

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

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	9
RESUMEN.....	10
ABSTRACT.....	11
INTRODUCCIÓN	12
DESARROLLO	13
1.Escenario 1	13
CONCLUSIONES	31
BIBLIOGRAFÍA.....	43

LISTA DE TABLAS

Tabla 1. Direccionamiento general en la topología.....	12
Tabla 2. Tareas que realizar en la creación de instancias virtuales de enrutamiento.....	19

LISTA DE FIGURAS

Figura 1. Topología propuesta en GNS3	13
Figura 2. Topología cableada en GNS3.....	14
Figura 3. Configuración guardada en R1	15
Figura 4. Configuración guardada en R2	16
Figura 5. Configuración guardada en R3	16
Figura 6. Configuración guardada en D1	17
Figura 7. Configuración guardada en D2	17
Figura 8. Configuración guardada en A1	18
Figura 9. Direcciones IPV4 IPV6 en PC1	19
Figura 10. Direcciones IPV4 IPV6 en PC2.....	19
Figura 11. Direcciones IPV4 IPV6 en PC3.....	19
Figura 12. Direcciones IPV4 IPV6 en PC4.....	20
Figura 13. Interfaces VRF en R1 activadas	23
Figura 14. Interfaces VRF en R2 activadas	25
Figura 15. Interfaces VRF en R3 activadas	26
Figura 16. Rutas estáticas en R1.....	27
Figura 17. Rutas estáticas en R3.....	27
Figura 18. Rutas estáticas en R2.....	28
Figura 19. Verificación de ping a VRFs en R3.....	51
Figura 20. Interfaz troncalizada a R1	31
Figura 21. Interfaz troncalizada a R3.....	54
Figura 22. Etherchannel entre Switch D1 y Switch A1	32
Figura 23. Etherchannel entre Switch D1 y Switch A1	
Figura 24. Puerto de acceso a Pc1	33
Figura 25. Puerto de acceso a Pc2.....	34
Figura 26. Puerto de acceso a Pc4.....	34
Figura 27. Puerto de acceso a Pc3.....	35
Figura 28. Ping de Pc1 a Pc2	35
Figura 29. Ping de Pc3 a Pc4	36

Figura 30. Autenticación AAA en Switch A1	40
Figura 31. Autenticación AAA en Switch D1	40
Figura 32. Autenticación AAA en Switch D2	41
Figura 33. Autenticación AAA en Router R1	41
Figura 34. Autenticación AAA en Router R2	41
Figura 35. Autenticación AAA en Router R3	41

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

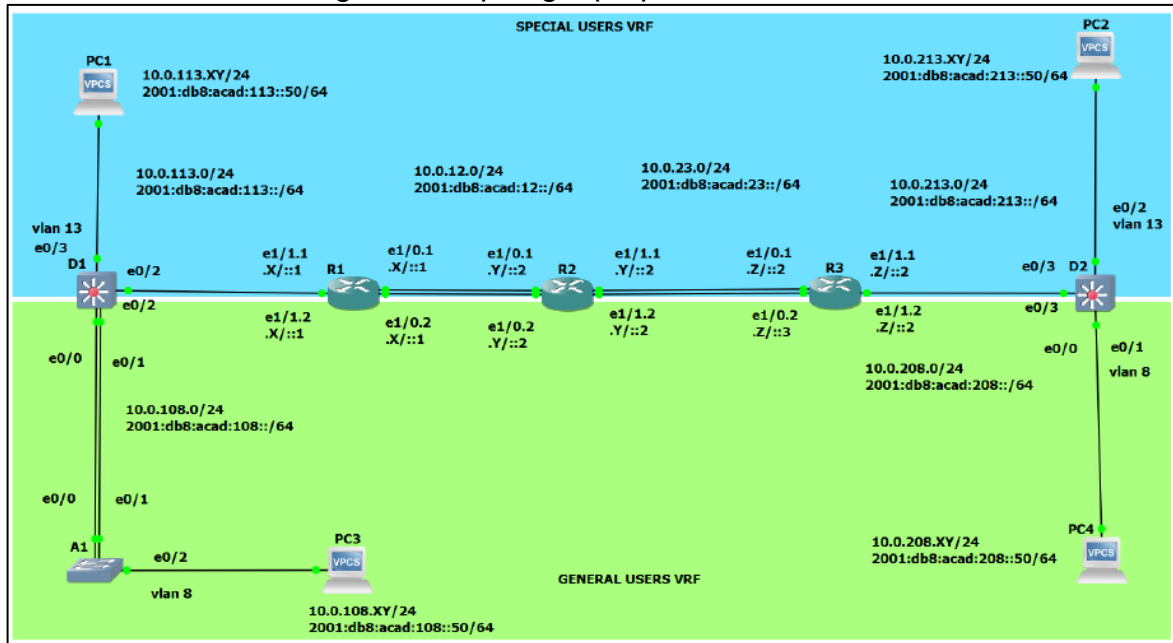


Tabla 1. Direccionamiento general en la topología

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.

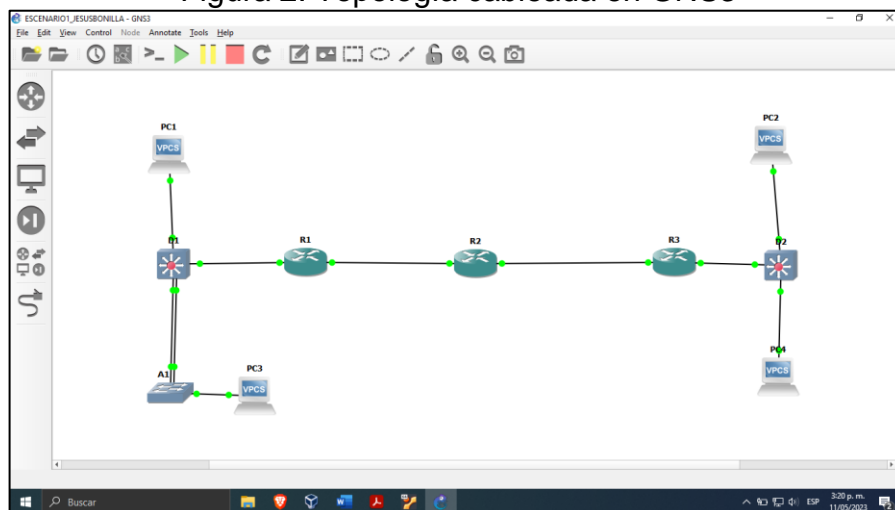
Instrucciones

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.

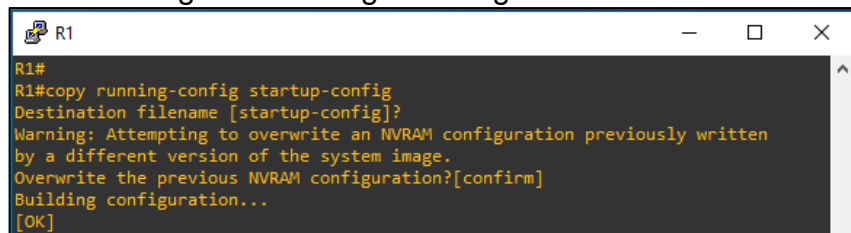
- a. Ingresar al modo de configuración global en cada uno de los dispositivos y aplicar la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.

Router R1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, 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 3. Configuración guardada en R1

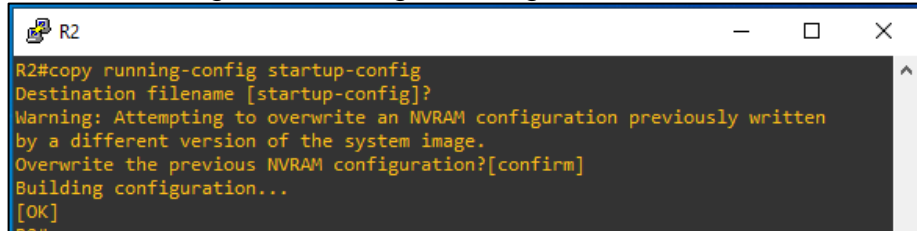


Router R2

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, 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 4. Configuración guardada en R2



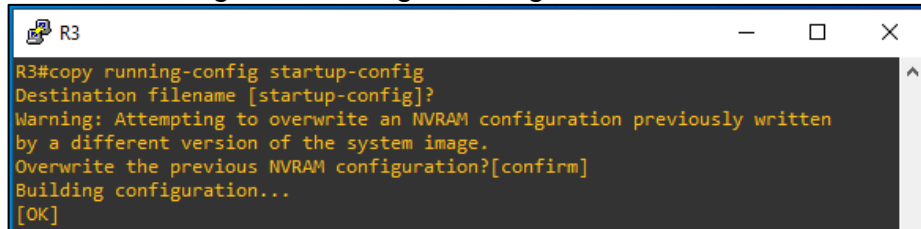
```
R2
R2#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

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
Cerrar sesión automática por inactividad
Evitar mensajes se intercalen con comandos
Salir del modo de configuración

Figura 5. Configuración guardada en R3



```
R3
R3#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

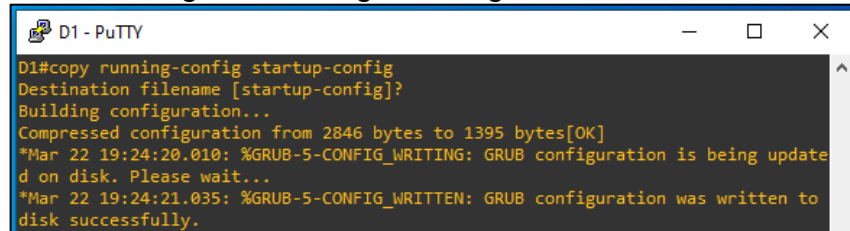
Switch D1

```
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
Cerrar 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	

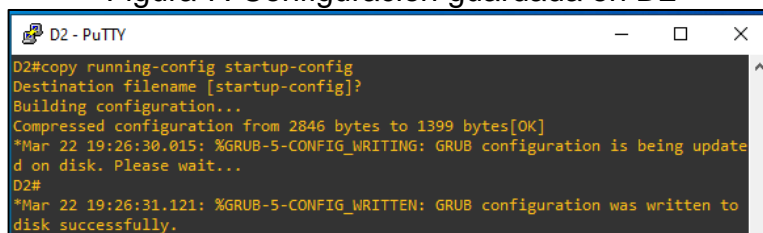
Figura 6. Configuración guardada en D1



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. Configuración guardada en D2

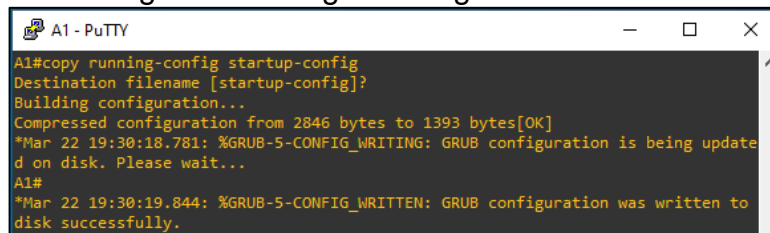


Switch A1

```
hostname A1
ipv6 unicast-routing
no ip domain lookup
banner motd # A1, ENCOR
Skills Assessment,
Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 8
name General_Users
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
Crea la VLAN identificada con 8
Nombra la VLAN creada
Salir del modo de configuración

Figura 8. Configuración guardada en A1



```
A1 - PuTTY
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2846 bytes to 1393 bytes[OK]
*Mar 22 19:30:18.781: %GRUB-5-CONFIG_WRITING: GRUB configuration is being update
d on disk. Please wait...
A1#
*Mar 22 19:30:19.844: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to
disk successfully.
```

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

```

PC1 - PuTTY
PC1> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO
RT
PC1      10.0.113.38/24  10.0.113.3   00:50:79:66:68:03  20008  127.0.0.
1:20009
fe80::250:79ff:fe66:6803/64
2001:db8:acad:113::50/64
    
```

Pc2

```

ip 10.0.213.38/24 10.0.213.5   Dirección IPV4 y gateway
ip 2001:db8:acad:213::50/64   Dirección IPV6
save                           Guardar configuración
show                            Mostrar datos PC
    
```

Figura 10. Direcciones IPV4 IPV6 en PC2

```

PC2 - PuTTY
PC2> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO
RT
PC2      10.0.213.38/24  10.0.213.5   00:50:79:66:68:02  20010  127.0.0.
1:20011
fe80::250:79ff:fe66:6802/64
2001:db8:acad:213::50/64
    
```

Pc3

```

ip 10.0.108.38/24 10.0.108.3   Dirección IPV4 y gateway
ip 2001:db8:acad:108::50/64   Dirección IPV6
save                           Guardar configuración
show                            Mostrar datos PC
    
```

Figura 11. Direcciones IPV4 IPV6 en PC3

```

PC3 - PuTTY
PC3> show

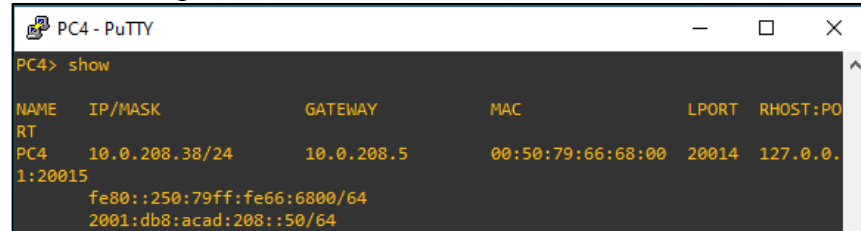
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO
RT
PC3      10.0.108.38/24  10.0.108.3   00:50:79:66:68:01  20012  127.0.0.
1:20013
fe80::250:79ff:fe66:6801/64
2001:db8:acad:108::50/64
    
```

Pc4

```
ip 10.0.208.38/24 10.0.208.5
ip 2001:db8:acad:208::50/64
save
show
```

Dirección IPv4 y gateway
Dirección IPv6
Guardar configuración
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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> In the Especial Users VRF Use dot1q encapsulation IPv4 and IPv6 GUA and link-local addresses Enable the interfaces Sub-interface 2: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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
vrf definition General_Users
address-family ipv4
exit
address-family ipv6
exit
vrf definition Especial_Users
address-family ipv4
exit
address-family ipv6
exit

```

Modo de configuración de terminal
 Creación y definición de VRF
 Habilitación de IPV4
 Salir del modo de configuración
 Habilitación de IPV6
 Salir del modo de configuración
 Creación y definición de VRF
 Habilitación de IPV4
 Salir del modo de configuración
 Habilitación de IPV6
 Salir del modo de configuración

Router R2

```

configure terminal
vrf definition General_Users
address-family ipv4
exit
address-family ipv6
exit
vrf definition Especial_Users
address-family ipv4
exit
address-family ipv6
exit

```

Modo de configuración de terminal
 Creación y definición de VRF
 Habilitación de IPV4
 Salir del modo de configuración
 Habilitación de IPV6
 Salir del modo de configuración
 Creación y definición de VRF
 Habilitación de IPV4
 Salir del modo de configuración
 Habilitación de IPV6
 Salir del modo de configuración

Router R3

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

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

Router R1

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

```

interface Ethernet1/1.1
encapsulation dot1q 13
vrf forwarding Especial_Users
ip address 10.0.113.3
255.255.255.0
no shutdown
ipv6 address fe80::1:3 link-local
ipv6 address
2001:db8:acad:113::1/64
exit
interface Ethernet1/1.2
encapsulation dot1q 8
vrf forwarding General_Users
ip address 10.0.108.3
255.255.255.0
no shutdown
ipv6 address fe80::1:4 link-local
ipv6 address
2001:db8:acad:108::1/64
exit
interface Ethernet1/1
no ip Address
no shutdown
exit
exit

```

ID de VLAN
Asignación de instancia VRF
Dirección IPv4

Habilitar la interfaz de red
Enlace directo

Dirección IPv6
Salir del modo de configuración
Subinterfaz en puerto Ethernet
ID de VLAN

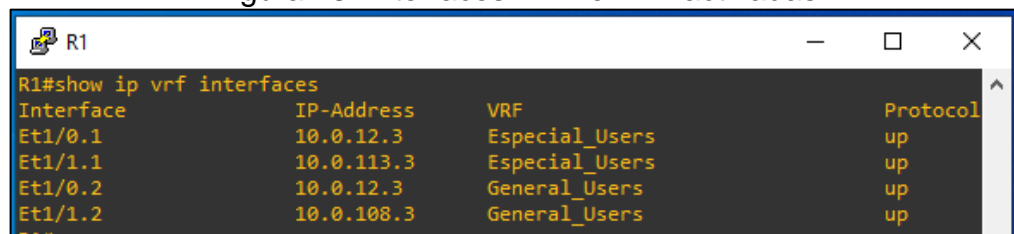
Asignación de instancia VRF
Dirección IPv4
Habilitar la interfaz de red
Enlace directo
Dirección IPv6

Salir del modo de configuración

Habilitar el puerto general con el fin que las subinterfaces también se activen

Salir del modo de configuración

Figura 13. Interfaces VRF en R1 activadas



Router R2

```

configure terminal
interface Ethernet1/0.1
encapsulation dot1q 13
vrf forwarding Especial_Users
ip address 10.0.12.8
255.255.255.0
no shutdown
ipv6 address fe80::2:1 link-local

```

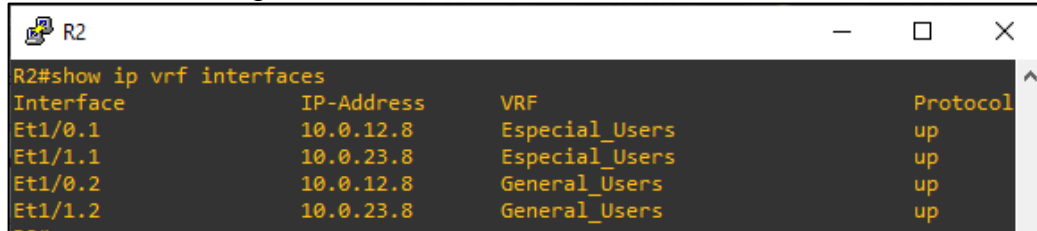
Modo de configuración de terminal
Subinterfaz en puerto Ethernet
ID de VLAN

Asignación de instancia VRF
Dirección IPv4

Habilitar la interfaz de red
Enlace directo

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

Figura 14. Interfaces VRF en R2 activadas



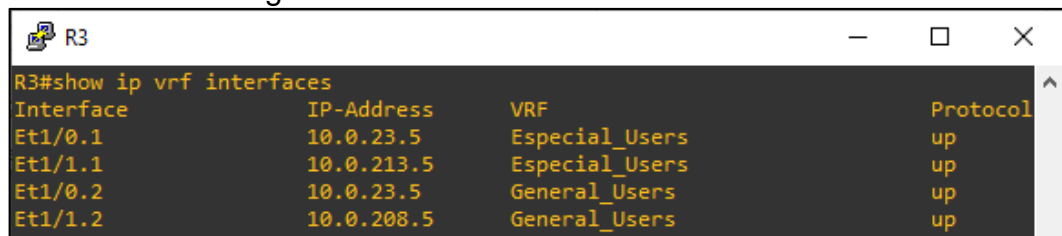
Interface	IP-Address	VRF	Protocol
Et1/0.1	10.0.12.8	Especial_Users	up
Et1/1.1	10.0.23.8	Especial_Users	up
Et1/0.2	10.0.12.8	General_Users	up
Et1/1.2	10.0.23.8	General_Users	up

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	Dirección IPv4
255.255.255.0	
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	Dirección IPv4
255.255.255.0	
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 subinterfases 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	Dirección IPv4
255.255.255.0	
no shutdown	Habilitar la interfaz de red
ipv6 address fe80::3:3 link-local	Enlace directo

ipv6 address	Dirección IPV6
2001:db8:acad:213::1/64	Salir del modo de configuración
exit	Subinterfaz en puerto Ethernet
interface Ethernet1/1.2	ID de VLAN
encapsulation dot1q 8	Asignación de instancia VRF
vrf forwarding General_Users	Dirección IPV4
ip address 10.0.208.5	
255.255.255.0	
no shutdown	Habilitar la interfaz de red
ipv6 address fe80::3:4 link-local	Enlace directo
ipv6 address	
2001:db8:acad:208::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 15. Interfaces VRF en R3 activadas



Interface	IP-Address	VRF	Protocol
Et1/0.1	10.0.23.5	Especial_Users	up
Et1/1.1	10.0.213.5	Especial_Users	up
Et1/0.2	10.0.23.5	General_Users	up
Et1/1.2	10.0.208.5	General_Users	up

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

Router R1

ip route vrf Especial_Users	Ruta estática para IPV4 Usuarios especiales en R2
0.0.0.0 0.0.0.0 10.0.12.8	
ip route vrf General_Users	Ruta estática para IPV4 Usuarios generales en R2
0.0.0.0 0.0.0.0 10.0.12.8	
ipv6 route vrf	Ruta estática para IPV6 Usuarios especiales en R2
Especial_Users ::/0	
2001:DB8:ACAD:12::2	
ipv6 route vrf	Ruta estática para IPV6 Usuarios generales en R2
General_Users ::/0	
2001:DB8:ACAD:12::2	

Figura 16. Rutas estáticas en R1

```
R1#show run | inc route
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
```

Router R3

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

Figura 17. Rutas estáticas en R3

```
R3#show run | inc route
ip route vrf Especial_Users 0.0.0.0 0.0.0.0 10.0.23.8
ip route vrf General_Users 0.0.0.0 0.0.0.0 10.0.23.8
ipv6 route vrf Especial_Users ::/0 2001:DB8:ACAD:23::2
ipv6 route vrf General_Users ::/0 2001:DB8:ACAD:23::2
```

Router R2

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

```

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

```

R2#show run | inc route
ip route vrf Especial_Users 10.0.113.0 255.255.255.0 10.0.12.3
ip route vrf Especial_Users 10.0.213.0 255.255.255.0 10.0.23.5
ip route vrf General_Users 10.0.108.0 255.255.255.0 10.0.12.3
ip route vrf General_Users 10.0.208.0 255.255.255.0 10.0.23.5
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

```

Tarea 2.4 verificar conectividad en cada VRF

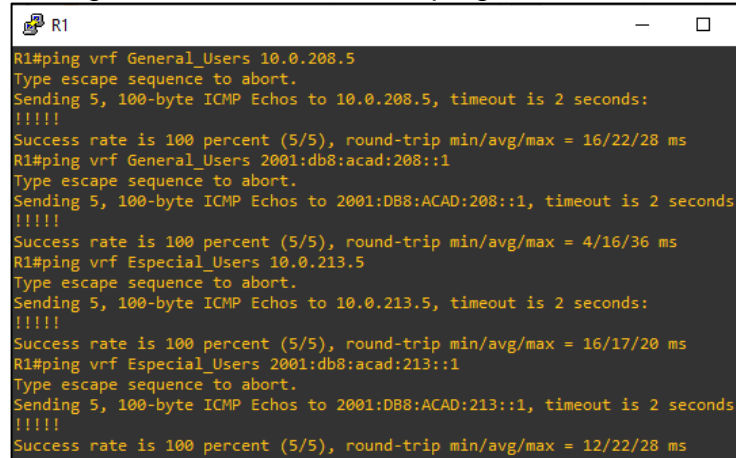
Desde R1, verificar conectividad a R3:

```

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



```
R1#ping vrf General_Users 10.0.208.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/22/28 ms
R1#ping vrf General_Users 2001:db8:acad:208::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/16/36 ms
R1#ping vrf Especial_Users 10.0.213.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/20 ms
R1#ping vrf Especial_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 = 12/22/28 ms
```

Parte 3. Configurar capa 2

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

Switch D1

```
configure terminal
int range e0/0-3
Shutdown
int range e1/0-3
Shutdown
int range e2/0-3
Shutdown
int range e3/0-3
Shutdown
exit
```

Modo de configuración de terminal

Rango de interfaces del switch
Desactiva las interfaces seleccionadas

Salir

Switch D2

```
configure terminal
int range e0/0-3
Shutdown
int range e1/0-3
Shutdown
int range e2/0-3
Shutdown
int range e3/0-3
Shutdown
exit
```

Modo de configuración de terminal

Rango de interfaces del switch
Desactiva las interfaces seleccionadas

Salir

Switch A1

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

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

Switch D1

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

Switch D2

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

Figura 20. Interfaz troncalizada a R1

```
D1 - PuTTY
D1#show interfaces trunk

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

Port      Vlans allowed on trunk
Et0/2     8,13

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

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

Figura 21. Interfaz troncalizada a R3

```
D2 - PuTTY
D2#show interfaces trunk

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

Port      Vlans allowed on trunk
Et0/3     8,13

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

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

Tarea 3.3 En los switch D1 y A1 configurar el EtherChannel

Switch D1

```
configure terminal
int range e0/0-1
channel-group 1
mode desirable
no shutdown
exit
```

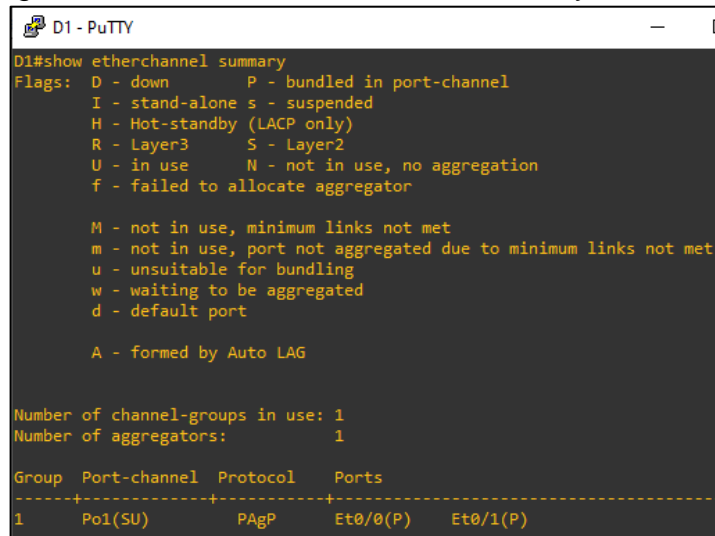
Modo de configuración de terminal
Interfaces conectadas a switch A1
Habilita la agrupación de puertos en el canal 1,
configura el modo como "desirable" y establece el
protocolo PAgP para la negociación de enlace.
Salir

Switch A1

```
configure terminal
int range e0/0-1
channel-group 1
mode desirable
no shutdown
exit
```

Modo de configuración de terminal
Interfaces conectadas a switch D1
Habilita la agrupación de puertos en el canal 1,
configura el modo como "desirable" y establece el
protocolo PAgP para la negociación de enlace.
Salir

Figura 22. Etherchannel entre Switch D1 y Switch A1



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

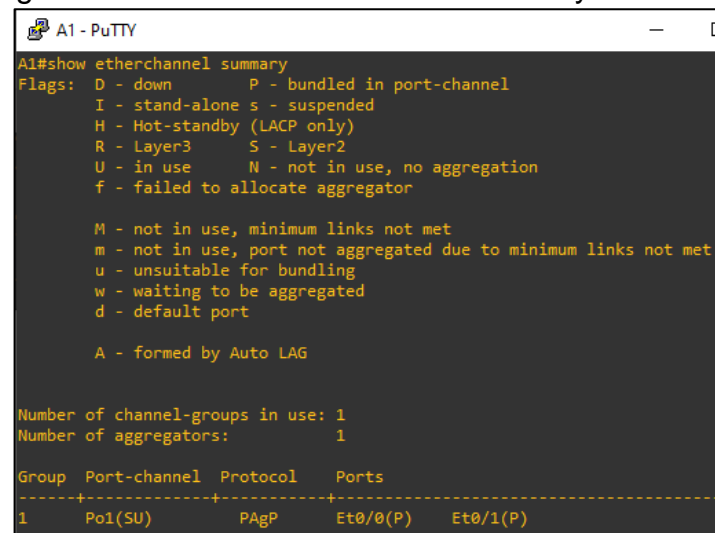
       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

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

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

Figura 23. Etherchannel entre Switch D1 y Switch A1



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

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

       A - formed by Auto LAG

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

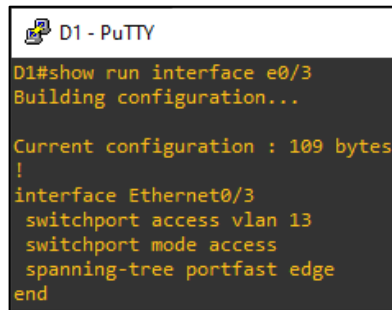
Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        PAgP        Et0/0(P)  Et0/1(P)
```


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

Switch D1 a Pc1

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

Figura 24. Puerto de acceso a Pc1



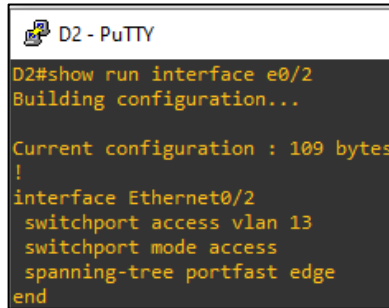
```
D1 - PuTTY
D1#show run interface e0/3
Building configuration...

Current configuration : 109 bytes
!
interface Ethernet0/3
  switchport access vlan 13
  switchport mode access
  spanning-tree portfast edge
end
```

Switch D2 a Pc2

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

Figura 25. Puerto de acceso a Pc2



```
D2 - PuTTY
D2#show run interface e0/2
Building configuration...

Current configuration : 109 bytes
!
interface Ethernet0/2
 switchport access vlan 13
 switchport mode access
 spanning-tree portfast edge
end
```

Switch D2 A Pc4

```
configure
terminal
int e0/1
switchport mode
access
switchport access
vlan 8
spanning-tree
portfast
no shutdown
exit
```

Modo de configuración de terminal

Interfaz conectada a PC4

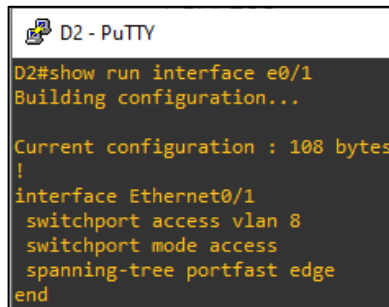
Configura la interfaz como un puerto de acceso

Asigna la VLAN 8 al puerto de acceso

Permite que la interfaz pase directamente del estado de bloqueo al estado de reenvío

Salir

Figura 26. Puerto de acceso a Pc4



```
D2 - PuTTY
D2#show run interface e0/1
Building configuration...

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

Switch A1 A Pc3

```
configure
terminal
int e0/2
switchport mode
access
```

Modo de configuración de terminal

Interfaz conectada a PC3

Configura la interfaz como un puerto de acceso

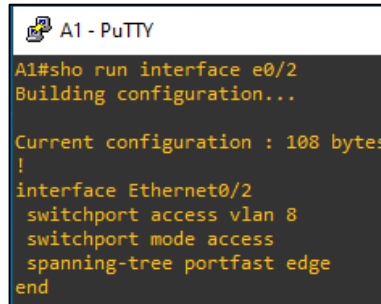
```
switchport access
vlan 8
spanning-tree
portfast
no shutdown
exit
```

Asigna la VLAN 8 al puerto de acceso

Permite que la interfaz pase directamente del estado de bloqueo al estado de reenvío

Salir

Figura 27. Puerto de acceso a Pc3



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

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

Tarea 3.5 Verificar conectividad de PC a PC

Desde PC1, verifique la conectividad IPv4 a PC2.

Figura 28. Ping de Pc1 a Pc2



```
PC1 - PuTTY
NAME IP/MASK GATEWAY MAC LPORT RHOST:PC
RT
PC1 10.0.113.38/24 10.0.113.3 00:50:79:66:68:00 20000 127.0.0.
1:20001
 fe80::250:79ff:fe66:6800/64
 2001:db8:acad:113::50/64

PC1> ping 10.0.213.38

10.0.213.38 icmp_seq=1 ttl=64 time=0.001 ms
10.0.213.38 icmp_seq=2 ttl=64 time=0.001 ms
10.0.213.38 icmp_seq=3 ttl=64 time=0.001 ms
10.0.213.38 icmp_seq=4 ttl=64 time=0.001 ms
10.0.213.38 icmp_seq=5 ttl=64 time=0.001 ms
```

Desde PC3, verifique la conectividad IPv4 e con PC4.

Figura 29. Ping de Pc3 a Pc4



```
PC3 - PuTTY
NAME IP/MASK GATEWAY MAC LPORT RHOST:PO
RT
PC3 10.0.108.38/24 10.0.108.3 00:50:79:66:68:02 20004 127.0.0.
1:20005
fe80::250:79ff:fe66:6802/64
2001:db8:acad:108::50/64

PC3> ping 10.0.208.38

10.0.208.38 icmp_seq=1 ttl=64 time=0.001 ms
10.0.208.38 icmp_seq=2 ttl=64 time=0.001 ms
10.0.208.38 icmp_seq=3 ttl=64 time=0.001 ms
10.0.208.38 icmp_seq=4 ttl=64 time=0.001 ms
10.0.208.38 icmp_seq=5 ttl=64 time=0.001 ms
```

Parte 4. Configurar la seguridad

Tarea 4.1 asegurar el acceso al modo EXE privilegiado

Switch A1

```
configure terminal
enable secret algorithm
script
enable secret
jesusbonilla385
exit
```

Modo de configuración de terminal
Especifica el algoritmo de cifrado
SCRIPT
Contraseña deseada
Salir

Switch D1

```
configure terminal
enable secret algorithm
script
enable secret
jesusbonilla385
exit
```

Modo de configuración de terminal
Especifica el algoritmo de cifrado
SCRIPT
Contraseña deseada
Salir

Switch D2

```
configure terminal
enable secret algorithm
script
enable secret
jesusbonilla385
exit
```

Modo de configuración de terminal
Especifica el algoritmo de cifrado
SCRIPT
Contraseña deseada
Salir

Router R1

```
configure terminal
enable secret algorithm
script
enable secret
jesusbonilla385
exit
```

Modo de configuración de terminal
Especifica el algoritmo de cifrado
SCRYPT
Contraseña deseada
Salir

Router R2

```
configure terminal
enable secret algorithm
script
enable secret
jesusbonilla385
exit
```

Modo de configuración de terminal
Especifica el algoritmo de cifrado
SCRYPT
Contraseña deseada
Salir

Router R3

```
configure terminal
enable secret algorithm
script
enable secret
jesusbonilla385
exit
```

Modo de configuración de terminal
Especifica el algoritmo de cifrado
SCRYPT
Contraseña deseada
Salir

Tarea 4.2 crear una cuenta de usuario local

Switch A1

```
configure terminal
username admin algorithm-
type scrypt secret
jesusbonilla385
username admin privilege 15
exit
```

Modo de configuración de terminal
Nombre de usuario
Contraseña deseada
Nivel de privilegio 15 para el usuario
local
Salir

Switch D1

```
configure terminal
```

Modo de configuración de terminal
Nombre de usuario

```
username admin algorithm-  
type scrypt secret  
jesusbonilla385  
username admin privilege 15  
exit
```

Contraseña deseada
Nivel de privilegio 15 para el usuario
local
Salir

Switch D2

```
configure terminal  
username admin algorithm-  
type scrypt secret  
jesusbonilla385  
username admin privilege 15  
exit
```

Modo de configuración de terminal
Nombre de usuario
Contraseña deseada
Nivel de privilegio 15 para el usuario
local
Salir

Router R1

```
configure terminal  
username admin algorithm-  
type scrypt secret  
jesusbonilla385  
username admin privilege 15  
exit
```

Modo de configuración de terminal
Nombre de usuario
Contraseña deseada
Nivel de privilegio 15 para el usuario
local
Salir

Router R2

```
configure terminal  
username admin algorithm-  
type scrypt secret  
jesusbonilla385  
username admin privilege 15  
exit
```

Modo de configuración de terminal
Nombre de usuario
Contraseña deseada
Nivel de privilegio 15 para el usuario
local
Salir

Router R3

```
configure terminal  
username admin algorithm-  
type 38crypt secret  
jesusbonilla385  
username admin privilege 15  
exit
```

Modo de configuración de terminal
Nombre de usuario
Contraseña deseada
Nivel de privilegio 15 para el usuario
local
Salir

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

Switch A1

```
configure terminal
aaa new-model
username admin secret
jesusbonilla385
aaa authentication login
default local
exit
```

Modo de configuración de terminal
Habilita la autenticación AAA para todas las líneas

Crea una base de datos de usuarios locales

Método de autenticación

Salir

Switch D1

```
configure terminal
aaa new-model
username admin secret
jesusbonilla385
aaa authentication login
default local
exit
```

Modo de configuración de terminal
Habilita la autenticación AAA para todas las líneas

Crea una base de datos de usuarios locales

Método de autenticación

Salir

Switch D2

```
configure terminal
aaa new-model
username admin secret
jesusbonilla385
aaa authentication login
default local
exit
```

Modo de configuración de terminal
Habilita la autenticación AAA para todas las líneas

Crea una base de datos de usuarios locales

Método de autenticación

Salir

Router R1

```
configure terminal
aaa new-model
username admin secret
jesusbonilla385
aaa authentication login
default local
exit
```

Modo de configuración de terminal
Habilita la autenticación AAA para todas las líneas

Crea una base de datos de usuarios locales

Método de autenticación

Salir

Router R2

```
configure terminal
aaa new-model
username admin secret
jesusbonilla385
aaa authentication login
default local
exit
```

Modo de configuración de terminal
Habilita la autenticación AAA para todas las líneas

Crea una base de datos de usuarios locales

Método de autenticación

Salir

Router R3

```
configure terminal
aaa new-model
username admin secret
jesusbonilla385
aaa authentication login
default local
exit
```

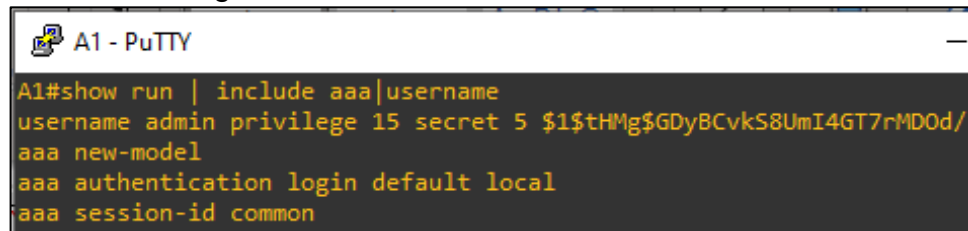
Modo de configuración de terminal
Habilita la autenticación AAA para todas las líneas

Crea una base de datos de usuarios locales

Método de autenticación

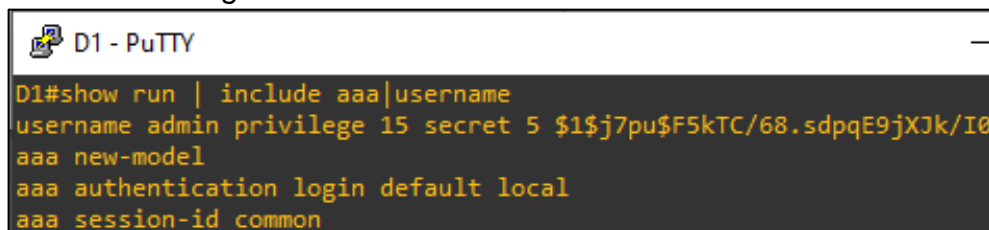
Salir

Figura 30. Autenticación AAA en Switch A1



```
A1-PuTTY
A1#show run | include aaa|username
username admin privilege 15 secret 5 $1$tHMg$GDyBCvkS8UmI4GT7rMD0d/
aaa new-model
aaa authentication login default local
aaa session-id common
```

Figura 31. Autenticación AAA en Switch D1



```
D1-PuTTY
D1#show run | include aaa|username
username admin privilege 15 secret 5 $1$j7pu$F5kTC/68.sdpqE9jXJk/I0
aaa new-model
aaa authentication login default local
aaa session-id common
```


Figura 32. Autenticación AAA en Switch D2

```
D2 - PuTTY
D2#show run | include aaa|username
username admin privilege 15 secret 5 $1$mHZW$.vJgktnlEYOTbzJqZ2qze.
aaa new-model
aaa authentication login default local
aaa session-id common
```

Figura 33. Autenticación AAA en Router R1

```
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$3k0o$mu65v6i3Z5urMYV.V.vXr0
```

Figura 34. Autenticación AAA en Router R2

```
R2
R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$vtec$NSQQGSsUD2wlSrrAGqD32.
```

Figura 35. Autenticación AAA en Router R3

```
R3
R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$jzH$Lx6VFuzSaDK9J/Vmeyt0Z1
```

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>