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

JAIRO ARTURO ESPITIA ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
DUITAMA
2020

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

JAIRO ARTURO ESPITIA ROJAS

Diplomado de opción de grado presentado para optar el título de INGENIERÍA ELECTRÓNICA

GUSTAVO ADOLFO RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
DUITAMA
2020

Nota de Aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Duitama, 30 de Mayo de 2020 (30, 05, 2020)

CONTENIDO

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

GLOSARIO

DNS: La sigla DNS proviene de la expresión inglesa Domain Name System: es decir, Sistema de Nombres de Dominio. Se trata de un método de denominación empleado para nombrar a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet).

PREFIJO IP: Es una forma particular de expresar las direcciones de red y sus máscaras a partir de identificar solamente la cantidad de bits que se encuentran en uno en la máscara de subred.

MÁSCARA DE SUBRED: La máscara de subred es particularmente necesaria al momento de señalar la dirección de red correspondiente a cada subred, y que es la que se encuentra referenciada en la tabla de enrutamiento.

PROTOCOLOS DE RED: Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

ROUTER: Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

INTERFAZ: Se denomina interfaz a cualquier medio que permita la interconexión de dos procesos diferenciados con un único propósito común. Se conoce como Interfaz Física a los medios utilizados para la conexión de un computador con el medio de transporte de la red.

RESUMEN

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

PALABRAS CLAVE: CISCO, Conmutación, Enrutamiento, Redes, Sistemas.

ABSTRACT

The selected evaluation "Practical skills test" is part of the evaluative activities of the CCNA Deepening Diploma, and seeks to identify the degree of development of competencies and skills that were acquired throughout the diploma. The essential thing is to test the levels of understanding and problem solving related to various aspects of Networking.

KEYWORDS: CISCO, Switching, Routing, Networks, Systems.

1. INTRODUCCIÓN

Para esta actividad, se realiza la solución a dos escenarios propuestos, donde se soportan con la respectiva documentación, las diferentes instrucciones y soportes gráficos que demuestren la ejecución y aplicación de los conocimientos adquiridos durante el transcurso del desarrollo del diplomado de profundización Cisco.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

Al final, cada proceso está debidamente documentado y consta de una evidencia que determina la operación y aplicación de cada una de las instrucciones requeridas para el cumplimiento de lo solicitado en cada uno de los escenarios y además de verificar el funcionamiento y el comportamiento de la red a medida que se va implementando cada uno de los cambios y configuración de los dispositivos.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Aplicar el respectivo enrutamiento enfocado a la configuración de dos escenarios propuestos que asemejan una situación problema de la vida cotidiana.

2.2 OBJETIVOS ESPECÍFICOS

Identificar los dispositivos que son utilizados para la construcción de la topología de red, permitiendo así la configuración y la implementación de las instrucciones de acuerdo a la topología seleccionada.

Realizar la configuración necesaria para la implementación de los protocolos, routing, DHCP, NAT, RIPv2 dando solución a los problemas expuestos en cada uno de los escenarios.

Verificar que las medidas de configuración utilizadas cumplan con los lineamientos expuestos en los escenarios propuestos y funcionen correctamente.

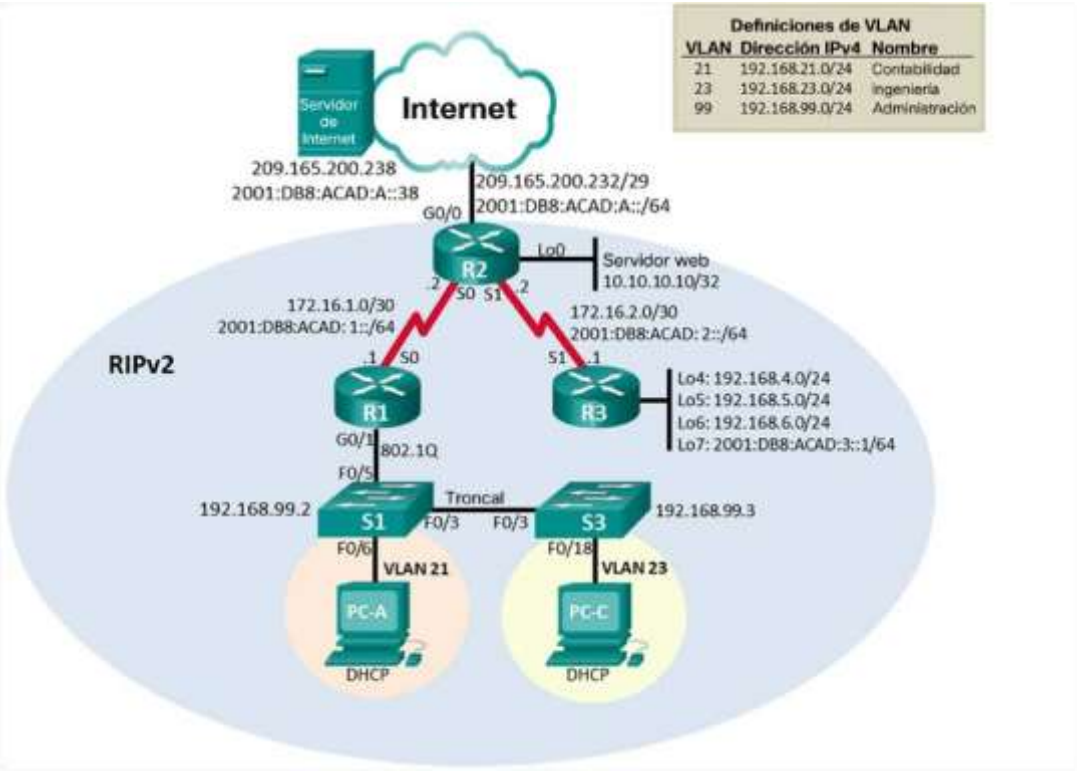
3. DESARROLLO DEL PROYECTO

3.1. Escenario 1

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

Topología

Figura 1. Topología de configuración del escenario 1



Fuente: Autor del proyecto

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	Router>enable Router#erase Router#erase startup-config Router#
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase sta Switch#erase startup-config
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash: Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Switch#

Tabla 1.Indicaciones para la verficación de la inicialización del router.

En este paso, se reinician cada uno de los Routers y switches a utilizar, con el fin de asegurar la disponibilidad y evitar configuraciones existentes no deseadas al momento de trabajar el escenario.

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):

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248

Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 2.Tareas de configuración del servidor de Internet.

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

De acuerdo a los direccionamientos estipulados en la topología, se procede a configurar el servidor de internet asignando la dirección IPv4, la máscara de subred para IPv4, el Gateway predeterminado, la dirección y gateway predeterminado IPv6.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado#

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

Tabla 3.Tarea de configuración de R1.

Nota: Todavía no configure G0/1.

De acuerdo a la topología, se procede a configurar los parametros de seguridad, etapas iniciales y direccionamiento a cada una de las interfaces en el router R1

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	

Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description R1 a R2 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)# R2(config-if)#exit
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description R2 a 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)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description R2 to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface lo0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

Tabla 4. Tarea de configuración de R2.

Al igual que en el anterior, se procede a realizar las configuraciones básicas y de seguridad en el Router R2, así como los direccionamientos en cada una de las interfaces a utilizar.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description R3 a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)#exit
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit

Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit.
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5. Tarea de configuración de R3.

En este paso, se configura los parametros básicos de R3, sus direccionamientos y asignaciones en cada una de las interfaces a utilizar.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohibe el acceso no autorizado#

Tabla 6.Tarea de configuración de S1.

Se configura la desactivación de la búsqueda DNS, las medidas de seguirdad a cada una de las líneas y se cifra el texto que no está cifrado, además de añadir un mensaje MOTD para los accesos no autorizados.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line con 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado#

Tabla 7.Configuraciones iniciales en S3.

Se configura la desactivación de la búsqueda DNS, las medidas de seguirdad a cada una de las líneas y se cifra el texto que no está cifrado, además de añadir un mensaje MOTD para los accesos no autorizados.

Paso 7: Verificar la conectividad de la red

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

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

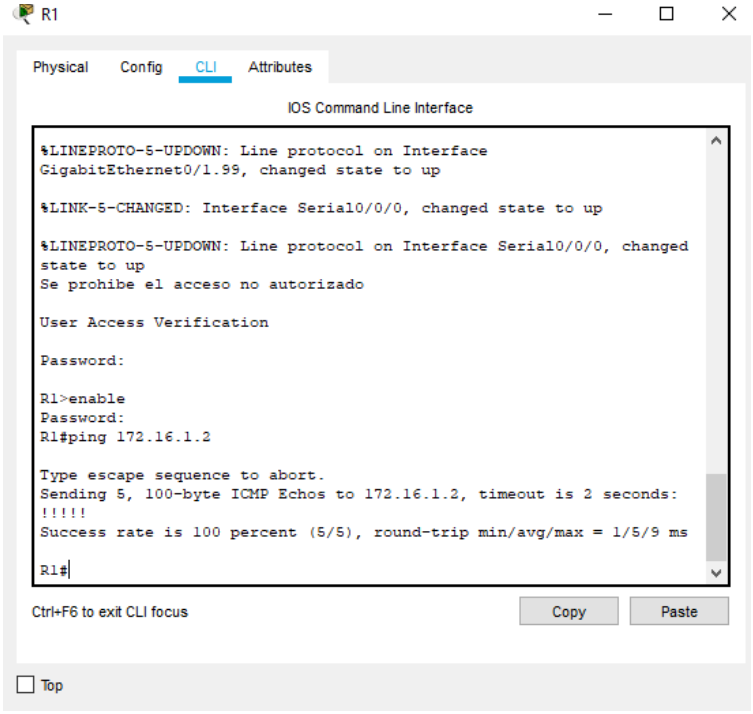
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!!

			Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/9 ms
R2	R3, S0/0/1	172.16.2.1	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 = 5/6/10 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

Tabla 8.Verificación de la conectividad.

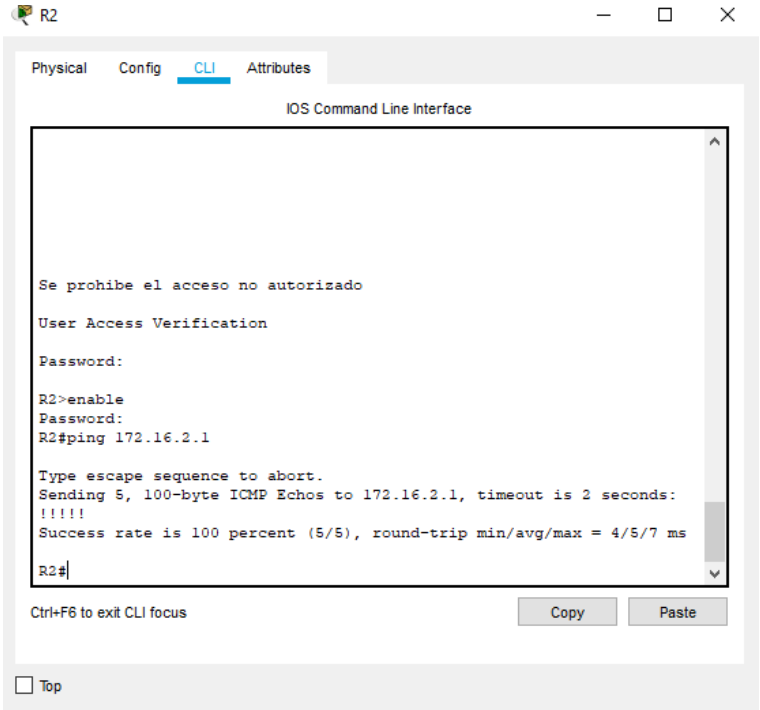
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 2. Ping desde el router R1 a R2 y a S0/0/0.



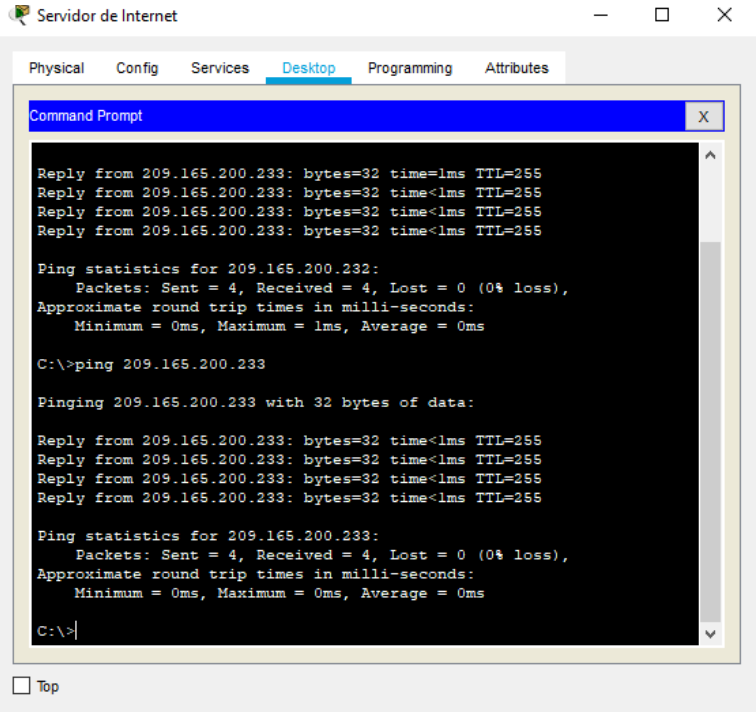
Fuente: Autor del proyecto

Figura 3. Ping desde el router R2 a R3 y a S0/0/1



Fuente: Autor del proyecto

Figura 4. Ping desde el Servidor de Internet al Gateway



Fuente: Autor del proyecto

Se verifica que la configuración de cada uno de los dispositivos fue efectiva y se pueda enlazar entre ellos.

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:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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

Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1.
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

Tabla 9.Asignación de la configuración en S1.

Se configuran las respectivas VLANS que serán utilizadas para separar la topología, se asigna el direccionamiento a la VLAN 99 con el fin de tener un control SVI, se asigna el Gateway por defecto y se crea la respectiva interface troncal que comunica con el S3, así como con el enlace con el R1.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)# S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)# S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 23	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Tabla 10.Asignación de la configuración en S3.

Se configuran las respectivas VLANS que serán utilizadas para separar la topología, se asigna el direccionamiento a la VLAN 99 con el fin de tener un control SVI, se asigna el Gateway por defecto y se crea la respectiva interface troncal que comunica con el S1.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown R1(config-if)#exit

Tabla 11.Configuración de subinterfaces en R1.

En este paso, se configuran las subinterfaces que comunican el R1 con S1, se asignan los respectivos puertos como acceso, se enciende la interfaz principal.

Paso 4: Verificar la conectividad de la red

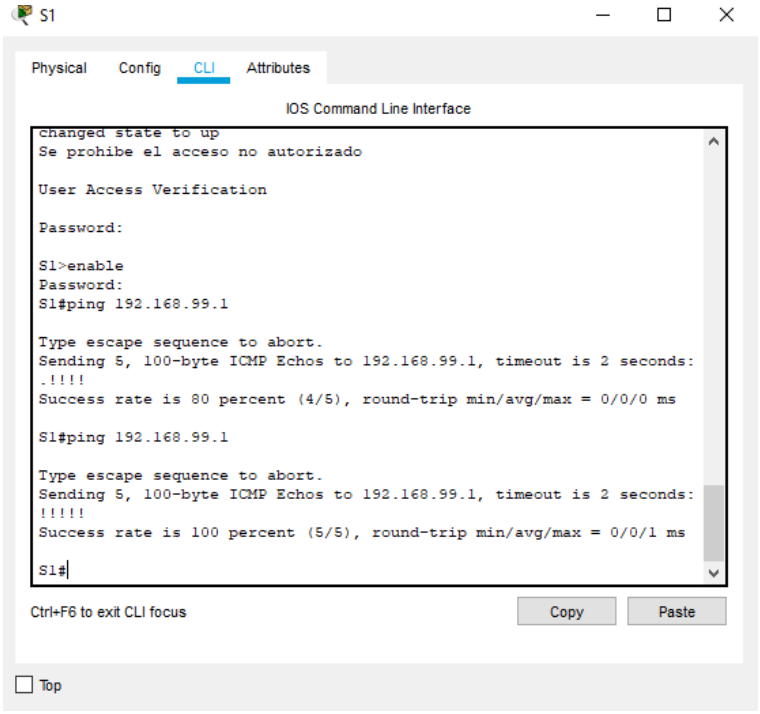
Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	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 = 0/0/0 ms S1#
S3	R1, dirección VLAN 23	192.168.23.1	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 S3#

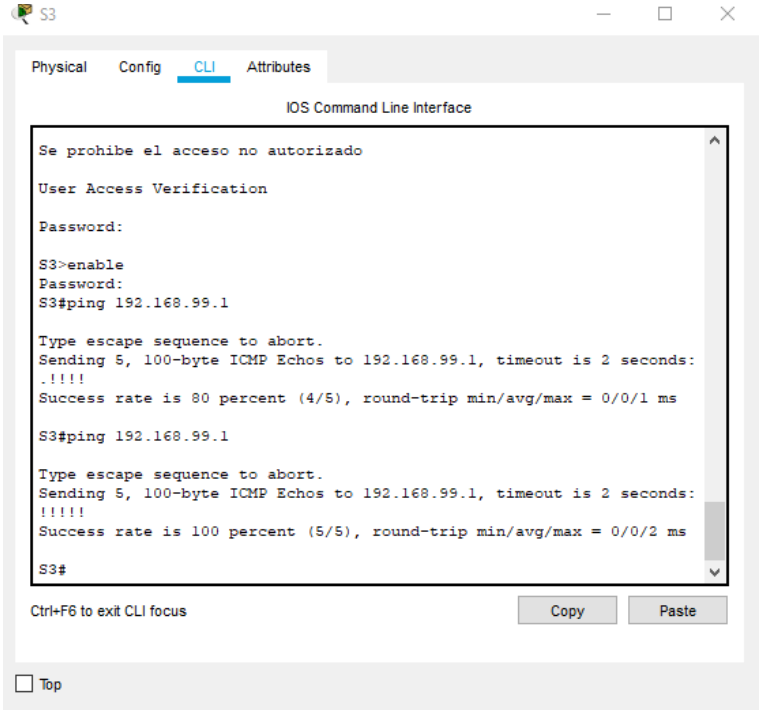
Tabla 12. Verificación de la conectividad entre los switches y el R1.

Figura 5. Ping desde el switch S1 al router R1 y a la dirección VLAN 99.



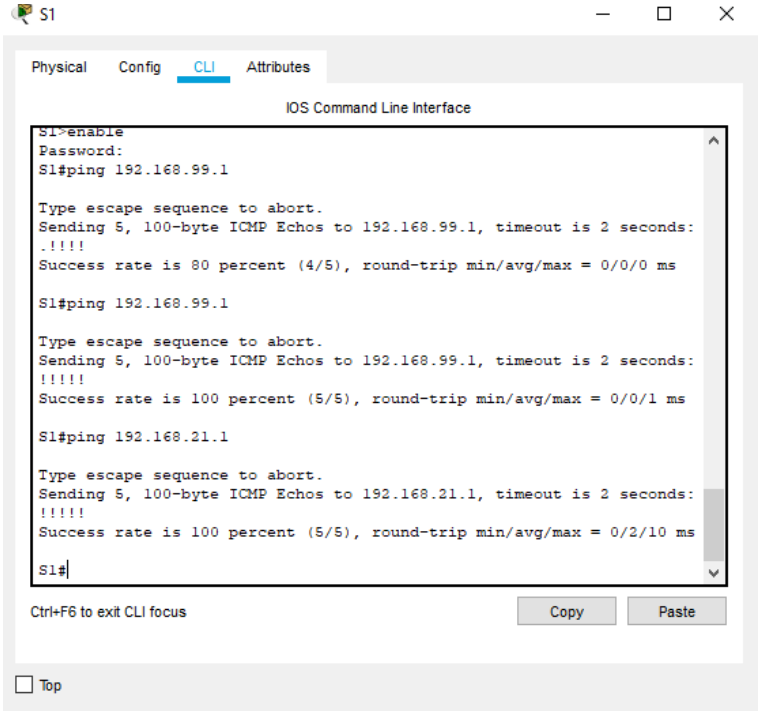
Fuente: Autor del proyecto

Figura 6. Ping desde el switch S3 al router R1 y a la dirección VLAN 99.



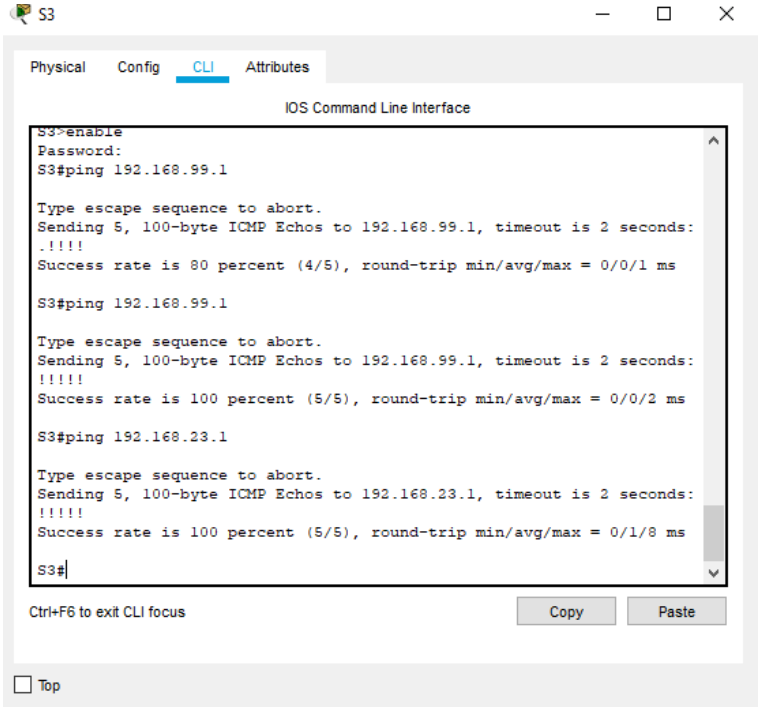
Fuente: Autor del proyecto

Figura 7. Ping desde el switch S1 al router R1 y a la dirección VLAN 21.



Fuente: Autor del proyecto

Figura 8. Ping desde el switch S3 al router R1 y a la dirección VLAN 23.



Fuente: Autor del proyecto

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:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route c C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gigabitEthernet 0/1.21 R1(config-router)#passive-interface gigabitEthernet 0/1.23 R1(config-router)#passive-interface gigabitEthernet 0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 13. Configuración del protocolo RIPv2 en el router R1.

Se asigna la configuración RIP en el router 1, se desactiva la sumarización automática y se configura las subinterfaces como pasivas.

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#do show ip route c C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 14. Configurar RIPv2 en el R2.

Se asigna la configuración RIP en el router 2, se desactiva la sumarización automática y se configura las subinterfaces como pasivas.

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2

Anunciar redes IPv4 conectadas directamente	R3(config-router)#do show ip route c C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6 R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 15. Configurar RIPv2 en el R3.

Se asigna la configuración RIP en el router 3, se desactiva la sumarización automática y se configura las subinterfaces como pasivas.

Paso 4: Verificar la información de RIP

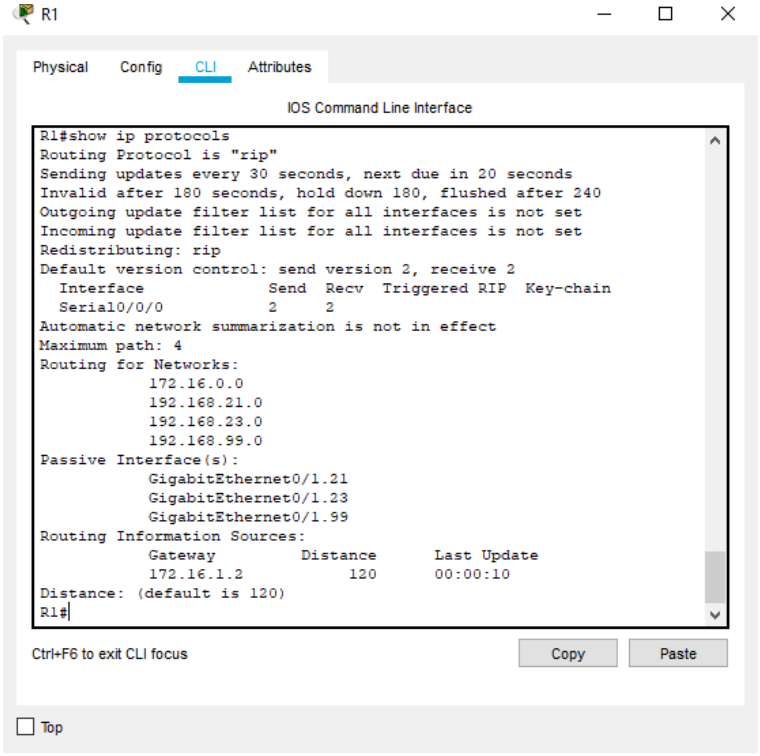
Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

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 rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show ip rip database

Tabla 16. Indica las validaciones de las configuraciones anteriores.

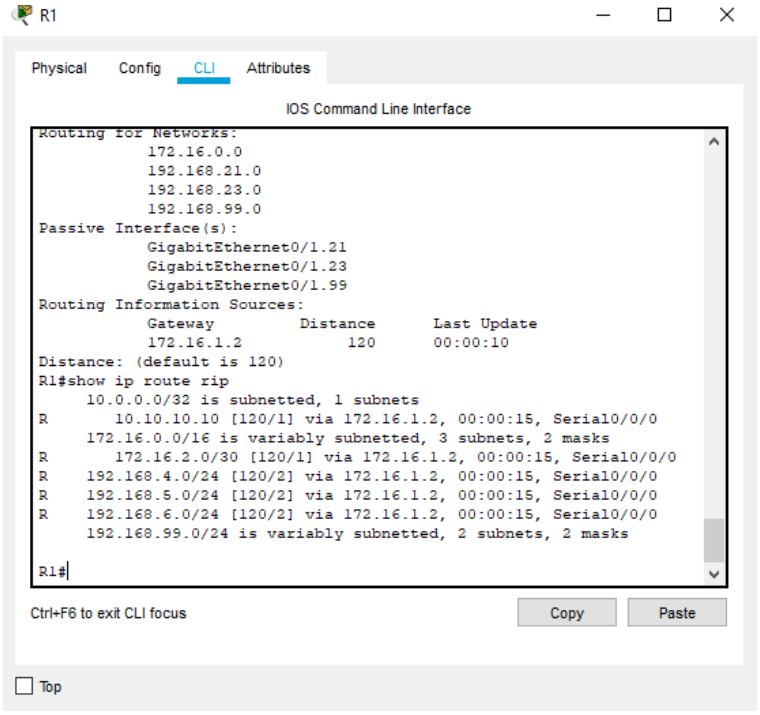
Se verifica a través de comandos el funcionamiento RIP, donde se evidencia las id del proceso, la id del Router, las redes de routing y las interfaces pasivas configuradas.

Figura 9. Verificación de las configuraciones en R1.



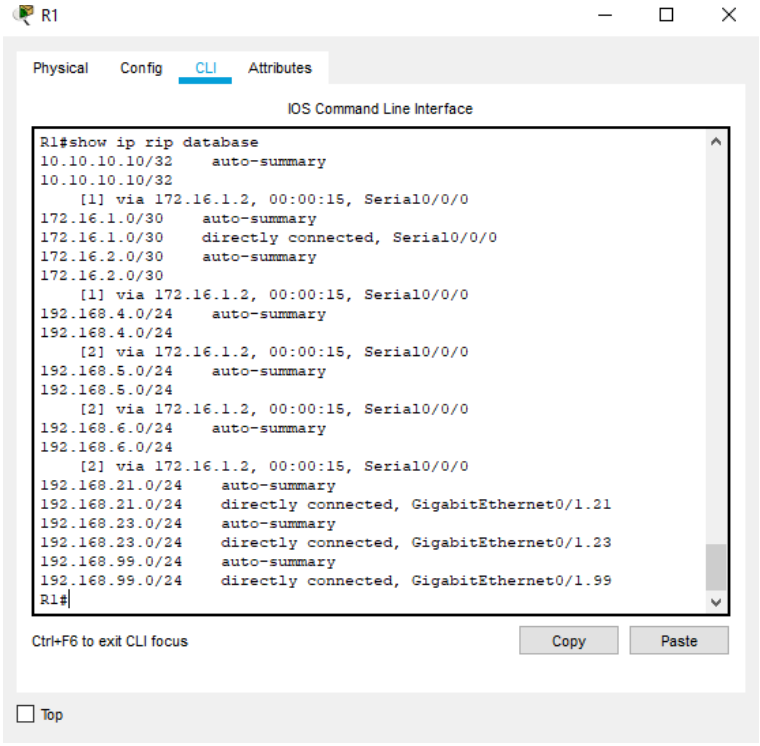
Fuente: Autor del proyecto

Figura 10. Verificación de rutas rip en R1.



Fuente: Autor del proyecto

Figura 11. Sección RIP en R1.



Fuente: Autor del proyecto

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

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

Tabla 17. Configuración del R1 como servidor de DHCP para las VLAN 21 y 23.

Se reservan las primeras 20 direcciones ip para la VLAN 21, se reserva de otras 20 direcciones ip para la VLAN 21. Se crea un pool DHCP, se le asigna un nombre, seasigna el gateway predeterminado, el router de defecto, nombre de dominio DNS, al igual para la VLAN 23.

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No soportado en el packet tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado en el packet tracer
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#interface serial0/0/0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#interface serial0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit

Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 18. Configuración NAT estática y dinámica en R2.

Se crea un usuario con los niveles de privilegio, se crea la nat estática para la dirección Loopback, se asigna a las interfaces y se configura una nat dinámica dentro de una ACL privada. Se defina la tradución dinámica de nat y el pool de direcciones.

Paso 3: Verificar el protocolo DHCP y la NAT estática

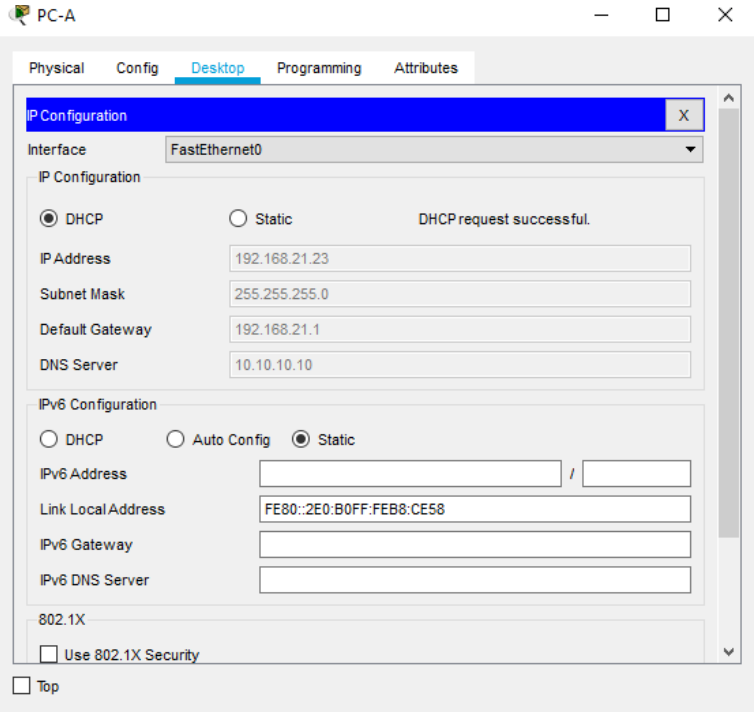
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Packet Tracer PC Command Line 1.0 C:\>ping 192.168.21.31 Pinging 192.168.21.31 with 32 bytes of data: Reply from 192.168.21.31: bytes=32 time=1ms TTL=128 Reply from 192.168.21.31: bytes=32 time<1ms TTL=128 Reply from 192.168.21.31: bytes=32 time<1ms TTL=128 Reply from 192.168.21.31: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.21.31: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\>
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

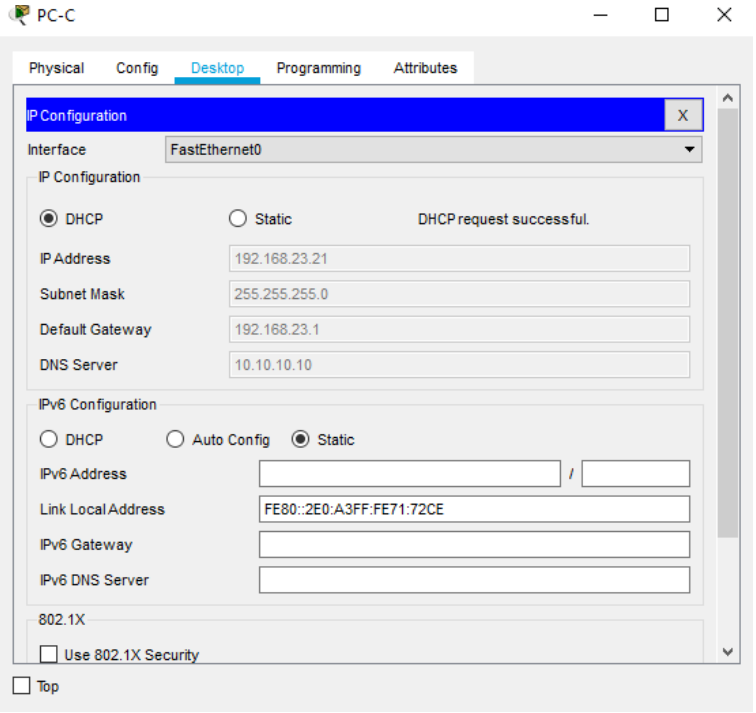
Tabla 19. Verificación del protocolo DHCP y la NAT estática.

Figura 12. Verificación DHCP en el PC-A.



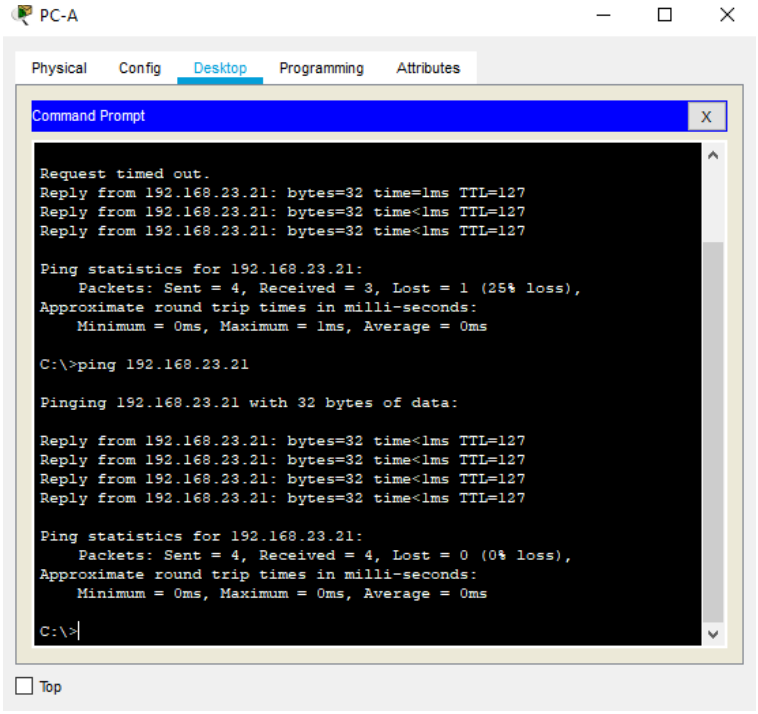
Fuente: Autor del proyecto.

Figura 13. Verificación DHCP en el PC-C.



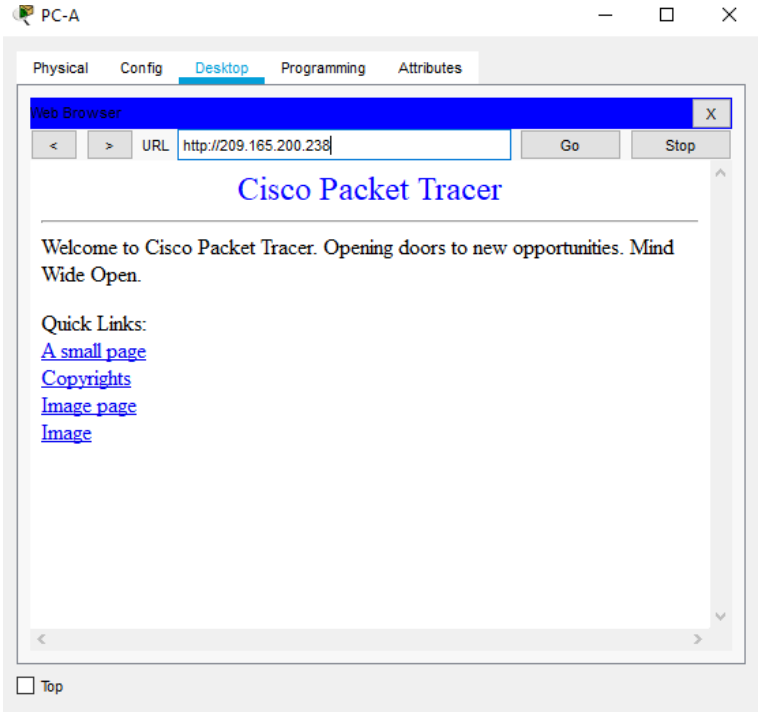
Fuente: Autor del proyecto.

Figura 14. Verificación ping entre PC-A y PC-C.



Fuente: Autor del proyecto.

Figura 15. Verificación del servidor web.



Fuente: Autor del proyecto.

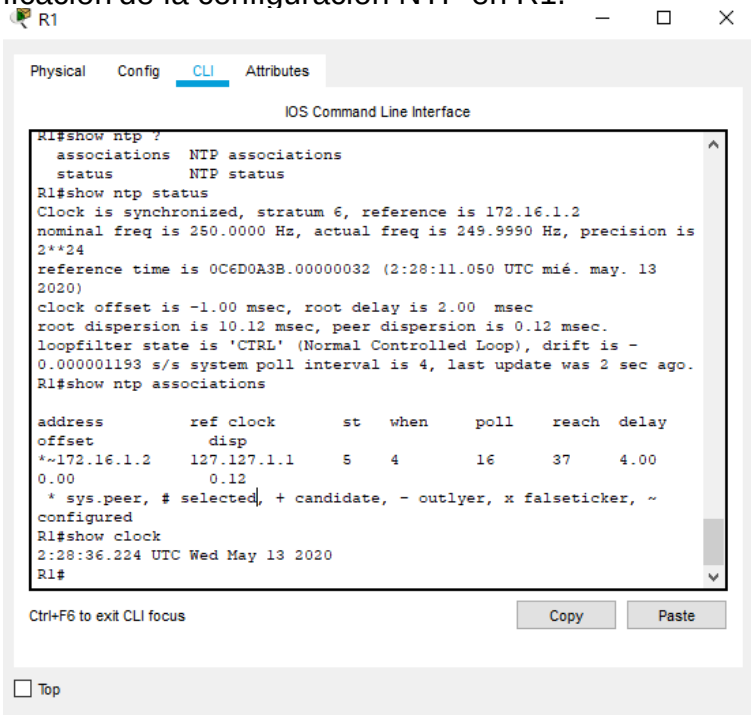
Se verifican que las configuraciones ACL y NAT funcionen correctamente y que las direcciones generadas hayan sido tomadas por los dispositivos finales.

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 02:22:50 13 May 2020
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp status Clock is synchronized, stratum 6, reference is 172.16.1.2 nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24 reference time is 0C6D0A3B.00000032 (2:28:11.050 UTC mié. may. 13 2020) clock offset is -1.00 msec, root delay is 2.00 msec root dispersion is 10.12 msec, peer dispersion is 0.12 msec. loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last update was 2 sec ago. R1#show ntp associations address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 4 16 37 4.00 0.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1#show clock 2:28:36.224 UTC Wed May 13 2020

Tabla 20. Asignación de NTP en R1 y R2.

Figura 16. Verificación de la configuración NTP en R1.



Fuente: Autor del proyecto.

Se configura la asignación de la fecha del reloj, se asigna master en R2 y el servidor en R1.

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

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

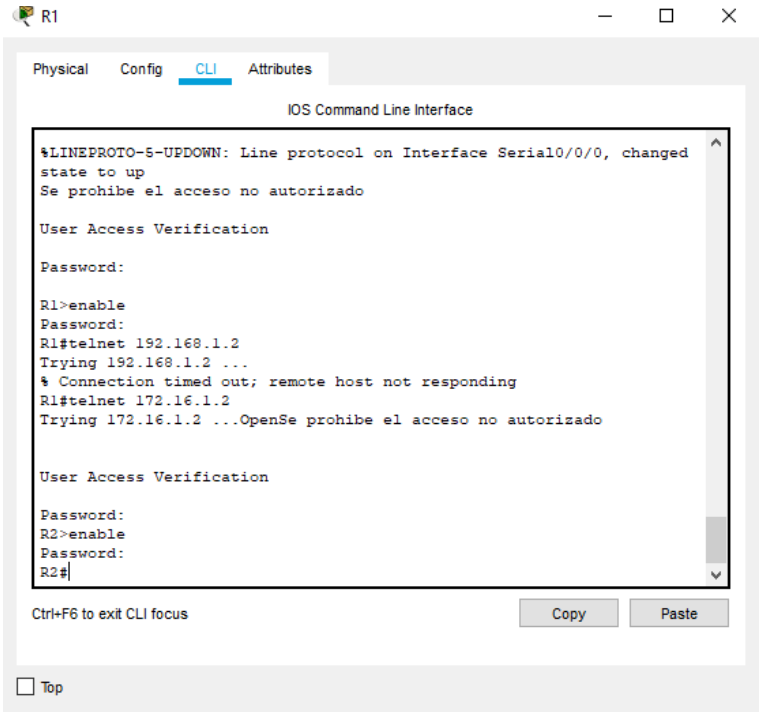
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#acc R2(config-line)#access R2(config-line)#access-class ADMIN-MGT in

Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#exit R2(config)#
Verificar que la ACL funcione como se espera	

Tabla 21. Restricciones de acceso a las líneas VTY en R2.

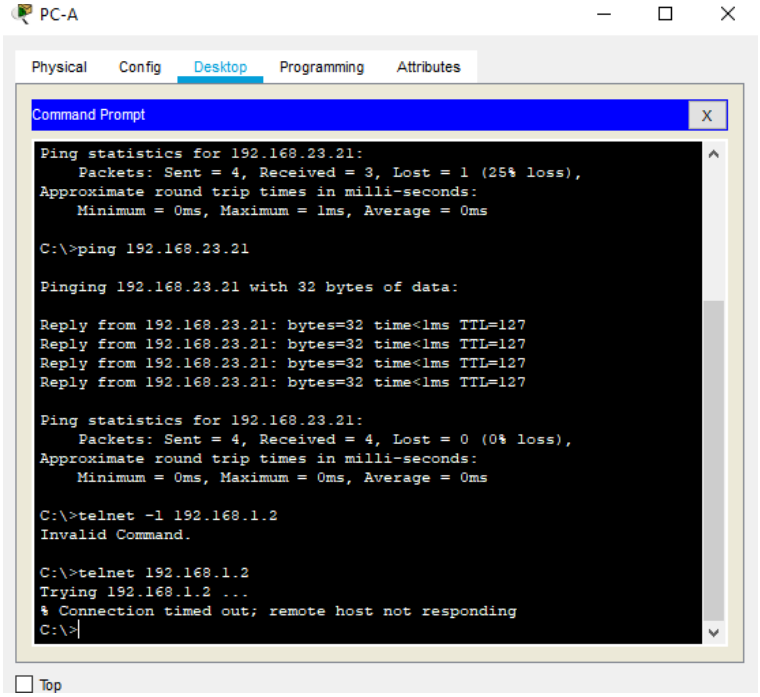
Se configura la lista de acceso para permitir que solo el R1 tenga acceso a R2, los demás son denegados. Además se configura una lista de acceso estándar en R2 para garantizar que solo una dirección de host tenga acceso a través de la línea VTY, ademas de asegurar el transporte de ingreso por Telnet.

Figura 17. Acceso Telnet desde R1.



Fuente: Autor del proyecto.

Figura 18. Acceso Telnet a R2 desde PC-A.



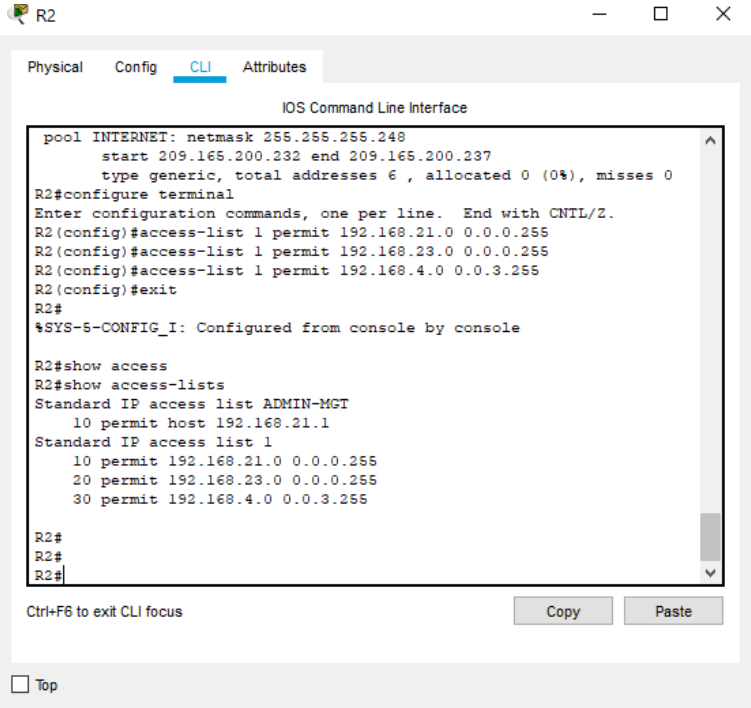
Fuente: Autor del proyecto.

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	
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface gi0/0 | include access list
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

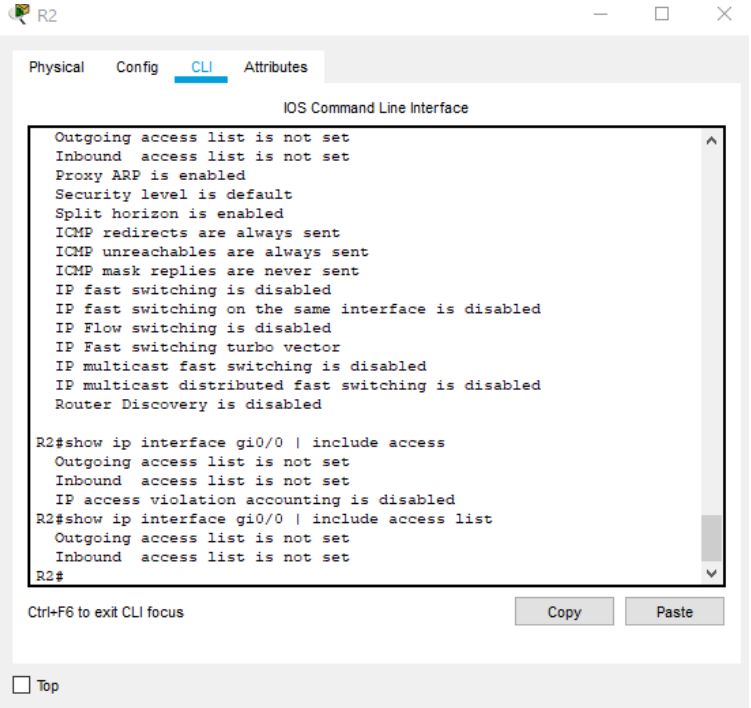
Tabla 22. Validación de las configuraciones en R2.

Figura 19. Listas de acceso en R2.



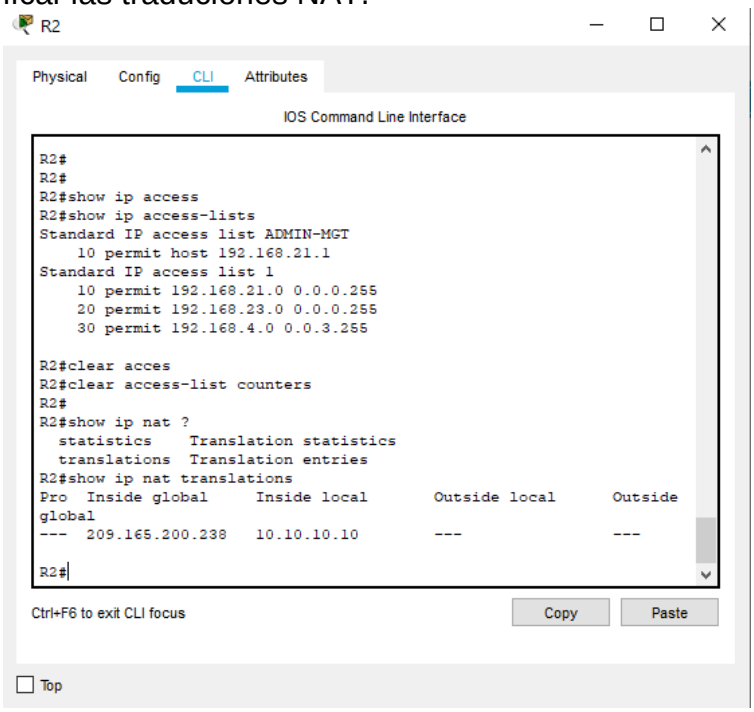
Fuente: Autor del proyecto.

Figura 20. ACL aplicadas en la interface de R2.



Fuente: Autor del proyecto.

Figura 21. Verificar las traduciones NAT.



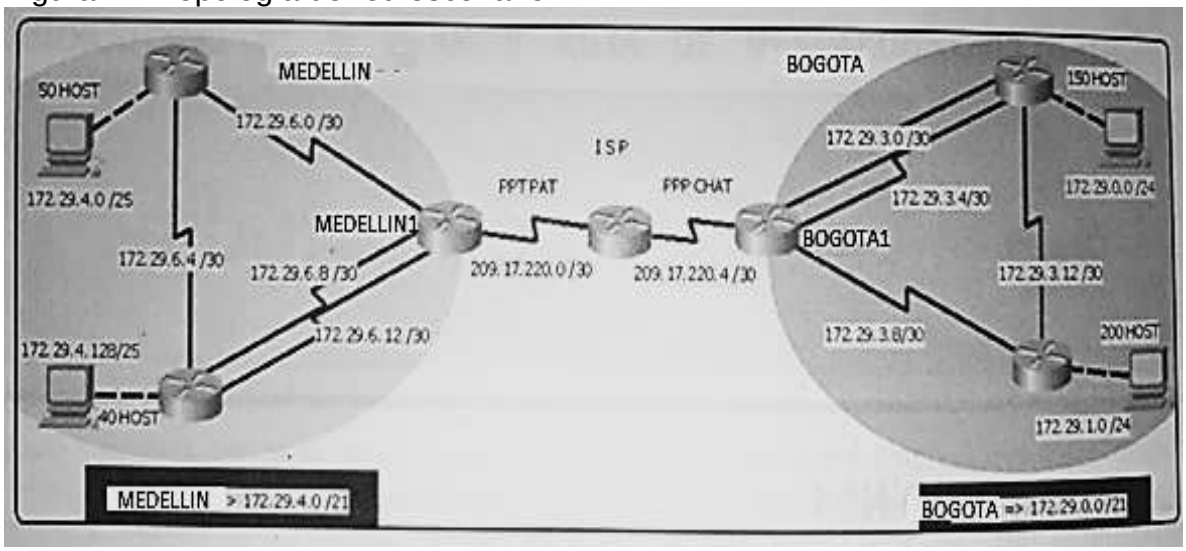
Fuente: Autor del proyecto.

3.2. Escenario 2

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

Topología de red

Figura 22. Topología de red escenario 2.



Fuente: Autor del proyecto.

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

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

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

- Realizar la conexión fisica de los equipos con base en la topología de red

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

CONFIGURACIÓN EN ISP

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#enable secret class
ISP(config)#line con 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd #El acceso no autorizado esta prohibido#
ISP(config)#interface serial 0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface serial 0/0/1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#
```

Se configura el router ISP con los criterios básicos, asignando hostname, contraseñas de consola, contraseñas del exec y advertencia de uso no autorizado.

CONFIGURACIÓN EN MEDELLIN1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN1
```

```
MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line con 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#line vty 0 4
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#banner motd #El acceso no autorizado esta prohibido#
MEDELLIN1(config)#interface serial 0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial 0/0/1
MEDELLIN1(config-if)#
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial 0/1/0
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial 0/1/1
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#
```

Se configura el router MEDELLIN1 con los criterios básicos, asignando hostname, contraseñas de consola, contraseñas del exec y advertencia de uso no autorizado.

CONFIGURACIÓN EN MEDELLIN2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN2
```

```
MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#line con 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#line vty 0 4
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#banner motd #El acceso no autorizado esta prohibido#
MEDELLIN2(config)#interface serial 0/0/1
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#
MEDELLIN2(config-if)#exit
MEDELLIN2(config)#
MEDELLIN2(config)#interface serial 0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#exit
MEDELLIN2(config)#interface fa0/0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#
MEDELLIN2(config-if)#exit
MEDELLIN2(config)#
```

Se configura el router MEDELLIN2 con los criterios básicos, asignando hostname, contraseñas de consola, contraseñas del exec y advertencia de uso no autorizado.

CONFIGURACIÓN EN MEDELLIN3

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#line con 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
```

```
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#line vty 0 4
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#banner motd #El acceso no autorizado esta prohibido#
MEDELLIN3(config)#interface serial 0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#
MEDELLIN3(config)#interface serial 0/1/0
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#interface serial 0/1/1
MEDELLIN3(config-if)#ip address 172.26.6.14 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#interface fa0/0
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#
```

Se configura el router MEDELLIN3 con los criterios básicos, asignando hostname, contraseñas de consola, contraseñas del exec y advertencia de uso no autorizado.

CONFIGURACIÓN EN BOGOTA1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA1
BOGOTA1(config)#no ip domain-lookup
BOGOTA1(config)#enable secret class
BOGOTA1(config)#line con 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#line vty 0 4
BOGOTA1(config-line)#password cisco
```

```
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#banner motd #El acceso no autorizado esta prohibido#
BOGOTA1(config)#interface serial 0/0/0
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/1/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/0/1
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
BOGOTA1(config)#
```

Se configura el router BOGOTA1 con los criterios básicos, asignando hostname, contraseñas de consola, contraseñas del exec y advertencia de uso no autorizado.

CONFIGURACIÓN EN BOGOTA2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA2
BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line con 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#line vty 0 4
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
```

```
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#banner motd #El acceso no autorizado esta prohibido#
BOGOTA2(config)#interface serial 0/1/0
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit
BOGOTA2(config)#interface serial 0/1/1
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit
BOGOTA2(config)#interface serial 0/0/0
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit
BOGOTA2(config)#interface fa0/0
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit
BOGOTA2(config)#
```

Se configura el router BOGOTA2 con los criterios básicos, asignando hostname, contraseñas de consola, contraseñas del exec y advertencia de uso no autorizado.

CONFIGURACIÓN EN BOGOTA3

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA3
BOGOTA3(config)#no ip domain-lookup
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line con 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#exit
BOGOTA3(config)#line vty 0 4
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#exit
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#banner motd #El acceso no autorizado esta prohibido#
BOGOTA3(config)#interface serial 0/0/0
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
```

```
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#exit
BOGOTA3(config)#
BOGOTA3(config)#interface serial 0/0/1
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 fa0/0
BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#exit
BOGOTA3(config)#
```

Se configura el router BOGOTA3 con los criterios básicos, asignando hostname, contraseñas de consola, contraseñas del exec y advertencia de uso no autorizado.

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.

CONFIGURACIÓN EN ISP

```
ISP(config)#router ospf 1
ISP(config-router)#router-id 1.1.1.1
ISP(config-router)#do show ip route c
 C   209.17.220.0/30 is directly connected, Serial0/0/0
 C   209.17.220.4/30 is directly connected, Serial0/0/1

ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
ISP(config-router)#
```

Se configura en ISP el protocolo OSPF version 2, asignando las redes de las interfaces que conectan con BOGOTA1 y MEDELLIN1 al area 0.

CONFIGURACIÓN EN MEDELLIN1

```
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 2.2.2.2
MEDELLIN1(config-router)#do show ip route c
 C   172.29.6.0/30 is directly connected, Serial0/0/1
 C   172.29.6.8/30 is directly connected, Serial0/1/0
```

```
 C   172.29.6.12/30 is directly connected, Serial0/1/1
 C   209.17.220.0/30 is directly connected, Serial0/0/0
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0
MEDELLIN1(config-router)#passive-interface fa0/0
MEDELLIN1(config-router)#passive-interface fa0/1
MEDELLIN1(config-router)#
```

Se asigna el protocolo OSPFv2 en MEDELLIN1, se asigna el direccionamiento a las interfaces además de seleccionar que interfaces son pasivas o no.

CONFIGURACIÓN EN MEDELLIN2

```
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 3.3.3.3
MEDELLIN2(config-router)#do show ip route c
 C   172.29.4.0/25 is directly connected, FastEthernet0/0
 C   172.29.6.0/30 is directly connected, Serial0/0/1
 C   172.29.6.4/30 is directly connected, Serial0/0/0
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 0
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN2(config-router)#passive-interface fa0/0
MEDELLIN2(config-router)#
```

Se asigna el protocolo OSPFv2 en MEDELLIN2, se asigna el direccionamiento a las interfaces además de seleccionar que interfaces son pasivas o no.

CONFIGURACIÓN EN MEDELLIN3

```
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 4.4.4.4
MEDELLIN3(config-router)#do show ip route c
 C   172.26.6.12/30 is directly connected, Serial0/1/1
 C   172.29.4.128/25 is directly connected, FastEthernet0/0
 C   172.29.6.4/30 is directly connected, Serial0/0/0
 C   172.29.6.8/30 is directly connected, Serial0/1/0
MEDELLIN3(config-router)#network 172.26.6.12 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 0
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0
```

```
MEDELLIN3(config-router)#passive-interface fa0/0
MEDELLIN3(config-router)#exit
```

Se asigna el protocolo OSPFv2 en MEDELLIN3, se asigna el direccionamiento a las interfaces además de seleccionar que interfaces son pasivas o no.

CONFIGURACIÓN EN BOGOTA1

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id     5.5.5.5
BOGOTA1(config-router)#do show ip route c
 C  172.29.3.0/30  is  directly  connected,  Serial0/1/0
 C  172.29.3.4/30  is  directly  connected,  Serial0/1/1
 C 172.29.3.8/30 is directly connected, Serial0/0/1
 C    209.17.220.4/30 is directly connected, Serial0/0/0
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
BOGOTA1(config-router)#passive-interface fa0/0
BOGOTA1(config-router)#passive-interface fa0/1
BOGOTA1(config-router)#exit
```

Se asigna el protocolo OSPFv2 en BOGOTA1, se asigna el direccionamiento a las interfaces además de seleccionar que interfaces son pasivas o no.

CONFIGURACIÓN EN BOGOTA2

```
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 6.6.6.6
BOGOTA2(config-router)#do show ip route c
 C    172.29.0.0/24 is directly connected, FastEthernet0/0
 C    172.29.3.0/30 is directly connected, Serial0/1/0
 C    172.29.3.4/30 is directly connected, Serial0/1/1
 C    172.29.3.12/30 is directly connected, Serial0/0/0
BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0
BOGOTA2(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA2(config-router)#passive-interface fa0/0
BOGOTA2(config-router)#
```

Se asigna el protocolo OSPFv2 en BOGOTA2, se asigna el direccionamiento a las interfaces además de seleccionar que interfaces son pasivas o no.

CONFIGURACIÓN EN BOGOTA3

```
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 7.7.7.7
BOGOTA3(config-router)#do show ip route c
 C   172.29.1.0/24 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
BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 0
BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA3(config-router)#passive-interface fa0/0
BOGOTA3(config-router)#exit
```

Se asigna el protocolo OSPFv2 en BOGOTA3, se asigna el direccionamiento a las interfaces además de seleccionar que interfaces son pasivas o no.

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.

CONFIGURACIÓN EN MEDELLIN1

```
MEDELLIN1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#
```

CONFIGURACIÓN EN BOGOTA1

```
BOGOTA1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#
```

En este paso se configura una ruta por defecto que comunican MEDELLIN1 y BOGOTA1 con ISP.

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.

CONFIGURACIÓN EN ISP

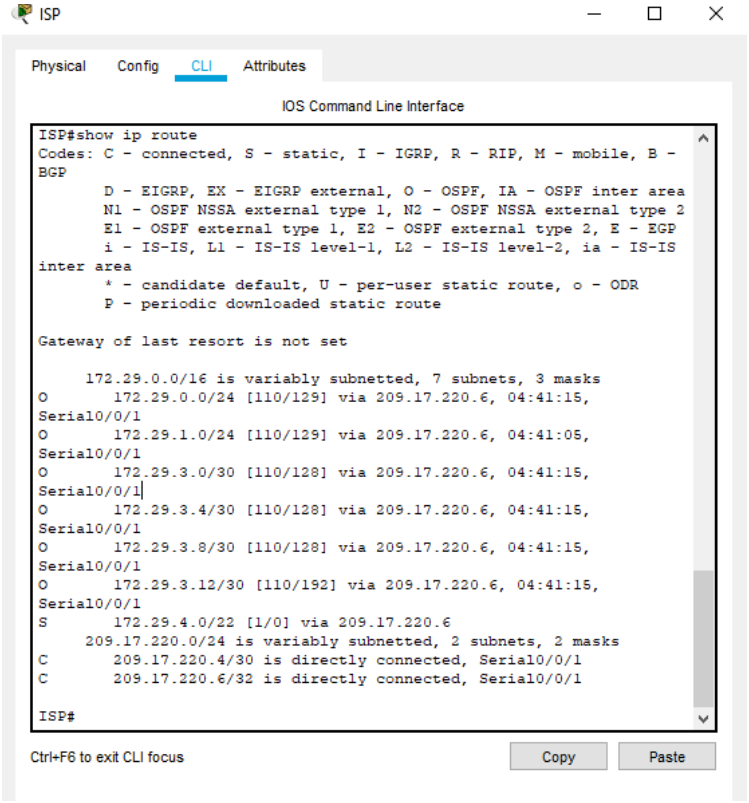
```
ISP#
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.6
ISP(config)#
```

Se sumarizan las subredes de BOGOTA y MEDELLLIN cada una a /22 y estas direcciones son incluidad en el router ISP como ruta estática dirigida a cada red interna.

Parte 2: Tabla de Enrutamiento.

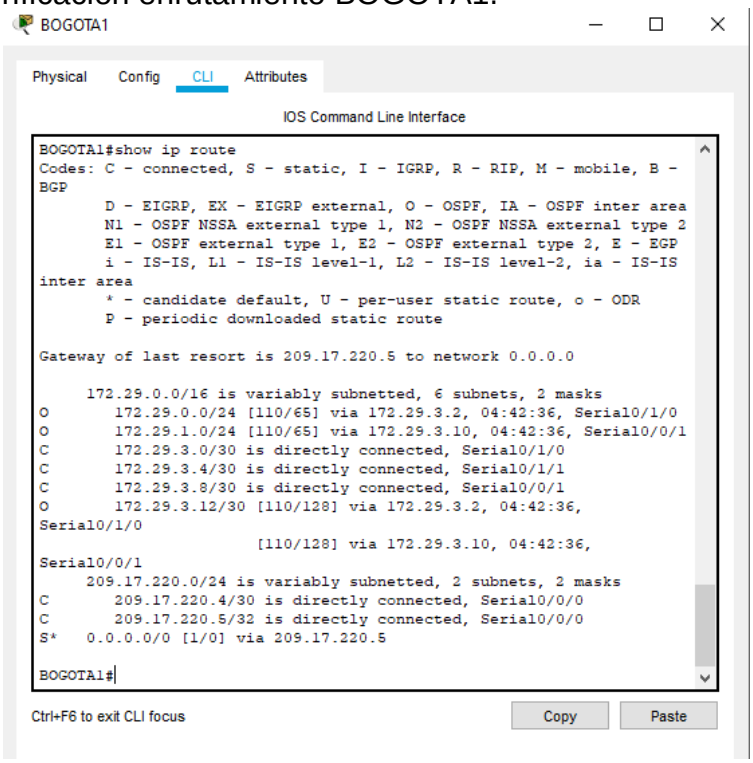
a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Figura 23. Verificación enrutamiento ISP.



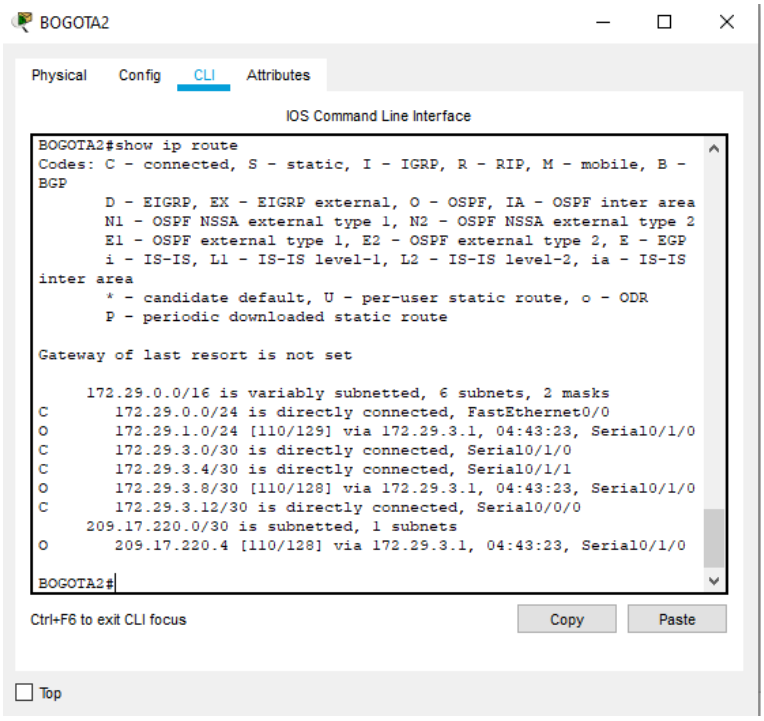
Fuente: Autor del proyecto.

Figura 24. . Verificación enrutamiento BOGOTA1.



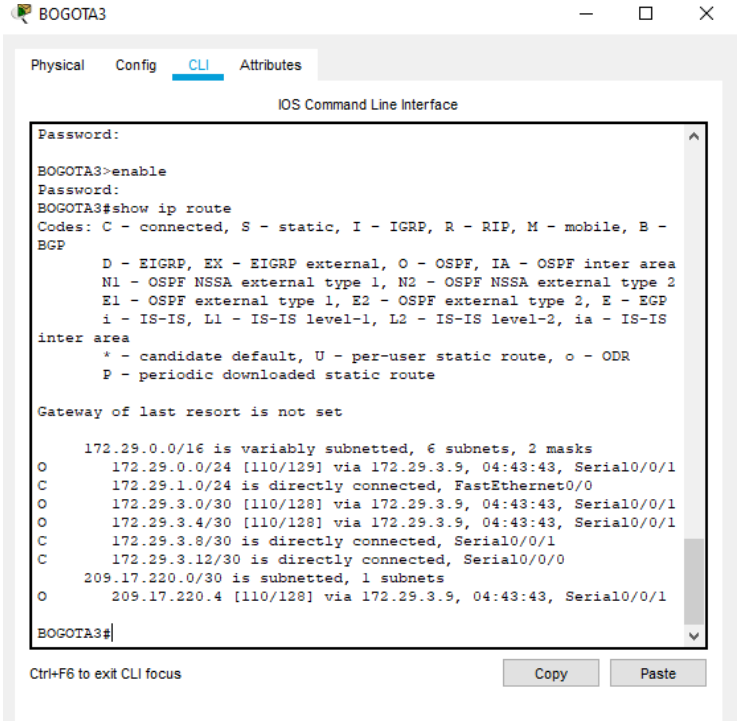
Fuente: Autor del proyecto.

Figura 25. Verificación enrutamiento BOGOTA2.



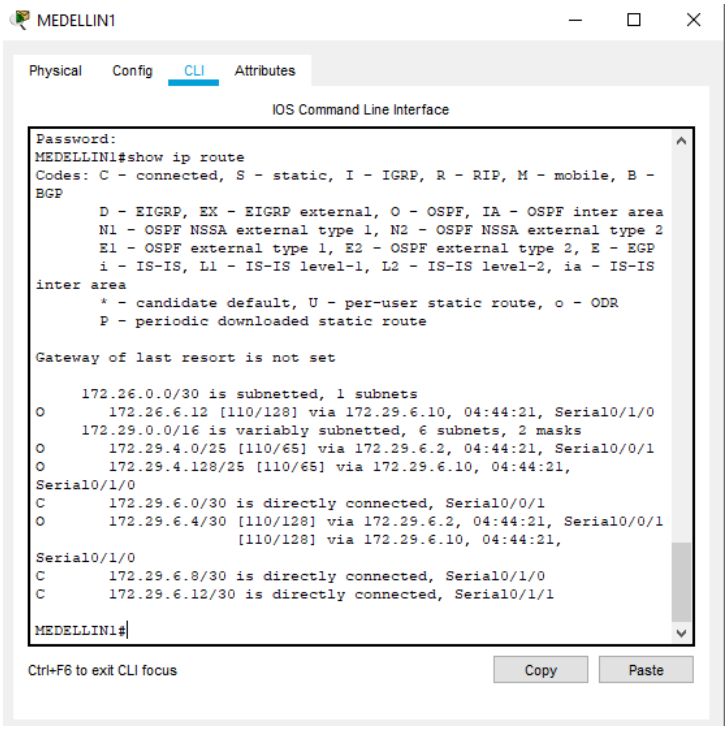
Fuente: Autor del proyecto.

Figura 26. Verificación enrutamiento BOGOTA3.



Fuente: Autor del proyecto.

Figura 27. Verificación enrutamiento MEDELLIN1.



Fuente: Autor del proyecto.

Figura 28. Verificación enrutamiento MEDELLIN2.

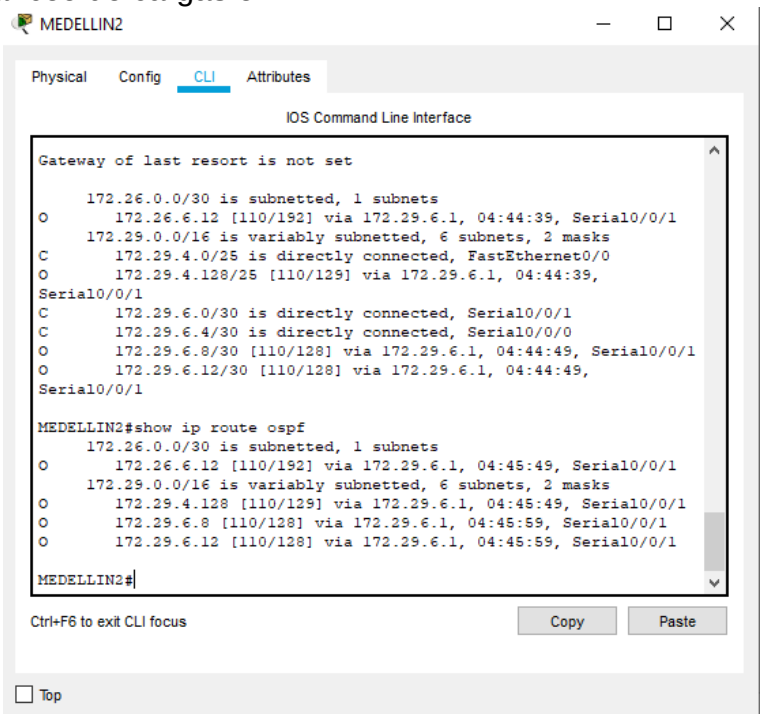
Fuente: Autor del proyecto.

Figura 29. Verificación enrutamiento MEDELLIN3.

Fuente: Autor del proyecto.

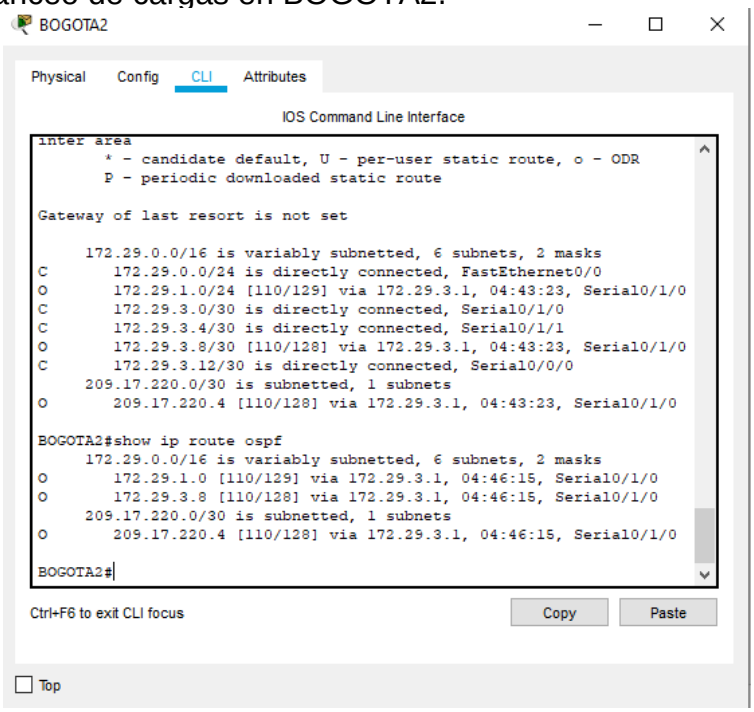
b. Verificar el balanceo de carga que presentan los routers.
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

Figura 30. Balanceo de cargas en MEDELLIN2.



Fuente: Autor del proyecto.

Figura 31. Balanceo de cargas en BOGOTA2.

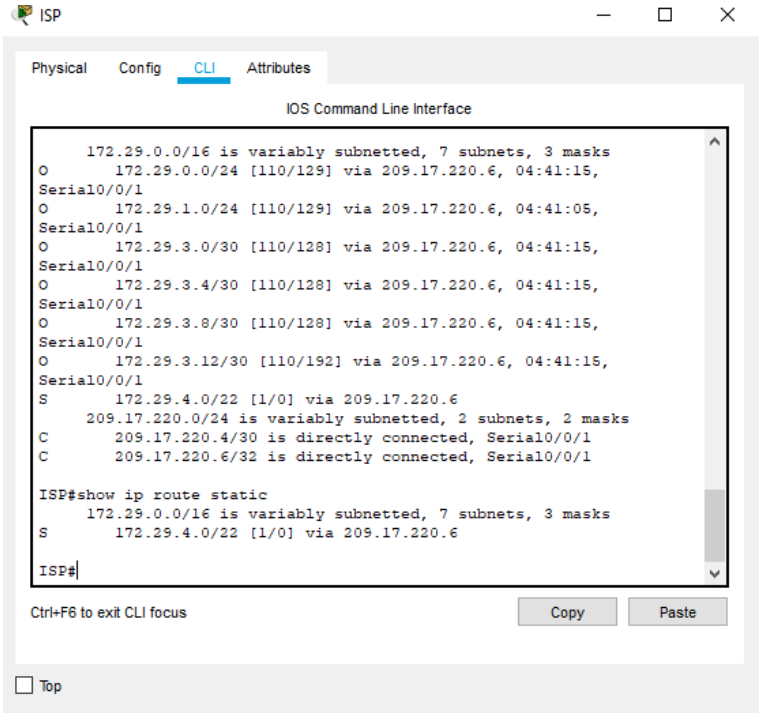


Fuente: Autor del proyecto.

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 32. Verificar en ISP rutas estáticas adicionales.



Fuente: Autor del proyecto.

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	BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#passive-interface fa0/0 BOGOTA1(config-router)#passive-interface fa0/1 BOGOTA1(config-router)#
Bogota2	BOGOTA2(config)#router ospf 1 BOGOTA2(config-router)#passive-interface s0/0/1 BOGOTA2(config-router)#passive-interface fa0/0 BOGOTA2(config-router)#
Bogota3	BOGOTA3(config)#router ospf 1 BOGOTA3(config-router)#passive-interface fa0/0 BOGOTA3(config-router)#passive-interface fa0/1
Medellín1	MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#passive-interface fa0/0 MEDELLIN1(config-router)#passive-interface fa0/1

Medellín2	MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#passive-interface fa0/0 MEDELLIN2(config-router)#passive-interface fa0/1 MEDELLIN2(config-router)#
Medellín3	MEDELLIN3(config)#router ospf 1 MEDELLIN3(config-router)#passive-interface fa0/0 MEDELLIN3(config-router)#passive-interface fa0/1 MEDELLIN3(config-router)#passive-interface s0/0/1 MEDELLIN3(config-router)#
ISP	No lo requiere

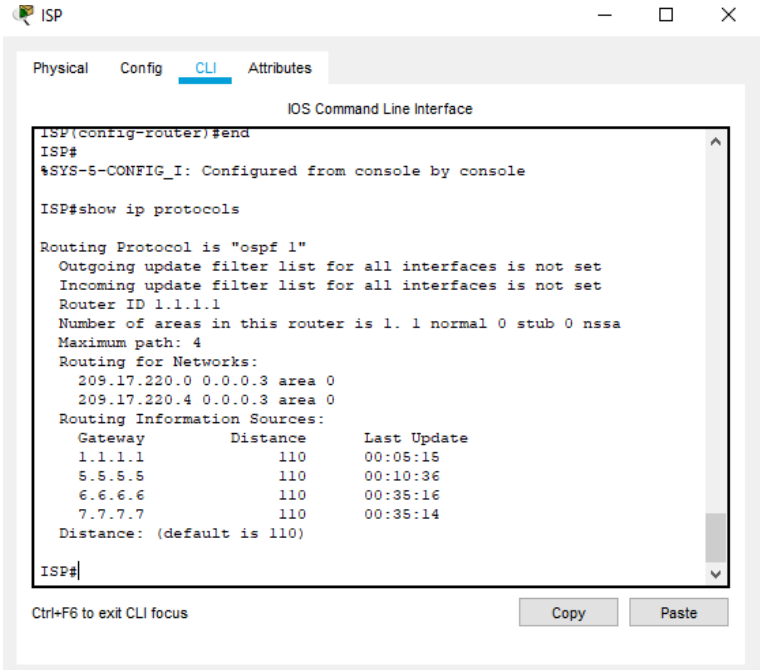
Tabla 23. Deshabilitar la propagación del protocolo OSPF en los router.

Se configuran los enlaces seriales de los Routers a excepción de ISP como interfaces no pasivas, esto significa que la propagación del protocolo OSPF esté deshabilitado para lo demás que no requieran de la propagación de las publicaciones.

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.

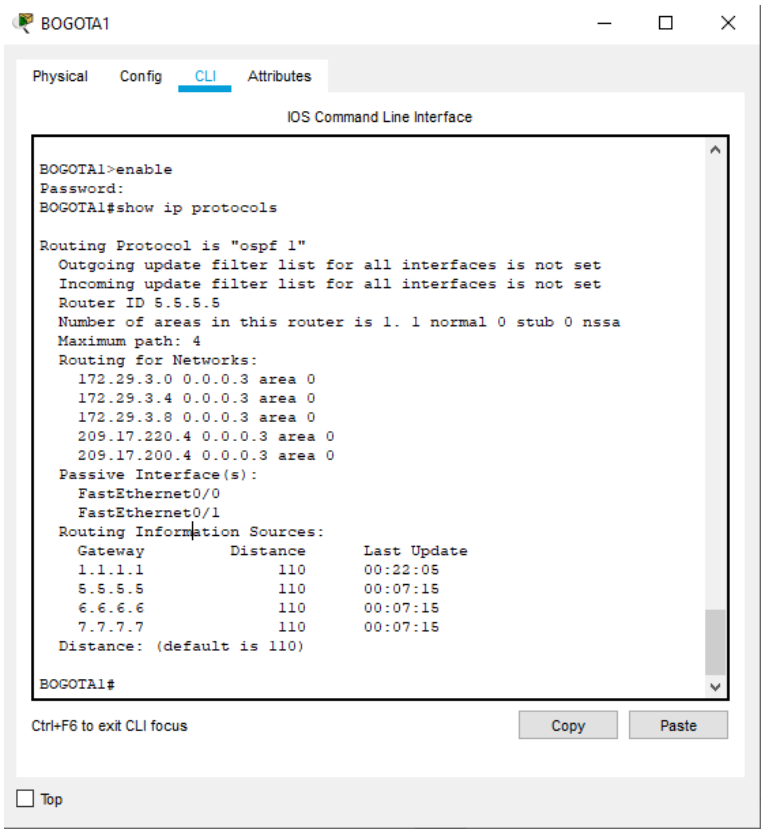
Figura 33. Verificación OSPF en ISP.



Fuente: Autor del proyecto.

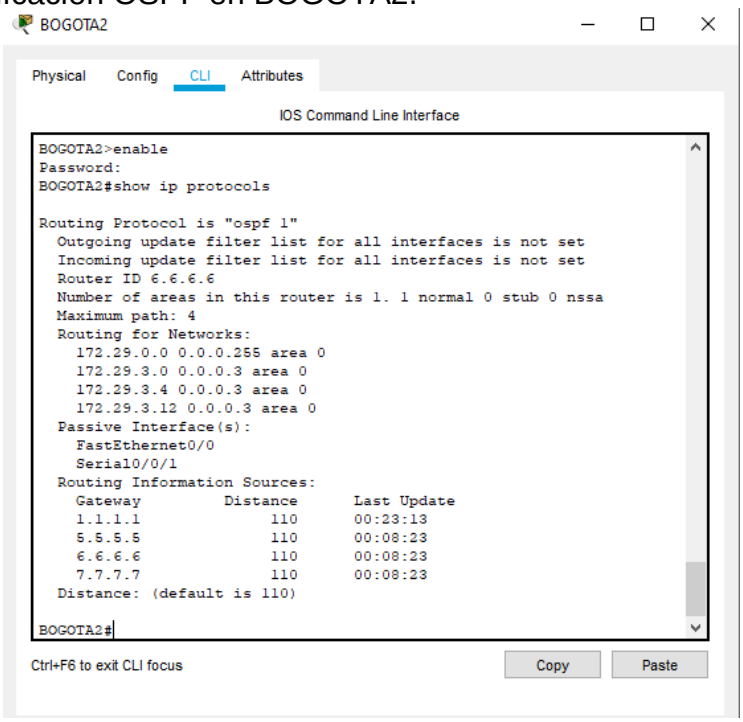
b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Figura 34. Verificación OSPF en BOGOTA1



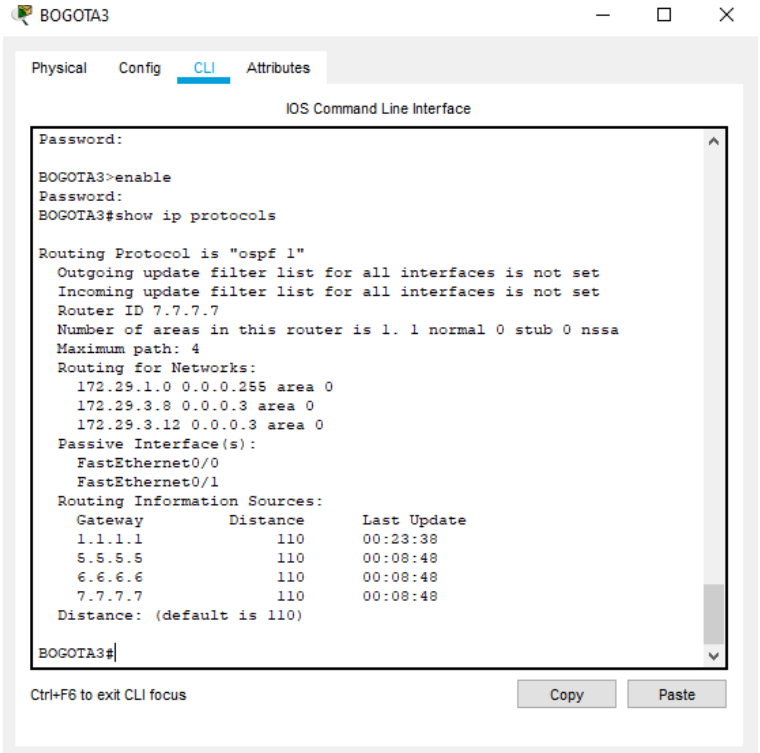
Fuente: Autor del proyecto.

Figura 35. Verificación OSPF en BOGOTA2.



Fuente: Autor del proyecto.

Figura 36. Verificación de la base de datos de OSPF en BOGOTA3.



Fuente: Autor del proyecto.

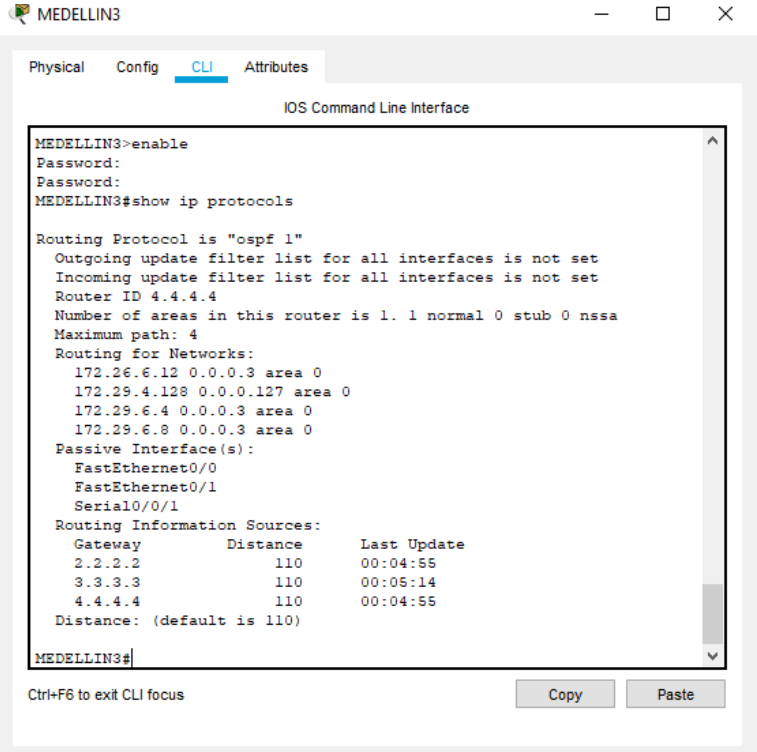
Figura 37. Verificación OSPF en MEDELLIN1

Fuente: Autor del proyecto.

Figura 38. Verificación OSPF en MEDELLIN2.

Fuente: Autor del proyecto.

Figura 39. Verificación OSPF en MEDELLIN3.



Fuente: Autor del proyecto.

Se verifican que las rutas OSPF que estén configuradas para cada Router.

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

CONFIGURACIÓN EN ISP

ISP#configure terminal
ISP(config)#username MEDELLIN1 password 12345
ISP(config)#interface serial 0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password 12345
ISP(config-if)#

CONFIGURACIÓN EN MEDELLIN1

MEDELLIN1#configure terminal

```
MEDELLIN1(config)#username ISP password 12345
MEDELLIN1(config)#interface serial 0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password 12345
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#
```

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

CONFIGURACIÓN EN ISP

```
ISP#configure terminal
ISP(config)#username BOGOTA1 password cisco
ISP(config)#interface serial 0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
ISP(config)#
```

CONFIGURACIÓN EN BOGOTA1

```
BOGOTA1#configure terminal
BOGOTA1(config)#interface serial 0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#exit
BOGOTA1(config)#
```

Parte 6: Configuración de PAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.
c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

CONFIGURACIÓN EN MEDELLIN1

```
MEDELLIN1>enable
Password:
MEDELLIN1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config-std-nacl)#exit
MEDELLIN1(config)#ip nat inside source list HOST interface s0/0/0 overload
MEDELLIN1(config)#interface serial 0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial 0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial 0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#interface serial 0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#
```

CONFIGURACIÓN EN BOGOTA1

```
BOGOTA1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.3.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list HOST interface s0/0/0 overload
BOGOTA1(config)#interface serial 0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#interface serial 0/0/1
BOGOTA1(config-if)#ip nat inside
```

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

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.
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

CONFIGURACIÓN EN MEDELLIN2

```
MEDELLIN2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#ip dhcp ex
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.3
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
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
MEDELLIN2(config)#
```

CONFIGURACIÓN EN MEDELLIN3

```
MEDELLIN3>enable
Password:
MEDELLIN3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#interface fastEthernet 0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#
```

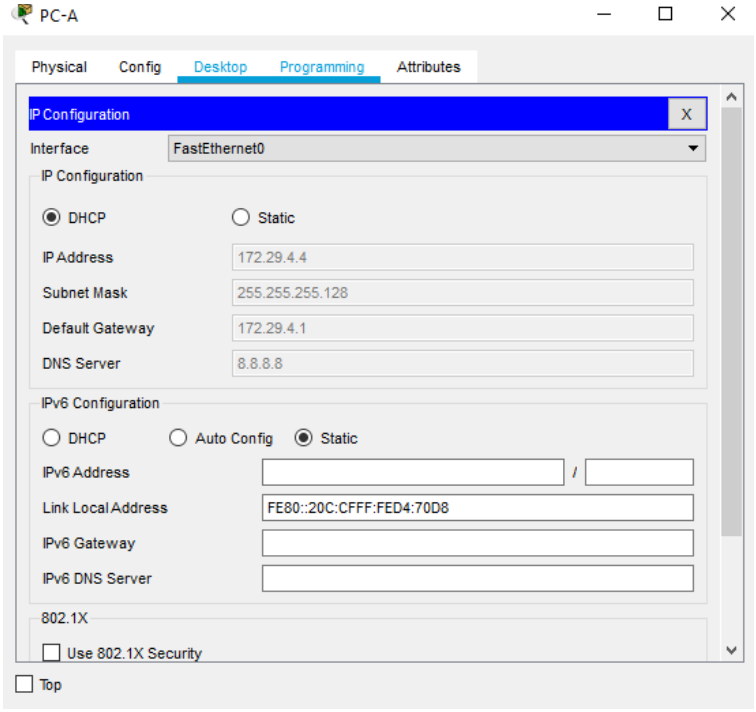
CONFIGURACIÓN EN BOGOTA2

```
BOGOTA2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#ip dhcp ex
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.4
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 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
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#
```

CONFIGURACIÓN EN BOGOTA3

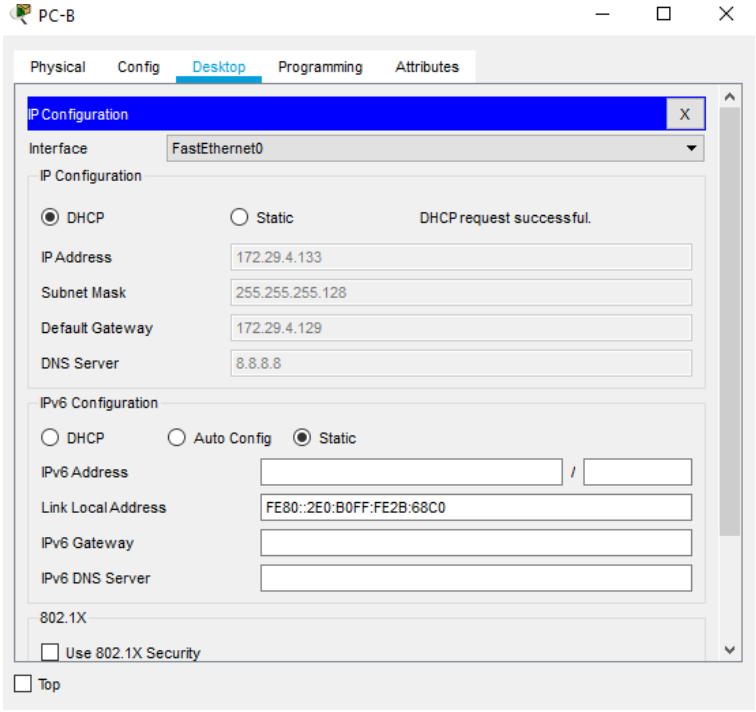
```
BOGOTA3>enable
Password:
BOGOTA3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#interface fa0/0
BOGOTA3(config-if)#ip helper
BOGOTA3(config-if)#ip helper-address 172.29.3.13
BOGOTA3(config-if)#exit
BOGOTA3(config)#
```

Figura 40. Configuración DHCP en PC-A.



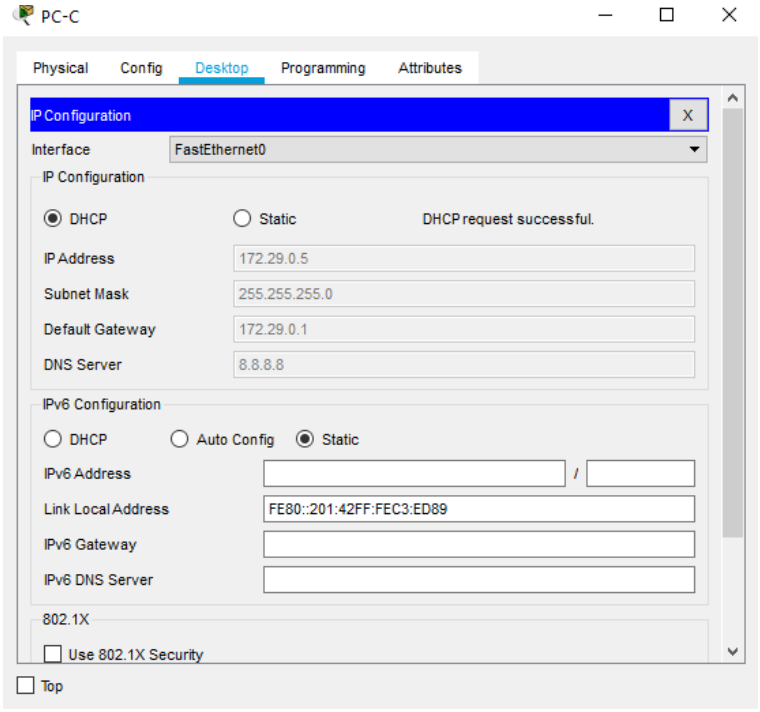
Fuente: Autor del proyecto.

Figura 41. Configuración DHCP en PC-B.



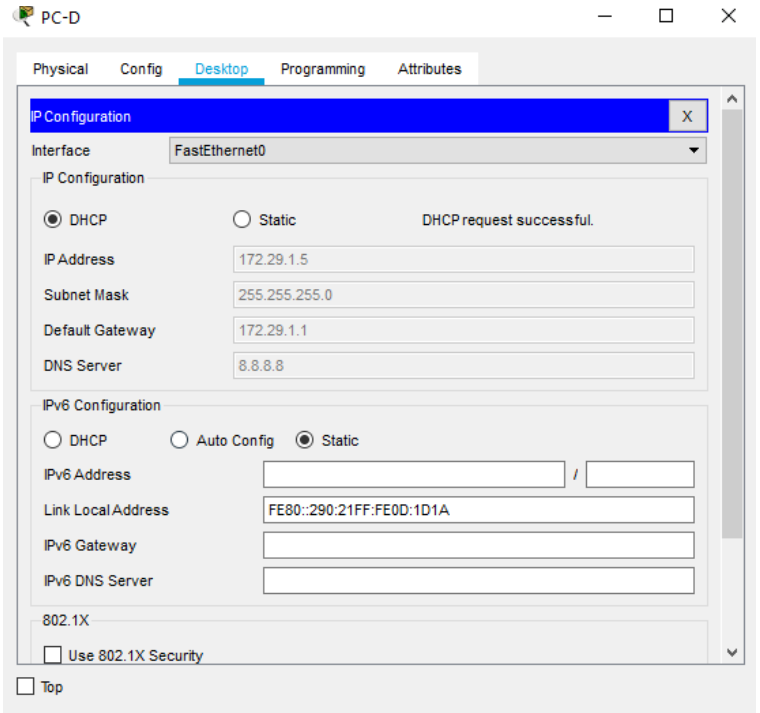
Fuente: Autor del proyecto.

Figura 42. Configuración DHCP en PC-C.



Fuente: Autor del proyecto.

Figura 43. Configuración DHCP en PC-D.



Fuente: Autor del proyecto.

CONCLUSIONES

En el desarrollo de esta prueba de habilidades se pusieron a prueba todos los conceptos adquiridos a través del desarrollo del curso enfocados, en la forma como se desenvuelve cada implementación de instrucciones que satisfaga los requerimientos de los escenarios, así como el cumplimiento de la topología asignada.

Las simulaciones están soportadas por Cisco, y cada uno de los dispositivos cuenta con su respectivo sistema operativo y su definición que permita realizar la asignación del direccionamiento y los respectivos cambios, rindiendo de la misma manera a un dispositivo real.

Cabe destacar, que además se hace uso de la implementación de protocolos como OSPFv2 y RIPv2, esto soporta y permite la comunicación entre diferentes dispositivos de redes distintas.

Finalmente, se configuró 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.

BIBLIOGRAFÍA

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

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1lhgTCtKY-7F5KIRC3