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

JAIME RIVERA SANCHEZ

UNIVERSIDAD NAICONAL ABIERTA Y A DISTANCIA, UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA
2020

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

JAIME RIVERA SANCHEZ

INFORME FINAL PARA OPTAR POR EL TÍTULO DE INGENIERO EN ELECTRONICA

HECTOR JULIAN PARRA (TUTOR)

UNIVERSIDAD NAICONAL ABIERTA Y A DISTANCIA, UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá. 26 de Mayo del 2020

DEDICATORIA

Este informe va dedicado a mi familia por todo su gran apoyo durante mi proceso formativo. En especial a mi esposa y mi hijo que son mi motivación para seguir adelante en el camino de la profesionalización.

AGRADECIMIENTOS

Agradezco a todas los tutores que fueron guía en mi formación académica, durante todos los semestres de estudios.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

GLOSARIO

OSPF: El protocolo Open Shortest Path First (OSPF), definido en RFC 2328, es un Internal Gateway Protocol (IGP) que se usa para distribuir la información de ruteo dentro de un solo sistema autónomo. Protocolo de Enrutamiento Dinámico.

RIPv2: El Protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento por vector-distancia, usada en miles de redes en todo el mundo. El hecho que RIP se base en estándares abiertos y que sea de fácil implementación hace que resulte atractivo para algunos administradores de redes, aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados

PPP: El protocolo punto a punto (PPP) es un protocolo TCP/IP que se emplea para conectar un sistema informático a otro. Las máquinas emplean PPP para comunicarse por la red telefónica o por Internet. Protocolos de autenticación.

NAT Network Address Translation: La traducción de direcciones de red (NAT) está diseñada para conservar direcciones IP. Permite que se conecten a Internet las redes de IP privada que emplean direcciones IP no registradas. NAT opera en routers, que en general conectan dos redes, y convierte las direcciones privadas (no exclusivas globalmente) de la red interna en direcciones legales, antes de que se reenvíen los paquetes a otra red.

PAT: Port Address Translation (PAT) también conocido como Network Address Port Translator (NAPT). Port Address Translation (PAT), es una extensión de la traducción de direcciones de red (NAT) que permite que varios dispositivos en una red de área local (LAN) se asignen a una sola dirección IP pública. El objetivo de PAT es conservar las direcciones IP. La dirección de dirección de puerto también se denomina portación, sobrecarga de puertos, NAT multiplexado a nivel de puerto y NAT de dirección única.

RESUMEN

En este informe se realiza el análisis de dos escenarios de redes, en los cuales emplearemos los protocolos RIP, PPP, OSPF, con el fin de realizar el direccionamiento de todo los equipos, computadores, router y switch, empleando los comandos necesarios para tal fin.

Inicialmente realizamos el restablecimiento y configuración de los equipos, luego configuramos todos los puertos ya sean seriales o Ethernet con sus correspondientes direcciones IPV4 o IPV6, creando así los enlaces entre dispositivos por medio de conexiones alámbricas o inalámbricas.

Seguido de esto comenzamos a emplear los protocolos de direccionamiento, según el caso, topología de red, y seguridad correspondiente.

En el escenario 1 es una red pequeña donde utilizamos el protocolo RIPv2, DHCP, NAT, NTP y routing entre VLAN, en las subredes asignadas. Además de ACLs.

En el escenario 2 se trata du una red empresarial con sedes distribuidas en dos ciudades, donde empleamos el protocolo OSPF, DHCP, encapsulamiento PPP, NAT y PAT.

Para verificar si los protocolos aplicados en cada caso son adecuados y funcionales, realizamos pruebas por medio de comandos como ping, además para visualizar si las configuraciones son correctas aplicamos los show ip route, show running-config entre otros.

PALABRAS CLAVE: direccionamiento, protocolo, enrutamiento dinámico, enrutamiento estático, métricas, network, address, translation, autentication

1. INTRODUCCIÓN

En el presente informe se realizara el análisis de dos escenarios de red, el primero es una LAN pequeña donde se realizará routing entre VLAN, y direccionamiento con el protocolo RIPv2. En el segundo escenario trabajaremos sobre una LAN empresarial donde llevaremos a cabo el direccionamiento de dos redes principales mediante el protocolo OPSF, habilitando el encapsulamiento PPP y su autenticación. Aplicando los conocimientos adquiridos sobre redes, conectividad IPV4 e IPV6, enrutamiento, y administración de redes.

Dando solución a los escenarios propuestos mediante la utilización de los protocolos ya mencionados, y teniendo en cuenta las subredes propuestas para cada escenario. Además usaremos el protocolo DHCP, traducción de direcciones NAT, las listas de control de acceso ACL y protocolo NTP. Probando y registrando los anteriores protocolos mediante comandos en el CLI de cada uno de los dispositivos.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Aplicar los conocimientos adquiridos sobre enrutamiento de redes, en la solución de los escenarios propuestos.

2.2 OBJETIVOS ESPECÍFICOS

- Aplicar el protocolo RIPv2 y OSPF para el direccionamiento de paquetes en los diferentes escenarios.
- Emplear los protocolos DHCP, NTP, PPP, ACL, y creación de VLANs.
- Manejar el direccionamiento en conectividad IPV4 e IPV6.
- Utilizar todos los parámetros y comandos de configuración en cada uno de los routers desde CLI, para el direccionamiento dinámico estático de redes.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICION DEL PROBLEMA

Dar solución a dos escenarios de red.

En el primer escenario debemos configurar una red pequeña para que admita conectividad IPv4 e IPv6, además seguridad de switches, routing entre VLAN, y la implementación del protocolo de routing dinámico RIPv2, junto con el protocolo de configuración de hosts dinámicos (DHCP), realizar la traducción de direcciones de red dinámicas y estáticas (NAT), crear las listas de control de acceso (ACL) y emplear el protocolo de tiempo de red (NTP) servidor/cliente. Para realizar la prueba y registro de la red, se utilizaran los comandos comunes de CLI.

En el segundo escenario se nos propone administrar una red empresarial que posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde debemos 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.

3.2 JUSTIFICACIÓN

Los problemas anteriormente propuestos se les debe dar solución por medio de los protocolos aprendidos como los son RIPv2, DHCP, VLANS, OSPF, y direccionamiento ip entre otros, estudiados en los módulos CCNA1 Y CCNA1. Con los cuales colocaremos en práctica todo lo aprendido en el presente curso.

4. DESARROLLO DEL ESCENARIO 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.

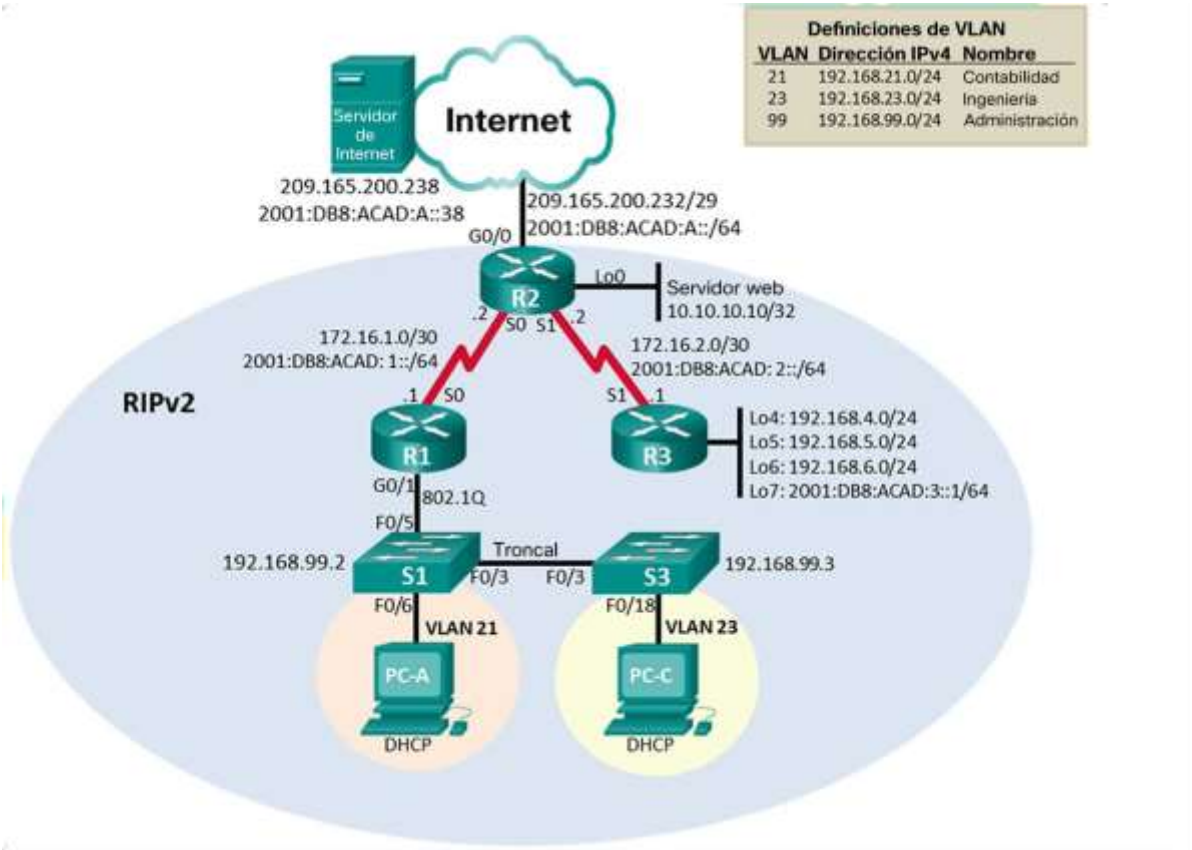


Figura 1 Topología a desarrollar escenario 1

4.1 Inicializar dispositivos

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

Se eliminaron las configuraciones y se cargó de nuevo la configuración de inicio de todos los routers y switches.

Tabla 1 Inicialización de dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	R1#erase startup-config
Volver a cargar todos los routers	R1#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	S1#erase startup-config S1#delete vlan.dat
Volver a cargar ambos switches	S1#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	S1#show flash S1#show vlan

4.2 Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Se configuro el servidor de internet de acuerdo con la topología sugerida.

Tabla 2 Configuración de computadora 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::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Paso 2: Configurar R1

Se realizó configuración del router 1 con sus parámetros iniciales e interfaces correspondientes.

Tabla 3 Configuración del router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R1(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 console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 15 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 prohíbe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#interface S0/0/0 R1(config-if)#description conexion al router 2 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
Rutas predeterminadas	R1(config)#ipv6 unicast-routing 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)#exit

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

Se realizó configuración del router 2 con sus parámetros iniciales e interfaces.

Tabla 4 Configuración del router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(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 console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 15 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	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface S0/0/0 R2(config-if)#description conexion al router 1 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

Interfaz S0/0/1	R2(config)#interface S0/0/1 R2(config-if)#description conexion al router 3 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
Interfaz G0/0 (simulación de Internet)	R2(config-if)#inter g0/0 R2(config-if)#description conexión a 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
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#description conexion al servidor web R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 unicast-routing R2(config)#ipv6 route ::/0 g0/0 R2(config)#exit

Paso 4: Configurar R3

Se realizó configuración inicial e interfaces del router 3, incluyendo las interfaces looback.

Tabla 5 Configuración del router 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(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 console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 15 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 prohíbe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#inter s0/0/1 R3(config-if)#description conexion al router 2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0

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

Paso 5: Configurar S1

Se realizó la configuración básica del switch 1.

Tabla 6 Configuración de switch 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(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 console 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 prohíbe el acceso no autorizado#

Paso 6: Configurar el S3

Se realizó la configuración básica del switch 3

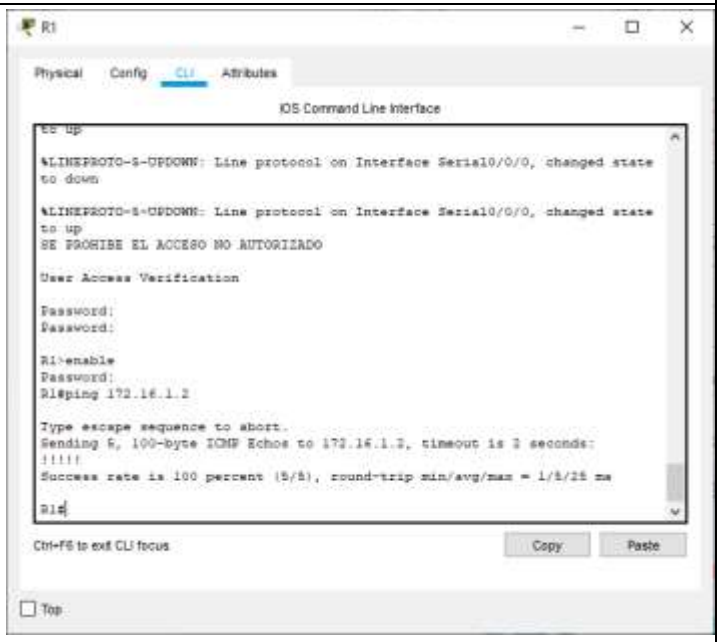
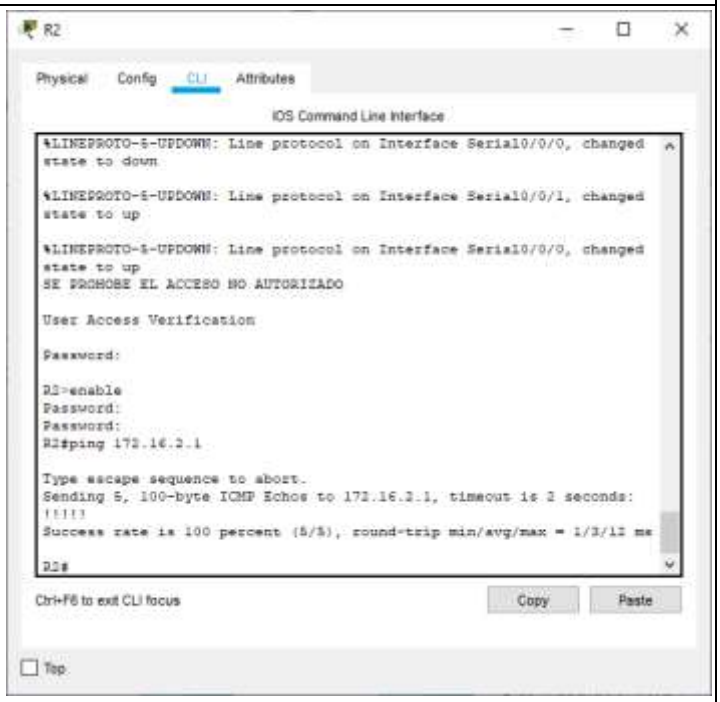
Tabla 7 Configuración de switch 3

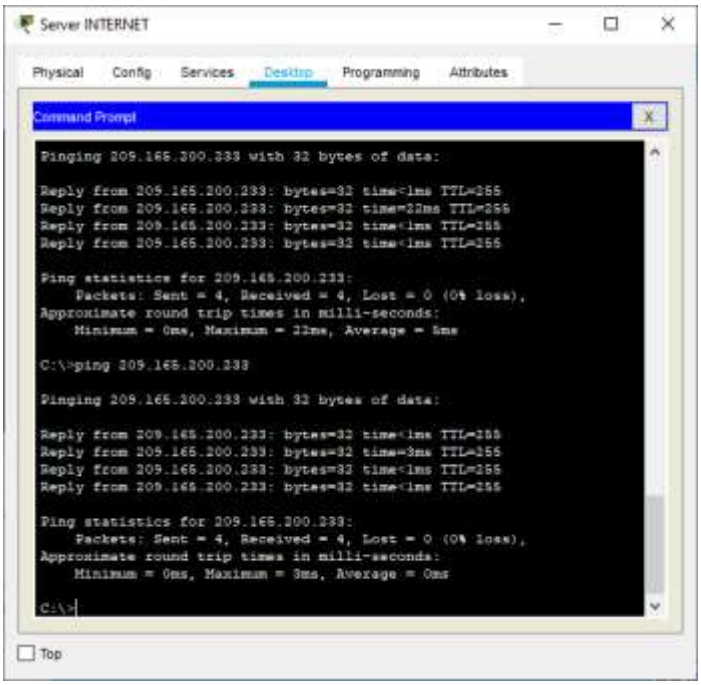
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password 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 prohíbe el acceso no autorizado#

Paso 7: Verificar la conectividad de la red

Se realizó verificación de la conectividad por medio del comando **ping** desde CLI en los routers y la ventana de comando del servidor de internet en la siguiente tabla.

Tabla 8 Verificación de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 Figura 2 Resultado ping entre R1 Y R2
R2	R3, S0/0/1	172.16.2.1	 Figura 3 Resultado ping entre R2 y R3

PC de Internet	Gateway predeterminado	209.165.200.233	 Figura 4 Resultado ping entre Pc de internet y Gateway predeterminado

4.3 Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

Se realizó configuración de las VLAN en el switch 1, con sus respectivos puertos de acceso y troncales.

Tabla 9 Configuración de VLAN switch 1

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

Asignar la dirección IP de administración.	S1(config)#int 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)#int range f0/3 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 1 S1(config-if-range)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#int range f0/5 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 1 S1(config-if-range)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

Se crearon las VLAN en el switch 3, con los respectivos puertos de acceso y troncales.

Tabla 10 Configuración de VLAN switch 3

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)#int vlan 99 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)#inter f0/3 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)#inter range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21 (Correccion f0/18 a la VLAN 23 Segun la topología)	S3(config)#inter f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#inter range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Se realizó configuración de las sub interfaces con 802.1Q en el router 1.

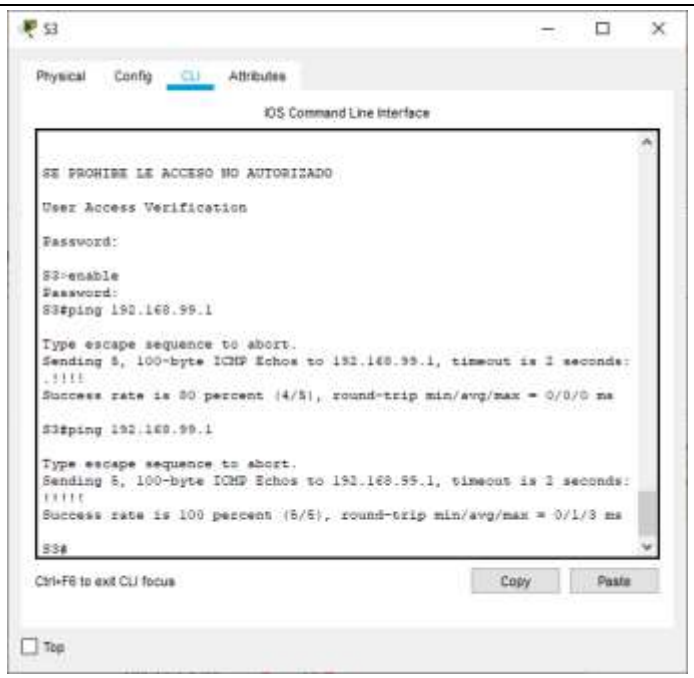
Tabla 11 Configuración de VLAN ROUTER 1

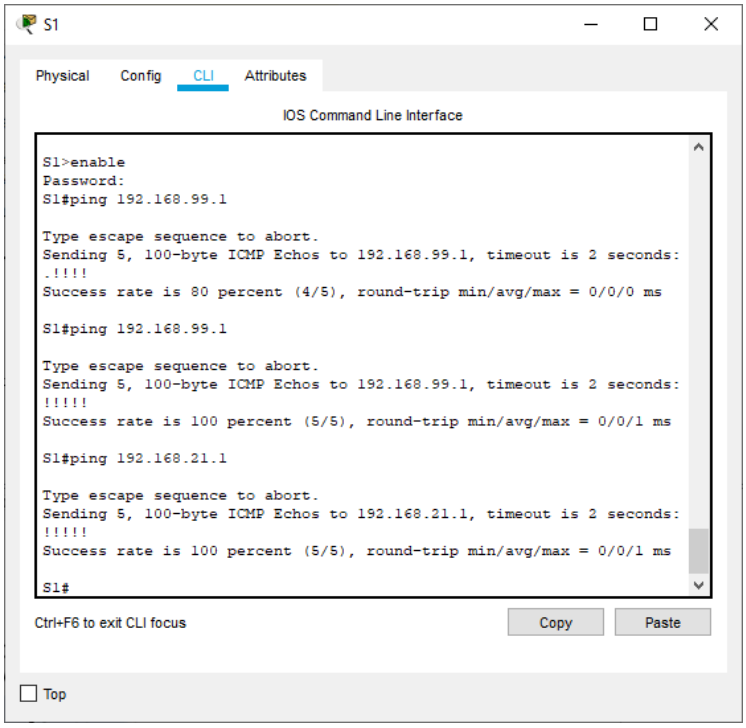
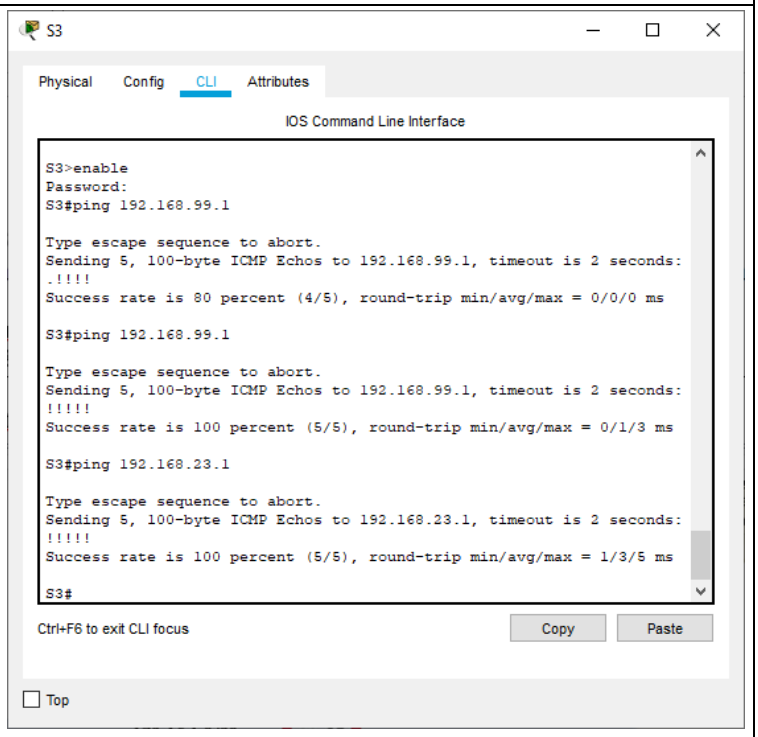
Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#inter g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#no shutdown R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#inter g0/1.23 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)#no shutdown R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#inter g0/1.99 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)#no shutdown R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#inter g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

Empleamos el comando **ping** para verificar la conectividad de los switch a el router 1.

Tabla 12 Verificación de conectividad entre switches y router 1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	 Figura 5 Resultado ping entre S1 y R1 VLAN 99
S3	R1, dirección VLAN 99	192.168.99.1	 Figura 6 Resultado ping entre S3 y R1 VLAN 99

S1	R1, dirección VLAN 21	192.168.21.1	 Figura 7 Resultado ping entre S1 y R1 VLAN 21
S3	R1, dirección VLAN 23	192.168.23.1	 Figura 8 Resultado ping entre S3 y R1 VLAN 23

4.4 Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Se realizó la configuración de protocolo RIPv2 en el router 1.

Tabla 13 Configuración de RIPv2 en el ROUTER 1

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)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

Se realizó la configuración del protocolo RIPv2 en el router 2.

Tabla 14 Configuración de RIPv2 en el ROUTER 2

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)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 **Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv2 en el R3

Se realizó la configuración del protocolo RIPv2 en el router 3

Tabla 15 Configuración de RIPv2 de ROUTER 3

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)#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 loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Paso 4: Verificar la información de RIP

Verificamos el protocolo RIPv2 por medio de los comandos adecuados en el CLI.

Tabla 16 Verificación de la información RIP

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?	R3#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R3#show ip route rip

Figura 9 Rutas RIP de R1

Figura 10 Rutas RIP de R2

	 Figura 11 Rutas RIP de R3
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show running-config □ section route rip

4.5 Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Se realizó la configuración del DHCP en el router .

Tabla 17 Configuración de DHCP en VLAN 21 Y 23 del router 1

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)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default 192.168.21.1 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	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)#default 192.168.23.1 R1(dhcp-config)#exit

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

Se realizó la configuración NAT estática y dinámica en el router 2.

Tabla 18 Configuración NAT del router 2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#inter loopback 0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#inter g0/0 R2(config-if)#ip nat outside 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 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

Verificamos la conexión de los protocolos DHCP Y NAT estático con ayuda del comando **ping.**

Tabla 19 Verificación del protocolo DHCP Y NAT

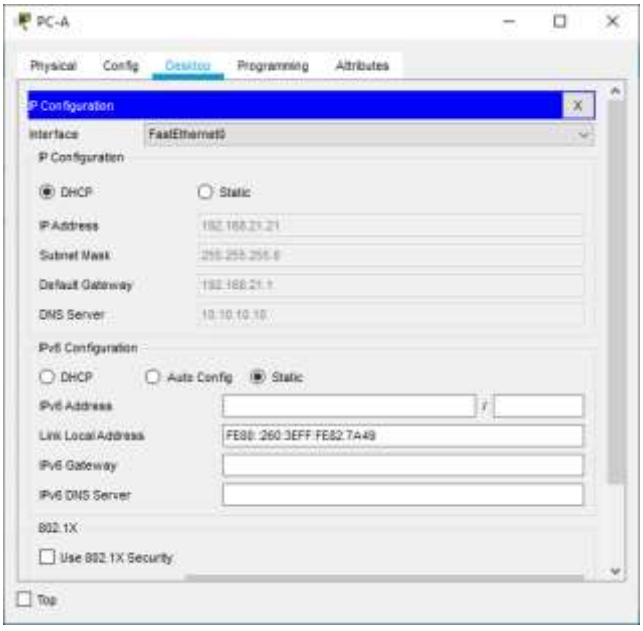
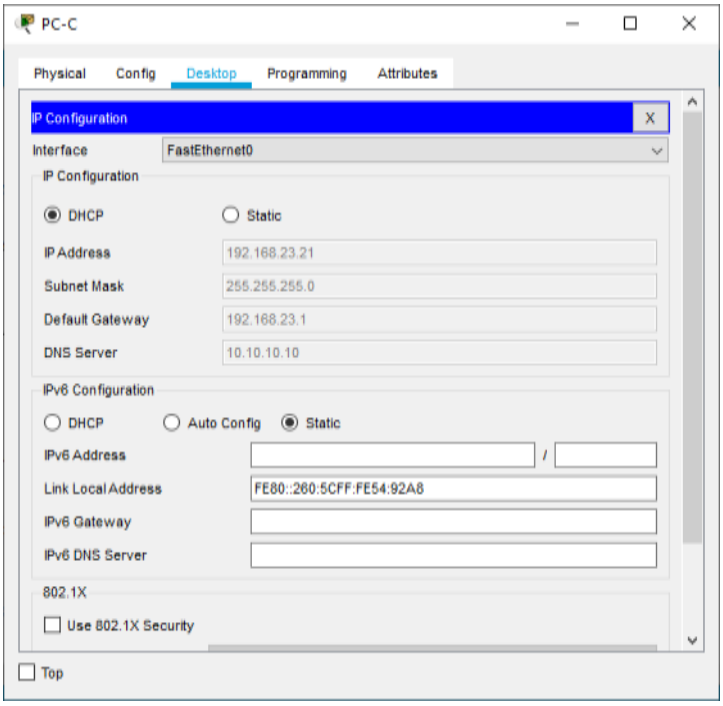
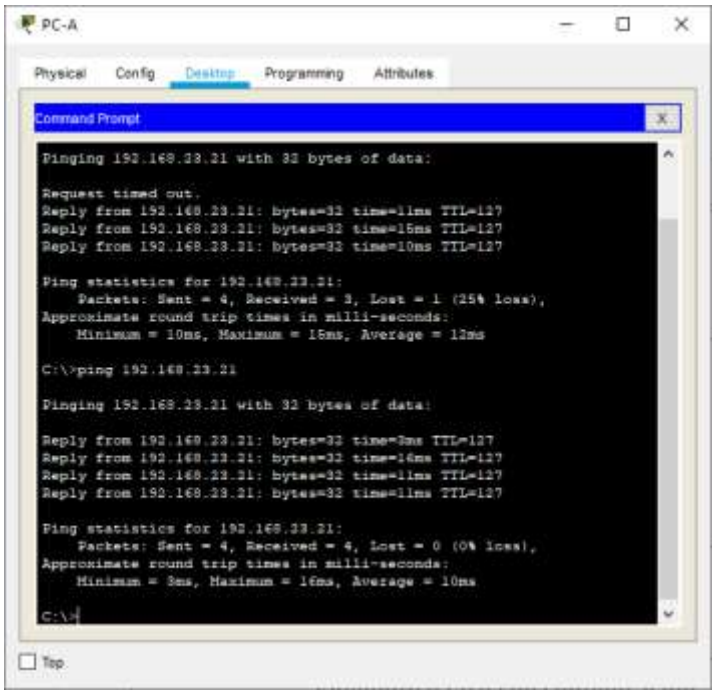
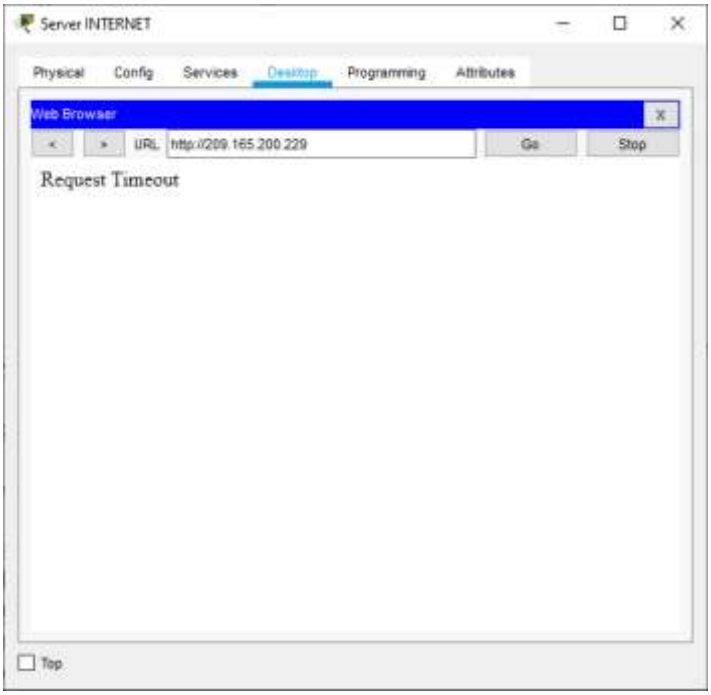
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	

Figura 12 Informacion DHCP de la PC-A

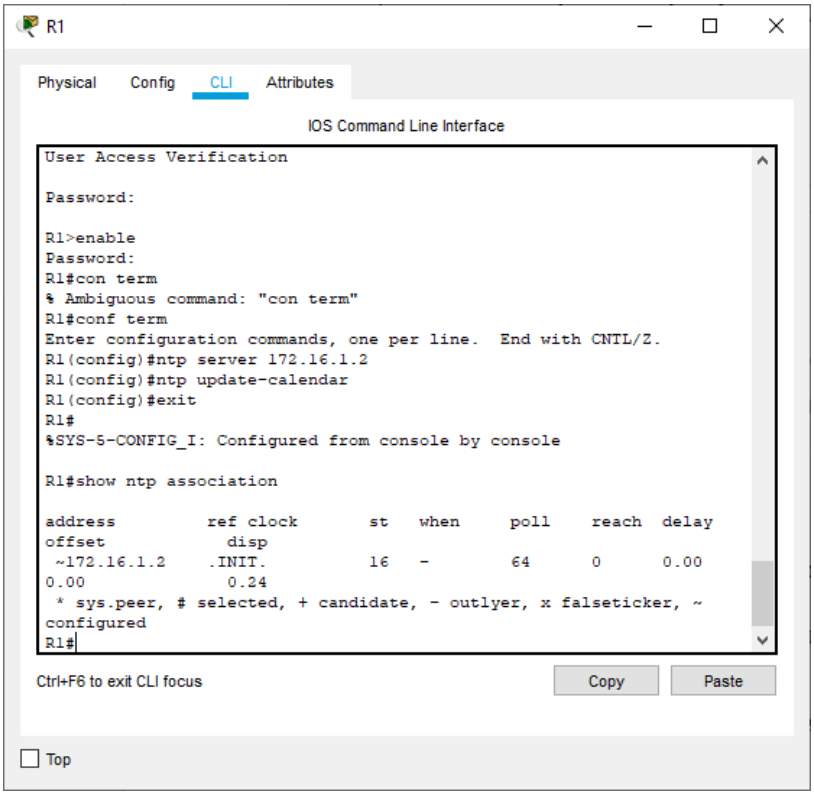
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Figura 13 Información DHCP de la PC-C
Verificar que la PC-A pueda hacer ping a la PC-C	 Figura 14 Ping entre la PC-A Y PC-C

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	 Figura 15 Navegador web de la PC Internet

4.6 Configurar NTP

Tabla 20 Configuración NTP de los router 1 y 2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**R2#clock set 9:00:00 5 march 2016**
Configure R2 como un maestro NTP.	R2#ntp master 5 R2#ntp master stratum 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 R1(config)#exit

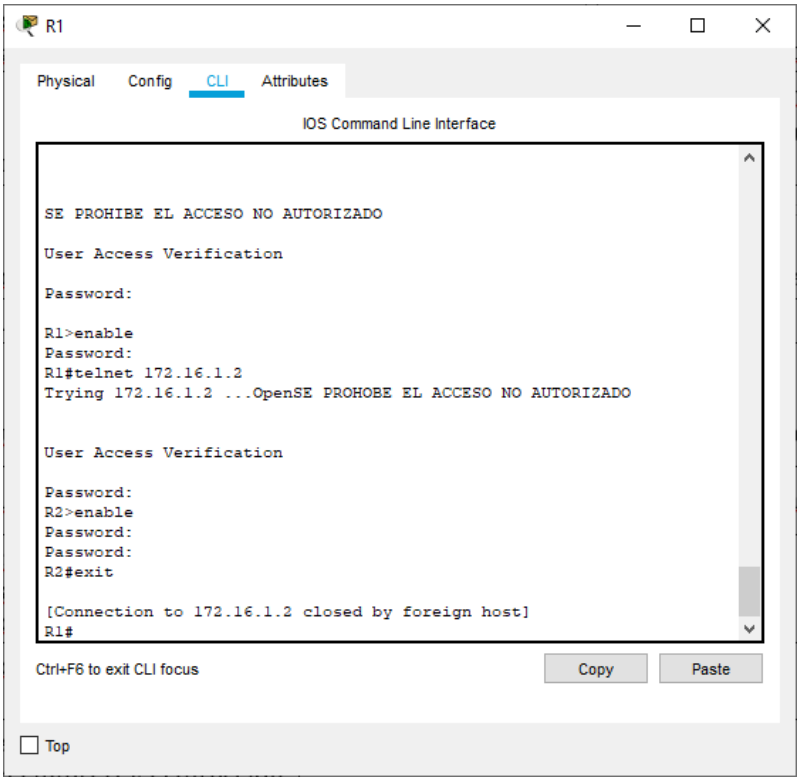
Verifique la configuración de NTP en R1.	 Figura 16 Verificacion de la configuracion NTP de R1 R1#show ntp association

4.7 Configurar y verificar las listas de control de acceso (ACL)

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

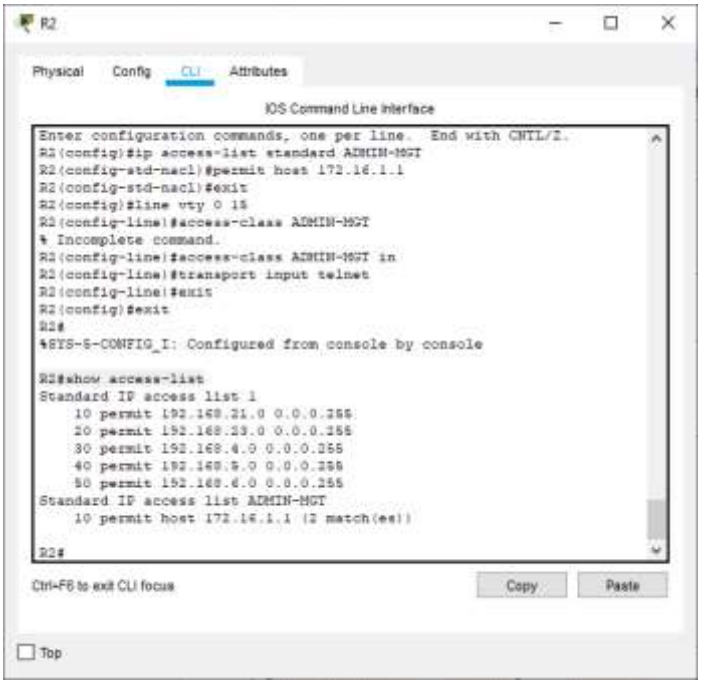
Tabla 21 Configuracion y verificación de las listas de control de acceso

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 15 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
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2  Figura 17 Conexion Telnet de R1

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

Tabla 22 Listas de acceso

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list  Figura 18 Access List de R2
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 interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

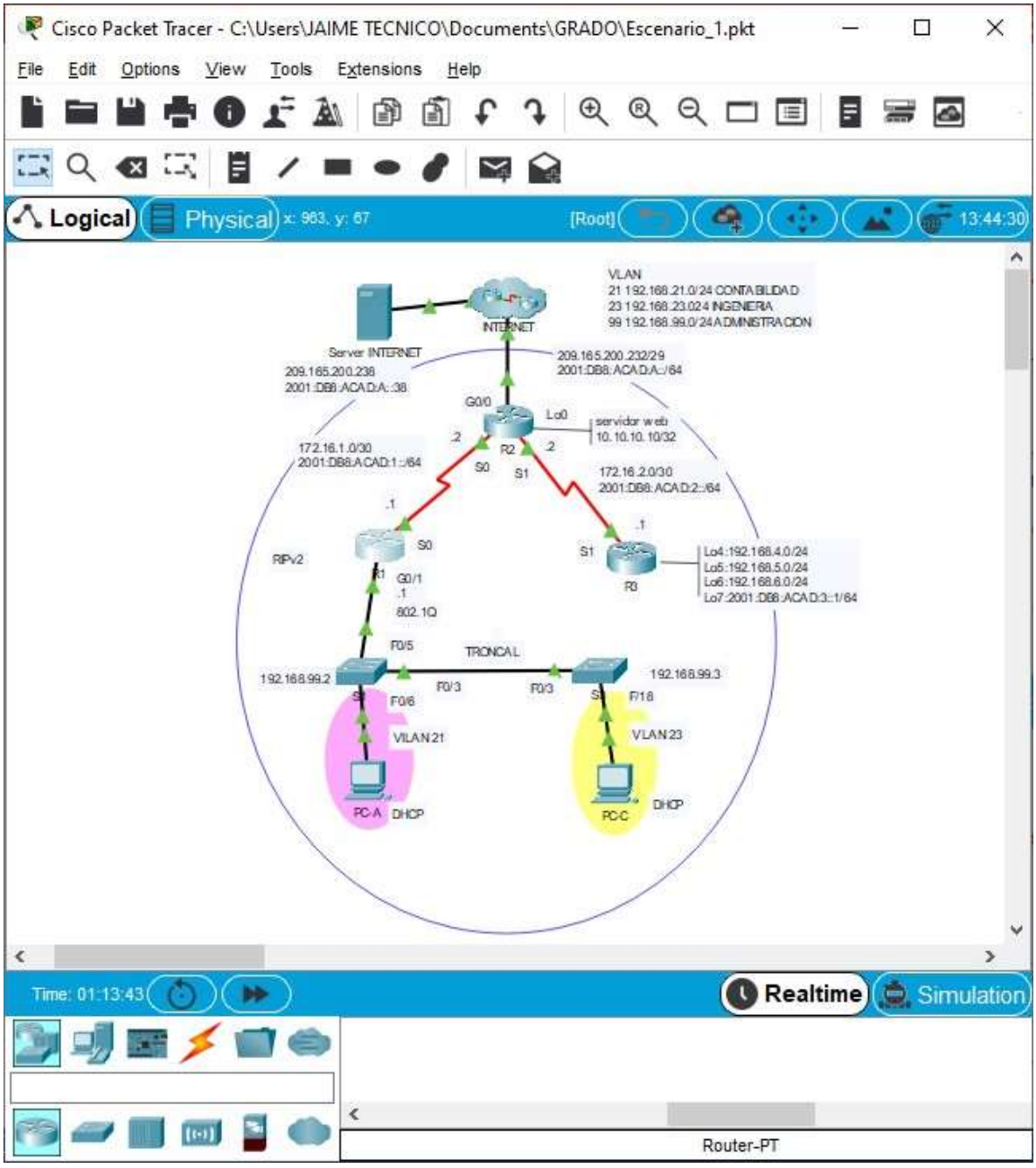


Figura 19 Topología desarrollada escenario 1

5. DESARROLLO DEL ESCENARIO 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

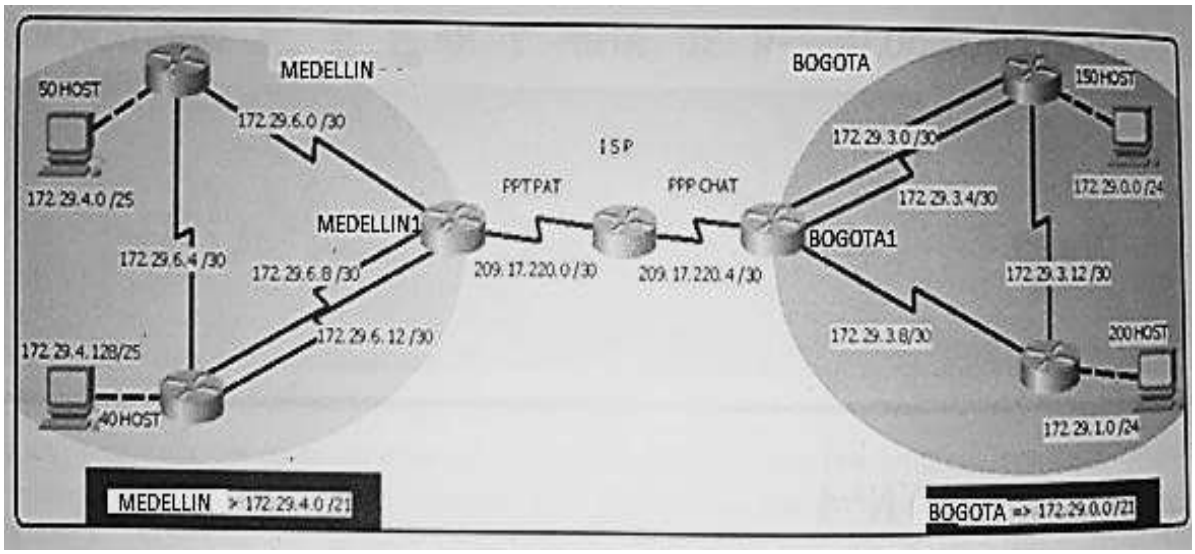


Figura 20 Topología a elaborar escenario 2

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.

6. DIGNOSTICO Y CONFIGURACION DE TODOS LOS EQUIPOS

Realizamos la configuración inicial de todos los equipos. (Asignar nombres de equipos, asignar claves de seguridad, etc). Además configuramos los puertos de acuerdo a la topología propuesta.

CONFIGURAR ROUTER DE ISP

Tabla 23 Configuración inicial del router ISP

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	ISP(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname ISP
Contraseña de exec privilegiado cifrada	ISP(config)#enable secret class
Contraseña de acceso a la consola	ISP(config)#line console 0 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#exit
Contraseña de acceso Telnet	ISP(config)#line vty 0 15 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#exit
Cifrar las contraseñas de texto no cifrado	ISP(config)#service password-encryption
Mensaje MOTD	ISP(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	ISP(config)#inter s0/0/0 ISP(config-if)#description conexion al router Medellin 1 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config)#clock rate 128000 ISP(config-if)#no shutdown

Interfaz S0/0/1	ISP(config-if)#inter s0/0/1 ISP(config-if)#description conexion al router BOGOTA 1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown

CONFIGURAR EL ROUTER BOGOTA 1

Tabla 24 Configuración inicial del router BOGOTA 1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	BOGOTA1(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname BOGOTA1
Contraseña de exec privilegiado cifrada	BOGOTA1(config)#enable secret class
Contraseña de acceso a la consola	BOGOTA1(config)#line console 0 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#exit
Contraseña de acceso Telnet	BOGOTA1(config)#line vty 0 15 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	BOGOTA1(config)#service password-encryption
Mensaje MOTD	BOGOTA1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	BOGOTA1(config)#inter s0/0/0 BOGOTA1(config-if)#description conexion al router ISP BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#no shutdown

Interfaz S0/0/1	BOGOTA1(config-if)#inter s0/0/1 BOGOTA1(config-if)#description conexion al router BOGOTA 2 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown
Interfaz S0/1/0	BOGOTA1(config-if)#inter s0/1/0 BOGOTA1(config-if)#description conexion al router BOGOTA 2 R BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shutdown
Interfaz S0/1/1	BOGOTA1(config-if)#inter s0/1/1 BOGOTA1(config-if)#description conexion al router BOGOTA 3 BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252 BOGOTA1(config-if)#no shutdown

CONFIGURAR ROUTER BOGOTA 2

Tabla 25 Configuración inicial del router BOGOTA 2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	BOGOTA2(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname BOGOTA2
Contraseña de exec privilegiado cifrada	BOGOTA2(config)#enable secret class
Contraseña de acceso a la consola	BOGOTA2(config)#line console 0 BOGOTA2(config-line)#password cisco BOGOTA2(config-line)#login BOGOTA2 (config-line)#exit
Contraseña de acceso Telnet	BOGOTA2(config)#line vty 0 15 BOGOTA2(config-line)#password cisco BOGOTA2(config-line)#login BOGOTA2(config-line)#exit

Cifrar las contraseñas de texto no cifrado	BOGOTA2(config)#service password-encryption
Mensaje MOTD	BOGOTA2(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	BOGOTA2(config)#inter s0/0/0 BOGOTA2(config-if)#description conexion al router BOGOTA 1 BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA2(config-if)#no shutdown
Interfaz S0/0/1	BOGOTA2(config-if)#inter s0/0/1 BOGOTA2(config-if)#description conexion al router BOGOTA 1R BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA2(config-if)#no shutdown
Interfaz S0/1/0	BOGOTA2(config-if)#inter s0/1/0 BOGOTA2(config-if)#description conexion al router BOGOTA 3 BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252 BOGOTA2(config-if)#clock rate 128000 BOGOTA2(config-if)#no shutdown
Interfaz G0/0	BOGOTA2(config-if)#inter g0/0 BOGOTA2(config-if)#description conexion al PC 2 BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0 BOGOTA2(config-if)#no shutdown

CONFIGURAR ROUTER BOGOTA 3

Tabla 26 Configuración inicial del router BOGOTA 3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	BOGOTA3(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname BOGOTA3
Contraseña de exec privilegiado cifrada	BOGOTA3(config)#enable secret class

Contraseña de acceso a la consola	BOGOTA3(config)#line console 0 BOGOTA3(config-line)#password cisco BOGOTA3(config-line)#login BOGOTA3(config-line)#exit
Contraseña de acceso Telnet	BOGOTA3(config)#line vty 0 15 BOGOTA3(config-line)#password cisco BOGOTA3(config-line)#login BOGOTA3 (config-line)#exit
Cifrar las contraseñas de texto no cifrado	BOGOTA3(config)#service password-encryption
Mensaje MOTD	BOGOTA3(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	BOGOTA3(config)#inter s0/0/0 BOGOTA3(config-if)#description conexion al router BOGOTA 2 BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA3(config-if)#no shutdown
Interfaz S0/0/1	BOGOTA3(config-if)#inter s0/0/1 BOGOTA3(config-if)#description conexion al router BOGOTA 1 BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252 BOGOTA3(config-if)#no shutdown
Interfaz G0/0	BOGOTA3(config-if)#inter g0/0 BOGOTA3(config-if)#description conexion al PC3 BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0 BOGOTA3(config-if)#no shutdown

CONFIGURAR ROUTER MEDELLIN 1

Tabla 27 Configuración inicial del router MEDELLIN 1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	MEDELLIN1(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname MEDELLIN1

Contraseña de exec privilegiado cifrada	MEDELLIN1(config)#enable secret class
Contraseña de acceso a la consola	MEDELLIN1(config)#line console 0 MEDELLIN1(config-line)#password cisco MEDELLIN1(config-line)#login MEDELLIN1(config-line)#exit
Contraseña de acceso Telnet	MEDELLIN1(config)#line vty 0 15 MEDELLIN1(config-line)#password cisco MEDELLIN1(config-line)#login MEDELLIN1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	MEDELLIN1(config)#service password-encryption
Mensaje MOTD	MEDELLIN1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	MEDELLIN1(config)#inter s0/0/0 MEDELLIN1(config-if)#description conexion al router ISP MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252 MEDELLIN1(config-if)#no shutdown
Interfaz S0/0/1	MEDELLIN1(config-if)#inter s0/0/1 MEDELLIN1(config-if)#description conexion al router MEDELLIN 2 MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown
Interfaz S0/1/0	MEDELLIN1(config-if)#inter s0/1/0 MEDELLIN1(config-if)#description conexion al router MEDELLIN 2 R MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shutdown

Interfaz S0/1/1	MEDELLIN1(config-if)#inter s0/1/1 MEDELLIN1(config-if)#description conexion al router MEDELLIN 3 MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252 MEDELLIN(config-if)#no shutdown

CONFIGURAR ROUTER MEDELLIN 2

Tabla 28 Configuración inicial del router MEDELLIN 2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	MEDELLIN2(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname MEDELLIN2
Contraseña de exec privilegiado cifrada	MEDELLIN2(config)#enable secret class
Contraseña de acceso a la consola	MEDELLIN2(config)#line console 0 MEDELLIN2(config-line)#password cisco MEDELLIN2(config-line)#login MEDELLIN2(config-line)#exit
Contraseña de acceso Telnet	MEDELLIN2(config)#line vty 0 15 MEDELLIN2(config-line)#password cisco MEDELLIN2(config-line)#login MEDELLIN2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	MEDELLIN2 (config)#service password-encryption
Mensaje MOTD	MEDELLIN2(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	MEDELLIN2(config)#inter s0/0/0 MEDELLIN2(config-if)#description conexion al router MEDELLIN 1 MEDELLIN2(config-if)#ip address 172.29.6.10 255.255.255.252 MEDELLIN2(config-if)#no shutdown

Interfaz S0/0/1	MEDELLIN2(config-if)#inter s0/0/1 MEDELLIN2(config-if)#description conexion al router MEDELLIN 1 R MEDELLIN2(config-if)#ip address 172.29.6.14 255.255.255.252 MEDELLIN2(config-if)#no shutdown
Interfaz S0/1/0	MEDELLIN2(config-if)#inter s0/1/0 MEDELLIN2(config-if)#description conexion al router MEDELLIN 3 MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252 MEDELLIN2(config-if)#clock rate 128000 MEDELLIN2(config-if)#no shutdown
Interfaz G0/1	MEDELLIN2(config-if)#inter g0/1 MEDELLIN2(config-if)#description conexion al PC1 MEDELLIN2(config-if)#ip address 172.29.4.129 255.255.255.128 MEDELLIN2(config-if)#no shutdown

CONFIGURAR ROUTER MEDELLIN 3

Tabla 29 Configuración inicial del router MEDELLIN 3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	MEDELLIN3(config)#no ip domain-lookup
Nombre del router	Router(config)#Hostname MEDELLIN3
Contraseña de exec privilegiado cifrada	MEDELLIN3(config)#enable secret class
Contraseña de acceso a la consola	MEDELLIN3(config)#line console 0 MEDELLIN3(config-line)#password cisco MEDELLIN3(config-line)#login MEDELLIN3(config-line)#exit
Contraseña de acceso Telnet	MEDELLIN3(config)#line vty 0 15 MEDELLIN3(config-line)#password cisco MEDELLIN3(config-line)#login MEDELLIN3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	MEDELLIN3(config)#service password-encryption

Mensaje MOTD	MEDELLIN3(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	MEDELLIN3(config)#inter s0/0/0 MEDELLIN3(config-if)#description conexion al router MEDELLIN 2 MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252 MEDELLIN3(config-if)#no shutdown
Interfaz S0/0/1	MEDELLIN3(config-if)#inter s0/0/1 MEDELLIN3(config-if)#description conexion al router MEDELLIN 1 MEDELLIN3(config-if)#ip address 172.29.6.2 255.255.255.252 MEDELLIN3(config-if)#no shutdown
Interfaz G0/1	MEDELLIN3(config-if)#inter g0/1 MEDELLIN3(config-if)#description conexion al PC0 MEDELLIN3(config-if)#ip address 172.29.4.1 255.255.255.128 MEDELLIN3(config-if)#no shutdown

7. CONEXIÓN FÍSICAS DE LOS EQUIPOS CON BASE EN LA TOPOLOGÍA DE RED

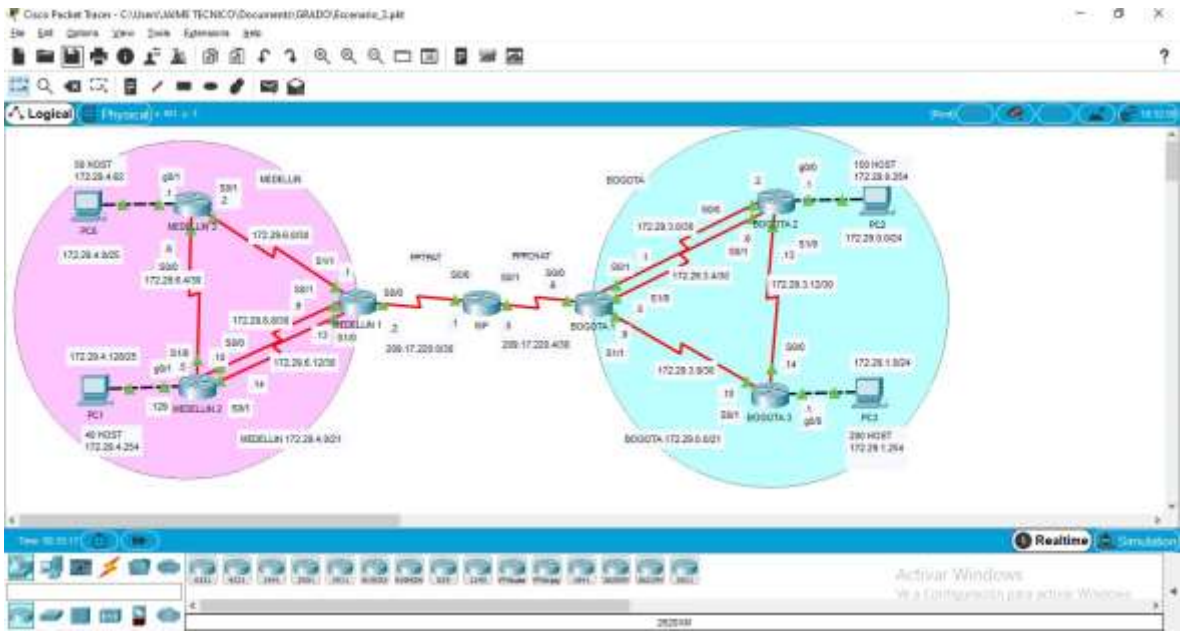


Figura 21 Topología escenario 2

TABLA DE DIRECCIONAMIENTO DE ACUERDO A LA TOPOLOGIA ESCENARIO 2

Tabla 30 Direcciones ip de todos los equipos

NOMBRE	RED	INTERFAZ	IP	SUB NET	GATEWAY
ISP	209.17.220.0/30	s0/0/0	209.17.220.1	255.255.255.252	
7.7.7.7	209.17.220.4/30	s0/0/1	209.17.220.5	255.255.255.252	
Bogota 1	209.17.220.4/30	s0/0/0	209.17.220.6	255.255.255.252	
ID OSPF	172.29.3.0/30	s0/0/1	172.29.3.1	255.255.255.252	
1.1.1.1	172.29.3.4/30	s0/1/0	172.29.3.5	255.255.255.252	
	172.29.3.8/30	s0/1/1	172.29.3.9	255.255.255.252	
Bogota 2	172.29.3.0/30	s0/0/0	172.29.3.2	255.255.255.252	

ID OSPF	172.29.3.4/30	s0/0/1	172.29.3.6	255.255.255.252	
2.2.2.2	172.29.3.12/30	s0/1/0	172.29.3.13	255.255.255.252	
	172.29.0.0/24	g0/0	172.29.0.1	255.255.255.0	
PC2	172.29.0.0/25		172.29.0.126	255.255.255.1	172.29.0.1
Bogota 3	172.29.3.12/30	s0/0/0	172.29.3.14	255.255.255.252	
ID OSPF	172.29.3.8/30	s0/0/1	172.29.3.10	255.255.255.252	
3.3.3.3	172.29.1.0/24	g0/0	172.29.1.1	255.255.255.0	
PC3	172.29.1.0/24		172.29.1.254	255.255.255.1	172.29.1.1
Medellin 1	209.17.220.0/30	s0/0/0	209.17.220.2	255.255.255.252	
ID OSPF	172.29.6.8/30	s0/0/1	172.29.6.9	255.255.255.252	
4.4.4.4	172.29.6.12/30	s0/1/0	172.29.6.13	255.255.255.252	
	172.29.6.0/30	s0/1/1	172.29.6.1	255.255.255.252	
Medellin 2	172.29.6.8/30	s0/0/0	172.29.6.10	255.255.255.252	
ID OSPF	172.29.6.12/30	s0/0/1	172.29.6.14	255.255.255.252	
5.5.5.5	172.29.6.4/30	s0/1/0	172.29.6.5	255.255.255.252	
	172.29.4.128/25	g0/1	172.29.4.129	255.255.255.128	
PC1	172.29.4.128/26		172.29.4.254	255.255.255.128	172.29.4.129
Medellin 3	172.29.6.4/30	s0/0/0	172.29.6.6	255.255.255.252	
ID OSPF	172.29.6.0/30	s0/0/1	172.29.6.2	255.255.255.252	
6.6.6.6	172.29.4.0/25	g0/1	172.29.4.1	255.255.255.128	
PCO	172.29.4.0/26		172.29.4.62	255.255.255.128	172.29.4.1

7.1 Configuración del enrutamiento

Tabla 31 Configuración de enrutamiento

Elemento o tarea de configuración	Especificación
a. Configuramos el enrutamiento con el protocolo OSPF, además se nombró cada dispositivo con un route-id, no se desactivo el auto-cost. Además se declaró la red principal.	ISP(config)#router ospf 1 ISP(config-router)#router-id 7.7.7.7 ISP(config-router)#network 209.17.220.0 0.0.0.255 area 0 ISP(config-router)#exit BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#router-id 1.1.1.1 BOGOTA1(config-router)#network 172.29.3.0 0.0.0.255 area 0 BOGOTA1(config-router)#exit BOGOTA2(config)#router ospf 1 BOGOTA2(config-router)#router-id 2.2.2.2 BOGOTA2(config-router)#network 172.29.3.0 0.0.0.255 area 0 BOGOTA2(config-router)#exit BOGOTA3(config)#router ospf 1 BOGOTA3(config-router)#router-id 3.3.3.3 BOGOTA3(config-router)#network 172.29.3.0 0.0.0.255 area 0 BOGOTA3(config-router)#exit MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#router-id 4.4.4.4 MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.255 area 0 MEDELLIN1(config-router)#exit MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#router-id 5.5.5.5

	MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.255 area 0 MEDELLIN2(config-router)#exit MEDELLIN3(config)#router ospf 1 MEDELLIN3(config-router)#route-id 6.6.6.6 MEDELLIN3(config-router)#network 172.29.6.0 0.0.0.255 area 0 MEDELLIN3(config-router)#exit
b. Se añadió a la configuración de enrutamiento una ruta por defecto desde router BOGOTA 1 Y MEDELLIN 1, hacia el router ISP, también a su vez se distribuyó mediante OSPF en las publicaciones.	BOGOTA1(config-)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 BOGOTA1(config)#route ospf 1 BOGOTA1(config-router)#default-information originate MEDELLIN1(config-)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 MEDELLIN1(config)#route ospf 1 MEDELLIN1(config-router)#default-information originate
c. Se crea una ruta estática desde el router dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.	ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/0/0 ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/0/1

7. 2 Tabla de Enrutamiento.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
b. Verificar el balanceo de carga que presentan los routers.
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

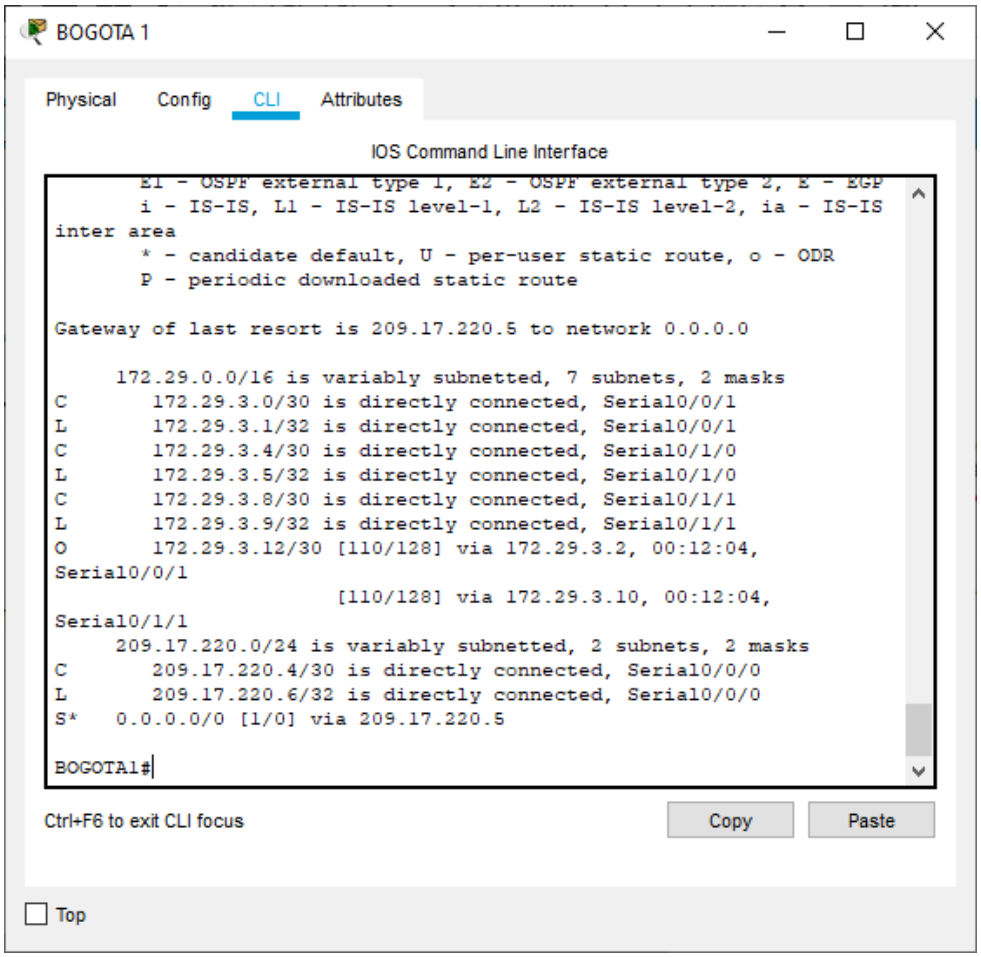


Figura 22 Tabla de enrutamiento BOGOTA 1

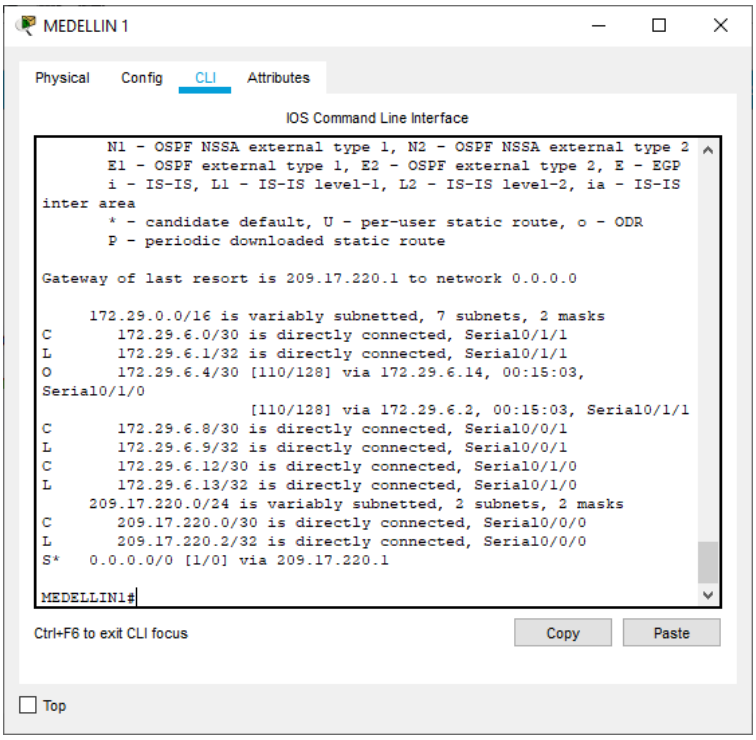


Figura 23 Tabla de enrutamiento MEDELLIN 1

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

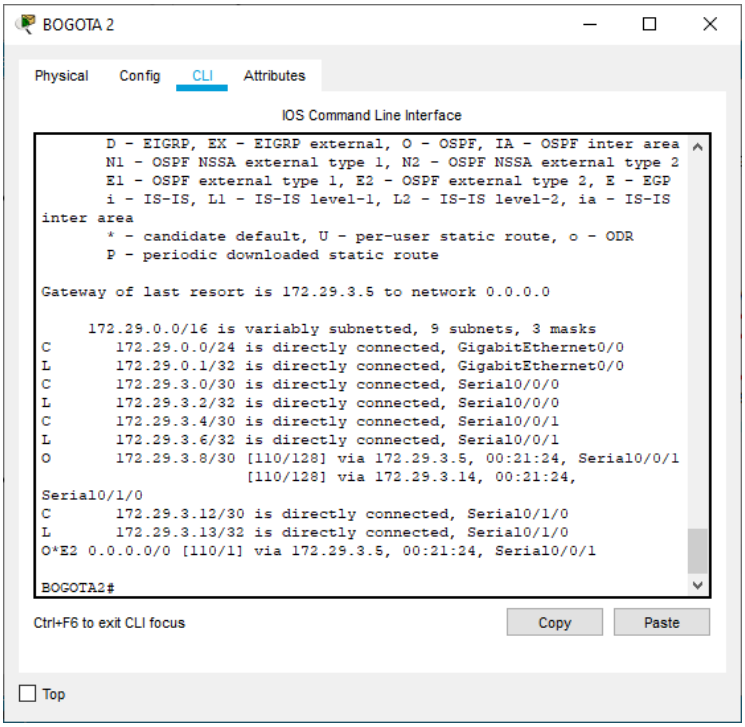


Figura 24 Tabla de enrutamiento BOGOTA 2

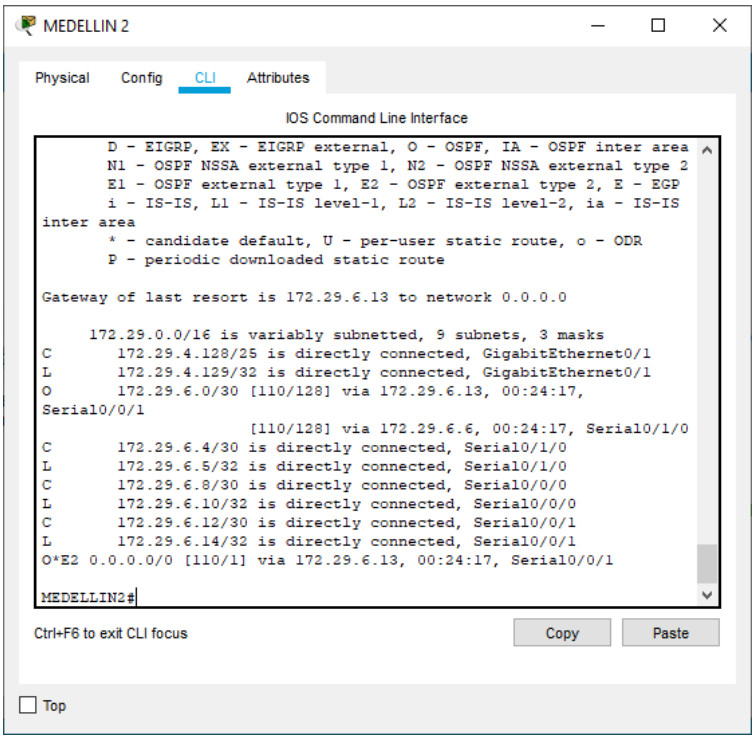


Figura 25 Tabla de enrutamiento MEDELLIN 2

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

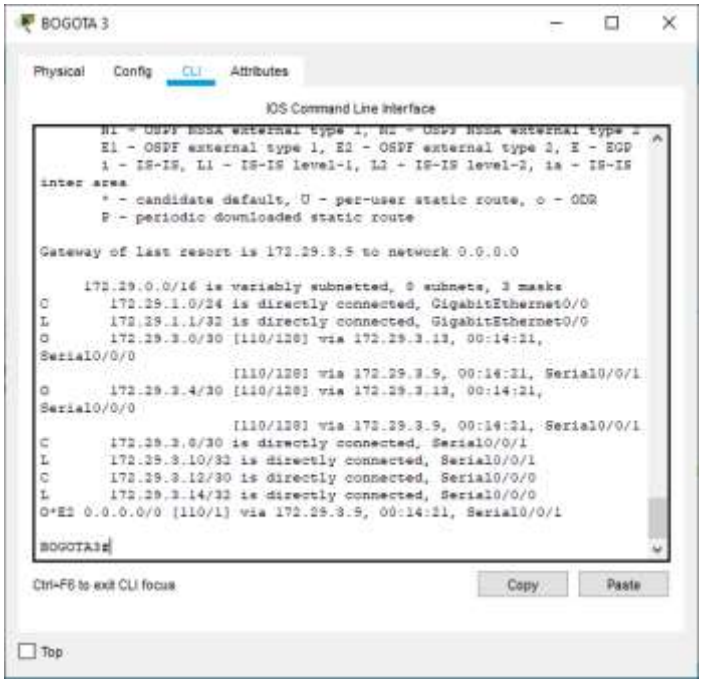


Figura 26 Tabla de enrutamiento BOGOTA 3

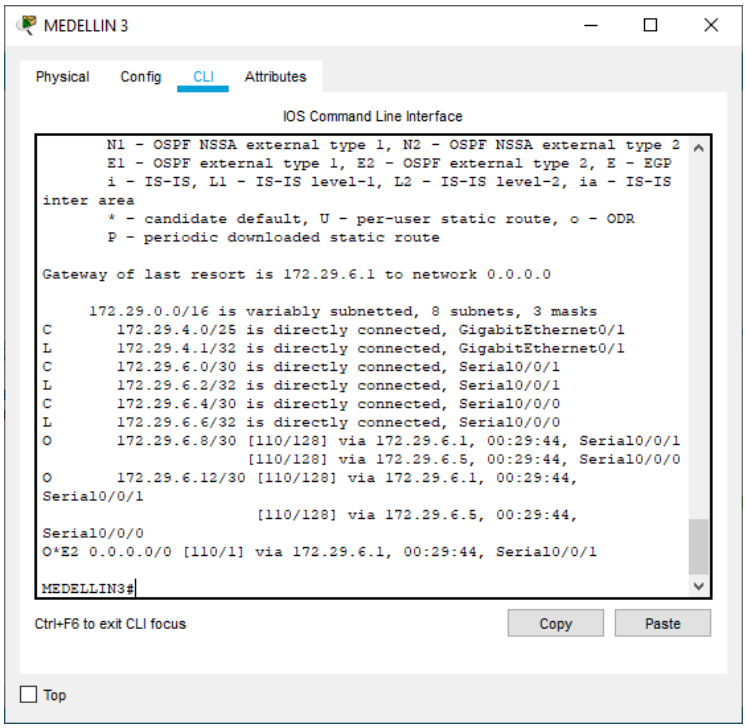


Figura 27 Tabla de enrutamiento MEDELLIN 3

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

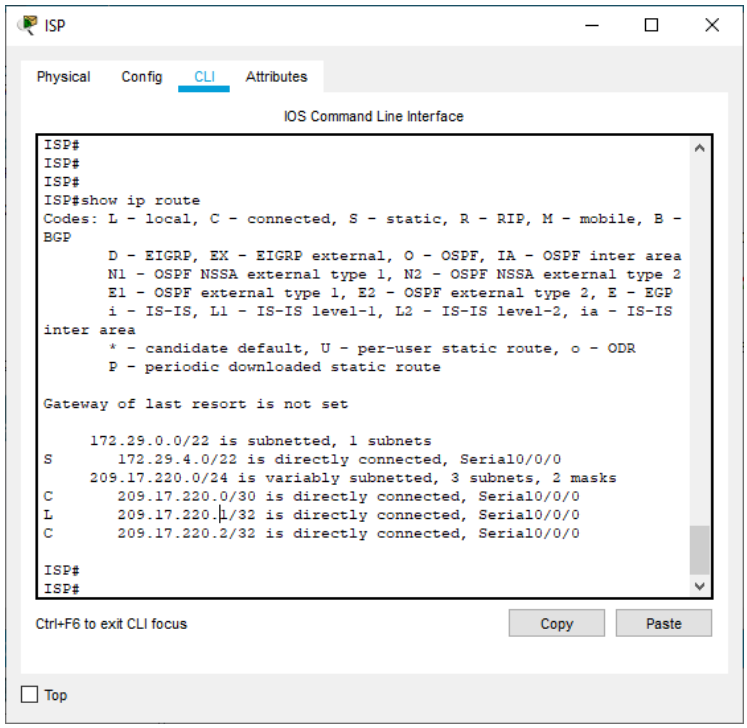


Figura 28 Tabla de enrutamiento ISP

7.3 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

7.4 Verificación del protocolo OSPF.

Tabla 32 Verificación del protocolo OSPF

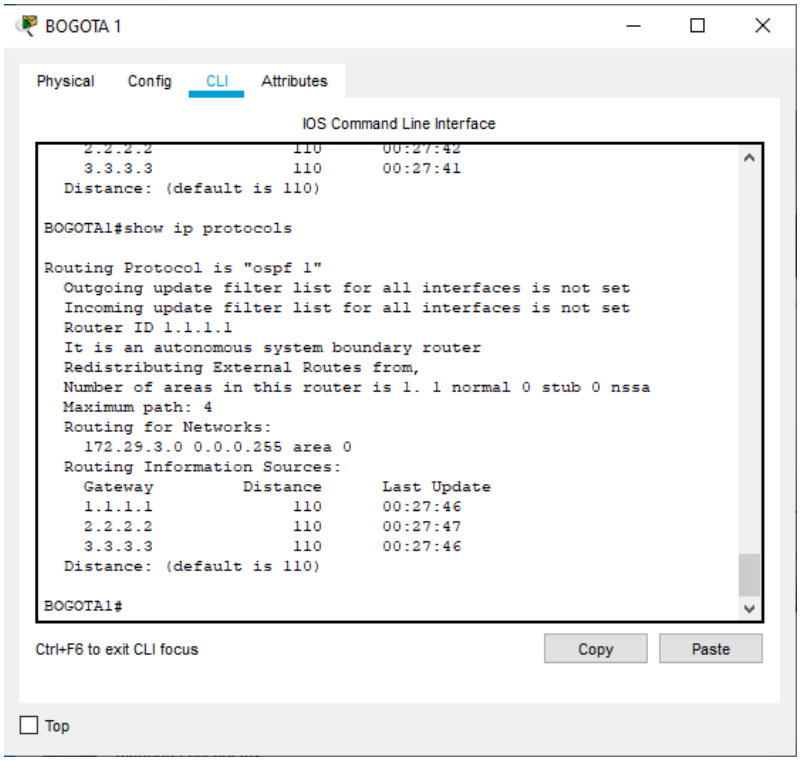
Elemento o tarea de configuración	Especificación
a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el **passive interface** para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.	

Figura 29 Verification del protocolo OSPF de BOGOTA 1

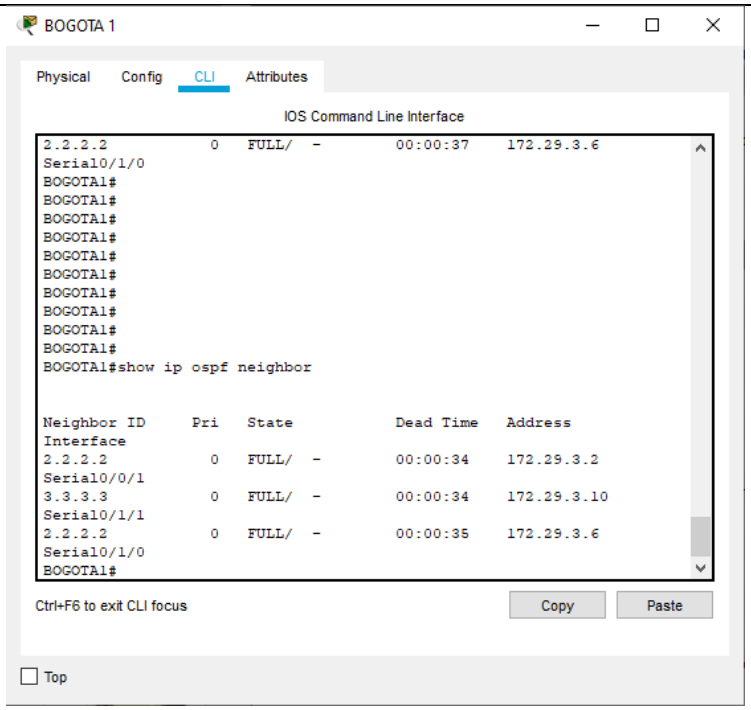


Figura 30 OSPF Neighbor de BOGOTA 1

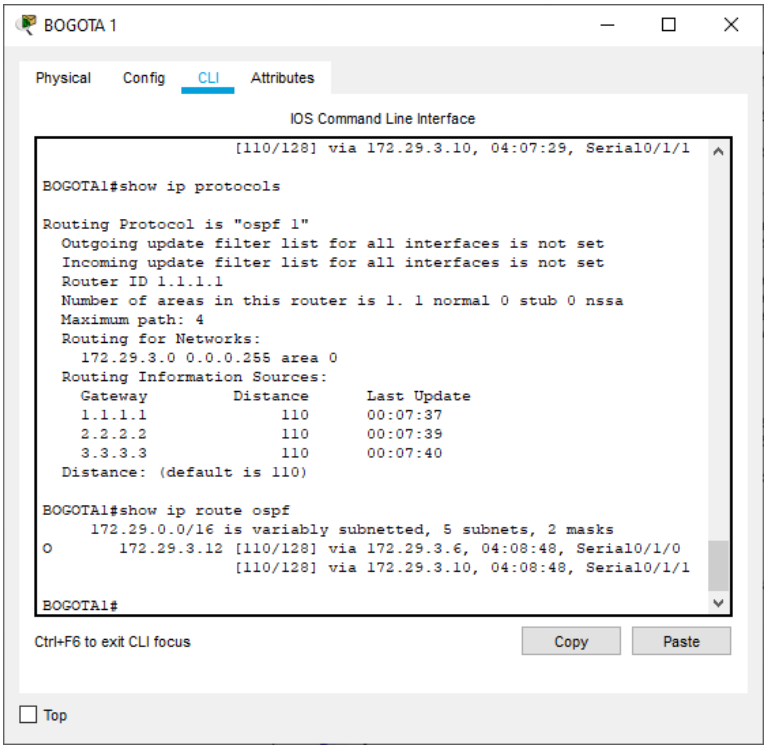


Figura 31 OSPF Route de BOGOTA 1

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.

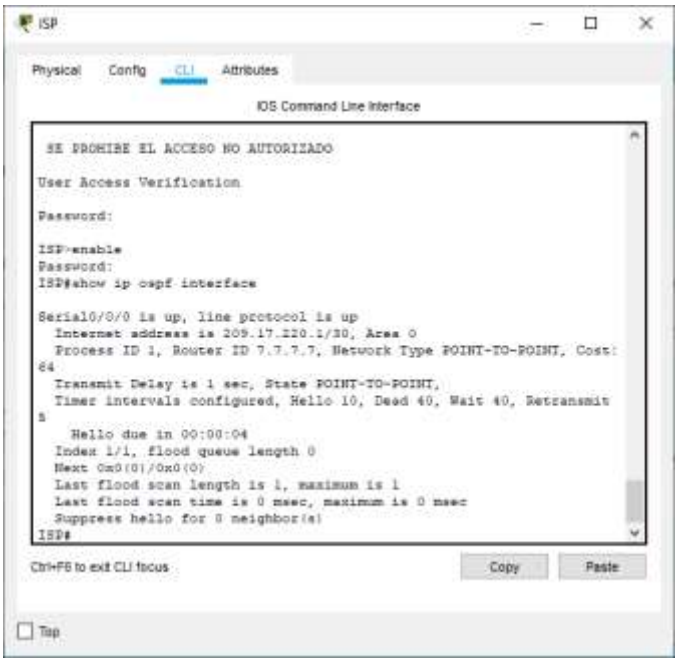


Figura 32 OSPF Interface de ISP

Figura 33 OSPF Interface de BOGOTA 1

Figura 34 OSPF Interface de BOGOTA 2

Figura 35 OSPF Interface de BOGOTA 3

Figura 36 OSPF Interface de MEDELLIN 1

Figura 37 OSPF Interface de MEDELLIN 2

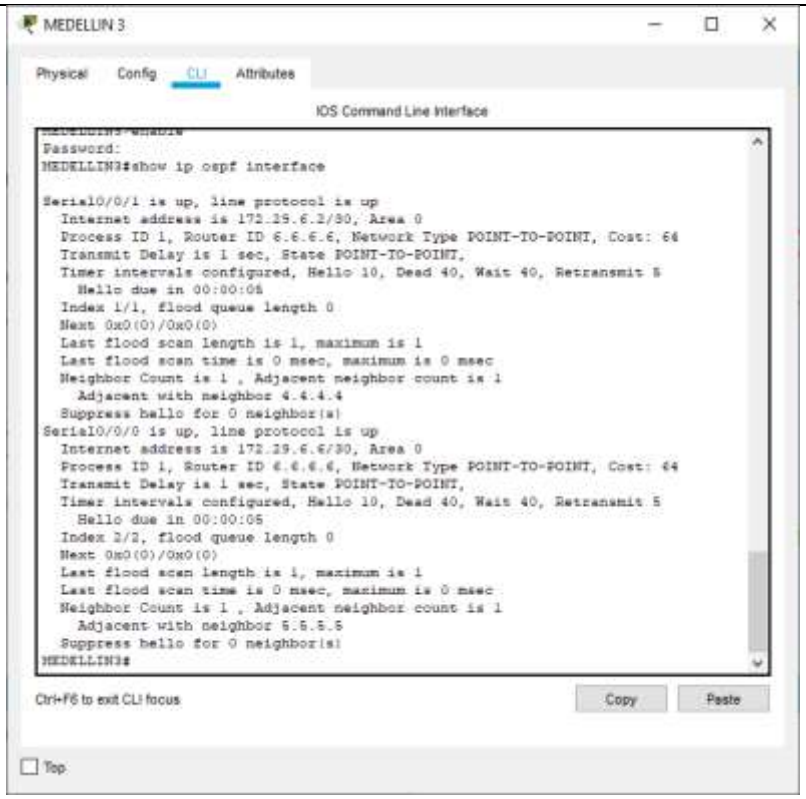


Figura 38 OSPF Interface de MEDELLIN 3

7.5 Configurar encapsulamiento y autenticación PPP.

Tabla 33 Configuración PPP

Elemento o tarea de configuración	Especificación
a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.	MEDELLIN1(config)#username adminmed1 password cisco MEDELLIN1(config)#inter s0/0/0 MEDELLIN1(config-if)#encapsulation ppp MEDELLIN1(config-if)#ppp authentication pap ISP(config)#inter s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp pap sent-username adminmed1 password cisco
b. El enlace Bogotá1 con ISP se debe configurar	BOGOTA1(config)#username ISP password cisco

con autenticación CHAT.	BOGOTA1(config)#inter s0/0/1 BOGOTA1(config-if)#encapsulation ppp BOGOTA1(config-if)#ppp authentication chap ISP(config)#username BOGOTA1 password cisco ISP(config)#inter s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap

7.6 Configuración de PAT.

Elemento o tarea de configuración	Especificación
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.	BOGOTA1(config)#inter s0/0/0 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#inter s0/0/1 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#inter s0/1/0 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#inter s0/1/1 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#end MEDELLIN1(config)#inter s0/0/0 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#inter s0/0/1 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#inter s0/1/0 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#inter s0/1/1 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#end
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	MEDELLIN1(config)#ip nat pool afuera 209.17.220.2 209.17.220.2 netmask 255.255.255.0 MEDELLIN1(config)#access-list 1 permit 172.29.6.0 0.0.0.255 MEDELLIN1(config)#ip nat inside source list 1 pool afuera overload

prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.	MEDELLIN1(config)#exit
c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.	BOGOTA1(config)#ip nat pool afuera 209.17.220.6 209.17.220.6 netmask 255.255.255.0 BOGOTA1(config)#access-list 1 permit 172.29.3.0 0.0.0.255 BOGOTA1(config)#ip nat inside source list 1 pool afuera overload BOGOTA1(config)#exit

7.7 Configuración del servicio DHCP.

Elemento o tarea de configuración	**Especificación**
a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.	MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5 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 5.5.5.5 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 5.5.5.5 MEDELLIN2(dhcp-config)#exit
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.	MEDELLIN3(config)#interface s0/1/0 MEDELLIN3(config-if)#ip helper-address 172.29.6.5 MEDELLIN3(config-if)#exit
c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.	MEDELLIN2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4 MEDELLIN2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.4 MEDELLIN2(config)#ip dhcp pool BOGOTA2 MEDELLIN2(dhcp-config)#network 172.29.1.0 255.255.255.0 MEDELLIN2(dhcp-config)#default-router 172.29.1.1 MEDELLIN2(dhcp-config)#dns-server 5.5.5.5 MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp pool BOGOTA3 MEDELLIN2(dhcp-config)#network 172.29.0.0 255.255.255.0 MEDELLIN2(dhcp-config)#default-router 172.29.0.1 MEDELLIN2(dhcp-config)#dns-server 5.5.5.5 MEDELLIN2(dhcp-config)#exit
d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.	BOGOTA1(config)#interface s0/0/1 BOGOTA1(config-if)#ip helper-address 172.29.3.13 BOGOTA1(config-if)#exit

CONCLUSIONES

Comprendí la importancia de los protocolos de direccionamiento dinámico OSPF y RIPv2, ya que estos nos permiten manejar actualizaciones de enrutamiento sin intervención de un administrador de red, contrario al enrutamiento estático.

Diferenciamos el funcionamiento de los protocolos OSPF y RIPv2, OSPF tiene en cuenta el estado de los enlaces mientras RIPv2 tiene en cuenta el vector distancia.

Analizamos que RIPv2 utiliza saltos como métrica para determinar la ruta de los datos, esto quiere decir que tiene en cuenta la cantidad de dispositivos para que los datos lleguen a su destino.

Dedujimos que OSPF emplea métricas por costo, es decir tiene en cuenta el ancho de banda de la interface, por lo cual es robusto y rápido estando acorde al escenario dos.

BIBLIOGRAFÍA

Sitio web, CISCO Networking Academy, CP CCNA2 I-2020, CCNA R&S: Routing and Switching Essentials (https://www.netacad.com/portal/learning)

Sitio web, CISCO Networking Academy, CP CCNA2 I-2020, CCNA R&S: Introduction to Networks (https://www.netacad.com/portal/learning)

Sitio web, CS071 21.01 OSPF - Protocolos de Enrutamiento Dinámicos (Marion, http://www.mariontechacademy.org/, 2013)