

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

GENNY ALEXANDRA PRISCO MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA - ECBTI

INGENIERIA DE SISTEMAS

VILLA DEL ROSARIO

2022

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

GENNY ALEXANDRA PRISCO MORENO

Diplomado como opcion de grado para optar el titulo de ingeniera de sistemas

PAULITA FLOR SALAZAR

Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA - ECBTI

INGENIERIA DE SISTEMAS

VILLA DEL ROSARIO

2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

VILLA DEL ROSARIO, 26 de noviembre de 2022

AGRADECIMIENTOS

Mi gratitud a la Universidad Nacional Abierta y a Distancia UNAD, a toda su red de tutores por compartir sus conocimientos y estar vigilantes a mi proceso de formación, a Diana Ortiz en el área administrativa del CCAV Pamplona por su apoyo y asesoría. Al sindicato de empleados y trabajadores de la educación SINTRENAL regional Norte de Santander, factor clave en la gestión de la beca que ayudó a hacer este sueño posible.

Agradezco a mi familia por creer siempre en mí. A mi compañera de vida por su apoyo, paciencia, por estar a mi lado en los días y noches más difíciles.

Gracias a Dios, al universo y todos los seres que de una u otra manera intervinieron en que culmine con éxito y llegue a la meta de mi título profesional, una de las más difíciles e importantes de mi vida.

TABLA DE CONTENIDO

GLOSARIO.....	8
RESUMEN.....	9
1. ESCENARIO 1.....	11
1.1. Topología.....	11
1.2. Construir red.....	11
1.3. Desarrollar el esquema de direccionamiento IP.....	11
1.4. Configurar los aspectos básicos de los dispositivos de la Red propuesta.....	13
1.4.1. Configurar R1.....	13
1.4.2. Configurar S1.....	15
1.4.3. Configurar los equipos.....	16
1.5. Probar y verificar la conectividad de extremo a extremo.....	17
2. ESCENARIO 2.....	21
2.1. Topología.....	21
2.2. Configuración aspectos básicos de los dispositivos.....	22
Fuente: Prueba de habilidades diplomado CCNA II-2022.....	25
2.2.1. Configuración R1.....	25
2.2.2. Configuración de S1.....	29
2.2.3. Configuración de S2.....	31
2.3. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel).....	34
2.3.1. Configurar S1.....	34
2.3.2. Configurar S2.....	36
2.4. Configurar soporte de host.....	38
2.4.1. Configurar R1.....	38
2.4.2. Configurar los servidores.....	39
2.5. Probar y verificar la conectividad de extremo a extremo.....	43
CONCLUSIONES.....	50
REFERENCIAS BIBLIOGRAFICAS.....	51
ANEXOS.....	53

LISTA DE FIGURAS

Figura 1. Topología Propuesta Escenario 1	11
Figura 2. Topología Escenario 1 en Packet Tracer.....	11
Figura 3 Comprobación conectividad desde PC-A	19
Figura 4 Comprobación conectividad desde PC-B	19
Figura 5 Comprobación conectividad desde PC-A	20
Figura 6 Comprobación configuración PC-B.....	20
Figura 7 Topología Escenario 2 Propuesto	21
Figura 8 Topología Escenario 2 en Packet Trace	21
Figura 9 Resultado reinicio de switch despues haber borrado la configuración inicial	23
Figura 10 Resultado óptimo de la configuración de la plantilla SDM.....	24
Figura 11 Configuración de interfaz G0/0/1 y subinterfaces en R1.....	28
Figura 12 Configuración de PC-A con DHCP.....	40
Figura 13 Configuración de PC-B con DHCP	40
Figura 14 Configuración PC-A.....	41
Figura 15 Configuración PC-B.....	42
Figura 16 Ping desde PC-A a R1, G0/0/1.2 y R1, G0/0/1.3	46
Figura 17 Figura 16 Ping desde PC-A a R1, G0/0/1.4 y S1 VLAN 4	47
Figura 18 Ping desde PC-A a S2 VLAN 4 y PC-B.....	47
Figura 19 Ping a R1 Bucle 0 desde PC-A y PC-B.....	48
Figura 20 Ping desde PC-B a R1, G0/0/1.2 y R1, G0/0/1.3	48
Figura 21 Ping desde PC-B a R1, G0/0/1.4 y S1 VLAN4	49
Figura 22 Ping desde PC-B a S2 VLAN4	49

LISTA DE TABLAS

Tabla 1	Tabla de direccionamiento.....	12
Tabla 2	Configuración de host PC-A.....	17
Tabla 3	Configuración de host PC-B.....	17
Tabla 4	Comprobación de conectividad Escenario 1	18
Tabla 5	VLAN.....	24
Tabla 6	Tabla de asignación de direcciones.....	25
Tabla 7	Configuración PC-A	41
Tabla 8	Configuración PC-B	42
Tabla 9	Verificación Conectividad Escenario 2	43

GLOSARIO

Enrutamiento: Proceso que facilita a los dispositivos interconectados, disponer de la mejor ruta en la emisión y recepción de los mensajes/paquetes¹

LAN: Red de área local, con extensión de algunos centenares de metros, generalmente se utiliza para conectar ordenadores, servidores, para compartir recursos².

VLAN: Es LAN virtual, son la forma en que divide la red en redes más pequeñas, de modo que los dispositivos y las personas dentro de una sola VLAN se comunican entre sí y no tienen que administrar el tráfico de otras redes.³

IPv4: Internet Protocol, en el cual se basa la transmisión de datos en internet. Dentro del protocolo IPv4 se denominan 4 octetos de 8 bits separados por un punto para especificar cada equipo en la red.⁴

IPv6: Es la nueva versión de protocolo IP, es una versión mejorada de IPv4, dentro de los cambios más importantes están la ampliación del campo de dirección IP a 128 bits y los campos de longitud fija para ⁴facilitar el proceso que se le da a cada datagrama.⁴

¹ LÓPEZ, Ricardo. Enrutamiento y configuración de redes. (2018)

² DORDOIGNE, José. Redes informáticas-Nociones fundamentales. (2015)

³ NETCAD. 3 VLANs. (2.022)

⁴ MERCADO, Gustavo. Implementación y Evaluación de métodos de Traslación de Protocolos para la transición IPv4-IPv6. (2011)

RESUMEN

El currículo CCNA de CISCO en este diplomado brinda la oportunidad de adquirir habilidades en un área de gran expansión y desarrollo tecnológico. Mediante la práctica de Switching, enrutamiento y Wireless Essentials se busca mejorar el conocimiento del funcionamiento de enrutadores y conmutadores en redes.

Los escenarios presentados contienen los dispositivos, configuraciones y protocolos que asemejan la realidad de topologías y necesidad de soluciones a las cuales nos vamos a enfrentar en nuestro campo laboral como futuros ingenieros de sistemas. En los router y switch se aplican configuraciones de nombre, dominio, usuarios administrativos; seguridad como contraseñas y claves, encriptación. Se configuran interfaces aplicando IPv4 e IPv6.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes.

ABSTRACT

The CISCO CCNA curriculum in this diploma provides the opportunity to acquire skills in an area of great expansion and technological development. Through the practice of Switching, routing and Wireless Essentials, the aim is to improve the knowledge of the operation of routers and switches in networks.

The scenarios presented contain the devices, configurations, and protocols that resemble the reality of topologies and solution needs that we are going to face in our field of work as future systems engineers. In routers and switches, name, domain, and administrative user configurations are applied; security such as passwords and keys, encryption. Interfaces are configured applying IPv4 and IPv6.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking.

INTRODUCCIÓN

CISCO a través del diplomado de diseño e implementación de soluciones integradas LAN/WAN – CCNA, brinda las herramientas para la creación, operación y mantenimiento de las redes. Los módulos en CCNA contienen los temas que se aplican en los escenarios 1 y 2 de este trabajo, presentándolos mediante contenido de valor mediante escenarios, videos, ejercicios, evaluaciones, además de su valiosa herramienta Packet Tracer.

En un primer ejercicio se aplica el desarrollo del direccionamiento IP, en este paso que es básico para las actividades siguientes, se debe conocer las clases y con ellas lo referente a los prefijos y por supuesto las máscaras. En este ejercicio es pertinente conocer la ventaja del subneteo ya que permite una mejor administración, control, tráfico y seguridad al segmentar la red.

En un segundo escenario se aplican conocimientos más avanzados de configuración de router y switch, interfaces y subinterfaces, creando troncales, VLAN, EtherChannel y SVI. Otro aparte muy importante es la implementación de seguridad en los dispositivos para la cual se aplican diferentes protocolos.

1. ESCENARIO 1

1.1. Topología

Figura 1. Topología Propuesta Escenario 1

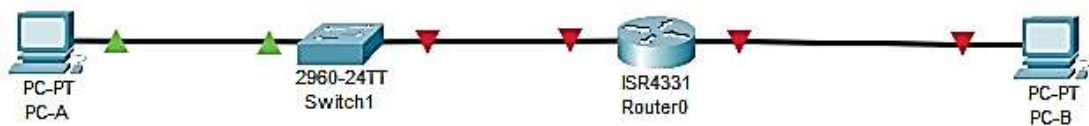


Fuente: Prueba de habilidades diplomado CCNA

1.2. Construir red

En el simulador Packet Tracer se desarrolla la red conforme a la topología lógica que se indica en la figura 1, la cual consta de un router, un switch, y dos host

Figura 2. Topología Escenario 1 en Packet Tracer



Fuente: Autor

1.3. Desarrollar el esquema de direccionamiento IP

De acuerdo al escenario propuesto se desarrolla el esquema de direccionamiento IP para la LAN 1 y la LAN 2. Para la dirección IPv4 se deben crear las dos subredes con la cantidad requerida de hosts y las direcciones se asignan de acuerdo con los requisitos de la tabla de direccionamiento.

Se toma el direccionamiento 172.XY.3.0 donde XY son los últimos dígitos de la identificación personal. Cedula 43157607. Según esto la dirección de red es: 172.7.3.0

Para la creación de las dos subredes solicitadas se tienen en cuenta las siguientes formulas:

$2^n - 2 =$ Cantidad de host (debe ser igual o mayor)

$2^n =$ redes

Según lo solicitado en host LAN1= 60 host y LAN 2 =20 host:

$2^7 - 2 = 126$ (si se tomaban 6 bits $2^6 = 64$ host y el requerimiento es de 80 en total)

Tabla 1 Tabla de direccionamiento

Ítem	Requerimiento
Dirección de Red	172.7.3.0
Requerimiento de host Subred LAN1	60 172.7.3.1 - 172.7.3.126
Requerimiento de host Subred LAN2	20 172.7.3.129 - 172.7.3.254
R1 G0/0/1	Última dirección de host de la subred LAN1 172.7.3.126
R1 G0/0/0	Última dirección de host de la subred LAN2 172.7.3.254
S1 SVI	Segunda dirección de host de la subred LAN1 172.7.3.2
PC-A	Décima dirección de host de la subred LAN1 172.7.3.10
PC-B	Décima dirección de host de la subred LAN2 172.7.3.138

Fuente: Autor

1.4. Configurar los aspectos básicos de los dispositivos de la Red propuesta

1.4.1. Configurar R1

El escenario planteado contiene un solo Router, haciendo clic se ingresa a CLI y se van aplicando los códigos que a continuación se listan según el requerimiento o tarea solicitada:

Desactivar la búsqueda DNS: En modo configuración global con el comando **no ip domain-lookup**

Nombre del router: El nombre asignado será R1, **hostname R1**

Nombre de dominio: el nombre para el dominio será ccna-sa.com, entonces la instrucción correcta es **ip domain-name ccna-sa.com**

Contraseña cifrada para el modo EXEC privilegiado: la contraseña para este modo es ciscoenpass, **enable password ciscoenpass**

Contraseña de acceso a la consola (ciscoconpass): las líneas de comando para acceso a consola y su asignación de contraseña:

```
Line console 0  
password ciscoconpass  
login  
exit
```

Establecer la longitud mínima para las contraseñas: Se pueden establecer la cantidad de caracteres a criterio propio, para este ejercicio es de 10:
security password min-length 10

Se debe crear un usuario administrativo en la base de datos local cuyo usuario es admin y la contraseña admin1pass: **username admin password admin1pass**

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local:

```
Line vty 0 15  
login local  
no password
```

Continuando con las medidas de seguridad en el router se configuran las líneas VTY para que acepten únicamente las conexiones SSH

```
transport input ssh
```

A continuación se hace cifrado de las contraseñas con el comando **service password-encryption**. Para verificar que las contraseñas estén cifradas se utiliza el comando **show running-config**.

Por último se genera una clave de cifrado RSA con módulo de 1024 bits: **crypto key generate rsa**

Se continúa con la configuración de un banner MOTD que debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece:

```
banner motd "R1-GENNY ALEXANDRA PRISCO MORENO- Ingeniería De Sistemas"
```

Ahora se da paso a la configuración de las interfaces, se debe establecer la descripción, la dirección IPv4 y ser activada, esto aplica tanto para la g/0/0/0 como para la g/0/0/1:

```
configure terminal  
interface serial 0/0/0  
ip address 172.7.3.254 255.255.255.128  
no shutdown  
exit
```

```
interface serial 0/0/1
ip address 172.7.3.126 255.255.255.128
no shutdown
exit
```

1.4.2. Configurar S1

La red tiene un solo Switch, haciendo clic se ingresa a CLI y se van aplicando los códigos que a continuación se listan según el requerimiento o tarea solicitada:

Desactivar la búsqueda DNS: En modo configuración global con el comando **no ip domain-lookup**

Nombre del router: El nombre asignado será R1, **hostname S1**

Nombre de dominio: el nombre para el dominio será ccna-sa.com, entonces la instrucción correcta es **ip domain-name ccna-sa.com**

Contraseña cifrada para el modo EXEC privilegiado: la contraseña para este modo es ciscoenpass, **enable password ciscoenpass**

Contraseña de acceso a la consola (ciscoconpass): las líneas de comando para acceso a consola y su asignación de contraseña:

```
Line console 0
password ciscoconpass
login
exit
```

Apagar todos los puertos sin usar: F0/1-4, F0/7-24, G0/1-2: esta configuración se puede realizar tomando rangos, el código es: **int range f0/1-4,f0/7-24,g0/1-2**

Se debe crear un usuario administrativo en la base de datos local cuyo usuario es admin y la contraseña admin1pass: **username admin password admin1pass**

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local:

```
Line vty 0 15  
login local  
no password
```

Continuando con las medidas de seguridad en el router se configuran las líneas VTY para que acepten únicamente las conexiones SSH

```
transport input ssh
```

A continuación se hace cifrado de las contraseñas con el comando **service password-encryption.**

Por último se genera una clave de cifrado RSA con módulo de 1024 bits: **crypto key generate rsa**

Se continúa con la configuración de un banner MOTD que debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece:

```
banner motd "S1-GENNY ALEXANDRA PRISCO MORENO- Ingeniería De Sistemas"
```

Se da paso a la configuración de la interfaz de administración (SVI) en la VLAN1, se debe establecer la descripción y la dirección IPv4, ante el comando de la VLAN **interface vlan1** se visualiza el mensaje **Mar 1 2:20:49.946: %SSH-5-ENABLED: SSH 1.99 has been enabled.*

Para establecer la ip: **ip address 172.7.3.2 255.255.255.128** y para activarlo **no shutdown**

1.4.3. Configurar los equipos

El siguiente paso es configurar los host de la red PC-A y PC-B conforme a la tabla de direccionamiento. Haciendo clic en cada host se ingresa a IP

CONFIGURATION y allí se ingresan los datos de IPv4, mascara y Gateway

Tabla 2 Configuración de host PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	00D0.D3E1.81D0
Dirección IPv4	172.7.3.10
Máscara de subred	255.255.255.128
Puerta de enlace IPv4 predeterminada	172.7.3.126

Fuente: Propia

Tabla 3 Configuración de host PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	00E0.F707.0D77
Dirección IPv4	172.7.3.138
Máscara de subred	255.255.255.254
Puerta de enlace IPv4	172.7.3.254

Fuente: Propia

1.5. Probar y verificar la conectividad de extremo a extremo

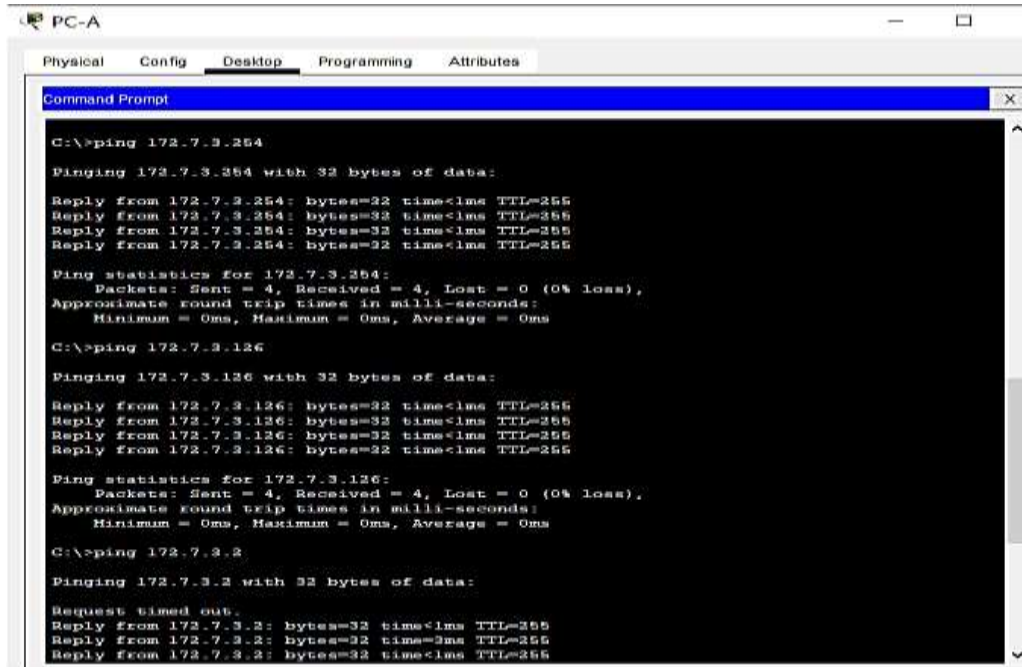
Mediante el comando ping se prueba la conectividad tal como se evidencia en la siguiente tabla, los resultados son positivos evidenciando el éxito de la configuración al hacer ping de extremo a extremo, se evidencia el recibido y la cero perdida de paquetes.

Tabla 4 Comprobación de conectividad Escenario 1

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.7.3.254	Ping statistics for 172.7.3.254: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1 G0/0/1	172.7.3.126	Ping statistics for 172.7.3.126: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	S1 VLAN 1	172.7.3.2	Ping statistics for 172.7.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	PC-B	172.7.3.138	Ping statistics for 172.7.3.138: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
PC-B	R1 G0/0/0	172.7.3.254	Ping statistics for 172.7.3.254: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1 G0/0/1	172.7.3.126	Ping statistics for 172.7.3.126: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
	S1 VLAN1	172.7.3.2	Ping statistics for 172.7.3.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Fuente: Autor

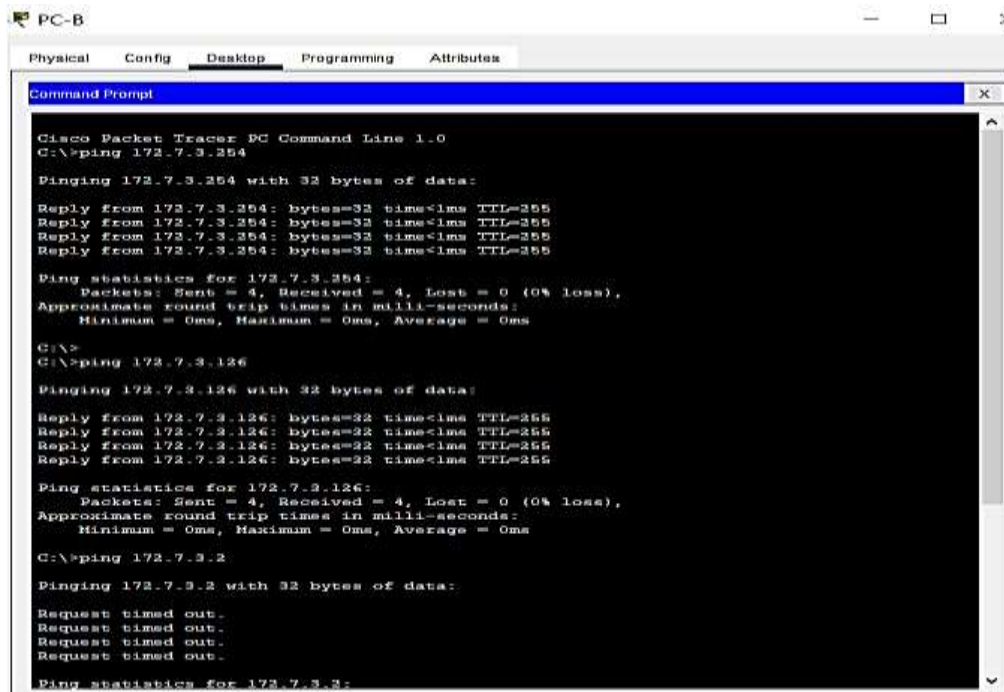
Figura 3 Comprobación conectividad desde PC-A



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.7.3.254
Pinging 172.7.3.254 with 32 bytes of data:
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Ping statistics for 172.7.3.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.7.3.126
Pinging 172.7.3.126 with 32 bytes of data:
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Ping statistics for 172.7.3.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.7.3.2
Pinging 172.7.3.2 with 32 bytes of data:
Request timed out.
Reply from 172.7.3.2: bytes=32 time<1ms TTL=255
Reply from 172.7.3.2: bytes=32 time<1ms TTL=255
Reply from 172.7.3.2: bytes=32 time<1ms TTL=255
```

Fuente: Autor

Figura 4 Comprobación conectividad desde PC-B

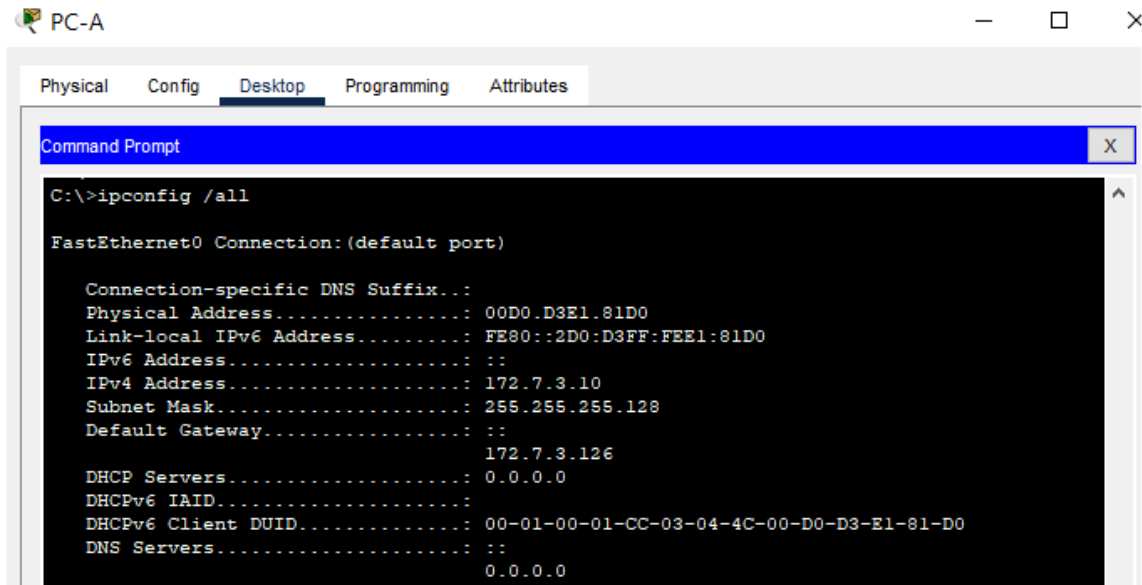


```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer DC Command Line 1.0
C:\>ping 172.7.3.254
Pinging 172.7.3.254 with 32 bytes of data:
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Reply from 172.7.3.254: bytes=32 time<1ms TTL=255
Ping statistics for 172.7.3.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
C:\>ping 172.7.3.126
Pinging 172.7.3.126 with 32 bytes of data:
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Reply from 172.7.3.126: bytes=32 time<1ms TTL=255
Ping statistics for 172.7.3.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.7.3.2
Pinging 172.7.3.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.7.3.2:
```

Fuente: Autor

Para evidenciar la configuración en el caso de los host se utiliza el comando ipconfig /all

Figura 5 Comprobación conectividad desde PC-A



The screenshot shows a Windows Command Prompt window titled "PC-A" with the "Desktop" tab selected. The command prompt displays the output of the "ipconfig /all" command for the "FastEthernet0" connection. The output includes details for DNS suffix, physical and link-local addresses, IPv4 and IPv6 addresses, subnet mask, default gateway, DHCP servers, IAID, Client DUID, and DNS servers.

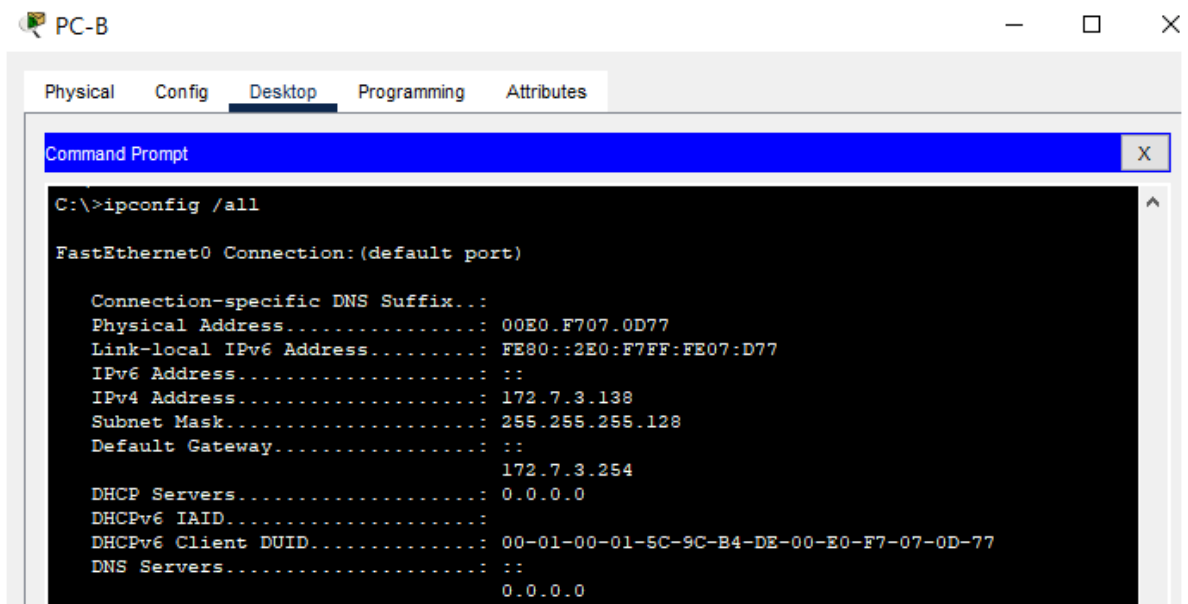
```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix... :
Physical Address. . . . . : 00D0.D3E1.81D0
Link-local IPv6 Address . . . . . : FE80::2D0:D3FF:FEE1:81D0
IPv6 Address. . . . . : ::
IPv4 Address. . . . . : 172.7.3.10
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : ::
                               172.7.3.126
DHCP Servers. . . . . : 0.0.0.0
DHCPv6 IAID. . . . . :
DHCPv6 Client DUID. . . . . : 00-01-00-01-CC-03-04-4C-00-D0-D3-E1-81-D0
DNS Servers. . . . . : ::
                               0.0.0.0
```

Fuente: Propia

Figura 6 Comprobación configuración PC-B



The screenshot shows a Windows Command Prompt window titled "PC-B" with the "Desktop" tab selected. The command prompt displays the output of the "ipconfig /all" command for the "FastEthernet0" connection. The output includes details for DNS suffix, physical and link-local addresses, IPv4 and IPv6 addresses, subnet mask, default gateway, DHCP servers, IAID, Client DUID, and DNS servers.

```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

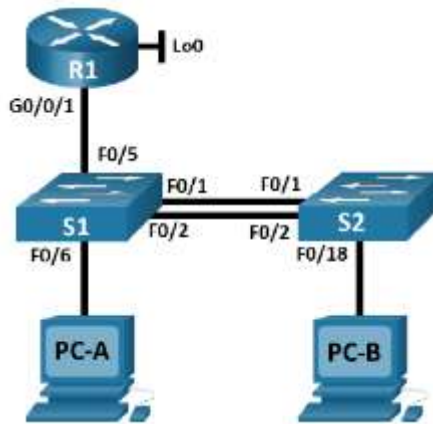
Connection-specific DNS Suffix... :
Physical Address. . . . . : 00E0.F707.0D77
Link-local IPv6 Address . . . . . : FE80::2E0:F7FF:FE07:D77
IPv6 Address. . . . . : ::
IPv4 Address. . . . . : 172.7.3.138
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : ::
                               172.7.3.254
DHCP Servers. . . . . : 0.0.0.0
DHCPv6 IAID. . . . . :
DHCPv6 Client DUID. . . . . : 00-01-00-01-5C-9C-B4-DE-00-E0-F7-07-0D-77
DNS Servers. . . . . : ::
                               0.0.0.0
```

Fuente: Propia

2. ESCENARIO 2

2.1. Topología

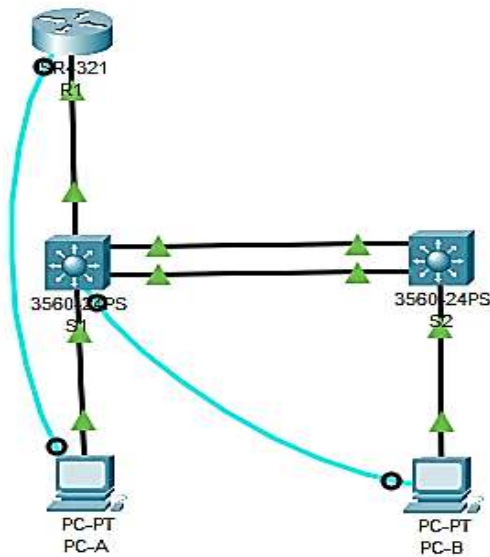
Figura 7 Topología Escenario 2 Propuesto



Fuente: Prueba de habilidades diplomado CCNA

Se realiza el montaje de la topología propuesta, se compone de un router , dos switch y dos equipos host.

Figura 8 Topología Escenario 2 en Packet Trace



Fuente: Propia

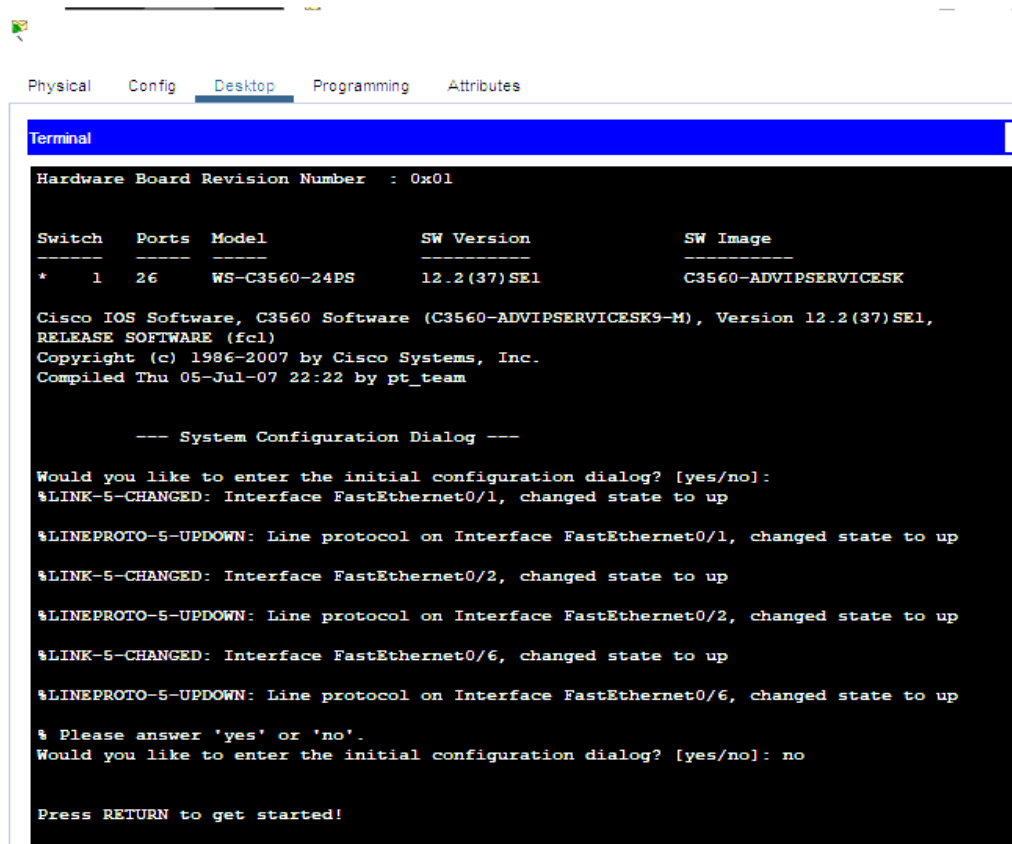
2.2. Configuración aspectos básicos de los dispositivos

Se debe inicializar y volver a cargar el router y el switch, primero se borran las configuraciones y luego se reinician. El primer paso es montar la topología solicitada en la figura 1. Se utiliza un Router (R1) , dos switchts (S1 y S2) y dos host (PC-A y PC-B)t. Se conectan siguiendo las indicaciones de la figura 2.

Para iniciar se conecta un cable de consola de PC-A a la consola de R1. En Terminal se inicializa con Enable, seguido el comando que borra la configuración de inicio : **erase startup-config**, seguido el comando **reload** para reiniciar.

Seguido de este paso se responde no a la pregunta si desea iniciar la configuración inicial, este mensaje significa que el R1 ya no tiene configuración de inicio. Conectar PC-B al S1 al puerto de consola. En PC-B ingresa al Terminal y realiza los mismos pasos anteriores que en eR1 para borrar la configuración inicial. Seguido, con el comando **delete vlan.dat**, seguido **Reload**, igualmente se responde no a la pregunta de iniciar la configuración inicial. Posterior cambia el cable de consola al S2 y realiza los mismos pasos.

Figura 9 Resultado reinicio de switch despues haber borrado la configuración inicial



```
Physical  Config  Desktop  Programming  Attributes

Terminal

Hardware Board Revision Number : 0x01

Switch  Ports  Model          SW Version      SW Image
-----  ---  -----
*  1    26    WS-C3560-24PS  12.2(37)SE1     C3560-ADVIPSERVICESK

Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!
```

Fuente: Propia

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Se ingresa a S2 (desde PC-B), **enable** . Antes de configurar la plantilla se utiliza **show sdm prefer** para verificar si el dispositivo ya tiene habilitado IPv6, al evidenciar solo IPV4 se utiliza el comando **sdm prefer dual-ipv4-and-ipv6 rounting** y luego reinicia con **reload**

Figura 10 Resultado óptimo de la configuración de la plantilla SDM

```
Switch>enable
Switch#show sdm prefer
The current template is "desktop IPv4 and IPv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:          3K
  number of directly-connected IPv4 hosts: 2K
  number of indirect IPv4 routes:        1K
number of IPv6 multicast groups:         1.125k
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes:  1K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:            0.5K
number of IPv4/MAC security aces:       1K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces:                0.625k
number of IPv6 security aces:           0.5K
```

Fuente: propia

Es importante tener en cuenta que este paso se realiza en ambos Switchs

Antes de iniciar la configuración de los dispositivos se debe tener en cuenta los siguientes datos para realizar de forma correcta conectividad tanto IPv4 como IPv6 , la creación de VLAN, Etherchannel y port-security.

Tabla 5 VLAN

Tabla de VLAN VLAN	Nombre de la VLAN
2	Docentes
3	Estudiantes
4	Invitados
5	Usuarios
6	Native

Fuente: Prueba de habilidades diplomado CCNA II-2022

Tabla 6 Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.XY.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3 <i>R1 G0/0/1.3</i>	10.XY.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.XY.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4 <i>VLAN S1 4</i> <i>S1 VLAN 4</i>	10.XY.8.98 /29	10.XY.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.XY.8.99 /29	10.XY.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC <i>PC-A NIC</i>	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Fuente: Prueba de habilidades diplomado CCNA II-2022

2.2.1. Configuración R1

Las tareas de configuración para R1 incluyen las siguientes:

Desactivar la búsqueda DNS: Se ingresa a R1 desde PC-A (mediante la conexión previa que se realizó en el paso anterior), en modo de configuración global, ingresa el comando **No ip domain-lookup**

Nombre del router: Continuando en modo de configuración global ingresa el nombre R1 mediante el comando **hostname R1**

Nombre de dominio: El nombre del dominio que se asignara es ccna-sa.com, la instrucción ingresada es **ip domain-name ccna-sa.com**
Contraseña cifrada para el modo EXEC privilegiado: La contraseña a utilizar será class con el comando **enable secret class**

Contraseña de acceso a la consola: Para asignar esta contraseña las líneas de comando en su orden son:

line console 0

password cisco /cisco es la contraseña

login / activa la contraseña

Establecer la longitud mínima para las contraseñas: En modo de configuración global se va a establecer la longitud para las contraseñas de 5 caracteres, con el comando **security password min-length 5**

Crear un usuario administrativo en la base de datos local: El usuario admin y contraseña admin1pass, la línea completa queda **username admin secret admin1pass**

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local y configurar VTY solo aceptando SSH. Los comandos en su orden son:

Line vty 0 15

Login local

transport input ssh

Cifrar las contraseñas de texto no cifrado: **service password-encryption** con este comando se aplica cifrado a las contraseñas

Configure un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que

pertenece. El comando queda: **banner motd "R1-GENNY ALEXANDRA PRISCO MORENO- Ingeniería De Sistemas"**

Habilitar el routing IPv6: Para habilitar el routing IPv6 en R1, en modo configuración global se ingresa el comando **ipv6 unicast-routing**

Configurar interfaz G0/0/1 y subinterfaces: Se debe establecer la dirección IPv4, la dirección local de enlace IPv6 como fe80::1, dirección IPv6 y activar la interfaz. Se utiliza como guía la tabla de direccionamiento, la cual indica 3 subinterfaces a configurar, R1 G0/0/1.2, R1 G0/0/1.3, R1 G0/0/1.4. Las líneas de comando para cada una de ellas en su orden son:

interface g0/0/1.2	/sub interface
encapsulation dot1Q 2	/encapsulación
description Docentes/nombre de la VLAN	
ip address 10.7.8.1 255.255.255.192	/IPv4 con mascara
ipv6 address 2001:db8:acad:a::1/64	/IPv6
ipv6 address fe80::1 link-local	/enlace local

interface g0/0/1.3	/sub interface
encapsulation dot1Q 3	/encapsulación
description Estudiantes	/nombre de la VLAN
ip address 10.7.8.65 255.255.255.224	/IPv4 con mascara
ipv6 address 2001:db8:acad:b::1/64	/IPv6
ipv6 address fe80::1 link-local	/enlace local

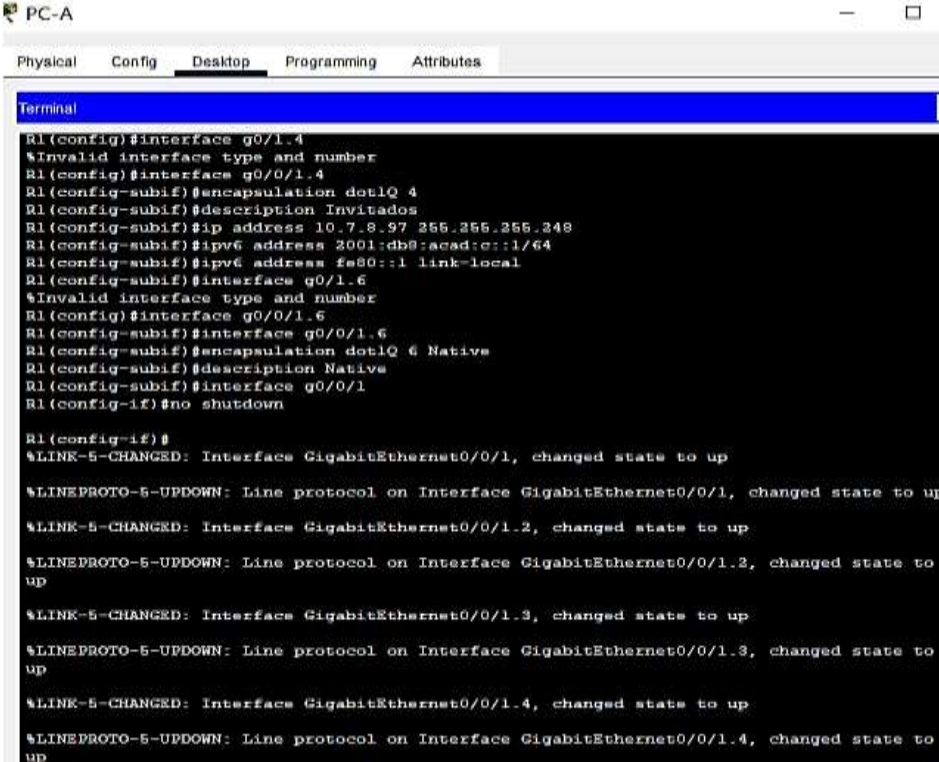
interface g0/1.4	/sub interface
encapsulation dot1Q 4	/encapsulación
description Invitados	/nombre de la VLAN
ip address 10.7.8.97 255.255.255.248	/IPv4 con mascara

ipv6 address 2001:db8:acad:c::1/64 /IPv6
ipv6 address fe80::1 link-local /enlace local

interface g0/1.6
encapsulation dot1Q 6 Native
description Native

Esta última interface corresponde a la VLAN nativa
Para activar la interfaz física con **no shutdown**

Figura 11 Configuración de interfaz G0/0/1 y subinterfaces en R1



```
PC-A
Physical Config Desktop Programming Attributes
Terminal
R1(config)#interface g0/1.4
%Invalid interface type and number
R1(config)#interface g0/0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Invitados
R1(config-subif)#ip address 10.7.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#interface g0/1.6
%Invalid interface type and number
R1(config)#interface g0/0/1.6
R1(config-subif)#interface g0/0/1.6
R1(config-subif)#encapsulation dot1Q 6 Native
R1(config-subif)#description Native
R1(config-subif)#interface g0/0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.2, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.3, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.4, changed state to up
```

Fuente: Propia

Configure el Loopback0 interface Establecer la descripción, dirección IPv4, dirección IPv6 y dirección local de enlace IPv6 como fe80::1.

Nuevamente tomamos como referencia los datos proporcionados en la tabla de direccionamiento y la línea de comandos es:

Interface loopback 0

Description loopback

ip address 209.165.201.1 255.255.255.224

ipv6 address 2001:db8:acad:209::1/64

ipv6 address fe80::1 link-local

Esta interfaz es útil en la administración del dispositivo ya asegura que por lo menos una interfaz esté siempre disponible

Generar una clave de cifrado RSA: En modo de configuración global ingresa el comando **crypto key generate rsa**, como módulo de 1024 bits

2.2.2. Configuración de S1

Para iniciar se debe conectar el cable de consola de PC-B a S1. En Terminal seguir las tareas de la tabla:

Desactivar la búsqueda DNS: En modo de configuración global, ingresa el comando **No ip domain-lookup**

Nombre del switch: Continuando en modo de configuración global ingresa el nombre S1 mediante el comando **hostname S1**

Nombre de dominio: El nombre del dominio que se asignara es ccna-sa.com, la instrucción ingresada es **ip domain-name ccna-sa.com**

Contraseña cifrada para el modo EXEC privilegiado: La contraseña a utilizar será class con el comando **enable secret class**

Contraseña de acceso a la consola: Para asignar esta contraseña las líneas de comando en su orden son:

line console 0

password cisco /cisco es la contraseña

login / activa la contraseña

Crear un usuario administrativo en la base de datos local: El usuario admin y contraseña admin1pass, en modo de configuración global la línea completa queda **username admin secret admin1pass**

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local y configurar VTY solo aceptando SSH: Los comandos en su orden son:

Line vty 0 15

Login local

transport input ssh

Cifrar las contraseñas de texto no cifrado: En modo de configuración global, **service password-encryption** con este comando se aplica cifrado a las contraseñas

Configure un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. El comando queda: **banner motd "S1-GENNY ALEXANDRA PRISCO MORENO- Ingeniería De Sistemas"**

Generar una clave de cifrado RSA: En modo de configuración global ingresa el comando **crypto key generate rsa**, como módulo de 1024 bits

Configurar la interfaz de administración (SVI) : Establecer la dirección IPv4 de capa 3, la dirección local de enlace IPv6 como FE80::98 para S1 y la dirección IPv6 de capa 3. Nuevamente tomamos como referente la la tabla de direccionamiento, esta indica que para S1 se debe configurar la VLAN4 con los parámetros allí establecidos, la configuración sería:

```
Interface vlan 4 /interface
ip address 10.7.8.98 255.255.255.248 /IPv4
ipv6 address 2001:db8:acad:c::98/64 /IPv6
ipv6 address FE80::98 link-local /enlace local
description vlan Invitados interface /descripción o nombre
no shutdown /activar la interfaz
exit
```

Configuración del gateway predeterminado: Configure la puerta de enlace predeterminada como 10.7.8.97 para IPv4 , **ip default-gateway 10.7.8.97**

2.2.3. Configuración de S2

Se realizan las mismas configuraciones de S1 en S2 pero teniendo en cuenta que el direccionamiento es diferente. Para iniciar se debe cambiar desde PB-B al puerto de consola de S2 y abrir nuevamente el terminal para ejecutar las tareas, iniciando en modo global:

Desactivar la búsqueda DNS: En modo de configuración global, ingresa el comando **No ip domain-lookup**

Nombre del switch: Continuando en modo de configuración global ingresa el nombre S1 mediante el comando **hostname S2**

Nombre de dominio: El nombre del dominio que se asignara es ccna-sa.com, la instrucción ingresada es **ip domain-name ccna-sa.com**

Contraseña cifrada para el modo EXEC privilegiado: La contraseña a utilizar será class con el comando **enable secret class**

Contraseña de acceso a la consola: Para asignar esta contraseña las líneas de comando en su orden son:

line console 0

password cisco /cisco es la contraseña

login / activa la contraseña

exit

Crear un usuario administrativo en la base de datos local: El usuario admin y contraseña admin1pass, en modo de configuración global la línea completa queda **username admin secret admin1pass**

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local y configurar VTY solo aceptando SSH: Los comandos en su orden son:

Line vty 0 15

Login local

transport input ssh

exit

Cifrar las contraseñas de texto no cifrado: En modo de configuración global, **service password-encryption** con este comando se aplica cifrado a las contraseñas

Configure un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. El comando queda: **banner motd "S2-GENNY ALEXANDRA PRISCO MORENO- Ingeniería De Sistemas"**

Generar una clave de cifrado RSA: En modo de configuración global ingresa el comando **crypto key generate rsa**, como módulo de 1024 bits

Configurar la interfaz de administración (SVI): Establecer la dirección IPv4 de capa 3, la dirección local de enlace IPv6 como FE80::98 para S1 y la dirección IPv6 de capa 3. Nuevamente se toma como referente la la tabla de direccionamiento, esta indica que para S2 se debe configurar la VLAN4 con los parámetros allí establecidos, la configuración sería:

```
Interface vlan 4 /interface
ip address 10.7.8.99 255.255.255.248 /IPv4
ipv6 address 2001:db8:acad:c::99/64 /IPv6
ipv6 address FE80::99 link-local /enlace local
description vlan Invitados interface /descripción o nombre
no shutdown /activar la interfaz
exit
```

Configuración del gateway predeterminado: Configure la puerta de enlace predeterminada como 10.7.8.97 para IPv4 , **ip default-gateway 10.7.8.97**

2.3. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

2.3.1. Configurar S1

Desde PC-B conectar al puerto de consola de S1, en Terminal seguir las tareas indicadas en la tabla:

Crear VLAN: En modo de configuración global crear las VLAN siguiendo la tabla de VLAN cada una con su respectiva descripción:

Vlan 2

Name Docentes

Vlan 3

Name Estudiantes

Vlan 4

Name Invitados

Vlan 5

Name Usuarios

Vlan 6

Crear troncos 802.1Q que utilicen la VLAN 6 nativa: Con la especificación Interfaces F0/1, F0/2 y F0/5 tal como la figura 1:

interface fa0/5 /interface conectada en S1 con R1

switchport trunk encapsulation dot1q

switchport mode trunk

.

.

switchport trunk Native vlan 6

interface range fa0/1-2 /se configura como rango de la 1 a la 2

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2: Se continua en la secuencia anterior con los siguientes comandos:

```
channel-group 1 mode active  
interface Port-channel 1  
switchport trunk encapsulation dot1q /configurar las troncales  
switchport mode trunk  
switchport trunk Native vlan 6  
channel-group 1 mode active
```

Configurar el puerto de acceso de host para VLAN 2: En la interface f0/6 la cual va de S1 a PC-A

```
Interface fa0/6  
switchport mode acces  
switchport acces vlan 2
```

Configurar la seguridad del puerto en los puertos de acceso, que para permitir 4 direcciones MAC la línea de comando quedaría: **switchport port-security maximum 4**

Proteja todas las interfaces no utilizadas: Asignar a VLAN 5, establecer en modo de acceso, agregar una descripción y apagar.

Se verifica cuales interface están en uso que para este ejercicio son fa0/1, fa0/2, fa0/5, fa0/6 y la fa0/18. Asi entoces se realiza la configuracion a las restantes:

```
Interface range fa0/3-4, fa0/7-24 /rango de interfaces no utilizadas  
Switchport mode acces  
Switchport acces vlan5  
Description No Esta En Uso  
shutdown
```

```
.  
.exit
```

2.3.2. Configurar S2

Se continua con la configuración del S2 con los mismos pasos del S1 pero teniendo en cuenta que la VLAN cambia. Primero se cambia al puerto de consola de S2, accede al Terminal. Como previamente se había asignado seguridad al switch se deben ingresar las contraseñas establecidas que fueron Cisco y class y continua con la línea de comandos en modo configuración global:

```
Vlan 2  
Name Docentes  
Vlan 3  
Name Estudiantes  
Vlan 4  
Name Invitados  
Vlan 5  
Name Usuarios  
Vlan 6  
Name native
```

Crear troncos 802.1Q que utilicen la VLAN 6 nativa: Según las indicaciones, a las Interfaces Interfaces F0/1 y F0/2

```
Interface range fa0/1-2  
shutdown  
switchport trunk encapsulation dot1q  
switchport mode trunk
```

switchport trunk Native vlan 6

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

channel-group 1 mode active

.

interface Port-channel 1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk Native vlan 6

Configurar el puerto de acceso de host para VLAN 3: En la interface f0/18 la cual va de S2 a PC-B

Interface fa0/18

switchport mode acces

switchport acces vlan 3

Configurar la seguridad del puerto en los puertos de acceso: Tener en cuenta que para permitir 4 direcciones MAC la línea de comando quedaria: **switchport port-security maximum 4**

Asegurar todas las interfaces no utilizadas: Asignar a VLAN 5, establecer en modo de acceso, agregar una descripción y apagar. Las interfaces no utilizadas van de la 3 a la 17 y de la 19 a la 24

Interface range fa0/3-17, fa0/19-24

Switchport mode acces

Switchport acces vlan 5

Description No Esta En Uso

shutdown

exit

Recordemos que se tenían las interfaces apagadas entonces se activan las dos al tiempo con el comando. (tener en cuenta que se debe hacer en ambos switches)

Interface range fa0/1-2

No shutdown

2.4. Configurar soporte de host

2.4.1. Configurar R1

Desde PC-A se accede a R1. Ingresar las contraseñas asignadas anteriormente y ejecutas las tareas solicitadas:

Configure Default Routing: Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0

ip route 0.0.0.0.0.0.0.0 loopback 0 /ruta por defecto para IPv4

.

.

ipv6 route ::/0 loopback 0 /ruta por defecto para IPv6

Configurar IPv4 DHCP para VLAN 2: Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

Se debe tener en cuenta que el rango en VLAN 2 es desde 10.7.8.1 al 10.7.8.62 teniendo en cuenta que es prefijo 26. Para hacer la creación con las últimas 10 direcciones la exclusión debe ser:

ip dhcp excluded-address 10.7.8.1 10.7.8.52 /rango excluido

```
Ip dhcp pool vlan2-Docentes /crear pool DHCP
Network 10.7.8.0 255.255.255.192
Default-router 10.7.8.1
Domain-name unad-ccna-sa.net /nombre de dominio
exit
```

Configurar DHCP IPv4 para VLAN 3: Crear un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

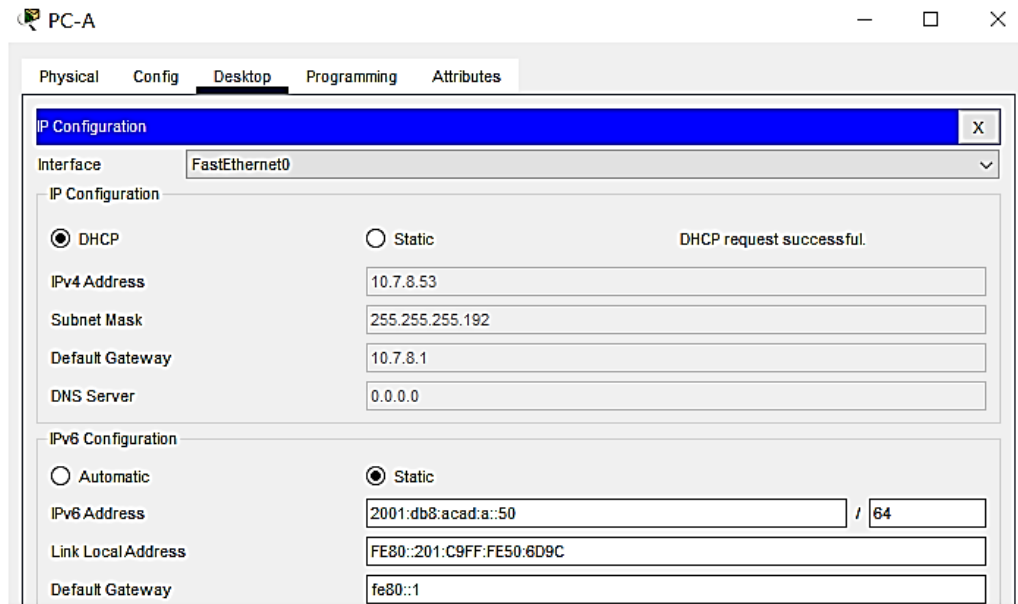
En esta el rango completo sería de la 10.7.8.65 a 10.7.8.94, entonces la exclusión queda:

```
Ip dhcp excluded-address 10.7.8.65 10.7.8.84 /rango excluido
Ip dhcp pool vlan3-Estudiantes
Network 10.7.8.64 255.255.255.224
Default-router 10.7.8.65
Domain-name unad-ccna-sb.net
exit
```

2.4.2. Configurar los servidores

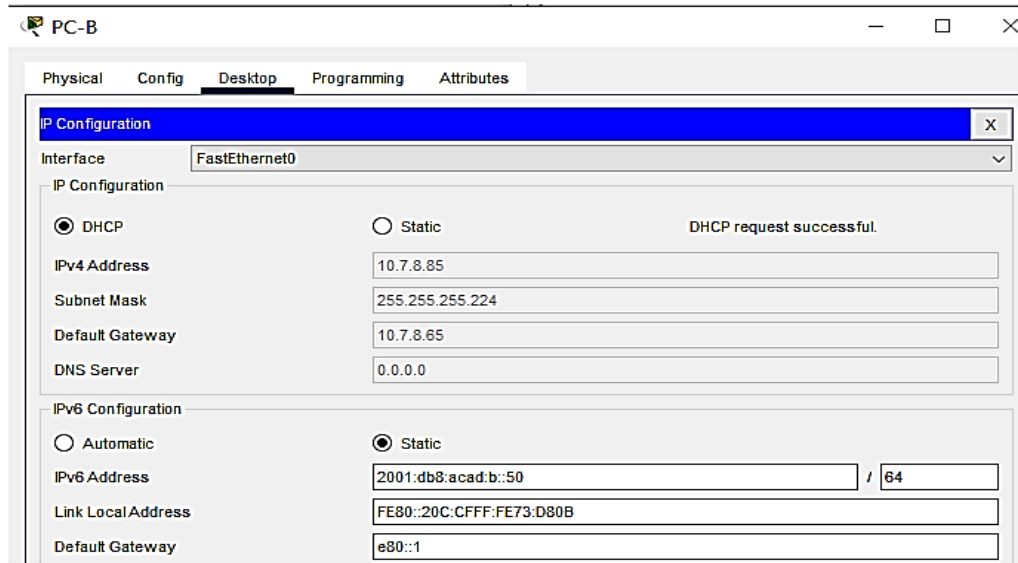
Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Ingresar a PC-A, en Desktop selecciona la opción IP Configuration, una vez allí dar clic en DHCP.

Figura 12 Configuración de PC-A con DHCP



Fuente: Propia

Figura 13 Configuración de PC-B con DHCP



Fuente: Propia

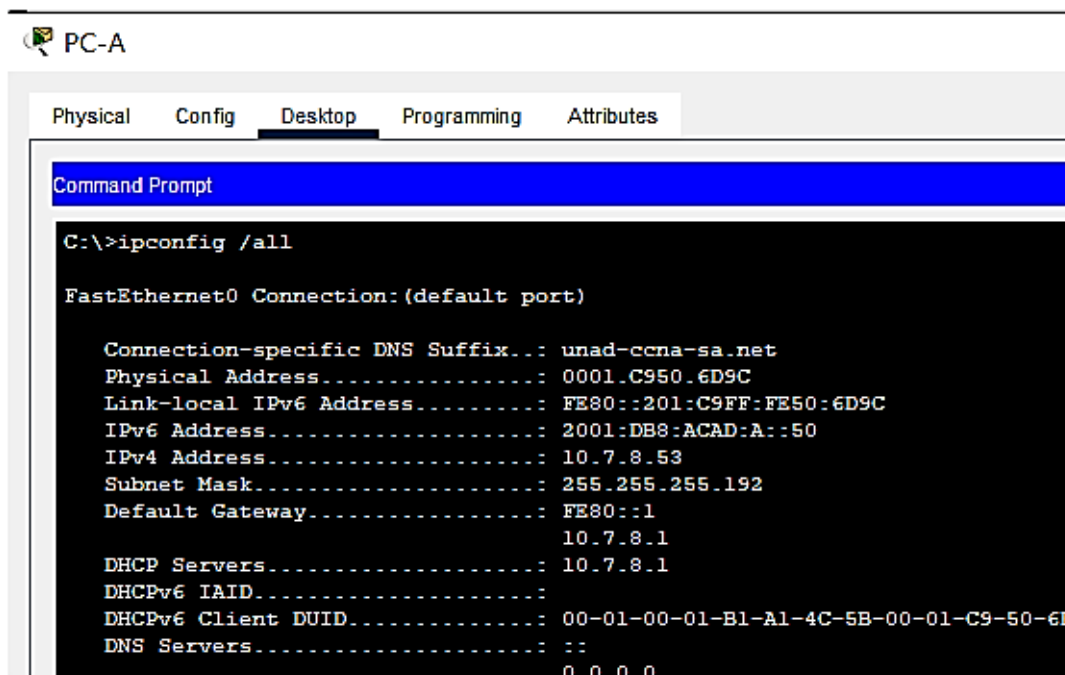
Después de configurar cada servidor, registrar las configuraciones de red del host con el comando **ipconfig /all** tanto en En PC-A y PC-B.
 Ingresar por Comand Prompt

Tabla 7 Configuración PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	0001.C950.6D9C
Dirección IP	10.7.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.7.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Propia

Figura 14 Configuración PC-A



Fuente: Propia

Tabla 8 Configuración PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	000C.CF73.D80B
Dirección IP	10.7.8.65
Máscara de subred	255.255.255.224
Gateway predeterminado	10.7.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Propia

Figura 15 Configuración PC-B

The screenshot shows the 'Desktop' tab of a PC configuration window. The 'Command Prompt' is open, displaying the output of the 'ipconfig /all' command. The output lists the following configuration details for the FastEthernet0 interface:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...: unad-ccna-sb.net
Physical Address.....: 000C.CF73.D80B
Link-local IPv6 Address.....: FE80::20C:CFFF:FE73:D80B
IPv6 Address.....: 2001:DB8:ACAD:B::50
IPv4 Address.....: 10.7.8.85
Subnet Mask.....: 255.255.255.224
Default Gateway.....: FE80::1
                        10.7.8.65
DHCP Servers.....: 10.7.8.65
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-5E-71-12-73-00-0C-CF-73-D8-0B
DNS Servers.....: ::
                        0.0.0.0
    
```

Fuente: Propia

2.5. Probar y verificar la conectividad de extremo a extremo

Mediante el comando ping se prueba la conectividad IPv4 e IPv6 entre todos los dispositivos de red. Como se muestra en la siguiente tabla e imágenes, los resultados de ping son exitosos, lo que demuestra la correcta conectividad y configuración de los dispositivos.

Tabla 9 Verificación Conectividad Escenario 2

Desde	A	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	IPv4 10.7.8.1	Ping statistics for 10.7.8.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
		IPv6 2001:db8:acad:a::1	Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1, G0/0/1.3	IPv4 10.7.8.65	Ping statistics for 10.7.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
		IPv6 2001:db8:acad:b::1	Ping statistics for 2001:DB8:ACAD:B::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1, G0/0/1.4	IPv4 10.7.8.97	nPing statistics for 10.7.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
		IPv6 2001:db8:acad:c::1	Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

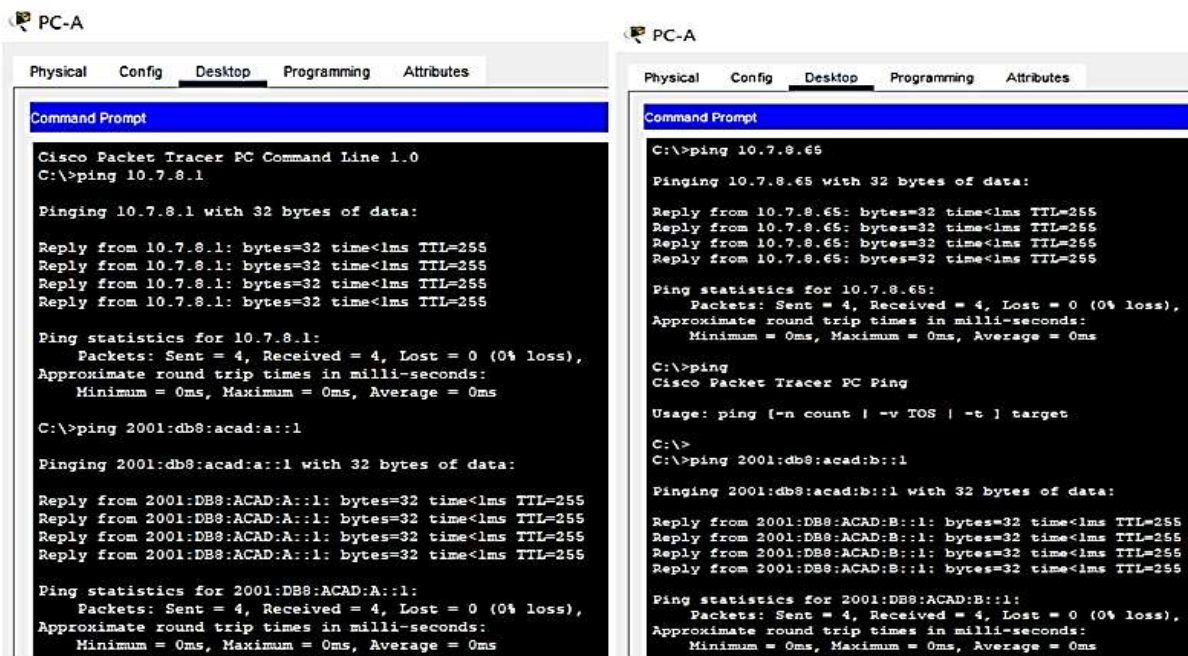
	S1, VLAN 4	IPv4 10.7.8.98	Ping statistics for 10.7.8.98: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss)
		IPv6 2001:db8:acad:c::98	Ping statistics for 2001:DB8:ACAD:C::98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	S2, VLAN 4	IPv4 10.7.8.99	Ping statistics for 10.7.8.99: Packets: Sent = 4, Received = 2, Lost = 2 (50% loss)
		IPv6 2001:db8:acad:c::99	Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	PC-B	IPv4 10.7.8.85	Ping statistics for 10.7.8.85: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss)
		IPv6 2001:DB8:ACAD:B::50	Ping statistics for 2001:DB8:ACAD:B::50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1 Bucle 0	IPv4 209.165.201.1	Ping statistics for 209.165.201.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
		IPv6 2001:db8:acad:209::1	Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
PC-B	R1 Bucle 0	IPv4	Ping statistics for 209.165.201.1:

		209.165.201.1	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
		IPv6 2001:db8:acad:209::1	Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1, G0/0/1.2	IPv4 10.7.8.1	Ping statistics for 10.7.8.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
		IPv6 2001:db8:acad:a::1	Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1, G0/0/1.3	IPv4 10.7.8.65	Ping statistics for 10.7.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
		IPv6 2001:db8:acad:b::1	Ping statistics for 2001:DB8:ACAD:B::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1, G0/0/1.4	IPv4 10.7.8.97	Ping statistics for 10.7.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
		IPv6 2001:db8:acad:c::1	Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	S1, VLAN 4	IPv4 10.7.8.98	ePing statistics for 10.7.8.98: Packets: Sent = 4, Received = 0,

			Lost = 4 (100% loss)
		IPv6 2001:db8:acad:c::98	Ping statistics for 2001:DB8:ACAD:C::98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	S2, VLAN 4	IPv4 10.7.8.99	Ping statistics for 10.7.8.99: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss)
		IPv6 2001:db8:acad:c::99	Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Fuente: Propia

Figura 16 Ping desde PC-A a R1, G0/0/1.2 y R1, G0/0/1.3



Fuente: Propia

Figura 17 Figura 16 Ping desde PC-A a R1, G0/0/1.4 y S1 VLAN 4

```

PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.7.8.97

Pinging 10.7.8.97 with 32 bytes of data:

Reply from 10.7.8.97: bytes=32 time=7ms TTL=255
Reply from 10.7.8.97: bytes=32 time<1ms TTL=255
Reply from 10.7.8.97: bytes=32 time<1ms TTL=255
Reply from 10.7.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.7.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.7.8.98

Pinging 10.7.8.98 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.7.8.98: bytes=32 time<1ms TTL=254
Reply from 10.7.8.98: bytes=32 time=9ms TTL=254

Ping statistics for 10.7.8.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 4ms

C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
    
```

Fuente: Propia

Figura 18 Ping desde PC-A a S2 VLAN 4 y PC-B

```

PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 10.7.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.7.8.99

Pinging 10.7.8.99 with 32 bytes of data:

Reply from 10.7.8.99: bytes=32 time=1ms TTL=254
Reply from 10.7.8.99: bytes=32 time<1ms TTL=254
Reply from 10.7.8.99: bytes=32 time<1ms TTL=254
Reply from 10.7.8.99: bytes=32 time=10ms TTL=254

Ping statistics for 10.7.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 2001:db8:acad:c::99

Pinging 2001:db8:acad:c::99 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=16ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms

PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.7.8.85

Pinging 10.7.8.85 with 32 bytes of data:

Reply from 10.7.8.85: bytes=32 time<1ms TTL=127
Reply from 10.7.8.85: bytes=32 time<1ms TTL=127
Reply from 10.7.8.85: bytes=32 time<1ms TTL=127
Reply from 10.7.8.85: bytes=32 time<1ms TTL=127

Ping statistics for 10.7.8.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:DB8:ACAD:B::50

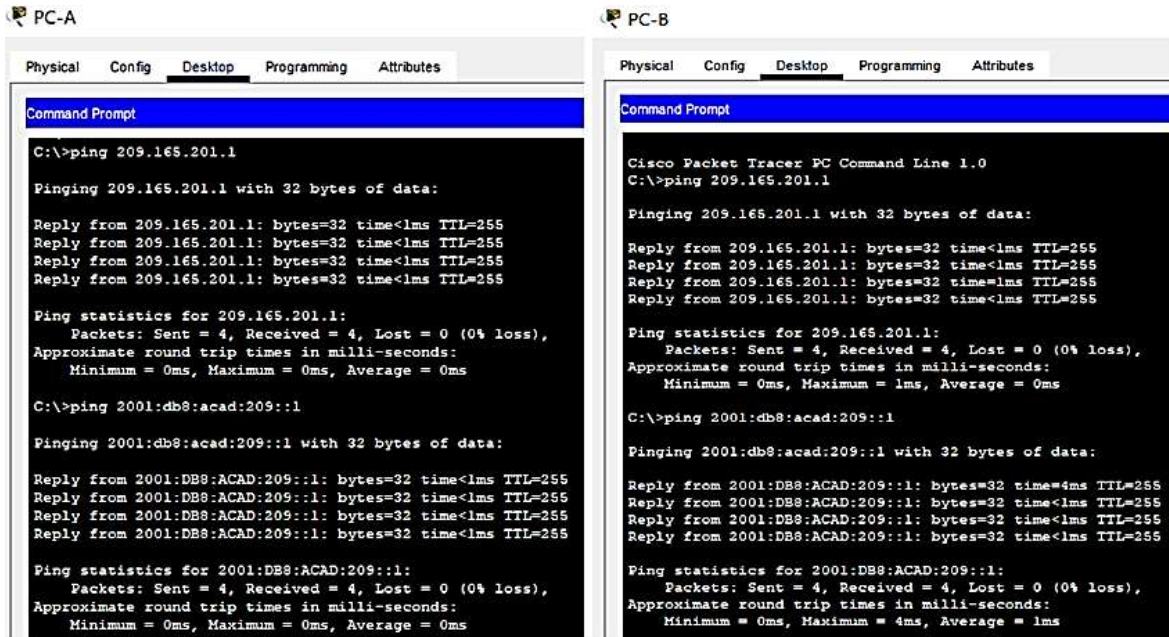
Pinging 2001:DB8:ACAD:B::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
    
```

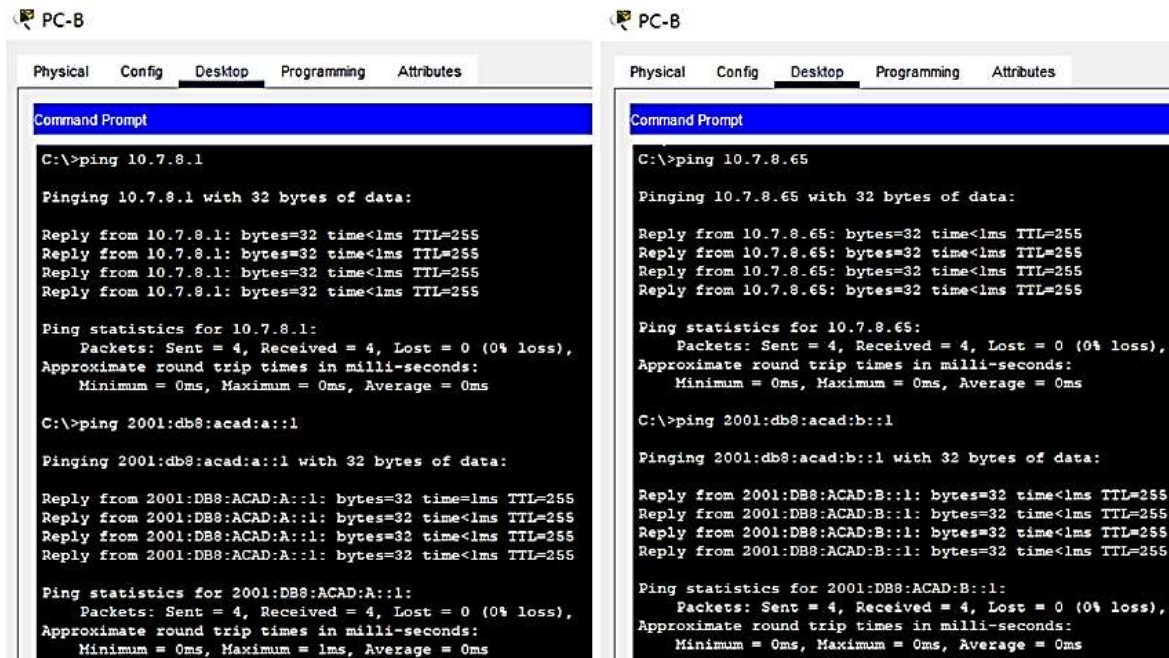
Fuente: Propia

Figura 19 Ping a R1 Bucle 0 desde PC-A y PC-B



Fuente: Propia

Figura 20 Ping desde PC-B a R1, G0/0/1.2 y R1, G0/0/1.3



Fuente: Propia

Figura 21 Ping desde PC-B a R1, G0/0/1.4 y S1 VLAN4

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.7.8.97
Pinging 10.7.8.97 with 32 bytes of data:
Reply from 10.7.8.97: bytes=32 time<1ms TTL=255
Reply from 10.7.8.97: bytes=32 time<1ms TTL=255
Reply from 10.7.8.97: bytes=32 time<1ms TTL=255
Reply from 10.7.8.97: bytes=32 time<1ms TTL=255
Ping statistics for 10.7.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2001:db8:acad:c::1
Pinging 2001:db8:acad:c::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.7.8.98
Pinging 10.7.8.98 with 32 bytes of data:
Request timed out.
Reply from 10.7.8.98: bytes=32 time<1ms TTL=254
Reply from 10.7.8.98: bytes=32 time<1ms TTL=254
Reply from 10.7.8.98: bytes=32 time<1ms TTL=254
Reply from 10.7.8.98: bytes=32 time<1ms TTL=254
Ping statistics for 10.7.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2001:db8:acad:c::98
Pinging 2001:db8:acad:c::98 with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Propia

Figura 22 Ping desde PC-B a S2 VLAN4

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.7.8.99
Pinging 10.7.8.99 with 32 bytes of data:
Request timed out.
Reply from 10.7.8.99: bytes=32 time<1ms TTL=254
Reply from 10.7.8.99: bytes=32 time=1ms TTL=254
Reply from 10.7.8.99: bytes=32 time<1ms TTL=254
Ping statistics for 10.7.8.99:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:db8:acad:c::99
Pinging 2001:db8:acad:c::99 with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Propia

CONCLUSIONES

La realización de este diplomado a través de sus escenarios permite la práctica de realizar una adecuada gestión de redes, desde su montaje inicial seleccionando y conectando los dispositivos pasando por la configuración en cuanto a direccionamiento IP, enrutamiento y seguridad hasta su optimización y solución de posibles fallos en las redes.

Dentro de los resultados se tiene la creación de redes mediante la utilización de la herramienta Packet Tracer de CISCO, esta herramienta permite simular escenarios y topologías de forma muy real y dinámica. Dichas simulaciones se ajustan a las realidades con las cuales nos podemos encontrar en nuestro ejercicio profesional, por ejemplo la configuración, administración y monitoreo de una red doméstica, red empresarial, configuración de dispositivos IoT, etc.

La correcta administración y optimización de las redes es un punto muy importante como futuros profesionales de sistemas, en un primer escenario se tiene la posibilidad de aplicar el subneteo permitiendo el mejoramiento de la administración ya que cada subred funciona de manera independiente en el envío y recepción de paquetes. Otro punto relevante es la implementación de medidas de seguridad en la red, la encriptación de contraseñas, seguridad en puertos, con protocolos como el SSH, entre otros los cuales fortalecen la seguridad de una red.

REFERENCIAS BIBLIOGRAFICAS

CASTAÑO, RIBES. Redes locales. ed. Madrid: Macmillan Iberia, S.A. . {En línea} (2013) . {05 de octubre de 2022} Disponible en: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?>

CISCO. Cisco [página web]. {05 de octubre de 2022} Disponible en <https://lms.netacad.com/course/view.php?id=1467468>

DORDOIGNE, José. Redes informáticas-Nociones fundamentales (5ª edición):(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...). Ediciones Eni. {En línea} (2015). {18 de noviembre de 2022} Disponible en:<https://books.google.es/books?id=HuwY1L0PEq8C&lpg=PA348&ots=N-1tanaQiy&dq=redes%20lan%20man%20y%20wan&lr&hl=es&pg=PA348#v=onepage&q=redes%20lan%20man%20y%20wan&f=false>

LÓPEZ, Ricardo. Enrutamiento y configuración de redes. Fundacion Universitaria del Area Andina. {En línea} (2018).{18 de noviembre de 2022} Disponible en: <https://digitk.areandina.edu.co/bitstream/handle/areandina/1495/74%20ENRUTAMIENTO%20Y%20CONFIGURACION%20DE%20REDES.pdf?sequence=1>

MERCADO, Gustavo. Implementación y Evaluación de métodos de Traslación de Protocolos para la transición IPv4-IPv6." XVII Congreso Argentino de Ciencias de la Computación. {En línea} (2011). {18 de noviembre de 2022} Disponible en: <http://sedici.unlp.edu.ar/handle/10915/18769>

SANCHEZ, Gerardo. Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6. {En línea} (2005) . {05 de octubre de 2022} Disponible en:http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/

ANEXOS

Anexo A – Descarga de archivo de simulacion Escenario 1 y Escenario 2

Enlace: <https://drive.google.com/drive/folders/1rIQ6V4pHRdpF-GdnorxfL6U2FiQWFc?usp=sharing>