

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

JORGE MANRIQUE CHAVARRO

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

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

JORGE MANRIQUE CHAVARRO

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN)

TUTOR
DIEGO EDINSON RAMIREZ

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

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Tunja 22, 05, 2020

Dedico este trabajo, primeramente, a Dios y la Santísima Virgen por el don de la salud y vida para poder lograr este objetivo, a mis padres, a mi novia y a las personas que siempre me han apoyado para finalizar con éxito este proceso.

AGRADECIMIENTOS

Agradezco primeramente a Dios por cada una de sus bendiciones recibidas, a mis padres y hermanos por su apoyo incondicional y un agradecimiento especial a la red de tutores de la Universidad Nacional Abierta y a Distancia por compartir sus conocimientos y acompañarnos a lo largo de este camino.

A mis compañeros por su colaboración, porque también fueron parte fundamental para lograr cumplir este sueño académico.

CONTENIDO

	Pág.
1 INTRODUCCIÓN	15
2 OBJETIVOS	16
2.1 OBJETIVO GENERAL	16
2.2 OBJETIVOS ESPECÍFICOS	16
3 PLANTEAMIENTO DEL PROBLEMA	17
3.1 DEFINICIÓN DEL PROBLEMA	17
3.2 JUSTIFICACIÓN	17
4 MATERIALES Y MÉTODOS	18
4.1 MATERIALES	18
4.1 METODOLOGÍA	18
5 DESARROLLO DEL PROYECTO	19
5.1 ESCENARIO 1	19
5.1.1 Parte 1: Inicializar dispositivos	20
5.1.2 Parte 2: Configurar los parámetros básicos de los dispositivos	21
5.1.3 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	38
5.1.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2	45
5.1.5 Parte 5: Implementar DHCP y NAT para IPv4	49
5.1.6 Parte 6: Configurar NTP	55
5.1.7 Parte 7: Configurar y verificar las listas de control de acceso (ACL)	56
5.2 ESCENARIO 2	61
5.2.1 Parte 1: Configuración del enrutamiento	71
5.2.2 Parte 2: Tabla de Enrutamiento.	75
5.2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.	83
5.2.4 Parte 4: Verificación del protocolo OSPF.	84
5.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.	91
5.2.6 Parte 6: Configuración de PAT.	93

5.2.7 Parte 7: Configuración del servicio DHCP.	96
CONCLUSIONES	100
BIBLIOGRAFÍA	101
ANEXOS	104

LISTA DE TABLAS

	Pág
Tabla 1: Inicializar y volver a cargar los routers y los switches	20
Tabla 2: Configurar la computadora de Internet	22
Tabla 3: Configurar R1	22
Tabla 4: Configurar R2	25
Tabla 5: Configurar R3	29
Tabla 6: Configurar S1	32
Tabla 7: Configurar el S3	34
Tabla 8: Verificar la conectividad de la red	35
Tabla 9: Configurar la seguridad del S1, las VLAN y el routing entre VLAN	38
Tabla 10: Configurar la seguridad del S3, las VLAN y el routing entre VLAN	40
Tabla 11: Configurar la seguridad del R1	42
Tabla 12: Verificar la conectividad de la red	43
Tabla 13: Configurar RIPv2 en el R1	45
Tabla 14: Configurar RIPv2 en el R2	47
Tabla 15: Configurar RIPv2 en el R3	48
Tabla 16: Verificar la información de RIP	49

Tabla 17: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	49
Tabla 18: Configurar la NAT estática y dinámica en el R2	51
Tabla 19: Verificar el protocolo DHCP y la NAT estática	53
Tabla 20: Configurar NTP	55
Tabla 21: Restringir el acceso a las líneas VTY en el R2	56
Tabla 22: Introducir el comando de CLI adecuado	59
Tabla 23: Configurar la topología de red, de acuerdo con las especificaciones	65
Tabla 24: Deshabilitar la propagación del protocolo OSPF	83

LISTA DE FIGURAS

	Pág
Figura 1: Topología escenario 1	19
Figura 2: Ping R1 to R2, S0/0/0	36
Figura 3: Ping R2 to R3, S0/0/1	36
Figura 4: PC de Internet to Gateway predeterminado	37
Figura 5: Ping de S1 a R1, dirección VLAN 99 y R1, dirección VLAN 21	44
Figura 6: Ping de S3 a R1, dirección VLAN 99 y R1, dirección VLAN 23	45
Figura 7: Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	53
Figura 8: Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	54
Figura 9: Verificar que la PC-A pueda hacer ping a la PC-C	54
Figura 10: Acceder al servidor web (209.165.200.229)	55
Figura 11: Prueba de Telnet de R1 a R2	57
Figura 12: Prueba de Telnet de R3 a R2	58
Figura 13: Topología del escenario 1 Finalizada en Packet Tracer	60
Figura 14: Topología de red escenario 2	61
Figura 15: Comando Show ip route en Bogota1	76

Figura 16: Comando Show ip route en Bogota2	77
Figura 17: Comando Show ip route en Bogota3	78
Figura 18: Comando Show ip route en Medellin1	79
Figura 19: Comando Show ip route en Medellin2	80
Figura 20: Comando Show ip route en Medellin3	81
Figura 21: Comando Show ip route en ISP	82
Figura 22: Show ip protocols en Bogota1	85
Figura 23: Show ip protocols en Bogota2	86
Figura 24: Show ip protocols en Bogota3	87
Figura 25: Show ip protocols en Medellin1	88
Figura 26: Show ip protocols en Medellin2	89
Figura 27: Show ip protocols en Medellin3	90
Figura 28: Show ip protocols en ISP	91
Figura 29: Verificamos mediante comando ping de Medellin1 a Medellin2 y Medellin3	95
Figura 30: Verificamos mediante comando ping de Bogota1 a Bogota2 y Bogota3	95
Figura 31: Configuración Med-PC1 y Med-PC2	97
Figura 32: Configuración Bog-PC1 y Bog-PC2	98
Figura 33: Topología del escenario 2 finalizada en Packet Tracer	99

LISTA DE ANEXOS

	Pág
Anexo 1: Escenario 1 archivo PKA	104
Anexo 2: Escenario 2 archivo PKA	104

GLOSARIO

IPv4 o IPv6: Direcciones de uso local, de 32 y 128 bits respectivamente.

DIRECCIÓN MAC: También se conoce como dirección física, dirección del hardware o dirección del adaptador de red

ISP: Proveedor de servicios de Internet.

RED LAN: Red de computadoras que abarca un área reducida

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

SUBRED: Uno o más enlaces que utilizan el mismo prefijo de red.

ROUTER: 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.

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.

DIRECCIÓN ANYCAST: Dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a uno-entre-vario.

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

RESUMEN

En este documento encontrará el desarrollo de dos escenarios propuestos en la prueba de habilidades, en el cual se realizarán configuraciones básicas y avanzadas en los diferentes dispositivos que se encuentran en cada una de las topologías propuestas, poniendo a prueba los conocimientos que se adquirieron durante el transcurso del diplomado de profundización cisco (diseño e implementación de soluciones integradas lan / wan), entre lo cuales trataremos temas como protocolos de routing dinámico (RIPv2), configuración de servers DHCP, Network Address Translation (NAT), Listas de control de acceso (ACL).

PALABRAS CLAVE: Trabajo de Grado, Packet Tracer, RIPv2, Protocolos de Seguridad, Cisco, Redes, IPv4, IPv6, DHCP, Diplomado, NAT, LAN, WAN, ACL.

1 INTRODUCCIÓN

Hoy en día es indispensable para las empresas contar con personal calificado e idóneo en el manejo de redes de comunicaciones, capaz de solucionar problemas reales a la brevedad y aplicando las normas vigentes, por eso es tan importante la certificación CCNA, ya que permite conocer o poner a prueba los conocimientos adquiridos de los estudiantes a lo largo del diplomado de profundización Cisco (diseño e implementación de soluciones integradas LAN/WAN) y llevarlo a un entorno laboral real.

En este documento se da la solución a los 2 escenarios propuestos, en los cuales se tratarán temas vistos a lo largo del diplomado como son: protocolos de routing dinámico (RIPv2), configuración de servers DHCP, Network Address Translation (NAT), Listas de control de acceso (ACL). Estos protocolos de seguridad se pueden aplicar en diferentes escenarios como empresas y hogares.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar el desarrollo de los dos escenarios propuestos en la prueba de habilidades utilizando la herramienta packet tracer, poniendo a prueba los niveles de comprensión y solución de problemas relacionados con Networking aplicando los conocimientos adquiridos durante el transcurso del diplomado

2.2 OBJETIVOS ESPECÍFICOS

- Implementar la topología propuesta para cada escenario mediante la herramienta de packet tracer.
- Realizar las conexiones solicitadas, utilizando el cableado de acuerdo con los diagramas de la topología.
- Realizar las configuraciones correspondientes a cada dispositivo de acuerdo con lo solicitado en cada escenario.
- Verificar que las redes y sus dispositivos funcionen de manera correcta.
- Generar un informe donde se evidencie el paso a paso del desarrollo de la prueba de habilidades prácticas CCNA.

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.

Excenario 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

Es necesario dar solución a los dos escenarios anteriormente mencionados con el objetivo de sustentar la prueba de habilidades correspondiente al diplomado de profundización Cisco, poniendo a prueba las habilidades adquiridas. Se implementará las topologías propuestas para lo cual se utilizará el simulador Packet Tracer, a su vez se realizará un paso a paso del proceso de desarrollo de cada ítem.

4 MATERIALES Y MÉTODOS

4.1 MATERIALES

- Computador portátil con sistema operativo Windows 10 de 64 bits.
- Software: Simulado packet tracer.
- Acceso a Internet.

4.1 METODOLOGÍA

Este trabajo se realizó de acuerdo con los escenarios planteados en la prueba de habilidades practicas CCNA mediante el uso de la herramienta Packet Tracer.

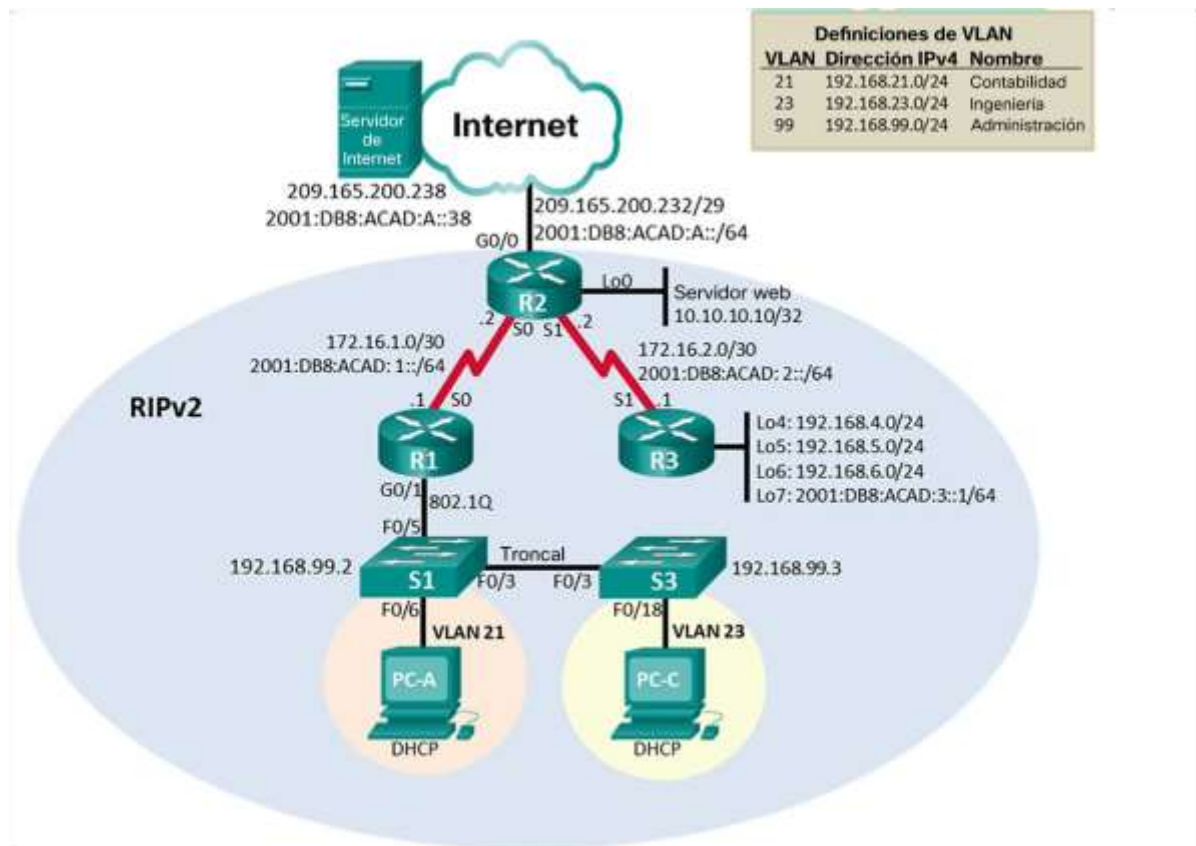
5 DESARROLLO DEL PROYECTO

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 escenario 1



Fuente: Prueba de habilidades prácticas CCNA

5.1.1 Parte 1: Inicializar dispositivos

5.1.1.1 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	Para esto 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	Utilizamos 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	Para Eliminar el archivo startup-config utilizamos el commando erase startup-config S1

	<p>Switch>enable Switch#erase startup-config S3 Switch>enable Switch#erase startup-config</p> <p>Para eliminar la base de datos de VLAN utilizamos el comando delete vlan.dat</p> <p>S1 Switch#delete vlan.dat</p> <p>S3 Switch#delete vlan.dat</p>
<p>Volver a cargar ambos switches</p>	<p>Para cargar los Switches utilizamos el comando reload</p> <p>S1 Switch#reload</p> <p>S3 Switch#reload</p>
<p>Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches</p>	<p>show flash</p> <p>S1 Switch#show flash:</p> <p>S3 Switch#show flash:</p>

Fuente: Autor

5.1.2 Parte 2: Configurar los parámetros básicos de los dispositivos

5.1.2.1 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.

5.1.2.2 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	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	Establecer class como contraseña cifrada R1(config)# enable secret class

Contraseña de acceso a la consola	<p>Establecer cisco como contraseña</p> <pre>R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit</pre>
Contraseña de acceso Telnet	<p>Establecer cisco como contraseña</p> <pre>R1(config)#line vty 0 4 R1(config-line)#pass R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit</pre>
Cifrar las contraseñas de texto no cifrado	<pre>R1(config)#service password-encryption</pre>
Mensaje MOTD	<p>Se prohíbe el acceso no autorizado.</p> <pre>R1(config)#banner motd #Se prohíbe el acceso no autorizado!#</pre>

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

Fuente: Autor

Nota: Todavía no configure G0/1.

5.1.2.3 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	Router(config)#no ip domain-lookup
Nombre del router	R2 Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	class R2(config)#enable secret class
Contraseña de acceso a la consola	cisco R2(config)#line console 0 R2(config-line)#pass R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	cisco R2(config)#line vty 0 4 R2(config-line)#pass 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 prohíbe el acceso no autorizado!#

<p>Interfaz S0/0/0</p>	<p>Establezca la descripción</p> <pre>R2(config)#interface s0/0/0 R2(config-if)#description conexion de R2- R1</pre> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.</p> <pre>R2(config-if)#ip address 172.16.1.2 255.255.255.252</pre> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre>R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64</pre> <p>Activar la interfaz</p> <pre>R2(config-if)#no shutdown</pre>
------------------------	--

<p>Interfaz S0/0/1</p>	<p>Establecer la descripción</p> <pre>R2(config)#interface s0/0/1 R2(config-if)#description conexion R2-R3</pre> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R2(config-if)#ip address 172.16.2.1 255.255.255.252</pre> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre>R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64</pre> <p>Establecer la frecuencia de reloj en 128000.</p> <pre>R2(config-if)#clock rate 128000</pre> <p>Activar la interfaz</p> <pre>R2(config-if)#no shutdown</pre>
------------------------	--

<p>Interfaz G0/0 (simulación de Internet)</p>	<p>Establecer la descripción.</p> <p>R2(config-if)#description conexion de R2-Internet</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>R2(config-if)#ip address 209.165.200.233 255.255.255.248</p> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <p>R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64</p> <p>Activar la interfaz</p> <p>R2(config-if)#no shutdown</p>
<p>Interfaz loopback 0 (servidor web simulado)</p>	<p>Establecer la descripción.</p> <p>R2(config)#interface loopback 0 R2(config-if)#des R2(config-if)#description servidor web simulado</p> <p>Establezca la dirección IPv4.</p> <p>R2(config-if)#ip address 10.10.10.10 255.255.255.255</p>

Ruta predeterminada	<p>Configure una ruta IPv4 predeterminada de G0/0.</p> <p>R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0</p> <p>Configure una ruta IPv6 predeterminada de G0/0.</p> <p>R2(config)#ipv6 route ::/0 g0/0</p>
---------------------	---

Fuente: Autor

5.1.2.4 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	<p>Router>en</p> <p>Router#conf t</p> <p>Enter configuration commands, one per line.</p> <p>End with CNTL/Z.</p> <p>Router(config)#no ip domain-lookup</p>
Nombre del router	<p>R3</p> <p>Router(config)#hostname R3</p>
Contraseña de exec privilegiado cifrada	<p>class</p> <p>R3(config)#enable secret class</p>

Contraseña de acceso a la consola	cisco R3(config)#line console 0 R3(config-line)#pass R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	cisco R3(config)#line vty 0 4 R3(config-line)#pas 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 prohíbe el acceso no autorizado!#

<p>Interfaz S0/0/1</p>	<p>Establecer la descripción</p> <pre>R3(config)#int s0/0/1 R3(config-if)#des R3(config-if)#description conexion de R3-R2</pre> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.</p> <pre>R3(config-if)#ip address 172.16.2.2 255.255.255.252</pre> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre>R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64</pre> <p>Activar la interfaz</p> <pre>R3(config-if)#no shutdown</pre>
<p>Interfaz loopback 4</p>	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0</pre>
<p>Interfaz loopback 5</p>	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0</pre>

Interfaz loopback 6	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0</pre>
Interfaz loopback 7	<p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre>R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64</pre>
Rutas predeterminadas	<pre>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</pre>

Fuente: Autor

5.1.2.5 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	<pre>Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup</pre>

Nombre del switch	S1 Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	class S1(config)#enable secret class
Contraseña de acceso a la consola	cisco S1(config)#line console 0 S1(config-line)#pass S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	cisco S1(config)#line vty 0 4 S1(config-line)#pass 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 prohíbe el acceso no autorizado!#

Fuente: Autor

5.1.2.6 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	Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	S3 Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	class S3(config)#enable secret class
Contraseña de acceso a la consola	cisco S3(config)#line console 0 S3(config-line)#pas S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	cisco S3(config)#line vty 0 4 S3(config-line)#pass 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	<p>Se prohíbe el acceso no autorizado.</p> <p>S3(config)#banner motd #Se prohíbe el acceso no autorizado!#</p>
--------------	---

Fuente: Autor

5.1.2.7 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:

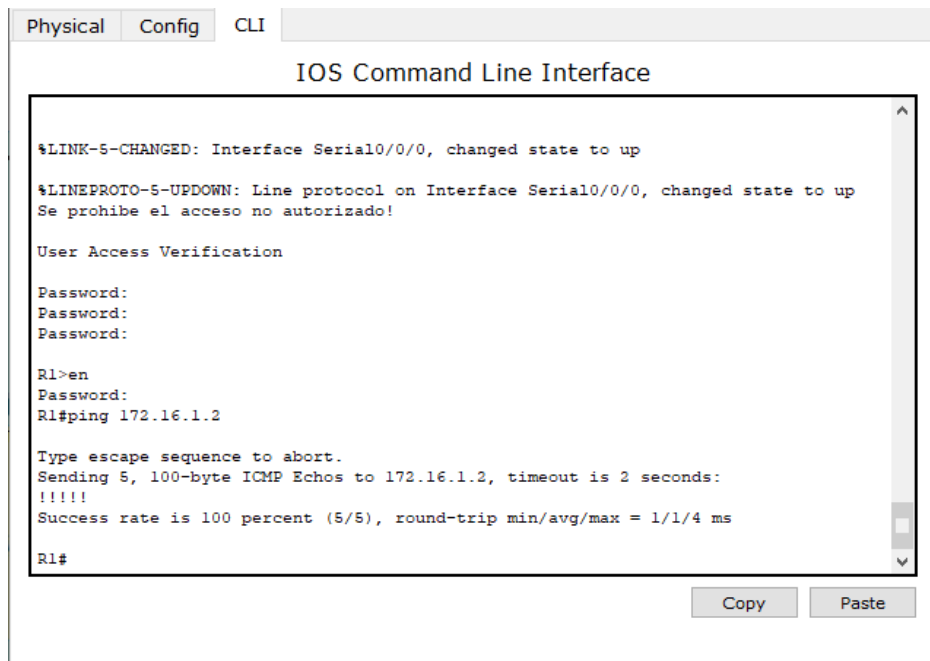
Tabla 8: Verificar la conectividad de la red

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

Fuente: Autor

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

Figura 2: Ping R1 to R2, S0/0/0



```
Physical Config CLI
IOS Command Line Interface

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Se prohíbe el acceso no autorizado!

User Access Verification

Password:
Password:
Password:

R1>en
Password:
R1#ping 172.16.1.2

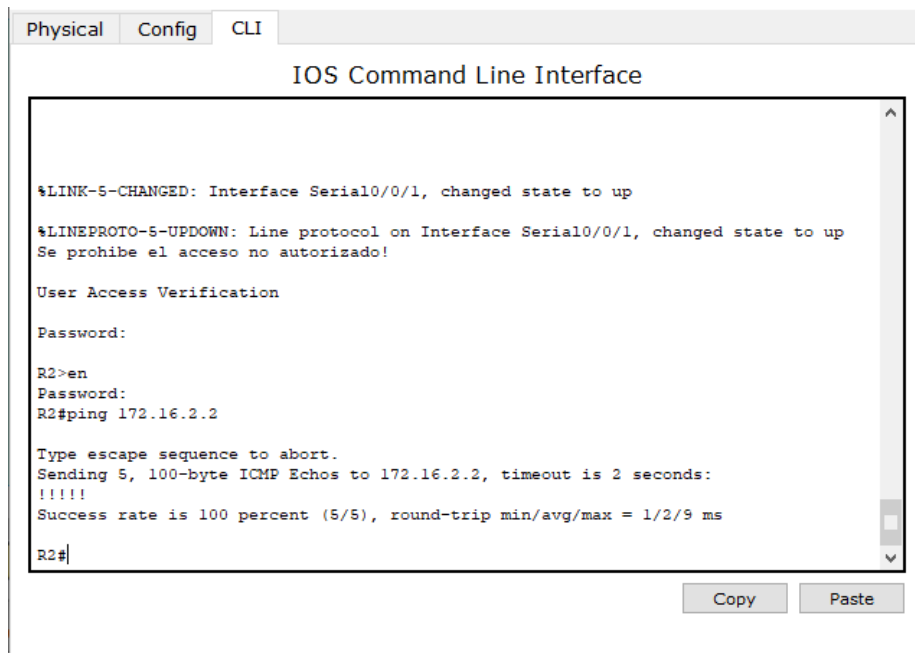
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#
```

Copy Paste

Fuente: Autor

Figura 3: Ping R2 to R3, S0/0/1



```
Physical Config CLI
IOS Command Line Interface

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Se prohíbe el acceso no autorizado!

User Access Verification

Password:

R2>en
Password:
R2#ping 172.16.2.2

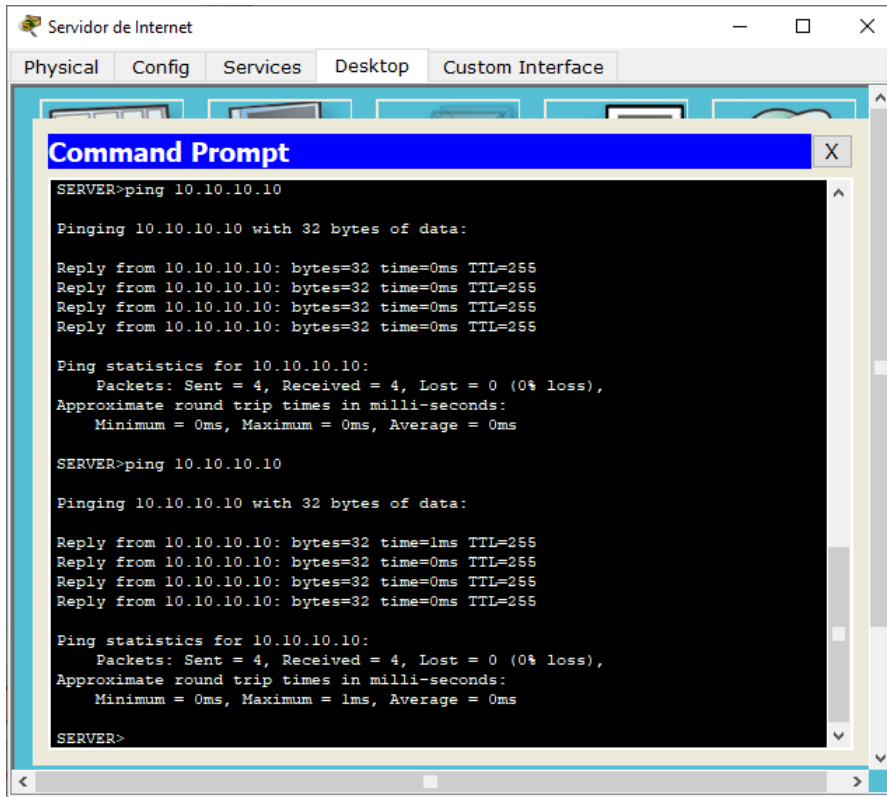
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

R2#
```

Copy Paste

Fuente: Autor.

Figura 4: PC de Internet to Gateway predeterminado



The image shows a screenshot of a virtual machine window titled "Servidor de Internet". The window has tabs for "Physical", "Config", "Services", "Desktop", and "Custom Interface". A "Command Prompt" window is open, displaying the following text:

```
SERVER>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=0ms TTL=255
Reply from 10.10.10.10: bytes=32 time=0ms TTL=255
Reply from 10.10.10.10: bytes=32 time=0ms TTL=255
Reply from 10.10.10.10: bytes=32 time=0ms TTL=255

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

SERVER>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=1ms TTL=255
Reply from 10.10.10.10: bytes=32 time=0ms TTL=255
Reply from 10.10.10.10: bytes=32 time=0ms TTL=255
Reply from 10.10.10.10: bytes=32 time=0ms TTL=255

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

SERVER>
```

Fuente: Autor

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

5.1.3.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9: Configurar la seguridad del S1, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<p>Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican</p> <p>S1>en Password: S1#conf t 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</p>
Asignar la dirección IP de administración.	<p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología</p> <p>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0</p>

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)#interface 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)#interface 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)#int 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.

5.1.3.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10: Configurar la seguridad del S3, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	Especificación
<p>Crear la base de datos de VLAN</p>	<p>Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.</p> <pre>S3>en Password: S3#conf t 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</pre>
<p>Asignar la dirección IP de administración</p>	<p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología</p> <pre>S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shu S3(config-if)#no shutdown S3(config-if)#exit</pre>

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)#interface 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)#interface 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.

5.1.3.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11: Configurar la seguridad del 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#conf t 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)#des 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)#interface g0/1 R1(config-if)#no shutdown

Fuente: Autor.

5.1.3.4 Paso 4: Verificar la conectividad de la red

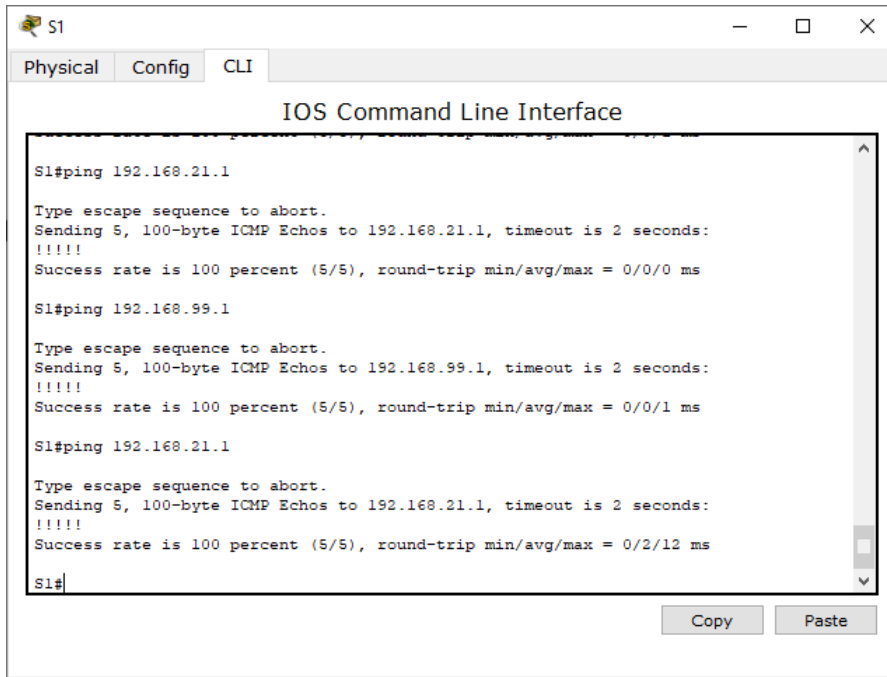
Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12: Verificar la conectividad de la red

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

Fuente: Autor

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



```
S1
Physical Config CLI
IOS Command Line Interface

S1#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

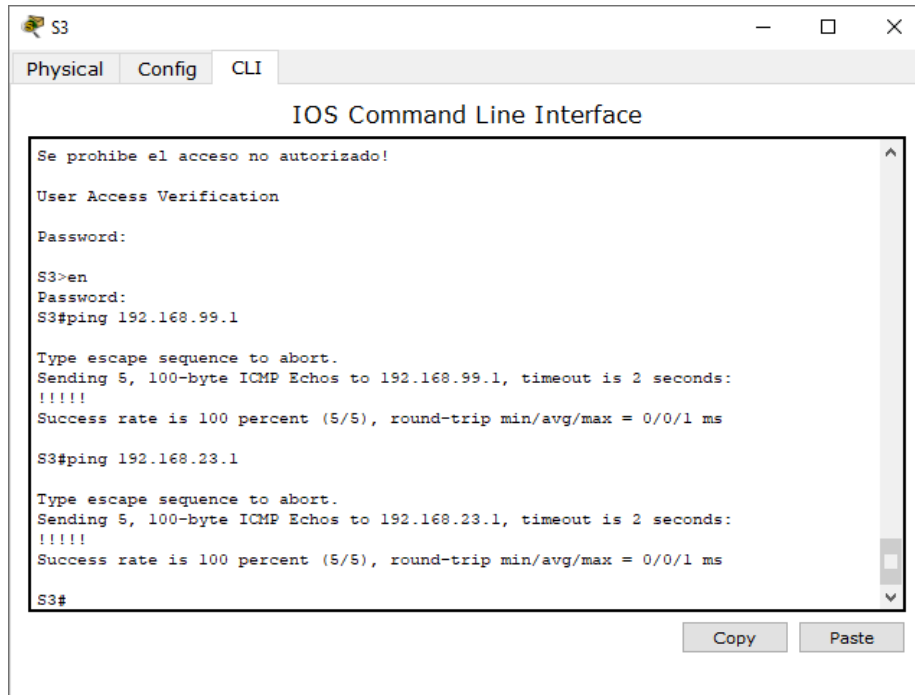
S1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/12 ms

S1#
```

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

5.1.4.1 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

<p>Anunciar las redes conectadas directamente</p>	<p>Asigne todas las redes conectadas directamente.</p> <p>Lo primero que hacemos es verificar las redes conectadas mediante el comando do show ip route connected</p> <pre>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</pre> <pre>R1(config-router)# 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</pre>
<p>Establecer todas las interfaces LAN como pasivas</p>	<pre>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</pre>
<p>Desactive la sumarización automática</p>	<pre>R1(config-router)#no auto-summary</pre>

Fuente: Autor.

5.1.4.2 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. Primero verificamos las redes 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.

5.1.4.3 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	Verificamos las redes 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)# 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.

5.1.4.4 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 interfaces pasivas configuradas en un router?	R1#Show ip protocols
¿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

5.1.5.1 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#conf t Enter configuration commands, one per line. End with CNTL/Z. 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

<p>Crear un pool de DHCP para la VLAN 21.</p>	<p>Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado</p> <pre>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</pre>
<p>Crear un pool de DHCP para la VLAN 23</p>	<p>Nombre: ENGR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado</p> <pre>R1(config)#ip dhcp pool ENGR 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</pre>

Fuente: Autor.

5.1.5.2 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	<p>Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15</p> <p>R2(config)#username webuser privilege 15 secret cisco12345</p>
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.	<p>Dirección global interna: 209.165.200.229</p> <p>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229</p>
Asignar la interfaz interna y externa para la NAT estática	<p>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</p>
Configurar la NAT dinámica dentro de una ACL privada	<p>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</p> <p>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</p>

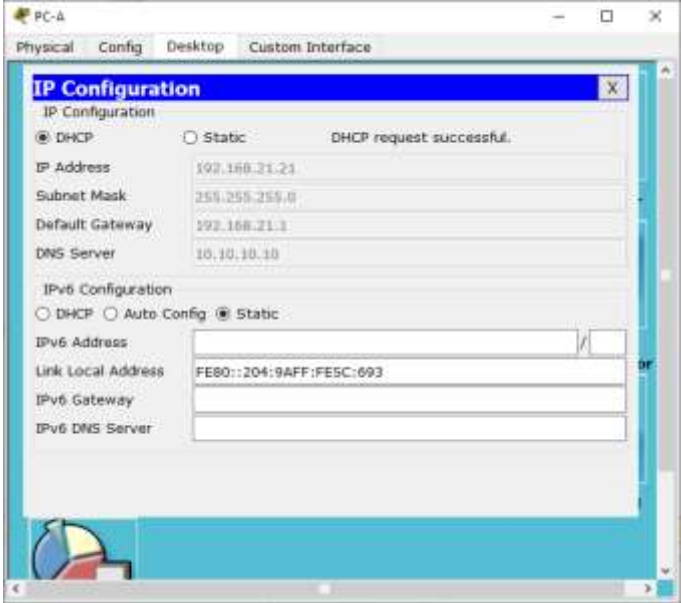
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Autor.

5.1.5.3 Paso 3: Verificar el protocolo DHCP y la NAT estática

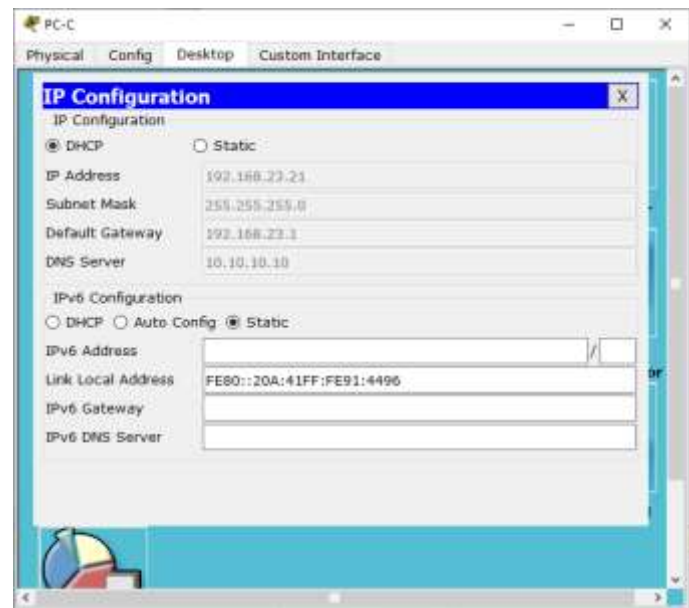
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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	<p data-bbox="792 380 1446 447">Figura 7: Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>  <p data-bbox="792 1087 987 1119">Fuente: Autor</p>

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

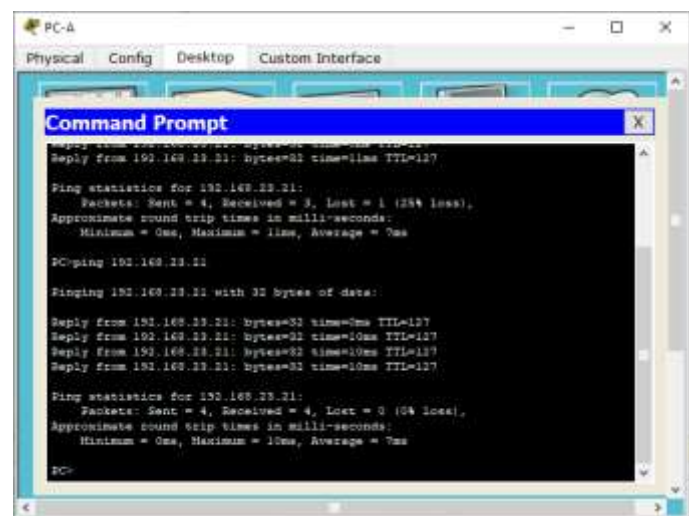
Figura 8: Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Fuente: Autor.

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

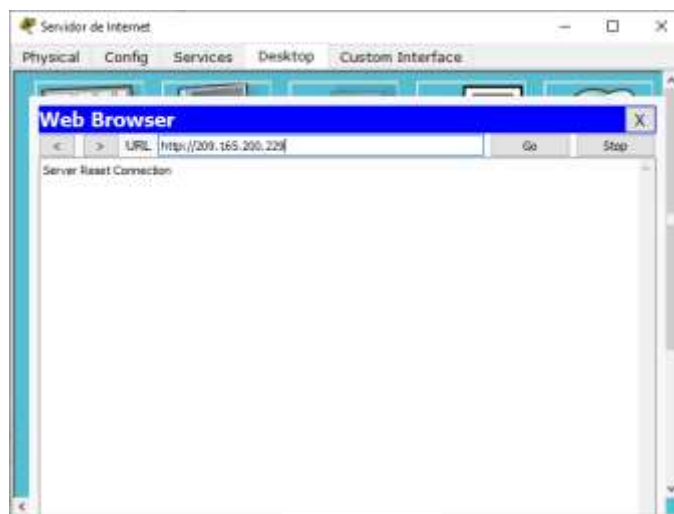
Figura 9: Verificar que la PC-A pueda hacer ping a la PC-C



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: Acceder al servidor web (209.165.200.229)



Fuente: Autor.

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.	<p>5 de marzo de 2016, 9 a. m.</p> <p>R2#clock set 09:00:00 5 March 2016</p>
Configure R2 como un maestro NTP.	<p>Nivel de estrato: 5</p> <p>R2(config)#ntp master 5</p>
Configurar R1 como un cliente NTP.	<p>Servidor: R2</p> <p>R1(config)#ntp server 172.16.1.2</p>

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)

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

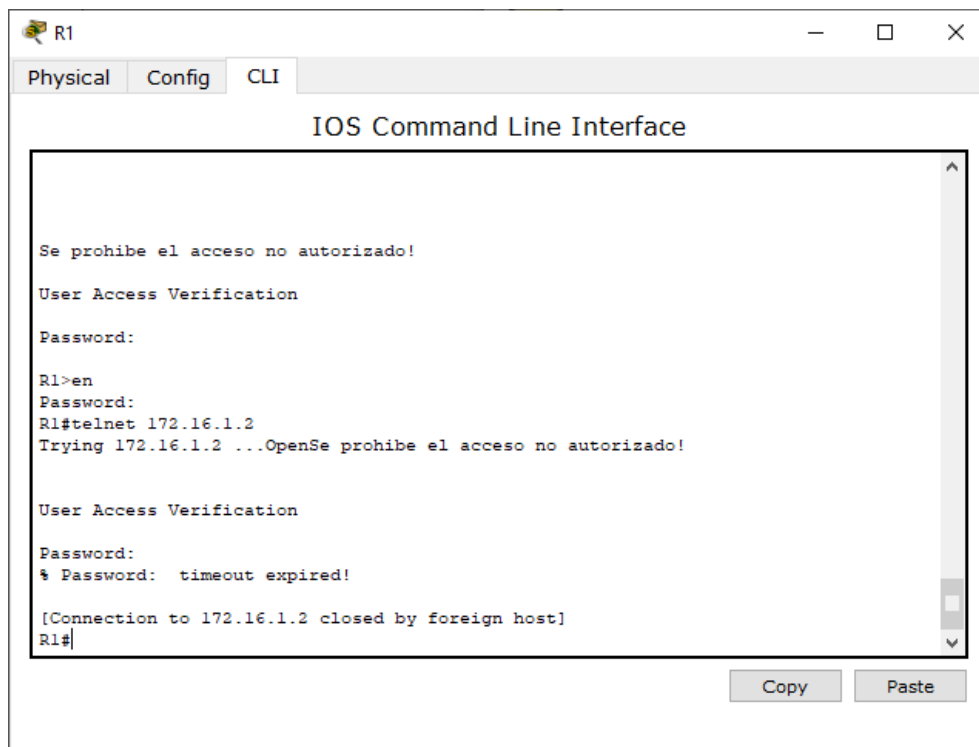
Tabla 21: Restringir el acceso a las líneas VTY en el R2

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#conf t 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

<p>Verificar que la ACL funcione como se espera</p>	<pre>R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado! User Access Verification Password: R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host</pre>
---	---

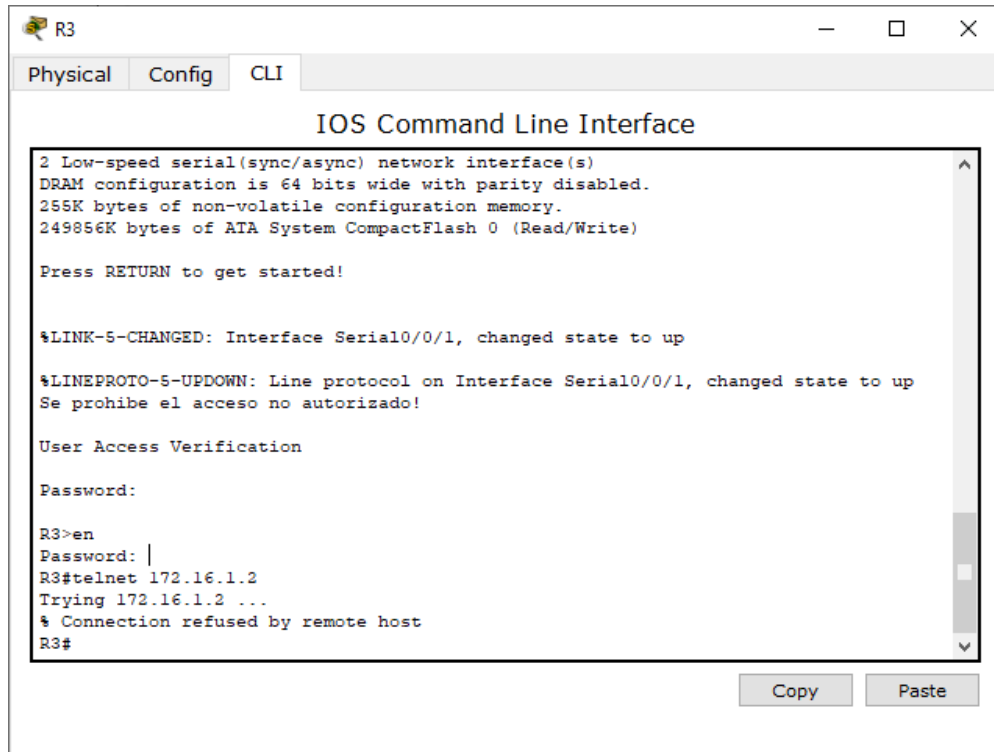
Fuente: Autor.

Figura 11: Prueba de Telnet de R1 a R2



Fuente: Autor.

Figura 12: Prueba de Telnet de R3 a R2



The screenshot shows a terminal window titled "R3" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" with the following text:

```
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Se prohíbe el acceso no autorizado!

User Access Verification

Password:

R3>en
Password: |
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

Fuente: Autor.

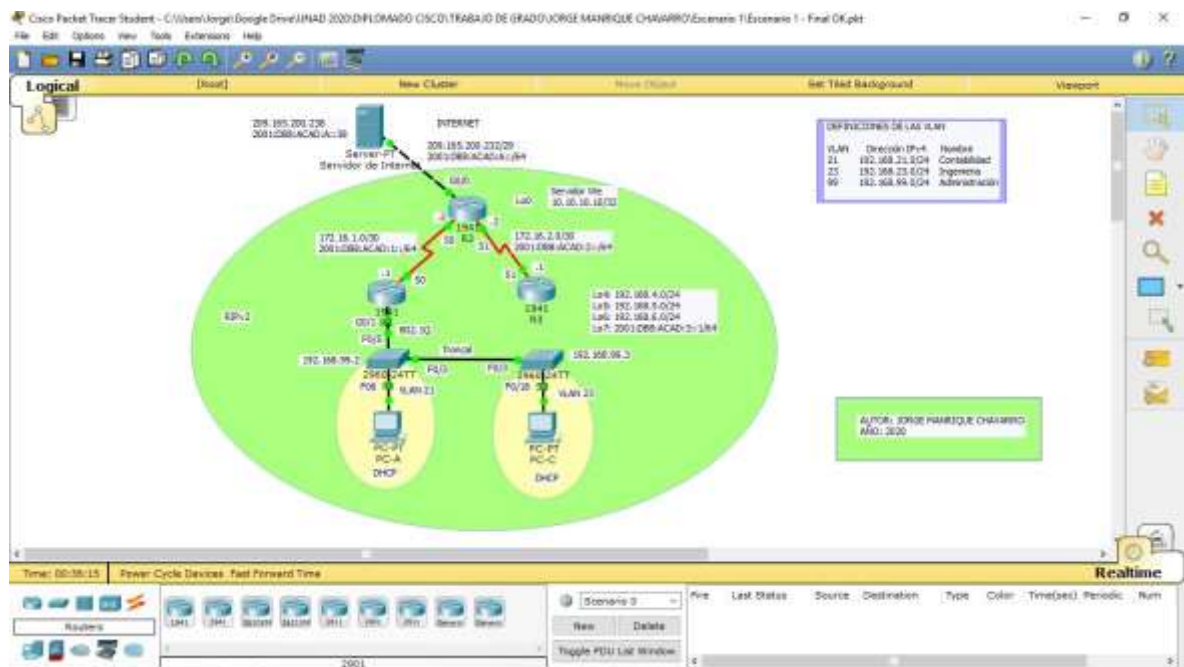
5.1.7.2 Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 22: Introducir el 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	<pre>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#</pre>
Restablecer los contadores de una lista de acceso	<pre>R2#clear access-list counters</pre>
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	<pre>R2#show ip interface</pre>
¿Con qué comando se muestran las traducciones NAT?	<p>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.</p> <pre>R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- ---</pre> <p>R2#</p>
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	<pre>R2(config)#clear ip nat translation *</pre>

Fuente: Autor.

Figura 13: Topología del escenario 1 Finalizada en Packet Tracer



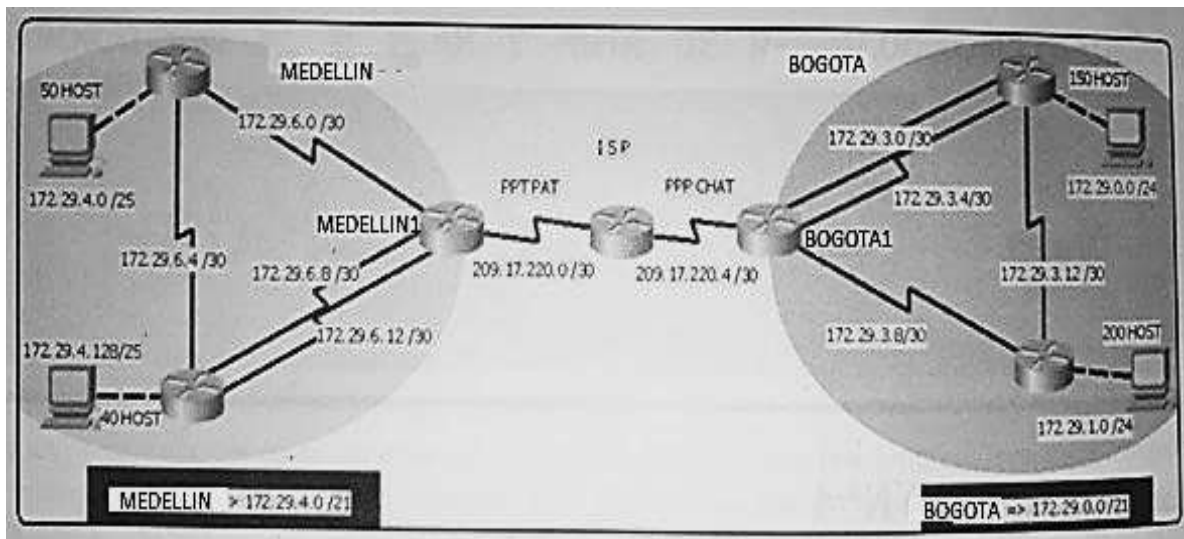
Fuente: Autor.

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 prácticas CCNA

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán 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).

ISP

```
Router>en
Router#conf t
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 prohíbe el acceso no autorizado.##%
```

Medellin1

```
Router>en
Router#conf t
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 prohíbe el acceso no autorizado.##
```

Medellin2

```
Router>en
Router#conf t
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 prohíbe el acceso no autorizado.#
```

Medellin3

```
Router>enable
Router#con
Router#conf
Router#configure te
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 prohíbe el acceso no autorizado.#
```

Bogota1

```
Router>enable
Router#con
Router#conf
Router#configure t
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 prohíbe el acceso no autorizado.#
```

Bogota2

```
Router>en
Router>enable
Router#conf
Router#configure te
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 prohíbe el acceso no autorizado.#

```

Bogota3

```

Router>en
Router>enable
Router#conf
Router#configure te
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 prohíbe el acceso no autorizado.#

```

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

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

Tabla 23: Configurar la topología de red, de acuerdo con las especificaciones

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.

Bogota1

Bogota1>en

Password:

Bogota1#conf t

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
Bogota1(config-if)#
```

Bogota2

```
Bogota2>en
Password:
Bogota2#conf t
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 sh
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
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)#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)#exit
Bogota2(config)#int g0/0
Bogota2(config-if)#description Connection to Bog-PC1
Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota2(config-if)#no shutdown
```

Bogota3

```
Bogota3>en
Password:
Bogota3#conf t
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 shu
Bogota3(config-if)#no shutdown
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)#exit
Bogota3(config)#int g0/0
Bogota3(config-if)#description Connection to Bog-PC2
Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota3(config-if)#no shu
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
```

Medellin1

```
Medellin1>en
Password:
Medellin1#conf t
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
```

Medellin2

```
Medellin2>en
Password:
Medellin2#conf t
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 shu
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 Med-PC1
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shu
Medellin2(config-if)#no shutdown
```

Medellin3

```
Medellin3>en
Password:
Password:
Medellin3#conf t
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 shu
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 shu
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 shu
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#int g0/0
Medellin3(config-if)#description Connection to Med-PC2
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shu
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
```

ISP

```
ISP>en
Password:
ISP#conf t
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)#exit
ISP#
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 shu
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.

Bogota1

```
Bogota1>en
Password:
Bogota1#conf t
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)#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)#
```

Bogota2

```
Bogota2#conf t
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
Bogota2(config)#
```

Bogota3

```
Bogota3>en
Password:
Bogota3#conf t
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
```

Medellin1

```
Medellin1#conf t
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
```

Medellin2

```
Medellin2>en
Password:
Medellin2#conf t
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
```

Medellin3

```
Medellin3>en
Password:
Medellin3#conf t
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)#
```

ISP

```
ISP#conf t
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.

Bogota1

```
Bogota1#conf t
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)#
```

Medellin1

```
Medellin1#conf t
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.

ISP

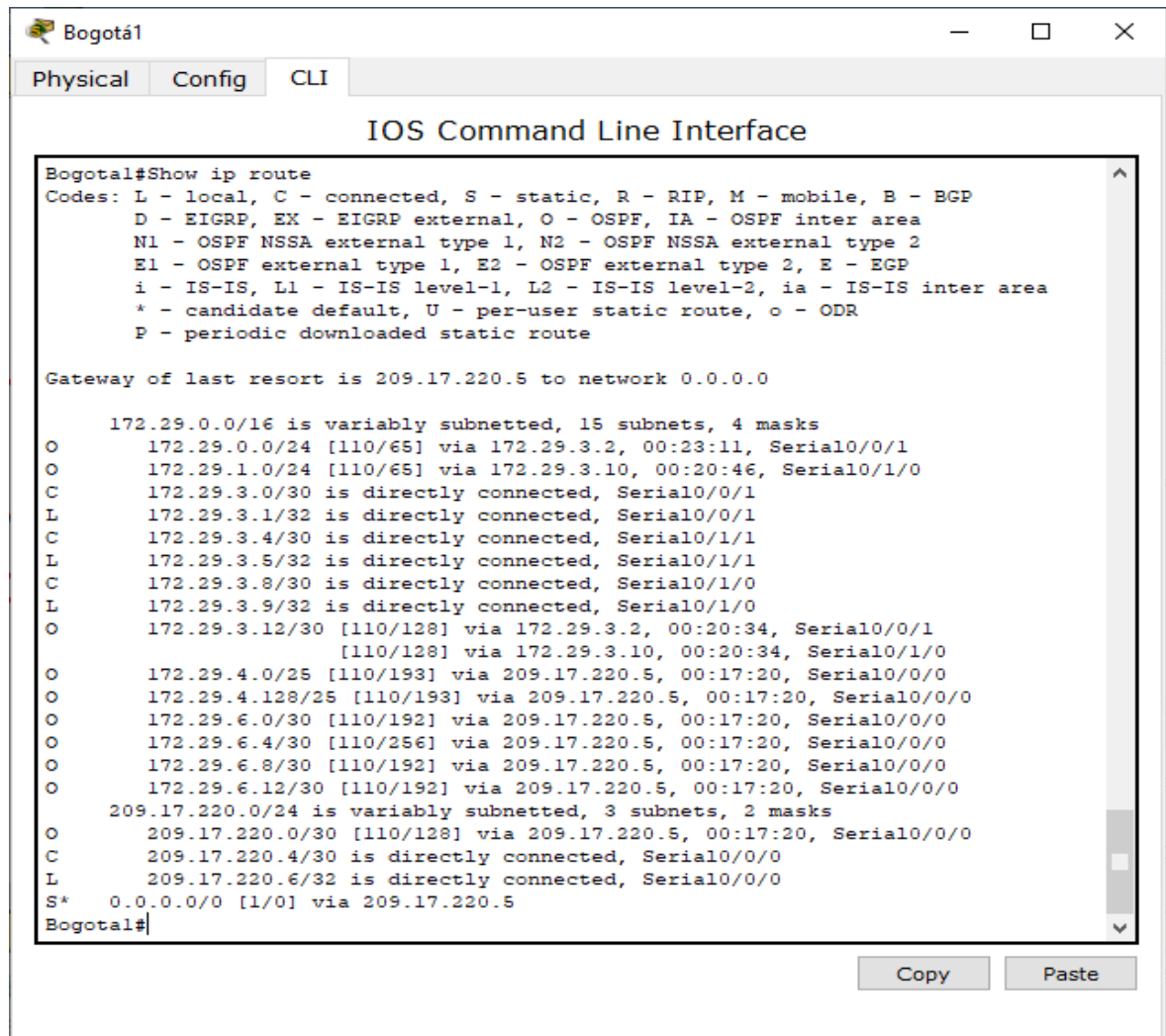
```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

5.2.2 Parte 2: Tabla de Enrutamiento.

- Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
- Verificar el balanceo de carga que presentan los routers.
- 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.
- Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
- 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: Comando Show ip route en Bogota1



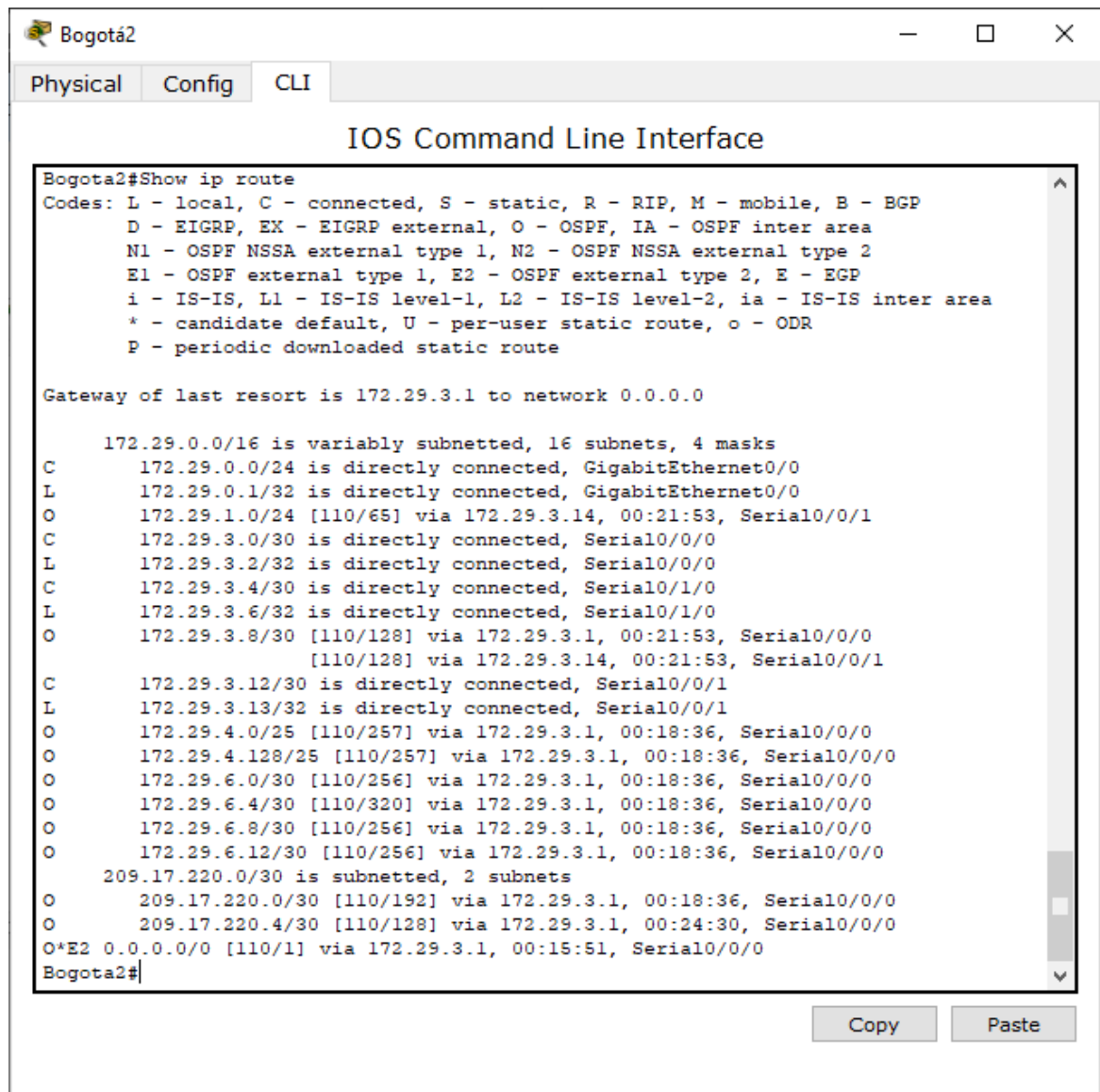
```
Bogota1#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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: Comando Show ip route en Bogota2



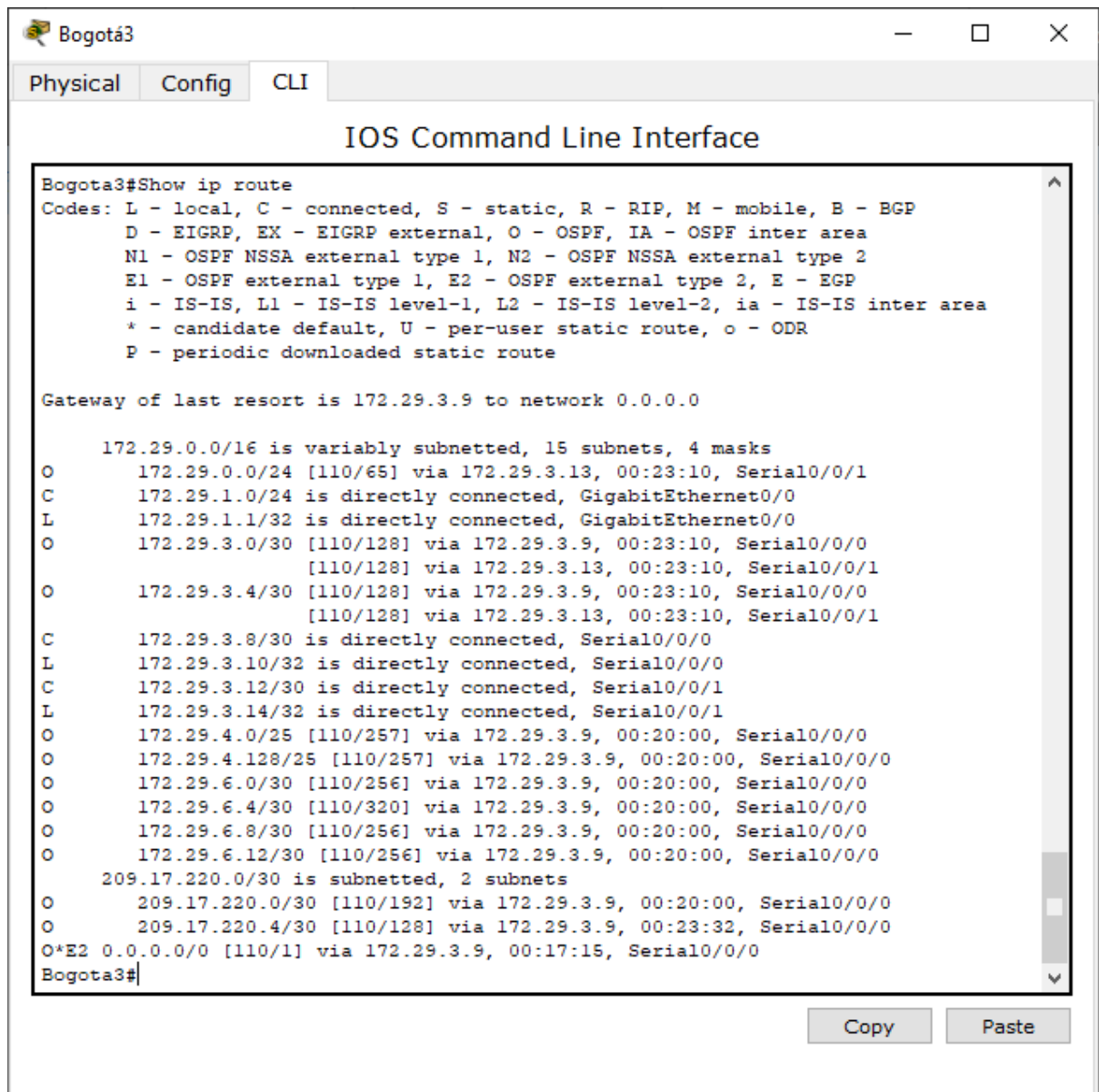
```
Bogota2#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - 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: Comando Show ip route en Bogota3



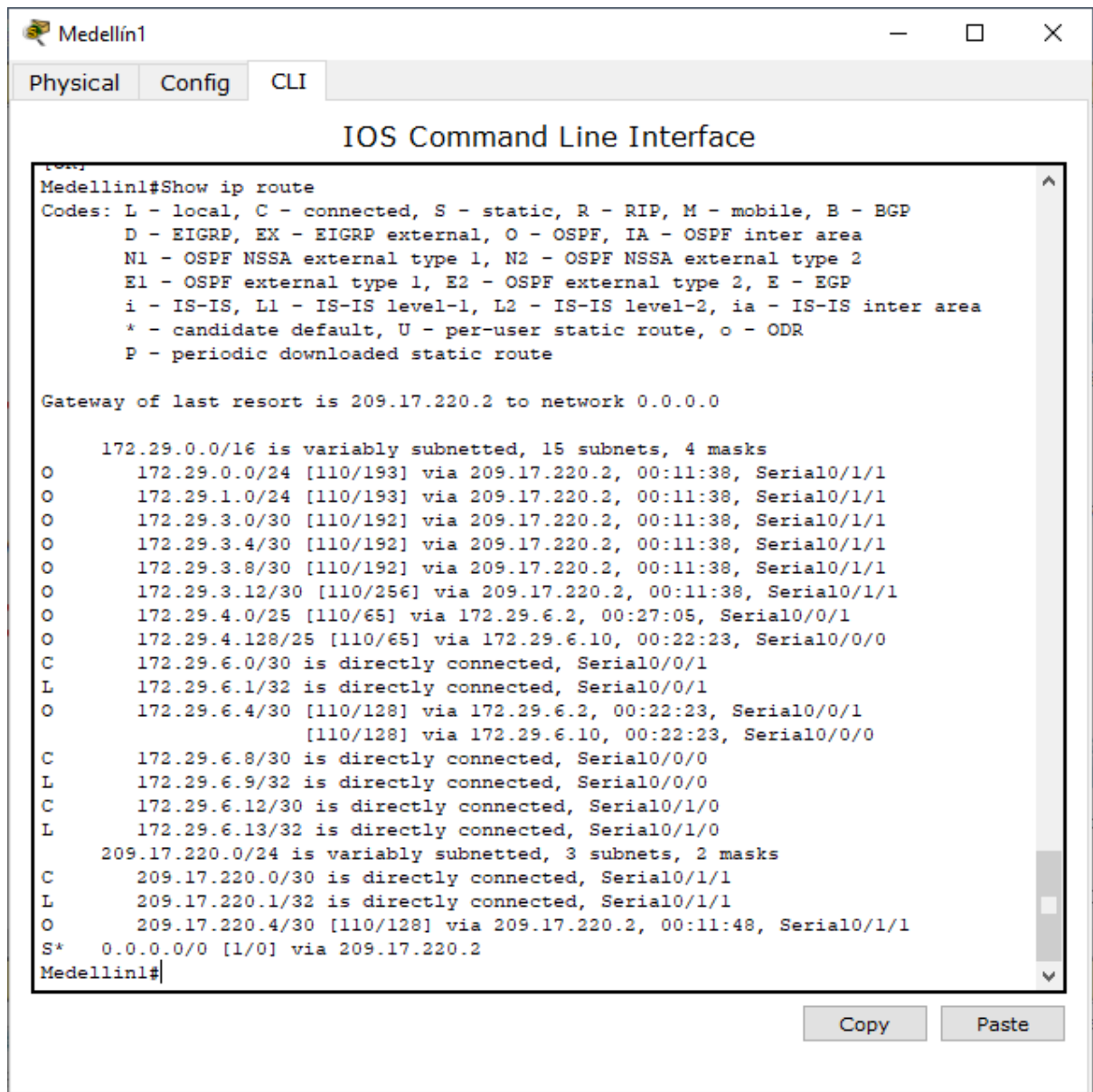
```
Bogota3#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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: Comando Show ip route en Medellín1



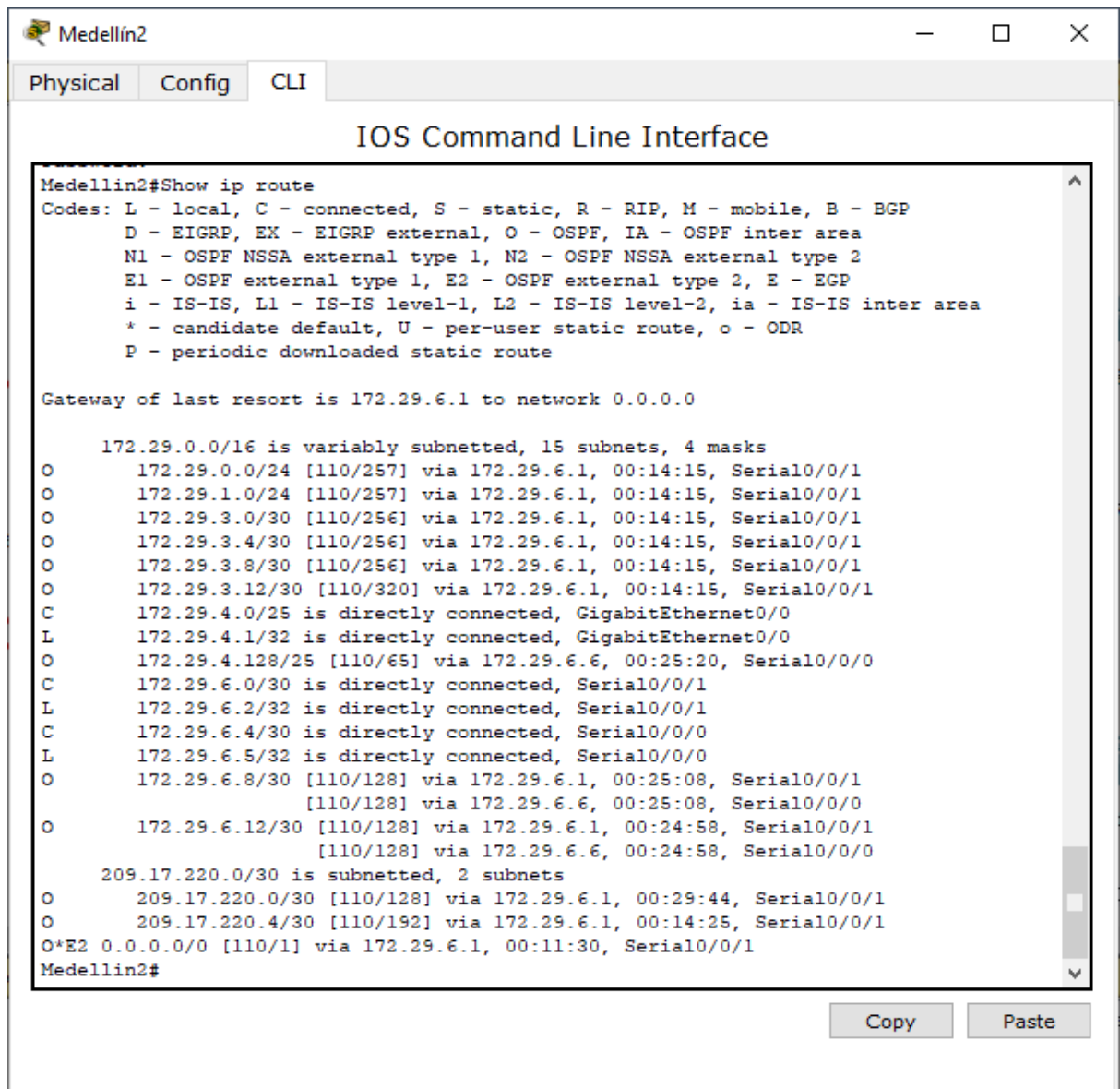
```
Medellin1#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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: Comando Show ip route en Medellín2



The screenshot shows a terminal window titled "Medellin2" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" displaying the output of the command "Medellin2#Show ip route". The output includes a legend for route codes, the gateway of last resort (172.29.6.1), and a list of routes with their respective metrics, protocols, and next-hop information. At the bottom right, there are "Copy" and "Paste" buttons.

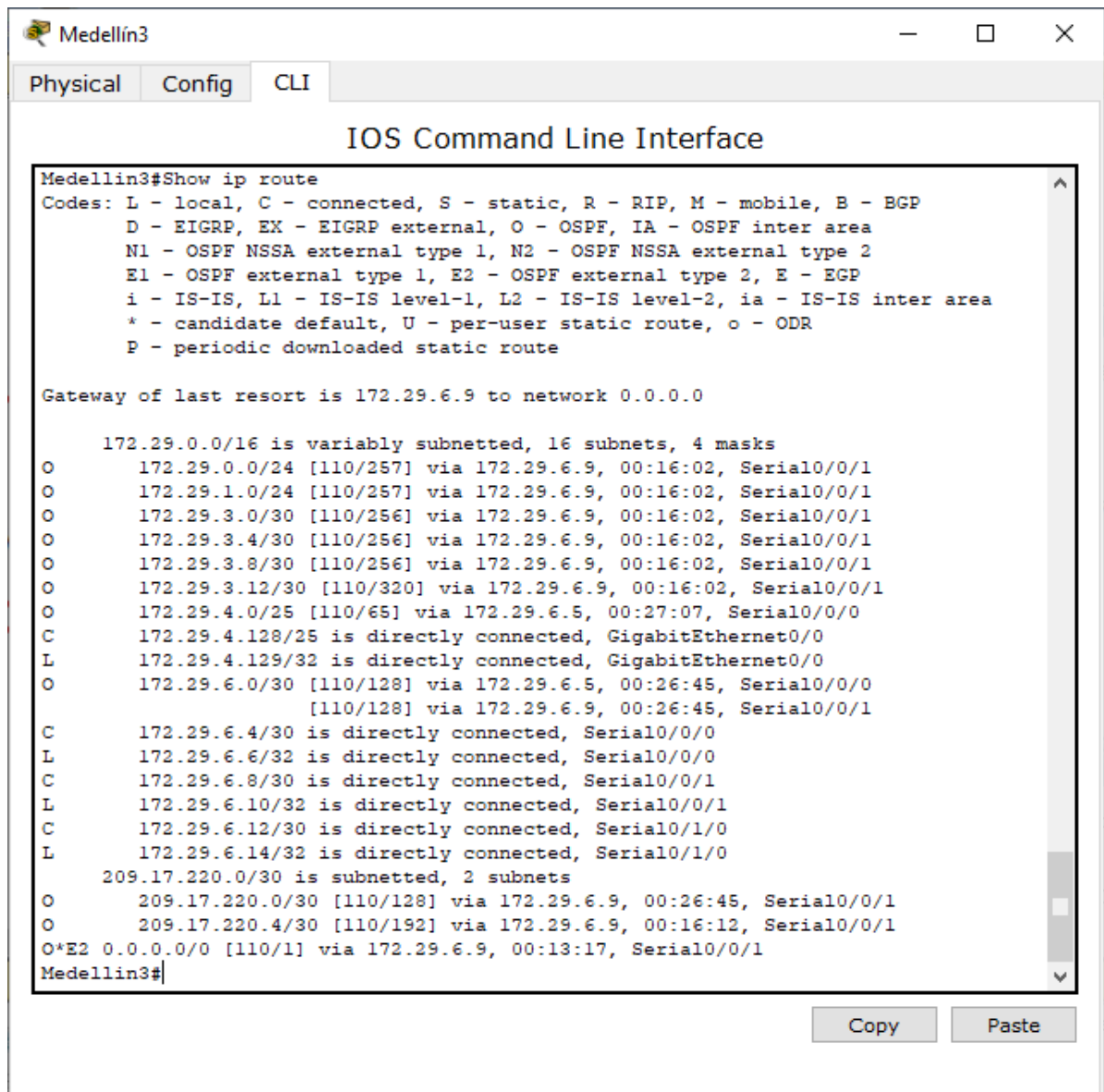
```
Medellin2#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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: Comando Show ip route en Medellín3



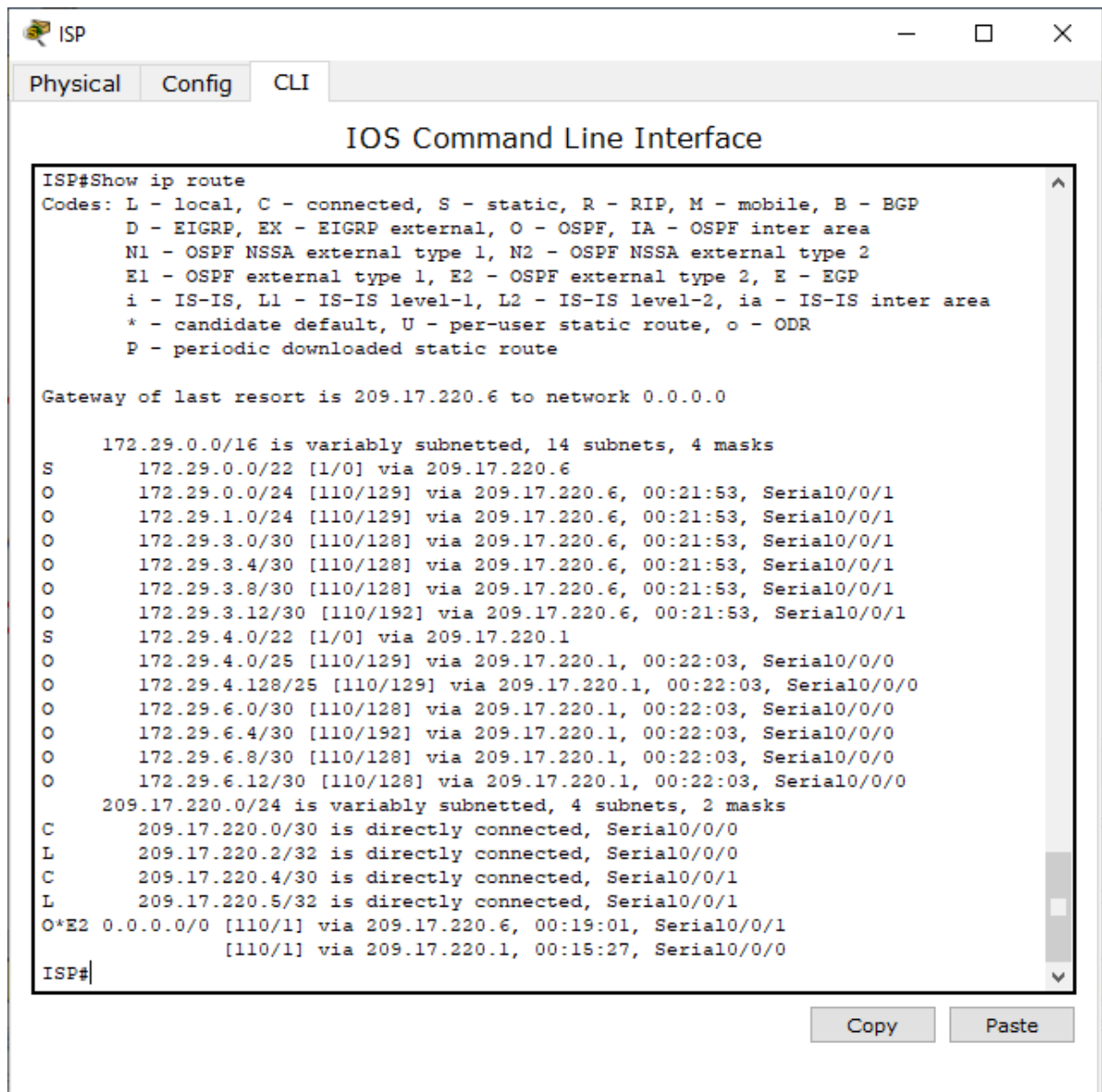
```
Medellin3#Show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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: 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.

Bogota1

```
Bogota1#conf t
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
```

Bogota2

```
Bogota2#conf t
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
```

Bogota3

```
Bogota3#conf t
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
```

Medellin1

```
Medellin1>en
Password:
Medellin1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#router ospf 1
Medellin1(config-router)#passive-interface s0/1/0
```

Medellin2

```
Medellin2#conf t
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
```

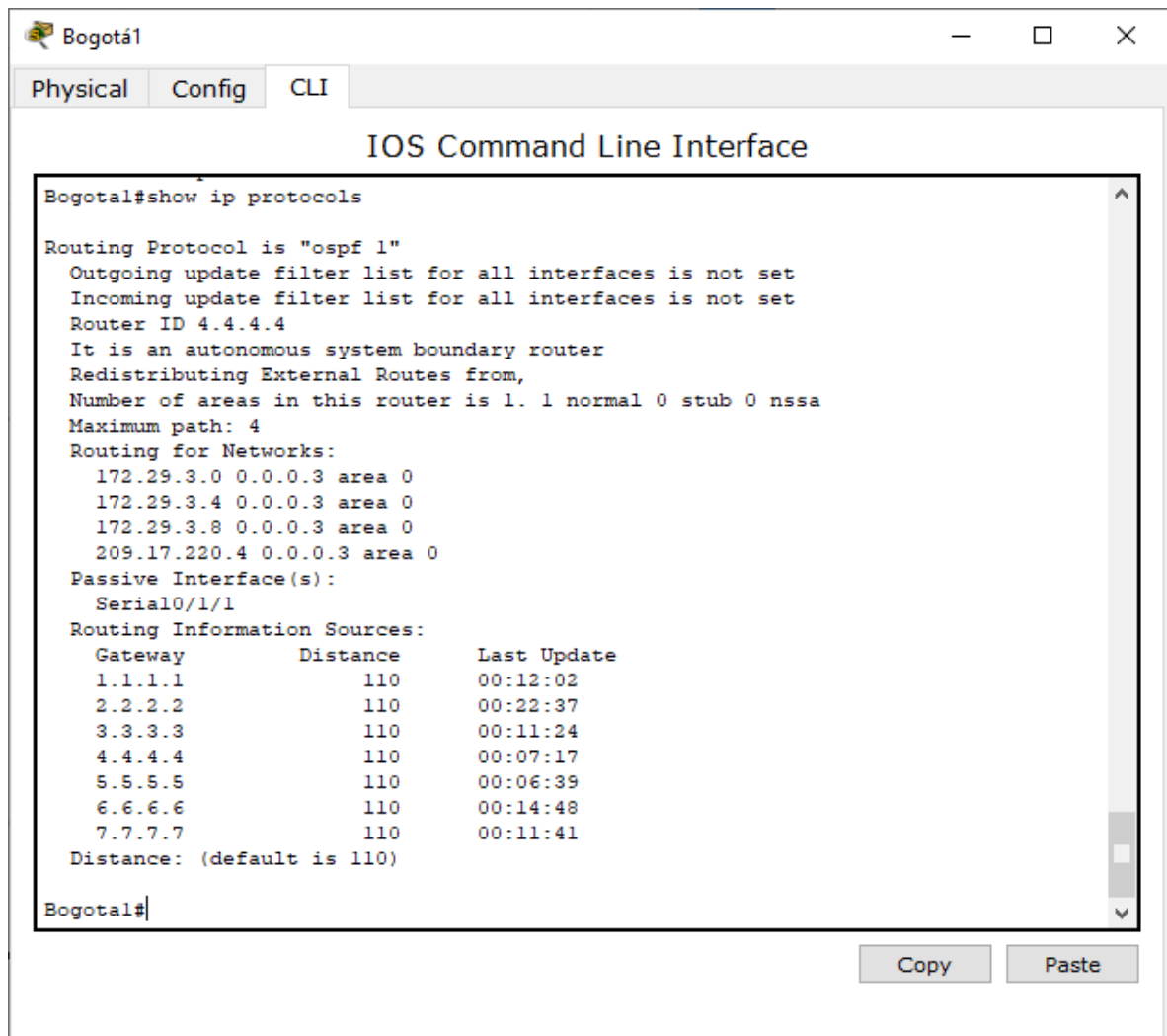
Medellin3

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

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: Show ip protocols en Bogota1



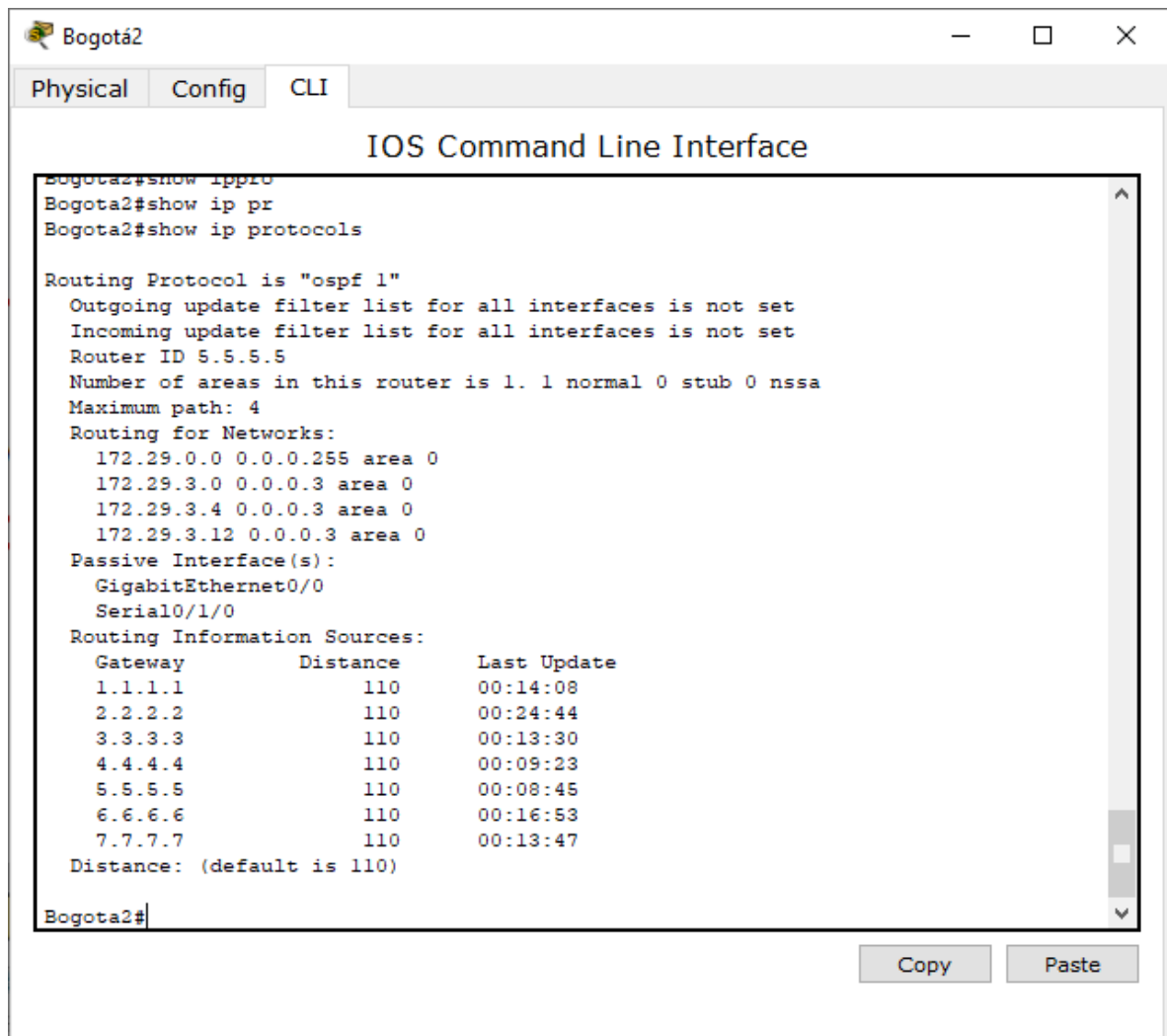
```
Bogota1#show ip protocols

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 4.4.4.4
  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:
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.8 0.0.0.3 area 0
    209.17.220.4 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:12:02
    2.2.2.2          110          00:22:37
    3.3.3.3          110          00:11:24
    4.4.4.4          110          00:07:17
    5.5.5.5          110          00:06:39
    6.6.6.6          110          00:14:48
    7.7.7.7          110          00:11:41
  Distance: (default is 110)

Bogota1#
```

Fuente: Autor.

Figura 23: Show ip protocols en Bogota2



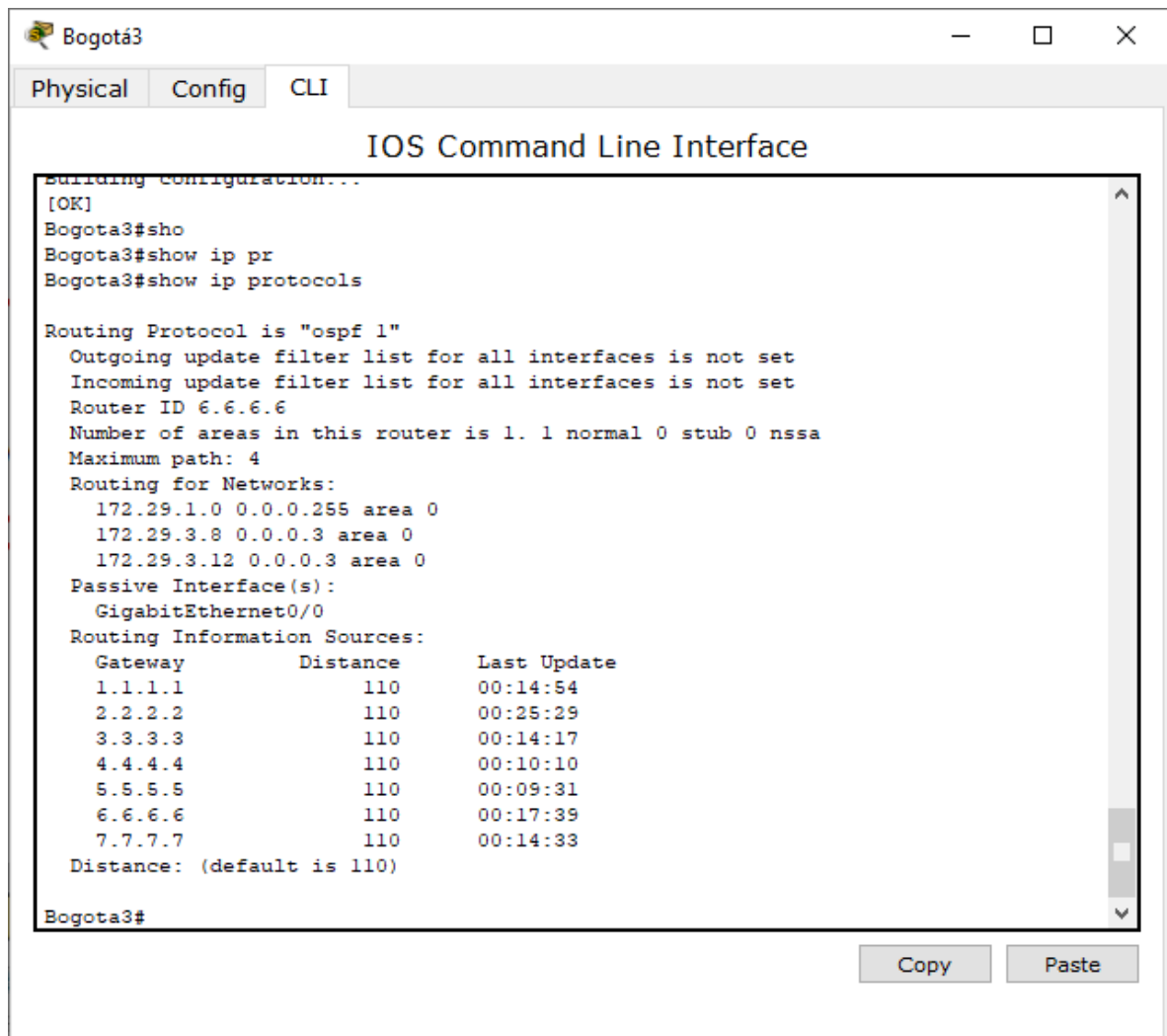
The screenshot shows a terminal window titled "Bogotá2" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" displaying the output of the command "show ip protocols". The output shows that OSPF is running on the router with a single area (area 0) and a router ID of 5.5.5.5. It lists several networks in area 0 and identifies passive interfaces. A table of routing information sources is also displayed, showing gateways, distances, and last update times.

```
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: Show ip protocols en Bogota3



The screenshot shows a terminal window titled "Bogotá3" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" displaying the output of the "show ip protocols" command. The output shows that OSPF is configured with Router ID 6.6.6.6 and three areas: 0.0.0.255, 0.0.0.3, and 0.0.0.3. It also lists routing information sources with their respective gateways, distances, and last update times.

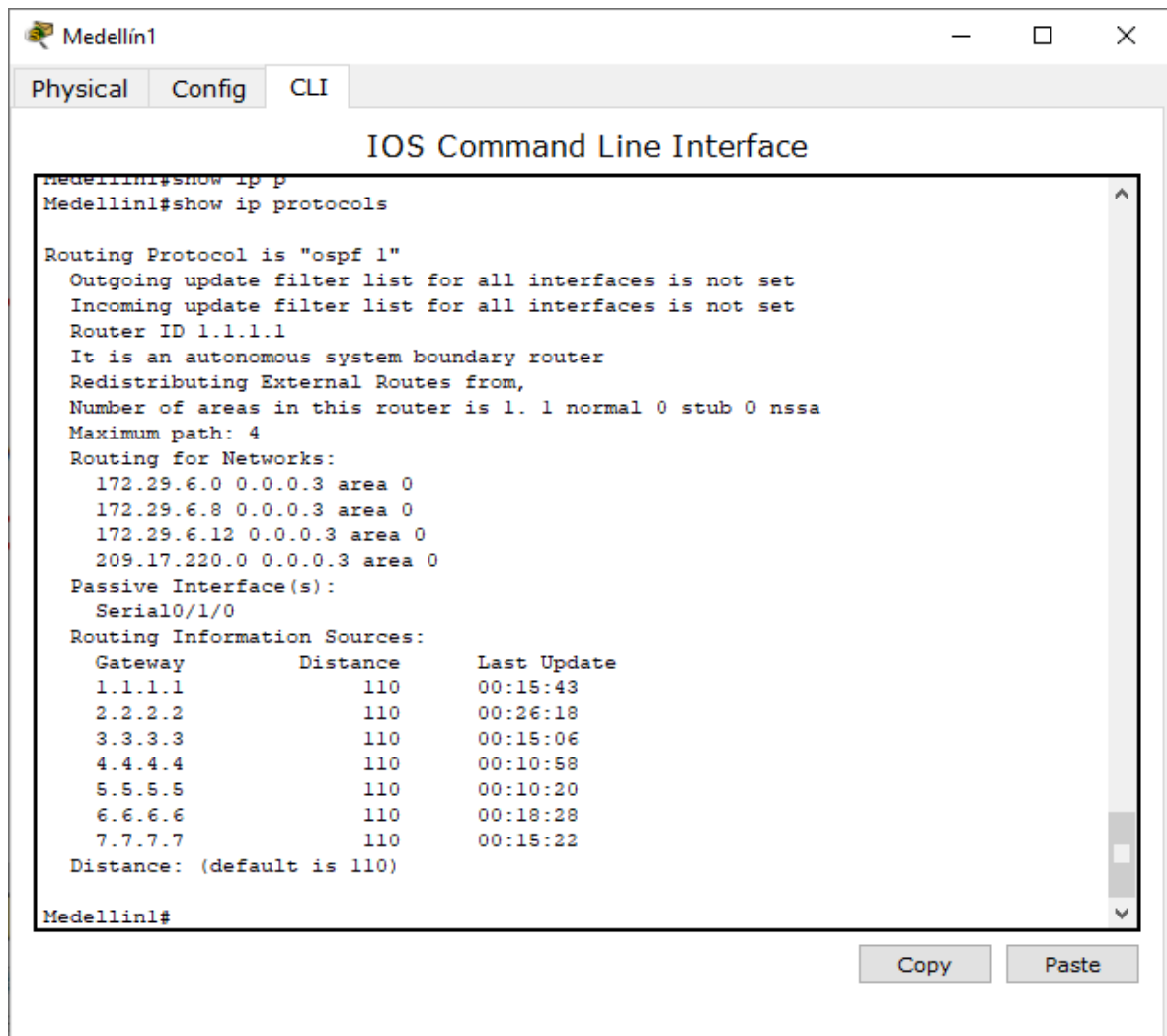
```
Building Configuration...
[OK]
Bogota3#sho
Bogota3#show ip pr
Bogota3#show ip protocols

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: Show ip protocols en Medellín1



The screenshot shows a window titled "Medellin1" with tabs for "Physical", "Config", and "CLI". The main area is labeled "IOS Command Line Interface" and displays the output of the command "show ip protocols". The output includes details about the OSPF configuration, such as the Router ID (1.1.1.1), the number of areas (1 normal, 0 stub, 0 nssa), and a list of routing information sources with their respective gateways, distances, and last update times.

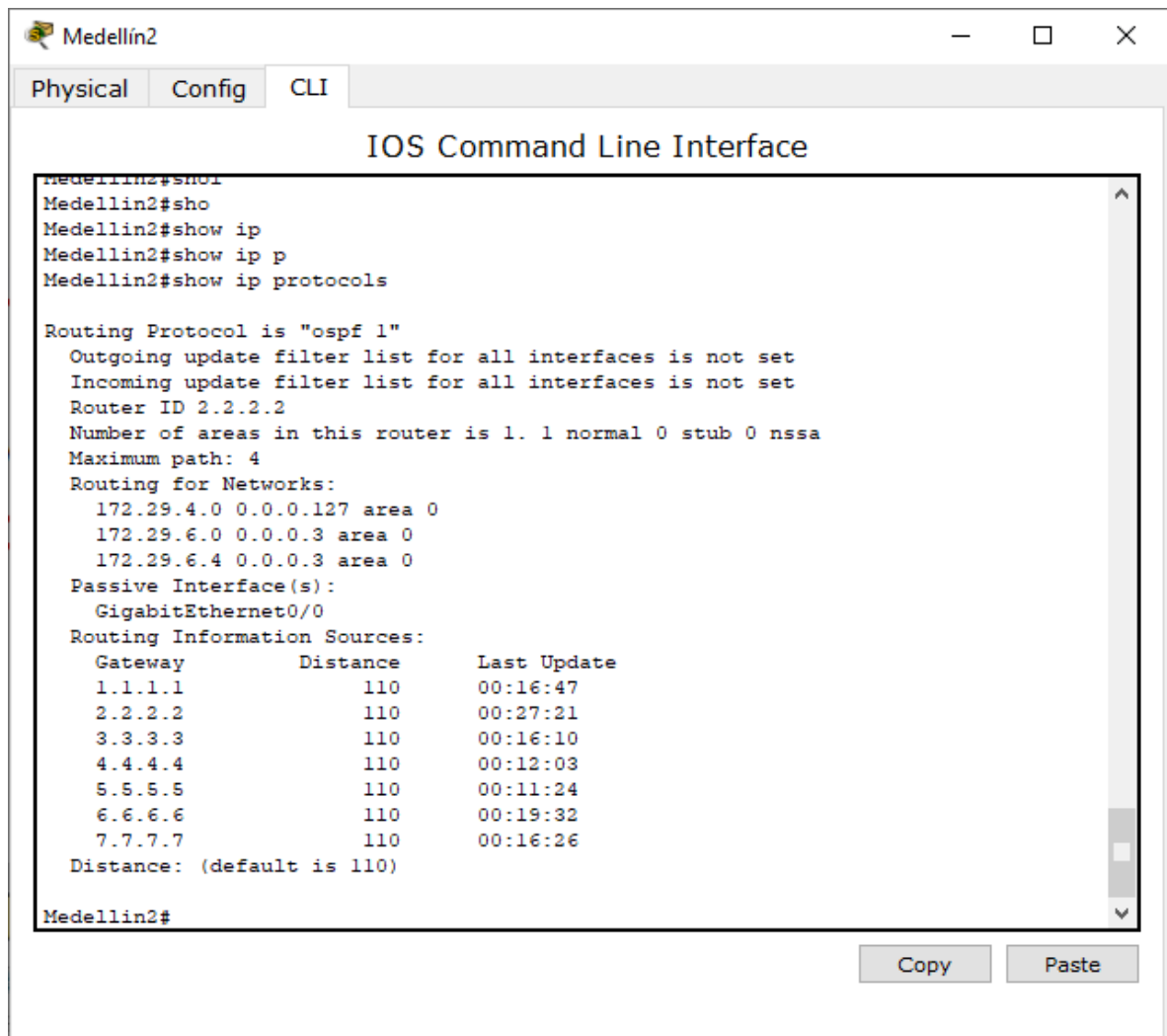
```
Medellin1#show ip p
Medellin1#show ip protocols

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: Show ip protocols en Medellín2



```
Medellin2#sho
Medellin2#sho
Medellin2#show ip
Medellin2#show ip p
Medellin2#show ip protocols

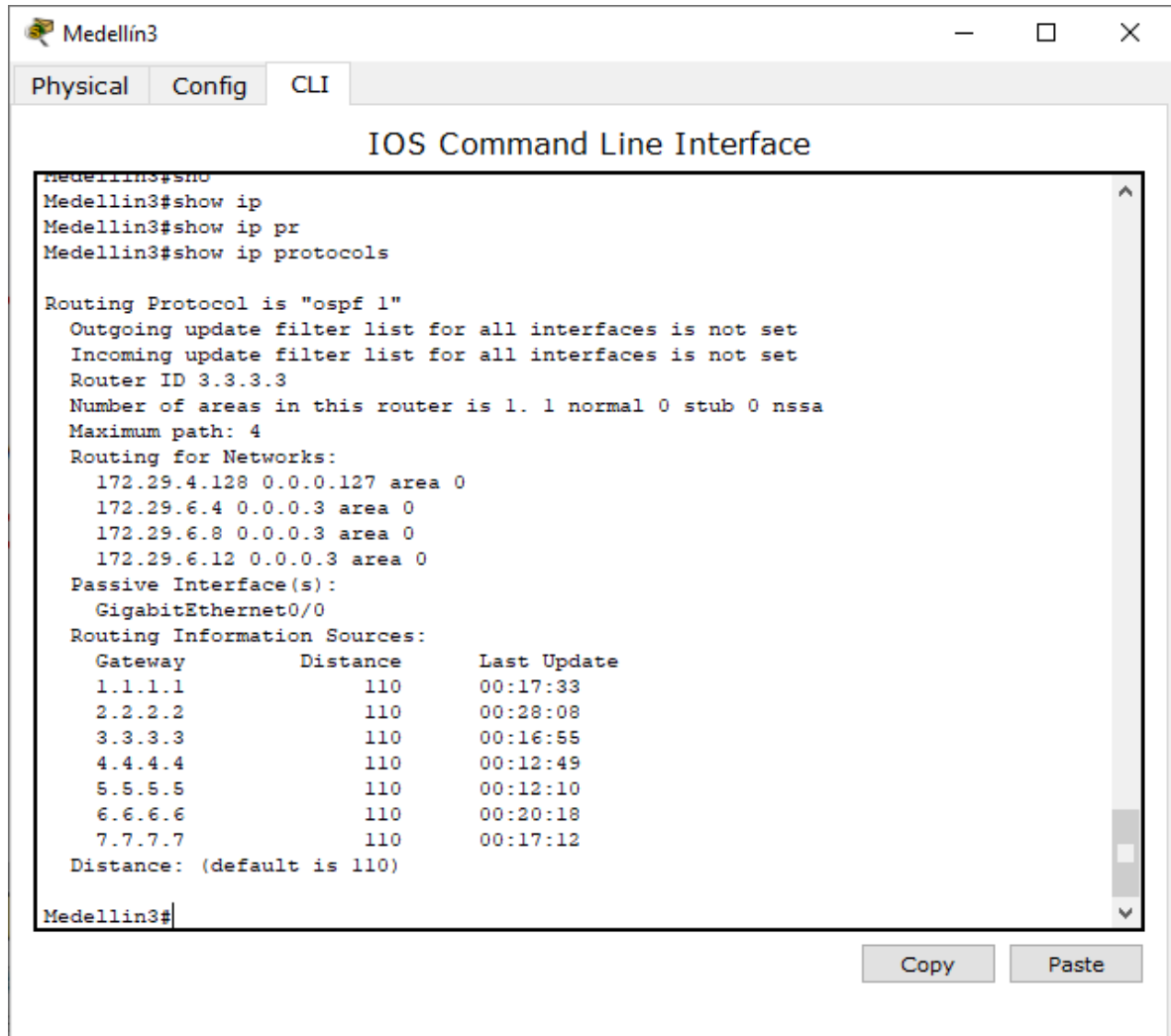
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.0 0.0.0.127 area 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#
```

Copy Paste

Fuente: Autor.

Figura 27: Show ip protocols en Medellín3



The screenshot shows a terminal window titled "Medellin3" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" where the following commands and output are displayed:

```
Medellin3#sho
Medellin3#show ip
Medellin3#show ip pr
Medellin3#show ip protocols

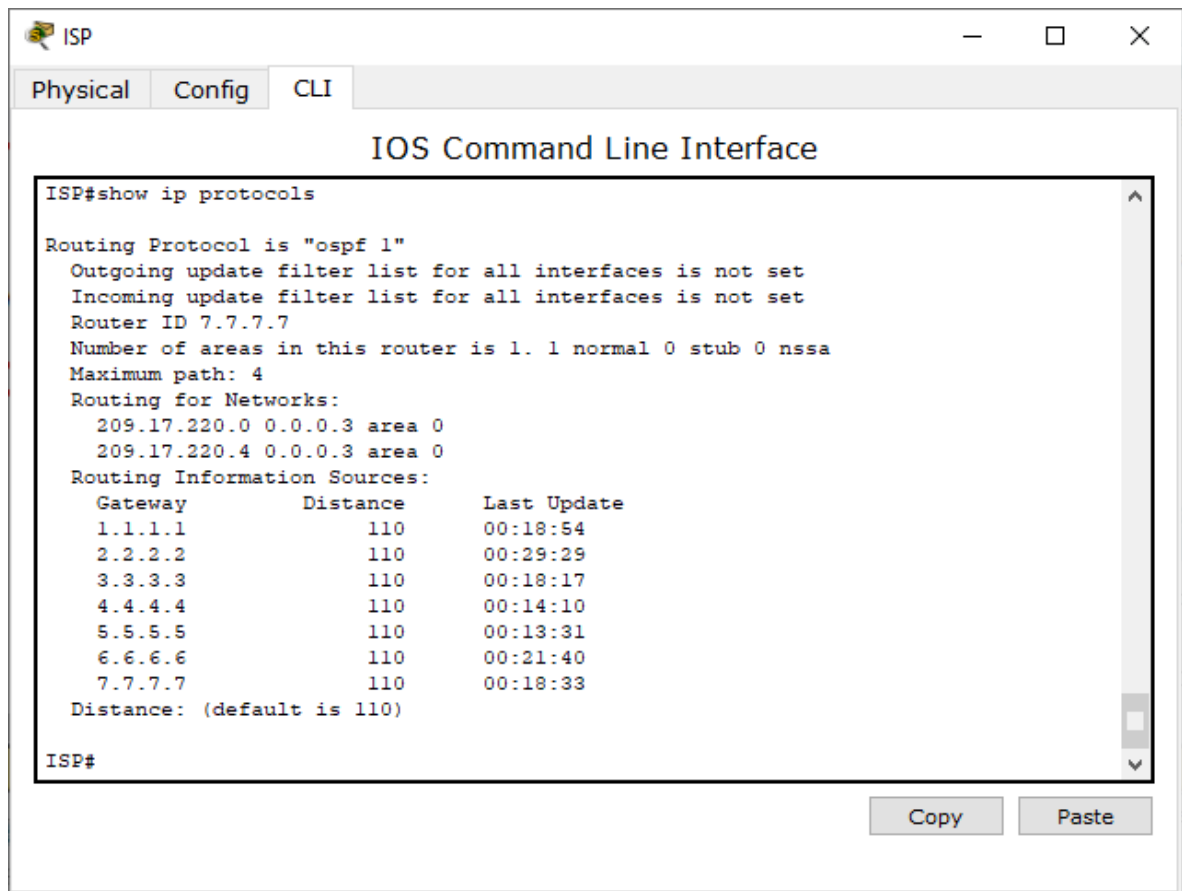
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.128 0.0.0.127 area 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#
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

Fuente: Autor.

Figura 28: 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 numeral a se realizaron las respectivas consultas con el 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.

A continuación, desarrollamos el punto **a y b de parte 5**.

Bogota1

```
Bogota1#conf t
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 shu
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
```

Medellin1

```
Medellin1#conf t
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 shu
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
```

ISP

```
ISP#conf t
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 shu
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, como 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, como diferente puerto.

A continuación, muestro el desarrollo Parte 6.

Bogota1

```

Bogota1#conf t
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

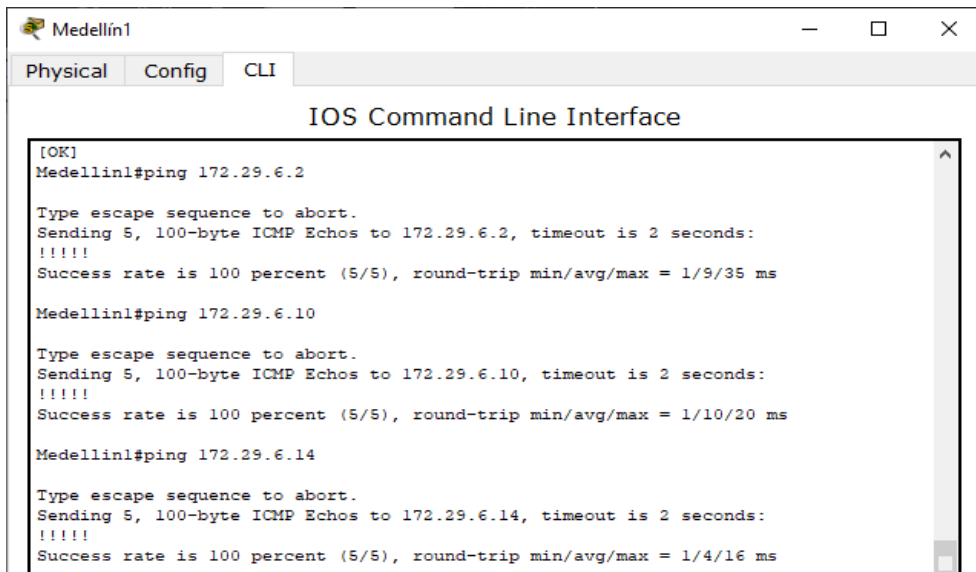
```

```
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
```

Medellin1

```
Medellin1#conf t
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: Verificamos mediante comando ping de Medellin1 a Medellin2 y Medellin3



```
[OK]
Medellin1#ping 172.29.6.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/35 ms

Medellin1#ping 172.29.6.10

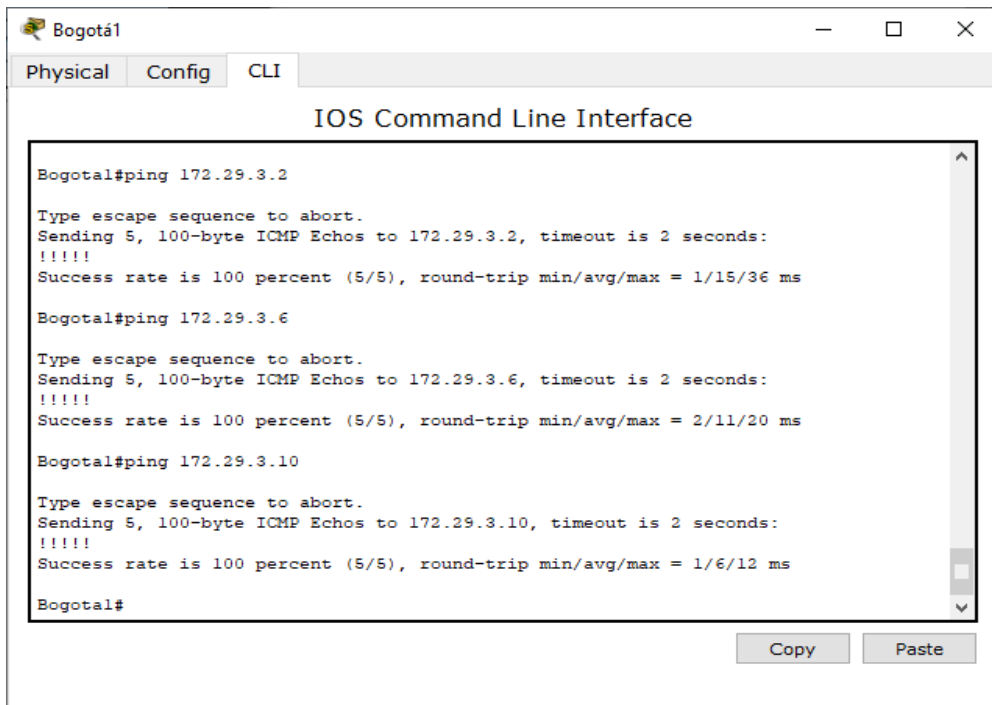
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.10, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/20 ms

Medellin1#ping 172.29.6.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.14, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
```

Fuente: Autor.

Figura 30: Verificamos mediante comando ping de Bogota1 a Bogota2 y Bogota3



```
Bogotá1#ping 172.29.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/36 ms

Bogotá1#ping 172.29.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/20 ms

Bogotá1#ping 172.29.3.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.10, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/12 ms

Bogotá1#
```

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.

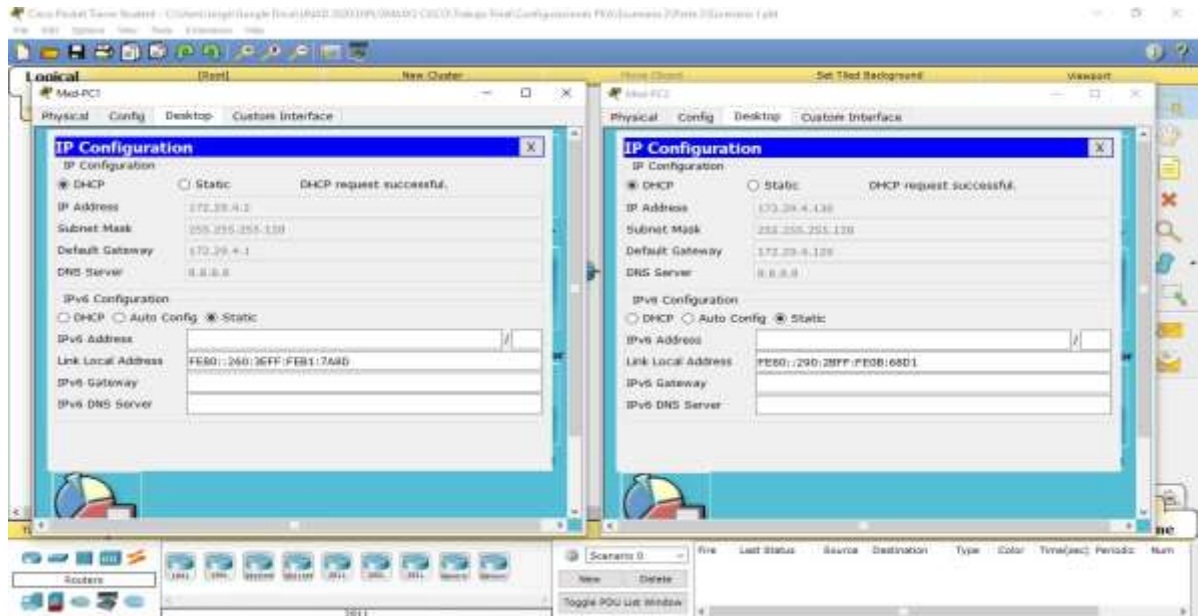
Medellin2

```
Medellin2#conf t
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)#
```

Teniendo en cuenta que Medellín3 tiene una red LAN conectada pero esta no realizara las veces de servidor DHCP, tenemos que configurar “ip helper” que aus ves permitirá ser un router de tránsito para llegar al router con el rol de DHCP. En este caso usaremos el comando ip helper-address para atrapar los broadcasts y redireccionarlos hacia la IP del router de Medellín2, la dirección IP de la interfaz de salida Medellín2 será (s0/0/0 - 172.29.6.5):

```
Medellin3#conf t
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 Med-PC1 y Med-PC2



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.

Bogota2

```
Bogota2#conf t
```

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)#

```

Teniendo en cuenta que Bogota3 tiene una red LAN conectada, pero esta no realizara las veces de servidor DHCP, tenemos que configurar "ip helper" que aus ves permitirá ser un router de tránsito para llegar al router con el rol de DHCP. En este caso usaremos el comando ip helper-address para atrapar los broadcasts y redireccionarlos hacia la IP del router de Bogota, la dirección IP de la interfaz de salida Bogota2 sera (s0/0/1 - 172.29.3.13):

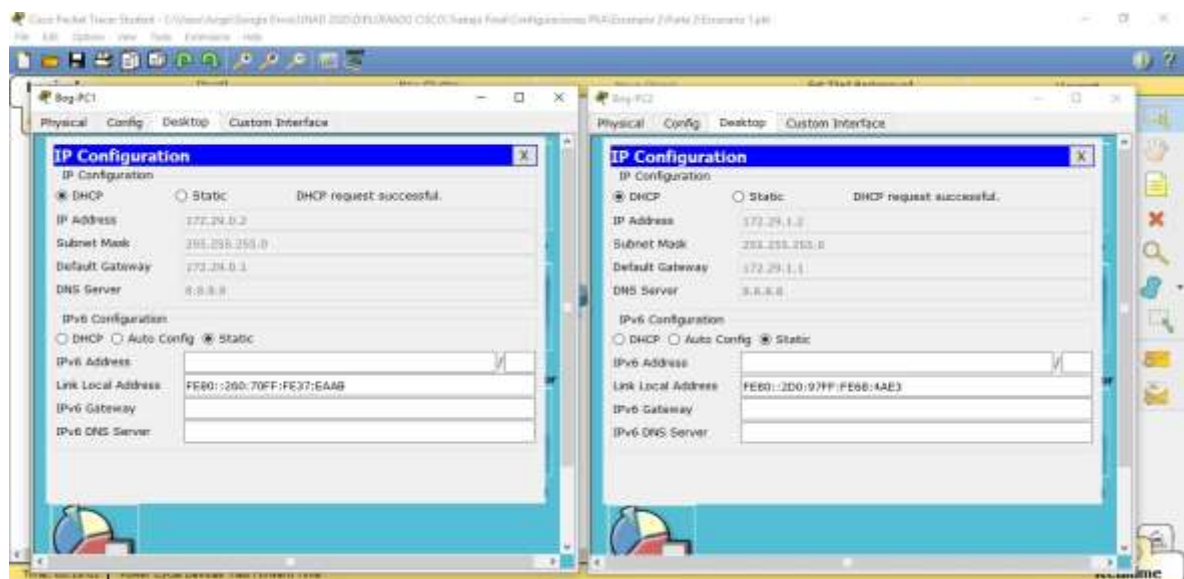
Bogota3

```

Bogota3#conf t
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

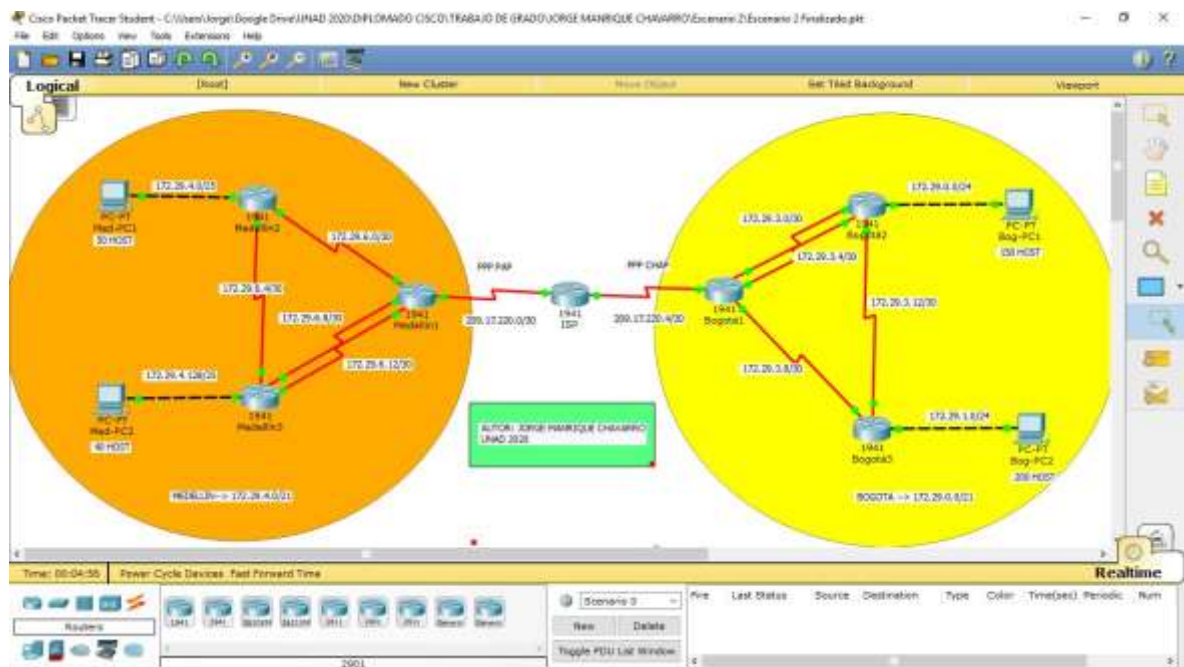
```

Figura 32: Configuración Bog-PC1 y Bog-PC2



Fuente: Autor.

Figura 33: Topología del escenario 2 finalizada en Packet Tracer



Fuente: Autor.

CONCLUSIONES

Se diseñaron e implementaron las topologías propuestas para cada escenario, para lo cual se agregaron los diferentes dispositivos en la herramienta de simulación packet tracer y posteriormente se procedió con el cableado correspondiente de acuerdo con lo solicitado.

Se realizó el desarrollo de los dos escenarios propuestos en la prueba de habilidades prácticas CCNA mediante la herramienta de packet tracer, aplicando los conocimientos adquiridos a lo largo del diplomado.

Se implementaron configuraciones básicas y avanzadas para cada dispositivo teniendo en cuenta los escenarios propuestos.

Se implementó el protocolo RIP el cual sirve para poder enrutar direcciones IPv4, este es un protocolo vector distancia el cual resume los límites en las redes principales con clase y se utiliza en redes pequeñas.

Se utilizó el protocolo OSPF el cual es utilizado en redes de mayor dimensión, teniendo en cuenta que ofrece una mayor escalabilidad en las redes y converge mejor que el protocolo RIP.

Se realizó la verificación de las redes y sus dispositivos, comprobando que el funcionamiento se realizara de forma correcta.

El desarrollo de la prueba de habilidades ha sido una herramienta de gran importancia, ya que nos permite conocer los retos que tendremos que afrontar y aplicar en futuros proyectos a nivel profesional y 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). 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). 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). 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). 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). 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). 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!AmlJYei-NT1IhgL9QChD1m9EuGqC>

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

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

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

ANEXOS

Anexo 1: Escenario 1 archivo PKA

URL: <https://bit.ly/2ZsXtF8>

Anexo 2: Escenario 2 archivo PKA

URL: <https://bit.ly/2M1SinH>