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

ÁNGELA MARÍA CALLE GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERA
INGENIERIA DE SISTEMAS
DOSQUEBRADAS
2020

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

ÁNGELA MARÍA CALLE GARCÍA

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

DIEGO EDISON RAMÍREZ CLAROS
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERA
INGENIERIA DE SISTEMAS
DOSQUEBRADAS
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Manizales, 20 de mayo de 2020

Dedicatoria:

Dedico este trabajo a Dios que me ha dado la oportunidad de culminar mi carrera.

AGRADECIMIENTOS

Gracias a Dios por darme la paciencia, la fortaleza y las capacidades para cumplir este sueño; a mis padres, hermanos y sobrinos por estar siempre presentes en cada etapa de este proceso.

A los tutores por su acompañamiento y su transmisión de conocimientos.

TABLA DE CONTENIDO

TABLAS

TABLA DE FIGURAS

GLOSARIO

ACL: le muestra al router los paquetes que debe aceptar o rechazar en base a las condiciones establecidas en ellas y que permiten la administración del tráfico y aseguran el acceso, bajo esas condiciones, hacia y desde una red

Encapsulamiento: es una forma de dar seguridad a los datos, ya que no son fácilmente visibles para cualquier usuario.

Enrutamiento: es la forma en que los enrutadores, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas (las más rápidas) para intercambiar datos entre las mismas.

Protocolos: Son reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física.

LAN: Sigla en inglés que significa Local Area Network. Es una red de área local de corto alcance.

NAT: Proceso mediante el cual se puede llegar a que redes de ordenadores utilicen un rango de direcciones especiales y se conecten a Internet usando una única dirección IP.

WAN: es la sigla de Wide Area Network (“Red de Área Amplia”). Esta es una red de rango más amplia y que une varias redes

RESUMEN

En este documento se prueban las habilidades aprendidas en el Seminario de Profundización CISCO que incluyen el soporte de LAN / WAN, así como la interconexión y configuración de cada dispositivo que conforma los dos escenarios propuestos, acorde con los lineamientos establecidos como el enrutamiento en soluciones de red, listas de control de acceso, OSPFv2, DHCP, protocolo Rip, NAT y CHAT. El proceso se realizó utilizando la herramienta de simulación Packet Tracer y aplicando los conocimientos que se aprendieron durante la carrera.

El diseño e implementación de redes, inicia con la configuración básica de los dispositivos que componen la topología de red, donde se usan comandos y protocolos de enrutamiento y seguridad y mediante comandos como show router, show ip protocols, ping se hace la demostración de la configuración y buen funcionamiento de la red

PALABRAS CLAVE: Redes, protocolos, comandos, direccionamiento ip, topología de red.

1. INTRODUCCIÓN

El presente trabajo contiene el desarrollo de la Evaluación – Prueba de habilidades prácticas CCNA, correspondiente a la finalización del Seminario de Profundización CISCO, el cual consta de dos escenarios, en los cuales se aplican los conocimientos aprendidos durante este periodo académico y que tiene como temáticas estudiadas: Fundamentos de Networking, Modelo OSI y Direccionamiento IP.

De acuerdo a las topologías de red planteadas y los requisitos solicitados para su implementación y funcionamiento se requiere de dispositivos de red, como: routers, servidores, switches, host y cables serial y ethernet, los cuales requieren una configuración básica de seguridad en dispositivos de comunicación, además de una aplicación de routing, Vlans, protocolo RIP, el servicio de DHCP, protocolo de enrutamiento OSPF, listas de acceso, NAT, configuración de encapsulamiento y autenticación PPP.

Para la realización de los dos laboratorios se utiliza como herramienta, el simulador Packet Tracert.

1. OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar las habilidades obtenidas durante este Seminario de Profundización CISCO, para identificar y aplicar una solución a un caso o situación estudio de problema de Networking basada en la vida real.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Configurar dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en los Router y demás políticas necesarias.
- Realizar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing, de DHCP, NAT, RIP Ver2 y demás permitiendo dar solución a ciertos problemas.
- Verificar las configuraciones y protocolos mediante comandos como: ping, show run, show ip protocols, show ip OSPF neighbor

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Escenario1: 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.

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.

3.2 JUSTIFICACIÓN

Los problemas planteados mediante los escenarios antes expuestos, representan dos casos de la vida real, por lo tanto, requieren una solución óptima mediante el diseño e implementación de redes telemáticas que permitan su conectividad y buen funcionamiento, por eso en este trabajo se muestra el paso a paso de cómo construir su topología y la configuración de sus dispositivos.

Las herramientas utilizadas para el desarrollo de esta prueba de habilidades es principalmente el simulador Packet Tracert, que permite la configuración y pruebas de las redes.

4. MATERIALES

4.1 MATERIALES

Computador.

Internet.

Simulador Packet Tracert.

4.2 METODOLOGÍA

Simulaciones.

Laboratorio remoto.

Asesorías por Skype.

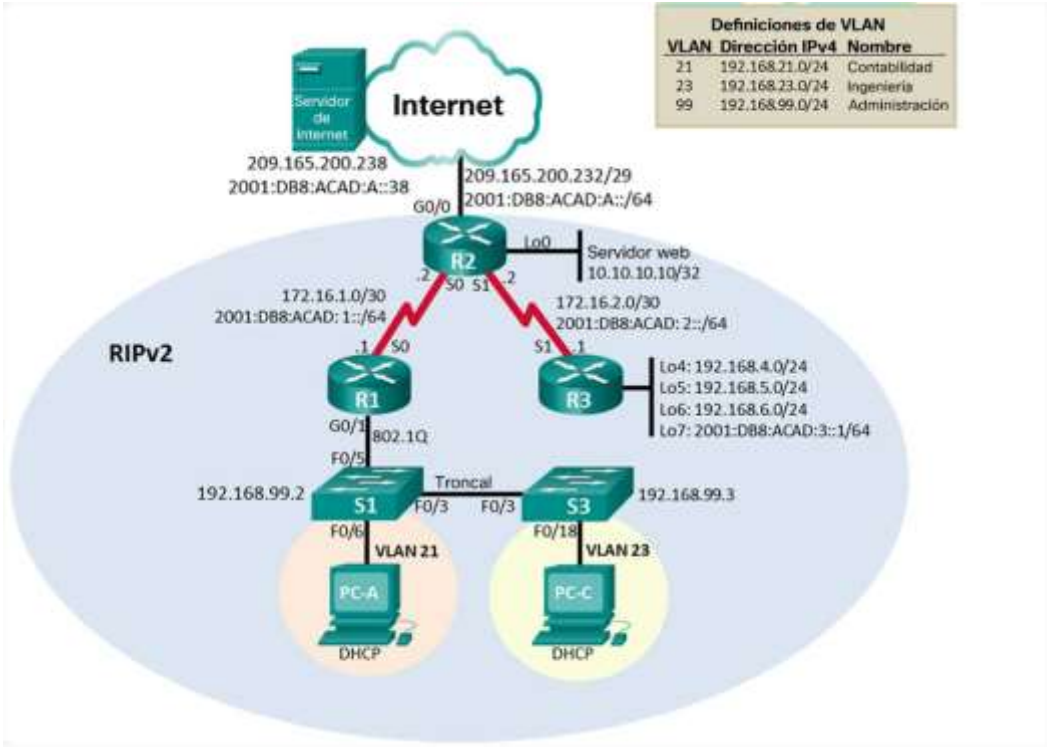
4. DESAROLLLO DEL PROYECTO
SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

5.1 ESCENARIO 1

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

5.1.1 TOPOLOGÍA DE RED

Figura 1. Topología de la red planteada escenario 1

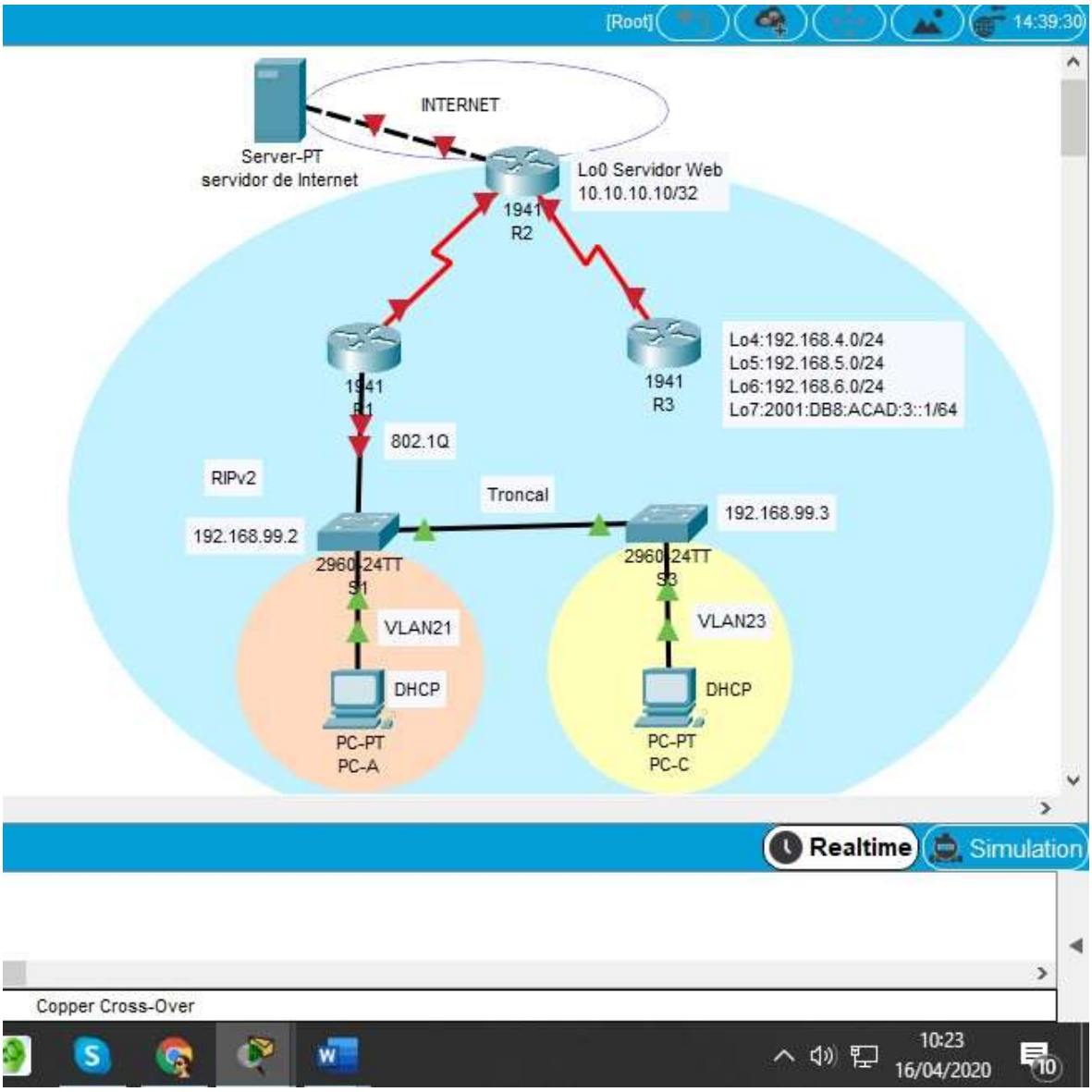


Dispositivos Requeridos

- 3 Routers (Cisco 1941) con 2 puertos FastEthernet, 2 puertos Seriales
- 2 Switches (Cisco 2960)
- 1 Servidor (Genérico PT)
- 2 PCs con sistema operativo Windows 7, con tarjeta de red

- Cables Serial y Ethernet

Figura 2. Topología de la red realizada escenario 1



5.1.1.1 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.

Para inicializar y volver a cargar los routers y los switches, utilizamos comandos que permitan eliminar el archivo startup-config del router o Switch, eliminar la base de datos de VLAN anterior, es decir que los dispositivos queden sin ninguna configuración y arrancar de cero.

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 está en la memoria flash en ambos switches	Switch>enable Switch#dir flash:

5.1.1.2 Parte 2: Configurar los parámetros básicos de 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 1. Direccionamiento

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

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.

En este paso empezamos a hacer la respectiva configuración de direccionamiento, de acuerdo a la tabla y la topología suministrada.

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	Cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	Cisco 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-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd %Se prohibe el acceso no autorizado%

Interfaz S0/0/0	Establezca la descripción R1(config)#int s0/0/0 R1(config-if)#description Connection to R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 Establecer la frecuencia de reloj en 128000 R1(config-if)#clock rate 128000 Activar la interfaz R1(config-if)#no shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config-if)#exit R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2
La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router#configure terminal Router(config)#no ip domain-lookup

Nombre del router	R2 Router#configure terminal Router(config)#no ip domain-lookup
Contraseña de exec privilegiado cifrada	Class R2(config)#enable secret class
Contraseña de acceso a la consola	Cisco R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	Cisco 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-line)#service password-encryption
Habilitar el servidor HTTP	Router (config) # ip http server Router (config) # ip http secure-server Router (config) # ip http autenticacion local Packet Tracert no soporta este comando
Mensaje MOTD	Se prohíbe el acceso no autorizado. R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	Establezca la descripción R2(config)#int s0/0/0 R2(config-if)#description Connection to R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 Activar la interfaz R2(config-if)#no shutdown

Interfaz S0/0/1	Establecer la descripción R2(config-if)#int s0/0/1 R2(config-if)#description Connection to R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)#ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config-if)#int g0/0 R2(config-if)#description Connection to Internet Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)#ip address 209.165.200.233 255.255.255.248 Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 Activar la interfaz R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config)#int g0/0 R2(config-if)#int loopback 0 Establezca la dirección IPv4. 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	Configure una ruta IPv4 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3
La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	R3 Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Class R3(config)#enable secret class
Contraseña de acceso a la consola	Cisco R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	Cisco 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-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/1	Establecer la descripción R3(config)#int s0/0/1 R3(config-if)#description Connection to R2 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R3(config-if)#ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1.
La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	S1 Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	Class S1(config)#enable secret class
Contraseña de acceso a la consola	Cisco S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	Cisco 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	Se prohíbe el acceso no autorizado. S1(config)#banner motd #Se prohbe el acceso no autorizado#

Paso 6: Configurar S3.
La configuración del S3 incluye las siguientes tareas:

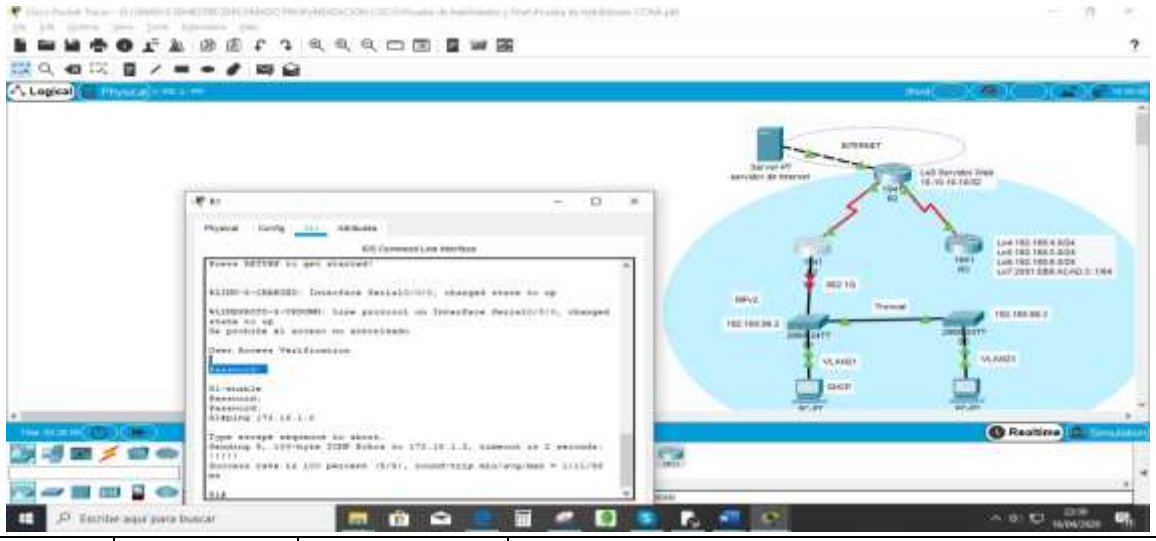
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#conf term Switch(config)#no ip domain-lookup
Nombre del switch	S3 Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	Class S3(config)#enable secret class
Contraseña de acceso a la consola	Cisco S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	Cisco 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	Se prohíbe el acceso no autorizado. S3(config-line)# banner motd #Se prohbe el acceso no autorizado#

Paso 7: Verificar la conectividad de la red
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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

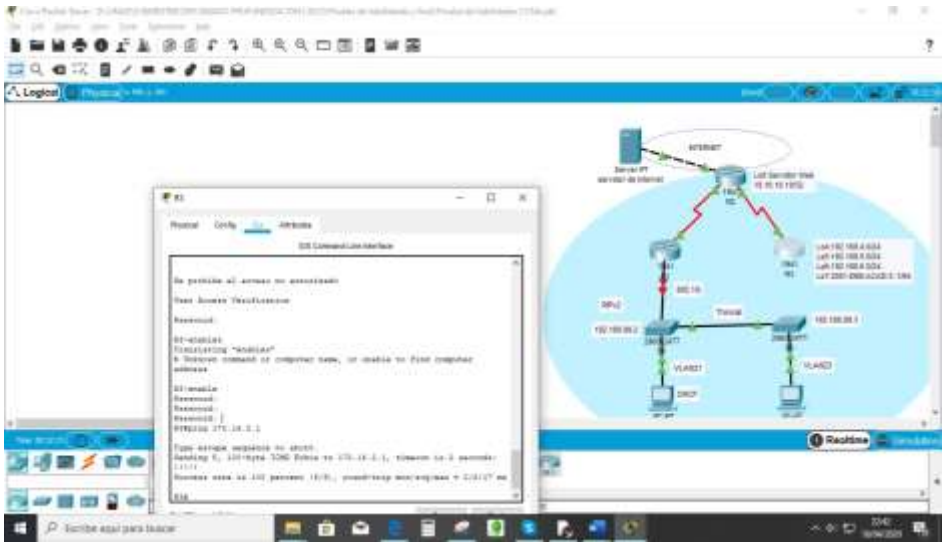
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2

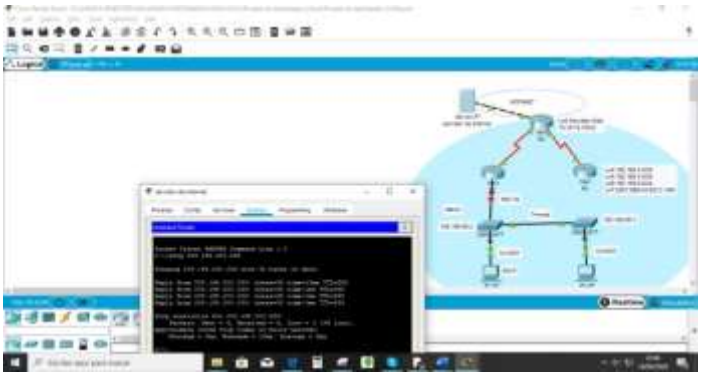
Figura 3. Ping de router 1 a router 2



R2	R3, S0/0/1	172.16.2.1	R3#ping 172.16.2.1

Figura 4. Ping de router 2 a router 3



PC de Inter-net	Gateway prede-termina-do	209.165.200 .233	C:\>ping 209.165.200.233 Figura 5. Ping de PC de Internet a Gateway predeterminado a 

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indicant S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config-vlan)#exit S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown

Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config-if)#exit S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#int 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	Utilizar la red VLAN 1 como VLAN nativa S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar S3
La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#

Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 Asignar la VLAN 21 R1(config-subif)#encapsulation dot1q 21 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.21.1 255.255.255.0

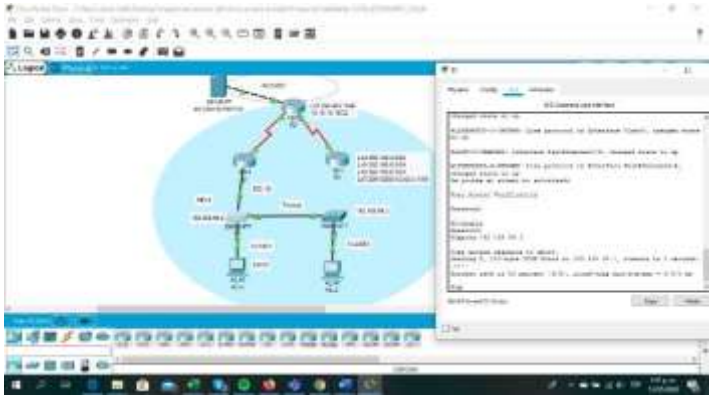
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 Asignar la VLAN 23 R1(config-subif)#encapsulation dot1q 23 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 Asignar la VLAN 99 R1(config-subif)#encapsulation dot1q 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad
Utilice el comando ping para probar la conectividad entre los switches y el R1.

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

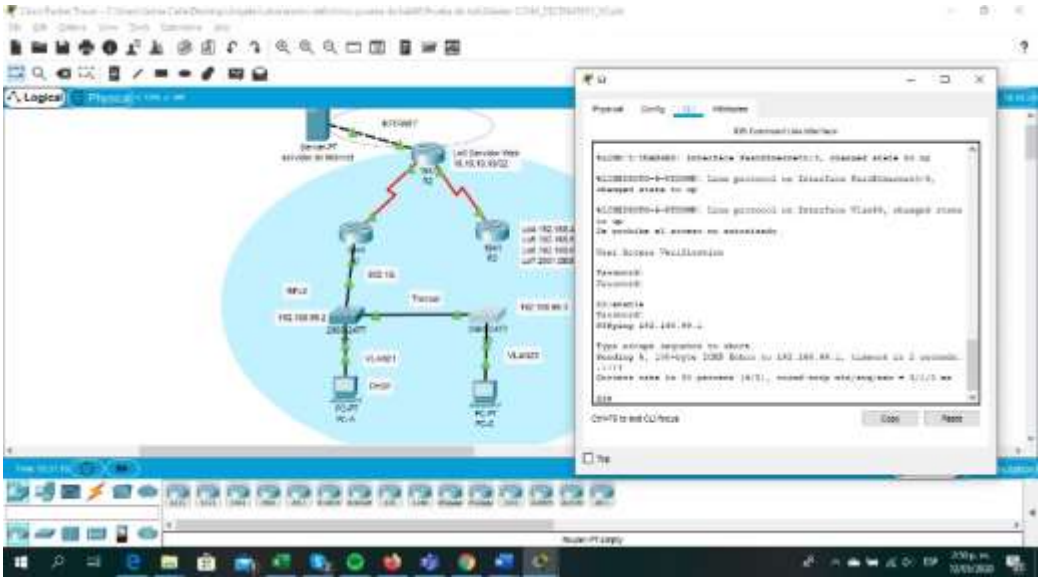
Desde	A	Dirección IP	Resultados de ping
S1	R1, dire-cción VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Figura 6. Ping desde S1 a R

Figura 7. Ping desde S1 a R



S3	R1, dire-cción VLAN 99	192.168.99.1	S3#ping 192.168.99.1

Figura 8. Ping desde S3 a R1



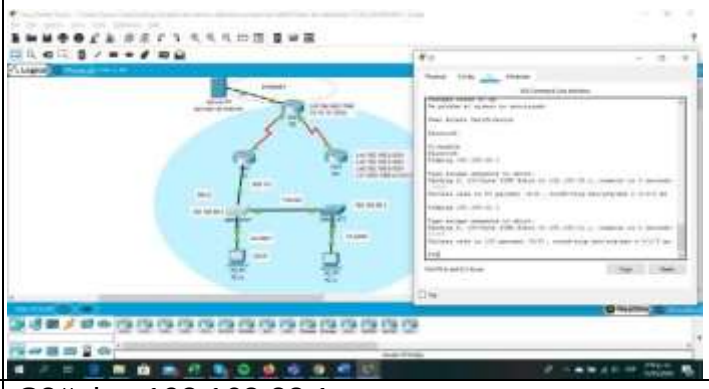
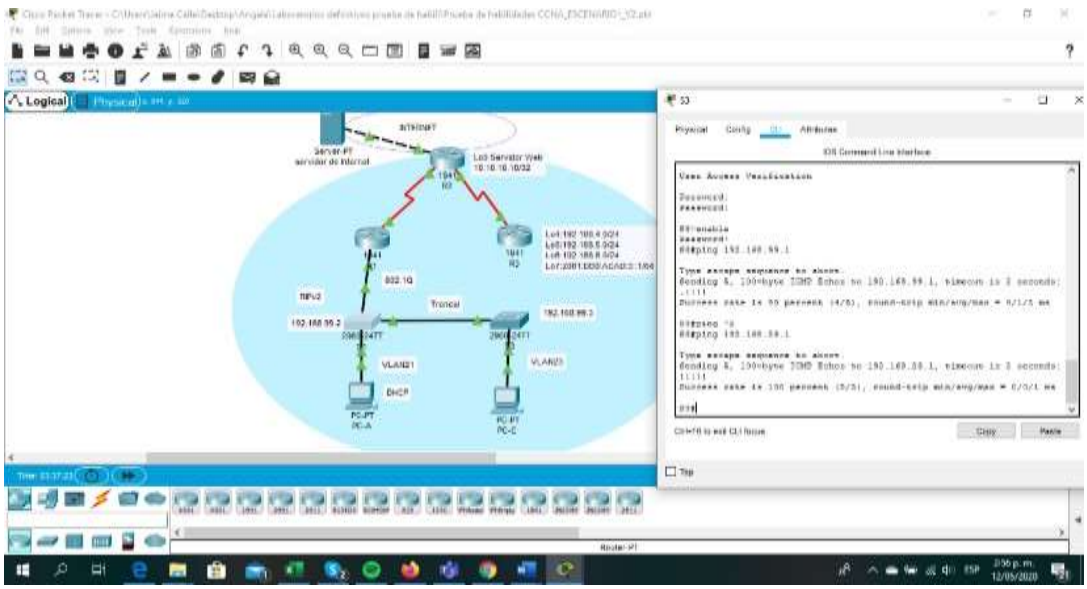
S1	R1, dire-cción VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Figura 8. Ping de S1 a R1 
S3	R1, dire-cción VLAN 23	192.168.23.1	S3#ping 192.168.23.1

Figura 9. Ping de S3 a R1



5.1.1.4 Parte 4: Configurar el protocolo del routing dinámico

Paso 1: Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0 R1(config-router)#
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:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2

Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#
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 RIPv3 en el R2
La configuración del R3 incluye las siguientes tareas:

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)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6 R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0 R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#no auto-summary
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 del RIP
La configuración del R3 incluye las siguientes tareas.

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

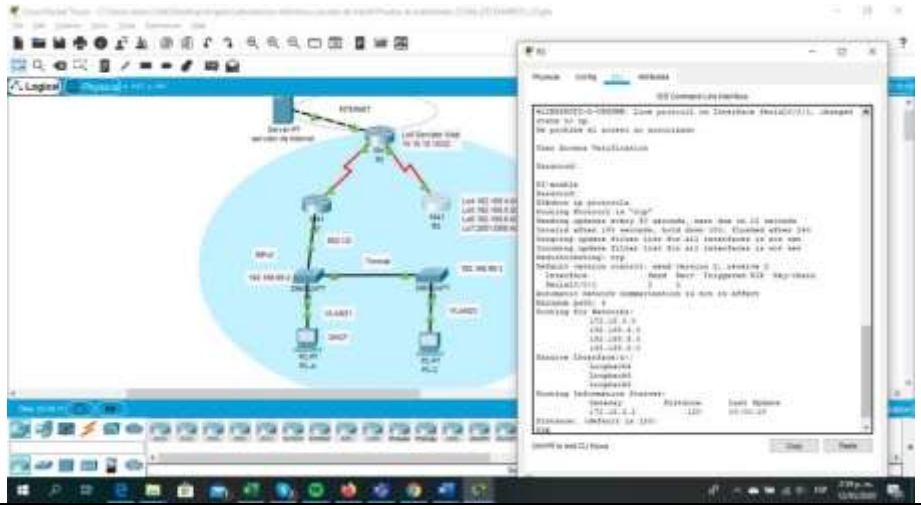
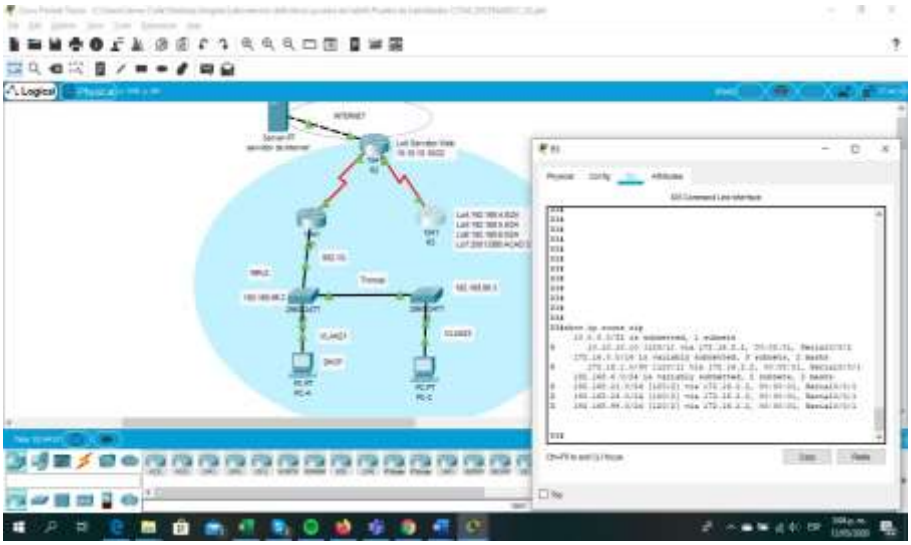
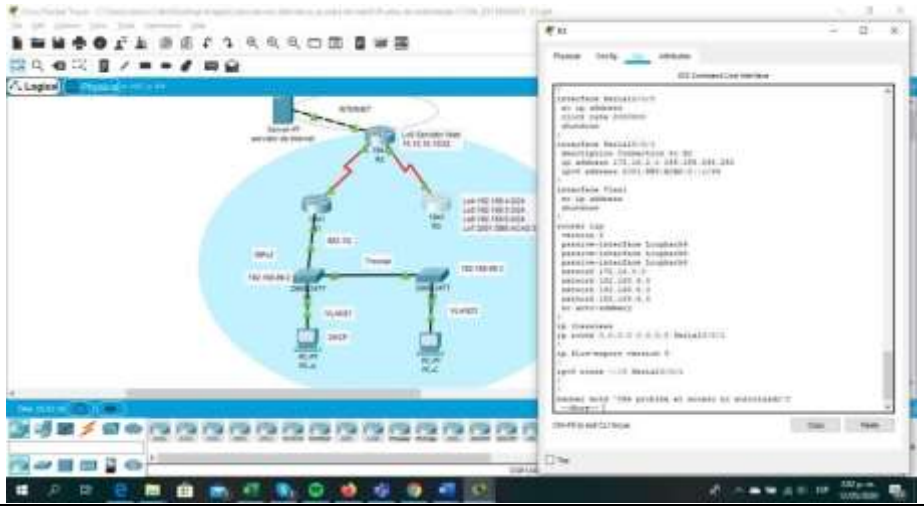
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configura-das en un router?	R3#show ip protocols Figura 10. Comando show ip protocols 
¿Qué comando muestra solo las rutas RIP?	R3#show ip route rip Figura 11.Comando show ip route 
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R3#show run section router rip

	Figura 12. Comando show run 

5.1.1.5 Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

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

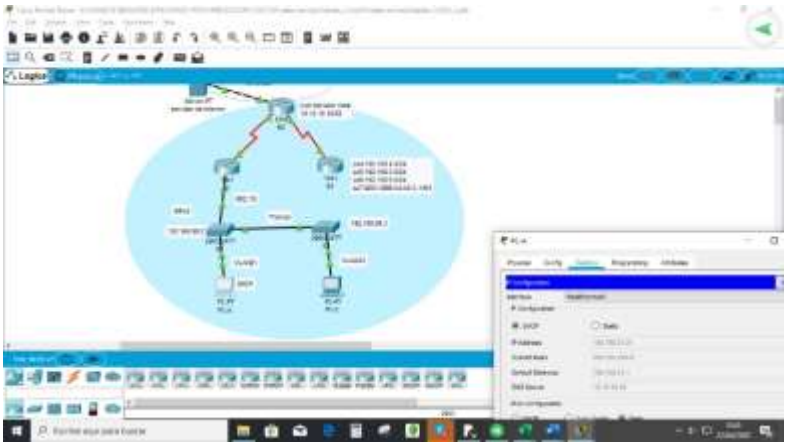
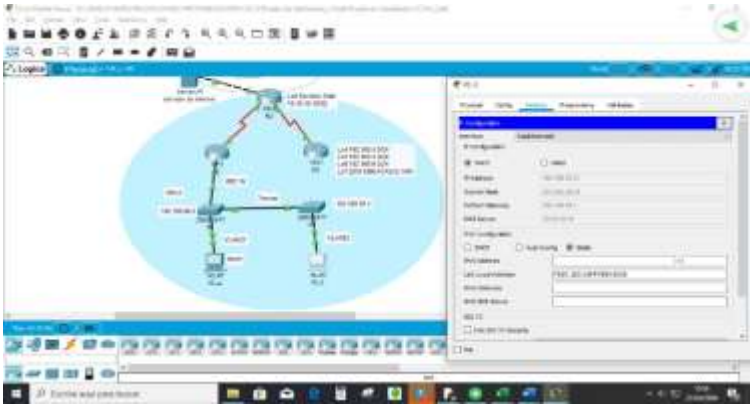
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Servidor DNS: 10.10.10.10 R1(dhcp-config)#dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)#domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.23.1

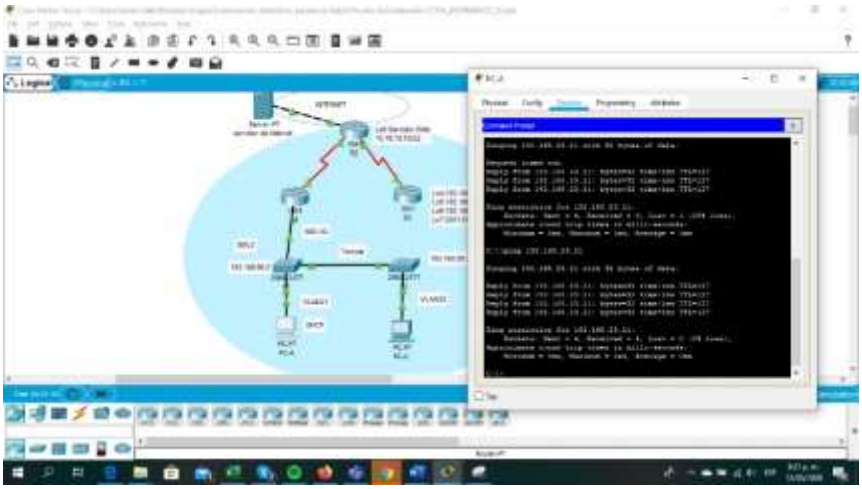
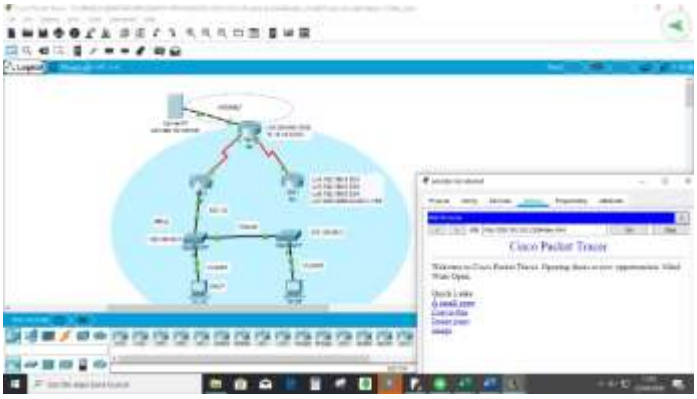
Paso 2: Configurar la NAT estática y dinámica en el R2.
La configuración del R2 incluye las siguientes tareas:

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

Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 2(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 192.4.0 0 0.0.3.255 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** – **209.165.200.248** 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.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 13. PC-A por DCHP 
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 14. PC-C por DHCP 

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 la PC-A a la PC-C 
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Figura 16. Acceso al servidor Web 

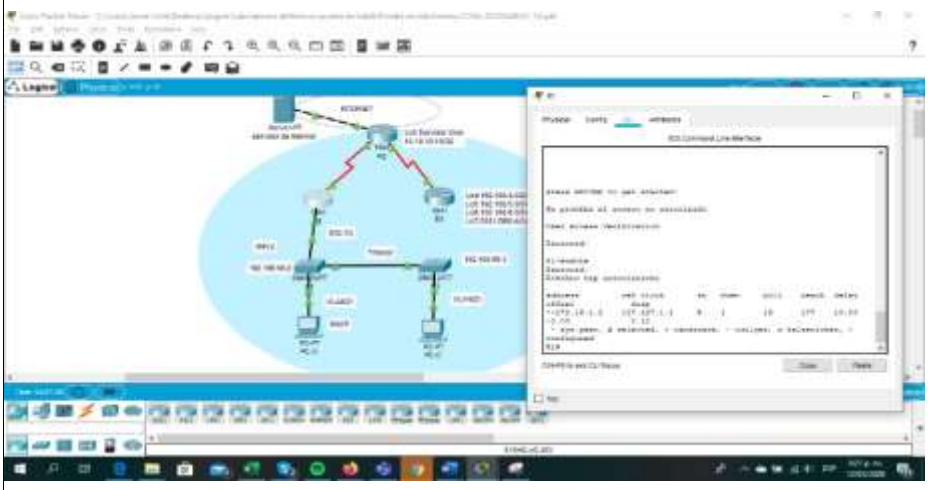
5.1.1.6 Parte 6: Configurar NTP

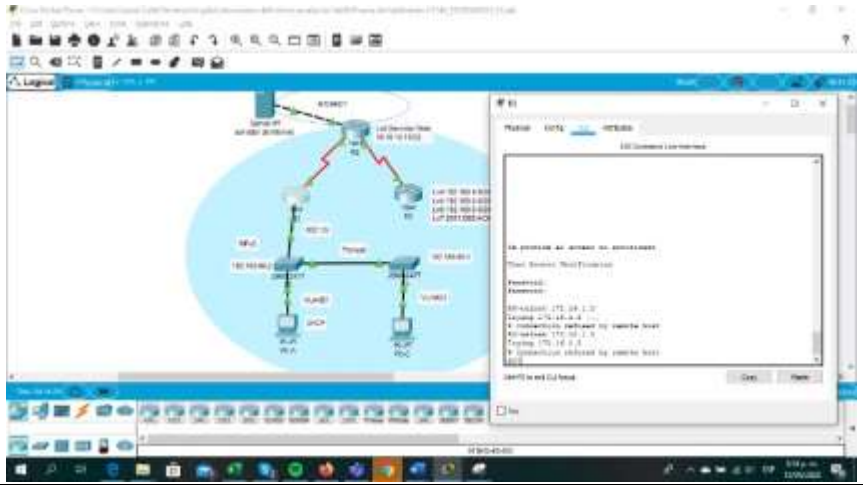
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp server 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

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

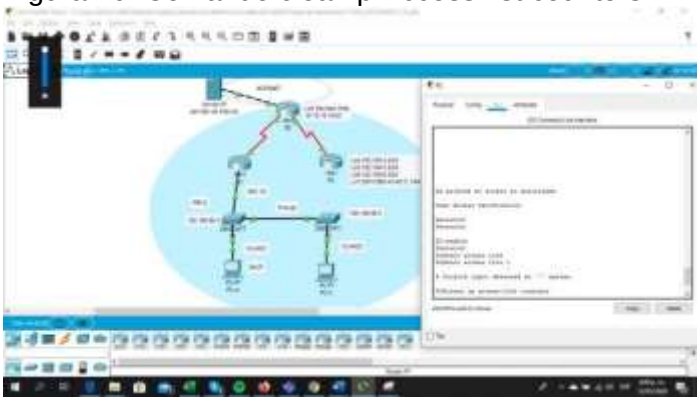
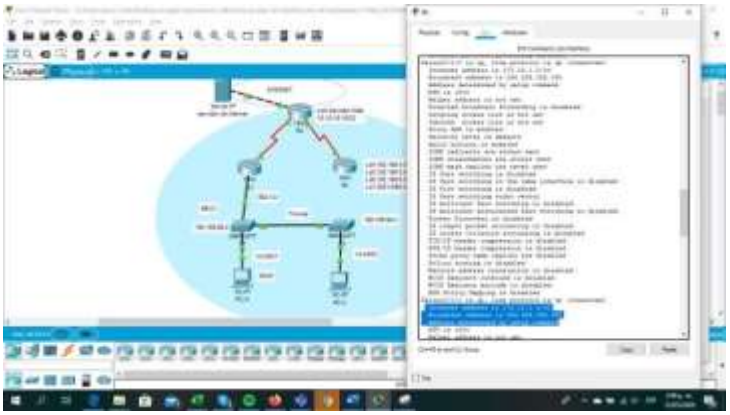
Paso 1: Restringir el acceso a las líneas VTY en el R2

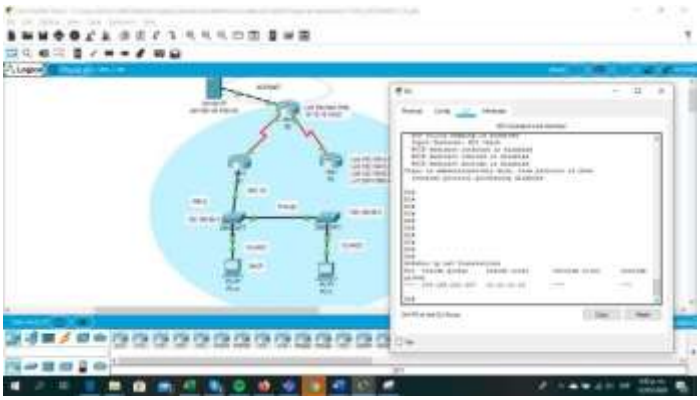
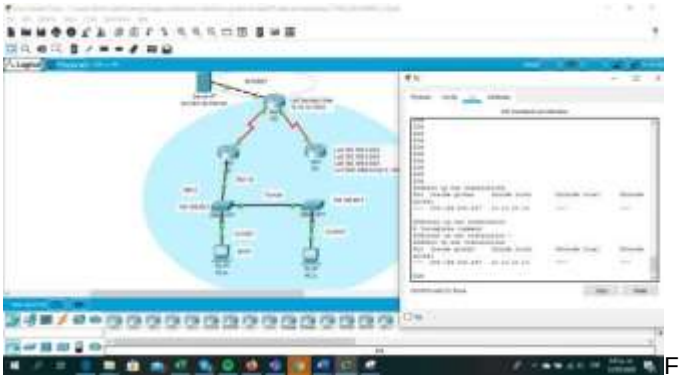
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** Figura 17. Comando show ntp associations  R2(config-std-nacl)# R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet

Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Figura 18. Funcionamiento de ACL 

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list Figura 19. Comando show acces-list en R2  R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (4 match(es)

Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters Packet Tracert no soporta este comando Figura 20. Comando clear ip Access-list counters  Comando clear ip Access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface Figura 21. Comando show ip interface 

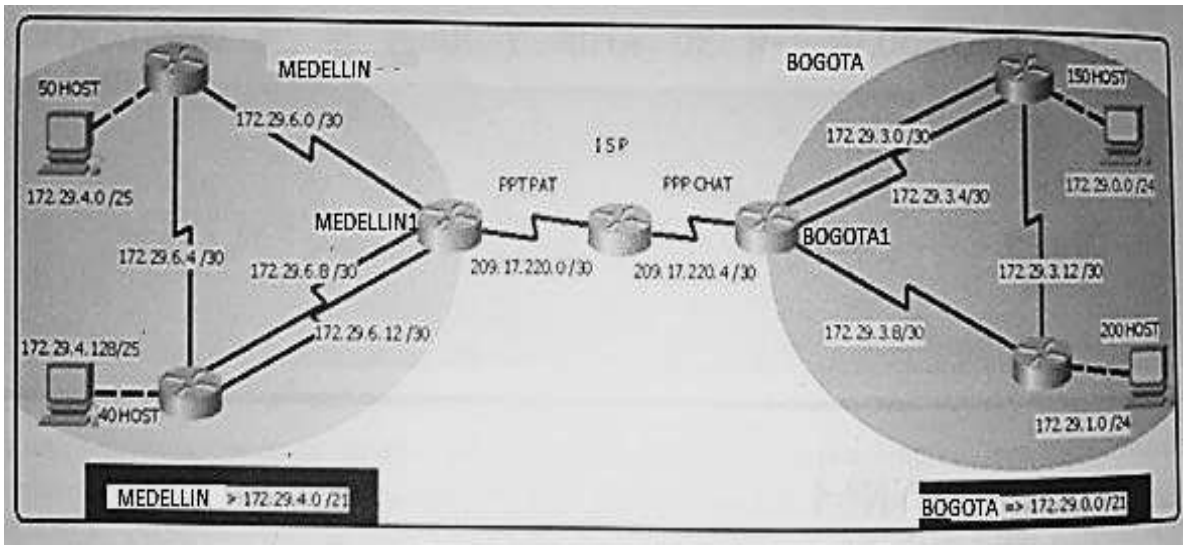
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2#show ip nat translations Figura 22. Comando show ip nat translations 
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * Figura 23. Comando show ip translations  F

5.2 ESCENARIO 2

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

5.2.1 TOPOLOGÍA DE RED

Figura 24. Topología de la red



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.

Como trabajo inicial se debe desarrollar lo siguiente:

a. Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
b. Rutinas de diagnóstico y configuración inicial.
   Se hace el diseño en Packet tracer con los equipos listos para su configuración, se agregaron módulos con puerto serial adicional para realizar la configuración en ciertos router que exigen más de dos conexiones por cable serial

c. Se configuran los routers se asigna el nombre y protocolos de seguridad, ejecutando las siguientes líneas de comandos:

RED MEDELLÍN
Router MEDELLÍN1
Router>enable
Router#config t
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#line vty 0 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#service password-encryption
MEDELLIN1 (config)#banner motd %Se prohibe el acceso no autorizado%

Router MEDELLIN2
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#no ip domain lookup
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#line vty 0 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#service password-encryption
MEDELLIN2(config)#banner motd %Se prohibe el acceso no autorizado%
Router MEDELLIN3
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco

MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#line vty 0 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#service password-encryption
MEDELLIN3(config)#banner motd %Se prohibe el acceso no autorizado%

RED ISP
Router ISP
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#service password-encryption
ISP(config)#banner motd %Se prohibe el acceso no autorizado%

RED BOGOTÁ
BOGOTÁ1
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname BOGOTA1
BOGOTA1(config)#enable secret class
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#line vty 0 15
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#service password-encryption
BOGOTA1(config)#banner motd %Se prohibe el acceso no autorizado%

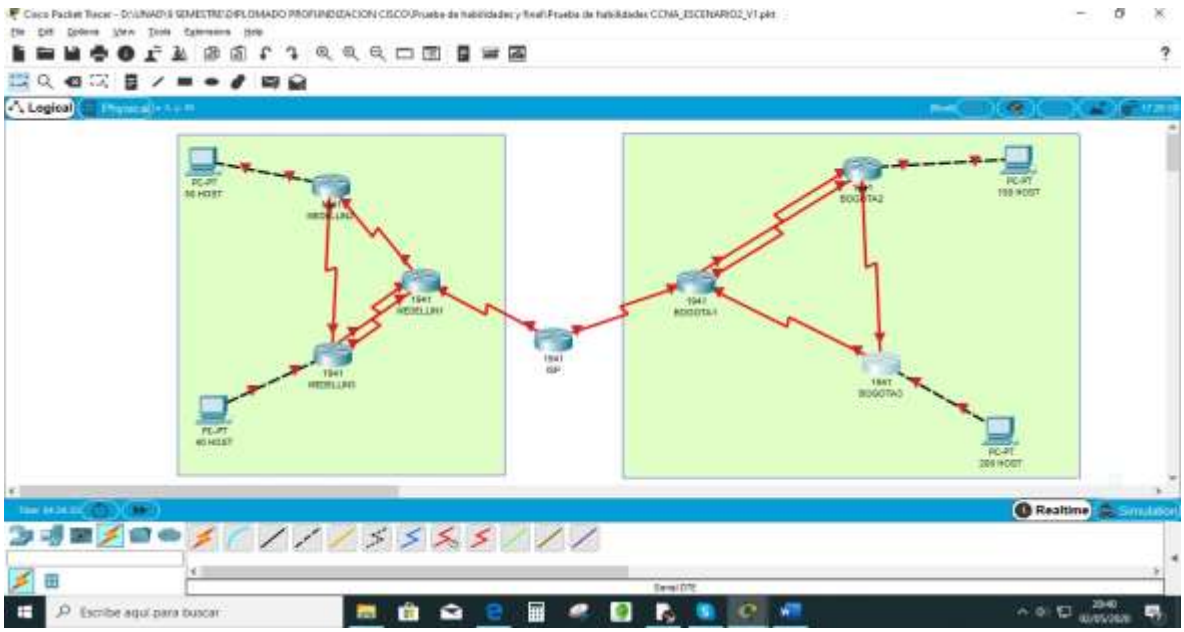
Router BOGOTÁ2
Router>enable
Router#conf t
Router(config)#no ip domain lookup

```
Router(config)#hostname BOGOTA2
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#service password-encryption
BOGOTA2(config)#banner motd %Se prohibe el acceso no autorizado%
```

```
Router BOGOTA3
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname BOGOTA3
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#service password-encryption
BOGOTA3(config)#banner motd %Se prohibe el acceso no autorizado%
BOGOTA3(config)#exit
```

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

Figura 25. Topología de la red realizada escenario 2



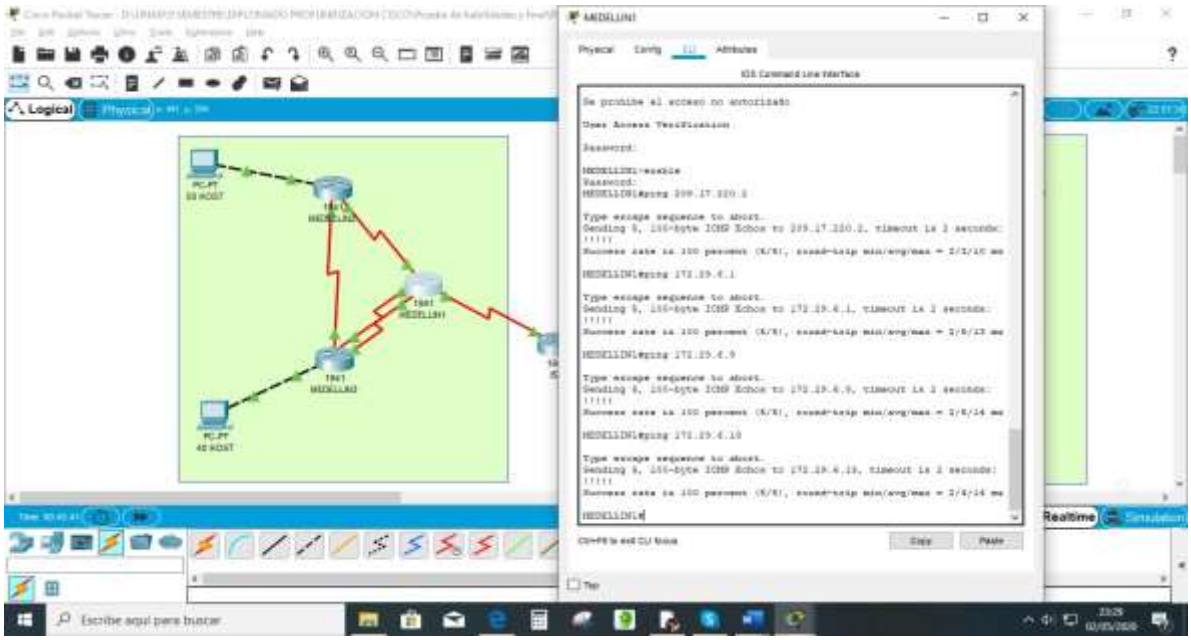
ISP
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown

ISP(config-if)#int s0/0/1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown

MEDELLÍN 1
MEDELLIN1#enable
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000

MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#

Figura 26. Ping de MEDELLIN1 a ISP

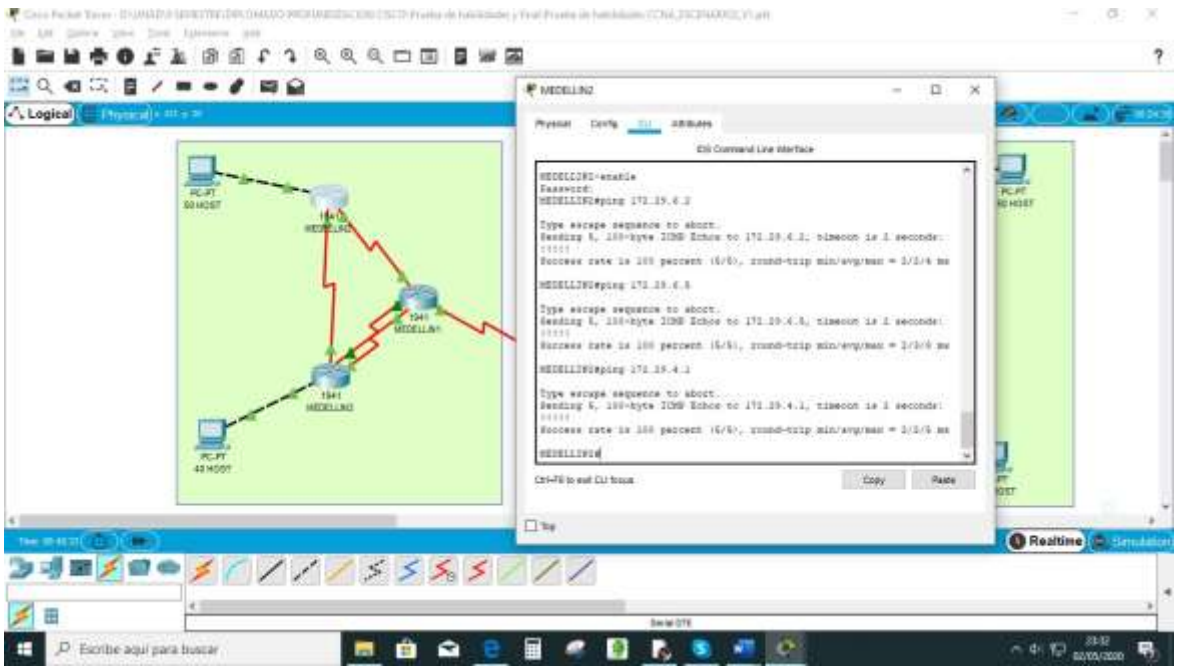


MEDELLÍN 2
MEDELLIN2(config)#int s0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#no shut

MEDELLIN2(config-if)#int s0/0/1
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 4000000
MEDELLIN2(config-if)#no shut

MEDELLIN2(config-if)#int g0/0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shut

Figura 27. Ping de MEDELLIN2 a MEDELLIN3-MEDELLIN1



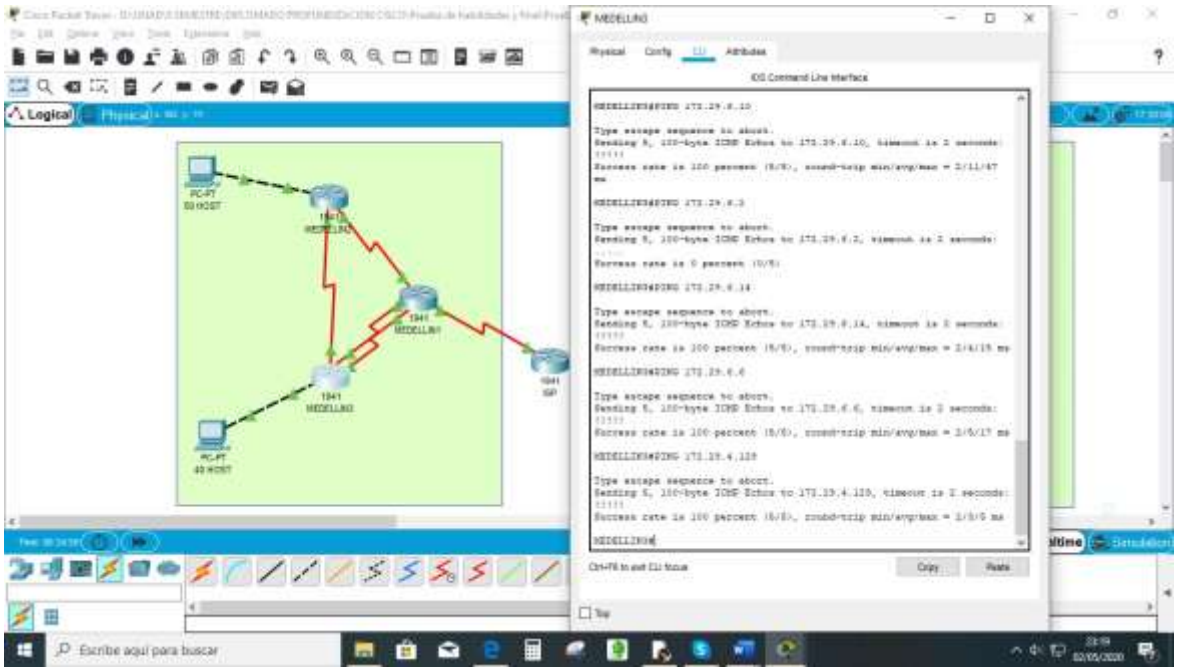
MEDELLÍN 3
MEDELLIN3>enable
Password:
MEDELLIN3#enable
MEDELLIN3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int s0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#no shut

MEDELLIN3(config-if)#int s0/0/1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#no shut

MEDELLIN3(config-if)#int s0/1/0
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#no shut

MEDELLIN3(config-if)#int g0/0
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)#no shut

Figura 28. Ping de MEDELLIN3 a MEDELLIN3-MEDELLIN1



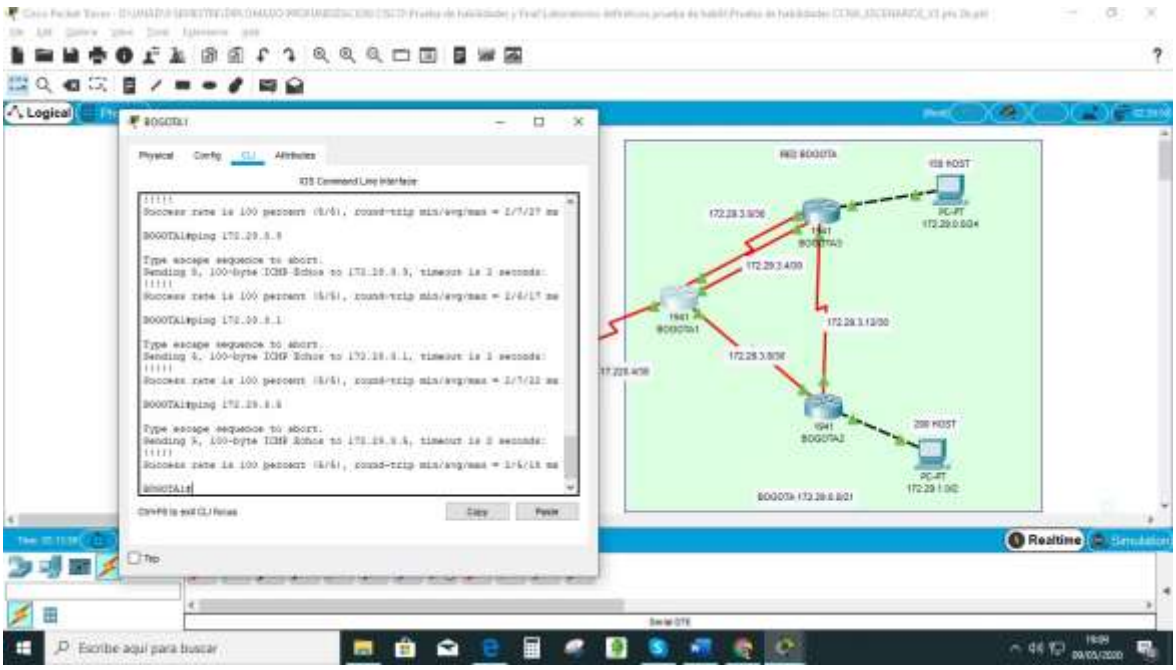
d. Configuración de Direccionamiento IP

Router BOGOTA 1
BOGOTA1#conf t
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#no shut
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shut

BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shut

BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shut

Figura 29. Ping de BOGOTA1 a BOGOTA2 – BOGOTA3

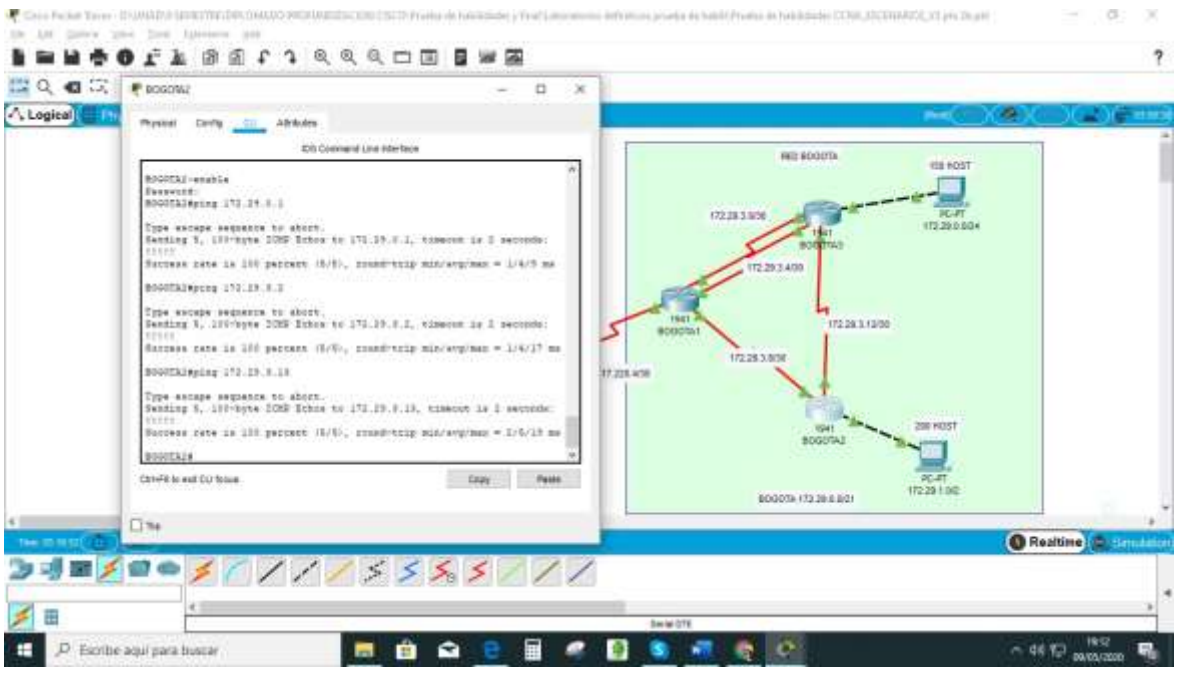


Router BOGOTA 2
BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)#no shut

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

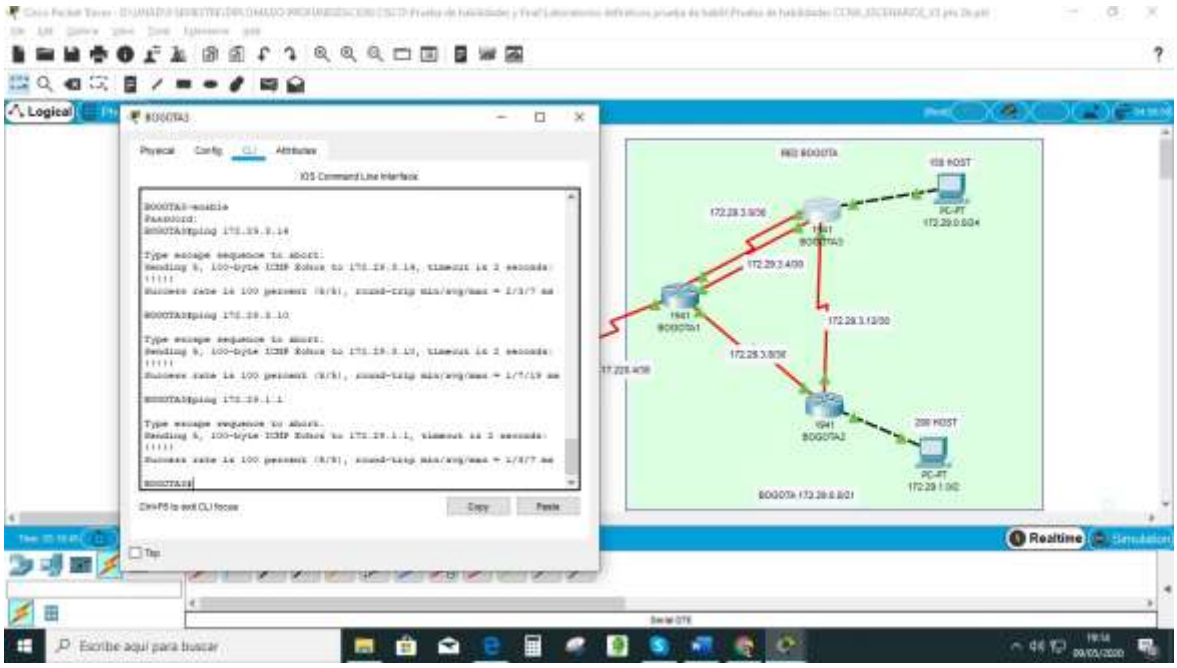
BOGOTA2(config-if)#int s0/0/1
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 4000000
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#
BOGOTA2(config-if)#int g0/0
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.252.0
BOGOTA2(config-if)#no shut

Figura 30. Ping de BOGOTA2 a BOGOTA3 – BOGOTA1



Router BOGOTÁ 3
BOGOTA3#int s0/0/0
BOGOTA3#conf t
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA3(config-if)#no shut
BOGOTA3(config)#int s0/1/0
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#int g0/0
BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA3(config-if)#no shut

Figura 31. Ping de BOGOTA3 a BOGOTA2 – BOGOTA1



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

5.2.1.1 Parte 1: Configuración del enrutamiento

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

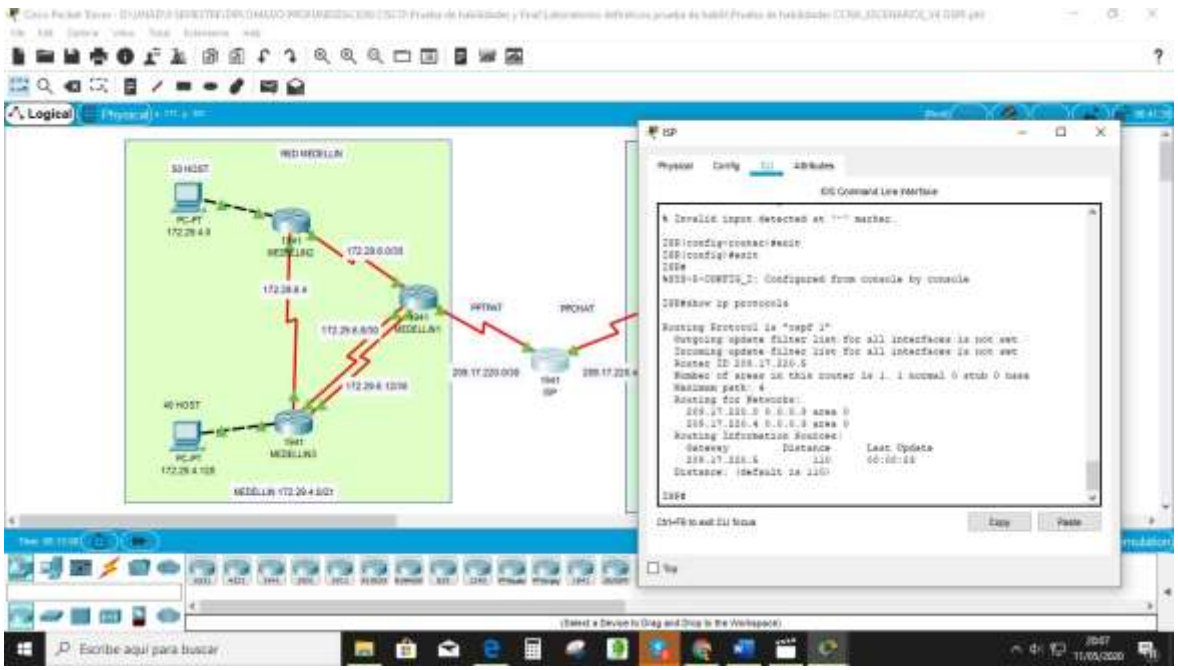
Para iniciar, se configuran las ip de todos los Router después se aplica el protocolo OSPF versión 2 y se aplica la sumarización automática:

RED ISP – ÁREA 0

ROUTER ISP
ISP>show ip route
C 209.17.220.0/30 is directly connected, Serial0/0/0
L 209.17.220.1/32 is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
L 209.17.220.5/32 is directly connected, Serial0/0/1
Configuración
ISP(config)#router ospf 1
ISP(config-router)#router-id 1.1.1.1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
Para verificar la configuración utilizamos los comandos

Show ip protocols

Figura 32. Comando show ip protocols router ISP



RED MEDELLÍN – ÁREA 1

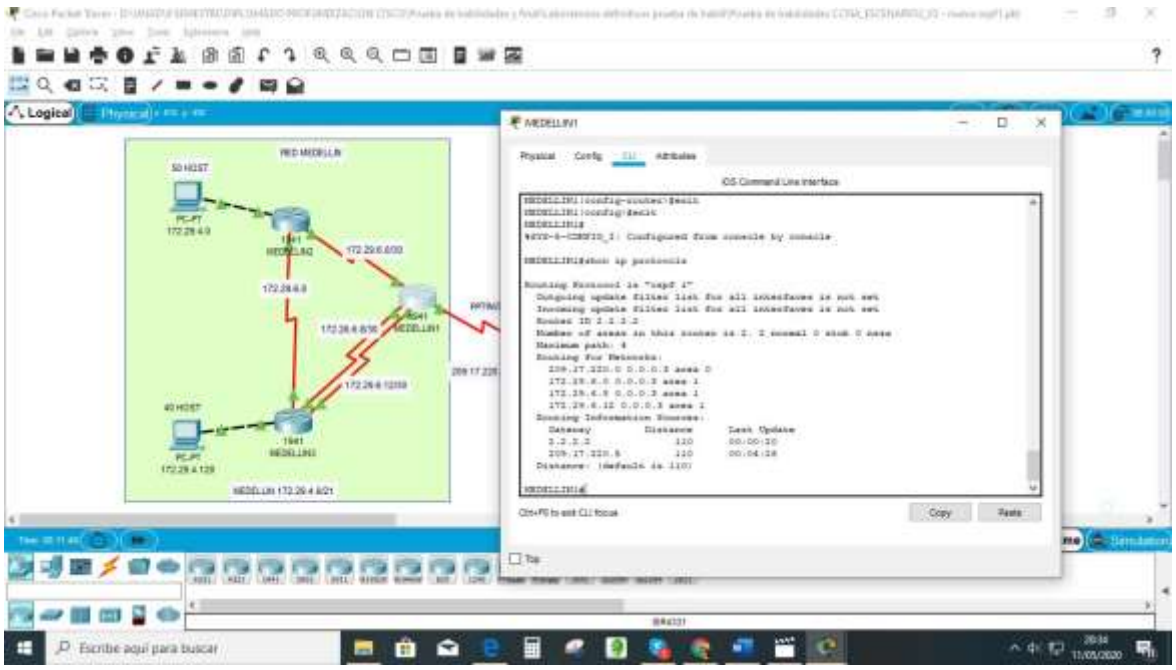
Configuración Router Medellín1

MEDELLIN1#show ip route
C 172.29.6.0/30 is directly connected, Serial0/0/1
L 172.29.6.1/32 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/0
L 172.29.6.9/32 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
L 172.29.6.13/32 is directly connected, Serial0/1/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/0/0
L 209.17.220.2/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 209.17.220.1
Configuramos Medellín1

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 2.2.2.2
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0

MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 1

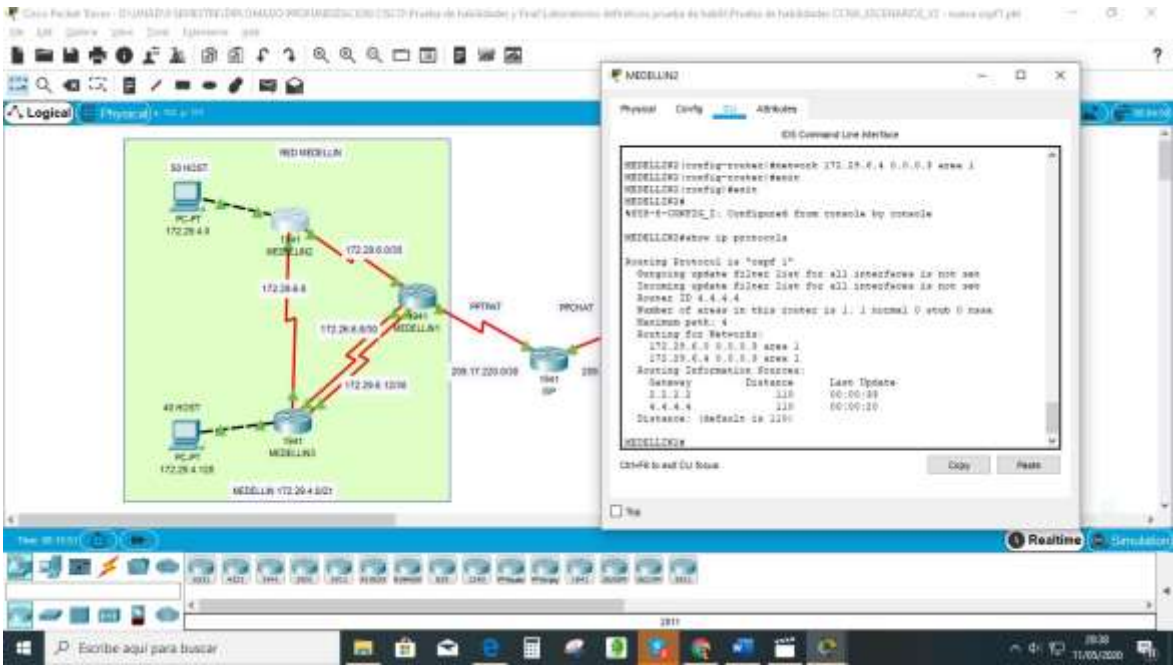
Figura 33. Comando show ip protocols router MEDELLIN1



MEDELLÍN 2
MEDELLIN2#show ip route
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
L 172.29.4.1/32 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
L 172.29.6.2/32 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
L 172.29.6.5/32 is directly connected, Serial0/0/1

Configuración OSPF 1
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 4.4.4.4
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 1

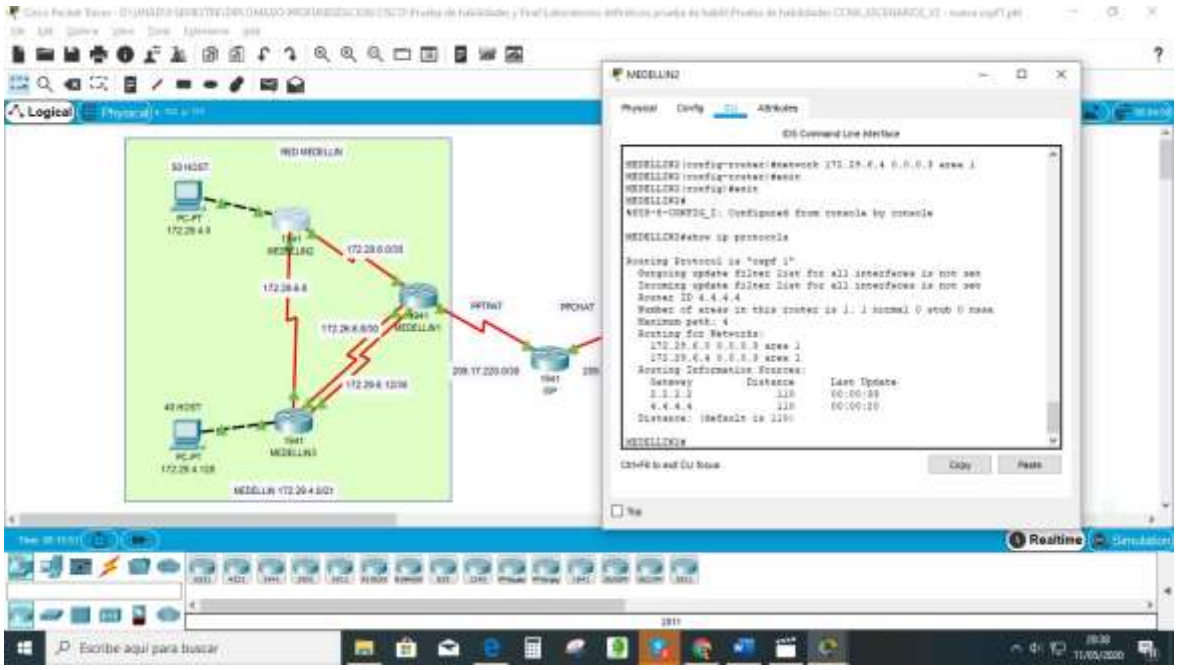
Figura 34. Comando show ip protocols router MEDELLIN2



Router MEDELLÍN 3
Miramos que redes están conectadas
MEDELLIN3#show ip route
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
L 172.29.4.129/32 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/1/0
L 172.29.6.6/32 is directly connected, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/0/0
L 172.29.6.10/32 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/0/1
L 172.29.6.14/32 is directly connected, Serial0/0/1

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 3.3.3.3
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.128 0.0.0.3 area 1
MEDELLIN3(config-router)#exit

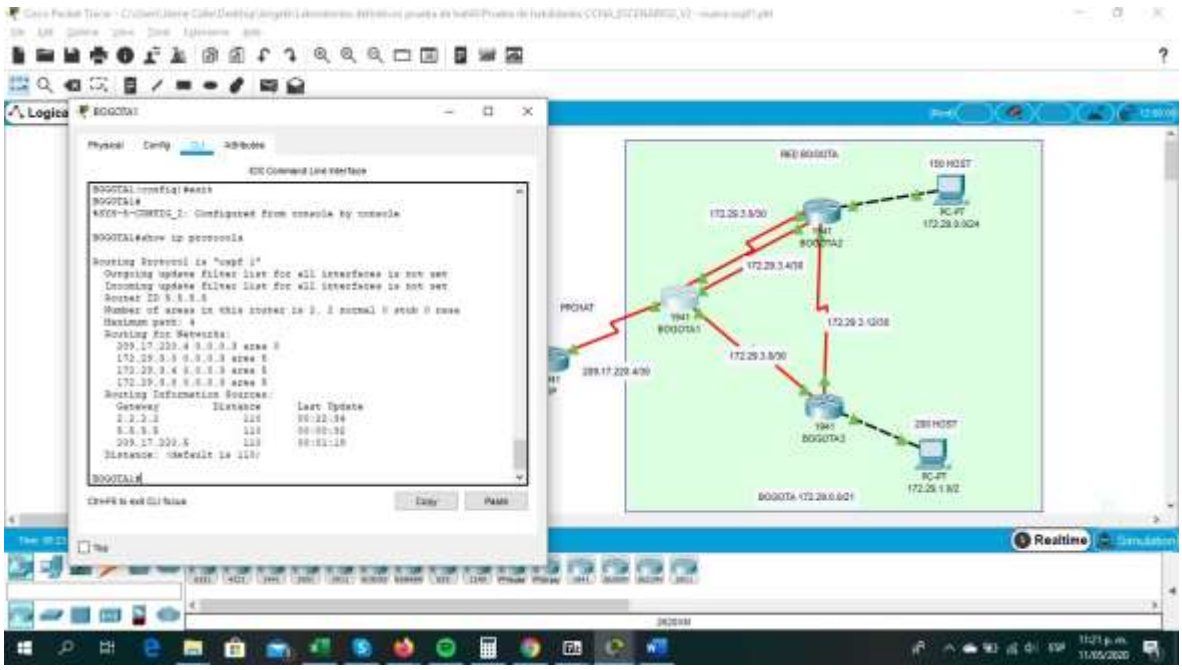
Figura 35. Comando show ip protocols router MEDELLIN3



RED BOGOTÁ – ÁREA 5
Router BOGOTÁ 1
BOGOTA1#show ip route
C 172.29.3.0/30 is directly connected, Serial0/1/0
L 172.29.3.1/32 is directly connected, Serial0/1/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
L 172.29.3.5/32 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
L 172.29.3.9/32 is directly connected, Serial0/0/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.4/30 is directly connected, Serial0/0/0
L 209.17.220.6/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 209.17.220.5

Configuración
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 5.5.5.5
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 5
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 5
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 5

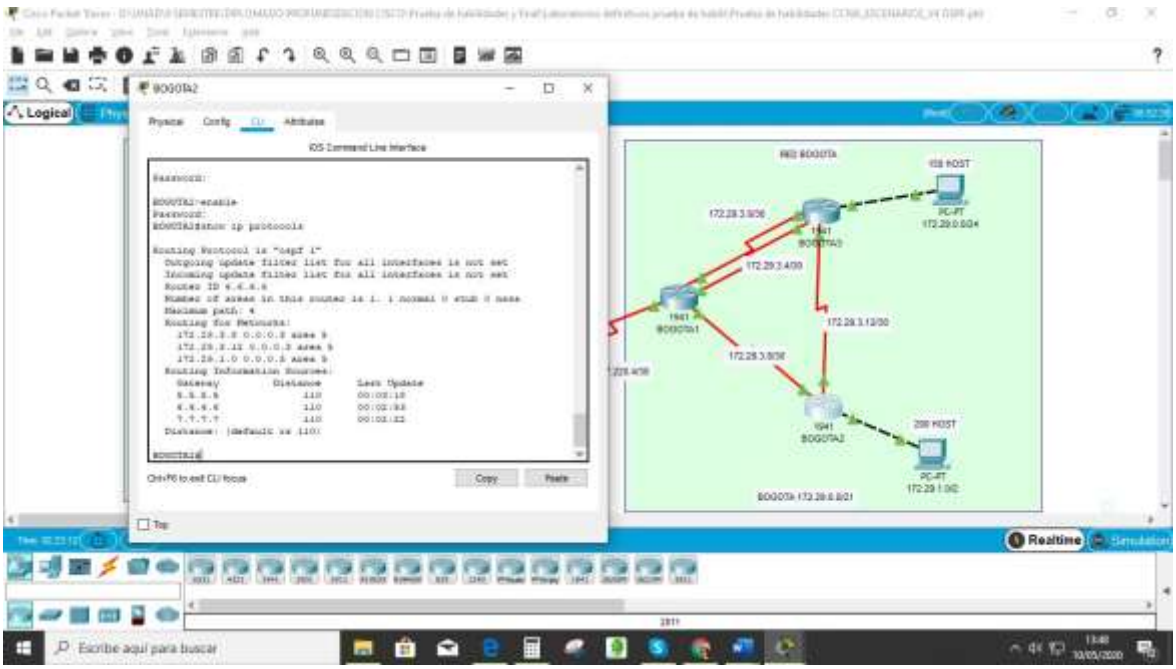
Figura 36. Comando show ip protocols router BOGOTA1



ROUTER BOGOTÁ 2
BOGOTA2#show ip route
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
L 172.29.1.1/32 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
L 172.29.3.10/32 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
L 172.29.3.13/32 is directly connected, Serial0/0/1

Configuración
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 6.6.6.6
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 5
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 5
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 5
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.3 area 5

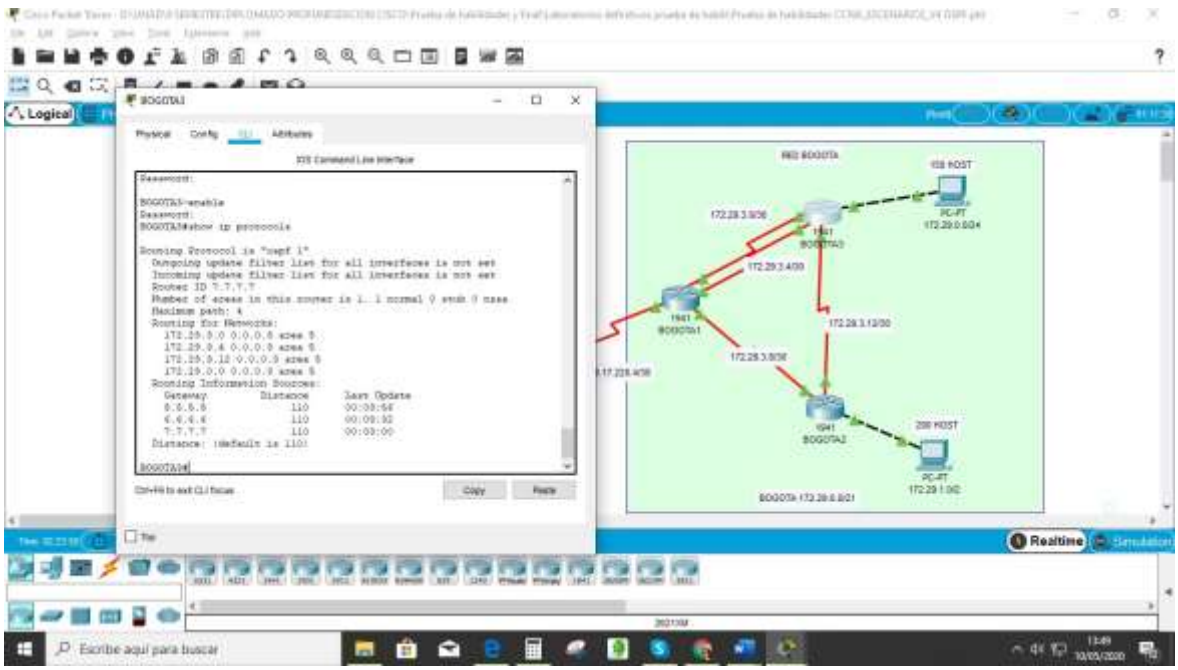
Figura 37. Comando show ip protocols router BOGOTA2



Router BOGOTA 3
BOGOTA3#show ip route
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
L 172.29.0.1/32 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
L 172.29.3.2/32 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
L 172.29.3.6/32 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0
L 172.29.3.14/32 is directly connected, Serial0/1/0

Configuración
BOGOTA3(config)#route ospf 1
BOGOTA3(config-router)#router-id 7.7.7.7
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 5
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 5
BOGOTA3(config-router)#
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 5
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.3 area 5

Figura 38. Comando show ip protocols router BOGOTA3



b. Los routers BOGOTA1 y MEDELLIN1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Configuración ruta por defecto de MEDELLIN1 Y BOGOTA1 hacia ISP

MEDELLÍN 1
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router rip
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#

BOGOTÁ 1
BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#route rip
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)#

Router Medellín 1
MEDELLIN1#conf t

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate

Router Bogotá 1
BOGOTA1#conf t
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate

Figura 39. Comando show ip route - visualizar la distribución en internet router MEDELLIN1

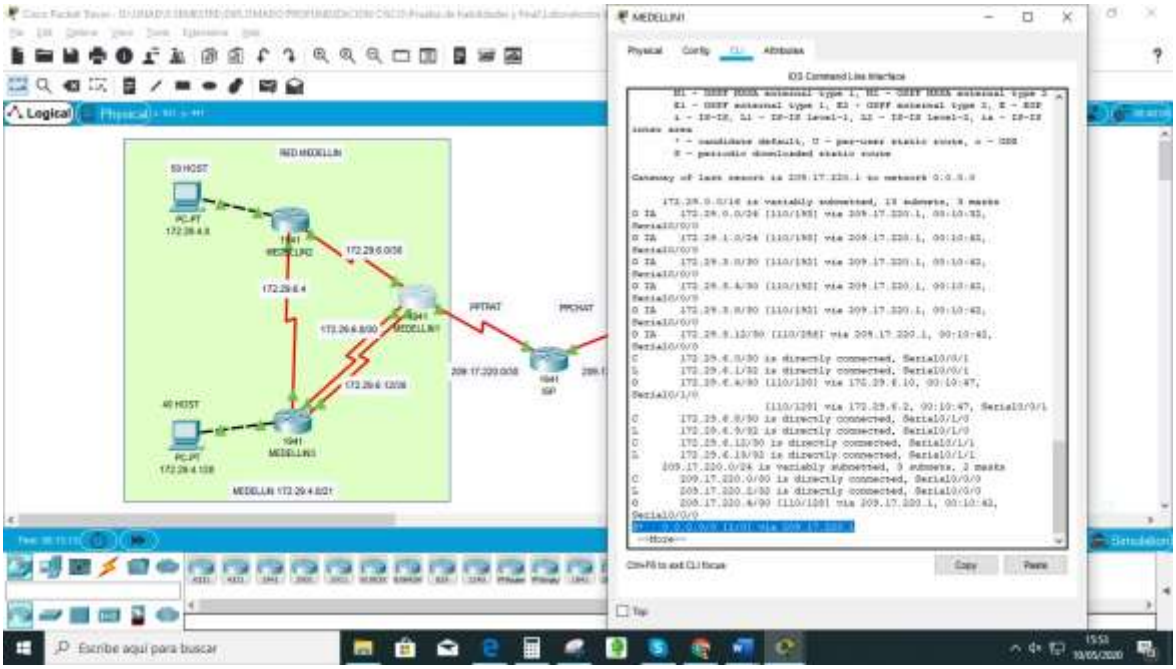
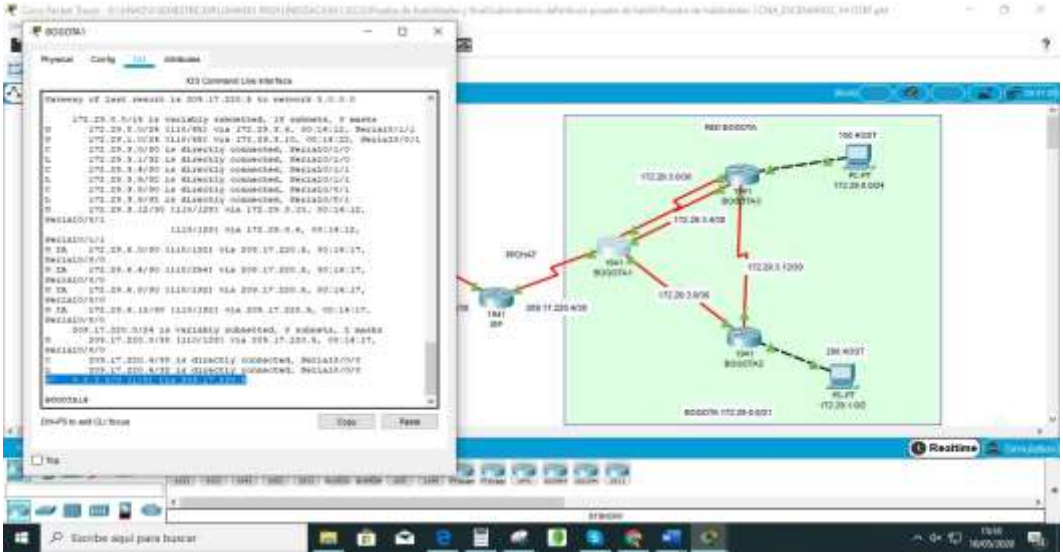


Figura 40. Comando show ip route - visualizar la distribución en internet router BOGOTÁ1



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.
Comandos usados para la ruta estática en ISP:

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

5.2.1.2 Parte 2: Tabla de Enrutamiento

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

Hacemos verificacion por medio de envio de paquetes para verificar redes y rutas

Figura 41. Simulación red Bogotá

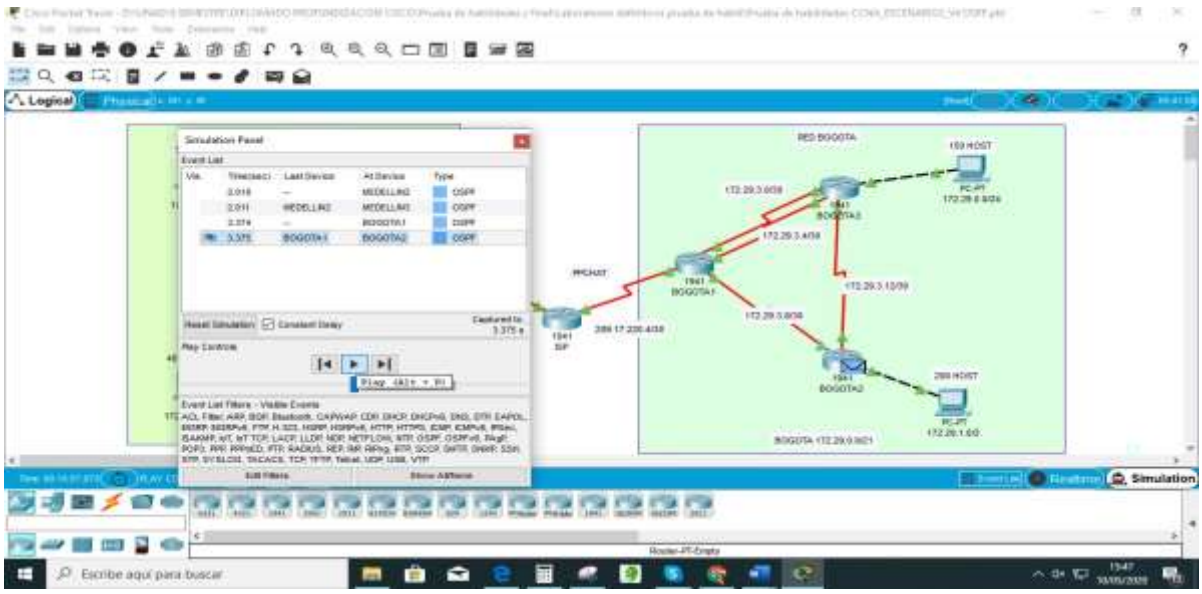


Figura 42. Simulación red Medellín Ruta BOGOTA3 - MEDELLIN2

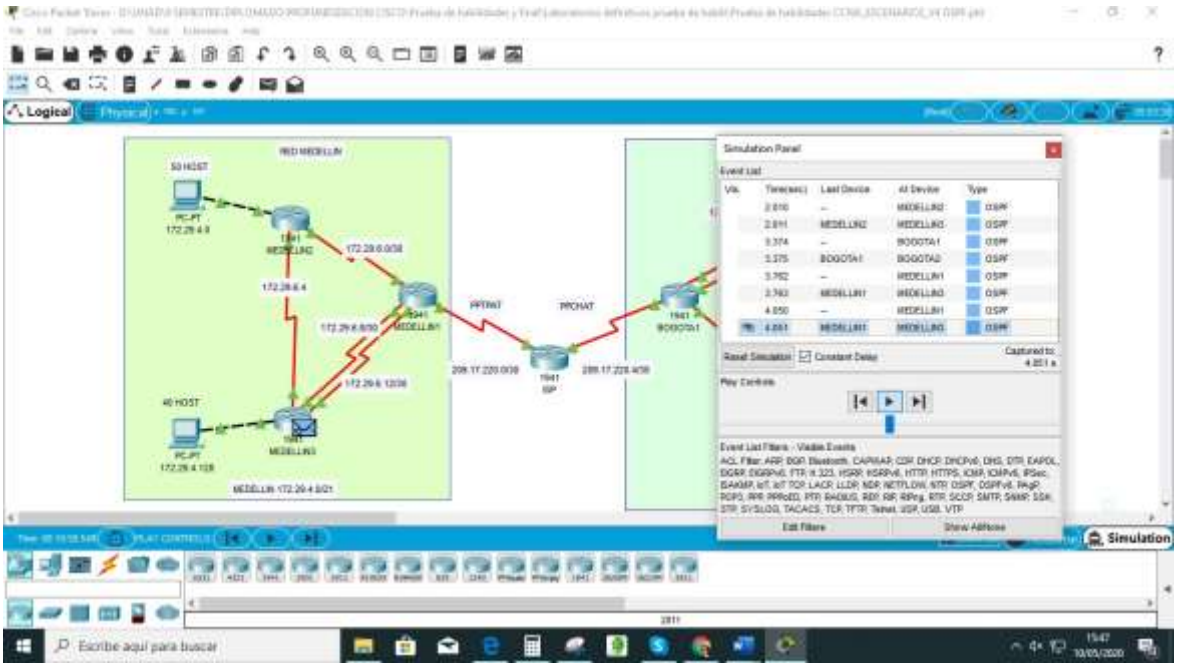
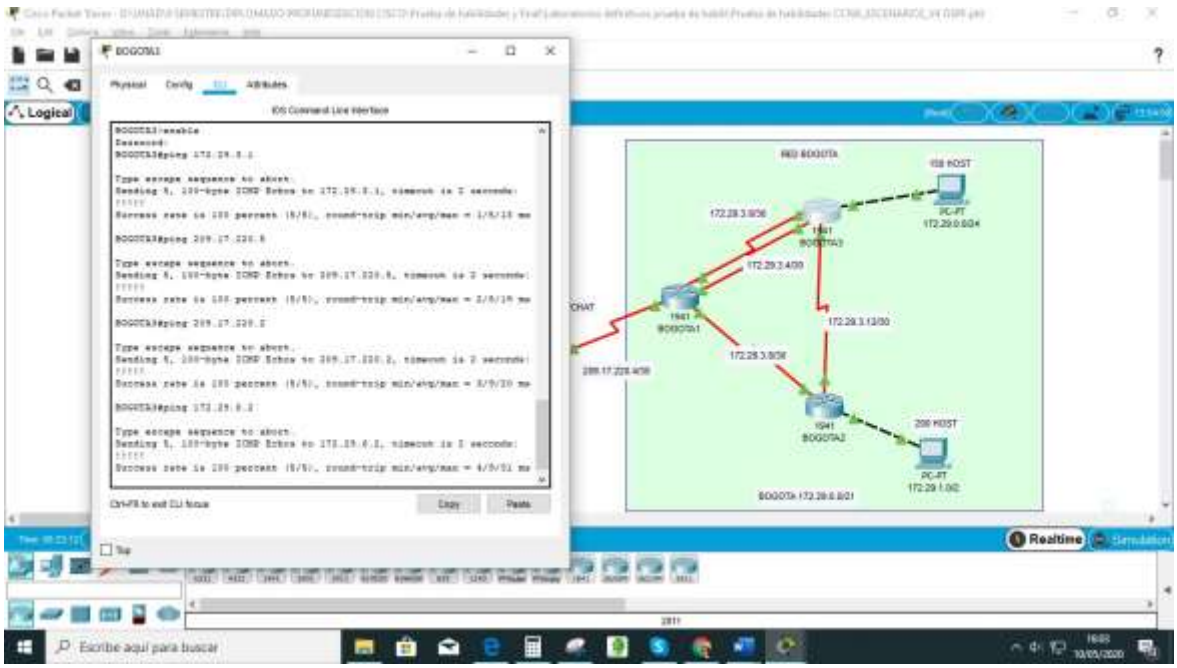
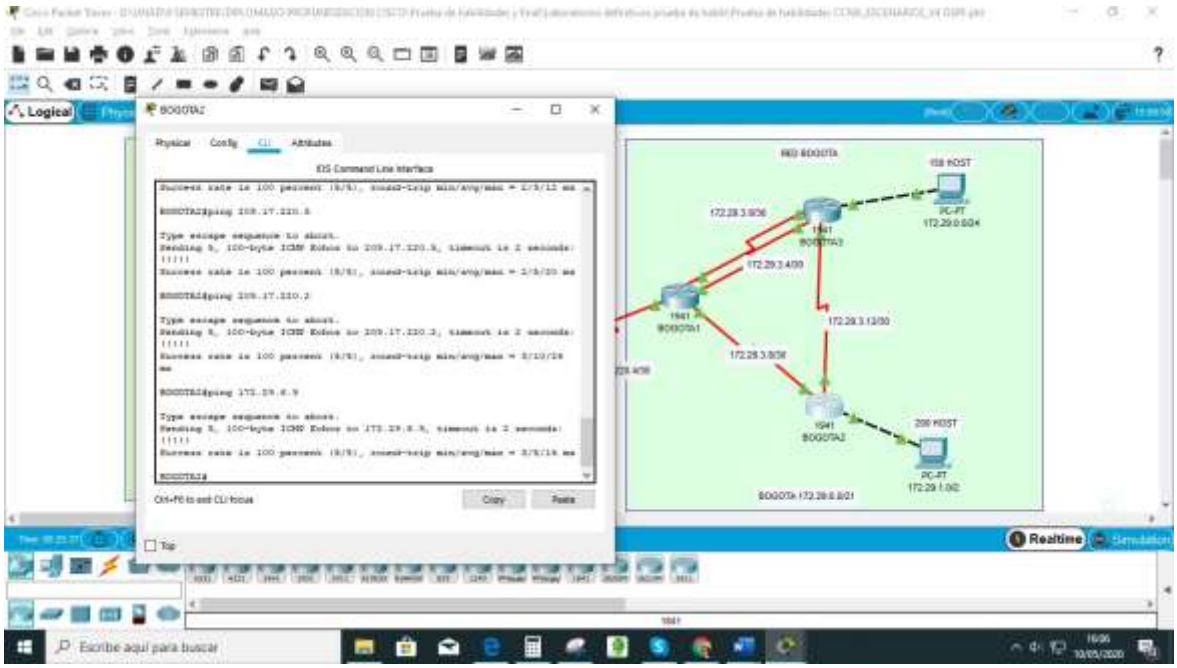


Figura 43. Ping BOGOTA3 - MEDELLIN2



Ruta Bogotá 2 Medellín 3

Figura 44. Ping BOGOTA2 – MEDELLIN3



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

Figura 45. Verificación de balanceo de carga en Bogotá1

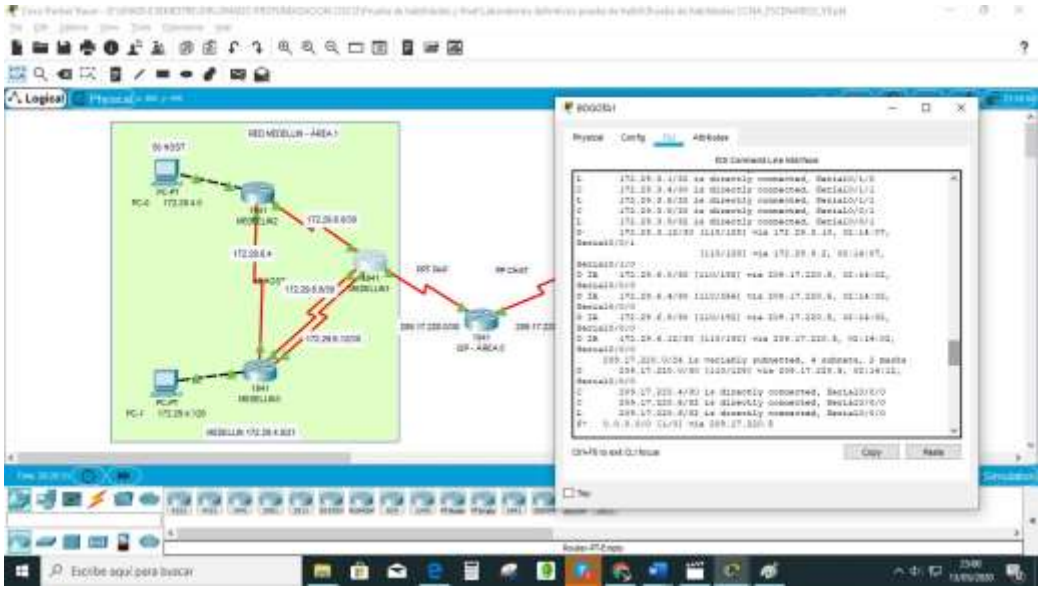
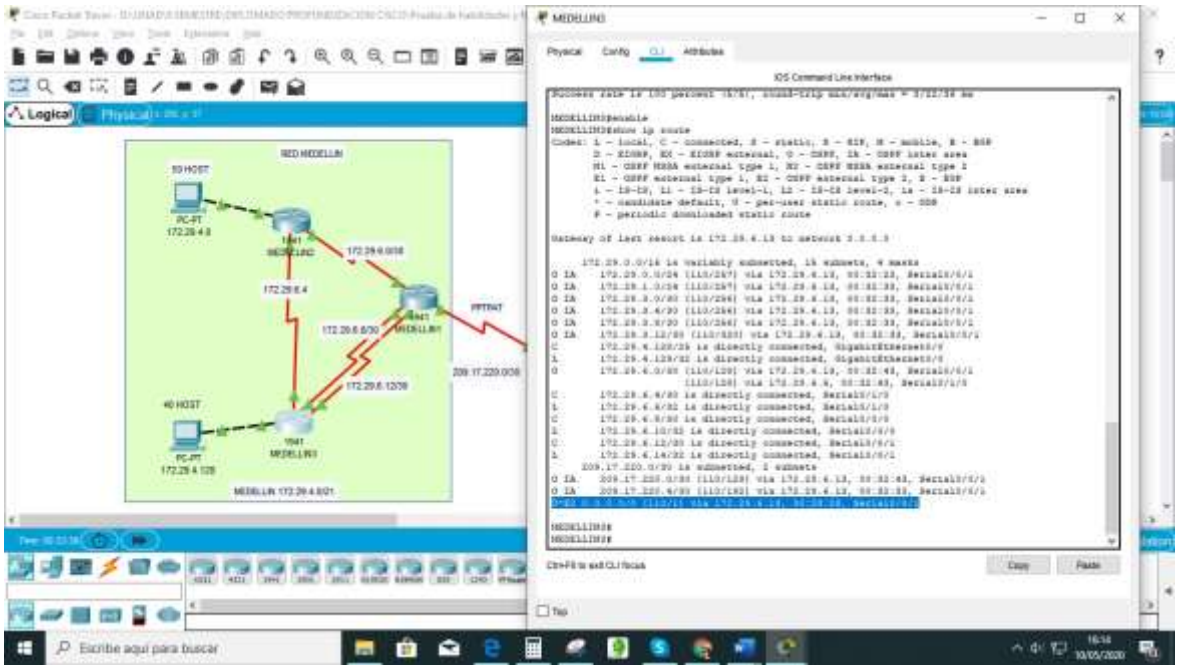
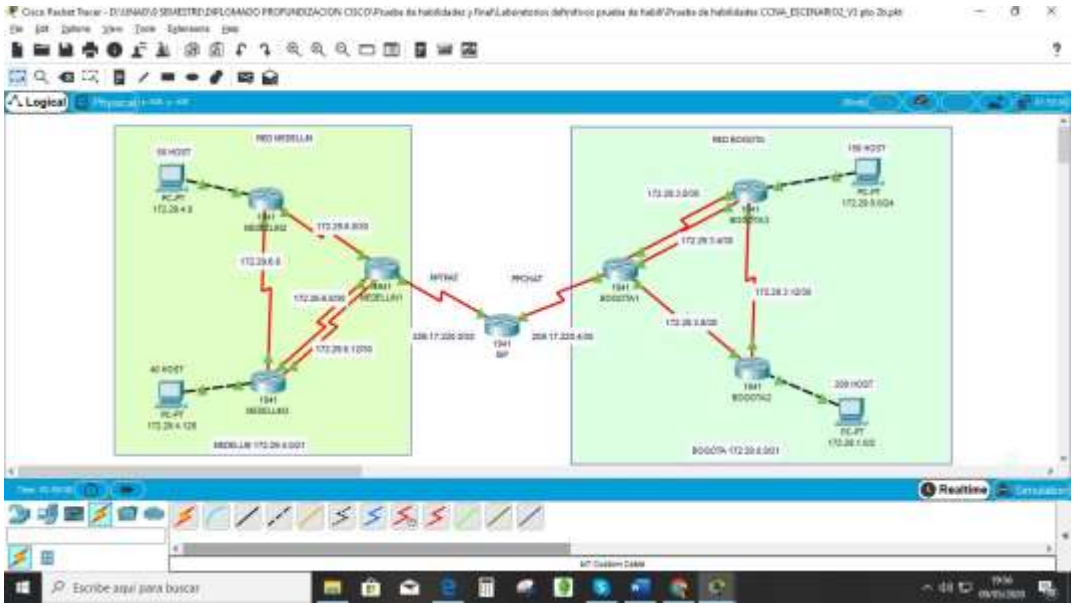


Figura 46. Verificación de balanceo de carga en Medellín1



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

Figura 47. Verificación de similitud en router Bogota1 y Medellin1



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

Figura 48. Redes conectadas directamente y recibidas OSPF

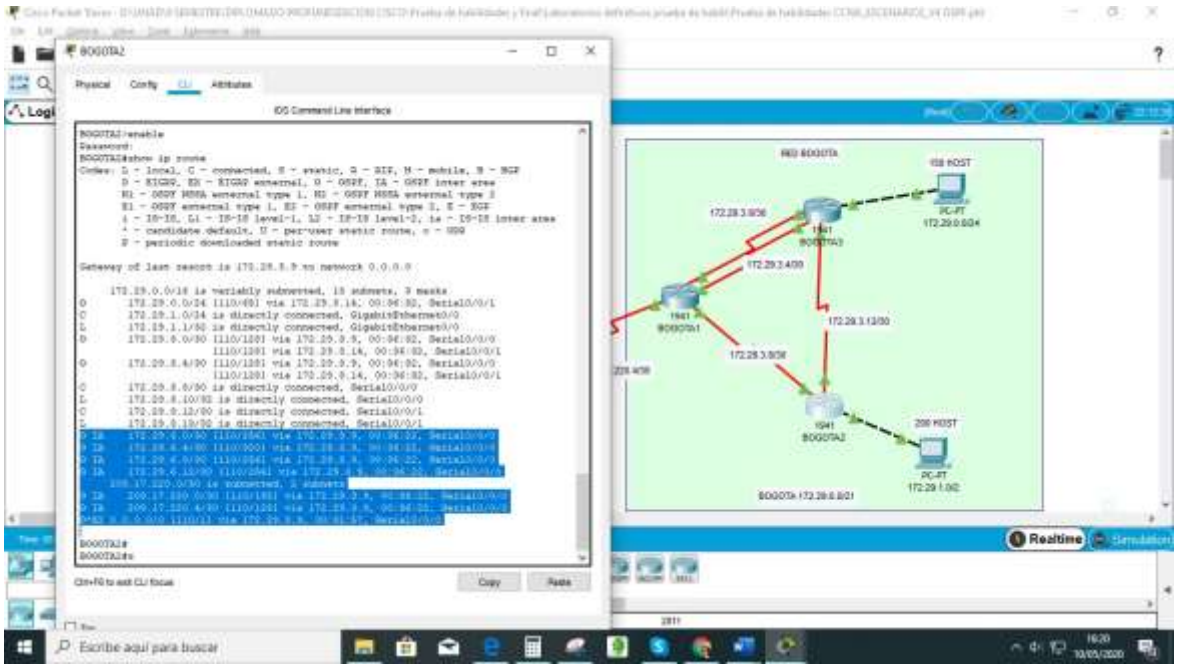
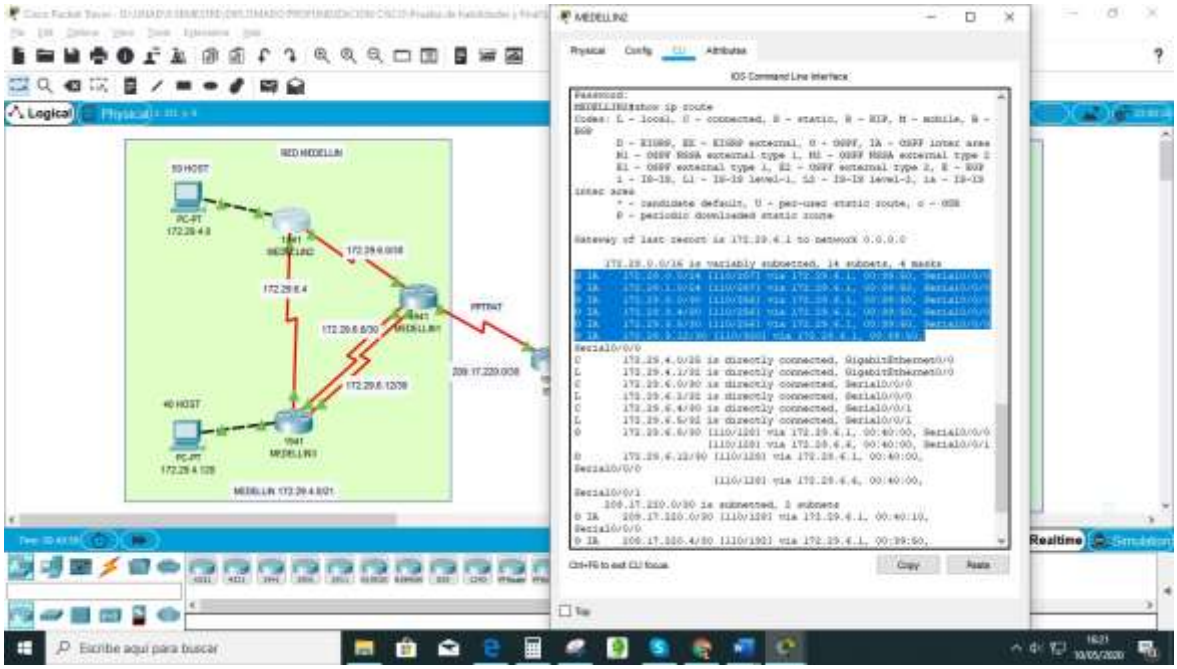


Figura 49. Redes conectadas directamente y recibidas por OSPF en Medellin2.



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

Figura 50. Verificación de cargas y rutas redundantes en Router Bogota3.

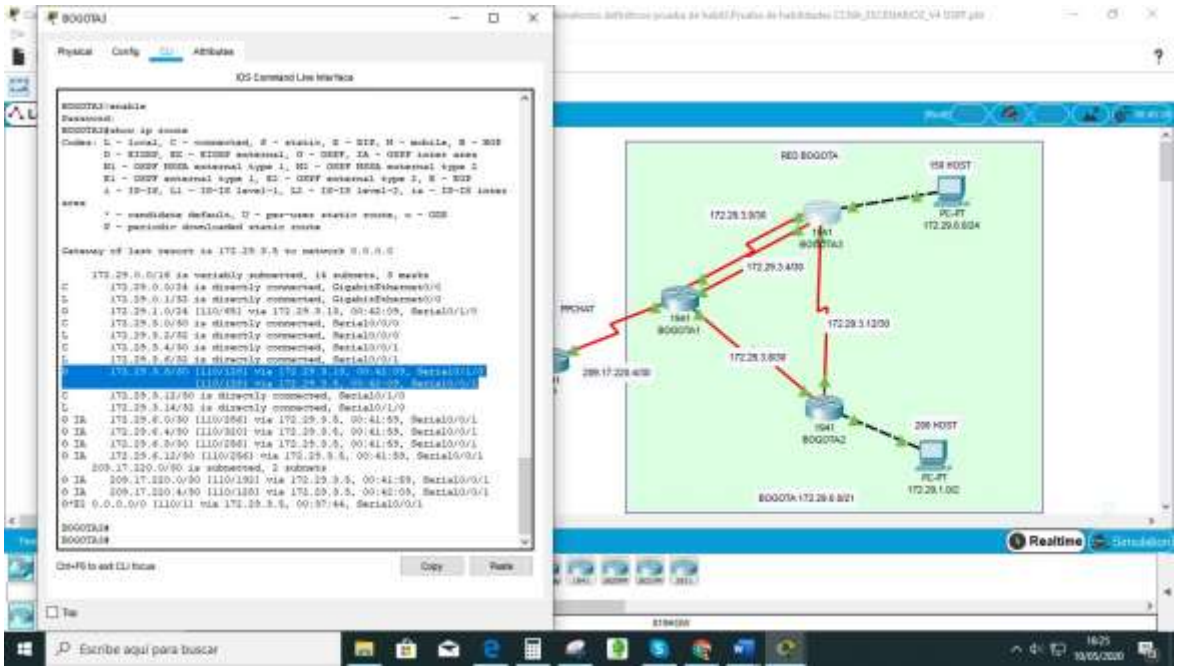
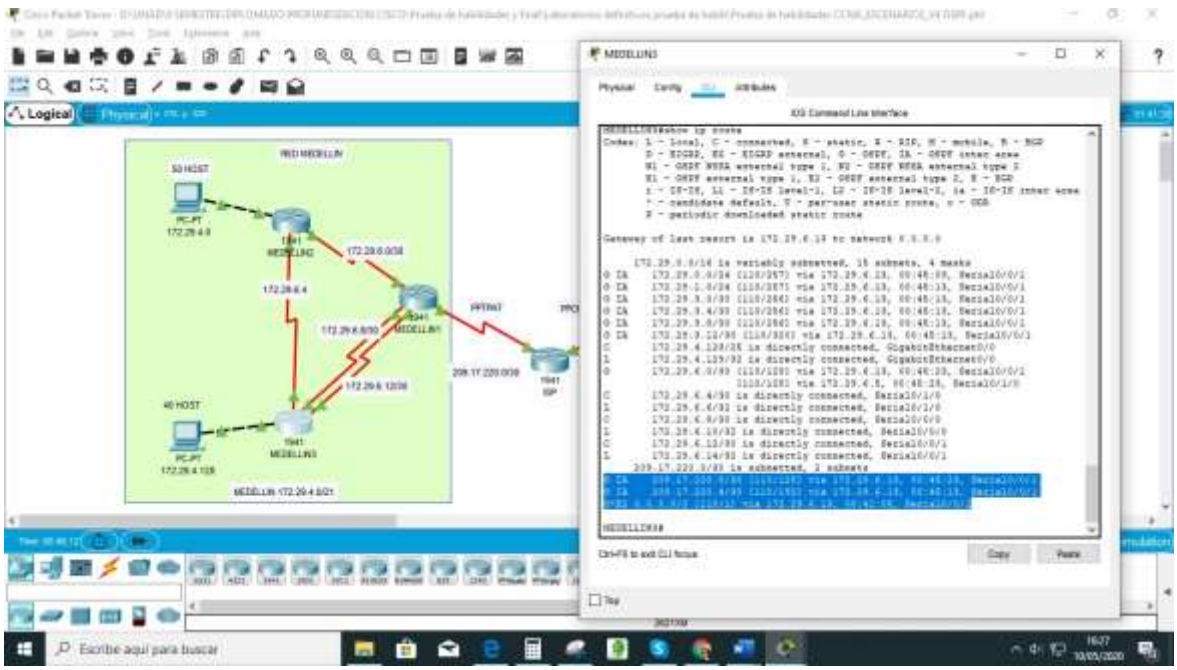
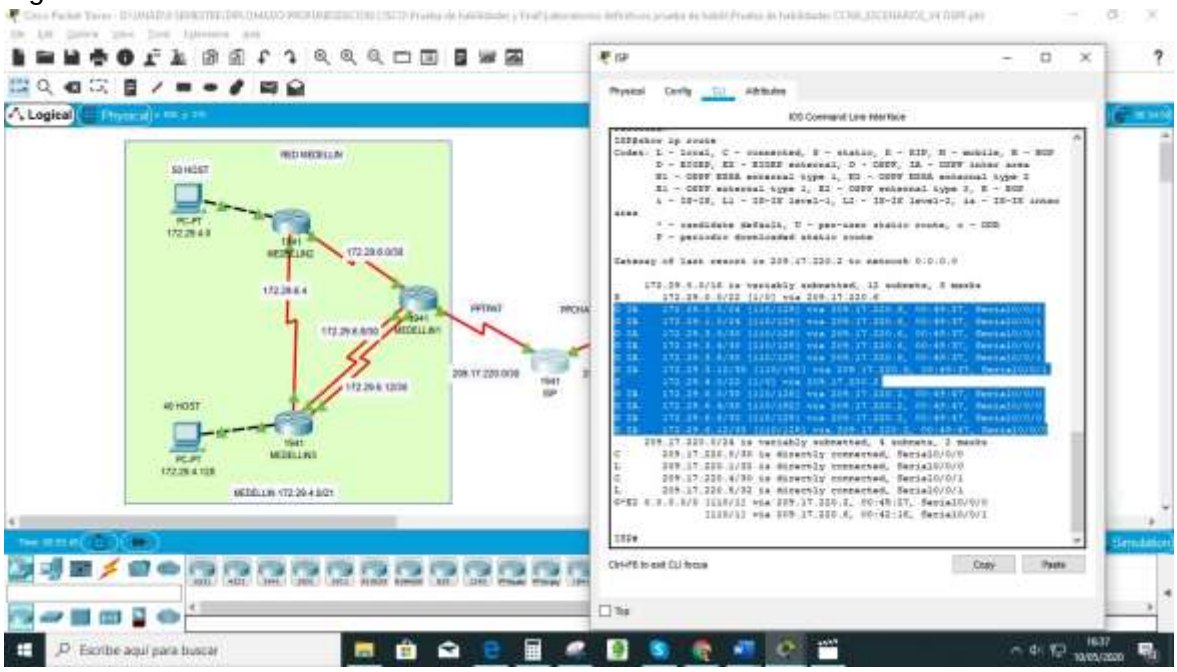


Figura 51. Verificación de cargas y rutas redundantes en Router Medellin3



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

Figura 52. Verificación de rutas estáticas en ISP.



5.2.1.3 Parte 3: Deshabilitar la propagación del protocolo OSPF

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

Tabla 2. Interfaces de cada router que no necesita activación

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

Interfaces de cada router que no necesita activación

BOGOTA1(config-router)#passive-interface s0/0/0

BOGOTA2(config-router)#passive-interface g0/0

BOGOTA3(config-router)#passive-interface g0/0

MEDELLIN1(config-router)#passive-interface s0/0/0

MEDELLIN2(config-router)#passive-interface g0/0

MEDELLIN3(config-router)#passive-interface g0/0

5.2.1.4 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.

Cuando se hizo la configuración del protocolo OSPF en cada router, se tuvieron en cuenta las interfaces pasivas, lo cual se evidencia en los pantallazos de la configuración inicial.

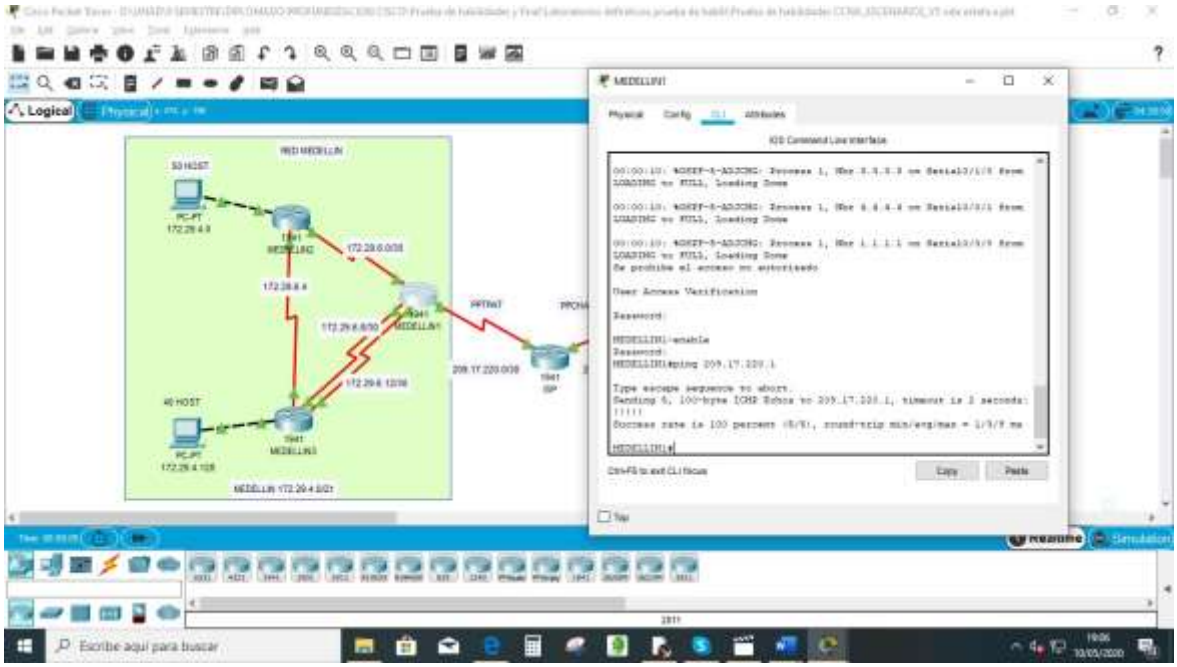
5.2.1.5 Parte 5: Configurar encapsulamiento y autenticación PPP

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.
Damos inicio con la configuración de los router de ISP, MEDELLIN1 Y BOGOTA1 para que usen en ciertas interfaces el método de encapsulación PPP, para posteriormente realizar la autenticación PAP en Medellin1 y CHAP en Bogota1:

Configuración ISP para MEDELLIN1
ISP(config)#username MEDELLIN1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco

Configuración MEDELIN1
MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco

Figura 53. Ping a la red MEDELLIN1 - ISP



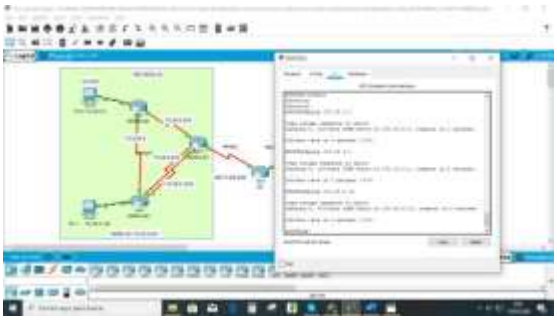
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Configuración ISP para BOGOTÁ1
ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap

Configuración BOGOTA1
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap

Ping ruta BOGOTA1 – ISP

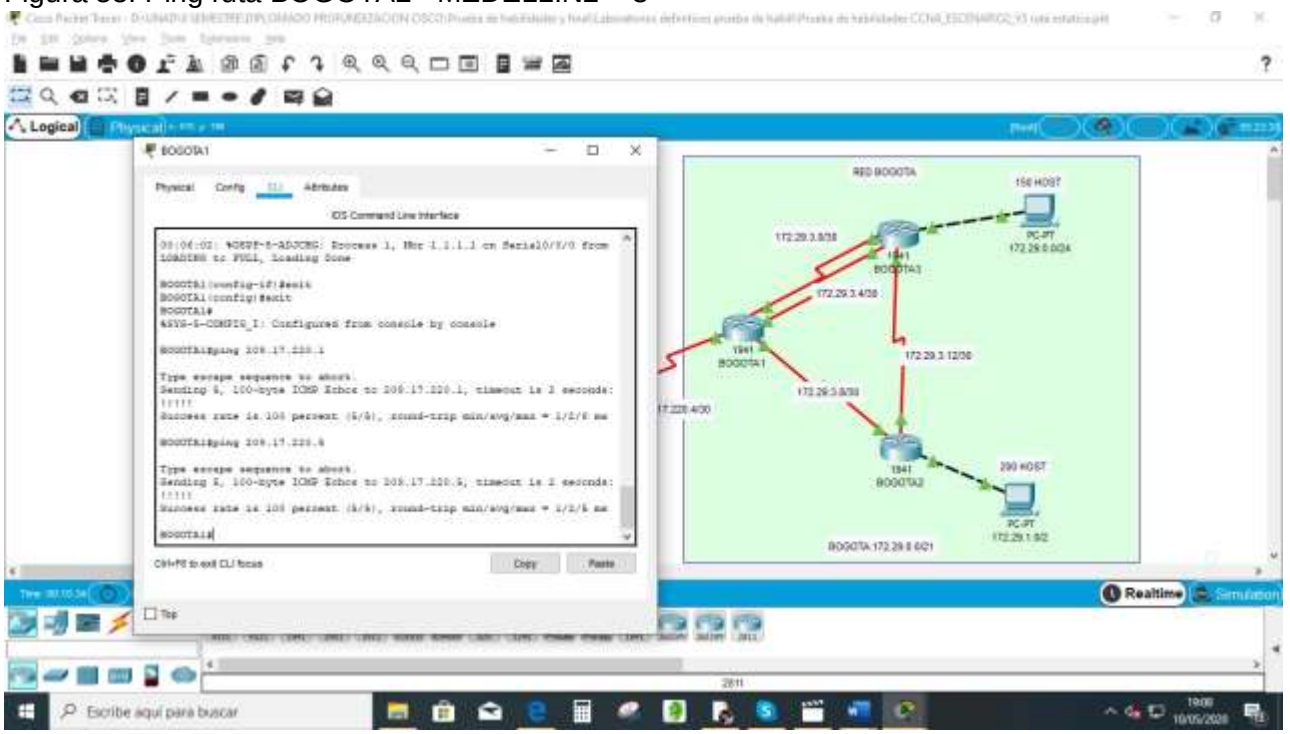
Figura 54. Ping ruta BOGOTA1 – ISP



5.2.1.6 Parte 6: Configuración de PAT

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

Figura 55. Ping ruta BOGOTA2– MEDELLIN2 – 3

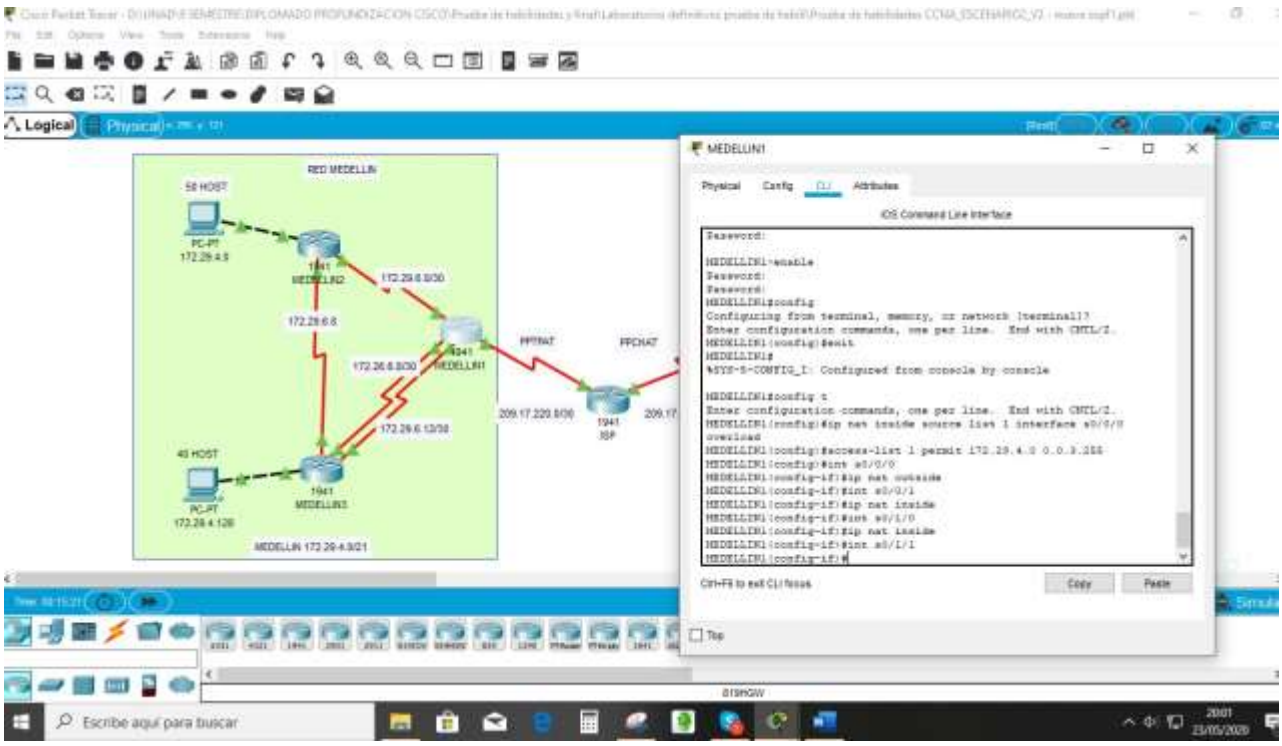


b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz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

Activación de la PAT en Medellin1.

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

Figura 56. Activación de la PAT en MEDELLIN1



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.

Activación de la PAT en Bogota1.

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

Figura 57. Activación de la PAT en BOGOTA1

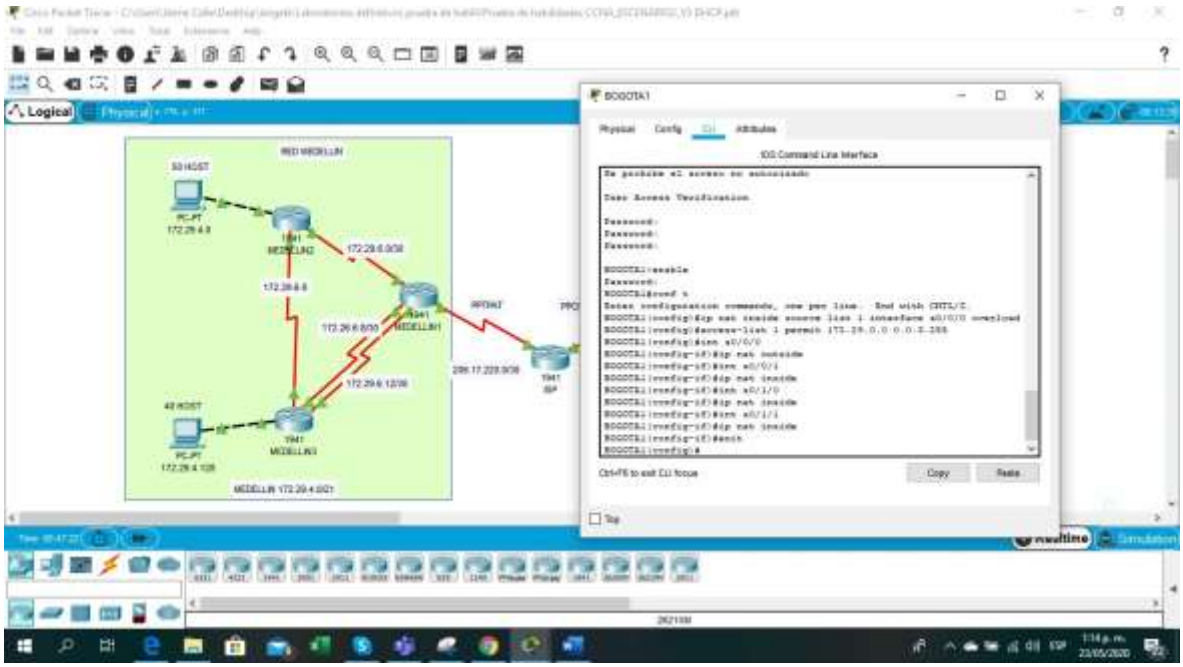
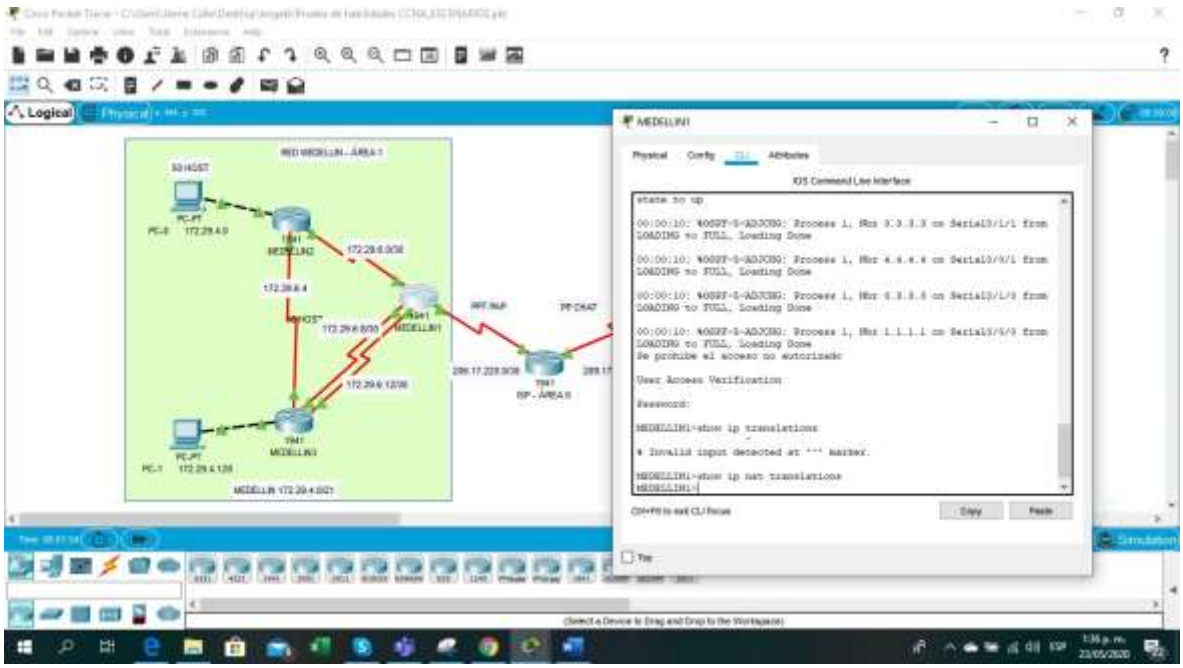


Figura 58. Ejecución del comando show ip nat translations en MEDELLIN1



5.2.1.7 Parte 7: Configuración del servicio DHCP

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

Configuración en el Router MEDELLIN2
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 MEDE2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDE3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit

Figura 59. Protocolo DHCP en MEDELLIN2

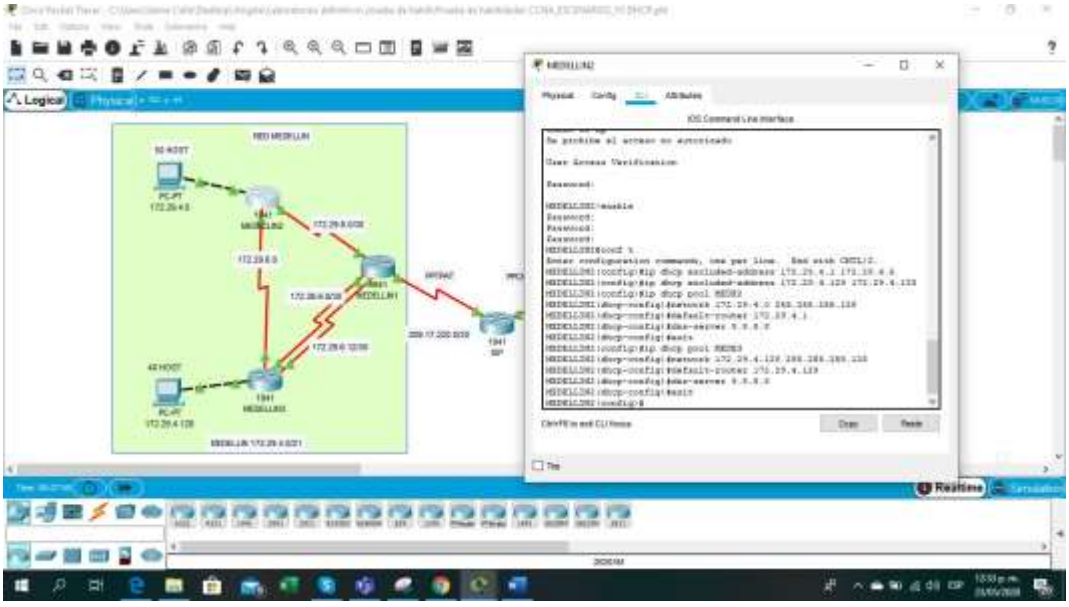
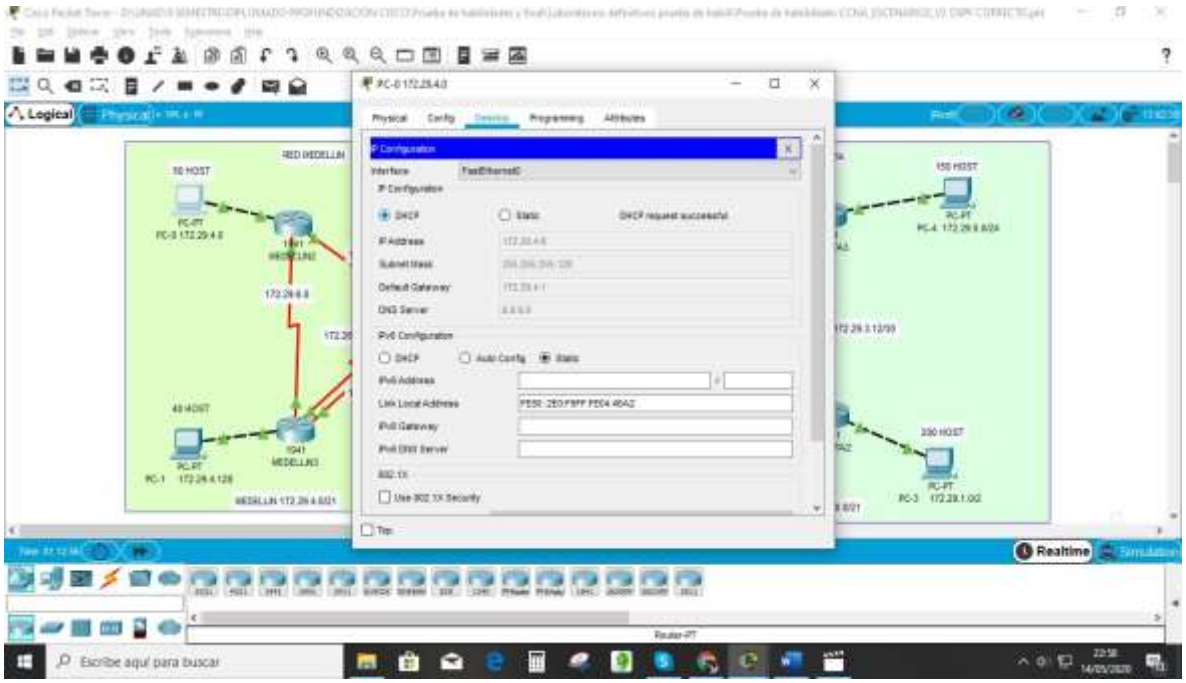


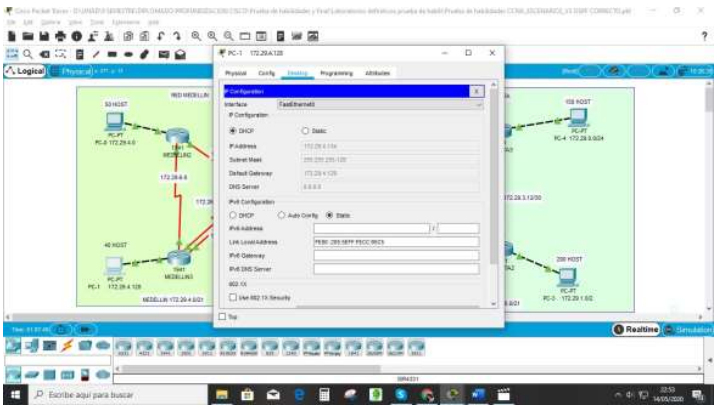
Figura 60. Configuración por DHCP PC0



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

```
MEDELLIN3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#
```

Figura 61. Configuración por DHCP PC1



c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

```
BOGOTA2
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 BOGO2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#ip dhcp pool BOGO3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default router 172.29.0.1
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#
```

Figura 62. Protocolo DHCP en BOGOTA2

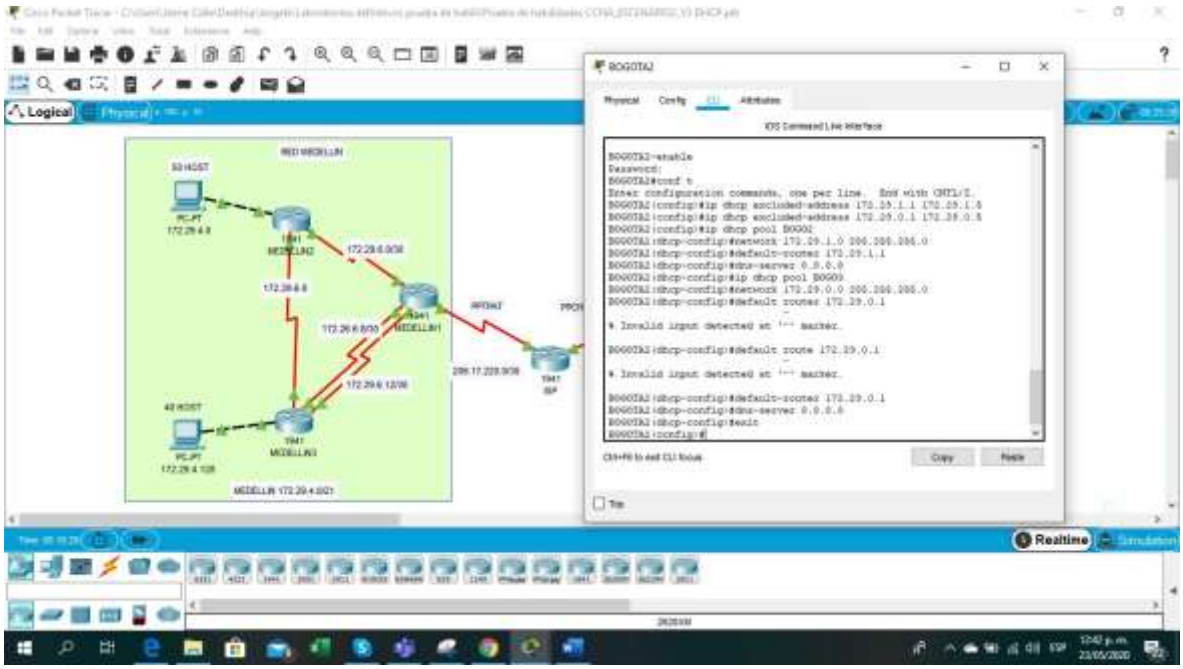


Figura 63. Ping de PC-1 a PC-0

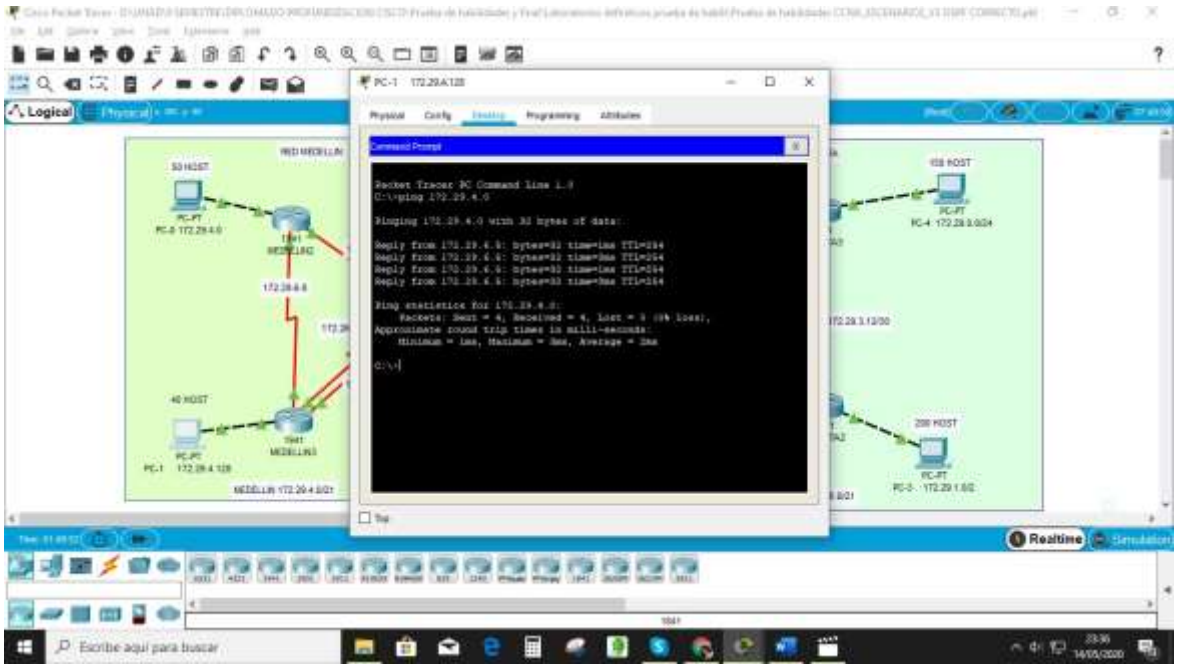


Figura 64. PC-3 por DHCP

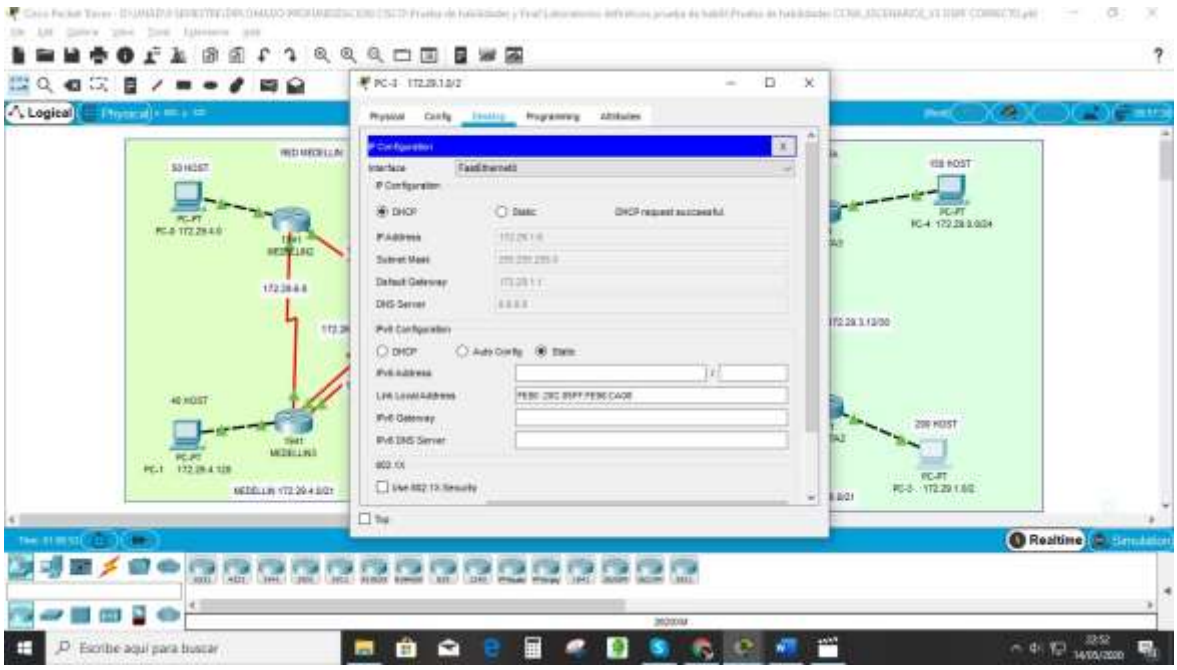


Figura 65. PC-4 por DHCP

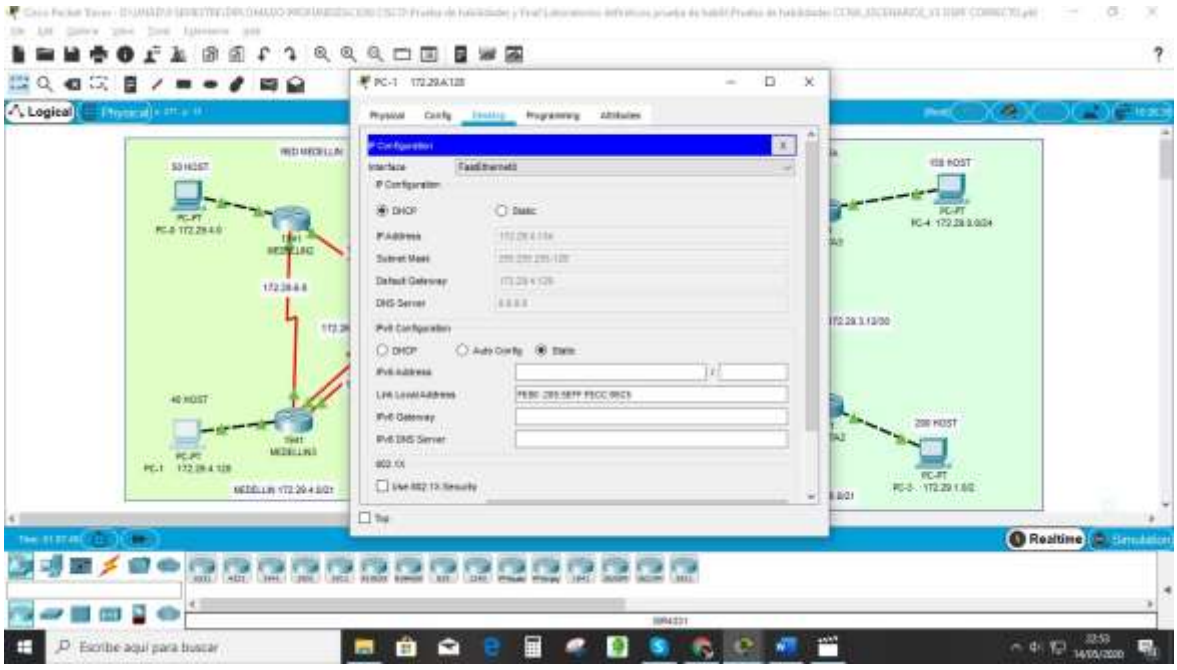


Figura66. Ping de PC-4 a PC-0

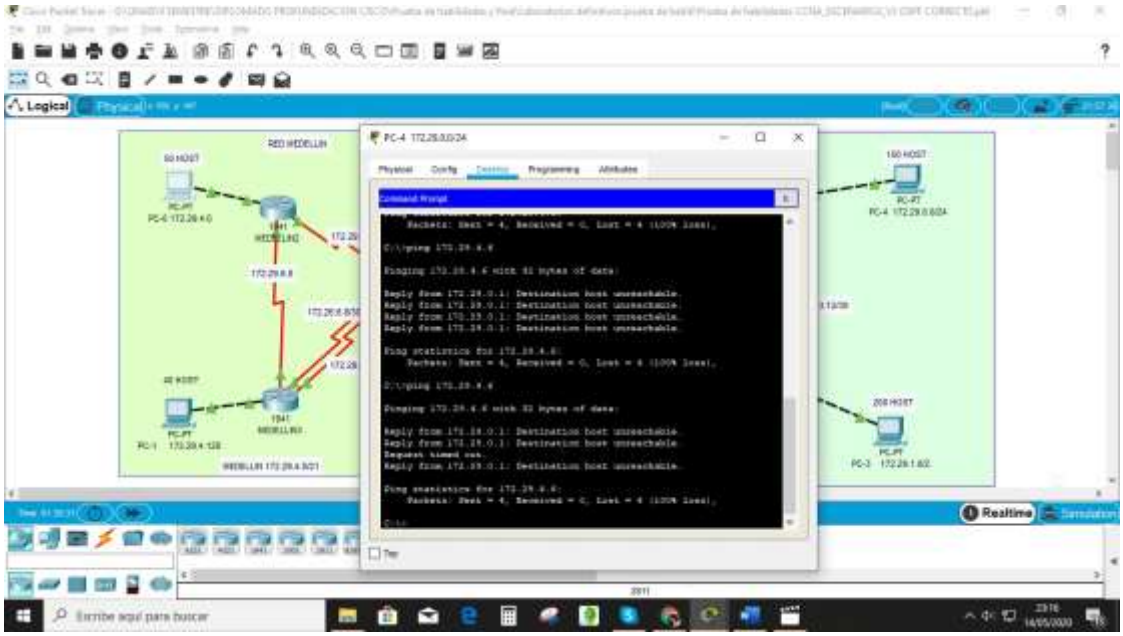
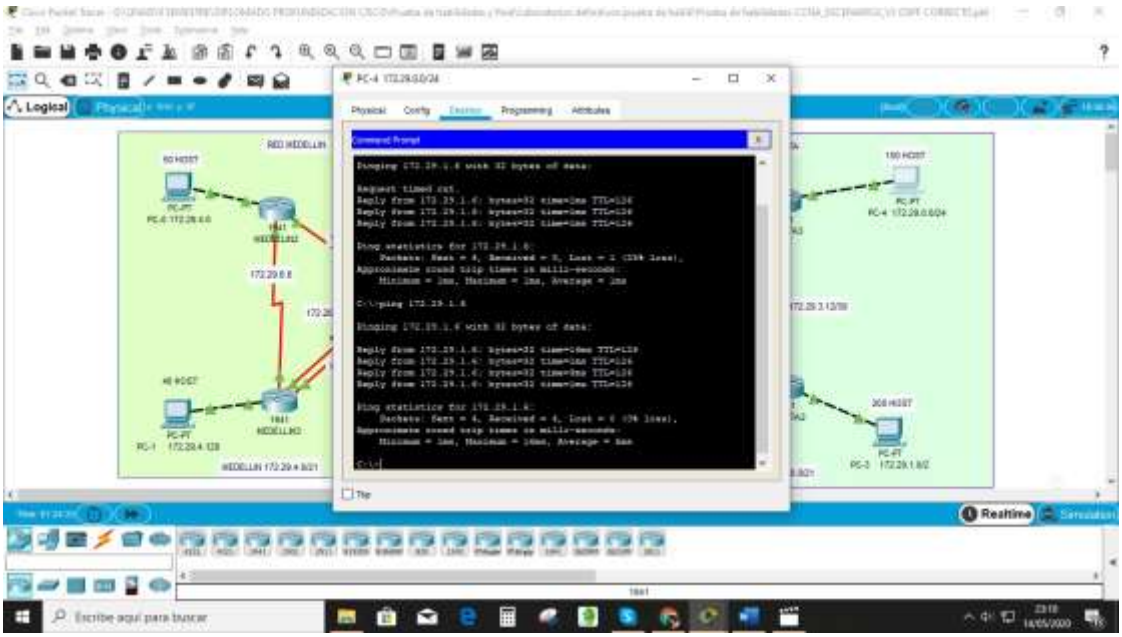


Figura 56. Ping de PC-4 a PC-3



d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

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

CONCLUSIONES

Esta Prueba de Habilidades ha sido muy enriquecedora para mi futuro profesional, ya que, de forma práctica, se aplicaron los conocimientos aprendidos durante este Diplomado de Profundización en CISCO y es la finalización de un proceso académico enfocado a la Ingeniería de Telecomunicaciones.

Desde el inicio es fundamental armar la red de forma correcta y su configuración puesto que ello permitirá que se dé una buena conectividad.

Los dispositivos utilizados, requieren una configuración básica de seguridad en dispositivos de comunicación, además de una aplicación de routing, Vlans, protocolo RIP, el servicio de DHCP, protocolo de enrutamiento OSPF, listas de acceso, NAT, configuración de encapsulamiento y autenticación PPP.

En cada configuración se evidencia su funcionamiento y estructura de la red mediante comandos como: ping, show ip route, show ip protocols, entre otros.

Las listas de control de acceso juegan un rol importante como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema. También permiten filtrar el tráfico de la red, y los tipos de ACL, así como la configuración en los dispositivos Cisco.

Aplicando el protocolo DHCP se puede administrar de forma sencilla la red, evitando posibles conflictos y malas configuraciones en los Hosts; NAT se usa para enmascarar la red interna y poder salir a través de una única dirección pública a internet, obteniendo con esto grandes ahorros en direcciones IPv4.

Los protocolos OSPF y RIP se asemejan, la diferencia está en que cada paquete enviado se hace a través del camino más corto, ya que en su configuración se utiliza la direcciones de los routers cercanos, de esta forma se conocen el número de saltos.

LISTA DE REFERENCIAS

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

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

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1