DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CRISTHIAN CAMILO VALENCIA REINA

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CRISTHIAN CAMILO VALENCIA REINA

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

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

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

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Pereira, 26 de junio de 2022

AGRADECIMIENTOS

A mi esposa y mi hijo, por ser el motor y la fuerza que impulsa el deseo de salir adelante cada día, por su acompañamiento en toda esta etapa educativa, por su amor, paciencia y apoyo, con el cual llegamos juntos a cumplir una meta más de muchas que nos hemos propuesto para nuestra vida.

A mi madre y a mi padre, por enseñarme la importancia del trabajo, el esfuerzo y la dedicación para lograr los objetivos en la vida, a mi hermano, por ser el amigo incondicional que la vida me regalo y del cual me siento orgulloso, a ellos que nunca me han dejado solo, siempre les estaré agradecido.

A todas las personas que han hecho posible llegar al final y concluir con éxito este paso tan importante para mi vida y la de mi familia, mil gracias.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ETHERCHANNEL: Tecnología que permite agrupar varios enlaces físicos en un solo enlace lógico, con lo cual se logra mayor redundancia, ancho de banda y respuesta a fallos en las conexiones de dispositivos de red.

INTERFAZ FISICA: Componente físico o de hardware con el cual se conecta un dispositivo o periférico a una red.

PROTOCOLO AAA: Conjunto de herramientas utilizadas para brindar seguridad y control de acceso a los dispositivos de red, combinando funciones de autenticación, autorización y registro.

PROTOCOLO DE ENRUTAMIENTO: Conjunto de procedimientos utilizados para la comunicación entre routers, con el fin de facilitar el intercambio de información de enrutamientos, actualización de tablas enrutamiento, selección de rutas y detección de cambios dentro de la red.

ROUTER: Dispositivo que permite interconectar diferentes redes, gestionar paquetes de datos, definir las mejores rutas de distribución mediante al análisis de tablas de enrutamiento y funcionalidades de seguridad de red.

ROUTER ON A STICK: Permite crear subinterfaces en un router utilizando una interfaz física del mismo, esto con el fin de maximizar la utilización de puertos del router, escalabilidad de red y mayor manejo de datos.

SWITCH: Dispositivo encargado de interconectar diversos equipos dentro de una red, ofrece escalabilidad y manejo de funciones básicas de conexión, hasta funciones avanzadas de configuración, enrutamiento y gestión para el manejo de datos a gran escala y altas velocidades de transmisión.

VLAN: Redes de área local virtuales, método que permite la creación de redes lógicas de manera independiente dentro de una sola red física, con el fin de segmentar y mejorar el manejo de red.

VRF: Enrutamiento virtual y reenvió, tecnología que permite que un router físico pueda tener y manejar múltiples routers virtuales, ejecutando tablas de enrutamiento virtuales simultáneamente y de manera independiente, sobre un mismo medio físico.

RESUMEN

El presente trabajo se elabora como prueba de las habilidades prácticas en electrónica y redes, adquiridas durante el transcurso del Diplomado de Profundización CISCO CCNP, para dar solución al escenario de red propuesto, en el cual se realizan configuraciones multi-VRF para segmentar e independizar dos grupos de usuarios de red que comparten medios físicos de conexión.

Mediante la utilización del software especializado para la simulación de redes GNS3, se construye la topología de red propuesta y se configuran ajustes básicos en cada uno de los dispositivos con tecnología CISCO integrados a la red y su respectivo direccionamiento de interfaces de acuerdo a la tabla de enrutamiento establecida, se configuran VRF y rutas estáticas en los dispositivos de capa 3 y se asignan mecanismos de seguridad en los equipos, así mismo, se configuran los dispositivos de capa 2, con los cuales, se logra la conmutación y conectividad con los host de usuario, verificando el funcionamiento de la red mediante la realización de pruebas de comunicación entre dispositivos finales.

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

ABSTRACT

The present work is elaborated as a test of the practical skills in electronics and networks, acquired during the course of the CISCO CCNP Deepening Diploma, to solve the proposed network scenario, in which multi-VRF configurations are made to segment and make two groups independent. of network users who share physical means of connection.

Through the use of specialized software for the simulation of GNS3 networks, the proposed network topology is built and basic settings are configured in each of the devices with CISCO technology integrated into the network and their respective interface addressing according to the table of established routing, VRF and static routes are configured in the layer 3 devices and security mechanisms are assigned in the equipment, likewise, the layer 2 devices are configured, with which switching and connectivity with the hosts of user, verifying the operation of the network by carrying out communication tests between end devices.

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

INTRODUCCIÓN

La globalización y la constante evolución tecnológica, han hecho necesaria una migración hacia sistemas autónomos con capacidades de procesamiento superior, los cuales permitan la interconexión, recepción y transmisión de datos de forma instantánea a nivel mundial, los sistemas de comunicación se encuentran basados en redes descentralizadas, las cuales utilizan diferentes protocolos para la conexión de todos los dispositivos que se vinculen a la red, de allí, la importancia de la implementación de tecnologías y equipos electrónicos, que permitan el manejo y administración eficiente de los datos transmitidos, ya sea en redes de pequeña, mediana o gran escala, por tal motivo, el Diplomado de Profundización CISCO CCNP, permite desarrollar la capacidad de brindar soluciones a problemáticas de red a nivel empresarial, comercial y de uso hogar, mediante la planificación e implementación de protocolos de red y configuración de dispositivos, los cuales permitan la adecuada conexión entre equipos de manera local o remota, ya sea de forma cableada o inalámbrica.

En el desarrollo del escenario de red propuesto, se realiza la configuración de dispositivos de conexión como los son routers y switches, dentro de una red empresarial, para la cual es necesario garantizar la conectividad entre usuarios de extremo a extremo, con independencia de grupo al cual pertenecen, dichos grupos, son separados mediante la creación de redes lógicas (VRF), las cuales deben soportar direccionamiento IPV4 e IPV6, tomando en cuenta que físicamente la red comparte una sola conexión entre dispositivos, se hace necesario crear sub interfaces y rutas estáticas para cada uno de los dispositivos de capa 3 y garantizar así la conexión entre cada uno de ellos.

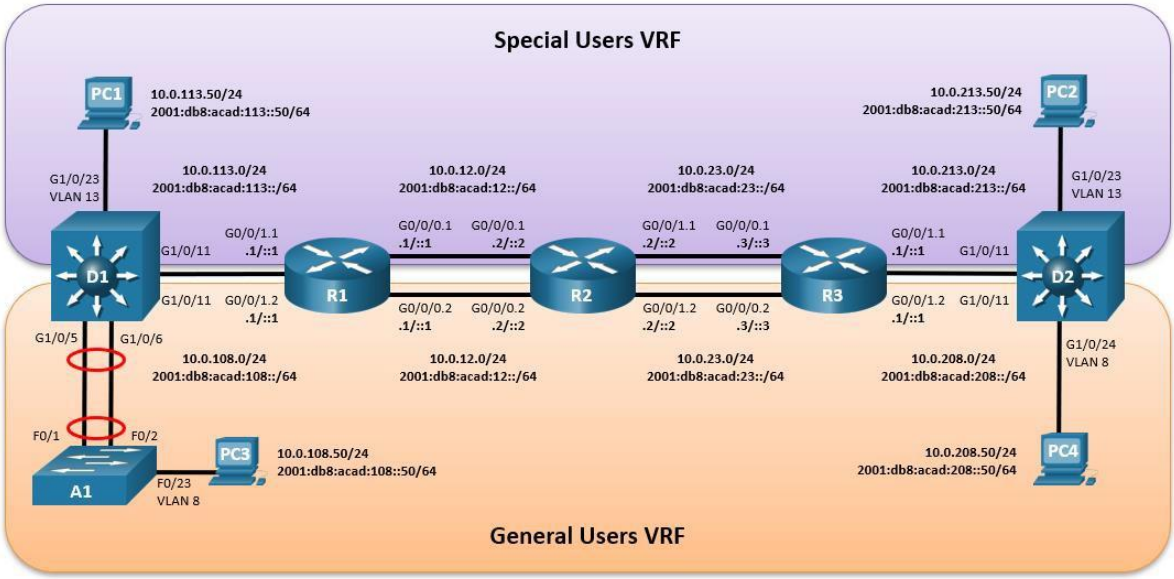
Las configuraciones de capa 2 se realizan con el fin de brindar el punto de conexión para cada uno de los hosts de usuario pertenecientes a cada VRF, para ello, se crean enlaces troncales y se definen protocolos para la configuración de enlaces EtherChannel en los switches requeridos, con el fin de evidenciar el funcionamiento de enlaces redundantes, con capacidad de equilibrar cargas ante fallos de conexión en dicho enlace, para los dispositivos de capa 2, se configuran los puertos de acceso para cada host teniendo en cuenta la red de área virtual a la cual pertenecen y se realizan pruebas de conectividad entre usuarios finales para comprobar la configuraciones y la independencia de las redes planteadas.

Como es necesario en toda topología de red, se configuran mecanismos de seguridad para cada uno de los dispositivos de la red, esto con el fin de garantizar accesibilidad a las configuraciones solo a usuarios acreditados que cuenten con usuario y contraseñas de los equipos, mediante la utilización de protocolos de autenticación como el AAA.

DESARROLLO DEL ESCENARIO PROPUESTO

La figura 1, muestra el diseño de la topología planteada para su implementación y configuración a partir del uso de software especializado GNS3.

Figura 1. Topología de red propuesta.



Fuente: Guía UNAD – CCNP Avance final.

Tabla 1. Direccionamiento de dispositivos.

Dispositivo	Interfaz propuesta	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
R1	G1/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G1/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G0/0.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G0/0.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G1/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G1/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G2/0.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	G2/0.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G2/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G2/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G0/0.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G0/0.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NADA	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NADA	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64

PC3	NADA	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NADA	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

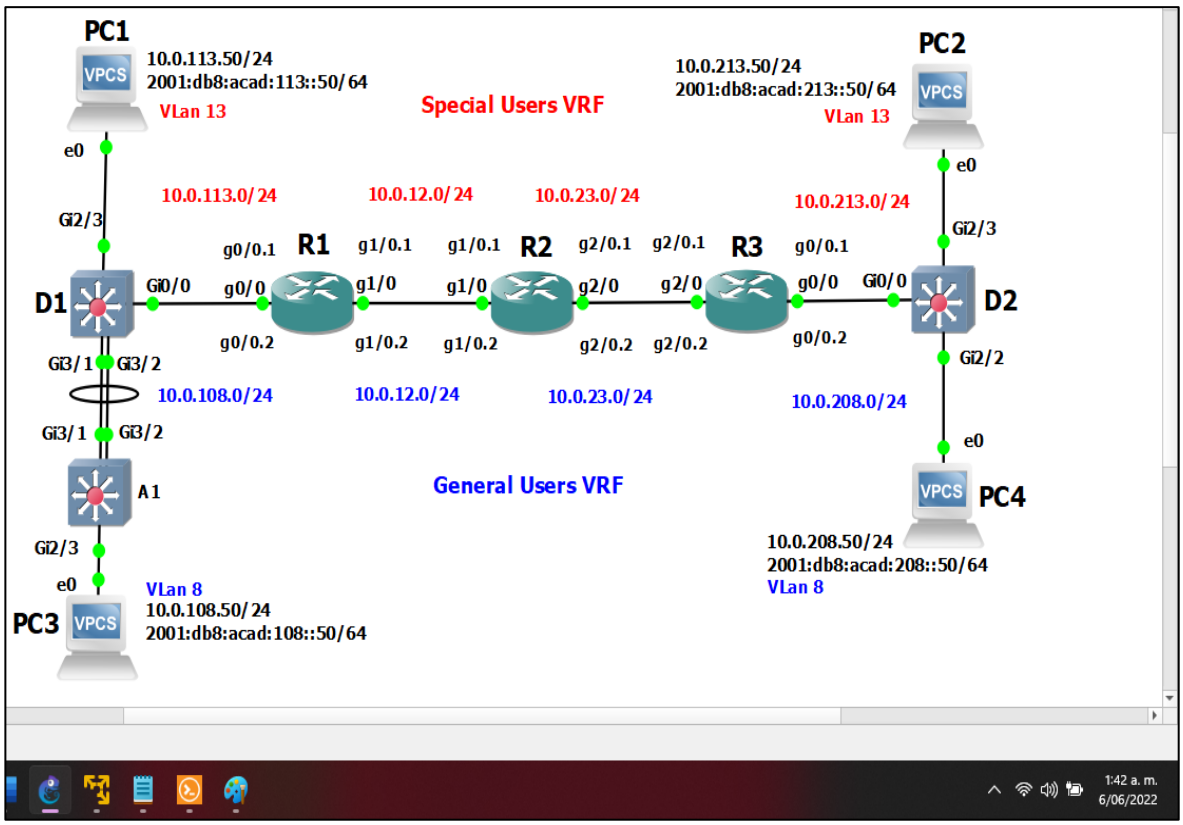
Fuente: Guía UNAD – CCNP Avance final.

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

Se realiza la configuración de la topología de red y las opciones básicas utilizando el software de simulación grafico de red GNS3.

Paso 1.1: Cablee la red como se muestra en la topología.

Figura 2. Topología de red propuesta en GNS3.



Fuente: Propia.

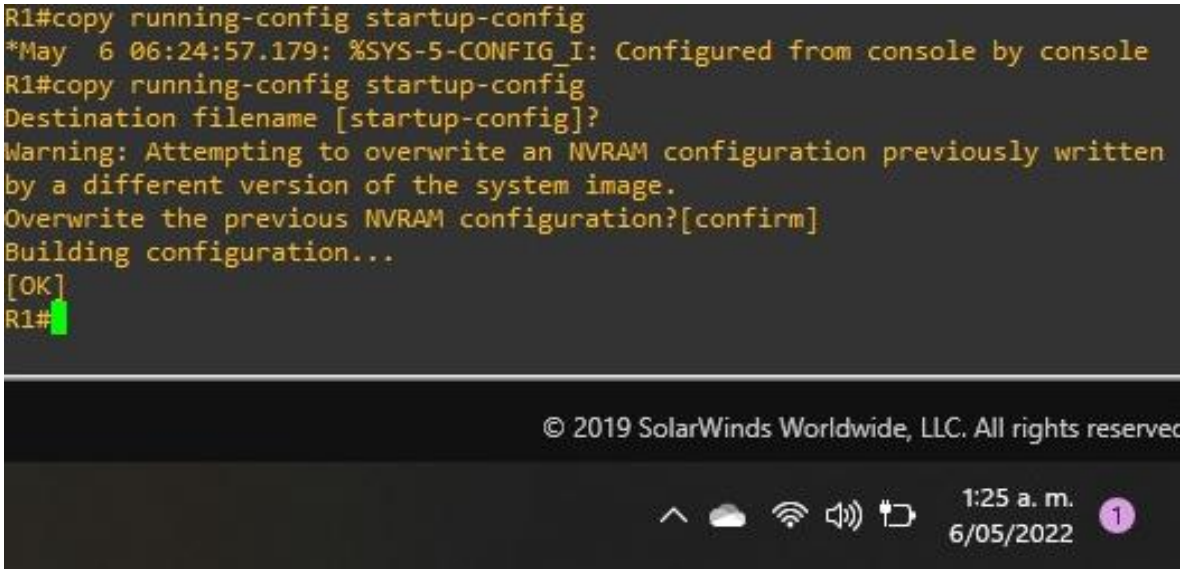
Paso 1.2: Configure los ajustes básicos para cada dispositivo.

Se realiza la configuración de los parámetros básicos para cada dispositivo de red.

Router R1

```
R1#conf term                                  //Modo configuración global
R1(config)#hostname R1                        //Nombre del Dispositivo R1
R1(config)#ipv6 unicast-routing               //Enrutamiento IPV6
R1(config)#no ip domain lookup                //Desactiva traducción de nombres a la dirección del dispositivo
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 2 #
                                              //Mensaje nombre de la practica en dispositivo
R1(config)#line con 0                         //Configuración línea de consola
R1(config-line)# exec-timeout 0 0             //Tiempo de desconexión de consola
R1(config-line)# logging synchronous          //Activa acceso sincrónico
R1(config-line)# exit
R1(config)#end                                //Sale de modo configuración
R1#copy running-config startup-config         //Guarda configuración en el dispositivo
```

Figura 3. Configuración ajustes básicos Router R1.



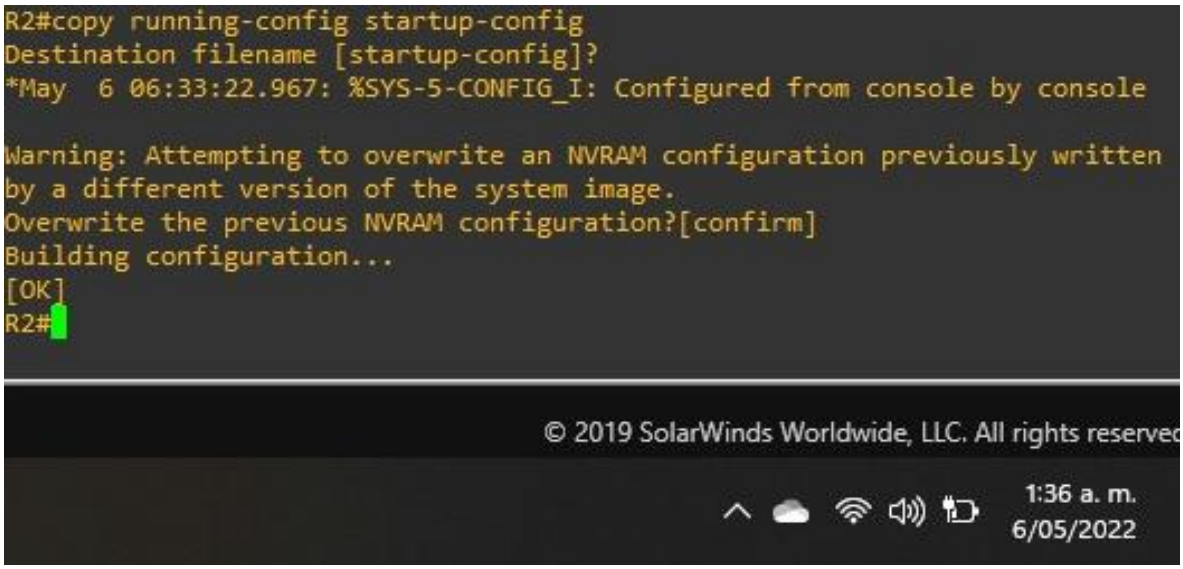
Fuente: Propia.

Router R2

```
R2#conf term                                  //Modo configuración global
R2(config)#hostname R2                        //Nombre del Dispositivo R2
R2(config)#ipv6 unicast-routing               //Enrutamiento IPV6
R2(config)#no ip domain lookup                //Desactiva traducción de nombres a la dirección del dispositivo
```

R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 2 # *//Mensaje nombre de la practica en dispositivo*
R2(config)#line con 0 *//Configuración línea de consola*
R2(config-line)# exec-timeout 0 0 *//Tiempo de desconexión de consola*
R2(config-line)# logging synchronous *//Activa acceso sincrónico*
R2(config-line)# exit
R2(config)#end *//Sale de modo configuración*
R2#copy running-config startup-config *//Guarda configuración en el dispositivo*

Figura 4. Configuración ajustes básicos Router R2.



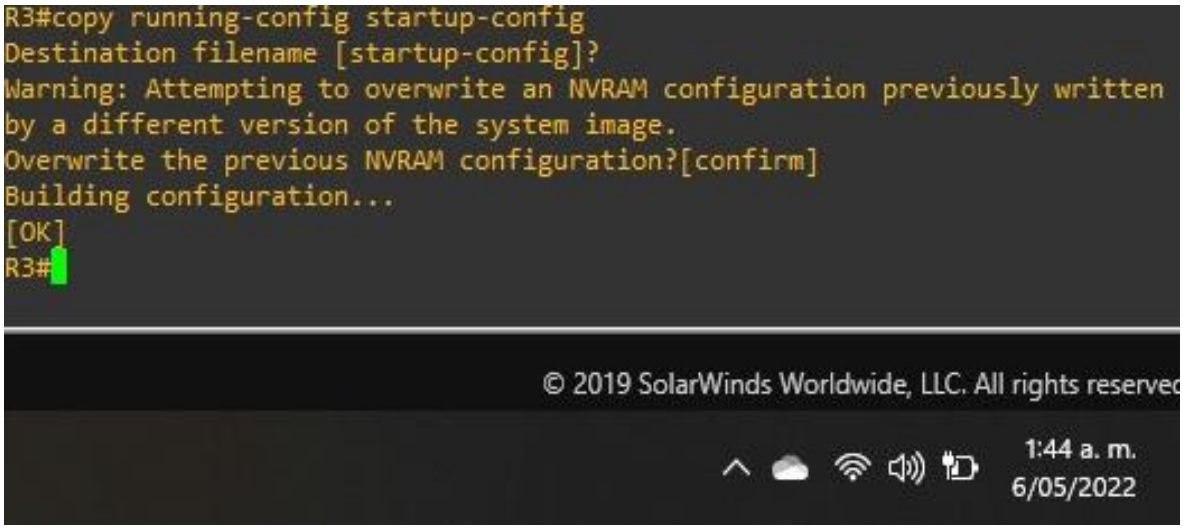
Fuente: Propia.

Router R3

R3#conf term *//Modo configuración global*
R3(config)#hostname R3 *//Nombre del Dispositivo R3*
R3(config)#ipv6 unicast-routing *//Enrutamiento IPV6*
R3(config)#no ip domain lookup *//Desactiva traducción de nombres a la dirección del dispositivo*
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 2 # *//Mensaje nombre de la practica en dispositivo*
R3(config)#line con 0 *//Configuración línea de consola*
R3(config-line)# exec-timeout 0 0 *//Tiempo de desconexión de consola*

R3(config-line)# logging synchronous //*Activa acceso sincrónico*
R3(config-line)# exit
R3(config)#end //*Sale de modo configuración*
R3#copy running-config startup-config //*Guarda configuración en el dispositivo*

Figura 5. Configuración ajustes básicos Router R3.



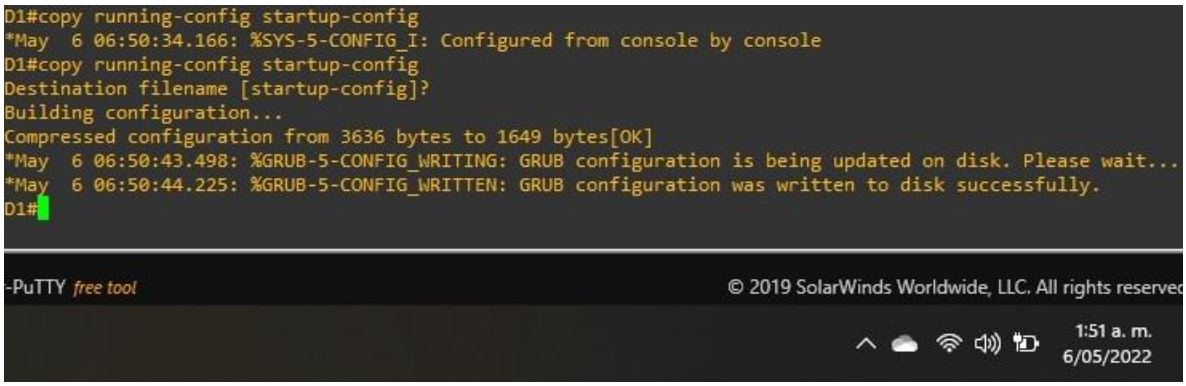
Fuente: Propia.

Switch D1

Switch>enable //*Ingreso a modo privilegiado*
Switch#conf term //*Modo configuración global*
Switch(config)#hostname D1 //*Nombre del Dispositivo D1*
D1(config)#ip routing //*Enrutamiento IPV4*
D1(config)#ipv6 unicast-routing //*Enrutamiento IPV6*
D1(config)#no ip domain lookup //*Desactiva traducción de nombres a la dirección del dispositivo*
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 2 # //*Mensaje nombre de la practica en dispositivo*
D1(config)#line con 0 //*Configuración línea de consola*
D1(config-line)# exec-timeout 0 0 //*Tiempo de desconexión de consola*
D1(config-line)# logging synchronous //*Activa acceso sincrónico*
D1(config-line)# exit
D1(config)#vlan 8 //*Configura Vlan 8*
D1(config-vlan)# name General-Users //*Asigna nombre a la Vlan 8*

D1(config-vlan)# exit
D1(config)#vlan 13 *//Configura Vlan 13*
D1(config-vlan)# name Special-Users *//Asigna nombre a la Vlan 13*
D1(config-vlan)# exit
D1(config)#end *//Sale de modo configuración*
D1#copy running-config startup-config *//Guarda configuración en el dispositivo*

Figura 6. Configuración ajustes básicos Switch D1.



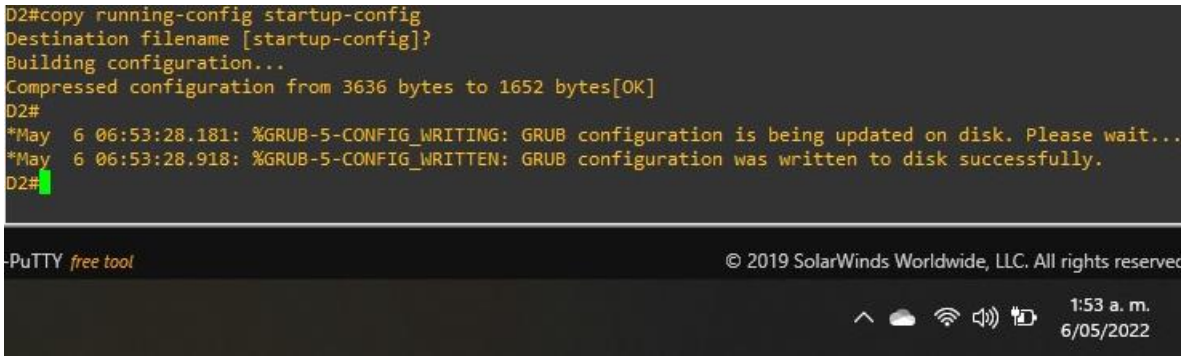
Fuente: Propia.

Switch D2

Switch>enable *//Ingreso a modo privilegiado*
Switch#conf term *//Modo configuración global*
Switch(config)#hostname D2 *//Nombre del Dispositivo D2*
D2(config)#ip routing *//Enrutamiento IPV4*
D2(config)#ipv6 unicast-routing *//Enrutamiento IPV6*
D2(config)#no ip domain lookup *//Desactiva traducción de nombres a la dirección del dispositivo*
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 2 # *//Mensaje nombre de la practica en dispositivo*
D2(config)#line con 0 *//Configuración línea de consola*
D2(config-line)# exec-timeout 0 0 *//Tiempo de desconexión de consola*
D2(config-line)# logging synchronous *//Activa acceso sincrónico*
D2(config-line)# exit
D2(config)#vlan 8 *//Configura Vlan 8*
D2(config-vlan)# name General-Users *//Asigna nombre a la Vlan 8*
D2(config-vlan)# exit
D2(config)#vlan 13 *//Configura Vlan 13*

D2(config-vlan)# name Special-Users //*Asigna nombre a la Vlan 13*
D2(config-vlan)# exit
D2(config)#end //*Sale de modo configuración*
D2#copy running-config startup-config //*Guarda configuración en el dispositivo*

Figura 7. Configuración ajustes básicos Switch D2.

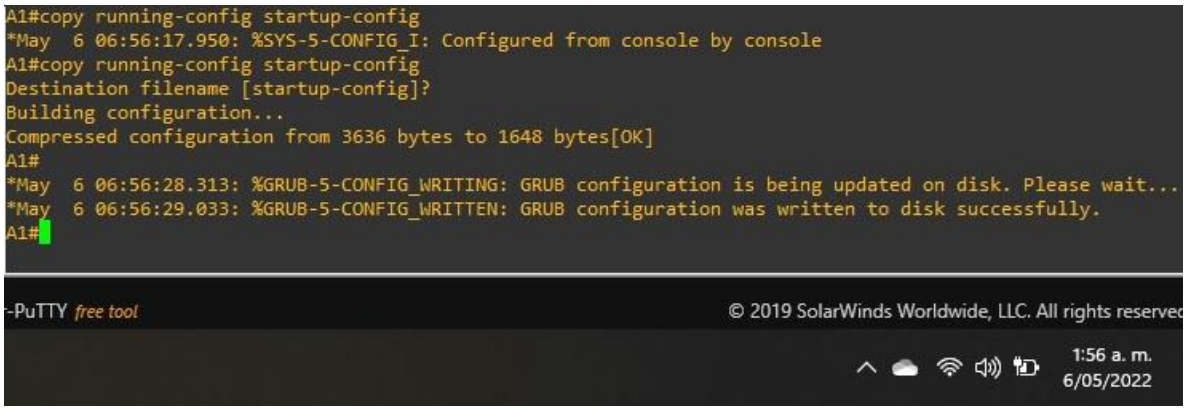


Fuente: Propia.

Switch A1

Switch>enable //*Ingreso a modo privilegiado*
Switch#conf term //*Modo configuración global*
Switch(config)#hostname A1 //*Nombre del Dispositivo A1*
A1(config)#ipv6 unicast-routing //*Enrutamiento IPV6*
A1(config)#no ip domain lookup //*Desactiva traducción de nombres a la dirección del dispositivo*
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 2 # //*Mensaje nombre de la practica en dispositivo*
A1(config)#line con 0 //*Configuración línea de consola*
A1(config-line)# exec-timeout 0 0 //*Tiempo de desconexión de consola*
A1(config-line)# logging synchronous //*Activa acceso sincrónico*
A1(config-line)# exit
A1(config)#vlan 8 //*Configura Vlan 8*
A1(config-vlan)# name General-Users //*Asigna nombre a la Vlan 8*
A1(config-vlan)# exit
A1(config)#end //*Sale de modo configuración*
A1#copy running-config startup-config //*Guarda configuración en el dispositivo*

Figura 8. Configuración ajustes básicos Switch A1.



Fuente: Propia.

Paso 1.3: Configure el direccionamiento de host PC1, PC2, PC3 y PC4 como se muestra en la tabla de direcciones.

Se asignan las direcciones IPV4 e IPV6 a cada uno de los hosts de la red, teniendo en cuenta la tabla de enrutamiento.

PC1> ip 10.0.113.50/24 10.0.113.1 *//Configura dirección IPV4*
PC1 : 10.0.113.50 255.255.255.0 10.0.113.1
PC1> ip 2001:db8:acad:113::50/64 *//Configura dirección IPV6*
PC1 : 2001:db8:acad:113::50/64
PC1> save *//Guarda configuraciones IPs PC1*

PC2> ip 10.0.213.50/24 10.0.213.1 *//Configura dirección IPV4*
PC2 : 10.0.213.50 255.255.255.0 10.0.213.1
PC2> ip 2001:db8:acad:213::50/64 *//Configura dirección IPV6*
PC2 : 2001:db8:acad:213::50/64
PC2> save *//Guarda configuraciones IPs PC2*

PC3> ip 10.0.108.50/24 10.0.108.1 *//Configura dirección IPV4*
PC3 : 10.0.108.50 255.255.255.0 10.0.108.1
PC3> ip 2001:db8:acad:108::50/64 *//Configura dirección IPV6*
PC3 : 2001:db8:acad:108::50/64
PC3> save *//Guarda configuraciones IPs PC3*

PC4> ip 10.0.208.50/24 10.0.208.1 *//Configura dirección IPV4*
PC4 : 10.0.208.50 255.255.255.0 10.0.208.1
PC4> ip 2001:db8:acad:208::50/64 *//Configura dirección IPV6*
PC4 : 2001:db8:acad:208::50/64
PC4> save *//Guarda configuraciones IPs PC4*

Figura 9. Configuración direccionamiento de host PC1, PC2, PC3 y PC4.

Fuente: Propia.

Parte 2: Configurar VRF y enrutamiento estático**.**

Se realiza la configuración de las VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de extremo a extremo y se verifican las configuraciones realizadas realizando ping desde el router R1 hacia el router R3 en cada VRF.

Paso 2.1: En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.

Se configuran dos VRF, Usuarios generales y Usuarios especiales, ambas VRF admiten IPv4 e IPv6.

Router R1:

```
R1#conf term                                  //Modo configuración global
R1(config)#vrf definition General-Users //Define VRF para usuarios generales
R1(config-vrf)# address-family ipv4       // Manejo de familia de protocolos  ipv4
R1(config-vrf-af)# address-family ipv6    // Manejo de familia de protocolos  ipv6
R1(config-vrf-af)# exit
R1(config-vrf)#vrf definition Special-Users //Define VRF para usuarios especiales
R1(config-vrf)# address-family ipv4       // Manejo de familia de protocolos  ipv4
R1(config-vrf-af)# address-family ipv6    // Manejo de familia de protocolos  ipv6
R1(config-vrf-af)# exit
```

Router R2:

```
R2#conf term                                  //Modo configuración global
R2(config)#vrf definition General-Users //Define VRF para usuarios generales
R2(config-vrf)# address-family ipv4       // Manejo de familia de protocolos  ipv4
R2(config-vrf-af)# address-family ipv6    // Manejo de familia de protocolos  ipv6
R2(config-vrf-af)# exit
R2(config-vrf)# vrf definition Special-Users //Define VRF para usuarios especiales
R2(config-vrf)# address-family ipv4       // Manejo de familia de protocolos  ipv4
R2(config-vrf-af)# address-family ipv6    // Manejo de familia de protocolos  iipv6
R2(config-vrf-af)# exit
```

Router R3:

```
R3#conf term                                  //Modo configuración global
R3(config)#vrf definition General-Users //Define VRF para usuarios generales
```

```
R3(config-vrf)# address-family ipv4       // Manejo de familia de protocolos  ipv4
R3(config-vrf-af)# address-family ipv6    // Manejo de familia de protocolos  ipv6
R3(config-vrf-af)# exit
R3(config-vrf)# vrf definition Special-Users //Define VRF para usuarios especiales
R3(config-vrf)# address-family ipv4       // Manejo de familia de protocolos  ipv4
R3(config-vrf-af)# address-family ipv6    // Manejo de familia de protocolos  ipv6
R3(config-vrf-af)# exit
```

Paso 2.2: En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direcciones anterior.

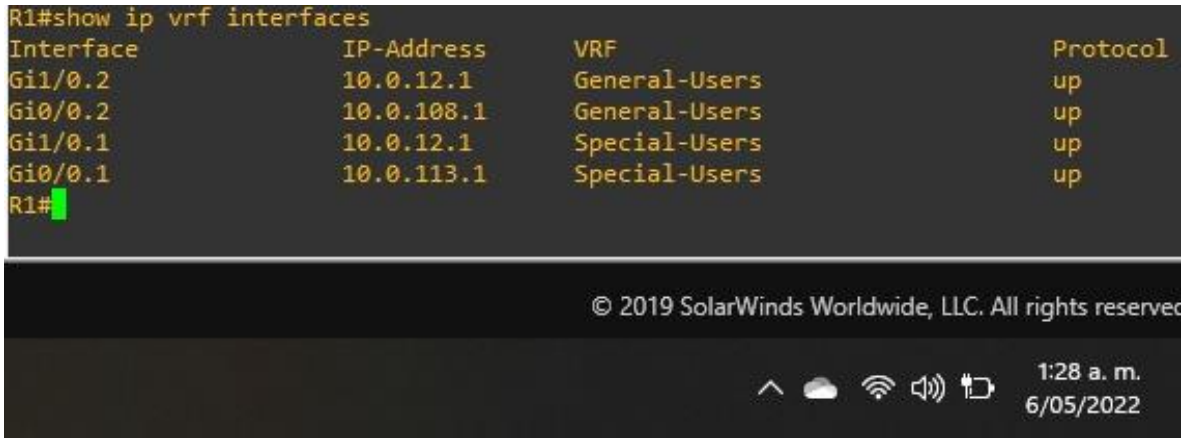
Todos los routers usan Router-On-A-Stick en sus interfaces G0/0.x para admitir la separación de los VRFs.Sub-interfaz.

Router R1:

```
R1(config-vrf)# interface g1/0.1                    //Ingresa subinterfaz para la VRF
R1(config-subif)#encapsulation dot1q 13             //Habilita 802.1Q asociado a Vlan 13
R1(config-subif)#  vrf forwarding Special-Users //Asigna la interfaz a la VRF S-U
R1(config-subif)#  ip address 10.0.12.1 255.255.255.0    //Configura dirección IPV4
R1(config-subif)#  ipv6 address fe80::1:1 link-local      //Configura link local
R1(config-subif)#  ipv6 address 2001:db8:acad:12::1/64 //Configura dirección IPV6
R1(config-subif)#  no shutdown                           //Activa la interfaz
R1(config-subif)#  exit
R1(config)#interface g0/0.1                         //Ingresa subinterfaz para la VRF
R1(config-subif)#  encapsulation dot1q 13        //Habilita 802.1Q asociado a Vlan 13
R1(config-subif)#  vrf forwarding Special-Users //Asigna la interfaz a la VRF S-U
R1(config-subif)#  ip address 10.0.113.1 255.255.255.0   //Configura dirección IPV4
R1(config-subif)#  ipv6 address fe80::1:3 link-local      //Configura link local
R1(config-subif)#  ipv6 address 2001:db8:acad:113::1/64 //Configura dirección IPV6
R1(config-subif)#  no shutdown                            //Activa la interfaz
R1(config-subif)#  exit
R1(config)# interface g1/0.2                         //Ingresa subinterfaz para la VRF
R1(config-subif)#  encapsulation dot1q 8          //Habilita 802.1Q asociado a Vlan 8
R1(config-subif)#  vrf forwarding General-Users //Asigna la interfaz a la VRF G-U
R1(config-subif)#  ip address 10.0.12.1 255.255.255.0    //Configura dirección IPV4
R1(config-subif)#  ipv6 address fe80::1:2 link-local      //Configura link local
R1(config-subif)#  ipv6 address 2001:db8:acad:12::1/64  //Configura dirección IPV6
R1(config-subif)#  no shutdown                           //Activa la interfaz
R1(config-subif)#  exit
```

```
R1(config)# interface g0/0.2                    //Ingresa subinterfaz para la VRF
R1(config-subif)#  encapsulation dot1q 8        //Habilita 802.1Q asociado a Vlan 8
R1(config-subif)#  vrf forwarding General-Users //Asigna la interfaz a la VRF G-U
R1(config-subif)#  ip address 10.0.108.1 255.255.255.0   //Configura dirección IPV4
R1(config-subif)#  ipv6 address fe80::1:4 link-local      //Configura link local
R1(config-subif)#  ipv6 address 2001:db8:acad:108::1/64  //Configura dirección IPV6
R1(config-subif)#  no shutdown                   //Activa la interfaz
R1(config-subif)#  exit
R1(config)# interface g1/0                      //Ingresa a la interfaz
R1(config-if)#  no ip address                   //Sin asignación de dirección IP
R1(config-if)#  no shutdown                     //Activa la interfaz
R1(config-if)#  exit
R1(config)#interface g0/0                       //Ingresa a la interfaz
R1(config-if)#  no ip address                   //Sin asignación de dirección IP
R1(config-if)#  no shutdown                     //Activa la interfaz
R1(config-if)#  exit
```

Figura 10. Configuración interfaces IPV4 e IPV6 para VRF en Router R1.



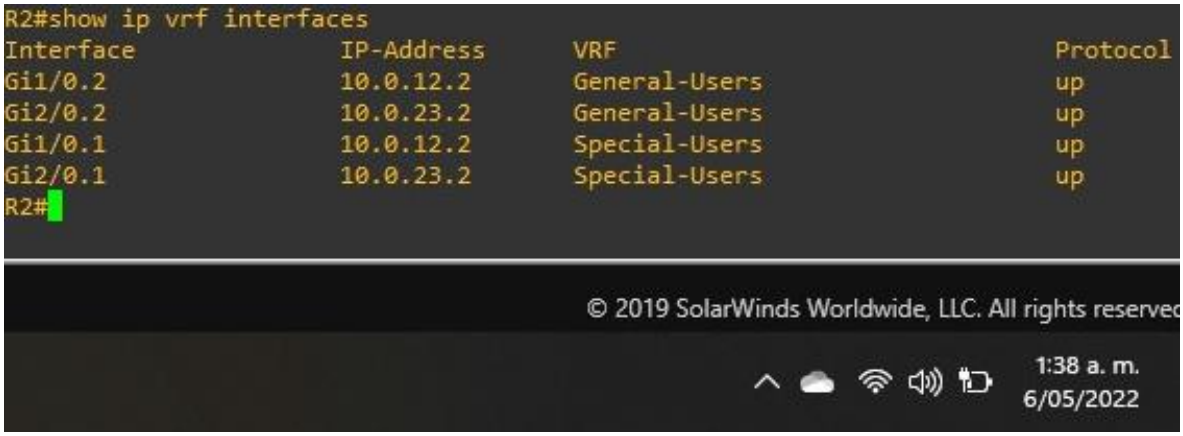
Fuente: Propia.

Router R2:

```
R2(config-vrf)#interface g1/0.1                 //Ingresa subinterfaz para la VRF
R2(config-subif)#  encapsulation dot1q 13       //Habilita 802.1Q asociado a Vlan 13
R2(config-subif)#  vrf forwarding Special-Users //Asigna la interfaz a la VRF S-U
R2(config-subif)#  ip address 10.0.12.2 255.255.255.0   //Configura dirección IPV4
R2(config-subif)#  ipv6 address fe80::2:1 link-local     //Configura link local
R2(config-subif)#  ipv6 address 2001:db8:acad:12::2/64  //Configura dirección IPV6
```

```
R2(config-subif)#  no shutdown                              //Activa la interfaz
R2(config-subif)#  exit
R2(config)#interface g2/0.1                          //Ingresa subinterfaz para la VRF
R2(config-subif)#  encapsulation dot1q 13         //Habilita 802.1Q asociado a Vlan 13
R2(config-subif)#  vrf forwarding Special-Users //Asigna la interfaz a la VRF S-U
R2(config-subif)#  ip address 10.0.23.2 255.255.255.0    //Configura dirección IPV4
R2(config-subif)#  ipv6 address fe80::2:3 link-local        //Configura link local
R2(config-subif)#  ipv6 address 2001:db8:acad:23::2/64  //Configura dirección IPV6
R2(config-subif)#  no shutdown                              //Activa la interfaz
R2(config-subif)#  exit
R2(config)# interface g1/0.2                          /Ingresa subinterfaz para la VRF
R2(config-subif)#  encapsulation dot1q 8          //Habilita 802.1Q asociado a Vlan 8
R2(config-subif)#  vrf forwarding General-Users //Asigna la interfaz a la VRF G-U
R2(config-subif)#  ip address 10.0.12.2 255.255.255.0    //Configura dirección IPV4
R2(config-subif)#  ipv6 address fe80::2:2 link-local        //Configura link local
R2(config-subif)#  ipv6 address 2001:db8:acad:12::2/64  //Configura dirección IPV6
R2(config-subif)#  no shutdown                             //Activa la interfaz
R2(config-subif)#  exit
R2(config)#interface g2/0.2                           /Ingresa subinterfaz para la VRF
R2(config-subif)#  encapsulation dot1q 8          //Habilita 802.1Q asociado a Vlan 8
R2(config-subif)#  vrf forwarding General-Users //Asigna la interfaz a la VRF G-U
R2(config-subif)#  ip address 10.0.23.2 255.255.255.0    //Configura dirección IPV4
R2(config-subif)#  ipv6 address fe80::2:4 link-local        //Configura link local
R2(config-subif)#  ipv6 address 2001:db8:acad:23::2/64  //Configura dirección IPV6
R2(config-subif)#  no shutdown                              //Activa la interfaz
R2(config-subif)#  exit
R2(config)# interface g1/0                            //Ingresa a la interfaz
R2(config-if)#  no ip address                         //Sin asignación de dirección IP
R2(config-if)#  no shutdown                           //Activa la interfaz
R2(config-if)#  exit
R2(config)#interface g2/0                             //Ingresa a la interfaz
R2(config-if)#  no ip address                         //Sin asignación de dirección IP
R2(config-if)#  no shutdown                           //Activa la interfaz
R2(config-if)#  exit
```

Figura 11. Configuración interfaces IPV4 e IPV6 para VRF en Router R2.



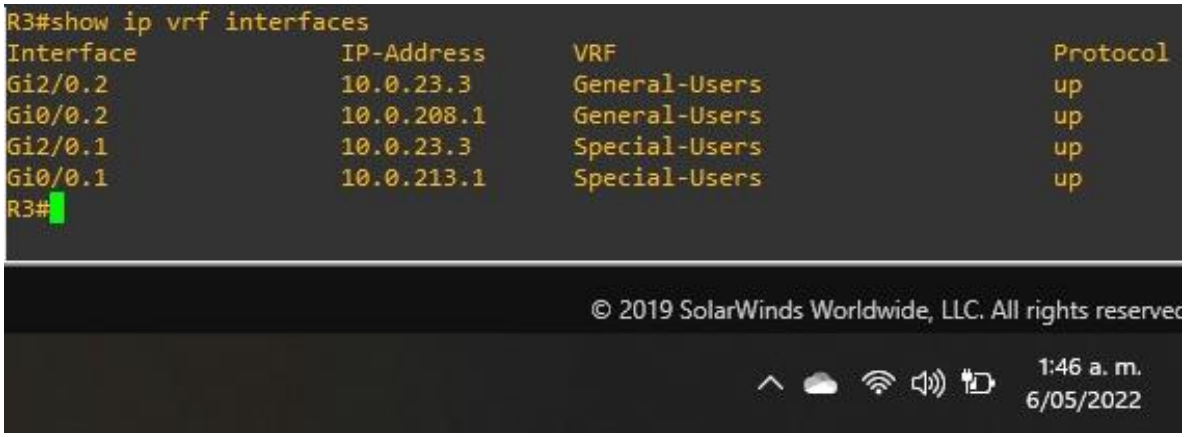
Fuente: Propia.

Router R3:

R3(config-vrf)#interface g2/0.1 *//Ingresa subinterfaz para la VRF*
R3(config-subif)# encapsulation dot1q 13 *//Habilita 802.1Q asociado a Vlan 13*
R3(config-subif)# vrf forwarding Special-Users *//Asigna la interfaz a la VRF S-U*
R3(config-subif)# ip address 10.0.23.3 255.255.255.0 *//Configura dirección IPV4*
R3(config-subif)# ipv6 address fe80::3:1 link-local *//Configura link local*
R3(config-subif)# ipv6 address 2001:db8:acad:23::3/64 *//Configura dirección IPV6*
R3(config-subif)# no shutdown *//Activa la interfaz*
R3(config-subif)# exit
R3(config)#interface g0/0.1 *//Ingresa subinterfaz para la VRF*
R3(config-subif)# encapsulation dot1q 13 *//Habilita 802.1Q asociado a Vlan 13*
R3(config-subif)# vrf forwarding Special-Users *//Asigna la interfaz a la VRF S-U*
R3(config-subif)# ip address 10.0.213.1 255.255.255.0 *//Configura dirección IPV4*
R3(config-subif)# ipv6 address fe80::3:3 link-local *//Configura link local*
R3(config-subif)# ipv6 address 2001:db8:acad:213::1/64 *//Configura dirección IPV6*
R3(config-subif)# no shutdown *//Activa la interfaz*
R3(config-subif)# exit
R3(config)# interface g2/0.2 *//Ingresa subinterfaz para la VRF*
R3(config-subif)# encapsulation dot1q 8 *//Habilita 802.1Q asociado a Vlan 8*
R3(config-subif)# vrf forwarding General-Users *//Asigna la interfaz a la VRF G-U*
R3(config-subif)# ip address 10.0.23.3 255.255.255.0 *//Configura dirección IPV4*
R3(config-subif)# ipv6 address fe80::3:2 link-local *//Configura link local*
R3(config-subif)# ipv6 address 2001:db8:acad:23::3/64 *//Configura dirección IPV6*
R3(config-subif)# no shutdown *//Activa la interfaz*
R3(config-subif)# exit

```
R3(config)#interface g0/0.2                          //Ingresa subinterfaz para la VRF
R3(config-subif)#  encapsulation dot1q 8             //Habilita 802.1Q asociado a Vlan 8
R3(config-subif)#  vrf forwarding General-Users     //Asigna la interfaz a la VRF G-U
R3(config-subif)#  ip address 10.0.208.1 255.255.255.0   //Configura dirección IPV4
R3(config-subif)#  ipv6 address fe80::3:4 link-local      //Configura link local
R3(config-subif)#  ipv6 address 2001:db8:acad:208::1/64 //Configura dirección IPV6
R3(config-subif)#  no shutdown                       //Activa la interfaz
R3(config-subif)#  exit
R3(config)# interface g2/0                           //Ingresa a la interfaz
R3(config-if)#  no ip address                        //Sin asignación de dirección IP
R3(config-if)#  no shutdown                          //Activa la interfaz
R3(config-if)#  exit
R3(config)#interface g0/0                            //Ingresa a la interfaz
R3(config-if)#  no ip address                        //Sin asignación de dirección IP
R3(config-if)#  no shutdown                          //Activa la interfaz
R3(config-if)#  exit
```

Figura 12. Configuración interfaces IPV4 e IPV6 para VRF en Router R3.



Fuente: Propia.

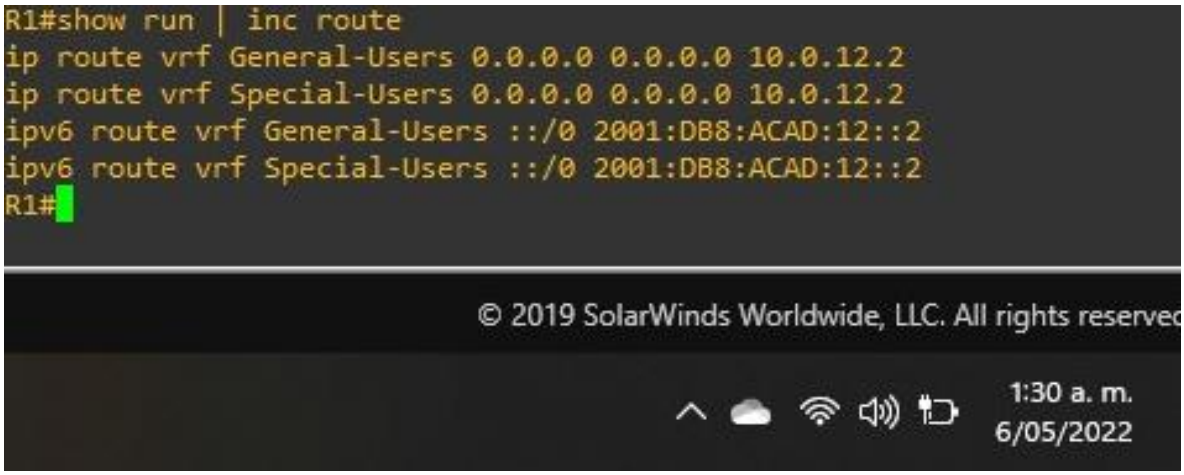
Paso 2.3: En R1 y R3, configure las rutas estáticas predeterminadas que apunten a R2.

Se realiza la configuración de las rutas estáticas predeterminadas para IPv4 e IPv6 en ambos VRF en los Router R1 y R3, tomando en cuenta la correcta asignación de las IPs, las mascaras de subred y las puertas de enlace, las cuales deben apuntar hacia el Router R2.

Router R1:

R1(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)# ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2
R1(config)# ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2
R1(config)# ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2
R1(config)# end

Figura 13. Configuración rutas estáticas predeterminadas Router R1.

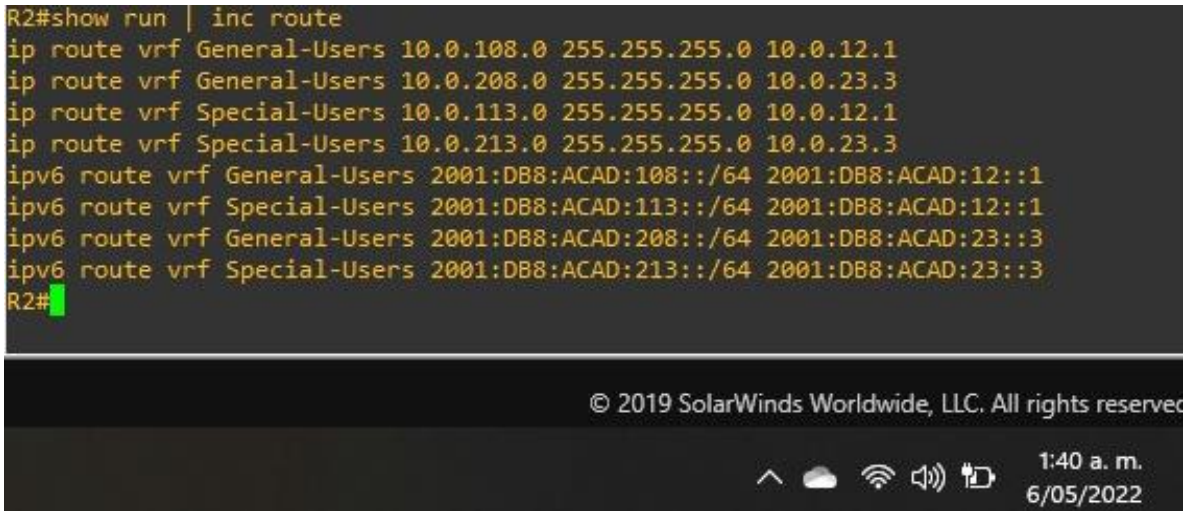


Fuente: Propia.

Router R2:

R2(config)#ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.1
R2(config)# ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.3
R2(config)#$ vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1
R2(config)#$ vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3
R2(config)# ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.1
R2(config)# ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.3
R2(config)#$ vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1
R2(config)#$ vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3
R2(config)# end

Figura 14. Configuración rutas estáticas predeterminadas Router R2.

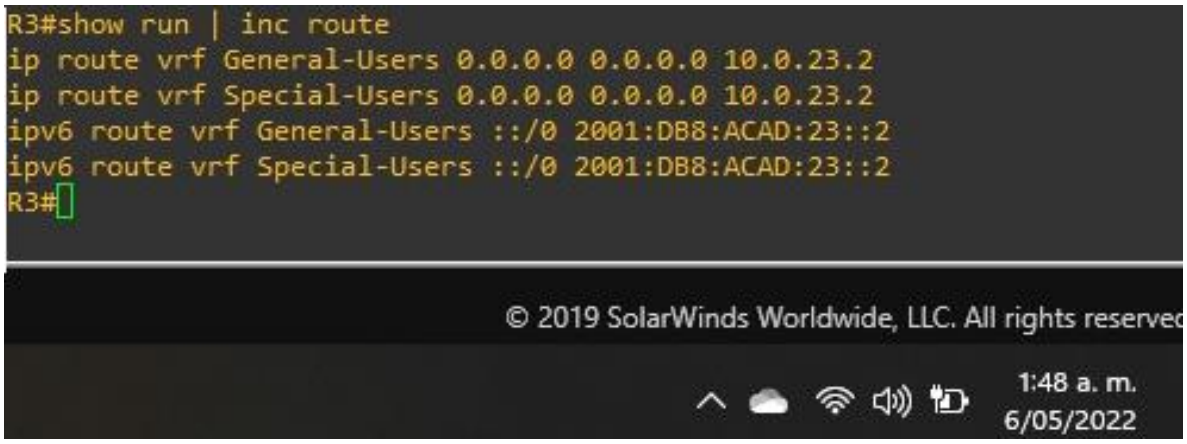


Fuente: Propia.

Router R3:

R3(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2
R3(config)# ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2
R3(config)# ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2
R3(config)# ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2
R3(config)# end

Figura 15. Configuración rutas estáticas predeterminadas Router R3.



Fuente: Propia.

Paso 2.4: Verifique la conectividad en cada VRF.

Desde el router R1 se verifica la conectividad hacia el router R3, mediante la realización de pings con las direcciones IPV4 e IPV6 asignadas:

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

Figura 16. Pruebas y verificación de conectividad entre Routers.

Fuente: Propia.

Los pings realizados desde el Router R1 hacia el Router R3, son exitosos, con lo cual se verifica el funcionamiento de las configuraciones de las VRFs y la correcta asignación de las subinterfaces generadas.

Parte 3: Configurar capa 2.

Se realiza la configuración de los switches para soportar la conectividad con los dispositivos finales de la red.

Paso 3.1: En D1, D2 y A1, deshabilite todas las interfaces.

En D1, D2 y A1, se deshabilitan las interfaces G0/0-3, G1/0-3, G2/0-3, G3/0-3.

Switch D1

D1(config)#interface range g0/0-3, g1/0-3, g2/0-3, g3/0-3 //*Rango de interfaces*
D1(config-if-range)# shutdown //*Desactiva interfaces*
D1(config-if-range)# exit

Switch D2

D2(config)#interface range g0/0-3, g1/0-3, g2/0-3, g3/0-3 //*Rango de interfaces*
D2(config-if-range)# shutdown //*Desactiva interfaces*
D2(config-if-range)# exit

Switch A1

A1(config)#interface range g0/0-3, g1/0-3, g2/0-3, g3/0-3 //*Rango de interfaces*
A1(config-if-range)# shutdown //*Desactiva interfaces*
A1(config-if-range)# exit

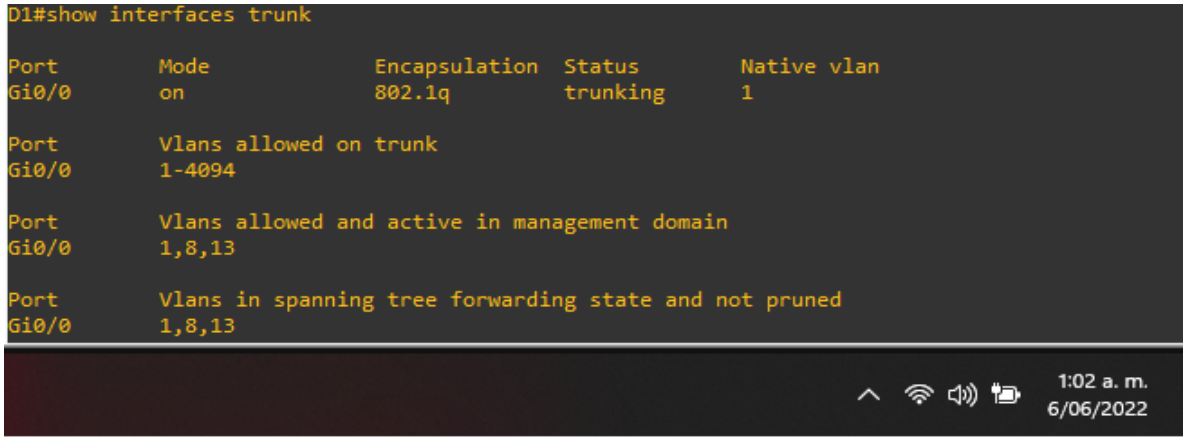
Paso 3.2: En D1 y D2 configure los enlaces troncales a R1 y R3.

En D1 y D2 se configura y habilita el enlace G0/0 como enlace troncal.

Switch D1

D1(config)#interface g0/0 //*Ingresa a la interfaz*
D1(config-if)#switchport trunk encapsulation dot1q //*Habilita encapsulación de enlace troncal*
D1(config-if)#switchport mode trunk //*Modo enlace troncal*
D1(config-if)#no shutdown //*Habilita la interfaz*
D1(config-if)#exit

Figura 17. Interfaces troncales switch D1.

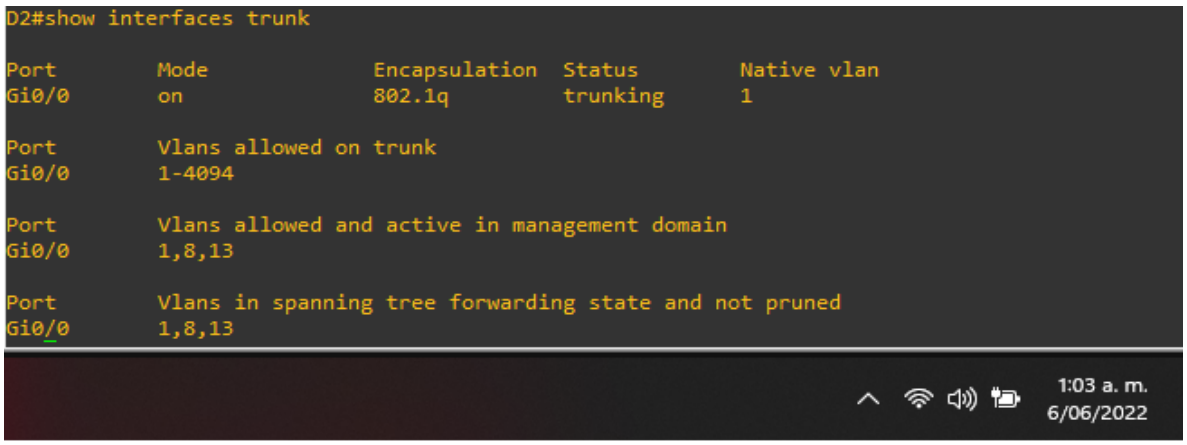


Fuente: Propia.

Switch D2

```
D2(config)#interface g0/0                          //Ingresa a la interfaz
D2(config-if)#switchport trunk encapsulation dot1q //Habilita encapsulación de enlace troncal
D2(config-if)#switchport mode trunk                //Modo enlace troncal
D2(config-if)#no shutdown                          //Habilita la interfaz
D2(config-if)#exit
```

Figura 18. Interfaces troncales switch D2.



Fuente: Propia.

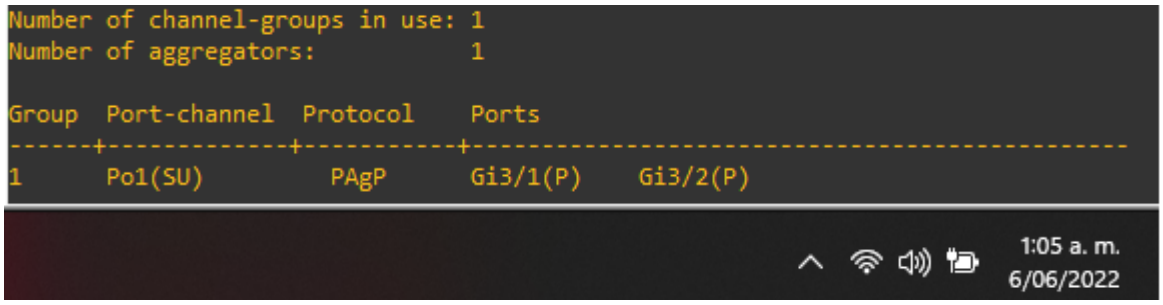
Paso 3.3: En D1 y A1, configure el EtherChannel.

En D1 y A1 se configuran y habilitan las interfaces G3/1-2 y el canal de puerto 1 usando el protocolo de agregación de puertos.

Switch D1

```
D1(config)#interface range g3/1-2                          //Rango de interfaces
D1(config-if-range)# switchport mode access                //Puerto en modo de acceso
D1(config-if-range)# switchport access vlan 8              //Asigna puerto a VLan 8
D1(config-if-range)# channel-protocol pagp                 //Protocolo PAgP
D1(config-if-range)# channel-group 1 mode desirable        //Canal en modo deseable
D1(config-if-range)# no shutdown                           //Habilita las interfaces
D1(config-if-range)# exit
```

Figura 19. Configuración EtherChannel switch D1.

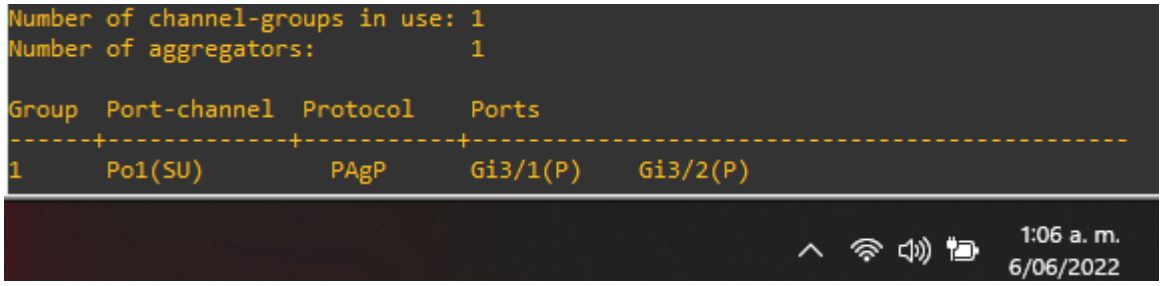


Fuente: Propia.

Switch A1

```
A1(config)#interface range g3/1-2                          //Rango de interfaces
A1(config-if-range)# switchport mode access                //Puerto en modo de acceso
A1(config-if-range)# switchport access vlan 8              //Asigna puerto a VLan 8
A1(config-if-range)# channel-protocol pagp                 //Protocolo PAgP
A1(config-if-range)# channel-group 1 mode desirable        //Canal en modo deseable
A1(config-if-range)# no shutdown                           //Habilita las interfaces
A1(config-if-range)# exit
```

Figura 20. Configuración EtherChannel switch A1.



Fuente: Propia.

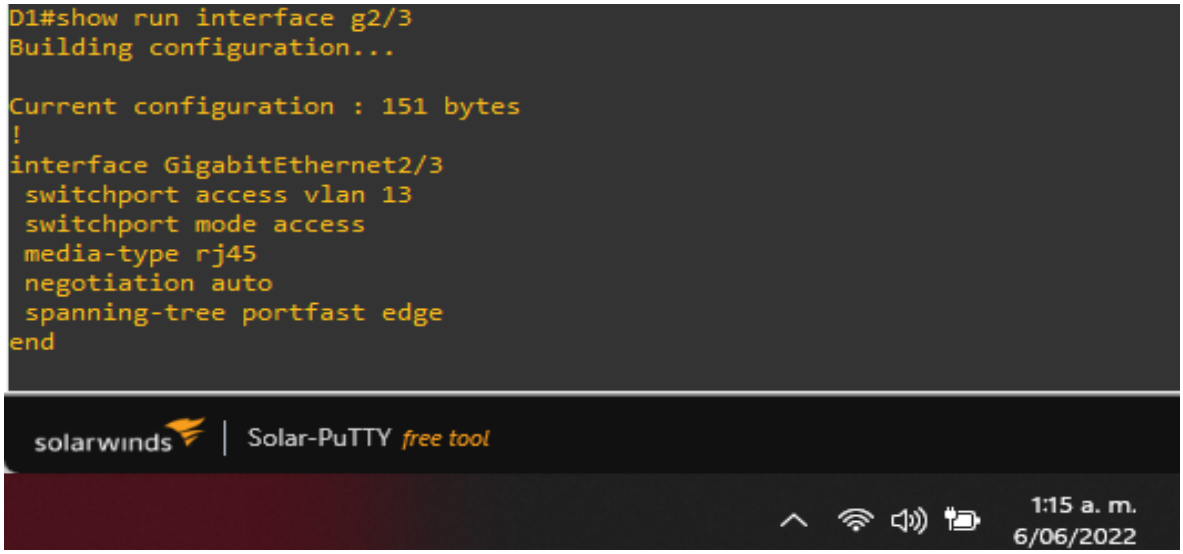
Paso 3.4: En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.

Se realiza la configuración y habilitación de los puertos de acceso en los switches teniendo en cuenta la interface utilizada y la VLan a la cual pertenece cada dispositivo final, por tanto, en D1 y D2, se configura la interface G2/3 como puerto de acceso en la Vlan 13 y se habilita el portfast, para la VLan 8, en D2 se configura la interface G2/2 como puerto de acceso, así como, la interface G2/3 en A1 y se habilita el portfast.

Switch D1

```
D1(config)#interface g2/3                  //Ingresa a la interfaz
D1(config-if)# switchport mode access      //Puerto en modo de acceso
D1(config-if)# switchport access vlan 13   //Asigna puerto a VLan 13
D1(config-if)# spanning-tree portfast      //Habilita Portfast en la interfaz
D1(config-if)# no shutdown                 //Habilita la interfaz
D1(config-if)# exit
```

Figura 21. Configuración puertos de acceso VLan 13 en switch D1.



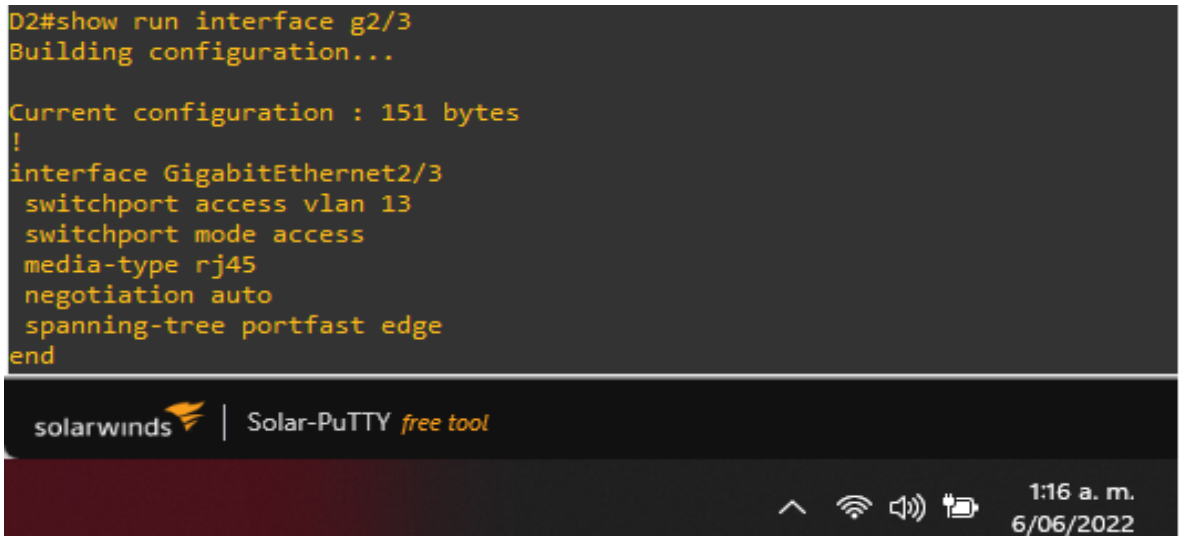
Fuente: Propia.

Switch D2

```
D2(config)#interface g2/3                  //Ingresa a la interfaz
D2(config-if)# switchport mode access      //Puerto en modo de acceso
D2(config-if)# switchport access vlan 13   //Asigna puerto a VLan 13
D2(config-if)# spanning-tree portfast      //Habilita Portfast en la interfaz
D2(config-if)# no shutdown                 //Habilita la interfaz
```

D2(config-if)# exit

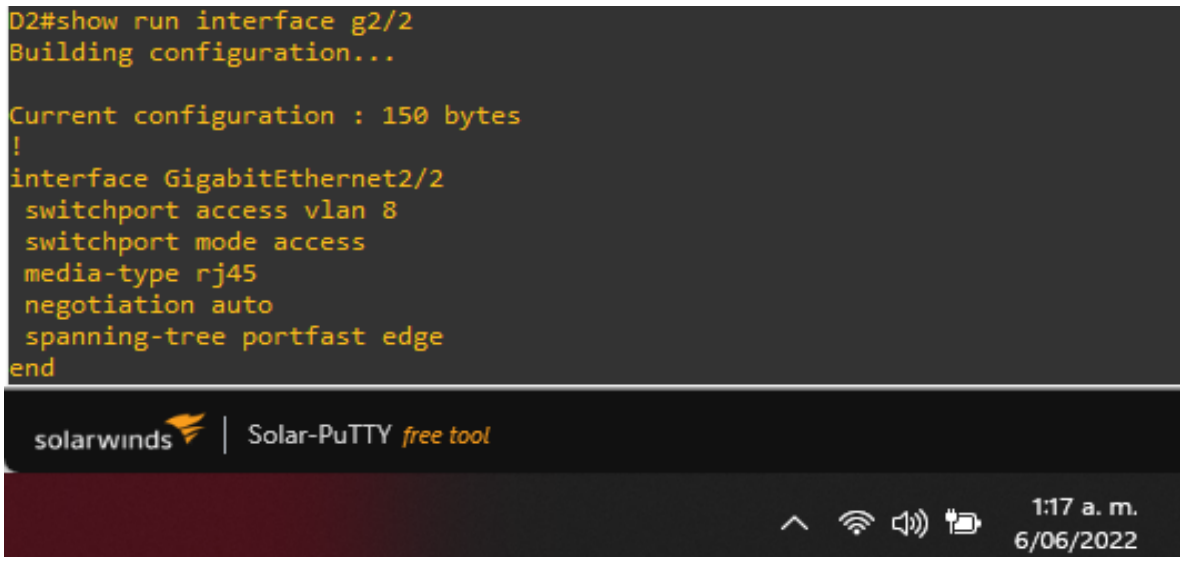
Figura 22. Configuración puertos de acceso VLan 13 en switch D2.



Fuente: Propia.

D2(config)#interface g2/2 *//Ingresa a la interfaz*
D2(config-if)# switchport mode access *//Puerto en modo de acceso*
D2(config-if)# switchport access vlan 8 *//Asigna puerto a VLan 8*
D2(config-if)# spanning-tree portfast *//Habilita Portfast en la interfaz*
D2(config-if)# no shutdown *//Habilita la interfaz*
D2(config-if)# exit

Figura 23. Configuración puertos de acceso VLan 8 en switch D2.

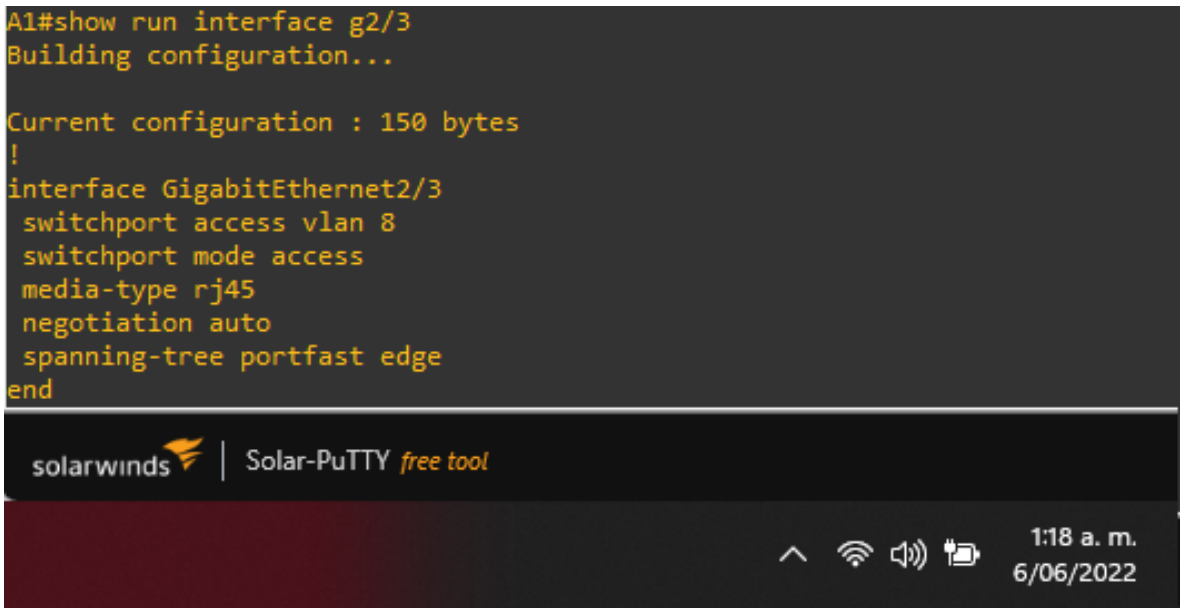


Fuente: Propia.

Switch A1

```
A1(config)#interface g2/3                    //Ingresa a la interfaz
A1(config-if)# switchport mode access        //Puerto en modo de acceso
A1(config-if)# switchport access vlan 8      //Asigna puerto a VLan 8
A1(config-if)# spanning-tree portfast        //Habilita Portfast en la interfaz
A1(config-if)# no shutdown                   //Habilita la interfaz
A1(config-if)# exit
```

Figura 24. Configuración puertos de acceso VLan 8 en switch A1.

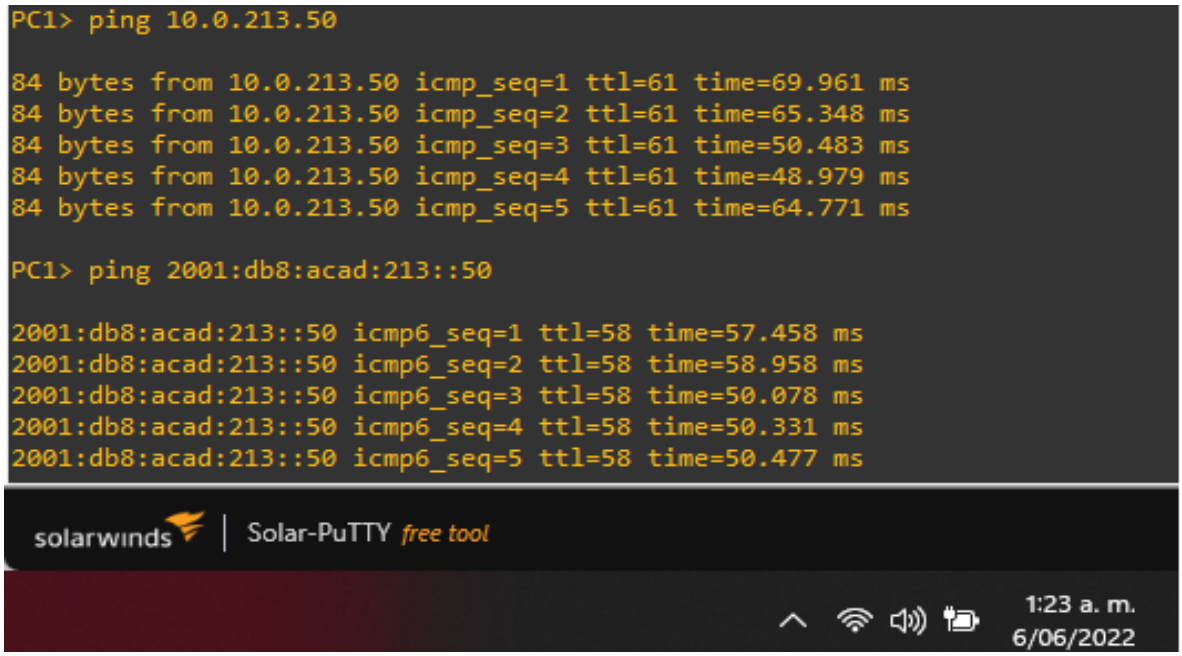


Fuente: Propia.

Paso 3.5: Verifique la conectividad de PC a PC.

Se verifica la conectividad entre equipos pertenecientes a la misma VRF (Special Users), realizando pings en IPV4 e IPV6 desde PC1 hacia PC2.

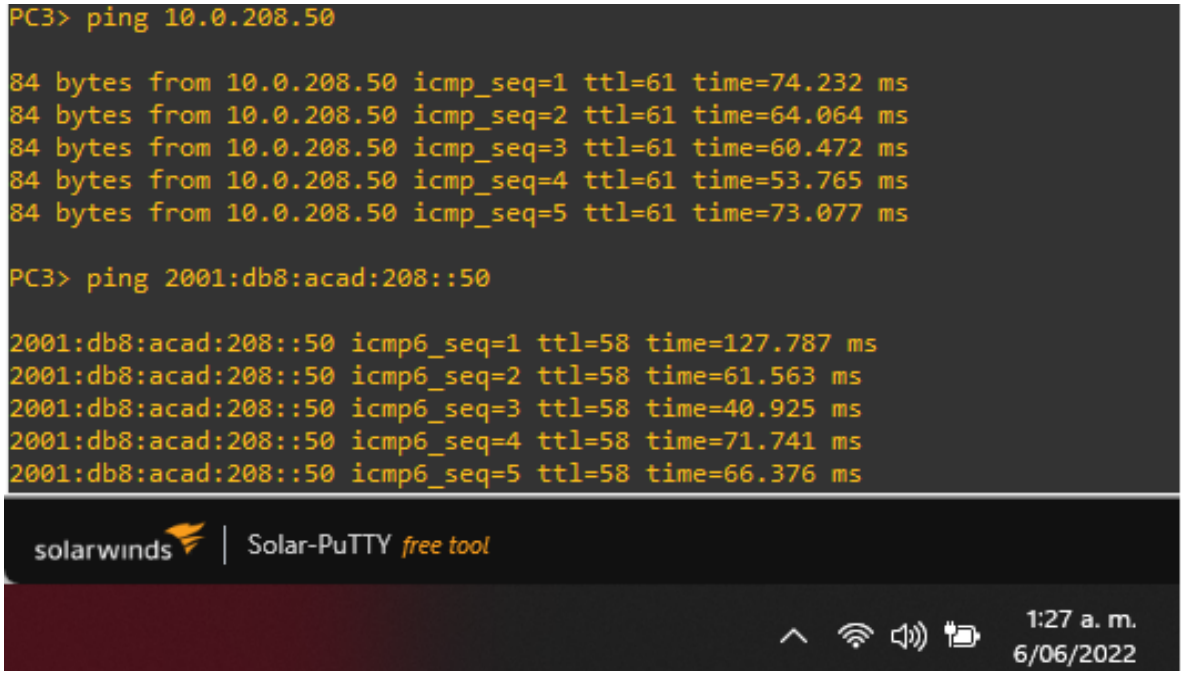
Figura 25. Pruebas y verificación de conectividad PC1 a PC2.



Fuente: Propia.

Se verifica la conectividad entre equipos pertenecientes a la misma VRF (General Users), realizando pings en IPV4 e IPV6 desde PC3 hacia PC4.

Figura 26. Pruebas y verificación de conectividad PC3 a PC4.

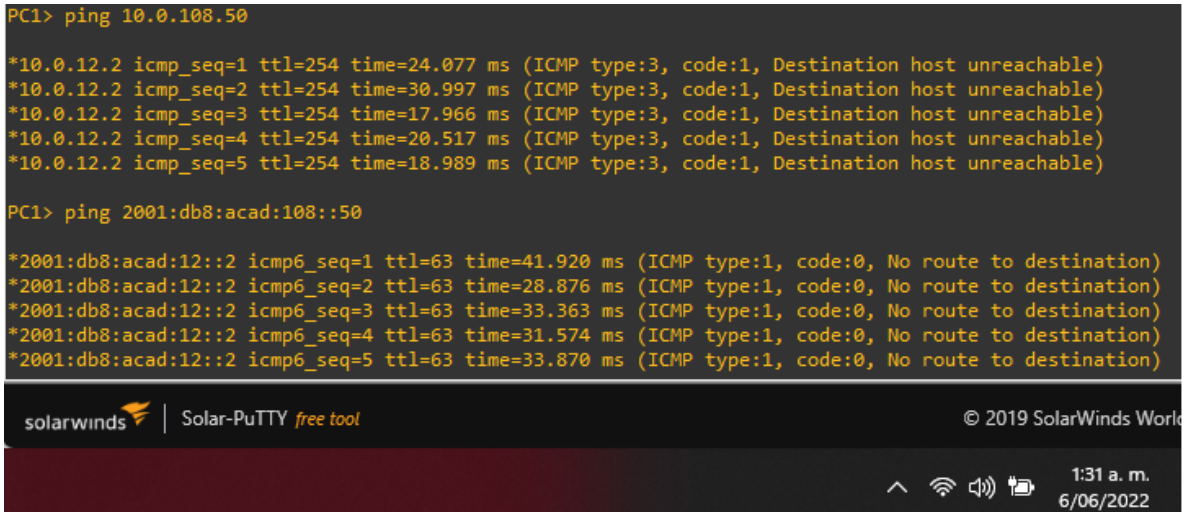


Fuente: Propia.

Los pings realizados entre los hosts pertenecientes a una misma VRF de la topología planteada, son exitosos, por tanto, las VRF configuradas, los enrutamientos estáticos en los dispositivos de capa 3 (Routers) y las configuraciones en los dispositivos de capa 2 (Switches), permiten la transmisión de datos de forma independiente en cada una de las redes.

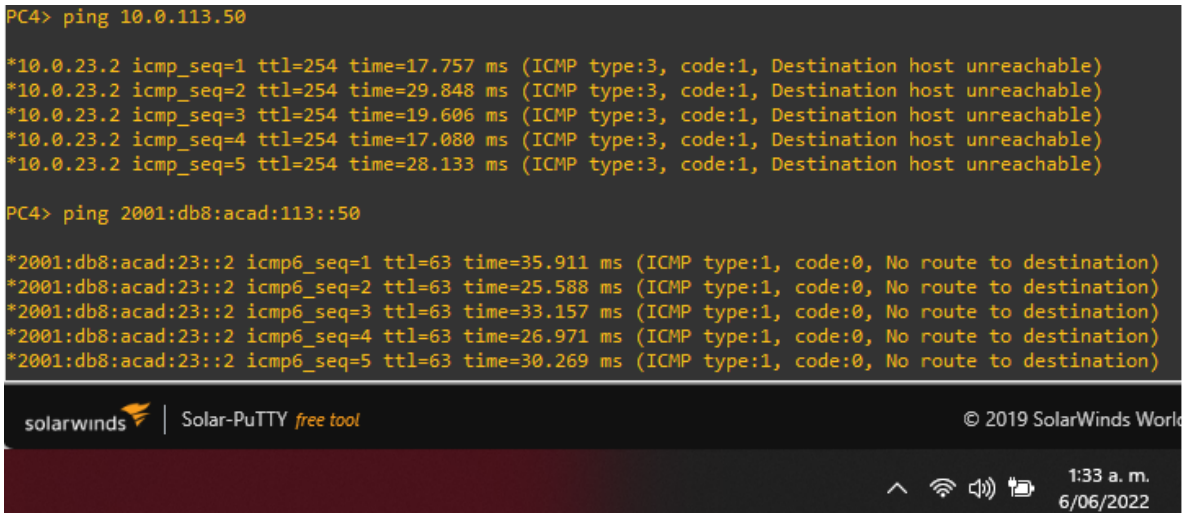
Se realizan pruebas de conectividad entre hosts pertenecientes a diferente VRF para verificar la independencia de cada red.

Figura 27. Pruebas y verificación de conectividad PC1 a PC3.



Fuente: Propia.

Figura 28. Pruebas y verificación de conectividad PC4 a PC1.



Fuente: Propia.

El tipo y código del mensaje ICPM, indica que los hosts que se encuentran en una VRF diferente no son accesibles, puesto que el Router intermedio asume que estas direcciones IP destino son inalcanzables, por tanto, los pings realizados en IPV4 e IPV6 no son exitosos y las VRF configuradas, efectivamente son independientes en funcionamiento y transmisión de datos.

Parte 4: configurar la seguridad.

Se realiza la configuración mecanismos de seguridad en los dispositivos de la topología, con lo cual se garantiza el acceso solo a los usuarios que cuenten con las credenciales establecidas.

Paso 4.1: En todos los dispositivos, asegure el modo EXEC privilegiado.

Se configura la contraseña **cisco12345cisco** para el ingreso al modo EXEC privilegiado, utilizando el algoritmo tipo **SCRYPT**.

Paso 4.2: En todos los dispositivos, cree una cuenta de usuario local.

Se configura un usuario local en cada uno de los dispositivos.

- Usuario: **admin**
- Nivel de privilegios: **15**
- Tipo de algoritmo: **SCRYPT**
- Contraseña: **cisco12345cisco**

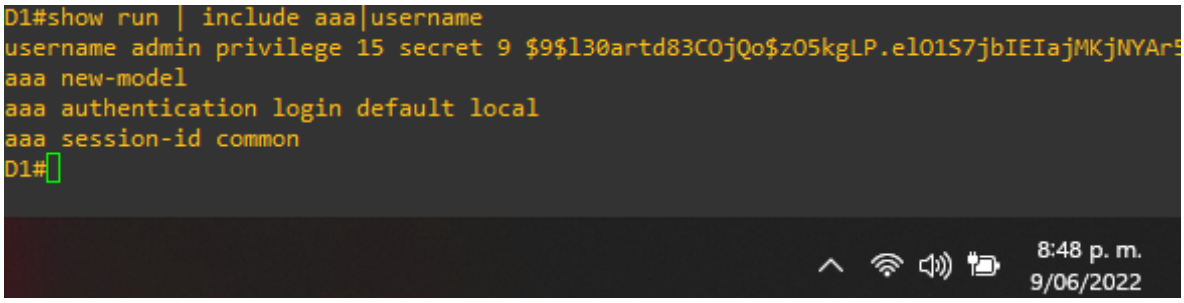
Paso 4.3: En todos los dispositivos, habilite AAA y la autenticación AAA.

Se habilita la autenticación AAA utilizando la base de datos local en todas las líneas.

Switch D1:

```
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
                                        //Habilita encriptar contraseña
D1(config)#username admin privilege 15 algorithm-type scrypt secret
cisco12345cisco                         //Creación de usuario, nivel de
privilegio y encriptación de contraseñas
D1(config)#aaa new-model                //Activa protocolos AAA
D1(config)#aaa authentication login default local   //Autenticación de inicio
D1(config)#end
```

Figura 29. Configuración de seguridad Switch D1.

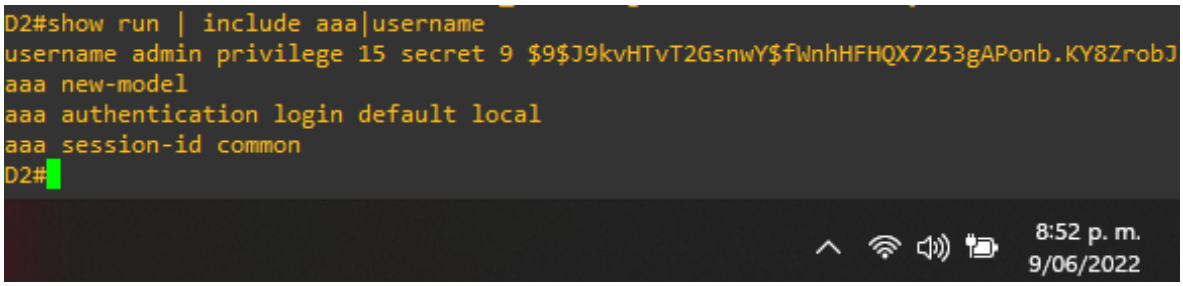


Fuente: Propia.

Switch D2:

D2(config)#enable algorithm-type scrypt secret cisco12345cisco *//Habilita encriptar contraseña*
D2(config)#username admin privilege 15 algorithm-type scrypt secret cisco12345cisco *//Creación de usuario, nivel de privilegio y encriptación de contraseñas*
D2(config)#aaa new-model *//Activa protocolos AAA*
D2(config)#aaa authentication login default local *//Autenticación de inicio*
D2(config)#end

Figura 30. Configuración de seguridad Switch D2.

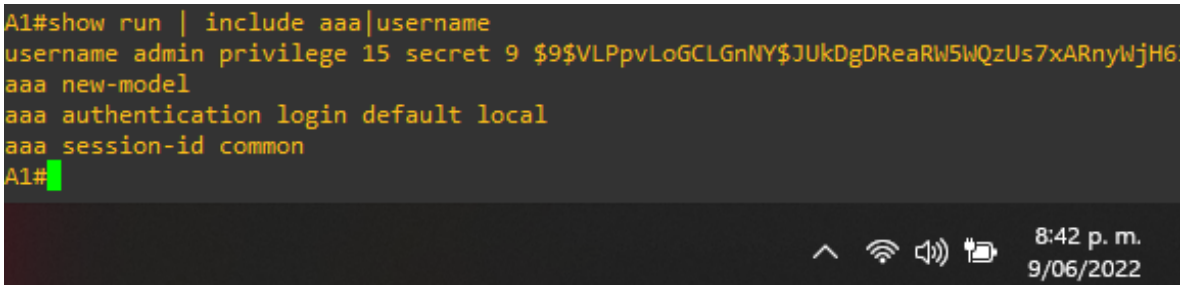


Fuente: Propia.

Switch A1:

A1(config)#enable algorithm-type scrypt secret cisco12345cisco *//Habilita encriptar contraseña*
A1(config)#username admin privilege 15 algorithm-type scrypt secret cisco12345cisco *//Creación de usuario, nivel de privilegio y encriptación de contraseñas*
A1(config)#aaa new-model *//Activa protocolos AAA*
A1(config)#aaa authentication login default local *//Autenticación de inicio*
A1(config)#end

Figura 31. Configuración de seguridad Switch A1.



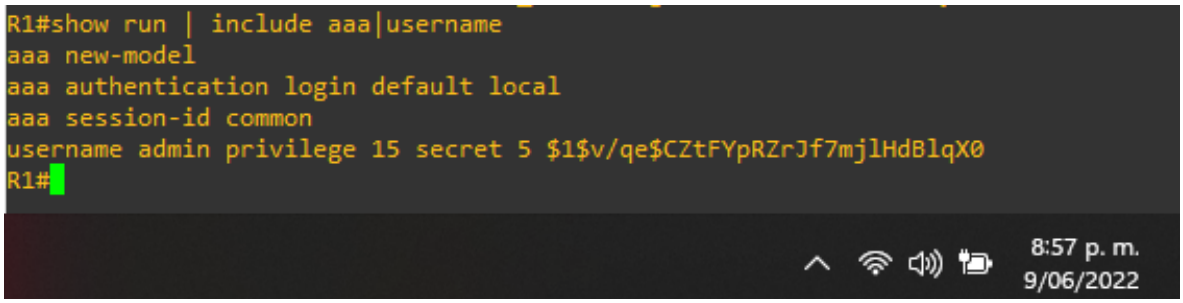
Fuente: Propia.

Para los routers R1, R2 y R3, se realiza la configuración de cuenta de usuario con contraseña secreta para el ingreso a los dispositivos, pero por configuración de la imagen en GNS3, el comando algorithm-type script no es soportado, por lo cual se realiza una configuración de alternativa de seguridad.

Router R1:

R1(config)#service password-encryption //*Encripta contraseñas*
R1(config)#enable secret cisco12345cisco //*Habilita ocultar contraseñas*
R1(config)#username admin secret 0 cisco12345cisco //*Genera usuario y contraseña*
R1(config)#username admin privilege 15 secret cisco12345cisco //*Usuario, nivel de privilegio y encripta contraseña ingresada*
R1(config)#aaa new-model //*Activa protocolos AAA*
R1(config)#aaa authentication login default local //*Autenticación de inicio*
R1(config)#end

Figura 32. Configuración de seguridad Router R1.



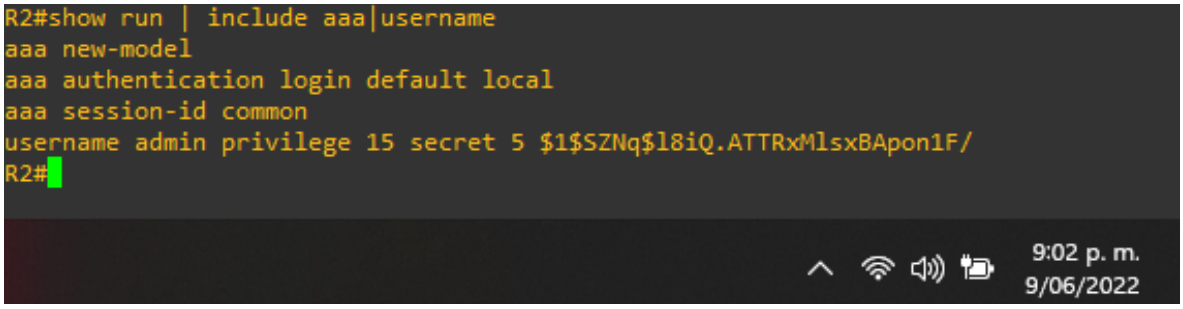
Fuente: Propia.

Router R2:

R2(config)#service password-encryption //*Encripta contraseñas*
R2(config)#enable secret cisco12345cisco //*Habilita ocultar contraseñas*

R2(config)#username admin secret 0 cisco12345cisco *//Genera usuario y contraseña*
R2(config)#username admin privilege 15 secret cisco12345cisco *//Usuario, nivel de privilegio y encripta contraseña ingresada*
R2(config)#aaa new-model *//Activa protocolos AAA*
R2(config)#aaa authentication login default local *//Autenticación de inicio*
R2(config)#end

Figura 33. Configuración de seguridad Router R2.

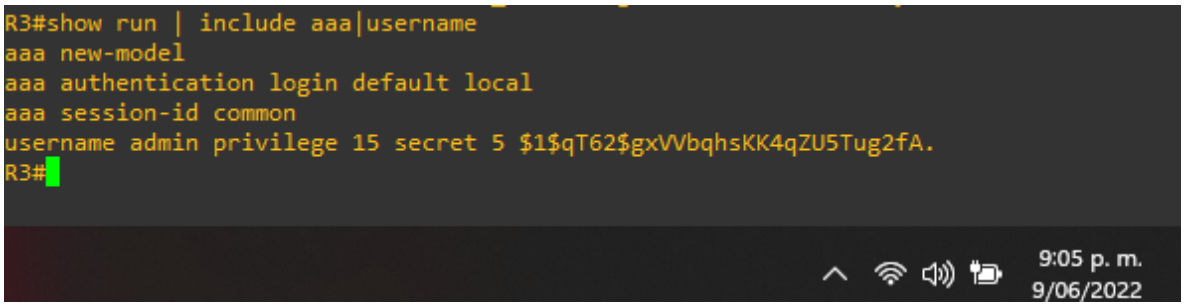


Fuente: Propia.

Router R3:

R3(config)#service password-encryption *//Encripta contraseñas*
R3(config)#enable secret cisco12345cisco *//Habilita ocultar contraseñas*
R3(config)#username admin secret 0 cisco12345cisco *//Genera usuario y contraseña*
R3(config)#username admin privilege 15 secret cisco12345cisco *//Usuario, nivel de privilegio y encripta contraseña ingresada*
R3(config)#aaa new-model *//Activa protocolos AAA*
R3(config)#aaa authentication login default local *//Autenticación de inicio*
R3(config)#end

Figura 34. Configuración de seguridad Router R3.



Fuente: Propia.

CONCLUSIONES

La configuración de las VRF dentro de la topología de red planteada, permite obtener varios routers virtuales dentro de un solo router físico, los cuales se configuran de forma independiente, asignando respectivamente una tabla de enrutamiento para cada VRF generada, permitiendo que las interfaces configuradas no entren en conflicto unas con otras, sin importar que se maneje la misma IP para dos interfaces simultáneamente, logrando así, independizar los grupos de usuarios de la red.

En el escenario propuesto se utilizan VRF lite para segmentar la topología de red, en este caso, una red empresarial en donde se busca separar dos grupos de usuarios, por tanto, se aíslan los usuarios que se encuentran en diferentes Vlans pero continúan ocupando una misma ruta para el envío y recepción de información, puesto que físicamente solo se tiene un enlace de conexión entre los equipos, de allí, la importancia de la virtualización de las conexiones para lograr la distribución y manejo sectorizado de la red, maximizando la capacidad de funcionamiento de los switches y routers.

La redundancia en las conexiones de la red, son importantes, porque permiten garantizar la conectividad de los dispositivos, puesto que, se está asegurando un enlace permanente al agruparse enlaces físicos en un solo enlace lógico, por tanto, en el EtherChannel configurado, si un enlace falla los demás asumen la carga, con la característica que es un enlace más veloz y si se presenta un cambio seria imperceptible para los usuarios finales que se están comunicando por él.

Los mecanismos de seguridad configurados en los dispositivos de conmutación y enrutamiento, permiten garantizar la accesibilidad al sistema y a las configuraciones de cada equipo, mediante asignación de usuarios, cifrado de contraseñas o niveles de privilegios, evitando así, que usuarios sin credenciales de acceso o privilegios de trabajo inicien sesión en los dispositivos, además, si es el caso, es posible realizar seguimiento mediante la revisión de registros como procedencia mediante direcciones IP o tiempos de ingreso, con lo cual, se incrementan los niveles de seguridad en los switches y los routers de la red, aprovechando protocolos de autenticación, como lo es el AAA.

Los softwares de simulación de redes como lo es el GNS3, permite realizar configuraciones en conmutadores, enrutadores, host, entre otros equipos de red, se debe tener en cuenta, la correcta instalación de la máquina virtual, el adecuado manejo y cargue de las imágenes IOS de los dispositivos y la demanda de sistema al momento de activar todos los equipos de la topología planteada, para reducir fallos y tiempos de espera en la simulación.

BIBLIOGRÁFIA

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

Edson Hernández. (2020, 14 septiembre). 01 VRF a Fondo: Implementación básica de VRF Lite. [Vídeo]. YouTube. https://www.youtube.com/watch?v=-vp6T1e4Qe4