PRUEBA DE HABILIDADES CCNA

DIANA KATERNIE GUACA

Diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN)

JUAN CARLOS VESGA
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICA TECNOLOGIA E INGIENERIA-ECBTI
INGENIERIA DE SISTEMAS
EL BORDO CAUCA
2020

CONTENIDO

LISTA DE IMAGNES

LISTA DE TABLAS

Pg.

1. INTRODUCCIÓN

Es importante dentro de una empresa los sistemas informáticos y para ello es importante también la configuración de los mismos, es decir tener en cuenta diferentes parámetros que son importantes a la hora de tomar información relevante de la información de entrada y salida dentro de los sistemas. Para ello es importante contar con conocimientos relacionados con ,ndos como lo es Ping, tranceroute, show IP Route al igual que otros ,ndos que son importantes a la hora de tomar información de los equipos que hacen parte de una red. En el presente documento se desarrolla la actividad correspondiente a la prueba habilidades prácticas relacionadas con CCNA a partir del desarrollo de dos escenarios con sus diferentes tipologías, en el primer escenario se configura una red para que está admita conectividad a partir de los protocolos ipv4 y ipv6, la seguridad de los switches, los routing entre VLAN entre otros protocolos Qué son implementados a partir del programa packet tracer. Y se realiza lo relacionado con la inicializacion de los dispositivos, inicialización y vuelta a cargar de los routers y switch, las configuraciones de los parámetros de estos dispositivos y la verificación de la conectividad de cada uno de estos al igual que la verificación de la información de los RIP entre otros protocolos que son importantes para el desarrollo del escenario. Por otro lado en el escenario numerados se implementa lo correspondiente a una empresa que contiene sucursales distribuidas en dos ciudades de Colombia lo cual son Bogotá y Medellín y dentro de ésta Se debe administrar una red para configurar y interconectarse entre sí en cada dispositivo que forman parte de este escenario para ello puesto importante realizar la tipología de la red como la configuración del enrutamiento, deshabilitacion de los programas del protocolo RIP la verificación del mismo, la configuración de encapsulamiento y autenticación de las PPP y su respectiva configuración del dhcp y entre otros parámetros que fueron importantes Dentro de este escenario.

2. DESARROLLO DE LOS ESCENARIOS

2.1. ESCENARIO 1

2.2.10. Problema

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

Topología

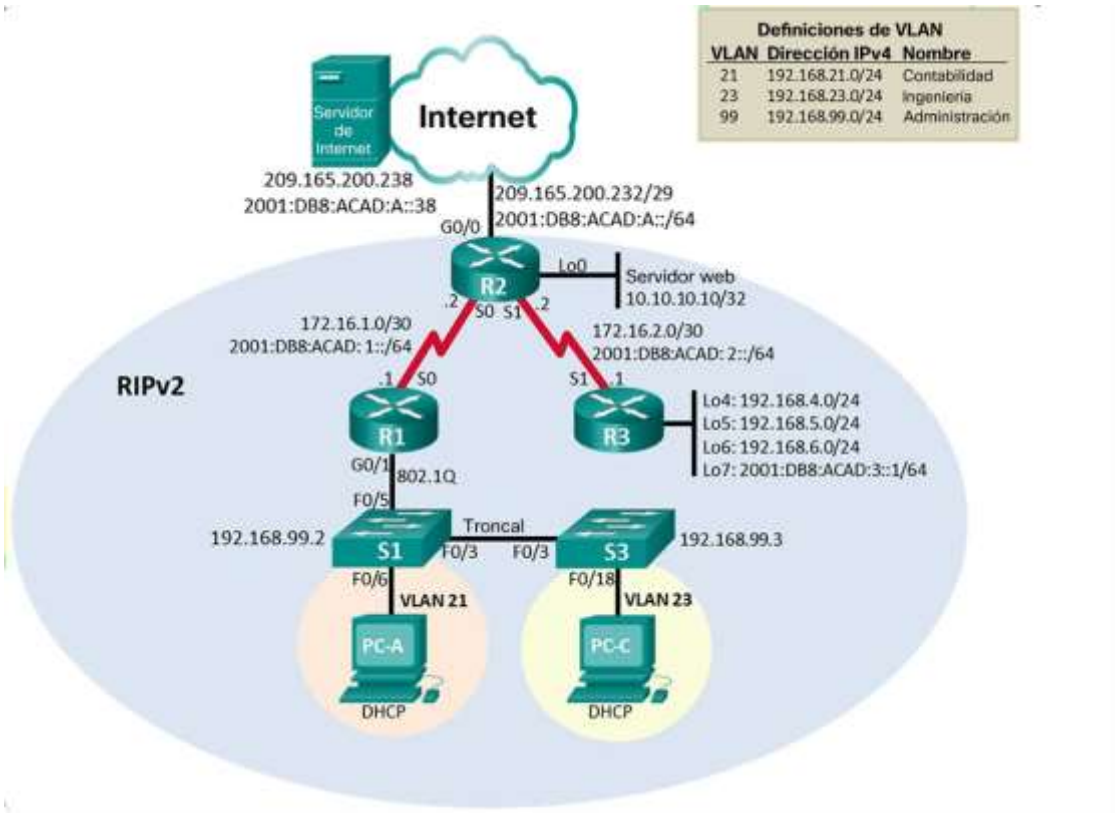

Figura 1 Topología escenario 1

2.2.11. Parte 1: Inicializar dispositivos

2.2.11.1. 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 Inicialización y volver a cargar los Reuters y los switches parte 1 escenario 1

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	erase startup-config del vlan.dat
Volver a cargar ambos switches	reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	show flash

2.2.12. Parte 2: Configurar los parámetros básicos de los dispositivos

2.2.12.1. 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 parte 2, paso 1 del escenario 1

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.230
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:2::30/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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.

2.2.12.2. Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configuración paso 1 de la parte 2, paso 2 del escenario 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
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	Service password-encyption
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

Nota: Todavía no configure G0/1.

2.2.12.3. Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4 Configurar R2 de la Parte 2, paso 1 del escenario 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
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	Service password-encyption
Habilitar el servidor HTTP	ip http server
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.

2.2.12.4. Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5 Configurar R3 de la parte 2, paso 4 del escenario 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup

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	Service password-encyption
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	

2.2.12.5. Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6 Configuración de S1 Parte 2, paso 5 de escenario 1

Elemento o tarea de configuración	*Especificación*
Desactivar la búsqueda DNS	*No ip domain lookup*
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	Service password-encyption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

2.2.12.6. Paso 6:Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7 Configuración S3 Parte 2, paso 6 de escenario 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
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	Service password-encyption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

2.2.12.7. 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 Verificación de conectividad de la red en Parte 2, paso 7 de escenario 1

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.12.2	Exitoso
R2	R3, S0/0/1	172.16.23.2	Exitoso

PC de Internet	Gateway predeterminado	209.165.200.225	Exitoso

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

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

2.2.13.1. Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9 Configuración de S1 de Parte 3, paso 1 de escenario 1

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	interface F0/6 switchport access vlan 21
Apagar todos los puertos sin usar	interface range F0/1-2, F0/4, F0/7-24, G0/1-2 shutdown

2.2.13.2. Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10 configuración de S3 de Parte 3, paso 2 de escenario 1

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	interface F0/18 switchport access vlan 23
Apagar todos los puertos sin usar	interface range F0/1-2, F0/4, F0/6-17, F0/19-24, G0/1-2 shutdown

2.2.13.3. Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 Configuración R1 de Parte 3, paso 3 de escenario 1

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	interface g0/1 no shutdown

2.2.13.4. 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 Verificación de conectividad de Parte 3, paso 4 de escenario 1

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

2.2.14. Parte 4:Configurar el protocolo de routing dinámico RIPv2

2.2.14.1. Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 Configuración de RIPv2 en el R1 de Parte 4, paso 1 de escenario 1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router rip version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.

Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary

2.2.14.2. Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14 Configuración de RIPv2 en el R2 de Parte 4, paso 2 de escenario 1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router rip version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	passive-interface lo0
Desactive la sumarización automática.	no auto-summary

2.2.14.3. Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15 Configuración de RIPv3 en el R1 de Parte 4, paso 3 de escenario 1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router rip version 2
Anunciar redes IPv4 conectadas directamente	network 172.16.0.0 network 192.168.4.0 network 192.168.5.0 network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface lo4 passive-interface lo5 passive-interface lo6
Desactive la sumarización automática.	no auto-summary

2.2.14.4. 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 Verificación de información de RIP de Parte 4, paso de escenario 1

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
¿Qué comando muestra solo las rutas RIP?	show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show run | section router RIP

2.2.15. Parte 5: Implementar DHCP y NAT para IPv4

2.2.15.1. 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 En parte 3, paso 1.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	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	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

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

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configuración R2 En parte 3, paso 2

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	ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	interface lo0 ip nat inside interface g0/0 ip nat outside
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: **209.165.200.225 – 209.165.200.228**
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

2.2.15.3. 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 en parte 3, paso 2

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	**C:\>ipconfig /all** **FastEthernet0 Connection:(default port)** **Connection-specific DNS Suffix..:** **Physical Address..... 0090.213B.E610** **Link-local IPv6 Address.....: FE80::290:21FF:FE3B:E610** **IP Address. .....: 192.168.21.21** **Subnet Mask. ..... : 255.255.255.0** **Default Gateway ..... : 192.168.21.1** **DNS Servers .....: 10.10.10.10** **DHCP Servers. .....: 192.168.21.1** **DHCPv6 Client DUID.....: 00-01-00 01-A2-07-32-C5-00-90-21-3B-E6-10**
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	**C:\>ipconfig /all** **FastEthernet0 Connection:(default port)** **Connection-specific DNS Suffix..:** **Physical Address..... 0004.9A32.A8C5** **Link-local IPv6 Address.....: FE80::204:9AFF:FE32:A8C5** **IP Address. .....: 192.168.23.21** **Subnet Mask. ..... : 255.255.255.0** **Default Gateway ..... : 192.168.23.1** **DNS Servers .....: 10.10.10.10** **DHCP Servers. .....: 192.168.23.1** **DHCPv6 Client DUID.....: 00-01-00-01-CE-16-91-9B-00-04-9A-32-A8-C5**
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	**C:\>ping 192.168.23.21** **Pinging 192.168.23.21 with 32 bytes of data:** **Request timed out.** **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 = 3, Lost = 1 (25% 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 (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** *y la contraseña* **cisco12345**	El navegador debe mostrar a ventana de inicio de sesión que solicita usuario y contraseña, packet tracer no soporta este procedimiento.

2.2.16. Parte 6: Configurar NTP

Tabla 20 Configuración de NTP en parte 6

Elemento o tarea de configuración	*Especificación*
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 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.	ntp update-calendar
Verifique la configuración de NTP en R1.	*R1#show ntp associations* *address ref clock st when poll reach delay offset disp* **~172.16.1.2 127.127.1.1 5 2 64 1 4.00 1.00 0.00* ** sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured*

2.2.17. Parte 7: Configurar y verificar las listas de control de acceso

(ACL)

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

Tabla 21 Restricción de acceso a linea VTY y R2 de Parte 7, paso 1

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	line vty 0 4 access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172·16·1·2 Trying 172·16·1·2 …OpenUnauthorized Access is Prohibited!^ User Access Verification Password: R2>en Password : R2#

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

Tabla 22 Introducir el comando de CLI en Parte 7, paso 2.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-lists
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección	show ip interface

en que se aplica?	
¿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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translations *

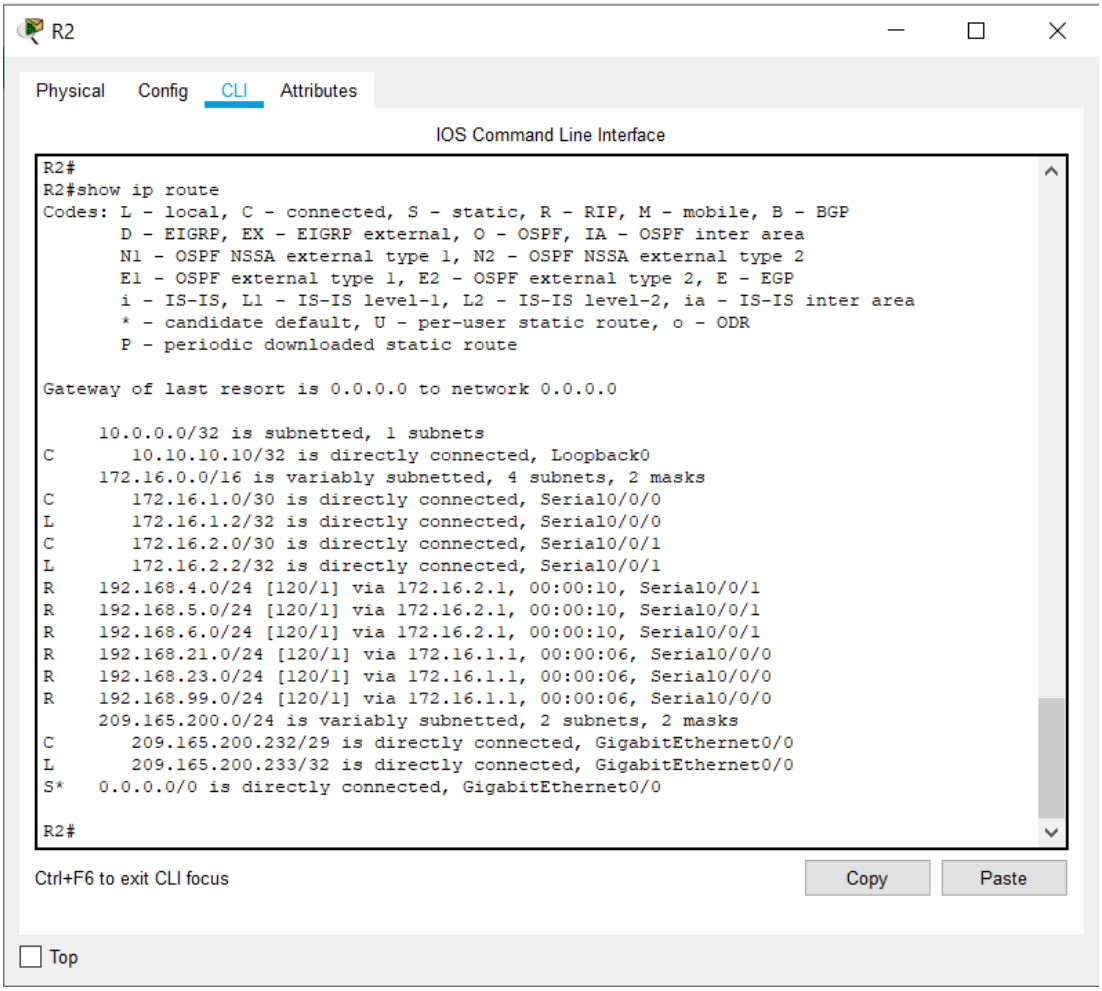

Figura 2 Verificación en simulador de escenario 1

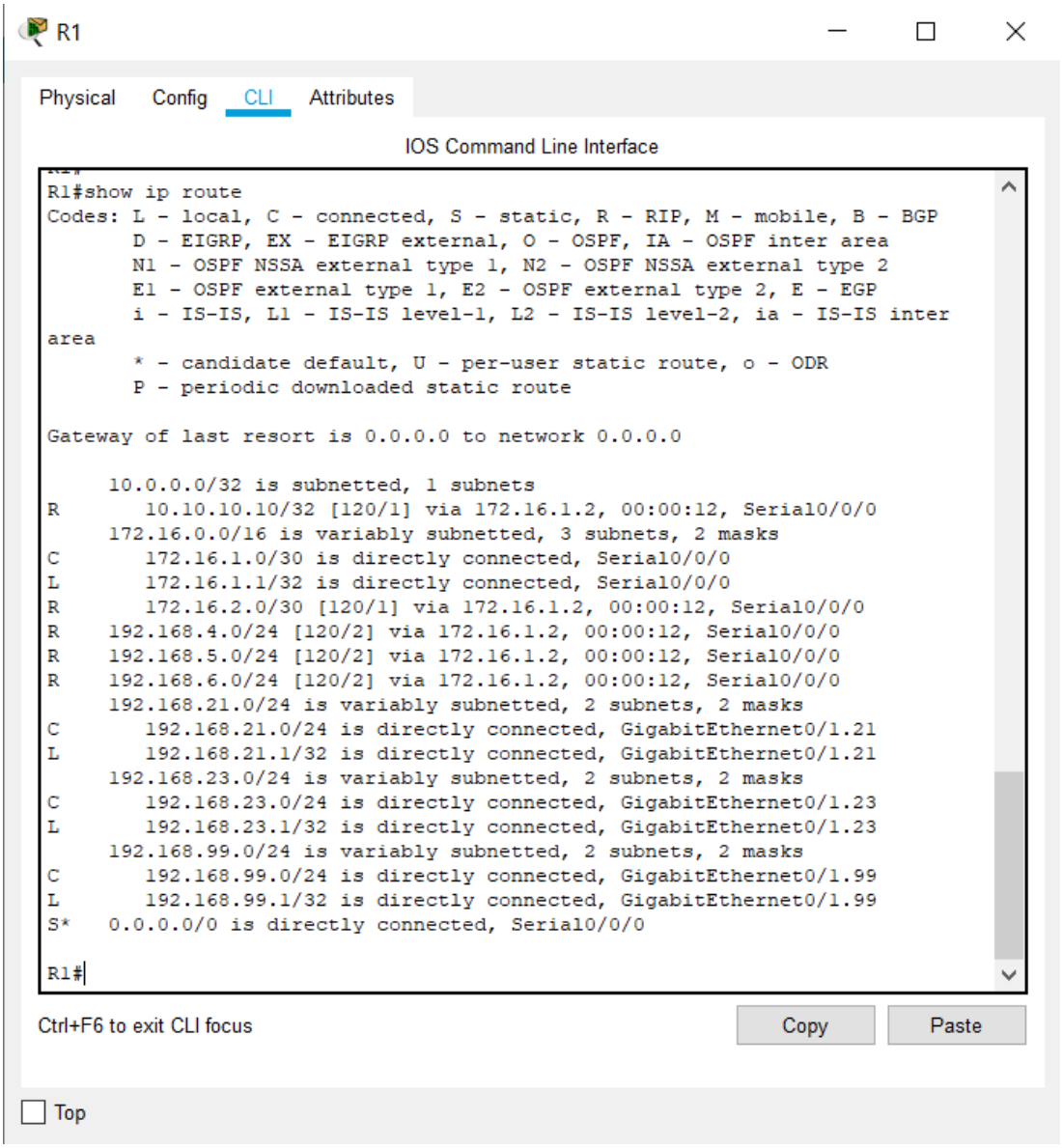

Figura 3 Verificación en simulador de escenario 1

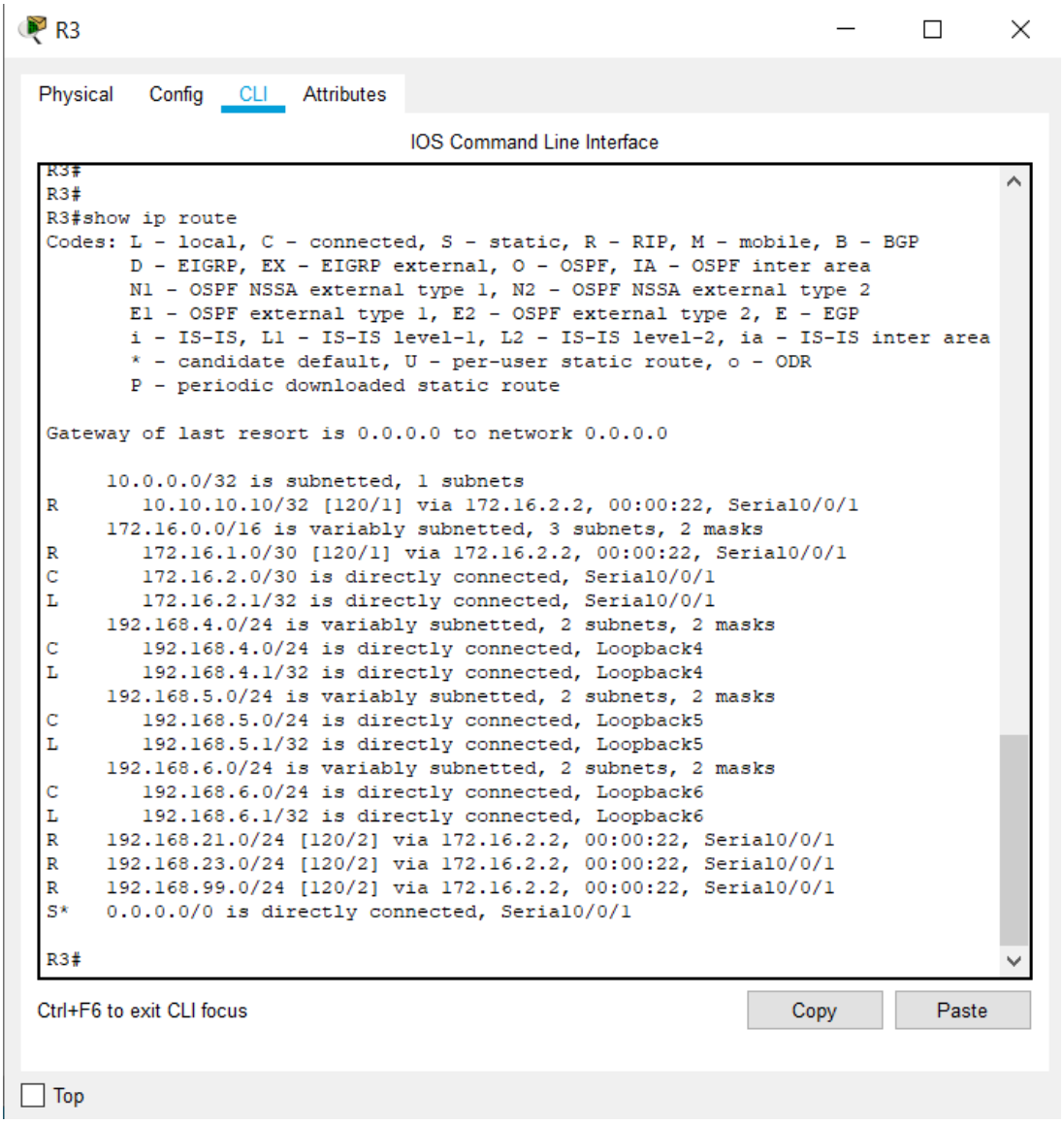

Figura 4 Verificación en simulador de escenario 1

2.2. 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.

2.2.18. Topología de red

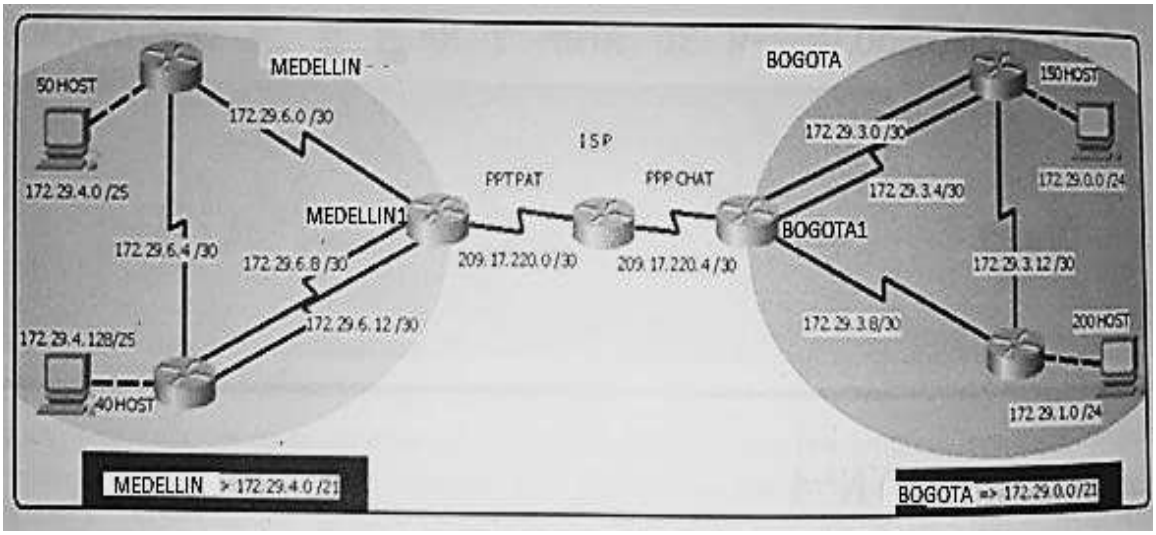

Figura 5 Topología de red del escenario 2

Este escenario plantea el uso de RIP 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.

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).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

2.2.19. Parte 1: Configuración del enrutamiento

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

2.2.20. 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 RIP.
- Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
- El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

2.2.21. Parte 3: Deshabilitar la propagación del protocolo RIP.

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

Tabla 23 Des habilitación de la propagación del protocolo RIP en escenario 2

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

2.2.22. Parte 4: Verificación del protocolo RIP.

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

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

2.2.23. Parte 5: Configurar encapsulamiento y autenticación PPP.

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.

2.2.24. Parte 6: Configuración de PAT.

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.

2.2.25. Parte 7: Configuración del servicio DHCP.

- 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.
- 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.

A continuación se muestra el proceso que se debe seguir para armar la topología del ESCENARIO número 2, sabiendo antes que nada los requerimientos de cada uno de estos dispositivos en lo que tiene que ver con la cantidad y tipo de interfaces disponibles:

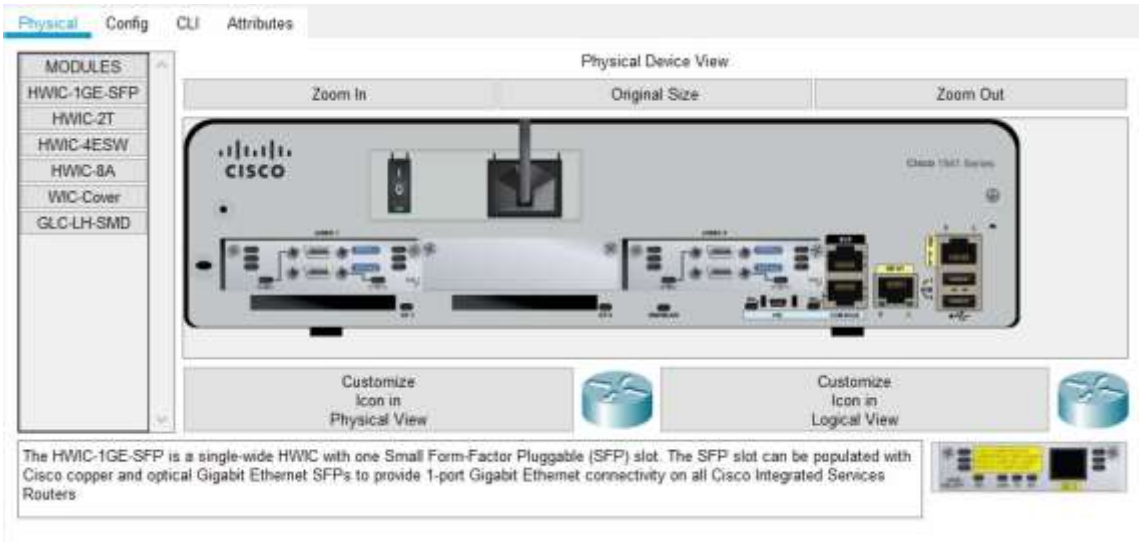

Figura 6 Proceso para armar topología del escenario 2

Figura 7 Proceso para armar topología del escenario 2

Figura 8 Dispositivo para el proceso de armar topología del escenario 2

Como conocemos que dispositivos vamos a emplear dentro de la topología podemos proceder a realizar el cableado de los mismos empleando la tecnología adecuada para este caso:

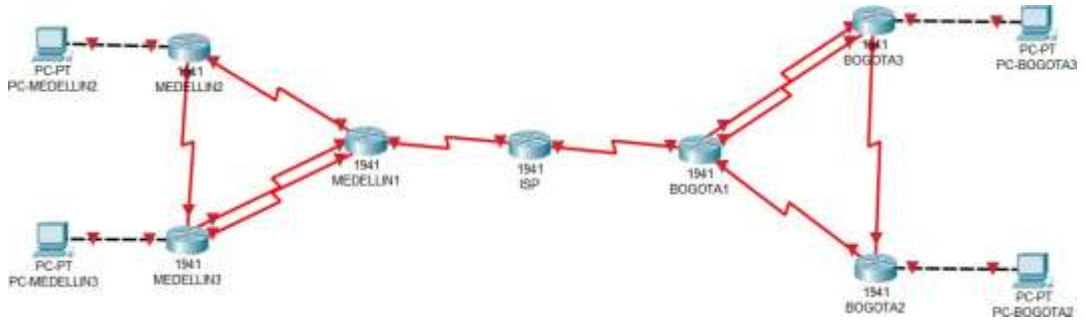

Figura 9 Conexiones de la topología del escenario 2

Debemos proceder a marcar cada uno de los dispositivos e interface que hacen parte del a red junto con las respectivas direcciones IP, esto con el fin de tener un control mucho más adecuado de cada uno de los pasos hechos hasta el momento.

Recordemos ante que nada que el ejercicio nos suministra las direcciones de red que vamos a emplear en cada uno de los rangos a configurar, estos parámetros los encontramos en la figura 5.

Esta información es la que nos sirve de base para poder iniciar nuestro proceso de configuración y asignación de direcciones IP a cada una de las interfaces o dispositivos:

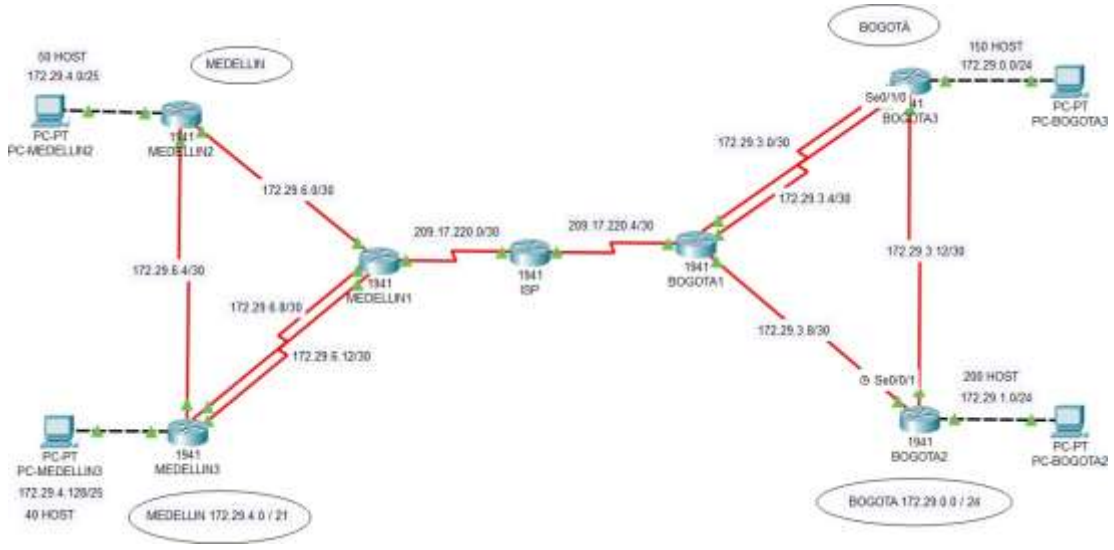

Figura 10 Diseño de la topología de red del escenario 2

2.2.25.1. Tabla de Direccionamiento

Procedemos entonces a formular nuestra tabla de direccionamiento:

Comenzamos identificando cada uno de los rangos de las diferentes SUBREDES.

Tabla 24 Direccionamiento del parte 7 de escenario 2

Dir. red	**Primera IP**	**Ultma IP**	**Broadcast.**	**Mascara.**
172.29.4.0/25	172.29.4.1	172.29.4.126	172.29.4.0	255.255.255.128
172.29.4.128/25	172.29.4.129	172.29.4.254	172.29.4.255	255.255.255.128
172.29.6.0/30	172.29.6.1	172.29.6.2	172.29.6.3	255.255.255.252
172.29.6.4/30	172.29.6.5	172.29.6.6	172.29.6.7	255.255.255.252
172.29.6.8/30	172.29.6.9	172.29.6.10	172.29.6.11	255.255.255.252
172.29.6.12/30	172.29.6.13	172.29.6.14	172.29.6.15	255.255.255.252
172.29.0.0/24	172.29.0.1	172.29.0.254	172.29.0.255	255.255.255.0
172.29.1.0/24	172.29.1.1	172.29.1.254	172.29.1.255	255.255.255.0
172.29.3.0/30	172.29.3.1	172.29.3.2	172.29.3.3	255.255.255.252
172.29.3.4/30	172.29.3.5	172.29.3.6	172.29.3.7	255.255.255.252
172.29.3.8/30	172.29.3.9	172.29.3.10	172.29.3.11	255.255.255.252

172.29.3.12/30	172.29.3.13	172.29.3.14	172.29.3.15	255.255.255.252
209.17.220.0/30	209.17.220.1	209.17.220.2	209.17.220.3	255.255.255.252
209.17.220.4/30	209.17.220.5	209.17.220.6	209.17.220.7	255.255.255.252

Ya conocemos el rango que le corresponde a cada una de las SUBREDES, es por esto que podemos proceder a asignar la dirección exacta a cada dispositivo:

Tabla 25 Direccionamiento y asignación exacta del parte 7 de escenario 2

Dispositivo	Interface	Dirección IP	Máscara de Subred	Puerta de Enlace
ISP	S0/0/0	209.165.200.1	255.255.255.252	
	S0/0/1	209.165.200.5	255.255.255.252	
MEDELLIN1	S0/0/0	209.165.200.2	255.255.255.252	
	S0/0/1	172.29.6.1	255.255.255.252	
	S0/1/0	172.29.6.9	255.255.255.252	
	S0/1/1	172.29.6.13	255.255.255.252	
MEDELLIN2	S0/0/0	172.29.6.2	255.255.255.252	
	S0/0/1	172.29.6.5	255.255.255.252	
	G0/0	172.29.4.1	255.255.255.128	
MEDELLIN3	S0/0/0	172.29.6.10	255.255.255.252	
	S0/0/1	172.29.6.14	255.255.255.252	
	S0/1/0	172.29.6.6	255.255.255.252	

	G0/0	172.29.4.129	255.255.255.128	
BOGOTA1	S0/0/0	209.165.200.6	255.255.255.252	
	S0/0/1	172.29.3.9	255.255.255.252	
	S0/1/0	172.29.3.1	255.255.255.252	
	S0/1/1	172.29.3.5	255.255.255.252	
BOGOTA2	S0/0/0	172.29.3.10	255.255.255.252	
	S0/0/1	172.29.3.13	255.255.255.252	
	G0/0	172.29.1.1	255.255.255.0	
BOGOTA3	S0/0/0	172.29.3.2	255.255.255.252	
	S0/0/1	172.29.3.6	255.255.255.252	
	S0/1/0	172.29.3.14	255.255.255.252	
	G0/0	172.29.0.1	255.255.255.0	
PC-MEDELLIN2	F0/0	DHCP	DHCP	DHCP
PC-MEDELLIN3	F0/0	DHCP	DHCP	DHCP
PC-BOGOTA2	F0/0	DHCP	DHCP	DHCP
PC-BOGOTA3	F0/0	DHCP	DHCP	DHCP

Podemos proceder a configurar, este proceso se lo detalla a continuación:

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

2.2.25.2. Router ISP:

```
hostname ISP
no ip domain-lookup
service password-encryption
enable secret class
banner motd %Acceso Restringido%
ip domain-name cisco.com
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

MEDELLIN1

```
hostname MEDELLIN1
no ip domain-lookup
service password-encryption
enable secret class
banner motd %Acceso Restringido%
ip domain-name cisco.com
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

MEDELLIN2

```
hostname MEDELLIN2
no ip domain-lookup
service password-encryption
enable secret class
banner motd %Acceso Restringido%
ip domain-name cisco.com
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

MEDELLIN3

```
hostname MEDELLIN3
no ip domain-lookup
service password-encryption
enable secret class
banner motd %Acceso Restringido%
ip domain-name cisco.com
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

BOGOTA1

```
hostname BOGOTA1
no ip domain-lookup
service password-encryption
enable secret class
banner motd %Acceso Restringido%
ip domain-name cisco.com
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

BOGOTA2

```
hostname BOGOTA2
no ip domain-lookup
service password-encryption
enable secret class
banner motd %Acceso Restringido%
ip domain-name cisco.com
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

BOGOTA3

```
hostname BOGOTA3
no ip domain-lookup
service password-encryption
enable secret class
banner motd %Acceso Restringido%
ip domain-name cisco.com
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

2.2.25.3. Configuración de direcciones IP:
2.2.25.4. ISP

```
Interface seriales ISP

interface Serial0/0/0
 ip address 209.17.220.1 255.255.255.252
 clock rate 4000000
 no shutdown

interface Serial0/0/1
 ip address 209.17.220.5 255.255.255.252
```

```
clock rate 4000000
no shutdown
```

MEDELLIN1

```
Interfaces seriales MEDELLIN 1:

interface Serial0/0/0
 ip address 209.17.220.2 255.255.255.252
 no shutdown

interface Serial0/0/1
 ip address 172.29.6.1 255.255.255.252
 clock rate 4000000
 no shutdown

interface Serial0/1/0
 ip address 172.29.6.9 255.255.255.252
 clock rate 4000000
 no shutdown

interface Serial0/1/1
 ip address 172.29.6.13 255.255.255.252
 clock rate 4000000
 no shutdown
```

MEDELLIN2

Interface seriales MEDELLIN 2:

```
interface GigabitEthernet0/0
 ip address 172.29.4.1 255.255.255.128
 no shutdown

interface Serial0/0/0
 ip address 172.29.6.2 255.255.255.252
 no shutdown

interface Serial0/0/1
 ip address 172.29.6.5 255.255.255.252
 clock rate 4000000
 no shutdown
```

MEDELLIN3

Interface bseriales MEDELLÍN 2:

```
interface GigabitEthernet0/0
 ip address 172.29.4.129 255.255.255.128
 no shutdown

interface Serial0/0/0
 ip address 172.29.6.10 255.255.255.252
 no shutdown

interface Serial0/0/1
 ip address 172.29.6.14 255.255.255.252
 no shutdown
```

```
interface Serial0/1/0
 ip address 172.29.6.6 255.255.255.252
 no shutdown
```

BOGOTA1

```
Interafce seriales BOGOTA 1:

interface Serial0/0/0
 ip address 209.17.220.6 255.255.255.252
 no shutdown

interface Serial0/0/1
 ip address 172.29.3.9 255.255.255.252
 no shutdown

interface Serial0/1/0
 ip address 172.29.3.1 255.255.255.252
 clock rate 4000000
 no shutdown

interface Serial0/1/1
 ip address 172.29.3.5 255.255.255.252
 no shutdown
```

BOGOTA2

```
Interface seriales BOGOTA 2:
```

```
interface GigabitEthernet0/0
 ip address 172.29.1.1 255.255.255.0
 no shutdown

interface Serial0/0/0
 ip address 172.29.3.10 255.255.255.252
 no shutdown

interface Serial0/0/1
 ip address 172.29.3.13 255.255.255.252
 clock rate 4000000
 no shutdown
```

BOGOTA3

```
Intrefaces seriales BOGOTA 3:

interface GigabitEthernet0/0
 ip address 172.29.0.1 255.255.255.0
 no shutdown

interface Serial0/0/0
 ip address 172.29.3.2 255.255.255.252
 no shutdown

interface Serial0/0/1
 ip address 172.29.3.6 255.255.255.252
 no shutdown

interface Serial0/1/0
```

```
ip address 172.29.3.14 255.255.255.252
no shutdown
```

2.2.25.5. Conexión fisica de los equipos con base en la topología de red

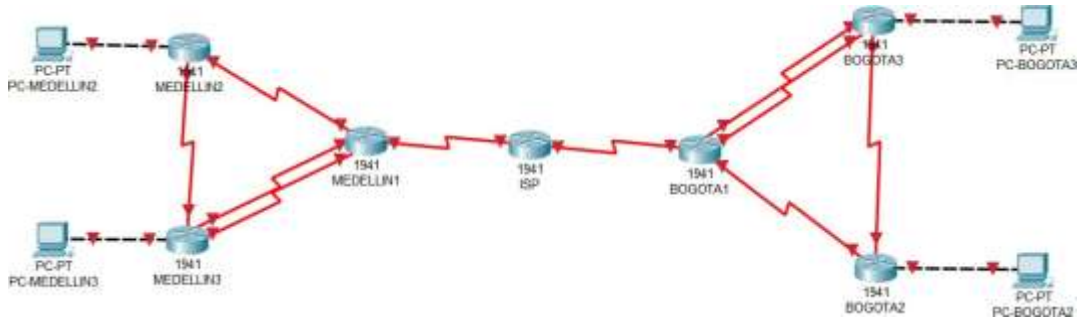

Figura 11 Conexión física de los equipos de Escenario 2

Luego de configurar las diferentes interfaces cada uno de los indicadores de los dispositivos cambia de color:

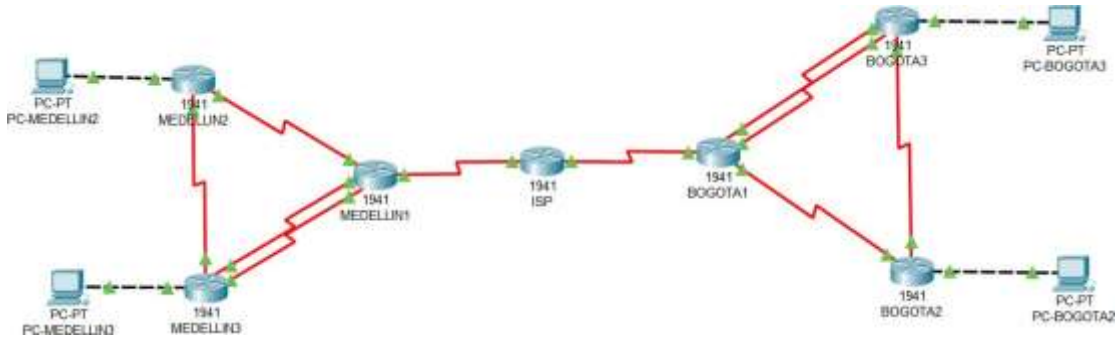

Figura 12 Configuración de las interface de escenario 2

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

2.2.25.6. Configuración del enrutamiento

Procedemos a configurar el enrutamiento RIP V2, el cual posibilita el intercambio de paquetes entre las diferentes subredes, no olvidemos algo importante es que debemos desactivar la autosumarización con el fin de tener las rutas de manera independiente:

Debemos activar el protocolo de enrutamiento en cada uno de los router, y ademas indicar que rutas se van a propagar:

Tabla 26 Configurar el enrutamiento RIP V2 PARA Medellin1 a Mefdellin2

MEDELLIN1 router rip version 2 network 172.29.0.0 no auto-summary	MEDELLIN2 router rip version 2 network 172.29.0.0 no auto-summary
MEDELLIN3 router rip version 2 network 172.29.0.0 no auto-summary	BOGOTA1 router rip version 2 network 172.29.0.0 no auto-summary
BOGOTA2 router rip version 2 network 172.29.0.0 no auto-summary	BOGOTA3 router rip version 2 network 172.29.0.0 no auto-summary

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 RIP.

Tabla 27 configurar el enrutamiento RIP V2 PARA Medellin1y Bogota1 del escenario 2

MEDELLIN1	BOGOTA1

ip route 0.0.0.0 0.0.0.0 209.17.220.1 router rip default-information originate	ip route 0.0.0.0 0.0.0.0 209.17.220.5 router rip default-information originate

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

ip route 172.29.4.0 255.255.252.0 209.17.220.2

ip route 172.29.0.0 255.255.252.0 209.17.220.6

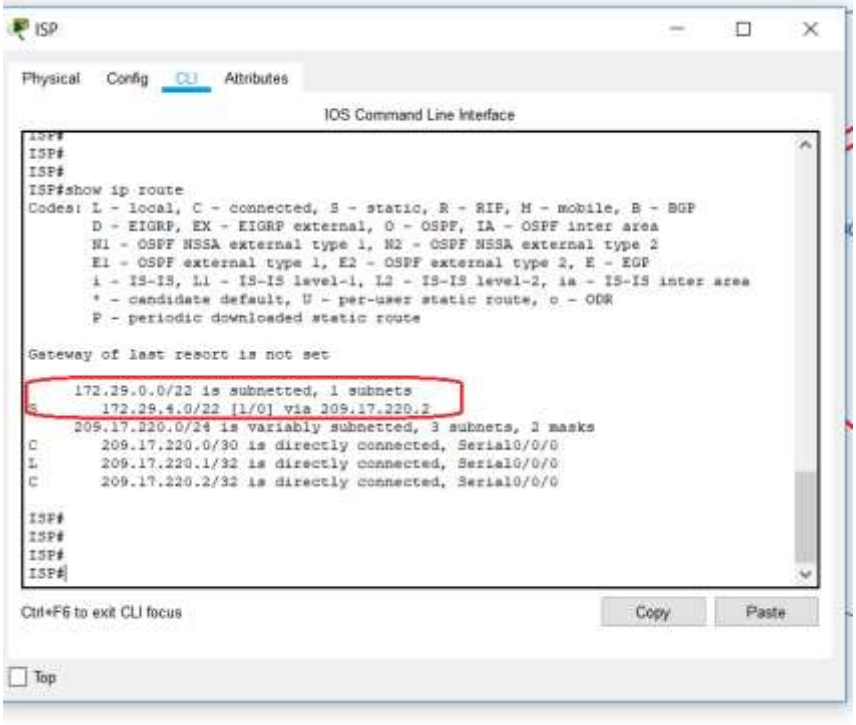

Figura 13 Ruta estática de Router ISP para cada red interna del escenario 2

2.2.26. Parte 2: Tabla de Enrutamiento.

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

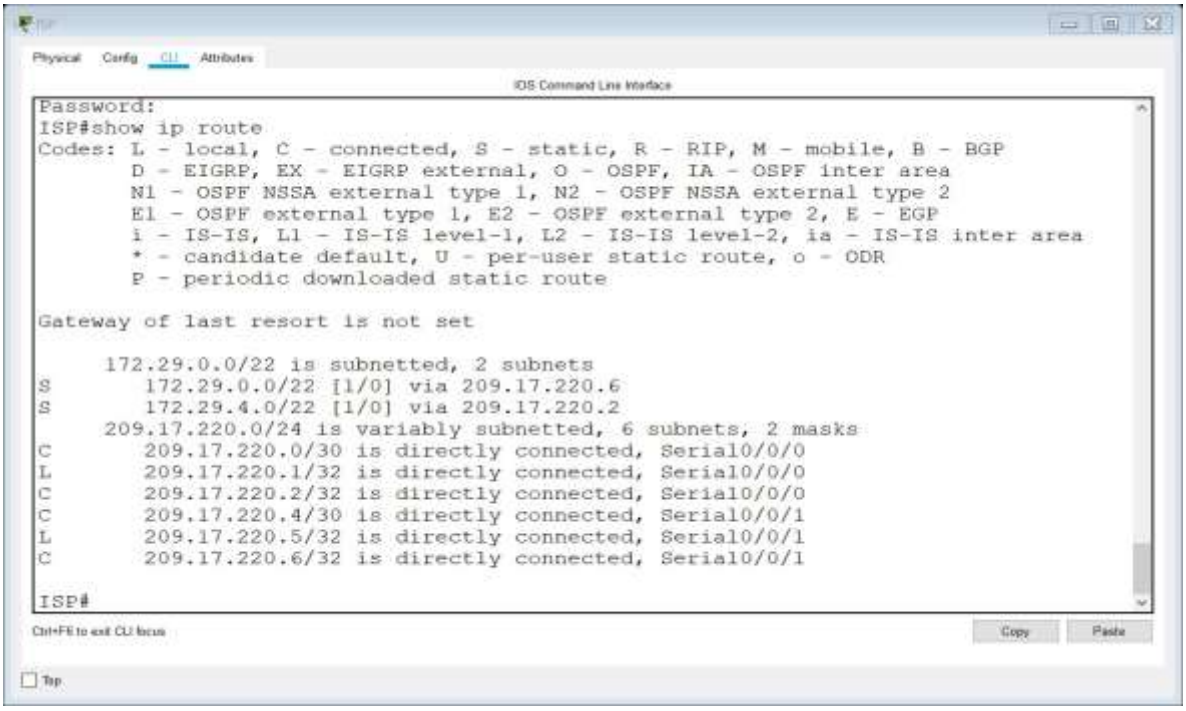

Figura 14 Comprobar redes y rutas en escenario 2

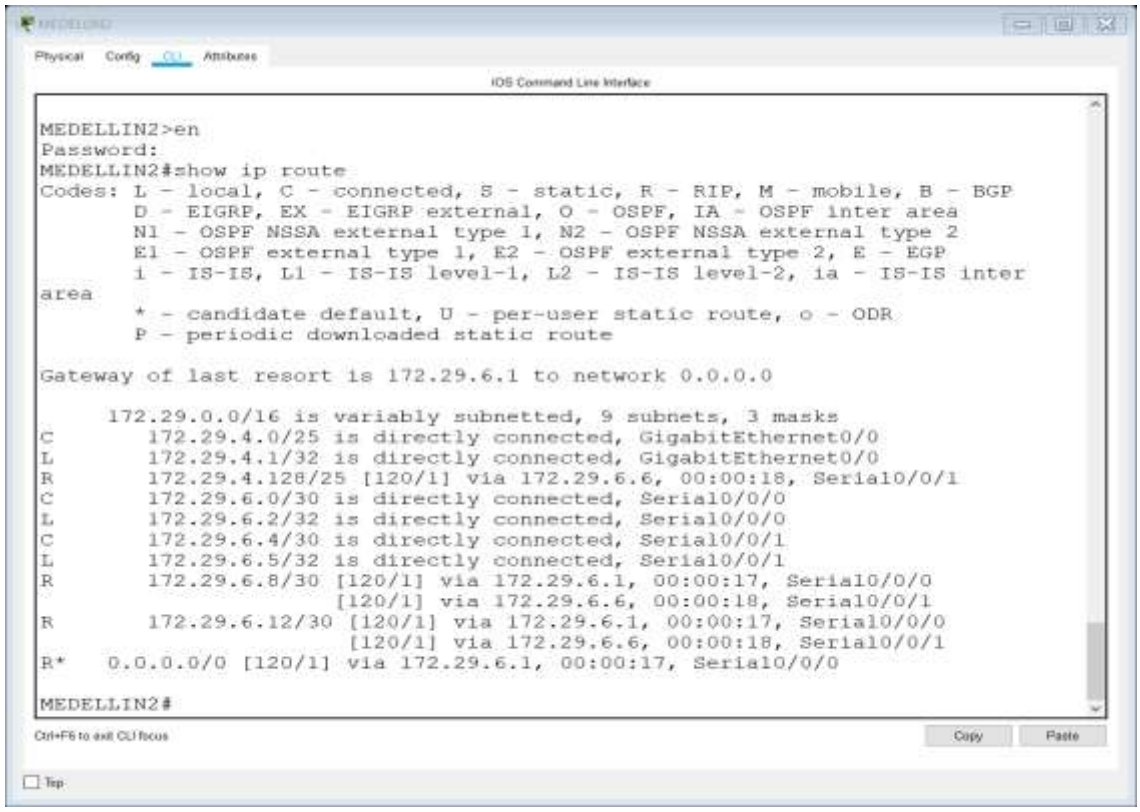

Figura 15 Comprobación redes y rutas en escenario 2

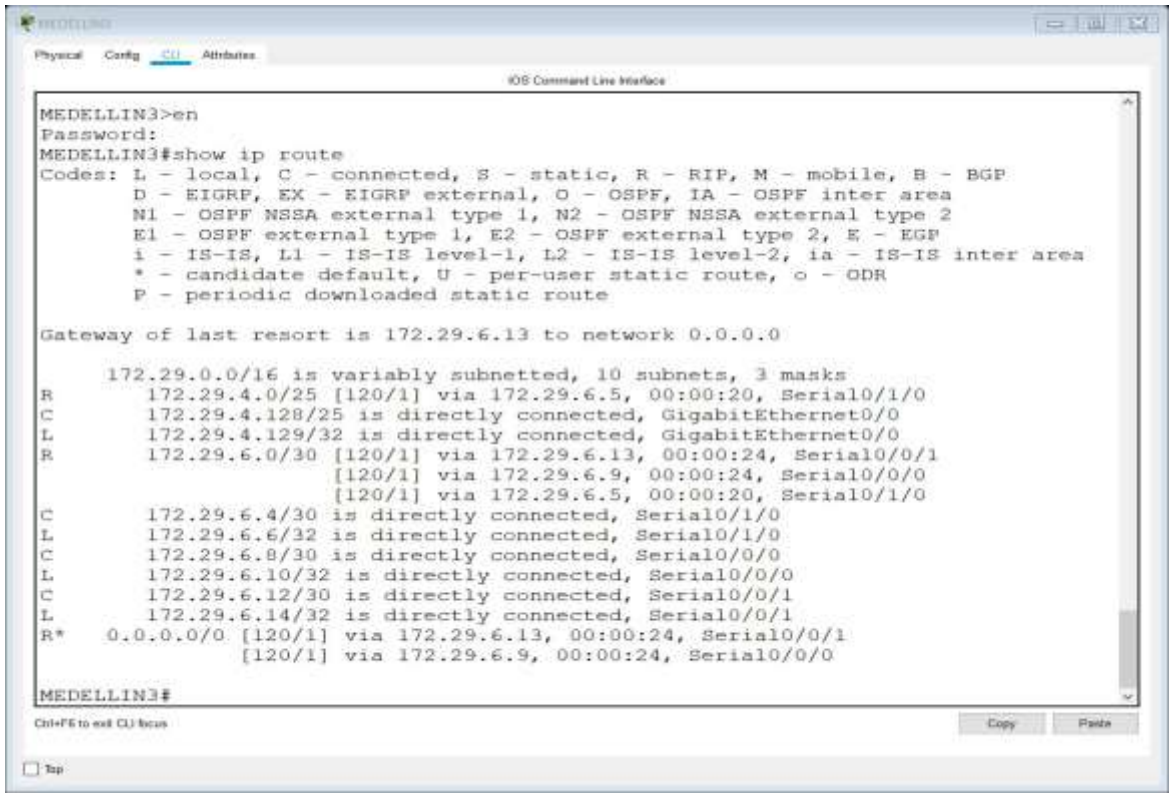

Figura 16 Comprobar redes y rutas en escenario 2

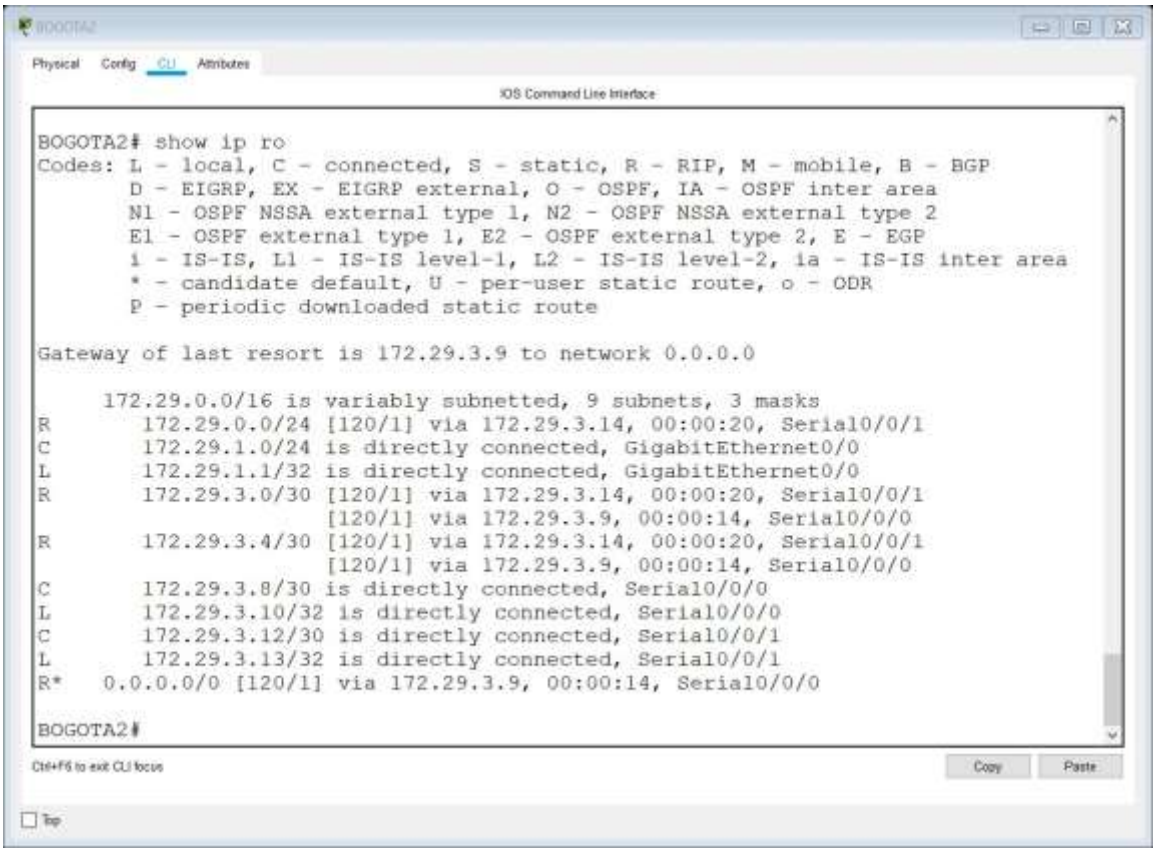

Figura 17 Comprobar redes y rutas en escenario 2

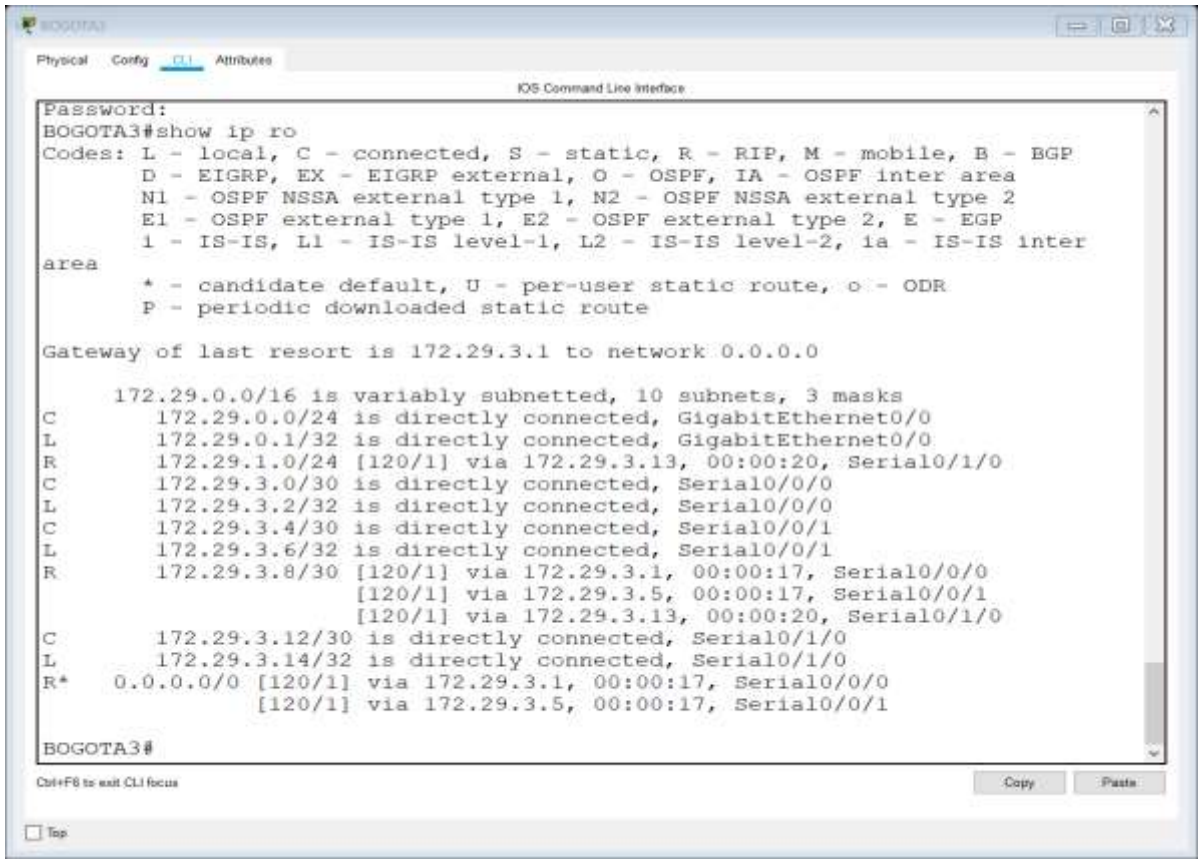

Figura 18 Comprobar redes y rutas en escenario 2

Con la aplicación del comando anterior podemos verificar que cada uno de los routers cuenta con un camino que le permite llegar a las diferentes subredes:

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 RIP.

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

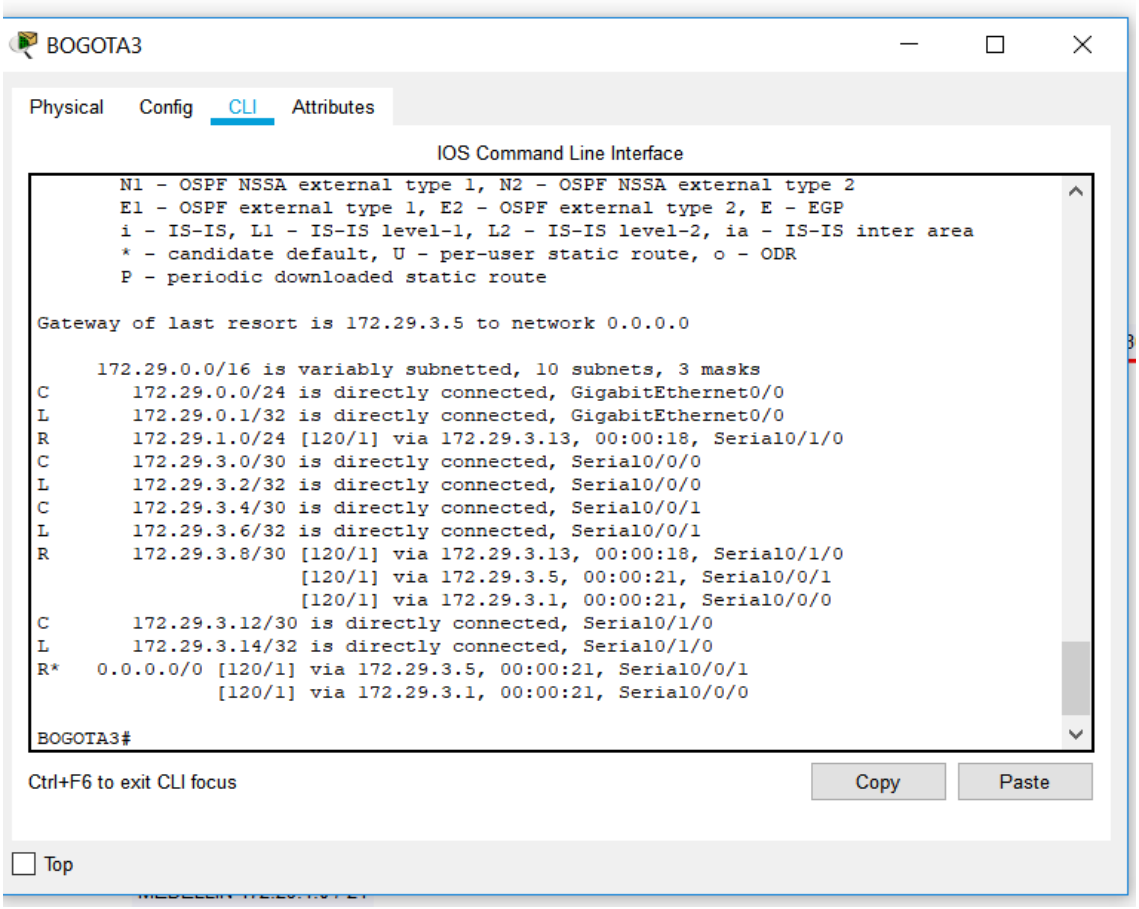

Figura 19 Comprobar redes y rutas en escenario 2

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

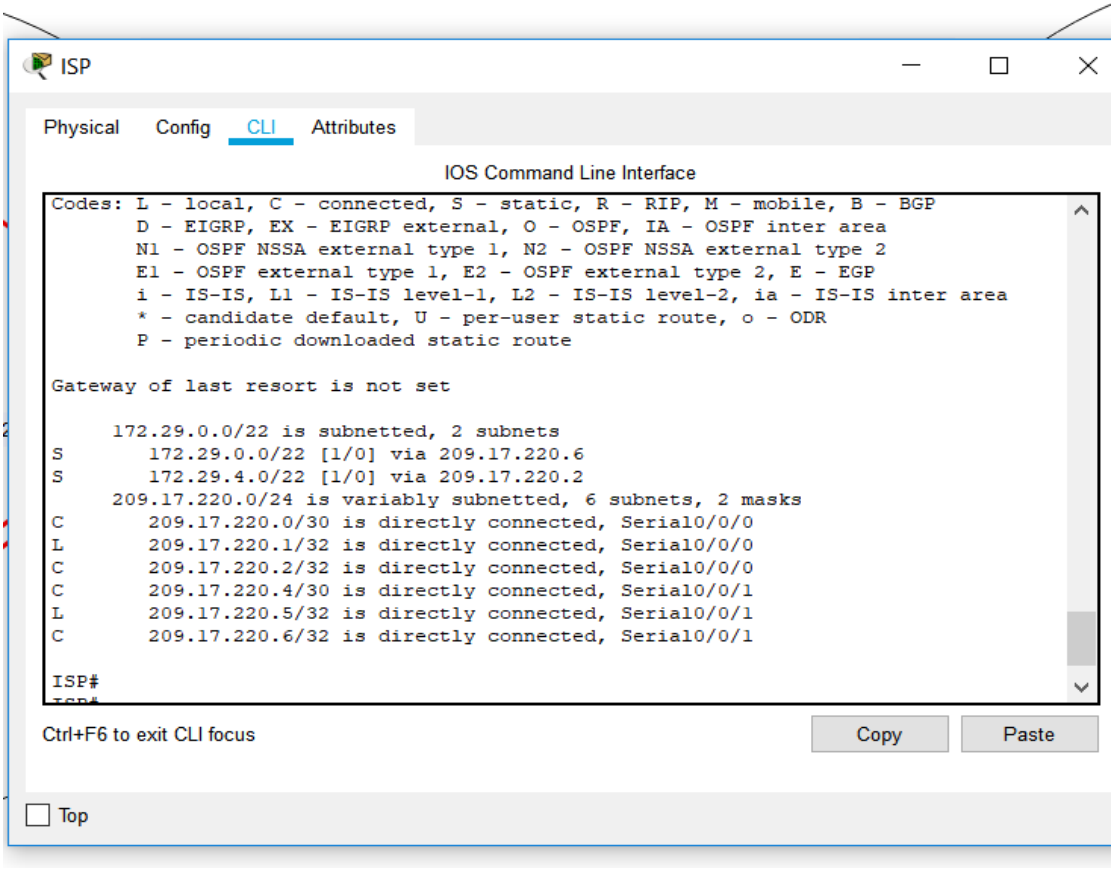

Figura 20 Comprobar redes y rutas en escenario 2

2.2.27. Parte 3: Deshabilitar la propagación del protocolo RIP.

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

Tabla 28 Des habilitación de la propagación del protocolo RIP, parte 3 del escenario 2

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

A continuación se muestra el comendo que debemos aplicar por cada una del as interfaces.

Tabla 29 Comando a implementar deshabilitar la propagación del protocolo RIP

MEDELLIN1 router rip passive-interface Serial0/0/0	MEDELLIN2 router rip passive-interface GigabitEthernet0/0
MEDELLIN3 router rip passive-interface GigabitEthernet0/0	BOGOTA1 router rip passive-interface Serial0/0/0
BOGOTA2 router rip passive-interface GigabitEthernet0/0	BOGOTA3 router rip passive-interface GigabitEthernet0/0

2.2.28. Parte 4: Verificación del protocolo RIP.

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

```
S*   0.0.0.0/0 [1/0] via 209.17.220.1

MEDELLIN1# show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 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
  Serial0/0/1           2     2
  Serial0/1/0           2     2
  Serial0/1/1           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     172.29.0.0
Passive Interface(s):
     Serial0/0/0
Routing Information Sources:
     Gateway         Distance      Last Update
     172.29.6.2           120      00:00:19
     172.29.6.14          120      00:00:18
     172.29.6.10          120      00:00:18
Distance: (default is 120)
MEDELLIN1#
```

Figura 21 Verificación del protocolo RIP, parte 4 escenario 2.

```
                     [120/1] via 172.29.6.6, 00:00:18, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:17, Serial0/0/0

MEDELLIN2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 4 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
  Serial0/0/1           2     2
  Serial0/0/0           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     172.29.0.0
Passive Interface(s):
     GigabitEthernet0/0
Routing Information Sources:
     Gateway         Distance      Last Update
     172.29.6.1           120      00:00:01
     172.29.6.6           120      00:00:01
Distance: (default is 120)
MEDELLIN2#
```

Figura 22 Verificación del protocolo RIP, parte 4 escenario 2.

```
MEDELLIN3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 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
  Serial0/0/1           2     2
  Serial0/0/0           2     2
  Serial0/1/0           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     172.29.0.0
Passive Interface(s):
     GigabitEthernet0/0
Routing Information Sources:
     Gateway         Distance      Last Update
     172.29.6.13           120      00:00:19
     172.29.6.9            120      00:00:19
     172.29.6.5            120      00:00:14
Distance: (default is 120)
MEDELLIN3#
```

Figura 23 Verificación del protocolo RIP, parte 4 escenario 2.

```
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#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 14 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
  Serial0/0/1           2     2
  Serial0/1/0           2     2
  Serial0/1/1           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     172.29.0.0
Passive Interface(s):
     Serial0/0/0
Routing Information Sources:
     Gateway         Distance      Last Update
     172.29.3.2            120      00:00:17
     172.29.3.6            120      00:00:17
     172.29.3.10           120      00:00:21
Distance: (default is 120)
BOGOTA1#
```

Figura 24 Verificación del protocolo RIP, parte 4 escenario 2.

```
R*   0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:14, Serial0/0/0

BOGOTA2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 13 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
  Serial0/0/1           2     2
  Serial0/0/0           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     172.29.0.0
Passive Interface(s):
     GigabitEthernet0/0
Routing Information Sources:
     Gateway         Distance      Last Update
     172.29.3.9           120      00:00:06
     172.29.3.14          120      00:00:08
Distance: (default is 120)
BOGOTA2#
```

Figura 25 Verificación del protocolo RIP, parte 4 escenario 2.

```
              [120/1] via 172.29.3.5, 00:00:17, Serial0/0/1

BOGOTA3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 0 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
  Serial0/0/1           2     2
  Serial0/1/0           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
     172.29.0.0
Passive Interface(s):
     GigabitEthernet0/0
Routing Information Sources:
     Gateway         Distance      Last Update
     172.29.3.1           120      00:00:26
     172.29.3.5           120      00:00:26
     172.29.3.13          120      00:00:07
Distance: (default is 120)
BOGOTA3#
```

Figura 26 Verificación del protocolo RIP, parte 4 escenario 2.

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

```
     172.29.6.10           120      00:00:18
Distance: (default is 120)
MEDELLIN1#show ip route rip
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.4.0/25 [120/1] via 172.29.6.2, 00:00:10, Serial0/0/1
R       172.29.4.128/25 [120/1] via 172.29.6.14, 00:00:21, Serial0/1/1
                        [120/1] via 172.29.6.10, 00:00:21, Serial0/1/0
R       172.29.6.4/30 [120/1] via 172.29.6.2, 00:00:10, Serial0/0/1
                      [120/1] via 172.29.6.14, 00:00:21, Serial0/1/1
                      [120/1] via 172.29.6.10, 00:00:21, Serial0/1/0
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks

MEDELLIN1#
```

Figura 27 Verificación y documentación la base de datos de RIP de cada Reuter

```
     172.29.6.1            120      00:00:01
     172.29.6.6            120      00:00:01
Distance: (default is 120)
MEDELLIN2#show ip route rip
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.4.128/25 [120/1] via 172.29.6.6, 00:00:17, Serial0/0/1
R       172.29.6.8/30 [120/1] via 172.29.6.1, 00:00:16, Serial0/0/0
                      [120/1] via 172.29.6.6, 00:00:17, Serial0/0/1
R       172.29.6.12/30 [120/1] via 172.29.6.1, 00:00:16, Serial0/0/0
                       [120/1] via 172.29.6.6, 00:00:17, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:16, Serial0/0/0

MEDELLIN2#
```

Figura 28 Verificación y documentación la base de datos de RIP de cada Reuter

```
     172.29.6.9            120      00:00:19
     172.29.6.5            120      00:00:14
Distance: (default is 120)
MEDELLIN3#show ip route rip
     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
R       172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:23, Serial0/1/0
R       172.29.6.0/30 [120/1] via 172.29.6.13, 00:00:08, Serial0/0/1
                      [120/1] via 172.29.6.9, 00:00:08, Serial0/0/0
                      [120/1] via 172.29.6.5, 00:00:23, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.6.13, 00:00:08, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.6.9, 00:00:08, Serial0/0/0

MEDELLIN3#
```

Figura 29 Verificación y documentación la base de datos de RIP de cada Reuter

```
     172.29.3.10           120       00:00:21
Distance: (default is 120)
BOGOTA1#show ip route rip
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.0.0/24 [120/1] via 172.29.3.2, 00:00:18, Serial0/1/0
                      [120/1] via 172.29.3.6, 00:00:18, Serial0/1/1
R       172.29.1.0/24 [120/1] via 172.29.3.10, 00:00:26, Serial0/0/1
R       172.29.3.12/30 [120/1] via 172.29.3.2, 00:00:18, Serial0/1/0
                       [120/1] via 172.29.3.6, 00:00:18, Serial0/1/1
                       [120/1] via 172.29.3.10, 00:00:26, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks

BOGOTA1#
```

Figura 30 Verificación y documentación la base de datos de RIP de cada Reuter

```
     172.29.3.9            120       00:00:06
     172.29.3.14           120       00:00:08
Distance: (default is 120)
BOGOTA2#show ip route rip
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.0.0/24 [120/1] via 172.29.3.14, 00:00:11, Serial0/0/1
R       172.29.3.0/30 [120/1] via 172.29.3.14, 00:00:11, Serial0/0/1
                      [120/1] via 172.29.3.9, 00:00:10, Serial0/0/0
R       172.29.3.4/30 [120/1] via 172.29.3.14, 00:00:11, Serial0/0/1
                      [120/1] via 172.29.3.9, 00:00:10, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:10, Serial0/0/0

BOGOTA2#
```

Figura 31 Verificación y documentación la base de datos de RIP de cada Reuter

```
     172.29.3.5            120       00:00:26
     172.29.3.13           120       00:00:07
Distance: (default is 120)
BOGOTA3#show ip route rip
     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
R       172.29.1.0/24 [120/1] via 172.29.3.13, 00:00:14, Serial0/1/0
R       172.29.3.8/30 [120/1] via 172.29.3.1, 00:00:07, Serial0/0/0
                      [120/1] via 172.29.3.5, 00:00:07, Serial0/0/1
                      [120/1] via 172.29.3.13, 00:00:14, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.3.1, 00:00:07, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 172.29.3.5, 00:00:07, Serial0/0/1

BOGOTA3#
```

Figura 32 Verificación y documentación la base de datos de RIP de cada Reuter

2.2.29. Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Tabla 30 Configuración de encapsulamiento y autenticación PPP, parte 5 de escenario 2

ISP	MEDELLIN1 username ISP password cisco

username MEDELLIN password cisco interface Serial0/0/0 encapsulation ppp ppp authentication pap ppp pap sent-username ISP password cisco	 interface Serial0/0/0 encapsulation ppp ppp authentication pap ppp pap sent-username MEDELLIN password cisco

El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

Tabla 31 Configuración con autenticación CHAP. Parte 5de escenario 2.

ISP	BOGOTA1
username BOGOTA password cisco interface Serial0/0/1 encapsulation ppp ppp authentication chap	username ISP password cisco interface Serial0/0/0 encapsulation ppp ppp authentication chap

2.2.30. Parte 6: Configuración de PAT.

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.

MEDELLIN1

ip nat inside source list 1 interface Serial0/0/0 overload

access-list 1 permit 172.29.4.0 0.0.3.255

interface Serial0/0/0

ip nat outside

interface Serial0/0/1

ip nat inside

interface Serial0/1/0

ip nat inside

interface Serial0/1/1

ip nat inside

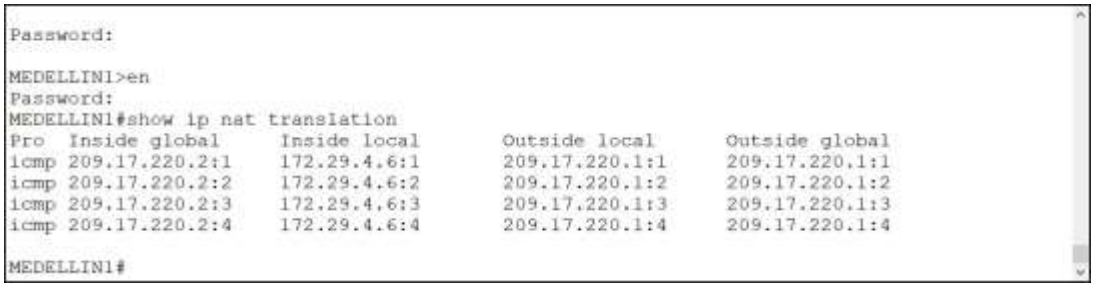

Figura 33 Configuración de PAT, parte 6 de escenario 2.

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.

BOGOTA1

ip nat inside source list 1 interface Serial0/0/0 overload

access-list 1 permit 172.29.0.0 0.0.3.255

interface Serial0/0/0

ip nat outside

interface Serial0/0/1

ip nat inside

interface Serial0/1/0

ip nat inside

interface Serial0/1/1

ip nat inside

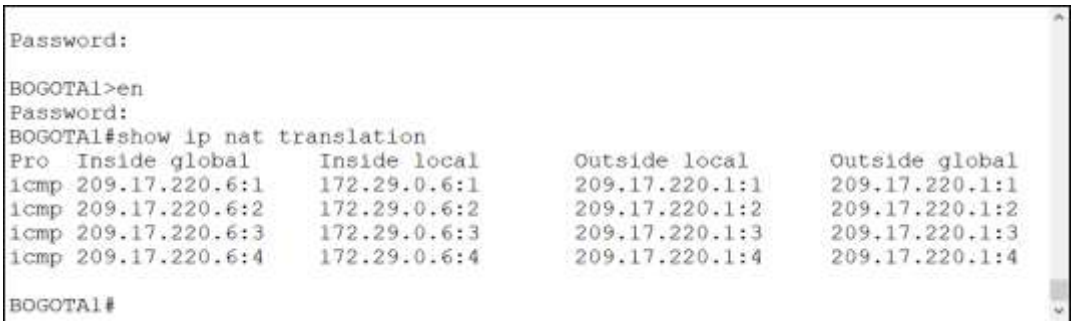

Figura 34 Configuración de PAT, parte 6 de escenario 2.

2.2.31. Parte 7: Configuración del servicio DHCP.

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

MEDELLIN2

ip dhcp excluded-address 172.29.4.1 172.29.4.5

ip dhcp excluded-address 172.29.4.129 172.29.4.133

ip dhcp pool MED2

network 172.29.4.0 255.255.255.128

default-router 172.29.4.1

dns-server 8.8.8.8

ip dhcp pool MED3

network 172.29.4.128 255.255.255.128

default-router 172.29.4.129

dns-server 8.8.8.8

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

MEDELLIN3

```
interface GigabitEthernet0/0
  ip helper-address 172.29.6.5
```

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

BOGOTA2

```
ip dhcp excluded-address 172.29.1.1 172.29.1.5
ip dhcp excluded-address 172.29.0.1 172.29.0.5
ip dhcp pool BOG2
 network 172.29.1.0 255.255.255.0
 default-router 172.29.1.1
 dns-server 8.8.8.8
ip dhcp pool BOG3
 network 172.29.0.0 255.255.255.0
 default-router 172.29.0.1
 dns-server 8.8.8.8
```

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

BOGOTA3

```
interface GigabitEthernet0/0
  ip helper-address 172.29.3.13
```

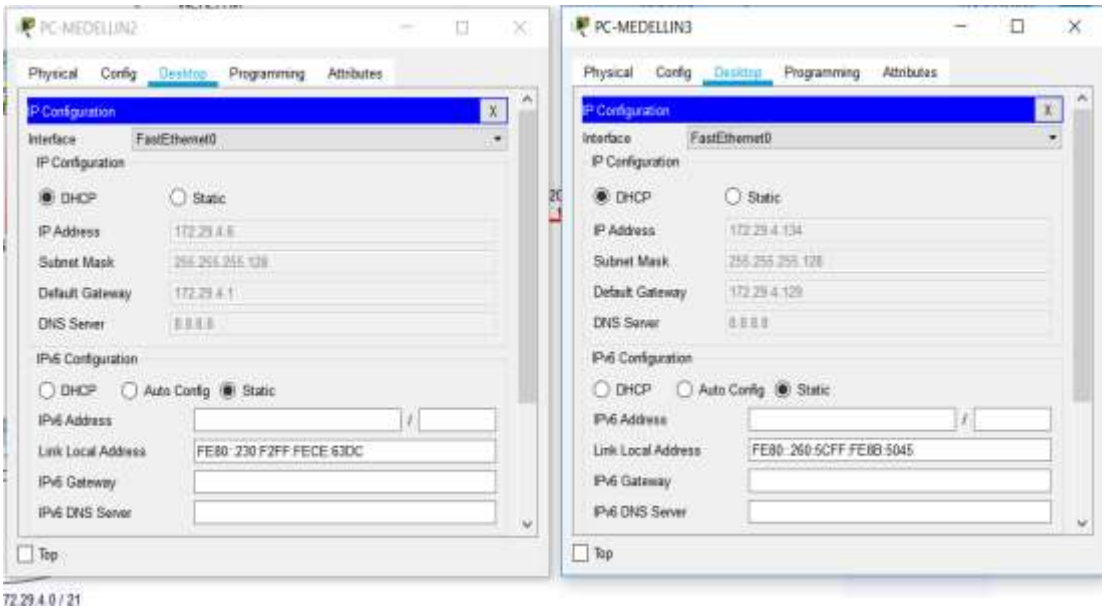

Figura 35 Configuración del servicio DHCP, Parte 7 de escenario 2.

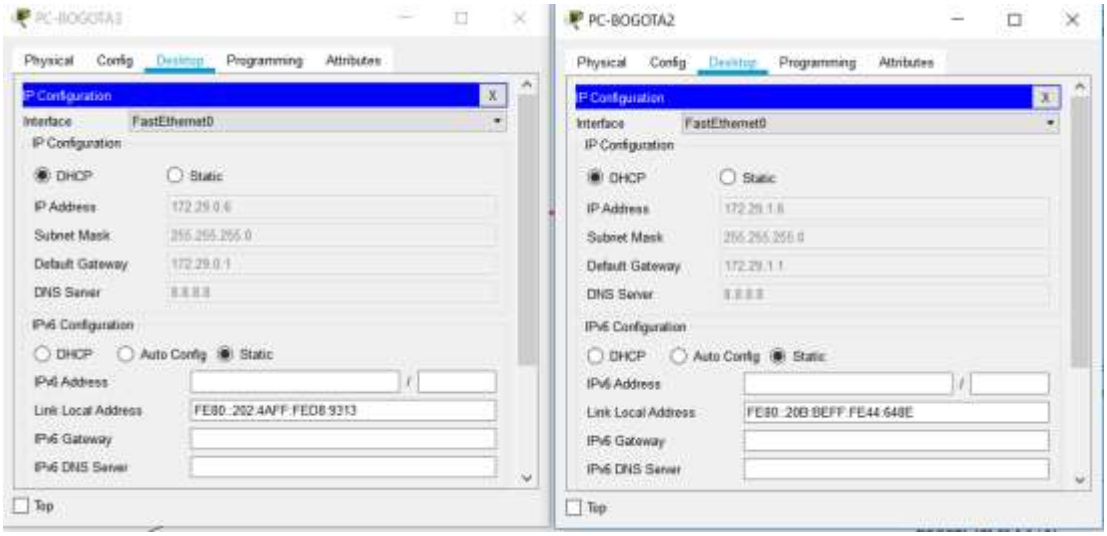

Figura 36 Configuración del servicio DHCP, Parte 7 de escenario 2.

3. CONCLUSIONES

Finalmente se desarrolló los escenarios correspondientes dados para la prueba de habilidades, donde se implementaron los diferentes topologías de la red como inicialización de los dispositivos vuelta de carga de los router y switch, al igual que la configuración de parámetros básicos dentro de los dispositivos, configuración de la computadora en la red de internet, verificación de la conectividad dentro de la red, la configuración de los tweets y en las redes, la configuración de los protocolos de routing Dinámico ripv2 la implementación de los de DHCP y NAT para los IPv4 para lo establecido dentro de el escenario 1. Por otro lado dentro del escenario número 2 se realiza la topología de la red de las dos ciudades de Medellín y Colombia con la configuración del enrutamiento, deshabilitacion de la propagación del protocolo RIP , verificación del protocolo RIP la configuración y encapsulamiento y autenticación de las PPP , configuración de las PAT y las respectivas configuraciones del DHCP logrando establecer la verificación del protocolo, la configuración del encapsulamiento y autenticación y las configuraciones del servicio DHCP.

4. REFERENCIAS BIBLIOGRÁFICAS

CISCO (2014) Configuraciones Recuperado de: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first- ospf/7039-1.html

CONFIGURACION VLANS (2014) Recuperado de: https://todopacketracer.com/2011/10/18/configuracion-de-vlans/

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY- 7F5KIRC3

UNAD (2014). Configuración de Switches y Routers [OVA].Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de https://www.eduangi.org/node186.html

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-packetmarking/10100-priorityvsbw.html