# SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

CLAUDIA MILENA TORRES LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
TUNJA -BOYACÁ
2020

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

CLAUDIA MILENA TORRES LOPEZ

Trabajo final del Diplomado de profundización CISCO

TUTOR:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
INGENIERÍA DE SISTEMAS
TUNJA-BOYACÁ
MAYO 2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Tunja, 23 de mayo de 2020

El presente trabajo lo dedico Principalmente a Dios por ser el inspirador y darme fuerza para continuar con este proceso. Y a mis padres e hijo que me acompañaron incondicionalmente.

## AGRADECIMIENTOS

Quiero expresar mis Agradecimientos a Dios, quien con su bendición siempre guio mi camino y no me dejo decaer en este proceso. A mis Padres, a mi Hijo, quienes con su apoyo y amor me enseñaron a no temer en las adversidades y lograr este sueño.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

# GLOSARIO

SWITCH: Es un dispositivo análogo que permite interconectar redes entre sí, operando la mejor ruta para que un determinado paquete de datos llegue a su destino.

ROUTER: es un dispositivo encargado de reenviar los paquetes entre distintas redes.

IP: es el sistema estándar que por el cual funciona el internet, por medio de un proceso de envío y recepción de información.

DNS: es un sistema de datos distribuidos que sirven para gestionar nombres de host y las direcciones IP asociadas a ellos.

CISCO: Es una empresa que fabrica dispositivos para redes locales y externas, su objetivo es conectar a todos y demostrar las cosas maravillosas que puede lograr con su visión clara del futuro.

SERVIDORES: es un equipo diseñado para procesar solicitudes y entregar datos a otros ordenadores que se pueden llamar clientes.

## RESUMEN

La realización de este trabajo es la evaluación “prueba de habilidades prácticas” siendo una actividad evaluativa del diplomado de profundización CCNA, la cual nos permite identificar el desarrollo de las competencias y habilidades que se fueron adquiriendo en el transcurso del diplomado, desarrollando dos escenarios por medio de la herramienta packet tracer, configurando y diseñando las topologías de red de acuerdo a la guía y realizando las conexiones adecuadas para cada caso verificando su correcto funcionamiento.



PALABRAS CLAVE: Evaluación, CISCO, conexiones, topologías, red.

# 1. INTRODUCCIÓN

El examen de pruebas de habilidades prácticas, es una actividad obligatoria requerida del diplomado de profundización de CCNA, comprendiendo todas las competencias brindadas durante el curso y aplicando todos los conocimientos adquiridos durante todo el curso y desarrollo del diplomado de cisco, dando solución a los diferentes ejercicios planteados como por ejemplo la configuración de cada uno de los dispositivos utilizando los comandos traceroute, show ip route, entre otros.

# 2. OBJETIVOS

## 2.1 OBJETIVO GENERAL

Realizar los dos casos de estudio planteados en la guía de Pruebas de Habilidades bajo el uso de tecnología CISCO, aplicando la solución del problema de Networking y poderla aplicar en nuestras experiencias diarias como Ingenieros de Sistemas

## 2.2 OBJETIVOS ESPECÍFICOS

Reconocer cuales son los dispositivos que se van a utilizar para la realizar la topología de la red.

Hacer la respectiva configuración de los dispositivos para que se puedan conectar y comunicar los Switchs, Routers, servidores y equipos.

Comprobar la respectiva conexión entre los dispositivos de una tecnología.

Realizar la configuración de las listas de control y acceso ACL.

# 3. MATERIALES Y MÉTODOS

## 3.1 MATERIALES

Programa Packert tracer, Guia de actividades, Computador, Internet.

## 3.2 METODOLOGÍA

La realización del trabajo se realizó con la guía de actividades que el tutor nos suministró para desarrollar la actividad.

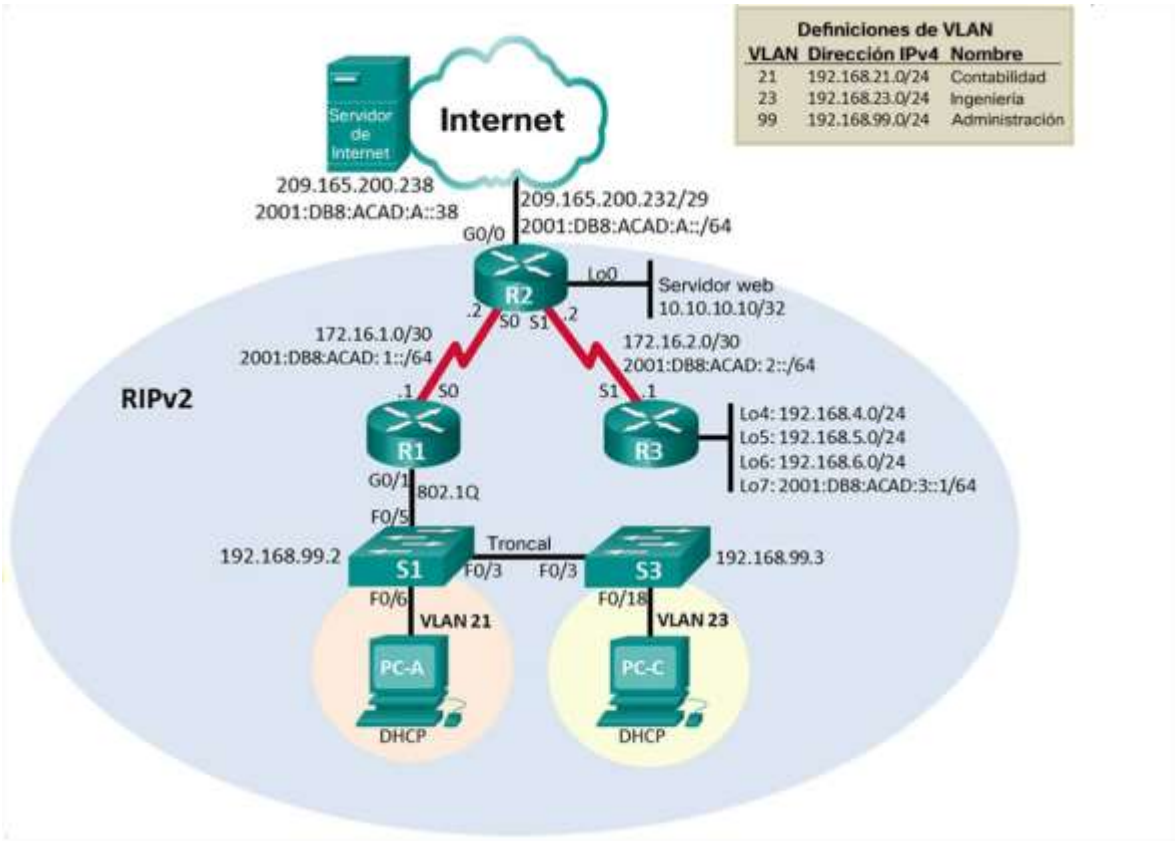
# 4. DESARROLLO DEL PROYECTO

## 4.1 ESCENARIO 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

### Topología

Figura 1: Topología de red escenario 1




Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

1. Inicializar dispositivos

Tabla 1. Tabla de Direccionamiento 1

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| Servidor PC | Nic | 209.165.200.238 | | 209.165.200.225 |
| | Nic | 2001:db8:acad:a::38 /64 | | 2001:DB8:ACAD:2::1 |
| R1 | S0/0/0 | 172.16.1.1 /30 | 255.255.255.252 | 172.16.1.1 |
| | | 2001:db8:acad:1:: /64 | | |
| | G0/1 | | | |
| R2 | G0/0 | 209.165.200.232 /29 | 255.255.255.0 | |
| | | 2001:db8:acad:a:: /64 | | |
| | S0/0/0 | 172.16.1.2 /30 | 255.255.0.0 | |
| | | 2001:db8:acad:2:: /64 | | |
| | S0/0/1 | 172.16.2.1 /30 | 255.255.255.252 | |
| | | 2001:db8:acad:2:: /64 | | |
| | Lo0 | 10.10.10.10 /32 servidor web | 255.0.0.0 | |
| R3 | S0/0/1 | 172.16.2.2 /30 | 255.255.255.252 | |
| | Lo4 | 192.168.4.1 /24 | 255.255.255.0 | |
| | Lo5 | 192.168.5.1 /24 | 255.255.255.0 | |
| | Lo6 | 192.168.6.1 /24 | 255.255.255.0 | |
| | Lo7 | 2001:db8:acad:3:: 1 /64 | 255.255.255.0 | |
| S1 | IP | 192.168.99.2 | | |
| | F0/5 R1 | | | |
| | F0/6 VLAN21 PCA | | | |
| | F0/3 TRONC S3 | | | |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |

Fuente: Autor

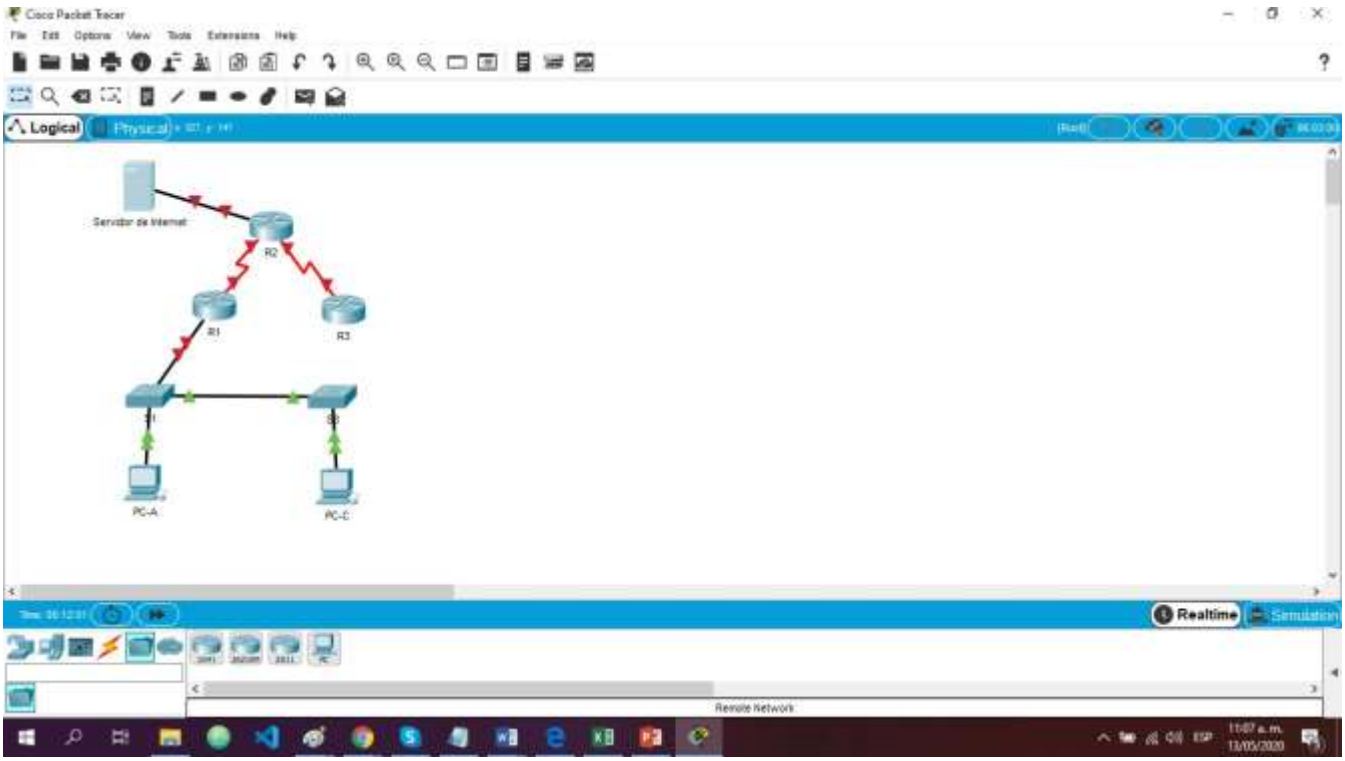



Figura 2. Creación de la red

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 2. Tareas y comandos

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | R1<br>Router#erase Startup-config<br>R2<br>Router#erase Startup-config<br>R3<br>Router#erase Startup-config |
| Volver a cargar todos los routers | R1<br>Router#reload<br>R2<br>Router#reload |

| | |
|---|---|
| | R3<br>Router#reload |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | Swich#erase startup-config |
| Volver a cargar ambos switches | Swich#reload |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | Swich#sh flash: |

Fuente Autor

Parte 2 Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 3. Elementos de Configuración

| Elemento o tarea de configuración | Especificación |
|---|---|
| Dirección IPv4 | 209.165.200.238 |
| Máscara de subred para IPv4 | 255.255.255.0 |
| Gateway predeterminado | 209.165.200.225 |
| Dirección IPv6/subred | 2001:db8:acad:a::38 /64 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:2::1 |

Fuente: Autor

**Nota:** Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

## Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4. Configuración R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R1<br>Router(config)#hostname R1 |
| Contraseña de exec privilegiado cifrada | Class<br>R1(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>R1(config)#line con 0<br>R1(config-line)#password cisco |
| Contraseña de acceso Telnet | Cisco<br>R1(config-line)#line vty 0 4<br>R1(config-line)#password cisco |
| Cifrar las contraseñas de texto no cifrado | R1(config-line)#service password-encryprion |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br>R1(config)#banner motd *Se prohibe el acceso No Autorizado* |

| | |
|---|---|
| Interfaz S0/0/0 | Establezca la descripción<br>R1(config)#int s/0/0/0<br>R1(config-if)#descrption conexion al R2<br>Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones<br>R1(config-if)#ip address 172.16.1.1 255.255.255.252<br>R1(config-if)#ipv6 address 2001:db8:acad:1::/64<br>Establecer la frecuencia de reloj en 128000<br>R1(config-if)#clock rate 128000<br>Activar la interfaz<br>R1(config-if)#no shutdown |
| Rutas predeterminadas | Configurar una ruta IPv4 predeterminada de S0/0/0<br>R1(config)#int s0/0/0<br>R1(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 Configurar una ruta IPv6 predeterminada de S0/0/0<br>R1(config)#ipv6 route ::/0 s0/0/0 |

Fuente: Autor

**Nota:** Todavía no configure G0/1.

### Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 5. Configuración R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R2<br>Router(config)#hostname R2 |

| | |
|---|---|
| Contraseña de exec privilegiado cifrada | Class<br>R2(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>R2(config)#line con 0<br>R2(config-line)#password<br>cisco R2(config-<br>line)#login<br>R2(config-line)#logging synchronous |
| Contraseña de acceso Telnet | cisco<br>R2(config)#line vty 0 4<br>R2(config-line)#password cisco<br>R2(config-line)#login<br>R2(config-line)#logging synchronous |
| Cifrar las contraseñas de texto no cifrado | R2(config)#service password-encryption |
| Habilitar el servidor HTTP | R2(config)# ip http secure-server |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br>R2(config)#banner motd *Se prohibe el acceso No Autorizado* |
| Interfaz S0/0/0 | Establezca la descripción<br>R2(config)#int s0/0/0<br>R2(config-if)#description Conexion al R1<br>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.<br>R2(config-if)#ip address 172.16.1.1 255.255.0.0<br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>R2(config-if)#ipv6 address 2001:db8:acad:1::/64<br>Activar la interfaz<br>R2(config-if)#no shutdown |

| | |
|---|---|
| Interfaz S0/0/1 | Establecer la descripción<br>R2(config)#int s0/0/1<br>R2(config-if)#description Conexion al R3<br>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br>R2(config-if)#ip address 172.161.2.0 255.255.0.0<br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>R2(config-if)#ipv6 address 2001:db8:acad:2::/64 Establecer la frecuencia de reloj en 128000.<br>R2(config-if)#clock rate 128000<br>Activar la interfaz<br>R2(config-if)#no shutdown |
| Interfaz G0/0 (simulación de Internet) | Establecer la descripción.<br>R2(config)#int g0/0<br>R2(config-if)#description Conexion al Servidor de Internet<br>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br>R2(config-if)#ip address 209.165.200.232 255.255.255.0<br>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.<br>R2(config-if)#ipv6 address 2001:db8:acad:a::/64<br>Activar la interfaz<br>R2(config-if)#no shutdown |
| Interfaz loopback 0 (servidor web simulado) | Establecer la descripción.<br>R2(config-if)#description Conexion al servidor Web<br>Establezca la dirección IPv4.<br>R2(config-if)#ip address 10.10.10.10 255.0.0.0 |

| | |
|---|---|
| Ruta predeterminada | Configure una ruta IPv4 predeterminada de G0/0.<br>R2(config-if)#ip route 0.0.0.0 0.0.0.0<br>Configure una ruta IPv6 predeterminada de G0/0.<br>ipv6 route ::/0 s0/0/0 |

Fuente: Autor

**Paso 4: Configurar R3**

La configuración del R3 incluye las siguientes tareas:

Tabla 6. Configuración R3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R3<br>Switch(config)#hostname R3 |
| Contraseña de exec privilegiado cifrada | Class<br>Router(config)#no ip domain-lookup |
| Contraseña de acceso a la consola | Cisco<br>R3(config)#line con 0<br>R3(config-line)#password cisco<br>R3(config-line)#login<br>R3(config-line)#logging synchronous |
| Contraseña de acceso Telnet | Cisco<br>R3(config-line)#line vty 0 4<br>R3(config-line)#login<br>R3(config-line)#logging synchronous |
| Cifrar las contraseñas de texto no cifrado | R3(config-line)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br>R3(config)#banner motd *Se prohibe el Acceso NO Autorizado* |

| | |
|---|---|
| Interfaz S0/0/1 | Establecer la descripción<br>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.<br>R3(config)#int s0/0/1<br>R3(config-if)#ip address 172.161.3.0 255.255.0.0<br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>R3(config-if)#ipv6 address 2001:db8:acad:2::/64<br>Activar la interfaz<br>R3(config-if)#no shutdown |
| Interfaz loopback 4 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br>R3(config-if)#no shutdown<br>R3(config-if)#no shutdown |
| Interfaz loopback 5 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br>R3(config-if)#int lo5<br>R3(config-if)#ip address 192.168.5.1 255.255.255.0 |
| Interfaz loopback 6 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br>R3(config-if)#int lo6<br>R3(config-if)#ip address 192.168.6.1 255.255.255.0 |
| Interfaz loopback 7 | Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>R3(config-if)#int lo7<br>R3(config-if)#ip address 192.168.7.1 255.255.255.0 |
| Rutas predeterminadas | R3(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.2.1 |
| | |

Fuente: Autor

**Paso 5: Configurar S1**

La configuración del S1 incluye las siguientes tareas:

Tabla 7. Configuración S1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |
| Nombre del switch | S1<br>Switch(config)#hostname S1 |
| Contraseña de exec privilegiado cifrada | Class<br>S1(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>S1(config)#line con 0<br>S1(config-line)#password cisco<br>S1(config-line)#login<br>S1(config-line)#logging Synchronous |
| Contraseña de acceso Telnet | Cisco<br>S1(config-line)#line vty 0 4<br>S1(config-line)#password cisco<br>S1(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | S1(config-line)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br>S1(config)#banner motd *Se prohibe el Acceso No Autorizado* |

Fuente: Autor

## Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 8. Configuración S3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |
| Nombre del switch | S3<br>Switch(config)#hostname S3 |
| Contraseña de exec privilegiado cifrada | Class<br>S3(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco<br>S3(config)#line con 0<br>S3(config-line)#password cisco<br>S3(config-line)#login<br>S3(config-line)#logging synchronous |
| Contraseña de acceso Telnet | Cisco<br>S3(config-line)#line vty 0 4<br>S3(config-line)#password cisco<br>S3(config-line)#login<br>S3(config-line)#logging synchronous |
| Cifrar las contraseñas de texto no cifrado | S3(config-line)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br>S3(config)#banner motd *Se prohibe el Acceso NO Autorizado* |

Fuente: Autor

**Paso 7: Verificar la conectividad de la red**

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

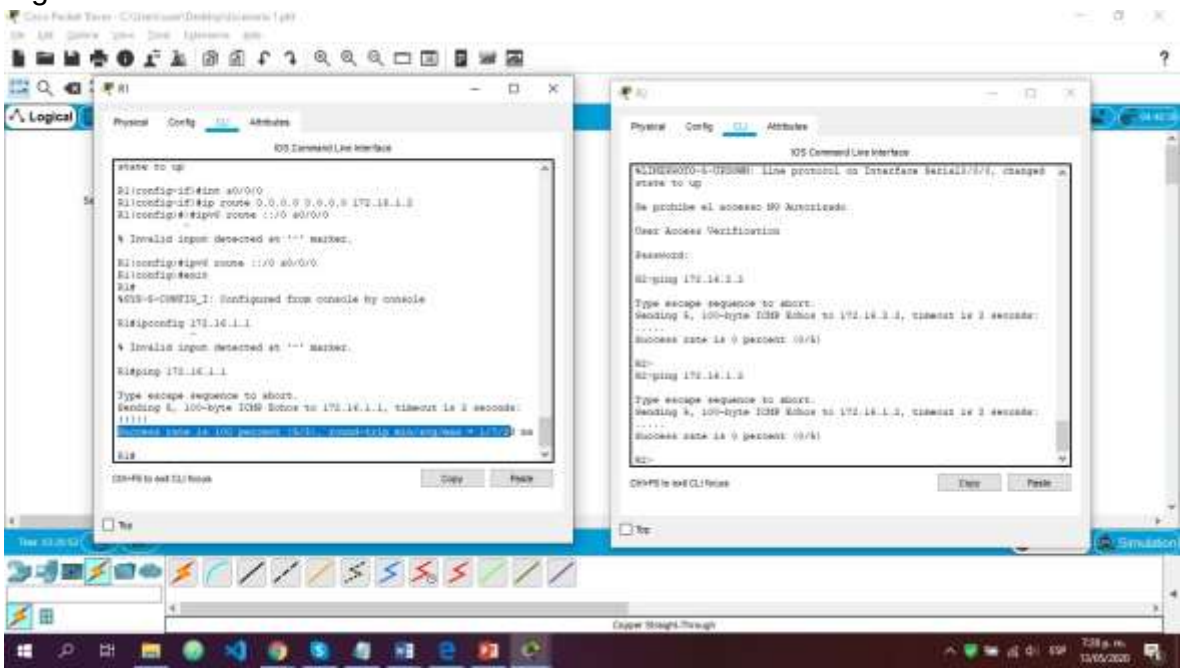
Tabla 9. Verificación conectividad de la red

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | R1= ping 172.16.1.2 | Satisfactorio |
| R2 | R3, S0/0/1 | R2= ping 172.16.2.2 | Satisfactorio |
| PC de Internet | Gateway predeterminado | PC= Ping 209.165.200.232 | |

Fuente: Autor

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 3. Creación de la Red escenario 1 – Evidencia



Fuente: Autor

**Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN**

Tabla de Direccionamiento

Tabla 9. Tabla de Direccionamiento VLANS1

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| R1 | G0/1.99 | 192.168.99.1 | 255.255.255.0 | N/A |
| | G0/1.21 | 192.168.21.1 | 255.255.255.0 | N/A |
| | G0/1.23 | 192.168.23.1 | 255.255.255.0 | N/A |
| | Lo0 | 209.165.200.225 | 255.255.255.224 | N/A |
| S1 | VLAN 99 | 192.168.99.2 | 255.255.255.0 | 192.168.99.1 |
| S2 | VLAN 99 | 192.168.99.3 | 255.255.255.0 | 192.168.99.1 |
| PC-A | NIC | 192.168.21.3 | 255.255.255.0 | 192.168.21.1 |
| PC-B | NIC | 192.168.23.3 | 255.255.255.0 | 192.168.21.1 |

Fuente: Autor

Especificaciones de la asignación de puertos de swich

Tabla 11. Tabla de Asignación del swich

| Puertos | Asignaciones | Red |
|---|---|---|
| S1 F0/1 | Enlace troncal de 802.1Q | N/A |
| S2 F0/1 | Enlace troncal de 802.1Q | N/A |
| S1 F0/5 | Enlace troncal de 802.1Q | N/A |
| S1 F0/6 | VLAN 21: Contabilidad | 192.168.21.0/24 |
| S2 F0/18 | VLAN 20: Ingeniería | 192.168.23.0/24 |

Fuente: Actor

**Paso 1: Configurar S1**

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Tabla de configuración S1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.<br><br>S1(config)#vlan 21<br>S1(config-vlan)#name Contabilidad<br>S1(config-vlan)#exit<br>S1(config)#vlan 23<br>S1(config-vlan)#name Ingenieria<br>S1(config-vlan)#exit<br>S1(config)#vlan 99<br>S1(config-vlan)#name Administracion |
| Asignar la dirección IP de administración. | Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología.<br>S1(config)#int vlan 99<br>S1(config-if)#ip address 192.168.99.2 255.255.255.0 |

| | |
|---|---|
| Asignar el gateway predeterminado | Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.<br>S1(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | Utilizar la red VLAN 1 como VLAN nativa<br>S1(config)#int f0/3<br>S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 |
| Forzar el enlace troncal en la interfaz F0/5 | Utilizar la red VLAN 1 como VLAN nativa<br>S1(config)#int f0/5<br>S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | Utilizar el comando interface range<br>S1(config)# int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access |
| Asignar F0/6 a la VLAN 21 | S1(config)#int f0/6<br>S1(config-if)#switchport mode access<br>S1(config-if)#switchport access vlan 21 |
| Apagar todos los puertos sin usar | S1(config)#int range f0/1-2,f0/4,f0/7-24 ,g0/1<br>S1(config-if-range)#shutdown |

Fuente: Autor

**Paso 8: Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Tabla de configuración S3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.<br>S3(config)#vlan 21<br>S3(config-vlan)#name Contabilidad<br>S3(config)#vlan 23<br>S3(config-vlan)#name ingenieria<br>S3(config)#vlan 99<br>S3(config-vlan)#name Administracion |
| Asignar la dirección IP de administración | Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología.<br>S3(config)#int vlan 99<br>S3(config-if)#ip address 192.168.99.3 255.255.255.0 |
| Asignar el gateway predeterminado. | Asignar la primera dirección IP en la subred como gateway predeterminado.<br>S3(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | Utilizar la red VLAN 1 como VLAN nativa<br>S3(config)#int f0/3<br>S3(config-if)#switchport mode trunk<br>S3(config-if)#switchport trunk native vlan1 |
| Configurar el resto de los puertos como puertos de acceso | Utilizar el comando interface range<br>S3(config)#int range f0/1-2, f0/4-24, g0/1-2<br>S3(config-if-range)#switchport mode access |
| Asignar F0/18 a la VLAN 21 | S3(config)#int f0/18<br>S3(config-if)#switchport mode access<br>S3(config-if)#switchport access vlan 21 |

| | |
|---|---|
| Apagar todos los puertos sin usar | S3(config)#int range f0/1-2,f0/4-17,f0/19-24 ,g0/1 S3(config-if-range)#shutdown |

Fuente: Autor

**Paso 9: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Tabla de configuración R1

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | Descripción: LAN de Contabilidad<br>R1(config)#int g0/1.21<br>R1(config-subif)#description LAN de Contabilidad<br>Asignar la VLAN 21<br>R1(config-subif)#encapsulation dot1Q 21<br>Asignar la primera dirección disponible a esta interfaz<br>R1(config-subif)#ip address 192.168.21.1 255.255.255.0 |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | Descripción: LAN de Ingeniería<br>R1(config)#int g0/1.23<br>R1(config-subif)#description LAN de Ingenieria<br><br>Asignar la VLAN 23<br>R1(config-subif)#encapsulation dot1Q 23<br><br>Asignar la primera dirección disponible a esta interfaz<br>R1(config-subif)#ip address 192.168.23.1 255.255.255.0 |

| | |
|---|---|
| Configurar la subinterfaz 802.1Q .99 en G0/1 | Descripción: LAN de Administración<br>R1(config)#int g0/1.99<br>R1(config-subif)#description LAN de Administracion<br><br>Asignar la VLAN 99<br>R1(config-subif)#encapsulation dot1Q 99<br><br>Asignar la primera dirección disponible a esta interfaz<br>R1(config-subif)#ip address 192.168.99.1 255.255.255.0 |
| Activar la interfaz G0/1 | R1(config)#int g0/1<br>R1(config-if)#no shutdow |

Fuente: Autor

**Paso 10: Verificar la conectividad de la red**

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

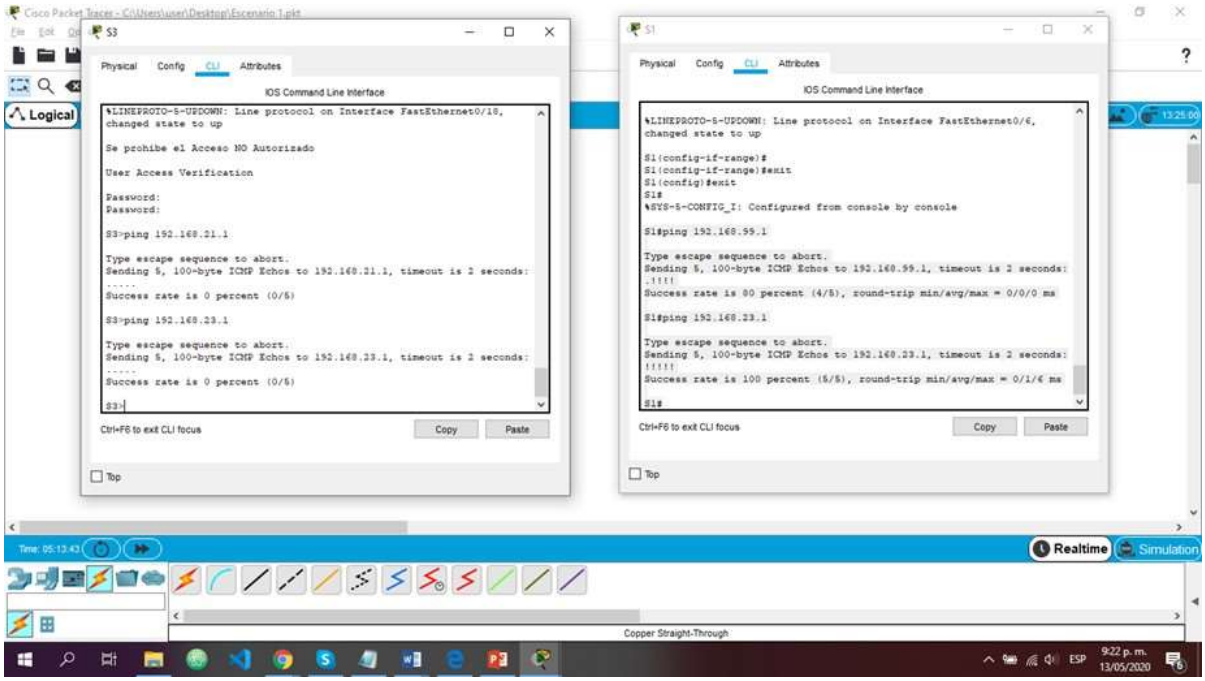
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 15. Tabla de conectividad de la red

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | Satisfactorio |
| S3 | R1, dirección VLAN 99 | 192.168.99.1 | No Satisfactorio |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | Satisfactorio |
| S3 | R1, dirección VLAN 23 | 192.168.23.1 | No Satisfactorio |

Fuente: Autor

Figura 3. Conexión de los dispositivos- Evidencia




Fuente: Autor

## Parte 4: Configurar el protocolo de routing dinámico RIPv2

### Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Tabla Configuración RIPv2 en el R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | R1#configure terminal<br>R1(config)#router rip<br>R1(config-router)#version 2 |
| Anunciar las redes conectadas directamente | Asigne todas las redes conectadas directamente.<br>R1(config-router)#network 172.16.0.0 |

| | |
|---|---|
| Establecer todas las interfaces LAN como pasivas | R1(config-router)#passive-interface g0/1 |
| Desactive la sumarización automática | R1(config-router)#no auto-summary |

Fuente: Autor

**Paso 2: Configurar RIPv2 en el R2**

La configuración del R2 incluye las siguientes tareas:

Tabla 17. Tabla Configuración RIPv2 en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | R3(config)#router rip<br>R3(config-router)#version 2 |
| Anunciar las redes conectadas directamente | **Nota:** Omitir la red G0/0.<br>R3(config-router)#network 172.16.0.0 |
| Establecer la interfaz LAN (loopback) como pasiva | R3(config-router)#passive-interface lo4 |
| Desactive la sumarización automática. | R3(config-router)#passive-interface lo5 |

Fuente: Autor

**Paso 3: Configurar RIPv3 en el R2**

La configuración del R3 incluye las siguientes tareas:

Tabla 18. Tabla Configuración RIPv3 en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | R3(config)#router rip<br>R3(config-router)#version 2 |
| Anunciar redes IPv4 conectadas directamente | R3(config-router)#network 172.16.0.0 |

| | |
|---|---|
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | R3(config router)#passive-interface lo4<br>R3(config-router)#passive- interface lo5<br>R3(config-router)#passive- interface lo6<br>R3(config-router)#passive-interface lo7 |
| Desactive la sumarización automática. | R3(config-router)#no auto-summary |

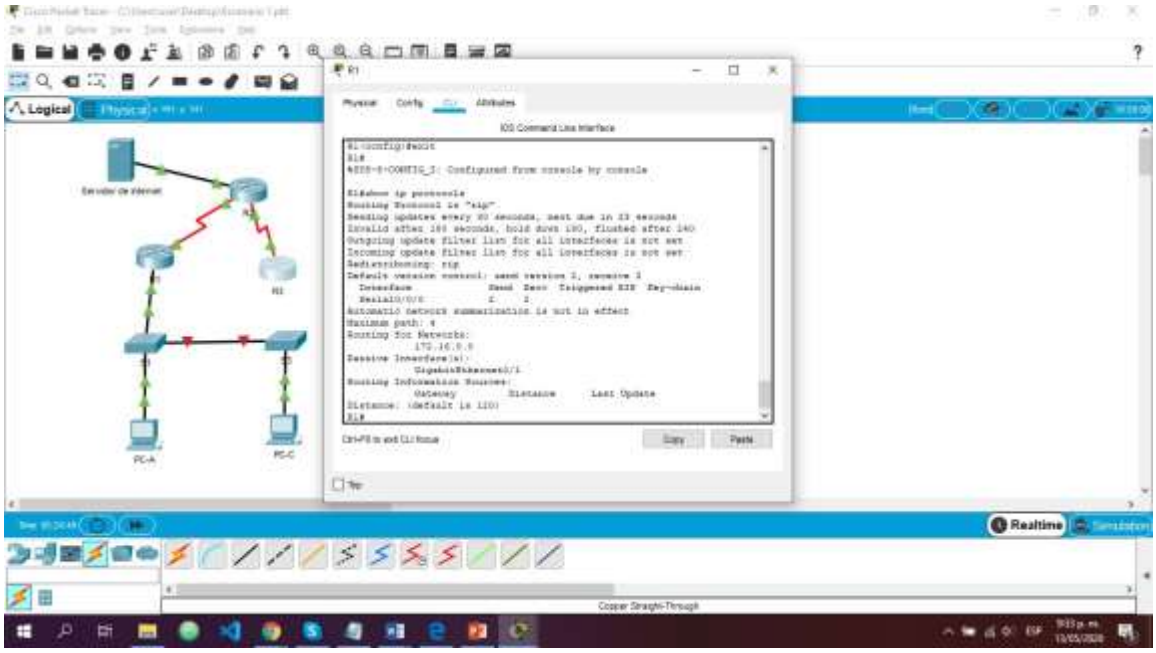
Fuente: Autor

**Paso 4: Verificar la información de RIP**

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

| Pregunta | Respuesta |
|---|---|
| ¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router? | R1#show ip protocols |
| | |

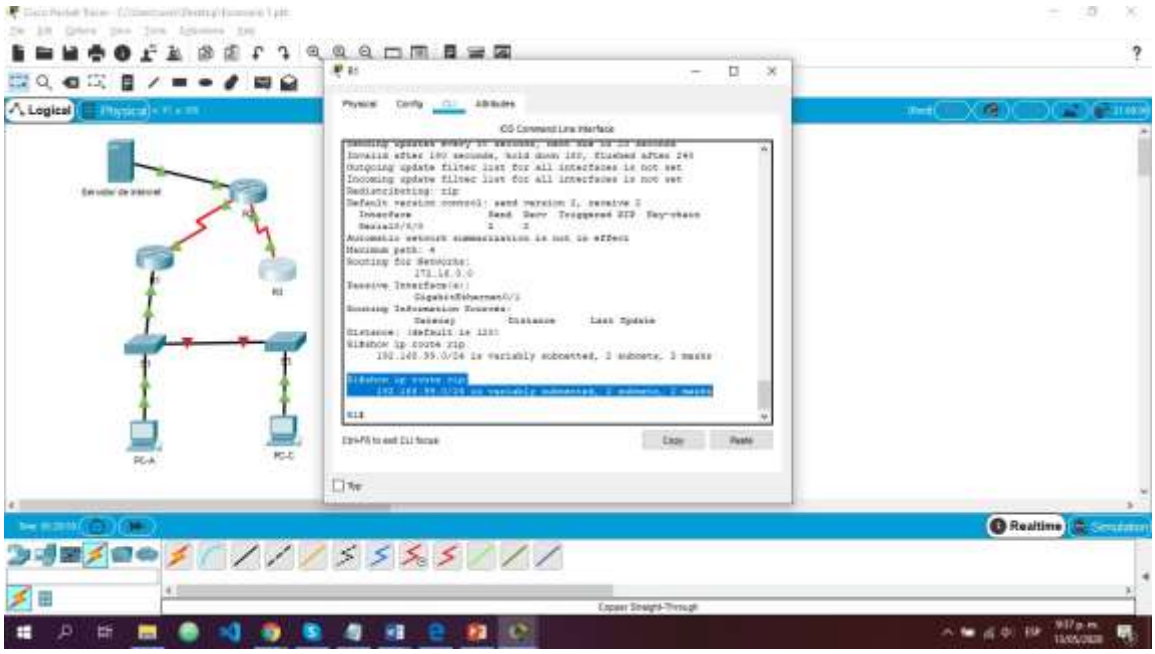
Figura 5.Evidencia de las interfaces del R1



Fuente: Actor

| | |
|---|---|
| ¿Qué comando muestra solo las rutas RIP? | R1#show ip route rip |

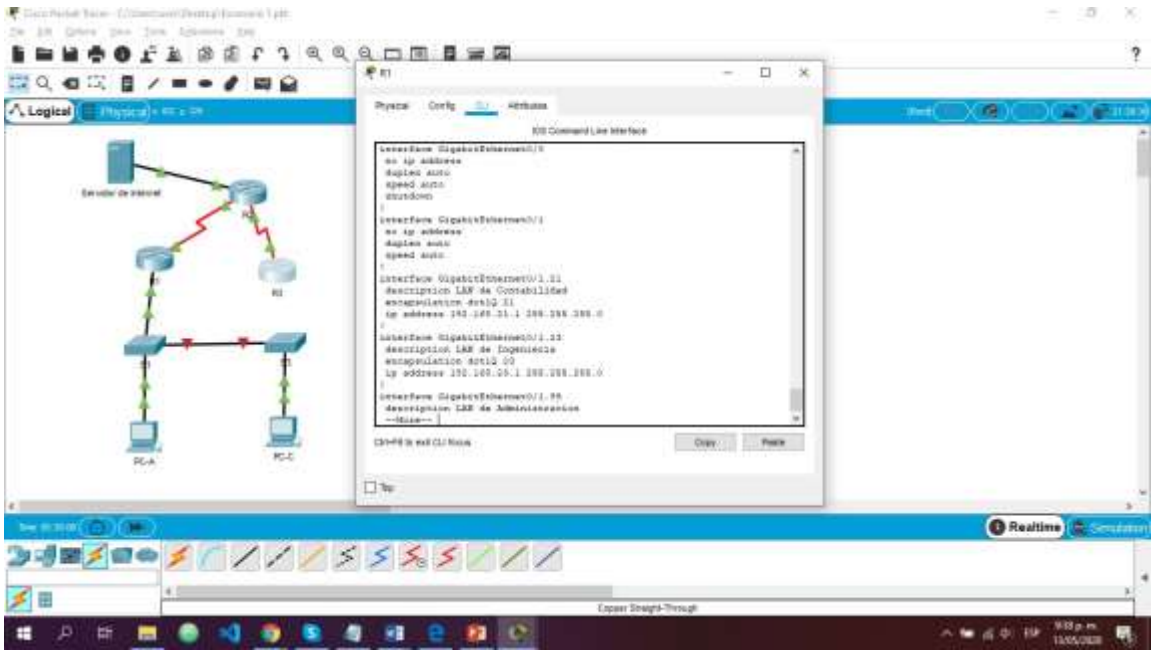
Figura 6. Evidencia del comando que muestra las rutas RIP



Fuente: Actor

| | |
|---|---|
| ¿Qué comando muestra la sección de RIP de la configuración en ejecución? | R1#show run |

Figura 7. Evidencia del comando de las rutas RIP



Fuente: Autor

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Tabla Implementación DHCP y NAT para IPv4

| Elemento o tarea de configuración | Especificación |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 |

| | |
|---|---|
| Crear un pool de DHCP para la VLAN 21. | Nombre: ACCT<br>R1(config)#ip dhcp pool ACCT<br>R1(dhcp-config)#NETwork 192.168.21.0 255.255.255.0<br>Servidor DNS: 10.10.10.10<br>R1(dhcp-config)#DNS-Server 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>R1(dhcp-config)#domain-name ccna-sa.com<br>Establecer el gateway predeterminado<br>R1(dhcp-config)#default-router 192.168.21.1 |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>R1(config)#ip dhcp pool ENGNR<br>R1(dhcp-config)#Network 192.168.23.0 255.255.255.0<br>Servidor DNS: 10.10.10.10<br>R1(dhcp-config)#DNS-SErver 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>R1(dhcp-config)#domain-name ccna-sa.com<br>Establecer el gateway predeterminado<br>R1(dhcp-config)#default-router 192.168.23.1 |

Fuente: Actor

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configuración de la NAT estática y dinámica en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear una base de datos local con una cuenta de usuario | Nombre de usuario: webuser<br>Contraseña: cisco12345<br>Nivel de privilegio: 15<br>R2(config)#username webuser privilege 15 secret cisco12345 |

| | |
|---|---|
| Habilitar el servicio del servidor HTTP | R2(config)#ip http server |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | R2(config)#ip http authentication local |
| Crear una NAT estática al servidor web. | Dirección global interna: 209.165.200.229<br>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 |
| Asignar la interfaz interna y externa para la NAT estática | R2(config-if)#int g0/0<br>R2(config-if)#ip nat inside<br>R2(config-if)#int s0/0/1<br>R2(config-if)#ip nat outside |
| Configurar la NAT dinámica dentro de una ACL privada | Lista de acceso: 1<br>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1<br>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255<br>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3<br>R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255<br>R2(config)#access-list 1 permit 192.168.5.0 0.0.3.255<br>R2(config)#access-list 1 permit 192.168.6.0 0.0.3.255 |
| Defina el pool de direcciones IP públicas utilizables. | Nombre del conjunto: INTERNET<br>El conjunto de direcciones incluye:<br>209.165.200.225 – 209.165.200.228<br>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 |
| Definir la traducción de NAT dinámica | R2(config)#ip nat inside source list 1 pool INTERNET |

Fuente: Actor

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

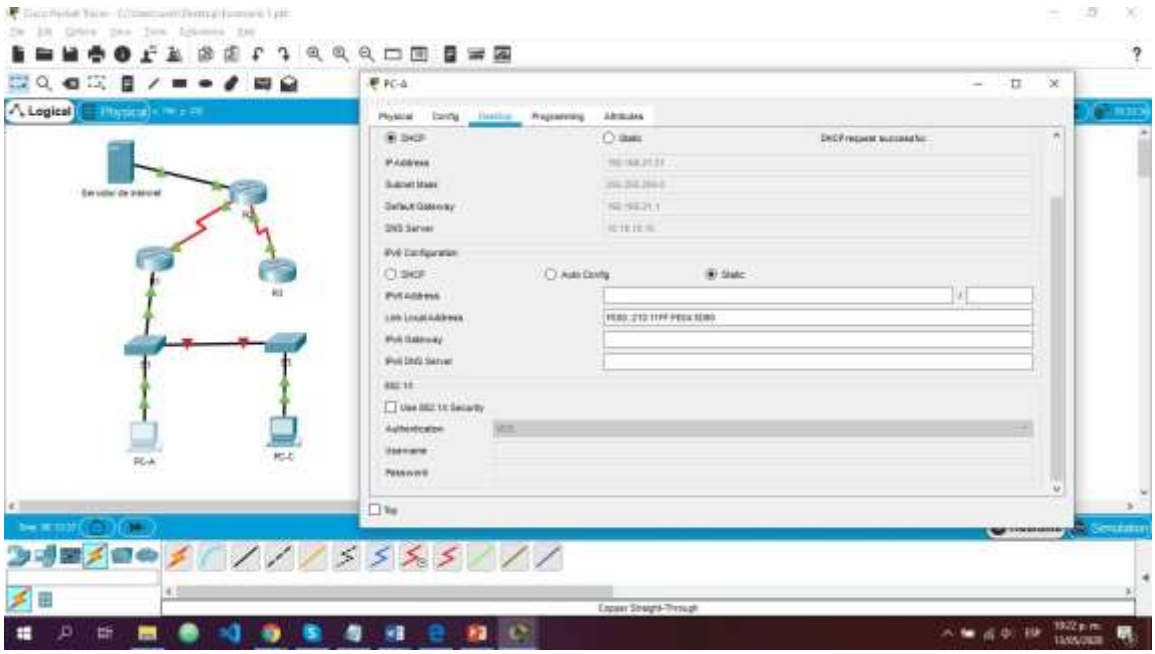
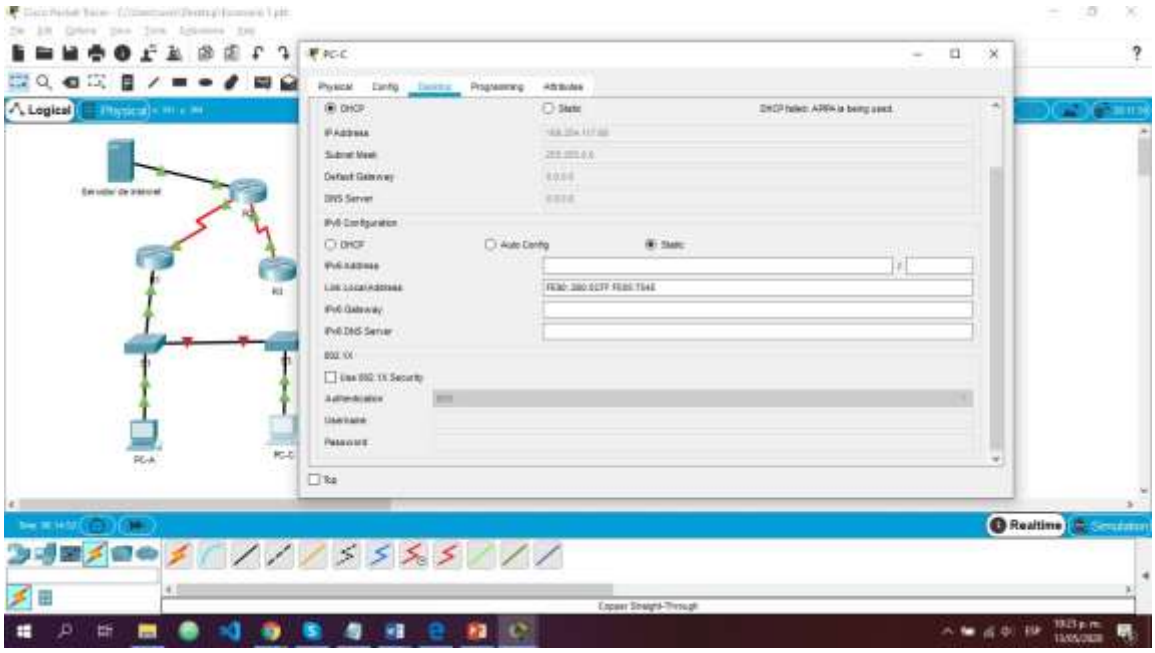
| Prueba | Resultados |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | |
| Figura 8. Evidencia Adquisición de ip del servidor DHCP<br>  <br>Fuente: Actor | |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | |

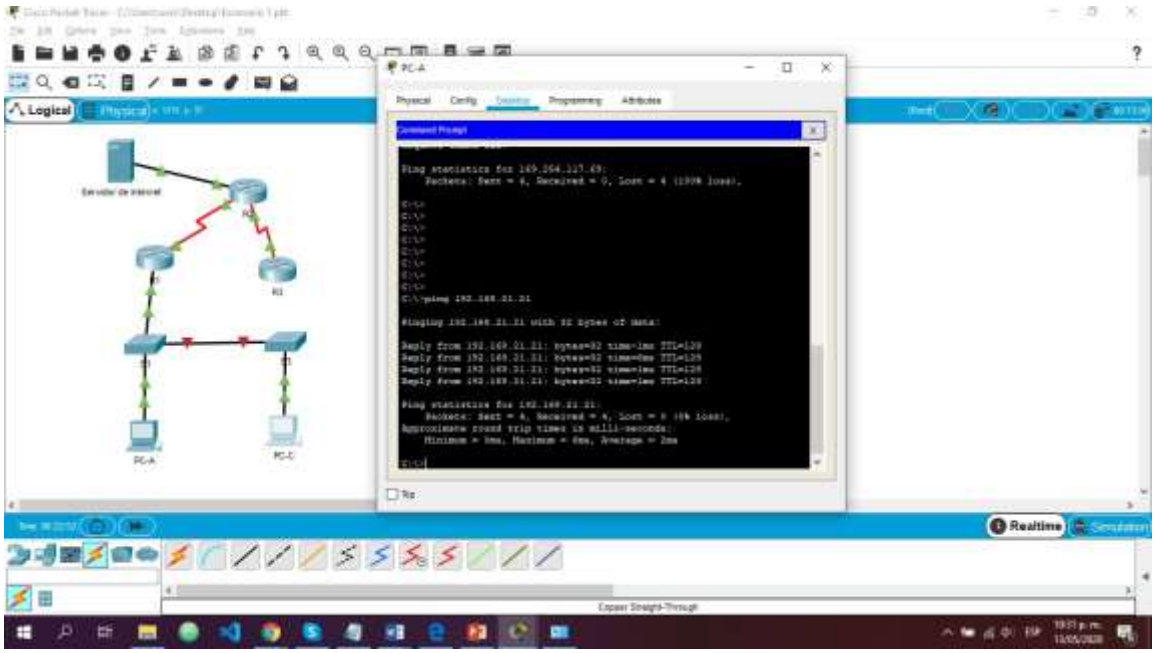
Figura 9. Evidencia de la verificación de la ip al servidor DHCP




Fuente: Actor

| | |
|---|---|
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC. | |

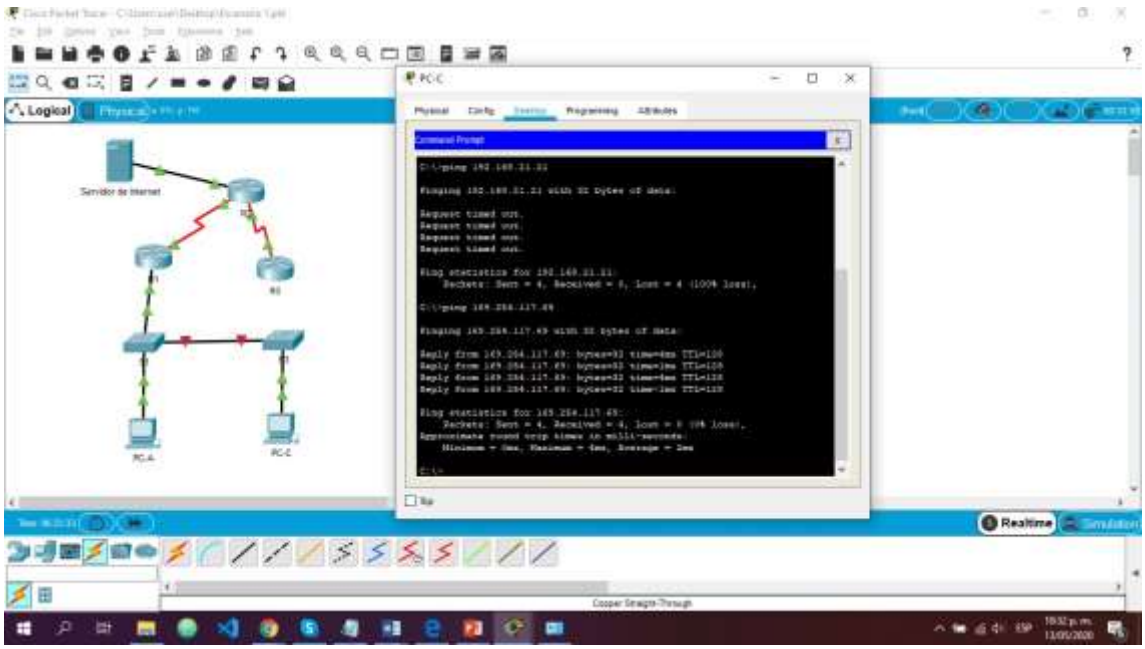
Figura 10. Evidencia del comando Ping



Fuente: Actor

| | |
|---|---|
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345** | |

Figura 11. Evidencia de Inicio de Sesión



Fuente:Actor

**Parte 6. Configurar NTP**

Tabla 23. Tabla configuración NTP

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | 5 de marzo de 2016, 9 a. m.<br>R2#clock set 09:00:00 March 5 2016 |
| Configure R2 como un maestro NTP. | Nivel de estrato: **5**<br>R2(config)#ntp master 5 |
| Configurar R1 como un cliente NTP. | Servidor: R2<br>R1(config)#ntp server 172.16.1.2 |
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | R1(config)# ntp update-calendar |
| Verifique la configuración de NTP en R1. | |

Fuente: Actor

**Parte 7: Configurar y verificar las listas de control de acceso (ACL)**

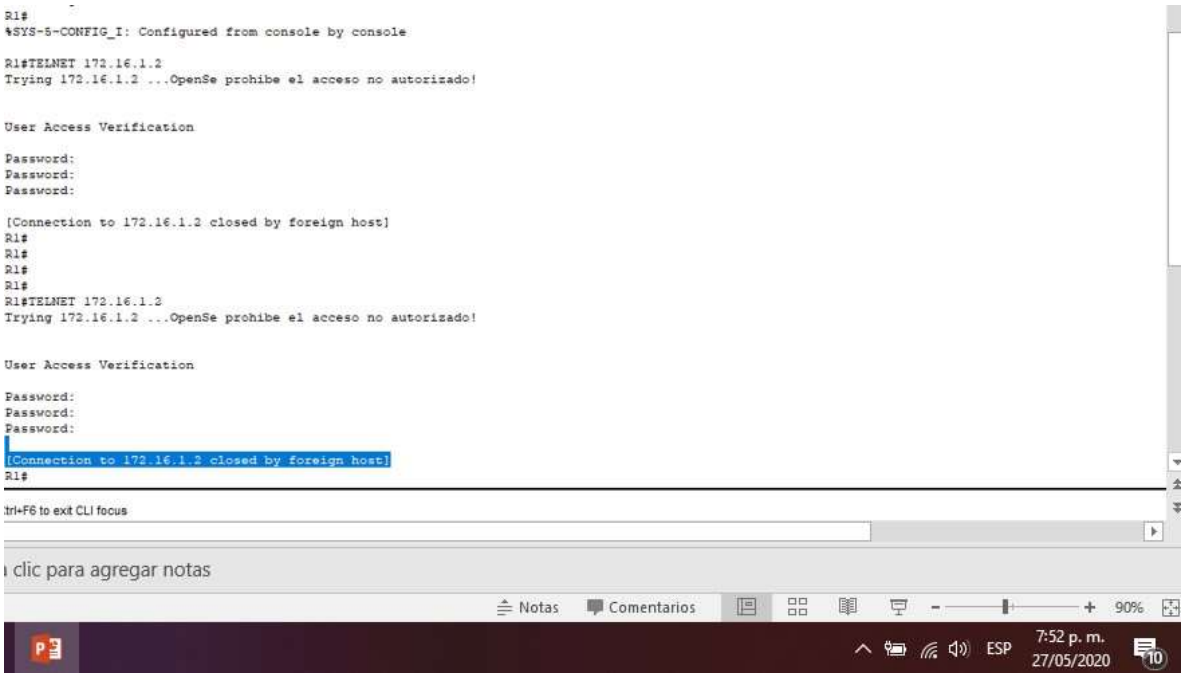
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 22. Tabla restringir acceso a las líneas VTY en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 | Nombre de la ACL: ADMIN-MGT<br>R2(config)#ip access-list standard ADMIN-MGT<br>R2(config-std nacl)#permit host 172.16.1.1 |
| Aplicar la ACL con nombre a las líneas VTY | R2(config)#line vty 0 4 |
| Permitir acceso por Telnet a las líneas de VTY | R2(config-line)#access- class ADMIN-MGT in |
| Verificar que la ACL funcione como se espera | R2#show run |

Fuente: Actor

Figura 13. Evidencia del funcionamiento de la ACL




Fuente: Actor

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 23. Comandos CLI

| Descripción del comando | Entrada del estudiante (comando) |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | R2#show running-config |

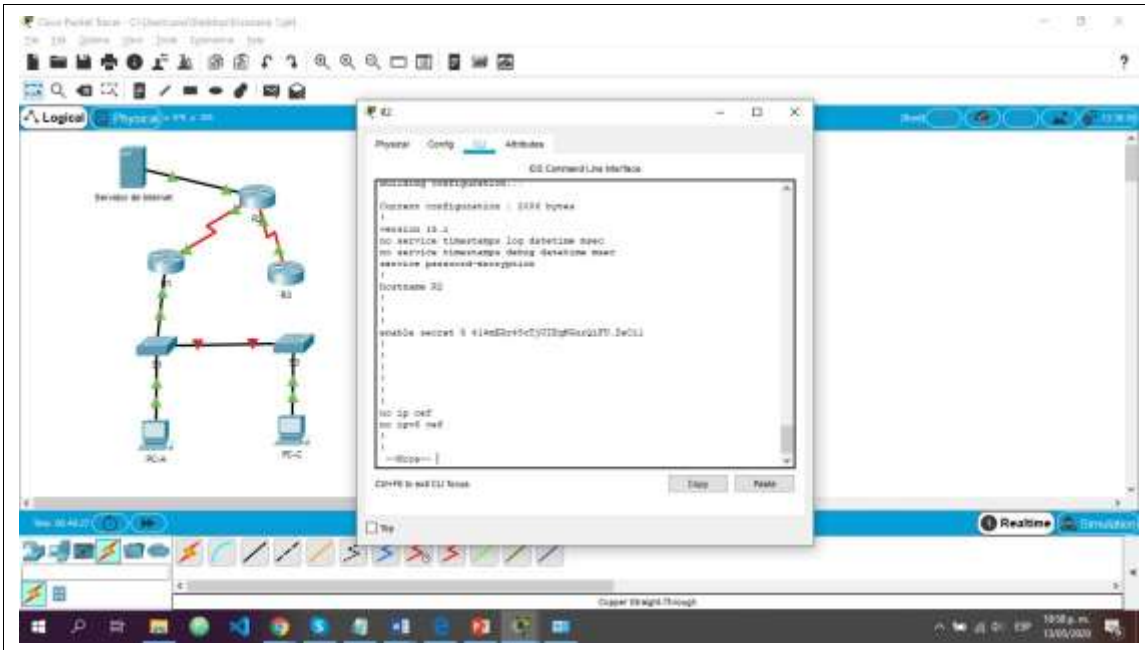


Figura 13. evidencia de la lista de acceso

| | |
|---|---|
| Restablecer los contadores de una lista de acceso | R2#clear access-list counter |
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | R2#show access-lists |

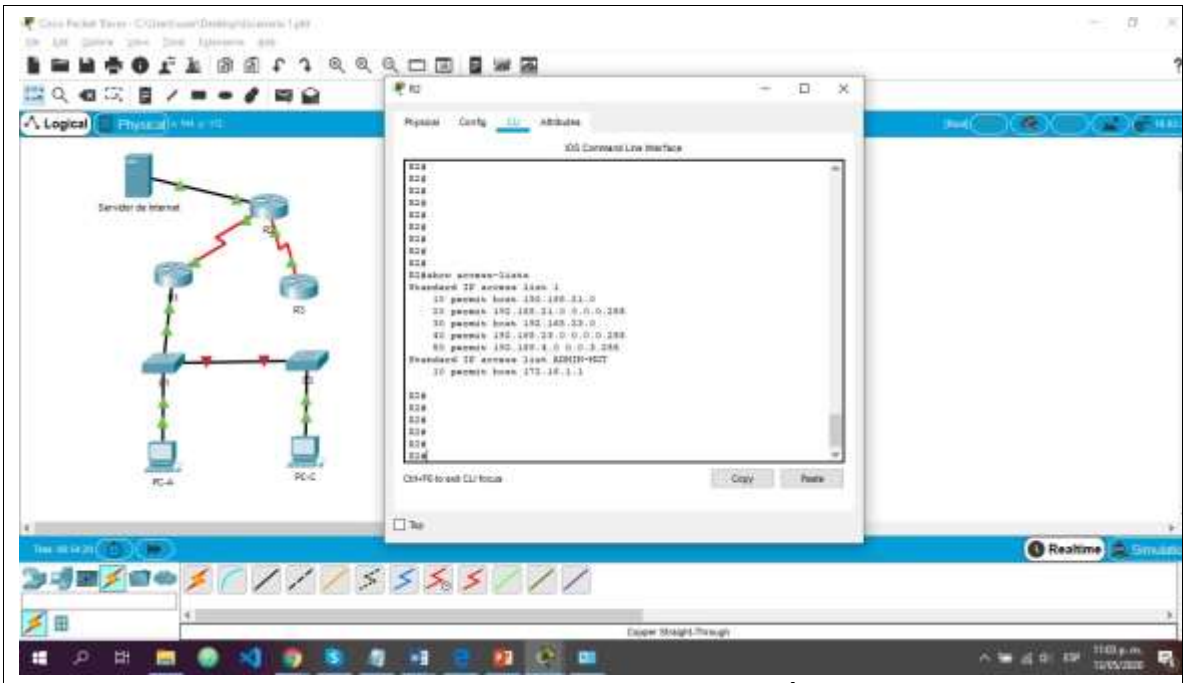



Figura 14. Evidencia de la aplicación ACL

| | |
|---|---|
| ¿Con qué comando se muestran las traducciones NAT? | **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.<br><br>R2#show ip nat translations |

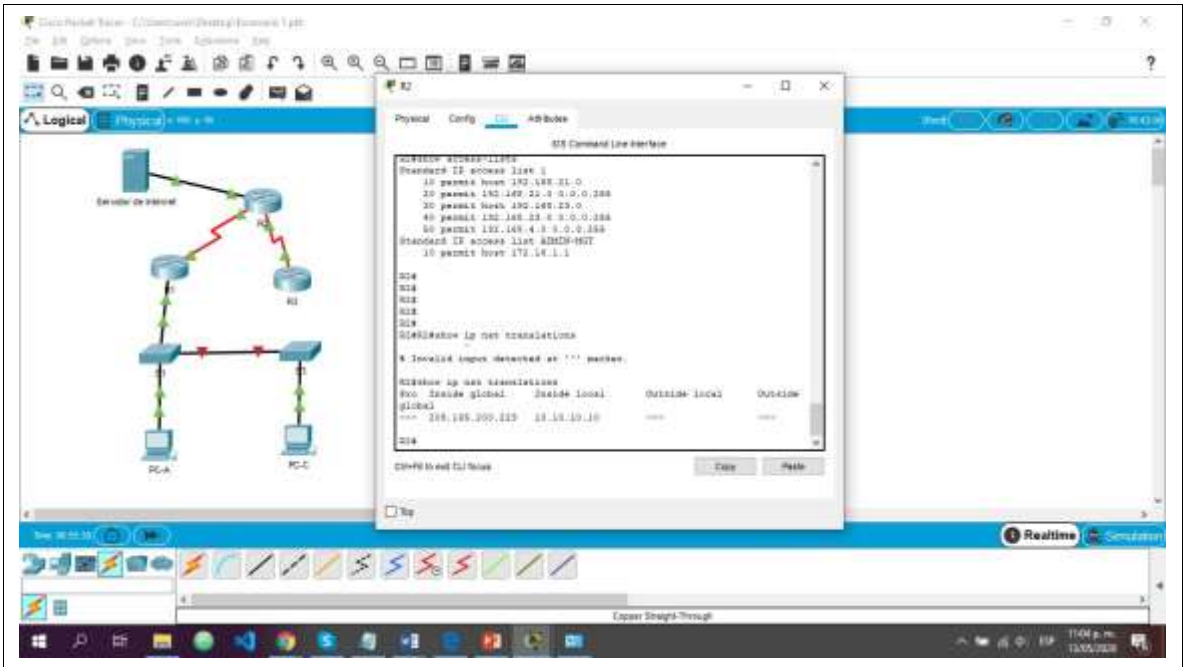


Figura 15. Verificación del comando las traducciones NAT

| | |
|---|---|
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | R2#clear ip nat translation |

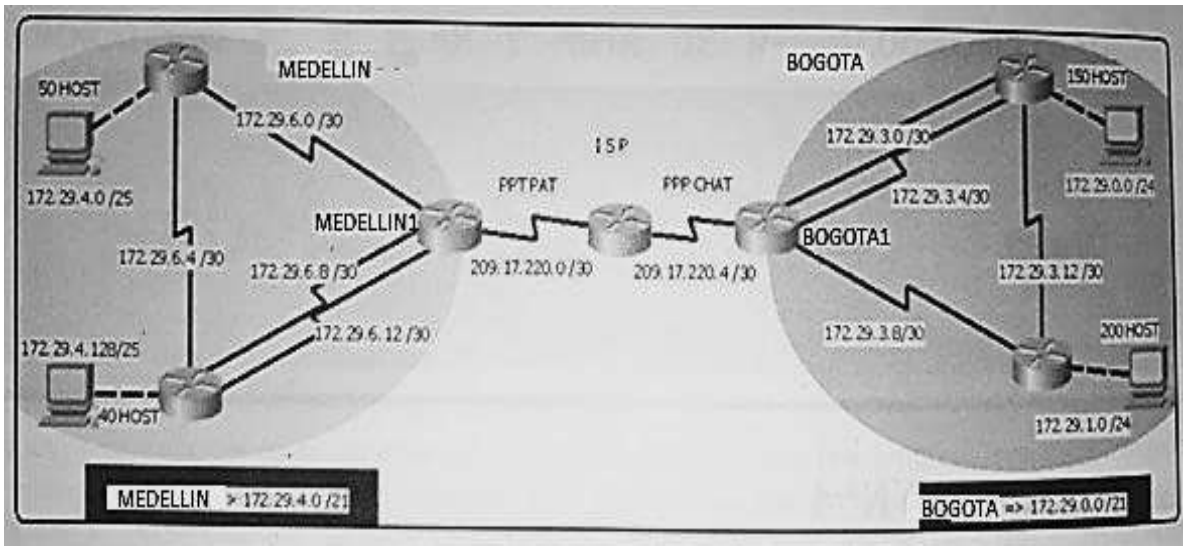
Fuente: Actor

## 4.2 ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

**Topología de red**

Figura 16. Topología de red Escenario 2




Fuente: Prueba de habilidades CCNA 2020, Cisco Academy

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

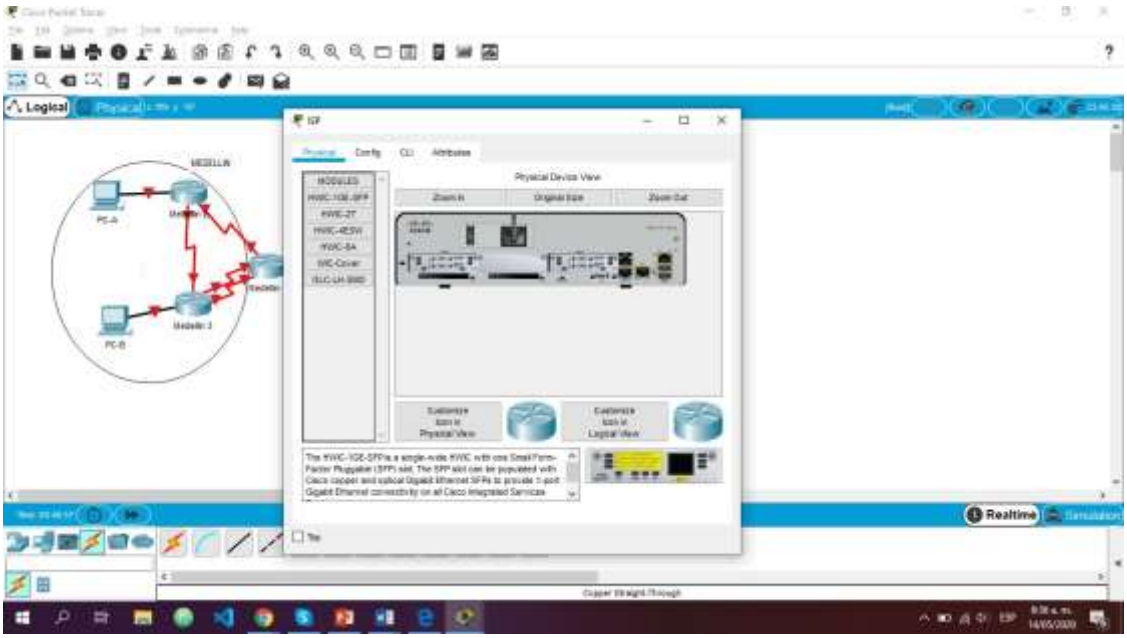
**Desarrollo**

Como trabajo inicial se debe realizar lo siguiente.

• Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Se agregan los puertos seriales a los routers

Figura 17.Topologia de la red Escenario 2 – evidencia




Fuente:Actor

Configuración del ISP

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login

ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#service password-encryption
ISP(config)#banner motd *Se prohibe el acceso no autorizado*
Configuración Medellin1

Router>enable Router
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname Medellin1
Medellin1(config)#enable secret class
Medellin1(config)#line console 0
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#line vty 0 15
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#service password-encryption
Medellin1(config)#banner motd *Se prohibe el acceso no autorizado*

Configuración Medellin2

Router>enable Router
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname Medellin2
Medellin2(config)#enable secret class
Medellin2(config)#line console 0
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#line vty 0 15
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#service password-encryption
Medellin2(config)#banner motd *Se prohibe el acceso no autorizado*

Configuración Medellin3

Router>enable Router
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname Medellin3
Medellin3(config)#enable secret class
Medellin3(config)#line console 0
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#line vty 0 15
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#service password-encryption
Medellin3(config)#banner motd *Se prohibe el acceso no autorizado*

- Realizar la conexión física de los equipos con base en la topología de red

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Tabla 24. Tabla de direccionamiento 2

| **Dispositivo** | **Interfaz** | **Dirección IP** | **Máscara de subred** | |
|---|---|---|---|---|
| ISP | S0//0/0 | 209.17.220.5 /30 | 255.255.255.252 | |
| | S0/0/1 | 209.17.220.1 / 30 | 255.255.255.252 | |
| MEDELLIN 1 | S0/0/0 | 172.29.6.13 / 30 | 255.255.255.252 | |
| | S0/0/1 | 209.17.220.2 / 30 | 255.255.255.252 | |
| | S0/1/0 | 172.29.6.9 /30 | 255.255.255.252 | |
| | S0/1/1 DCE | 172.29.6.1 / 30 | 255.255.255.252 | |

| | | | | |
|---|---|---|---|---|
| MEDELLIN 2 | G0/0 | 172.29.4.1 /25 | 255.255.255.128 | |
| | S0/0/1 DCE | 172.29.6.5 /30 | 255.255.255.252 | |
| | S0/1/1 | 172.29.6.2 /30 | 255.255.255.252 | |
| MEDELLIN 3 | G0/0 | 172.29.4.129 /25 | 255.255.255.128 | |
| | S0/0/1 | 172.29.6.6 /30 | 255.255.255.252 | |
| | S0/1/0 DCE | 172.29.6.10 /30 | 255.255.255.252 | |
| | S0/0/0 DCE | 172.29.6.14 /30 | 255.255.255.252 | |
| BOGOTA 1 | S0/0/0 | 209.17.220.6 /30 | 255.255.255.252 | |
| | S0/1/0 | 172.29.3.1 / 30 | 255.255.255.252 | |
| | S0/0/1 DCE | 172.29.3.9 /30 | 255.255.255.252 | |
| | S0/1/1 | 172.29.3.5 / 30 | 255.255.255.252 | |
| BOGOTA 2 | G0/0 | 172.29.1.1 / 24 | 255.255.255.0 | |
| | S0/0/0 DCE | 172.29.3.13 /30 | 255.255.255.252 | |
| | S0/0/1 | 172.29.3.10 /30 | 255.255.255.252 | |
| BOGOTA 3 | G0/0 | 172.29.0.1 /24 | 255.255.255.0 | |
| | S0/1/1 | 172.29.3.6 /30 | 255.255.255.252 | |
| | S0/1/0 DCE | 172.29.3.2 /30 | 255.255.255.252 | |
| | S0/0/0 | 172.29.3.14 | 255.255.255.252 | |

| | | | | |
|---|---|---|---|---|
| | | /30 | | |
| PC-A | NIC | 172.29.4.12 | 255.255.255.0 | 172.29.4.1 |
| PC-B | NIC | 172.29.4.133 | 255.255.255.0 | 172.29.4.129 |
| PC-C | NIC | 172.29.1.14 | 255.255.255.0 | 172.29.1.1 |

Fuente: Actor

ASIGNAR DIRECCIONES IP EN LAS INTERFACES DE LOS DISPOSITIVOS

ISP

```
ISP(config)#interface s0/0/0
ISP(config-if)#description conexion ISP-Bogota1
ISP(config-if)#ip address 209.17.220.5 25.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown

ISP(config-if)#int s0/0/1
ISP(config-if)#description Conexion ISP-Medellin1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown
```

BOGOTA 1

```
Bogota1(config)#interface Serial0/0/0
Bogota1(config-if)#description Conexion Bogota1-ISP
Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit

Bogota1(config)#int s0/1/0
Bogota1(config-if)#description Conexion Bogota1-Bogota3
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit

Bogota1(config)#int s0/0/1
Bogota1(config-if)#description Conexion Bogota1-Bogota2
```

```
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit

Bogota1(config)#int s0/1/1
Bogota1(config-if)#description Coneexion Bogota3
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#no shutdown
```

BOGOTA 2

```
Bogota2(config)#int g0/0
Bogota2(config-if)#description Conexion PC-C
Bogota2(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shutdown

Bogota2(config)#int s0/0/0
Bogota2(config-if)#description Conexion Bogota3
Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config)#interface S0/0/1
Bogota2(config-if)#description Conexion Bogota1
Bogota2(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota2(config-if)#no shutdown
```

BOGOTA 3

```
Bogota3(config)#interface GigabitEthernet0/0
Bogota3(config-if)#description Conexion PC-D
Bogota3(config-if)#ip address 172.29.0.1 255.255.255.0

Bogota3(config)#interface s0/1/1
Bogota3(config-if)#description Conexion Bogota1
Bogota3(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota3(config-if)#clock rate 128000
```

Bogota3(config)#int s0/1/0
Bogota3(config-if)#description Conexion Bogota1
Bogota3(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota3(config-if)#clock rate 128000

Bogota3(config-if)#int s0/0/0
Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota3(config-if)#no shutdown

MEDELLIN1

Medellin1(config)#interface Serial0/0/0
Medellin1(config-if)#description Conexion Medellin3
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.25

Medellin1(config)#interface s0/0/1
Medellin1(config-if)#description Conexion ISP
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config)# int s0/1/1
Medellin1(config-if)#description Conexion Medellin2
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 4000000

Medellin1(config-if)#description Conexion PC-A
Medellin1(config-if)#ip address 172.29.4.1 255.255.255.128

Medellin1(config)#interface s0/1/1
Medellin1(config-if)#description Conexion Medellin1
Medellin1(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit

MEDELLIN 3

Medellin3(config)#int g0/0
Medellin3(config-if)#description Conexion PC-B
Medellin3(config-if)#ip address 172.29.4.133 255.255.255.128
Medellin3(config-if)#no shutdown

```
Medellin3(config)#int s0/0/1
Medellin3(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin3(config-if)#no shutdown

Medellin3(config)#int s0/1/0
Medellin3(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin3(config-if)#no shutdown
```

Parte 1: Configuración del enrutamiento

a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

```
Medellin1(config)#route ospf 1
Medellin1(config-router)#network 172.29.6.2 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.2 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.2 0.0.0.3 area 0
Medellin1(config-router)#no auto-summary

Medellin3(config)#router ospf 1
Medellin3(config-router)#network 172.29.6.5 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.13 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.9 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.4.0 0.0.0.255 area 0
Medellin3(config-router)#no auto-cost

medellin2(config)#router ospf 1
medellin2(config-router)#network 172.29.6.1 0.0.0.3 area 0
medellin2(config-router)#network 172.29.6.1 0.0.0.3 area 0
medellin2(config-router)#network 172.29.4.0 0.0.0.255 area 0

Bogota1(config)#router ospf 1
Bogota1(config-router)#network 172.29.3.10 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.6 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.2 0.0.0.3 area 0

Bogota2(config)#router ospf 1
Bogota2(config-router)#network 172.29.3.9 0.0.0.3 area 0
```

```
Bogota2(config-router)#network 172.29.3.14 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.1.0 0.0.0.255 area 0
Bogota2(config-router)#network 172.29.1.0 0.0.0.255 area 0

Bogota3(config)#router ospf 1
Bogota3(config-router)#network 172.29.3.13 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.5 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.1 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 0
```

b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

```
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
Bogota1(config)#router ospf 1
Bogota1(config-router)#default-information originate

Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Medellin1(config)#router ospf 1
Medellin1(config-router)#default-information originate
Medellin1(config-router)#exit
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
Medellin1(config)#router ospf 1
Medellin1(config-router)#network 209.17.220.1 0.0.0.3 area 0

ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.6 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.6 0.0.0.3 area 0
```

c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

Sumarización de la Red Bogotá

Tabla 25. Sumarización Red Bogotá

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 172.29.0.0/24 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 172.29.1.0/24 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 172.29.3.0/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 172.29.3.4/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 172.29.3.8/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 172.20.3.12/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 172.29.0.0/22 |

Fuente: Actor

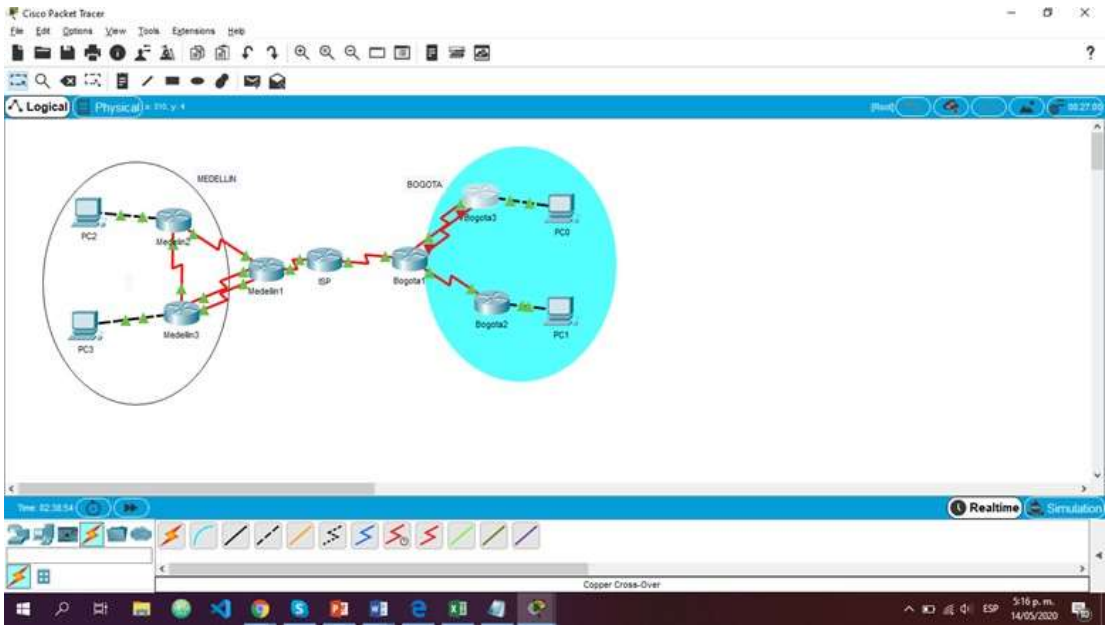
Sumarización de la red Medellín

Tabla 26. Sumarización Medellín

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 172.29.4.0/25 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 172.29.4.128/25 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 172.29.6.0/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 172.20.6.4/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 172.20.6.8/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 172.20.6.12/30 |
| 172 | 29 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 172.29.4.0/22 |

Fuente: Actor

Figura 18. conexión de los dispositivos




Fuente: Actor

**Parte 2: Tabla de Enrutamiento**.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

b. Verificar el balanceo de carga que presentan los routers.

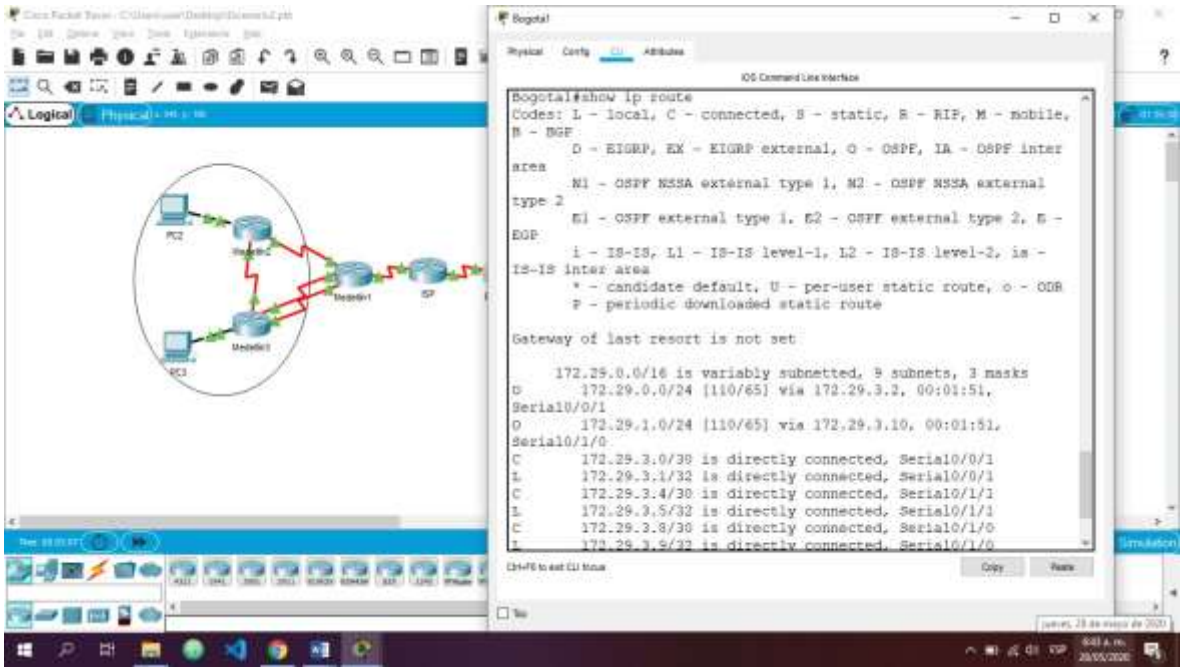
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

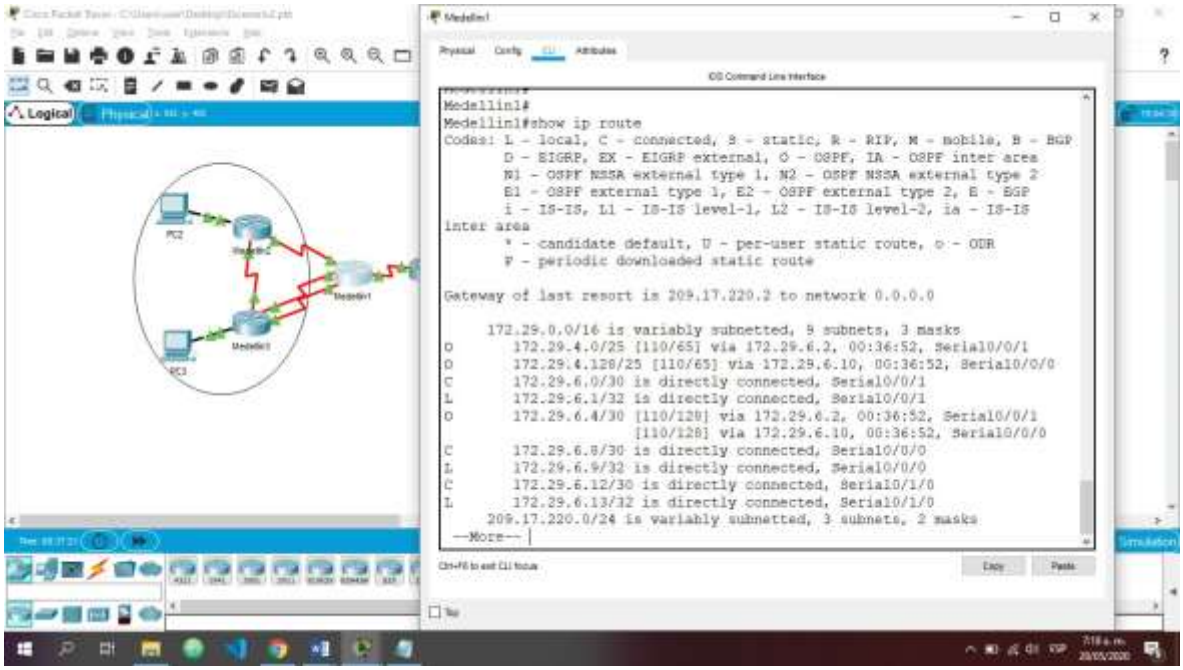
f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Figura 19. verificación de la tabla de enrutamiento Bogotá1




Fuente: Actor

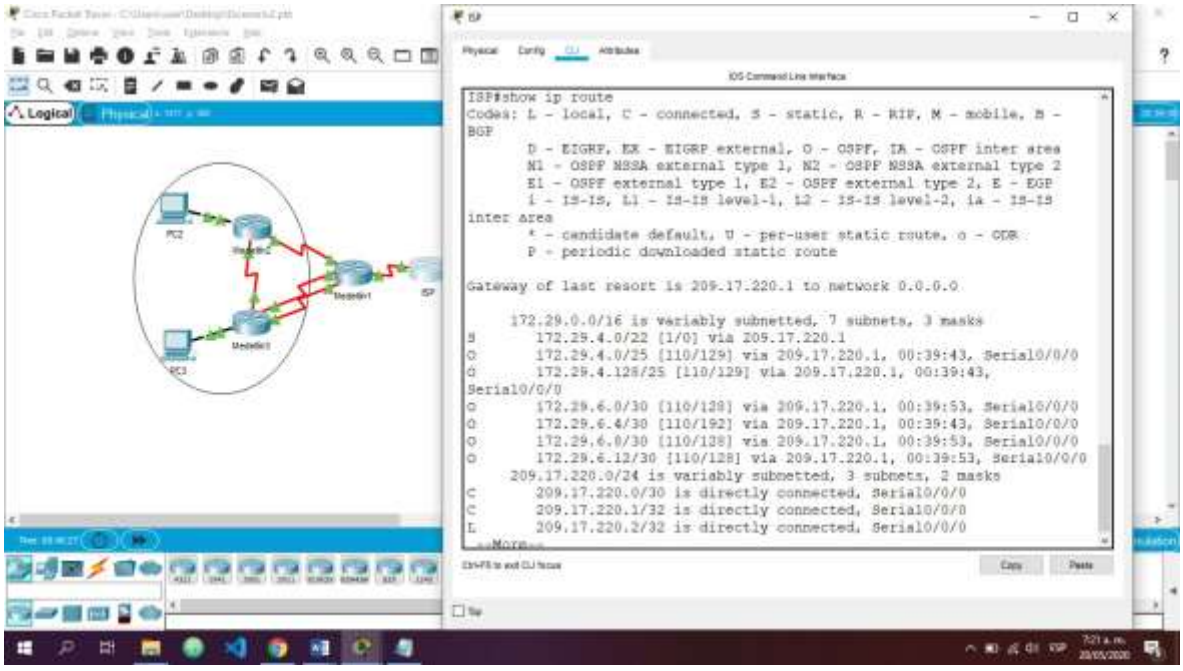
Figura 20. verificación de la tabla de enrutamiento Medellin1




Fuente: Actor

Figura 21. verificación de la tabla de enrutamiento ISP

.




Fuente: Actor

Parte 3: Deshabilitar la propagación del protocolo OSPF.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 27. Tabla de interfaces del router

| ROUTER | INTERFAZ |
|---|---|
| Bogota1 | SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1 |
| Bogota2 | SERIAL0/0/0; SERIAL0/0/1 |
| Bogota3 | SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0 |
| Medellín1 | SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1 |
| Medellín2 | SERIAL0/0/0; SERIAL0/0/1 |
| Medellín3 | SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0 |
| ISP | No lo require |

Fuente: Actor

Configuración Bogota1

```
Bogota1#Enable
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Bogota1(config)#router ospf 1
Bogota1(config-router)#passive-interface s0/1/1
Bogota1(config-router)#Exit
```

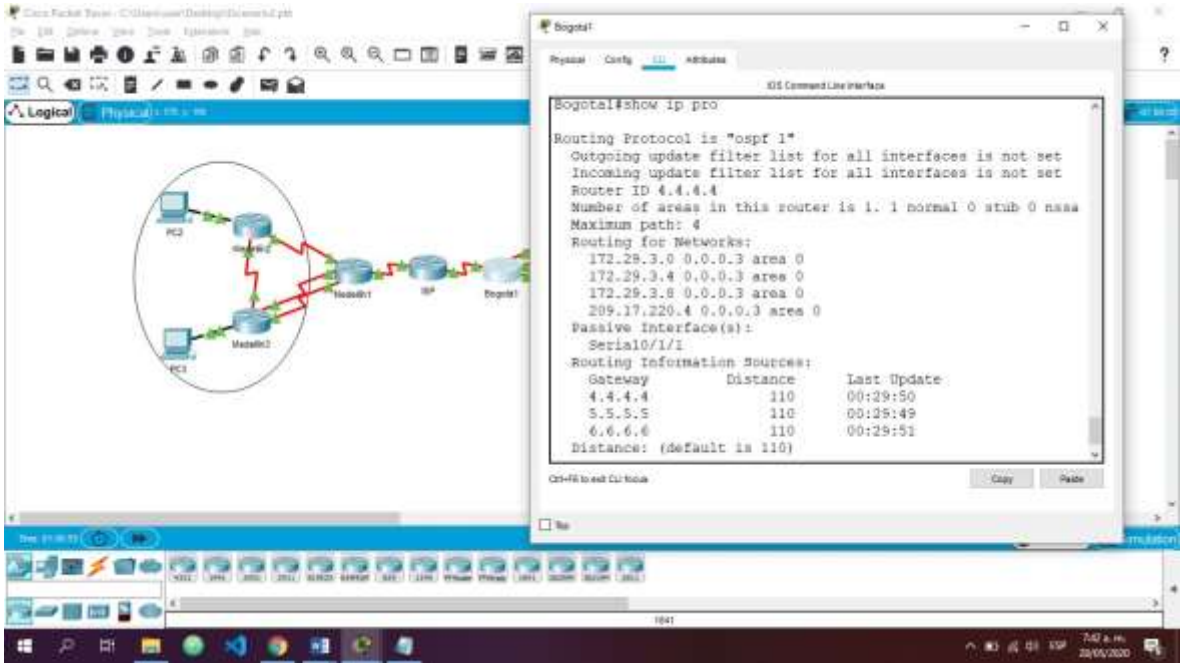
Configuración Medellin1

```
Medellin1#enable
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Medellin1(config)#router ospf 1
Medellin1(config-router)#passive-interface s0/1/0
Medellin1(config-router)#Exit
```

**Parte 4: Verificación del protocolo OSPF.**

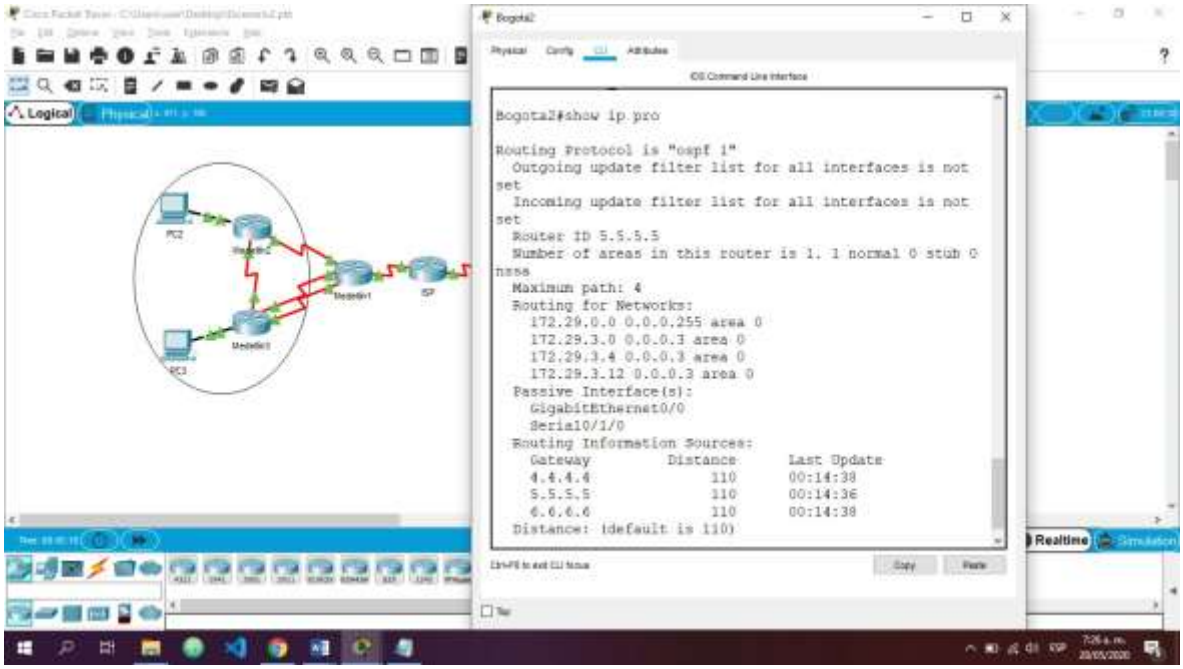
a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Figura 22. Verificar el comando de enrutamiento Bogota1



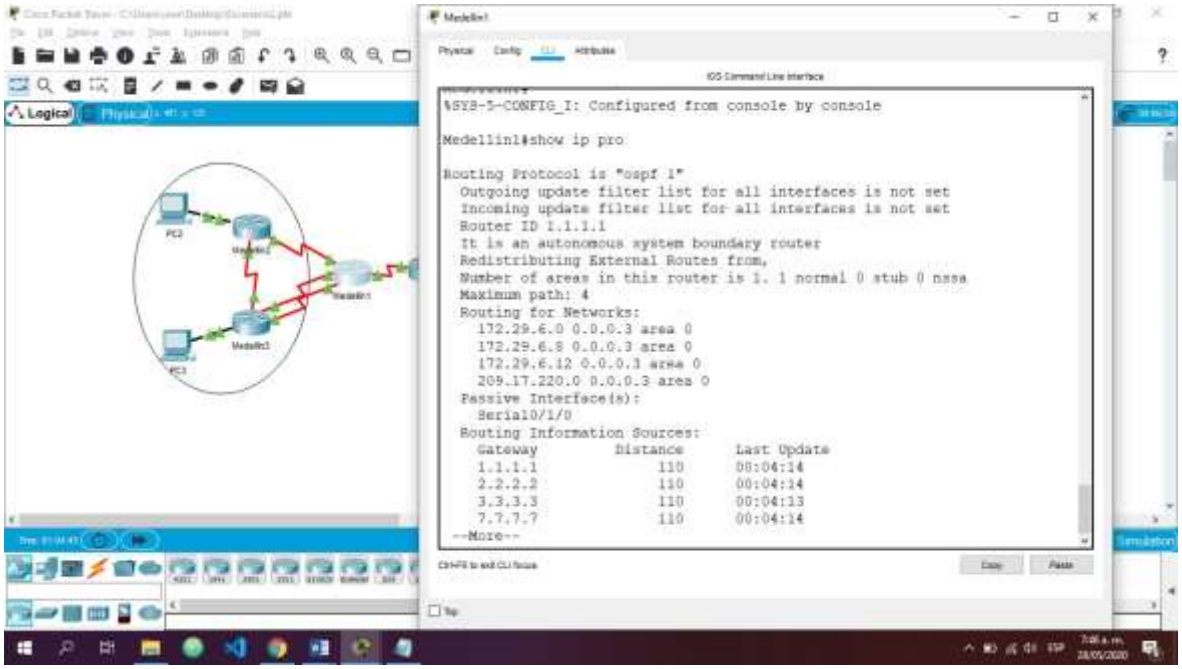

Fuente: Autor

Figura 23. verificar el comando de enrutamiento Bogotá2



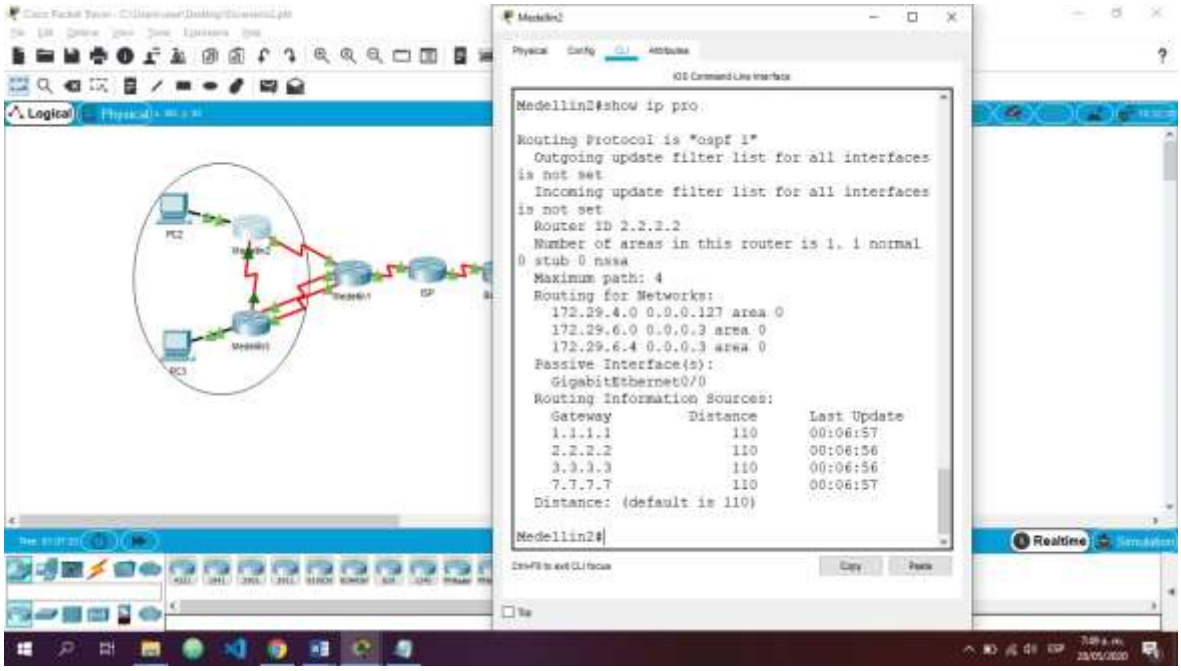

Fuente: Actor

Figura 24. Verificar el comando de enrutamiento Medellin1



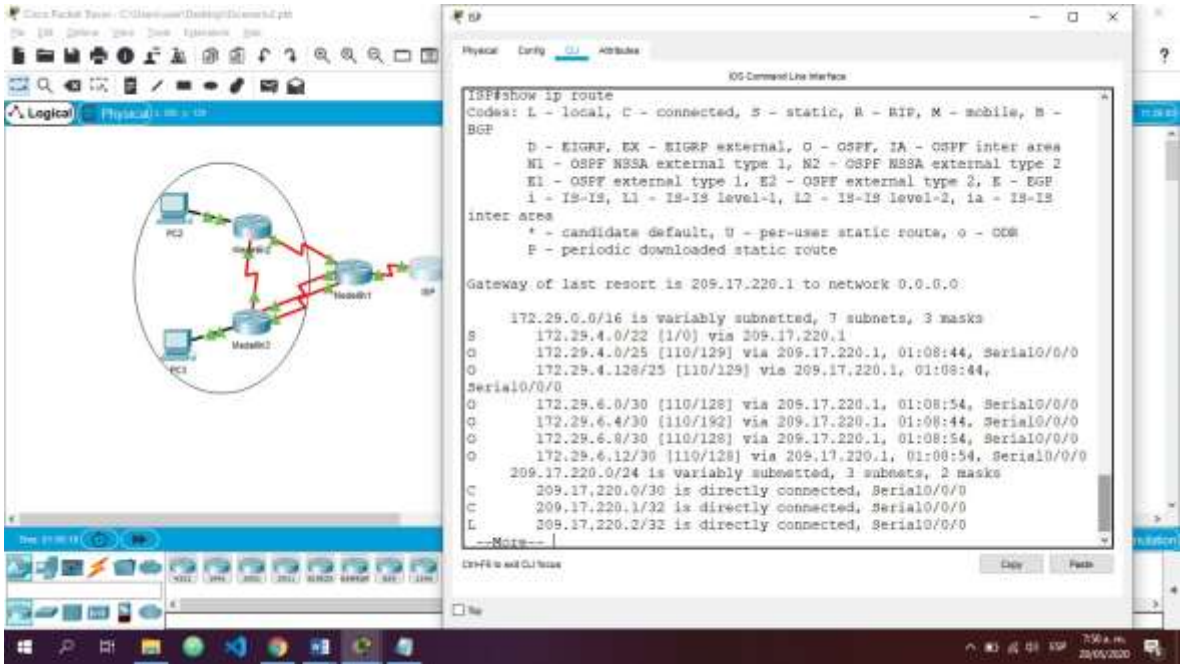

Fuente: Actor

Figura 25. Verificar el comando de enrutamiento Medellin2



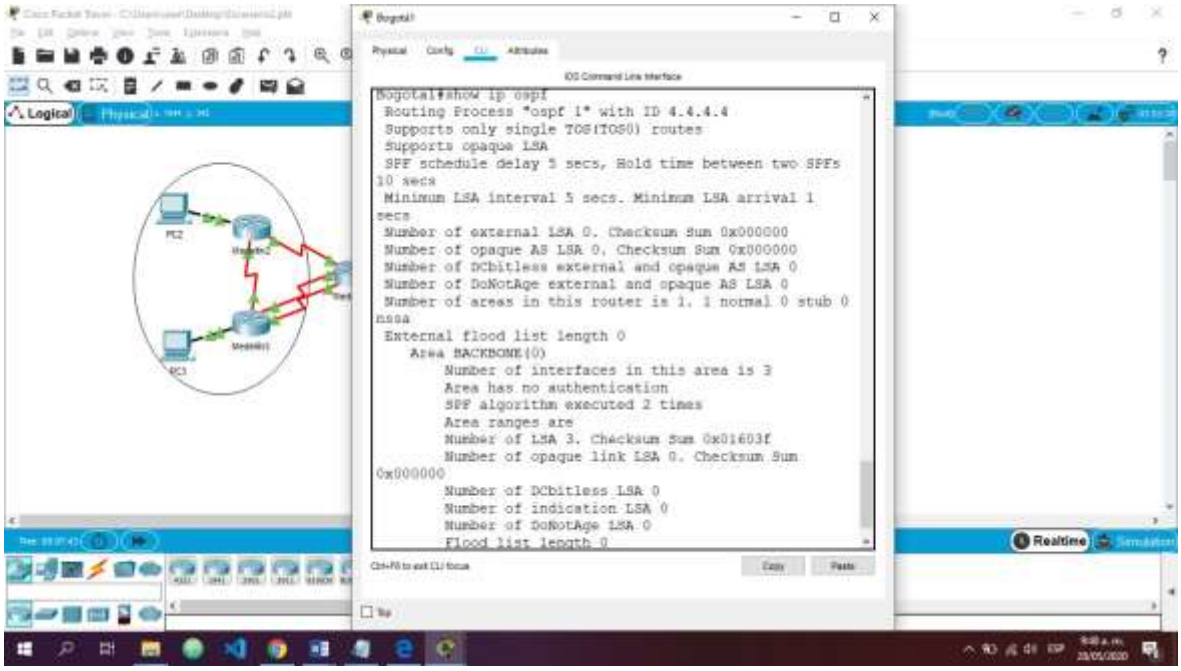

Fuente: Actor

Figura 26. Verificar el comando de enrutamiento ISP



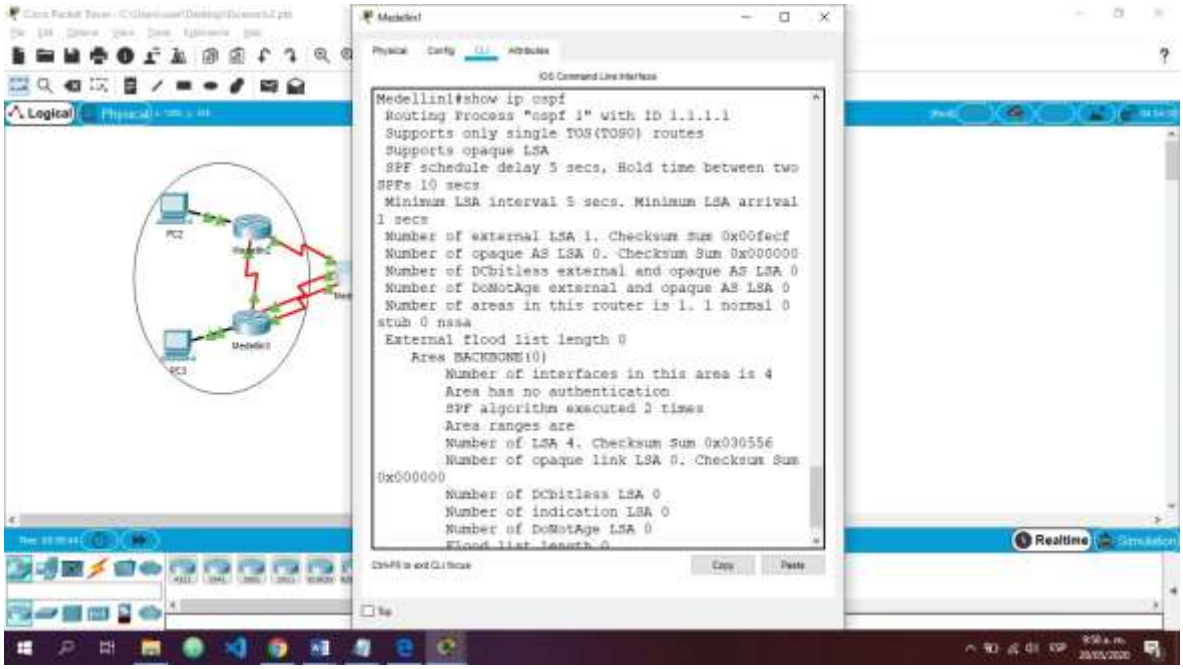

Fuente: Actor

Figura 27. Verificación del comando para evidenciar el enrutamiento Bogota1



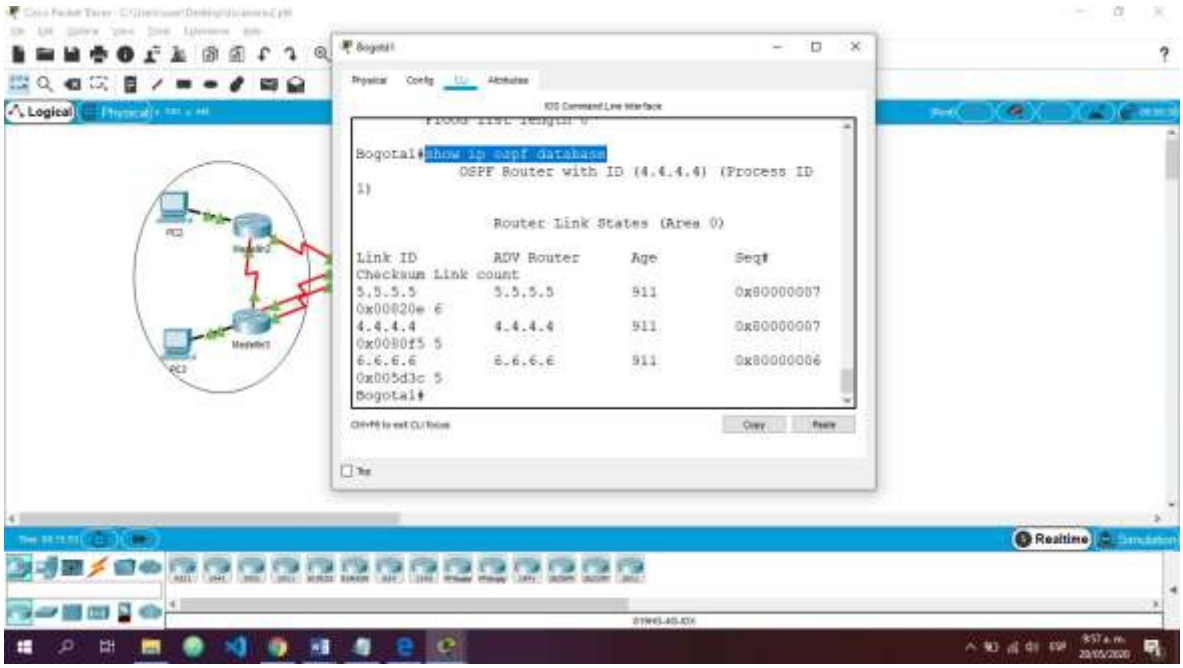

Fuente: Actor

Figura 28. Verificación del comando para evidenciar el enrutamiento Medellin1



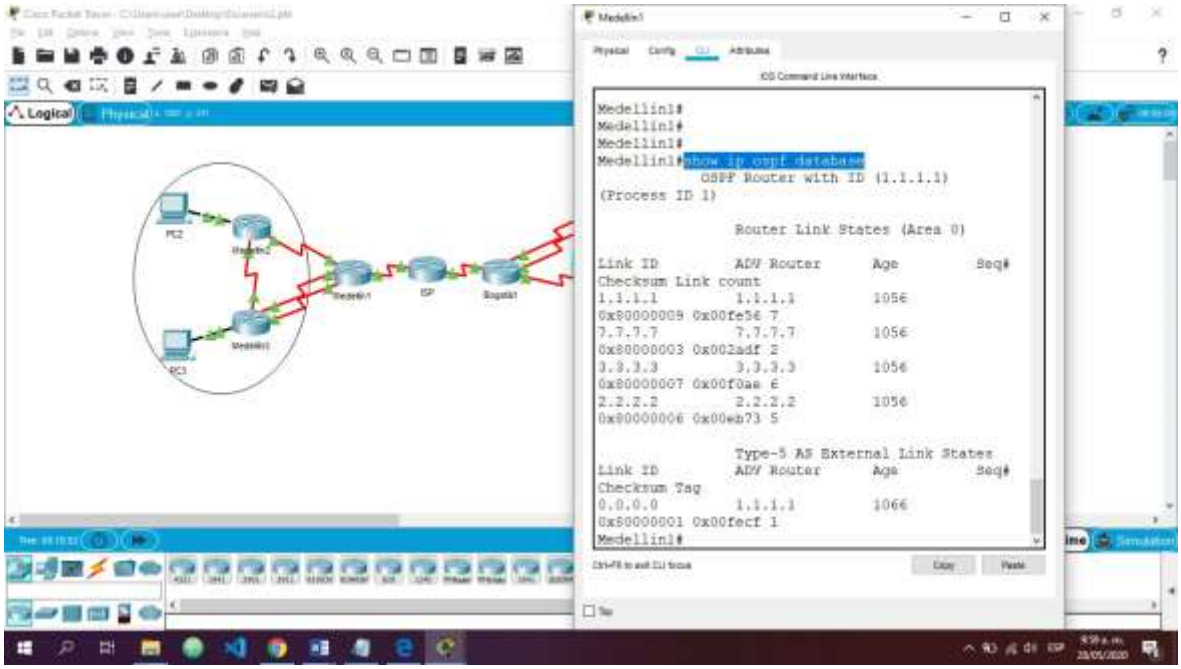

Fuente: Actor1

Figura 29. Verificación de la base de datos OPSF en el Router Bogota1




Fuente: Actor

Figura 30. Verificación de la base de datos OPSF en el Router Medellin1




Fuente: Actor

**Parte 5: Configurar encapsulamiento y autenticación PPP.**

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

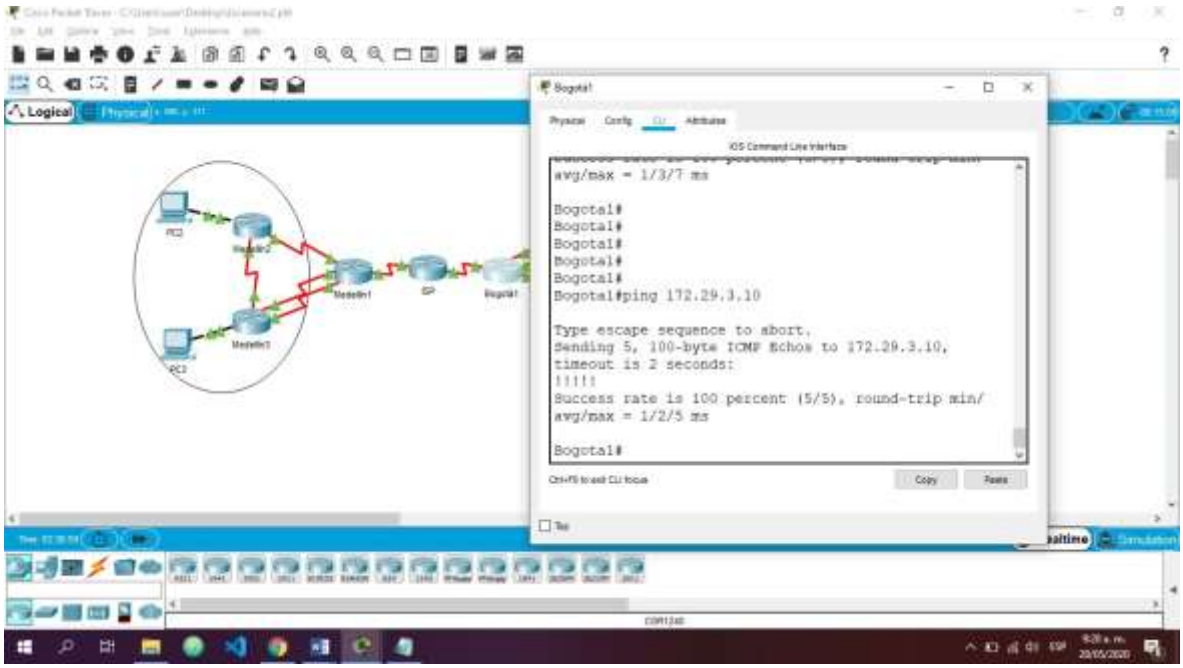
```
Medellin1#Enable
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#username ISP Password 12345
Medellin1 (config)#interface S0/0/1
Medellin1(config-if)#encapsulation ppp
Medellin1 (config-if)#ppp authentication pap
Medellin1 (config-if)#ppp pap sent-username Medellin1
Medellin1(config-if)#exit
```

b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

```
Bogota1#Enable
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#username ISP password 12345
Bogota1(config)#int s0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#exit
```

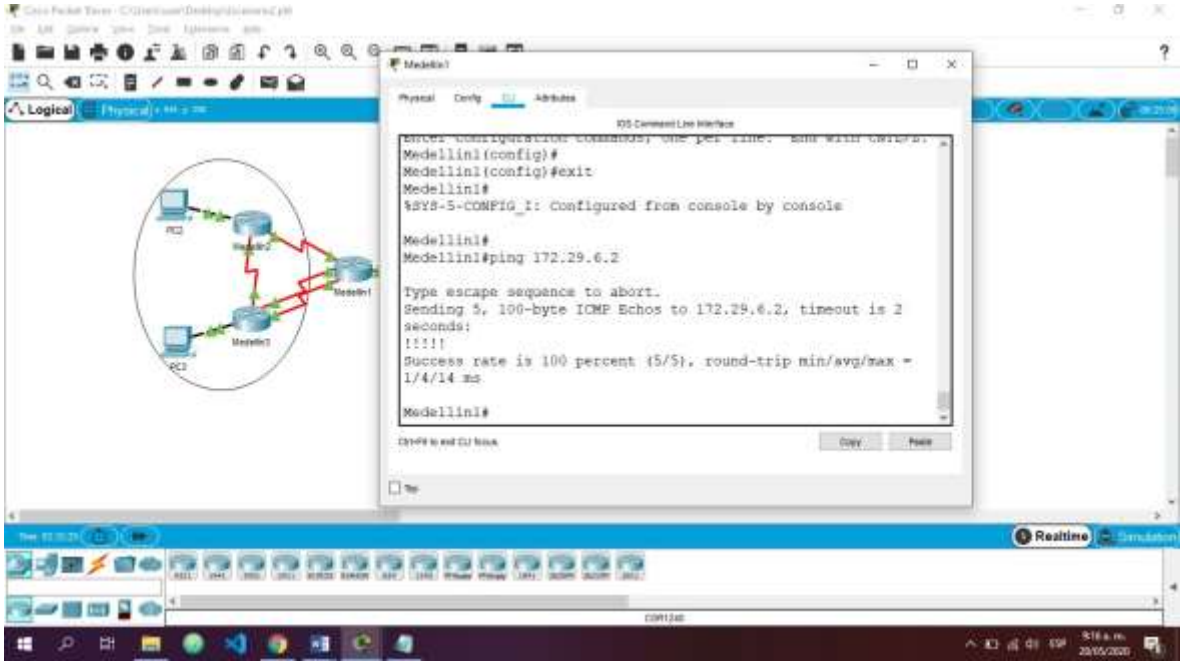
```
ISP#Enable
ISP#configure terminal
ISP(config)#username ISP password 12345
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
```

Figura 31. Verificación Ping a Bogota1




Fuente: Actor

Figura 32. Verificación del Ping a Medellin1




Fuente: Actor

**Parte 6: Configuración de PAT.**

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

Medellin1#show ip nat nat translations

c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Configuración Bogotá1

```
Bogota1#Enable
Bogota1#configure terminal
Bogota1(config)#ip access-list standard host
Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
Bogota1(config-std-nacl)#exit
Bogota1(config)#ip nat inside source list Host interface s0/0/0 overload
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#exit
Bogota1(config)#int s0/0/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/1
Bogota1(config-if)#ip nat inside
```

Bogota1(config-if)#exit

Configuración Medellin1

Medellin1#Enable
Medellin1#configure terminal
Medellin1(config)#ip access-list standard host
Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
Medellin1(config-std-nacl)#exit
Medellin1(config)#ip nat inside source list HOST interface s0/1/1 overload
Medellin1(config)#int s0/0/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#int s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/1
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#exit
Medellin1(config)#exit

**Parte 7: Configuración del servicio DHCP.**

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan

```
Medellin2#Enable
Medellin2#configure terminal
Medellin2(config)# ip dhcp excluded-address 172.29.4.1 172.29.4.9
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138
Medellin2(config)# ip dhcp pool MED-SERVIDOR_DHCP
Medellin2(config)# Network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#Default-router 172.29.4.1
Medellin2(dhcp-config)# dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
```

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

```
Medellin3#Enable
Medellin3#configure terminal
Medellin3(config)#int g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
Medellin3(config-if)#exit
```

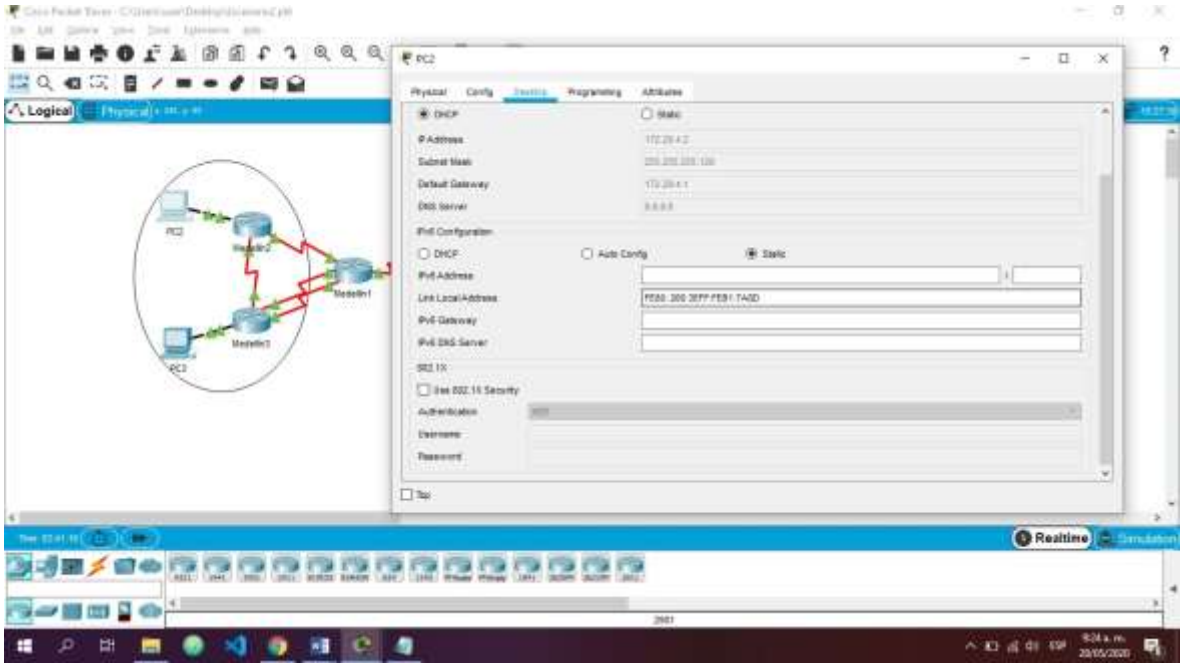
c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

```
Bogota2#Enable
Bogota2#configure terminal
Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
Bogota2(config)#ip dhcp pool Bog-Servido_dhcp
Bogota2(dhcp-config)#Network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.4.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#exit
```

Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2

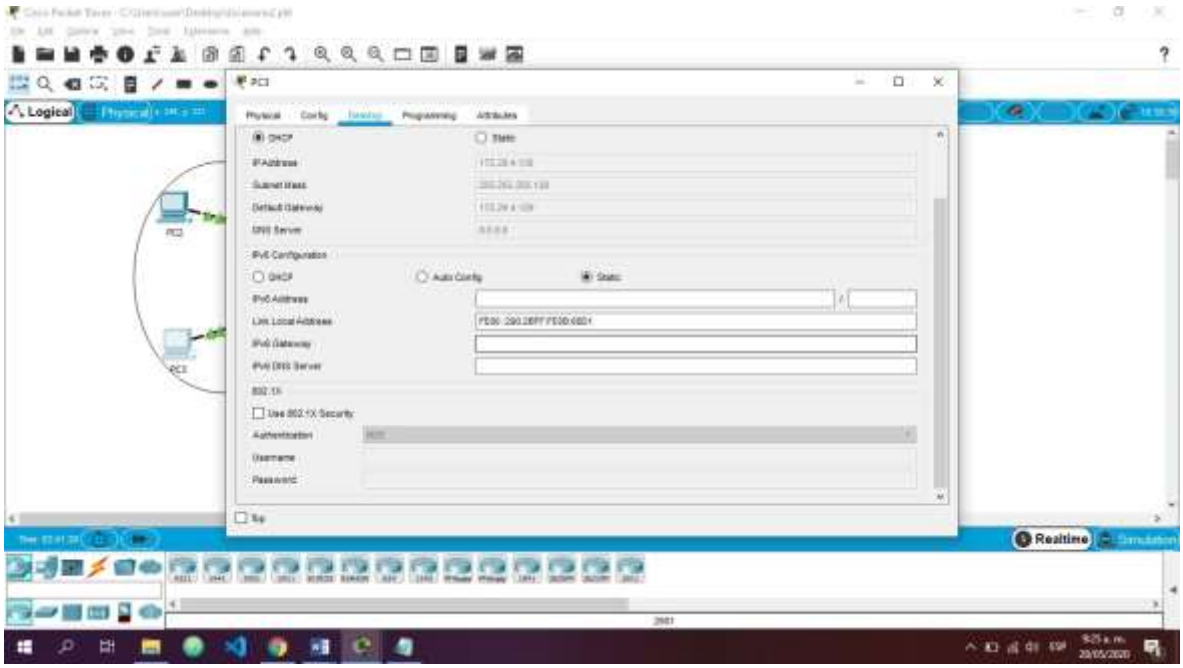
Bogota1#configure terminal
Bogota1(config)#int g0/0
Bogota1(config-if)#ip helper-address 172.29.3.13
Bogota1(config-if)#exit

Figura 33. Configuración de la PC2



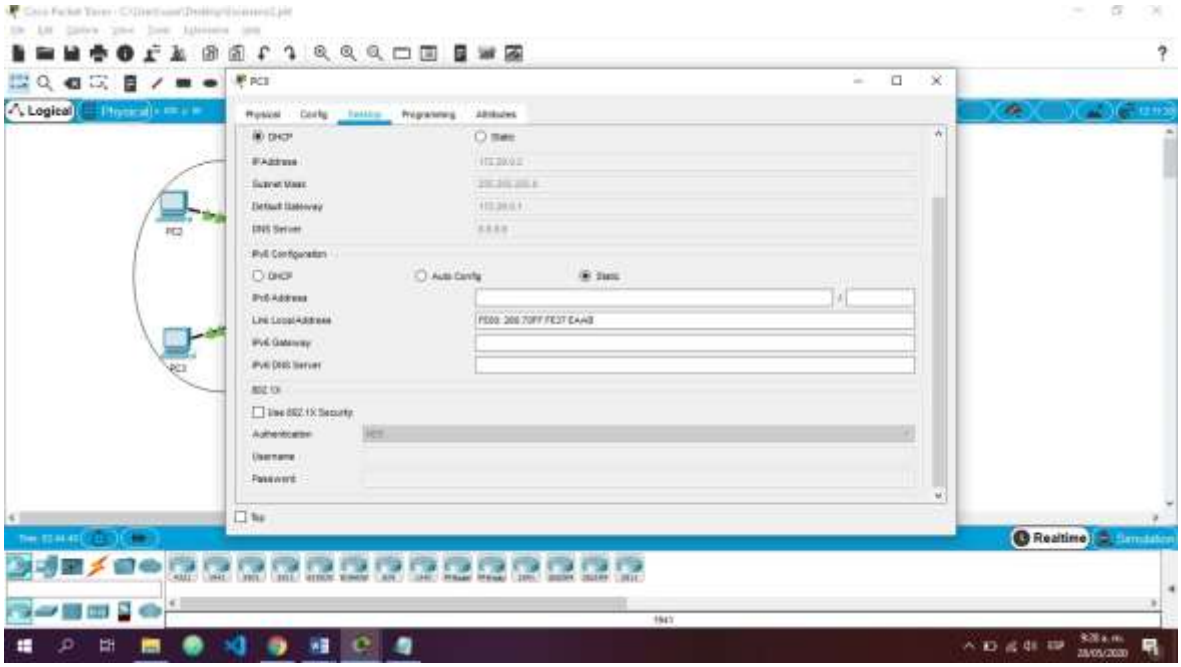

Fuente: Actor

Figura 34. Configuración de la PC3



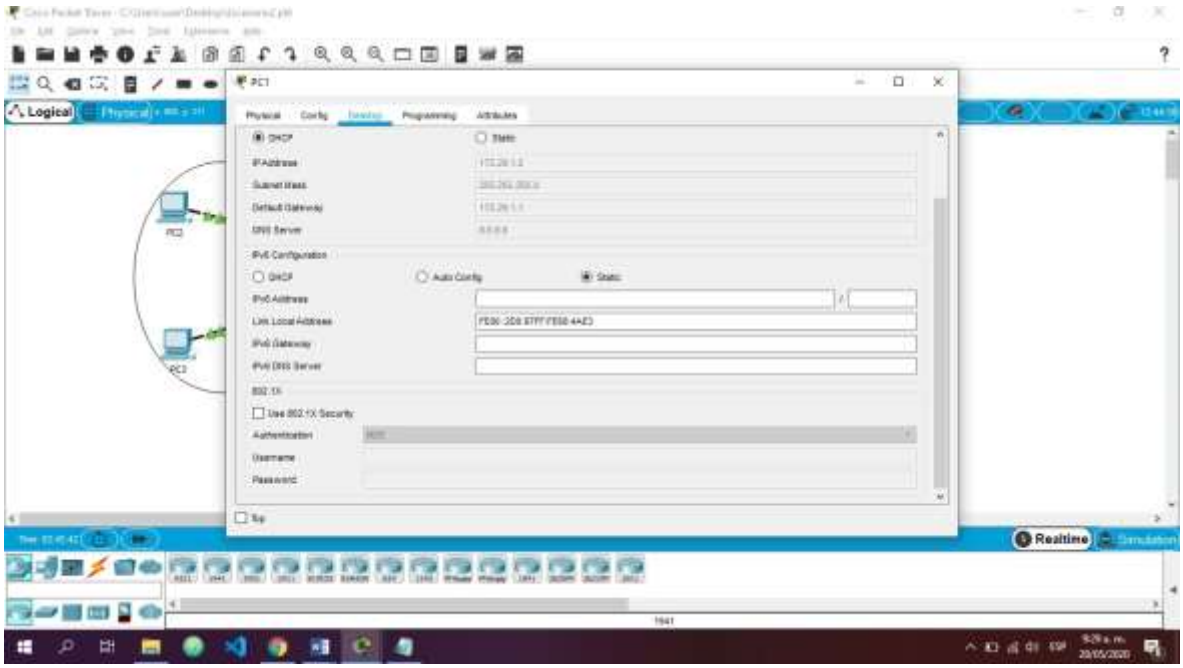
Fuente: Actor

Figura 35. Configuración PC0



Fuente: Actor

Figura 36. Configuración PC1




Fuente: Actor

# CONCLUSIONES

Con la realización de los 2 escenarios de cisco se logró identificar los diferentes comandos necesarios para el correcto funcionamiento de los ejercicios de acuerdo a las necesidades de cada ejercicio, garantizando la correcta configuración de los dispositivos de red de acuerdo a lo solicitado en la guía, identificando y comprendiendo los protocolos de seguridad de una red.

Con OSPF, no hay limitación para el conteo de saltos ya que permite una definición lógica de redes en la que los routers se pueden dividir en áreas

Los protocolos RIP nos permiten intercambiar información con las IP que se encuentran conectadas verificando el correcto funcionando de enrutamiento OSPF.

Con la utilización de DHCP, nos permite asignar automáticamente las direcciones IP en cada uno de los equipos, comunicándose de manera eficiente a los puntos finales.

Con la utilización de la NAT habilitamos la comunicación entre las redes internas.

BIBLIOGRAFIAS


- CISCO. (2019). Routing and switching de CCNA1 I-2019: Routing and switching. Introducción a las redes.Recuperado de https://1314297.netacad.com/courses/792191

- CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

- Colaboradores de Wikipedia. (2019b, 30 abril). Máscara de red - Wikipedia, la enciclopedia libre. Recuperado 5 junio, 2019, de https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

- Victor E. Martinez G, V. E. M. (2015, 22 abril). Configuración de RIPv2 (protocolo dinámico). Recuperado 5 junio, 2019, de http://theosnews.com/2013/02/configuracion-de-ripv2-protocolo-dinamico/