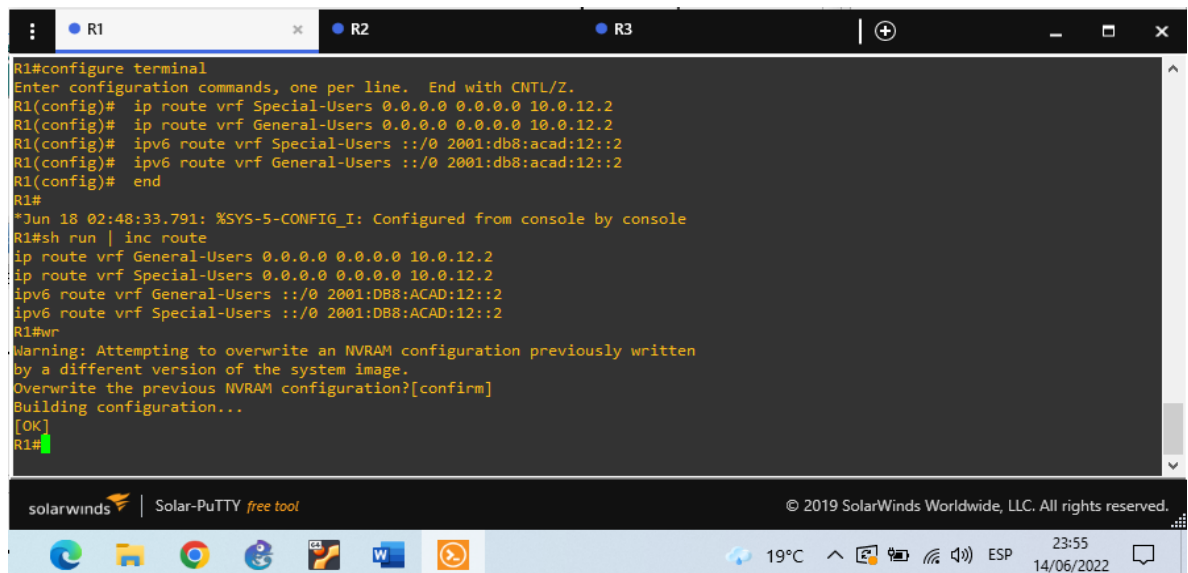
Configuración de ruta estática en ipv4 para VRF General-Users a través de R2

Configuración de ruta estática en ipv6 para VRF Special-Users a través de R2

Configuración de ruta estática en ipv6 para VRF General-Users a través de R2

Regresa al modo privilegiado

Figura 10. Visualización configuración, donde se incluyen las rutas en R1



```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)# ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)# ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2
R1(config)# ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2
R1(config)# end
R1#
*Jun 18 02:48:33.791: %SYS-5-CONFIG_I: Configured from console by console
R1#sh run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2
R1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#
```

Fuente: Autoría propia

- **Router R2**

configure terminal

```
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 10.0.23.3
```

```
ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1
```

```
ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3
```

```
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 10.0.23.3
```

```
ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1
```

```
ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3
```

```
end
```

- **Descripción de cada comando utilizado**

Ingresa al modo de configuración global

Configuración de ruta estática en ipv4 para VRF Special-Users a través de R1

Configuración de ruta estática en ipv4 para VRF Special-Users a través de R3

Configuración de ruta estática en ipv6 para VRF Special-Users a través de R1

Configuración de ruta estática en ipv6 para VRF Special-Users a través de R3

Configuración de ruta estática en ipv4 para VRF General-Users a través de R1

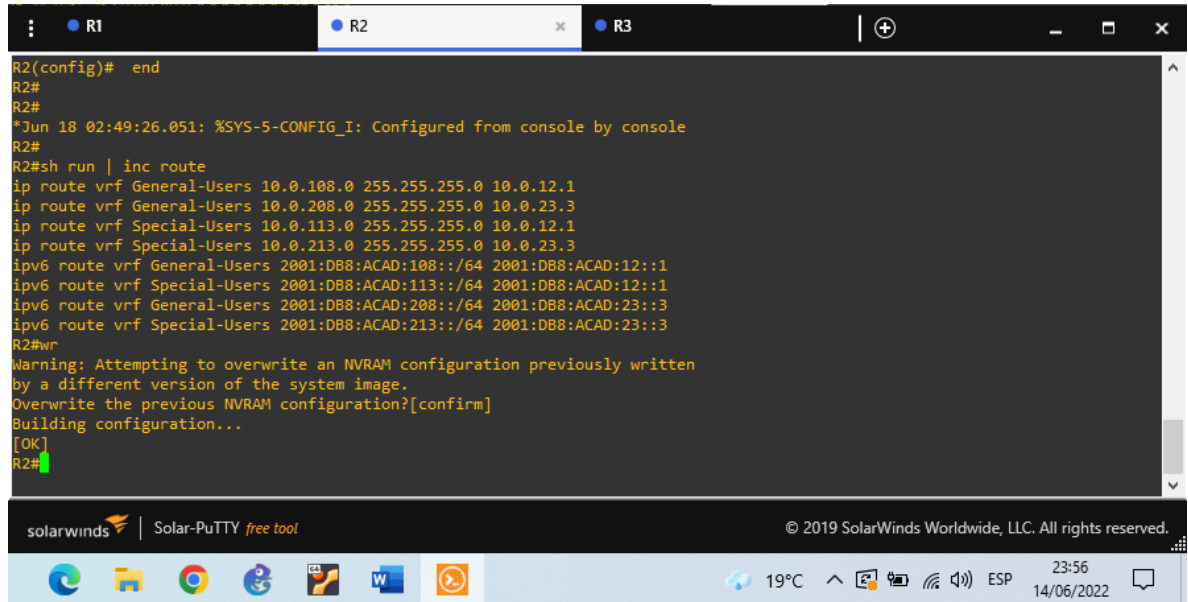
Configuración de ruta estática en ipv4 para VRF General-Users a través de R3

Configuración de ruta estática en ipv6 para VRF General-Users a través de R1

Configuración de ruta estática en ipv6 para VRF General-Users a través de R3

Regresa al modo privilegiado

Figura 11. Visualización configuración, donde se incluyen las rutas en R2



```
R2(config)# end
R2#
R2#
*Jun 18 02:49:26.051: %SYS-5-CONFIG_I: Configured from console by console
R2#
R2#sh run | inc route
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 10.0.23.3
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 10.0.23.3
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
R2#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#
```

Fuente: Autoría propia

Router R3

configure terminal

```
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2
```

```
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2
```

```
ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2
```

```
ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2
```

```
end
```

- **Descripción de cada comando utilizado**

Ingresa al modo de configuración global

Configuración de ruta estática en ipv4 para VRF Special-Users a través de R2

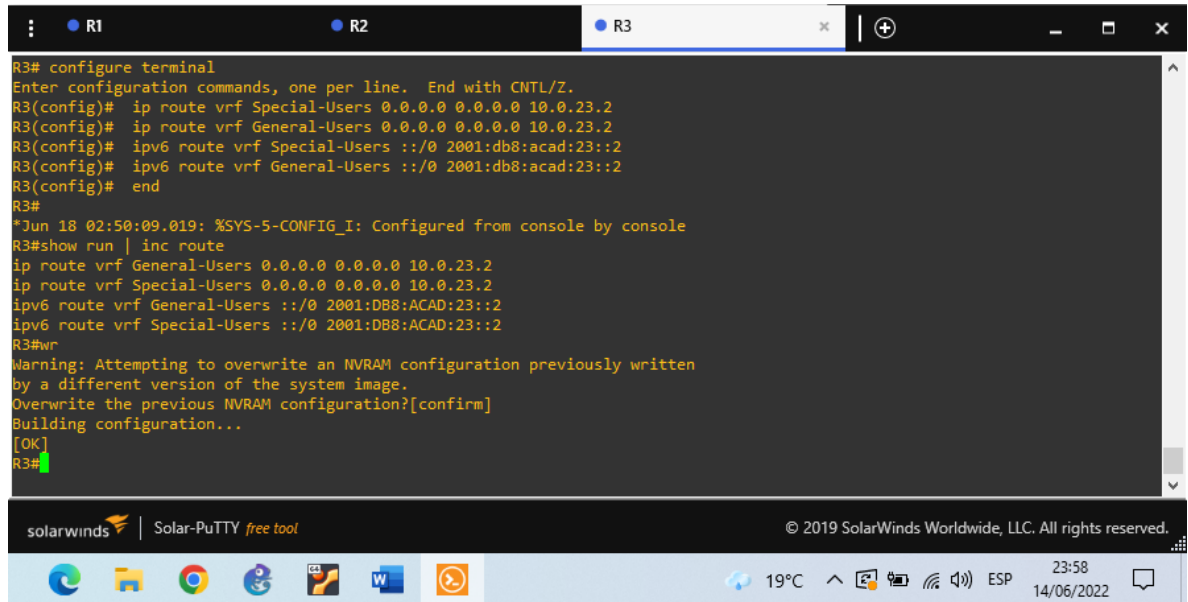
Configuración de ruta estática en ipv4 para VRF General-Users a través de R2

Configuración de ruta estática en ipv6 para VRF Special-Users a través de R2

Configuración de ruta estática en ipv6 para VRF General-Users a través de R2

Regresa al modo privilegiado

Figura 12. Visualización configuración, donde se incluyen las rutas en R3



```
R3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2
R3(config)# ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2
R3(config)# ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2
R3(config)# ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2
R3(config)# end
R3#
*Jun 18 02:50:09.019: %SYS-5-CONFIG_I: Configured from console by console
R3#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:23::2
R3#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#
```

Fuente: Autoría propia

En las figuras 10, 11 y 12 se observan las configuraciones que se están corriendo en los Routers R1, R2 y R3 respectivamente, en donde se filtra la información de las rutas estáticas y se evidencia el direccionamiento entre los Routers R1 y R3 hacia R2, y de R2 hacia R1 y R3.

Paso 2.4: Verificación conexión de VRF

Verificar la conexión entre VRF, realizando una prueba de "PING" desde R1 hacia R3, en ambas VRF y dirección IPv4 e IPv6.

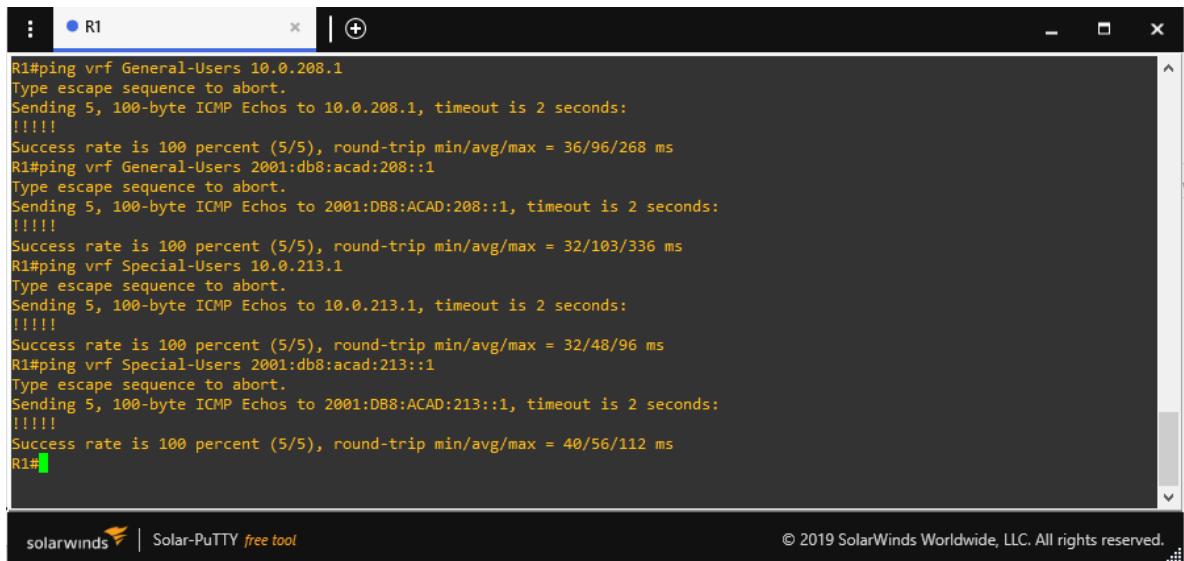
- **Router R1**

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

- **Descripción de cada comando utilizado**

- # Determinar el estado de la vrf General-Users con prueba “Ping” en dirección ipv4
- # Determinar el estado de la vrf General-Users con prueba “Ping” en dirección ipv6
- # Determinar el estado de la vrf Special-Users con prueba “Ping” en dirección ipv4
- # Determinar el estado de la vrf Special-Users con prueba “Ping” en dirección ipv6

Figura 13. Visualización conectividad entre R1 y R3 con cada VRF y familia.



```
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 = 36/96/268 ms
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 100 percent (5/5), round-trip min/avg/max = 32/103/336 ms
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 = 32/48/96 ms
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 = 40/56/112 ms
R1#
```

Fuente: Autoría propia

En la figura 13 se detalla el comando “ping” utilizado para determinar el estado de la conectividad entre los Routers R1 y R3 pasando por R2, se realiza la prueba en cuatro (4) oportunidades, en direccionamiento IPv4 hacia la VRF General-Users, en direccionamiento IPv6 hacia la VRF General-Users, en direccionamiento IPv4 hacia la VRF Special-Users y en direccionamiento IPv6 hacia la VRF Special-Users, y se observa que todas las pruebas de conectividad dieron exitosas.

Parte 3: Configuración Switches

Configurar los Switches D1, D2 y A1, con el propósito de evidenciar el correcto funcionamiento de la configuración de red, haciendo ping exitoso entre los computadores que se encuentran en cada VRF, esto se logra por medio de la correcta implementación de los enlaces troncales, configuración de EtherChannel y habitación de portfast, entre otros.

Tabla 4. Tareas y especificaciones de configuración en la Parte 3.

Paso	Tarea
3.1	Deshabilitar las interfaces de los Switch D1, D2 y A1.
3.2	Configurar y habilitar la interfaz Ethernet 2/3 como enlace troncal.
3.3	Configuración de EtherChannel, con la intención de agrupar lógicamente varios enlaces físicos, y tratándola como si fuese un solo enlace.
3.4	Configurar los puertos de acceso de cada Equipo de cómputo en D1, D2 y A1, habilitando el PortFast en cada uno y asignan su VLAN correspondiente.
3.5	Verificar la conectividad entre los Equipos de cómputo PC1 y PC2 y entre PC3 y PC4, tanto en IPv4 como en IPv6.

Fuente: Autoría propia

Paso 3.1: Deshabilitar interfaces

Deshabilitar las interfaces de los Switch D1, D2 y A1.

- **Switch D1**

```
configure terminal
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3, e4/0-3, e5/0-3
shutdown
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Ingresa a todas las interfaces por medio del comando rango
Se deshabilitan las interfaces
Regresa al modo de configuración global

- **Switch D2**

```
configure terminal
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3, e4/0-3, e5/0-3, e6/0-3, e7/0-3
shutdown
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Ingresa a todas las interfaces por medio del comando rango
Se deshabilitan las interfaces
Regresa al modo de configuración global

- **Switch A1**

```
configure terminal
interface range e0/0-3, e1/0-3
shutdown
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Ingresa a todas las interfaces por medio del comando rango
Se deshabilitan las interfaces
Regresa al modo de configuración global

Paso 3.2: Configuración enlace troncal

Configurar y habilitar la interfaz Ethernet 2/3 como enlace troncal, en donde se habilita el encapsulamiento dot1q y se añaden las VLAN del enlace troncal.

- **Switch D1**

```
configure terminal
interface ethernet2/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 8,13
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Ingresa a la interfaz Ethernet 2/3
# Se configura el tipo de encapsulación a utilizar
# Se configura el enlace troncal estático
# Se permite el puerto troncal a las vlan 8 y 13
# Se habilita la interfaz
# Regresa al modo de configuración global
```

- **Switch D2**

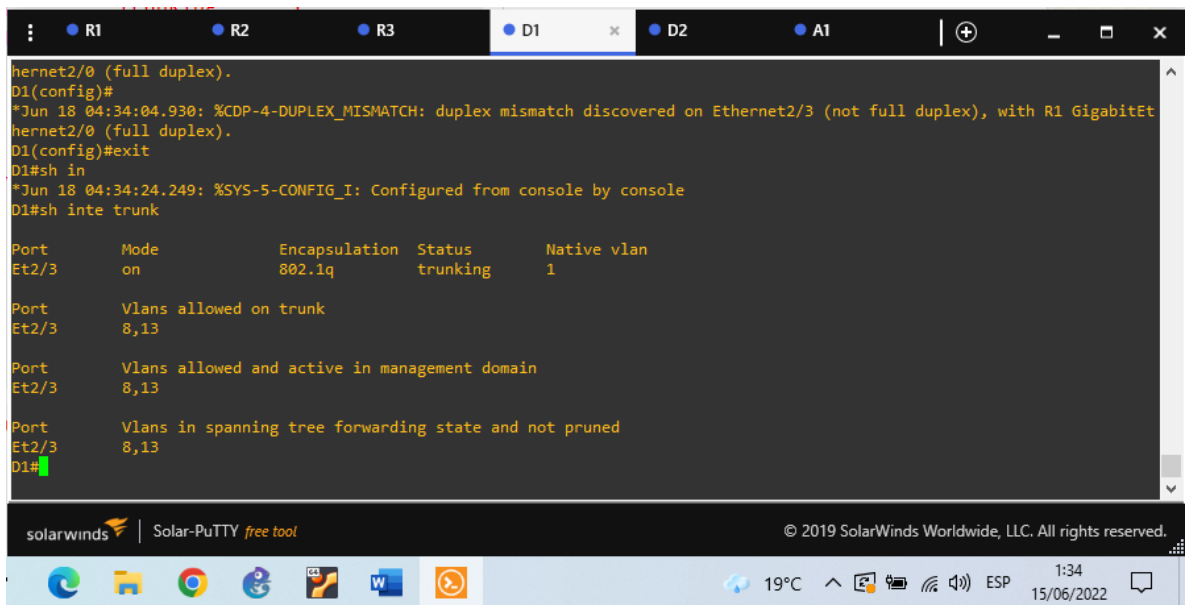
```
configure terminal
interface ethernet2/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 8,13
no shutdown
exit
```

- **Descripción de cada comando utilizado**

- # Ingresa a modo de configuración global
- # Ingresa a la interfaz Ethernet 2/3
- # Se configura el tipo de encapsulación a utilizar
- # Se configura el enlace troncal estático
- # Se permite el puerto troncal a las vlan 8 y 13
- # Se habilita la interfaz
- # Regresa al modo de configuración global

En las figuras 14 y 15 se observan los resultados en los Switches D1 y D2 respectivamente, al realizar el comando “show interface trunk”, el cual es utilizado para verificar varios aspectos de los enlaces troncales, como el puerto utilizado, el encapsulamiento, el estado, el modo, las VLANs asignadas, entre otros.

Figura 14. Visualización configuración enlaces troncales en D1



```
hernet2/0 (full duplex).
D1(config)#
*Jun 18 04:34:04.930: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/3 (not full duplex), with R1 GigabitEt
hernet2/0 (full duplex).
D1(config)#exit
D1#sh in
*Jun 18 04:34:24.249: %SYS-5-CONFIG_I: Configured from console by console
D1#sh inte trunk

Port      Mode           Encapsulation  Status        Native vlan
Et2/3     on             802.1q         trunking      1

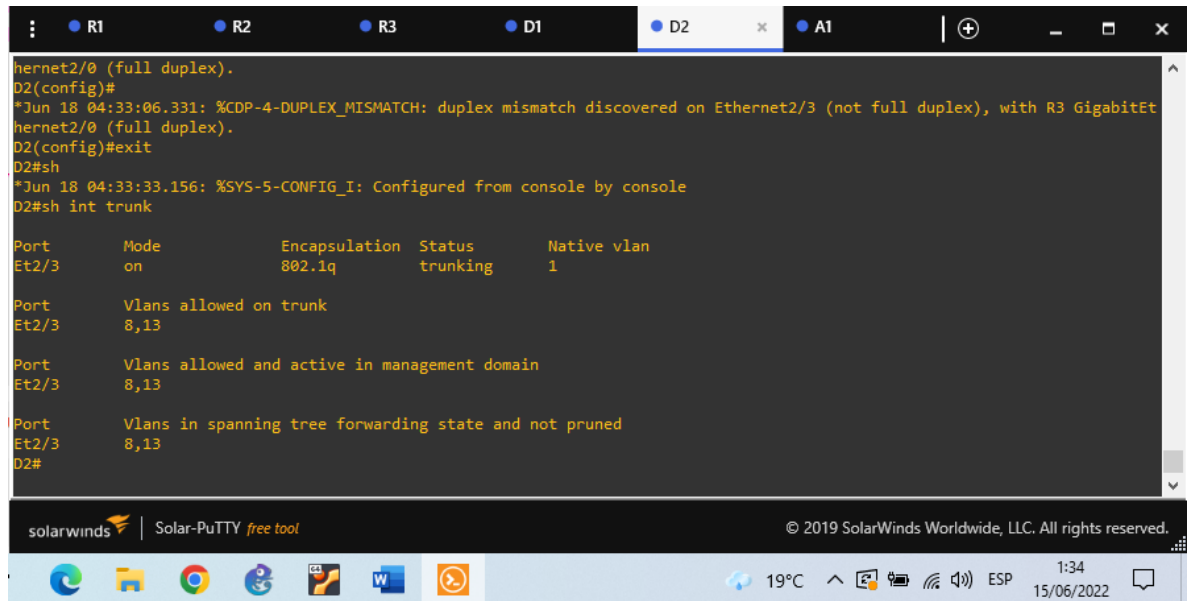
Port      Vlans allowed on trunk
Et2/3     8,13

Port      Vlans allowed and active in management domain
Et2/3     8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et2/3     8,13
D1#
```

Fuente: Autoría propia

Figura 15. Visualización configuración enlaces troncales en D2



```
hernet2/0 (full duplex).
D2(config)#
*Jun 18 04:33:06.331: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/3 (not full duplex), with R3 GigabitEt
hernet2/0 (full duplex).
D2(config)#exit
D2#sh
*Jun 18 04:33:33.156: %SYS-5-CONFIG_I: Configured from console by console
D2#sh int trunk

Port      Mode           Encapsulation  Status        Native vlan
Et2/3     on             802.1q         trunking      1

Port      Vlans allowed on trunk
Et2/3     8,13

Port      Vlans allowed and active in management domain
Et2/3     8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et2/3     8,13
D2#
```

Fuente: Autoría propia

Paso 3.3: Configuración EtherChannel

Configuración de EtherChannel, con la intención de agrupar lógicamente varios enlaces físicos como si fuese un solo enlace.

- **Switch D1**

```
configure terminal
interface port-channel 1
switchport mode access
switchport access vlan 8
interface range e1/1-2
switchport mode access
switchport access vlan 8
channel-group 1 mode desirable
no shutdown
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se ingresa a la configuración de la interfaz del canal del puerto 1
Se establece el puerto en modo de acceso
Se asigna el puerto a la VLAN 8
Se accede al rango de interfaces ethernet 1/1-2
Se establece el puerto en modo de acceso
Se asigna el puerto a la VLAN 8
Se asignan a el canal del puerto 1, y se determina el modo deseable
Se habilita la interfaz
Regresa al modo de configuración global

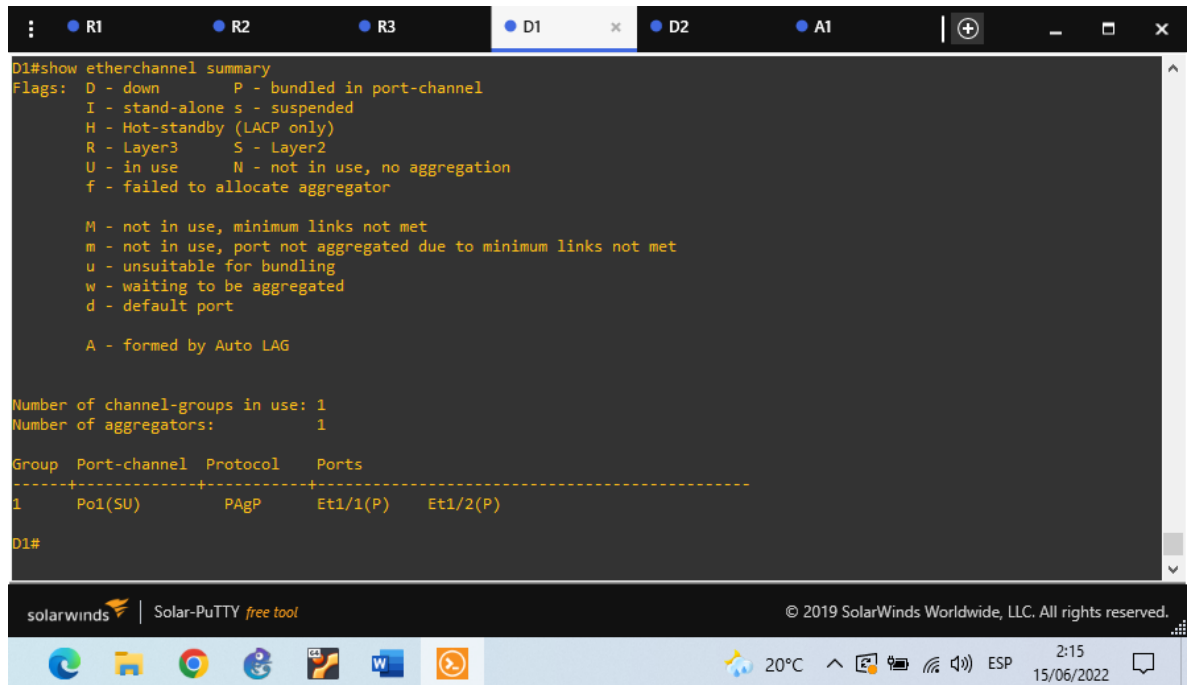
- **Switch A1**

```
configure terminal
interface port-channel 1
switchport mode access
switchport access vlan 8
interface range e0/1-2
switchport mode access
switchport access vlan 8
channel-group 1 mode desirable
no shutdown
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se ingresa a la configuración de la interfaz del canal del puerto 1
Se establece el puerto en modo de acceso
Se asigna el puerto a la VLAN 8
Se accede al rango de interfaces ethernet 1/1-2
Se establece el puerto en modo de acceso
Se asigna el puerto a la VLAN 8
Se asignan a el canal del puerto 1, y se determina el modo deseable
Se habilita la interfaz
Regresa al modo de configuración global

Figura 16. Visualización del canal de puertos en D1



```
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        Et1/1(P)  Et1/2(P)

D1#
```

Fuente: Autoría propia

En la figura 16 se muestra el resultado del comando “show etherchannel summary” donde se observa la información del canal de puerto, como el número de canales en uso, las interfaces asignadas, así como el tipo de puerto utilizado, en este caso “SU” indica que pertenece a la capa 2 y se encuentra en uso.

Paso 3.4: Configurar puertos de acceso

Configurar los puertos de acceso de cada Equipo de cómputo en D1, D2 y A1, habilitando el PortFast en cada uno y asignan su VLAN correspondiente.

- **Switch D1 – Interface Ethernet 5/3**

```
configure terminal
interface ethernet5/3
switchport mode access
switchport access vlan 13
spanning-tree portfast
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Ingresa a la interfaz Ethernet 5/3
# Se establece el puerto en modo de acceso
# Se asigna el puerto a la VLAN 13
# Se habilita el PortFast, dejando el puerto en estado de reenvió
# Se habilita la interfaz
# Regresa al modo de configuración global
```

- **Switch D2 – Interface Ethernet 5/3**

```
configure terminal
interface ethernet5/3
switchport mode access
switchport access vlan 13
spanning-tree portfast
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Ingresa a la interfaz Ethernet 5/3
# Se establece el puerto en modo de acceso
# Se asigna el puerto a la VLAN 13
# Se habilita el PortFast, dejando el puerto en estado de reenvió
# Se habilita la interfaz
# Regresa al modo de configuración global
```

- **Switch D2 – Interface Ethernet 6/0**

```
interface ethernet6/0
switchport mode access
switchport access vlan 8
spanning-tree portfast
no shutdown
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a la interfaz Ethernet 6/0
# Se establece el puerto en modo de acceso
# Se asigna el puerto a la VLAN 8
# Se habilita el PortFast, dejando el puerto en estado de reenvió
# Se habilita la interfaz
# Regresa al modo de configuración global
```

- **Switch A1 – Interface Ethernet 1/3**

```
configure terminal
interface ethernet1/3
switchport mode access
switchport access vlan 8
spanning-tree portfast
no shutdown
exit
```

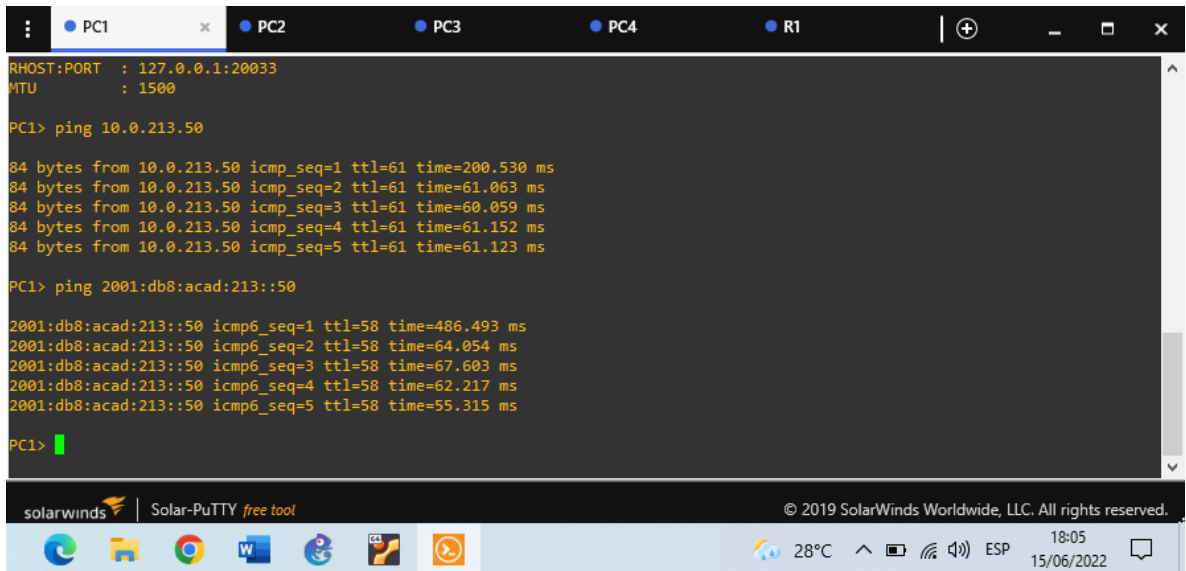
- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Ingresa a la interfaz Ethernet 1/3
# Se establece el puerto en modo de acceso
# Se asigna el puerto a la VLAN 8
# Se habilita el PortFast, dejando el puerto en estado de reenvió
# Se habilita la interfaz
# Regresa al modo de configuración global
```

Paso 3.5: Conectividad entre equipos de cómputo

Verificar la conectividad entre los Equipos de cómputo PC1 y PC2 y entre PC3 y PC4, tanto en IPv4 como en IPv6.

Figura 17. Visualización conectividad entre PC1 y PC2.



```
RHOST:PORT : 127.0.0.1:20033
MTU : 1500

PC1> ping 10.0.213.50

84 bytes from 10.0.213.50 icmp_seq=1 ttl=61 time=200.530 ms
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=61.063 ms
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=60.059 ms
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=61.152 ms
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=61.123 ms

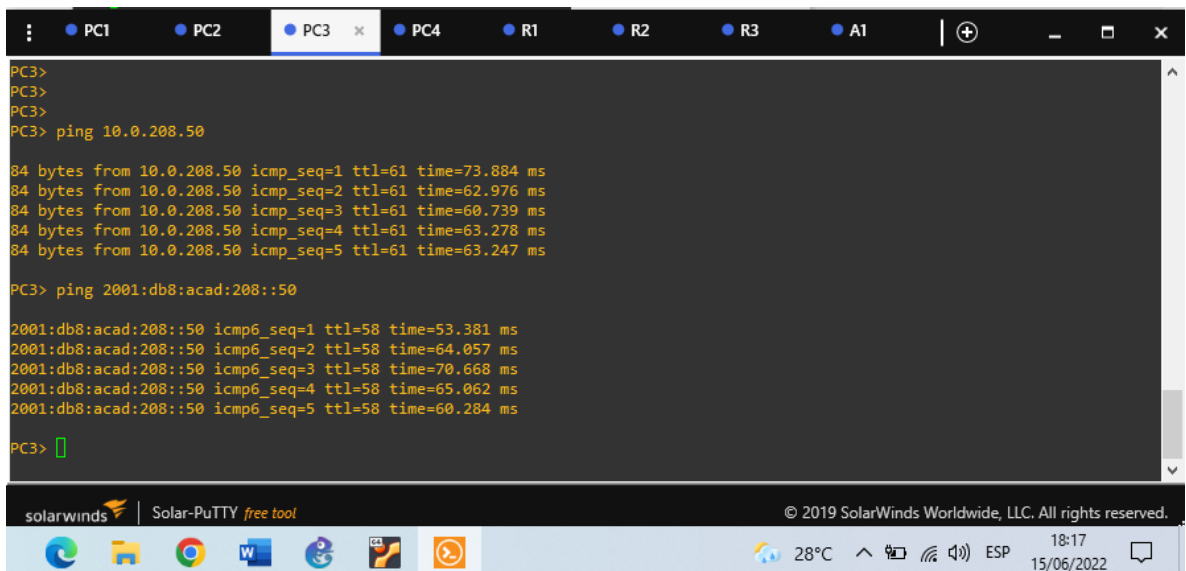
PC1> ping 2001:db8:acad:213::50

2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=486.493 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=64.054 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=67.603 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=62.217 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=55.315 ms

PC1> █
```

Fuente: Autoría propia

Figura 18. Visualización conectividad entre PC3 y PC4.



```
PC3>
PC3>
PC3>
PC3> ping 10.0.208.50

84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=73.884 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=62.976 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=60.739 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=63.278 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=63.247 ms

PC3> ping 2001:db8:acad:208::50

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=53.381 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=64.057 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=70.668 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=65.062 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=60.284 ms

PC3> █
```

Fuente: Autoría propia

En las figuras 17 y 18 se reflejan las pruebas de conectividad entre PC1 y PC2, así como PC3 y PC4 respectivamente, estas verificaciones se realizan tanto en IPv4 como en IPv6 e infiere que la configuración se realizó de manera exitosa, puesto que se tiene conectividad en la VRF de extremo a extremo.

Parte 4: Configurar seguridad de los dispositivos

Instaurar la configuración necesaria para establecer los mecanismos de seguridad en los dispositivos de red de la topología, configurar el modo EXEC privilegiado, además de crear cuenta de usuario local y habilitar la autenticación AAA.

Tabla 5. Tareas y especificaciones de configuración en la Parte 4.

Paso	Tarea
4.1	Configurar y habilitar la seguridad de todos los dispositivos de red, con un tipo de algoritmo scrypt y con contraseña, en el modo EXEC privilegiado.
4.2	Configuración de una cuenta de usuario local, con nivel de privilegio 15, tipo de algoritmo scrypt y contraseña.
4.3	Configuración y habilitación de la autenticación AAA usando la base de datos local.

Paso 4.1: Configuración seguridad en modo EXEC

Configurar y habilitar la seguridad de todos los dispositivos de red, con un tipo de algoritmo scrypt y con contraseña, en el modo EXEC privilegiado.

- **Router R1**

```
configure terminal
enable algorithm-type scrypt secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se configura y habilita la contraseña al modo EXEC privilegiado por algoritmo
SCRYPT
# Regresa al modo privilegiado
```

- **Router R2**

```
configure terminal
enable algorithm-type scrypt secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se configura y habilita la contraseña al modo EXEC privilegiado por algoritmo
SCRYPT
# Regresa al modo privilegiado
```

- **Router R3**

```
configure terminal
enable algorithm-type scrypt secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se configura y habilita la contraseña al modo EXEC privilegiado por algoritmo
SCRYPT
# Regresa al modo privilegiado
```

- **Switch D1**

```
configure terminal
enable secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se configura y habilita la contraseña al modo EXEC privilegiado
# Regresa al modo privilegiado
```

- **Switch D2**

```
configure terminal
enable secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se configura y habilita la contraseña al modo EXEC privilegiado
# Regresa al modo privilegiado
```

- **Switch A1**

```
configure terminal
enable secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se configura y habilita la contraseña al modo EXEC privilegiado
# Regresa al modo privilegiado
```

Paso 4.2: Configuración seguridad con usuario local

Configuración de una cuenta de usuario local con nivel de privilegio 15 que indica que incluye todos los comandos, el tipo de algoritmo scrypt y la contraseña.

- **Router R1**

```
configure terminal
username admin privilege 15 algorithm-type scrypt secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se indica el nombre de usuario, el nivel de privilegio y la clave encriptada
```

Regresa al modo privilegiado

- **Router R2**

```
configure terminal
username admin privilege 15 algorithm-type scrypt secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se indica el nombre de usuario, el nivel de privilegio y la clave encriptada
Regresa al modo privilegiado

- **Router R3**

```
configure terminal
username admin privilege 15 secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se indica el nombre de usuario, el nivel de privilegio y la clave encriptada
Regresa al modo privilegiado

- **Switch D1**

```
configure terminal
username admin privilege 15 secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se indica el nombre de usuario, el nivel de privilegio y la clave encriptada
Regresa al modo privilegiado

- **Switch D2**

```
configure terminal
username admin privilege 15 secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se indica el nombre de usuario, el nivel de privilegio y la clave encriptada
# Regresa al modo privilegiado
```

- **Switch A1**

```
configure terminal
username admin privilege 15 secret cisco12345cisco
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global
# Se indica el nombre de usuario, el nivel de privilegio y la clave encriptada
# Regresa al modo privilegiado
```

Paso 4.3: Configuración y autenticación AAA

Configuración y habilitación de la autenticación AAA usando la base de datos local.

- **Router R1**

```
configure terminal
aaa new-model
aaa authentication login default local
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se crea un nuevo modelo de configuración AAA
Se habilita la autenticación AAA y se compara con los usuarios locales
Regresa al modo privilegiado

- **Router R2**

```
configure terminal  
aaa new-model  
aaa authentication login default local  
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se crea un nuevo modelo de configuración AAA
Se habilita la autenticación AAA y se compara con los usuarios locales
Regresa al modo privilegiado

- **Router R3**

```
configure terminal  
aaa new-model  
aaa authentication login default local  
exit
```

- **Descripción de cada comando utilizado**

Ingresa a modo de configuración global
Se crea un nuevo modelo de configuración AAA
Se habilita la autenticación AAA y se compara con los usuarios locales #
Regresa al modo privilegiado

- **Switch D1**

```
configure terminal  
aaa new-model  
aaa authentication login default local  
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global  
# Se crea un nuevo modelo de configuración AAA  
# Se habilita la autenticación AAA y se compara con los usuarios locales  
# Regresa al modo privilegiado
```

- **Switch D2**

```
configure terminal  
aaa new-model  
aaa authentication login default local  
exit
```

- **Descripción de cada comando utilizado**

```
# Ingresa a modo de configuración global  
# Se crea un nuevo modelo de configuración AAA  
# Se habilita la autenticación AAA y se compara con los usuarios locales  
# Regresa al modo privilegiado
```

- **Switch A1**

```
configure terminal  
aaa new-model  
aaa authentication login default local  
exit
```

- Descripción de cada comando utilizado

- # Ingresa a modo de configuración global
- # Se crea un nuevo modelo de configuración AAA
- # Se habilita la autenticación AAA y se compara con los usuarios locales
- # Regresa al modo privilegiado

Figura 19. Verificación de configuración AAA y usuario en Router R1

```

R1#sh vrf
  Name          Default RD      Protocols      Interfaces
  General-Users <not set>      ipv4,ipv6     Gi1/0.2
  General-Users 10.0.108.1     General-Users  up
  Special-Users 10.0.12.1     Special-Users  up
  Special-Users 10.0.113.1    Special-Users  up

R1#
R1#
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 9 $9$RZo8abJ/.8UwZK$YPrVjysGK8F9QSo4bqDJKUGK4o5q$W0sKtkWYV.t5rQ
R1#
  
```

Fuente: Autoría propia

Figura 20. Verificación de configuración AAA y usuario en Router R2

```

R2#sh vrf
  Interface      IP-Address      VRF          Protocol
  Gi1/0.2        10.0.12.2       General-Users up
  Gi2/0.2        10.0.23.2       General-Users up
  Gi1/0.1        10.0.12.2       Special-Users up
  Gi2/0.1        10.0.23.2       Special-Users up

R2#sh vrf
  Name          Default RD      Protocols      Interfaces
  General-Users <not set>      ipv4,ipv6     Gi1/0.2
  General-Users 10.0.108.1     General-Users  up
  Special-Users 10.0.12.1     Special-Users  up
  Special-Users 10.0.113.1    Special-Users  up

R2#
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 9 $9$H.qLFwYKvROrz4$u0Qa8u0tiy5hwgueioAWdeyPRGJ4gN1QCXFzSUqIMzE
R2#
  
```

Fuente: Autoría propia

Figura 21. Verificación de configuración AAA y usuario en Router R3

```
Interface      IP-Address    VRF            Protocol
Gi1/0.2       10.0.23.3    General-Users  up
Gi2/0.2       10.0.208.1   General-Users  up
Gi1/0.1       10.0.23.3    Special-Users  up
Gi2/0.1       10.0.213.1   Special-Users  up
R3#sh vrf
  Name          Default RD    Protocols     Interfaces
  General-Users <not set>    ipv4,ipv6    Gi1/0.2
  Special-Users <not set>    ipv4,ipv6    Gi2/0.2
  Special-Users <not set>    ipv4,ipv6    Gi1/0.1
  Special-Users <not set>    ipv4,ipv6    Gi2/0.1
R3#
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 9 $9$Eub5y32pXwpTfK$Tqp0ECynIX1rbY55P4Lfeker1XK6nA8SJ2H2gAwdDKg
R3#
```

Fuente: Autoría propia

Figura 22. Verificación de configuración AAA y usuario en Switch A1

```
A1#sh run | include route
A1#sh run | include ro
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
ipv6 unicast-routing
  channel-group 1 mode desirable
  channel-group 1 mode desirable
ip forward-protocol nd
control-plane
  logging synchronous
  logging synchronous
A1#
A1#
A1#
A1#show run | include aaa|username
username admin privilege 15 secret 5 $1$hFpm$3yR9I77htM9nDp77x0N0F.
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```

Fuente: Autoría propia

Figura 23. Verificación de configuración AAA y usuario en Switch D1

```
D1, ENCOR Skills Assessment, Scenario 2
User Access Verification
Username: admin
Password:
D1#show run | include aaa|username
username admin privilege 15 secret 5 $1$tjEM$c/PzhF3lJeJ58xM/mPCzW.
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
*Jun 18 21:03:29.755: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/3 (not full duplex), with R1 GigabitEt
hernet2/0 (full duplex).
D1#
```

Fuente: Autoría propia

Figura 24. Verificación de configuración AAA y usuario en Switch D2

```
*Jun 18 21:01:43.327: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/3 (not full duplex), with R3 GigabitEt
hernet2/0 (full duplex).
*Jun 18 21:02:39.488: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/3 (not full duplex), with R3 GigabitEt
hernet2/0 (full duplex). D2, ENCOR Skills Assessment, Scenario 2
User Access Verification
Username: admin
Password:
D2#show run | include aaa|username
username admin privilege 15 secret 5 $1$y0xm$YlDPm6NqRVQ8Gy/2cJrtH0
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```

Fuente: Autoría propia

En las figuras 19, 20, 21, 22, 23 y 24, correspondientes al Router R1, Router R2, Router R3, Switch D1, Switch D2 y Switch A1 respectivamente, se visualiza la respuesta al comando “show run | include aaa|username” utilizado para observar la configuración que se está corriendo en el momento y filtrando las palabras “aaa” y “username” lo que hace referencia al nombre de usuario creado y el nivel de

privilegio, así como la contraseña encriptada, además de la configuración del nuevo modelo aaa, la autenticación creada localmente y verificación del ID de sesión para el servicio aaa.

SIMULACIÓN

<https://drive.google.com/drive/folders/16qowcWj3uDj2e2yv0fyisxrD7HnmF2my?usp=sharing>

CONCLUSIONES

Hoy en día es fundamental la configuración básica de las Lan Virtuales, y es que, el crear redes lógicas nos permite segmentar adecuadamente la red para así usar cada subinterfaz de forma diferente, ya sea como backup, para equilibrar cargas entre redes, aumentar el nivel de seguridad, optimizar la red, entre muchas otras características. El utilizar VLAN en el presente proyecto es fundamental ya que, se puede dividir la red lógicamente para dos VRF como lo es General-Users y Special-Users, cada uno con la posibilidad de configurar de forma diferente.

La implementación de las dos VRF facilita el separar el tráfico de la red utilizando la misma cantidad de routers, ganando flexibilidad y reduciendo el dinero invertido, y es que las VRF permiten que el router ejecute más de una tabla de enrutamiento simultáneamente, siendo estas independientes entre sí y en el caso del proyecto utilizando la misma dirección IP. La configuración de las VRF se basa en la definición de cada una, asignación de protocolos de enrutamiento y posterior a ello, asociar a cada VLAN creada.

A lo largo de las actividades se ha visto la importancia que tiene la seguridad en los diferentes dispositivos de red, y es que al tener un dispositivo “de fabrica” se tiene opciones generales que si no se configuran pueden presentar un problema a cualquier red, es por esto que, a priori la primer recomendación en la implementación es apagar todos los puertos y solo encender los puertos que se utilizan, además, estos deberían de tener una contraseña de ingreso y estar cifrados, para así evitar el ingreso de usuarios no autorizados a los dispositivos, un ejemplo de ello es el algoritmo SCRYPT, el cual es considerado un algoritmo de difícil descifrado.

Con el desarrollo en el simulador de red GNS3 se encontraron diferentes inconvenientes, desde el proceso de instalación de las IOS como la configuración de los dispositivos de red, y es que las versiones entre dispositivos permiten una gran variedad de comandos que se dejan de utilizar, así como comandos nuevos y nuevas mejoras en la configuración. Sin embargo, con la realización exitosa de la configuración de los dispositivos se observa el gran poder de funcionamiento del software GNS3, que permite la configuración simulada como si fuese un ambiente real.

BIBLIOGRAFÍA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). BGP. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

UNAD (2017). Configuración de Switches y Routers [OVA]. <https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC>