

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

OSCAR HERNAN SUESCUN PAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA.
INGENIERIA DE SISTEMAS
PALMIRA
2020

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

OSCAR HERNAN SUESCUN PAZ

INFORME FINAL PARA OBTENER EL TÍTULO DE INGENIERO DE SISTEMAS

HECTOR JULIAN PARRA
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA.
INGENIERIA DE SISTEMAS
PALMIRA
2020

A Dios, por haberme
acompañado a lo largo de mi
carrera, por ser mi fortaleza en
momentos de dificultad y por
brindarme una vida llena de
aprendizajes, experiencias y
felicidad

AGRADECIMIENTOS

Doy gracias a Dios por permitirme culminar este proyecto. A mis padres por su paciencia, colaboración y apoyo incondicional, infinitas gracias.

TABLA DE CONTENIDO

INTRODUCCIÓN	11
1. OBJETIVOS	12
1.1 OBJETIVO GENERAL	12
1.2 OBJETIVOS ESPECIFICOS	12
2. PLANTEAMIENTO DEL PROBLEMA	13
2.1 DEFINICIÓN DEL PROBLEMA	13
2.2 JUSTIFICACIÓN	13
3. ESCENARIO 1	14
3.1 TOPOLOGÍA	14
3.2 PARTE 1. INICIALIZAR DISPOSITIVOS	15
3.2.1 Paso 1. Inicializar y volver a cargar los routers y los switches	15
3.3 PARTE 2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS	15
3.3.1 Paso 1. Configurar la computadora de Internet	15
3.3.2 Paso 2. Configurar R1	16
3.3.3 Paso 3. Configurar R2	17
3.3.4 Paso 4. Configurar R3	19
3.3.5 Paso 5. Configurar S1	20
3.3.6 Paso 6. Configurar el S3	21
3.3.7 Paso 7. Verificar la conectividad de la red	22
3.4 PARTE 3. CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN 23	23
3.4.1 Paso 1. Configurar S1	23
3.4.2 Paso 2. Configurar el S3	24
3.4.3 Paso 3. Configurar R1	25
3.4.4 Paso 4. Verificar la conectividad de la red	26
3.4 PARTE 4. CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2	27
3.4.1 Paso 1. Configurar RIPv2 en el R1	27
3.4.2 Paso 2. Configurar RIPv2 en el R2	28
3.4.3 Paso 3. Configurar RIPv2 en el R3	28
3.4.4 Paso 4. Verificar la información de RIP	29
3.5 PARTE 5. IMPLEMENTAR DHCP Y NAT PARA IPV4	30

3.5.1	Paso 1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 30	
3.5.2	Paso 2. Configurar la NAT estática y dinámica en el R2.....	31
3.5.3	Paso 3. Verificar el protocolo DHCP y la NAT estática	32
3.6	PARTE 6. CONFIGURAR NTP.....	34
3.7	PARTE 7. CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)	34
3.7.1	Paso 1. Restringir el acceso a las líneas VTY en el R2.....	34
3.7.2	Paso 2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente 35	
4.	ESCENARIO 2	37
4.1	TOPOLOGIA.....	37
4.2	DESARROLLO	38
4.3	CONEXIÓN FISICA	47
4.4	PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO	47
4.5	PARTE 2: TABLA DE ENRUTAMIENTO	49
4.6	PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF .	53
4.7	PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF	55
4.8	PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP	62
4.9	PARTE 6: CONFIGURACIÓN DE PAT	64
4.10	PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP	65
5.	CONCLUSIONES.....	68
6.	BIBLIOGRAFIA	69

LISTA DE TABLAS

Tabla 1. Borrar y cargar configuración en los routers.....	15
Tabla 2. Configuración de computadora de internet.....	16
Tabla 3. Configuración de Router R1	17
Tabla 4. Configuración de Router R2.....	19
Tabla 5. Configuración de Router R3.....	20
Tabla 6. Configuración de Switch S1	21
Tabla 7. Configuración de Switch S3	21
Tabla 8. Verificación de la conexión de red.....	22
Tabla 9. Configuración de VLANs en Switch 1.....	24
Tabla 10. Configuración de Vlan en Switch 3.....	25
Tabla 11. Configuración de dot1Q en R1	25
Tabla 12. Verificación de la conexión entre Vlan.....	26
Tabla 13. Configuración de RIPv2 en Router R1	27
Tabla 14. Configuración de RIPv2 en Router R2	28
Tabla 15. Configuración de RIPv2 en Router R3	29
Tabla 16. Verificación de RIPv2 en Router R3.....	30
Tabla 17. Configuración de DHCP en Router R1	31
Tabla 18. Configuración de NAT interna y externa en Router R2	32
Tabla 19. Verificación de conexión entre PC-A y PC-C	33
Tabla 20. Configuración de NTP en Router R1 y R2.....	34
Tabla 21. Configuración de ACL en Router R1	35
Tabla 22. Prueba de comandos en la CLI	36

LISTA DE FIGURAS

Figura 1. Diagrama de red	14
Figura 2. Ping R1 a R2.....	22
Figura 3. Ping R2 a R3.....	22
Figura 4. Ping a puerta de enlace	22
Figura 5. Ping de S1 a R1	26
Figura 6. Ping S3 a R1	26
Figura 7. Ping S1 a R1.....	26
Figura 8. Ping S3 a R1	26
Figura 9. Show IP protocols R3.....	29
Figura 10. Show IP route RIP R3.....	29
Figura 11. Show run R3	30
Figura 12. DHCP PC-A	32
Figura 13. DHCP PC-C	33
Figura 14. Ping de PC-A a PC-C.....	33
Figura 15. Acceso a servidor Web	33
Figura 16. Telnet a R2	35
Figura 17. Show access-list R2.....	35
Figura 18. Show IP NAT translation R2	36
Figura 19. Diagrama de red escenario 2.....	37
Figura 20. Diagrama de red escenario 2 CISCO	47
Figura 21. Show IP route Bogota 1	49
Figura 22. Show IP route Bogota 2	50

Figura 23. Show IP route Bogota 3	50
Figura 24. Show IP route Medellin 1	51
Figura 25. Show IP route Medellin 2	51
Figura 26. Show IP route Medellin 3	52
Figura 27. Show IP route ISP.....	53
Figura 28. Show IP protocols Medellin 1	56
Figura 29. Show IP protocols Medellin 2	56
Figura 30. Show IP protocols Medellin 3	57
Figura 31. Show IP protocols Bogota 1	57
Figura 32. Show IP protocols Bogota 2	58
Figura 33. Show IP protocols Bogota 3	58
Figura 34. Show IP ospf Medellin 1	59
Figura 35. Show IP ospf Medellin 2.....	60
Figura 36. Show IP ospf Medellin 3.....	60
Figura 37. Show IP ospf Bogota 1	61
Figura 38. Show IP ospf Bogota 2.....	61
Figura 39. Show IP route Bogota 3	62

RESUMEN

CCNA (Cisco Certified Networking Associate) es una de las certificaciones más importantes dentro de la industria de la Tecnología de la Información. Esta certificación representa el nivel asociado, orientada a habilidades prácticas en el diagnóstico y solución de problemas específicos de redes.

Un profesional que está certificado en Cisco CCNA Routing and Switching, tiene los conocimientos necesarios para instalar y configurar la infraestructura de redes que conecta todos los dispositivos dentro de una empresa.

Palabras clave

Routing and Switching, infraestructura de redes, introducción a redes

INTRODUCCIÓN

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.

En el presente trabajo, se plantean dos escenarios donde se aplicarán los conocimientos adquiridos por medio de la práctica en los cursos CCNA1- Introduction to Networks y CCNA2-Routing and Switching donde se implementan redes pequeñas con una variedad de aplicaciones.

Lo anterior con base en la utilización de recursos y herramientas que se trabajaron en función de los protocolos y soporte de las comunicaciones por medio de las redes de datos, generando soluciones a problemas de conectividad. De igual manera se implementarán los diferentes niveles de seguridad aplicados a al escenario con el fin de mantener la integridad de la red y sus dispositivos frente a cualquier tipo amenaza.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Aplicar los conocimientos obtenidos en las prácticas, teorías para identificar y aplicar una solución a un caso o situación estudio de problema de Networking basada en la vida real.

1.2 OBJETIVOS ESPECIFICOS

- Usar los conocimientos adquiridos en networking para la configuración y solución de problemas en routers y switch.
- Usar de protocolos RIP, OSPF y enrutamiento para la distribución de datos a través de routers, con la implementación de métodos de aprendizaje y/o distribución de enrutamientos, balanceos de tráfico y encapsulamientos para la consecución de redes empresariales.
- Implementar redes a través de router y switch para la solución de necesidades típicas en organizaciones.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

Se plantean 2 escenarios donde se debe dar solución según los requerimientos solicitados en la guía y aplicar los conocimientos adquiridos en el transcurso del curso introducción a la red, switching and routing.

2.2 JUSTIFICACIÓN

Dar solución a estos 2 casos es necesario implementando todos los protocolos de internet 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.

3. ESCENARIO 1

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

3.1 TOPOLOGÍA

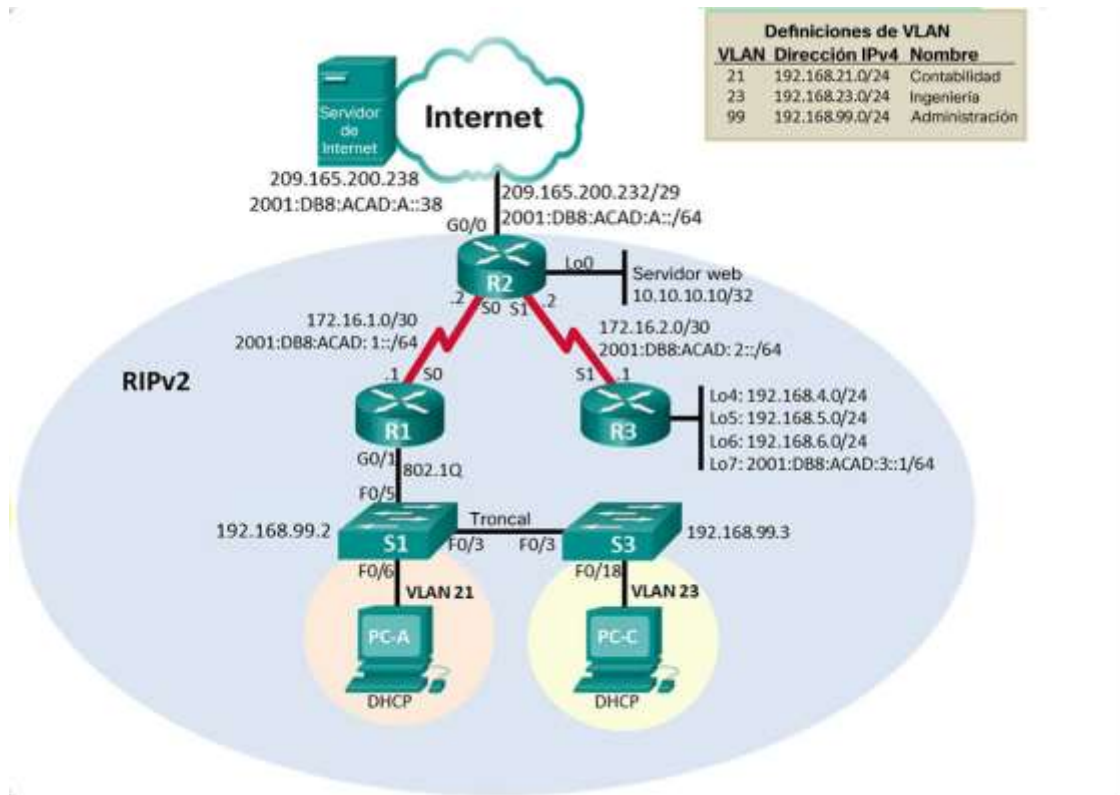


Figura 1. Diagrama de red

3.2 PARTE 1. INICIALIZAR DISPOSITIVOS

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

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

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

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

Tabla 1. Borrar y cargar configuración en los routers

3.3 PARTE 2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

3.3.1 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):

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

Tabla 2. Configuración de computadora de internet

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.

3.3.2 Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

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 R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption
Mensaje MOTD	R1(config)#banner motd # Enter TEXT message. End with the character '#'. se prohíbe el acceso no autorizado.#

Interfaz S0/0/0	R1(config)#interface s0/0/0 R1(config-if)#description Conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 unicast-routing R1(config)#ipv6 route::/0 s0/0/0

Tabla 3. Configuración de Router R1

Nota: Todavía no configure G0/1.

3.3.3 Paso 3. Configurar R2

La configuración del R2 incluye las siguientes tareas:

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 R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	Ip http server - No soportado

Mensaje MOTD	<pre>R2(config)#banner motd # Enter TEXT message. End with the character '#'. Se prohíbe el acceso no autorizado.#</pre>
Interfaz S0/0/0	<pre>R2(config)#interface s0/0/0 R2(config-if)#description conexion a R1 R2(config-if)#ip address 172.161.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown</pre>
Interfaz S0/0/1	<pre>R2(config)#interface s0/0/1 R2(config-if)#description conexion a R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown</pre>
Interfaz G0/0 (simulación de Internet)	<pre>R2(config)#interface g0/0 R2(config-if)#description conexion a Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown</pre>
Interfaz loopback 0 (servidor web simulado)	<pre>R2(config)#interface lo0 R2(config-if)#description conexion a servidor web simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown R2(config-if)#exit</pre>

Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 unicast-routing ::0 g0/0
---------------------	--

Tabla 4. Configuración de Router R2

3.3.4 Paso 4. Configurar R3

La configuración del R3 incluye las siguientes tareas:

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 R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado.#
Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#description conexión a R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R3(config-if)#no shutdown

Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)#ipv6 address 2001:DBA:ACAD:3::1/64 R3(config- if)#no shutdown R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 unicast-routing R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5. Configuración de Router R3

3.3.5 Paso 5. Configurar S1

La configuración del S1 incluye las siguientes tareas:

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 S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #se prohíbe el acceso no autorizado.#

Tabla 6. Configuración de Switch S1

3.3.6 Paso 6. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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

Tabla 7. Configuración de Switch S3

3.3.7 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:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	<pre>R1>ping 172.16.1.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds: Success rate is 0 percent (0/5)</pre> <p style="text-align: center;"><i>Figura 2. Ping R1 a R2</i></p>
R2	R3, S0/0/1	172.16.2.1	<pre>R2>ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/8 ms</pre> <p style="text-align: center;"><i>Figura 3. Ping R2 a R3</i></p>
PC de Internet	Gateway predeterminado	209.165.200.233	<pre>C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p style="text-align: center;"><i>Figura 4. Ping a puerta de enlace</i></p>

Tabla 8. Verificación de la conexión de red

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

3.4 PARTE 3. CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

3.4.1 Paso 1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

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)#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 S1(config-if)#exit</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 f0/3 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)#interface f0/5 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)#int range f0/1-2,f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access</pre>

Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 9. Configuración de VLans en Switch 1

3.4.2 Paso 2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S3(config)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit

Asignar F0/18 a la VLAN 23	S3(config)#interface f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 10. Configuración de Vlans en Switch 3

3.4.3 Paso 3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description LAN de contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface g0/1.23 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 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface g0/1.99 R1(config-subif)#description LAN de administracion R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no shutdown

Tabla 11. Configuración de dot1Q en R1

3.4.4 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:

Des de	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	<pre>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 0 percent (0/5)</pre> <p style="text-align: center;"><i>Figura 5. Ping de S1 a R1</i></p>
S3	R1, dirección VLAN 99	192.168.99.1	<pre>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 0 percent (0/5)</pre> <p style="text-align: center;"><i>Figura 6. Ping S3 a R1</i></p>
S1	R1, dirección VLAN 21	192.168.21.1	<pre>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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms</pre> <p style="text-align: center;"><i>Figura 7. Ping S1 a R1</i></p>
S3	R1, dirección VLAN 23	192.168.23.1	<pre>S3>ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: Success rate is 0 percent (0/5)</pre> <p style="text-align: center;"><i>Figura 8. Ping S3 a R1</i></p>

Tabla 12. Verificación de la conexión entre Vlans

3.4 PARTE 4. CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2

3.4.1 Paso 1. Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	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 192.168.99.00
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary R1(config-router)#exi

Tabla 13. Configuración de RIPv2 en Router R1

3.4.2 Paso 2. Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.0 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 14. Configuración de RIPv2 en Router R2

3.4.3 Paso 3. Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.23.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 15. Configuración de RIPv2 en Router R3

3.4.4 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:

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	<pre>R3# R3#show ip protocols Routing Protocol is "rip" Sending updates every 30 seconds, next due in 1 seconds Invalid after 180 seconds, hold down 180, flushed after 240 Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Redistributing: rip Default version control: send version 2, receive 2 Interface Send Recv Triggered RIP Key-chain Serial0/0/1 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</pre> <p><i>Figura 9. Show IP protocols R3</i></p>
¿Qué comando muestra solo las rutas RIP?	<pre>R3#show ip route rip 10.0.0.0/32 is subnetted, 1 subnets R 10.10.10.10 [120/1] via 172.16.2.1, 00:00:14, Serial0/0/1 192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks</pre> <p><i>Figura 10. Show IP route RIP R3</i></p>
¿Qué comando muestra la sección	R3#show run

de RIP de la configuración en ejecución?	<pre> router rip version 2 passive-interface Loopback4 passive-interface Loopback5 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> <p style="text-align: right;"><i>Figura 11. Show run R3</i></p>
--	--

Tabla 16. Verificación de RIPv2 en Router R3

3.5 PARTE 5. IMPLEMENTAR DHCP Y NAT PARA IPV4

3.5.1 Paso 1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

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

Crear un pool de DHCP para la VLAN 23	<pre> R1(config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com </pre>
---------------------------------------	--

Tabla 17. Configuración de DHCP en Router R1

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

La configuración del R2 incluye las siguientes tareas:

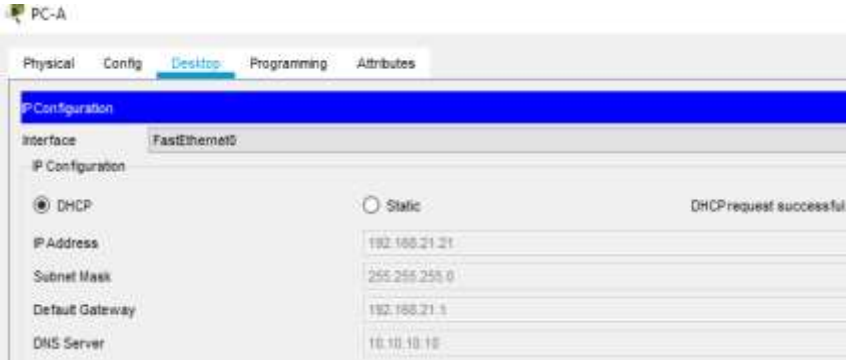
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser secret cisco12345 privilege 15
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication
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	<pre> R2(config)#interface g0/0 R2(config-if)#ip nat inside R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit </pre>
Configurar la NAT dinámica dentro de una ACL privada	<pre> 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 </pre>

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

Tabla 18. Configuración de NAT interna y externa en Router R2

3.5.3 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.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 <p style="text-align: center;"><i>Figura 12. DHCP PC-A</i></p>

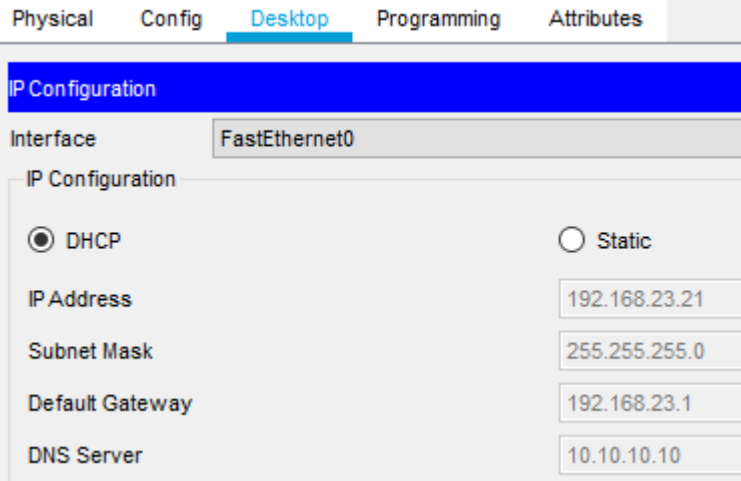
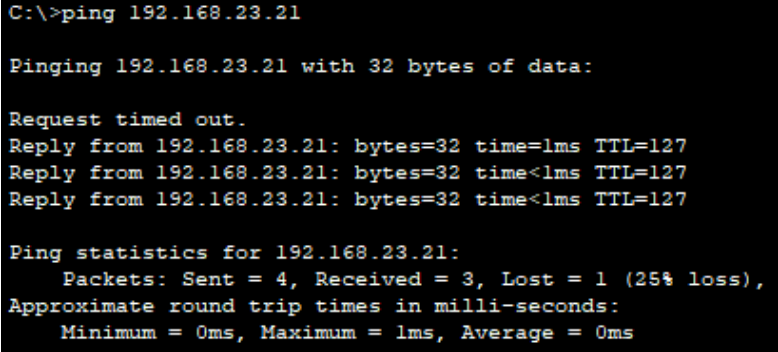
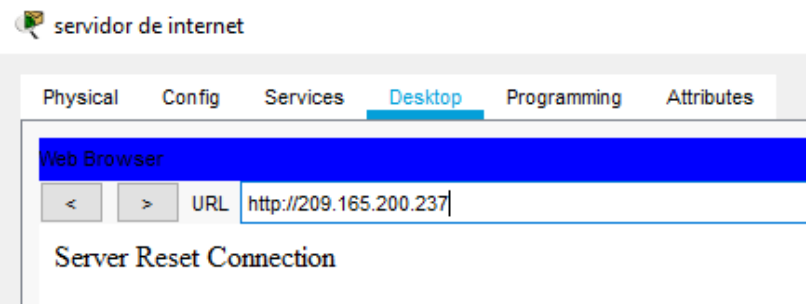
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	 <p style="text-align: center;"><i>Figura 13. DHCP PC-C</i></p>
<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p>Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	 <p style="text-align: center;"><i>Figura 14. Ping de PC-A a PC-C</i></p>
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.29) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	 <p style="text-align: center;"><i>Figura 15. Acceso a servidor Web</i></p>

Tabla 19. Verificación de conexión entre PC-A y PC-C

3.6 PARTE 6. CONFIGURAR NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 06:10:00 10 april 2020
Configure R2 como un maestro NTP.	R2#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.	R1(config)#show ntp associations

Tabla 20. Configuración de NTP en Router R1 y R2

3.7 PARTE 7. CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

3.7.1 Paso 1. 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	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet

<p>Verificar que la ACL funcione como se espera</p>	<pre>R1>enable Password: R1#telnet 172.16.1.1 Trying 172.16.1.1 ...OpenSe prohíbe el acceso a usuario no autorizados User Access Verification Password:</pre> <p style="text-align: right;"><i>Figura 16. Telnet a R2</i></p>
---	--

Tabla 21. Configuración de ACL en Router R1

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

Descripción del comando	Entrada del estudiante (comando)
<p>Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció</p>	<pre>R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es))</pre> <p style="text-align: right;"><i>Figura 17. Show access-list R2</i></p>
<p>Restablecer los contadores de una lista de acceso</p>	<p>R2#clear access-list counters</p>
<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</p>	<p>R2#show interface</p>

<p>¿Con qué comando se muestran las traducciones NAT?</p>	<pre>R2>show ip nat translation Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- --- --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1027 209.165.200.238:1027</pre> <p><i>Figura 18. Show IP NAT translation R2</i></p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<pre>R2#clear ip nat translation *</pre>

Tabla 22. Prueba de comandos en la CLI

4. 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.

4.1 TOPOLOGIA

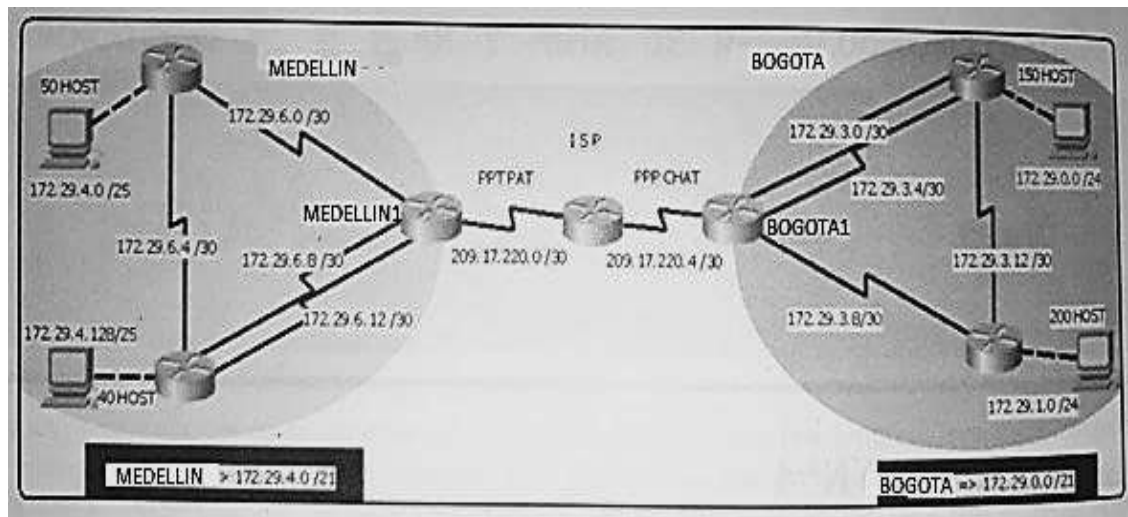


Figura 19. Diagrama de red escenario 2

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

4.2 DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

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

Router ISP

```
Router(config)#hostname ISP
```

```
ISP(config)#enable secret administrador
```

```
ISP(config)#line console 0
```

```
ISP(config-line)#password cisco
```

```
ISP(config-line)#login
```

```
ISP(config-line)#exit
```

```
ISP(config)#line vty 0 4
```

```
ISP(config-line)#password cisco
```

```
ISP(config-line)#exit
```

```
ISP(config)#service password-encryption
```

```
ISP(config)#banner motd #Se prohíbe el acceso no autorizado.#
```

```
ISP(config)#interface s0/0/0
```

```
ISP(config-if)#description conexion ISP-Medellin1
```

```
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
```

```
ISP(config-if)#no shutdown
```

```
ISP(config)#interface s0/0/1
```

```
ISP(config-if)#description conexion ISP-Bogota1
```

```
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
```

ISP(config-if)#no shutdown

Router Bogota 1

Router(config)#hostname Bogota1

Bogota1(config)#enable secret administrador

Bogota1(config)#line console 0

Bogota1(config-line)#password cisco

Bogota1(config-line)#login

Bogota1(config-line)#exit

Bogota1(config)#line vty 0 4

Bogota1(config-line)#password cisco

Bogota1(config-line)#exit

Bogota1(config)#service password-encryption

Bogota1(config)#banner motd #Se prohíbe el acceso no autorizado.#

Bogota1(config)#interface s0/0/0

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-if)#exit

Bogota1(config)#interface s0/0/1

Bogota1(config-if)#description conexion Bogota1-Bogota3

Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252

Bogota1(config-if)#no shutdown

```
Bogota1(config-if)#exit
Bogota1(config)#interface s0/1/0
Bogota1(config-if)#description conexion2 Bogota1-Bogota3
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface s0/1/1
Bogota1(config-if)#description conexion Bogota1-Bogota2
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
```

Router Bogota 2

```
Router(config)#hostname Bogota2
Bogota2(config)#enable secret administrador
Bogota2(config)#line console 0
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#exit
Bogota2(config)#line vty 0 4
Bogota2(config-line)#password cisco
Bogota2(config-line)#exit
Bogota2(config)#service password-encryption
Bogota2(config)#banner motd #Se prohíbe el acceso no autorizado.#
```



```
Bogota2(config)#interface s0/0/0
Bogota2(config-if)#description conexion Bogota2-Bogota1
Bogota2(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota2(config-if)#exit
Bogota2(config)#interface s0/0/1
Bogota2(config-if)#description conexion Bogota2-Bogota3
Bogota2(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface g0/0
Bogota2(config-if)#description conexion Bogota-PCB2
Bogota2(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
```

Router Bogota 3

```
Bogota3(config)#enable secret administrador
Bogota3(config)#line console 0
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#exit
Bogota3(config)#line vty 0 4
Bogota3(config-line)#password cisco
```

```
Bogota3(config-line)#exit
Bogota3(config)#service password-encryption
Bogota3(config)#banner motd #Se prohíbe el acceso no autorizado.#
Bogota3(config)#interface s0/0/0
Bogota3(config-if)#description conexion1 Bogota3-Bogota1
Bogota3(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota3(config-if)#clock rate 180000
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#interface s0/0/1
Bogota3(config-if)#description conexion2 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-if)#exit
Bogota3(config)#interface s0/1/0
Bogota3(config-if)#description conexion Bogota3-Bogota2
Bogota3(config-if)#ip address 172.19.3.13 255.255.255.252
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#interface g0/0
Bogota3(config-if)#description Bogota3-PCB1
Bogota3(config-if)#ip address 172.29.0.1 255.255.255.0
```

```
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Router Medellin 1
Router(config)#hostname Medellin1
Medellin1(config)#enable secret administrador
Medellin1(config)#line console 0
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#exit
Medellin1(config)#line vty 0 4
Medellin1(config-line)#password cisco
Medellin1(config)#service password-encryption
Medellin1(config)#banner motd #Se prohíbe el acceso no autorizado.#
Medellin1(config)#interface s0/0/0
Medellin1(config-if)#description conexion Medellin1-ISP
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-line)#exit
Medellin1(config)#interface s0/0/1
Medellin1(config-if)#description conexion Medellin1-Medellin2
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#no shutdown
```

```
Medellin1(config-if)#exit
Medellin1(config)#interface s0/1/0
Medellin1(config-if)#description conexion1 Medellin1-Medellin3
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface s0/1/1
Medellin1(config-if)#description conexion2 Medellin1-Medellin3
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
```

Router Medellin 2

```
Medellin2(config)#enable secret administrador
Medellin2(config)#line console 0
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#exit
Medellin2(config)#line vty 0 4
Medellin2(config-line)#password cisco
Medellin2(config-line)#exit
Medellin2(config)#service password-encryption
Medellin2(config)#banner motd #Se prohíbe el acceso no autorizado.#
Medellin2(config)#interface s0/0/0
```

Medellin2(config)#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-line)#exit

Medellin2(config)#interface s0/0/1

Medellin2(config)#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-line)#exit

Medellin2(config)#interface g0/0

Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128

Medellin2(config-if)#description conexion Medellin2-PCM1

Medellin2(config-if)#no shutdown

Medellin2(config-if)#exit

Router Medellin 3

Router(config)#hostname Medellin3

Medellin3(config)#enable secret administrador

Medellin3(config)#line console 0

Medellin3(config-line)#password cisco

Medellin3(config-line)#login

Medellin3(config-line)#exit

```
Medellin3(config)#line vty 0 4
Medellin3(config-line)#password cisco
Medellin3(config-line)#exit
Medellin3(config)#service password-encryption
Medellin3(config)#banner motd #Se prohíbe el acceso no autorizado.#
Medellin3(config)#interface s0/0/0
Medellin3(config-if)#description conexion1 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-if)#exit
Medellin3(config)#interface s0/0/1
Medellin3(config-if)#description conexion2 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-if)#exit
Medellin3(config)#interface s0/1/0
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface g0/0
Medellin3(config-if)#description conexion Medellin3-PCM2
```

```
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
```

```
Medellin3(config-if)#no shutdown
```

```
Medellin3(config-if)#exit
```

4.3 CONEXIÓN FÍSICA

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

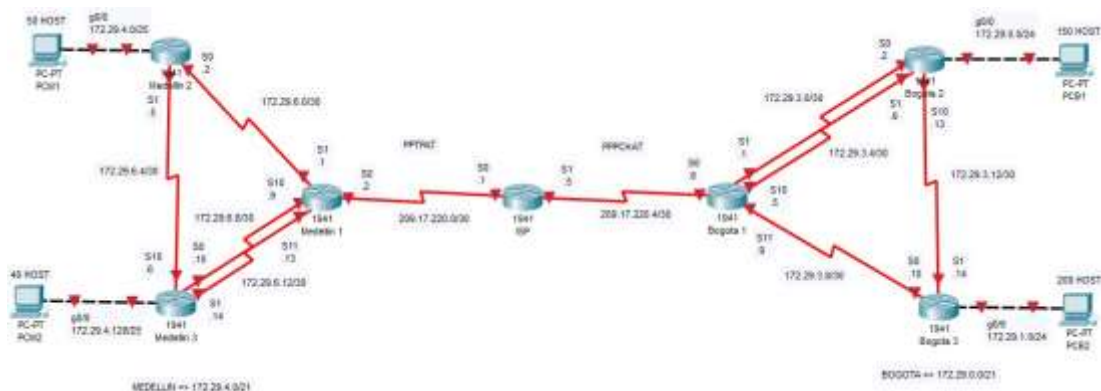


Figura 20. Diagrama de red escenario 2 CISCO

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

4.4 PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

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

Router Medellin 1

```
Medellin1(config)#router ospf 2
```

```
Medellin1(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

Router Medellin 2

```
Medellin2(config)#router ospf 2
```

```
Medellin2(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

```
Medellin2(config-router)#exit
```

Router Medellin 3

```
Medellin3(config)#router ospf 2
```

```
Medellin3(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

```
Medellin3(config-router)#exit
```

Router Bogota 1

```
Bogota1(config)#router ospf 2
```

```
Bogota1(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

```
Bogota1(config-router)#exit
```

Router Bogota 2

```
Bogota2(config)#router ospf 2
```

```
Bogota2(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

```
Bogota2(config-router)#exit
```

Router Bogota 3

```
Bogota3(config)#router ospf 2
```

```
Bogota3(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

```
Bogota3(config-router)#exit
```

b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Bogota 1

```
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

```
Bogota1(config)#exit
```


Medellin 1

```
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

```
Medellin1(config)#exit
```

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

Router ISP

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
```


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

```
ISP(config)#exit
```

4.5 PARTE 2: TABLA DE ENRUTAMIENTO.

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

Router Bogota 1



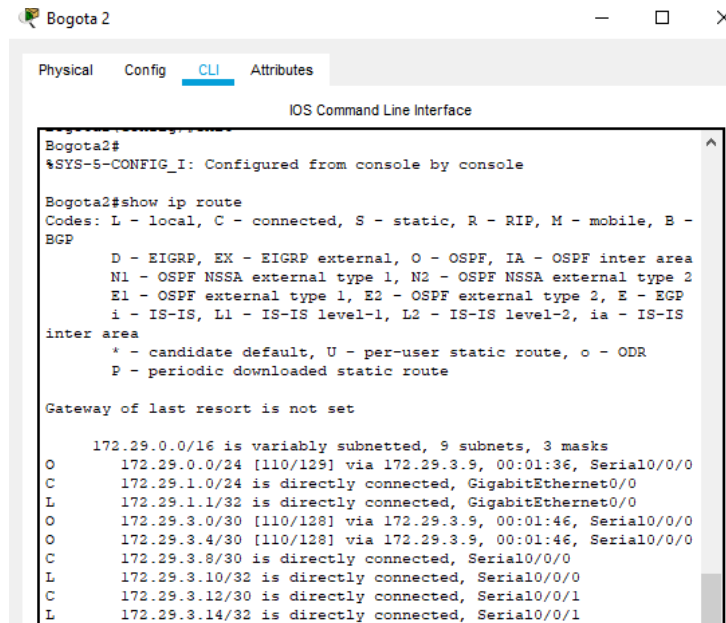
```
Bogota 1
Physical Config CLI Attributes
IOS Command Line Interface
Bogota1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF 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 209.17.220.5 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O 172.29.0.0/24 [110/65] via 172.29.3.2, 00:03:42, Serial0/0/1
O 172.29.1.0/24 [110/65] via 172.29.3.10, 00:03:52, Serial0/1/1
C 172.29.3.0/30 is directly connected, Serial0/0/1
L 172.29.3.1/32 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/0
L 172.29.3.5/32 is directly connected, Serial0/1/0
C 172.29.3.8/30 is directly connected, Serial0/1/1
L 172.29.3.9/32 is directly connected, Serial0/1/1
O 172.29.3.12/30 [110/128] via 172.29.3.10, 00:03:52,
Serial0/1/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.4/30 is directly connected, Serial0/0/0
```

Figura 21. Show IP route Bogota 1

Router Bogota 2

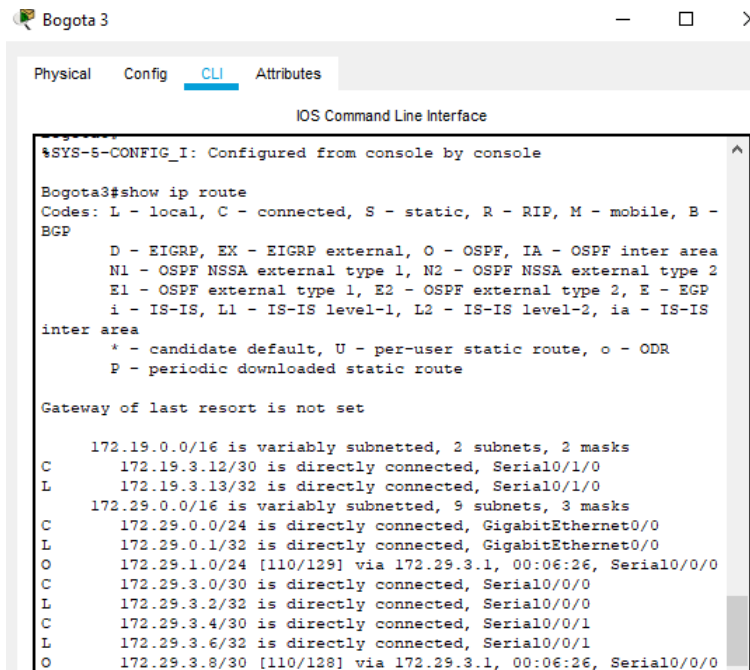


```
Bogota 2
Physical Config CLI Attributes
IOS Command Line Interface
Bogota2#
%SYS-5-CONFIG_I: Configured from console by console
Bogota2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        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 not set

      172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/129] via 172.29.3.9, 00:01:36, Serial0/0/0
C       172.29.1.0/24 is directly connected, GigabitEthernet0/0
L       172.29.1.1/32 is directly connected, GigabitEthernet0/0
O       172.29.3.0/30 [110/128] via 172.29.3.9, 00:01:46, Serial0/0/0
O       172.29.3.4/30 [110/128] via 172.29.3.9, 00:01:46, 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       172.29.3.14/32 is directly connected, Serial0/0/1
```

Figura 22. Show IP route Bogota 2

Router Bogota 3

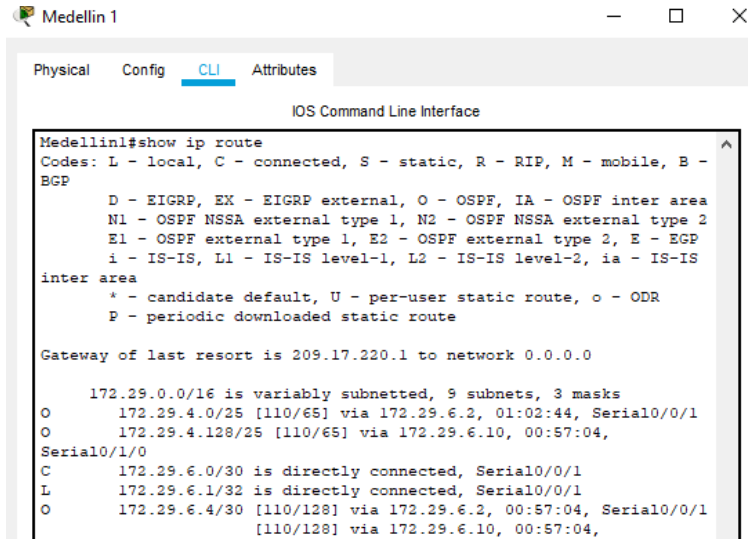


```
Bogota 3
Physical Config CLI Attributes
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
Bogota3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - 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 not set

      172.19.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.19.3.12/30 is directly connected, Serial0/1/0
L       172.19.3.13/32 is directly connected, Serial0/1/0
      172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.0.0/24 is directly connected, GigabitEthernet0/0
L       172.29.0.1/32 is directly connected, GigabitEthernet0/0
O       172.29.1.0/24 [110/129] via 172.29.3.1, 00:06:26, Serial0/0/0
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 172.29.3.1, 00:06:26, Serial0/0/0
```

Figura 23. Show IP route Bogota 3

Router Medellin 1



The screenshot shows the CLI of Router Medellin 1. The command 'show ip route' has been executed, displaying the routing table. The output includes a legend for route codes (L, C, S, R, M, B, BGP, D, N1, N2, E1, E2, E, i, L1, L2, ia), a note about the gateway of last resort (209.17.220.1), and a list of routes for the 172.29.0.0/16 network. The routes are: 172.29.4.0/25 via 172.29.6.2 (Serial0/0/1), 172.29.4.128/25 via 172.29.6.10 (Serial0/1/0), 172.29.6.0/30 (Serial0/0/1), 172.29.6.1/32 (Serial0/0/1), and 172.29.6.4/30 via 172.29.6.2 (Serial0/0/1).

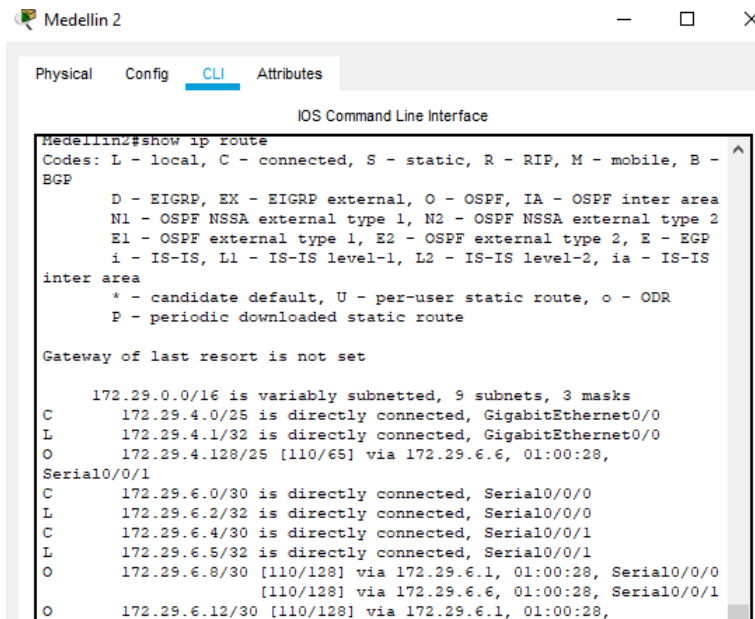
```
Medellin1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2,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

Gateway of last resort is 209.17.220.1 to network 0.0.0.0

   172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.2, 01:02:44, Serial0/0/1
O       172.29.4.128/25 [110/65] via 172.29.6.10, 00:57:04,
Serial0/1/0
C       172.29.6.0/30 is directly connected, Serial0/0/1
L       172.29.6.1/32 is directly connected, Serial0/0/1
O       172.29.6.4/30 [110/128] via 172.29.6.2, 00:57:04, Serial0/0/1
        [110/128] via 172.29.6.10, 00:57:04,
```

Figura 24. Show IP route Medellin 1

Router Medellin 2



The screenshot shows the CLI of Router Medellin 2. The command 'show ip route' has been executed, displaying the routing table. The output includes a legend for route codes (L, C, S, R, M, B, BGP, D, N1, N2, E1, E2, E, i, L1, L2, ia), a note that the gateway of last resort is not set, and a list of routes for the 172.29.0.0/16 network. The routes are: 172.29.4.0/25 (GigabitEthernet0/0), 172.29.4.1/32 (GigabitEthernet0/0), 172.29.4.128/25 via 172.29.6.6 (Serial0/0/1), 172.29.6.0/30 (Serial0/0/0), 172.29.6.2/32 (Serial0/0/0), 172.29.6.4/30 (Serial0/0/1), 172.29.6.5/32 (Serial0/0/1), 172.29.6.8/30 via 172.29.6.1 (Serial0/0/0) and 172.29.6.6 (Serial0/0/1), and 172.29.6.12/30 via 172.29.6.1 (Serial0/0/1).

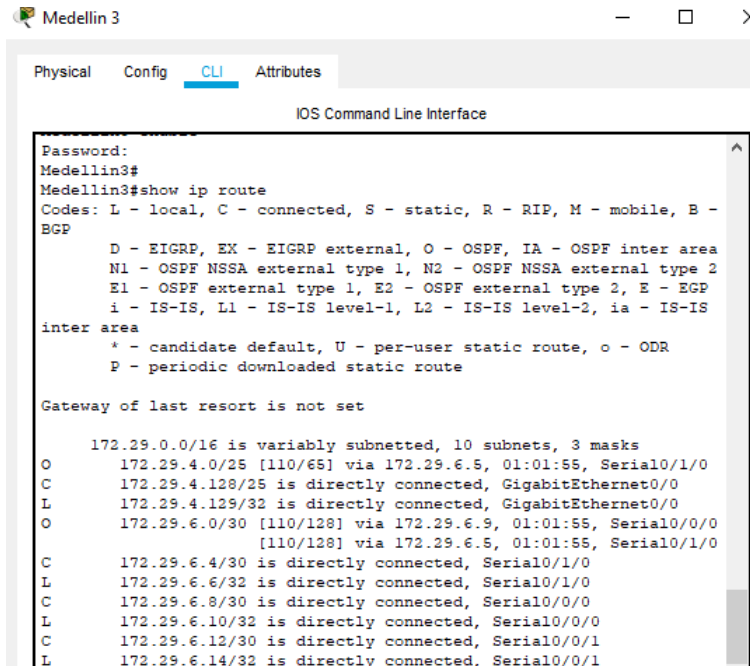
```
Medellin2#show ip Route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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 not set

   172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.4.0/25 is directly connected, GigabitEthernet0/0
L       172.29.4.1/32 is directly connected, GigabitEthernet0/0
O       172.29.4.128/25 [110/65] via 172.29.6.6, 01:00:28,
Serial0/0/1
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 172.29.6.1, 01:00:28, Serial0/0/0
        [110/128] via 172.29.6.6, 01:00:28, Serial0/0/1
O       172.29.6.12/30 [110/128] via 172.29.6.1, 01:00:28,
```

Figura 25. Show IP route Medellin 2

Router Medellin 3



```
Medellin 3
Physical Config CLI Attributes
IOS Command Line Interface
Password:
Medellin3#
Medellin3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O    172.29.4.0/25 [110/65] via 172.29.6.5, 01:01:55, Serial0/1/0
C    172.29.4.128/25 is directly connected, GigabitEthernet0/0
L    172.29.4.129/32 is directly connected, GigabitEthernet0/0
O    172.29.6.0/30 [110/128] via 172.29.6.9, 01:01:55, Serial0/0/0
        [110/128] via 172.29.6.5, 01:01:55, Serial0/1/0
C    172.29.6.4/30 is directly connected, Serial0/1/0
L    172.29.6.6/32 is directly connected, Serial0/1/0
C    172.29.6.8/30 is directly connected, Serial0/0/0
L    172.29.6.10/32 is directly connected, Serial0/0/0
C    172.29.6.12/30 is directly connected, Serial0/0/1
L    172.29.6.14/32 is directly connected, Serial0/0/1
```

Figura 26. Show IP route Medellin 3

- Verificar el balanceo de carga que presentan los routers.
- Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
- Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
- Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

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

```

ISP
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

ISP(config)#
ISP(config)#exit
ISP#
%SYS-5-CONFIG_I: Configured from console by console

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 not set

      172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0/22 [1/0] via 209.17.220.6
S       172.29.4.0/22 [1/0] via 209.17.220.2
      209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.1/32 is directly connected, Serial0/0/0
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.5/32 is directly connected, Serial0/0/1

ISP#
  
```

Figura 27. Show IP route ISP

4.6 PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

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

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1

Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Router Medellin 1

Medellin1(config)#router ospf 2

Medellin1(config-router)#passive-interface s0/0/0

Medellin2(config-router)#exit

Router Medellin 2

Medellin2(config)#router ospf 2

Medellin2(config-router)#passive-interface g0/0

Medellin2(config-router)#exit

Router Medellin 3

Medellin3(config)#router ospf 2

Medellin3(config-router)#passive-interface g0/0

Medellin3(config-router)#exit

Router Bogota 1

```
Bogota1(config)#router ospf 2
```

```
Bogota1(config-router)#passive-interface s0/0/0
```

```
Bogota1(config-router)#exit
```

Router Bogota 2

```
Bogota2(config)#router ospf 2
```

```
Bogota2(config-router)#passive-interface g0/0
```

```
Bogota2(config-router)#exit
```

Router Bogota 3

```
Bogota3(config)#router ospf 2
```

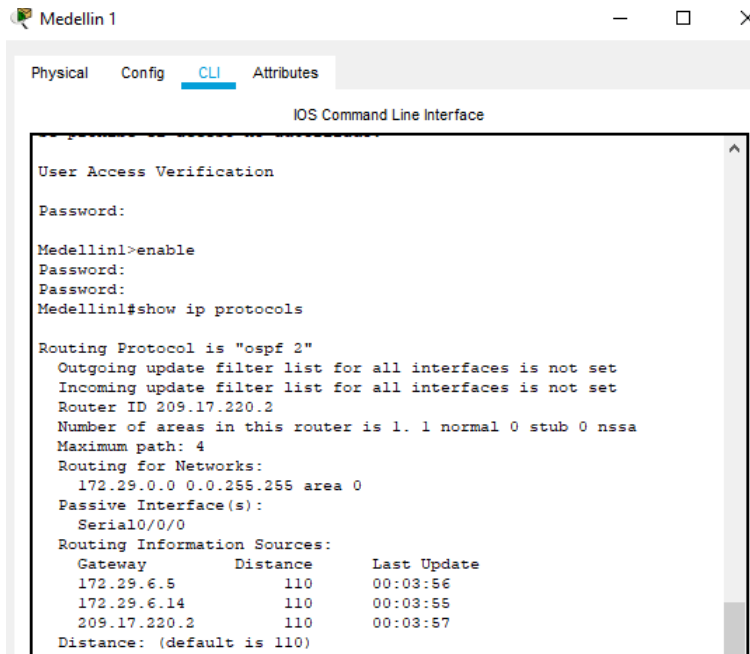
```
Bogota3(config-router)#passive-interface g0/0
```

```
Bogota3(config-router)#exit
```

4.7 PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

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

Medellín 1

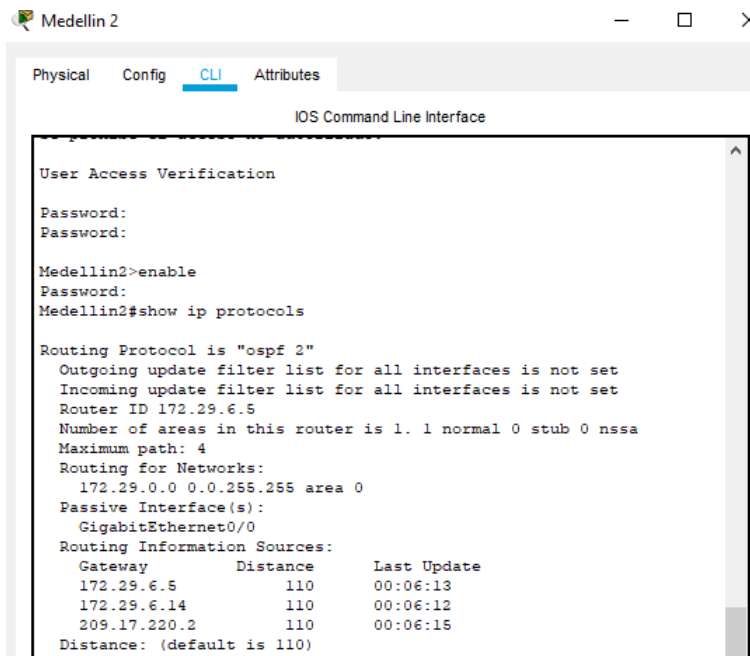


```
Medellin1>enable
Medellin1#show ip protocols

Routing Protocol is "ospf 2"
  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
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.255.255 area 0
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
  172.29.6.5         110          00:03:56
  172.29.6.14        110          00:03:55
  209.17.220.2       110          00:03:57
  Distance: (default is 110)
```

Figura 28. Show IP protocols Medellin 1

Medellín 2

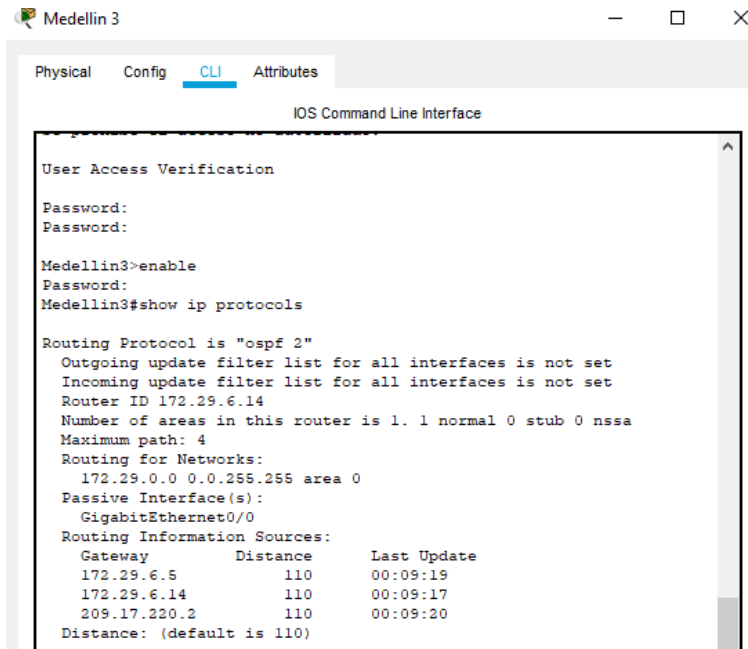


```
Medellin2>enable
Medellin2#show ip protocols

Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.6.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.255.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
  172.29.6.5         110          00:06:13
  172.29.6.14        110          00:06:12
  209.17.220.2       110          00:06:15
  Distance: (default is 110)
```

Figura 29. Show IP protocols Medellin 2

Medellín 3



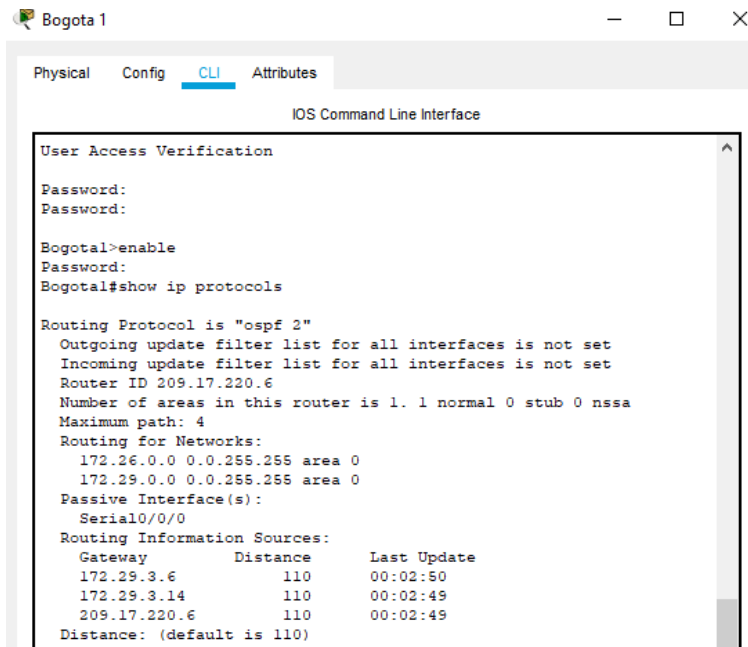
```
Medellin3
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Password:
Password:
Medellin3>enable
Password:
Medellin3#show ip protocols

Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.6.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.255.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.6.5       110          00:09:19
    172.29.6.14     110          00:09:17
    209.17.220.2    110          00:09:20
  Distance: (default is 110)
```

Figura 30. Show IP protocols Medellin 3

Bogotá 1



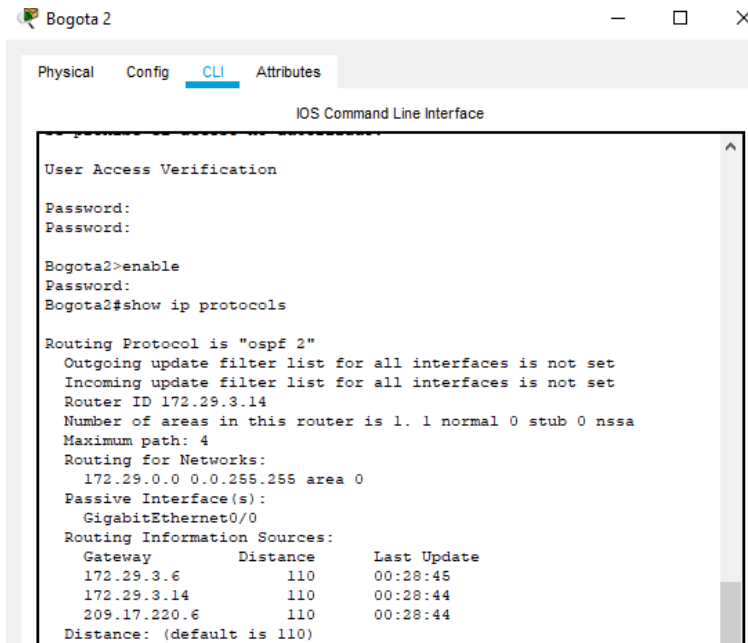
```
Bogota 1
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Password:
Password:
Bogotal>enable
Password:
Bogotal#show ip protocols

Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.26.0.0 0.0.255.255 area 0
    172.29.0.0 0.0.255.255 area 0
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.6       110          00:02:50
    172.29.3.14     110          00:02:49
    209.17.220.6    110          00:02:49
  Distance: (default is 110)
```

Figura 31. Show IP protocols Bogota 1

Bogotá 2



```
Bogota 2
Physical Config CLI Attributes
IOS Command Line Interface

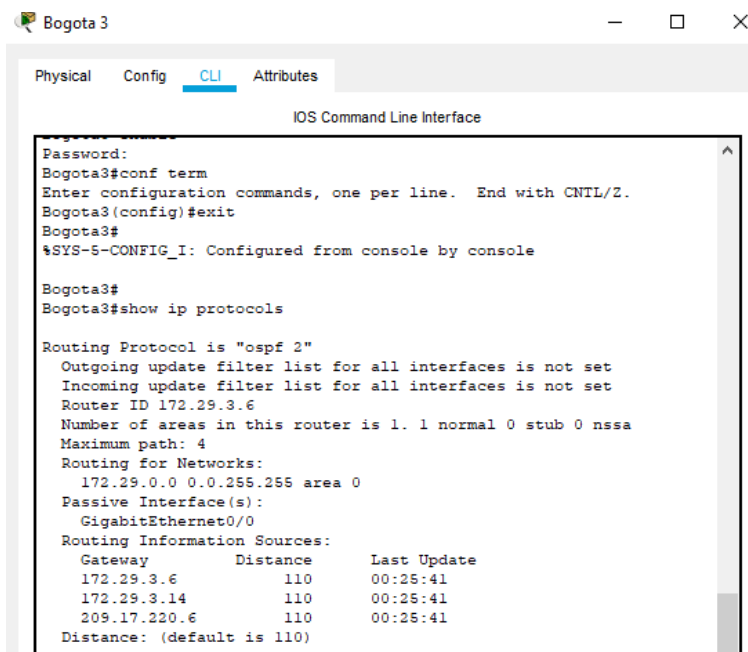
User Access Verification
Password:
Password:

Bogota2>enable
Password:
Bogota2#show ip protocols

Routing Protocol is "ospf 2"
  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:
    172.29.0.0 0.0.255.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.6       110          00:28:45
    172.29.3.14      110          00:28:44
    209.17.220.6     110          00:28:44
  Distance: (default is 110)
```

Figura 32. Show IP protocols Bogota 2

Bogotá 3



```
Bogota 3
Physical Config CLI Attributes
IOS Command Line Interface

Password:
Bogota3#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Bogota3(config)#exit
Bogota3#
%SYS-5-CONFIG_I: Configured from console by console

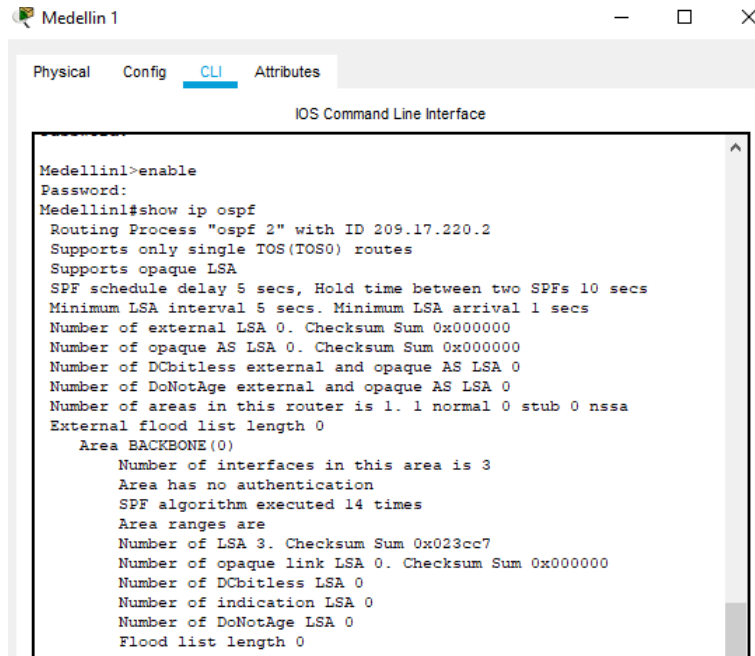
Bogota3#
Bogota3#show ip protocols

Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.3.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.255.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.6       110          00:25:41
    172.29.3.14      110          00:25:41
    209.17.220.6     110          00:25:41
  Distance: (default is 110)
```

Figura 31. Show IP protocols Bogota 1

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

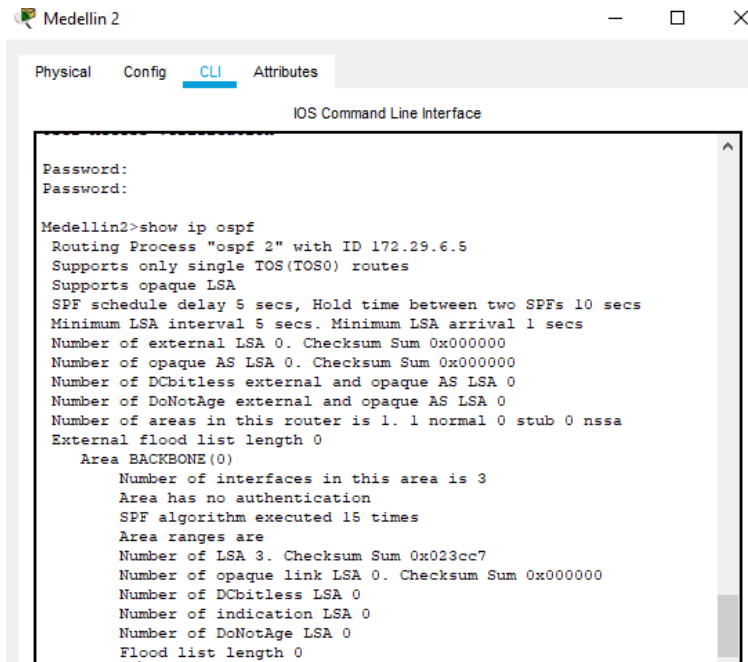
Medellín 1



```
Medellin 1
Physical Config CLI Attributes
IOS Command Line Interface
Medellin1>enable
Password:
Medellin1#show ip ospf
Routing Process "ospf 2" with ID 209.17.220.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 14 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x023cc7
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Figura 34. Show IP ospf Medellin 1

Medellín 2



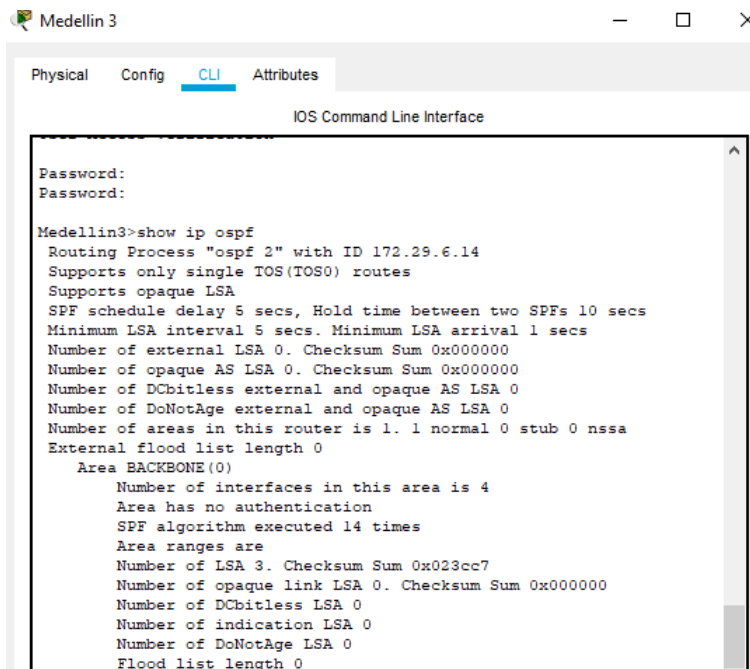
```
Medellin2
Physical Config CLI Attributes
IOS Command Line Interface

Password:
Password:

Medellin2>show ip ospf
Routing Process "ospf 2" with ID 172.29.6.5
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 15 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x023cc7
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Figura 35. Show IP ospf Medellin 2

Medellín 3



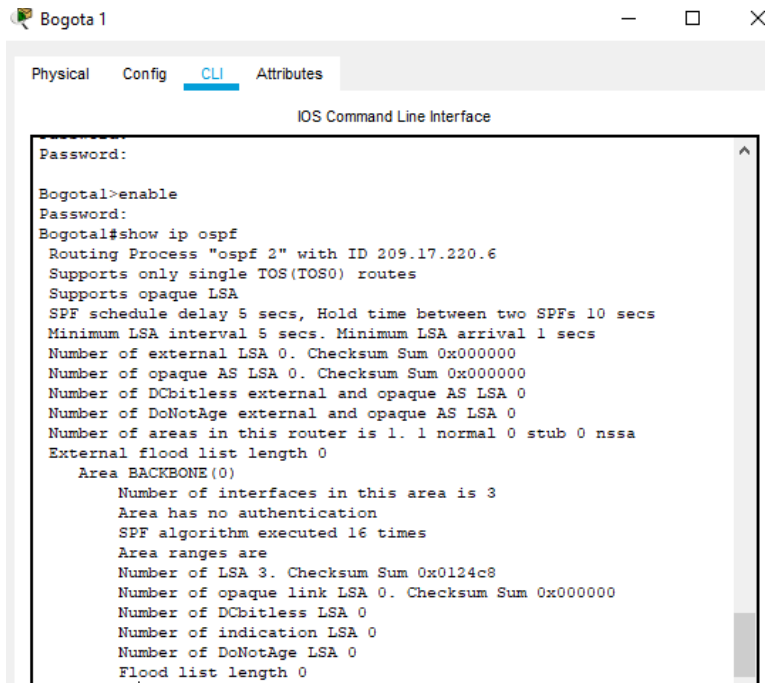
```
Medellin3
Physical Config CLI Attributes
IOS Command Line Interface

Password:
Password:

Medellin3>show ip ospf
Routing Process "ospf 2" with ID 172.29.6.14
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 4
    Area has no authentication
    SPF algorithm executed 14 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x023cc7
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Figura 36. Show IP ospf Medellin 3

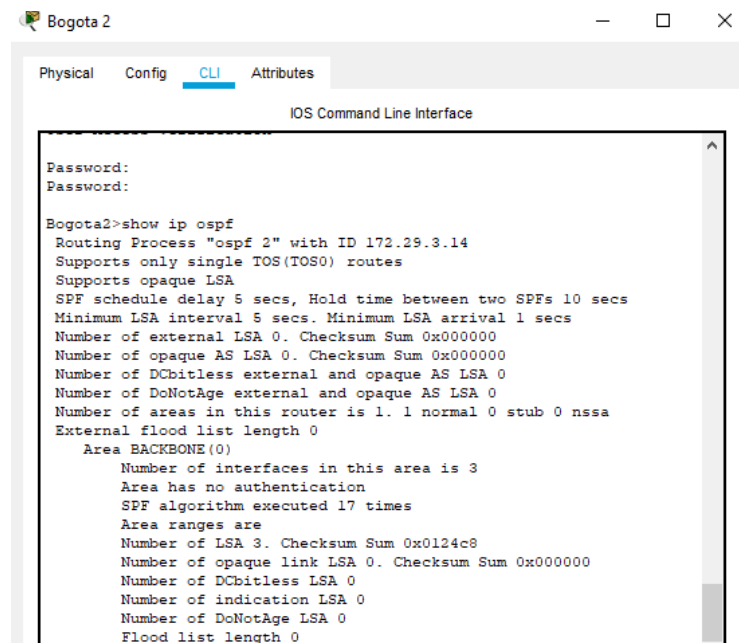
Bogotá 1



```
Bogota 1
Physical Config CLI Attributes
IOS Command Line Interface
Password:
Bogota1>enable
Password:
Bogota1#show ip ospf
Routing Process "ospf 2" with ID 209.17.220.6
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 16 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x0124c8
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Figura 37. Show IP ospf Bogota 1

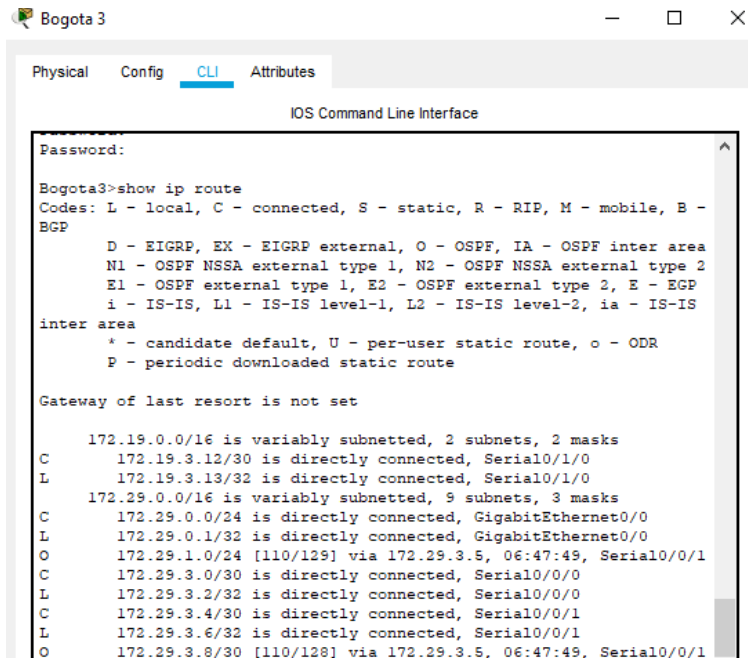
Bogotá 2



```
Bogota 2
Physical Config CLI Attributes
IOS Command Line Interface
Password:
Password:
Bogota2>show ip ospf
Routing Process "ospf 2" with ID 172.29.3.14
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 17 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x0124c8
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Figura 38. Show IP ospf Bogota 2

Bogotá 3



```
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 not set

172.19.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.19.3.12/30 is directly connected, Serial0/1/0
L       172.19.3.13/32 is directly connected, Serial0/1/0
L       172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.0.0/24 is directly connected, GigabitEthernet0/0
L       172.29.0.1/32 is directly connected, GigabitEthernet0/0
O       172.29.1.0/24 [110/129] via 172.29.3.5, 06:47:49, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/0/0
L       172.29.3.2/32 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/0/1
L       172.29.3.6/32 is directly connected, Serial0/0/1
O       172.29.3.8/30 [110/128] via 172.29.3.5, 06:47:49, Serial0/0/1
```

Figura 39. Show IP route Bogotá 3

4.8 PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

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

Router ISP

```
ISP(config)#username Medellin1 password admin
```

```
ISP(config)#interface s0/0/0
```

```
ISP(config-if)#encapsulation ppp
```

```
ISP(config-if)#ppp authentication pap
```

```
ISP(config-if)#ppp pap sent-username ISP password 0 admin
```

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

Router Medellin1

```
Medellin1(config)#username ISP password admin
```

```
Medellin1(config)#interface s0/0/0
```

```
Medellin1(config-if)#encapsulation ppp
```

```
Medellin1(config-if)#ppp authentication pap
```

```
Medellin1(config-if)#ppp pap sent-username Medellin1 password 0 admin
```

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

b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Router ISP

```
ISP(config)#username Bogota1 password admin
```

```
ISP(config)#interface s0/0/1
```

```
ISP(config-if)#encapsulation ppp
```

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

Router Bogota 1

```
Bogota1(config)#username ISP password admin
```

```
Bogota1(config)#interface s0/0/0
```

```
Bogota1(config-if)#encapsulation ppp
```

```
Bogota1(config-if)#ppp authentication chap
```

```
Bogota1(config-if)#exit
```

4.9 PARTE 6: CONFIGURACIÓN DE PAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

Router Medellin1

```
Medellin1(config)#ip nat inside source list 1 interface s0/0/0 overload
```

Router Bogota 1

```
Bogota1(config)#ip nat inside source list 1 interface s0/0/0 overload
```

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

Router Medellin1

```
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
```

```
Medellin1(config)#interface s0/0/0
```

```
Medellin1(config-if)#ip nat outside
```

```
Medellin1(config-if)#interface s0/0/1
```

```
Medellin1(config-if)#ip nat inside
```

```
Medellin1(config-if)#interface s0/1/0
```

```
Medellin1(config-if)#ip nat inside
```

```
Medellin1(config-if)#interface s0/1/1
```

```
Medellin1(config-if)#ip nat inside
```



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

```
Medellin1(config)#exit
```

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

Router Bogota1

```
Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
```

```
Bogota1(config)#interface s0/0/0
```

```
Bogota1(config-if)#ip nat outside
```

```
Bogota1(config-if)#interface s0/0/1
```

```
Bogota1(config-if)#ip nat inside
```

```
Bogota1(config-if)#interface s0/1/0
```

```
Bogota1(config-if)#ip nat inside
```

```
Bogota1(config-if)#interface s0/1/1
```

```
Bogota1(config-if)#ip nat inside
```

```
Bogota1(config-if)#exit
```

```
Bogota1(config)#exit
```

4.10 PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.

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

Medellin2

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
```

```
Medellin2(config)#ip dhcp pool medellin2
```

```
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.218
```

```
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
```

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

Router Medellin3

```
Medellin3(config)#interface g0/0
```

```
Medellin3(config-if)#ip helper-address 172.29.6.5
```

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

Router Bogota2

```
Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
```

```
Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
```

```
Bogota2(config)#ip dhcp pool bogota2
```

```
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
```

```
Bogota2(dhcp-config)#default-router 172.29.1.1
```

```
Bogota2(dhcp-config)#exit
```

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

```
Bogota3(config)#int g0/0
```

```
Bogota3(config-if)#ip helper-address 172.29.3.13
```

```
Bogota3(config-if)#exit
```

5. CONCLUSIONES

El comando `no ip domain-lookup` desactiva la traducción de nombres a dirección del dispositivo, cualquier error de digitación nos ahorraría segundos valiosos.

Proteger los routers y switches Cisco es de gran importancia para reforzar la seguridad de la red, por eso es necesario establecer contraseña de acceso para iniciar sesión en el dispositivo y habilitar la consola de línea de comandos, la terminal virtual, además se debe encriptar las contraseñas, inhabilitar servicios no utilizados y mostrar mensaje de advertencia cuando el acceso es incorrecto.

La configuración de IPv6 en una red interna es importante para las empresas o los hogares porque cada vez hay un crecimiento exponencial de dispositivos conectados que necesitarían tener una conexión permanente a Internet con una dirección IP exclusiva.

La interfaz loopback es una interfaz lógica del router por lo tanto no se asigna a un puerto físico, es muy útil para probar y administrar un router como por ejemplo prueba de procesos de routing interno.

En el escenario 1 el router 2 conectado a Internet tiene configurada la NAT estática interna y externa que permite a los PC tener conexión a Internet y utilizar servicios de correo, navegación y compartir archivos.

El protocolo 802.1Q nos permite compartir múltiples redes lógicas por el mismo medio físico. En este caso las VLAN 21, 23 y 99 que están configuradas en los switches y que se comunican con el router 1

6. BIBLIOGRAFIA

Course (2019). Introducción a redes. Recuperado de <http://static-course-assets.s3.amazonaws.com/ITN50ES/module4/index.html#4.5.1.2>

Course (2019). Principios básicos de routing y switching. Recuperado de <http://static-course-assets.s3.amazonaws.com/ITN50ES/module4/index.html#4.5.1.2>

Fernández, L. (2020). Aprende sobre redes con estos cursos gratuitos de Cisco. Recuperado de <https://www.redeszone.net/tutoriales/redes-cable/cursos-cisco-gratuitos/>

Gerometta, O. (2013). Apunte Rápido CCNA R&S v5.0. Recuperado de <http://librosnetworking.blogspot.com/2013/10/apunte-rapido-ccna-r-v50.html>

Gerometta, O. (2014). Principio de redes TCP/IP v5.1. Recuperado de <http://librosnetworking.blogspot.com/2014/03/principios-de-redes-tcpip-v51.html>

Gerometta, O. (2014). Operación de dispositivos Cisco IOS v5.1. Recuperado de <http://librosnetworking.blogspot.com/2014/04/operacion-de-dispositivos-cisco-ios-v51.html>

Netacad (2020). Estoy aprendiendo. Recuperado de <https://www.netacad.com/portal/learning>