

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

MAURICIO BAUTISTA ARTEAGA

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

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

MAURICIO BAUTISTA ARTEAGA

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO  
DE INGENIERO DE SISTEMAS

DIRECTORA:  
PAULITA FLOR  
INGENIERA DE TELECOMUNICACIONES

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

Nota de Aceptación

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Cali, 27 de noviembre de 2022

#### Dedicatoria

A Dios que siempre me ha guiado en la búsqueda continua del conocimiento y a mi madre por su sacrificio y esfuerzo en todo momento.

## AGRADECIMIENTOS

Mi etapa académica profesional ha sido como subir una montaña con varios picos cada vez más altos, y en el caminar por estos picos han estado muchas personas, pero antes de cada uno ha estado Dios acompañándome, brindándome fortaleza para seguir en la búsqueda de mis proyectos, por esto agradezco primero a Dios por las bendiciones de salud, capacidades, oportunidades y ánimo que me da cada día con lo que siempre he logrado conseguir mis metas. Agradezco a mi familia cercana que siempre ha estado presente y que cada uno ha enriquecido mi vida con su apoyo y amor, en especial a mi madre que su esfuerzo y dedicación siempre se enfocó en permitirme tener la mejor educación dentro de sus posibilidades. Mis agradecimientos también a mi primo John Henry porque su apoyo me permitió tener la posibilidad de continuar con mis estudios. Finalmente agradezco a los directores de curso, tutores, compañeros de estudio y demás personas que en algún momento me han compartido su conocimiento.

## CONTENIDO

|  | Pág. |
|--|------|
| INTRODUCCIÓN .....   | 13   |
| DESARROLLO DEL PROYECTO .....  | 14   |
| 1. Escenario 1 .....   | 14   |
| 1.1. Construcción de la red del Escenario 1 en el simulador. ....                              | 14   |
| 1.2. Desarrollo del esquema de direccionamiento IP para LAN 1 y LAN 2 .....                    | 14   |
| 1.3. Configuración de aspectos básicos de seguridad para el escenario 1 ....                   | 15   |
| 1.3.1. Configuración de aspectos básicos.....  | 15   |
| 1.3.2. Configuración de equipos.....   | 19   |
| 1.4. Prueba y verificación de conectividad de extremo a extremo .....                          | 20   |
| 2. Escenario 2 .....   | 25   |
| 2.1 Construcción de la red del Escenario 2 .....   | 26   |
| 2.1.1 Inicializar y volver a cargar el router.....   | 26   |
| 2.1.2 Configuración de R1.....   | 27   |
| 2.1.3 Configuración de S1 y S2.....  | 30   |
| 2.1.4 Configuración de la infraestructura de red (VLAN, Trunking,<br>EtherChannel) de S1 ..... | 32   |
| 2.1.5 Configuración de la infraestructura de red (VLAN, Trunking,<br>EtherChannel) de S2.....  | 34   |
| 2.2 Configuración soporte de host.....   | 35   |
| 2.2.1 Configuración de R1.....   | 35   |
| 2.2.2 Configuración de los host PC-A y PC-B .....  | 37   |
| 2.2.3 Prueba y verificación de la conectividad de extremo a extremo.....                       | 38   |
| CONCLUSIONES .....   | 51   |
| BIBLIOGRAFÍA .....   | 52   |
| ANEXOS .....   | 53   |

## LISTA DE TABLAS

|  | Pág. |
|--|------|
| Tabla 1 Direccionamiento IP, Escenario 1.....                              | 15   |
| Tabla 2 Procedimiento de configuración para R1 .....                       | 15   |
| Tabla 3 Procedimiento de configuración para S1 .....                       | 17   |
| Tabla 4 Configuración de PC-A .....  | 19   |
| Tabla 5 Configuración de PC-B .....  | 20   |
| Tabla 6 Prueba de conectividad.....  | 21   |
| Tabla 7 Nombre de las VLAN .....   | 25   |
| Tabla 8 Direccionamiento IPv4 e IPv6, Escenario 2 .....                    | 25   |
| Tabla 9 Configuración de R1, Escenario 2. ....                             | 27   |
| Tabla 10 Configuración de S1 y S2, Escenario 2.....                        | 30   |
| Tabla 11 Configuración de infraestructura de red para S1, Escenario 2..... | 32   |
| Tabla 12 Configuración de infraestructura de red para S2, Escenario 2..... | 34   |
| Tabla 13 Configuración de soporte de host para R1, Escenario 2.....        | 36   |
| Tabla 14 Configuración de red de PC-A, Escenario 2 .....                   | 37   |
| Tabla 15 Configuración de red de PC-B, Escenario 2 .....                   | 38   |
| Tabla 16 Verificación de conectividad, Escenario 2.....                    | 39   |

## LISTA DE FIGURAS

|   | Pág. |
|---|------|
| Figura 1 Topología del Escenario 1 en el simulador Packet Tracer..... | 14   |
| Figura 2 Prueba de configuración PC-A .....                           | 19   |
| Figura 3 Prueba de configuración PC-B .....                           | 20   |
| Figura 4 Prueba de conectividad PC-A a R1 G0/0/0.....                 | 21   |
| Figura 5 Prueba de conectividad PC-A a R1 G0/0/1.....                 | 21   |
| Figura 6 Prueba de conectividad PC-A a S1 .....                       | 22   |
| Figura 7 Prueba de conectividad PC-A a PC-B .....                     | 22   |
| Figura 8 Prueba de conectividad PC-B a R1 G0/0/0.....                 | 23   |
| Figura 9 Prueba de conectividad PC-B a R1 G0/0/1.....                 | 23   |
| Figura 10 Prueba de conectividad PC-B a S1 .....                      | 24   |
| Figura 11 Prueba de conectividad PC-B a PC-A .....                    | 24   |
| Figura 12 Topología de la red del escenario 2.....                    | 26   |
| Figura 13 Configuraciones de red PC-A .....                           | 37   |
| Figura 14 Configuraciones de red PC-B .....                           | 38   |
| Figura 15 Prueba de conectividad entre PC-A y R1 G0/0/1.20 IPv4.....  | 39   |
| Figura 16 Prueba de conectividad entre PC-A y R1 G0/0/1.20 IPv6.....  | 39   |
| Figura 17 Prueba de conectividad entre PC-A y R1 G0/0/1.30 IPv4.....  | 40   |
| Figura 18 Prueba de conectividad entre PC-A y R1 G0/0/1.30 IPv6.....  | 40   |
| Figura 19 Prueba de conectividad entre PC-A y R1 G0/0/1.40 IPv4.....  | 41   |
| Figura 20 Prueba de conectividad entre PC-A y R1 G0/0/1.40 IPv6.....  | 41   |
| Figura 21 Prueba de conectividad entre PC-A y S1 VLAN40 IPv4 .....    | 42   |
| Figura 22 Prueba de conectividad entre PC-A y S2 VLAN40 IPv4 .....    | 42   |
| Figura 23 Prueba de conectividad entre PC-A y PC-B IPv4 .....         | 43   |
| Figura 24 Prueba de conectividad entre PC-A y PC-B IPv6 .....         | 43   |
| Figura 25 Prueba de conectividad entre PC-A y R1 Bucle 0 IPv4 .....   | 44   |
| Figura 26 Prueba de conectividad entre PC-A y R1 Bucle 0 IPv6 .....   | 45   |
| Figura 27 Prueba de conectividad entre PC-B y R1 Bucle 0 IPv4 .....   | 45   |
| Figura 28 Prueba de conectividad entre PC-B y R1 Bucle 0 IPv6 .....   | 46   |
| Figura 29 Prueba de conectividad entre PC-B y R1 G0/0/1.20 IPv4.....  | 46   |
| Figura 30 Prueba de conectividad entre PC-B y R1 G0/0/1.20 IPv6.....  | 47   |
| Figura 31 Prueba de conectividad entre PC-B y R1 G0/0/1.30 IPv4.....  | 47   |
| Figura 32 Prueba de conectividad entre PC-B y R1 G0/0/1.30 IPv6.....  | 48   |
| Figura 33 Prueba de conectividad entre PC-B y R1 G0/0/1.40 IPv4.....  | 48   |
| Figura 34 Prueba de conectividad entre PC-B y R1 G0/0/1.40 IPv6.....  | 49   |
| Figura 35 Prueba de conectividad entre PC-B y S1 VLAN 40 IPv4 .....   | 49   |



Figura 36 Prueba de conectividad entre PC-B y S2 VLAN 40 IPv4. ....50

## GLOSARIO

**GATEWAYS:** “El nombre general para una máquina que realiza una conexión entre dos o más redes y provee la traducción necesaria, tanto en términos de hardware como de software, es puerta de enlace (gateway)”<sup>1</sup>.

**LAN:** Redes de área Local (Local Area Network), Tanenbaum las define como: “son redes de propiedad privada que operan dentro de un solo edificio, como una casa, oficina o fábrica. Las redes LAN se utilizan ampliamente para conectar computadoras personales y electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información”<sup>2</sup>.

**MAN:** Es una red de área metropolitana (Metropolitan Area Network), Tanenbaum nos presenta la siguiente definición: “Las redes MAN comúnmente cubren toda una ciudad. El sistema de televisión por cable es un ejemplo, ya que ahora muchas personas lo utilizan para acceder a Internet”<sup>3</sup>.

**MODELO OSI:** “desarrollada por la Organización Internacional de Normas (iso) como el primer paso hacia la estandarización internacional de los protocolos utilizados en las diversas capas (Day y Zimmerman, 1983). Este modelo se revisó en 1995 (Day, 1995) y se le llama Modelo de referencia OSI (Interconexión de Sistemas Abiertos, del inglés Open Systems Interconnection)”<sup>4</sup>

**TCP/IP (TRANSPORT CONTROL PROTOCOL / INTERNET PROTOCOL):** “se denomina globalmente como la familia de protocolos TCP/IP. Esta familia consiste en una extensa colección de protocolos que se han especificado como estándares de Internet por parte de IAB (Internet Architecture Board)”<sup>5</sup>.

**TOPOLOGÍA:** “se hace referencia a la disposición física de las estaciones en el medio de transmisión. Si hay sólo dos estaciones (es decir, un terminal y un

---

<sup>1</sup> TANENBAUM, Andrew S. Redes de Computadoras. Prentice Hall, 2003. p.25

<sup>2</sup> Ibíd., p.17

<sup>3</sup> Ibíd., p.73

<sup>4</sup> Ibíd., p.35

<sup>5</sup> STALLINGS, William. Comunicaciones y Redes de Computadores. Prentice Hall, 2001. p. 40

computador, o dos computadores), el enlace es punto a punto. Si hay más de dos estaciones, entonces se trata de una topología multipunto”<sup>6</sup>.

**WAN:** “se considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan, al menos parcialmente, circuitos proporcionados por una entidad proveedora de servicios de telecomunicación.”<sup>7</sup>.

---

<sup>6</sup> STALLINGS, William. Comunicaciones y Redes de Computadores. Prentice Hall, 2001. p. 197

<sup>7</sup> Ibíd., p.15

## RESUMEN

En este documento se desarrolla de manera práctica, y con el fin de reconocer y apropiar los conocimientos adquiridos durante el diplomado de profundización Cisco (diseño e implementación de soluciones integradas LAN/WAN), una evaluación denominada "Prueba de habilidades prácticas" que consiste en la comprensión, análisis, documentación y desarrollo de dos escenarios de redes simulados.

El Escenario 1 comprende la configuración de dispositivos de una red que tiene un router, un switch y dos computadores conectados por cable de red, a los que hay que diseñar el esquema de direccionamiento IPv4 y se deben administrar de forma segura. El Escenario 2 propone una red más amplia, donde hay que configurar un router, dos switches, y un equipo conectado a cada switch, que admitan conectividad IPv4 e IPv6, asegurándose administrar los dispositivos de manera segura y configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

**PALABRAS CLAVE:** CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

## ABSTRACT

This document presents in a practical way, and with the purpose of recognizing and appropriating the knowledge acquired during the Cisco in-depth certificate course (design and implementation of integrated LAN/WAN solutions), an evaluation called "Practical Skills Test" which consists of the comprehension, analysis, documentation and development of two simulated network scenarios.

Scenario 1 includes the configuration of devices in a network that has a router, a switch and two computers connected by network cable, to which the IPv4 addressing scheme must be designed and securely managed. Scenario 2 proposes a larger network, where it is necessary to configure a router, two switches, and a computer connected to each switch, supporting IPv4 and IPv6 connectivity, making sure to manage the devices in a secure way and to configure routing between VLAN, DHCP, Etherchannel and port-security.

**KEYWORDS:** CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

## INTRODUCCIÓN

Como parte de las actividades evaluativas del Diplomado de Profundización CISCO (diseño e implementación de soluciones integradas LAN/WAN), se realizan dos actividades que contemplan el uso de las habilidades y competencias adquiridas en el transcurso de curso. Las actividades consisten en el desarrollo de dos escenarios de red con topologías diferentes y se desarrollan en el simulador Cisco Packet Tracer vr. 8.2.0.0162.

Los escenarios se desarrollaron mediante un proceso de configuración paso a paso de los dispositivos que integran la red utilizando los comandos Cisco IOS, con la debida documentación de los comandos utilizados y el registro de los resultados obtenidos de comunicación en cada caso con el uso del comando ping.

A partir de los escenarios planteados se trabajaron conceptos de direccionamientos de entornos de red con conectividad IPv4 e IPv6, se realizó la configuración de enrutamientos entre redes estáticas y DHCP y se crearon políticas de seguridad de capa 2 donde se tiene en cuenta la MAC de los dispositivos para evitar conexiones indeseadas a puertos o equipos específicos (port-security).

## DESARROLLO DEL PROYECTO

En la presente prueba de habilidades se presentan dos escenarios, cada uno desarrollado en la herramienta de simulación de redes Cisco Packet Tracer Vr. 8.2.0.0162, escenarios con los que se presentan las habilidades y competencias adquiridas en el diplomado.

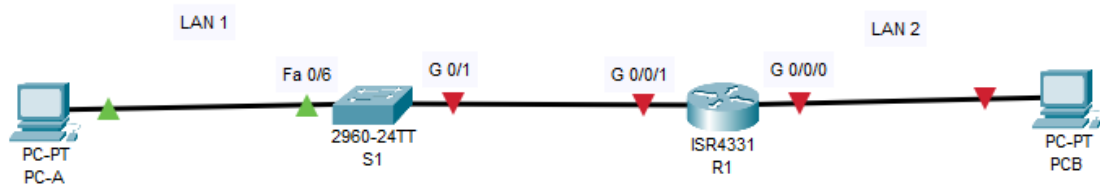
### 1. Escenario 1

En este primer escenario se configuran los dispositivos de una red pequeña que contiene un router, un switch y dos equipos.

#### 1.1. Construcción de la red del Escenario 1 en el simulador.

La figura 1 muestra la topología del escenario 1 implementada en el simulador Packet Tracer. Se utilizaron un swiche 2960-24TT, un router ISR4331 y dos PC.

Figura 1 Topología del Escenario 1 en el simulador Packet Tracer



Fuente: Autor

#### 1.2. Desarrollo del esquema de direccionamiento IP para LAN 1 y LAN 2

La configuración del direccionamiento se realiza a partir de los datos presentes en la tabla 1, en la que se suministran las IP para el subnetting y los requerimientos para la LAN1 (60 host) y la LAN2 (20 hosts).

Tabla 1 Direccionamiento IP, Escenario 1.

| Ítem                                | Requerimiento   |
|-------------------------------------|---|
| Dirección de red                    | 172.34.3.0  |
| Requerimientos de host Subred LAN 1 | 60 – IP 172.34.3.0 / 26 (62 hosts)                              |
| Requerimientos de host Subred LAN 2 | 20 – IP 172.34.3.64 / 27 (27 hosts)                             |
| R1 G0/0/1                           | Última dirección de host de la subred LAN 1<br>172.34.3.62 / 26 |
| R1 G0/0/0                           | Última dirección de host de la subred LAN 2<br>172.34.3.94 / 27 |
| S1 SVI                              | Segunda dirección de host de la subred LAN 1<br>172.34.3.2 / 26 |
| PC – A                              | Decima dirección de host de la subred LAN 1<br>172.34.3.10 / 26 |
| PC – B                              | Decima dirección de host de la subred LAN 2<br>172.34.3.74 / 27 |

Fuente: Autor

### 1.3. Configuración de aspectos básicos de seguridad para el escenario 1

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola. En los siguientes apartados se realiza paso a paso la configuración.

#### 1.3.1. Configuración de aspectos básicos

En la tabla 2 se muestran las tareas básicas de configuración para R1.

Tabla 2 Procedimiento de configuración para R1

| Tarea   | Especificación | Comando                               |
|---|----------------|---------------------------------------|
| Desactivar la búsqueda DNS                        | ----           | Router(config)#no ip domain-lookup    |
| Nombre del router                                 | R1             | Router(config)#hostname R1            |
| Nombre del dominio                                | ccna-sa.com    | R1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass    | R1(config)#enable secret ciscoenpass  |
| Contraseña de acceso                              | ciscoconpass   | R1(config)#line console 0             |

| <b>Tarea</b>  | <b>Especificación</b>  | <b>Comando</b>   |
|---|--|--|
| a la consola  |  | R1(config-line)#password<br>ciscoconpass<br>R1(config-line)#login  |
| Establecer la longitud mínima para las contraseñas                                  | 10 caracteres  | R1(config)#security passwords min-length 10  |
| Crear un usuario administrativo en la base de datos local                           | Nombre de usuario: admin<br>Contraseña: admin1pass   | R1(config)#username admin<br>password admin1pass   |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | ----   | R1(config)#line vty 0 15<br>R1(config-line)#login local  |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH            | ----   | R1(config-line)#transport input SSH  |
| Cifrar las contraseñas de texto no cifrado  | ----   | R1(config)#service password-encryption   |
| Configurar un banner MOTD   | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. | R1(config)#banner motd #R1 -<br>Mauricio Bautista Arteag - Ingenieria<br>de Sistemas#  |
| Configuración de interface G0/0/0   | Establecer la descripción<br>Establecer la dirección IPv4<br>Activar la interfaz.                                    | R1(config)#interface GigabitEthernet<br>0/0/0<br><br>R1(config-if)#Description R1 a PC-B<br><br>R1(config-if)#ip address 172.34.3.94<br>255.255.255.224<br><br>R1(config-if)#no shutdown |
| Configuración de interface G0/0/1   | Establecer la descripción<br>Establecer la dirección IPv4<br>Activar la interfaz.                                    | R1(config)#interface GigabitEthernet<br>0/0/1<br><br>R1(config-if)#Description R1 a PC-A<br><br>R1(config-if)#ip address 172.34.3.62   |



| Tarea                            | Especificación      | Comando   |
|----------------------------------|---------------------|---|
|                                  |                     | 255.255.255.192<br><br>R1(config-if)#no shutdown                                  |
| Generar una clave de cifrado RSA | Módulo de 1024 bits | R1(config)#crypto key generate rsa<br>How many bits in the modulus [512]:<br>1024 |

Fuente: Autor

En la tabla 3 se describen las tareas básicas de configuración para S1.

Tabla 3 Procedimiento de configuración para S1

| Tarea   | Especificación                                     | Comando  |
|---|--|--|
| Desactivar la búsqueda DNS  | ----   | Switch>enable<br>Switch#configure terminal<br>Enter configuration commands, one per line. End with CNTL/Z.<br>Switch(config)#no ip domain-lookup |
| Nombre del switch   | S1   | Switch(config)#hostname S1   |
| Nombre del dominio  | ccna-sa.com  | S1(config)#ip domain-name ccna-sa.com  |
| Contraseña cifrada para el modo EXEC privilegiado                                   | ciscoenpass  | S1(config)#enable secret<br>ciscoenpass  |
| Contraseña de acceso a la consola   | ciscoconpass                                       | S1(config)#line console 0<br>S1(config-line)#password<br>ciscoconpass<br>S1(config-line)#login<br>S1(config-line)#exit                           |
| Apagar todos los puertos sin usar   | F0/1-4, F0/7-24, G0/1-2                            | S1(config)#interface range F0/1-4,F0/7-24,G0/1-2<br>S1(config-if-range)#shutdown   |
| Crear un usuario administrativo en la base de datos local                           | Nombre de usuario: admin<br>Contraseña: admin1pass | S1(config)#username admin<br>password admin1pass   |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | ----   | S1(config)#line vty 0 15<br>S1(config-line)#login local  |

|  |  |  |
|--|--|--|
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | ----   | S1(config-line)#transport input ssh<br>S1(config-line)#login local   |
| Cifrar las contraseñas de texto no cifrado                               | ----   | S1(config)#service password-encryption   |
| Configurar un banner MOTD  | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. | S1(config)#banner motd #S1 - Mauricio Bautista Arteaga - Ingenieria de Sistemas#   |
| Generar una clave de cifrado RSA   | Módulo de 1024 bits  | S1(config)#crypto key generate rsa<br>The name for the keys will be:<br>S1.ccna-sa.com<br>Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.<br><br>How many bits in the modulus [512]:<br>1024<br>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK] |
| Configure la interfaz de administración (SVI) en VLAN1                   | Establecer la descripción<br>Establecer la dirección IPv4  | S1(config)#int vlan 1<br>S1(config-if)#ip address 172.34.3.2 255.255.255.192<br>S1(config-if)#description Interfaz VLAN1<br>S1(config-if)#no shutdown<br>S1(config-if)#exit<br>S1(config)#ip default-gateway 172.34.3.62   |

Fuente: Autor

### 1.3.2. Configuración de equipos

Los equipos host PC-A y PC-B se configuran conforme a la tabla 4 y 5, aquí se aprecia el direccionamiento de cada equipo.

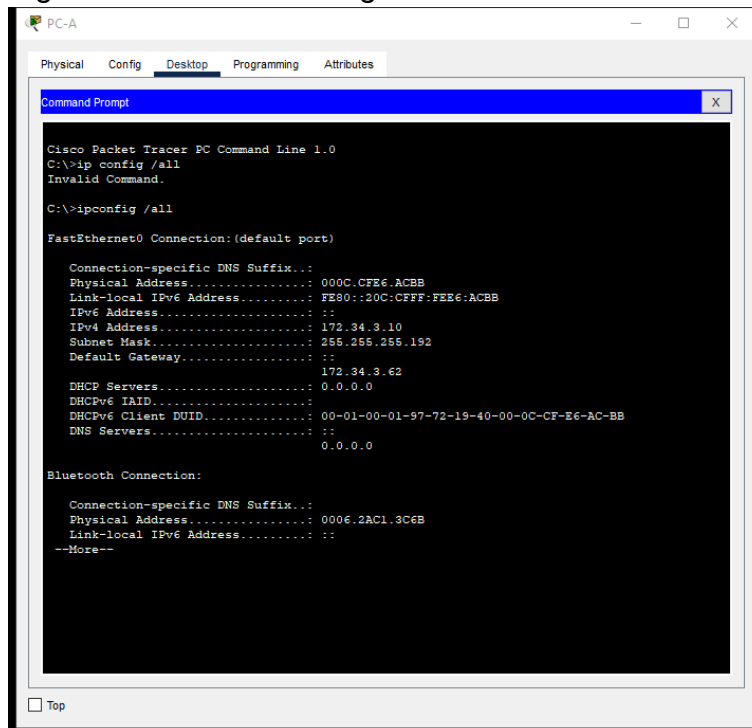
Tabla 4 Configuración de PC-A

| Configuración de red de PC - A       |                 |
|--------------------------------------|-----------------|
| Descripción                          | PC-A            |
| Dirección física                     | 000C.CFE6.ACBB  |
| Dirección IPv4                       | 172.34.3.10/26  |
| Máscara de subred                    | 255.255.255.192 |
| Puerta de enlace IPv4 predeterminada | 172.34.3.62     |

Fuente: Autor

La figura 2 detalla la configuración del PC-A donde podemos observar el uso del comando “*ip config /all*” para mostrar el detalle de la conexión que corresponde a los valores de la tabla 4.

Figura 2 Prueba de configuración PC-A



Fuente: Autor

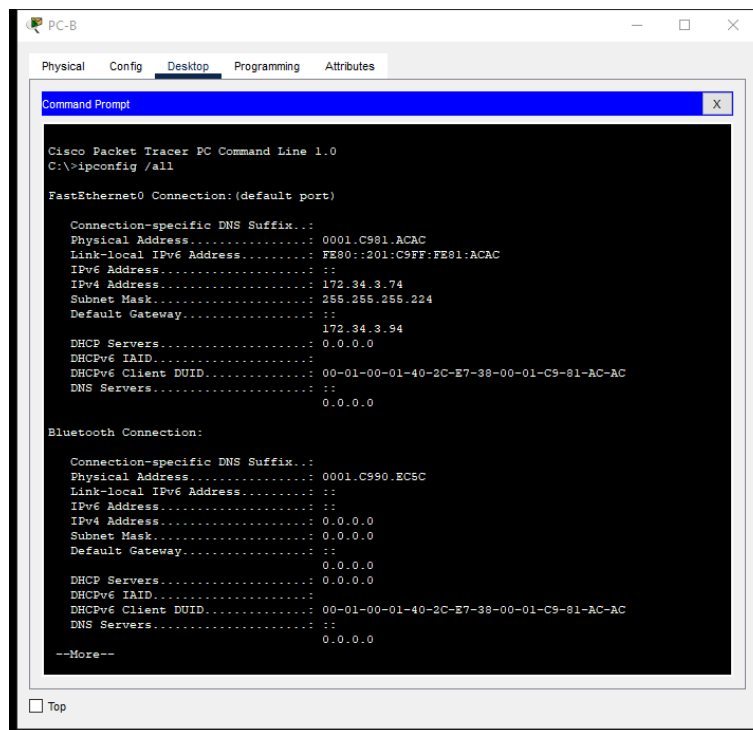
Tabla 5 Configuración de PC-B

| Configuración de red de PC - B       |                 |
|--------------------------------------|-----------------|
| Descripción                          | PC-B            |
| Dirección física                     | 0001.C981.ACAC  |
| Dirección IPv4                       | 172.34.3.74     |
| Máscara de subred                    | 255.255.255.224 |
| Puerta de enlace IPv4 predeterminada | 172.34.3.94     |

Fuente: Autor

La figura 3 detalla la configuración del PC-B donde podemos observar el uso del comando “*ip config /all*” para mostrar el detalle de la conexión que corresponde a los valores de la tabla 5.

Figura 3 Prueba de configuración PC-B

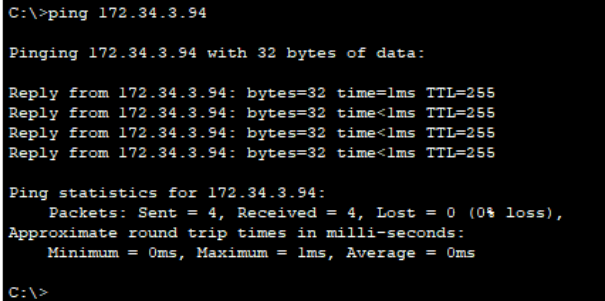
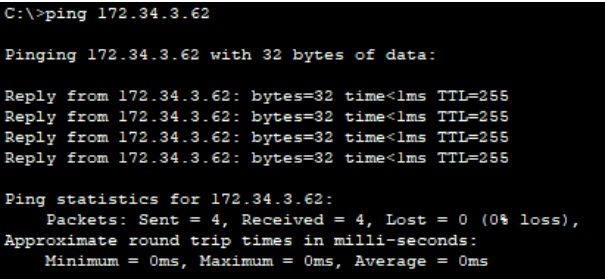


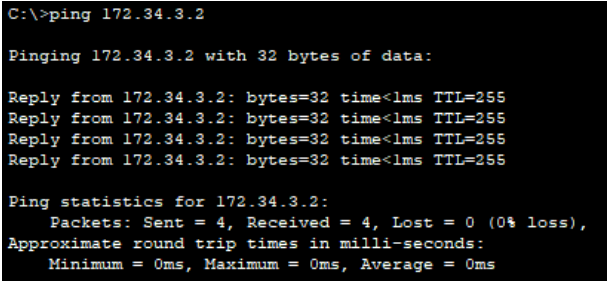
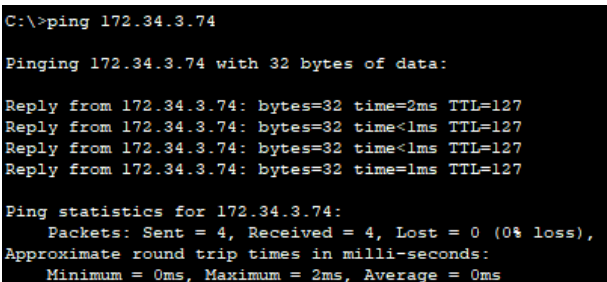
Fuente: Autor

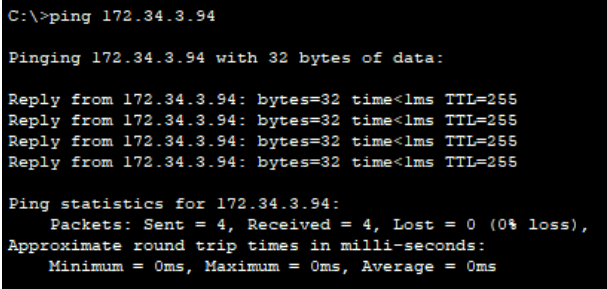
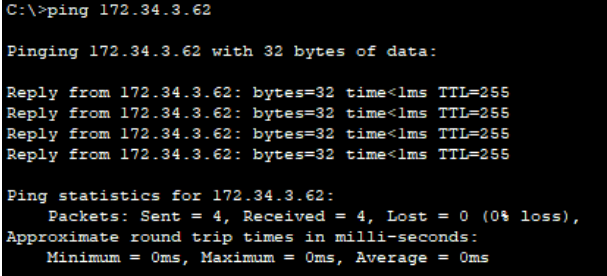
#### 1.4. Prueba y verificación de conectividad de extremo a extremo

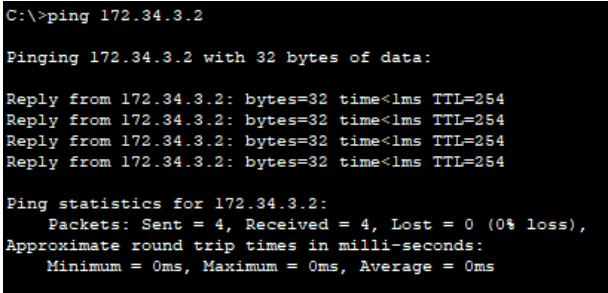
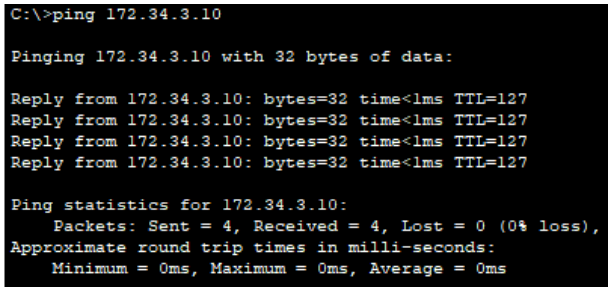
La tabla 6 registra las pruebas de comunicación entre equipos utilizando el comando *ping* hacia cada dirección IP.

Tabla 6 Prueba de conectividad

| Desde | A         | Dirección IP | Resultados de ping  |
|-------|-----------|--------------|---|
| PC-A  | R1 G0/0/0 | 172.34.3.94  | <p>Figura 4 Prueba de conectividad PC-A a R1 G0/0/0</p>  <pre>C:\&gt;ping 172.34.3.94  Pinging 172.34.3.94 with 32 bytes of data:  Reply from 172.34.3.94: bytes=32 time&lt;1ms TTL=255 Reply from 172.34.3.94: bytes=32 time&lt;1ms TTL=255 Reply from 172.34.3.94: bytes=32 time&lt;1ms TTL=255 Reply from 172.34.3.94: bytes=32 time&lt;1ms TTL=255  Ping statistics for 172.34.3.94:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 1ms, Average = 0ms  C:\&gt;</pre> <p>Fuente: Autor</p> <p>En la figura cuatro se observa que la configuración de la comunicación desde PC-A hasta R1 G0/0/0 es correcta debido a que el ping a la IP 172.34.3.94 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|       | R1 G0/0/1 | 172.34.3.62  | <p>Figura 5 Prueba de conectividad PC-A a R1 G0/0/1</p>  <pre>C:\&gt;ping 172.34.3.62  Pinging 172.34.3.62 with 32 bytes of data:  Reply from 172.34.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.34.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.34.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.34.3.62: bytes=32 time&lt;1ms TTL=255  Ping statistics for 172.34.3.62:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p>Fuente: Autor</p> <p>En la figura cinco se observa que la configuración de la comunicación desde PC-A hasta R1 G0/0/1 es correcta debido a que el ping a la IP 172.34.3.62 se valida con cuatro paquetes enviados y cuatro recibidos.</p>         |

|  |             |             |  |
|--|-------------|-------------|--|
|  | S1<br>VLAN1 | 172.34.3.2  | <p>Figura 6 Prueba de conectividad PC-A a S1</p>  <p>Fuente: Autor</p> <p>En la figura seis se observa que la configuración de la comunicación desde PC-A hasta S1 VLAN1 es correcta debido a que el ping a la IP 172.34.3.2 se valida con cuatro paquetes enviados y cuatro recibidos.</p>  |
|  | PC-B        | 172.34.3.74 | <p>Figura 7 Prueba de conectividad PC-A a PC-B</p>  <p>Fuente: Autor</p> <p>En la figura siete se observa que la configuración de la comunicación desde PC-A hasta PC-B es correcta debido a que el ping a la IP 172.34.3.74 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |

|      |           |             |   |
|------|-----------|-------------|---|
| PC-B | R1 G0/0/0 | 172.34.3.94 | <p>Figura 8 Prueba de conectividad PC-B a R1 G0/0/0</p>  <p>Fuente: Autor</p> <p>En la figura ocho se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/0 es correcta debido a que el ping a la IP 172.34.3.94 se valida con cuatro paquetes enviados y cuatro recibidos.</p>    |
|      | R1 G0/0/1 | 172.34.3.62 | <p>Figura 9 Prueba de conectividad PC-B a R1 G0/0/1</p>  <p>Fuente: Autor</p> <p>En la figura nueve se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/1 es correcta debido a que el ping a la IP 172.34.3.62 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |

|  |             |             |  |
|--|-------------|-------------|--|
|  | S1<br>VLAN1 | 172.34.3.2  | <p>Figura 10 Prueba de conectividad PC-B a S1</p>  <p>Fuente: Autor</p> <p>En la figura 10 se observa que la configuración de la comunicación desde PC-B hasta S1 VLAN1 es correcta debido a que el ping a la IP 172.34.3.2 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  | PC-A        | 172.34.3.10 | <p>Figura 11 Prueba de conectividad PC-B a PC-A</p>  <p>Fuente: Autor</p> <p>En la figura 11 se observa que la configuración de la comunicación desde PC-A hasta PB-B es correcta debido a que el ping a la IP 172.34.3.10 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |

Fuente: Autor



## 2. Escenario 2

En este segundo escenario se configura una red pequeña con un router, dos switches y dos equipos con capacidad para conectividad IPv4 e IPv6. Se realiza una administración de seguridad para el router y los switches y se configura el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

A continuación se referencian en La tabla 7 la identificación de cada VLAN que se van a configurar en el escenario 2.

Tabla 7 Nombre de las VLAN

| VLAN | Nombre de la VLAN |
|------|-------------------|
| 20   | Docentes          |
| 30   | Estudiantes       |
| 40   | Invitados         |
| 50   | Usuarios          |
| 56   | Native            |

Fuente: Autor

La asignación de direcciones se representa en la tabla 8 tanto para IPv4 como para Pv6, con la puerta de enlace predeterminada donde corresponda.

Tabla 8 Direccionamiento IPv4 e IPv6, Escenario 2

| Dispositivo / interfaz | Dirección IP / prefijo   | Puerta de enlace predeterminada |
|------------------------|--------------------------|---------------------------------|
| R1 G0/0/1.20           | 10.34.8.1 /26            | No corresponde                  |
|                        | 2001:db8:acad:a: :1 /64  | No corresponde                  |
| R1 G0/0/1.30           | 10.34.8.65 /27           | No corresponde                  |
|                        | 2001:db8:acad:b: :1 /64  | No corresponde                  |
| R1 G0/0/1.40           | 10.34.8.97 /29           | No corresponde                  |
|                        | 2001:db8:acad:c::1 /64   | No corresponde                  |
| R1 G0/0/1.56           | No corresponde           | No corresponde                  |
| R1 Loopback0           | 209.165.201.1 /27        | No corresponde                  |
|                        | 2001:db8:acad:209: :1/64 | No corresponde                  |
| S1 VLAN 40             | 10.34.8.98 /29           | 10.34.8.97                      |
|                        | 2001:db8:acad:c: :98 /64 | No corresponde                  |
|                        | fe80: :98                | No corresponde                  |
| S2 VLAN 40             | 10.34.8.99 /29           | 10.34.8.97                      |
|                        | 2001:db8:acad:c: :99 /64 | No corresponde                  |
|                        | fe80: :99                | No corresponde                  |
| PC-A NIC               | Dirección DHCP para      | DHCP para puerta de             |

|          |                          |  |
|----------|--------------------------|--|
|          | IPv4                     | 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  |

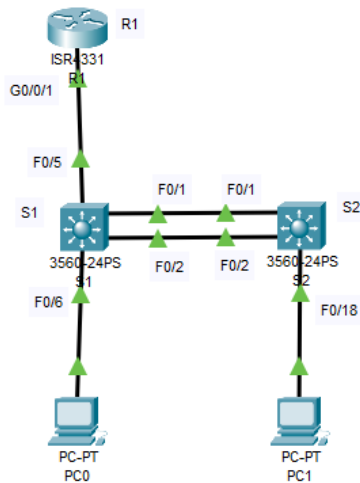
Fuente: Autor

Nota: No hay ninguna interfaz en el router que admita VLAN 50.

## 2.1 Construcción de la red del Escenario 2

La simulación se realiza en Packet Tracer de acuerdo con la topología de la red que se ilustra en la figura 12.

Figura 12 Topología de la red del escenario 2



Fuente: Autor

Para la configuración de los aspectos básicos de los dispositivos se siguen los siguientes pasos.

### 2.1.1 Inicializar y volver a cargar el router

Se accede al router mediante el puerto de consola y se elimina la configuración inicial desde el modo privilegiado y finalmente se reinicia.

```
Router>enable
Router#erase startup-config
```

El comando *erase startup-config* elimina la configuración de inicio de la NVRAM.

```
Router#reload
```

Con el comando *reload* se reinicia el router y se elimina la configuración anterior de la memoria.

Con los switches se realiza un proceso similar pero adicional se debe verificar si se crearon VLAN en el switch.

```
Switch>en
Switch#show flash
Switch#erase startup-config
Switch#reload
```

Después de recargar el switch procedemos a configurar la plantilla SDM para que admita IPv4 e IPv6 según la necesidad y se vuelve a recargar, para ello necesitamos estar en modo de configuración global. La configuración se realiza con la siguiente secuencia de comandos en cada switch.

```
Switch#config terminal
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#reload
```

### 2.1.2 Configuración de R1

En la tabla 9 se identifican todas las tareas requeridas para configurar R1 con el correspondiente comando y/o especificación.

Tabla 9 Configuración de R1, Escenario 2.

| Tarea                      | Especificación | Comando                                   |
|----------------------------|----------------|---|
| Desactivar la búsqueda DNS |                | Router(config)#no ip domain-lookup        |
| Nombre del router          | R1             | Router(config)#hostname R1<br>R1(config)# |

|  |   |   |
|--|---|---|
| Nombre de dominio  | ccna-sa.com   | R1(config)#ip domain-name ccna-sa.com   |
| Contraseña cifrada para el modo EXEC privilegiado                                    | class   | R1(config)#enable secret class  |
| Contraseña de acceso a la consola  | cisco   | R1(config)#line console 0<br>R1(config-line)#password cisco<br>R1(config-line)#login<br>R1(config-line)#exit  |
| Establecer la longitud mínima para las contraseñas                                   | 5 caracteres  | R1(config)#security passwords min-length 5  |
| Crear un usuario administrativo en la base de datos local                            | Nombre de usuario: admin<br>Password: admin1pass  | R1(config)#username admin<br>privilege 1 secret admin1pass  |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local |   | R1(config)#line vty 0 4<br>R1(config-line)#login local  |
| Configurar VTY solo aceptando SSH  |   | R1(config-line)#transport input ssh   |
| Cifrar las contraseñas de texto no cifrado   |   | R1(config)#service password-encryption  |
| Configure un MOTD Banner   | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.  | R1(config)#banner motd # R1 -<br>Mauricio Bautista Arteaga -<br>Ingenieria de Sistemas #  |
| Habilitar el routing IPv6  |   | R1(config)#ipv6 unicast-routing   |
| Configurar interfaz G0/0/1 y subinterfaces   | Establezca la descripción<br>Establece la dirección IPv4.<br>Establezca la dirección local de enlace IPv6 como fe80: :1<br>Establece la dirección IPv6.<br>Activar la interfaz. | <b>R1 G0/0/1.40</b><br>R1(config)#interface g0/0/1.20<br>R1(config-subif)#encapsulation dot1q 20<br>R1(config-subif)#description VLAN Docentes<br>R1(config-subif)#ip address 10.34.8.1 255.255.255.192<br>R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64<br>R1(config-subif)#ipv6 address |

|                                  |  |  |
|----------------------------------|--|--|
|                                  |  | <pre> fe80::1 link-local  <b>R1 G0/0/1.30</b> R1(config)#interface g0/0/1.30 R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#description VLAN Estudiantes R1(config-subif)#ip address 10.34.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local  <b>R1 G0/0/1.40</b> R1(config)#interface g0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description VLAN Invitados R1(config-subif)#ip address 10.34.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local  <b>R1 G0/0/1.56</b> R1(config)#interface g0/0/1.56 R1(config-subif)#encapsulation dot1q 56 R1(config-subif)#description VLAN Native R1(config-subif)#interface g0/0/1 R1(config-if)#no shutdown </pre> |
| Configure el Loopback0 interface | <p>Establezca la descripción</p> <p>Establece la dirección IPv4.</p> <p>Establece la dirección IPv6.</p> <p>Establezca la dirección local de</p> | <pre> R1(config-if)#interfase loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description Internet </pre>  |

|                                  |                          |   |
|----------------------------------|--------------------------|---|
|                                  | enlace IPv6 como fe80::1 | R1(config-if)#exit  |
| Generar una clave de cifrado RSA | Módulo de 1024 bits      | R1(config)#crypto key generate rsa<br>How many bits in the modulus [512]:<br>1024 |

Fuente: Autor

### 2.1.3 Configuración de S1 y S2

En la tabla 10 se presenta la configuración paso a paso de los switches S1 y S2, identificando las tareas realizadas, las recomendaciones y el código utilizado.

Tabla 10 Configuración de S1 y S2, Escenario 2

| Tarea   | Especificación           | Comando  |
|---|--------------------------|--|
| Desactivar la búsqueda DNS.                       |                          | <b>S1 y S2</b><br>Switch(config)#no ip domain lookup   |
| Nombre del switch                                 | S1 o S2, según proceda   | <b>S1</b><br>Switch(config)#hostname S1<br><br><b>S2</b><br>Switch(config)#hostname S2   |
| Nombre de dominio                                 | ccna-sa.com              | <b>S1 y S2</b><br>S1(config)#ip domain-name ccna-sa.com<br>S2(config)#ip domain-name ccna-sa.com   |
| Contraseña cifrada para el modo EXEC privilegiado | class                    | <b>S1 y S2</b><br>S1(config)#enable secret class<br>S2(config)#enable secret class   |
| Contraseña de acceso a la consola                 | cisco                    | <b>S1</b><br>S1(config)#line console 0<br>S1(config-line)#password cisco<br>S1(config-line)#login<br>S1(config-line)#exit<br><br><b>S2</b><br>S2(config)#line console 0<br>S2(config-line)#password cisco<br>S2(config-line)#login<br>S2(config-line)#exit |
| Crear un usuario administrativo en la             | Nombre de usuario: admin | <b>S1</b><br>S1(config)#username admin secret  |

|  |  |  |
|--|--|--|
| base de datos local  | Password:<br>admin1pass  | admin1pass<br><br><b>S2</b><br>S2(config)#username admin secret<br>admin1pass  |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local |  | <b>S1</b><br>S1(config)#line vty 0 15<br>S1(config-line)#login local<br><br><b>S2</b><br>S2(config)#line vty 0 15<br>S2(config-line)#login local   |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH             |  | <b>S1</b><br>S1(config-line)#transport input ssh<br>S1(config-line)#exit<br><br><b>S2</b><br>S2(config-line)#transport input ssh<br>S2(config-line)#exit   |
| Cifrar las contraseñas de texto no cifrado   |  | <b>S1</b><br>S1(config)#service password-encryption<br><br><b>S2</b><br>S2(config)#service password-encryption   |
| Configurar un MOTD Banner  | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. | <b>S1</b><br>S1(config)#banner motd # S1 -<br>Mauricio Bautista Arteaga -<br>Ingenieria de Sistemas #<br><br><b>S2</b><br>S2(config)#banner motd # S2 -<br>Mauricio Bautista Arteaga -<br>Ingenieria de Sistemas # |
| Generar una clave de cifrado RSA   | Módulo de 1024 bits  | <b>S1</b><br>S1(config)#crypto key generate rsa<br>How many bits in the modulus [512]:<br>1024<br><br><b>S2</b><br>S2(config)#crypto key generate rsa<br>How many bits in the modulus [512]:<br>1024               |

|  |   |  |
|--|---|--|
| Configurar la interfaz de administración (SVI) | Establecer la dirección IPv4 de capa 3<br>Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2<br>Establecer la dirección IPv6 de capa 3 | <b>S1</b><br>S1(config)#interface vlan 40<br>S1(config-if)#ip address 10.34.8.98 255.255.255.248<br>S1(config-if)#ipv6 address 2001:db8:acad:c::98/64<br>S1(config-if)#ipv6 address FE80::98 link-local<br>S1(config-if)#no shutdown<br>S1(config-if)#exit<br><br><b>S2</b><br>S2(config)#interface vlan 40<br>S2(config-if)#ip address 10.34.8.99 255.255.255.248<br>S2(config-if)#ipv6 address 2001:db8:acad:c::99/64<br>S2(config-if)#ipv6 address FE80::99 link-local<br>S2(config-if)#no shutdown<br>S2(config-if)#exit |
| Configuración del gateway predeterminado       | Configure la puerta de enlace predeterminada como 10.34.8.97 para IPv4  | <b>S1</b><br>S1(config)#ip default-gateway 10.34.8.97<br><br><b>S2</b><br>S2(config)#ip default-gateway 10.34.8.97   |

Fuente: Autor

#### 2.1.4 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) de S1

La configuración de la infraestructura de red de S1 incluye las tareas presentadas en la tabla 11 con la respectiva especificación y comandos.

Tabla 11 Configuración de infraestructura de red para S1, Escenario 2

| Tarea      | Especificación  | Comando  |
|------------|---|--|
| Crear VLAN | VLAN 20, nombre Docentes<br>VLAN 30, nombre Estudiantes | <b>S1</b><br>S1(config)#vlan 20<br>S1(config-vlan)#name Docentes<br>S1(config-vlan)#exit |



|   |   |  |
|---|---|--|
|   | VLAN 40, nombre Invitados<br>VLAN 50, nombre Usuarios<br>VLAN 56, nombre Native | S1(config)#vlan 30<br>S1(config-vlan)#name Estudiantes<br>S1(config-vlan)#exit<br>S1(config)#vlan 40<br>S1(config-vlan)#name Invitados<br>S1(config-vlan)#exit<br>S1(config)#vlan 50<br>S1(config-vlan)#name Usuarios<br>S1(config-vlan)#exit<br>S1(config)#vlan 56<br>S1(config-vlan)#name Native<br>S1(config-vlan)#exit                             |
| Crear troncos 802.1Q que utilicen la VLAN 56 nativa                             | Interfaces F0/1, F0/2 y F0/5  | S1(config)#interface range fa0/1-2, fa0/5<br>S1(config-if-range)#switchport trunk encapsulation dot1q<br>S1(config-if-range)#switchport mode trunk<br>S1(config-if-range)#switchport trunk native vlan 56  |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación                                      | S1(config-if-range)#interface range fa0/1-2<br>S1(config-if-range)#channel-group 1 mode active<br>S1(config-if-range)#exit<br>S1(config)#interface port-channel 1<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk encapsulation dot1q<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk native vlan 56 |
| Configurar el puerto de acceso de host para VLAN 20                             | Interface F0/6  | S1(config)#interface fa0/6<br>S1(config-if)#switchport mode acces<br>S1(config-if)#switchport acces vlan 20  |
| Configurar la seguridad del puerto en los puertos de acceso                     | Permitir 4 direcciones MAC  | S1(config-if)#switchport port-security maximum 4   |
| Proteja todas las interfaces no utilizadas                                      | Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y      | S1(config-if)#interface range fa0/3-4<br>S1(config-if-range)#switchport mode access<br>S1(config-if-range)#switchport access vlan 50   |

|  |        |  |
|--|--------|--|
|  | apagar | S1(config-if-range)#description<br>Interface sin uso<br>S1(config-if-range)#shutdown |
|--|--------|--|

Fuente: Autor

### 2.1.5 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) de S2

La configuración de la infraestructura de red de S2 se desarrolla en la tabla 12, donde se procede a crear las VLAN, y se les asigna seguridad a los puertos.

Tabla 12 Configuración de infraestructura de red para S2, Escenario 2

| Tarea   | Especificación   | Comando   |
|---|--|---|
| Crear VLAN  | VLAN 20, nombre Docentes<br>VLAN 30, nombre Estudiantes<br>VLAN 40, nombre Invitados<br>VLAN 50, nombre Usuarios<br>VLAN 56, nombre Native | S2(config)#vlan 20<br>S2(config-vlan)#name Docentes<br>S2(config-vlan)#exit<br>S2(config)#vlan 30<br>S2(config-vlan)#name Estudiantes<br>S2(config-vlan)#exit<br>S2(config)#vlan 40<br>S2(config-vlan)#name Invitados<br>S2(config-vlan)#exit<br>S2(config)#vlan 50<br>S2(config-vlan)#name Usuarios<br>S2(config-vlan)#exit<br>S2(config)#vlan 56<br>S2(config-vlan)#name Native<br>S2(config-vlan)#exit |
| Crear troncos 802.1Q que utilicen la VLAN 56 nativa                             | Interfaces F0/1 y F0/2   | S2(config)#interface range fa0/1-2<br>S2(config-if-range)#shutdown<br>S2(config-if-range)#switchport trunk encapsulation dot1q<br>S2(config-if-range)#switchport mode trunk<br>S2(config-if-range)#switchport trunk native vlan 56  |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación   | S2(config-if-range)#channel-group 1 mode active<br>S2(config-if-range)#<br>Creating a port-channel interface Port-channel 1<br>S2(config-if-range)#interface port-  |

|   |   |   |
|---|---|---|
|   |   | channel 1<br>S2(config-if)#switchport trunk encapsulation dot1q<br>S2(config-if)#switchport mode trunk<br>S2(config-if)#switchport trunk native vlan 56   |
| Configurar el puerto de acceso del host para la VLAN 30 | Interfaz F0/18  | S2(config-if)#interface fa0/18<br>S2(config-if)#switchport mode access<br>S2(config-if)#switchport access vlan 30   |
| Configure port-security en los access ports             | permite 4 MAC addresses   | S2(config-if)#switchport port-security maximum 4  |
| Asegure todas las interfaces no utilizadas.             | Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar | S2(config-if)#interface range fa0/3-17<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 50<br>S2(config-if-range)#description Interface sin uso<br>S2(config-if-range)#shutdown<br>S2(config-if-range)#interface range fa0/19-24<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 50<br>S2(config-if-range)#description Interface sin uso<br>S2(config-if-range)#shutdown |

Fuente: Autor

## 2.2 Configuración soporte de host

En este apartado se configura rutas predeterminadas para IPv4 e IPv6 en el router y se crean grupos DHCP en las VLAN 20 y VLAN 30.

### 2.2.1 Configuración de R1

En la tabla 13 se muestra la configuración del soporte host para R1, se configura DHCP para VLAN 20 y VLAN 30.

Tabla 13 Configuración de soporte de host para R1, Escenario 2

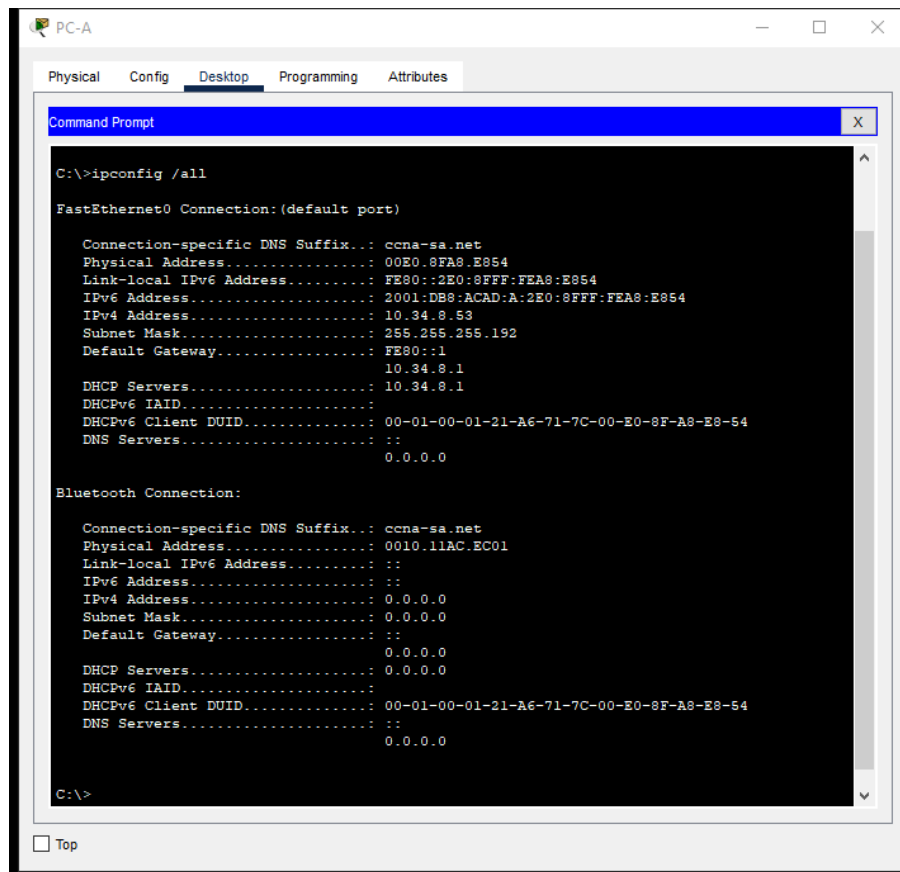
| Tarea                             | Especificación  | Comando   |
|-----------------------------------|---|---|
| Configure Default Routing         | Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0  | R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0<br>R1(config)#ipv6 route ::/0 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 unadccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada | R1(config)#ip dhcp excluded-address 10.34.8.1 10.34.8.52<br>R1(config)#ip dhcp pool vlan20-Docentes<br>R1(dhcp-config)#network 10.34.8.0 255.255.255.192<br>R1(dhcp-config)#default-router 10.34.8.1<br>R1(dhcp-config)#domain-name ccna-sa.net<br>R1(dhcp-config)#exit       |
| Configurar DHCP IPv4 para VLAN 30 | Cree un grupo DHCP para VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Nombre de dominio unadccna-sb.net.  | R1(config)#ip dhcp excluded-address 10.34.8.65 10.34.8.84<br>R1(config)#ip dhcp pool vlan30-Estudiantes<br>R1(dhcp-config)#network 10.34.8.64 255.255.255.224<br>R1(dhcp-config)#default-router 10.34.8.65<br>R1(dhcp-config)#domain-name ccna-sb.net<br>R1(dhcp-config)#exit |

Fuente: Autor

### 2.2.2 Configuración de los host PC-A y PC-B

Se requiere configurar los equipos host PC-A y PC-B (tabla 13 y 14) para que utilicen DHCP para IPv4 y asignen estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, se registran las configuraciones de red del host con el comando ipconfig /all (figura 13 y 14).

Figura 13 Configuraciones de red PC-A



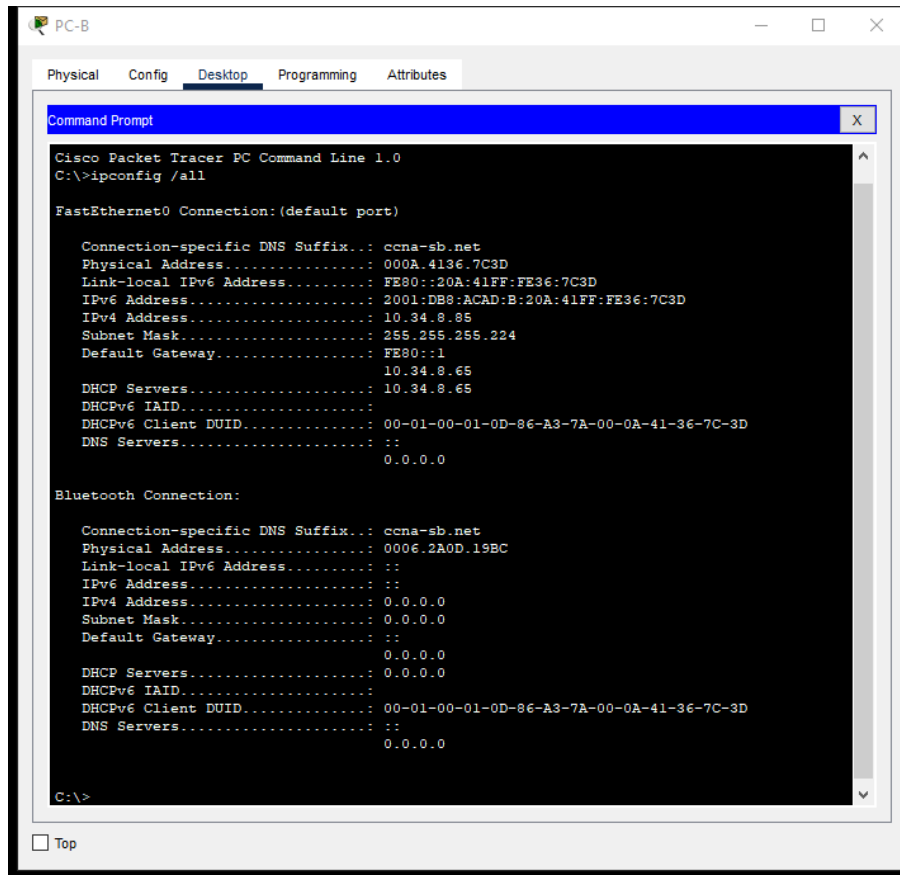
Fuente: Autor

Tabla 14 Configuración de red de PC-A, Escenario 2

| Configuración de red de PC-A |                 |
|------------------------------|-----------------|
| Descripción                  | ccna-sa.net     |
| Dirección física             | 00E0.8FA8.E854  |
| Dirección IP                 | 10.34.8.53      |
| Mascara de subred            | 255.255.255.192 |
| Gateway predeterminado       | 10.34.8.1       |
| Gateway predeterminado IPv6  | FE80::1         |

Fuente: Autor

Figura 14 Configuraciones de red PC-B



Fuente: Autor

Tabla 15 Configuración de red de PC-B, Escenario 2

| Configuración de red de PC-B |                 |
|------------------------------|-----------------|
| Descripción                  | ccna-sb.net     |
| Dirección física             | 000A.4136.7C3D  |
| Dirección IP                 | 10.34.8.85      |
| Mascara de subred            | 255.255.255.224 |
| Gateway predeterminado       | 10.34.8.65      |
| Gateway predeterminado IPv6  | FE80::1         |

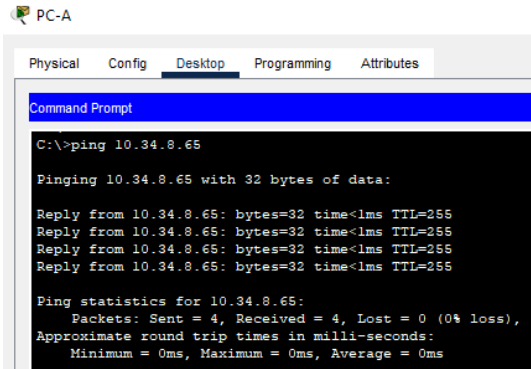
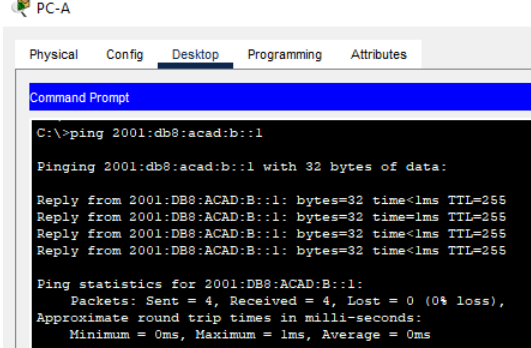
Fuente: Autor

### 2.2.3 Prueba y verificación de la conectividad de extremo a extremo

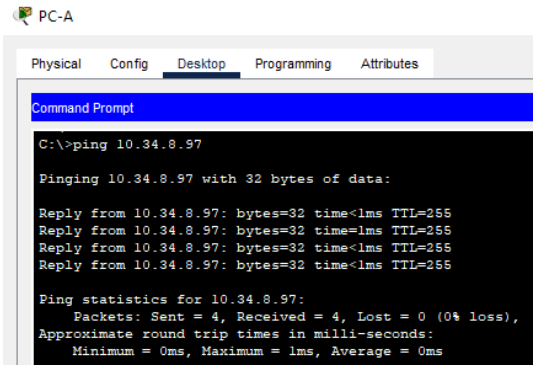
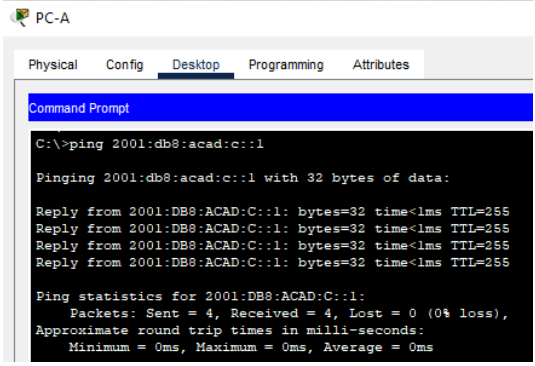
Mediante el comando *ping* se prueba la conectividad IPv4 e IPv6 entre todos los dispositivos de la red, el resultado se muestra en la tabla 16.

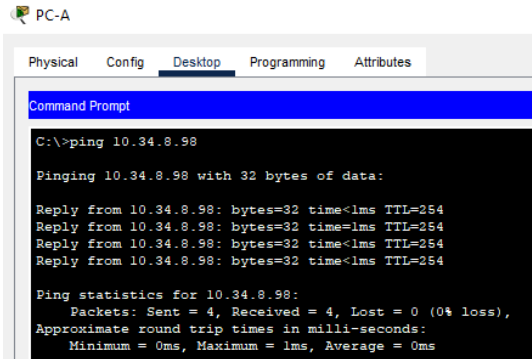
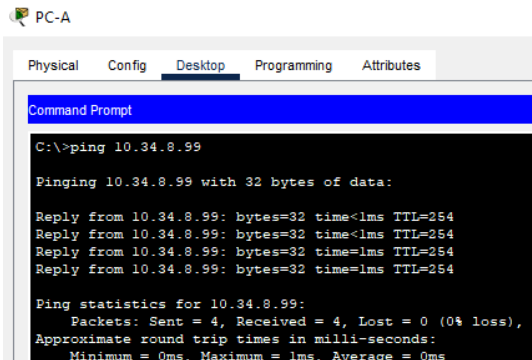
Tabla 16 Verificación de conectividad, Escenario 2

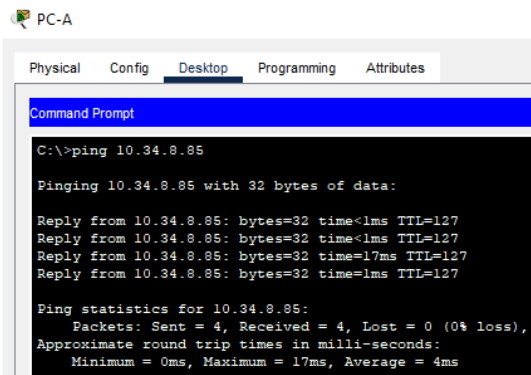
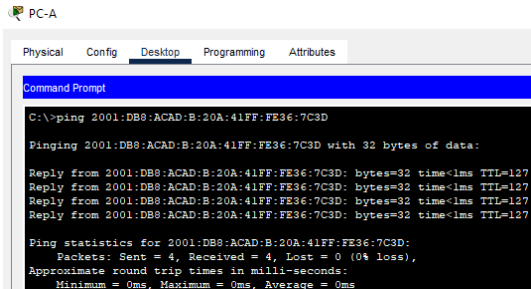
| De   | A                | IPv4<br>IPv6 | Dirección IP       | Resultados de ping   |
|------|------------------|--------------|--------------------|--|
| PC-A | R1,<br>G0/0/1.20 | IPv4         | 10.34.8.1          | <p>Figura 15 Prueba de conectividad entre PC-A y R1 G0/0/1.20 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 15 se observa que la configuración de la comunicación desde PC-A hasta R1 G0/0/1.20 es correcta debido a que el ping a la IPv4 10.34.8.1 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|      |                  | IPv6         | 2001:db8:acad:a::1 | <p>Figura 16 Prueba de conectividad entre PC-A y R1 G0/0/1.20 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 16 se observa que la configuración de la comunicación desde PC-A hasta R1 G0/0/1.20 es correcta debido a que el ping a la</p>   |

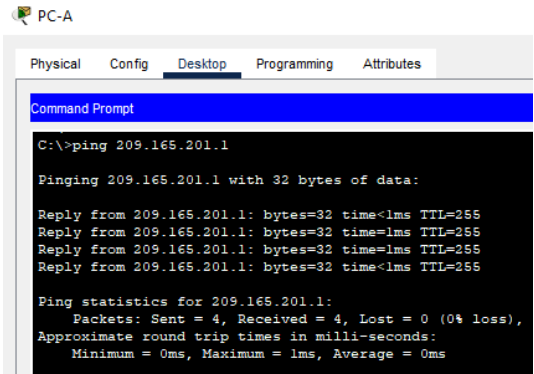
|  |                  |      |                    |   |
|--|------------------|------|--------------------|---|
|  |                  |      |                    | IPv6 2001:db8:acad:a::1 se valida con cuatro paquetes enviados y cuatro recibidos.  |
|  | R1,<br>G0/0/1.30 | IPv4 | 10.34.8.65         | <p>Figura 17 Prueba de conectividad entre PC-A y R1 G0/0/1.30 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 17 se observa que la configuración de la comunicación desde PC-A hasta R1 G0/0/1.30 es correcta debido a que el ping a la IPv4 10.34.8.65 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  |                  | IPv6 | 2001:db8:acad:b::1 | <p>Figura 18 Prueba de conectividad entre PC-A y R1 G0/0/1.30 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 18 se observa que la configuración de la comunicación desde PC-A hasta R1 G0/0/1.30 es</p>   |

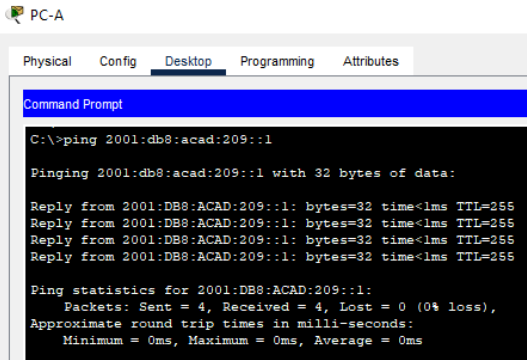
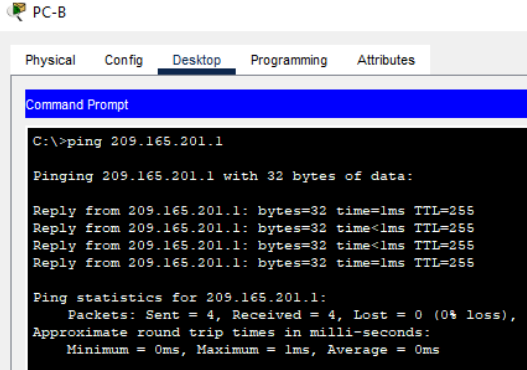


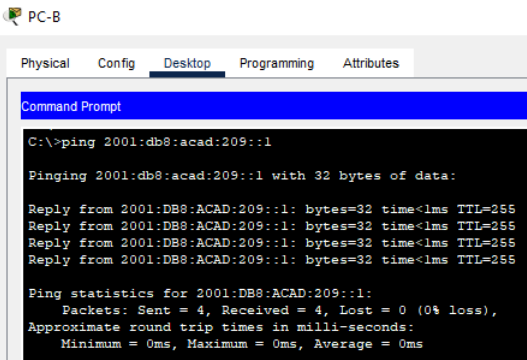
|  |                  |      |                    |   |
|--|------------------|------|--------------------|---|
|  |                  |      |                    | correcta debido a que el ping a la IPv6 2001:db8:acad:b::1 se valida con cuatro paquetes enviados y cuatro recibidos.   |
|  | R1,<br>G0/0/1.40 | IPv4 | 10.34.8.97         | <p>Figura 19 Prueba de conectividad entre PC-A y R1 G0/0/1.40 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 19 se observa que la configuración de la comunicación desde PC-A hasta R1 G0/0/1.40 es correcta debido a que el ping a la IPv4 10.34.8.97 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  |                  | IPv6 | 2001:db8:acad:c::1 | <p>Figura 20 Prueba de conectividad entre PC-A y R1 G0/0/1.40 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 20 se observa que la configuración de la comunicación</p>  |

|  |             |      |                     |   |
|--|-------------|------|---------------------|---|
|  |             |      |                     | desde PC-A hasta R1 G0/0/1.40 es correcta debido a que el ping a la IPv6 2001:db8:acad:c::1 se valida con cuatro paquetes enviados y cuatro recibidos.  |
|  | S1, VLAN 40 | IPv4 | 10.34.8.98          | <p>Figura 21 Prueba de conectividad entre PC-A y S1 VLAN40 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 21 se observa que la configuración de la comunicación desde PC-A hasta S1 VLAN40 es correcta debido a que el ping a la IPv4 10.34.8.98 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  |             | IPv6 | 2001:db8:acad:c::98 | No se valida conectividad   |
|  | S2, VLAN 40 | IPv4 | 10.34.8.99          | <p>Figura 22 Prueba de conectividad entre PC-A y S2 VLAN40 IPv4</p>  <p>Fuente: Autor</p>   |

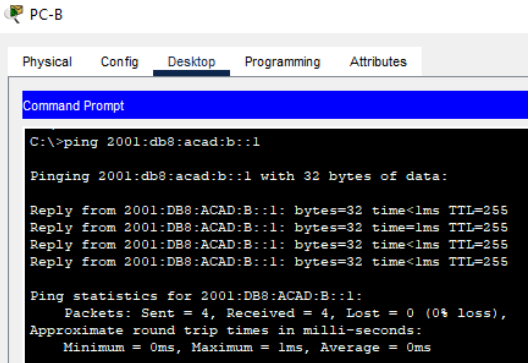
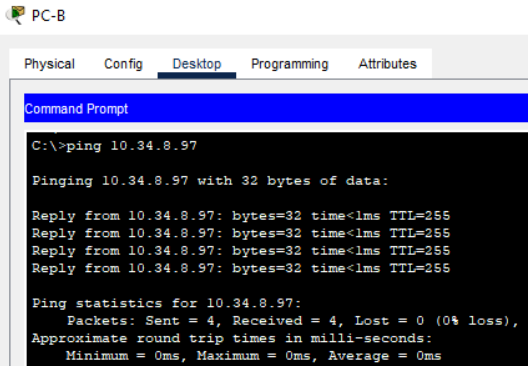
|  |      |      |                                    |  |
|--|------|------|------------------------------------|--|
|  |      |      |                                    | <p>En la figura 22 se observa que la configuración de la comunicación desde PC-A hasta S2 VLAN40 es correcta debido a que el ping a la IPv4 10.34.8.99 se valida con cuatro paquetes enviados y cuatro recibidos.</p>  |
|  |      | IPv6 | 2001:db8:acad:c::99                | No se valida conectividad  |
|  | PC-B | IPv4 | 10.34.8.85                         | <p>Figura 23 Prueba de conectividad entre PC-A y PC-B IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 23 se observa que la configuración de la comunicación desde PC-A hasta PC-B es correcta debido a que el ping a la IPv4 10.34.8.85 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  |      | IPv6 | 2001:db8:acad:b:20a:41ff:fe36:7c3d | <p>Figura 24 Prueba de conectividad entre PC-A y PC-B IPv6</p>   |

|  |            |      |               |   |
|--|------------|------|---------------|---|
|  |            |      |               | <p>Fuente: Autor</p> <p>En la figura 24 se observa que la configuración de la comunicación desde PC-A hasta PC-B es correcta debido a que el ping a la IPv6 2001:db8:acad:b:20a:41ff:fe36:7c3d se valida con cuatro paquetes enviados y cuatro recibidos.</p>   |
|  | R1 Bucle 0 | IPv4 | 209.165.201.1 | <p>Figura 25 Prueba de conectividad entre PC-A y R1 Bucle 0 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 25 se observa que la configuración de la comunicación desde PC-A hasta R1 Bucle 0 es correcta debido a que el ping a la IPv4 209.165.201.1 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |

|      |            |      |                      |   |
|------|------------|------|----------------------|---|
|      |            | IPv6 | 2001:db8:acad:209::1 | <p>Figura 26 Prueba de conectividad entre PC-A y R1 Bucle 0 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 26 se observa que la configuración de la comunicación desde PC-A hasta R1 Bucle 0 es correcta debido a que el ping a la IPv6 2001:db8:acad:209::1 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
| PC-B | R1 Bucle 0 | IPv4 | 209.165.201.1        | <p>Figura 27 Prueba de conectividad entre PC-B y R1 Bucle 0 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 27 se observa que la configuración de la comunicación desde PC-B hasta R1 Bucle 0 es correcta debido a que el ping a la IPv4 209.165.201.1 se valida con cuatro paquetes enviados y cuatro recibidos.</p>      |

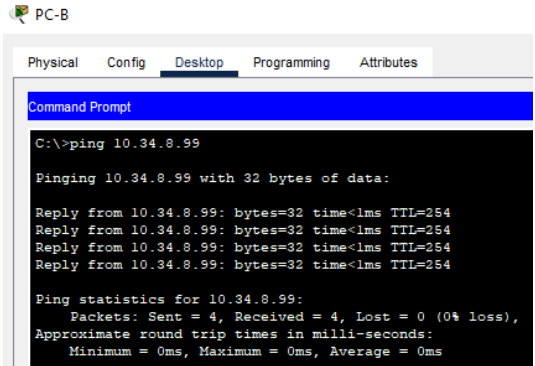
|  |                  |      |                      |   |
|--|------------------|------|----------------------|---|
|  |                  | IPv6 | 2001:db8:acad:209::1 | <p>Figura 28 Prueba de conectividad entre PC-B y R1 Bucle 0 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 28 se observa que la configuración de la comunicación desde PC-B hasta R1 Bucle 0 es correcta debido a que el ping a la IPv6 2001:db8:acad:209::1 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  | R1,<br>G0/0/1.20 | IPv4 | 10.34.8.1            | <p>Figura 29 Prueba de conectividad entre PC-B y R1 G0/0/1.20 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 29 se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/1.20 es correcta debido a que el ping a la IPv4 10.34.8.1 se valida con cuatro paquetes enviados y cuatro recibidos.</p>      |

|  |                  |      |                    |   |
|--|------------------|------|--------------------|---|
|  |                  | IPv6 | 2001:db8:acad:a::1 | <p>Figura 30 Prueba de conectividad entre PC-B y R1 G0/0/1.20 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 30 se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/1.20 es correcta debido a que el ping a la IPv6 2001:db8:acad:a::1 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  | R1,<br>G0/0/1.30 | IPv4 | 10.34.8.65         | <p>Figura 31 Prueba de conectividad entre PC-B y R1 G0/0/1.30 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 31 se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/1.30 es correcta debido a que el ping a la IPv4 10.34.8.65 se valida con cuatro paquetes enviados y cuatro recibidos.</p>       |

|  |                  |      |                    |   |
|--|------------------|------|--------------------|---|
|  |                  | IPv6 | 2001:db8:acad:b::1 | <p>Figura 32 Prueba de conectividad entre PC-B y R1 G0/0/1.30 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 32 se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/1.30 es correcta debido a que el ping a la IPv6 2001:db8:acad:b::1 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  | R1,<br>G0/0/1.40 | IPv4 | 10.34.8.97         | <p>Figura 33 Prueba de conectividad entre PC-B y R1 G0/0/1.40 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 33 se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/1.40 es correcta debido a que el ping a la IPv4 10.34.8.97 se valida con cuatro paquetes enviados y cuatro</p>                  |



|  |             |      |                    |   |
|--|-------------|------|--------------------|---|
|  |             |      |                    | recibidos.  |
|  |             | IPv6 | 2001:db8:acad:c::1 | <p>Figura 34 Prueba de conectividad entre PC-B y R1 G0/0/1.40 IPv6</p>  <p>Fuente: Autor</p> <p>En la figura 34 se observa que la configuración de la comunicación desde PC-B hasta R1 G0/0/1.40 es correcta debido a que el ping a la IPv6 2001:db8:acad:c::1 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  | S1, VLAN 40 | IPv4 | 10.34.8.98         | <p>Figura 35 Prueba de conectividad entre PC-B y S1 VLAN 40 IPv4</p>  <p>Fuente: Autor</p> <p>En la figura 35 se observa que la configuración de la comunicación desde PC-B hasta S1 VLAN40 es correcta debido a que el ping a la IPv4 10.34.8.98 se valida con cuatro</p>  |

|  |             |      |                     |   |
|--|-------------|------|---------------------|---|
|  |             |      |                     | paquetes enviados y cuatro recibidos.   |
|  |             | IPv6 | 2001:db8:acad:c::98 | No se valida la conectividad  |
|  | S2, VLAN 40 | IPv4 | 10.34.8.99          | <p>Figura 36 Prueba de conectividad entre PC-B y S2 VLAN 40 IPv4.</p>  <p>Fuente: Autor</p> <p>En la figura 36 se observa que la configuración de la comunicación desde PC-B hasta S2 VLAN40 es correcta debido a que el ping a la IPv4 10.34.8.99 se valida con cuatro paquetes enviados y cuatro recibidos.</p> |
|  |             | IPv6 | 2001:db8:acad:c::99 | No se valida conectividad   |

Fuente: Autor

## CONCLUSIONES

Antes de iniciar con la configuración básica de la red es necesario establecer el Subneteo de la red, esto garantiza que la red adquiera mayor claridad, que la comunicación sea controlada y que el proceso siguiente de configuración de los dispositivos se realice con mejor veracidad.

La configuración básica de una red implica varias tareas entre las que se destacan la correcta elección de los dispositivos y medios de transmisión, el nombramiento de estos dispositivos, la configuración de puertos y la configuración de la seguridad.

Se considera indispensable al momento de configurar una red Cisco seguir los protocolos de seguridad para prevenir y supervisar accesos no autorizados. En este contexto y en relación con el escenario 2, las redes Cisco tienen múltiples capas de seguridad tanto externas como internas, una de estas consiste en la seguridad de puerto que limita la cantidad de direcciones MAC y solo permite el acceso a las MAC identificadas.

## BIBLIOGRAFÍA

CASTAÑO, Rafael. Redes locales. Madrid: Macmillan Iberia S.A., 2012.

CISCO. Configuración básica de un router. Introducción a las redes. {En línea}. (2020). Disponible en: <<https://contenthub.netacad.com/itn/10.0.1>>

EL SUBNETTING para sacar el máximo partido a tu red [Anónimo]. IONOS Digital Guide [página web]. [Consultado el 21, octubre, 2022]. Disponible en Internet: <<https://www.ionos.es/digitalguide/servidores/know-how/subnetting-como-funcionan-las-subredes/>>.

ARIGANELLO, Ernesto. Redes Cisco Guía de estudio para la certificación CCNA 200-301. Madrid: RA-MA Editorial, 2020.

STALLINGS, William. Comunicaciones y Redes de Computadores. Madrid: Pearson Educación, 2004.

TANENBAUM, Andrew. Redes de Computadoras. México: Pearson Educación, 2012.

## ANEXOS

Anexo 1. Archivos de simulación - Prueba de habilidades práctica CCNA –  
Escenarios 1 y 2

Enlace de descarga de las simulaciones de los escenarios:

[https://drive.google.com/drive/folders/1864HzObTvUUQpwx5Cq8aYQRnH\\_T8ZtO?usp=sharing](https://drive.google.com/drive/folders/1864HzObTvUUQpwx5Cq8aYQRnH_T8ZtO?usp=sharing)