

Solución De Dos Estudios De Caso Bajo El Uso De Tecnología Cisco

Omar Danilo Rivera Barrios

Universidad Nacional Abierta y a Distancia UNAD
Escuela De Ciencias Básicas, Tecnología Ingeniería
Ingeniería de Sistemas
Bogotá D.C.
2020

Solución De Dos Estudios De Caso Bajo El Uso De Tecnología Cisco

Omar Danilo Rivera Barrios

Asesor: Hector Julián Parra

Universidad Nacional Abierta y a Distancia UNAD
Escuela De Ciencias Básicas, Tecnología Ingeniería
Ingeniería de Sistemas

Bogotá D.C.

2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá D.C. 06 de mayo de 2020

Dedicatoria

Le quiero agradecer primero a Dios por permitirme culminar mi carrera profesional teniendo el intelecto y capacidad para poder aprender cada día más.

Le agradezco a mi esposa e hijo por su apoyo, colaboración y ayuda incondicional, siempre con una sonrisa y una voz de aliento para seguir adelante.

AGRADECIMIENTOS

Realizo un profundo agradecimiento a todos los tutores, directores de curso y compañeros quienes fueron un punto de apoyo y ayuda para cumplir todas las metas propuestas a lo largo de mi carrera.

TABLA DE CONTENIDO

INTRODUCCIÓN.....	19
OBJETIVOS	20
OBJETIVO GENERAL	20
OBJETIVOS ESPECÍFICOS	20
PLANTEAMIENTO DEL PROBLEMA.....	21
DEFINICIÓN DEL PROBLEMA.....	21
JUSTIFICACIÓN.....	21
MARCO TEÓRICO.....	22
MATERIALES Y MÉTODOS.....	23
MATERIALES	23
METODOLOGÍA	23
1. ESCENARIO 1	24
1.1. PARTE 1: INICIALIZAR DISPOSITIVOS	24
1.1.1. Paso1: Inicializar y volver a cargar los routers y los switches.....	24
1.2. PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS.....	25
1.2.1. Paso 1: Configurar la computadora de Internet	25
1.2.2. Paso 2: Configurar R1	25
1.2.3. Paso 3: Configurar R2.....	26
1.2.4. Paso 4: Configurar R3.....	28
1.2.5. Paso 5: Configurar S1	29
1.2.6. Paso 6: Configurar S3.....	29
1.2.7. Paso 7: Verificar la conectividad de la red.....	30
1.3. PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN	31
1.3.1. Paso 1: Configurar S1	31
1.3.2. Paso 2: Configurar S3	32
1.3.3. Paso 3: Configurar R1	33
1.3.4. Paso 4: Verificar la conectividad de la red.....	34
1.4. PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2.....	36
1.4.1. Paso 1: Configurar RIPv2 en el R1.....	36

1.4.2.	Paso 2: Configurar RIPv2 en el R2.....	37
1.4.3.	Paso 3: Configurar RIPv2 en el R3.....	38
1.4.4.	Paso 4: Verificar la información de RIP	39
1.5.	PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPv4	41
1.5.1.	Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	41
1.5.2.	Paso 2: Configurar la NAT estática y dinámica en el R2	41
1.5.3.	Paso 3: Verificar el protocolo DHCP y la NAT estática	42
1.6.	PARTE 6: CONFIGURAR NTP.....	44
1.7.	PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL).....	45
1.7.1.	Paso 1: Restringir el acceso a las líneas VTY en el R2	45
1.7.2.	Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	46
2.	ESCENARIO 2	47
2.1.	PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO.....	52
2.1.1.	Paso 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.....	52
2.1.2.	Paso 2: Los routers Bogotá1 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.....	57
2.1.3.	Paso 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.....	57
2.2.	PARTE 2: TABLA DE ENRUTAMIENTO	57
2.2.1.	Paso 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.....	57
2.2.2.	Paso 2: Verificar el balanceo de carga que presentan los routers.	61
2.2.3.	Paso 3: 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.	64
2.2.4.	Paso 4: Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.....	65
2.2.5.	Paso 5: Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.	66
2.2.6.	Paso 6: El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.	67

2.3.	PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF	68
2.4.	PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.....	69
2.4.1.	Paso 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.....	69
2.4.2.	Paso 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.	72
2.5.	PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP	78
2.5.1.	Paso 1: Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.....	78
2.5.2.	Paso 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.....	78
2.6.	PARTE 6: CONFIGURACIÓN DE NAT.....	79
2.6.1.	Paso 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.	79
2.6.2.	Paso 2: 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, con diferente puerto.	79
2.6.3.	Paso 3: 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, con diferente puerto.	79
2.7.	PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP	80
2.7.1.	Paso 1: Configurar la red Medellín2 y Medellín3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.....	80
2.7.2.	Paso 2: El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.	81
2.7.3.	Paso 3: Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.	81

2.7.4. Paso 4: Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.....	81
RECOMENDACIONES.....	82
CONCLUSIONES	83
REFERENCIAS BIBLIOGRÁFICAS.....	84

LISTA DE TABLAS

Tabla 1 Inicializar y volver a cargar los routers y los switches	24
Tabla 2 Configurar la computadora de Internet.....	25
Tabla 3 Configurar R1	25
Tabla 4 Configurar R2	26
Tabla 5 Configurar R3	28
Tabla 6 Configurar S1.....	29
Tabla 7 Configurar S3.....	29
Tabla 8 Verificar la conectividad de la red	30
Tabla 9 Configurar S1.....	32
Tabla 10 Configurar S3.....	32
Tabla 11 Configurar R1	33
Tabla 12 Verificar la conectividad de la red	34
Tabla 13 Configurar RIPv2 en el R1	36
Tabla 14 Configurar RIPv2 en el R2	37
Tabla 15 Configurar RIPv2 en el R3	38
Tabla 16 Verificar la información de RIP.....	39
Tabla 17 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	41
Tabla 18 Configurar la NAT estática y dinámica en el R2	41
Tabla 19 Verificar el protocolo DHCP y la NAT estática.....	42
Tabla 20 Configurar NTP	44
Tabla 21 Restringir el acceso a las líneas VTY en el R2.....	45
Tabla 22 Introducir el comando de CLI	46
Tabla 23 Configuración inicial de dispositivos.....	47
Tabla 24 Direccionamiento IP de los dispositivos	51
Tabla 25 Configuración protocolo OSPF.....	52
Tabla 26 Configuración OSPF	57
Tabla 27 Configuración ruta estática	57
Tabla 28 Enrutamiento de los dispositivos.....	57
Tabla 29 Verificación de balanceo de carga	61
Tabla 30 Validación de los routers	64
Tabla 31 Conexiones OSPF	65
Tabla 32 Rutas routers	66
Tabla 33 Rutas estáticas	67
Tabla 34 Interfaces que no necesitan desactivación.....	68
Tabla 35 Desactivación de interfaces	68
Tabla 36 Protocolo OSPF.....	69
Tabla 37 Base de datos de OSPF	72
Tabla 38 Autenticación PAT	78
Tabla 39 Autenticación CHAT.....	78
Tabla 40 Configuración NAT MEDELLIN1	79
Tabla 41 Configuración NAT BOGOTA1.....	79
Tabla 42 Configuración DHCP Medellín	80

Tabla 43 Configuración broadcast MEDELLIN3.....	81
Tabla 44 Configuración DHCP Bogotá.....	81
Tabla 45 Configuración broadcast BOGOTA1	81

LISTA DE ILUSTRACIONES

Ilustración 1 Topología de escenario 1	24
Ilustración 2 Ping 172.16.1.2	30
Ilustración 3 Ping 172.16.2.1	31
Ilustración 4 Ping 209.165.200.233.....	31
Ilustración 5 Ping 192.168.99.1.....	34
Ilustración 6 Ping 192.168.99.1.....	35
Ilustración 7 Ping 192.168.21.1.....	35
Ilustración 8 Ping 192.168.23.1.....	36
Ilustración 9 PC-A DHCP.....	43
Ilustración 10 PC-C DHCP.....	43
Ilustración 11 Ping PC-C.....	44
Ilustración 12 Web 209.165.200.237	44
Ilustración 13 Verificar la ACL.....	46
Ilustración 14 Topología de escenario 2	47
Ilustración 15 Conexión física de los equipos	51
Ilustración 16 Enrutamiento ISP.....	58
Ilustración 17 Enrutamiento BOGOTA1	58
Ilustración 18 Enrutamiento BOGOTA2	59
Ilustración 19 Enrutamiento BOGOTA3	59
Ilustración 20 Enrutamiento MEDELLIN1	60
Ilustración 21 Enrutamiento MEDELLIN2.....	60
Ilustración 22 Enrutamiento MEDELLIN3.....	61
Ilustración 23 Balanceo de carga ISP	61
Ilustración 24 Balanceo de carga BOGOTA1	62
Ilustración 25 Balanceo de carga BOGOTA2.....	62
Ilustración 26 Balanceo de carga BOGOTA3.....	63
Ilustración 27 Balanceo de carga MEDELLIN1	63
Ilustración 28 Balanceo de carga MEDELLIN2	64
Ilustración 29 Balanceo de carga MEDELLIN3	64
Ilustración 30 Validación BOGOTA1	65
Ilustración 31 Validación MEDELLIN1	65
Ilustración 32 OSPF BOGOTA2.....	66
Ilustración 33 OSPF MEDELLIN2	66
Ilustración 34 Rutas BOGOTA3.....	67
Ilustración 35 Rutas MEDELLIN3	67
Ilustración 36 Rutas estáticas ISP	68
Ilustración 37 Protocolo ISP.....	69
Ilustración 38 Protocolo BOGOTA1	70
Ilustración 39 Protocolo BOGOTA2	70
Ilustración 40 Protocolo BOGOTA3	71
Ilustración 41 Protocolo MEDELLIN1	71
Ilustración 42 Protocolo MEDELLIN2.....	72

Ilustración 43 Protocolo MEDELLIN3.....	72
Ilustración 44 OSPF ISP	73
Ilustración 45 OSPF BOGOTA1.....	74
Ilustración 46 OSPF BOGOTA2.....	75
Ilustración 47 OSPF BOGOTA3.....	75
Ilustración 48 OSPF MEDELLIN1	76
Ilustración 49 OSPF MEDELLIN2	77
Ilustración 50 OSPF MEDELLIN3	77

GLOSARIO

CABLE: Medio de transmisión de cable de cobre o fibra óptica envuelto en una cubierta protectora.

DIRECCIÓN IP CON CLASE: En los primeros tiempos de IPv4, las direcciones IP estaban divididas en 5 clases, particularmente Clase A, Clase B, Clase C, Clase D y Clase E.

ETHERNET: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3.

FLASH: Tecnología desarrollada por Intel y cuya licencia le ha sido otorgada a otras empresas de semiconductores. La memoria Flash es un almacenamiento no volátil que se puede borrar y reprogramar de forma eléctrica. Permite que las imágenes de software se guarden, arranquen y rescriban según sea necesario.

GATEWAY: Dispositivo de una red que sirve como punto de acceso a otra red. El gateway predeterminado es utilizado por un host cuando la dirección de destino de un paquete IP pertenece a algún lugar fuera de la subred local. Un router es un buen ejemplo de un gateway predeterminado.

HOST: Sistema de computación en una red. Es similar al nodo, salvo que el host generalmente indica un sistema de computación, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluidos servidores de acceso y routers.

IP: Protocolo de Internet. Protocolo de capa de red en el stack TCP/IP que brinda un servicio de internetworking sin conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad.

IPv6: Protocolo de capa de red para trabajos de Internet conmutados por paquetes. Sucesor de IPv4 para uso general en Internet.

LAN: El término Red de área local (LAN) hace referencia a una red local, o a un grupo de redes locales interconectadas, que están bajo el mismo control administrativo. En las primeras épocas del networking, las LAN se definían como pequeñas redes que existían en una única ubicación física. A pesar de que las LAN pueden ser una única red local instalada en una vivienda u oficina pequeña, la definición de LAN ha evolucionado y ahora incluye redes locales interconectadas compuestas por muchos cientos de hosts, instaladas en múltiples edificios y ubicaciones.

LOOPBACK: 127.0.0.1 es una dirección IP disponible en todos los dispositivos para ver si la tarjeta NIC de ese dispositivo funciona. Si se envía algo a 127.0.0.1, hace un loop back en sí misma y por consiguiente envía los datos a la NIC de ese

dispositivo. Si se obtiene una respuesta positiva a un ping 127.0.0.1, se sabe que la tarjeta NIC funciona correctamente.

NVRAM: Memoria de acceso aleatorio no volátil. Memoria de acceso aleatorio que, cuando la computadora se apaga, el contenido de la NVRAM permanece allí.

PAQUETE: Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes con mayor frecuencia se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

ROUTER: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red. Ocasionalmente, se denomina gateway (aunque esta definición de gateway está cayendo más en desuso).

VLSM: máscara de subred de longitud variable. Capacidad para especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

RESUMEN

En el presente trabajo tomaremos 2 casos de uso concernientes a la configuración de redes empresariales, aplicar las configuraciones necesarias para que los escenarios propuestos funcionen y además demostrar de forma gráfica lo que ocurre al hacer dicha configuración.

Cada comando y configuración hecha en el simulador Packet Tracer fue posible gracias al curso CCNA1 y CCNA2 de CISCO Networking, de donde se logró adquirir los conocimientos necesarios para lograr a una solución de los escenarios propuestos.

PALABRAS CLAVES

Lan, IPv4, IPv6, Router, Switches, Servidor Web, Pc, CISCO, Ping, Traceroute, Show IP Route.

INTRODUCCIÓN

Las redes computacionales han sido uno de los pilares de la tecnología informática, a la par que se construyen nuevas herramientas tecnológicas deben ser implementadas en redes existentes, las cuales no pueden ser reemplazadas de inmediato, pero sí actualizadas constantemente, es así como entender los principios básicos de funcionamiento de estas es imperativo para un profesional de la ingeniería de sistemas. Ahora bien, dentro de todas las empresas de tecnología informática está CISCO Systems, empresa que ha brindado herramientas para que una red informática cuente con el grado de sofisticación suficiente para funcionar globalmente sin ningún problema y siempre brindando el servicio para el que fue construida dicha red.

La siguiente evaluación, recoge la información obtenida a través del desarrollo de dos ejercicios prácticos entregados y en este se hacen las observaciones, especificaciones técnicas, las limitaciones y las conclusiones surgidas tras el desarrollo, análisis y comprensión de las actividades propuestas, para alcanzar un grado de desarrollo de competencias y habilidades adquiridas en el diplomado de profundización Cisco (Diseño e implementación de soluciones integradas LAN/WAN).

OBJETIVOS

OBJETIVO GENERAL

Poder resolver mediante el conocimiento adquirido dos escenarios propuestos en la prueba de habilidades prácticas de acuerdo con el curso CCNA de CISCO.

OBJETIVOS ESPECÍFICOS

Identificar que dispositivos utilizar para la construcción de una topología de red.

Configurar dispositivos de comunicación como Routers, Switches, Servidores.

Implementar seguridad en los Routers, Switches y aplicar las políticas necesarias.

Realizar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing, de DHCP, NAT, RIP Ver2 y demás permitiendo dar solución a ciertos problemas.

PLANTEAMIENTO DEL PROBLEMA

DEFINICIÓN DEL PROBLEMA

Realizar las tareas asignadas en cada uno de los dos escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

JUSTIFICACIÓN

A lo largo de la carrera de Ingeniería de sistemas de la Universidad Nacional Abierta y a Distancia (UNAD), se ha logrado obtener el conocimiento necesario para desempeñarse como un gran profesional. Al llegar al final de la carrera se opta por el DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) para lograr adquirir el conocimiento necesario para poder desenvolverse en un ámbito de redes a nivel profesional.

MARCO TEÓRICO

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

MATERIALES Y MÉTODOS

MATERIALES

Software: Packet Tracer 7.3.0

METODOLOGÍA

Teniendo en cuenta que la Prueba de habilidades está conformada por dos escenarios, el estudiante deberá realizar el proceso de configuración usando la siguiente herramienta: Packet Tracer.

1. ESCENARIO 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI, como se muestra en la ilustración 1.

Topología

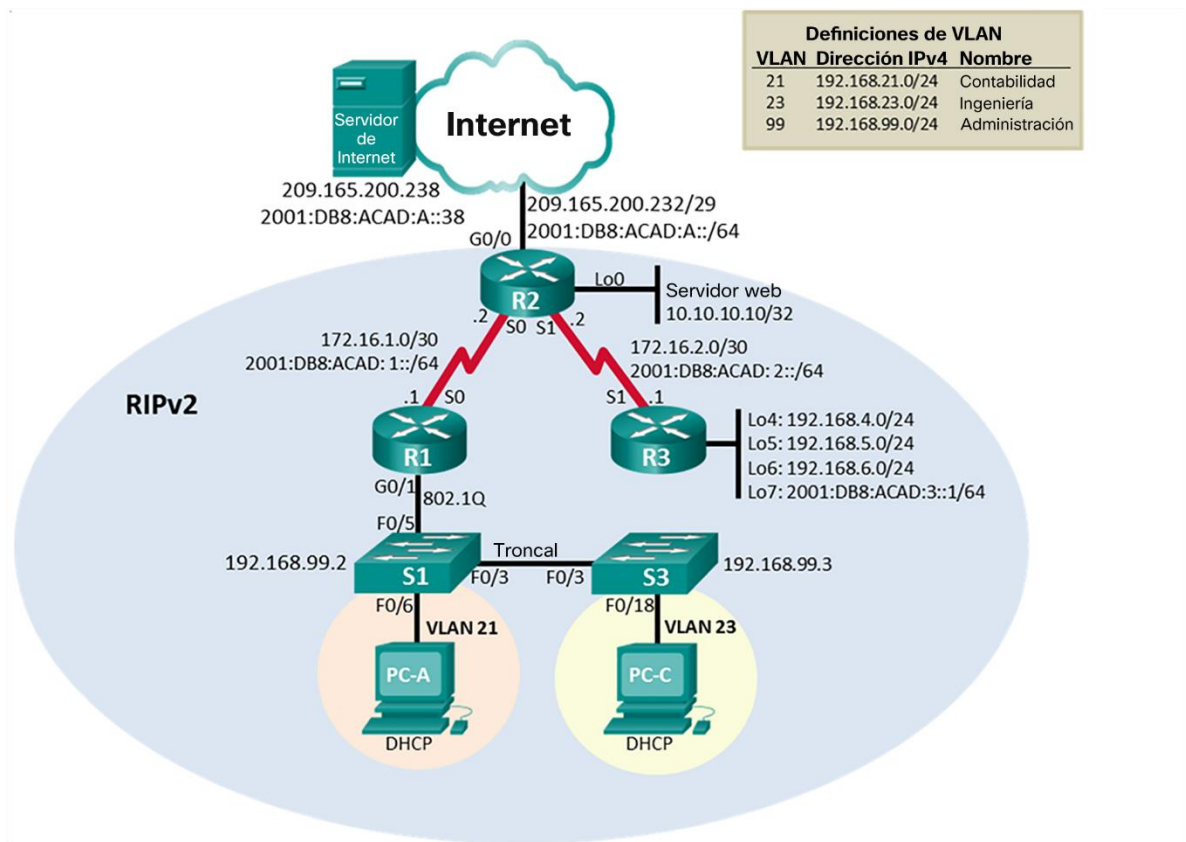


Ilustración 1 Topología de escenario 1

1.1. PARTE 1: INICIALIZAR DISPOSITIVOS

1.1.1. Paso1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tarea	Comando de IOS
-------	----------------

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

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

1.2. PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS 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 Configurar la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

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.

1.2.2. Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configurar R1

Elemento o tarea de configuración	Especificación
--	-----------------------

Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd \$Se prohíbe el acceso no autorizado.\$
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description Connection to 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 shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

1.2.3. Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4 Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class

Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd \$Se prohíbe el acceso no autorizado.\$
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#Interface Loopback0 R2(config-if)#ip address 10.10.10.10 255.255.255.255
Rutas predeterminadas	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

1.2.4. Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5 Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd \$Se prohíbe el acceso no autorizado.\$
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#Interface Loopback4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#Interface Loopback5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#Interface Loopback6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#Interface Loopback7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

Rutas Predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1 R3(config)#ipv6 route ::/0 serial 0/0/1
-----------------------	---

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	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd \$Se prohíbe el acceso no autorizado.\$

1.2.6. Paso 6: Configurar S3

Tabla 7 Configurar S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login

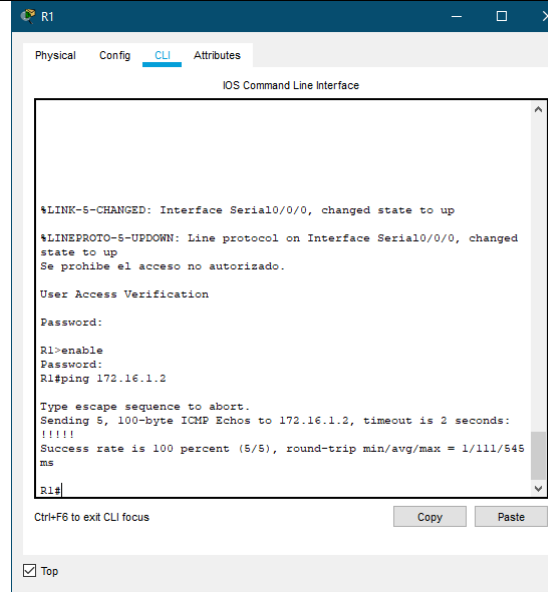
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd \$Se prohíbe el acceso no autorizado.\$

1.2.7. Paso 7: Verificar la conectividad de la red

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

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

Tabla 8 Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 <p style="text-align: right;"><i>Ilustración 2 Ping 172.16.1.2</i></p>

R2	R3, S0/0/1	172.16.2.1	<p style="text-align: center;"><i>Ilustración 3 Ping 172.16.2.1</i></p>
PC de Internet	Gateway predeterminado	209.165.200.233	<p style="text-align: center;"><i>Ilustración 4 Ping 209.165.200.233</i></p>

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

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 Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>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</pre>
Asignar la dirección IP de administración.	<pre>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown</pre>
Asignar el gateway predeterminado	<pre>S1(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</pre>
Forzar el enlace troncal en la interfaz F0/5	<pre>S1(config-if)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access</pre>
Asignar F0/6 a la VLAN 21	<pre>S1(config-if-range)#interface fastEthernet 0/6 S1(config-if)#switchport access vlan 21</pre>
Apagar todos los puertos sin usar	<pre>S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown</pre>

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	<pre>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</pre>
Asignar la dirección IP de administración	<pre>S3(config-vlan)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown</pre>
Asignar el gateway predeterminado.	<pre>S3(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S3(config)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access</pre>
Asignar F0/18 a la VLAN 23	<pre>S3(config-if-range)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 23</pre>
Apagar todos los puertos sin usar	<pre>S3(config-if)#interface range f0/1-2, f0/4- 17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown</pre>

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	<pre>R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0</pre>

Configurar la subinterfaz 802.1Q .23 en G0/1	<pre>R1(config-subif)#interface gigabitEthernet 0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0</pre>
Configurar la subinterfaz 802.1Q .99 en G0/1	<pre>R1(config-subif)#interface gigabitEthernet 0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0</pre>
Activar la interfaz G0/1	<pre>R1(config-subif)#int g0/1 R1(config-if)#no shutdown</pre>

1.3.4. Paso 4: Verificar la conectividad de la red

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

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

Tabla 12 Verificar la conectividad de la red

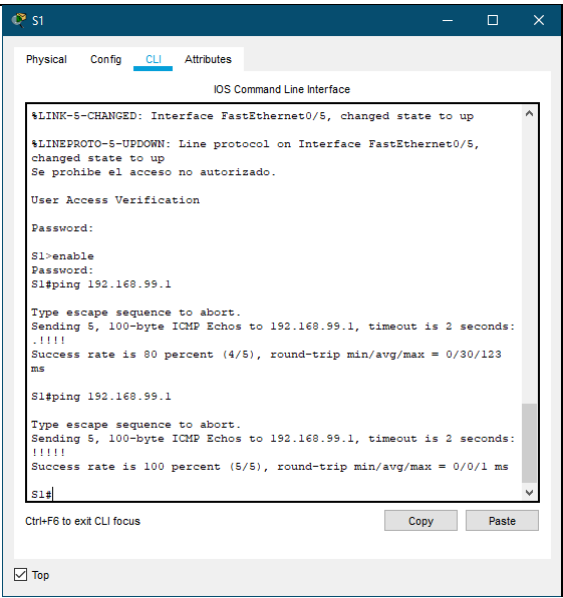
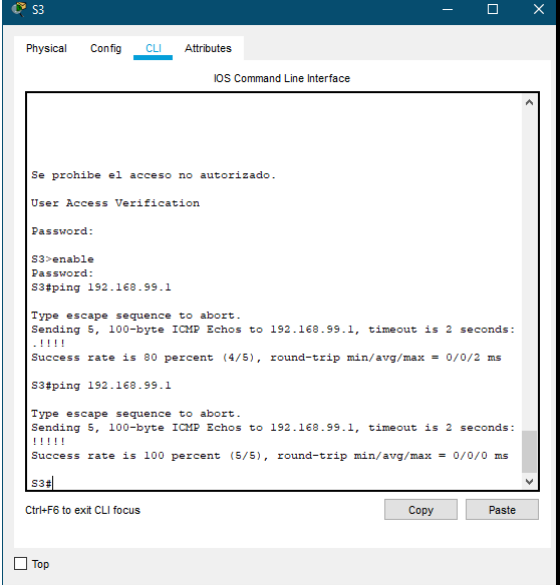
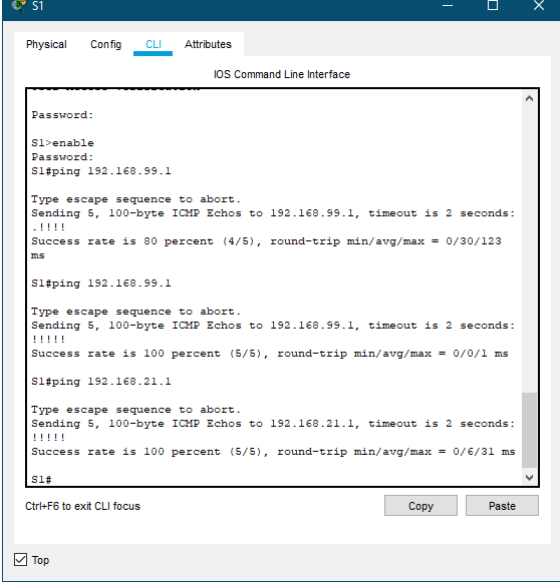
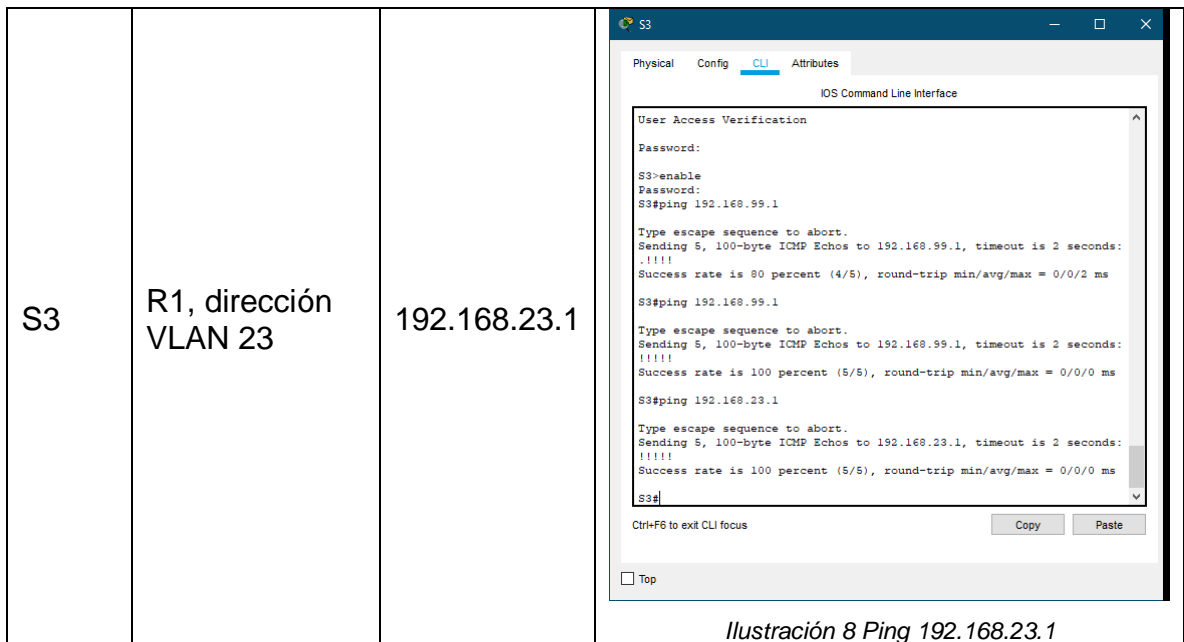
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	 <pre> S1# S1#enable S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/30/123 ms S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms S1# </pre>

Ilustración 5 Ping 192.168.99.1

S3	R1, dirección VLAN 99	192.168.99.1	 <pre> S3 Physical Config CLI Attributes IOS Command Line Interface Se prohíbe el acceso no autorizado. User Access Verification Password: S3>enable Password: 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 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms 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 S3# </pre>
<i>Ilustración 6 Ping 192.168.99.1</i>			
S1	R1, dirección VLAN 21	192.168.21.1	 <pre> S1 Physical Config CLI Attributes IOS Command Line Interface Password: S1>enable Password: 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 80 percent (4/5), round-trip min/avg/max = 0/30/123 ms S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/31 ms S1# </pre>
<i>Ilustración 7 Ping 192.168.21.1</i>			



1.4. PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2

1.4.1. Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	<pre> R1(config)#router rip R1(config-router)#version 2 </pre>

<p>Anunciar las redes conectadas directamente</p>	<pre>R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0</pre>
<p>Establecer todas las interfaces LAN como pasivas</p>	<pre>R1(config-router)#passive-interface gigabitEthernet 0/1.21 R1(config-router)#passive-interface gigabitEthernet 0/1.23 R1(config-router)#passive-interface gigabitEthernet 0/1.99</pre>
<p>Desactive la sumarización automática</p>	<pre>R1(config-router)#no auto-summary</pre>

1.4.2. Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14 Configurar RIPv2 en el R2

<p>Elemento o tarea de configuración</p>	<p>Especificación</p>
<p>Configurar RIP versión 2</p>	<pre>R2(config)#router rip R2(config-router)#version 2</pre>

Anunciar las redes conectadas directamente	<pre>R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0</pre>
Establecer la interfaz LAN (loopback) como pasiva	<pre>R2(config-router)#passive-interface loopback 0</pre>
Desactive la sumarización automática.	<pre>R2(config-router)#no auto-summary</pre>

1.4.3. Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15 Configurar RIPv2 en el R3

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

<p>Anunciar redes IPv4 conectadas directamente</p>	<pre>R3(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6 R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0</pre>
<p>Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas</p>	<pre>R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6</pre>
<p>Desactive la sumarización automática.</p>	<pre>R3(config-router)#no auto-summary</pre>

1.4.4. Paso 4: Verificar la información de RIP

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

Tabla 16 Verificar la información de RIP

Pregunta	Respuesta
<p>¿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?</p>	<pre>R3#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</pre>

	<pre> Interface Send Recv Triggered RIP Key-chain Serial0/0/1 2 2 Automatic network summarization is not in effect Maximum path: 4 Routing for Networks: 172.16.0.0 192.168.4.0 192.168.5.0 192.168.6.0 Passive Interface(s): Loopback4 Loopback5 Loopback6 Routing Information Sources: Gateway Distance Last Update 172.16.2.2 120 00:00:19 Distance: (default is 120) </pre>
<p>¿Qué comando muestra solo las rutas RIP?</p>	<pre> R3#show ip route rip 10.0.0.0/32 is subnetted, 1 subnets R 10.10.10.10 [120/1] via 172.16.2.2, 00:00:07, Serial0/0/1 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks R 172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:07, Serial0/0/1 192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks R 192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:07, Serial0/0/1 R 192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:07, Serial0/0/1 R 192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:07, Serial0/0/1 </pre>
<p>¿Qué comando muestra la sección de RIP de la configuración en ejecución?</p>	<pre> R3#show run section router rip router rip version 2 passive-interface Loopback4 passive-interface Loopback5 </pre>

	<pre> passive-interface Loopback6 network 172.16.0.0 network 192.168.4.0 network 192.168.5.0 network 192.168.6.0 no auto-summary </pre>
--	---

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

Las tareas de configuración para R1 incluyen las siguientes:

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

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	<pre> R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 </pre>
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	<pre> R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 </pre>
Crear un pool de DHCP para la VLAN 21.	<pre> R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 </pre>
Crear un pool de DHCP para la VLAN 23	<pre> R1(dhcp-config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 </pre>

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
--	-----------------------

Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gigabitEthernet 0/0 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
Configurar la NAT dinámica dentro de una ACL privada	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
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

1.5.3. Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 19 Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
---------------	-------------------

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

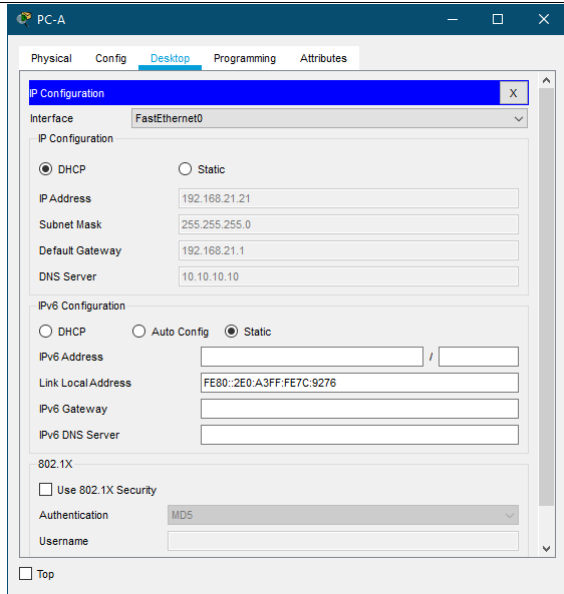


Ilustración 9 PC-A DHCP

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

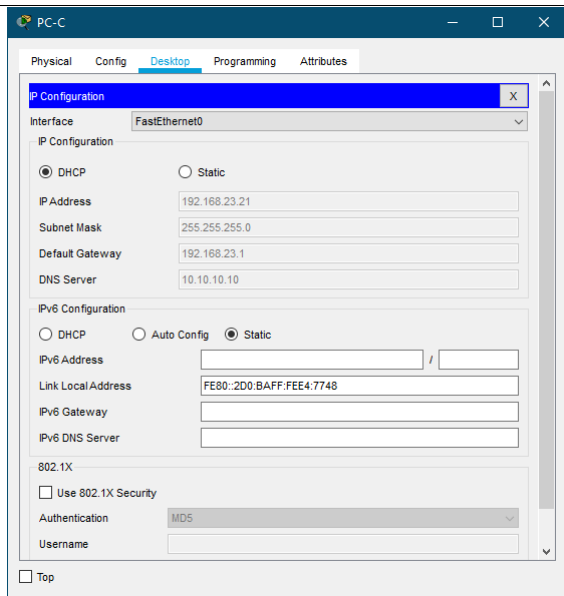
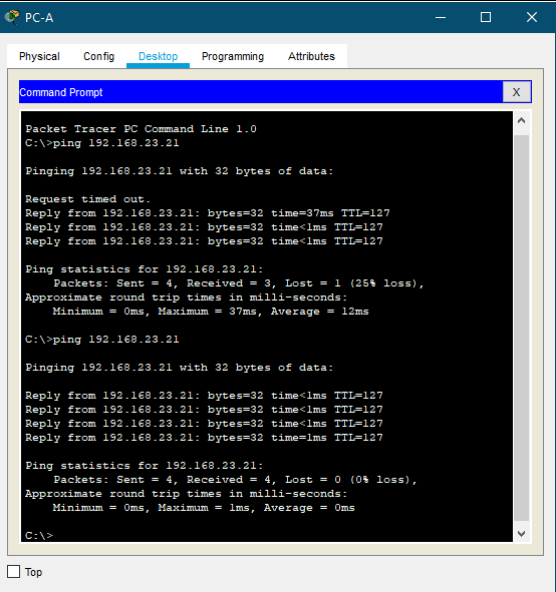
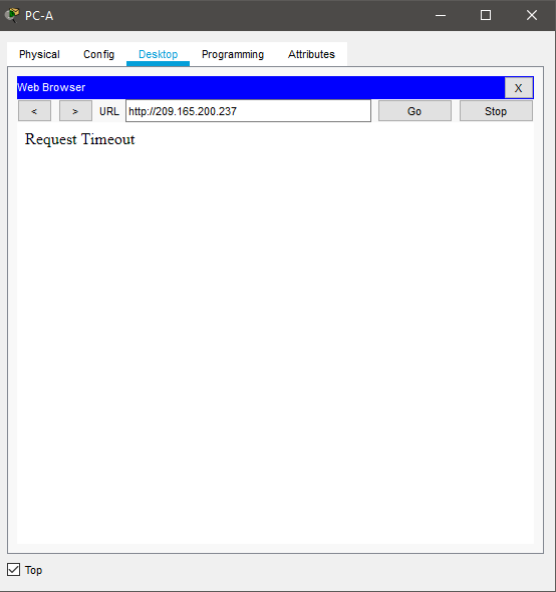


Ilustración 10 PC-C DHCP

<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p>Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	 <p style="text-align: right;"><i>Ilustración 11 Ping PC-C</i></p>
<p>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</p>	 <p style="text-align: right;"><i>Ilustración 12 Web 209.165.200.237</i></p>

1.6. PARTE 6: CONFIGURAR NTP

Tabla 20 Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016

Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	<pre>R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 8 16 177 6.00 726223572452.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured</pre>

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	<pre>R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1</pre>
Aplicar la ACL con nombre a las líneas VTY	<pre>R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in</pre>
Permitir acceso por Telnet a las líneas de VTY	<pre>R2(config-line)#transport input telnet</pre>

Verificar que la ACL funcione como se espera

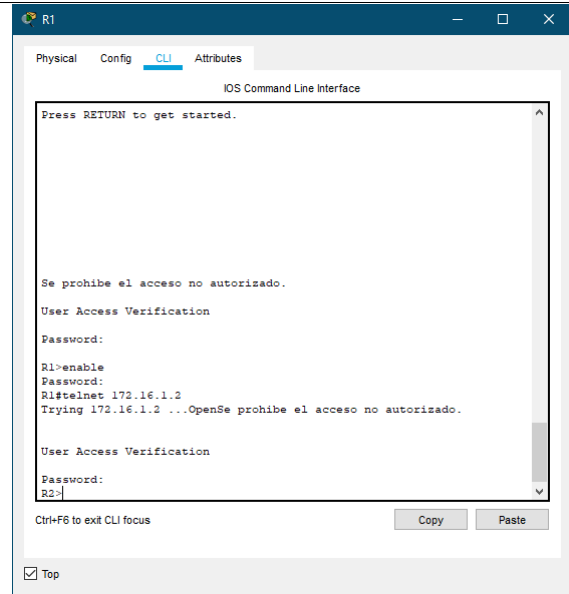


Ilustración 13 Verificar la ACL

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

Tabla 22 Introducir el comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

2. ESCENARIO 2

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

Topología

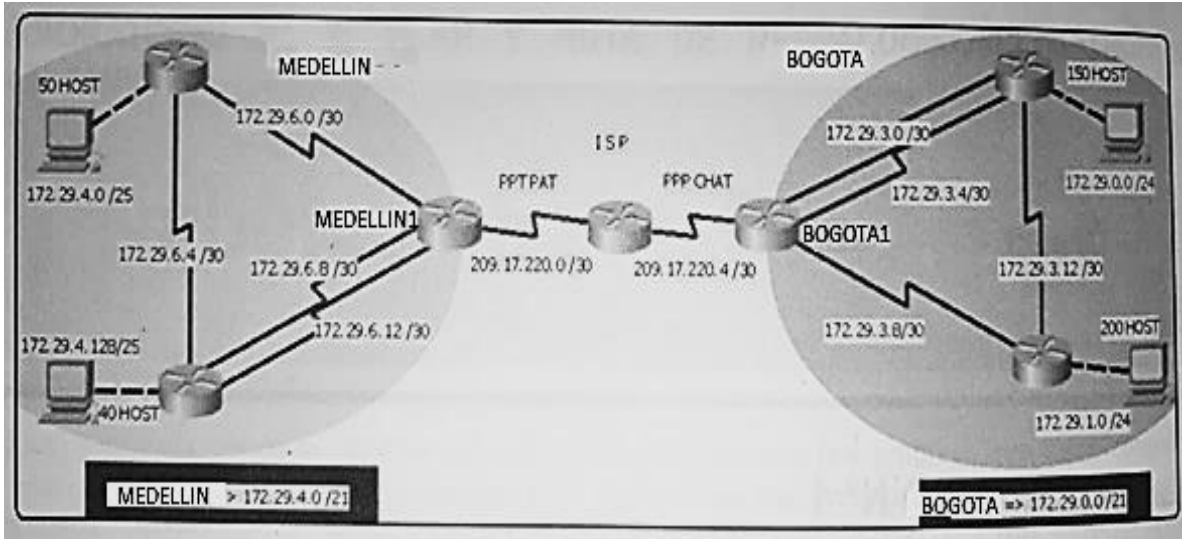


Ilustración 14 Topología de escenario 2

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

Los routers Bogotá2 y Medellín2 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 Bogotá1 y Medellín1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

Tabla 23 Configuración inicial de dispositivos

Router	Comandos
ISP	Router>enable Router#configure terminal

	<pre> Router(config)#no ip domain-lookup Router(config)#hostname ISP ISP(config)#enable secret class ISP(config)#line console 0 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#line vty 0 15 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#service password- encryption ISP(config)#banner motd \$Se prohíbe el acceso no autorizado.\$ ISP(config)#end </pre>
<p>BOGOTA1</p>	<pre> Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#hostname BOGOTA1 BOGOTA1(config)#enable secret class BOGOTA1(config)#line console 0 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#line vty 0 15 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#service password- encryption BOGOTA1(config)#banner motd \$Se prohíbe el acceso no autorizado.\$ BOGOTA1(config)#end </pre>
<p>BOGOTA2</p>	<pre> Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#hostname BOGOTA2 BOGOTA2(config)#enable secret class BOGOTA2(config)#line console 0 BOGOTA2(config-line)#password cisco BOGOTA2(config-line)#login BOGOTA2(config-line)#line vty 0 15 </pre>

	<pre> BOGOTA2 (config-line)#password cisco BOGOTA2 (config-line)#login BOGOTA2 (config-line)#service password- encryption BOGOTA2 (config)#banner motd \$Se prohíbe el acceso no autorizado.\$ BOGOTA2 (config)#end </pre>
BOGOTA3	<pre> Router>enable Router#configure terminal Router (config)#no ip domain-lookup Router (config)#hostname BOGOTA3 BOGOTA3 (config)#enable secret class BOGOTA3 (config)#line console 0 BOGOTA3 (config-line)#password cisco BOGOTA3 (config-line)#login BOGOTA3 (config-line)#line vty 0 15 BOGOTA3 (config-line)#password cisco BOGOTA3 (config-line)#login BOGOTA3 (config-line)#service password- encryption BOGOTA3 (config)#banner motd \$Se prohíbe el acceso no autorizado.\$ BOGOTA3 (config)#end </pre>
MEDELLIN1	<pre> Router>enable Router#configure terminal Router (config)#no ip domain-lookup Router (config)#hostname MEDELLIN1 MEDELLIN1 (config)#enable secret class MEDELLIN1 (config)#line console 0 MEDELLIN1 (config-line)#password cisco MEDELLIN1 (config-line)#login MEDELLIN1 (config-line)#line vty 0 15 MEDELLIN1 (config-line)#password cisco MEDELLIN1 (config-line)#login MEDELLIN1 (config-line)#service password- encryption MEDELLIN1 (config)#banner motd \$Se prohíbe el acceso no autorizado.\$ MEDELLIN1 (config)#end </pre>
MEDELLIN2	<pre> Router>enable </pre>

	<pre> Router#configure terminal Router(config)#no ip domain-lookup Router(config)#hostname MEDELLIN2 MEDELLIN2(config)#enable secret class MEDELLIN2(config)#line console 0 MEDELLIN2(config-line)#password cisco MEDELLIN2(config-line)#login MEDELLIN2(config-line)#line vty 0 15 MEDELLIN2(config-line)#password cisco MEDELLIN2(config-line)#login MEDELLIN2(config-line)#service password- encryption MEDELLIN2(config)#banner motd \$Se prohíbe el acceso no autorizado.\$ MEDELLIN2(config)#end </pre>
<p>MEDELLIN3</p>	<pre> Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#hostname MEDELLIN3 MEDELLIN3(config)#enable secret class MEDELLIN3(config)#line console 0 MEDELLIN3(config-line)#password cisco MEDELLIN3(config-line)#login MEDELLIN3(config-line)#line vty 0 15 MEDELLIN3(config-line)#password cisco MEDELLIN3(config-line)#login MEDELLIN3(config-line)#service password- encryption MEDELLIN3(config)#banner motd \$Se prohíbe el acceso no autorizado.\$ MEDELLIN3(config)#end </pre>

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

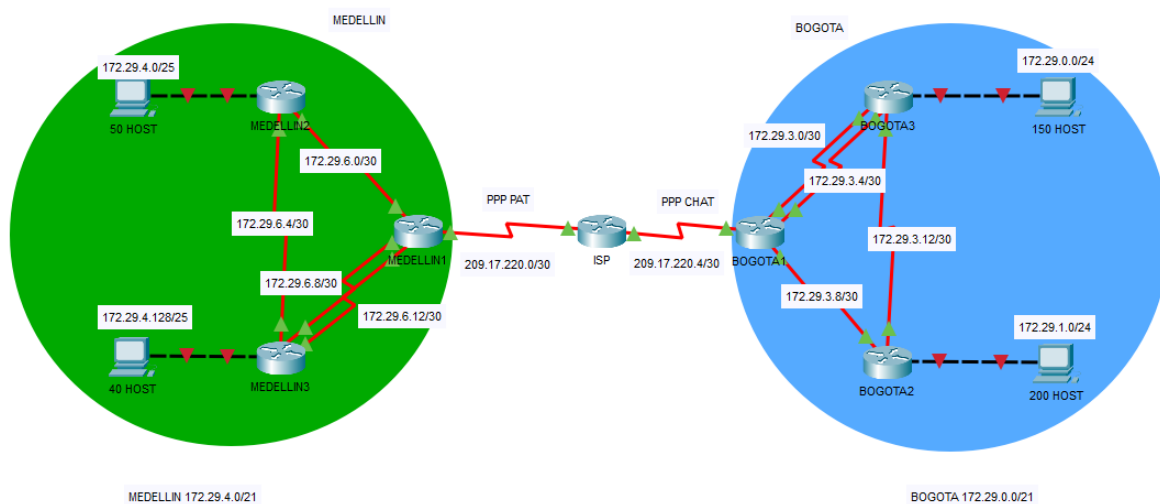


Ilustración 15 Conexión física de los equipos

Tabla 24 Direcccionamiento IP de los dispositivos

Router - Conexiones	Conexión	IP
ISP BOGOTA1	Se0/0/0 – Se0/0/0	209.17.220.5/30 – 209.17.220.6/30
BOGOTA1 BOGOTA2	Se0/0/1 – Se0/0/0	172.29.3.9/30 – 172.29.3.10/30
BOGOTA1 BOGOTA3	Se0/1/0 – Se0/0/0	172.29.3.1/30 – 172.29.3.2/30
BOGOTA1 BOGOTA3	Se0/1/1 – Se0/0/1	172.29.3.5/30 – 172.29.3.6/30
BOGOTA2 BOGOTA3	Se0/0/1 – Se0/1/0	172.29.3.13/30 – 172.29.3.14/30
ISP MEDELLIN1	Se0/0/1 – Se0/0/0	209.17.220.1/30 – 209.17.220.2/30
MEDELLIN1 MEDELLIN2	Se0/0/1 – Se0/0/0	172.29.6.1/30 – 172.29.6.2/30
MEDELLIN1 MEDELLIN3	Se0/1/0 – Se0/0/0	172.29.6.13/30 – 172.29.6.14/30
MEDELLIN1 MEDELLIN3	Se0/1/1 – Se0/0/1	172.29.6.9/30 – 172.29.6.10/30
MEDELLIN2 MEDELLIN3	Se0/0/1 – Se0/1/0	172.29.6.5/30 – 172.29.6.6/30

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

2.1. PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

- ### 2.1.1. Paso 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Tabla 25 Configuración protocolo OSPF

Router	Comandos
ISP	<pre>ISP(config)#interface serial 0/0/0 ISP(config-if)#description Conexion ISP-BOGOTA1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown ISP(config-if)#interface serial 0/0/1 ISP(config-if)#description Conexion ISP-MEDELLIN1 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown ISP(config)#router ospf 1 ISP(config-router)#network 209.17.220.4 255.255.255.252 area 1 ISP(config-router)#network 209.17.220.0 255.255.255.252 area 1 ISP(config-router)#no auto-summary ISP(config-router)#exit</pre>
BOGOTA1	<pre>BOGOTA1(config)#interface serial 0/0/0 BOGOTA1(config-if)#description Conexion BOGOTA1-ISP BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown BOGOTA1(config)#interface serial 0/0/1 BOGOTA1(config-if)#description Conexion BOGOTA1-BOGOTA2 BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252 BOGOTA1(config-if)#clock rate 128000</pre>

	<pre> BOGOTA1(config-if)#no shutdown BOGOTA1(config)#interface serial 0/1/0 BOGOTA1(config-if)#description Conexion BOGOTA1-BOGOTA3 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown BOGOTA1(config)#interface serial 0/1/1 BOGOTA1(config-if)#description Conexion BOGOTA1-BOGOTA3 BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#network 209.17.220.4 255.255.255.252 area 1 BOGOTA1(config-router)#network 172.29.3.8 255.255.255.252 area 1 BOGOTA1(config-router)#network 172.29.3.0 255.255.255.252 area 1 BOGOTA1(config-router)#network 172.29.3.4 255.255.255.252 area 1 BOGOTA1(config-router)#no auto-summary BOGOTA1(config-router)#exit </pre>
<p>BOGOTA2</p>	<pre> BOGOTA2(config)#interface Serial 0/0/0 BOGOTA2(config-if)#description Conexion BOGOTA2-BOGOTA1 BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252 BOGOTA2(config-if)#clock rate 128000 BOGOTA2(config-if)#no shutdown BOGOTA2(config)#interface Serial 0/0/1 BOGOTA2(config-if)#description Conexion BOGOTA2-BOGOTA3 BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252 BOGOTA2(config-if)#clock rate 128000 BOGOTA2(config-if)#no shutdown BOGOTA2(config)#router ospf 1 BOGOTA2(config-router)#network 172.29.3.8 255.255.255.252 area 1 </pre>

	<pre> BOGOTA2(config-router)#network 172.29.3.12 255.255.255.252 area 1 BOGOTA2(config-router)#network 172.29.1.0 255.255.255.0 area 1 BOGOTA2(config-router)#no auto-summary BOGOTA2(config-router)#exit </pre>
<p>BOGOTA3</p>	<pre> BOGOTA3(config)#interface serial 0/0/0 BOGOTA3(config-if)#description Conexion BOGOTA3-BOGOTA1 BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA3(config-if)#clock rate 128000 BOGOTA3(config-if)#no shutdown BOGOTA3(config)#interface serial 0/0/1 BOGOTA3(config-if)#description Conexion BOGOTA3-BOGOTA1 BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA3(config-if)#clock rate 128000 BOGOTA3(config-if)#no shutdown BOGOTA3(config)#interface Serial 0/1/0 BOGOTA3(config-if)#description Conexion BOGOTA3-BOGOTA2 BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA3(config-if)#clock rate 128000 BOGOTA3(config-if)#no shutdown BOGOTA3(config)#router ospf 1 BOGOTA3(config-router)#network 172.29.3.0 255.255.255.252 area 1 BOGOTA3(config-router)#network 172.29.3.4 255.255.255.252 area 1 BOGOTA3(config-router)#network 172.29.3.12 255.255.255.252 area 1 BOGOTA3(config-router)#network 172.29.0.0 255.255.255.0 area 1 BOGOTA3(config-router)#no auto-summary BOGOTA3(config-router)#exit </pre>
<p>MEDELLIN1</p>	<pre> MEDELLIN1(config)#interface serial 0/0/0 MEDELLIN1(config-if)#description Conexion MEDELLIN1-ISP MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252 </pre>

	<pre> MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown MEDELLIN1(config)#interface serial 0/0/1 MEDELLIN1(config-if)#description Conexion MEDELLIN1-MEDELLIN2 MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown MEDELLIN1(config-if)#interface serial 0/1/0 MEDELLIN1(config-if)#description Conexion MEDELLIN1-MEDELLIN3 MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown MEDELLIN1(config)#interface serial 0/1/1 MEDELLIN1(config-if)#description Conexion MEDELLIN1-MEDELLIN3 MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#network 209.17.220.0 255.255.255.252 area 1 MEDELLIN1(config-router)#network 172.29.6.0 255.255.255.252 area 1 MEDELLIN1(config-router)#network 172.29.6.8 255.255.255.252 area 1 MEDELLIN1(config-router)#network 172.29.6.12 255.255.255.252 area 1 MEDELLIN1(config-router)#no auto-summary MEDELLIN1(config-router)#exit </pre>
<p>MEDELLIN2</p>	<pre> MEDELLIN2(config)#interface serial 0/0/0 MEDELLIN2(config-if)#description Conexion MEDELLIN2-MEDELLIN1 MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252 MEDELLIN2(config-if)#clock rate 128000 MEDELLIN2(config-if)#no shutdown MEDELLIN2(config)#interface serial 0/0/1 </pre>

	<pre> MEDELLIN2 (config-if) #description Conexion MEDELLIN2-MEDELLIN3 MEDELLIN2 (config-if) #ip address 172.29.6.5 255.255.255.252 MEDELLIN2 (config-if) #clock rate 128000 MEDELLIN2 (config-if) #no shutdown MEDELLIN2 (config) #router ospf 1 MEDELLIN2 (config-router) #network 172.29.6.0 255.255.255.252 area 1 MEDELLIN2 (config-router) #network 172.29.6.4 255.255.255.252 area 1 MEDELLIN2 (config-router) #network 172.29.4.0 255.255.255.0 area 1 MEDELLIN2 (config-router) #no auto-summary MEDELLIN2 (config-router) #exit </pre>
<p>MEDELLIN3</p>	<pre> MEDELLIN3 (config) #interface serial 0/0/0 MEDELLIN3 (config-if) #description Conexion MEDELLIN3-MEDELLIN1 MEDELLIN3 (config-if) #ip address 172.29.6.14 255.255.255.252 MEDELLIN3 (config-if) #clock rate 128000 MEDELLIN3 (config-if) #no shutdown MEDELLIN3 (config) #interface serial 0/0/1 MEDELLIN3 (config-if) #description Conexion MEDELLIN3-MEDELLIN1 MEDELLIN3 (config-if) #ip address 172.29.6.10 255.255.255.252 MEDELLIN3 (config-if) #clock rate 128000 MEDELLIN3 (config-if) #no shutdown MEDELLIN3 (config) #interface serial 0/1/0 MEDELLIN3 (config-if) #description Conexion MEDELLIN3-MEDELLIN2 MEDELLIN3 (config-if) #ip address 172.29.6.6 255.255.255.252 MEDELLIN3 (config-if) #clock rate 128000 MEDELLIN3 (config-if) #no shutdown MEDELLIN3 (config) #router ospf 1 MEDELLIN3 (config-router) #network 172.29.6.8 255.255.255.252 area 1 MEDELLIN3 (config-router) #network 172.29.6.12 255.255.255.252 area 1 MEDELLIN3 (config-router) #network 172.29.6.4 255.255.255.252 area 1 </pre>

	<pre>MEDELLIN3(config-router)#network 172.29.4.128 255.255.255.0 area 1 MEDELLIN3(config-router)#no auto-summary MEDELLIN3(config-router)#exit</pre>
--	--

2.1.2. Paso 2: Los routers Bogotá1 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 26 Configuración OSPF

Router	Comandos
BOGOTA1	<pre>BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#default-information originate BOGOTA1(config-router)#exit</pre>
MEDELLIN1	<pre>MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#default- information originate MEDELLIN1(config-router)#exit</pre>

2.1.3. Paso 3: El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se suman las subredes de cada uno a /22.

Tabla 27 Configuración ruta estática

Router	Comandos
ISP	<pre>ISP(config)#ip route 172.29.0.0 255.255.252.0 serial 0/0/0 ISP(config)#ip route 172.29.4.0 255.255.252.0 serial 0/1/0 ISP(config)#exit</pre>

2.2. PARTE 2: TABLA DE ENRUTAMIENTO

2.2.1. Paso 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Tabla 28 Enrutamiento de los dispositivos

Router	Especificación
--------	----------------

ISP

```

IOS Command Line Interface

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

Gateway of last resort is 209.17.220.6 to network 0.0.0.0

 172.29.0.0/16 is variably subnetted, 9 subnets, 2 masks
S   172.29.0.0/22 is directly connected, Serial0/0/0
O   172.29.3.0/30 [110/128] via 209.17.220.6, 01:28:07, Serial0/0/0
O   172.29.3.4/30 [110/128] via 209.17.220.6, 01:28:07, Serial0/0/0
O   172.29.3.8/30 [110/128] via 209.17.220.6, 01:28:07, Serial0/0/0
O   172.29.3.12/30 [110/192] via 209.17.220.6, 01:28:07, Serial0/0/0
O   172.29.6.0/30 [110/128] via 209.17.220.2, 01:28:07, Serial0/0/1
O   172.29.6.4/30 [110/152] via 209.17.220.2, 01:28:07, Serial0/0/1
O   172.29.6.8/30 [110/128] via 209.17.220.2, 01:28:07, Serial0/0/1
O   172.29.6.12/30 [110/128] via 209.17.220.2, 01:28:07, Serial0/0/1
209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C   209.17.220.0/30 is directly connected, Serial0/0/1
L   209.17.220.1/32 is directly connected, Serial0/0/1
C   209.17.220.4/30 is directly connected, Serial0/0/0
L   209.17.220.5/32 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 209.17.220.6, 00:24:35, Serial0/0/0
      [110/1] via 209.17.220.2, 00:21:04, Serial0/0/1

ISP#
  
```

Ilustración 16 Enrutamiento ISP

BOGOTA1

```

IOS Command Line Interface

BOGOTA1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

 172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
C   172.29.3.0/30 is directly connected, Serial0/1/0
L   172.29.3.1/32 is directly connected, Serial0/1/0
C   172.29.3.4/30 is directly connected, Serial0/1/1
L   172.29.3.5/32 is directly connected, Serial0/1/1
C   172.29.3.8/30 is directly connected, Serial0/0/1
L   172.29.3.9/32 is directly connected, Serial0/0/1
O   172.29.3.12/30 [110/128] via 172.29.3.6, 01:31:46, Serial0/1/1
      [110/128] via 172.29.3.10, 01:31:46, Serial0/0/1
O   172.29.6.0/30 [110/192] via 209.17.220.5, 01:31:46, Serial0/0/0
O   172.29.6.4/30 [110/256] via 209.17.220.5, 01:31:46, Serial0/0/0
O   172.29.6.8/30 [110/192] via 209.17.220.5, 01:31:46, Serial0/0/0
O   172.29.6.12/30 [110/192] via 209.17.220.5, 01:31:46, Serial0/0/0
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
O   209.17.220.0/30 [110/128] via 209.17.220.5, 01:31:46, Serial0/0/0
C   209.17.220.4/30 is directly connected, Serial0/0/0
L   209.17.220.6/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 is directly connected, Serial0/0/0

BOGOTA1#
  
```

Ilustración 17 Enrutamiento BOGOTA1

BOGOTA2

```

BOGOTA2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.29.3.9 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 10 subnets, 2 masks
O 172.29.3.0/30 [110/128] via 172.29.3.14, 01:34:34, Serial0/0/1
  [110/128] via 172.29.3.9, 01:34:34, Serial0/0/0
O 172.29.3.4/30 [110/128] via 172.29.3.14, 01:34:34, Serial0/0/1
  [110/128] via 172.29.3.9, 01:34:34, Serial0/0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
L 172.29.3.10/32 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
L 172.29.3.13/32 is directly connected, Serial0/0/1
O 172.29.6.0/30 [110/256] via 172.29.3.9, 01:34:34, Serial0/0/0
O 172.29.6.4/30 [110/320] via 172.29.3.9, 01:34:34, Serial0/0/0
O 172.29.6.8/30 [110/256] via 172.29.3.9, 01:34:34, Serial0/0/0
O 172.29.6.12/30 [110/256] via 172.29.3.9, 01:34:34, Serial0/0/0
O 209.17.220.0/30 is subnetted, 2 subnets
O 209.17.220.0/30 [110/192] via 172.29.3.9, 01:34:34, Serial0/0/0
O 209.17.220.4/30 [110/128] via 172.29.3.9, 01:34:34, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:31:09, Serial0/0/0
BOGOTA2#

```

Ilustración 18 Enrutamiento BOGOTA2

BOGOTA3

```

BOGOTA3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
C 172.29.3.0/30 is directly connected, Serial0/0/0
L 172.29.3.2/32 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
L 172.29.3.6/32 is directly connected, Serial0/0/1
O 172.29.3.8/30 [110/128] via 172.29.3.13, 01:37:24, Serial0/1/0
  [110/128] via 172.29.3.1, 01:37:24, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/1/0
L 172.29.3.14/32 is directly connected, Serial0/1/0
O 172.29.6.0/30 [110/256] via 172.29.3.1, 01:37:14, Serial0/0/0
O 172.29.6.4/30 [110/320] via 172.29.3.1, 01:37:14, Serial0/0/0
O 172.29.6.8/30 [110/256] via 172.29.3.1, 01:37:14, Serial0/0/0
O 172.29.6.12/30 [110/256] via 172.29.3.1, 01:37:14, Serial0/0/0
O 209.17.220.0/30 is subnetted, 2 subnets
O 209.17.220.0/30 [110/192] via 172.29.3.1, 01:37:14, Serial0/0/0
O 209.17.220.4/30 [110/128] via 172.29.3.1, 01:37:24, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:33:49, Serial0/0/0
BOGOTA3#

```

Ilustración 19 Enrutamiento BOGOTA3

MEDELLIN1

```

MEDELLIN1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
O 172.29.3.0/30 [110/192] via 209.17.220.1, 01:38:19, Serial0/0/0
O 172.29.3.4/30 [110/192] via 209.17.220.1, 01:38:19, Serial0/0/0
O 172.29.3.8/30 [110/192] via 209.17.220.1, 01:38:19, Serial0/0/0
O 172.29.3.12/30 [110/256] via 209.17.220.1, 01:38:19, Serial0/0/0
C 172.29.6.0/30 is directly connected, Serial0/0/1
L 172.29.6.1/32 is directly connected, Serial0/0/1
O 172.29.6.4/30 [110/128] via 172.29.6.2, 01:38:19, Serial0/0/1
  [110/128] via 172.29.6.10, 01:38:19, Serial0/1/1
C 172.29.6.8/30 is directly connected, Serial0/1/1
L 172.29.6.9/32 is directly connected, Serial0/1/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
L 172.29.6.13/32 is directly connected, Serial0/1/0
L 209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/0/0
L 209.17.220.2/32 is directly connected, Serial0/0/0
O 209.17.220.4/30 [110/128] via 209.17.220.1, 01:38:19, Serial0/0/0
S* 0.0.0.0/0 is directly connected, Serial0/0/0

MEDELLIN1#

```

Ilustración 20 Enrutamiento MEDELLIN1

MEDELLIN2

```

MEDELLIN2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

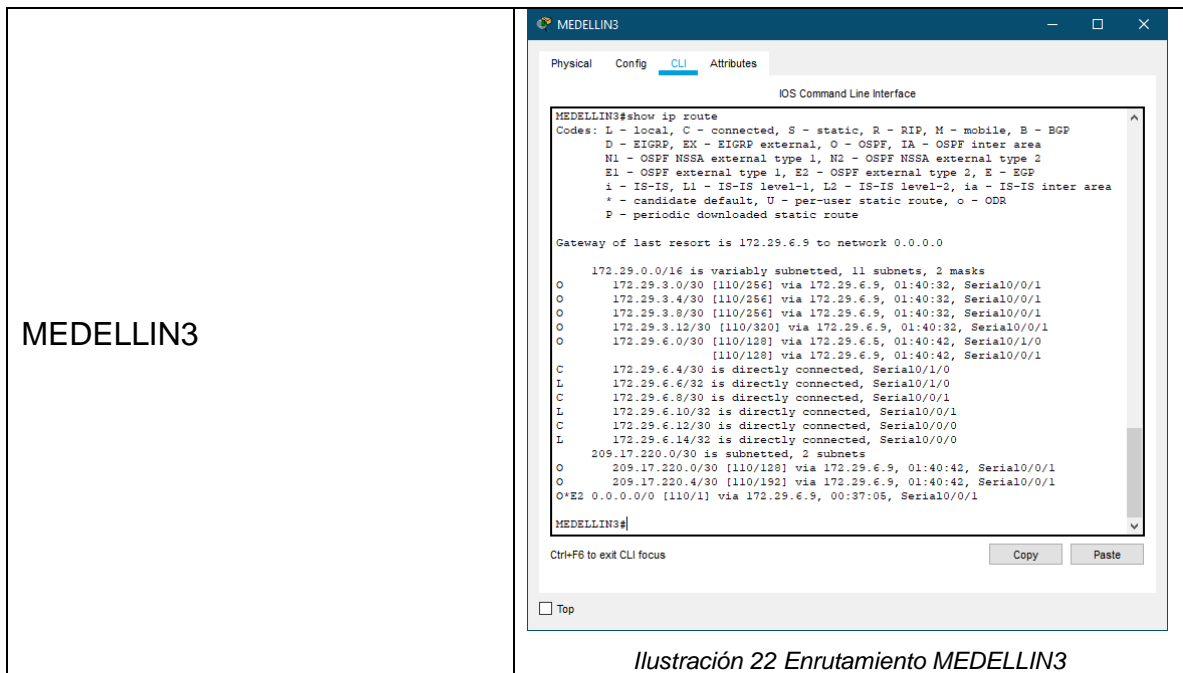
Gateway of last resort is 172.29.6.1 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 10 subnets, 2 masks
O 172.29.3.0/30 [110/256] via 172.29.6.1, 01:39:37, Serial0/0/0
O 172.29.3.4/30 [110/256] via 172.29.6.1, 01:39:37, Serial0/0/0
O 172.29.3.8/30 [110/256] via 172.29.6.1, 01:39:37, Serial0/0/0
O 172.29.3.12/30 [110/320] via 172.29.6.1, 01:39:37, Serial0/0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
L 172.29.6.2/32 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
L 172.29.6.5/32 is directly connected, Serial0/0/1
O 172.29.6.8/30 [110/128] via 172.29.6.6, 01:39:47, Serial0/0/1
  [110/128] via 172.29.6.1, 01:39:47, Serial0/0/0
O 172.29.6.12/30 [110/128] via 172.29.6.6, 01:39:47, Serial0/0/1
  [110/128] via 172.29.6.1, 01:39:47, Serial0/0/0
O 209.17.220.0/30 is subnetted, 2 subnets
O 209.17.220.0/30 [110/128] via 172.29.6.1, 01:39:47, Serial0/0/0
O 209.17.220.4/30 [110/192] via 172.29.6.1, 01:39:37, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:36:10, Serial0/0/0

MEDELLIN2#

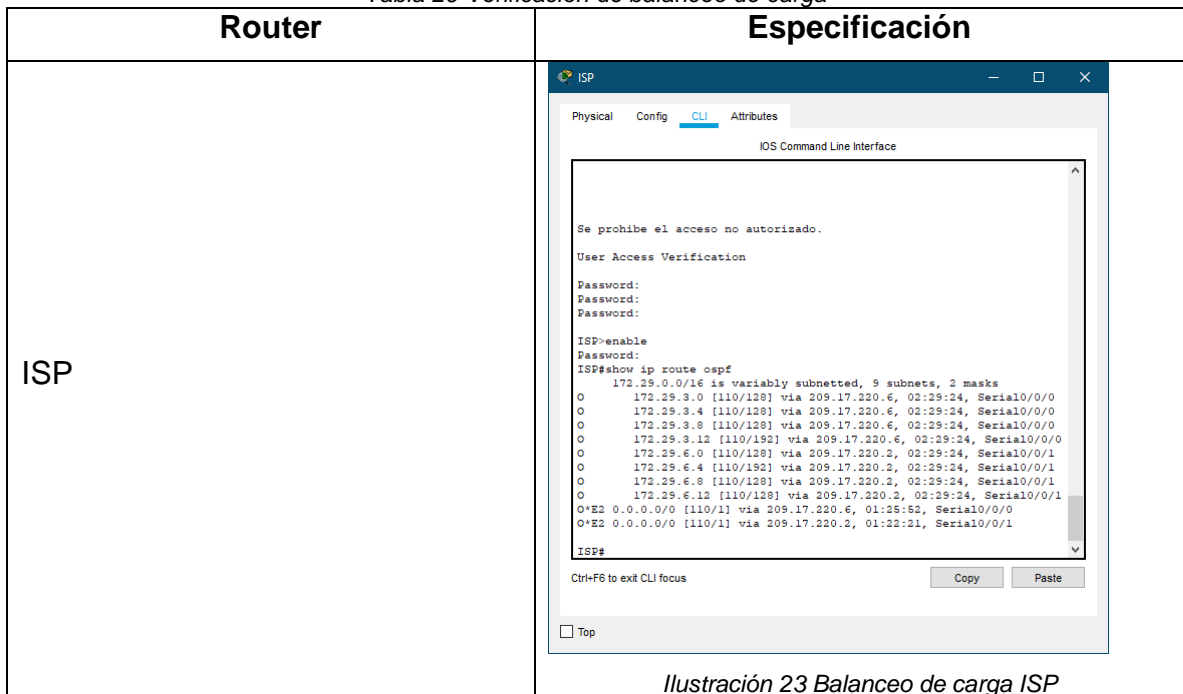
```

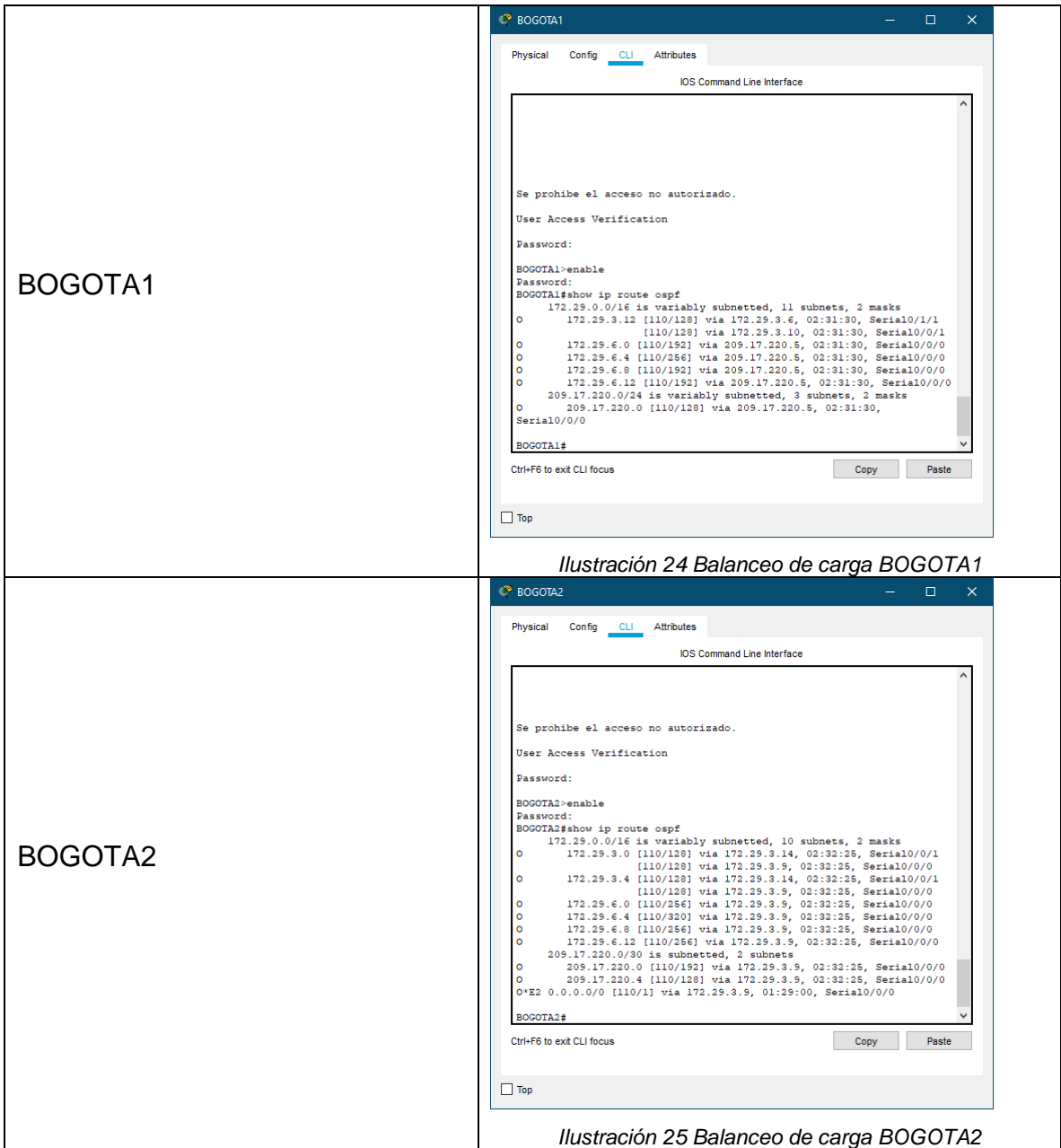
Ilustración 21 Enrutamiento MEDELLIN2



2.2.2. Paso 2: Verificar el balanceo de carga que presentan los routers.

Tabla 29 Verificación de balanceo de carga





BOGOTA3

```
IOS Command Line Interface

Se prohíbe el acceso no autorizado.

User Access Verification

Password:

BOGOTA3>enable
Password:
BOGOTA3#show ip route ospf
 172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
O   172.29.3.8 [110/128] via 172.29.3.1, 02:33:42, Serial0/1/0
O   172.29.6.0 [110/256] via 172.29.3.1, 02:33:32, Serial0/0/0
O   172.29.6.4 [110/320] via 172.29.3.1, 02:33:32, Serial0/0/0
O   172.29.6.8 [110/256] via 172.29.3.1, 02:33:32, Serial0/0/0
O   172.29.6.12 [110/256] via 172.29.3.1, 02:33:32, Serial0/0/0
209.17.220.0/30 is subnetted, 2 subnets
O   209.17.220.0 [110/192] via 172.29.3.1, 02:33:32, Serial0/0/0
O   209.17.220.4 [110/128] via 172.29.3.1, 02:33:42, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 01:30:07, Serial0/0/0

BOGOTA3#

Ctrl+F6 to exit CLI focus
```

Ilustración 26 Balanceo de carga BOGOTA3

MEDELLIN1

```
IOS Command Line Interface

Se prohíbe el acceso no autorizado.

User Access Verification

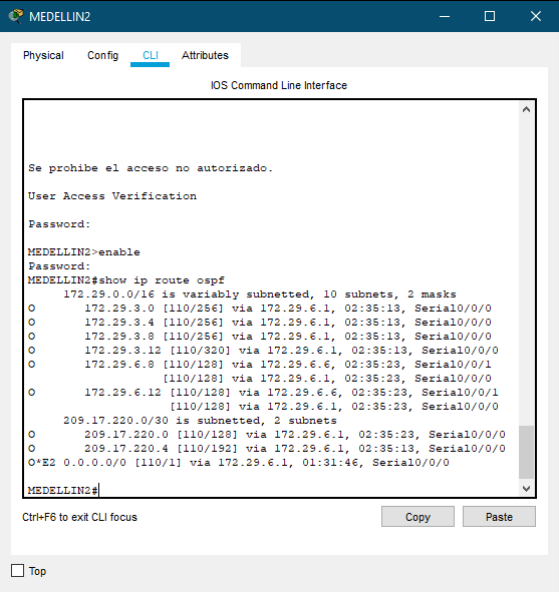

Password:

MEDELLIN1>enable
Password:
MEDELLIN1#show ip route ospf
 172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
O   172.29.3.0 [110/192] via 209.17.220.1, 02:34:40, Serial0/0/0
O   172.29.3.4 [110/192] via 209.17.220.1, 02:34:40, Serial0/0/0
O   172.29.3.8 [110/192] via 209.17.220.1, 02:34:40, Serial0/0/0
O   172.29.3.12 [110/256] via 209.17.220.1, 02:34:40, Serial0/0/0
O   172.29.6.4 [110/128] via 172.29.6.2, 02:34:40, Serial0/0/1
    [110/128] via 172.29.6.10, 02:34:40, Serial0/1/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
O   209.17.220.4 [110/128] via 209.17.220.1, 02:34:40,
Serial0/0/0

MEDELLIN1#

Ctrl+F6 to exit CLI focus
```

Ilustración 27 Balanceo de carga MEDELLIN1

<p>MEDELLIN2</p>	 <p>MEDELLIN2</p>
<p><i>Ilustración 28 Balanceo de carga MEDELLIN2</i></p>	
<p>MEDELLIN3</p>	 <p>MEDELLIN3</p>
<p><i>Ilustración 29 Balanceo de carga MEDELLIN3</i></p>	

2.2.3. Paso 3: 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.

Tabla 30 Validación de los routers

Router	Especificación
--------	----------------

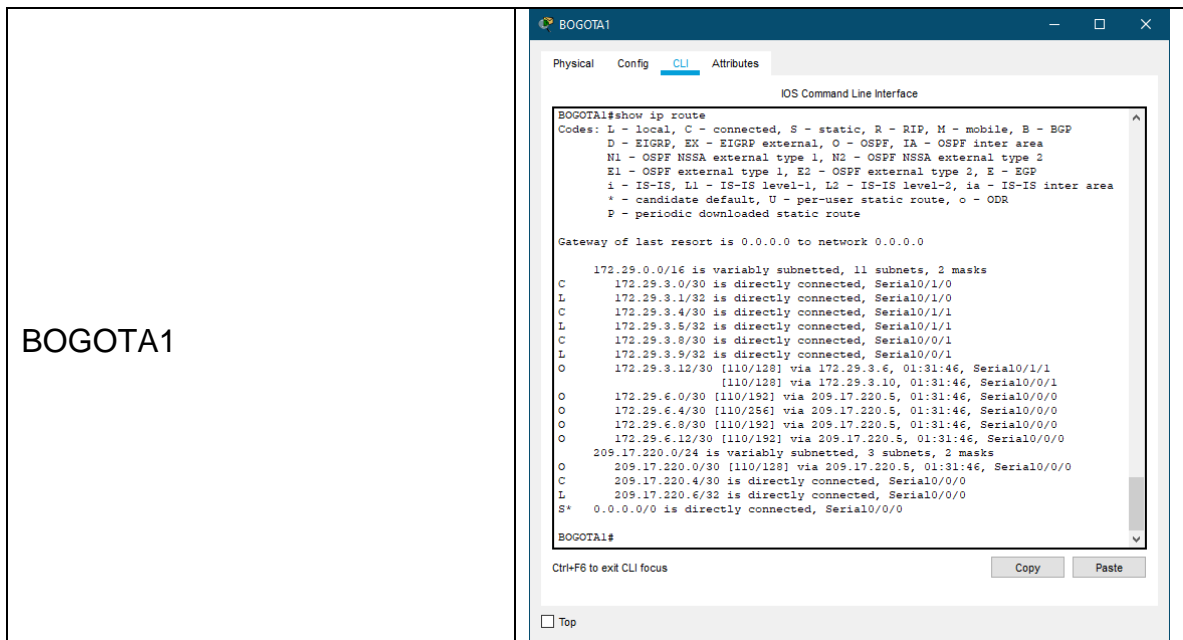


Ilustración 30 Validación BOGOTA1

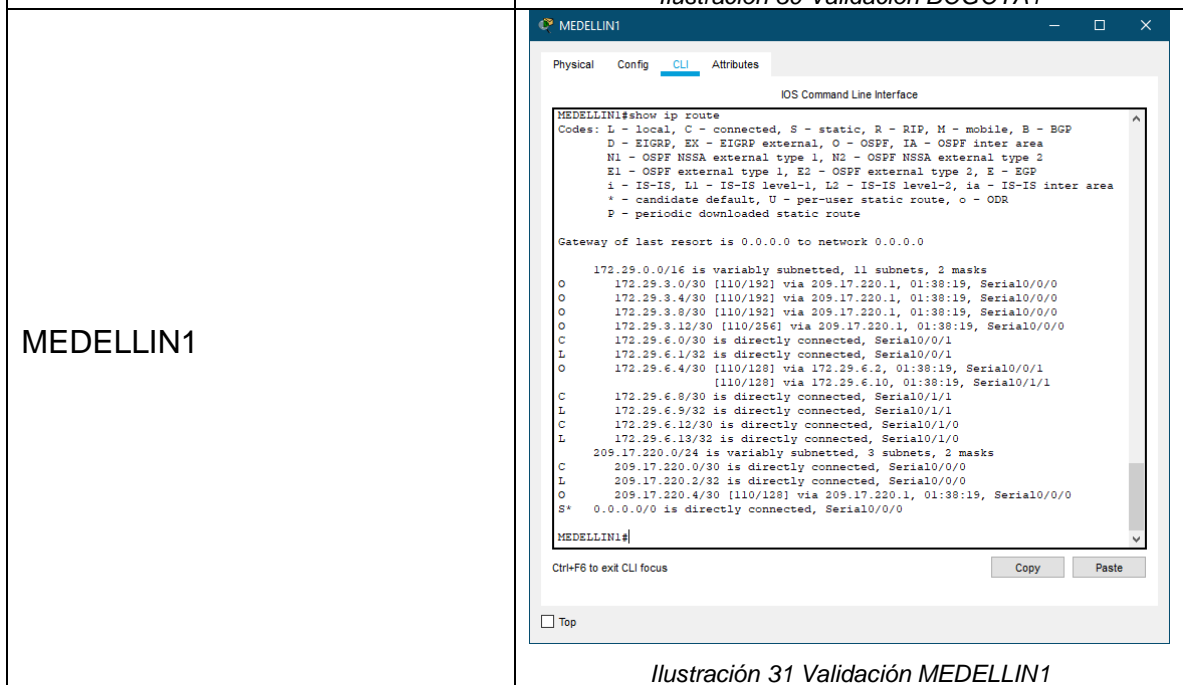


Ilustración 31 Validación MEDELLIN1

2.2.4. Paso 4: Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

Tabla 31 Conexiones OSPF

Router	Especificación
--------	----------------

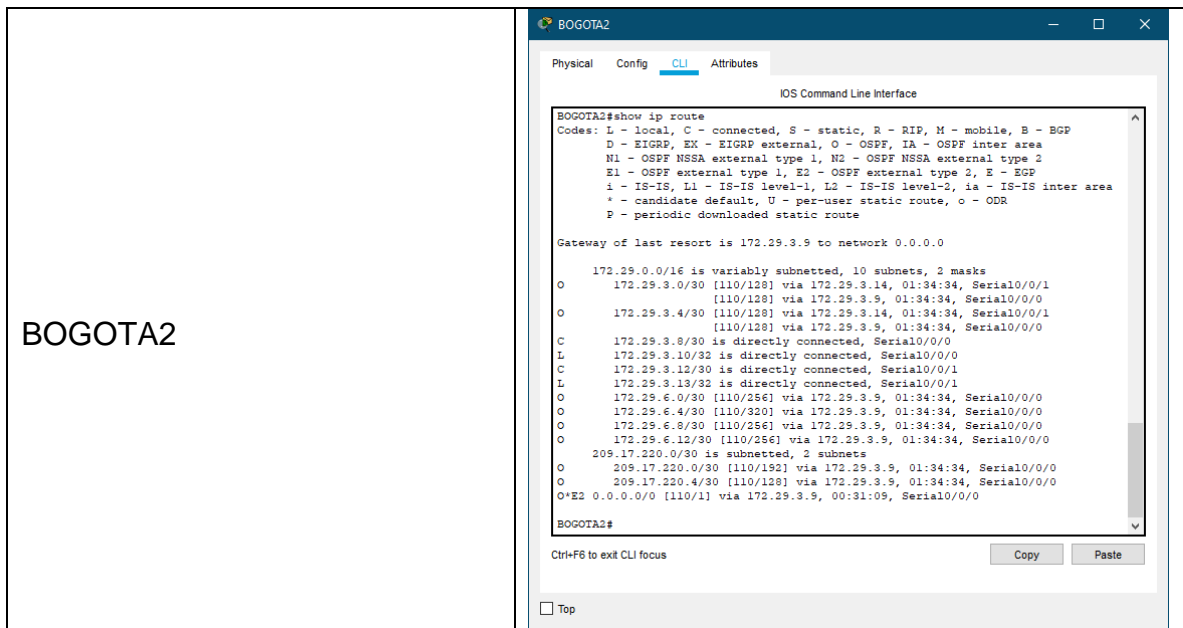


Ilustración 32 OSPF BOGOTA2

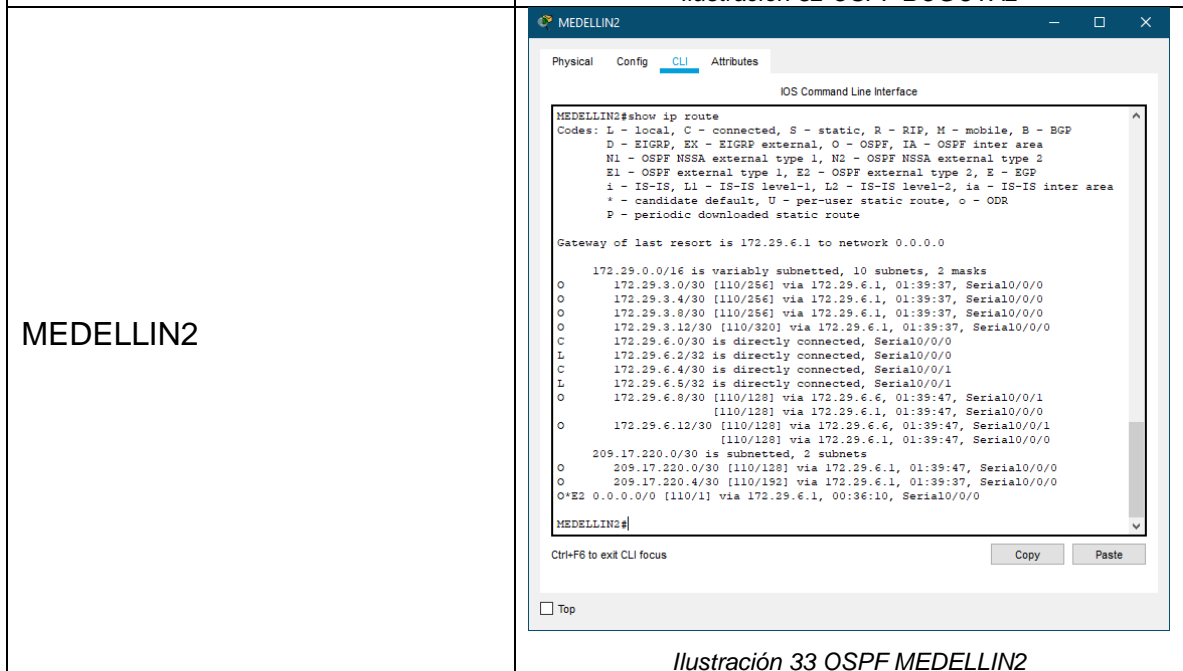


Ilustración 33 OSPF MEDELLIN2

2.2.5. Paso 5: Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Tabla 32 Rutas routers

Router	Especificación
--------	----------------

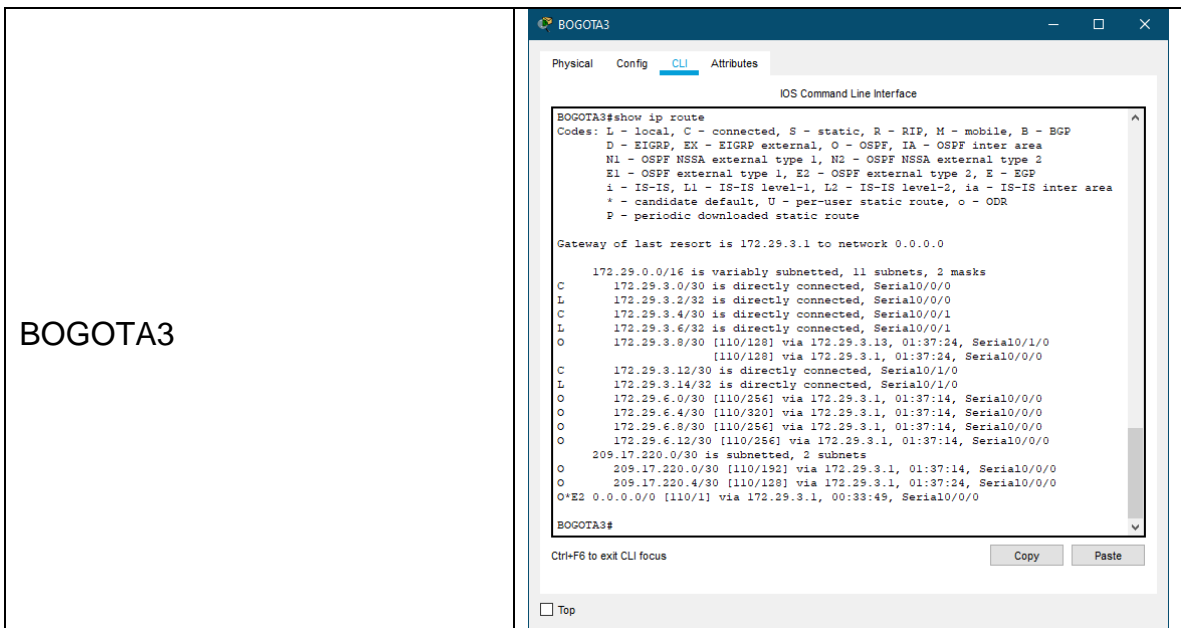


Ilustración 34 Rutas BOGOTA3

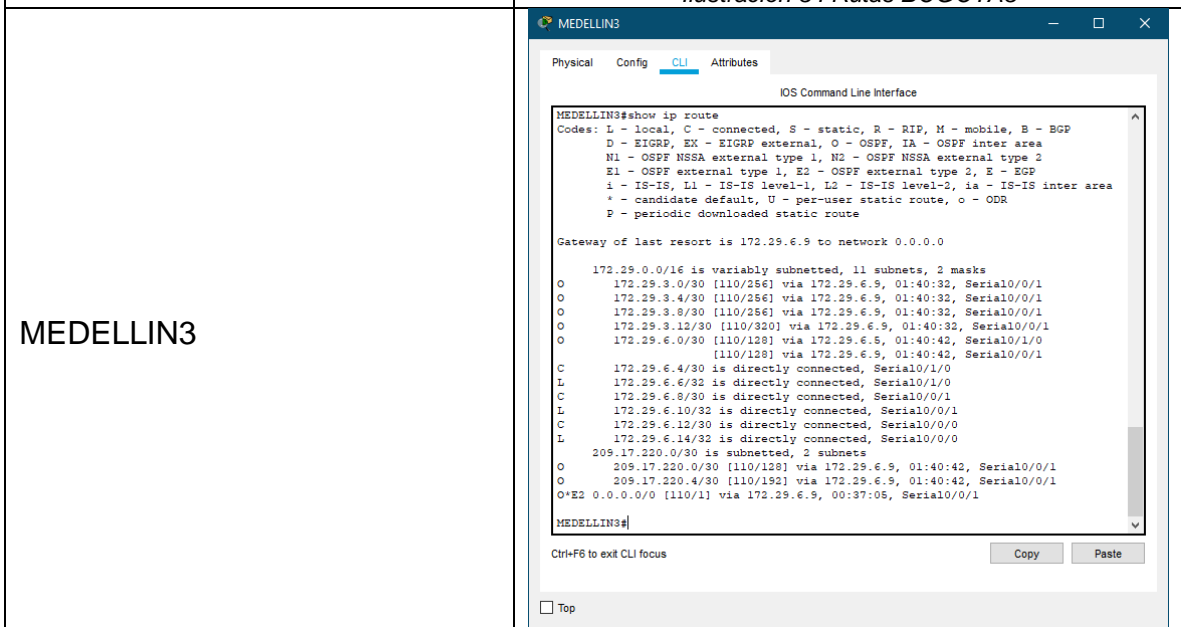


Ilustración 35 Rutas MEDELLIN3

2.2.6. Paso 6: El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Tabla 33 Rutas estáticas

Router	Especificación
--------	----------------

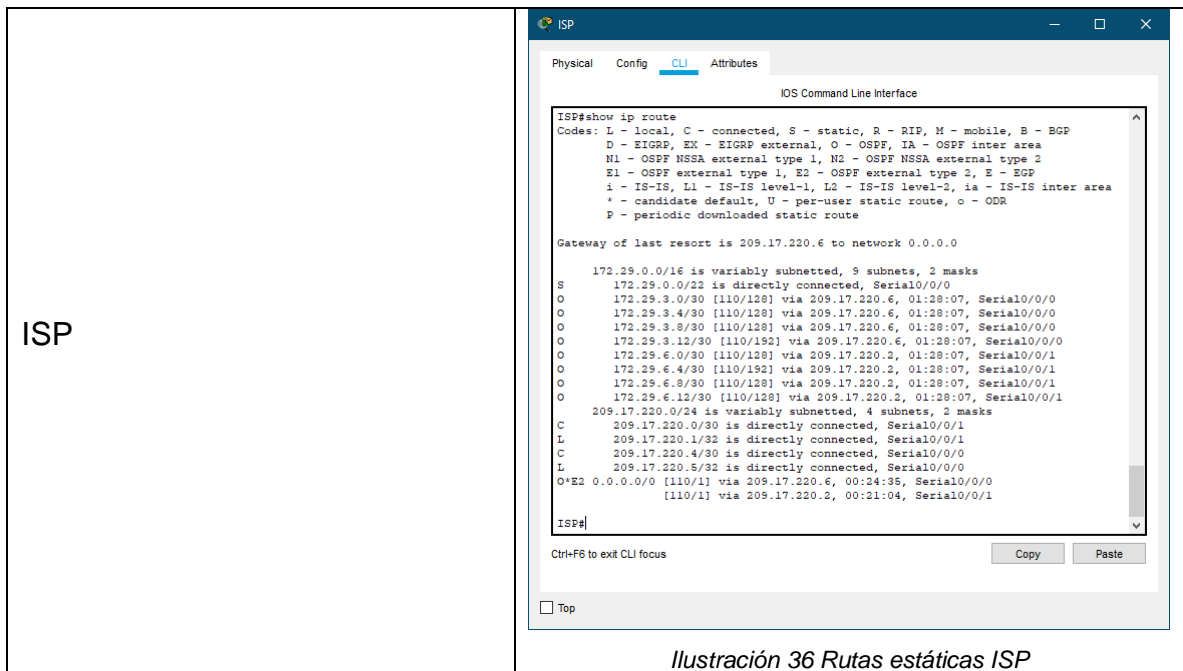


Ilustración 36 Rutas estáticas ISP

2.3. PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF

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

Tabla 34 Interfaces que no necesitan desactivación

Router	Interfaz
Bogotá1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogotá2	SERIAL0/0/0; SERIAL0/0/1
Bogotá3	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

Tabla 35 Desactivación de interfaces

Router	Comandos
BOGOTA3	BOGOTA3(config)#route ospf 1 BOGOTA3(config-router)#passive-interface serial 0/1/1

	BOGOTA3 (config-router) #exit
MEDELLIN3	MEDELLIN3 (config) #route ospf 1 MEDELLIN3 (config-router) #passive-interface serial 0/1/1 MEDELLIN3 (config-router) #exit

2.4. PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF

2.4.1. Paso 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.

Tabla 36 Protocolo OSPF

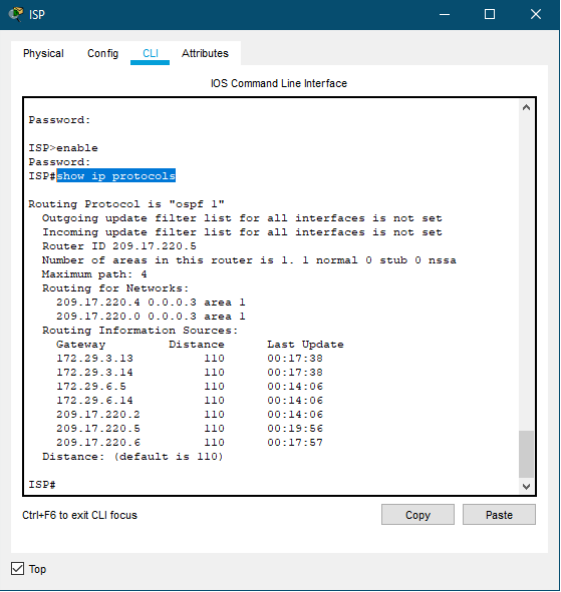
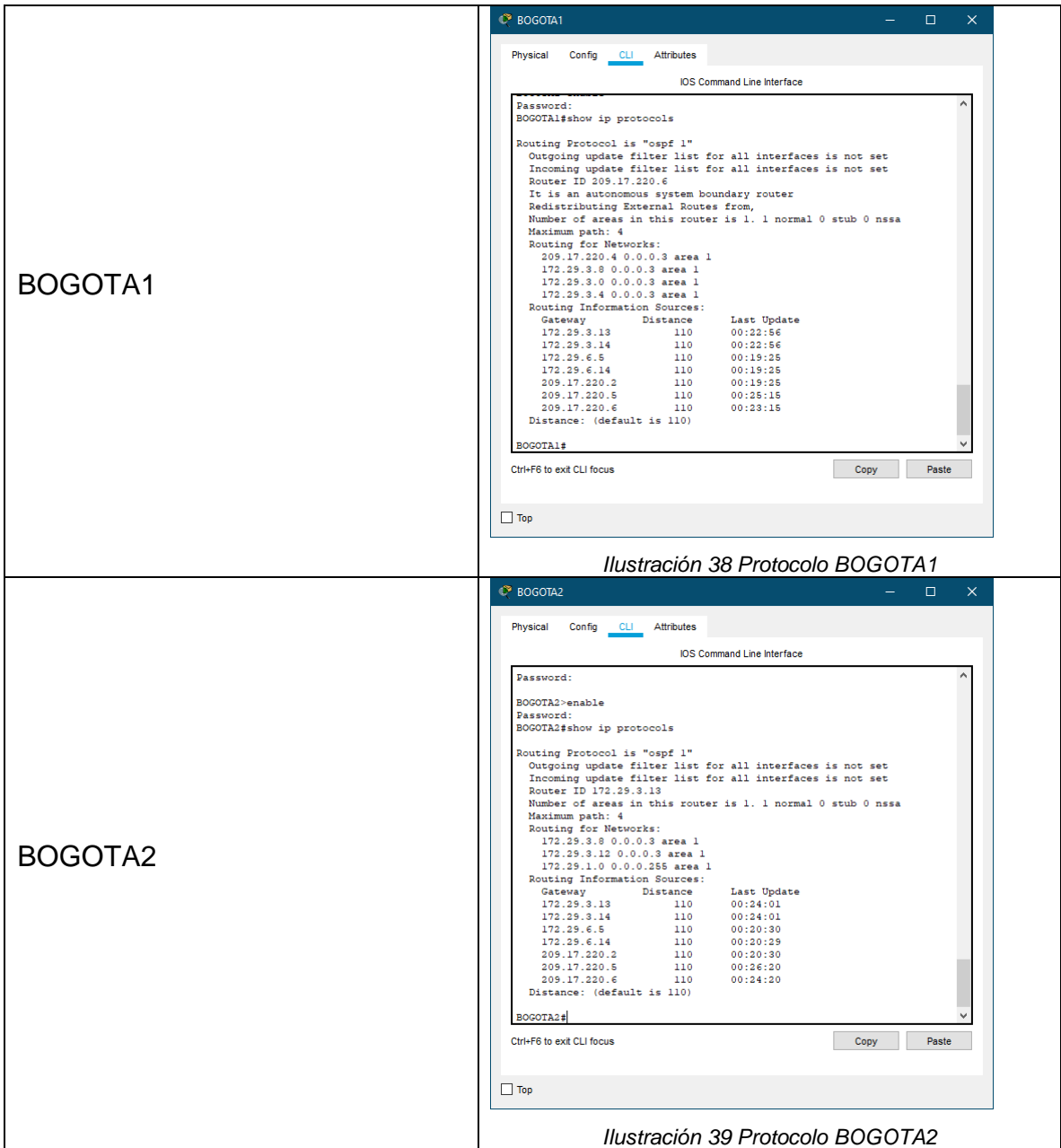
Router	Especificación
ISP	 <pre> Password: ISP>enable Password: ISP# show ip protocols Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 209.17.220.5 Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 209.17.220.4 0.0.0.3 area 1 209.17.220.0 0.0.0.3 area 1 Routing Information Sources: Gateway Distance Last Update 172.29.3.13 110 00:17:38 172.29.3.14 110 00:17:38 172.29.6.5 110 00:14:06 172.29.6.14 110 00:14:06 209.17.220.2 110 00:14:06 209.17.220.5 110 00:19:56 209.17.220.6 110 00:17:57 Distance: (default is 110) ISP# </pre> <p>Ctrl+F6 to exit CLI focus</p> <p><input checked="" type="checkbox"/> Top</p>

Ilustración 37 Protocolo ISP



BOGOTA3

```
BOGOTA3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.3.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.12 0.0.0.3 area 1
    172.29.0.0 0.0.0.255 area 1
  Passive Interface(s):
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
  172.29.3.13       110           00:24:44
  172.29.3.14       110           00:24:44
  172.29.6.5        110           00:21:13
  172.29.6.14       110           00:21:13
  209.17.220.2      110           00:21:14
  209.17.220.5      110           00:27:03
  209.17.220.6      110           00:25:04
  Distance: (default is 110)

BOGOTA3#
```

Ilustración 40 Protocolo BOGOTA3

MEDELLIN1

```
MEDELLIN1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.2
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.0 0.0.0.3 area 1
    172.29.6.0 0.0.0.3 area 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
  172.29.3.13       110           00:26:12
  172.29.3.14       110           00:26:12
  172.29.6.5        110           00:22:41
  172.29.6.14       110           00:22:41
  209.17.220.2      110           00:22:41
  209.17.220.5      110           00:28:31
  209.17.220.6      110           00:26:31
  Distance: (default is 110)

MEDELLIN1#
```

Ilustración 41 Protocolo MEDELLIN1

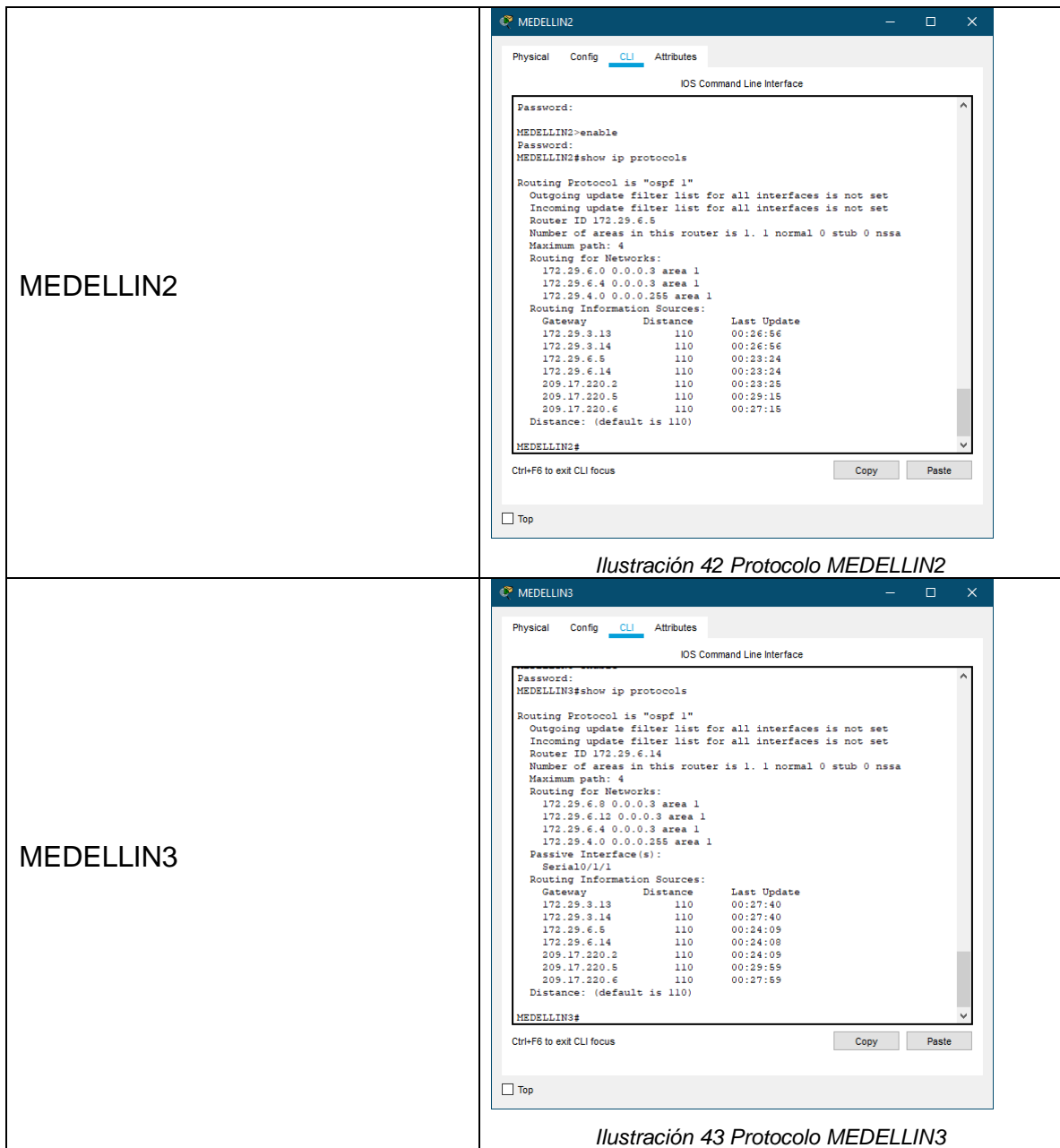


Ilustración 42 Protocolo MEDELLIN2

Ilustración 43 Protocolo MEDELLIN3

2.4.2. Paso 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.

Tabla 37 Base de datos de OSPF

Router	Especificación
--------	----------------

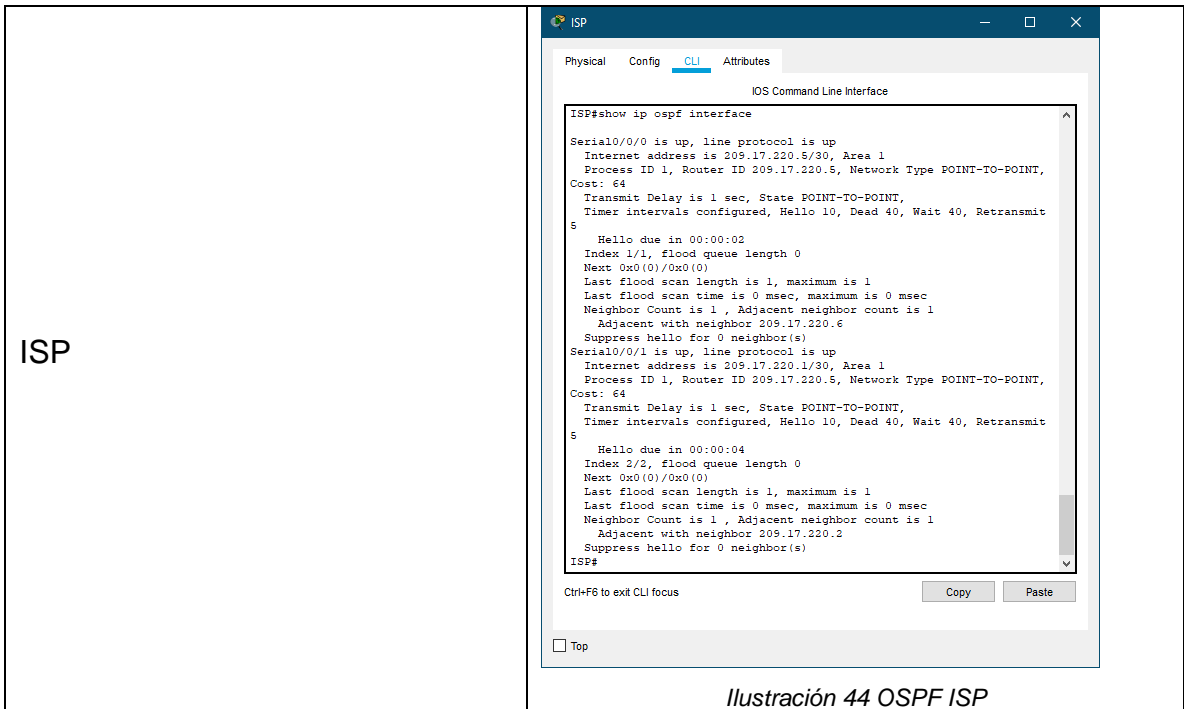
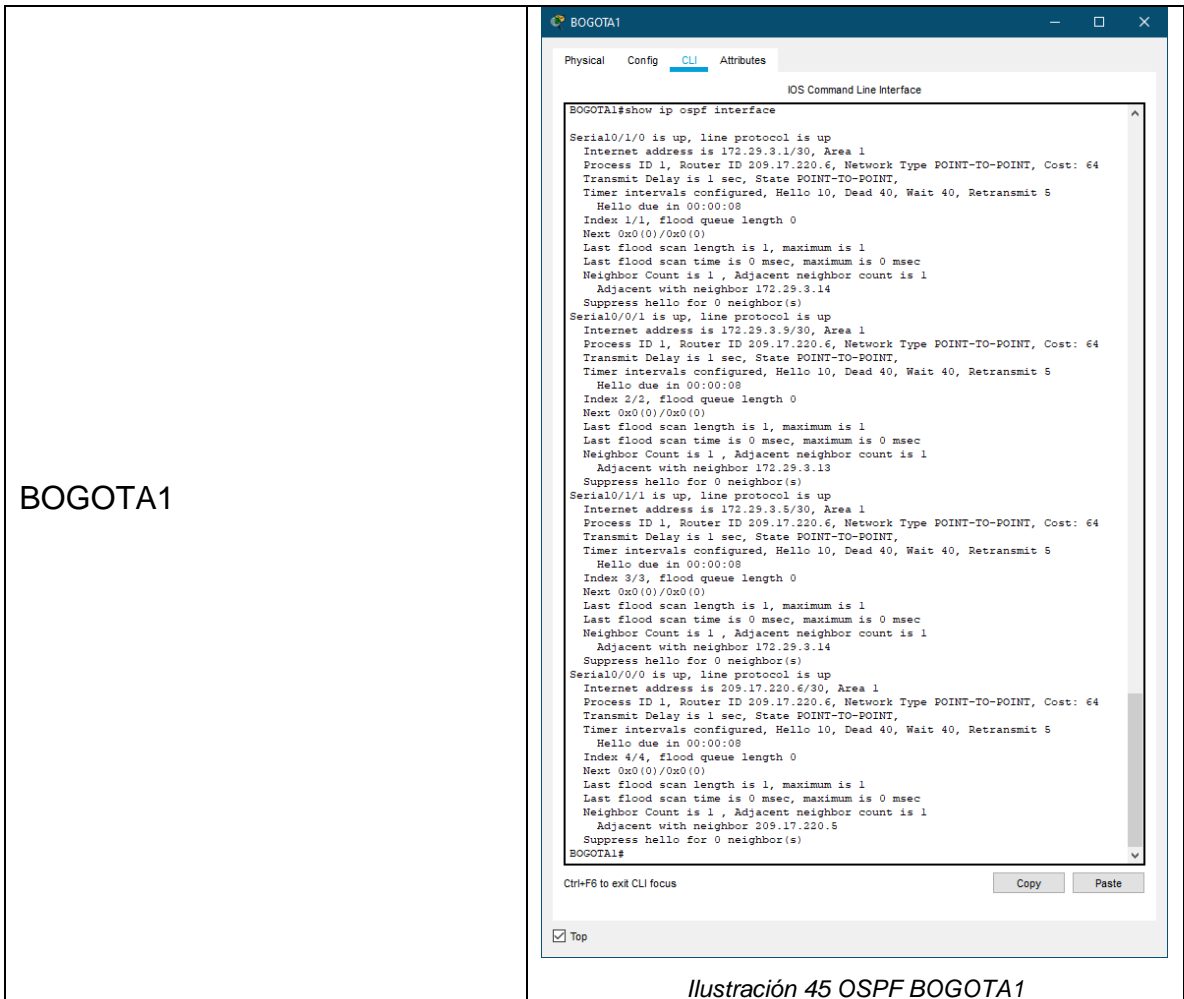


Ilustración 44 OSPF ISP



BOGOTA1

Ilustración 45 OSPF BOGOTA1

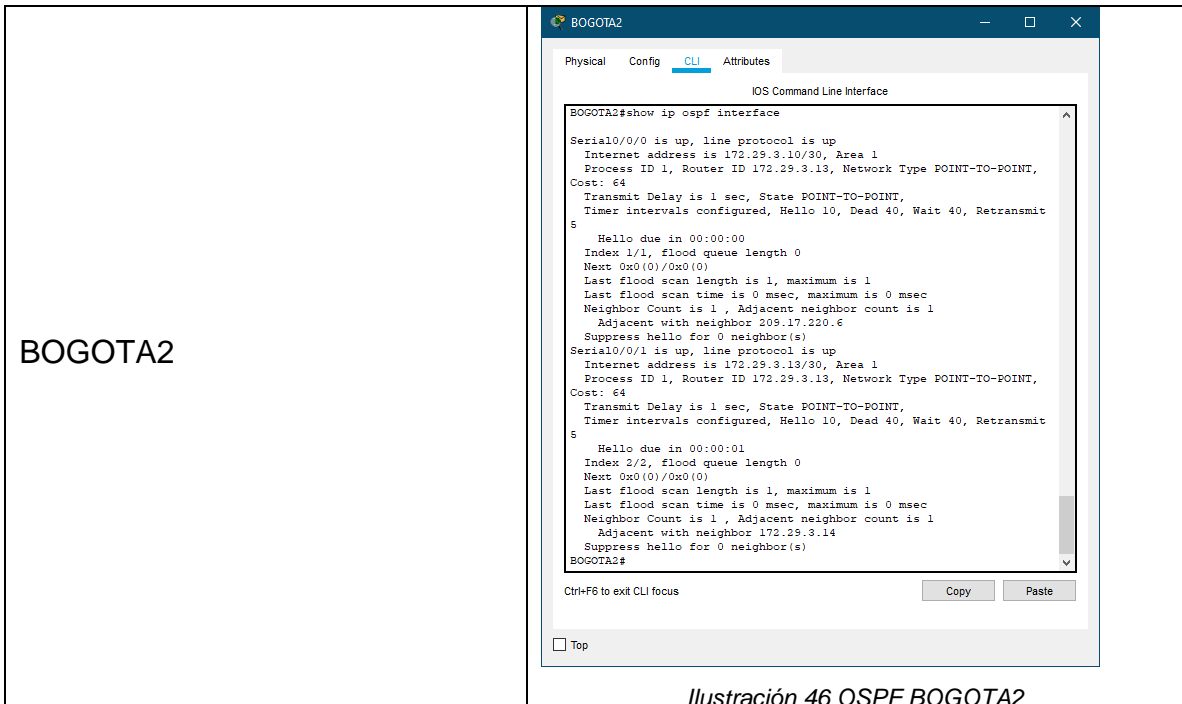


Ilustración 46 OSPF BOGOTA2

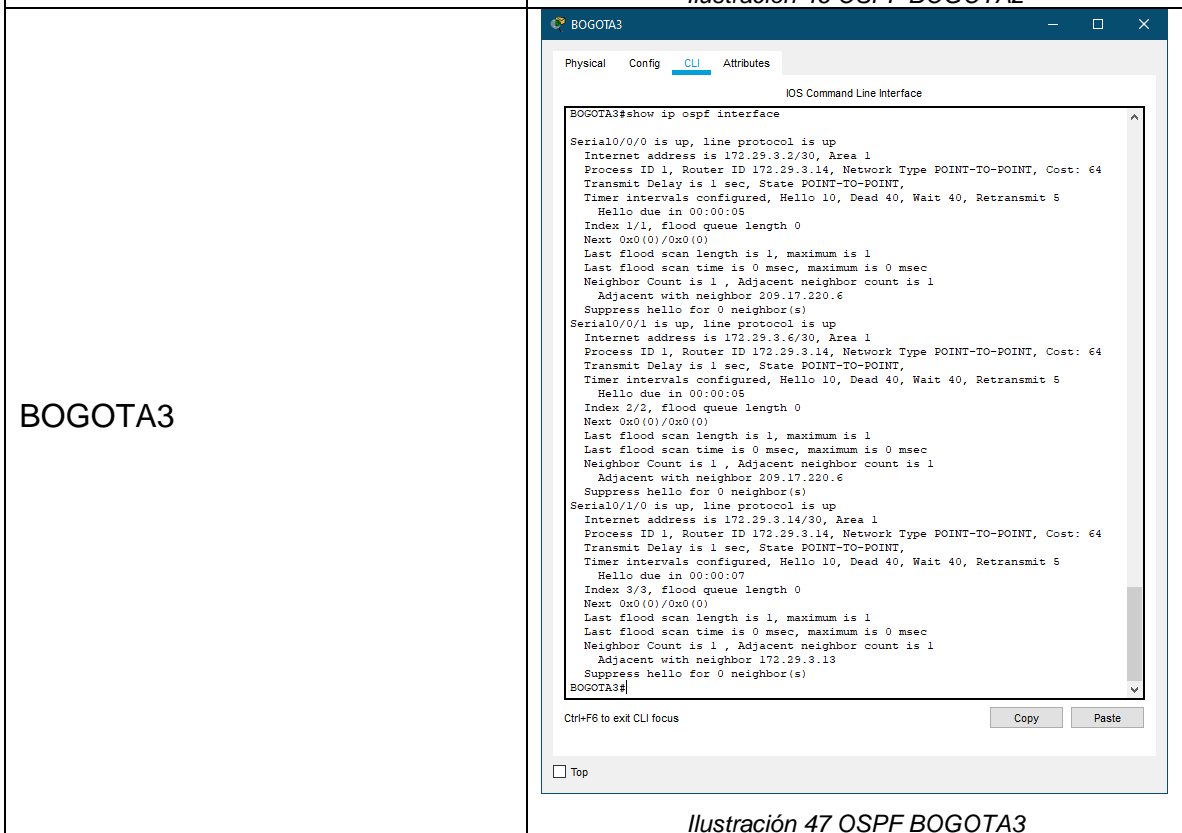


Ilustración 47 OSPF BOGOTA3

MEDELLIN1

The screenshot shows a network device's CLI window with the following content:

```
MEDELLIN1#show ip ospf interface
Serial0/0/1 is up, line protocol is up
Internet address is 172.29.6.1/30, Area 1
Process ID 1, Router ID 209.17.220.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 172.29.6.5
Suppress hello for 0 neighbor(s)
Serial0/1/0 is up, line protocol is up
Internet address is 172.29.6.13/30, Area 1
Process ID 1, Router ID 209.17.220.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 172.29.6.14
Suppress hello for 0 neighbor(s)
Serial0/1/1 is up, line protocol is up
Internet address is 172.29.6.9/30, Area 1
Process ID 1, Router ID 209.17.220.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 172.29.6.14
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet address is 209.17.220.2/30, Area 1
Process ID 1, Router ID 209.17.220.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 209.17.220.5
Suppress hello for 0 neighbor(s)
MEDELLIN1#
```

At the bottom of the window, there are buttons for "Copy" and "Paste", and a "Top" link.

Ilustración 48 OSPF MEDELLIN1

MEDELLIN2

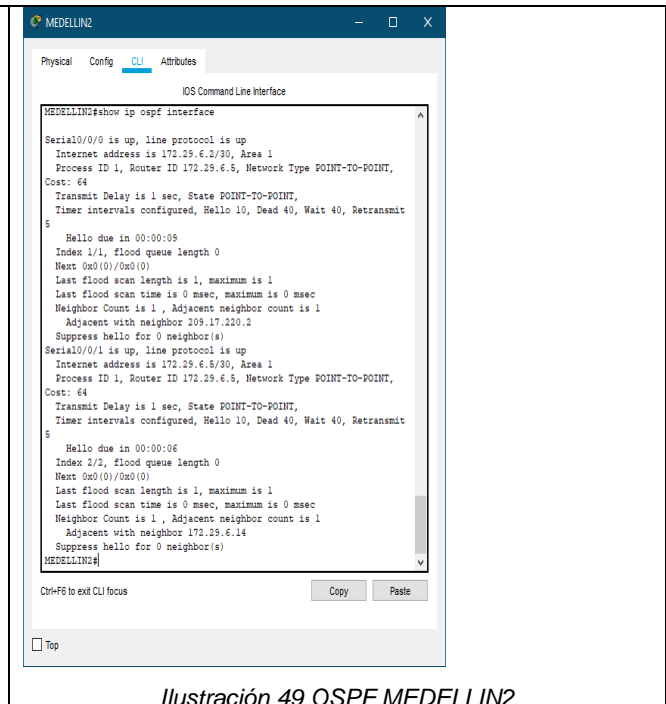


Ilustración 49 OSPF MEDELLIN2

MEDELLIN3

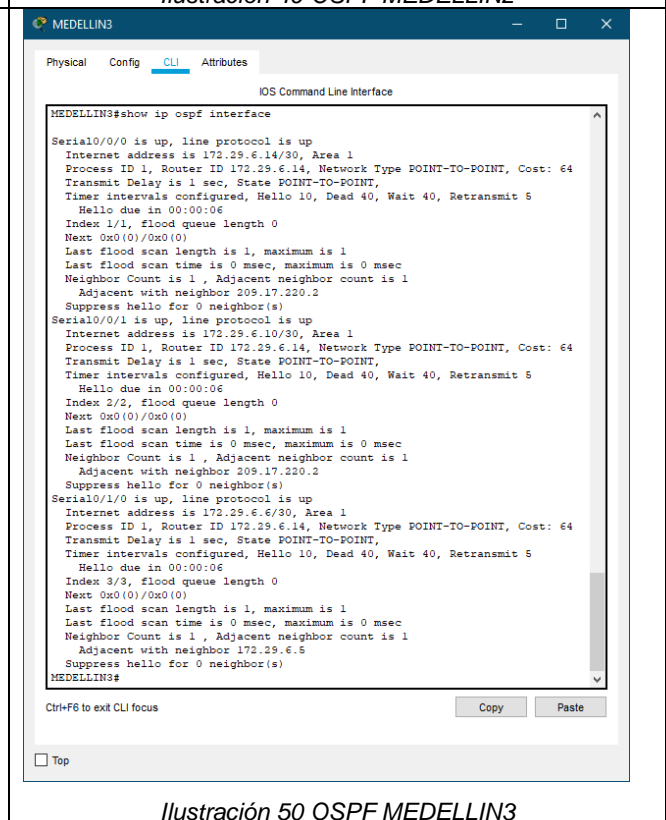


Ilustración 50 OSPF MEDELLIN3

2.5. PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

2.5.1. Paso 1: Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

Tabla 38 Autenticación PAT

Router	Comandos
ISP	<pre>ISP(config)#interface serial 0/0/1 ISP(config-if)#encapsulation PPP ISP(config-if)#PPP authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config-if)#exit</pre>
MEDELLIN1	<pre>MEDELLIN1(config)#interface serial 0/0/0 MEDELLIN1(config-if)#encapsulation PPP MEDELLIN1(config-if)#PPP authentication pap MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco MEDELLIN1(config-if)#exit</pre>

2.5.2. Paso 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Tabla 39 Autenticación CHAT

Router	Comandos
ISP	<pre>ISP(config)#interface serial 0/0/0 ISP(config-if)#encapsulation PPP ISP(config-if)#ppp authentication chap ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config-if)#exit</pre>
BOGOTA1	<pre>BOGOTA1(config)#interface serial 0/0/0 BOGOTA1(config-if)#encapsulation PPP BOGOTA1(config-if)#ppp authentication chap BOGOTA1(config-if)#ppp pap sent-username BOGOTA1 password cisco BOGOTA1(config-if)#exit</pre>

2.6. PARTE 6: CONFIGURACIÓN DE NAT

2.6.1. Paso 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.

2.6.2. Paso 2: 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, con diferente puerto.

Tabla 40 Configuración NAT MEDELLIN1

Router	Comandos
MEDELLIN1	<pre> MEDELLIN1(config)#ip access-list standard host MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255 MEDELLIN1(config-std-nacl)#exit MEDELLIN1(config)#ip nat inside source list host interface serial 0/0/0 overload MEDELLIN1(config)#interface serial 0/0/0 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#interface serial 0/0/1 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#interface serial 0/1/0 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#interface serial 0/1/1 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#exit MEDELLIN1(config)# </pre>

2.6.3. Paso 3: 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, con diferente puerto.

Tabla 41 Configuración NAT BOGOTA1

Router	Comandos
--------	----------

BOGOTA1	<pre> BOGOTA1(config)#ip access-list standard host BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255 BOGOTA1(config-std-nacl)#exit BOGOTA1(config)#ip nat inside source list host interface serial 0/0/0 overload BOGOTA1(config)#interface serial 0/0/0 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#interface serial 0/0/1 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#interface serial 0/1/0 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#interface serial 0/1/1 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#exit BOGOTA1(config)# </pre>
----------------	---

2.7. PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP

2.7.1. Paso 1: Configurar la red Medellín2 y Medellín3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

Tabla 42 Configuración DHCP Medellín

Router	Comandos
MEDELLIN2	<pre> MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5 MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133 MEDELLIN2(config)#ip dhcp pool MEDELLIN2 MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.1 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp pool MEDELLIN3 MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.129 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit </pre>

2.7.2. Paso 2: El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

Tabla 43 Configuración broadcast MEDELLIN3

Router	Comandos
MEDELLIN3	<pre>MEDELLIN3(config)#interface serial 0/1/0 MEDELLIN3(config-if)#ip helper-address 172.29.6.5 MEDELLIN3(config-if)#exit</pre>

2.7.3. Paso 3: Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

Tabla 44 Configuración DHCP Bogotá

Router	Comandos
MEDELLIN2	<pre>MEDELLIN2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4 MEDELLIN2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.4 MEDELLIN2(config)#ip dhcp pool BOGOTA2 MEDELLIN2(dhcp-config)#network 172.29.1.0 255.255.255.0 MEDELLIN2(dhcp-config)#default-router 172.29.1.1 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp pool BOGOTA3 MEDELLIN2(dhcp-config)#network 172.29.0.0 255.255.255.0 MEDELLIN2(dhcp-config)#default-router 172.29.0.1 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit</pre>

2.7.4. Paso 4: Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Tabla 45 Configuración broadcast BOGOTA1

Router	Comandos
BOGOTA1	<pre>BOGOTA1(config)#interface serial 0/0/1 BOGOTA1(config-if)#ip helper-address 172.29.3.13 BOGOTA1(config-if)#exit</pre>

RECOMENDACIONES

Para el desarrollo de las tareas y dar solución a los escenarios propuestas en este trabajo sobre prueba de habilidades prácticas que forman parte de las actividades evaluativas del Diplomado de Profundización CCNA, se recomienda realizar los talleres y evaluaciones que se encuentran alojados en la página Cisco Networking Academy Builds IT Skills & Education For Future Careers y lograr adquirir los conocimientos necesarios para tal fin.

CONCLUSIONES

Todo el trabajo realizado demuestra el aprendizaje obtenido y el manejo de la herramienta de simulación más importante de CISCO que es Packet Tracer, donde se inició con actividades para conocer el entorno de trabajo y las herramientas que como estudiante se tienen en el momento de realizar los escenarios propuestos.

REFERENCIAS BIBLIOGRÁFICAS

CISCO. Asignación de direcciones IP. Fundamentos de Networking. {En línea}. {10 de abril de 2020} Disponible en: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. Capa de Transporte. Fundamentos de Networking. {En línea}. {10 de abril de 2020} Disponible en: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. {En línea}. {10 de abril de 2020} Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. Exploración de la red. Fundamentos de Networking. {En línea}. {10 de abril de 2020} Disponible en: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

CISCO. Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. {En línea}. {10 de abril de 2020} Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

CISCO. VLANs. Principios de Enrutamiento y Conmutación. {En línea}. {10 de abril de 2020} Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

Wikipedia, La enciclopedia libre. Mascara de Red. {En línea} {17 de abril de 2020} Disponible en: [https://es.wikipedia.org/w/index.php?title=M%C3%A1scara de red&oldid=124552884](https://es.wikipedia.org/w/index.php?title=M%C3%A1scara_de_red&oldid=124552884).