

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

FREDY ANDRES MORA GUERRERO

TUTOR:

JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI  
INGENIERÍA DE SISTEMAS  
VILLAVICENCIO, META

2020

## CONTENIDO

INTRODUCCION .....	8
OBJETIVOS.....	9
General .....	9
Específicos.....	9
ESCENARIO 1.....	10
Parte 1: Inicializar dispositivos.....	10
Paso 1: Inicializar y volver a cargar los routers y los switches.....	10
Parte 2: Configurar los parámetros básicos de los dispositivos .....	11
Paso 1: Configurar la computadora de Internet.....	11
Paso 2 Configuración Inicial R1 .....	11
Paso 3 Configuración inicial R2 .....	12
Paso 4 Configuración inicial R3 .....	14
Paso 5 Configuración inicial S1 .....	15
Paso 6 Configuración inicial S3 .....	16
Paso 7 Verificación de la conectividad de la red .....	17
Parte 3 Configurar la seguridad del switch, las VLAN y el routing entre VLAN .....	18
Paso 1 Configuración VLANS1 .....	18
Paso 2 Configuración Vlan en el S3.....	19
Paso 3: Configuración Vlan de R1 .....	20
Paso 4: Verificar la conectividad de la red .....	21
Parte 4: Configurar el protocolo de routing dinámico RIPv2.....	22
Paso 1: Configurar RIPv2 en el R1 .....	22
Paso 2: Configurar RIPv2 en el R2 .....	23
Paso 3: Configuración RIPv3 en el R3.....	24
Paso 4: Verificación de la información de RIP.....	24
Parte 5: Implementar DHCP y NAT para IPv4.....	25
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	25
Paso 2: Configurar la NAT estática y dinámica en el R2 .....	26

Paso 3: Verificar el protocolo DHCP y la NAT estática.....	27
Parte 6: Configurar NTP .....	30
Parte 7: Configurar y verificar las listas de control de acceso (ACL).....	30
Paso 1: Restringir el acceso a las líneas VTY en el R2.....	30
Paso 2: Introducir el comando de CLI .....	31
ESCENARIO 2.....	36
Paso 1 Configuración Inicial Router ISP .....	37
Paso 2 Configuración Inicial Router Medellín 1 .....	37
Paso 3 Configuración inicial Router Medellín 2 .....	38
Paso 4 Configuración inicial Router Medellín 3 .....	38
Paso 5 Configuración inicial Router Bogota 1 .....	39
Paso 6 Configuración inicial Router Bogotá 2 .....	39
Paso 7 Configuración inicial Router Bogotá 3 .....	40
Paso 8 Conexiones Físicas.....	40
Parte 1: Configuración del enrutamiento .....	41
Paso 1 Enrutamiento Router Medellin1 .....	41
Paso 2 Enrutamiento Router Medellin2.....	42
Paso 3 Enrutamiento Router Medellin3.....	43
Paso 4 Enrutamiento Router ISP .....	43
Paso 5 Enrutamiento Router Bogota1.....	44
Paso 6 Enrutamiento Router Bogota2.....	45
Paso 7 Enrutamiento Router Bogota3.....	45
Paso 8 Configuración OSPF Router Medellin1 .....	46
Paso 9 Configuración OSPF Router Medellin2 .....	46
Paso 10 Configuración OSPF Router Medellin3 .....	47
Paso 11 Configuración OSPF Router Bogota1 .....	48
Paso 12 Configuración OSPF Router Bogota2 .....	48
Paso 13 Configuración OSPF Router Bogota3 .....	49
Paso 14 Configuración OSPF Router ISP .....	49
Paso 15 Configuración OSPF Router Medellin1 .....	50

Paso 16 Configuración OSPF Router Bogota1 .....	50
Paso 17 Configuración Ruta Estática Router ISP .....	50
Parte 2: Tabla de Enrutamiento.....	50
Parte 3: Deshabilitar la propagación del protocolo OSPF.....	57
Paso 1 Deshabilitar Interfaz Router Bogota1 .....	58
Paso 2 Deshabilitar Interfaz Router Bogota2 .....	58
Paso 3 Deshabilitar Interfaz Router Bogota3 .....	58
Paso 4 Deshabilitar Interfaz Router Medellin1 .....	58
Paso 5 Deshabilitar Interfaz Router Medellin2 .....	58
Paso 6 Deshabilitar Interfaz Router Medellin3 .....	59
Parte 4: Verificación del protocolo OSPF.....	59
Paso 7 Autenticación Chat Router Medellin1 .....	65
Paso 8 Autenticación Chat Router Bogota1 .....	66
Paso 9 Autenticación Chat Router ISP .....	66
Parte 5: Configuración de PAT.....	67
Parte 6: Configuración del servicio DHCP .....	70
Comando Guardar .....	74
CONCLUSIONES .....	76
BIBLIOGRAFIA.....	77

## LISTA DE FIGURAS

Figura 1. Diseño de la topología escenario 1 .....	10
Figura 2 ping desde R1 a R2.....	17
Figura 3. ping desde R2 a R3.....	17
Imagen 4. ping desde PC a Gateway. ....	18
Figura 5. ping desde S1 a R1 Vlan 99.....	21
Figura 6. ping desde S3 a R1 Vlan 99.....	22
Figura 7. ping desde S1 a R1 Vlan 21 .....	22
Figura 8. ping desde S3 a R1 Vlan 23.....	22
Figura 9. Verificación protocolos. ....	25
Figura 10. Verificación Rip .....	25
Figura 11. Verificación secciones rip .....	25
Figura 12. Verificación DHCP PC-A .....	28
Figura 13. Verificación DHCP PC-C. ....	28
Figura 14. ping desde PC-A hasta PC-C.....	29
Figura 15. probar acceso al servidor web.....	29
Figura 16. Verificación de NTP.....	30
Figura 17. Prueba de conexión telnet de R1 y R2. ....	31
Figura 18. Solucion Escenario 1.....	35
Figura 19. Imagen Escenario 2.....	36
Figura 20. Verificación route en Medellin1 .....	51
Figura 21 verificación route Medellin2 .....	52
Figura 22. Verificación route Medellin3 .....	53
Figura 23. Verificación route ISP.....	54
Figura 24. Verificación route Bogota1 .....	55

Figura 25. Verificación route Bogota2 .....	56
Figura 26. Verificación route Bogota2 .....	57
Figura 27. Verificación protocolos Medellin1 .....	59
Figura 28. Verificación protocolos Medellin2 .....	60
Figura 29. Verificación protocolos Medellin3 .....	61
Figura 30. Verificación protocolos ISP .....	62
Figura 31. Verificación protocolos Bogota1 .....	63
Figura 32. Verificación protocolos Bogota2 .....	64
Figura 33. Verificación protocolos Bogota3 .....	65
Figura 34. Ping Desde Medellin1 a Medellin2 y Medellin3 .....	69
Figura 35. Ping desde Bogota1 a Bogota2 y Bogota3 .....	69
Figura 36. Verificación Dhcp PC-A .....	71
Figura 37. Verificación Dhcp PC-B .....	71
Figura 38 Verificación Dhcp PC-C .....	73
Figura 39. Verificación Dhcp PC-D .....	73
Figura 40. Estructura Escenario 2 .....	75

## LISTA DE TABLAS

Tabla 1. Direccionamiento IPV4 e IPV6 .....	10
Tabla 2. Topologías de red.....	41
Tabla 3. Interfaces a deshabilitar.....	58

## INTRODUCCION

Durante el desarrollo de este trabajo realizaremos la aplicación de los conocimientos adquiridos a lo largo del curso para configurar los diferentes dispositivos de red y equipo de cómputo para hacer posible sus respectivas interconexiones y transferencia de datos. Realizaremos el respectivo diseño para cada uno de los casos propuestos, con sus equipos de cómputo, router, switches y tendido del cableado adecuado para cada una de las conexiones. Ejecutaremos comandos pertinentes para configurar protocolos ipv4 e ipv6 para cada uno de los equipos, emitiremos comando para comprobar las configuraciones y así analizar el funcionamiento. Realizaremos la configuración y habilitación de protocolo DHCP en los router para que asignen automáticamente dirección ip a los equipos de cómputo instalados en la red.

## OBJETIVOS

### General

1. Poner en práctica las codificaciones vistas a lo largo del curso para hacer posibles la interconexión entre diferentes dispositivos de red para simular redes Lan, Wan.

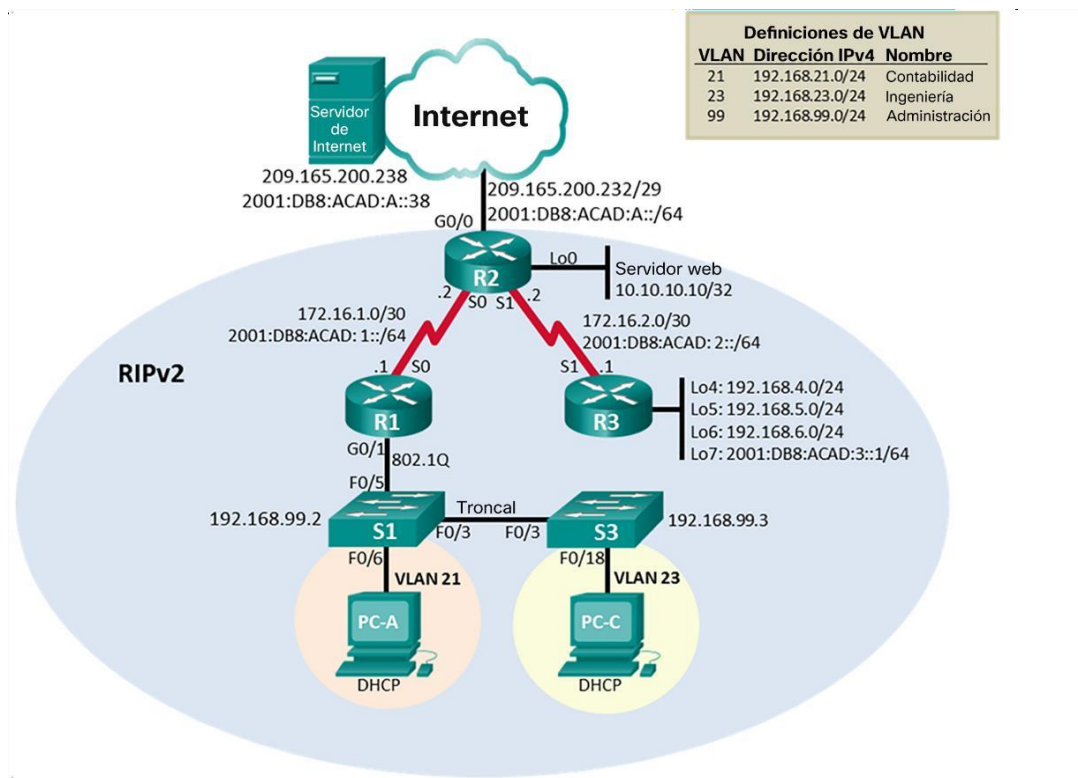
### Específicos

1. Diseñar la estructura física de la topología propuesta empleando router, switches, servidores y computadores para crear redes de tipo LAN y WAN.
2. Configurar los parámetros básicos para los equipos, tanto de configuración como de seguridad para poder garantizar el correcto funcionamiento de estos. Por medio de estas configuraciones estaremos restringiendo el acceso a las configuraciones de los equipos.
3. Simular la interconexión entre los diferentes equipos de red y terminales por medio de comando ping y de navegador para probar el acceso a los servidores. Verificar las rutas y las traducciones que tiene la red por medio de los dispositivos.

## ESCENARIO 1

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

Figura 1. Diseño de la topología escenario 1



Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

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

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

✓ Eliminar el archivo startup-config de todos los routers

```
Router#erase startup-config
```

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

*Router#erase startup-config*

*Router#delete vlan.dat*

- ✓ Volver a cargar ambos switches

*Router#Reload*

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

*Router#dir flash*

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 1. Direccionamiento IPv4 e IPv6

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

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2 Configuración Inicial R1

Las tareas de configuración para R1 incluyen las siguientes:

- ✓ Desactivar la búsqueda DNS  
*Router(config)#no ip domain-lookup*
- ✓ Nombre del router R1  
*Router(config)#hostname R1*
- ✓ Contraseña de exec privilegiado cifrada class  
*R1(config)#enable secret class*
- ✓ Contraseña de acceso a la consola cisco

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
```

- ✓ Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
```

- ✓ Mensaje MOTD

```
R1(config)#banner motd $Se prohíbe el acceso no autorizado!$
```

- ✓ Interfaz S0/0/0: 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)#int s0/0/0
R1(config-if)#description Conecta con R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
```

- ✓ Rutas predeterminadas

Configurar una ruta IPv4 predeterminada de S0/0/0

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

Nota: Todavía no configure G0/1.

Paso 3 Configuración inicial R2

La configuración del R2 incluye las siguientes tareas:

- ✓ Desactivar la búsqueda DNS

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

- ✓ Nombre del router R2

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

✓ Contraseña de exec privilegiado cifrada *class*  
*R2(config)#enable secret class*

✓ Contraseña de acceso a la consola cisco  
*R2(config)#line console 0*  
*R2(config-line)#password cisco*  
*R2(config-line)#login*

✓ Contraseña de acceso Telnet  
Cisco  
*R2(config)#line vty 0 4*  
*R2(config-line)#password cisco*  
*R2(config-line)#login*

✓ Cifrar las contraseñas de texto no cifrado  
*R2(config)#service password-encryption*

✓ Mensaje MOTD  
*R2(config)#banner motd \$Se prohíbe el acceso no autorizado!\$*

✓ Interfaz S0/0/0: Establezca la descripción

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

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

Establecer la frecuencia de reloj en 128000

Activar la interfaz

*R2(config)#int s0/0/0*

*R2(config-if)#description Conecta con R1*

*R2(config-if)#ip address 172.16.1.2 255.255.255.252*

*R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64*

*R2(config-if)#clock rate 128000*

*R2(config-if)#no shutdown*

- ✓ Rutas predeterminadas: Configurar una ruta IPv4 predeterminada de S0/0/0  
*R1(config)#ip route 0.0.0.0 0.0.0.0 g0/0*  
 Configurar una ruta IPv6 predeterminada de S0/0/0  
*R1(config)#ipv6 route ::/0 g0/0*

#### Paso 4 Configuración inicial R3

La configuración del R3 incluye las siguientes tareas:

- ✓ Desactivar la búsqueda DNS  
*Router(config)#no ip domain-lookup*
- ✓ Nombre del router R3  
*Router(config)#hostname R3*
- ✓ Contraseña de exec privilegiado cifrada *class*  
*R3(config)#enable secret class*
- ✓ Contraseña de acceso a la consola cisco  
*R3(config)#line console 0*  
*R3(config-line)#password cisco*  
*R3(config-line)#login*
- ✓ Contraseña de acceso Telnet cisco  
*R3(config)#line vty 0 4*  
*R3(config-line)#password cisco*  
*R3(config-line)#login*
- ✓ Cifrar las contraseñas de texto no cifrado  
*R3(config)#service password-encryption*
- ✓ Mensaje MOTD  
*R3(config)#banner motd \$Se prohíbe el acceso no autorizado!\$*
- ✓ Interfaz S0/0/1: 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)#int s0/0/1
R3(config-if)#description Conecta con R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no shutdown
```

- ✓ Interfaz loopback 4: Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config-if)#int lo4
R3(config-if)#ip address 172.16.4.1 255.255.255.0
R3(config-if)#no shutdown
```

- ✓ Interfaz loopback 5: Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config-if)#int lo5
R3(config-if)#ip address 172.16.5.1 255.255.255.0
R3(config-if)#no shutdown
```

- ✓ Interfaz loopback 6: Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config-if)#int lo6
R3(config-if)#ip address 172.16.6.1 255.255.255.0
R3(config-if)#no shutdown
```

- ✓ Interfaz loopback 7: Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

```
R3(config-if)#int lo7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#no shutdown
```

#### Paso 5 Configuración inicial S1

La configuración del S1 incluye las siguientes tareas:

- ✓ Desactivar la búsqueda DNS  

```
Switch(config)#no ip domain-lookup
```
- ✓ Nombre del Switch S1  

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

- ✓ Contraseña de exec privilegiado cifrada class  
*S1(config)#enable secret class*
- ✓ Contraseña de acceso a la consola cisco  
*S1(config)#line console 0*  
*S1(config-line)#password cisco*  
*S1(config-line)#login*
- ✓ Contraseña de acceso Telnet cisco  
*S1(config)#line vty 0 4*  
*S1(config-line)#password cisco*  
*S1(config-line)#login*
- ✓ Cifrar las contraseñas de texto no cifrado  
*S1(config)#service password-encryption*
- ✓ Mensaje MOTD  
*S1(config)#banner motd \$Se prohíbe el acceso no autorizado!\$*

### Paso 6 Configuración inicial S3

La configuración del S3 incluye las siguientes tareas:

- ✓ Desactivar la búsqueda DNS  
*Switch(config)#no ip domain-lookup*
- ✓ Nombre del router  
*Switch(config)#hostname S3*
- ✓ Contraseña de exec privilegiado cifrada class  
*S3(config)#enable secret class*
- ✓ Contraseña de acceso a la consola cisco  
*S3(config)#line console 0*  
*S3(config-line)#password cisco*  
*S3(config-line)#login*
- ✓ Contraseña de acceso Telnet  
*S3(config)#line vty 0 4*  
*S3(config-line)#password cisco*

*S3(config-line)#login*

- ✓ Cifrar las contraseñas de texto no cifrado

*S3(config)#service password-encryption*

- ✓ Mensaje MOTD

*S3(config)#banner motd \$Se prohíbe el acceso no autorizado!\$*

Paso 7 Verificación de 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:

Figura 2 ping desde R1 a R2

```
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 = 1/3/7 ms

R1#
```

Figura 3. ping desde R2 a R3

```
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 = 1/2/7 ms
```

Imagen 4. ping desde PC a Gateway

```
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=1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

### Parte 3 Configurar la seguridad del switch, las VLAN y el routing entre VLAN

#### Paso 1 Configuración VLANS1

La configuración del S1 incluye las siguientes tareas:

- ✓ Crear la base de datos de VLAN: Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.  
*S1(config)#vlan 21*  
*S1(config-vlan)#name contabilidad*  
*S1(config-vlan)#vlan 23*  
*S1(config-vlan)#name Ingenieria*  
*S1(config-vlan)#vlan 99*  
*S1(config-vlan)#name 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)#vlan 99*  
*S1(config-vlan)#ip address 192.168.99.2 255.255.255.0*  
*S1(config-vlan)#no shutdown*
- ✓ Asignar el gateway predeterminado: Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.  
*S1(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  
*S1(config)#int fa0/3*  
*S1(config)#switchport mode trunk*  
*S1(config)#switchport trunk native vlan 1*
  
- ✓ Forzar el enlace troncal en la interfaz F0/5: Utilizar la red VLAN 1 como VLAN nativa  
*S1(config)#int fa0/5*  
*S1(config)#switchport mode trunk*  
*S1(config)#switchport trunk native vlan 1*
  
- ✓ Configurar el resto de los puertos como puertos de acceso: Utilizar el comando interface range  
*S1(config)#int range fa0/1-2, fa0/4, fa0/6-24, g0/1-2*  
*S1(config-if-range)#switchport mode access*
  
- ✓ Asignar F0/6 a la VLAN 21  
*S1(config)#int fa0/6*  
*S1(config-int)#switchport mode access*  
*S1(config-int)#switchport access vlan 21*
  
- ✓ Apagar todos los puertos sin usar  
*S1(config)#int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2*  
*S1(config-if-range)#shutdown*

## Paso 2 Configuración Vlan en el S3

La configuración del S3 incluye las siguientes tareas:

- ✓ Crear la base de datos de VLAN: Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.  
*S3(config)#vlan 21*  
*S3(config-vlan)#name contabilidad*  
*S3(config-vlan)#vlan 23*  
*S3(config-vlan)#name Ingenieria*  
*S3(config-vlan)#vlan 99*  
*S3(config-vlan)#name 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 99*  
*S3(config-vlan)#ip address 192.168.99.3 255.255.255.0*

*S3(config-vlan)#no shutdown*

- ✓ Asignar el gateway predeterminado: Asignar la primera dirección IP en la subred como gateway predeterminado.

*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)#int fa0/3*

*S3(config)#switchport mode trunk*

*S3(config)#switchport trunk native vlan 1*

- ✓ Configurar el resto de los puertos como puertos de acceso: Utilizar el comando `interface range`

*S3(config)#int range fa0/1-2, fa0/4, fa0/6-24, g0/1-2*

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

- ✓ Asignar F0/18 a la VLAN 23

*S3(config-if-range)#int fa0/18*

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

- ✓ Apagar todos los puertos sin usar

*S3(config-if)#int range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2*

*S3(config-if-range)#shutdown*

### Paso 3: Configuración Vlan de 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(config)#int g0/1.21*

*R1(config-subif)#description VLAN 21 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 23 Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
```

- ✓ 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 99 Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
```

- ✓ Activar la interfaz G0/1  

```
R1(config)#int g0/1
R1(config-if)#no shutdown
```

Paso 4: Verificar la conectividad de la red

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

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

Figura 5. ping desde S1 a R1 Vlan 99

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#
```

Figura 6. ping desde S3 a R1 Vlan 99

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms
```

Figura 7. ping desde S1 a R1 Vlan 21

```
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 = 0/0/3 ms
```

Figura 8. ping desde S3 a R1 Vlan 23

```
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
```

#### Parte 4: Configurar el protocolo de routing dinámico RIPv2

##### Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

- ✓ Configurar RIP versión 2  
*R1(config)#router rip*  
*R1(config-router)#version 2*
  
- ✓ Anunciar las redes conectadas directamente: Asigne todas las redes conectadas directamente.  
*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

```
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
```

## Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

- ✓ Configurar RIP versión 2

```
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
C 10.10.10.0/24 is directly connected, GigabitEthernet0/1
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
```

- ✓ Establecer la interfaz LAN (loopback) como pasiva

```
R2(config-router)#passive-interface lo0
```

- ✓ Desactive la sumarización automática.

```
R1(config-router)#no auto-summary
```

### Paso 3: Configuración RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

- ✓ Configurar 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
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
```

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

```
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#passive-interface s0/0/1
```

- ✓ Desactive la sumarización automática.

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

### Paso 4: Verificación de 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?

```
R3#show ip protocols
```

Figura 9. Verificación protocolos

```
R3#show ip protocols
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
  Serial0/0/1        2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.16.0.0
  192.168.4.0
  192.168.5.0
  192.168.6.0
Passive Interface(s):
  Loopback4
  Loopback5
  Loopback6
Routing Information Sources:
  Gateway            Distance      Last Update
  172.16.2.2         120          00:00:04
Distance: (default is 120)
```

Figura 10. Verificación 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, 00:00:11, 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, 00:00:11, 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, 00:00:11, Serial0/0/1
R   192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:11, Serial0/0/1
R   192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:11, Serial0/0/1
```

Figura 11. Verificación secciones rip

```
R3#show run | section router rip
router rip
  version 2
  passive-interface Loopback4
  passive-interface Loopback5
  passive-interface Loopback6
  network 172.16.0.0
  network 192.168.4.0
  network 192.168.5.0
  network 192.168.6.0
  no auto-summary
```

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: 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*
- ✓ Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas  
*R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20*
- ✓ Crear un pool de DHCP para la VLAN 21:  
Nombre: ACCT  
Servidor DNS: 10.10.10.10  
Nombre de dominio: ccna-sa.com  
Establecer el gateway predeterminado  
*R1(config)#ip dhcp pool AACT*  
*R1(dhcp-config)#network 192.168.21.0 255.255.255.0*  
*R1(dhcp-config)#dns-server 10.10.10.10*  
*R1(dhcp-config)#domain-name ccna-sa.com*  
*R1(dhcp-config)#default-router 192.168.21.1*
- ✓ Crear un pool de DHCP para la VLAN 21  
Nombre: ENGR  
Servidor DNS: 10.10.10.10  
Nombre de dominio: ccna-sa.com  
Establecer el gateway predeterminado  
*R1(config)#ip dhcp pool ENGR*  
*R1(dhcp-config)#network 192.168.23.0 255.255.255.0*  
*R1(dhcp-config)#dns-server 10.10.10.10*  
*R1(dhcp-config)#domain-name ccna-sa.com*  
*R1(dhcp-config)#default-router 192.168.23.1*

Paso 2: 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(config)#user webuser privilege 15 secret cisco12345*
- ✓ Habilitar el servicio del servidor HTTP  
*R2(config)#ip http server*  
^

*% Invalid input detected at '^' marker.  
"Comando no soportado"*

- ✓ Configurar el servidor HTTP para utilizar la base de datos local para la autenticación  
*R2(config)#ip http authentication local ^  
% Invalid input detected at '^' marker.  
"Comando no soportado"*
  
- ✓ Crear una NAT estática al servidor web: Dirección global interna: 209.165.200.229  
*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  
*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*  
Permitir la traducción de un resumen de las redes LAN (loopback) en el R3  
*R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255*
  
- ✓ Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET  
El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236  
*R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248*
  
- ✓ Definir la traducción de NAT dinámica  
*R2(config)#ip nat inside source list 1 pool INTERNET*

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Figura 12. Verificación DHCP PC-A

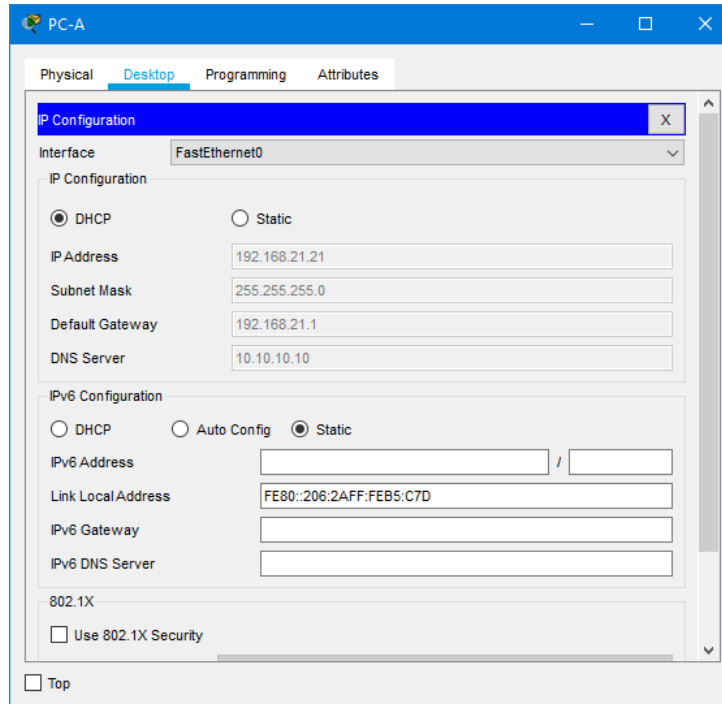
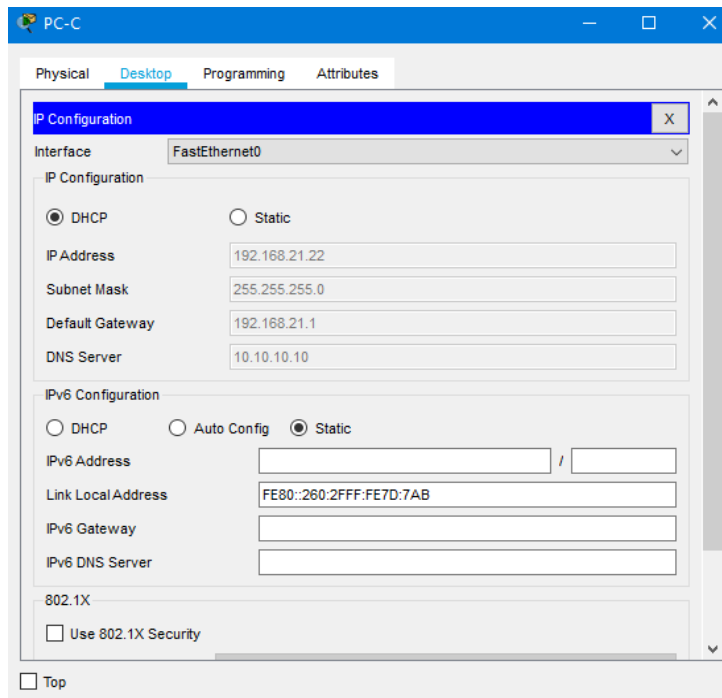
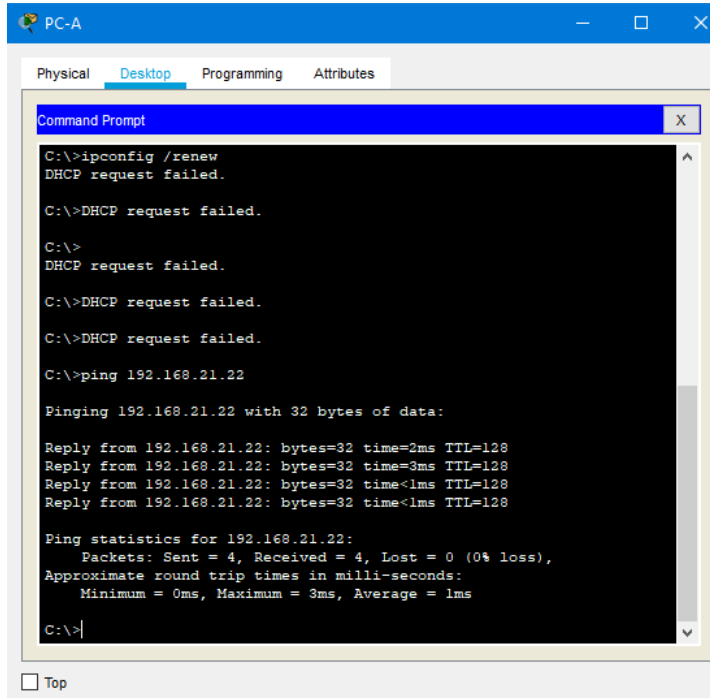


Figura 13. Verificación DHCP PC-C



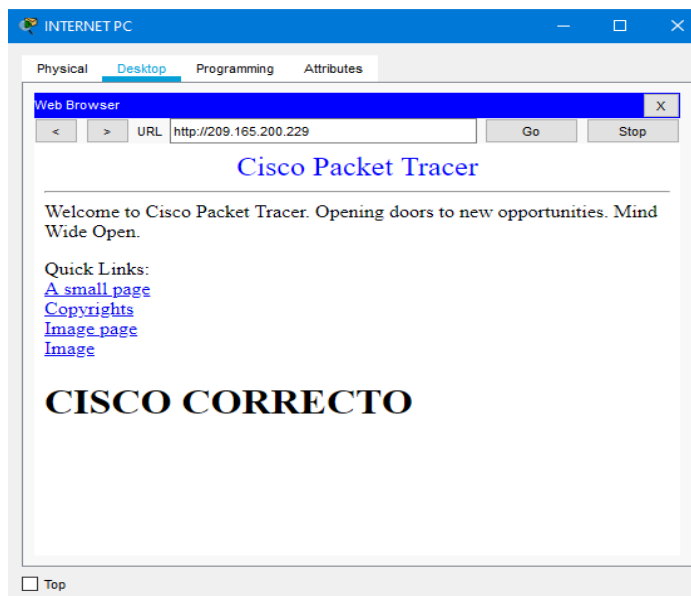
- ✓ Verificar que la PC-A pueda hacer ping a la PC-C  
Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 14. ping desde PC-A hasta PC-C



Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Figura 15. probar acceso al servidor web



## Parte 6: Configurar NTP

- ✓ Ajuste la fecha y hora en R2. "5 de marzo de 2016, 9 a. m."  
*R2#clock set 09:00:00 5 mar 2019*
  
- ✓ Configure R2 como un maestro NTP: Nivel de estrato: 5  
*R2(config)#ntp master 5*
  
- ✓ Configurar R1 como un cliente NTP: Servidor: R2  
*R1(config)# ntp server 10.10.10.1*
  
- ✓ Configure R1 para actualizaciones de calendario periódicas con hora NTP.  
*R1(config)# ntp update-calendar*
  
- ✓ Verifique la configuración de NTP en R1.  
*R1#show ntp associations*

Figura 16. Verificación de NTP

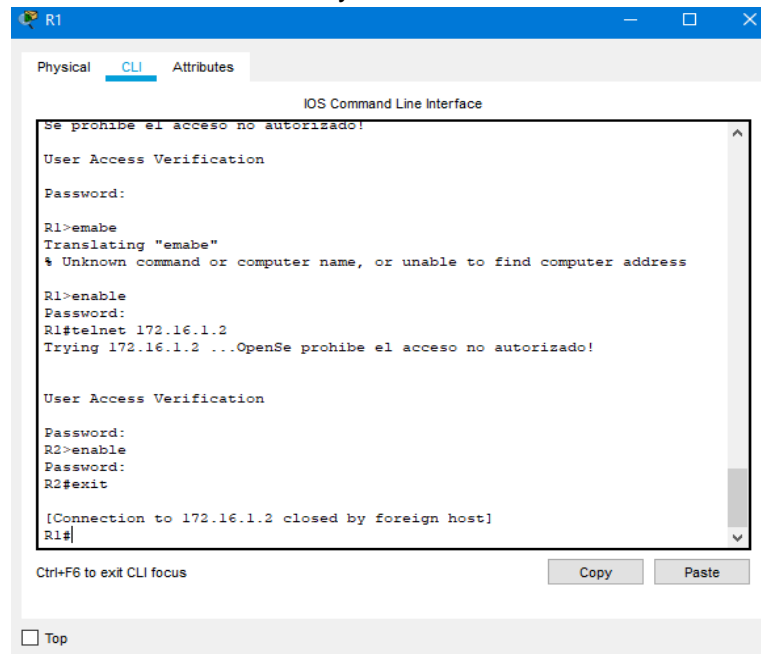
```
R1#show ntp associations
address      ref clock      st  when    poll  reach  delay      offset      disp
~10.10.10.1  .INIT.         16  -       64    0      0.00       0.00       0.48
~127.127.1.1 .LOCL.         4   46      64    377    0.00       0.00       0.48
~172.16.1.2  127.127.1.1   5   62      64    377    4.00       30237001.00  0.48
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

## Parte 7: Configurar y verificar las listas de control de acceso (ACL)

### Paso 1: 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*
  
- ✓ 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-std-nacl)#permit host 172.16.1.1*
  
- ✓ Verificar que la ACL funcione como se espera

Figura 17. Prueba de conexión telnet de R1 y R2



Paso 2: Introducir el comando de CLI

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
```

```
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))
```

- ✓ Restablecer los contadores de una lista de acceso

```
R2#clear access-list counters
```

```
R2#clear ip access-list counters
```

```
^
```

```
% Invalid input detected at '^' marker.
```

Comando no compatible con Packet Tracer

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

```
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*

*IP output packet accounting is disabled*

*IP access violation accounting is disabled*

*TCP/IP header compression is disabled*

*RTP/IP header compression is disabled*

*Probe proxy name replies are disabled*

*Policy routing is disabled*

*Network address translation is disabled*

*BGP Policy Mapping is disabled*

*Input features: MCI Check*

*WCCP Redirect outbound is disabled*

*WCCP Redirect inbound is disabled*

*WCCP Redirect exclude is disabled*

*GigabitEthernet0/1 is up, line protocol is up (connected)*

*Internet address is 10.10.10.1/24*

*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*  
*IP output packet accounting is disabled*  
*IP access violation accounting is disabled*  
*TCP/IP header compression is disabled*  
*RTP/IP header compression is disabled*  
*Probe proxy name replies are disabled*  
*Policy routing is disabled*  
*Network address translation is disabled*  
*BGP Policy Mapping is disabled*  
*Input features: MCI Check*  
*WCCP Redirect outbound is disabled*  
*WCCP Redirect inbound is disabled*  
*WCCP Redirect exclude is disabled*  
*Serial0/0/0 is up, line protocol is up (connected)*  
*Internet address is 172.16.1.2/30*  
*Broadcast address is 255.255.255.255*  
*Address determined by setup command*  
*MTU is 1500*  
*Helper address is not set*  
*Directed broadcast forwarding is disabled*  
*Outgoing access list is not set*  
*Inbound access list is not set*  
*Proxy ARP is enabled*  
*Security level is default*  
*Split horizon is enabled*

*ICMP redirects are always sent*  
*ICMP 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*  
*IP output packet accounting is disabled*  
*IP access violation accounting is disabled*  
*TCP/IP header compression is disabled*  
*RTP/IP header compression is disabled*  
*Probe proxy name replies are disabled*  
*Policy routing is disabled*  
*Network address translation is disabled*  
*WCCP Redirect outbound is disabled*  
*WCCP Redirect exclude is disabled*  
*BGP Policy Mapping is disabled*  
*Serial0/0/1 is up, line protocol is up (connected)*  
*Internet address is 172.16.2.1/30*  
*Broadcast address is 255.255.255.255*  
*Address determined by setup command*  
*MTU is 1500*  
*Helper address is not set*  
*Directed broadcast forwarding is disabled*  
*Outgoing access list is not set*  
*Inbound access list is not set*  
*Proxy ARP is enabled*  
*Security level is default*  
*Split horizon is enabled*  
*ICMP redirects are always sent*  
*ICMP 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*  
*IP output packet accounting is disabled*  
*IP access violation accounting is disabled*  
*TCP/IP header compression is disabled*  
*RTP/IP header compression is disabled*  
*Probe proxy name replies are disabled*  
*Policy routing is disabled*  
*Network address translation is disabled*  
*WCCP Redirect outbound is disabled*  
*WCCP Redirect exclude is disabled*  
*BGP Policy Mapping is disabled*  
*Vlan1 is administratively down, line protocol is down*  
*Internet protocol processing disabled*

✓ ¿Con qué comando se muestran las traducciones NAT?

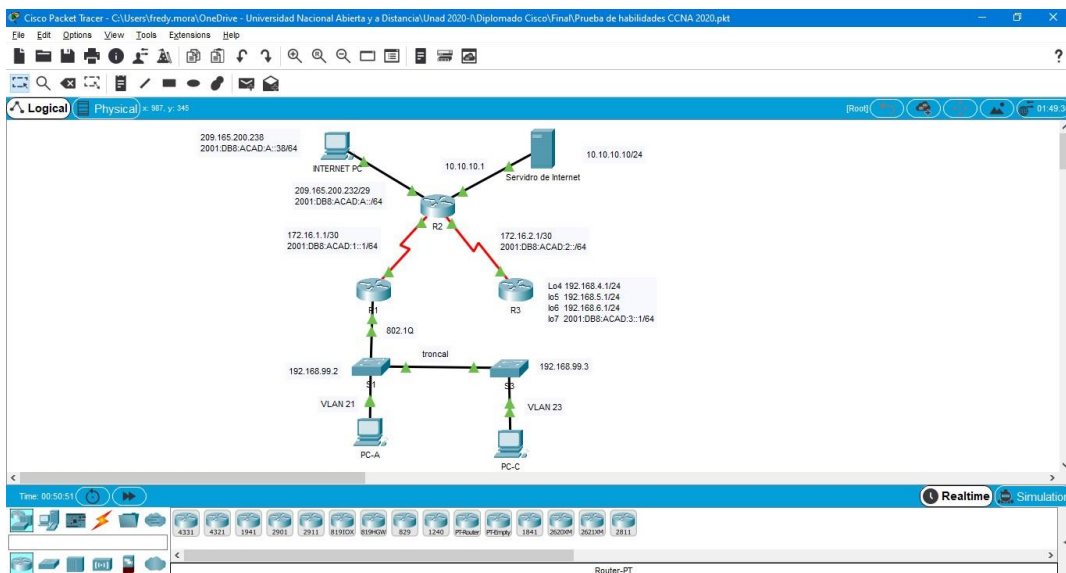
Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet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

R2#show ip nat translations

Pro Inside global Inside local Outside local Outside global

```
--- 209.165.200.229 10.10.10.10 --- ---
```

Figura 18. Solucion Escenario 1

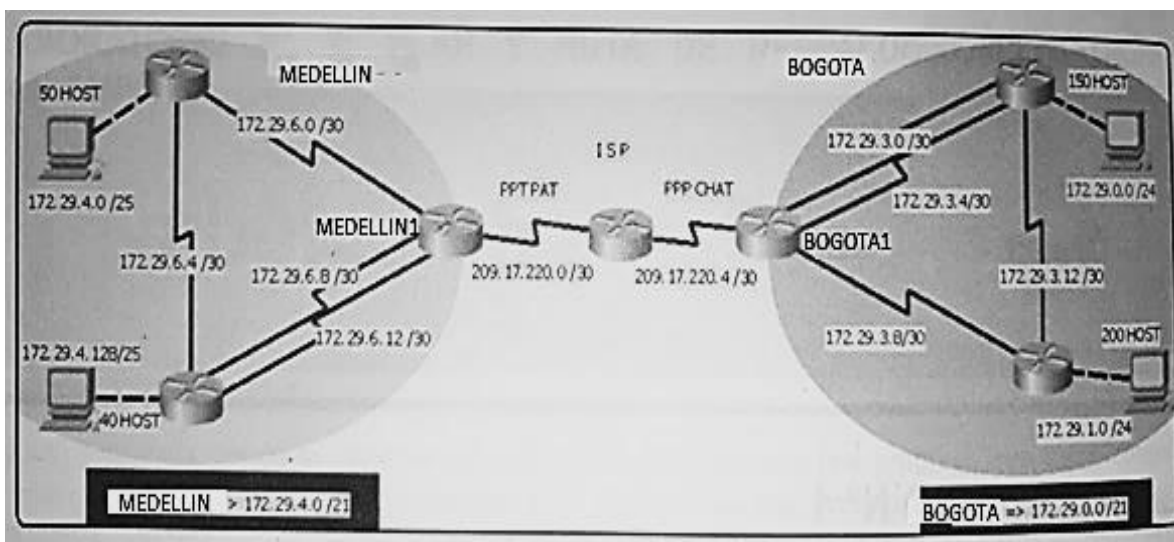


## ESCENARIO 2

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

Figura 19. Imagen 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.

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).

## Paso 1 Configuración Inicial Router ISP

```
Router>enable
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#service password-encryption
ISP(config)#banner motd $Se prohíbe el acceso no autorizado$
ISP(config)#
```

## Paso 2 Configuración Inicial Router Medellín 1

```
Router>enable
Router#configure terminal
Router(config)#hostname Medellin1
Medellin1(config)#enable secret class
Medellin1(config)#line console 0
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#line vty 0 15
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#service password-encryption
```

*Medellin1(config)#banner motd \$Se prohíbe el acceso no autorizado\$*

### Paso 3 Configuración inicial Router Medellín 2

*Router>enable*

*Router#configure terminal*

*Router(config)#hostname Medellín2*

*Medellin2(config)#enable secret class*

*Medellin2(config)#line console 0*

*Medellin2(config-line)#password cisco*

*Medellin2(config-line)#login*

*Medellin2(config-line)#line vty 0 15*

*Medellin2(config-line)#password cisco*

*Medellin2(config-line)#login*

*Medellin2(config-line)#service password-encryption*

*Medellin2(config)#banner motd \$Se prohíbe el acceso no autorizado\$*

*Medellin2(config)#*

### Paso 4 Configuración inicial Router Medellín 3

*Router>enable*

*Router#configure terminal*

*Router(config)#hostname Medellín3*

*Medellin3(config)#enable secret class*

*Medellin3(config)#line console 0*

*Medellin3(config-line)#password cisco*

*Medellin3(config-line)#login*

*Medellin3(config-line)#line vty 0 15*

*Medellin3(config-line)#password cisco*

*Medellin3(config-line)#login*

*Medellin3(config-line)#service password-encryption*

*Medellin3(config)#banner motd \$Se prohíbe el acceso no autorizado\$*

## Paso 5 Configuración inicial Router Bogota 1

*Router>enable*

*Router#configure terminal*

*Router(config)#hostname Bogota1*

*Bogota1(config)#enable secret class*

*Bogota1(config)#line console 0*

*Bogota1(config-line)#password cisco*

*Bogota1(config-line)#login*

*Bogota1(config-line)#line vty 0*

*Bogota1(config-line)#line vty 0 15*

*Bogota1(config-line)#password cisco*

*Bogota1(config-line)#login*

*Bogota1(config-line)#service password-encryption*

*Bogota1(config)#banner motd \$Se prohíbe el acceso no autorizado\$*

## Paso 6 Configuración inicial Router Bogotá 2

*Router>enable*

*Router#configure terminal*

*Router(config)#hostname Bogota2*

*Bogota2(config)#enable secret class*

*Bogota2(config)#line console 0*

*Bogota2(config-line)#password cisco*

*Bogota2(config-line)#login*

*Bogota2(config-line)#line vty 0*

*Bogota2(config-line)#line vty 0 15*

```
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#service password-encryption
Bogota2(config)#banner motd $Se prohíbe el acceso no autorizado$
```

## Paso 7 Configuración inicial Router Bogotá 3

```
Router>enable
Router#configure terminal
Router(config)#hostname Bogota3
Bogota3(config)#enable secret class
Bogota3(config)#line console 0
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#line vty 0
Bogota3(config-line)#line vty 0 15
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#service password-encryption
Bogota3(config)#banner motd $Se prohíbe el acceso no autorizado$
```

## Paso 8 Conexiones Físicas

Realizar la conexión física de los equipos con base en la topología de red  
Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Tabla 2. Topologías de red

Dispositivo	Interfaz	Dirección Ip	Mascara de subred
MEDELLIN1	S0/0/1	172.29.6.1	255.255.255.252
	S0/1/0	172.29.6.9	255.255.255.252
	S0/1/1	172.29.6.13	255.255.255.252
	S0/0/0	209.17.220.1	255.255.255.252
MEDELLIN2	S0/0/1	172.29.6.2	255.255.255.252
	S0/0/0	172.29.6.5	255.255.255.252
	G0/0	172.29.4.1	255.255.255.128
MEDELLIN3	S0/0/0	172.29.6.6	255.255.255.252
	S0/1/0	172.29.6.10	255.255.255.252
	S0/1/1	172.29.6.14	255.255.255.252
	G0/0	172.29.4.129	255.255.255.128
ISP	S0/0/0	209.17.220.2	255.255.255.252
	S0/0/1	209.17.220.5	255.255.255.252
Bogota1	S0/0/1	172.29.3.8	255.255.255.252
	S0/0/0	172.29.3.0	255.255.255.252
	S0/1/1	172.29.3.4	255.255.255.252
	S0/1/0	172.29.3.8	255.255.255.252
Bogota2	S0/0/0	172.29.3.2	255.255.255.242
	S0/1/1	172.29.3.6	255.255.255.242
	S0/0/1	172.29.3.13	255.255.255.242
	G0/0	172.29.0.1	255.255.255.0
Bogota3	S0/1/0	172.29.3.10	255.255.255.252
	S0/0/1	172.29.3.14	255.255.255.252
	G0/0	172.29.1.1	255.255.255.0

## Parte 1: Configuración del enrutamiento

### Paso 1 Enrutamiento Router Medellin1

```
Medellin1(config)#int s0/0/1
```

```
Medellin1(config-if)#description Conexion con Medellin2
```

```
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
```

```
Medellin1(config-if)#clock rate 128000
```

```
Medellin1(config-if)#no shutdown
```

```
Medellin1(config)#int s0/1/0
```

```
Medellin1(config-if)#description Conexion con Medellin3
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config)#int s0/1/1
Medellin1(config-if)#description Conexion con Medellin3
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config)#int s0/0/0
Medellin1(config-if)#description Conexion con ISP
Medellin1(config-if)#ip address 209.17.220.1 255.255.255.252
```

## Paso 2 Enrutamiento Router Medellin2

```
Medellin2(config)#int s0/0/0
Medellin2(config-if)#description Connection to Medellin3
Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config)#int s0/0/1
Medellin2(config-if)#description Connection to Medellin1
Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config)#int g0/0
Medellin2(config)#description Conexion con PC-A
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)# no shutdown
```

### Paso 3 Enrutamiento Router Medellin3

```
Medellin3(config)#int s0/0/0
Medellin3(config-if)# description Conexion con Medellin2
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
Medellin3(config)#int s0/1/0
Medellin3(config-if)#description Conexion con Medellin1
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
Medellin3(config)#int s0/1/1
Medellin3(config-if)#description Conexion con Medellin1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
Medellin3(config)#int g0/0
Medellin3(config-if)#description Conexión con PC-B
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
```

### Paso 4 Enrutamiento Router ISP

```
ISP(config)#int s0/0/0
ISP(config-if)#description Conexion con Medellin1
ISP(config-if)#ip address 209.17.220.2 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
```

```
ISP(config)#int s0/0/1
ISP(config-if)#description Conexion con Bogota1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
```

## Paso 5 Enrutamiento Router Bogota1

```
Bogota1(config)#int s0/0/1
Bogota1(config-if)#description Conexion con 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)#int s0/0/0
Bogota1(config-if)#description Conexion con Bogota2
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)#int s0/1/1
Bogota1(config-if)#description Conexion con Bogota2
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)#int s0/1/0
Bogota1(config-if)#description Conexion con 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
```

## Paso 6 Enrutamiento Router Bogota2

```
Bogota2(config)#int s0/0/0
Bogota2(config-if)#description Conecta con Bogota1
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)#int s0/1/1
Bogota2(config-if)#description Conexion con Bogota1
Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config)#int s0/0/1
Bogota2(config-if)#description Conexion con 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)#int g0/0
Bogota2(config-if)#description Conexion con el PC-C
Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota2(config-if)#no shutdown
```

## Paso 7 Enrutamiento Router Bogota3

```
Bogota3(config)#int s0/1/0
Bogota3(config-if)#description Conexion con Bogota1
Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shutdown
```

```
Bogota3(config)#int s0/0/1
Bogota3(config-if)#description Conexion con 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)#int g0/0
Bogota3(config-if)#description Conexion con PC-D
Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota3(config-if)#no shutdown
```

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

#### Paso 8 Configuración OSPF Router Medellin1

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#router-id 1.1.1.1
Medellin1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/0/0
Medellin1(config-router)#network 172.129.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.129.6.8 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
```

#### Paso 9 Configuración OSPF Router Medellin2

```
Medellin2(config)#router ospf 1
Medellin2(config-router)#router-id 2.2.2.2
```

```
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, Serial0/0/1
C 172.29.6.4/30 is directly connected, Serial0/0/0
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)# network 172.29.6.4 0.0.0.127 area 0
Medellin2(config-router)#
00:50:39: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/0 from LOADING to FULL,
Loading Done
```

#### Paso 10 Configuración OSPF Router Medellin3

```
Medellin3(config)#router ospf 1
Medellin3(config-router)#router 3.3.3.3
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, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
02:03:19: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL,
Loading Done
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)#
02:03:41: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1/0 from LOADING to FULL,
Loading Done
```

*Medellin3(config-router)#*

*02:03:49: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1/1 from LOADING to FULL, Loading Done*

## Paso 11 Configuración OSPF Router Bogota1

*Bogota1(config)#router ospf 1*

*Bogota1(config-router)#router 4.4.4.4*

*Bogota1(config-router)#do show ip route connected*

*C 172.29.3.0/30 is directly connected, Serial0/0/0*

*C 172.29.3.4/30 is directly connected, Serial0/1/1*

*C 172.29.3.8/30 is directly connected, Serial0/1/0*

*C 209.17.220.4/30 is directly connected, Serial0/0/1*

*Bogota1(config-router)#network 172.29.3.0 0.0.0.3 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*

## Paso 12 Configuración OSPF Router Bogota2

*Bogota2(config)#router ospf 1*

*Bogota2(config-router)#router-id 5.5.5.5*

*Bogota2(config-router)#do show ip route connected*

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

*C 172.29.3.0/30 is directly connected, Serial0/0/0*

*C 172.29.3.4/30 is directly connected, Serial0/1/1*

*C 172.29.3.12/30 is directly connected, Serial0/0/1*

*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)#*

00:06:00: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING to FULL, Loading Done

Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0

### Paso 13 Configuración OSPF Router Bogota3

Bogota3(config)#router ospf 1

Bogota3(config-router)#router-id 6.6.6.6

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, Serial0/1/0

C 172.29.3.12/30 is directly connected, Serial0/0/1

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)#

00:18:50: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/1/0 from LOADING to FULL, Loading Done

Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0

Bogota3(config-router)#

00:19:11: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL, Loading Done

### Paso 14 Configuración OSPF Router ISP

ISP(config)#router ospf 1

ISP(config-router)#router-id 7.7.7.7

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

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

C 209.17.220.4/30 is directly connected, Serial0/0/1

ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0

ISP(config-router)#

07:22:11: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

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

07:22:11: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/1 from LOADING to FULL, Loading Done

- b. Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

## Paso 15 Configuración OSPF Router Medellin1

```
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2
```

```
Medellin1(config)#router ospf 1
```

```
Medellin1(config-router)#default-information originate
```

## Paso 16 Configuración OSPF Router Bogota1

```
Bogota1(config)#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
```

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

## Paso 17 Configuración Ruta Estática Router ISP

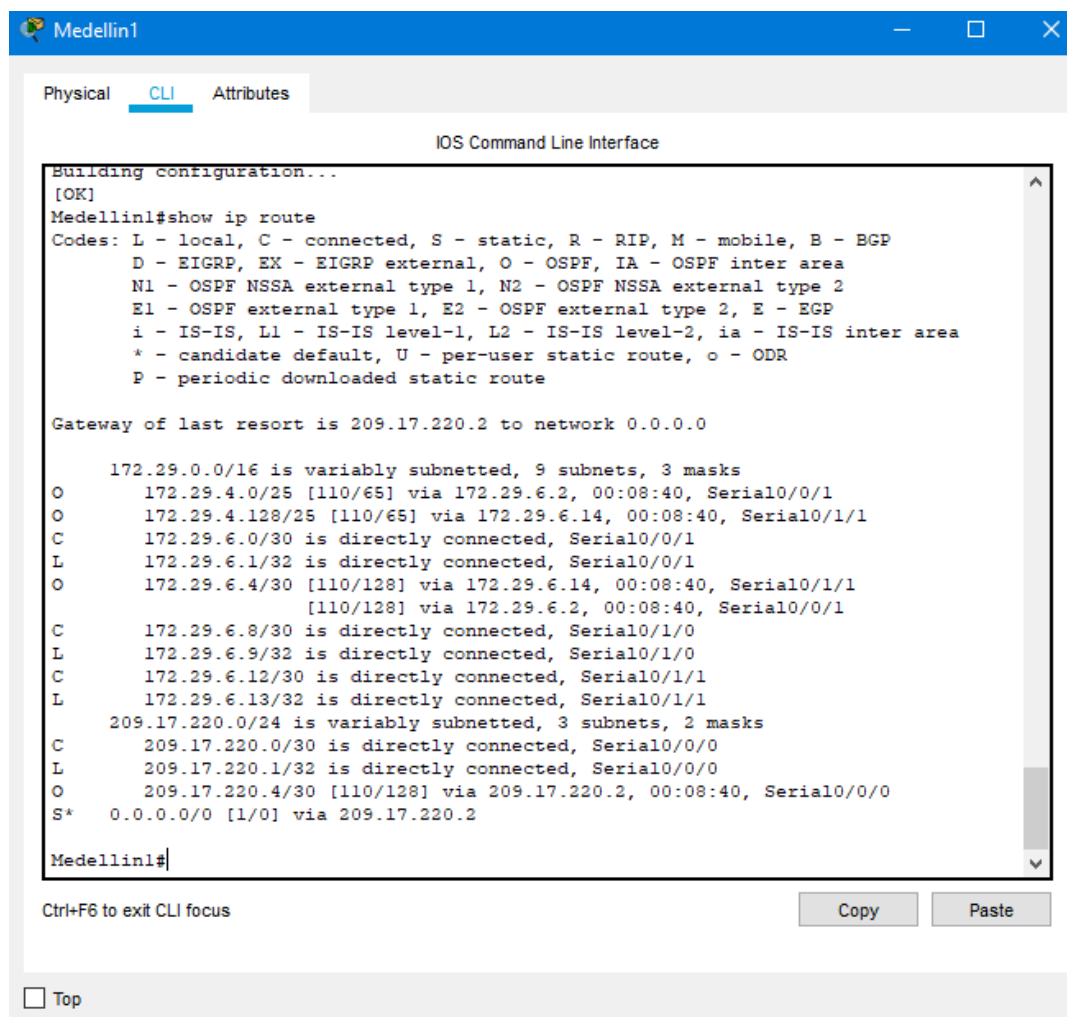
```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
```

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

## 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.

Figura 20. Verificación route en Medellin1



The screenshot shows a window titled 'Medellin1' with three tabs: 'Physical', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The text in the window is as follows:

```
Building configuration...
[OK]
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 209.17.220.2 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O     172.29.4.0/25 [110/65] via 172.29.6.2, 00:08:40, Serial0/0/1
O     172.29.4.128/25 [110/65] via 172.29.6.14, 00:08:40, Serial0/1/1
C     172.29.6.0/30 is directly connected, Serial0/0/1
L     172.29.6.1/32 is directly connected, Serial0/0/1
O     172.29.6.4/30 [110/128] via 172.29.6.14, 00:08:40, Serial0/1/1
      [110/128] via 172.29.6.2, 00:08:40, Serial0/0/1
C     172.29.6.8/30 is directly connected, Serial0/1/0
L     172.29.6.9/32 is directly connected, Serial0/1/0
C     172.29.6.12/30 is directly connected, Serial0/1/1
L     172.29.6.13/32 is directly connected, Serial0/1/1
O     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C     209.17.220.0/30 is directly connected, Serial0/0/0
L     209.17.220.1/32 is directly connected, Serial0/0/0
O     209.17.220.4/30 [110/128] via 209.17.220.2, 00:08:40, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.2

Medellin1#
```

At the bottom of the window, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons: 'Copy' and 'Paste'. A 'Top' button is also visible at the bottom left of the window frame.

Figura 21 verificación route Medellín2

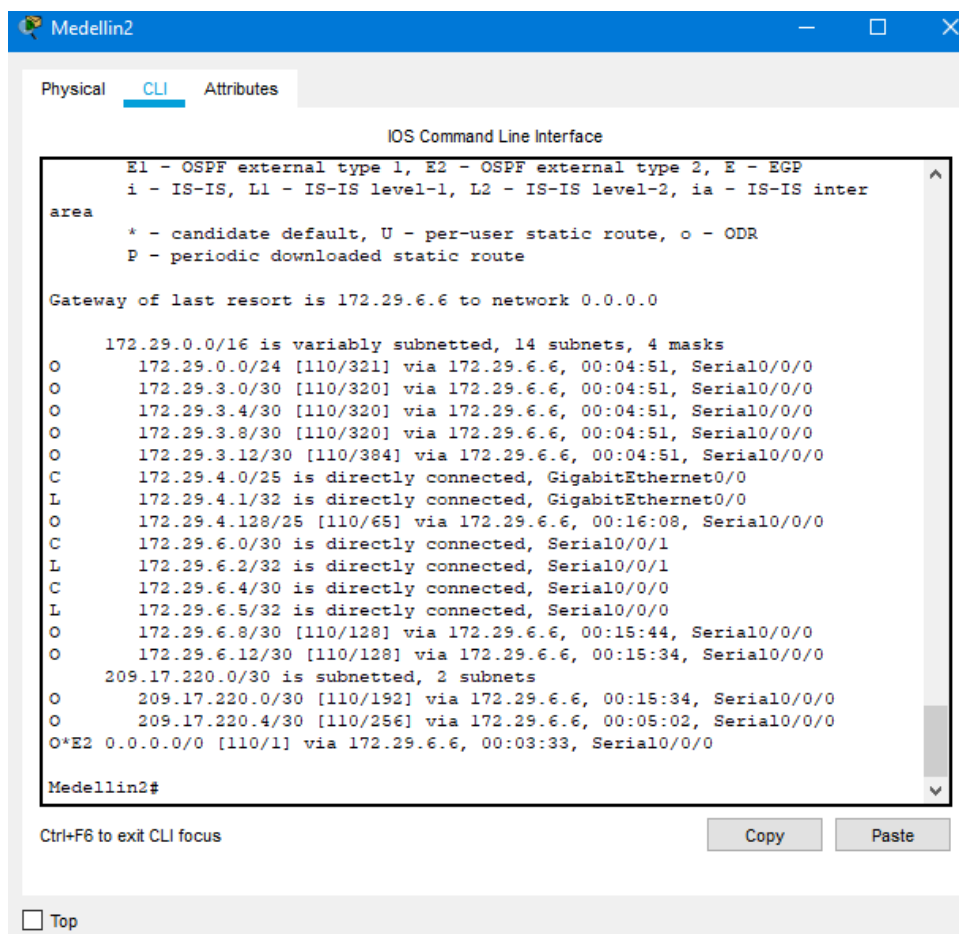


Figura 22. Verificación route Medellin3

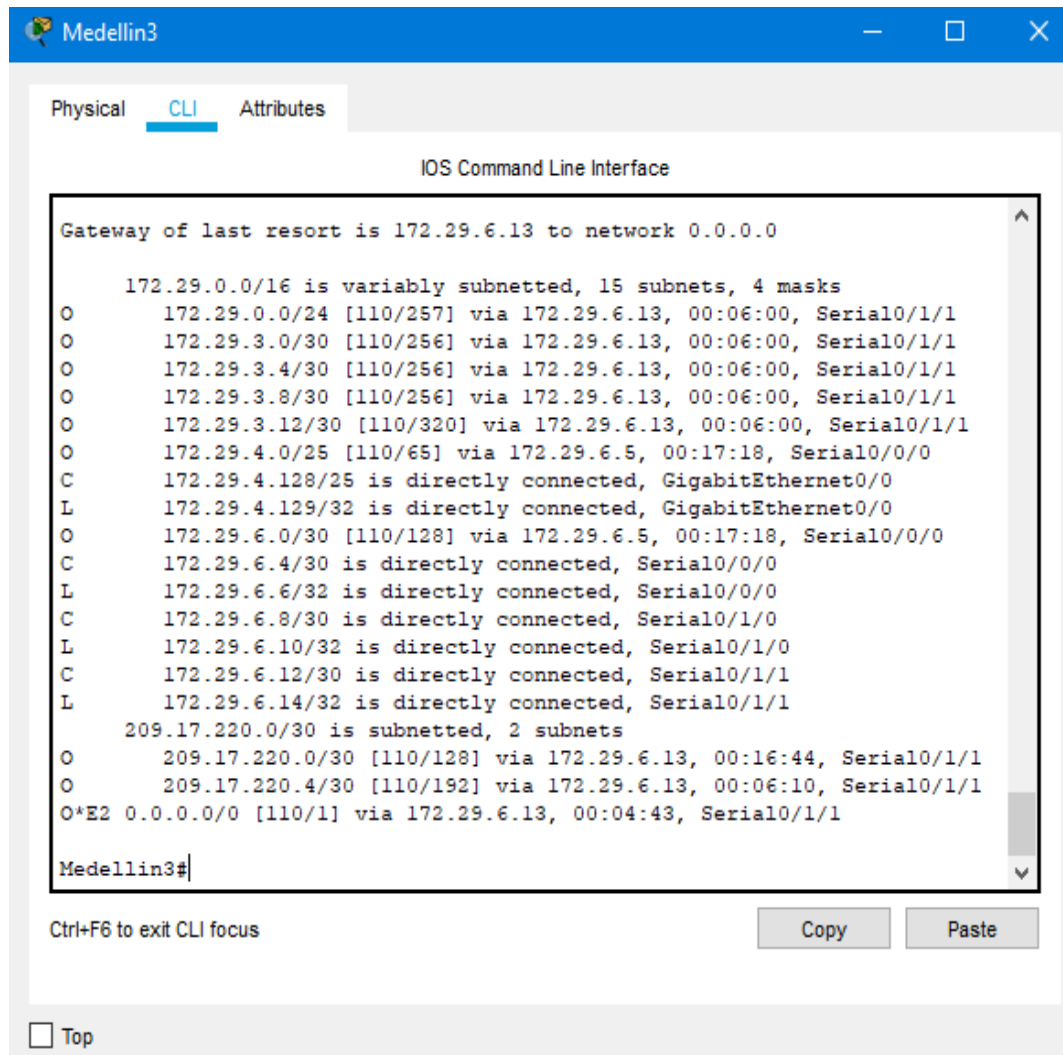


Figura 23. Verificación route ISP

```
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 209.17.220.1 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 209.17.220.6
O       172.29.0.0/24 [110/129] via 209.17.220.6, 00:07:07, Serial0/0/1
O       172.29.3.0/30 [110/128] via 209.17.220.6, 00:07:07, Serial0/0/1
O       172.29.3.4/30 [110/128] via 209.17.220.6, 00:07:07, Serial0/0/1
O       172.29.3.8/30 [110/128] via 209.17.220.6, 00:07:07, Serial0/0/1
O       172.29.3.12/30 [110/192] via 209.17.220.6, 00:07:07, Serial0/0/1
S       172.29.4.0/22 [1/0] via 209.17.220.1
O       172.29.4.0/25 [110/193] via 209.17.220.1, 00:07:17, Serial0/0/0
O       172.29.4.128/25 [110/129] via 209.17.220.1, 00:07:17, Serial0/0/0
O       172.29.6.0/30 [110/256] via 209.17.220.1, 00:07:17, Serial0/0/0
O       172.29.6.4/30 [110/192] via 209.17.220.1, 00:07:17, Serial0/0/0
O       172.29.6.8/30 [110/192] via 209.17.220.1, 00:07:17, Serial0/0/0
O       172.29.6.12/30 [110/128] via 209.17.220.1, 00:07:17, Serial0/0/0
    209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.2/32 is directly connected, Serial0/0/0
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.5/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 209.17.220.1, 00:06:40, Serial0/0/0
       [110/1] via 209.17.220.6, 00:04:41, Serial0/0/1
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 24. Verificación route Bogota1

```
Bogota1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.5 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 14 subnets, 4 masks
O       172.29.0.0/24 [110/65] via 172.29.3.2, 00:11:22, Serial0/0/0
C       172.29.3.0/30 is directly connected, Serial0/0/0
L       172.29.3.1/32 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/1/0
L       172.29.3.9/32 is directly connected, Serial0/1/0
O       172.29.3.12/30 [110/128] via 172.29.3.2, 00:11:22, Serial0/0/0
O       172.29.4.0/25 [110/257] via 209.17.220.5, 00:08:02, Serial0/0/1
O       172.29.4.128/25 [110/193] via 209.17.220.5, 00:08:02, Serial0/0/1
O       172.29.6.0/30 [110/320] via 209.17.220.5, 00:08:02, Serial0/0/1
O       172.29.6.4/30 [110/256] via 209.17.220.5, 00:08:02, Serial0/0/1
O       172.29.6.8/30 [110/256] via 209.17.220.5, 00:08:02, Serial0/0/1
O       172.29.6.12/30 [110/192] via 209.17.220.5, 00:08:02, Serial0/0/1
O       209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
O       209.17.220.0/30 [110/128] via 209.17.220.5, 00:08:02, Serial0/0/1
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.6/32 is directly connected, Serial0/0/1
S*     0.0.0.0/0 [1/0] via 209.17.220.5
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 25. Verificación route Bogota2

```
Bogota2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

 172.29.0.0/16 is variably subnetted, 15 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
C    172.29.3.0/30 is directly connected, Serial0/0/0
L    172.29.3.2/32 is directly connected, Serial0/0/0
C    172.29.3.4/30 is directly connected, Serial0/1/1
L    172.29.3.6/32 is directly connected, Serial0/1/1
O    172.29.3.8/30 [110/128] via 172.29.3.1, 00:12:30, Serial0/0/0
C    172.29.3.12/30 is directly connected, Serial0/0/1
L    172.29.3.13/32 is directly connected, Serial0/0/1
O    172.29.4.0/25 [110/321] via 172.29.3.1, 00:08:57, Serial0/0/0
O    172.29.4.128/25 [110/257] via 172.29.3.1, 00:08:57, Serial0/0/0
O    172.29.6.0/30 [110/384] via 172.29.3.1, 00:08:57, Serial0/0/0
O    172.29.6.4/30 [110/320] via 172.29.3.1, 00:08:57, Serial0/0/0
O    172.29.6.8/30 [110/320] via 172.29.3.1, 00:08:57, Serial0/0/0
O    172.29.6.12/30 [110/256] via 172.29.3.1, 00:08:57, Serial0/0/0
 209.17.220.0/30 is subnetted, 2 subnets
O    209.17.220.0/30 [110/192] via 172.29.3.1, 00:08:57, Serial0/0/0
O    209.17.220.4/30 [110/128] via 172.29.3.1, 00:12:30, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:07:44, Serial0/0/0
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 26. Verificación route Bogota3

```

Bogota3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.3.9 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, 00:02:19, Serial0/0/1
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, 00:02:19, Serial0/1/0
    [110/128] via 172.29.3.13, 00:02:19, Serial0/0/1
O   172.29.3.4/30 [110/128] via 172.29.3.9, 00:02:19, Serial0/1/0
C   172.29.3.8/30 is directly connected, Serial0/1/0
L   172.29.3.10/32 is directly connected, Serial0/1/0
C   172.29.3.12/30 is directly connected, Serial0/0/1
L   172.29.3.14/32 is directly connected, Serial0/0/1
O   172.29.4.0/25 [110/321] via 172.29.3.9, 00:02:19, Serial0/1/0
O   172.29.4.128/25 [110/257] via 172.29.3.9, 00:02:19, Serial0/1/0
O   172.29.6.0/30 [110/384] via 172.29.3.9, 00:02:19, Serial0/1/0
O   172.29.6.4/30 [110/320] via 172.29.3.9, 00:02:19, Serial0/1/0
O   172.29.6.8/30 [110/320] via 172.29.3.9, 00:02:19, Serial0/1/0
O   172.29.6.12/30 [110/256] via 172.29.3.9, 00:02:19, Serial0/1/0
209.17.220.0/30 is subnetted, 2 subnets
O   209.17.220.0/30 [110/192] via 172.29.3.9, 00:02:19, Serial0/1/0
O   209.17.220.4/30 [110/128] via 172.29.3.9, 00:02:19, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:02:19, Serial0/1/0
    
```

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.

Tabla 3. Interfaces a deshabilitar.

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

Paso 1 Deshabilitar Interfaz Router Bogota1

*Bogota1(config)#router ospf 1*

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

Paso 2 Deshabilitar Interfaz Router Bogota2

*Bogota2(config)#router ospf 1*

*Bogota2(config-router)#passive-interface s0/1/0*

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

Paso 3 Deshabilitar Interfaz Router Bogota3

*Bogota3(config)#router ospf 1*

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

Paso 4 Deshabilitar Interfaz Router Medellin1

*Medellin1(config)#router ospf 1*

*Medellin1(config-router)#passive-interface s0/1/0*

Paso 5 Deshabilitar Interfaz Router Medellin2

*Medellin2(config)#router ospf 1*

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

## Paso 6 Deshabilitar Interfaz Router Medellin3

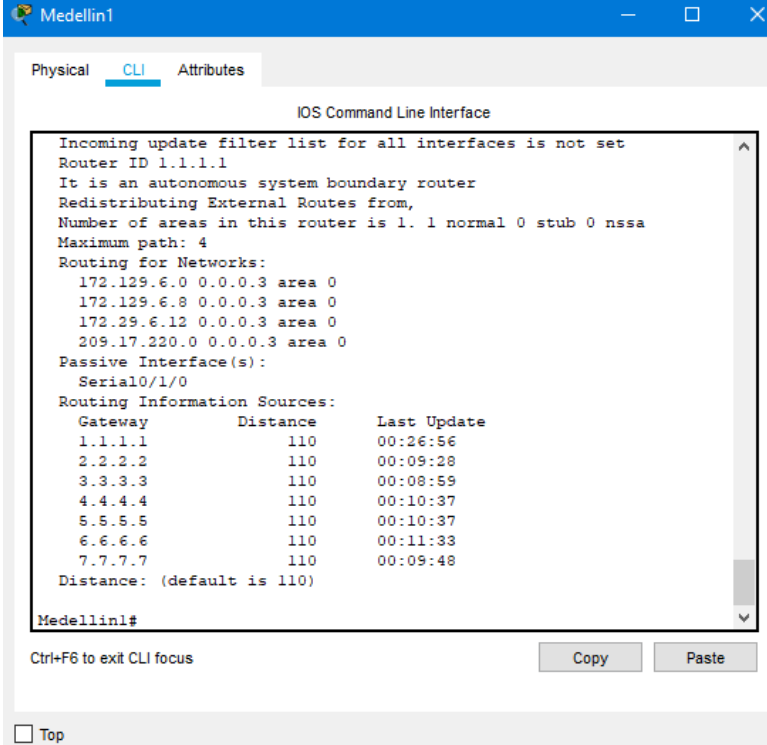
*Medellin3(config)#router ospf 1*

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

## 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.

Figura 27. Verificación protocolos Medellin1



The screenshot shows the CLI of router Medellin1. The output of the 'show ip ospf' command is as follows:

```
IOS Command Line Interface
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
It is an autonomous system boundary router
Redistributing External Routes from,
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 172.129.6.0 0.0.0.3 area 0
 172.129.6.8 0.0.0.3 area 0
 172.29.6.12 0.0.0.3 area 0
 209.17.220.0 0.0.0.3 area 0
Passive Interface(s):
 Serial0/1/0
Routing Information Sources:
Gateway          Distance    Last Update
1.1.1.1          110        00:26:56
2.2.2.2          110        00:09:28
3.3.3.3          110        00:08:59
4.4.4.4          110        00:10:37
5.5.5.5          110        00:10:37
6.6.6.6          110        00:11:33
7.7.7.7          110        00:09:48
Distance: (default is 110)
Medellin1#
```

Figura 28. Verificación protocolos Medellín2

```
Medellin2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.0 0.0.0.127 area 0
    172.29.6.0 0.0.0.3 area 0
    172.29.6.0 0.0.0.127 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:27:35
    2.2.2.2          110          00:10:07
    3.3.3.3          110          00:09:38
    4.4.4.4          110          00:11:16
    5.5.5.5          110          00:11:16
    6.6.6.6          110          00:12:12
    7.7.7.7          110          00:10:27
  Distance: (default is 110)

Medellin2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 29. Verificación protocolos Medellín3

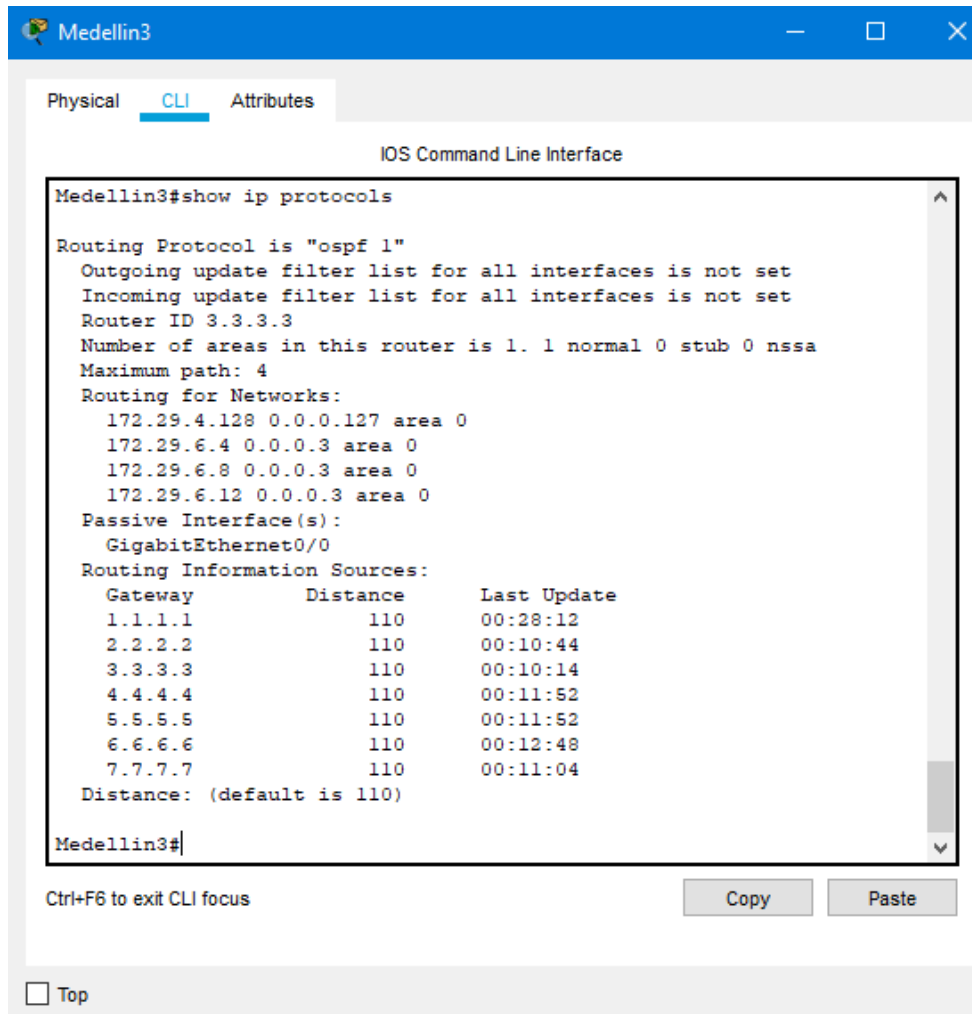


Figura 30. Verificación protocolos ISP

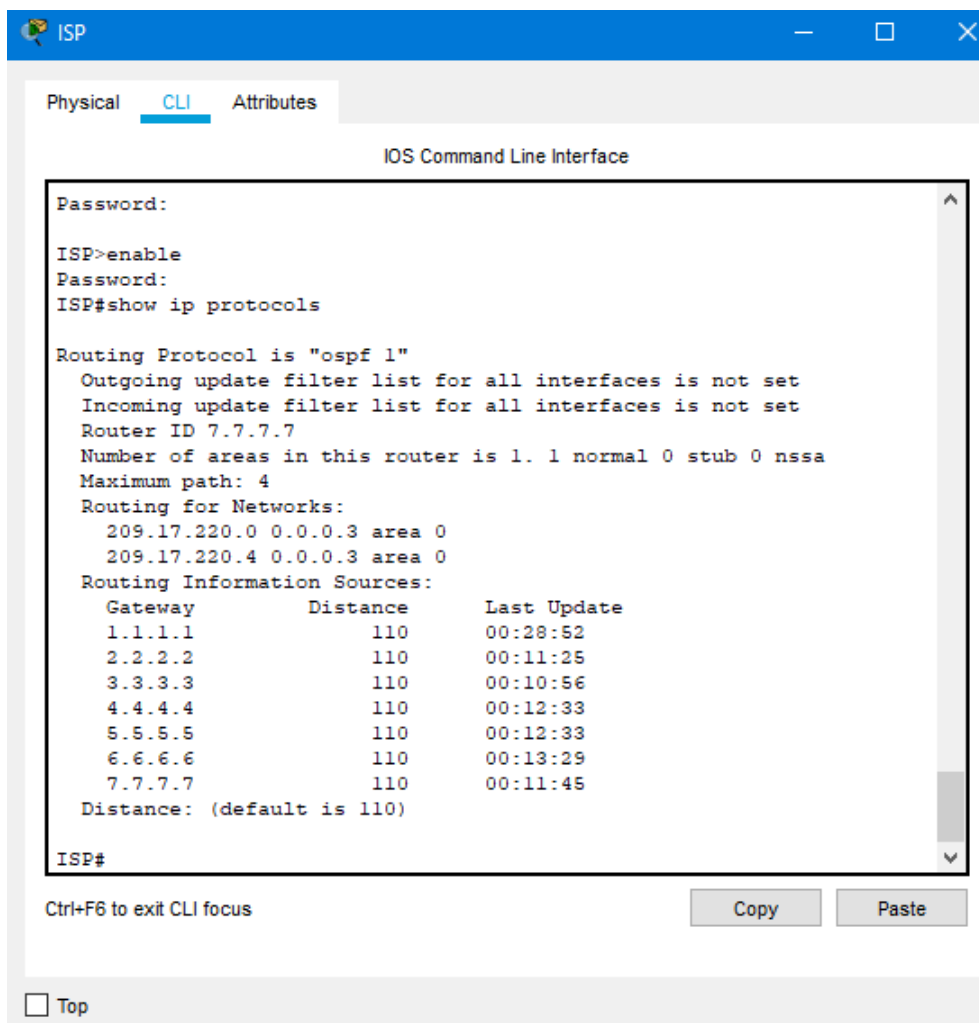
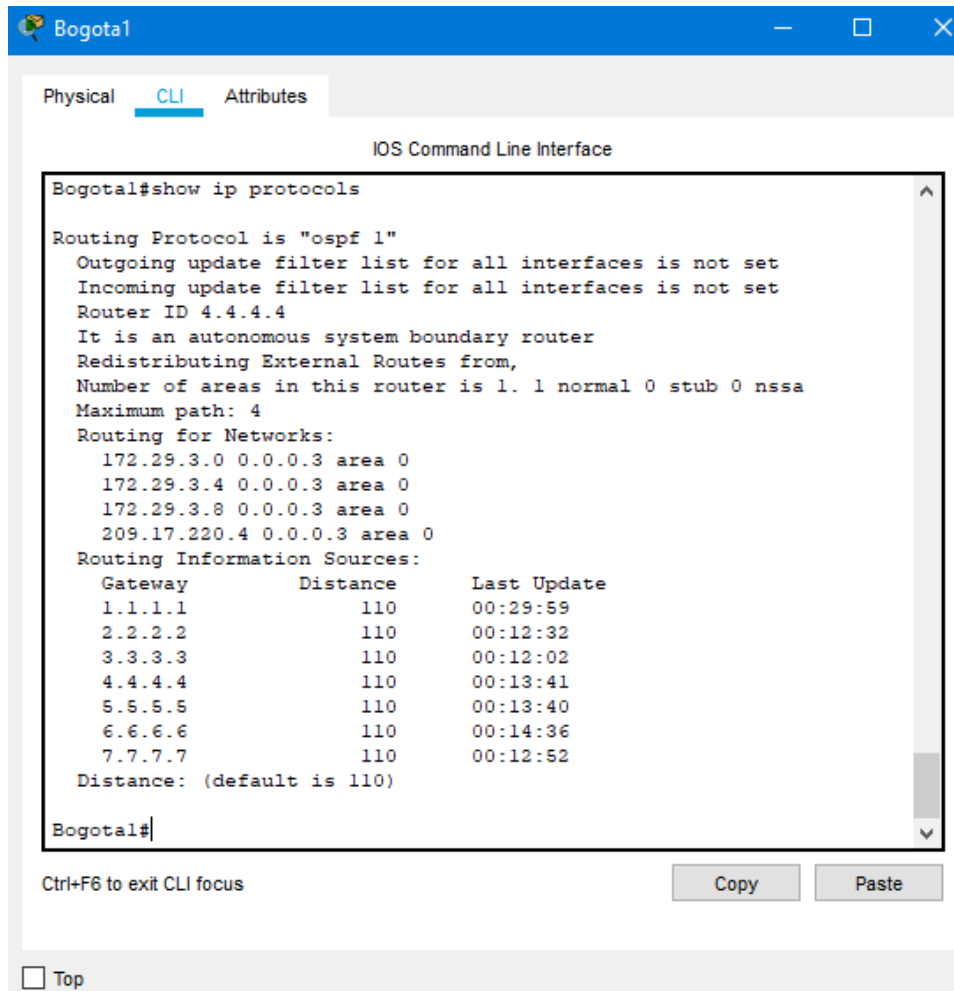


Figura 31. Verificación protocolos Bogota1



The screenshot shows a terminal window titled "Bogota1" with tabs for "Physical", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The user has entered the command "Bogotal#show ip protocols". The output shows OSPF configuration details, including the router ID (4.4.4.4), autonomous system boundary status, and a list of routing information sources with their respective gateways, distances, and last update times.

```
Bogotal#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 4.4.4.4
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.8 0.0.0.3 area 0
    209.17.220.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:29:59
    2.2.2.2          110          00:12:32
    3.3.3.3          110          00:12:02
    4.4.4.4          110          00:13:41
    5.5.5.5          110          00:13:40
    6.6.6.6          110          00:14:36
    7.7.7.7          110          00:12:52
  Distance: (default is 110)

Bogotal#
```

Below the terminal output, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste". At the bottom left, there is a "Top" button with a square icon.

Figura 32. Verificación protocolos Bogota2

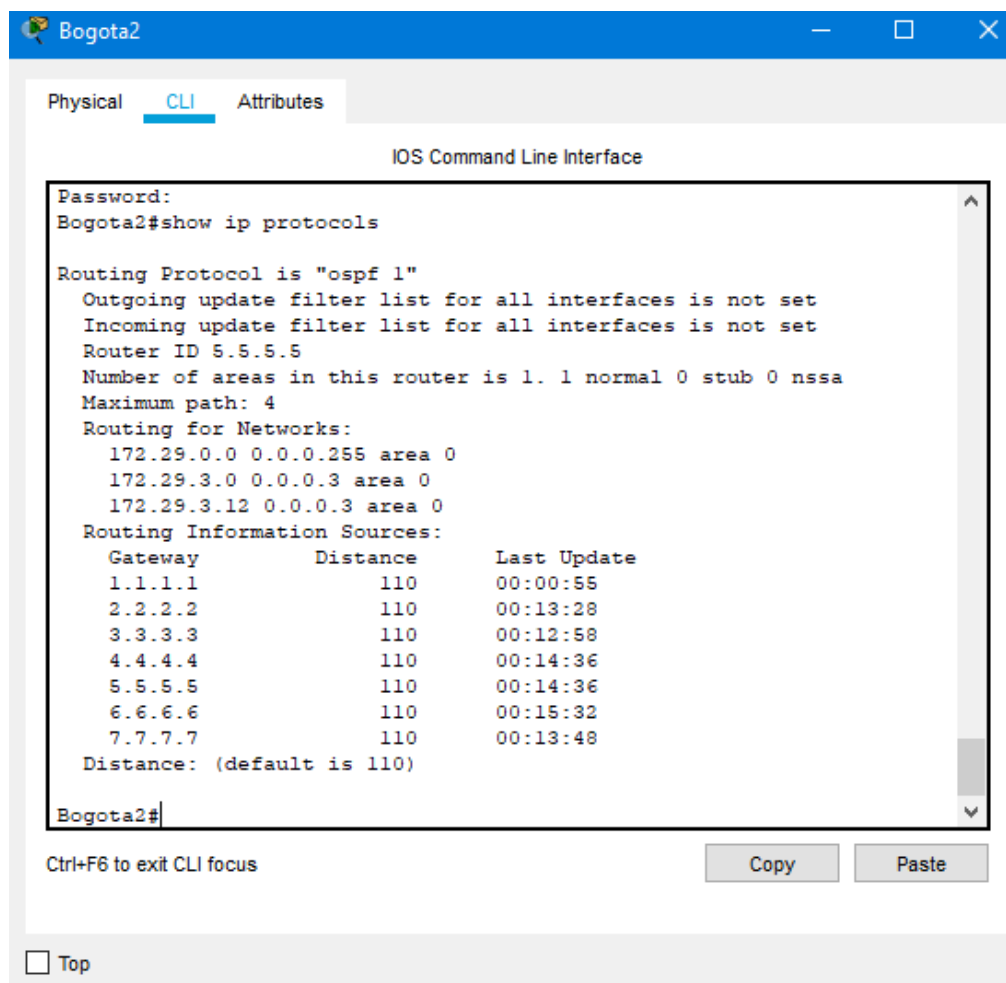
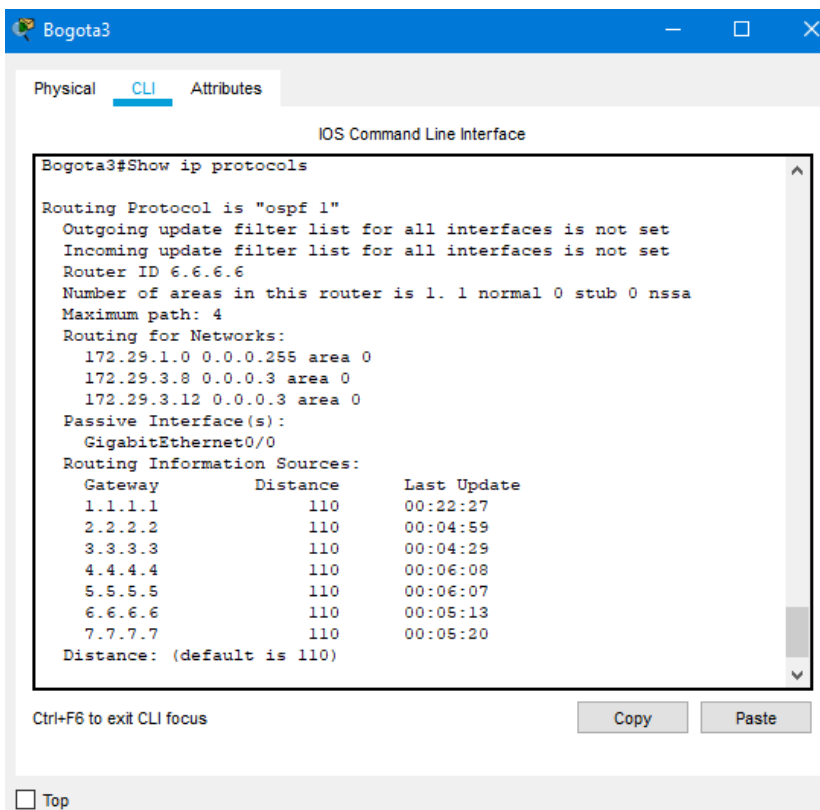


Figura 33. Verificación protocolos Bogota3



The screenshot shows a terminal window titled 'Bogota3' with tabs for 'Physical', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the output of the command 'Show ip protocols'. The output shows OSPF configuration details, including the router ID (6.6.6.6), number of areas (1), and a list of routing information sources with their respective gateways, distances, and last update times.

```
Bogota3#Show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 6.6.6.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.1.0 0.0.0.255 area 0
    172.29.3.8 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:


| Gateway | Distance | Last Update |
|---------|----------|-------------|
| 1.1.1.1 | 110      | 00:22:27    |
| 2.2.2.2 | 110      | 00:04:59    |
| 3.3.3.3 | 110      | 00:04:29    |
| 4.4.4.4 | 110      | 00:06:08    |
| 5.5.5.5 | 110      | 00:06:07    |
| 6.6.6.6 | 110      | 00:05:13    |
| 7.7.7.7 | 110      | 00:05:20    |


  Distance: (default is 110)
```

- 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.

*Este paso fue resuelto en el punto anterior con el comando show ip route.*

#### Parte 5: Configurar encapsulamiento y autenticación PPP.

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

#### Paso 7 Autenticación Chat Router Medellín1

```
Medellin1(config)#int s0/1/1
```

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

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

00:00:49: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 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)#ppp pap sent-username Medellin password cisco

#### Paso 8 Autenticación Chat Router Bogota1

Bogota1(config)#int s0/0/0

Bogota1(config-if)#encapsulation ppp

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Bogota1(config-if)#no shutdown

Bogota1(config-if)#exit

Bogota1(config)#username ISP secret cisco

Bogota1(config)#int s0/0/0

Bogota1(config-if)#ppp authentication chap

#### Paso 9 Autenticación Chat Router ISP

ISP(config)#int s0/0/0

ISP(config-if)#encapsulation ppp

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

11:27:15: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

ISP(config-if)#no shutdown

ISP(config-if)#exit

```

ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
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 authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#exit
ISP(config)#username bogota secret cisco
ISP(config)#int s0/0/1
ISP(config-if)#ppp authentication chap

```

#### Parte 5: 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.

```

Medellin1(config)#ip access-list standard host
Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
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)#exit
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
%SYS-5-CONFIG_I: Configured from console by console
Medellin1#show ip nat translation

```

- 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.

```

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#
%SYS-5-CONFIG_I: Configured from console by console
Bogota1#show ip nat translation
```

Figura 34. Ping Desde Medellin1 a Medellin2 y Medellin3

```
Medellin1#ping 172.29.6.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/14 ms

Medellin1#ping 172.29.6.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.14, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Medellin1#
```

Figura 35. Ping desde Bogota1 a Bogota2 y Bogota3

```
Bogota1#ping 172.29.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

Bogota1#ping 172.29.3.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/12 ms

Bogota1#ping 172.29.3.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/14 ms
```

Parte 6: 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(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)#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
```

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

```
Medellin3(config)#int g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
```

*Nota:* Es necesario configurar “ip helper” el cual permitirá ser un router de tránsito para llegar al router con el rol de DHCP. Por lo anterior utilizamos el comando ip helper-address para atrapar los broadcasts y redireccionarlos hacia la IP del router de Medellín2

Figura 36. Verificación Dhcp PC-A

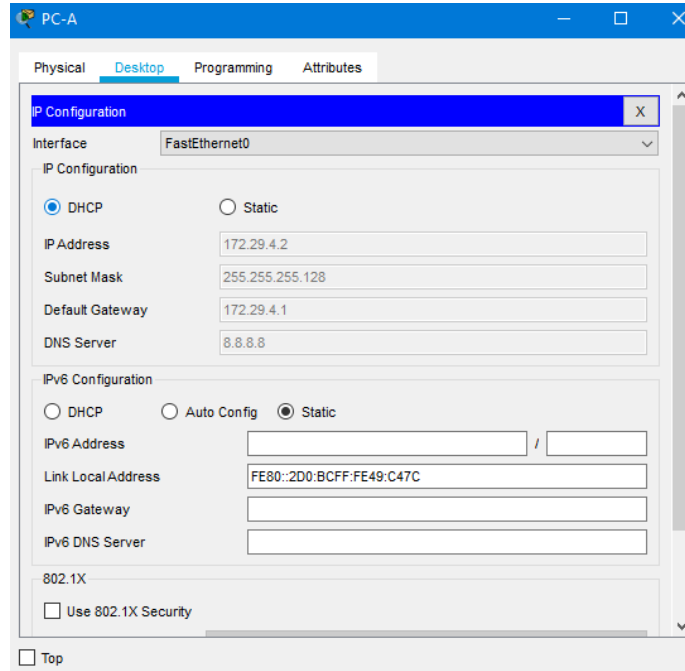
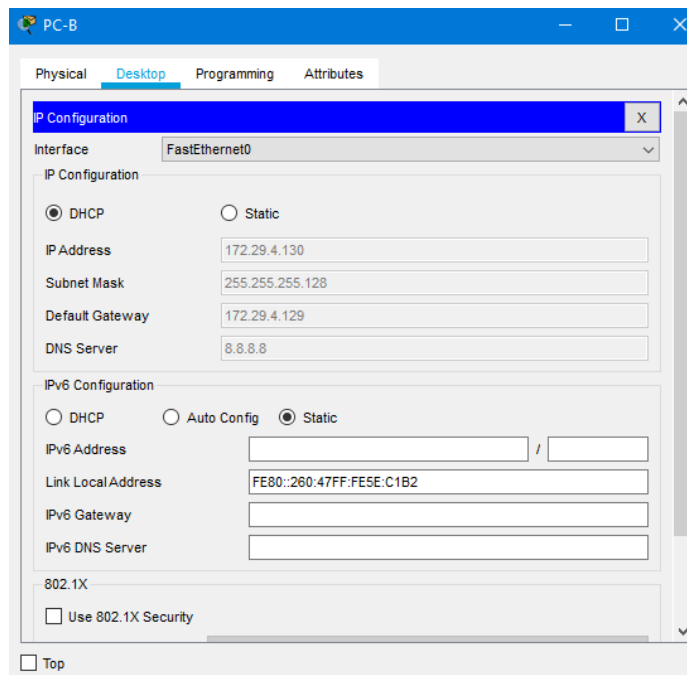


Figura 37. Verificación Dhcp PC-B



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

```
Bogota2(config)#ip dhcp excluded-address 172.29.0.1
Bogota2(config)#ip dhcp pool bogota2
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 172.29.1.1
Bogota2(config)#ip dhcp pool bogota3
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.1.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
```

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

```
Bogota3(config)#int g0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
```

*Nota:* Es necesario configurar "ip helper" el cual permitirá ser un router de tránsito para llegar al router con el rol de DHCP. Por lo anterior utilizamos el comando ip helper-address para atrapar los broadcasts y redireccionarlos hacia la IP del router de bogota2

Figura 38 Verificación Dhcp PC-C

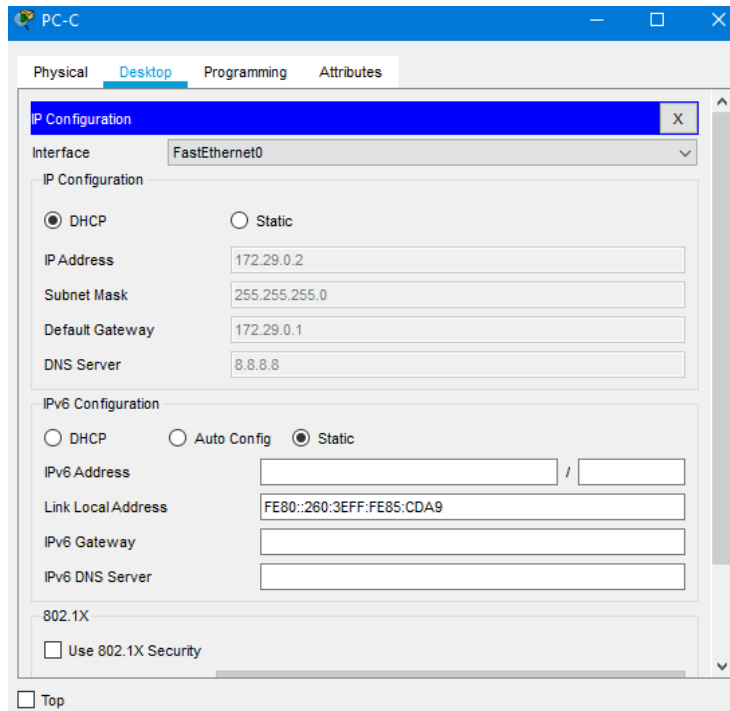
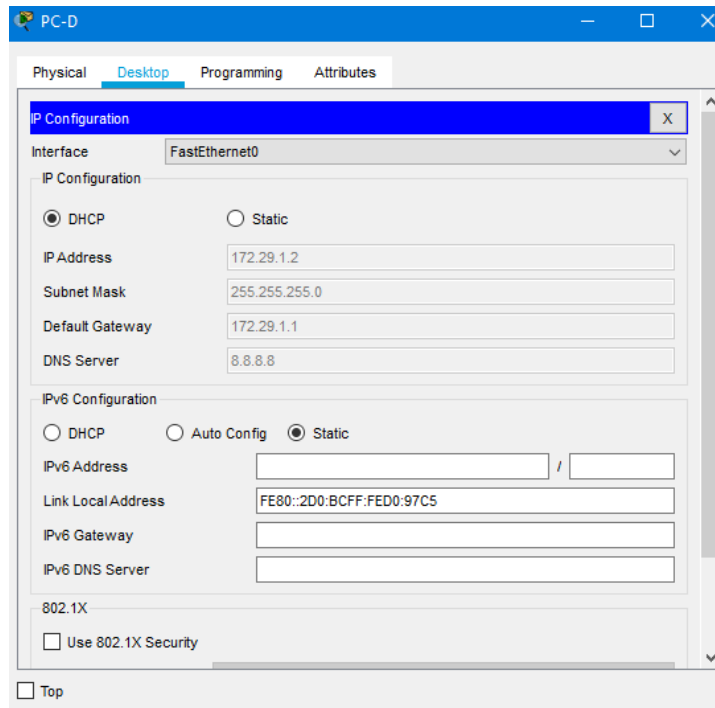


Figura 39. Verificación Dhcp PC-D



## Comando Guardar

Para cada uno de los router una vez finalizadas las configuraciones se debe ejecutar el siguiente comando para guardar las configuraciones y evitar que al apagarlos se reinicien las configuraciones.

```
Bogota1#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
Bogota2#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
Bogota3#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
Medellin1#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
Medellin2#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

Building configuration...

[OK]

Medellin3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

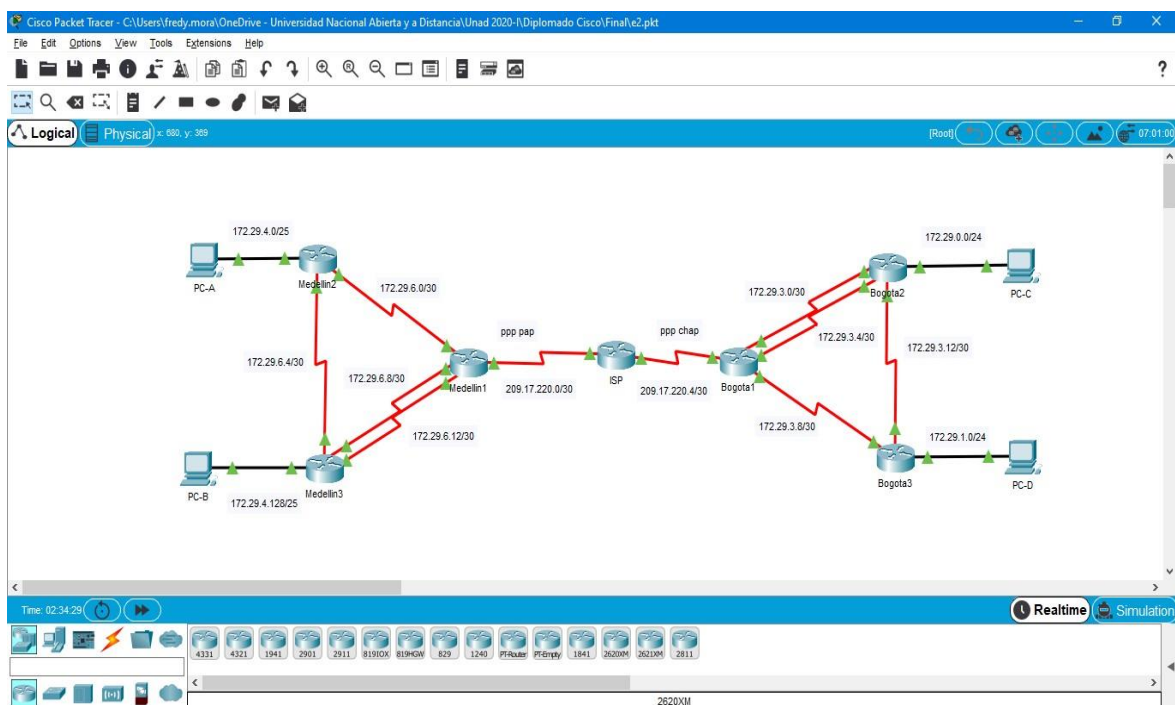
ISP#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Figura 40. Estructura Escenario 2



## CONCLUSIONES

1. Pusimos en práctica las configuraciones básicas de seguridad para brindar confiabilidad a cada uno de los dispositivos, cerrando la puerta a posibles manipulaciones indeseadas de las configuraciones de los dispositivos.
2. Estudiamos e implementamos la codificación necesaria para configurar las VLAN en los Switches para posteriormente configurar un router como servidor DHCP para que los equipos tomen una dirección ip disponible de manera automática.
3. Diseñamos la estructura propuesta para el caso, realizamos la adición de interfaces necesarias para lograr la conexión entre los dispositivos por medio de cables serial, configuramos el direccionamiento Ipv4 e Ipv6 para finalmente realizar la prueba del comando ping.
4. Realizamos la configuración del comando para hacer posible el enrutamiento por el protocolo OSPF, para especificar rutas predeterminadas para lograr la interconexión, habilitamos el encapsulamiento y su respectiva autenticación.
5. Ejecutamos los comandos necesarios para consultar las rutas de la red y las respectivas traducciones, estableceremos algunas interfaces como pasivas y finalmente validamos que las conexiones se establezcan de manera correcta.

## BIBLIOGRAFIA

1. Alex Alvarez. (2009). Comandos Basicos de un Router Cisco. mayo 17 de 2009, de Wordpress Sitio web: <https://alexalvarez0310.wordpress.com/category/comandos-basicos-de-un-router-cisco/>
2. Cisco. (2006). NAT: Definiciones locales y globales. Agosto 24 del 2006, de Cisco Sitio web: [https://www.cisco.com/c/es\\_mx/support/docs/ip/network-address-translation-nat/4606-8.html](https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/4606-8.html)
3. Cisco. (2020). Configurar ACL de IP de uso general. Abril 29 del 2020, de Cisco Sitio web: [https://www.cisco.com/c/es\\_mx/support/docs/ip/access-lists/26448-ACLsamples.html](https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html)
4. Cisco. (2005). Guía de diseño de OSPF. Agosto 10 del 2005, de Cisco Sitio web: [https://www.cisco.com/c/es\\_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html](https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html)
5. Cisco. (2005). Configuración dinámica de las opciones del servidor DHCP. Octubre 12 del 2005, de cisco Sitio web: [https://www.cisco.com/c/es\\_mx/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html](https://www.cisco.com/c/es_mx/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html)