

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA

CISCO

ANDRES MAURICIO PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI  
INGENIERÍA DE SISTEMAS  
POPAYAN  
2022

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

ANDRES MAURICIO PEREZ

Diplomado De Opción De Grado Presentado Para Optar El  
Título De Ingeniero De Sistemas

DIRECTOR:  
PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI  
INGENIERÍA DE SISTEMAS  
POPAYÁN  
2022

Nota de aceptación:

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Popayán, 17 de diciembre de 2022

## **AGRADECIMIENTOS**

Agradezco a los tutores que han sido parte fundamental para el desarrollo de los conocimientos y por ser esas personas que guían el camino de la formación para futuros profesionales. También agradezco a mis padres que desde siempre me han apoyado en las decisiones que sean beneficiosas para mí.

## CONTENIDO

AGRADECIMIENTOS .....	4
LISTA DE FIGURAS .....	8
GLOSARIO .....	11
RESUMEN.....	12
ABSTRACT.....	13
INTRODUCCION.....	14
DESARROLLO DEL TRABAJO.....	15
Escenario 1 .....	15
Condiciones de direccionamiento .....	16
Configuraciones de direccionamiento en los dispositivos .....	17
Configuraciones de direccionamiento por interfaz en los hosts .....	20
Verificación de conectividad de los dispositivos .....	22
Escenario 2.....	25
Inicialización y carga en el router y el switch .....	26

Configurar R1 .....	27
Configurar S1 y S2.....	30
Configurar infraestructura de red VLAN, Trunking y EtherChannel en S1 y S2. .....	33
Configurar soporte de host en R1 .....	37
Configuración de direccionamiento por interfaz de los hosts.....	38
Probar y verificar la conectividad de extremo a extremo .....	40
CONCLUSIONES .....	48
BIBLIOGRAFÍA.....	49
ANEXOS.....	50

## LISTA DE TABLAS

Tabla 1. Características de la dirección IPv4 para LAN1. ....	16
Tabla 2. Características de la dirección IPv4 para LAN2. ....	17
Tabla 3. Direcciones IP para las interfaces de conexión de los dispositivos.....	17
Tabla 4. Listado de VLAN's. ....	26
Tabla 5. Lista con las direcciones a configurar. ....	27
Tabla 6. Tareas para configurar en R1 .....	27
Tabla 7. Tareas para configurar S1 y S2 .....	30
Tabla 8. Tareas para configuración de infraestructura de red en S1 .....	33
Tabla 9. Tareas para configuración de infraestructura de red en S2 .....	34
Tabla 10. Tareas para configuración de soporte host en R1.....	37

## LISTA DE FIGURAS

Figura 1. Primer escenario según la guía de trabajo.....	15
Figura 2. Simulación realizada con base al escenario de la figura 1.....	15
Figura 3. Direccionamiento IPv4 en el host A .....	20
Figura 4. Direccionamiento IPv4 en el host B .....	21
Figura 5. Escenario de red con las interfaces activadas.....	21
Figura 6. Prueba de ping desde PCA a R1 G0/0/0 .....	22
Figura 7. Prueba de ping desde PCA a R1 G0/0/1 .....	22
Figura 8. Prueba de ping desde PCA a S1 VLAN 1 .....	23
Figura 9. Prueba de ping desde PCA a PCB .....	23
Figura 10. Prueba de ping desde PCB a R1 G0/0/0 .....	23
Figura 11. Prueba de ping desde PCB a R1 G0/0/1 .....	24
Figura 12. Prueba de ping desde PCB a PCA. ....	24
Figura 13. Segundo escenario según la guía de trabajo.....	25
Figura 14. Simulación realizada con base al escenario de la figura 13.....	25

Figura 15. Visualización de las interfaces en el router R1 .....	30
Figura 16. Visualización de las VLAN e interfaces configuradas en S1 .....	36
Figura 17. Visualización de las VLAN e interfaces configuradas en S2 .....	37
Figura 18. Uso de DHCP y asignación de IPv6 en PCA. ....	38
Figura 19. Uso de DHCP y asignación de IPv6 en PCB. ....	39
Figura 20. Información de direccionamiento en PCA. ....	39
Figura 21. Información de direccionamiento en PCB. ....	40
Figura 22. Ping desde PCA hacia G0/0/1.20 en IPv4 e IPv6 .....	41
Figura 23. Ping desde PCA hacia G0/0/1.30 en IPv4 e IPv6 .....	41
Figura 24. Ping desde PCA hacia G0/0/1.40 en IPv4 e IPv6 .....	42
Figura 25. Ping desde PCA hacia S1 VLAN 40 .....	42
Figura 26. Ping desde PCA hacia S2 VLAN 40 .....	43
Figura 27. Ping desde PCA hacia PCB IPv4 e IPv6. ....	43
Figura 28. Ping desde PCA hacia R1 Loop0. ....	44

Figura 29. Ping desde PCB hacia R1 Loop0.....	44
Figura 30. Ping desde PCB hacia G0/0/1.20 en IPv4 e IPv6 .....	45
Figura 31. Ping desde PCB hacia G0/0/1.30 en IPv4 e IPv6 .....	45
Figura 32. Ping desde PCB hacia G0/0/1.40 en IPv4 e IPv6 .....	46
Figura 33. Ping desde PCB hacia S1 VLAN 40 .....	46
Figura 34. Ping desde PCB hacia S2 VLAN 40 .....	47

## GLOSARIO

**PACKET TRACER:** Es un programa enfocado en la simulación de redes ya bien sea por uso de interfaz gráfica o manual mediante códigos de red para la configuración de dispositivos de telecomunicaciones como routers, switches, repetidores entre otros. <sup>1</sup>

**OSPF:** Es un protocolo de redes con el cual se puede gestionar rutas y nuevos caminos entre varios dispositivos conectados empleando el algoritmo Dijkstra para calcular la ruta más corta en una conexión ya bien sea para comunicación o relación de dispositivos vecinos. <sup>2</sup>

**DHCP:** Es un protocolo de red que tiene gestión tipo cliente/servidor con el cual se asigna de forma dinámica con base a un dirección establecida un host o dirección a otros dispositivos de la red, asignándoles de igual manera, una gateway y mascara de red. <sup>3</sup>

**PROTOCOLO:** Los protocolos de red suelen ser un conjunto de reglas de redes los cuales efectúan sobre las distintas capas del modelo OSI con el fin de gestionar y realizar funciones en un escenario de red ya bien sea para la comunicación o administración de estos. <sup>4</sup>

**VLAN:** Es como tal un grupo o conexión de red de área local virtual con las cuales se establecen o se crean redes lógicas independientes todas dentro de una red física con el fin de categorizar y gestionar mejor los equipos en una red. <sup>5</sup>

---

<sup>1</sup> «Manual de uso Packet Tracer 5», asej.com.co, [http://asej.com.co/files/23\\_10\\_2013\\_02\\_24\\_37\\_upload.pdf](http://asej.com.co/files/23_10_2013_02_24_37_upload.pdf), ingreso el 15 de diciembre 2022

<sup>2</sup> «Guía para el análisis del protocolo de encaminamiento OSPF en redes inalámbricas aplicado en nuevas tecnologías», repository.usta.edu.co, <https://repository.usta.edu.co/bitstream/handle/11634/22858/2020fernandoflorez.pdf?sequence=6&isAllowed=y>, ingreso el 15 de diciembre 2022

<sup>3</sup> «Diseño e implementación de una aplicación prototipo para ofrecer el servicio de DHCP sobre una SDN», bibdigital.epn.edu.ec, <https://bibdigital.epn.edu.ec/handle/15000/14783>, ingreso el 15 de diciembre 2022

<sup>4</sup> «Protocolos de redes: guía completa con los protocolos básicos», <https://www.redeszone.net/>, <https://www.redeszone.net/tutoriales/internet/protocolos-basicos-redes/>, ingreso el 15 de diciembre 2022

<sup>5</sup> «VLANs: Qué son, tipos y para qué sirven», <https://www.redeszone.net/>, <https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>, ingreso el 15 de diciembre 2022

## RESUMEN

En este informe se dispone el desarrollo y la solución con respecto al trabajo “Evaluación – Prueba de habilidades practica CCNA”, en el cual se identifica los conocimientos adquiridos durante el transcurso del diplomado sobre direccionamiento, protocolos, configuraciones básicas y seguridad en dispositivos de red que en este caso se identifican tras el desarrollo de dos escenarios en el programa Packet Tracer, como tal, en estos dos escenarios se realiza primero una configuración básica de nombre, asignación de credenciales, uso de cifrado para contraseñas y configuraciones para consola, con ello se emplea VLSM para realizar el calculo de direccionamiento con base a una IP fija cambiando ciertos parámetros que se detallan mas adelante, y con ello asignar dichos rangos a las interfaces de los dispositivos y con ello realizar pruebas de ping para garantizar que exista conexión entre ellos.

Con base al segundo escenario se realiza el procedimiento similar mencionado anteriormente, ahora empleando sub-interfaces, VLAN's y configuración de las interfaces para trabajar en modo troncal y a su vez, empleando también el protocolo IPv6 en cada uno de los dispositivos.

Por último, se expone conclusiones generales sobre lo observado durante el desarrollo del trabajo, los inconvenientes y posibles mejoras a dichas problemáticas mencionadas.

Palabras clave: DIRECCIONAMIENTO, DISPOSITIVO, ESCENARIO, PACKET TRACER, VLAN

## ABSTRACT

This report presents the development and solution regarding the work "Evaluation - Test of CCNA practical skills", in which the knowledge acquired during the course of the course on addressing, protocols, basic configurations and security in network devices is identified. that in this case are identified after the development of two scenarios in the Packet Tracer program, as such, in these two scenarios a basic configuration of name, assignment of credentials, use of encryption for passwords and configurations for console is carried out first, with this VLSM is used to calculate addressing based on a fixed IP by changing certain parameters that are detailed later, and thereby assign these ranges to device interfaces and thereby perform ping tests to ensure that there is a connection between them.

Based on the second scenario, the similar procedure mentioned above is carried out, now using sub-interfaces, VLANs and interface configuration to work in trunk mode and, in turn, also using the IPv6 protocol in each of the devices.

Finally, general conclusions are presented about what was observed during the development of the work, the inconveniences, and possible improvements for about problems mentioned.

Keywords: ADDRESSING, DEVICE, SCENARIO, PACKET TRACER, VLAN

## INTRODUCCION

La comprensión del funcionamiento de los dispositivos de red o que hacen uso de esta que se emplean en el día a día suele ser un campo ignorado por las personas que no tienen relación con esta temática o no se ven interesados ya bien sea porque desde un punto de vista externo se suelen ver estas temáticas complejas y de difícil acceso, pero que mediante programas como Packet Tracer se puede realizar una introducción de forma más amena y sencilla a estos conocimientos.

Como tal esa es la finalidad que se busca con este curso ya que mediante el uso de dichos programas para emulación o simulación de redes, se puede llevar de manera sencilla, la aprehensión de las temáticas sobre direccionamiento, enrutamiento, aplicación de protocolos, cálculo de direccionamiento entre otros, que mediante el estudio de solo teoría puede llegar a ser tedioso y que en campo puede llegar a ser complicado manipular dichos dispositivos si no se tienen los conocimientos y que mediante el uso de estos programas no supone ningún problema.

El desarrollo de los dos escenarios mencionados anteriormente permiten exponer precisamente el cómo se llegó a recopilar y comprender de manera rápida, los distintos tipos de conocimientos, herramientas y ayudas con las que se puede disponer al emplear Packet Tracer y que a su vez, agiliza y permite el desarrollo de este trabajo puesto que en ambos escenarios se aplican dichos conocimientos de forma secuencial, haciendo uso de la CLI o interfaz gráfica de los dispositivos y así mismo usar la terminal de comandos con las instrucciones ya conocidas para garantizar eficiencia y funcionamiento en ambos escenarios.

## DESARROLLO DEL TRABAJO

A continuación, se presenta el desarrollo de los dos escenarios de forma seccionada:

### Escenario 1.

Para la primera parte, la guía de trabajo sugiere el siguiente escenario de red.

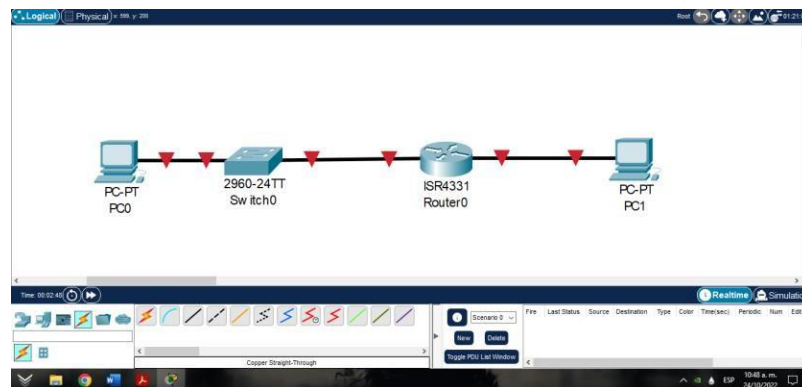
Figura 1. Primer escenario según la guía de trabajo.



Fuente: Prueba de habilidades.

Para este caso como ya se mencionó, la simulación de los escenarios se lleva a cabo en el programa Packet Tracer.

Figura 2. Simulación realizada con base al escenario de la figura 1.



Fuente: Autor

Para este primer escenario se pide configurar los dispositivos con los siguientes parámetros y requisitos teniendo en cuenta primeramente dicho enunciado:

### **Condiciones de direccionamiento**

*Cada estudiante tomara el direccionamiento 172.XY.3.0 donde XY corresponde a los dos ultimo dígitos del documento.*

Por ello, la dirección IP que se usa es 172.31.3.0.

Analizando la figura 1 y los requisitos que se mencionan en la guía, la cantidad total de hosts que son necesarios son 80, al analizar la IP a utilizar y con los conocimientos de direccionamiento se sabe con certeza que al usar el ultimo octeto se puede contar con 254 hosts disponibles (teniendo en cuenta dos direcciones para el gateway y el broadcast). Los requisitos que lista la guía de forma más detallada son:

- Hosts para subred LAN1: 60
- Hosts para subred LAN2: 20
- R1 G0/0/1 para la última dirección de host de la subred LAN1.
- R1 G0/0/0 para la última dirección de host de la subred LAN2.
- PC-A para la décima dirección de host de la subred LAN1.
- PC-B para la décima dirección de host de la subred LAN2.

Como se observa que la LAN1 requiere 60 hosts, el direccionamiento será:

Tabla 1. Características de la dirección IPv4 para LAN1.

Dirección IP	172.31.3.0/26.
Rango de direcciones	172.31.3.1-172.31.3.62
Total host	64
Broadcast	172.31.3.63

Fuente: Autor

Con base a la tabla 1, se puede observar que se puede garantizar que se tengan 60 hosts y quedan 2 direcciones disponibles excluyendo la gateway y el broadcast.

Para la LAN2 se necesitan 20 hosts, entonces el direccionamiento será:

Tabla 2. Características de la dirección IPv4 para LAN2.

Segmentación de IP	172.31.3.64/27.
Rango de hosts	172.31.3.65-172.31.3.94
Total host	32
Broadcast	172.31.3.95

Fuente: Autor

Con base a la tabla 2, se puede observar que se puede garantizar que se tengan 20 hosts y quedan 10 direcciones disponibles excluyendo la gateway y el broadcast.

Al realizar el direccionamiento para las LAN, los requisitos previos mencionados anteriormente para el direccionamiento de las interfaces serán:

Tabla 3. Direcciones IP para las interfaces de conexión de los dispositivos.

R1 G0/0/1	172.31.3.62/26
R1 G0/0/0	172.31.3.94/27
PC-A	172.31.3.11/26
PC-B	172.31.3.75/27

Fuente: Autor

### ***Configuraciones de direccionamiento en los dispositivos***

Con los direccionamientos calculados para los dispositivos de la red y las interfaces respectivas, se accede al escenario de red construido en Packet Tracer y mediante la CLI de cada dispositivo se ingresan los comandos respectivos para cada uno, así como para la configuración básica de datos y parámetros:

- enable
- conf t #Modo de configuración del terminal
- hostname R1 #Asignacion de nombre al router
- int gi 0/0/0 #Ingreso la interfaz especificada
- ip address 172.31.3.94 255.255.255.224 #Asignacion de dirección
- no shutdown #Habilitar interfaz
- exit
- int gi 0/0/1 #Ingreso la interfaz especificada
- ip address 172.31.3.62 255.255.255.192 #Asignacion de dirección
- no shutdown #Habilitar interfaz

Con las configuraciones básicas en los dispositivos, se procede a configurar los parámetros básicos en cuanto a la seguridad en los dispositivos como se observa a continuación:

- no ip domain-lookup #desactiva traducción de nombre dirección del dispositivo
- security passwords min-length 10 #longitud de contraseña
- username admin password admin1pass #usuario y contraseña
- line console 0 #modo de configuración en línea
- login local #habilita base de datos local
- exit
- line vty 0 4 #acceso a las líneas virtuales de 0 a 4
- login local #autenticacion del usuario
- exit
- enable secret ciscoenpass #asignacion contraseña encriptada
- line console 0 #modo de configuración en línea
- password ciscoconpass #asignacion contraseña
- exit

Finalmente, se configura un nombre de dominio, uso del servicio de cifrado, configuración de banner, permitir conexiones SSH y guardado de configuración.

- ip domain name cca-sa.com #asignacion de nombres de dominios
- crypto key generate rsa #uso del servicio de cifrado
- banner motd % R1 Andres Mauricio Perez Ingeniería de sistemas %

- ip ssh version 2 #establecer versión de SSH
- line vty 0 4 #acceso a las líneas virtuales de 0 a 4
- transport input ssh #permitir conexiones SSH en vty
- login local #Autenticación del usuario.
- exit
- copy running-config startup-config #guardado de configuración

De igual manera, se lista los comandos empleados para la configuración básica en el switch S1.

- enable
- conf t #Modo de configuración del terminal
- hostname S1 #Asignación de nombre al switch
- no ip domain-lookup #desactiva traducción de nombre dirección del dispositivo
- username admin password admin1pass
- line console 0 #modo de configuración en línea
- login local #autenticación del usuario
- exit
- line vty 0 4 #acceso a las líneas virtuales de 0 a 4
- login local #autenticación del usuario
- exit
- enable secret ciscoenpass #asignación contraseña encriptada
- line console 0 #modo de configuración en línea
- password ciscoconpass #asignación contraseña
- exit

Con la siguiente sección de comandos, se asigna el nombre del dominio, el mensaje de inicio, se configuran las líneas VTY para conexiones SSH, se genera clave de cifrado RSA y se autentifica mediante login.

- ip domain name ccna-sa.com #asignación de nombres de dominios
- banner motd % S1 Andres Mauricio Perez Ingeniería de sistemas %  
#configuración nombre
- ip ssh version 2 #establecer versión de SSH
- crypto key generate rsa #uso del servicio de cifrado
- line vty 0 4 #acceso a las líneas virtuales de 0 a 4
- transport input ssh #permitir conexiones SSH en vty

- login local #Autenticacion del usuario.
- exit

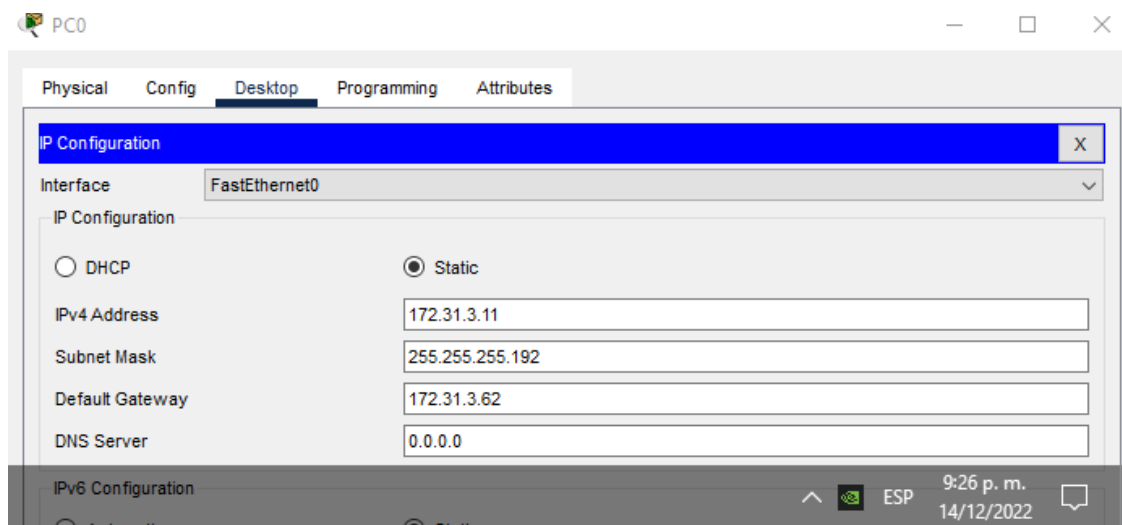
Finalmente se configura la interfaz VLAN1 y el direccionamiento asignado a esta.

- int vlan 1 #ingreso a la interfaz vlan1
- ip address 172.31.3.2 255.255.255.192 #asignacion de dirección
- no shutdown #activacion de interfaz
- exit
- ip default-gateway 172.31.3.62 #asignacion de gateway predeterminada
- exit
- copy running-config startup-config #guardado de configuración

### **Configuraciones de direccionamiento por interfaz en los hosts**

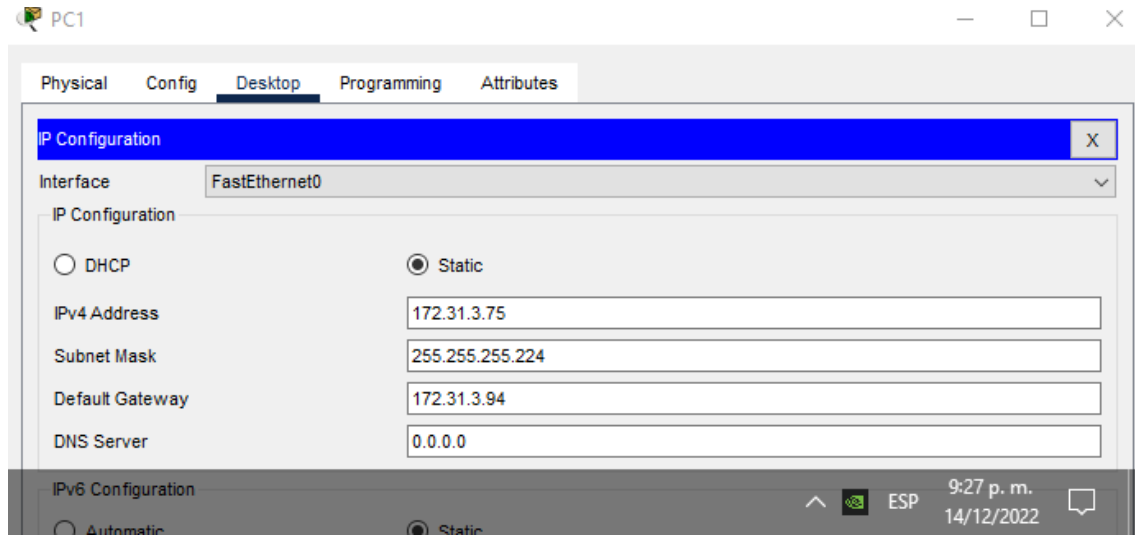
Luego de realizar las configuraciones en los routers y switches, se accede a la interfaz de los hosts y se asignan sus respectivos direccionamientos.

Figura 3. Direccionamiento IPv4 en el host A.



Fuente: Autor

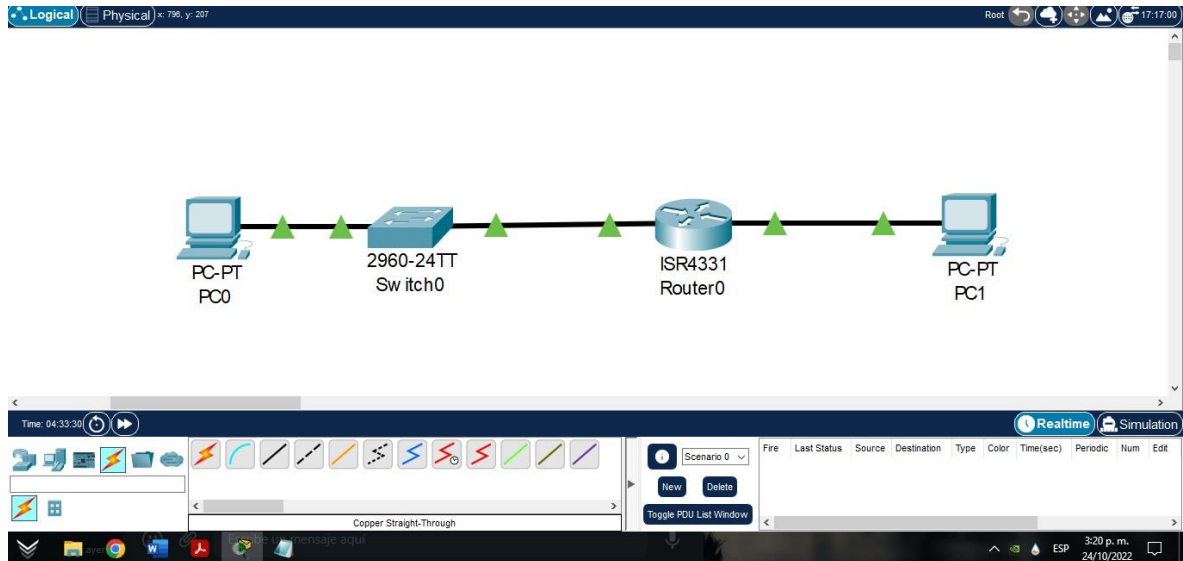
Figura 4. Direccionamiento IPv4 en el host B.



Fuente: Autor

Al realizar todas las configuraciones, se puede observar en la siguiente figura como el color de las interfaces cambian a estado verde, lo que indica que estas encuentran activadas.

Figura 5. Escenario de red con las interfaces activadas.



Fuente: Autor

## Verificación de conectividad de los dispositivos

Luego de esto, se realizan pruebas de ping desde los hosts a cada uno de los dispositivos de la red para verificar la conectividad.

Con las pruebas de ping realizadas anteriormente se puede constatar que el direccionamiento fue acertado.

Figura 6. Prueba de ping desde PCA a R1 G0/0/0

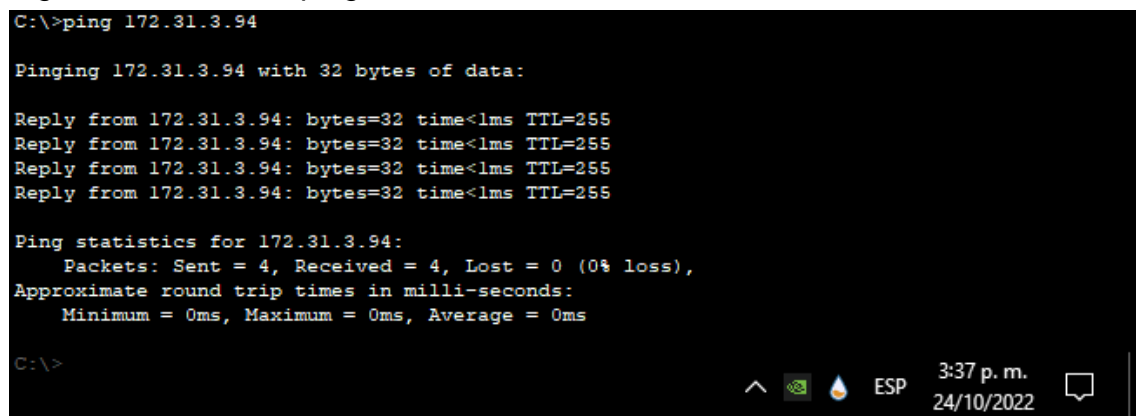
```
C:\>ping 172.31.3.94

Pinging 172.31.3.94 with 32 bytes of data:

Reply from 172.31.3.94: bytes=32 time<lms TTL=255
Reply from 172.31.3.94: bytes=32 time<lms TTL=255
Reply from 172.31.3.94: bytes=32 time<lms TTL=255
Reply from 172.31.3.94: bytes=32 time<lms TTL=255

Ping statistics for 172.31.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



Fuente: Autor

Figura 7. Prueba de ping desde PCA a R1 G0/0/1

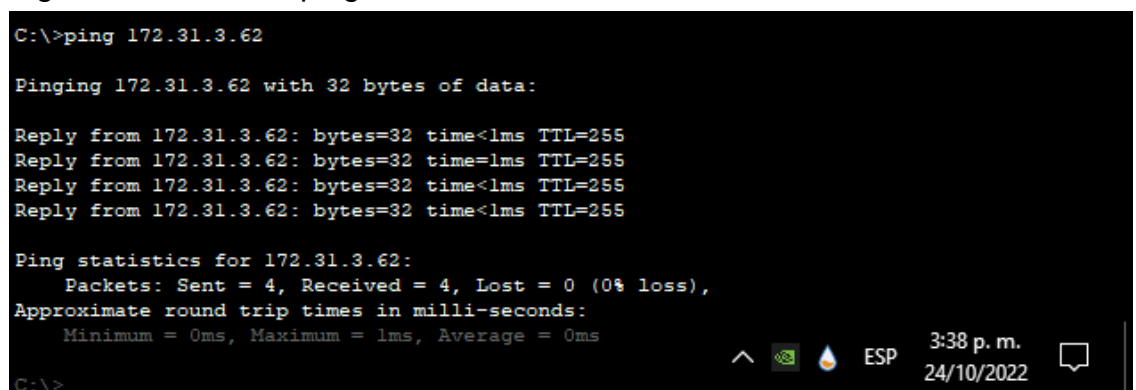
```
C:\>ping 172.31.3.62

Pinging 172.31.3.62 with 32 bytes of data:

Reply from 172.31.3.62: bytes=32 time<lms TTL=255
Reply from 172.31.3.62: bytes=32 time=lms TTL=255
Reply from 172.31.3.62: bytes=32 time<lms TTL=255
Reply from 172.31.3.62: bytes=32 time<lms TTL=255

Ping statistics for 172.31.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = lms, Average = 0ms

C:\>
```



Fuente: Autor

Figura 8. Prueba de ping desde PCA a S1 VLAN 1

```
C:\>ping 172.31.3.3

Pinging 172.31.3.3 with 32 bytes of data:

Reply from 172.31.3.3: bytes=32 time<lms TTL=255
Reply from 172.31.3.3: bytes=32 time<lms TTL=255
Reply from 172.31.3.3: bytes=32 time<lms TTL=255
Reply from 172.31.3.3: bytes=32 time<lms TTL=255

Ping statistics for 172.31.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 9. Prueba de ping desde PCA a PCB

```
C:\>ping 172.31.3.75

Pinging 172.31.3.75 with 32 bytes of data:

Reply from 172.31.3.75: bytes=32 time<lms TTL=127
Reply from 172.31.3.75: bytes=32 time<lms TTL=127
Reply from 172.31.3.75: bytes=32 time<lms TTL=127
Reply from 172.31.3.75: bytes=32 time<lms TTL=127

Ping statistics for 172.31.3.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 10. Prueba de ping desde PCB a R1 G0/0/0

```
C:\>ping 172.31.3.94

Pinging 172.31.3.94 with 32 bytes of data:

Reply from 172.31.3.94: bytes=32 time<lms TTL=255
Reply from 172.31.3.94: bytes=32 time<lms TTL=255
Reply from 172.31.3.94: bytes=32 time<lms TTL=255
Reply from 172.31.3.94: bytes=32 time<lms TTL=255

Ping statistics for 172.31.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 11. Prueba de ping desde PCB a R1 G0/0/1

```
C:\>ping 172.31.3.62

Pinging 172.31.3.62 with 32 bytes of data:

Reply from 172.31.3.62: bytes=32 time<lms TTL=255
Reply from 172.31.3.62: bytes=32 time<lms TTL=255
Reply from 172.31.3.62: bytes=32 time<lms TTL=255
Reply from 172.31.3.62: bytes=32 time<lms TTL=255

Ping statistics for 172.31.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

Figura 12. Prueba de ping desde PCB a PCA.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.31.3.11

Pinging 172.31.3.11 with 32 bytes of data:

Reply from 172.31.3.11: bytes=32 time<lms TTL=127
Reply from 172.31.3.11: bytes=32 time<lms TTL=127
Reply from 172.31.3.11: bytes=32 time<lms TTL=127
Reply from 172.31.3.11: bytes=32 time<lms TTL=127

Ping statistics for 172.31.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

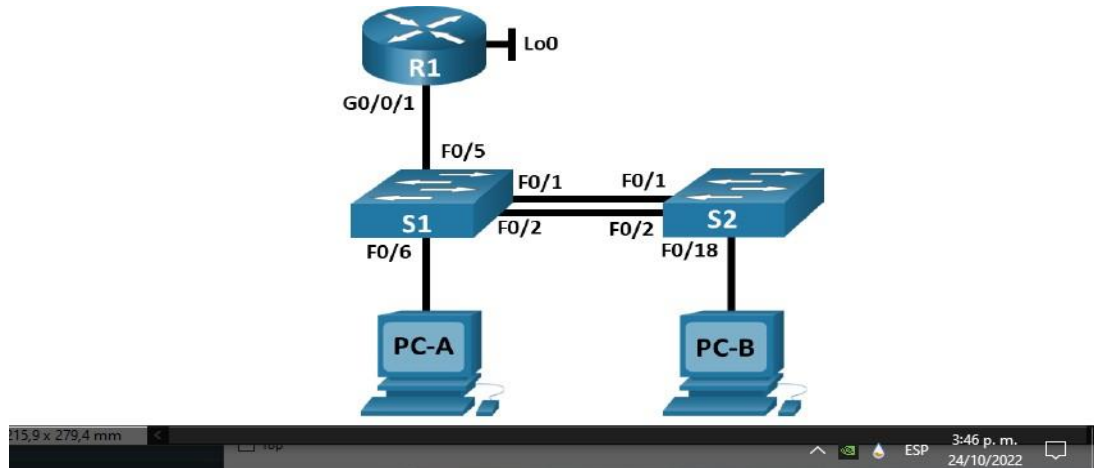
Fuente: Autor

Con los resultados anteriores, se puede observar que efectivamente el direccionamiento realizado fue correcto como ya se mencionó, y que así mismo la red puede estar dispuesta para hacer otro uso de protocolos en caso de que se quiera expandir dicho escenario.

## Escenario 2.

Para la segunda parte, la guía de trabajo sugiere el siguiente escenario de red.

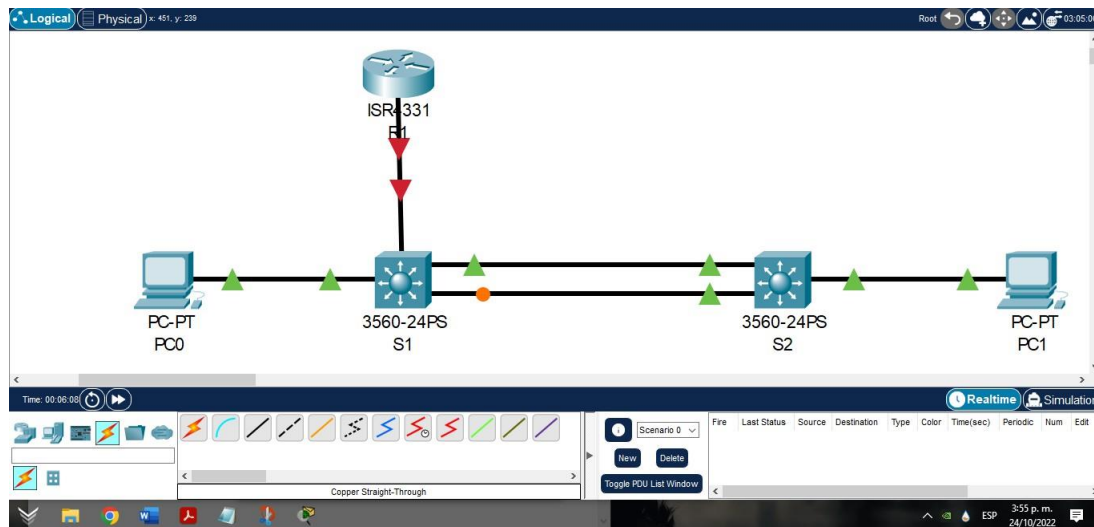
Figura 13. Segundo escenario según la guía de trabajo.



Fuente: Autor

Para este caso como ya se mencionó, la simulación de los escenarios se lleva a cabo en el programa Packet Tracer.

Figura 14. Simulación realizada con base al escenario de la figura 13.



Fuente: Autor

Para este segundo escenario se pide configurar los dispositivos vistos en la figura 13 con el fin de garantizar en todos ellos conectividad IPv4 e IPv6, así como configurar enrutamiento entre VLAN, DHCP, EthernetChannel y Port-Security.

### ***Inicialización y carga en el router y el switch.***

En todos los switches y routers de la topología se borra la configuración de inicio y las VLAN's, así como volver a cargar los dispositivos, así mismo se configura la plantilla SDM para que estos soporten IPv6, para llevar a cabo estas tareas se realizaron los siguientes comandos.

- erase startup-config #borrado de configuración
- reload #recarga del dispositivo

Para los switches se emplea:

- erase startup-config #borrado de configuración
- delete vlan.dat #borrado de vlan
- reload #recarga del dispositivo

Ahora se carga la plantilla SDM para que los dispositivos admitan IPv4 e IPv6 mediante los comandos:

- sdm prefer dual-ipv4-and-ipv6 default #preferencias para IPv4 e IPv6
- reload #recarga del dispositivo

Se asegura que en ambos switches se ejecuten los comandos anteriores.

Antes de acceder a la configuración de los dispositivos, se proporciona la siguiente información para configuración.

Tabla 4. Listado de VLAN's.

VLAN	Nombre de VLAN
20	Docentes
30	Universitarios
40	Invitados
50	Usuarios
60	Native

Fuente: Autor

Tabla 5. Lista con las direcciones a configurar.

Dispositivo/Interfaz	Dirección IPv4	Dirección IPv6
R1 G0/0/1.20	10.31.8.1 /26	2001:db8:acad:a: :1 /64
R1 G0/0/1.30	10.31.8.65 /27	2001:db8:acad:b: :1 /64
R1 G0/0/1.40	10.31.8.97 /29	2001:db8:acad:c: :1 /64
R1 G0/0/1.60	--	--
R1 Loopback0	209.165.201.1 /27	2001:db8:acad:209: :1 /64
S1 VLAN 40	10.31.8.98 /29	2001:db8:acad:c: :98 /64
S2 VLAN 40	10.31.8.99 /29	2001:db8:acad:c: :99 /64
PCA NIC	DHCP	2001:db8:acad:a: :50 /64
PCB NIC	DHCP	2001:db8:acad:b: :50 /64

### **Configurar R1**

La configuración del router se lleva a cabo mediante la CLI del mismo, las tareas que se requieren en el dispositivo son:

Tabla 6. Tareas para configurar en R1.

Tarea	Especificación
Desactivar la búsqueda DNS	--
Nombre del router	R1
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC	class
Contraseña de acceso a la consola	cisco
Longitud mínima para las contraseñas	5 caracteres
Usuario administrativo en base de datos local	Usuario: admin Password: admin1pass
Configuración inicio sesión en líneas VTY	--
Configuración líneas VTY para solo SSH	--
Cifrar contraseñas de texto no cifrado	--

Configure un banner	Se establece el nombre del dispositivo, del autor y del programa académico
Habilitar routing IPv6	--
Configuración interfaz g0/0/1	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.
Tarea	Especificación
Configuración Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1
Generar clave de cifrado RSA	Modulo 1024 bits

Fuente: Autor

Los comandos para llevar a cabo las tareas anteriores de forma secuencial se listan a continuación:

- enable
- conf ter
- no ip domain lookup
- hostname R1
- ip domain-name ccna-sa.com
- enable password ciscoenpass
- enable secret ciscoenpass
- line console 0
- password ciscoconpass
- login
- security passwords min-length 5
- username admin secret admin1pass
- line vty 0 15
- login local
- transport input ssh
- service password-encryption
- banner motd & R1 Andres Mauricio Perez Ingenieria de Sistemas &
- ipv6 unicast-routing
- int g0/0/1.20

- encapsulation dot1q 20
- description Docentes
- ip address 10.31.8.1 255.255.255.192
- ipv6 address 2001:db8:acad:a::1/64
- ipv6 address fe80::1 link-local
- int g0/0/1.30
- description Estudiantes
- ip address 10.31.8.65 255.255.255.224
- encapsulation dot1q 30
- ip address 10.31.8.65 255.255.255.224
- ipv6 address 2001:db8:acad:b::1/64
- ipv6 address fe80::1 link-local
- int g0/0/1.40
- encapsulation dot1q 40
- description Invitados
- ip address 10.31.8.97 255.255.255.248
- ipv6 address 2001:db8:acad:c::1/64
- ipv6 address fe80::1 link-local
- int g0/0/1.60
- encapsulation dot1q 60
- description Native
- int g0/0/1
- no shutdown
- int loopback0
- ip address 209.165.201.1 255.255.255.224
- ipv6 address 2001:db8:acad:209::1/64
- ipv6 address fe80::1 link-local
- description Internet
- exit
- crypto key generate rsa
- end
- copy running-config startup-config

Se puede comprobar de igual manera que las interfaces se configuraron.

Figura 15. Visualización de las interfaces en el router R1.

```

R1#
R1#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0    unassigned      YES unset  administratively down  down
GigabitEthernet0/0/1    unassigned      YES unset  up          up
GigabitEthernet0/0/1.20 2010.31.8.1     YES manual up          up
GigabitEthernet0/0/1.30 2010.31.8.65    YES manual up          up
GigabitEthernet0/0/1.40 2010.31.8.97    YES manual up          up
GigabitEthernet0/0/1.60 unassigned      YES unset  up          up
GigabitEthernet0/0/2    unassigned      YES unset  administratively down  down
Loopback0                209.165.201.1  YES manual up          up
Vlan1                    unassigned      YES unset  administratively down  down
R1#
    
```

Fuente: Autor

### Configurar S1 y S2.

La configuración de los switches se lleva a cabo mediante la CLI del mismo, las tareas que se requieren los dispositivos son:

Tabla 7. Tareas para configurar S1 y S2.

Tarea	Especificación
Desactivar la búsqueda DNS	--
Nombre del switch	S1 – S2
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC	class
Contraseña de acceso a la consola	cisco
Usuario administrativo en base de datos local	Usuario: admin Password: admin1pass
Configuración inicio sesión en líneas VTY	--
Configuración líneas VTY para solo SSH	--
Cifrar contraseñas de texto no cifrado	--
Configure un banner	Se establece el nombre del dispositivo, del autor y del programa académico

Generar clave de cifrado RSA	Modulo 1024 bits
Habilitar routing IPv6	--
Configuración interfaz SVI	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3
Configuración gateway predeterminado	Configure la puerta de enlace predeterminada como 10.31.8.97 para IPv4

Fuente: Autor

Los comandos para llevar a cabo las tareas anteriores en S1 de forma secuencial se listan a continuación.

- enable
- conf ter
- no ip domain lookup
- hostname S1
- ip domain-name ccna-sa.com
- enable secret ciscoenpass
- line console 0
- password ciscoconpass
- login
- exit
- username admin secret admin1pass
- line vty 0 15
- login local
- transport input ssh
- exit
- service password-encryption
- banner motd & S1 Andres Mauricio Perez Ingenieria de Sistemas &
- crypto key generate rsa
- int vlan 40
- ip address 10.31.8.98 255.255.255.248
- ipv6 address 2001:db8:acad:c::98/64
- ipv6 address fe80::98 link-local
- description Interfaz Invitados
- no shutdown
- exit

- ip default-gateway 10.31.8.97
- end
- copy running-config startup-config

Los comandos para llevar a cabo las tareas anteriores en S2 de forma secuencial se listan a continuación:

- enable
- conf ter
- no ip domain lookup
- hostname S2
- ip domain-name ccna-sa.com
- enable secret ciscoenpass
- line console 0
- password ciscoconpass
- login
- exit
- username admin secret admin1pass
- line vty 0 15
- login local
- transport input ssh
- exit
- service password-encryption
- banner motd & S2 Andres Mauricio Perez Ingenieria de Sistemas &
- crypto key generate rsa
- int vlan 40
- ip address 10.31.8.99 255.255.255.248
- ipv6 address 2001:db8:acad:c::99/64
- ipv6 address fe80::99 link-local
- description Interfaz Invitados
- no shutdown
- exit
- ip default-gateway 10.31.8.97
- end
- copy running-config startup-config

## **Configurar infraestructura de red VLAN, Trunking y EtherChannel en S1 y S2.**

La configuración de infraestructura de red en los conmutadores o switches S1 y S2 se listan a continuación.

Tabla 8. Tareas para configuración de infraestructura de red en S1.

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 60, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 60 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 20	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar

Fuente: Autor

Los comandos para llevar a cabo las tareas anteriores en S1 de forma secuencial se listan a continuación.

- conf ter
- vlan 20
- name Docentes
- vlan 30
- name Estudiantes
- vlan 40
- name Invitados
- vlan 50
- name Usuarios
- vlan 60
- name Native

- exit
- int f0/5
- switchport trunk encapsulation dot1q
- switchport mode trunk
- switchport trunk native vlan 60
- int range f0/1-2
- shutdown
- channel-group 1 mode active
- int port-channel 1
- switchport trunk encapsulation dot1q
- switchport mode trunk
- switchport trunk native vlan 60
- int f0/6
- switchport mode access
- switchport access vlan 20 --
- switchport port-security
- switchport port-security maximum 3
- int range f0/3-4
- switchport mode access
- switchport access vlan 50
- description Deshabilitado
- shutdown
- int range f0/7-24
- switchport mode access
- switchport access vlan 50
- description Deshabilitado
- shutdown
- int range g0/1-2
- switchport mode access
- switchport access vlan 50
- description Deshabilitado
- shutdown

Así mismo, las tareas para realizar la configuración de interfaz de red para S2 se listan a continuación.

Tabla 9. Tareas para configuración de infraestructura de red en S2.

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes

	VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 60, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 60 nativa	Interfaces F0/1, F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 30	Interface F0/18
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar

Fuente: Autor

Los comandos para llevar a cabo las tareas anteriores en S2 de forma secuencial se listan a continuación.

- conf ter
- vlan 20
- name Docentes
- vlan 30
- name Estudiantes
- vlan 40
- name Invitados
- vlan 50
- name Usuarios
- vlan 60
- name Native
- exit
- int range f0/1-2
- shutdown
- switchport trunk encapsulation dot1q
- switchport mode trunk
- switchport trunk native vlan 60
- channel-group 1 mode active
- int port-channel 1

- switchport trunk encapsulation dot1q
- switchport mode trunk
- switchport trunk native vlan 60
- int f0/18
- switchport mode access
- switchport access vlan 30
- switchport port-security
- switchport port-security maximum 3
- int range f0/3-17
- switchport mode access
- switchport access vlan 50
- description Deshabilitado
- shutdown
- int range f0/19-24
- switchport mode access
- switchport access vlan 50
- description Deshabilitado
- shutdown
- int range g0/1-2
- switchport mode access
- switchport access vlan 50
- description Deshabilitado
- shutdown

De igual manera, mediante el comando show vlan brief se puede llevar a cabo la verificación de las VLAN y asignación de puertos previamente asignados.

Figura 16. Visualización de las VLAN e interfaces configuradas en S1.

```

S1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                 active    Po1, Fa0/1, Fa0/2
20   Docentes                 active    Fa0/6
30   Estudiantes              active
40   Invitados                active
50   Usuarios                  active    Fa0/3, Fa0/4, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
60   Native                   active
1002 fddi-default             active
1003 token-ring-default     active
1004 fddinet-default         active
1005 trnet-default          active
S1#

```

Fuente: Autor

Figura 17. Visualización de las VLAN e interfaces configuradas en S2.

```
S2#show vlan brief
-----
VLAN Name                Status    Ports
-----
 1    default                active    Po1, Fa0/1, Fa0/2
 20   Docentes                 active
 30   Estudiantes              active    Fa0/18
 40   Invitados                active
 50   Usuarios                 active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24, Gig0/1, Gig0/2

 60   Native                   active
1002  fddi-default              active
1003  token-ring-default        active
1004  fddinet-default           active
1005  trnet-default             active
S2#
```

Fuente: Autor

### **Configurar soporte de host en R1**

Las tareas de configuración para el soporte de host en R1 se lista en la siguiente tabla a continuación.

Tabla 10. Tareas para configuración de soporte host en R1.

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 20	Cree un grupo DHCP para VLAN 20, 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
Configurar DHCP IPv4 para VLAN 30	Cree un grupo DHCP para VLAN 30, 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

Fuente: Autor

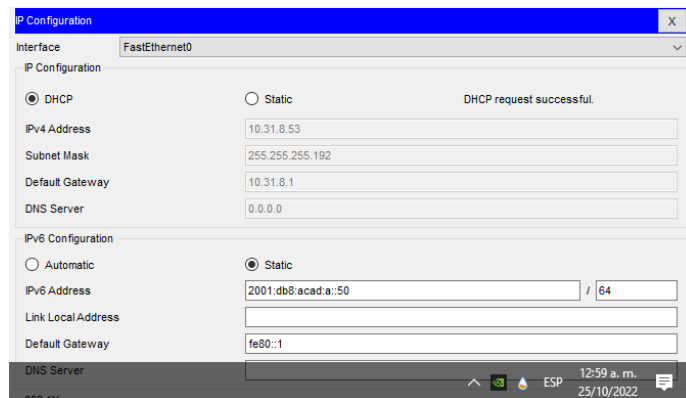
Los comandos para llevar a cabo las tareas anteriores en R1 de forma secuencial se listan a continuación:

- conf ter
- ip route 0.0.0.0 0.0.0.0 loopback 0
- ipv6 route ::/0 loopback 0
- ip dhcp excluded-address 10.31.8.2 10.31.8.51
- ip dhcp pool VLAN20-Docentes
- network 10.31.8.0 255.255.255.192
- default-router 10.31.8.1
- domain-name unad-ccna-sa.net
- exit
- ip dhcp excluded-address 10.31.8.65 10.31.8.84
- ip dhcp pool VLAN30-Estudiantes
- network 10.31.8.64 255.255.255.224
- default-router 10.31.8.65
- domain-name unad-ccna-sb.net
- exit

### ***Configuración de direccionamiento por interfaz de los hosts***

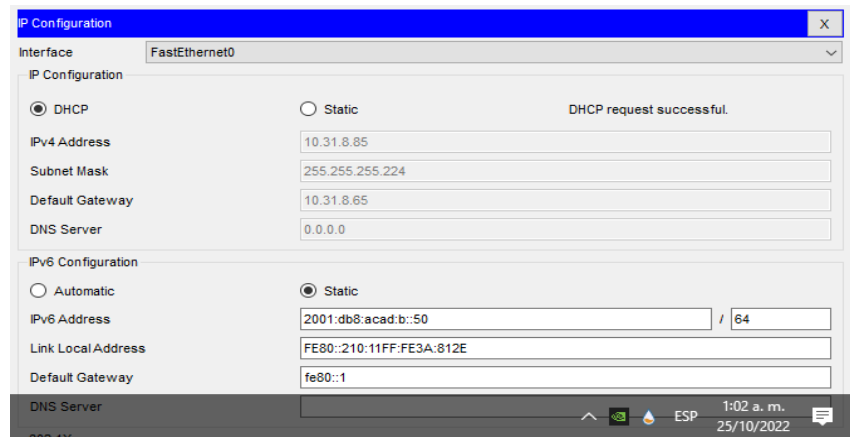
Como ultima parte de configuración, se detalla a continuación procedimiento por interfaz gráfica del direccionamiento que se le asigno a los equipos mediante DHCP para IPv4 y asignaciones estáticas de IPv6 según la tabla de direcciones mostrada anteriormente.

Figura 18. Uso de DHCP y asignación de IPv6 en PCA.



Fuente: Autor

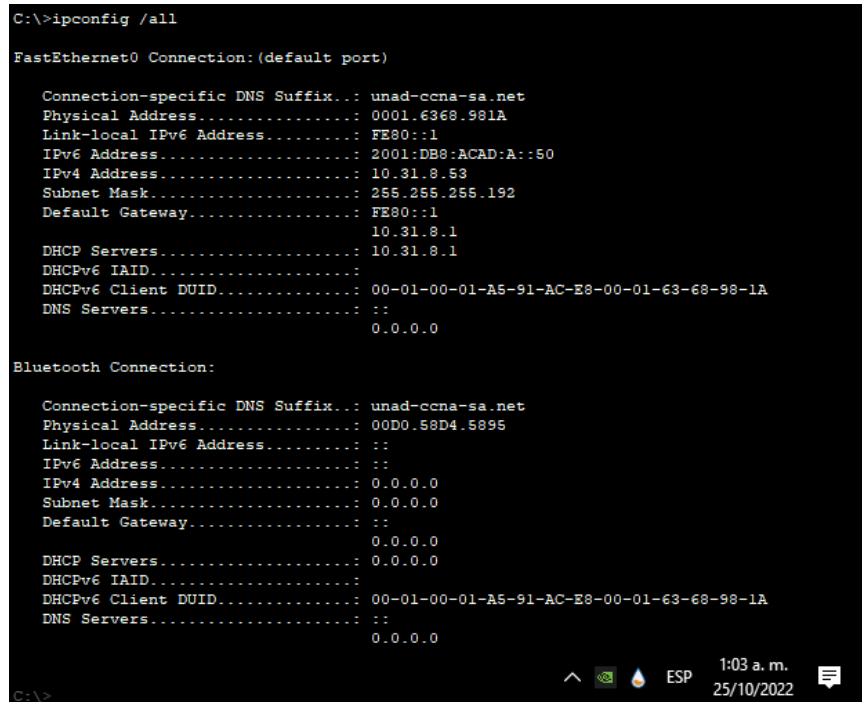
Figura 19. Uso de DHCP y asignación de IPv6 en PCB.



Fuente: Autor

Con ello, mediante el comando ipconfig /all se registra a continuación cada una de las direcciones configuradas en los hosts.

Figura 20. Información de direccionamiento en PCA.



Fuente: Autor

Figura 21. Información de direccionamiento en PCB.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...: unad-ccna-sb.net
    Physical Address.....: 0010.113A.812E
    Link-local IPv6 Address.....: FE80::210:11FF:FE3A:812E
    IPv6 Address.....: 2001:DB8:ACAD:B::50
    IPv4 Address.....: 10.31.8.85
    Subnet Mask.....: 255.255.255.224
    Default Gateway.....: FE80::1
                        10.31.8.65
    DHCP Servers.....: 10.31.8.65
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-36-BA-57-BE-00-10-11-3A-81-2E
    DNS Servers.....:
                        0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...: unad-ccna-sb.net
    Physical Address.....: 0090.0C53.3D9C
    Link-local IPv6 Address.....:
    IPv6 Address.....:
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....:
                        0.0.0.0
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-36-BA-57-BE-00-10-11-3A-81-2E
    DNS Servers.....:
                        0.0.0.0
```

Fuente: Autor

***Probar y verificar la conectividad de extremo a extremo.***

A continuación, se presenta una serie de registros visuales con base a pruebas de ping entre todas las interfaces y protocolos IPv4, IPv6 y la VLAN40.

Figura 22. Ping desde PCA hacia G0/0/1.20 en IPv4 e IPv6.

```
C:\>ping 10.31.8.1

Pinging 10.31.8.1 with 32 bytes of data:

Reply from 10.31.8.1: bytes=32 time<1ms TTL=255
Reply from 10.31.8.1: bytes=32 time<1ms TTL=255
Reply from 10.31.8.1: bytes=32 time<1ms TTL=255
Reply from 10.31.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.31.8.1:
    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:a::1

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

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=8ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

Fuente: Autor

Figura 23. Ping desde PCA hacia G0/0/1.30 en IPv4 e IPv6.

```
C:\>ping 10.31.8.65

Pinging 10.31.8.65 with 32 bytes of data:

Reply from 10.31.8.65: bytes=32 time<1ms TTL=255
Reply from 10.31.8.65: bytes=32 time<1ms TTL=255
Reply from 10.31.8.65: bytes=32 time<1ms TTL=255
Reply from 10.31.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.31.8.65:
    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::1

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

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

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

C:\>
```

Fuente: Autor

Figura 24. Ping desde PCA hacia G0/0/1.40 en IPv4 e IPv6.

```
C:\>ping 10.31.8.97

Pinging 10.31.8.97 with 32 bytes of data:

Reply from 10.31.8.97: bytes=32 time<1ms TTL=255
Reply from 10.31.8.97: bytes=32 time<1ms TTL=255
Reply from 10.31.8.97: bytes=32 time<1ms TTL=255
Reply from 10.31.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.31.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, 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

C:\>
```

Fuente: Autor

Figura 25. Ping desde PCA hacia S1 VLAN 40.

```
C:\>ping 10.31.8.98

Pinging 10.31.8.98 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.31.8.98: bytes=32 time<1ms TTL=254
Reply from 10.31.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.31.8.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% 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:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fuente: Autor

Figura 26. Ping desde PCA hacia S2 VLAN 40.

```
C:\>ping 10.31.8.99

Pinging 10.31.8.99 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.31.8.99: bytes=32 time<1ms TTL=254
Reply from 10.31.8.99: bytes=32 time<1ms TTL=254

Ping statistics for 10.31.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

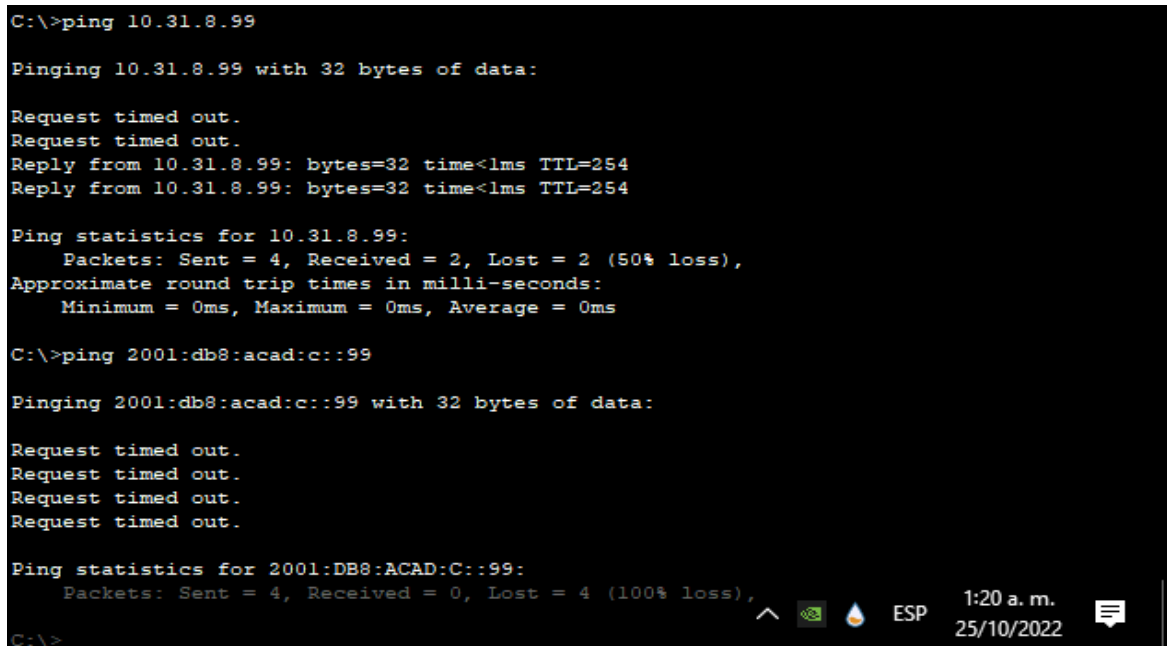
C:\>ping 2001:db8:acad:c::99

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

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```



Fuente: Autor

Figura 27. Ping desde PCA hacia PCB IPv4 e IPv6.

```
C:\>ping 10.31.8.85

Pinging 10.31.8.85 with 32 bytes of data:

Request timed out.
Reply from 10.31.8.85: bytes=32 time=9ms TTL=127
Reply from 10.31.8.85: bytes=32 time<1ms TTL=127
Reply from 10.31.8.85: bytes=32 time<1ms TTL=127

Ping statistics for 10.31.8.85:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 3ms

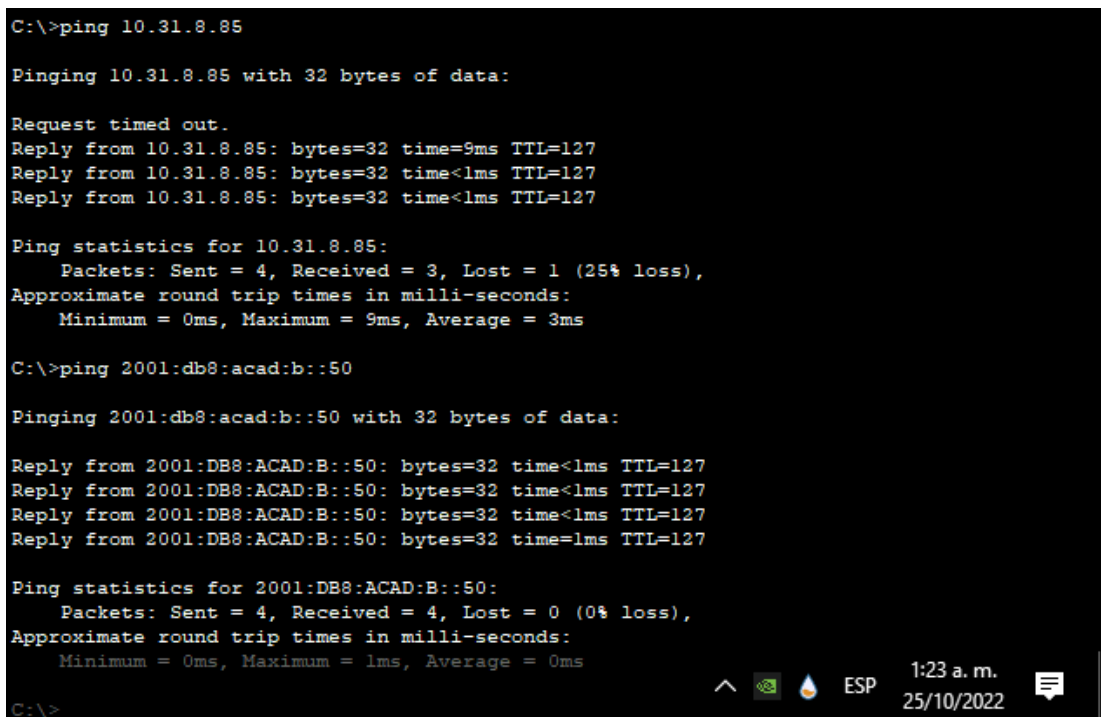
C:\>ping 2001:db8:acad:b::50

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 = 1ms, Average = 0ms

```



Fuente: Autor

Figura 28. Ping desde PCA hacia R1 Loop0.

```
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 209.165.201.1: bytes=32 time<lms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time=lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = lms, Average = 0ms

C:\>
```

Fuente: Autor

Figura 29. Ping desde PCB hacia R1 Loop0.

```
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255

Ping statistics for 209.165.201.1:
    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:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

Figura 30. Ping desde PCB hacia G0/0/1.20 en IPv4 e IPv6.

```
C:\>ping 10.31.8.1

Pinging 10.31.8.1 with 32 bytes of data:

Reply from 10.31.8.1: bytes=32 time<lms TTL=255
Reply from 10.31.8.1: bytes=32 time<lms TTL=255
Reply from 10.31.8.1: bytes=32 time<lms TTL=255
Reply from 10.31.8.1: bytes=32 time<lms TTL=255

Ping statistics for 10.31.8.1:
    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:a::1

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

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255

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

C:\>
```

Fuente: Autor

Figura 31. Ping desde PCB hacia G0/0/1.30 en IPv4 e IPv6.

```
C:\>ping 10.31.8.65

Pinging 10.31.8.65 with 32 bytes of data:

Reply from 10.31.8.65: bytes=32 time<lms TTL=255
Reply from 10.31.8.65: bytes=32 time<lms TTL=255
Reply from 10.31.8.65: bytes=32 time<lms TTL=255
Reply from 10.31.8.65: bytes=32 time=lms TTL=255

Ping statistics for 10.31.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = lms, Average = 0ms

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

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

Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=lms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255

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

C:\>
```

Fuente: Autor

Figura 32. Ping desde PCB hacia G0/0/1.40 en IPv4 e IPv6.

```
C:\>ping 10.31.8.97

Pinging 10.31.8.97 with 32 bytes of data:

Reply from 10.31.8.97: bytes=32 time<1ms TTL=255
Reply from 10.31.8.97: bytes=32 time<1ms TTL=255
Reply from 10.31.8.97: bytes=32 time<1ms TTL=255
Reply from 10.31.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.31.8.97:
    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=8ms 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 = 8ms, Average = 2ms

C:\>
```

Fuente: Autor

Figura 33. Ping desde PCB hacia S1 VLAN 40.

```
C:\>ping 10.31.8.98

Pinging 10.31.8.98 with 32 bytes of data:

Request timed out.
Reply from 10.31.8.98: bytes=32 time<1ms TTL=254
Reply from 10.31.8.98: bytes=32 time=10ms TTL=254
Reply from 10.31.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.31.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

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

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

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fuente: Autor

Figura 34. Ping desde PCB hacia S2 VLAN 40.

```
C:\>ping 10.31.8.99

Pinging 10.31.8.99 with 32 bytes of data:

Request timed out.
Reply from 10.31.8.99: bytes=32 time<1ms TTL=254
Reply from 10.31.8.99: bytes=32 time<1ms TTL=254
Reply from 10.31.8.99: bytes=32 time<1ms TTL=254

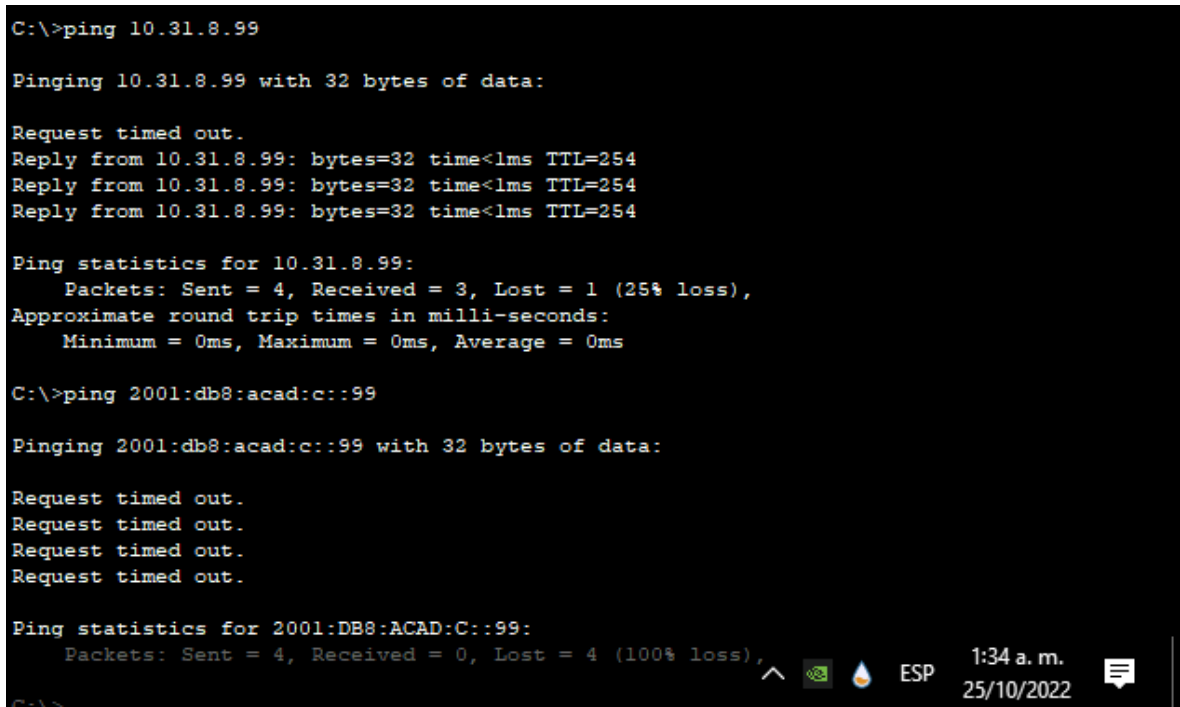
Ping statistics for 10.31.8.99:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

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

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

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



Fuente: Autor

Con base a las figuras anteriores y los resultados obtenidos se puede observar que la mayoría de los pings fueron satisfactorios, se detalla que fallaron algunos pings (IPv6) posiblemente debido al no configurarse una IPv6 de manera local en SVI ya que ese fue el punto donde no se registró conexión, por lo demás se concluye que la configuración fue correcta.

## CONCLUSIONES

Con base a los dos escenarios desarrollados anteriormente, se puede constatar como mediante la aplicación de protocolos y direccionamiento se puede llegar a gestionar de manera mucho más eficiente cualquier escenario de red local, el protocolo DHCP permite detallar como se gestiona el direccionamiento de cualquier hosts en la red evitando la configuración de forma manual y que de igual manera se puede realizar exclusión de rango de direcciones para evitar direccionamientos iguales, así mismo, mediante el uso de VLAN y protocolos como 802.11Q se permite la comunicación de dichos dispositivos de manera seccionada y sin que exista interferencia en los mismos al trabajar sobre la misma red física, el primer escenario permite observar la facilidad con la que se puede llegar a detectar cualquier falla en una red mediante las pruebas de ping de extremo a extremo y así reducir el área de búsqueda de problemas en caso que se hable de redes de mayor tamaño.

Así mismo, aunque el segundo escenario emplea protocolos para el direccionamiento automático, también como se observó, se debe ser consiente que los dispositivos admitan dichos protocolos como se identificó para el direccionamiento de IPv6 en los switches que de forma predeterminada no admiten dicho protocolo y que en ocasiones también deben ser dispositivos compatibles con las instrucciones de CISCO, por último, se puede observar como las VLAN pueden llegar a funcionar como dominios de difusión lógica y que permite dividir grupos de usuarios en red y que aparte de hacer más eficiente la gestión de datos, puede garantizar mayor seguridad en dicha red en caso que se conecten equipos remotos y se configuren una VLAN para los mismos con reglas de bloqueo y acceso limitado a los demás equipos.

## BIBLIOGRAFÍA

BITACORABYTE. Configurar DHCP en router CISCO. {En línea} (2017) {14 de diciembre de 2022}. Disponible en: <https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco>

HUCABY, MCQUERRY, David, Sthepen. VLANs and Trunking.iscopress. {En línea} (2022) {14 de diciembre de 2022}. Disponible en: <https://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3>

JIMENEZ, Julio. Understand the ping and traceroute commands. Cisco. {En línea} (2022) {14 de diciembre de 2022}. Disponible en: <https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html>

LLUCH, Ernest. ¿Cómo configurar una VLAN en Cisco Switch?. Netcloudengineering. . {En línea} (2022) {14 de diciembre de 2022}. Disponible en: <https://netcloudengineering.com/configuracion-vlan-cisco-switch/#:~:text=Se%20conoce%20como%20Virtual%20LAN,pueden%20mantener%20comunicaci%C3%B3n%20entre%20s%C3%AD.>

PEREZ, José. Cómo habilitar el soporte de IPv6 en un Switch Cisco Catalisys 3560. Red10Education. {En línea} (2018) {14 de diciembre de 2022}. Disponible en: <https://red10education.com/blog/como-habilitar-el-soporte-de-ipv6-en-un-switch-cisco-catalisys-3560/>

ROUSE, Margaret. ¿Qué son y para qué sirven los protocolos de comunicación de redes?. Kionetworks. {En línea} (2019) {14 de diciembre de 2022}. Disponible en: <https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes>

## ANEXOS

Anexo A: Simulaciones

<https://drive.google.com/drive/folders/1BnGxsZBCtGu3avlyrudSIQyvsNoMnMMf?usp=sharing>