

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

HECTOR JOSE MALDONADO CARO

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

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

HECTOR JOSE MALDONADO CARO

Diplomado como opción de grado presentado para optar  
el título de INGENIERO EN SISTEMAS

PAULITA FLOR SALAZAR

Director

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

BOGOTA

2022

NOTA DE ACEPTACIÓN

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Bogotá, 27 de noviembre de 2022.

Este trabajo está dedicado a DIOS y mi familia, los cuales fueron el motor principal para alcanzar mis logros profesionales.

## AGRADECIMIENTOS

El presente trabajo de grado para ostentar el título de Ingeniero de Sistemas tiene un significado muy importante para mi vida profesional, ha sido parte del esfuerzo incondicional, de antemano le doy gracias a la Directora del programa Paulita Flor Salazar, quien con su experiencia y experticia nos logro guiar de la mejor manera para así llegar a feliz término de la opción de grado como Ingeniero de Sistemas.

## TABLA DE CONTENIDO

|  |    |
|--|----|
| GLOSARIO.....  | 10 |
| RESUMEN.....   | 12 |
| INTRODUCCIÓN.....  | 13 |
| 1. DESARROLLO ESCENARIO 1.....   | 14 |
| 1.1. Topología.....  | 14 |
| 1.2. PARTE 1: Construyendo la Red.....   | 14 |
| 1.3. PARTE 2: Desarrolle el esquema de direccionamiento IP.....                                  | 15 |
| 1.4. PARTE 3: Configure aspectos básicos.....  | 17 |
| 1.4.1. Paso 1: configurar los ajustes básicos.....   | 17 |
| 1.4.2. Paso 2: Verificamos a ingresar la configuración del dispositivo.....                      | 19 |
| 1.4.3. Paso 3: Las tareas de configuración de Swich S1.....                                      | 21 |
| 1.4.4. Paso 4: Procedimiento configuración básica del dispositivo Switch S1<br><u>22</u>         |    |
| 1.4.5. Paso 5: Configurar los equipos PC.....  | 24 |
| 1.4.5.1. Configuración PC A.....   | 24 |
| 1.4.5.2. Configuración PC-B.....   | 25 |
| 1.4.5.3. Pruebas de conectividad entre dispositivos.....   | 28 |
| 2. DESARROLLO ESCENARIO 2.....   | 33 |
| 2.1 Topología.....   | 33 |
| Creación de la Topología lógica de red.....  | 34 |
| 2.2 PARTE 1: Iniciación de dispositivos.....   | 36 |
| 2.2.1 Paso 1: Inicializar y cargar los Router y los Switches.....                                | 36 |
| 2.2.2 Paso 2: Configuración R1.....  | 37 |
| 2.2.3 Paso 3 Configuración S1 y S2.....  | 40 |
| 2.2.4 Parte 4: Configuración de la infraestructura de red (VLAN, Trunking,<br>EtherChannel)..... | 43 |
| 2.2.4.1 Paso 1 Configurar S1.....  | 43 |
| 2.2.4.2 Paso 2 Configure el S2.....  | 45 |
| 2.2.4.3 Parte 5 Configurar soporte de host.....  | 47 |

|  |    |
|--|----|
| 2.2.5 Paso 1 Configure R1 .....  | 47 |
| 2.2.6 Paso 2 Configurar los servidores.....                                | 48 |
| 2.2.7 Paso 3 Probar y verificar la conectividad de extremo a extremo ..... | 49 |
| 2.2.7.1 PRUEBAS DE CONECTIVIDAD.....                                       | 50 |
| CONCLUSIONES .....   | 51 |
| REFERENCIAS BIBLIOGRÁFICAS.....  | 52 |
| ANEXOS.....  | 53 |

## LISTA DE FIGURAS

|   |    |
|---|----|
| Figura 1 Topología de red escenario 1 .....   | 14 |
| Figura 2 Cableado red acuerdo escenario 1. ....   | 14 |
| Figura 3 Topología escenario 1. ....  | 16 |
| Figura 4 Configuración total del dispositivo R1 .....   | 21 |
| Figura 5 Configuración total del dispositivo S1 .....   | 24 |
| Figura 6 Configuración PC-A .....   | 25 |
| Figura 7 Configuración PC-B .....   | 26 |
| Figura 8 Dirección Mac PC-A- Comando ipconfig /all .....  | 26 |
| Figura 9 Dirección Mac PC-B - Comando ipconfig /all .....   | 27 |
| Figura 10 Comando tracert – desde PCA Verificando Conectividad entre dispositivos ....  | 28 |
| Figura 11 Comando tracert – desde PCB Verificando Conectividad entre dispositivos ....  | 29 |
| Figura 12 Prueba Conectividad desde PCA 172.26.3.10 A G/0/0/0 172.26.3.94.....  | 30 |
| Figura 13 Prueba Conectividad desde PCA 172.26.3.10 A G/0/0/1 172.26.3.94.....  | 30 |
| Figura 14 Prueba Conectividad desde PCA 172.26.3.10 A s1 vlan 1 172.26.3.2 .....  | 31 |
| Figura 15 Prueba Conectividad desde PCA 172.26.3.10 A PCB 172.26.3.2.....   | 31 |
| Figura 16 Prueba Conectividad desde PCB 172.26.3.74 Hacia G0/0/0 172.26.3.94 -<br>G0/0/1 172.26.3.62 – S1 VLAN1 172.26.3.2..... | 32 |
| Figura 17 Topología de red escenario 2 .....  | 33 |
| Figura 18 Montaje en Packet Tracer escenario 2.....   | 34 |
| Figura 19 Reinicio de Switches.....   | 36 |
| Figura 20 Prueba conectividad desde PCA – IPV4.....   | 50 |
| Figura 21 Prueba conectividad desde PC-B – IPV6.....  | 50 |

## LISTA DE TABLAS

|  |    |
|--|----|
| Tabla 1 Asignación de subredes.....  | 15 |
| Tabla 2 configuración básica y asignación de direcciones IP.....           | 16 |
| Tabla 3 configuración básica R1.....                                       | 18 |
| Tabla 4 Configuración básica S1.....                                       | 21 |
| Tabla 5 Configuración PC-A.....  | 24 |
| Tabla 6 Configuración PC-B.....  | 25 |
| Tabla 7 VLAN Escenario 2.....  | 35 |
| Tabla 8 Tabla asignación de direcciones escenario 2.....                   | 35 |
| Tabla 9 Configuración básica ROUTER 1 – nombre, dominios, contraseñas..... | 37 |
| Tabla 10 Continuación configuración básica ROUTER 1.....                   | 38 |
| Tabla 11 Configuración interfaces R1.....                                  | 39 |
| Tabla 12 configuración básica del S1 y S2 – contraseñas y VLAN.....        | 40 |
| Tabla 13 Continuación configuración básica del S1 y S2.....                | 41 |
| Tabla 14 creación de VLAN – S1.....  | 43 |
| Tabla 15 Creación de VLAN – s2.....  | 45 |
| Tabla 16 Configuración R1 – DHCP.....                                      | 47 |
| Tabla 17 configuración PC-A.....   | 48 |
| Tabla 18 Configuración PC-B.....   | 48 |
| Tabla 19 Verificación de conectividad desde PC-A y PC-B.....               | 49 |

## GLOSARIO

**DIRRECCION IP:** Número de Identificación única de un dispositivo en la red para poder establecer comunicación e intercambiar diferentes servicios. Además, una dirección IP consta de dos partes, una identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red.<sup>1</sup>

**DHCP:** El protocolo de configuración dinámica de host (DHCP) permite a los dispositivos de red obtener una dirección IP cuando se conecta a la red.<sup>2</sup>

**DNS:** Es el sistema de nombres de dominio, esta información sirve para que el usuario no escriba en su navegador una dirección IP, sino no por el contrario digite directamente la información del servicio.<sup>3</sup>

**IPV4:** Es la cuarta versión del protocolo de internet IP, usa direcciones de 32 bits y será reemplazado en el futuro por IPV6.

**IPV6:** Protocolo de comunicación en internet mas reciente, con alto potencial de crecimiento en múltiples dispositivos interconectados en las diferentes redes.

**MODELO OSI:** El modelo OSI, afronta el problema de las comunicaciones de datos y las redes informáticas dividiéndolo en niveles. Cada participante de la comunicación incorpora como mínimo uso de los mismos, y los equipos terminales los incorporan todos.<sup>4</sup>

---

<sup>1</sup> ARIGANELLO Ernesto; Técnicas de configuración de routers cisco (2014)

<sup>2</sup> ARIGANELLO Ernesto; Técnicas de configuración de routers cisco (2014)

<sup>3</sup> MAESTRE Javier; El derecho del nombre de dominio (2001)

<sup>4</sup> BARCELÓ José, ÍÑIGO Jordi, MARTÍ Ramon, PEIG Enric y PERRAMON Xavier; Redes de computadores (2004)

**ROUTER:** Es un encaminador es un dispositivo de red que permite la interconexión de redes al nivel de la capa de Red del Modelo de Referencia OSI.<sup>5</sup>

**VPN:** Una VPN es una Red Privada Virtual, se utiliza principalmente para conectar dos redes privadas a través de la red publica de datos, proporcionando un túnel para encapsular un protocolo en otro.<sup>6</sup>

---

<sup>5</sup> MATURRO Gerardo; Guía para laboratorios de redes (2007)

<sup>6</sup> ARIGANELLO Ernesto; Técnicas de configuración de routers cisco (2014)

## RESUMEN.

En el desarrollo de la presente actividad se va a implementar 2 redes corporativas la cuales serán implementadas bajo la tecnología CISCO, el cual es uno de los aspectos más importantes en el diseño de la misma ya que nos brinda confiabilidad y seguridad a nuestra red.

Realizaremos la configuración de cada uno de los dispositivos que hacen parte de la misma, indicaremos cada uno de los comandos aplicado y los resultados obtenidos del mismo. Aplicaremos direccionamiento IPV4 e IPV6 junto con la técnica de VLSM para crear las diferentes subredes ajustadas a las necesidades indicadas, configuraremos los protocolos de enrutamiento adecuados o crearemos rutas por defecto dependiendo de la necesidad aplicaremos todo lo que tiene que ver con la creación y configuración de las VLAN, ACL y DHCP.

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

## ABSTRACT.

In the development of this activity, 2 corporate networks will be implemented which will be implemented under CISCO technology, which is one of the most important aspects in its design since it provides reliability and security to our network.

We will carry out the configuration of each of the devices that are part of it, we will indicate each of the applied commands and the results obtained from it. We will apply IPV4 and IPV6 addressing together with the VLSM technique to create the different subnets adjusted to the indicated needs, we will configure the appropriate routing protocols or we will create default routes depending on the need, we will apply everything that has to do with the creation and configuration of VLANs, ACLs, and DHCP.

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

## INTRODUCCIÓN

A lo largo de la historia los avances tecnológicos e informáticos han avanzado de manera vertiginosa, el intercambio de información cumple un papel importante en el desarrollo de nuestra sociedad u organización, razón por la cual se hace necesario almacenarla, analizarla y así mismo se comparte, puede utilizarse constantemente en cualquier parte bajo diferentes dispositivos interconectados a la red.

Debemos estar actualizándonos constantemente ya que esta rama cambia mucho, siempre hay avances mejorando. Por este motivo por medio del desarrollo de esta actividad lo que busca es que profundicemos, que analicemos y que actuemos en el desarrollo e implementación de 2 redes que van a exigir un poco de esas destrezas que seguramente adquirimos en el desarrollo de tantos laboratorios y ejercicios prácticos.

Se nos suministra el diseño de 2 redes, la cuales tienes una serie de parámetros los cuales debemos cumplir a total satisfacción, realizar la configuración y realizar las pruebas necesarias con el fin de verificar el correcto funcionamiento de cada uno de los pasos configurados.

Todo el proceso de direccionamiento realizado en las 2 redes, se la va a desarrollar utilizando VLSM implementando tanto en IPV4 como en IPV6, además se implementarán rutas por defecto que me permite el intercambio de mensajes entre redes diferentes, se configurará VLAN que me permitirá tener un mayor control de mi red mejorando notablemente los aspectos de seguridad de la misma.

## 1. DESARROLLO ESCENARIO 1

El desarrollo del primer escenario tiene como propósito configurar todos los dispositivos de una red simulada, de igual forma se debe implementar el esquema de subredes para las redes propuestas y administrar de manera segura los dispositivos de interconexión.

### 1.1. Topología

*Figura 1 Topología de red escenario 1*



Fuente: Prueba de habilidades diplomado CCNA.

### 1.2. PARTE 1: Construyendo la Red

Para esta actividad se crea la topología de red, se deben implementar y configurar los aspectos propuestos en el escenario No 1, en el simulador Packet Tracer se deben interconectar un Router, un switch y dos computadores, a través de sus respectivos puertos destinados para cada equipo. El direccionamiento IP se realizará mediante protocolo IPv4

*Figura 2 Cableado red acuerdo escenario 1.*



Fuente: Autoría Propia

### 1.3. PARTE 2: Desarrolle el esquema de direccionamiento IP

La pequeña red LAN tendrá el siguiente esquema, deberá funcionar bajo el protocolo de internet IPv4, sus respectivas subredes, la red LAN1 deberá contener 60 host y la LAN2 20 host, información de vital importancia para generar una red escalable en caso de requerir algún puerto de conexión, el direccionamiento se realizará correspondiente a la siguiente información.

Subneteo del rango IP:

Lo primero que debemos hacer en el caso de que conocemos la TOPOLOGÍA con los requisitos de cada una de las subredes es proceder a Subneteo el rango asignado, el mismo nos queda de la siguiente manera:

La red en general está formada por 2 subredes acuerdo lo descrito en la siguiente tabla:

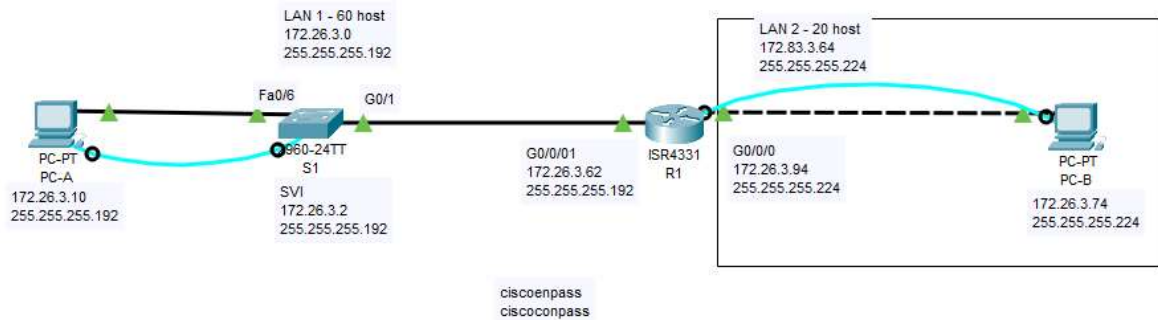
*Tabla 1 Asignación de subredes*

| RED   | N° IP | dir red     | masc            | /  | broadcast   | disponibles | N° HOST |
|-------|-------|-------------|-----------------|----|-------------|-------------|---------|
| LAN 1 | 60    | 172.26.3.0  | 255.255.255.192 | 26 | 172.26.3.63 | 62          | 60      |
| LAN 2 | 20    | 172.26.3.64 | 255.255.255.224 | 27 | 172.26.3.95 | 30          | 20      |

Fuente: Autoría Propia

Como ya conocemos los rangos IP para cada una de las subredes podemos proceder a realizar la asignación de la IP correspondiente a cada una de las interfaces que intervienen, este queda como se indica a continuación:

Figura 3 Topología escenario 1.



Fuente: Autoría Propia

Procedemos a realizar la asignación a cada interfaz y a realizar las primeras configuraciones a cada uno de los dispositivos.

Tabla 2 configuración básica y asignación de direcciones IP.

| Item                              | Requerimiento  |
|-----------------------------------|--|
| Dirección de Red                  | 172.26.3.0 donde X corresponde a los últimos dos dígitos de su cédula.                                 |
| Requerimiento de host Subred LAN1 | 60   |
| Requerimiento de host Subred LAN2 | 20   |
| R1 G0/0/1                         | Última dirección de host de la subred LAN1<br><br>Int g0/0/1<br>Ip address 172.26.3.62 255.255.255.192 |
| R1 G0/0/0                         | Última dirección de host de la subred LAN2<br><br>Int g0/0/0<br>Ip address 172.26.3.94 255.255.255.224 |

|        |  |
|--------|--|
| S1 SVI | Segunda dirección de host de la subred LAN1<br><br>Int vlan 1<br>Ip address 172.26.3.2 255.255.255.192 |
| PC-A   | Décima dirección de host de la subred LAN1<br><br>IP: 172.26.3.10<br>Mask: 255.255.255.192             |
| PC-B   | Décima dirección de host de la subred LAN2<br><br>IP: 172.26.3.74<br>Mask: 255.255.255.224             |

Fuente: Autoría Propia

#### 1.4. PARTE 3: Configure aspectos básicos

##### 1.4.1. Paso 1: configurar los ajustes básicos

Como siguiente paso se procede a realizar la configuración básica de R1 con el fin de agregar seguridad al mismo y poder configurar sus interfaces, de igual forma se configurarán varios parámetros necesarios para el desarrollo de la actividad dentro de los cuales encontraremos las siguientes: Nombre del router, Desactivar la búsqueda DNS, Nombre de dominio, asignación de contraseñas con sus respectivos cifrados, configuración de Baners, etc; El proceso es indicado a continuación. Ver tabla No 3.

Tabla 3 configuración básica R1.

| Tarea  | Especificación   |
|--|--|
| Desactivar la búsqueda DNS   | <p>Procedemos a desactivar la búsqueda DNS aplicando el siguiente comando en el router R1.</p> <p>No ip domain lookup</p>  |
| Nombre del router  | <p>Agregamos el nombre al dispositivo con el fin de poderlo identificar de una manera sencilla</p> <p>hostname R1</p>  |
| Nombre de dominio  | <p>ccna-sa.com</p> <p>ip domain-name ccna-sa.com</p>   |
| Contraseña cifrada para el modo EXEC privilegiado                                    | <p>Debemos cifrar nuestras contraseñas:</p> <p>Ciscoenpass</p> <p>enable secret ciscoenpass</p>  |
| Contraseña de acceso a la consola  | <p>Procedemos a configurar nuestras líneas de consola empleando la contraseña:</p> <p>Ciscoconpass</p> <p>line console 0<br/>password ciscoconpass<br/>login</p> |
| Establecer la longitud mínima para las contraseñas                                   | <p>Establecemos una condición con el fin de que el tamaño mínimo de las contraseñas sea de 10 caracteres:</p> <p>security password min-length 10</p>             |
| Crear un usuario administrativo en la base de datos local                            | <p>Nombre de usuario: <b>admin</b><br/>Password: <b>admin1pass</b></p> <p>username admin secret admin1pass</p>   |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | <p>Procedemos a configurar las líneas vty 0 15</p> <p>line vty 0 15<br/>login local</p>  |
| Configurar VTY solo aceptando SSH  | <p>transport input ssh<br/>login</p>   |
| Cifrar las contraseñas de texto no cifrado   | <p>De esta manera logramos que las contraseñas permanezcan encriptadas y que permanezcan ocultas.</p>  |

|                                  |   |
|----------------------------------|---|
|                                  | Service password-encryption   |
| Configure un MOTD Banner         | Este mensaje aparece cada vez que ingresamos a un dispositivo, es un mensaje persuasivo.<br><br>banner motd % Se prohíbe el acceso no autorizado.%                      |
| Configurar interfaz G0/0/0       | Establezca la descripción Establece la dirección IPv4.<br>Activar la interfaz.<br><br>Config t<br>Int g0/0/0<br>Ip address 172.26.3.94 255.255.255.224                  |
| Configurar interfaz G0/0/1       | Establezca la descripción Establece la dirección IPv4.<br>Activar la interfaz.<br><br>Configure terminal<br>Interface g0/0/01<br>Ip address 172.26.3.62 255.255.255.192 |
| Generar una clave de cifrado RSA | Modulo de 1024 bits<br><br>crypto key generate rsa general-keys modulus 1024  |

Fuente: Autoría Propia

1.4.2. Paso 2: Verificamos a ingresar la configuración del dispositivo tal como se muestra a continuación:

|  |   |
|--|---|
| Router(config)#hostname R1                 | Asigno nombre al Router                           |
| R1(config)#no ip domain-lookup             | Se desactiva Búsqueda DNS                         |
| R1(config)#ip domain-name ccna-sa.com      | Se asigna nombre dominio                          |
| R1(config)#enable secret ciscoenpass       | Se configura contraseña modo privilegiado         |
| R1(config)#line console 0                  | Ingreso a la línea de consola                     |
| R1(config-line)#password ciscoconpass      | Asignación de contraseña para acceso a la consola |
| R1(config-line)#login                      | Habilitación de contraseña, autenticación local   |
| R1(config-line)#exit                       | Se retrocede                                      |
| R1(config)#security password min-length 10 | Asignación longitud mínima para la contraseña     |
| R1(config)#username admin secret           | Se crea usuario y se asigna                       |

|   |  |
|---|--|
| admin1pass  | contraseña                                     |
| R1(config)#line vty 0 15  | Sesión línea vty uso de la base de datos       |
| R1(config-line)#login local   | Autenticación local                            |
| R1(config-line)#transport input ssh                                   | Configuración vty aceptando solo protocolo ssh |
| R1(config-line)#exit  | Se retrocede                                   |
| R1(config)#   |  |
| R1(config)#service password-encryption                                | Se cifran las contraseñas de texto no cifradas |
| R1(config)#banner motd %R1 Hector Maldonado – Ingeniería de Sistemas% | Configuración banner Bienvenida                |

R1(config)#do wr

Procedemos a realizar la configuración de las interfaces de este dispositivo:

|  |   |
|--|---|
| R1(config)#int g0/0/1  | Se configura la interfaz g0/0/1                                 |
| R1(config-if)#ip address 172.26.3.62 255.255.255.192         | Se configura la IPv4 172.26.3.62 255.255.255.192 con su mascara |
| R1(config-if)#no shutdown                                    | Activar una interfaz del router                                 |
| R1(config-if)#   |   |
| R1(config-if)#int g0/0/0                                     | Se configura la interfaz g0/0/0                                 |
| R1(config-if)#ip address 172.26.3.94 255.255.255.224         | Se configura la IPv4 172.26.3.94 255.255.255.224 con su mascara |
| R1(config-if)#no shutdown                                    | Activar una interfaz del router                                 |
| R1(config-if)#   |   |
| R1(config)#crypto key generate rsa general-keys modulus 1024 | Se genera clave de cifrado RSA                                  |

*Figura 4 Configuración total del dispositivo R1*

```

R1(config)#no ip domain lookup
R1(config)#hostname R1
R1(config)#ip domain-name ccna-sa.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#security password min-length 10
R1(config)#username admin secret adminlpass
R1(config)#
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#
R1(config-line)#service password-encryption
R1(config)#banner motd %prohibido el acceso no autorizado%
R1(config)#
R1(config)#int g0/0/1
R1(config-if)#ip address 172.26.3.62 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#int g0/0/0
R1(config-if)#ip address 172.26.3.94 255.255.255.224
R1(config-if)#no shutdown

```

Fuente: Autoría Propia

#### 1.4.3. Paso 3: Las tareas de configuración de Swich S1.

La configuración del dispositivo de interconexión incluye lo siguiente:

*Tabla 4 Configuración básica S1.*

| <b>Tarea</b>                | <b>Especificación</b>  |
|-----------------------------|--|
| Desactivar la búsqueda DNS. | Debemos desactivar la búsqueda DNS de esta manera ahorramos recursos:<br><br>No ip domain lookup   |
| Nombre del switch           | Agregamos el nombre a nuestro dispositivo S1 con el fin de poderlo identificar, por lo general en redes más grandes se emplean nombres más extensos para identificarlos con seguridad. |

|  |   |
|--|---|
|  | hostname S1   |
| Nombre de dominio  | ccna-sa.com<br>ip domain-name ccna-sa.com   |
| Contraseña cifrada para el modo EXEC privilegiado                                    | Creamos la contraseña de EXEC privilegiado y la ciframos Ciscoenpass<br>enable secret ciscoenpass   |
| Contraseña de acceso a la consola  | Ciscoconpass<br>line console 0<br>password ciscoconpass<br>login  |
| Crear un usuario administrativo en la base de datos local                            | Nombre de usuario: admin<br>Password: admin1pass<br>username admin secret admin1pass  |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | line vty 0 15<br>login local  |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH             | transport input ssh   |
| Cifrar las contraseñas de texto no cifrado   | Este comando nos sirve para cifrar todas las contraseñas que aún no lo han hecho.<br>Service password-encryption  |
| Configurar un MOTD Banner  | Configuramos el mensaje que aparece en el dispositivo cuando ingresamos al mismo:<br>banner motd % Se prohíbe el acceso no autorizado.%                     |
| Generar una clave de cifrado RSA   | Módulo de 1024 bits<br>crypto key generate rsa general-keys modulus 1024  |
| Configurar la interfaz de administración (SVI)                                       | Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento<br>int vlan 1<br>description subnet A<br>ip address 172.26.3.2 255.255.255.192 |

|  |   |
|--|---|
| Configuración del gateway predeterminado | Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.<br><br>ip default-gateway 172.26.3.62 |
|--|---|

Fuente: Autoría Propia

#### 1.4.4. Paso 4: Procedimiento configuración básica del dispositivo Switch S1.

Como se indica en la tabla anterior:

|  |  |
|--|--|
| Switch(config)#hostname S1                                   | Se asigna nombre al switch                     |
| S1(config)#no ip domain-lookup                               | Se desactiva búsqueda DNS                      |
| S1(config)#ip domain-name ccna-sa.com                        | Asignación nombre de dominio                   |
| S1(config)#enable secret ciscoenpass                         | Configuración contraseña modo privilegiado     |
| S1(config)#line console 0                                    | Ingreso a la línea de consola                  |
| S1(config-line)#password ciscoconpass                        | Se asigna contraseña de acceso a consola       |
| S1(config-line)#login  | Habilitar contraseña, se autentica en local    |
| S1(config-line)#exit   | Se regresa un paso                             |
| S1(config)#username admin secret admin1pass                  | Se crea usuario y se asigna contraseña         |
| S1(config)#line vty 0 15                                     | Se inicia sección para utilizar base de datos  |
| S1(config-line)#login local                                  | Se autentica localmente                        |
| S1(config-line)#transport input ssh                          | Solo acepta protocolo ssh                      |
| S1(config)#service password-encryption                       | Se cifran las contraseñas en texto no cifradas |
| S1(config)#banner motd %prohibido acceso sin autorizacin%    | Banner de acceso restringido                   |
| S1(config)#crypto key generate rsa general-keys modulus 1024 | Se genera clave de cifrado rsa                 |

#### 1.1.1 Paso 5: Procedimiento configuración interfaces del S1:

|   |  |
|---|--|
| S1(config)#int vlan 1                               | Se Configura la interfaz de administración         |
| S1(config-if)#description subnetA                   | Descripción de la subred                           |
| S1(config-if)#ip address 172.26.3.2 255.255.255.192 | Asignación de dirección IPv4 con su mascara de red |
| S1(config-if)#ip default-gateway 172.26.3.62        | Configuración del Gateway determinado              |
| S1(config)#do wr                                    |  |

*Figura 5 Configuración total del dispositivo S1*

```
S1(config)#
S1(config)#no ip domain-lookup
S1(config)#hostname S1
S1(config)#ip domain-name ccna-sa.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#int range g1/0/1-4
interface range not validated - command rejected
S1(config)#username admin secret adminlpass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#service password-encryption
S1(config)#banner motd %prohibido acceso sin autorizacin%
S1(config)#int vlan 1
S1(config-if)#description subnet A
S1(config-if)#ip address 172.26.3.2 255.255.255.192
S1(config-if)#ip default-gateway 172.26.3.62
S1(config)#no shutdown
```

Fuente: Autoría Propia

#### 1.4.5. Paso 5: Configurar los equipos PC.

Inicialmente se debe configurar los equipos host PC-A y PC-B, basados en las tablas de direccionamiento proporcionadas, de igual forma se deben realizar pruebas con el comando ipconfig /all.

##### 1.4.5.1. Configuración PC A

Para realizar la respectiva configuración del computador A, debemos entrar a la interfaz de Packet Tracer y se selecciona el aparte Desktop, posterior de ingresa al icono de configuración IP y se asignan las diferentes direcciones IPv4 y demás descritos en la tabla 5.

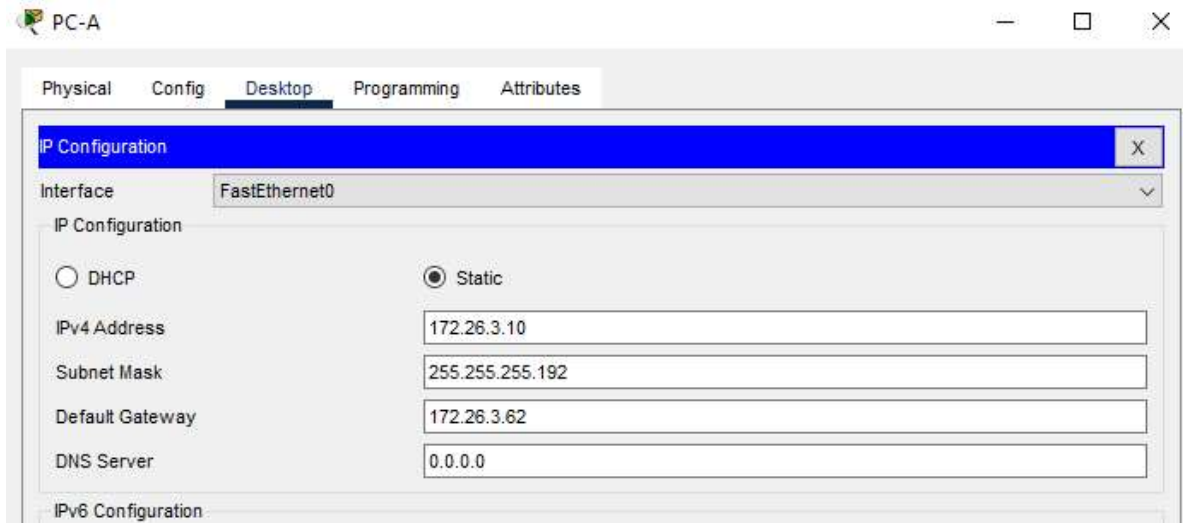
*Tabla 5 Configuración PC-A.*

| PC-A Network Configuration |                |
|----------------------------|----------------|
| Descripción                | PC-A           |
| Dirección física           | 0006 2A38 082B |
| Dirección IP               | 172.26.3.10    |

|                        |                 |
|------------------------|-----------------|
| Máscara de subred      | 255.255.255.192 |
| Gateway predeterminado | 172.26.3.62     |

Fuente: Autoría Propia

*Figura 6 Configuración PC-A*



Fuente: Autoría Propia

#### 1.4.5.2. Configuración PC-B

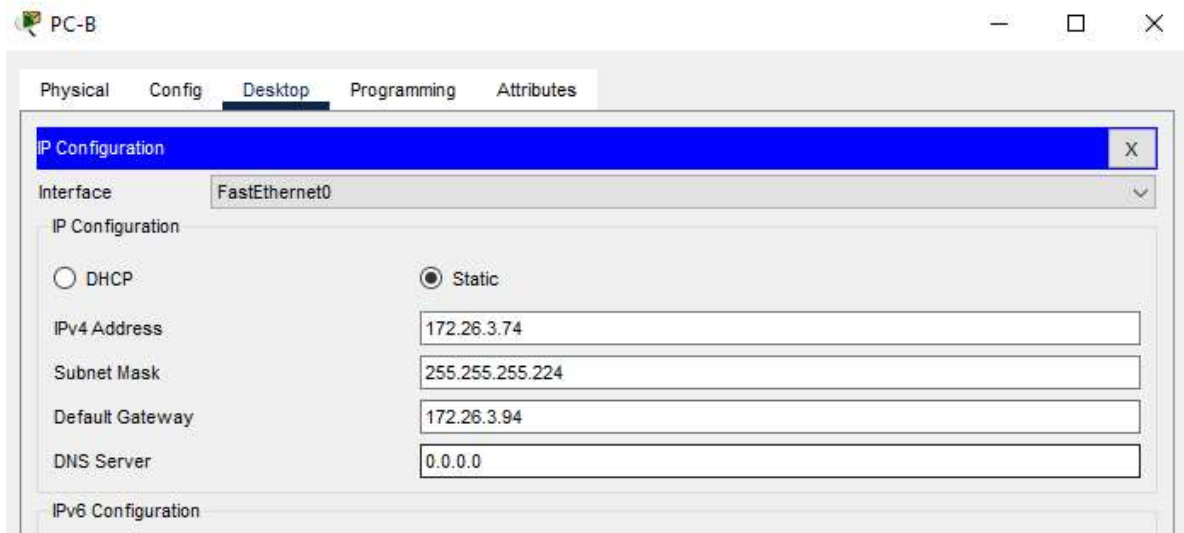
Para realizar la respectiva configuración del computador B, debemos entrar a la interfaz de Packet Tracer y se selecciona el aparte Desktop, posterior de ingresa al icono de configuración IP y se asignan las diferentes direcciones IPv4 y demás descritos en la tabla 6.

*Tabla 6 Configuración PC-B*

| <b>PC-B Network Configuration</b> |                 |
|-----------------------------------|-----------------|
| Descripción                       | PC-B            |
| Dirección física                  | 00E0 8FEC 9189  |
| Dirección IP                      | 172.26.3.74     |
| Máscara de subred                 | 255.255.255.224 |
| Gateway predeterminado            | 172.26.3.94     |

Fuente: Autoría Propia

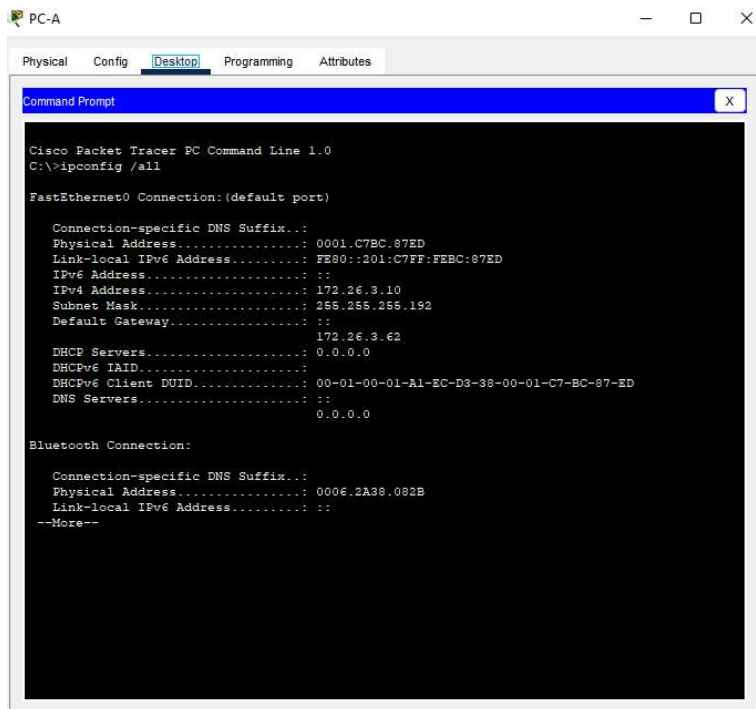
Figura 7 Configuración PC-B



Fuente: Autoría Propia

En el simulador ingresamos al aparte configuración – terminal, para poder desplegar el comando ipconfig /all para obtener la información referenciada en la figura 8.

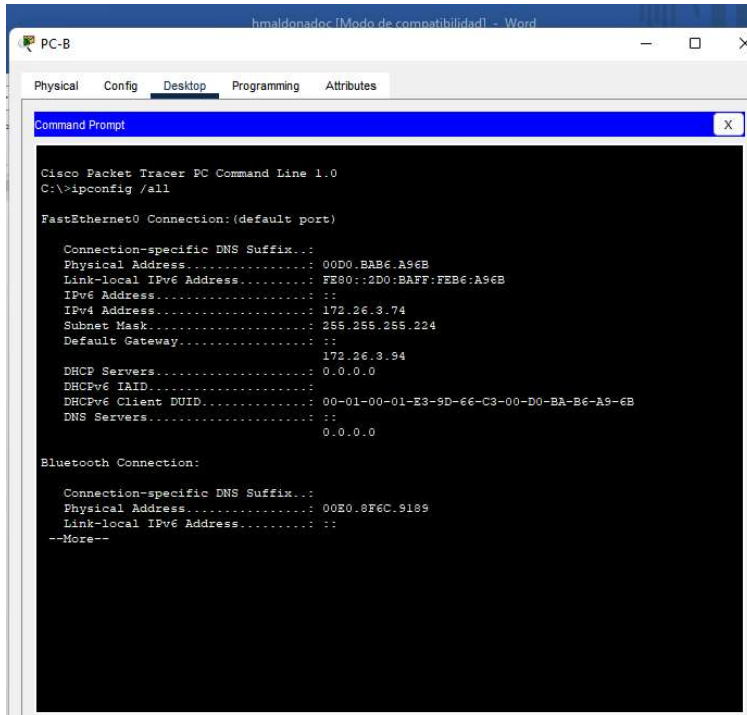
Figura 8 Dirección Mac PC-A- Comando ipconfig /all



Fuente: Autoría Propia

De igual forma ingresamos al simulador al aparte configuración – comand pront, para poder desplegar el comando ipconfig para obtener la información referenciada en la figura 9.

*Figura 9 Dirección Mac PC-B - Comando ipconfig /all*



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

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix... :
Physical Address. . . . . : 00D0.BAB6.A96B
Link-local IPv6 Address . . . . . : FE80::2D0:BAFF:FEB6:A96B
IPv6 Address. . . . . :
IPv4 Address. . . . . : 172.26.3.74
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . :
DHCP Servers. . . . . : 172.26.3.94
DHCPv6 IAID. . . . . : 0.0.0.0
DHCPv6 Client DUID. . . . . : 00-01-00-01-E3-9D-66-C3-00-D0-BA-B6-A9-6B
DNS Servers. . . . . :
0.0.0.0

Bluetooth Connection:

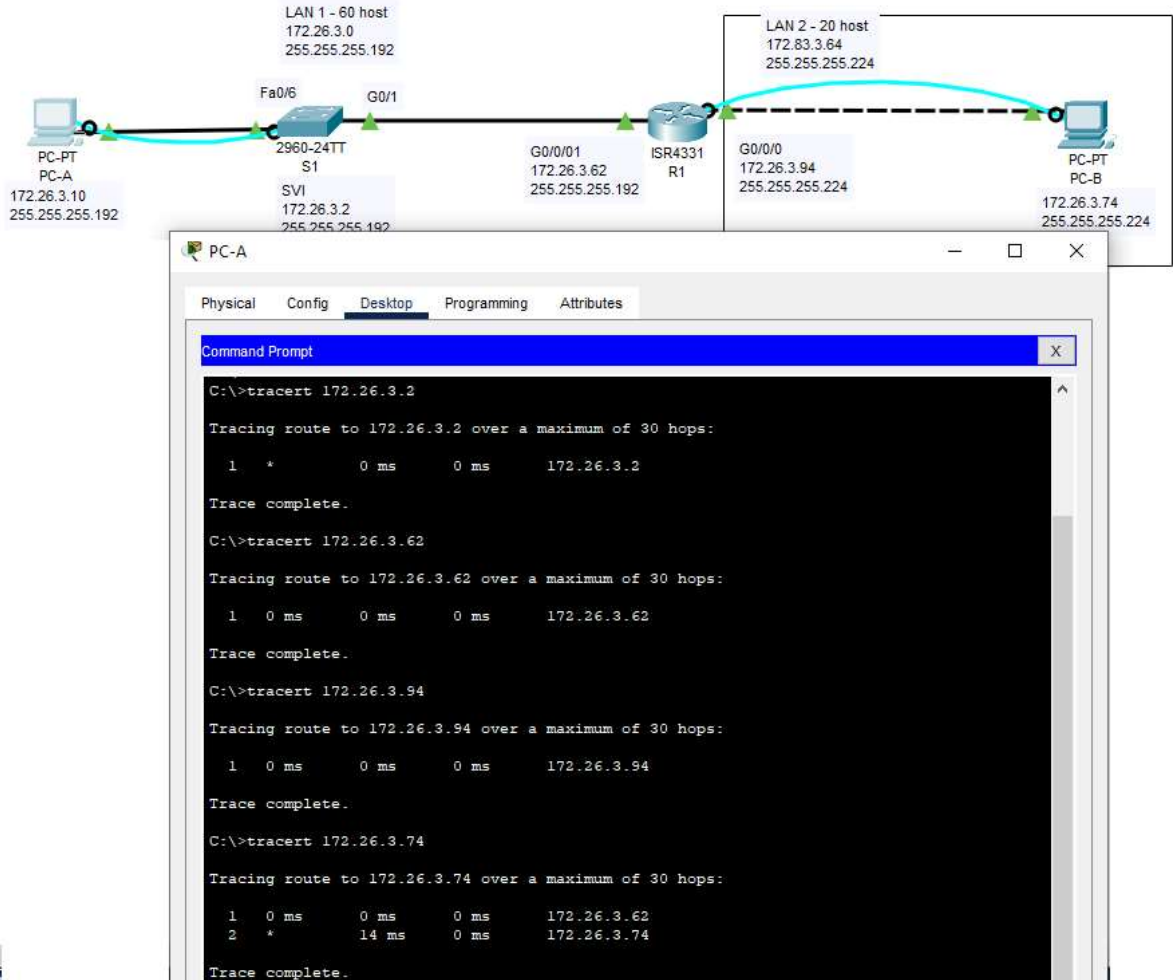
Connection-specific DNS Suffix... :
Physical Address. . . . . : 00E0.8F6C.9189
Link-local IPv6 Address. . . . . :
--More--
```

Fuente: Autoría Propia

### 1.4.5.3. Pruebas de conectividad entre dispositivos.

- Desde PCA hacia los diferentes puertos de la red.

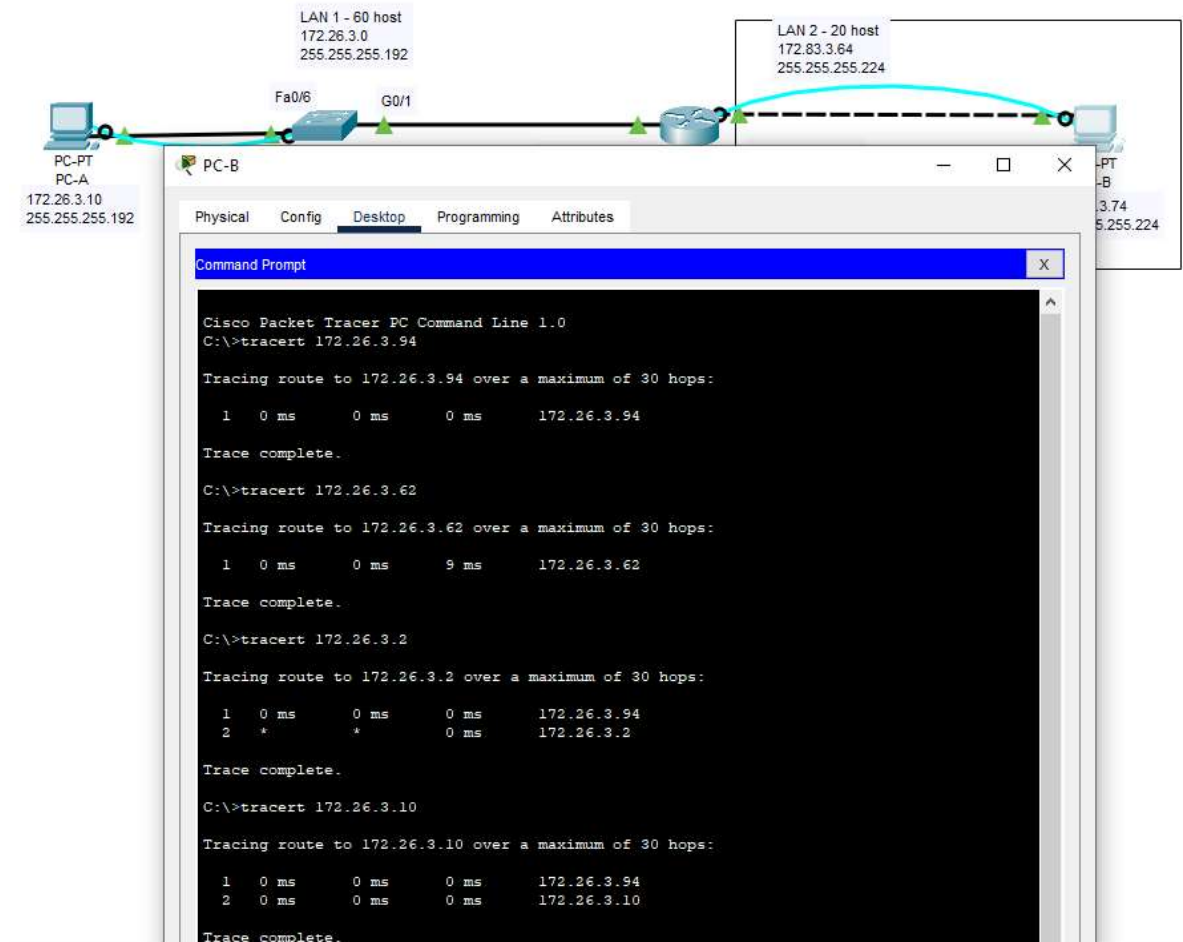
Figura 10 Comando *tracert* – desde PCA Verificando Conectividad entre dispositivos



Fuente: Autoría Propia

Procedemos a realizar la verificación de lo hecho hasta el momento, para nuestro caso vamos a emplear el comando PING desde PCB hacia los diferentes puntos de la red.

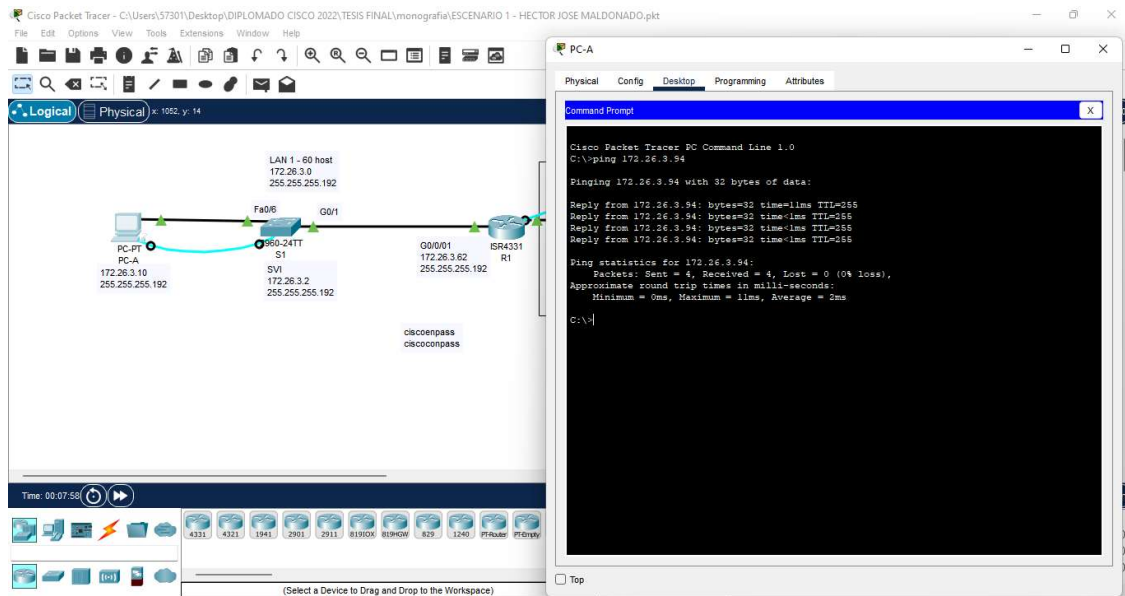
Figura 11 Comando *tracert* – desde PCB Verificando Conectividad entre dispositivos



Fuente: Autoría Propia

Se despliega el comando ping para verificar conectividad entre los siguientes dispositivos desde PCA 172.26.3.10 A G/0/0/0 172.26.3.94

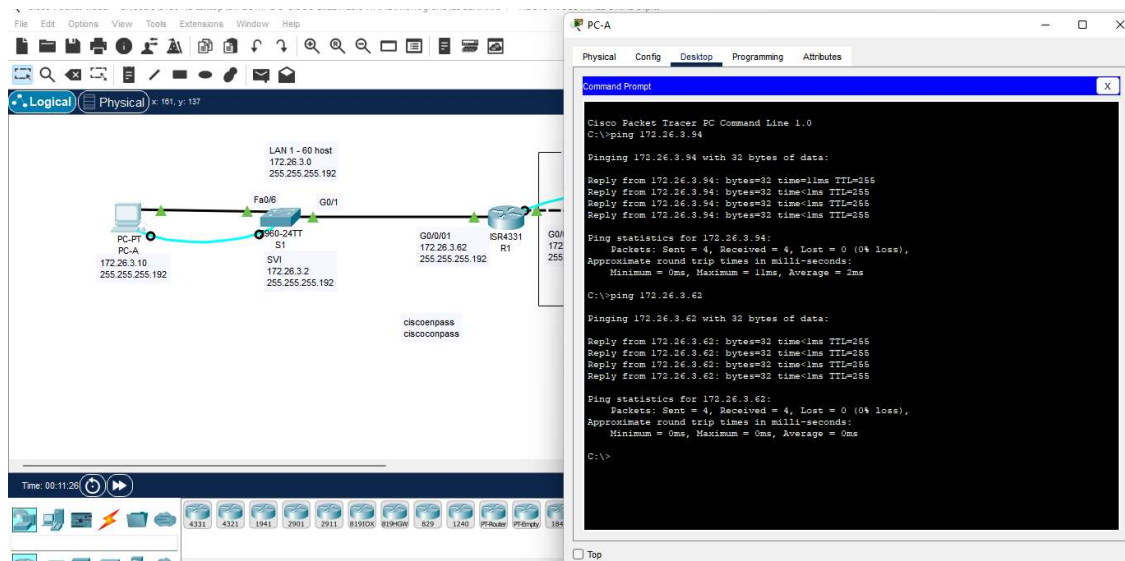
Figura 12 Prueba Conectividad desde PCA 172.26.3.10 A G/0/0/0 172.26.3.94



Fuente: Autoría Propia

Se despliega el comando ping para verificar conectividad entre los siguientes dispositivos desde PCA 172.26.3.10 A G/0/0/1 172.26.3.94

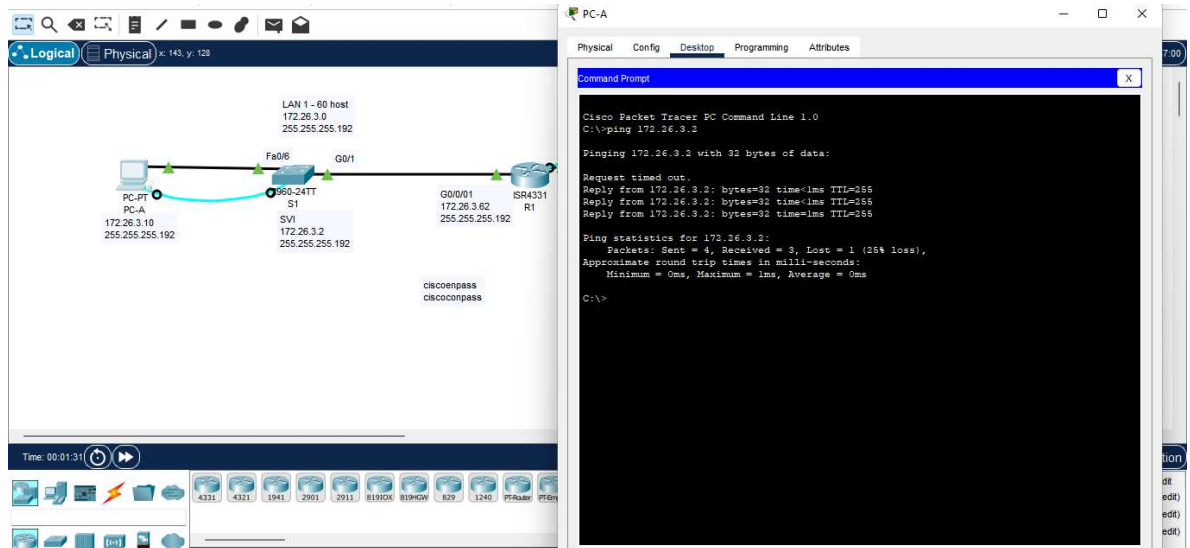
Figura 13 Prueba Conectividad desde PCA 172.26.3.10 A G/0/0/1 172.26.3.94



Fuente: Autoría Propia

Se despliega el comando ping para verificar conectividad entre los siguientes dispositivos desde PCA 172.26.3.10 A s1 vlan 1 172.26.3.2

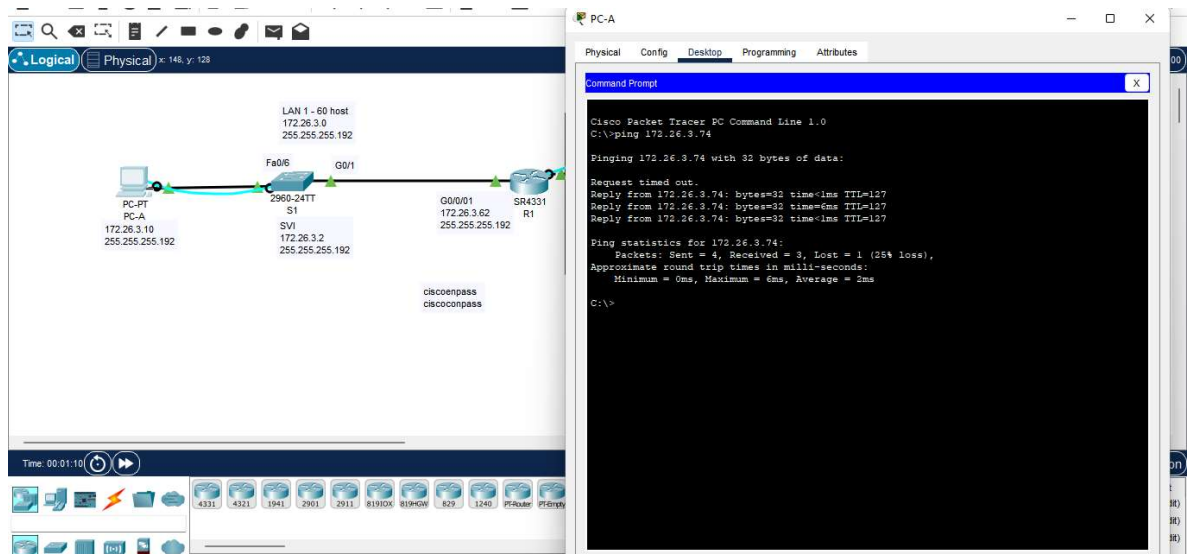
Figura 14 Prueba Conectividad desde PCA 172.26.3.10 A s1 vlan 1 172.26.3.2



Fuente: Autoría Propia

Se despliega el comando ping para verificar conectividad entre los siguientes dispositivos desde PCA 172.26.3.10 A PCB 172.26.3.2

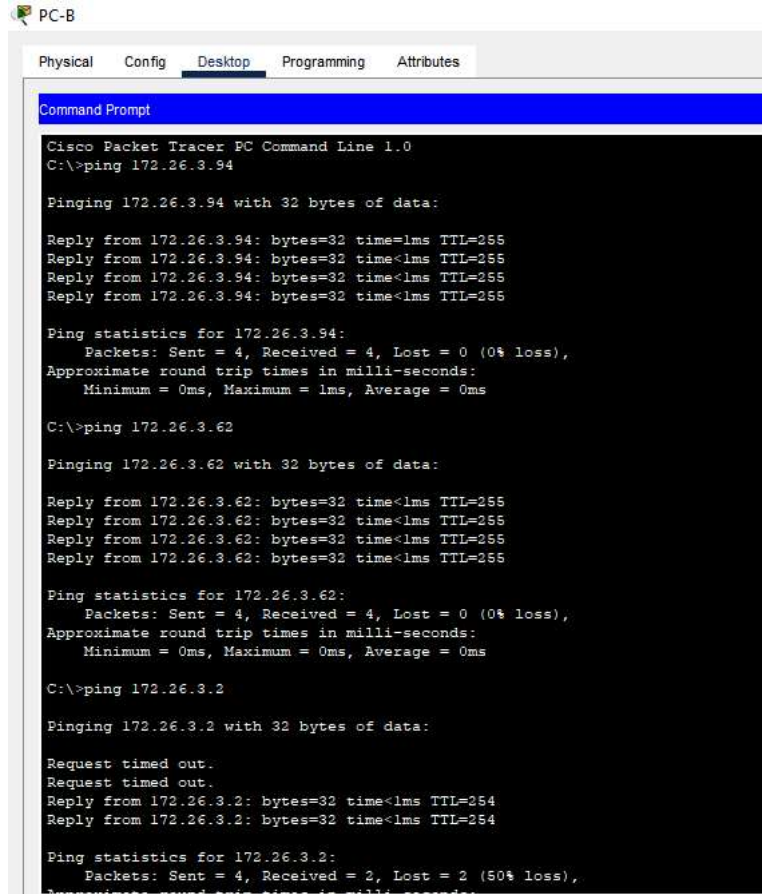
Figura 15 Prueba Conectividad desde PCA 172.26.3.10 A PCB 172.26.3.2



Fuente: Autoría Propia

Se despliega el comando ping para verificar conectividad entre los siguientes dispositivos desde PCB 172.26.3.74 Hacia G0/0/0 172.26.3.94 - G0/0/1 172.26.3.62 – S1 VLAN1 172.26.3.2

Figura 16 Prueba Conectividad desde PCB 172.26.3.74 Hacia G0/0/0 172.26.3.94 - G0/0/1 172.26.3.62 – S1 VLAN1 172.26.3.2



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.26.3.94

Pinging 172.26.3.94 with 32 bytes of data:

Reply from 172.26.3.94: bytes=32 time<1ms TTL=255
Reply from 172.26.3.94: bytes=32 time<1ms TTL=255
Reply from 172.26.3.94: bytes=32 time<1ms TTL=255
Reply from 172.26.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.26.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.26.3.62

Pinging 172.26.3.62 with 32 bytes of data:

Reply from 172.26.3.62: bytes=32 time<1ms TTL=255
Reply from 172.26.3.62: bytes=32 time<1ms TTL=255
Reply from 172.26.3.62: bytes=32 time<1ms TTL=255
Reply from 172.26.3.62: bytes=32 time<1ms TTL=255

Ping statistics for 172.26.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.26.3.2

Pinging 172.26.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 172.26.3.2: bytes=32 time<1ms TTL=254
Reply from 172.26.3.2: bytes=32 time<1ms TTL=254

Ping statistics for 172.26.3.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
```

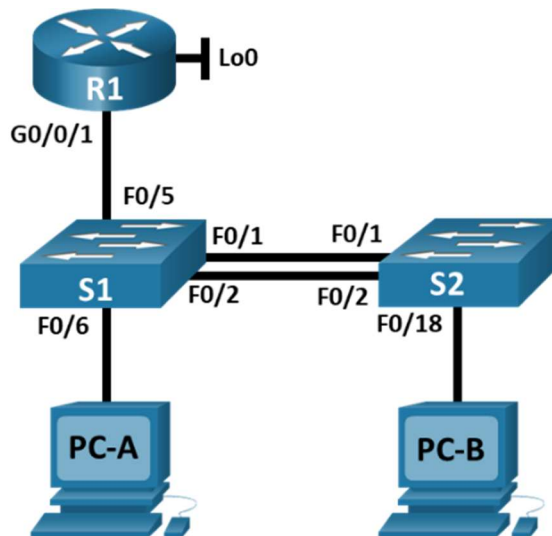
Fuente: Autoría Propia

## 2. DESARROLLO ESCENARIO 2

Para este escenario corresponde configurar los respectivos dispositivos de una red pequeña, conformados por 01 router, 02 swiche y 02 computadores. De igual forma se deben configurar tanto para conectividad IPv4 como IPv6, permitiendo a los equipos estar conectados en todo tiempo. Así mismo se deben administrar de manera segura, para no permitir vulneraciones de seguridad para la red propuesta. Ver figura 17.

### 2.1 Topología

*Figura 17 Topología de red escenario 2*

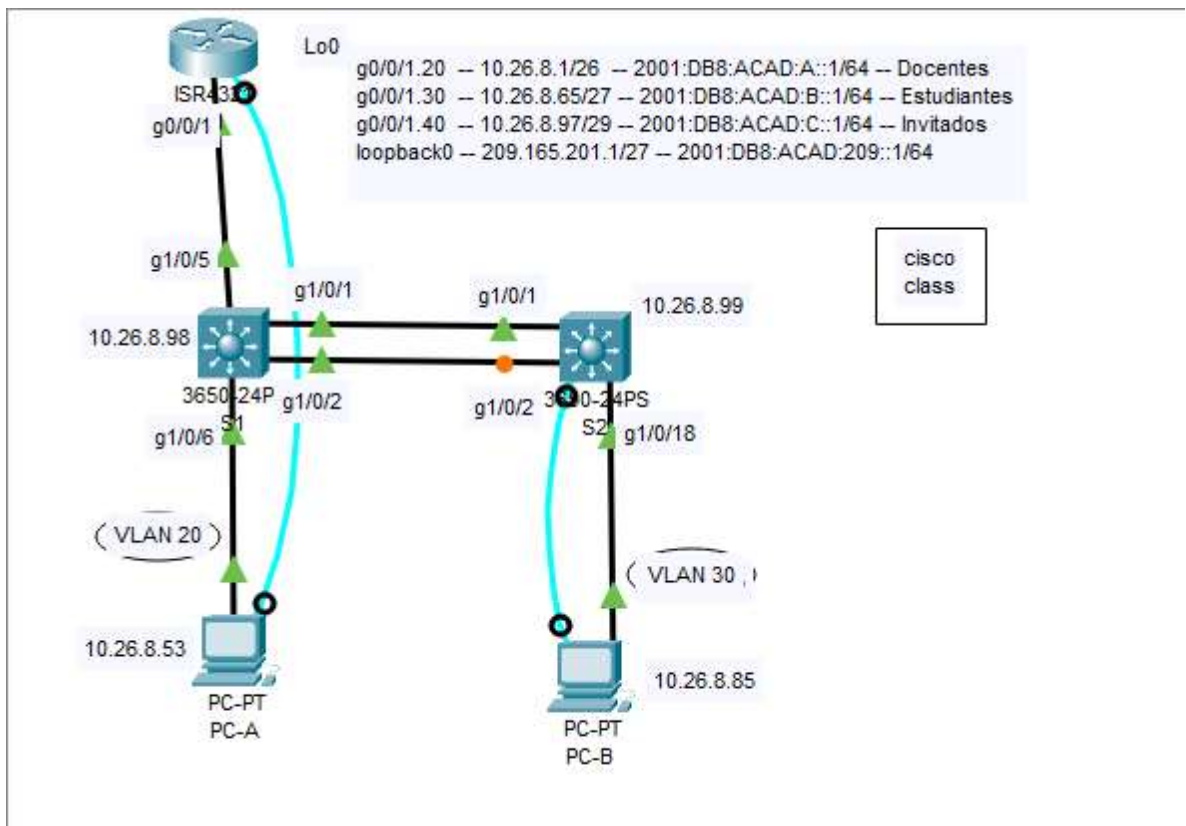


Fuente: Prueba de habilidades diplomado CCNA.

Creación de la Topología lógica de red.

En este aparte se crea la topología de la red lógica, se configuran los aspectos básicos solicitados para el escenario 2, todo este montaje se realiza en el simulador, programa de gran utilidad para realizar el respectivo cableado de los diferentes dispositivos que interactúan en la red. De igual manera nos permitirá realizar los direccionamientos IPv4 e IPv6. Ver Figura 18.

Figura 18 Montaje en Packet Tracer escenario 2



Fuente: Autoría Propia

Tabla 7 VLAN Escenario 2

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

Fuente Autoría propia.

Tabla 8 Tabla asignación de direcciones escenario 2

| Dispositivo / interfaz                            | Dirección IP / Prefijo    | Puerta de enlace predeterminada                |
|---|---------------------------|--|
| R1 G0/0/1.20                                      | 10.26.8.1 /26             | No corresponde                                 |
|   | 2001:db8:acad:a: :1 /64   | No corresponde                                 |
| R1 G0/0/1.30<br><i>R1 G0/0/1.3</i>                | 10.26.8.65 /27            | No corresponde                                 |
|   | 2001:db8:acad:b: :1 /64   | No corresponde                                 |
| R1 G0/0/1.40                                      | 10.26.8.97 /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 4<br><i>VLAN S1 4</i><br><i>S1 VLAN 4</i> | 10.26.8.98 /29            | 10.26.8.97                                     |
|   | 2001:db8:acad:c: :98 /64  | No corresponde                                 |
|   | fe80: :98                 | No corresponde                                 |
| S2 VLAN 4   | 10.26.8.99 /29            | 10.26.8.97                                     |
|   | 2001:db8:acad:c: :99 /64  | No corresponde                                 |
|   | fe80: :99                 | No corresponde                                 |
| PC-A NIC<br><i>PC-A NIC</i>                       | Dirección DHCP para IPv4  | DHCP para puerta de enlace predeterminada IPv4 |
|   | 2001:db8:acad:a: :50 /64  | fe80::1  |
| PC-B NIC  | DHCP para dirección IPv4  | DHCP para puerta de enlace predeterminada IPv4 |
|   | 2001:db8:acad:b: :50 /64  | fe80::1  |

Fuente: Prueba de habilidades CCNA, Cisco Academy.

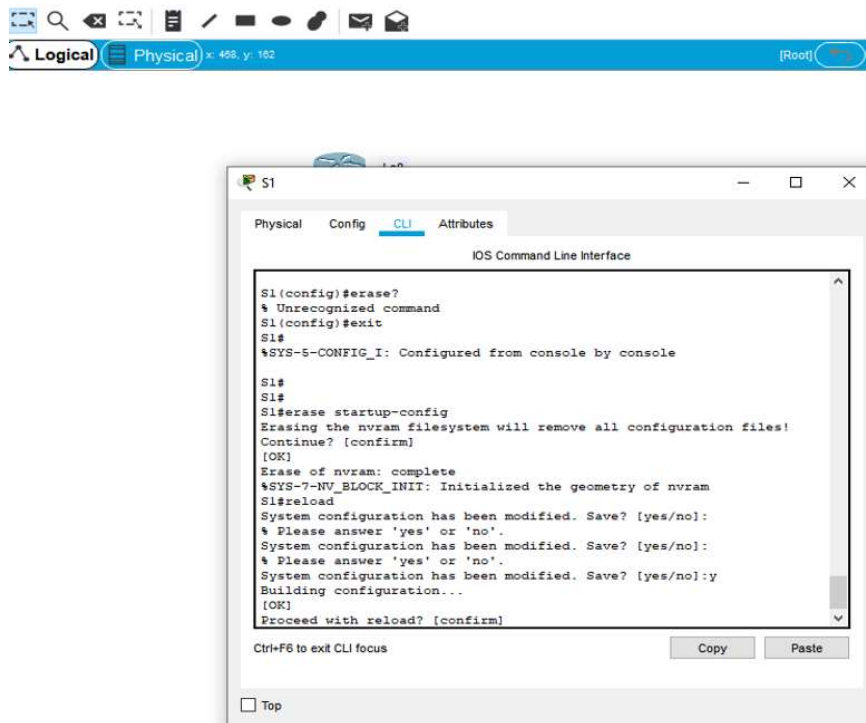
## 2.2 PARTE 1: Iniciación de dispositivos.

### 2.2.1 Paso 1: Inicializar y cargar los Router y los Switches.

Para la eliminación de la configuración de los switches, ingresamos al sistema operativo de cada equipo para iniciar los respectivos procedimientos, mediante comandos utilizados para cada tarea. Para nuestro caso el comando descrito lo debemos ejecutar en los 2 switches:

```
Switch>enable (accedemos al modo privilegiado)  
Switch# erase startup-config (borramos la config de los Switch)  
Switch# Reload (Vuelve a cargar el Switch)  
Switch# config t (Ingresa nuevamente al modo configuración)  
Switch (config) # sdm prefer dual-ipv4-and-ipv6 default (habilitamos las  
características IPV6)  
Switch (config) # exit  
Switch# Reload (Reiniciamos)
```

Figura 19 Reinicio de Switches



Fuente: Autoría propia

### 2.2.2 Paso 2: Configuración R1

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 9 Configuración básica ROUTER 1 – nombre, dominios, contraseñas.*

| Tarea  | Especificación  |
|--|---|
| Desactivar la búsqueda DNS   | <i>no ip domain-lookup</i>  |
| Nombre del Router  | R1<br><i>hostname R1</i>  |
| Nombre de dominio  | <i>ccna-sa.com</i><br><i>ip domain-name ccna-sa.com</i>                                     |
| Contraseña cifrada para el modo EXEC privilegiado                                    | Class<br><i>enable secret class</i>   |
| Contraseña de acceso a la consola  | cisco<br><i>line con 0</i><br><i>password cisco</i><br><i>login</i>                         |
| Establecer la longitud mínima para las contraseñas                                   | 5 caracteres<br><i>security passwords min-length 5</i>                                      |
| Crear un usuario administrativo en la base de datos local                            | Nombre de usuario: admin<br>Password: admin1pass<br><i>username admin secret admin1pass</i> |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | <i>line vty 0 4</i><br><i>login local</i>   |

*Fuente: Autoría propia*

*Tabla 10 Continuación configuración básica ROUTER 1*

| Tarea                                      | Especificación  |
|--|---|
| Cifrar las contraseñas de texto no cifrado | <i>service password-encryption</i>  |
| Configurar VTY solo aceptando SSH          | <i>line vty 0 4<br/>transport input ssh</i>   |
| Configure un MOTD Banner                   | <p>Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> <pre><i>banner motd &amp; Router R1 HECTOR JOSE MALDONADO Código: 72'213.126 INGENIERIA DE SISTEMAS 203092_10 &amp;</i></pre> |
| Habilitar el routing IPv6                  | <i>ipv6 unicast-routing</i>   |

*Fuente: Autoría propia*

Tabla 11 Configuración interfaces R1

|   |   |
|---|---|
| <p>Configurar interfaz G0/0/1 y subinterfaces</p> | <p>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.</p> <pre> interface GigabitEthernet0/0/1.20 description Docentes encapsulation dot1Q 20 ip address 10.26.8.1 255.255.255.192 ipv6 address FE80::1 link-local ipv6 address 2001:DB8:ACAD:A::1/64  interface GigabitEthernet0/0/1.30 description Estudiantes encapsulation dot1Q 30 ip address 10.26.8.65 255.255.255.224 ipv6 address FE80::1 link-local ipv6 address 2001:DB8:ACAD:B::1/64  interface GigabitEthernet0/0/1.40 description Invitados encapsulation dot1Q 40 ip address 10.26.8.97 255.255.255.248 ipv6 address FE80::1 link-local ipv6 address 2001:DB8:ACAD:C::1/64  interface GigabitEthernet0/0/1.56 description Native encapsulation dot1Q 56 native no ip address  interface GigabitEthernet0/0/1 no shutdown </pre> |
|---|---|

|                                  |   |
|----------------------------------|---|
| Configure el Loopback0 interface | <p>Establezca la descripción<br/> Establece la dirección IPv4.<br/> Establece la dirección IPv6.<br/> Establezca la dirección local de enlace IPv6 como fe80::1</p> <pre>interface Loopback0 description INTERNET ip address 209.165.201.1 255.255.255.224 ipv6 address FE80::1 link-local ipv6 address 2001:DB8:ACAD:209::1/64</pre> |
| Generar una clave de cifrado RSA | <p>Módulo de 1024 bits</p> <pre>crypto key generate rsa general-keys modulus 1024</pre>   |

*Fuente: Autoría propia*

### 2.2.3 Paso 3 Configuración S1 y S2.

Las tareas de configuración incluyen lo siguiente:

*Tabla 12 configuración básica del S1 y S2 – contraseñas y VLAN.*

| Tarea                       | Especificación   |
|-----------------------------|--|
| Desactivar la búsqueda DNS. | <i>no ip domain-lookup</i>   |
| Nombre del switch           | S1 o S2, según proceda<br><br><i>hostname S1</i><br><i>hostname S2</i> |
| Nombre de dominio           | <i>ccna-sa.com</i><br><br><i>ip domain-name ccna-sa.com</i>            |

*Fuente: Autoría propia*

Tabla 13 Continuación configuración básica del S1 y S2

| Tarea  | Especificación   |
|--|--|
| Contraseña cifrada para el modo EXEC privilegiado                                    | <i>username admin secret class</i>   |
| Contraseña de acceso a la consola  | <i>cisco</i><br><br><i>line con 0</i><br><i>password cisco</i><br><i>login</i>   |
| Crear un usuario administrativo en la base de datos local                            | Nombre de usuario: admin<br>Password: admin1pass<br><br><i>username admin secret admin1pass</i>  |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | <i>line vty 0 4</i><br><i>login local</i>  |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH             | <i>line vty 0 4</i><br><i>transport input ssh</i>  |
| Cifrar las contraseñas de texto no cifrado   | <i>service password-encryption</i>   |
| Configurar un MOTD Banner  | <i>banner motd &amp;</i><br><i>Router R1</i><br><i>HECTOR JOSE MALDONADO</i><br><i>Código: 72'213.126</i><br><i>INGENIERIA DE SISTEMAS</i><br><i>203092_10</i><br><i>&amp;</i> |
| Generar una clave de cifrado RSA   | Módulo de 1024 bits<br><br><i>crypto key generate rsa general-keys modulus 1024</i>  |

|   |  |
|---|--|
| <p>Configurar la interfaz de administración (SVI)</p> | <p>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</p> <pre> interface Vlan40 description INTERFACE ADMINISTRACIÓN ip address 10.26.8.98 255.255.255.248 ipv6 address FE80::98 link-local ipv6 address 2001:DB8:ACAD:C::98/64 no shutdown  interface Vlan40 description INTERFACE ADMINISTRACIÓN ip address 10.26.8.99 255.255.255.248 ipv6 address FE80::99 link-local ipv6 address 2001:DB8:ACAD:C::99/64 no shutdown </pre> |
| <p>Configuración del gateway predeterminado</p>       | <p>Configure la puerta de enlace predeterminada como 10.26.8.97 para IPv4</p> <pre> ip default-gateway 10.26.8.97 </pre>   |

*Fuente: Autoría propia*

## 2.2.4 Parte 4: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

### 2.2.4.1 Paso 1 Configurar S1

La configuración del S1 incluye las siguientes tareas:

*Tabla 14 creación de VLAN – S1*

| <b>Tarea</b>  | <b>Especificación</b>  |
|---|--|
| 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<br><br>vlan 20<br>name Docentes<br>vlan 30<br>name Estudiantes<br>vlan 40<br>name Invitados<br>vlan 50<br>name Usuarios<br>vlan 56<br>name Native   |
| Crear troncos 802.1Q que utilicen la VLAN 56 nativa | Interfaces F0/1, F0/2 y F0/5<br><br><i>Interface GigabitEthernet1/0/1-2</i><br><i>switchport trunk native vlan 56</i><br><i>switchport trunk encapsulation dot1q</i><br><i>switchport mode trunk</i><br><br><i>interface GigabitEthernet1/0/5</i><br><i>switchport trunk native vlan 56</i><br><i>switchport trunk encapsulation dot1q</i><br><i>switchport mode trunk</i> |

| <b>Tarea</b>  | <b>Especificación</b>   |
|---|---|
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación<br><br><i>interface GigabitEthernet1/0/1-2<br/>channel-group 1 mode active</i>   |
| Configurar el puerto de acceso de host para VLAN 20                             | Interface F0/6<br><br><i>interface GigabitEthernet1/0/6<br/>switchport access vlan 20<br/>switchport mode access<br/>switchport nonegotiate</i>   |
| Configurar la seguridad del puerto en los puertos de acceso                     | Permitir 4 direcciones MAC<br><br><i>interface GigabitEthernet1/0/6<br/>switchport nonegotiate<br/>switchport port-security<br/>switchport port-security maximum 4</i>  |
| Proteja todas las interfaces no utilizadas                                      | Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar<br><br><i>interface range G1/0/3-4, G1/0/7-24, G1/1/1-4<br/>description NO ESTA EN USO<br/>switchport access vlan 50<br/>switchport mode access<br/>switchport nonegotiate<br/>shutdown</i> |

Fuente: Autoría propia

### 2.2.4.2 Paso 2 Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

*Tabla 15 Creación de VLAN – s2*

| Tarea  | Especificación   |
|--|--|
| <p>Crear VLAN</p>  | <p>VLAN 20, nombre Docentes<br/>           VLAN 30, nombre Estudiantes<br/>           VLAN 40, nombre Invitados<br/>           VLAN 50, nombre Usuarios<br/>           VLAN 56, nombre Native</p> <p>El proceso lo iniciamos desde el S2, debemos crear cada una de ellas y luego le asignamos un nombre:</p> <pre>           vlan 20           name Docentes           vlan 30           name Estudiantes           vlan 40           name Invitados           vlan 50           name Usuarios           vlan 56           name Native           </pre> |
| <p>Crear troncos 802.1Q que utilicen la VLAN 6 nativa</p>                              | <p>En modo de configuración se coloca el comando para troncales 802.1Q que utilicen la Vlan nativa asi: Interfaces F0/1 y F0/2</p> <pre>           interface GigabitEthernet1/0/1-2           switchport mode trunk           switchport trunk native vlan 56           switchport trunk encapsulation dot1q           </pre>  |
| <p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> | <p>Usar el protocolo LACP para la negociación</p> <pre>           interface GigabitEthernet1/0/1-2           channel-group 1 mode active           </pre>  |

| Tarea   | Especificación  |
|---|---|
| Configurar el puerto de acceso del host para la VLAN 30 | <p>En modo de configuración iniciamos llamamos la int f0/18 para configurar el puerto de acceso de host para Vlan 3 se utiliza el siguiente comando:</p> <pre>interface GigabitEthernet1/0/18 switchport access vlan 30 switchport mode access switchport nonegotiate</pre> |
| Configure port-security en los access ports             | <p>En modo de configuración de la interfaz se configura para que solo permitir 4 direcciones MAC con el siguiente comando:</p> <pre>interface GigabitEthernet1/0/18 switchport nonegotiate switchport port-security maximum 4</pre>   |
| Asegure todas las interfaces no utilizadas.             | <p>Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar</p> <pre>interface range G1/0/3-17, G1/0/19-24, G1/1/1-4 description NO ESTA EN USO switchport access vlan 50 switchport mode access switchport nonegotiate shutdown</pre>             |

Fuente: Autoría propia

### 2.2.4.3 Parte 5 Configurar soporte de host

### 2.2.5 Paso 1 Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 16 Configuración R1 – DHCP*

| <b>Tarea</b>                      | <b>Especificación</b>  |
|-----------------------------------|--|
| Configure Default Routing         | Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0<br><br><i>ip route 0.0.0.0 0.0.0.0 Loopback0</i><br><i>ipv6 route ::/0 Loopback0</i>  |
| 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<br><br><i>ip dhcp excluded-address 10.26.8.1 10.26.8.52</i><br><i>ip dhcp pool VLAN 20 - Docentes</i><br><i>network 10.26.8.0 255.255.255.192</i><br><i>default-router 10.26.8.1</i><br><i>domain-name unad-ccna-sa.net</i>       |
| 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<br><br><i>ip dhcp excluded-address 10.26.8.65 10.26.8.84</i><br><i>ip dhcp pool VLAN 30 - Estudiantes</i><br><i>network 10.26.8.64 255.255.255.224</i><br><i>default-router 10.26.8.65</i><br><i>domain-name unad-ccna-sb.net</i> |

*Fuente: Autoría propia*

## 2.2.6 Paso 2 Configurar los servidores

El desarrollo de trabajo integra la configuración de los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Posterior se debe verificar mediante el comando ipconfig /all, toda la información contenida en los mismos.

Después de configurar cada servidor, registre las configuraciones de red del host con

*Tabla 17 configuración PC-A*

| <b>PC-A Network Configuration</b> |                        |
|-----------------------------------|------------------------|
| Descripción                       | <i>PC-A</i>            |
| Dirección física                  | <i>000A.F319.DABE</i>  |
| Dirección IP                      | <i>10.26.8.53</i>      |
| Máscara de subred                 | <i>255.255.255.192</i> |
| Gateway predeterminado            | <i>10.26.8.1</i>       |
| Gateway predeterminado IPv6       | <i>FE80::1</i>         |

*Fuente: Autoría propia*

*Tabla 18 Configuración PC-B*

| <b>Configuración de red de PC-C</b> |                        |
|-------------------------------------|------------------------|
| Descripción                         | <i>PC-B</i>            |
| Dirección física                    | <i>000A.F319.DABE</i>  |
| Dirección IP                        | <i>10.26.8.85</i>      |
| Máscara de subred                   | <i>255.255.255.192</i> |
| Gateway predeterminado              | <i>10.26.8.1</i>       |
| Gateway predeterminado IPv6         | <i>FE80::1</i>         |

*Fuente: Autoría propia*

### 2.2.7 Paso 3 Probar y verificar la conectividad de extremo a extremo

Se debe realizar las respectivas verificaciones de conectividad con los protocolos de internet IPv4 e IPv6

*Tabla 19 Verificación de conectividad desde PC-A y PC-B*

| <b>Desde</b> | <b>A</b>     | <b>de Internet</b>  | <b>Dirección IP</b>   | <b>Resultados de ping</b> |
|--------------|--------------|---------------------|-----------------------|---------------------------|
| PC-A         | R1, G0/0/1.2 | Dirección           | 10.26.8.1             | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:a :1    | <i>Exitoso</i>            |
|              | R1, G0/0/1.3 | Dirección           | 10.26.8.65            | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:b :1    | <i>Exitoso</i>            |
|              | R1, G0/0/1.4 | Dirección           | 10.26.8.97            | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:c :1    | <i>Exitoso</i>            |
|              | S1, VLAN 4   | Dirección           | 10.26.8.98            | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:c :98   | <i>Exitoso</i>            |
| S2, VLAN 4   | Dirección    | 10.26.8.99.         | <i>Exitoso</i>        |                           |
|              | IPv6         | 2001:db8:acad:c :99 | <i>Exitoso</i>        |                           |
|              | PC-B         | Dirección           | IP address will vary. | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:b :50   | <i>Exitoso</i>            |
|              | R1 Bucle 0   | Dirección           | 209.165.201.1         | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:209: :1 | <i>Exitoso</i>            |
| PC-B         | R1 Bucle 0   | Dirección           | 209.165.201.1         | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:209::1  | <i>Exitoso</i>            |
|              | R1, G0/0/1.2 | Dirección           | 10.26.8.1             | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:a::1    | <i>Exitoso</i>            |
|              | R1, G0/0/1.3 | Dirección           | 10.26.8.65            | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:b::1    | <i>Exitoso</i>            |
|              | R1, G0/0/1.4 | Dirección           | 10.26.8.97            | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:c::1    | <i>Exitoso</i>            |
|              | S1, VLAN 4   | Dirección           | 10.26.8.98            | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:c::98   | <i>Exitoso</i>            |
|              | S2, VLAN 4   | Dirección           | 10.26.8.99.           | <i>Exitoso</i>            |
|              |              | IPv6                | 2001:db8:acad:c::99   | <i>Exitoso</i>            |

*Fuente: Prueba de habilidades CCNA.*

## 2.2.7.1 PRUBAS DE CONECTIVIDAD.

Figura 20 Prueba conectividad desde PCA – IPV4.

The screenshot displays a network topology in Cisco Packet Tracer. On the left, a router (ISR 320) is connected to a switch (3650-24F S1) via g0/0/1 and g0/0/5. The switch S1 is connected to PC-A (PC-PT) via g1/0/6. On the right, another switch (3650-24F S2) is connected to the router via g1/0/1 and g1/0/5, and to PC-B (PC-PT) via g1/0/18. The switches S1 and S2 are interconnected via g1/0/1 and g1/0/2. The router's Lo0 interface is configured with three IPv4 addresses: 10.26.8.1/26, 10.26.8.65/27, and 10.26.8.97/29. The terminal window on the right shows the following commands and outputs:

```

C:\>ping 10.26.8.1
Pinging 10.26.8.1 with 32 bytes of data:
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Ping statistics for 10.26.8.1:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.26.8.65
Pinging 10.26.8.65 with 32 bytes of data:
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Ping statistics for 10.26.8.65:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.26.8.97
Pinging 10.26.8.97 with 32 bytes of data:
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Ping statistics for 10.26.8.97:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
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=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

Fuente: Autoría propia

Figura 21 Prueba conectividad desde PC-B – IPV6.

This screenshot shows the same network topology as Figure 20. The terminal window on the right shows IPv6 connectivity tests from PC-B:

```

C:\>ping 10.26.8.85 with 32 bytes of data:
Reply from 10.26.8.85: bytes=32 time=1ms TTL=128
Reply from 10.26.8.85: bytes=32 time=1ms TTL=128
Reply from 10.26.8.85: bytes=32 time=1ms TTL=128
Reply from 10.26.8.85: bytes=32 time=1ms TTL=128
Ping statistics for 10.26.8.85:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.26.8.1
Pinging 10.26.8.1 with 32 bytes of data:
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Reply from 10.26.8.1: bytes=32 time=1ms TTL=255
Ping statistics for 10.26.8.1:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms
C:\>ping 10.26.8.65
Pinging 10.26.8.65 with 32 bytes of data:
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Reply from 10.26.8.65: bytes=32 time=1ms TTL=255
Ping statistics for 10.26.8.65:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.26.8.97
Pinging 10.26.8.97 with 32 bytes of data:
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Reply from 10.26.8.97: bytes=32 time=1ms TTL=255
Ping statistics for 10.26.8.97:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
  
```

Fuente: Autoría propia

## CONCLUSIONES

- Luego de realizar el proceso de configuración hemos podido verificar que tenemos total conectividad dentro de nuestras redes configuradas, comprendemos el proceso de desarrollo e implementación de nuestra red aplicando para ello comandos específicos para cada una de las situaciones.
- El material de apoyo con el cual se cuenta para el desarrollo del Diplomado es muy completo, y junto con el acompañamiento de los TUTORES fue posible culminar el desarrollo del mismo.
- PACKET TRACER se convirtió en nuestra mano derecha, gracias a este podemos realizar el montaje de la red simulada con el fin de poder verificar el correcto funcionamiento de la misma.
- Veo con agrado que los temas han sido asimilados por nuestra parte, estamos en condiciones de configurar redes de mediana complejidad, aportando de manera significativa experiencia y conocimiento a empresas medianas que así lo requiera.
- A todo el direccionamiento IP de la red aplicamos VLSM lo cual nos permitió optimizar el número de direcciones por cada subred de acuerdo a los requerimientos específicos.
- Comprendo el funcionamiento de cada uno de los protocolos de enrutamiento dentro de la red, las posibilidades que cada uno de ellos tiene y las diferentes alternativas en las cuales es conveniente su configuración.
- Se documentó cada uno de los pasos realizados en la red y en cada uno de los dispositivos, lo cual permitió y posibilitó en gran medida el encontrar errores de configuración. Nuestra red es totalmente funcional.

## REFERENCIAS BIBLIOGRÁFICAS

- [1] ABAD Alfredo., Redes locales, Mac Graw Hill, {En Línea} (2012) {22 octubre 2022} Disponible en <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjil9qox8r7AhVjmlQIHWTVCkwQFnoECA8QAQ&url=https%3A%2F%2Fjuanantonioleonlopez.files.wordpress.com%2F2017%2F11%2Fredes-locales.pdf&usq=AOvVaw2yIK3vXSSC5OcuFlywenYy>
- [2] ANDREW s. Tanenbaum. Redes de Computadoras (Cuarta Edición). Mexico. PEARSON Prentice Hall. {En Línea} (2003) {19 octubre 2022} Disponible en <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwigsPmFu8r7AhXOQTABHamUBKoQFnoECAkQAQ&url=https%3A%2F%2Fbibliotecavirtualapure.files.wordpress.com%2F2015%2F06%2Fredes-de-computadoras-freelibros-org.pdf&usq=AOvVaw3VWrfyxpTHg6tAm7P74btQ>
- [3] FROM, R., FRAHIM, E. CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. {En Línea}(2015), {19 octubre 2022} Disponible en [https://books.google.com.co/books?hl=es&lr=&id=dkDsJmnsejEC&oi=fnd&pg=PR8&dq=CISCO+Press+\(Ed\).+Spanning+Tree+Implementation.+Implementing+Cisco+IP+Switched+Networks+\(SWITCH\)+&ots=XRgQWGbApp&sig=O7jaBFnMXM5g9Li37qG\\_5CKXhGM&redir\\_esc=y#v=onepage&q&f=false](https://books.google.com.co/books?hl=es&lr=&id=dkDsJmnsejEC&oi=fnd&pg=PR8&dq=CISCO+Press+(Ed).+Spanning+Tree+Implementation.+Implementing+Cisco+IP+Switched+Networks+(SWITCH)+&ots=XRgQWGbApp&sig=O7jaBFnMXM5g9Li37qG_5CKXhGM&redir_esc=y#v=onepage&q&f=false)
- [4] TEARE, D., VACHON B., GRAZIANI, R. CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. {En Línea} (2015) {19 octubre 2022} Disponible en [https://books.google.es/books?hl=es&lr=&id=z5f4BQAAQBAJ&oi=fnd&pg=PR8&dq=Implementation.+Implementing+Cisco+IP+Routing+\(ROUTE\)+Foundation+Learning+Guide+CCNP+ROUTE+300-101.+&ots=4oL5Ny6Tcq&sig=7kxJOalJgXH0HIF2nnDdbefA9EE#v=onepage&q=Implementation.%20Implementing%20Cisco%20IP%20Routing%20\(ROUTE\)%20Foundation%20Learning%20Guide%20CCNP%20ROUTE%20300-101.&f=false](https://books.google.es/books?hl=es&lr=&id=z5f4BQAAQBAJ&oi=fnd&pg=PR8&dq=Implementation.+Implementing+Cisco+IP+Routing+(ROUTE)+Foundation+Learning+Guide+CCNP+ROUTE+300-101.+&ots=4oL5Ny6Tcq&sig=7kxJOalJgXH0HIF2nnDdbefA9EE#v=onepage&q=Implementation.%20Implementing%20Cisco%20IP%20Routing%20(ROUTE)%20Foundation%20Learning%20Guide%20CCNP%20ROUTE%20300-101.&f=false)

## ANEXOS

Anexo A descarga archivos simulación Escenarios 1 y 2.

Enlace: [https://drive.google.com/drive/folders/1PXMrngYH4Kai - FbJsaQSw1P\\_AJWbaT?usp=share link](https://drive.google.com/drive/folders/1PXMrngYH4Kai - FbJsaQSw1P_AJWbaT?usp=share_link)