DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JESÚS ALBERTO BONILLA HERNÁNDEZ

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JESÚS ALBERTO BONILLA HERNÁNDEZ

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

DIRECTOR:
JOHN HAROLD PEREZ CALDERÓN

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

BOGOTÁ, 21 de marzo de 2023

AGRADECIMIENTOS

La realización del presente contenido converge todo lo adquirido en un periodo de tiempo extenso pues data de bastantes años atrás y cada peldaño no ha sido fácil de escalar. Por lo tanto, la salud mental, física, familiar, económica y en fin, tantos factores que hay que sortear para la realización de una carrera profesional, forjan una personalidad y una ética que se espera sostener en el trascurso de formación de un profesional y hacen parte fundamental del criterio a aplicar en el trabajo y en la vida personal. Cada detalle del contenido realizado supone un gran esfuerzo y con precisión al detalle con el fin de entregar calidad. Por lo tanto aquí se ve reflejado el agradecimiento a mi familia, esposa Cindy e hijo Alejo, que son el motor que impulsa el día a día.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

IPV6: IPv6 es una versión del protocolo de Internet (IP) que sucede a IPv4. Utiliza una dirección de 128 bits, lo que permite un número mucho mayor de direcciones IP únicas que IPv4, que utiliza una dirección de 32 bits. Esto significa que IPv6 puede soportar un número mucho mayor de dispositivos conectados a Internet.
IPv6 también ofrece mejoras en la seguridad de la red, ya que incluye soporte integrado para la autenticación y la privacidad de los datos, lo que ayuda a prevenir ataques como el spoofing de direcciones IP.

PING: es una utilidad de red que se utiliza para probar la conectividad entre dispositivos en una red IP. El comando Ping envía paquetes de datos a una dirección IP de destino y espera una respuesta. Si el dispositivo de destino responde, significa que está en línea y se puede establecer una conexión con él.

RUTA ESTÁTICA: son rutas cuando se necesita tener un control preciso sobre el camino que tomarán los paquetes en la red, ya sea para evitar una congestión en la red o para asegurar que los paquetes se enruten a través de una ruta específica para cumplir con ciertas políticas de seguridad o cumplimiento.

VLAN: "*Virtual Local Area Network*" (Red de Área Local Virtual) y es una tecnología de red que permite segmentar una red física en múltiples redes lógicas aisladas.
VLAN permite agrupar múltiples dispositivos de red en una red lógica separada, independiente de la ubicación física de los dispositivos en la red. Esto se logra asignando puertos de switch a una VLAN específica, de manera que solo los dispositivos que pertenecen a esa VLAN puedan comunicarse entre sí.

VRF: *Virtual Routing and Forwarding* (Enrutamiento y Reenvío Virtual) y es una tecnología de red que permite la creación de múltiples instancias virtuales de una red de área local (LAN) o de una red de área amplia (WAN) en una sola red física.
VRF permite a los administradores de red crear redes virtuales separadas y aisladas en una red física compartida. Cada VRF tiene su propia tabla de enrutamiento, lo que significa que los paquetes que se envían a través de una VRF específica solo se reenvían a los destinos que están en la misma VRF. Esto proporciona una forma segura y eficiente de mantener múltiples redes separadas y protegerlas de interferencias y accesos no autorizados.

RESUMEN

En un escenario de red se han creado cuatro VRF (Virtual Routing and Forwarding) diferentes en dos VLAN (Virtual Local Area Network) distintas utilizando el software GNS3. El objetivo de la configuración es generar conectividad dentro de cada VLAN, pero a través de diferentes VRF.

Para lograr esto, se han creado dos VLAN, cada una con dos VRF. La VLAN 13 tiene dos VRF "Especial_Users", mientras que la VLAN 8 tiene dos VRF "General_Users". Cada VRF tiene una dirección IP única dentro de su VLAN, lo que permite la conectividad dentro de la misma VLAN, pero no con los VRF de la otra VLAN.

Se han asignado puertos de switch a cada VLAN y se han configurado enrutadores para conectividad entre VLAN. Cada puerto de switch está configurado para etiquetar el tráfico de VLAN, lo que asegura que los paquetes sean enviados a través de la VLAN correcta. Los enrutadores también se han configurado con enrutamiento inter-VLAN y con una tabla de rutas que contiene las rutas estáticas a través de los diferentes VRF.

La configuración de cuatro VRF diferentes en dos VLAN distintas permite la conectividad dentro de cada VLAN, pero no entre los VRF de diferentes VLAN. Esto es útil para mantener la privacidad y la seguridad de los datos en la red. La configuración se ha realizado utilizando el software GNS3, que es una herramienta de simulación de redes que permite a los usuarios crear y probar topologías de red complejas en un entorno virtual.

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

ABSTRACT

In a network scenario, four different VRFs (Virtual Routing and Forwarding) have been created in two different VLANs (Virtual Local Area Network) using the GNS3 software. The goal of the configuration is to generate connectivity within each VLAN, but through different VRFs.

To achieve this, two VLANs have been created, each with two VRFs. VLAN 13 has two "Special_Users" VRFs, while VLAN 8 has two "General_Users" VRFs. Each VRF has a unique IP address within its VLAN, allowing connectivity within the same VLAN, but not with VRFs on the other VLAN.

Switch ports have been assigned to each VLAN and routers have been configured for inter-VLAN connectivity. Each switch port is configured to VLAN traffic tagging, which ensures that packets are sent through the correct VLAN. The routers have also been configured with inter-VLAN routing and with a route table containing the static routes through the different VRFs.

The configuring four different VRFs on two different VLANs allows connectivity within each VLAN, but not between VRFs on different VLANs. This is useful for maintaining the privacy and security of data on the network. The configuration has been done using the GNS3 software, which is a network simulation tool that allows users to create and test complex network topologies in a virtual environment.

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

INTRODUCCIÓN

El diplomado CCNP (*Cisco Certified Network Professional*) es una certificación avanzada de redes de Cisco que se enfoca en el diseño, implementación y mantenimiento de redes de área amplia (WAN) y redes de área local (LAN). El objetivo principal de este diplomado es que los profesionales de redes adquieran un conjunto de habilidades técnicas avanzadas que les permitan diseñar e implementar redes de alta disponibilidad y seguridad, en un entorno empresarial.

El diplomado CCNP es un programa de capacitación técnica que consta de varios cursos y exámenes que abarcan áreas de enrutamiento, conmutación, seguridad y diseño de redes. Uno de los escenarios resueltos a continuación, es la configuración de VRF (Virtual Routing and Forwarding), una técnica que permite a múltiples instancias de una red compartir el mismo hardware de enrutamiento, pero mantenerse completamente aislados unos de otros en términos de dirección IP y tablas de enrutamiento.

Y el otro escenario resuelto es la configuración de switches con puertos de acceso y autenticación AAA (*Authentication, Authorization, and Accounting*). Esto implica la creación de VLANs, la configuración de puertos de switch para asegurar el tráfico de datos y la implementación de medidas de seguridad para restringir el acceso no autorizado a la red. CCNP es un programa de capacitación avanzado que brinda a los profesionales de redes una serie de habilidades técnicas para diseñar e implementar redes de alta disponibilidad, seguridad y escalabilidad.

DESARROLLO

1. Escenario 1

Figura 1. Topología propuesta en GNS3

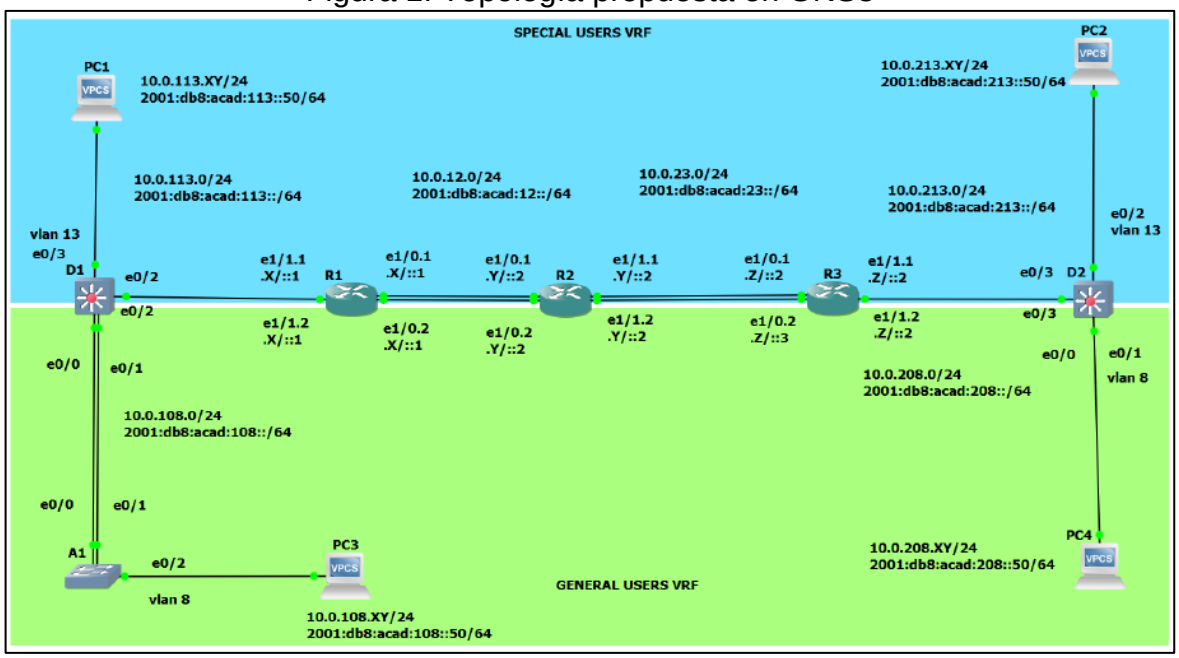


Tabla 1. Direccionamiento general en la topología

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.3/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.3/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.3/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.3/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.8/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.8/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.8/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.8/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.5/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.5/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.5/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.5/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.38/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.38/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.38/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.38/24	2001:db8:acad:208::50/64	EUI-64

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

Escenario

Es necesario 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. Verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según lo requerido.

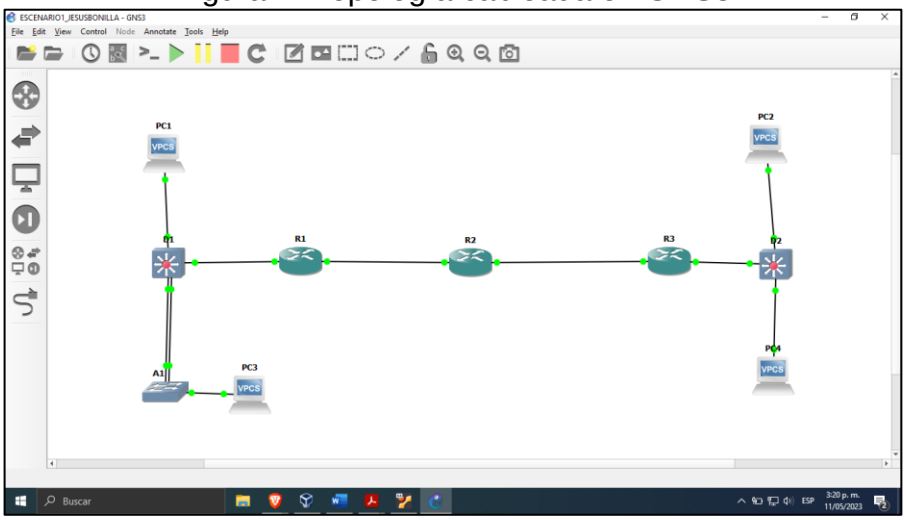
Instrucciones

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

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

Conectar los dispositivos como se muestra en el diagrama de topología y cablear según sea necesario.

Figura 2. Topología cableada en GNS3



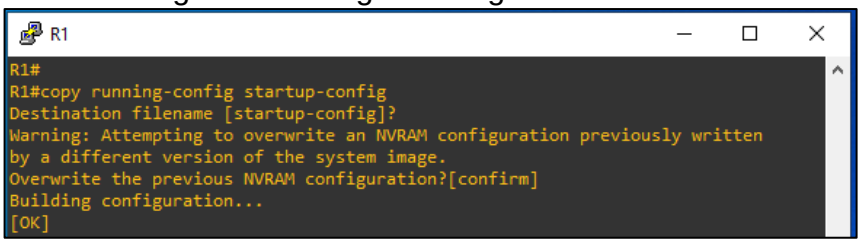
Paso 2: Configurar los ajustes básicos para cada dispositivo.

a. Ingresar al modo de configuración global en cada uno de los dispositivos y aplicar la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.

Router R1

`hostname R1`	Establece el nombre del host
`ipv6 unicast-routing`	Habilitar el enrutamiento unicast IPv6
`no ip domain lookup`	Deshabilitar la función búsqueda
`banner motd # R1, ENCOR Skills Assessment, Scenario 2 #`	Establecer un mensaje de aviso
`line con 0`	Configurar primera línea de consola
`exec-timeout 0 0`	Cierre sesión automática por inactividad
`logging synchronous`	Evitar mensajes se intercalen con comandos
`exit`	Salir del modo de configuración

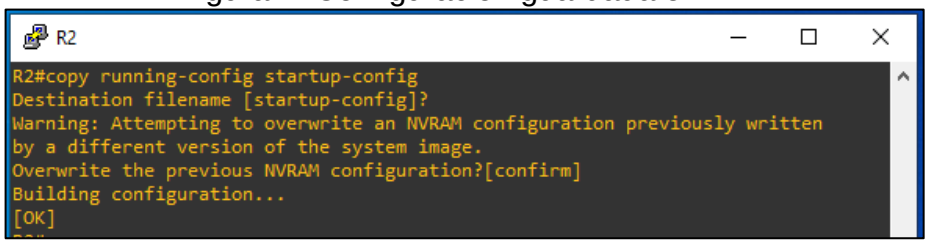
Figura 3. Configuración guardada en R1



Router R2

`hostname R2`	Establece el nombre del host
`ipv6 unicast-routing`	Habilitar el enrutamiento unicast IPv6
`no ip domain lookup`	Deshabilitar la función búsqueda
`banner motd # R2, ENCOR Skills Assessment, Scenario 2 #`	Establecer un mensaje de aviso
`line con 0`	Configurar primera línea de consola
`exec-timeout 0 0`	Cierre sesión automática por inactividad
`logging synchronous`	Evitar mensajes se intercalen con comandos
`exit`	Salir del modo de configuración

Figura 4. Configuración guardada en R2



Router R3

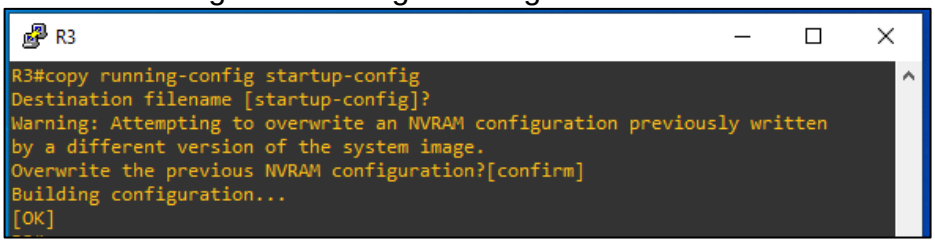
```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR
Skills Assessment,
Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

Establece el nombre del host
Habilitar el enrutamiento unicast IPv6
Deshabilitar la función búsqueda

Establecer un mensaje de aviso

Configurar primera línea de consola
Cierre sesión automática por inactividad
Evitar mensajes se intercalen con comandos
Salir del modo de configuración

Figura 5. Configuracion guardada en R3



Switch D1

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

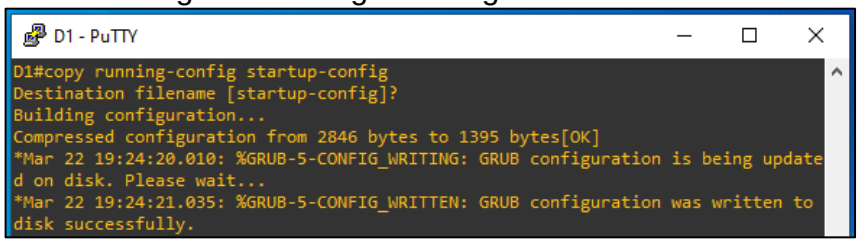
Establece el nombre del host
Habilitar enrutamiento IP en el dispositivo
Habilitar el enrutamiento unicast IPv6
Deshabilitar la función búsqueda

Establecer un mensaje de aviso

Configurar primera línea de consola
Cierre sesión automática por inactividad
Evitar mensajes se intercalen con comandos
Salir del modo de configuración
Crea la VLAN identificada con 8

`vlan 8`	Nombra la VLAN creada
`name General_Users`	Salir del modo de configuración
`exit`	Crea la VLAN identificada con 13
`vlan 13`	Nombra la VLAN creada
`name Especial_Users`	Salir del modo de configuración
`exit`	

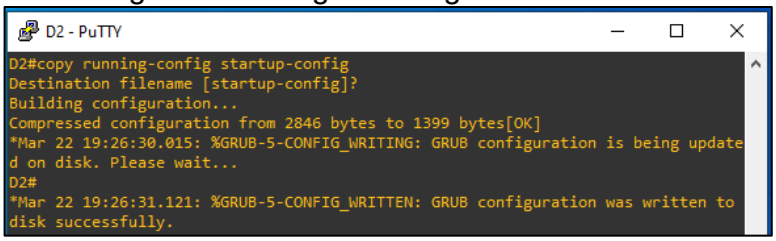
Figura 6.Configuracion guardada en D1



Switch D2

`hostname D2`	Establece el nombre del host
`ip routing`	Habilitar enrutamiento IP en el dispositivo
`ipv6 unicast-routing`	Habilitar el enrutamiento unicast IPv6
`no ip domain lookup`	Deshabilitar la función búsqueda
`banner motd # D2, ENCOR Skills Assessment, Scenario 2 #`	Establecer un mensaje de aviso
`line con 0`	Configurar primera línea de consola
`exec-timeout 0 0`	Cierre sesión automática por inactividad
`logging synchronous`	Evitar mensajes se intercalen con comandos
`exit`	Salir del modo de configuración
`vlan 8`	Crea la VLAN identificada con 8
`name General_Users`	Nombra la VLAN creada
`exit`	Salir del modo de configuración
`vlan 13`	Crea la VLAN identificada con 13
`name Especial_Users`	Nombra la VLAN creada
`exit`	Salir del modo de configuración

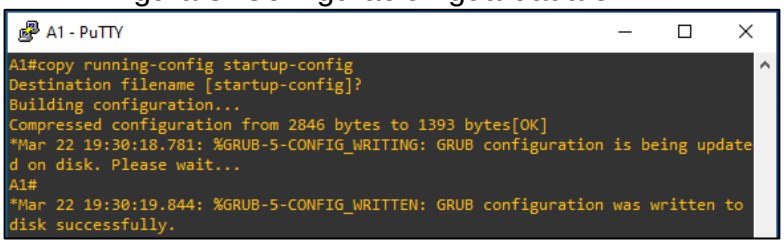
Figura 7. Configuracion guardada en D2



Switch A1

`hostname A1`	Establece el nombre del host
`ipv6 unicast-routing`	Habilitar el enrutamiento unicast IPv6
`no ip domain lookup`	Deshabilitar la función búsqueda
`banner motd # A1, ENCOR Skills Assessment, Scenario 2 #`	Establecer un mensaje de aviso
`line con 0`	Configurar primera línea de consola
`exec-timeout 0 0`	Cierre sesión automática por inactividad
`logging synchronous`	Evitar mensajes se intercalen con comandos
`exit`	Salir del modo de configuración
`vlan 8`	Crea la VLAN identificada con 8
`name General_Users`	Nombra la VLAN creada
`exit`	Salir del modo de configuración

Figura 8. Configuracion guardada en A1



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

Las configuraciones de los dispositivos se guardan mediante el comando:

Código de configuración

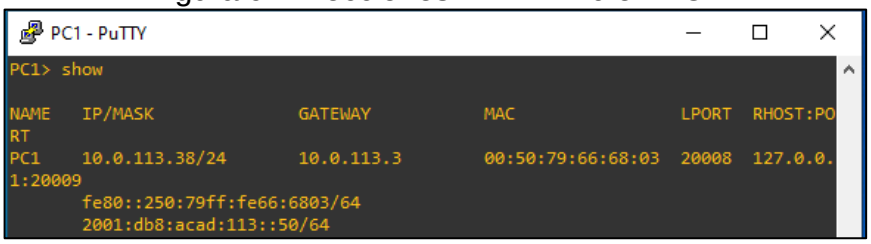
`copy running-config startup-config`	Guardar la configuración actual

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

Pc1

`ip 10.0.113.38/24 10.0.113.3`	Dirección IPV4 y gateway
`ip 2001:db8:acad:113::50/64`	Dirección IPV6
`save`	Guardar configuración
`show`	Mostrar datos PC

Figura 9. Direcciones IPV4 IPV6 en PC1

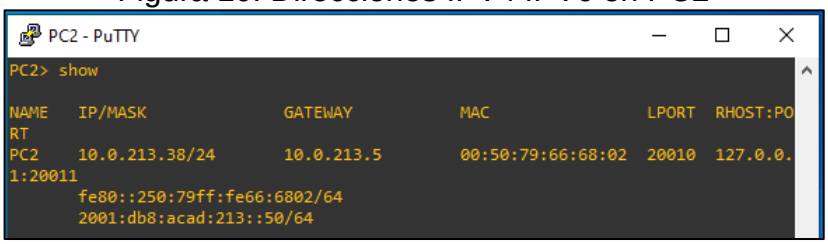


Pc2

```
ip 10.0.213.38/24 10.0.213.5
ip 2001:db8:acad:213::50/64
save
show
```

Dirección IPV4 y gateway
Dirección IPV6
Guardar configuración
Mostrar datos PC

Figura 10. Direcciones IPV4 IPV6 en PC2

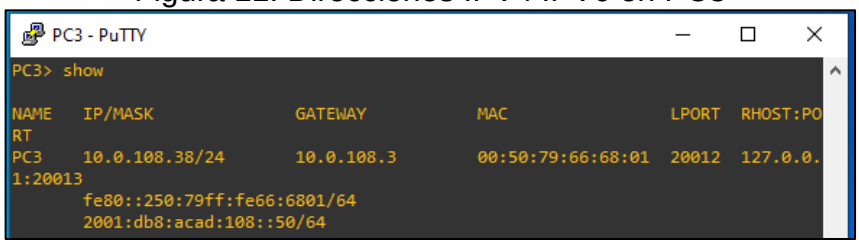


Pc3

```
ip 10.0.108.38/24 10.0.108.3
ip 2001:db8:acad:108::50/64
save
show
```

Dirección IPV4 y gateway
Dirección IPV6
Guardar configuración
Mostrar datos PC

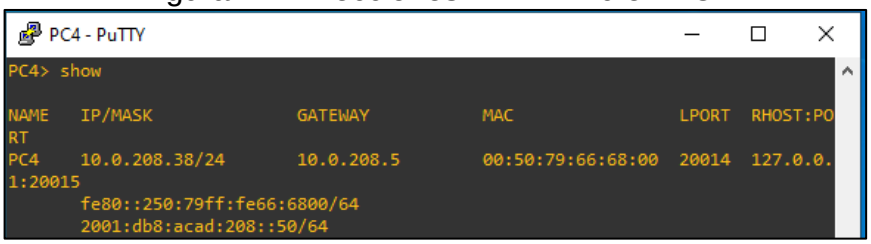
Figura 11. Direcciones IPV4 IPV6 en PC3



Pc4

```
ip 10.0.208.38/24 10.0.208.5    Dirección IPV4 y gateway
ip 2001:db8:acad:208::50/64     Dirección IPV6
save                            Guardar configuración
show                            Mostrar datos PC
```

Figura 12. Direcciones IPV4 IPV6 en PC4



Parte 2: configurar VRF y enrutamiento estático

En esta parte, configurar 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 se debe poder hacer ping a R3 en cada VRF.

Las tareas de configuración son las siguientes:

Tabla 2. Tareas que realizar en la creación de instancias virtuales de enrutamiento

Task	Task	Specification
2.1	On R1, R2, and R3, configure VRF-Lite VRFs as shown in the topology diagram.	Configure two VRFs: • General_Users • Especial_Users The VRFs must support IPv4 and IPv6.
2.2	On R1, R2, and R3, configure IPv4 and IPv6 interfaces on each VRF as detailed in the addressing table above.	All routers will use Router-On-A-Stick on their e1/1.x interfaces to support separation of the VRFs. Sub-interface 1: • In the Especial Users VRF • Use dot1q encapsulation • IPv4 and IPv6 GUA and link-local addresses • Enable the interfaces Sub-interface 2: • In the General Users VRF • Use dot1q encapsulation • IPv4 and IPv6 GUA and link-local addresses • Enable the interfaces
2.3	On R1 and R3, configure default static routes pointing to R2.	Configure VRF static routes for both IPv4 and IPv6 in both VRFs.

2.4	Verify connectivity in each VRF.	From R1, verify connectivity to R3: • ping vrf General_Users 10.0.208.5 • ping vrf General_Users 2001:db8:acad:208::1 • ping vrf Especial_Users 10.0.213.5 • ping vrf Especial_Users 2001:db8:acad:213::1

Tarea 2.1 creación de las VRF en los router R1, R2 y R3

Router R1

`configure terminal`	Modo de configuración de terminal
`vrf definition General_Users`	Creación y definición de VRF
`address-family ipv4`	Habilitación de IPV4
`exit`	Salir del modo de configuración
`address-family ipv6`	Habilitación de IPV6
`exit`	Salir del modo de configuración
`vrf definition Especial_Users`	Creación y definición de VRF
`address-family ipv4`	Habilitación de IPV4
`exit`	Salir del modo de configuración
`address-family ipv6`	Habilitación de IPV6
`exit`	Salir del modo de configuración

Router R2

`configure terminal`	Modo de configuración de terminal
`vrf definition General_Users`	Creación y definición de VRF
`address-family ipv4`	Habilitación de IPV4
`exit`	Salir del modo de configuración
`address-family ipv6`	Habilitación de IPV6
`exit`	Salir del modo de configuración
`vrf definition Especial_Users`	Creación y definición de VRF
`address-family ipv4`	Habilitación de IPV4
`exit`	Salir del modo de configuración
`address-family ipv6`	Habilitación de IPV6
`exit`	Salir del modo de configuración

Router R3

`configure terminal`	Modo de configuración de terminal
`vrf definition General_Users`	Creación y definición de VRF
`address-family ipv4`	Habilitación de IPV4
`exit`	Salir del modo de configuración
`address-family ipv6`	Habilitación de IPV6
`exit`	Salir del modo de configuración
`vrf definition Especial_Users`	Creación y definición de VRF
`address-family ipv4`	Habilitación de IPV4
`exit`	Salir del modo de configuración
`address-family ipv6`	Habilitación de IPV6
`exit`	Salir del modo de configuración

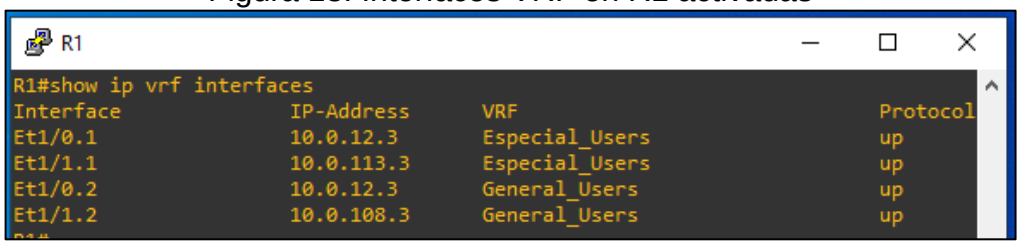
Tarea 2.2 configuración de las interfaces IPV4 IPV6 de acuerdo con la tabla de enrutamiento

Router R1

`configure terminal`	Modo de configuración de terminal
`interface Ethernet1/0.1`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 13`	ID de VLAN
`vrf forwarding Especial_Users`	Asignación de instancia VRF
`ip address 10.0.12.3 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::1:1 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:12::1/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/0.2`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 8`	ID de VLAN
`vrf forwarding General_Users`	Asignación de instancia VRF
`ip address 10.0.12.3 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::1:2 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:12::1/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/0`	Habilitar el puerto general con el fin que las subinterfaces también se activen
`no ip Address`	
`no shutdown`	
`exit`	Subinterfaz en puerto Ethernet

`interface Ethernet1/1.1`	ID de VLAN
`encapsulation dot1q 13`	Asignación de instancia VRF
`vrf forwarding Especial_Users`	Dirección IPV4
`ip address 10.0.113.3 255.255.255.0`	
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::1:3 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:113::1/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/1.2`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 8`	ID de VLAN
`vrf forwarding General_Users`	Asignación de instancia VRF
`ip address 10.0.108.3 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::1:4 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:108::1/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/1`	Habilitar el puerto general con el fin que las subinterfaces también se activen
`no ip Address`	
`no shutdown`	
`exit`	Salir del modo de configuración
`exit`	

Figura 13. Interfaces VRF en R1 activadas

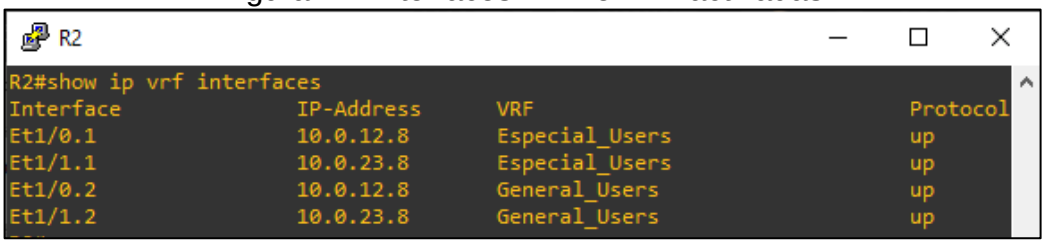


Router R2

`configure terminal`	Modo de configuración de terminal
`interface Ethernet1/0.1`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 13`	ID de VLAN
`vrf forwarding Especial_Users`	Asignación de instancia VRF
`ip address 10.0.12.8 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::2:1 link-local`	Enlace directo

`ipv6 address 2001:db8:acad:12::2/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/0.2`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 8`	ID de VLAN
`vrf forwarding General_Users`	Asignación de instancia VRF
`ip address 10.0.12.8 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::2:2 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:12::2/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/0`	Habilitar el puerto general con el fin que las subinterfaces también se activen
`no ip Address`	
`no shutdown`	
`exit`	
`interface Ethernet1/1.1`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 13`	ID de VLAN
`vrf forwarding Especial_Users`	Asignación de instancia VRF
`ip address 10.0.23.8 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::2:3 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:23::2/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/1.2`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 8`	ID de VLAN
`vrf forwarding General_Users`	Asignación de instancia VRF
`ip address 10.0.23.8 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::2:4 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:23::2/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/1`	Habilitar el puerto general con el fin que las subinterfaces también se activen
`no ip Address`	
`no shutdown`	
`exit`	
`exit`	Salir del modo de configuración

Figura 14. Interfaces VRF en R2 activadas



Router R3

`configure terminal`	Modo de configuración de terminal
`interface Ethernet1/0.1`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 13`	ID de VLAN
`vrf forwarding Especial_Users`	Asignación de instancia VRF
`ip address 10.0.23.5 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::3:1 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:23::3/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/0.2`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 8`	ID de VLAN
`vrf forwarding General_Users`	Asignación de instancia VRF
`ip address 10.0.23.5 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::3:2 link-local`	Enlace directo
`ipv6 address 2001:db8:acad:23::3/64`	Dirección IPV6
`exit`	Salir del modo de configuración
`interface Ethernet1/0`	Habilitar el puerto general con el fin que las subinterfaces también se activen
`no ip Address`	
`no shutdown`	
`exit`	
`interface Ethernet1/1.1`	Subinterfaz en puerto Ethernet
`encapsulation dot1q 13`	ID de VLAN
`vrf forwarding Especial_Users`	Asignación de instancia VRF
`ip address 10.0.213.5 255.255.255.0`	Dirección IPV4
`no shutdown`	Habilitar la interfaz de red
`ipv6 address fe80::3:3 link-local`	Enlace directo

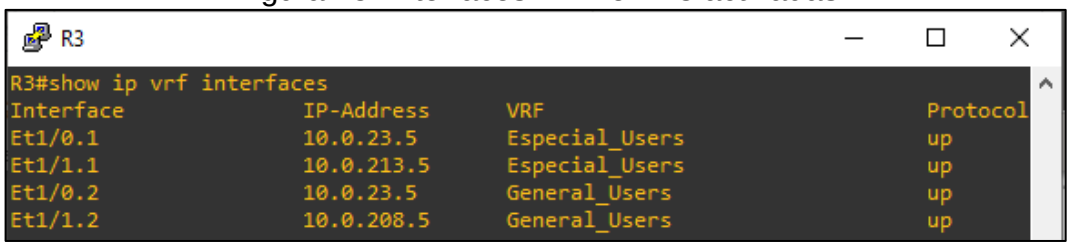
```
ipv6 address
2001:db8:acad:213::1/64
exit
interface Ethernet1/1.2
encapsulation dot1q 8
vrf forwarding General_Users
ip address 10.0.208.5
255.255.255.0
no shutdown
ipv6 address fe80::3:4 link-local
ipv6 address
2001:db8:acad:208::1/64
exit
interface Ethernet1/1
no ip Address
no shutdown
exit
exit
```

Dirección IPV6
Salir del modo de configuración
Subinterfaz en puerto Ethernet
ID de VLAN
Asignación de instancia VRF
Dirección IPV4

Habilitar la interfaz de red
Enlace directo

Dirección IPV6
Salir del modo de configuración
Habilitar el puerto general con el fin que las subinterfaces también se activen
Salir del modo de configuración

Figura 15. Interfaces VRF en R3 activadas



Tarea 2.3 Configurar las rutas estáticas para IPV4 e IPV6 en ambas VRFs.

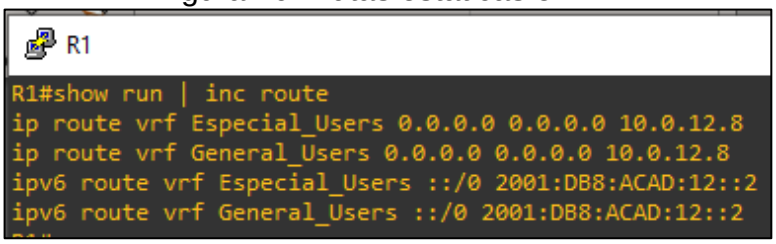
Router R1

```
ip route vrf Especial_Users
0.0.0.0 0.0.0.0 10.0.12.8
ip route vrf General_Users
0.0.0.0 0.0.0.0 10.0.12.8
ipv6 route vrf
Especial_Users ::/0
2001:DB8:ACAD:12::2
ipv6 route vrf
General_Users ::/0
2001:DB8:ACAD:12::2
```

Ruta estática para IPV4 Usuarios especiales en R2
Ruta estática para IPV4 Usuarios generales en R2
Ruta estática para IPV6 Usuarios especiales en R2

Ruta estática para IPV6 Usuarios generales en R2

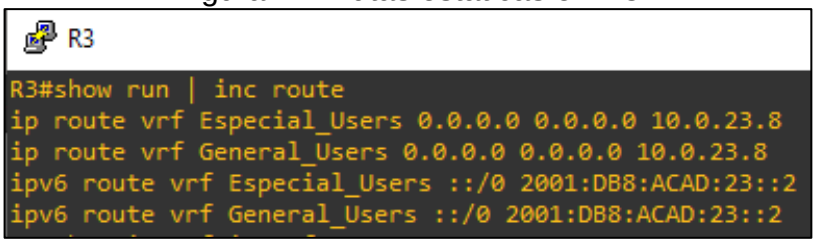
Figura 16. Rutas estáticas en R1



Router R3

`ip route vrf Especial_Users 0.0.0.0 0.0.0.0 10.0.23.8`	Ruta estática para IPV4 Usuarios especiales en R2
`ip route vrf General_Users 0.0.0.0 0.0.0.0 10.0.23.8`	Ruta estática para IPV4 Usuarios generales en R2
`ipv6 route vrf Especial_Users ::/0 2001:DB8:ACAD:23::2`	Ruta estática para IPV6 Usuarios especiales en R2
`ipv6 route vrf General_Users ::/0 2001:DB8:ACAD:23::2`	Ruta estática para IPV6 Usuarios generales en R2

Figura 17. Rutas estáticas en R3



Router R2

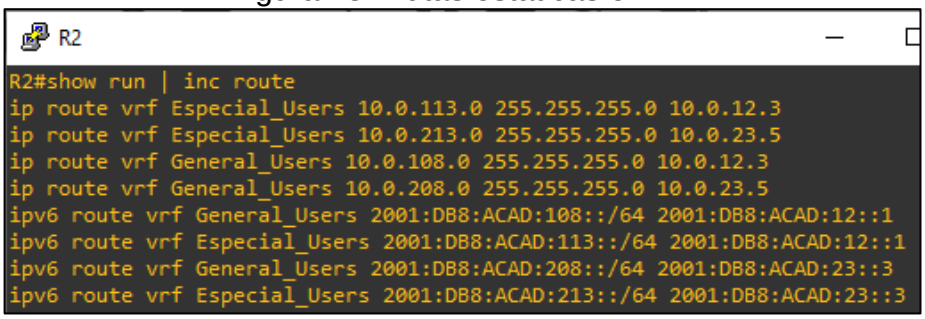
`ip route vrf Especial_Users 10.0.113.0 255.255.255.0 10.0.12.3`	Ruta estática para IPV4 Usuarios especiales en R2
`ip route vrf Especial_Users 10.0.213.0 255.255.255.0 10.0.23.5`	
`ip route vrf General_Users 10.0.208.0 255.255.255.0 10.0.23.5`	Ruta estática para IPV4 Usuarios generales en R2
`ip route vrf General_Users 10.0.108.0 255.255.255.0 10.0.12.3`	

```
ipv6 route vrf General_Users
2001:DB8:ACAD:108::/64
2001:DB8:ACAD:12::1
ipv6 route vrf Especial_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 Especial_Users
2001:DB8:ACAD:213::/64
2001:DB8:ACAD:23::3
```

Ruta estática para IPV6 Usuarios generales en R2

Ruta estática para IPV6 Usuarios generales en R2

Figura 18. Rutas estáticas en R2

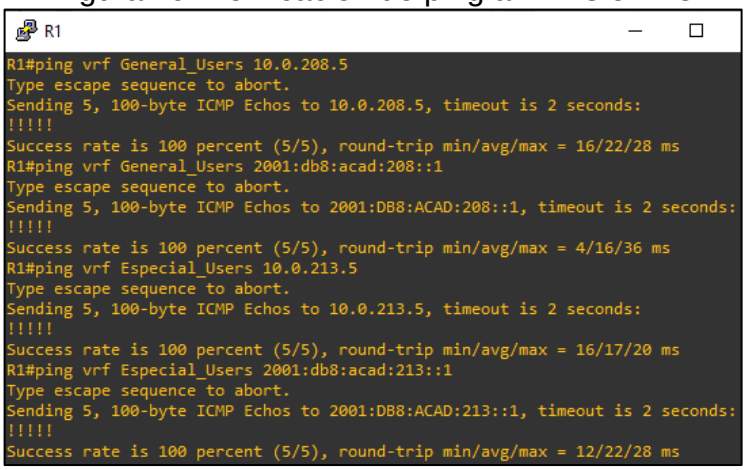


Tarea 2.4 verificar conectividad en cada VRF

Desde R1, verificar conectividad a R3:

ping vrf General_Users 10.0.208.5
ping vrf General_Users 2001:db8:acad:208::1
ping vrf Especial_Users 10.0.213.5
ping vrf Especial_Users 2001:db8:acad:213::1

Figura 19. Verificación de ping a VRFs en R3



Parte 3. Configurar capa 2

Tarea 3.1 En los switch D1, D2, y A1 desactivar todas las interfaces

Switch D1

```
configure terminal          Modo de configuración de terminal
int range e0/0-3
Shutdown
int range e1/0-3
Shutdown                    Rango de interfaces del switch
int range e2/0-3            Desactiva las interfaces seleccionadas
Shutdown
int range e3/0-3
Shutdown
exit                        Salir
```

Switch D2

```
configure terminal          Modo de configuración de terminal
int range e0/0-3
Shutdown
int range e1/0-3
Shutdown                    Rango de interfaces del switch
int range e2/0-3            Desactiva las interfaces seleccionadas
Shutdown
int range e3/0-3
Shutdown
exit                        Salir
```

Switch A1

`configure terminal`	Modo de configuración de terminal
`int range e0/0-3`	
`Shutdown`	
`int range e1/0-3`	
`Shutdown`	Rango de interfaces del switch
`int range e2/0-3`	Desactiva las interfaces seleccionadas
`Shutdown`	
`int range e3/0-3`	
`Shutdown`	
`exit`	Salir

Tarea 3.2 En los switch D1, D2 configurar enlaces troncalizados a R1 y R3

Switch D1

`configure terminal`	Modo de configuración de terminal
`int e0/2`	Interfaz conectada a R1
`switchport trunk encapsulation dot1q`	Encapsulación de VLAN en puerto de switch configurado como un enlace troncal
`switchport mode trunk`	
`switchport trunk allowed vlan 8,13`	Permite el tráfico de VLAN específicas a través de un puerto de switch configurado como un enlace troncal
`switchport mode trunk`	Puerto de switch como un enlace troncal
`no shutdown`	Activa las interfaces seleccionadas
`exit`	Salir

Switch D2

`configure terminal`	Modo de configuración de terminal
`int e0/3`	Interfaz conectada a R1
`switchport trunk encapsulation dot1q`	Encapsulación de VLAN en puerto de switch configurado como un enlace troncal
`switchport mode trunk`	
`switchport trunk allowed vlan 8,13`	Permite el tráfico de VLAN específicas a través de un puerto de switch configurado como un enlace troncal
`switchport mode trunk`	Puerto de switch como un enlace troncal
`no shutdown`	Activa las interfaces seleccionadas
`exit`	Salir

Figura 20. Interfaz troncalizada a R1

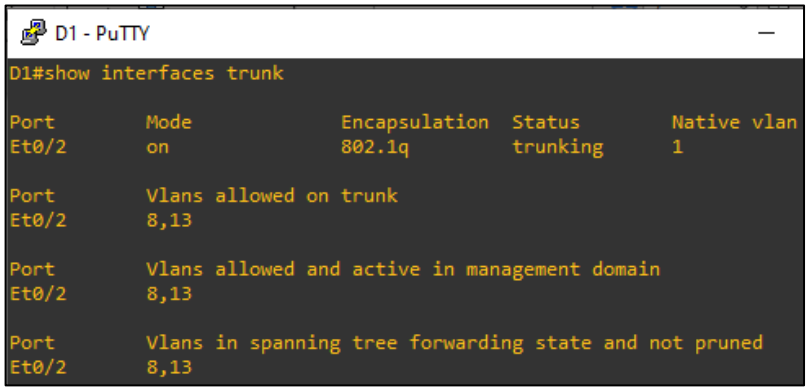
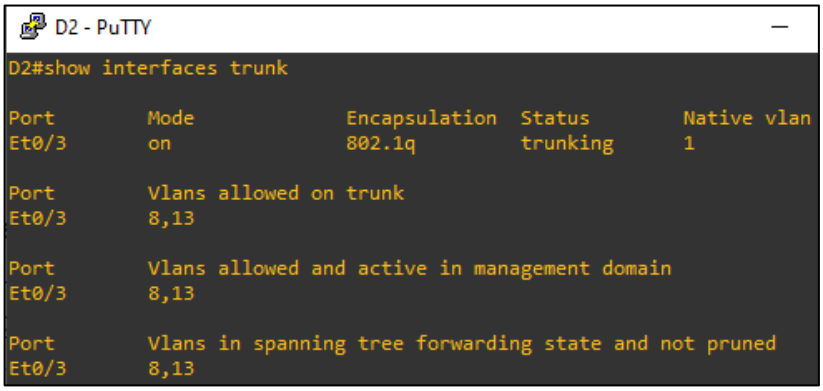


Figura 21. Interfaz troncalizada a R3



Tarea 3.3 En los switch D1 y A1 configurar el EtherChannel

Switch D1

`configure terminal`	Modo de configuración de terminal
`int range e0/0-1`	Interfaces conectadas a switch A1
`channel-group 1 mode desirable`	Habilita la agrupación de puertos en el canal 1, configura el modo como "desirable" y establece el protocolo PAgP para la negociación de enlace.
`no shutdown`	
`exit`	Salir

Switch A1

`configure terminal`	Modo de configuración de terminal
`int range e0/0-1`	Interfaces conectadas a switch D1
`channel-group 1 mode desirable`	Habilita la agrupación de puertos en el canal 1, configura el modo como "desirable" y establece el protocolo PAgP para la negociación de enlace.
`no shutdown`	
`exit`	Salir

Figura 22. Etherchannel entre Switch D1 y Switch A1

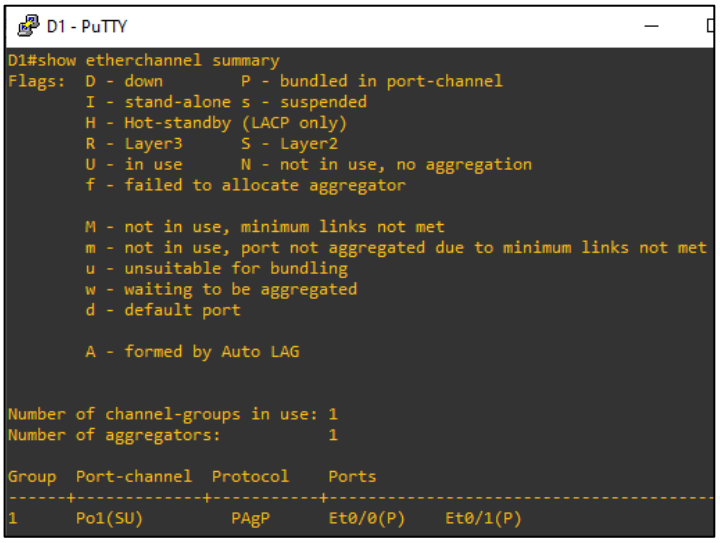
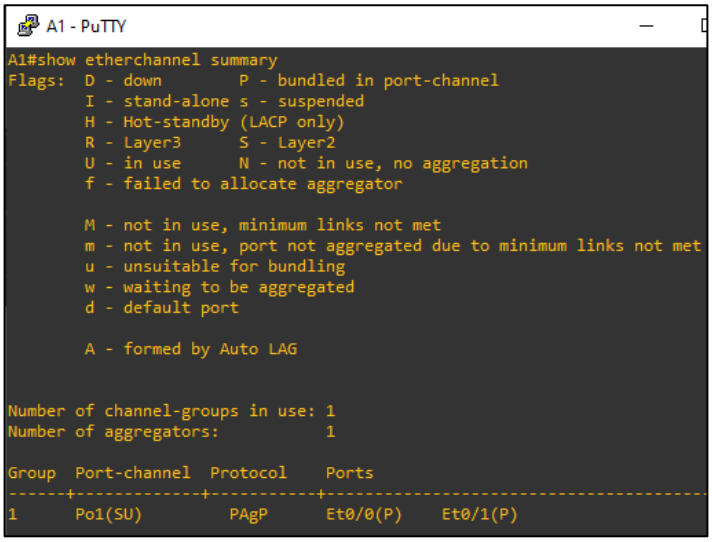


Figura 23. Etherchannel entre Switch D1 y Switch A1

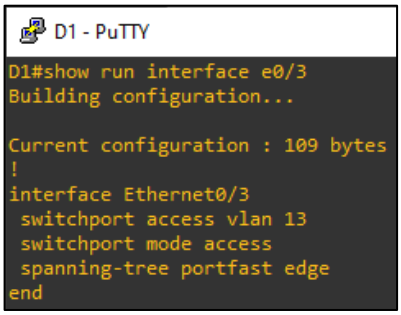


Tarea 3.4 En D1, D2 y A1, configurar los puertos de acceso para PC1, PC2, PC3 y PC4.

Switch D1 a Pc1

`configure terminal`	Modo de configuración de terminal
`int e0/3`	Interfaz conectada a PC1
`switchport mode access`	Configura la interfaz como un puerto de acceso
`switchport access vlan 13`	Asigna la VLAN 13 al puerto de acceso
`spanning-tree portfast`	Permite que la interfaz pase directamente del estado de bloqueo al estado de reenvío
`no shutdown`	
`exit`	Salir

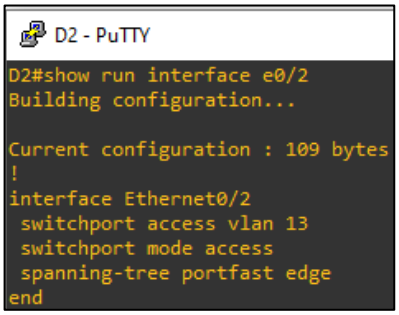
Figura 24. Puerto de acceso a Pc1



Switch D2 a Pc2

`configure terminal`	Modo de configuración de terminal
`int e0/2`	Interfaz conectada a PC2
`switchport mode access`	Configura la interfaz como un puerto de acceso
`switchport access vlan 13`	Asigna la VLAN 13 al puerto de acceso
`spanning-tree portfast`	Permite que la interfaz pase directamente del estado de bloqueo al estado de reenvío
`no shutdown`	
`exit`	Salir

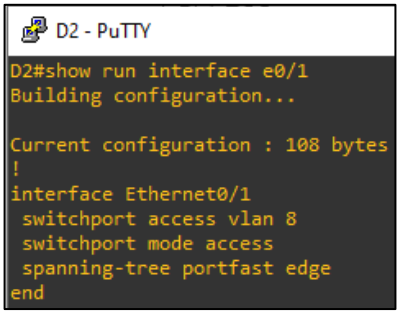
Figura 25. Puerto de acceso a Pc2



Switch D2 A Pc4

`configure terminal`	Modo de configuración de terminal
`int e0/1`	Interfaz conectada a PC4
`switchport mode access`	Configura la interfaz como un puerto de acceso
`switchport access vlan 8`	Asigna la VLAN 8 al puerto de acceso
`spanning-tree portfast`	Permite que la interfaz pase directamente del estado de bloqueo al estado de reenvío
`no shutdown`	
`exit`	Salir

Figura 26. Puerto de acceso a Pc4

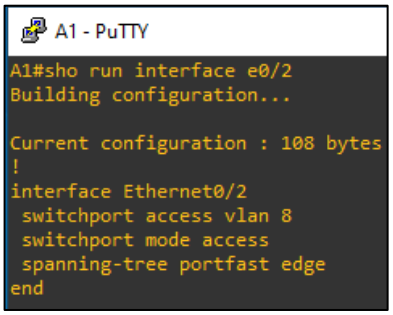


Switch A1 A Pc3

`configure terminal`	Modo de configuración de terminal
`int e0/2`	Interfaz conectada a PC3
`switchport mode access`	Configura la interfaz como un puerto de acceso

`switchport access vlan 8`	Asigna la VLAN 8 al puerto de acceso
`spanning-tree portfast`	Permite que la interfaz pase directamente del estado de bloqueo al estado de reenvío
`no shutdown`	
`exit`	Salir

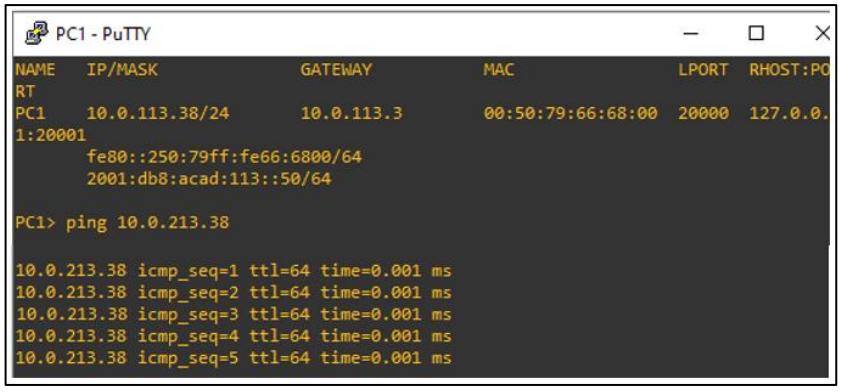
Figura 27. Puerto de acceso a Pc3



Tarea 3.5 Verificar conectividad de PC a PC

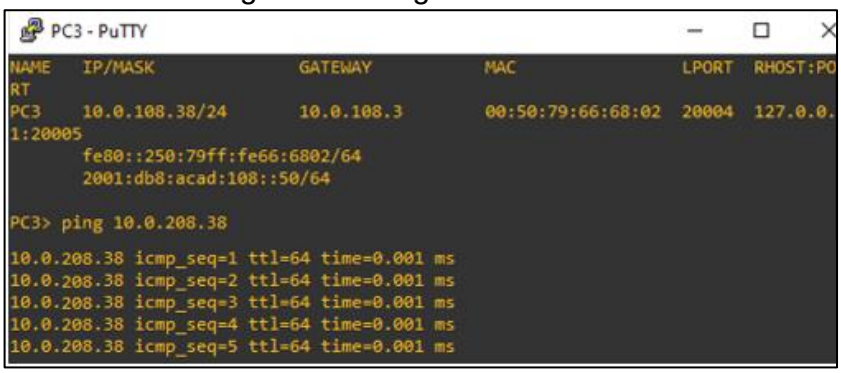
Desde PC1, verifique la conectividad IPv4 a PC2.

Figura 28. Ping de Pc1 a Pc2



Desde PC3, verifique la conectividad IPv4 e con PC4.

Figura 29. Ping de Pc3 a Pc4



Parte 4. Configurar la seguridad

Tarea 4.1 asegurar el acceso al modo EXE privilegiado

Switch A1

`configure terminal`	Modo de configuración de terminal
`enable secret algorithm scrypt`	Especifica el algoritmo de cifrado SCRYPT
`enable secret jesusbonilla385`	Contraseña deseada
`exit`	Salir

Switch D1

`configure terminal`	Modo de configuración de terminal
`enable secret algorithm scrypt`	Especifica el algoritmo de cifrado SCRYPT
`enable secret jesusbonilla385`	Contraseña deseada
`exit`	Salir

Switch D2

`configure terminal`	Modo de configuración de terminal
`enable secret algorithm scrypt`	Especifica el algoritmo de cifrado SCRYPT
`enable secret jesusbonilla385`	Contraseña deseada
`exit`	Salir

Router R1

`configure terminal`	Modo de configuración de terminal
`enable secret algorithm scrypt`	Especifica el algoritmo de cifrado SCRYPT
`enable secret jesusbonilla385`	Contraseña deseada
`exit`	Salir

Router R2

`configure terminal`	Modo de configuración de terminal
`enable secret algorithm scrypt`	Especifica el algoritmo de cifrado SCRYPT
`enable secret jesusbonilla385`	Contraseña deseada
`exit`	Salir

Router R3

`configure terminal`	Modo de configuración de terminal
`enable secret algorithm scrypt`	Especifica el algoritmo de cifrado SCRYPT
`enable secret jesusbonilla385`	Contraseña deseada
`exit`	Salir

Tarea 4.2 crear una cuenta de usuario local

Switch A1

`configure terminal`	Modo de configuración de terminal
`username admin algorithm-type scrypt secret jesusbonilla385`	Nombre de usuario Contraseña deseada
`username admin privilege 15`	Nivel de privilegio 15 para el usuario local
`exit`	Salir

Switch D1

`configure terminal`	Modo de configuración de terminal Nombre de usuario

`username admin algorithm-type scrypt secret jesusbonilla385`	Contraseña deseada
`username admin privilege 15`	Nivel de privilegio 15 para el usuario local
`exit`	Salir

Switch D2

`configure terminal`	Modo de configuración de terminal
`username admin algorithm-type scrypt secret jesusbonilla385`	Nombre de usuario Contraseña deseada
`username admin privilege 15`	Nivel de privilegio 15 para el usuario local
`exit`	Salir

Router R1

`configure terminal`	Modo de configuración de terminal
`username admin algorithm-type scrypt secret jesusbonilla385`	Nombre de usuario Contraseña deseada
`username admin privilege 15`	Nivel de privilegio 15 para el usuario local
`exit`	Salir

Router R2

`configure terminal`	Modo de configuración de terminal
`username admin algorithm-type scrypt secret jesusbonilla385`	Nombre de usuario Contraseña deseada
`username admin privilege 15`	Nivel de privilegio 15 para el usuario local
`exit`	Salir

Router R3

`configure terminal`	Modo de configuración de terminal
`username admin algorithm-type 38cript secret jesusbonilla385`	Nombre de usuario Contraseña deseada
`username admin privilege 15`	Nivel de privilegio 15 para el usuario local
`exit`	Salir

Tarea 4.3 Habilitar autenticación AAA usando la base de datos local en todas las líneas.

Switch A1

`configure terminal`	Modo de configuración de terminal
`aaa new-model`	Habilita la autenticación AAA para todas las líneas
`username admin secret jesusbonilla385`	Crea una base de datos de usuarios locales
`aaa authentication login default local`	Método de autenticación
`exit`	Salir

Switch D1

`configure terminal`	Modo de configuración de terminal
`aaa new-model`	Habilita la autenticación AAA para todas las líneas
`username admin secret jesusbonilla385`	Crea una base de datos de usuarios locales
`aaa authentication login default local`	Método de autenticación
`exit`	Salir

Switch D2

`configure terminal`	Modo de configuración de terminal
`aaa new-model`	Habilita la autenticación AAA para todas las líneas
`username admin secret jesusbonilla385`	Crea una base de datos de usuarios locales
`aaa authentication login default local`	Método de autenticación
`exit`	Salir

Router R1

`configure terminal`	Modo de configuración de terminal
`aaa new-model`	Habilita la autenticación AAA para todas las líneas
`username admin secret jesusbonilla385`	Crea una base de datos de usuarios locales
`aaa authentication login default local`	Método de autenticación
`exit`	Salir

Router R2

`configure terminal`	Modo de configuración de terminal
`aaa new-model`	Habilita la autenticación AAA para todas las líneas
`username admin secret jesusbonilla385`	Crea una base de datos de usuarios locales
`aaa authentication login default local`	Método de autenticación
`exit`	Salir

Router R3

`configure terminal`	Modo de configuración de terminal
`aaa new-model`	Habilita la autenticación AAA para todas las líneas
`username admin secret jesusbonilla385`	Crea una base de datos de usuarios locales
`aaa authentication login default local`	Método de autenticación
`exit`	Salir

Figura 30. Autenticación AAA en Switch A1

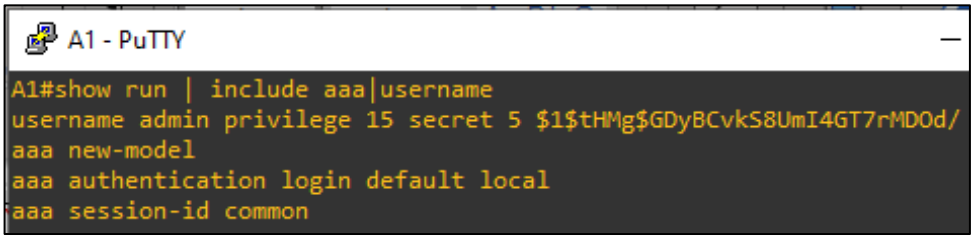


Figura 31. Autenticación AAA en Switch D1

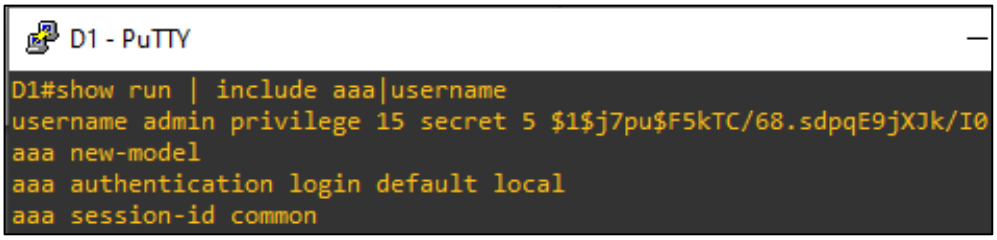


Figura 32. Autenticación AAA en Switch D2

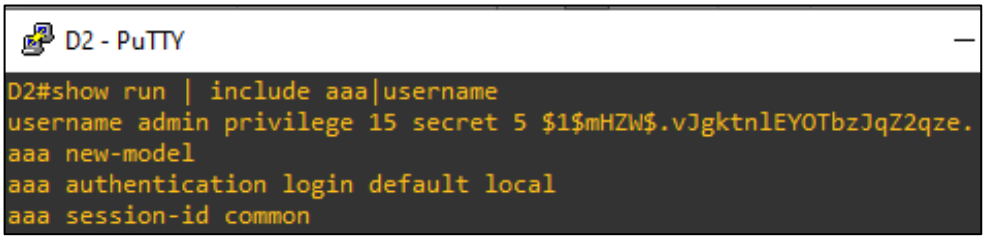


Figura 33. Autenticación AAA en Router R1

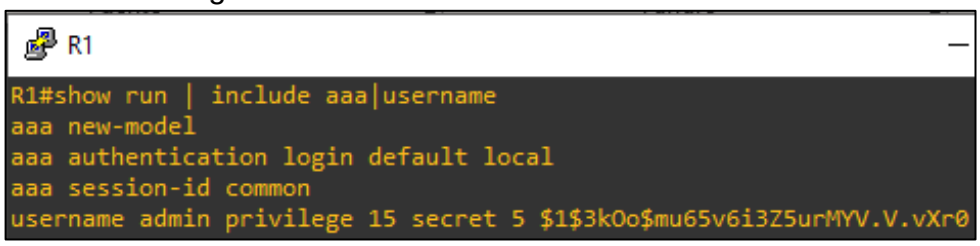


Figura 34. Autenticación AAA en Router R2

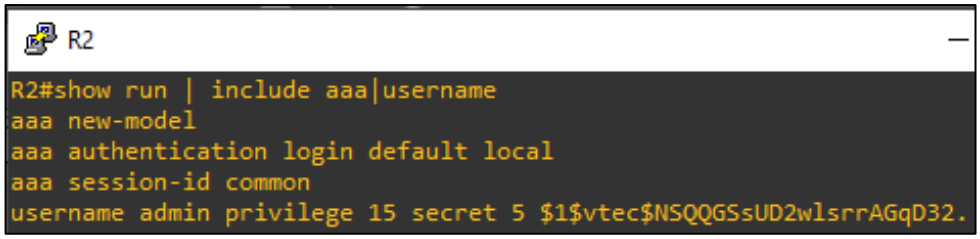
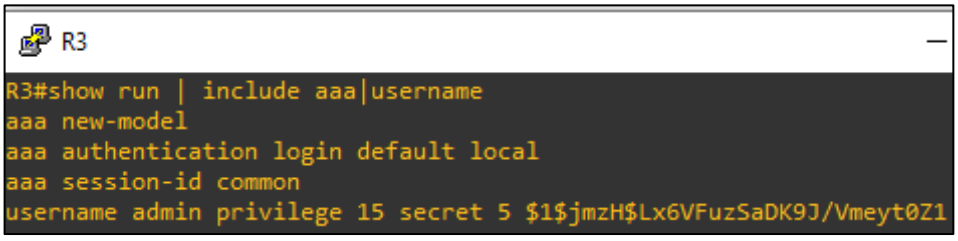


Figura 35. Autenticación AAA en Router R3



CONCLUSIONES

La construcción del escenario de vrf en GNS3, planteó grandes desafíos en varios sentidos y uno de ellos fue la necesidad de información, pues contenía puntos clave en la programación de los dispositivos y un solo error en el código o en alguno innecesariamente ingresado podría presentar falla al momento de corroborar la funcionalidad de la red.

El escenario de configuración de switches con puertos de acceso y autenticación AAA demostró la importancia de implementar medidas de seguridad para proteger la red empresarial de acceso no autorizado. La creación de VLANs, la configuración de puertos de switch y la implementación de autenticación AAA ayudaron a restringir el acceso no autorizado a la red y aseguraron el tráfico de datos. En general, estas configuraciones mejoran la seguridad y la disponibilidad de la red, lo que es esencial en un entorno empresarial en constante evolución.

La configuración de VRF en un entorno empresarial es una técnica importante para garantizar la seguridad y el aislamiento de múltiples instancias de red. En el escenario resuelto de configuración de VRF en el software GNS3, se crearon cuatro VRF separados, dos en cada VLAN. Esto permitió que los dispositivos de red en diferentes VLANs compartieran el mismo hardware de enrutamiento, pero mantuvieran una completa separación en términos de direcciones IP y tablas de enrutamiento.

BIBLIOGRAFÍA

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). Enterprise Network Architecture. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8