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

ELSA YANETH GONZALEZ MUÑOZ

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

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

ELSA YANETH GONZALEZ MUÑOZ

Trabajo final para optar por el título de Ingeniería de Sistemas

TUTOR
DIEGO EDINSON RAMIREZ

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

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Tunja 22, 05, 2020

Dedico este trabajo a mis padres y hermanos por su trabajo y comprensión, a mi novio por su apoyo incondicional a lo largo de esta carrera, para lograr cumplir mis objetivos y poder superar con éxito los obstáculos que se presentaron.

AGRADECIMIENTOS

Primeramente, agradecer a Dios y a María Santísima por el don de la vida y salud, para poder llegar a este punto, a mi familia por apoyarmen siempre y cada uno de mis compañeros que también fueron parte importante en este proceso.

A la Universidad Nacional Abierta y a Distancia, por abrirme sus puertas y a su red de tutores por impartir sus conocimientos y así lograr cumplir un sueño de superación personal.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág

LISTA DE ANEXOS

GLOSARIO

CISCO: Es una empresa de origen estadounidense principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones

RED: conjunto de elementos como cables, conductores que sirven para la comunicación entre computadores.

RED LAN: Red de computadoras que abarca un área reducida

RED WAN: Una red de área amplia, (Wide Área Network), es una que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

DHCP:(Dynamic Host Configuration Protocol, protocolo de configuración de host dinámico), protocolo que permite a un dispositivo que navegue por internet poder obtener la configuración de red de forma automática y consecutiva.

DNS: Domain Name System (sistema de nombres de dominio), es el sistema que permite resolver nombres de una red, sin necesidad de conocer la IP.

ROUTER: conocido también como enrutador es un dispositivo que opera en capa tres de nivel tres. Así permite que varias redes u ordenadores conecten entre sí.

SWITCH: es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI.

GATEWAY: Es la puerta de enlace en una red, la cual permite la conexión a redes diferentes a la red interna del contexto.

INTERFAZ: En redes, el término se utiliza para mencionar cierto conector, que permite enviar y recibir paquetes.

IP: Protocolo de internet, elemento lógico que permite enviar y recibir datos mediante una red.

RESUMEN

El presente trabajo forma porte del Diplomado de Profundización CCNA, que busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo de este diplomado; consiste en desarrollar dos escenarios propuestos, configurándolos mediante la herramienta Packet Tracer, se desarrollaron teniendo en cuenta los conceptos básicos de la redes y de las nuevas tecnologías de la información y aplicando todos los conocimientos adquiridos en este diplomado; encontramos diferentes actividades como la configuración de cada uno de los dispositivos y describiendo detalladamente el paso a paso de las etapas realizadas; lo anterior con el fin que los profesionales profundicen en el campo de las Redes y Telecomunicaciones practicando con el uso de herramientas de simulación, aplicando comandos reales en diferentes dispositivos de red, mediante la interfaz de línea de comandos (CLI).

PALABRAS CLAVE: Diplomado, CISCO CCNA, Trabajo de grado, Packet Tracer, Router, Switch, Direccionamiento, Redes, IPv4, IPv6, DHCP, LAN, WAN.

1. INTRODUCCIÓN

A través de la prueba de habilidades se busca establecer los conocimientos adquiridos en el transcurso del diplomado de profundización Cisco (diseño e implementación de soluciones integradas LAN/WAN), en este documento se desarrollarán los 2 escenarios propuestos, donde se implementarán diferentes comandos para la configuración de los dispositivos bajo la tecnología de Cisco para el cual utilizaremos el software Packet Tracer.

Esta práctica es muy importante tanto a nivel profesional como personal, puesto que con la obtención de la certificación CCNA, nos permite abrir puertas en el mundo laboral, como bien sabemos en la actualidad las empresas en general están en busca de personal calificado para desempeñar labores de administración de redes de comunicaciones seguras.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Analizar y desarrollar los dos escenarios propuestos, aplicando los conocimientos adquiridos a lo largo del Diplomado de Profundización CCNA y utilizando la herramienta de simulación Packet Tracer

2.2 OBJETIVOS ESPECÍFICOS

Diseñar las topologías de red propuestas para el desarrollo de esta actividad.

Realizar las configuraciones solicitadas para cada uno de los dispositivos que hacen parte de la topología como los son Servidor, Router, Switch y PCs.

Realizar las conexiones adecuadas para cada caso según lo solicitado y verificar su correcto funcionamiento.

Generar el informe y las evidencias del desarrollo de la actividad.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Escenario 1: 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.

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.

3.2 JUSTIFICACIÓN

El desarrollo de los dos escenarios propuestos se realiza con el fin de poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking y demás conocimientos adquiridos a lo largo del diplomado de profundización CCNA ofrecido por la Universidad Nacional Abierta y a Distancia, utilizando herramientas de simulación en este caso se utilizará Packet Tracer; como producto se obtendrá un documento donde se detalle cada uno de los pasos realizados

4. MATERIALES Y MÉTODOS

4.1 MATERIALES

Computador, herramienta de simulación Packert Tracer, plataforma CISCO, internet.

4.2 METODOLOGÍA

El trabajo se realiza consultando las guías y material dispuestos por el tutor donde se indica los pasos a seguir para el correcto desarrollo.

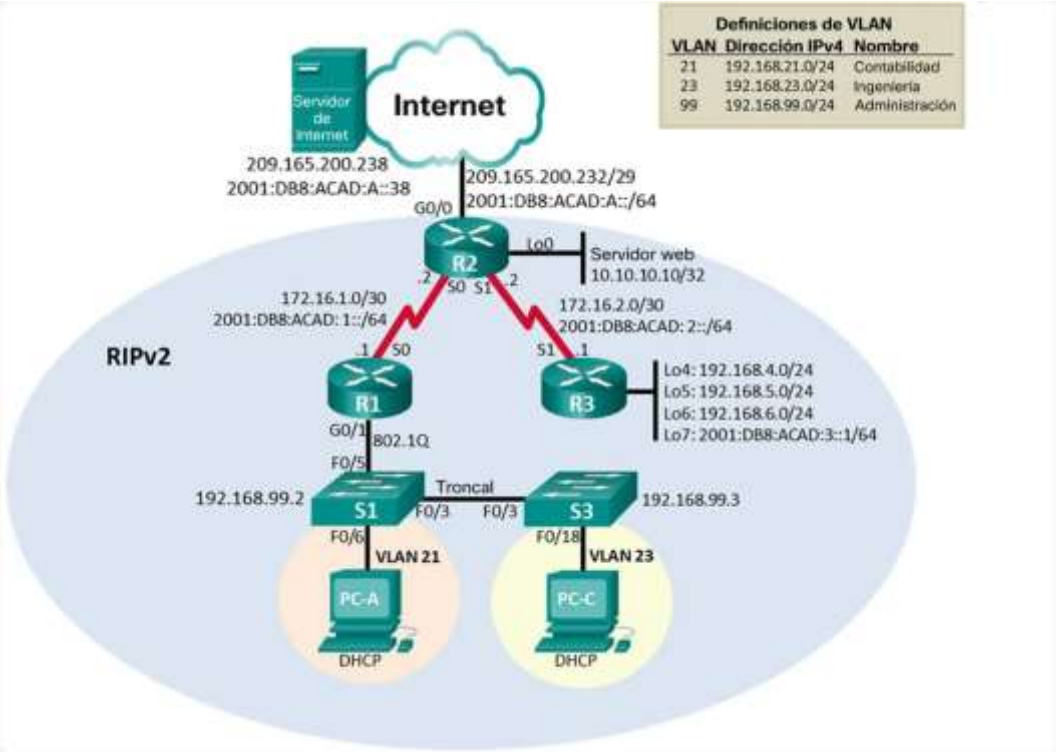
5. DESARROLLO DEL PROYECTO

5.1 ESCENARIO 1

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.

5.1.1 Parte 1: Inicializar dispositivos

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 1. Inicializar y volver a cargar los routers y los switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Debemos de acceder en los dispositivos al modo exec privilegiado mediante el comando **enable** utilizamos el comando **erase startup-config** R1 Router>enable Router#erase startup-config R2 Router>enable Router#erase startup-config R3 Router>enable Router#erase startup-config
Volver a cargar todos los routers	Es necesario para Volver a cargar los Router escribir el commando reload R1 Router#reload R2 Router#reload R3 Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Debemos de acceder en los dispositivos al modo privilegiado mediante el comando **enable** utilizamos el comando **erase startup-config**

	S1 Switch>enable Switch#erase startup-config S3 Switch>enable Switch#erase startup-config Para poder eliminar correctamente la base de datos de VLAN temenos que escribir el commando delete vlan.dat S1 Switch#delete vlan.dat S3 Switch#delete vlan.dat
Volver a cargar ambos switches	Para cargar los Switches utlizamos el commando reload S1 Switch#reload S3 Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Escribimos el commando **show flash** para verificar que ya no está la base de datos VLAN en la memoria flash S1 Switch#show flash: S3 Switch#show flash: 64016384 bytes total (59601463 bytes free)

Fuente: Autor

5.1.2 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 2. Configurar la computadora de Internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::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 3. Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Accedemos a la configuracion global del dispositivo y digitamos el commando **no ip domain-lookup** Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Escribir **R1** como nombre del dispositivo Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	Escribir **class** como contraseña R1(config)#enable secret class
Contraseña de acceso a la consola	Escribir **cisco** como contraseña R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#ex
Contraseña de acceso Telnet	Escribir **cisco** como contraseña R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	**Se prohíbe el acceso no autorizado**. R1(config)#banner motd #Se prohibe el acceso no autorizado!#

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz R1(config)#interface s0/0/0 R1(config-if)#description R1 - R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#no shutdown R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0 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 4. Configurar R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Accedemos a la configuracion global del dispositivo y digitamos el commando **no ip domain-lookup** Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Escribir R2 como nombre del dispositivo Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Escribir **class** como contraseña R2(config)#enable secret class
Contraseña de acceso a la consola	Escribir **cisco** como contraseña R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	Escribir **cisco** como contraseña R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server

Mensaje MOTD	**Se prohíbe el acceso no autorizado**. R2(config)#banner motd #Se prohibe el acceso no autorizado!#
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2(config)#interface s0/0/0 R2(config-if)#description R2-R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz R2(config)#interface s0/0/1 R2(config-if)#description R2-R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz R2(config)#int g0/0 R2(config-if)#description R2-Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config)#interface loopback 0 R2(config-if)#description servidor web simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Fuente: Autor

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configurar R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Accedemos a la configuracion global del dispositivo y digitamos el commando **no ip domain-lookup** Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Escribimos **R3** como nombre del dispositivo Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Escribimos **class** como contraseña R3(config)#enable secret class
Contraseña de acceso a la consola	Escribimos **cisco** como contraseña R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	Escribimos **cisco** como contraseña R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	**Se prohíbe el acceso no autorizado**. R3(config)#banner motd #Se prohibe el acceso no autorizado!#

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3(config)#int s0/0/1 R3(config-if)#description R3-R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface loopback 5 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. R3(config)#interface loopback 6 R3(config-if)# 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. R3(config)#interface loopback 7 R3(config-if)# R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#interface s0/0/1 R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1 R3(config)#interface s0/0/1 R3(config-if)#ipv6 route ::/0 s0/0/1

Fuente: Autor

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configurar S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Accedemos a la configuracion global del dispositivo y digitamos el commando **no ip domain-lookup** Switch>en Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch	Escribir **S1** como nombre del dispositivo Switch(config)#hostname S1

Contraseña de exec privilegiado cifrada	Escribir **class** como contraseña S1(config)#enable secret class
Contraseña de acceso a la consola	Escribir **cisco** como contraseña S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	Escribir **cisco** como contraseña S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	**Se prohíbe el acceso no autorizado**. 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 7. Configurar el S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Accedemos a la configuracion global del dispositivo y digitamos el commando **no ip domain-lookup** Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Escribir **S3** como nombre del dispositivo Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	Escribir **class** como contraseña S3(config)#enable secret class
Contraseña de acceso a la consola	Escribir **cisco** como contraseña S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	Escribir **cisco** como contraseña S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	**Se prohíbe el acceso no autorizado**. S3(config)#banner motd #Se prohibe el acceso no autorizado!#

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:

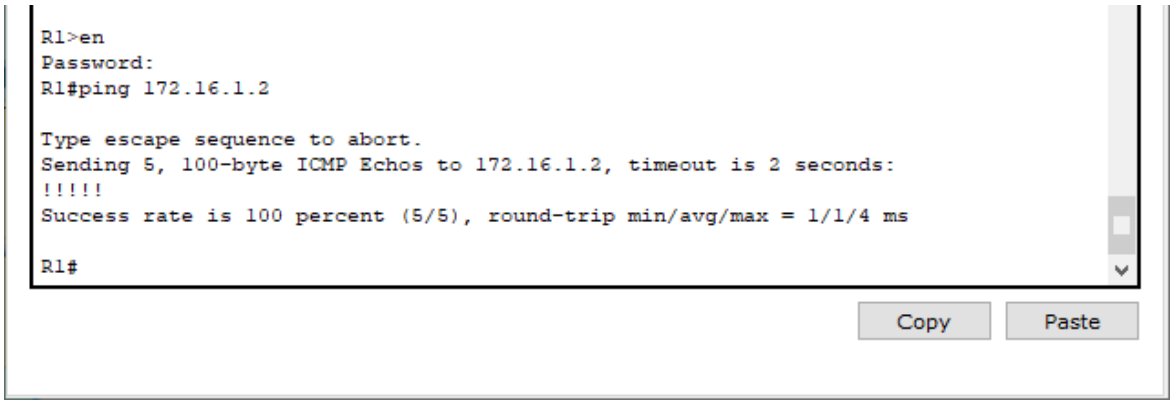
Tabla 8. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Correcto
R2	R3, S0/0/1	172.16.2.2	Correcto
PC de Internet	Gateway predeterminado	10.10.10.10	Correcto

Fuente: Autor

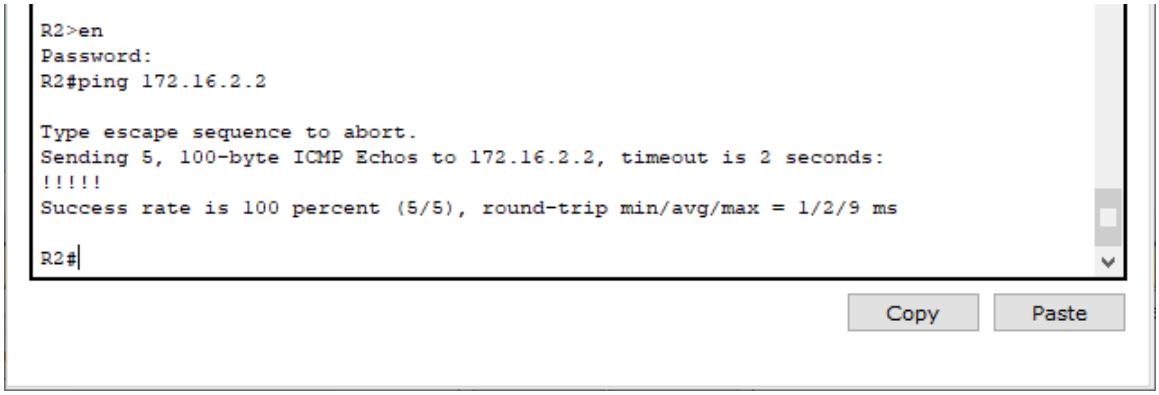
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 2. Ping R1 con R2, S0/0/0



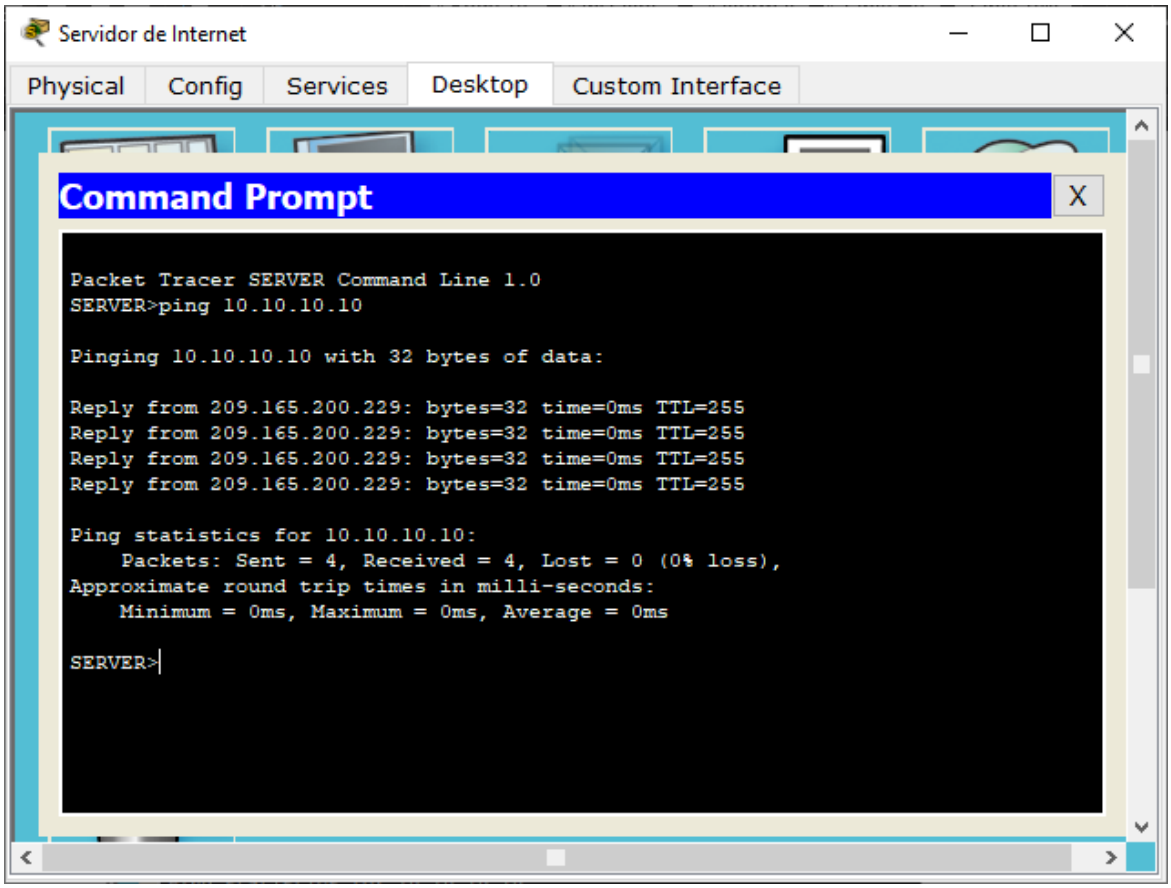
Fuente: Autor

Figura 3. Ping R2 con R3, S0/0/1



Fuente: Autor

Figura 4. PC de Internet con Gateway predeterminado



Fuente: Autor

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configurar la seguridad de 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 S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
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 S1(config)#interface vlan 99 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. 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 S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	**Utilizar la red VLAN 1 como VLAN nativa** S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	**Utilizar el comando interface range** S1(config)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente: Autor

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configurar la seguridad de 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. S3>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
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 S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. 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 S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#interface range f0/1-2, f0/4-24, g0/1-2
Asignar F0/18 a la VLAN 23	S3(config)#int f0/8 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Fuente: Autor

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configurar la seguridad de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#interface g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)#interface g0/1.23 R1(config-subif)#description LAN de Ingeniera R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit

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

Fuente: Autor

Paso 4: Verificar la conectividad de la red

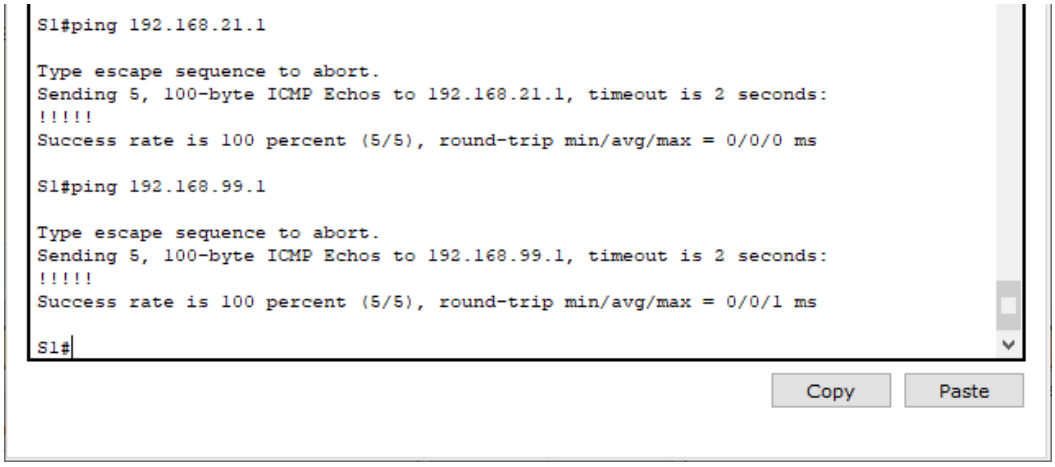
Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Correcto
S3	R1, dirección VLAN 99	192.168.99.1	Correcto
S1	R1, dirección VLAN 21	192.168.21.1	Correcto
S3	R1, dirección VLAN 23	192.168.23.1	Correcto

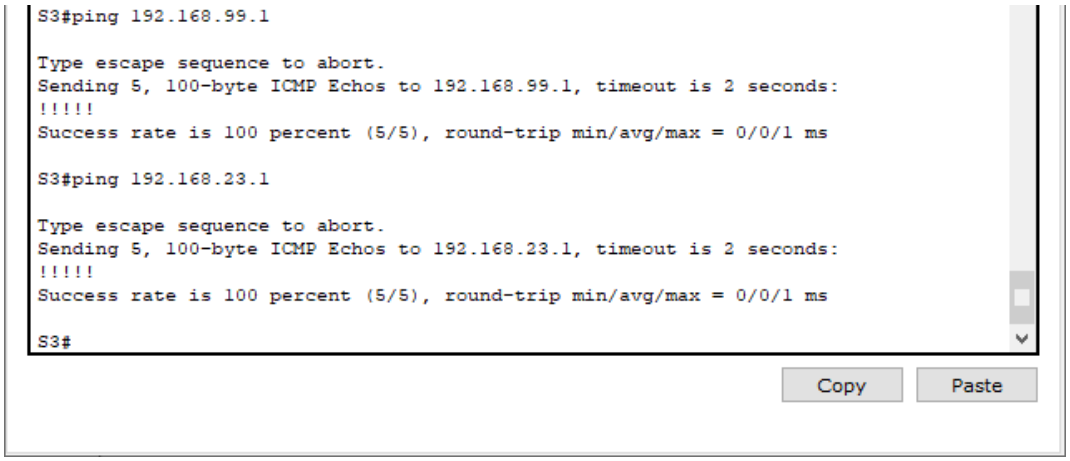
Fuente: Autor

Figura 5. Ping de S1 a R1, dirección VLAN 99 y R1, dirección VLAN 21



Fuente: Autor

Figura 6. Ping de S3 a R1, dirección VLAN 99 y R1, dirección VLAN 23



Fuente: Autor

5.1.4 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 13. Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. Revisamos que redes están conectadas R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 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 14. Configurar RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. Revisamos que redes están conectadas R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Fuente: Autor

Paso 3: Configurar RIPv2 en el R3
La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configurar RIPv2 en el R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2

Anunciar redes IPv4 conectadas directamente	Revisamos que redes están conectadas R3(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6 R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
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:

Tabla 16. Verificar la información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las	R1#Show ip protocols

interfaces pasivas configuradas en un router?	
¿Qué comando muestra solo las rutas RIP?	R1# Show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1# Show run

Fuente: Autor

5.1.5 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 17. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)# 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** Servidor DNS: **10.10.10.10** Nombre de dominio: **ccna-sa.com** Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	Nombre: **ENGNR** Servidor DNS: **10.10.10.10** Nombre de dominio: **ccna-sa.com** Establecer el gateway predeterminado R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1

Fuente: Autor

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configurar 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** Contraseña: **cisco12345** Nivel de privilegio: **15** 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)# R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** 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)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255

Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** 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

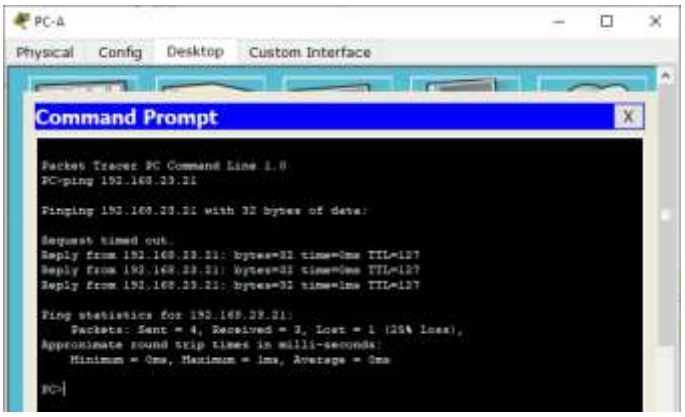
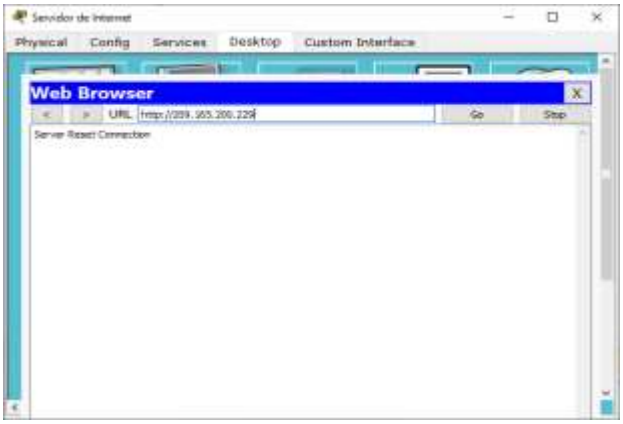
Fuente: Autor

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.

Tabla 19. Verificar el protocolo DHCP y la NAT estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 7. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP  Fuente: Autor

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 8. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP  Fuente: Autor
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Figura 9. Verificar que la PC-A pueda hacer ping a la PC-C  Fuente: Autor
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 10. Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229)  Fuente: Autor

5.1.6 Parte 6: Configurar NTP

Tabla 20. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 5 March 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5 R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 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.	R1#show ntp associations

Fuente: Autor

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

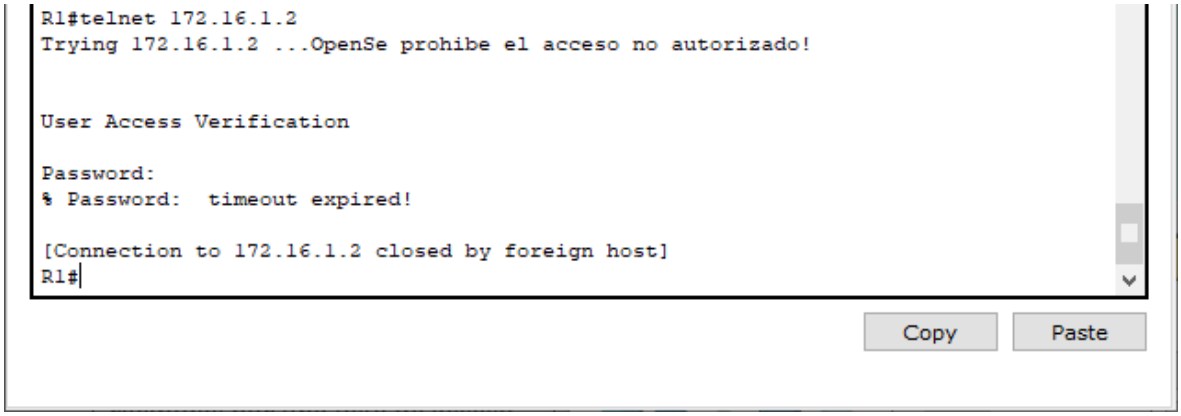
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 21. Restringir el 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** R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado! User Access Verification Password: R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host

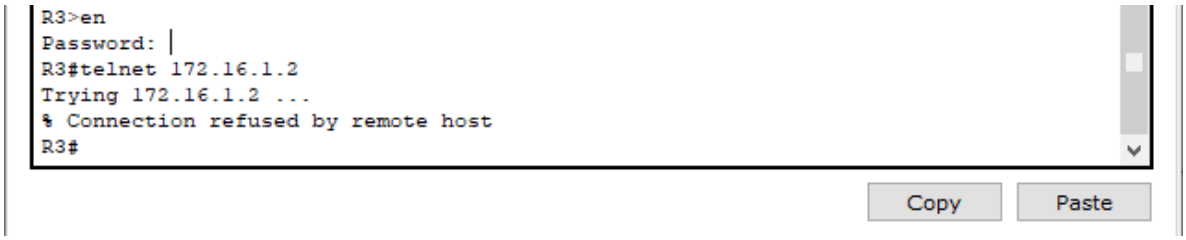
Fuente: Autor

Figura 11. Prueba de Telnet de R1 a R2



Fuente: Autor

Figura 12. Prueba de Telnet de R3 a R2



Fuente: Autor

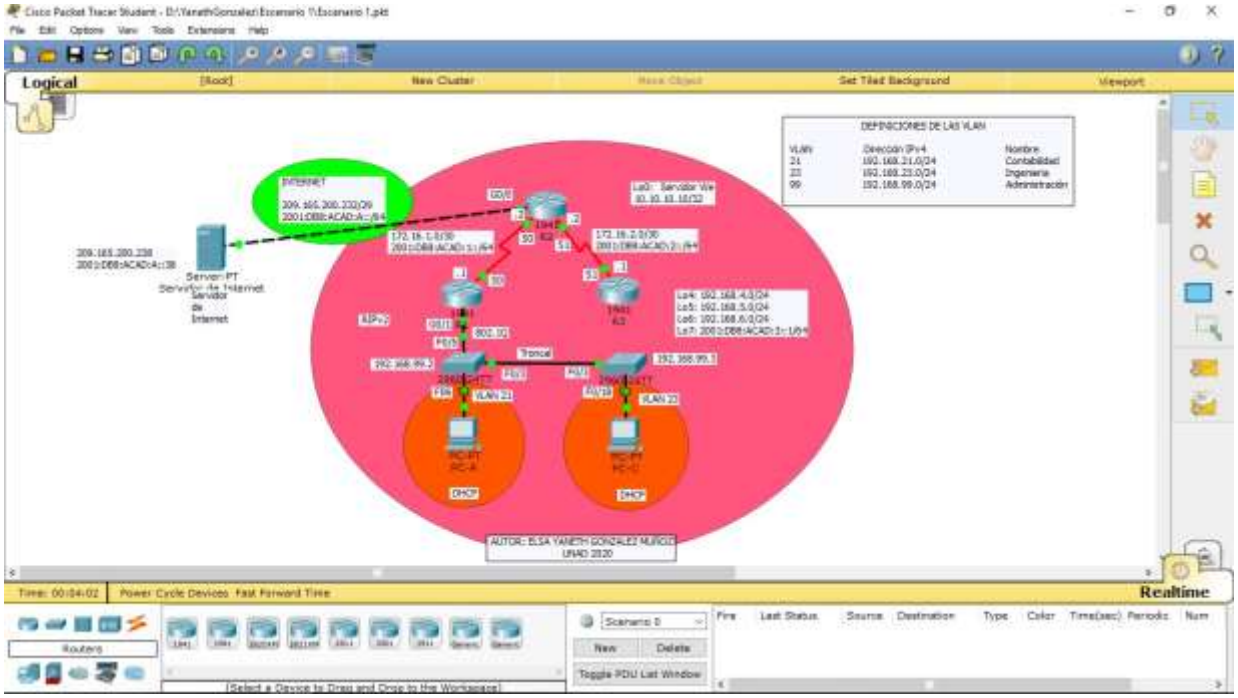
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 22. Comando de CLI adecuado

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 access-list Standard IP access list 1 10 permit 192.168.4.0 0.0.0.255 20 permit 192.168.5.0 0.0.0.255 30 permit 192.168.6.0 0.0.0.255 40 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) R2#
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿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. R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- --- R2#
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2(config)#clear ip nat translation *

Fuente: Autor

Figura 13. Evidencia: Topología realizada en Packet Tracer



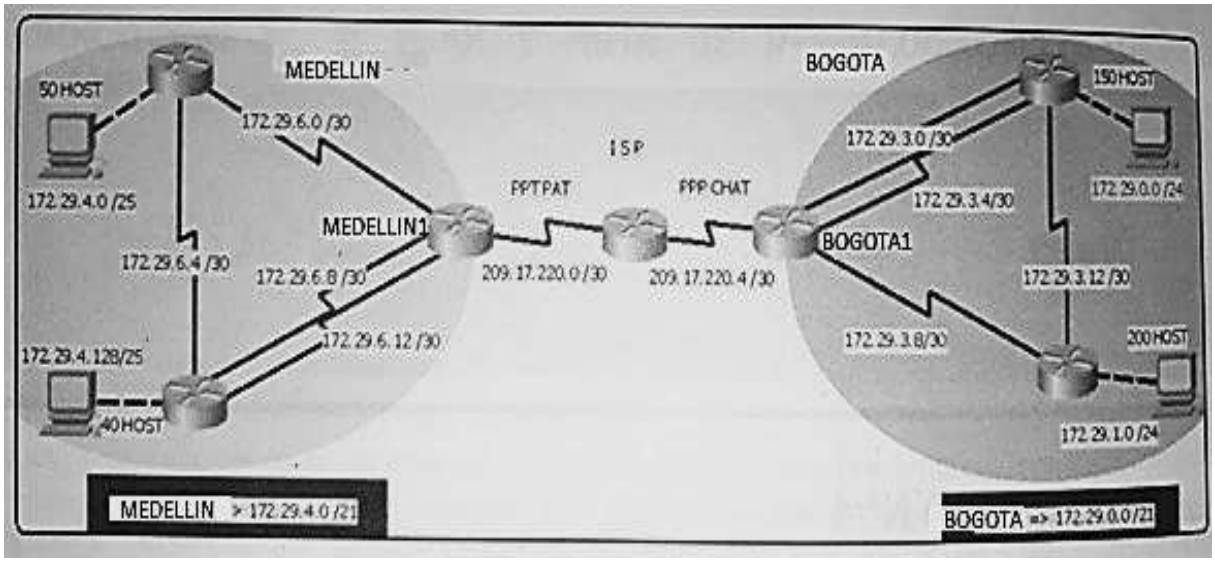
Fuente: Autor

5.2 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 14. 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).

Router(config)# no ip domain-lookup

Procedemos con la 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.#%

Realizamos la configuración Medellín1

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.#

Realizamos la configuración Medellín2

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)#ser
Medellin2(config-line)#exit
Medellin2(config)#ser
Medellin2(config)#service pa
Medellin2(config)#service password-encryption
Medellin2(config)#banner motd #Se prohibe el acceso no autorizado.#

Realizamos la configuración Medellín3

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.#

Realizamos la configuración Bogota1

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname Bogota1
Bogota1(config)#enable secret class
Bogota1(config)#line console 0
Bogota1(config-line)#password cisco
Bogota1(config-line)#login
Bogota1(config-line)#exit
Bogota1(config)#line vty 0 15
Bogota1(config-line)#password cisco
Bogota1(config-line)#lo
Bogota1(config-line)#login
Bogota1(config-line)#exit
Bogota1(config)#service password-encryption
Bogota1(config)#banner motd #Se prohibe el acceso no autorizado.#

Realizamos la configuración Bogota2

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname Bogota2
Bogota2(config)#enable secret class
Bogota2(config)#line console 0
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#exit
Bogota2(config)#line vty 0 15
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#exit
Bogota2(config)#service password-encryption

Bogota2(config)#banner motd #Se prohibe el acceso no autorizado.#

Realizamos la configuración Bogota3

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname Bogota3
Bogota3(config)#enable secret class
Bogota3(config)#line console 0
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#exit
Bogota3(config)#line vty 0 15
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#exit
Bogota3(config)#service password-encryption
Bogota3(config)#banner motd #Se prohibe el acceso no autorizado.#

• Realizar la conexión fisica de los equipos con base en la topología de red

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

Tabla 23. Configuración de la topología de red del escenario 2

Dispositivo	**Interfaz**	**Dirección IP**	**Máscara de subred**	**Máscara wildcard**	**Gateway predeterminado**
Bogota1	S0/0/0	209.17.220.6	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.1	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.3.9	255.255.255.252	0.0.0.3	NA
	S0/1/1	172.29.3.5	255.255.255.252	0.0.0.3	NA
Bogota2	S0/0/0	172.29.3.2	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.13	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.3.6	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.0.1	255.255.255.0	0.0.0.255	NA
Bogota3	S0/0/0	172.29.3.10	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.14	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.1.1	255.255.255.0	0.0.0.255	NA
Medellin1	S0/0/0	172.29.6.9	255.255.255.252	0.0.0.3	NA

	S0/0/1	172.29.6.1	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.6.13	255.255.255.252	0.0.0.3	NA
	S0/1/1	209.17.220.1	255.255.255.252	0.0.0.3	NA
Medellin2	S0/0/0	172.29.6.5	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.2	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.4.1	255.255.255.128	0.0.0.127	NA
Medellin3	S0/0/0	172.29.6.6	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.10	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.6.14	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.4.129	255.255.255.128	0.0.0.127	NA
ISP	S0/0/0	209.17.220.2	255.255.255.252	0.0.0.3	NA
	S0/0/1	209.17.220.5	255.255.255.252	0.0.0.3	NA
Med-PC1	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.1
Med-PC2	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.129
Bog-PC1	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.0.1
Bog-PC2	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.1.1

Fuente: Autor

Configurando Bogota1

```
Bogota1>enable
Password:
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#int s0/0/0
Bogota1(config-if)#description Connection to 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 s0/0/1
Bogota1(config-if)#description Connection to Bogota2
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/0
Bogota1(config-if)#description Connection to Bogota3
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 Connection to Bogota2
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
```

Configurando Bogota2

```
Bogota2>enable
Password:
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#int s0/0/0
Bogota2(config-if)#description Connection to Bogota1
Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota2(config-if)#no shutdown
Bogota2(config-if)#
Bogota2(config-if)#exit
Bogota2(config)#
Bogota2(config)#int s0/0/1
Bogota2(config-if)#description Connection to 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-if)#
Bogota2(config-if)#exit
Bogota2(config)#int s0/1/0
Bogota2(config-if)#description Connection to Bogota1
Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota2(config-if)#no shu
Bogota2(config-if)#no shutdown
Bogota2(config-if)#
Bogota2(config-if)#exit
Bogota2(config)#
Bogota2(config)#int g0/0
Bogota2(config-if)#description Connection to PC1-Bogota
Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota2(config-if)#no shutdown
Bogota2(config-if)#
```

Configurando Bogota3

```
Bogota3>enable
Password:
Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#int s0/0/0
Bogota3(config-if)#description Connection to Bogota1
Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota3(config-if)#no shutdown
Bogota3(config-if)#
Bogota3(config-if)#exit
Bogota3(config)#int s0/0/1
Bogota3(config-if)#description Connection to Bogota2
Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota3(config-if)#no shutdown
Bogota3(config-if)#
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#int g0/0
Bogota3(config-if)#description Connection to PC2-Bogota
Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
```

Configurando Medellin1

```
Medellin1>enable
Password:
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#int s0/0/0
Medellin1(config-if)#description Connection to Medellin3
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#int s0/0/1
```

```
Medellin1(config-if)#description Connection to Medellin2
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/0
Medellin1(config-if)#description Connection to Medellin3
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/1
Medellin1(config-if)#description Connection to ISP
Medellin1(config-if)#ip address 209.17.220.1 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#
```

Configurando Medellin2

```
Medellin2>enable
Password:
Medellin2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#int s0/0/0
Medellin2(config-if)#description Connection to Medellin3
Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#int s0/0/1
Medellin2(config-if)#description Connection to Medellin1
Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#no shu
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#int g0/0
Medellin2(config-if)#description Connection to PC1-Medellin
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shutdown
```

Configurando Medellin3

```
Medellin3>enable
Password:
Medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#int s0/0/0
Medellin3(config-if)#description Connection to Medellin2
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#int s0/0/1
Medellin3(config-if)#description Connection to Medellin1
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#int s0/1/0
Medellin3(config-if)#description Connection to Medellin1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#int g0/0
Medellin3(config-if)#description Connection to PC2-Medellin
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
```

Configurando ISP

```
ISP>enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/0
ISP(config-if)#description Connection to Medellin1
ISP(config-if)#ip address 209.17.220.2 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shu
```

```
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#exit
ISP(config)#int s0/0/1
ISP(config-if)#description Connection to Bogota1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#exit
```

5.2.1 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.

Configurando enrutamiento en Bogota1

```
Bogota1>enable
Password:
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#router ospf 1
Bogota1(config-router)#router-id 4.4.4.4
Bogota1(config-router)#do show ip route connected
C   172.29.3.0/30 is directly connected, Serial0/0/1
C   172.29.3.4/30 is directly connected, Serial0/1/1
C   172.29.3.8/30 is directly connected, Serial0/1/0
 C   209.17.220.4/30 is directly connected, Serial0/0/0
Bogota1(config-router)#
Bogota1(config-router)#
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 0
Bogota1(config-router)#exit
Bogota1(config)#
```

Configurando enrutamiento en Bogota2

```
Bogota2>enable
Password:
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#router ospf 1
Bogota2(config-router)#router-id 5.5.5.5
Bogota2(config-router)#do show ip route connected
 C   172.29.0.0/24 is directly connected, GigabitEthernet0/0
 C   172.29.3.0/30 is directly connected, Serial0/0/0
 C   172.29.3.4/30 is directly connected, Serial0/1/0
 C   172.29.3.12/30 is directly connected, Serial0/0/1
Bogota2(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota2(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#exit
```

Configurando enrutamiento en Bogota3

```
Bogota3>enable
Password:
Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#router ospf 1
Bogota3(config-router)#router-id 6.6.6.6
Bogota3(config-router)#do show ip route connected
 C   172.29.1.0/24 is directly connected, GigabitEthernet0/0
 C   172.29.3.8/30 is directly connected, Serial0/0/0
 C   172.29.3.12/30 is directly connected, Serial0/0/1
Bogota3(config-router)#network 172.29.1.0 0.0.0.255 area 0
Bogota3(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota3(config-router)#exit
```

Configurando enrutamiento en Medellin1

```
Medellin1>enable
Password:
```

```
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#router ospf 1
Medellin1(config-router)#router-id 1.1.1.1
Medellin1(config-router)#do show ip route connected
C   172.29.6.0/30  is directly connected, Serial0/0/1
C   172.29.6.8/30  is directly connected, Serial0/0/0
C   172.29.6.12/30 is directly connected, Serial0/1/0
 C   209.17.220.0/30 is directly connected, Serial0/1/1
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 0
Medellin1(config-router)#exit
```

Configurando enrutamiento en Medellin2

```
Medellin2>enable
Password:
Medellin2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#router ospf 1
Medellin2(config-router)#router-id 2.2.2.2
Medellin2(config-router)#do show ip route connected
 C   172.29.4.0/25 is directly connected, GigabitEthernet0/0
 C   172.29.6.0/30 is directly connected, Serial0/0/1
 C   172.29.6.4/30 is directly connected, Serial0/0/0
Medellin2(config-router)#
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#exit
```

Configurando enrutamiento en Medellin3

```
Medellin3>enable
Password:
Medellin3#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#router ospf 1
Medellin3(config-router)#
Medellin3(config-router)#router-id 3.3.3.3
Medellin3(config-router)#do show ip route connected
 C   172.29.4.128/25 is directly connected, GigabitEthernet0/0
 C   172.29.6.4/30 is directly connected, Serial0/0/0
 C   172.29.6.8/30 is directly connected, Serial0/0/1
 C   172.29.6.12/30 is directly connected, Serial0/1/0
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin3(config-router)#exit
Medellin3(config)#
```

Configurando enrutamiento en ISP

```
ISP>enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#router ospf 1
ISP(config-router)#router-id 7.7.7.7
ISP(config-router)#do show ip route connected
 C   209.17.220.0/30  is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.4 0.0.0.3 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.

Configurando ruta por defecto de Bogota1 hacia el ISP

```
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
Bogota1(config-router)#exit
Bogota1(config)#
```

Configurando ruta por defecto de Medellin1 hacia el ISP

```
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2
Medellin1(config)#router ospf 1
Medellin1(config-router)#default-information originate
Medellin1(config-router)#exit
```

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.

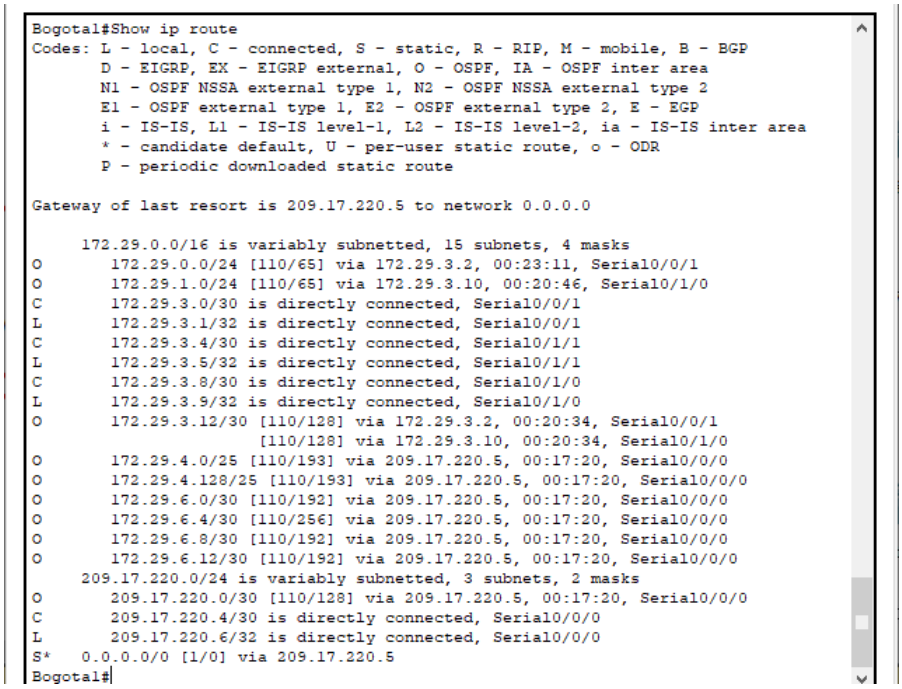
Configurando rutas estáticas en ISP

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

5.2.2 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 15. Ingresamos el comando Show ip route en Bobota1



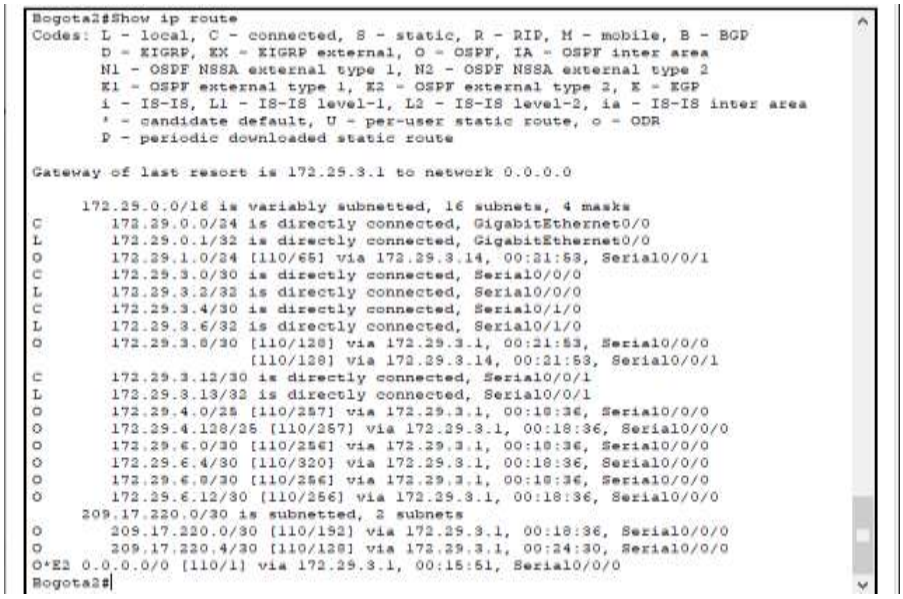
```
Bogota1#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.5 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O       172.29.0.0/24 [110/65] via 172.29.3.2, 00:23:11, Serial0/0/1
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:20:46, Serial0/1/0
C       172.29.3.0/30 is directly connected, Serial0/0/1
L       172.29.3.1/32 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/1/0
L       172.29.3.9/32 is directly connected, Serial0/1/0
O       172.29.3.12/30 [110/128] via 172.29.3.2, 00:20:34, Serial0/0/1
                       [110/128] via 172.29.3.10, 00:20:34, Serial0/1/0
O       172.29.4.0/25 [110/193] via 209.17.220.5, 00:17:20, Serial0/0/0
O       172.29.4.128/25 [110/193] via 209.17.220.5, 00:17:20, Serial0/0/0
O       172.29.6.0/30 [110/192] via 209.17.220.5, 00:17:20, Serial0/0/0
O       172.29.6.4/30 [110/256] via 209.17.220.5, 00:17:20, Serial0/0/0
O       172.29.6.8/30 [110/192] via 209.17.220.5, 00:17:20, Serial0/0/0
O       172.29.6.12/30 [110/192] via 209.17.220.5, 00:17:20, Serial0/0/0
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
O       209.17.220.0/30 [110/128] via 209.17.220.5, 00:17:20, Serial0/0/0
C       209.17.220.4/30 is directly connected, Serial0/0/0
L       209.17.220.6/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.5
Bogota1#
```

Fuente: Autor

Figura 16. Ingresamos el comando Show ip route en Bogota2



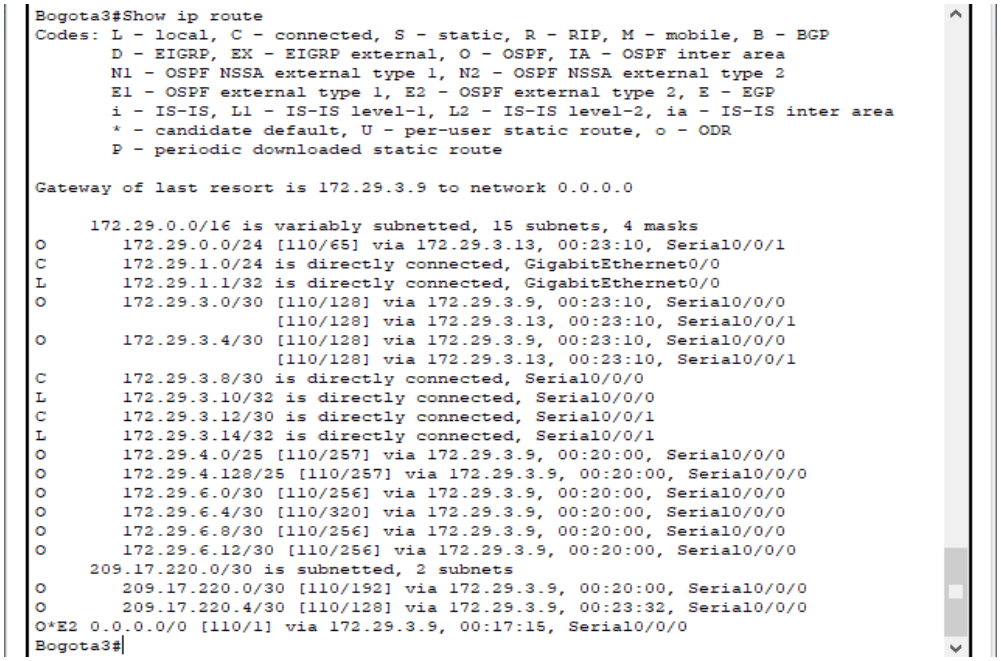
```
Bogota2#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 16 subnets, 4 masks
C       172.29.0.0/24 is directly connected, GigabitEthernet0/0
L       172.29.0.1/32 is directly connected, GigabitEthernet0/0
O       172.29.1.0/24 [110/65] via 172.29.3.14, 00:21:53, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/0/0
L       172.29.3.2/32 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/1/0
L       172.29.3.6/32 is directly connected, Serial0/1/0
O       172.29.3.8/30 [110/128] via 172.29.3.1, 00:21:53, Serial0/0/0
                      [110/128] via 172.29.3.14, 00:21:53, Serial0/0/1
C       172.29.3.12/30 is directly connected, Serial0/0/1
L       172.29.3.13/32 is directly connected, Serial0/0/1
O       172.29.4.0/25 [110/257] via 172.29.3.1, 00:18:36, Serial0/0/0
O       172.29.4.128/25 [110/257] via 172.29.3.1, 00:18:36, Serial0/0/0
O       172.29.6.0/30 [110/256] via 172.29.3.1, 00:18:36, Serial0/0/0
O       172.29.6.4/30 [110/320] via 172.29.3.1, 00:18:36, Serial0/0/0
O       172.29.6.8/30 [110/256] via 172.29.3.1, 00:18:36, Serial0/0/0
O       172.29.6.12/30 [110/256] via 172.29.3.1, 00:18:36, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0/30 [110/192] via 172.29.3.1, 00:18:36, Serial0/0/0
O       209.17.220.4/30 [110/128] via 172.29.3.1, 00:24:30, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:15:51, Serial0/0/0
Bogota2#
```

Fuente: Autor

Figura 17. Ingresamos el comando Show ip route en Bogota3



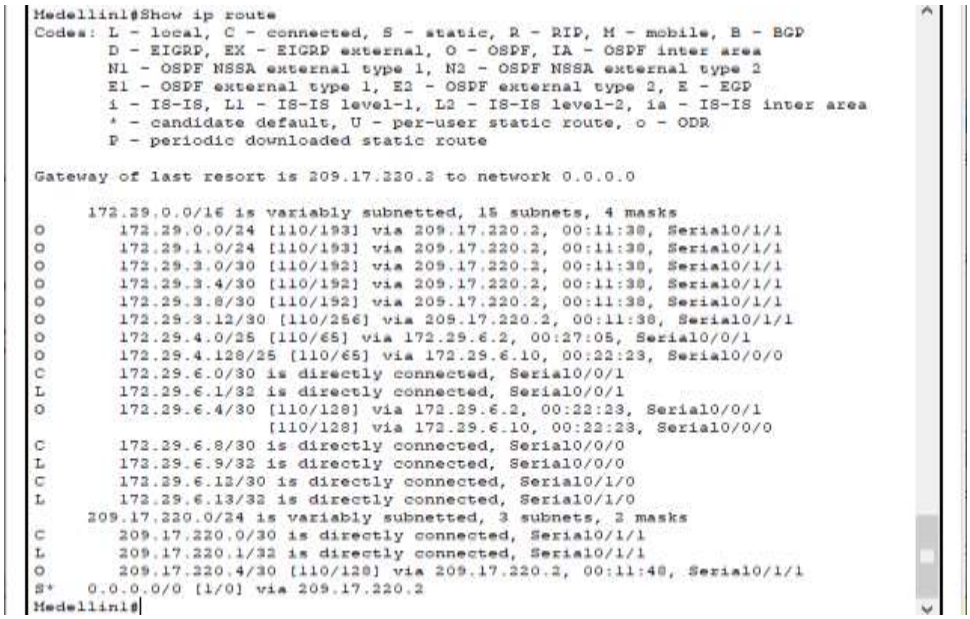
```
Bogota3#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.3.9 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O       172.29.0.0/24 [110/65] via 172.29.3.13, 00:23:10, Serial0/0/1
C       172.29.1.0/24 is directly connected, GigabitEthernet0/0
L       172.29.1.1/32 is directly connected, GigabitEthernet0/0
O       172.29.3.0/30 [110/128] via 172.29.3.9, 00:23:10, Serial0/0/0
                      [110/128] via 172.29.3.13, 00:23:10, Serial0/0/1
O       172.29.3.4/30 [110/128] via 172.29.3.9, 00:23:10, Serial0/0/0
                      [110/128] via 172.29.3.13, 00:23:10, Serial0/0/1
C       172.29.3.8/30 is directly connected, Serial0/0/0
L       172.29.3.10/32 is directly connected, Serial0/0/0
C       172.29.3.12/30 is directly connected, Serial0/0/1
L       172.29.3.14/32 is directly connected, Serial0/0/1
O       172.29.4.0/25 [110/257] via 172.29.3.9, 00:20:00, Serial0/0/0
O       172.29.4.128/25 [110/257] via 172.29.3.9, 00:20:00, Serial0/0/0
O       172.29.6.0/30 [110/256] via 172.29.3.9, 00:20:00, Serial0/0/0
O       172.29.6.4/30 [110/320] via 172.29.3.9, 00:20:00, Serial0/0/0
O       172.29.6.8/30 [110/256] via 172.29.3.9, 00:20:00, Serial0/0/0
O       172.29.6.12/30 [110/256] via 172.29.3.9, 00:20:00, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0/30 [110/192] via 172.29.3.9, 00:20:00, Serial0/0/0
O       209.17.220.4/30 [110/128] via 172.29.3.9, 00:23:32, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:17:15, Serial0/0/0
Bogota3#
```

Fuente: Autor

Figura 18. Ingresamos el comando Show ip route en Medellin1



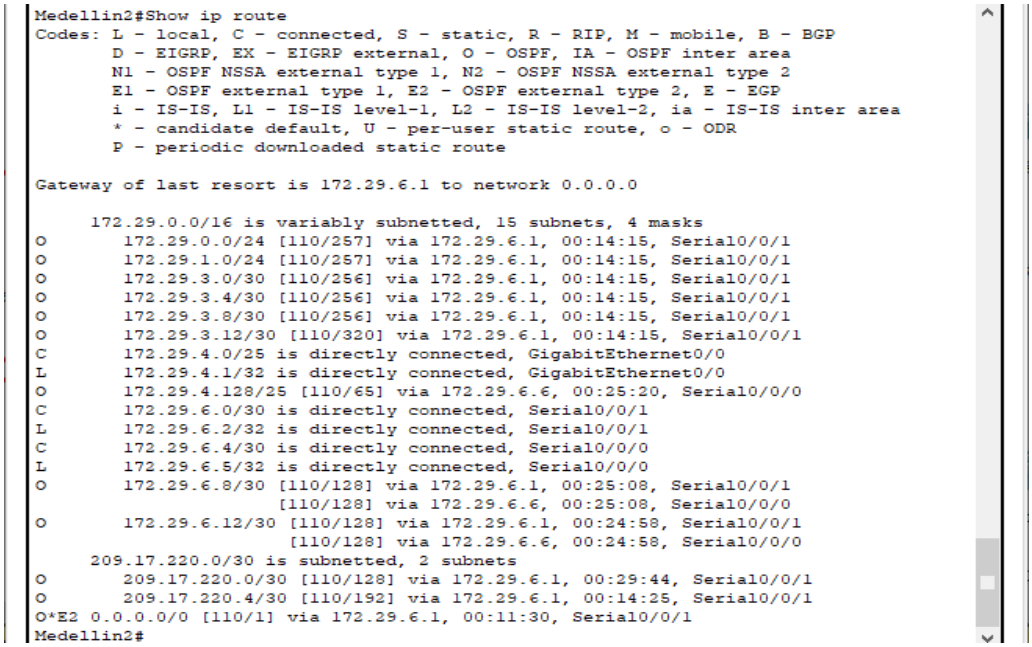
```
Medellin1#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.2 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O       172.29.0.0/24 [110/193] via 209.17.220.2, 00:11:38, Serial0/1/1
O       172.29.1.0/24 [110/193] via 209.17.220.2, 00:11:38, Serial0/1/1
O       172.29.3.0/30 [110/192] via 209.17.220.2, 00:11:38, Serial0/1/1
O       172.29.3.4/30 [110/192] via 209.17.220.2, 00:11:38, Serial0/1/1
O       172.29.3.8/30 [110/192] via 209.17.220.2, 00:11:38, Serial0/1/1
O       172.29.3.12/30 [110/256] via 209.17.220.2, 00:11:38, Serial0/1/1
O       172.29.4.0/25 [110/65] via 172.29.6.2, 00:27:05, Serial0/0/1
O       172.29.4.128/25 [110/65] via 172.29.6.10, 00:22:23, Serial0/0/0
C       172.29.6.0/30 is directly connected, Serial0/0/1
L       172.29.6.1/32 is directly connected, Serial0/0/1
O       172.29.6.4/30 [110/128] via 172.29.6.2, 00:22:23, Serial0/0/1
                      [110/128] via 172.29.6.10, 00:22:23, Serial0/0/0
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.9/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/1/0
L       172.29.6.13/32 is directly connected, Serial0/1/0
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/1/1
L       209.17.220.1/32 is directly connected, Serial0/1/1
O       209.17.220.4/30 [110/128] via 209.17.220.2, 00:11:48, Serial0/1/1
S*   0.0.0.0/0 [1/0] via 209.17.220.2
Medellin1#
```

Fuente: Autor

Figura 19. Ingresamos el comando Show ip route en Medellin2



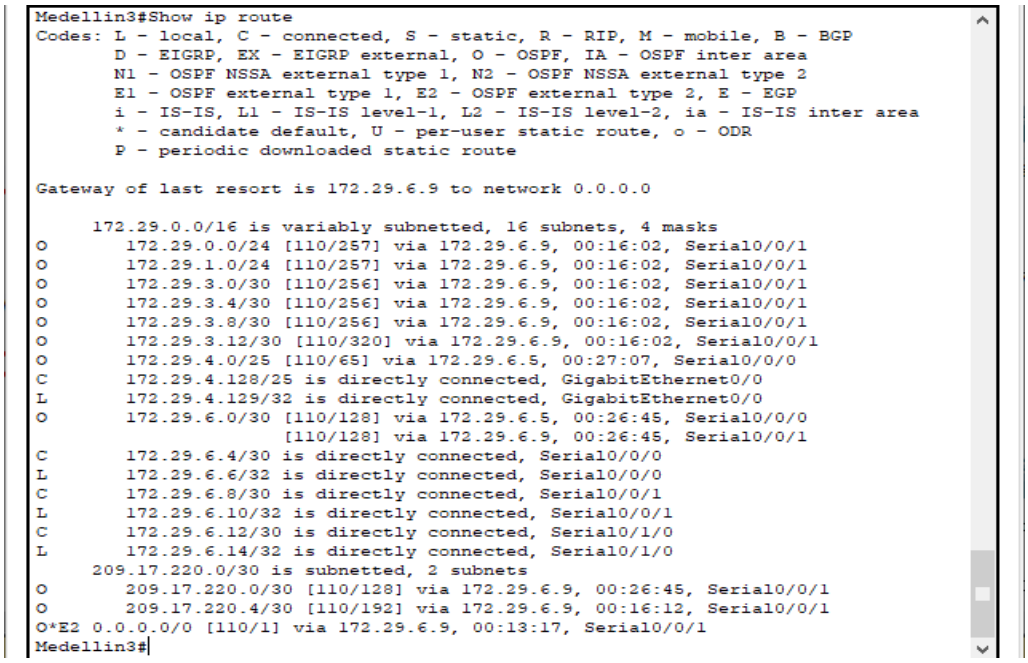
```
Medellin2#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.6.1 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O       172.29.0.0/24 [110/257] via 172.29.6.1, 00:14:15, Serial0/0/1
O       172.29.1.0/24 [110/257] via 172.29.6.1, 00:14:15, Serial0/0/1
O       172.29.3.0/30 [110/256] via 172.29.6.1, 00:14:15, Serial0/0/1
O       172.29.3.4/30 [110/256] via 172.29.6.1, 00:14:15, Serial0/0/1
O       172.29.3.8/30 [110/256] via 172.29.6.1, 00:14:15, Serial0/0/1
O       172.29.3.12/30 [110/320] via 172.29.6.1, 00:14:15, Serial0/0/1
C       172.29.4.0/25 is directly connected, GigabitEthernet0/0
L       172.29.4.1/32 is directly connected, GigabitEthernet0/0
O       172.29.4.128/25 [110/65] via 172.29.6.6, 00:25:20, Serial0/0/0
C       172.29.6.0/30 is directly connected, Serial0/0/1
L       172.29.6.2/32 is directly connected, Serial0/0/1
C       172.29.6.4/30 is directly connected, Serial0/0/0
L       172.29.6.5/32 is directly connected, Serial0/0/0
O       172.29.6.8/30 [110/128] via 172.29.6.1, 00:25:08, Serial0/0/1
                      [110/128] via 172.29.6.6, 00:25:08, Serial0/0/0
O       172.29.6.12/30 [110/128] via 172.29.6.1, 00:24:58, Serial0/0/1
                       [110/128] via 172.29.6.6, 00:24:58, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0/30 [110/128] via 172.29.6.1, 00:29:44, Serial0/0/1
O       209.17.220.4/30 [110/192] via 172.29.6.1, 00:14:25, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:11:30, Serial0/0/1
Medellin2#
```

Fuente: Autor

Figura 20. Ingresamos el comando Show ip route en Medellin3



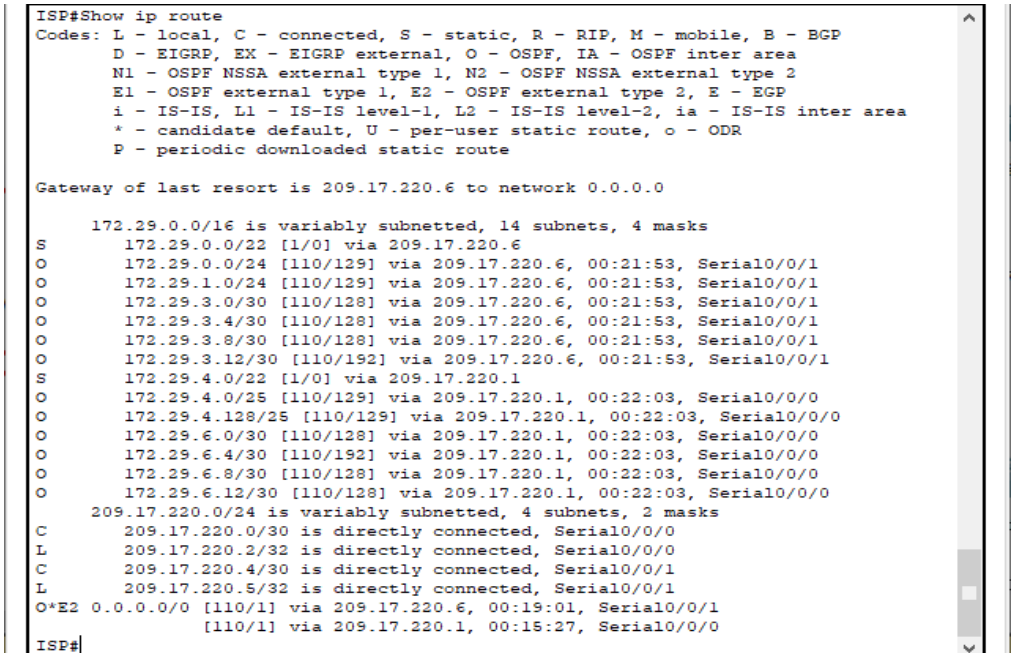
```
Medellin3#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.6.9 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 16 subnets, 4 masks
O       172.29.0.0/24 [110/257] via 172.29.6.9, 00:16:02, Serial0/0/1
O       172.29.1.0/24 [110/257] via 172.29.6.9, 00:16:02, Serial0/0/1
O       172.29.3.0/30 [110/256] via 172.29.6.9, 00:16:02, Serial0/0/1
O       172.29.3.4/30 [110/256] via 172.29.6.9, 00:16:02, Serial0/0/1
O       172.29.3.8/30 [110/256] via 172.29.6.9, 00:16:02, Serial0/0/1
O       172.29.3.12/30 [110/320] via 172.29.6.9, 00:16:02, Serial0/0/1
O       172.29.4.0/25 [110/65] via 172.29.6.5, 00:27:07, Serial0/0/0
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
O       172.29.6.0/30 [110/128] via 172.29.6.5, 00:26:45, Serial0/0/0
                      [110/128] via 172.29.6.9, 00:26:45, Serial0/0/1
C       172.29.6.4/30 is directly connected, Serial0/0/0
L       172.29.6.6/32 is directly connected, Serial0/0/0
C       172.29.6.8/30 is directly connected, Serial0/0/1
L       172.29.6.10/32 is directly connected, Serial0/0/1
C       172.29.6.12/30 is directly connected, Serial0/1/0
L       172.29.6.14/32 is directly connected, Serial0/1/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0/30 [110/128] via 172.29.6.9, 00:26:45, Serial0/0/1
O       209.17.220.4/30 [110/192] via 172.29.6.9, 00:16:12, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.9, 00:13:17, Serial0/0/1
Medellin3#
```

Fuente: Autor

Figura 21. Ingresamos el comando Show ip route en ISP



```
ISP#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.6 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 14 subnets, 4 masks
S       172.29.0.0/22 [1/0] via 209.17.220.6
O       172.29.0.0/24 [110/129] via 209.17.220.6, 00:21:53, Serial0/0/1
O       172.29.1.0/24 [110/129] via 209.17.220.6, 00:21:53, Serial0/0/1
O       172.29.3.0/30 [110/128] via 209.17.220.6, 00:21:53, Serial0/0/1
O       172.29.3.4/30 [110/128] via 209.17.220.6, 00:21:53, Serial0/0/1
O       172.29.3.8/30 [110/128] via 209.17.220.6, 00:21:53, Serial0/0/1
O       172.29.3.12/30 [110/192] via 209.17.220.6, 00:21:53, Serial0/0/1
S       172.29.4.0/22 [1/0] via 209.17.220.1
O       172.29.4.0/25 [110/129] via 209.17.220.1, 00:22:03, Serial0/0/0
O       172.29.4.128/25 [110/129] via 209.17.220.1, 00:22:03, Serial0/0/0
O       172.29.6.0/30 [110/128] via 209.17.220.1, 00:22:03, Serial0/0/0
O       172.29.6.4/30 [110/192] via 209.17.220.1, 00:22:03, Serial0/0/0
O       172.29.6.8/30 [110/128] via 209.17.220.1, 00:22:03, Serial0/0/0
O       172.29.6.12/30 [110/128] via 209.17.220.1, 00:22:03, Serial0/0/0
     209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.2/32 is directly connected, Serial0/0/0
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.5/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 209.17.220.6, 00:19:01, Serial0/0/1
               [110/1] via 209.17.220.1, 00:15:27, Serial0/0/0
ISP#
```

Fuente: Autor

5.2.3 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 24. Deshabilitar la propagación del protocolo OSPF

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
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 requiere

Fuente: Autor

Configuración en Bogota1

```
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 en Bogota2

```
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#router ospf 1
Bogota2(config-router)#passive-interface s0/1/0
Bogota2(config-router)#passive-interface g0/0
Bogota2(config-router)#exit
```

Configuración en Bogota3

```
Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#router ospf 1
Bogota3(config-router)#passive-interface g0/0
Bogota3(config-router)#exit
```

Configuración en Medellin1

```
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)#
```

Configuración en Medellin2

```
Medellin2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#router ospf 1
Medellin2(config-router)#passive-interface g0/0
```

Medellin2(config-router)#exit

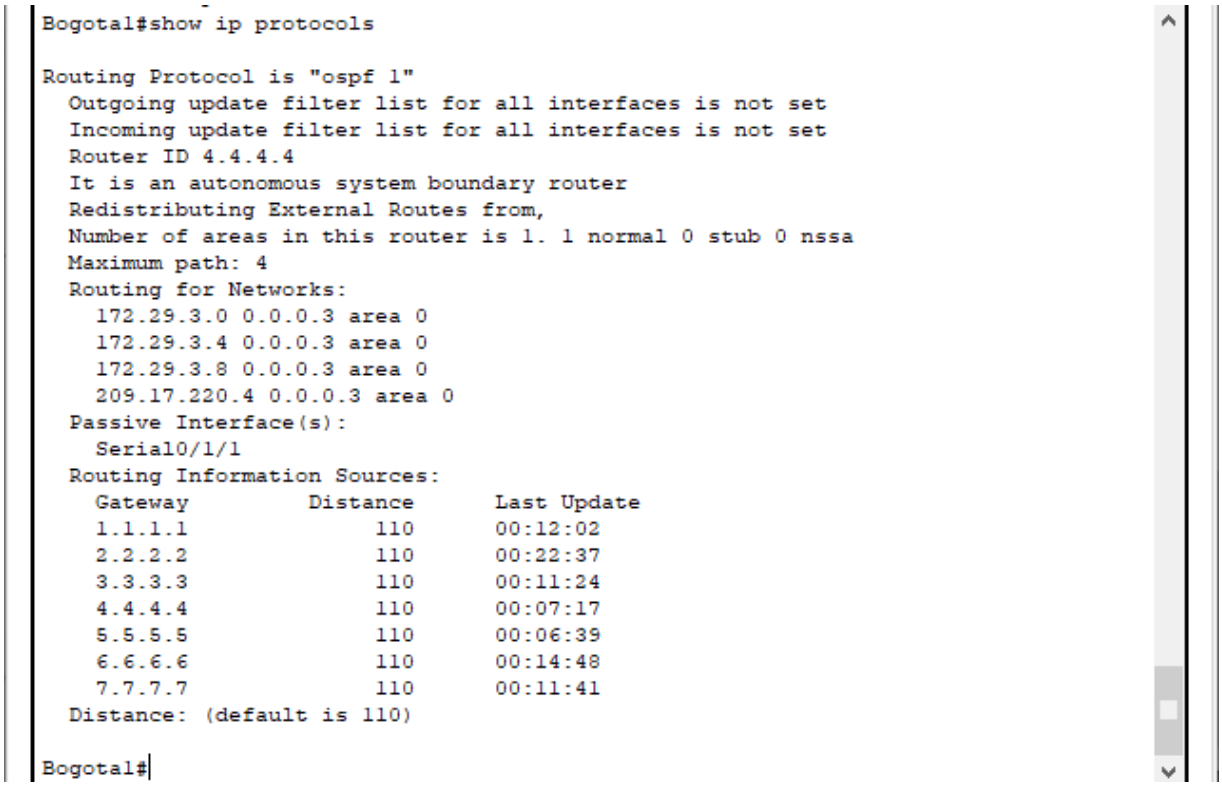
Configuración en Medellin3

Medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#router ospf 1
Medellin3(config-router)#passive-interface g0/0
Medellin3(config-router)#exit

5.2.4 Parte 4: Verificación del protocolo OSPF.

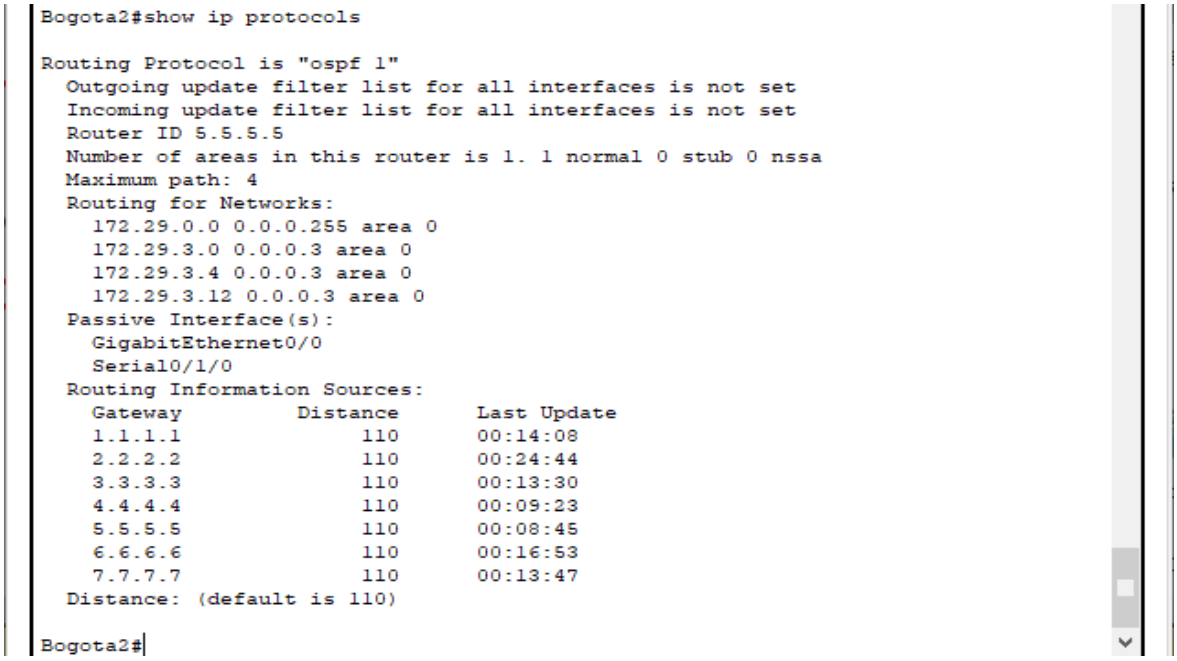
a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el **passive interface** para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Figura 22. Ingresamos el comando Show ip protocols en Bogota1



Fuente: Autor

Figura 23. Ingresamos el comando Show ip protocols en Bogota2



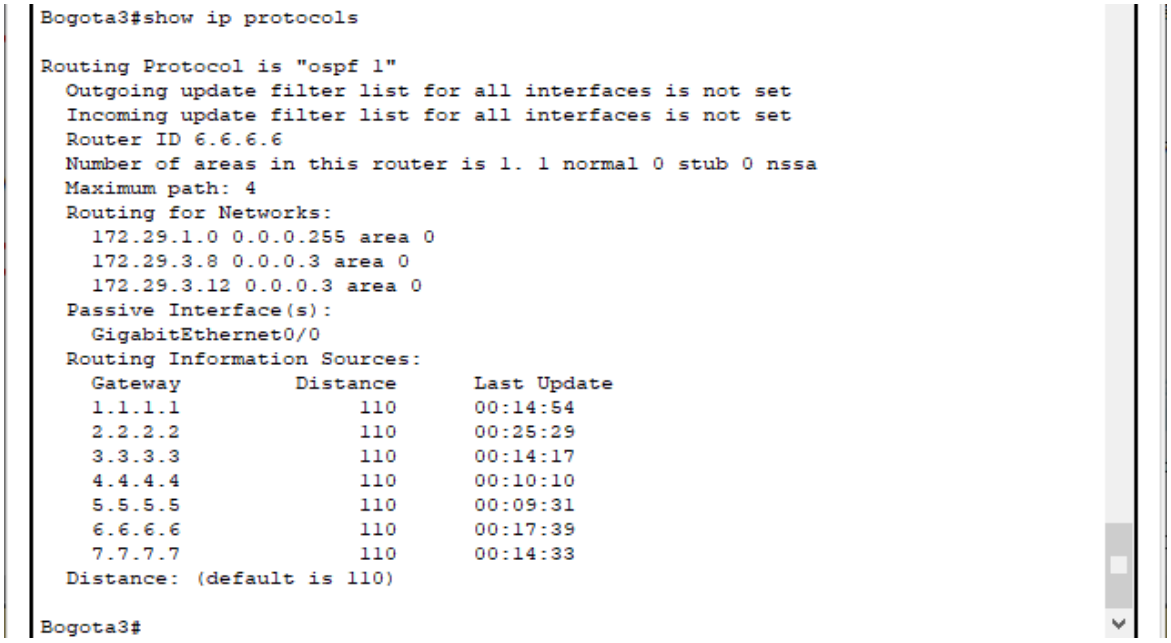
```
Bogota2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 5.5.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.255 area 0
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    Serial0/1/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:14:08
    2.2.2.2              110      00:24:44
    3.3.3.3              110      00:13:30
    4.4.4.4              110      00:09:23
    5.5.5.5              110      00:08:45
    6.6.6.6              110      00:16:53
    7.7.7.7              110      00:13:47
  Distance: (default is 110)

Bogota2#
```

Fuente: Autor

Figura 24. Ingresamos el comando Show ip protocols en Bogota3



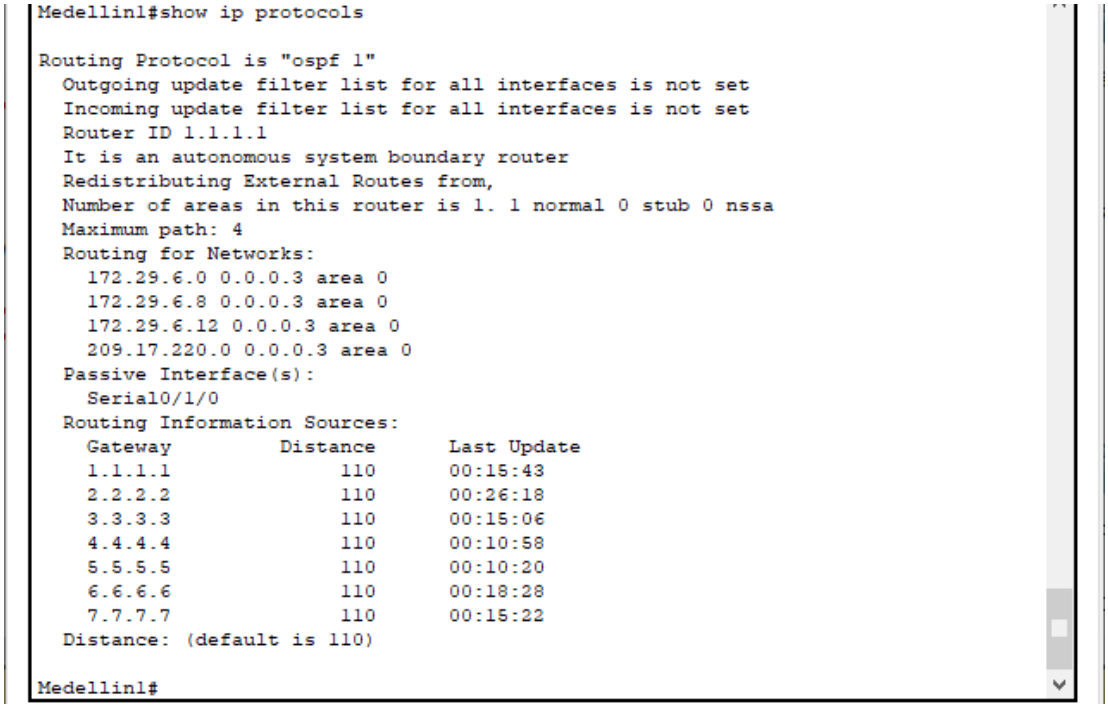
```
Bogota3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 6.6.6.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.1.0 0.0.0.255 area 0
    172.29.3.8 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:14:54
    2.2.2.2              110      00:25:29
    3.3.3.3              110      00:14:17
    4.4.4.4              110      00:10:10
    5.5.5.5              110      00:09:31
    6.6.6.6              110      00:17:39
    7.7.7.7              110      00:14:33
  Distance: (default is 110)

Bogota3#
```

Fuente: Autor

Figura 25. Ingresamos el comando Show ip protocols en Medellin1



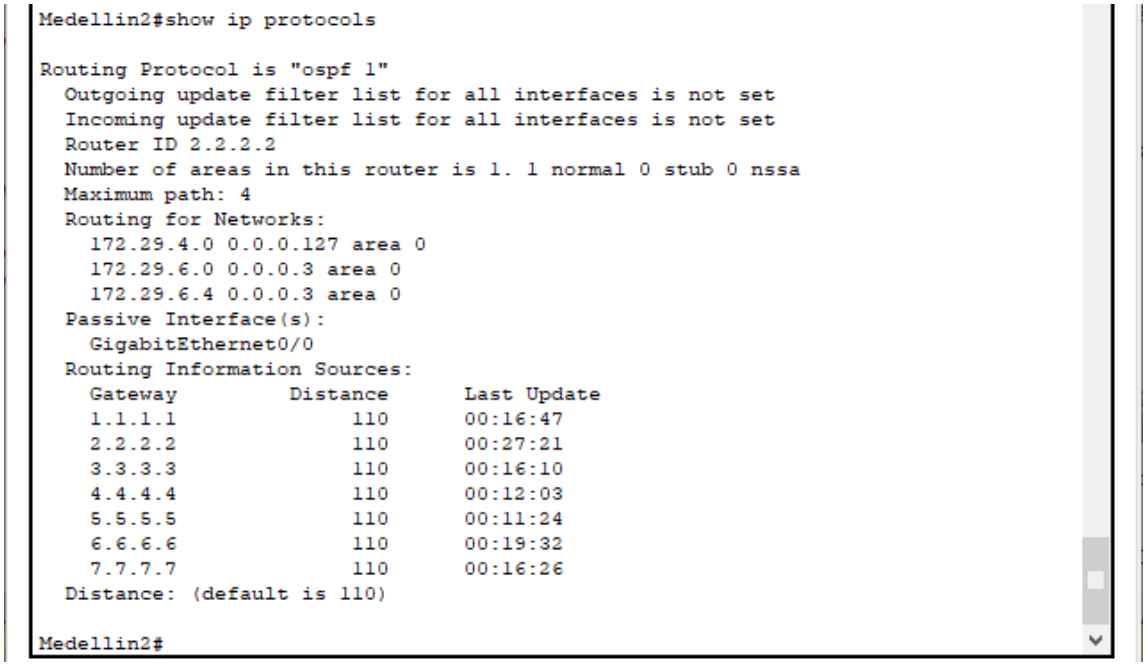
```
Medellin1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.0 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
    209.17.220.0 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/1/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:15:43
    2.2.2.2              110      00:26:18
    3.3.3.3              110      00:15:06
    4.4.4.4              110      00:10:58
    5.5.5.5              110      00:10:20
    6.6.6.6              110      00:18:28
    7.7.7.7              110      00:15:22
  Distance: (default is 110)

Medellin1#
```

Fuente: Autor

Figura 26. Ingresamos el comando Show ip protocols en Medellin2



```
Medellin2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.0 0.0.0.127 area 0
    172.29.6.0 0.0.0.3 area 0
    172.29.6.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:16:47
    2.2.2.2              110      00:27:21
    3.3.3.3              110      00:16:10
    4.4.4.4              110      00:12:03
    5.5.5.5              110      00:11:24
    6.6.6.6              110      00:19:32
    7.7.7.7              110      00:16:26
  Distance: (default is 110)

Medellin2#
```

Fuente: Autor

Figura 27. Ingresamos el comando Show ip protocols en Medellin3

```
Medellin3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.128 0.0.0.127 area 0
    172.29.6.4 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:17:33
    2.2.2.2              110      00:28:08
    3.3.3.3              110      00:16:55
    4.4.4.4              110      00:12:49
    5.5.5.5              110      00:12:10
    6.6.6.6              110      00:20:18
    7.7.7.7              110      00:17:12
  Distance: (default is 110)

Medellin3#
```

Fuente: Autor

Figura 28. Ingresamos el comando, Show ip protocols en ISP

```
ISP#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 7.7.7.7
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.0 0.0.0.3 area 0
    209.17.220.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:18:54
    2.2.2.2              110      00:29:29
    3.3.3.3              110      00:18:17
    4.4.4.4              110      00:14:10
    5.5.5.5              110      00:13:31
    6.6.6.6              110      00:21:40
    7.7.7.7              110      00:18:33
  Distance: (default is 110)

ISP#
```

Fuente: Autor

b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

En el ítem anterior se realizado el desarrollo de este donde se mostraron las respectivas consultas a través del comando show ip route

5.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Desarrollo Parte 5.

Configurando Bogota1

```
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#interface Serial0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#username ISP secret cisco
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#exit
```

Configurando Medellin1

```
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#interface Serial0/1/1
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#username ISP secret cisco
Medellin1(config)#int s0/1/1
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username MEDELLIN password cisco
```

```
Medellin1(config-if)#exit
```

Continuamos con la configuración de ISP

```
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface Serial0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shu
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface Serial0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#username MEDELLIN secret cisco
ISP(config)#int s0/0/0
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#exit
ISP(config)#username BOGOTA secret cisco
ISP(config)#int s0/0/1
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
```

5.2.6 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.
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.

En esta parte se desarrolla lo solicitado en los ítem de la Parte 6.

Configurando Bogota1

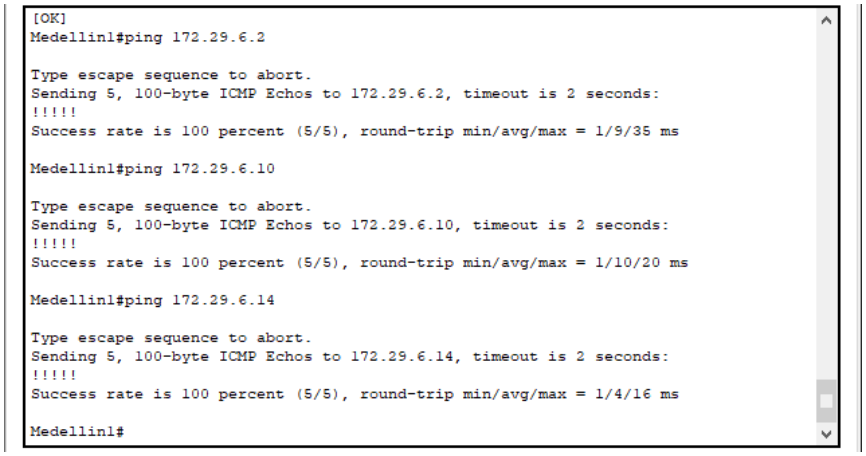
```
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#ip access-list standard HOST
Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
Bogota1(config-std-nacl)#exit
Bogota1(config)#ip nat inside source list HOST interface s0/0/0 overload
Bogota1(config)#int 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
Bogota1(config)#exit
Bogota1#show ip nat translation
```

Configurando Medellein1

```
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
```

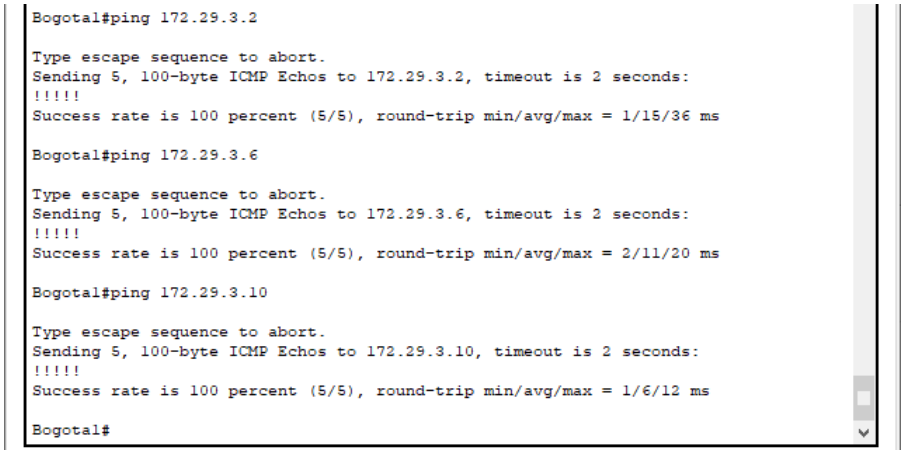
```
Medellin1(config)#int s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/1
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#exit
Medellin1(config)#exit
Medellin1#show ip nat translation
```

Figura 29. Utilizamos el comando ping de Medellin1 a Medellin2 y Medellin3



Fuente: Autor

Figura 30. Utilizamos el comando ping de Bogota1 a Bogota2 y Bogota3



Fuente: Autor

5.2.7 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.
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

A continuación, configuramos Medellin2

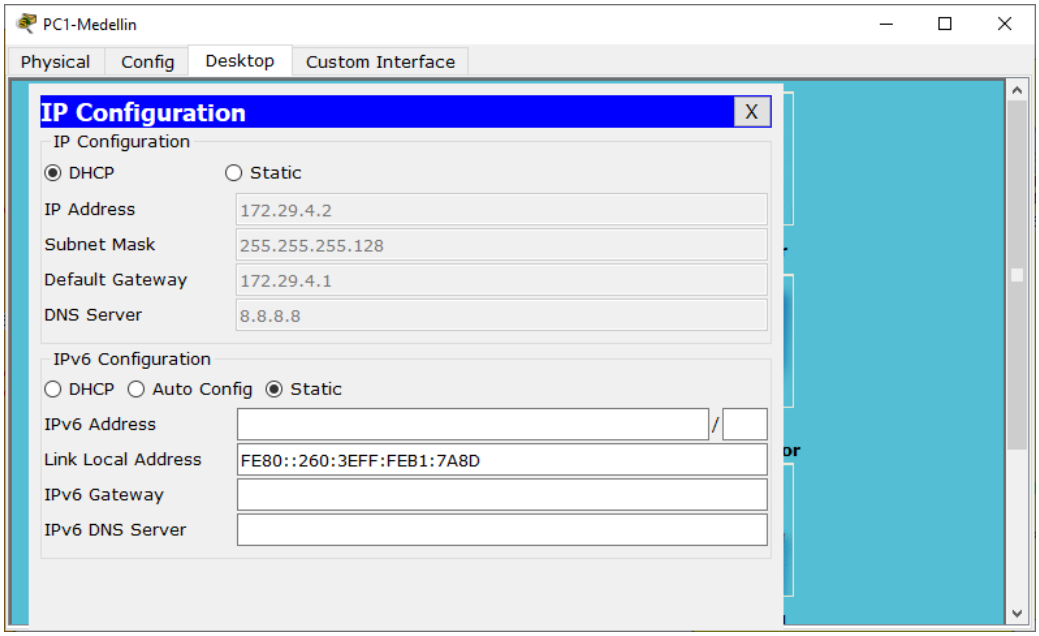
```
Medellin2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#ip dhcp excluded-address 172.29.4.1
Medellin2(config)#ip dhcp pool MEDELLIN2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp excluded-address 172.29.4.29
Medellin2(config)#ip dhcp pool MEDELLIN3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
Medellin2(config)#
```

Ya que Medellin3 tiene Red LAN pero servirá como Servidor DHCP se requiere configurar “ip helper” el cual permitirá hacer de un router de tránsito para llegar al router con el rol de DHCP. Tenemos que usar el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la IP del router de Medellin2, la dirección IP de la interfaz de salida Medellin2 será (s0/0/0 - 172.29.6.5):

Configuramos Medellin3

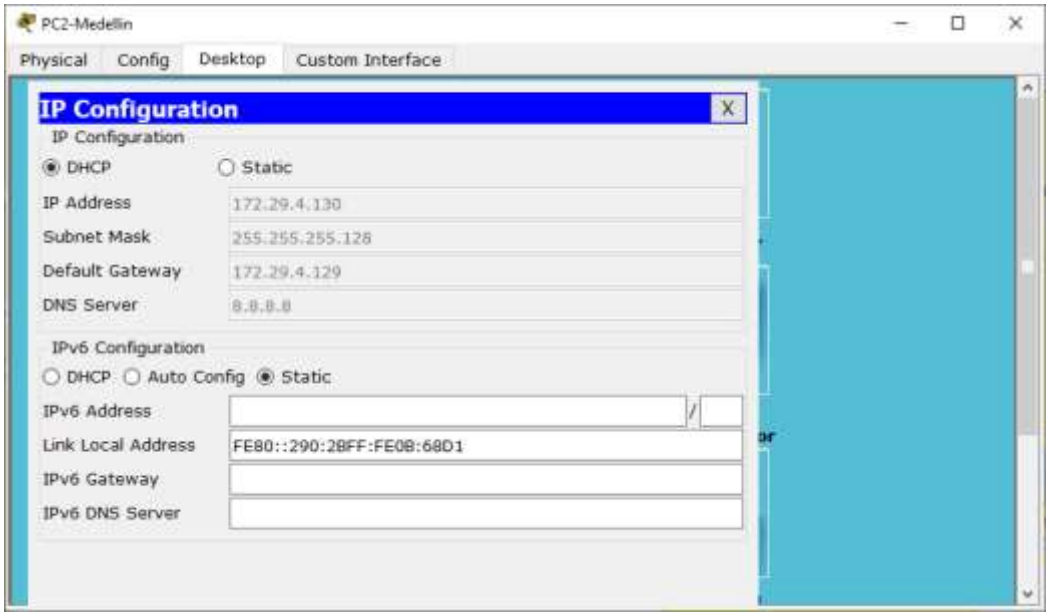
```
Medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#int g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
Medellin3(config-if)#exit
```

Figura 31. Configuración PC1-Medellin



Fuente: Autor

Figura 32. Configuración PC2-Medellin



Fuente: Autor

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

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

Configuramos Bogota2

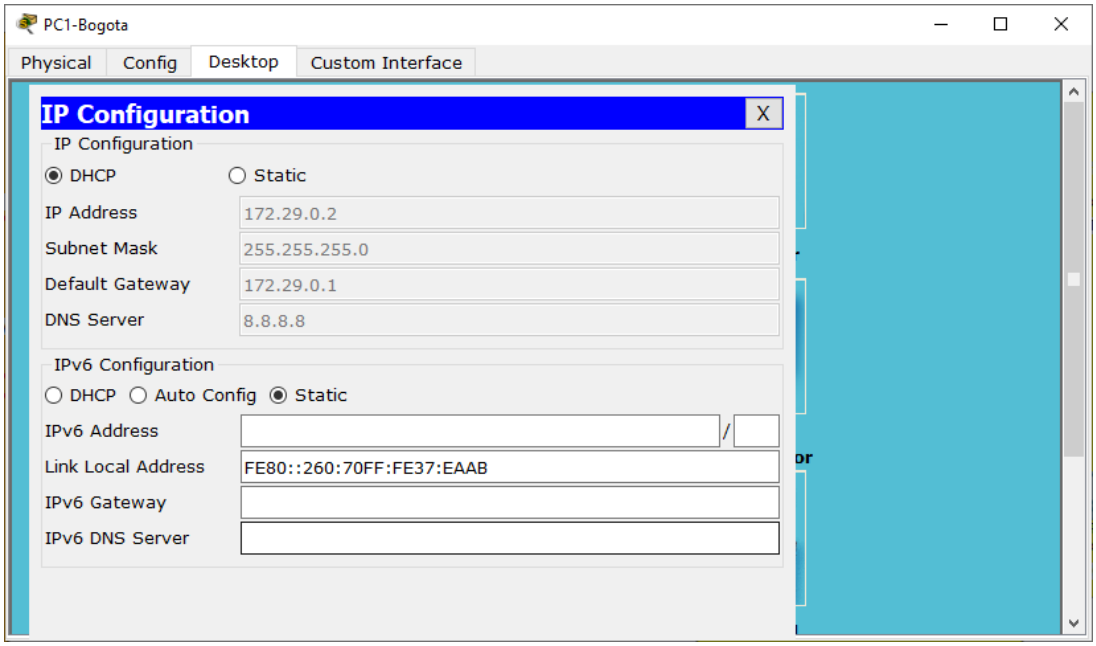
```
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#ip dhcp excluded-address 172.29.0.1
Bogota2(config)#ip dhcp pool BOGOTA2
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.0.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#exit
Bogota2(config)#ip dhcp excluded-address 172.29.1.1
Bogota2(config)#ip dhcp pool BOGOTA3
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.1.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#exit
Bogota2(config)#
```

Ya que Bogota3 tiene Red LAN pero servirá como Servidor DHCP se requiere configurar “ip helper” el cual permitirá hacer de un router de tránsito para llegar al router con el rol de DHCP. Tenemos que usar el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la IP del router de Bogota2, la dirección IP de la interfaz de salida Bogota2 será (s0/0/1 - 172.29.3.13):

Configuramos Bogota3

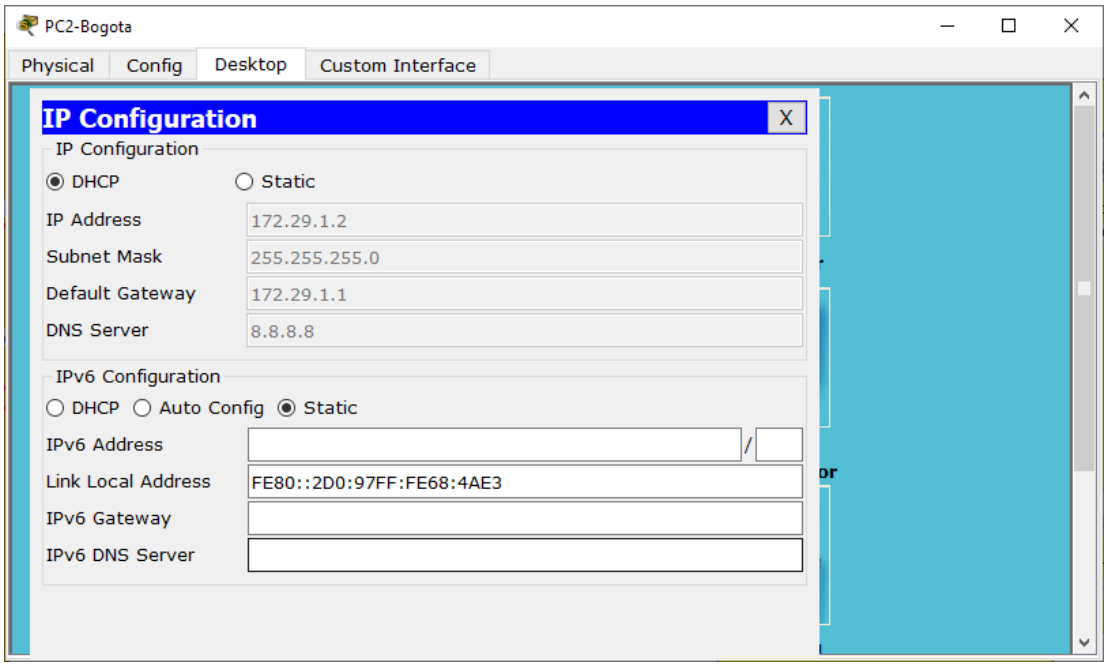
```
Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#int g0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
Bogota3(config-if)#exit
```

Figura 33. Configuración PC1-Bogota



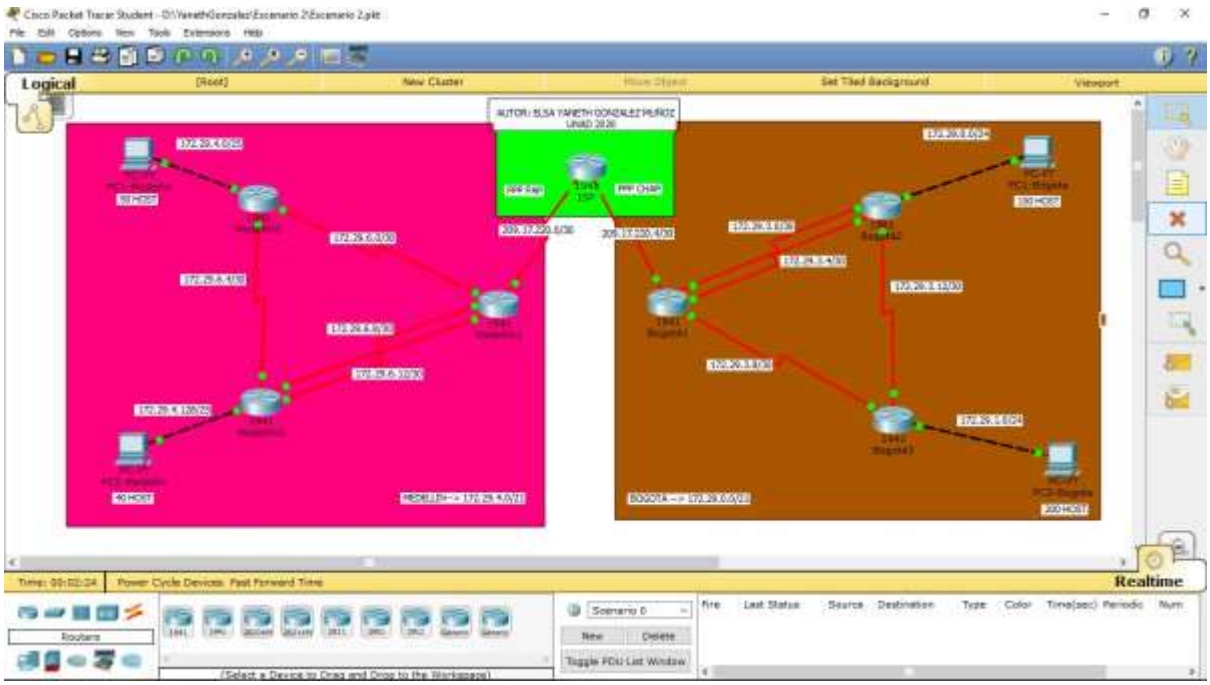
Fuente: Autor

Figura 34. Configuración PC2-Bogota



Fuente: Autor

Figura 35. Evidencia: Topología realizada en Packet Tracer



Fuente: Autor

CONCLUSIONES

Se logró desarrollar los dos escenarios propuestos por la Universidad Nacional Abierta y Distancia, dentro del Diplomado de Profundización CCNA como trabajo de grado, aplicando los conocimientos adquiridos a lo largo de dicho diplomado, utilizando Packet Tracer como herramienta de simulación, donde se diseñó la topología de las redes y la respectiva configuración de cada uno de sus dispositivos.

se utilizaron diferentes comandos que nos permiten verificar el estado de la conexión de la red, se establecieron contraseñas de acceso en el modo Exe privilegiado, consola y telnet para que el administrador de la red tenga control de los equipos.

Se utilizó el protocolo de enrutamiento RIP siendo éste un vector distancia que se utiliza para enrutar direcciones IPv4 en redes pequeñas y el protocolo de enrutamiento OSPF que hace posible la gestión de grandes redes.

OSPF tiene mejor aproximación que RIP ya que los cambios en el ruteo se propagan en forma instantánea y no periódica

Desarrollando este tipo de actividades nos permite darnos una idea de los retos que se nos pueden presentar en un futuro en nuestra vida laboral.

BIBLIOGRAFÍA

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

ANEXOS

ANEXO 1: ARCHIVO PKT ESCENARIO 1

https://drive.google.com/open?id=1JIA96g02Fe3AQ4b6DDWJdcmTQdImcPM7

ANEXO 2: ARCHIVO PKT ESCENARIO 2
https://drive.google.com/open?id=1O6SFfLU0qFJor7dlQ-TVqvZTOSUvn0qH