

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHON ELKIN FLÓREZ NOVOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA -ECBTI
INGENIERIA ELECTRONICA
SOGAMOSO
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHON ELKIN FLÓREZ NOVOA

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

DIRECTOR:
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA ELECTRONICA
SOGAMOSO
2023

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Sogamoso, 4 de mayo de 2023

AGRADECIMIENTOS

Mis más sinceros agradecimientos a Dios, primeramente, familia, amigos, profesores y compañeros, por apoyarme en diferentes etapas de mi proceso académico y poder culminar un logro más en mi preparación profesional y llegar a ser un ingeniero electrónico para el servicio de la sociedad.

CONTENIDO

	Pág.
AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	7
LISTA DE FIGURAS.....	8
GLOSARIO.....	9
RESUMEN.....	10
ABSTRACT.....	11
INTRODUCCIÓN.....	12
ESCENARIO PROPUESTO	13
PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DEL DISPOSITIVO Y EL DIRECCIONAMIENTO DE LA INTERFAZ.	15
Paso 1: Cablee la red como se muestra en la topología.	15
Paso 2: Configure los ajustes básicos para cada dispositivo.....	15
PARTE 2: CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO.....	23
2.1 En R1, R2 y R3, configure VRF VRF-Lite como se muestra en el diagrama de topología.....	24
2.2 En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.	26
2.3 En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF .	31
2.4 Verifique la conectividad en cada VRF.....	33
PARTE 3. CONFIGURAR CAPA 2	38
3.1 En D1, D2, and A1, apagar las interfaces	39
3.2 En D1 y D2, configure el enlace troncal hacia R1 y R3.....	40
3.3 En D1y A1, configure EtherChannel.....	40
3.4 En D1, D2, y A1, configure los puertos de acceso para PC1, PC2, PC3, y PC4.....	41
3.5 Verifique la conectividad	42
PARTE 4. CONFIGURACION DE SEGURIDAD	46
4.1 En todos los dispositivos configurar contraseña secreta EXE mode.	46

4.2	En todos los dispositivos crear un usuario local.....	48
4.3	En todos los dispositivos configure ingreso AAA con autenticación AAA. 49	
4.4	Verificación de configuración de seguridad username y AAA.....	50
	CONCLUSIONES	53
	BIBLIOGRAFÍA.....	54

LISTA DE TABLAS

	Pag.
Tabla 1. Configuración Básica Router R1	16
Tabla 2. Parte dos configuraciones VRF y rutas estáticas	23
Tabla 3 . Configuración de dispositivos capa 2	38
Tabla 4. Tareas de configuración de seguridad.	46

LISTA DE FIGURAS

	Pag.
Figura 1. Escenario 1.	13
Figura 2. Escenario en GNS3	15
Figura 3. enrutamiento ip en todos los PC	22
Figura 4. configuración VRF en R1	33
Figura 5. configuración VRF en R2	33
Figura 6.configuración VRF en R3	34
Figura 7. Rutas estáticas en R1	34
Figura 8 .Rutas estáticas en R2	35
Figura 9. Rutas estáticas en R3	35
Figura 10. Ping a la interfaz E1/1.2 Ipv4	36
Figura 11. Ping a la interfaz E1/1.2 Ipv6	36
Figura 12. ping a la interfaz E1/1.1 Ipv4	36
Figura 13. Ping a la interfaz E1/1.1 Ipv6	37
Figura 14. conexión entre PC2 y PC4	37
Figura 15. Ping PC1 a PC2	43
Figura 16. Ping PC3 - PC4 ping 10.	43
Figura 17. Comando Interfaces Trunk en D1	44
Figura 18. comando Interfaces Trunk en D2	44
Figura 19. EtherChannel en D1	45
Figura 20. EtherChannel en A1	45
Figura 21. Username y autenticación AAA en R1	51
Figura 22. Username y autenticación AAA en R2	51
Figura 23. Username y autenticación AAA en R3	51
Figura 24. Username y autenticación AAA en D1	52
Figura 25. Username y autenticación AAA en A1	52
Figura 26. Username y autenticación AAA en D2	52

GLOSARIO

CISCO, Empresa global con sede en California, Estados Unidos que se encarga de la fabricación, y distribución de dispositivos para telecomunicaciones, estándares y protocolos para redes convergentes.

DIRECCIONAMIENTO: Son las direcciones ip en que están conectados los dispositivos, la cual una dirección de red es dividida en subredes más pequeñas, la dirección de cada dispositivo es única y está limitada a la máscara de subred.

NETWORKING. Aplicado a redes de cómputo, es el trabajo en redes de telecomunicaciones, el diseño y la construcción de una red realizado por profesionales o personas afines, hay gran cantidad de empresas que se dedican a este tipo de actividad, existe en network marketing que son las empresas que por medio de internet ofrecen productos y servicios.

ROUTER. Dispositivo que almacena la configuración de la red para conectarse con otros dispositivos en una red, contiene la información de enrutamiento, segmentación de la red y protocolos de configuración, está conectado con cableado estructurado (cable utp y fibra óptica), algunos Routers son inalámbricos permitiendo conexiones DHCP, su campo de acceso es limitado.

SWITCH O ENRUTADOR, es un dispositivo de conexión y telecomunicaciones que conecta otros switch o dispositivos finales en una red LAN. Se compone de un gran número de puertos conectados por cable utp.

VRF, Permite conectar varios dispositivos con una misma dirección de red. Y trabajar simultáneamente. Siendo redes informáticas con protocolos de enrutamiento IP, en un mismo dispositivo permite mayor integración y control de la red. Funcionan en dispositivos de capa 3 (Routers)

RESUMEN

En este trabajo se da solución a un escenario, se realiza una propuesta en donde se crea una red que contiene dos tipos de usuarios que dividen la red. Para un mejor uso del direccionamiento de la red, se implementa una técnica de enrutamiento VRF que permita usar una misma dirección en dos interfaces diferentes en un mismo dispositivo Routers.

Se configura la tecnología VRF en los tres Routers según la topología de red, se selecciona un enrutamiento estático que permita la accesibilidad de la red con una conectividad de extremo a extremo.

Este trabajo se compone de cuatro partes, la primera es la configuración básica de la red, la segunda es configurar VRF y las rutas estáticas, el tercer paso es la configuración de la capa 2 (adecuación del switch) y el último paso es la configuración de la seguridad de la red, al finalizar la conectividad de los dispositivos se podrá comunicar los host finales de las diferentes LAN.

Los grupos de los usuarios generales y los usuarios especiales no tendrán conectividad entre ellos, este escenario es común en las redes LAN empresariales que buscan tener más beneficios y menos costos en la implementación y ejecución de las redes de datos LAN o WAN.

Para realizar este trabajo se investigó en fuentes referenciadas de artículos científicos, en E-biblioteca y en las referencias del curso.

Palabras clave: cisco, CCNP, Electrónica, Redes, Router, Switch,

ABSTRACT

In this work, a solution to a scenario is given, a proposal is made where a network is created that contains two types of users that divide the network. For better use of network addressing, a VRF routing technique is implemented that allows the use of the same address on two different interfaces on the same router device.

The VRF technology is configured in the three Routers according to the network topology, a static routing is selected that allows the accessibility of the network with end-to-end connectivity.

This work is made up of four parts, the first is the basic configuration of the network, the second is to configure VRF and static routes, the third step is the configuration of layer 2 (suitability of the switches) and the last step is the configuration of the network security, at the end of the connectivity of the devices it will be possible to communicate the final hosts of the different LANs.

The groups of general users and special users will not have connectivity between them, this scenario is common in business LANs that seek to have more benefits and less costs in the implementation and execution of LAN or WAN data networks. To carry out this work, I investigated in referenced sources of scientific articles, in the E-library and in the references of the course.

Keywords: cisco, CCNP, Electronic, networking, routing, switching,

INTRODUCCIÓN

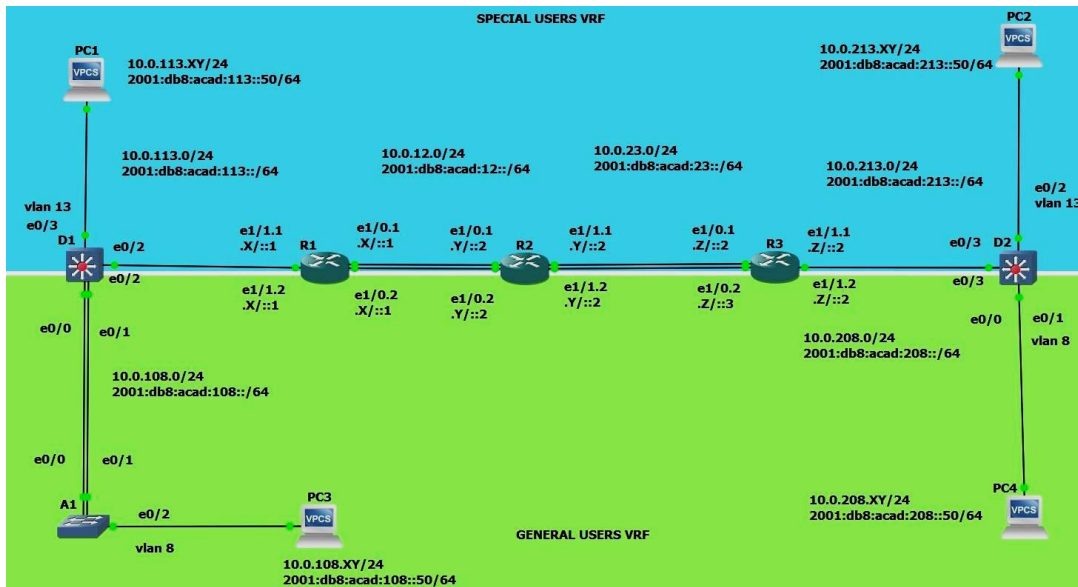
Este informe corresponde a la actividad final del diplomado de profundización de cisco CCNP , en donde se estructura un escenario de red en donde se implementan protocolos de enrutamiento ipv4 e ipv6, protocolos STP , configuración de Routers, switch y dispositivos finales o host, la creación de vlan en una red convergente.

Se diseña una red escalable, la configuración básica de los dispositivos de la red, la implementación de protocolos VRF, y dos usuarios que no se conectan y su tabla de enrutamiento es independiente.

El uso de softwares especializados para la creación y configuración de redes donde se establezcan los dispositivos y diferentes comandos se ha seleccionado GNS3 que permite las configuraciones avanzadas de este tipo de redes, el escenario 1 propuesto hace semejanza a un escenario común entre redes convergentes empresariales

ESCENARIO PROPUESTO

Figura 1. Escenario 1.



Fuente: Guía Prueba de Habilidades escenario CCNP

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. Para el desarrollo de la actividad, se tomarán los valores de la tabla de direccionamiento.

Con base al escenario propuesto, se realiza un diseño de red con una configuración multi VRF con los dos escenarios cada uno con su direccionamiento y configuraciones básicas

TABLA DE DIRECCIONAMIENTO

Tabla 1.Tabla de direccionamiento.

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.6/24	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	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.3/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.3/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.16/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.16/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.16/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.16/24	2001:db8:acad:208::50/64	EUI-64

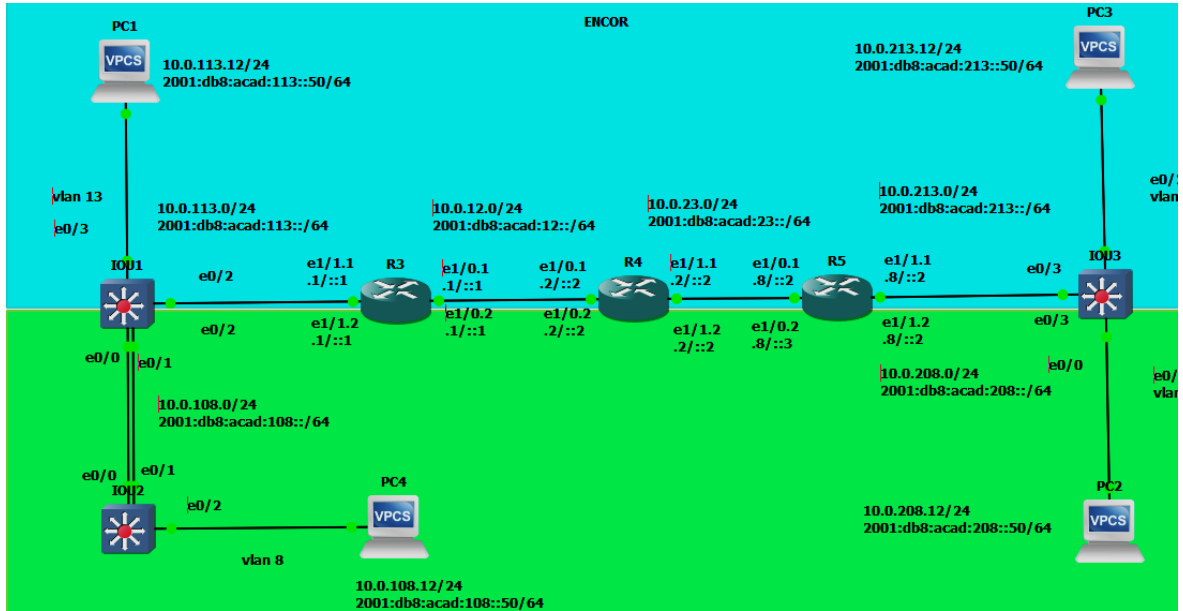
Fuente: Documento guía de escenario CCNP

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

En la Parte 1, configurará la topología de la red y configurará los ajustes básicos.

Paso 1: Cablee la red como se muestra en la topología.

Figura 2. Escenario en GNS3



Fuente: Escenario simulado en GNS3

Objetivos

Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

Parte 2: Configurar VRF y rutas estáticas.

Parte 3: Configurar Capa 2

Parte 4: Configurar seguridad

Paso 2: Configure los ajustes básicos para cada dispositivo.

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

Configuración básica en R1

CODIGO	DESCRIPCION
Enable	Ingresa a modo global del dispositivo.
Configure terminal hostname R1	Ingresa al modo de configuración Se le configura el nombre al dispositivo con el que se identifica en la red
ipv6 unicast-routing	Habilita la interfaz para protocolo de enrutamiento ipv6.
no ip domain lookup	Desactiva la búsqueda de DNS.
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #	Escribe el mensaje del día que se muestra al iniciar el dispositivo, es un aviso.
line con 0 exec-timeout 0 0	Ingresa a la interface de consola Estima el tiempo de espera de 0 segundos.
logging synchronous	Sincroniza los mensajes, contraseñas y demás en el registro syslo.
exit	Salida de la interfaz

Configuración básica en R2

CODIGO	DESCRIPCION
Enable	Ingresa a modo global del dispositivo.
Configure terminal hostname R2	Ingresa al modo de configuración Se le configura el nombre al dispositivo con el que se identifica en la red
ipv6 unicast-routing	Habilita la interfaz para protocolo de enrutamiento ipv6.
no ip domain lookup	Desactiva la búsqueda de DNS.
banner motd # R2, ENCOR SkillsAssessment, Scenario 2 #	Escribe el mensaje del día que se muestra al iniciar el dispositivo, es un aviso.
line con 0 exec-timeout 0 0	Ingresa a la interface de consola Estima el tiempo de espera de 0

logging synchronous	segundos. Sincroniza los mensajes, contraseñas y demás en el registro syslo.
exit	Sale de la interfaz

Configuración básica e n R3

CODIGO	DESCRIPCION
Enable	Ingresa a modo global del dispositivo.
Configure terminal	Ingresa al modo de configuración
hostname R3	Se le configura el nombre al dispositivo con el que se identifica en la red
ipv6 unicast-routing	Habilita la interfaz para protocolo de enrutamiento ipv6.
no ip domain lookup	Desactiva la búsqueda de DNS.
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #	Escribe el mensaje del día que se muestra al iniciar el dispositivo, es un aviso.
line con 0	Ingresa a la interface de consola
exec-timeout 0 0	Estima el tiempo de espera de 0 segundos.
logging synchronous	Sincroniza los mensajes, contraseñas y demás en el registro syslo.
exit	Sale de la interfaz

Configuración básica e n D1

CODIGO	DESCRIPCION
Enable	Ingresa a modo global del dispositivo.
Configure terminal	Ingresa al modo de configuración
hostname D1	Se le configura el nombre al dispositivo con el que se identifica en la red

ipv6 unicast-routing	Habilita la interfaz para protocolo de enrutamiento ipv6.
no ip domain lookup	Desactiva la búsqueda de DNS.
banner motd # D1, ENCOR SkillsAssessment, Scenario 2 #	Escribe el mensaje del día que se muestra al iniciar el dispositivo, es un aviso.
line con 0	Ingresa a la interface de consola
exec-timeout 0 0	Estima el tiempo de espera de 0 segundos.
logging synchronous	Sincroniza los mensajes, contraseñas y demás en el registro syslog.
exit	Sale de la interfaz
vlan 8	Crea la vlan 8
name General-Users	Adiciona la vlan al usuario General-Users
Exit	Sale de la interfaz
vlan 13	Crea la vlan 13
name Special-Users	Adiciona a la vlan el usuario Special-Users
Exit	Sale de la interfaz

Configuración básica en D2

CODIGO	DESCRIPCION
Enable	Ingresa a modo global del dispositivo.
Configure terminal	Ingresa al modo de configuración
hostname D2	Se le configura el nombre al dispositivo con el que se identifica en la red
ipv6 unicast-routing	Habilita la interfaz para protocolo de enrutamiento ipv6.
no ip domain lookup	Desactiva la búsqueda de DNS.

banner motd # D2, ENCOR SkillsAssessment, Scenario 2 #	Escribe el mensaje del día que se muestra al iniciar el dispositivo, es unaviso.
line con 0	Ingresa a la interface de consola
exec-timeout 0 0	Estima el tiempo de espera de 0segundos.
logging synchronous	Sincroniza los mensajes, contraseñas ydemás en el registro syslo.
exit	Sale de la interfaz
vlan 8	Crea la vlan 8
name General-Users	Adiciona la vlan al usuario General- Users
Exit	Sale de la interfaz
vlan 13	Crea la vlan 13
name Special-Users	Adiciona a la vlan el usuario Special- Users
Exit	Sale de la interfaz

Configuración básica e n A1

CODIGO	DESCRIPCION
Enable	Ingresa a modo global del dispositivo.
Configure terminal	Ingresa al modo de configuración
hostname A1	Se le configura el nombre al dispositivocon el que se identifica en la red
ipv6 unicast-routing	Habilita la interfaz para protocolo deenrutamiento ipv6.
no Ip domain lookup	Desactiva la búsqueda de DNS.
banner motd # A1, ENCOR SkillsAssessment, Scenario 2 #	Escribe el mensaje del día que se muestra al iniciar el dispositivo, es unaviso.

line con 0	Ingresa a la interface de consola
exec-timeout 0 0	Estima el tiempo de espera de 0segundos.
logging synchronous	Sincroniza los mensajes, contraseñas ydemás en el registro syslo.
exit	Sale de la interfaz
vlan 8	Crea la vlan 8
name General-Users	Adiciona la vlan al usuario General- Users
Exit	Sale de la interfaz

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

Configuración en R1

R1#copy run star	Guarda la configuración en la
Destination filename	NVRAM del dispositivo.
[startup- config]?	
Building configuration...	
[OK]	

Configuración en R2

R2#copy run star	Guarda la configuración en la
Destination filename	NVRAM del dispositivo.
[startup- config]?	
Building configuration...	
[OK]	

Configuración en R3

R3#copy run star	Guarda la configuración en la
Destination filename	NVRAM del dispositivo.
[startup- config]?	
Building configuration...	
[OK]	

Configuración en D1

D1#copy run star	Guarda la configuración en la
Destination filename	NVRAM del dispositivo.
[startup- config]?	
Building configuration...	
[OK]	

D2#copy run star
Destination filename
[startup- config]?
Building configuration...
[OK]

Configuración en D2
Guarda la configuración en la
NVRAM del dispositivo.

A1#copy run star
Destination filename
[startup- config]?
Building configuration...
[OK]

Configuración en A1
Guarda la configuración en la
NVRAM del dispositivo.

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

Configuración protocolo
Ipv6 e Ipv4 de la tabla de
direccionamiento en PC1,

PC1> ip 10.0.113.16/24 10.0.113.1
PC1> ip 2001:db8:acad:113::50/64

Configuración protocolo
Ipv6 e Ipv4 de la tabla de
direccionamiento en PC2,

PC2> ip 10.0.213.16/24 10.0.213.3
PC2> ip 201:db8:acad:213::50/54

Configuración protocolo
Ipv6 e Ipv4 de la tabla de
direccionamiento en PC3,

PC3> ip 10.0.108.16/24 10.0.108.1
PC3> ip 2001:db8:acad:108::50/64

Configuración protocolo
Ipv6 e Ipv4 de la tabla de
direccionamiento en PC4,

PC4> ip 10.0.208.16/24 10.0.208.3
PC4> ip 2001:db8:acad:208::50/64

Verificar configuración de PCs

comando Show

Figura 3. enrutamiento ip en todos los PC

```
PC1> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.0.113.16/24 10.0.113.1 00:50:79:66:68:00 10004 127.0.0.1:10005
fe80::250:79ff:fe66:6800/64
2001:db8:acad:113::50/64
PC1>
```

```
PC2> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.213.16/24 10.0.213.3 00:50:79:66:68:01 10008 127.0.0.1:10009
fe80::250:79ff:fe66:6801/64
201:db8:acad:213::50/54
PC2>
```

```
PC3> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.108.16/24 10.0.108.1 00:50:79:66:68:02 10006 127.0.0.1:10007
fe80::250:79ff:fe66:6802/64
2001:db8:acad:108::50/64
PC3>
```

```
PC4> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.0.208.16/24 10.0.208.3 00:50:79:66:68:03 10010 127.0.0.1:10011
fe80::250:79ff:fe66:6803/64
2001:db8:acad:208::50/64
PC4>
```

Fuente: escenario simulación GNS3

PARTE 2: CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO

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

Sus tareas de configuración son las siguientes:

Tabla 2. Parte dos configuraciones VRF y rutas estáticas

Tarea #	Tarea	Especificación
2.1	En R1, R2 y R3, configure VRF VRF-Lite como se muestra en el diagrama de topología.	Configure dos VRF: Usuarios generales Usuarios especiales Los VRF deben admitir IPv4 e IPv6.
2.2	En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.	Todos los Routers utilizarán Reuter-En-A-Stick en sus interfaces G0/0/1.x para admitir la separación de los VRF. Subinterfaz 1: En el VRF de usuarios especiales Usar encapsulación dot1q 13 IPv4 e IPv6 GUA y direcciones locales de enlace Habilitar las interfaces Subinterfaz 2: En el VRF de usuarios generales Usar encapsulación dot1q 8 IPv4 e IPv6 GUA y direcciones locales de enlace Habilitar las interfaces
2.3	En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.	Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.
2.4	Verifique la conectividad en cada VRF.	Desde R1, verifique la conectividad con R3: ping VRF General-Usuarios 10.0.208.Z ping VRF General-Users

		2001:db8:acad:208::1 ping VRF Special-Users 10.0.213.Z ping VRF Special-Users 2001:db8:acad:213::1
--	--	---

Fuente: Documento Guía de Habilidades Practicas CCNP

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

Configure dos VRF:
 Usuarios generales
 Usuarios especiales

Los VRF deben admitir IPv4 e IPv6

CONFIGURACION VRF EN R1

CODIGO	DESCRIPCION
enable	Ingresar a modo global.
Configure terminal	Ingresar al modo de configuración
vrf definition Special-Users	crea la VRF Special-Users.
description Special-Users	Crea una descripción en la interfaz VRF Special-Users
address-family ipv4	Habilita familia de direcciones IPV4
exit	Sale de la interfaz
description Special-Users	Describe la VRF como Special Users
address-family ipv6	Habilita familia de direcciones IPV6
exit	Sale de la interfaz
vrf definition General-Users	Crea la VRF General-Users.
description General-Users	Crea una descripción en la interfaz la VRF General-Users
address-family ipv4	Habilita familia de direcciones IPV4
exit	Sale de la interfaz
description General-Users	Describe la VRF como General-Users
address-family ipv6	Habilita familia de direcciones IPV6
Exit	Sale de la interfaz

CONFIGURACION VRF EN R2

CODIGO	DESCRIPCION
enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuraci3n
vrf definition Special-Users	crea la VRF Special-Users.
description Special-Users	Crea una descripci3n en la interfaz VRF Special-Users
address-family ipv4	Habilita familia de direcciones IPV4
exit	Sale de la interfaz
description Special-Users	Describe la VRF como Special Users
address-family ipv6	Habilita familia de direcciones IPV6
exit	Sale de la interfaz
vrf definition General-Users	Crea la VRF General-Users.
description General-Users	Crea una descripci3n en la interfaz la VRF General-Users
address-family ipv4	Habilita familia de direcciones IPV4
exit	Sale de la interfaz
description General-Users	Describe la VRF como General-Users
address-family ipv6	Habilita familia de direcciones IPV6
Exit	Sale de la interfaz

CONFIGURACION VRF EN R3

CODIGO	DESCRIPCION
enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuraci3n
vrf definition Special-Users	crea la VRF Special-Users.
description Special-Users	Crea una descripci3n en la interfaz VRF Special-Users
address-family ipv4	Habilita familia de direcciones IPV4
exit	Sale de la interfaz
description Special-Users	Describe la VRF como Special Users
address-family ipv6	Habilita familia de direcciones IPV6
exit	Sale de la interfaz
vrf definition General-Users	Crea la VRF General-Users.
description General-Users	Crea una descripci3n en la interfaz la VRF General-Users
address-family ipv4	Habilita familia de direcciones IPV4
exit	Sale de la interfaz

description General-Users	Describe la VRF como General-Users
address-family ipv6	Habilita familia de direcciones IPV6
Exit	Salida de la interfaz

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

Descripción

Todos los Routers utilizarán Router-En-A-Stick en sus interfaces G0/0/1.x para admitir la separación de los VRF.

Subinterfaz 1:

En el VRF de usuarios especiales

- Usar encapsulación dot1q 13
- IPv4 e IPv6 GUA y direcciones locales de enlace
- Habilitar las interfaces

Subinterfaz 2:

En el VRF de usuarios generales

- Usar encapsulación dot1q 8
- IPv4 e IPv6 GUA y direcciones locales de enlace

Habilitar las interfaces

Configuración de interfaces Ipv4 e Ipv6 VRF en R1

	ROUTER R1
Código	Descripción
enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface e1/0.1	Crea una subinterfaz
encapsulation dot1q 13	Código de encapsulación 802.1Q VLAN 13.
vrf forward Special-Users	Activa el VRF de Special-Users
ip address 10.0.12.1 255.255.255.0	Ingresa la dirección ip y la máscara de subred ipv4.
ipv6 address fe80::1:1 link- local	Ingresa la dirección de enlace local ipv6
ipv6 address 2001:db8:acad:12::1/64	Ingresa la dirección ipv6
no shutdown	Enciende la interfaz

```
exit
interface e1/0.2
encapsulation dot1q 8
vrf forward General-Users
ip address 10.0.12.1
255.255.255.0
ipv6 address fe80::1:2 link-
local
ipv6 address
2001:db8:acad:12::1/64
no shutdown
exit
```

```
interface e1/0
no ip address
no shutdown
exit
```

```
interface e1/1.1
encapsulation dot1q 13
vrf forward Special-Users
ip address 10.0.113.1
255.255.255.0
ipv6 address fe80::1:3 link-
local
ipv6 address
2001:db8:acad:113::1/64
no shutdown
exit
```

```
interface e1/1.2
encapsulation dot1q 8
vrf forward General-Users
ip address 10.0.108.1
255.255.255.0
ipv6 address fe80::1:4 link-
local
ipv6 address
2001:db8:acad:108::1/64
```

Sale de la interfaz
Crea una subinterfaz
Código de encapsulación 802.1Q
VLAN 8.
activa VRF de General-Users
Ingresa la dirección ip y la máscara de
subred ipv4
Ingresa la dirección de enlace local ipv6
Ingresa la dirección ipv6
Enciende la interfaz
Sale de la interfaz

Ingresa a la interface
No configura dirección en la interface
Enciende la interfaz
Sale de la interfaz
Sale de la interfaz
Código de encapsulación 802.1Q
VLAN 13.
Activa el VRF de Special-Users
Ingresa la dirección ip y la máscara de
subred ipv4.
Ingresa la dirección de enlace local ipv6
Ingresa la dirección ipv6

Enciende la interfaz
Sale de la interfaz
Sale de la interfaz
Código de encapsulación 802.1Q
VLAN 8.
activa VRF de General-Users
Ingresa la dirección ip y la máscara de
subred ipv4.
Ingresa la dirección de enlace local ipv6
Ingresa la dirección ipv6

no shutdown	Enciende la interfaz
exit	Salida de la interfaz
interface e1/1	Ingresa a la interfaz
no ip address	No configura dirección en la interfaz
no shutdown	Enciende la interfaz
exit	Salida de la interfaz

Configuración de interfaces Ipv4 e Ipv6 VRF en R2

Código	Descripción
enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface e1/0.1	Crea una subinterfaz
encapsulation dot1q 13	Código de encapsulación 802.1Q VLAN 13.
vrf forward Special-Users	Activa el VRF de Special-Users
ip address 10.0.12.6 255.255.255.0	Ingresa la dirección ip y la máscara de subred ipv4.
ipv6 address fe80::2:1 link- local	Ingresa la dirección de enlace local ipv6
ipv6 address 2001:db8:acad:12::2/64	Ingresa la dirección ipv6
no shutdown	Enciende la interfaz
exit	Salida de la interfaz
interface e1/0.2	Crea una subinterfaz
encapsulation dot1q 8	Código de encapsulación 802.1Q VLAN 8.
vrf forward General-Users	activa VRF de General-Users
ip address 10.0.12.6 255.255.255.0	Ingresa la dirección ip y la máscara de subred ipv4
ipv6 address fe80::2:2 link- local	Ingresa la dirección de enlace local ipv6
ipv6 address 2001:db8:acad:12::2/64	Ingresa la dirección ipv6
no shutdown	Enciende la interfaz
exit	Salida de la interfaz
interface e1/0	Ingresa a la interfaz

no ip address	No configura dirección en la interface
no shutdown	Enciende la interfaz
exit	Salida de la interfaz
interface e1/1.1	Salida de la interfaz
encapsulation dot1q 13	Código de encapsulación 802.1Q VLAN 13.
vrf forward Special-Users	Activa el VRF de Special-Users
ip address 10.0.23.6 255.255.255.0	Ingresa la dirección ip y la máscara de subred ipv4.
ipv6 address fe80::2:3 link- local	Ingresa la dirección de enlace local ipv6
ipv6 address 2001:db8:acad:23::2/64	Ingresa la dirección ipv6
no shutdown	Enciende la interfaz
exit	Salida de la interfaz
interface e1/1.2	Salida de la interfaz
encapsulation dot1q 8	Código de encapsulación 802.1Q VLAN 8.
vrf forward General-Users	activa VRF de General-Users
ip address 10.0.23.6 255.255.255.0	Ingresa la dirección ip y la máscara de subred ipv4.
ipv6 address fe80::2:4 link- local	Ingresa la dirección de enlace local ipv6
ipv6 address 2001:db8:acad:23::2/64	Ingresa la dirección ipv6
no shutdown	Enciende la interfaz
exit	Salida de la interfaz
interface e1/1	Ingresa a la interface
no ip address	No configura dirección en la interface
no shutdown	Enciende la interfaz
exit	Salida de la interfaz

Configuración de interfaces Ipv4 e Ipv6 VRF en R3

ROUTER R3

Código	Descripción
enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface e1/0.1	Crea una subinterfaz

<pre> encapsulation dot1q 13 vrf forward Special-Users ip address 10.0.23.3 255.255.255.0 ipv6 address fe80::3:1 link- local ipv6 address 2001:db8:acad:23::3/64 no shutdown exit interface e1/0.2 encapsulation dot1q 8 vrf forward General-Users ip address 10.0.23.3 255.255.255.0 ipv6 address fe80::3:2 link- local ipv6 address 2001:db8:acad:23::3/64 no shutdown exit interface e1/0 no ip address no shutdown exit interface e1/1.1 encapsulation dot1q 13 vrf forward Special-Users ip address 10.0.213.3 255.255.255.0 ipv6 address fe80::3:3 link- local ipv6 address 2001:db8:acad:213::1/64 no shutdown exit interface e1/1.2 </pre>	<p>Código de encapsulación 802.1Q VLAN 13.</p> <p>Activa el VRF de Special-Users</p> <p>Ingresar la dirección ip y la máscara de subred ipv4.</p> <p>Ingresar la dirección de enlace local ipv6</p> <p>Ingresar la dirección ipv6</p> <p>Enciende la interfaz</p> <p>Sale de la interfaz</p> <p>Crea una subinterfaz</p> <p>Código de encapsulación 802.1Q VLAN 8.</p> <p>activa VRF de General-Users</p> <p>Ingresar la dirección ip y la máscara de subred ipv4</p> <p>Ingresar la dirección de enlace local ipv6</p> <p>Ingresar la dirección ipv6</p> <p>Enciende la interfaz</p> <p>Sale de la interfaz</p> <p>Ingresar a la interface</p> <p>No configura dirección en la interface</p> <p>Enciende la interfaz</p> <p>Sale de la interfaz</p> <p>Sale de la interfaz</p> <p>Código de encapsulación 802.1Q VLAN 13.</p> <p>Activa el VRF de Special-Users</p> <p>Ingresar la dirección ip y la máscara de subred ipv4.</p> <p>Ingresar la dirección de enlace local ipv6</p> <p>Ingresar la dirección ipv6</p> <p>Enciende la interfaz</p> <p>Sale de la interfaz</p> <p>Sale de la interfaz</p>
---	---

encapsulation dot1q 8	Código de encapsulación 802.1Q VLAN 8.
vrf forward General-Users	activa VRF de General-Users
ip address 10.0.208.3 255.255.255.0	Ingresa la dirección ip y la máscara de subred ipv4.
ipv6 address fe80::3:4 link- local	Ingresa la dirección de enlace local ipv6
ipv6 address 2001:db8:acad:208::1/64	Ingresa la dirección ipv6
no shutdown	Enciende la interfaz
exit	Sale de la interfaz
interface e1/1	Ingresa a la interface
no ip address	No configura dirección en la interface
no shutdown	Enciende la interfaz
exit	Sale de la interfaz

2.3 En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF

Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.

ROUTER R1

Código	Descripción
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.6	Se crea una Ruta estática direccionamiento IPv4 VRF Special-Users.
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.6	Se crea una Ruta estática direccionamiento IPv4 paraVRF General-Users.
ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2	Se crea una R uta estática IPv6 para VRF Special-Users.
ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2	Se crea una Ruta estática con direccionamiento IPv6 paraVRF General-Users.

ROUTER R2

Código	Descripción
--------	-------------

ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.1	Se crea una Ruta estática direccionamiento IPv4 VRF Special-Users.
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.3	Se crea una Ruta estática direccionamiento IPv4 VRF Special-Users.
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.1	Se crea una Ruta estática direccionamiento IPv4 para VRF General-Users
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.3	Se crea una Ruta estática direccionamiento IPv4 para VRF General-Users
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1	Se crea una Ruta estática IPv6 para VRF Special-Users. .
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3	Se crea una Ruta estática IPv6 para VRF Special-Users.
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1	Se crea una Ruta estática con direccionamiento IPv6 para VRF General-Users.
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3	Se crea una Ruta estática con direccionamiento IPv6 para VRF General-Users.

ROUTER R3

Código	Descripción
ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.6	Se crea una Ruta estática direccionamiento IPv4 VRF Special-Users.
ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.6	Se crea una Ruta estática direccionamiento IPv4 paraVRF General-Users


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

Se crea una Ruta estática IPv6 para VRF Special-Users.

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

Se crea una Ruta estática con direccionamiento IPv6 para VRF General-Users.

2.4 Verifique la conectividad en cada VRF.

Al terminar de configurar las VRF y la ruta estática, se puede verificar con el comando ping la conectividad entre las partes.

Desde R1, verifique la conectividad con R3:

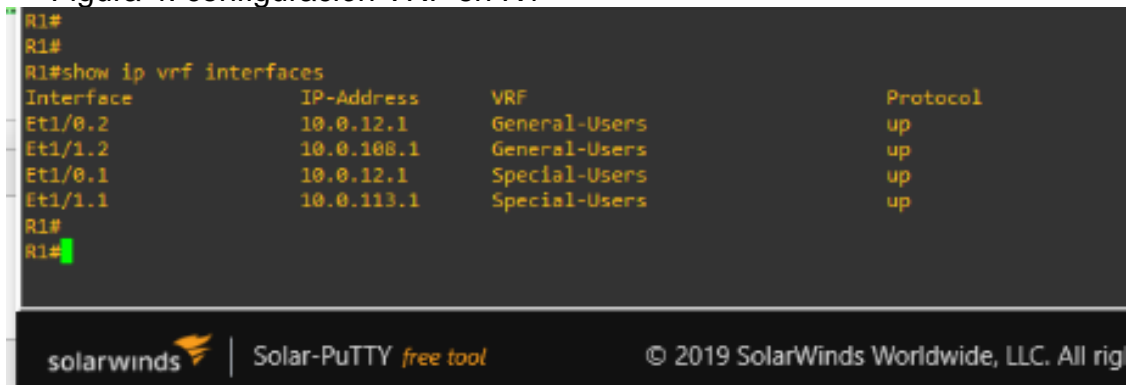
```
ping VRF General-Usuarios 10.0.208.Z
```

el comando show ip vrf interfaces muestra las interfaces vrf del router.

En R1 verifique las interfaces configuradas

Figura 4. configuración VRF en R1

```
R1#
R1#
R1#show ip vrf interfaces
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.1       General-Users    up
Et1/1.2        10.0.108.1      General-Users    up
Et1/0.1        10.0.12.1       Special-Users    up
Et1/1.1        10.0.113.1      Special-Users    up
R1#
R1#
```

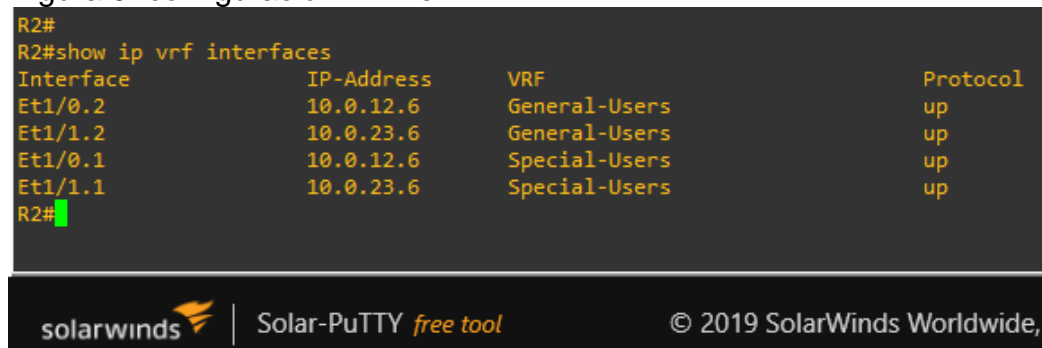


Fuente: escenario simulación GNS3

En R2 verifique las interfaces configuradas

Figura 5. configuración VRF en R2

```
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#
```

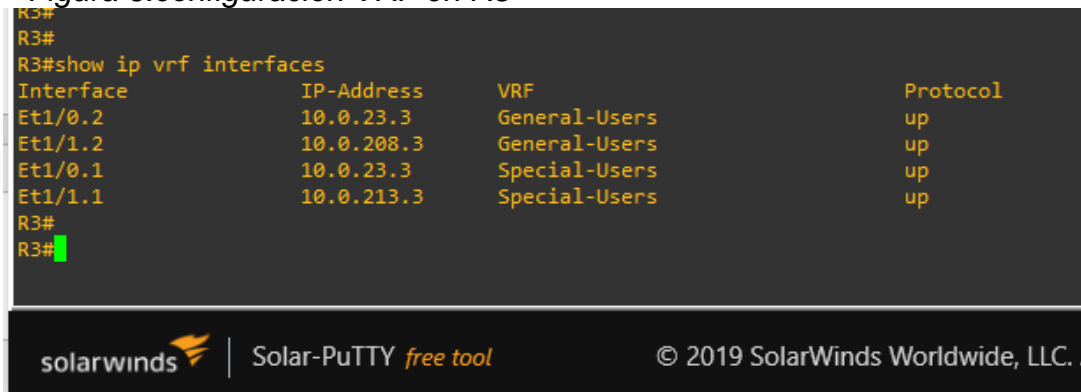


Fuente: escenario simulación GNS3

En R3 verifique las interfaces configuradas

Figura 6. configuración VRF en R3

```
R3#  
R3#  
R3#show ip vrf interfaces  
Interface          IP-Address      VRF              Protocol  
Et1/0.2            10.0.23.3      General-Users    up  
Et1/1.2            10.0.208.3     General-Users    up  
Et1/0.1            10.0.23.3      Special-Users    up  
Et1/1.1            10.0.213.3     Special-Users    up  
R3#  
R3#
```



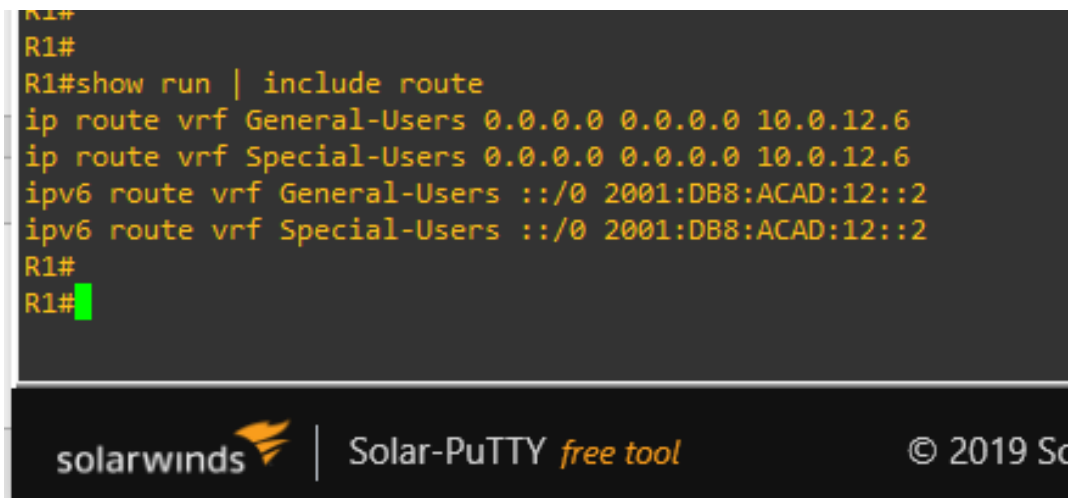
Fuente: escenario simulación GNS3

Verificar las rutas estáticas en los router.
el comando show run | include route muestra el direccionamiento de las rutas por donde va redirigido el tráfico de la red.

Ruta estática en router R1

Figura 7. Rutas estáticas en R1

```
R1#  
R1#  
R1#show run | include 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#  
R1#
```

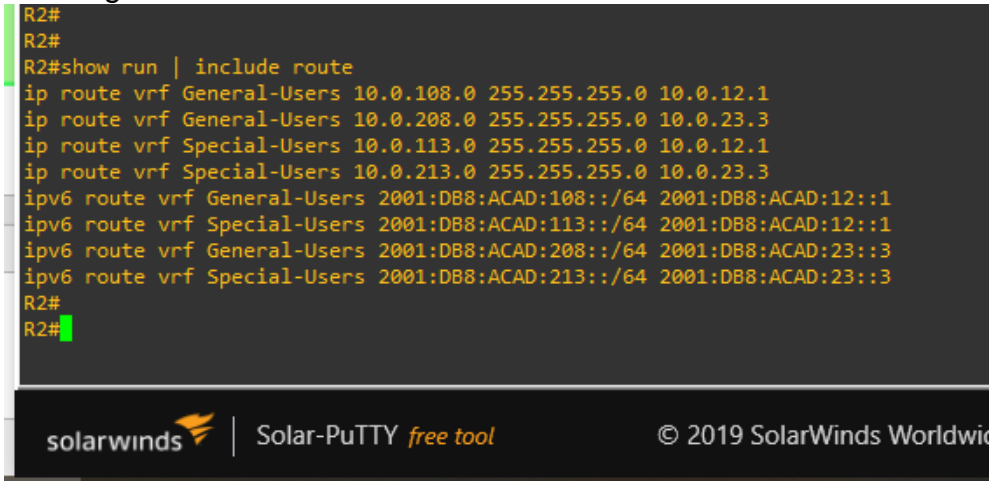


Fuente: escenario simulación GNS3

Ruta estática en router R2

Figura 8 .Rutas estáticas en R2

```
R2#
R2#
R2#show run | include route
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.1
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.3
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.1
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.3
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3
R2#
R2#
```

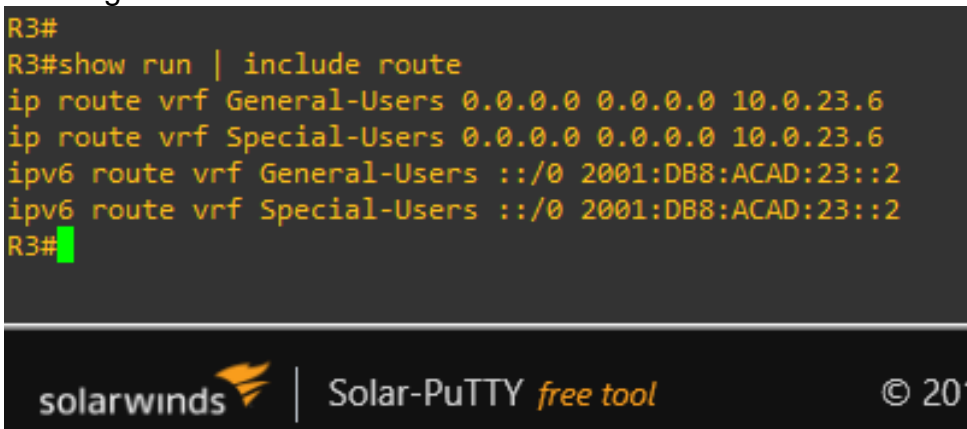


Fuente: escenario simulación GNS3

Ruta estática en router R3

Figura 9. Rutas estáticas en R3

```
R3#
R3#show run | include 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: escenario simulación GNS3

2.4. Verificar la conectividad en los VRF.

Desde R1, verificar conectividad con R3

- ping vrf General-Users 10.0.208.3

Figura 10. Ping a la interfaz E1/1.2 Ipv4

```
R1#  
R1#ping vrf General-Users 10.0.208.3  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.208.3, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/40/64 ms  
R1#
```

solarwinds | Solar-PuTTY *free tool* © 2019 SolarWinds World

Fuente: escenario simulación GNS3

- ping vrf General-Users 2001:db8:acad:208::1

Figura 11. Ping a la interfaz E1/1.2 Ipv6

```
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 = 56/78/104 ms  
R1#
```

solarwinds | Solar-PuTTY *free tool*

Fuente: escenario simulación GNS3

- ping vrf Special-Users 2001:db8:acad:213::1

Figura 12. ping a la interfaz E1/1.1 Ipv6

```
R1#  
R1#ping vrf Special-Users 2001:db8:acad:213::1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/40 ms  
R1#
```

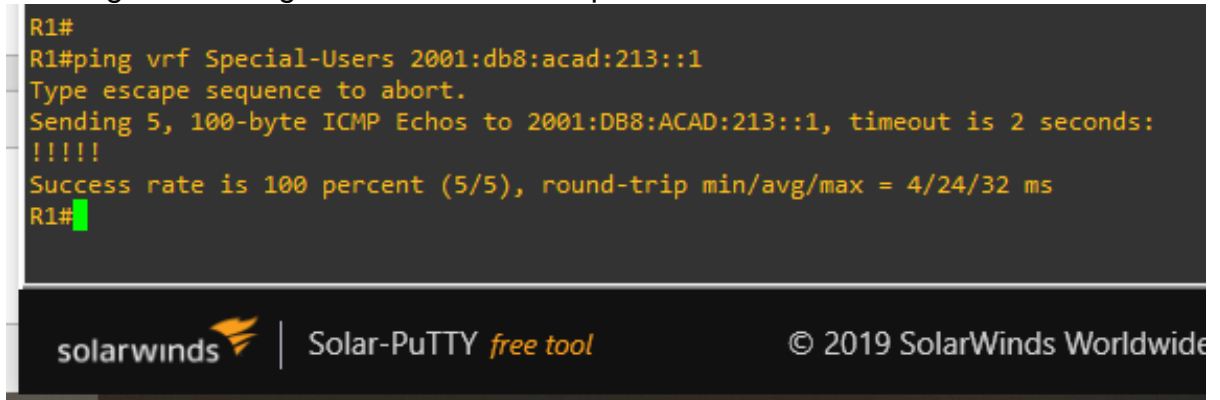
solarwinds | Solar-PuTTY *free tool* © 2019 SolarWinds Worldw

Fuente: escenario simulación GNS3

ping vrf Special-Users 2001:db8:acad:213::1

Figura 13. Ping a la nterfaz E1/1.1 Ipv6

```
R1#  
R1#ping vrf Special-Users 2001:db8:acad:213::1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/24/32 ms  
R1#
```



Fuente: escenario simulación GNS3

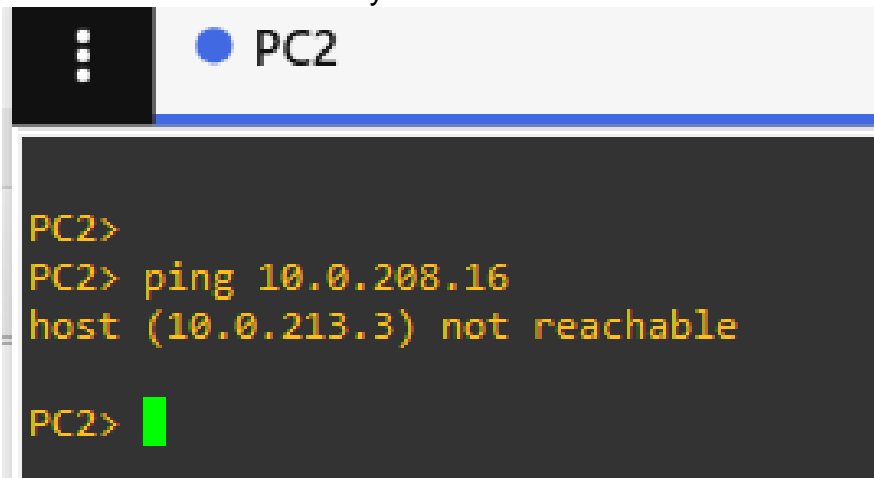
Con las configuraciones realizadas hasta el momento, se tiene que R1 no está habilitado para realizar ping entre PC2 o PC4. Por lo tanto, este deberá fallar.

Comando:

ping 10.0.208.16

Figura 14. conexión entre PC2 y PC4

```
PC2  
PC2>  
PC2> ping 10.0.208.16  
host (10.0.213.3) not reachable  
PC2>
```



Fuente: escenario simulación GNS3

PARTE 3. CONFIGURAR CAPA 2

En esta parte, se tendrán que configurar los Switches para soportar la conectividad con los dispositivos finales.

Las tareas de configuración son las siguientes:

Tabla 3 . Configuración de dispositivos capa 2

Tarea #	Tarea	Especificación
3.1	En D1, D2 y A1, deshabilite todas las interfaces.	En D1 y D2, cierre G1/0/1 a G1/0/24. En A1, apague F0/1 – F0/24, G0/1 – G0/2.
3.2	En D1 y D2, configure los enlaces troncales a R1 y R3.	Configure y habilite el enlace G1/0/11 como enlace troncal.
3.3	En D1 y A1, configure el EtherChannel.	En D1, configure y habilite: <ul style="list-style-type: none"> • Interfaz G1/0/5 y G1/0/6 • Canal de puerto 1 mediante PAgP En A1, configure enable: <ul style="list-style-type: none"> • Interfaz F0/1 y F0/2 • Canal de puerto 1 mediante PagP •
3.4	En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.	Configure y habilite los puertos de acceso de la siguiente manera: <ul style="list-style-type: none"> • En D1, configure la interfaz G1/0/23 como puerto de acceso en VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/23 como puerto de acceso en VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/24 como puerto de acceso

		<p>en VLAN 8 y habilite Portfast.</p> <ul style="list-style-type: none"> En A1, configure la interfaz F0/23 como puerto de acceso en VLAN 8 y habilite Portfast.
3.5	Verifique la conectividad de PC a PC.	<p>Desde PC1, verifique la conectividad IPv4 e IPv6 a PC2.</p> <p>Desde PC3, verifique la conectividad IPv4 e IPv6 con PC4.</p>

Fuente: Guía de Actividades escenario CCNP

3.1 En D1, D2, and A1, apagar las interfaces

Se apaga las interfaces de todos los switches

SWITCH D1

CODIGO	DESCRIPCION
Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	se selecciona el rango de la interfaz del SW D1
shutdown	Apaga las interfaces
exit	Sale de la interfaz

SWITCH D2

CODIGO	DESCRIPCION
Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	se selecciona el rango de la interfaz del SW D2
shutdown	Apaga las interfaces
exit	Sale de la interfaz

SWITCH A1

CODIGO	DESCRIPCION
Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	se selecciona el rango de la interfaz del SW D1
shutdown	Apaga las interfaces
exit	Sale de la interfaz

3.2 En D1 y D2, configure el enlace troncal hacia R1 y R3

SWITCH D1	
CODIGO	DESCRIPCION
Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface e0/2	Ingresa a la interfaz e0/2
switchport trunk encapsulation dot1q	Se activa el puerto de encapsulación enlace troncal dotq1
switchport mode trunk	Activa la interface en modo troncal
no shutdown	prende las interfaces
exit	Sale de la interfaz
SWITCH D2	
Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface e0/3	Ingresa a la interfaz e0/3
switchport trunk encapsulation dot1q	Se activa el puerto de encapsulación enlace troncal dotq1
switchport mode trunk	Activa la interface en modo troncal
no shutdown	Prende las interfaces
exit	Sale de la interfaz

3.3 En D1y A1, configure EtherChannel.

Configurar el ether channel enlace troncal de encapsulación estándar 802.1q.

Ether channel SWITCH D1	
CODIGO	DESCRIPCION
Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface range e0/0, e0/1	selecciona un grupo de interfaces
switchport trunk encapsulation dot1q	Se activa el puerto de encapsulación enlace troncal dotq1
switchport mode trunk	Activa la interface en modo troncal
channel-group 1 mode desirable	Activa la interface para el tráfico de paquetes
no shutdown	Enciende la interface
exit	Sale de la interfaz

Ether channel SWITCH A1

Enable	Ingres a modo global.
Configure terminal	Ingres a al modo de configuraci3n
interface range e0/0, e0/1	selecciona un grupo de interfaces
switchport trunk encapsulation dot1q	Se activa el puerto de encapsulaci3n enlace troncal dotq1
switchport mode trunk	Activa la interface en modo troncal
channel-group 1 mode desirable	Activa la interface para el tráfico de paquetes
no shutdown	Enciende la interface
exit	Sale de la interfaz

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

Puertos De Acceso Switch D1

CODIGO	DESCRIPCION
Enable	Ingres a modo global.
Configure terminal	Ingres a al modo de configuraci3n
interface e0/3	Ingres a la interface
switchport mode access	Se activa el modo de acceso
Switchport Access vlan 13	Asigna el puerto a la vlan 13
spanning-tree portfast	Habilita la protecci3n BPDU al puerto portfast
No shutdown	Enciende la interface
exit	Sale de la interfaz

Puertos De Acceso Switch D2

Enable	Ingres a modo global.
Configure terminal	Ingres a al modo de configuraci3n
interface e0/2	Ingres a la interface
switchport mode access	Se activa el modo de acceso
Switchport Access vlan 13	Asigna el puerto a la vlan 13
spanning-tree portfast	Habilita la protecci3n BPDU al puerto portfast
No shutdown	Enciende la interface
exit	Sale de la interfaz
interface e0/1	Ingres a la interface

switchport mode access	Se activa el modo de acceso
Switchport Access vlan 8	Asigna el puerto a la vlan 8
spanning-tree portfast	Habilita la protección BPDU al puerto portfast
No shutdown	Enciende la interface
exit	Sale de la interfaz

Puertos De Acceso Switch A1

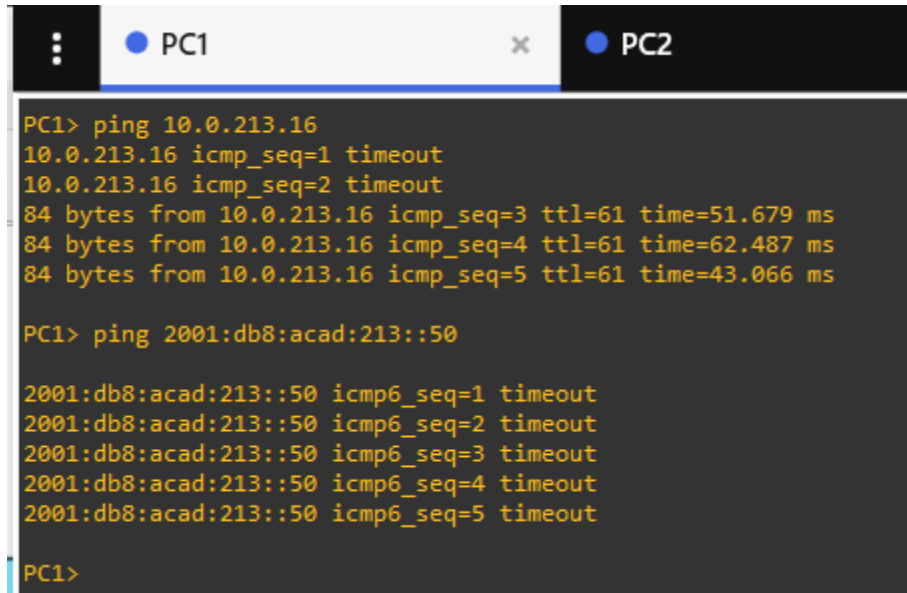
CODIGO	DESCRIPCION
Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
interface e0/2	Ingresa a la interface
switchport mode access	Se activa el modo de acceso
Switchport Access vlan 8	Asigna el puerto a la vlan 8
spanning-tree portfast	Habilita la protección BPDU al puerto portfast
No shutdown	Enciende la interface
exit	Sale de la interfaz

3.5 Verifique la conectividad

Desde el pc1 verifique la conectividad ipv4 e ipv6

- Desde PC1 se realiza un comando ping 10.0.213.16 ipv4 y ping 2001:db8:acad:213::50, ipv6.

Figura 15. Ping PC1 a PC2



```
PC1> ping 10.0.213.16
10.0.213.16 icmp_seq=1 timeout
10.0.213.16 icmp_seq=2 timeout
84 bytes from 10.0.213.16 icmp_seq=3 ttl=61 time=51.679 ms
84 bytes from 10.0.213.16 icmp_seq=4 ttl=61 time=62.487 ms
84 bytes from 10.0.213.16 icmp_seq=5 ttl=61 time=43.066 ms

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

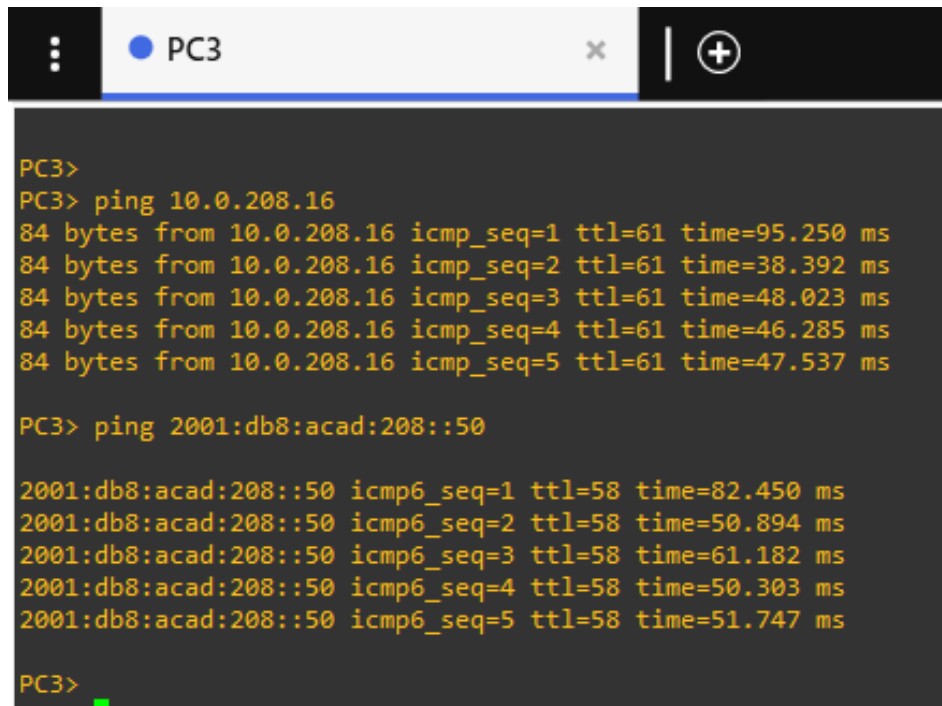
2001:db8:acad:213::50 icmp6_seq=1 timeout
2001:db8:acad:213::50 icmp6_seq=2 timeout
2001:db8:acad:213::50 icmp6_seq=3 timeout
2001:db8:acad:213::50 icmp6_seq=4 timeout
2001:db8:acad:213::50 icmp6_seq=5 timeout

PC1>
```

Fuente: escenario simulación GNS3

Para PC3, verificar conectividad IPv4 e IPv6 hacia PC4.

Figura 16. Ping PC3 - PC4 ping 10.



```
PC3>
PC3> ping 10.0.208.16
84 bytes from 10.0.208.16 icmp_seq=1 ttl=61 time=95.250 ms
84 bytes from 10.0.208.16 icmp_seq=2 ttl=61 time=38.392 ms
84 bytes from 10.0.208.16 icmp_seq=3 ttl=61 time=48.023 ms
84 bytes from 10.0.208.16 icmp_seq=4 ttl=61 time=46.285 ms
84 bytes from 10.0.208.16 icmp_seq=5 ttl=61 time=47.537 ms

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

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=82.450 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=50.894 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=61.182 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=50.303 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=51.747 ms

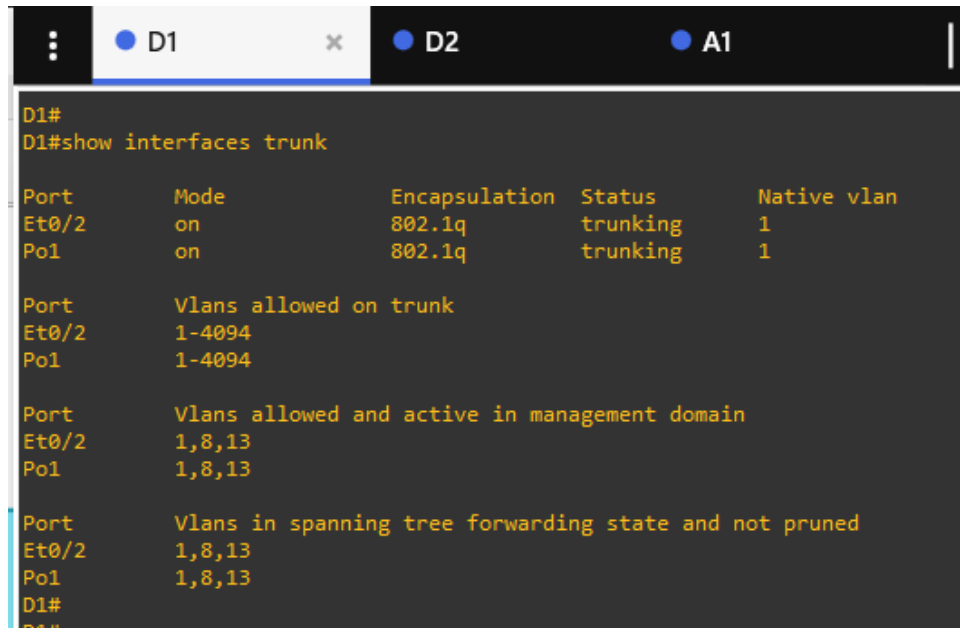
PC3>
```

Fuente: escenario simulación GNS3

Comandos de verificación L2 Network:

D1# show interfaces trunk:

Figura 17. Comando Interfaces Trunk en D1



```
D1#
D1#show interfaces trunk

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

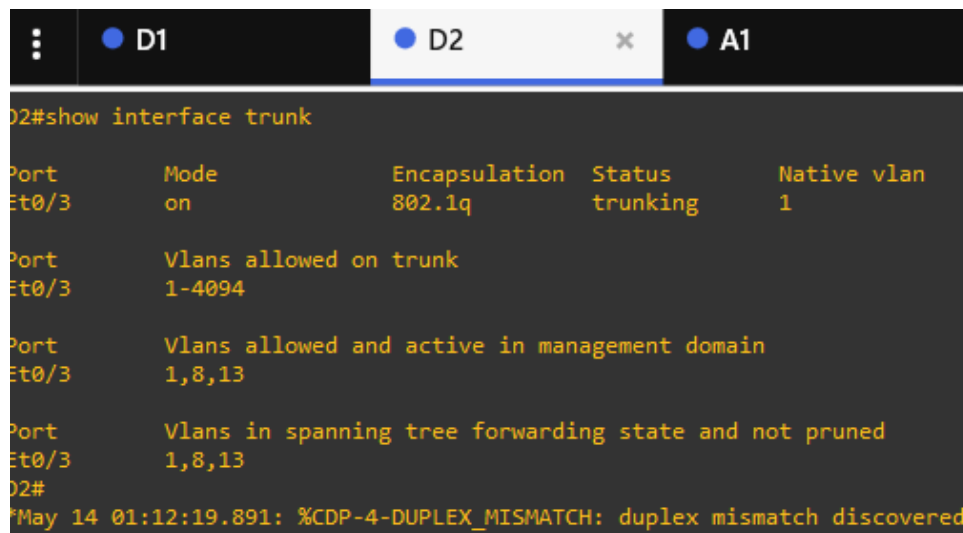
Port      Vlans allowed on trunk
Et0/2     1-4094
Po1       1-4094

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

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

Fuente: escenario simulación GNS3

Figura 18. comando Interfaces Trunk en D2



```
D2#show interface trunk

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

Port      Vlans allowed on trunk
Et0/3     1-4094

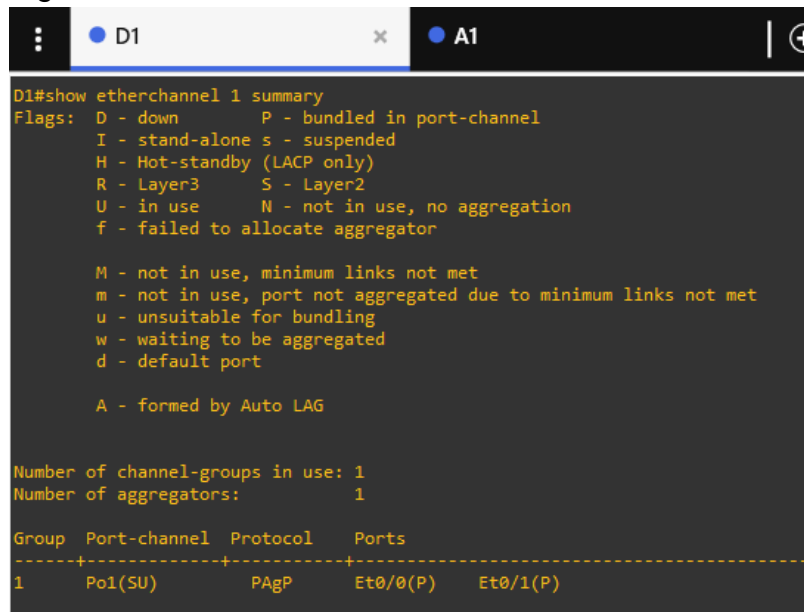
Port      Vlans allowed and active in management domain
Et0/3     1,8,13

Port      Vlans in spanning tree forwarding state and not pruned
Et0/3     1,8,13
D2#
*May 14 01:12:19.891: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered
```

Fuente: escenario simulación GNS3

Verificación de ether-channel

Figura 19. EtherChannel en D1



```
D1#show etherchannel 1 summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

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

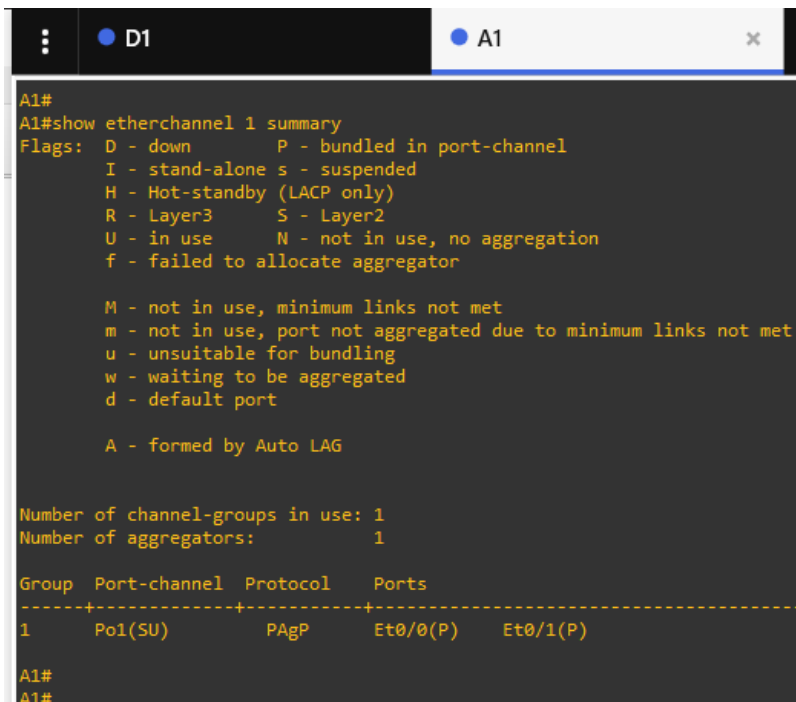
       A - formed by Auto LAG

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

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

Fuente: escenario simulación GNS3

Figura 20. EtherChannel en A1



```
A1#
A1#show etherchannel 1 summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

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

       A - formed by Auto LAG

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

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

A1#
A1#
```

Fuente: escenario simulación GNS3

PARTE 4. CONFIGURACION DE SEGURIDAD

En esta parte se realizará la configuración de varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tabla 4. Tareas de configuración de seguridad.

Task#	Task	Specification
4.1	On all devices, secure privileged EXEC mode.	Configure an enable secret as follows: <ul style="list-style-type: none"> • Algorithm type: SCRYPT • Password: <i>jhon163</i> •
4.2	On all devices, create a local user account.	Configure a local user: <ul style="list-style-type: none"> • Name: admin • Privilege level: 15 • Algorithm type: SCRYPT • Password: <i>jhon163</i>
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

Fuente: Guía de Actividades escenario CCNP

4.1 En todos los dispositivos configurar contraseña secreta EXEC mode.

Contraseña: *jhon163*

CONTRASEÑA SECRETA ROUTER R1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
<i>enable secret jhon163</i>	Habilita una contraseña secreta de acceso
Service password-encryption	Activa el cifrado de contraseñas
exit	Sale de la interfaz

CONTRASEÑA SECRETA ROUTER R2

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
<i>enable secret jhon163</i>	Habilita una contraseña secreta de acceso
Service password-encryption	Activa el cifrado de contraseñas
Exit	Sale de la interfaz

CONTRASEÑA SECRETA ROUTER R3

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
<i>enable secret jhon163</i>	Habilita una contraseña secreta de acceso
Service password-encryption	Activa el cifrado de contraseñas
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH D1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
<i>enable secret jhon163</i>	Habilita una contraseña secreta de acceso
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH D2

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
<i>enable secret jhon163</i>	Habilita una contraseña secreta de acceso
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH A1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
<i>enable secret jhon163</i>	Habilita una contraseña secreta de acceso
Service password-encryption	Activa el cifrado de contraseñas
exit	Sale de la interfaz

4.2 En todos los dispositivos crear un usuario local.

CONTRASEÑA SECRETA ROUTER R1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
Username admin secret 0	Crea un usuario local
<i>jhon163</i>	Con una contraseña
Username admin privilege 15	Crea un nombre de usuario , con
secret <i>jhon163</i>	privilegio total y contraseña secreta,
exit	Sale de la interfaz

CONTRASEÑA SECRETA ROUTER R2

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
Username admin secret 0	Crea un usuario local
<i>jhon163</i>	Con una contraseña
Username admin privilege 15	Crea un nombre de usuario , con
secret <i>jhon163</i>	privilegio total y contraseña secreta,
exit	Sale de la interfaz

CONTRASEÑA SECRETA ROUTER R3

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
Username admin secret 0	Crea un usuario local
<i>jhon163</i>	Con una contraseña
Username admin privilege 15	Crea un nombre de usuario , con
secret <i>jhon163</i>	privilegio total y contraseña secreta,
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH D1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
Username admin secret 0	Crea un usuario local
<i>jhon163</i>	Con una contraseña
Username admin privilege 15	Crea un nombre de usuario , con
secret <i>jhon163</i>	privilegio total y contraseña secreta,
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH D2

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
Username admin secret 0 <i>jhon163</i>	Crea un usuario local Con una contraseña
Username admin privilege 15 secret <i>jhon163</i>	Crea un nombre de usuario , con privilegio total y contraseña secreta,
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH A1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
Username admin secret 0 <i>jhon163</i>	Crea un usuario local Con una contraseña
Username admin privilege 15 secret <i>jhon163</i>	Crea un nombre de usuario , con privilegio total y contraseña secreta,
exit	Sale de la interfaz

4.3 En todos los dispositivos configure ingreso AAA con autenticación AAA.

CONTRASEÑA SECRETA ROUTE D1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
aaa new-model	Activa AAA nivel de seguridad en el dispositivo
aaa authentication login default local	Activa la autenticación del usuario local para acceso seguro.
username admin password <i>jhon163</i>	Usuario admin con contraseña de acceso.
exit	Sale de la interfaz

CONTRASEÑA SECRETA ROUTE D2

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
aaa new-model	Activa AAA nivel de seguridad en el dispositivo
aaa authentication login default local	Activa la autenticación del usuario local para acceso seguro.
username admin password <i>jhon163</i>	Usuario admin con contraseña de acceso.
exit	Sale de la interfaz

CONTRASEÑA SECRETA ROUTE D3

Enable	Ingresa a modo global.
--------	------------------------

Configure terminal	Ingresa al modo de configuración
aaa new-model	Activa AAA nivel de seguridad en el dispositivo
aaa authentication login default local	Activa la autenticación del usuario local para acceso seguro.
username admin password <i>jhon163</i>	Usuario admin con contraseña de acceso.
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH D1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
aaa new-model	Activa AAA nivel de seguridad en el dispositivo
aaa authentication login default local	Activa la autenticación del usuario local para acceso seguro.
username admin password <i>jhon163</i>	Usuario admin con contraseña de acceso.
exit	Sale de la interfaz

CONTRASEÑA SECRETA SWITCH D2

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
aaa new-model	Activa AAA nivel de seguridad en el dispositivo
aaa authentication login default local	Activa la autenticación del usuario local para acceso seguro.
username admin password <i>jhon163</i>	Usuario admin con contraseña de acceso.
exit	Sale de la interfaz

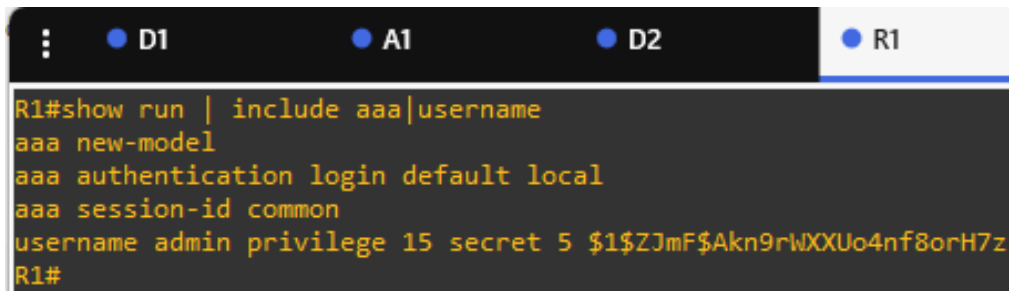
CONTRASEÑA SECRETA SWITCH A1

Enable	Ingresa a modo global.
Configure terminal	Ingresa al modo de configuración
aaa new-model	Activa AAA nivel de seguridad en el dispositivo
aaa authentication login default local	Activa la autenticación del usuario local para acceso seguro.
username admin password <i>jhon163</i>	Usuario admin con contraseña de acceso.
exit	Sale de la interfaz

4.4 Verificación de configuración de seguridad **username y AAA**

Comando: show run | include aaa|username

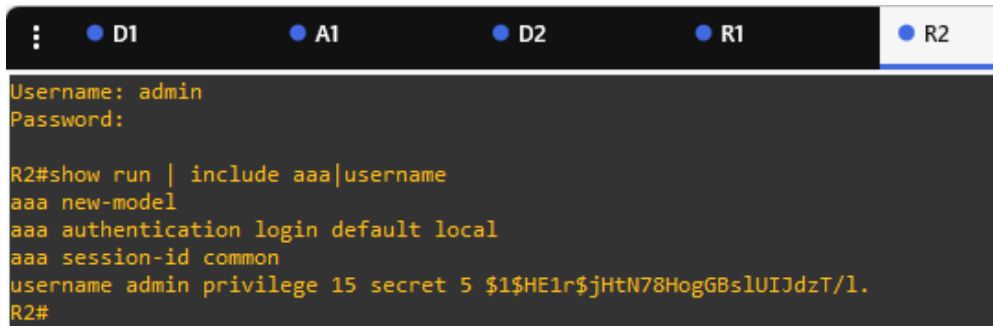
Figura 21. Username y autenticación AAA en R1



```
R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$ZJmF$Akn9rWXXUo4nf8orH7z
R1#
```

Fuente: escenario simulación GNS3

Figura 22. Username y autenticación AAA en R2

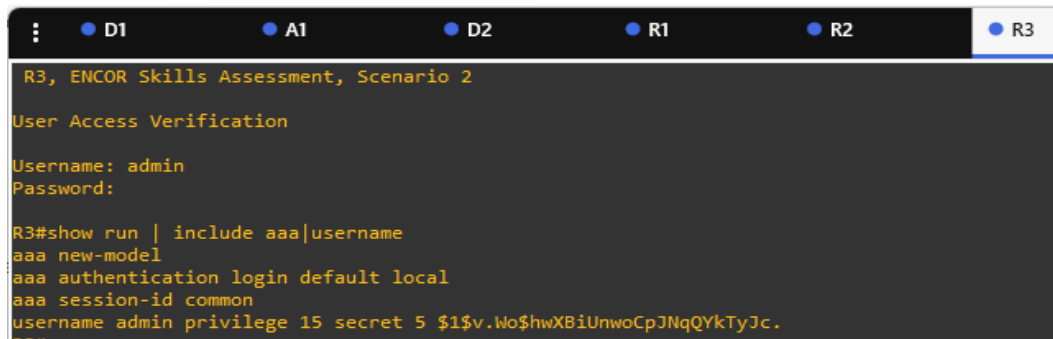


```
Username: admin
Password:

R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$HE1r$jHtN78HogGBs1UIJdzT/1.
R2#
```

Fuente: escenario simulación GNS3

Figura 23. Username y autenticación AAA en R3

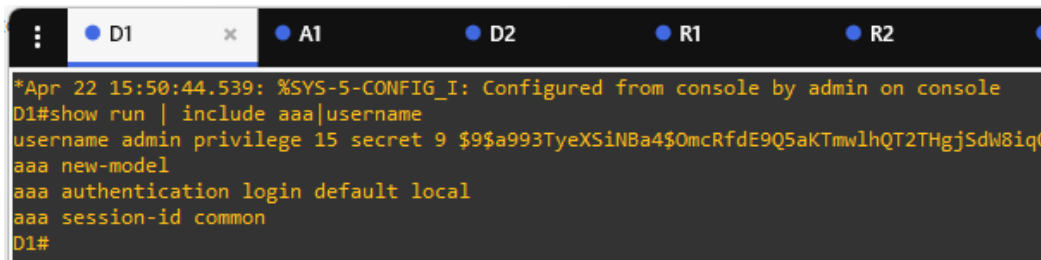


```
R3, ENCOR Skills Assessment, Scenario 2
User Access Verification
Username: admin
Password:

R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$v.Wo$hwXBiUnwoCpJNqQYkTyJc.
R3#
```

Fuente: escenario simulación GNS3

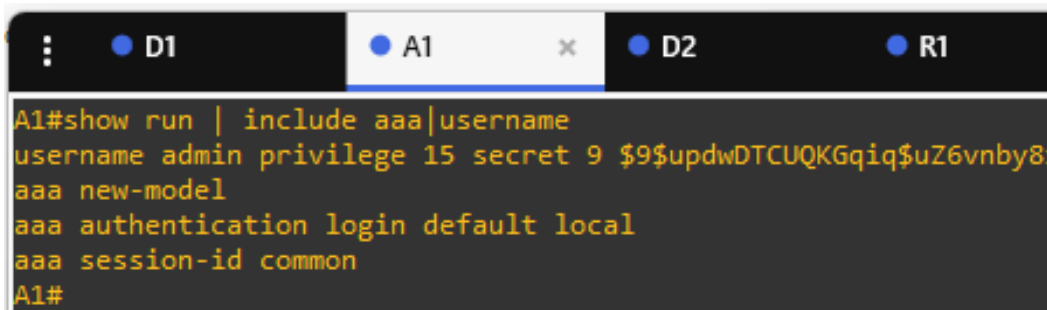
Figura 24. Username y autenticación AAA en D1



```
*Apr 22 15:50:44.539: %SYS-5-CONFIG_I: Configured from console by admin on console
D1#show run | include aaa|username
username admin privilege 15 secret 9 $9$a993TyeXSINBa4$0mcRfdE9Q5aKTmwlhQT2THgjSdW8iq
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
```

Fuente: Escenario de emulación GNS3

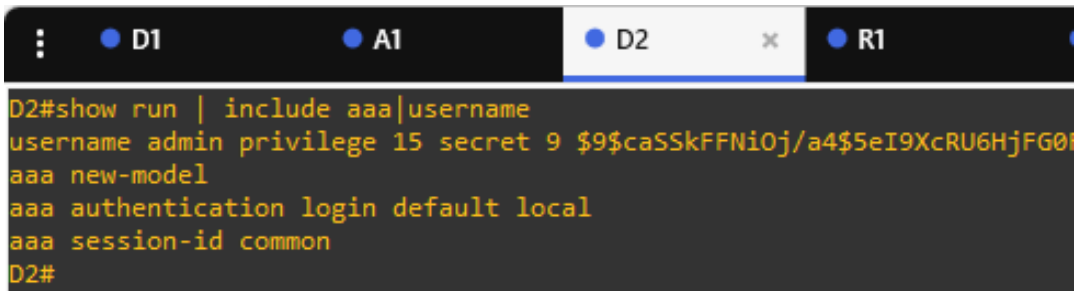
Figura 25. Username y autenticación AAA en A1



```
A1#show run | include aaa|username
username admin privilege 15 secret 9 $9$updwDTCUQKGqiq$uZ6vnby8
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```

Fuente: escenario simulación GNS3

Figura 26. Username y autenticación AAA en D2



```
D2#show run | include aaa|username
username admin privilege 15 secret 9 $9$caSSkFFNiOj/a4$5eI9XcRU6HjFG0
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```

Fuente: escenario simulación GNS3

CONCLUSIONES

En el diseño de la topología propuesta que da resultado a un escenario que exige una implementación VRF se aplican los conocimientos necesarios para este tipo de redes, en las cuales hay dos tipos de clientes, los usuarios especiales y los usuarios generales, independientes una de la otra.

La implementación de una red multi VTF-lite, en dos redes independientes con un mismo direccionamiento en un único dispositivo, es una tecnología de redes que permite el mejor uso del hardware, implementando una red confiable, rápida y segura mediante protocolos de seguridad AAA, con la creación de un usuario admin el cual es solicitado en el ingreso global en el dispositivo, las dos vrf no tienen comunicación entre ellas, el tráfico de red es independiente.

Las rutas estáticas configuradas agilizan el tráfico de paquetes aumentando el ancho de banda disponible, no presentan actualizaciones y solo pueden ser cambiadas en forma manual en la configuración del dispositivo.

BIBLIOGRAFÍA

Dávila, L. P.. VRF (Virtual Routing and Forwarding). Cisco.com.[En línea] (2018, junio 27) disponible en <https://community.cisco.com/t5/documentos-routing-y-switching/vrf-virtual-routing-and-forwarding/ta-p/3406835>

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

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

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

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

UNAD (2020). Configuración de Switches y Routers [OVA]. <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>