DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRACTICAS CCNP

JUAN CAMILO QUINTERO GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2022

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JUAN CAMILO QUINTERO GARCIA

Diplomado de opción de grado presentado para optar el
título de INGENIERO DE TELECOMUNICACIONES

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2022

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá Junio 26 2022

AGRADECIMIENTOS

Agradecido en primera medida con Dios, que me ha puesto hasta este punto después de 5 años, mostrándome que el sacrificio, la lucha, la constancia y la humildad fueron las mejores herramientas que me pudo haber dado para asumir este reto que estoy a portas de culminar.

Le agradezco por haberme llenado de vida y de salud en este tiempo para poder completar uno de mis objetivos.

A mis padres, mi esposa y mis amigos que a lo largo de este tiempo me entendieron en las veces que tuve que ausentarme o no estuve en algún momento con ellos, debido a los compromisos adquiridos con mi estudio, agradezco la enorme ayuda en el día a día, aconsejándome, alentándome y no dejando que desfalleciera en momentos difíciles a lo largo de mi tiempo de estudio.

Por último, un agradecimiento a la Universidad Nacional Abierta y a Distancia, la cual, debido a su metodología aplicada, me favoreció enormemente a lograr mi objetivo de graduarme como ingeniero, gracias a cada uno de sus colaboradores, tutores, directores de curso, asesores que permitieron no solo cumplir mi objetivo, sino que, lograr una numerosa cantidad de conocimientos que aplicaré y seguiré fortaleciendo cada día de mi vida.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CISCO: Empresa de origen estadounidense fabricante de dispositivos, para redes, esta empresa también presta sus servicios de soluciones de red.

CERTIFICACIÓN CISCO: Es un plus agregado a su hoja de vida o currículum, la cual demuestra posee conocimientos prácticos sobre redes. Las habilidades que usted tiene con estas certificaciones, son las de operar, configurar, administrar una red cisco y solucionar problemas en redes.

RED: Es la interconexión de distintos números de sistemas informáticos a través de una serie dispositivos de telecomunicaciones y un medio físico, su función es compartir información a través de paquete de datos.

IPV4: Es el nombre de protocolo de Internet utilizado actualmente para las direcciones IP de los dominios, esta utiliza direcciones de 32 bits con hasta 12 caracteres, combinando todos los dígitos es posible un máximo de alrededor de 4.300 millones de direcciones IP.

IPV6: Es un nuevo protocolo con el que se generan nuevos tipos de direcciones IP, a diferencia de IPV4, está compuesta por direcciones IP más largas y complejas, teniendo un espacio de 128 bits, es capaz de albergar alrededor de 340 sextillones de direcciones IP.

VRF: Es un enrutamiento virtual y reenvío, la cual permite que el enrutador ejecute más de una tabla de enrutamiento simultáneamente, de manera que puede utilizar la dirección IP asignada a dos interfaces diferentes en un enrutador al mismo tiempo.

RESUMEN

El diplomado de profundización de CISCO CCNP, es un compendio de actividades de aprendizaje teórico – práctico en donde fortalecimos las competencias en redes y telecomunicaciones, en donde se certificaron la adquisición de conocimientos para la administración de dispositivos de red, mediante el estudio de la arquitectura TCP/IP.
Por medio de actividades evaluativas con referencias a unidades de lectura propuestas en la plataforma NETACAD, se evaluaron los conocimientos adquiridos por parte de nosotros los estudiantes, reforzándolos con metodología práctica en la plataforma CISCO PACKET TRACER y GNS3, las cuales, por medio de ejercicios propuestos a lo largo del diplomado, se logró el aprendizaje de comandos IOS de configuración avanzada en routers, switches, protocolos de enrutamiento EIGRP Y BGP.

Por medio de la misma plataforma práctica de laboratorios propuestos a lo largo del tiempo, se permitió realizar el análisis sobre el comportamiento de múltiples protocolos, desarrollando ejercicios basados en diferentes topologías de red.

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

ABSTRACT

The CISCO CCNP deepening diploma course is a compendium of theoretical and practical learning activities where we strengthened the competences in networks and telecommunications, where the acquisition of knowledge for the administration of network devices was certified, through the study of TCP/IP architecture.
By means of evaluative activities with references to reading units proposed in the NETACAD platform, the knowledge acquired by the students was evaluated, reinforcing them with practical methodology in the CISCO PACKET TRACER and GNS3 platform, which, by means of exercises proposed throughout the course, students learned how to use IOS commands for advanced configuration in routers, switches, EIGRP and BGP routing protocols.

Additionally, by means of the same practical platform of laboratories proposed throughout the course, it is possible to analyze the behavior of multiple protocols, evaluating the performance of a network topology

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

INTRODUCCION

Lograr comprender los conceptos de la administración de una red mediante el uso de herramientas tecnológicas teórico – prácticas, con el fin de fortalecer los conocimientos adquiridos a lo largo del diplomado de profundización CISCO CCNP en todo lo relacionado con la administración de una red.

Por medio de un escenario propuesto de forma evaluativa, se debe realizar la debida configuración desde la construcción de la red, la configuración de cada dispositivo y el direccionamiento de las interfaces, la configuración de las rutas estáticas y la configuración del VRF.

En este escenario se evaluarán las habilidades de cada estudiante de acuerdo a las configuraciones realizadas cumpliendo con las especificaciones proporcionadas, teniendo como fin el funcionamiento óptimo de la red propuesta en el escenario 2.

DESARROLLO ESCENARIO PROPUESTO

En el siguiente escenario propuesto, se abordará la recopilación de conocimientos adquiridos a lo largo de los cursos tomados en cisco, y durante el periodo de aprendizaje realizado en el diplomado de Cisco CCNP.

El escenario consiste por medio de pasos solicitados a lo largo del siguiente trabajo final, en construir la siguiente topología de red, configurar los ajustes básicos de cada uno de los dispositivos, así como el direccionamiento de cada uno de ellos.

En procesos siguientes deberemos configurar el VRF (Virtual Routing Forwading) en los dispositivos como enrutadores, adecuando en ellos las rutas estáticas para poder realizar la admisión de acceso de un extremo a otro, esto deberá ser respaldado por la verificación de trazabilidad de rutas (Ping), entre los mismos.

Como finalidad obtendremos la comunicación de la topología aplicando diferentes procesos de programación, utilizando VRF, Sub-Interfaces, habilitando varias tablas de routing en simultánea.

Topología de Red

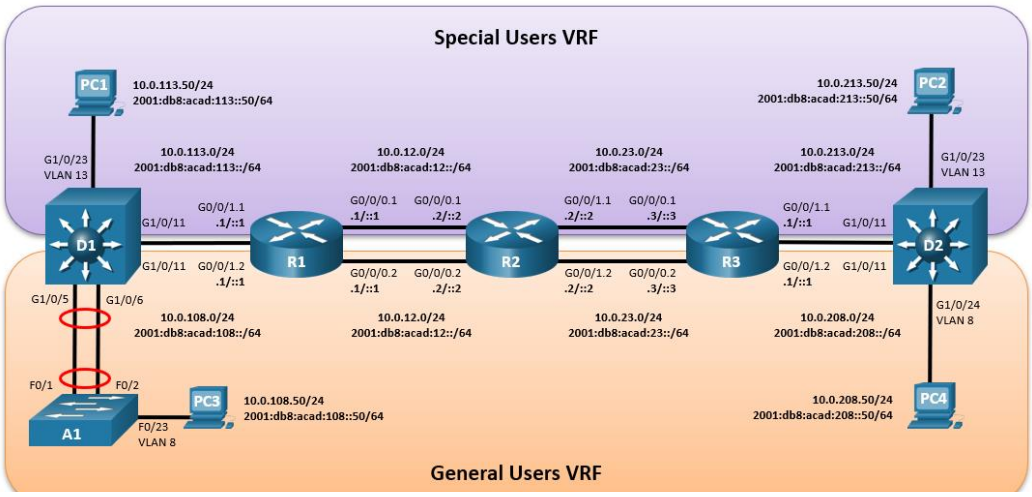

Ilustración 1. Topología Propuesta. Fuente: Rúbrica de evaluación UNAD.

Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G0/0/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G0/0/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G0/0/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G0/0/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G0/0/1.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	G0/0/1.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G0/0/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G0/0/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G0/0/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G0/0/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

Tabla 1. Direccionamiento de los equipos.

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

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

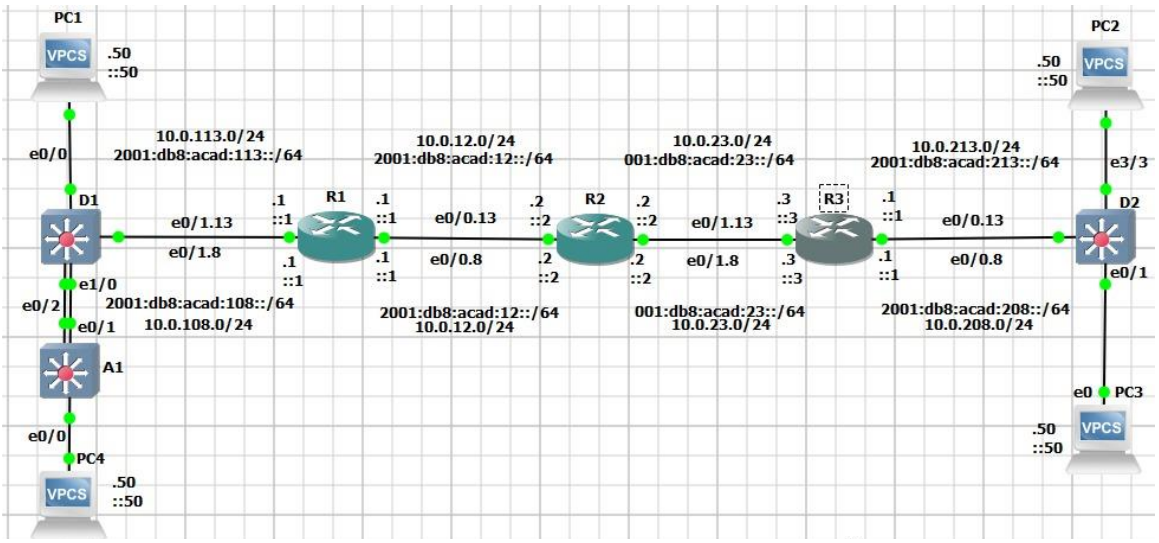

Ilustración 2. Topología Implementada.

1.2: Configure los ajustes básicos para cada dispositivo.

R1
hostname R1 //Asigno nombre al router
ipv6 unicast-routing //Habilito el modo de configuración global Ipv6 en el router
banner motd # R1, ENCOR Skills Assessment, Scenario 2 # //Mensaje que se presenta a todo aquel que se conecta al enrutador
line con 0 //Ingresamos al modo de configuración de la linea de la consola
exec-timeout 0 0 //Establezco el tiempo de espera inactiva de la sesión remota
logging synchronous //Evitamos que los mensajes inesperados nos desplacen los comandos que estamos escribiendo
exit //Salimos de la configuración

Router R2

R2
hostname R2 // Asigno nombre al router
ipv6 unicast-routing // Habilito el modo de configuración global Ipv6 en el router
banner motd # R2, ENCOR Skills Assessment, Scenario 2 # //Mensaje que se presenta a todo aquel que se conecta al enrutador
line con 0 //Ingresamos al modo de configuración de la linea de la consola
exec-timeout 0 0 // establezco el tiempo de espera inactiva de la sesión remota
logging synchronous // evitamos que los mensajes inesperados nos desplacen los comandos que estamos escribiendo
exit // Salimos de la configuración

Router R3

R3
hostname R3 // Asigno nombre al router
ipv6 unicast-routing // Habilito el modo de configuración global Ipv6 en el router
banner motd # R3, ENCOR Skills Assessment, Scenario 2 # // Mensaje que se presenta a todo aquel que se conecta al enrutador
line con 0 //Ingresamos al modo de configuración de la linea de la consola

exec-timeout 0 0 // establezco el tiempo de espera inactiva de la sesión remota
logging synchronous // evitamos que los mensajes inesperados nos desplacen los comandos que estamos escribiendo
exit // Salimos de la configuración

Switch D1

hostname D1 // Asigno nombre al Switch
ip routing ipv6 unicast-routing // Habilito el modo de configuración global Ipv6 en el Switch
no ip domain lookup // Desactivo la instrucción de traducción de nombres
banner motd # D1, ENCOR Skills Assessment, Scenario 2 // Mensaje que se presenta a todo aquel que se conecta al Switch
line con 0 //Ingresamos al modo de configuración de la linea de la consola
exec-timeout 0 0 //Establezco el tiempo de espera inactiva de la sesión remota
logging synchronous 0 //Evitamos que los mensajes inesperados nos desplacen los comandos que estamos escribiendo
exit // Salimos de la configuración
vlan 8 // Creamos una VLAN
name General-Users // Nombramos a la VLAN creada
exit // Salimos de la configuración
vlan 13 // Creamos una vlan
name Special-Users // Nombramos a la VLAN creada
exit // Salimos de la configuración

Switch D2

SW2

hostname D2 // Asigno nombre al Switch
ip routing ipv6 unicast-routing // Habilito el modo de configuración global Ipv6 en el Switch
no ip domain lookup // Desactivo la instrucción de traducción de nombres
banner motd # D2, ENCOR Skills Assessment, Scenario 2 // Mensaje que se presenta a todo aquel que se conecta al Switch
line con 0 //Ingresamos al modo de configuración de la linea de la consola

```
exec-timeout 0 0                    // establezco el tiempo de espera inactiva de la sesión remota
logging synchronous 0               // evitamos que los mensajes inesperados nos desplacen los comandos que estamos escribiendo
exit                                // Salimos de la configuración
vlan 8                              // Creamos una VLAN
name General-Users                  // Nombramos a la VLAN creada
exit                                // Salimos de la configuración
vlan 13                             // creación de vlan
name Special-Users                  // Nombramos a la VLAN creada
exit                                // Salimos de la configuración
```

Switch A1

```
hostname A1                         // Asigno nombre al Switch
ip routing ipv6 unicast-routing     // Habilito el modo de configuración global Ipv6 en el Switch
no ip domain lookup                 // Desactivo la instrucción de traducción de nombres
banner motd # A1, ENCOR Skills Assessment, Scenario 2    // Mensaje que se presenta a todo aquel que se conecta al Switch
line con 0                          // Ingresamos al modo de configuración de la linea de la consola
exec-timeout 0 0                    // Establezco el tiempo de espera inactiva de la sesión remota
logging synchronous 0               // Evitamos que los mensajes inesperados nos desplacen los comandos que estamos escribiendo
exit                                // Salimos de la configuración
vlan 8                              // Creamos una VLAN
name General-Users                  // Nombramos a la VLAN creada
exit                                // Salimos de la configuración
```

Parte 2: configurar VRF y enrutamiento estático.

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

Router R1

R1

```
vrf definition General-Users          // Se define la vfr
address-family ipv4                   // Habilito el protocolo ipv4
exit-address-family                   // Salimos de la configuración
address-family ipv6                   // Habilito el protocolo ipv6
exit-address-family                   // Salimos de la configuración
vrf definition Special-Users          // Se define la vfr
address-family ipv4                   // Habilito el protocolo ipv4
exit-address-family                   // Salimos de la configuración
address-family ipv6                   // Habilito el protocolo ipv6
exit-address-family                   // Salimos de la configuración
```

Router R2

R2

```
vrf definition General-Users          // Se define la vfr
address-family ipv4                   // Habilito el protocolo ipv4
exit-address-family                   // Salimos de la configuración
address-family ipv6                   // Habilito el protocolo ipv6
exit-address-family                   // Salimos de la configuración
vrf definition Special-Users          // Se define la vfr
address-family ipv4                   // Habilito el protocolo ipv4
exit-address-family                   // Salimos de la configuración
address-family ipv6                   // Habilito el protocolo ipv6
exit-address-family                   // Salimos de la configuración
```

Router R3

R3

```
vrf definition General-Users          // Se define la vrf
address-family ipv4                   // Habilito el protocolo ipv4
exit-address-family                   // Salimos de la configuración
address-family ipv6                   // Habilito el protocolo ipv6
```

```
exit-address-family                    // salimos de la configuración
vrf definition Special-Users           // Se define la vrf
address-family ipv4                     // Habilito el protocolo ipv4
exit-address-family                     // Salimos de la configuración
address-family ipv6                     // Habilito el protocolo ipv6
exit-address-family                    // Salimos de la configuración
```

2.2 En R1, R2 y R3, configure IPv4 e Interfaces IPv6 en cada VRF como detallada en la tabla de direccionamiento anterior.

Router R1

```
R1
interface Ethernet0/0.8                    // Creamos la sub-interfaz
 encapsulation dot1Q 8                     // Se permite trunk con la vlan
 vrf forwarding General_Users              // Se asocia la vrf con la sub-if ip
 ip address 10.0.12.1 255.255.255.0       // Se asigna una dirección ipv4
 ipv6 address FE80::1:1 link-local         // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:12::1/64       // Se asigna una dirección ipv6

interface Ethernet0/0.13                   // Creamos la sub-interfaz
encapsulation dot1Q 13                     // Se permite trunk con la vlan
vrf forwarding Special_Users               // Se asocia la vrf con la sub-if
ip address 10.0.12.1 255.255.255.0         // Se asigna una dirección ipv4
 ipv6 address FE80::1:2 link-local         // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:12::1/64       // Se asigna una dirección ipv6

interface Ethernet0/1.8                    // Creamos la sub-interfaz
encapsulation dot1Q 8                      // Se permite trunk con la vlan
 vrf forwarding General_Users              // Se asocia la vrf con la sub-if ip
 ip address 10.0.108.1 255.255.255.0       // Se asigna una dirección ipv4
 ipv6 address FE80::1:3 link-local         // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:108::1/64 // Se asigna una dirección ipv6


interface Ethernet0/1.13                   // Creamos la sub-interfaz
 encapsulation dot1Q 13                    // Se permite trunk con la vlan
 vrf forwarding Special_Users              // Se asocia la vrf con la sub-if ip
 ip address 10.0.113.1 255.255.255.0       // Se asigna una dirección ipv4
 ipv6 address FE80::1:4 link-local         // Se asigna un local link ipv6
ipv6 address 2001:DB8:ACAD:113::1/64  // Se asigna una dirección ipv6
```

Router R2

```
R2
interface Ethernet0/0.8                    // Creamos la sub-interfaz
 encapsulation dot1Q 8                     // Se permite trunk con la vlan
 vrf forwarding General_Users              // Se asocia la vrf con la sub-if ip
```

```
ip address 10.0.12.2 255.255.255.0          // Se asigna una dirección ipv4
ipv6 address FE80::2:1 link-local           // Se asigna un local link ipv6
ipv6 address 2001:DB8:ACAD:12::2/64   // Se asigna una dirección ipv6


interface Ethernet0/0.13                    // Creamos la sub-interfaz
 encapsulation dot1Q 13                     // Se permite trunk con la vlan
 vrf forwarding Special_Users               // Se asocia la vrf con la sub-if ip
 ip address 10.0.12.2 255.255.255.0         // Se asigna una dirección ipv4
 ipv6 address FE80::2:2 link-local          // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:12::2/64   // Se asigna una dirección ipv6

interface Ethernet0/1.13                    // Creamos la sub-interfaz
 encapsulation dot1Q 13                      // Se permite trunk con la vlan
 vrf forwarding Special_Users               // Se asocia la vrf con la sub-if ip
 ip address 10.0.23.2 255.255.255.0         // Se asigna una dirección ipv4
 ipv6 address FE80::2:4 link-local          // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:23::2/64   // Se asigna una dirección ipv6

interface Ethernet0/1.8                     // Creamos la sub-interfaz
 encapsulation dot1Q 8                      // Se permite trunk con la vlan
 vrf forwarding General_Users               // Se asocia la vrf con la sub-if ip
 ip address 10.0.23.2 255.255.255.0         // Se asigna una dirección ipv4
 ipv6 address FE80::2:3 link-local          // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:23::2/64   // Se asigna una dirección ipv6
```

Router R3

```
R3
interface Ethernet0/0.8                     // Creamos la sub-interfaz
encapsulation dot1Q 8                       // Se permite trunk con la vlan
vrf forwarding General_Users                // Se asocia la vrf con la sub-if ip
ip address 10.0.208.1 255.255.255.0         // Se asigna una dirección ipv4
ipv6 address FE80::3:1 link-local           // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:208::1/64 // Se asigna una dirección ipv6

interface Ethernet0/0.13                    // Creamos la sub-interfaz
 encapsulation dot1Q 13                      // Se permite trunk con la vlan
 vrf forwarding Special_Users               // Se asocia la vrf con la sub-if ip
 ip address 10.0.213.1 255.255.255.0        // Se asigna una dirección ipv4
 ipv6 address FE80::3:2 link-local          // Se asigna una dirección local link
 ipv6 address 2001:DB8:ACAD:213::1/64 // Se asigna una dirección ipv6
```

```
interface Ethernet0/1.13                    // Creamos la sub-interfaz
encapsulation dot1Q 13                      // Se permite trunk con la vlan
vrf forwarding Special_Users                // Se asocia la vrf con la sub-if ip
ip address 10.0.23.3 255.255.255.0          // Se asigna una dirección ipv4
 ipv6 address FE80::3:4 link-local          // Se asigna una dirección local link
 ipv6 address 2001:DB8:ACAD:23::3/64        // Se asigna una dirección ipv6

interface Ethernet0/1.8                     // Creamos la sub-interfaz
encapsulation dot1Q 8                       // Se permite trunk con la vlan
vrf forwarding General_Users                // Se asocia la vrf con la sub-if ip
ip address 10.0.23.3 255.255.255.0          // Se asigna una dirección ipv4
ipv6 address FE80::3:3 link-local           // Se asigna una dirección local link
ipv6 address 2001:DB8:ACAD:23::3/64         // Se asigna una dirección ipv6
```

2.3 En R1 y R3, configure la estática predeterminada rutas que apuntan a R2.

Router R1

ip route vrf General_Users 10.0.23.0 255.255.255.0 10.0.12.2 // Ruta hacia la red que se quiere alcanzar
ip route vrf General_Users 10.0.208.0 255.255.255.0 10.0.12.2 // Ruta hacia la red que se quiere alcanzar
ip route vrf Special_Users 10.0.23.0 255.255.255.0 10.0.12.2 // Ruta hacia la red que se quiere alcanzar
ip route vrf Special_Users 10.0.213.0 255.255.255.0 10.0.12.2 // Ruta hacia la red que se quiere alcanzar

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

Rutas estáticas hacia las redes que se quieren alcanzar en ipv6.

Router R2

R2
ip route vrf General_Users 10.0.108.0 255.255.255.0 10.0.12.1 // Ruta hacia la red que se quiere alcanzar
ip route vrf General_Users 10.0.208.0 255.255.255.0 10.0.23.3 // Ruta hacia la red que se quiere alcanzar
ip route vrf Special_Users 10.0.113.0 255.255.255.0 10.0.12.1 // Ruta hacia la red que se quiere alcanzar
ip route vrf Special_Users 10.0.213.0 255.255.255.0 10.0.23.3 // Ruta hacia la red que se quiere alcanzar

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

Rutas estáticas hacia las redes que se quieren alcanzar en ipv6.

Router R3

R3
ip route vrf General_Users 10.0.12.0 255.255.255.0 10.0.23.2 // Ruta hacia la red que se quiere alcanzar
ip route vrf General_Users 10.0.108.0 255.255.255.0 10.0.23.2 // Ruta hacia la red que se quiere alcanzar
ip route vrf Special_Users 10.0.12.0 255.255.255.0 10.0.23.2 // Ruta hacia la red que se quiere alcanzar
ip route vrf Special_Users 10.0.113.0 255.255.255.0 10.0.23.2 // Ruta hacia la red que se quiere alcanzar

ipv6 route vrf General_Users 2001:DB8:ACAD:12::/64 2001:DB8:ACAD:23::2
ipv6 route vrf Special_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

Rutas estáticas hacia las redes que se quieren alcanzar en ipv6.

2.4 Verificar la conectividad en cada VRF

ping vrf General_Users 10.0.208.1

```
R1#ping vrf General_Users 10.0.208.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

Ilustración 3. Prueba conexión mediante comando ping

ping vrf General_Users 2001:db8:acad:208::1

```
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 = 1/1/2 ms
R1#
```

Ilustración 4. Prueba conexión mediante comando ping

ping vrf Special_Users 10.0.213.1

```
R1#ping vrf Special_Users 10.0.213.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

Ilustración 5. Prueba conexión mediante comando ping

ping vrf Special_Users 2001:db8:acad:213::1

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

Ilustración 6.Prueba conexión mediante comando ping

Parte 3. Configurar Capa 2

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

Swtich D1

D1
D1(config-if-range)#int range e1/0 -3, e2/0 -3, e3/0 -3 // Seleccionamos un rango de interfaces para ingresar en simultanea para poder aplicar la siguiente configuración
D1(config-if-range)#shutdown // apagamos las interfaces seleccionadas anteriormente

Swtich D2

D2
D2(config-if-range)#int ran e0/2-3, e1/0-3, e2/0-3,e3/0-2 // Seleccionamos un rango de interfaces para ingresar en simultanea para poder aplicar la siguiente configuración.
D2(config-if-range)#shutdown // apagamos las interfaces seleccionadas anteriormente

Swtich A1

A1
A1(config)#int ran e1/0-3,e2/0-3,e3/0-3 // Seleccionamos un rango de interfaces para ingresar en simultanea para poder aplicar la siguiente configuración.
A1(config-if-range)#shutdown // apagamos las interfaces seleccionadas anteriormente

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

D1

```
interface Ethernet0/1
 switchport trunk allowed vlan 8,13          // Permite vlan 8 y 13 en trunk
 switchport trunk encapsulation dot1q        // Permite dot1q para trunk
 switchport mode trunk                       // Troncalizar puerto
```

D2

```
interface Ethernet0/0
 switchport trunk allowed vlan 8,13          // Permite vlan 8 y 13 en trunk
 switchport trunk encapsulation dot1q        // Permite dot1q para trunk
 switchport mode trunk                       // Troncalizar puerto
```

R3

```
interface Ethernet0/0.8                      // Creamos la sub-interfaz
encapsulation dot1Q 8                        // Se permite trunk con la vlan
vrf forwarding General_Users                 // Se asocia la vrf con la sub-if ip
ip address 10.0.208.1 255.255.255.0          // Se asigna una dirección ipv4
ipv6 address FE80::3:1 link-local            // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:208::1/64 // Se asigna una dirección ipv6

interface Ethernet0/0.13                     // Creamos la sub-interfaz
 encapsulation dot1Q 13                       // Se permite trunk con la vlan
 vrf forwarding Special_Users                // Se asocia la vrf con la sub-if ip
 ip address 10.0.213.1 255.255.255.0         // Se asigna una dirección ipv4
 ipv6 address FE80::3:2 link-local           // Se asigna una dirección local link
 ipv6 address 2001:DB8:ACAD:213::1/64 // Se asigna una dirección ipv6

interface Ethernet0/1.13                     // Creamos la sub-interfaz
encapsulation dot1Q 13                       // Se permite trunk con la vlan
vrf forwarding Special_Users                 // Se asocia la vrf con la sub-if ip
ip address 10.0.23.3 255.255.255.0           // Se asigna una dirección ipv4
 ipv6 address FE80::3:4 link-local           // Se asigna una dirección local link
 ipv6 address 2001:DB8:ACAD:23::3/64   // Se asigna una dirección ipv6

interface Ethernet0/1.8                      // Creamos la sub-interfaz
encapsulation dot1Q 8                        // Se permite trunk con la vlan
vrf forwarding General_Users                 // Se asocia la vrf con la sub-if ip
```

```
ip address 10.0.23.3 255.255.255.0        // Se asigna una dirección ipv4
ipv6 address FE80::3:3 link-local         // Se asigna una dirección local link
ipv6 address 2001:DB8:ACAD:23::3/64       // Se asigna una dirección ipv6
```

R1

```
interface Ethernet0/0.8                   // Creamos la sub-interfaz
 encapsulation dot1Q 8                    // Se permite trunk con la vlan
 vrf forwarding General_Users             // Se asocia la vrf con la sub-if
 ip address 10.0.12.1 255.255.255.0       // Se asigna una dirección ipv4
 ipv6 address FE80::1:1 link-local        // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:12::1/64      // Se asigna una dirección ipv6

interface Ethernet0/0.13                  // Creamos la sub-interfaz
encapsulation dot1Q 13                    // Se permite trunk con la vlan
vrf forwarding Special_Users              // Se asocia la vrf con la sub-if
ip address 10.0.12.1 255.255.255.0        // Se asigna una dirección ipv4
 ipv6 address FE80::1:2 link-local        // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:12::1/64      // Se asigna una dirección ipv6

interface Ethernet0/1.8                   // Creamos la sub-interfaz
encapsulation dot1Q 8                     // Se permite trunk con la vlan
 vrf forwarding General_Users             // Se asocia la vrf con la sub-if ip
 ip address 10.0.108.1 255.255.255.0      // Se asigna una dirección ipv4
 ipv6 address FE80::1:3 link-local        // Se asigna un local link ipv6
 ipv6 address 2001:DB8:ACAD:108::1/64 // Se asigna una dirección ipv6


interface Ethernet0/1.13                  // Creamos la sub-interfaz
 encapsulation dot1Q 13                   // Se permite trunk con la vlan
 vrf forwarding Special_Users             // Se asocia la vrf con la sub-if ip
 ip address 10.0.113.1 255.255.255.0      // Se asigna una dirección ipv4
 ipv6 address FE80::1:4 link-local        // Se asigna un local link ipv6
ipv6 address 2001:DB8:ACAD:113::1/64  // Se asigna una dirección ipv6
```

3.3 En D1 y A1, configure el EtherChannel.

D1

```
interface Ethernet1/0                    // Ingresamos a la Interfaz
 switchport trunk allowed vlan 8         // Permite solo en trunk vlan 8
 switchport trunk encapsulation dot1q    // Permite dot1q para trunk
 switchport mode trunk                   // Troncalizar puerto
 channel-group 1 mode desirable          // Configuramos el modo deseado
     PAgP en el grupo del canal 1

interface Ethernet0/2                    // Ingresamos a la Interfaz
 switchport trunk allowed vlan 8         // Permite solo en trunk vlan 8
 switchport trunk encapsulation dot1q    // Permite dot1q para trunk
 switchport mode trunk                   // Troncalizar puerto
 channel-group 1 mode desirable          // Configuramos el modo deseado
     PAgP en el grupo del canal 1
interface Port-channel1                  // Se crea port channel
 switchport trunk allowed vlan 8         // Permite solo en trunk vlan 8
 switchport trunk encapsulation dot1q    // Permite dot1q para trunk
 switchport mode trunk                   // Troncalizar puerto
```

A1

```
interface Ethernet0/1                    // Ingresamos a la Interfaz
 switchport trunk allowed vlan 8         // Permite solo en trunk vlan 8
 switchport trunk encapsulation dot1q    // Permite dot1q para trunk
 switchport mode trunk                   // Troncalizar puerto
 channel-group 1 mode desirable          // Configuramos el modo deseado
     PAgP en el grupo del canal 1

interface Ethernet0/2                    // Ingresamos a la Interfaz
 switchport trunk allowed vlan 8         // Permite solo en trunk vlan 8
 switchport trunk encapsulation dot1q    // Permite dot1q para trunk
 switchport mode trunk                   // Troncalizar puerto
 channel-group 1 mode desirable          // Configuramos el modo deseado
     PAgP en el grupo del canal 1

interface Port-channel1                  // Se crea port channel
 switchport trunk allowed vlan 8         // Permite solo en trunk vlan 8
 switchport trunk encapsulation dot1q    // Permite dot1q para trunk
 switchport mode trunk                   // Troncalizar puerto
```

Se verifica port cannel.

Show etherchannel detail | section Et0/1 //validar configuración en específico para Et0/1
Show etherchannel detail | section Et0/1 //validar configuración en específico para Et0/2
Show etherchannel summ //validar que el protocolo está arriba o en producción.

```
A1#sh etherchannel detail | s Et0/1
Port: Et0/1
Et0/1     SC    U6/S7   H       30s      1        128        Any      18
Et0/1     D1                    aabb.cc80.0400   Et1/0        4s SC      10001
  0     00     Et0/1    Desirable-Sl       0
A1#sh etherchannel detail | s Et0/2
Port: Et0/2
Et0/2     SC    U6/S7   H       30s      1        128        Any      18
Et0/2     D1                    aabb.cc80.0400   Et0/2       17s SC      10001
  0     00     Et0/2    Desirable-Sl       0
Time since last port bundled:    0d:00h:05m:19s    Et0/2
A1#
A1#sh etherchannel summ
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      Et0/1(P)    Et0/2(P)

A1#
```

Ilustración 7. Port-channel en producción.

3.4 En D1, D2 y A1, configure en acceso los Puerto en PC1, PC2, PC3, y PC4

D1

```
interface Ethernet0/0          // Ingreso al puerto
switchport access vlan 13      // Se permite el paso de vlan en acceso
switchport mode Access         // Se permite el puerto en acceso
```

D2

```
interface Ethernet0/1          // Ingreso al puerto
switchport access vlan 8       // Se permite el paso de vlan en acceso
switchport mode Access         // Se permite el puerto en acceso

interface Ethernet3/3          // Ingreso al puerto
switchport access vlan 13      // Se permite el paso de vlan en acceso
switchport mode Access         // Se permite el puerto en acceso
```

A1

```
interface Ethernet0/0          // Ingreso al puerto
switchport access vlan 8       // Se permite el paso de vlan en acceso
switchport mode Access         // Se permite el puerto en acceso
```

PC1

```
ip 10.0.113.50/24 10.0.113.1   // Asignación ipv4
ip 2001:db8:acad:113::50/64    // Asignación ipv6
save                           // Guardar
```

PC2

```
ip 10.0.213.50/24 10.0.213.1   // Asignación ipv4
ip 2001:db8:acad:213::50/64    // Asignación ipv6
save                           // Guardar
```

PC3

```
ip 10.0.108.50/24 10.0.108.1   // Asignación ipv4
ip 2001:db8:acad:108::50/64    // Asignación ipv6
```

save // Guardar

PC4

ip 10.0.208.50/24 10.0.208.1 // Asignación ipv4
ip 2001:db8:acad:208::50/64 // Asignación ipv6
save // Guardar

3.5 verificar de PC A PC conectividad

Desde PC1 A PC2 ipv4

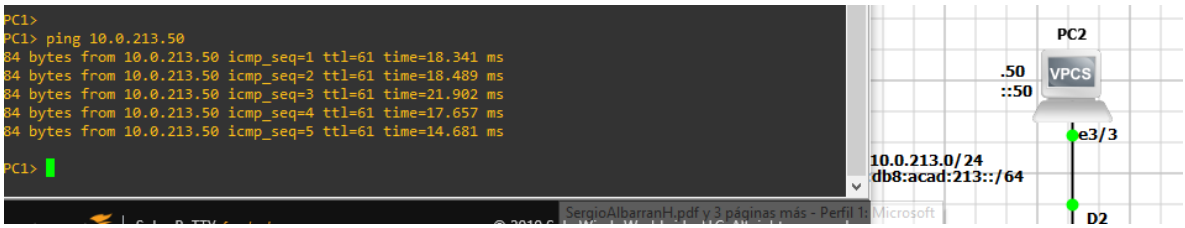

Ilustración 8. Prueba de ping de PC-1 A PC-2. Ipv4

Desde PC1 A PC2 ipv6

Ilustración 9. Prueba de ping de PC-1 A PC-2. Ipv6

Desde PC2 A PC1 ipv4

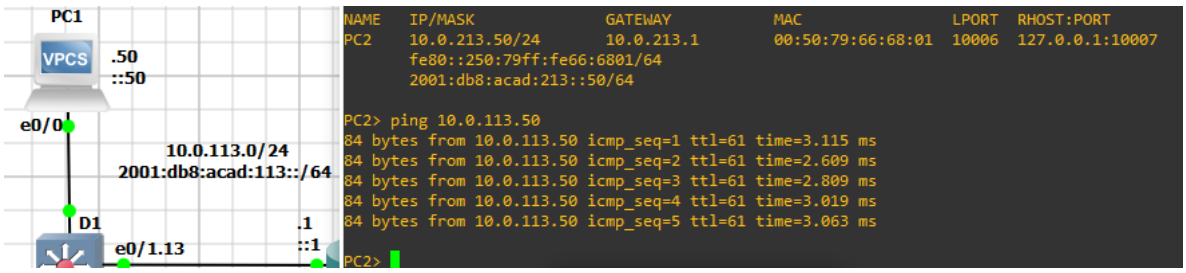

Ilustración 10. Prueba de ping de PC-2 A PC-1. Ipv4

Desde PC2 A PC1 ipv6

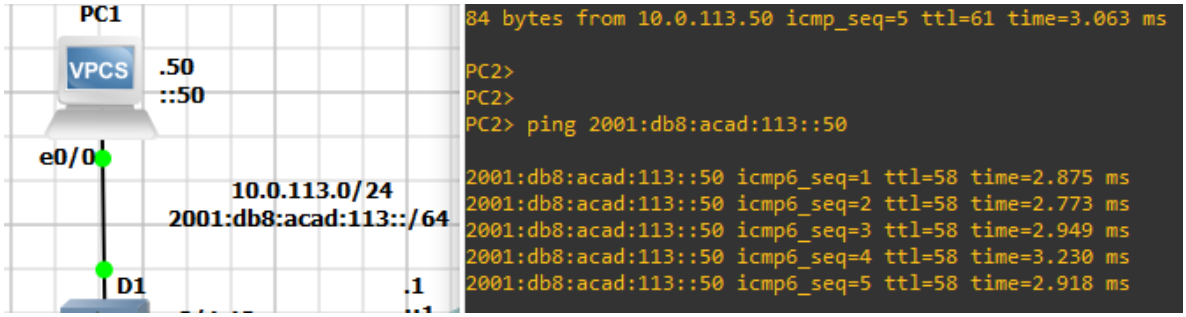

Ilustración 11. Prueba de ping de PC-2 A PC-1. Ipv6

Desde PC3 A PC4 ipv4

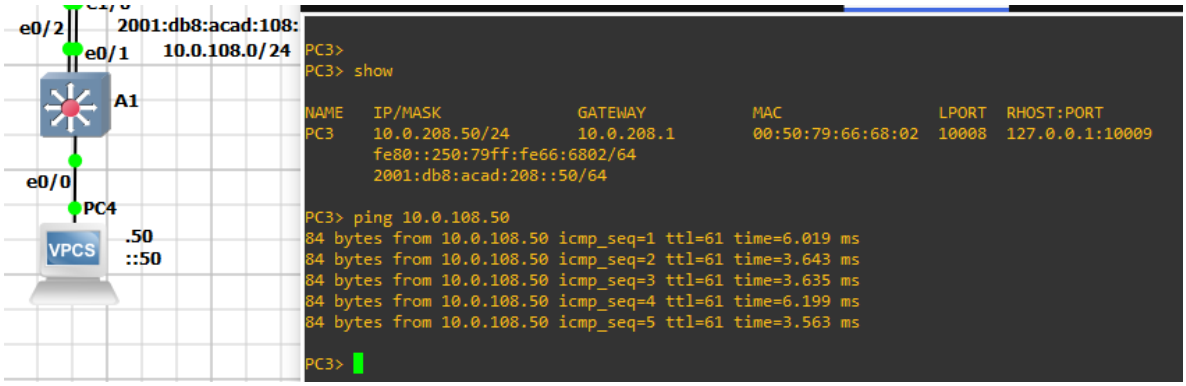

Ilustración 12. Prueba de ping de PC-3 A PC-4. Ipv4

Desde PC3 A PC4 ipv6

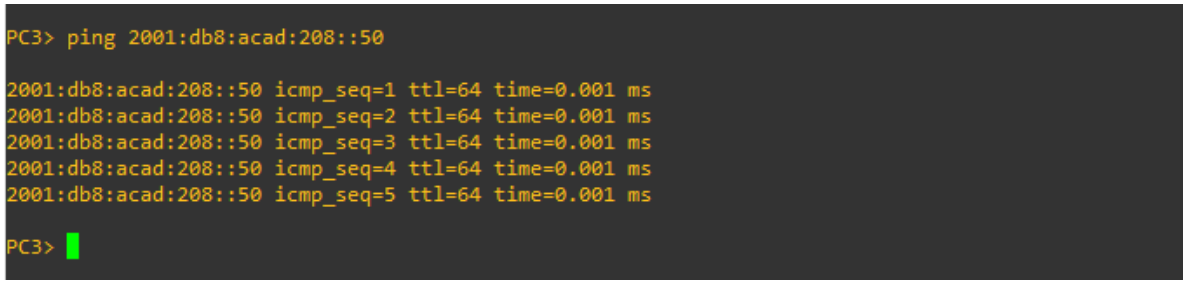

Ilustración 13. Prueba de ping de PC-3 A PC-4. Ipv6

Desde PC4 A PC3 ipv4

```
PC4> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC4    10.0.108.50/24       10.0.108.1        00:50:79:66:68:03  10010  127.0.0.1:10011
       fe80::250:79ff:fe66:6803/64
       2001:db8:acad:108::50/64

PC4> ping  10.0.208.50
84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=3.963 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=4.071 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=2.714 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=3.476 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=5.279 ms

PC4>
```

Ilustración 14. Prueba de ping de PC-4 A PC-3. Ipv4

Desde PC4 A PC3 ipv6

```
PC4> ping  2001:db8:acad:208::50

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=30.287 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=3.180 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=3.276 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=3.166 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=4.275 ms

PC4>
```

Ilustración 15. Prueba de ping de PC-4 A PC-3. Ipv6

Parte 4. Configurar Seguridad

4.1 En todos los dispositivos, modo EXE privilegiado seguro.

R1

```
service password-encryption          // encripción en el router
enable secret pass cisco             // habilitamos la clave secreta cisco
```

R2

```
service password-encryption          // encripción en el router
enable secret pass cisco             // habilitamos la clave secreta cisco
```

R3

```
service password-encryption          // encripción en el router
enable secret pass cisco             // habilitamos la clave secreta cisco
```

D1

```
service password-encryption          // encripción en el switch
enable secret pass cisco             // habilitamos la clave secreta cisco
```

D2

```
service password-encryption          // encripción en el switch
enable secret pass cisco             // habilitamos la clave secreta cisco
```

A1

```
service password-encryption          // encripción en el switch
enable secret pass cisco             // habilitamos la clave secreta cisco
```

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

A1

A1(config)#

A1(config)#username admin privilege 15 password 0 cisco12345cisco.
// Se crea usuario con privilegio 15.

D1

D1(config)#

D1(config)#username admin privilege 15 password 0 cisco12345cisco.
// Se crea usuario con privilegio 15.

R1

R1(config)#

R1(config)#username admin privilege 15 password 0 cisco12345cisco.
// Se crea usuario con privilegio 15.

R2

R2(config)#

R2(config)#username admin privilege 15 password 0 cisco12345cisco.
// Se crea usuario con privilegio 15.

R3

R3(config)#

R3(config)#username admin privilege 15 password 0 cisco12345cisco.
// Se crea usuario con privilegio 15.

D2

D2(config)#

D2(config)#username admin privilege 15 password 0 cisco12345cisco.
// Se crea usuario con privilegio 15.

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

A1

```
A1#show run  | section aaa                    // Buscar por sección en el equipo
aaa new-model                                 //Se crea el Nuevo modelo de
    autenticación
aaa authentication login default local        //Su autenticación local con claves
    locales
aaa session-id common                         //Sesión identificada como común
```

D1

```
D1#show run  | section aaa                    // Buscar por sección en el equipo
aaa new-model                                 //Se crea el Nuevo modelo de
    autenticación
aaa authentication login default local        //Su autenticación local con claves
    locales
aaa session-id common                         //Sesión identificada como común
```

R1

```
R1#show run  | section aaa                    // Buscar por sección en el equipo
aaa new-model                                 //Se crea el Nuevo modelo de
    autenticación
aaa authentication login default local        //Su autenticación local con claves
    locales
aaa session-id common                         //Sesión identificada como común
```

R2

```
R1#show run  | section aaa                    // Buscar por sección en el equipo
aaa new-model                                 //Se crea el Nuevo modelo de
    autenticación
aaa authentication login default local        //Su autenticación local con claves
    locales
aaa session-id common                         //Sesión identificada como común
```

R3

```
R3#show run  | section aaa                    // Buscar por sección en el equipo
aaa new-model                                 //Se crea el Nuevo modelo de
    autenticación
aaa authentication login default local        //Su autenticación local con claves
    locales
aaa session-id common                         //Sesión identificada como común
```

D2

D1#show run | section aaa	// Buscar por sección en el equipo
aaa new-model	//Se crea el Nuevo modelo de autenticación
aaa authentication login default local	//Su autenticación local con claves locales
aaa session-id common	//Sesión identificada como común

Validación en equipo.

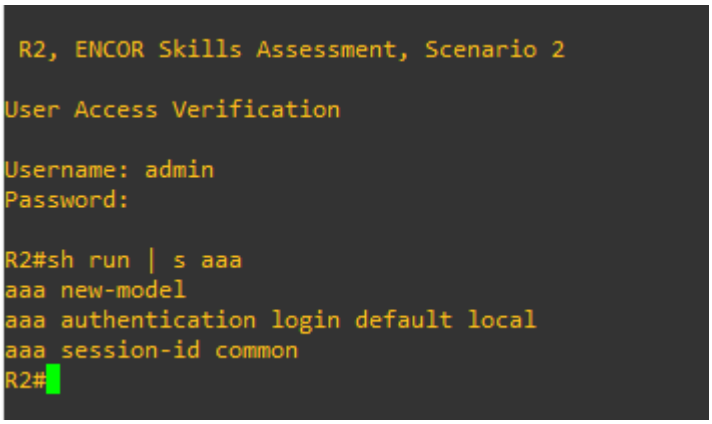

Ilustración 16. Verificación ingreso a equipo y autenticación aaa.

CONCLUSIONES

En el anterior escenario propuesto, se practicó la recopilación de conocimientos adquiridos a lo largo de los cursos tomados en cisco, y durante el periodo de aprendizaje realizado en el diplomado de Cisco CCNP.

El escenario consistió en construir una red propuesta, la cual se debió configurar los ajustes básicos de cada uno de los dispositivos, así como el direccionamiento de cada uno de ellos.

Procesos seguidos a configurar el VRF (Virtual Routing Forwading) en los dispositivos como enrutadores, adecuando en ellos las rutas estáticas para poder realizar la admisión de acceso de un extremo a otro, esto deberá ser respaldado por la verificación de trazabilidad de rutas (Ping), entre los mismos.

Como paso final obtuvimos la comunicación de la topología aplicando diferentes procesos de programación, utilizando VRF, Sub-Interfaces, habilitando varias tablas de routing en simultánea.

BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced OSPF. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Assurance. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC