DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI-203092_21)

JAIME ALBERTO BECERRA PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES

DUITAMA, BOYACA

2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI-203092_21)

JAIME ALBERTO BECERRA PÉREZ

Diplomado de opción de grado presentado para optar el título de

INGENIERO DE TELECOMUNICACIONES

Presentado a:

MSc. Diego Edison Ramírez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES

DUITAMA, BOYACA

2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Duitama 28 de julio de 2020 (29, 07, 2020)

Dedico este trabajo primordialmente a Dios, ya que es gracias a él que logre alcanzar este sueño y a mi querida familia que me han acompañado y apoyado en este camino e impulsado para que triunfe cada día más.

AGRADECIMIENTOS

Quiero agradecerle principalmente a Dios por bendecirme todos los días y darme una familia que siempre me ha apoyado incondicionalmente en mis sueños.

Agradecerle a la Universidad Nacional Abierta y a Distancia, a sus docentes en especial al profesor Diego Edison Ramírez por haber compartido sus conocimientos a lo largo de mi formación como profesional en este diplomado.

Agradecerles a todas las personas que me brindaron su apoyo para poder seguir adelante con este sueño.

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

ACL: Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI. [1]

DHCP: Reduce en gran medida los errores que se producen cuando las direcciones IP se asignan de forma manual, y puede estirar las direcciones IP al limitar el tiempo que un dispositivo puede mantener una dirección IP individual. DHCP está disponible tanto para IPv4 (DHCPv4) como para IPv6 (DHCPv6). En esta sección, se explora la funcionalidad, y características de DHCPv4. [2]

NAT ESTATICA: Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. [3]

NAT DINAMICA: El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública. Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando. [4]

NTP: Network Time Protocol, es un protocolo diseñado para sincronizar los relojes de las estaciones de trabajo a través de la red. La versión 3 de este protocolo es un Internet Draft Standard, formalizado en la RFC 1305. El protocolo NTP versión 4 es una importante revisión del estandard mencionado, y se encuentra en desarrollo, pero aún no ha sido formalizado en una RFC. Una versión simple de NTP (SNTP) versión 4 se describe en la RFC 2030. [5]

OSPF: Open Shortest Path First (OSPF), camino más corto primero, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstra enlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo. [6]

PPP: Protocolo punto a punto (PPP) (en inglés Point-to-Point Protocol), es un protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entre medias de ambos. Está estandarizado en el documento RFC 1661. Puede proporcionar autenticación, cifrado de la transmisión1 y compresión. [7]

PAT: La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos, ya que es el utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. Además del ahorro económico, también se ahorran direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública. [8]

RIP: (Routing information protocolo, protocolo de información de encaminamiento) RIP es un protocolo de encaminamiento interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a internet como infovia, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos. [9]

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local. [10]

RESUMEN

La sistemática empleada para el desarrollo de la prueba de habilidades practicas es el análisis, la indagación y la lectura crítica relacionada con la comprensión y solución de dificultades relacionadas con varios aspectos de Networking**, c**on el fin de adquirir el conocimiento y las destrezas mediante el software cisco Packet Tracer.

Palabras Claves: CISCO, Habilidades, Networking, Redes,

1. INTRODUCCIÓN

En este informe se da solución a dos escenarios, los cuales están basados en inconvenientes habituales en las organizaciones, asimismo se desarrollarán con el fin de poner en práctica y demostrar lo aprendido durante el curso diplomado de profundización en cisco LAN, WAN.

En el primer escenario se realizarán las configuraciones básicas de los Router y de los switch, también se configurarán las interfaces, las VLAN y se utilizará el protocolo de routing dinámico RIPv2, se implementará el protocolo DHCP y NAT para ipv4, al mismo tiempo de configurar y verificar las listas de control de acceso (ACL).

El segundo escenario, es acerca de una empresa que posee sucursales distribuidas en las ciudades de Bogotá y Medellín, y para estas se considera el uso de OSPF como protocolo de enrutamiento, ya que se tendran rutas por defecto redistribuidas; asimismo, se habilitara el encapsulamiento PPP y su autenticación, ademas del servicio DHCP a su propia red LAN y a los routers de cada ciudad, tambien se debera configurar PPP en los enlaces hacia el ISP, con autenticación y se habilitara NAT de sobrecarga en los routers Bogota1 y medellin1.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Configurar dos redes LAN/WAN por medio de protocolos que proporcionen conectividad y seguridad en la red.

2.2 OBJETIVOS ESPECIFICOS

Investigar sobre los fundamentos de los protocolos de redes LAN/WAN.

Realizar e implementar las configuraciones de las redes por medio del software cisco packet tracer.

Configurar cada red con conectividad IPv4 e IPv6 y con los protocolos de redes RIP, VLAN, OSPFv2, DHCP, NAT y ACL; según cada topología de las redes.

Verificar los resultados de las configuraciones y de conectividad entre los dispositivos.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Se administran dos redes LAN/WAN a partir de una serie de configuraciones que permitan fortalecer los conocimientos adquiridos durante el transcurso del diplomado.

3.2 JUSTIFICACIÓN

Este informe se realiza bajo la necesidad de aplicar los conocimientos en dar soluciones a las redes de comunicaciones LAN/WAN, con la implementación de estas herramientas, generando una mejor aplicación de la teoría aprendida para mejorar cada vez más la administración de redes.

4. MARCO TEÓRICO

4.1 RED DE COMUNICACIONES

Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/Slave-). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc.). La información se puede transmitir de forma analógica, digital o mixta, pero en cualquier caso las conversiones, si las hay, siempre se realizan de forma transparente al usuario, el cual maneja la información de forma analógica exclusivamente.

Las redes más habituales son las de ordenadores, las de teléfono, las de transmisión de audio (sistemas de megafonía o radio ambiental) y las de transmisión de vídeo (televisión o vídeo vigilancia). [11]

4.2 CAPACIDAD DE TRANSMISIÓN

La capacidad de transmisión indica el número de bits por segundo que se pueden transmitir a través de una conexión. A menudo se llama erróneamente velocidad de transmisión (que depende de la capacidad y de otros factores) o ancho de banda (que es la amplitud de onda utilizable). En este texto usaremos ancho de banda como sinónimo de capacidad de transmisión excepto cuando se hable explícitamente de frecuencias de onda. [11]

4.3 ENCAMINAMIENTO (ENRUTAMIENTO O ROUTING)

Cada nodo intermedio de una comunicación debe conocer dónde ha de enviar el paquete que ha recibido. En el caso de los circuitos (conmutados o virtuales) solo se toma la decisión en el inicio de la conexión. En el caso de paquetes conmutados (datagramas) se toma la decisión con cada paquete. Este proceso de decisión se denomina encaminamiento (routing).

La solución más sencilla pero ineficaz es enviar el paquete por todos los interfaces menos por el que llegó (inundación). Es el funcionamiento de los concentradores. Este sistema no se considera un protocolo de encaminamiento. Para

encaminadores (router) sencillos se puede utilizar configuraciones estáticas de encaminamiento.

Los encaminadores más modernos permiten utilizar auténticos protocolos de encaminamiento dinámico que sirven para intercambiar información entre encaminadores y adaptarse a situaciones cambiantes de tráfico basándose en:

- Capacidad del enlace.
- Tráfico medio.
- Retardo.
- Fiabilidad.

Las técnicas básicas son:

- Vector de distancia: Cada encaminador mantiene una tabla con las distancias mínimas hacia cada posible destino y el interfaz de salida. Les pasa esta información a todos sus vecinos. Tiene el problema de la cuenta a infinito.
- Estado de enlace. Identifica a sus vecinos y su coste y manda esa información a todos los encaminadores de la red. Con esa información se calcula el mapa de la red.

Debido a que los protocolos de encaminamiento no son escalables se utiliza encaminamiento jerárquico. Esto simplifica el intercambio de información, aunque puede no aprovechar todos los caminos mínimos. [11]

4.4 TIPOS DE RED

Las redes se pueden clasificar de diferentes maneras. Las principales clasificaciones son:

- Por su extensión: Redes de área personal (PAN), local (LAN), extensa (WAN)... (ver cuadro inferior).
- Por su topología: Estrella, bus, anillo, malla, mixta.
- Por su conexión física: se clasifican en redes punto a punto (unicast) y redes multipunto o de difusión (broadcast).
- Por su técnica de transmisión de datos: líneas dedicadas, circuito conmutado o paquetes conmutados.
- Por su uso: se clasifican en redes privadas o corporativas y redes públicas.

4.5 PROTOCOLOS DE RED

Un protocolo de red designa el conjunto de reglas que rigen el intercambio de información a través de una red de computadoras.

Este protocolo funciona de la siguiente forma, cuando se transfiere información de un ordenador a otro, por ejemplo, mensajes de correo electrónico o cualquier otro tipo de datos esta no es transmitida de una sola vez, sino que se divide en pequeñas partes. [12]

Lista de protocolos según el nivel de red del modelo OSI:

- ARP (Address Resolution Protocol): protocolo de resolución de direcciones.
- BGP (Border Gateway Protocol: protocolo de frontera de entrada).
- EGP (Exterior Gateway Protocol: protocolo de entrada exterior).
- ICMP (Internet Control Message Protocol: protocolo de acceso a la red).
- IGMP: protocolo de la gerencia del grupo de Internet.
- IPv4: protocolo de internet versión 4.
- IPv6: protocolo de internet versión 6.
- IPX: red interna del intercambio del paquete.
- IS-IS: sistema intermedio a sistema intermedio.
- MPLS: multiprotocolo de conmutaciòn de etiquetas.
- OSPF: abrir la trayectoria más corta primero.
- RARP: protocolo de resoluciòn de direcciones inverso. [12]

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Los materiales que usaron en el desarrollo del trabajo son:

- Guías y documentación CCNA I – II.
- Cisco Packet Tracer 7.3.0.
- Equipo de cómputo básico con sistema operativo Windows 10 Home.

5.2 METODOLOGÍA

- Las técnicas o parámetros usados en el desarrollo del trabajo son:
- Configuración de direccionamiento IPv4 y IPv6
- Realización de las respectivas tablas de enrutamiento.
- Configuración del protocolo RIP, OSPF, DHCP y VTP.
- Creación de las direcciones de red dinámicas y estáticas NAT.
- Habilitación del encapsulamiento PPP y su autenticación
- Asignación de listas de acceso ACL
- Traducción de las direcciones IP sobre NAT-PAT.
- Verificación de la conectividad.

6. DESARROLLO DEL PRIMER ESCENARIO

En esta práctica 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.

6.1 TOPOLOGÍA DEL PRIMER ESCENARIO

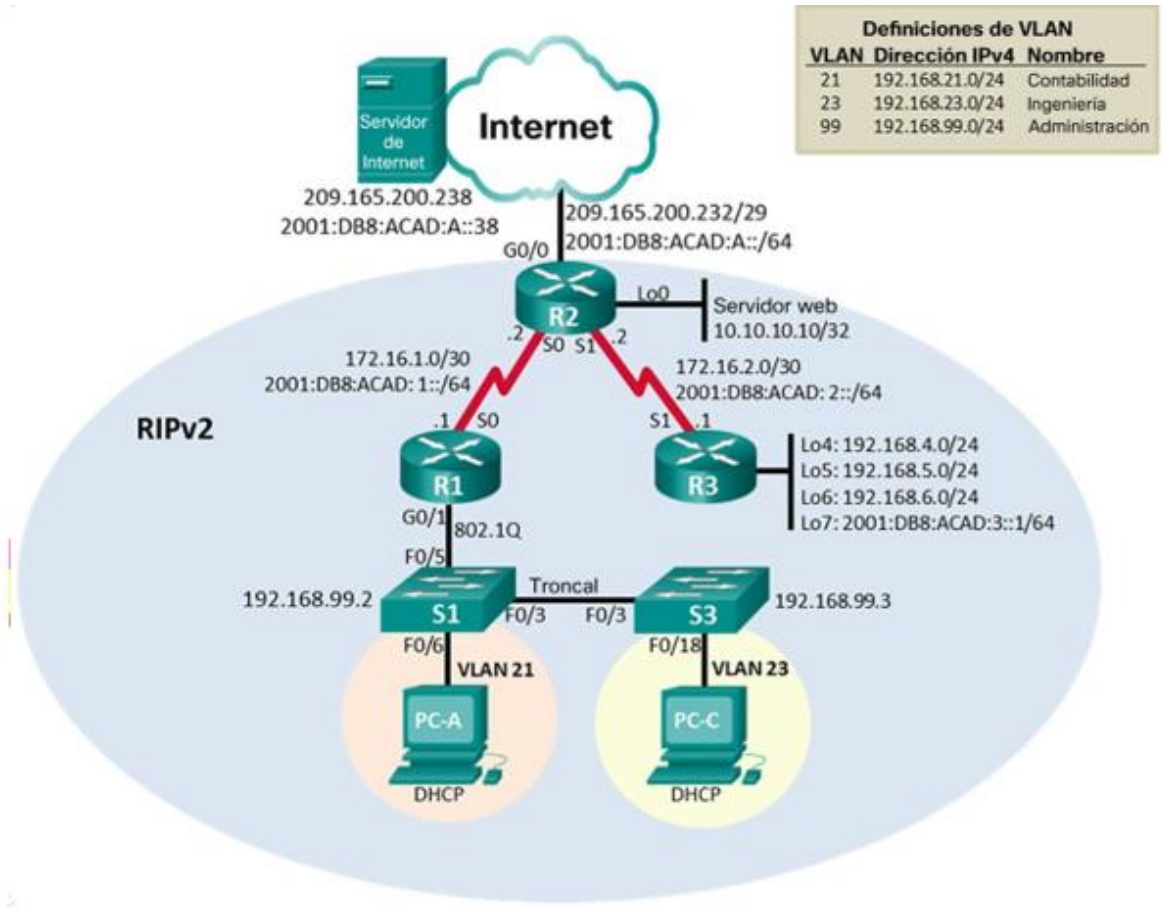

Ilustración 1 Topología de la red del primer escenario

6.2 PARTE 1: ARMAR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS.

En esta primera parte, se establece la topología de la red y se borra cualquier configuración anterior que tengan los dispositivos.

Paso 1: Realizar el cableado de red tal como se muestra en la topología

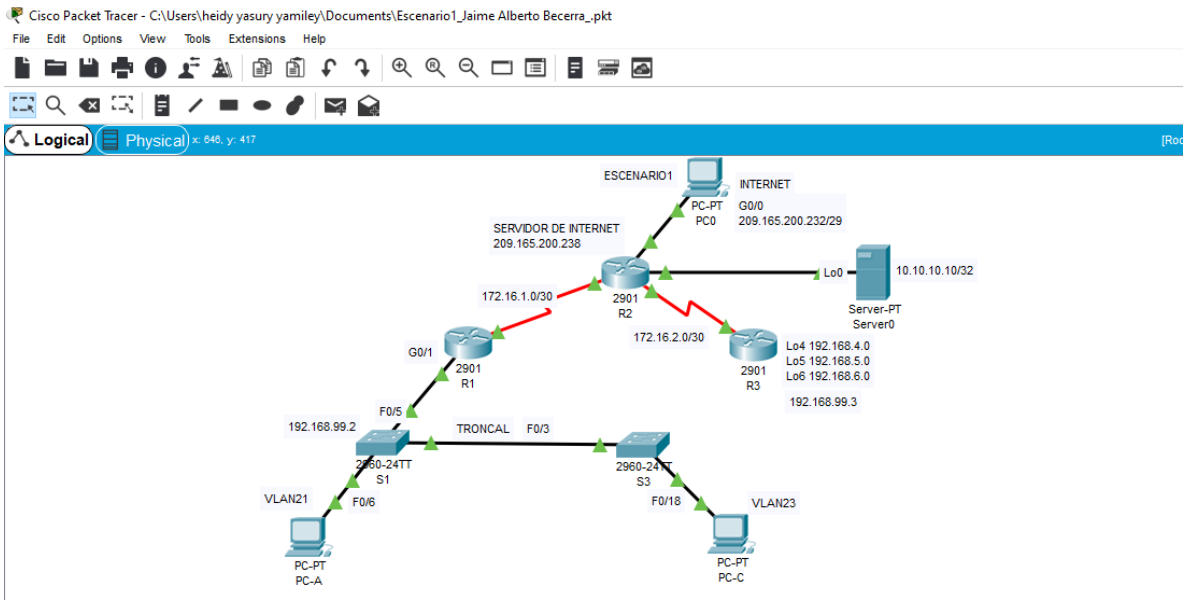

Ilustración 2 Topología de la red del primer escenario en Cisco Packet Tracer

Paso 2: Inicializar y vuelva a cargar los router y los switch

Por medio del comando erase startup-config eliminamos los archivos y con el comando reload volverá a cargar los dispositivos.

TAREA	**COMANDO DE IOS**
Eliminar el archivo startup-config de todos los routers	**Router#Erase startup-config** **Switch#Erase startup-config**
Volver a cargar todos los routers	**Router#Reload**

	Switch#Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	**Router#Erase startup-config** **Router#Delete vlan.dat** **Switch#Erase startup-config** **Switch#Delete vlan.dat**
Volver a cargar ambos switches	**Router# Reload** **Switch#Reload**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	**Router#Show flash** **Switch#Reload**

Tabla 1 Indicaciones para la verificación inicial de los dispositivos del primer escenario

Por medio de los siguientes comandos.se realizan las configuraciones de formateo y reinicio tanto en los Routers como en los Switch.

- Router R1

Route>enable

Router#erase startup-config

Router#reload

- Router R2

Route>enable

Router#erase startup-config

Router#reload

- Router R3

Route>enable

Router#erase startup-config

Router#reload

- Switch S1

Switch>enable

Switch#erase startup-config

Switch#delete vlan.dat

Switch#reload

Switch#show flash

- Switch S3

Switch>enable

Switch#erase startup-config

Switch#delete vlan.dat

Switch#reload

Switch#show flash

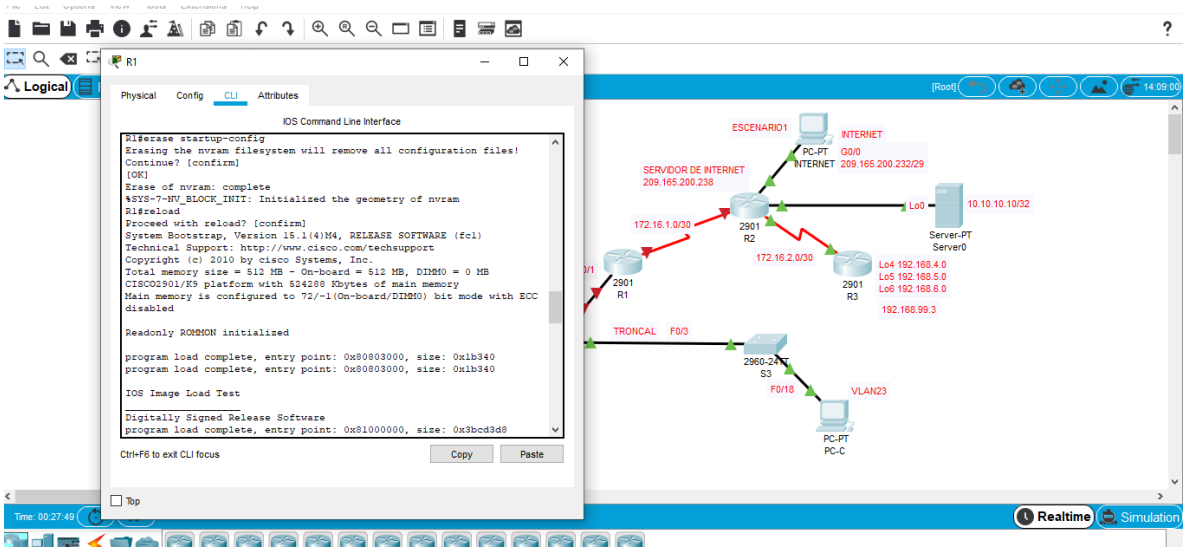

Ilustración 3 Configuraciones de Inicio en el Router R1

6.3 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: Configurar la computadora de Internet

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Dirección IPv4	**209.165.200.238**
Máscara de subred para IPv4	**255.255.255.248**
Gateway predeterminado	**209.165.200.225**
Dirección IPv6/subred	**2001:DB8:ACAD:A::38/64**
Gateway predeterminado IPv6	**2001:DB8:ACAD:2::1**

Tabla 2 Indicaciones para configurar la computadora red internet

Paso 2: Configurar R1

Por medio de los siguientes comandos se realizan las configuraciones basicas de los dispositivos que nos piden en la segunda parte del escenario.

Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#enable secret cisco
R1(config)#line console 0
R1(config)#password cisco
R1(config)#login
R1(config)#line vty 0 4
R1(config)#password cisco
R1(config)#login
R1(config)#service password-encryption
R1(config)#no ip domain-lookup
R1(config)#enable secret class

R1(config)#banner motd $Sin autorizacion el acceso es prohibido$

R1(config)#interface s0/3/0

R1(config-if)#description connection to R2

R1(config-if)#ip address 172.16.1.1 255.255.255.252

R1(config-if)#clock rate 12800

R1(config-if)#no shutdown

R1(config)#interface s0/3/0

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

R1(config-if)#no shutdown

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/3/0

R1(config)#ipv6 route ::/0 s0/3/0

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Desactivar la búsqueda DNS	**R1(config)#no ip domain-lookup**
Nombre del router	**Router(config)#hostname R1**
Contraseña de exec privilegiado cifrada	**R1(config)#enable secret class**
Contraseña de acceso a la consola	**R1(config)#password cisco**
Contraseña de acceso Telnet	**R1(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**R1(config)#service password-encryption**
Mensaje MOTD	**R1(config)#banner motd $Se prohibe el acceso no autorizado$**
Interfaz S0/0/0	**R1(config)#interface s0/3/0** **R1(config-if)#ip address 172.16.1.1 255.255.255.252** **R1(config-if)#clock rate 128000** **R1(config-if)#no shutdown** **R1(config)#interface s0/3/0** **R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64**

	R1(config-if)#no shutdown
Rutas predeterminadas	**R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/3/0** **R1(config)#ipv6 route ::/0 serial s0/3/0**

Tabla 3 Indicaciones para configurar a R1

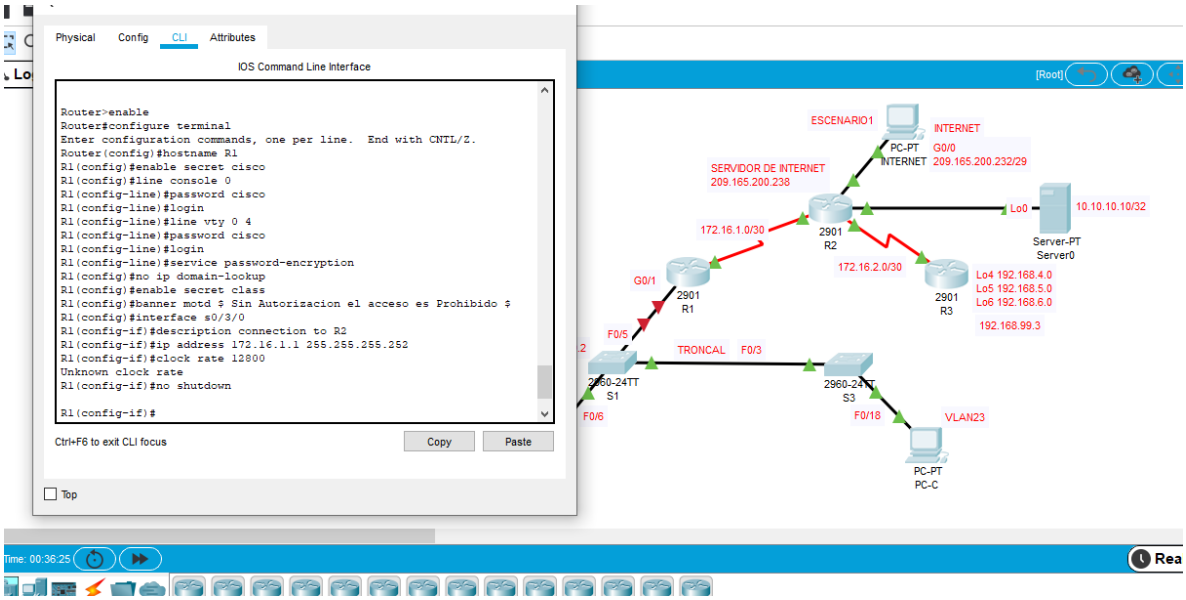

Ilustración 4 Configuración básica del Router R1

Paso 3: Configurar R2

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

Router>enable

Router#configure terminal

Router(config)#hostname R2

R2(config)#no ip domain-lookup

R2(config)#service password-encryption

R2(config)#enable secret class

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

R2(config)#enable secret cisco

R2(config)#line console 0

```
R2(config)#password cisco
R2(config)#login
R2(config)#line vty 0 4
R2(config)#password cisco
R2(config)#login
R2(config)#interface s0/3/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config)#interface s0/3/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown
R2(config)#interface s0/3/1
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config)#interface s0/3/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#no shutdown
R2(config)#interface g0/0
R2(config-if)#ip address 209.165.200.232 255.255.255.240
R2(config-if)#no shutdown
R2(config)#interface g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::/64
R2(config-if)#no shutdown
R2(config)#interface loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#no shutdown
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)#ipv6 route ::/0 g0/0
```

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	**R2(config)#no ip domain-lookup**
Nombre del router	**Router(config)#hostname R2**
Contraseña de exec privilegiado cifrada	**R2(config)#enable secret class**
Contraseña de acceso a la consola	**R2(config)#password cisco**
Contraseña de acceso Telnet	**R2(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**R2(config)#service password-encryption**
Habilitar el servidor HTTP	
Mensaje MOTD	**R2(config)#banner motd $Se prohibe el acceso no autorizado$**
Interfaz S0/0/0	**R2(config)#interface s0/3/0** **R2(config-if)#ip address 172.16.1.2 255.255.255.252** **R2(config-if)#clock rate 128000** **R2(config-if)#no shutdown** **R2(config)#interface s0/3/0** **R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64** **R2(config-if)#no shutdown**
Interfaz S0/0/1	**R2(config)#interface s0/3/1** **R2(config-if)#ip address 172.16.2.2 255.255.255.252** **R2(config-if)#clock rate 12800** **R2(config-if)#no shutdown** **R2(config)#interface s0/3/1** **R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64** **R2(config-if)#no shutdown**

Interfaz G0/0 (simulación de Internet)	**R2(config)#interface s0/3/1** **R2(config-if)#ip address 172.16.2.2 255.255.255.252** **R2(config-if)#clock rate 12800** **R2(config-if)#no shutdown** **R2(config)#interface s0/3/1** **R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64** **R2(config-if)#no shutdown**
Interfaz loopback 0 (servidor web simulado)	**R2(config)#interface loopback 0** **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 route ::/0 g0/0**

Tabla 4 Indicaciones para configurar a R2

Paso 4: Configurar R3

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

Router>enable

Router#configure terminal

Router(config)#hostname R3

R3(config)#no ip domain-lookup

R3(config)#service password-encryption

R3(config)#enable secret class

R3(config)#banner motd $Se prohibe el acceso no autorizado$

R3(config)#enable secret cisco

R3(config)#line console 0

R3(config)#password cisco

R3(config)#login

```
R3(config)#line vty 0 4
R3(config)#password cisco
R3(config)#login
R3(config)#interface s0/3/1
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown
R3(config)#interface s0/3/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no shutdown
R3(config)#interface loopback 4
R3(config-if)#ip address 192.168.4.0 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface loopback 5
R3(config-if)#ip address 192.168.5.0 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface loopback 6
R3(config-if)#ip address 192.168.6.0 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#no shutdown
```

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Desactivar la búsqueda DNS	**R3(config)#no ip domain-lookup**
Nombre del router	**Router(config)#hostname R3**
Contraseña de exec privilegiado cifrada	**R3(config)#enable secret class**

Contraseña de acceso a la consola	**R3(config)#password cisco**
Contraseña de acceso Telnet	**R3(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**R3(config)#service password-encryption**
Mensaje MOTD	**R3(config)#banner motd $Se prohibe el acceso no autorizado$**
Interfaz S0/0/1	**R3(config)#interface s0/3/1** **R3(config-if)#ip address 172.16.2.1 255.255.255.252** **R3(config-if)#clock rate 128000** **R3(config-if)#no shutdown** **R3(config)#interface s0/3/1** **R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64** **R3(config-if)#no shutdown**
Interfaz loopback 4	**R3(config)#interface loopback 4** **R3(config-if)#ip address 192.168.4.0 255.255.255.0** **R3(config-if)#no shutdown**
Interfaz loopback 5	**R3(config)#interface loopback 5** **R3(config-if)#ip address 192.168.5.0 255.255.255.0** **R3(config-if)#no shutdown**
Interfaz loopback 6	**R3(config)#interface loopback 6** **R3(config-if)#ip address 192.168.6.0 255.255.255.0** **R3(config-if)#no shutdown**
Interfaz loopback 7	**R3(config)#interface loopback 7** **R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64** **R3(config-if)#no shutdown**

Tabla 5 Indicaciones para configurar a R3

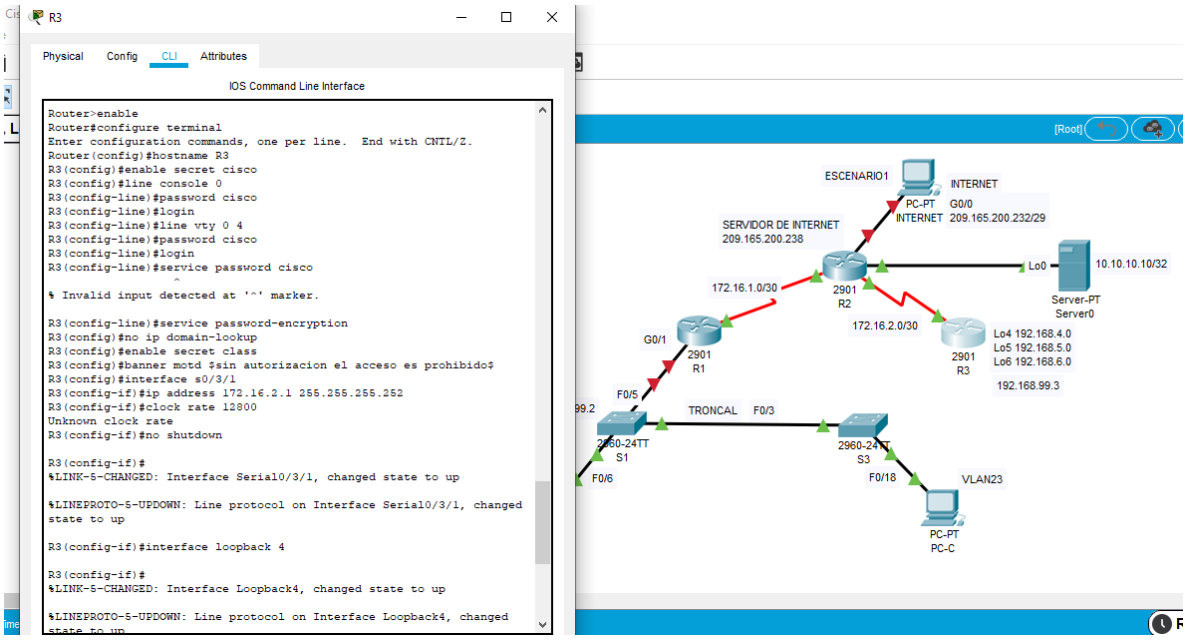

Ilustración 5 Configuración básica del Router R3

Paso 5: Configurar S1

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

Switch>enable

Switch#configure terminal

Switch(config)#hostname S1

S1(config)#no ip domain-lookup

S1(config)#service password-encryption

S1(config)#enable secret class

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

S1(config)#enable secret cisco

S1(config)#line console 0

S1(config)#password cisco

S1(config)#login

S1(config)#line vty 0 15

S1(config)#password cisco

S1(config)#login

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	**S1(config)#no ip domain-lookup**
Nombre del switch	**Switch(config)#hostname S1**
Contraseña de exec privilegiado cifrada	**S1(config)#enable secret class**
Contraseña de acceso a la consola	**S1(config)#password cisco**
Contraseña de acceso Telnet	**S1(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**S1(config)#service password-encryption**
Mensaje MOTD	**S1(config)#banner motd $Se prohibe el acceso no autorizado$**

Tabla 6 Indicaciones para configurar a S1

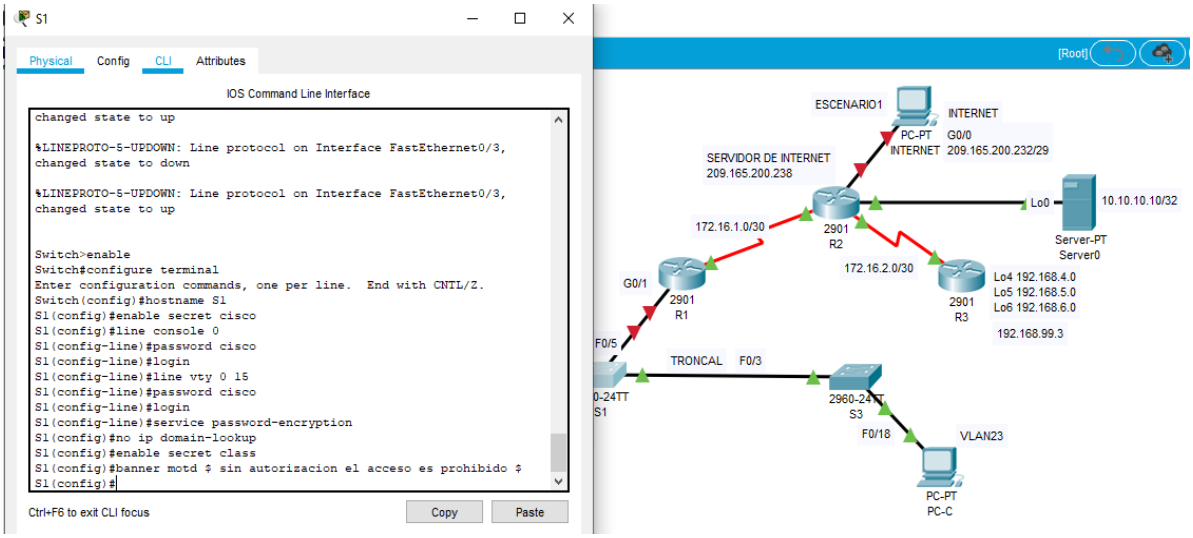

Ilustración 6 Configuración básica del Switch S1

Paso 6: Configurar el S3

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

Switch>enable

Switch#configure terminal

Switch(config)#hostname S3

S3(config)#no ip domain-lookup

S3(config)#service password-encryption

S3(config)#enable secret class

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

S3(config)#enable secret cisco

S3(config)#line console 0

S3(config)#password cisco

S3(config)#login

S3(config)#line vty 0 15

S3(config)#password cisco

S3(config)#login

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Desactivar la búsqueda DNS	**S3(config)#no ip domain-lookup**
Nombre del switch	**Switch(config)#hostname S3**
Contraseña de exec privilegiado cifrada	**S3(config)#enable secret class**
Contraseña de acceso a la consola	**S3(config)#password cisco**
Contraseña de acceso Telnet	**S3(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**S3(config)#service password-encryption**

Mensaje MOTD	**S3(config)#banner motd $Se prohibe el acceso no autorizado$**

Tabla 7 Indicaciones para configurar a S3

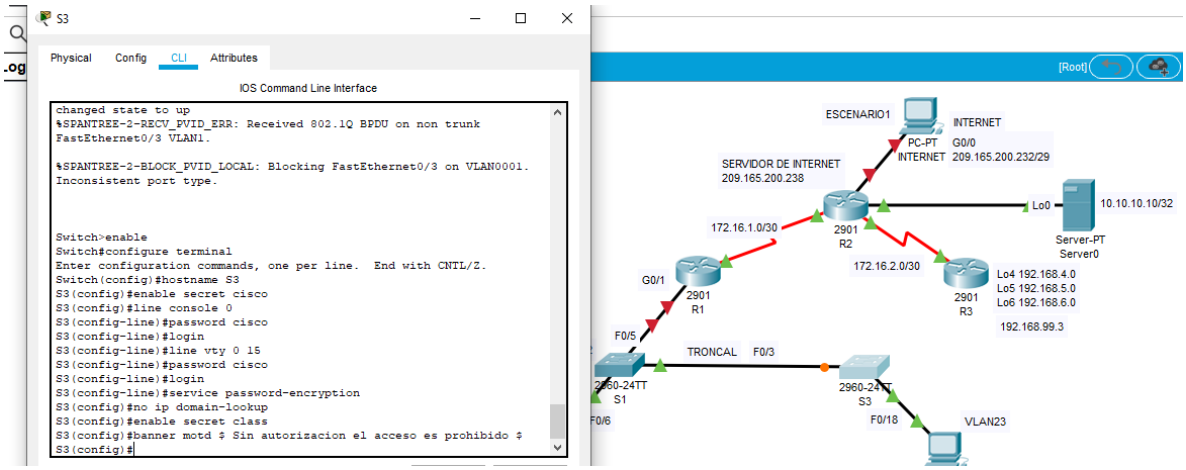

Ilustración 7 Configuración básica del Switch S3

Paso 7: Verificar la conectividad de la red

En este paso vamos a utilizar el comando ping en cada uno de los dispositivos para probar la conectividad entre los dispositivos de red.

DESDE	A	DIRECCIÓN IP	RESULTADOS DE PING
R1	R2, S0/0/0	172.16.1.2	**R1#ping 172.16.1.2** **Success rate is 100 percent(5/5), round-trip min/avg/max = 1/9/38 ms**
R2	R3, S0/0/1	172.16.2.1	**R1#ping 172.16.1.2** **Success rate is 100 percent(5/5) round-trip min/avg/max = 1/2/8 ms**
PC de Internet	Gateway predeterminado	209.165.200.232	**>ping 209.165.200.232** **Reply from 209.165.200.232: bytes=32 time<1ms TTL=255**

Tabla 8 Verificación de conectividad en los routers y en el PC de internet

En las ilustraciones que observaremos a continuación se muestran los comandos tal como se escribirían en la ventana CLI del router y los resultados de conexión obtenidos en los router y el PC de internet.

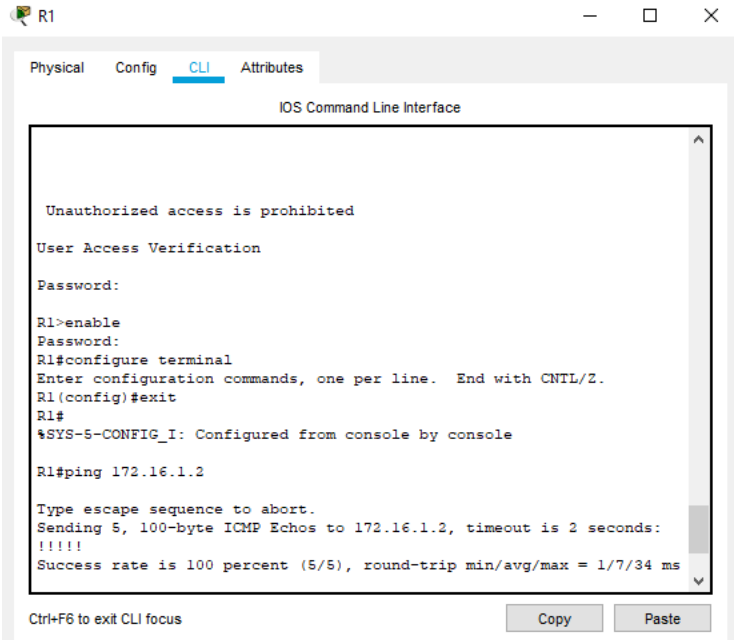

Ilustración 8 Verificación de las configuraciones basicas ping desde R1 a R2

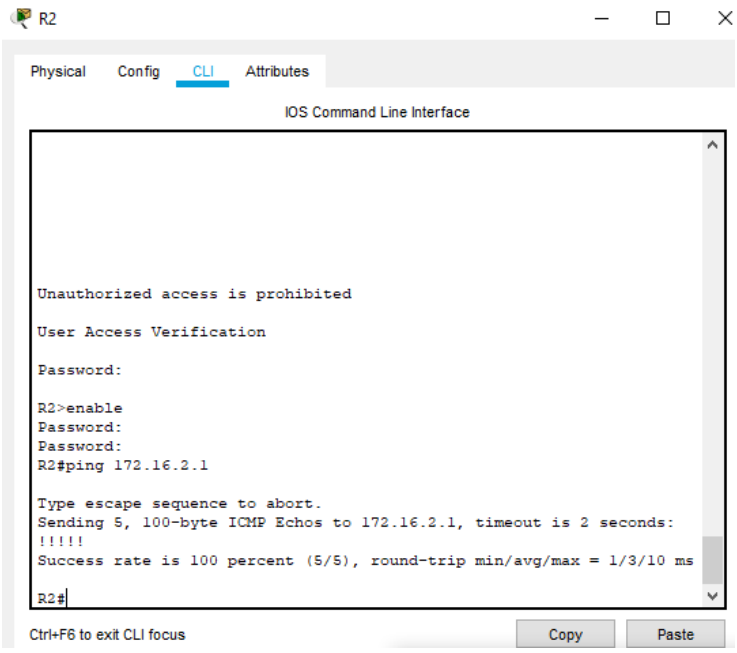

Ilustración 9 Verificación de las configuraciones basicas ping desde R2 a R3

6.4 PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

Paso 1: Configurar S1

```
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
S1(config-vlan)#exit
S1(config-if)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config)#ip default-gateway 192.168.99.1
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#interface fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface fa0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#no shutdown
S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#no shutdown
S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2
```

S1(config-if-range)#shutdown

TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear la base de datos de VLAN	**S1(config)#vlan 21** **S1(config-vlan)#name contabilidad** **S1(config-vlan)#vlan 23** **S1(config-vlan)#name ingenieria** **S1(config-vlan)#vlan 99** **S1(config-vlan)#name administración** **S1(config-vlan)#exit**
Asignar la dirección IP de administración.	**S1(config-if)#interface vlan 99** **S1(config-if)#ip address 192.168.99.2 255.255.255.0** **S1(config-if)#no shutdown**
Asignar el gateway	**S1(config)#ip default-gateway 192.168.99.1**
Forzar el enlace troncal en la interfaz F0/3	**S1(config)#interface fa0/3** **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 1**
Forzar el enlace troncal en la interfaz F0/5	**S1(config-if)#interface fa0/5** **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 1** **S1(config-if)#no shutdown**
Configurar el resto de los puertos como puertos de acceso	**S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S1(config-if-rangen)#switchport mode access**
Asignar F0/6 a la VLAN 21	**S1(config-if)#interface fa0/6** **S1(config-if)#switchport mode access** **S1(config-if)#switchport access vlan 21** **S1(config-if)#no shutdown**
Apagar todos los puertos sin usar	**S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S1(config-if-range)#shutdown**

Tabla 9 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de S1.

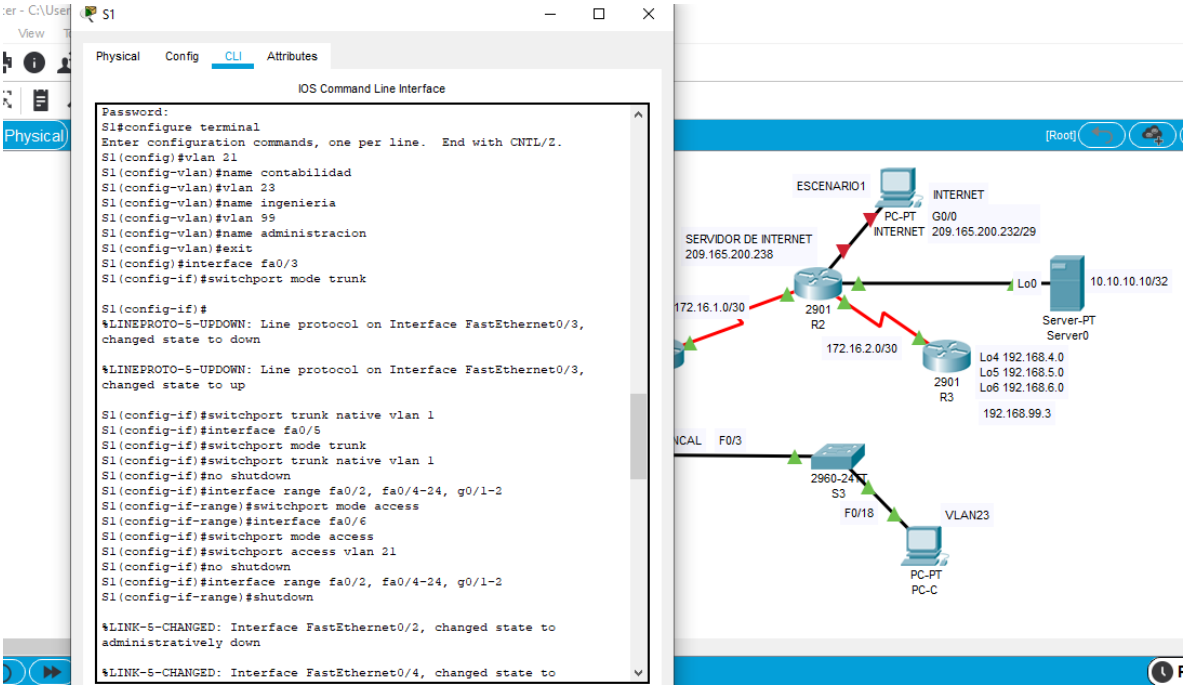

Ilustración 10 Configuración de las vlan en el S1

Paso 2: Configurar el S3

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

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 administración

S3(config-vlan)#exit

S3(config)#interface vlan 99

S3(config-if)#ip address 192.168.99.3 255.255.255.0

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.99.1

S3(config)#interface fa0/3

S3(config-if)#switchport mode trunk

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

S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2

S3(config-if)#switchport mode access

S3(config-if)#interface fa0/18

S3(config-if)#switchport mode access

S3(config-if)#switchport access vlan 23

S3(config-if-range)#no shutdown

S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2

S3(config-if-range)#shutdown

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Crear la base de datos de VLAN	**S3(config)#vlan 21** **S3(config-vlan)#name contabilidad** **S3(config-vlan)#vlan 23** **S3(config-vlan)#name ingenieria** **S3(config-vlan)#vlan 99** **S3(config-vlan)#name administración** **S3(config-vlan)#exit**
Asignar la dirección IP de administración	**S3(config)#interface vlan 99** **S3(config-if)#ip address 192.168.99.3 255.255.255.0** **S3(config-if)#exit**
Asignar el gateway predeterminado.	**S3(config)#ip default-gateway 192.168.99.1**
Forzar el enlace troncal en la interfaz F0/3	**S3(config)#interface fa0/3** **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-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S3(config-if)#switchport mode access**

Asignar F0/18 a la VLAN 21	**S3(config-if)#interface fa0/18** **S3(config-if)#switchport mode access** **S3(config-if)#switchport access vlan 23** **S3(config-if-range)#no shutdown**
Apagar todos los puertos sin usar	**S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S3(config-if-range)#shutdown**

Tabla 10 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de S3.

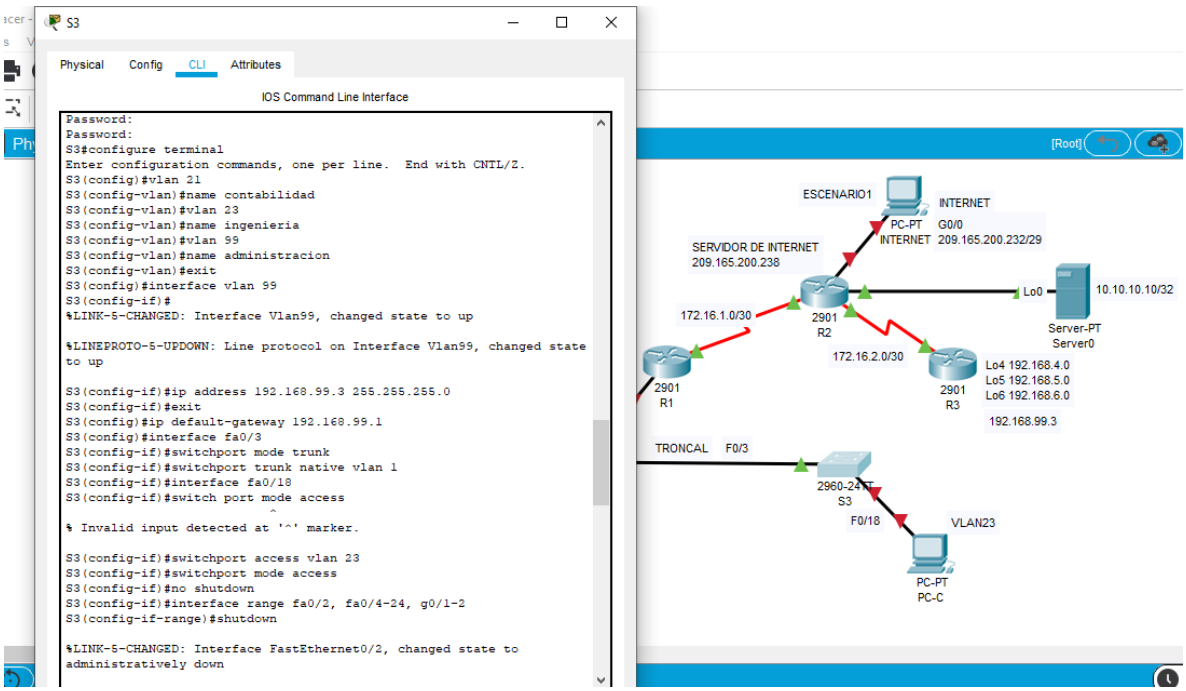

Ilustración 11 Configuración de las vlan en el S3

Paso 3: Configurar R1

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

R1(config)#interface g0/1.21

R1(config-subif)#description accounting LAN

R1(config-subif)#Encapsulation dot1q 21

R1(config-subif)#Ip address 192.168.21.1 255.255.255.0

R1(config-subif)# interface g0/1.23

R1(config-subif)#description accounting LAN

R1(config-subif)#Encapsulation dot1q 23

R1(config-subif)#Ip address 192.168.23.1 255.255.255.0

R1(config-subif)# interface g0/1.99

R1(config-subif)#description accounting LAN

R1(config-subif)#Encapsulation dot1q 99

R1(config-subif)#Ip address 192.168.99.1 255.255.255.0

R1(config-subif)# interface g0/1

R1(config-subif)#no shutdown

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Configurar la subinterfaz 802.1Q .21 en G0/1	**R1(config)#interface g0/1.21** **R1(config-subif)#description accounting LAN** **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)# interface g0/1.23** **R1(config-subif)#description accounting LAN** **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 G0/1	**R1(config-subif)# interface g0/1.99** **R1(config-subif)#description accounting LAN** **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)# interface g0/1** **R1(config-subif)#no shutdown**

Tabla 11 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de R1

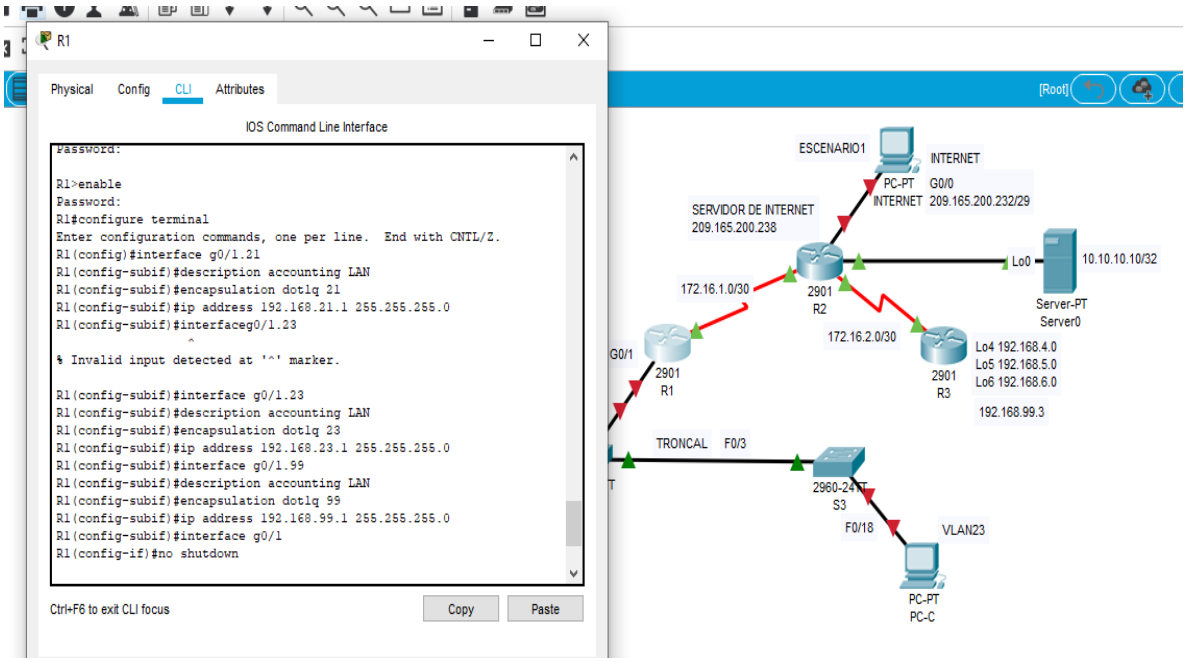

Ilustración 12 Configuración de las vlan en el R1

Paso 4: Verificar la conectividad de la red

Se utiliza el comando ping en cada uno de los dispositivos para probar la conectividad entre los dispositivos de red.

DESDE	A	DIRECCIÓN IP	RESULTADOS DE PING
S1	R1, dirección VLAN 99	192.168.99.1	**S1#ping 192.168.99.1** Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	**S3#ping 192.168.99.1** Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	192.168.21.1	**S1#ping 192.168.21.1** Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S3	R1, dirección VLAN 23	192.168.23.1	**S3#ping 192.168.23.1** Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Tabla 12 Verificación de conectividad entre S1, S3 y R1

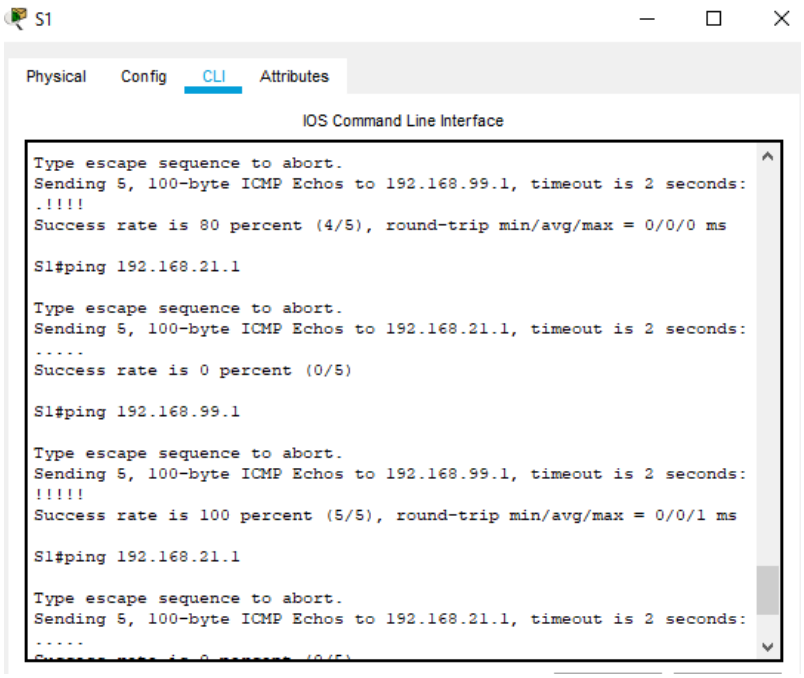

Ilustración 13 Verificación de la vlan 99 desde S1

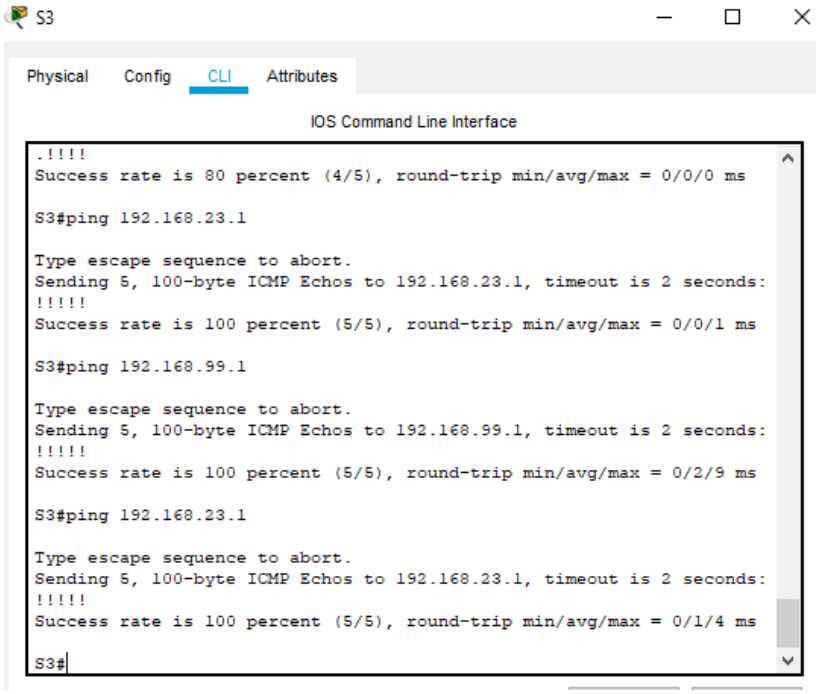

Ilustración 14 Verificación de la vlan 99 desde S3

6.5 PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

Paso 1: Configurar RIPv2 en el R1

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

R1(config)#router rip

R1(config-router)#version 2

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

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Configurar RIP versión 2	**R1(config)#router rip** **R1(config-router)#version 2**
Anunciar las redes conectadas directamente	**R1(config-router)#network 172.16.1.0** **R1(config-router)#network 192.168.21.0** **R1(config-router)#network 192.168.23.0** **R1(config-router)#network 192.168.99.0**
Establecer todas las interfaces LAN como pasivas	**R1(config-router)#passive-interface g0/1.21** **R1(config-router)#passive-interface g0/1.23** **R1(config-router)#passive-interface g0/1.99**
Desactive la sumarización automática	**R1(config-router)#no auto-summary**

Tabla 13 Indicaciones para configurar RIPv2 en R1

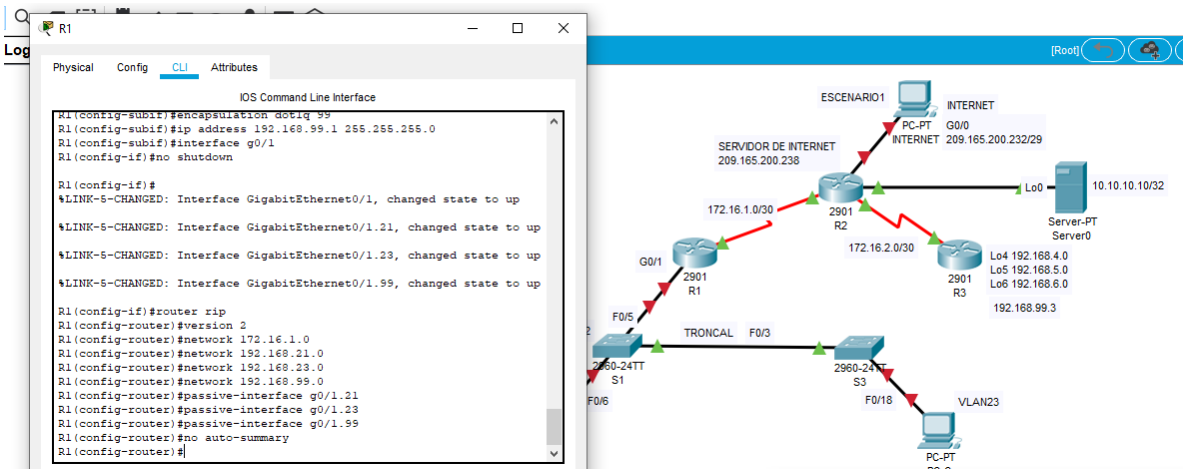

Ilustración 15 Configuración en R1 el protocolo RIPV2

Paso 2: Configurar RIPv2 en el R2

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 172.16.1.0

R2(config)#network 172.16.2.0

R2(config-router)#network 10.10.10.10

R2(config-router)#network 192.168.4.0

R2(config-router)#network 192.168.5.0

R2(config-router)#network 192.168.6.0

R2(config-router)#passive-interface lo4

R2(config-router)#passive-interface lo5

R2(config-router)#passive-interface lo6

R2(config-router)#no auto-summary

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar RIP versión 2	**R2(config)#router rip** **R2(config-router)#version 2**
Anunciar las redes conectadas directamente	**R2(config-router)#network 172.16.1.0** **R2(config-router)#network 172.16.2.0** **R2(config-router)#network 10.10.10.10** **R2(config-router)#network 192.168.4.0** **R2(config-router)#network 192.168.5.0** **R2(config-router)#network 192.168.6.0**
Establecer la interfaz LAN (loopback) como pasiva	**R2(config-router)#passive-interface lo4** **R2(config-router)#passive-interface lo5** **R2(config-router)#passive-interface lo6**
Desactive la sumarización automática.	**R2(config-router)#no auto-summary**

Tabla 14 Indicaciones para configurar RIPv2 en R2

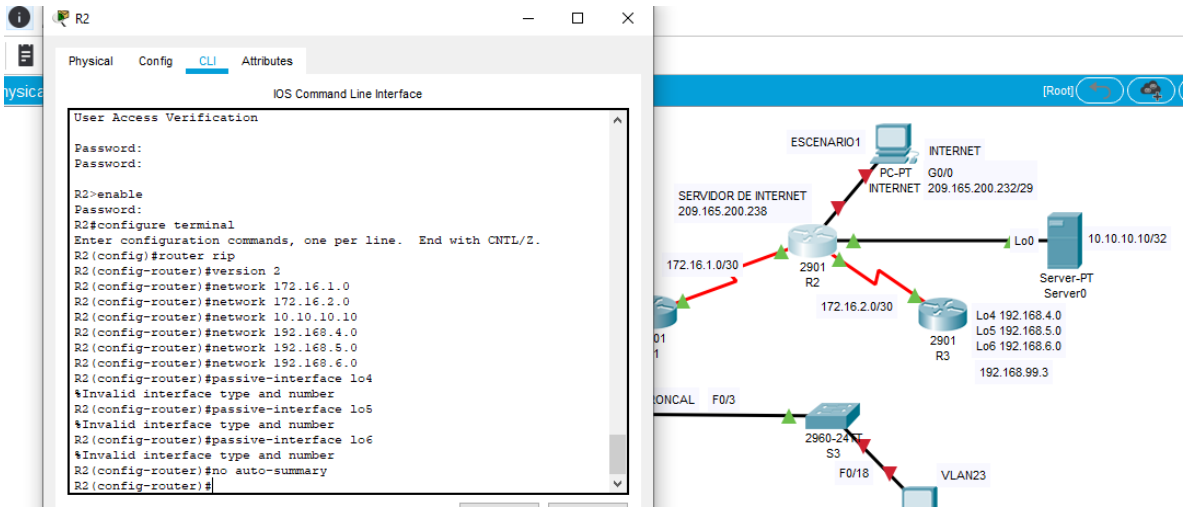

Ilustración 16 Configuración en R2 el protocolo RIPV2

Paso 3: Configurar RIPv2 en el R3

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

R3(config)#router rip

R3(config-router)#version 2

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 lo4

R3(config-router)#passive-interface lo5

R3(config-router)#passive-interface lo6

R3(config-router)#no auto-summary

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Configurar RIP versión 2	**R3(config)#router rip** **R3(config-router)#version 2**
Anunciar redes IPv4 conectadas directamente	**R3(config-router)#network 172.16.2.0** **R3(config-router)#network 192.168.4.0** **R3(config-router)#network 192.168.5.0** **R3(config-router)#network 192.168.6.0**
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	**R3(config-router)#passive-interface lo4** **R3(config-router)#passive-interface lo5** **R3(config-router)#passive-interface lo6**
Desactive la sumarización automática.	**R3(config-router)#no auto-summary**

Tabla 15 Indicaciones para configurar RIPv2 en R3

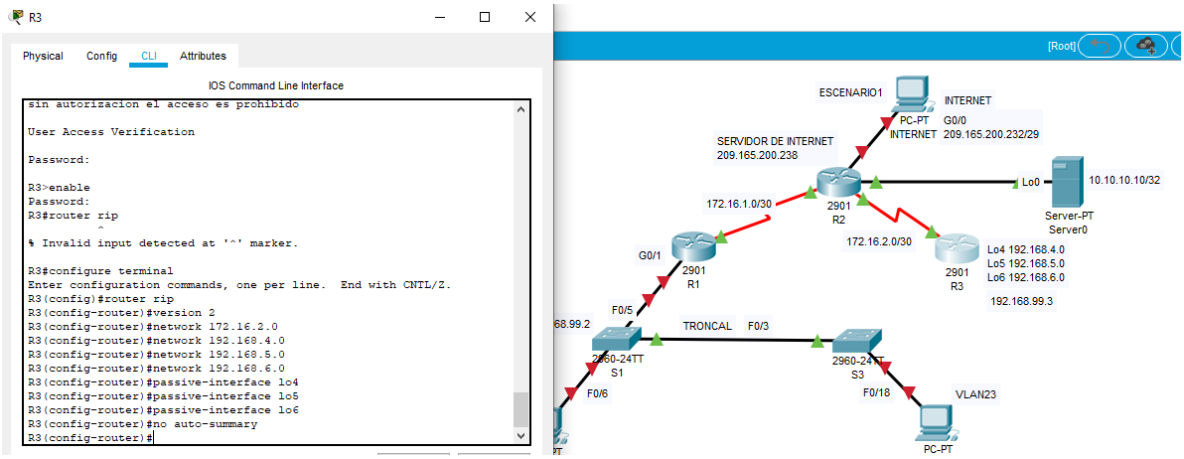

Ilustración 17 Configuración en R3 el protocolo RIPV2

Paso 4: Verificar la información de RIP

PREGUNTA	RESPUESTA
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	**R1#Show ip protocols** **R2#Show ip protocols** **R3#Show ip protocols**
¿Qué comando muestra solo las rutas RIP?	**R1#Show ip route rip** **R2#Show ip route rip** **R3#Show ip route rip**
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	**R1#Show run** **R2#Show run** **R3#Show run**

Tabla 16 Comandos para realizar las verificaciones de las configuraciones que se realizaron

R1#Show ip protocols

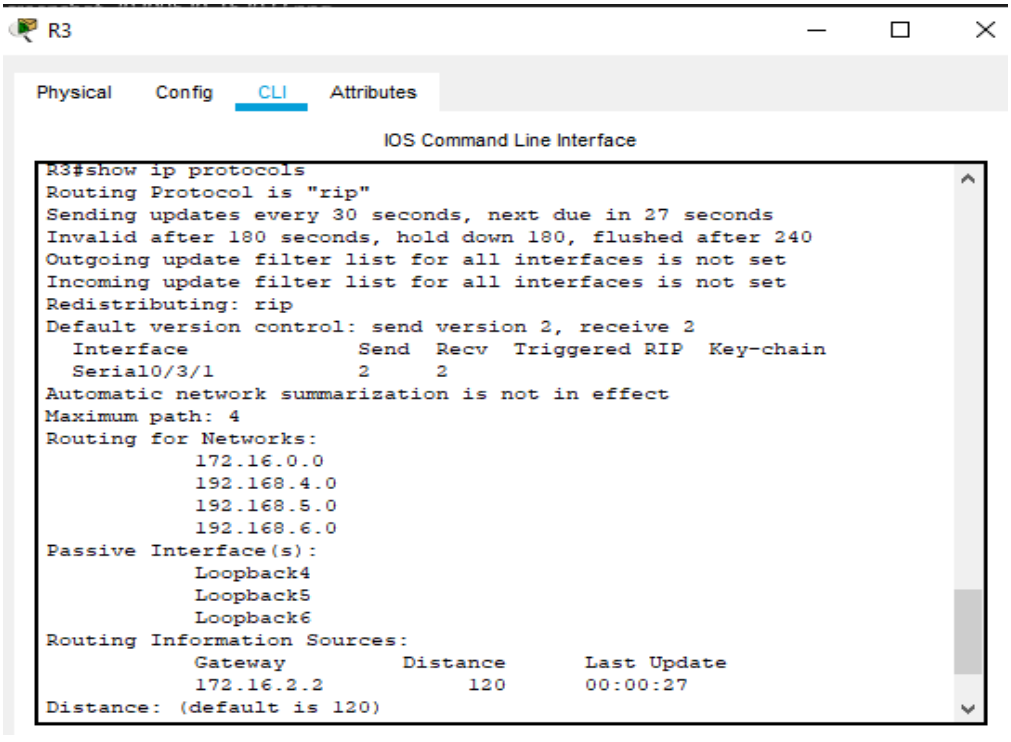

Ilustración 18 Verificación de la información por medio del comando show ip protocols en R1

R1#Show ip route rip

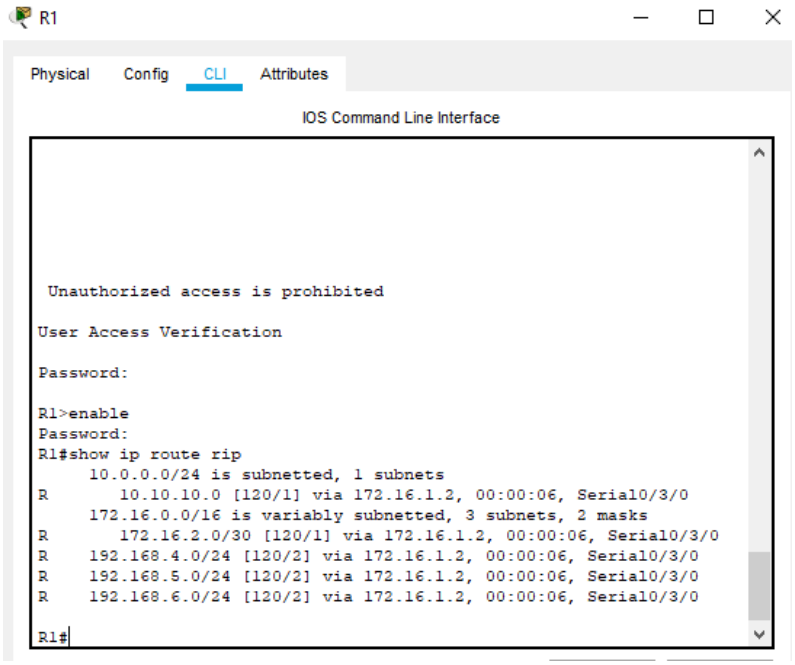

Ilustración 19 Verificación de la información por medio del comando show ip route rip en R1

R1#Show run

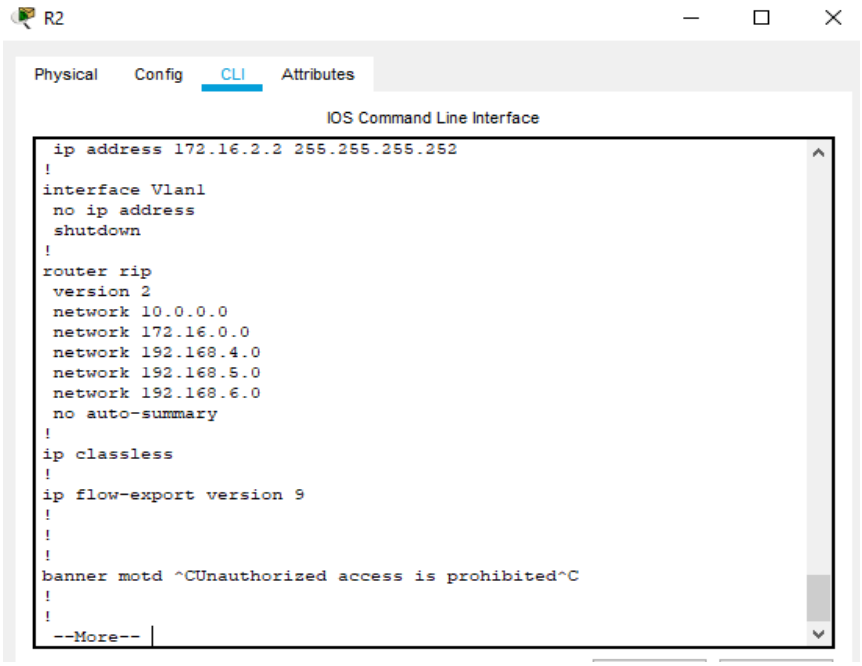

Ilustración 20 Verificación de la información por medio del comando show run en R1

6.6 PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

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

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

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(config)#dns-server 10.10.10.10

R1(config)#domain-name ccna-sa.com

R1(config)#default-router 192.168.21.1

R1(config)#ip dhcp pool ENGNR

R1(config)#dns-server 10.10.10.10

R1(config)#domain-name ccna-sa.com

R1(config)#default-router 192.168.23.1

R1(config)#network 192.168.23.0 255.255.255.0

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	**R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20**
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	**R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20**
Crear un pool de DHCP para la VLAN 21.	**R1(config)#ip dchp pool ACCT** **R1(config)#dns-server 10.10.10.10** **R1(config)#domain-name ccna-sa.com** **R1(config)#default-router 192.168.21.1**
Crear un pool de DHCP para la VLAN 23	**R1(config)#ip dhcp pool ENGNR** **R1(config)#dns-server 10.10.10.10**

	R1(config)#domain-name ccna-sa.com **R1(config)#default-router 192.168.23.1**

Tabla 17 Indicaciones para configurar R1 como servidor de DHCP

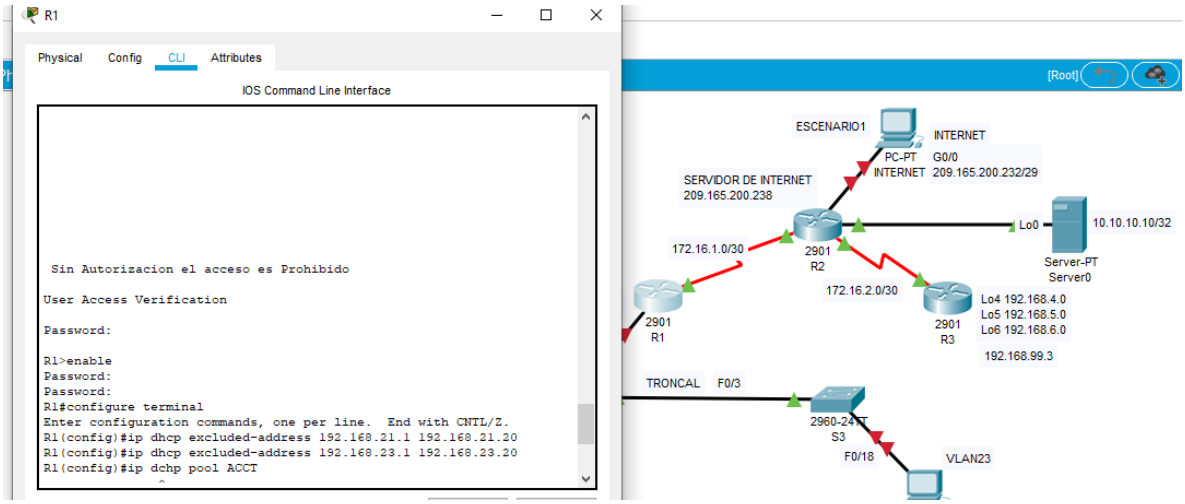

Ilustración 21 Configuración DHCP en R1

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

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R2.

R2(config)#user webuser privilege 15 secret cisco12345

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

R2(config)#interface gi0/1

R2(config)#ip nat outside

R2(config)#interface fa0/6

R2(config)#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

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear una base de datos local con una cuenta de usuario	**R2(config)#user webuser privilege 15 secret cisco12345**
Habilitar el servicio del servidor HTTP	**Packet Tracer no procesa la configuraion HTTP**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	**R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	**R2(config)#interface gi0/1** **R2(config)#ip nat outside** **R2(config)#interface fa0/6** **R2(config)#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** **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**
Defina el pool de direcciones IP públicas utilizables.	**R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248**
Definir la traducción de NAT dinámica	**R2(config)#ip nat inside source list 1 pool INTERNET**

Tabla 18 Indicaciones para realizar la configuración NAT en R2

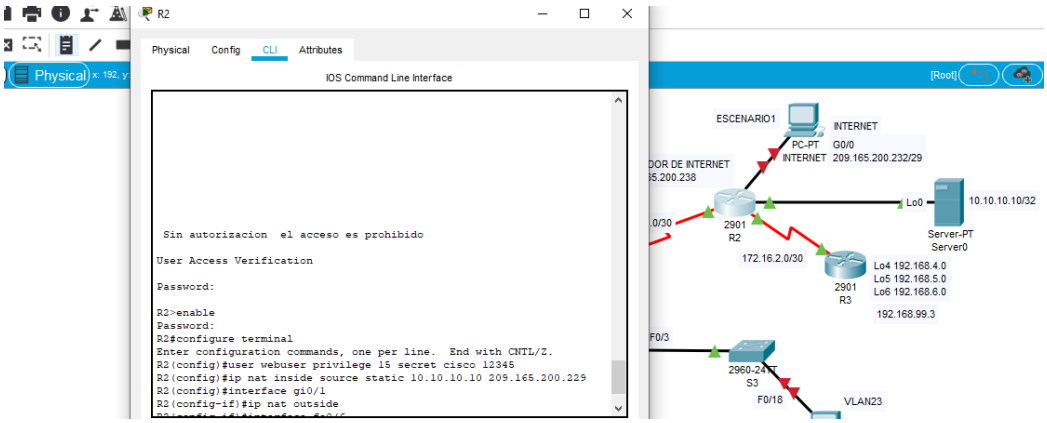

Ilustración 22 Configuración DHCP en R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

En las ilustraciones que observamos a continuación se muestra si en cada PC está funcionando el protocolo DHCP y si hay comunicación entre el PC-A y el PC-C.

PRUEBA	RESULTADOS
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	**DHCP request successful**
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	**DHCP request successful**
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	**Successful**
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	**Successful**

Tabla 19 Verificación del protocolo DHCP y NAT en los dispositivos

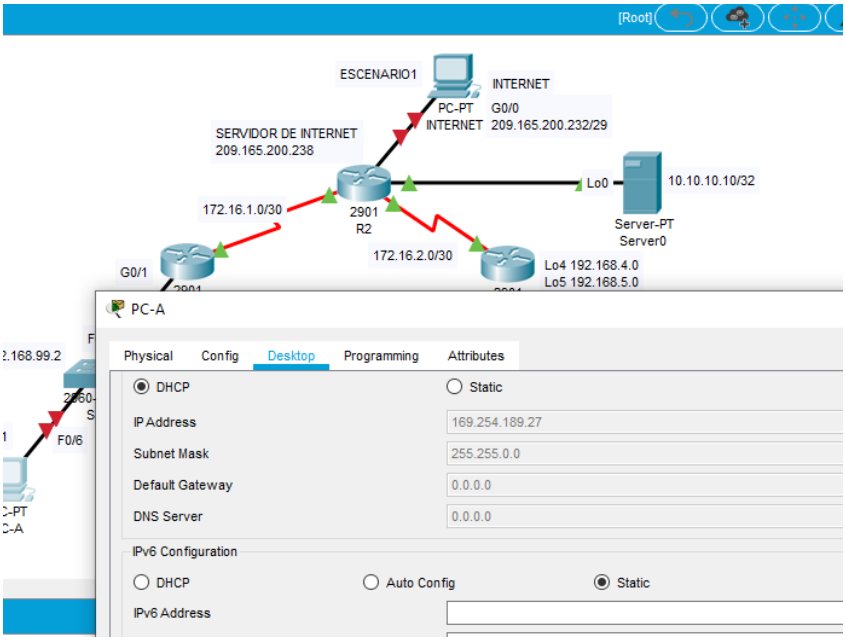

Ilustración 23 Verificación en el PC-A

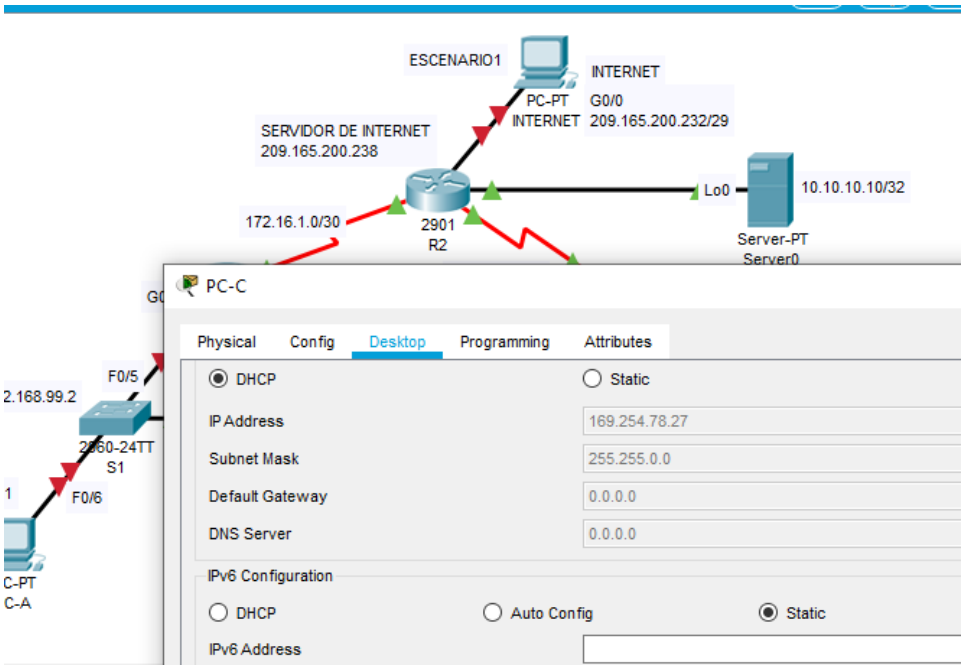

Ilustración 24 Verificación de DHCP en PC-C

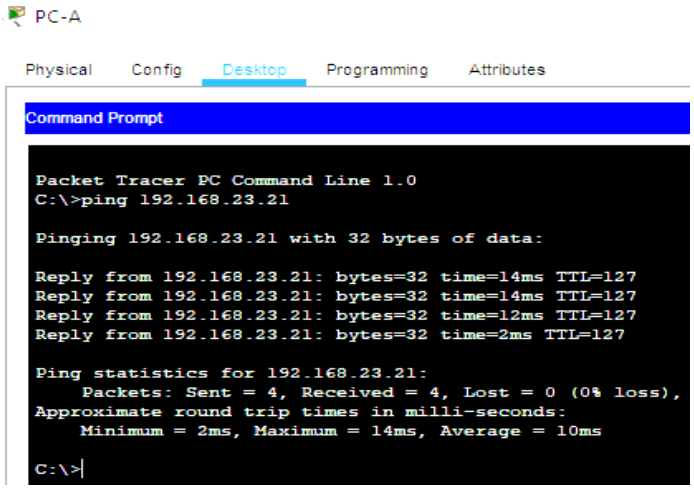

Ilustración 25 Verificación desde el PC-A al PC-C

6.7 PARTE 6: CONFIGURAR NTP

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R1 y R2

R2#clock set 09:00:00 05 march 2016

R2(config)#ntp master 5

R1(config)#ntp client 5

R1(config)#ntp update-calendar

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**R2#clock set 09:00:00 05 march 2016**
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** **R1#show clock**

Tabla 20 Indicaciones para configurar NTP en R1 Y R2

6.8 PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

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

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R2, para restringir el acceso a las líneas de control de acceso.

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

R2(config-std-nacl)#permit host 172.16 1.1

R2(config-std-nacl)#exit

R2(config-line)#line vty 0 4

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

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	**R2(config)#ip access-list standart ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	**R2(config-line)#line vty 0 4**
Permitir acceso por Telnet a las líneas de VTY	**R2(config-line)#access-class ADMIN-MGT in**
Verificar que la ACL funcione como se espera	

Tabla 21 Indicaciones para configurar y verificar las ACL

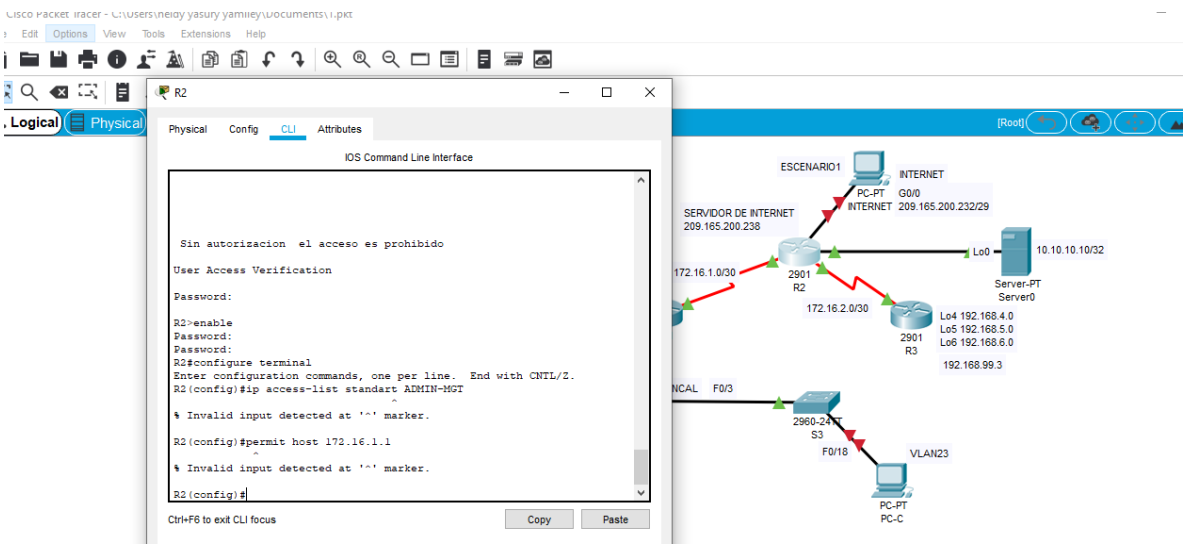

Ilustración 26 Configuración de los accesos

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
R2(config)#access-list 101 permit tcp any host 209.165.200.229 eq www
R2(config)#access-list 101 permit icmp any any echo-reply
```

Ilustración 27 Lista de acceso en el Router R2

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

Tabla 22 Comandos para realizar las verificaciones de las configuraciones realizadas en

DESCRIPCIÓN DEL COMANDO	ENTRADA DEL ESTUDIANTE (COMANDO)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	**#show ip access list**
Restablecer los contadores de una lista de acceso	**#clear ip**
¿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**
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	**#clear ip nat translations**

los dispositivos

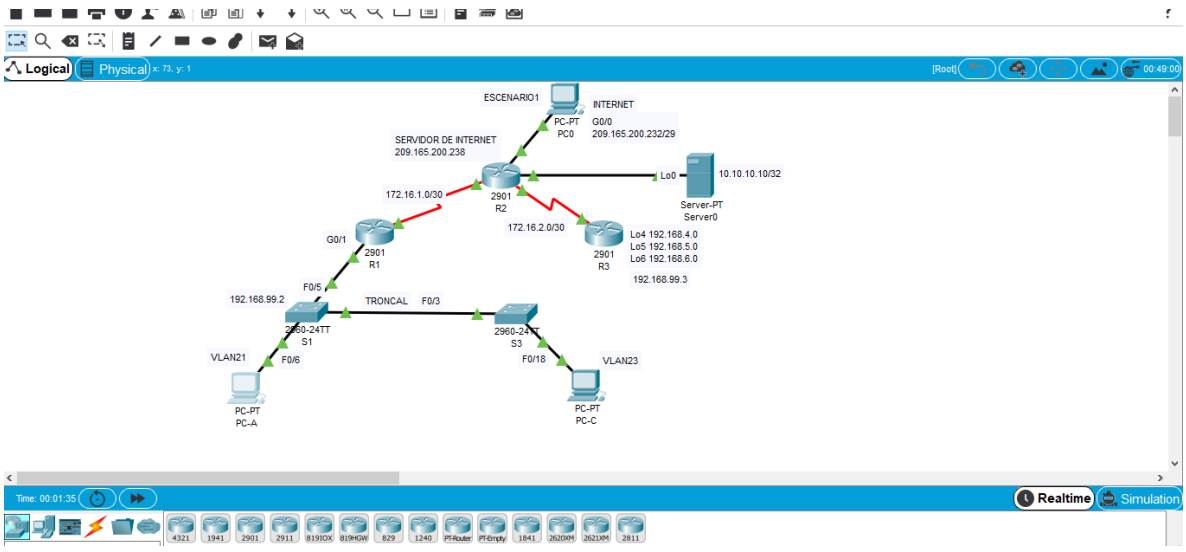

Ilustración 28 Verificación del show interface en R2

7. DESARROLLO DEL SEGUNDO ESCENARIO

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.

7.2 TOPOLOGÍA DEL SEGUNDO ESCENARIO

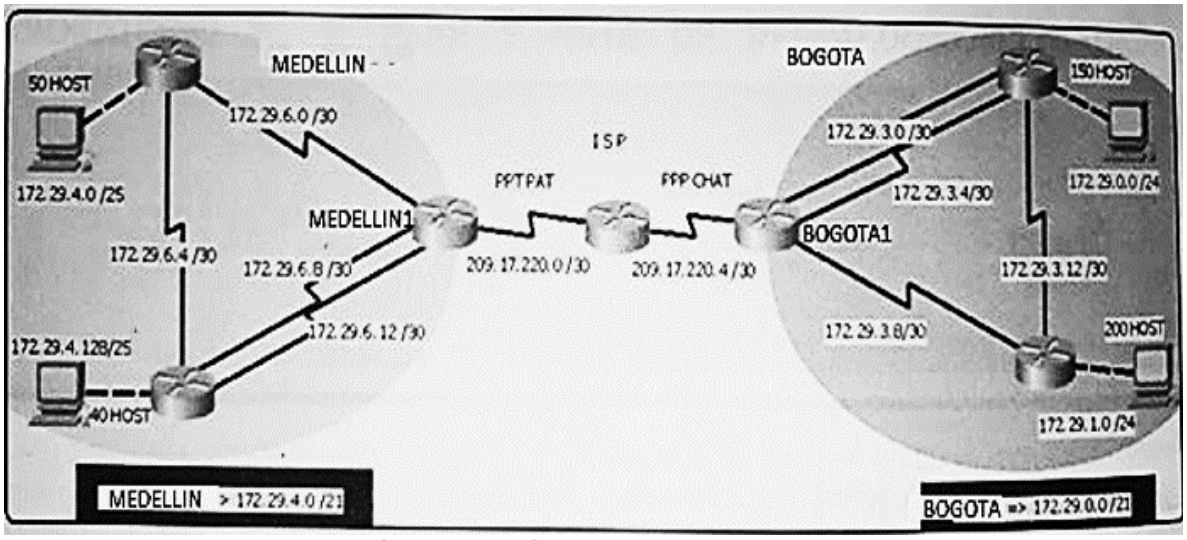

Ilustración 29 Topología de la red del segundo escenario

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.

7.3 PARTE 1: ARMAR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS

En esta primera parte, se establece la topología de la red y se borra cualquier configuración anterior que tengan los dispositivos.

Paso 1: Realizar el cableado de red tal como se muestra en la topología

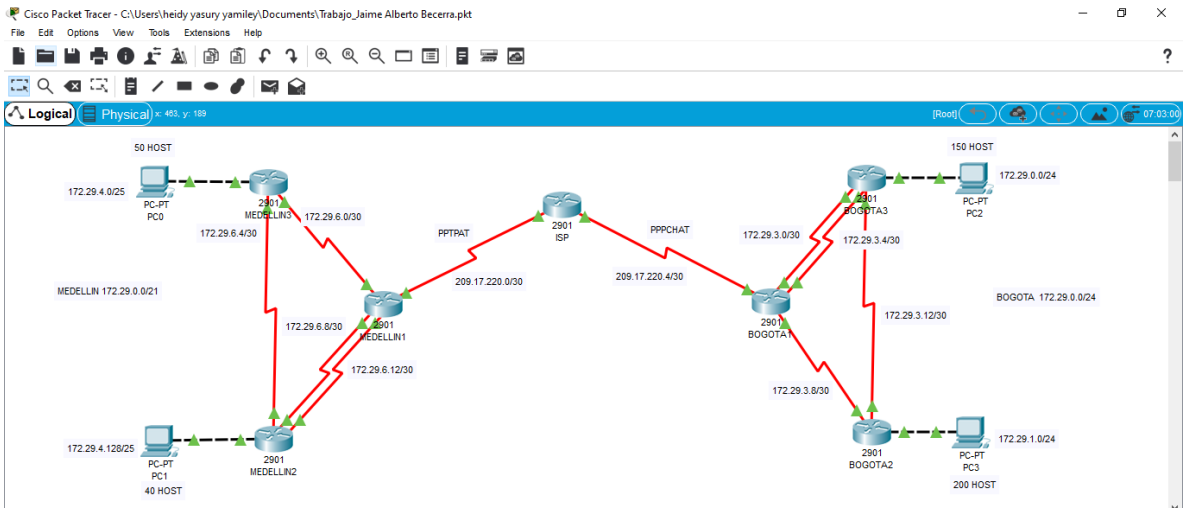

Ilustración 30 Topología de la red en Cisco Packet Tracer del segundo escenario

7.4 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: Configurar los Routers

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router según les corresponde.

- ISP

Router>enable

Router#configure terminal

Router(config)#hostname ISP

ISP(config)#no ip domain-lookup

ISP(config)#service password-encryption

ISP(config)#enable secret class

ISP(config)#banner motd $Se prohibe el acceso no autorizado$

ISP(config)#enable secret cisco

ISP(config)#line console 0

ISP(config)#password cisco

ISP(config)#login

ISP(config)#line vty 0 4

ISP(config)#password cisco

ISP(config)#login

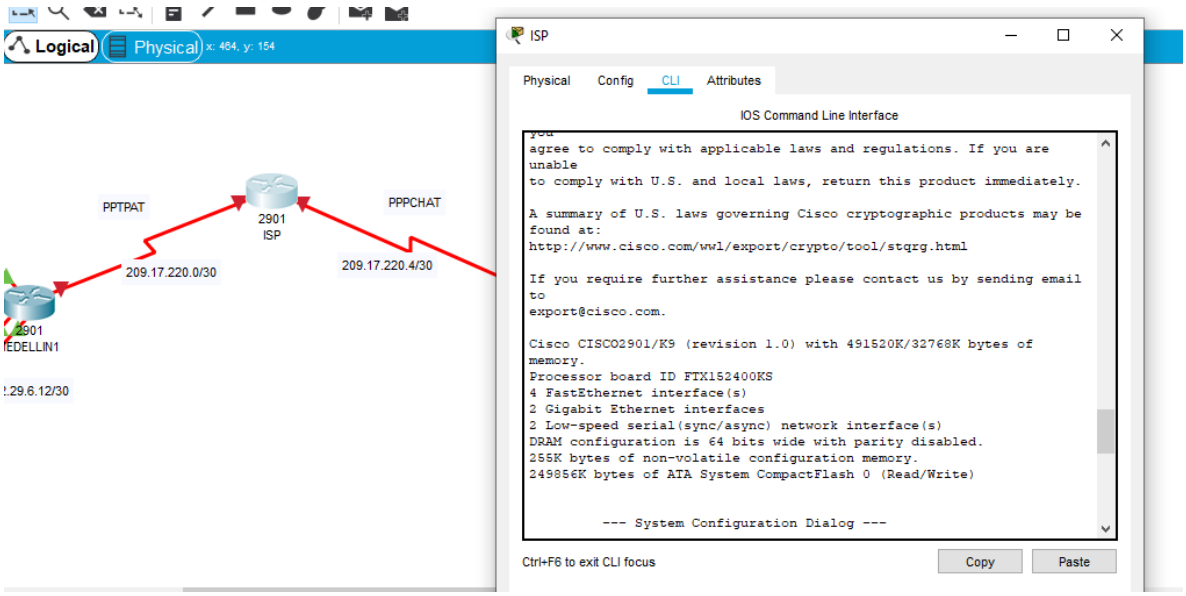

Ilustración 31 Configuraciones básicas en Router ISP

- MEDELLIN 1

Router> enable

Router#configure terminal

Router(config)#hostname MEDELLIN1

MEDELLIN1(config)#enable secret cisco.

MEDELLIN1(config-line)#line console 0

MEDELLIN1(config-line)#password cisco

MEDELLIN1(config-line)#login

MEDELLIN1(config-line)#line vty 0 4

MEDELLIN1(config-line)#password cisco

MEDELLIN1(config-line)#login

MEDELLIN1(config-line)#exit.

MEDELLIN1(config)#service password-encryption

MEDELLIN1(config)#do write

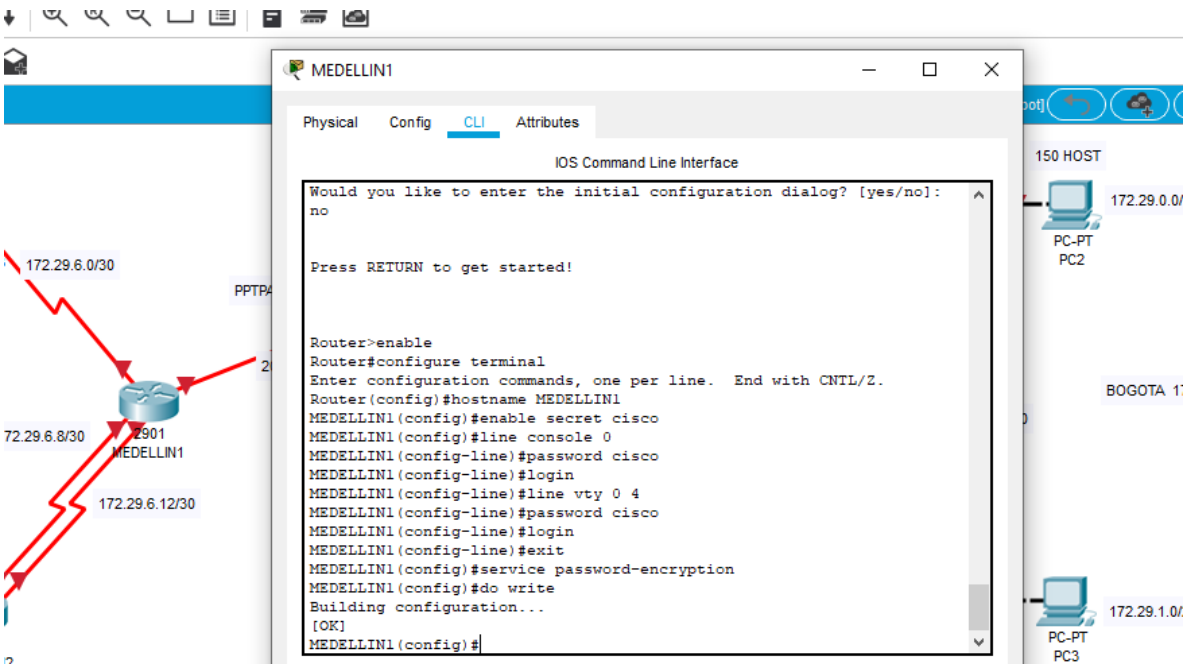

Ilustración 32 Configuraciones básicas en Router MEDELLIN1

- MEDELLIN 2

Router> enable

Router#configure terminal

Router(config)#hostname MEDELLIN2

MEDELLIN2(config)#enable secret cisco.

MEDELLIN2(config)#line console 0

MEDELLIN2(config-line)#password cisco

MEDELLIN2(config-line)#login

MEDELLIN2(config-line)#line vty 0 4

MEDELLIN2(config-line)#password cisco

MEDELLIN2(config-line)#login

MEDELLIN2(config-line)#exit.

MEDELLIN2(config)#service password-encryption

MEDELLIN2(config)#do write

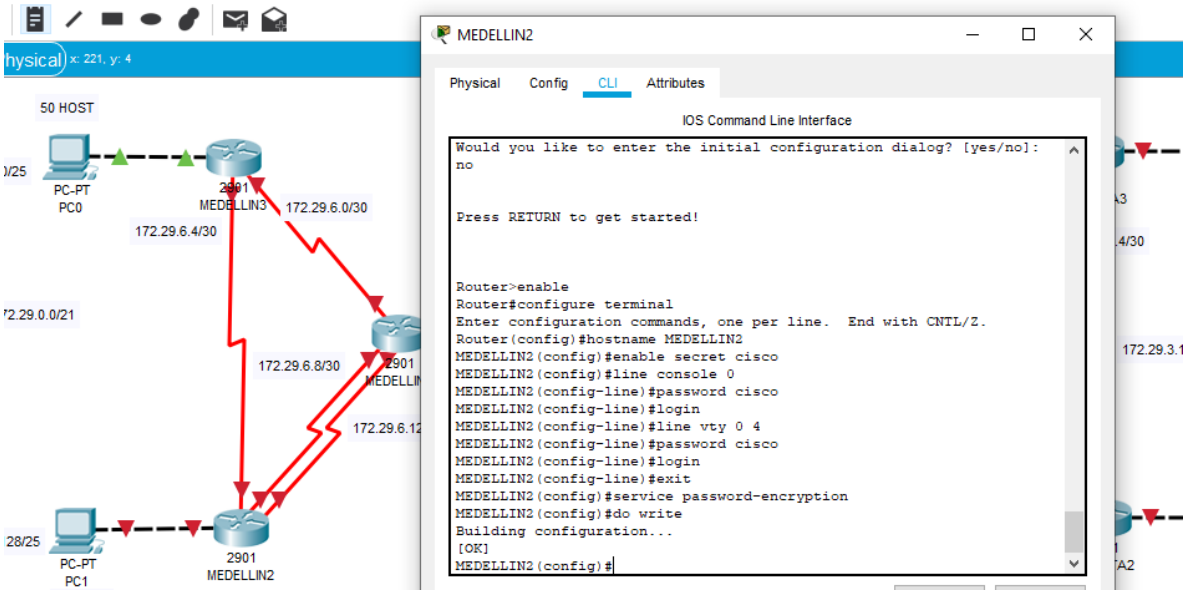

Ilustración 33 Configuraciones básicas en Router MEDELLIN2

- MEDELLIN 3

Router> enable

Router#configure terminal

Router(config)#hostname MEDELLIN3

MEDELLIN3(config)#enable secret cisco.

MEDELLIN3(config-line)#line console 0

MEDELLIN3(config-line)#password cisco

MEDELLIN3(config-line)#login

MEDELLIN3(config-line)#line vty 0 4

MEDELLIN3(config-line#password cisco

MEDELLIN3(config-line)#login

MEDELLIN3(config-line)#exit.

MEDELLIN3(config)#service password-encryption

MEDELLIN3(config)#do write

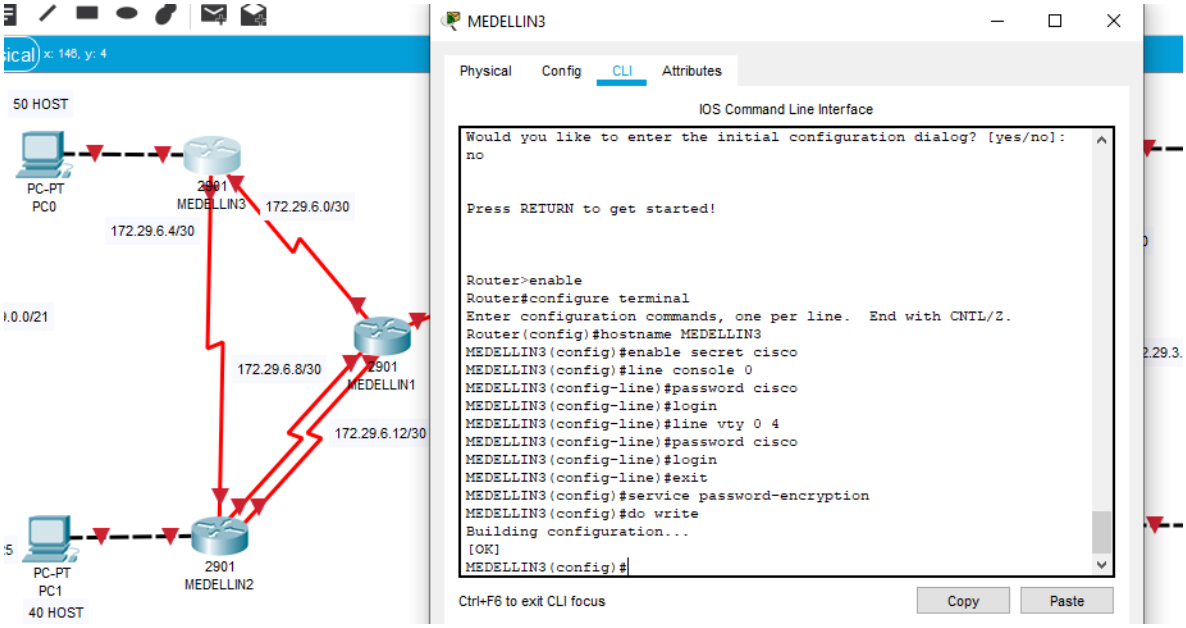

Ilustración 34 Configuraciones básicas en Router MEDELLIN3

- BOGOTA 1

Router> enable

Router#configure terminal

Router(config)#hostname BOGOTA1

BOGOTA1(config)#enable secret cisco.

BOGOTA1(config)#line console 0

BOGOTA1(config-line)#password cisco

BOGOTA1(config-line)#login

BOGOTA1(config-line)#line vty 0 4

BOGOTA1(config-line)#password cisco

BOGOTA1(config-line)#login

BOGOTA1(config-line)##exit.

BOGOTA1(config)#service password-encryption

BOGOTA1(config)#do write

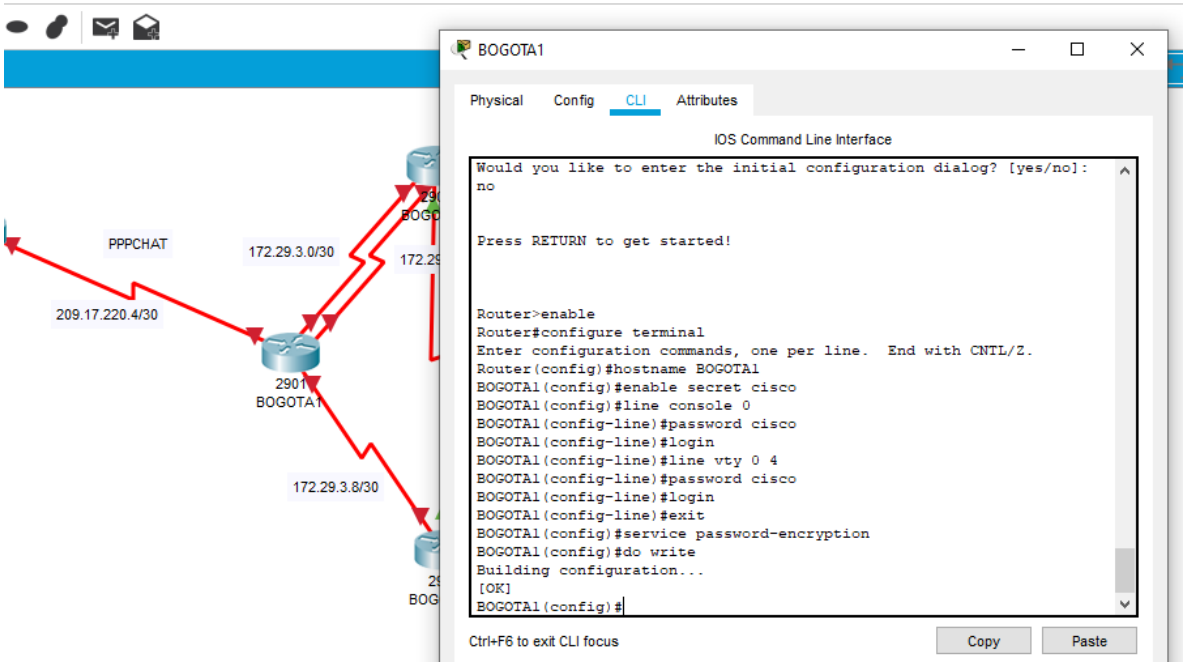

Ilustración 35 Configuraciones básicas en Router BOGOTA1

- BOGOTA 2 (B2)

Router> enable

Router#configure terminal

Router(config)#hostname BOGOTA2

BOGOTA2(config)#enable secret cisco.

BOGOTA2(config)#line console 0

BOGOTA2(config-line)#password cisco

BOGOTA2(config-line)#login

BOGOTA2(config-line)#line vty 0 4

BOGOTA2(config-line)#password cisco

BOGOTA2(config-line)#login

BOGOTA2(config-line)#exit.

BOGOTA2(config)#service password-encryption

BOGOTA2(config)#do write

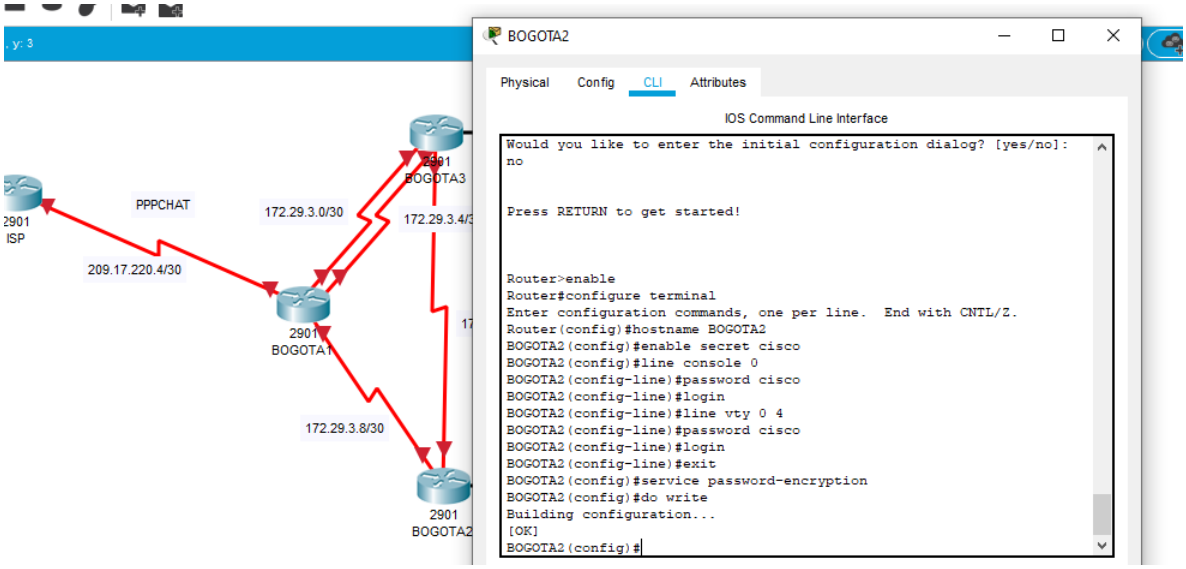

Ilustración 36 Configuraciones básicas en Router BOGOTA2

- BOGOTA 3 (B3)

Router> enable

Router#configure terminal

Router(config)#hostname BOGOTA3

BOGOTA3(config)#enable secret cisco.

BOGOTA3(config)#line console 0

BOGOTA3(config-line)#password cisco

BOGOTA3(config-line)#login

BOGOTA3(config-line)##line vty 0 4

BOGOTA3(config-line)##password cisco

BOGOTA3(config-line)##login

BOGOTA3(config-line)##exit.

BOGOTA3(config)#service password-encryption

BOGOTA3(config)#do write

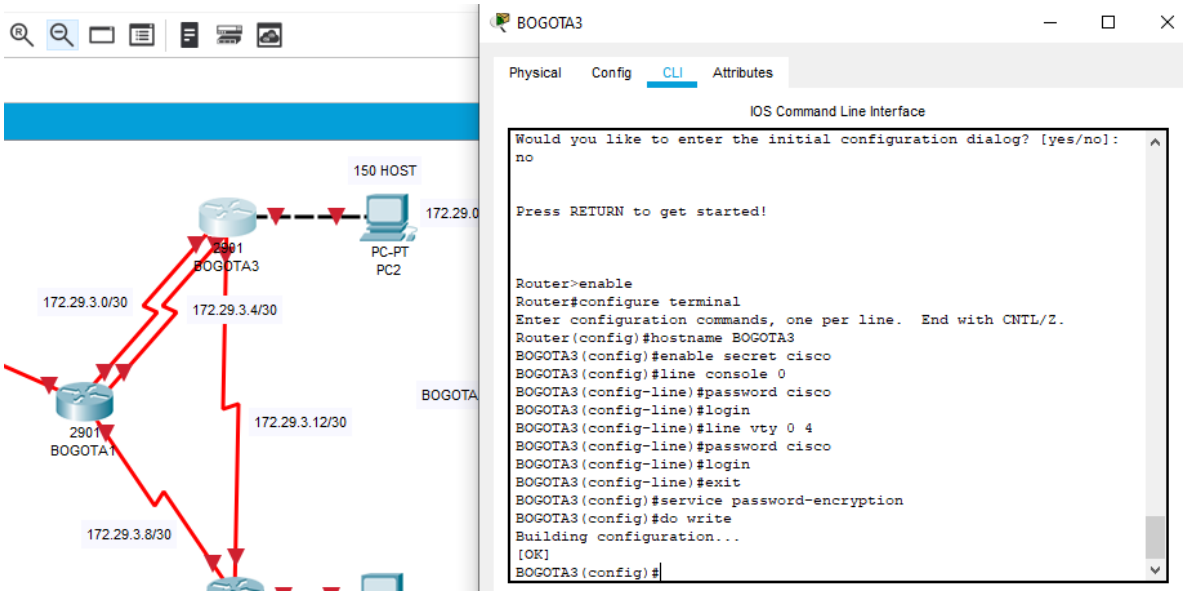

Ilustración 37 Configuraciones básicas en Router BOGOTA3

7.5 PARTE 3: CONFIGURACIÓN DEL ENRUTAMIENTO

Paso 1: Configurar los puertos seriales de cada router

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router según les corresponde.

- ISP

ISP(config)#interface s0/3/0

ISP(config-if)#ip address 209.17.220.5 255.255.255.252

ISP(config-if)#no shutdown

ISP(config-if#exit

ISP(config)#interface s0/3/1

ISP(config-if)#ip address 209.17.220.1 255.255.255.252

ISP(config-if)#no shutdown

ISP(config-router)#exit

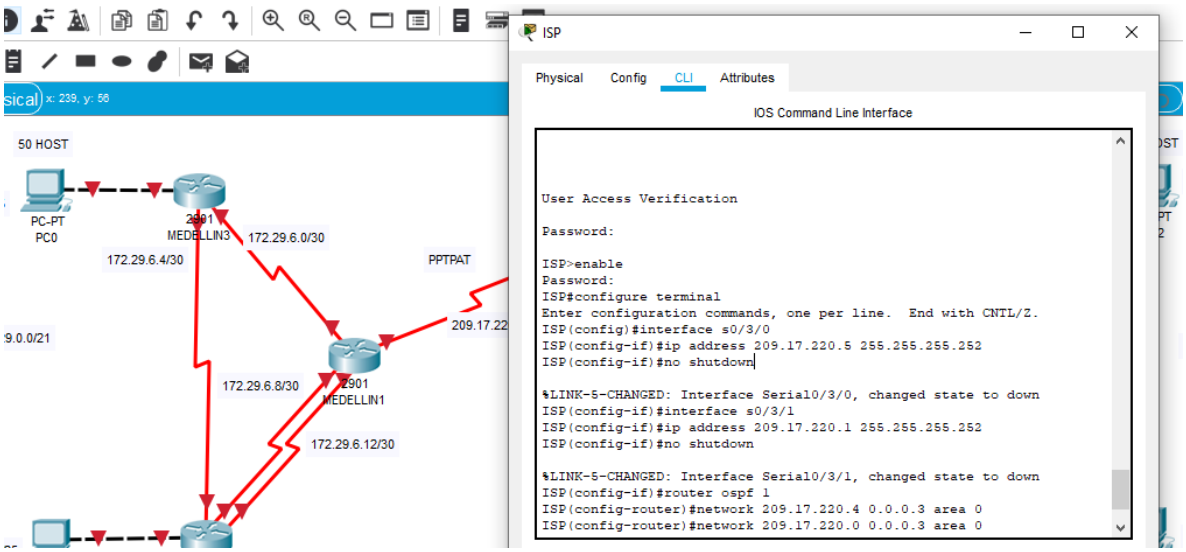

Ilustración 38 Configuración de enrutamiento en el Router ISP

- MEDELLIN 1

MEDELLIN1 (config)#interface s0/3/1 (Ruta por defecto al ISP)
MEDELLIN1 (config-if)#ip address 209.17.200.2 255.255.255.252
MEDELLIN1 (config-if)#no shutdown
MEDELLIN1 (config-if#exit
MEDELLIN1 (config)#interface s0/3/0
MEDELLIN1 (config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1 (config-if)#no shutdown
MEDELLIN1 (config-if#exit
MEDELLIN1 (config)#interface s0/1/0
MEDELLIN1 (config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1 (config-if)#no shutdown
MEDELLIN1 (config-router)#exit
MEDELLIN1 (config)#interface s0/1/1
MEDELLIN1 (config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1 (config-if)#no shutdown

MEDELLIN1 (config-router)#exit
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN1 (config-router)#no auto-summary

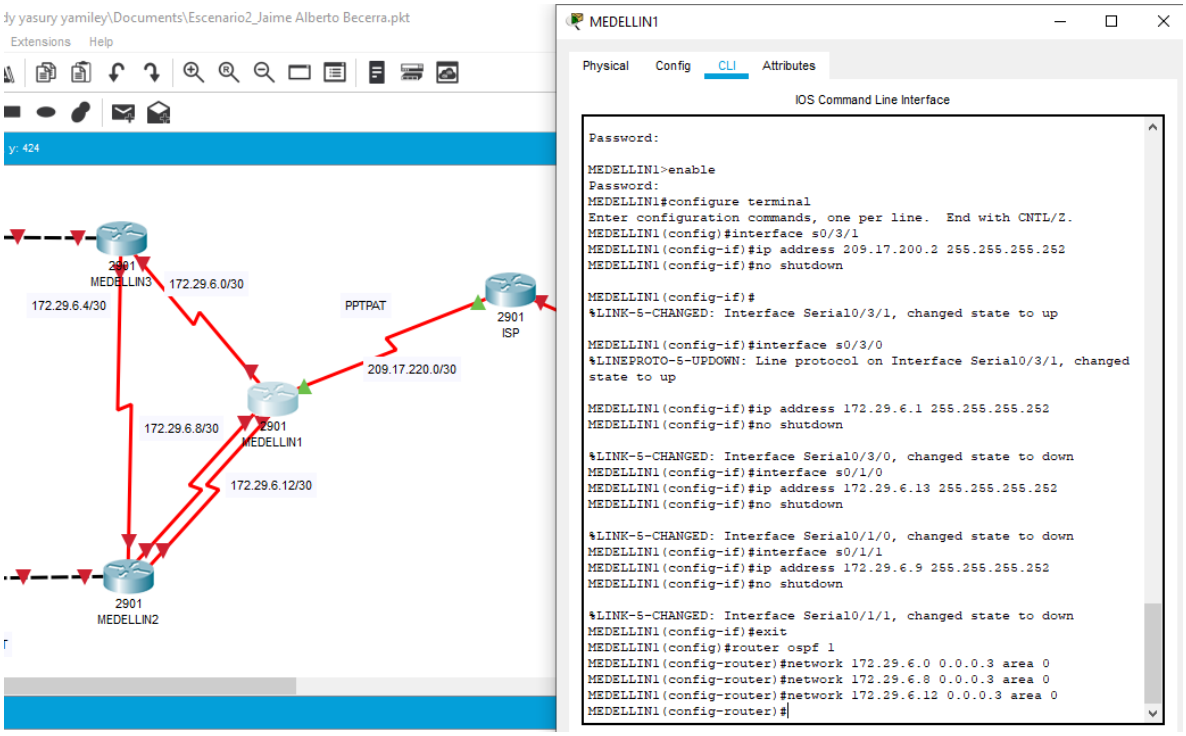

Ilustración 39 Configuración de enrutamiento en el Router MEDELLIN1

- MEDELLIN 2

MEDELLIN2(config)#interface s0/1/0

MEDELLIN2(config-if)#ip address 172.29.6.14 255.255.255.252

MEDELLIN2 (config-if)#no shutdown

MEDELLIN2 (config-if#exit

MEDELLIN2 (config)#interface s0/1/1

MEDELLIN2 (config-if)#ip address 172.29.6.10 255.255.255.252

MEDELLIN2 (config-if)#no shutdown

MEDELLIN2 (config-if#exit

MEDELLIN2 (config)#interface s0/3/1
MEDELLIN2 (config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN2 (config-if)#no shutdown
MEDELLIN2 (config)#interface gi0/0
MEDELLIN2 (config-if)#ip address 172.29.4.130 255.255.255.128
MEDELLIN2 (config-if)#no shutdown
MEDELLIN2 (config-router)#exit
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#network 172.29.4.128 0.0.0.255 area 0
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.8 0.0.0.255 area 0
MEDELLIN2(config-router)#network 172.29.6.12 0.0.0.255 area 0
MEDELLIN2(config-router)#no auto-summary

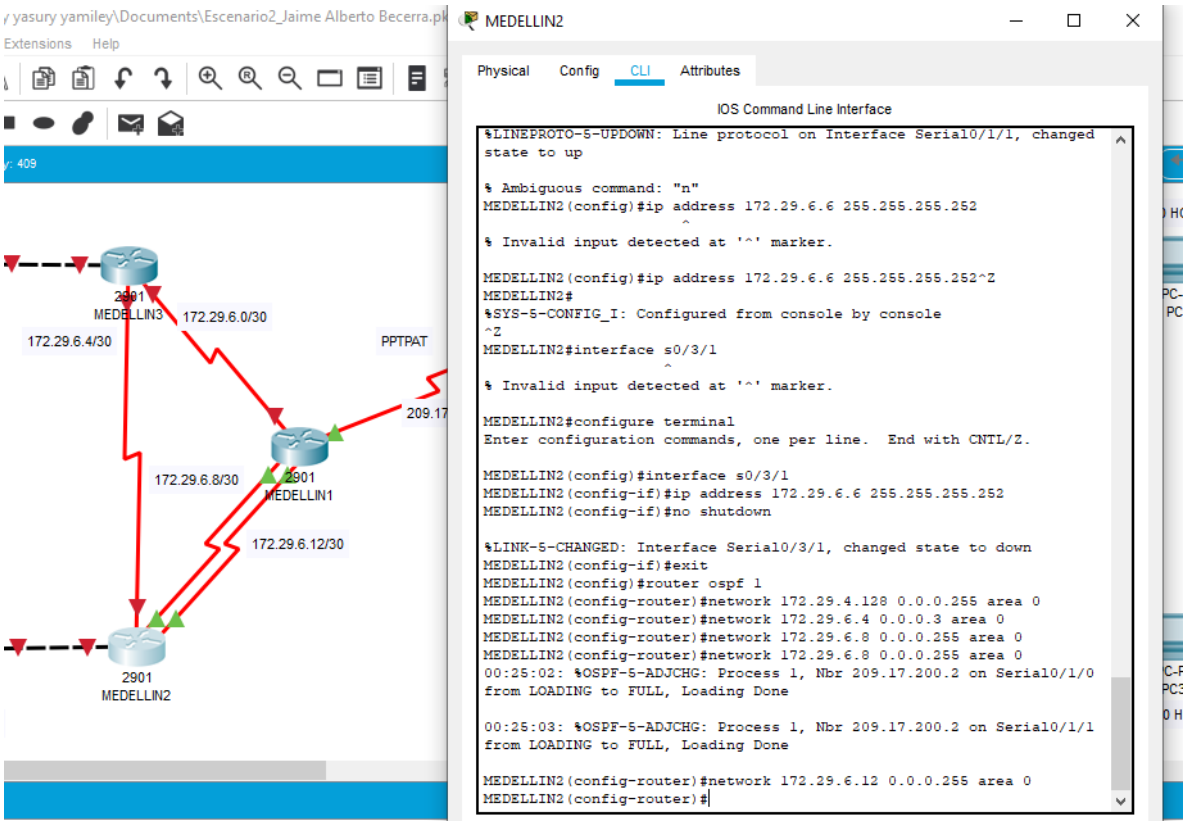

Ilustración 40 Configuración de enrutamiento en el Router MEDELLIN2

- MEDELLIN 3

MEDELLIN3(config)#interface s0/3/0
MEDELLIN3(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN3 (config-if)#no shutdown
MEDELLIN3 (config-if#exit
MEDELLIN3 (config)#interface s0/3/1
MEDELLIN3 (config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN3 (config-if)#no shutdown
MEDELLIN3 (config-if#exit
MEDELLIN2 (config)#interface gi0/0
MEDELLIN2 (config-if)#ip address 172.29.4.2 255.255.255.252
MEDELLIN2 (config-if)#no shutdown
MEDELLIN2 (config-router)#exit
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#network 172.29.4.0 0.0.0.255 area 0
MEDELLIN3(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.255 area 0
MEDELLIN3(config-router)#no auto-summary

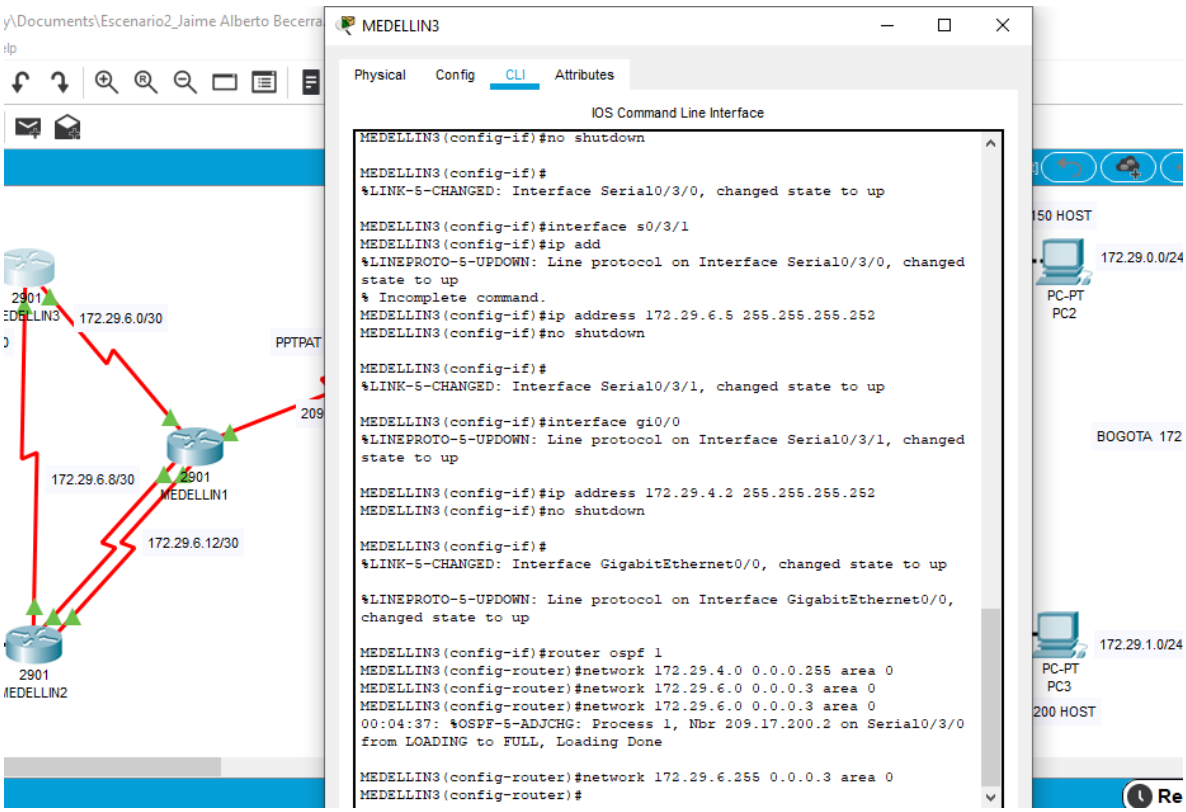

Ilustración 41 Configuración de enrutamiento en el Router MEDELLIN 3

- BOGOTA 1 (B1)

BOGOTA1 (config)#interface s0/3/0 (Ruta por defecto al ISP)
BOGOTA1 (config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1 (config-if)#no shutdown
BOGOTA1 (config-if#exit
BOGOTA1(config)#interface s0/3/1
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if#exit
BOGOTA1(config)#interface s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA (config-if)#no shutdown
BOGOTA1(config-router)#exit
BOGOTA1(config)#interface s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-router)#exit
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 1
BOGOTA1(config-router)#no auto-summary

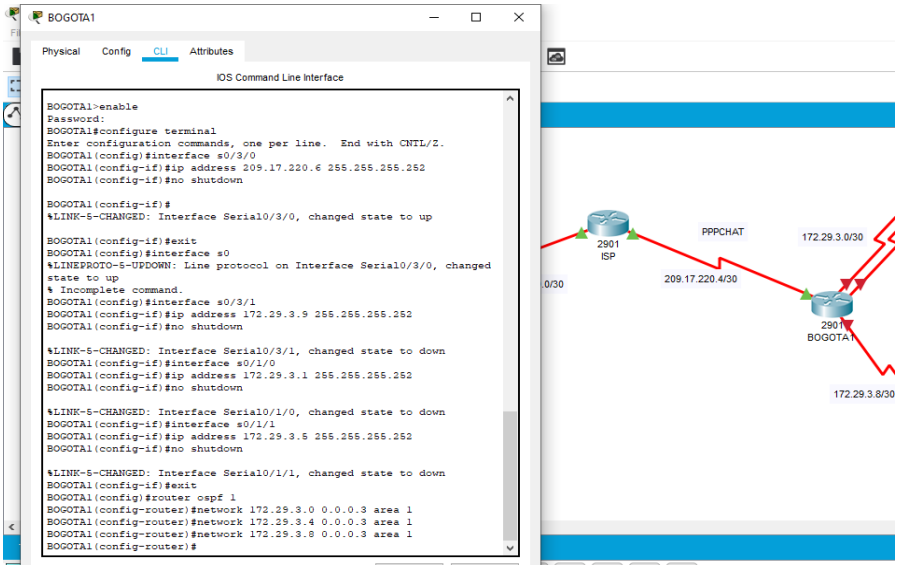

Ilustración 42 Configuración de enrutamiento en el Router BOGOTA 1

- BOGOTA 2 (B2)

BOGOTA2(config)#interface s0/3/1
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if#exit
BOGOTA2(config)#interface s0/3/0
BOGOTA2(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-router)#exit
BOGOTA2(config)#interface gi0/0
BOGOTA2(config-if)#ip address 172.29.1.2 255.255.255.0
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-router)#exit
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 1
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 1
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 1
BOGOTA2(config-router)#no auto-summary

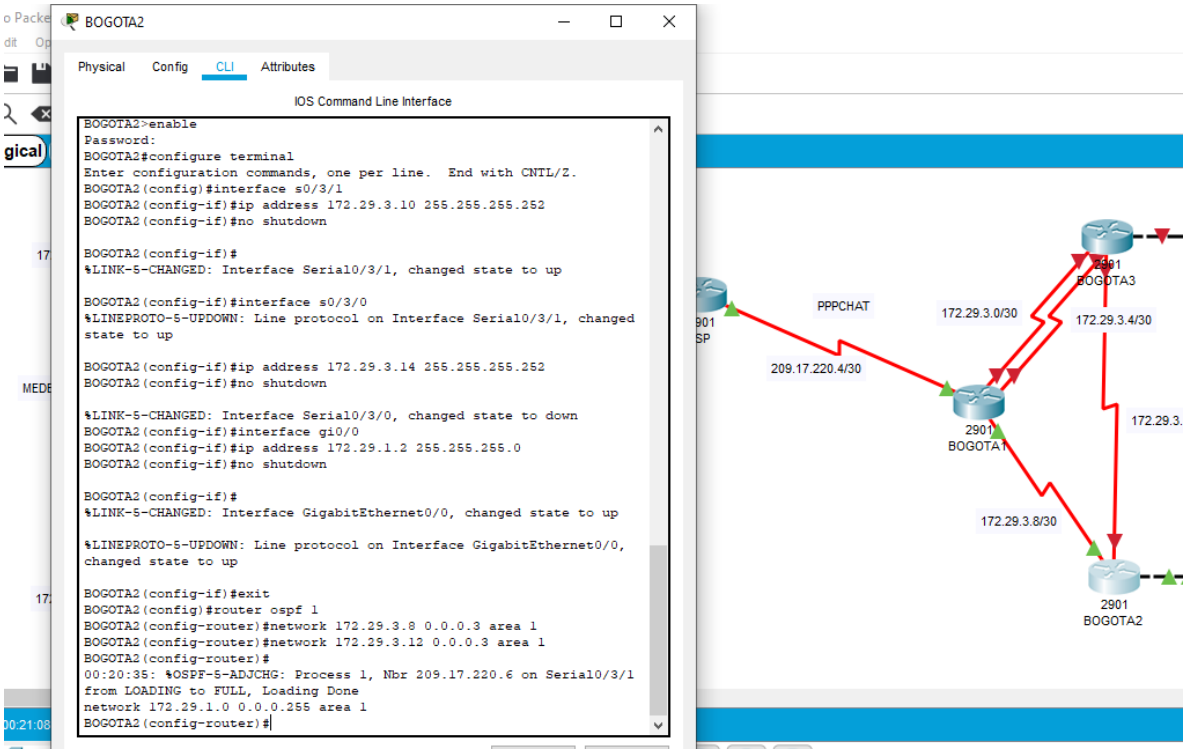

Ilustración 43 Configuración de enrutamiento en el Router BOGOTA 2

- BOGOTA 3 (B3)

```
BOGOTA3(config)#interface s0/1/0
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if#exit
BOGOTA3(config)#interface s0/1/1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-router)#exit
BOGOTA3(config)#interface s0/3/0
BOGOTA3(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-router)#exit
BOGOTA3(config)#interface gi0/0
BOGOTA3(config-if)#ip address 172.29.0.2 255.255.255.0
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-router)#exit
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 1
BOGOTA3(config-router)#no auto-summary
```

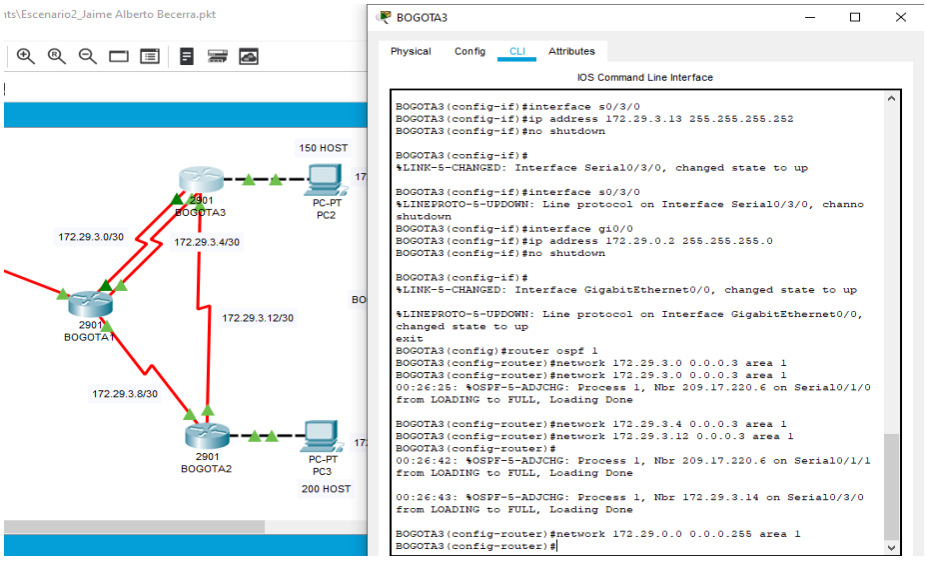

Ilustración 44 Configuración de enrutamiento en el Router BOGOTA3

Paso 2: Configurar el Protocolo OSPF en los routers

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router según les corresponde.

- ISP

ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.0 0.0.0.3 area0
ISP(config-router)#no auto-summary

- MEDELLIN 1

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN1(config-router)#no auto-summary

- MEDELLIN 2

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#network 172.29.4.128 0.0.0.255 area 0
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.8 0.0.0.255 area 0
MEDELLIN2(config-router)#network 172.29.6.12 0.0.0.255 area 0
MEDELLIN2(config-router)#no auto-summary

- MEDELLIN 3 (M3)

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#network 172.29.4.0 0.0.0.255 area 0
MEDELLIN3(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.255 area 0

MEDELLIN3(config-router)#no auto-summary

- BOGOTA 1 (B1)

BOGOTA1(config)#router ospf 1

BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 1

BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 1

BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 1

BOGOTA1(config-router)#no auto-summary

- BOGOTA 2 (B2)

BOGOTA2(config)#router ospf 1

BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 1

BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 1

BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 1

BOGOTA2(config-router)#no auto-summary

- BOGOTA 3 (B3)

BOGOTA3(config)#router ospf 1

BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 1

BOGOTA3(config-router)#no auto-summary

Paso 3: Configurar en el router ISP una ruta estatica dirigida hacia MEDELLIN1 y BOGOTA1

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de ISP, MEDELLIN1 y BOGOTA1.

- ISP

ISP>enable

ISP#configure terminal

ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/3/0

ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/3/1

ISP(config)#ip route 172.29.4.128 255.255.255.128 s0/3/0

ISP(config)#ip route 172.29.1.0 255.255.255.0 s0/3/1

ISP(config)#exit

- MEDELLIN 1

MEDELLIN1>enable

MEDELLIN1#configure terminal

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

MEDELLIN1(config)#exit

- BOGOTA 1 (B1)

BOGOTA1>enable

BOGOTA1#configure terminal

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

BOGOTA1(config)#exit

7.6 PARTE 4: TABLA DE ENRUTAMIENTO

Paso 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Para realizar la verificación del enrutamiento en cada uno de los routers utilizaremos el comando show ip route, este nos permitirá ver como quedo el enrutamiento. La verificacion se puede realizar por medio de envio de paquetes para verificar redes y rutas.

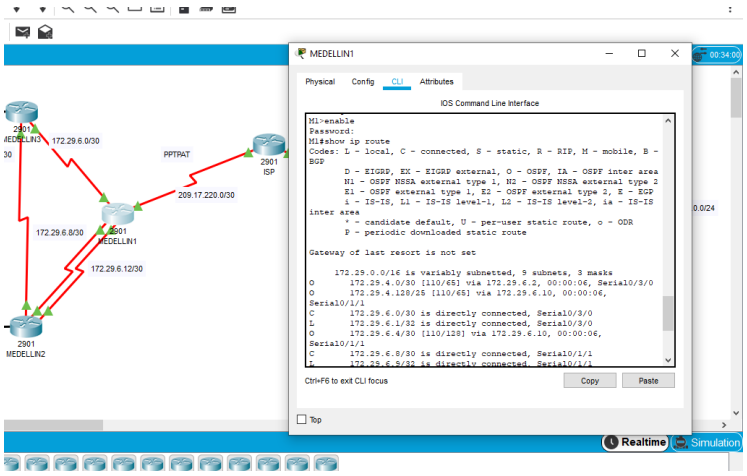

Ilustración 45 Verificación del enrutamiento en M1

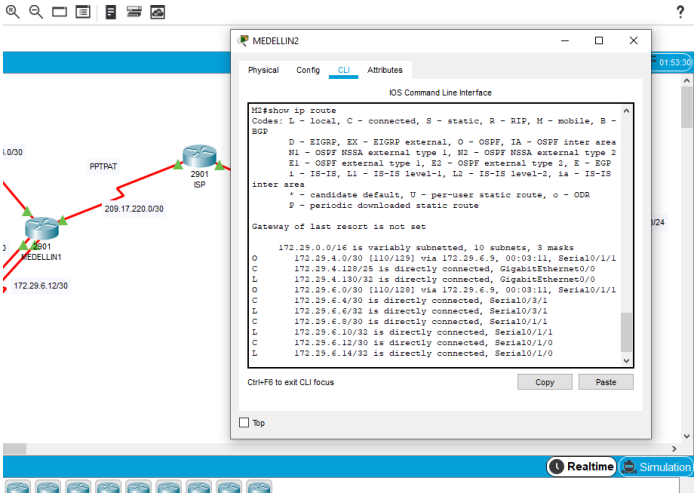

Ilustración 46 Verificación del enrutamiento en M2

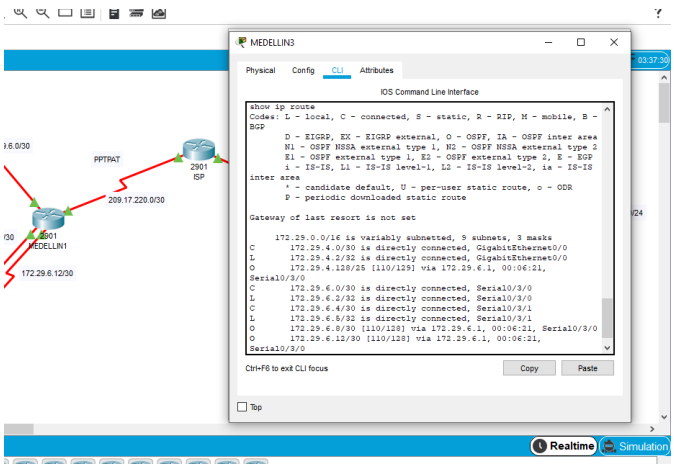

Ilustración 47 Verificación del enrutamiento en M3

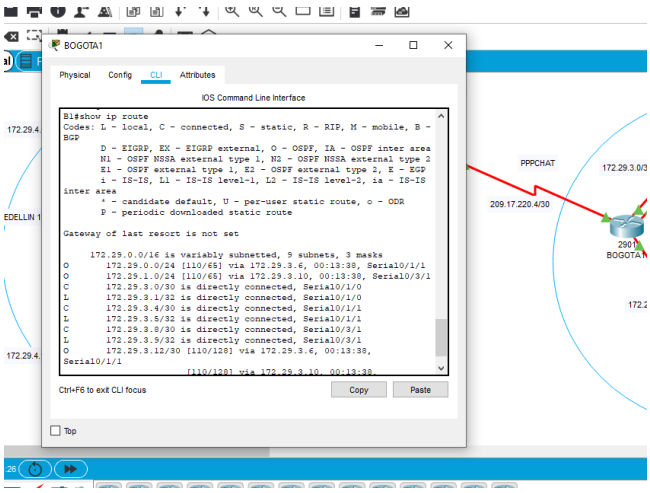

Ilustración 48 Verificación del enrutamiento en B1

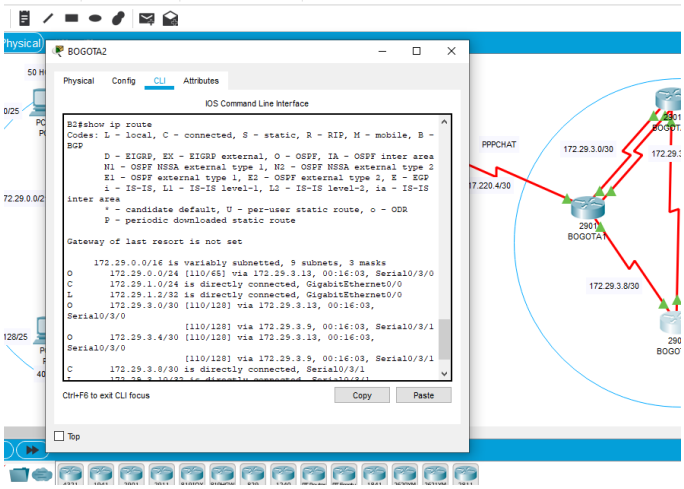

Ilustración 49 Verificación del enrutamiento en B2

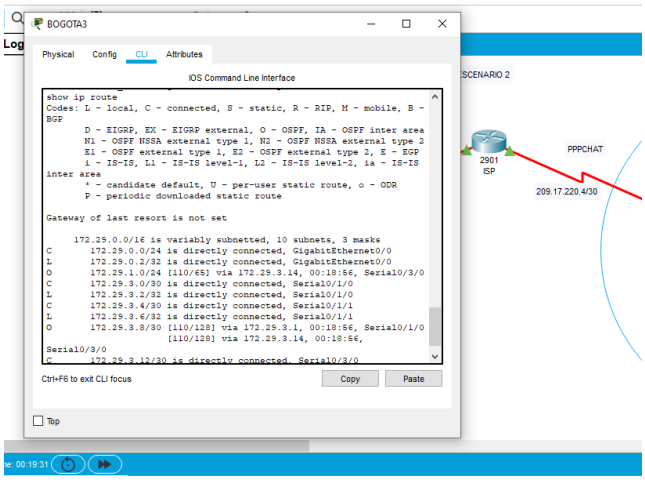

Ilustración 50 Verificación del enrutamiento en B3

Paso 2: Verificar el balanceo de carga que presentan los routers.

La verificacion del balanceo de cargas se ve en las conexiones dobles en donde se balancea el envio de informacion tambien lo podemos ver en las rutas delos router con mas de una conexión. Como por ejemplo medellin 1 donde en la ruta 172.29.6.4/30 encontramos e rutas de transito de informacion por medio del comando **show ip route.**

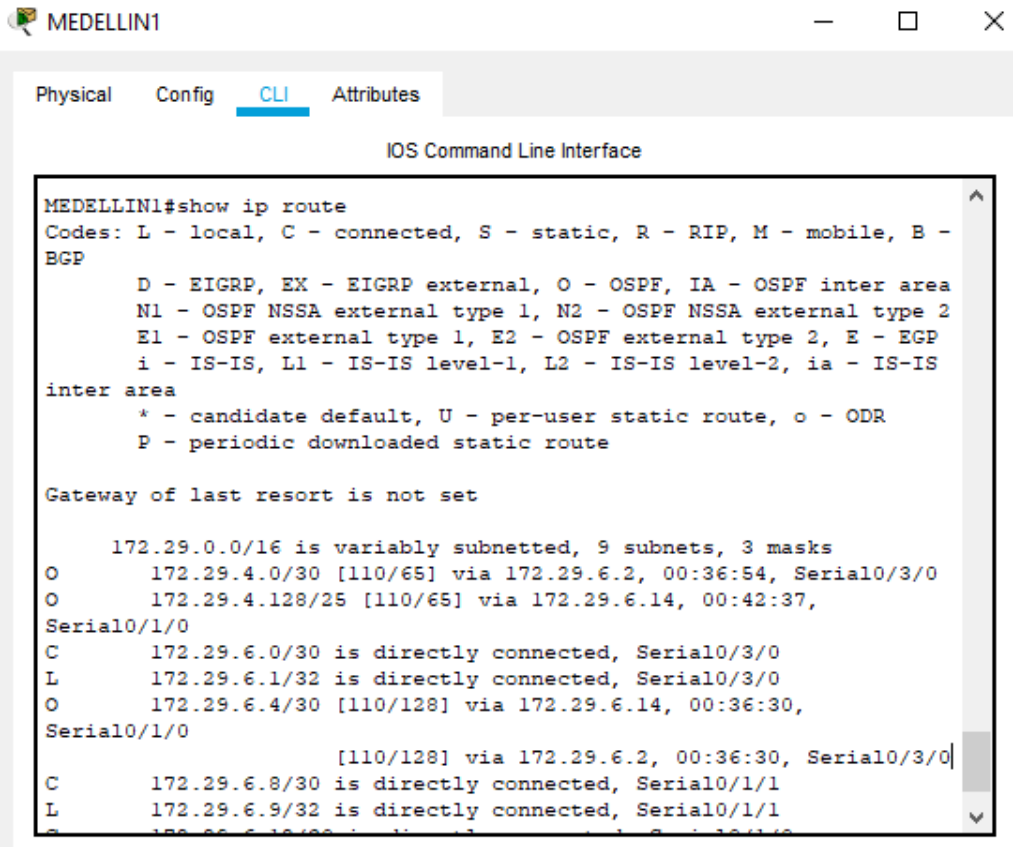

Ilustración 51 Verificación de balanceo de cargas en MEDELLIN 1

Paso 3: Verificar que en los routers Bogotá1 y Medellín1 hay cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Si, podemos observar que Bogotá1 y Medellín1son redes iguales, en numero de conexiones, ya que estas se conectan a igual numero de routers y al mismo tiempo se conectan con el router ISP.

Paso 4: Verificar que en los routers Medellín2 y Bogotá2 también se presentan redes conectadas directamente y recibidas mediante OSPF.

Por medio del comando show ip route podemos verificar que efectivamente en los router Medellin 2 y Bogota 2 también se presentan redes conectadas directamente.

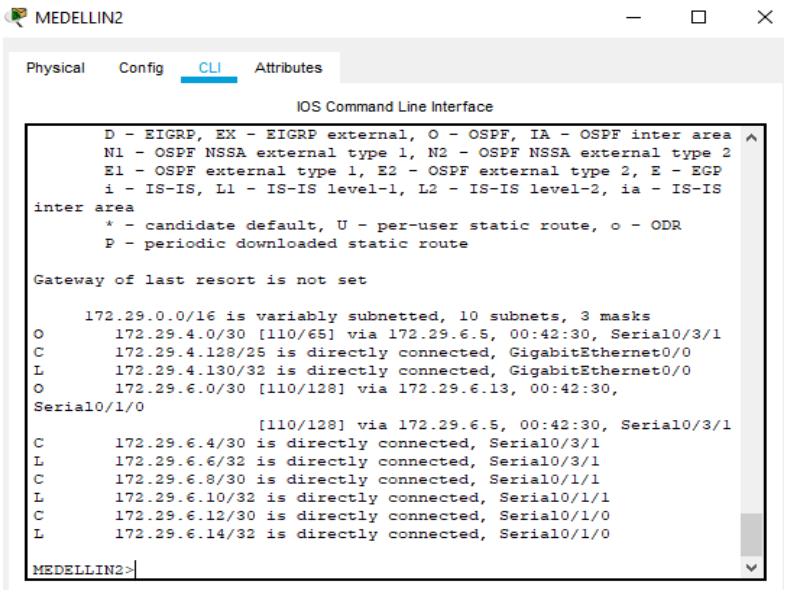

Ilustración 52 Verificación de las redes conectadas y recibidas por OSPF en M2

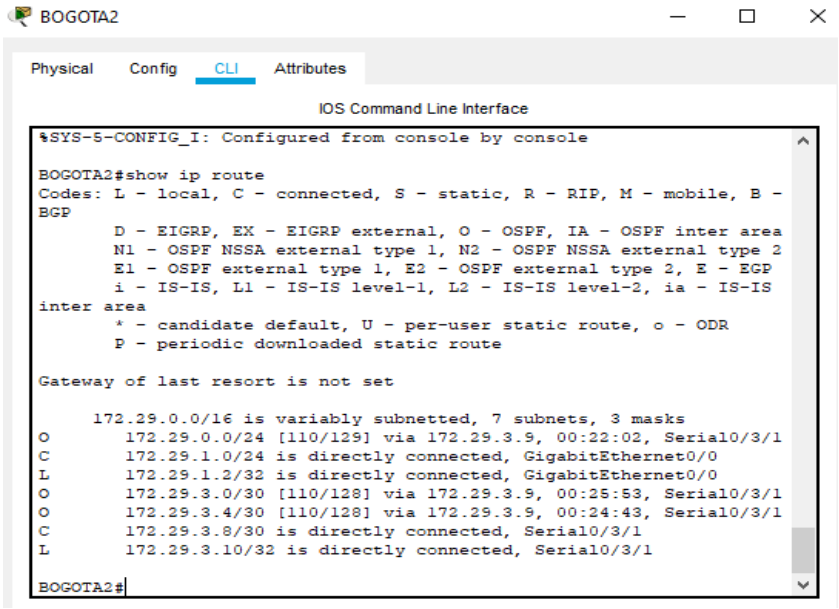

Ilustración 53 Verificación de las redes conectadas y recibidas por OSPF en B2

Paso 5: Verificar que las tablas de los router restantes permiten visualizar rutas redundantes para el caso de la ruta por defecto.

Por medio del codigo show ip route se puede observar en medellin 3 y bogota 3

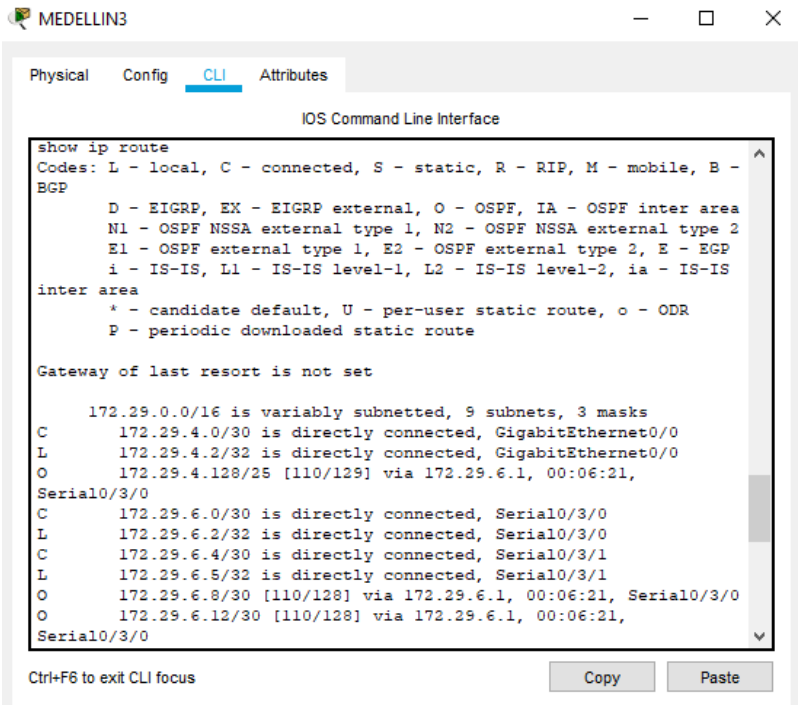

Ilustración 54 Verificación de las rutas redundantes en M3

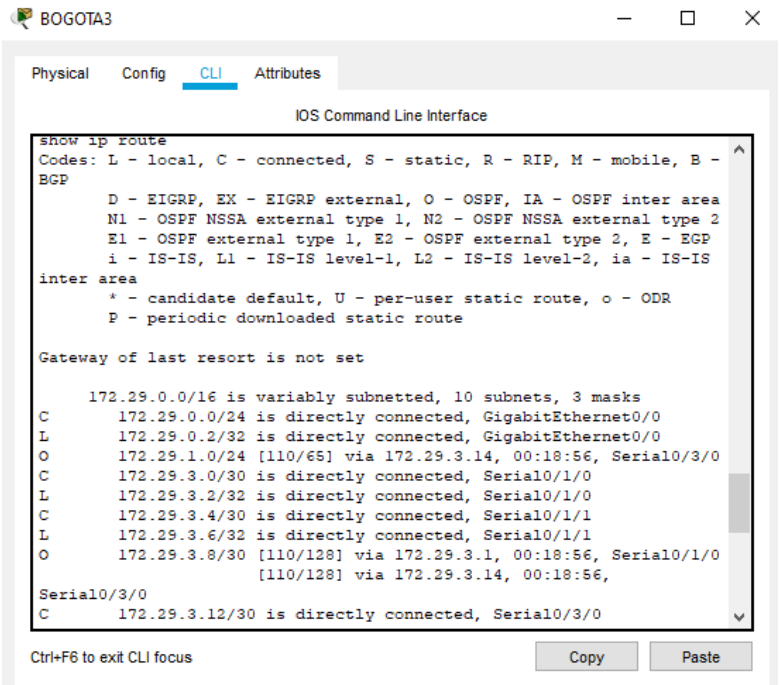

Ilustración 55 Verificación de las rutas redundantes en B3

Paso 6: Verificar que el router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Efectivamente el router ISP se configuro desde el inicio por medio de las interfaces pasivas para que solo indicara las rutas directamente conectadas en la zona de medellin y en la zona de bogota.

7.7 PARTE 5: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

Paso 1: Deshabilitar la propagación del protocolo OSPF

Para no propagar las publicaciones por interfaces que no lo requieran en la siguiente tabla se indican las interfaces de cada Router que no necesitan desactivación.

Este procedimiento se desactivo previamente en la tercera parte, cuando se realizaron las configuraciones y asignaciones de los puertos seriales.

ROUTER	INTERFAZ
Bogota1	SERIAL0/3/0; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/3/0; SERIAL0/3/1
Bogota3	SERIAL0/1/0; SERIAL0/1/1; SERIAL0/3/0
Medellín1	SERIAL0/3/0; SERIAL0/1/1; SERIAL0/1/1
Medellín2	SERIAL0/3/0; SERIAL0/3/1
Medellín3	SERIAL0/1/0; SERIAL0/1/1; SERIAL0/3/0
ISP	No lo requiere

Tabla 23 Des habilitación de los puertos seriales.

7.8 PARTE 6: VERIFICAR EL PROTOCOLO OSPF.

Paso 1: 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.

El comando passive-interface evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente

MEDELLIN2(config)# Do show ip route connected para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. Se utilizará el comando passiveinterface.Para configurar una única interfaz como pasiva. También Configurará OSPF Para que todas las interfaces del Router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

Paso 2: 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.

Esta verificacion se realizara en casi todos los routers excepto en el router ISP, por medio del commando do show ip route connected. Podemos apreciar las rutas que están conectadas con su dirección IP y el puerto de conexión.

- MEDELLIN 1 (M1)

MEDELLIN1#configure terminal

MEDELLIN1(config)# Router ospf 1

MEDELLIN1(config)# Do show ip route connected

Ilustración 56 Verificación de OSPF en M1

- MEDELLIN 2

MEDELLIN2#configure terminal

MEDELLIN2(config)# Router ospf 1

Ilustración 57 Verificación de OSPF en M2

- MEDELLIN 3

MEDELLIN3#configure terminal

MEDELLIN3(config)# Router ospf 1

MEDELLIN3(config)# Do show ip route connected

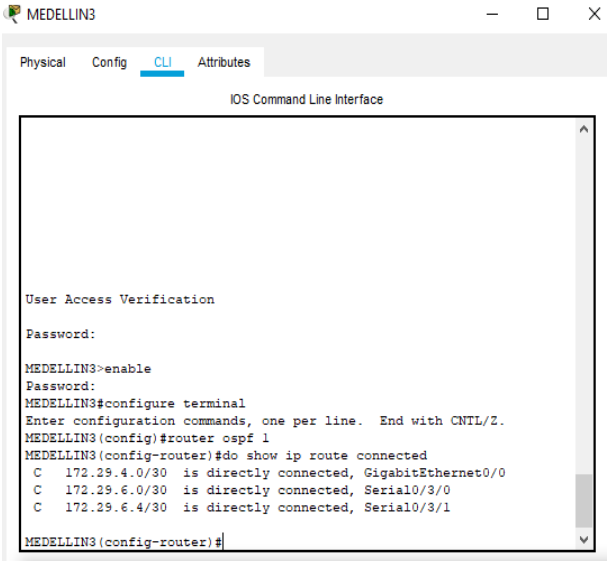

Ilustración 58 Verificación de OSPF en M3

- BOGOTA 1

BOGOTA1#configure terminal

BOGOTA1(config)# Router ospf 1

BOGOTA1(config)# Do show ip route connected

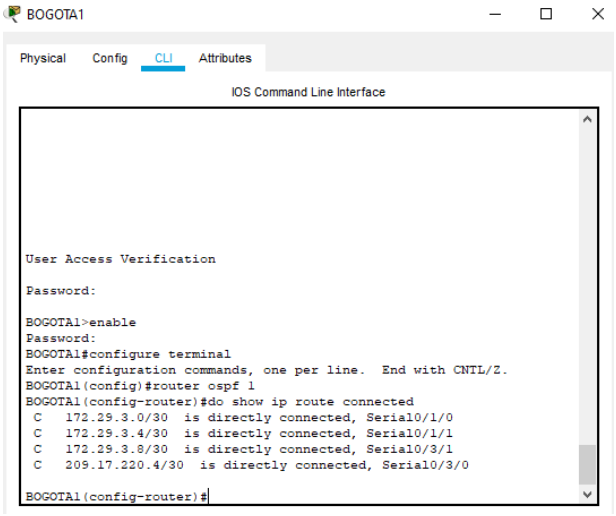

Ilustración 59 Verificación de OSPF en B1

- BOGOTA 2 (B2)

BOGOTA2#configure terminal

BOGOTA2(config)# Router ospf 1

BOGOTA2(config)# Do show ip route connected

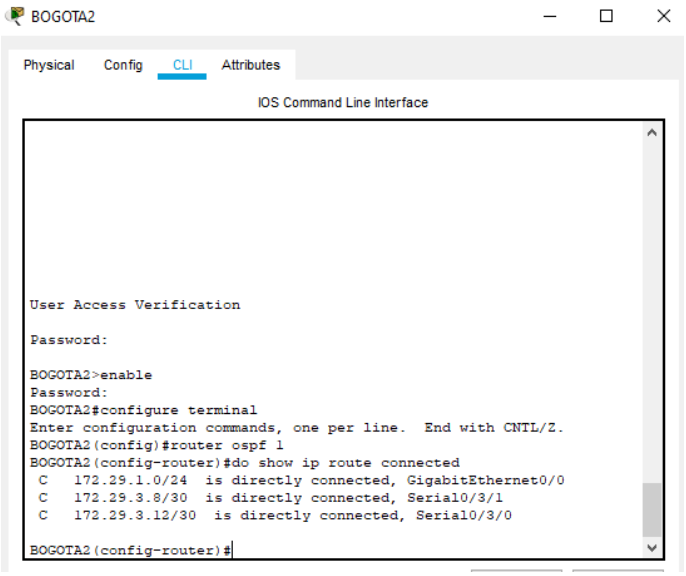

Ilustración 60 Verificación de OSPF en B2

- BOGOTA 3 (B3)

BOGOTA3#configure terminal

BOGOTA3(config)# Router ospf 1

BOGOTA3(config)# Do show ip route connected

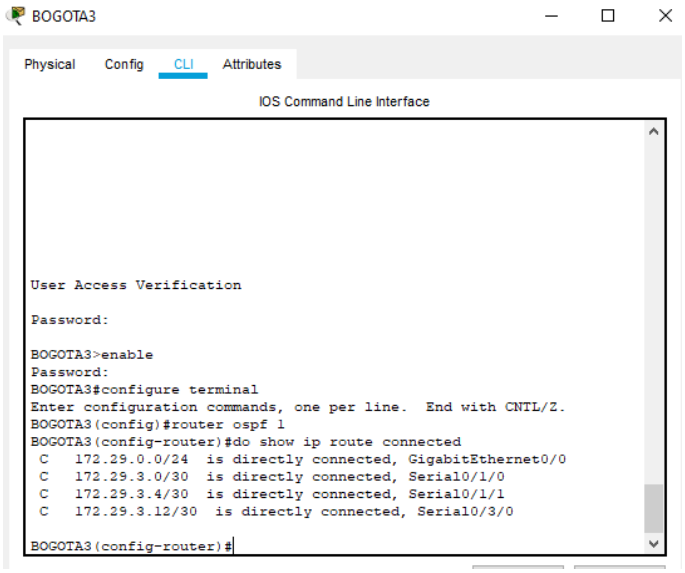

Ilustración 61 Verificación de OSPF en B3

En las figuras podemos apreciar las rutas que están conectadas con su dirección IP y el puerto de conexión.

7.8 PARTE 7: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

Paso 1: Según la topología se requiere que el enlace Medellín1 (M1) con ISP sea configurado con autenticación PAT.

- ISP

ISP(config)#Configure terminal

ISP(config)#Int s0/3/0

ISP(config)#Encapsulation pp

ISP(config)#Ppp pap sent-username ISP password cisco

IPS(config)#exit

- MEDELLIN1

MEDELLIN1(config)#Configure terminal

MEDELLIN1(config)#Int s0/3/1

MEDELLIN1(config)#Encapsulation ppp

MEDELLIN1(config)#Ppp authentication pap

MEDELLIN1(config)#Ppp pap sent-username ISP password cisco

MEDELLIN1(config)#exit

Paso 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Para realizar este paso, se realizarán configuraciones tanto en el router ISP como en BOGOTA 1. A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router ISP Y BOGOTA 1.

- BOGOTA 1

BOGOTA1 (config)#configure terminal

BOGOTA1 (config)#username ISP password cisco

BOGOTA1 (config)#Interface s0/3/0

BOGOTA1 (config)#encapsulation ppp

BOGOTA1 (config)#ppp authentication chap

BOGOTA1 (config)#exit

- ISP

ISP(config)#Configure terminal

ISP(config)#Interface s0/3/0

ISP(config)#encapsulation ppp

ISP(config)#ppp authentication chap

ISP(config)#exit

7.9 PARTE 8: CONFIGURACIÓN DE PAT.

Paso 1: 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.

- MEDELLIN1

MEDELLIN1(config)# Ip nat inside source list 1 interface s0/3/1 overload
MEDELLIN1(config)# Access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)# Int s0/3/0
MEDELLIN1(config)# Ip nat outside
MEDELLIN1(config)# Int s0/3/1
MEDELLIN1(config)# Ip nat outside
MEDELLIN1(config)# Int s0/1/0
MEDELLIN1(config)# Ip nat outside
MEDELLIN1(config)# Int s0/1/1
MEDELLIN1(config)# Ip nat outside

- BOGOTA1

BOGOTA1(config)# Ip nat inside source list 1 interface s0/3/0 overload
BOGOTA1(config)# Access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#Interface s0/3/0
BOGOTA1(config)# Ip nat outside
BOGOTA1(config)# Int s0/3/1
BOGOTA1(config)# Ip nat outside
BOGOTA1(config)# Int s0/1/0
BOGOTA1(config)# Ip nat outside
BOGOTA1(config)# Int s0/1/1
BOGOTA1(config)# Ip nat outside

Paso 2: Verificar lo indicado en el paso anterior, luego 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 0/3/0 del router Medellín1, cómo diferente puerto

Paso 3: 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 0/3/0 del router Bogotá1, cómo diferente puerto.

7.10 PARTE 9: CONFIGURACIÓN DEL SERVICIO DHCP.

Paso 1: Configurar la red Medellín2 y Medellín3 donde el Router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.

A continuación, se muestran los comandos para realizar la configuración DHCP en MEDELLIN2 y MEDELLIN3,

- MEDELLIN 2

```
MEDELLIN2(config)# Ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2 (config)# Ip dhcp excluded-address 172.29.4.129 172.29.4.133
MEDELLIN2 (config)# Ip dhcp pool M2
MEDELLIN2 (config)# Network 172.29.4.0 255.255.255.128
MEDELLIN2 (config)# Default-router 172.29.4.1
MEDELLIN2 (config)# Dns-server 5.5.5.5
MEDELLIN2 (config)# exit
MEDELLIN2 (config)# Ip dhcp pool M3
MEDELLIN2 (config)# Network 172.29.4.128 255.255.255.128
MEDELLIN2 (config)# Default-router 172.29.4.129
MEDELLIN2 (config)# Dns-server 5.5.5.5
MEDELLIN2 (config)# Dns-server 5.5.5.5
```

Paso 2: El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

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

Paso 3: Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

Comprobamos configuración DHCP en PC0

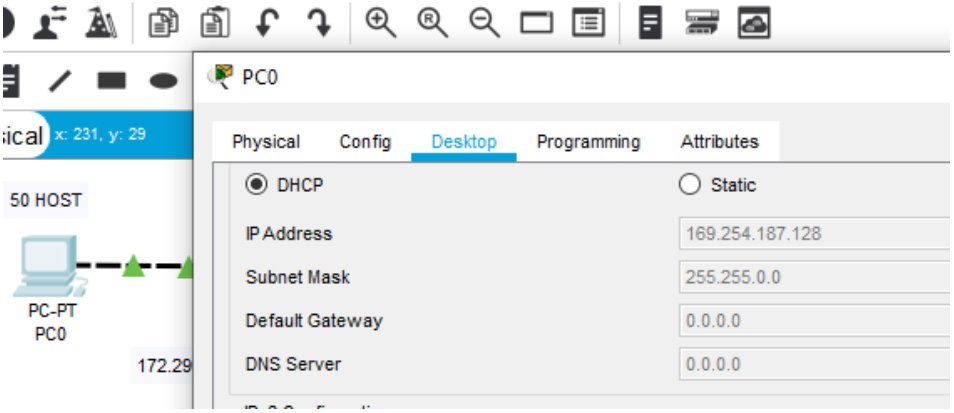

Ilustración 62 Verificación de configuración DHCP en PC0

Comprobamos configuración DHCP en PC1

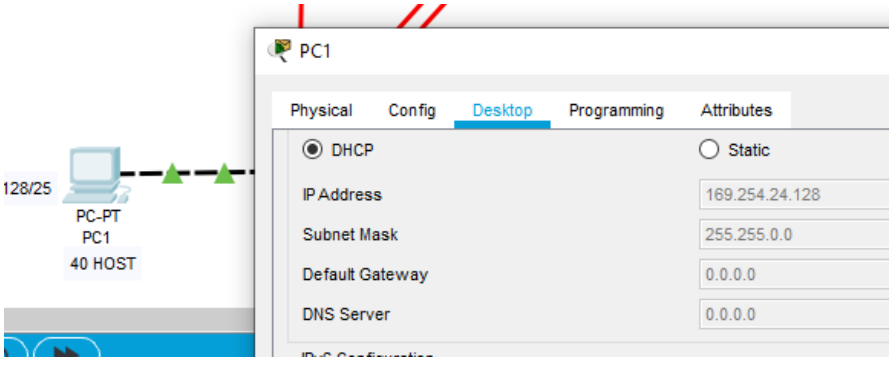

Ilustración 63 Verificación de configuración DHCP en PC1

Comprobamos configuración DHCP en PC3

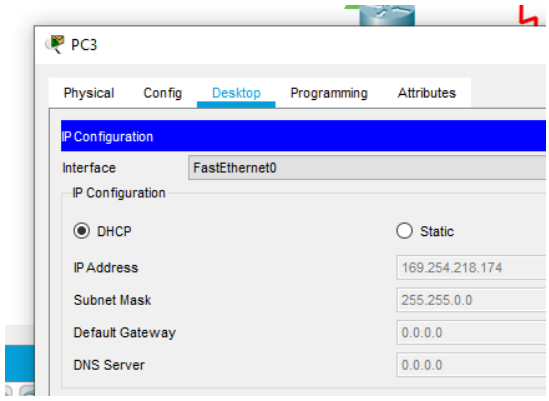

Ilustración 64 Verificación de configuración DHCP en PC3

Comprobamos configuración DHCP en PC2

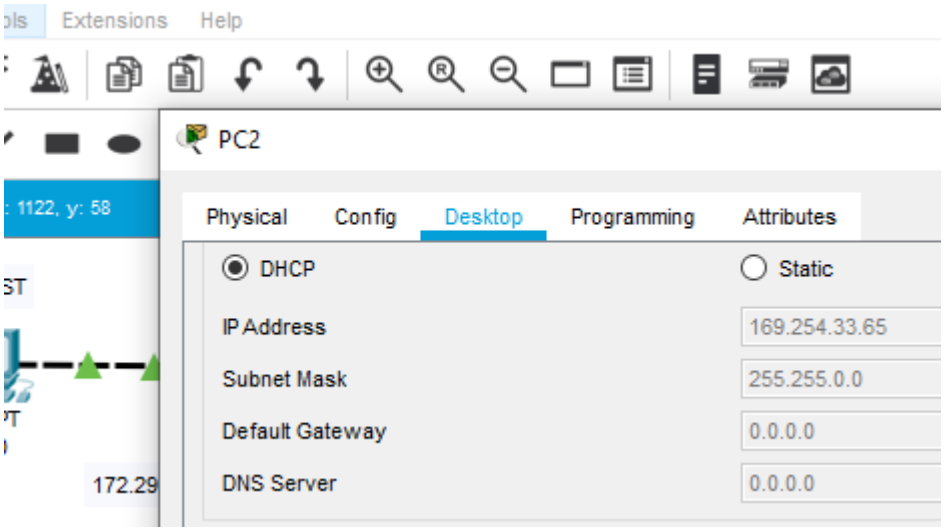

Ilustración 65 Verificación de configuración DHCP en PC2

Paso 4: Configure el Router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del Router Bogotá2.

- **BOGOTA 2**

BOGOTA2(config)# Ip dhcp excluded-address 172.29.1..1 172.29.1.5

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

BOGOTA2(config)# Ip dhcp pool BOGOTA2

BOGOTA2(config)# Network 172.29.1.0 255.255.255.0
BOGOTA2(config)# Default-router 172.29.0.1
BOGOTA2(config)# Dns-server 5.5.5.5
BOGOTA2(config)#exit
BOGOTA2(config)#Ip dhcp pool BOGOTA3
BOGOTA2(config)#Network 172.29.4.128 255.255.255.128
BOGOTA2(config)#Default-router 172.29.0.1
BOGOTA2(config)#Dns-server 5.5.5.5
BOGOTA2(config)#exit

- **BOGOTA 3**

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

CONCLUSIONES

Con el desarrollo de los escenarios identificamos, analizamos y configuramos una Red de Comunicaciones implementando proocolos de seguridad como el protocolo OSPF (Open Shortest Path First) que es un protocolo de routing de estado de enlace para las redes IP y este se definió OSPFv2 para redes IPv4, para detectar fallas de enlace y de seguridad en los dispositivos, haciendo que estos no sean vulnerables a amenazas.

Se comprendió la importancia de las configuraciones básicas de los dispositivos que componen una red de Comunicaciones, como es el caso de los Routers, Switch, PC'S. Ya que sin estas previas configuraciones sería más difícil dar solución a los escenarios propuestos.

Se desarrollaron los escenarios simulando a través de la herramienta Packet Tracer, el cual es un programa fácil de comprender y dominar

Se practicaron las habilidades y conocimientos adquiridos en networking, frente a la solución de problemas de configuración de redes.

BIBLIOGRAFIA

Temática: Configuración y conceptos básicos de Switching CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0 .1.1

Temática: VLANs CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0 .1.1

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

REFERENCIAS

[1] WIKIPEDIA. (s.f.) ACL. Recuperado de https://es.wikipedia.org/wiki/Lista_de_control_de_acceso#:~:text=Las%20ACL%20permiten%20controlar%20el,de%20acuerdo%20a%20alguna%20condici%C3%B3n.&text=Tanto%20servidores%20individuales%20como%20enrutadores%20pueden%20tener%20ACL%20de%20redes.

[2] CCNA. *DHCP*. Recuperado de https://www.CCNA.coma

[3]. NAT ESTATICA. Recuperado de https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona

[4] XATAKA. NAT DINAMICA. Recuperado de https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona

[5] ECURED. NTP. Recuperado de https://www.ecured.cu/NTP

[6] Enrutamiento dinámico OSPF con Packet Tracer. OSPF. Recuperado de https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer

[7] WIKIPEDIA (s.f) PPP (Point-to-Point Protocol). Recuperado de https://es.wikipedia.org/wiki/PointtoPoint_Protocol#:~:text=Protocolo%20punto%20a%20punto%20(PPP)%20(en%20ingl%C3%A9s%20Point%2D,dos%20nodos%20de%20una%20red.

[8] XAKATA. PAT. Recuperado de https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona

[9] HERRAMIENTAS WEB. RIP, Recuperado de https://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html

[10] WIKIPEDIA. (s.f.). *VLAN*. Recuperado de http://redestelematicas.com/

[11] MONOGRAFIAS. Redes y Comunicaciones. Recuperado de: https://www.monografias.com/trabajos-pdf2/redes-comunicaciones/redes-comunicaciones.pdf

[12] WIKIPEDIA.PROTOCOLOS DE RED. Recuperado de: https://es.wikipedia.org/wiki/Anexo:Protocolos_de_red#:~:text=Un%20protocolo%20de%20red%20designa,de%20una%20red%20de%20computadoras.