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

HUMBERTO NIAMPIRA RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA DE SISTEMAS
BOGOTÁ D.C.
2020

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

HUMBERTO NIAMPIRA RODRIGUEZ

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

TUTOR
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA DE SISTEMAS
BOGOTÁ D.C.
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C. 15 de mayo de 2020

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

1. INTRODUCCIÓN

El presente trabajo es desarrollado y presentado como opción de grado para optar el título de ingeniero de sistemas, denominado como diplomado de profundización en diseño e implementación de soluciones integradas LAN/WAN el cual en su contenido compone los módulos Network Fundamentals (CCNA1 R&S) y Routing and Switching Fundamentals (CCNA2 R&S), dicho diplomado sumerge al estudiante en el aprendizaje de conceptos de redes empresariales así como la práctica y solución de problemas en infraestructura en una red convergente.

Su desarrollo se presenta bajo dos escenarios que busca como objetivos solucionar y/o resolver la configuración de redes pequeñas empresariales, en dispositivos como router, switches, servidores y computadores. Se pondrá en práctica la configuración en temas como: el direccionamiento IP que permita conectividad en IPv4 e IPv6, la configuración de parámetros básicos de dispositivos y temas de seguridad de Router, Switchs y PC. Implementación básica de protocolos de routing OSPF versión 2 para la propagación de rutas predeterminadas.

Así como la implementación básica de protocolos de routing RIP versión 2, implementación de servicios DHCP y NAT para IPv4. De igual manera se pone en práctica lo aprendido en la configuración de encapsulamiento y autenticación PPP, que busca obtener seguridad en el enlace de dos sedes a través de autenticación PAT como también la autenticación tipo CHAT.

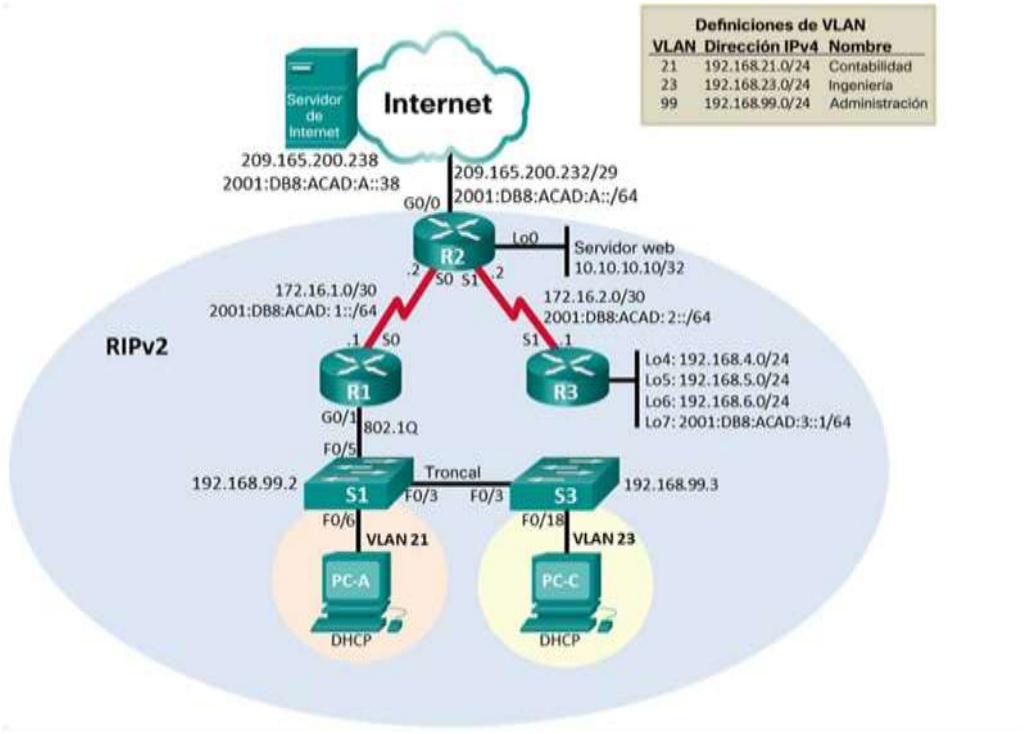
Lo anterior se trabajará realizando el diseño de tipologías de red, apoyados en la herramienta de aprendizaje y simulación Packet Tracer de Cisco

2. DESARROLLO DEL PROYECTO

6.1 DESARROLLO ESCENARIO 1

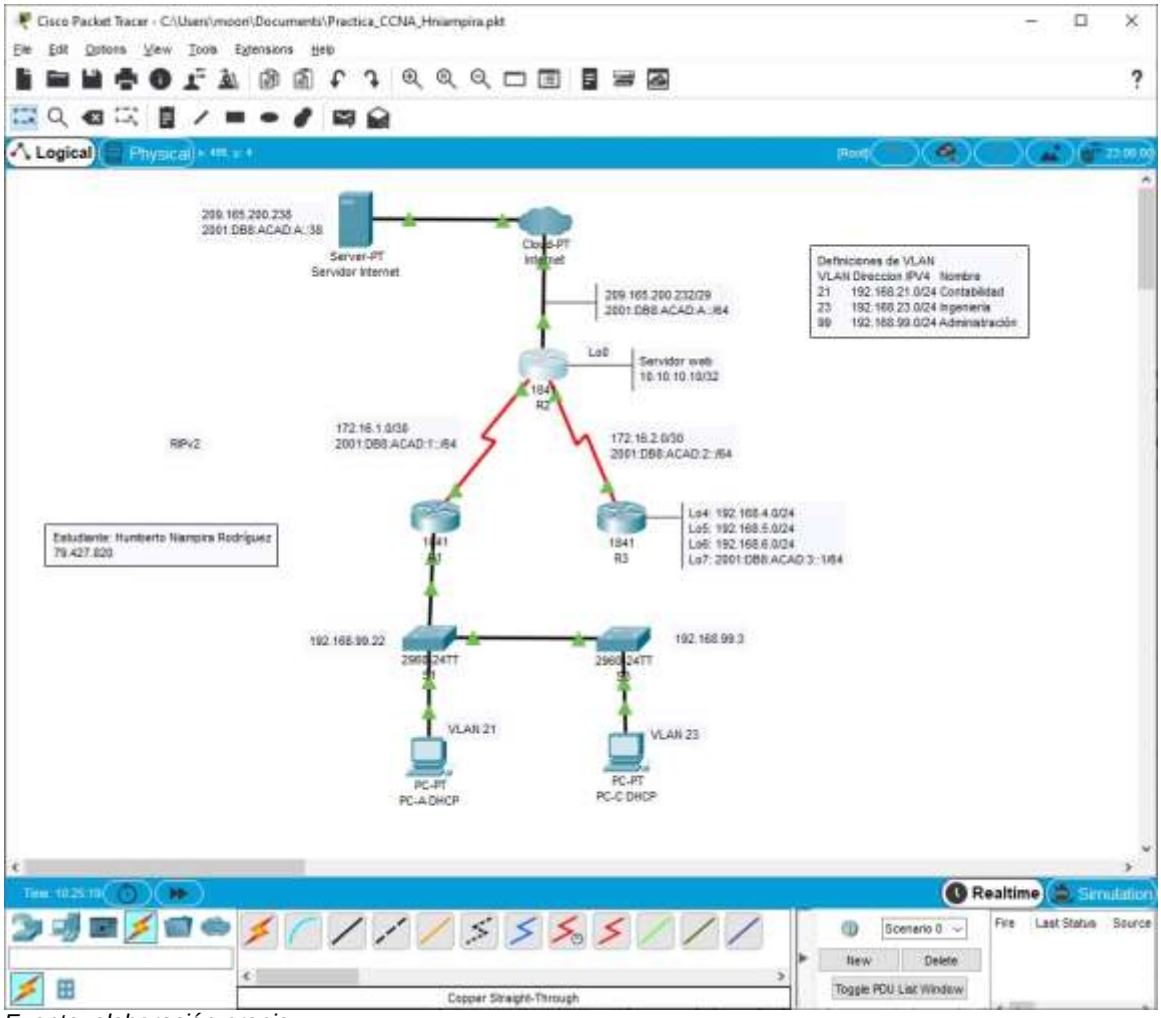
Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de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

Figura 1. Topología de red propuesto para el escenario 1



Fuente: guía Prueba de habilidades CCNA.

Figura 2. Topología de red desarrollado para el escenario 1



Fuente: elaboración propia

6.1.1 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.

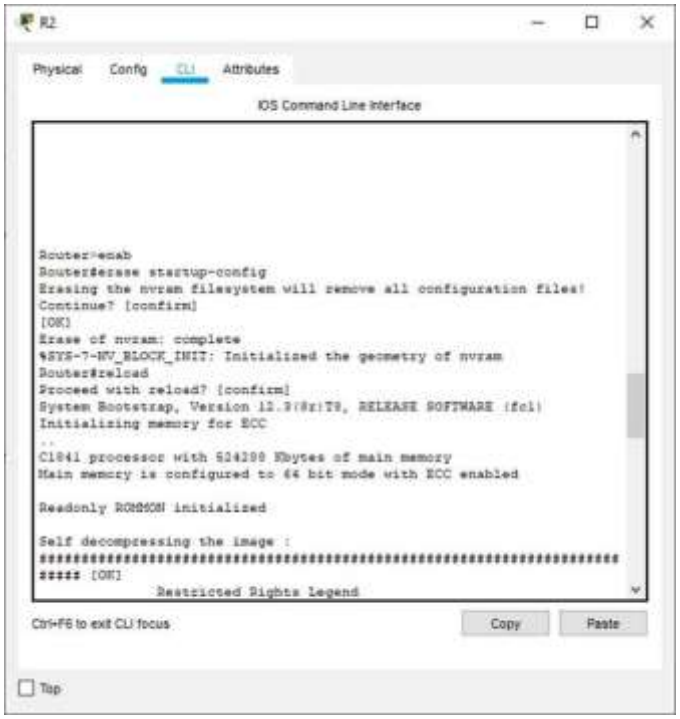
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 1. Comandos IOS Etapa 1. Inicializar dispositivos routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Erase startup-config Delete vlan.dat
Volver a cargar ambos switches	reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Show vlan brief

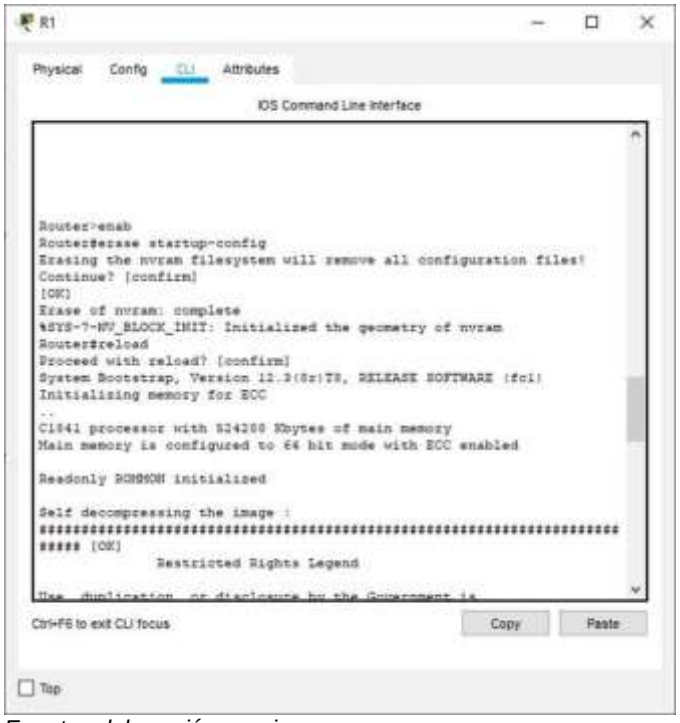
Fuente: guía Prueba de habilidades CCNA

Figura 3. Eliminado configuraciones e inicio R2



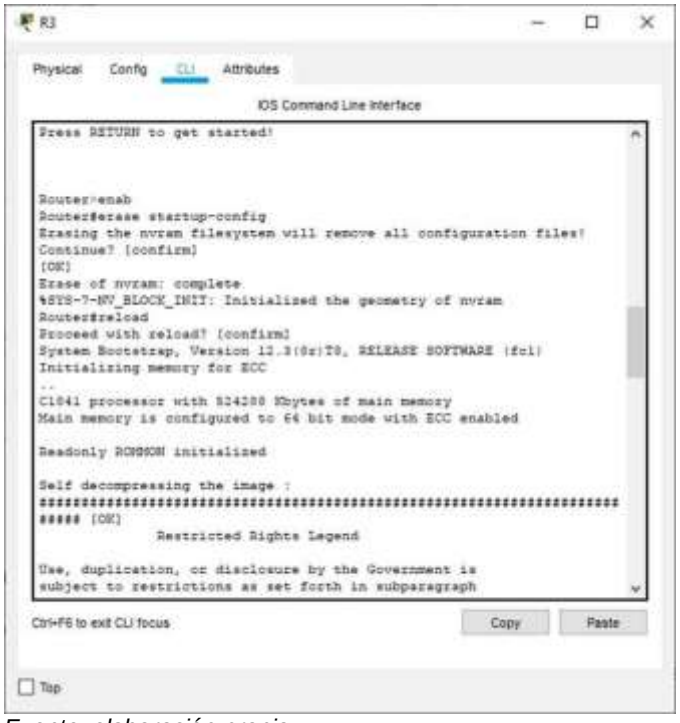
Fuente: elaboración propia

Figura 4. Eliminado configuraciones e inicio R1



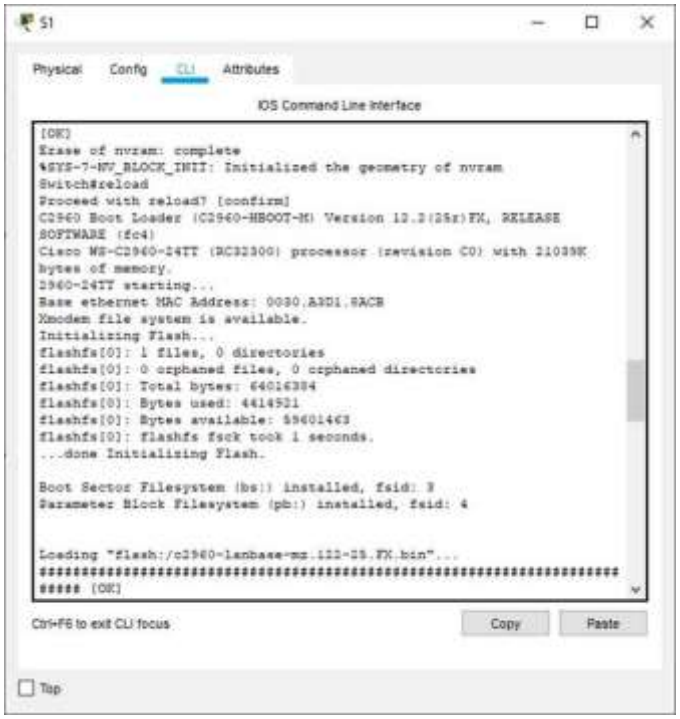
Fuente: elaboración propia

Figura 5. Eliminado configuraciones e inicio R3



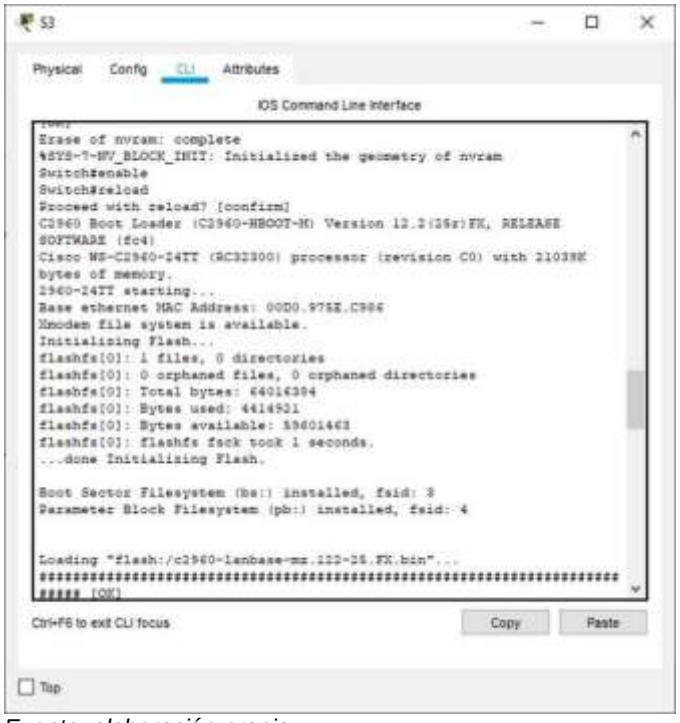
Fuente: elaboración propia

Figura 6. Eliminado configuraciones e inicio S1



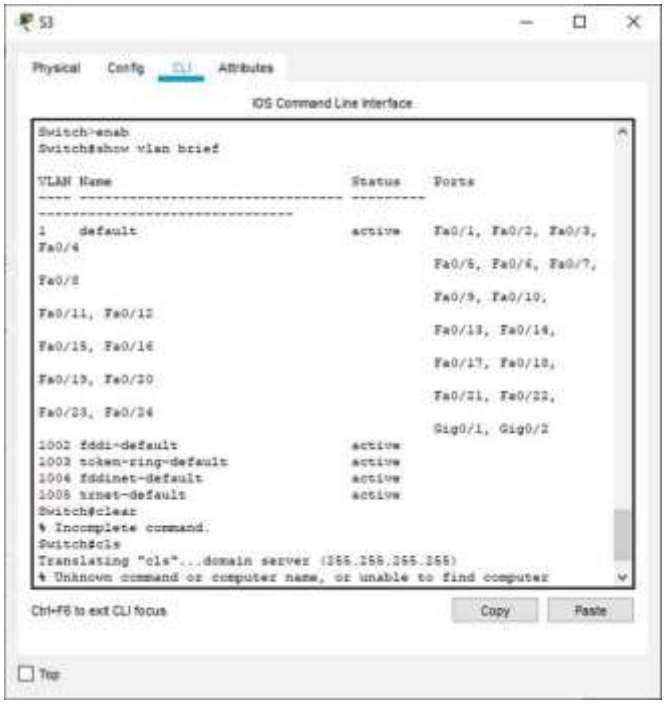
Fuente: elaboración propia

Figura 7. Eliminado configuraciones e inicio S3



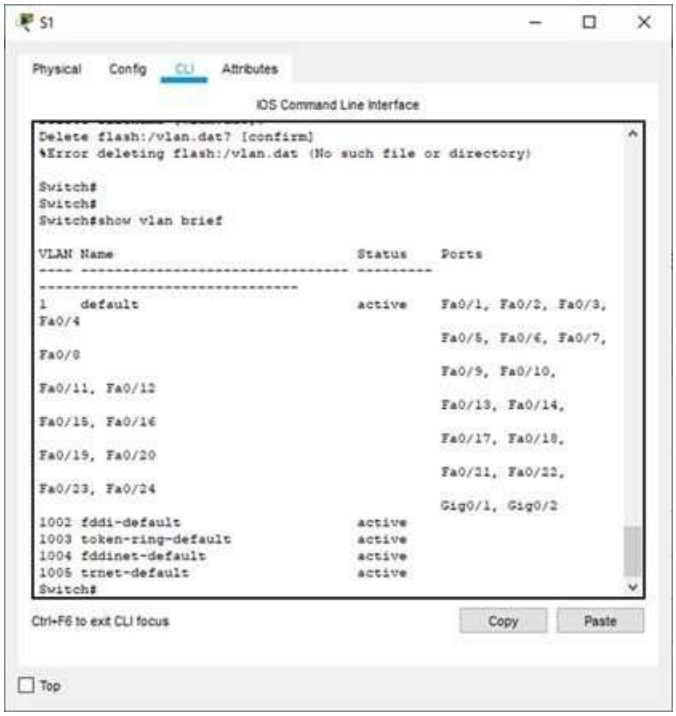
Fuente: elaboración propia

Figura 8. Verificación de la base de datos de VLAN de la memoria flash S3



Fuente: elaboración propia

Figura 9. Verificación de la base de datos de VLAN de la memoria flash S1



Fuente: elaboración propia

6.1.2 Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

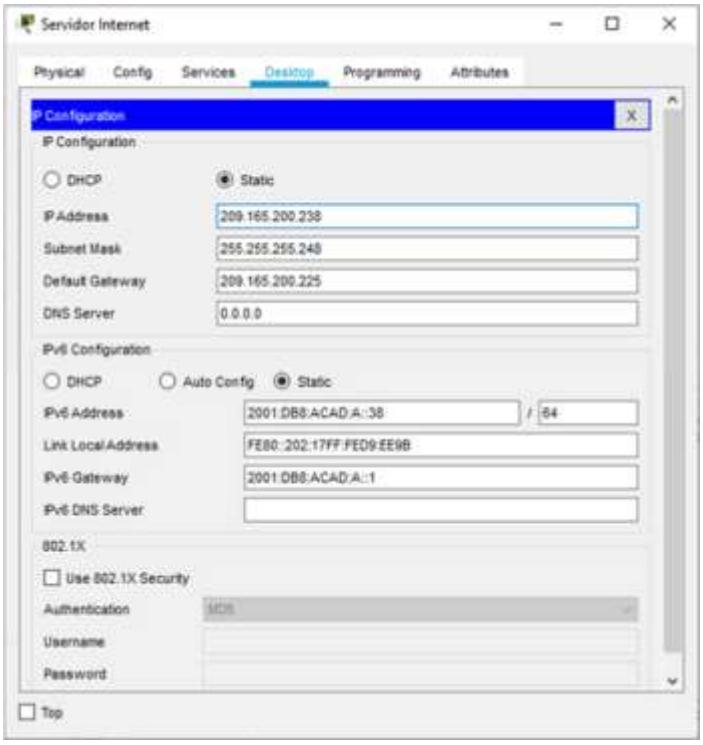
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 2. Datos de configuración servidor de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: guía Prueba de habilidades CCNA

Figura 10. Configuración básica para servidor internet



Fuente: elaboración propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Datos de configuración para el router R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/1/0	Establezca la descripción: description R1-R2 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
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/1/0 Configurar una ruta IPv6 predeterminada de S0/1/0

Fuente: guía Prueba de habilidades CCNA

Código configuración R1

Router>enable

Router#config terminal

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

Router(config) #no ip domain-lookup

Router(config) #hostname R1

R1 (config) #enable secret class

R1 (config) # line console 0

R1 (config-line) #password cisco

R1 (config-line) #login

R1 (config-line) #exit

R1 (config) #line vty 0 15

R1(config-line) #password cisco

R1(config-line) #login

R1(config-line) #exit

R1(config) #service password-encryption

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

R1(config) #int s0/1/0

R1(config-if) #description R1-R2

R1(config-if) #ip address 172.16.1.1 255.255.255. 252

R1(config-if) #ipv6 address 2001:DB8:ACAD:1::1/64

R1(config-if) #clock rate 128000

R1(config-if) #no shutdown

R1(config-if) #exit

R1(config) #ip route 0.0.0.0 0.0.0.0 s0/1/0

R1(config) #ipv6 route ::/0 s0/1/0

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Datos de configuración router R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción: descripción R2-R1 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
Interfaz S0/1/0	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Elemento o tarea de configuración	Especificación
Interfaz f0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback f0/0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de f0/0. Configure una ruta IPv6 predeterminada de f0/0.

Fuente: guía Prueba de habilidades CCNA

Código configuración R2

Router>enable

Router#config terminal

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

Router(config) #no ip domain-lookup

Router(config) #hostname R2

R2 (config) #enable secret class

R2 (config) # line console 0

R2 (config-line) #password cisco

R2 (config-line) #login

R2 (config-line) #exit

R2 (config) #line vty 0 15

R2 (config-line) #password cisco

R2 (config-line) #login

R2 (config-line) #exit

R2 (config) #service password-encryption

R2 (config) #banner motd # Se prohíbe el acceso no autorizado#

R2 (config)#ip http server

R2 (config) #int s0/0/0

R2 (config-if) #description R2-R1

R2 (config-if) #ip address 172.16.1.2 255.255.255.252

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

R2 (config-if) #no shutdown

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

R2 (config-if)#description R2-R3

R2 (config-if)#ip address 172.16.2.2 255.255.255.252

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

R2 (config-if)#clock rate 128000

R2 (config-if)#no shutdown

R2 (config-if)#int f0/0

R2 (config-if)#description R2-Internet

R2 (config-if)#ip address 209.165.200.225 255.255.255.248

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

R2 (config-if)#no shutdown

R2 (config-if)#int loopback 0

R2 (config-if)#ip address 10.10.10.10 255.255.255.255

R2 (config-if)#no shutdown

R2 (config-if)#exit

R2 (config)#ip route 0.0.0.0 0.0.0.0 f0/0

R1(config) #ipv6 route ::/0 f0/0

R2 (config)#

Paso 4. Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Datos de configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	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
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Fuente: guía Prueba de habilidades CCNA

Código configuración R3

```
Router>en
Router#config t
Router (config)#no ip domain-lookup
Router (config)#hostname R3
R3 (config)#enable secret class
R3 (config)#line console 0
R3 (config-line)#password cisco
R3 (config-line)#login
R3 (config-line)#exit
R3 (config)#line vty 0 15
R3 (config-line)#password cisco
R3 (config-line)#login
R3 (config-line)#exit
R3 (config)#service password-encryption
R3 (config)#banner motd # Se prohíbe el acceso no autorizado #
R3 (config)#int s0/0/0
R3 (config-if)#description R3-R2
R3 (config-if)#ip address 172.16.2.2 255.255.255.252
R3 (config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3 (config-if)#no shutdown
R3 (config-if)#int lo4
R3 (config-if)#ip add 192.168.4.1 255.255.255.0
R3 (config-if)#no shutdown
R3 (config-if)#int lo5
R3 (config-if)#ip add 192.168.5.1 255.255.255.0
R3 (config-if)#no shutdown
R3 (config-if)#int lo6
```

R3 (config-if)#ip add 192.168.6.1 255.255.255.0

R3 (config-if)#no shutdown

R3 (config-if)#int lo7

R3 (config-if)#ipv6 add 2001:DB8:ACAD:3::1/64

R3 (config-if)#no shutdown

R3 (config-if)#exit

R3 (config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

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

Paso 5. Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Datos de configuracion S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: guía Prueba de habilidades CCNA

Código configuración S1

Switch>en

Switch#config t

Switch(config)#no ip domain-lookup

Switch(config)#hostname S1

S1 (config)#enable secret class

S1 (config)#line console 0

S1 (config-line)#password cisco

S1 (config-line)#login

S1 (config-line)#line vty 0 4

S1 (config-line)#password cisco

S1 (config-line)#login

S1 (config-line)#service password-encryption

S1 (config)#banner motd # Se prohíbe el acceso no autorizado#

S1 (config)#exit

Paso 6. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Datos de configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: guía Prueba de habilidades CCNA

Código configuración S3

Switch>enab

Switch#config t

Switch(config)#no ip domain-lookup

Switch(config)#hostname S3

S3 (config)#enable secret class

S3 (config)#line console 0

S3 (config-line)#password cisco

S3 (config-line)#login

S3 (config-line)#line vty 0 4

S3 (config-line)#password cisco

S3 (config-line)#login

S3 (config-line)#service password-encryption

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

S3 (config)#exit

Paso 7. Verificar la conectividad de la red

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

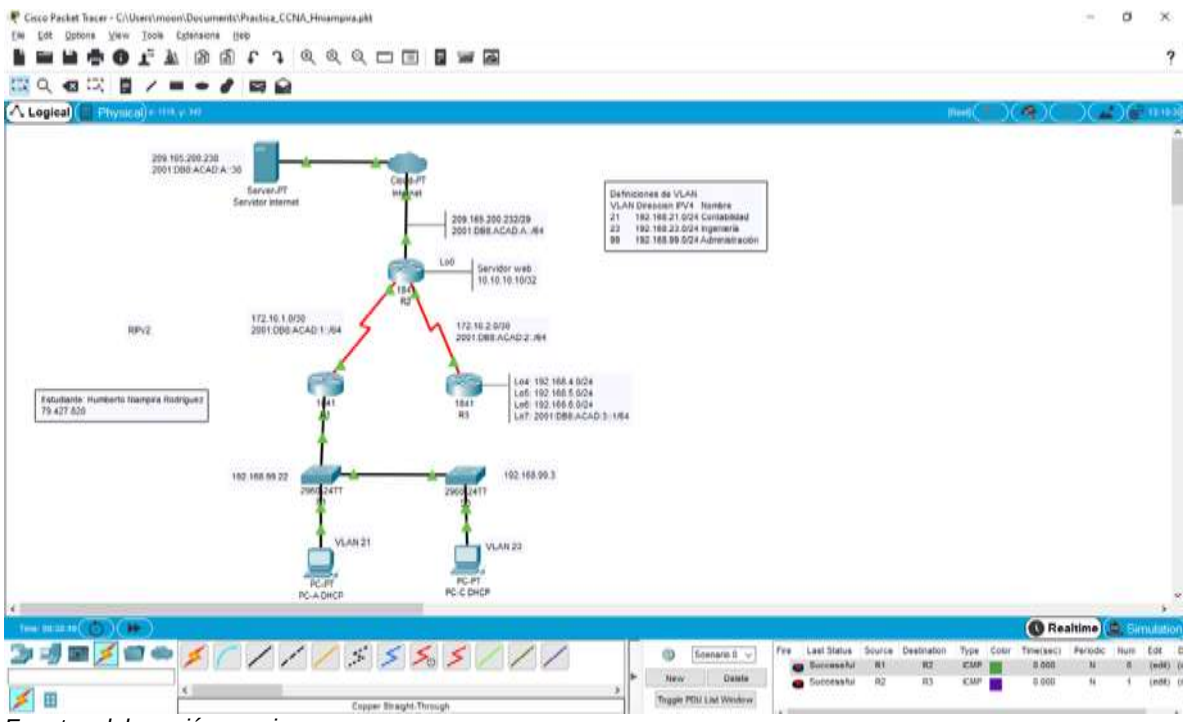
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8. Conectividad entre dispositivos

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success - Éxito
R2	R3, S0/0/0	172.16.2.2	Success - Éxito
PC de Internet	Gateway predeterminado	209.165.200.238	

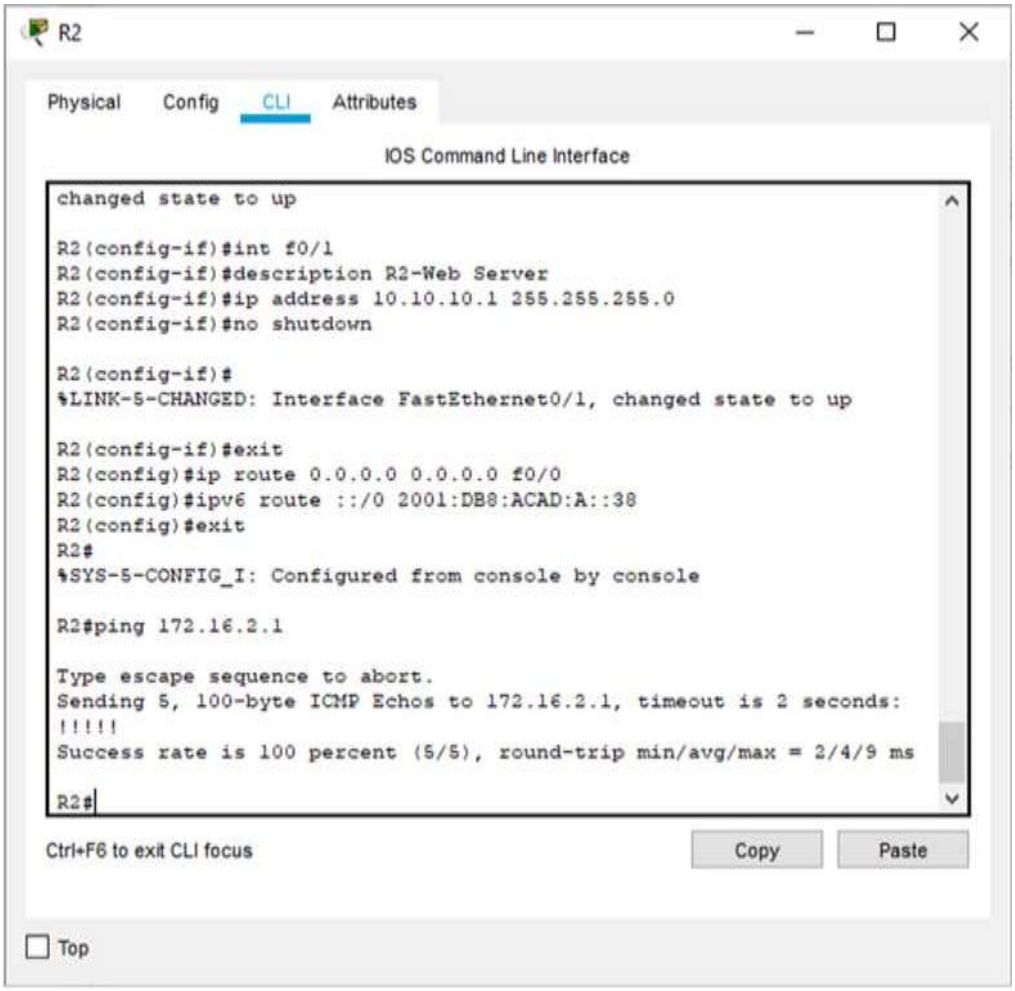
Fuente: guía Prueba de habilidades CCNA

Figura 11. Ping de R1 a R2 y de R2 a R3



Fuente: elaboración propia

Figura 12. Verificación de Ping de R2 a R3



Fuente: elaboración propia

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configuración del switch S1

Elemento o tarea de configuración	Especificación
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
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
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	Switchport Access vlan
Apagar todos los puertos sin usar	shutdown

Fuente: guía Prueba de habilidades CCNA

Código configuración del Switch S1

S1#config t

S1 (config)#vlan 21

S1 (config-vlan)#name Contabilidad

S1 (config-vlan)#vlan 23

S1 (config-vlan)#name Ingenieria

S1 (config-vlan)#vlan 99

S1 (config-vlan)#name Administracion

S1 (config-vlan)#exit

S1 (config)#int vlan 99

S1 (config-if)#ip address 192.168.99.22 255.255.255.0

S1 (config-if)#no shut

S1 (config-if)#exit

S1 (config)#ip default-gateway 192.168.99.1

S1 (config)#int range f0/3, f0/5

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

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

S1 (config-if-range)#int range f0/1-2, f0/4, f0/6-24, g0/1-2

S1 (config-if-range)#switchport mode access

S1 (config-if-range)#int f0/6

S1 (config-if)#switchport access vlan 21

S1 (config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2

S1 (config-if)#shutdown

S1 (config-if)#exit

Paso 2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configuración del switch S3

Elemento o tarea de configuración	Especificación
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.
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
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.

Elemento o tarea de configuración	Especificación
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	
Apagar todos los puertos sin usar	

Fuente: guía Prueba de habilidades CCNA

Código configuración Switch S3

S3#config t

S3 (config)#vlan 21

S3 (config-vlan)#name Contabilidad

S3 (config-vlan)#vlan 23

S3 (config-vlan)#name Ingenieria

S3 (config-vlan)#vlan 99

S3 (config-vlan)#name Administracion

S3 (config-vlan)#exit

S3 (config)#int vlan 99

S3 (config-if)#ip address 192.168.99.3 255.255.255.0

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

S3 (config)#int f0/3

S3 (config-if)#switchport mode trunk

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

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

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

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

S3 (config-if)#switchport access vlan 23

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

S3 (config-if-range)#shut

S3 (config-if)#exit

Paso 3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Datos configuración subinterfaz para R1

Elemento o tarea de configuración	Especificación
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
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
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
Activar la interfaz f0/1	

Fuente: guía Prueba de habilidades CCNA

Código configuración de la subinterfaz para R1

R1#config t

R1(config)#int f0/1.21

R1(config-subif)#description LAN de Contabilidad

R1(config-subif)#encapsulation dot1q 21

R1(config-subif)#ip add 192.168.21.1 255.255.255.0

R1(config)#int f0/1.23

R1(config-subif)#description LAN de Ingenieria

R1(config-subif)#encapsulation dot1q 23

R1(config-subif)#ip add 192.168.23.1 255.255.255.0

R1(config)#int f0/1.99

R1(config-subif)#description LAN de Administracion

R1(config-subif)#encapsulation dot1q 99

R1(config-subif)#ip add 192.168.99.1 255.255.255.0

R1(config-subif)#exit

Paso 4. Verificar la conectividad de la red

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

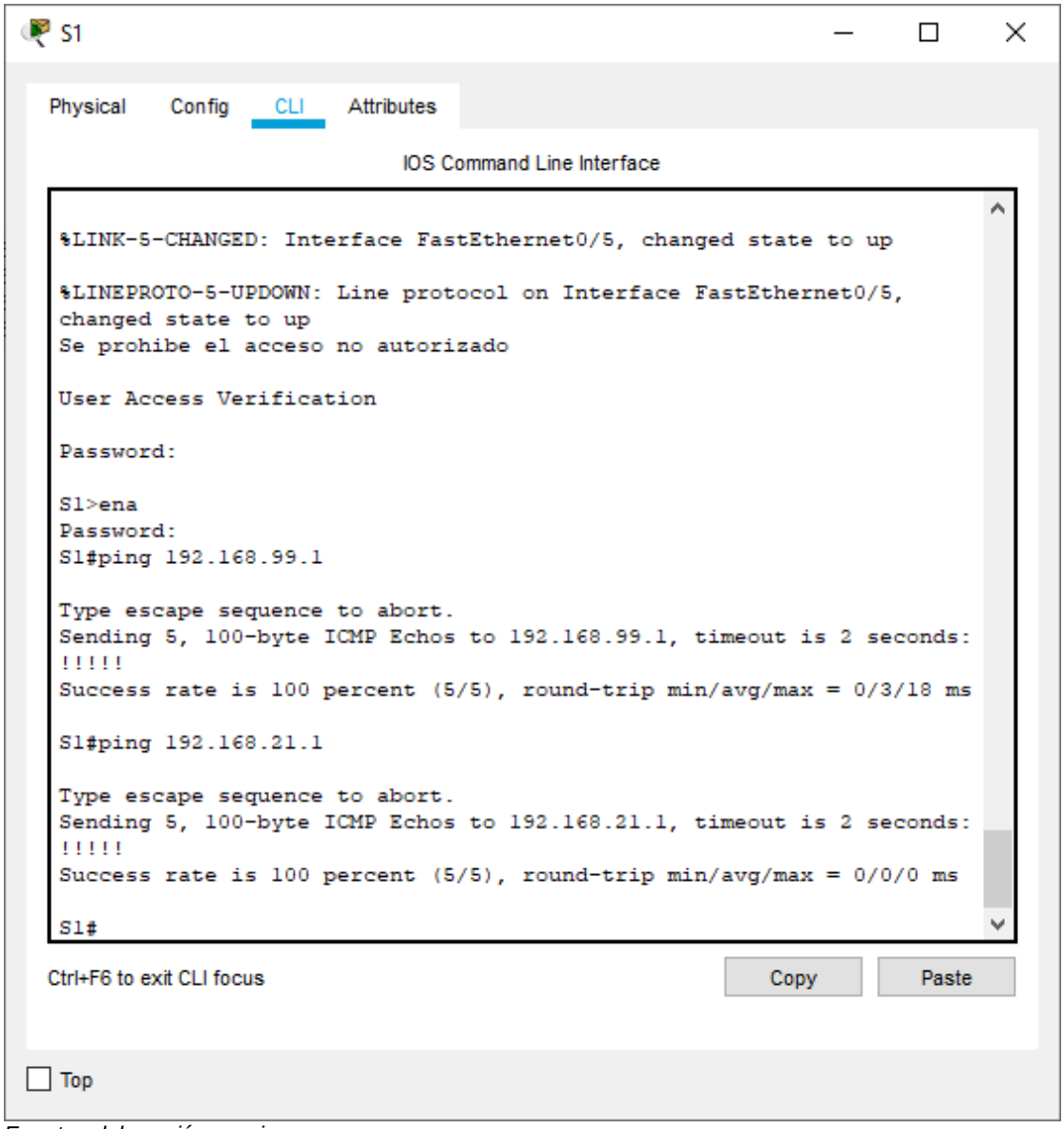
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Datos verificación conectividad Switches y R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Success - Éxito
S3	R1, dirección VLAN 99	192.168.99.1	Success - Éxito
S1	R1, dirección VLAN 21	192.168.21.1	Success - Éxito
S3	R1, dirección VLAN 23	192.168.23.1	Success - Éxito

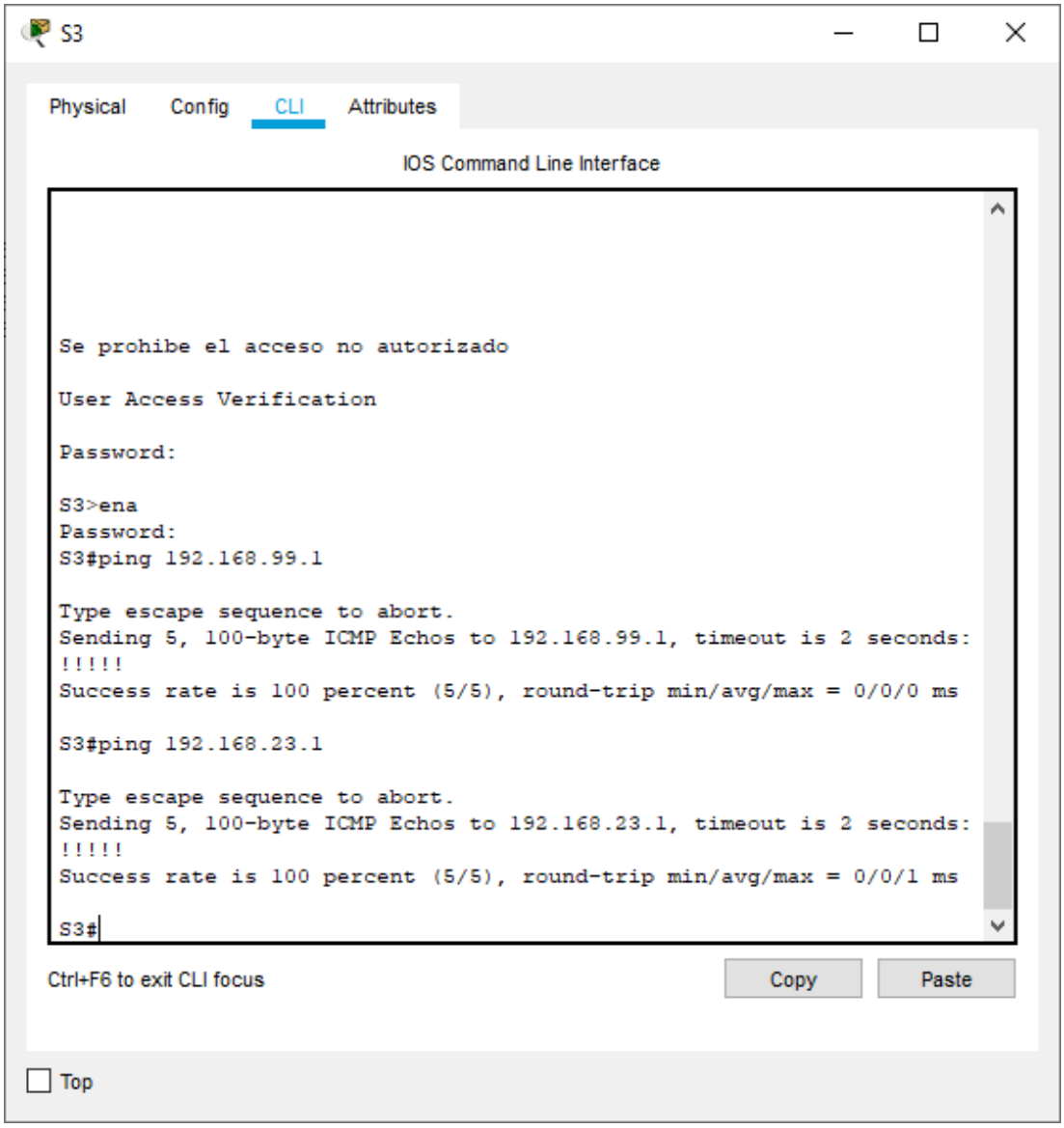
Fuente: guía Prueba de habilidades CCNA

Figura 13. Verificación Ping S1 con R1 VLAN 99 Y R1 VLAN 21



Fuente: elaboración propia

Figura 14. Verificación Ping S3 con R1 VLAN 99 y R1 vlan 23



Fuente: elaboración propia

6.1.4 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:

Tabla 13. Datos de configuración RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente: guía Prueba de habilidades CCNA

Código configuración RIPv2 en el R1

```
R1#conf t
R1 (config)#router rip
R1 (cofig-router)#version 2
R1 (cofig-router)#Network 192.168.21.1
R1 (cofig-router)#Network 192.168.23.1
R1 (cofig-router)#Network 192.168.99.1
R1 (cofig-router)#Network 172.16.1.0
R1 (cofig-router)#passive-interface f0/0.21
R1 (cofig-router)#passive-interface f0/0.23
R1 (cofig-router)#passive-interface f0/0.99
R1 (cofig-router)#passive-interface s0/1/0
R1 (cofig-router)#no auto-summary
```

Paso 2. Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Datos de configuración RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red f0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Fuente: guía Prueba de habilidades CCNA

Código configuración RIPv2 en el R2

R2#conf t

R2 (config)#router rip

R2 (cofig-router)#version 2

R2 (cofig-router)#Network 10.10.10.1

R2 (cofig-router)#Network 172.16.1.1

R2 (cofig-router)#Network 172.16.2.1

R2 (cofig-router)#passive-interface f0/1

R2 (cofig-router)#passive-interface s0/0/0

R2 (cofig-router)#passive-interface s0/1/0

R2 (cofig-router)#no auto-summary

Paso3. Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Fuente: guía Prueba de habilidades CCNA

Código configuración RIPv2 en el R3

R3#conf t

R3 (config)#router rip

R3 (cofig-router)#version 2

R3 (cofig-router)#Network 172.16.2.0

R3 (cofig-router)#Network 192.168.4.0

R3 (cofig-router)#Network 192.168.5.0

R3 (cofig-router)#Network 192.168.6.0

R3 (cofig-router)#passive-interface lo4

R3 (cofig-router)#passive-interface lo5

R3 (cofig-router)#passive-interface lo6

R3 (cofig-router)#no auto-summary

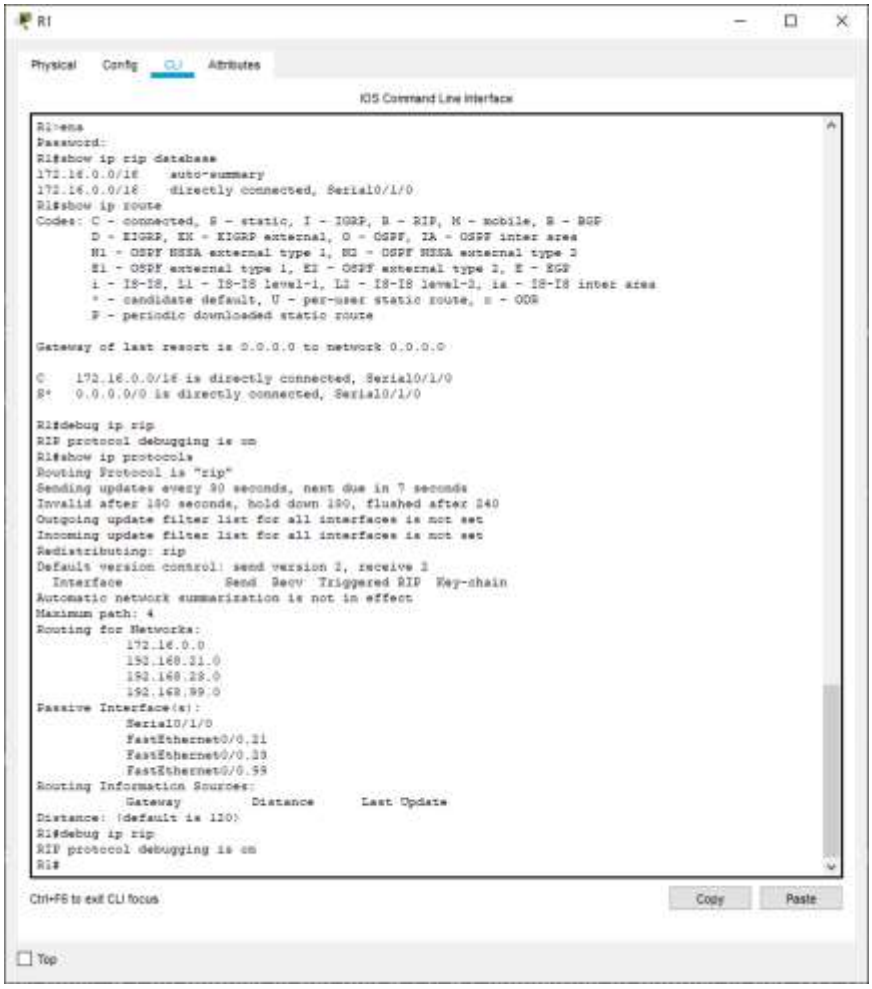
Paso 4. Verificar la información de RIP

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

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

Fuente: guía Prueba de habilidades CCNA

Figura 15. Comandos de verificación RIP



Fuente: elaboración propia

6.1.5 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:

Tabla 15. Datos de configuración de R1 como servidor DHCP para VLAN 21 Y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	192.168.23.1 192.168.23.21
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
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Fuente: guía Prueba de habilidades CCNA

Código configuración DHCP para R1

```
R1#config t
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#ip default-gateway 192.168.21.1
R1(config)#ip dhcp pool ENGNR
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)#ip default-gateway 192.168.23.1

R1(dhcp-config)#exit

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

La configuración del R2 incluye las siguientes tareas:

Tabla 16. Datos de configuración NAT estática y dinámica para R2

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**
Habilitar el servicio del servidor HTTP	ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	Ip nat inside / outside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225 – 209.165.200.228**
Definir la traducción de NAT dinámica	

Fuente: guía Prueba de habilidades CCNA

Código configuración DHCP para R2

R2#config t

R2 (config)#user webuser privilege 15 secret cisco12345

R2 (config)#ip nat inside source static 10.10.10.10 209.165.200.229

R2 (config)#int loopback 0

R2 (config-if)#ip nat inside

R2 (config-if)#int f0/0

R2 (config-if)#ip nat outside

R2 (config)#access-list 1 permit 192.168.21.00.0.0.255

R2 (config)#access-list 1 permit 192.168.23.00.0.0.255

R2 (config)#access-list 1 permit 192.168.4.0

R2 (config)#access-list 1 permit 192.168.5.0

R2 (config)#access-list 1 permit 192.168.6.0

R2 (config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

R2 (config)#

Paso 3. Verificar el protocolo DHCP y la NAT estática

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

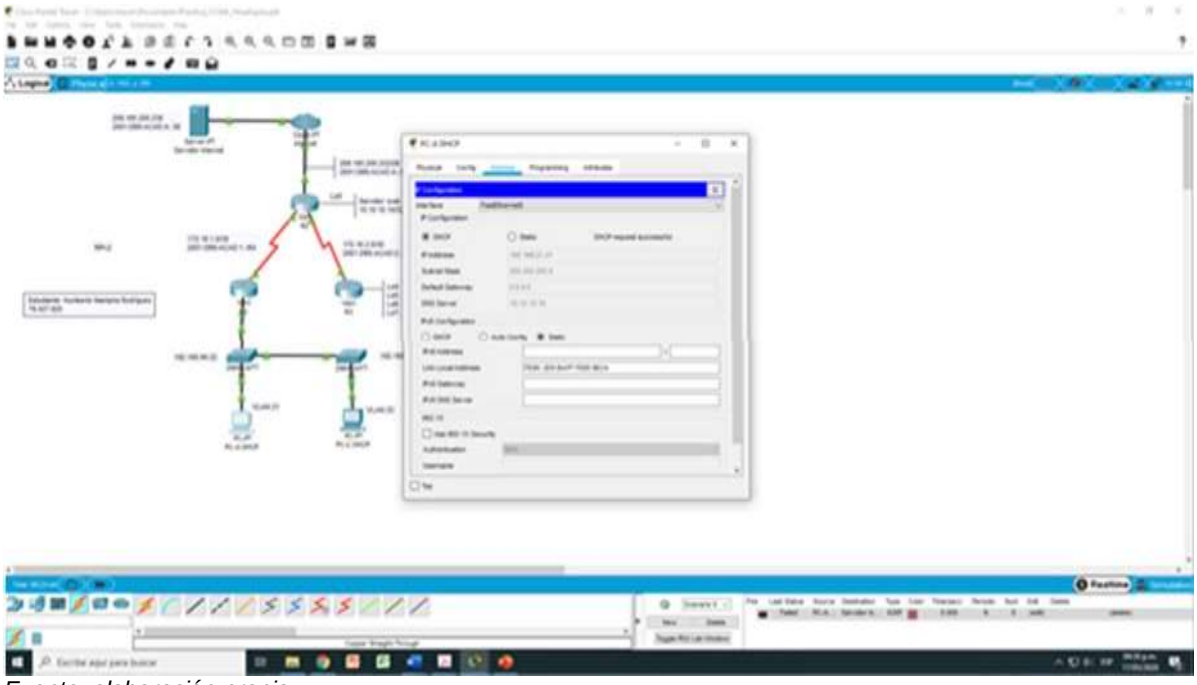
Tabla 17. Verificación del protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ver figura 29

Prueba	Resultados
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ver figura 30
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	
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**	Ver figura 31

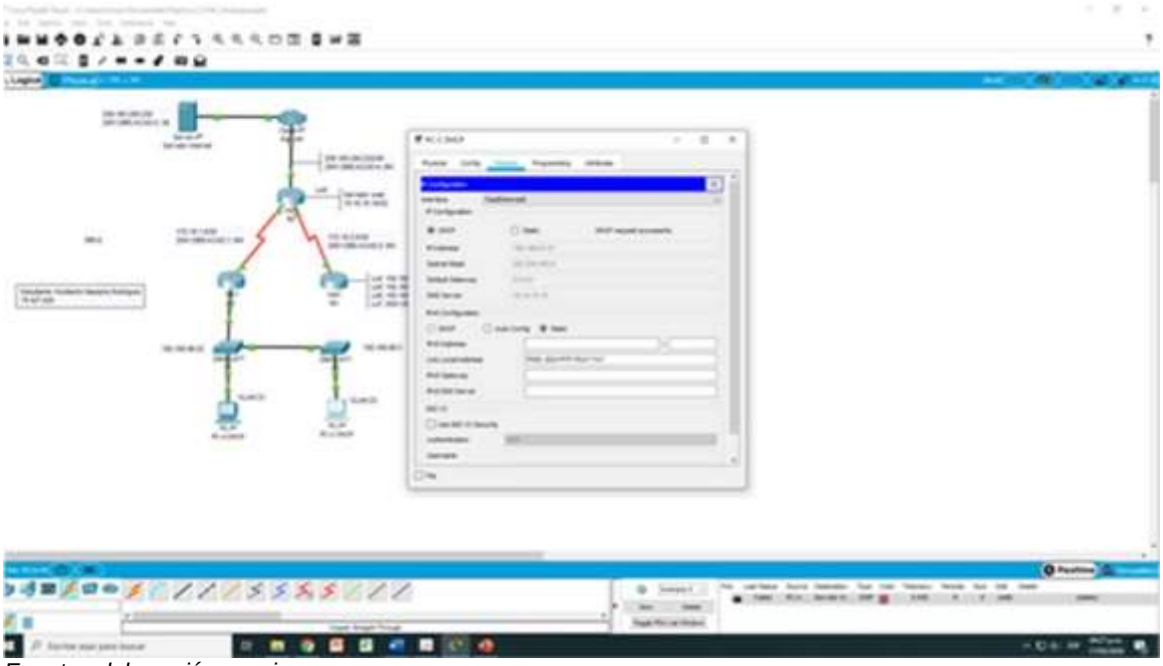
Fuente: guía Prueba de habilidades CCNA

Figura 16. Modo DHCP PC-A



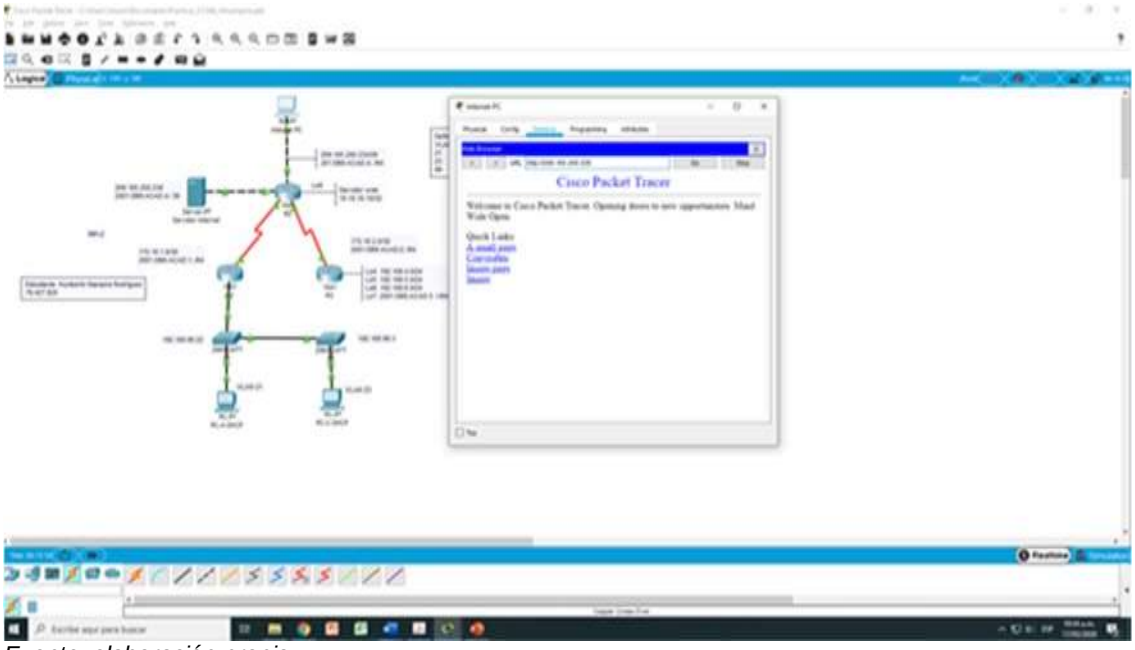
Fuente: elaboración propia

Figura 17. Modo DHCP PC-C



Fuente: elaboración propia

Figura 18. Acceso al sitio web 209.165.200.229 desde la PC de Internet



Fuente: elaboración propia

6.1.6 Parte 6. Configurar NTP

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

Configuración en R2 de ajuste de fecha y hora

R2>enab

R2#clock set 9:00:00 5 march 2016

R2# config t

R2 (config)#ntp master 5

Configuración como cliente en R1 de NTP

R1#config t

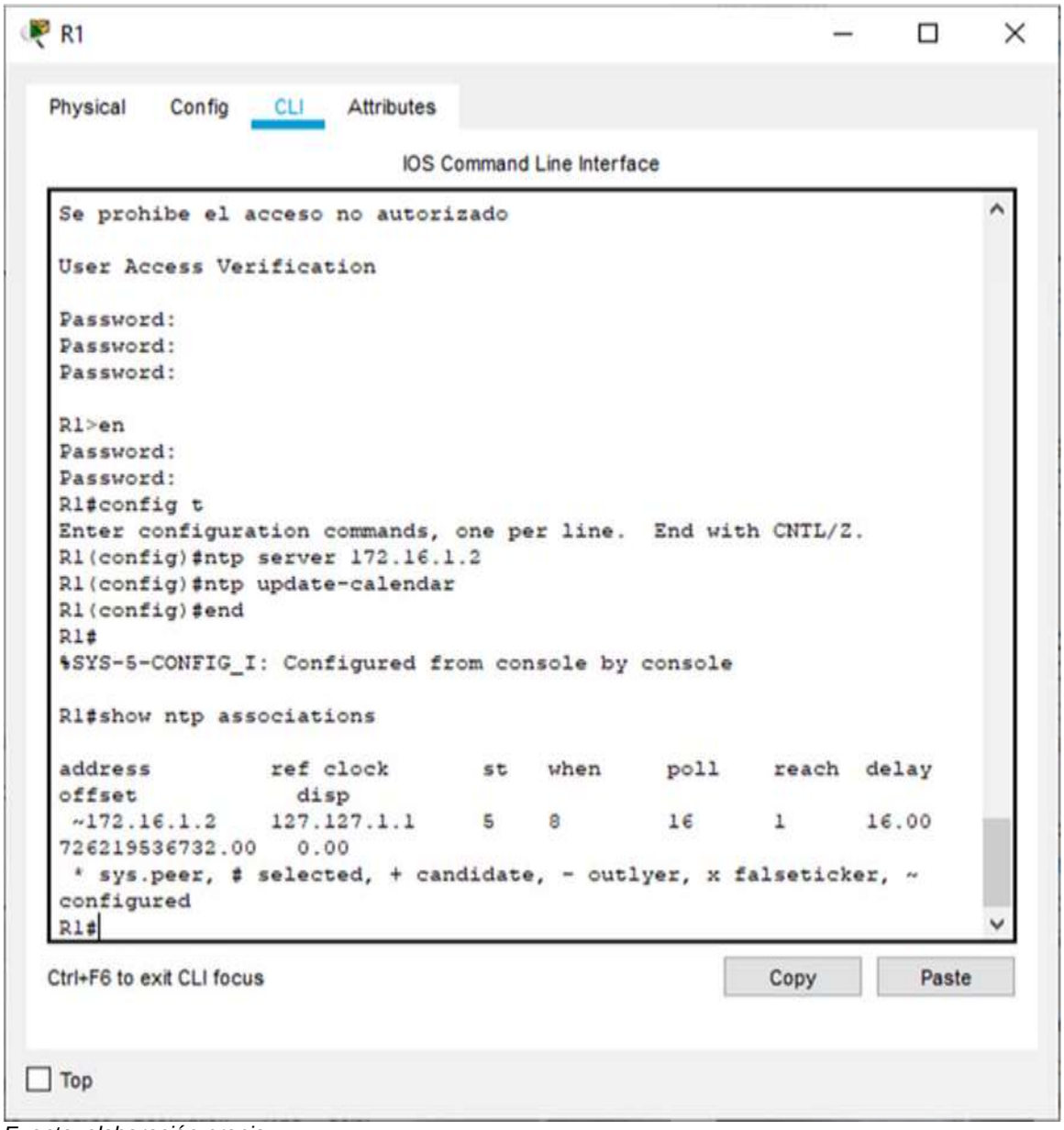
R1 (Config)#ntp server 172.16.1.2

R1 (Config)#ntp update-calendar

R1 (Config)#end

R1#show ntp associations

Figura 19. Configuración y verificación de NTP para R1



Fuente: elaboración propia

6.1.7 Parte 7: 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**
Aplicar la ACL con nombre a las líneas VTY	line vty 0 15
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

R2#config t

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

Con la siguiente línea debemos permitir acceso al R1

R2(config-std-nacl)#permit host 172.16.1.1

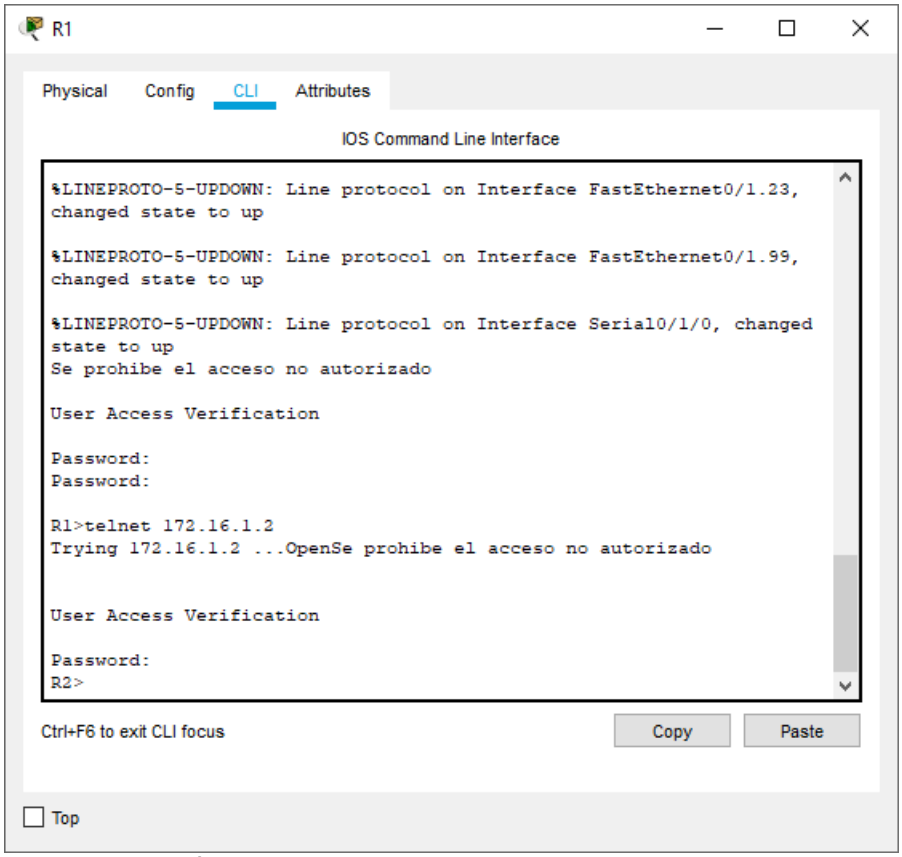
R2(config-std-nacl)#line vty 0 15

R2(config-line)#transport input telnet

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

R2(config-line)#exit

Figura 20. Verificación de ACL de conexión del R1 al R2



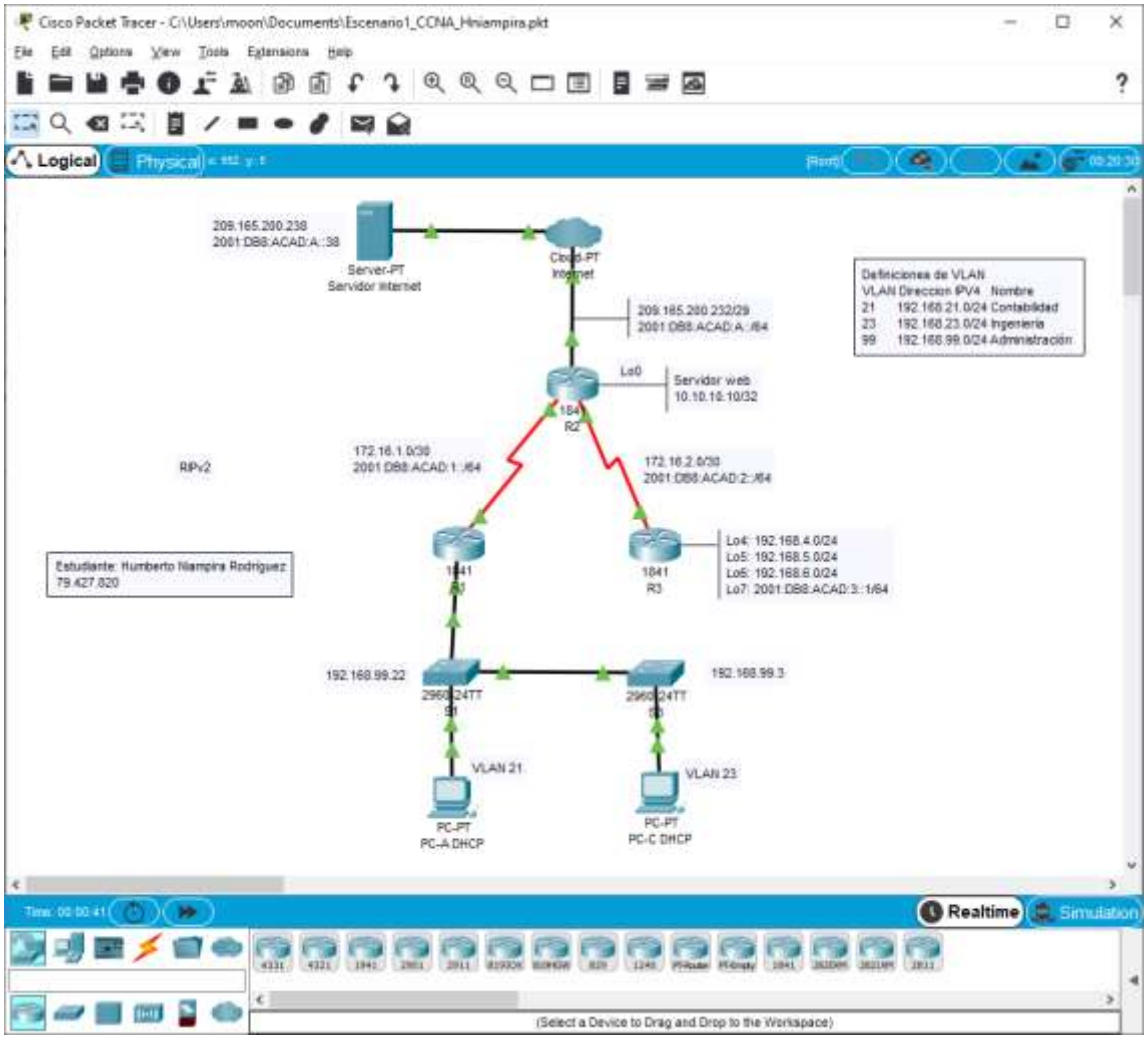
Fuente: elaboración propia

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	show access-lists
Restablecer los contadores de una lista de acceso	clear Access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show interface

Descripción del comando	Entrada del estudiante (comando)
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 ---
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation

Figura 21. Resultado final topología escenario 1



Fuente: elaboración propia

6.1.8 Análisis de resultados escenario 1

Se cumplieron con los propósitos establecidos para el desarrollo de las pruebas de habilidades, se lograron aplicar entre otros aspectos, la utilización de comandos requeridos para la configuración de router y switchs. La optimización de memoria en los router implementando y configurando rutas estáticas y predeterminadas a través de los protocolos IPv4 e IPv6. También se evidencia la importancia de la implementación y configuración de redes VLAN y enlaces troncales en una organización, ya que, a través de estas permiten mejorar el rendimiento de la red, así como también implementar medidas de seguridad como la encriptación de contraseñas de acceso que controlan qué hosts se pueden comunicar debidamente.

Se cumplió con la debida configuración de dispositivos router y switch, aunque considero que se debe estudiar las prestaciones que ofrece cada referencia de dispositivos Cisco, dado que algunos manejan características de seguridad y rendimiento mejores que otros, pero ello depende del escenario a desarrollar de acuerdo con la finalidad y tipo de red requerido, sumado a lo anterior también se debe resaltar la importancia de identificar el tipo de interfaz a utilizar.

Aunque se configuro una red pequeña para facilitar el aprendizaje, encontré dificultades específicamente en el direccionamiento IP y el manejo del protocolo IPv6, en temas de manejo de su longitud frente a los tipos de dirección, debo ahondar más sobre el tema dado que a futuro muy cercano debemos de trabajar de lleno con estas direcciones de red.

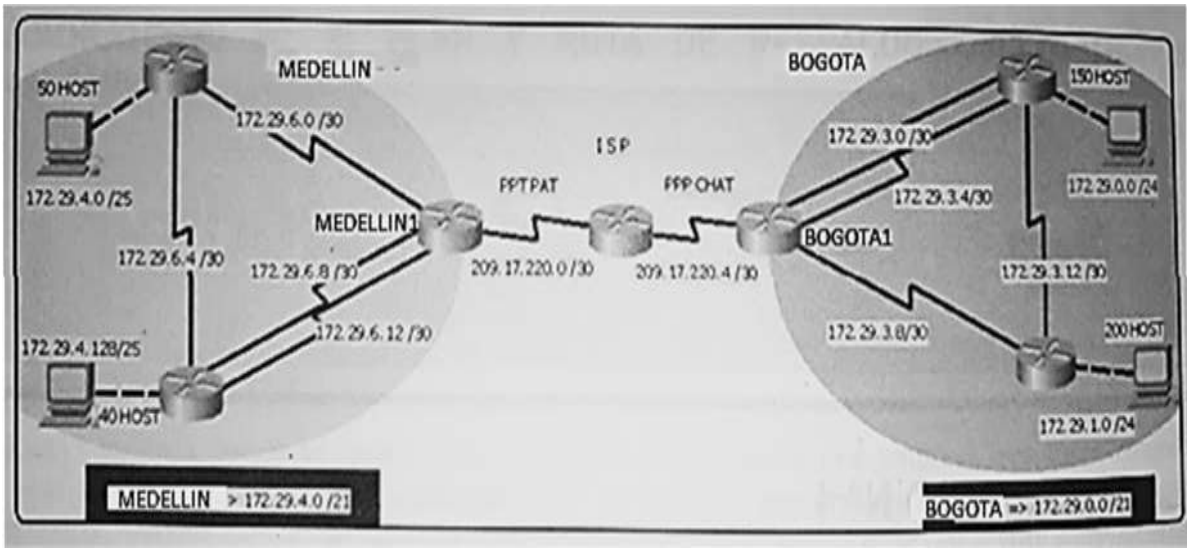
Sería interesante incluir en las pruebas de habilidades, la implementación de la técnica dual-stack la cual permite coexistir dos tecnologías de red como son IPv4 e IPv6 sobre un mismo enlace de red, dado que fue visto en los talleres del curso.

Por último, debo resaltar que la herramienta de simulación packet tracer ha facilitado el aprendizaje, pero se debería incluir en dicho proceso la practica en un laboratorio real, donde se pueda interactuar con dispositivos en la conexión y configuración de cada dispositivo.

6.2 ESCENARIO 2

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

Figura 22. Topología de red propuesto para el escenario 2



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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

Configuración inicial router ISP

Router>en

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname ISP

ISP(config)#service password-encryption

ISP(config)#enable secret class

ISP(config)#banner motd #acceso no autorizado#

ISP(config)#line console 0

ISP(config-line)#password cisco

ISP(config-line)#login

ISP(config-line)#line vty 0 4

ISP(config-line)#password class

ISP(config-line)#login

Configuración inicial router BOGOTA1

Router>en

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname BOGOTA1

BOGOTA1(config)#service password-encryption

BOGOTA1(config)#enable secret class

BOGOTA1(config)#banner motd #acceso no autorizado#

BOGOTA1(config)#line console 0

BOGOTA1(config-line)#password cisco

BOGOTA1(config-line)#login

BOGOTA1(config-line)#line vty 0 4

BOGOTA1(config-line)#password class

BOGOTA1(config-line)#login

Configuración inicial router BOGOTA2

Router>en

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname BOGOTA2

BOGOTA2(config)#service password-encryption

BOGOTA2(config)#enable secret class

BOGOTA2(config)#banner motd #acceso no autorizado#

BOGOTA2(config)#line console 0

BOGOTA2(config-line)#password cisco

BOGOTA2(config-line)#login

BOGOTA2(config-line)#line vty 0 4

BOGOTA2(config-line)#password class

BOGOTA2(config-line)#login

Configuración inicial router BOGOTA3

Router>en

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname BOGOTA3

BOGOTA3(config)#service password-encryption

BOGOTA3(config)#enable secret class

BOGOTA3(config)#banner motd #acceso no autorizado#

BOGOTA3(config)#line console 0

BOGOTA3(config-line)#password cisco

BOGOTA3(config-line)#login

BOGOTA3(config-line)#line vty 0 4

BOGOTA3(config-line)#password class

BOGOTA3(config-line)#login

Configuración inicial router MEDELLIN1

Router>en

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname MEDELLIN1

MEDELLIN1(config)#service password-encryption

MEDELLIN1 (config)#enable secret class

MEDELLIN1 (config)#banner motd #acceso no autorizado#

MEDELLIN1 (config)#line console 0

MEDELLIN1 (config-line)#password cisco

MEDELLIN1 (config-line)#login

MEDELLIN1 (config-line)#line vty 0 4

MEDELLIN1 (config-line)#password class

MEDELLIN1 (config-line)#login

Configuración inicial router MEDELLIN2

Router>en

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname MEDELLIN2

MEDELLIN2(config)#service password-encryption

MEDELLIN2 (config)#enable secret class

MEDELLIN2 (config)#banner motd #acceso no autorizado#

MEDELLIN2 (config)#line console 0

MEDELLIN2 (config-line)#password cisco

MEDELLIN2 (config-line)#login

MEDELLIN2 (config-line)#line vty 0 4

MEDELLIN2 (config-line)#password class

MEDELLIN2 (config-line)#login

Configuración inicial router MEDELLIN3

Router>en

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname MEDELLIN3

MEDELLIN3(config)#service password-encryption

MEDELLIN3 (config)#enable secret class

MEDELLIN3 (config)#banner motd #acceso no autorizado#

MEDELLIN3 (config)#line console 0

MEDELLIN3 (config-line)#password cisco

MEDELLIN3 (config-line)#login

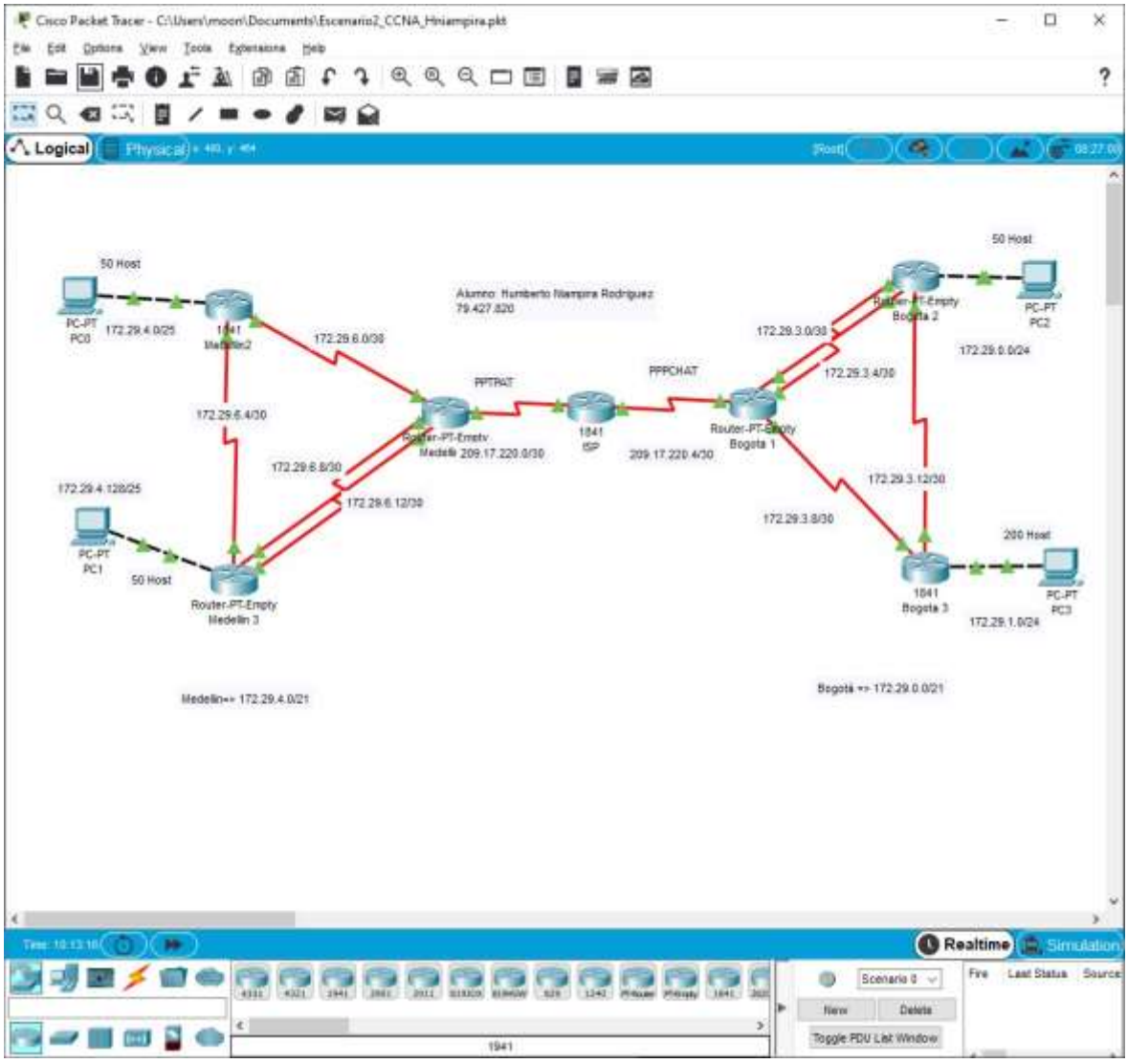
MEDELLIN3 (config-line)#line vty 0 4

MEDELLIN3 (config-line)#password class

MEDELLIN3 (config-line)#login

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

Figura 23. Diseño topología escenario 2



Fuente: elaboración propia

6.2.1 Parte 1: Configuración del enrutamiento

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

Código configuración enrutamiento router ISP

```
ISP>enab
ISP#conf t
ISP(config)#int s0/0/0
ISP(config-if)#description ISP-MEDELLIN1
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#no shu
ISP(config-if)#exit
ISP(config)#int s0/0/1
ISP(config-if)#description ISP-BOGOTA1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#no shu
ISP(config-if)#exit
ISP(config-if)#router ospf 1
ISP(config-router)#router-id 1.1.1.1
ISP (config-router)#passive-interface f0/0
ISP (config-router)#passive-interface f0/1
ISP(config-router)# network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)# network 209.17.220.4 0.0.0.3 area 0
ISP(config-router)# do show ip route connected
```

Código configuración enrutamiento en router Medellin1

```
MEDELLIN1>enable
MEDELLIN1#config t
MEDELLIN1(config)#int S3/0
MEDELLIN1(config-if)#description MEDELLIN1-ISP
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown
```

MEDELLIN1(config-if)#exit

MEDELLIN1(config)#interface s0/0
MEDELLIN1(config-if)# description MEDELLIN1-MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

MEDELLIN1(config)#interface s2/0
MEDELLIN1(config-if)# description MEDELLIN1-MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

MEDELLIN1(config)#interface s1/0
MEDELLIN1(config-if)# description MEDELLIN1-MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

Configuramos el Protocolo OSPF V2
MEDELLIN1 (config)#router ospf 1
MEDELLIN1 (config-router)#router-id 2.2.2.2
MEDELLIN1 (config-router)# network 172.29.6.0 0.0.0.255 area 0
MEDELLIN1 (config-router)# network 172.29.6.12 0.0.0.255 area 0
MEDELLIN1 (config-router)# network 172.29.6.8 0.0.0.255 area 0
MEDELLIN1(config-router)#no auto-summary

Código configuración enrutamiento en router MEDELLIN2

MEDELLIN2 >enab

MEDELLIN2 #config t

MEDELLIN2(config)#interface s0/0/0

MEDELLIN2(config-if)#description MEDELLIN2-MEDELLIN1

MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252

MEDELLIN2(config-if)#no shutdown

MEDELLIN2(config-if)#exit

MEDELLIN2(config)#interface s0/0/1

MEDELLIN2(config-if)# description MEDELLIN2-MEDELLIN3

MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252

MEDELLIN2(config-if)#no shu

MEDELLIN2(config-if)#exit

MEDELLIN2(config)#interface f0/0

MEDELLIN2(config-if)# description MEDELLIN2-PC0

MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.252

MEDELLIN2(config-if)#no shu

MEDELLIN2(config-if)#exit

Configuramos el Protocolo OSPF V2

MEDELLIN2 (config)#router ospf 1

MEDELLIN2 (config-router)#router-id 3.3.3.3

MEDELLIN2 (config-router)#passive-interface f0/1

MEDELLIN2 (config-router)# network 172.29.6.4 0.0.0.3 area 0

MEDELLIN2 (config-router)# network 172.29.6.0 0.0.0.3 area 0

MEDELLIN2 (config-router)# network 172.29.4.0 0.0.0.255 area 0

MEDELLIN2(config-router)#no auto-summary

Código configuración enrutamiento en router MEDELLIN3:

MEDELLIN3 >enab

MEDELLIN3 #config t

MEDELLIN3(config)#interface s2/0

MEDELLIN3(config-if)#description MEDELLIN3-MEDELLIN1

MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252

MEDELLIN3(config-if)#no shutdown

MEDELLIN3(config-if)#exit

MEDELLIN3(config)#interface s1/0

MEDELLIN3(config-if)# description MEDELLIN3-MEDELLIN2

MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252

MEDELLIN3(config-if)#no shu

MEDELLIN3(config-if)#exit

MEDELLIN3(config)#interface s0/0

MEDELLIN3(config-if)#description MEDELLIN3-MEDELLIN1

MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252

MEDELLIN3(config-if)#no shu

MEDELLIN3(config-if)#exit

MEDELLIN3(config)#interface f3/0

MEDELLIN3(config-if)#description MEDELLIN3-PC1

MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.252

MEDELLIN3(config-if)#no shu

MEDELLIN3(config-if)#exit

Configuramos el Protocolo OSPF V2

MEDELLIN3 (config)#router ospf 1

MEDELLIN3 (config-router)#router-id 4.4.4.4

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

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

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

MEDELLIN3 (config-router)# network 172.29.4.128 0.0.0.255 area 0

MEDELLIN3 (config-router)#no auto-summary

Código configuración enrutamiento el router BOGOTA1:

BOGOTA1 >enab

BOGOTA1 #config t

BOGOTA1(config)#interface s3/0

BOGOTA1 (config-if)#description BOGOTA1-ISP

BOGOTA1 (config-if)#ip address 209.17.220.5 255.255.255.252

BOGOTA1 (config-if)#no shutdown

BOGOTA1 (config-if)#exit

BOGOTA1 (config)#interface s2/0

BOGOTA1 (config-if)# description BOGOTA1-BOGOTA2

BOGOTA1 (config-if)#ip address 172.29.3.1 255.255.255.252

BOGOTA1 (config-if)#no shu

BOGOTA1 (config-if)#exit

BOGOTA1 (config)#interface S1/0

BOGOTA1 (config-if)# description BOGOTA1-BOGOTA3

BOGOTA1 (config-if)#ip address 172.29.3.9 255.255.255.252

BOGOTA1 (config-if)#no shu

BOGOTA1 (config-if)#exit

BOGOTA1 (config)#interface S0/0

BOGOTA1 (config-if)# description BOGOTA1-BOGOTA2

BOGOTA1 (config-if)#ip address 172.29.3.5 255.255.255.252

BOGOTA1 (config-if)#no shu

BOGOTA1 (config-if)#exit

Configuramos el Protocolo OSPF V2

BOGOTA1 (config)#router ospf 1

BOGOTA1 (config-router)#router-id 5.5.5.5

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

BOGOTA1 (config-router)# network 172.29.3.0 0.0.0.3 area 0

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

BOGOTA1 (config-router)#no auto-summary

Código configuración enrutamiento en router BOGOTA2:

BOGOTA2 >enab

BOGOTA2 #config t

BOGOTA2 (config)#interface s0/0

BOGOTA2 (config-if)#description BOGOTA2-BOGOTA1

BOGOTA2 (config-if)#ip address 172.29.3.1 255.255.255.252

BOGOTA2 (config-if)#no shutdown

BOGOTA2 (config-if)#exit

BOGOTA2 (config)#interface s2/0

BOGOTA2 (config-if)#description BOGOTA2-BOGOTA1

BOGOTA2 (config-if)#ip address 172.29.3.5 255.255.255.252

BOGOTA2 (config-if)#no shutdown

BOGOTA2 (config-if)#exit

BOGOTA2 (config)#interface s1/0

BOGOTA2 (config-if)# description BOGOTA2-BOGOTA3

BOGOTA2 (config-if)#ip address 172.29.3.13 255.255.255.252

BOGOTA2 (config-if)#no shu

BOGOTA2 (config-if)#exit

BOGOTA2 (config)#interface F3/0

BOGOTA2 (config-if)# description BOGOTA2-PC2

BOGOTA2 (config-if)#ip address 172.29.0.1 255.255.255.252

BOGOTA2 (config-if)#no shu

BOGOTA2 (config-if)#exit

Configuramos el Protocolo OSPF V2

BOGOTA2 (config)#router ospf 1

BOGOTA2 (config-router)#router-id 6.6.6.6

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

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

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

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

BOGOTA2 (config-router)#no auto-summary

Código configuración enrutamiento en router BOGOTA3:

BOGOTA3>enab

BOGOTA3#config t

BOGOTA3 (config)#interface s0/0/1

BOGOTA3 (config-if)#description BOGOTA3-BOGOTA1

BOGOTA3 (config-if)#ip address 172.29.3.10 255.255.255.252

BOGOTA3 (config-if)#no shutdown

BOGOTA3 (config-if)#exit

BOGOTA3 (config)#interface s0/0/0

BOGOTA3 (config-if)# description BOGOTA3-BOGOTA2

BOGOTA3 (config-if)#ip address 172.29.3.14 255.255.255.252

BOGOTA3 (config-if)#no shu

BOGOTA3 (config-if)#exit

BOGOTA3 (config)#interface f0/0

BOGOTA3 (config-if)# description BOGOTA3-PC3

BOGOTA3 (config-if)#ip address 172.29.1.2 255.255.255.252

BOGOTA3 (config-if)#no shu

BOGOTA3 (config-if)#exit

Configuramos el Protocolo OSPF V2

BOGOTA3 (config)#router ospf 1

BOGOTA3 (config-router)#router-id 7.7.7.7

BOGOTA3 (config-router)#passive-interface f0/1

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

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

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

BOGOTA3 (config-router)#no auto-summary

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

Código configuración Bogotá1

BOGOTA1>ena

BOGOTA1#conf t

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.6

BOGOTA1(config)#route OSPF 1

BOGOTA1(config-router)#default-information originate

BOGOTA1(config-router)#

Código configuración MEDELLIN1

MEDELLIN>enable

MEDELLIN#conf t

MEDELLIN(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

MEDELLIN(config)#router OSPF

MEDELLIN(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.

Código asignación ruta estática para Medellin y Bogotá

Resultado de sumarización para Medellin - 172.29.4.0/22

Resultado de sumarización para Bogota - 172.29.0.0/22

Se configura en el router ISP la ruta hacia cada red interna

ISP>enab

ISP#conf t

ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/0/0

ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/0/1

ISP(config)#exit

6.2.2 Parte 2: Tabla de Enrutamiento.

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

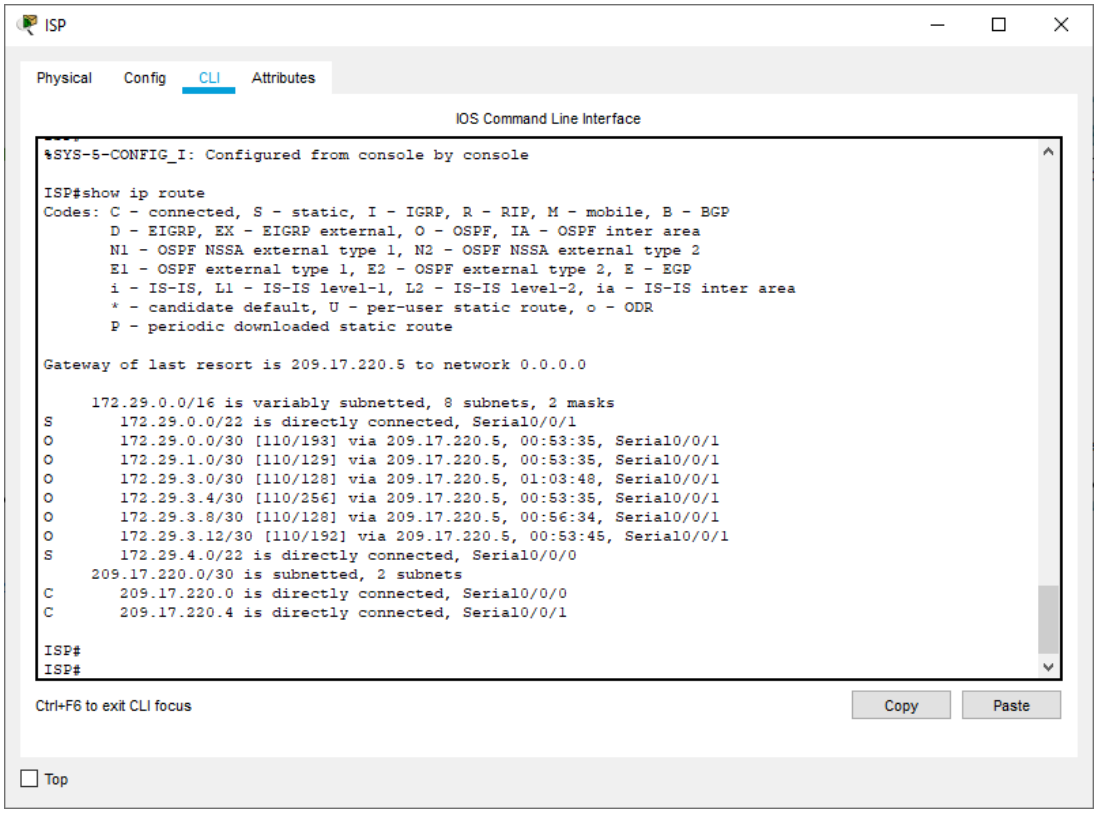
El siguiente código nos muestra todas las rutas OSPF configuradas en ISP.

O 172.29.0.0/30 [110/193] via 209.17.220.5, 00:53:35, Serial0/0/1
O 172.29.1.0/30 [110/129] via 209.17.220.5, 00:53:35, Serial0/0/1
O 172.29.3.0/30 [110/128] via 209.17.220.5, 01:03:48, Serial0/0/1
O 172.29.3.4/30 [110/256] via 209.17.220.5, 00:53:35, Serial0/0/1
O 172.29.3.8/30 [110/128] via 209.17.220.5, 00:56:34, Serial0/0/1
O 172.29.3.12/30 [110/192] via 209.17.220.5, 00:53:45, Serial0/0/1

El siguiente código nos muestra las rutas estáticas presentes en la tabla

S 172.29.0.0/22 is directly connected, Serial0/0/1
S 172.29.4.0/22 is directly connected, Serial0/0/0

Figura 24. Verificación tabla enrutamiento para ISP



Fuente: elaboración propia

Para el router Medellin1 encontramos las rutas OSPF configuradas:

O 172.29.4.0 [110/65] via 172.29.6.2, 00:42:49, Serial0/0
O 172.29.4.128 [110/65] via 172.29.6.14, 00:24:35, Serial2/0
O 172.29.6.4 [110/128] via 172.29.6.2, 00:24:35, Serial0/0

Rutas conectadas directamente

C 172.29.6.0/30 is directly connected, Serial0/0
C 172.29.6.8/30 is directly connected, Serial1/0
C 172.29.6.12/30 is directly connected, Serial2/0
C 209.17.220.0/30 is directly connected, Serial3/0

Rutas estáticas y predeterminadas

S* 0.0.0.0/0 [1/0] via 209.17.220.1

Para el router Medellin2 encontramos las rutas OSPF configuradas:

O 172.29.4.128 [110/129] via 172.29.6.2, 00:35:16, Serial0/0/0
O 172.29.6.8 [110/128] via 172.29.6.2, 00:48:22, Serial0/0/0
O 172.29.6.12 [110/128] via 172.29.6.2, 00:49:06, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.2, 00:22:45, Serial0/0/0

Rutas conectadas directamente

C 172.29.4.0/30 is directly connected, FastEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1

Para el router Medellin3 encontramos las rutas OSPF

O 172.29.4.0 [110/129] via 172.29.6.13, 00:37:38, Serial2/0
O 172.29.6.0 [110/128] via 172.29.6.13, 00:37:38, Serial2/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 00:25:03, Serial2/0

Rutas conectadas directamente

C 172.29.4.128/30 is directly connected, FastEthernet3/0
C 172.29.6.4/30 is directly connected, Serial1/0
C 172.29.6.8/30 is directly connected, Serial0/0
C 172.29.6.12/30 is directly connected, Serial2/0

Para el router Bogota1 encontramos las rutas OSPF configuradas:

O 172.29.0.0 [110/129] via 172.29.3.10, 01:13:11, Serial1/0
O 172.29.1.0 [110/65] via 172.29.3.10, 01:13:11, Serial1/0
O 172.29.3.12 [110/128] via 172.29.3.10, 01:13:21, Serial1/0
209.17.220.0/30 is subnetted, 2 subnets

O 209.17.220.0 [110/128] via 209.17.220.5, 01:06:55, Serial3/0

Rutas conectadas directamente

C 172.29.3.0/30 is directly connected, Serial2/0
C 172.29.3.4/30 is directly connected, Serial0/0
C 172.29.3.8/30 is directly connected, Serial1/0
C 209.17.220.4/30 is directly connected, Serial3/0

Para el router Bogota2 encontramos las rutas OSPF configuradas:

O 172.29.1.0 [110/65] via 172.29.3.14, 01:15:03, Serial1/0
O 172.29.3.8 [110/128] via 172.29.3.14, 01:15:13, Serial1/0
209.17.220.0/30 is subnetted, 2 subnets
O 209.17.220.0 [110/256] via 172.29.3.14, 01:08:48, Serial1/0
O 209.17.220.4 [110/192] via 172.29.3.14, 01:15:13, Serial1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.14, 00:30:05, Serial1/0

Rutas conectadas directamente
C 172.29.0.0/30 is directly connected, FastEthernet3/0
C 172.29.3.0/30 is directly connected, Serial0/0
C 172.29.3.4/30 is directly connected, Serial2/0

C 172.29.3.12/30 is directly connected, Serial1/0

Para el router Bogota3 encontramos las rutas OSPF configuradas:

O 172.29.0.0 [110/65] via 172.29.3.13, 01:16:47, Serial0/0/0
O 172.29.3.0 [110/128] via 172.29.3.9, 01:16:47, Serial0/0/1
[110/128] via 172.29.3.13, 01:16:47, Serial0/0/0
O 172.29.3.4 [110/128] via 172.29.3.13, 01:16:47, Serial0/0/0
209.17.220.0/30 is subnetted, 2 subnets
O 209.17.220.0 [110/192] via 172.29.3.9, 01:10:22, Serial0/0/1
O 209.17.220.4 [110/128] via 172.29.3.9, 01:17:26, Serial0/0/1

O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:31:39, Serial0/0/1

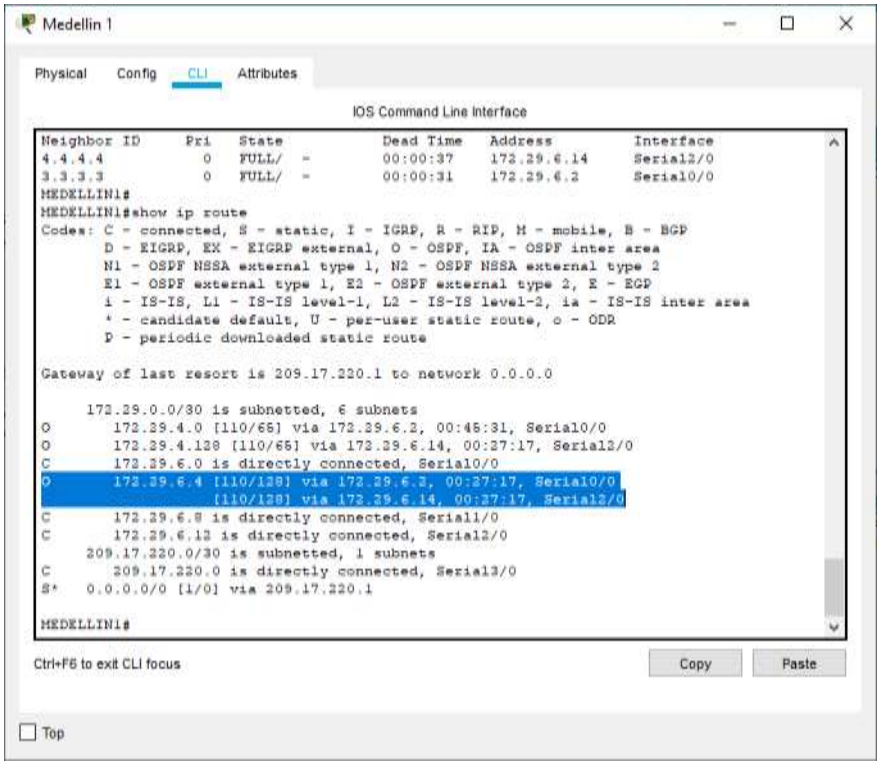
Conectadas directamente
C 172.29.1.0/30 is directly connected, FastEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/1

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

b. Verificar el balanceo de carga que presentan los routers.

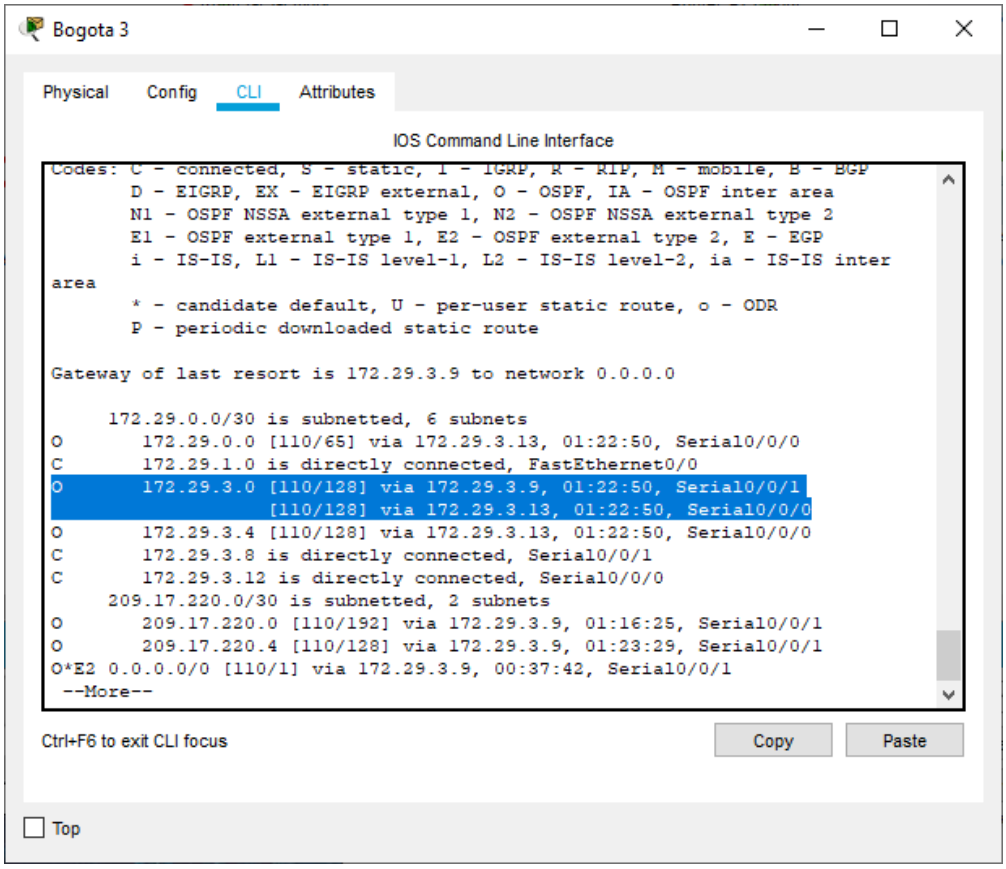
Se realiza la verificación en los router Medellin1 y Bogota2, quienes tienen asignado dos seriales

Figura 25. Verificación de balanceo de carga del router Medellin1



Fuente: elaboración propia

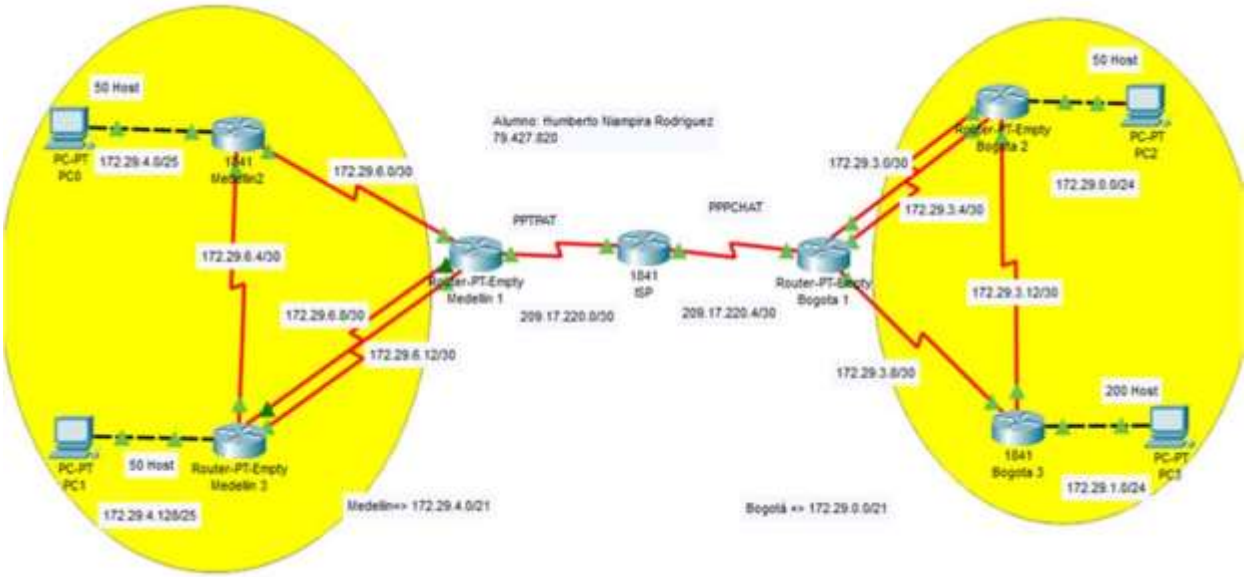
Figura 26. Verificación de balanceo de carga del router Bogota 2



Fuente: elaboración propia

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.

Figura 27. Similitud en los router Medellin1, Bogota 1

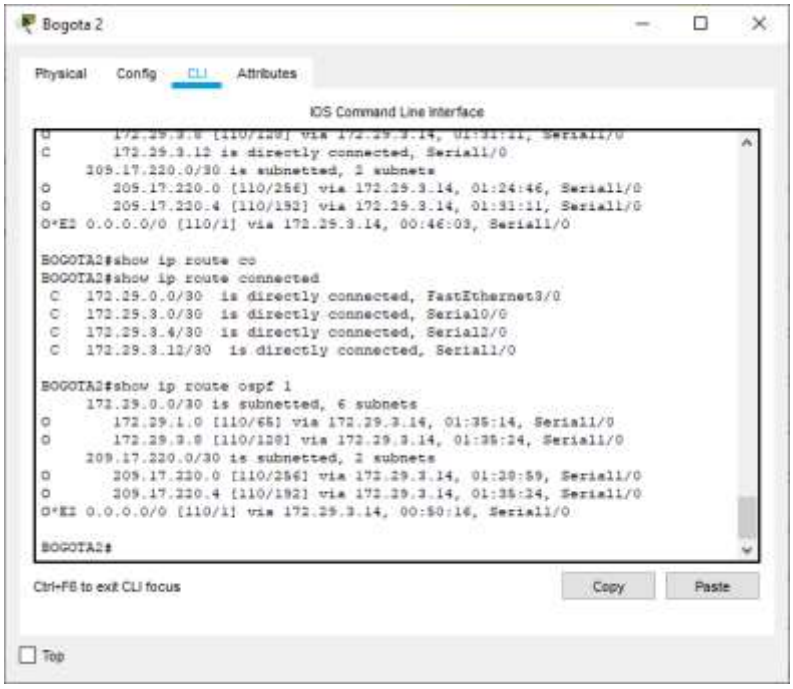


Fuente: elaboración propia

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

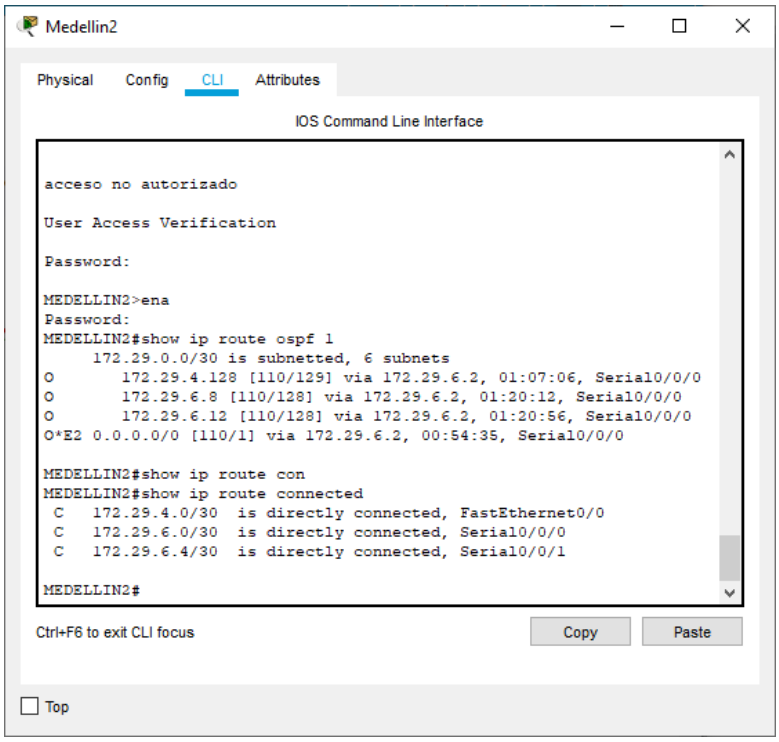
Con los comandos “show ip route connected” y “show ip route ospf 1” se evidencia en la figura No 28 las conexiones directas y por OSPF

Figura 28. Conexiones directas y recibidas por OSPF en router Bogota 2



Fuente: elaboración propia

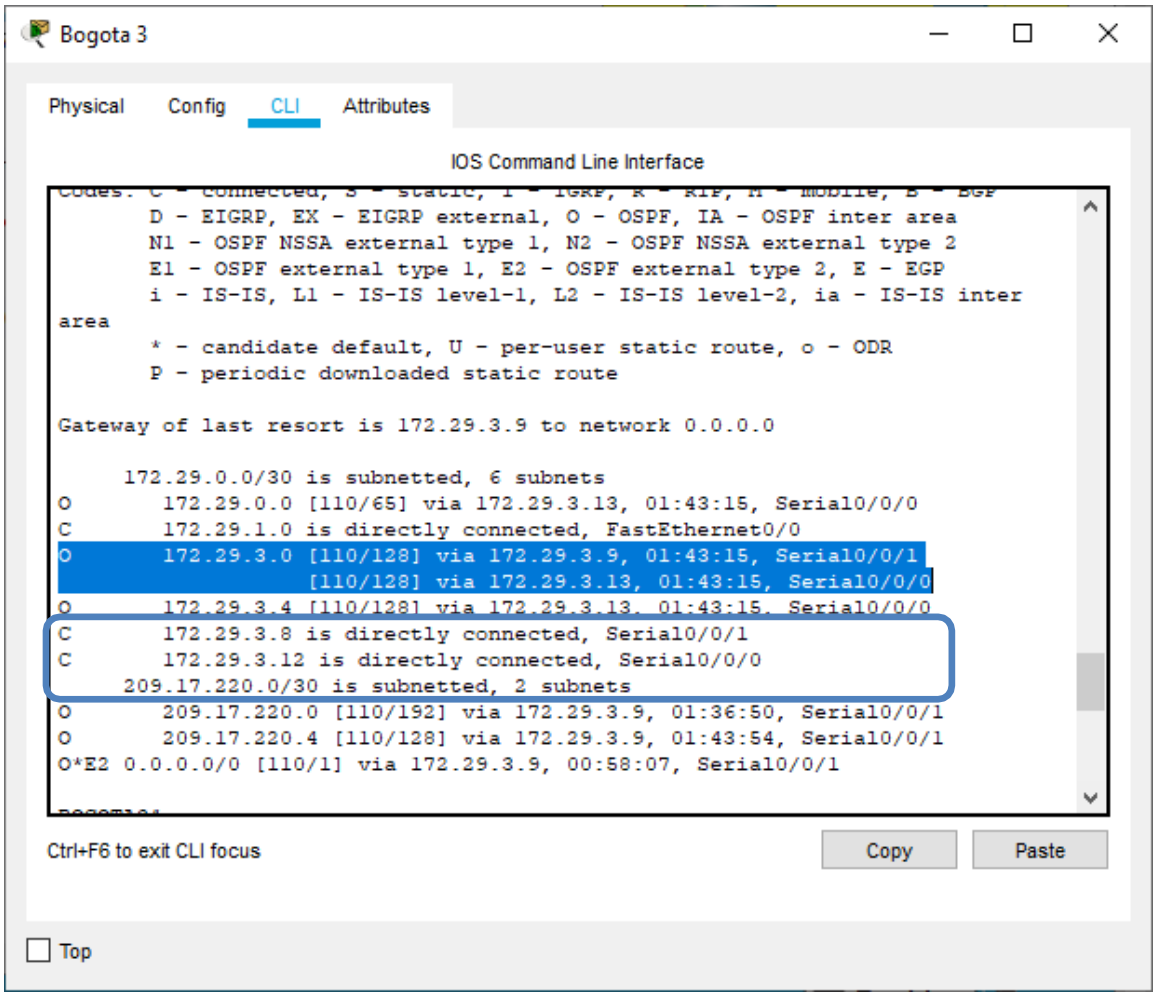
Figura 29. Conexiones directas y recibidas por OSPF en router Medellin 2



Fuente: elaboración propia

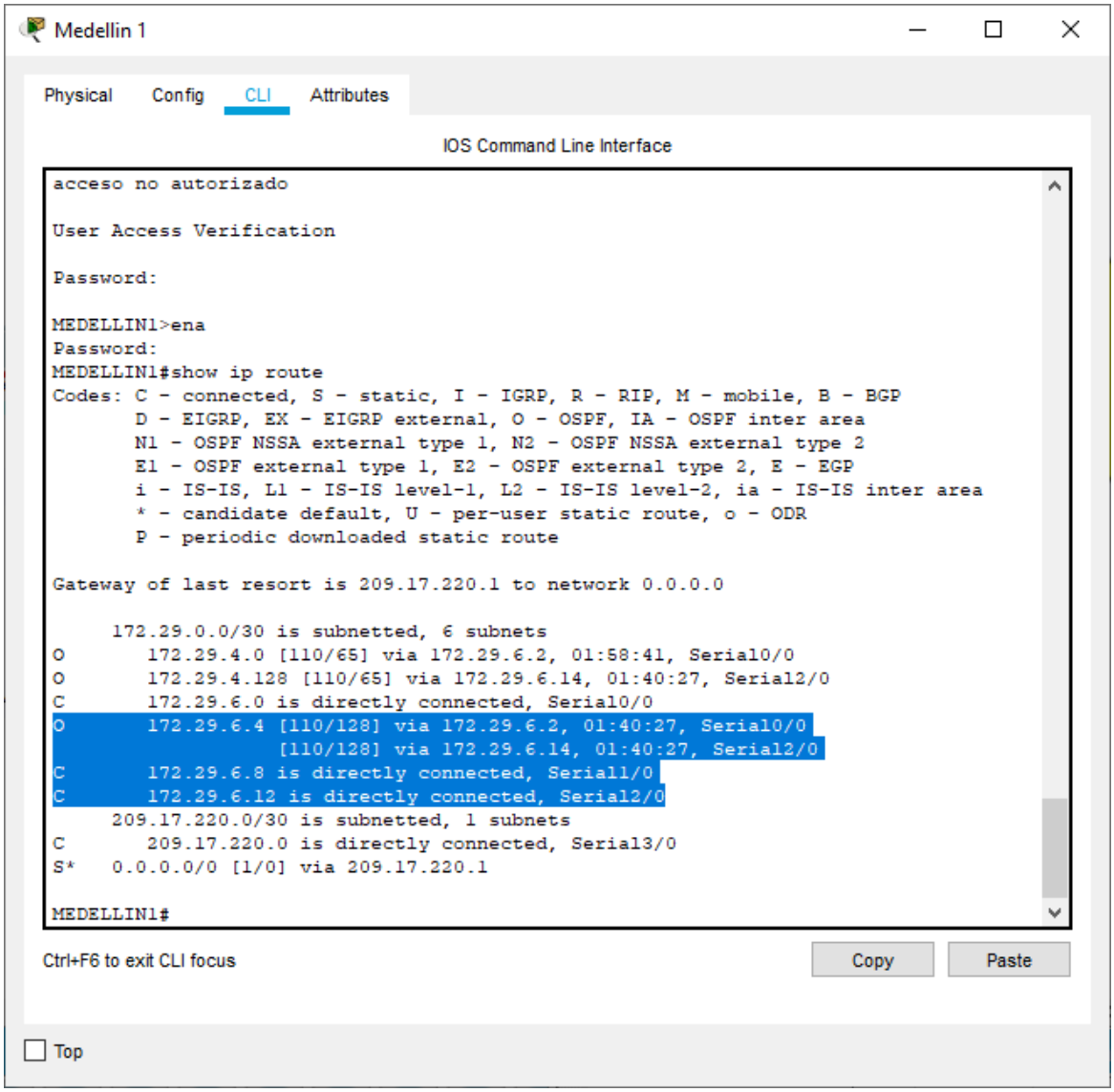
e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Figura 30. Verificación de rutas redundantes en Bogota 3



Fuente: elaboración propia

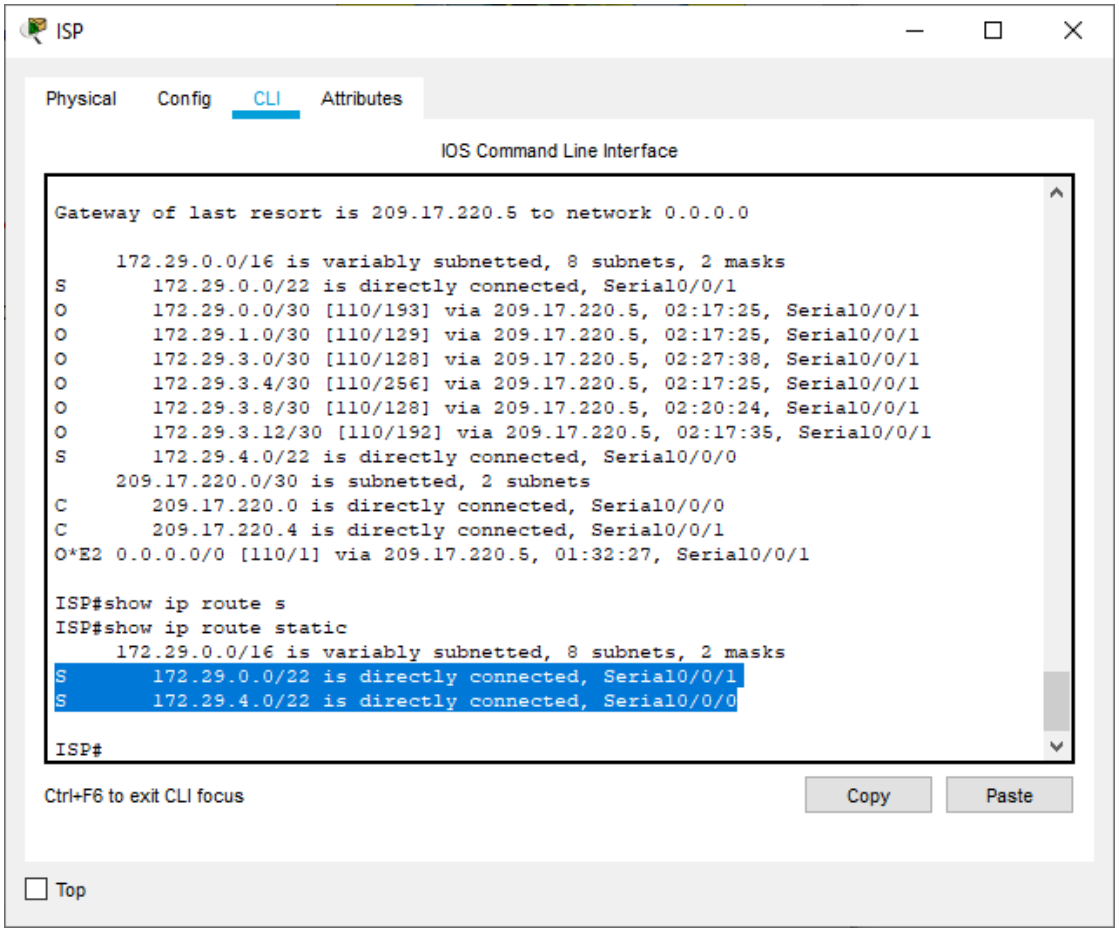
Figura 31. Verificación de rutas redundantes en Medellin 1



Fuente: elaboración propia

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

Figura 32. Verificación de rutas estaticas en ISP



Fuente: elaboración propia

6.2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

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

Para tipología diseñada fueron tenidas en cuenta dichas interfaces pasivas que se deshabilitaron en la configuración de cada router, las cuales fueron;

MEDELLIN2 (config-router)#passive-interface f0/1

BOGOTA3 (config-router)#passive-interface f0/1

6.2.4 Parte 4: Verificación del protocolo OSPF.

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

Las siguientes son las configuraciones asignada a cada router en la aplicación del protocolo OSPF:

Configuración OSPF V2 para el router MEDELLIN1

MEDELLIN1 (config)#router ospf 1

MEDELLIN1 (config-router)#router-id 2.2.2.2

MEDELLIN1 (config-router)# network 172.29.6.0 0.0.0.255 area 0

MEDELLIN1 (config-router)# network 172.29.6.12 0.0.0.255 area 0

MEDELLIN1 (config-router)# network 172.29.6.8 0.0.0.255 area 0

Configuración OSPF V2 para el router MEDELLIN2

MEDELLIN2 (config)#router ospf 1

MEDELLIN2 (config-router)#router-id 3.3.3.3

MEDELLIN2 (config-router)#passive-interface f0/1

MEDELLIN2 (config-router)# network 172.29.6.4 0.0.0.3 area 0

MEDELLIN2 (config-router)# network 172.29.6.0 0.0.0.3 area 0

MEDELLIN2 (config-router)# network 172.29.4.0 0.0.0.255 area 0

Configuración OSPF V2 para el router MEDELLIN3

MEDELLIN3 (config)#router ospf 1

MEDELLIN3 (config-router)#router-id 4.4.4.4

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

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

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

MEDELLIN3 (config-router)# network 172.29.4.128 0.0.0.255 area 0

Configuración OSPF V2 para el router BOGOTA1

BOGOTA1 (config)#router ospf 1

BOGOTA1 (config-router)#router-id 5.5.5.5

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

BOGOTA1 (config-router)# network 172.29.3.0 0.0.0.3 area 0

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

Configuración OSPF V2 para el router BOGOTA2

BOGOTA2 (config)#router ospf 1

BOGOTA2 (config-router)#router-id 6.6.6.6

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

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

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

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

Configuración OSPF V2 para el router BOGOTA3

BOGOTA3 (config)#router ospf 1

BOGOTA3 (config-router)#router-id 7.7.7.7

BOGOTA3 (config-router)#passive-interface f0/1

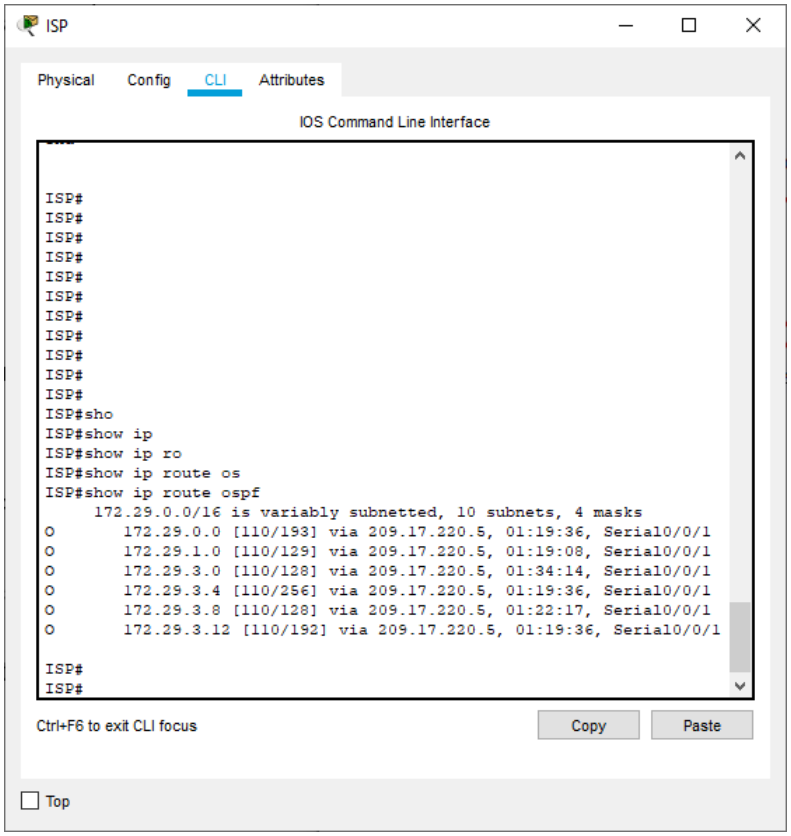
BOGOTA3 (config-router)# network 172.29.3.8 0.0.0.3 area 0

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

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

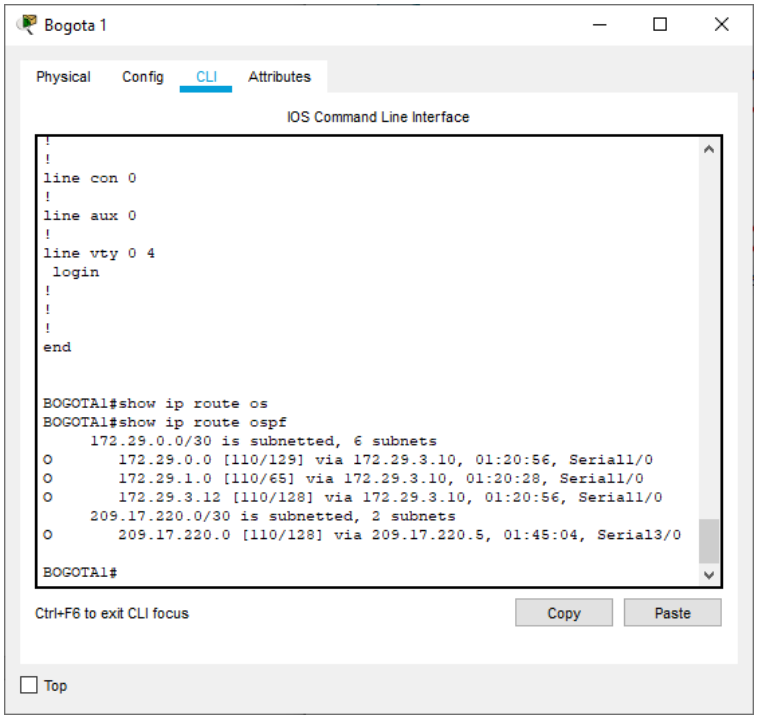
b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Figura 33. Verificación de configuración base de datos OSPF al router ISP



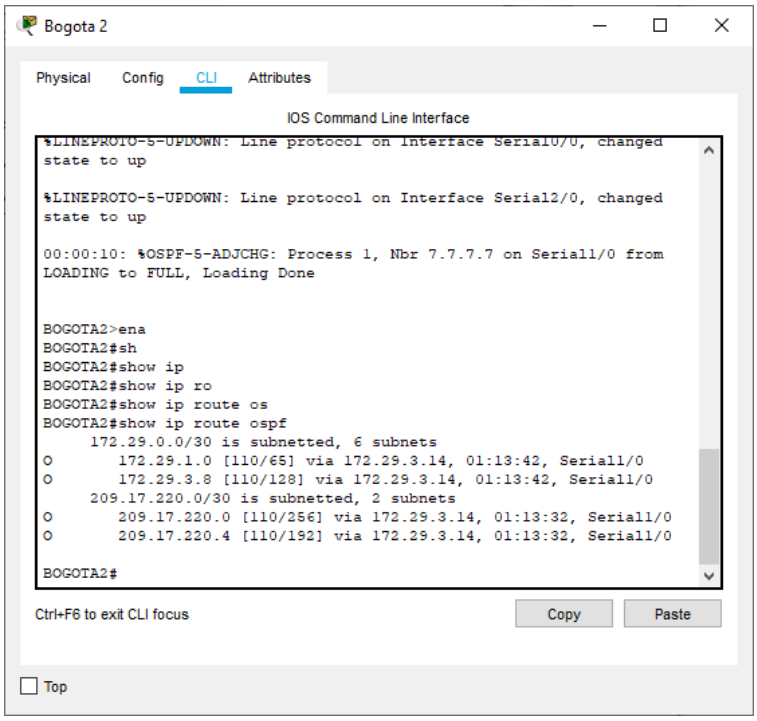
Fuente: elaboración propia

Figura 34. Verificación de configuración base de datos OSPF al router Bogota 1



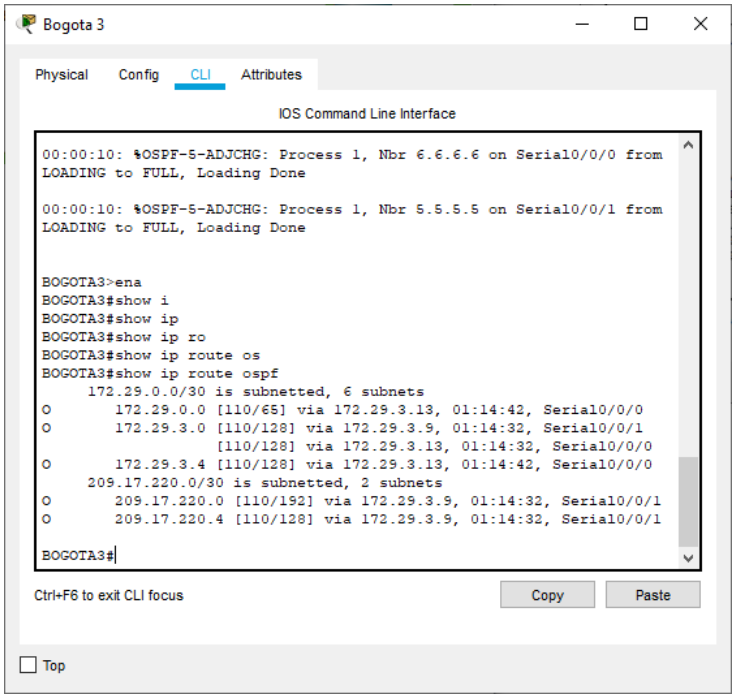
Fuente: elaboración propia

Figura 35. Verificación de configuración base de datos OSPF al router Bogota 2



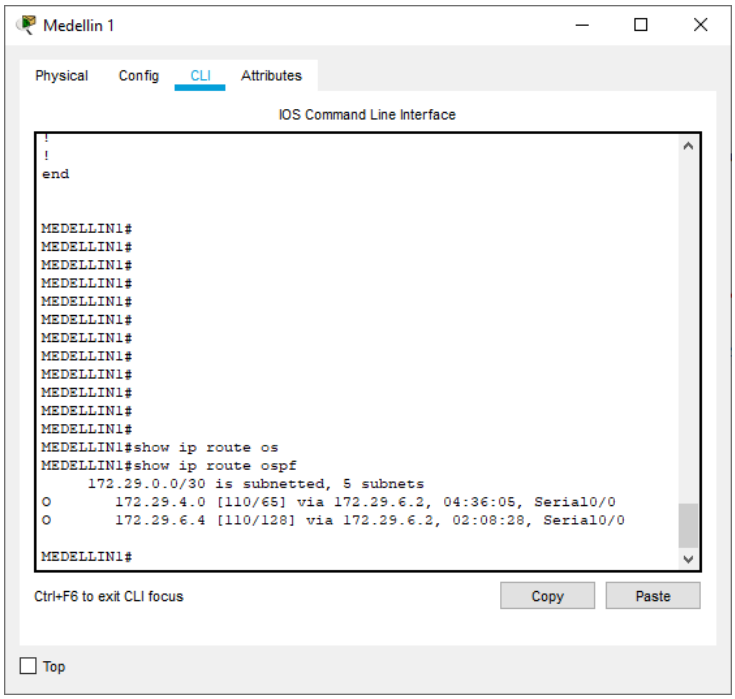
Fuente: elaboración propia

Figura 36. Verificación de configuración base de datos OSPF al router Bogota 3



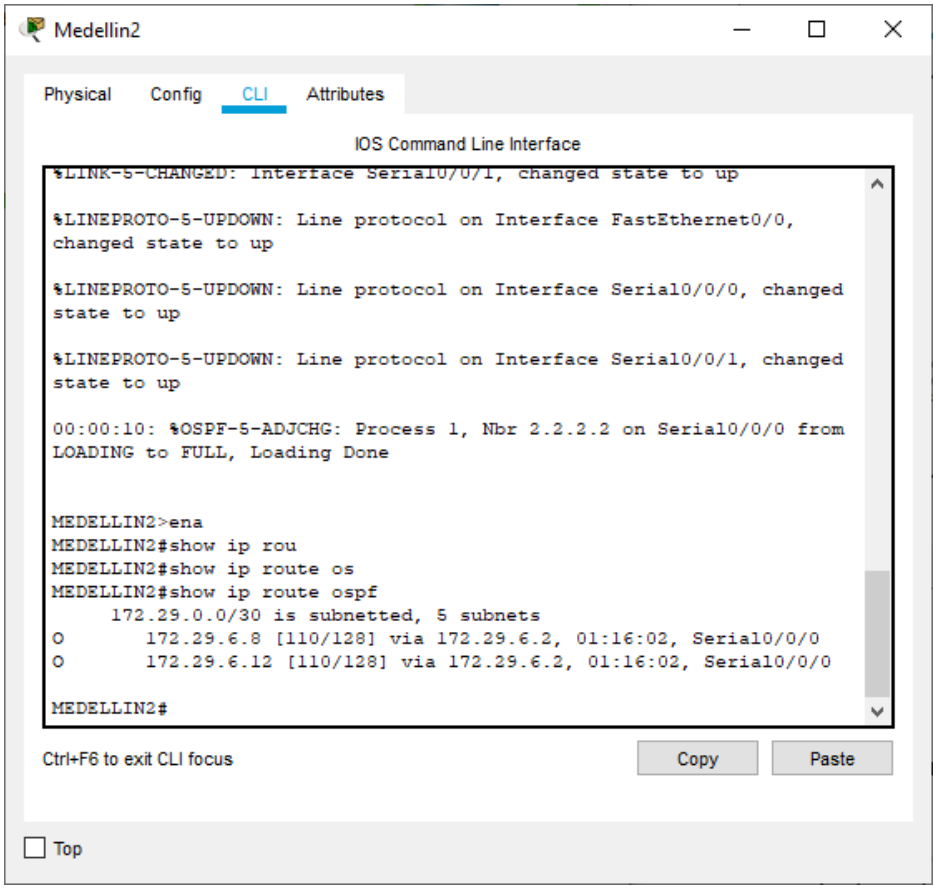
Fuente: elaboración propia

Figura 37. Verificación de configuración base de datos OSPF al router Medellin 1



Fuente: elaboración propia

Figura 38. Verificación de configuración base de datos OSPF al router Medellin 2



Fuente: elaboración propia

6.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Se ejecuta los siguientes comandos en ISP

ISP>enab

ISP#config t

ISP(config)#username MEDELLIN1 password cisco

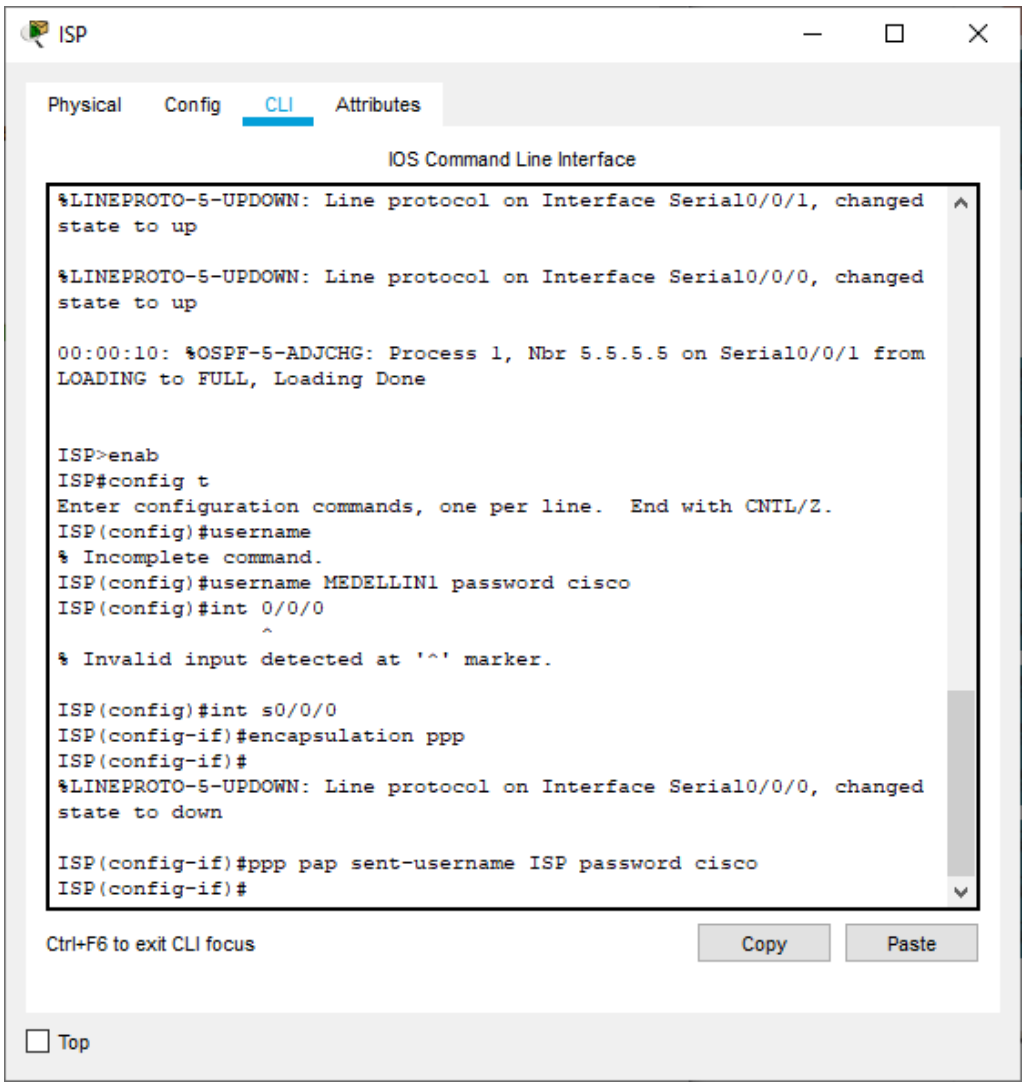
ISP(config)#int s0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication pap

ISP(config-if)#ppp pap sent-username ISP password cisco

Figura 39. Configuración de autenticación PAP en router ISP



Fuente: elaboración propia

MEDELLIN1>enable

MEDELLIN1#conf t

MEDELLIN1(config)#username ISP password cisco

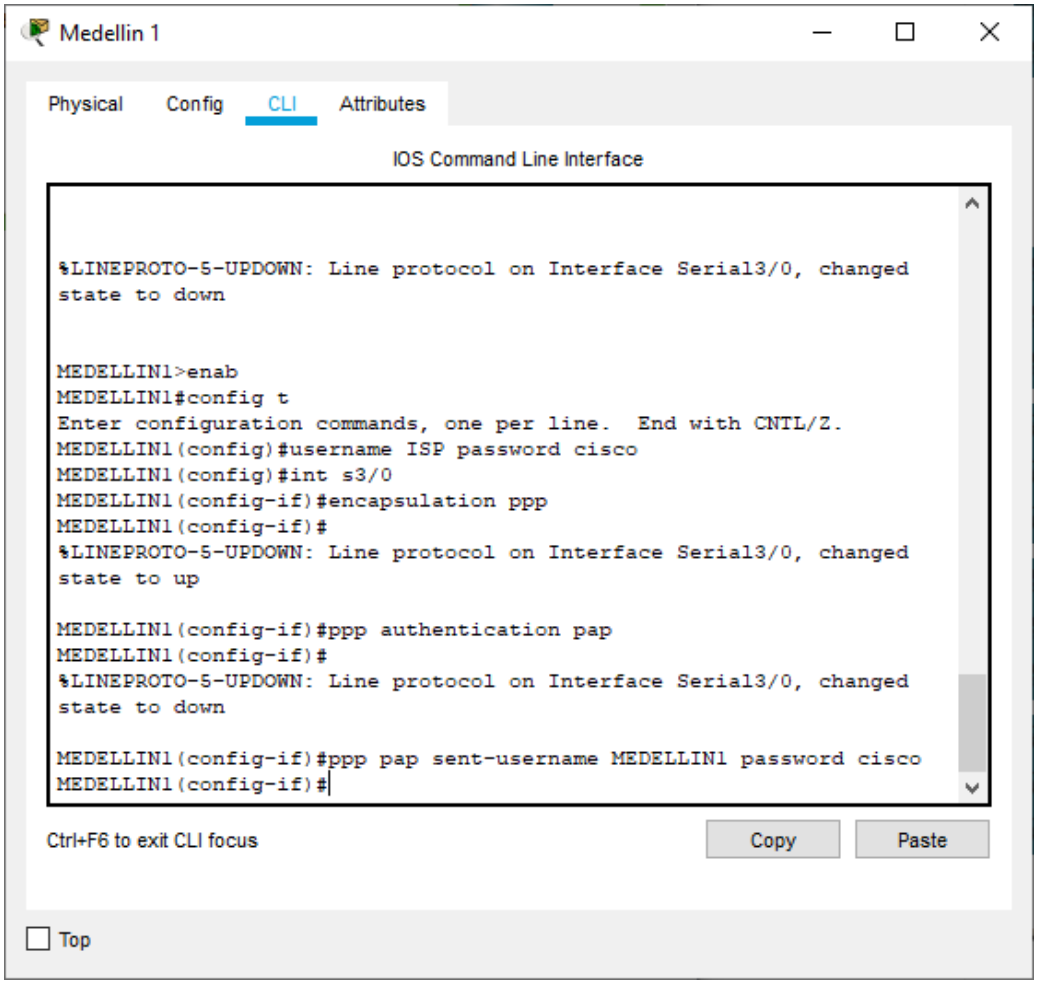
MEDELLIN1(config)#int s3/0

MEDELLIN1(config-if)#encapsulation ppp

MEDELLIN1(config-if)#ppp authentication pap

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

Figura 40. Configuración de autenticación PAP en router Medellin 1



Fuente: elaboración propia

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

Se ejecutan los siguientes comandos en router ISP

ISP#enab

ISP#config t

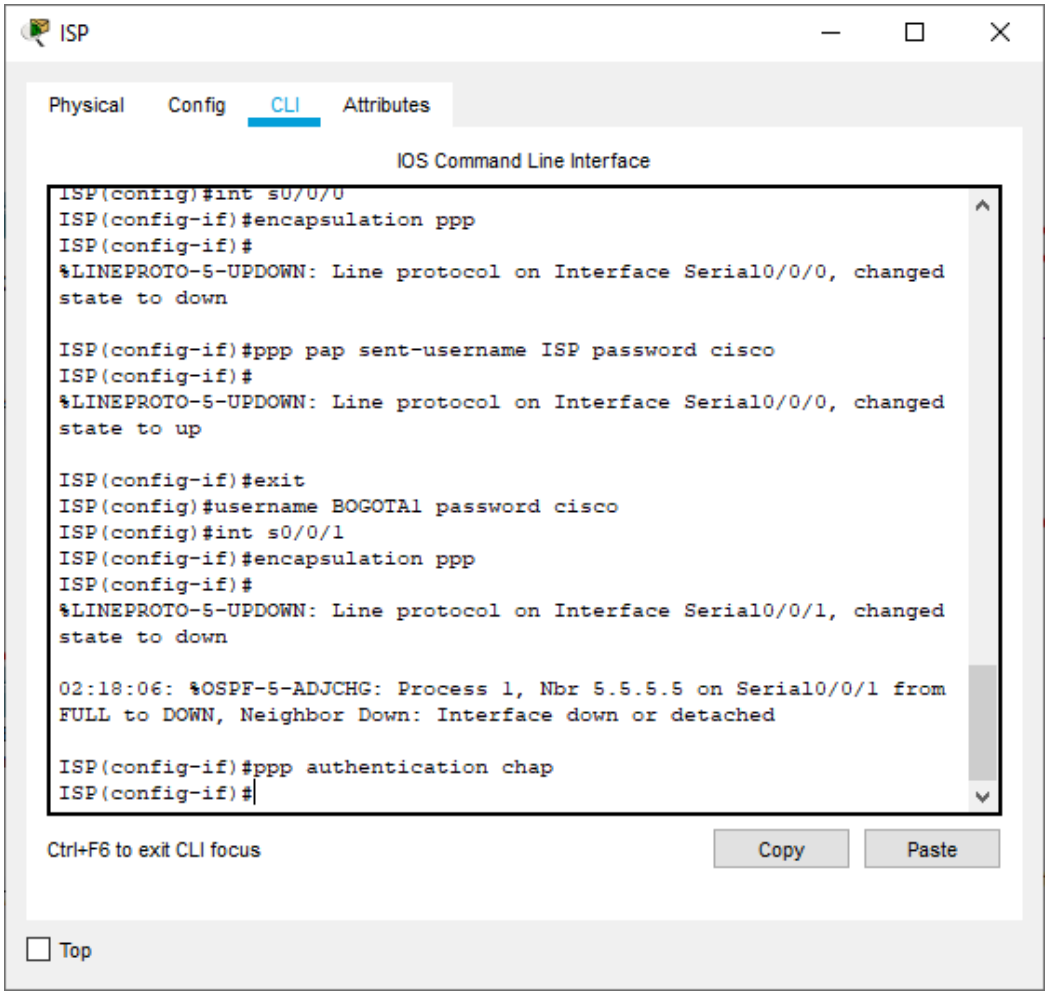
ISP(config)#username BOGOTA1 password cisco

ISP(config)#int s0/0/1

ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication chap

Figura 41. Configuración autenticación CHAP en router ISP



Fuente: elaboración propia

Se ejecutan los siguientes comandos en router BOGOTA1

BOGOTA1>enab

BOGOTA1#config t

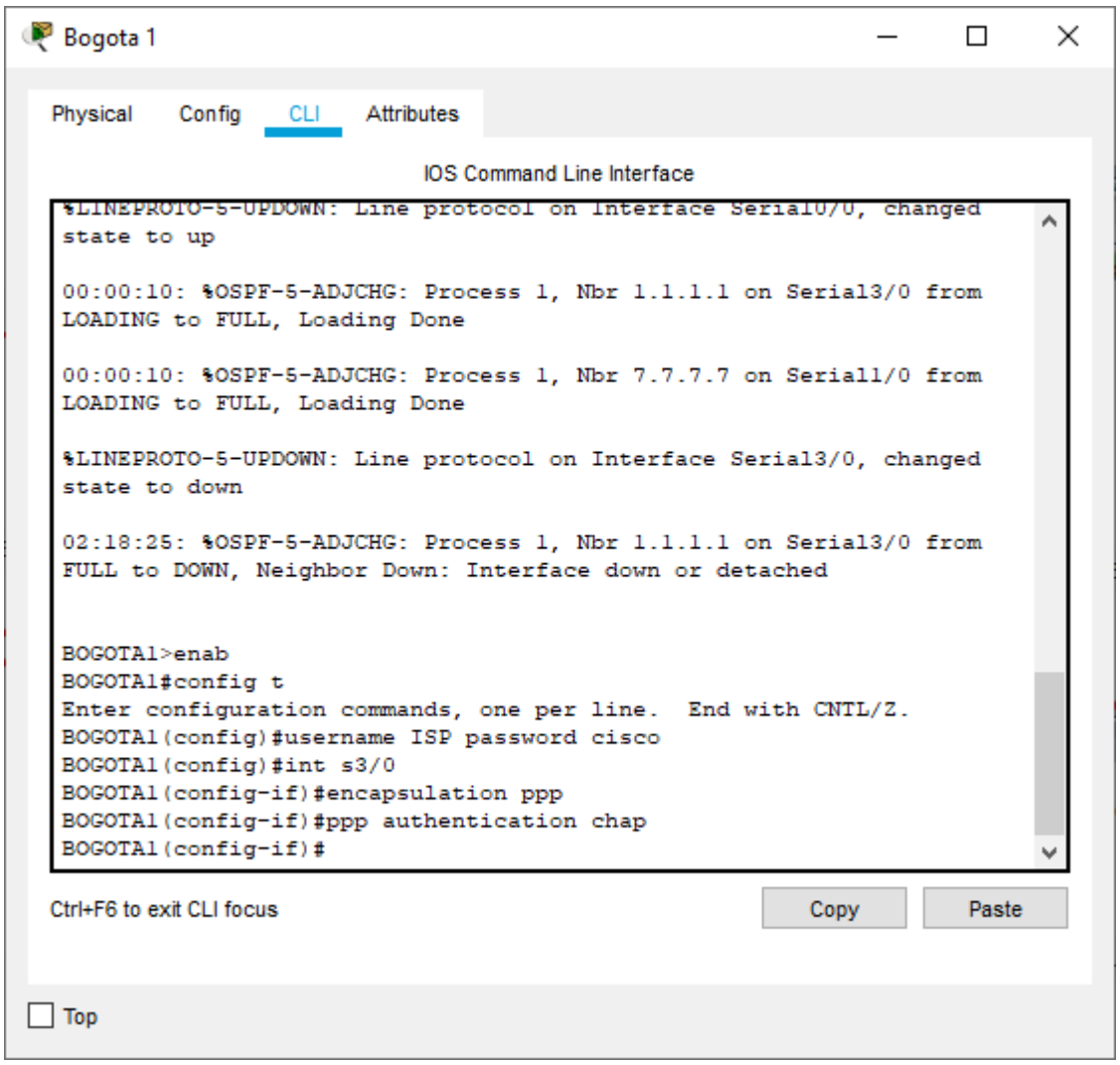
BOGOTA1(config)#username ISP password cisco

BOGOTA1(config)#int s3/0

BOGOTA1(config-if)#encapsulation ppp

BOGOTA1(config-if)#ppp authentication chap

Figura 42. Configuración autenticación CHAP en router Bogota 1



Fuente: elaboración propia

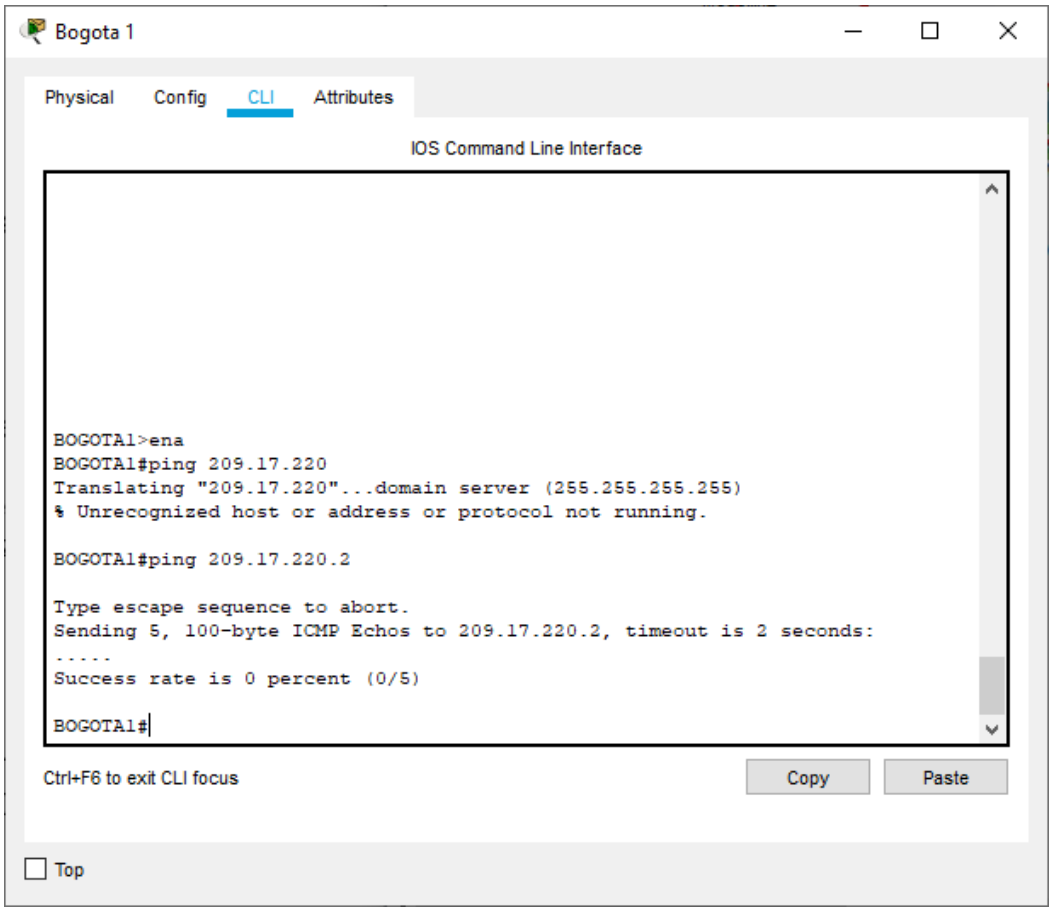
6.2.6 Parte 6: Configuración de PAT.

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

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

Al realizar ping del router Bogota1 al router Medellin 1 se evidencia que no se tiene respuesta

Figura 43. Verificación ping Bogotá 1 a Medellin 1



Fuente: elaboración propia

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>enab

MEDELLIN1#config t

MEDELLIN1(config)# ip nat inside source static 172.29.4.0 0.0.0.255

MEDELLIN1(config)#int s3/0

MEDELLIN1(config-if)#ip nat outside

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#int s1/0

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#int s2/0

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#int s0/0

MEDELLIN1(config-if)#ip nat inside

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>enab

BOGOTA1#conf t

BOGOTA1(config)# ip nat inside source static 172.29.0.0 0.0.0.255

BOGOTA1(config)#int s3/0

BOGOTA1(config-if)#ip nat outside

BOGOTA1(config-if)#ip nat intside

BOGOTA1(config-if)#int s0/0

BOGOTA1(config-if)#ip nat inside

BOGOTA1(config-if)#int s1/0

BOGOTA1(config-if)#ip nat inside

BOGOTA1(config-if)#int s2/0

BOGOTA1(config-if)#ip nat inside

6.2.7 Parte 7: Configuración del servicio DHCP.

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

Configuración DHCP en MEDELLIN2

MEDELLIN2>ena

MEDELLIN2#config t

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133

MEDELLIN2(config)#ip dhcp pool MEDELLIN2

MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128

MEDELLIN2(dhcp-config)#default-router 172.29.4.1

MEDELLIN2(dhcp-config)#dns-server 8.8.8.8

MEDELLIN2(dhcp-config)#exit

MEDELLIN2(config)#ip dhcp pool MEDELLIN3

MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128

MEDELLIN2(dhcp-config)#default-router 172.29.4.129

MEDELLIN2(dhcp-config)#dns-server 8.8.8.8

MEDELLIN2(dhcp-config)#exit

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

Creación de direccionamiento a MEDELLIN3.

MEDELLIN3>en

MEDELLIN3#conf t

MEDELLIN(config)#Int fa3/0

MEDELLIN3(config-if)#ip helper-addres 172.29.6.5

MEDELLIN(config-if)#exit

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

Creación del direccionamiento en Bogota2

BOGOTA2>ena

BOGOTA2#conf t

BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5

BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5

BOGOTA2(config)#ip dhcp pool BOG2

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

BOGOTA2(dhcp-config)#exit

BOGOTA2(dhcp-config)#ip dhcp pool BOG3

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

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

Creación de direccionamiento en Bogotá3.

BOGOTA>ena

BOGOTA#conf t

BOGOTA(config)#int s2/0

BOGOTA(config-if)#ip helper-address 172.29.3.13

6.2.7 Análisis de resultados escenario 2

En el desarrollo del escenario 2, se volvió a poner en practica la configuración de dispositivos específicamente router, donde se trabajo exclusivamente dichos dispositivos para la conectividad de varias sedes.

Para este modelo se trabajaron los temas de enrutamiento con el protocolo OSPF ver 2, la configuración de encapsulamiento y autenticación PPP donde se logro que el router ISP frente al router MEDELLIN1 se configurara con autenticación PAT, mientras que el router BOGOTA1 frente a ISP se implementara la autenticación CHAT

Para este segundo escenario se logra entender mejor la utilidad de configuración de los servicios DHCP para asignaciones de dirección IP cuando se cuentan con un numero mayor de Host.

El Desarrollo de este escenario 2 me permitirá implementarlo en la empresa donde laboró, ya que cuenta con dos sedes y una tercera en proceso de apertura. De estas sedes la conexión solo se trabaja por VPN.

En este escenario debo manifestar que encontré dificultad para el manejo de interfaz de conexión entre los siete routers, donde se presentó confusión en la entrada y salida de datos de acuerdo con el enrutamiento establecido. Debo expresar que se repitió el diseño y configuración de dispositivos de dicho escenario al no lograr la propagación del protocolo OSPF y la configuración del servicio DHCP, logrando así identificar el error mal codificado en los procesos de configuración a través del CLI.

3. CONCLUSIONES

Culminado el proceso de aprendizaje y de prácticas puedo inferir que se ha adquirido habilidades en el manejo de networking. Dicen que la practica hace al maestro de lo cual en cierta manera es verdad, luego de revisada la documentación bibliográfica sugerida y leído todos los módulos que ofrecen en la plataforma educativa de CCNA1 y CCNA2, considero que la práctica de cada uno de los temas fortalece y afianza dichos conocimientos y permite que se adquieran habilidades y competencias para la productividad en el campo de la ingeniería de sistemas.

Debo señalar que la columna principal para el aprendizaje de redes es el software Packet Tracer, que acerca al estudiante a la simulación y comportamiento muy real en la configuración y puesta a producción de dispositivos como switches, routers, hubs y servidores entre otros.

Para el escenario 1 se concluye que la configuración de dispositivos dependerá entre otros, del correcto diseño de la topología de red, la identificación y configuración de interfaces para cada dispositivo, así como el correcto direccionamiento de dichas interfaces. Otro aspecto para destacar en el desarrollo de este escenario es el aprendizaje adquirido en la configuración y direccionamiento IP de conectividad IPv4 e IPv6 en dispositivos como routers, pc, switchs y servidores. La configuración de parámetros básicos de dispositivos en lo referente a temas de seguridad en switch y routing entre Vlan, por otro lado, se implementan protocolos de routing OSPF y RIP versión 2 para la propagación de rutas predeterminadas.

Para el escenario 2 se aprendió a realizar la configuración de redes LAN para donde se simula la interconexión entre ciudades a través de dispositivos router. En dicho escenario se trabajo con la aplicación de protocolos de enrutamiento como OSPF versión 2, configuración de enlaces aplicando autenticación PPP.

Por último, se logra aprender a administrar y automatizar la asignación de direcciones IP implementando el protocolo DHCP para configurar automáticamente parámetros de configuración IP en host y NAT para traducir direcciones e intercomunicar redes de distintas clases.

4. REFERENCIAS BIBLIOGRAFICAS

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

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assetss3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

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

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

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

CISCO. (2020). Networking Academy. CCNA1 Routing and Switching: Introducción a las redes. Routing y switching de CCNA2: Principios básicos de routing y switching. Recuperado de la pagina web: https://www.netacad.com/

CISCO. (2017). 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

CISCO. (2017). 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

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYeiNT1IhgCT9VCtl_pLtPD9