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

GILBERTO JAVIER ALARCÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
CCAV PUERTO COLOMBIA
BARRANQUILLA, ATLÁNTICO
2020

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

GILBERTO JAVIER ALARCÓN

TUTOR
GUSTAVO ADOLFO RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
BARRANQUILLA, ATLÁNTICO
2020

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE GRAFICAS

RESUMEN

El siguiente trabajo tiene como objetivo, evaluar competencias y habilidades para el diseño e implementación de soluciones de red escalables, LAN y WAN, a través del uso de la herramienta de simulación Packet Tracer. En este documento se describen cada uno de los pasos ejecutados y los resultados obtenidos en el desarrollo de 2 escenarios de red propuestos, que ponen a prueba la comprensión y aplicación de las temáticas vistas en los módulos CP CCNA1 Y CP CCNA 2.

Palabras claves: configuración, red, Internet, enrutamiento, CISCO, VLAN, LAN, WAN, protocolo.

ABSTRACT

The following work aims to evaluate competencies and skills for the design and implementation of scalable network solutions, LAN and WAN, through the use of the Packet Tracer simulation tool. This document describes each of the steps carried out and the results obtained in the development of two proposed network scenarios, which test the understanding and application of the themes seen in the CP CCNA1 and CP CCNA2 modules.

Keywords: configuration, network, Internet, routing, CISCO, VLAN, LAN, WAN, Protocol.

GLOSARIO

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

Red: Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes. En inglés se le conoce como Network. El internet está compuesto de miles de redes, por lo tanto internet también se le conoce como "la red".

DNS: Servidor de Nombres de Dominio. Servidor automatizado utilizado en el internet cuya tares es convertir a nombres fáciles de Recordar (como www.panamacom.com) a direcciones numéricas de IP.

DHCP: Siglas del inglés "Dynamic Host Configuración Protocolo." Protocolo Dinámico de Configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a las diferentes computadoras de la red.

LAN (Local Área Network). Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones.

WAN, Siglas del inglés Wide Área Network (Red de área Amplia). Es una red de computadoras conectadas entre sí. Usando líneas terrestres o satélites para interconectar redes LAN en un área geográfica extensa que puede ser hasta de miles de kilómetros.

VLAN, Siglas de virtual LAN (red de área local virtual)- Es un método que permite crear redes lógicas independientes compartiendo dispositivos físicos de red, ofreciendo una subdivisión por grupos garantizando la comunicación y envío de los datos en la red como si se tratará de redes aisladas.

NAT: Network Address Translation o Network Address Translator es la traducción de IPs privados de una red en IP públicos, para que la red pueda enviar paquetes al exterior, y viceversa**.**

Servidor: Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

Switch: permiten que los dispositivos en su red se comuniquen entre sí, recibiendo paquetes de datos y direccionándolos al destinatario correcto. Al hacer posible que la información y los recursos sean compartidos, los switches le ayudan a ahorrar dinero e incrementar la productividad.

Router: Un router es un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino.

Telnet: Comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.

Ping (Buscador de paquetes de Internet): Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

Dirección IP: Dirección que se utiliza para identificar un equipo o dispositivo en una red.

INTRODUCCIÓN

La evolución de Internet ha constituido toda una revolución para las comunicaciones, ya que ha permitido la aparición de múltiples servicios como videoconferencias, chats, email, foros de discusión, transferencia de archivos, etc. que facilitan la interacción sincrónica y asincrónica de personas en ubicaciones distantes. Todo lo anterior es posible gracias a un trabajo conjunto entre hardware y software que permite una rápida y eficaz conectividad en el mundo actual. Otro factor importante de esta revolución tecnológica ha sido la aparición de IPV6, el cual representa la solución a la escasez de direcciones IP que estaba experimentando Internet en la última década y, a su vez, constituye el cimiento que posibilitará el despliegue de Internet de las cosas.

En el presente trabajo se propone la implementación de infraestructuras de red a través de dos casos de estudios que ponen a prueba la comprensión y aplicación de las temáticas vistas en los módulos CP CCNA1 Y CP CCNA 2 de Cisco Networking Academy. Estos 2 escenarios incluyen la implantación de los protocolos de routing dinámico RIPv2 y OSPF, protocolo de configuración de hosts dinámicos (DHCP), traducción de direcciones de red PAT y NAT, listas de control de acceso (ACL), protocolo de tiempo de red (NTP) servidor/cliente, direccionamiento IP versión 4 y 6, sistema de autenticación CHAP, seguridad y configuración de equipos CISCO. Para el desarrollo de los dos casos de estudios se realizarán por medio del programa de simulación de red Packet Tracer.

El presente trabajo debe contener las diferentes configuraciones aplicadas en cada uno de los equipos de red, verificación exitosa de las conexiones por medio de imágenes y las respectivas conclusiones finales. Adicionalmente, los archivos de simulación en Packet Tracer o GNS3 asociados a la actividad servirán de soporte para evidenciar el correcto funcionamiento de las dos topologías implementadas.

OBJETIVOS

OBJETIVO GENERAL

Implementar soluciones LAN/WAN bajo el uso de tecnología Cisco que permita evidenciar la adquisición de competencias y habilidades relacionadas con el montaje, inicialización, configuración, seguridad y conectividad de los diferentes dispositivos que conformaran los 2 escenarios de red propuestos.

OBJETIVOS ESPECIFICOS

- ✓ Documentar cada una de las configuraciones realizadas en los equipos de red.
- ✓ Evidenciar la conectividad de los de escenarios de red propuestos, por medio de la utilización de los comandos ping, traceroute, show ip route, entre otros.
- ✓ Emplear una herramienta de simulación de red para desarrollar el montaje y configuración de las dos topologías de red propuestas.
- ✓ Configurar protocolos que posibiliten la comunicación entre los diversos dispositivos de red de los 2 escenarios propuestos.

DESARROLLO 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

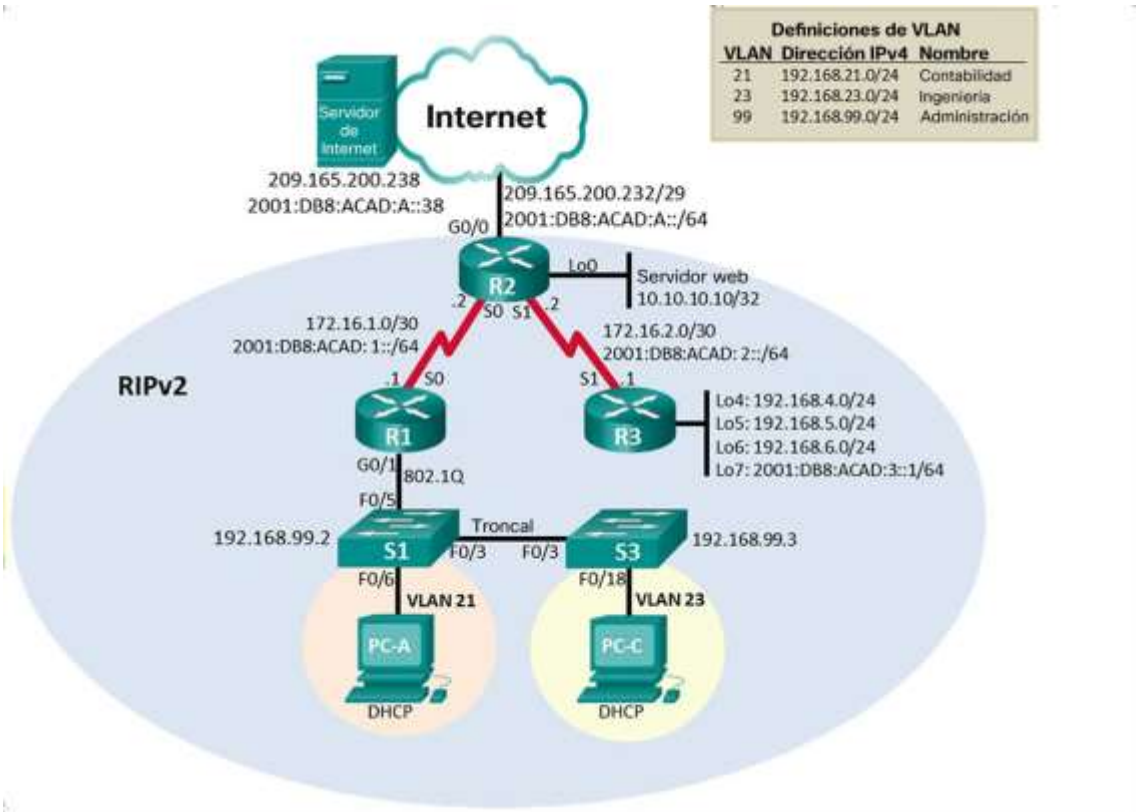

Figura 1. Escenario de red 1

1.1 Parte 1: Inicializar dispositivos

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

Router#erase startup-config // Eliminar el archivo startup-config de todos los routers
Router#reload // Volver a cargar todos los routers

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

Nota: Estas configuraciones se hacen por lo general en laboratorios físicos.

1.2 Parte 2: Configurar los parámetros básicos de los dispositivos

1.2.1 Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238/29
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 1. Configuración de direcciones en la computadora de Internet.

Clase c

Network:	209.165.200.232/29	11010001.10100101.11001000.11101**.000**
HostMin:	209.165.200.233	11010001.10100101.11001000.11101 **001**
HostMax:	209.165.200.238	11010001.10100101.11001000.11101 **110**
Broadcast:	209.165.200.239	11010001.10100101.11001000.11101 111
Hosts:	6	

Tabla 2. Subnnetting : red 209.165.200.232.

1.2.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Configuraciones básicas en R1

Router(config)#no ip domain-lookup **// Desactivar la búsqueda DNS**
Router(config)#hostname R1 **// Nombre del router**
R1(config)#enable secret class **// Contraseña de exec privilegiado cifrada**
R1(config)#line console 0 **// Contraseña de acceso a la consola**
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15 **// Contraseña de acceso Telnet**
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption **// Cifrar las contraseñas de texto no cifrado**
R1(config)#banner motd #Se prohibe el acceso no autorizado. # **// Mensaje MOTD**

Configuración Interfaz S0/0/0

R1(config)#int s0/0/0
R1(config-if)#description Connection R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:ACAD:1::1/64
R1(config-if)#clock rate 128000

R1(config-if)#no shutdown

Configuración de rutas predeterminadas IPV4 e IPV6: Permite al router enviar paquetes a las redes que no estan incluidas en la tabla de enrutamiento

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 unicast-routing **//Habilitar protocolo IPV6**
R1(config)#ipv6 route ::/0 s0/0/0

Verificación de tabla de enrutamiento en R1

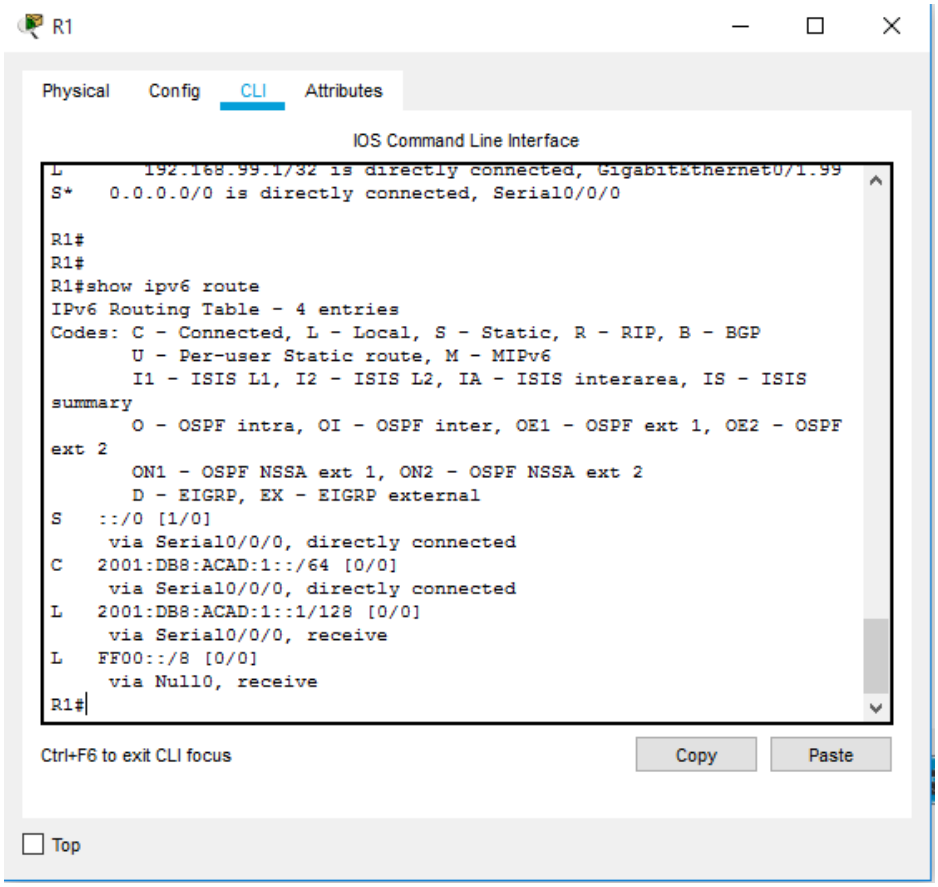

Figura 2.Verificación de tabla de enrutamiento IPV6 en R1.

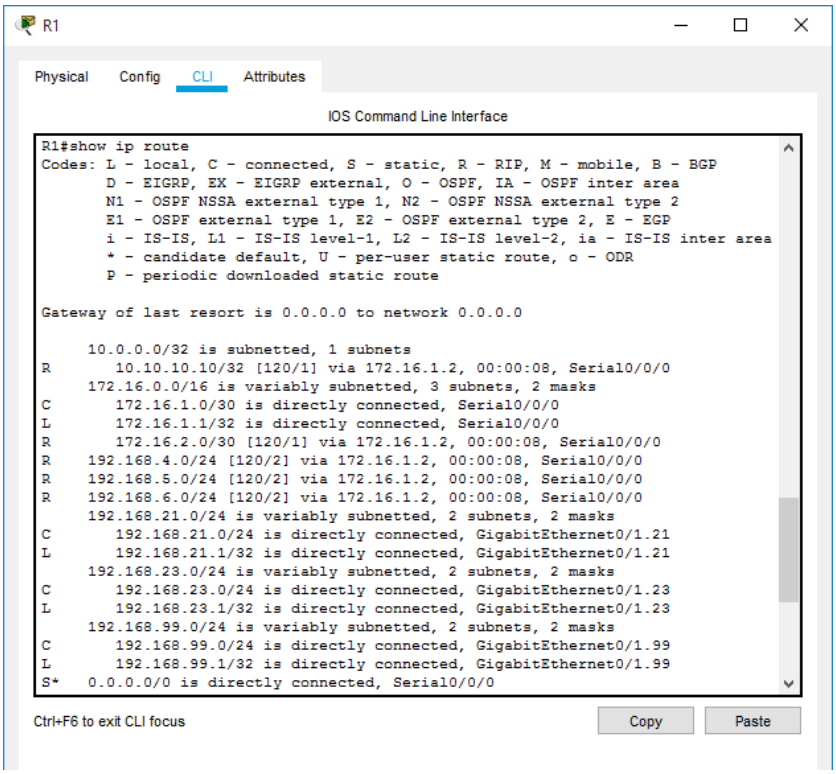

Figura 3. Tabla de enrutamiento IPV4 en R1.

1.2.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

```
Router>en
Router#config t
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.#
```

Habilitar el servidor HTTP

R2(config)#ip http server

Configuración de interfaz S0/0/0

R2(config)#int s0/0/0
R2(config-if)#description Connection to R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown

Configuración de interfaz S0/0/1

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

Configuración de interfaz g0/0

R2(config-if)#int g0/0
R2(config-if)#description Connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown

Interfaz loopback o (servidor web simulado)

R2(config-if)#int loopback 0
R2(config-if)#description servidor web simulado
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#no shutdown

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

Verificación de tabla de enrutamiento R2

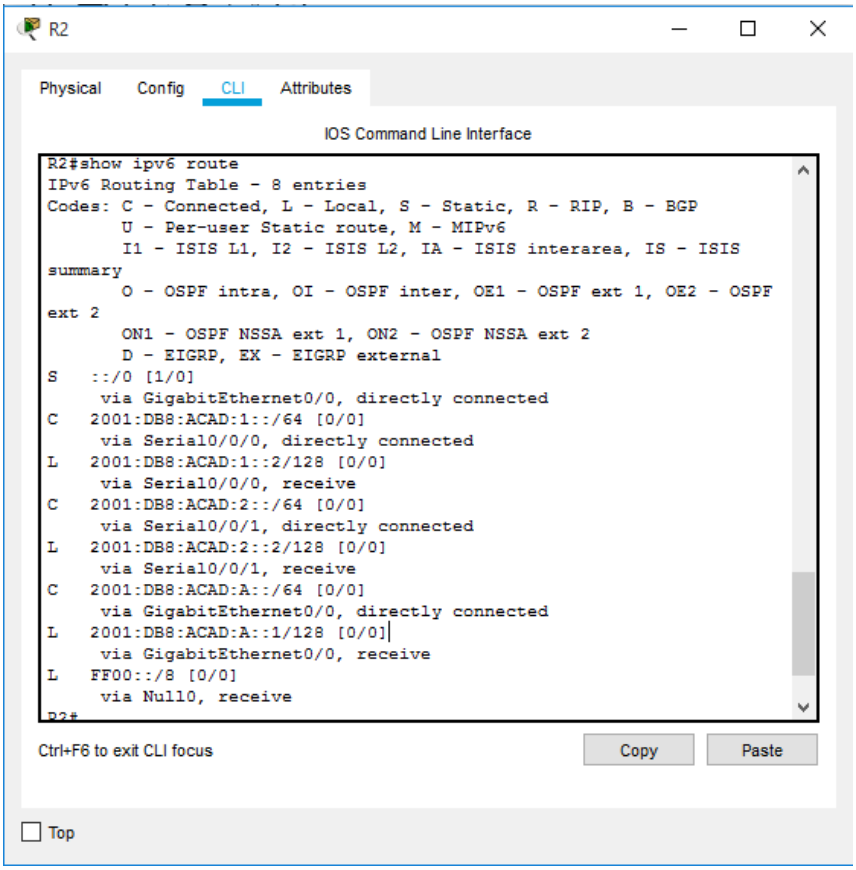

Figura 4. Verificación de tabla de enrutamiento IPV6 en R2

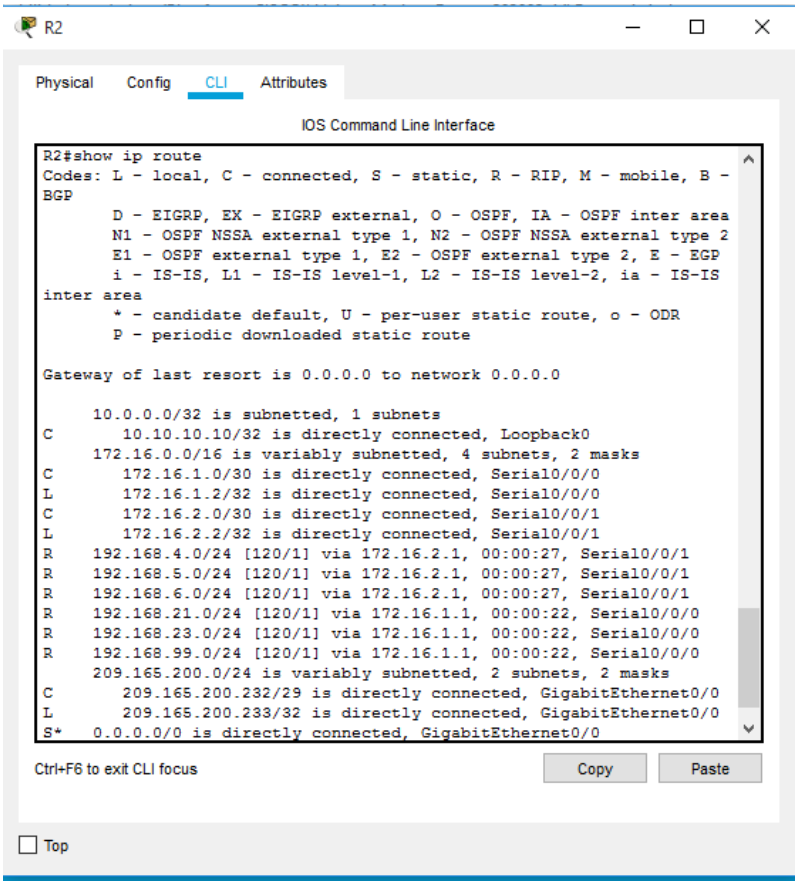

Figura 5.Tabla de enrutamiento IPV4 en R2.

1.2.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

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.#

Interfaz S0/0/1

```
R3(config)#int s0/0/1
R3(config-if)#Description Connection 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 shutdown
```

Interfaz loopback 4

```
R3(config-if)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
```

Interfaz loopback 5

```
R3(config-if)#int loopback 5
R3(config-if)#
R3(config-if)#ip address 192.168.5.1 255.255.255.0
```

Interfaz loopback 6

```
R3(config-if)#int loopback 6
R3(config-if)#
R3(config-if)#ip address 192.168.6.1 255.255.255.0
```

Interfaz loopback 7

```
R3(config-if)#int loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
```

Rutas predeterminadas

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 route ::/0 s0/0/1
```

Verificación de tabla de enrutamiento R3

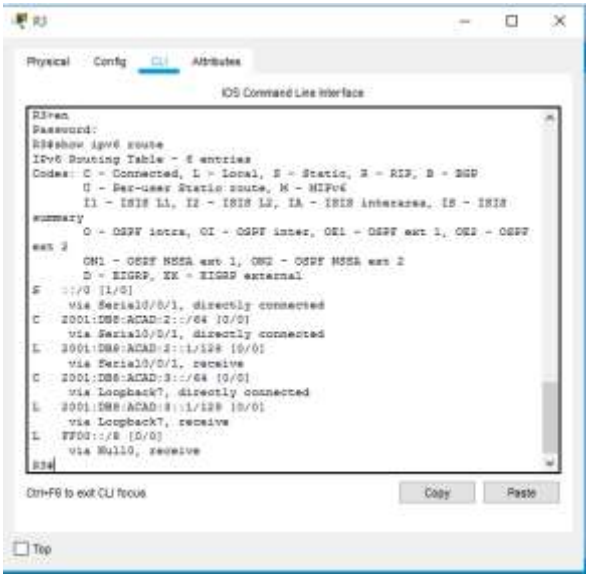

Figura 6.Verificación tabla de enrutamiento IPV6 en R3.

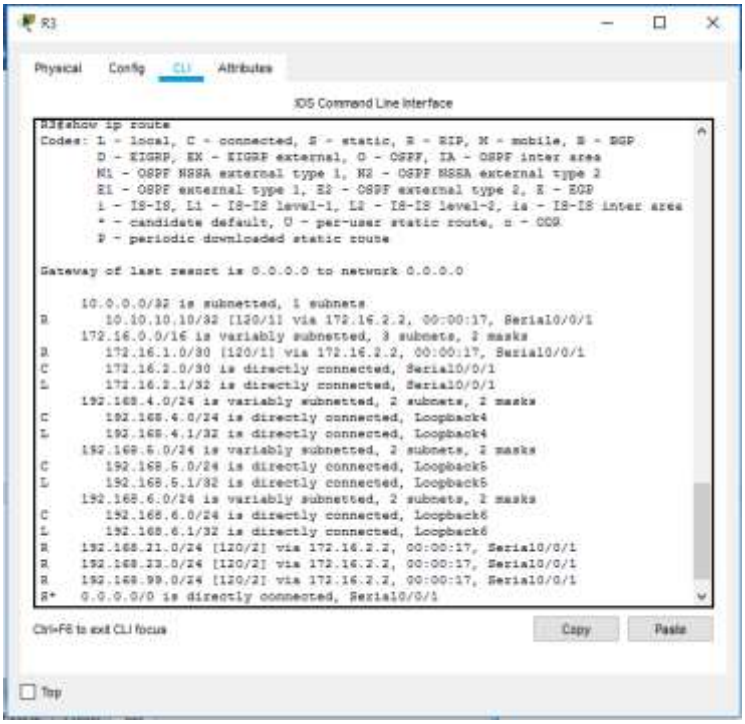

Figura 7.Tabla de enrutamiento IPV6 en R3.

.

1.2.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

```
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.#
```

1.2.6 Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

```
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-line)# banner motd #Se prohibe el acceso no autorizado.#
```

1.2.7 Paso 7 Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	5/5
R2	R3, S0/0/1	172.16.2.2	5/5
PC de Internet	Gateway predeterminado	209.165.200.233	Packets: Sent = 4, Received = 4, Lost = 0

Verificación de ping R1 a R2 y viceversa

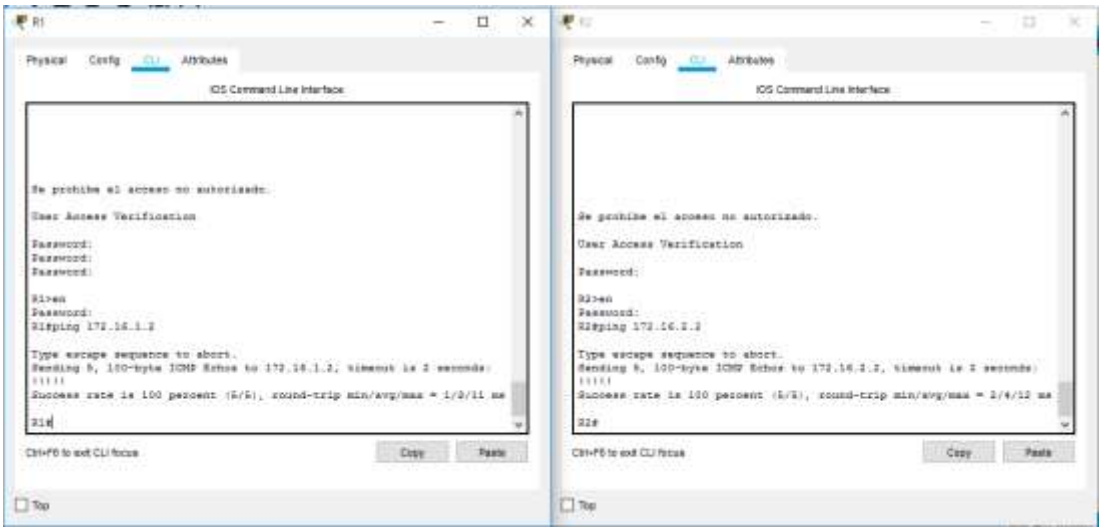

Figura 8. Verificación de conectividad entre R1 y R2

Servidor de Internet: Conexión.

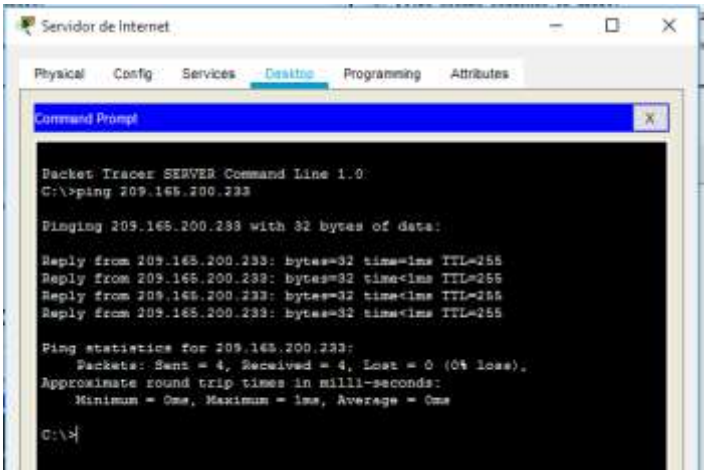

Figura 9. Verificación de conectividad a Servidor de Internet.

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

1.3.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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 Administración
```

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)#no shutdown
```

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 f0/3
S1(config-if)#switchport mode trunk
```

Forzar el enlace troncal en la interfaz F0/5

```
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
```

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
```

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

1.3.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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

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)#no shutdown

Asignar el gateway predeterminado.
S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso
S3(config)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode Access

Asignar F0/18 a la VLAN 23
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23

Apagar todos los puertos sin usar

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

Verificación de VLAN configuradas S1 Y S2

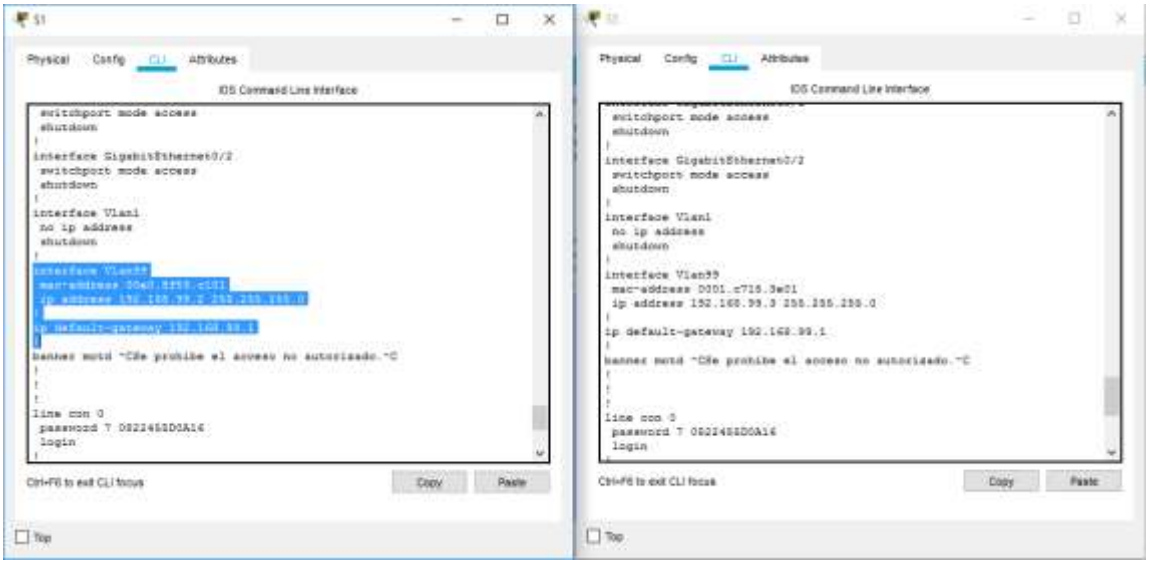

Figura 10. Verificación de VLAN configuradas en S1 y S2

Verificación de asignación de vlan en S1(21 a F0/6) y S2(23 a F0/18)

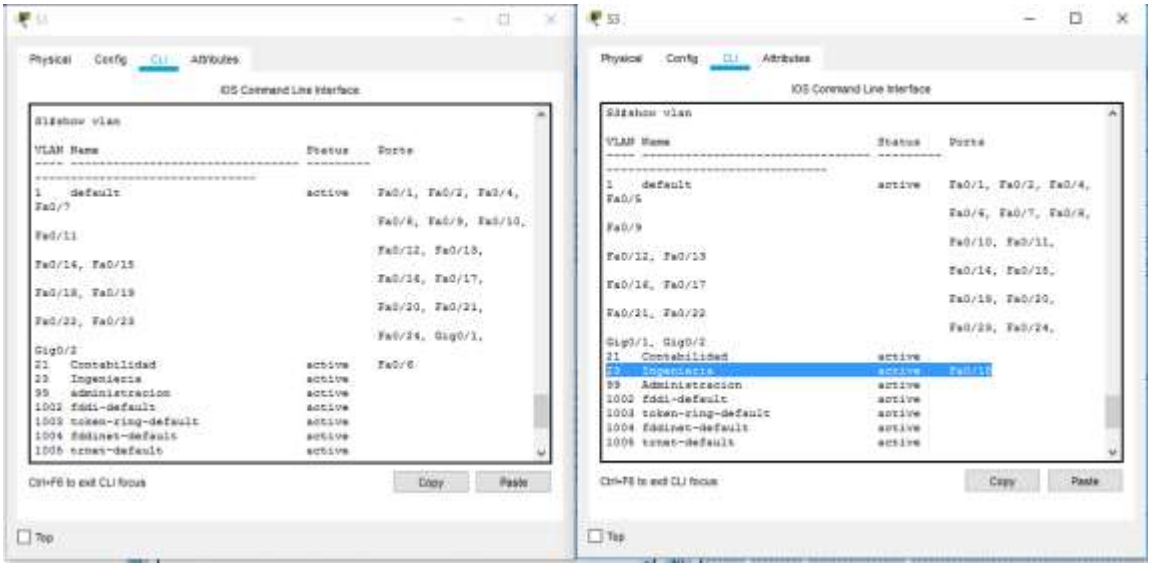

Figura 11. Verificación de asignación de VLAN en S1 (21 a F0/6) y S3 (23 A F0/18)

1.3.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Configurar la subinterfaz 802.1Q .21 en G0/1

```
R1(config)#int 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
```

Configurar la subinterfaz 802.1Q .23 en G0/1

```
R1(config-subif)#int 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
```

Configurar la subinterfaz

802.1Q .99 en G0/1R1(config-subif)#int 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
```

Activar la interfaz G0/1

```
R1(config-subif)#int g0/1
R1(config-if)#no shutdown
```

1.3.4 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	5/5
S3	R1, dirección VLAN 99	192.168.99.1	5/5
S1	R1, dirección VLAN 21	192.168.21.1	5/5
S3	R1, dirección VLAN 23	192.168.23.1	5/5

Tabla 3. Verificar la conectividad de la red

Comprobacion de conexiones S3 a R1 y S1 a R1

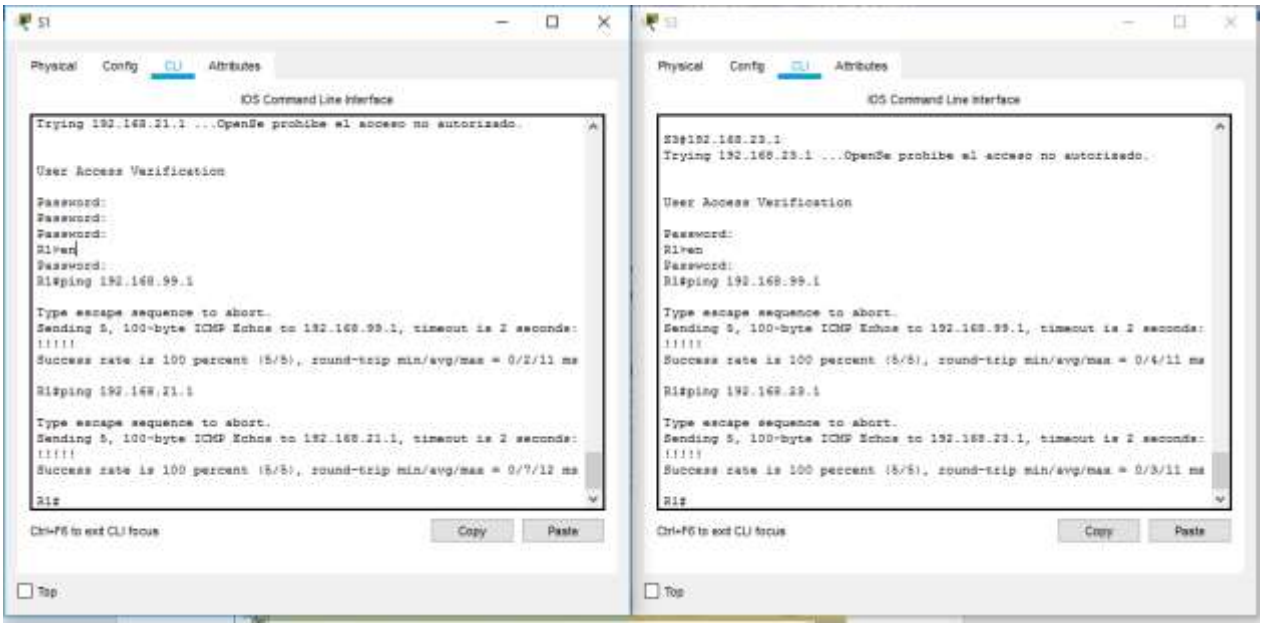

Figura 12. Comprobación de conexiones S3 a R1 y S1 a R1

1.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2

1.4.1 Paso1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Configurar RIP versión 2
R1(config)#router rip
R1(config-router)#version 2

Anunciar las redes conectadas directamente
R1(config-router)#do show ip route connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0

R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0

Establecer todas las interfaces LAN como pasivas
R1(config-router)#passive-interface 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

1.4.2 Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Configurar RIP versión 2
R2(config)#router rip
R2(config-router)#version 2

Anunciar las redes conectadas directamente
R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0

Establecer la interfaz LAN (loopback) como pasiva
R2(config-router)#passive-interface loopback 0

Desactive la sumarización automática.
R2(config-router)#no auto-summary

1.4.1 Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Anunciar redes IPv4 conectadas directamente

```
R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
```

Establecer todas las interfaces de LAN IPv4 (Loopback) como

```
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
```

1.4.2 Parte 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?	**R1#show ip protocols**
¿Qué comando muestra solo las rutas RIP?	**R2#show ip route rip**
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	**R1#show running-config | section router rip** % Invalid input detected at '^' marker. Comando no soportado por PACKET TRACER, se debe usar Usar **show run**

Tabla 4. Verificar la información de RIP a través de comandos.

Verificación del comando show ip protocols en R1, R2 y R3

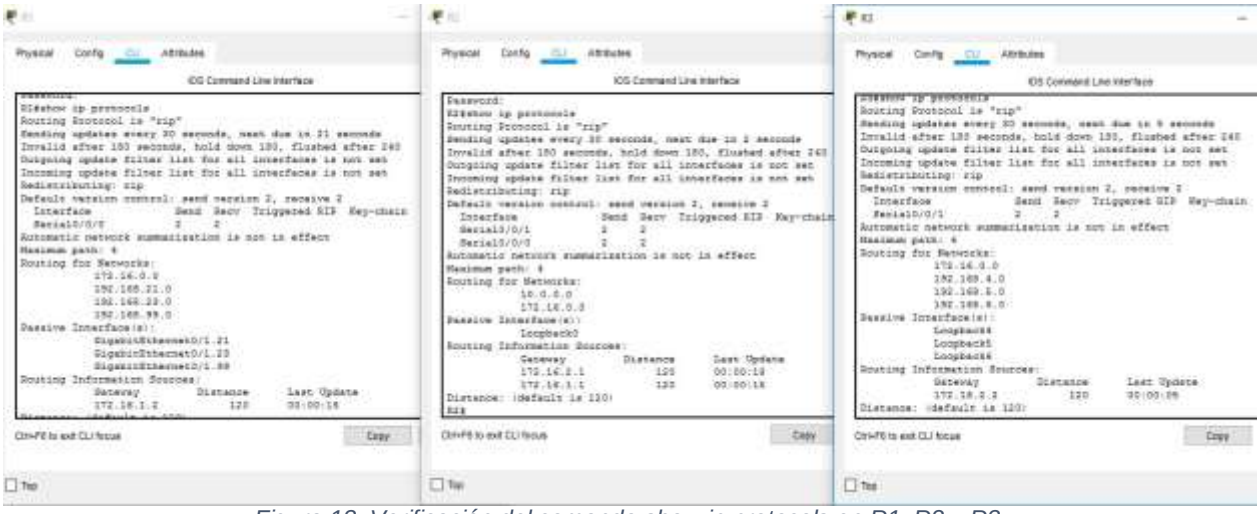

Figura 13. Verificación del comando show ip protocols en R1, R2 y R3.

Verificación del comando show ip route rip R1, R2 y R3

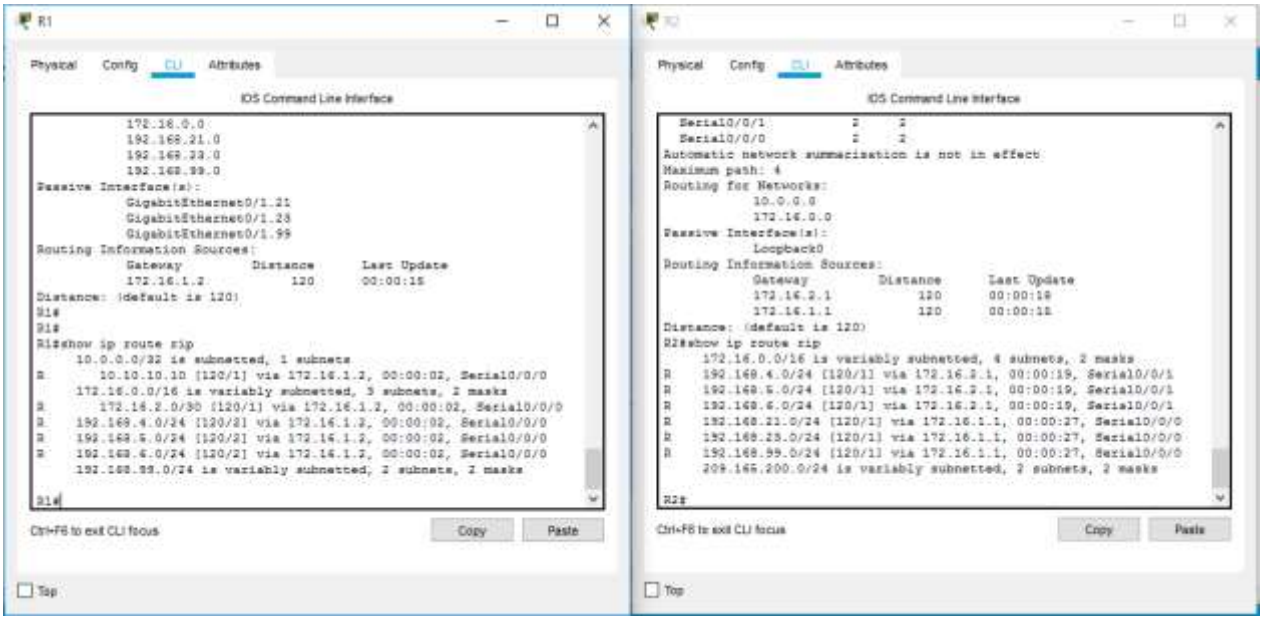

Figura 14. Verificación del comando show ip route rip R1 y R2

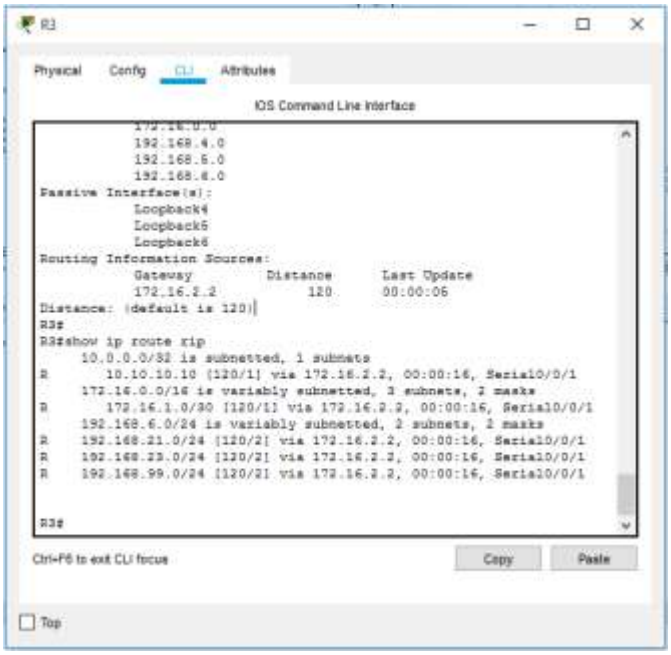

Figura 15. Verificación del comando show ip route rip R3.

Verificación del protocolo RIPv2 a través del comando show run R1, R2 y R3

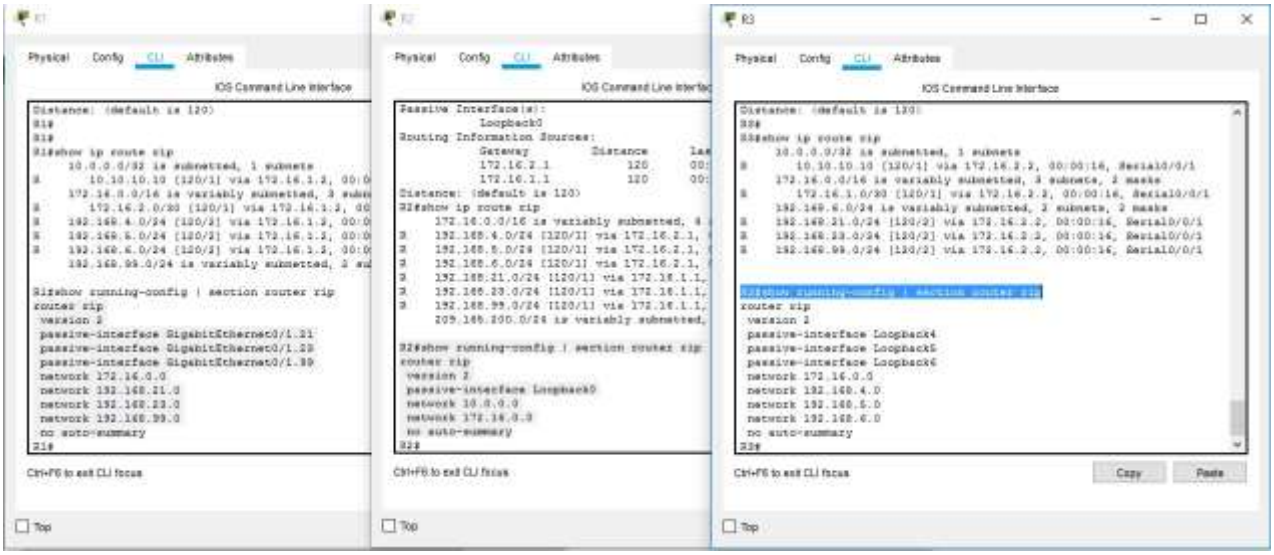

Figura 16. Verificación del protocolo RIPv2 a través del comando show running-config | section router rip R1, R2 y R3.

1.5 Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

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)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com

Crear un pool de DHCP para la VLAN 23

R1(dhcp-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

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

La configuración del R2 incluye las siguientes tareas:

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
Nota. ip http server no es soportado por Packet Tracer.

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

R2(config)#ip http authentication local

Nota. ip http authentication local no es soportado por Packet Tracer.

Crear una NAT estática al servidor web (Dirección global interna: 209.165.200.237**).**

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237

Asignar la interfaz interna y externa para la NAT estática

R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside

Configurar la NAT dinámica dentro de una ACL privada

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255**// Permitir la traducción de las redes de Contabilidad**

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255**// Permitir la traducción de las redes Ingeniería**

R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 **// 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
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

Definir la traducción de NAT dinámica

R2(config)#ip nat inside source list 1 pool INTERNET

NOTA: Para crear una NAT estática al servidor web se usó la dirección global interna: **209.165.200.237**, recordemos que el rango de direcciones esta comprendido desde la

209.165.200.233 ocupada por la G0/0 **hasta la 209.165.200.238** ocupada por el servidor de internet.

1.5.3 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	Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-A pueda hacer ping a la PC-C	Satisfactorio
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.2237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet tracer no soporta este procedimiento, ya que el comando ip http server en R2 tampoco es soportado por este este software

Tabla 5. Verificar el protocolo DHCP y la NAT estática.

Verificación servidor DHCP en PC-A y PC-C

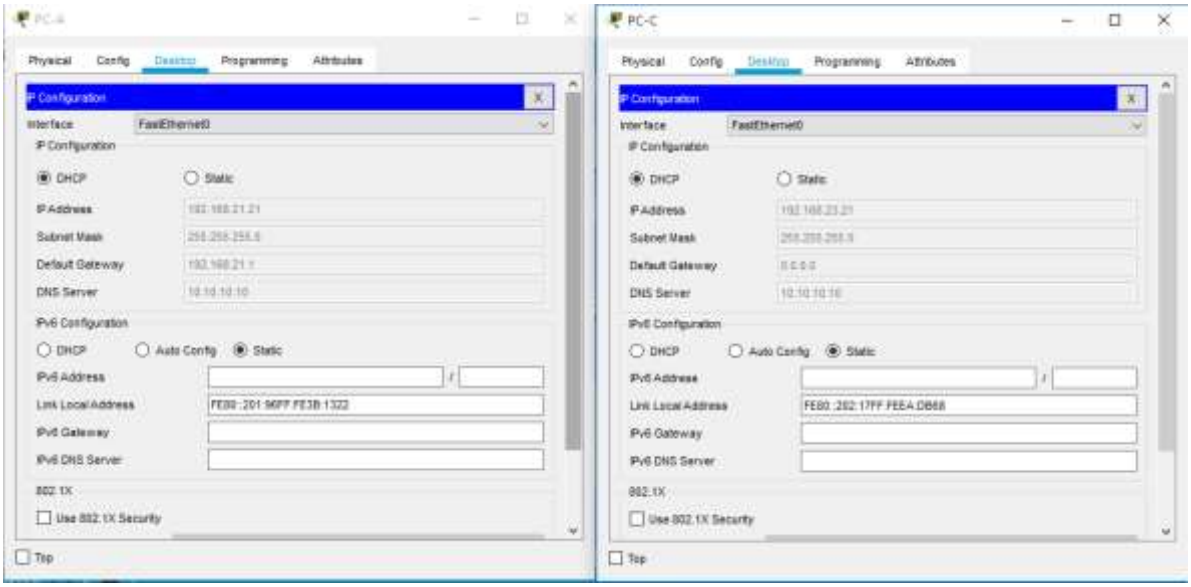

Figura 17. Verificación servidor DHCP en PC-A y PC-C

Verificación Ping PC-A y PC-C

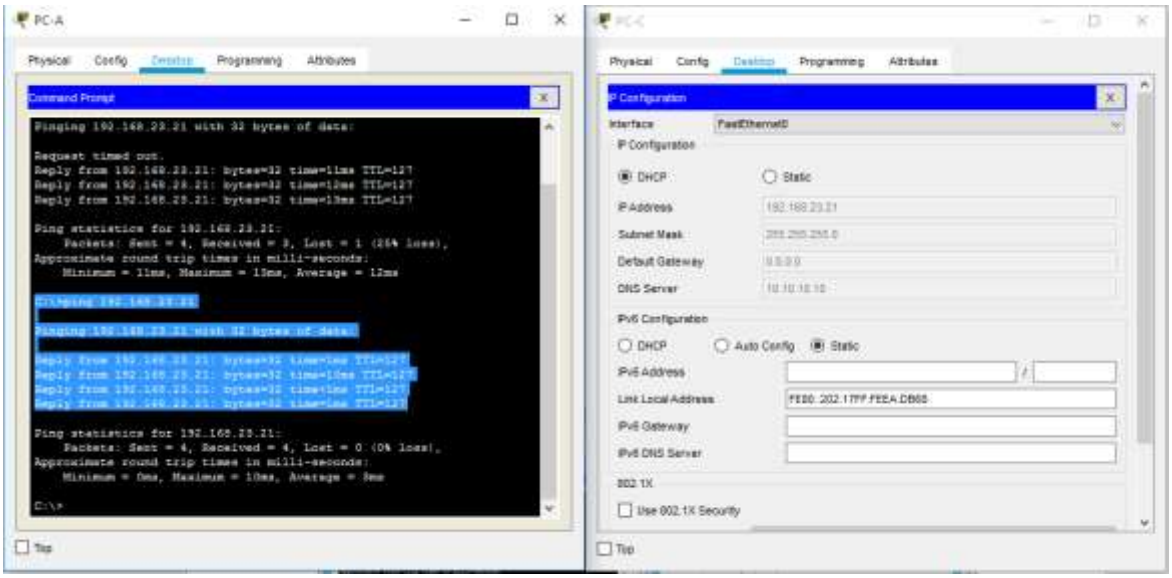

Figura 18. Verificación Ping PC-A y PC-C

1.6 Parte 6: Configurar NTP

Ajuste la fecha y hora en R2.
R2#clock set 14:25:00 july 01 2020

Configure R2 como un maestro NTP.
R2(config)#ntp master 5

Configurar R1 como un cliente NTP.
R1(config)#ntp server 172.16.1.2

Configure R1 para actualizaciones de calendario periódicas con hora NTP.R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1.
R1#show ntp associations

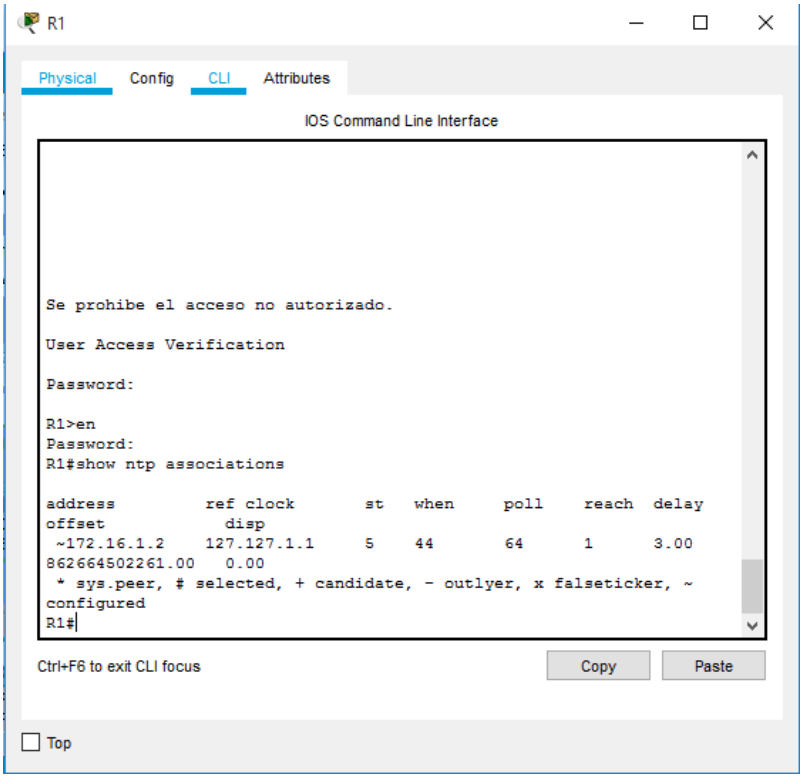

Figura 19. Verificación comando show ntp associations

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

1.7.1 Restringir el acceso a las líneas VTY en el R2

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión
Telnet con R2 Nombre de la ACL: ADMIN-MGT

R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1

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
Verificar que la ACL funcione como se espera Satisfactorio
R1>en
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado.

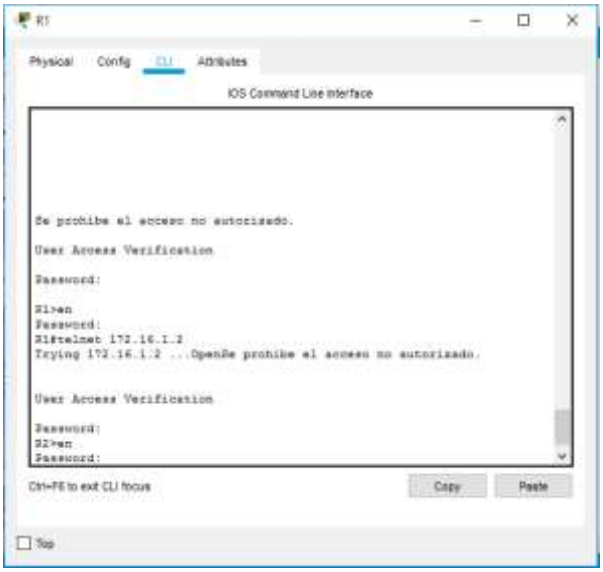

Figura 20. Verificación del funcionamiento de Telnet en R2.

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

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

R2#show access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
R2#show ip access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

Restablecer los contadores de una lista de acceso

R2#clear access-list counters
R2#show ip access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? R/show ip interface

¿Con qué comando se muestran las traducciones NAT?
R/show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.234:1025192.168.23.2:1025 209.165.200.238:80 209.165.200.238:80

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

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---

Interfaz y la dirección ACL en que se aplica

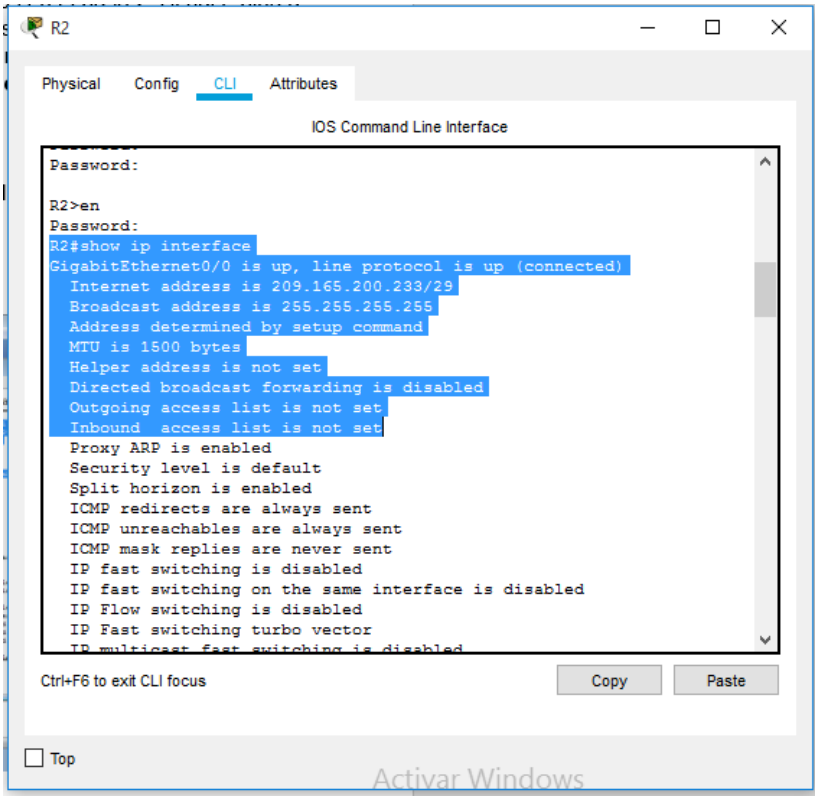

Figura 21. Verificar Interfaz y la dirección ACL a que se aplica

Verificación del comando show ip nat translations

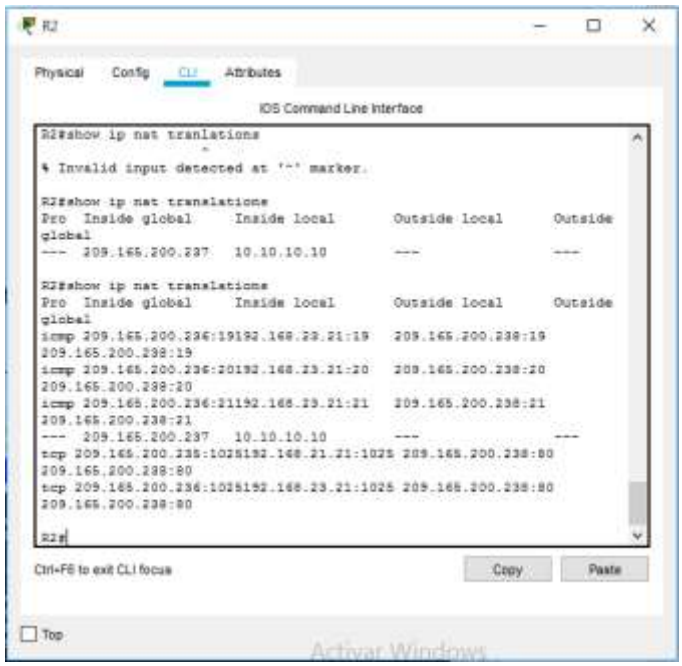

Figura 22. Verificación del comando show ip nat translations.

Verificación de conexión entre PC-A y PC-C al servidor web

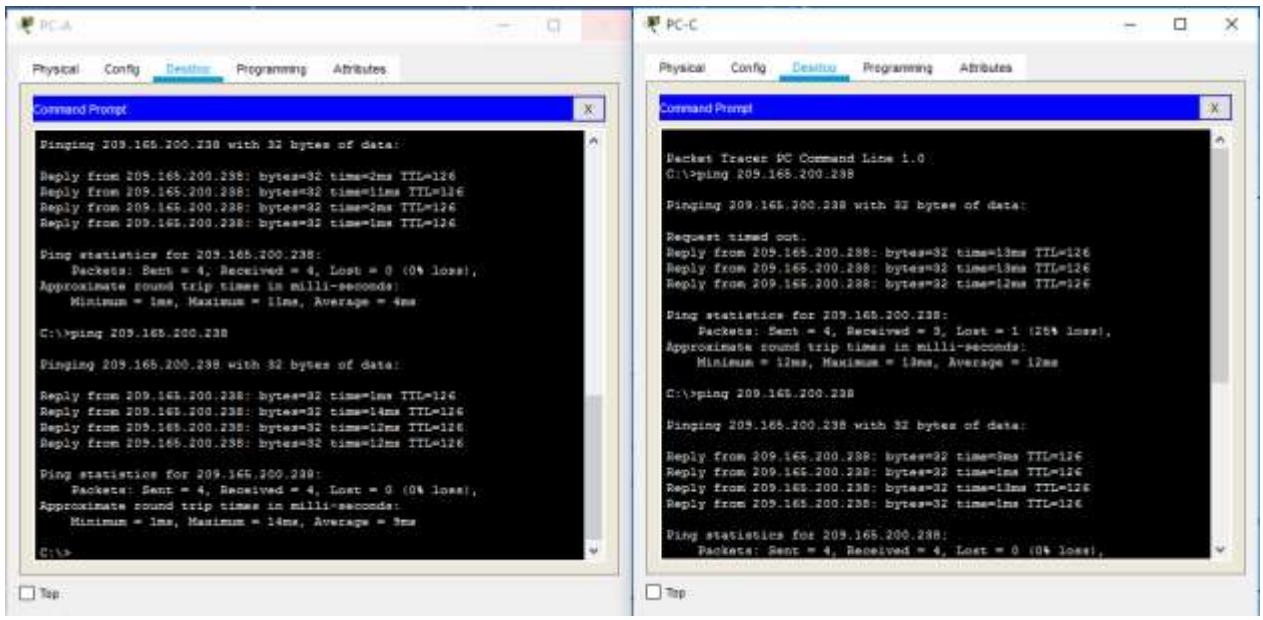

Figura 23. Verificación de conexión entre PC-A y PC-C al servidor web desde el Command Prompt

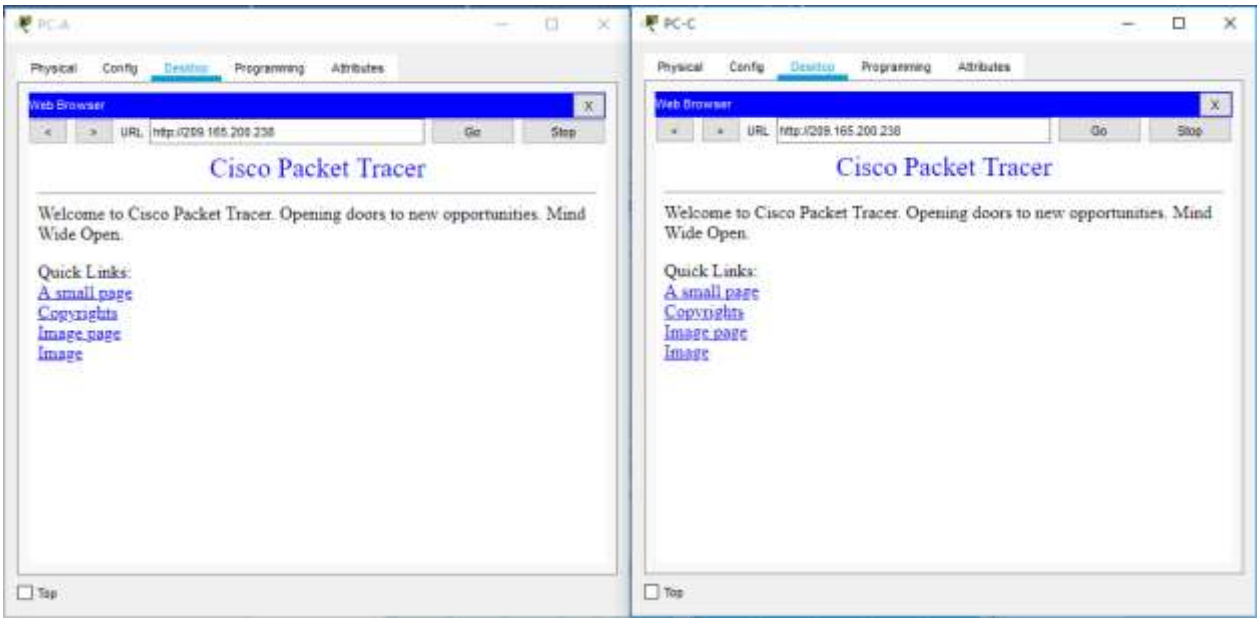

Figura 24. Verificación de conexión entre PC-A y PC-C al servidor web desde el navegador.

.

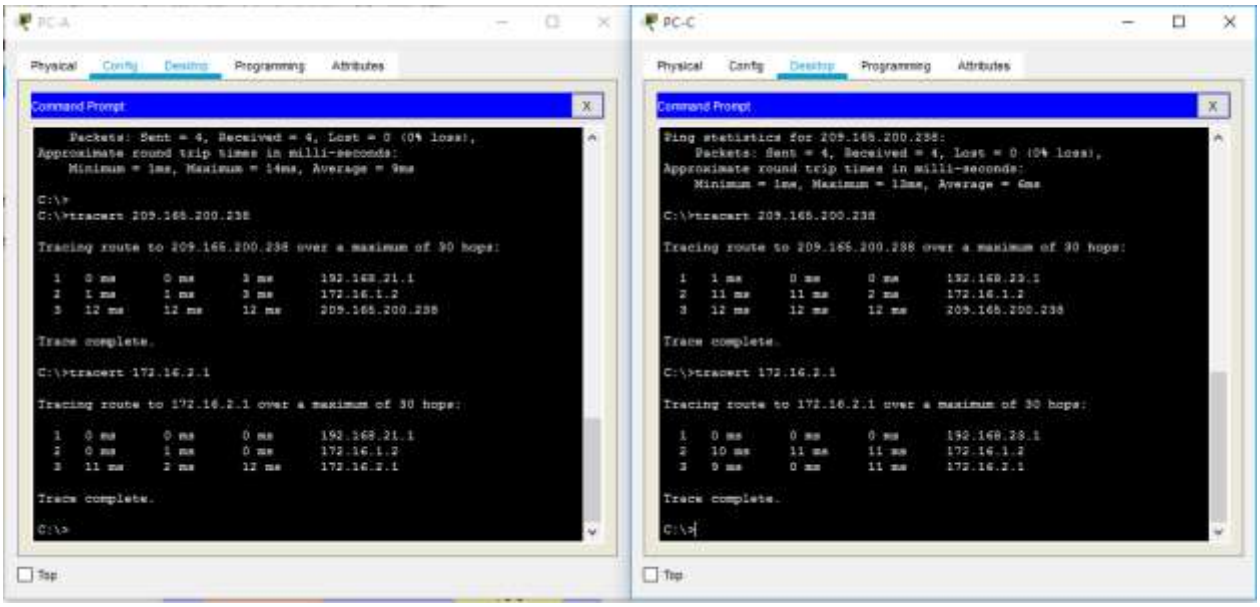

Figura 25. Verificación de la ruta de destino de PC-A y PC-C hasta el servidor de internet a través del comando tracert.

DESARROLLO 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

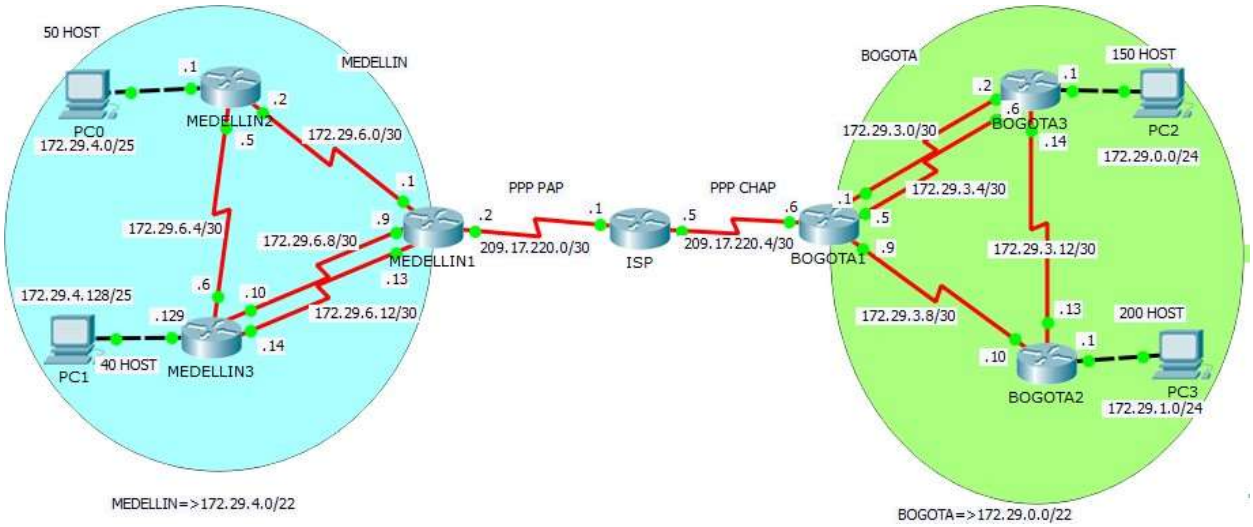

Figura 26. Escenario de red 2

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

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

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

Rutinas de diagnotico aplicadas a todos los routers

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #Acceso no autorizado-Gilberto Javier Alarcón#
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

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

2.1 Parte 1: Configuración del enrutamiento

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

Configuracion OSPF versión 2 en BOGOTA1

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 1.1.1.1
BOGOTA1(config-router)#passive-interface s0/0/0
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.255 area 0
```

Configuracion OSPF versión 2 en BOGOTA2

```
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 2.2.2.2
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA2(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

Configuracion OSPF versión 2 en BOGOTA3

```
BOGOTA3(config)#no router ospf 1
```

```
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 3.3.3.3
BOGOTA3(config-router)#passive-interface g0/0
BOGOTA3(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

Configuracion OSPF versión 2 en MEDELLIN1

```
MEDELLIN1(config)#router ospf 2
MEDELLIN1(config-router)#router-id 1.1.1.1
MEDELLIN1(config-router)#passive-interface s0/0/0
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.255 area 1
```

Configuracion OSPF versión 2 en MEDELLIN2

```
MEDELLIN2(config)#router ospf 2
MEDELLIN2(config-router)#router-id 2.2.2.2
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#network 172.29.0.0 0.0.255.255 area 1
```

Configuracion OSPF versión 2 en MEDELLIN3

```
MEDELLIN3(config)#router ospf 2
MEDELLIN3(config-router)#router-id 3.3.3.3
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#network 172.29.0.0 0.0.255.255 area 1
```

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

Configuración ruta por defecto hacia el ISP y redistribución dentro de las publicaciones

Medellín1

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router ospf 2
MEDELLIN1(config-router)#default-information originate
```

Bogota1

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
```

BOGOTA1(config-router)#default-information originate

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

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

2.2 Parte 2: Tabla de Enrutamiento.

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

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

RTA/ Los enrutadores detectan varias trayectorias para llegar a otra red o subred y seleccionan la ruta con la minima distancia. Si la distancia administrativa es la misma en todos los casos, entonces el router escoge la de mas bajo costo o metrica.

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.

RTA/Estos dos routers permiten el acceso a internet y redistribuyen la ruta estática por defecto a lo routers que tengan adayacencia con cada uno de ellos.

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF. RTA/ Las rutas conectadas mediante OSPF en la tabla de enrutamiento comienzan con la letra 'O'.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto. RTA/ Medellin3 a Medellin1 o Bogotá1 a Bogota2 poseen diversas rutas para comunicarse entre sí.

Tablas de enrutamiento Bogota

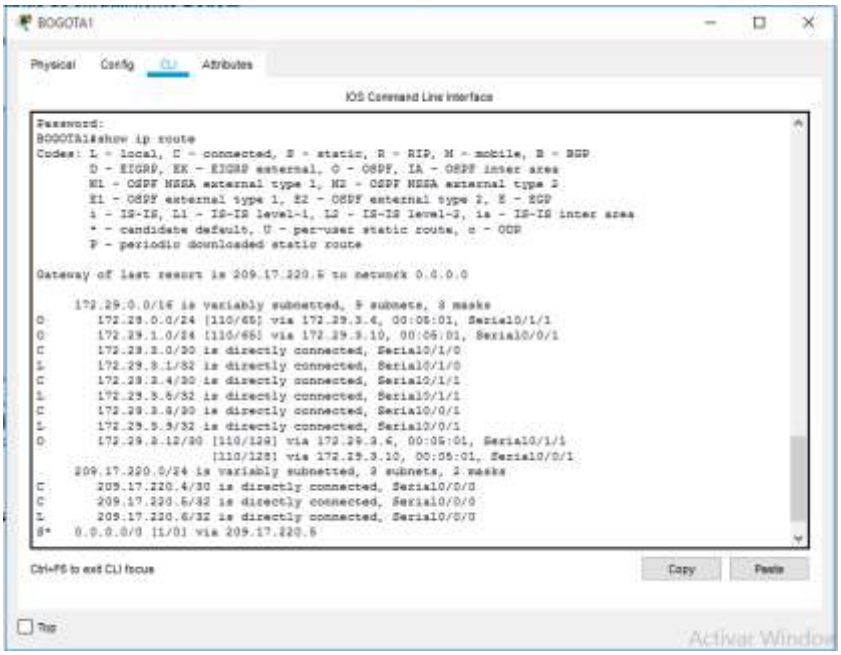

Figura 27. Tablas de enrutamiento BOGOTA1.

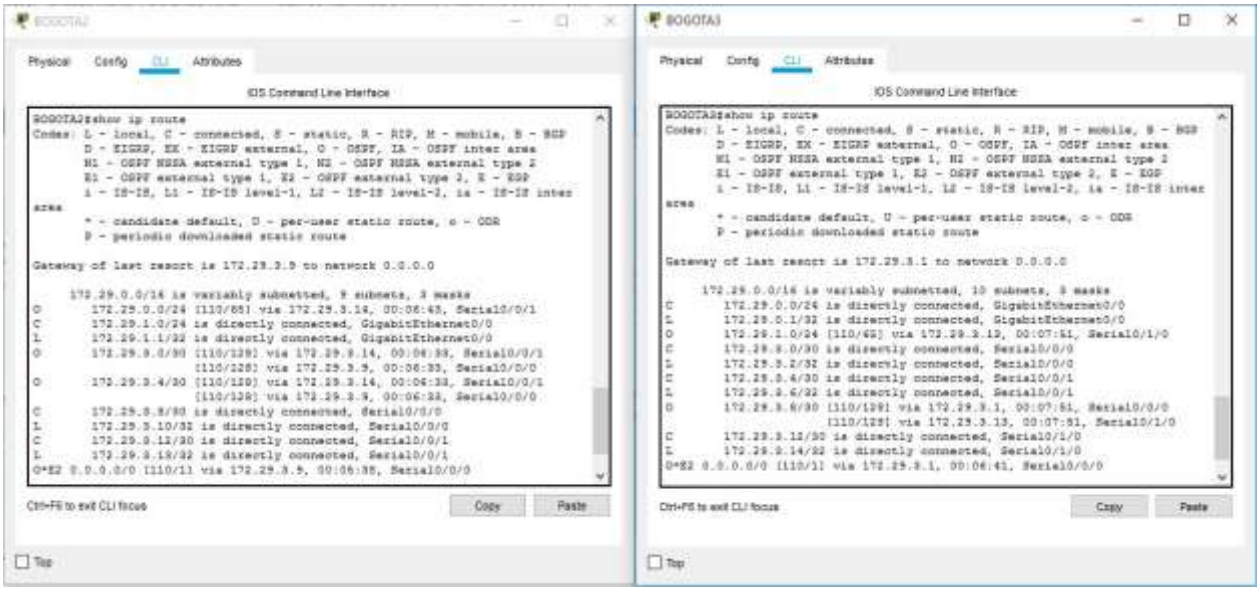

Figura 28. Tablas de enrutamiento BOGOTA2 y BOGOTA3.

Tablas de enrutamiento Medellin

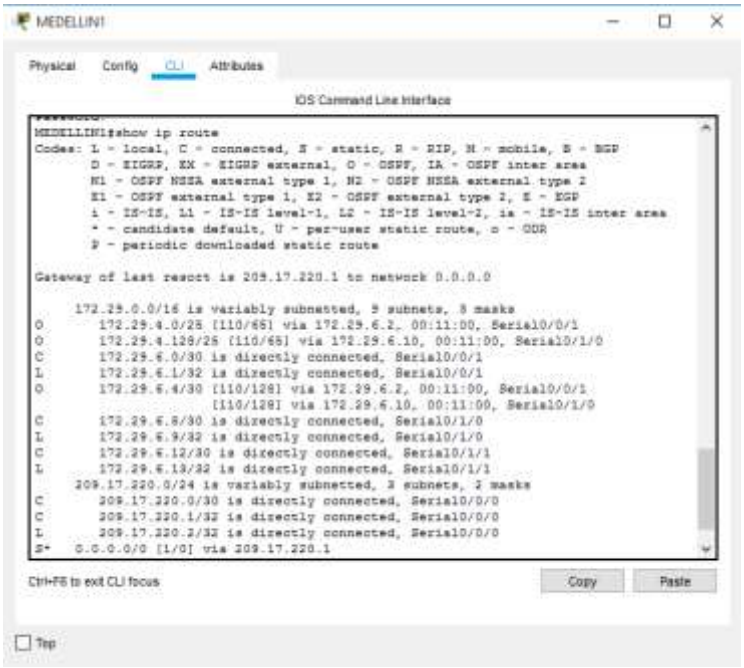

Figura 29. Tablas de enrutamiento MEDELLIN1.

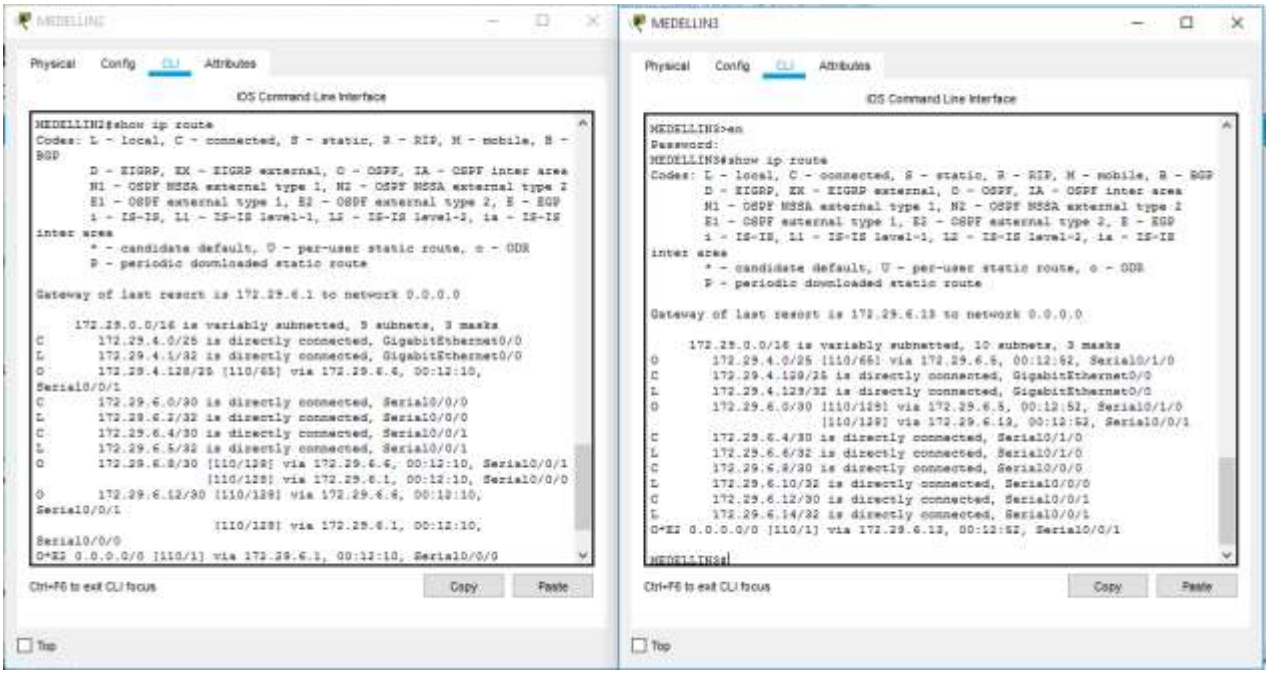

Figura 30. Tabla de enrutamiento MEDELLIN2 y MEDELLIN3.

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

Tabla de enrutamiento ISP

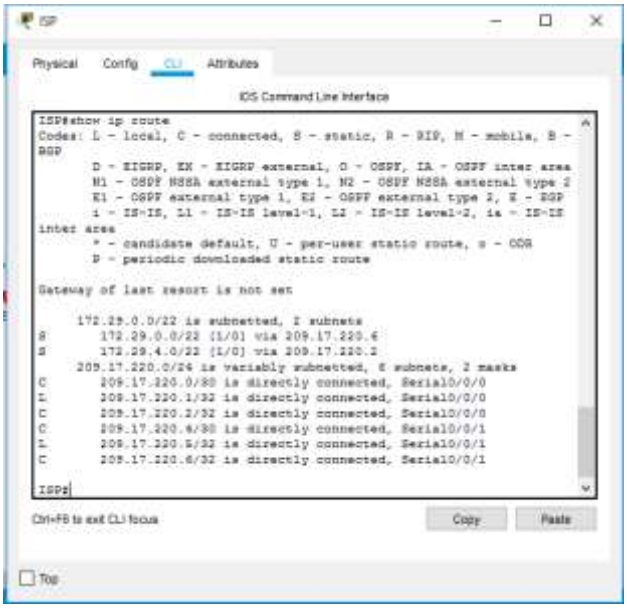

Figura 31. Tabla de enrutamiento ISP.

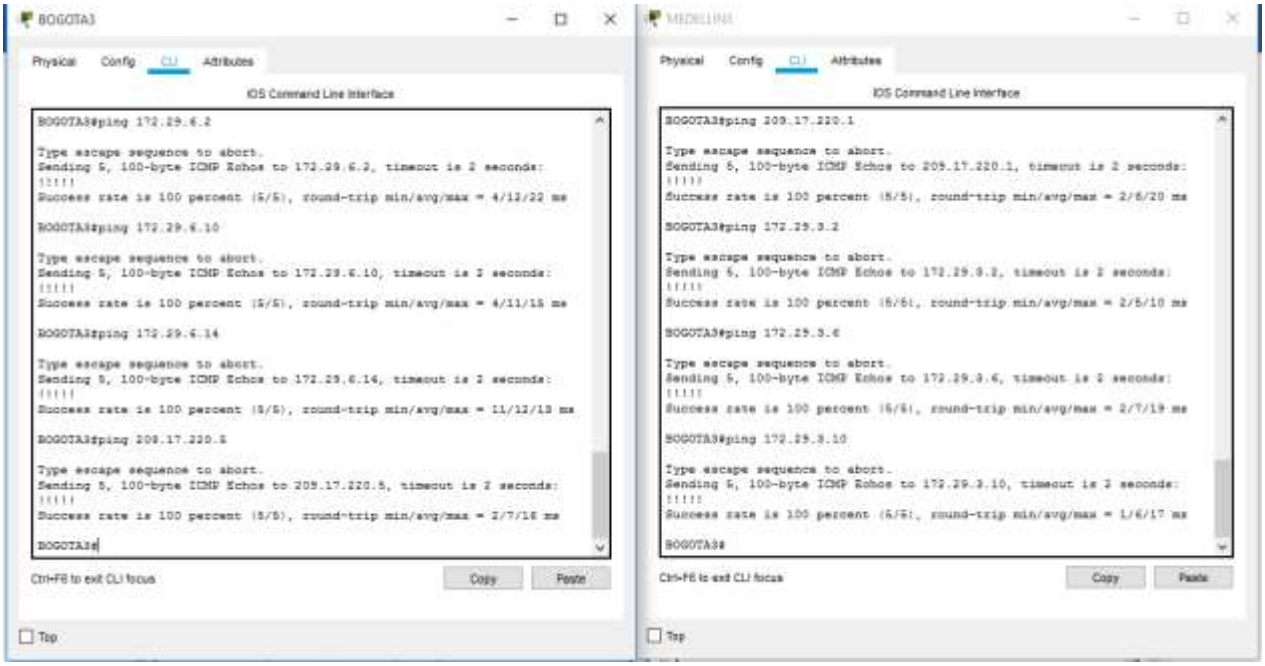

Figura 32. Verificación de conectividad de extremo a extremo entre los Routers de Bogotá y Medellín (BOGOTA3 y MEDELLIN 3).

2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

Esta operación fue realizada en la parte 1 utilizando el comando passive-interface [NUMERO INTERFAZ]

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

Tabla 6.Interfaces que no requieren deshabilitar la propagación del protocolo OSPF.

2.4 Parte 4: Verificación del protocolo OSPF.

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.

Bogotá

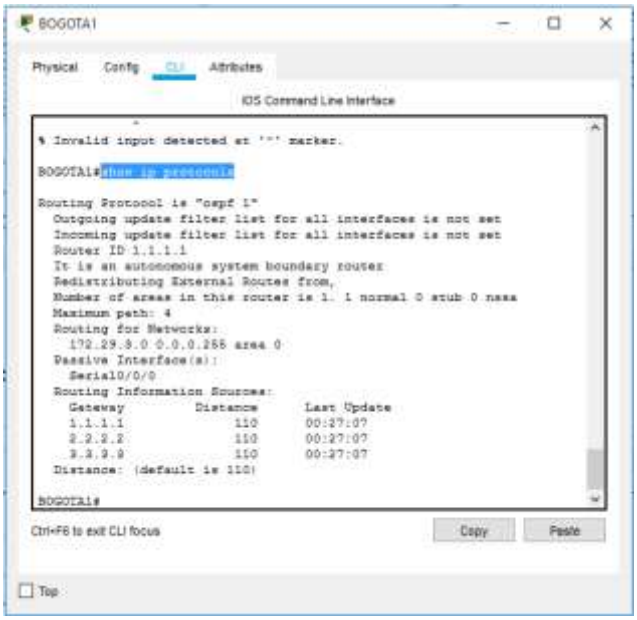

Figura 33. Verificación del protocolo OSPF en BOGOTA1.

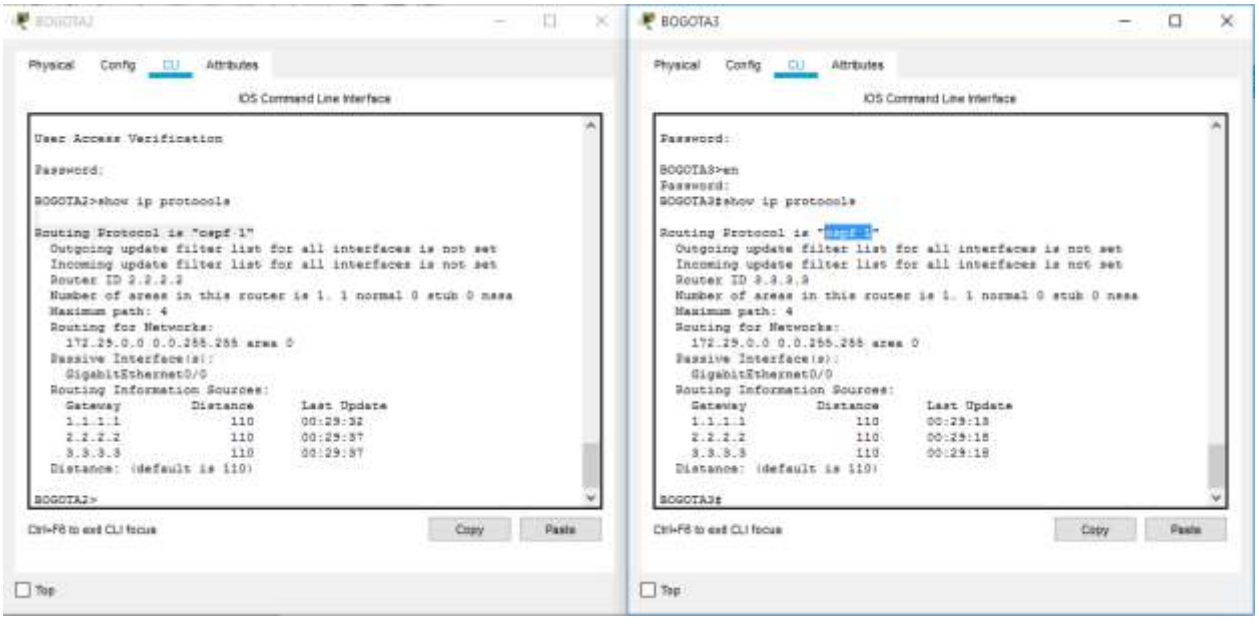

Figura 34. Verificación del protocolo OSPF en BOGOTA2 y BOGOTA3.

Medellín

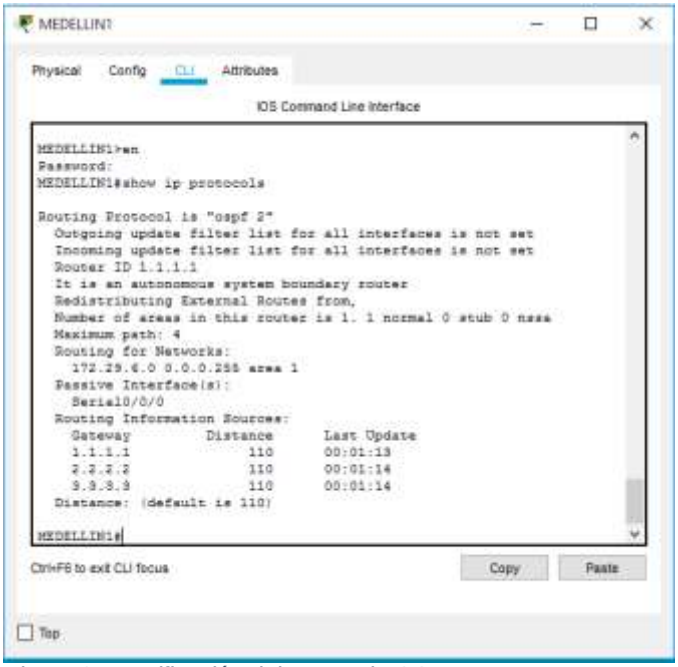

Figura 35. Verificación del protocolo OSPF en MEDELLIN1.

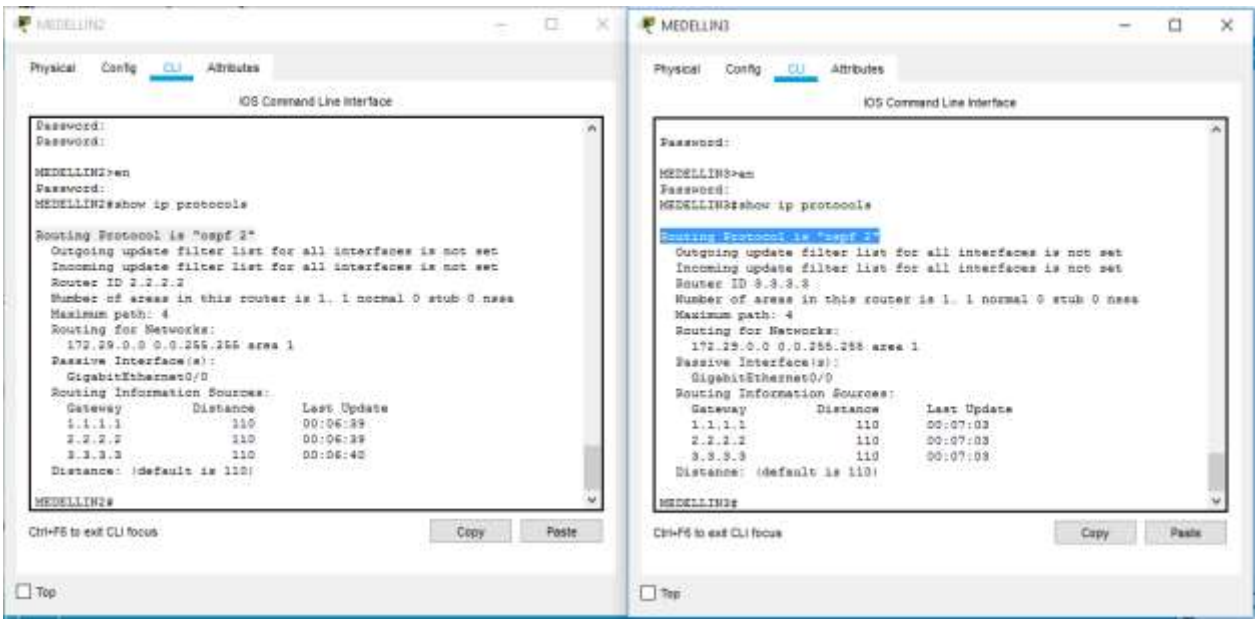

Figura 36. Verificación del protocolo OSPF en MEDELLIN2 y MEDELLIN3.

a. 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.

Bogotá

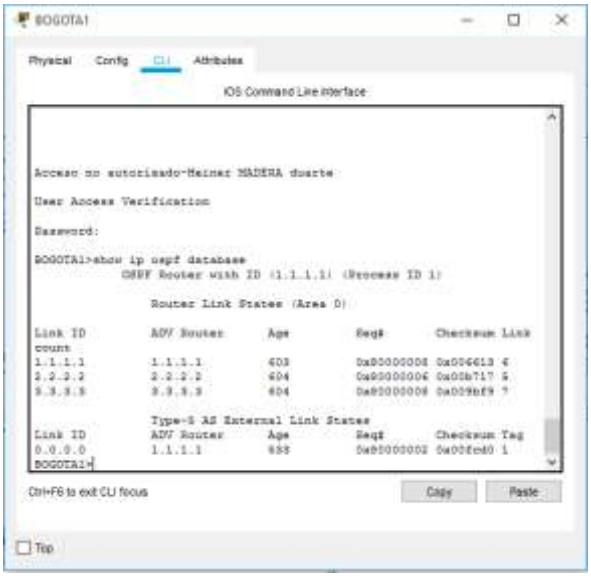

Figura 37. Base de datos de OSPF de BOGOTA1

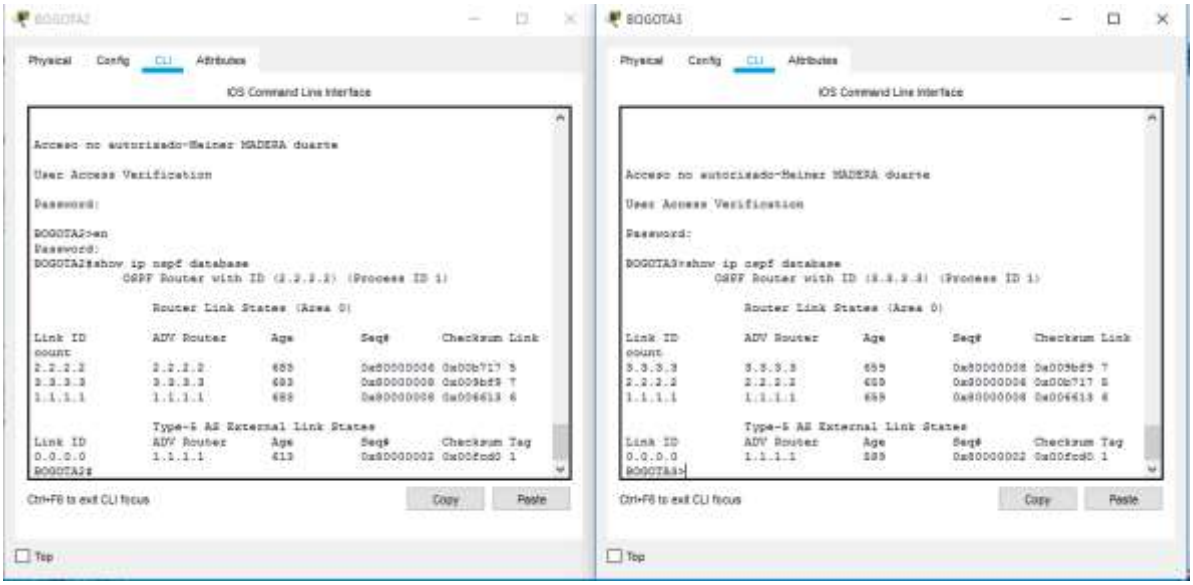

Figura 38. Base de datos de OSPF BOGOTA2 y BOGOTA3

Medellín

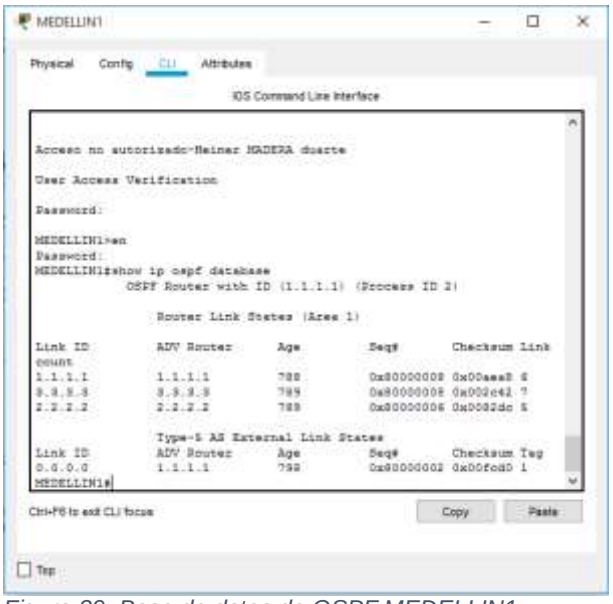

Figura 39. Base de datos de OSPF MEDELLIN1.

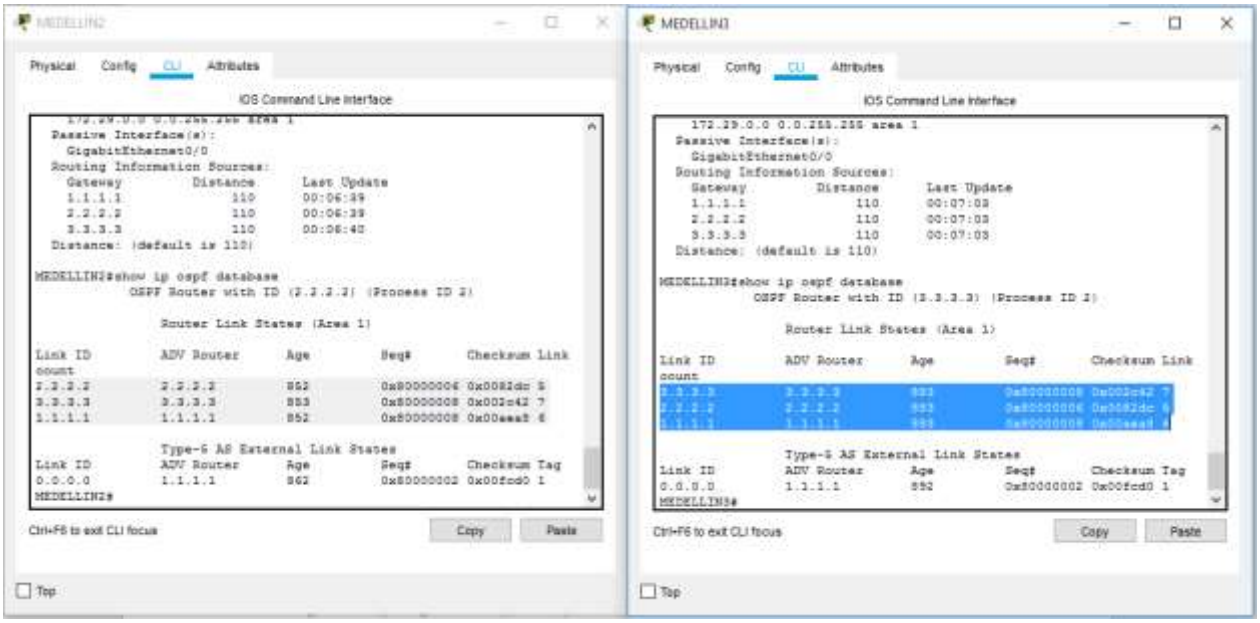

Figura 40. Base de datos de OSPF MEDELLIN2 y MEDELLIN3.

2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Configuración PAP en el ISP

ISP(config)#username MEDELLIN1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco

Configuración PAP en MEDELLIN1

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 password cisco

Verificación pap entre ISP y MEDELLIN1

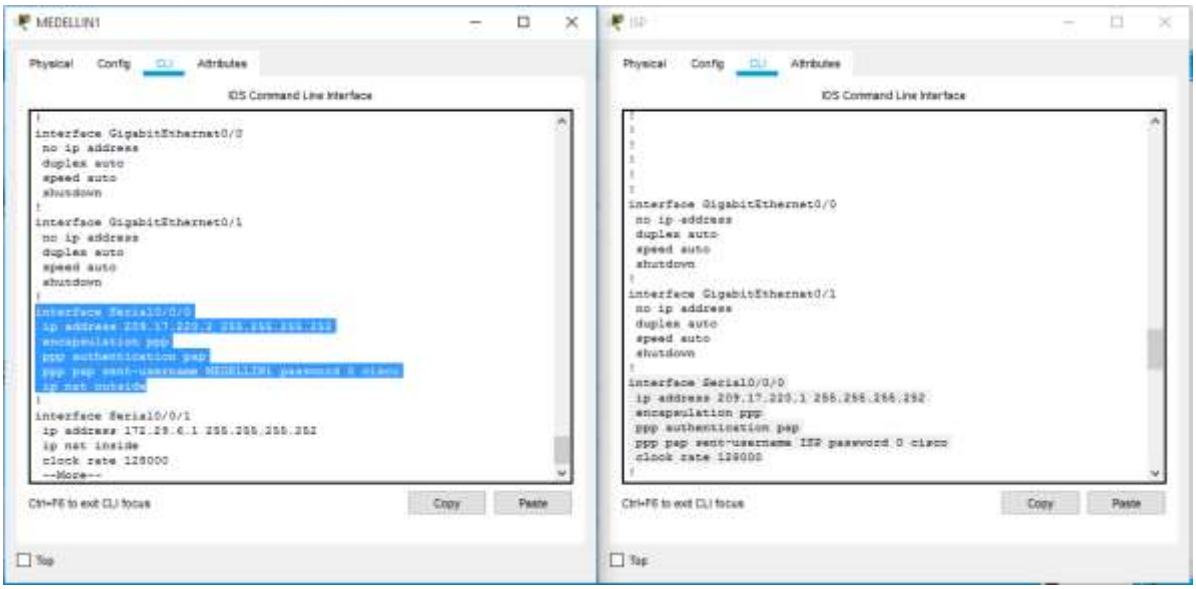

Figura 41. Verificación PAP entre ISP y MEDELLIN1.

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

Configuración CHAP ISP

ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#
ISP(config-if)#ppp authentication chap
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Configuración CHAP BOGOTA1

BOGOTA1>en
BOGOTA1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#username ISP password cisco
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
BOGOTA1(config-if)#ppp authentication chap

Nota: Se debe guardar la configuración y reiniciar los routers ISP, MEDELLIN1 Y

BOGOTA1

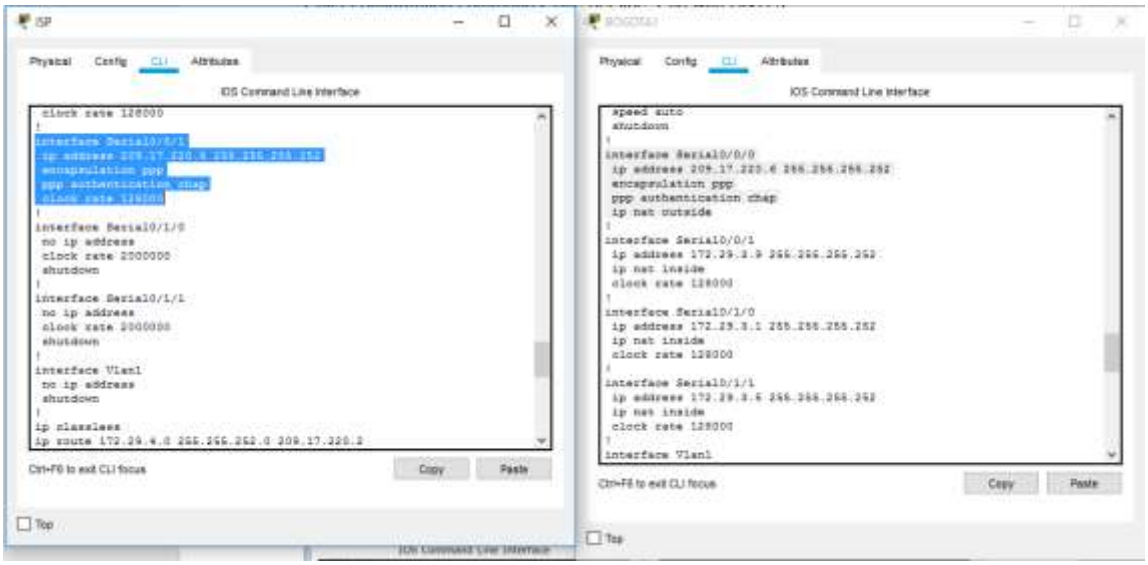

Figura 42. Verificación CHAP entre ISP y BOGOTA1.

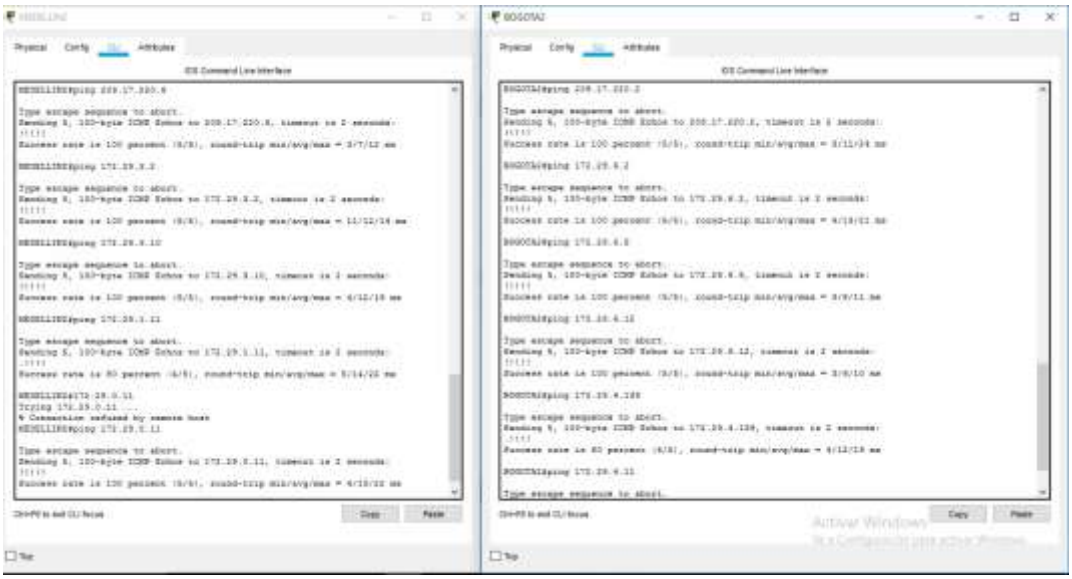

Figura 43. Ping de extremo a extremo (MEDELLIN2 Y BOGOTA2).

2.6 Parte 6: Configuración de PAT.

a. **En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1**.

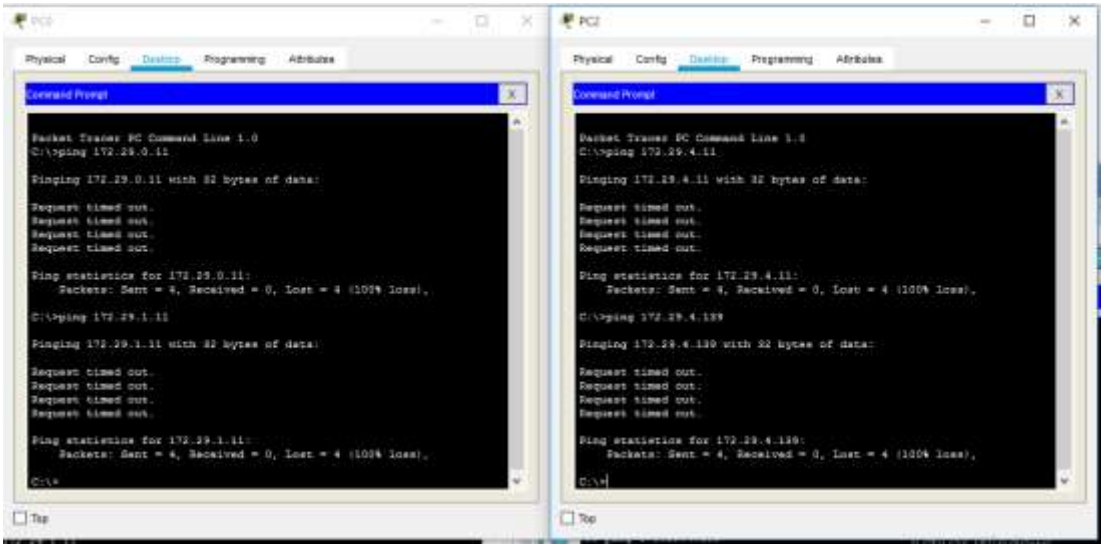

Figura 44. Ping de extremo a extremo (No funciona).

b. **Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto**.

```
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#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
```

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 inside source list 1 interface s0/0/0 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
```

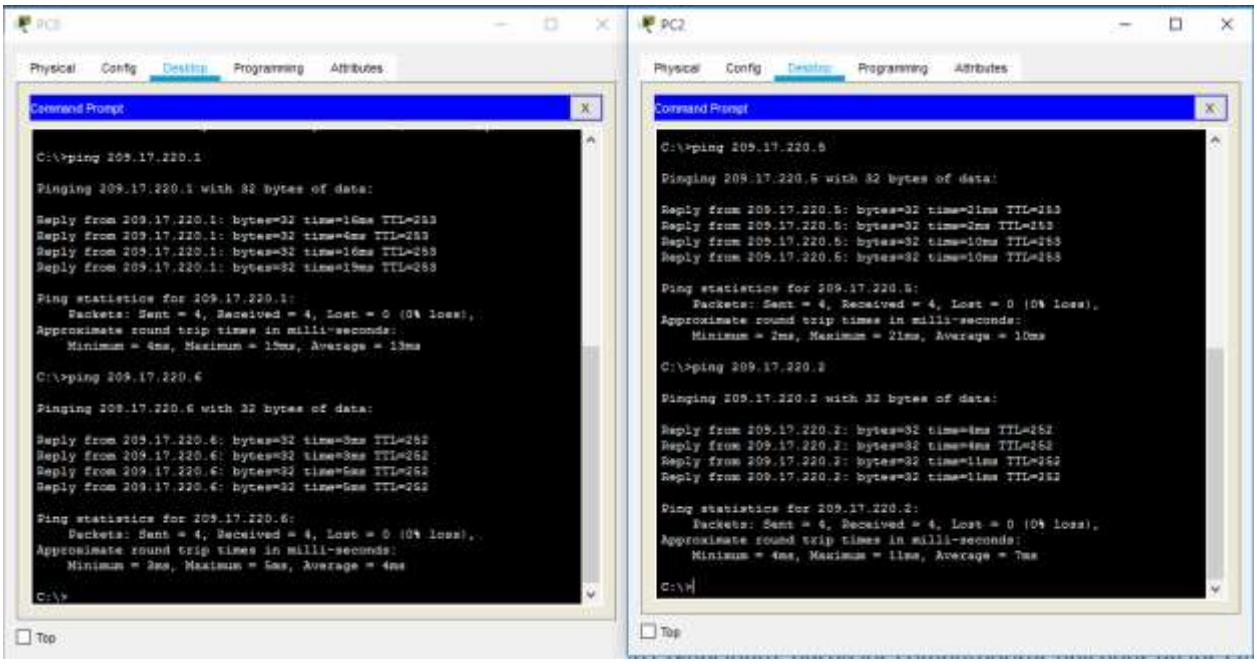

Figura 45. Ping a ISP, Medellin1 y Bogota1 (Funciona), desde los computadores ubicadas en las LAN de Medellín y Bogotá.

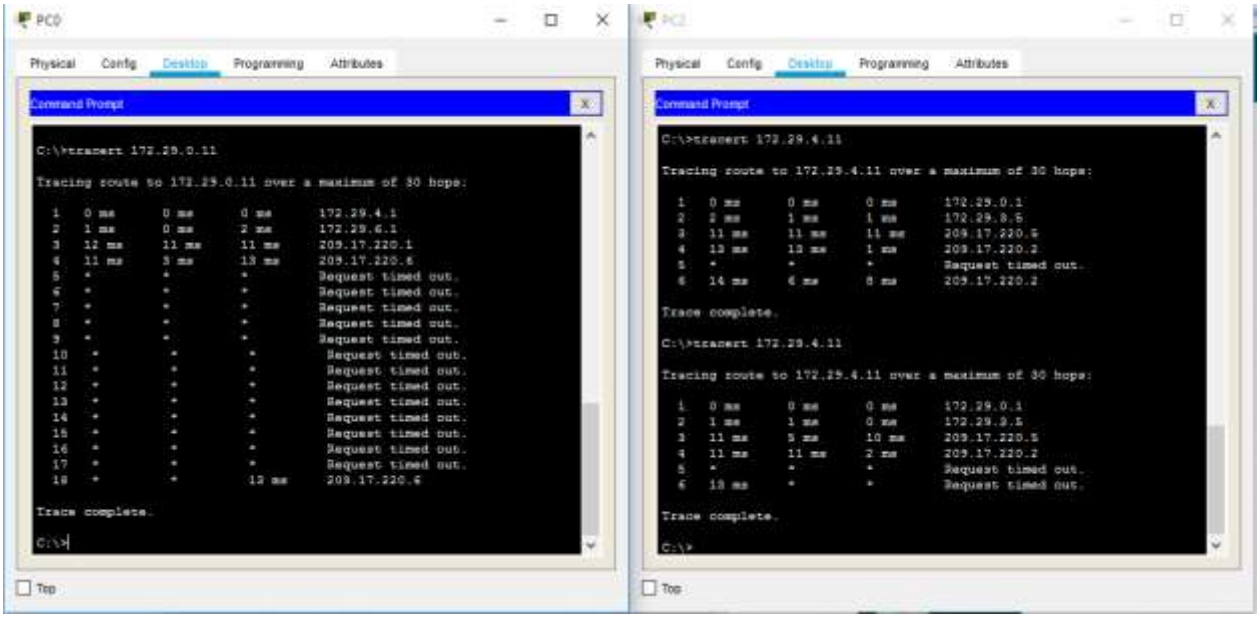

Figura 46.Verificación de la ruta de destino de PC0 y PC2 hasta el otro extremo a través del comando tracert.

Resultados: el PCO ubicado en una de las subredes de Medellín no puede hacer ping más allá de la dirección 209.17.220.6 que corresponde al router BOGOTA1, esto se debe a la configuración de NAT.

2.7 Parte 7: Configuración del servicio DHCP.

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

```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138
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 2.2.2.2
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 2.2.2.2
```

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

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
```

Verificación DHCP MEDELLIN2 y MEDELLIN3

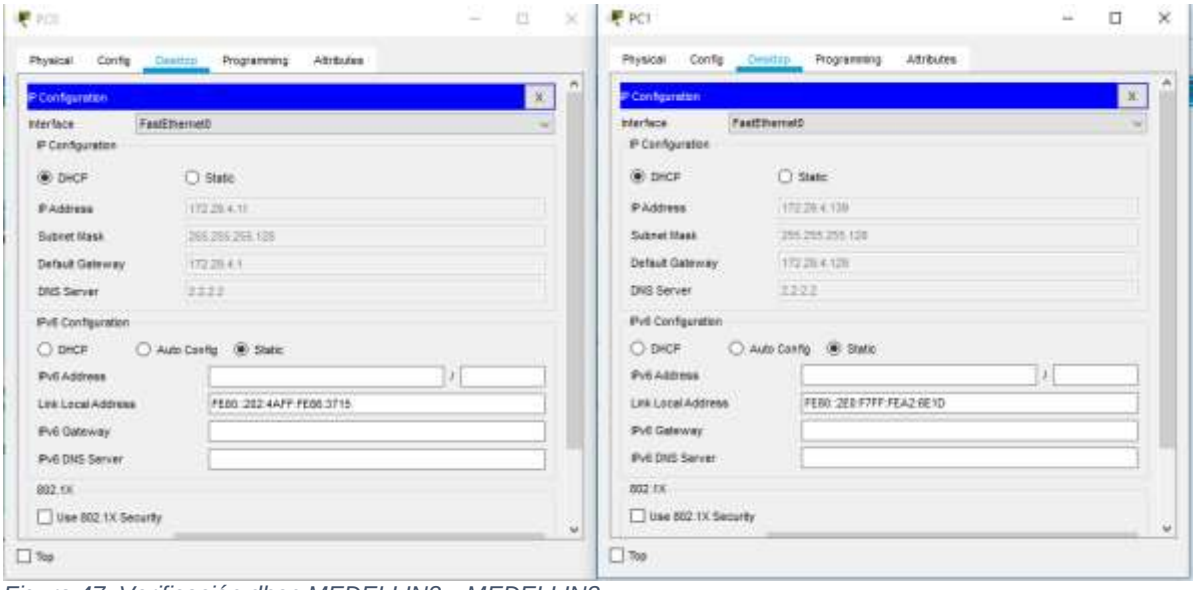

Figura 47. Verificación dhcp MEDELLIN2 y MEDELLIN3.

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

Router BOGOTA2

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
BOGOTA2(config)#ip dhcp pool BOG2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 2.2.2.2
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#ip dhcp pool BOG3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 2.2.2.2
```

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

Router BOGOTA3

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

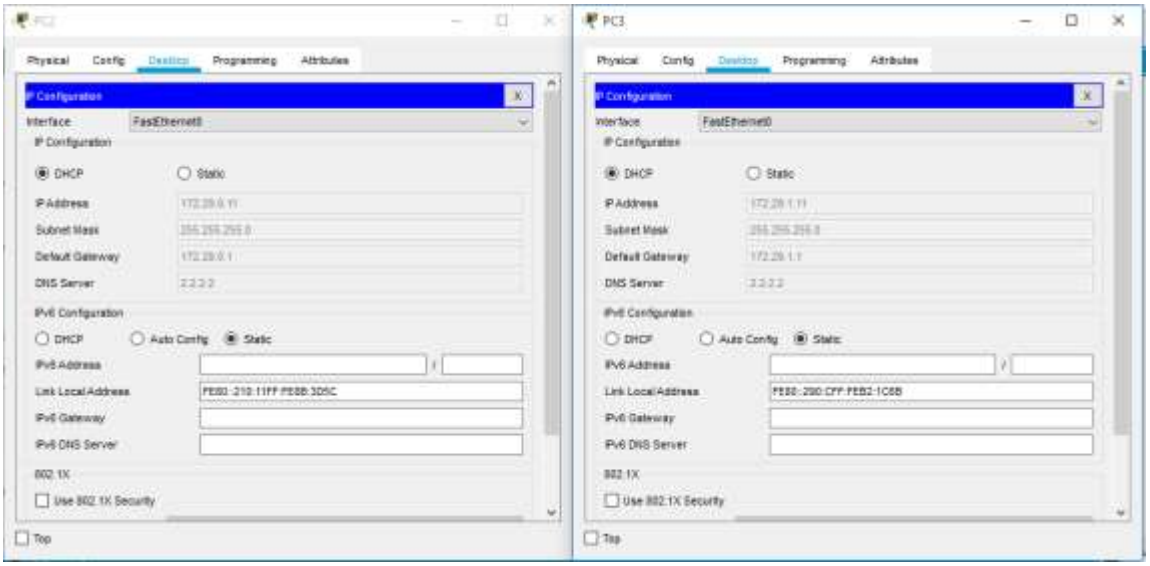

Figura 48. Verificación del servicio dhcp BOGOTA2 y BOGOTA3

CONCLUSIONES

Al configurar la autenticación CHAP Y PAP se presentaron algunos problemas de conexión entre las subredes del escenario 2. Para solucionar lo anterior se guardó la configuración y se reiniciaron los routers ISP, MEDELLIN1 y BOGOTA1.

PAT y NAT se utilizan para solucionar el problema de agotamiento de direcciones ipv4, a través de la traducción de direcciones LAN que no son globalmente únicas a un espacio de direcciones global que pueda conectarse a la WAN.

PAT es muy utilizada en los servicios de internet de los hogares ya que usa una dirección IP única para muchas direcciones locales, mediante la utilización de diversos puertos.

OSPFv2 y RIPv2 son protocolos de enrutamiento dinámico que agilizan los procesos de administración de las redes.

RIP2 realiza sumarización automática en los routers de borde, mientras que en OSPFv2 no es necesario.

OSPFv2 es muy utilizado en la actualidad debido a su rápida convergencia.

Al Configurar interfaces pasivas en los puertos que no necesitan la propagación de protocolos de enrutamiento, evita actualizaciones innecesarias que implican desperdicio de ancho de banda, desperdicio de recursos y riesgos en la seguridad de la red.

Los comandos ip http server y ip http authentication local no están soportados por Packet Tracer, por esta razón no se pudo simular en la computadora de Internet el navegador para acceder al servidor web (209.165.200.237)**.**

BIBLIOGRAFÍA

AbaNet. Glosario de términos. {En línea}. {30 junio de 2020} disponible en: (http://www.abanet.net/glosario.html)

Ariganello, Ernesto. (2016). REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 4ª edición actualizada. Grupo Editorial RA-MA. {En línea}. {30 junio de 2020}. Disponible en: (https://books.google.com.co/books?hl=en&lr=&id=tpBFDwAAQBAJ&oi=fnd&pg=PT7&dq=redes+y+cisco&ots=k5T0x7_M1O&sig=2Y2r0L57mQs-Q3rU1VhstqkAF2s&redir_esc=y#v=onepage&q=redes%20y%20cisco&f=false)

CISCO. Cisco.com Worldwide {En línea}. {21 mayo de 2020}. Disponible en: (https://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_network_assistant/version5_0/quick/guide/Spanish/gsg_esp/cnapref.html)

CISCO. Conceptos sobre tecnología de redes {En línea}. {30 junio de 2020} disponible en: (https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdfs/smb-redes-mx.pdf)

Cruz Domínguez José Martín, Mora Cárdenas Gloria Evila], Beatriz Sauza Avila, Pérez Castañeda Suly Sendy, Cruz Ramírez Dorie. Seguridad en redes LAN implementando VLAN {En línea}. {30 Junio de 2020} disponible en: (https://repository.uaeh.edu.mx/revistas/index.php/sahagun/article/download/2355/2357?inline=1)

MARION, Luis. [mariontechacademy]. (2013, Noviembre 11). CS071 21.04 OSPF - Ruta Acceso a Internet en Packet Tracer [Archivo de video].Disponible en: (https://www.youtube.com/watch?v=vQROsYyB89Q&t=4838s)

Matturro, Gerardo (2007). Introducción a la configuración de routers cisco. {En línea}. {30 junio de 2020}. Recuperado de:(https://www. ort. edu. uy/fi/pdf/configuracionroutersciscomatturro. Pdf)

SOLUTECSA. Glosario de Internet e informática. {En línea}. {30 junio de 2020} disponible en: (https://www.internetglosario.com/450/Protocolo.html)

Archivos de la actividad

Escenario1

https://drive.google.com/file/d/1YwLQvuKnv7eVE5Mlv_JFeaj3L-FxMpMw/view?usp=sharing

Escenario2

https://drive.google.com/file/d/1c6-30SA48aJlQ_x3bnoe4f_UEPz3ZYIk/view?usp=sharing