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

GUSTAVO ADOLFO MIRANDA PINZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA (ECBTI)

INGENIERIA DE SISTEMAS

BARRANCABERMEJA

2020

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

GUSTAVO ADOLFO MIRANDA PINZÓN

Diplomado de profundización CISCO (Diseño e implementación de soluciones integradas LAN/WAN)

Director/Tutor
Juan Carlos Vesga Ferreira

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA (ECBTI)

INGENIERIA DE SISTEMAS

BARRANCABERMEJA

2020

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

En el presente trabajo se encuentra el desarrollo de dos estudios de caso bajo el uso de tecnología Cisco, con el cual se afianzarán los conocimientos adquiridos durante el desarrollo del Diplomado de Profundización Cisco, el cual nos ayuda para desempeñar en nuestra profesión actualmente se están teniendo en cuenta los nuevos retos que debe asumir la comunidad en el mundo, estos escenarios, las redes informáticas y la conectividad son claves en la comunicación del planeta, entenderlas y apropiarnos de ellas son obligación como estudiantes de ingeniería de sistemas. Nos permite demostrar su importancia y el uso adecuado de las mismas por medio del presente se obtiene un soporte de ese conocimiento.

INTRODUCCIÓN

Una red representa la interconexión de un conjunto determinado de computadores, a través de dispositivos alámbricos o inalámbricos que, gracias a impulsos eléctricos, ondas electromagnéticas u otros medios físicos, pueden enviar y recibir información relevante en paquetes de datos, como también, compartir sus recursos y actuar como un conjunto organizado.

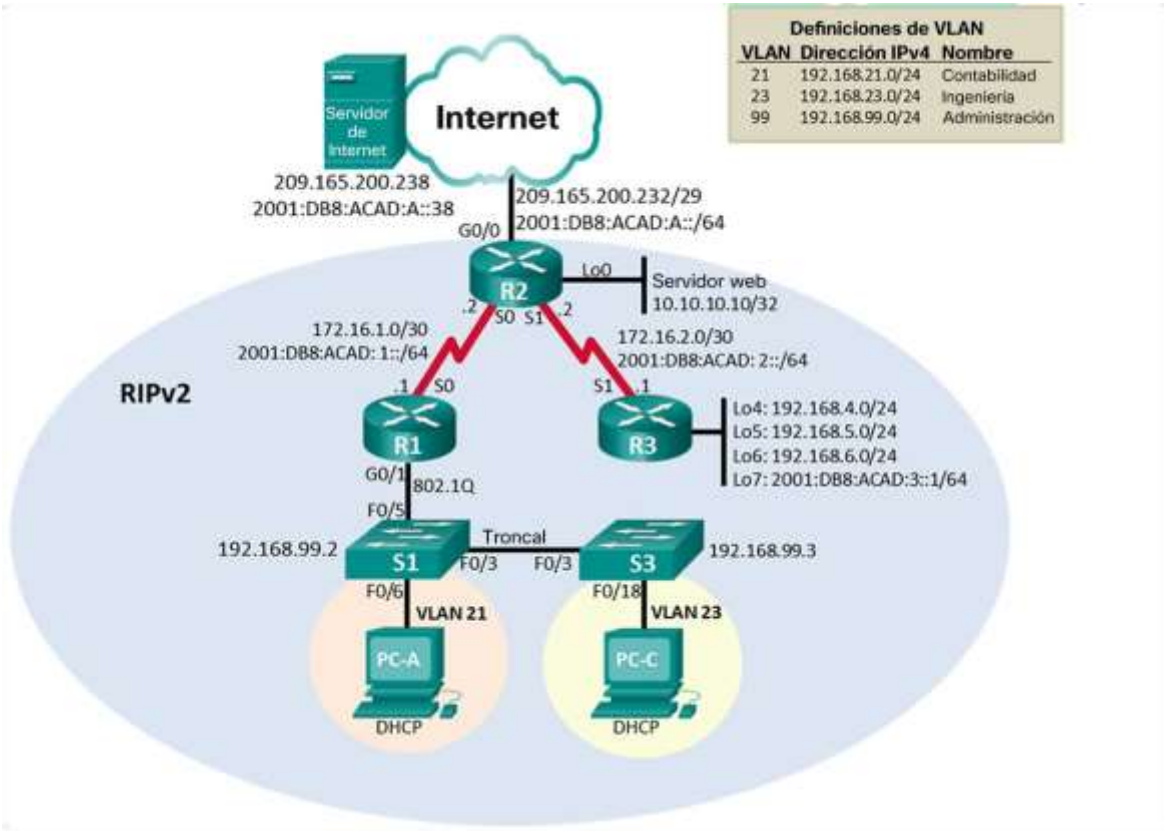
A continuación, se mostrará el desarrollo de dos escenarios de situaciones de la vida real mediante la herramienta Cisco Packet Tracer, la cual permitirá realizar la simulación de los casos propuestos con el fin de afianzar los conocimientos actuales sobre el manejo y configuración de dispositivos de red.

Asimismo, los temas que se involucran en el desarrollo de los escenarios son, Fundamentos de Networking, Direccionamiento IP, Configuración de sistemas de red soportados en VLANs y Enrutamiento en soluciones de red.

1 PRIMER ESCENARIO

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

Figura 1.Topología de red escenario 1



Fuente: Prueba de habilidades CCNA 2020, Cisco Academy

1.1 PARTE 1: INICIALIZAR DISPOSITIVOS

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 dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>en Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK] Erase of nvram: complete
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]y
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>en Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK] Erase of nvram: complete Switch#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]y
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]y
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash Switch#show flash Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Esto se verifica en los dos switch.

Fuente: Autor

1.2 PARTE 2: COFIGURAR LOS PARAMETROS BASICOS DE LOS DISPOSITIVOS

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):

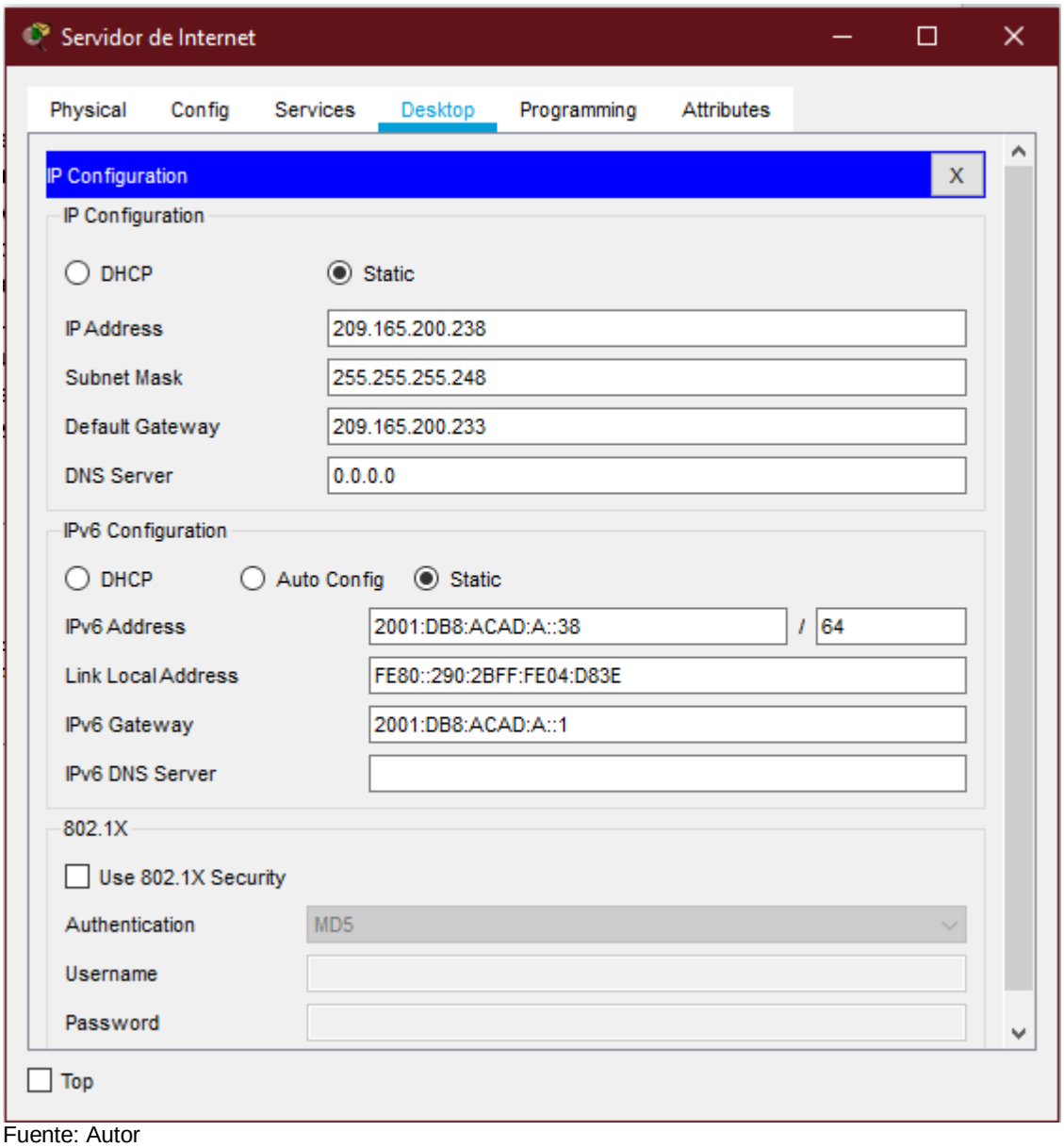
Tabla 2. Configuración Computadora Internet

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: Las direcciones se ajustaron teniendo en cuenta la topología asignada y de acuerdo con el Subneteo de las subredes IPv4 y IPv6.

Figura 2. Configuración IP Servidor de Internet



Fuente: Autor

1.2.2 Paso 2: configurar R1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No existe ningún servidor DNS
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Impide que las contraseñas aparezcan como texto no cifrado
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0
Códigos IOS utilizados	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname R1 R1(config)#enable secret class R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#service password-encryption

	R1(config)#banner motd #Se prohibe el acceso no autorizado# R1(config)#int s0/0/0 R1(config-if)#description Conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no sh R1(config-if)#exit R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#

Fuente: Autor

1.2.3 Paso 3: configurar R2.

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configuración R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de

	topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.
Códigos IOS utilizados	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname R2 R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#service password-encryption R2(config)#banner motd #Se prohibe el acceso no autorizado# R2(config)#int s0/0/0 R2(config-if)#description Conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no sh R2(config-if)#int s0/0/1 R2(config-if)#description Conexion a R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no sh R2(config-if)#int g0/0 R2(config-if)#description Conexion a Internet R2(config-if)#ip address 209.165.200.233

	255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no sh R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Servidor Web simulado R2(config-if)#exit R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Fuente: Autor

1.2.4 Paso 4: configurar R3.

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	Configure una ruta IPv4 predeterminada S0/0/1. Configure una ruta IPv6 predeterminada S0/0/1.
Códigos IOS utilizados	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname R3 R3(config)#enable secret class R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#service password-encryption R3(config)#banner motd #Se prohibe el acceso no autorizado# R3(config)#int s0/0/1 R3(config-if)#description Conexion a R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no sh R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Fuente: Autor

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	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Códigos IOS Utilizados	Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#hostname S1 S1(config)#enable secret class S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#service password-encryption S1(config)#banner motd %Se prohibe el acceso no autorizado%

Fuente: Autor

1.2.6 Paso 6: configurar S3.

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Configurar S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Códigos IOS utilizados	Switch>enable Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#hostname S3 S3(config)#enable secret class S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#service password-encryption S3(config)#banner motd %Se prohibe el acceso no autorizado%

Fuente: Autor

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. Conectividad entre los dispositivos de red.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.2	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

Fuente: Autor.

Figura 3. Ping de R1 a R2

```
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 = 4/4/6 ms
```

Fuente: Autor.

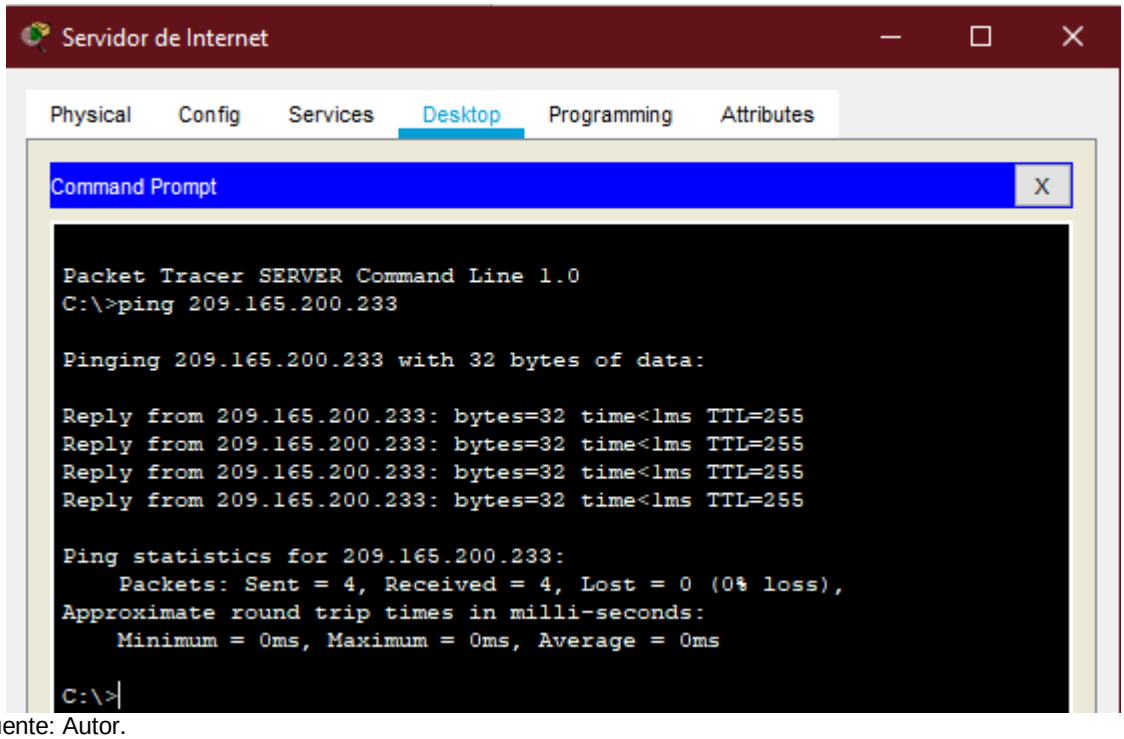
Figura 4. Ping de R2 a R3

```
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 = 2/3/5 ms
```

Fuente: Autor.

Figura 5. Ping del servidor de Internet al Gateway



Fuente: Autor.

1.3 PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

1.3.1 Paso 1: configurar S1.

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configuración S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	
Códigos IOS utilizados	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)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit S1(config)#int vlan 99 S1(config-if)# S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no sh S1(config-if)#exit S1(config)#ip default-gateway 192.168.99.1 S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente: Autor.

1.3.2 Paso 2: configurar S3.

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configurar S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	
Códigos IOS Utilizados	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)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit S3(config)#int vlan 99 S3(config-if)# S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no sh S3(config-if)#exit S3(config)#ip default-gateway 192.168.99.1

	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Fuente: Autor.

1.3.3 Paso 3: configurar R1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configurar 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
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
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
Activar la interfaz G0/1	
Códigos IOS Utilizados	R1>en Password: R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1.21 R1(config-subif)#description Contabilidad LAN R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#int g0/1.23 R1(config-subif)#description Ingenieria LAN

	R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#int g0/1.99 R1(config-subif)#description Administracion LAN R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#int g0/1 R1(config-if)#no sh

Fuente: Autor.

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. Conectividad entre los dispositivos de red

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

Fuente: Autor.

Figura 6. Ping de S1 a R1-VLAN99

```
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 = 0/0/4 ms
```

Fuente: Autor.

Figura 7. Ping de S1 a R1-VLAN21

```
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 = 0/0/1 ms
```

Fuente: Autor.

Figura 8. Ping a S3 a R1-VLAN99

```
S3#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 = 0/0/0 ms
```

Fuente: Autor.

Figura 9. Ping de S3 a R1-VLAN23

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: Autor.

1.4 PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINAMICO RIPV2

1.4.1 Paso 1: configurar RIPv2 en el R1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Configuración R1-RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	

Desactive la sumarización automática	
Códigos IOS Utilizados	R1>en Password: R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router rip R1(config-router)#version 2 R1(config-router)#do show ip route connected 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 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)#no auto-summary

Fuente: Autor.

Figura 10. Redes directamente conectadas en R1

```
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
```

Fuente: Autor.

1.4.2 Paso 2: configurar RIPv2 en el R2.

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configuración R2-RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Códigos IOS utilizados	R2#conf t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#router rip R2(config-router)#version 2 R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#passive-interface loopback 0 R2(config-router)#no auto-summary

Fuente: Autor.

Figura 11. Redes directamente conectadas a R2

```
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
```

Fuente: Autor.

1.4.3 Paso 3: configurar RIPv3 en el R3.

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configuración R3-RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	
Códigos IOS utilizados	R3>en Password: R3#conf t Enter configuration commands, one per line. End with CNTL/Z. R3(config)#router rip R3(config-router)#version 2 R3(config-router)#do show ip route connected R3(config-router)#network 172.16.2.0

	R3(config-router)#network 172.16.4.0 R3(config-router)#network 172.16.5.0 R3(config-router)#network 172.16.6.0 R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#no auto-summary

Fuente: Autor.

Figura 12. Redes directamente conectadas a R3

```
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
```

Fuente: Autor.

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. Información 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?	Show ip protocols R1#show ip protocols Routing Protocol is "rip" Sending updates every 30 seconds, next due in 1 seconds Invalid after 180 seconds, hold down 180, flushed after 240 Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Redistributing: rip Default version control: send version 2, receive 2 Interface Send Recv Triggered RIP Key-chain Serial0/0/0 2 2 Automatic network

	summarization is not in effect Maximum path: 4 Routing for Networks: 172.16.0.0 192.168.21.0 192.168.23.0 192.168.99.0 Passive Interface(s): GigabitEthernet0/1.21 GigabitEthernet0/1.23 GigabitEthernet0/1.99 Routing Information Sources: Gateway Distance Last Update 172.16.1.2 120 00:00:04 Distance: (default is 120)
¿Qué comando muestra solo las rutas RIP?	Show ip route rip R1#show ip route rip 10.0.0.0/32 is subnetted, 1 subnets R 10.10.10.10 [120/1] via 172.16.1.2, 00:00:08, Serial0/0/0 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks R 172.16.2.0/30 [120/1] via 172.16.1.2, 00:00:08, Serial0/0/0 192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run router rip version 2 passive-interface GigabitEthernet0/1.21 passive-interface GigabitEthernet0/1.23 passive-interface GigabitEthernet0/1.99 network 172.16.0.0 network 192.168.21.0 network 192.168.23.0 network 192.168.99.0 no auto-summary

Fuente: Autor.

1.5 PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

1.5.1 Paso 1: configurar el R1 como servidor de DHCP para las VLAN 21 Y 23.

Tabla 17. Configuración de R1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Códigos IOS Utilizados	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 R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com

Fuente: Autor

1.5.2 Paso 2: configurar la NAT estática y dinámica en el R2.

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configuración de la NAT estática y dinámica en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236
Definir la traducción de NAT dinámica	
Códigos IOS utilizados	R2>en Password: R2#CONF T Enter configuration commands, one per line. End with CNTL/Z. R2(config)#username webuser privilege 15 secret cisco12345 R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 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 R2(config)#access-list 1 permit

	192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248 R2(config)#ip nat inside source list 1 pool INTERNET

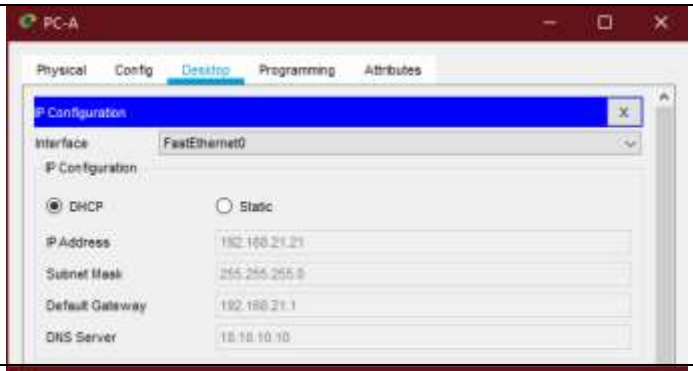
Fuente: Autor.

Nota: Los comandos ip http server, ip http authentication local y ip http secure-server no son compatibles con Packet Tracer.

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. Verificación del protocolo DHCP y la NAT estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-A pueda	C:\>ping 192.168.23.21

hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Pinging 192.168.23.21 with 32 bytes of data: Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time=1ms TTL=127 Reply from 192.168.23.21: bytes=32 time=1ms TTL=127 Ping statistics for 192.168.23.21: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	

Fuente: Autor.

Nota: La conexión al servidor web no fue posible porque el comando ip http server no es compatible con los routers para activar el servicio.

1.6 PARTE 6: CONFIGURAR NTP

Tabla 20. Configurar NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**10 de mayo de 2020, 12:00 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	
Códigos IOS utilizados	R2>en Password: R2#clock set 00:00:00 10 May 2020 R2#conf t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ntp master 5 R2(config)#end R1>en Password: R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ntp server 172.16.1.2 R1(config)#ntp update-calendar R1(config)#exit

	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 1 16 7 4.00 858087603291.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Fuente: Autor.

1.7 PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

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**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	
Códigos IOS Utilizados	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 R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#transport input telnet R2(config-line)#exit R2(config)#exit R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado User Access Verification Password: R2>exit [Connection to 172.16.1.2 closed

	by foreign host] R1# R3>en Password: R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host R3#

Fuente: Autor.

Figura 13. Acceso a R2 desde R1

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado


User Access Verification

Password:
R2>exit

[Connection to 172.16.1.2 closed by foreign host]
R1#
```

Fuente: Autor.

Figura 14. Acceso a R2 desde R3

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

Fuente: Autor.

1.7.2 Paso 2: introducir el comando CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 22. Comandos CLI

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso	R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255

desde la última vez que se restableció	Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (8 match(es))
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters ^ % Invalid input detected at '^' marker. No compatible con packet tracer.
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface R2>en Password: R2#show ip interface GigabitEthernet0/0 is up, line protocol is up (connected) Internet address is 209.165.200.233/29 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is disabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP Fast switching turbo vector IP multicast fast switching is disabled IP multicast distributed fast switching is disabled Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Probe proxy name replies are disabled Policy routing is disabled Network address translation is disabled BGP Policy Mapping is disabled Input features: MCI Check

	WCCP Redirect outbound is disabled WCCP Redirect inbound is disabled WCCP Redirect exclude is disabled GigabitEthernet0/1 is administratively down, line protocol is down (disabled) Internet protocol processing disabled Serial0/0/0 is up, line protocol is up (connected) Internet address is 172.16.1.2/30 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is disabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP Fast switching turbo vector IP multicast fast switching is disabled IP multicast distributed fast switching is disabled Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Probe proxy name replies are disabled Policy routing is disabled Network address translation is disabled WCCP Redirect outbound is disabled WCCP Redirect exclude is disabled BGP Policy Mapping is disabled Serial0/0/1 is up, line protocol is up (connected) Internet address is 172.16.2.1/30 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 Helper address is not set

	Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is disabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP Fast switching turbo vector IP multicast fast switching is disabled IP multicast distributed fast switching is disabled Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Probe proxy name replies are disabled Policy routing is disabled Network address translation is disabled WCCP Redirect outbound is disabled WCCP Redirect exclude is disabled BGP Policy Mapping is disabled Loopback0 is up, line protocol is up (connected) Internet address is 10.10.10.10/32 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1514bytes Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is disabled IP fast switching on the same interface is disabled IP Flow switching is disabled

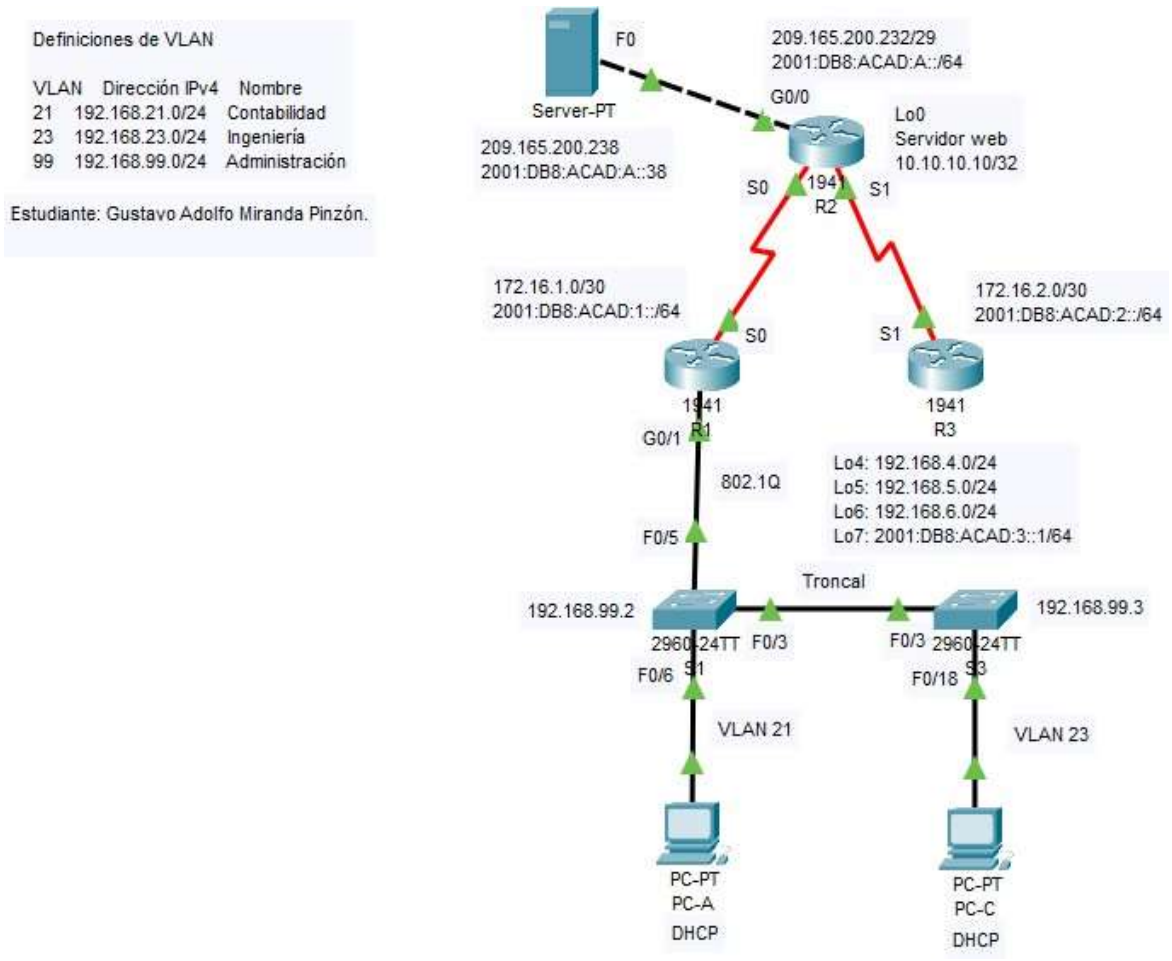
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
	
	Show ip nat translations
	`R2#show ip nat translations`
	`Pro Inside global Inside local Outside local Outside global`
	`icmp 209.165.200.233:2 192.168.21.21:2 209.165.200.238:2 209.165.200.238:2`
	`icmp 209.165.200.233:3 192.168.21.21:3 209.165.200.238:3 209.165.200.238:3`
	`icmp 209.165.200.233:4 192.168.21.21:4 209.165.200.238:4 209.165.200.238:4`
	`icmp 209.165.200.233:5 192.168.21.21:5 209.165.200.238:5 209.165.200.238:5`
	`icmp 209.165.200.233:6 192.168.21.21:6 209.165.200.238:6 209.165.200.238:6`
	`icmp 209.165.200.233:7 192.168.21.21:7 209.165.200.238:7 209.165.200.238:7`
	`icmp 209.165.200.233:8 192.168.21.21:8 209.165.200.238:8 209.165.200.238:8`
	`icmp 209.165.200.234:10 192.168.23.21:10 209.165.200.238:10 209.165.200.238:10`
	`icmp 209.165.200.234:11 192.168.23.21:11 209.165.200.238:11 209.165.200.238:11`
	`icmp 209.165.200.234:12 192.168.23.21:12 209.165.200.238:12 209.165.200.238:12`
	`icmp 209.165.200.234:13 192.168.23.21:13 209.165.200.238:13 209.165.200.238:13`
	`icmp 209.165.200.234:14 192.168.23.21:14 209.165.200.238:14 209.165.200.238:14`
	`icmp 209.165.200.234:15 192.168.23.21:15 209.165.200.238:15`
	`icmp 209.165.200.234:16 192.168.23.21:16 209.165.200.238:16 209.165.200.238:16`
	`--- 209.165.200.237 10.10.10.10 --- ---`

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *
	`R2#clear ip nat translation *`
	`R2#show ip nat translations`
	`Pro Inside global Inside local Outside local Outside global`
	`--- 209.165.200.237 10.10.10.10 --- ---`

Fuente: Autor.

1.8 PARTE 8: RED FINALIZADA EN CISCO PACKET TRACER

Figura 15. Red realizada en Cisco Packet Tracer

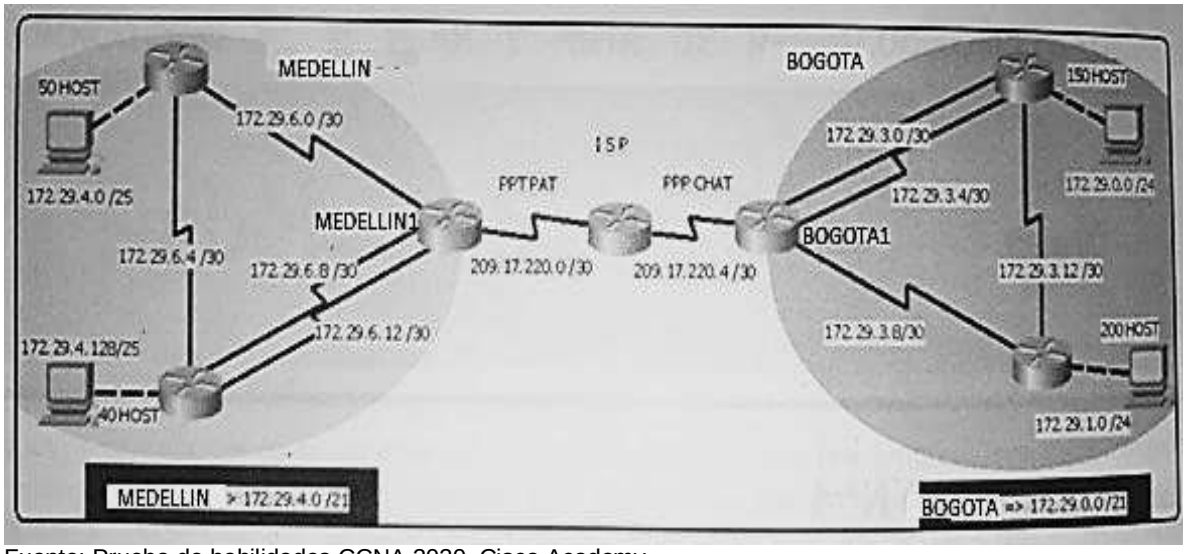


Fuente: Autor.

2 SEGUNDO ESCENARIO

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.

Figura 16. Topología de la red



Fuente: Prueba de habilidades CCNA 2020, Cisco Academy

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad. Debe configurar PPP en los enlaces hacia el ISP, con autenticación. Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

2.1 DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

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

Tabla 23. Configuración inicial de los elementos de red

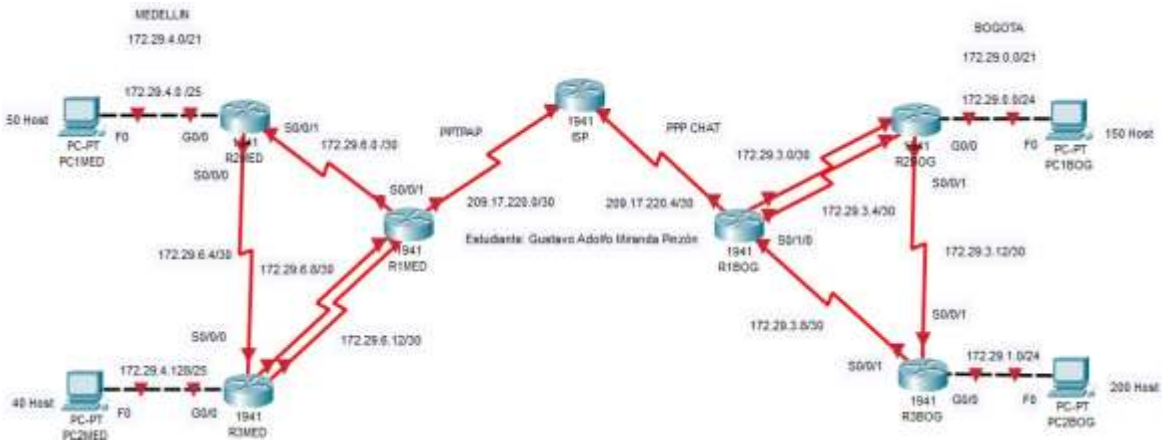
ELEMENTO	COMANDO IOS
ISP	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname ISP ISP(config)#enable secret class ISP(config)#line console 0 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#line vty 0 15 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#service password-encryption ISP(config)#banner motd %Se prohibe el acceso no autorizado% ISP(config)#
R1MED	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1MED R1MED(config)#enable secret class R1MED(config)#line console 0 R1MED(config-line)#password cisco R1MED(config-line)#login R1MED(config-line)#line vty 0 15 R1MED(config-line)#password cisco R1MED(config-line)#login R1MED(config-line)#service password-encryption R1MED(config)#banner motd %Se prohibe el acceso no autorizado% R1MED(config)#
R2MED	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R2MED R2MED(config)#enable secret class R2MED(config)#line console 0 R2MED(config-line)#password cisco

	R2MED(config-line)#login R2MED(config-line)#line vty 0 15 R2MED(config-line)#password cisco R2MED(config-line)#login R2MED(config-line)#service password-encryption R2MED(config)#banner motd %Se prohibe el acceso no autorizado% R2MED(config)#
R3MED	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R3MED R3MED(config)#enable secret class R3MED(config)#line console 0 R3MED(config-line)#password cisco R3MED(config-line)#login R3MED(config-line)#line vty 0 15 R3MED(config-line)#password cisco R3MED(config-line)#login R3MED(config-line)#service password-encryption R3MED(config)#banner motd %Se prohibe el acceso no autorizado% R3MED(config)#
R1BOG	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1BOG R1BOG(config)#enable secret class R1BOG(config)#line console 0 R1BOG(config-line)#password cisco R1BOG(config-line)#login R1BOG(config-line)#line vty 0 15 R1BOG(config-line)#password cisco R1BOG(config-line)#login R1BOG(config-line)#service password-encryption R1BOG(config)#banner motd %Se prohibe el acceso no autorizado% R1BOG(config)#
R2BOG	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R2BOG R2BOG(config)#enable secret class R2BOG(config)#line console 0 R2BOG(config-line)#password cisco R2BOG(config-line)#login R2BOG(config-line)#line vty 0 15 R2BOG(config-line)#password cisco R2BOG(config-line)#login R2BOG(config-line)#service password-encryption R2BOG(config)#banner motd %Se prohibe el acceso no autorizado%

	R2BOG(config)#
R3BOG	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R3BOG R3BOG(config)#enable secret class R3BOG(config)#line console 0 R3BOG(config-line)#password cisco R3BOG(config-line)#login R3BOG(config-line)#line vty 0 15 R3BOG(config-line)#password cisco R3BOG(config-line)#login R3BOG(config-line)#service password-encryption R3BOG(config)#banner motd %Se prohibe el acceso no autorizado% R3BOG(config)#

Fuente: Autor.

Figura 17. Red realizada



Fuente: Autor.

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

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

Tabla 24. Tabla de direcciones IP

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Máscara wildcard	Gateway predeterminado
R1MED	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
R2MED	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
R3MED	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
R1BOG	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
R2BOG	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
R3BOG	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

PC1MED	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.1
PC2MED	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.129
PC1BOG	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.0.1
PC2BOG	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.1.1

Fuente: Autor.

Nota: Las direcciones de la tabla se obtuvieron teniendo en cuenta la topología presentada.

Tabla 25. Configuración de los Routers y ISP

ELEMENTO	COMANDO IOS
R1MED	R1MED>en Password: R1MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R1MED(config)#int s0/0/0 R1MED(config-if)#description Conexion a R3MED R1MED(config-if)#ip address 172.29.6.9 255.255.255.252 R1MED(config-if)#clock rate 128000 R1MED(config-if)#no sh R1MED(config)#int s0/0/1 R1MED(config-if)#description Conexion a R2MED R1MED(config-if)#ip address 172.29.6.1 255.255.255.252 R1MED(config-if)#clock rate 128000 R1MED(config-if)#no sh R1MED(config)#int s0/1/0 R1MED(config-if)#description Conexion a R3MED R1MED(config-if)#ip address 172.29.6.13 255.255.255.252 R1MED(config-if)#clock rate 128000 R1MED(config-if)#no sh R1MED(config)#int s0/1/1 R1MED(config-if)#description Conexion al

	ISP R1MED(config-if)#ip address 209.17.220.1 255.255.255.252 R1MED(config-if)#no sh
R2MED	R2MED>en Password: R2MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R2MED(config)#int s0/0/0 R2MED(config-if)#description Conexion a R3MED R2MED(config-if)#ip address 172.29.6.5 255.255.255.252 R2MED(config-if)#clock rate 128000 R2MED(config-if)#no sh R2MED(config)#int s0/0/1 R2MED(config-if)#description Conexion a R1MED R2MED(config-if)#ip address 172.29.6.2 255.255.255.252 R2MED(config-if)#no sh R2MED(config)#int g0/0 R2MED(config-if)#description Conexion a PC1MED R2MED(config-if)#ip address 172.29.4.1 255.255.255.128 R2MED(config-if)#no sh
R3MED	R3MED>en Password: R3MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R3MED(config)#int s0/0/0 R3MED(config-if)#description Conexion a R2MED R3MED(config-if)#ip address 172.29.6.6 255.255.255.252 R3MED(config-if)#no sh R3MED(config)#int s0/0/1 R3MED(config-if)#description Conexion a R1MED R3MED(config-if)#ip address 172.29.6.10 255.255.255.252 R3MED(config-if)#no sh

	R3MED(config)#int s0/1/0 R3MED(config-if)#description Conexion a R1MED R3MED(config-if)#ip address 172.29.6.14 255.255.255.252 R3MED(config-if)#no sh R3MED(config)#int g0/0 R3MED(config-if)#description Conexion a PC2MED R3MED(config-if)#ip address 172.29.4.129 255.255.255.128 R3MED(config-if)#no sh
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 Conexion a R1MED ISP(config-if)#ip address 209.17.220.2 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no sh ISP(config)#int s0/0/1 ISP(config-if)#description Conexion a R1BOG ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no sh
R1BOG	R1BOG>en Password: R1BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R1BOG(config)#int s0/0/0 R1BOG(config-if)#description Conexion a ISP R1BOG(config-if)#ip address 209.17.220.6 255.255.255.252 R1BOG(config-if)#no sh R1BOG(config)#int s0/0/1 R1BOG(config-if)#description Conexion a

	R2BOG R1BOG(config-if)#ip address 172.29.3.1 255.255.255.252 R1BOG(config-if)#clock rate 128000 R1BOG(config-if)#no sh R1BOG(config)#int s0/1/0 R1BOG(config-if)#description Conexion a R3BOG R1BOG(config-if)#ip address 172.29.3.9 255.255.255.252 R1BOG(config-if)#clock rate 128000 R1BOG(config-if)#no sh R1BOG(config)#int s0/1/1 R1BOG(config-if)#description Conexion a R2BOG R1BOG(config-if)#ip address 172.29.3.5 255.255.255.252 R1BOG(config-if)#clock rate 128000 R1BOG(config-if)#no sh
R2BOG	R2BOG>en Password: R2BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R2BOG(config)#int s0/0/0 R2BOG(config-if)#description Conexion a R1BOG R2BOG(config-if)#ip address 172.29.3.2 255.255.255.252 R2BOG(config-if)#no sh R2BOG(config)#int s0/0/1 R2BOG(config-if)#description Conexion a R3BOG R2BOG(config-if)#ip address 172.29.3.13 255.255.255.252 R2BOG(config-if)#clock rate 128000 R2BOG(config-if)#no sh R2BOG(config)#int s0/1/0 R2BOG(config-if)#description Conexion a R1BOG R2BOG(config-if)#ip address 172.29.3.6 255.255.255.252 R2BOG(config-if)#no sh

	R2BOG(config)#int g0/0 R2BOG(config-if)#description Conexion a PC1BOG R2BOG(config-if)#ip address 172.29.0.1 255.255.255.0 R2BOG(config-if)#no sh
R3BOG	R3BOG>en Password: R3BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R3BOG(config)#int s0/0/0 R3BOG(config-if)#description Conexion R1BOG R3BOG(config-if)#ip address 172.29.3.10 255.255.255.252 R3BOG(config-if)#no sh R3BOG(config)#int s0/0/1 R3BOG(config-if)#description Conexion a R2BOG R3BOG(config-if)#ip address 172.29.3.14 255.255.255.252 R3BOG(config-if)#no sh R3BOG(config)#int g0/0 R3BOG(config-if)#description Conexion a PC2BOG R3BOG(config-if)#ip address 172.29.1.1 255.255.255.0 R3BOG(config-if)#no sh

Fuente: Autor.

2.2 PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

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

Tabla 26. Configuración OSPF versión 2 en los dispositivos

ELEMENTO	COMANDO IOS
R1MED	R1MED>en Password: R1MED#conf t Enter configuration commands, one per line. End with CNTL/Z.

	R1MED(config)#router ospf 1 R1MED(config-router)#router-id 1.1.1.1 R1MED(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 R1MED(config-router)#network 172.29.6.0 0.0.0.3 area 0 R1MED(config-router)#network 172.29.6.8 0.0.0.3 area 0 R1MED(config-router)#network 172.29.6.12 0.0.0.3 area 0 R1MED(config-router)#network 209.17.220.0 0.0.0.3 area 0 R1MED(config-router)#exit
R2MED	R2MED>en Password: R2MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R2MED(config)#router ospf 1 R2MED(config-router)#router-id 2.2.2.2 R2MED(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 R2MED(config-router)#network 172.29.4.0 0.0.0.127 area 0 R2MED(config-router)#network 172.29.6.0 0.0.0.3 area 0 R2MED(config-router)# 00:10:28: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done R2MED(config-router)#network

	172.29.6.4 0.0.0.3 area 0
R3MED	R3MED>en Password: R3MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R3MED(config)#router ospf 1 R3MED(config-router)#router-id 3.3.3.3 R3MED(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 R3MED(config-router)#network 172.29.4.128 0.0.0.127 area 0 R3MED(config-router)#network 172.29.6.4 0.0.0.3 area 0 R3MED(config-router)# 00:12:50: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done R3MED(config-router)#network 172.29.6.8 0.0.0.3 area 0 R3MED(config-router)# 00:13:01: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done R3MED(config-router)#network 172.29.6.12 0.0.0.3 area 0 R3MED(config-router)# 00:13:23: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1/0 from LOADING to FULL, Loading Done
R1BOG	R1BOG>en Password: R1BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R1BOG(config)#router ospf 1 R1BOG(config-router)#router-id 4.4.4.4

	R1BOG(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 R1BOG(config-router)#network 172.29.3.0 0.0.0.3 area 0 R1BOG(config-router)#network 172.29.3.4 0.0.0.3 area 0 R1BOG(config-router)#network 172.29.3.8 0.0.0.3 area 0 R1BOG(config-router)#network 209.17.220.4 0.0.0.3 area 0
R2BOG	R2BOG>en Password: R2BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R2BOG(config)#router ospf 1 R2BOG(config-router)#router-id 5.5.5.5 R2BOG(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 R2BOG(config-router)#network 172.29.0.0 0.0.0.255 area 0 R2BOG(config-router)#network 172.29.3.0 0.0.0.3 area 0 R2BOG(config-router)# 00:17:55: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING to FULL, Loading Done R2BOG(config-router)#network 172.29.3.4 0.0.0.3 area 0

	R2BOG(config-router)#network 172.29.3.12 0.0.0.3 area 0 00:18:11: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/1/0 R2BOG(config-router)#network 172.29.3.12 0.0.0.3 area 0
R3BOG	R3BOG>en Password: R3BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R3BOG(config)#router ospf 1 R3BOG(config-router)#router-id 6.6.6.6 R3BOG(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 R3BOG(config-router)#network 172.29.1.0 0.0.0.255 area 0 R3BOG(config-router)#network 172.29.3.8 0.0.0.3 area 0 R3BOG(config-router)# 00:20:27: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING to FULL, Loading Done R3BOG(config-router)#network 172.29.3.12 0.0.0.3 area 0 R3BOG(config-router)# 00:20:38: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL, Loading Done
ISP	ISP>en Password: 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)# 00:21:44: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0 ISP(config-router)# 00:22:04: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/1 from LOADING to FULL, Loading Done

Fuente: Autor.

2.2.2 Los routers Bogota1 y Medellín1 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.

Tabla 27. Configuración ruta R1MED y R1BOG

ELEMENTO	COMANDO IOS
R1MED	R1MED>en Password: R1MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R1MED(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2 R1MED(config)#router ospf 1 R1MED(config-router)#default-information originate R1MED(config-router)#exit
R1BOG	R1BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R1BOG(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 R1BOG(config)#router ospf 1 R1BOG(config-router)#default-information originate R1BOG(config-router)#exit

Fuente: Autor.

2.2.3 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.

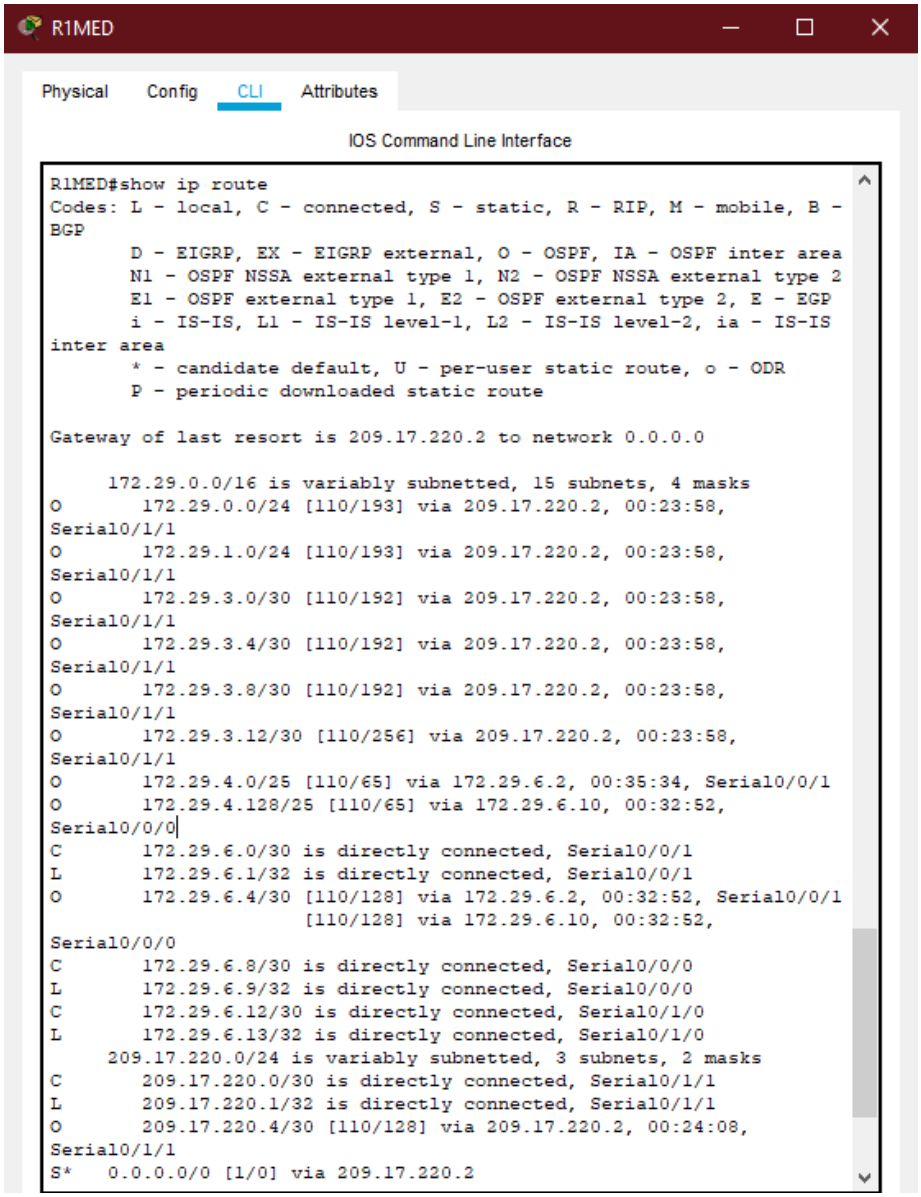
Tabla 28. Configuración ruta estática Router ISP

ELEMENTO	COMANDO IOS
ISP	ISP>en Password: ISP#conf t Enter configuration commands, one per line. End with CNTL/Z. 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

Fuente: Autor.

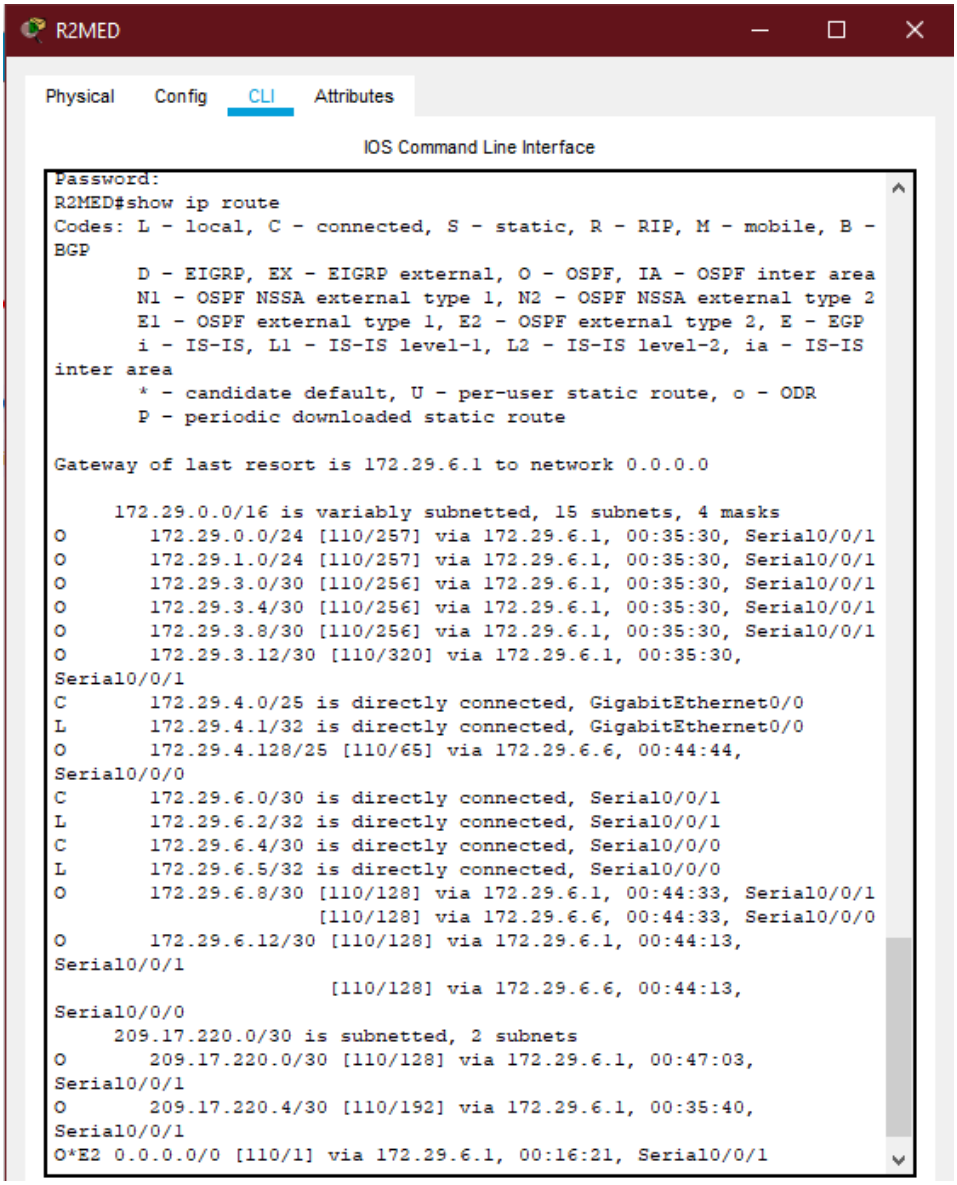
2.3 PARTE 2: TABLA DE ENRUTAMIENTO

Figura 18. Show ip route en R1MED



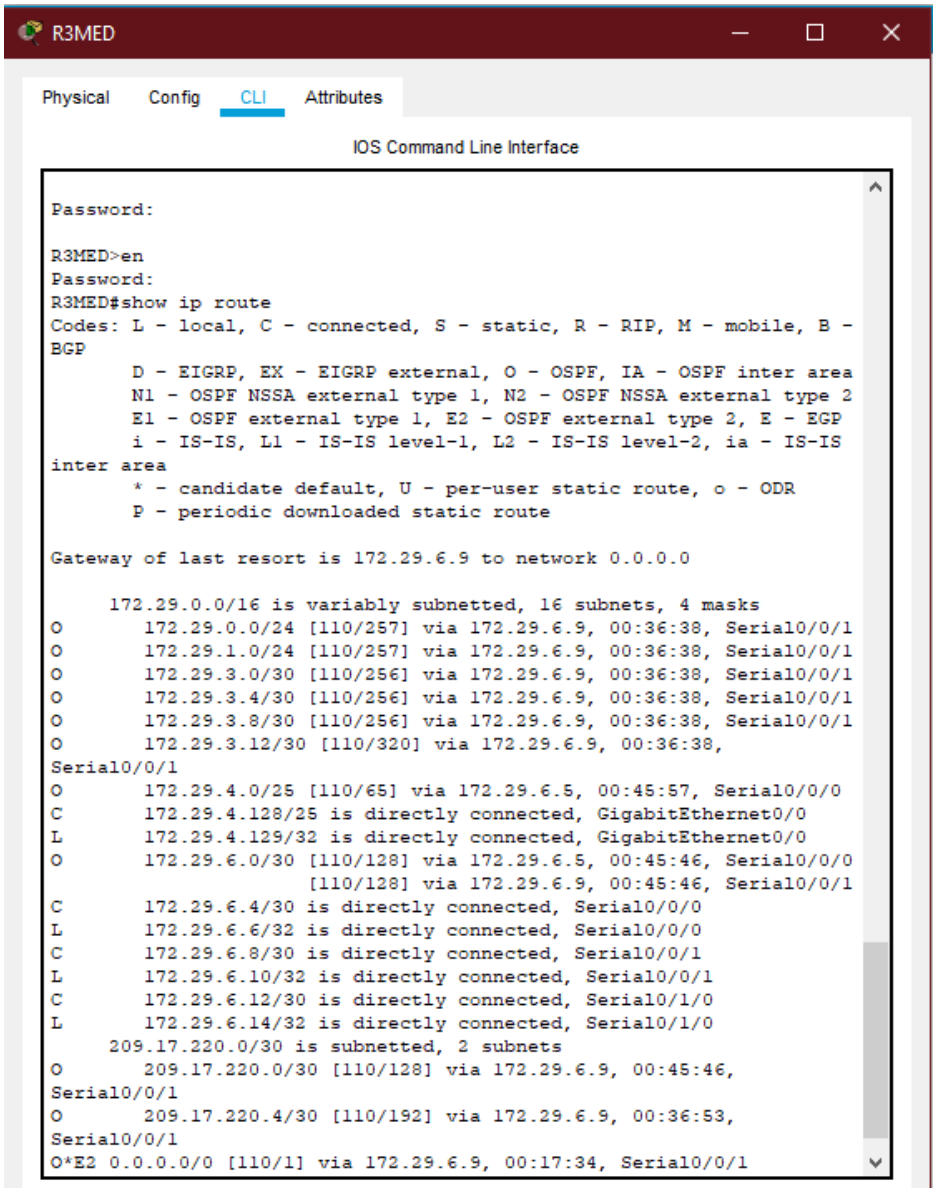
Fuente: Autor.

Figura 19. Show ip route en R2MED



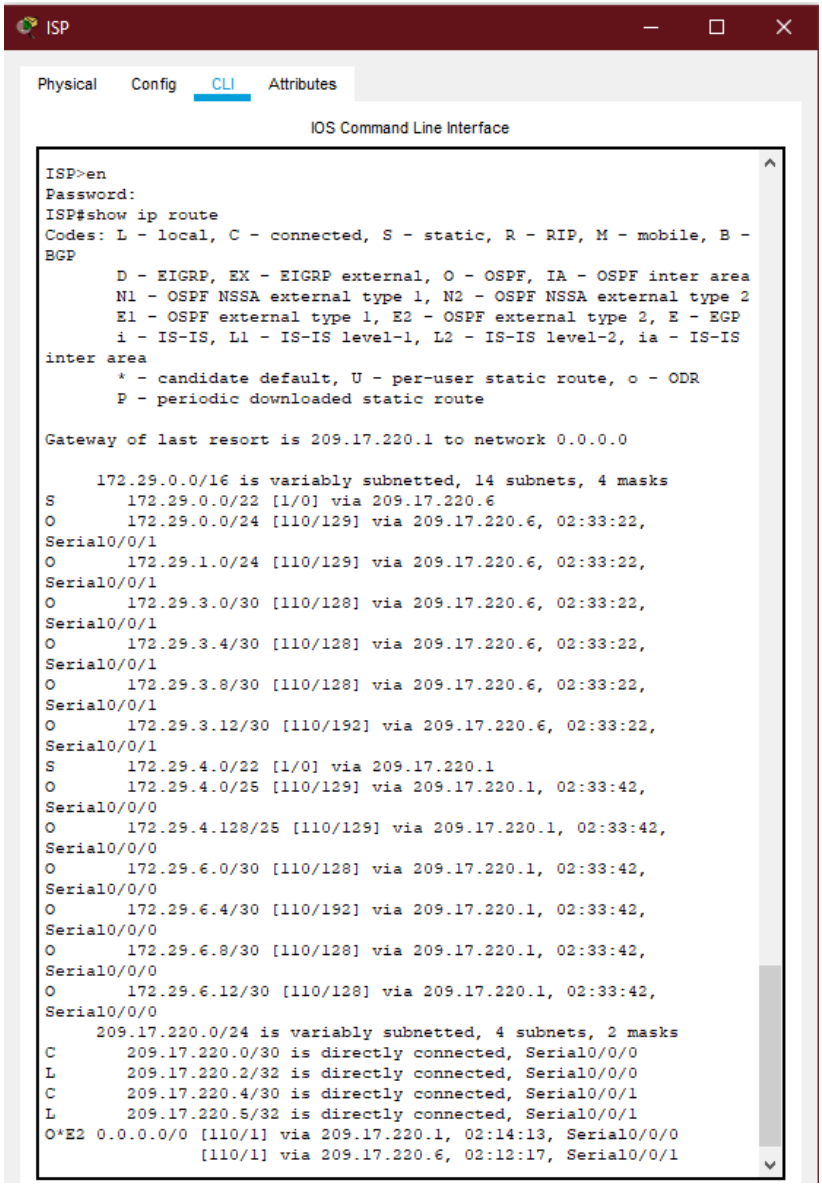
Fuente: Autor.

Figura 20. Show ip route en R3MED



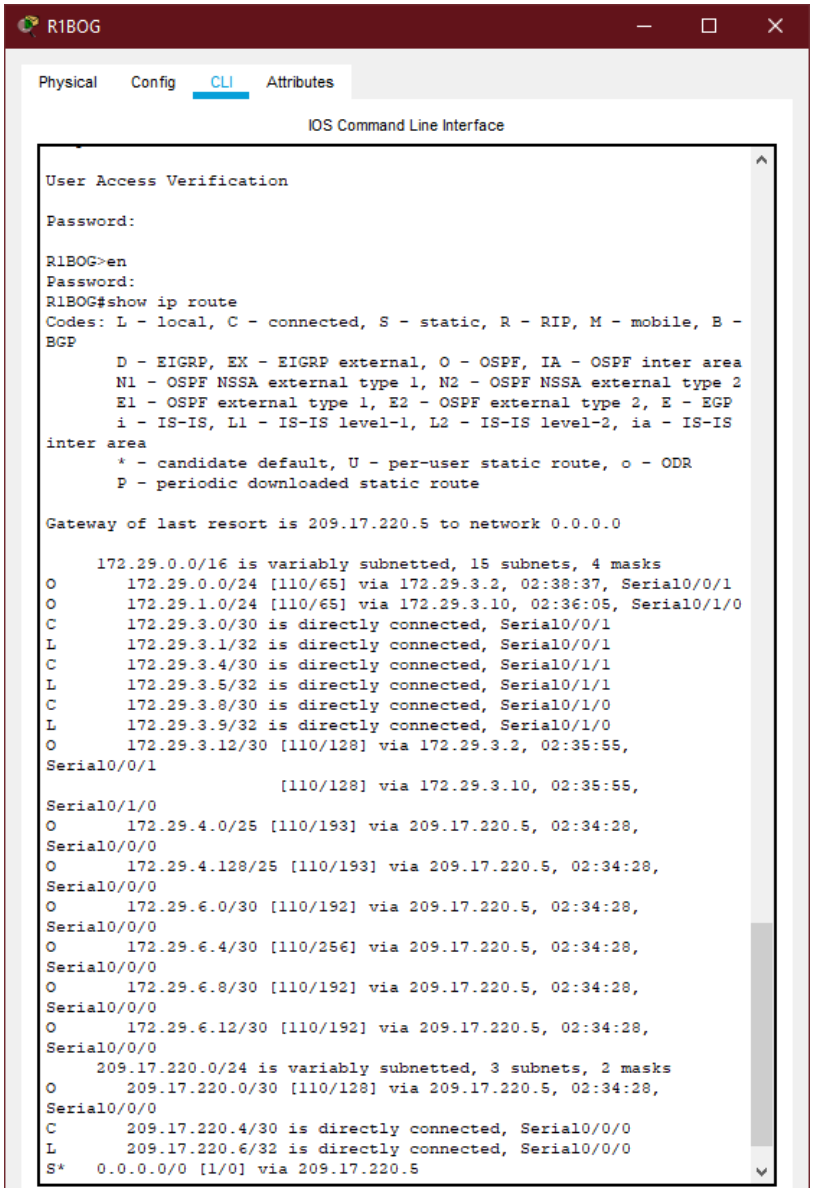
Fuente: Autor.

Figura 21. Show ip route ISP



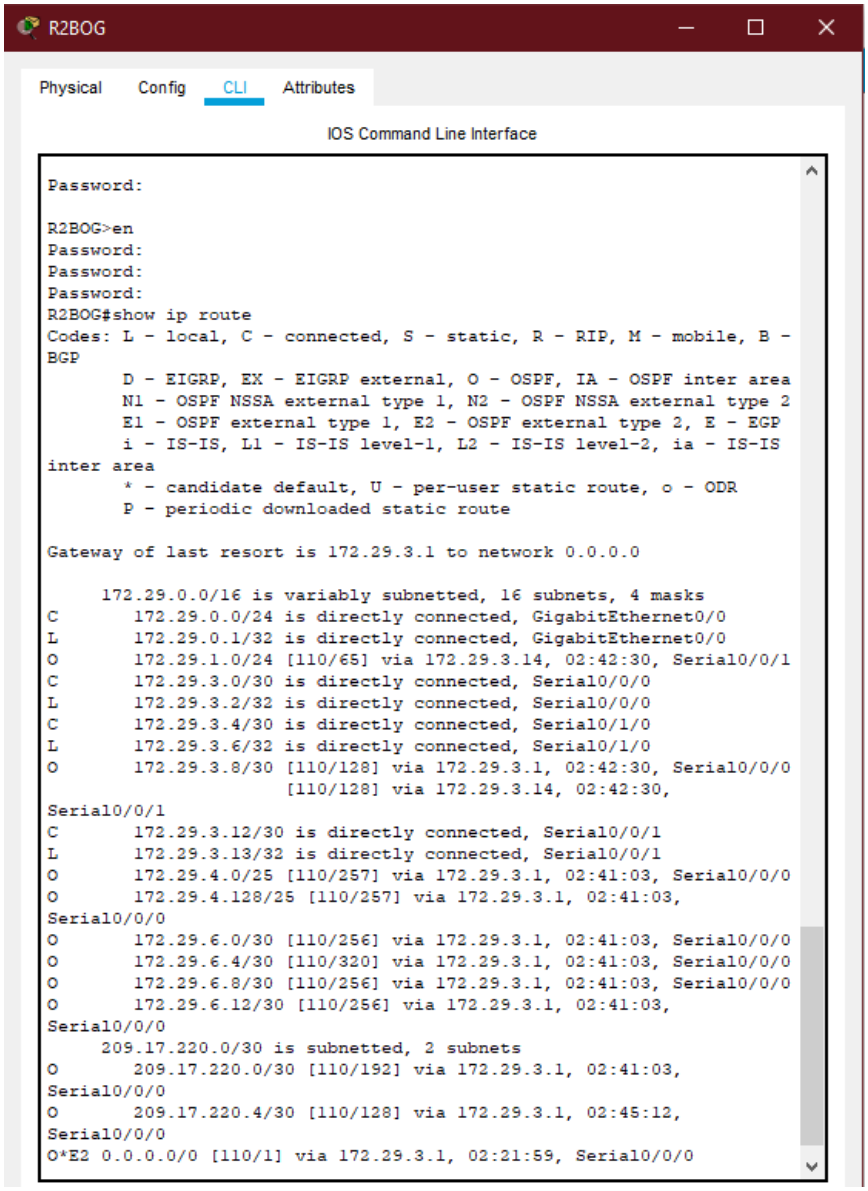
Fuente: Autor.

Figura 22. Show ip route en R1BOG



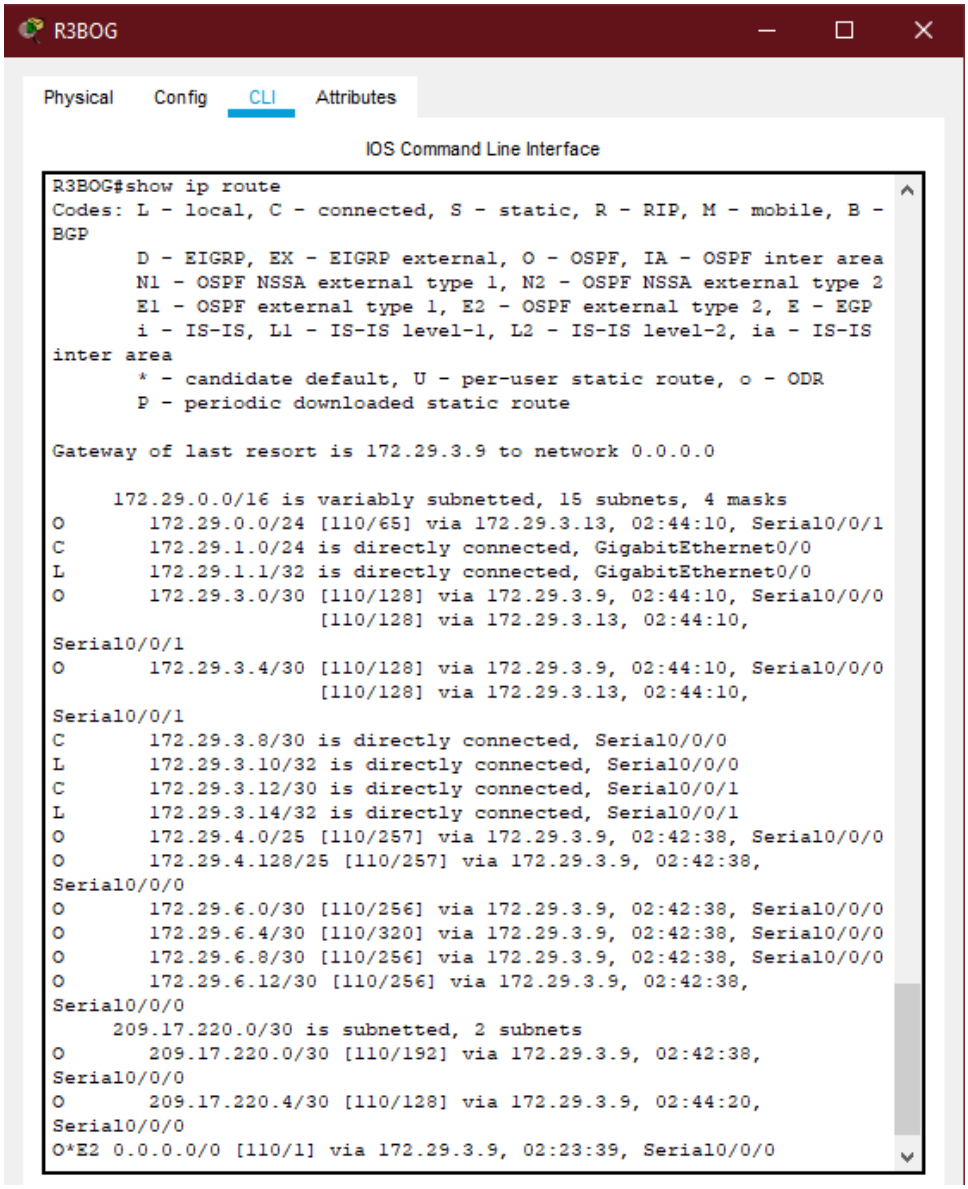
Fuente: Autor.

Figura 23. Show ip route en R2BOG



Fuente: Autor.

Figura 24. Show ip route en R3BOG



Fuente: Autor.

2.4 PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

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

Tabla 29. Tabla de interfaces en cada Router

ROUTER	**INTERFAZ**
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Fuente: Prueba de habilidades CCNA 2020, Cisco Academy

Tabla 30. Configuración para deshabilitar la propagación del protocolo OSPF

ELEMENTO	**COMANDOS IOS**
R1MED	R1MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R1MED(config)#router ospf 1 R1MED(config-router)#passive-interface s0/1/0 R1MED(config-router)# 00:04:02: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Interface down or detached
R2MED	R2MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R2MED(config)#router ospf 1 R2MED(config-router)#passive-interface g0/0 R2MED(config-router)#exit
R3MED	R3MED>en

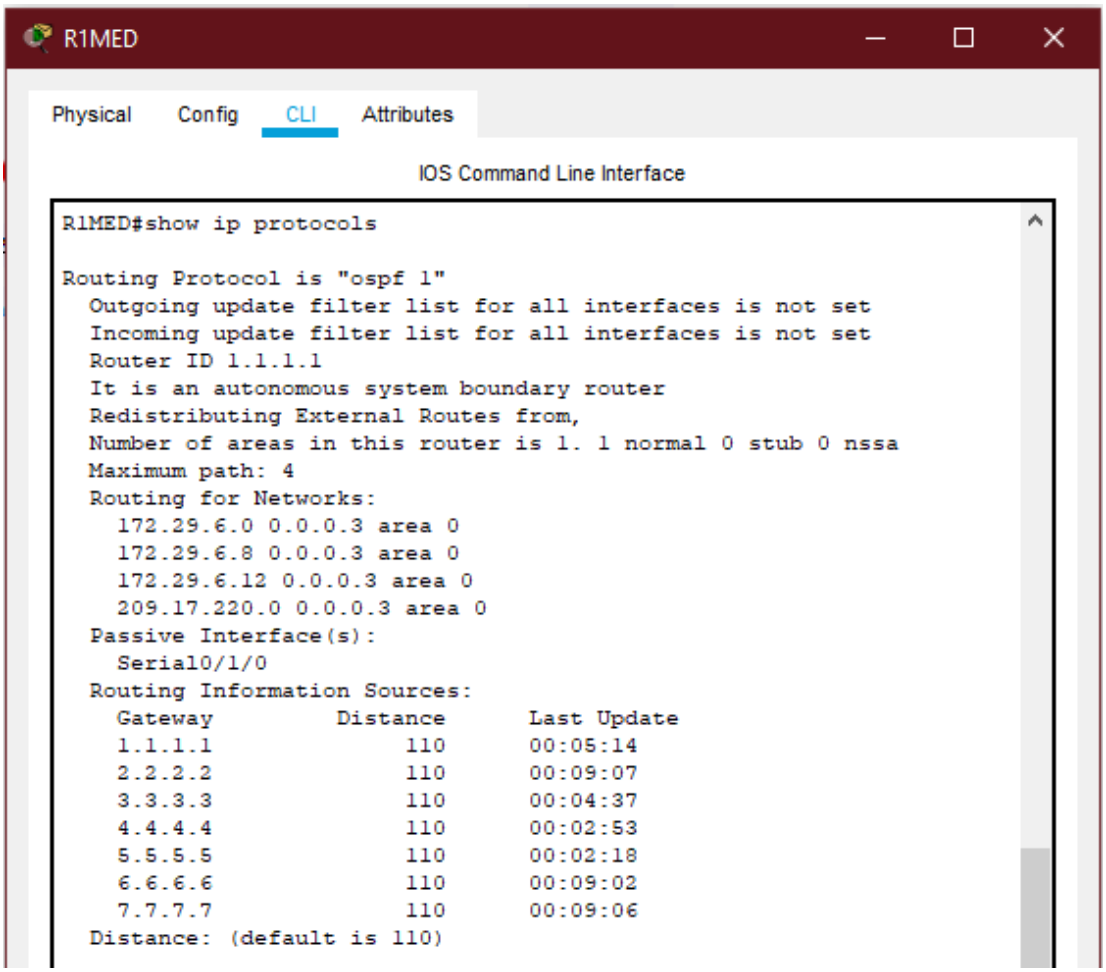
	Password: R3MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R3MED(config)#router ospf 1 R3MED(config-router)#passive-interface g0/0 R3MED(config-router)#exit
R1BOG	R1BOG>en Password: R1BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R1BOG(config)#router ospf 1 R1BOG(config-router)#passive-interface s0/1/1 R1BOG(config-router)# 00:06:24: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1/1 from FULL to DOWN, Neighbor Down: Interface down or detached
R2BOG	R2BOG(config)#router ospf 1 R2BOG(config-router)#passive-interface s0/1/0 R2BOG(config-router)#passive-interface g0/0 R2BOG(config-router)#exit
R3BOG	R3BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R3BOG(config)#router ospf 1 R3BOG(config-router)#passive-interface g0/0 R3BOG(config-router)#exit

Fuente: Autor.

2.5 PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF

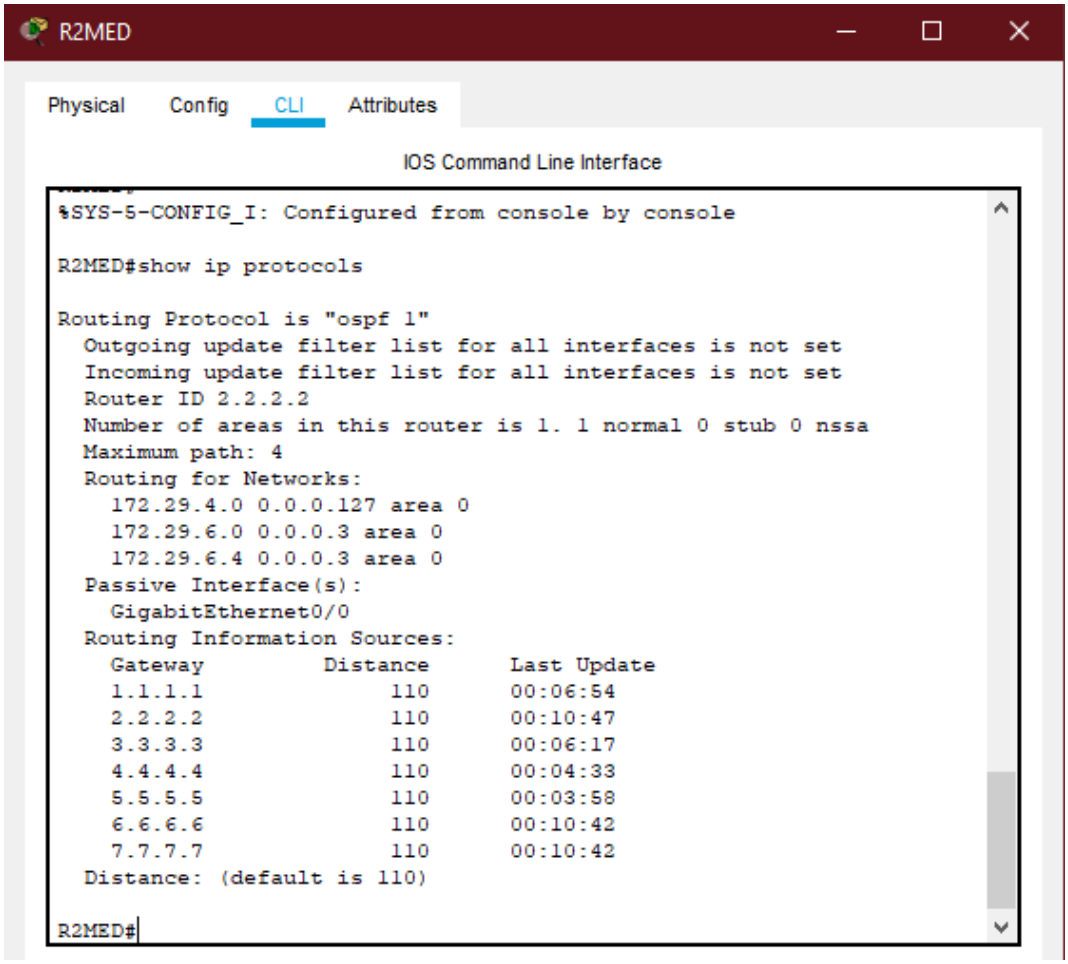
2.5.1 Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Figura 25. Show ip protocols en R1MED



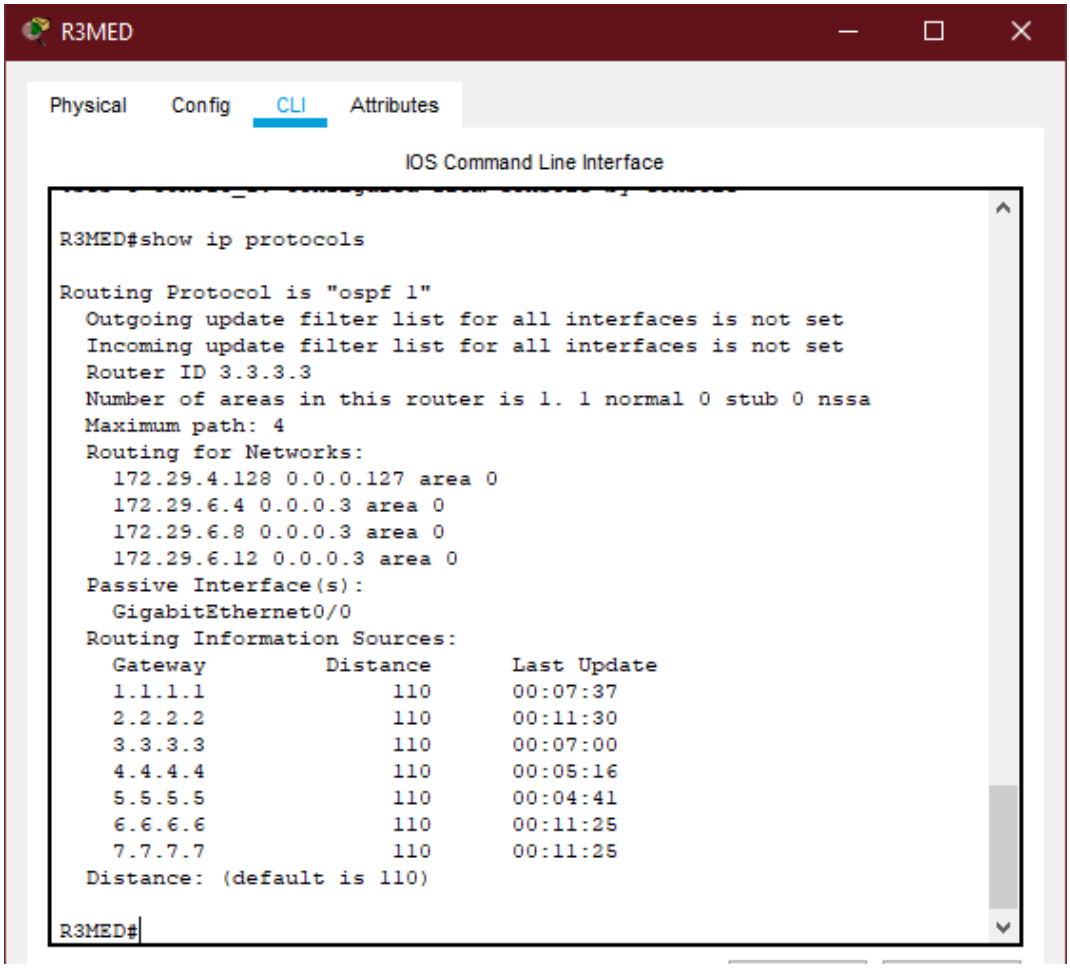
Fuente: Autor.

Figura 26. Show ip protocols en R2MED



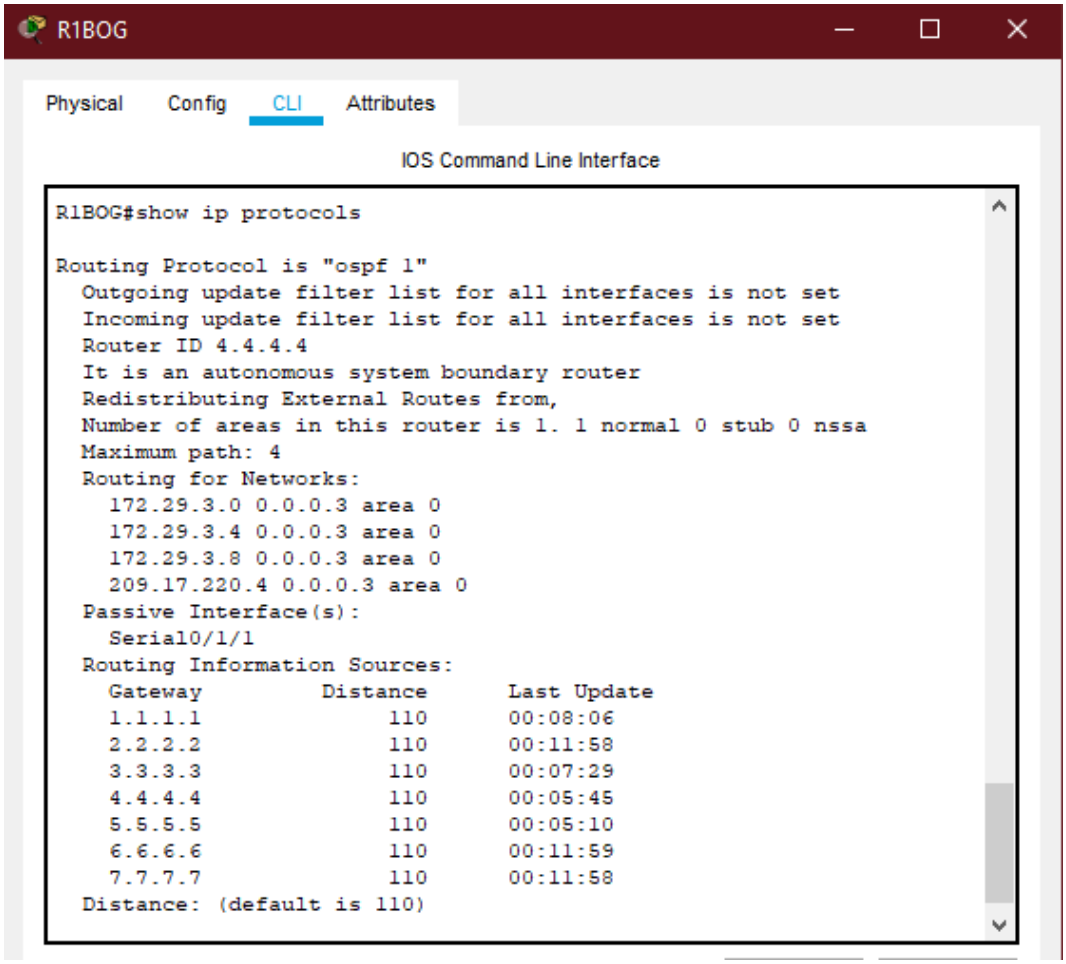
Fuente: Autor.

Figura 27. Show ip protocols en R3MED



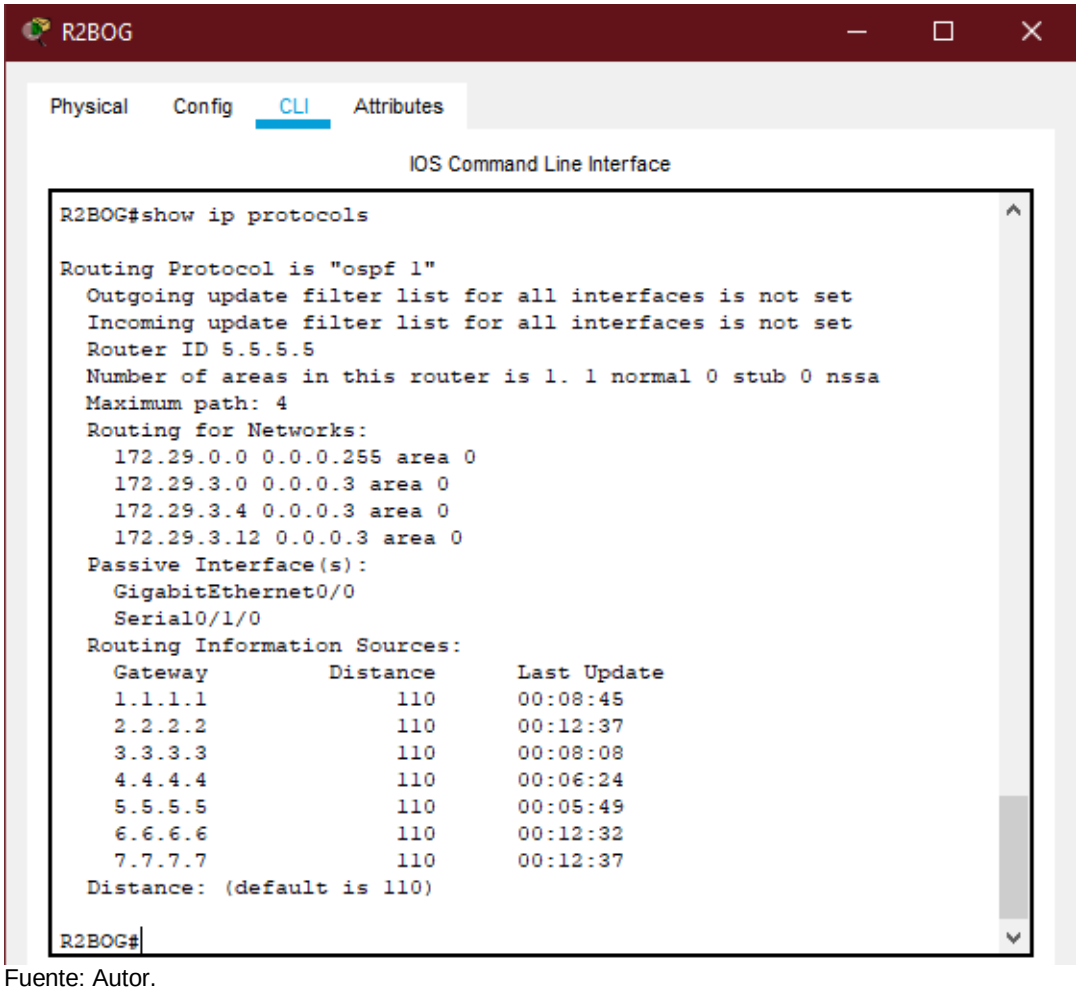
Fuente: Autor.

Figura 28. Show ip protocols en R1BOG



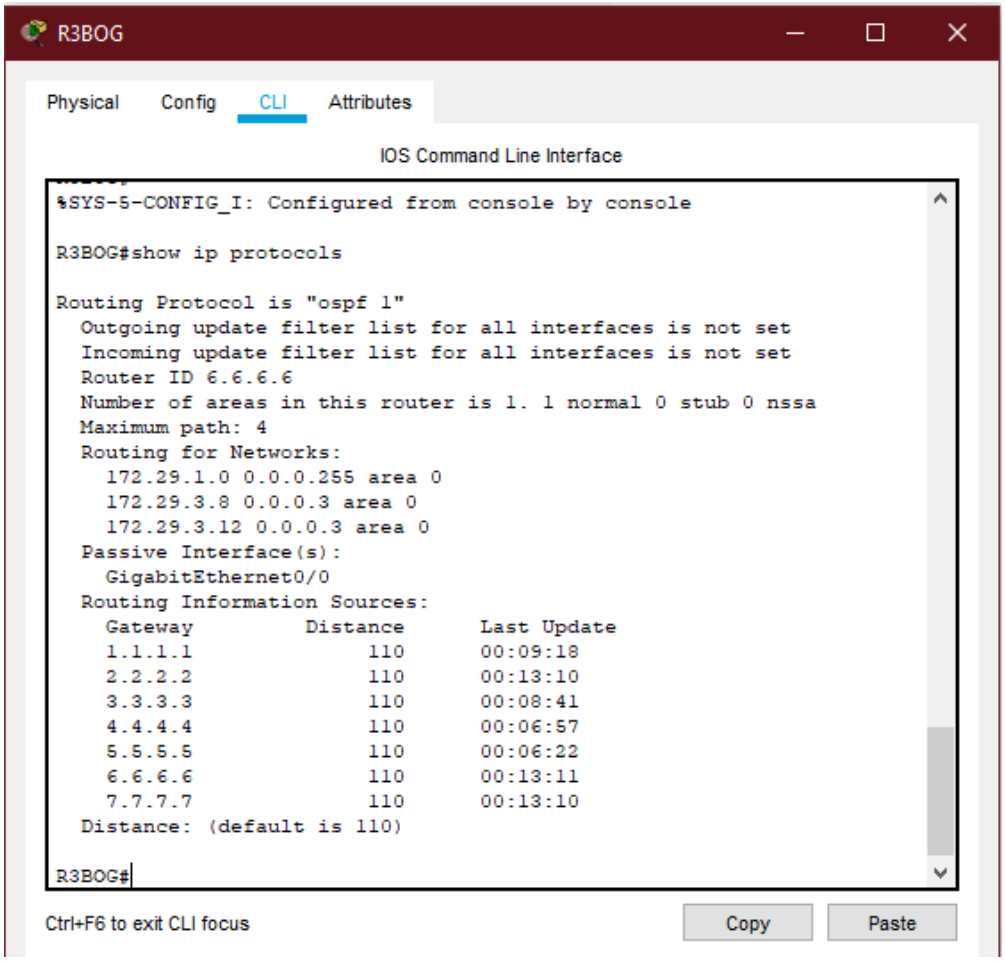
Fuente: Autor.

Figura 29. Show ip protocols en R2BOG



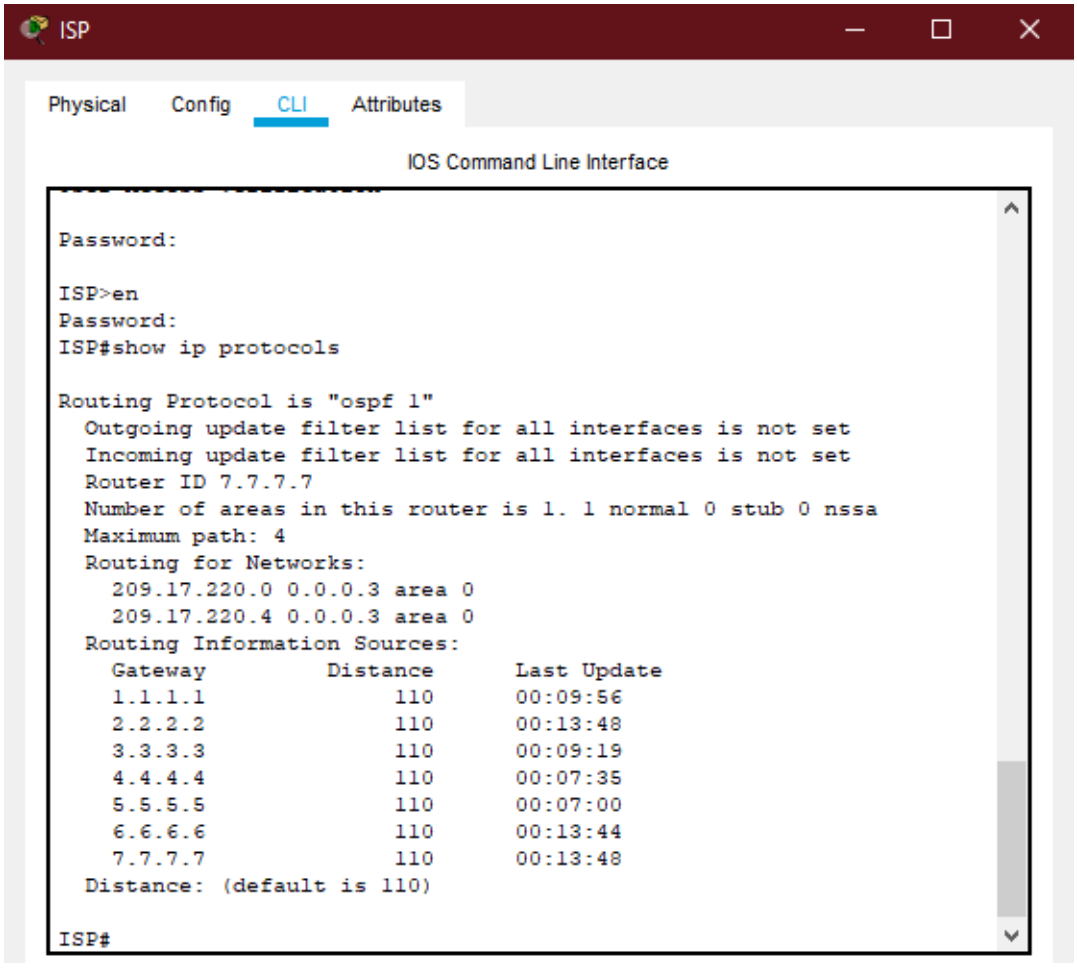
Fuente: Autor.

Figura 30. Show ip protocols en R3BOG



Fuente: Autor.

Figura 31. Show ip protocols en ISP



Fuente: Autor.

25.2 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.

Esto fue resuelto en el punto, PARTE 2: TABLA DE ENRUTAMIENTO.

2.6 PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

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

Tabla 31. Configuración encapsulamiento y autenticación PPP

ELEMENTO	COMANDOS IOS
R1MED	R1MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R1MED(config)#int s0/1/1 R1MED(config-if)#encapsulation ppp R1MED(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to down 00:16:39: %OSPF-5-ADJCHG: Process 1, Nbr 7.7.7.7 on Serial0/1/1 from FULL to DOWN, Neighbor Down: Interface down or detached R1MED(config-if)#no sh R1MED(config-if)#exit R1MED(config)#username ISP secret cisco R1MED(config)#int s0/1/1 R1MED(config-if)#ppp authentication pap R1MED(config-if)#ppp pap sent-username MEDELLIN password cisco R1MED(config-if)#exit
R1BOG	R1BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R1BOG(config)#int s0/0/0 R1BOG(config-if)#encapsulation ppp R1BOG(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down 00:19:10: %OSPF-5-ADJCHG: Process 1, Nbr 7.7.7.7 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached R1BOG(config-if)#no sh R1BOG(config-if)#exit R1BOG(config)#username ISP secret cisco R1BOG(config)#int s0/0/0 R1BOG(config-if)#ppp authentication chap R1BOG(config-if)#exit

ISP	ISP#conf t Enter configuration commands, one per line. End with CNTL/Z. ISP(config)#int s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#no sh ISP(config-if)#exit ISP(config)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#no sh 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

Fuente: Autor.

2.7 PARTE 6: CONFIGURACIÓN DE PAT

2.7.1 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. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

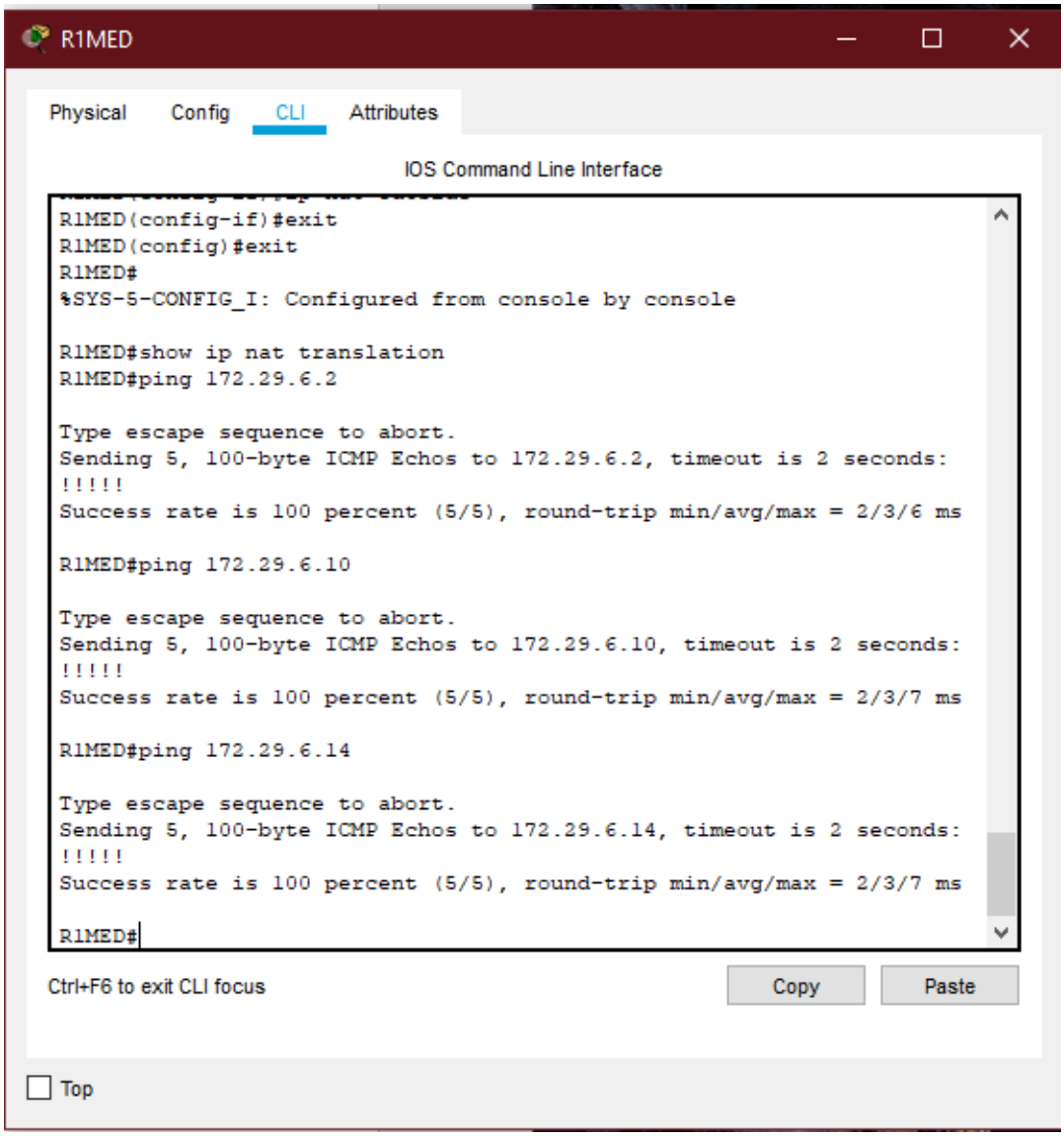
Tabla 32. Configuración de PAT

ELEMENTOS	COMANDOS IOS
R1MED	R1MED(config)#ip access-list standard HOST R1MED(config-std-nacl)#permit 172.29.4.0 0.0.0.127

	R1MED(config-std-nacl)#exit R1MED(config)#ip nat inside source list HOST interface s0/1/1 overload R1MED(config)#int s0/0/0 R1MED(config-if)#ip nat inside R1MED(config-if)#exit R1MED(config)#int s0/0/1 R1MED(config-if)#ip nat inside R1MED(config-if)#exit R1MED(config)#int s0/1/0 R1MED(config-if)#ip nat inside R1MED(config-if)#exit R1MED(config)#int s0/1/1 R1MED(config-if)#ip nat outside R1MED(config-if)#exit R1MED(config)#exit
R1BOG	R1BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R1BOG(config)#ip access-list standard HOST R1BOG(config-std-nacl)#permit 172.29.0.0 0.0.0.255 R1BOG(config-std-nacl)#exit R1BOG(config)#ip nat inside source list HOST interface s0/0/0 overload R1BOG(config)#int s0/0/0 R1BOG(config-if)#ip nat outside R1BOG(config-if)#exit R1BOG(config)#int s0/0/1 R1BOG(config-if)#ip nat inside R1BOG(config-if)#exit R1BOG(config)#int s0/1/0 R1BOG(config-if)#ip nat inside R1BOG(config-if)#exit R1BOG(config)#int s0/1/1 R1BOG(config-if)#ip nat inside R1BOG(config-if)#exit R1BOG(config)#exit

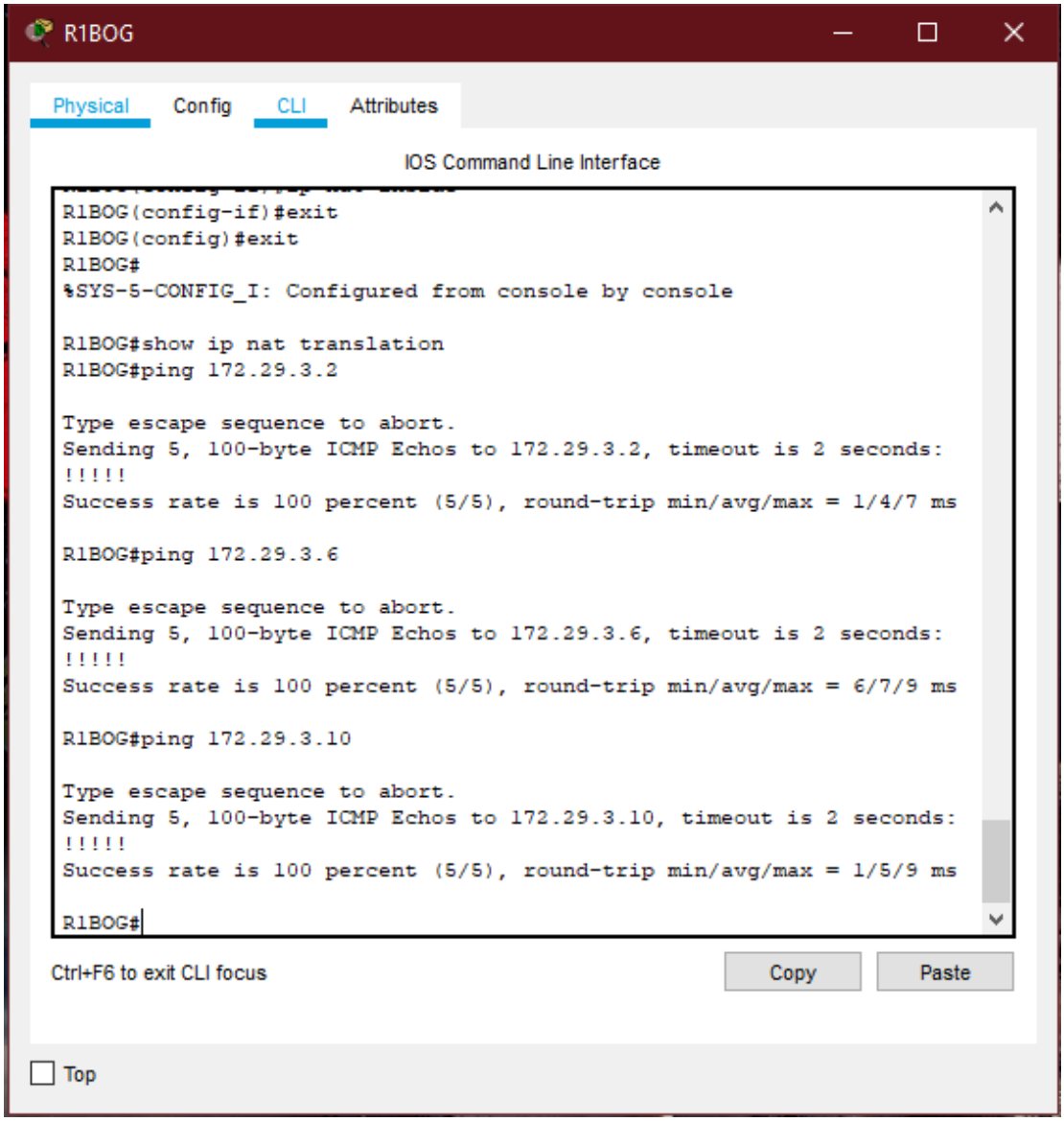
Fuente: Autor.

Figura 32. Ping desde R1MED a R2MED Y R3MED



Fuente: Autor.

Figura 33. Ping de R1BOG a R2BOG y R3BOG



Fuente: Autor.

2.8 PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP

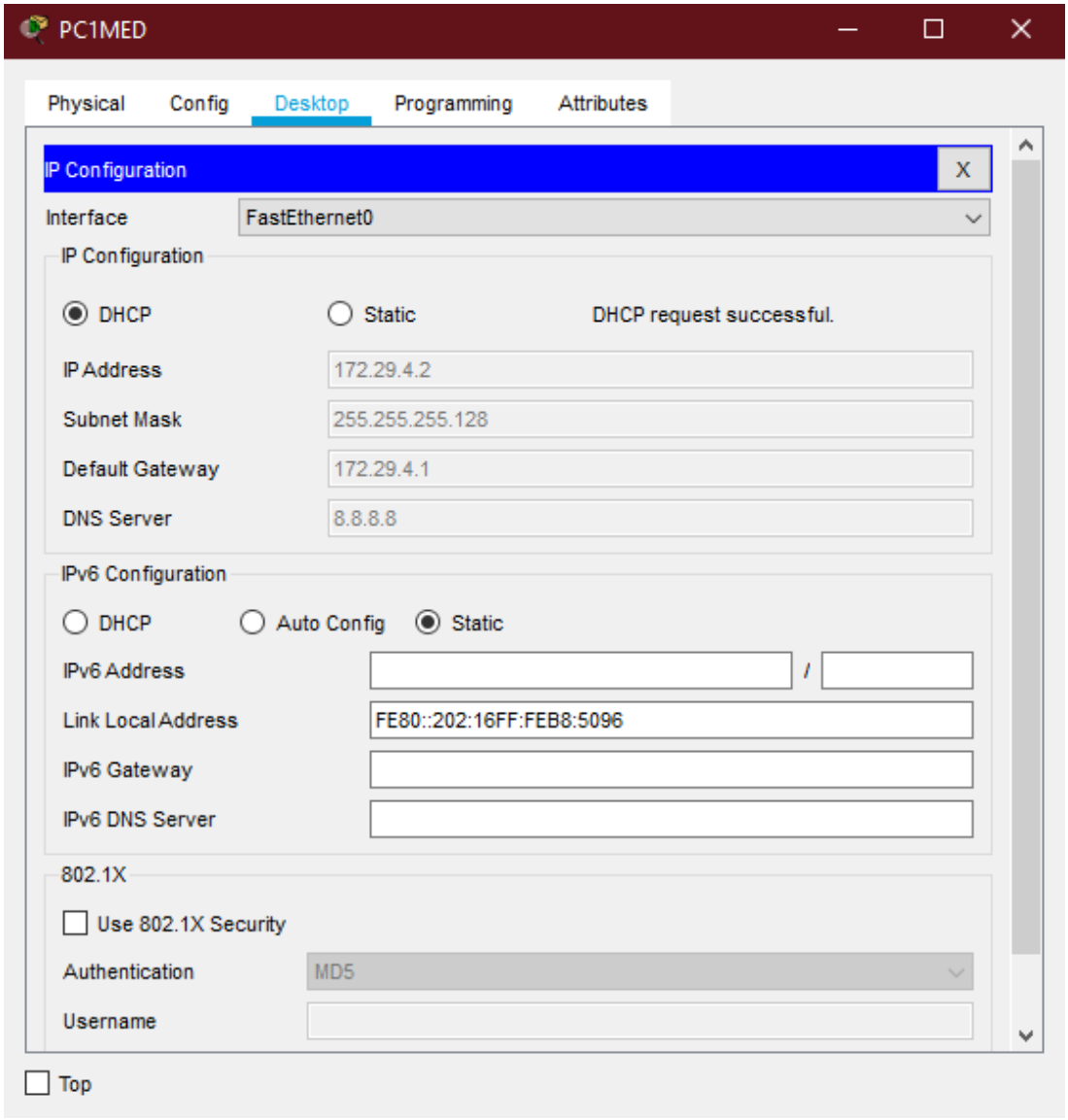
2.8.1 Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

Tabla 33. Configuración servicio DHCP

ELEMENTOS	COMANDOS IOS
R2MED	R2MED>en Password: R2MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R2MED(config)#ip dhcp excluded-address 172.29.4.1 R2MED(config)#ip dhcp pool R2MED R2MED(dhcp-config)#network 172.29.4.0 255.255.255.128 R2MED(dhcp-config)#default-router 172.29.4.1 R2MED(dhcp-config)#dns-server 8.8.8.8 R2MED(dhcp-config)#exit R2MED(config)#ip dhcp excluded-address 172.29.4.29 R2MED(config)#ip dhcp pool R3MED R2MED(dhcp-config)#network 172.29.4.128 255.255.255.128 R2MED(dhcp-config)#default-router 172.29.4.129 R2MED(dhcp-config)#dns-server 8.8.8.8 R2MED(dhcp-config)#exit R2MED(config)#
R3MED	R3MED>en Password: R3MED#conf t Enter configuration commands, one per line. End with CNTL/Z. R3MED(config)#int g0/0 R3MED(config-if)#ip helper-address 172.29.6.5 R3MED(config-if)#exit

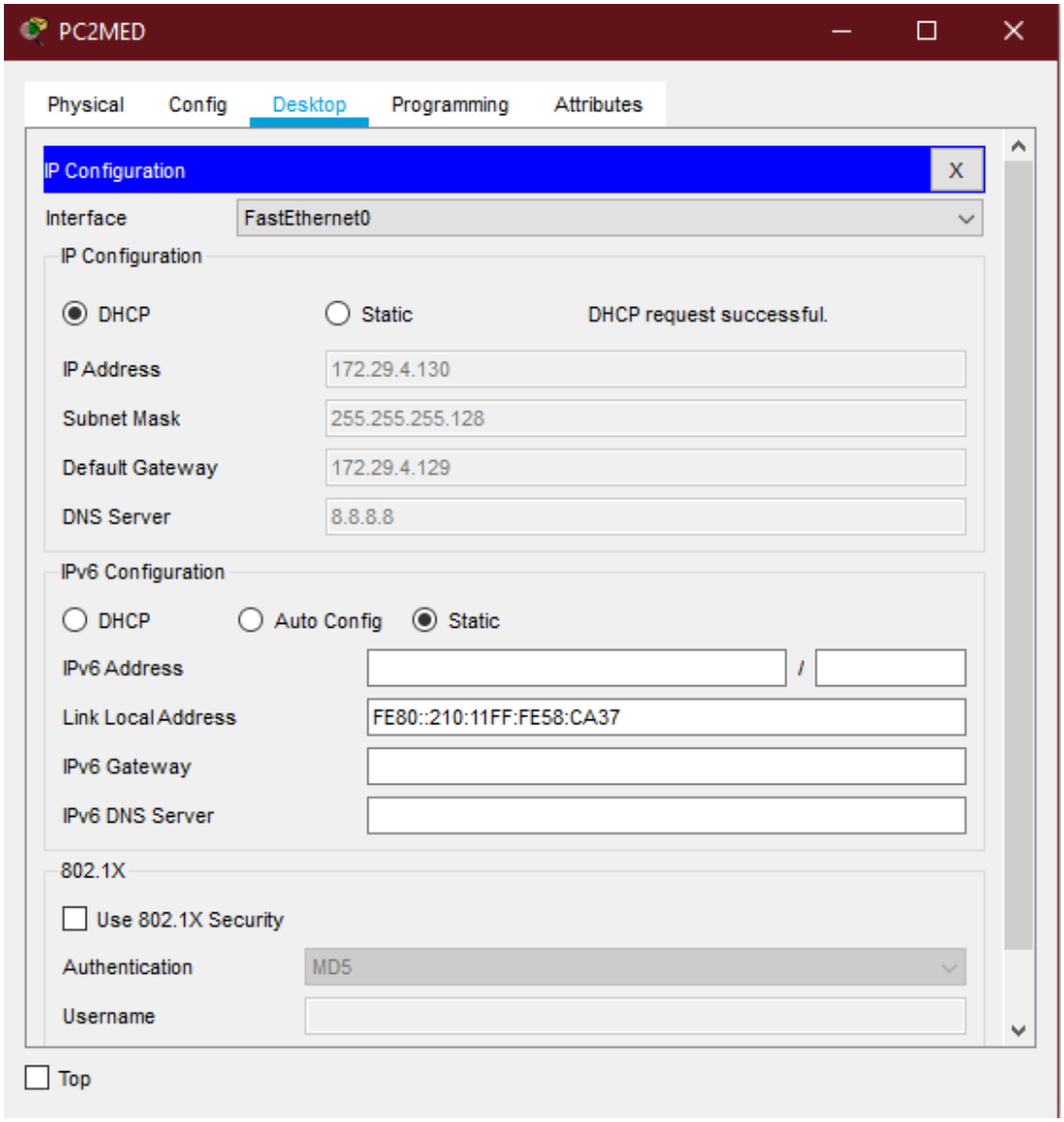
Fuente: Autor.

Figura 34. Configuración ip PC1MED



Fuente: Autor.

Figura 35. Configuración ip PC2MED



Fuente: Autor.

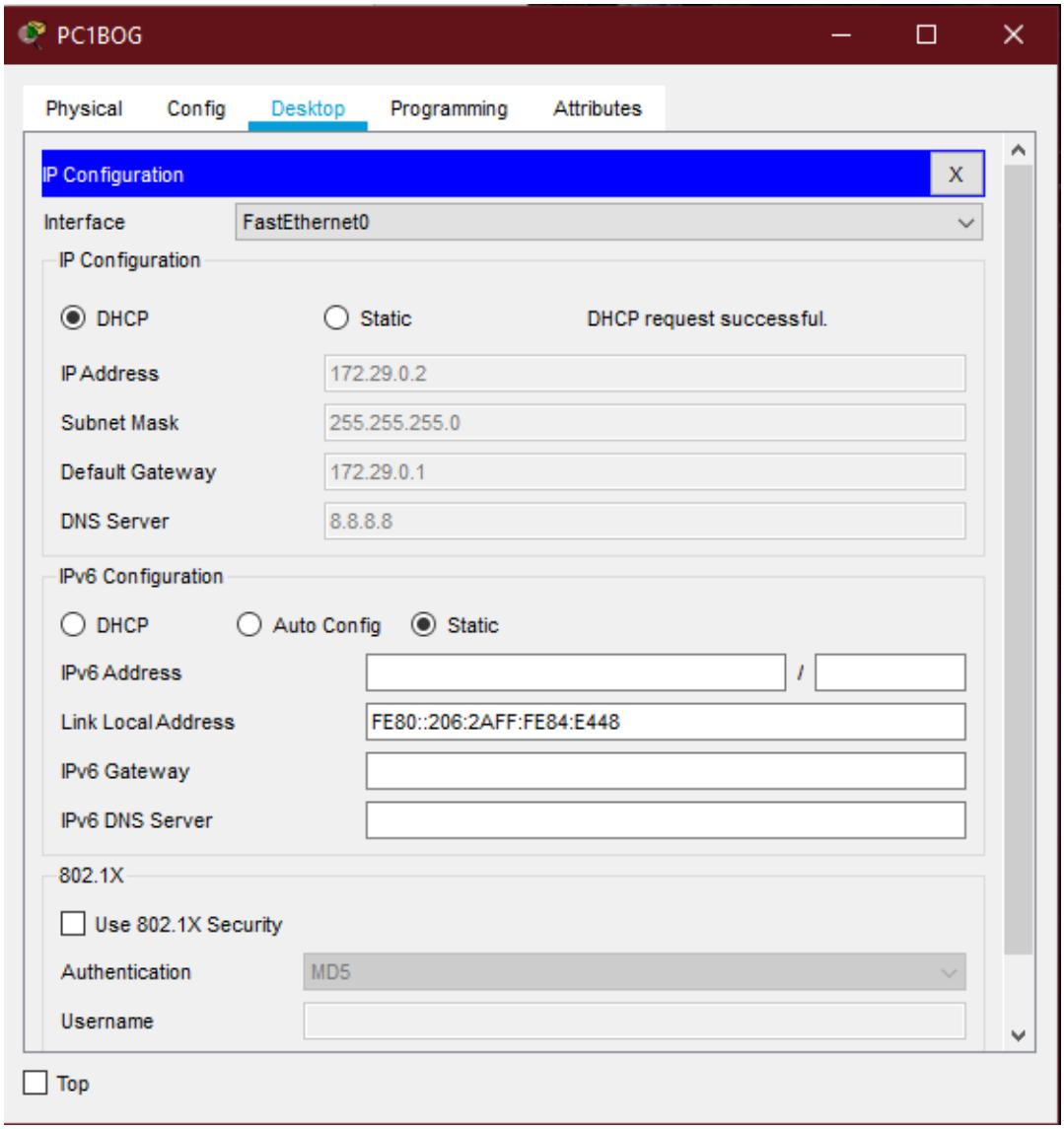
2.8.2 Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Tabla 34. Configuración servicio DHCP

ELEMENTOS	COMANDOS IOS
R2BOG	R2BOG>en Password: R2BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R2BOG(config)#ip dhcp exluced-address 172.29.0.1 R2BOG(config)#ip dhcp excluded-address 172.29.0.1 R2BOG(config)# R2BOG(config)#ip dhcp pool R2BOG R2BOG(dhcp-config)#network 172.29.0.0 255.255.255.0 R2BOG(dhcp-config)#default-router 172.29.0.1 R2BOG(dhcp-config)#dns-server 8.8.8.8 R2BOG(dhcp-config)#exit R2BOG(config)#ip dhcp excluded-address 172.29.1.1 R2BOG(config)#ip dhcp pool R3BOG R2BOG(dhcp-config)#network 172.29.1.0 255.255.255.0 R2BOG(dhcp-config)#default-router 172.29.1.1 R2BOG(dhcp-config)#dns-server 8.8.8.8 R2BOG(dhcp-config)#exit
R3BOG	R3BOG>en Password: R3BOG#conf t Enter configuration commands, one per line. End with CNTL/Z. R3BOG(config)#int g0/0 R3BOG(config-if)#ip helper-address 172.29.3.13 R3BOG(config-if)#exit

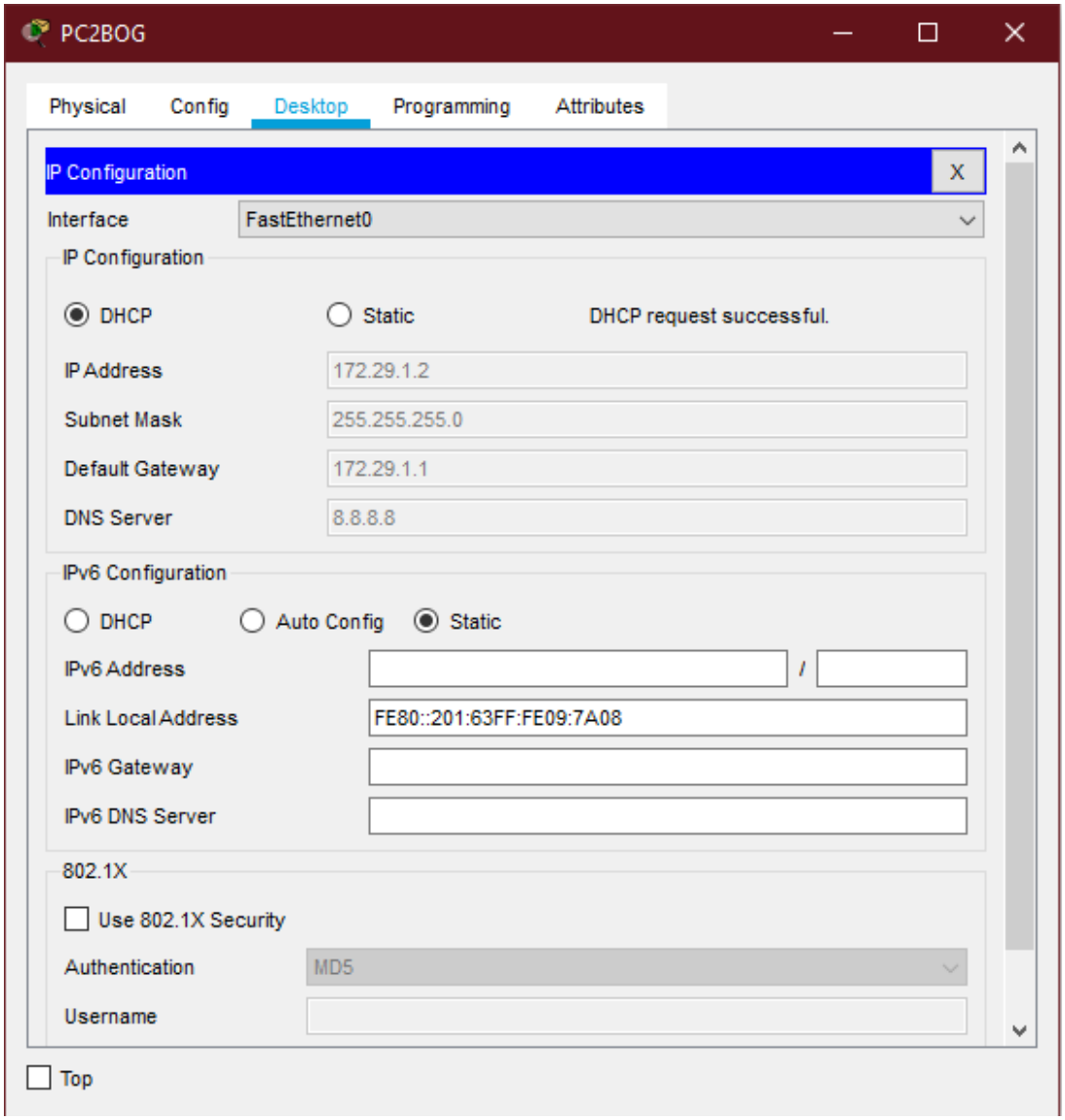
Fuente: Autor.

Figura 36. Configuración ip PC1BOG



Fuente: Autor.

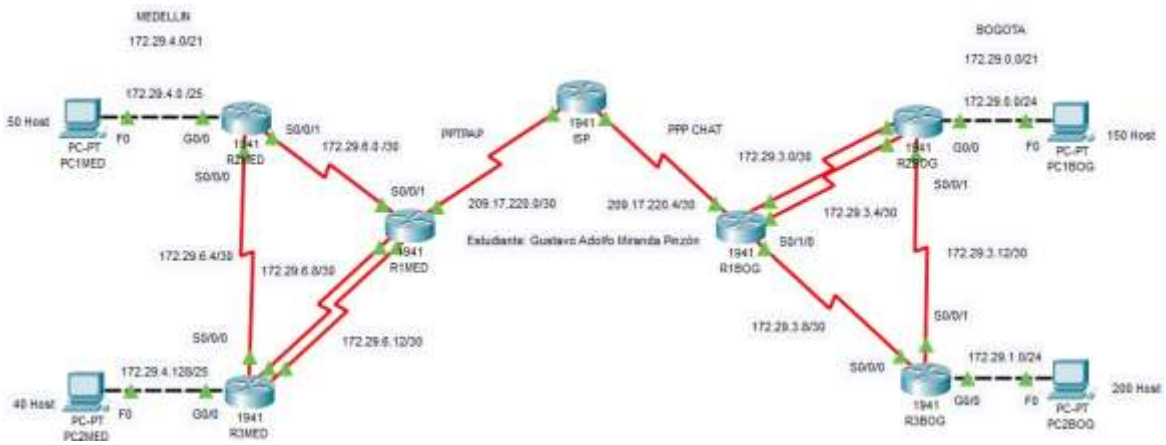
Figura 37. Configuración ip PC2BOG



Fuente: Autor.

2.9 PARTE 8: RED FINALIZADA EN CISCO PACKET TRACER

Figura 38. Red realizada en Cisco Packet Tracer



Fuente: Autor.

3 CONCLUSIONES

Con el presente trabajo se comprende la manera en cómo se configuran los dispositivos de red para que funcionen de forma correcta. Además, el uso y el significado de los Comandos iOS, los cuales son muy utilizados para configurar, diagnosticar, entre otras cosas, los dispositivos de una red. De igual manera, como se debe realizar la conexión de una red entre sus dispositivos y el diagnostico de errores de estos para dar soluciones optimas. También, se dan a conocer y se aplican, las medidas de seguridad que se deben realizar en los routers y switches para mantenerlos seguros.

Asimismo, específicamente por medio del escenario 2, se comprendió como realizar conexiones entre dispositivos de red, como también, su configuración y diagnóstico. En este caso se aplicaron comandos avanzados en routers, implementando OSPF y encapsulamiento, lo cual permite un enrutamiento óptimo y seguro entre los dispositivos.

Para finalizar, se aprende y entiende que las redes son algo muy importante en la actualidad, pues permiten el contacto en todo el mundo ya que de ellas depende la comunicación dentro de empresas, casas, etc., por tanto, es de gran relevancia que se conozca su complejidad y desarrollo, lo cual se logra en gran medida con el desarrollo del presente trabajo, lo que hace que las redes sean un elemento vital para el avance de nuestra sociedad moderna.

BIBLIOGRAFÍA

CISCO. Asignación de direcciones IP. Fundamentos de Networking, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. Exploración de la red. Fundamentos de Networking, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. Conceptos de Routing. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. DHCP. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. Enrutamiento Estático. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. Listas de control de acceso. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. OSPF de una sola área. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. Protocolos y comunicaciones de red. Fundamentos de Networking, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. SubNetting. Fundamentos de Networking, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. Soluciones de Red. Fundamentos de Networking, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. VLANs. Principios de Enrutamiento y Conmutación, 2017. {En línea}. {Consultado 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

UNAD. Principios de Enrutamiento [OVA], 2017. {En línea}. {Consultado 2020}. Disponible en https://1drv.ms/u/s!AmlJYei-NT1IhgOyjWeh6timi_Tm

ESTELA, María. ¿Qué es una red?, 2019. {En línea}. {Consultado 2020}. Disponible en https://concepto.de/red-2/

UNAD. Diseño y configuración de redes con Packet Tracer [OVA], 2017. {En línea}. {Consultado 2020}. Disponible en https://1drv.ms/u/s!AmlJYei-NT1IhgCT9VCtl_pLtPD9

UNAD. PING y TRACER como estrategia en procesos de Networking [OVA], 2017. {En línea}. {Consultado 2020}. Disponible en https://1drv.ms/u/s!AmlJYei-NT1IhgTCtKY-7F5KIRC3

UNAD. Configuración de Switches y Routers [OVA], 2017. {En línea}. {Consultado 2020}. Disponible en https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC