

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CESAR AUGUSTO GONZALEZ PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
DOSQUEBRADAS
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CESAR AUGUSTO GONZALEZ PEREZ

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

DIRECTOR:
Msc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
DOSQUEBRADAS
2023

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Dosquebradas, 4 de Mayo del 2023

AGRADECIMIENTOS

Quiero agradecerle principalmente a Dios por bendecirme todos los días y darme vida y salud para seguir adelante, por guiarme por el camino correcto y cuidarme durante todo mi tiempo de vida estudiantil, por ser mi apoyo y fortaleza en esos momentos de debilidad en los cuales quise dejar todo, gracias Dios por nunca abandonarme y siempre estar ahí para darme nuevas fuerzas.

Agradecerles a mis padres por ser los principales creyentes en mi sueño, por confiar y creer en que yo si sería capaz de lograrlo, gracias a esa inspiración era que podía seguir adelante cada día sin importar lo difícil de la situación, por los consejos que me dieron en momentos difíciles y por los principios que me enseñaron desde niño ya que gracias a eso soy el hombre que soy y espero ser un gran profesional.

Agradecerle a la Universidad UNAD, a sus docentes por haber compartido sus conocimientos a lo largo de mi formación como profesional.

Agradecerles a todas las personas que me brindaron su apoyo con las actividades que hice para poder financiar mis estudios, a mis amigos y compañeros que estuvieron a mi lado cuando necesité un apoyo moral para poder seguir adelante muchas gracias por todo.

CONTENIDO

	Pág.
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN.....	10
DESARROLLO	11
1. ESCENARIO.....	11
1.1 PARTE 1: CONSTRUCCIÓN DE LA RED Y DEL DIRECCIONAMIENTO DE LA RED	11
1.2 PARTE 2: CONFIGURACIÓN DE LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS Y ASIGNACIÓN DE DIRECCIONES IP A LOS PCS.....	13
1.3 PARTE 3: CONFIGURACIÓN VRF Y EL ENRUTAMIENTO ESTÁTICO.....	20
1.4 PARTE 4: CONFIGURACIÓN CAPA 2	29
1.5 PARTE 5: CONFIGURACIÓN DE SEGURIDAD	35
CONCLUSIONES	40
REFERENCIAS	41

LISTA DE FIGURAS

	Pág.
Figura 1 Configuración de los Slot en los Switches	11
Figura 2 Configuración de los Slot en los Routers	12
Figura 3 Realización de la topología en GNS3.	12
Figura 4 Guardando las configuraciones en R1	17
Figura 5 Guardando las configuraciones en R2.....	18
Figura 6 Guardando las configuraciones en R3.....	18
Figura 7 Guardando las configuraciones en D1	18
Figura 8 Guardando las configuraciones en D2.....	18
Figura 9 Guardando las configuraciones en A1	18
Figura 10 Configuración de las direcciones IP en PC1	19
Figura 11 Configuración de las direcciones IP en PC2.....	19
Figura 12 Configuración de las direcciones IP en PC3.....	19
Figura 13 Configuración de las direcciones IP en PC4.....	20
Figura 14 Ping vrf general-users 10.0.208.7	27
Figura 15 Ping vrf general-users 2001:db8:acad:208::1	27
Figura 16 Ping vrf special-users 10.0.213.7.....	27
Figura 17 Ping vrf special-users 2001:db8:acad:213::1	27
Figura 18 Verificación de VRF en R1.....	27
Figura 19 Verificación de VRF en R2.....	28
Figura 20 Verificación de VRF en R3.....	28
Figura 21 Verificación de las rutas estáticas en R1	28
Figura 22 Verificación de las rutas estáticas en R2	28
Figura 23 Verificación de las rutas estáticas en R3	28
Figura 24 Verificación de conexión de PC1 a PC2	32
Figura 25 Verificación de conexión de PC2 a PC1	32
Figura 26 Verificación de conexión de PC3 a PC4	33
Figura 27 Verificación de conexión de PC4 a PC3	33
Figura 28 Verificación troncal en D1	33
Figura 29 Verificación troncal en D2	34
Figura 30 Verificación de los puertos etherchannel en D1.....	34
Figura 31 Verificación de los puertos etherchannel en A1	34
Figura 32 Verificación de la interfaz e0/3 en D1	35
Figura 33 Verificación de la interfaz e0/1 y e0/2 en D2.....	35
Figura 34 Verificación de la interfaz e0/2 en A1.....	35
Figura 35 Verificación de la seguridad en R1	38
Figura 36 Verificación de la seguridad en R2	38
Figura 37 Verificación de la seguridad en R3	38
Figura 38 Verificación de la seguridad en D1	38
Figura 39 Verificación de la seguridad en D2	38
Figura 40 Verificación de la seguridad en A1	39

LISTA DE TABLAS

	Pág.
Tabla 1 Tabla de direccionamiento.....	13
Tabla 2 Configuración básica del Router R1	13
Tabla 3 Configuración básica del Router R2	14
Tabla 4 Configuración básica del Router R3	14
Tabla 5 Configuración básica del Switch D1.....	15
Tabla 6 Configuración básica del Switch D2.....	16
Tabla 7 Configuración básica del Switch A1.....	16
Tabla 8 Configuración VRF-Lite del Router R1.....	20
Tabla 9 Configuración VRF-Lite del Router R2.....	20
Tabla 10 Configuración VRF-Lite del Router R3.....	21
Tabla 11 Configuración de las rutas estáticas del Router R1	21
Tabla 12 Configuración de las rutas estáticas del Router R2	23
Tabla 13 Configuración de las rutas estáticas del Router R3	24
Tabla 14 Configuración de las rutas estáticas del Router R1	25
Tabla 15 Configuración de las rutas estáticas del Router R2	25
Tabla 16 Configuración de las rutas estáticas del Router R3	26
Tabla 17 Apagado de las interfaces de los switches	29
Tabla 18 Configuración de los enlaces troncales en D1	29
Tabla 19 Configuración de los enlaces troncales en D2	29
Tabla 20 Configuración Etherchannel en D1	30
Tabla 21 Configuración Etherchannel en A1	30
Tabla 22 Configuración del acceso en D1	31
Tabla 23 Configuración del acceso en D2	31
Tabla 24 Configuración del acceso en A1	31
Tabla 25 Configuración de seguridad en R1.....	36
Tabla 26 Configuración de seguridad en R2.....	36
Tabla 27 Configuración de seguridad en R3.....	36
Tabla 28 Configuración de seguridad en D1.....	37
Tabla 29 Configuración de seguridad en D2.....	37
Tabla 30 Configuración de seguridad en A1.....	37

GLOSARIO

DIRECCIONAMIENTO: Configuración de la red de tal forma que a cada equipo le corresponde una única y exclusiva dirección, con el fin de que no haya errores a la hora de transmitir y recibir datos.

ENRUTAMIENTO: Proceso de selección de rutas en cualquier red.

ENRUTAMIENTO ESTÁTICO: Un administrador de red utiliza tablas estáticas para configurar y seleccionar manualmente las rutas de red.

ENRUTAMIENTO VIRTUAL Y REENVÍO (VRF): Es una tecnología incluida en routers de red IP (Internet Protocol) que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar al simultáneamente.

PROTOCOLO DE AGREGACIÓN DE PUERTOS (PAGP): Es un protocolo de red propiedad de Cisco Systems, que se utiliza para la agregación de enlaces automatizada de puertos de conmutadores Ethernet, conocida como EtherChannel.

PORTFAST: Es una función que permite a las estaciones de usuarios finales obtener acceso inmediato a la red de capa 2.

PUERTO TRUNK: Es un enlace entre dos switches. En dicho enlace cada puerto debe configurarse en cada switch en modo trunk. De esta forma, el tráfico de las VLANs fluye a través de los diferentes switches en la red.

SPANNING TREE PROTOCOL (STP): Se diseñó para permitir la existencia de varios caminos físicos que otorgasen redundancia a nuestras redes mientras se evitaba que la posible generación de bucles afectase negativamente.

RED DE ÁREA LOCAL VIRTUAL (VLAN): Es una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo.

RESUMEN

El presente explica paso a paso la administración correcta de una red; en la cual, el propósito es establecer independencia y conexión dentro de la misma mejorando la comunicación entre el grupo de los usuarios generales y el grupo de los usuarios especiales que se crearon a través de utilizar la tecnología multi-VRF. La red se construyó en el software GNS3 teniendo en cuenta primeramente la realización de las configuraciones iniciales en cada dispositivo agregado al área de trabajo del software; de modo que, seguidamente se seleccionan las rutas de forma manual en los routers; se configuran los puertos en modo trunk, se utiliza el protocolo PAgP para la configuración etherchannel en los switches, se asignan los puertos de acceso según las VLAN y se configura la seguridad de toda la red por medio del protocolo AAA. De esta manera, los resultados evidencian un acceso controlado y seguro y asimismo conectividad en cada grupo que conforma la red.

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

ABSTRACT

This explains step by step the correct management of a network; in which, the purpose is to establish independence and connection within it by improving communication between the group of general users and the group of special users that were created through using multi-VRF technology. The network was built on GNS3 software taking into account first the initial configurations in each device added to the software workspace; so that routes are selected manually on routers; ports are configured in trunk mode, the PAgP protocol is used for etherchannel configuration on switches, access ports are assigned according to VLANs and the security of the entire network is configured by means of the AAA protocol. In this way, the results show controlled and secure access and connectivity in each group that makes up the network.

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

INTRODUCCIÓN

Es esencial elegir una configuración de red correcta para respaldar el flujo de tráfico a través de esta, así como respaldar y mejorar la seguridad y la estabilidad de la red.

Por lo tanto, el presente documento está basado en el diseño y configuración de un escenario LAN/WAN manejando herramientas de simulación en el software GNS3, con el fin de realizar un análisis sobre el comportamiento de múltiples configuraciones, se evalúa el desempeño de los routers y de los switches con direccionamiento IPv4 e IPv6 mediante el uso de comandos de administración avanzados para protocolos de enrutamiento; asimismo se diseña e implementan soluciones de red escalables, mediante el uso de los principios y conmutación de paquetes en ambientes LAN y WAN.

Todo esto con el fin de que los dispositivos que conforman la red intercambien información y sus recursos de forma segura.

DESARROLLO

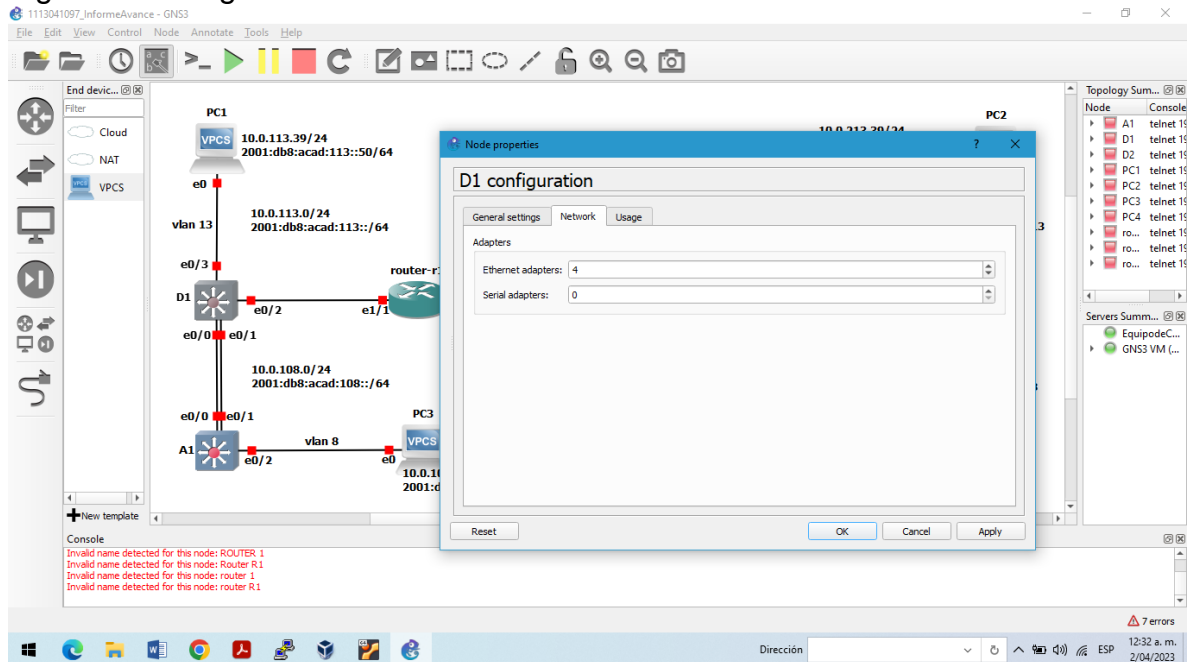
1. ESCENARIO

En este escenario se configurara la tecnología multi-VRF en la red para que admita "Usuarios generales" y "Usuarios especiales" considerando que los dos grupos no deberán poder comunicarse entre sí. Se debe configurar los router, los switch y PCs para que acepten tanto la conectividad IPv4 como IPv6, deberá haber accesibilidad completa de un extremo a otro.

1.1 PARTE 1: CONSTRUCCIÓN DE LA RED Y DEL DIRECCIONAMIENTO DE LA RED

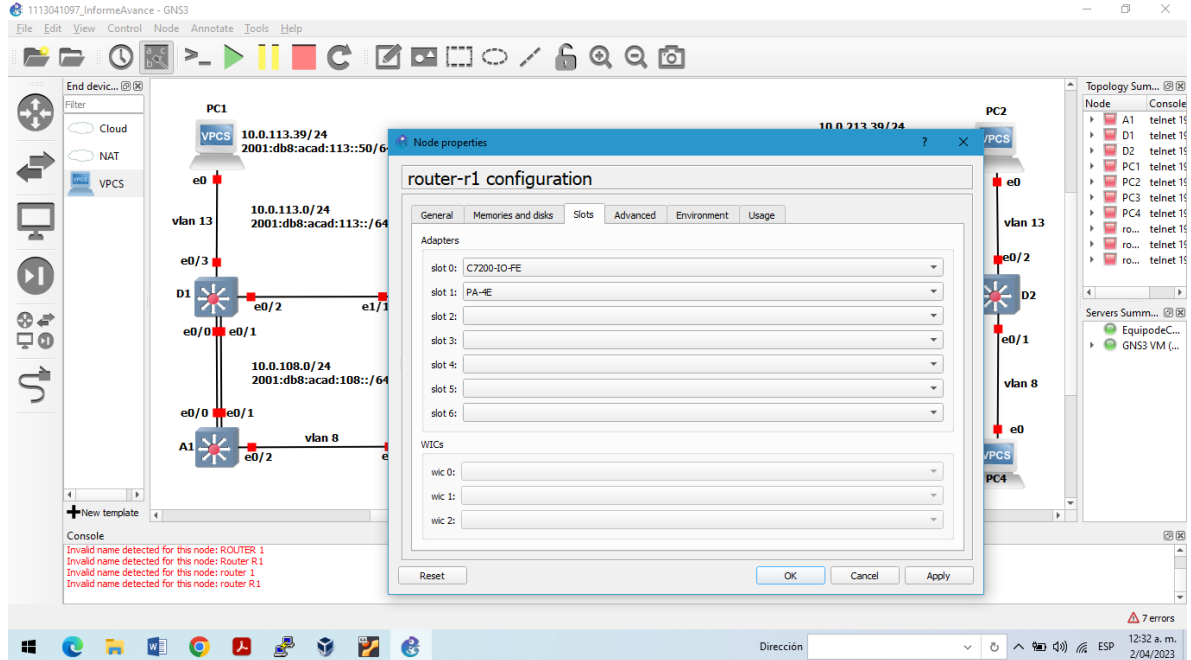
La red está compuesta por: 3 Routers, 2 Switches, 1 Switch, y 4 PCs, además se tiene en cuenta que los dispositivos se conectan por medio de cables Ethernet. Despues de agregar los dispositivos a la ventana de trabajo de GNS3 se configuran los slots para que poder realizar el cableado en la red.

Figura 1 Configuración de los Slot en los Switches



Fuente: Propia

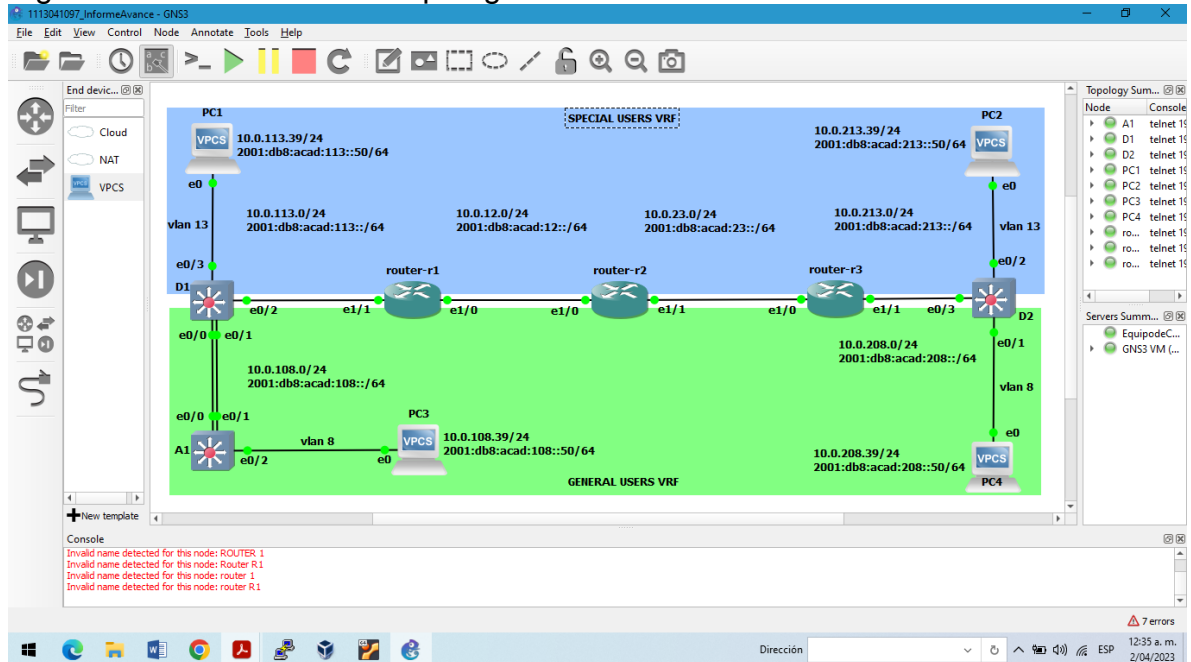
Figura 2 Configuración de los Slot en los Routers



Fuente: Propia

Se construye la red, conectando cada uno de sus dispositivos mediante cables Ethernet como se muestra en la topología.

Figura 3 Realización de la topología en GNS3.



Fuente: Propia

Tabla 1 Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E1/0.1	10.0.12.3/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.3/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.3/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.3/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.9/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.9/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.9/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.9/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.7/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.7/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.7/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.7/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.39/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.39/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.39/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.39/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Guía CCNP

1.2 PARTE 2: CONFIGURACIÓN DE LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS Y ASIGNACIÓN DE DIRECCIONES IP A LOS PCS

Para cada dispositivo se realiza en el modo de configuración global de cada uno de ellos aplicando los comandos que se aprecian en las siguientes tablas.

Router R1

Tabla 2 Configuración básica del Router R1

Comando	Descripción
configure terminal	#Cambia a modo Configuración
hostname R1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router

line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración

Fuente: Propia

Router R2

Tabla 3 Configuración básica del Router R2

Comando	Descripción
configure terminal	#Cambia a modo Configuración
hostname R2	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # R2, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración

Fuente: Propia

Router R3

Tabla 4 Configuración básica del Router R3

Comando	Descripción
configure terminal	#Cambia a modo Configuración
hostname R3	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router

no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración

Fuente: Propia

Switch D1

Tabla 5 Configuración básica del Switch D1

Comando	Descripción
configure terminal	#Cambia a modo Configuración
hostname D1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración
vlan 8	#Crea una VLAN con un número de ID válido
name general-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado

vlan 13	#Crea una VLAN con un número de ID válido
name special-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado

Fuente: Propia

Switch D2

Tabla 6 Configuración básica del Switch D2

Comando	Descripción
configure terminal	#Cambia a modo Configuración
hostname D2	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración
vlan 8	#Crea una VLAN con un número de ID válido
name general-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado
vlan 13	#Crea una VLAN con un número de ID válido
name special-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado

Fuente: Propia

Switch A1

Tabla 7 Configuración básica del Switch A1

Comando	Descripción
configure terminal	#Cambia a modo Configuración
hostname A1	#Asignación de un nombre
ipv6 unicast-routing	#Habilita el routing IPv6 en el router
no ip domain lookup	#Desactiva la traducción de nombres a dirección del router basado en DNS del host
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #	#Permite configurar un mensaje de advertencia el mensaje aparece al encender el router
line con 0	#Ingresar al modo de configuración de línea 0 de la consola
exec-timeout 0 0	#Establece el tiempo de espera inactivo de la sesión remota
logging synchronous	#Evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
exit	#Sale del modo de configuración
vlan 8	#Crea una VLAN con un número de ID válido
name general-users	#Especifica un nombre único para identificar la VLAN
exit	#Vuelve al modo EXEC privilegiado
vlan 13	#Crea una VLAN con un número de ID válido
name special-users	#Especifica un nombre único para identificar la VLAN

Fuente: Propia

En cada uno de los dispositivos anteriores por último se coloca el comando running-config al archivo startup-config.

#copy running-config startup-config

Figura 4 Guardando las configuraciones en R1

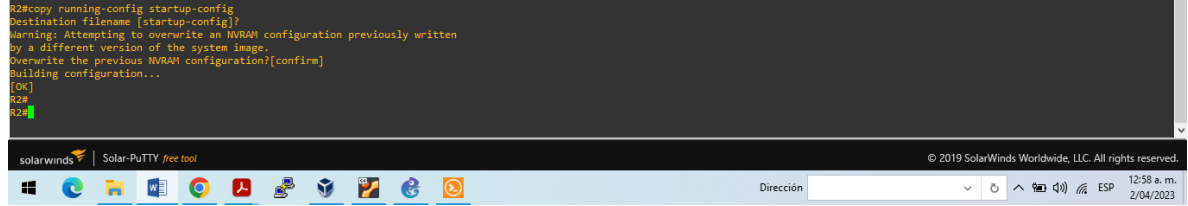
```

R1#copy running-config startup-config
Destination filename [startup-config]?
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#

```

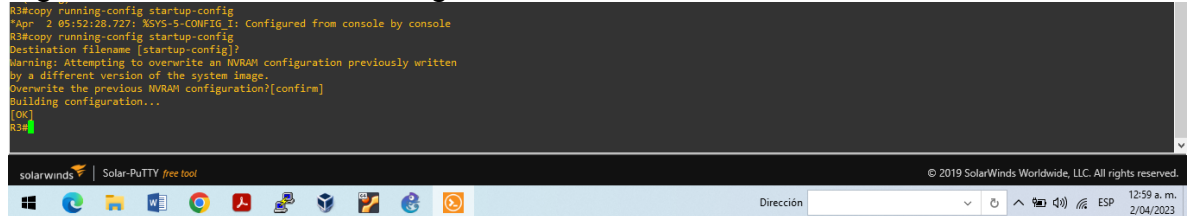
Fuente: Propia

Figura 5 Guardando las configuraciones en R2



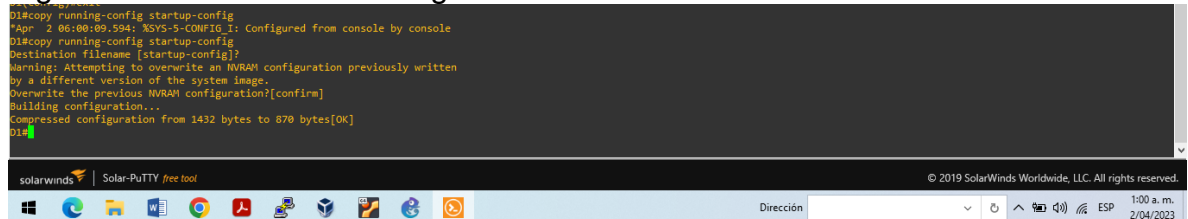
Fuente: Propia

Figura 6 Guardando las configuraciones en R3



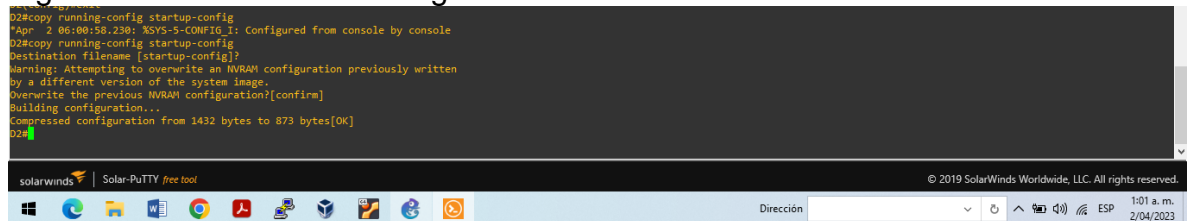
Fuente: Propia

Figura 7 Guardando las configuraciones en D1



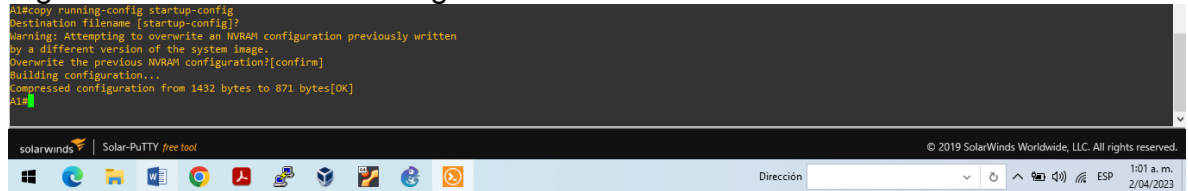
Fuente: Propia

Figura 8 Guardando las configuraciones en D2



Fuente: Propia

Figura 9 Guardando las configuraciones en A1



Fuente: Propia

A los PC1, PC2, PC3 y PC4, de acuerdo a la Tabla 1 se les asigna la dirección IP.

PC1

```
#ip 10.0.113.39/24 10.0.113.3  
#ip 2001:DB8:ACAD:113::50/64
```

Figura 10 Configuración de las direcciones IP en PC1

```
PC1> sh  
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT  
PC1 10.0.113.39/24 10.0.113.3 00:50:79:66:68:00 20032 127.0.0.1:20033  
fe80::25e:79ff:fe66:6800/64  
2001:db8:acad:113::50/64  
PC1>
```

Fuente: Propia

PC2

```
#ip 10.0.213.39/24 10.0.213.7  
#ip 2001:DB8:ACAD:213::50/64
```

Figura 11 Configuración de las direcciones IP en PC2

```
PC2> sh  
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT  
PC2 10.0.213.39/24 10.0.213.7 00:50:79:66:68:01 20034 127.0.0.1:20035  
fe80::25e:79ff:fe66:6801/64  
2001:db8:acad:213::50/64  
PC2>
```

Fuente: Propia

PC3

```
#ip 10.0.108.39/24 10.0.108.3  
#ip 2001:DB8:ACAD:108::50/64
```

Figura 12 Configuración de las direcciones IP en PC3

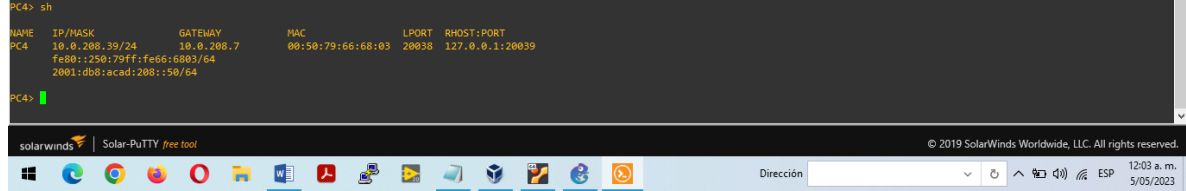
```
PC3> sh  
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT  
PC3 10.0.108.39/24 10.0.108.3 00:50:79:66:68:02 20036 127.0.0.1:20037  
fe80::25e:79ff:fe66:6802/64  
2001:db8:acad:108::50/64  
PC3>
```

Fuente: Propia

PC4

```
#ip 10.0.208.39/24 10.0.208.7  
#ip 2001:DB8:ACAD:208::50/64
```

Figura 13 Configuración de las direcciones IP en PC4



Fuente: Propia

1.3 PARTE 3: CONFIGURACIÓN VRF Y EL ENRUTAMIENTO ESTÁTICO

En esta parte se configura VRF-Lite (Virtual Routing and Forwarding) para realizar la segmentación del tráfico cuando tenemos diferentes clientes o cuando necesitamos que el tráfico de management quede aislado del resto, esta configuración se realiza en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro, para ello se aplican los pasos y comandos que se aprecian a continuación.

Router R1

Tabla 8 Configuración VRF-Lite del Router R1

Comando	Descripción
configure terminal	#Cambia a modo Configuración
vrf definition special-users	#Crea instancia de enrutamiento
description special-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description special-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6
exit	#Sale del modo de configuración
vrf definition general-users	#Crea instancia de enrutamiento
description general-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description general-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6

Fuente: Propia

Router R2

Tabla 9 Configuración VRF-Lite del Router R2

Comando	Descripción
configure terminal	#Cambia a modo Configuración

vrf definition special-users	#Crea instancia de enrutamiento
description special-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description special-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6
exit	#Sale del modo de configuración
vrf definition general-users	#Crea instancia de enrutamiento
description general-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description general-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6

Fuente: Propia

Router R3

Tabla 10 Configuración VRF-Lite del Router R3

Comando	Descripción
configure terminal	#Cambia a modo Configuración
vrf definition special-users	#Crea instancia de enrutamiento
description special-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description special-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6
exit	#Sale del modo de configuración
vrf definition general-users	#Crea instancia de enrutamiento
description general-users	#Describe la vrf
address-family ipv4	#Modo configuración familia ipv4
exit	#Sale del modo de configuración
description general-users	#Describe la vrf
address-family ipv6	#Modo configuración familia ipv6

Fuente: Propia

En R1, R2 y R3, se configuran las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento para así seguir las siguientes tablas.

Router R1

Tabla 11 Configuración de las rutas estáticas del Router R1

Comando	Descripción
configure terminal	#Cambia a modo Configuración

interface e1/0.1	#Ingresa a la interface Ethernet 1/0.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.12.3 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:1 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0.2	#Ingresa a la interface Ethernet 1/0.2
encapsulation dot1q 8	#Se establece el tipo de encapsulación
vrf forward general-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.12.3 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:2 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0	#Ingresa a la interface Ethernet 1/0
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.1	#Ingresa a la interface Ethernet 1/1.1
encapsulation dot1q 13	#Se establece el tipo de encapsulación
vrf forward special-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.113.3 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:3 link-local	#Configura link-local
ipv6 address 2001:db8:acad:113::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.2	#Ingresa a la interface Ethernet 1/1.2
encapsulation dot1q 8	#Establece el tipo de encapsulación
vrf forward general-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.108.3 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::1:4 link-local	#Configura link-local
ipv6 address 2001:db8:acad:108::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1	#Ingresa a la interface Ethernet 1/1
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz

exit	#Sale del modo de configuración
------	---------------------------------

Fuente: Propia

Router R2

Tabla 12 Configuración de las rutas estáticas del Router R2

Comando	Descripción
configure terminal	#Cambia a modo Configuración
interface e1/0.1	#Ingresa a la interface Ethernet 1/1.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.12.9 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:1 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0.2	#Ingresa a la interface Ethernet 1/1.2
encapsulation dot1q 8	#Se establece el tipo de encapsulación
vrf forward general-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.12.9 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:2 link-local	#Configura link-local
ipv6 address 2001:db8:acad:12::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0	#Ingresa a la interface Ethernet 1/1
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.1	#Ingresa a la interface Ethernet 1/2.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.23.9 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:3 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.2	#Ingresa a la interface Ethernet 1/2.2
encapsulation dot1q 8	#Establece el tipo de encapsulación
vrf forward general-users	#Asocia interface a tabla de enrutamiento

ip address 10.0.23.9 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::2:4 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::2/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1	#Ingresa a la interface Ethernet 1/2
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Fuente: Propia

Router R3

Tabla 13 Configuración de las rutas estáticas del Router R3

Comando	Descripción
configure terminal	#Cambia a modo Configuración
interface e1/0.1	#Ingresa a la interface Ethernet 1/2.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.23.7 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::3:1 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::3/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0.2	#Ingresa a la interface Ethernet 1/2.2
encapsulation dot1q 8	#Se establece el tipo de encapsulación
vrf forward general-users	#Asocia la interface a la tabla de enrutamiento
ip address 10.0.23.7 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::3:2 link-local	#Configura link-local
ipv6 address 2001:db8:acad:23::3/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/0	#Ingresa a la interface Ethernet 1/2
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.1	#Ingresa a interface Ethernet 1/0.1
encapsulation dot1q 13	#Establece el tipo de encapsulación
vrf forward special-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.213.7 255.255.255.0	#Asigna dirección IPv4

ipv6 address fe80::3:3 link-local	#Configura link-local
ipv6 address 2001:db8:acad:213::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1.2	#Ingresa a la interface Ethernet 1/0.2
encapsulation dot1q 8	#Establece el tipo de encapsulación
vrf forward general-users	#Asocia interface a tabla de enrutamiento
ip address 10.0.208.7 255.255.255.0	#Asigna dirección IPv4
ipv6 address fe80::3:4 link-local	#Configura link-local
ipv6 address 2001:db8:acad:208::1/64	#Configura IPv6
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e1/1	#Ingresa a la interface Ethernet 1/0
no ip address	#No se le asigna dirección IP
no shutdown	#Activa la interfaz

Fuente: Propia

La configuración de rutas estáticas VRF para IPv4 e IPv6 en ambos VRF, por medio de los siguientes comandos:

Router R1

Tabla 14 Configuración de las rutas estáticas del Router R1

Comando	Descripción
configure terminal	#Cambia a modo Configuración
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.9	#Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.9	#Ruta estática predeterminada IPv4 para VRF General-Users.
ipv6 route vrf special-users ::/0 2001:db8:acad:12::2	#Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf general-users ::/0 2001:db8:acad:12::2	#Ruta estática predeterminada IPv6 para VRF General-Users.

Fuente: Propia

Router R2

Tabla 15 Configuración de las rutas estáticas del Router R2

Comando	Descripción
configure terminal	#Cambia a modo Configuración
ip route vrf special-users 10.0.113.0 255.255.255.0 10.0.12.3	#Ruta estática predeterminada IPv4 para VRF Special-Users.

ip route vrf special-users 10.0.213.0 255.255.255.0 10.0.23.7	#Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf general-users 10.0.108.0 255.255.255.0 10.0.12.3	#Ruta estática predeterminada IPv4 para VRF General-Users.
ip route vrf general-users 10.0.208.0 255.255.255.0 10.0.23.7	#Ruta estática predeterminada IPv4 para VRF General-Users.
ipv6 route vrf special-users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1	#Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf special-users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3	#Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf general-users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1	#Ruta estática predeterminada IPv6 para VRF General-Users.
ipv6 route vrf general-users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3	#Ruta estática predeterminada IPv6 para VRF General-Users.

Fuente: Propia

Router R3

Tabla 16 Configuración de las rutas estáticas del Router R3

Comando	Descripción
configure terminal	#Cambia a modo Configuración
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.23.9	#Ruta estática predeterminada IPv4 para VRF Special-Users.
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.23.9	#Ruta estática predeterminada IPv4 para VRF General-Users.
ipv6 route vrf special-users ::/0 2001:db8:acad:23::2	#Ruta estática predeterminada IPv6 para VRF Special-Users.
ipv6 route vrf general-users ::/0 2001:db8:acad:23::2	#Ruta estática predeterminada IPv6 para VRF General-Users.

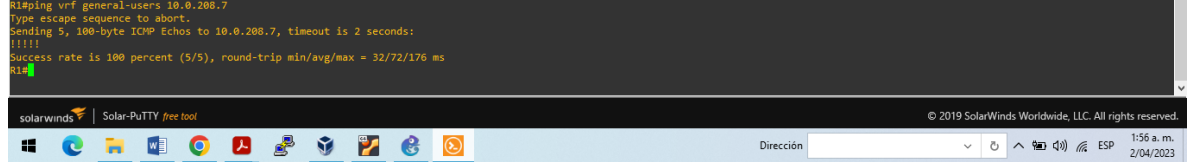
Fuente: Propia

Ahora bien, por medio del comando ping podemos probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red, en esta parte de la configuración primero verificamos la conexión desde el Router R1 al R3, como se evalúa a continuación:

```
#ping vrf general-users 10.0.208.7
```

Figura 14 Ping vrf general-users 10.0.208.7

```
R1#ping vrf general-users 10.0.208.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.7, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/72/176 ms
R1#
```

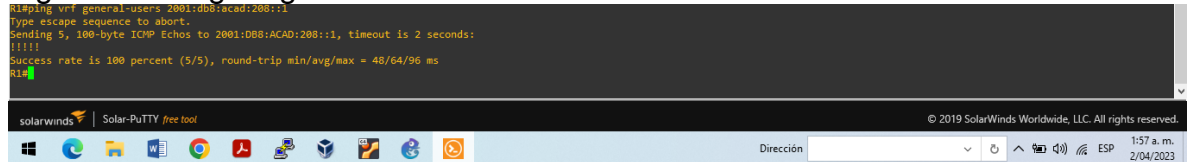


Fuente: Propia

#ping vrf general-users 2001:db8:acad:208::1

Figura 15 Ping vrf general-users 2001:db8:acad:208::1

```
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 = 48/64/96 ms
R1#
```

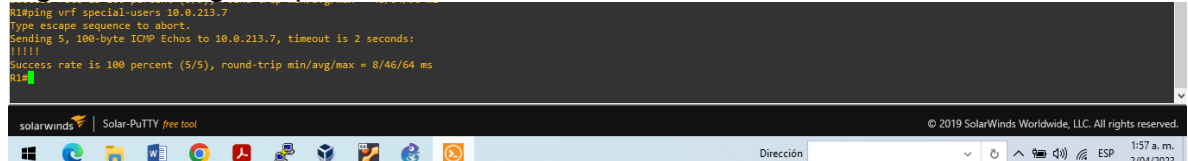


Fuente: Propia

#ping vrf special-users 10.0.213.7

Figura 16 Ping vrf special-users 10.0.213.7

```
R1#ping vrf special-users 10.0.213.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.7, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/46/64 ms
R1#
```

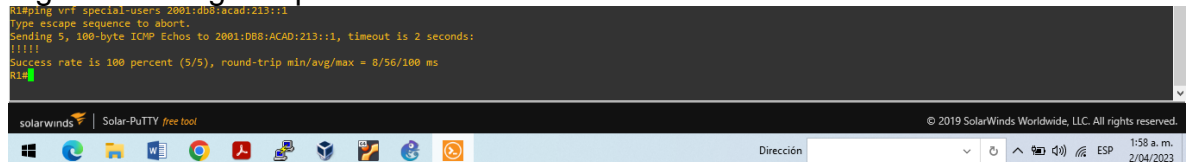


Fuente: Propia

#ping vrf special-users 2001:db8:acad:213::1

Figura 17 Ping vrf special-users 2001:db8:acad:213::1

```
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 = 8/56/100 ms
R1#
```

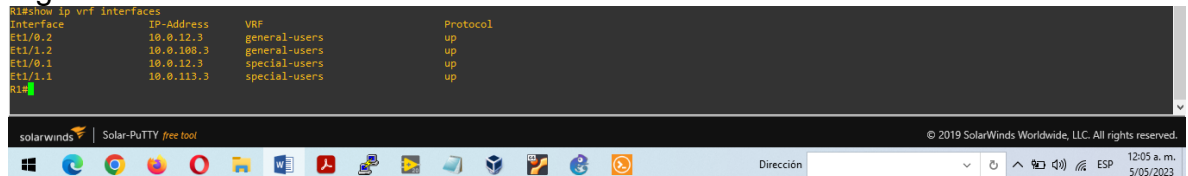


Fuente: Propia

Verificación de las configuraciones VRF

Figura 18 Verificación de VRF en R1

```
R1#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0/2        10.0.12.3       general-users    up
Et1/1/2        10.0.100.3      general-users    up
Et1/0/1        10.0.12.3       special-users    up
Et1/1/1        10.0.113.3      special-users    up
R1#
```



Fuente: Propia

Figura 19 Verificación de VRF en R2

```
R2#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.9       general-users    up
Et1/1.2        10.0.23.9       general-users    up
Et1/0.1        10.0.12.9       special-users    up
Et1/1.1        10.0.23.9       special-users    up
R2#
```

Fuente: Propia

Figura 20 Verificación de VRF en R3

```
R3#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.23.7       general-users    up
Et1/1.2        10.0.200.7      general-users    up
Et1/0.1        10.0.23.7       special-users    up
Et1/1.1        10.0.213.7      special-users    up
R3#
```

Fuente: Propia

Verificación de las configuraciones de las rutas estáticas en los routers
#show run | inc route

Figura 21 Verificación de las rutas estáticas en R1

```
R1#show run | inc route
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.9
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.9
ipv6 route vrf special-users ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf general-users ::/0 2001:DB8:ACAD:12::2
R1#
```

Fuente: Propia

Figura 22 Verificación de las rutas estáticas en R2

```
R2#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.9       general-users    up
Et1/1.2        10.0.23.9       general-users    up
Et1/0.1        10.0.12.9       special-users    up
Et1/1.1        10.0.23.9       special-users    up
R2#show run | inc route
ip route vrf general-users 10.0.108.0 255.255.255.0 10.0.12.3
ip route vrf general-users 10.0.200.0 255.255.255.0 10.0.23.7
ip route vrf special-users 10.0.113.0 255.255.255.0 10.0.12.3
ip route vrf special-users 10.0.213.0 255.255.255.0 10.0.23.7
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:200::/64 2001:DB8:ACAD:23::3
ipv6 route vrf special-users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3
R2#
```

Fuente: Propia

Figura 23 Verificación de las rutas estáticas en R3

```
R3#show run | inc route
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.23.9
ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.23.9
ipv6 route vrf special-users ::/0 2001:DB8:ACAD:23::2
ipv6 route vrf general-users ::/0 2001:DB8:ACAD:23::2
R3#
```

Fuente: Propia

1.4 PARTE 4: CONFIGURACIÓN CAPA 2

En esta parte se configuran los switches para soportar conectividad con los dispositivos que conforman la red. Por lo tanto, para iniciar con esta parte de la configuración de la red, primero se deshabilitan los puertos de los switches D1, D2 y A1.

Tabla 17 Apagado de las interfaces de los switches

Comando	Descripción
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	/#Rango de todas las interfaces que contienen los switch
shutdown	#Deshabilita todas las interfaces
exit	#Sale del modo de configuración

Fuente: Propia

En D1 y D2, se configuran los enlaces troncales a R1 y R3. Teniendo en cuenta que los enlaces troncales es un enlace de capa 2 del modelo OSI entre dos switches que transportan el tráfico para todas las VLAN. Asimismo en esta parte se configura y habilita el enlace e0/3 como enlace troncal.

Switch D1

Tabla 18 Configuración de los enlaces troncales en D1

Comando	Descripción
interface e0/2	#Ingresa a la interface de Ethernet 0/0
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
no shutdown	#Apaga la interfaz
exit	#Sale del modo de configuración

Fuente: Propia

Switch D2

Tabla 19 Configuración de los enlaces troncales en D2

Comando	Descripción
interface e0/3	#Ingresa a la interface de Ethernet 0/0
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
no shutdown	#Apaga la interfaz
exit	#Sale del modo de configuración

Fuente: Propia

En D1 y A1, se configura el EtherChannel con PAgP, por medio de los comandos que se muestran en las siguientes tablas:

Switch D1

Tabla 20 Configuración Etherchannel en D1

Comando	Descripción
interface e0/0	#Ingresa a la interface de Ethernet 0/1
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e0/1	#Ingresa a la interface de Ethernet 0/1
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Fuente: Propia

Switch A1

Tabla 21 Configuración Etherchannel en A1

Comando	Descripción
interface e0/0	#Ingresa a la interface de Ethernet 0/1
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e0/1	#Ingresa a la interface de Ethernet 0/1
switchport trunk encapsulation dot1q	#Enlace troncal estándar IEEE 802.1Q
switchport mode trunk	#Modo de enlace troncal permanente
channel-group 1 mode desirable	#Establece el puerto en modo activo
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Fuente: Propia

En D1, D2 y A1 Configuran los puertos de acceso para PC1, PC2, PC3 y PC4 en D1, D2 y A1. Teniendo en cuenta que para llevar esto a cabo, se configura y habilitan los puertos de acceso de modo que en D1, la interfaz E0/3 tenga acceso a la VLAN 13, la interfaz E0/2 de D2 tenga acceso a la VLAN 8 y la interfaz E0/1 a la VLAN 13

y en A1 la interfaz E0/2 a la VLAN 8. por medio de los comandos que se muestran en las siguientes tablas:

Switch D1

Tabla 22 Configuración del acceso en D1

Comando	Descripción
interface e0/3	#Ingresa a la interface de Ethernet 0/3
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 13	#Asigna al puerto la VLAN 13
spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Fuente: Propia

Switch D2

Tabla 23 Configuración del acceso en D2

Comando	Descripción
interface e0/2	#Ingresa a la interface de Ethernet 0/2
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 13	#Asigna al puerto la VLAN 13
spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración
interface e0/1	#Ingresa a la interface de Ethernet 0/1
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 8	#Asigna al puerto la VLAN 8
spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz
exit	#Sale del modo de configuración

Fuente: Propia

Switch A1

Tabla 24 Configuración del acceso en A1

Comando	Descripción
interface e0/2	#Ingresa a la interface de Ethernet 0/2
switchport mode access	#Establece el puerto en modo de acceso
switchport access vlan 8	#Asigna al puerto la VLAN 8

spanning-tree portfast	#Habilita Portfast
no shutdown	#Activa la interfaz

Fuente: Propia

Ahora bien, por medio del comando ping podemos probar la conectividad

```
#ping 10.0.213.39
#ping 2001:db8:acad:213::50/64
```

Figura 24 Verificación de conexión de PC1 a PC2

```
PC1> ping 10.0.213.39
10.0.213.39 icmp_seq=1 timeout
10.0.213.39 icmp_seq=2 timeout
10.0.213.39 icmp_seq=3 timeout
10.0.213.39 icmp_seq=4 timeout
10.0.213.39 icmp_seq=5 timeout

PC1> ping 10.0.213.39
64 bytes from 10.0.213.39 icmp_seq=1 ttl=61 time=277.755 ms
64 bytes from 10.0.213.39 icmp_seq=2 ttl=61 time=95.824 ms
64 bytes from 10.0.213.39 icmp_seq=3 ttl=61 time=50.281 ms
64 bytes from 10.0.213.39 icmp_seq=4 ttl=61 time=70.306 ms
64 bytes from 10.0.213.39 icmp_seq=5 ttl=61 time=288.404 ms

PC1> ping 2001:db8:acad:213::50/64
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=351.838 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=132.605 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=81.163 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=72.864 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=67.896 ms

PC1>
```

Fuente: Propia

```
#ping 10.0.113.39
#ping 2001:db8:acad:113::50/64
```

Figura 25 Verificación de conexión de PC2 a PC1

```
PC2 10.0.213.39/24 10.0.213.7 00:50:79:66:68:01 20034 127.0.0.1:20035
fe80::250:79ff:fe66:6801/64
2001:db8:acad:213::50/64

PC2> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.213.39/24 10.0.213.7 00:50:79:66:68:01 20034 127.0.0.1:20035
fe80::250:79ff:fe66:6801/64
2001:db8:acad:213::50/64

PC2> ping 10.0.113.39
64 bytes from 10.0.113.39 icmp_seq=1 ttl=61 time=182.465 ms
64 bytes from 10.0.113.39 icmp_seq=2 ttl=61 time=83.182 ms
64 bytes from 10.0.113.39 icmp_seq=3 ttl=61 time=189.291 ms
64 bytes from 10.0.113.39 icmp_seq=4 ttl=61 time=73.679 ms
64 bytes from 10.0.113.39 icmp_seq=5 ttl=61 time=67.719 ms

PC2> ping 2001:db8:acad:113::50/64
2001:db8:acad:113::50 icmp6_seq=1 ttl=58 time=94.470 ms
2001:db8:acad:113::50 icmp6_seq=2 ttl=58 time=78.609 ms
2001:db8:acad:113::50 icmp6_seq=3 ttl=58 time=73.936 ms
2001:db8:acad:113::50 icmp6_seq=4 ttl=58 time=60.852 ms
2001:db8:acad:113::50 icmp6_seq=5 ttl=58 time=100.262 ms

PC2>
```

Fuente: Propia

```
#ping 10.0.208.39
#ping 2001:db8:acad:208::50/64
```

Figura 26 Verificación de conexión de PC3 a PC4

```
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.108.39/24 10.0.108.3 00:50:79:66:68:02 20036 127.0.0.1:20037
fe80::250:79ff:fe66:6802/64
2001::db8:acad:108::50/64

PC3> ping 10.0.208.39

84 bytes from 10.0.208.39 icmp_seq=1 ttl=61 time=145.509 ms
84 bytes from 10.0.208.39 icmp_seq=2 ttl=61 time=102.027 ms
84 bytes from 10.0.208.39 icmp_seq=3 ttl=61 time=122.030 ms
84 bytes from 10.0.208.39 icmp_seq=4 ttl=61 time=151.633 ms
84 bytes from 10.0.208.39 icmp_seq=5 ttl=61 time=126.756 ms

PC3> ping 2001::db8:acad:208::50/64

2001::db8:acad:208::50 icmp6_seq=1 ttl=58 time=175.885 ms
2001::db8:acad:208::50 icmp6_seq=2 ttl=58 time=84.813 ms
2001::db8:acad:208::50 icmp6_seq=3 ttl=58 time=112.555 ms
2001::db8:acad:208::50 icmp6_seq=4 ttl=58 time=129.159 ms
2001::db8:acad:208::50 icmp6_seq=5 ttl=58 time=73.763 ms

PC3> █
```

Fuente: Propia

```
#ping 10.0.108.39
#ping 2001::db8:acad:108::50/64
```

Figura 27 Verificación de conexión de PC4 a PC3

```
fe80::250:79ff:fe66:6803/64
2001::db8:acad:208::50/64

PC4> ping 10.0.108.39

84 bytes from 10.0.108.39 icmp_seq=1 ttl=61 time=164.834 ms
84 bytes from 10.0.108.39 icmp_seq=2 ttl=61 time=67.422 ms
84 bytes from 10.0.108.39 icmp_seq=3 ttl=61 time=101.767 ms
84 bytes from 10.0.108.39 icmp_seq=4 ttl=61 time=289.506 ms
84 bytes from 10.0.108.39 icmp_seq=5 ttl=61 time=232.432 ms

PC4> ping 2001::db8:acad:108::50/64

2001::db8:acad:108::50 icmp6_seq=1 ttl=58 time=142.068 ms
2001::db8:acad:108::50 icmp6_seq=2 ttl=58 time=178.851 ms
2001::db8:acad:108::50 icmp6_seq=3 ttl=58 time=93.902 ms
2001::db8:acad:108::50 icmp6_seq=4 ttl=58 time=56.778 ms
2001::db8:acad:108::50 icmp6_seq=5 ttl=58 time=95.381 ms

PC4> █
```

Fuente: Propia

Verificación de las configuraciones de los enlaces troncales
#show interfaces trunk

Figura 28 Verificación troncal en D1

```
May 5 05:31:44.889: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/2 (not f
ull duplex), with R1 Ethernet1/2 (full duplex).
D1#
D1#
D1#show interfaces trunk

Port      Mode         Encapsulation  Status        Native vlan
Et0/2    on           802.1q         trunking     1
Po1      on           802.1q         trunking     1

Port      Vlans allowed on trunk
Et0/2    1-4094
Po1      1-4094

Port      Vlans allowed and active in management domain
Et0/2    1,8,13
Po1      1,8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/2    1,8,13
Po1      1,8,13
D1# █
```

Fuente: Propia

Figura 29 Verificación troncal en D2

```
May 5 05:32:35:007: KCDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet3/3 (not full duplex), with R3 Ethernet1/1 (full duplex).
D2#show interfaces trunk

Port      Mode          Encapsulation  Status        Native vlan
Et0/3    on            802.1q         trunking     1

Port      Vlans allowed on trunk
Et0/3    1-4094

Port      Vlans allowed and active in management domain
Et0/3    1,8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/3    1,8,13
D2#
```

Fuente: Propia

Verificación de los puertos EthernetChannel
#show etherchannel summary

Figura 30 Verificación de los puertos etherchannel 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        Et0/0(P)  Et0/1(P)
D1#
```

Fuente: Propia

Figura 31 Verificación de los puertos etherchannel en 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        Et0/0(P)  Et0/1(P)
A1#
```

Fuente: Propia

Verificación de las interfaces configuradas según cada switch
#show run interface e0/3

Figura 32 Verificación de la interfaz e0/3 en D1

```
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

```
#show run interface e0/2
#show run interface e0/1
```

Figura 33 Verificación de la interfaz e0/1 y e0/2 en 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#show run interface e0/1
Building configuration...

Current configuration : 108 bytes
!
interface Ethernet0/1
 switchport access vlan 8
 switchport mode access
 spanning-tree portfast edge
end
D2#
```

Fuente: Propia

```
#show run interface e0/2
```

Figura 34 Verificación de la interfaz e0/2 en A1

```
A1#show run interface e0/2
Building configuration...

Current configuration : 108 bytes
!
interface Ethernet0/2
 switchport access vlan 8
 switchport mode access
 spanning-tree portfast edge
end
A1#
```

Fuente: Propia

1.5 PARTE 5: CONFIGURACIÓN DE SEGURIDAD

En esta parte, la configuración consiste en utilizar la arquitectura AAA que representa las siglas Authentication (Autenticación), Authorization (Autorización) y Accounting (Registro), esta arquitectura de seguridad aprueba la gestión de acceso al definir políticas de seguridad. En todos los dispositivos se configura y habilita el

modo EXEC privilegiado seguro, para ello se aplican los comandos que se aprecian a continuación:

Router R1

Tabla 25 Configuración de seguridad en R1

Comando	Descripción
enable secret cesar097	#Habilita la contraseña cesar097
username admin privilege 15 secret cesar097	#Configuración del nombre de usuario, nivel de privilegio 15 y contraseña secreta encriptada cesar097
aaa new-model	#Habilita el uso de listas para los métodos de autenticación.
aaa authentication login default local	#Activación predeterminada de inicio de sesión de autenticación AAA.

Fuente: Propia

Router R2

Tabla 26 Configuración de seguridad en R2

Comando	Descripción
enable secret cesar097	//Habilita la contraseña cesar097
username admin privilege 15 secret cesar097	//Configuración del nombre de usuario, nivel de privilegio 15 y contraseña secreta encriptada cesar097
aaa new-model	//Habilita el uso de listas para los métodos de autenticación.
aaa authentication login default local	//Activación predeterminada de inicio de sesión de autenticación AAA.

Fuente: Propia

Router R3

Tabla 27 Configuración de seguridad en R3

Comando	Descripción
enable secret cesar097	#Habilita la contraseña cesar097
username admin privilege 15 secret cesar097	#Configuración del nombre de usuario, nivel de privilegio 15 y contraseña secreta encriptada cesar097
aaa new-model	#Habilita el uso de listas para los métodos de autenticación.
aaa authentication login default local	#Activación predeterminada de inicio de sesión de autenticación AAA.

Fuente: Propia

Switch D1

Tabla 28 Configuración de seguridad en D1

Comando	Descripción
enable algorithm-type scrypt secret cesar097	#Habilita la contraseña cesar097
username admin privilege 15 algorithm-type scrypt secret cesar097	#Configuración del nombre de usuario, nivel de privilegio 15 y contraseña secreta encriptada cesar097
aaa new-model	#Habilita el uso de listas para los métodos de autenticación.
aaa authentication login default local	#Activación predeterminada de inicio de sesión de autenticación AAA.

Fuente: Propia

Switch D2

Tabla 29 Configuración de seguridad en D2

Comando	Descripción
enable algorithm-type scrypt secret cesar097	#Habilita la contraseña cesar097
username admin privilege 15 algorithm-type scrypt secret cesar097	#Configuración del nombre de usuario, nivel de privilegio 15 y contraseña secreta encriptada cesar097
aaa new-model	#Habilita el uso de listas para los métodos de autenticación.
aaa authentication login default local	#Activación predeterminada de inicio de sesión de autenticación AAA.

Fuente: Propia

Switch A1

Tabla 30 Configuración de seguridad en A1

Comando	Descripción
enable algorithm-type scrypt secret cesar097	#Habilita la contraseña cesar097
username admin privilege 15 algorithm-type scrypt secret cesar097	#Configuración del nombre de usuario, nivel de privilegio 15 y contraseña secreta encriptada cesar097
aaa new-model	#Habilita el uso de listas para los métodos de autenticación.
aaa authentication login default local	#Activación predeterminada de inicio de sesión de autenticación AAA.

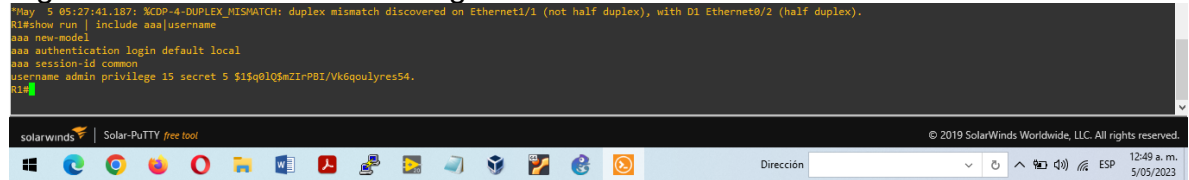
Fuente: Propia

Verificación del nombre de usuario y la autenticación AAA.

#show run | include aaa|username

Figura 35 Verificación de la seguridad en R1

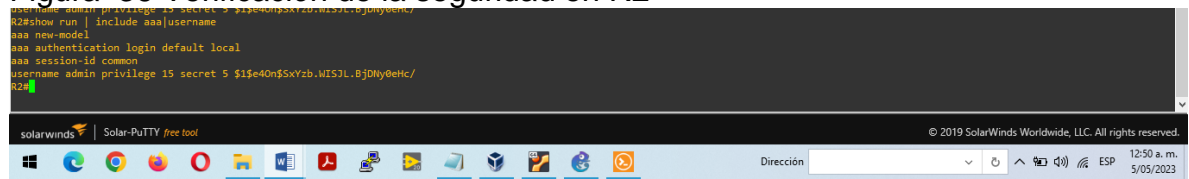
```
May 5 05:27:41.187: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with D1 Ethernet0/2 (half duplex).
R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$q0lQmZrP8l/Vk6qulyres54.
R1#
```



Fuente: Propia

Figura 36 Verificación de la seguridad en R2

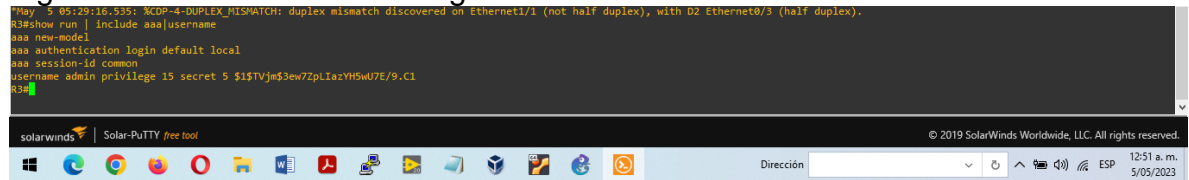
```
May 5 05:29:16.535: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with R2 Ethernet0/3 (half duplex).
R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1e40n$5xYzb.WIS3L.Bj0Ny0eHc/
R2#
```



Fuente: Propia

Figura 37 Verificación de la seguridad en R3

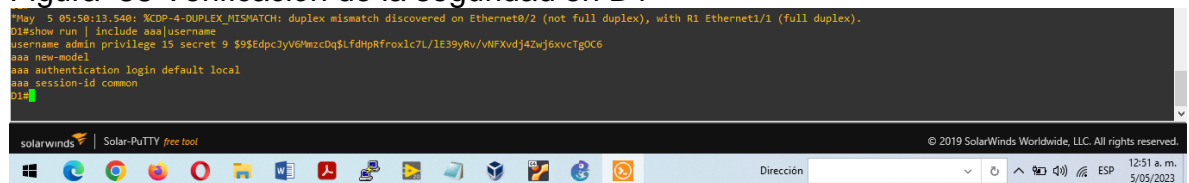
```
May 5 05:29:16.535: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with D2 Ethernet0/3 (half duplex).
R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$TVjm$3ew7ZpLTazYH5wU7E/9.C1
R3#
```



Fuente: Propia

Figura 38 Verificación de la seguridad en D1

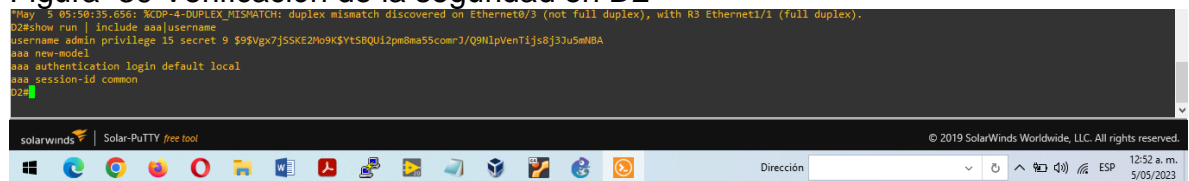
```
May 5 05:50:13.540: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/2 (not full duplex), with R1 Ethernet1/1 (full duplex).
D1#show run | include aaa|username
username admin privilege 15 secret 9 $9$Edpc3yV0mzcdq$LfDhRfRoxlc7L/1E39yRv/vNFxvdj4Zuj6xvctG0C6
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
```



Fuente: Propia

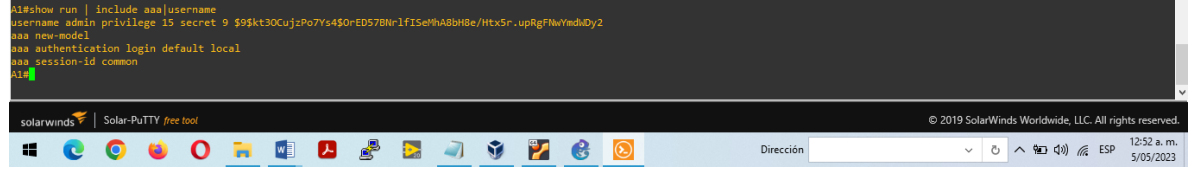
Figura 39 Verificación de la seguridad en D2

```
May 5 05:50:13.540: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/3 (not full duplex), with R3 Ethernet1/1 (full duplex).
D2#show run | include aaa|username
username admin privilege 15 secret 9 $9$Vgx7j$5KE2M9K$Yt$BQU12pm8ma55com7j/Q9N1pvent1js8j3JusmNBA
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```



Fuente: Propia

Figura 40 Verificación de la seguridad en A1



Fuente: Propia

CONCLUSIONES

El escenario desarrollado permite el desarrollo y mejora del manejo de habilidades a la hora de solucionar los requerimientos de una red; además de comprender cuál es la mejor implementación de los comandos necesarios para la configuración de cada dispositivo con el fin de lograr el correcto funcionamiento de la red. Por esta razón, se logró garantizar fácilmente la independencia de los usuarios especiales y los usuarios generales que conforman la red aplicando la configuración VRF, una configuración nueva que parecía un reto pero que logro ser de la que más beneficios se obtuvo, pues reduce la necesidad de implementar muchos dispositivos en una red; ya que los dos grupos pueden estar configurados en el mismo router y aun así tener completa independencia.

Asimismo, después del establecimiento de contraseñas, nombres y el mensaje de advertencia, se observa que esto apoya mucho a las siguientes configuraciones que se realizan en los dispositivos; sobre todo en la parte de implementar la seguridad por medio de la arquitectura AAA que permite la gestión de acceso definiendo políticas de un acceso y comunicación segura en la red.

Además se puede concluir que la implementación de las rutas estáticas en la red trabajada permite proporcionar seguridad a la hora de realizar la transmisión entre los enrutadores los cuales comparten diferentes redes lógicas. Observando que con esto si se puede garantizar un bajo consumo de ancho de banda de la red.

Al final, es importante realizar las evaluaciones correspondientes, utilizar las configuraciones necesarias ya conocidas y mencionados con anterioridad en cada dispositivo y guardar las mismas; de esta manera, se concluye que la red obtenida es funcional y segura; por ende, se sugiere apropiar más los conocimientos del uso de tecnología para estimular el funcionamiento, configuración y diseño ya que todavía queda mucho por aprender de las redes LAN/WAN.

REFERENCIAS

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

UNAD (2020). Configuración de Switches y Routers [OVA]. <https://1drv.ms/u/s!AmIJYei-NT1lhqL9QChD1m9EuGqC>

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

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

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

EDGEWORTH, Bradley, et al. IP Routing Essentials. CCNP and CCIE Enterprise Core ENCORA 350-401. ciscopress. [en línea], 2020. Disponible en <https://1drv.ms/b/s!AAIGg5JUgUBthk8>