DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JAIBERTH ALFONSO HENAO SÁNCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA INGENIERÍA DE TELECOMUNICACIONES

MEDELLIN - ANTIOQUIA

MAYO DE 2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JAIBERTH ALFONSO HENAO SÁNCHEZ

TRABAJO ESCRITO PARA OPTAR POR EL TÍTULO DE:

INGENIERO DE TELECOMUNICACIONES

ASESOR

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA INGENIERÍA DE TELECOMUNICACIONES

MEDELLIN - ANTIOQUIA

MAYO DE 2020

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

Firma Jurado

_____

Firma Tutor

Medellín – 20 de mayo del 2020

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Las habilidades prácticas que se adquieren realizando el curso de certificación cisco CCNA1 y CCNA2, sin duda son una herramienta valiosa para adentrarse en el mundo de la programación de dispositivos de red. En el caso de packet tracer como herramienta de simulación de redes, es de igual importancia el aprendizaje del entorno de simulación para posteriormente poder trabajar en equipos físicos y reales como administradores de redes; por lo tanto, le damos total atención al desarrollo de ejercicios prácticos que nos permitirán adoptar dichas competencias y poder disfrutar de tan útil tecnología.

ABSTRACT

The practical skills acquired by taking the Cisco CCNA1 and CCNA2 certification course are certainly a valuable tool for entering the world of network device programming. In the case of packet tracer as a network simulation tool, learning the simulation environment is of equal importance in order to later be able to work on real and physical teams as network administrators; therefore, we give full attention to the development of practical exercises that will allow us to adopt these skills and be able to enjoy such useful technology.

GLOSARIO

ACL: Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios accedan los recursos específicos.

Enrutamiento: También llamado ruteo, es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

Escenario: Es la interfaz de la herramienta de packet tracer, donde se visualiza todo el tema de configuración y los diferentes dispositivos para una mejor comprensión y detalle.

IPv4: Es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

IPv6: Es un sistema direccional del 128-bit usado para identificar un dispositivo en una red. Es el sucesor al IPv4 y a la mayoría de la versión reciente del sistema direccional usado en las redes informáticas.

Protocolos: Son el conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento. Dicha información se usa para construir y mantener las tablas de enrutamiento.

INTRODUCCIÓN

Las tecnologías de la información y las comunicaciones (TIC), han influido enormemente en la forma en como vemos el mundo hoy en día, se han implementado maneras de comunicación instantánea, formas de vender (E-comerce) y una multitud de aplicaciones que mejoran la calidad de vida de las personas que la utilizan.

Las tecnologías cisco, has sido desde sus inicios, un referente tecnológico en la implementación de redes de distribución de datos y tecnologías inteligentes modernas, y por esto, la importancia de la adquisición de habilidades que permitan utilizar todos estos recursos en beneficio de las personas. Dicho esto, el presente trabajo nos permitirá la adquisición de esas competencias mediante dos ejercicios completos con cierto grado de complejidad para demostrar y reforzar los conocimientos adquiridos en el diplomado de profundización cisco.

OBJETIVOS

OBJETIVO GENERAL

Plasmar de manera organizada y clara, las habilidades obtenidas en el desarrollo del curso de profundización cisco

OBJETIVOS ESPECIFICOS

- Investigar la aplicación de protocolos de enrutamiento en dispositivos cisco como OSPF y NAT

- Efectuar diagramas de diseños de redes y su respectiva configuración en el entorno de cisco packet tracer.

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

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

Topología

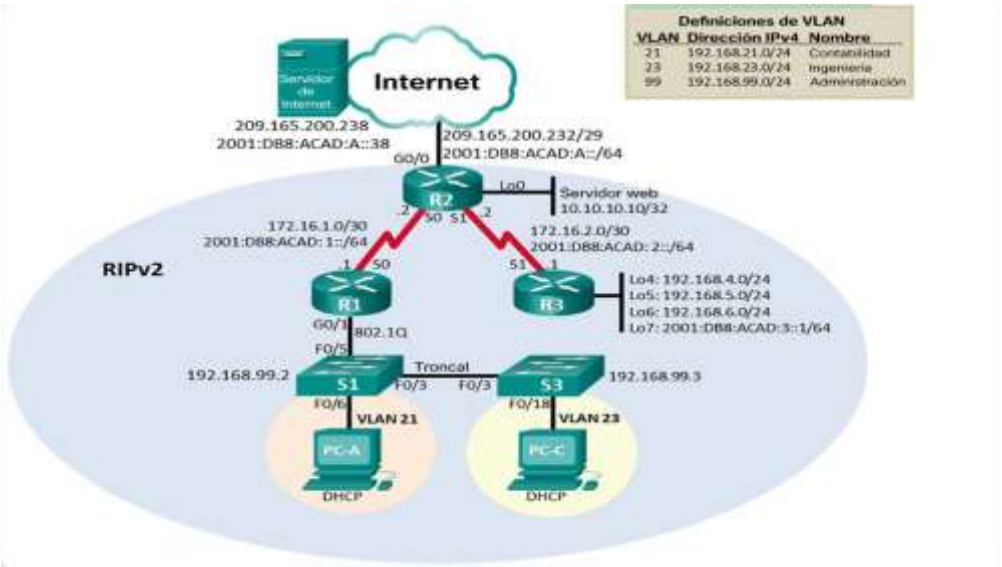

Figura 1. Escenario 1 Propuesto

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

Tabla 1. Configuración De Comando IOS

Router>en
Router#erase startup-config
Router#reload

Switch>en

Switch#erase startup-config

Switch#delete vlan.dat

Switch#reload

Switch#show flash

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 2: 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. Configuración Computadora 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.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Tabla 3. Configuración R1

Nota: Todavía no configure G0/1.

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
```

```
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd "Se prohibe el acceso no autorizado"

R1(config)#int s0/0/0
R1(config-if)#description conection to 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 shu
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 route ::/0 s0/0/0
```

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco

Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Habilitar el servidor HTTP	ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Tabla 4. Configuración R2

```
Router>en
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#banner motd "Se prohibe el acceso no autorizado"
```

```
R2(config)#int s0/0/0
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 shu

R2(config-if)#int s0/0/1
R2(config-if)#description conection to 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 shu

R2(config-if)#int g0/0
R2(config-if)#description conection 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 shu

R2(config)#int loopback 0

R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description simulated Web Server
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)#ipv6 route ::/0 g0/0
```

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz

Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Tabla 5. Configuración R3

```
Router>en
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd "Se prohibe el acceso no autorizado"
```

```
R3(config)#int s0/0/1
R3(config-if)#description conection to 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 shu

R3(config-if)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1
```

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class

Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 6. Configuración S1

```
Switch>en
Switch#config t
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd "Se prohibe el acceso no autorizado"
```

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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

Tabla 7. Configuración S3

```
Switch>en
Switch#config t
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
```

S3(config-line)#login

S3(config-line)#service password-encryption

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

Paso 8: 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**	**Success (5/5)**
R2	R3, S0/0/1	**172.16.2.1**	**Success (5/5)**
PC de Internet	Gateway predeterminado	**209.165.200.233**	**Success (5/5)**

Tabla 8. Verificación Conectividad

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

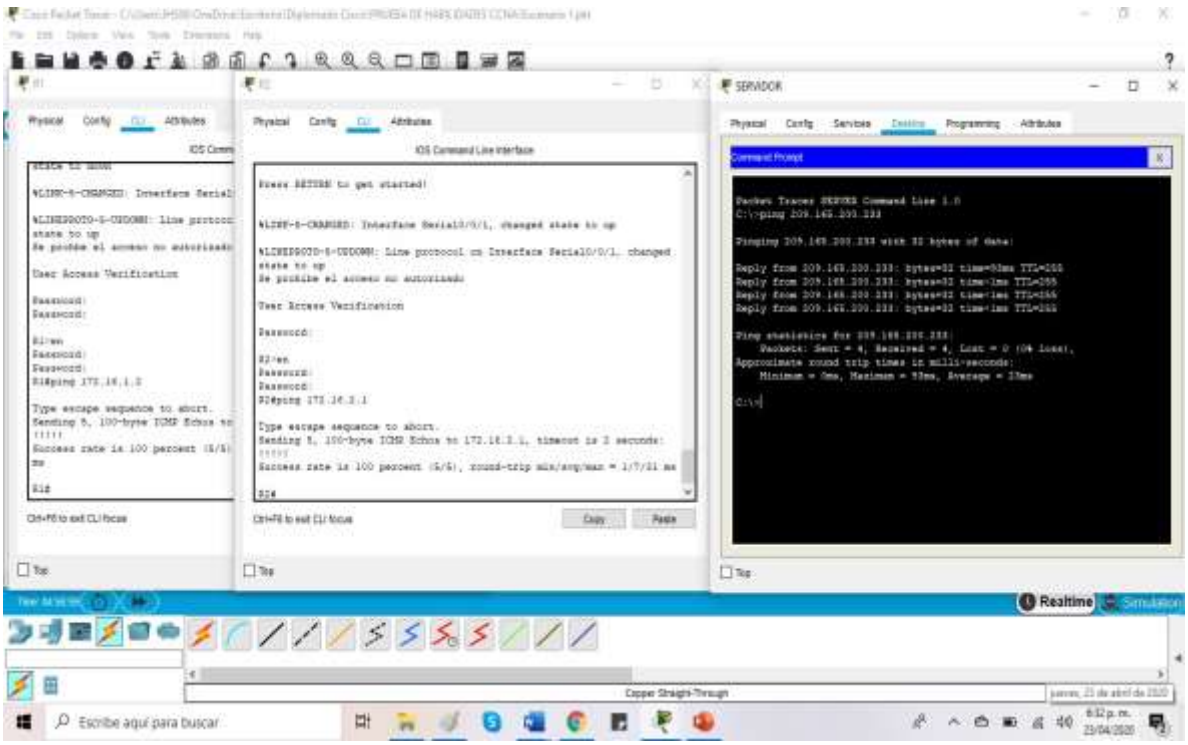

Figura 2. Ping R1 A R2

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican

Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 9. Configuración Seguridad S1

S1>en
Password:
S1#config t
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad

```
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shu
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
```

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	int f0/18 switchport access vlan 23
Apagar todos los puertos sin usar	int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 shutdown

Tabla 10. Base De Datos Vlan En S3

S3>en
Password:
S3#config t
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad

```
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shu
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S1(config-if-range)#shutdown
```

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	int g0/1 no shutdown

Tabla 11. Configuración 802.1Q .23 En R1

```
R1>en
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.21
R1(config-subif)#description vlan 21
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
```

```
R1(config-subif)#int g0/1.23
R1(config-subif)#description vlan 23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description vlan 23
R1(config-subif)#description vlan 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shutdown
```

Paso 4: Verificar la conectividad de la red

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

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

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Success (5/5)
S3	R1, dirección	192.168.99.1	Success (5/5)

	n VLAN 99		
S1	R1, direcció n VLAN 21	192.168.21. 1	Success (5/5)
S3	R1, direcció n VLAN 23	192.168.23. 1	Success (5/5)

Tabla 12: Verificación De Conectividad 2

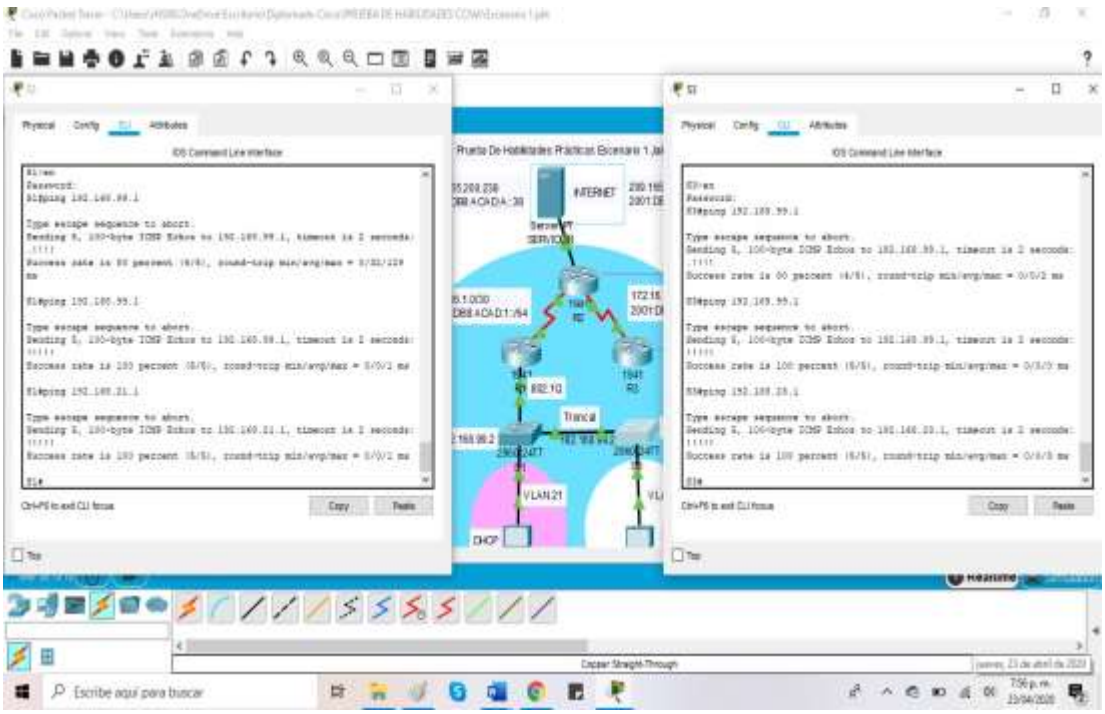

Figura 3. Evidencia Conectividad S1 A S3

Parte 3: 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	router rip version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary

Tabla 13. Configuración RIPv2 En R1

```
R1>en
Password:
R1#config t
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
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
```

R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary

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	router rip version 2
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. network 10.10.10.10 network 172.16.1.0 network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	passive-interface loopback 0
Desactive la sumarización automática.	no auto-summary

Tabla 14. Configuración RIPv2 En R2

R2>en
Password:
R2#config t
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show ip route connected
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0

R2(config-router)#network 172.16.2.0

R2(config-router)#passive-interface loopback 0

R2(config-router)#no auto-summary

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router rip version 2
Anunciar redes IPv4 conectadas directamente	network 172.16.2.0 network 192.168.4.0 network 192.168.5.0 network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface loopback 4 passive-interface loopback 5 passive-interface loopback 6
Desactive la sumarización automática.	no auto-summary

Tabla 15. Configuración RIPv3 En R2

R3>en

Password:

R3#config t

R3(config)#router rip

R3(config-router)#do show ip route connected

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
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary

Paso 4: Verificar la información de RIP

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

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

Tabla 16. Verificación Información RIP

Parte 4: 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	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	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Tabla 17. Configuración R1 Como Servidor DHCP

R1>en
Password:
R1#config t
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
```

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	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.237

Asignar la interfaz interna y externa para la NAT estática	ip nat inside source static 10.10.10.10 209.165.200.237 int g0/0 ip nat outside int s0/0/0 ip nat inside int s0/0/1 ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

Tabla 18. Configuración NAT En R2

R2>en
Password:
R2#config t
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server
R2(config)#ip http authentication local

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
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 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

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

Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Succesful
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Succesful

Tabla 19. Verificación Protocolo DHCP Y NAT

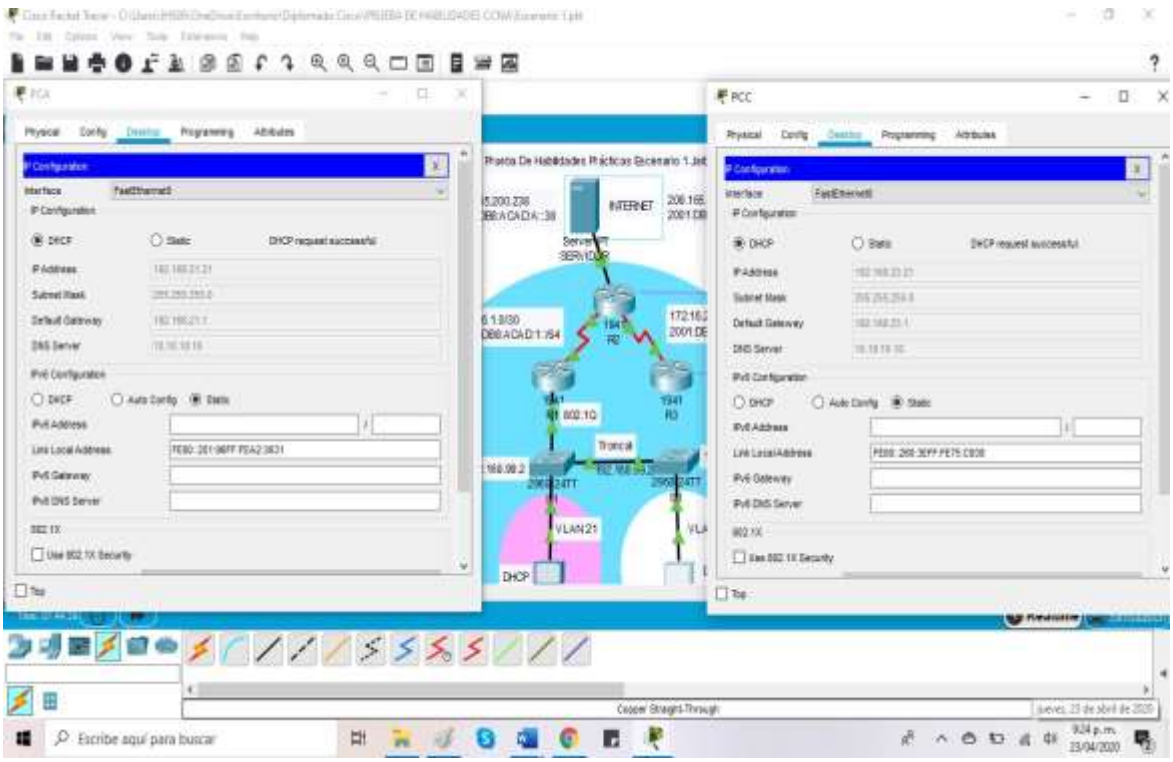

Figura 4. Verificación Protocolo DHCP

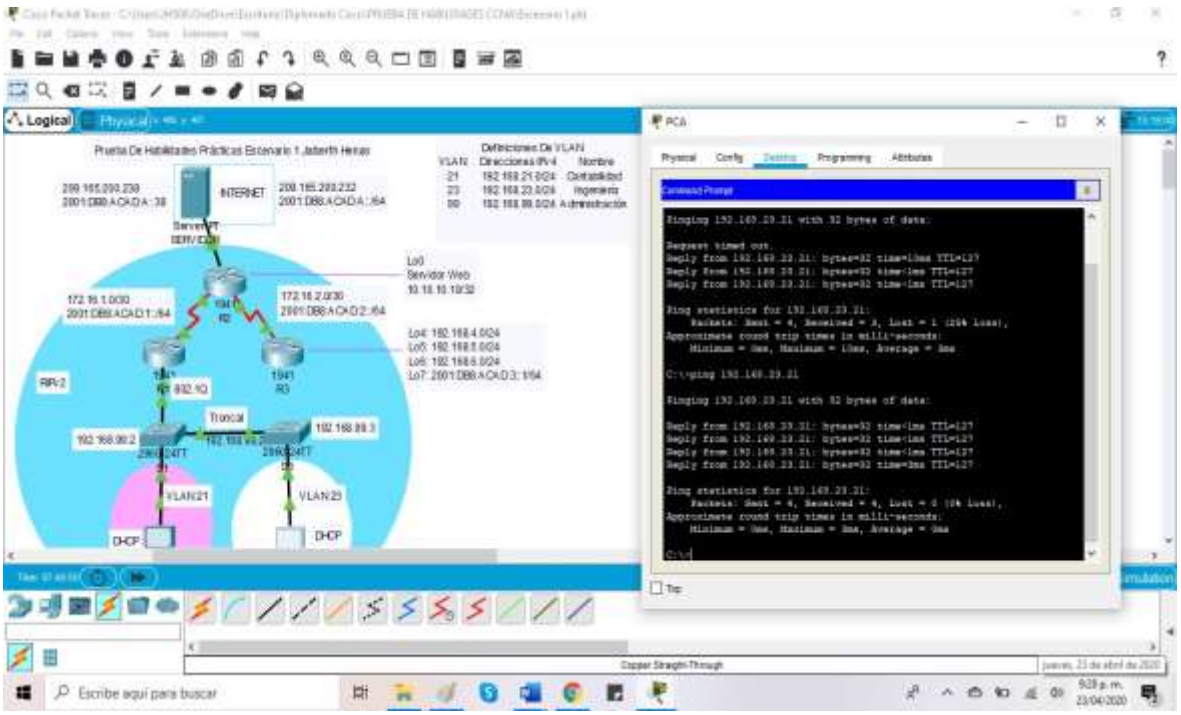

Figura 5. Ping PCA A PCC

Parte 5: Configurar NTP

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

Tabla 20. Configuración Protocolo NTP

```
R2>en
Password:
R2#clock set 09:00:00 05 march 2016
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5

R1>en
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#exit
R1#show ntp associations
```

Parte 6: Configurar y verificar las listas de control de acceso (ACL)

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet

Verificar que la ACL funcione como se espera	Succesful

Tabla 21. Restricción De Acceso A R2

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

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

R2(config-std-nacl)#exit

R2(config)#line vty 0 15

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

R2(config-line)#transport input telnet

R1#telnet 172.16.2.1

Trying 172.16.2.1 ...OpenSe prohibe el acceso no autorizado

User Access Verification

Password:

R3>

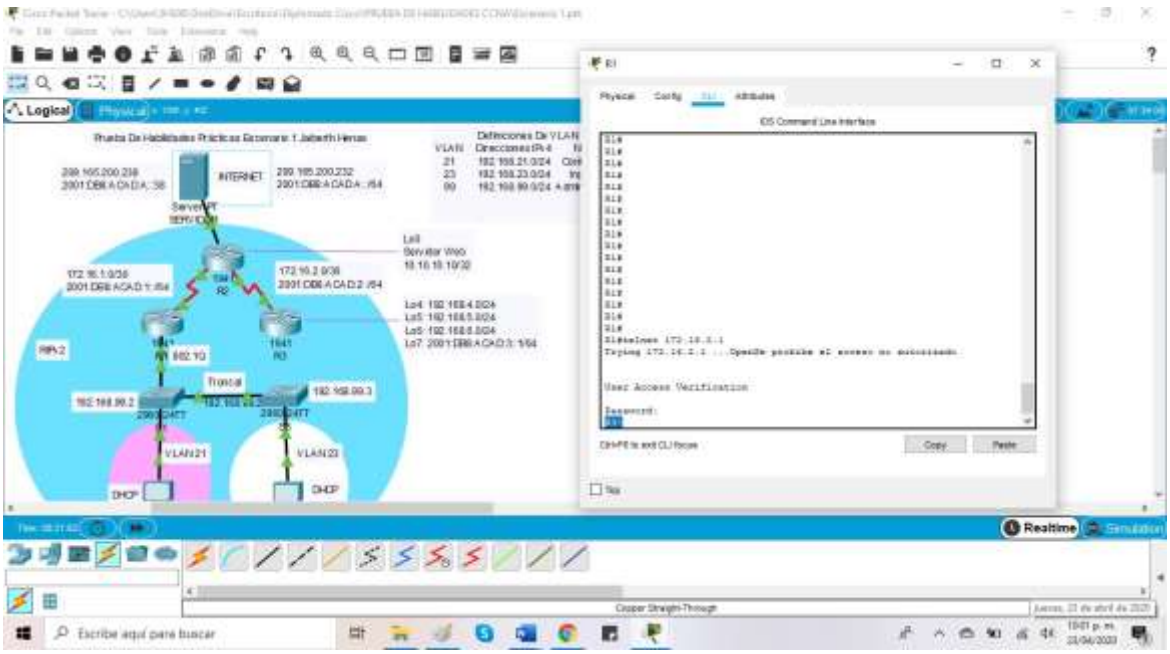

Figura 6: Evidencia Restricción Acceso

Paso 2: R3> Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
Restablecer los contadores de una lista de acceso	clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation *

Tabla 22. Configuración Para Reestablecer Contadores

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

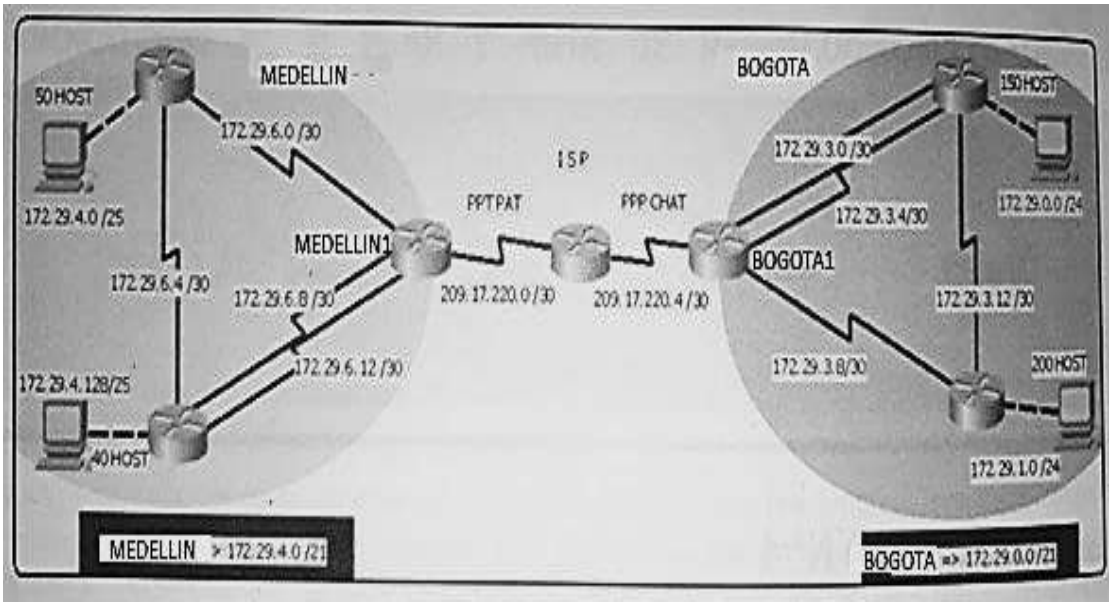

Figura 7. Escenario 2 Propuesto

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

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

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

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

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

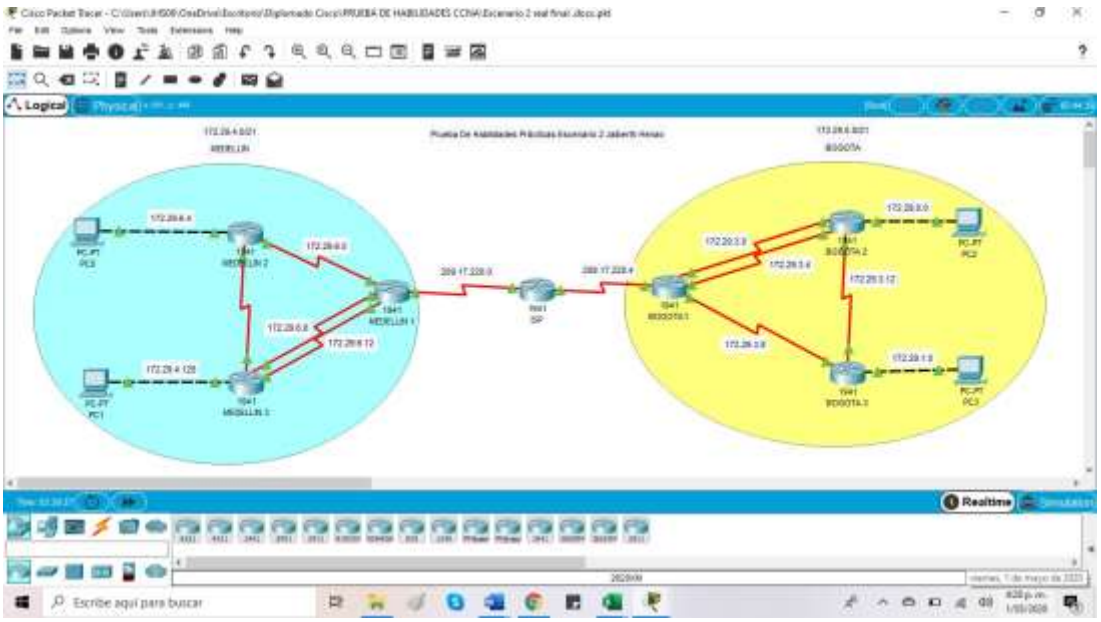

Figura 8. Escenario 2 Packet Tracer

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.

Router#config t

Router(config)#hostname ISP

CONFIGURACION EN ROUTER ISP

ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#description ISP-MEDELLIN1
ISP(config-if)#clock rate 128000
ISP(config-if)#no shu

ISP(config-if)#int s0/0/1
ISP(config-if)#description ISP-BOGOTA1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shu

ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.0 255.255.255.252 area 0
ISP(config-router)#network 209.17.220.4 255.255.255.252 area 0

CONFIGURACION ROUTER MEDELLIN 1

Router>en
Router#config t
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#description MEDELLIN1-ISP
MEDELLIN1(config-if)#no shu

MEDELLIN1(config)#int s0/0/1

MEDELLIN1(config-if)# ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)# description MEDELLIN1-MEDELLIN2
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu

MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)# ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)# description MEDELLIN1- MEDELLIN3
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu

MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)# ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)# description MEDELLIN3-MEDELLIN1
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 209.17.220.0 255.255.255.252 area 0
MEDELLIN1(config-router)#network 172.29.6.0 255.255.255.252 area 0
MEDELLIN1(config-router)#network 172.29.8.0 255.255.255.252 area 0
MEDELLIN1(config-router)#network 172.29.12.0 255.255.255.252 area 0

CONFIGURACION ROUTER MEDELLIN 2

INTERFAZ S0/0/0
MEDELLIN2#config t
MEDELLIN2(config)#int s0/0/0
MEDELLIN2(config-if)# ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)# description MEDELLIN1-MEDELLIN2

MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shut

MEDELLIN2(config-if)#int s0/0/1
MEDELLIN2(config-if)# ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)# description MEDELLIN2-MEDELLIN1
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shu

MEDELLIN2(config-if)#int g0/0
MEDELLIN2(config-if)# ip address 172.29.4.1 255.255.255.252
MEDELLIN2(config-if)# description MEDELLIN2-PC0
MEDELLIN2(config-if)#no shu

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#network 172.29.6.0 255.255.255.252 area 0
MEDELLIN2(config-router)#network 172.29.6.4 255.255.255.252 area 0

CONFIGURACION ROUTER MEDELLIN3

INTERFAZ s0/0/0
Router#
Router#conf t
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#int s0/0/0
MEDELLIN3(config-if)# ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)# description MEDELLIN3-MEDELLIN2
MEDELLIN3(config-if)#no shu

MEDELLIN3(config-if)#int s0/1/0

MEDELLIN3(config-if)# ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)# description MEDELLIN3-MEDELLIN2
MEDELLIN3(config-if)#no shu

MEDELLIN3(config-if)#int s0/1/1
MEDELLIN3(config-if)# ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)# description MEDELLIN1-MEDELLIN3
MEDELLIN3(config-if)#no shu

MEDELLIN3(config-if)#int g0/0
MEDELLIN3(config-if)# ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)# description MDELLIN3-PC1
MEDELLIN3(config-if)#no shu

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#network 172.29.6.4 255.255.255.252 area 0
MEDELLIN3(config-router)#network 172.29.6.8 255.255.255.252 area 0
MEDELLIN3 (config-router)#network 172.29.6.12 255.255.255.252 area 0

CONFIGURACION ROUTER BOGOTA 1

Router>en
Router#config t
Router(config)#hostname BOGOTA1
BOGOTA1(config-if)#int s0/0/0
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#description BOGOTA1-BOGOTA3
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shu

BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip address 209.17.220.5 255.255.255.252
BOGOTA1(config-if)#description BOGOTA1-ISP
BOGOTA1(config-if)#no shu

BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#description BOGOTA2-BOGOTA1
BOGOTA1(config-if)#no shu

BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#description BOGOTA1-BOGOTA2
BOGOTA1(config-if)#no shu

BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#network 172.29.3.8 255.255.255.252 area 0
BOGOTA1(config-router)#network 172.29.3.4 255.255.255.252 area 0
BOGOTA1(config-router)#network 172.29.3.3 255.255.255.252 area 0
BOGOTA1(config-router)#network 209.17.220.4 255.255.255.252 area 0

CONFIGURACION ROUTER BOGOTA 2

Router#conf t
Router#hostname BOGOTA2
BOGOTA2(config)#int s0/0/1
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#description BOGOTA2-BOGOTA3
BOGOTA2(config-if)#no shu

BOGOTA2(config-if)#int s0/1/0
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA2(config-if)#description BOGOTA1-BOGOTA2
BOGOTA2(config-if)#no shu

BOGOTA2(config-if)#int s0/1/1
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)#description BOGOTA2-BOGOTA1
BOGOTA2(config-if)#no shu

BOGOTA2(config-if)#int g0/0
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA2(config-if)#description BOGOTA2-PC2
BOGOTA2(config-if)#no shu

BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#network 172.29.3.4 255.255.255.252 area 0
BOGOTA2(config-router)#network 172.29.3.4 255.255.255.252 area 0
BOGOTA2(config-router)#network 172.29.3.0 255.255.255.252 area 0
BOGOTA2(config-router)#network 172.29.3.12 255.255.255.252 area 0

CONFIGURACION ROUTER BOGOTA 3

Router>en
Router#config t
Router(config)#hostname BOGOTA3
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA3(config-if)#description BOGOTA3-BOGOTA1
BOGOTA3(config-if)#no shu

```
BOGOTA3(config-if)#int s0/0/1
BOGOTA3(config-if)#ip address 172.168.3.14 255.255.255.252
BOGOTA3(config-if)#description BOGOTA3-BOGOTA2
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shu

BOGOTA3(config-if)#int g0/0
BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA3(config-if)#description BOGOTA3-PC3
BOGOTA3(config-if)#no shu

BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#network 172.29.3.8 255.255.255.252 area 0
BOGOTA3(config-router)#network 172.29.3.12 255.255.255.252 area 0
```

parte 2: configuración de enrutamiento

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.

```
MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#exit
MEDELLIN1#show ip route
```

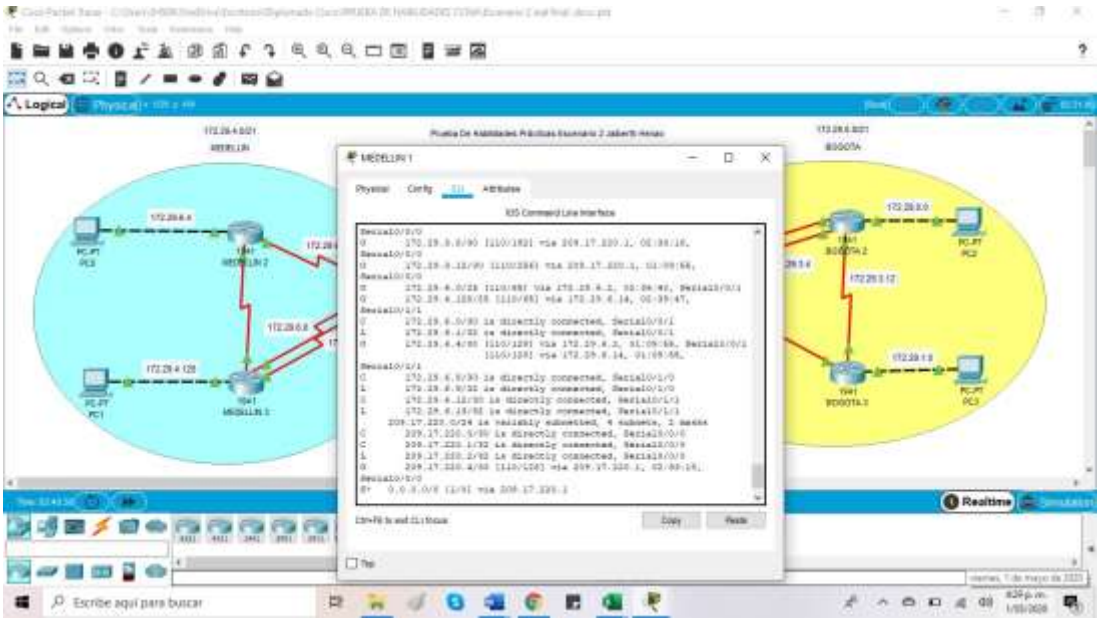

Figura 9. Comando “Show Ip Route” Medellin1

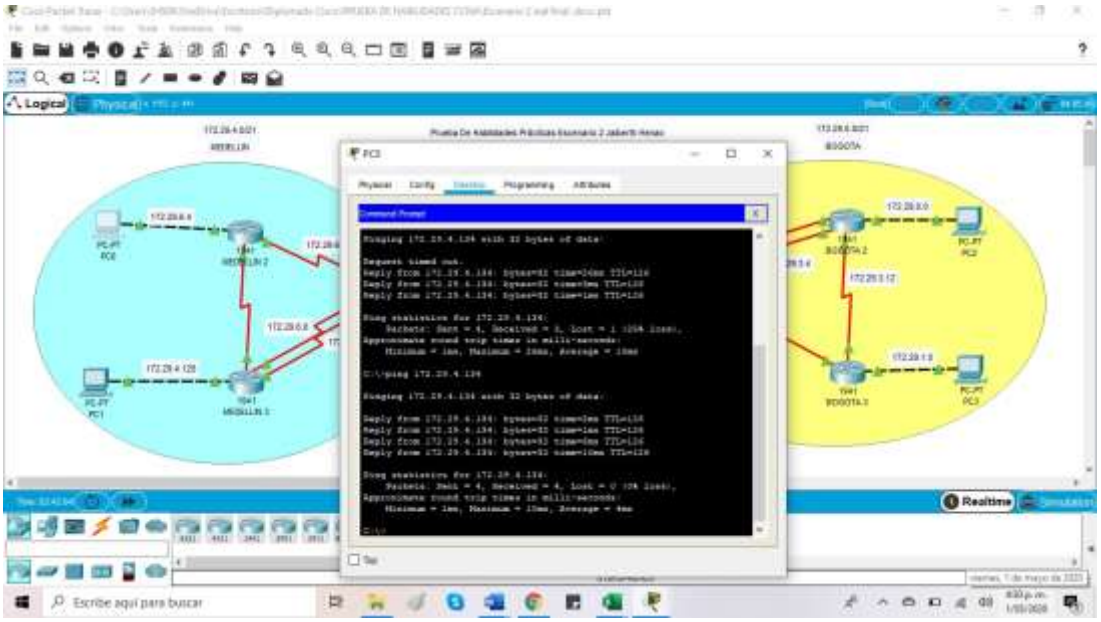

Figura 10. Ping Red MEDELLIN De PC0 A PC1

BOGOTA1>en

BOGOTA1#config t

BOGOTA1(config)# ip route 0.0.0.0 0.0.0.0 209.17.220.5

BOGOTA1(config)#exit

BOGOTA1#show ip route

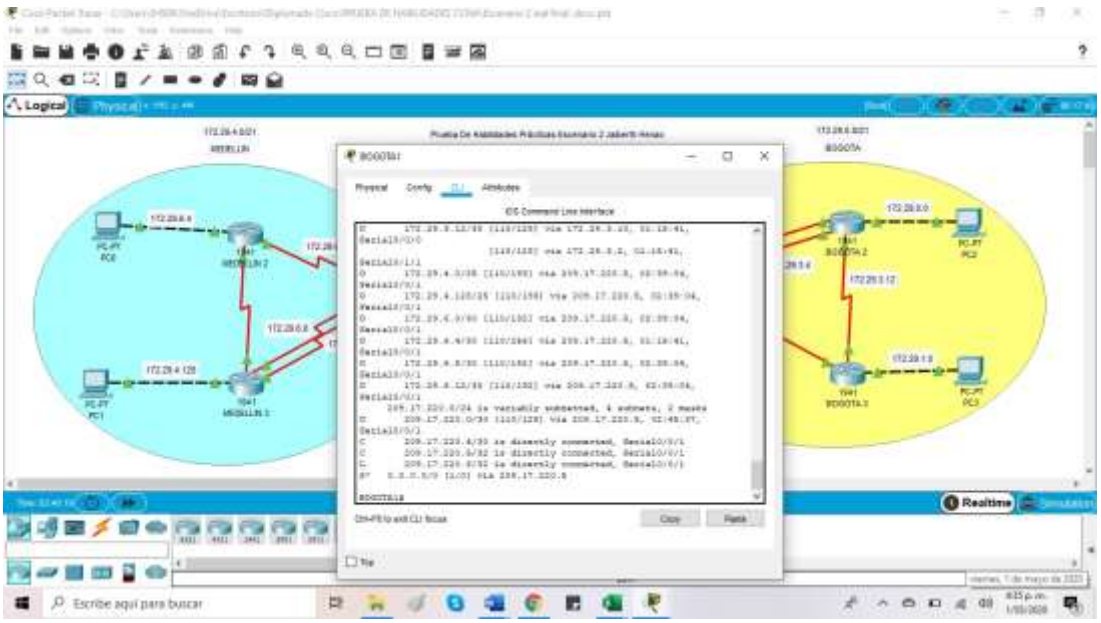

Figura 11. Comando Show Ip Route Router Bogota 1

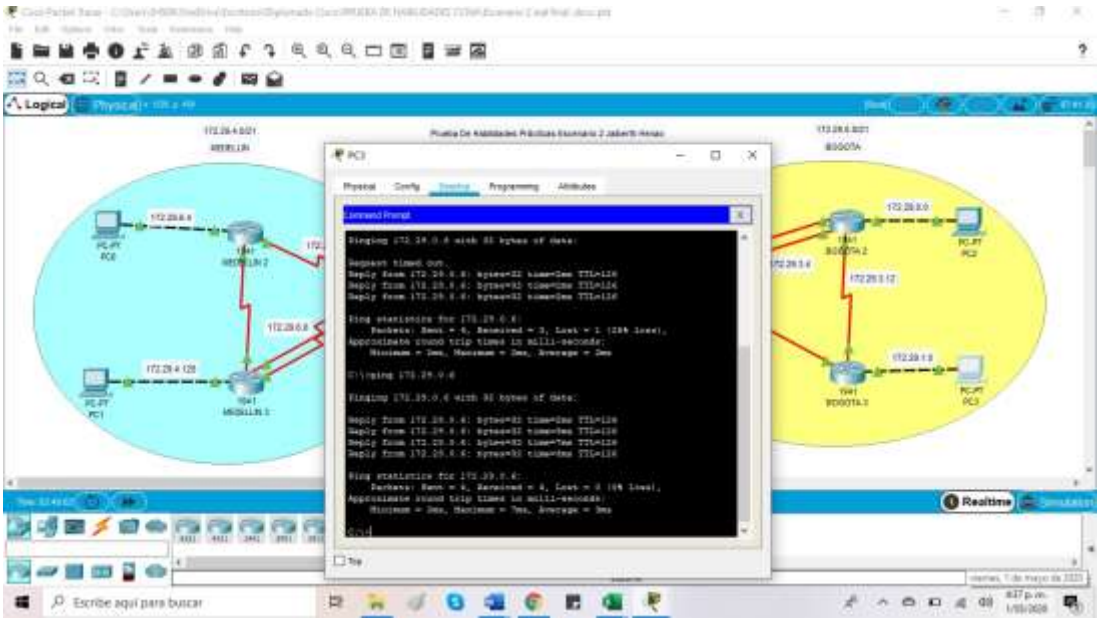

Figura 12. Ping Red BOGOTA De PC3 A PC2

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

ISP#config t
ISP(config)# ip route 172.29.4.0 255.255.255.0 S0/0/0
ISP(config)# ip route 172.29.0.0 255.255.255.0 S0/0/1
ISP(config)# ip route 172.29.1.0 255.255.255.0 S0/0/1
ISP(config)# ip route 172.29.4.128 255.255.255.128 S0/0/0

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

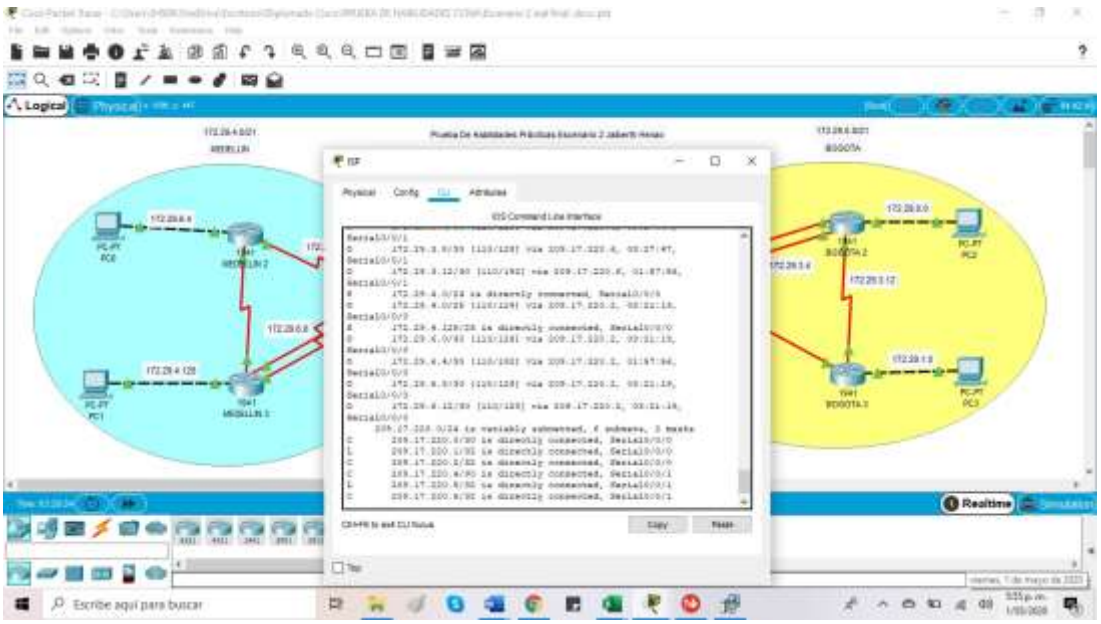

Figura 13. Tabla Enrutamiento Router ISP

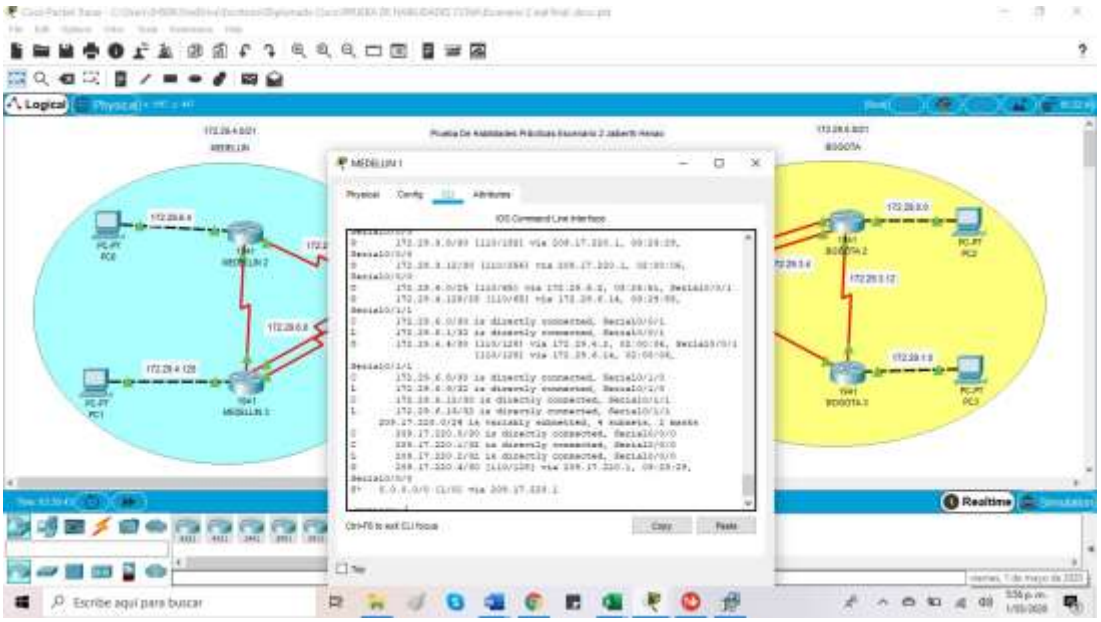

Figura 14. Tabla Enrutamiento Medellín1

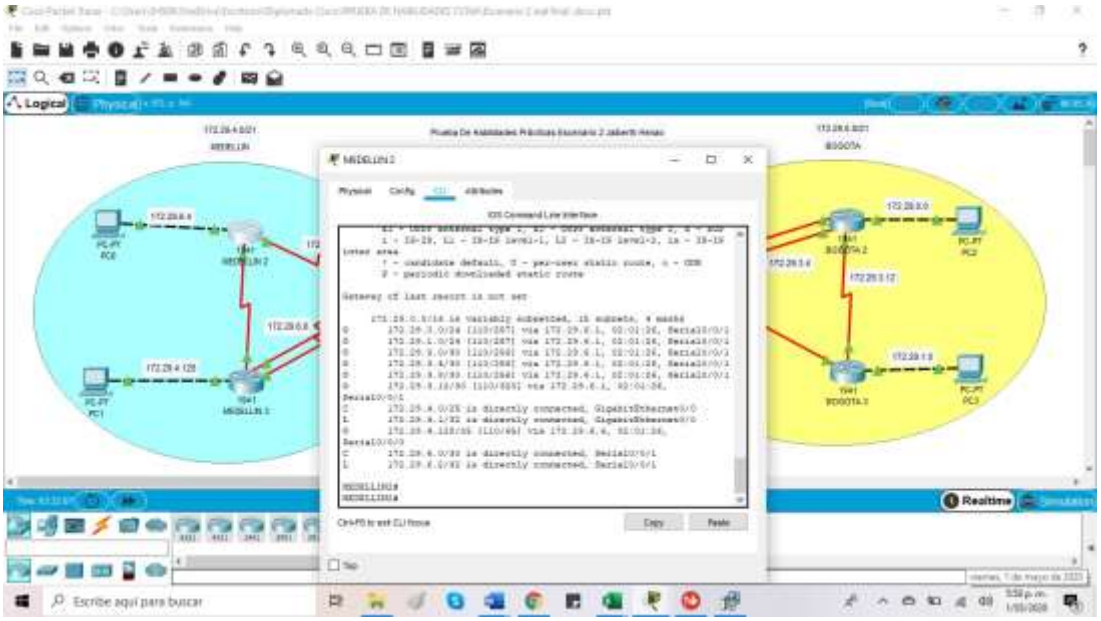

Figura 15. Tabla Enrutamiento Medellin2

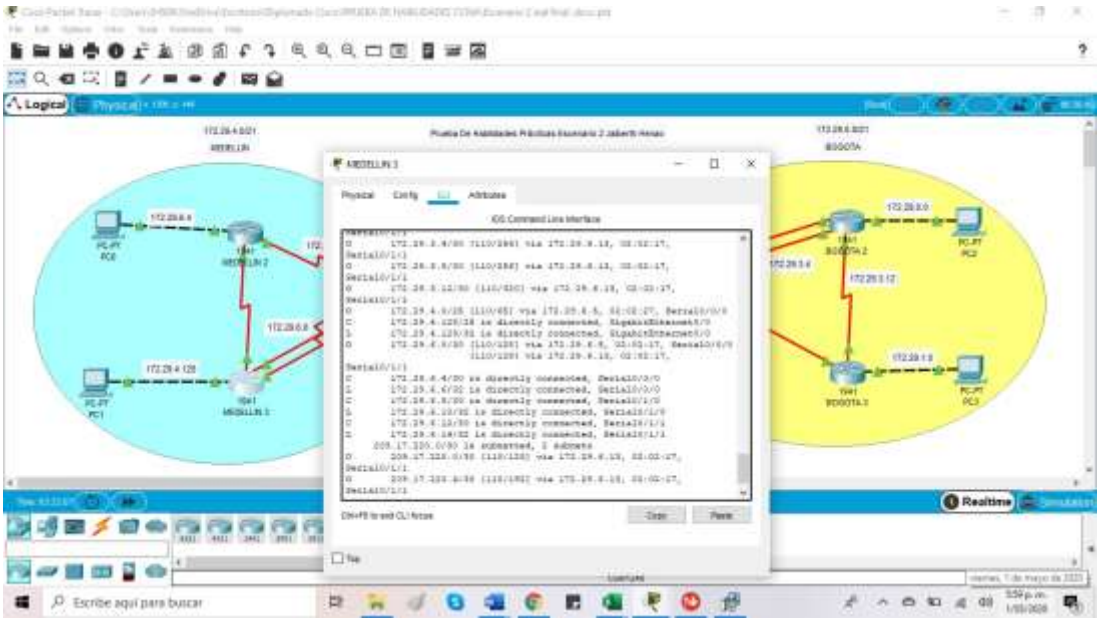

Figura 16. Tabla Enrutamiento Medellin3

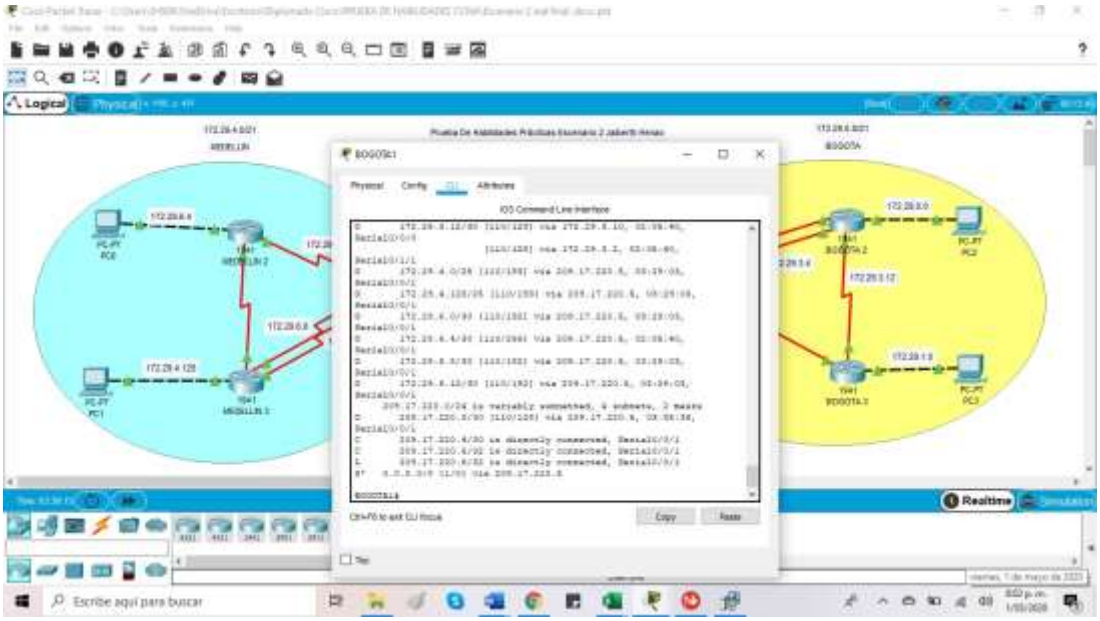

Figura 17. Tabla Enrutamiento Bogota1

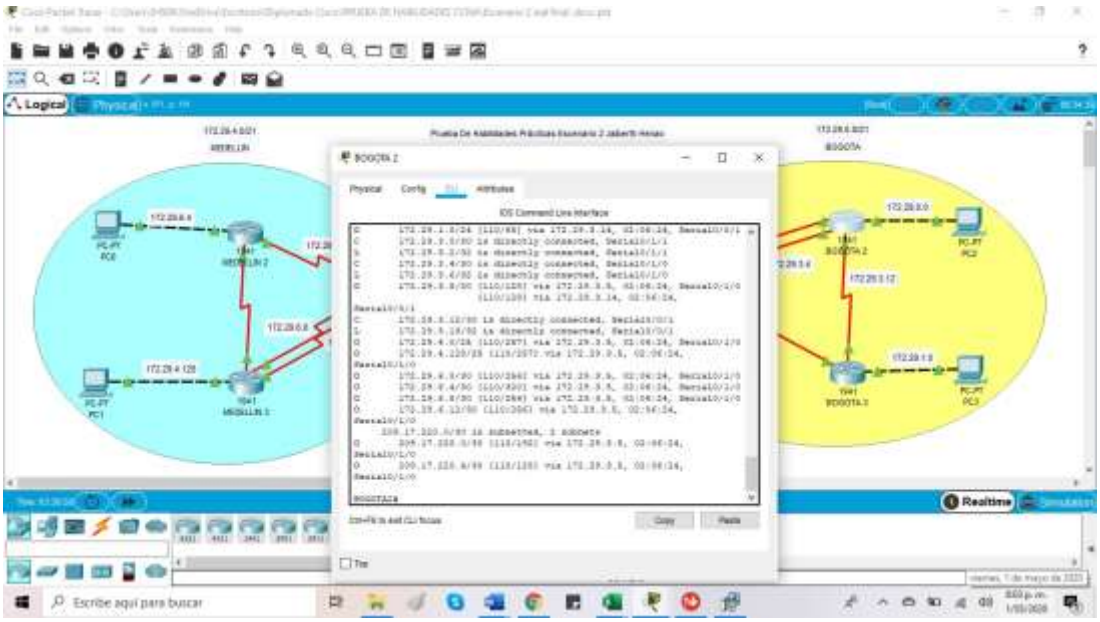

Figura 18. Tabla Enrutamiento Bogota2

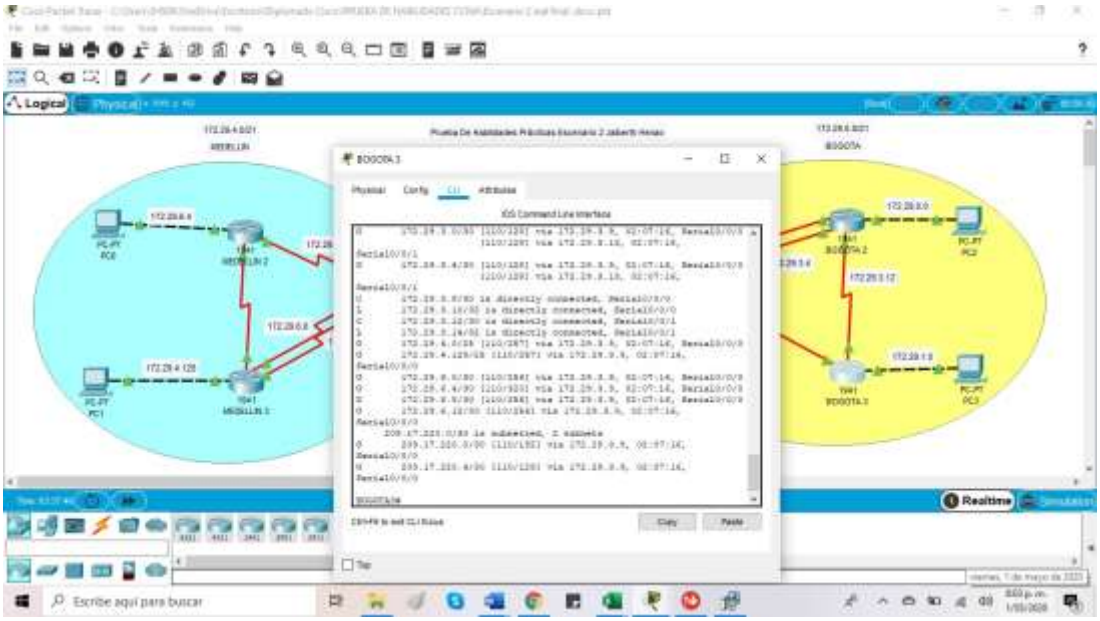

Figura 19. Tabla Enrutamiento Bogota3

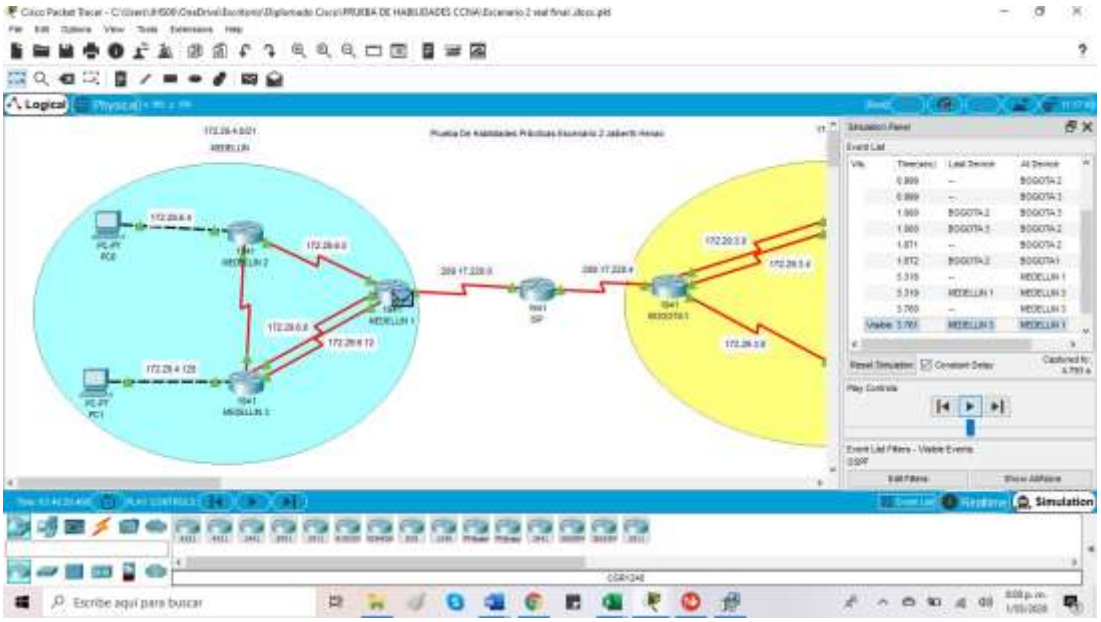

Figura 20. Envío De Paquetes Desde Medellin2 A Medellin1

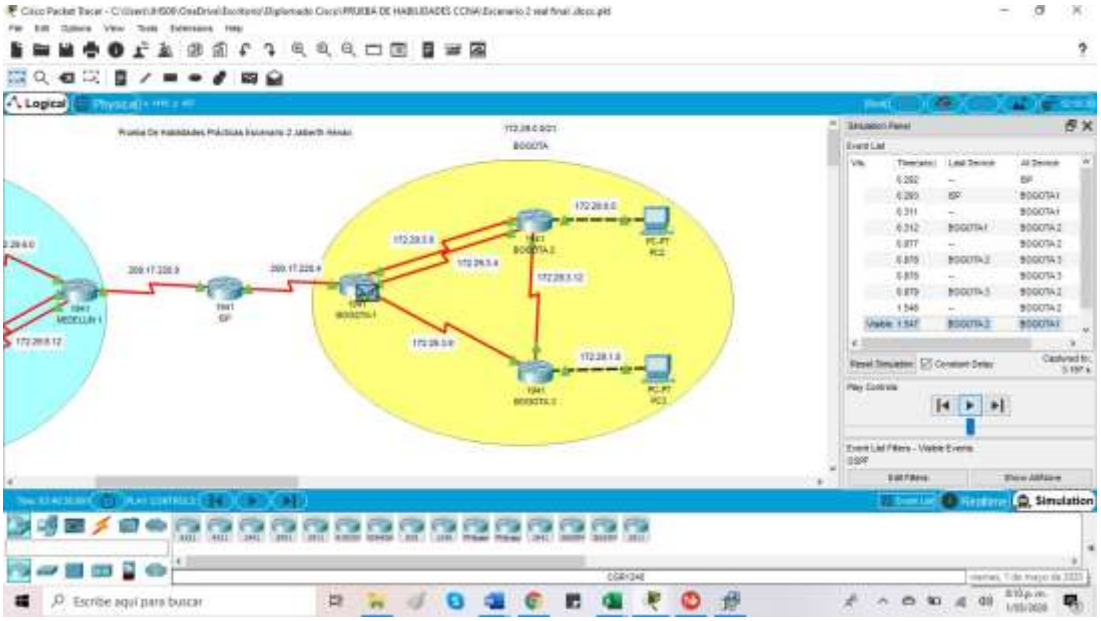

Figura 21. Pantallazo Envío Desde Paquetes Bogota2- Bogota1

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	**TERFAZ**
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

Tabla 23. Configuración 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.

MEDELLIN2>en

MEDELLIN2#show ip ospf interface

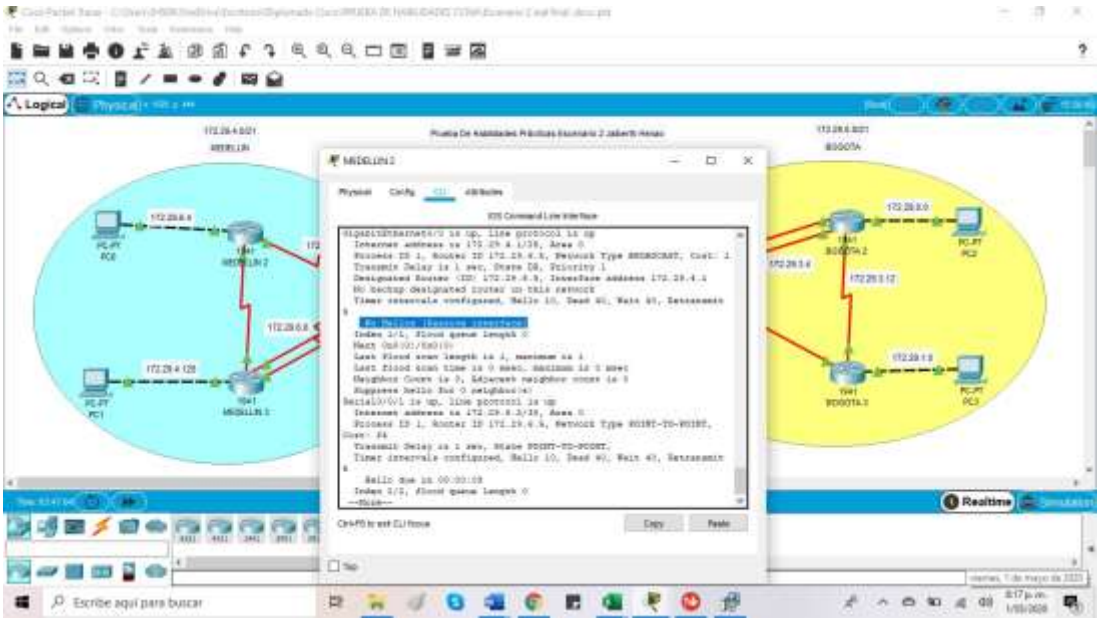

Figura 22. Passive Interface Router Medellin2

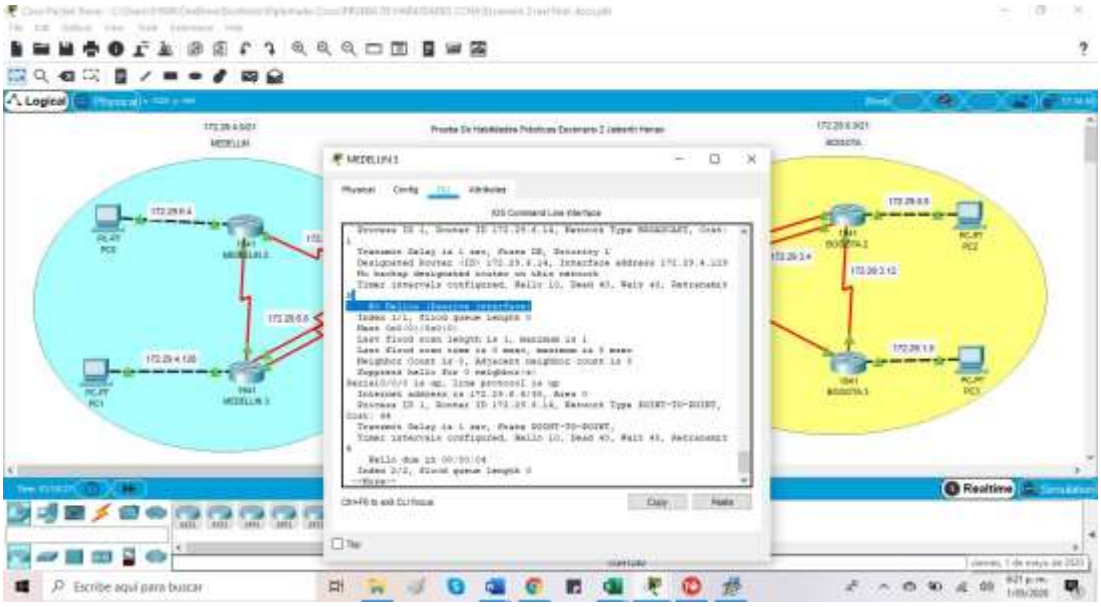

Figura 23. Passive Interface Router Medellin3

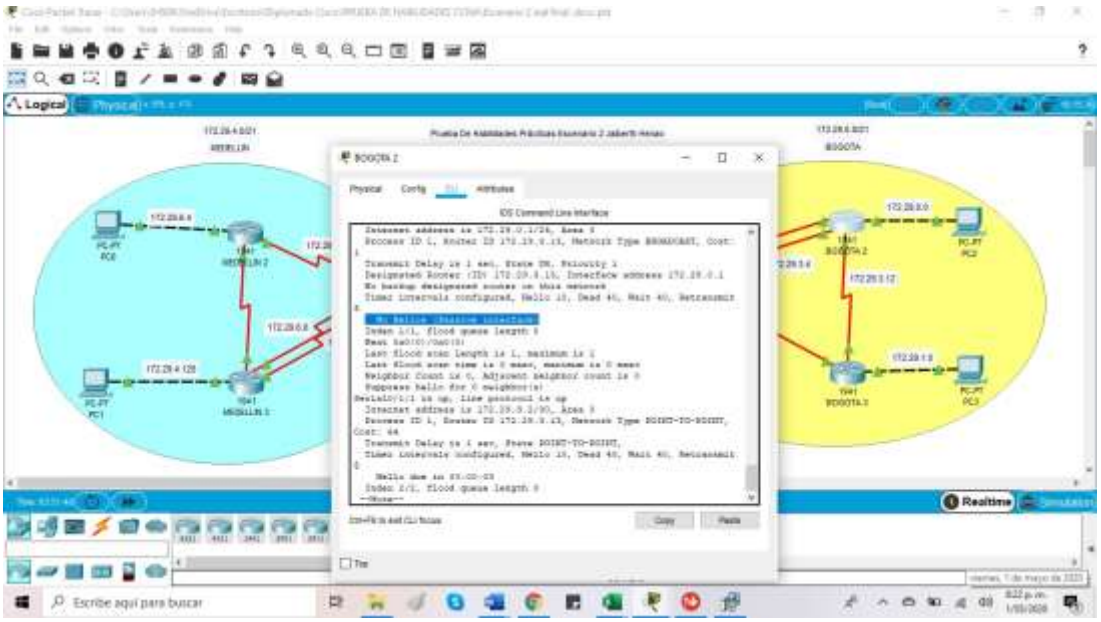

Figura 24. Passive Interface Router Bogota2

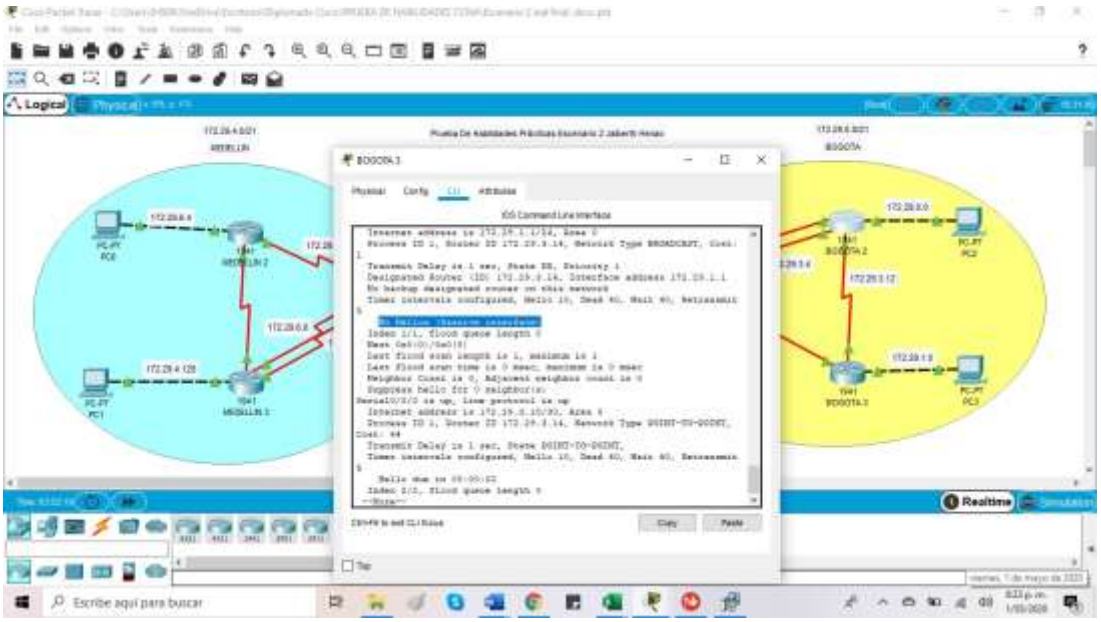

Figura 25. Passive Interface Router Bogota3

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

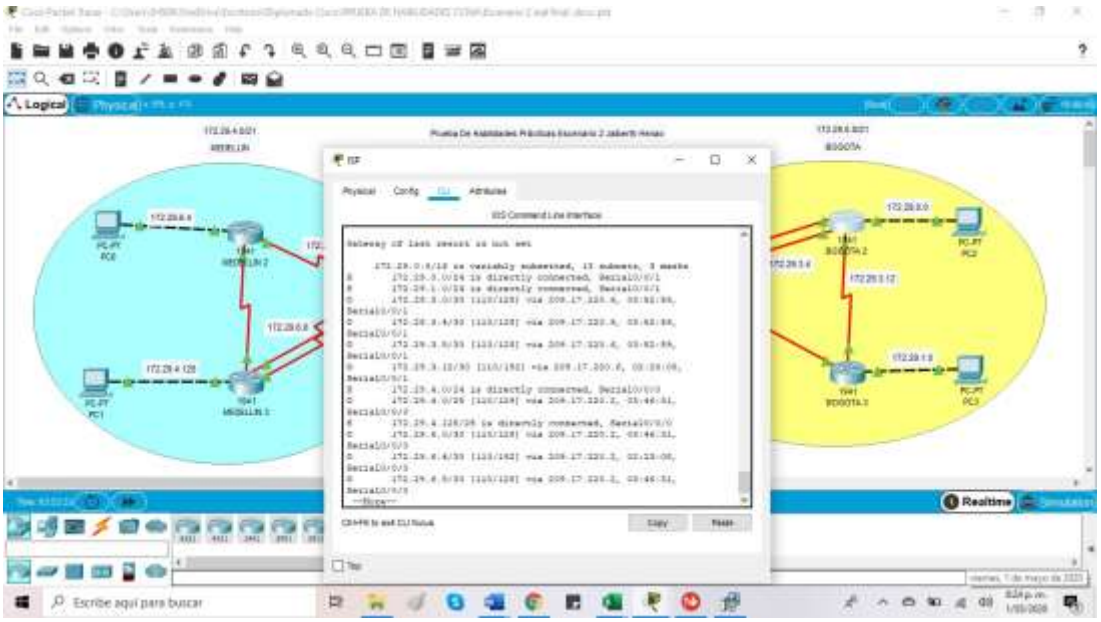

Figura 26. Rutas En Router Isp

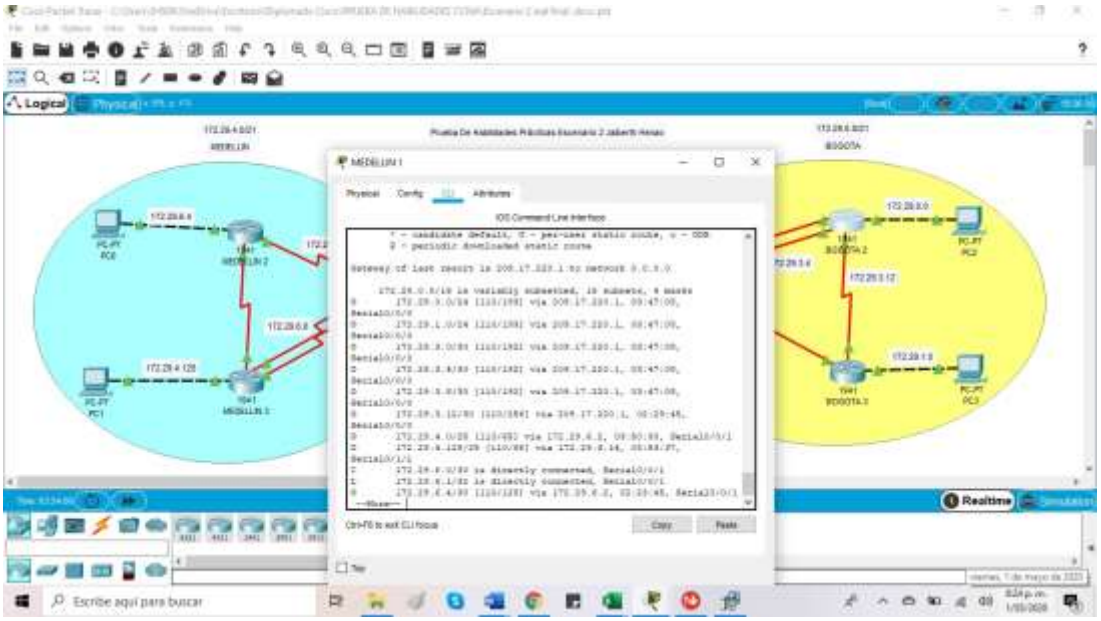

Figura 27. Rutas En Router Medellin1

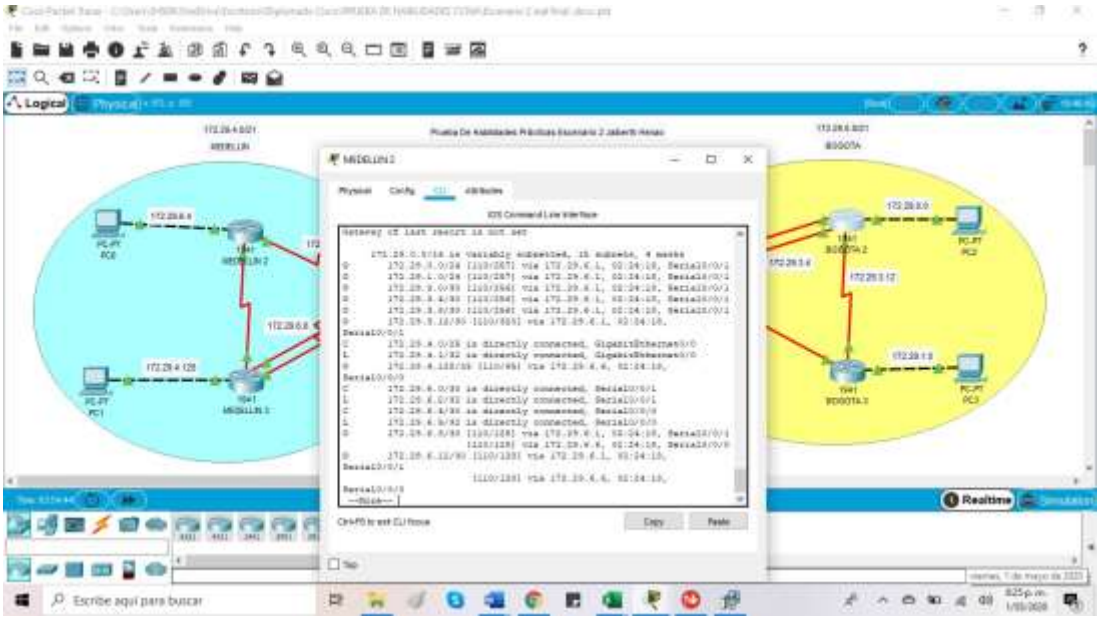

Figura 28. Rutas En Router Medellin2

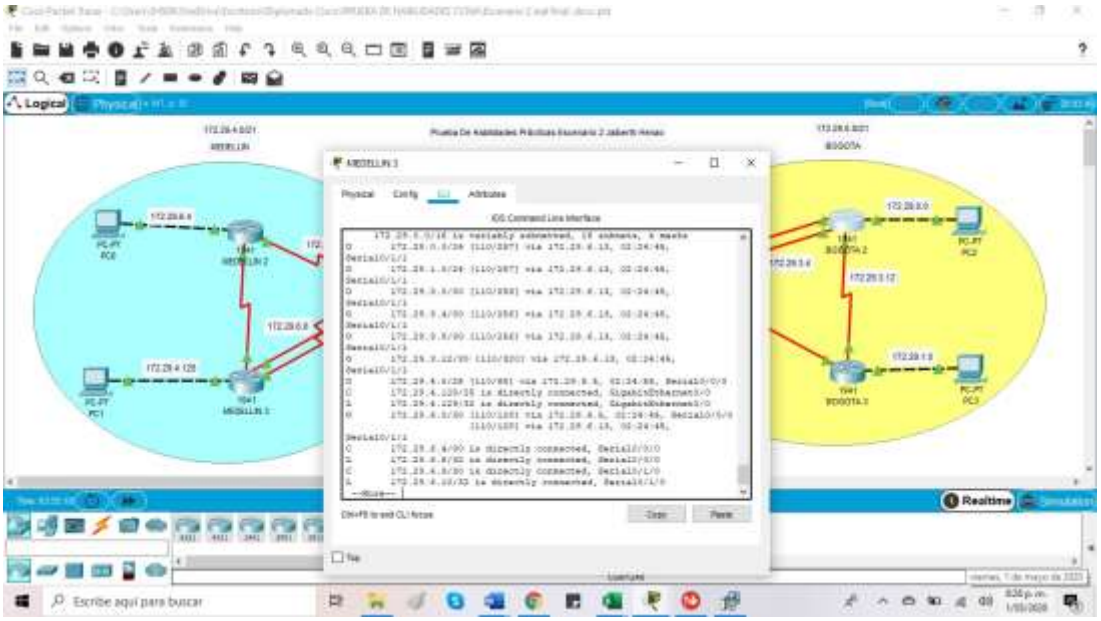

Figura 29. Rutas En Router Medellin3

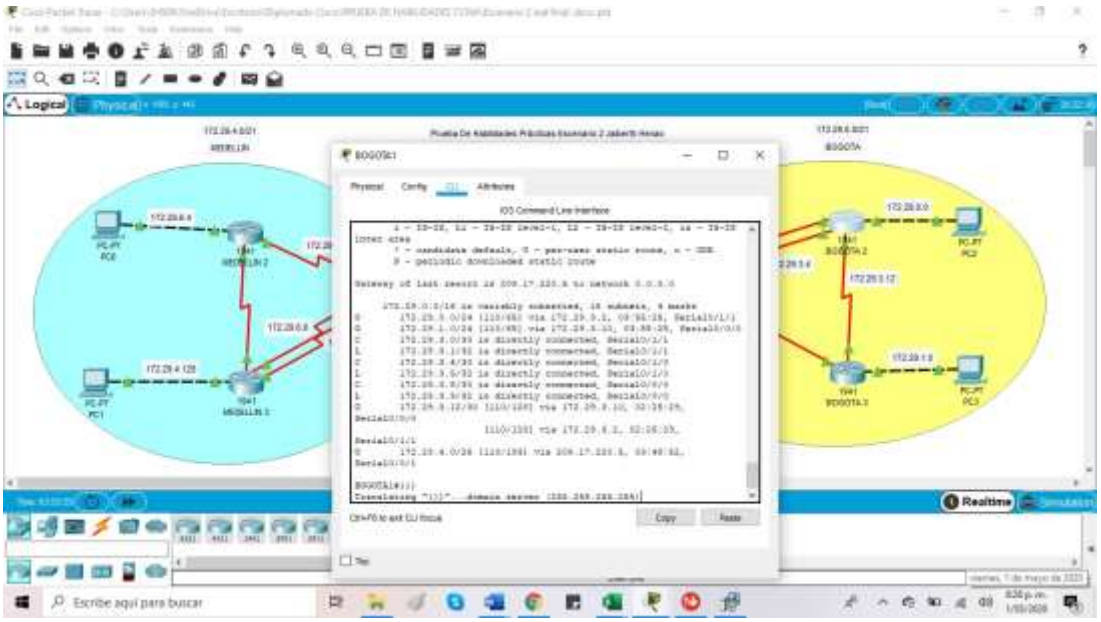

Figura 30. Rutas En Router Bogota1

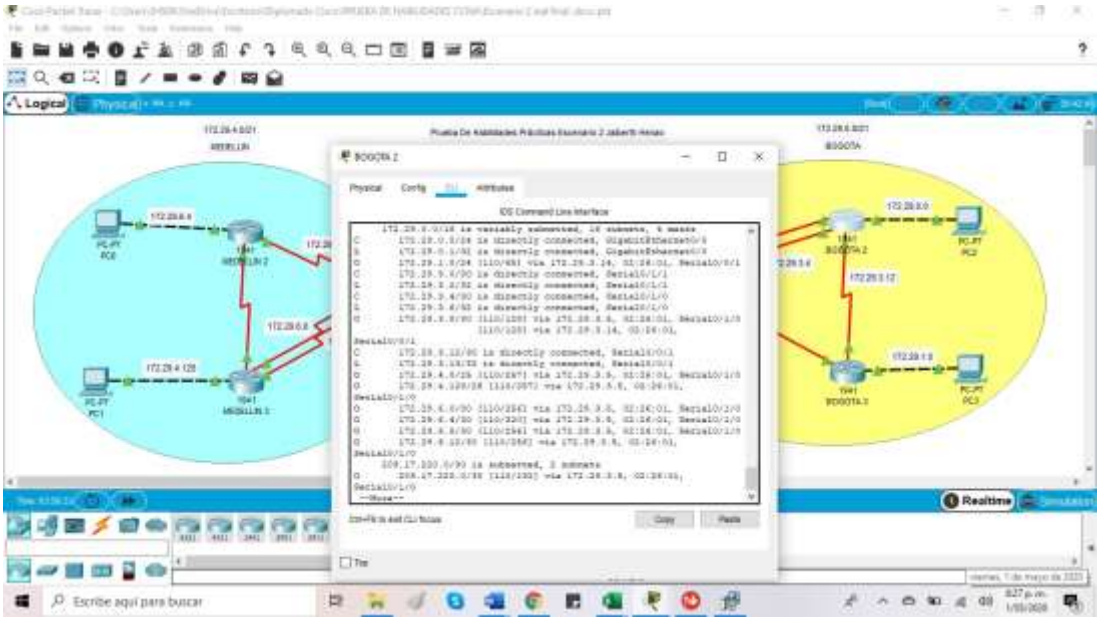

Figura 31. Rutas En Router Bogota2

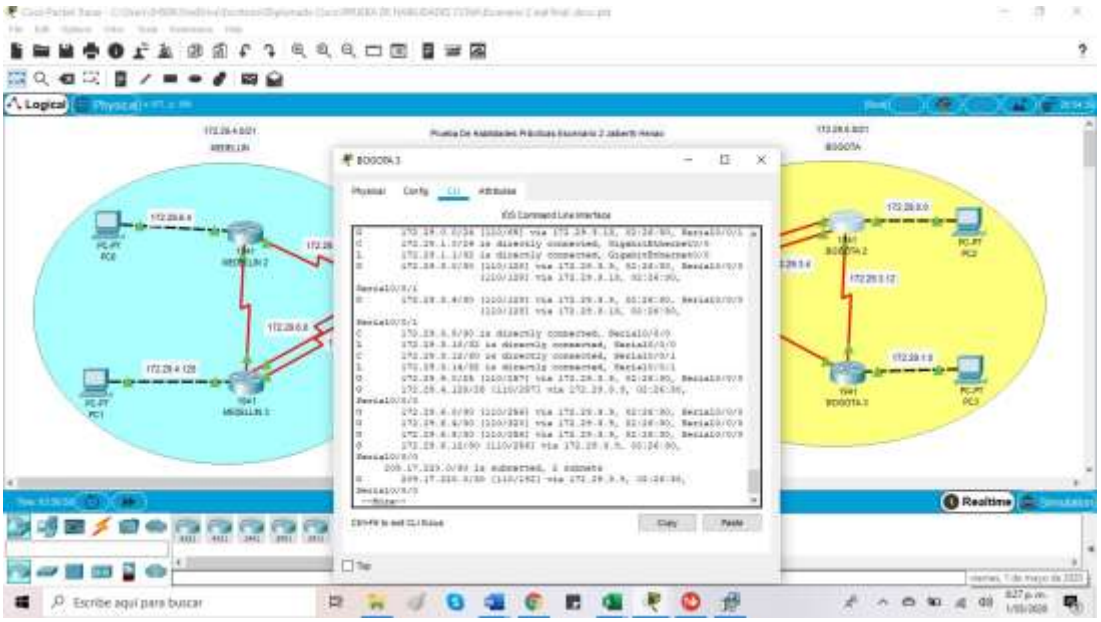

Figura 32. Rutas En Router Bogota3

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

IPS

ISP#conf t

ISP(config)#username MEDELLIN1 pass cisco

ISP(config)#int s0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication pap

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

ISP(config-if)#exit

MEDELLIN1

MEDELLIN1#config t

MEDELLIN1(config)#user

MEDELLIN1(config)#username ISP password cisco

MEDELLIN1(config)#int s0/0/0

MEDELLIN1(config-if)#encapsulation ppp

MEDELLIN1(config-if)#PPP Authentication pap

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

MEDELLIN1(config-if)#end

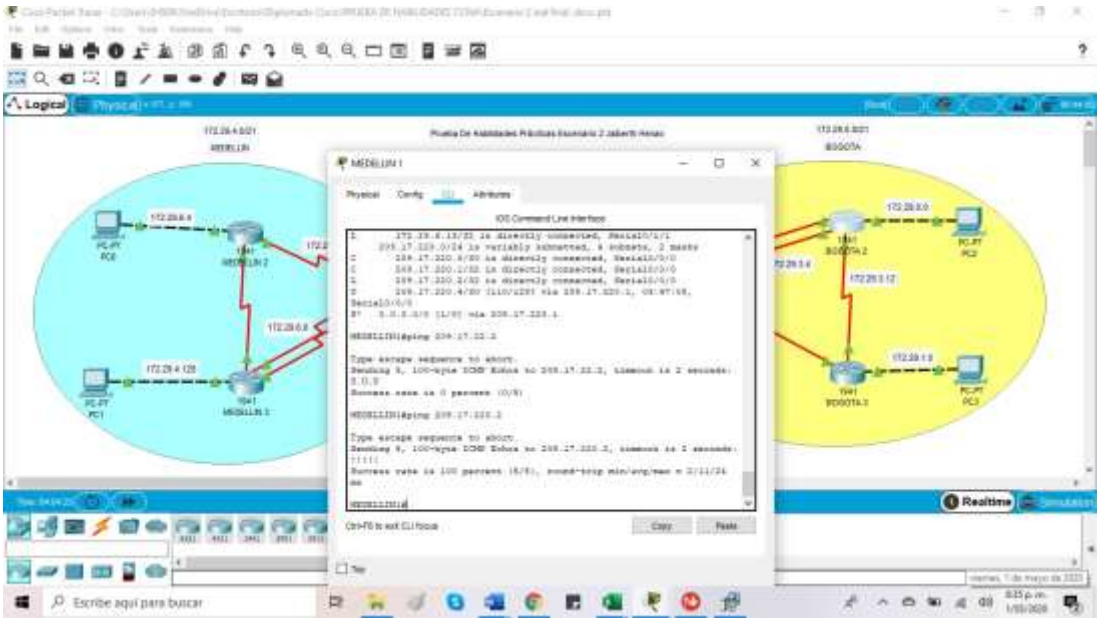

Figura 33. Ping a Router ISP

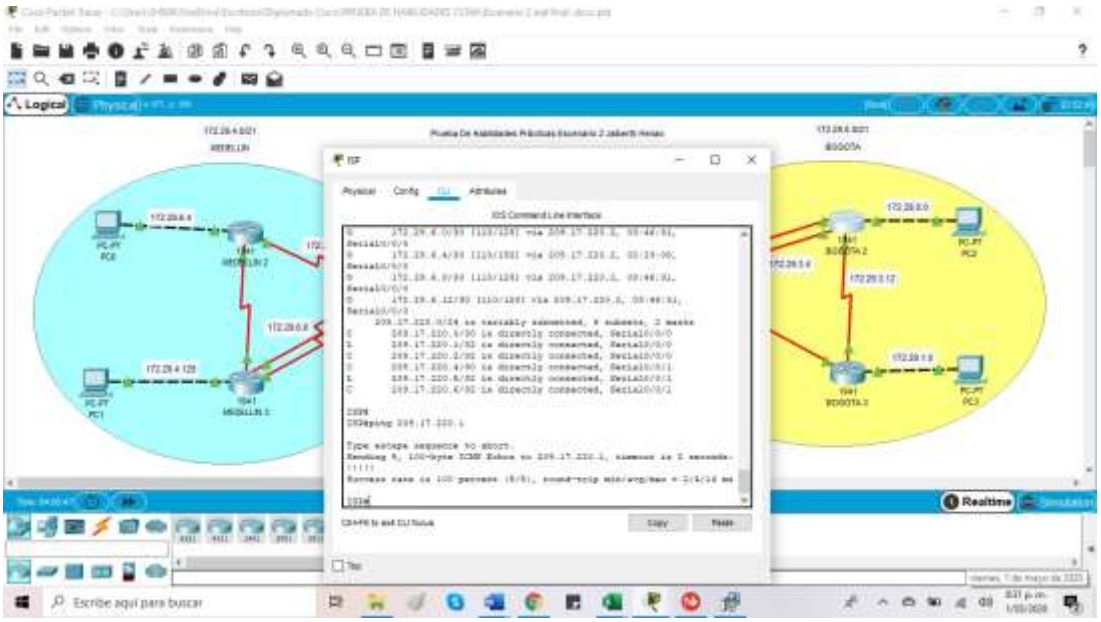

Figura 34. Ping a Router Medellin1

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

ISP

ISP(config)#user

ISP(config)#username BOGOTA1 password cisco

ISP(config)#int s0/0/1

ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication chap

ISP(config-if)#end

BOGOTA1

BOGOTA1>en

BOGOTA1#config t

BOGOTA1(config)#username ISP pass cisco

BOGOTA1(config)#int s0/0/1

BOGOTA1(config-if)#encapsulation ppp

BOGOTA1(config-if)#ppp authentication chap

BOGOTA1(config-if)#end

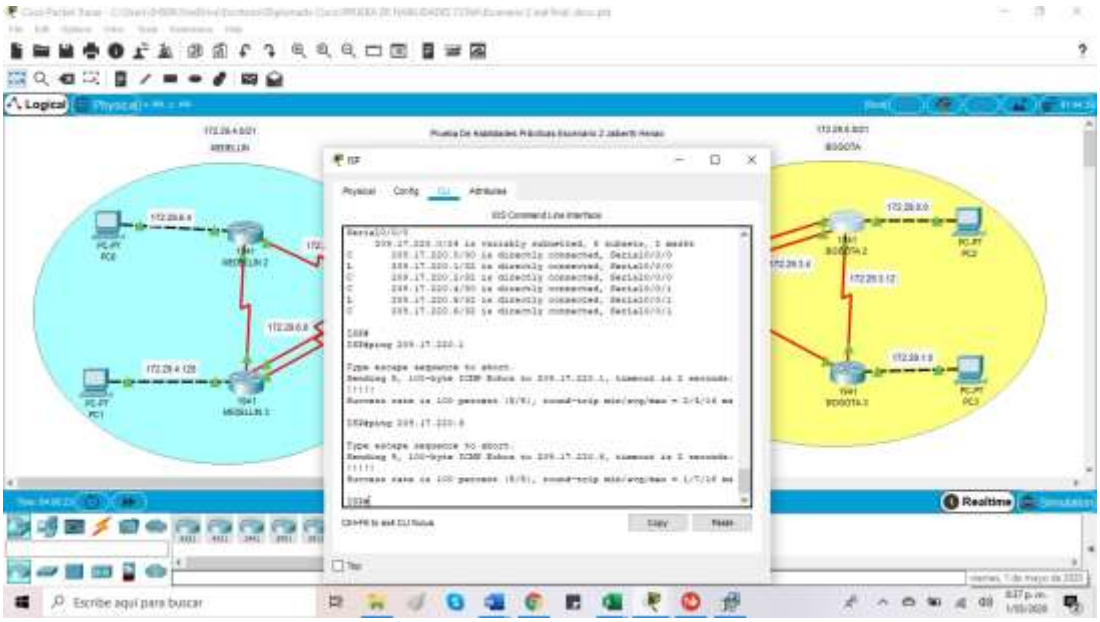

Figura 35. Pantallazo Ping a Bogota1

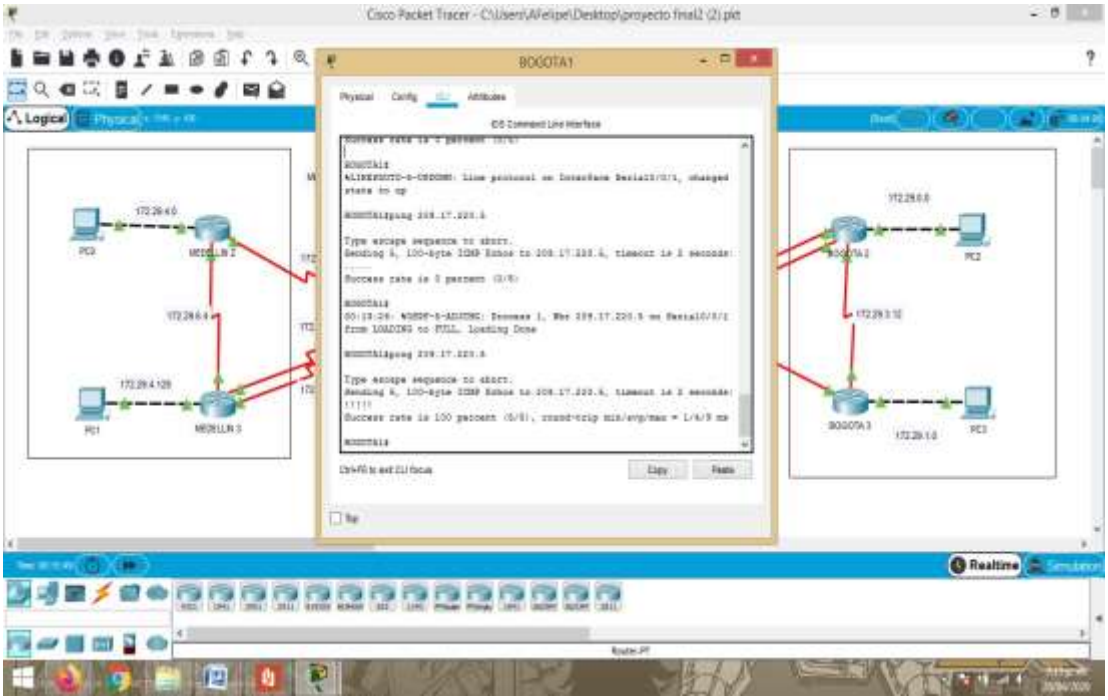

Figura 36. Ping a Router ISP

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.

CONFIGURACION NAT EN ROUTER MEDELLIN1

```
MEDELLIN1>en
MEDELLIN1#conf t
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)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#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.

CONFIGURACION NAT BOGOTA1

```
BOGOTA1>en
BOGOTA1#config t
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list HOST interface s0/0/1 overload
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
```

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.

CONFIGURACION DE DHCP ROUTER MEDELLIN2

MEDELLIN2(config)#ip dhcp pool Med2
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 Med3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit

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

CONFIGURACION ROUTER MEDELLIN3

MEDELLIN3>en
MEDELLIN3#conf t
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#

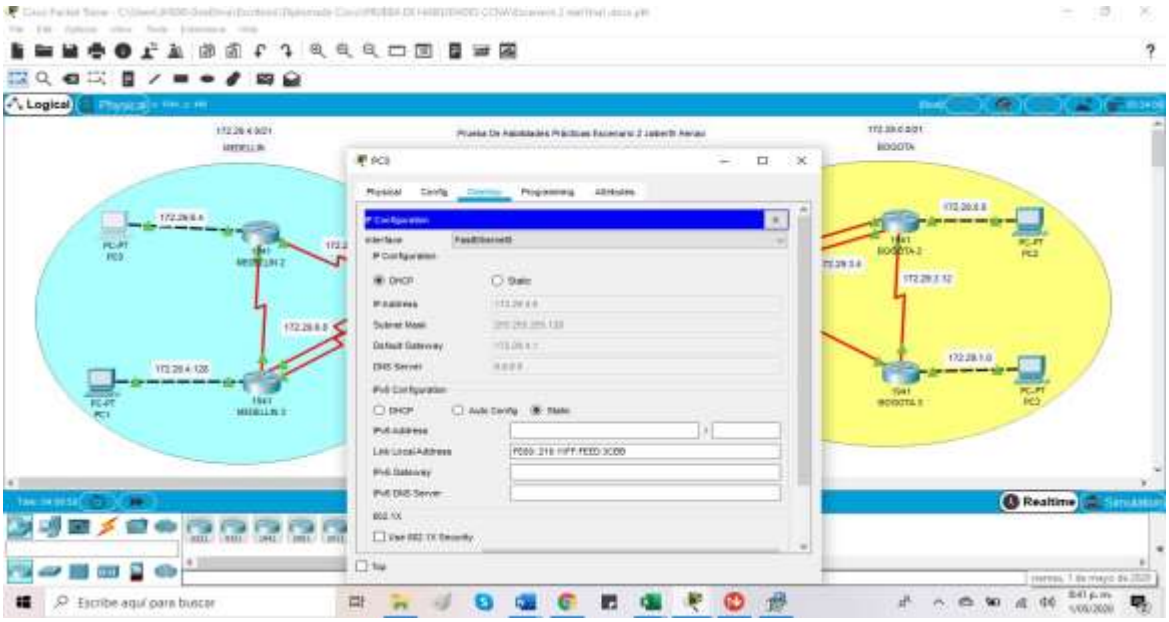

Figura 37. Evidencia Configuración DHCP PC0

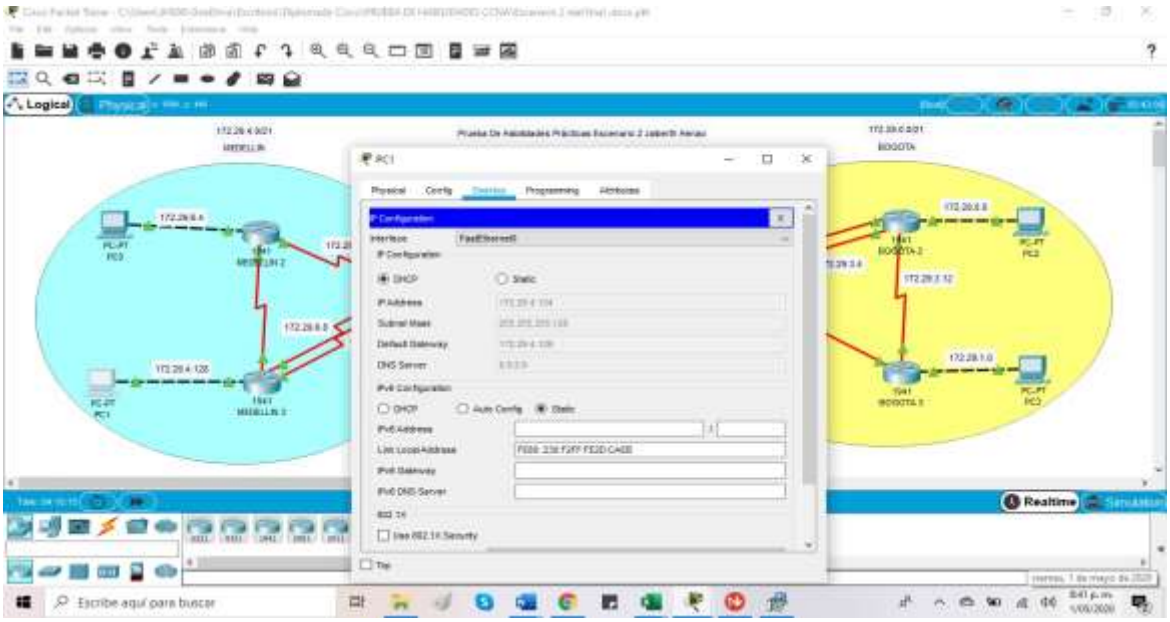

Figura 38. Evidencia Configuración DHCP PC1

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

d. Configurar la red Bogotá2 y Bogotá3 donde el router BOGOTA2 debe ser el servidor DHCP para ambas redes Lan.

BOGOTA2

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp pool Bog2
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(config)#ip dhcp pool Bog3
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
```

BOGOTA3

```
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
BOGOTA3(config-if)#exit
```

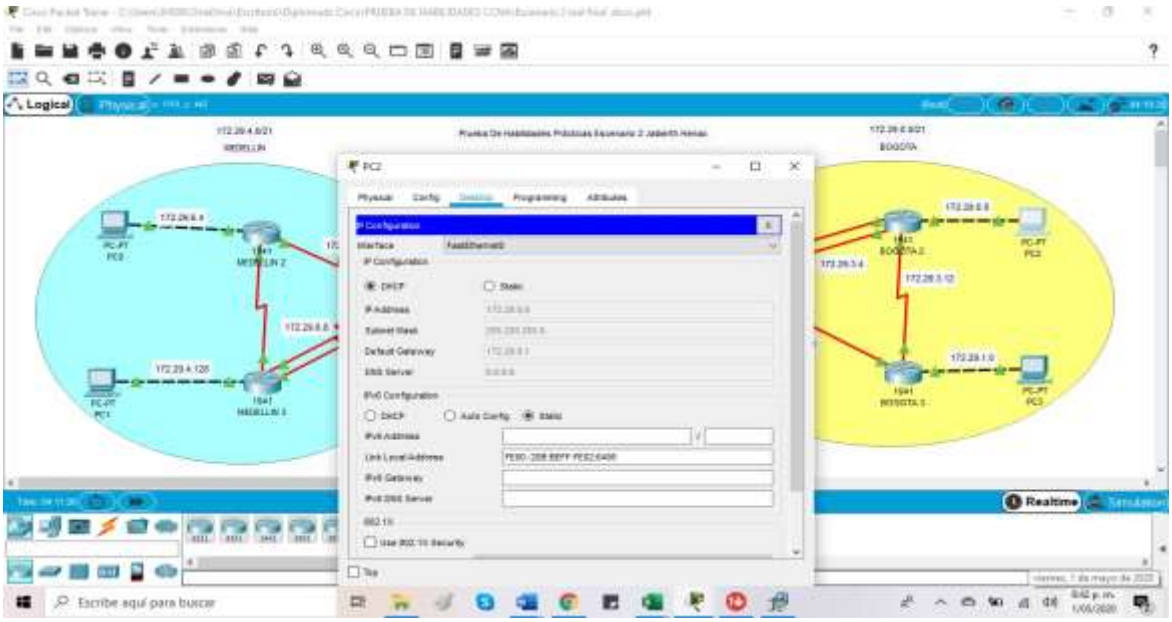

Figura 39. Evidencia Configuración DHCP En PC2

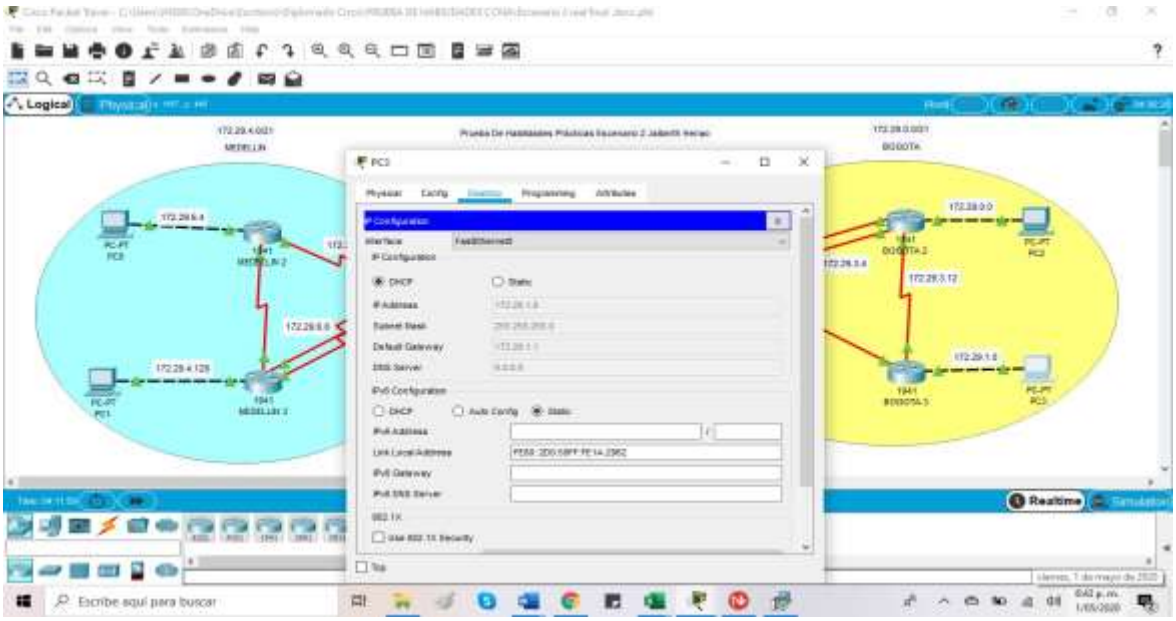

Figura 40. Evidencia Configuración DHCP En PC3

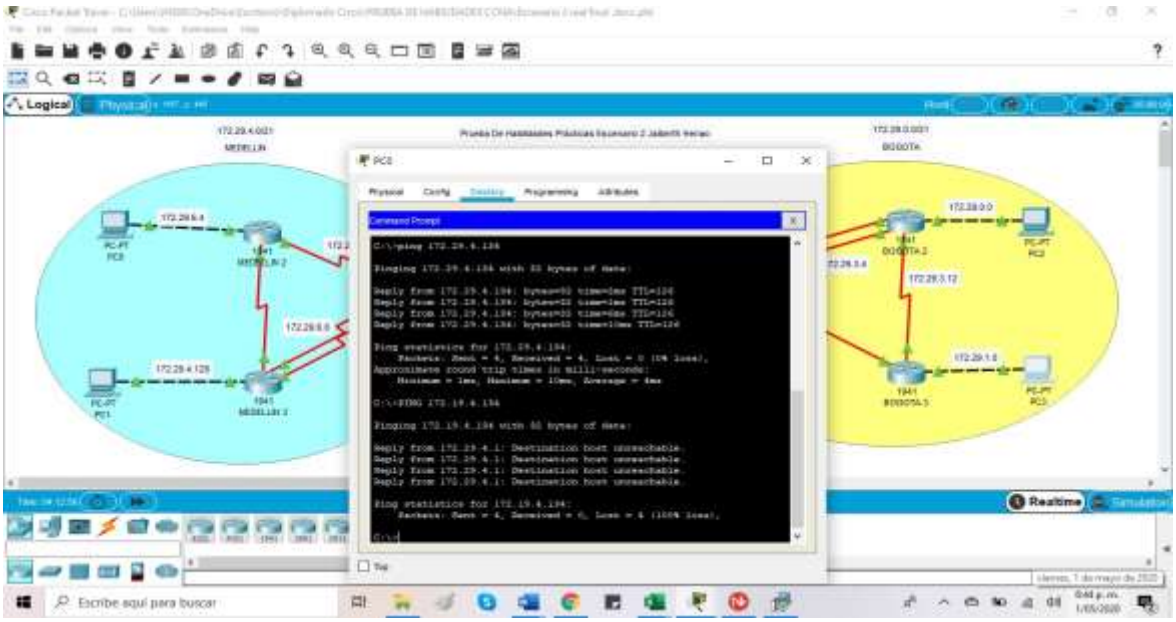

Figura 41. Ping De PC0 A PC1

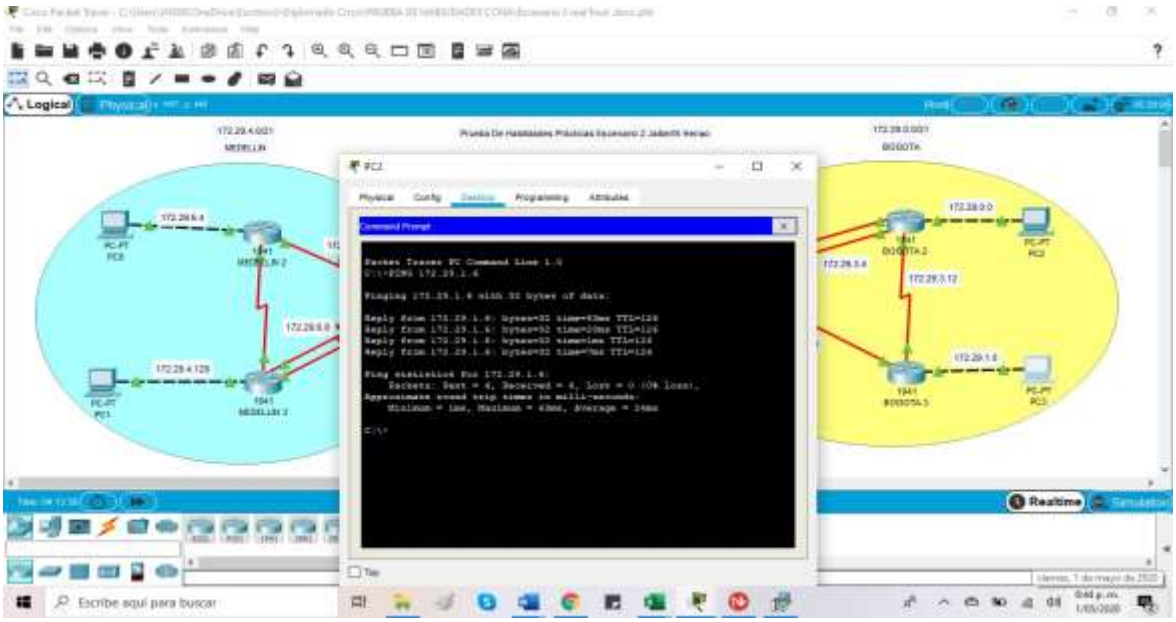

Figura 42. Ping De PC2 A PC3

CONCLUSIONES

El uso de las diferentes tecnologías de cisco, en este caso la del simulador “Cisco Packet Tracer” han permitido desarrollar destrezas y habilidades en la configuración y uso de los distintos dispositivos de red que posee la herramienta.

Las competencias que se han implementado y adquirido durante el desarrollo de la presente prueba de habilidades prácticas, sin duda son un paso fundamental en la motivación para seguir estudiando el tema de redes y en la preparación para la certificación CCNA

Se ha reflexionado en la importancia de los conocimientos adquiridos en esta prueba como es el caso del protocolo “OSPF” y “NAT” y como son muy importantes y una buena solución a problemas de enrutamiento de redes.

BIBLIOGRAFÍA

ENRUTAMIENTO DINÁMICO. “Principios de Enrutamiento y Conmutación” (2017). Disponible en: https://static-course assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

LISTAS DE CONTROL DE ACCESO. “Principios de Enrutamiento y Conmutación”. (2017). Disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

OSPF DE UNA SOLA ÁREA. “Principios de Enrutamiento y Conmutación” (2017). Disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

PROTOCOLOS DHCP. “Principios de Enrutamiento y Conmutación”. (2017). Disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

TRADUCCIÓN DE DIRECCIONES IP PARA IPV4. “Principios de Enrutamiento y Conmutación”. (2017). Disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1