

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JULIAN ALFONSO RODRIGUEZ PAREDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JULIAN ALFONSO RODRIGUEZ PAREDES

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

Director
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C
2023

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C, 02 de mayo de 2023

AGRADECIMIENTOS

Quiero expresar mis sentimientos de gratitud sincera a todas las personas que han sido un apoyo para lograr la meta de culminar mis estudios y obtener el honorable título de Ingeniero Electrónico. Agradezco en primer lugar a Dios todo Poderoso por darme esta oportunidad, a mi Madre Rosalba que desde el cielo se alegra con mis logros, a mi Padre Alfonso y hermanita Eliana quienes han sido en muchas ocasiones mis patrocinadores y animadores durante esta carrera profesional. Sin duda a mi esposa Luisa Fernanda, a mis hijos Isabella y Juan José que han sido mi motivación para no desfallecer y continuar adelante a pesar de la fatiga y el cansancio, han sido ellos testigos de mis noches de estudio y hasta algunas amanecidas sacrificadas que hoy valen la pena recordar.

Así mismo quiero agradecer a todos los diferentes Directores de cursos y Tutores que me ayudaron y enseñaron demasiado a través de los encuentros sincrónicos y de sus valiosas retroalimentaciones a cada uno de mis trabajos; a la Universidad Nacional Abierta y a Distancia muchísimas gracias por este tipo de educación que me permitió terminar mis estudios profesionales desde la virtualidad y con una excelente plataforma educativa, muy completa y eficiente en todos los aspectos.

CONTENIDO

AGRADECIMIENTOS	4
LISTA DE FIGURAS	6
LISTA DE TABLAS	7
GLOSARIO	8
RESUMEN	9
ABSTRACT	10
INTRODUCCIÓN	11
DESARROLLO DEL ESCENARIO PROPUESTO	12
1.CONSTRUIR LA RED, CONFIGURAR LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES.....	14
1.1 Cablee la red como se muestra en la topología. Conecte los dispositivos como se muestra en el diagrama de topología y cablee según sea necesario.	14
1.2 Configure los ajustes básicos para cada dispositivo.....	14
2. CONFIGURAR VRF Y RUTAS ESTÁTICAS	19
2.1 Configurar en los routers R1, R2 y R3, VRF Lite en los VRFS “General-users y Special-Users” de acuerdo con la topología establecida, permitiendo los protocolos IPv6 e IPv4:	19
2.2 Configurar las interfaces IPv4 y IPv6 en los routers R1, R2 y R3 para cada VRF de acuerdo con lo establecido en la tabla de direccionamiento.	20
2.3. Configurar las rutas estáticas predeterminadas que apuntan a R2, en R1 y R3.....	24
2.4 Verificar el direccionamiento IP de las interfaces VRF implementadas en los Router R1, R2 y R3	25
3. CONFIGURAR CAPA 2	27
3.1 Deshabilitar todas las interfaces en D1, D2, y A1, en D1 y D2, Deshabilitar G1/0/1 to G1/0/24. En A1, Deshabilitar F0/1 – F0/24, G0/1 – G0/2.	27
3.2 En D1 y D2, Configurar los enlaces troncales para R1 and R3. Configurar y habilitar G1/0/11, como enlace troncal.	27
3.3 En D1 y A1, configurar EtherChannel.....	28
3.4 En D1, D2 y A1, configurar los puertos de acceso PC1, PC2, PC3, and PC4.	29
3.5 Verificar conectividad de PC a PC.	31
4. CONFIGURACIÓN DE LA SEGURIDAD	33
4.1 en todos los dispositivos, configurar la seguridad privilegiada en modo EXE.	33
4.2 En todos los dispositivos, crear una cuenta de usuario local.	33
4.3 En todos los dispositivos, habilitar la autenticación AAA.....	33
CONCLUSIONES	36
BIBLIOGRAFIA	37

LISTA DE FIGURAS

Figura 1: Topología propuesta para la actividad.....	12
Figura 2: Topología de la red en GNS3	14
Figura 3: Comprobación con el comando show del PC1	17
Figura 4: Comprobación con el comando show del PC2	17
Figura 5: Comprobación configuración PC3	18
Figura 6: Configuración PC4.....	18
Figura 7: Configuración VRF Lite en R1	19
Figura 8: Configuración VRF Lite en R2	20
Figura 9: Configuración VRF Lite en R3	20
Figura 10: Revisión de la configuración las interfaces IPv4 y IPv6 en R1	21
Figura 11: Revisión de la configuración las interfaces IPv4 y IPv6 en R2	23
Figura 12: Revisión de la configuración las interfaces IPv4 y IPv6 en R3	24
Figura 13: Rutas estáticas en R1.....	25
Figura 14: Rutas estáticas en R2.....	25
Figura 15: Rutas estáticas en R3.....	25
Figura 16: Direccionamiento interfaces VRFS en R1	25
Figura 17: Direccionamiento interfaces VRFS en R2	26
Figura 18: Direccionamiento interfaces VRFS en R3	26
Figura 19: Verificación conectividad de R1 a R3	26
Figura 20: verificación interfaces troncales.....	28
Figura 21: Verificación configuración etherchannel y protocolo PAgP en D1	29
Figura 22: verificación de portfast habilitado para vlan 13 en D1	30
Figura 23: Ping 10.0.213.36.....	31
Figura 24: ping 2001:db8:acad:213::50	31
Figura 25: Ping 10.0.208.36.....	31
Figura 26: Ping 2001:db8:acad:208::50	32
Figura 27: ping desde PC1 a PC3	32
Figura 28: Verificación configuración Usuario, autenticación AAA y encriptación de password en A1	34
Figura 29: Verificación configuración Usuario, autenticación AAA y encriptación de password en D1	34
Figura 30: Verificación configuración Usuario, autenticación AAA y encriptación de password en D2	34
Figura 31: Verificación configuración Usuario, autenticación AAA y encriptación de password en R1	34
Figura 32: Verificación configuración Usuario, autenticación AAA y encriptación de password en R2	35
Figura 33: Verificación configuración Usuario, autenticación AAA y encriptación de password en R3	35

LISTA DE TABLAS

Tabla 1. Enrutamiento y direccionamiento planteado para la actividad.....	12
Tabla 2. Enrutamiento y direccionamiento ajustado a cédula 80165362.....	13

GLOSARIO

ENLACES TRONCALES: Son enlaces de la capa 2 del modelo OSI y consiste en la conexión punto a punto entre dos dispositivos de una red para permitir el transporte del tráfico de datos de varias Vlans.

ENRUTAMIENTO ESTATICO: Consiste en la creación de rutas estáticas para el direccionamiento fijo en redes que se crean con parámetros constantes, lo cual ofrece ventajas como seguridad, facilidad en la solución de problemas y baja sobrecarga de la red informática.

ROUTER: Es un dispositivo intermedio de una red informática que permite el envío y recepción de datos con base en una tabla de enrutamiento y direccionamiento IP.

STP (Spanning Tree Protocol): Es un protocolo que permite generar enlaces redundantes, para garantizar la conectividad de una red LAN al momento de presentarse fallas en sus dispositivos como Switches y Routers.

SWITCH: es un dispositivo que permite la interconexión de dispositivos a una red informática, además de ofrecer muchas características y opciones avanzadas para la optimización de las redes.

VFR (Virtual Routing and Forwarding): traducido al español es una tecnología de enrutamiento virtual y reenvío que ofrece la posibilidad de crear en un router más de una tabla de enrutamiento completamente independientes, característica que hace posible la utilización de direcciones IP iguales asignadas a interfaces diferentes.

VLAN (Virtual LAN): son redes lógicas que se pueden crear dentro de una red física con el fin de ofrecer mayores prestaciones y segmentaciones necesarias en una red permitiendo el tráfico de datos de manera segura entre cada subred virtual.

RESUMEN

El presente documento se fundamenta en la aplicación de conocimientos de enrutamiento y direccionamiento de redes, configuraciones de protocolos y en general diversos aspectos de Networking, puestos de manifiesto en la implementación de una red con una configuración especial multi-VRF en la cual se admiten dos tipos de usuarios "Usuarios generales" y "Usuarios especiales", permitiéndose la comunicación solo entre los dispositivos finales de cada VRF y quedar aislados de los dispositivos de la otra VRF configurada.

Se parte inicialmente de una configuración básica de todos los dispositivos, luego la configuración de VRF-Lite de los dispositivos intermedios, enrutamiento estático y configuración de switches capa 2 para permitir la conectividad de un extremo al otro de la red. Finalmente, se realiza una configuración de seguridad con algoritmos de encriptación y autenticación AAA de usuarios.

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

ABSTRACT

This document is based on the application of knowledge of network routing and addressing, protocol configurations and, in general, various aspects of Networking, revealed in the implementation of a network with a special multi-VRF configuration in which two types of users “General Users” and “Special Users”, which the end devices of each VRF must communicate with each other and remain isolated from the devices of the other configured VRF.

Initially, it starts with a basic configuration of all the devices, then the VRF-Lite configuration of the intermediate devices, static routing and configuration of layer 2 switches to allow connectivity from one end of the network to the other. Finally a security configuration is carried out with encryption algorithms and AAA authentication of users.

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

INTRODUCCIÓN

Las redes y sus diferentes protocolos de enrutamiento permiten una gran variedad de beneficios para las empresas y organizaciones al momento de implementar y gestionar sus datos. Un ejemplo claro es el uso de configuraciones de protocolos de enrutamiento especiales en los dispositivos intermedios como routers y switches como las VRFs (Virtual Routing Forwarding) que permiten generar tablas de enrutamiento adicionales que se pueden ejecutar simultáneamente y permiten características como la utilización de direcciones IP iguales asignadas en un enrutador al mismo tiempo. También es posible desde un mismo hardware la separación del tráfico e intercambio de información y enrutamiento de distintos clientes.

En esta actividad se pretende realizar la configuración multi-VRF en una red que tiene dos tipos de clientes denominados "Usuarios generales" y "Usuarios especiales", configurando Vlan, VRFs y sus respectivas rutas estáticas. Para ello se utilizarán comandos IOS de configuración avanzada que permiten configurar cada dispositivo, ya sean routers y switches con base en una tabla de enrutamiento planteada para esta red compuesta por tres routers, tres switches capa2 y cuatro dispositivos finales.

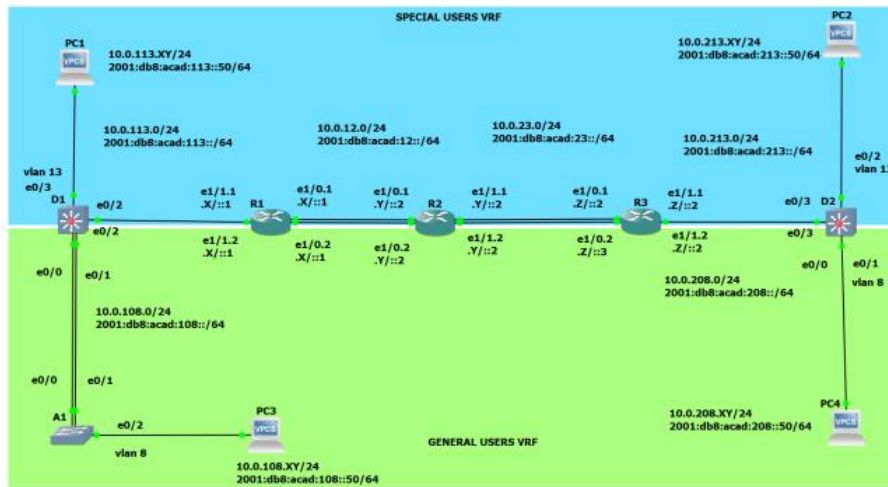
La implementación de la topología de la red se realizará en el software GNS3, en el cual se realizará la configuración y cargue de los routers y switches de la familia Cisco; La red permitirá direccionamiento IPv4 e IPv6 y se configurarán los switches capa 2 habilitando los enlaces troncalizados por Etherchannel bajo protocolo PAgP que permita agregar puertos, con ello se logrará obtener conectividad entre los PCs pertenecientes a cada usuario.

Por último, se realizará la configuración de seguridad en los dispositivos de la red con configuración de encriptación del modo de acceso y protocolo de autenticación AAA.

DESARROLLO DEL ESCENARIO PROPUESTO

Topología de la red propuesta a implementar:

Figura 1: Topología propuesta para la actividad



Fuente 1: Guía de actividades UNAD

La tabla de direccionamiento planteada es la siguiente, la cual se ajustará de acuerdo con la indicación de los últimos tres dígitos de la cédula para las letras X, Y, Z, para mi caso mi cédula es 80.165.362, por lo cual X=3, Y=6, Z=2.

Tabla 1. Enrutamiento y direccionamiento planteado para la actividad.

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.X/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.X/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.X/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.X/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.Y/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.Y/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.Y/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.Y/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.Z/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.Z/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.Z/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.Z/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.XY/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.XY/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.XY/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.XY/24	2001:db8:acad:208::50/64	EUI-64

Fuente 2: Guía de actividades UNAD

Tabla 2. Enrutamiento y direccionamiento ajustado a cédula 80165362.

Device	Interface	IPv4 Address	IPv6 Address	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	10.0.12.6/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.6/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.6/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.6/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.2/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.2/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.36/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.36/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.36/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.36/24	2001:db8:acad:208::50/64	EUI-64

Fuente 3: Diseño propio

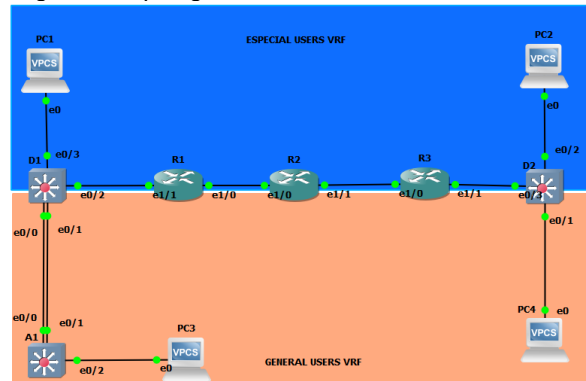
Escenario

En esta evaluación de habilidades, usted es responsable de completar la configuración multi-VRF de la red que admite "Usuarios generales" y "Usuarios especiales". Una vez finalizado, debería haber accesibilidad completa de un extremo a otro y los dos grupos no deberían poder comunicarse entre sí. Asegúrese de verificar que sus configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según lo requerido.

1.CONSTRUIR LA RED, CONFIGURAR LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES

1.1 Cablee la red como se muestra en la topología. Conecte los dispositivos como se muestra en el diagrama de topología y cablee según sea necesario.

Figura 2: Topología de la red en GNS3



Fuente 4: Julian Rodriguez-diseño propio

Para lograr la implementación de esta tipología en GNS3 fue necesario la configuración de dispositivos Cisco en GNS3 cargando las imágenes de los dispositivos routers (Cisco7200) y switches (IOU L2), así mismo se realizó la configuración y cargue de la licencia a través de la aplicación putty.

1.2 Configure los ajustes básicos para cada dispositivo.

Ingresa al modo de configuración global en cada uno de los dispositivos y aplique la configuración básica.

Para la configuración de los dispositivos routers y switches se manejan los mismos comandos los cuales se describen a continuación con una breve descripción de su función dentro de la configuración básica.

Router R1

```
R1#config terminal // Ingreso al modo de configuración global
R1(config)#hostname R1 // asignación de nombre al dispositivo
R1(config)#ipv6 unicast-routing // Habilitación de enrutamiento ipv6
R1(config)#no ip domain lookup // desactivación de búsqueda DNS
R1(config)#banner motd # R1,ENCOR Skills Assessment, Scenario 2 # // mensaje de advertencia
R1(config)#line con 0 // permite que se ejecute una sola consola
R1(config-line)#exec-timeout 0 0 // Evita que el tiempo en consola se agote
R1(config-line)#logging synchronous //envía todos los mensajes de consola hacia abajo sin interrumpir los comandos ingresados para una configuración
R1(config-line)#exit
```

```
R1(config)#exit
R1#copy running-config startup-config // guarda la configuración en memoria MVRAM
```

Router R2

```
R2#config terminal
R2(config)#hostname R2 // asignación de nombre al dispositivo
R2(config)#ipv6 unicast-routing //Habilitación de enrutamiento ipv6
R2(config)#no ip domain lookup //desactivación de búsqueda de nombres de dominio al
ingresar un comando erróneamente
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 2 # // mensaje de
advertencia
R2(config)#line con 0 //permite que se ejecute una sola consola
R2(config-line)#exec-timeout 0 0 // Evita que el tiempo en consola se agote
R2(config-line)#logging synchronous // envía todos los mensajes de consola hacia abajo sin
interrumpir los comandos ingresados para una configuración.
R2(config-line)#exit
R2(config)#exit
R2#copy running-config startup-config // guarda la configuración en memoria MVRAM
```

Router R3

```
R3#config terminal
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario2 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#exit
R3#copy running-config startup-config // guarda la configuración en memoria MVRAM
```

Switch D1

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

```
D1(config-line)#exit
D1(config)#vlan 8 // Creación de la vlan
D1(config-vlan)#name General-Users // Asignación de nombre
D1(config-vlan)#exit
D1(config)#vlan 13 // Creacion de la vlan
D1(config-vlan)#name Special-Users // Asignación de nombre
D1(config-vlan)#exit
D1(config)#exit
D1#copy running-config startup-config
```

Switch D2

```
S1#config terminal
S1(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 2 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 8 // Creación de la vlan
D2(config-vlan)#name General-Users // Asignación de nombre
D2(config-vlan)#exit
D2(config)#vlan 13
D2(config-vlan)#name Special-Users
D2(config-vlan)#exit
D2(config)#exit
D2#copy running-config startup-config
```

Switch A1

```
A1#config terminal
A1(config)#hostname A1
A1(config)#ipv6 unicast-routing
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 2#
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 8 // Creación de la vlan
A1(config-vlan)#name General-Users // Asignación de nombre
```



```
A1(config-vlan)#exit
A1(config)#exit
A1#copy running-config startup-config
```

Guarde las configuraciones en cada uno de los dispositivos.

Se realiza la configuración de cada host final de acuerdo con los datos suministrados en la tabla de enrutamiento, y a través del comando “copy running-config startup-config” se guarda la información de la configuración en la memoria NVRAM.

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

La configuración de los hosts finales de la red se realiza de manera muy sencilla, simplemente ingresando las direcciones IP y al final mediante el comando “save”, se guarda la información ingresada en cada host. Adicionalmente con el comando show se verifica su configuración:

PC1

```
ip 10.0.113.36/24 10.0.113.3 //asignación de IP y mascara de subred
ip 2001:db8:acad:113::50/64 auto //Asignación de ipv6
save // Guardar configuración
```

Figura 3: Comprobación con el comando show del PC1

```
PC1> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.0.113.36/24 10.0.113.3 00:50:79:66:68:00 20032 127.0.0.1:20033
fe80::250:79ff:fe66:6800/64
2001:db8:acad:113::50/64
```

Fuente 5: Diseño propio

PC2

```
ip 10.0.213.36/24 10.0.213.2
ip 2001:db8:acad:213::50/64 auto
save
```

Figura 4: Comprobación con el comando show del PC2

```
PC2> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.213.36/24 10.0.213.2 00:50:79:66:68:01 20034 127.0.0.1:20035
fe80::250:79ff:fe66:6801/64
2001:db8:acad:213::50/64
```

Fuente 6: Diseño propio

PC3

```
ip 10.0.108.36/24 10.0.108.3
ip 2001:db8:acad:108::50/64 auto
save
```

Figura 5: Comprobación configuración PC3

```
PC3> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.108.36/24 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
```

Fuente 7: Diseño propio

PC4
ip 10.0.208.36/24 10.0.208.2
ip 2001:db8:acad:208::50/64 auto
save

Figura 6: Configuración PC4

```
PC4> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.0.208.36/24 10.0.208.2 00:50:79:66:68:03 20038 127.0.0.1:20039
fe80::250:79ff:fe66:6803/64
2001:db8:acad:208::50/64
```

Fuente 8: Diseño propio

2. CONFIGURAR VRF Y RUTAS ESTÁTICAS

En esta parte de la evaluación de habilidades, configurará VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF.

2.1 Configurar en los routers R1, R2 y R3, VRF Lite en los VRFS “General-users y Special-Users” de acuerdo con la topología establecida, permitiendo los protocolos IPv6 e IPv4:

Inicialmente se debe ingresar al modo de configuración global en incluir comandos para la creación de VRF en los routers. La siguiente configuración aplica para los tres routers (R1, R2 y R3):

```
Config terminal // ingresa a modo configuración global
vrf definition General-Users // definir la VRF General-Users
address-family ipv4 // acepta ipv4
address-family ipv6 //acepta ipv4
vrf definition Special-Users // definir la VRF Special-Users
address-family ipv4 // acepta ipv4
address-family ipv6 //acepta ipv4
exit
```

Para comprobar la configuración se ingresa el comando “do show running vrf”, tal como se muestra en la siguiente gráfica, lo cual aplica para los otros routers de la misma manera:

Figura 7: Configuración VRF Lite en R1



```
R1(config)#do show running vrf
Building configuration...

Current configuration : 259 bytes
vrf definition General-Users
|
| address-family ipv4
| exit-address-family
|
| address-family ipv6
| exit-address-family
|
vrf definition Special-Users
|
| address-family ipv4
| exit-address-family
|
| address-family ipv6
| exit-address-family
|
--More--
```

Fuente 9: Diseño propio

Figura 8: Configuración VRF Lite en R2

```
R2(config)#do show running vrf
Building configuration...

Current configuration : 259 bytes
vrf definition General-Users
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
!
vrf definition Special-Users
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
!
--More--
```

Fuente 10: Diseño propio

Figura 9: Configuración VRF Lite en R3

```
R3(config)#do show running vrf
Building configuration...

Current configuration : 259 bytes
vrf definition General-Users
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
!
vrf definition Special-Users
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
!
--More--
```

Fuente 11: Diseño propio

2.2 Configurar las interfaces IPv4 y IPv6 en los routers R1, R2 y R3 para cada VRF de acuerdo con lo establecido en la tabla de direccionamiento.

Se deben realizar las respectivas configuraciones de direccionamiento ip para garantizar la separación de las VRF Especial-Users y General-Users.

Iniciamos con R1, para ello es importante activar en gns3 este router e ingresar a consola para realizar las respectivas configuraciones:

Sub-interface e1/0.1:

interface e1/0.1 // selección de la subinterfaz para ingresar a configurar
encapsulation dot1q 13 // habilitación del protocolo 802.1Q con vlan 13

vrf forwarding Special-Users // se genera la instancia para enrutamiento de VRF

ip address 10.0.12.3 255.255.255.0 // cargue de dirección IP y máscara de subred

ipv6 address fe80::1:1 link-local // cargue de máscara de subred IPv6

ipv6 address 2001:db8:acad:12::1/64 // cargue de dirección IPv6

no shutdown // activación de la subinterfaz

exit

```

Sub-interface e1/0.2:
interface e1/0.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.12.3 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:acad:12::1/64
no shutdown
exit

```

```

Sub-interface e1/1.1:
interface e1/1.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.113.3 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:acad:113::1/64
no shutdown
exit

```

```

Sub-interface e1/1.2:
interface e1/1.2
encapsulation dot1q 8
vrf forwarding General-Users
ip address 10.0.108.3 255.255.255.0
ipv6 address fe80::1:4 link-local
ipv6 address 2001:db8:acad:108::1/64
no shutdown
exit

```

Por último, se comprueba la configuración realizada verificando con los comandos “show ip interface brief” y “show ipv6 interface brief”:

Figura 10: Revisión de la configuración las interfaces IPv4 y IPv6 en R1

```

R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Apr 18 15:37:01.143: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
*Apr 18 15:37:02.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to up
R1(config)#exit
R1#
*Apr 18 15:37:11.839: %SYS-5-COMPIL_I: Configured from console by console
R1#show ip interface brief
Interface              IP-Address      OK? Method Status  Protocol
FastEthernet0/0        unassigned     YES unset  administratively down  down
Ethernet1/0            unassigned     YES unset  up      up
Ethernet1/0.1         10.0.12.3      YES manual  up      up
Ethernet1/0.2         10.0.12.3      YES manual  up      up
Ethernet1/1           unassigned     YES unset  up      up
Ethernet1/1.1         10.0.113.3     YES manual  up      up
Ethernet1/1.2         10.0.108.3     YES manual  up      up
Ethernet1/2           unassigned     YES unset  administratively down  down
Ethernet1/3           unassigned     YES unset  administratively down  down
R1#

```

Fuente 12: Diseño propio

Continuamos con configuración en R2:

Sub-interface e1/0.1:

```
interface e1/0.1 // selección de la subinterface para ingresar a configurar
encapsulation dot1q 13 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding Special-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.12.6 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::2:1 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:12::2/64// cargue de dirección IPv6
no shutdown // activación de la subinterface
exit
```

Sub-interface e1/0.2:

```
interface e1/0.2 // selección de la subinterface para ingresar a configurar
encapsulation dot1q 8 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding General-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.12.6 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::2:2 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:12::2/64// cargue de dirección IPv6
no shutdown // activación de la subinterface
exit
```

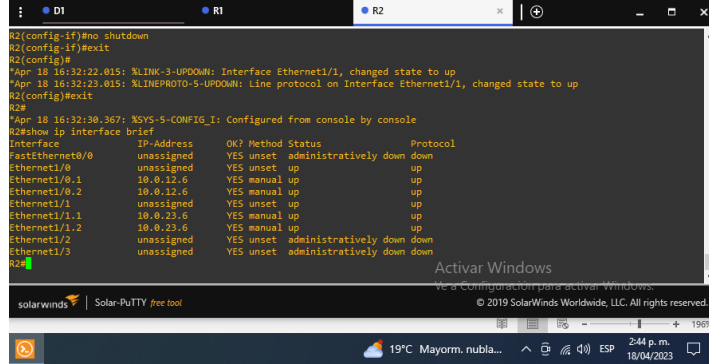
Sub-interface e1/1.1:

```
interface e1/1.1 // selección de la subinterface para ingresar a configurar
encapsulation dot1q 13 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding Special-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.23.6 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::2:3 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:23::2/64// cargue de dirección IPv6
no shutdown // activación de la subinterface
exit
```

Sub-interface e1/1.2:

```
interface e1/1.2 // selección de la subinterface para ingresar a configurar
encapsulation dot1q 8 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding General-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.23.6 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::2:4 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:23::2/64// cargue de dirección IPv6
no shutdown // activación de la subinterface
exit
```

Figura 11: Revisión de la configuración las interfaces IPv4 y IPv6 en R2



```
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Apr 18 16:32:22.015: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
*Apr 18 16:32:23.015: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to up
R2(config)#exit
R2#
*Apr 18 16:32:30.367: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip interface brief
Interface      IP-Address      OK? Method Status  Protocol
FastEthernet0/0 unassigned      YES unset  administratively down down
Ethernet1/0    unassigned      YES unset  up      up
Ethernet1/0.1  10.0.12.6       YES manual  up      up
Ethernet1/0.2  10.0.12.6       YES manual  up      up
Ethernet1/1    unassigned      YES unset  up      up
Ethernet1/1.1  10.0.23.6       YES manual  up      up
Ethernet1/1.2  10.0.23.6       YES manual  up      up
Ethernet1/2    unassigned      YES unset  administratively down down
Ethernet1/3    unassigned      YES unset  administratively down down
R2#
```

Fuente 13: Diseño propio

Continuamos con router R3:

Sub-interface e1/0.1:

```
interface e1/0.1 // selección de la subinterface para ingresar a configurar
encapsulation dot1q 13 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding Special-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.23.2 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::3:1 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:23::3/64// cargue de dirección IPv6
no shutdown // activación de la subinterface
exit
```

Sub-interface e1/0.2:

```
interface e1/0.2 // selección de la subinterface para ingresar a configurar
encapsulation dot1q 8 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding General-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.23.2 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::3:2 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:23::3/64// cargue de dirección IPv6
no shutdown // activación de la subinterface
exit
```

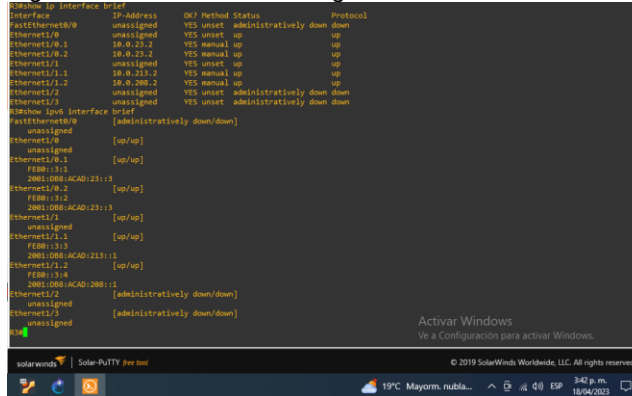
Sub-interface e1/1.1:

```
interface e1/1.1 // selección de la subinterface para ingresar a configurar
encapsulation dot1q 13 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding Special-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.213.2 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::3:3 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:213::1/64// cargue de dirección IPv6
no shutdown // activación de la subinterface
exit
```

Sub-interface e1/1.2:

```
interface e1/1.2 // selección de la subinterfaz para ingresar a configurar
encapsulation dot1q 8 // habilitación del protocolo 802.1Q con vlan 13
vrf forwarding General-Users // se genera la instancia para enrutamiento de VRF
ip address 10.0.208.2 255.255.255.0 // cargue de dirección IP y mascara de subred
ipv6 address fe80::3:4 link-local // cargue de mascara de subred IPv6
ipv6 address 2001:db8:acad:208::1/64// cargue de dirección IPv6
no shutdown // activación de la subinterfaz
exit
```

Figura 12: Revisión de la configuración las interfaces IPv4 y IPv6 en R3



Fuente 14: Diseño propio

2.3. Configurar las rutas estáticas predeterminadas que apuntan a R2, en R1 y R3.

Para R1: Se debe tomar como base en las subinterfaces del router 2 E1/0.1 y E1/0.2

```
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.6
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.6
ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2
ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2
end
```

Para R2: Se deben tomar como base las subinterfaces de R1 E1/0.1 y E1/0.2 y R3 las subinterfaces E1/0.1 y E1/1.2:

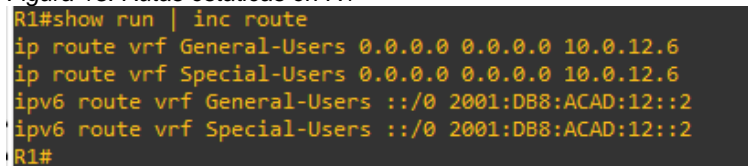
```
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.3
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.3
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.2
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.2
ipv6 route vrf General-Users 2001:db8:acad:108::/64 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
```


Para R3: Se debe tomar como base las subinterfaces de R2 E1/1.1 y E1/1.2

```
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.6
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.6
ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2
ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2
```

Para verificar el direccionamiento estático en cada Router se utiliza el comando `show run | inc route`

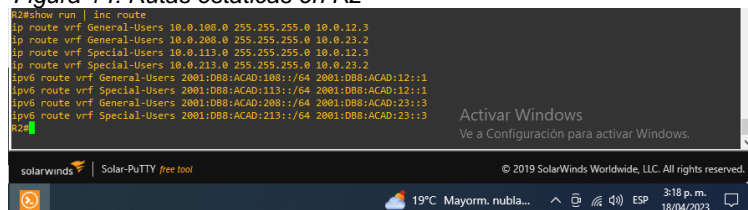
Figura 13: Rutas estáticas en R1



```
R1#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.6
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.6
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:12::2
R1#
```

Fuente 15: Diseño propio

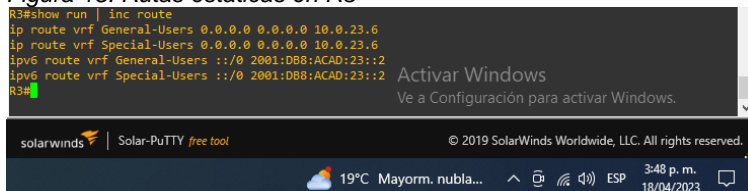
Figura 14: Rutas estáticas en R2



```
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 10.0.208.0 255.255.255.0 10.0.23.2
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.2
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.2
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#
```

Fuente 16: Diseño propio

Figura 15: Rutas estáticas en R3



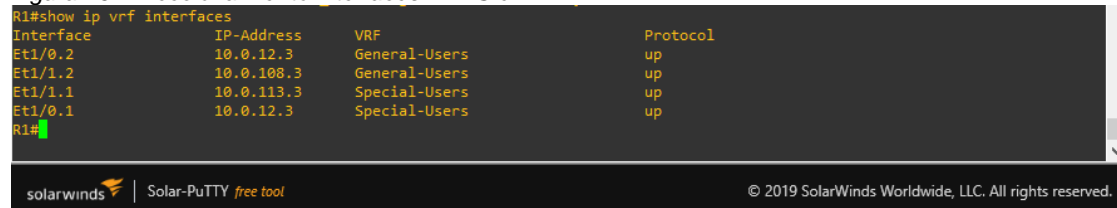
```
R3#show run | inc route
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.6
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.6
ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:23::2
R3#
```

Fuente 17: Diseño propio

2.4 Verificar el direccionamiento IP de las interfaces VRF implementadas en los Router R1, R2 y R3

Para realizar esta verificación se usa el comando “`show ip vrf interfaces`” en todos los routers:

Figura 16: Direccionamiento interfaces VRFS 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        10.0.108.3      General-Users    up
Et1/1.1        10.0.113.3      Special-Users    up
Et1/0.1        10.0.12.3       Special-Users    up
R1#
```

Fuente 18: Diseño propio

Figura 17: Direccionamiento interfaces VRFs en R2

```
R2#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.6       General-Users    up
Et1/1.2        10.0.23.6       General-Users    up
Et1/0.1        10.0.12.6       Special-Users    up
Et1/1.1        10.0.23.6       Special-Users    up
R2#
```

Fuente 19:Diseño propio

Figura 18: Direccionamiento interfaces VRFs en R3

```
R3#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.23.2       General-Users    up
Et1/1.2        10.0.208.2      General-Users    up
Et1/0.1        10.0.23.2       Special-Users    up
Et1/1.1        10.0.213.2      Special-Users    up
R3#
```

Fuente 20:Diseño propio

Para verificar la conectividad desde R1 hacia R3 se realiza un ping a las VRF General-User y Special-Users

- ping vrf General-Users 10.0.208.2
- ping vrf General-Users 2001:db8:acad:208::1
- ping vrf Special-Users 10.0.213.2
- ping vrf Special-Users 2001:db8:acad:213::1

Figura 19: Verificación conectividad de R1 a R3

```
R1#ping vrf General-Users 10.0.208.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/55/104 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 = 32/55/116 ms
R1#ping vrf Special-Users 10.0.213.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/42/48 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 = 32/41/56 ms
R1#
```

Fuente 21:Diseño propio

3. CONFIGURAR CAPA 2

En esta parte, tendrá que configurar los Switches para soportar la conectividad con los dispositivos finales. Las tareas de configuración, son las siguientes:

3.1 Deshabilitar todas las interfaces en D1, D2, y A1, en D1 y D2, Deshabilitar G1/0/1 to G1/0/24. En A1, Deshabilitar F0/1 – F0/24, G0/1 – G0/2.

Para deshabilitar todas las interfaces que no están siendo usadas en los dispositivos D1, D2 y A1 se verifica cuales están vacías, esto se puede observar desde la topología en GNS3 parándose con el mouse encima de cada dispositivo. Al hacerlo se observan las interfaces e1/0-3, e2/0-3 y e3/0-3 las cuales serán deshabilitadas.

Configuración Switch D1:

```
interface range e1/0-3, e2/0-3, e3/0-3 // Rango de interfaces en D1
shutdown // Deshabilita las interfaces en cada rango.
exit
```

Configuración Switch D2:

```
interface range e1/0-3, e2/0-3, e3/0-3 // Rango de las interfaces en D2
shutdown // Deshabilita las interfaces en cada rango.
exit
```

Configuración Switch A1:

```
interface range e1/0-3, e2/0-3, e3/0-3 // Rango de las interfaces en A1
shutdown // Deshabilita las interfaces en cada rango.
exit
```

3.2 En D1 y D2, Configurar los enlaces troncales para R1 and R3. Configurar y habilitar G1/0/11, como enlace troncal.

Configuración para D1:

Se configura la interface e0/2 que es la que está conectada a R1

```
interface e0/2 // Ingreso a la interfaz para iniciar configuración
switchport trunk encapsulation dot1q // configura el enlace con protocolo 802.1Q
switchport mode trunk // configure la interfaz como enlace troncalizado
no shutdown // Habilita la interfaz
exit
```

Se verifica configuración de D1 mediante el comando show interfaces trunk:

Figura 20: verificación interfaces troncales

```
D1#show interfaces trunk
Port      Mode          Encapsulation  Status        Native vlan
Et0/0     on            802.1q         trunking      1
Et0/1     on            802.1q         trunking      1
Et0/2     on            802.1q         trunking      1

Port      Vlans allowed on trunk
Et0/0     1-4094
Et0/1     1-4094
Et0/2     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1,8,13
Et0/1     1,8,13
Et0/2     1,8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     1,8,13
Et0/1     1,8,13
Et0/2     1,8,13
```

Fuente 22: Diseño propio

Configuración para D2: Se configura la interface e0/3 que es la que está conectada a R3

```
interface e0/3 // Ingreso a la interfaz para iniciar configuración
switchport trunk encapsulation dot1q // configura el enlace con protocolo 802.1Q
switchport mode trunk // configure la interfaz como enlace troncalizado
no shutdown // Habilita la interfaz
exit
```

3.3 En D1 y A1, configurar EtherChannel

En D1, Configurar y habilitar:

Interface G1/0/5 and G1/0/6

Port Channel 1 using PAgP

Se realiza configuración a las interfaces conectadas a A1 que son e0/0 y e0/1

```
interface range e0/0-1 // configuración rango de interfaces
switchport trunk encapsulation dot1q // configura el enlace con protocolo 802.1Q
switchport mode trunk // configura las interfaces como enlace troncalizado
channel-group 1 mode desirable // pone en modo activo los puertos del canal1, negociando el
estado al recibir paquetes PAgP
no shutdown // Habilita la interfaz
exit
```

Figura 21: Verificación configuración etherchannel y protocolo PAgP 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(30)        PAgP        Et0/0(1)  Et0/1(1)

D1#
Msg 18 13:58:41.119: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/2 (not full duplex), with R1 Ethernet1/1 (full duplex).
D1#
```

Fuente 23: Diseño propio

En A1, configurar y habilitar:
Interface F0/1 and F0/2
Port Channel 1 using PAgP

Se realiza configuración a las interfaces conectadas a D1 que son e0/0 y e0/1

```
interface range e0/0-1 // configuración rango de interfaces
switchport trunk encapsulation dot1q // configura el enlace con protocolo 802.1Q
switchport mode trunk // configura las interfaces como enlace troncalizado
channel-group 1 mode desirable // pone en modo activo los puertos del canal1, negociando el
estado al recibir paquetes PAgP
no shutdown // Habilita la interfaz
exit
```

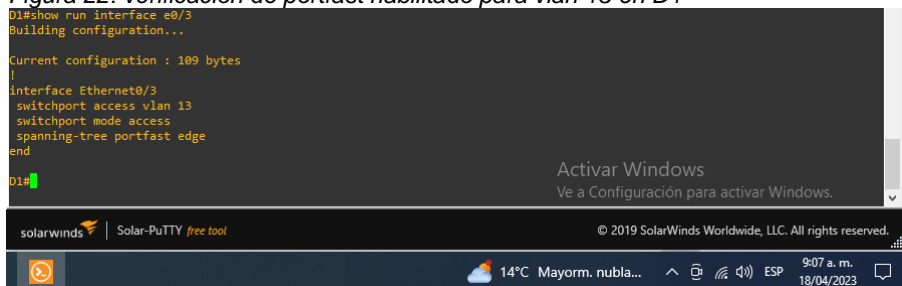
3.4 En D1, D2 y A1, configurar los puertos de acceso PC1, PC2, PC3, and PC4.

En D1, configure la interface G1/0/23 como Puerto de acceso de VLAN 13 y habilite Portfast.

La interface usada para la conexión de la VLAN13 es e0/3

```
interface e0/3 // ingresa a configuración de interfaz
switchport mode access // configura el Puerto en modo de acceso
switchport access vlan 13 // permite asignar el Puerto a la VLAN13
spanning-tree portfast // permite activar la protección BPDU con el PortFast habilitado
no shutdown // permite habilitar y activar la interfaz
exit
```

Figura 22: verificación de portfast habilitado para vlan 13 en D1



Fuente 24: Diseño propio

En D2, configure la interface G1/0/23 puerto de acceso de VLAN 13 y habilite Portfast.

La interface usada para la conexión de la VLAN13 es e0/2

```
interface e0/2// ingresa a configuración de interfaz
switchport mode access // configura el Puerto en modo de acceso
switchport access vlan 13 // permite asignar el Puerto a la VLAN13
spanning-tree portfast // permite activar la protección BPDU con el PortFast habilitado
no shutdown // permite habilitar y activar la interfaz
exit
```

En D2, configure interface G1/0/24 como Puerto de acceso de VLAN 8 y habilite Portfast.

La interface usada para la conexión de la VLAN8 es e0/0

```
interface e0/0// ingresa a configuración de interfaz
switchport mode access // configura el Puerto en modo de acceso
switchport access vlan 8 // permite asignar el Puerto a la VLAN8
spanning-tree portfast // permite activar la protección BPDU con el PortFast habilitado
no shutdown // permite habilitar y activar la interfaz
exit
```

En A1, configure interface G1/0/24 como Puerto de acceso de VLAN 8 y habilite Portfast.

La interface usada para la conexión de la VLAN8 es e0/2

```
interface e0/2// ingresa a configuración de interfaz
switchport mode access // configura el Puerto en modo de acceso
switchport access vlan 8 // permite asignar el Puerto a la VLAN8
spanning-tree portfast // permite activar la protección BPDU con el PortFast habilitado
no shutdown // permite habilitar y activar la interfaz
```

3.5 Verificar conectividad de PC a PC.

Desde PC1, verificar conectividad IPv4 y IPv6 hacia PC2.

A continuación, se verifica la conectividad de los computadores que hacen parte de la VRF “Usuarios Especiales”, a través del comando ping desde PC1 a la dirección IPv4 e IPv6 del PC2:

Figura 23: Ping 10.0.213.36

```
PC1> ping 10.0.213.36
84 bytes from 10.0.213.36 icmp_seq=1 ttl=61 time=323.759 ms
84 bytes from 10.0.213.36 icmp_seq=2 ttl=61 time=64.098 ms
84 bytes from 10.0.213.36 icmp_seq=3 ttl=61 time=59.164 ms
84 bytes from 10.0.213.36 icmp_seq=4 ttl=61 time=110.275 ms
84 bytes from 10.0.213.36 icmp_seq=5 ttl=61 time=58.993 ms
PC1> []
```

Fuente 25: Diseño propio

Figura 24: ping 2001:db8:acad:213::50

```
PC1> ping 2001:db8:acad:213::50
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=125.105 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=57.007 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=45.188 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=49.225 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=63.768 ms
PC1> []
```

Fuente 26: Diseño propio

Desde PC3, verificar conectividad IPv4 y IPv6 hacia PC4

A continuación, se verifica la conectividad de los computadores que hacen parte de la VRF “Usuarios Generales”, a través del comando ping desde PC3 a la dirección IPv4 e IPv6 del PC4:

Figura 25: Ping 10.0.208.36

```
PC3> ping 10.0.208.36
84 bytes from 10.0.208.36 icmp_seq=1 ttl=61 time=84.187 ms
84 bytes from 10.0.208.36 icmp_seq=2 ttl=61 time=62.283 ms
84 bytes from 10.0.208.36 icmp_seq=3 ttl=61 time=61.157 ms
84 bytes from 10.0.208.36 icmp_seq=4 ttl=61 time=60.169 ms
84 bytes from 10.0.208.36 icmp_seq=5 ttl=61 time=60.219 ms
PC3> []
```

Fuente 27: Diseño propio

Figura 26: Ping 2001:db8:acad:208::50

```
PC3> ping 2001:db8:acad:208::50
2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=90.561 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=61.149 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=61.223 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=60.198 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=59.062 ms
PC3> 
```

Fuente 28: Diseño propio

Ahora se verifica que no haya comunicación entre los PCs de Especial-Users y General-Users, haciendo ping por ejemplo de PC1 a PC3:

Figura 27: ping desde PC1 a PC3

```
PC1> ping 10.0.108.36
*10.0.12.6 icmp_seq=1 ttl=254 time=73.758 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.6 icmp_seq=2 ttl=254 time=69.714 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.6 icmp_seq=3 ttl=254 time=25.558 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.6 icmp_seq=4 ttl=254 time=27.886 ms (ICMP type:3, code:1, Destination host unreachable)
*10.0.12.6 icmp_seq=5 ttl=254 time=26.818 ms (ICMP type:3, code:1, Destination host unreachable)
PC1> 
```

Fuente 29: Diseño propio

4. CONFIGURACIÓN DE LA SEGURIDAD

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

4.1 en todos los dispositivos, configurar la seguridad privilegiada en modo EXE.

Configure an enable secret as follows:

Algorithm type: SCRYPT

Password: nombrestudianteXYZ

Para este paso se realizan el mismo código en todos los dispositivos de la red:

Para R1,R2;R3, D1, D2 y A1

enable algorithm-type SCRYPT secret JULIAN362// permite habilitar algoritmo de encriptación y asignación de contraseña según lo establecido en la guía de actividades.

4.2 En todos los dispositivos, crear una cuenta de usuario local.

Se aplica el mismo código en todos los equipos de red para crear la cuenta de usuario local.

Configure a local user:

- Name: admin
- Privilege level: 15
- Algorithm type: SCRYPT
- Password: nombrestudianteXYZ.

Para R1,R2;R3, D1, D2 y A1:

username admin privilege 15 algorithm-type SCRYPT secret JULIAN362

// permite configurar el nombre de usuario y nivel de privilegio y configuración de encriptación de clave secreta.

4.3 En todos los dispositivos, habilitar la autenticación AAA.

Enable AAA authentication using the local database on all lines

Para habilitar la autenticación AAA en todos los dispositivos (R1, R2, R3, D1, D2 y A1) de red se aplica el siguiente código:

aaa new-model //habilita el uso de listas en metodos de autenticación

aaa authentication login default local // realiza la habilitación de inicio de sesión con autenticación AAA predeterminada

end // fin de la configuración de autenticación

Finalmente, para verificar la configuración de nombre de usuario, autenticación AAA y clave encriptada, realizada a cada dispositivo intermedio se realiza a través del comando show run | include aaa|username, así:

Figura 28: Verificación configuración Usuario, autenticación AAA y encriptación de password en A1

```
*Apr 21 02:49:38.286: %SYS-5-CONFIG_I: Configured from console by console
A1#show run | include aaa|username
username admin privilege 15 secret 9 $9$vrFLFumvBoB/34$DYXuniRxeMrvOu4I6UT94XIcU3aB5YyBV8ilyk6L3Q
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```

Fuente 30: Diseño propio

Figura 29: Verificación configuración Usuario, autenticación AAA y encriptación de password en D1

```
*Apr 21 02:58:35.596: %SYS-5-CONFIG_I: Configured from console by console
D1#show run | include aaa|username
username admin privilege 15 secret 9 $9$nPIbJx1NU3iKB4$jzx104bbsmiJHJVDD5n8nXgLyPhT.q0EzLzxC0gZug
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
*Apr 21 02:57:01.587: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/2 (not full duplex), with R1 Ethernet1/1 (full duplex).
D1#
```

Fuente 31: Diseño propio

Figura 30: Verificación configuración Usuario, autenticación AAA y encriptación de password en D2

```
D2#show run | include aaa|username
username admin privilege 15 secret 9 $9$4QjdhQ4hUqznuq$WKNFY1MOVIgw57ns7m9h7YiApfZijvPie11xFDLhTc
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```

Fuente 32: Diseño propio

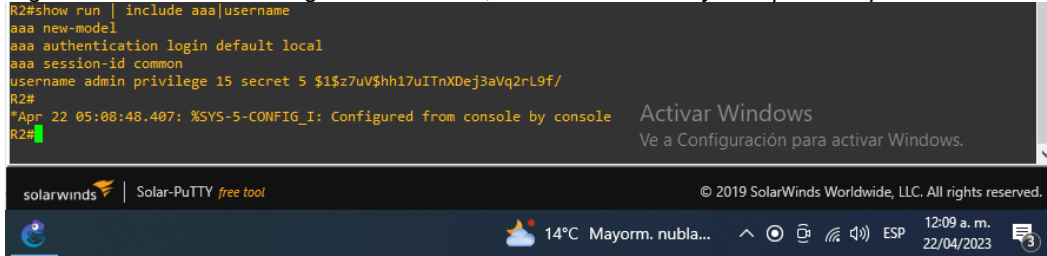
Figura 31: Verificación configuración Usuario, autenticación AAA y encriptación de password en R1

```
R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$/21t$kptC2G5Ivsfd0XZ8vca8M0
R1#
*Apr 22 04:24:51.979: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with D1 Ethernet0/2 (half duplex).
R1#
```

Fuente 33: Diseño propio

Figura 32: Verificación configuración Usuario, autenticación AAA y encripción de password en R2

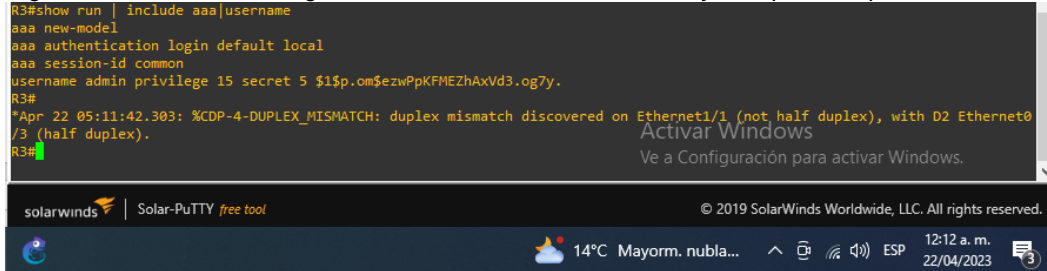
```
R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$z7uV$hh17uITnXDej3aVq2rL9f/
R2#
*Apr 22 05:08:48.407: %SYS-5-CONFIG_I: Configured from console by console
R2#
```



Fuente 34: Diseño propio

Figura 33: Verificación configuración Usuario, autenticación AAA y encripción de password en R3

```
R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$p.om$ezwPpKFMEZhAxVd3.og7y.
R3#
*Apr 22 05:11:42.303: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with D2 Ethernet0/3 (half duplex).
R3#
```



Fuente 35: Diseño propio

CONCLUSIONES

Se logró realizar la configuración de dispositivos Cisco en GNS3 y su correcta instalación, lo cual permitió realizar la implementación de la topología de red para la presente actividad.

Se logró realizar la configuración básica de los dispositivos de la red planteada para la actividad, posteriormente se realizaron las configuraciones VRF creando las tablas de enrutamiento virtuales que permiten generar independencia entre las VRFs Usuarios Especiales y Usuarios Generales, rutas estáticas para la conexión de extremo a extremo, configuración tanto para protocolo IPv4 e IPv6.

De igual manera se pudo realizar las configuraciones de las interfaces IPv4 y IPv6 en los routers R1, R2 y R3 de acuerdo con la tabla de direccionamiento planteada, usando comandos especiales como los usados para la generación de VRF como por ejemplo “vrf forwarding”, “ip route vrf”, y otros comandos muy importantes para verificación de configuración como “show ip vrf interfaces”

Se logró la creación de redes vlans configuradas en los switches dentro de una misma red física para permitir la conectividad con los dispositivos finales de las redes independientes denominadas “Especial-Users” y “General-Users”.

BIBLIOGRAFIA

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

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

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

EDGEWORTH, Bradley, et al. VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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