SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

MATEO ALLAN ECHEVERRI

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA EN ELECTRONICA
DOSQUEBRADAS - RISARALDA
2020

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

MATEO ALLAN ECHEVERRI

DIPLOMADO DE PROFUNDIZACIÓN CISCO DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES WAN/LAN

TUTOR:
DIEGO EDINSON RAMIREZ CLAROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA EN ELECTRONICA
DOSQUEBRADAS – RISARALDA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Dosquebradas, 29/05/2020

DEDICATORIA

Dedico este trabajo a mis padres quienes han sido grandes partícipes de este proceso tan arduo y extenso, también quiero dedicarlo a mi familia en general quienes han representado igualmente un gran apoyo para culminar con éxitos esta etapa de mi vida.

AGRADECIMIENTOS

Primero que todo quiero dar gracias Dios por todas las bendiciones recibidas, entre ellas el poder finalizar con éxito este camino tan arduo como estudiante; a mis padres que son un ejemplo a seguir y quienes han sido un gran apoyo en este recorrido. Agradezco a mi familia en general porque me han brindado de igual manera ese apoyo incondicional en todo momento, a mis compañeros de estudios quienes han representado un pilar importante en mi carrera, a mis tutores y directivos de curso quienes me han brindado su asesoría en los momentos en que se presentan dudas e inconvenientes, en general agradezco a esta gran comunidad denominada UNAD, Universidad Nacional Abierta y a Distancia.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pag.

LISTA DE GRÁFICAS

Pág

LISTA DE FIGURAS

Pag.

GLOSARIO

DHCP: El protocolo de configuración dinámica de host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP

PAP: son las siglas de Password Authentication Protocol un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet

CHAP: Es un método de autenticación remota o inalámbrica. Diversos proveedores de servicios emplean CHAP.

VLAN: Es el acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

SUMARIZACION: La sumarización de rutas es una técnica empleada en enrutamiento IP avanzado que permite sintetizar múltiples rutas IP contiguas en una única ruta.

OSPF: Es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol, que usa el algoritmo para calcular la ruta más corta entre dos nodos.

RIP: Es un protocolo de puerta de enlace interna o interior utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol a las que se encuentran conectados.

RESUMEN

A través del acuerdo realizado entre la UNAD y Academia CISCO Networking, se pretendió realizar el diplomado de profundización en el cual se pretende fortalecer las competencias de los estudiantes guiados hacia la implementación de redes que busca la solución LAN y WAN, donde los estudiantes afianzarán los conocimientos en este campo.

En la plataforma de Cisco Networking se realizarán una serie de evaluaciones concretas en donde el estudiante tendrá un tiempo de 2 horas y media para responderlas donde se evalúan los temas consignados en los diferentes capítulos de la plataforma, además también se realizarán una serie de trabajos colaborativos a través de la plataforma de la UNAD donde el tutor encargado y el director del curso, evaluarán el contenido de los mismos.

ABSTRACT

Through the agreement made between the UNAD and the CISCO Networking Academy, it is intended to carry out the deepening diploma in which it is intended to strengthen the competences of the students guided towards the implementation of networks that the LAN and WAN solution seeks, where the students will strengthen the knowledge in this field.

In the Cisco Networking platform, a series of specific evaluations will be carried out, where the student will have a time of 2 and a half hours to answer them, where the topics included in the different titles of the platform will be evaluated, and a series of collaborative works will also be carried out. through the UNAD platform where the tutor in charge and the course director, evacuate their content.

PALABRAS CLAVE: Prueba de habilidades, Trabajo final diplomado profundización, Proyecto de Grado

1. INTRODUCCIÓN

Las telecomunicaciones y las nuevas técnicas de información y comunicación han tomado un inalcanzable avance siendo papel indispensable para el desarrollo de la humanidad. La educación cumple el rol fundamental para la orientación e implantación de esta nueva evolución en cuanto a la tecnología, para la muestra u botón la UNAD ha brindado la oportunidad de que el estudiante tenga contacto con la realidad a través de lo virtual en este aspecto desarrollando el presente Caso de Estudio, donde se pone en práctica los conocimientos adquiridos en el transcurso del desarrollo de este seminario de profundización.

Se configuran servidores DHCP, el cual es un protocolo de difusión que trabaja de forma predeterminada en donde sus paquetes no pasan a través de enrutadores. Un agente de retransmisión DHCP recibe cualquier difusión DHCP de la subred y la reenvía a la dirección IP especificada en una subred distinta. La meta es profundizar en la conformación de redes de datos especialmente “Internet” y para ello se describen los dispositivos utilizados para una red y se explican con la simulación en el programa Packet Tracer como es el intercambio de paquetes y a la vez permite observar el comportamiento de la red creada.

Este entorno es la base para el aprendizaje del estudiante porque desarrolla las habilidades que necesita en esta sociedad tan acelerada en cuanto a toma de decisiones, pensamiento crítico, innovador siempre buscando dar solución a dificultades presentadas en todos los ámbitos de la vida diaria.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Analizar los casos de estudio CCNA1 Y CCNA2 asignados implementando soluciones integradas LAN-WAN mediante la utilización de la herramienta de simulación Packet Tracer.

2.2 OBJETIVOS ESPECÍFICOS

Diseñar las topologías de los casos de estudio CCNA1 Y CCNA2 utilizando PKT.

Conectar y configurar redes utilizando los comandos IOS de Cisco para Routers y Switches.

Facilitar la conectividad entre los dispositivos de las redes realizando la sumarización de las mismas

Conectar dispositivos y desarrollar un esquema de direccionamiento y prueba.

Determinar la cantidad de Host y Subredes de una red.

Diferenciar los diferentes tipos de protocolos empleados en cada escenario.

Configurar los diferentes enrutamientos en cada dispositivo de las redes planteadas.

Determinar la mejor ruta de un Router en un diagrama de redes.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Para entrar en contexto en cuanto a lo que se va a realizar, se requiere solucionar dos problemas reflejados en dos escenarios respectivamente, donde se describen una serie de pasos a seguir para desarrollar de forma correcta dos escenarios que serán configurados en dos protocolos completamente diferentes, uno es mediante RIP y el otro mediante enrutamiento OSPF. En el primer escenario se trabajaran con redes IPv4 e IPv6, mientras que en el segundo escenario solo se emplearán las redes IPv4 respectivamente.

3.2 JUSTIFICACIÓN

Las redes es nuestro tema en el diario vivir desde el más pobre hasta el más rico, este fenómeno no conoce clero, raza, ni límites geográficos. Es por ello que las redes hoy día representan un avance tecnológico muy importante, hacen parte de nuestras vidas, procuramos que la mayoría de las tareas que realizamos estén en la red disponible para todo el que lo requiera, (moda, alimentación, salud, diversión, trabajo, educación etc.…), por ejemplo, se puede ver que la falta de tiempo, no es una excusa para empezar un proceso de estudio, en la actualidad existe un gran número de instituciones virtuales como la reconocida cisco Networking que ofrece la tecnología de la información y la comunicación (TIC), para mejorar las competencias de carreras y las oportunidades económicas en todo el mundo, promueven la educación a distancia, facilitando que las personas obtengan sus títulos sin tener que salir de la casa y desde cualquier parte del mundo. En este trabajo se analizarán muchos de los dispositivos que hacen posible esta comunicación, entre ellos el Switch, que es el más utilizado para interconectar redes de área local; Firewall, que proporciona seguridad a las redes; Router, que ayuda a direccionar mensajes mientras viajan a través de la red, entre otros.

4. MARCO TEÓRICO

Vamos a empezar hablando sobre los protocolos de enrutamiento, los cuales se definen como una herramienta que permite la comunicación entre los router. La configuración permite a estos equipos seleccionar la ruta que tomara un paquete entre dos nodos en una red de computadores. Los routers sólo conocen las redes conectadas directamente a ellos y a través de los protocolos de enrutamiento los routers anuncian estas redes a los vecinos en primera instancia y luego al resto de equipos de la red, de tal forma los routers adquieren el conocimiento de la topología de la red.

Los diferentes protocolos de enteramientos activos son:

- RIP (Routing Information Protocol): es uno de los protocolos más antiguos y es ampliamente usado en la actualidad. RIP es un protocolo que tiene como base un vector distancia que usa como métrica el conteo de saltos. este protocolo previene los loops a través de la implementación de un numero límite de saltos permitidos en los caminos de origen y destino

- OSPF (Open Short est Path First): OSPF es un protocolo de enrutamiento con dos características relevantes, es un protocolo libre y está basado en el algoritmo de la ruta más corta primero (ShortestPathFirsó SPF). Este es un protocolo basado en el estado de la conexión el cual solicita el envío de los avisos de estado de conexión (Link-StateAdvertisementsóLSAs) a todos los demás routers que se encuentra en la misma área jerárquica. La informacion de las interfaces conectadas, las métricas usadas y otras variables son incluidas en los LSAs de OSPF. Debido a que este protocolo acumula información de los estados de conexión, este utiliza el algoritmo SPF para el cálculo del camino mas corto hacia cada nodo.

- IS-IS (Instermediante system to intermediate system): Este es un protocolo de enrutamiento de estado de conexión. Opera de manera segura enviando información de la topología a través de la red de Routers. Los paquetes se envían por el mejor camino que posee el router de la topología de la red. IS-IS es un IGP (Internal Gateway Protocol), creado para el uso de un único administrador de dominio o solo una red.

- EIGRP (Enhanced Interior Gateway Routing Protocol): Este es un protocolo propietario de CISCO basado en IGRP (Interior Gateway Routing Protocol). EIGRP es un protocolo de enrutamiento que se basa en vectores distancia con

optimizadores para minimizar la inestabilidad de enrutamiento ante cambios en la topología de la red, el uso de ancho de banda y poder de procesamiento del Router. Los equipos que tengan este tipo de protocolo configurado distribuirán la información de enrutamiento a los vecinos con IGRP. La mayoría de las optimizaciones de enrutamiento están basadas en el Diffusing Update Algorithm (DUAL) quien garantiza la operación libre de Loops y provee una convergencia más rápida de los Router

- BGP (Border Gateway protocol): Este protocolo direcciona el tráfico entre redes o grupo de redes que tiene un mimo administrador y políticas de enrutamiento comunes, también conocidos como sistemas autónomas. El BGP intercambia información de enrutamiento por el internet y es el protocolo usado en las IPS Este es un protocolo robusto y escalable; una evidencia de estas características es el hecho de que es el protocolo empleado utiliza distintos parámetros de rutas, atributos de llamada, para definir las políticas de parámetros de rutas atributos de llamada, para definir las políticas de enrutamiento y mantener un estado estable de enrutamiento. Los equipos configurados con BGP intercambian toda la información de enrutamiento con sus vecinos la primera vez que es establecida la conexión TCP. Cuando se genera algún cambio sobre la tabla de enrutamiento el router tan solo envía las rutas que han cambiado. BGP no realiza actualizaciones periódicas y aquellas que son enviadas solo contienen la ruta óptima para una red de destino.

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Los materiales que se emplearon para dicho trabajo fueron los siguientes:

Simulador de Redes Packet Tracer
Dispositivos como routers, Switches, y PC´S de manera simulada
Computador para poder descargar dicho simulador
Material de apoyo empleado como guía

5.2 METODOLOGÍA

Para el desarrollo del trabajo se desarrollaron principalmente dos protocolos de enrutamiento los cuales son el RIP y el OSPF, el primero empleado para configurar la red del primer escenario propuesto, y el segundo protocolo para configurar la red del segundo escenario respectivamente.

6. DESARROLLO DEL PROYECTO

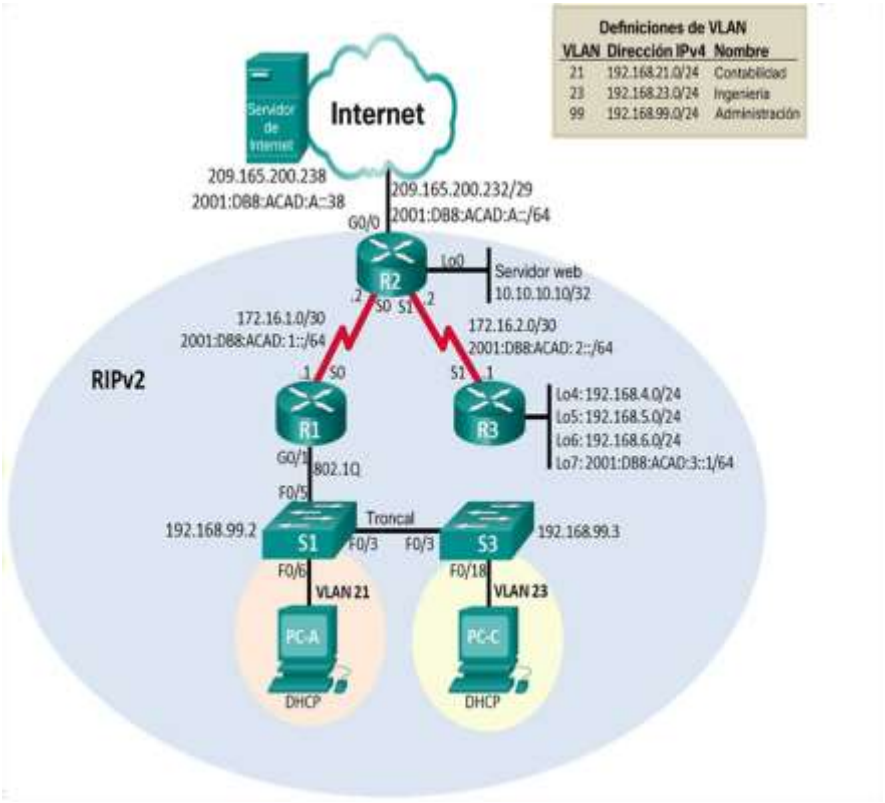
SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

ESCENARIO 1

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

TOPOLOGÍA DE RED

Grafica 1. Topología del scenario 1



Parte 1: Inicializar dispositivos

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla N°1

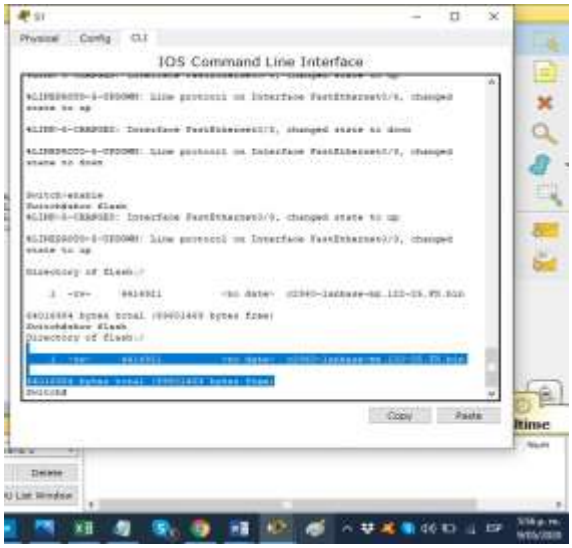
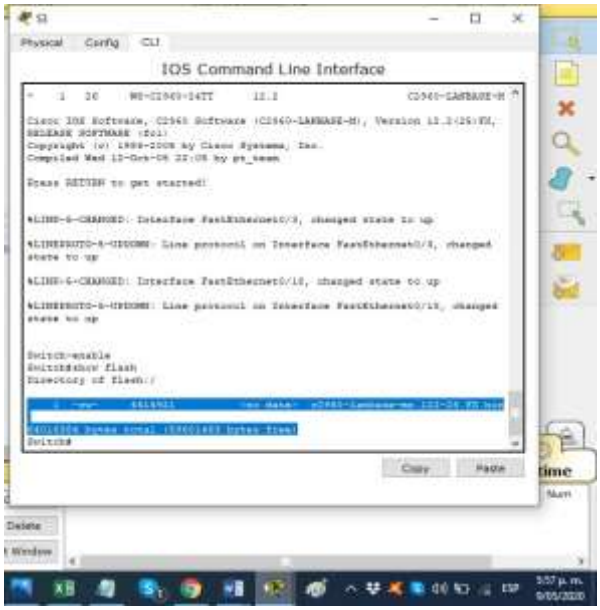
Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash Figura 1. Verificación mediante comando show Flash en S1  Fuente: Allan Echeverri Mateo

	Figura 2. Verificación mediante comando show Flash en S3  Fuente: Allan Echeverri Mateo

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla N°2

Elemento o tarea de configuración	Especificación
Dirección IPv4	Estas direcciones se configuran dentro del servidor web, previamente calculándola dentro de los rangos permitidos para su correcto funcionamiento, ya que de otra manera no permitirá hacer ping a los dispositivos. 209.165.200.238

Máscara de subred para IPv4	Se debe ingresar al servidor para colocarla 255.255.255.48
Gateway predeterminado	Se debe ingresar al servidor para colocarla 209.165.200.233
Dirección IPv6/subred	Se debe ingresar al servidor para colocarla 2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	Se debe ingresar al servidor para colocarla 2001:DB8:ACAD:A::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla N°3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login

Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd %Unauthorized Access is Prohibited!%
Interfaz S0/0/0	R1(config)#interface s0/0/0 R1(config-if)#description conection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla N°4

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2

Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	A pesar de que se introduce el comando **ip http server** packet tracer no lo soporta
Mensaje MOTD	R2(config)#banner motd %Unauthorized Access is Prohibited!%
Interfaz S0/0/0	R2(config)#interface s0/0/0 R2(config-if)#description conection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#interface s0/0/1 R2(config-if)#description conection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#interface g0/0 R2(config-if)#description conection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado)	R2(config-if)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulated Web Server R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla N°5

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd %Unauthorized Access is Prohibited!%

Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#description conection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#interface loopback 4 R3(config-if)#ip addres 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#interface loopback 5 R3(config-if)#ip addres 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#interface loopback 6 R3(config-if)#ip addres 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla N°6

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1

Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)# banner motd %Unauthorized Access is Prohibited!%

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla N°7

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login

Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)# banner motd %Unauthorized Access is Prohibited!%

Paso 7: Verificar la conectividad de la red

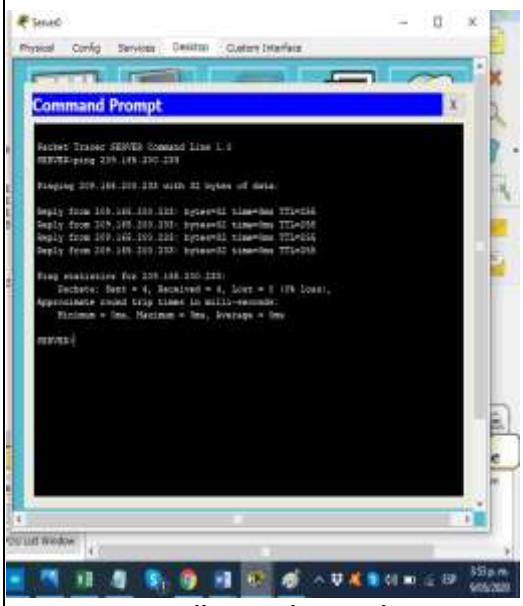
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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

Tabla N°8

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1>enable R1#ping 172.16.1.2 Figura 3. Ping realizado desde R1 a R2 

			Fuente: Allan Echeverri Mateo
R2	R3, S0/0/1	172.16.2.1	R2>enable R2#ping 172.16.2.1 Figura 4. Ping realizado desde R2 a R3  Fuente: Allan Echeverri Mateo
PC de Internet	Gateway predeterminado	209.165.200.233	SERVER>ping 209.165.200.233 Figura 5. Ping realizado desde el servidor

			 Fuente: Allan Echeverri Mateo

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas, donde se busca crear la base de datos VLAN para dichos dispositivos:

Tabla N°9

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1>enable S1#config terminal S1(config)#vlan 21 S1(config-vlan)#name Accounting S1(config-vlan)#vlan 23 S1(config-vlan)#name Engineering S1(config-vlan)#vlan 99 S1(config-vlan)#name Management S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 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 f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2

Apagar todos los puertos sin usar	S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla N°10

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3>enable S3#config terminal S3(config)#vlan 21 S3(config-vlan)#name Accounting S3(config-vlan)#vlan 23 S3(config-vlan)#name Engineering S3(config-vlan)#vlan 99 S3(config-vlan)#name Management 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)#no shutdown 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 f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#interface range f0/1-2, f0/4-24, g0/1-2
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range f0/1-2, f0/4-24, g0/1-2

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

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla N°11

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1>enable R1#config terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#interface g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#interface g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#interface g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

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

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

Tabla N°12

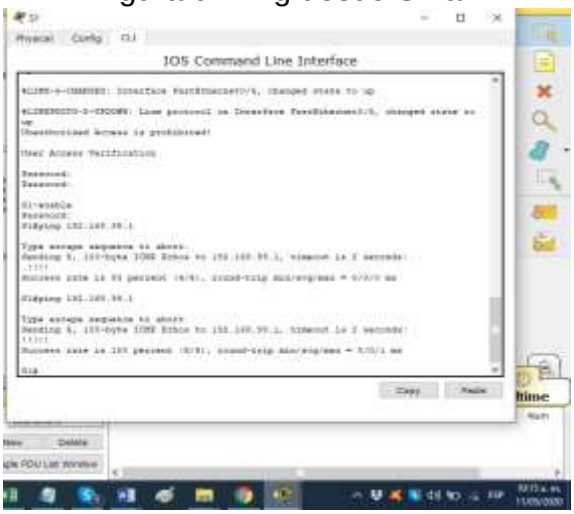
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1>enable S1#ping 192.168.99.1 Figura 6. Ping desde S1 a R1  Fuente: Allan Echeverri Mateo
S3	R1, dirección VLAN 99	192.168.99.1	S3>enable S3#ping 192.168.99.1

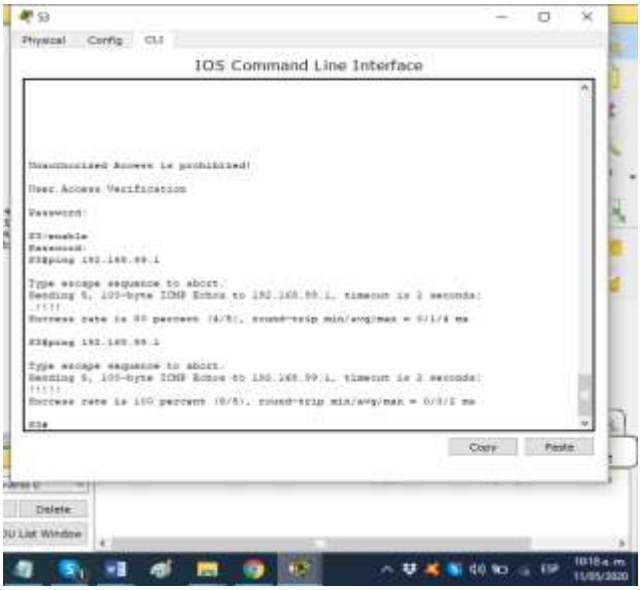
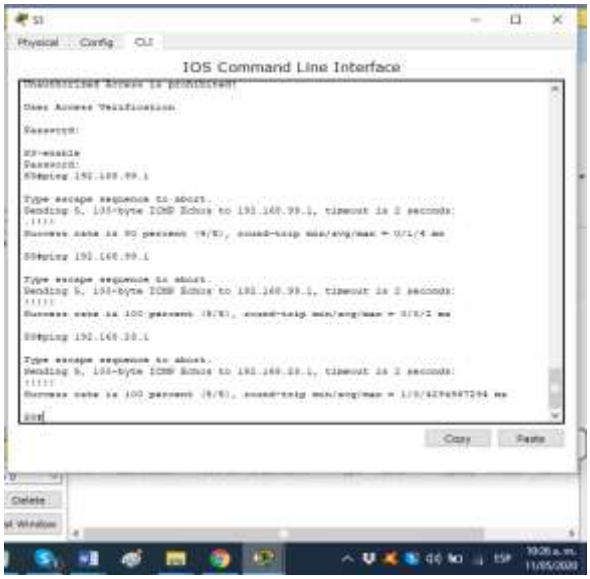
			Figura 7. ping desde S3 a R1  Fuente: Allan Echeverri Mateo
S1	R1, dirección VLAN 21	192.168.21.1	S1>enable S1#ping 192.168.21.1 Figura 8. Ping desde S1  Fuente: Allan Echeverri Mateo
S3	R1, dirección VLAN 23	192.168.23.1	S3>enable S3#ping 192.168.23.1

			Figura 9. Ping desde S3  Fuente: Allan Echeverri Mateo

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla N°13

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1>enable R1#config terminal R1(config)#router rip R1(config-router)#version 2 R1(config-router)#do show ip route connected

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

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla N°14

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2>enable R2#config terminal R2(config)#router rip R2(config-router)#version 2 R2(config-router)#do show ip route connected

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

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas, donde se requiere configurar el protocolo RIP en los dispositivos relacionados a continuación:

Tabla N°15

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3>enable R3#config terminal R3(config)#router rip R3(config-router)#version 2 R3(config-router)#do show ip route connected
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 172.16.4.0 R3(config-router)#network 172.16.5.0 R3(config-router)#network 172.16.6.0

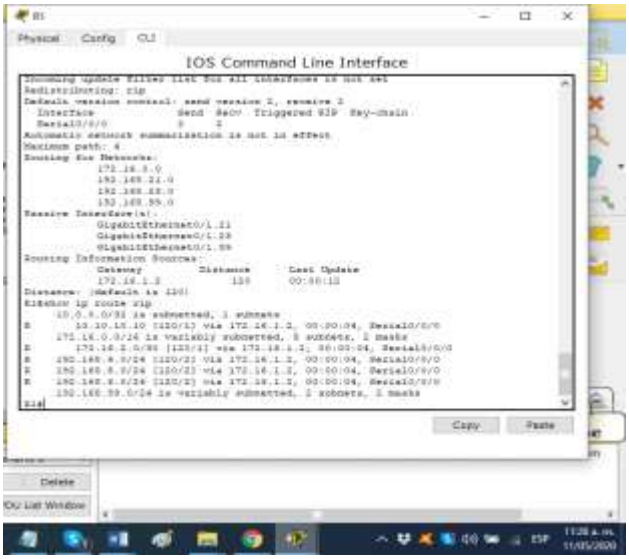
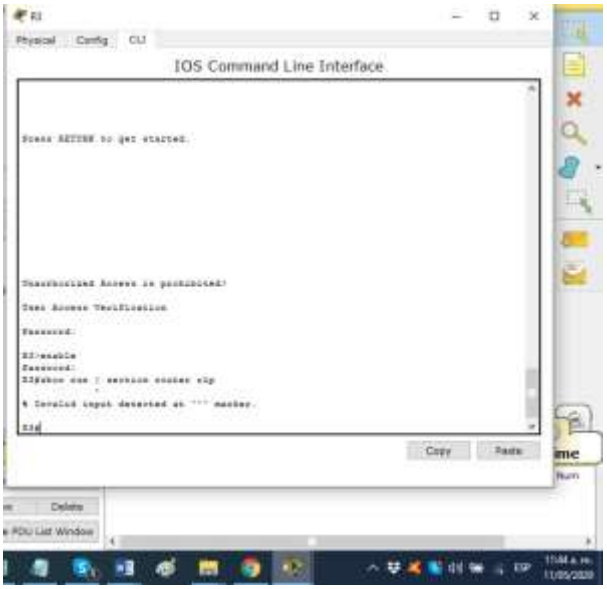
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Paso 4: Verificar la información de RIP

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

Tabla N°16

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 protocol Figura 10. Protocolo rip en R1  Fuente: Allan Echeverri Mateo

¿Qué comando muestra solo las rutas RIP?	Show ip route rip Figura 11. Protocolo para mostrar solo rutas rip en R1  Fuente: Allan Echeverri Mateo
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run | section router rip, como no soporta este commando, solo se emplea show run. Figura 12. Protocolo ip en R3  Fuente: Allan Echeverri Mateo

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla N°17

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1>enable R1#config terminal R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.1.20
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.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

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

La configuración del R2 incluye las siguientes tareas:

Tabla N°18

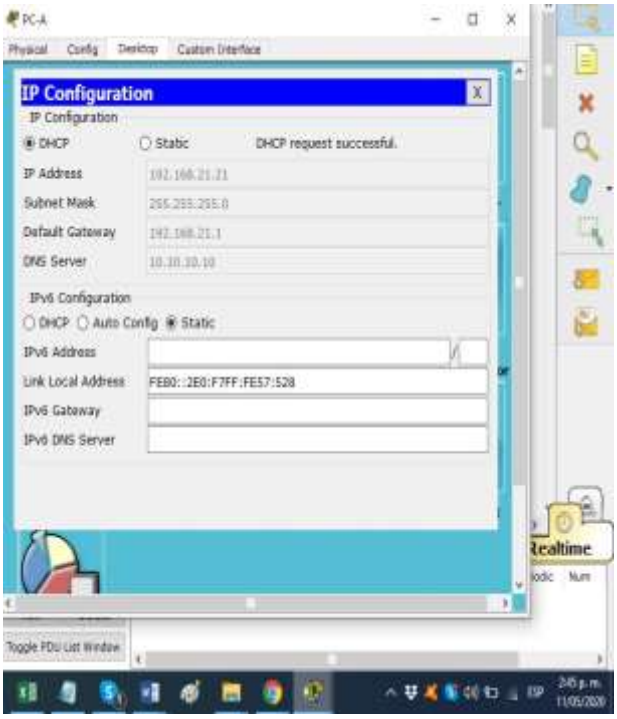
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: 15 R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet tracer no soporta dichos comandos para habilitar el servidor HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local, pero packet Tracer no soporta este comando.
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)# interface g0/0 R2(config)# ip nat outside R2(config)# interface s0/0/0 R2(config)# ip nat inside R2(config)# interface s0/0/1 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

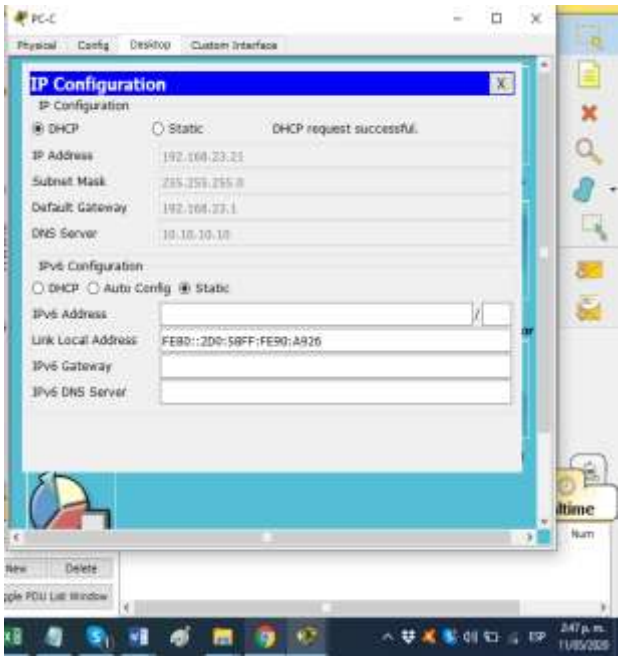
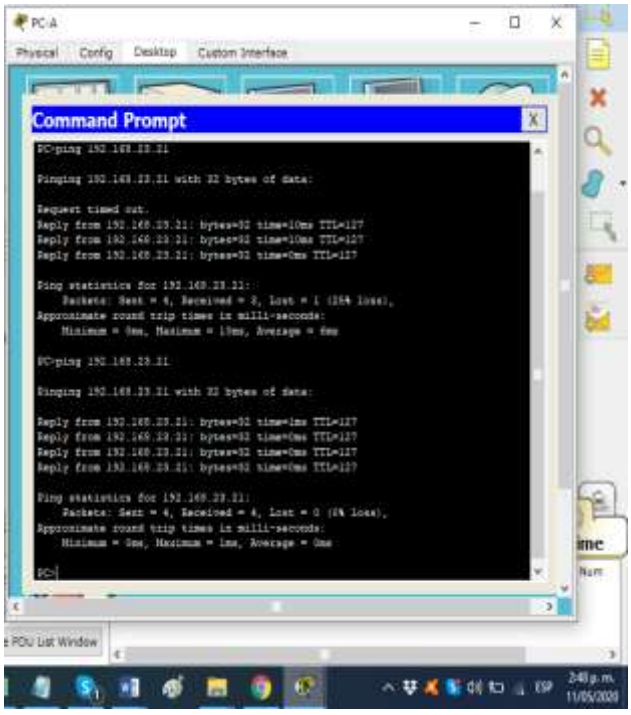
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.233** – **209.165.200.236** R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

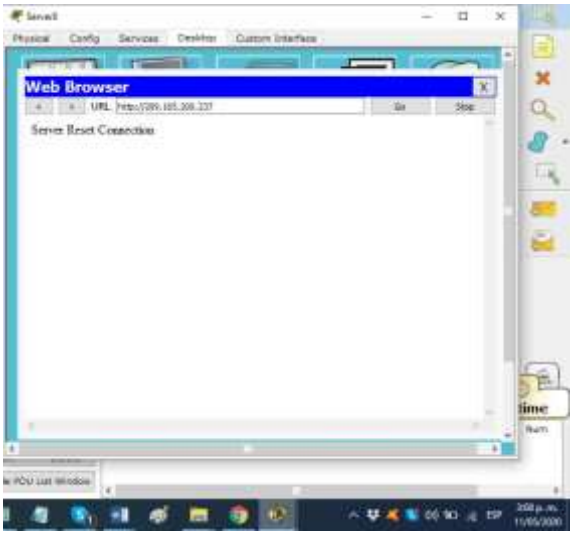
Paso 3. Verificar el protocolo DHCP y la NAT estática

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

Tabla N°19

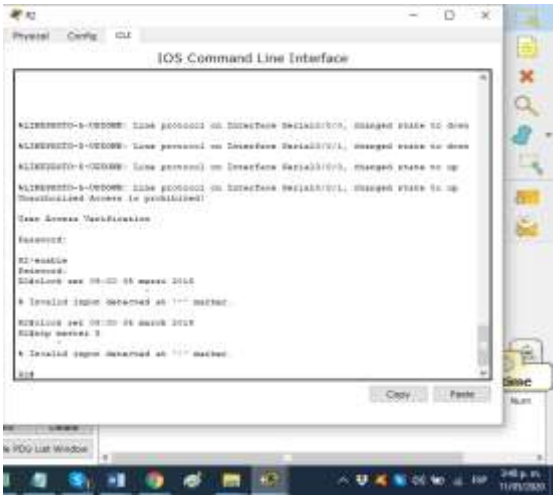
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 13. Verificación información DHCP en PC-A  Fuente: Allan Echeverri Mateo

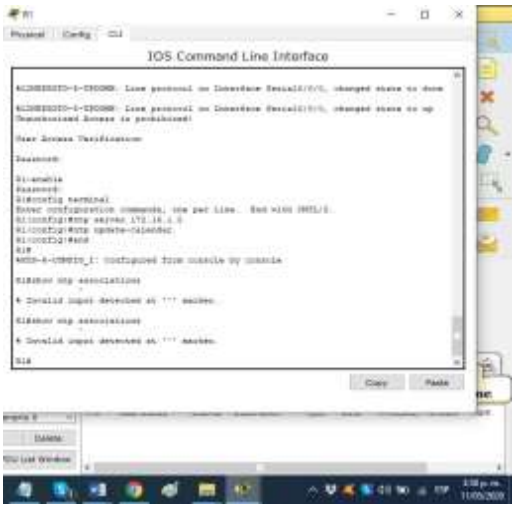
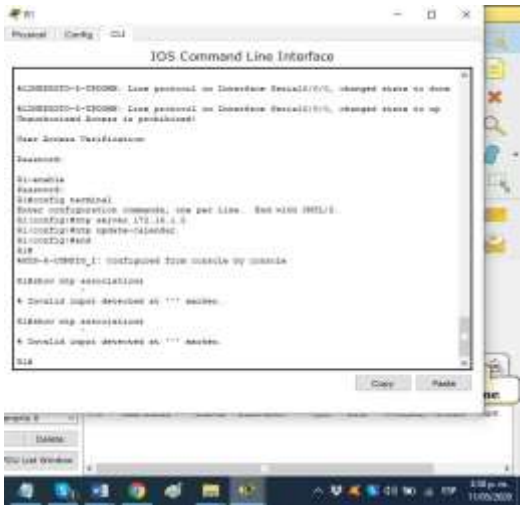
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 14. Verificación información DHCP en PC-C  Fuente: Allan Echeverri Mateo
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Figura 15. Ping de PC-A a PC-C  Fuente: Allan Echeverri Mateo

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**	No es posible realizar dicha conexión porque packet Tracer no reconoce dichos comandos Figura 16. Acceso servidor Web desde el servidor  Fuente: Allan Echeverri Mateo

Parte 6: Configurar NTP

Tabla N°20

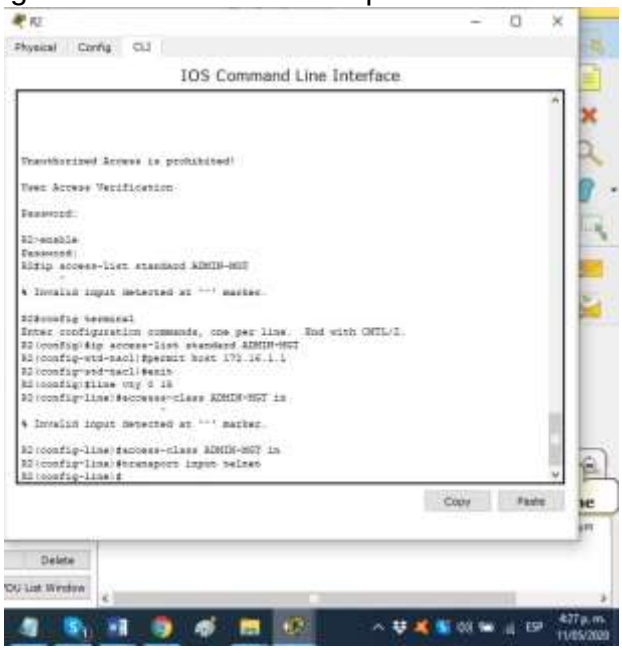
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 23:52:00 03 may 2020**.** Figura 17. Ajuste de fecha y hora en R2  Fuente: Allan Echeverri Mateo

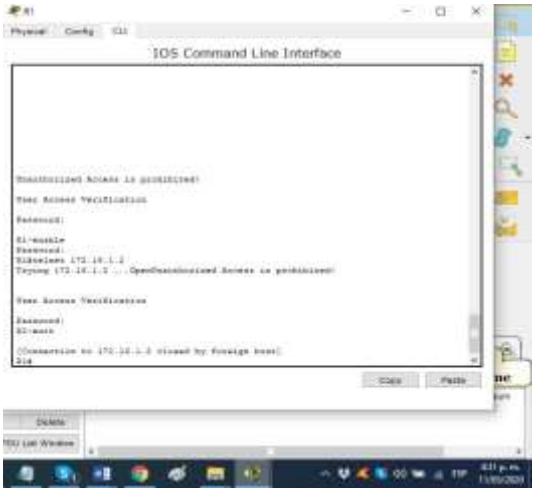
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2 R1(config)#ntp update-calendar Figura 18. Configuración NTP en R1  Fuente: Allan Echeverri Mateo
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2#ntp server 172.16.1.2 R2#ntp update-calendar
Verifique la configuración de NTP en R1.	R2#show ntp associations Figura 19. Mostrar las NTP asociadas  Fuente: Allan Echeverri Mateo

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

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

Tabla N°21

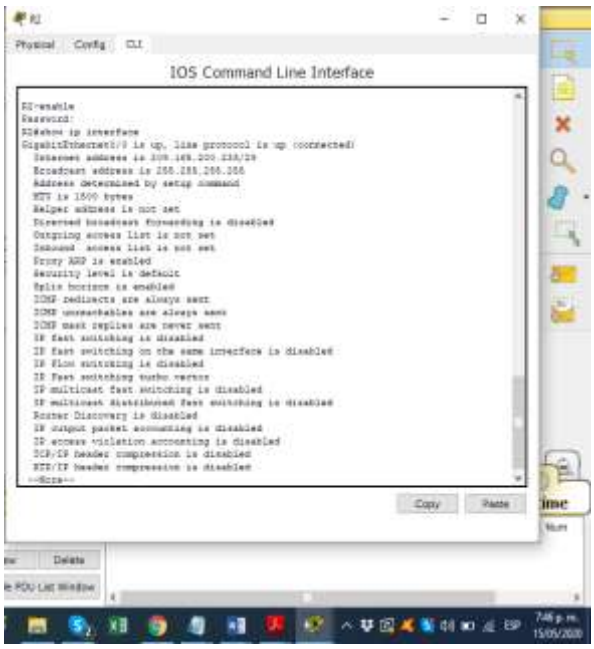
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	Packet tracer no soporta el commando “imput” Figura 20. Permitir acceso por telnet a VTY  Fuente: Allan Echeverri Mateo

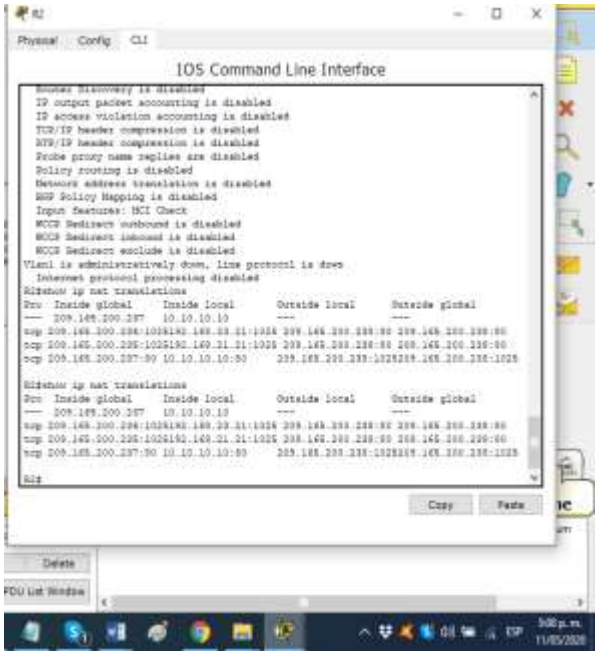
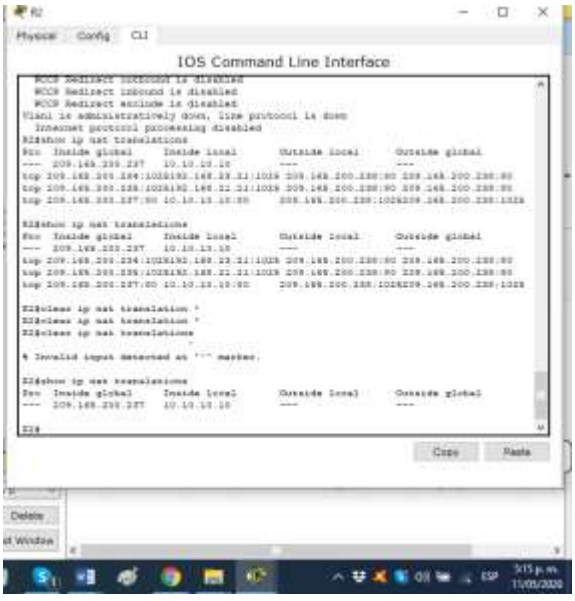
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Figura 21. Verificación telnet  Fuente: Allan Echeverri Mateo

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

Tabla N°22

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2# show access-list R2#show ip access-list Figura 22. Mostrar listas de acceso ip en R2  Fuente: Allan Echeverri Mateo

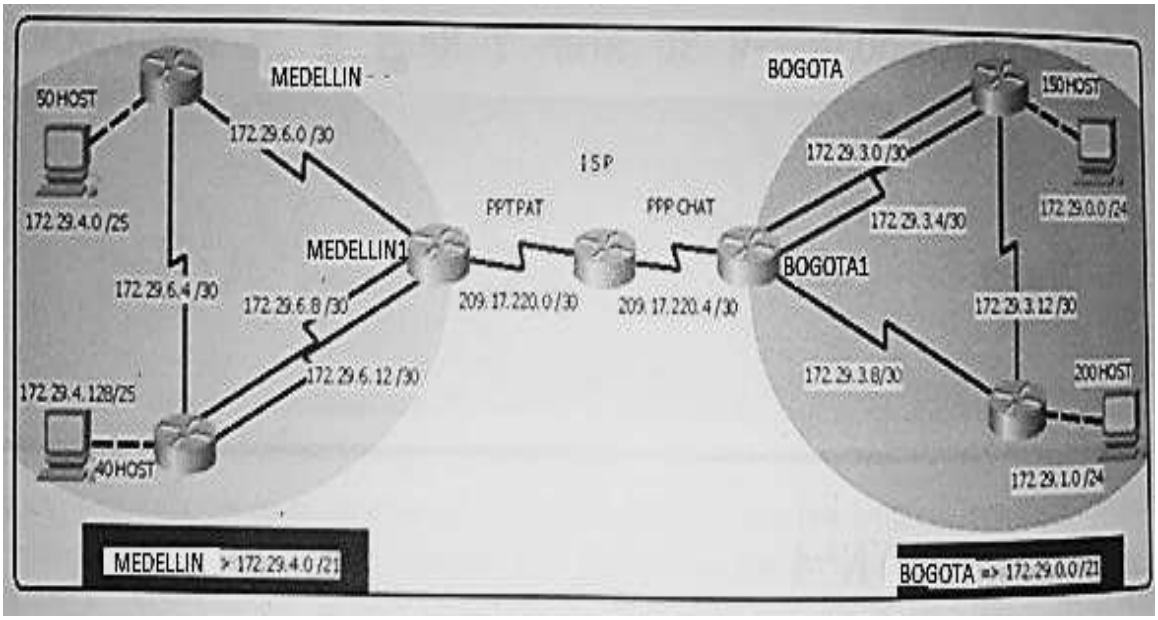
Restablecer los contadores de una lista de acceso	R2# clear ip access-list counters R2# clear ip ? Figura 23. Restablecer los contadres en R2  Fuente: Allan Echeverri Mateo
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2# show ip interface Figura 24. Mostrar interfaz ACL en R2  Fuente: Allan Echeverri Mateo

¿Con qué comando se muestran las traducciones NAT?	R2# Show ip nat translations Figura 25. Mostrar traducciones NAT en R2  Fuente: Allan Echeverri Mateo
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations Figura 26. Eliminar traducciones NAT  Fuente: Allan Echeverri Mateo

DESARROLLO DEL ESCENARIO 2

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

TOPOLOGIA DE RED



Grafica 2. Topología del escenario 2

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

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

DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

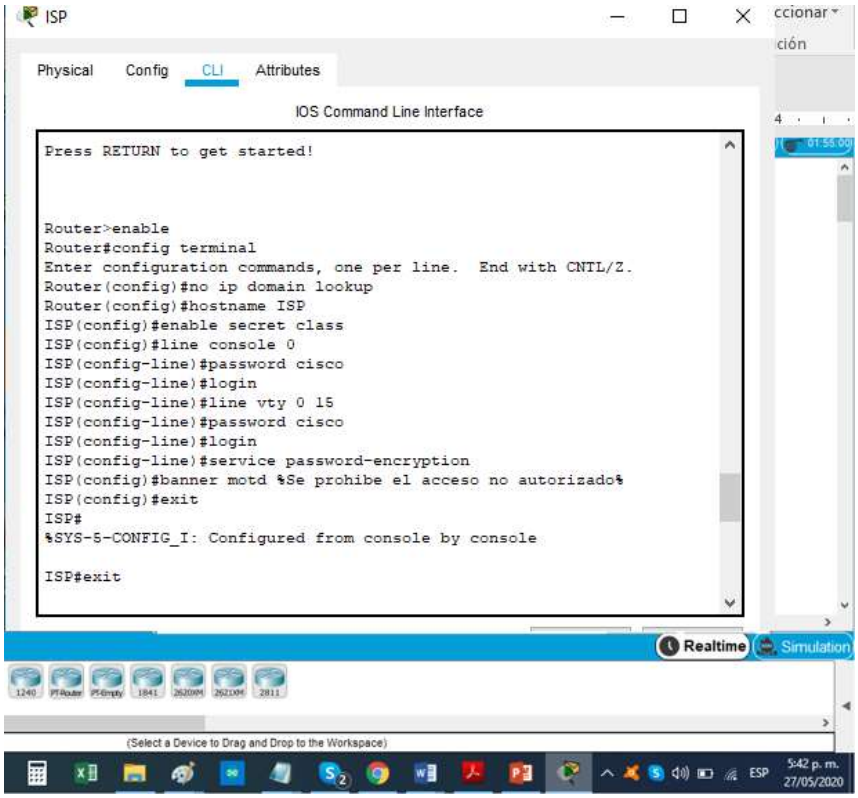
- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Configuracion seguridad en ISP

enable
config terminal
no ip domain lookup
hostname ISP
enable secret class
line console 0
password cisco
login
line vty 0 15
password cisco
login
service password-encryption
banner motd %Se prohibe el acceso no autorizado%

Se muestra mediante la siguiente figura, la configuración realizada en ISP, este mismo paso se realiza para todos los routers

Figura 27. Configuracion de seguridad en ISP



Fuente: Allan Echeverri Mateo

Configuracion seguridad en Medellin 1

```
enable
config terminal
no ip domain lookup
hostname Medellin1
enable secret class
line console 0
password cisco
login
line vty 0 15
password cisco
login
service password-encryption
banner motd %Se prohibe el acceso no autorizado%
```

Configuración seguridad en Medellin 2

```
enable
config terminal
no ip domain lookup
hostname Medellin2
enable secret class
line console 0
password cisco
login
line vty 0 15
password cisco
login
service password-encryption
banner motd %Se prohibe el acceso no autorizado%
```

Configurar seguridad en Medellin 3

```
enable
config terminal
no ip domain lookup
hostname Medellin3
enable secret class
line console 0
password cisco
login
line vty 0 15
password cisco
login
service password-encryption
banner motd %Se prohibe el acceso no autorizado%
```

Configurar seguridad en Bogotá 1

```
enable
config terminal
no ip domain lookup
hostname Bogota1
enable secret class
line console 0
password cisco
login
line vty 0 15
password cisco
login
service password-encryption
banner motd %Se prohibe el acceso no autorizado%
```

Configurar seguridad en Bogotá 2

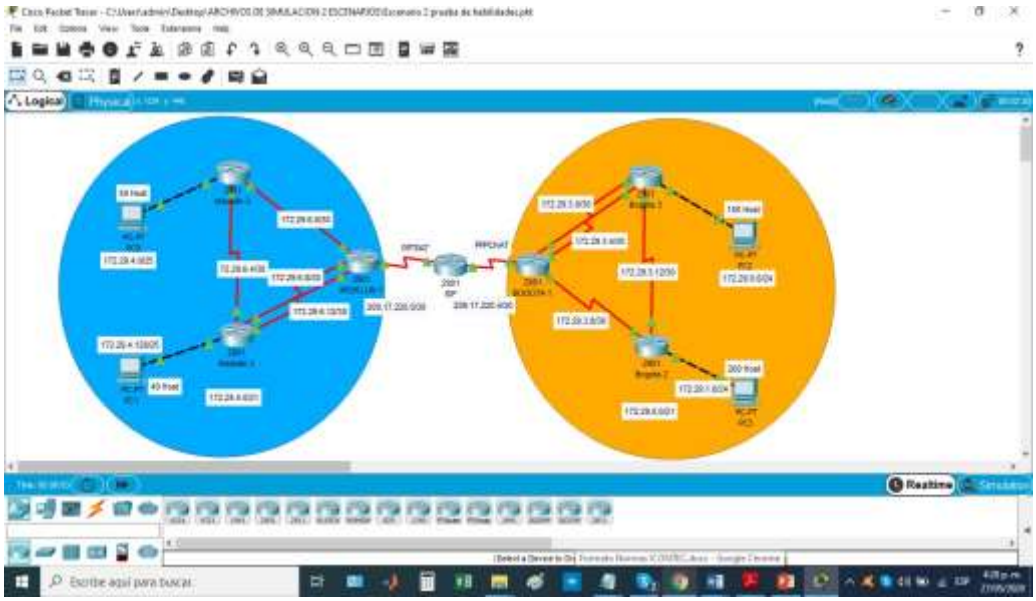
```
enable
config terminal
no ip domain lookup
hostname Bogota2
enable secret class
line console 0
password cisco
login
line vty 0 15
password cisco
login
service password-encryption
banner motd %Se prohibe el acceso no autorizado%
```

Configurar seguridad en Bogota 3

```
enable
config terminal
no ip domain lookup
hostname Bogota3
enable secret class
line console 0
password cisco
login
line vty 0 15
password cisco
login
service password-encryption
banner motd %Se prohibe el acceso no autorizado%
```

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

Figura 28. Montaje del escenario 2 en Packet Tracer



Fuente: Allan Echeverri Mateo

Parte 1: Configuración del enrutamiento

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

Nota: No se requiere desactivar la sumarización automática en OSPFv2 y se declaran redes separadas

Se procede a realizar la configuración respectiva en cada router.

configuracion Router IPS:

enable

config terminal

hostname ISP

interface s0/0/0

ip address 209.17.220.1 255.255.255.252

clock rate 4000000

no shutdown

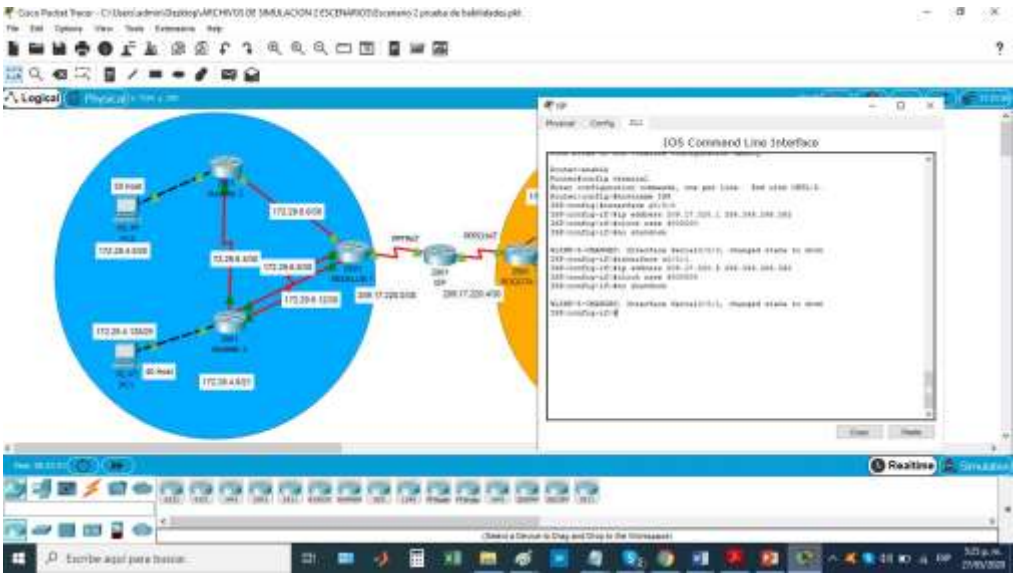
interface s0/0/1

ip address 209.17.220.5 255.255.255.252

clock rate 4000000

no shutdown

Figura 29. Configuración enrutamiento en ISP

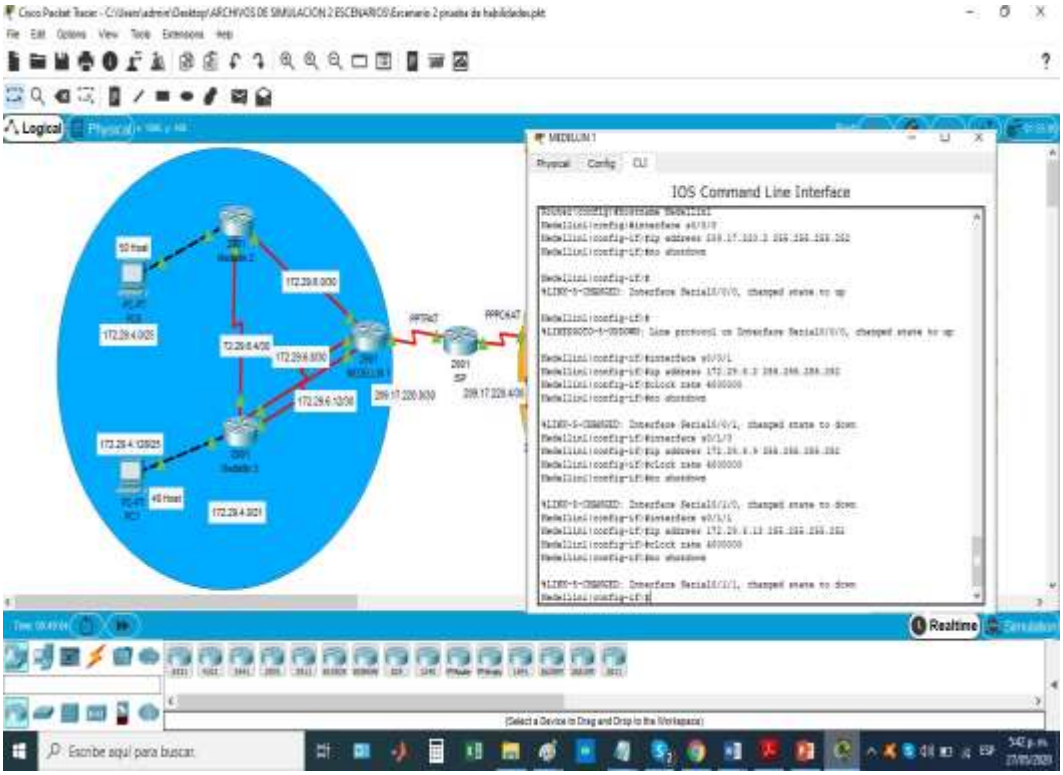


Fuente: Allan Echeverri Mateo

Configuracion Medellin 1

enable
config terminal
hostname Medellin1
interface s0/0/0
ip address 209.17.220.2 255.255.255.252
no shutdown
interface s0/0/1
ip address 172.29.6.2 255.255.255.252
clock rate 4000000
no shutdown
interface s0/1/0
ip address 172.29.6.9 255.255.255.252
clock rate 4000000
no shutdown
interface s0/1/1
ip address 172.29.6.13 255.255.255.252
clock rate 4000000
no shutdown

Figura 30. Configuración enrutamiento en Medellin 1

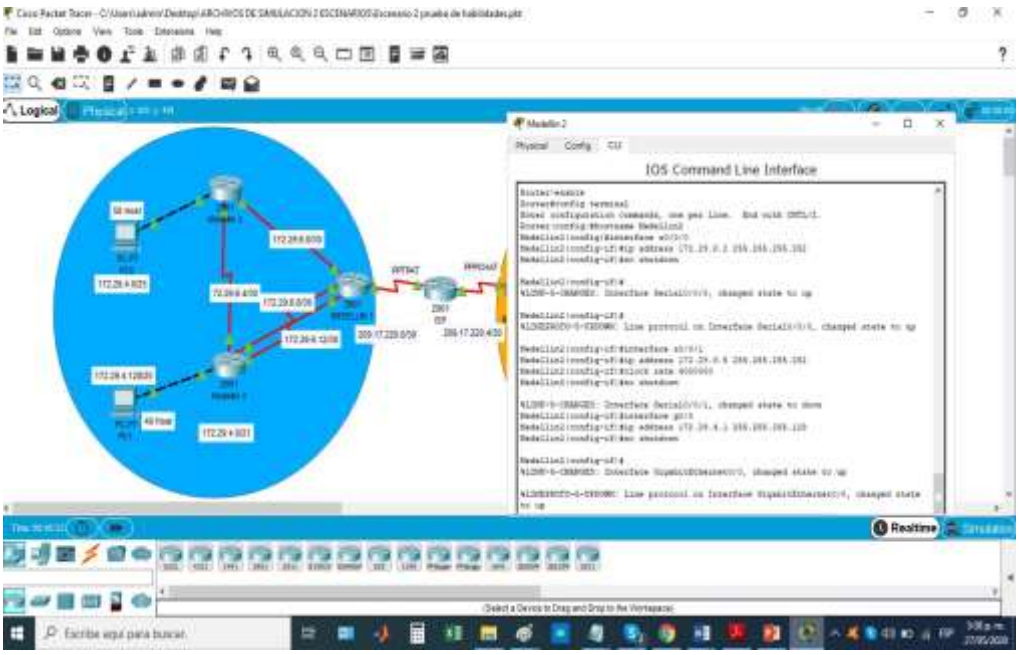


Fuente: Allan Echeverri Mateo

Configuracion Medellin 2

enable
config terminal
hostname Medellin2
interface s0/0/0
ip address 172.29.6.2 255.255.255.252
no shutdown
interface s0/0/1
ip address 172.29.6.5 255.255.255.252
clock rate 4000000
no shutdown
interface g0/0
ip address 172.29.4.1 255.255.255.128
no shutdown

Figura 31. Configuración enrutamiento en Medellin 2

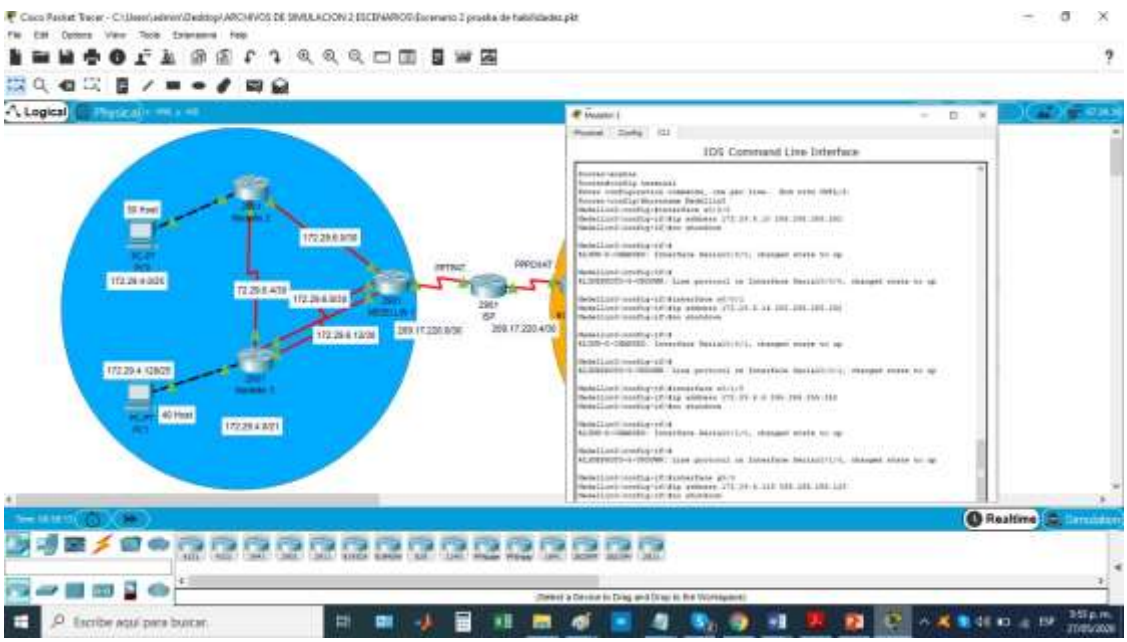


Fuente: Allan Echeverri Mateo

Configuracion Medellin 3

enable
config terminal
hostname Medellin3
interface s0/0/0
ip address 172.29.6.10 255.255.255.252
no shutdown
interface s0/0/1
ip address 172.29.6.14 255.255.255.252
no shutdown
interface s0/1/0
ip address 172.29.6.6 255.255.255.252
no shutdown
interface g0/0
ip address 172.29.4.129 255.255.255.128
no shutdown
interface s0/1/0
ip address 172.29.3.14 255.255.255.252
no shutdown

Figura 32. Configuración enrutamiento en Medellin 3

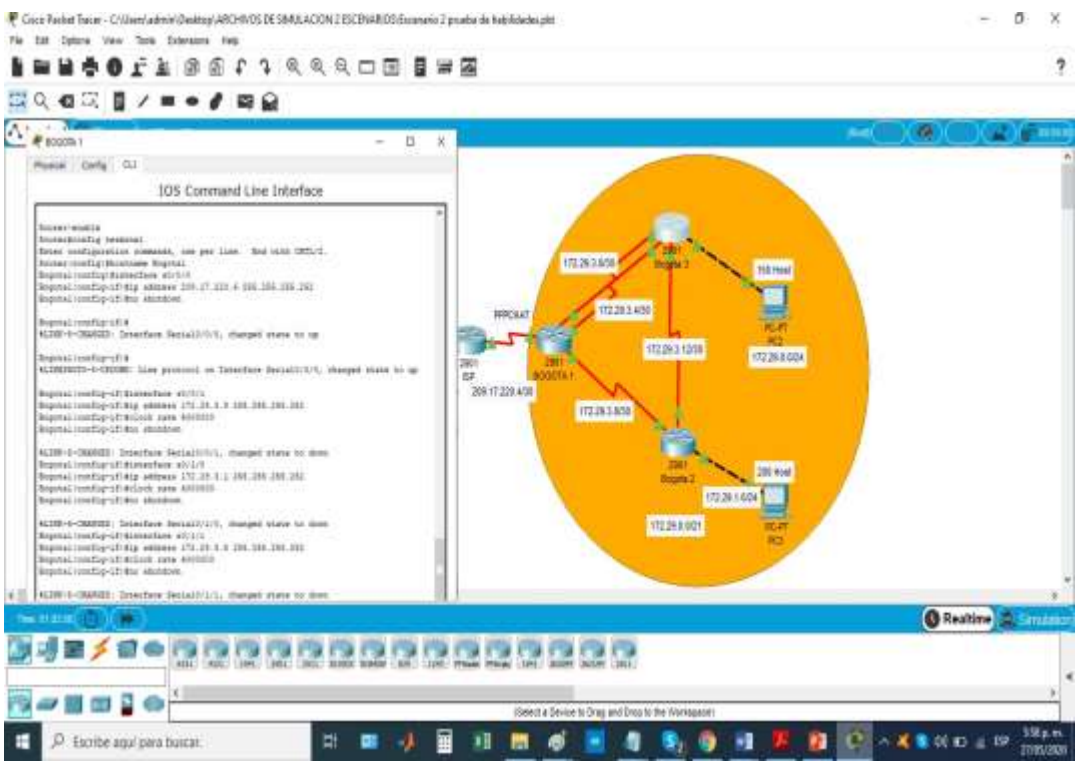


Fuente: Allan Echeverri Mateo

Configuración Bogotá 1:

```
enable
config terminal
hostname Bogota1
interface s0/0/0
ip address 209.17.220.6 255.255.255.252
no shutdown
interface s0/0/1
ip address 172.29.3.9 255.255.255.252
clock rate 4000000
no shutdown
interface s0/1/0
ip address 172.29.3.1 255.255.255.252
clock rate 4000000
no shutdown
interface s0/1/1
ip address 172.29.3.5 255.255.255.252
clock rate 4000000
no shutdown
```

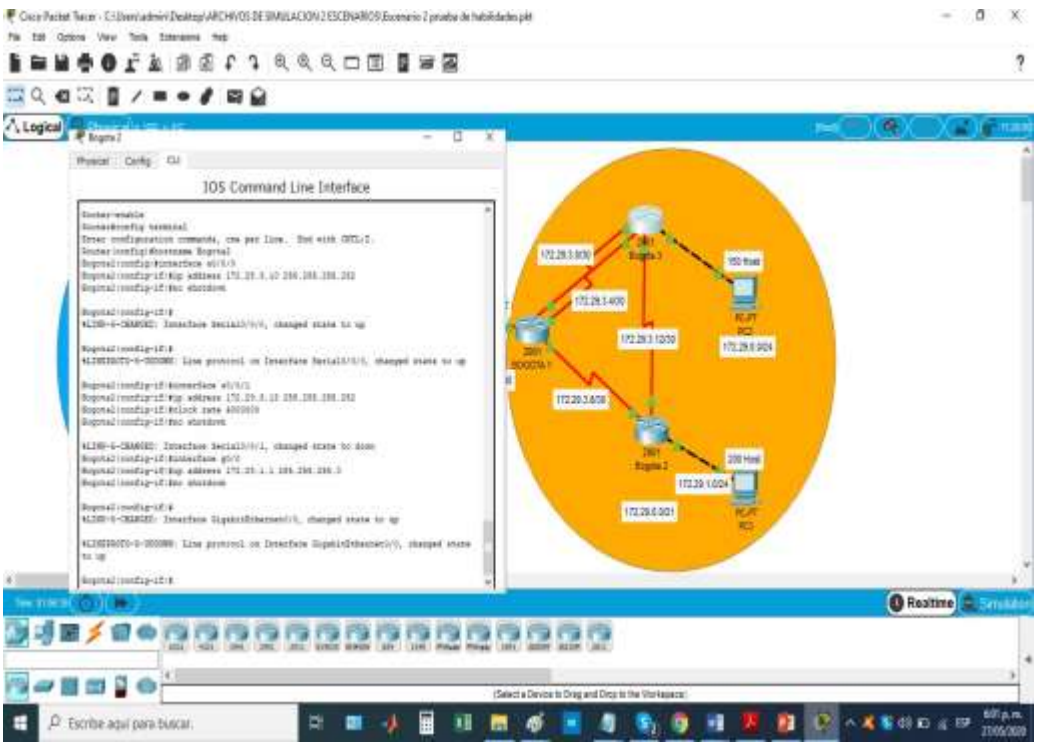
Figura 33. Configuración enrutamiento en Bogota 1



Fuente: Allan Echeverri Mateo

Configuracion Bogotá 2:
enableno
config terminal
hostname Bogota2
interface s0/0/0
ip address 172.29.3.10 255.255.255.252
no shutdown
interface s0/0/1
ip address 172.29.3.13 255.255.255.252
clock rate 4000000
no shutdown
interface g0/0
ip address 172.29.1.1 255.255.255.0
no shutdown

Figura 34. Configuración enrutamiento en Bogota 2

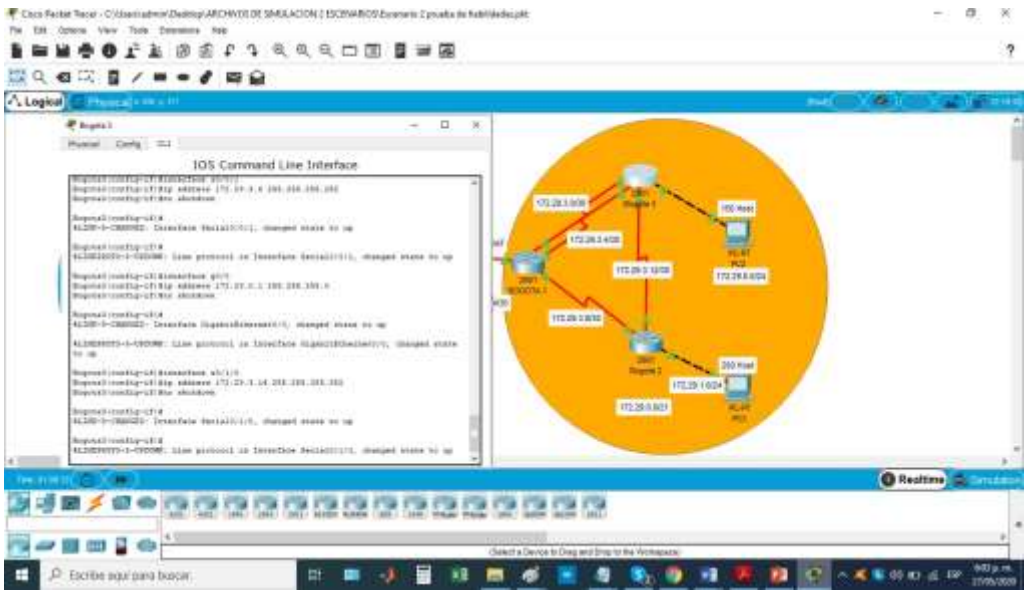


Fuente: Allan Echeverri Mateo

Configuracion Bogotá 3:

enable
config terminal
hostname Bogota3
interface s0/0/0
ip address 172.29.3.2 255.255.255.252
no shutdown
interface s0/0/1
ip address 172.29.3.6 255.255.255.252
no shutdown
interface g0/0
ip address 172.29.0.1 255.255.255.0
no shutdown
interface s0/1/0
ip address 172.29.3.14 255.255.255.252
no shutdown

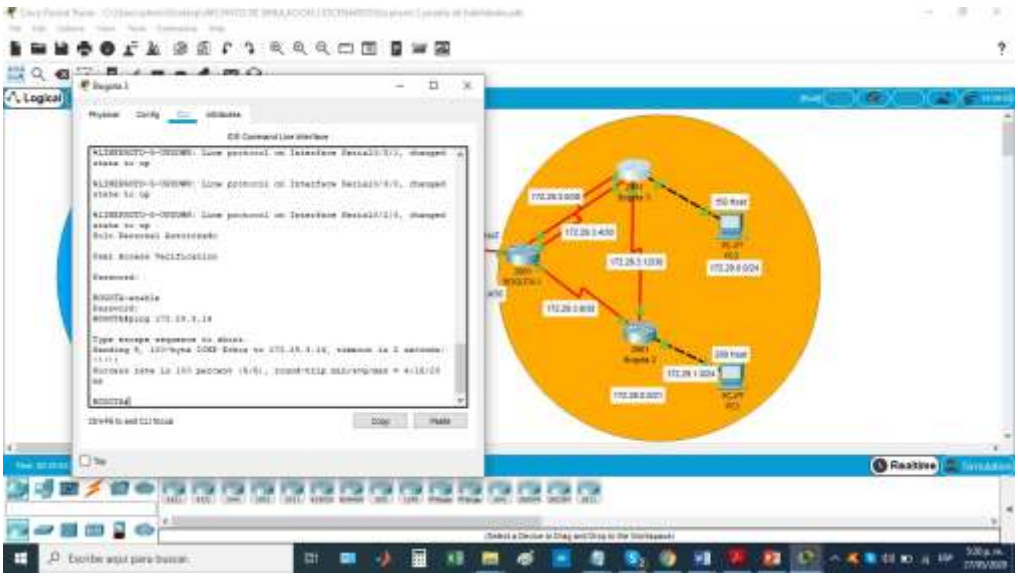
Figura 35. Configuración enrutamiento en Bogota 3



Fuente: Allan Echeverri Mateo

Verificamos la conectividad mediante la realización de un ping del router Bogotá 3 a Bogotá 2

Figura 36. Ping de Bogotá 3 a Bogotá 2



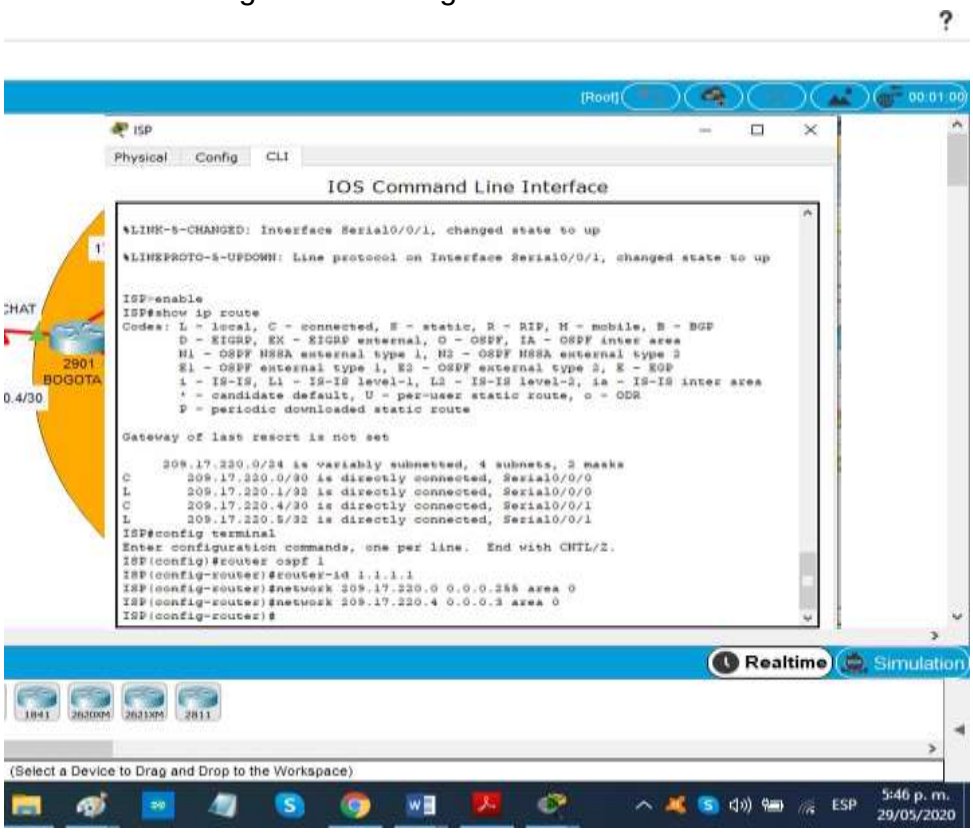
Fuente: Allan Echeverri Mateo

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

Enrutamiento OSPF en ISP:
enable
config terminal
router ospf 1
router-id 1.1.1.1
network 209.17.220.0 0.0.0.255 area 0
network 209.17.220.4 0.0.0.3 area 0

Verificamos mediante la siguiente imagen la configuración OSPF, de igual forma se realiza en todos los dispositivos:

Figura 37. Configuración OSPF en ISP



Fuente: Allan Echeverri Mateo

Enrutamiento OSPF en Medellin 1:
enable
config terminal
router ospf 1
router-id 2.2.2.2
network 172.29.6.0 0.0.0.255 area 1
network 172.29.6.8 0.0.0.3 area 1
network 172.29.6.12 0.0.0.3 area 1
network 209.17.220.0 0.0.0.3 area 0

Enrutamiento OSPF en Medellin 2:
enable
config terminal
router ospf 1
router-id 3.3.3.3
network 172.29.4.0 0.0.0.255 area 1
network 172.29.6.0 0.0.0.3 area 1
network 172.29.6.4 0.0.0.3 area 1

Enrutamiento OSPF en Medellin 3:
enable
config terminal
router ospf 1
router-id 4.4.4.4
network 172.29.4.128 0.0.0.255 area 1
network 172.29.6.4 0.0.0.3 area 1
network 172.29.6.4 0.0.0.3 area 1
network 172.29.6.8 0.0.0.3 area 1
network 172.29.6.12 0.0.0.3 area 1

Enrutamiento OSPF en Bogota 1:
enable
config terminal
router ospf 1
router-id 5.5.5.5
network 172.29.3.0 0.0.0.255 area 2
network 172.29.3.4 0.0.0.3 area 2
network 172.29.3.8 0.0.0.3 area 2
network 209.17.220.4 0.0.0.3 area 0

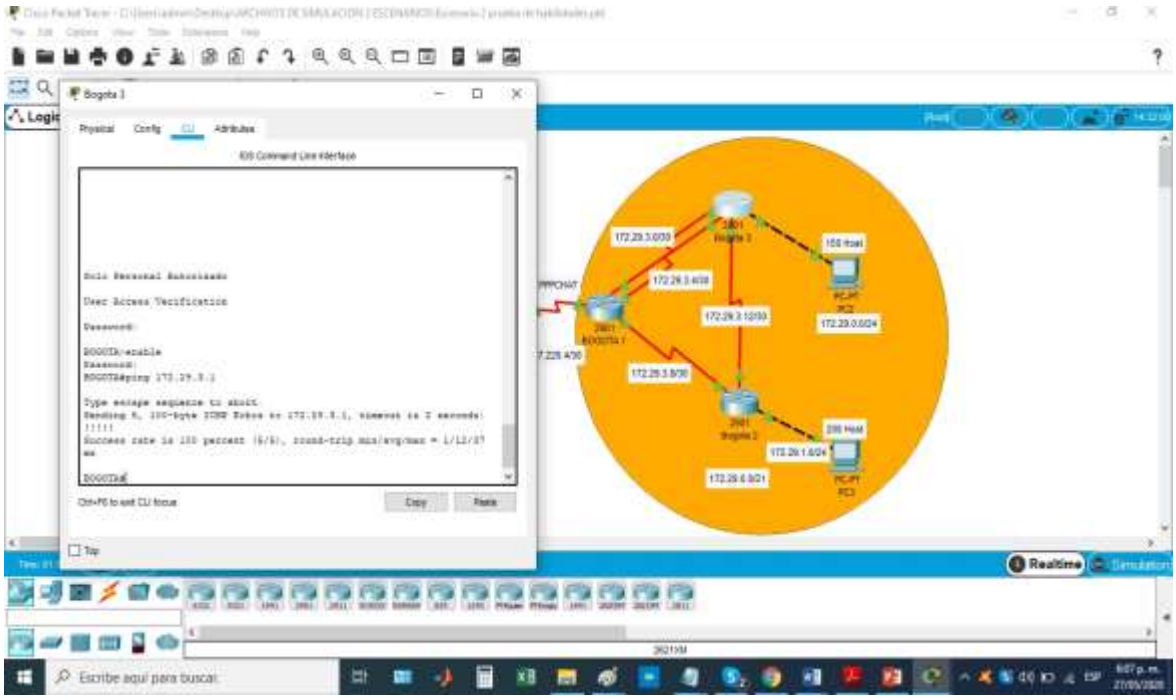
Enrutamiento OSPF en Bogota 2:
enable
config terminal
router ospf 1

router-id 6.6.6.6
network 172.29.1.0 0.0.0.255 area 2
network 172.29.3.8 0.0.0.3 area 2
network 172.29.3.8 0.0.0.3 area 2
network 172.29.3.12 0.0.0.3 area 2

Enrutamiento OSPF en Bogota 3:
enable
config terminal
router ospf 1
router-id 7.7.7.7
network 172.29.0.0 0.0.0.255 area 2
network 172.29.3.0 0.0.0.3 area 2
network 172.29.3.4 0.0.0.3 area 2
network 172.29.3.12 0.0.0.3 area 2

verificamos mediante ping en bogota 3

Figura 38.Ping en bogota 3



Fuente: Allan Echeverri Mateo

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

configurar sumarizacion en el ISP:

enable

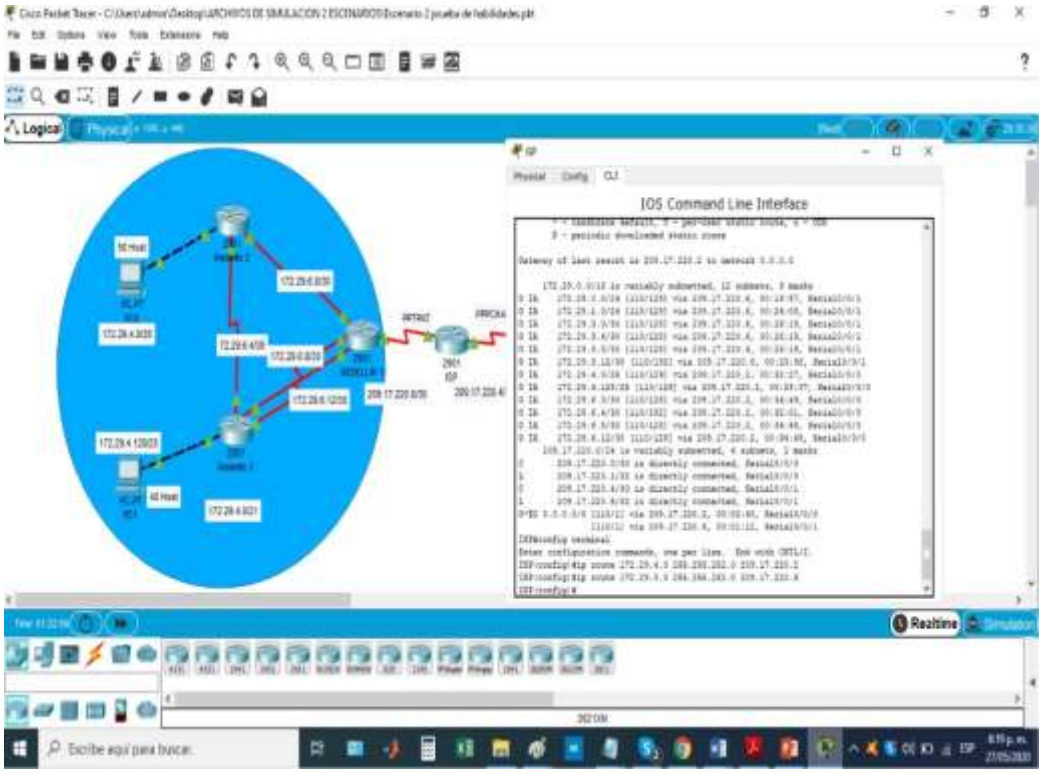
config terminal

ip route 172.29.4.0 255.255.252.0 209.17.220.2

ip route 172.29.0.0 255.255.252.0 209.17.220.6

Verificamos la sumarizacion realizada en el ISP

Figura 39. Sumarizacion en ISP



Fuente: Allan Echeverri Mateo

Parte 2: Tabla de Enrutamiento.

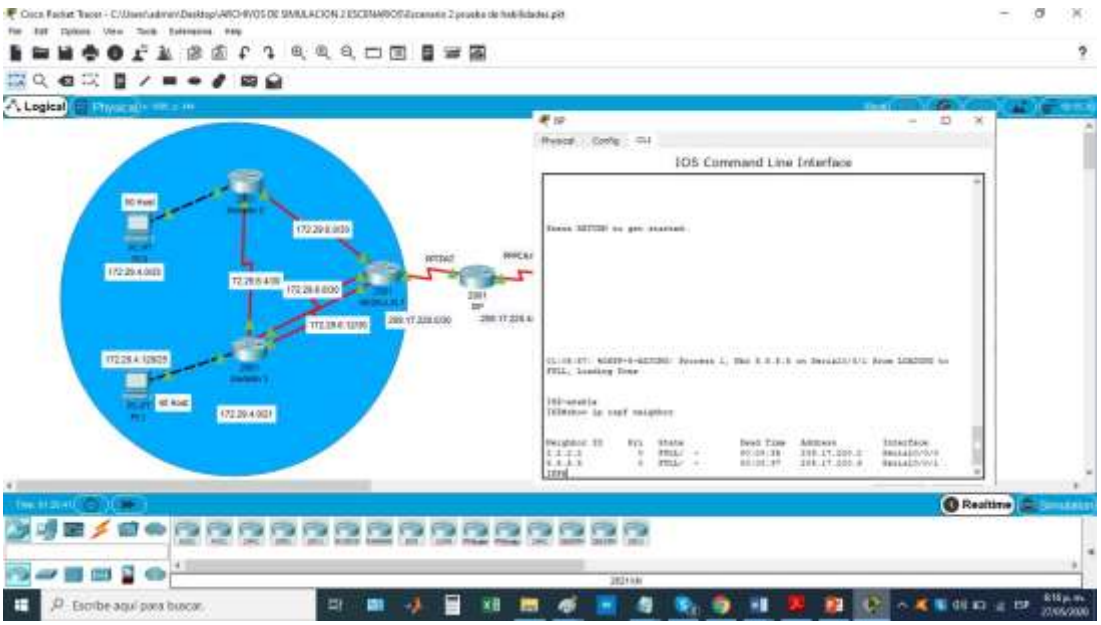
a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Verificar config ospf en ISP:

enable

show ip ospf neighbor

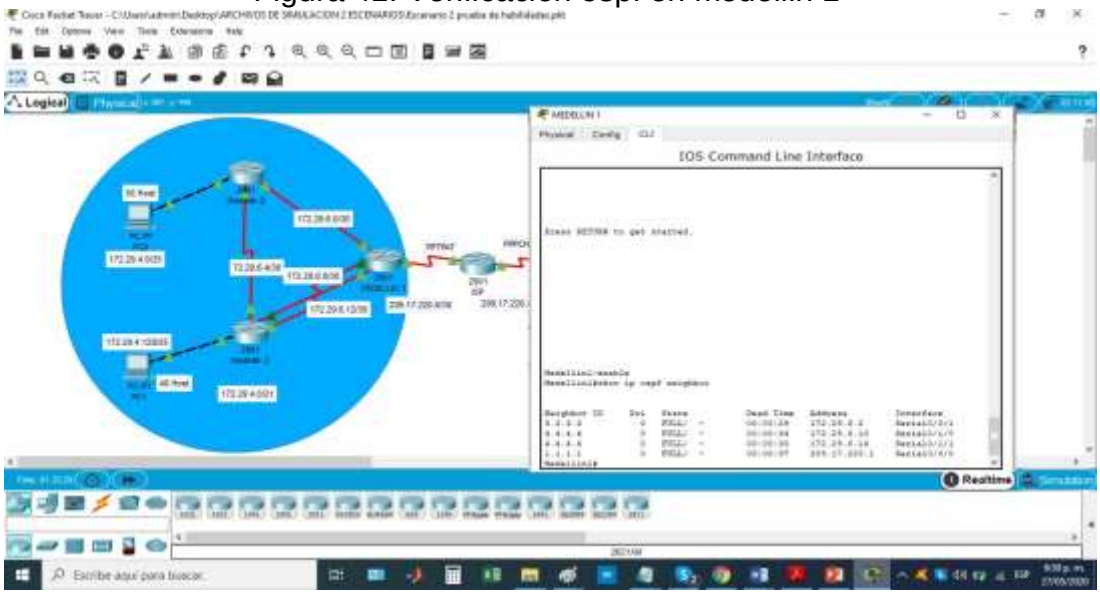
Figura 40.verificar confguracion ospf en ISP



Fuente: Allan Echeverri Mateo

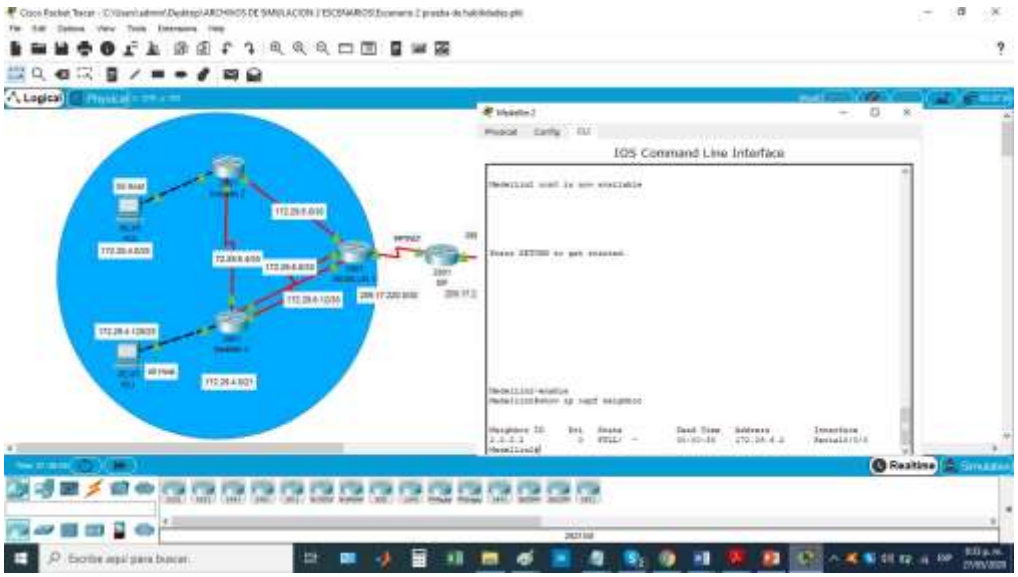
Verificar config ospf en medellin 1, 2 y 3:
enable
show ip ospf neighbor

Figura 41. Verificacion ospf en medellin 1



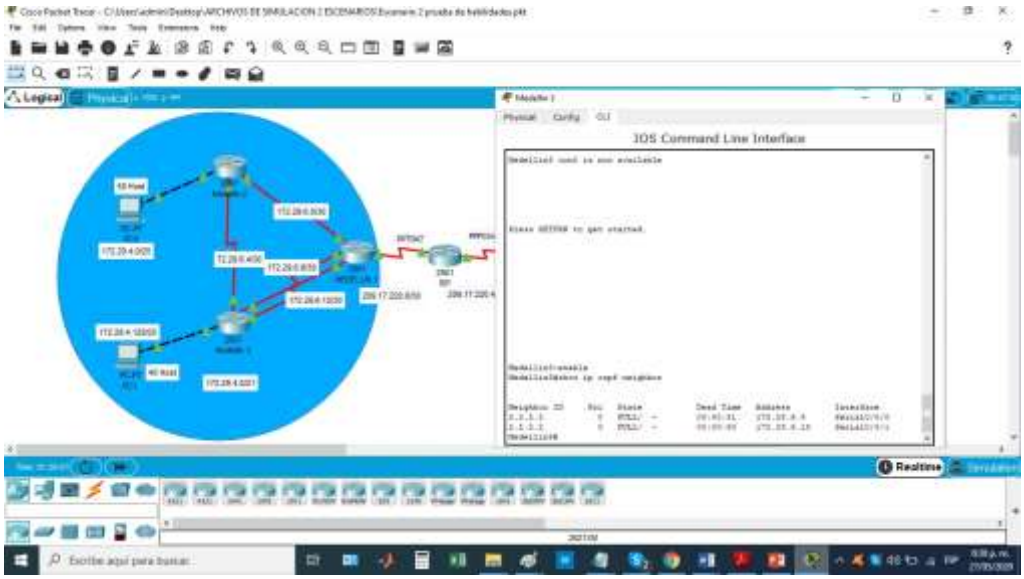
Fuente: Allan Echeverri Mateo

Figura 42. Verificacion ospf en medellin 2



Fuente: Allan Echeverri Mateo

Figura 43. Verificacion ospf en medellin 3



Fuente: Allan Echeverri Mateo

Verificar config ospf en bogota 1, 2 y 3:
enable
show ip ospf neighbor

Figura 44. Verificacion ospf en bogota 1

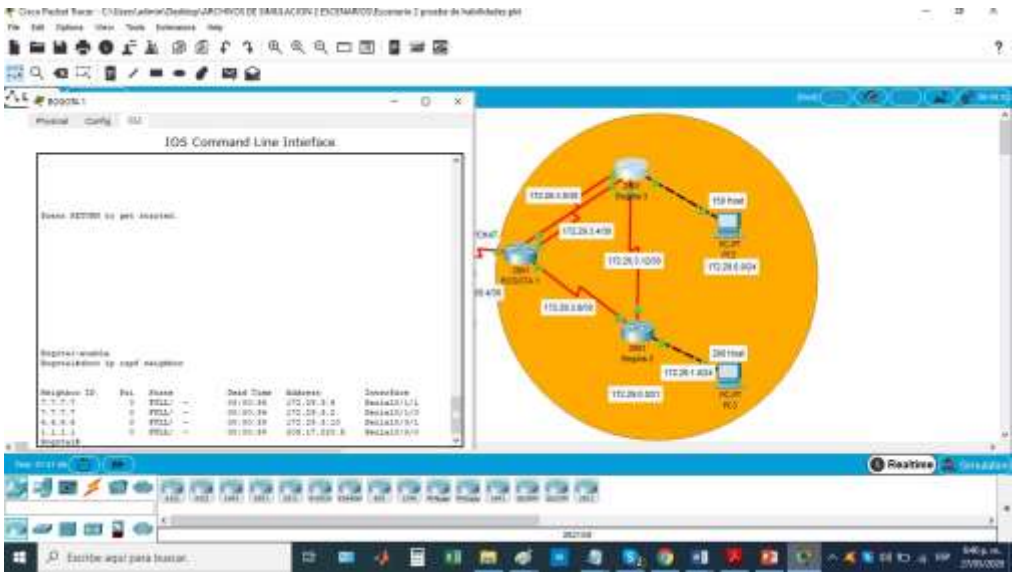
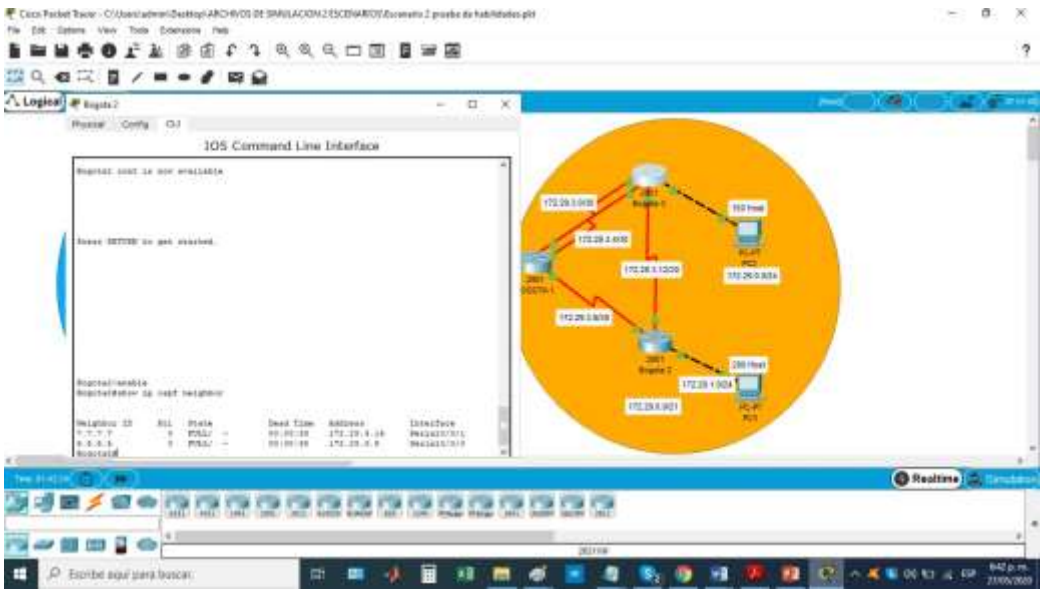
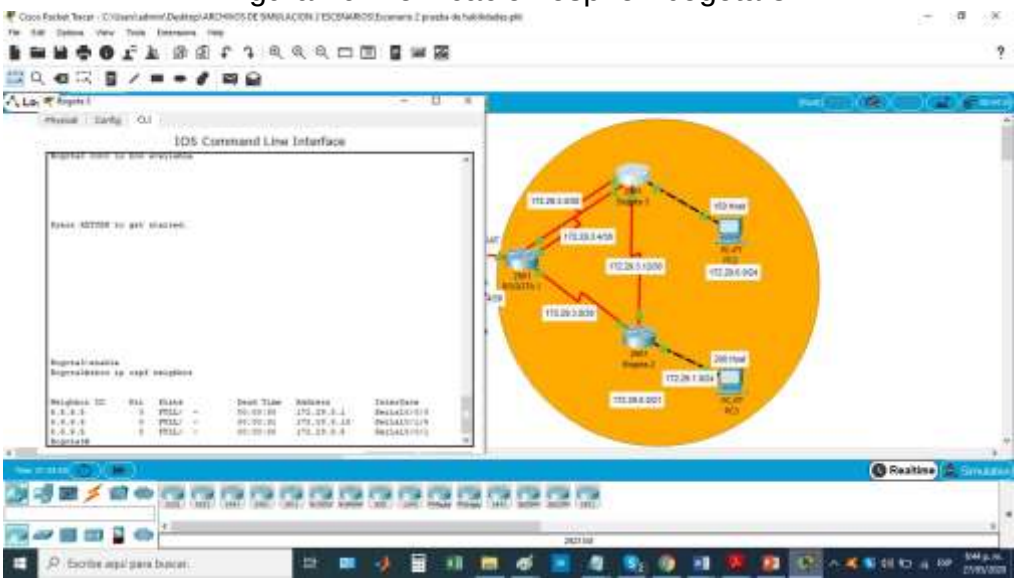


Figura 45. Verificacion ospf en bogota 2



Fuente:Allan Echeverri Mateo

Figura 46. Verificacion ospf en bogota 3



Fuente: Allan Echeverri Mateo

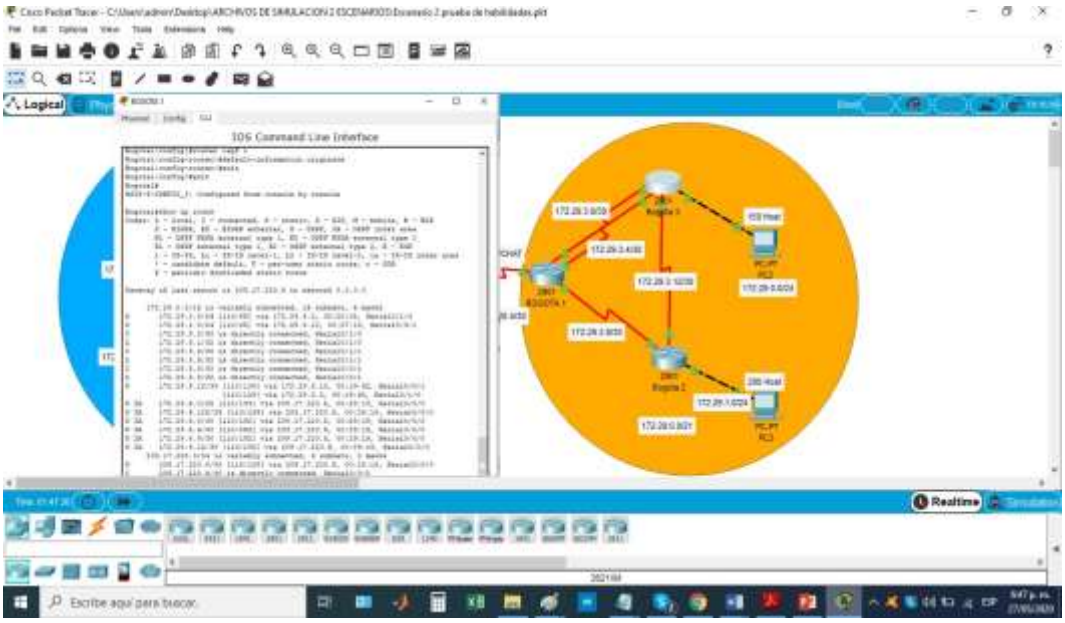
b. Verificar el balanceo de carga que presentan los routers.

Verificamos balanceo de carga en bogota 1:

enable

show ip route

Figura 47. Verificacion rutas ip en bogota 1



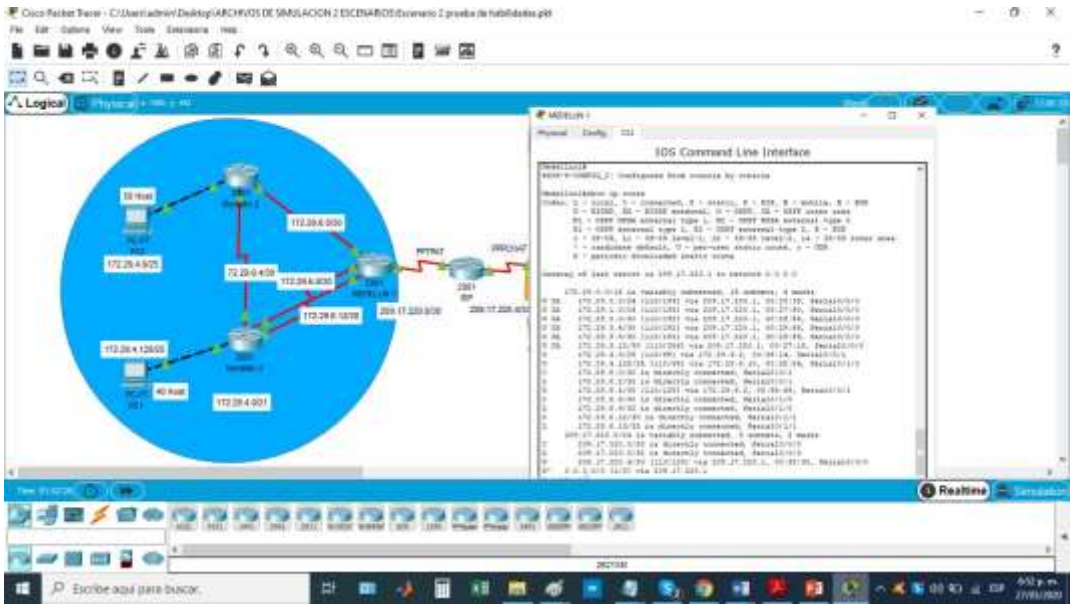
Fuente:Allan Echeverri Mateo

Verificamos balanceo de carga en medellin 1:

enable

show ip route

Figura 48. Verificacion ip en medellin 1



Fuente: Allan Echeverri Mateo

c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

configurar ruta por defecto medellin 1:

config terminal

ip route 0.0.0.0 0.0.0.0 209.17.220.1

router ospf 1

default-information originate

config ruta por defecto bogota 1:

config terminal

ip route 0.0.0.0 0.0.0.0 209.17.220.5

router ospf 1

default-information originate

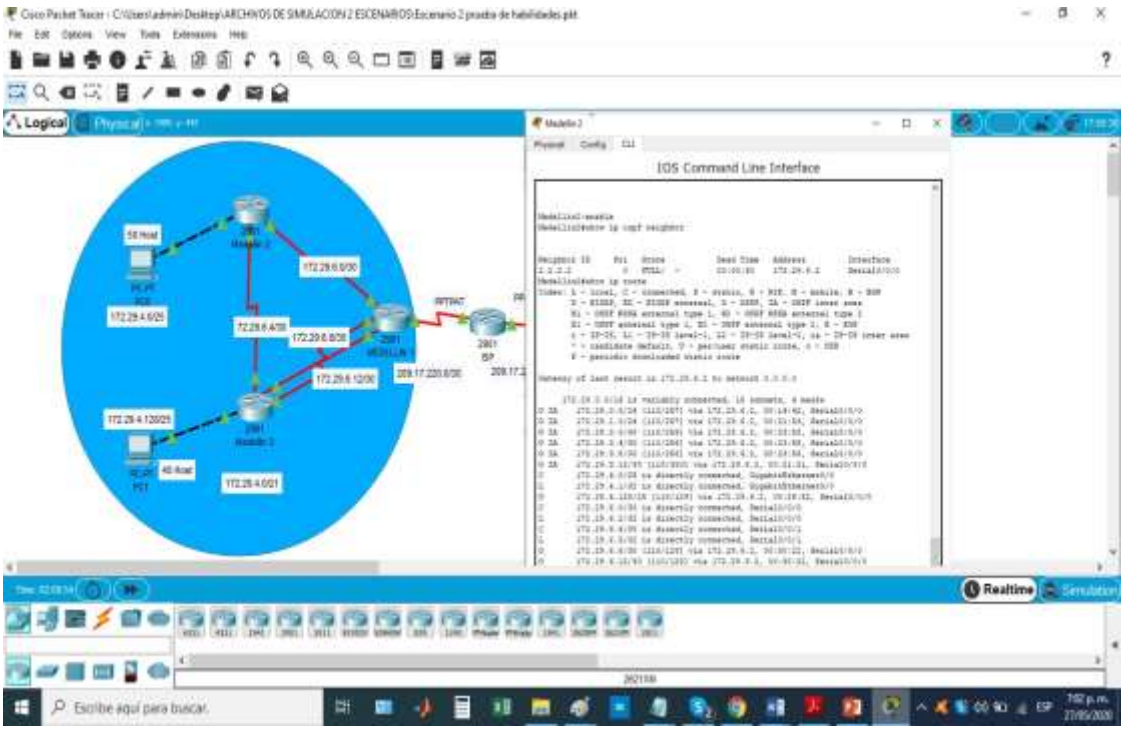
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

verificamos en medellin 2 la configuración:

enable

show ip route

Figura 49. Verificacion ip en medellin 2



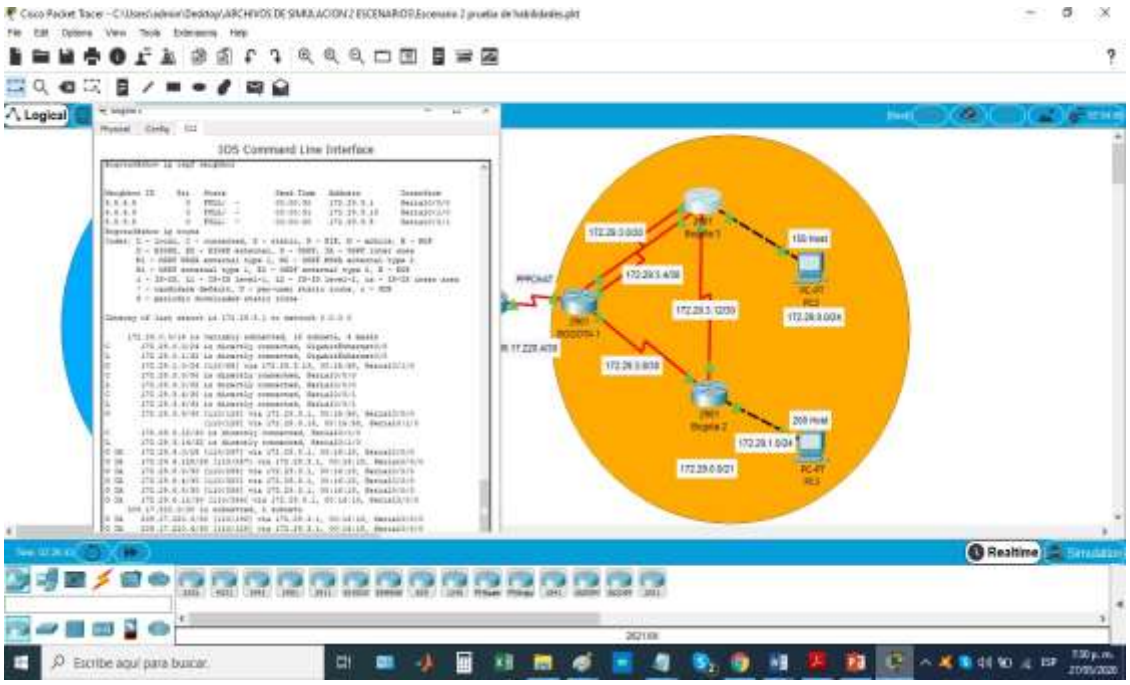
Fuente:Allan Echeverri Mateo

verificamos en bogota 3 la config:

enable

show ip route

Figura 50. Verificacion ip en bogota 3



Fuente: Allan Echeverri Mateo

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

Se ve también en Parte 2: a. las rutas OSPF (O) con doble ruta hacia un mismo destino.

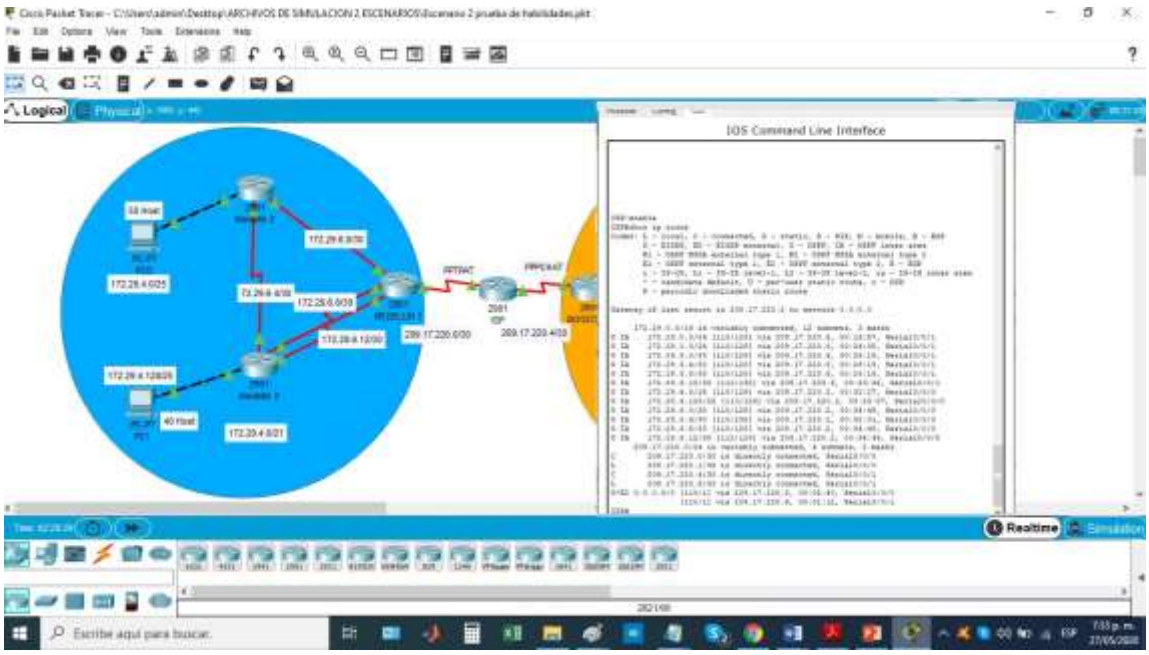
f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

verificamos redes conectadas a ISP:

enable

show ip route

Figura 51. Verificacion redes conectadas en ISP



Fuente: Allan Echeverri Mateo

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

Medellin 1
router ospf 1
passive-interface Serial0/0/0

Medellin 2
router ospf 1
passive-interface GigabitEthernet0/0

Medellin 3
router ospf 1
passive-interface GigabitEthernet0/0

Bogota 1
router ospf 1
passive-interface Serial0/0/0

Bogota 2
router ospf 1
passive-interface GigabitEthernet0/0

Bogota 3
router ospf 1
passive-interface GigabitEthernet0/0

Parte 4: Verificación del protocolo OSPF.

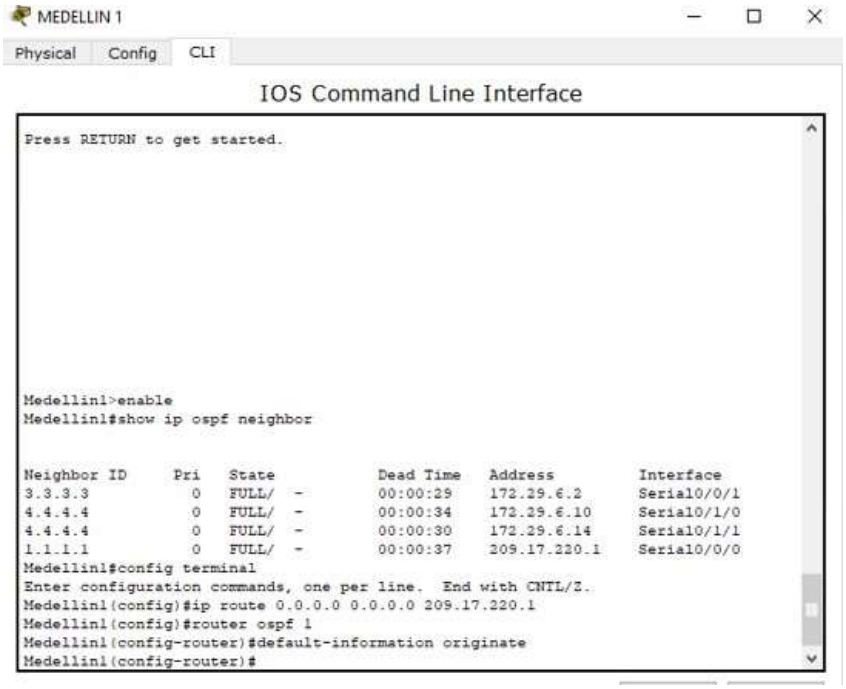
a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.
Medellin 1

Se verifica la información mediante las siguientes imágenes, así mismo este comando se ejecuta para todos los dispositivos:

Medellin 1#Show ip ospf neighbor

Figura 52. Verificación protocolo OSPF en medellín 1



Fuente: Allan Echeverri Mateo

Medellin 2# Show ip ospf neighbor

Figura 53. Verificación protocol OSPF en Medellin 2

Fuente: Allan Echeverri Mateo

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

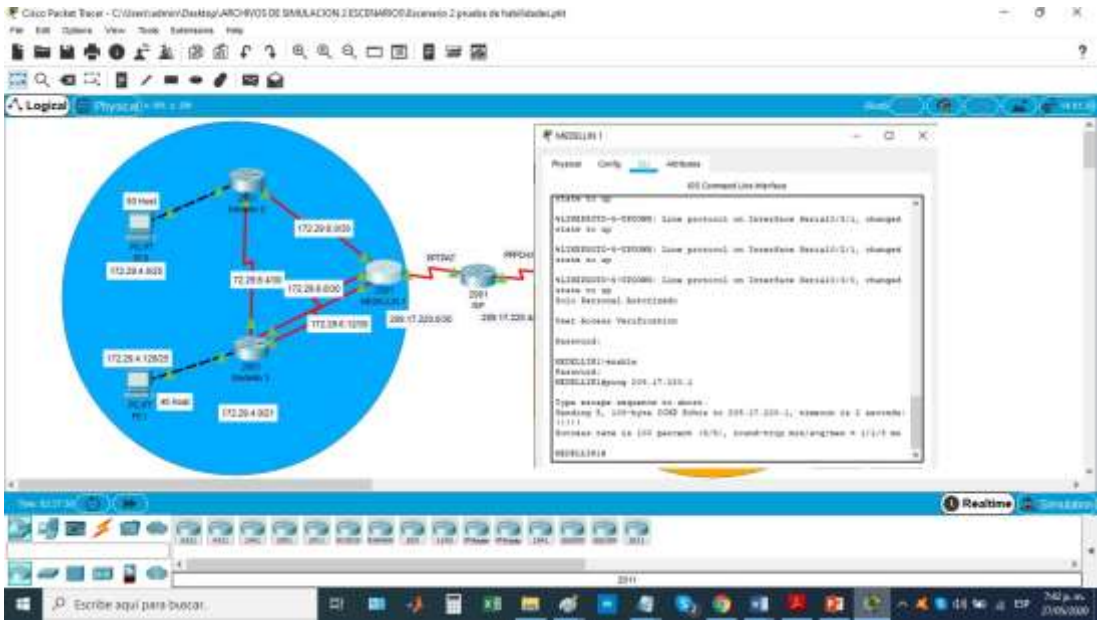
Nota: La autenticación debería ser PAP

ppp pap sent-username ISP password cisco

configuracion CHAP en el Medellin 1:
enable
config terminal
username ISP password cisco
interface s0/0/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username Medellin1 password cisco

verificamos mediante ping en Medellin 1:
enable
ping 209.17.220.1

Figura 54.verificacion ping en medellin 1

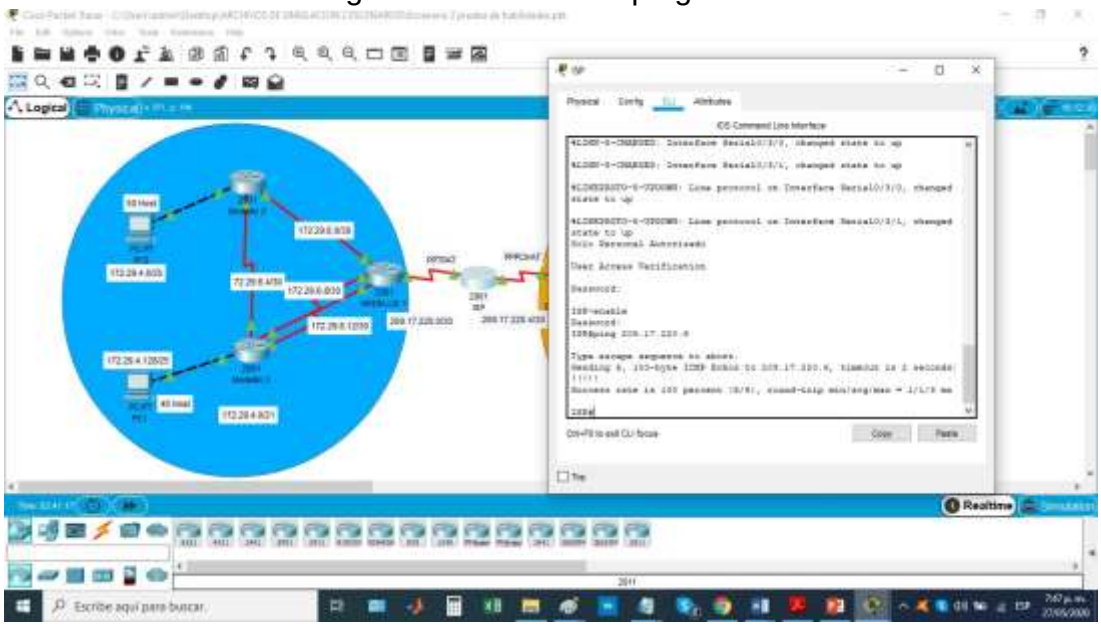


Fuente: Allan Echeverri Mateo

configuracion CHAP en el ISP para bogota:
enable
config terminal
username Bogota1 password cisco
interface s0/0/1
encapsulation ppp
ppp authentication chap

verificamos mediante ping en ISP:
enable
ping 209.17.220.6

Figura 55.verificacion ping en ISP



Fuente: Allan Echeverri Mateo

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

Nota: La autenticación debería ser CHAP

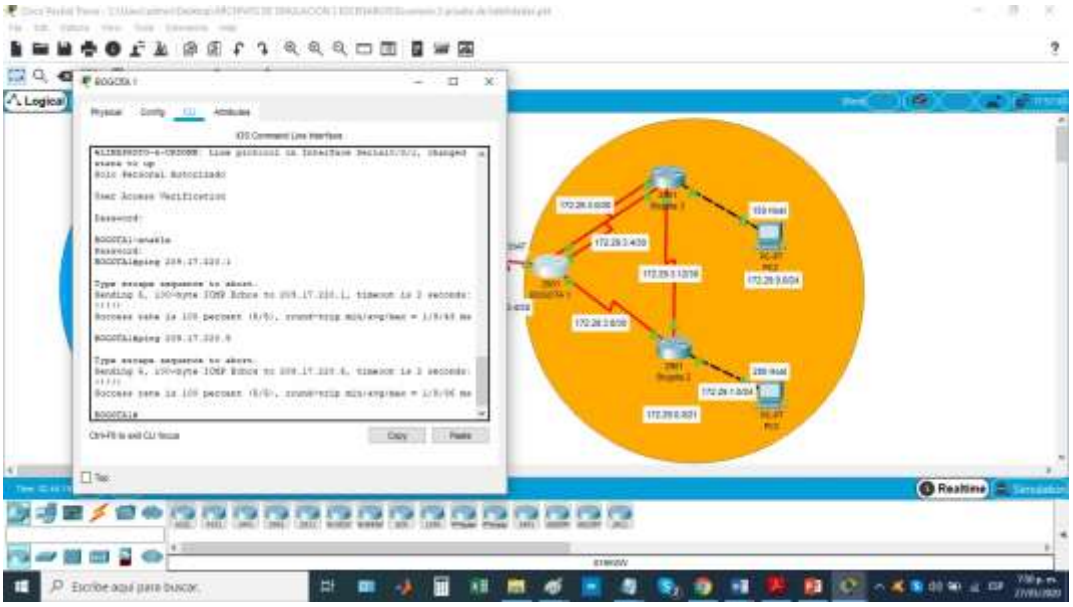
Configuracion CHAP en el ISP:
enable
config terminal
username Medellin1 password cisco
interface s0/0/0
encapsulation ppp
ppp authentication pap

Configuracion CHAP en el Bogota 1:
enable
config terminal
username ISP password cisco
interface s0/0/0
encapsulation ppp
ppp authentication chap

Parte 6: Configuración de PAT.

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

Figura 56. Ping desde Bogotá 1 a ISP y Medellín 1



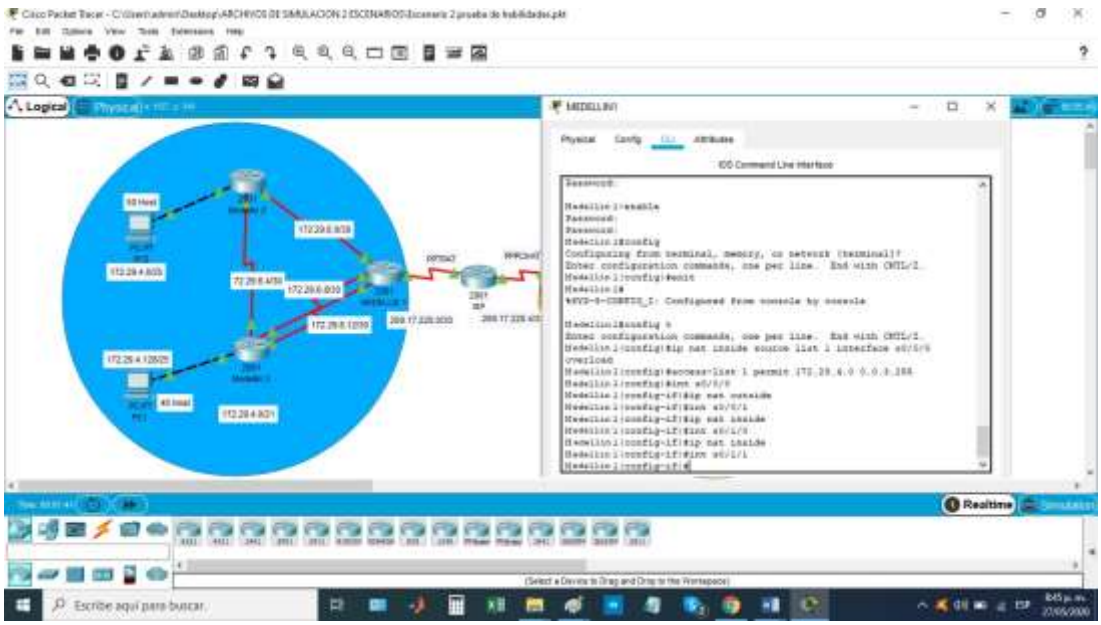
Fuente: Allan Echeverri Mateo

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

Configuramos la PAT en medellin 1:
ip nat inside source list 1 interface s0/0/0 overload
access-list 1 permit 172.29.4.0 0.0.3.255
int s0/0/0
ip nat outside
int s0/0/1
ip nat inside
int s0/1/0
ip nat inside
int s0/1/1

Procedemos a mostrar la PAT en medellín 1 ya activada

Figura 57. Activación PAT en Medellín 1

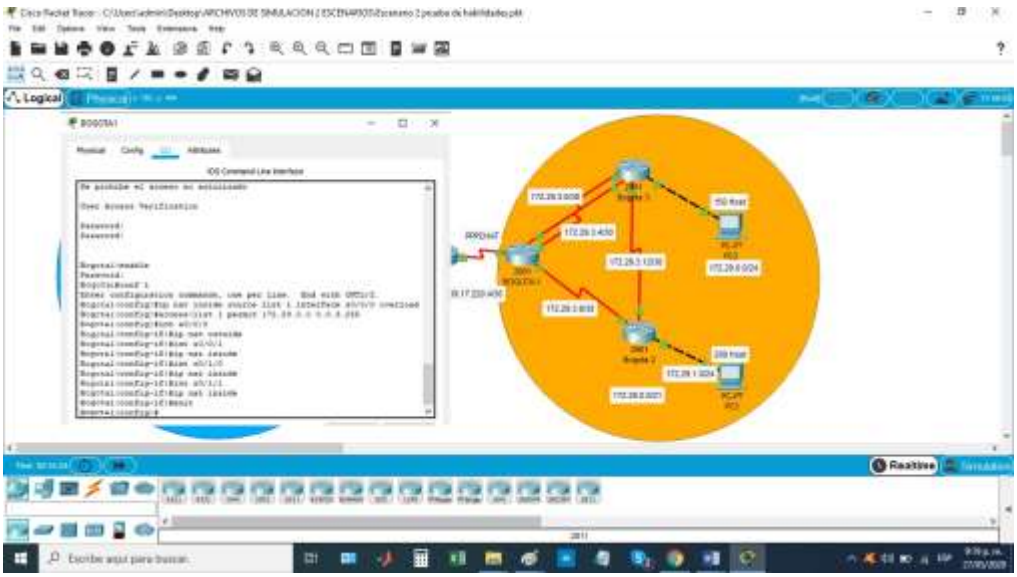


Fuente: Allan Echeverri Mateo

Configuramos la PAT en bogota 1:
ip nat inside source list 1 interface s0/0/0 overload
access-list 1 permit 172.29.0.0 0.0.3.255
int s0/0/0
ip nat outside
int s0/0/1
ip nat inside
int s0/1/0
ip nat inside

int s0/1/1
ip nat inside

Figura 58. Activación PAT en Bogota 1



Fuente: Allan Echeverri Mateo

c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Configuramos la NAT en bogota 1:
ip nat outside
interface s0/0/1
ip nat inside
interface s0/1/0
ip nat inside
interface s0/1/1
ip nat inside

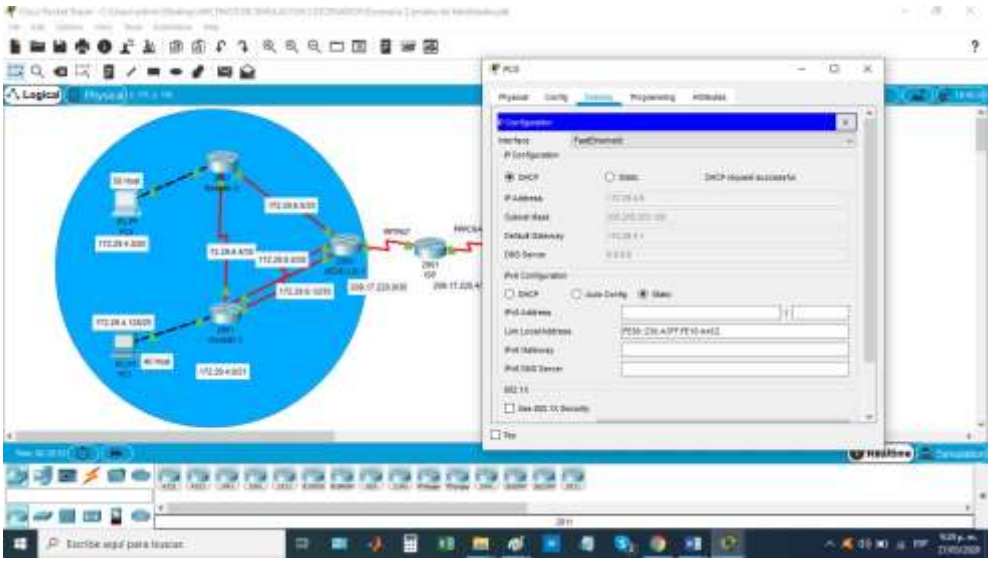
Parte 7: Configuración del servicio DHCP.
a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

Configuacion servicio DHCP en medellin 2:

enable
config terminal
ip dhcp excluded-address 172.29.4.1 172.29.4.5
ip dhcp excluded-address 172.29.4.129 172.29.4.133
ip dhcp pool Medellin2
network 172.29.4.0 255.255.255.128
default-router 172.29.4.1
dns-server 8.8.8.8
exit
ip dhcp pool Medellin3
network 172.29.4.128 255.255.255.128
default-router 172.29.4.129
dns-server 8.8.8.8
exit

verificamos en PC-0 que tenga la informacion DHCP

Figura 59. Verificación información DHCP en PC-0



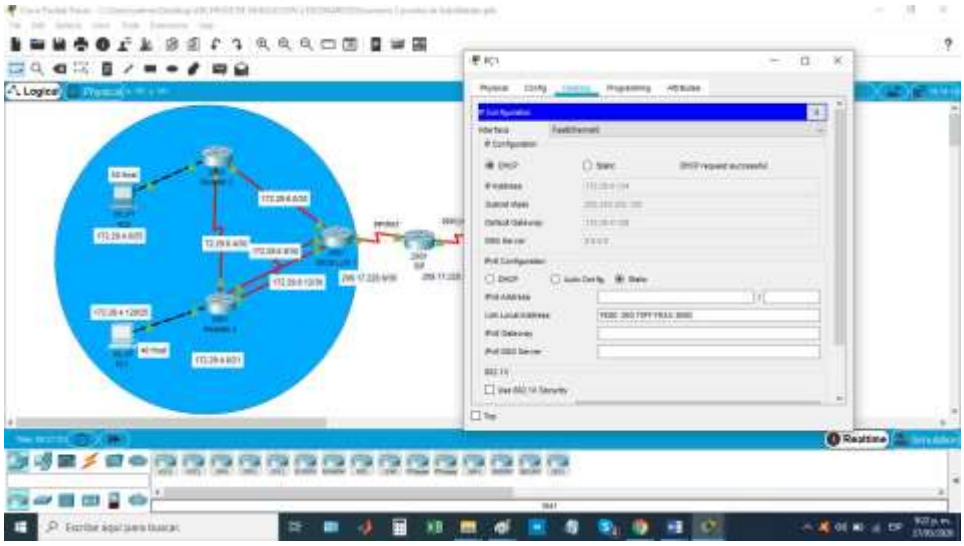
Fuente: Allan Echeverri Mateo

Configuracion servicio DHCP en medellin 3:

enable
config terminal
interface g0/0
ip helper-address 172.29.6.5

verificamos en PC-1 que tenga la informacion DHCP

Figura 60. Verificación información DHCP en PC-1



Fuente: Allan Echeverri Mateo

Configuracion servicio DHCP en Bogota 1:

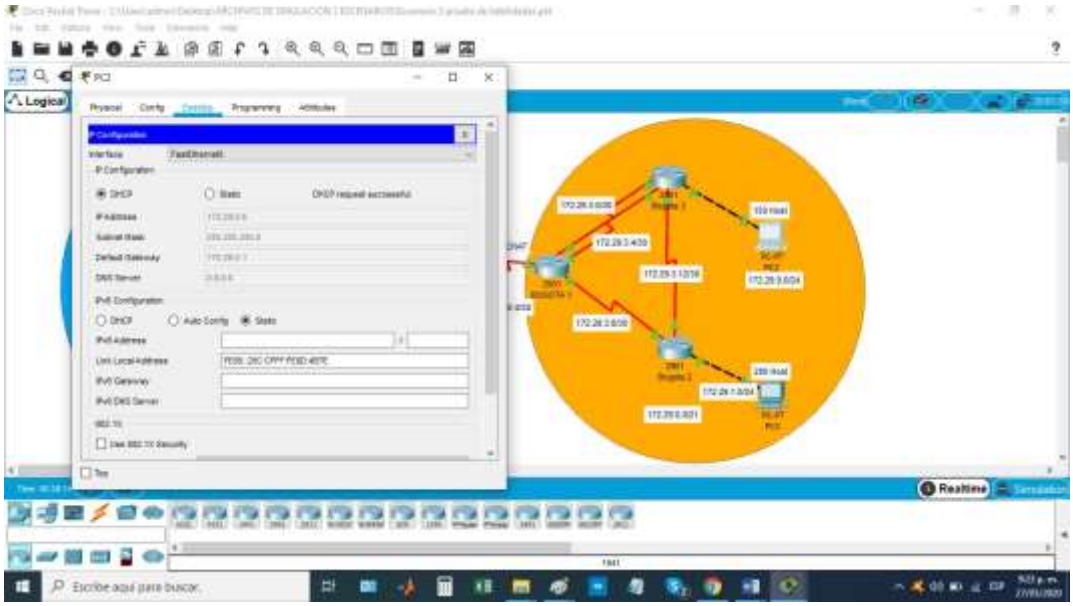
```
enable
config terminal
ip dhcp excluded-address 172.29.1.1 172.29.1.5
ip dhcp excluded-address 172.29.0.1 172.29.0.5
ip dhcp pool Bogota2
network 172.29.1.0 255.255.255.0
default-router 172.29.1.1
dns-server 8.8.8.8
ip dhcp pool Bogota3
exit
ip dhcp pool Bogota3
network 172.29.0.0 255.255.255.0
default-router 172.29.0.1
dns-server 8.8.8.8
```

configuramos DHCP en Bogota 3:

```
enable
config terminal
interface g0/0
ip helper-address 172.29.3.13
```

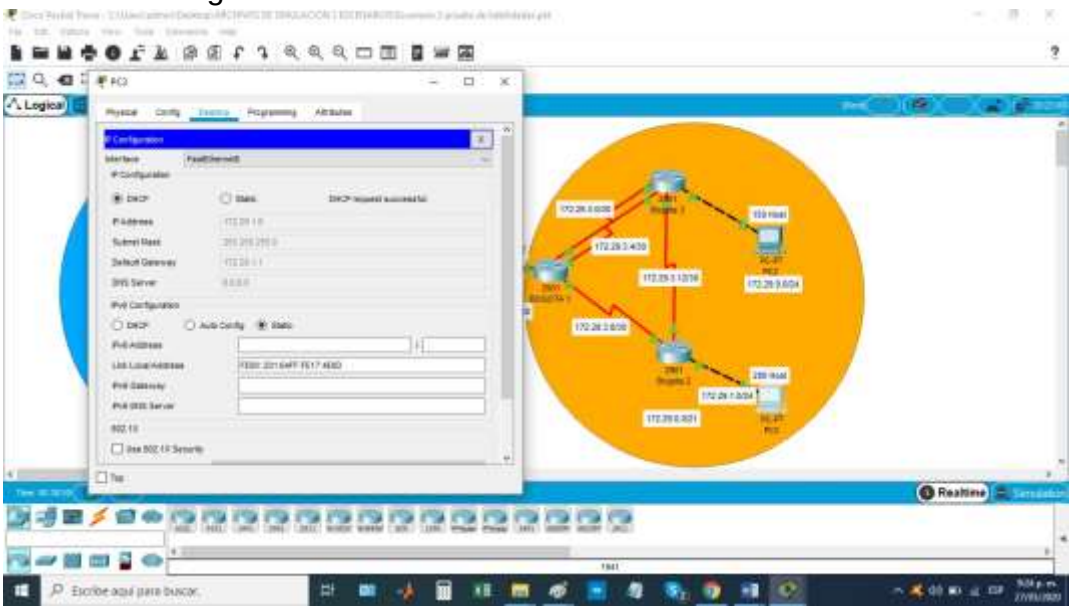
verificamos en PC-2 y PC-3 que tengan la informacion DHCP

Figura 61. Verificación información DHCP en PC-2



Fuente: Allan Echeverri Mateo

Figura 62. Verificación información DHCP en PC-3



Fuente: Allan Echeverri Mateo

6.1 ANÁLISIS DEL DESARROLLO DEL PROYECTO

El desarrollo de los 2 escenarios propuestos se dio de una manera ardua y laboriosa, ya que me equivoque muchas veces y no me funcionaba la conectividad a la hora de probar los pings en los diferentes dispositivos, ya que me faltaban algunos pasos o configuraba mal las direcciones IP en los dispositivos, pero al final se pudieron resolver dichos problemas.

Hay que resaltar que cada escenario fue configurado en un protocolo diferente, el primero con RIP y el segundo con OSPF, ya que son diferentes y cada uno requiere de una configuración distinta, pasos nuevos y adecuaciones que varían en cada dispositivo.

6.2 CRONOGRAMA

Fecha	Tiempo empleado	Punto Trabajado
07/05/2020	6 horas	Parte 1 y 2 escenario 1
10/05/2020	7 horas	Parte 2 y 3 Escenario 1
12/05/2020	5 horas	Parte 4 escenario 1
14/05/2020	8 horas	Parte 5 6 y 7 escenario 1
15/05/2020	6 horas	Parte 1 y2 escenario 2
19/05/2020	7 horas	Parte 3, 4 y 5 escenario 2
20/05/2020	8 horas	Parte 6 y 7 escenario 2, adecuación del cuerpo del trabajo
21/05/2020	4 horas	Adecuación cuerpo del trabajo

CONCLUSIONES

Pienso que el protocolo de enrutamiento OSPF a pesar de que busca calcular la ruta más corta entre nodos, me parece que es un poco más extensa en cuanto a configuración, ya que se deben configurar diferentes parámetros dentro de la misma como NAT, CHAP, PPP entre otros.

Se debe usar la versión 2 del OSPF ya que en el segundo escenario de la prueba se emplean solo redes IPv4

El enrutamiento RIP constituye un protocolo de puerta de enlace interna entre routers, que nos permite validar la información de las configuraciones que vamos realizando en cuanto a interfaces, rutas y dispositivos conectados en una red tanto IPV4 como IPV6

El uso de la plataforma de CISCO es una gran ayuda y representa una herramienta de una gran importancia ya que facilita el entendimiento en cuanto al tema de las telecomunicaciones y sus afines, mostrando de forma interactiva el proceso y desarrollo de una red de esta índole.

El encriptar las claves y poner seguridad a los dispositivos representa una gran opción si se requiere implementar dicho sistema a la solución de un problema real, como la red de telecomunicaciones de una empresa, un hospital, una entidad bancaria entre otros.

RECOMENDACIONES

En el desarrollo de este trabajo se me presentaron varias dificultades en cuanto a la solución del escenario 2, tanto así que tuve que cambiar la versión del packet tracer porque en la versión 6.2 student que empleé en el primer escenario no me quería darpara el segundo, así que descargué la versión 7.3 la más actualizada y luego de muchas horas de intentar por fin me funcionó y pude cumplir con lo requerido en el trabajo, así que si no funciona con una versión es mejor descargar otra y probar de nuevo.

Otra recomendación que doy es verificar muy bien el orden de los pasos a la hora de configurar, ya que en mi caso primero estaba configurando los servidores DHCP antes que la PAT, por lo que no me permitía verificar la información en los PC-2 y PC-3 respectivamente, una vez hice de nuevo todos los pasos en el orden correspondiente pude ve que me funciono correctamente.

BIBLIOGRAFÍA

(*Cómo Configurar RIP - CCNA Desde Cero*, n.d.) Disponible en: https://ccnadesdecero.com/curso/configurar-rip/

(*Configuración del Protocolo de enrutamiento OSPF en Packet Tracer — Steemit*, n.d.) Disponible en: https://steemit.com/spanish/@michelylopez/configuracion-del-protocolo-de-enrutamiento-ospf-en-packet-tracer

(*IPv6 Routing: RIP for IPv6 - Cisco*, n.d.) Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/xe-3s/asr1000/ip6-rip-xe.html

(*RIP - PPP PAP CHAP - DHCP - PAT - YouTube*, n.d.) Disponible en: https://www.youtube.com/watch?v=ANBWSadVSPY

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9