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

MARÍA TERESA JARAMILLO MONCADA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
CIENCIAS BASICAS TECNOLOGÍA E INGENIRÍA
INGENIERIA DE SISTEMAS
GRANADA
2020

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

MARÍA TERESA JARAMILLO MONCADA

PRUEBA DE HABILIDADES TRABAJO DE GRADO

DIEGO EDINSON RAMIREZ INGENIERO ELECTRONICO ESPECIALISTA EN GERENCIA DE PROYECTOS, MASTER EN GERENCIA DE PROYECTOS DE TELECOMUNICACIONES

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
CIENCIAS BASICAS TECNOLOGÍA E INGENIRÍA
INGENIERIA DE SISTEMAS
GRANADA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

2020

Dedicatoria

Dedico este trabajo a mi familia que siempre me ha ayudado a edificarme como persona, siempre de la mano de Dios.

AGRADECIMIENTOS

Dedico este trabajo a todos los docentes que ha hecho parte de mi proceso de formación, siempre atentos a colaborar para que sea mejor cada día, al profesor Diego Édison Ramírez, por su entrega su tiempo y dedicación para tratar de ayudar, al ingeniero John Soto que con su alegría característica nos complicaba los trabajos para ir más allá de lo propuesto y así enriquecer más nuestro proceso de formación.

A mis familiares que me han dado la oportunidad de emprender este viaje de aprendizaje y han estado ahí acompañándome, a mi prima Angela Paola Delgado quien apoya, orienta y fortalece mi proceso, a mi amiga Tatiana Perdomo quien me anima en los momentos más difíciles dándome la fortaleza para cumplir con todas las responsabilidades en este largo caminar.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Con el desarrollo del siguiente trabajo se pondrán a prueba las habilidades adquiridas en el trasncurso del diplomado de pronfundizacion CISCO, por medio de dos casos de estudio.

Para cumplir con los objetivos y dar solución a lo planteado se utilizó la herramienta Cisco Packet Traser, la cual permite realizar configuraciones en cada uno de los dispositivos y asi poder realizar el montaje, aplicando protocolos RIp V2 y OSPF según lo requerido en la guía, además de utilizar servicios DHCP, listas de acceos y traducción de direcciones NAT.

GLOSARIO

ROUTER: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

SWITCH: es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta

PROTOCOLO RIP: Routing Information Protocol (RIP), es un protocolo de puerta de enlace interna o interior (Interior Gateway Protocol, IGP) utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados.

PROTOCOLO OSPF: Open Shortest Path First (OSPF), Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

IPV6: El IPv6 es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones. Su desarrollo comenzó en diciembre de 1998 cuando Steve Deering y Robert Hinden, empleados de Cisco y Nokia publicaron una especificación formal del protocolo a través de un RFC1 2 y aún continua su implementación.

SERVIDOR: es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

1. INTRODUCCIÓN

A lo largo del desarrollo de las actividades propuestas en el diplomado se ha adquirido diversos conocimientos que permitirán desarrollar las actividades propuestas, en el siguiente trabajo se expondrá algunas de esas habilidades para darle solución a los escenarios expuestos, donde se debe desde aplicar la configuración mas básica, como también se debe configurar Network Address translatio (NAT), listas de control ACL, servidores Dhcp, routing dinamico RIPv2, OSPF, entre otros.

Esta prueba no sirve para obtener una nota, por el contrario es la ocasión perfecta para demostrar lo que se ha aprendido, además de abrir las puestar para seguir empapándose del tema, y seguir adquiriendo nuevos conocimientos.

2 DESARROLLO DE LOS DOS ESCENARIOS

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.

Topología

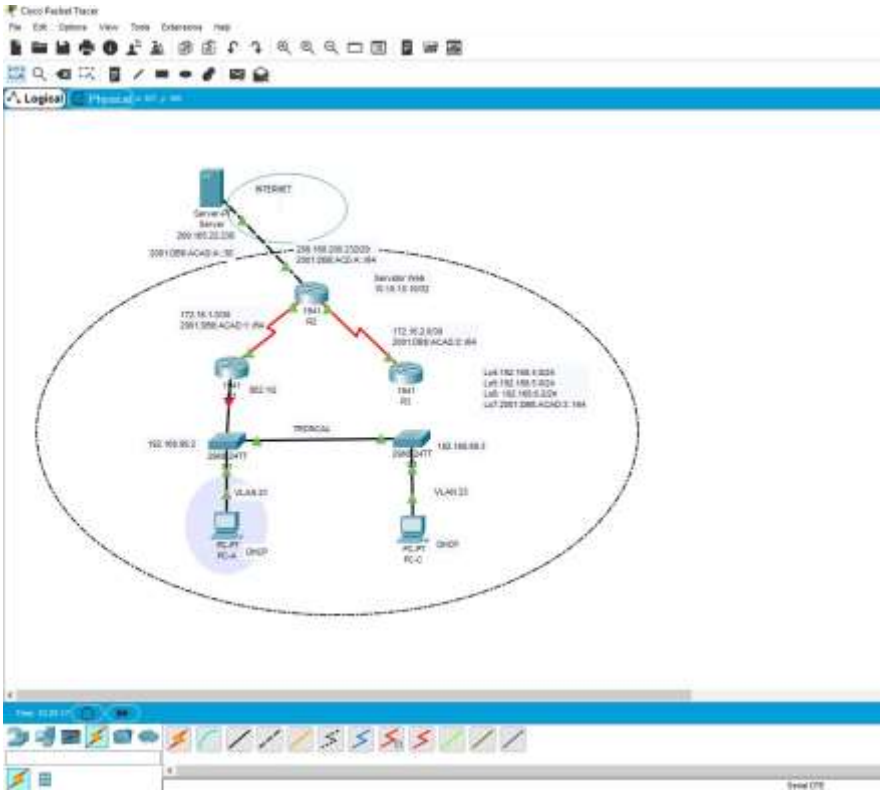


Figura 1 topologia escenario 1

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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	“Luego de tener la topologia lista accedemos al R1, vamos a cli y escribimos el siguiente codigo”: *en* *erase startup-config*
Volver a cargar todos los routers	“Seguidamente se recargan los router o con el commando” *reload*
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	“Para iniciar la configuracion de los switches y eliminar las VLAN, primero accedemos al S1 y escribimos el siguiente commando” *en* *erase startup-config* *delete vlan.dat*
Volver a cargar ambos switches	“Seguidamente se recargan los router o con el commando” *reload*
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	“Para esta verificacion se hace el s1 y escribimos” *en* *dir flash:*

Step 1: Parte 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
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	“Para esto vamos a la consola del R1 y escribilmos” *en* *config t* *no ip domain-lookup*
Nombre del router	“Seguidamente para asignar el nombre se escribe” *hostname R1*
Contraseña de exec privilegiado cifrada	“Para asignar la contraseña en la misma consola y siguiendo la liena de codigo escribimos” *Enable secret class*
Contraseña de acceso a la consola	“Para la asignación de la contraseña de acceso se debe escribir el siguiente codigo” *Line console 0* *Password cisco* *login*
Contraseña de acceso Telnet	Siguiendo la linea de commando escribimos *Line vty 0 15* *Password cisco* *login*
Cifrar las contraseñas de texto no cifrado	Para el cifrado es necesario escribir *Service password-encryption*
Mensaje MOTD	Una vez cifrado escribimos el mensaje del motd por si alguien va aingresar para ello utilizamos *Banner motd “Se prohíbe el acceso no autorizado”*
Interfaz S0/0/0	Establezca la descripción: para esto se hace escribiendo el siguiente comando, como estamos seleccionando la interfaz *Description connection R2* Establecer la dirección IPv4 para ello se utiliza *Ip address 172.16.1.1 255.255.255.252* Establecer la dirección IPv6 *Ipv6 addres 2001:DB8:ACAD:1::1/64* Establecer la frecuencia de reloj en 128000 *Clock rate 128000* Activar la interfaz *No shutdown*

Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0, para esto debemos hacerlo por las rutas predeterminada como se muestra continuación *Ip route 0.0.0.0 0.0.0.0 s0/0/0* Configurar una ruta IPv6 predeterminada de S0/0/0 *Ipv6 route ::/0 s0/0/0*

Nota: Todavía no configure G0/1.

Paso 2: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Para esto vamos a la consola del R1 y escribilmos *en* *config t* *no ip domain-lookup*
Nombre del router	Seguidamente para asignar el nombre se escribe *hostname R2*
Contraseña de exec privilegiado cifrada	Para asignar la contraseña en la misma consola y siguiendo la liena de codigo escribimos *Enable secret class*
Contraseña de acceso a la consola	Para la asignación de la contraseña de acceso se debe escribir el siguiente codigo *Line console 0* *Password cisco* *login*
Contraseña de acceso Telnet	Siguiendo la linea de commando escribimos *Line vty 0 15* *Password cisco* *login*
Cifrar las contraseñas de texto no cifrado	Para el cifrado es necesario escribir *Service password-encryption*
Habilitar el servidor HTTP	*Ip http server*
Mensaje MOTD	Una vez cifrado escribimos el mensaje del motd por si alguien va aingresar para ello utilizamos *Banner motd "Se prohíbe el acceso no autorizado"*

Interfaz S0/0/0	Primero seleccionamos la interface *Int s0/0/0* Luego hacemos la description *Description connection to R1* Asignamos ipv4 *Ip address 172.16.1.2 255.255.255.252* Luego ipv6 *Ipv6 address 2001:DB8:ACAD:1::2/64* Y finalmente encendemos *No shutdown*
Interfaz S0/0/1	Primero seleccionamos la interface *Int s0/0/1* Luego hacemos la description *Description connection to R3* Asignamos ipv4 *Ip address 172.16.2.2 255.255.255.252* Luego ipv6 *Ipv6 address 2001:DB8:ACAD:2::2/64* Luego establecemos la frecuencia del reloj Clock rate 128000 Y finalmente encendemos *No shutdown*
Interfaz G0/0 (simulación de Internet)	Seleccionamos la interface *Int g0/0* Luego hacemos la descripcion *Description connection to internet* Asignamos la ipv4 y pv6 *Ip add 209.165.200.233 255.255.255.248* *Ipv6 add 2001:DB8:ACAD:a::1/64* *No shut*
Interfaz loopback 0 (servidor web simulado)	Sleccionamos la interface para la simulacion *Int loopback 0* Luego asignamos la direccion ipv4 *Ip add 10.10.10.10 255.255.255.255* Y la description *Description Simulador de servidor web*
Ruta predeterminada	Salimos una vez con exit Luego escribimos Ip route 0.0.0.0 0.0.0.0 g0/0 Ipv6 route ::/0 g0/0

Paso 3: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para esto vamos a la consola del R3 y escribilmos *en* *config t* *no ip domain-lookup*
Nombre del router	Seguidamente para asignar el nombre se escribe *hostname R3*
Contraseña de exec privilegiado cifrada	Para asignar la contraseña en la misma consola y siguiendo la liena de codigo escribimos *Enable secret class*
Contraseña de acceso a la consola	Para la asignación de la contraseña de acceso se debe escribir el siguiente codigo *Line console 0* *Password cisco* *login*
Contraseña de acceso Telnet	Siguiendo la linea de commando escribimos *Line vty 0 15* *Password cisco* *login*
Cifrar las contraseñas de texto no cifrado	Para el cifrado es necesario escribir *Service password-encryption*
Mensaje MOTD	Una vez cifrado escribimos el mensaje del motd por si alguien va aingresar para ello utilizamos *Banner motd "Se prohíbe el acceso no autorizado"*

Interfaz S0/0/1	Primero seleccionamos la interface *Int s0/0/1* Luego agregamos la descripcion *Description conexion a R2* Luego asignamos ipv4 y Ipv6 *Ip add 172.16.2.1 255.255.255.252* *Ipv6 add 2001:DBA:ACAD:2::1/64* Luego encendemos con *No shut*
Interfaz loopback 4	*Int loopback 4* *Ip add 192.168.4.1 255.255.255.0*
Interfaz loopback 5	*Int loopback 5* *Ip add 192.168.5.1 255.255.255.0*
Interfaz loopback 6	*Int loopback 6* *Ip add 192.168.6.1 255.255.255.0*
Interfaz loopback 7	Para el loopback 7 se asigna ipv6 *Int loopback 7* *Ipv6 add 2001:Db8:ACAD:3::1/64*
Rutas predeterminadas	Ip route 0.0.0.0 0.0.0.0 s0/0/1 Ipv6 route ::/0 s0/0/1

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*En* *Config t* *No ip domain-lookup*
Nombre del switch	*Hostname S1*
Contraseña de exec privilegiado cifrada	*Enable secret class*
Contraseña de acceso a la consola	*Line console 0* *Password cisco* *Login*
Contraseña de acceso Telnet	*Line vty 0 15* *Password cisco*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Mensaje MOTD	*Banner motd "Se prohíbe el acceso no autorizado"*

Paso 5: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*En* *Config t* *No ip domain-lookup*
Nombre del switch	*Hostname S3*
Contraseña de exec privilegiado cifrada	*Enable secret class*
Contraseña de acceso a la consola	*Line console 0* *Password cisco* *Login*
Contraseña de acceso Telnet	*Line vty 0 15* *Password cisco*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Mensaje MOTD	*Banner motd "Se prohíbe el acceso no autorizado"*

Paso 6: 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:

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

Figura 2 ping desde R1 a R2

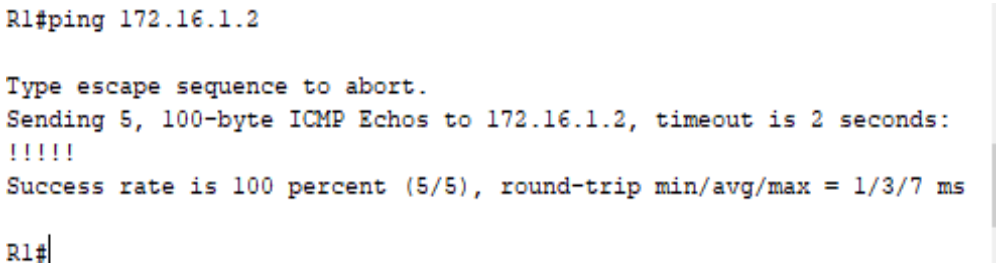


Figura 3. ping desde R2 a R3

```
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
```

Figura 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 2: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Para asignar el nombre de las vlan accedeos al S1 y escribimos el siguiente commando *Vlan 21* *Name contabilidad* Y ya asignamos los nombres y se debe hacer los mismo con las otras dos *Vlan 23* *name ingenieria* *Vlan 99* *Name administracion*

Asignar la dirección IP de administración.	Para asignar la ip debe salir con exity luego seleccionamos la interface y completamos el codigo *Int vlan 99* *Ip add 192.168.99.2 255.255.255.0* *No shut*
Asignar el gateway predeterminado	Para ello debemos escribir *Ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	*Int f0/3* *Switchport mode trunk* *Switchport trunk native vlan 1*
Forzar el enlace troncal en la interfaz F0/5	*Int f0/3* *Switchport mode trunk* *Switchport trunk native vlan 1*
Configurar el resto de los puertos como puertos de acceso	*int range f0/1-2, f0/4, f0/6-24, g0/1-2*
Asignar F0/6 a la VLAN 21	*switchport access vlan 21*
Apagar todos los puertos sin usar	*int range f0/1-2, f0/4, f0/7-24, g0/1-2* *shutdown*

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Para asignar el nombre de las vlan accedeos al S1 y escribimos el siguiente commando *Vlan 21* *Name contabilidad* Y ya asignamos los nombres y se debe hacer los mismo con las otras dos *Vlan 23* *name ingenieria* *Vlan 99* *Name administracion*
Asignar la dirección IP de administración	*Ip add 192.168.99.3 255.255.255.0* *No shut*
Asignar el gateway predeterminado.	*Ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	*Int f0/3* *Switchport mode trunk* *Switchport trunk native vlan 1*

Configurar el resto de los puertos como puertos de acceso	*int range f0/1-2, f0/4-24, g0/1-2*
Asignar F0/18 a la VLAN 23	*Switchport mode acess vlan 23*
Apagar todos los puertos sin usar	*int range f0/1-2, f0/4-17,f0/24, g0/1-2* *shutdown*

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Para poder realizare esta paso debemos ingresar al router 1 y entrear a config *En* *Config t* Luego seleccionamos la subinterfaz *Int g0/1.21* Asignamos la descripcion *Description LAN de contabilidad* Luego asignamos la direccion *Ip add 192.168.21.1 255.255.255.0*
Configurar la subinterfaz 802.1Q .23 en G0/1	Para poder realizare esta paso debemos ingresar al router 1 y entrear a config *En* *Config t* Luego seleccionamos la subinterfaz *Int g0/1.23* Asignamos la descripcion *Description LAN de* ingenieria Luego asignamos la direccion *Ip add 192.168.23.1 255.255.255.0*
Configurar la subinterfaz 802.1Q .99 en G0/1	Para poder realizare esta paso debemos ingresar al router 1 y entrear a config *En* *Config t* Luego seleccionamos la subinterfaz *Int g0/1.99* Asignamos la descripcion *Description LAN de administracion* Luego asignamos la direccion *Ip add 192.168.99.1 255.255.255.0*

Activar la interfaz G0/1	Seleccionamos la interfaz *Int g0/1* *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
```

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 5: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Para la configuracion hacemos los siguiente, vamos a R1 *R1(config)router rip* *Version 2*
Anunciar las redes conectadas directamente	Para ver las redes conectadas escribimos *Do show ip route connected* *Luego anunciamos las redes* network 172.16.1.0 network 172.168.21.0 network 172.168.23.0 network 172.168.99.0
Establecer todas las interfaces LAN como pasivas	Para poder asignarlas como pasivas se debe escribir el siguiente commando *passive-interface g0/1.21* luego este para la vlan 23 *passive-interface g0/1.23* y pr ultimo *passive-interface g0/1.99*
Desactive la sumarización automática	*no auto-summary*

Paso 6: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	*en* *Config t* *Ruouter rip* *Version 2*

Anunciar las redes conectadas directamente	*Do show ip route connectec* *Network 10.10.10.10* *Network 172.16.1.0* *Network 172.16.2.0*
Establecer la interfaz LAN (loopback) como pasiva	Para esto utilizamos *Passive-interface loopback 0*
Desactive la sumarización automática.	*No auto-summary*

Paso 7: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	*en* *config t* *router rip* *version 2*
Anunciar redes IPv4 conectadas directamente	*do show ip route connected* *172.16.2.0* *network 172.168.4.0* *network 172.168.5.0* *network 172.168.6.0*
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	*passive-interface loopback 4* *passive-interface loopback 5* *passive-interface loopback 6*
Desactive la sumarización automática.	*no auto-summary*

Paso 8: Verificar la información de RIP

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

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas RIP?	Show ip route ip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run

Figura 9 verificacion de 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:

Elemento o tarea de configuración	Especificación

Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Par apoder reservalas debos aplicar el siguiente codigo *En* *Config t* *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	*En* *Config t* *Ip dhcp excluded-address 192.168.23.1 192.168.23.20*
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT *ip dhcp pool ACCT* *network 192.168.21.0 255.255.255.0* *default-router 192.168.21.1* Servidor DNS: 10.10.10.10 *dns-server 10.10.10.10* Nombre de dominio: ccna-sa.com *domain-name ccna-sa.com*
Crear un pool de DHCP para la VLAN 23	Nombre: ACCT *ip dhcp pool ACCT* *network 192.168.23.0 255.255.255.0* *default-router 192.168.23.1* Servidor DNS: 10.10.10.10 *dns-server 10.10.10.10* Nombre de dominio: ccna-sa.com *domain-name ccna-sa.com*

Paso 9: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** *username 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: **209.165.200.237** *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	*access-list 1 permit 192.168.21.0 0.0.0.255* *access-list 1 permit 192.168.23.0 0.0.0.255* *access-list 1 permit 192.168.4.0 0.0.3.255*
Defina el pool de direcciones IP públicas utilizables.	*ip nat pool INTERNET 209.165.200.233 209.168.200.236 netmask 255.255.255.248*
Definir la traducción de NAT dinámica	*ip nat inside source list 1 pool INTERNET*

Paso 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.

Figura 13 resultados dhcp Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

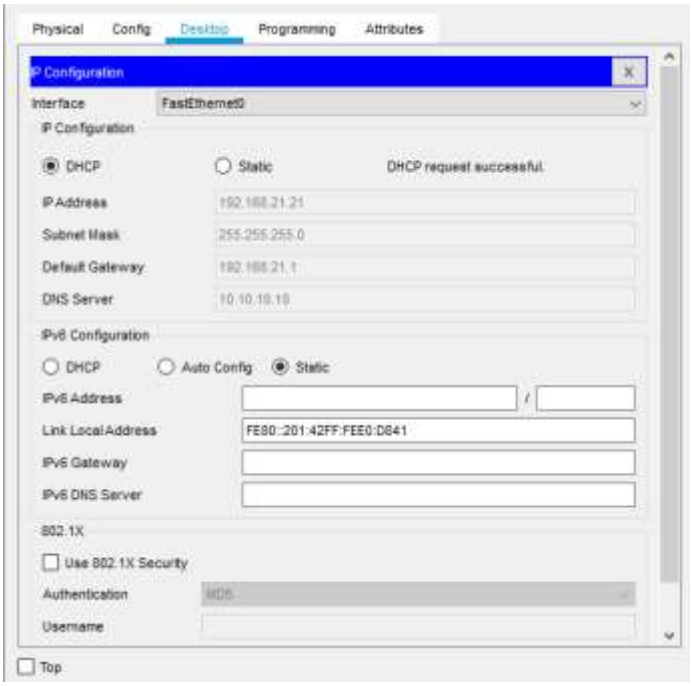
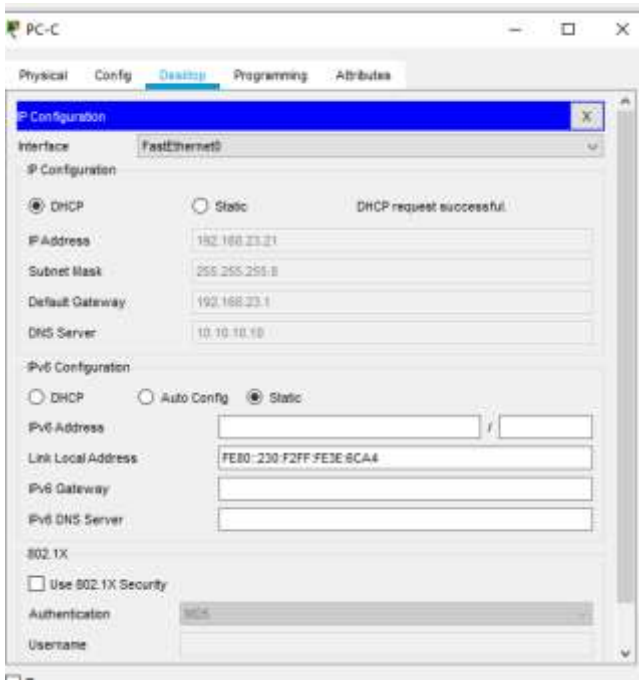
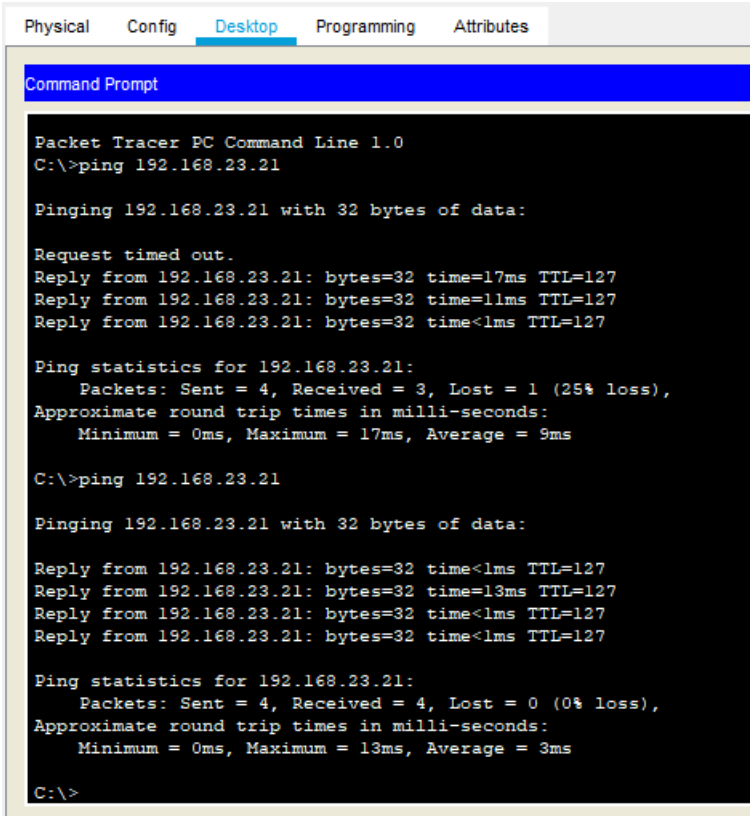


Figura 14Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



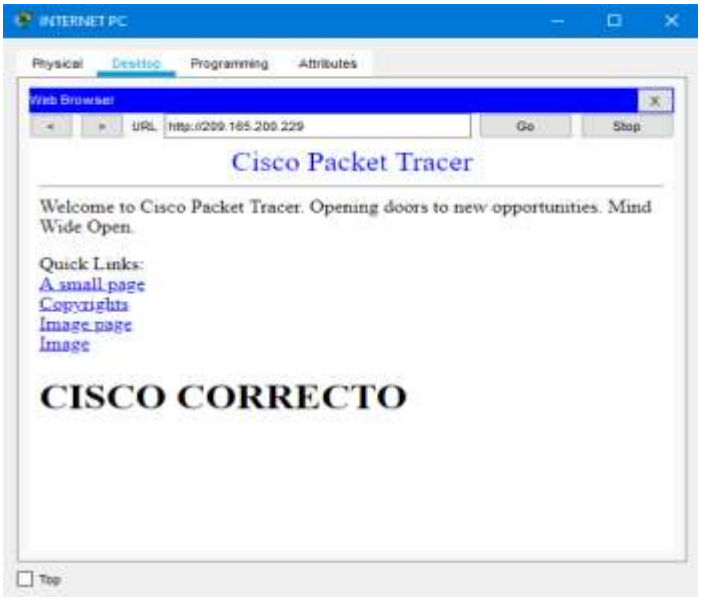
Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 15 Verificar que la PC-A pueda hacer ping a la 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 16. probar acceso al servidor web



Parte 3: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** *clock set 9:00:00 5 march 2016*
Configure R2 como un maestro NTP.	Nivel de estrato: **5** *ntp master 5*
Configurar R1 como un cliente NTP.	Servidor: **R2** ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar

Verifique la configuración de NTP en R1.
figura 17 verificacion NTP

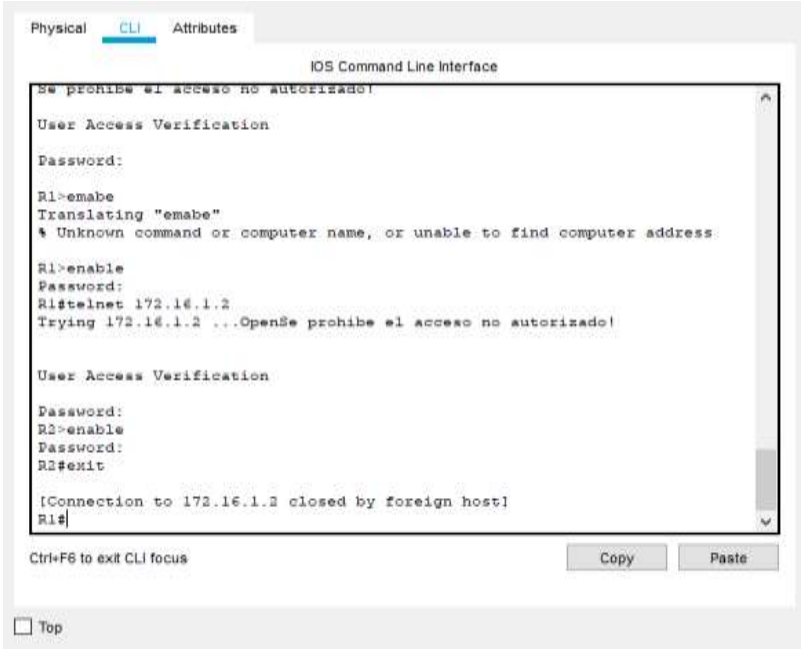
```
R1#show ntp associations

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
```

Parte 4: Configurar y verificar las listas de control de acceso (ACL)

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** ip access-list standard ADMIN-MGT permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	line vty 0 15 access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohbe el acceso no autorizado User Access Verification Password:

Figura 18. Prueba de conexión telnet de R1 y R2



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

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show 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)) show ip access-list
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?	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 unreachables 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 unreachables 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 unreachables 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 unreachables 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?	show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translations *

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

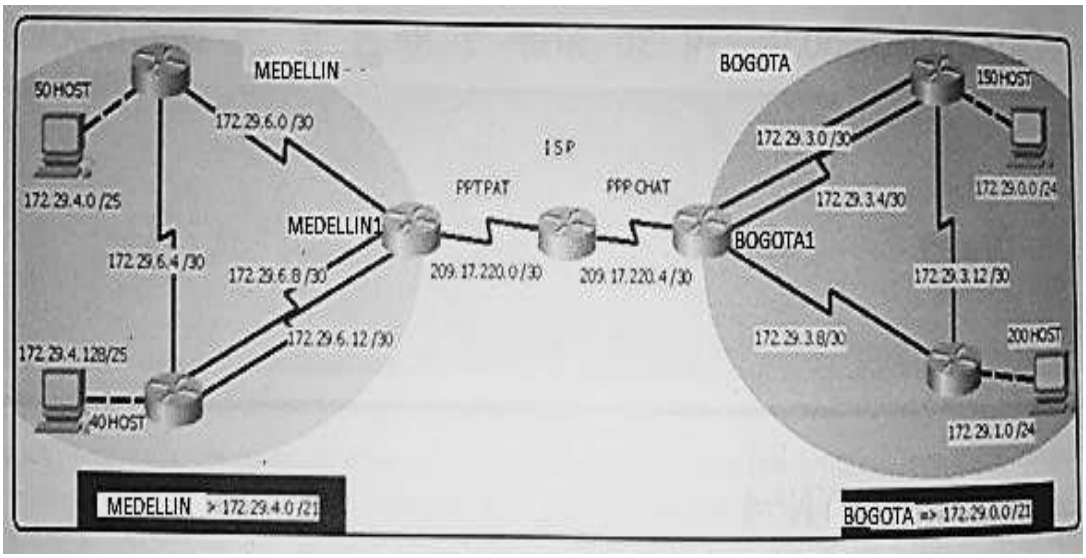


Figura19 topologia escenario 2

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

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

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).
- Como ya se había configurado en el primer escenario vamos a trabjar con esa configuración básica.

Asignacion de nombre, para esto se utiliza el siguiente comando
En
Config t
Hostname Medellin1

Para la asignaciond e contraseña EXEC privilegiado
Enable secret class

Para la asignación de contraseñas de EXEC de usuarios y líneas VTY
Line console 0
Password cisco
Login
Exit
Line vty 0 15
Password cisco
Login
Exit

Para el cifrado de contraseñas
Service password-encryption

Motd
Banner motd “solo personal autorizado”
exit
Guardar las configuraciones NVRAM
Copy running-config startup-config

Y se realiza el mismo proceso con los demás dispositivos
Medellin2

Asignacion de nombre, para esto se utiliza el siguiente comando
En
Config t
Hostname Medellin2

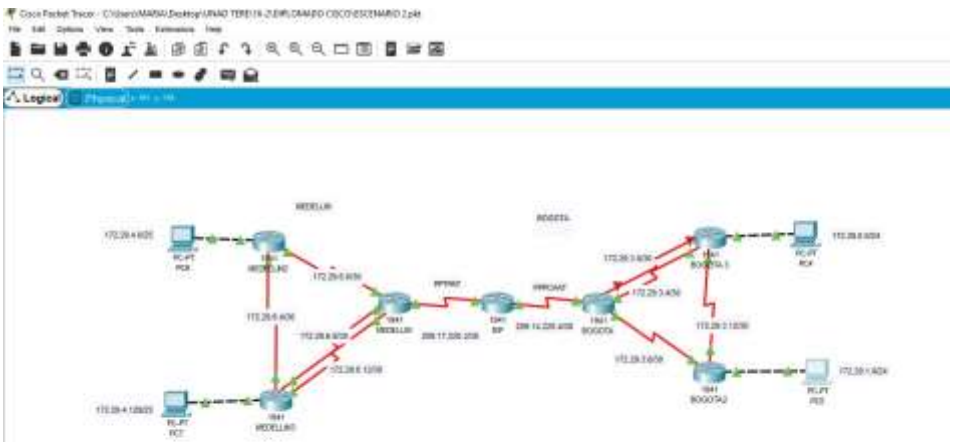
Para la asignaciond e contraseña EXEC privilegiado
Enable secret class

Para la asignación de contraseñas de EXEC de usuarios y líneas VTY
Line console 0
Password cisco
Login
Exit
Line vty 0 15
Password cisco
Login
Exit

Para el cifrado de contraseñas
Service password-encryption

Motd
Banner motd “solo personal autorizado”
exit
Guardar las configuraciones NVRAM
Copy running-config startup-config

- Realizar la conexión fisica de los equipos con base en la topología de red
  Figura 20 topologia porpia escenario 2



- *Tabla de direccionamiento*

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
	S/0/0/1	172.29.3.14	255.255.255.252
	G0/0	172.29.1.1	255.255.255.0

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

Aignacion ip ISP
Ingresamos encedemos e ingresamos a configuración
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z
Seleccionamos la interface
ISP(config)#int s0/1/1
Asignamos la dirección ip
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
Activamos con el comando
ISP(config-if)#no shut
Seleccionamos la interface
ISP(config-if)#int s0/1/0
Agregamos la ip y la submascara de red
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
Activamos
ISP(config-if)#no shut

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.

Primero encedemos accedemos a configuración y activamos el protocolo osfp
Medellin(config)#router ospf 1
Seleccionamos una identidad puede ser 1.1.1.1 2.2.2.2 o el numero que se desee
Medellin(config-router)#router-id 1.1.1.1
Verificamos que redes hay conectadas
Medellin(config-router)#do show ip route connected
Enunciamos las redes
Medellin(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin(config-router)#network 172.29.6.12 0.0.0.3 area 0
Asignamos la interface pasiva
Medellin(config-router)#passive-interface s0/0/1

Repetir en todos los routers
Medellin2>en
Password:
Medellin2#config
Medellin2(config)#router ospf 1
Medellin2(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/1/1
Medellin2(config-router)#router-id 1.1.1.1
Medellin2(config-router)#network 172.29.4.0 0.0.0.3 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)#passive-onterface g0/0
Medellin2(config-router)#passive-interface g0/0

Medellin3(config-router)#exit
Medellin3(config)#int g0/0
Medellin3(config-if)#ip add 172.29.4.129 255.255.255.128
Medellin3(config-if)#int s0/0/1
Medellin3(config-if)#ip add 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shut down
Medellin3(config-if)#int s0/1/1
Medellin3(config-if)#ip add 172.29.6.10 255.255.255.252
Medellin3(config-if)#no shut
Medellin3(config-if)#int s0/1/0
Medellin3(config-if)#ip add 172.26.6.14 255.255.255.252
Medellin3(config-if)#exit
Medellin3(config)#router ospf 3
Medellin3(config-router)#router-id 3.3.3.3
Medellin3(config-router)#network 172.29.4.128 0.0.0.3 area 0

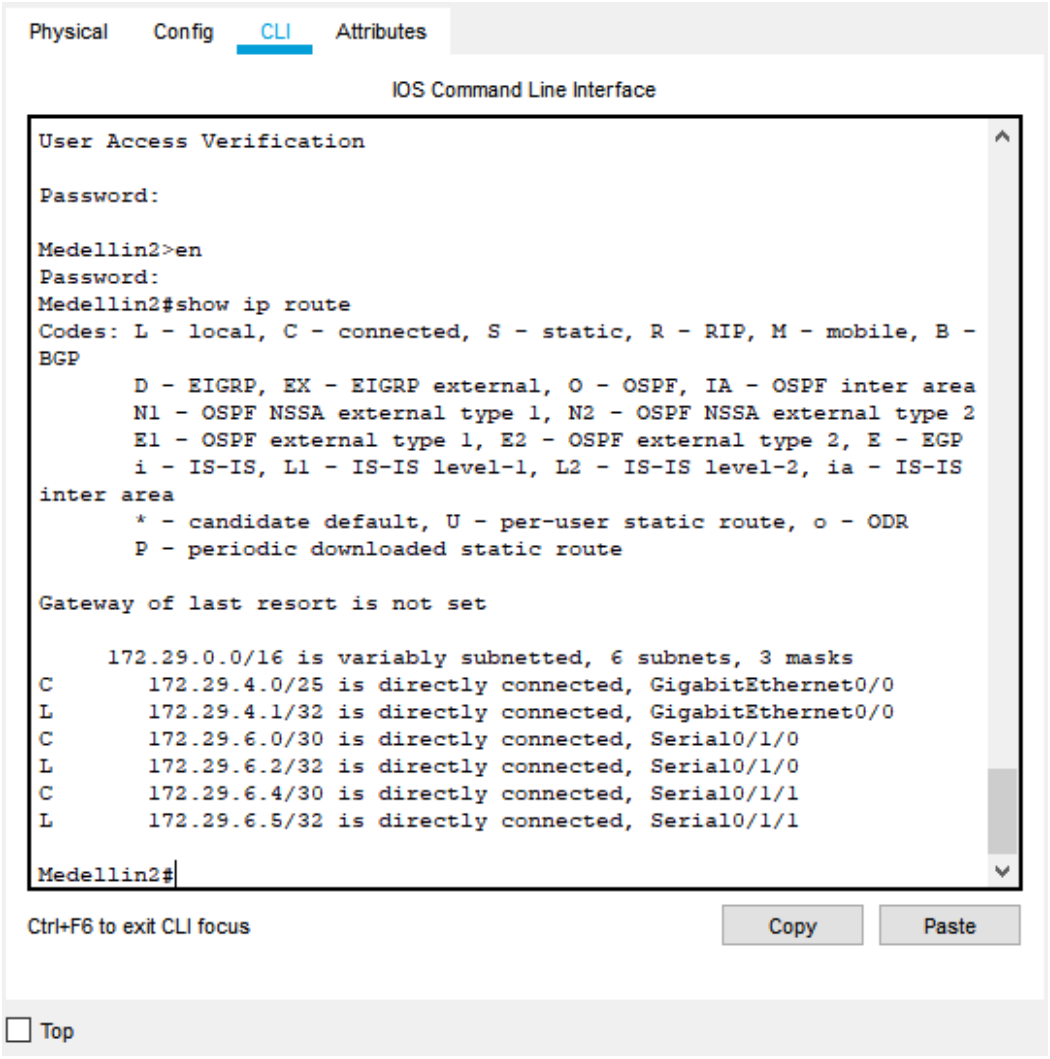
```
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin3(config-router)#passive-interface g0/0
Medellin3(config-router)#

Bogota#confi t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#int s0/0/0
Bogota(config-if)#ip add 209.17.220.6 255.255.255.252
Bogota(config-if)#no shutdown
Bogota(config-if)#int s0/1/0
Bogota(config-if)#ip add 172.29.3.1 255.255.255.252
Bogota(config-if)#no shut
Bogota(config-if)#int s0/0/1
Bogota(config-if)#ip add 172.29.3.9 255.255.255.252
Bogota(config-if)#no shut down
Bogota(config-if)#exit
Bogota(config)#router ospf 4
Bogota(config-router)#router-id 4.4.4.4
Bogota(config-router)#network 172.29.3.0 0.0.0.3 area 1
Bogota(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota(config-router)#passive-interface s0/0/0

Bogota2>en
Password:
Bogota2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#int s0/1/1
Bogota2(config-if)#ip add 172.29.3.10 255.255.255.252
Bogota2(config-if)#no shut
Bogota2(config-if)#int s0/1/0
Bogota2(config-if)#ip add 172.29.3.13 255.255.255.252
Bogota2(config-if)#clock rate 4000000
Bogota2(config-if)#no shut
Bogota2(config-if)#int g0/0
Bogota2(config-if)#ip add 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shut
Bogota2(config-if)#exit
Bogota2(config)#router ospf 4
Bogota2(config-router)#router-id 5.5.5.5
Bogota2(config-router)#network 172.29.1.0 0.0.0.3 area 0
Bogota2(config-router)#no network 172.29.1.0 0.0.0.3 area 0
```

```
Bogota2(config-router)#network 172.29.1.0 0.0.0.3 area 1
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 1
Bogota2(config-router)#passive-interface g0/0


Bogota3(config-if)#int s0/1/1
Bogota3(config-if)#ip add 172.29.3.6 255.255.255.252
Bogota3(config-if)#no shut
Bogota3(config-if)#int g0/0
Bogota3(config-if)#int g0/0
Bogota3(config-if)#ip add 172.29.0.1 255.255.255.0
Bogota3(config-if)#no shut
Bogota3(config-if)#
Bogota3(config-if)#exit
Bogota3(config)#router ospf 5
Bogota3(config-router)#router-id 5.5.5.5
Bogota3(config-router)#network 172.29.0.0 0.0.0.5 area 1
Bogota3(config-router)#network 172.29.0.0 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.29.12 0.0.0.3 area 1
Bogota3(config-router)#
```

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.

```
Medellin(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Medellin(config)#router rip
Medellin(config-router)#default-information originate
```

Figura 21 show ip router



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.

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

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 22. Verificación route en Medellin1

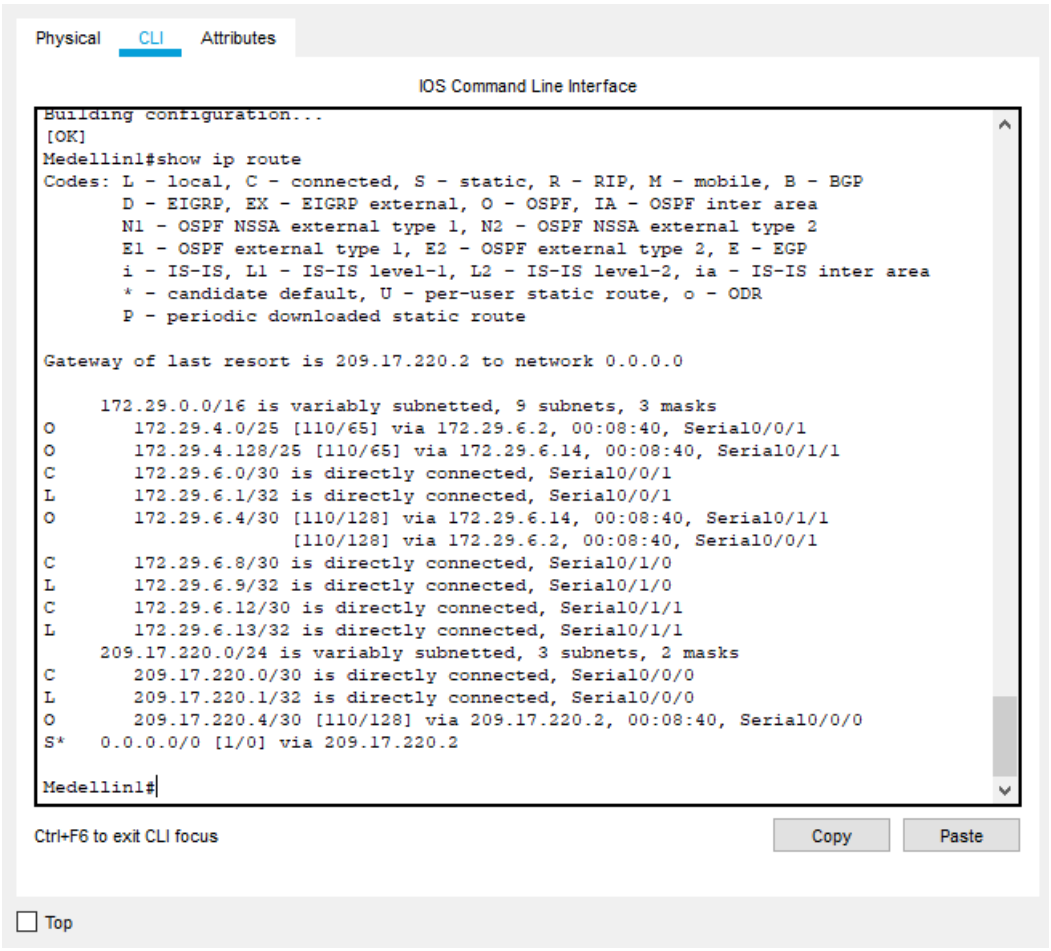


Figura 23 verificación route Medellin2

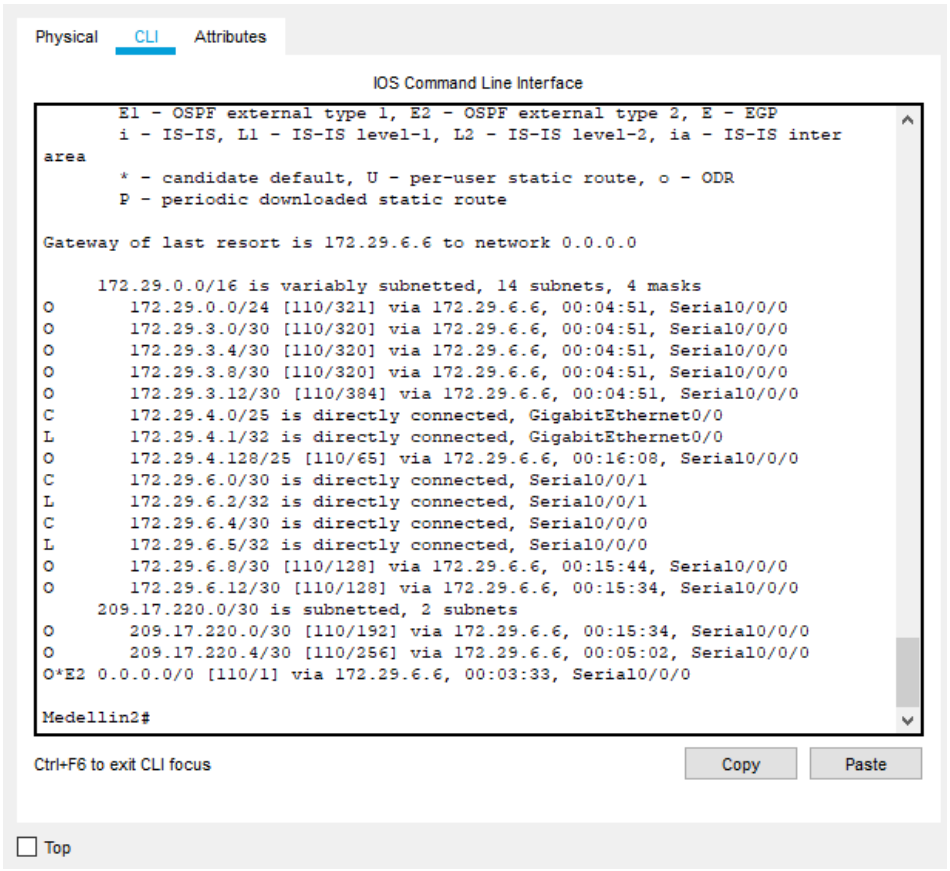


Figura 24. Verificación route Medellin3

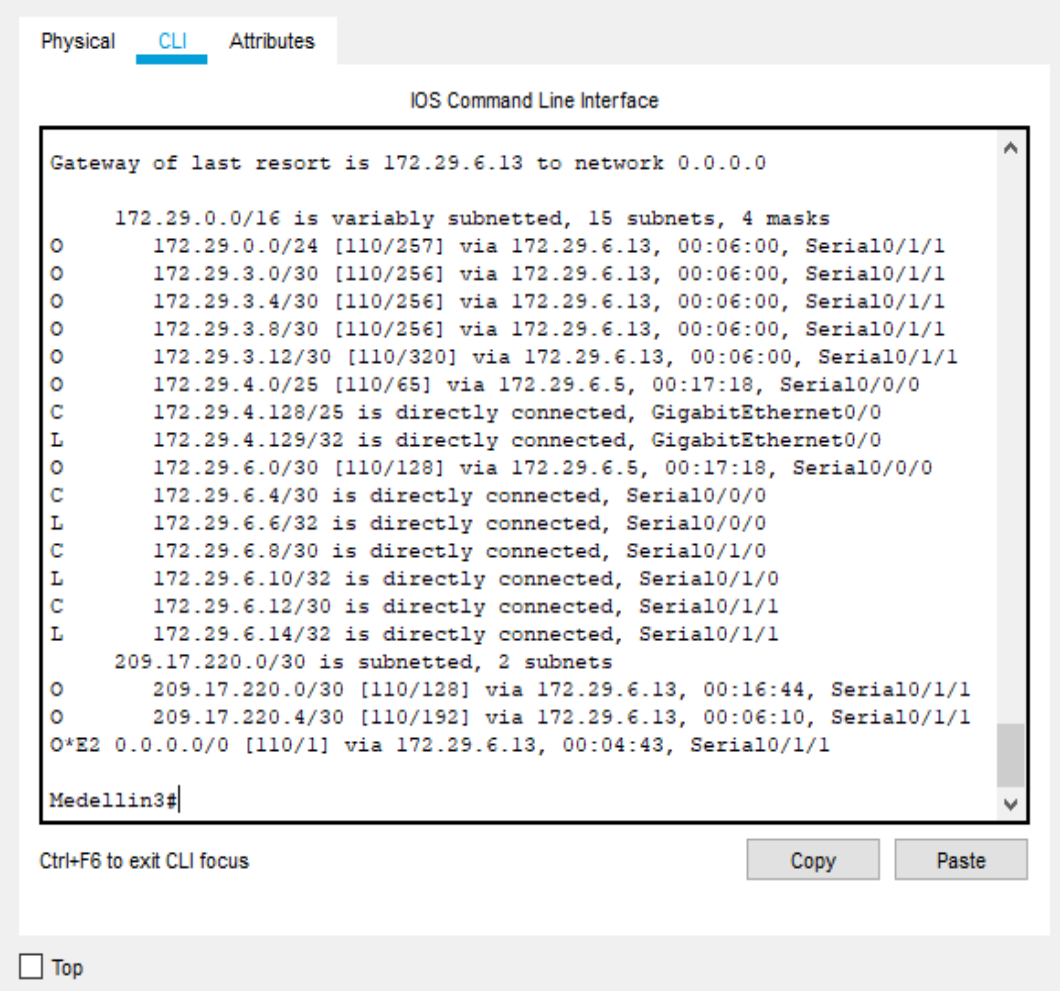


Figura 25. Verificación route ISP

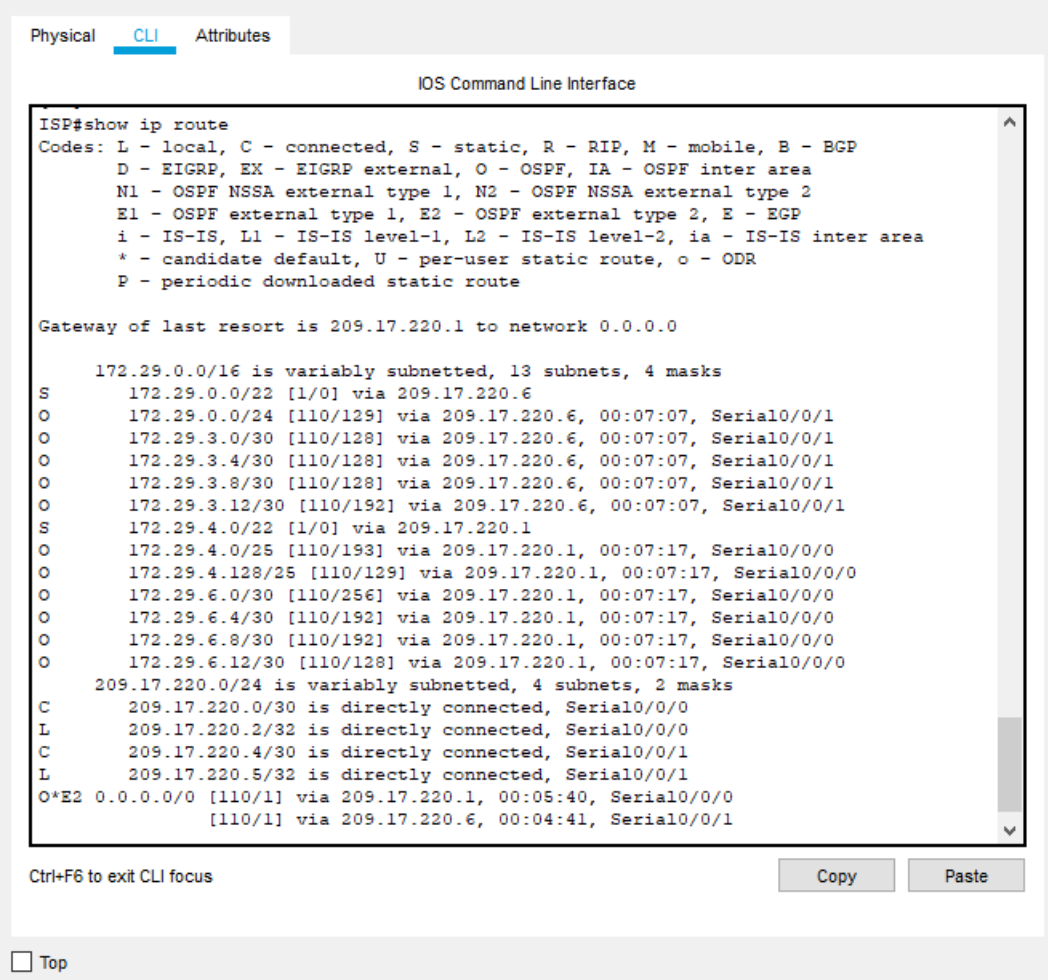


Figura 26. Verificación route Bogota1

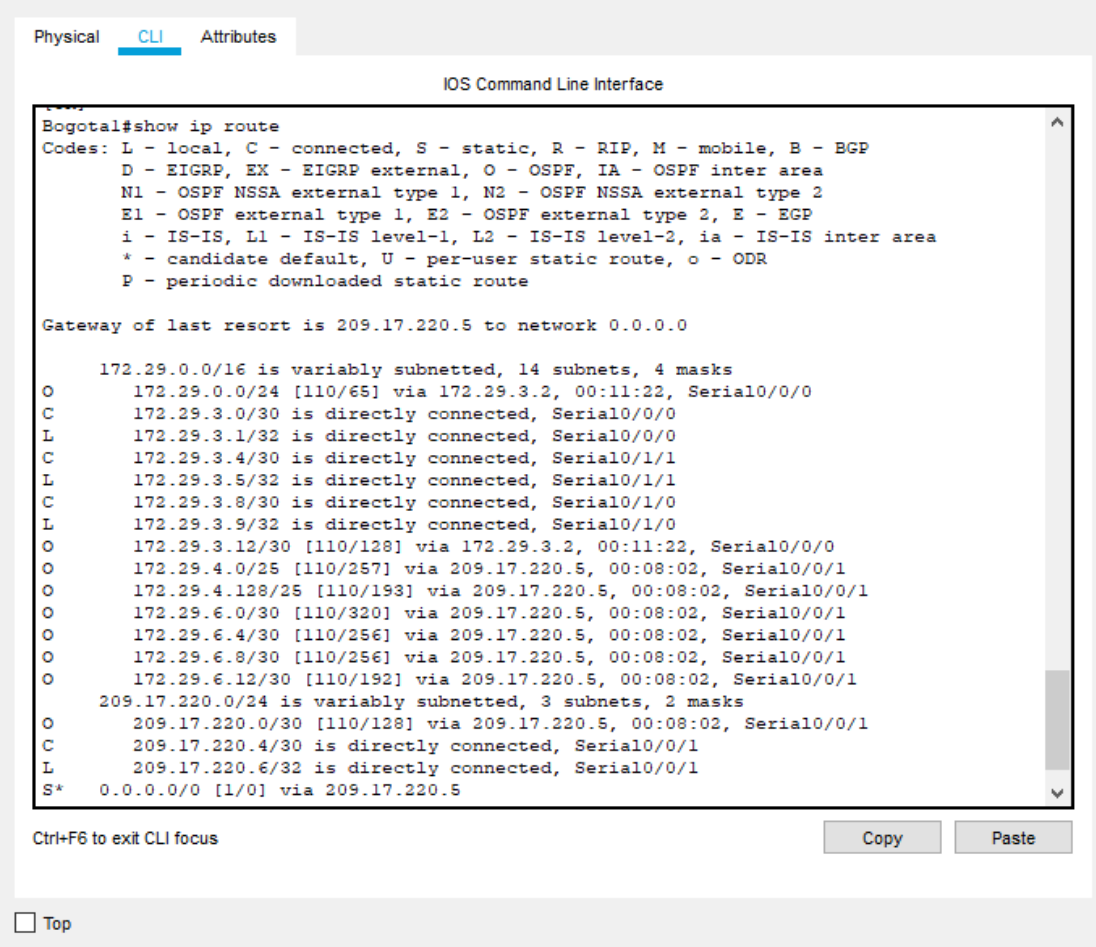


Figura 27. Verificación route Bogota2

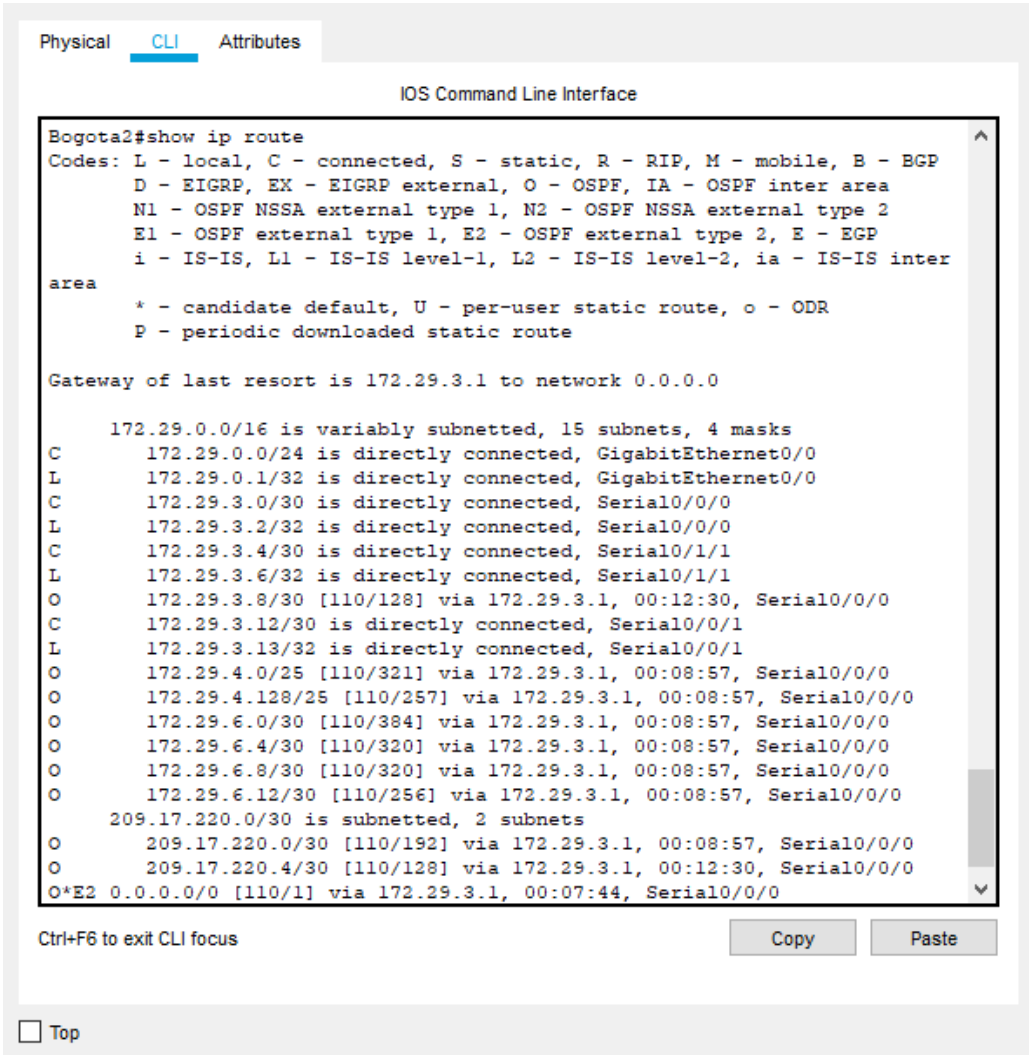
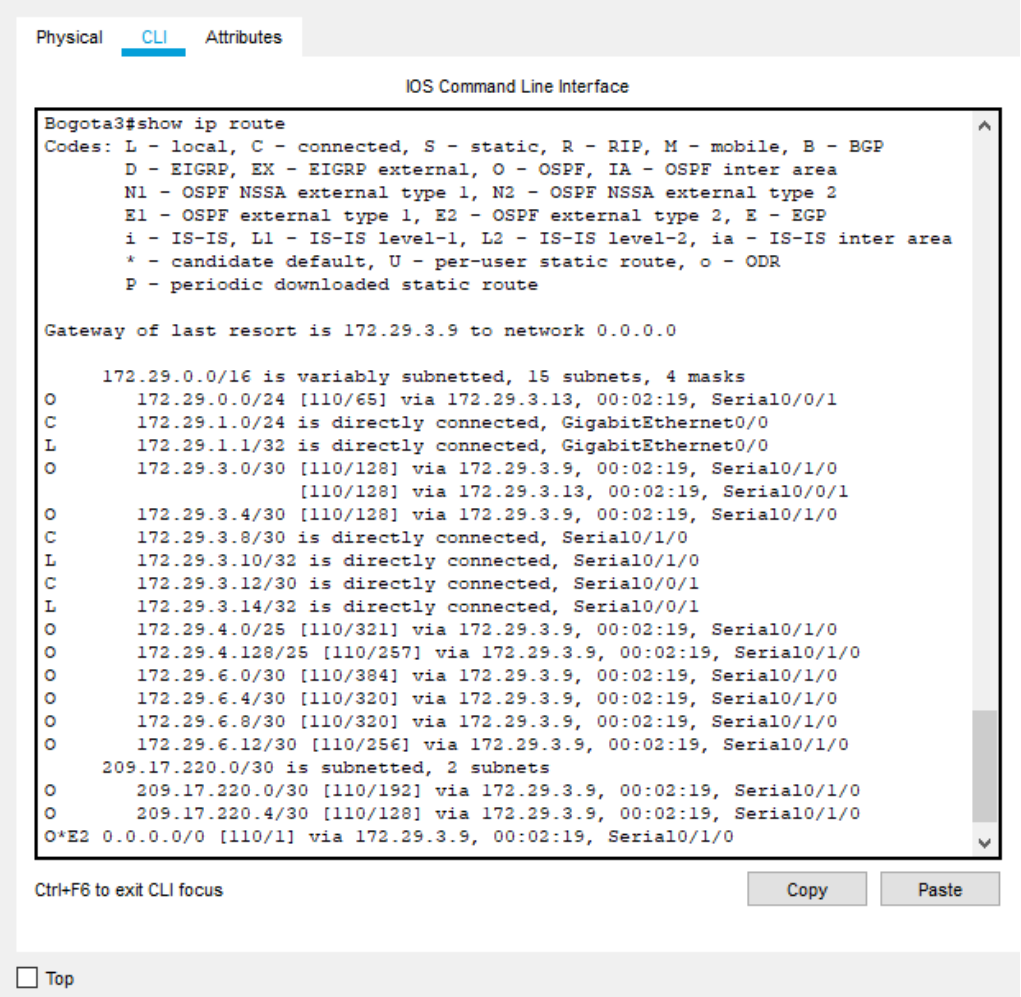


Figura 28. Verificación route Bogota3



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

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(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 29. Verificación protocolos Medellin1

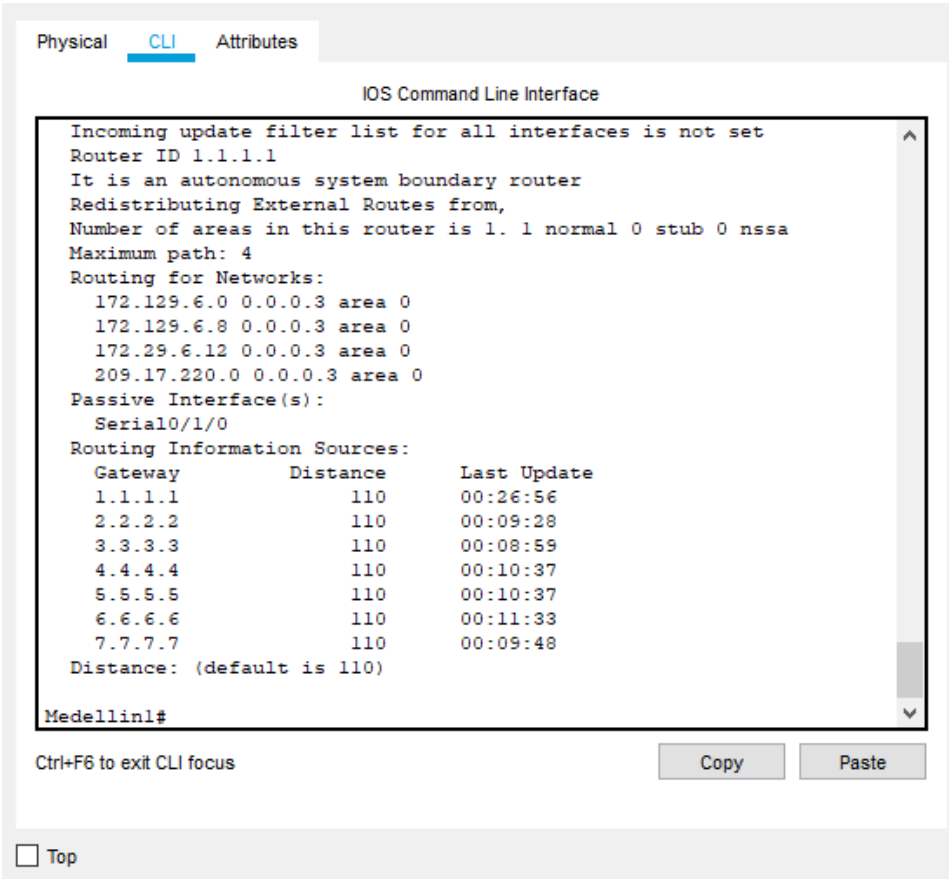


Figura 30. Verificación protocolos Medellin2

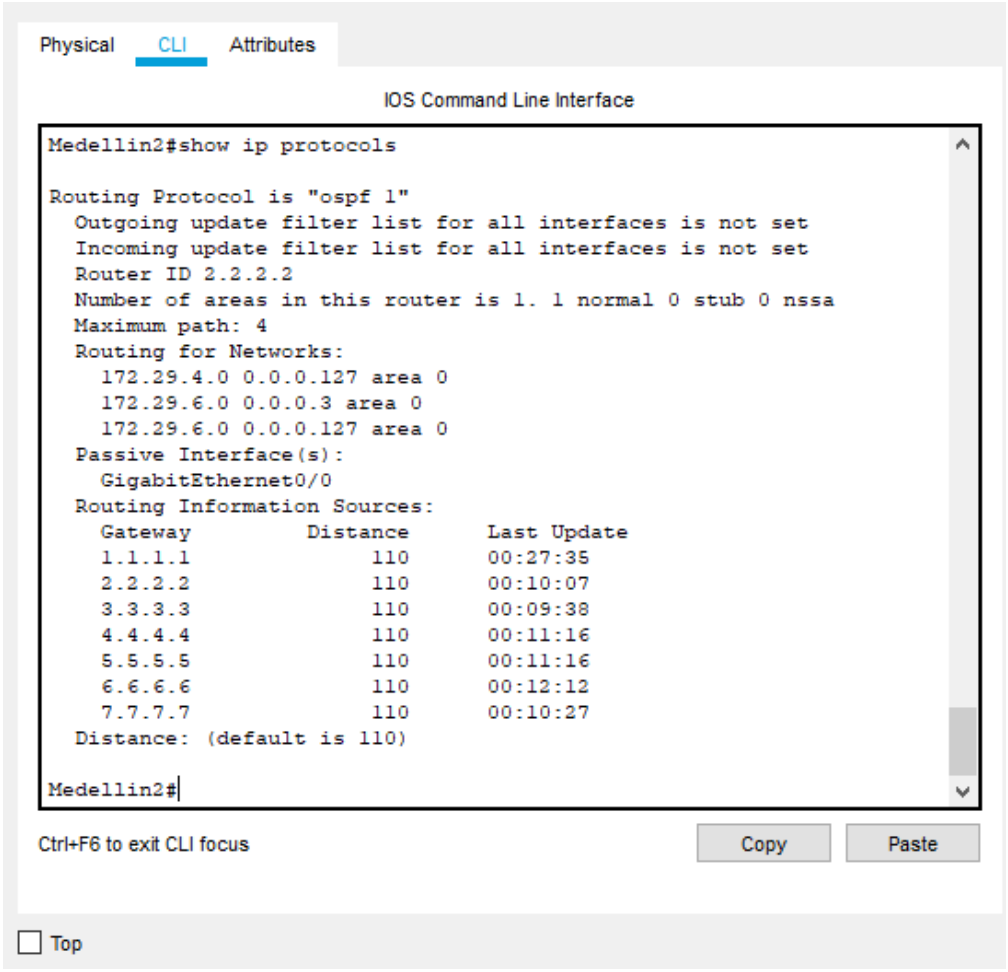


Figura 31. Verificación protocolos Medellin3

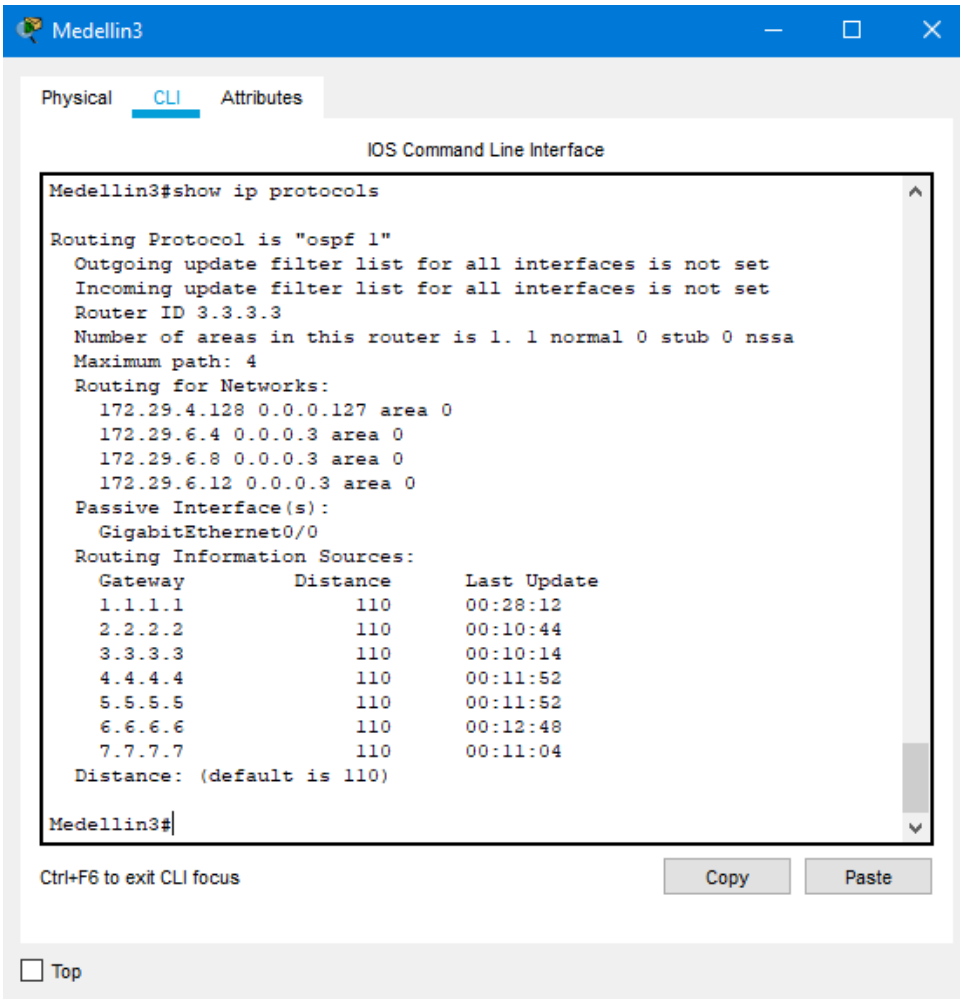

Medellin3
Physical
CLI
Attributes
IOS Command Line Interface
Medellin3#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.4.128 0.0.0.127 area 0
172.29.6.4 0.0.0.3 area 0
172.29.6.8 0.0.0.3 area 0
172.29.6.12 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:28:12
2.2.2.2 110 00:10:44
3.3.3.3 110 00:10:14
4.4.4.4 110 00:11:52
5.5.5.5 110 00:11:52
6.6.6.6 110 00:12:48
7.7.7.7 110 00:11:04
Distance: (default is 110)
Medellin3#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

Figura 32. Verificación protocolos ISP

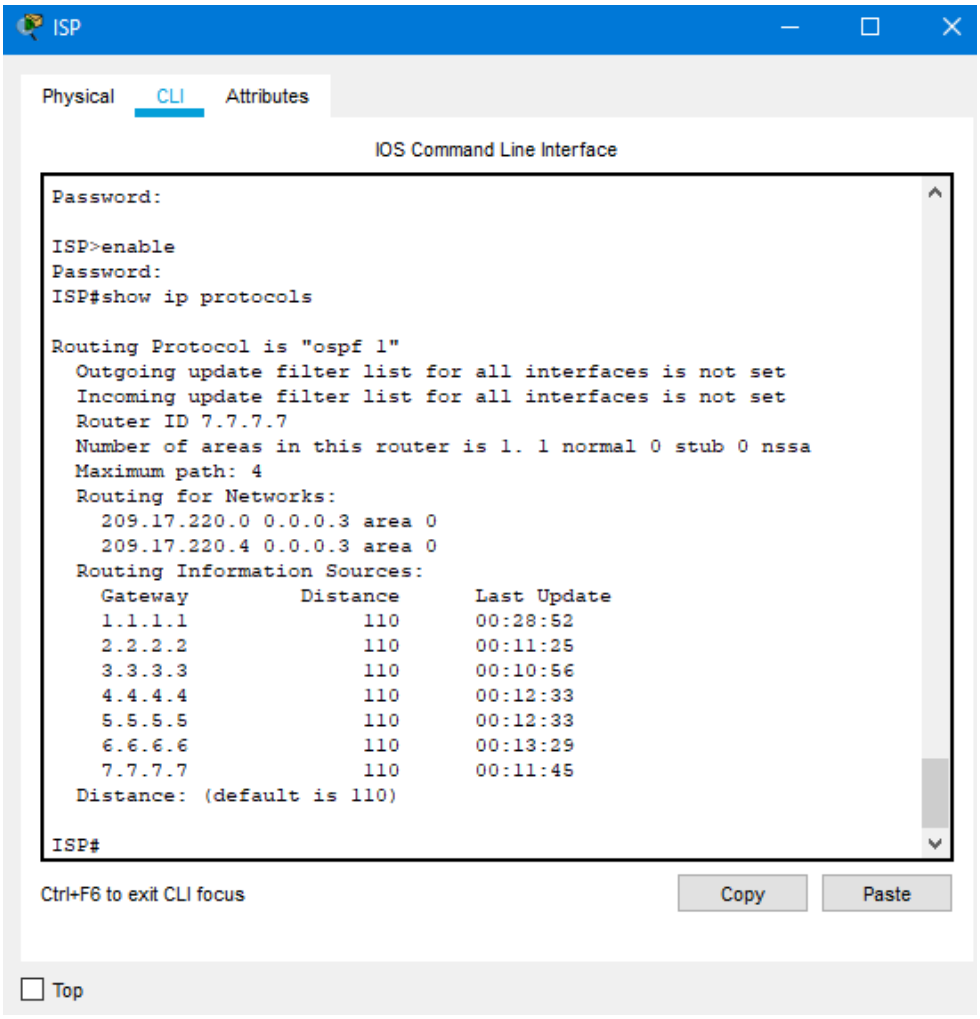


Figura 33. Verificación protocolos Bogota1

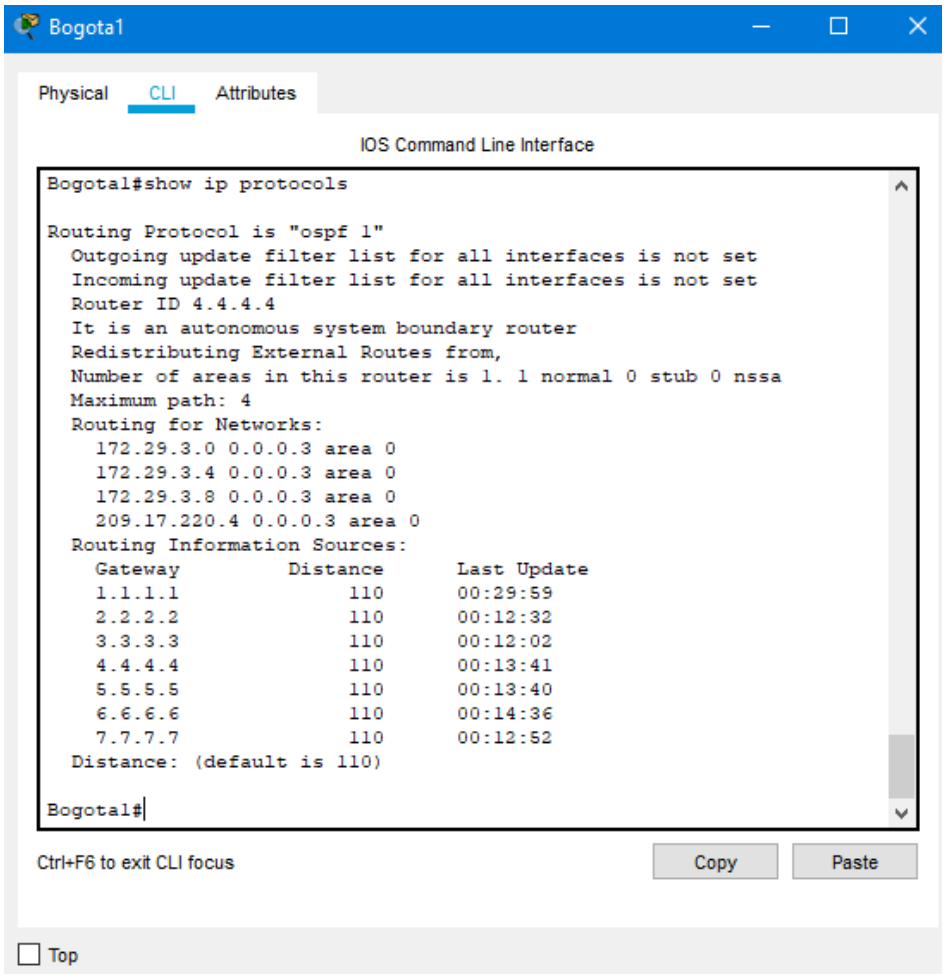


Figura 34. Verificación protocolos Bogota2

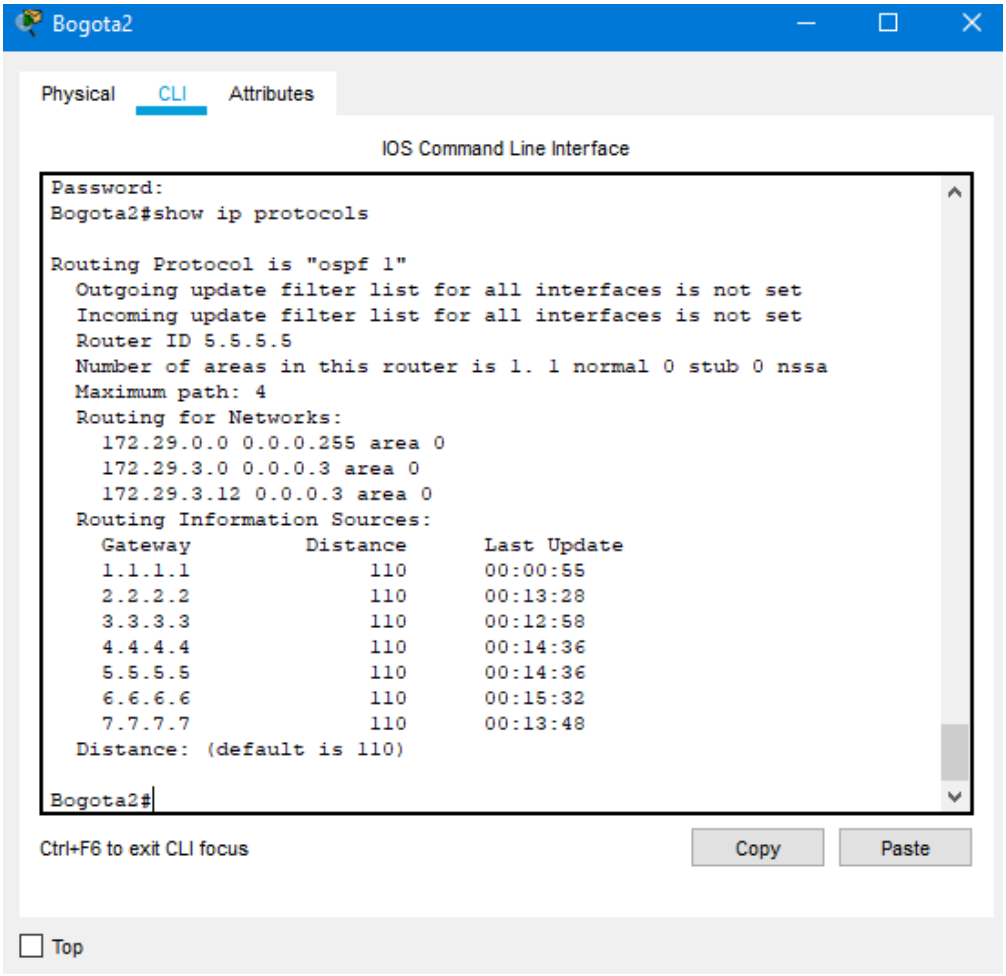
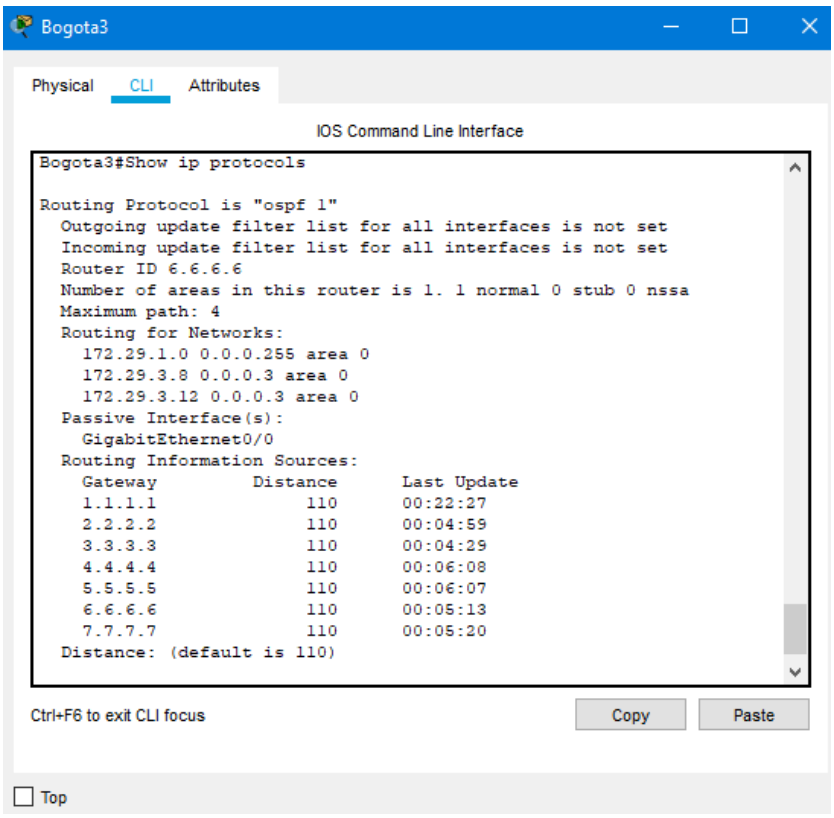


Figura 35. Verificación protocolos Bogota3



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.

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

ISP(config)#username MEDELLIN password cisco
ISP(config)#in s0/1/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco

Medellin(config)#username ISP password cisco
Medellin(config)#int s0/0/1
Medellin(config-if)#encapsulation ppp
Medellin(config-if)#ppp authentication pap
Medellin(config-if)#ppp pap sent-username Medellin1 password cisco

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

```
ISP(config)#username Bogota1 password cisco
ISP(config)#int s0/1/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#
ISP(config-if)#ppp authentication chap
ISP(config-if)
```

```
Bogota(config)#username ISP password cisco
Bogota(config)#int s0/0/0
Bogota(config-if)#encapsulation ppp
Bogota(config-if)#ppp authentication chap
```

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.

```
Medellin#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#ip nat inside source list 1 interface s0/0/1 overload
Medellin(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin(config)#int s0/0/1
Medellin(config-if)#ip nat outside
Medellin(config-if)#int s0/0/0
Medellin(config-if)#ip nat inside
Medellin(config-if)#int s0/1/1
Medellin(config-if)#ip nat inside
Medellin(config-if)#int s0/1/0
Medellin(config-if)#ip nat inside
```

```
Bogota(config)#ip nat inside source list 1 interface s0/0/0 overload
Bogota(config)#access-list 1 permit 172.29.0.0 0.0.3.255
Bogota(config)#int s0/0/0
```

```
Bogota(config-if)#ip nat outside
Bogota(config-if)#int s0/1/0
Bogota(config-if)#ip nat inside
Bogota(config-if)#int s0/0/1
Bogota(config-if)#ip nat inside
Bogota(config-if)#int s0/1/1
Bogota(config-if)#ip nat inside
```

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.

```
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 36. Ping Desde Medellin1 a Medellin2 y Medellin3

```
Medellinl#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

Medellinl#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)
```

Figura 37. Ping desde Bogota1 a Bogota2 y Bogota3

```
Bogotal#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)

Bogotal#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

Bogotal#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 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(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
```

Figura 38. Verificación Dhcp PC-A

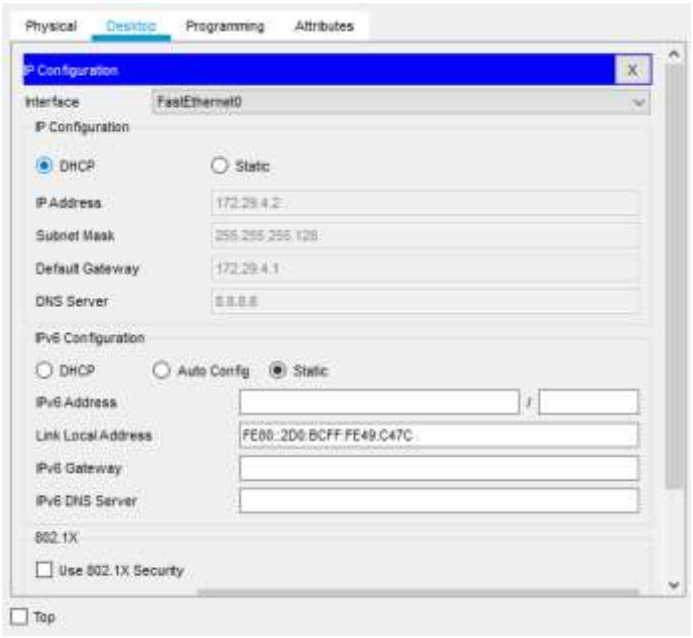
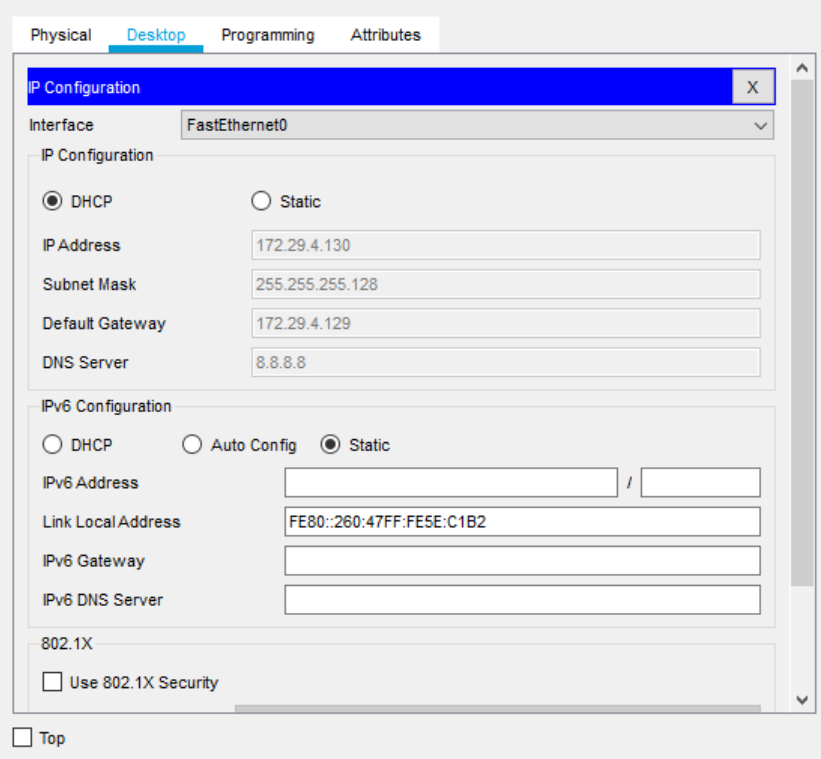


Figura 39. Verificación Dhcp PC-B



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

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-addres para atrapar los broadcasts y redireccionarlos hacia la IP del router de bogota2

Figura 40 Verificación Dhcp PC-C

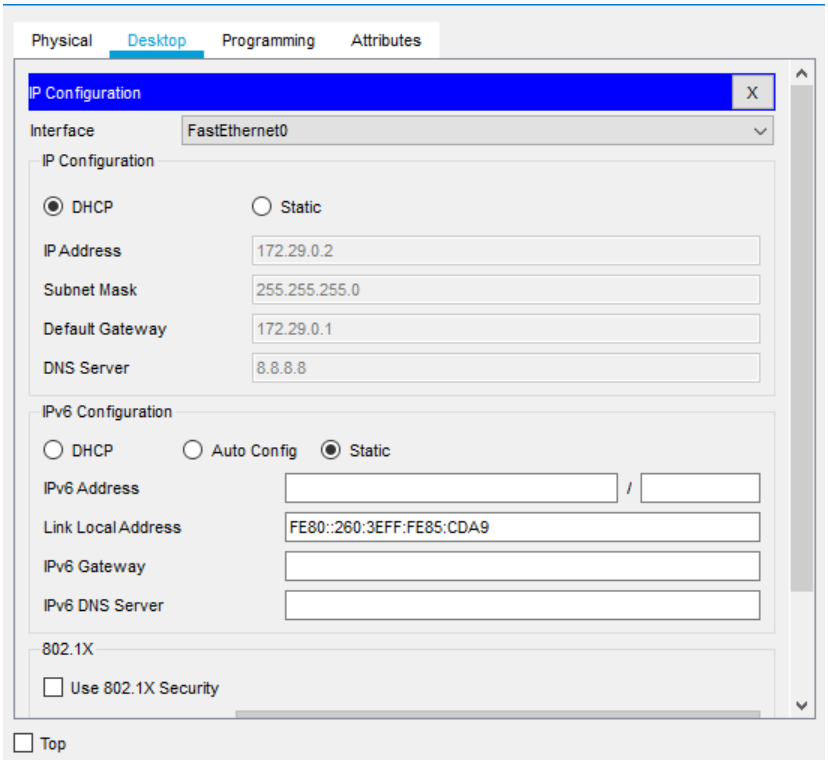
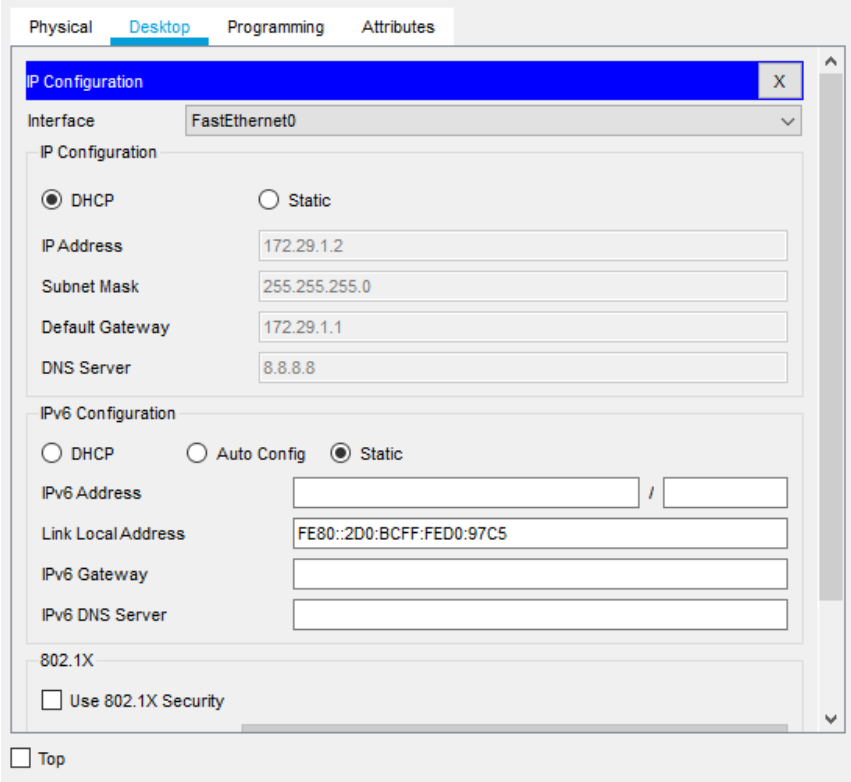


Figura 41. Verificación Dhcp PC-D



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]

CONCLUSIONES

Con el desarrollo de los escenarios se implementó la configuracion necesaria para activar la vlan en los switches y ai poder configurar un router como servidor Dhcp, haciendo el direccionamiento ip automático.

Se establecieron las conexiones e interfaces necesarias para obtener conexión entre todos los dispositivos de la red, por medio de direccionamiento IPV4 e IPV6.

Para configurar correctamente es de vital importancia establecer orden en la red, teniendo presente como se va a trabajar el direccionamiento de cada ruta, la interfaz y el tipo de conexión de cada puerto.

Aplicar configuración ppp, permite tener mayor seguridad en la red, no cualquier persona podría manipularla.

Para el desarrollo del según escenario fue necesario implementar OSPF, DHCP por medio de Router implementando NAT, PAT, PPP, PAP y CHAP; para las redes de Medellín y Bogotá, para ser conectadas hacia ISP

Aplicar dhcp en las redes sobre todo en el segundo escenario centraliza la información y así no habrá choque de direcciones en ninguna sucursal, teniendo presente que en cada router se realizó la exclusión de las direcciones ya asignadas.

BIBLIOGRAFÍA

Eugenio Duarte, E. D. (2016, 13 abril). Cisco CCNA – Cómo Configurar DHCP En Cisco Router. Recuperado de http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurardhcp-en-cisco-router/

Colaboradores de Wikipedia. (2019b, 30 abril). Máscara de red - Wikipedia, la enciclopedia libre. Recuperado de https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

Conmutador (dispositivo de red). (2020). Retrieved 27 May 2020, from https://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red

Router. (2020). Retrieved 27 May 2020, from https://es.wikipedia.org/wiki/Router

Temática: Enrutamiento Dinámico
CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static- courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Temática: OSPF de una sola área
CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static- courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

Temática: Listas de control de acceso
CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static- courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

Temática: DHCP
CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static- courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Temática: Traducción de direcciones IP para IPv4
CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static- courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1