

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CAMILO ANDRÉS RODRÍGUEZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CAMILO ANDRÉS RODRÍGUEZ

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

TUTOR
JOHN HAROLD PÉREZ CALDERÓN

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

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

ACACIAS, 01 de mayo de 2023

CONTENIDO

LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	8
RESUMEN.....	9
Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica	9
ABSTRACT.....	10
Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.....	10
INTRODUCCIÓN	11
ESCENARIO PROPUESTO	12
Recursos requeridos:.....	12
Topología de la Red	13
Tabla de direccionamiento.....	13
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz	14
Paso 2: se procede a realizar la configuración básica de cada dispositivo, incluyendo los hosts.	15
Parte 2: configurar VRF y enrutamiento estático	22
Verificación:	34
Parte 3: configurar los Switches para soportar la conectividad con los dispositivos finales.....	35
Parte 4- configuración de seguridad en los dispositivos.....	43
CONCLUSIONES	52
REFERENTES BIBLIOGRÁFICOS.....	53

LISTA DE TABLAS

Tabla 1 - Tabla de direccionamiento.....	13
Tabla 2 - Tabla de cableado	14
Tabla 3 - Configuración básica R1	15
Tabla 4 - Configuración básica R2.....	16
Tabla 5 - Configuración básica R3.....	17
Tabla 6 - Configuración básica D1	18
Tabla 7 - Configuración básica D2.....	19
Tabla 8 - Configuración básica A1	20
Tabla 9 - Configuración básica PCs.....	21
Tabla 10 - Configuración VRFs en R1, R2 y R3	22
Tabla 11 - Configuración VRFs Special-Users y VLAN 13 en R1	23
Tabla 12 - Configuración VRFs Special-Users y VLAN 13 en R1	24
Tabla 13 - Configuración VRFs Special-Users y VLAN 13 en R2	25
Tabla 14 - Configuración VRFs General-Users y VLAN 8 en R2.....	26
Tabla 15 - Configuración VRFs Special-Users y VLAN 13 en R3.....	27
Tabla 16 - Configuración VRFs General-Users y VLAN 8 en R2.....	28
Tabla 17 - Static routes R1	29
Tabla 18 - Static routes R2	30
Tabla 19 - Static routes R3	31
Tabla 20-Configuraciones paso 3 en D1.....	36
Tabla 21-Configuraciones paso 3 en D2.....	37
Tabla 22-Configuraciones paso 3 en A1	38
Tabla 23-Configuraciones paso 4 en R1.....	44
Tabla 24-Configuraciones paso 4 en R2.....	45
Tabla 25-Configuraciones paso 4 en R3.....	46
Tabla 26-Configuraciones paso 4 en D1.....	47
Tabla 27-Configuraciones paso 4 en A1.....	48
Tabla 28-Configuraciones paso 4 en D2.....	49

LISTA DE FIGURAS

Figura 1-Topología de la Red	13
Figura 2- Red Creada	14
Figura 3 - Verificación de la configuración de R1 con el comando show running-config	15
Figura 4 - Verificación de la configuración de R2 con el comando show running-config	16
Figura 5 - Verificación de la configuración de R3 con el comando show running-config	17
Figura 6-Verificación de la configuración de D1 con el comando show running-config	18
Figura 7 - Verificación de la configuración de D2 con el comando show running-config	19
Figura 8 - Verificación de la configuración de A1 con el comando show running-config	20
Figura 9 - Configuración direcciones PC1 con el comando show	21
Figura 10 - Configuración direcciones PC2 con el comando show	21
Figura 11 - Configuración direcciones PC3 con el comando show	21
Figura 12 - Configuración direcciones PC4 con el comando show	21
Figura 13 - Definición VRFs en R2	22
Figura 14-VRFs Special-Users y VLAN 13 en R1	23
Figura 15- General-Users y VLAN 8 en R1	24
Figura 16- VRFs Special-Users y VLAN 13 en R2	25
Figura 17-VRFs General-Users y VLAN 8 en R2	26
Figura 18-VRFs Special-Users y VLAN 13 en R3	27
Figura 19-VRFs General-Users y VLAN 8 en R3	28
Figura 20 - Static routes R1	29
Figura 21-Static routes R2	30
Figura 22-Static routes R3	31
Figura 23- Verificación con el comando "show ip vrf interfaces" en R1	32
Figura 24-Verificación con el comando "show ip vrf interfaces" en R2	32
Figura 25 - Verificación con el comando "show ip vrf interfaces" en R3	32
Figura 26 - Verificación con el comando "show run inc route" en R1	33
Figura 27- Verificación con el comando "show run inc route" en R2	33
Figura 28- Verificación con el comando "show run inc route" en R3	33
Figura 29- prueba de conexión entre dispositivos usando ping en R1	34
Figura 30-prueba de conexión entre dispositivos usando ping en R3	34
Figura 31 - show etherchannel summary en A1	39
Figura 32-comando "show run interface e0/2" en A1	39
Figura 33 - show interfaces trunk en D1	40
Figura 34 - show etherchannel summary en D1	40
Figura 35-show run interface e0/3 en D1	40

Figura 36-show interfaces trunk en D2	41
Figura 37-show run interface e0/1 y e0/2 en D2	41
Figura 38-Ping de PC1 a PC2.....	42
Figura 39-Ping de PC2 a PC1.....	42
Figura 40-Ping de PC3 a PC4.....	42
Figura 41-Ping de PC4 a PC3.....	42
Figura 42-cambio de imagen ISO para los routers	43
Figura 43-Configuraciones paso 4 en R1	44
Figura 44 - Configuraciones paso 4 en R2	45
Figura 45-Configuraciones paso 4 en R3	46
Figura 46 - Configuraciones paso 4 en D1	47
Figura 47 -Configuraciones paso 4 en A1.....	48
Figura 48 - Configuraciones paso 4 en D2	49
Figura 49-Uso del comando "show run include aaa username" en R1	50
Figura 50-Uso del comando "show run include aaa username" en R2	50
Figura 51-Uso del comando "show run include aaa username" en R3	50
Figura 52-Uso del comando "show run include aaa username" en A1	51
Figura 53-Uso del comando "show run include aaa username" en D1	51
Figura 54-Uso del comando "show run include aaa username" en D2	51

GLOSARIO

ETHERCHANNEL: Sistema que permite agregar enlaces con la finalidad de aumentar el ancho de banda disponible.

PAGP: (Port Aggregation Protocol) es un protocolo propietario de Cisco. Los paquetes PAGP son intercambiados entre switch a través de los enlaces configurados para ello. Los vecinos son identificados y sus capacidades comparadas con las capacidades locales

RUTA ESTATICA: define el camino a utilizar por un paquete, añadiendo el próximo salto al que se enviará el tráfico.

VLAN: (Virtual LAN) proveen seguridad, segmentación, flexibilidad, permiten agrupar usuarios de un mismo dominio de broadcast con independencia de su ubicación física en la red. Usando la tecnología VLAN se pueden agrupar lógicamente puertos del switch y los usuarios conectados a ellos en grupos de trabajo con interés común. Una VLAN por definición es un dominio de difusión creado de forma lógica.

VRF: (Virtual Routing and Forwarding) es una instancia de enrutamiento específica para un cliente. proporciona un aislamiento de las rutas del cliente, la información que contienen debe ser intercambiada entre los diferentes routers PE. Debe ejecutarse un protocolo de enrutamiento entre todos los routers PE para intercambiar la información de enrutamiento del cliente sin involucrar a los routers

VTP: (VLAN Trunking Protocol) permite intercambiar información sobre VLAN entre trunk de forma que los switches de la red tengan la base de datos de VLAN sincronizadas en todo momento desde un punto central de la red.

RESUMEN

Día a día, la implementación de redes ha permitido que la globalización avance hasta el punto en el que nos encontramos actualmente, es por ello que el personal encargado de diseñar, implementar, mantener y configurar dichas redes, debe estar en la capacidad de hacerlo de una manera que aproveche todas las ventajas y características de los dispositivos que tiene a su alcance, así como de velar por la correcta implementación de la seguridad, evitando accesos indeseados que puedan perjudicar al usuario o empresa propietaria de la red.

Es por esto, que la empresa CISCO se encarga de capacitar y certificar personal mediante sus plataformas *Netacad* y *Cisco Skills For All*, mediante las cuales los aprendices podrán mejorar sus habilidades en telecomunicaciones, gracias a cursos y diplomados que complementen sus conocimientos y permitan lograr su certificación como aprendiz, profesional o experto.

En base a lo anterior, los aprendices del diplomado de profundización CCNP, están en capacidad de crear redes en las cuales demuestre las competencias adquiridas y pueda diseñar de manera ágil las configuraciones que permitan la implementación de VLANs, VRFs, puertos troncales y de acceso, así como el uso de EtherChannel y PAgP, entre otras habilidades, sin dejar de lado las respectivas configuraciones básicas, como lo es asignar nombres a los dispositivos o complejas como lo es establecer usuarios y claves encriptadas con el algoritmo tipo Script.

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

ABSTRACT

Day by day, the implementation of networks has allowed globalization to advance to the point where we are currently, which is why the personnel in charge of designing, implementing, maintaining and configuring said networks must be able to do so a way that takes advantage of all the advantages and characteristics of the devices at your disposal, as well as ensuring the correct implementation of security, avoiding unwanted access that could harm the user or company that owns the network.

For this reason, the CISCO company is in charge of training and certifying personnel through its Netacad and Cisco Skills For All platforms, through which apprentices can improve their telecommunications skills, thanks to courses and diplomas that complement their knowledge and allow them to achieve their certification as an apprentice, professional or expert.

Based on the above, the apprentices of the diplomado de profundización CCNP are able to create networks in which they demonstrate the acquired skills and can quickly design the configurations that allow the implementation of VLANs, VRFs, trunk and access ports, as well as the use of EtherChannel and PAgP, among other skills, without neglecting the respective basic configurations, such as assigning names to the devices or complex ones, such as establishing users and passwords encrypted with the algorithm-type Scrypt .

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

INTRODUCCIÓN

La configuración de switches y routers es quizás la parte más importante para el correcto diseño de las redes actuales, razón por la cual los aprendices logran demostrar sus capacidades en procesos de habilitación de redes, estructurando redes conmutadas y configuración básica de dispositivos, aplicando el funcionamiento de VRFs y VLANs que le permiten entender las características, infraestructura y funcionamiento de las redes jerárquicas convergentes. Logrando con esto diseñar y simular soluciones de red escalables, haciendo uso de configuraciones básicas e identificación de dispositivos, asignando direcciones IPv4 e IPv6, así como su respectivo proceso de encapsulamiento entre VLANs, para que al final con el correcto enrutamiento estático logremos la comunicación entre los hosts presentes entre redes LAN y WAN.

Para finalizar, se habilitan las interfaces troncales de los switches que se conectan directamente con los routers de borde, también se configura y habilita el EtherChannel entre switches, haciendo uso del protocolo propiedad de Cisco PAgP, para luego en todos los dispositivos implementar la seguridad con encriptado y habilitación de usuario con privilegios de administrador.

ESCENARIO PROPUESTO

Para esta actividad, el estudiante debe realizar las tareas asignadas en el escenario propuesto, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos *ping*, *traceroute*, *show ip route*, entre otros.

Por lo cual el estudiante es responsable de:

- 1) Completar la configuración multi-VRF de la red que admite "Usuarios generales" y "Usuarios especiales".
- 2) Una vez finalizado, debe haber accesibilidad completa de un extremo a otro de la red.
- 3) Los dos grupos no deben poder comunicarse entre sí.
- 4) Verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según los requerimientos.

Recursos requeridos:

- 1) 3 routers cisco 7200 - imagen c7200-adventerprisek9-mz.152-4.M7
- 2) 3 switches cisco capa 2
- 3) 4 host (PCs)

Topología de la Red

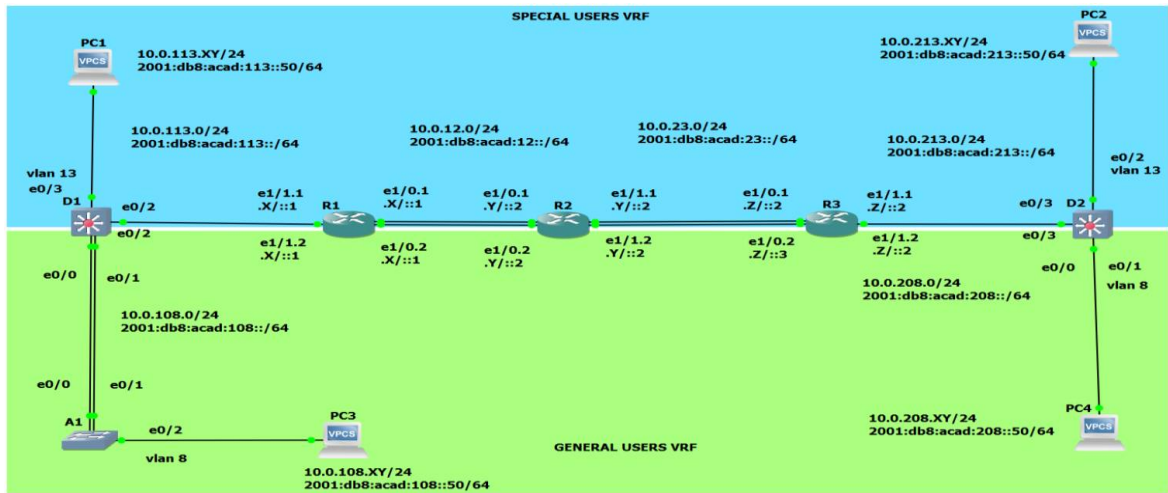


Figura 1-Topología de la Red

Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0.1	10.0.12.2/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.2/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.2/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.2/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.1/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.1/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.1/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.1/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.10/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.10/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.10/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.10/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.21/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.21/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.21/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.21/24	2001:db8:acad:208::50/64	EUI-64

Tabla 1 - Tabla de direccionamiento

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

Se realiza la adecuación de la red en el software emulador GNS3, incorporando cada dispositivo y realizando el respectivo cableado según lo estipulado en los lineamientos de la rúbrica de actividades.

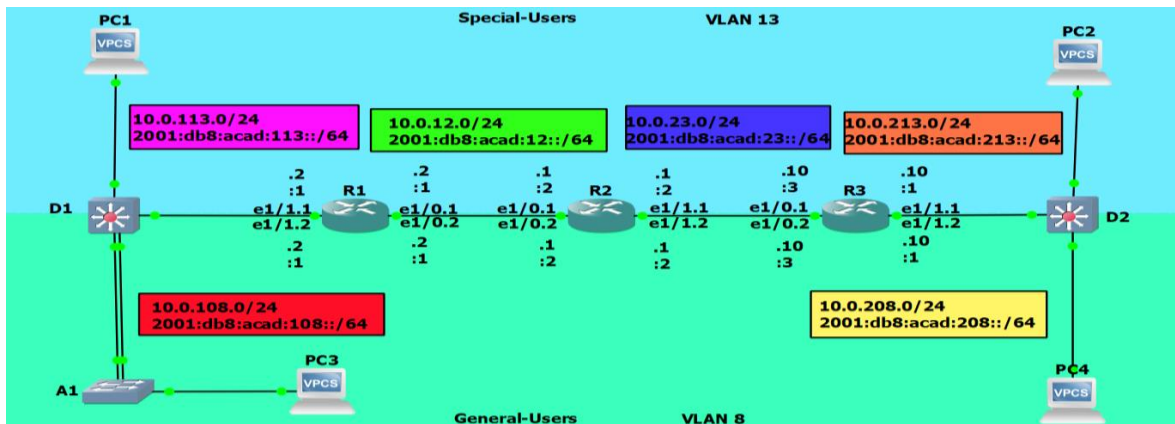


Figura 2- Red Creada

Dispositivo	Interfaz		Conectado con		VRF	Vlan
	Física	Lógica	Dispositivo	Interfaz		
R1	Eth1/1	ETH 1/1.1	D1	Eth 0/2	Special-U	13
		ETH 1/1.2	D1	Eth 0/2	General-U	8
	Eth 1/0	ETH 1/0.1	R2	Eth 1/0.1	Special-U	13
		ETH 1/0.2	R2	Eth 1/0.2	General-U	8
R2	Eth 1/0	ETH 1/0.1	R1	Eth 1/0.1	Special-U	13
		ETH 1/0.2	R1	Eth 1/0.2	General-U	8
	Eth 1/1	ETH 1/1.1	R3	Eth 1/0.1	Special-U	13
		ETH 1/1.2	R3	Eth 1/0.2	General-U	8
R3	Eth 1/0	ETH 1/0.1	R2	Eth 1/1.1	Special-U	13
		ETH 1/0.2	R2	Eth 1/1.2	General-U	8
	Eth 1/1	ETH 1/1.1	D2	Eth 0/3	Special-U	13
		ETH 1/1.2	D2	Eth 0/3	General-U	8
D1	Eth 0/0	N/A	A1	Eth 0/0	General-U	8
	Eth 0/1	N/A	A1	Eth 0/1	General-U	8
	Eth 0/2	N/A	R1	Eth 1/1.1	Special-U	13
N/A		R1	Eth 1/1.2	General-U	8	
D2	Eth 0/1	N/A	PC4	Eth 0/0	General-U	8
	Eth 0/2	N/A	PC2	Eth 0/0	Special-U	13
	Eth 0/3	N/A	R3	Eth 1/1.1	Special-U	13
		N/A	R3	Eth 1/1.2	General-U	8
A1	Eth 0/0	N/A	D1	Eth 0/0	General-U	8
	Eth 0/1	N/A	D1	Eth 0/1	General-U	8
	Eth 0/2	N/A	PC1	Eth 0/0	General-U	8

Tabla 2 - Tabla de cableado

Paso 2: Se procede a realizar la configuración básica de cada dispositivo, incluyendo los hosts.

Configuración básica R1	
Comando	Función
<i>Enable</i>	Ingresa al <i>CLI</i>
<i>Configure terminal</i>	Ingresa al modo privilegiado
<i>hostname R1</i>	" <i>Hostname</i> " asigna el nombre al dispositivo
<i>ipv6 unicast-routing</i>	Habilita el uso de IPV6 para el reenvío de paquetes unidifusión
<i>no ip domain lookup</i>	Deshabilita el proceso de traducción de palabras mal digitadas al DNS
<i>banner motd # R1, ENCOR Skills Assessment, Scenario 2 #</i>	Ingresa el mensaje que se mostrara antes de ingresar al <i>CLI</i>
<i>line console 0</i>	ingresa al modo de configuración de línea de la consola, el cero (0) representa la primera
<i>exec-timeout 0 0</i>	Elimina el tiempo de espera por inactividad en la consola (viene predeterminado a 10 minutos)
<i>logging synchronous</i>	Evita mensajes de <i>logging</i> que interrumpen al revisar las configuraciones.
<i>Interface e1/0</i> <i>No shutdown</i> <i>Interface e1/1</i> <i>No shutdown</i>	Se encienden las interfaces de las cuales se va a hacer uso.
<i>end</i>	Sale del modo privilegiado en que se encuentre

Tabla 3 - Configuración básica R1

```

R1#sh run
Building configuration...

Current configuration : 2601 bytes
!
! Last configuration change at 00:28:12 UTC Fri Mar 31 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
control-plane
!
banner motd ^C R1, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login
  
```

Figura 3 - Verificación de la configuración de R1 con el comando show running-config

Configuración básica R2	
Comando	Función
<i>Enable</i>	Ingresa al <i>CLI</i>
<i>Configure terminal</i>	Ingresa al modo privilegiado
<i>hostname R1</i>	“Hostname” asigna el nombre al dispositivo
<i>ipv6 unicast-routing</i>	Habilita el uso de IPV6 para el reenvío de paquetes unidifusión
<i>no ip domain lookup</i>	Deshabilita el proceso de traducción de palabras mal digitadas al DNS
<i>banner motd # R2, ENCOR Skills Assessment, Scenario 2 #</i>	Ingresa el mensaje que se mostrara antes de ingresar al <i>CLI</i>
<i>line console 0</i>	ingresa al modo de configuración de línea de la consola, el cero (0) representa la primera
<i>exec-timeout 0 0</i>	Elimina el tiempo de espera por inactividad en la consola (viene predeterminado a 10 minutos)
<i>logging synchronous</i>	Evita mensajes de <i>logging</i> que interrumpen al revisar las configuraciones.
<i>Interface e1/0</i> <i>No shutdown</i> <i>Interface e1/1</i> <i>No shutdown</i>	Se encienden las interfaces de las cuales se va a hacer uso.
<i>end</i>	Sale del modo privilegiado en que se encuentre

Tabla 4 - Configuración básica R2

```

R2#sh runn
Building configuration...

Current configuration : 2541 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
control-plane
!
banner motd ^C R2, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login

```

Figura 4 - Verificación de la configuración de R2 con el comando show running-config

Configuración básica R3	
Comando	Función
<i>Enable</i>	Ingresa al <i>CLI</i>
<i>Configure terminal</i>	Ingresa al modo privilegiado
<i>hostname R3</i>	" <i>Hostname</i> " asigna el nombre al dispositivo
<i>ipv6 unicast-routing</i>	Habilita el uso de IPV6 para el reenvío de paquetes unidifusión
<i>no ip domain lookup</i>	Deshabilita el proceso de traducción de palabras mal digitadas al DNS
<i>banner motd # R3, ENCOR Skills Assessment, Scenario 2 #</i>	Ingresa el mensaje que se mostrara antes de ingresar al <i>CLI</i>
<i>line console 0</i>	ingresa al modo de configuración de línea de la consola, el cero (0) representa la primera
<i>exec-timeout 0 0</i>	Elimina el tiempo de espera por inactividad en la consola (viene predeterminado a 10 minutos)
<i>logging synchronous</i>	Evita mensajes de <i>logging</i> que interrumpen al revisar las configuraciones.
<i>Interface e1/0</i> <i>No shutdown</i> <i>Interface e1/1</i> <i>No shutdown</i>	Se encienden las interfaces de las cuales se va a hacer uso.
<i>end</i>	Sale del modo privilegiado en que se encuentre

Tabla 5 - Configuración básica R3

```

R3#sh runn
Building configuration...

Current configuration : 2543 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
control-plane
!
banner motd ^C R3, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login

```

Figura 5 - Verificación de la configuración de R3 con el comando show running-config

Configuración básica D2	
Comando	Función
<i>Enable</i>	Ingresa al <i>CLI</i>
<i>Configure terminal</i>	Ingresa al modo privilegiado
<i>hostname D1</i>	“Hostname” asigna el nombre al dispositivo
<i>ipv6 unicast-routing</i>	Habilita el uso de IPV6 para el reenvío de paquetes unidifusión
<i>no ip domain lookup</i>	Deshabilita el proceso de traducción de palabras mal digitadas al DNS
<i>banner motd # D2, ENCOR Skills Assessment, Scenario 2 #</i>	Ingresa el mensaje que se mostrara antes de ingresar al <i>CLI</i>
<i>line console 0</i>	ingresa al modo de configuración de línea de la consola, el cero (0) representa la primera
<i>exec-timeout 0 0</i>	Elimina el tiempo de espera por inactividad en la consola (viene predeterminado a 10 minutos)
<i>logging synchronous</i>	Evita mensajes de <i>logging</i> que interrumpen al revisar las configuraciones.
<i>VLAN 8</i>	Crea una VLAN (red de área local virtual) y le asigna un número de identificación
<i>Name General-Users</i>	Da nombre a la VLAN creada anteriormente
<i>VLAN 13</i>	Crea una VLAN (red de área local virtual) y le asigna un número de identificación
<i>Name Special-Users</i>	Da nombre a la VLAN creada anteriormente
<i>exit</i>	Sale del modo privilegiado en que se encuentre
<i>Interface range e0/0-3</i> <i>Dúplex Full</i>	se habilita el dúplex full en las interfaces a usar, para que sea compatible con el router

Tabla 7 - Configuración básica D2

```

D2#sh runn
Building configuration...

Current configuration : 1563 bytes
!
! Last configuration change at 14:33:16 UTC Fri Mar 31 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname D2
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip http server
no ip http secure-server
!
!
!
control-plane
!
banner motd ^C D2, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!
!
end

```

Figura 7 - Verificación de la configuración de D2 con el comando show running-config

Configuración básica A1	
Comando	Función
<i>Enable</i>	Ingresa al <i>CLI</i>
<i>Configure terminal</i>	Ingresa al modo privilegiado
<i>hostname A1</i>	“Hostname” asigna el nombre al dispositivo
<i>ipv6 unicast-routing</i>	Habilita el uso de IPV6 para el reenvío de paquetes unidifusión
<i>no ip domain lookup</i>	Deshabilita el proceso de traducción de palabras mal digitadas al DNS
<i>banner motd # A1, ENCOR Skills Assessment, Scenario 2 #</i>	Ingresa el mensaje que se mostrara antes de ingresar al <i>CLI</i>
<i>line console 0</i>	ingresa al modo de configuración de línea de la consola, el cero (0) representa la primera
<i>exec-timeout 0 0</i>	Elimina el tiempo de espera por inactividad en la consola (viene predeterminado a 10 minutos)
<i>logging synchronous</i>	Evita mensajes de <i>logging</i> que interrumpen al revisar las configuraciones.
<i>VLAN 8</i>	Crea una VLAN (red de área local virtual) y le asigna un número de identificación
<i>Name General-Users</i>	Da nombre a la VLAN creada anteriormente
<i>exit</i>	Sale del modo privilegiado en que se encuentre
<i>Interface range e0/0-3</i> <i>Dúplex Full</i>	se habilita el dúplex full en las interfaces a usar, para que sea compatible con el D1

Tabla 8 - Configuración básica A1

```

A1#sh run
Building configuration...

Current configuration : 1553 bytes
!
! Last configuration change at 14:40:21 UTC Fri Mar 31 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname A1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
banner motd ^C A1, ENCOR Skills Assessment, Scenario 2 ^C
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

Figura 8 - Verificación de la configuración de A1 con el comando show running-config

Configuración básica PC1, PC2, PC3, PC4	
Comando	Función
<i>Ip [ip address] [mask] [gateway] IPv6 [IPv6 address / mask]</i>	Se configuran las direcciones IPv4, IPv6, máscara de subred y Gateway.
<i>Save</i>	Guarda la información en la memoria
<i>Show</i>	Se revisa que se efectuaran los cambios

Tabla 9 - Configuración básica PCs

```
PC1> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC1      10.0.113.21/24   10.0.113.2       00:50:79:66:68:03 10004  127.0.0.1:10005
          fe80::250:79ff:fe66:6803/64
          2001:db8:acad:113::50/64
```

Figura 9 - Configuración direcciones PC1 con el comando show

```
PC2> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC2      10.0.213.21/24   10.0.213.10      00:50:79:66:68:01 10006  127.0.0.1:10007
          fe80::250:79ff:fe66:6801/64
          2001:db8:acad:213::50/64
```

Figura 10 - Configuración direcciones PC2 con el comando show

```
PC3> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC3      10.0.108.21/24   10.0.108.2       00:50:79:66:68:02 10008  127.0.0.1:10009
          fe80::250:79ff:fe66:6802/64
          2001:db8:acad:108::50/64
```

Figura 11 - Configuración direcciones PC3 con el comando show

```
PC4> show
NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
PC4      10.0.208.21/24   10.0.208.10      00:50:79:66:68:00 10010  127.0.0.1:10011
          fe80::250:79ff:fe66:6800/64
          2001:db8:acad:208::50/64
```

Figura 12 - Configuración direcciones PC4 con el comando show

Parte 2: Configurar VRF y enrutamiento estático.

Se procede a realizar las configuraciones necesarias para crear 2 VRF (*virtual route and forwarding*) denominadas Special-Users ligada a la VLAN 13 y General-Users ligada a la VLAN 8. Posteriormente se crearán las rutas estáticas de cada router, de forma que se pueda hacer ping en cada VRF entre los enrutadores.

El proceso de crear las VRFs es el mismo en los tres Routers.

Configuración VRFs en R1, R2 y R3	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
Vrf definition Special-Users Address-family ipv4 Address-family ipv6 Vrf definition General-Users Address-family ipv4 Address-family ipv6	Se definen las dos VRFs y se habilita el uso en familias IPv4 e IPv6

Tabla 10 - Configuración VRFs en R1, R2 y R3

```
hostname R2
!
boot-start-marker
boot-end-marker
!
!
vrf definition General-Users
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
vrf definition Special-Users
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
```

Figura 13 - Definición VRFs en R2

Se realizan las configuraciones necesarias para las VRFs. Las IP se habilitan en cada interfaz del router.

Configuración VRFs Special-Users y VLAN 13 en R1	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
Interface e1/0.1	Se crea la subinterfaz Ethernet 1/0.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.12.2 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/1.1	Se crea la subinterfaz Ethernet 1/1.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.113.2 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/0.1	Se ingresa a la interfaz Ethernet 1/0.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::1:1 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:12::1/64</i>	Se asigna la dirección IPv6 y la máscara de subred
Interface e1/1.1	Se ingresa a la interfaz Ethernet 1/1.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::1:3 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:113::1/64</i>	Se asigna la dirección IPv6 y la máscara de subred

Tabla 11 - Configuración VRFs Special-Users y VLAN 13 en R1

```

interface Ethernet1/0
no ip address
duplex full
!
interface Ethernet1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address FE80::1:1 link-local
ipv6 address 2001:DB8:ACAD:12::1/64
!
interface Ethernet1/1.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.113.2 255.255.255.0
ipv6 address FE80::1:3 link-local
ipv6 address 2001:DB8:ACAD:113::1/64
!

```

Figura 14-VRFs Special-Users y VLAN 13 en R1

Configuración VRFs General-Users y VLAN 8 en R1	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
Interface e1/0.2	Se crea la subinterfaz Ethernet 1/0.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.12.2 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/1.2	Se crea la subinterfaz Ethernet 1/1.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.108.2 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/0.2	Se ingresa a la interfaz Ethernet 1/0.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::1:2 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:12::1/64</i>	Se asigna la dirección IPv6 y la máscara de subred
Interface e1/1.2	Se ingresa a la interfaz Ethernet 1/1.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::1:4 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:108::1/64</i>	Se asigna la dirección IPv6 y la máscara de subred
<i>Interface e1/0</i> <i>No shutdown</i> <i>Interface e1/1</i> <i>No shutdown</i>	Se encienden las interfaces de las cuales se va a hacer uso.

Tabla 12 - Configuración VRFs Special-Users y VLAN 13 en R1

```
interface Ethernet1/0.2
 encapsulation dot1q 8
 vrf forwarding General-Users
 ip address 10.0.12.2 255.255.255.0
 ipv6 address FE80::1:2 link-local
 ipv6 address 2001:DB8:ACAD:12::1/64
!
```

```
interface Ethernet1/1.2
 encapsulation dot1q 8
 vrf forwarding General-Users
 ip address 10.0.108.2 255.255.255.0
 ipv6 address FE80::1:4 link-local
 ipv6 address 2001:DB8:ACAD:108::1/64
!
```

Figura 15- General-Users y VLAN 8 en R1

Configuración VRFs Special-Users y VLAN 13 en R2	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
Interface e1/0.1	Se crea la subinterfaz Ethernet 1/0.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.12.1 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/1.1	Se crea la subinterfaz Ethernet 1/1.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.23.1 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/0.1	Se ingresa a la interfaz Ethernet 1/0.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::2:1 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:12::2/64</i>	Se asigna la dirección IPv6 y la máscara de subred
Interface e1/1.1	Se ingresa a la interfaz Ethernet 1/1.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::2:3 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:23::2/64</i>	Se asigna la dirección IPv6 y la máscara de subred

Tabla 13 - Configuración VRFs Special-Users y VLAN 13 en R2

```

interface Ethernet1/0
no ip address
duplex full
!
interface Ethernet1/0.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.12.1 255.255.255.0
ipv6 address FE80::2:1 link-local
ipv6 address 2001:DB8:ACAD:12::2/64
!
interface Ethernet1/1.1
encapsulation dot1q 13
vrf forwarding Special-Users
ip address 10.0.23.1 255.255.255.0
ipv6 address FE80::2:3 link-local
ipv6 address 2001:DB8:ACAD:23::2/64
!

```

Figura 16- VRFs Special-Users y VLAN 13 en R2

Configuración VRFs General-Users y VLAN 8 en R2	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
Interface e1/0.2	Se crea la subinterfaz Ethernet 1/0.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.12.1 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/1.2	Se crea la subinterfaz Ethernet 1/1.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.23.1 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/0.2	Se ingresa a la interfaz Ethernet 1/0.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::2:2 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:12::2/64</i>	Se asigna la dirección IPv6 y la máscara de subred
Interface e1/1.2	Se ingresa a la interfaz Ethernet 1/1.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::2:4 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:23::2/64</i>	Se asigna la dirección IPv6 y la máscara de subred
<i>Interface e1/0</i> <i>No shutdown</i> <i>Interface e1/1</i> <i>No shutdown</i>	Se encienden las interfaces de las cuales se va a hacer uso.

Tabla 14 - Configuración VRFs General-Users y VLAN 8 en R2

```

!
interface Ethernet1/0.2
 encapsulation dot1Q 8
 vrf forwarding General-Users
 ip address 10.0.12.1 255.255.255.0
 ipv6 address FE80::2:2 link-local
 ipv6 address 2001:DB8:ACAD:12::2/64
!
interface Ethernet1/1.2
 encapsulation dot1Q 8
 vrf forwarding General-Users
 ip address 10.0.23.1 255.255.255.0
 ipv6 address FE80::2:4 link-local
 ipv6 address 2001:DB8:ACAD:23::2/64
!

```

Figura 17-VRFs General-Users y VLAN 8 en R2

Configuración VRFs Special-Users y VLAN 13 en R3	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
Interface e1/0.1	Se crea la subinterfaz Ethernet 1/0.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.23.10 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/1.1	Se crea la subinterfaz Ethernet 1/1.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.213.10 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/0.1	Se ingresa a la interfaz Ethernet 1/0.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::3:1 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:23::3/64</i>	Se asigna la dirección IPv6 y la máscara de subred
Interface e1/1.1	Se ingresa a la interfaz Ethernet 1/1.1
<i>Encapsulation dot1q 13</i>	Se asocia la VLAN 13 con la subinterfaz
<i>Vrf forwarding Special-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::3:3 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:213::1/64</i>	Se asigna la dirección IPv6 y la máscara de subred

Tabla 15 - Configuración VRFs Special-Users y VLAN 13 en R3

```

interface Ethernet1/0
no ip address
duplex full
!
interface Ethernet1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.23.10 255.255.255.0
ipv6 address FE80::3:1 link-local
ipv6 address 2001:DB8:ACAD:23::3/64

interface Ethernet1/1
no ip address
duplex full
!
interface Ethernet1/1.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.213.10 255.255.255.0
ipv6 address FE80::3:3 link-local
ipv6 address 2001:DB8:ACAD:213::1/64

```

Figura 18-VRFs Special-Users y VLAN 13 en R3

Configuración VRFs General-Users y VLAN 8 en R3	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
Interface e1/0.2	Se crea la subinterfaz Ethernet 1/0.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.23.10 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/1.2	Se crea la subinterfaz Ethernet 1/1.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IP address 10.0.208.10 255.255.255.0</i>	Se asigna la dirección IPv4 y la máscara de subred
Interface e1/0.2	Se ingresa a la interfaz Ethernet 1/0.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::3:2 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:23::3/64</i>	Se asigna la dirección IPv6 y la máscara de subred
Interface e1/1.2	Se ingresa a la interfaz Ethernet 1/0.2
<i>Encapsulation dot1q 8</i>	Se asocia la VLAN 8 con la subinterfaz
<i>Vrf forwarding General-Users</i>	Se asocia la interfaz con la VRF nombrada
<i>IPv6 address fe80::3:4 link-local</i>	Se asigna el enlace-local
<i>IPv6 address 2001:db8:acad:208::1/64</i>	Se asigna la dirección IPv6 y la máscara de subred
<i>Interface e1/0 No shutdown Interface e1/1 No shutdown</i>	Se encienden las interfaces de las cuales se va a hacer uso.

Tabla 16 - Configuración VRFs General-Users y VLAN 8 en R2

```

!
interface Ethernet1/0.2
 encapsulation dot1Q 8
 vrf forwarding General-Users
 ip address 10.0.23.10 255.255.255.0
 ipv6 address FE80::3:2 link-local
 ipv6 address 2001:DB8:ACAD:23::3/64
!
interface Ethernet1/1.2
 encapsulation dot1Q 8
 vrf forwarding General-Users
 ip address 10.0.208.10 255.255.255.0
 ipv6 address FE80::3:4 link-local
 ipv6 address 2001:DB8:ACAD:208::1/64
!

```

Figura 19-VRFs General-Users y VLAN 8 en R3

Para finalizar este paso, se procede a realizar las rutas estáticas en cada router, que permitan el envío de paquetes a través de otras redes que no estén conectadas directamente a una de sus interfaces o en su red local, para esto se hizo uso de los siguientes comandos:

- 1) ***ip route vrf [vrf name] [ip address] [subnet mask] [next hope]***
- 2) ***ipv6 route vrf [vrf name] [ip address] [subnet mask] [next hope]***

Static routes R1
<pre>ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.1 ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.1 ip route vrf Special-Users 10.0.23.0 255.255.255.0 10.0.12.1 ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.12.1 ipv6 route vrf General-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2 ipv6 route vrf Special-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2 ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:12::2 ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:12::2</pre>

Tabla 17 - Static routes R1

```
ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.1
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.1
ip route vrf Special-Users 10.0.23.0 255.255.255.0 10.0.12.1
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.12.1
!
ipv6 route vrf General-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:12::2
```

Figura 20 - Static routes R1

Static routes R2

```
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.2
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.10
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.2
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.10

ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3
```

Tabla 18 - Static routes R2

```
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.2
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.10
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.2
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.10
!
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3
```

Figura 21-Static routes R2

Static routes R3
<pre> ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.1 ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.1 ip route vrf Special-Users 10.0.12.0 255.255.255.0 10.0.23.1 ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.23.1 ipv6 route vrf Special-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2 ipv6 route vrf General-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2 ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:23::2 ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:23::2 </pre>

Tabla 19 - Static routes R3

```

no ip http secure-server
ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.1
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.1
ip route vrf Special-Users 10.0.12.0 255.255.255.0 10.0.23.1
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.23.1
!
ipv6 route vrf Special-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2
ipv6 route vrf General-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:23::2
!

```

Figura 22-Static routes R3

Verificación de la correcta configuración de las VRF en cada dispositivo enrutador.

Como método de Comprobación de la correcta configuración de las VRF, se procede a usar el comando “*show IP VRF interfaces*” desde cada *router*, en donde se evidenciarán las características de cada vrf en el dispositivo.

```
R1#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.2       General-Users    up
Et1/1.2        10.0.108.2      General-Users    up
Et1/0.1        10.0.12.2       Special-Users    up
Et1/1.1        10.0.113.2      Special-Users    up
R1#
```

Figura 23- Verificación con el comando “show ip vrf interfaces” en R1

```
R2#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.12.1       General-Users    up
Et1/1.2        10.0.23.1       General-Users    up
Et1/0.1        10.0.12.1       Special-Users    up
Et1/1.1        10.0.23.1       Special-Users    up
R2#
```

Figura 24-Verificación con el comando “show ip vrf interfaces” en R2

```
R3#show ip vrf interface
Interface      IP-Address      VRF              Protocol
Et1/0.2        10.0.23.10      General-Users    up
Et1/1.2        10.0.208.10     General-Users    up
Et1/0.1        10.0.23.10      Special-Users    up
Et1/1.1        10.0.213.10     Special-Users    up
R3#
```

Figura 25 - Verificación con el comando “show ip vrf interfaces” en R3

Verificación de las rutas estáticas en cada enrutador.

Como método de verificación de las rutas estáticas, se hace uso del comando “*show run | inc route*”, que nos permite evidenciar cada ruta, junto con la dirección, máscara de subred y próximo salto.

```
R1#show run | inc route
ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.1
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.1
ip route vrf Special-Users 10.0.23.0 255.255.255.0 10.0.12.1
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.12.1
ipv6 route vrf General-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users 2001:DB8:ACAD:23::/64 2001:DB8:ACAD:12::2
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:12::2
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:12::2
R1#
```

Figura 26 - Verificación con el comando “*show run | inc route*” en R1

```
R2#show run | inc route
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.2
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.10
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.2
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.10
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1
ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3
ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3
R2#
```

Figura 27- Verificación con el comando “*show run | inc route*” en R2

```
R3#show run | inc route
ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.1
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.1
ip route vrf Special-Users 10.0.12.0 255.255.255.0 10.0.23.1
ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.23.1
ipv6 route vrf Special-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2
ipv6 route vrf General-Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2
ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:23::2
ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:23::2
R3#
```

Figura 28- Verificación con el comando “*show run | inc route*” en R3

Verificación: Para finalizar este paso, se realiza la verificación realizando ping desde R1 hasta R3 en las siguientes direcciones:

Pings a realizar en R1:

```
ping vrf General-Users 10.0.208.10
ping vrf General-Users 2001:db8:acad:208::1
ping vrf Special-Users 10.0.213.10
ping vrf Special-Users 2001:db8:acad:213::1
```

```
R1#ping vrf General-Users 10.0.208.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/43/88 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 = 24/31/36 ms
R1#ping vrf Special-Users 10.0.213.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/40 ms
R1#ping vrf Special-Users 2001:db8:acad:213::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/37/40 ms
R1#
```

Figura 29- prueba de conexión entre dispositivos usando ping en R1

Pings a realizar en R3:

```
ping vrf General-Users 10.0.108.2
ping vrf General-Users 2001:db8:acad:108::1
ping vrf Special-Users 10.0.113.2
ping vrf Special-Users 2001:db8:acad:113::1
```

```
R3# ping vrf General-Users 10.0.108.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.108.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/40 ms
R3#
R3# ping vrf General-Users 2001:db8:acad:108::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:108::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms
R3#
R3# ping vrf Special-Users 10.0.113.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.113.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/29/44 ms
R3#
R3# ping vrf Special-Users 2001:db8:acad:113::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:113::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/32 ms
R3#
```

Figura 30-prueba de conexión entre dispositivos usando ping en R3

Parte 3: Configurar los Switches para soportar la conectividad con los dispositivos finales.

3.1 deshabilitar todas las interfaces en los switches L2 y L3.

3.2 Configurar y habilitar el modo *trunk* en los switches que presentan cableado con los *border router*.

3.2.1 EN D1 Configure y habilite LA INTERFAZ e0/2 en modo trunk hacia r1.

3.2.2 EN D2 Configure y habilite LA INTERFAZ e0/3 en modo trunk hacia r3.

3.3 Configurar EtherChannel, habilitando *portchannel* 1 y haciendo uso de *PAGP* en las interfaces que entrelazan a D1 y A1.

3.3.1 en D1, configure y habilite las interfaces e0/0 y e0/1, Port Channel 1 usando PAgP.

3.3.2 en A1, configure y habilite las interfaces e0/0 y e0/1, Port Channel 1 usando PAgP.

3.4 En D1, D2, and A1, configurar access ports para PC1, PC2, PC3, and PC4.

3.4.1 On D1, configure interface e0/3 as an access port in VLAN 13 and enable Portfast.

3.4.2 On D2, configure interface e0/2 as an access port in VLAN 13 and enable Portfast.

3.4.3 On D2, configure interface e0/1 as an access port in VLAN 8 and enable Portfast.

3.4.4 On A1, configure interface e0/2 as an access port in VLAN 8 and enable Portfast.

3.5 Verificar la conectividad realizando ping en IPv4 e IPv6 desde PC1 a PC2 y de PC3 a PC4.

Configuraciones paso 3 en D1	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
3.1 Apagar todas las interfaces	
<i>Interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3</i>	Se selecciona el rango de interfaces que se van a trabajar
<i>Shutdown</i>	Se apagan las interfaces seleccionadas
3.2 configurar el modo <i>trunk</i> hacia el <i>border router</i> R1	
<i>Interface e0/2</i>	Se selecciona la interfaz a intervenir
<i>Switchport trunk encapsulation dot1q</i>	Se indica que la interfaz usara encapsulamiento IEEE 802.1Q en las tramas
<i>Switchport mode trunk</i>	Obligamos el puerto a ser un puerto troncal
<i>Switchport trunk allowed Vlan 8, 13</i>	Permite el modo troncal en las 2 Vlan
<i>No shutdown</i>	Se enciende la interfaz
3.3 Configurar el <i>Etherchannel</i>	
<i>Interface port-channel 1</i>	Se configura la interfaz del canal puerto 1
<i>Interface range e0/0-1</i>	Se selecciona el rango de las interfaces a intervenir
<i>Switchport mode access</i>	Se habilita en modo acceso
<i>Switchport access Vlan 8</i>	Se habilita el modo acceso a la Vlan 8
<i>Channel-group 1 mode desirable</i>	Asignamos el Puerto 1 y se configura en modo deseable
<i>No shutdown</i>	Se enciende la interfaz
3.4 configurar puertos de acceso en Vlan 13 y habilitar <i>Portfast</i>	
<i>Interface e0/3</i>	Se selecciona la interfaz a intervenir
<i>Switchport mode access</i>	Se habilita en modo acceso
<i>Switchport access vlan 13</i>	Se habilita el modo acceso a la Vlan 13
<i>Spanning-tree portfast</i>	Habilita el STP Portfast
<i>No shutdown</i>	Se enciende la interfaz

Tabla 20-Configuraciones paso 3 en D1

Configuraciones paso 3 en D2	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
3.1 Apagar todas las interfaces	
<i>Interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3</i>	Se selecciona el rango de interfaces que se van a trabajar
<i>Shutdown</i>	Se apagan las interfaces seleccionadas
3.2 configurar el modo <i>trunk</i> hacia el <i>border router</i> R3	
<i>Interface e0/3</i>	Se selecciona la interfaz a intervenir
<i>Switchport trunk encapsulation dot1q</i>	Se indica que la interfaz usara encapsulamiento IEEE 802.1Q en las tramas.
<i>Switchport mode trunk</i>	obligamos el puerto a ser un puerto troncal
<i>Switchport trunk allowed Vlan 8, 13</i>	Permite el modo troncal en las 2 Vlan
<i>No shutdown</i>	Se enciende la interfaz
3.4 configurar puertos de acceso en Vlan 8,13 y habilitar <i>Portfast</i>	
<i>Interface e0/2</i>	Se selecciona la interfaz a intervenir
<i>Switchport mode access</i>	Se habilita en modo acceso
<i>Switchport access vlan 13</i>	Se habilita el modo acceso a la Vlan 13
<i>Spanning-tree portfast</i>	Habilita el STP Portfast
<i>No shutdown</i>	Se enciende la interfaz
<i>Interface e0/1</i>	Se selecciona la interfaz a intervenir
<i>Switchport mode access</i>	Se habilita en modo acceso
<i>Switchport access vlan 8</i>	Se habilita el modo acceso a la Vlan 8
<i>Spanning-tree portfast</i>	Habilita el STP Portfast
<i>No shutdown</i>	Se enciende la interfaz

Tabla 21-Configuraciones paso 3 en D2

Configuraciones paso 3 en A1	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
3.1 Apagar todas las interfaces	
<i>Interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3</i>	Se selecciona el rango de interfaces que se van a trabajar
<i>Shutdown</i>	Se apagan las interfaces seleccionadas
3.3 Configurar el Etherchannel	
<i>Interface port-channel 1</i>	Se configura la interfaz del canal puerto 1
<i>Interface range e0/0-1</i>	Se selecciona la interfaz a intervenir
<i>Switchport mode access</i>	Se habilita en modo acceso
<i>Switchport access Vlan 8</i>	Se habilita el modo acceso a la Vlan 8
<i>Channel-group 1 mode desirable</i>	Asignamos el Puerto 1 y de configura en modo deseable
<i>No shutdown</i>	Se enciende la interfaz
3.4 configurar puertos de acceso en Vlan 8 y habilitar <i>Portfast</i>	
<i>Interface e0/2</i>	Se selecciona la interfaz a intervenir
<i>Switchport mode access</i>	Se habilita en modo acceso
<i>Switchport access vlan 8</i>	Se habilita el modo acceso a la Vlan 8
<i>Spanning-tree portfast</i>	Habilita el STP Portfast
<i>No shutdown</i>	Se enciende la interfaz

Tabla 22-Configuraciones paso 3 en A1

Con el objetivo de verificar que efectivamente se realizaron las configuraciones de enlaces troncales, de acceso y *EtherChannel*, se procede a ejecutar los comandos “*show interfaces trunk*”, “*show etherchannel summary*” y “*show run interface [et 0/x]*” en cada uno de los switches e interfaces intervenidas.

Verificaciones paso 3 en 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)
```

Figura 31 - show etherchannel summary en A1

```
A1# show 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
```

Figura 32-comando "show run interface e0/2" en A1

Verificaciones paso 3 en switch D1

```
D1# show interface 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
D1#
```

Figura 33 - show interfaces trunk en D1

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

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

        A - formed by Auto LAG

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

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

Figura 34 - show etherchannel summary en D1

```
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
```

Figura 35-show run interface e0/3 en D1

Verificaciones paso 3 en switch D2

```
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
```

Figura 36-show interfaces trunk en D2

```
interface Ethernet0/1
switchport access vlan 8
switchport mode access
spanning-tree portfast edge
end

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
```

Figura 37-show run interface e0/1 y e0/2 en D2

Verificación de conectividad entre PCS.

```
PC1> ping 10.0.213.21
84 bytes from 10.0.213.21 icmp_seq=1 ttl=61 time=46.709 ms
84 bytes from 10.0.213.21 icmp_seq=2 ttl=61 time=48.491 ms
84 bytes from 10.0.213.21 icmp_seq=3 ttl=61 time=47.846 ms
84 bytes from 10.0.213.21 icmp_seq=4 ttl=61 time=38.546 ms
84 bytes from 10.0.213.21 icmp_seq=5 ttl=61 time=41.068 ms

PC1> ping 2001:db8:acad:213::50
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=51.337 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=51.341 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=50.706 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=61.699 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=51.120 ms
```

Figura 38-Ping de PC1 a PC2

```
PC2> ping 10.0.113.21
10.0.113.21 icmp_seq=1 timeout
10.0.113.21 icmp_seq=2 timeout
84 bytes from 10.0.113.21 icmp_seq=3 ttl=61 time=46.952 ms
84 bytes from 10.0.113.21 icmp_seq=4 ttl=61 time=40.124 ms
84 bytes from 10.0.113.21 icmp_seq=5 ttl=61 time=48.939 ms

PC2> ping 2001:db8:acad:113::50
2001:db8:acad:113::50 icmp6_seq=1 ttl=58 time=83.014 ms
2001:db8:acad:113::50 icmp6_seq=2 ttl=58 time=50.900 ms
2001:db8:acad:113::50 icmp6_seq=3 ttl=58 time=41.634 ms
2001:db8:acad:113::50 icmp6_seq=4 ttl=58 time=51.591 ms
2001:db8:acad:113::50 icmp6_seq=5 ttl=58 time=42.761 ms
```

Figura 39-Ping de PC2 a PC1

```
PC3> ping 10.0.208.21
84 bytes from 10.0.208.21 icmp_seq=1 ttl=61 time=55.439 ms
84 bytes from 10.0.208.21 icmp_seq=2 ttl=61 time=42.632 ms
84 bytes from 10.0.208.21 icmp_seq=3 ttl=61 time=39.490 ms
84 bytes from 10.0.208.21 icmp_seq=4 ttl=61 time=40.391 ms
84 bytes from 10.0.208.21 icmp_seq=5 ttl=61 time=45.886 ms

PC3> ping 2001:db8:acad:208::50
2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=50.288 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=50.967 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=40.751 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=40.948 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=41.171 ms
```

Figura 40-Ping de PC3 a PC4

```
PC4> ping 10.0.108.21
84 bytes from 10.0.108.21 icmp_seq=1 ttl=61 time=51.736 ms
84 bytes from 10.0.108.21 icmp_seq=2 ttl=61 time=42.341 ms
84 bytes from 10.0.108.21 icmp_seq=3 ttl=61 time=41.120 ms
84 bytes from 10.0.108.21 icmp_seq=4 ttl=61 time=40.547 ms
84 bytes from 10.0.108.21 icmp_seq=5 ttl=61 time=33.614 ms

PC4> ping 2001:db8:acad:108::50/64
2001:db8:acad:108::50 icmp6_seq=1 ttl=58 time=72.866 ms
2001:db8:acad:108::50 icmp6_seq=2 ttl=58 time=51.070 ms
2001:db8:acad:108::50 icmp6_seq=3 ttl=58 time=50.695 ms
2001:db8:acad:108::50 icmp6_seq=4 ttl=58 time=51.473 ms
2001:db8:acad:108::50 icmp6_seq=5 ttl=58 time=51.309 ms
```

Figura 41-Ping de PC4 a PC3

Parte 4- Configuración de seguridad en los dispositivos.

Se debe instaurar mecanismos de seguridad a los dispositivos existentes en la topología.

Las tareas de configuración son las siguientes:

4.1 en todos los dispositivos instaurar seguridad al modo privilegiado EXEC de la siguiente manera:

Tipo de algoritmo: SCRYPT
Contraseña: camilorodriguez210

4.2 en todos los dispositivos crear una cuenta de usuario local con los siguientes datos:

Name: admin
Privilege level: 15
Algorithm type: SCRYPT
Password: camilorodriguez210

4.3 en todos los dispositivos, habilitar AAA y autenticación AAA.

Habilitando autenticación AAA y usando la base de datos local en todas las líneas.

Nota: En vista que la versión de los router C7200 aportada inicialmente por los tutores, no es compatible con el tipo de configuración de seguridad que se debe implementar, se procede a realizar la actualización de la versión e instalarla en R1, R2 Y R3 de nuestra simulación realizada en GNS3.

Imagen antigua: c7200-advipservicesk9-mz.152-4.S5

Imagen nueva: c7200-adventerprisek9-mz.152-4.M7

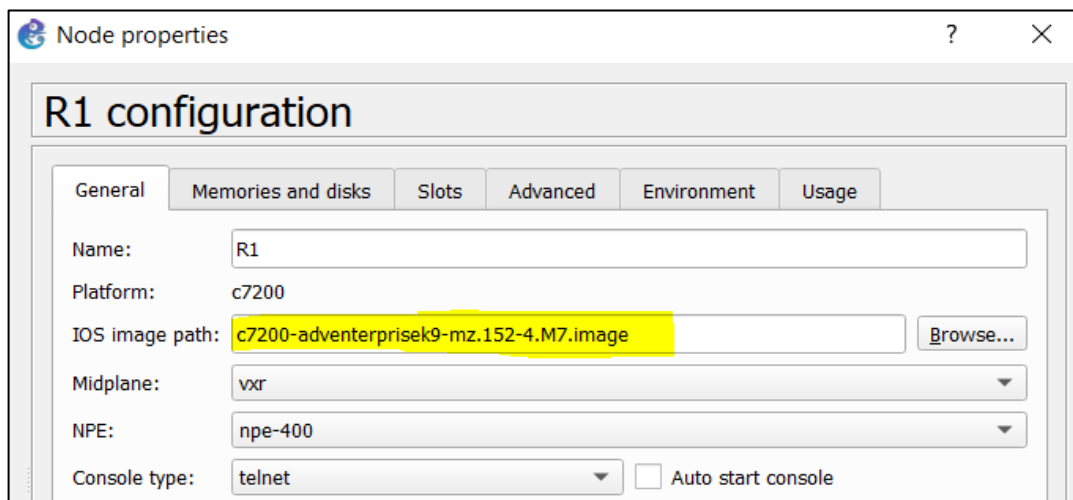


Figura 42-cambio de imagen ISO para los routers

Configuraciones de seguridad en R1	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
4.1 configurar seguridad al modo privilegiado <i>EXE</i>	
<i>Enable algorithm-type scrypt secret camilorodriguez210</i>	Configuramos y habilitamos la contraseña sugerida para el modo <i>EXE</i> , haciendo uso del algoritmo <i>SCRYPT</i>
4.2 crear una cuenta de usuario local.	
<i>Username admin privilege 15 algorithm-type scrypt secret camilorodriguez210</i>	Asignamos el nombre de usuario, nivel de privilegio y clave encriptada
4.3 habilite AAA y autenticación AAA.	
<i>AAA new-model</i>	Crea un nuevo modelo de configuración basado en AAA
<i>AAA authentication login default local</i>	Habilita la autenticación en el mismo modelo AAA- lo compara con los usuarios locales
<i>End</i>	Regresa al modo de inicio
<i>Erase nvram</i>	Borramos la <i>nvram</i>
<i>copy running-config startup-config</i>	Se guarda la configuración

Tabla 23-Configuraciones paso 4 en R1

```

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable algorithm-type scrypt secret camilorodriguez210
R1(config)#$min privilege 15 algorithm-type scrypt secret camilorodriguez210
R1(config)#AAA new-model
R1(config)#AAA authentication login default local
R1(config)#exit
R1#era
*Apr 28 22:47:44.143: %SYS-5-CONFIG_I: Configured from console by console
R1#erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
R1#
*Apr 28 22:47:57.895: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

```

Figura 43-Configuraciones paso 4 en R1

Configuraciones de seguridad en R2	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
4.1 configurar seguridad al modo privilegiado <i>EXE</i>	
<i>Enable algorithm-type scrypt secret camilorodriguez210</i>	Configuramos y habilitamos la contraseña sugerida para el modo <i>EXE</i> , haciendo uso del algoritmo <i>SCRYPT</i>
4.2 crear una cuenta de usuario local.	
<i>Username admin privilege 15 algorithm-type scrypt secret camilorodriguez210</i>	Asignamos el nombre de usuario, nivel de privilegio y clave encriptada
4.3 habilite AAA y autenticación AAA.	
<i>AAA new-model</i>	Crea un nuevo modelo de configuración basado en AAA
<i>AAA authentication login default local</i>	Habilita la autenticación en el mismo modelo AAA- lo compara con los usuarios locales
<i>End</i>	Regresa al modo de inicio
<i>Erase nvram</i>	Borramos la <i>nvram</i>
<i>copy running-config startup-config</i>	Se guarda la configuración

Tabla 24-Configuraciones paso 4 en R2

```

R2#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#Enable algorithm-type scrypt secret camilorodriguez210
R2(config)#$min privilege 15 algorithm-type scrypt secret camilorodriguez210
R2(config)#Aaa new-model
R2(config)#Aaa authentication login default local
R2(config)#Exit
R2#
*Apr 28 22:50:18.675: %SYS-5-CONFIG_I: Configured from console by console
R2#Erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
R2#
*Apr 28 22:50:33.115: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

```

Figura 44 - Configuraciones paso 4 en R2

Configuraciones de seguridad en R3	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
4.1 configurar seguridad al modo privilegiado <i>EXE</i>	
<i>Enable algorithm-type scrypt secret camilorodriguez210</i>	Configuramos y habilitamos la contraseña sugerida para el modo <i>EXE</i> , haciendo uso del algoritmo <i>SCRYPT</i>
4.2 crear una cuenta de usuario local.	
<i>Username admin privilege 15 algorithm-type scrypt secret camilorodriguez210</i>	Asignamos el nombre de usuario, nivel de privilegio y clave encriptada
4.3 habilite AAA y autenticación AAA.	
<i>AAA new-model</i>	Crea un nuevo modelo de configuración basado en AAA
<i>AAA authentication login default local</i>	Habilita la autenticación en el mismo modelo AAA- lo compara con los usuarios locales
<i>End</i>	Regresa al modo de inicio
<i>Erase nvram</i>	Borramos la <i>nvram</i>
<i>copy running-config startup-config</i>	Se guarda la configuración

Tabla 25-Configuraciones paso 4 en R3

```

R3#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#Enable algorithm-type scrypt secret camilorodriguez210
R3(config)#$min privilege 15 algorithm-type scrypt secret camilorodriguez210
R3(config)#Aaa new-model
R3(config)#Aaa authentication login default local
R3(config)#Exit
R3#
*Apr 28 22:51:59.431: %SYS-5-CONFIG_I: Configured from console by console
R3#Erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
R3#
*Apr 28 22:52:25.271: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

```

Figura 45-Configuraciones paso 4 en R3

La configuración para los switches es la misma.

Configuraciones de seguridad en D1	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
4.1 configurar seguridad al modo privilegiado <i>EXE</i>	
<i>Enable algorithm-type scrypt secret camilorodriguez210</i>	Configuramos y habilitamos la contraseña sugerida para el modo <i>EXE</i> , haciendo uso del algoritmo <i>SCRYPT</i>
4.2 crear una cuenta de usuario local.	
<i>Username admin privilege 15 algorithm-type scrypt secret camilorodriguez210</i>	Asignamos el nombre de usuario, nivel de privilegio y clave encriptada
4.3 habilite AAA y autenticación AAA.	
<i>AAA new-model</i>	Crea un nuevo modelo de configuración basado en AAA
<i>AAA authentication login default local</i>	Habilita la autenticación en el mismo modelo AAA- lo compara con los usuarios locales
<i>End</i>	Regresa al modo de inicio
<i>Erase nvram</i>	Borramos la <i>nvram</i>
<i>copy running-config startup-config</i>	Se guarda la configuración

Tabla 26-Configuraciones paso 4 en D1

```

D1#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#Enable algorithm-type scrypt secret camilorodriguez210
D1(config)#$min privilege 15 algorithm-type scrypt secret camilorodriguez210
D1(config)#Aaa new-model
D1(config)#Aaa authentication login default local
D1(config)#Exit
D1#
*Apr 25 22:26:34.477: %SYS-5-CONFIG_I: Configured from console by console

```

Figura 46 - Configuraciones paso 4 en D1

Configuraciones de seguridad en A1	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
4.1 configurar seguridad al modo privilegiado <i>EXE</i>	
<i>Enable algorithm-type scrypt secret camilorodriguez210</i>	Configuramos y habilitamos la contraseña sugerida para el modo <i>EXE</i> , haciendo uso del algoritmo <i>SCRYPT</i>
4.2 crear una cuenta de usuario local.	
<i>Username admin privilege 15 algorithm-type scrypt secret camilorodriguez210</i>	Asignamos el nombre de usuario, nivel de privilegio y clave encriptada
4.3 habilite AAA y autenticación AAA.	
<i>AAA new-model</i>	Crea un nuevo modelo de configuración basado en AAA
<i>AAA authentication login default local</i>	Habilita la autenticación en el mismo modelo AAA- lo compara con los usuarios locales
<i>End</i>	Regresa al modo de inicio
<i>Erase nvram</i>	Borramos la <i>nvram</i>
<i>copy running-config startup-config</i>	Se guarda la configuración

Tabla 27-Configuraciones paso 4 en A1

```

A1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#Enable algorithm-type scrypt secret camilorodriguez210
A1(config)#Username admin privilege 15 algorithm-type scrypt secret camilorodr$
A1(config)#Aaa new-model
A1(config)#Aaa authentication login default local
A1(config)#Exit
***

```

Figura 47 -Configuraciones paso 4 en A1

Configuraciones de seguridad en D2	
Comando	Función
<i>Configure terminal</i>	Ingresa al modo privilegiado
4.1 configurar seguridad al modo privilegiado <i>EXE</i>	
<i>Enable algorithm-type scrypt secret camilorodriguez210</i>	Configuramos y habilitamos la contraseña sugerida para el modo <i>EXE</i> , haciendo uso del algoritmo <i>SCRYPT</i>
4.2 crear una cuenta de usuario local.	
<i>Username admin privilege 15 algorithm-type scrypt secret camilorodriguez210</i>	Asignamos el nombre de usuario, nivel de privilegio y clave encriptada
4.3 habilite AAA y autenticación AAA.	
<i>AAA new-model</i>	Crea un nuevo modelo de configuración basado en AAA
<i>AAA authentication login default local</i>	Habilita la autenticación en el mismo modelo AAA- lo compara con los usuarios locales
<i>End</i>	Regresa al modo de inicio
<i>Erase nvram</i>	Borramos la <i>nvram</i>
<i>copy running-config startup-config</i>	Se guarda la configuración

Tabla 28-Configuraciones paso 4 en D2

```

D2#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#Enable algorithm-type scrypt secret camilorodriguez210
D2(config)#$min privilege 15 algorithm-type scrypt secret camilorodriguez210
D2(config)#Aaa new-model
D2(config)#Aaa authentication login default local
D2(config)#Exit
D2#
*Apr 25 22:28:11.721: %SYS-5-CONFIG_I: Configured from console by console

```

Figura 48 - Configuraciones paso 4 en D2

Para comprobar que efectivamente se realizaron las configuraciones necesarias solicitadas en el paso No. 4, que logren demostrar la correcta implementación de seguridad haciendo uso del tipo de algoritmo SCRYPT y el nivel de privilegio 15. Se realiza la verificación haciendo uso del comando “*show run | include aaa|username*”, que nos filtra el usuario y nivel de privilegios creados.

```
R1#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 9 $9$0Sr3yRGv1QPXv.$1iiAyJ/DJVMVeLzZA0hT7DkiJbkXVkofojG7RPaotJ.
R1#
```

Figura 49-Uso del comando “*show run | include aaa|username*” en R1

```
R2#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 9 $9$93y.AcTkuz77QE$9hCbpdfE.Eesq5gaYk0nozteiVdL0p.YU3w//0xccxQ
R2#
```

Figura 50-Uso del comando “*show run | include aaa|username*” en R2

```
R3#show run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 9 $9$24Me9T0j59GF5k$DsFcdn/YJSNyFH8Aop9IuEhpJRN.w5cFD/Ur/jj8UfU
R3#
```

Figura 51-Uso del comando “*show run | include aaa|username*” en R3

```
A1#show run | include aaa|username
username admin privilege 15 secret 9 $9$P/vTVjAgQEGCpq$Cqnnfoy0uxtSTbABRUJDGGnHxKooaX4dELF00U4Mo0A
aaa new-model
aaa authentication login default local
aaa session-id common
A1#
```

Figura 52-Uso del comando “show run | include aaa|username” en A1

```
D1#show run | include aaa|username
username admin privilege 15 secret 9 $9$qTi7wVjjRsci9a$rcvqHQ/o0Z0FWP6oE4jB83zXA6rnYx02SEzw0UaPD3g
aaa new-model
aaa authentication login default local
aaa session-id common
D1#
```

Figura 53-Uso del comando “show run | include aaa|username” en D1

```
D2#show run | include aaa|username
username admin privilege 15 secret 9 $9$b/igJScLME/uYa$CX3qJYGZLKvesOsgi4fVUd8rI.wPhpqwJBBmyOZ9cqY
aaa new-model
aaa authentication login default local
aaa session-id common
D2#
```

Figura 54-Uso del comando “show run | include aaa|username” en D2

CONCLUSIONES

Una red perfectamente constituida permite la conexión de los usuarios sin interferencias, *overlapping*, *solapamiento* o vulneraciones a su seguridad, por esta razón se puede concluir la importancia que representa en la actualidad el diseño eficiente de las redes para ser implementadas en ambientes corporativos, logrando todo esto con el uso de ambientes simulados, gracias a softwares de diseño y configuración de redes como lo es GNS3.

En base a lo anterior, podemos inferir la importancia del diseño para una correcta estructuración de redes conmutadas, con la configuración básica de los dispositivos, así como el funcionamiento de VLANs que logran agrupar ciertos usuarios, dependiendo del área o dominio, o de VRFs que permiten ejecutar más de una tabla de enrutamiento al tiempo desde el mismo *router*.

Por otro lado, no se puede dejar atrás la importancia que tiene la implementación de seguridad en las redes, esto ya que actualmente cualquier intromisión a una LAN o WAN puede significar un verdadero dolor de cabeza, así como pérdidas materiales o monetarias para las empresas, motivo por el cual se realizan las configuraciones en todos los dispositivos L2 y L3, implementando la seguridad para ingresar al modo EXE, con habilitación de usuario y privilegios de administrador, al igual que contraseñas encriptadas de tipo 9, gracias al algoritmo SCRYPT.

REFERENTES BIBLIOGRÁFICOS

BACHA, Donald. CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram. [s.l.]: Pearson IT Certification, 2022. ISBN 9780136891932.

BARRIENTOS, Enrique. REDES CISCO CCNP a Fondo, Guía de estudio para Profesionales. México: Alfaomega Grupo Editor, S A. de C.V., 2010. 921 p.

WALLACE, Kevin. CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. [s.l.]: Pearson Education, Limited. ISBN 9780133149937.