

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

ANGIE NATALIA MENDOZA MENDOZA

TUTOR: JUAN CARLOS VESGA

GRUPO: 203092_8

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN
DE SOLUCIONES INTEGRADAS LAN / WAN
VÉLEZ
2020**

TABLA DE CONTENIDO

INTRODUCCIÓN	6
1. ESCENARIO 1	7
1.1. INICIALIZAR DISPOSITIVOS	8
1.2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS 11	
1.2.1 Configurar R1	11
1.2.2. Configurar R2	14
1.2.3. Configurar R3	16
1.2.4. Configurar S1	20
1.2.5. Configurar el S3	22
1.3. VERIFICAR LA CONECTIVIDAD DE LA RED	24
1.4.1 Configurar S1	25
1.4.2. Configurar el S3	27
1.4.3. Configurar R1	29
1.5. VERIFICAR LA CONECTIVIDAD DE LA RED	30
1.6. CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2	31
1.6.1 Configurar RIPv2 en el R1	31
1.6.2. Configurar RIPv2 en el R2	32
1.6.3. Configurar RIPv3 en el R2	33
1.7. VERIFICAR LA INFORMACIÓN DE RIP	34
.....	35
1.8. IMPLEMENTAR DHCP Y NAT PARA IPV4	36
1.9. CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2	37
1.10. VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA	39
1.11. CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL) 42	
2. ESCENARIO 2	46
2.1. PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO	47
2.2. PARTE 2: TABLA DE ENRUTAMIENTO	66

2.3. PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.....	71
2.4. PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF	73
2.5. PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP. 77	
2.6. PARTE 6: CONFIGURACIÓN DE PAT	78
2.7. PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.....	82
3. CONCLUSIONES	87
4. ANEXOS	88
REFERENCIAS BIBLIOGRÁFICAS.....	89

TABLA DE ILUSTRACIONES

Ilustración 1. Topología de la red.....	7
Ilustración 2. Ping de R1 a R2.....	24
Ilustración 3. Ping R2 a R3	24
Ilustración 4. Ping pc de internet a gateway predeterminado	25
Ilustración 5. Ping S1 a R1 Vlan 99.....	31
Ilustración 6. Ping S3 a R1 vlan 99	31
Ilustración 7. Ping S1 al R1 vlan 21	31
Ilustración 8. Ping S3 a R1 vlan 23	31
Ilustración 9. Comando show ip protocols.....	35
Ilustración 10. Comando show ip route rip	35
Ilustración 11. Prueba DHCP en PC-A.....	39
Ilustración 12. Prueba DHCP en PC-C	40
Ilustración 13. Ping PC-A a PC-C	40
Ilustración 14. Uso de navegador web.....	41
Ilustración 15. comando show ntp associations	42
Ilustración 16. Comando verificar ACL.....	43
Ilustración 17. Comando show access-list	43
Ilustración 18. Comando para restablecer los contadores de una lista de acceso	43
Ilustración 19. Comando para mostrar que ACL se aplica a una interfaz y dirección	44
Ilustración 20. Comando show ip nat translations	45
Ilustración 21. Topología configurada	45
Ilustración 22. Topología escenario 2	46
Ilustración 23. Comando show ip route en ISP	67
Ilustración 24. Comando show ip route en MEDELLIN1	68
Ilustración 25. show ip route en MEDELLIN2.....	68
Ilustración 26. Comando show ip route en MEDELLIN3	69

Ilustración 27. Comando show ip route en BOGOTA1.....	69
Ilustración 28. Comando show ip route en BOGOTA2.....	70
Ilustración 29. Comando show ip route en BOGOTA3.....	70
Ilustración 30. Comando show ip protocols en MEDELLIN1.....	74
Ilustración 31. Comando show ip protocols en MEDELLIN2.....	74
Ilustración 32. Protocolo show ip protocols en MEDELLIN3.....	75
Ilustración 33. Protocolo show ip protocols en BOGOTA1.....	75
Ilustración 34. Protocolo show ip protocols en BOGOTA2.....	76
Ilustración 35. Protocolo show ip en BOGOTA3.....	77
Ilustración 36. Ping MEDELLIN1 a MEDELLIN2 Y MEDELLIN3.....	81
Ilustración 37. Ping de BOGOTA1 a BOGOTA2 y BOGOTA3.....	82
Ilustración 38. DHCP en PC-3.....	85
Ilustración 39. DHCP en PC-4.....	85
Ilustración 40. Topología configurada escenario 2.....	86

INTRODUCCIÓN

A partir del estudio de las temáticas relacionadas con exploración de la red, configuración de un sistema operativo de red, protocolos y comunicaciones de red, acceso a la red, ethernet, capa de red, capa de transporte, asignación de direcciones IP, subNetting, capa de Aplicación, y soluciones de Red, introducción a redes conmutadas, configuración, conceptos básicos de switching, VLANs, conceptos de routing, enrutamiento entre VLANs, enrutamiento estático en la plataforma Cisco, enrutamiento dinámico, OSPF de una sola área, listas de control de acceso, DHCP y traducción de direcciones IP para IPv4 estudiadas en la plataforma Cisco se presenta el desarrollo de dos escenarios según la prueba de habilidades prácticas del curso Diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN las cuales se desarrollan partir de cisco packet tracer.

DESARROLLO

Descripción de escenarios propuestos para la prueba de habilidades

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.

Topología

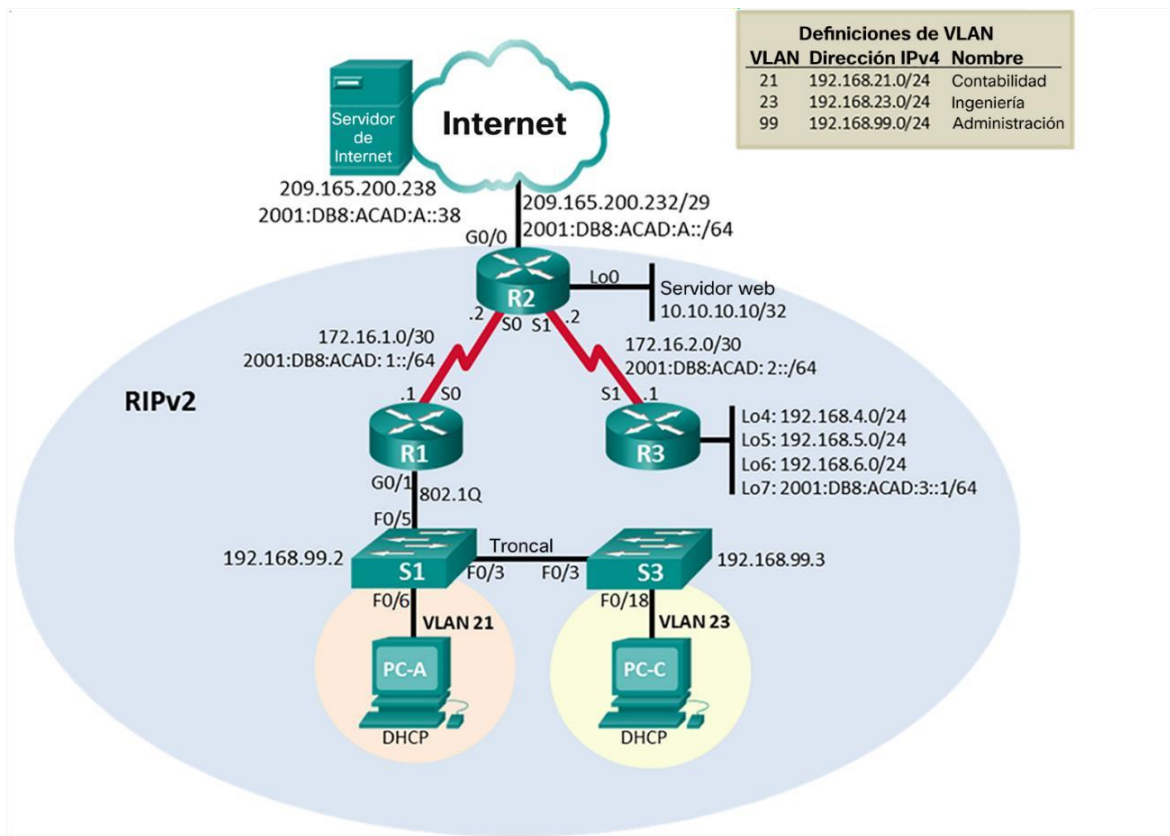


Ilustración 1. Topología de la red

1.1. INICIALIZAR DISPOSITIVOS

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.

- Eliminar el archivo startup-config de todos los routers

Para eliminar el archivo startup-config usamos el siguiente comando que nos permite borrar el contenido de la NVRAM de cada uno de los routers:

Router 1

```
Router>enable
```

```
Router# Erase startup-config
```

Router 2

```
Router>enable
```

```
Router# Erase startup-config
```

Router 3

```
Router>enable
```

```
Router# Erase startup-config
```

- Volver a cargar todos los routers

Con el uso del siguiente comando en cada uno de los routers, los volvemos a cargar.

Router 1

```
Router>enable
```

```
Router# reload
```

Router 2

```
Router>enable
```

```
Router# reload
```

Router 3

```
Router>enable
```

```
Router# reload
```

- Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

El commando utilizado para eliminar el archive startup-config de los switches el siguiente, el cual nos permite borrar el contenido de la NVRAM de cada switch:

Router 1

```
Switch>enable
```

```
Switch #Erase startup-config
```

Router 2

```
Switch>enable
```

```
Switch #Erase startup-config
```

Router 3

```
Switch>enable
```

```
Switch #Erase startup-config
```

- Para eliminar la base de datos de VLAN que exista en los switch se utiliza el siguiente commando:

Switch 1

```
Switch>enable
```

```
Switch # delete vlan.data
```

Switch 3

```
Switch >enable
```

Switch # delete vlan.data

- Volver a cargar ambos switches

Para Volver a cargar los switch utilizamos el comando siguiente que Tambien usamos en los routers en el modo exe privilegiado:

Switch 1

Switch>enable

Switch# reload

Switch 3

Switch>enable

Switch# reload

- Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Para verificar la base de datos de VLAN usamos el siguiente comando el modo exec privilegiado:

Switch 1

Switch> enable

Switch# show vlan brief

Switch 3

Switch> enable

Switch# show vlan brief

Para verificar la memoria flash usamos el siguiente código:

Switch 1

Switch> enable

Switch#show flash

Switch 3

Switch> enable

Switch#show flash

1.2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

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 La tomamos de la imagen
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233 primera ip en la red
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1 primera dirección

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.

1.2.1 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

- Desactivar la búsqueda DNS

Usamos el siguiente comando para desactivar la búsqueda de DNS en el router R1:

```
Router<enable
```

```
Router#conf t
```

```
Router(config)no ip domain-lookup
```

- Nombre del router

Para nombrar un router usamos el siguiente comando en el modo exec privilegiado:

```
Router>enable
```

```
Router# configure terminal
```

```
Router(config) hostname R1
```

- Contraseña de exec privilegiado cifrada

Para configurar la contraseña cifrada en el modo exe privilegiado (class) se usa el siguiente commando y se usa con el fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración.:

```
R1>enable
R1# configure terminal
R1(config)#enable password class
R1(config)#enable secret class
```

- Contraseña de acceso a la consola: Cisco

Para configurar la contraseña de acceso a consola ingresamos a línea de consola y asignamos la contraseña que deseamos utilizar en este caso cisco:

```
R1>enable
R1# configure terminal
R1(config)#line console 0 //ingresar al modo de configuración de la consola
R1(config-line)#password cisco //para indicar la contraseña de consola.
R1(config-line)#login // para habilitar la contraseña de seguridad de consola
utilizando un sistema de seguridad simple.
```

- Contraseña de acceso Telnet

Para conseguir la contraseña de acceso de telnet usamos el siguiente comando:

```
R1>enable
R1# configure terminal
```

```
R1(config)# line vty 0 4          // permiten el acceso a un dispositivo Cisco a través
de Telnet en lineas vty.
```

```
R1(config-line)# password cisco //se asigna la contraseña
```

```
R1(config-line)# Login          //habilita la contraseña de seguridad
```

```
R1(config-line)# exit          //salir
```

- Cifrar las contraseñas de texto no cifrado

Para cifrar las contraseñas usamos el siguiente comando en el modo exec privilegiado:

```
R1>enable
```

```
R1#configure terminal
```

```
R1(config)# service password-encryption //encripta la contraseña
```

- Mensaje MOTD

Para configurar el mensaje en el inicio del router usamos el siguiente Código:

```
R1>enable
```

```
Password: cisco
```

```
R1#conf t
```

```
R1(config)# banner motd #Prohibido el acceso no autorizado#
```

- Interfaz S0/0/0

Establezca la descripción

Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones

Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones

Establecer la frecuencia de reloj en 128000

Activar la interfaz

```
R1(config)#interface s0/0/0
R1(config-if)# ip address 172.16.1.1 255.255.255.252 //asigna la dirección ipv4
con su mascara a la interfaz mencionada
R1(config-if)#exit
R1(config)#interface s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 // asigna la dirección ipv6 con
su mascara a la interfaz mencionada.
R1(config-if)#no shutdown //activa la interfaz
R1(config-if)#clock rate 128000 //establece la frecuencia de reloj
R1(config-if)#no shutdown //activa la interfaz
R1(config-if)#
```

- Rutas predeterminadas

Configurar una ruta IPv4 predeterminada de S0/0/0

```
R1#configure terminal
R1(config) ip route 0.0.0.0.0.0.0.0 s0/0/0
```

Configurar una ruta IPv6 predeterminada de S0/0/0

```
R1#configure terminal
R1(config)# ipv6 route ::/0 S0/0/0
```

Nota: Todavía no configure G0/1.

1.2.2. Configurar R2

La configuración del R2 incluye las siguientes tareas:

- Desactivar la búsqueda DNS

```
Router>enable
```

```
Router#
```

```
Rouer#conf t
```

```
Router(config)# no ip domain-lookup
```

- Nombre del router

Para configurar el nombre del router usamos el siguiente código:

```
Router (config)#
```

```
Router(config)hostname R2
```

- Contraseña de exec privilegiado cifrada: Class

```
R2#conf t
```

```
R2(config)#enable password class
```

```
R2(config)#enable secret class
```

- Contraseña de acceso a la consola: Cisco

```
R2>enable
```

```
R2# configure terminal
```

```
R2(config)#line console 0 //ingresar al modo de configuración de la consola
```

```
R2(config-line)#password cisco //para indicar la contraseña de consola.
```

```
R2(config-line)#login // para habilitar la contraseña de seguridad de consola utilizando un sistema de seguridad simple
```

- Contraseña de acceso Telnet

```
Cisco
```

```
R2>enable
```

```
R2# configure terminal
```

```
R2(config)# line vty 0 4 // permiten el acceso a un dispositivo Cisco a través de Telnet en lineas vty.
```

```
R2(config-line)# password cisco //se asigna la contraseña
```

```
R2(config-line)# Login //habilita la contraseña de seguridad
```

```
R2(config-line)# exit //salir
```

- Cifrar las contraseñas de texto no cifrado

```
R2#configure terminal
```

```
R2(config)#service password-encryption
```

- Habilitar el servidor HTTP

Activar este protocolo nos permite utilizar una transferencia segura de datos en el navegador, con el siguiente comando lo activamos en nuestro router R2.

```
R2#configure terminal
```

```
R2(config)# ip http secure-server
```

```
R2(config)# end
```

- Mensaje MOTD

Para configurar el mensaje en el inicio del router usamos el Código siguiente:

```
R2>enable
```

```
Password: cisco
```

```
R2#conf t
```

```
R2(config)# banner motd #Prohibido el acceso no autorizado#
```

1.2.3. Configurar R3

La configuración del R3 incluye las siguientes tareas:

- Desactivar la búsqueda DNS

```
Router>enable
```

```
Router#conf t
```

```
Router(config)#no ip domain-lookup //desactiva la búsqueda DNS
```

- Nombre del router: R3

```
Router# configure terminal
```

```
Router(config) #hostname R3 //Asigna el nombre del router R3.
```

- Contraseña de exec privilegiado cifrada: Class

```
R3>enable
```

```
R3#conf t
```

```
R3(config)#enable password class
```

```
R3(config)#enable secret class
```

- Contraseña de acceso a la consola: Cisco

```
R3#conf t
```

```
R3(config)# line console 0 //ingresa al modo de configuración de la consola.
```

```
R3(config-line)# password cisco //se asigna la contraseña
```

```
R3(config-line)# login //habilitar la contraseña de seguridad de consola utilizando un sistema de seguridad simple.
```

- Contraseña de acceso Telnet: Cisco

```
R3>enable
```

```
R3# configure terminal
```

```
R3(config)# line vty 0 4 // permiten el acceso a un dispositivo Cisco a través de Telnet en líneas vty.
```

```
R3(config-line)# password cisco //se asigna la contraseña
```

```
R3(config-line)# Login //habilita la contraseña de seguridad
```

```
R3(config-line)# exit //salir
```

- Cifrar las contraseñas de texto no cifrado

```
R3#configure terminal
```

```
R3(config)#service password-encryption
```

- Mensaje MOTD

```
R3#configure terminal
```

```
R3(config)# banner motd #Se prohíbe el acceso no autorizado#
```

- Interfaz S0/0/1

Establecer la descripción

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

Activar la interfaz

```
R3(config)#interface s0/0/1
```

```
R3(config-if)# ip address 172.16.2.1 255.255.255.252 //asigna la dirección ipv4 con su mascara a la interfaz mencionada
```

```
R3(config-if)#exit
```

```
R3(config)#interface s0/0/1
```

```
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 // asigna la dirección ipv6 con su mascara a la interfaz mencionada.
```

```
R3(config-if)#no shutdown //activa la interfaz
```

- Interfaz loopback 4

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config)#interface loopback 4 //se digita que interfaz se va a configurar.
```

```
R3(config-if)# ip address 192.168.4.1 255.255.255.0 //asigna la dirección ip y mascara de subred a la interfaz lo4
```

```
R3(config-if)#exit
```

- Interfaz loopback 5

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config)#interface loopback 5 //se digita que interfaz se va a configurar.  
R3(config-if)# ip address 192.168.5.1 255.255.255.0 //asigna la dirección ip y  
mascara de subred a la interfaz lo5  
R3(config-if)#exit
```

- Interfaz loopback 6

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config)#interface loopback 6 //se digita que interfaz se va a configurar.  
R3(config-if)# ip address 192.168.6.1 255.255.255.0 //asigna la dirección ip y  
mascara de subred a la interfaz lo6  
R3(config-if)#exit
```

- Interfaz loopback 7

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

```
R3(config)#interface loopback 7 //se digita que interfaz se va a configurar.  
R3(config-if)# ip address 2001:DB8:ACAD:3::1/64 //asigna la dirección ip y mascara  
de subred a la interfaz lo7  
R3(config-if)#exit
```

- Rutas predeterminadas

Configure una ruta IPv4 predeterminada de s0/0/1.

```
R3(config)#ip route 0.0.0.0.0.0.0 s0/0/1
```

Configure una ruta IPv6 predeterminada de s0/0/1

```
R3(config)#ipv6 route ::/0 s0/0/1
```

1.2.4. Configurar S1

La configuración del S1 incluye las siguientes tareas:

- Desactivar la búsqueda DNS

```
Switch>enable
```

```
Switch#conf t
```

```
Switch(config)#no ip domain-lookup
```

- Nombre del switch

Para configurar el nombre del switch usamos el siguiente comando:

```
Switch (config)#hostname S1
```

```
S1(config)#
```

- Contraseña de exec privilegiado cifrada: Class

Para configurar la contraseña cifrada en el modo exe privilegiado (class) se usa el siguiente commando y se usa con el fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración:

```
S1>enable
```

```
S1# configure terminal
```

```
S1(config)#enable password class
```

```
S1(config)#enable secret class
```

- Contraseña de acceso a la consola: Cisco

```
S1>enable
```

```
S1# configure terminal
```

```
S1(config)#line console 0 //ingresar al modo de configuración de la consola
S1(config-line)#password cisco //para indicar la contraseña de consola.
R1(config-line)#login // para habilitar la contraseña de seguridad de consola
utilizando un sistema de seguridad simple.
```

- Contraseña de acceso Telnet: Cisco

```
S1>enable
S1# configure terminal
S1(config)# line vty 0 4 // permiten el acceso a un dispositivo Cisco a través de
Telnet en líneas vty.
S1(config-line)# password cisco //se asigna la contraseña
S1(config-line)# Login //habilita la contraseña de seguridad
S1(config-line)# exit //salir
```

- Cifrar las contraseñas de texto no cifrado

Para cifrar las contraseñas usamos el siguiente comando en el modo exec privilegiado:

```
S1>enable
S1#configure terminal
S1(config)#service password-encryption //encripta la contraseña
```

- Mensaje MOTD: Se prohíbe el acceso no autorizado.

Para configurar un mensaje usamos el comando `banner motd ##` para que aparezca en el inicio el mensaje que deseamos, en este caso “se prohíbe el acceso no autorizado”:

```
S1>enable
S1#configure terminal
```

S1(config)#banner motd #se prohíbe el acceso no autorizado# //muestra en la configuración del router el mensaje.

1.2.5. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

- Desactivar la búsqueda DNS

```
Switch>enable
```

```
Switch#conf t
```

```
Switch(config)#no ip domain-lookup
```

- Nombre del switch: S3

```
Switch#conf t
```

```
Switch(config)#hostname S3
```

- Contraseña de exec privilegiado cifrada: Class

Para configurar la contraseña cifrada en el modo exe privilegiado (class) se usa el siguiente comando y se usa con el fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración.:

```
S3>enable
```

```
S3# configure terminal
```

```
S3(config)#enable password class
```

```
S3(config)#enable secret class
```

- Contraseña de acceso a la consola: Cisco

Para configurar la contraseña de acceso a consola ingresamos a línea de consola y asignamos la contraseña que deseamos utilizar en este caso cisco:

```
S3>enable
S3# configure terminal
S3(config)#line console 0 //ingresar al modo de configuración de la consola
S3(config-line)#password cisco //para indicar la contraseña de consola.
S3(config-line)#login // para habilitar la contraseña de seguridad de consola
utilizando un sistema de seguridad simple.
```

- Contraseña de acceso Telnet: Cisco

Para conseguir la contraseña de acceso de telnet usamos el siguiente comando:

```
S3>enable
S3# configure terminal
S3(config)# line vty 0 4 // permiten el acceso a un dispositivo Cisco a través de
Telnet en líneas vty.
S3(config-line)# password cisco //se asigna la contraseña
S3(config-line)# Login //habilita la contraseña de seguridad
S3(config-line)# exit //salir
```

- Cifrar las contraseñas de texto no cifrado

Para cifrar las contraseñas usamos el siguiente comando en el modo exec privilegiado:

```
S3>enable
S3#configure terminal
S3(config)# service password-encryption //encripta la contraseña
```

- Mensaje MOTD

Se usa el siguiente Código para que muestre en la pantalla el mensaje que queremos:

```
S3#conf t
```

```
S3(config)#banner motd # Se prohíbe el acceso no autorizado#
```

1.3. 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	172.16.1.2	<p>Exitoso</p> <pre>R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/69/292 ms</pre> <p><i>Ilustración 2. Ping de R1 a R2</i></p>
R2	R3, S0/0/1	172.16.2.1	<p>Exitoso</p> <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 = 1/11/63 ms</pre> <p><i>Ilustración 3. Ping R2 a R3</i></p>
PC de Interne t	Gateway predeter minado	209.165.20 0.233	Exitoso

			<pre>Packet Tracer SERVER Command Line 1.0 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=318ms TTL=255 Reply from 209.165.200.233: bytes=32 time<lms TTL=255 Reply from 209.165.200.233: bytes=32 time<lms TTL=255 Reply from 209.165.200.233: bytes=32 time<lms 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 = 318ms, Average = 79ms</pre>
			<p><i>Ilustración 4. Ping pc de internet a gateway predeterminado</i></p>

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

1.4. CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

1.4.1 Configurar S1

La configuración del S1 incluye las siguientes tareas:

- Crear la base de datos de VLAN

Para crear y nombrar cada una de las VLAN de la table usamos el siguiente comando:

S1>enable

Password: cisco

S1#conf t

S1(config)#vlan 21 //se nombra la vlan 21 que se va a trabajar

S1(config-vlan)#name Contabilidad //con este comando se le asigna el nombre a la vlan

S1(config)#vlan 23

S1(config-vlan)#name Ingenieria

S1(config)#vlan 99

S1(config-vlan)#name Administración

- Asignar la dirección IP de administración.

Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología

```
S1(config)#interface vlan 99 //se llama la interfaz vlan 99
```

```
S1(config-if)# ip address 192.168.99.2 255.255.255.0 //asigna la dirección ip a la interfaz vlan 99
```

```
S1(config-if)# no shutdown //activa la interfaz
```

- Asignar el gateway predeterminado

Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

```
S1#conf t
```

```
S1(config)# ip default-gateway 192.168.99.1 //asigna la dirección ip como el gateway predeterminado.
```

- Forzar el enlace troncal en la interfaz F0/3

Utilizar la red VLAN 1 como VLAN nativa

```
S1(config)# int f0/3
```

```
S1(config-if)# switchport trunk nativa vlan 1
```

- Forzar el enlace troncal en la interfaz F0/5

Utilizar la red VLAN 1 como VLAN nativa

```
S1(config-if)# int f0/5
```

```
S1(config-if)# switchport mode trunk
```

```
S1(config-if)# switchport trunk native vlan 1
```

- Configurar el resto de los puertos como puertos de acceso

Utilizar el comando interface range

```
S1#configure terminal
```

```
S1(config-if)# interface range f0/1-2, f0/4, f0/6-24, g0/1-2 //se escribe el rango de interfaces que se van a configurar
```

```
S1(config-if)# switchport mode access //se configuran los puertos como puertos de acceso.
```

- Asignar F0/6 a la VLAN 21

```
S1(config-if)# switchport access vlan 21 //se usa para asignar f0/6 a la vlan 21
```

- Apagar todos los puertos sin usar

```
S1(config-if)# interface range f0/1-2, f0/4, f0/7-24, g0/1-2 //se escriben el rango de interfaces que se van a apagar.
```

```
S1(config-if-range) # shutdown // se apagan
```

1.4.2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

- Crear la base de datos de VLAN

Para crear y nombrar cada una de las VLAN de la table usamos el siguiente comando:

```
S3>enable
```

```
S3#conf t
```

```
S3(config)#vlan 21
```

```
S3(config-vlan)# name Contabilidad
```

```
S3(config)#vlan 23
```

```
S3(config-vlan)# name Ingenieria
```

```
S3(config)#vlan 99
```

```
S3(config-vlan)# name Administración
```

- Asignar la dirección IP de administración

Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología

```
S3(config-vlan) #int vlan 99
```

```
S3(config-if) #ip address 192.168.99.3 255.255.255.0 /asigna la dirección ip y la mascara de subred
```

```
S3(config-if) #no shutdown //active la interfaz
```

- Asignar el gateway predeterminado.

Asignar la primera dirección IP en la subred como gateway predeterminado.

```
S3#config t
```

```
S3(config)#ip default-gateway 192.168.99.1
```

- Forzar el enlace troncal en la interfaz F0/3

Utilizar la red VLAN 1 como VLAN nativa

```
S3(config-if) # switchport mode trunk
```

```
S3(config-if) # switchport trunk native vlan 1
```

- Configurar el resto de los puertos como puertos de acceso

Utilizar el comando interface range

```
S3(config)# interface range f0/1-2, f0/4-24, g0/1-2
```

```
S3(config-if-range)# switchport mode access
```

- Asignar F0/18 a la VLAN 23

```
S3(config-if-range)# int f0/18
```

```
S3(config-if)# switchport access vlan 23
```

- Apagar todos los puertos sin usar

```
S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
```

```
S3(config)#shutdown //se apagan los puertos anteriores
```

1.4.3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

- Configurar la subinterfaz 802.1Q .21 en G0/1

Descripción: LAN de Contabilidad

Asignar la VLAN 21

Asignar la primera dirección disponible a esta interfaz

```
R1#conf t
```

```
R1(config t)# int 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
```

- Configurar la subinterfaz 802.1Q .23 en G0/1

Descripción: LAN de Ingeniería

Asignar la VLAN 23

Asignar la primera dirección disponible a esta interfaz

```
R1(config)# int g0/1.23
```

```
R1(config-subif)# description VLAN 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

Descripción: LAN de Administración

Asignar la VLAN 99

Asignar la primera dirección disponible a esta interfaz

```
R1(config)# int g0/1.99
```

```
R1(config-subif)# description VLAN de Administracion
```

```
R1(config-subif)# encapsulation dot1q 99
```

```
R1(config-subif)# ip address 192.168.99.1 255.255.255.0
```

```
R1(config-subif)# exit
```

- Activar la interfaz G0/1

```
R1(config)# int g0/1 //se escribe la interfaz que se va a activar
```

```
R1(config-if)#no shutdown //activa la interfaz
```

1.5. 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:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso

			<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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms</pre> <p style="text-align: center;"><i>Ilustración 5. Ping S1 a R1 Vlan 99</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 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms</pre> <p style="text-align: center;"><i>Ilustración 6. Ping S3 a R1 vlan 99.</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 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms</pre> <p style="text-align: center;"><i>Ilustración 7. Ping S1 al R1 vlan 21</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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms</pre> <p style="text-align: center;"><i>Ilustración 8. Ping S3 a R1 vlan 23</i></p>

1.6. CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2

1.6.1 Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

- Configurar RIP versión 2

Para activar y configurar RIP versión 2 se usa el siguiente código:

```
R1(config) #router rip
```

```
R1(config-router)# version
```

- Anunciar las redes conectadas directamente

Asigne todas las redes conectadas directamente.

```
R1(config)# router rip
```

```
R1(config-router)# version 2
```

```
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
```

- Establecer todas las interfaces LAN como pasivas

Para establecer las interfaces LAN como pasivas se usa el siguiente Código:

```
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
```

1.6.2. Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

- Configurar RIP versión 2

```
R2#conf t
```

```
R2(config)# router rip
```

```
R2(config-router)# version 2
```

- Anunciar las redes conectadas directamente

Nota: Omitir la red G0/0.

```
R2(config-router)#do show ip route connected
```

Este despliega las redes conectadas y se anuncian

```
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial10/0/0
C 172.16.2.0/30 is directly connected, Serial10/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
```

```
R2(config-router)# network 10.10.10.10
```

```
R2(config-router)# network 172.16.1.0
```

```
R2(config-router)# network 172.16.2.0
```

- Establecer la interfaz LAN (loopback) como pasiva

Para establecer la interfaz lan loopback 0 como pasiva se usa el siguiente comando:

```
R2(config-router)#passive-interface loopback 0
```

- Desactive la sumarización automática.

```
R2(config-router)# no auto-summary
```

1.6.3. Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

- Configurar RIP versión 2

Se usa el siguiente comando para activar el uso de la RIP versión 2

```
R3(config)#router rip
```

```
R3(config-router) version 2
```

- Anunciar redes IPv4 conectadas directamente

```
R3(config-router)# do show ip route connected
```

Se anuncian las redes ipv4 conectadas directamente

```
C 172.16.2.0/30 is directly connected, Serial10/0/1
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
```

- Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

Para establecer ls interfaces loopback como pasivas se usa el siguiente comando:

```
R3(config-router)# passive-interface loopback 4
```

```
R3(config-router)# passive-interface loopback 5
```

```
R3(config-router)# passive-interface loopback 6
```

- Desactive la sumarización automática.

Para desactivar la sumarización automática se usa el siguiente comando:

```
R3(config-router)# no auto-summary
```

1.7. VERIFICAR LA INFORMACIÓN DE RIP

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

- ¿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?

```
Router #Show ip protocols
```

```

R3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 5 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
  
```

Ilustración 9. Comando show ip protocols

- ¿Qué comando muestra solo las rutas RIP?

Router #Show ip route rip

```

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, 00:00:00, 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, 00:00:00, 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, 00:00:00, Serial0/0/1
R   192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:00, Serial0/0/1
R   192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:00, Serial0/0/1
  
```

Ilustración 10. Comando show ip route rip

- ¿Qué comando muestra la sección de RIP de la configuración en ejecución?

Router#Show run

1.8. IMPLEMENTAR DHCP Y NAT PARA IPV4

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

Las tareas de configuración para R1 incluyen las siguientes:

- 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 //las direcciones ip excluidas desde la primera ip hasta la última utilizable
```

- 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 //las direcciones ip excluidas desde la primera ip hasta la última utilizable
```

- Crear un pool de DHCP para la VLAN 21.

Nombre: ACCT

Servidor DNS: 10.10.10.10

Nombre de dominio: ccna-sa.com

Establecer el gateway predeterminado

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
```

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
```

```
R1(config)#ip dhcp pool ACT
```

```
R1(config-config)#network 192.168.21.0 255.255.255.0 R1(config-config)#default-router 192.168.21.0
```

```
R1(config-config)#dns-server 10.10.10.10
```

```
R1(config-config)#domain-name ccna-sa.com //se asigna el nombre del dominio
```

- Crear un pool de DHCP para la VLAN 23

Nombre: ENGNR

Servidor DNS: 10.10.10.10

Nombre de dominio: ccna-sa.com

Establecer el gateway predeterminado

Se usa el siguiente commando para la configuración:

```
R1(dhcp-config)# ip dhcp pool ENGNR
```

```
R1(dhcp-config)# NETWORK 192.168.23.0 255.255.255.0
```

```
R1(dhcp-config)#default-router 192.168.23.1
```

```
R1(dhcp-config)#domain-name ccna-sa.com
```

1.9. CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

- Crear una base de datos local con una cuenta de usuario:

Nombre de usuario: webuser

Contraseña: cisco12345

Nivel de privilegio: 15

```
R2#conf t
```

```
R2(config)#username webuser privilege 15 secret cisco12345
```

- Habilitar el servicio del servidor HTTP

```
R2#configure terminal
```

```
R2(config)#ip http server
```

- Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

```
R2#configure terminal
```

```
R2(config)#ip http authentication local
```

- Crear una NAT estática al servidor web.

Dirección global interna: 209.165.200.237

```
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)#int g0/0
```

```
R2(config-if)#ip nat outside
```

```
R2(config-if)#int s0/0/0
```

```
R2(config-if)#ip nat inside
```

```
R2(config-if)#int s0/0/1
```

```
R2(config-if)#ip nat inside
```

- Configurar la NAT dinámica dentro de una ACL privada:

Lista de acceso: 1

Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1

Permitir la traducción de un resumen de las redes LAN (loopback) en el R3

```
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
```

- Defina el pool de direcciones IP públicas utilizables

Nombre del conjunto: INTERNET

El conjunto de direcciones incluye:

209.165.200.225 – 209.165.200.228 No se emplean las direcciones dadas teniendo en cuenta que en nuestra red el rango es 209.165.200.233 a 209.165.200.238

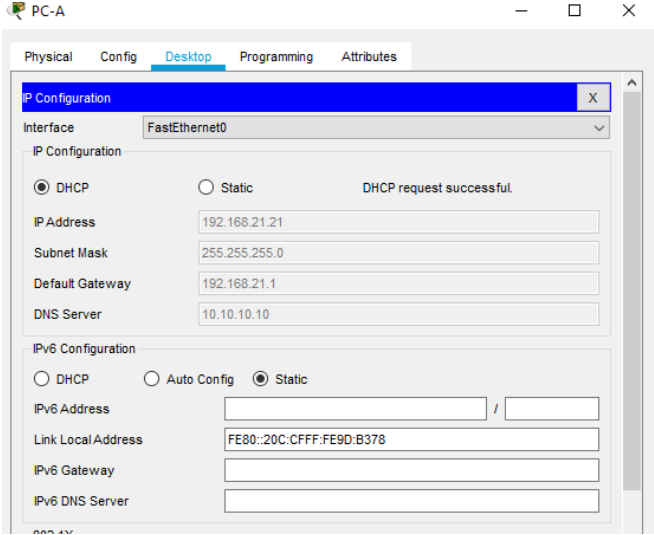
```
R2(config)#ip nat pool INTERNET 209.200.233 209.165.200.236 netmask 255.255.255.248
```

- Definir la traducción de NAT dinámica

```
R2(config)#ip nat inside source list 1 pool INTERNET
```

1.10. 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
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	 <p><i>Ilustración 11. Prueba DHCP en PC-A</i></p>

<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	
------------------------------------------------------------------------------------	--

Ilustración 12. Prueba DHCP en PC-C

<p>Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	<pre>C:\>ping 192.168.23.21 Pinging 192.168.23.21 with 32 bytes of data: Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time=1ms TTL=127 Reply from 192.168.23.21: bytes=32 time=1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.23.21: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre>
--------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Ilustración 13. Ping PC-A a PC-C

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

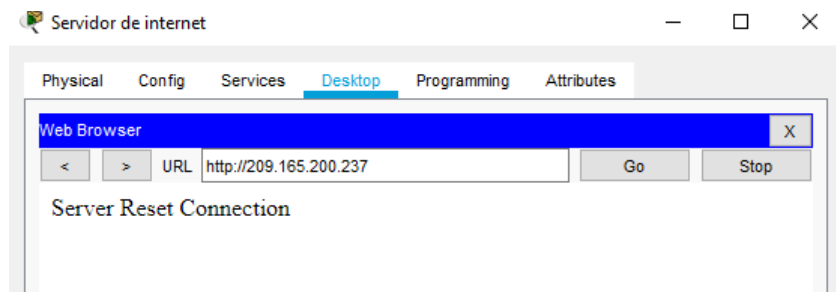


Ilustración 14. Uso de navegador web

Configurar NTP

- Ajuste la fecha y hora en R2: 5 de marzo de 2016, 9 a. m.

```
R2#clock set 9:00:00 05 march 2016
```

- Configure R2 como un maestro NTP.

Nivel de estrato: 5

```
R2#conf t
```

```
R2(config)# ntp master 5
```

- Configurar R1 como un cliente NTP: Servidor: R2

```
R1(config)#ntp server 172.16.1.2
```

- Configure R1 para actualizaciones de calendario periódicas con hora NTP.

```
R1(config)# ntp update-calendar
```

R1(config)#exit

- Verifique la configuración de NTP en R1

R1#show ntp associations

```
R1#show ntp associations
```

```
address          ref clock      st  when   poll   reach  delay
offset          disp
~172.16.1.2     127.127.1.1   5   0      16     3      8.00
725585235106.00  0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
```

Ilustración 15. comando show ntp associations

1.11. CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

Restringir el acceso a las líneas VTY en el R2

- Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

Nombre de la ACL: ADMIN-MGT

```
R2(config)#ip access-list standard ADMIN-MGT
```

```
R2(config-std-nacl)#permit nost 172.16.1.1
```

- Aplicar la ACL con nombre a las líneas VTY

```
R2(config)#line vty 0 4
```

```
R2(config-line)#access-class ADMIN-MGT in
```

Permitir acceso por Telnet a las líneas de VTY

```
R2(config-line)# transport input telnet
```

- Verificar que la ACL funcione como se espera

```

R1>enable
R1#telnet 172.16.1.2

R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenProhibido el acceso no autorizado

User Access Verification

Password:
R2>xit
Translating "xit"
% Unknown command or computer name, or unable to find computer
address

R2>|

```

Ilustración 16. Comando verificar ACL

Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

- Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

```

R2#show access-list

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))

```

Ilustración 17. Comando show access-list

- Restablecer los contadores de una lista de acceso

```

R2#clear ip access-list counters

R2#clear ip access-list counters
^
% Invalid input detected at '^' marker.

```

Ilustración 18. Comando para restablecer los contadores de una lista de acceso

- ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

#Show ip interface

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
--More-- |
```

Ilustración 19. Comando para mostrar que ACL se aplica a una interfaz y dirección

- ¿Con qué comando se muestran las traducciones NAT?

Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

Show ip nat translations

```

R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
global
--- 209.165.200.237    10.10.10.10      ---                ---
tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1030 209.165.200.238:1030
tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1031 209.165.200.238:1031
    
```

Ilustración 20. Comando show ip nat translations

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

Clear ip translations *

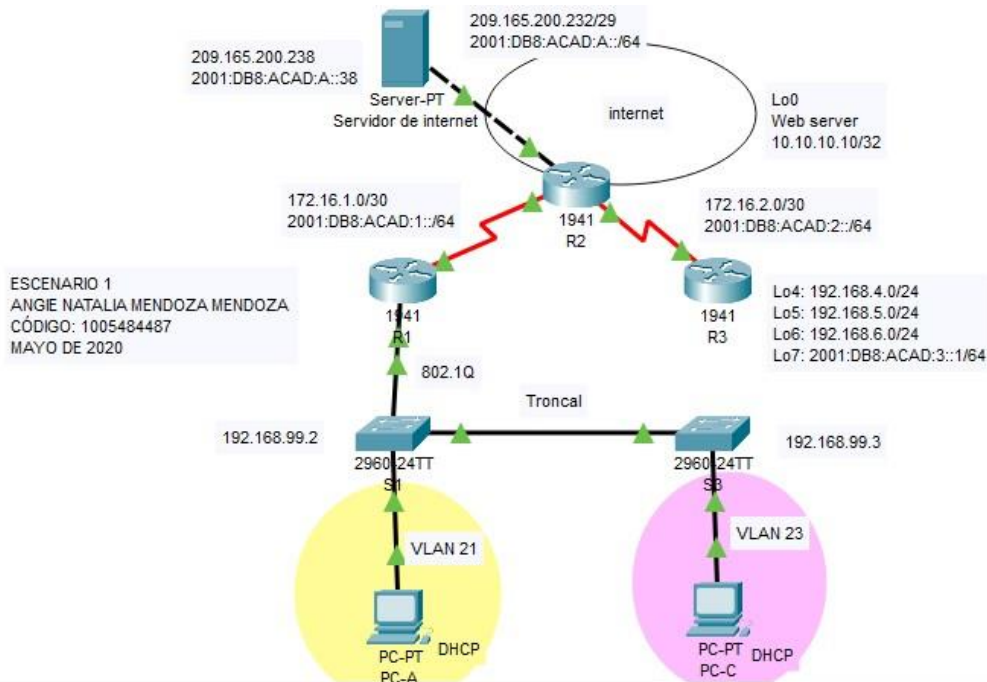


Ilustración 21. Topología configurada

2. ESCENARIO 2

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

Topología de red

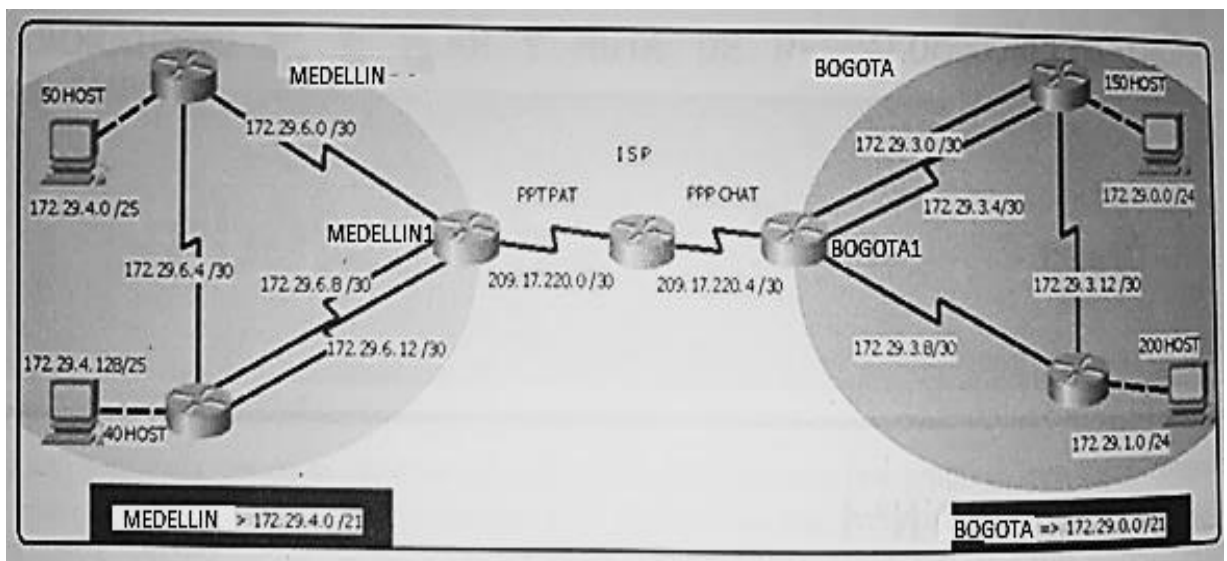


Ilustración 22. Topología escenario 2

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.

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).

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

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

2.1. PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

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

1. Configuración del router ISP

- Configuración del nombre

```
Router>enable
```

```
Router#conf t
```

```
Router#hostname ISP
```

- Configuración general

```
ISP>enable
```

```
ISP#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
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 4
```

```
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)#
```

Configuración interfaces

- Interfaz S0/1/0

```
ISP>enable
ISP#conf t
ISP(config)#int s0/1/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252 //dirección ip de acuerdo
a la topología.
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
```

```
ISP>enable
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/1/0
ISP(config-if)#
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
This command applies only to DCE interfaces
ISP(config-if)#no shutdown
```

- Interfaz s0/0/0

```
ISP(config-if)#int s0/0/0
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ISP(config-if)#exit
```

- Configuración del protocolo OSPF V2

```
ISP#conf t
```

```
ISP(config)#router ospf 2 // configuración global para habilitar OSPF en ISP
```

```
ISP(config-router)#do show ip route connected
```

```
C 209.17.220.0/30 is directly connected, Serial0/1/0
```

```
C 209.17.220.4/30 is directly connected, Serial0/0/0
```

Se configuran las instrucciones network para las redes utilizando la ID de área 0

```
ISP(config-router)#network 209.17.220.0 0.0.0.255 area 0
```

```
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
```

```
ISP(config-router)#ISP(config-router)#do show ip route connected
```

- Configuración de la desactivación de la sumarización automática

```
ISP(config-router)#no auto-summary
```

```
ISP(config-router)#
```

2. Configuración del router MEDELLIN1

- Configuración del nombre del router

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#hostname MEDELLIN1
```

- Configuración general

```
MEDELLIN1>enable
```

```
MEDELLIN1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
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 4
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)#
```

Configuración de interfaces

- Interface s0/1/0

```
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#description MEDELLIN1 A ISP
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#shutdown
MEDELLIN1(config-if)#exit
```

- Interface s0/0/0

```
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#description MEDELLIN1-MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#shutdown
MEDELLIN1(config-if)#exit
```

```
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#description MEDELLIN1-MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN1(config-if)#shutdown
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#
```

- Interface s0/0/1

```
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#description MEDELLIN1-MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#shutdown
MEDELLIN1(config-if)#exit
```

- Interface s0/1/1

```
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#description MEDELLIN1-MEDELLIN3/2
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#shutdown
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#
```

- Configurar el protocolo ospf

```
MEDELLIN1>enable
MEDELLIN1#conf t
    MEDELLIN1(config)#router ospf 1 //configuración global para habilitar OSPF
    en MEDELLIN1
MEDELLIN1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/1/0
```

Se configuran las instrucciones network para las redes utilizando la ID de área 0

```
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.255 area 0
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0
MEDELLIN1(config-router)#
```

- Configurar la desactivación de la sumarización automática

```
MEDELLIN1(config-router)#no auto-summary
MEDELLIN1(config-router)#
    MEDELLIN1(config-router)#no auto-summary
    MEDELLIN1(config-router)#|
```

3. Configuración router MEDELLIN2

- Nombre del router

```
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#
```

- Configuración general

```
MEDELLIN2>enable
```

```
MEDELLIN2#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
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 4
```

```
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)#
```

Configuración de interfaces:

- Interface s0/0/0

```
MEDELLIN2(config)#int s0/0/0
```

```
MEDELLIN2(config-if)#description MEDELLIN2-MEDELLIN1
```

```
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
```

```
MEDELLIN2(config-if)#clock rate 128000
```

```
MEDELLIN2(config-if)#shutdown
```

```
MEDELLIN2(config-if)#exit
```

- Interface s0/1/0

```
MEDELLIN2(config)#int s0/1/0
```

```
MEDELLIN2(config-if)#description MEDELLIN2-MEDELLIN3
```

```
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
```

```
MEDELLIN2(config-if)#clock rate 128000
```

```
MEDELLIN2(config-if)#shutdown
```

```
MEDELLIN2(config-if)#exit
```

- Intergace g0/0

```
MEDELLIN2(config)#int g0/0
```

```
MEDELLIN2(config-if)#description MEDELLIN2-PC1
```

```
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128.
```

```
MEDELLIN2(config-if)#shutdown
```

- Configuración del protocolo OSP V2

```
MEDELLIN2>ENABLE
```

```
MEDELLIN2#CONF T
```

```
MEDELLIN2(config)#ROUTER OSPF 1 //configuración global para  
habilitar OSPF en MEDELLIN2
```

```
MEDELLIN2(config-router)#DO SHOW IP ROUTE CONNECTED
```

```
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
```

```
C 172.29.6.0/30 is directly connected, Serial0/0/0
```

```
C 172.29.6.4/30 is directly connected, Serial0/1/0
```

Se configuran las instrucciones network para las redes utilizando la ID de área 0

```
MEDELLIN2(config-router)#NETWORK 172.29.4.0 0.0.0.255 AREA 0
```

```
MEDELLIN2(config-router)#NETWORK 172.29.6.0 0.0.0.3 AREA 0
```

```
MEDELLIN2(config-router)#NETWORK 172.29.6.4 0.0.0.3 AREA 0
```

```
MEDELLIN2(config-router)#
```

- Configuración de la desactivación de la sumarización automática.

```
MEDELLIN2(config-router)#no auto-summary
```

4. Configuración Router MEDELLIN3

- Configuración del nombre

```
ROUTER>enable
```

```
ROUTER#conf t
```

```
ROUTER#hostname MEDELLIN3
```

- Configuración general

```
MEDELLIN3>enable
```

```
MEDELLIN3#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
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 4
```

```
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)#
```

Configuración de las interfaces

- Interface s0/0/1

```
MEDELLIN3(config)#int s0/1/1
```

```
MEDELLIN3(config-if)#description MEDELLIN3-MEDELLIN2_2
```

```
MEDELLIN3(config-if)#description MEDELLIN3-MEDELLIN1_2
```

```
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
```

```
MEDELLIN3(config-if)#clock rate 128000
```

```
MEDELLIN3(config-if)#no shutdown
```

- Interface s0/0/1

```
MEDELLIN3(config)#int s0/0/1
```

```
MEDELLIN3(config-if)#description 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
```

- Interface s0/1/1

```
MEDELLIN3(config)#int s0/1/0
```

```
MEDELLIN3(config-if)#description 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
```

- G0/0

```
MEDELLIN3(config)#int g0/0
```

```
MEDELLIN3(config-if)#description MEDELLIN1-PC2
```

```
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
```

```
MEDELLIN3(config-if)#no shutdown
```

- Configuración del protocolo OSPF

```
MEDELLIN3>enable
```

```
MEDELLIN3#conf t
```

```
MEDELLIN3(config)#router ospf 1 //configuración global para habilitar OSPF
```

```
en MEDELLIN3
```

```
MEDELLIN3(config-router)#do show ip route connected
```

- C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
- C 172.29.6.4/30 is directly connected, Serial0/0/1
- C 172.29.6.8/30 is directly connected, Serial0/1/0
- C 172.29.6.12/30 is directly connected, Serial0/1/1

configuran las instrucciones network para las redes utilizando la ID de área 0

```
MEDELLIN3(config-router)#network 172.29.4.18 0.0.0.255 area 0
```

```
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0
```

```
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0
```

```
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0
```

```
MEDELLIN3(config-router)#
```

- Configuración no auto sumarización

```
MEDELLIN3(config-router)#no auto-summary
```

5. ROUTER BOGOTA1

- Configuración nombre del router

```
Router(config)#hostname BOGOTA1
```

- Configuración general

```
BOGOTA1>enable
```

```
BOGOTA1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
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 4
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)#
```

- Configuración interfaces

Interfaz s0/0/0

```
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#description 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
```

- Interfaz s0/0/1

```
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#description BOGOTA1-BOGOTA2_1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
```

- Interfaz s0/1/0

```
BOGOTA1(config)#int s0/1/0
BOGOTA1(config-if)#description BOGOTA1-BOGOTA2_2
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
```

```
BOGOTA1(config-if)#clock rate 128000
```

```
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#exit
```

- Interfaz s0/1/1

```
BOGOTA1(config)#int s0/1/1
```

```
BOGOTA1(config-if)#description BOGOTA1-BOGOTA3
```

```
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
```

```
BOGOTA1(config-if)#clock rate 128000
```

```
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#exit
```

- Configuración del protocolo OSPF

```
BOGOTA1>enable
```

```
BOGOTA1#conf t
```

```
BOGOTA1(config)#router ospf 1 //configuración global para habilitar OSPF en
```

```
BOGOTA1
```

```
BOGOTA1(config-router)#do show ip route connected
```

```
C 172.29.3.0/30 is directly connected, Serial0/1/0
```

```
C 172.29.3.4/30 is directly connected, Serial0/0/1
```

```
C 172.29.3.8/30 is directly connected, Serial0/1/1
```

```
C 209.17.220.4/30 is directly connected, Serial0/0/0
```

```
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.255 area 0
```

```
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 0
```

```
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 0
```

```
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
```

```
BOGOTA1(config-router)#
```

- Desactivación de la sumarización automática

```
BOGOTA1(config-router)#no auto-summary
```

6. CONFIGURACIÓN ROUTER BOGOTA 2

- Configuración nombre

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#hostname BOGOTA2
```

- Configuración general

```
BOGOTA2>enable
```

```
BOGOTA2#conf t
```

```
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 4
```

```
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)#
```

- Configuración de interfaces o puertos

```
Interfaz s0/0/1
```

```
BOGOTA2(config)#int s0/0/1
```

```
BOGOTA2(config-if)#description BOGOTA2-BOGOTA1_2
```

```
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
```

```
BOGOTA2(config-if)#clock rate 128000
```

```
BOGOTA2(config-if)#no shutdown
```

- Interfaz s0/1/0

```
BOGOTA2(config)#int s0/1/0
```

```
BOGOTA2(config-if)#description BOGOTA2-BOGOTA1_1
```

```
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
```

```
BOGOTA2(config-if)#clock rate 128000
```

```
BOGOTA2(config-if)#no shutdown
```

```
BOGOTA2(config-if)#exit
```

- Interfaz s0/0/0

```
BOGOTA2(config)#int s0/0/0
```

```
BOGOTA2(config-if)#description 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-if)#exit
```

- Interfaz g0/0

```
BOGOTA2(config)#int g0/0
```

```
BOGOTA2(config-if)#description BOGOTA2-PC3
```

```
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
```

```
BOGOTA2(config-if)#no shutdown
```

- Configuración de OSPF

```
BOGOTA2>enable
```

```
BOGOTA2#conf t
```

```
BOGOTA2(config)#router ospf 1    ///configuración global para habilitar OSPF en
BOGOTA2
```

```
BOGOTA2(config-router)#do show ip route connected
```

Se configuran las instrucciones network para las redes utilizando la ID de área 0

```
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
```

```
C 172.29.3.0/30 is directly connected, Serial0/1/0
```

```
C 172.29.3.4/30 is directly connected, Serial0/0/1
```

```
C 172.29.3.12/30 is directly connected, Serial0/0/0
```

```
BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0
```

```
BOGOTA2(config-router)#network 172.29.3.0 0.0.0.3 area 0
```

```
BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area 0
```

```
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0
```

```
BOGOTA2(config-router)#
```

- Desactivación de auto sumarización automática

```
BOGOTA2(config-router)#no auto-summary
```

7. Configuración de router BOGOTA3

- Configuración del nombre

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#hostname BOGOTA3
```

- Configuración general

```
BOGOTA3>enable
```

```
BOGOTA3#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
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 4
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)#
```

Configuración de las interfaces

- Interface s0/0/0

```
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#description 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-if)#exit
```

- Interface s0/1/1

```
BOGOTA3(config)#int s0/1/1
BOGOTA3(config-if)#description BOGOTA3-BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA3(config-if)#shutdown
BOGOTA3(config-if)#exit
```

- G0/0

```
BOGOTA3(config)#int g0/0
```

```
BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0
```

```
BOGOTA3(config-if)#no shutdown
```

- Configuración del protocolo OSPF

```
BOGOTA3>enable
```

```
BOGOTA3#conf t
```

```
BOGOTA3(config)#router ospf 1 //configuración global para habilitar OSPF en  
BOGOTA3
```

```
BOGOTA3(config-router)#do show ip route connected
```

```
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
```

```
C 172.29.3.8/30 is directly connected, Serial0/1/1
```

```
C 172.29.3.12/30 is directly connected, Serial0/0/0
```

Se configuran las network para las redes en BOGOTA3 utilizando la ID de área 0.

```
BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 0
```

```
BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 0
```

```
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0
```

```
BOGOTA3(config-router)#
```

- Configurar la desactivación de la sumarización automática

```
BOGOTA3(config-router)#no auto-summary
```

- 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.

- Router BOGOTA1

```
BOGOTA1>enable
BOGOTA1#conf t
BOGOTA1(config-router)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)#
```

- Router MEDELLÍN1

```
MEDELLIN1>enable
MEDELLIN1#conf t
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#
```

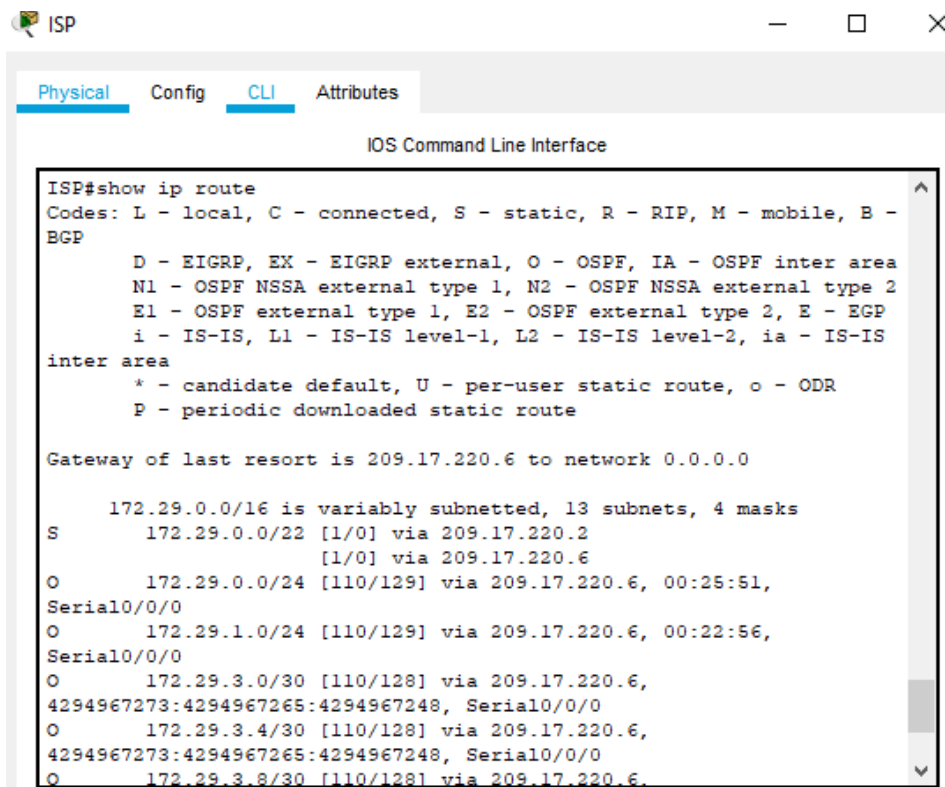
- c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se suman las subredes de cada uno a /22.

```
ISP>enable
ISP#conf t
ISP>enable
ISP#conf t
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
%Invalid next hop address (it's this router)
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.5
```

```
%Invalid next hop address (it's this router)
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#
```

2.2. PARTE 2: TABLA DE ENRUTAMIENTO.

- a) Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
- b) Verificar el balanceo de carga que presentan los routers.
- c) 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.
- d) Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
- e) Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
- f) El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.



```

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, 13 subnets, 4 masks
S       172.29.0.0/22 [1/0] via 209.17.220.2
        [1/0] via 209.17.220.6
O       172.29.0.0/24 [110/129] via 209.17.220.6, 00:25:51,
Serial0/0/0
O       172.29.1.0/24 [110/129] via 209.17.220.6, 00:22:56,
Serial0/0/0
O       172.29.3.0/30 [110/128] via 209.17.220.6,
4294967273:4294967265:4294967248, Serial0/0/0
O       172.29.3.4/30 [110/128] via 209.17.220.6,
4294967273:4294967265:4294967248, Serial0/0/0
O       172.29.3.8/30 [110/128] via 209.17.220.6,
4294967273:4294967265:4294967248, Serial0/0/0
    
```

Ilustración 23. Comando show ip route en ISP

```

MEDELLIN1
Physical Config CLI Attributes
IOS Command Line Interface
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, 15 subnets, 4 masks
O 172.29.0.0/24 [110/193] via 209.17.220.1, 00:26:51,
Serial0/1/0
O 172.29.1.0/24 [110/193] via 209.17.220.1, 00:23:56,
Serial0/1/0
O 172.29.3.0/30 [110/192] via 209.17.220.1,
4294967273:4294967266:4294967243, Serial0/1/0
O 172.29.3.4/30 [110/192] via 209.17.220.1,
4294967273:4294967266:4294967243, Serial0/1/0
O 172.29.3.8/30 [110/192] via 209.17.220.1,
4294967273:4294967266:4294967243, Serial0/1/0
O 172.29.3.12/30 [110/256] via 209.17.220.1, 00:26:31

```

Ilustración 24. Comando show ip route en MEDELLIN1

```

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

Gateway of last resort is 172.29.6.1 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O 172.29.0.0/24 [110/257] via 172.29.6.1, 00:27:35, Serial0/0/0
O 172.29.1.0/24 [110/257] via 172.29.6.1, 00:24:45, Serial0/0/0
O 172.29.3.0/30 [110/256] via 172.29.6.1, 00:29:51, Serial0/0/0
O 172.29.3.4/30 [110/256] via 172.29.6.1, 00:29:51, Serial0/0/0
O 172.29.3.8/30 [110/256] via 172.29.6.1, 00:29:51, Serial0/0/0
O 172.29.3.12/30 [110/320] via 172.29.6.1, 00:27:15,
Serial0/0/0
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 [110/129] via 172.29.6.1,

```

Ilustración 25. show ip route en MEDELLIN2

```

MEDELLIN3
Physical Config CLI Attributes
IOS Command Line Interface
MEDELLIN3>enable
MEDELLIN3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 172.29.6.13 to network 0.0.0.0

        172.29.0.0/16 is variably subnetted, 16 subnets, 4 masks
O       172.29.0.0/24 [110/257] via 172.29.6.13, 00:28:08,
Serial0/1/1
O       172.29.1.0/24 [110/257] via 172.29.6.13, 00:25:18,
Serial0/1/1
O       172.29.3.0/30 [110/256] via 172.29.6.13,
4294967273:4294967267:4294967259, Serial0/1/1
O       172.29.3.4/30 [110/256] via 172.29.6.13,
4294967273:4294967267:4294967259, Serial0/1/1
O       172.29.3.8/30 [110/256] via 172.29.6.13,
4294967273:4294967267:4294967259, Serial0/1/1

```

Ilustración 26. Comando show ip route en MEDELLIN3

```

BOGOTA 1
Physical Config CLI Attributes
IOS Command Line Interface
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 209.17.220.5 to network 0.0.0.0

        172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O       172.29.0.0/24 [110/65] via 172.29.3.2, 00:28:44, Serial0/1/0
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:25:54, Serial0/1/1
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, Serial0/0/1
L       172.29.3.5/32 is directly connected, Serial0/0/1
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 172.29.3.2, 00:25:33,
Serial0/1/0
                [110/128] via 172.29.3.10, 00:25:33,
Serial0/1/1
O       172.29.4.0/25 [110/193] via 209.17.220.5,
4294967273:4294967267:4294967294, Serial0/0/0
--More--

```

Ilustración 27. Comando show ip route en BOGOTA1

BOGOTA2

Physical Config CLI Attributes

IOS Command Line Interface

```

BGP
  D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
  E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
  i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
  * - candidate default, U - per-user static route, o - ODR
  P - periodic downloaded static route

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

  172.29.0.0/16 is variably subnetted, 16 subnets, 4 masks
C    172.29.0.0/24 is directly connected, GigabitEthernet0/0
L    172.29.0.1/32 is directly connected, GigabitEthernet0/0
O    172.29.1.0/24 [110/65] via 172.29.3.14, 00:25:51, Serial0/0/0
C    172.29.3.0/30 is directly connected, Serial0/1/0
L    172.29.3.2/32 is directly connected, Serial0/1/0
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, 00:25:51, Serial0/1/0
      [110/128] via 172.29.3.14, 00:25:51,
Serial0/0/0
C    172.29.3.12/30 is directly connected, Serial0/0/0
L    172.29.3.13/32 is directly connected, Serial0/0/0
--More--
  
```

Ilustración 28. Comando show ip route en BOGOTA2

BOGOTA 3

Physical Config CLI Attributes

IOS Command Line Interface

```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
  * - candidate default, U - per-user static route, o - ODR
  P - periodic downloaded static route

Gateway of last resort is 172.29.3.9 to network 0.0.0.0

  172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O    172.29.0.0/24 [110/65] via 172.29.3.13, 00:26:58, 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, 00:26:58, Serial0/1/1
      [110/128] via 172.29.3.13, 00:26:58,
Serial0/0/0
O    172.29.3.4/30 [110/128] via 172.29.3.9, 00:26:58, Serial0/1/1
      [110/128] via 172.29.3.13, 00:26:58,
Serial0/0/0
C    172.29.3.8/30 is directly connected, Serial0/1/1
L    172.29.3.10/32 is directly connected, Serial0/1/1
C    172.29.3.12/30 is directly connected, Serial0/0/0
L    172.29.3.14/32 is directly connected, Serial0/0/0
--More--
  
```

Ilustración 29. Comando show ip route en BOGOTA3

2.3. PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

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

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 MEDELLIN1

```
MEDELLIN1>enable
```

```
MEDELLIN1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
MEDELLIN1(config)#router ospf 1
```

```
MEDELLIN1(config-router)#passive-interface s0/0/1 //se define la interfaz pasiva
```

```
MEDELLIN1(config-router)
```

- Router MEDELLIN2

```
MEDELLIN2>enable
```

```
MEDELLIN2#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
MEDELLIN2(config)#router ospf 1
```

```
MEDELLIN2(config-router)#passive-interface g0/0 //se define la interfaz pasiva
```

- Router MEDELLIN3

```
MEDELLIN3>enable
```

```
MEDELLIN3#conf t
```

```
MEDELLIN3(config)#router ospf 1
```

```
MEDELLIN3(config-router)#passive-interface g0/0 //se define la interfaz pasiva
```

```
MEDELLIN3(config-router)#
```

- Router BOGOTA1

```
BOGOTA1>enable
```

```
BOGOTA1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BOGOTA1(config)#router ospf 1
```

```
BOGOTA1(config-router)#passive-interface s0/0/1 //se define la interfaz pasiva
```

```
BOGOTA1(config-router)#
```

```
01:04:30: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.3.13 on Serial0/0/1 from  
FULL to DOWN, Neighbor Down: Interface down or detached
```

- Router BOGOTA2:

```
BOGOTA2>enable
```

```
BOGOTA2#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BOGOTA2(config)#router ospf 1
```

```
BOGOTA2(config-router)#passive-interface g0/0 //se define la interfaz pasiva
```

```
BOGOTA2(config-router)#
```

- Router BOGOTA3

```
BOGOTA3>enable
```

```
BOGOTA3#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BOGOTA3(config)#router ospf 1
```

```
BOGOTA3(config-router)#passive-interface g0/0 //se define la interfaz pasiva
```

```
BOGOTA3(config-router)#
```

2.4. PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

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

MEDELLIN 1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

MEDELLIN1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 5 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
Serial0/0/0          2     2
Serial0/1/1          2     2
Serial0/0/1          2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance    Last Update
  172.29.6.2      120        00:00:27
  172.29.6.14    120        00:00:08
Distance: (default is 120)

--More--
    
```

Ilustración 30. Comando show ip protocols en MEDELLIN1

MEDELLIN 2

Physical Config **CLI** Attributes

IOS Command Line Interface

```

MEDELLIN2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 19 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
GigabitEthernet0/0  2     2
Serial0/1/0          2     2
Serial0/0/0          2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance    Last Update
  172.29.6.1      120        00:00:06
Distance: (default is 120)

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
--More--
    
```

Ilustración 31. Comando show ip protocols en MEDELLIN2

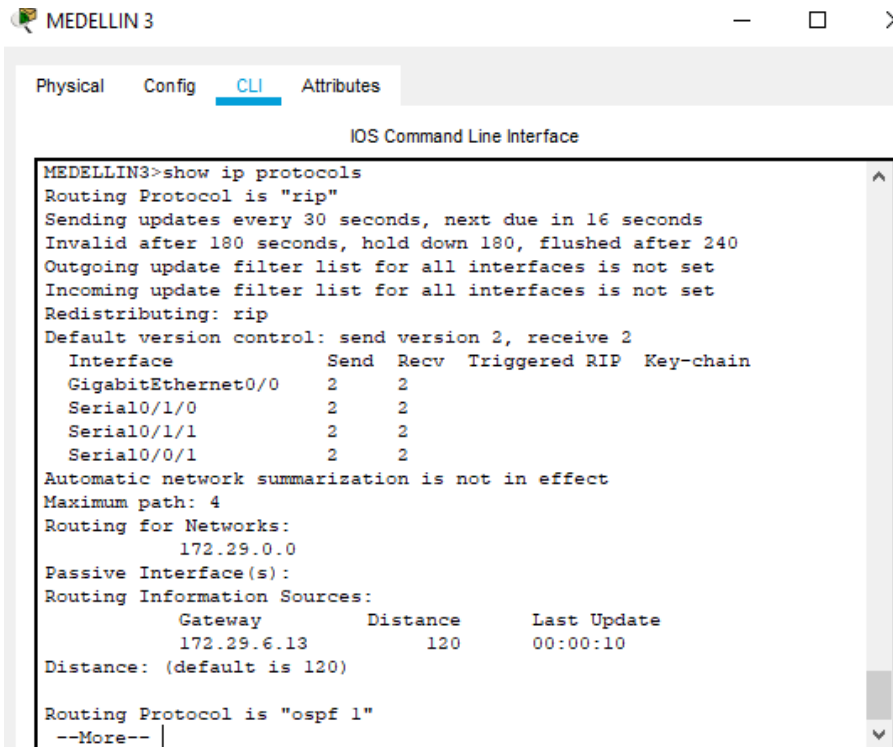


Ilustración 32. Protocolo show ip protocols en MEDELLIN3

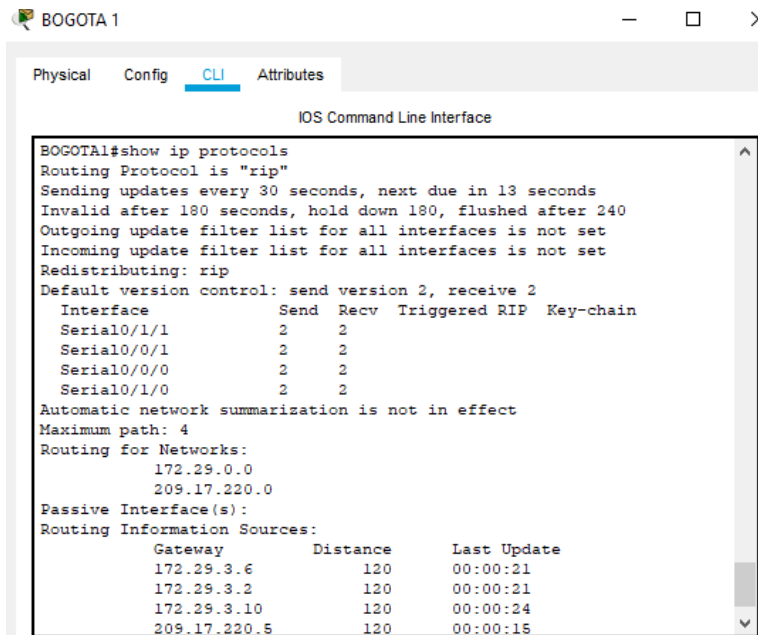


Ilustración 33. Protocolo show ip protocols en BOGOTA1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 15 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
GigabitEthernet0/0  2     2
Serial0/0/1         2     2
Serial0/1/0         2     2
Serial0/0/0         2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  172.29.3.14     120          00:00:16
  172.29.3.5      120          00:00:09
  172.29.3.1      120          00:00:09
Distance: (default is 120)

--More--

```

Ilustración 34. Protocolo show ip protocols en BOGOTA2

Physical Config **CLI** Attributes

IOS Command Line Interface

```

BOGOTA3>enable
BOGOTA3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 23 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
GigabitEthernet0/0  2     2
Serial0/1/1         2     2
Serial0/0/0         2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  172.29.3.13     120          00:00:05
  172.29.3.9      120          00:00:26
Distance: (default is 120)

--More--

```

Ilustración 35. Protocolo show ip en BOGOTA3

2.5. PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

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

```
MEDELLIN1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
MEDELLIN1(config)#int s0/1/1
```

```
MEDELLIN1(config-if)#encapsulation ppp
```

```
MEDELLIN1(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to down
```

```
04:12:24: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.14 on Serial0/1/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
MEDELLIN1(config-if)#no shutdown
```

```
MEDELLIN1(config-if)#exit
```

```
MEDELLIN1(config)#username ISP secret cisco
```

```
MEDELLIN1(config)#int s0/1/1
```

```
MEDELLIN1(config-if)#ppp authentication pap
```

```
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN password cisco
```

```
MEDELLIN1(config-if)#exit
```

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

```
BOGOTA1>enable
```

```
BOGOTA1#conf t
```

```
BOGOTA1(config)#int s0/1/0
```

```
BOGOTA1(config-if)#encapsulation ppp
```

```
BOGOTA1(config-if)#
```

```
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#exit
```

```
BOGOTA1(config)#int s0/1/0
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#exit
BOGOTA1(config)#
ISP>enable
ISP#conf t
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#username MEDELLIN secret cisco
ISP(config)#int s0/1/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#username MEDELLIN secret cisco
ISP(config)#int s0/0/0
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#exit
ISP(config)#username BOGOTA secret cisco
ISP(config)#int s0/1/0
ISP(config-if)#ppp authentication chap
ISP(config-if)#
```

2.6. PARTE 6: CONFIGURACIÓN DE PAT.

- a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers

internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

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

- Configuración NAT del router MEDELLIN1

```
MEDELLIN1>enable
```

```
MEDELLIN1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
MEDELLIN1(config)#ip access-list standard HOST
```

```
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
```

```
MEDELLIN1(config-std-nacl)#exit
```

```
MEDELLIN1(config)#ip nat inside source list HOST interface s0/1/1 overload
```

```
MEDELLIN1(config)#int s0/0/0
```

```
MEDELLIN1(config-if)#ip nat inside
```

```
MEDELLIN1(config-if)#exi
```

```
MEDELLIN1(config)#int s0/0/1
```

```
MEDELLIN1(config-if)#ip nat inside
```

```
MEDELLIN1(config-if)#exit
```

```
MEDELLIN1(config)#int s0/1/0
```

```
MEDELLIN1(config-if)#ip nat inside
```

```
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#show ip nat translation
MEDELLIN1#
```

- Configuración NAT del router BOGOTA1

```
BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list HOST interface s0/0/0 overload
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#exit
```

BOGOTA1#

BOGOTA1#show ip nat translation

BOGOTA1#

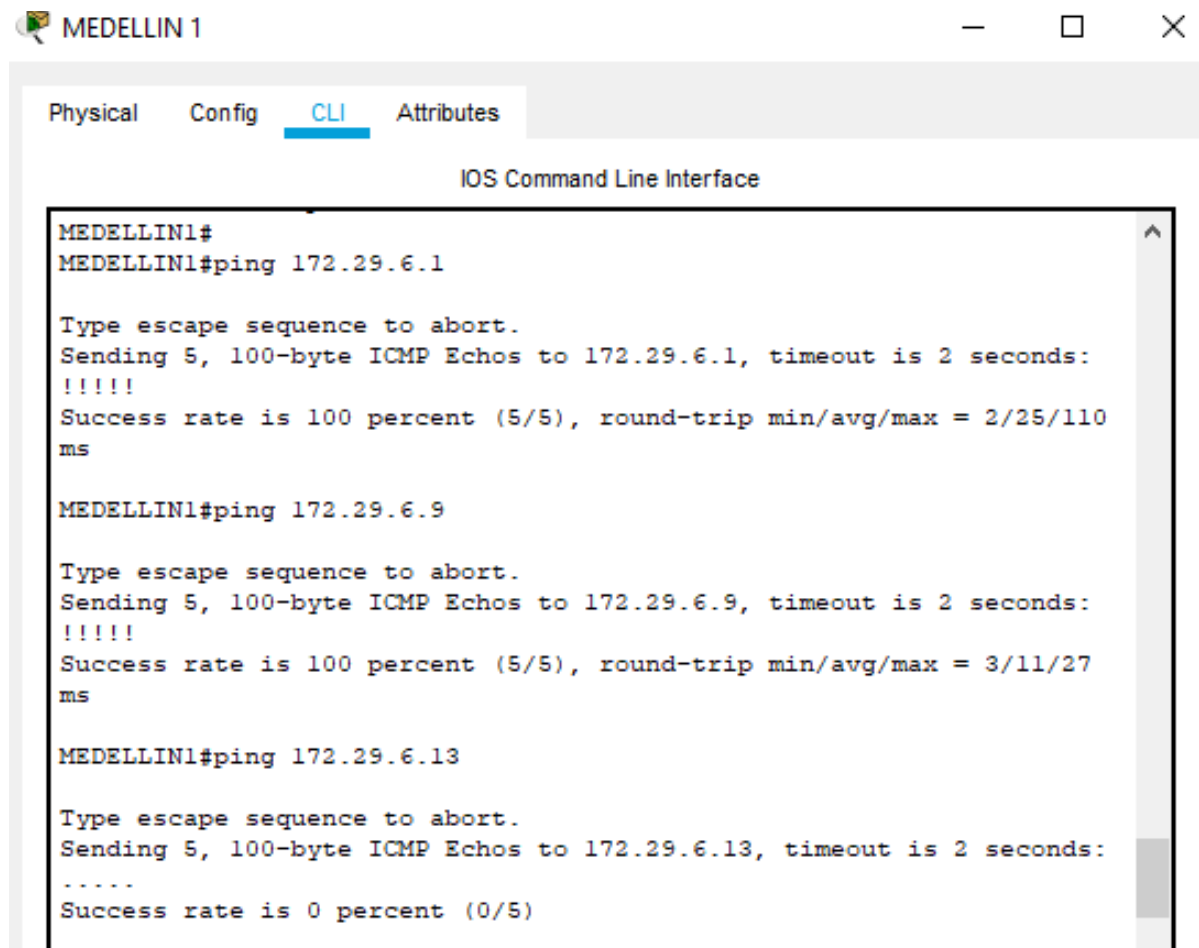
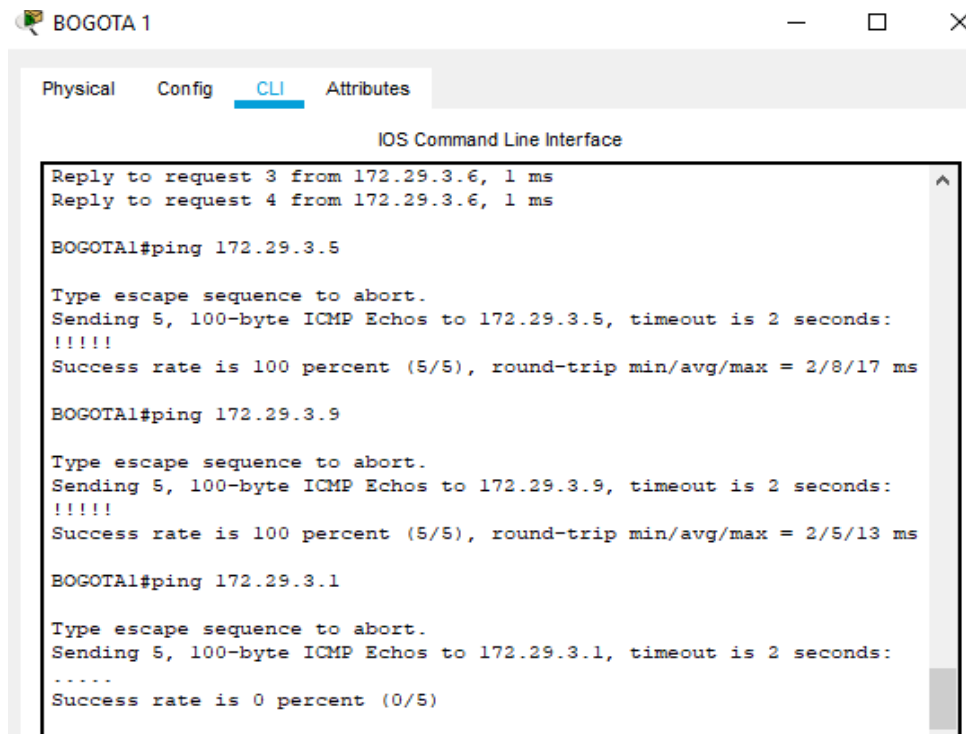


Ilustración 36. Ping MEDELLIN1 a MEDELLIN2 Y MEDELLIN3



```

BOGOTA 1
Physical Config CLI Attributes
IOS Command Line Interface
Reply to request 3 from 172.29.3.6, 1 ms
Reply to request 4 from 172.29.3.6, 1 ms
BOGOTAL#ping 172.29.3.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/17 ms
BOGOTAL#ping 172.29.3.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.9, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/13 ms
BOGOTAL#ping 172.29.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

Ilustración 37. Ping de BOGOTA1 a BOGOTA2 y BOGOTA3

2.7. PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.

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

```
MEDELLIN2>enable
```

```
MEDELLIN2#conf t
```

```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1
```

```
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
```

```
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
```

```
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
```

```
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
```

```
MEDELLIN2(dhcp-config)#exit
```

```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.29
```

```
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#
```

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

```
MEDELLIN3>enable
MEDELLIN3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#
```

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

- Configuración del router BOGOTA2

```
BOGOTA2>enable
BOGOTA2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 //se excluye la ip
```

```
BOGOTA2(config)#ip dhcp pool BOGOTA2 //se crea el pool de DHCP
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.0
BOGOTA2(config)#ip dhcp pool BOGOTA3 //se crea el pool de DHCP
BOGOTA2(dhcp-config)#ip dhcp excluded-address 172.29.1.1
BOGOTA2(config)#ip dhcp pool BOGOTA3 //se crea el pool de DHCP
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#
```

- Configuración router BOGOTA3

```
BOGOTA3>enable
BOGOTA3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13 //se configura "ip helper"
que permite ser un router de tránsito para llegar al router BOGOTA2 con el rol de
DHCP.
BOGOTA3(config-if)#exit
BOGOTA3(config)#
```

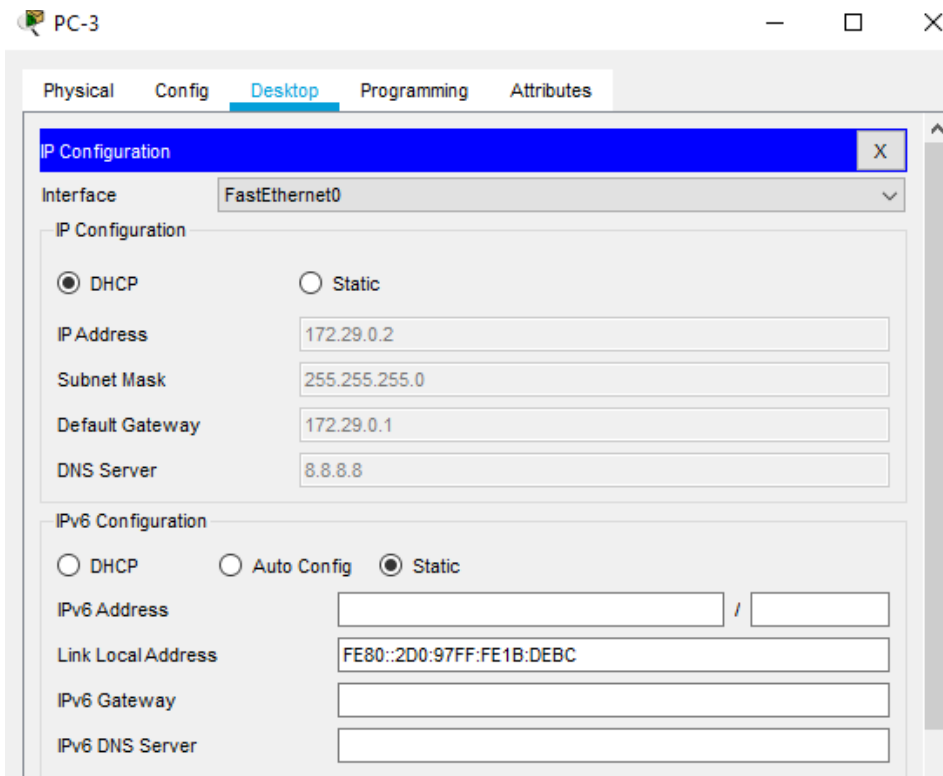


Ilustración 38. DHCP en PC-3

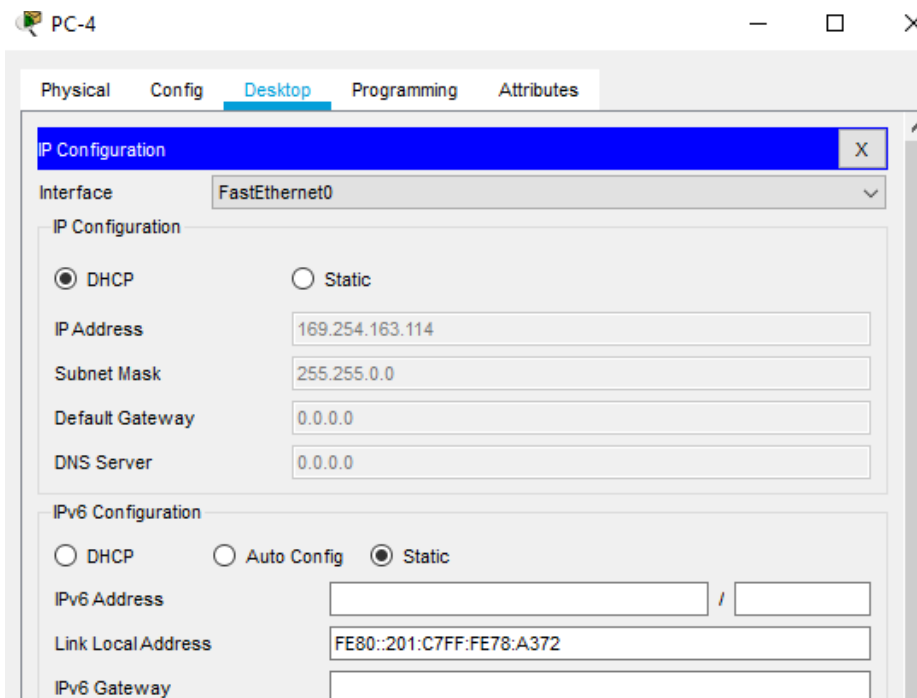


Ilustración 39. DHCP en PC-4

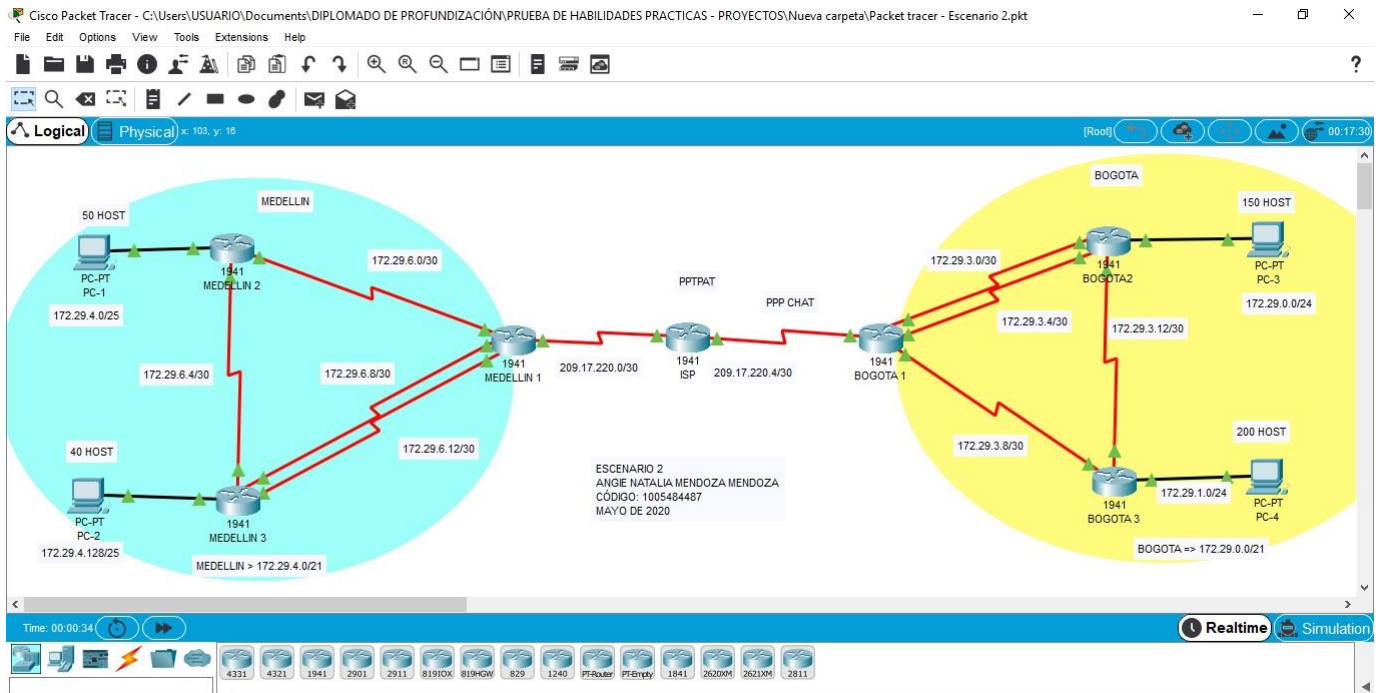


Ilustración 40. Topología configurada escenario 2

3. CONCLUSIONES

- ✚ A partir del estudio y desarrollo de cada uno de los ejercicios propuestos en las lecturas de la plataforma cisco, como en los dos escenarios propuestos en la plataforma cisco, nos muestran un panorama general y una mejor comprensión del funcionamiento de dos redes en todos sus aspectos, como también con el uso de los recursos y/o simuladores desarrollados, en este caso cisco packet tracer.
- ✚ Con el desarrollo y estudio de cada una de las actividades y temáticas de la plataforma cisco, nos muestra a través de los simuladores como es el funcionamiento de una red, la configuración de cada uno de los dispositivos utilizados, los procedimientos básicos, el direccionamiento ipv4 e ipv6 de cada uno de los host conectados, los protocolos y comunicaciones de red, enrutamiento estático y dinámico, listas de control de acceso entre otros, el cual nos da una idea a la hora de experimentar y trabajar redes ya sea a través de simuladores o ya en una red física como tal.

4. ANEXOS

Link donde se encuentran alojados el desarrollo de los dos escenarios:

<https://drive.google.com/drive/folders/1vSmln5FWM-AJzJccCRi6u5QkojApXEYt?usp=sharing>

REFERENCIAS BIBLIOGRÁFICAS

Configuración básica del router con Cisco Configuration Professional. [En línea] Disponible en: https://www.cisco.com/c/es_mx/support/docs/cloud-systems-management/configuration-professional/111999-basic-router-config-ccp-00.pdf

CISCO, Configuración inicial de un router. Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/4.1.3.4/4.1.3.4.html>

CISCO. Manejo del vlan.dat en el Switches del Cisco Catalyst que funciona con el Cisco IOS Software. [En línea]. [19 de diciembre de 2008]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-2940-series-switches/109304-manage-vlandat.html

CISCO. Configuración de Gateway de último recurso mediante comandos IP. [En línea]. [10 de agosto de 2005]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/16448-default.html

Configuración del protocolo OSPF. [En línea]. Disponible en: <https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/6-configuracion-del-encaminamiento/2-encaminamiento-dinamico/6-protocolo-ospf/6-configuracion-del-protocolo-ospf>

CISCO. Especificar una dirección IP de siguiente salto para rutas estáticas. [En línea]. [04 de junio de 2019] Disponible en: https://www.cisco.com/c/es_mx/support/docs/dial-access/floating-static-route/118263-technote-nexthop-00.html

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

https://www.cisco.com/c/es_mx/support/docs/ip/dynamic-address-allocation-resolution/19580-dhcp-multintwk.html

Rodrigo. Conexiones telnet y configuración de contraseñas. {En línea}. {03 de marzo de 2012}. Disponible en: <https://todopacketracer.com/2011/06/21/conexiones-telnet-y-configuracion-de-contrasenas/>

ROSALES, Delfi. Configuraciones Básicas de un Router o Switch Cisco. {En línea}. Disponible en: <https://delfirosales.blogspot.com/2011/02/configuraciones-basicas-de-un-router-o.html>

TEMA 2 - Inicio y configuración de un router, rutas estáticas rutas estáticas, registros de configuración. {En línea}. Disponible en:
http://informatica.uv.es/iiguia/AER/Tema2_Carga_Config.pdf