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

SINDY ALEJANDRA HERNÁNDEZ RAMOS

INFORME PRUEBA DE HABILIDADES PRACTICAS CISCO CCNA
PARA OPTAR AL TÍTULO EN INGENIERÍA DE SISTEMAS

HECTOR JULIAN PARRA
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
BOGOTÁ, COLOMBIA
MAYO, 2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 15 de mayo, 2020

Dedicado a mis padres Cecilia Ramos, Alberto Hernández, a mi hermana Ledis Carolina; quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo, responsabilidad y valentía, de no temer de las adversidades porque Dios está conmigo siempre.

AGRADECIMIENTOS

Agradezco a mis hermanos Sandra Hernández y Luis Hernández por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento al extender su mano en situaciones difíciles.

A mi abuela Isabel Ramos que con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Finalmente, agradezco a la Universidad UNAD por las enseñanzas y los conocimientos adquiridos y a Dios por permitirme llegar a esta etapa tan importante de mi vida.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

Vivimos en un mundo en constante desarrollo tecnológico encontramos redes complejas como redes de alta capacidad, con la llegada de (www) World Wide Web; esto hace a su vez que los dispositivos de redes como los Switch, Routers, Satélites, computadores, celulares, entre otros; evolucionen en sus funcionalidades, capacidad, conectividad y en su ancho de banda, ahora encontramos las redes (Wifi) inalámbricas, que se han vuelto muy popular en pleno siglo XXI; ya que el número de usuarios de Internet a nivel mundial creció de una manera bastante rápida por lo que las empresas más grandes que manejan las redes vieron la necesidad de crear el internet de las cosas, así como el direccionamiento que se manejaba de IPv4 a IPv6.

Entre más crece la red mayor será la inseguridad y vulnerabilidad ante los ataques informáticos; por lo que los dispositivos cambian sus estrategias en seguridad, por esta razón se crean nuevos software de IOS que se adaptan a las nuevas tecnologías para mantener la seguridad de sus clientes al conectarse a Internet como en seguridad de cifrado en los paquetes que viajan a través de la red, conexiones remotas con claves cifradas, NAT, PAT, DHCP que es una manera que manejan las compañías de redes para mantener la escalabilidad dentro de la red LAN y WAN, así como se implementa PPP, PAP, CHAP, ACL, NTP, VLANs para separar dependencias, seguridad de puertos, RIPv2; además encontramos la Inteligencia en el flujo de datos y redes automatizadas.

Los protocolos como OSPF, permiten mejorar el ancho de banda, el costo, por donde se va a transmitir el mensaje, así como proporcionar sus rutas por medio de un algoritmo que separa las redes según su área configurada, dando como prioridad la ruta más rápida y menos congestionada para que el Router envié el paquete hasta llegar a su destino final.

Con la evolución de la tecnología, encontramos la fibra óptica que es el único medio hasta el momento, el más rápido en envió de datos; pero las compañías siempre estarán en constante desarrollo y pronto nacerán nuevas tecnologías para adaptarse a las necesidades de los usuarios y de seguridad a nivel mundial; ya que el mundo de las redes es el futuro.

PALABRAS CLAVE: Redes, Cisco, CCNA.

ABSTRACT

We live in a world in constant technological development, we find complex networks such as high capacity networks, with the arrival of (www) World Wide Web; This in turn makes network devices such as switches, routers, satellites, computers, cell phones, among others; evolve in their functionalities, capacity, connectivity and bandwidth, now we find wireless (Wi-Fi) networks, which have become very popular in the 21st century; Since the number of Internet users worldwide grew quite quickly, the largest companies that manage networks saw the need to create the Internet of Things, as well as the addressing that was handled from IPv4 to IPv6. .

The more the network grows, the greater the insecurity and vulnerability to computer attacks; As devices change their security strategies, for this reason new IOS software is created that adapt to new technologies to maintain the security of their clients when connecting to the Internet, as well as encryption security in the packets that travel through network, remote connections with encrypted keys, NAT, PAT, DHCP which is a way that network companies manage to maintain scalability within the network LAN and WAN, as well as PPP, PAP, CHAP, ACL, NTP is implemented, VLANs to separate dependencies, port security, RIPv2; In addition we find Intelligence in the data flow and automated networks.

Protocols such as OSPF, allow to improve bandwidth, cost, where the message will be transmitted, as well as provide their routes through an algorithm that separates networks according to their configured area, giving priority to the fastest route and less congested for the Router to send the packet until it reaches its final destination.

With the evolution of technology, we find fiber optics which is the only medium so far, the fastest in sending data; but companies will always be in constant development and new technologies will soon be born to adapt to the needs of users and security worldwide; since the world of networks is the future.

KEY WORDS: *Networks, Cisco, CCNA.*

1. INTRODUCCIÓN

En el presente informe se realizará dos tipos de escenarios, el primero aborda los temas de seguridad de redes implementados en VLANs, ACL, DHCP, NAT, NTP, RIPv2; para ser implementado en direcciones de IPv4 e IPv6, calculando rutas resumidas para su direccionamiento.

En el segundo escenario se abordarán los temas sobre el protocolo de enrutamiento de OSPF, para configurar una red de Medellín y Bogotá que conecta con ISP; ademas se implementará otras configuraciones de requerimiento como DHCP por Router, NAT, PAT, PPP, PAP y CHAP; donde se calculará el direccionamiento de cada red, con sus repectivas rutas resumidas y de wildcard.

El tema principal es configurar los dispositivos como Routers, Switch y computadores de acuerdo con los requerimientos asignados para cada escenario, asumiendo el rol de administrador de red se cumplirá los objetivos del presente informe y se abordarán los temas de lo aprendido a lo largo del curso de CISCO CCNA, para aplicarlo a los escenarios y así llegar a su solución.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar los diferentes escenarios de redes de datos, aplicando los conocimientos adquiridos durante el curso de Cisco CCNA.

2.2 OBJETIVOS ESPECÍFICOS

- Analizar los escenarios propuestos para así llegar a su solución.
- Demostrar las habilidades en la configuración de dispositivos de red implementadas en Cisco Packet Tracer de acuerdo con las topologías.

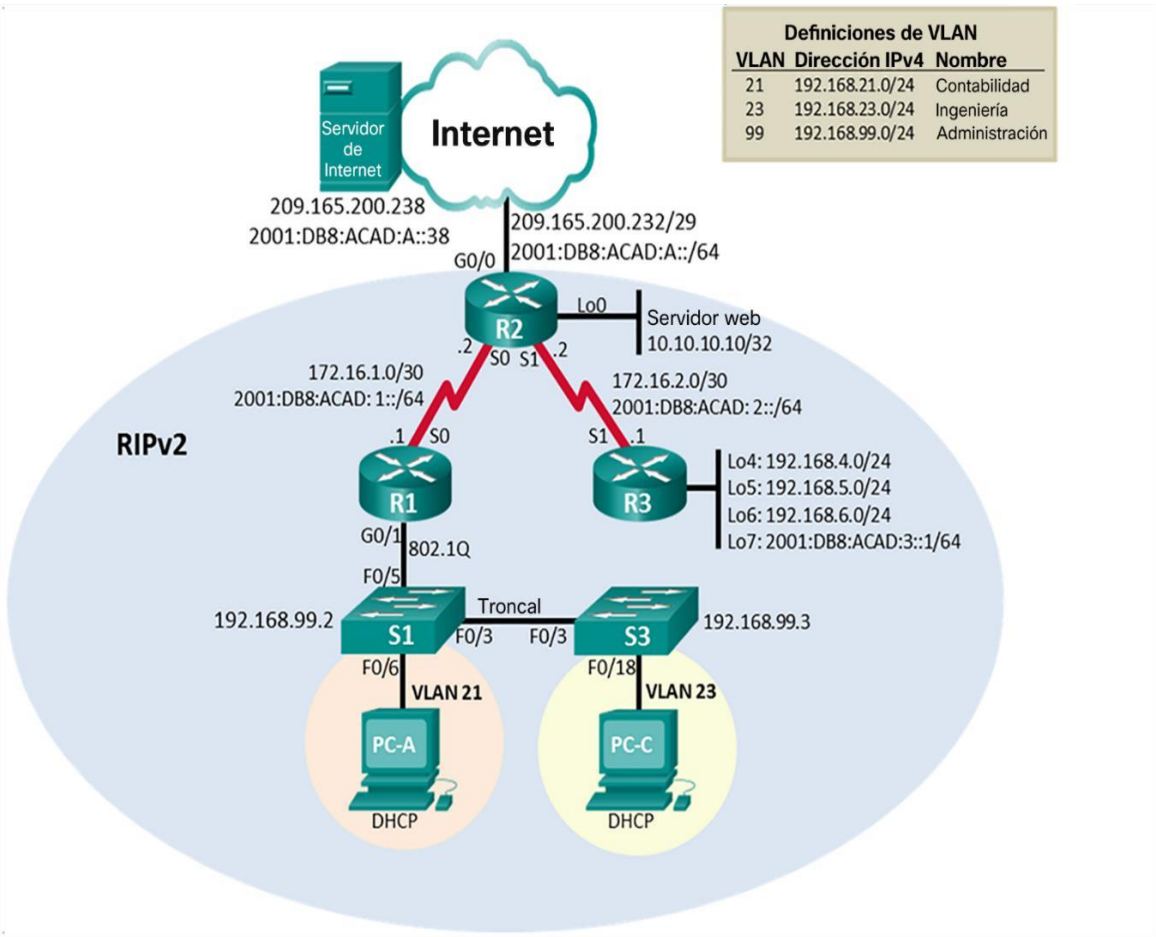
3. DESARROLLO DE LOS DOS ESCENARIOS

3.1 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.

Topología de red.

Figura 1. Topología escenario 1.



Dispositivos:

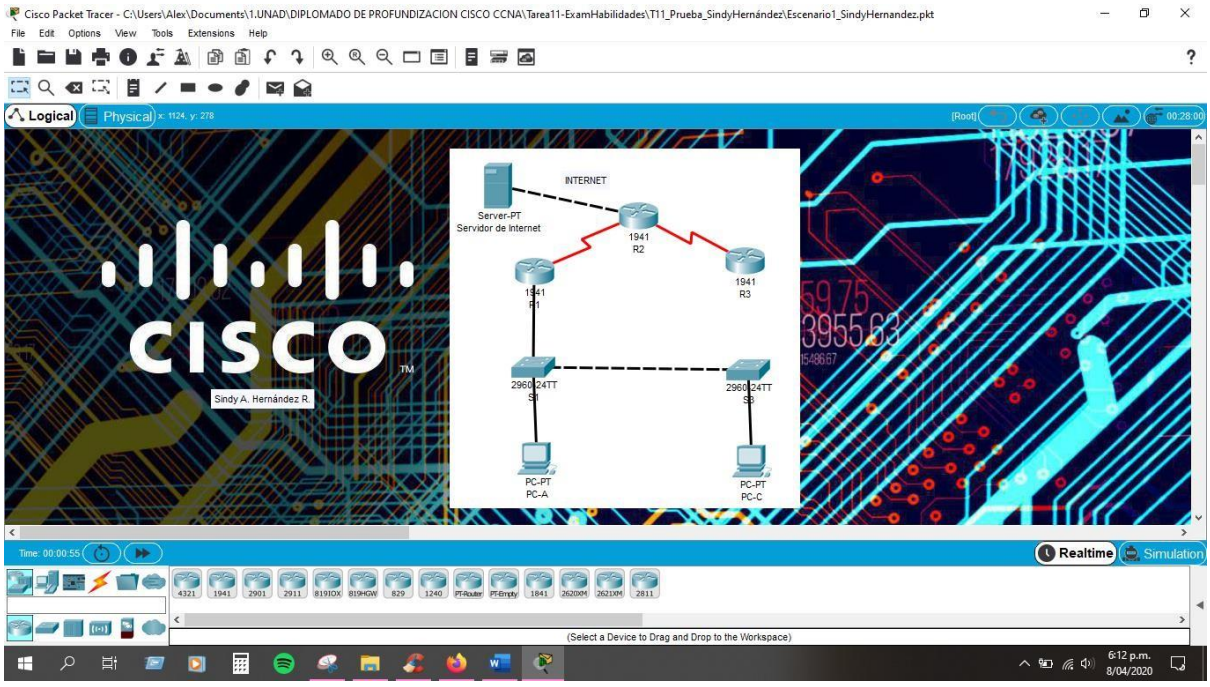
- ✓ 3 Routers 1941 series.
- ✓ 1 Servidor.
- ✓ 2 Switch Catalyst 2960 Series.
- ✓ 2 Computadores.

Parte 1: Inicializar dispositivos

Se inicia con la topología en el programa de Cisco Packet Tracer versión 7.2.1; se cambian los nombres para cada uno de los dispositivos de acuerdo con la topología.

Luego se debe incluir a cada Router sus respectivos puertos WAN, por lo tanto, se apaga los Routers y se adicionan sus tarjetas de interfaz WAN para los enlaces seriales, ya que por defecto el Router 1941 series no lo trae incluido.

Figura 2. Topología de red en Cisco Packet Tracer escenario 1.



Paso 1: Inicializar y volver a cargar los Routers y los Switch

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Antes de configurar una red, se debe realizar un previo reinicio para quitar configuraciones anteriores que puedan afectar el funcionamiento de la red que se va a configurar.

Tabla 1. Comandos para inicialización y carga de los dispositivos.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>en Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>en Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] Switch#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Parte 2: Configurar los parámetros básicos de los dispositivos

Primero, analizando la topología se realiza la tabla para verificar sus respectivas direcciones IP utilizables y máscaras para cada red.

Para las redes de IPv4

Tabla 2. Cálculo para las redes de IPv4 Routers.

R1		
Address:	172.16.1.0	10101100.00010000.00000001.000000 00
Netmask:	255.255.255.252 = 30	11111111.11111111.11111111.111111 00
Network:	172.16.1.0/30	10101100.00010000.00000001.000000 00
HostMin:	172.16.1.1	10101100.00010000.00000001.000000 01
HostMax:	172.16.1.2	10101100.00010000.00000001.000000 10
Broadcast:	172.16.1.3	10101100.00010000.00000001.000000 11
R2		

Address:	209.165.200.232	11010001.10100101.11001000.11101 110
Netmask:	255.255.255.248 = 29	11111111.11111111.11111111.11111 000
Network:	209.165.200.232/29	11010001.10100101.11001000.11101 000
HostMin:	209.165.200.233	11010001.10100101.11001000.11101 001
HostMax:	209.165.200.238	11010001.10100101.11001000.11101 110
Broadcast:	209.165.200.239	11010001.10100101.11001000.11101 111
R3		
Address:	172.16.2.0	10101100.00010000.00000010.000000 00
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111 00
Network:	172.16.2.0/30	10101100.00010000.00000010.000000 00
HostMin:	172.16.2.1	10101100.00010000.00000010.000000 01
HostMax:	172.16.2.2	10101100.00010000.00000010.000000 10
Broadcast:	172.16.2.3	10101100.00010000.00000010.000000 11

Tabla 3. Cálculo para las redes de IPv4 Switch.

VLAN 21 Contabilidad		
Address:	192.168.21.0	11000000.10101000.00010101. 00000000
Netmask:	255.255.255.0 = 24	11111111.11111111.11111111. 00000000
VLAN 23 Ingeniería		
Address:	192.168.23.0	11000000.10101000.00010111. 00000000
Netmask:	255.255.255.0 = 24	11111111.11111111.11111111. 00000000
VLAN 99 Administración		
Address:	192.168.99.0	11000000.10101000.01100011. 00000000
Netmask:	255.255.255.0 = 24	11111111.11111111.11111111. 00000000

Tabla 4. Cálculo para las interfaces de loopback R1.

Loopback 1		
Address:	10.10.10.10	00001010.00001010.00001010.00001010
Netmask:	255.255.255.255 = 32	11111111.11111111.11111111.11111111
Wildcard:	0.0.0.0	00000000.00000000.00000000.00000000

Tabla 5. Cálculo para las interfaces de loopback en R3.

Loopback 4		
Address:	192.168.4.0	11000000.10101000.00000100. 00000000
Netmask:	255.255.255.0 = 24	11111111.11111111.11111111. 00000000
Wildcard:	0.0.0.255	00000000.00000000.00000000. 11111111
Loopback 5		
Address:	192.168.5.0	11000000.10101000.00000101. 00000000
Netmask:	255.255.255.0 = 24	11111111.11111111.11111111. 00000000
Wildcard:	0.0.0.255	00000000.00000000.00000000. 11111111

Loopback 6		
Address:	192.168.6.0	11000000.10101000.00000110. 00000000
Netmask:	255.255.255.0 = 24	11111111.11111111.11111111. 00000000
Wildcard:	0.0.0.255	00000000.00000000.00000000. 11111111

Para las redes de IPv6

Tabla 6. Cálculo para las redes de IPv6 Routers.

R1		
Address:	2001:DB8:ACAD:1::/64	2001:0DB8:ACAD:0001:0000:0000:0000:0000
Address:	2001:DB8:ACAD:1::1	2001:0DB8:ACAD:0001:0000:0000:0000:0001
R2		
Address:	2001:DB8:ACAD:A::38/64	2001:0DB8:ACAD:000a:0000:0000:0000:0000
Address:	2001:DB8:ACAD:A::1	2001:0DB8:ACAD:000a:0000:0000:0000:0001
R3		
Address:	2001:DB8:ACAD:2::/64	2001:0DB8:ACAD:0002:0000:0000:0000:0000
Address:	2001:DB8:ACAD:2::1	2001:0DB8:ACAD:0002:0000:0000:0000:0001

Tabla 7. Cálculo para las interfaces de loopback en R3.

Loopback 7		
Address:	2001:DB8:ACAD:3::1/64	2001:0DB8:ACAD:0003:0000:0000:0000:0001

Paso 2: Configurar la computadora de Internet

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

Teniendo en cuenta la tabla de direcciones para las redes de IPV6 e IPV4 se proporciona las direcciones en la tarjeta de red del servidor de internet.

Tabla 8. Direcciónes IP para servidor de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
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.

Del Paso 3 al Paso 7, los comandos emitidos en los dispositivos de red para Routers y Switch; hacen parte de la configuración inicial de los dispositivos de red, proporcionando claves, cifrado, acceso remoto, local y líneas de configuraciones; así como también se emiten menajes del día para evitar posibles accesos no autorizados al dispositivo, se nombran los dispositivos y se describen para no confundir al momento de emitir o realizar alguna prueba de conectividad.

Es necesario nombrar los dispositivos ya que se debe tener un orden en la topología para así llegar a una solución; en caso de tener una falla en alguna red sea LAN o WAN se puede verificar más rápidamente que dispositivo es el que requiere la atención del administrador de red y así corregir rápidamente.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Comandos iniciales en R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco

	R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description WANS0 connection to R1 R1(config-if)#ip add 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shut
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 4: Configurar R2

Se proporcionan las direcciones de loopback, así como las rutas predeterminadas para la red IPv4 e IPv6.

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Comandos iniciales en R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login

	R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description WANS0 connection to R2 R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:1::2/64 R2(config-if)#no shut R2(config-if)#exit
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description WANS1 connection to R2 R2(config-if)#ip add 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shut R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description ServidorInternet connection to R2 R2(config-if)#ip add 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64 R2(config-if)#no shut
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)#ip add 10.10.10.10 255.255.255.255 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)#end

Paso 5: Configurar R3

Se proporcionan las direcciones de loopback, así como las rutas predeterminadas para la red IPv4 e IPv6.

La configuración del R3 incluye las siguientes tareas:

Tabla 11. Comandos iniciales en R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description WANS1 connection to R3 R3(config-if)#ip add 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64 R3(config-if)#no shut
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip add 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip add 192.168.5.1 255.255.255.0.

Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip add 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ipv6 add 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 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Comandos iniciales del switch S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Comandos iniciales del switch S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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 S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &

Paso 8: Verificar la conectividad de la red

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

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

Tabla 14. Verificar la conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success
R2	R3, S0/0/1	172.16.2.1	Success
PC de Internet	Gateway predeterminado	209.165.200.233	Success

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

De acuerdo con la tabla anterior, se realiza capturas de las pruebas de conectividad entre Routers mediante ping, así como en PC de Internet.

Figura 3. Ping de conectividad del Router R1 hacia R2 serial 0.

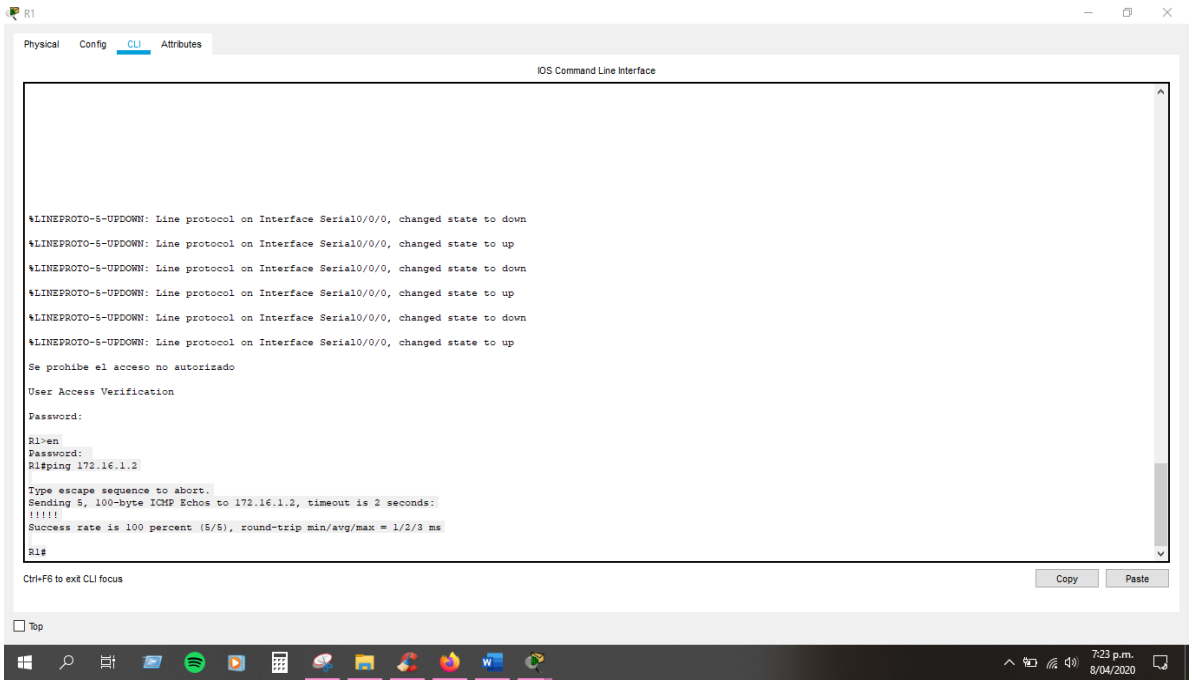


Figura 4. Ping de conectividad del Router R2 hacia R3 serial 1.

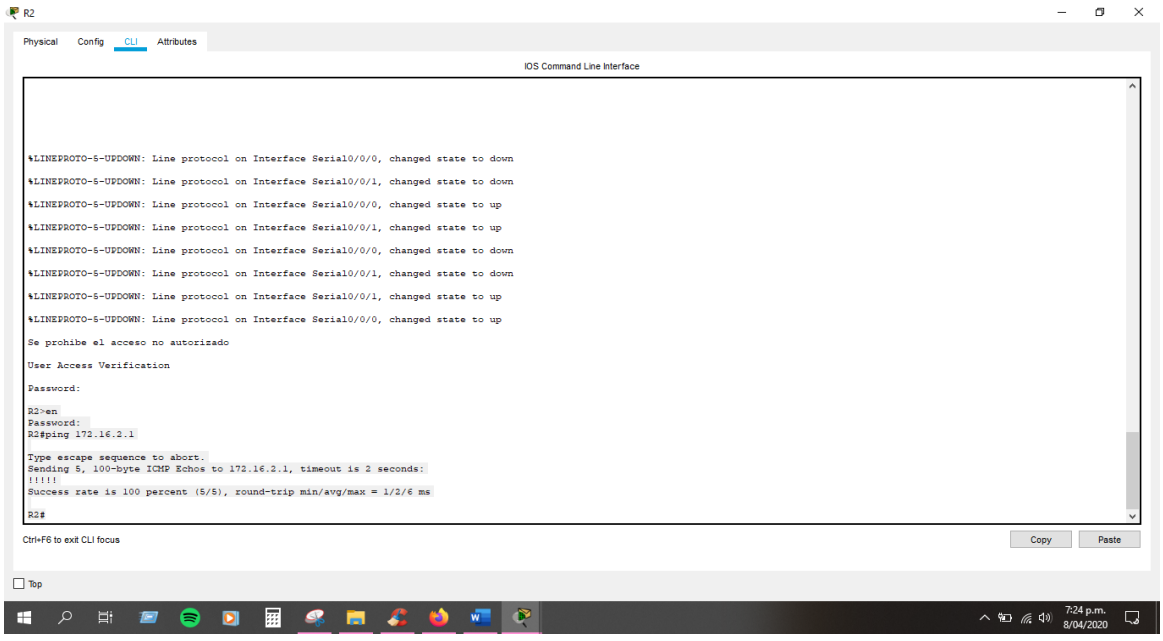
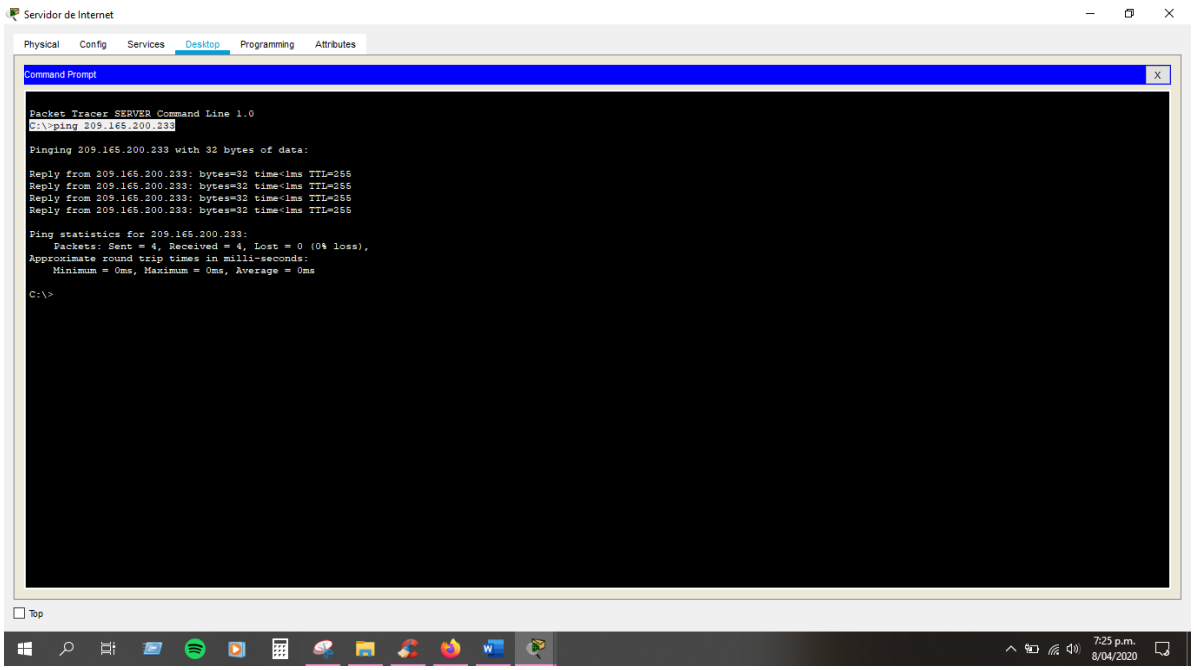


Figura 5. Ping desde Servidor Internet hacia G0/0 del Router R2.



Parte 3: Configurar la seguridad del Switch, las VLAN y el Routing entre VLAN

En el paso 9 al paso 10; se configuran los dispositivos del Switch en S1 y S3, creando sus VLANs correspondientes, así como configurando sus puertos de acceso y troncales para llevar una mejor administración de los datos que viajan a través de la red; además se apagan los puertos que no están en uso para evitar posibles vulnerabilidades en la red, esto con el fin de proporcionar mayor seguridad.

Paso 9: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 15. Comandos VLAN Switch S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit

Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip add 192.168.99.2 255.255.255.0 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)#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	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	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)#shut

Paso 10: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Comandos VLAN Switch S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#int vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el Gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	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)#shut

Paso 11: Configurar R1

Se realiza la configuración de las subinterfaces para establecer una red IP, especificando las VLAN a la cual se asocia las subinterfaces para no confundir al momento de verificar y proporcionar las direcciones de enrutamiento para intra-VLAN.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Comandos subinterfaz 802.1Q en R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shut

Paso 12: Verificar la conectividad de la red

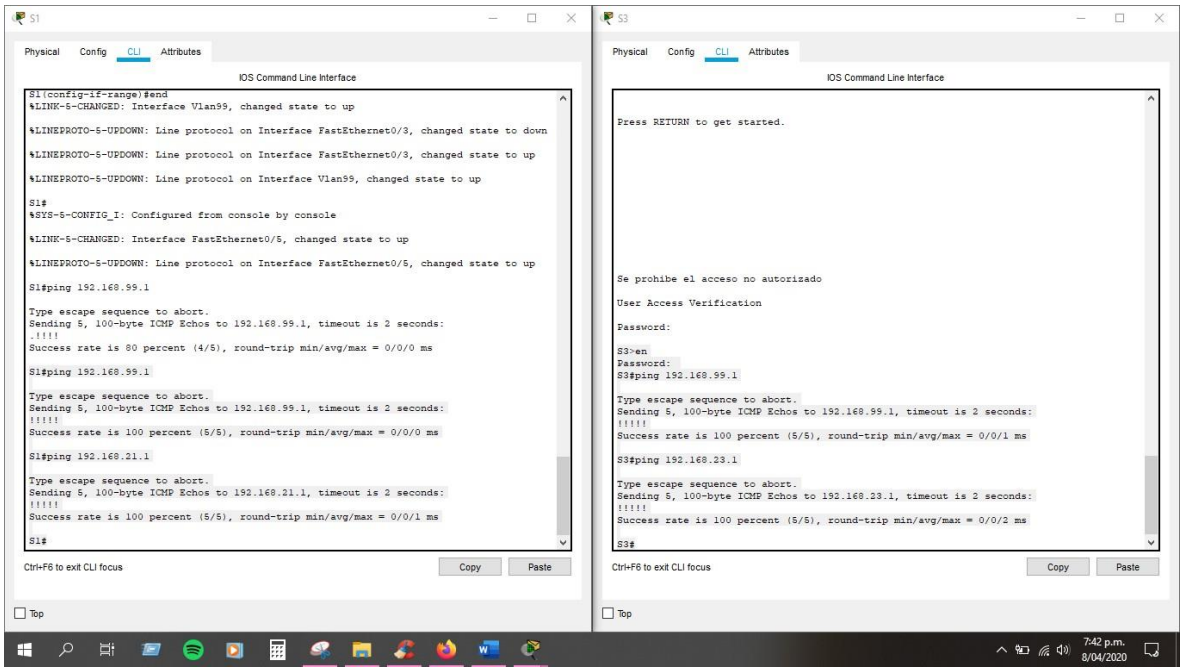
Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 18. Verificar la conectividad de redes VLAN.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Success
S3	R1, dirección VLAN 99	192.168.99.1	Success
S1	R1, dirección VLAN 21	192.168.21.1	Success
S3	R1, dirección VLAN 23	192.168.23.1	Success

De acuerdo con la tabla anterior, se realiza capturas de las pruebas de conectividad hacia las VLANs emitidas en los Switch S1 y S3 mediante ping.

Figura 6. Conectividad hacia VLANs mediante ping Switch S1 Y S3 a R1.



Parte 4: Configurar el protocolo de routing dinámico RIPv2

Del paso 13 al paso 15; se activa el protocolo de RIPv2; ya que la topología tiene las direcciones IP en VLSM por lo tanto se requiere la versión 2, así que se verifican las redes directamente conectadas y además se desactivan las interfaces que no requieren el protocolo de RIPv2 por no tener conexiones adyacentes.

Paso 13: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Comandos para RIPv2 en 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	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
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 14: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Comandos para RIPv2 en R2.

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
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 15: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Comandos para RIPv2 en R3.

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
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 16: 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 22. Comandos show para RIP.

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

De acuerdo con la tabla anterior, se realiza capturas de pruebas de los comandos emitidos en los Routers R1, R2 y R3.

Figura 7. Verificación show ip protocols en R1 y R2.

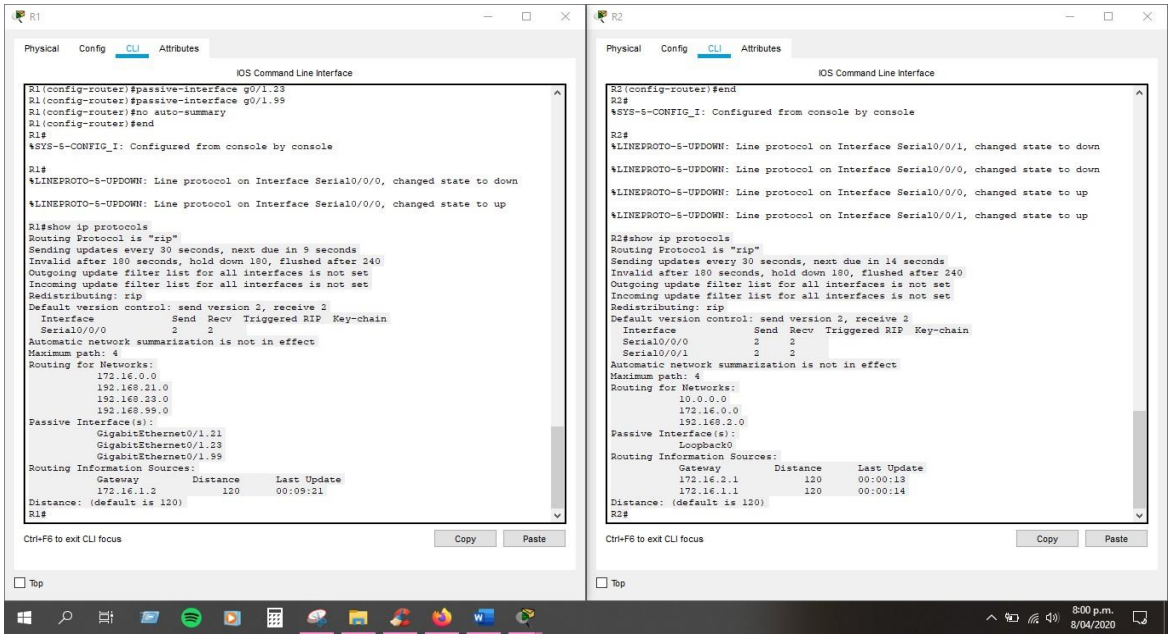


Figura 8. Verificación show ip protocols en R3.

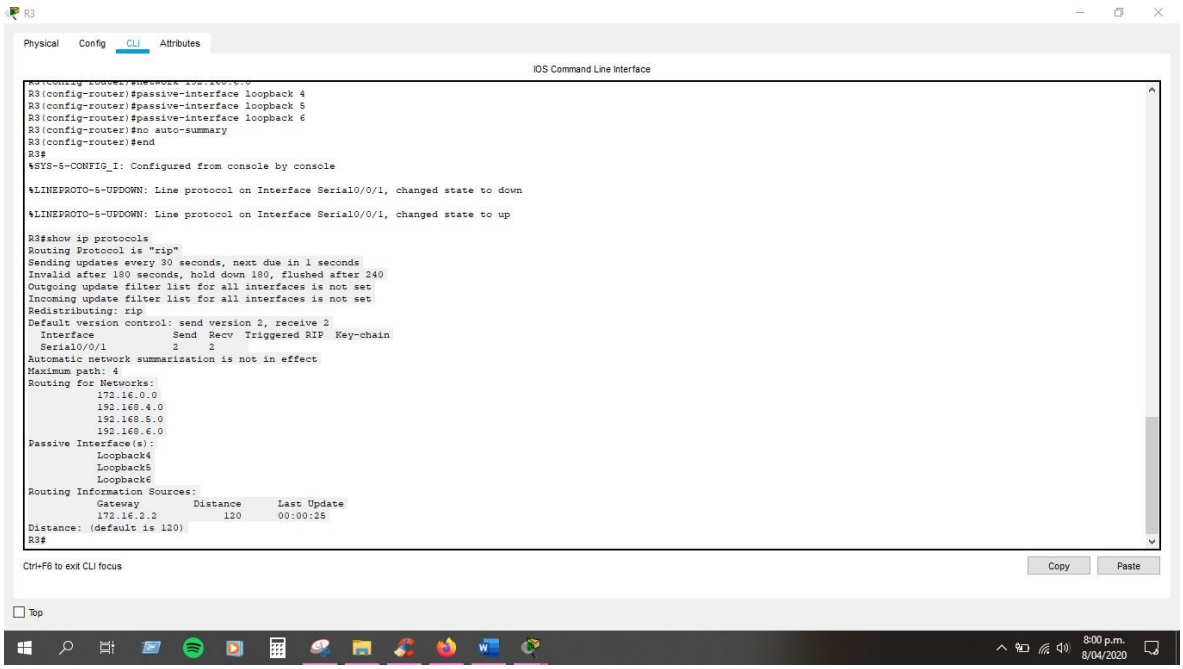


Figura 9. Verificación Show ip route rip en R1 y R2.

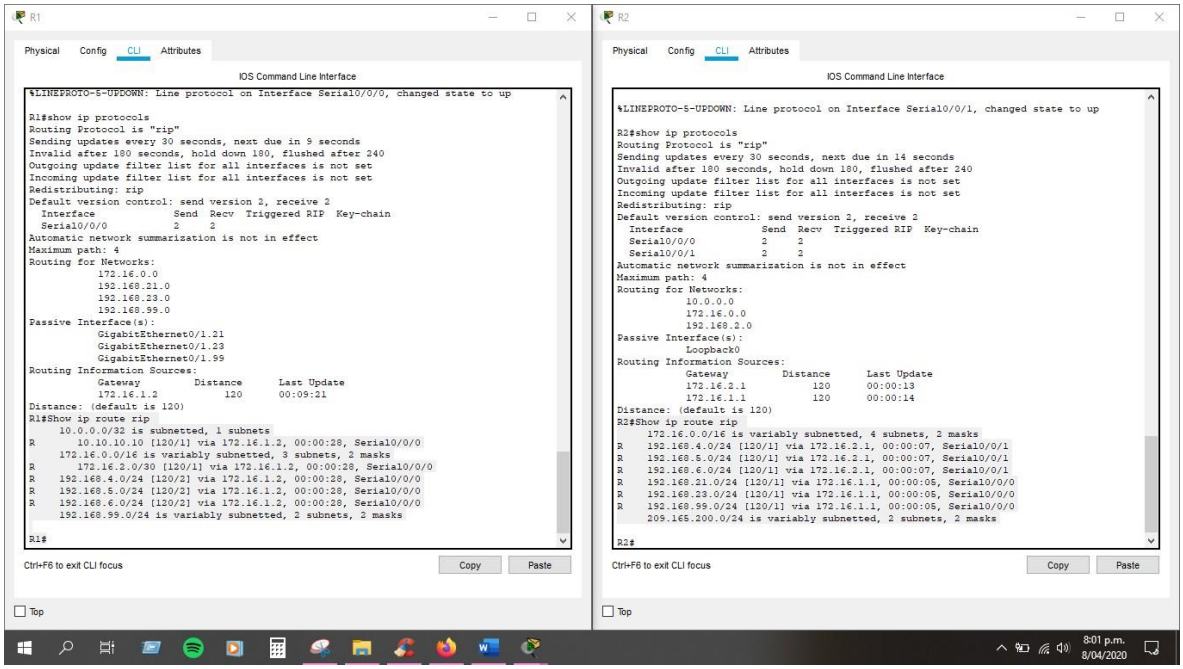


Figura 10. Verificación Show ip route rip en R3.

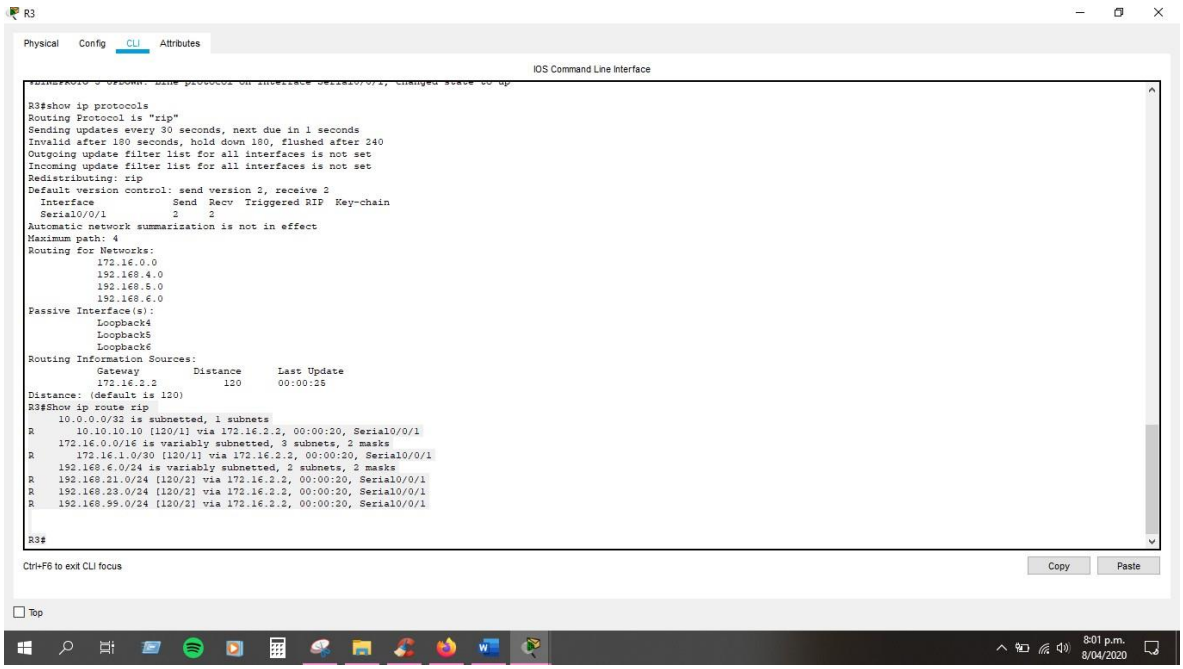


Figura 11. Verificación show run en R1 y R2.

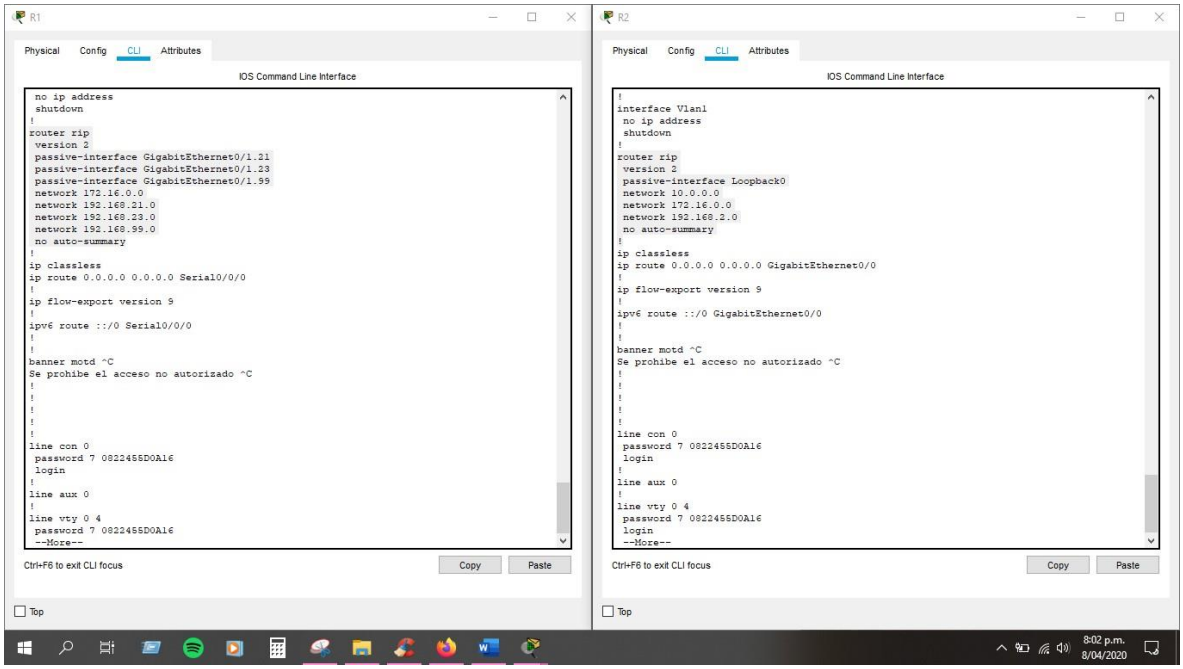
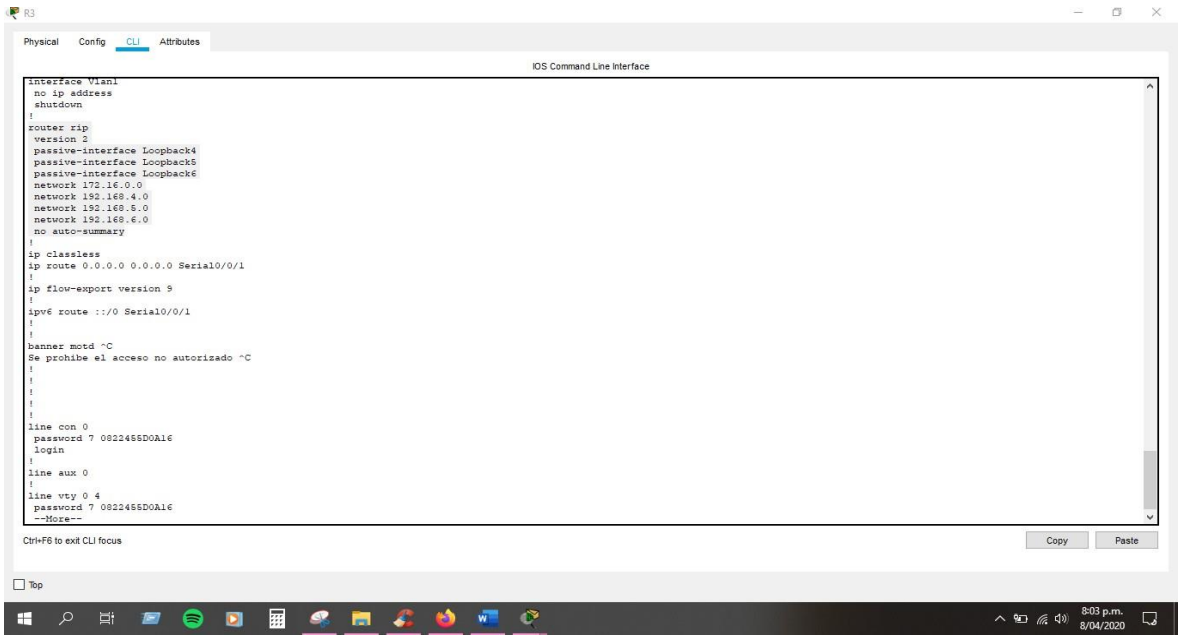


Figura 12. Verificación show run en R3.



Parte 5: Implementar DHCP y NAT para IPv4

Paso 17: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Se realiza la configuración en el Router R1 para proporcionar direccionamiento por DHCP para las VLAN 21 y VLAN 23, estableciendo las primeras 20 direcciones IP como reserva para cada VLAN; ya que cada VLAN maneja diferentes subredes se requiere configurar 2 pool diferentes para así asignar las direcciones a cada una.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Comandos para DHCP y NAT en R1.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10

	R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

Paso 18: Configurar la NAT estática y dinámica en el R2

Se establece configuración NAT para rutas estáticas de una IP privada hacia una IP publica en este caso para conectarse al servidor web, así también se define las listas de acceso de forma dinámica dentro de la ACL privada.

Se realiza la sumarización de las redes de Loopback; para establecer una red resumida junto con la Wildcard, para crear la lista de acceso e incluirla en la NAT dinámica del Router R2.

Tabla 24. Cálculo de sumarización para las interfaces de Loopback.

Loopback		
Address:	192.168.4.0	11000000.10101000.00000100. 00000000
Address:	192.168.5.0	11000000.10101000.00000101. 00000000
Address:	192.168.6.0	11000000.10101000.00000110. 00000000
Nueva red		
Network	192.168.4.0/22	11000000.10101000.00000100. 00000000
Wildcard:	0.0.3.255	00000000.00000000.00000011. 11111111

La configuración del R2 incluye las siguientes tareas:

Tabla 25. Comandos para NAT estática y dinámica en R2.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#Ip http server

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#Ip http authentication local
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)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 19: 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 26. Verificar el protocolo DHCP y la NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	success
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	success
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	success
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237)	No se ha logrado porque al realizar la activación en http server en el Router el comando no es compatible con Packet Tracer

Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	

De acuerdo con la tabla anterior, se realiza capturas de DHCP establecidas en las tarjetas de red de los host y pruebas de conectividad emitidas de Host y servidor.

Figura 13. PC-A información de IP del servidor de DHCP.

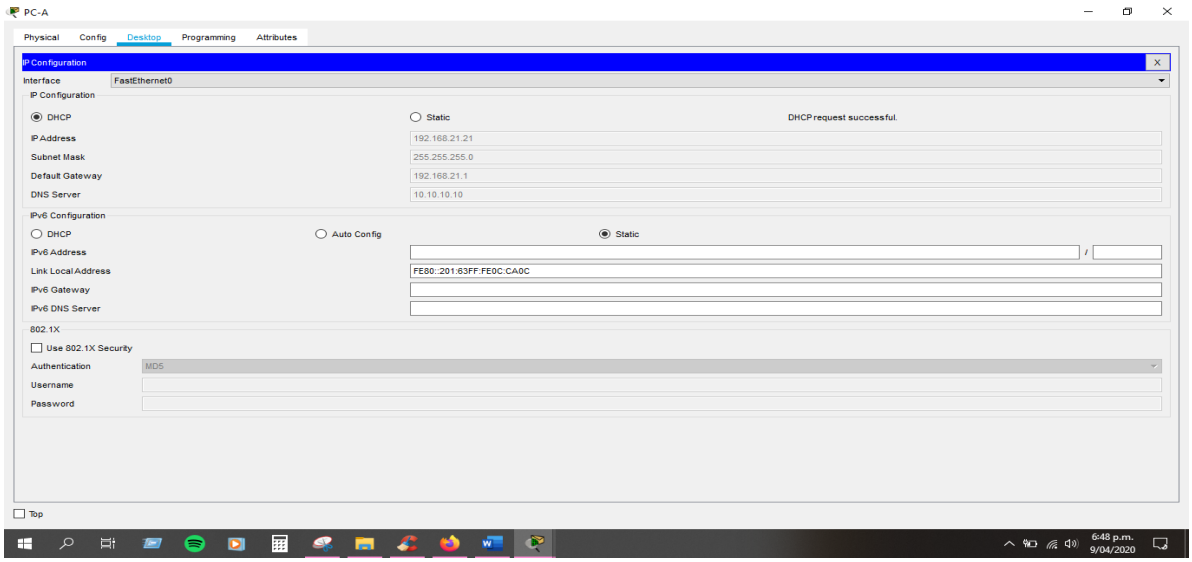


Figura 14. PC-C información de IP del servidor de DHCP.

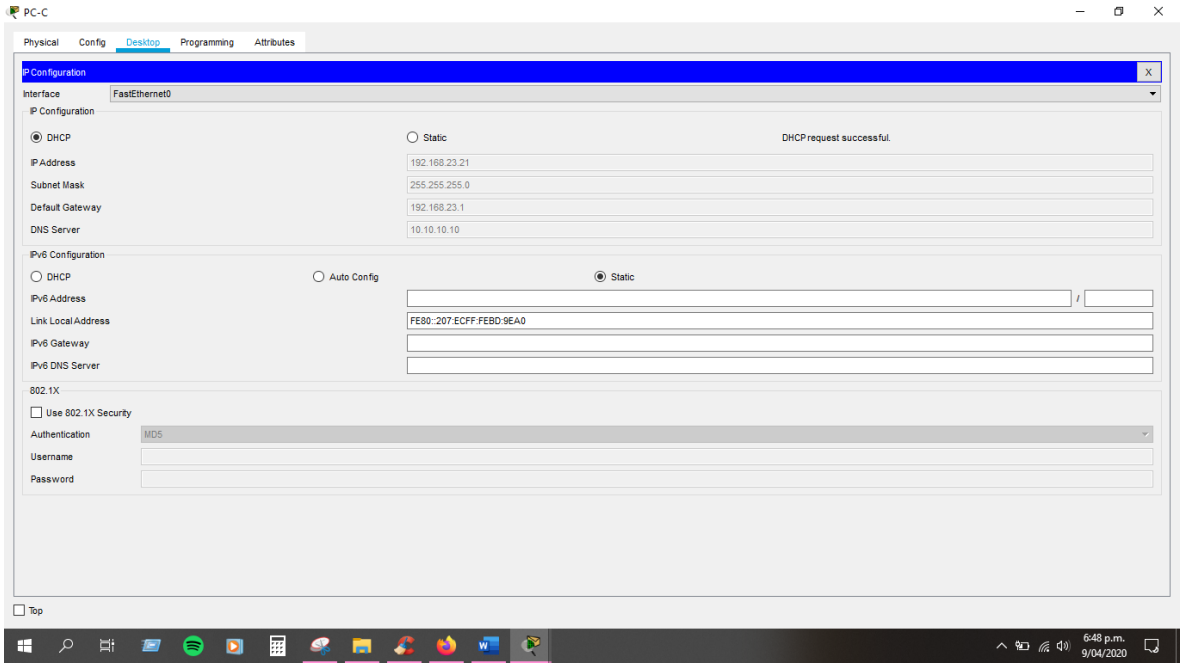


Figura 15. PC-A ping hacia PC-C.

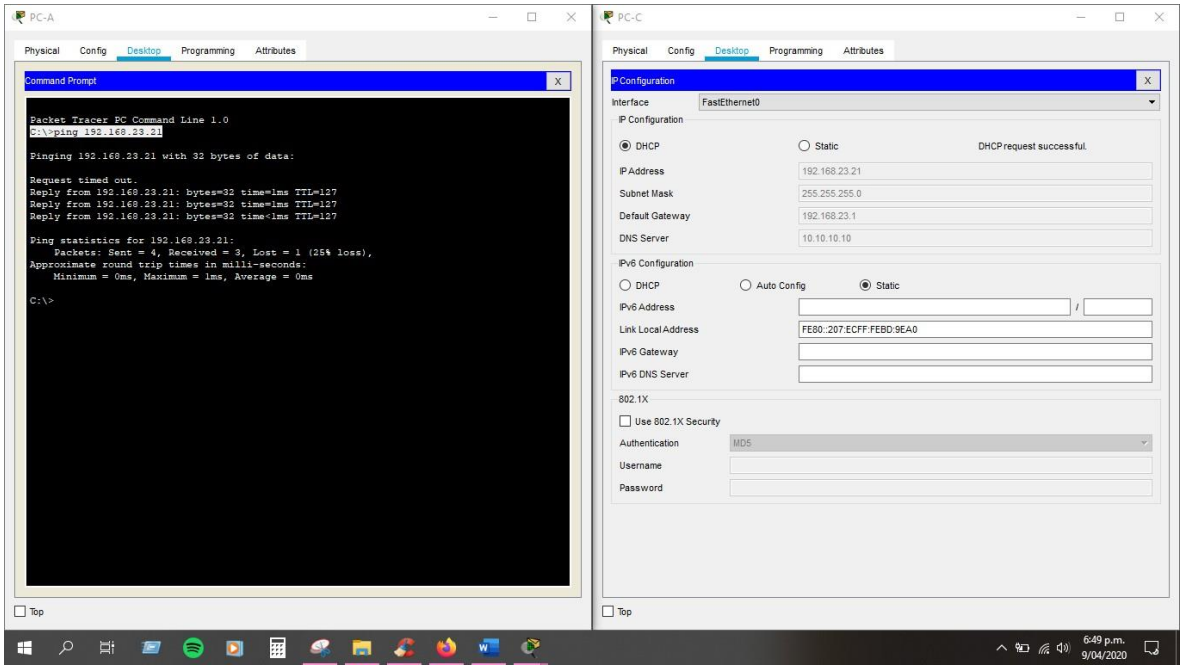
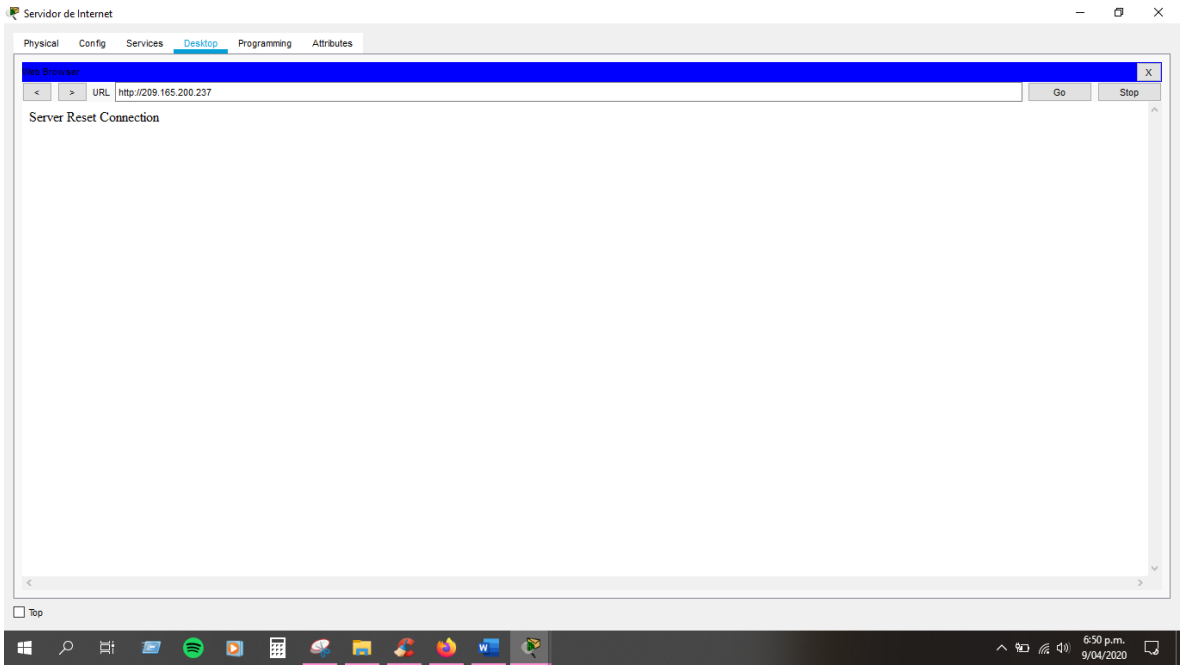


Figura 16. Servidor Web del Servidor Internet.



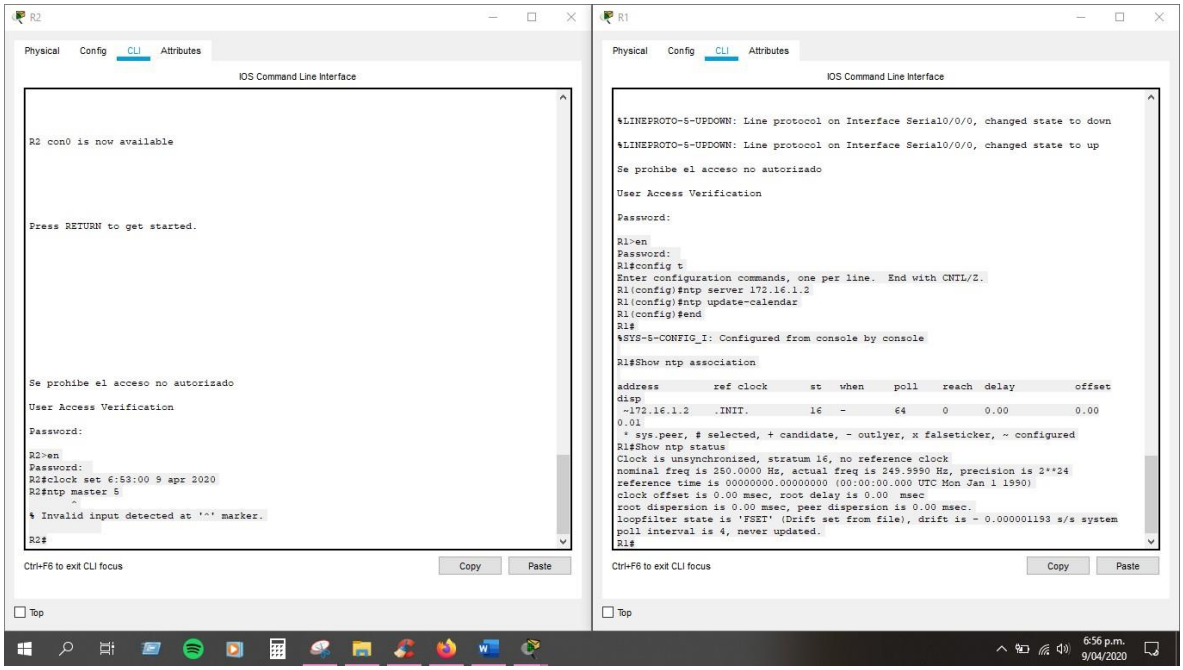
Parte 6: Configurar NTP

Se establece NTP para proporcionar la hora automáticamente a los hosts conectados al mismo y así es más factible llevar un control del tiempo sobre el acceso de los hosts conectados a la red.

Tabla 27. Comandos para NTP en R2.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 6:53:00 9 apr 2020
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2#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.	ntp update-calendar
Verifique la configuración de NTP en R1.	Show ntp association Show ntp status

Figura 17. Configuración NTP en R1 y R2.



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

Paso 20: Restringir el acceso a las líneas VTY en el R2

Se realiza la configuración ACL para que solo se permita conexión mediante Telnet a R1 con R2 y así restringir el acceso a esa conexión a otros dispositivos de la red.

Tabla 28. Comandos para lineas VTY en 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** ip access-list standard ADMIN-MGT permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	Line vty 0 15
Permitir acceso por Telnet a las líneas de VTY	access-class ADMIN-MGT in transport input telnet
Verificar que la ACL funcione como se espera	telnet 172.16.1.2

De acuerdo con la tabla anterior, se realiza capturas de pruebas Telnet establecidas para R1y R2, además se verifica que ACL restrinja el acceso del Router R3 a Telnet.

Figura 18. Configuración NTP en R2 y verificación ACL Telnet R1.

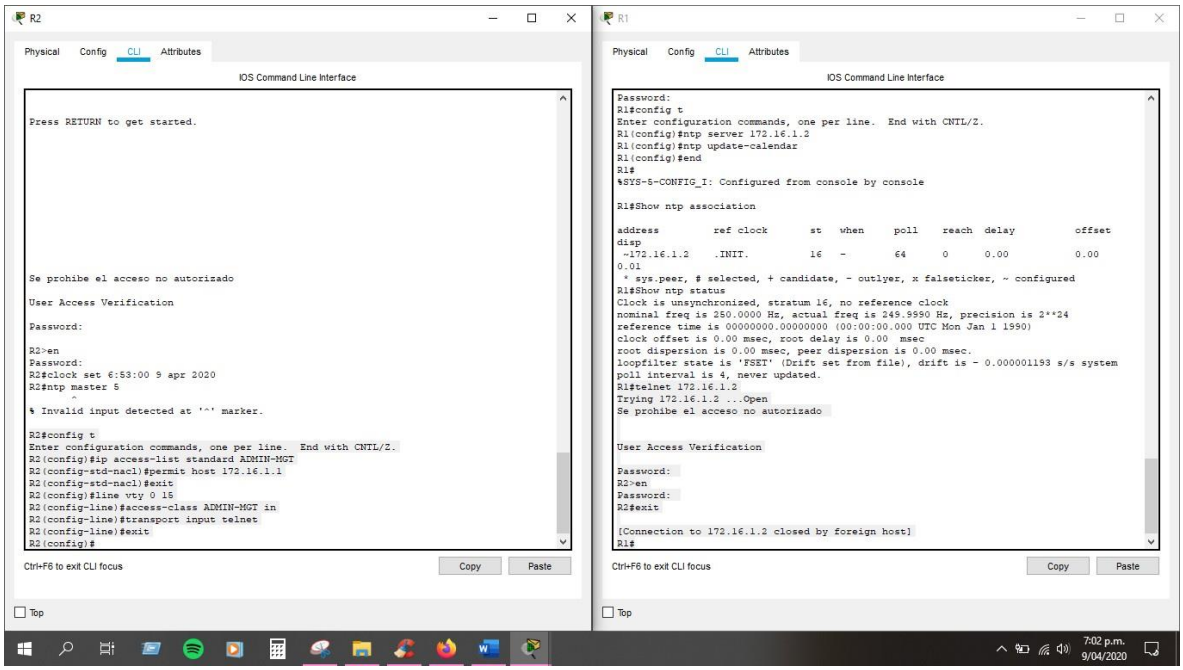
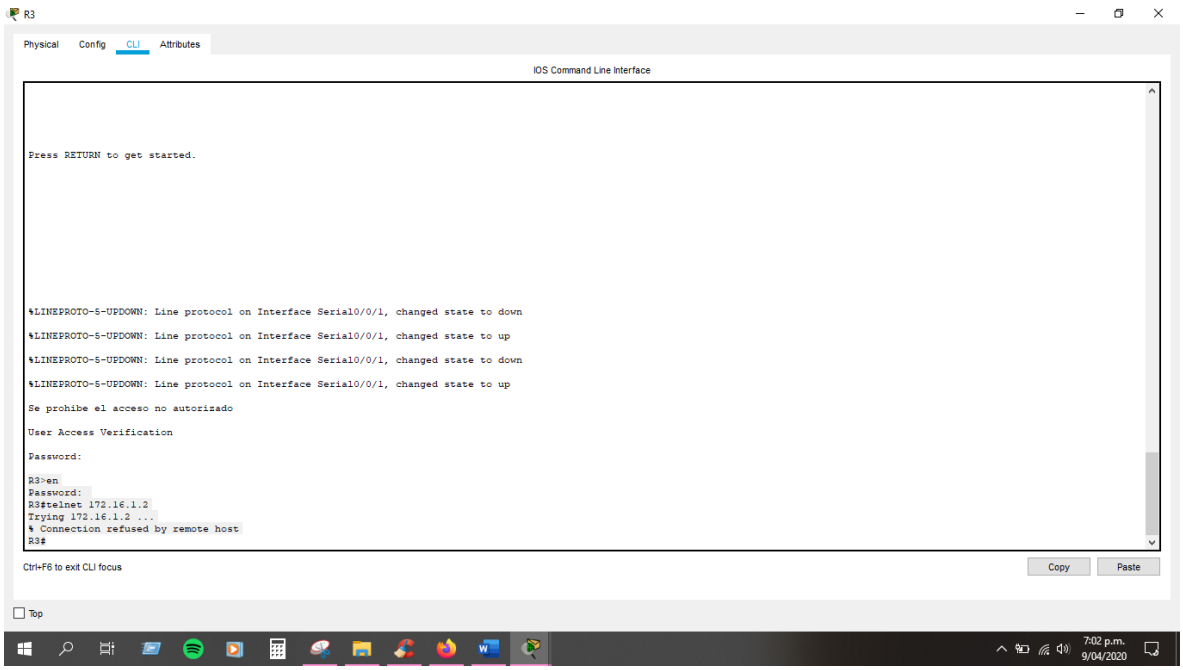


Figura 19. Verificación Telnet en R3.



Paso 21: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 29. Comandos de CLI.

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

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translations *

De acuerdo con la tabla anterior, se realiza capturas de prueba de comandos Show y Clear en el Router, así como pruebas de conectividad emitidos en los Host.

Figura 20. Comandos lista de acceso, restablecer acceso y ACL para R2.

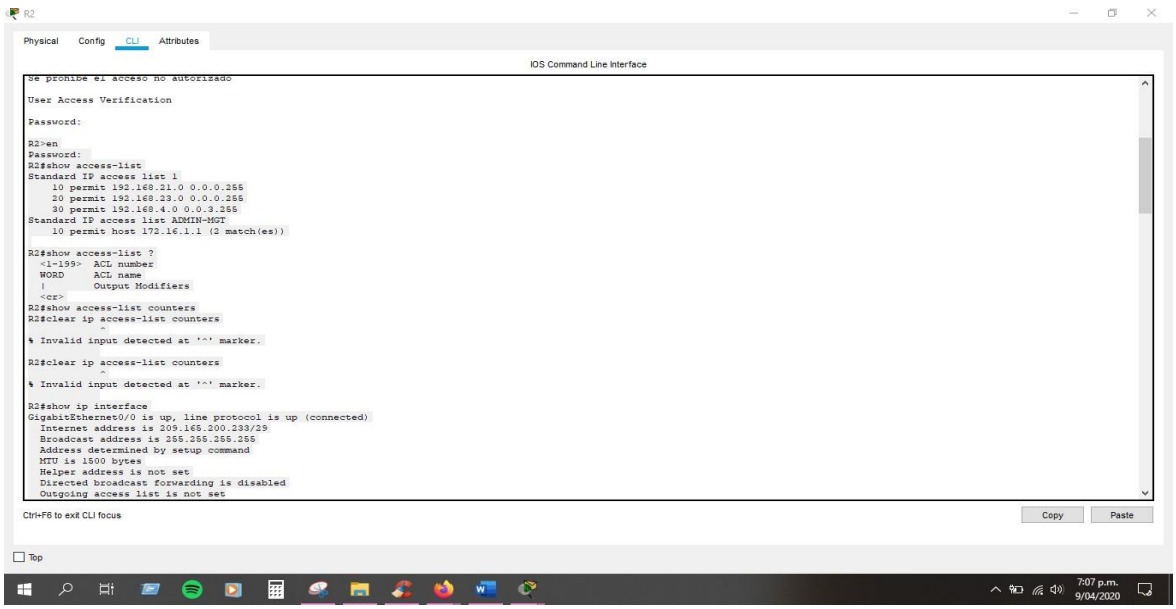


Figura 21. Ping de PC-A y PC-C hacia el servidor de Internet.

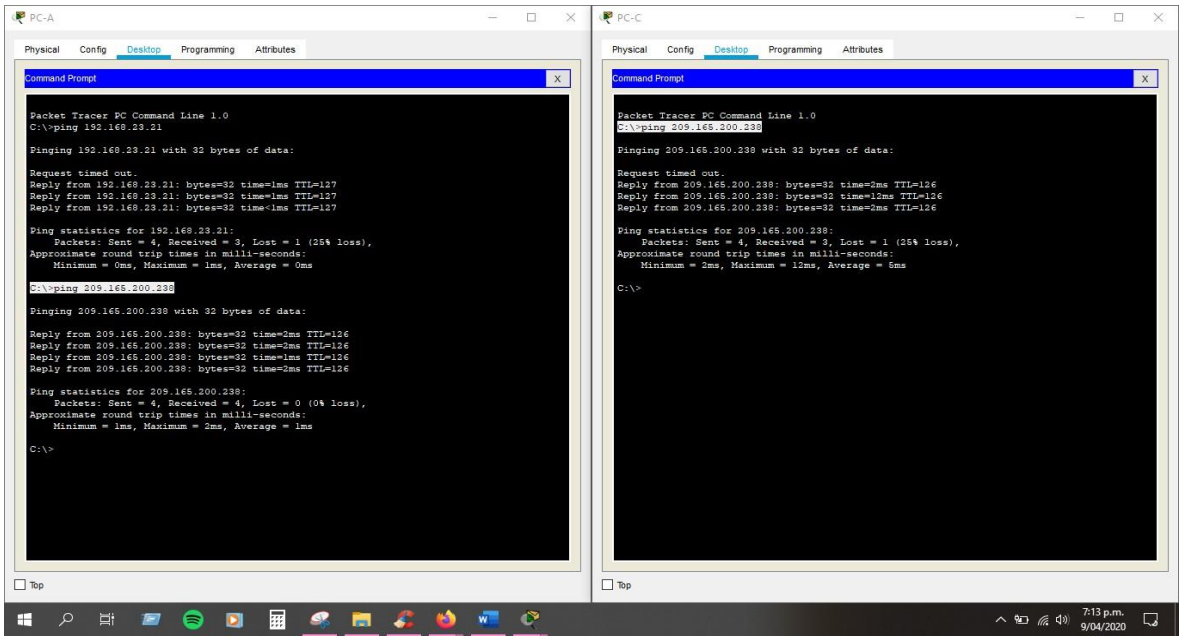


Figura 22. Conectividad PC-A y PC-C hacia el Servidor de Internet.

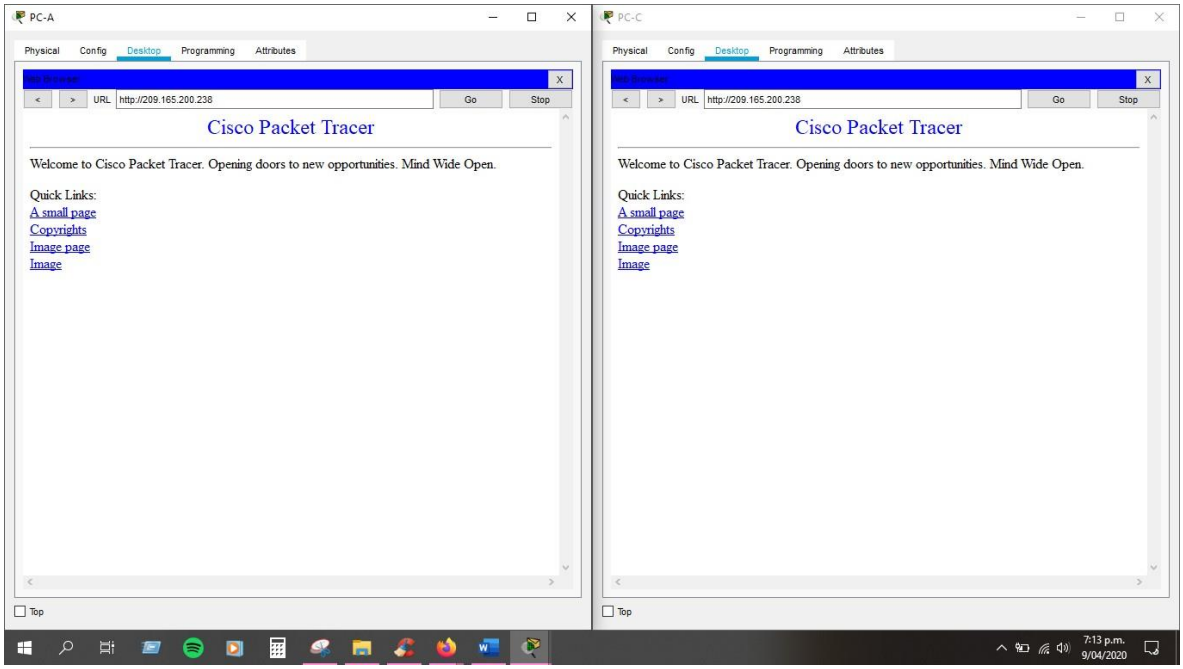
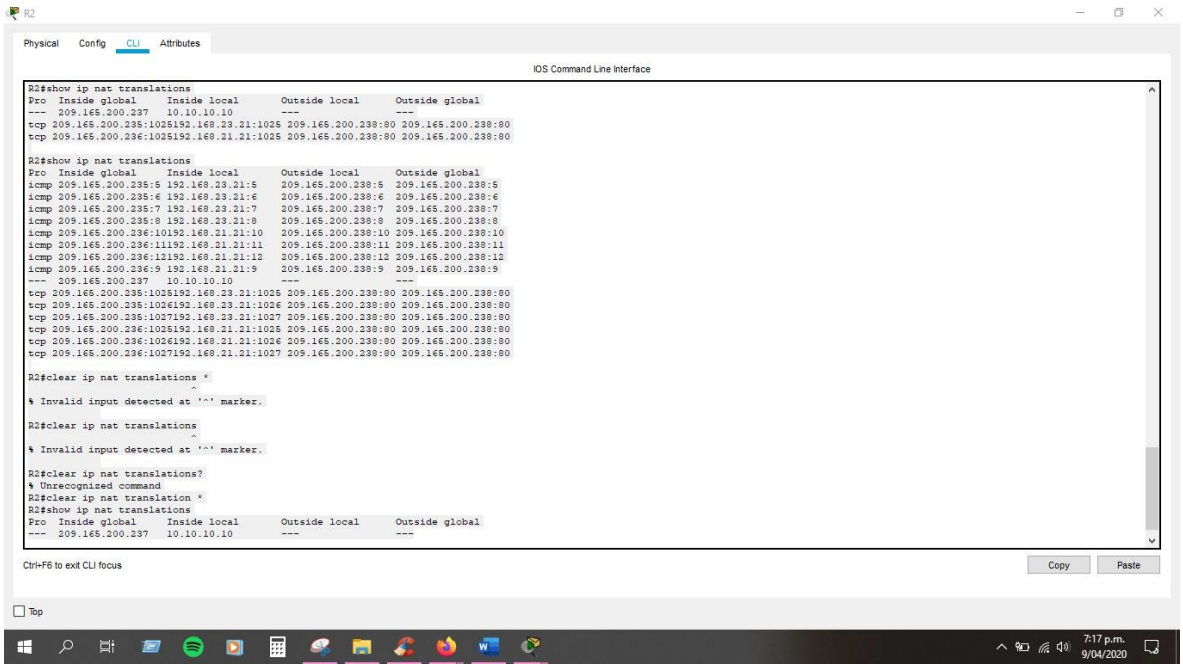


Figura 23. Traducciones NAT en R2 de las redes de PC-A y PC-C emitidas.

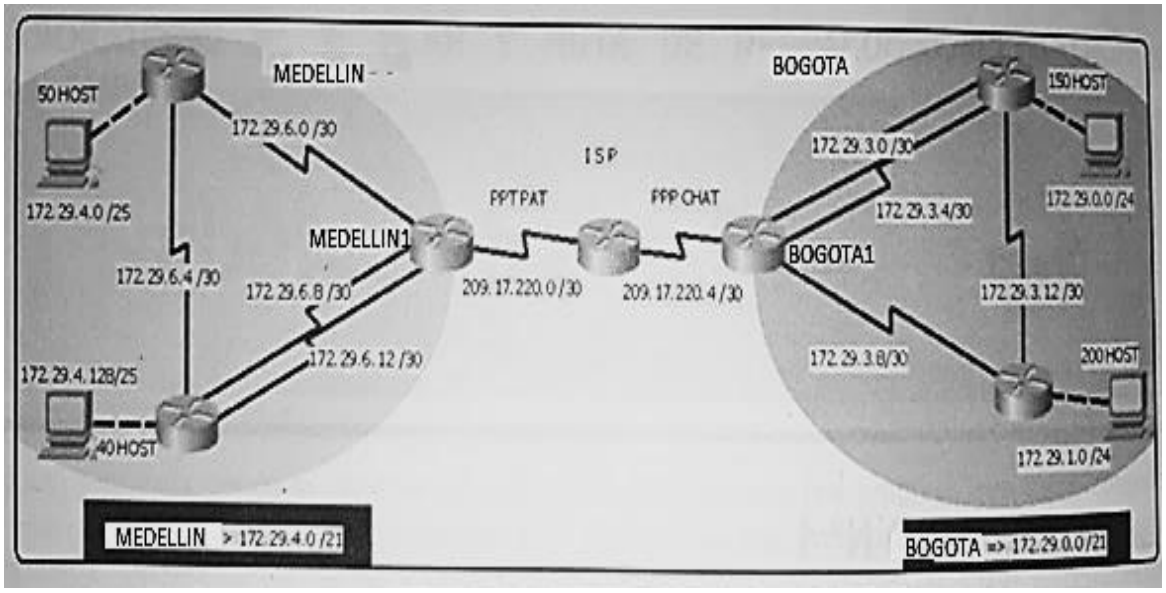


3.2 ESCENARIO 2

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.

Topología de red.

Figura 24. Topología 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.

Dispositivos:

- ✓ 7 Routers 1941 series.
- ✓ 4 Computadores.

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

Configuracion inicial de los Routers

Se establece contraseñas de acceso a las lineas, asi como el nombre de los disporistivos , el mensaje del día para advertir sobre el acceso no autorizado y se encripta las contraseñas de acceso para establecer la seguridad en la red.

ISP

```
Router>enable
Router#config 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)#exit
ISP(config)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd &
Enter TEXT message. End with the character '&'.
Se prohibe el acceso no autorizado &
```

Medellín 1

```
Router>enable
Router#config 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)#exit
Medellin1(config)#line vty 0 15
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
```

```
Medellin1(config-line)#exit
Medellin1(config)#service password-encryption
Medellin1(config)#banner motd &
enter text message. end with the character '&'.
se prohibe el acceso no autorizado &
```

Medellín 2

```
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)#exit
Medellin2(config)#line vty 0 15
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#exit
Medellin2(config)#service password-encryption
Medellin2(config)#banner motd &
Enter TEXT message. End with the character '&'.
Se prohibe el acceso no autorizado &
```

Medellín 3

```
Router>enable
Router#config 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
Medellin3config-line)#exit
Medellin3(config)#line vty 0 15
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#exit
Medellin3(config)#service password-encryption
Medellin3(config)#banner motd &
```

```
Enter TEXT message. End with the character '&'.
Se prohibe el acceso no autorizado &
```

Bogotá 1

```
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)#exit
Bogota1(config)#line vty 0 15
Bogota1(config-line)#password cisco
Bogota1(config-line)#login
Bogota1(config-line)#exit
Bogota1(config)#service password-encryption
Bogota1(config)#banner motd &
Enter TEXT message. End with the character '&'.
Se prohibe el acceso no autorizado &
```

Bogotá 2

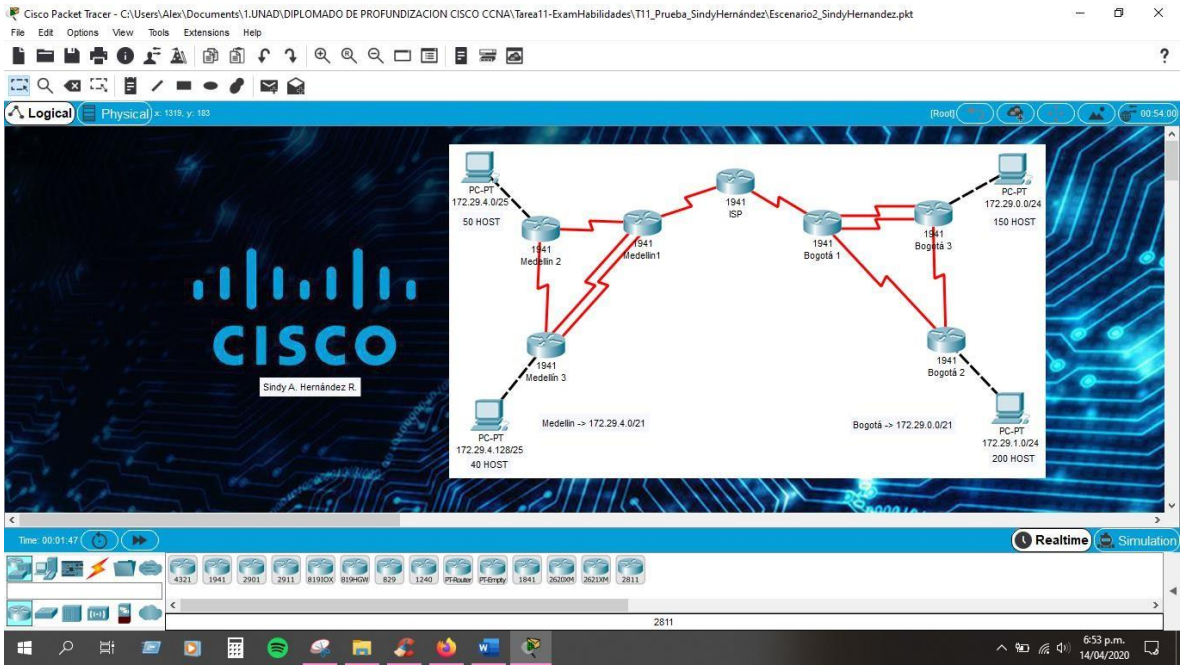
```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname Bogota2
Bogota2(config)#enable secret class
Bogota2(config)#line console 0
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#exit
Bogota2(config)#line vty 0 15
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#exit
Bogota2(config)#service password-encryption
Bogota2(config)#banner motd &
Enter TEXT message. End with the character '&'.
Se prohibe el acceso no autorizado &
```

Bogotá 3

```
Router>enable
Router#config 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)#exit
Bogota3(config)#line vty 0 15
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#exit
Bogota3(config)#service password-encryption
Bogota3(config)#banner motd &
Enter TEXT message. End with the character '&'.
Se prohibe el acceso no autorizado &
```

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

Figura 25. Topología de red en Cisco Packet Tracer escenario 2.



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

Para realizar la configuracion mediante las redes de IPV4 dadas, se realiza una previo calculo de las redes para hallar e identificar las IP utilizables correspondientes para cada red, asi como la máscara de subred, Boadcast, Wildcard, etc.

ISP (Clase C)

Tabla 30. Cálculo para la red para seriales de ISP.

Address:	**209.17.220.0**	**11010001.00010001.11011100.000000**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	209.17.220.0	11010001.00010001.11011100.000000	00
Broadcast:	209.17.220.3	11010001.00010001.11011100.000000	11
HostMin:	209.17.220.1	11010001.00010001.11011100.000000	01
HostMax:	209.17.220.2	11010001.00010001.11011100.000000	10
Address:	**209.17.220.4**	**11010001.00010001.11011100.000001**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	209.17.220.4	11010001.00010001.11011100.000001	00
Broadcast:	209.17.220.7	11010001.00010001.11011100.000001	11
HostMin:	209.17.220.5	11010001.00010001.11011100.000001	01
HostMax:	209.17.220.6	11010001.00010001.11011100.000001	10

Medellín (Clase B)

Tabla 31. Cálculo para la red seriales de Medellín.

Address:	**172.29.6.0**	**10101100.00011101.00000110.000000**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	172.29.6.0	10101100.00011101.00000110.000000	00
Broadcast:	172.29.6.3	10101100.00011101.00000110.000000	11
HostMin:	172.29.6.1	10101100.00011101.00000110.000000	01
HostMax:	172.29.6.2	10101100.00011101.00000110.000000	10
Address:	**172.29.6.4**	**10101100.00011101.00000110.000001**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	172.29.6.4	10101100.00011101.00000110.000001	00
Broadcast:	172.29.6.7	10101100.00011101.00000110.000001	11

HostMin:	172.29.6.5	10101100.00011101.00000110.000001	01
HostMax:	172.29.6.6	10101100.00011101.00000110.000001	10
Address:	**172.29.6.8**	**10101100.00011101.00000110.000010**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	172.29.6.8	10101100.00011101.00000110.000010	00
Broadcast:	172.29.6.11	10101100.00011101.00000110.000010	11
HostMin:	172.29.6.9	10101100.00011101.00000110.000010	01
HostMax:	172.29.6.10	10101100.00011101.00000110.000010	10
Address:	**172.29.6.12**	**10101100.00011101.00000110.000011**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	172.29.6.12	10101100.00011101.00000110.000011	00
Broadcast:	172.29.6.15	10101100.00011101.00000110.000011	11
HostMin:	172.29.6.13	10101100.00011101.00000110.000011	01
HostMax:	172.29.6.14	10101100.00011101.00000110.000011	10

Medellín LAN (Clase B)

Tabla 32. Cálculo para la redes LAN de Medellín.

Address:	**172.29.4.0**	**10101100.00011101.00000100.0**	**0000000**
Netmask:	255.255.255.128=25	11111111.11111111.11111111.1	0000000
Wildcard:	0.0.0.127	00000000.00000000.00000000.0	1111111
Network:	172.29.4.0	10101100.00011101.00000100.0	0000000
Broadcast:	172.29.4.127	10101100.00011101.00000100.0	1111111
HostMin:	172.29.4.1	10101100.00011101.00000100.0	0000001
HostMax:	172.29.4.126	10101100.00011101.00000100.0	1111110
Address:	**172.29.4.128**	**10101100.00011101.00000100.1**	**0000000**
Netmask:	255.255.255.128=25	11111111.11111111.11111111.1	0000000
Wildcard:	0.0.0.127	00000000.00000000.00000000.0	1111111
Network:	172.29.4.128	10101100.00011101.00000100.1	0000000
Broadcast:	172.29.4.255	10101100.00011101.00000100.1	1111111
HostMin:	172.29.4.129	10101100.00011101.00000100.1	0000001
HostMax:	172.29.4.254	10101100.00011101.00000100.1	1111110

Bogotá Seriales (Clase B)

Tabla 33. Cálculo para la redes seriales de Bogotá.

Address:	**172.29.3.0**	**10101100.00011101.00000011.000000**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11

Network:	172.29.3.0	10101100.00011101.00000011.000000	00
Broadcast:	172.29.3.3	10101100.00011101.00000011.000000	11
HostMin:	172.29.3.1	10101100.00011101.00000011.000000	01
HostMax:	172.29.3.2	10101100.00011101.00000011.000000	10
Address:	**172.29.3.4**	**10101100.00011101.00000011.000001**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	172.29.3.4	10101100.00011101.00000011.000001	00
Broadcast:	172.29.3.7	10101100.00011101.00000011.000001	11
HostMin:	172.29.3.5	10101100.00011101.00000011.000001	01
HostMax:	172.29.3.6	10101100.00011101.00000011.000001	10
Address:	**172.29.3.8**	**10101100.00011101.00000011.000010**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	172.29.3.8	10101100.00011101.00000011.000010	00
Broadcast:	172.29.3.11	10101100.00011101.00000011.000010	11
HostMin:	172.29.3.9	10101100.00011101.00000011.000010	01
HostMax:	172.29.3.10	10101100.00011101.00000011.000010	10
Address:	**172.29.3.12**	**10101100.00011101.00000011.000011**	**00**
Netmask:	255.255.255.252=30	11111111.11111111.11111111.111111	00
Wildcard:	0.0.0.3	00000000.00000000.00000000.000000	11
Network:	172.29.3.12	10101100.00011101.00000011.000011	00
Broadcast:	172.29.3.15	10101100.00011101.00000011.000011	11
HostMin:	172.29.3.13	10101100.00011101.00000011.000011	01
HostMax:	172.29.3.14	10101100.00011101.00000011.000011	10

Bogotá LAN (Clase B)

Tabla 34. Cálculo para la redes LAN de Bogotá.

Address:	**172.29.0.0**	**10101100.00011101.00000000.**	**00000000**
Netmask:	255.255.255.0=24	11111111.11111111.11111111.	00000000
Wildcard:	0.0.0.255	00000000.00000000.00000000.	11111111
Network:	172.29.0.0	10101100.00011101.00000000.	00000000
Broadcast:	172.29.0.255	10101100.00011101.00000000.	11111111
HostMin:	172.29.0.1	10101100.00011101.00000000.	00000001
HostMax:	172.29.0.254	10101100.00011101.00000000.	11111110
Address:	**172.29.1.0**	**10101100.00011101.00000001.**	**00000000**
Netmask:	255.255.255.0=24	11111111.11111111.11111111.	00000000
Wildcard:	0.0.0.255	00000000.00000000.00000000.	11111111
Network:	172.29.1.0	10101100.00011101.00000001.	00000000
Broadcast:	172.29.1.255	10101100.00011101.00000001.	11111111
HostMin:	172.29.1.1	10101100.00011101.00000001.	00000001

HostMax:	172.29.1.254	10101100.00011101.00000001. 11111110

Luego de calcular cada red correspondiente antes de empezar con la parte 1; se realiza la configuración de cada router para Bogotá, Medellín e ISP con su respectivas direcciones IP de acuerdo con la topología dada.

ISP

```
ISP>en
Password:
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/0
ISP(config-if)#description S00ISP connection to S010Med1
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#exit
ISP(config)#int s0/0/1
ISP(config-if)#description S001ISP connection to S000Bog1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#end
```

Medellín 1

```
Medellin1>en
Password:
Medellin1#en
Medellin1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#int s0/1/0
Medellin1(config-if)#description S010Med1 connection to S000ISP
Medellin1(config-if)#ip add 209.17.220.2 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shut
Medellin1(config-if)#exit
Medellin1(config)#int s0/0/0
Medellin1(config-if)#description S000Med1 connection to S001Med2
Medellin1(config-if)#ip add 172.29.6.1 255.255.255.252
Medellin1(config-if)#no shut
Medellin1(config-if)#exit
Medellin1(config)#int s0/0/1
Medellin1(config-if)#description S001Med1 connection to S001Med2
Medellin1(config-if)#ip add 172.29.6.9 255.255.255.252
```

```
Medellin1(config-if)#no shut
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/1
Medellin1(config-if)#description S011Med1 connection to S010Med3
Medellin1(config-if)#ip add 172.29.6.13 255.255.255.252
Medellin1(config-if)#no shut
Medellin1(config-if)#end
```

Medellín 2

```
Medellin2>en
Password:
Medellin2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#int s0/0/1
Medellin2(config-if)#description S001Med2 connection to S00Med1
Medellin2(config-if)#ip add 172.29.6.2 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shut
Medellin2(config-if)#exit
Medellin2(config)#int s0/0/0
Medellin2(config-if)#description S000Med2 connection to S000Med3
Medellin2(config-if)#ip add 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shut
Medellin2(config-if)#exit
Medellin2(config)#int g0/0
Medellin2(config-if)#description G00Med2 connection to FA0PC50HOST
Medellin2(config-if)#ip add 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shut
Medellin2(config-if)#end
```

Medellín 3

```
Medellin3>en
Password:
Medellin3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#int s0/0/0
Medellin3(config-if)#description S000Med3 connection to S000Med2
Medellin3(config-if)#ip add 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shut
Medellin3(config-if)#exit
Medellin3(config)#int s0/0/1
Medellin3(config-if)#description S001Med3 connection to S001Med1
```

```
Medellin3(config-if)#ip add 172.29.6.10 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shut
Medellin3(config-if)#exit
Medellin3(config)#int s0/1/0
Medellin3(config-if)#description S010Med3 connection to S011Med1
Medellin3(config-if)#ip add 172.29.6.14 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shut
Medellin3(config-if)#exit
Medellin3(config)#int g0/0
Medellin3(config-if)#description G00Med3 connection to FA0PC40HOST
Medellin3(config-if)#ip add 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shut
Medellin3(config-if)#end
```

Bogotá 1

```
Bogota1>en
Password:
Bogota1#en
Bogota1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#int s0/0/0
Bogota1(config-if)#description S000Bog1 connection to S001ISP
Bogota1(config-if)#ip add 209.17.220.6 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shut
Bogota1(config-if)#exit
Bogota1(config)#int s0/0/1
Bogota1(config-if)#description S001Bog1 connection to S001Bog3
Bogota1(config-if)#ip add 172.29.3.5 255.255.255.252
Bogota1(config-if)#no shut
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/0
Bogota1(config-if)#description S010Bog1 connection to S010Bog3
Bogota1(config-if)#ip add 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shut
Bogota1(config-if)#int s0/1/1
Bogota1(config-if)#description S011Bog1 connection to S001Bog2
Bogota1(config-if)#ip add 172.29.3.9 255.255.255.252
Bogota1(config-if)#no shut
Bogota1(config-if)#end
```

Bogotá 2

```
Bogota2>en
Password:
Bogota2#en
Bogota2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#int s0/0/0
Bogota2(config-if)#description S000Bog2 connection to S000Bog3
Bogota2(config-if)#ip add 172.29.3.13 255.255.255.252
Bogota2(config-if)#no shut
Bogota2(config-if)#exit
Bogota2(config)#int s0/0/1
Bogota2(config-if)#description S001Bog1 connection to S001Bog1
Bogota2(config-if)#ip add 172.29.3.10 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shut
Bogota2(config-if)#exit
Bogota2(config)#int g0/0
Bogota2(config-if)#description G00Bog2 connection to F00PC200HOST
Bogota2(config-if)#ip add 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shut
Bogota2(config-if)#end
```

Bogotá 3

```
Bogota3>en
Password:
Bogota3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#int s0/0/0
Bogota3(config-if)#description S000Bog3 connection to S000Bog2
Bogota3(config-if)#ip add 172.29.3.14 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shut
Bogota3(config-if)#exit
Bogota3(config)#int s0/0/1
Bogota3(config-if)#description S001Bog3 connection to S001Bog1
Bogota3(config-if)#ip add 172.29.3.6 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shut
Bogota3(config-if)#exit
Bogota3(config)#int s0/1/0
Bogota3(config-if)#description S010Bog3 connection to S010Bog1
Bogota3(config-if)#ip add 172.29.3.2 255.255.255.252
```

```
Bogota3(config-if)#no shut
Bogota3(config-if)#exit
Bogota3(config)#int g0/0
Bogota3(config-if)#description G00Bog3 connection to FA0PC150HOST
Bogota3(config-if)#ip add 172.29.0.1 255.255.255.0
Bogota3(config-if)#no shut
Bogota3(config-if)#end
```

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.

Por ser OSPF no requeire desactivar sumarizacion automática; ya que este no realiza sumarización, OSPF utiliza otro medio como ABR que es para sumarizacion y por lo tanto se requiere configurar manualmente, asi se quisiera implementar el router utilizado no reconoce el comando por lo tanto la desactivación de sumarización automática en OSPF para este caso se omite.

Para declarar la red principal se require realizar la sumarización de las redes principales de Bogotá y Medellín, asi como se muestra en la siguiente tabla:

Tabla 35. Sumarización para hallar la red principal.

Red principal	Red	Binario
Bogotá	172.29.0.0	1010 1100. 0001 1101. 0000 0000. 0000 0000
Medellín	172.29.4.0	1010 1100. 0001 1101. 0000 0100. 0000 0000
New Network		
Red	172.29.0.0	1010 1100. 0001 1101. 0000 0000. 0000 0000
/21	255.255.248.0	1111 1111. 1111 1111. 1111 1000. 0000 0000
Wildcard	0.0.7.255	0000 0000. 0000 0000. 0000 0111. 1111 1111

Luego de hallar la red principal se procede a realizar la configuración en los dispositivos de red declarando la red principal junto con la Wildcard teniendo en cuenta cada red establecida y el cálculo previo realizado al comienzo para establecer OSPF en área 0.

Bogotá 1

```
Bogota1>en
Password:
Bogota1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#router ospf 1
```

```
Bogota1(config-router)#do show ip route connected
 C 172.29.3.0/30 is directly connected, Serial0/1/0
 C 172.29.3.4/30 is directly connected, Serial0/0/1
 C 172.29.3.8/30 is directly connected, Serial0/1/1
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.0.0 0.0.7.255 area 0
Bogota1(config-router)#default-information originate
Bogota1(config-router)#end
```

Bogotá 2

```
Bogota2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#router ospf 1
Bogota2(config-router)#do show ip route connected
 C   172.29.1.0/24 is directly connected, GigabitEthernet0/0
 C   172.29.3.8/30 is directly connected, Serial0/0/1
 C   172.29.3.12/30 is directly connected, Serial0/0/0
Bogota2(config-router)#network 172.29.1.0 0.0.0.255 area 0
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.0.0 0.0.7.255 area 0
Bogota2(config-router)#default-information originate
```

Bogotá 3

```
Bogota3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#router ospf 1
Bogota3(config-router)#do show ip route connected
 C   172.29.0.0/24 is directly connected, GigabitEthernet0/0
 C   172.29.3.0/30 is directly connected, Serial0/1/0
 C   172.29.3.4/30 is directly connected, Serial0/0/1
 C   172.29.3.12/30 is directly connected, Serial0/0/0
Bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.0.0 0.0.7.255 area 0
Bogota3(config-router)#default-information originate
```

Medellín 1

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#do show ip route connected
 C   172.29.6.0/30 is directly connected, Serial0/0/0
 C   172.29.6.8/30 is directly connected, Serial0/0/1
 C   172.29.6.12/30 is directly connected, Serial0/1/1
 C   209.17.220.0/30 is directly connected, Serial0/1/0
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.0.0 0.0.7.255 area 0
Medellin1(config-router)#default-information originate
```

Medellín 2

```
Medellin2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#router ospf 1
Medellin2(config-router)#do show ip route connected
 C   172.29.4.0/25 is directly connected, GigabitEthernet0/0
 C   172.29.6.0/30 is directly connected, Serial0/0/1
 C   172.29.6.4/30 is directly connected, Serial0/0/0
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#network 172.29.0.0 0.0.7.255 area 0
Medellin2(config-router)#default-information originate
Medellin2(config-router)#end
```

Medellín 3

```
Medellin3>en
Password:
Medellin3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#router ospf 1
Medellin3(config-router)#do show ip route connected
 C   172.29.4.128/25 is directly connected, GigabitEthernet0/0
 C   172.29.6.4/30 is directly connected, Serial0/0/0
 C   172.29.6.8/30 is directly connected, Serial0/0/1
 C   172.29.6.12/30 is directly connected, Serial0/1/0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
```

```
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin3(config-router)#network 172.29.0.0 0.0.7.255 area 0
Medellin3(config-router)#default-information originate
Medellin3(config-router)#end
```

b. Los routers Bogotá 1 y Medellín 1 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.

Se establece la ruta por defecto en Bogotá y Medellín hacia una IP pública ISP, para redistribuir la informacion entre los routers adyacentes al protocolo OSPF se establece el comando default-information originate asi el router actualiza el mapeo de rutas estableciendo la nueva configuración.

Bogotá 1

```
Bogota1#config 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)#router ospf 1
Bogota1(config-router)#default-information originate
```

Medellín 1

```
Medellin1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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
```

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.

Se organiza la infomación de acuerdo con los datos que nos da la topología:

Cidr: /22
Clase: B
Subnet Mask: 255.255.252.0

Tabla 36. Sumarización de redes internas para ruta estática de ISP.

Network Bogotá	Binario
172.29.0.0	1010 1100. 0001 1101. 0000 0000. 0000 0000
172.29.1.0	1010 1100. 0001 1101. 0000 0001. 0000 0000

172.29.3.0	1010 1100. 0001 1101. 0000 0011. 0000 0000
172.29.3.4	1010 1100. 0001 1101. 0000 0011. 0000 0100
172.29.3.8	1010 1100. 0001 1101. 0000 0011. 0000 1000
172.29.3.12	1010 1100. 0001 1101. 0000 0011. 0000 1100
Network ISP	
172.29.0.0	1010 1100. 0001 1101. 0000 0000. 0000 0000
255.255.252.0	1111 1111. 1111 1111. 1111 1100. 0000 0000
Network Medellín	
172.29.4.0	1010 1100. 0001 1101. 0000 0100. 0000 0000
172.29.4.128	1010 1100. 0001 1101. 0000 0100. 1000 0000
172.29.6.0	1010 1100. 0001 1101. 0000 0110. 0000 0000
172.29.6.4	1010 1100. 0001 1101. 0000 0110. 0000 0100
172.29.6.8	1010 1100. 0001 1101. 0000 0110. 0000 1000
172.29.6.12	1010 1100. 0001 1101. 0000 0110. 0000 1100
Network ISP	
172.29.4.0	1010 1100. 0001 1101. 0000 0100. 0000 0000
255.255.252.0	1111 1111. 1111 1111. 1111 1111. 1111 1000

Se establece la configuración de ruta estática por defecto de ISP mediante OSPF hacia las redes internas de Bogotá y Medellín.

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
ISP(config)#router ospf 1
ISP(config-router)#default-information originate
ISP(config-router)#exit
```

Parte 2: Tabla de Enrutamiento.

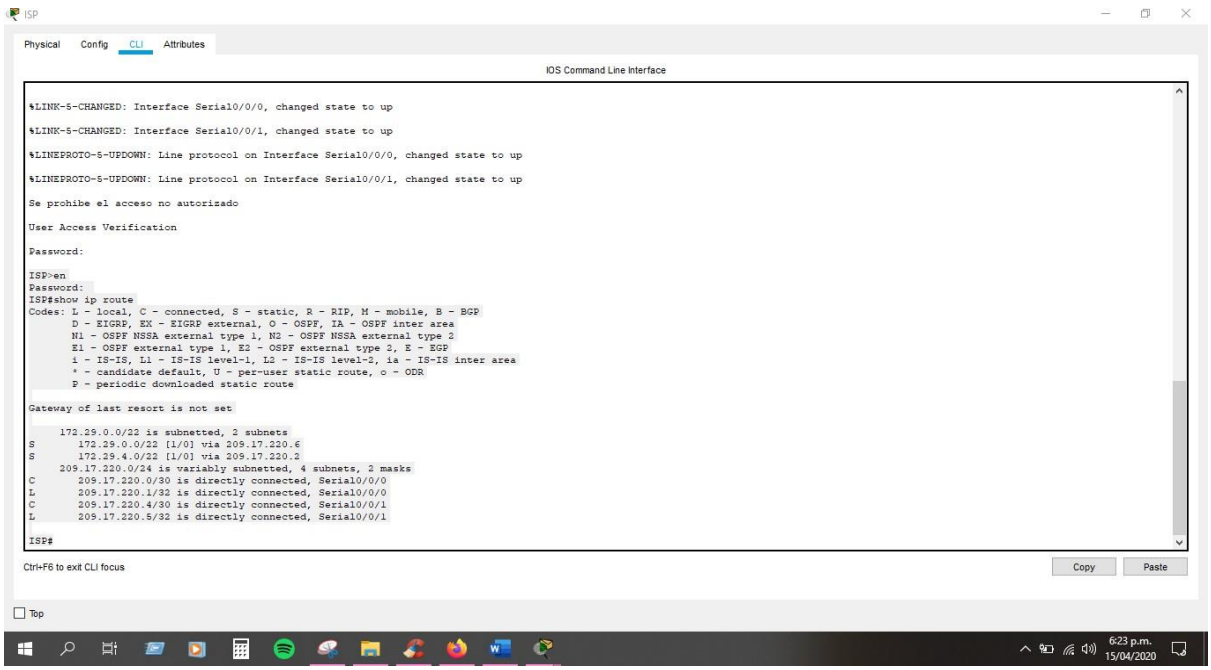
a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Para verificar se implementa el siguiente comando:

ISP

```
ISP#show ip route
```

Figura 26. Verificación de Redes y rutas Router ISP.



Bogotá

Bogota#show ip route

Figura 27. Verificación de Redes y rutas Router Bogotá 1.

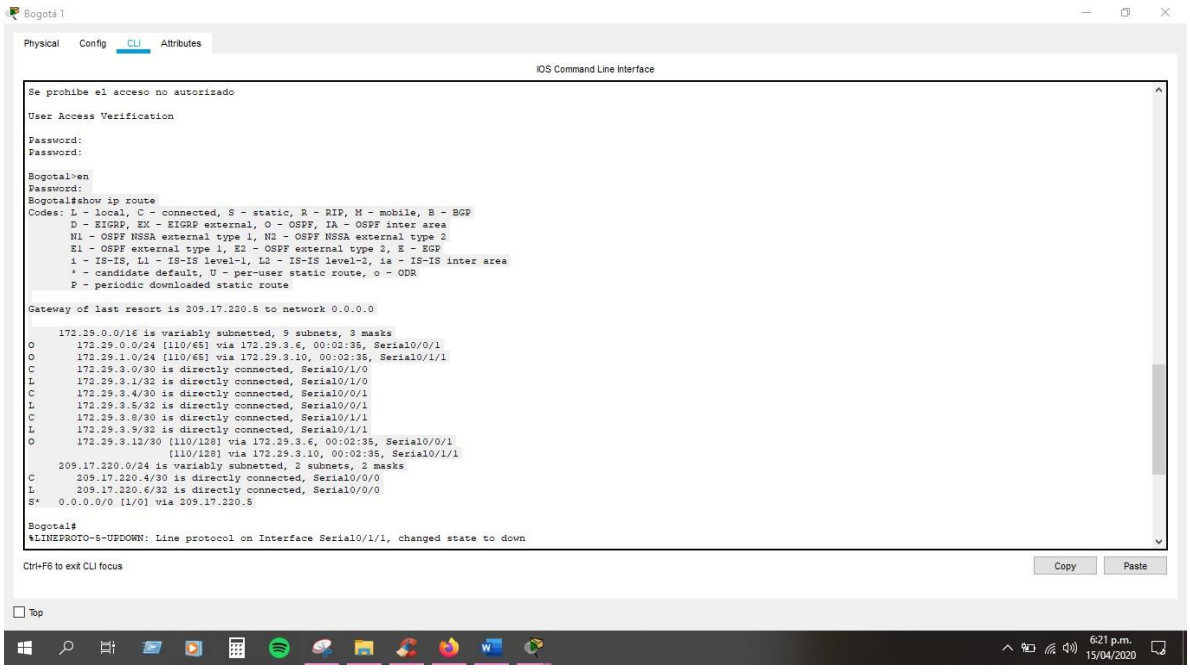


Figura 28. Verificación de Redes y rutas Router Bogotá 2.

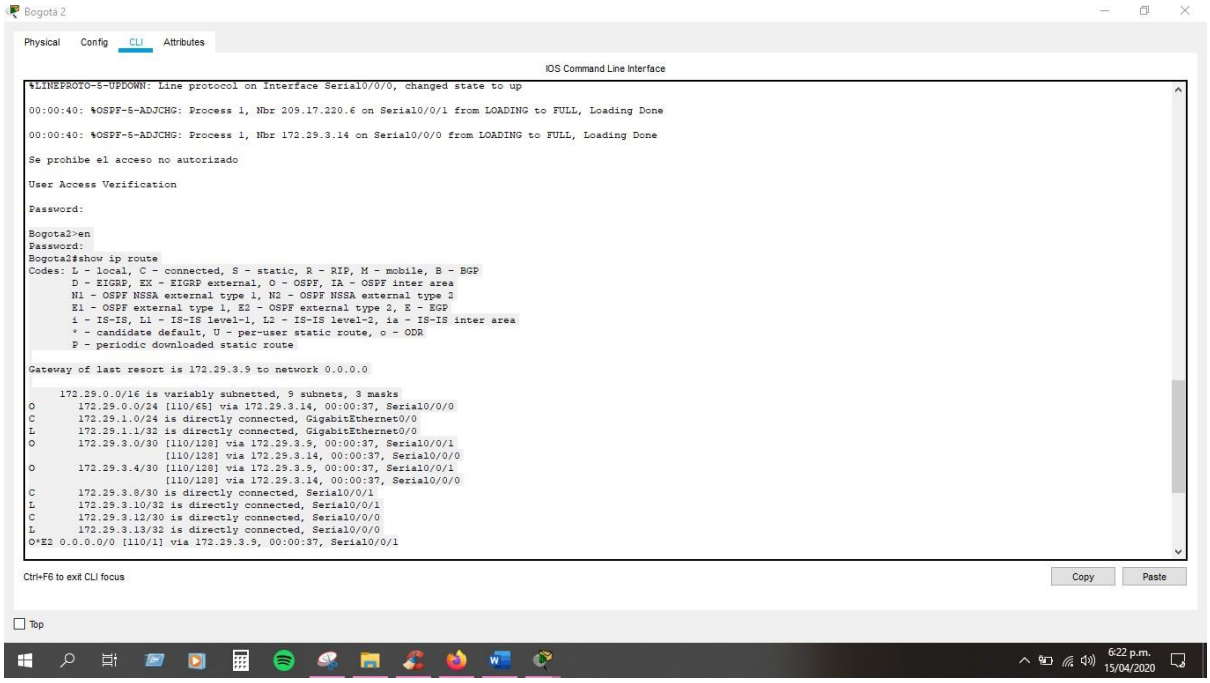
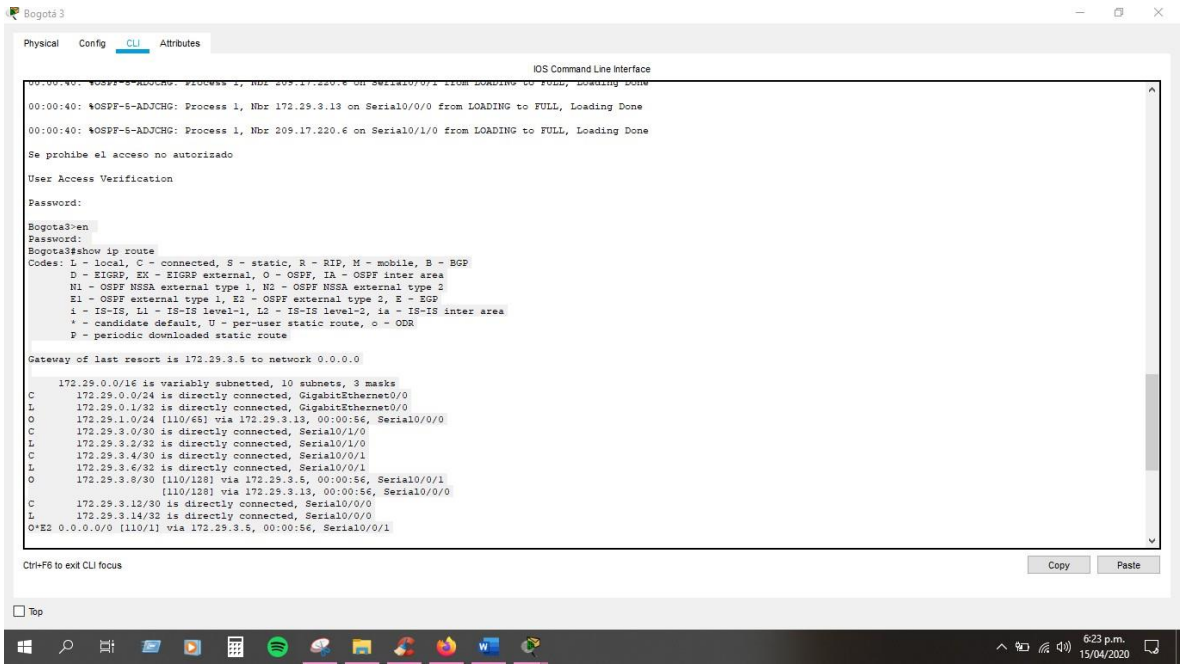


Figura 29. Verificación de Redes y rutas Router Bogotá 3.



Medellín

Medellin#show ip route

Figura 30. Verificación de Redes y rutas Router Medellín 1.

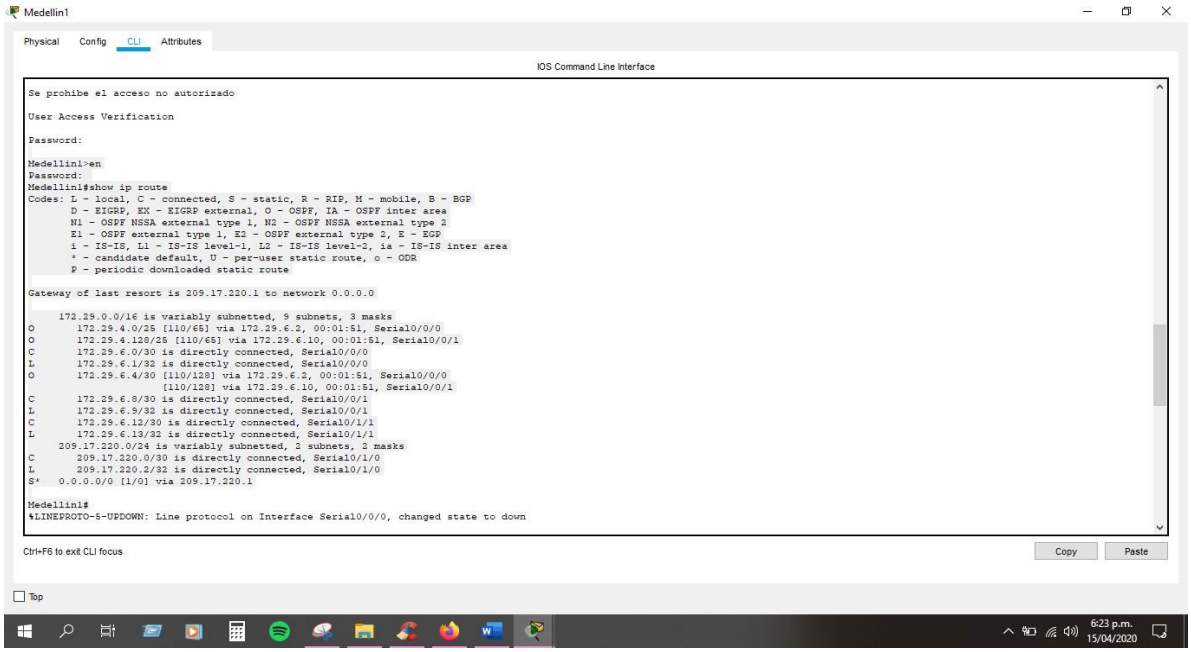


Figura 31. Verificación de Redes y rutas Router Medellín 2.

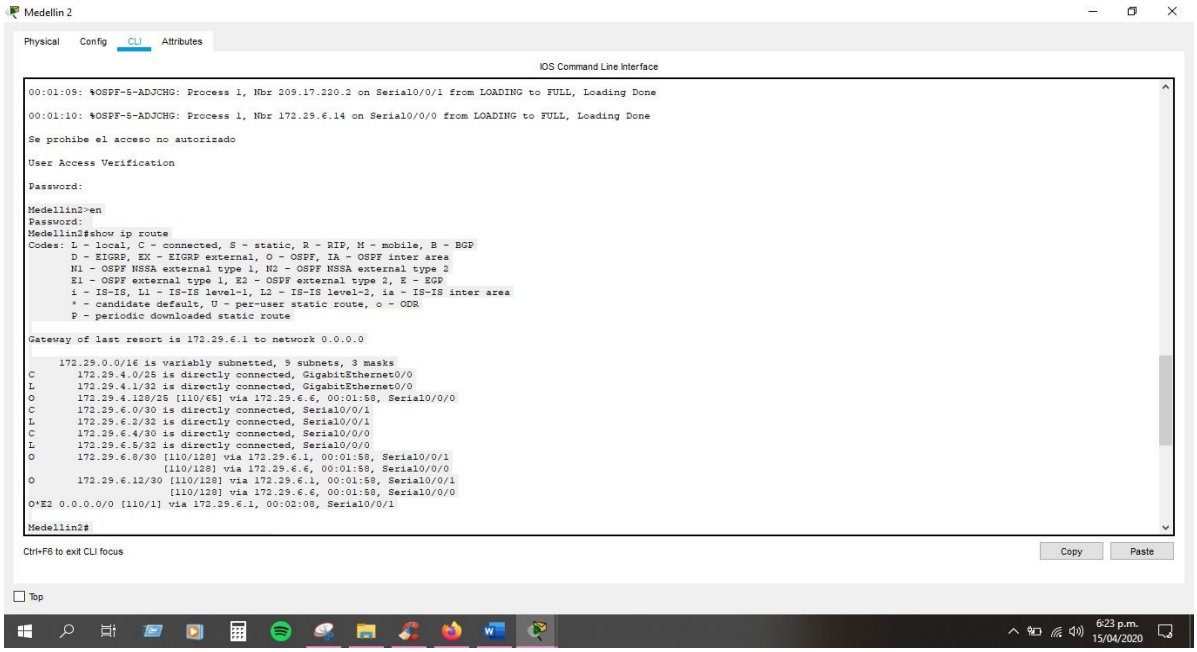
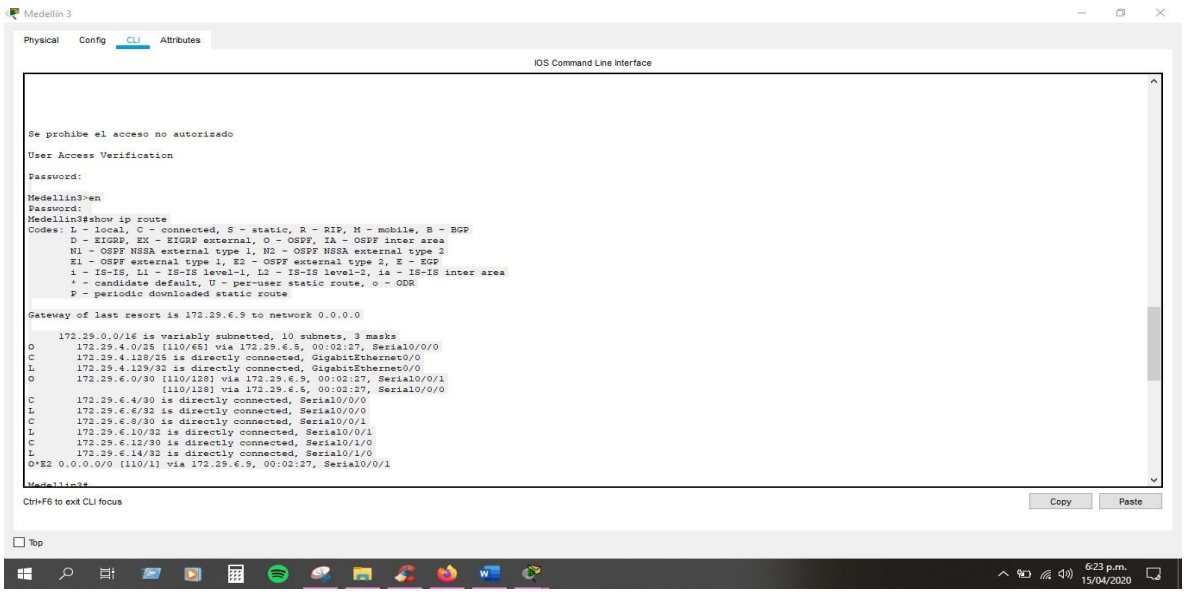


Figura 32. Verificación de Redes y rutas Router Medellín 3.



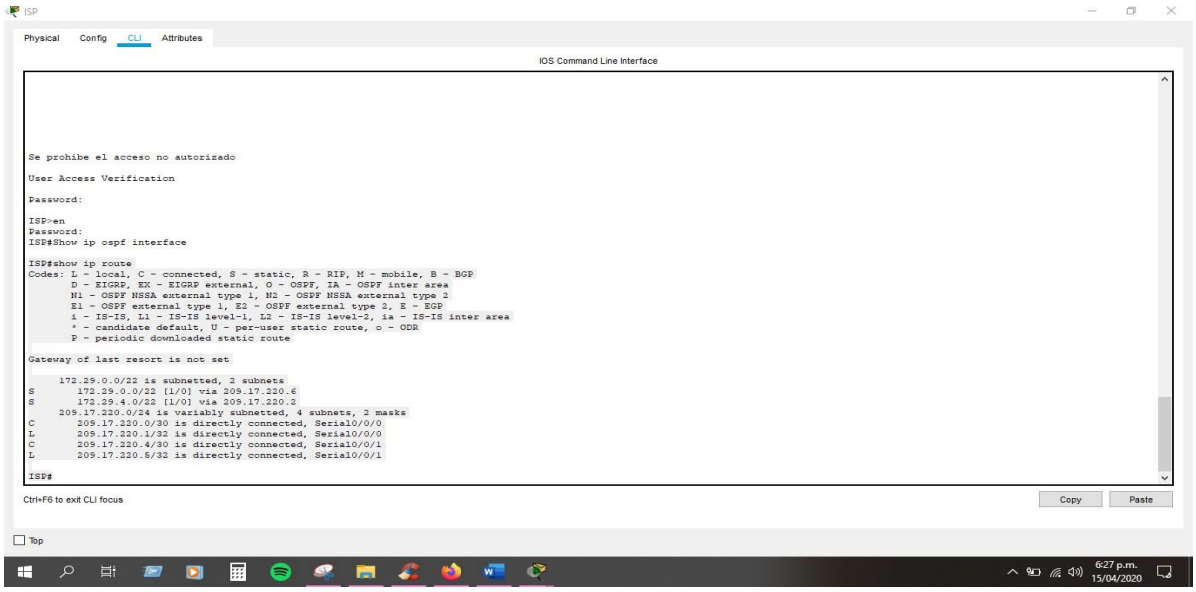
b. Verificar el balanceo de carga que presentan los Routers.

Para verificar se implementa el siguiente comando en los Routers:

ISP

ISP#Show ip route

Figura 33. Verificación balanceo de carga del Router ISP.



Bogotá

Bogota#Show ip route

Figura 34. Verificación balanceo de carga del Router Bogotá 1.

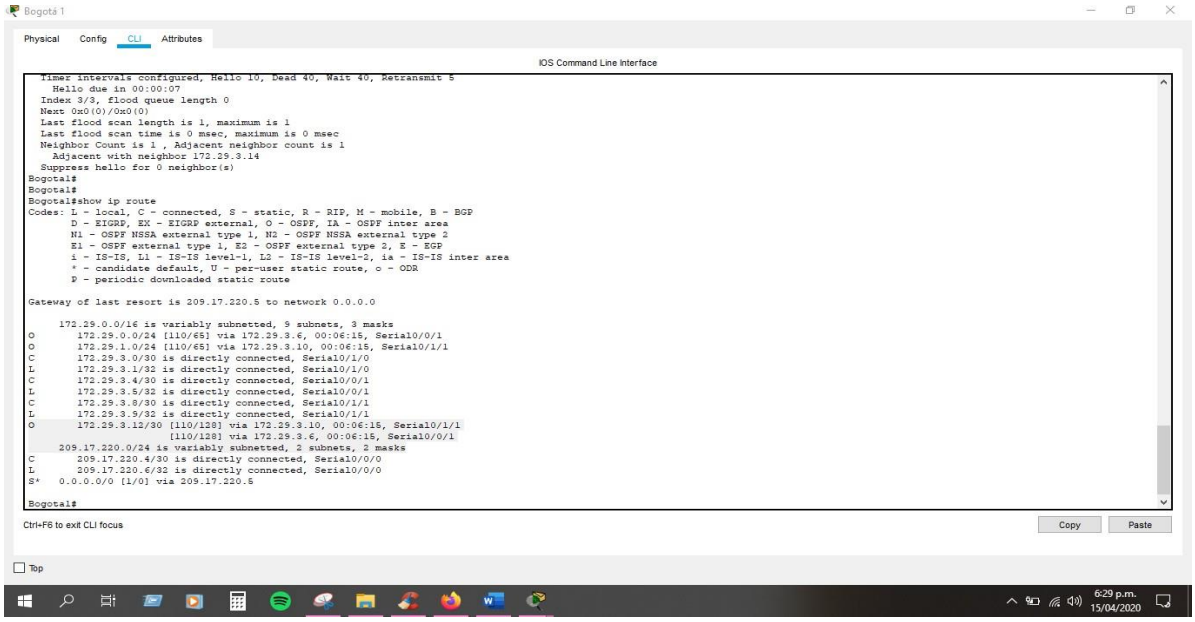


Figura 35. Verificación balanceo de carga del Router Bogotá 2.

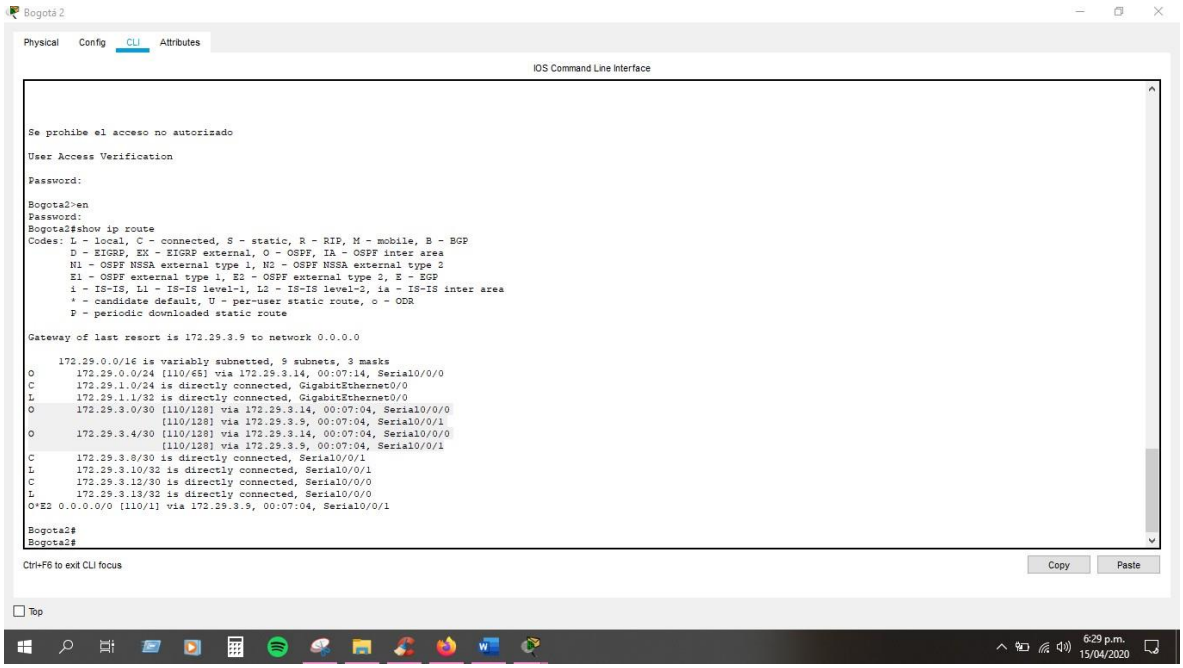
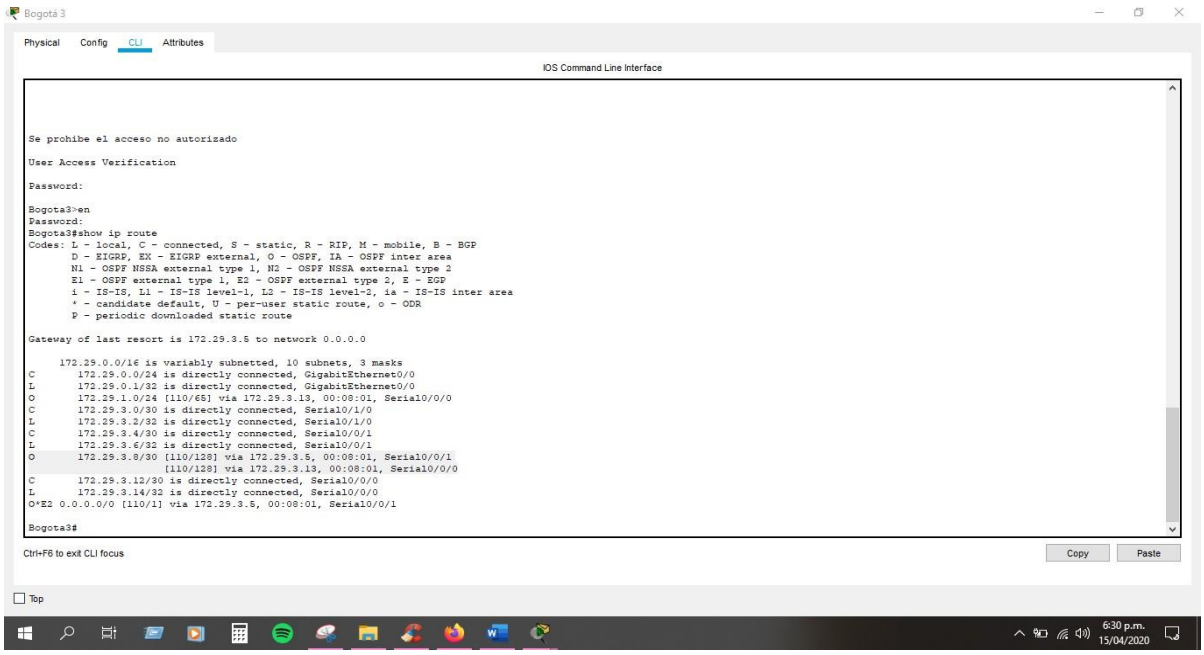


Figura 36. Verificación balanceo de carga del Router Bogotá 3.



Medellín

Medellin#Show ip route

Figura 37. Verificación balanceo de carga del Router Medellín 1.

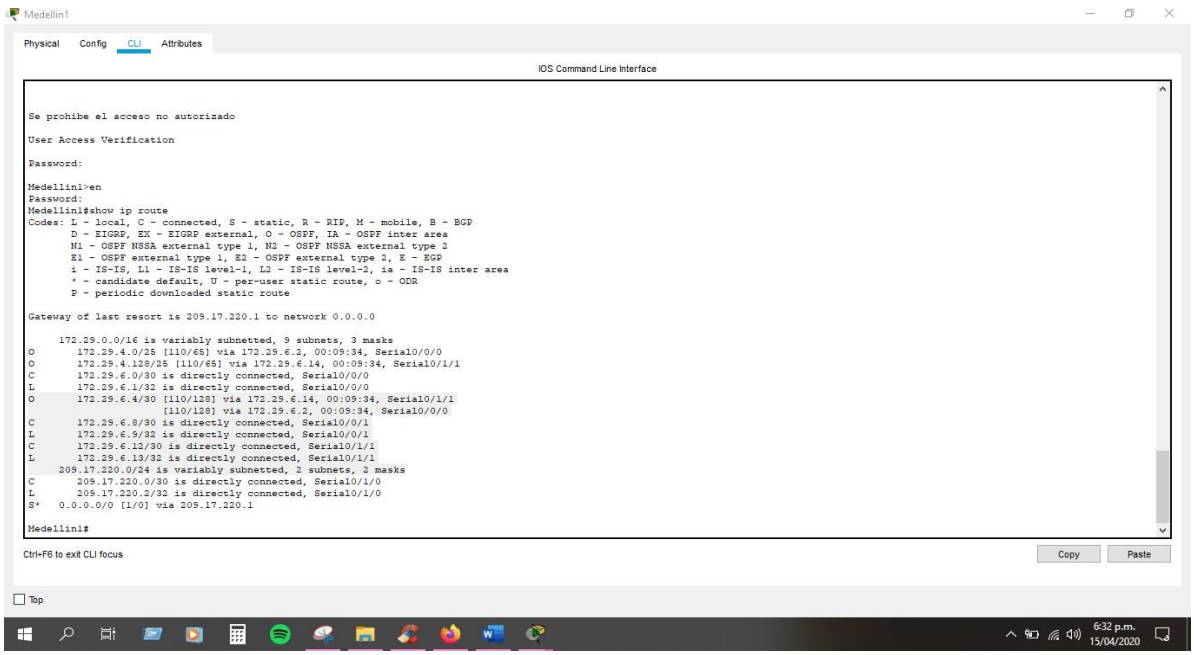


Figura 38. Verificación balanceo de carga del Router Medellín 2.

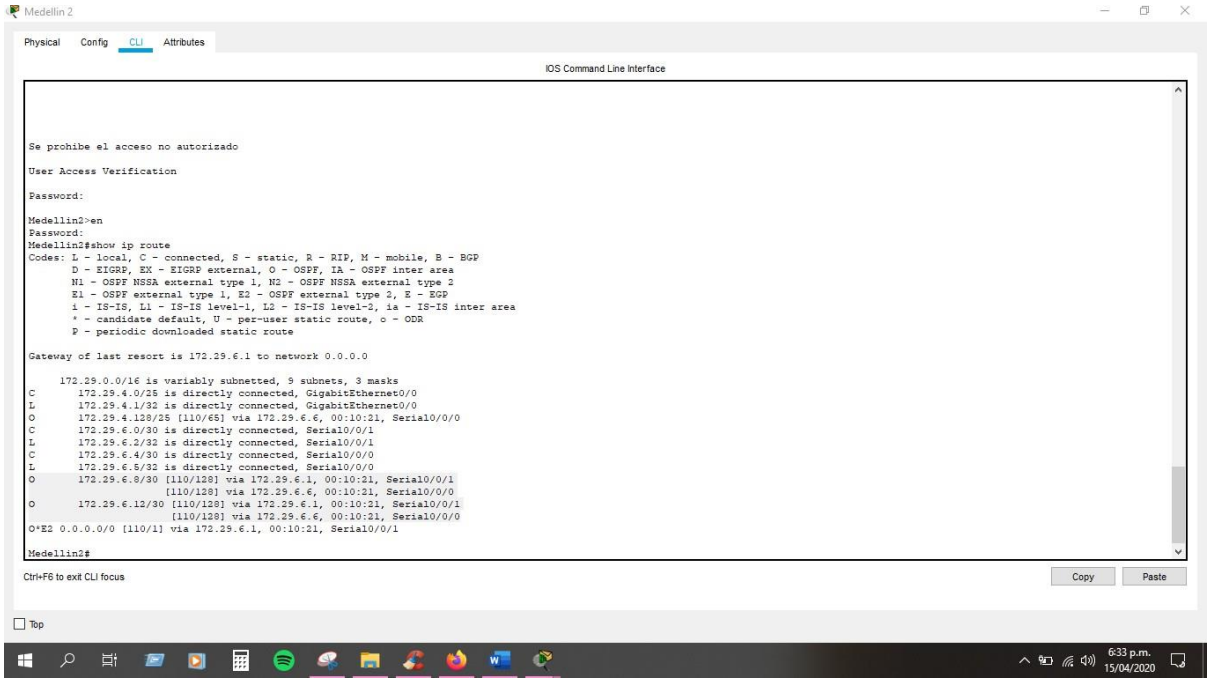
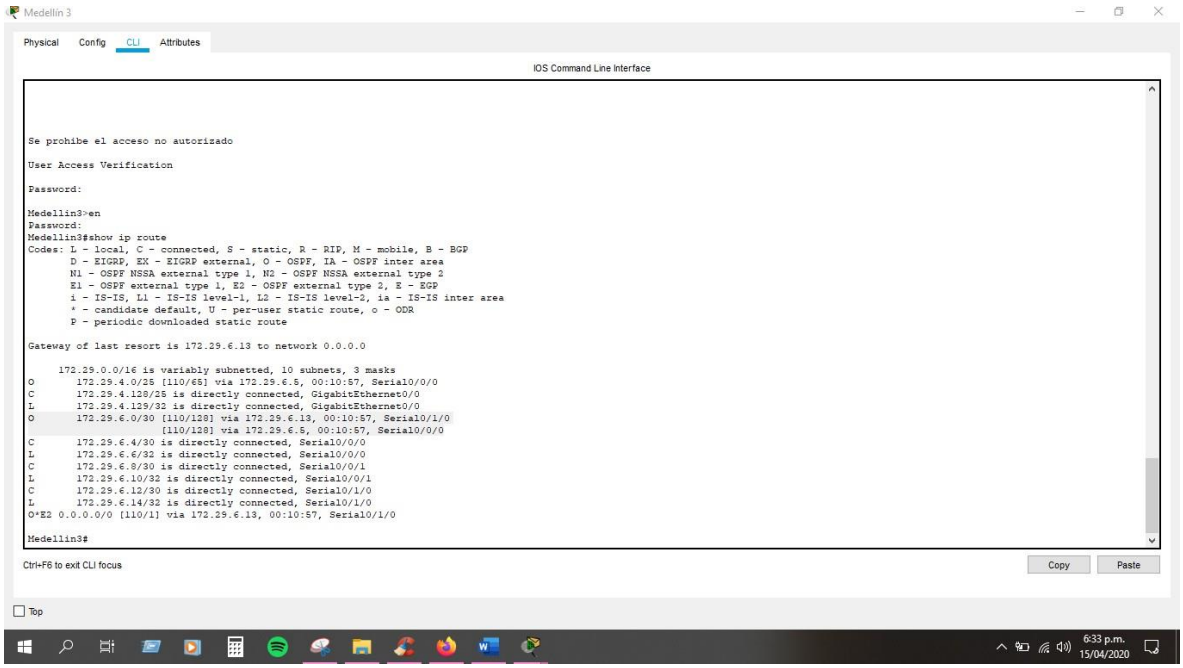


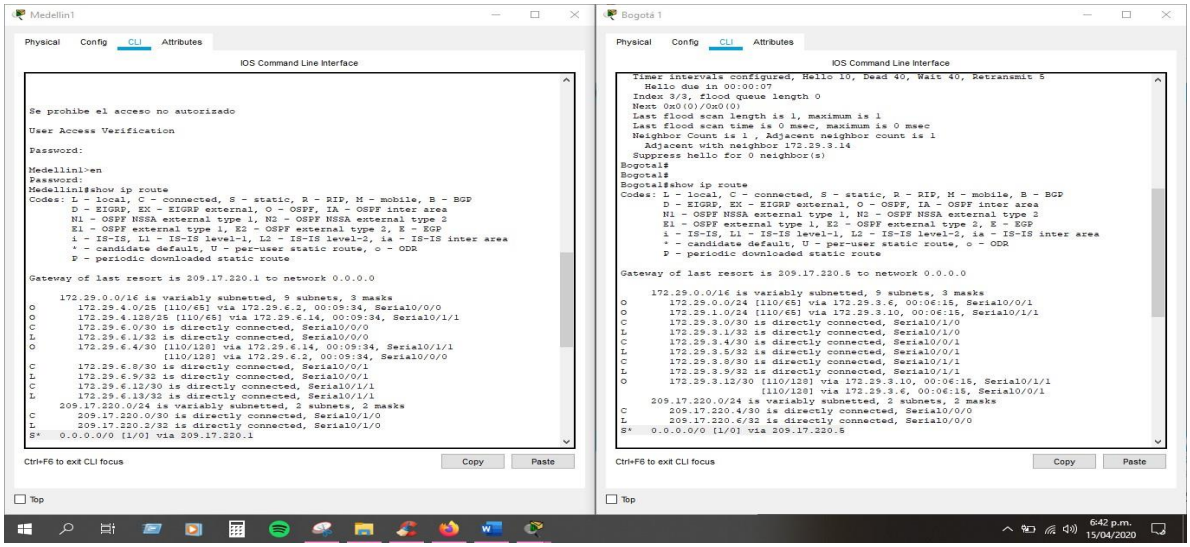
Figura 39. Verificación balanceo de carga del Router Medellín 3.



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.

Para verificar se emite el siguiente comando show ip route en los Routers.

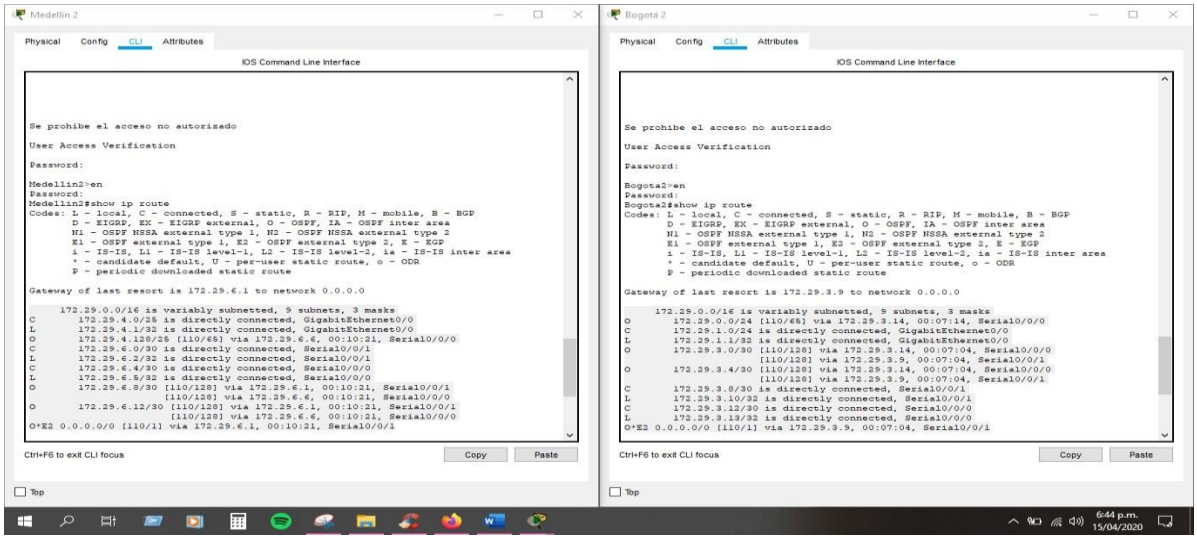
Figura 40. Verificación de rutas para Bogotá 1 y Medellín 1.



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

Para verificar se emite el siguiente comando show ip route en los Routers.

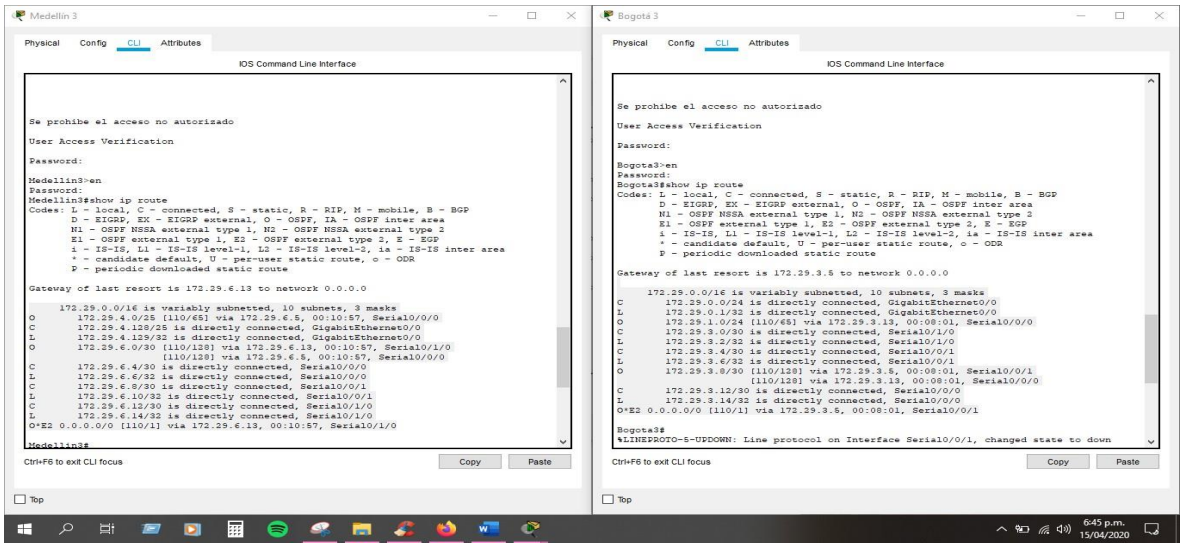
Figura 41. Verificación de rutas para Bogotá 2 y Medellín 2.



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

Para verificar se emite el siguiente comando show ip route en los Routers.

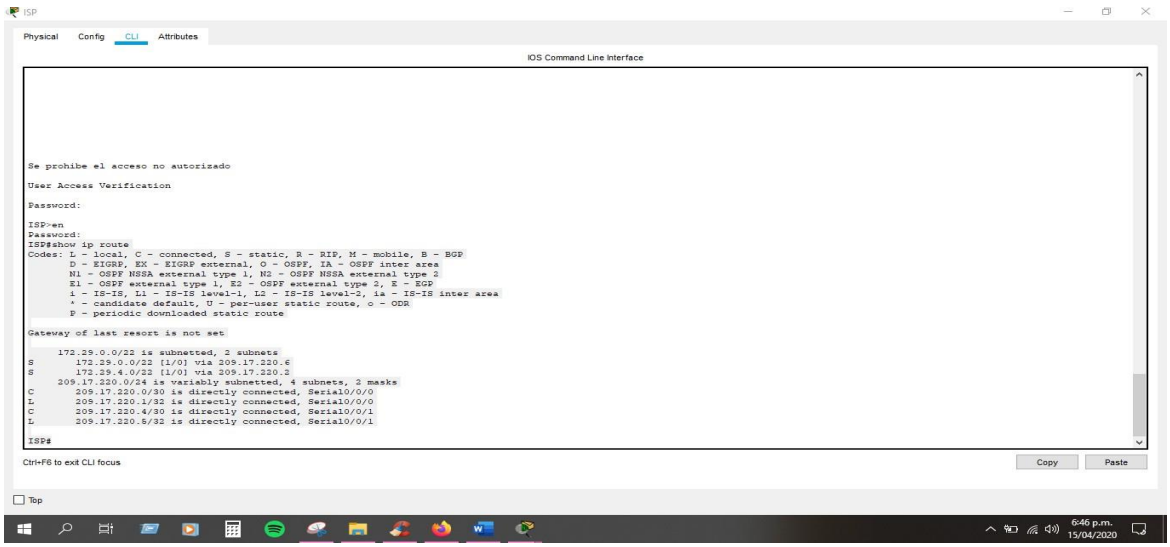
Figura 42. Verificación de rutas para Bogotá 3 y Medellín 3.



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

Para verificar se emite el siguiente comando show ip route en el Router.

Figura 43. Verificación de rutas para ISP.



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 37. Interfaces que no requieren desactivación en OSPF.

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

Teniendo en cuenta la tabla, se configura las interfaces a pasivas desactivando seriales que no presentan alguna conexión física, así como las interfaces de Gigabit Ethernet que traen los Routers por defecto, para las redes de Bogotá y Medellín.

Bogotá 1

```
Bogota1(config)#router ospf 1
Bogota1(config-router)#passive-interface serial0/0/0
Bogota1(config-router)#passive-interface gigabitethernet 0/0
Bogota1(config-router)#passive-interface gigabitethernet 0/1
Bogota1(config-router)#default-information originate
```

Bogotá 2

```
Bogota2(config)#router ospf 1
Bogota2(config-router)#passive-interface gigabitethernet 0/1
Bogota2(config-router)#passive-interface gigabitethernet 0/0
Bogota2(config-router)#passive-interface serial0/1/0
Bogota2(config-router)#passive-interface serial0/1/1
Bogota2(config-router)#default-information originate
```

Bogotá 3

```
Bogota3(config)#router ospf 1
Bogota3(config-router)#passive-interface gigabitethernet 0/1
Bogota3(config-router)#passive-interface gigabitethernet 0/0
Bogota3(config-router)#passive-interface serial0/1/1
```

Bogota3(config-router)#default-information originate

Medellín 1

Medellin1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#router ospf 1
Medellin1(config-router)#passive-interface gigabitethernet 0/0
Medellin1(config-router)#passive-interface gigabitethernet 0/1
Medellin1(config-router)#passive-interface serial0/1/0
Medellin1(config-router)#default-information originate

Medellín 2

Medellin2(config)#router ospf 1
Medellin2(config-router)#passive-interface gigabitethernet 0/1
Medellin2(config-router)#passive-interface gigabitethernet 0/0
Medellin2(config-router)#default-information originate

Medellín 3

Medellin3(config)#router ospf 1
Medellin3(config-router)#passive-interface gigabitethernet 0/1
Medellin3(config-router)#passive-interface gigabitethernet 0/0
Medellin3(config-router)#passive-interface serial0/1/1
Medellin3(config-router)#default-information originate

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.

Para verificar se emite el siguiente comando show ip protocols en los Routers.

Bogotá

show ip protocols

Figura 44. Verificación del protocolo OSPF en Bogotá 1.

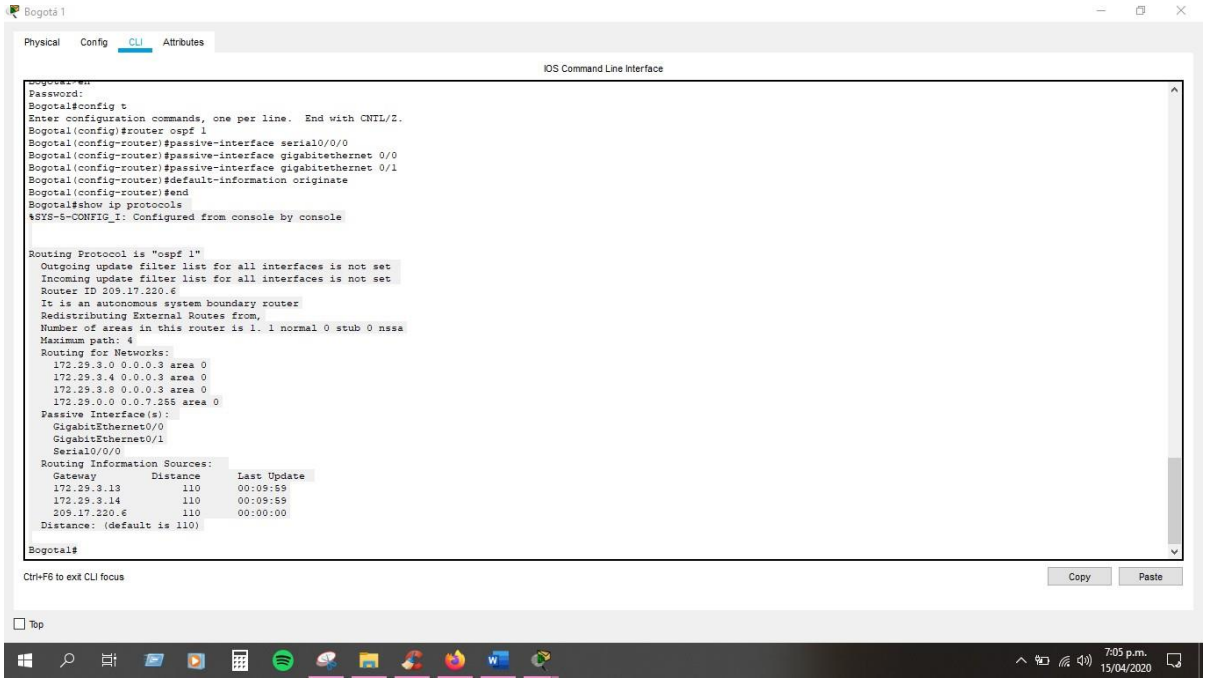


Figura 45. Verificación del protocolo OSPF en Bogotá 2.

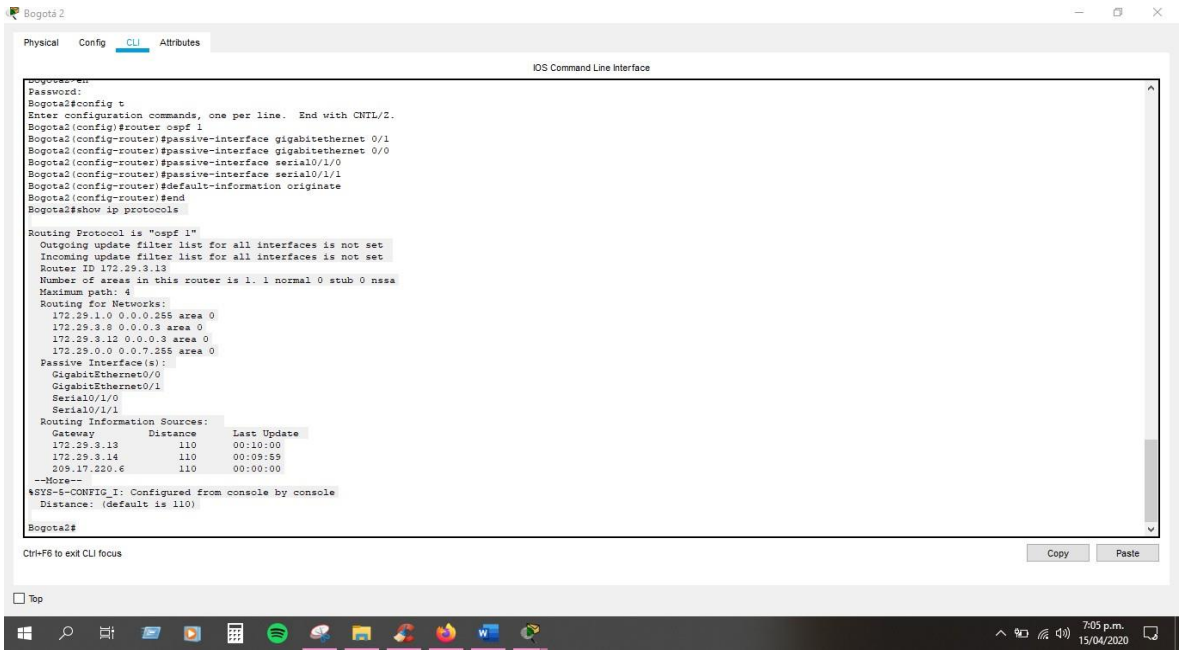
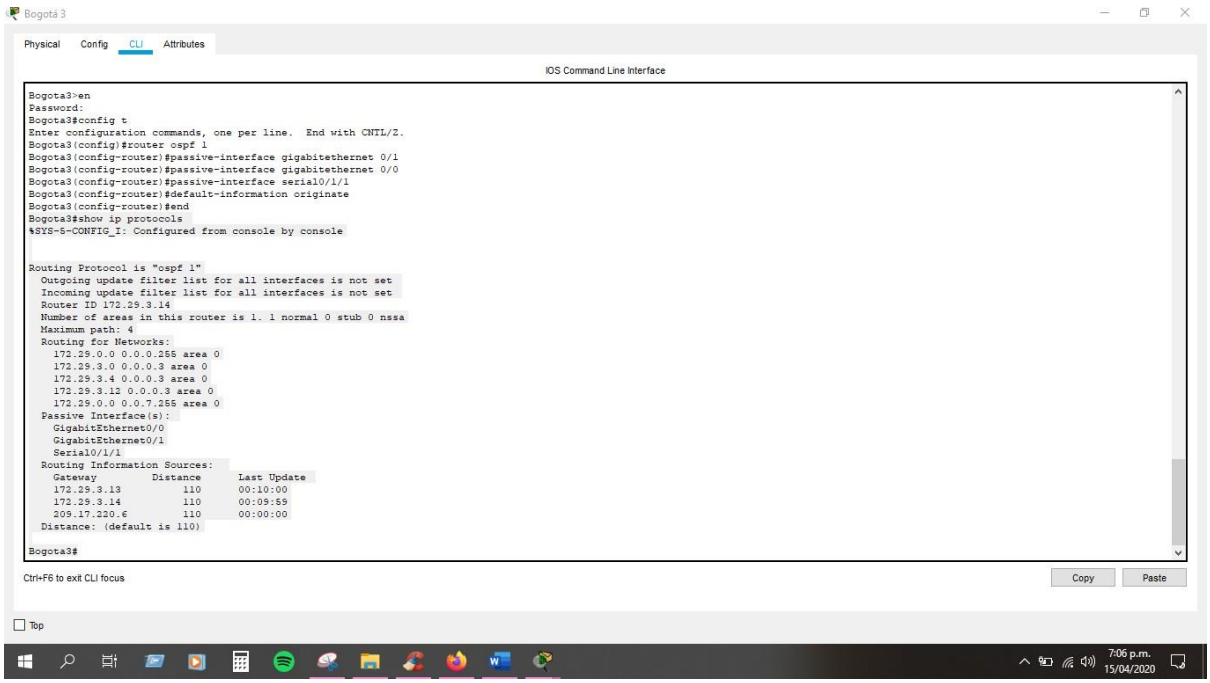


Figura 46. Verificación del protocolo OSPF en Bogotá 3.



Medellín

Figura 47. Verificación del protocolo OSPF en Medellín 1.

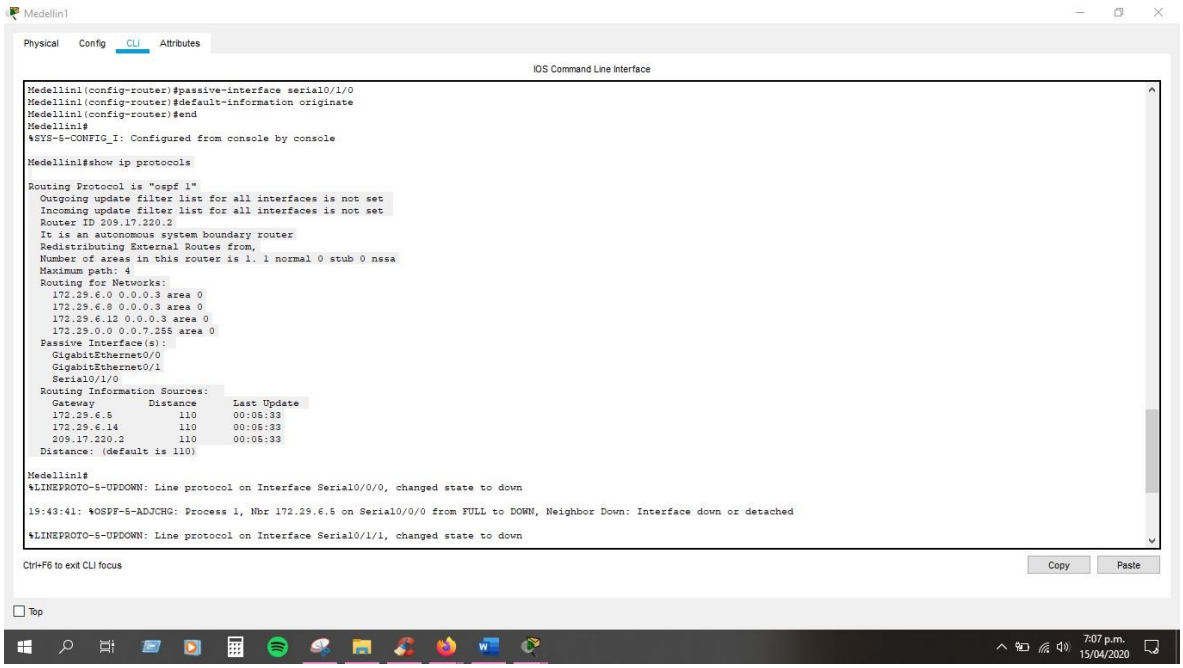


Figura 48. Verificación del protocolo OSPF en Medellín 2.

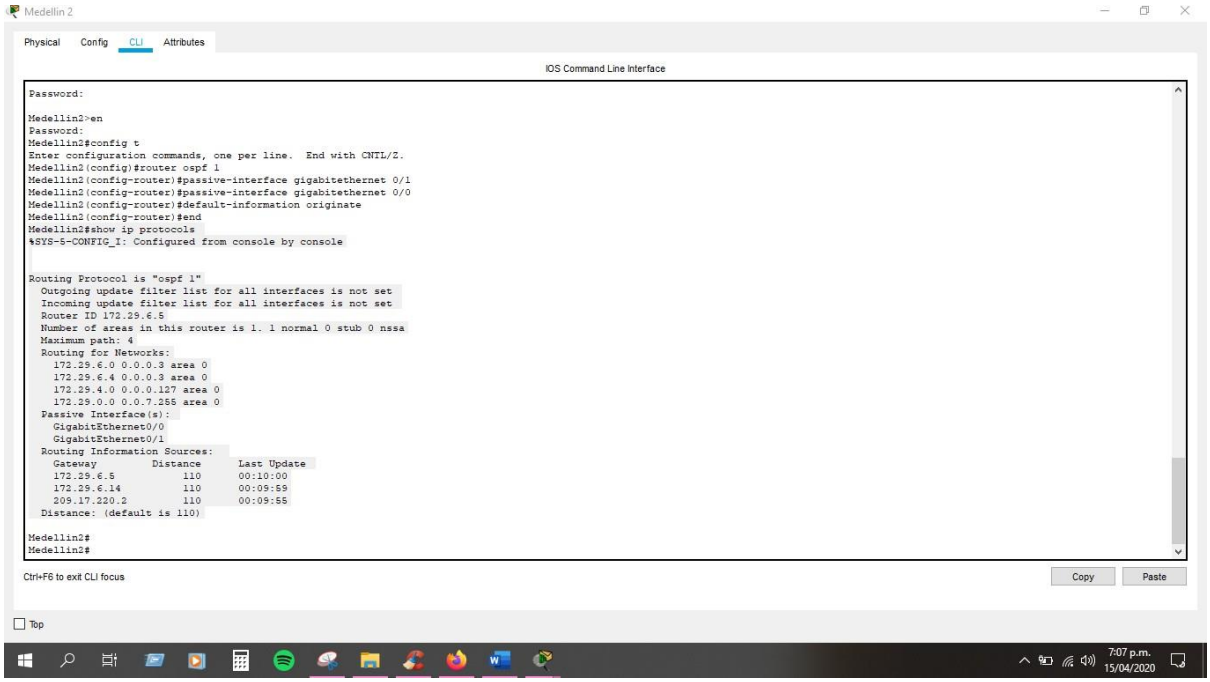
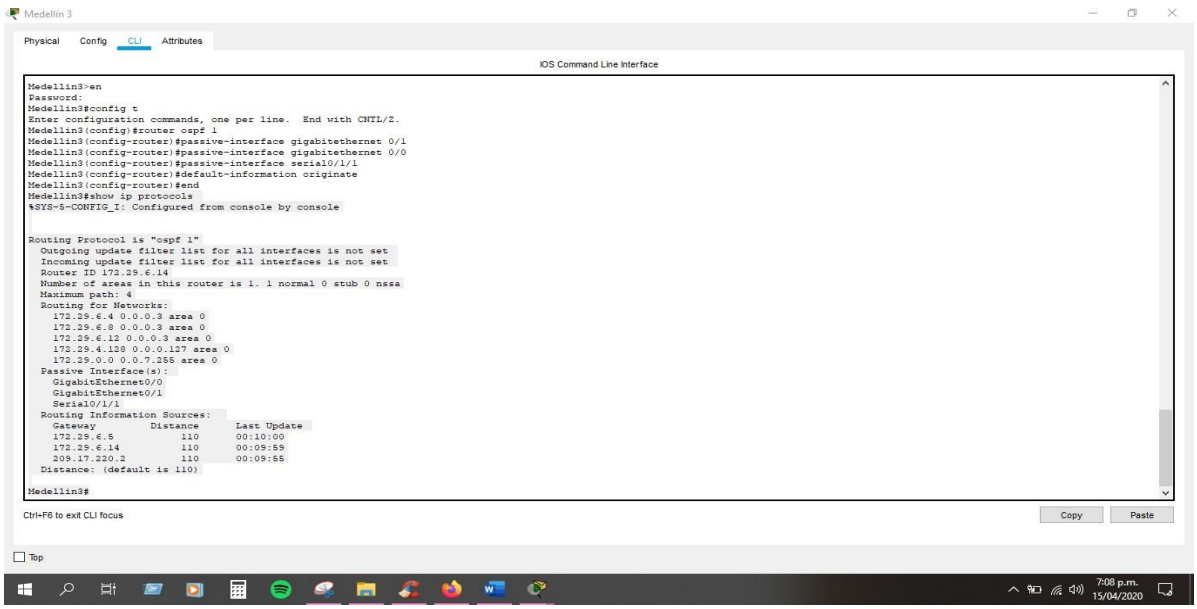


Figura 49. Verificación del protocolo OSPF en Medellín 3.



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.

Para verificar se emite el siguiente comando show ip route ospf en los Routers.

Bogotá

Figura 50. Verificación de las bases de datos de OSPF en Bogotá 1.

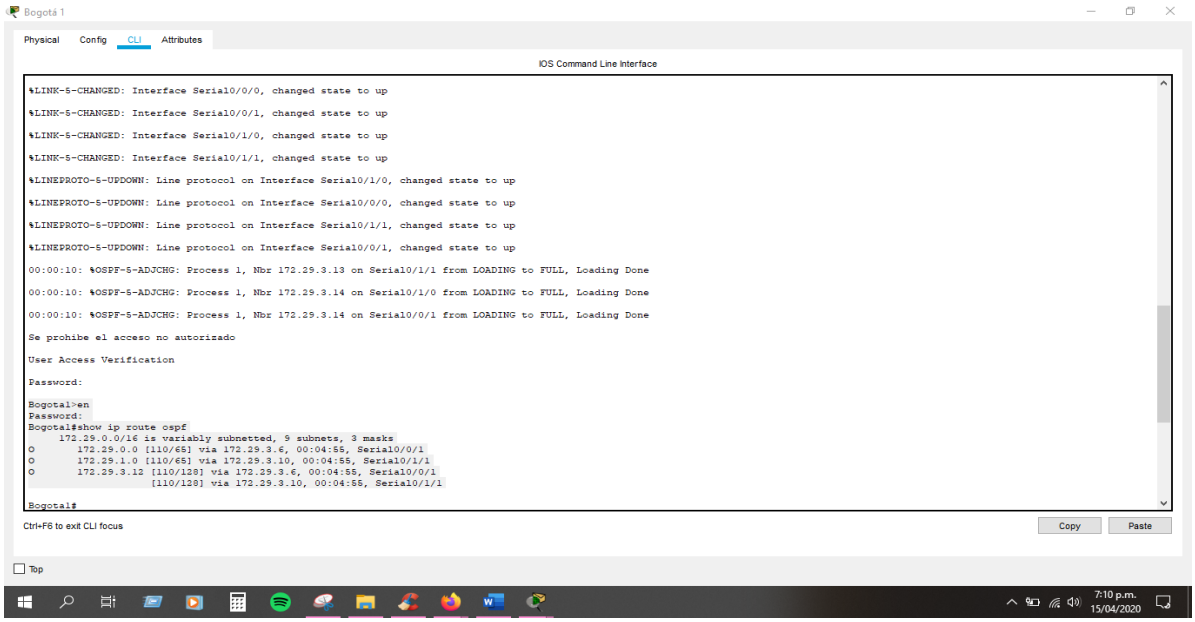


Figura 51. Verificación de las bases de datos de OSPF en Bogotá 2.

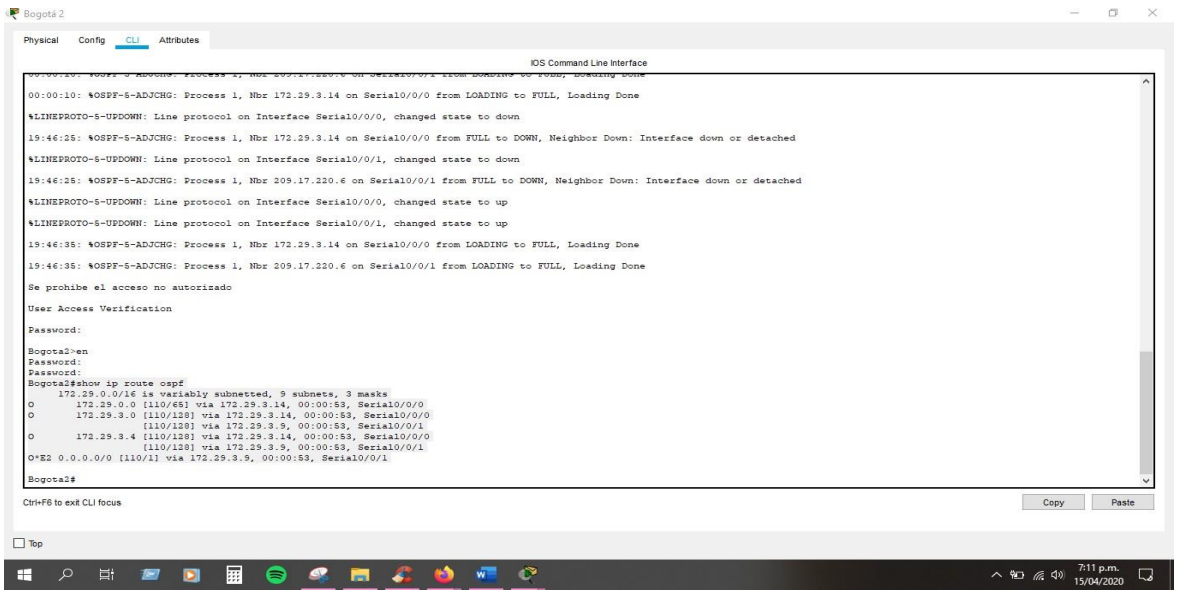
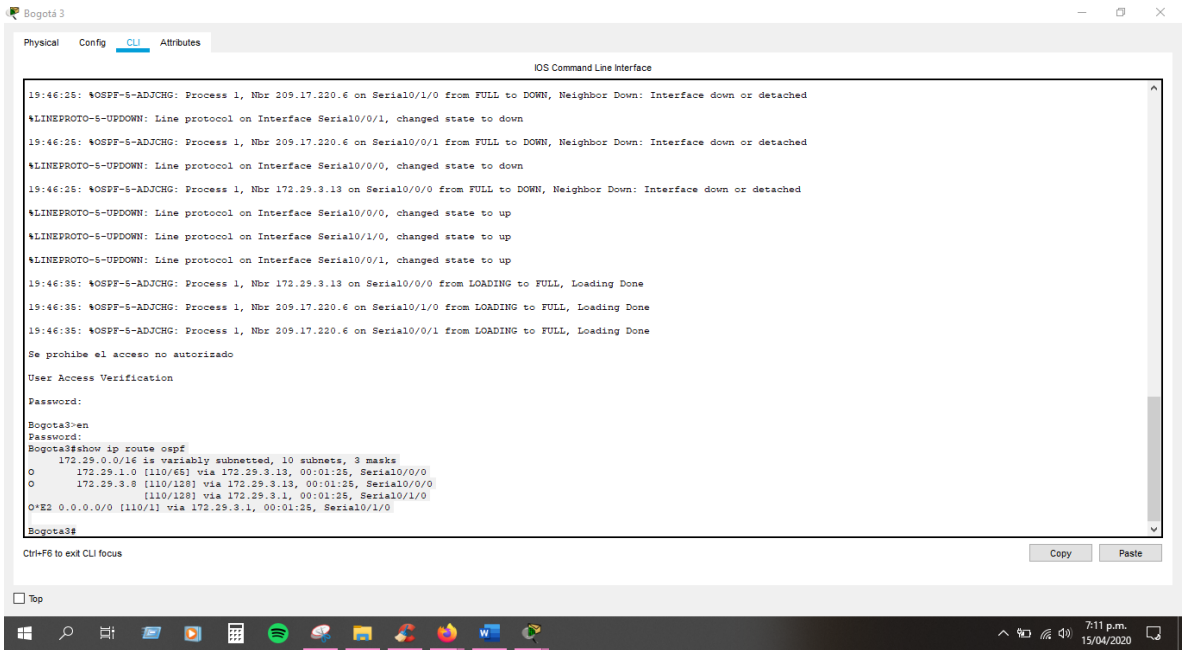


Figura 52. Verificación de las bases de datos de OSPF en Bogotá 3.



Medellín

Figura 53. Verificación de las bases de datos de OSPF en Medellín 1.

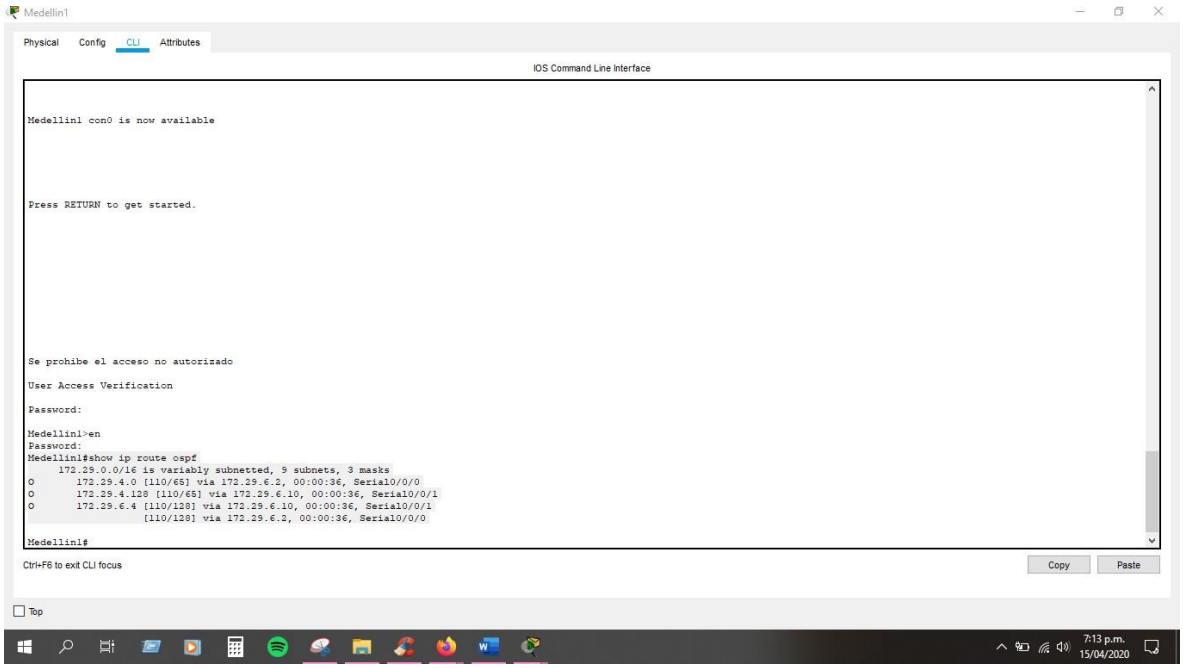


Figura 54. Verificación de las bases de datos de OSPF en Medellín 2.

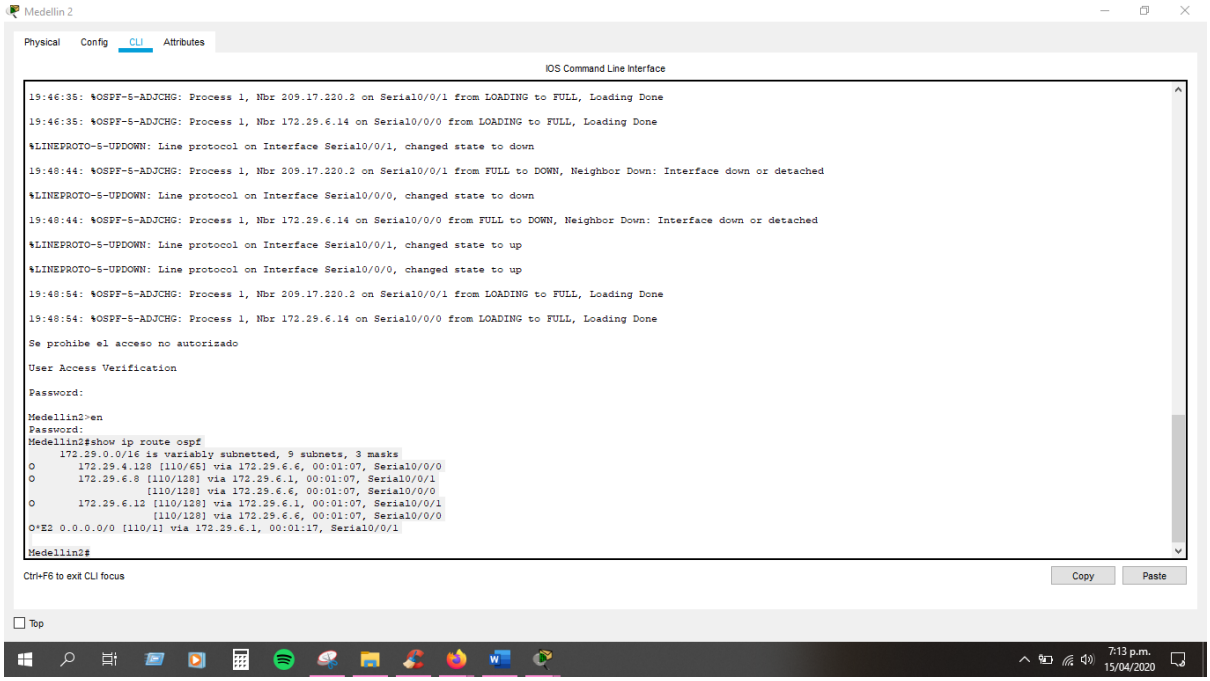
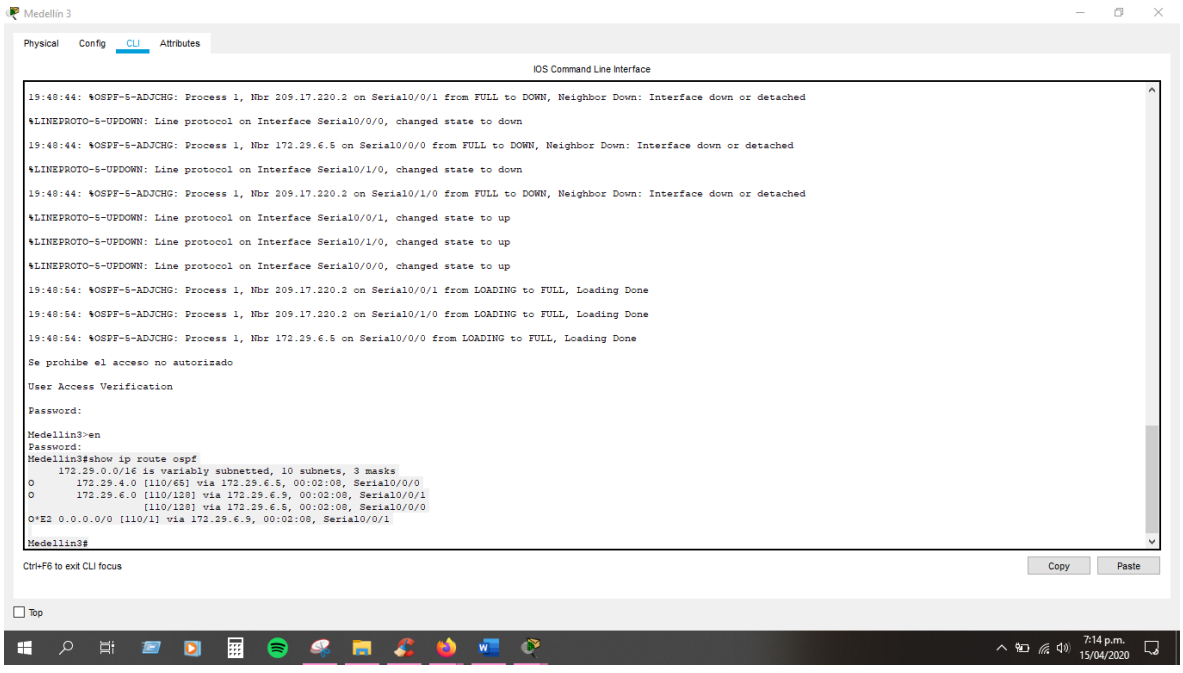


Figura 55. Verificación de las bases de datos de OSPF en Medellín 3.



Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Se activa PPP con autenticación PAP para crear un enlace punto a punto se proporciona un usuario y contraseña para los dos Routers Medellín 1 e ISP.

Medellín 1

```
Medellin1(config)#int s0/1/0
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username Medellin1 password cisco123
Medellin1(config-if)#exit
Medellin1(config)#username ISP password cisco123
```

ISP

```
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 cisco123
ISP(config-if)#exit
ISP(config)#username Medellin1 password cisco123
```

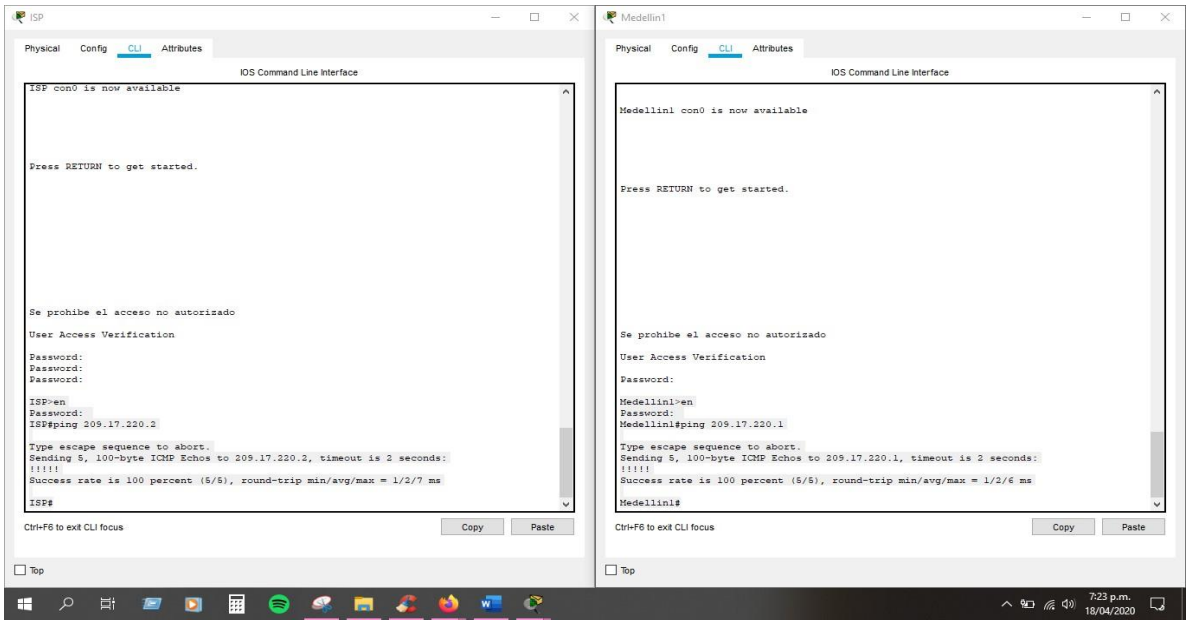
Para verificar la conectividad de PPP, se realiza un ping entre los dos Routers, además de proporciona la captura de los resultados al implementar la prueba.

Comandos utilizados para realizar el ping entre ISP y Medellín 1:

```
ISP#ping 209.17.220.2
```

```
Medellin1#ping 209.17.220.1
```

Figura 56. Verificación PAP mediante ping de Medellín 1 e ISP.



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

Se activa PPP con autenticación CHAP para crear una conexión, proporcionando un usuario y contraseña para los dos Routers Bogotá 1 e ISP.

Bogotá 1

Bogota1(config)#int s0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#exit
Bogota1(config)#username ISP password cisco123

ISP

ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
ISP(config)#username Bogota1 password cisco123

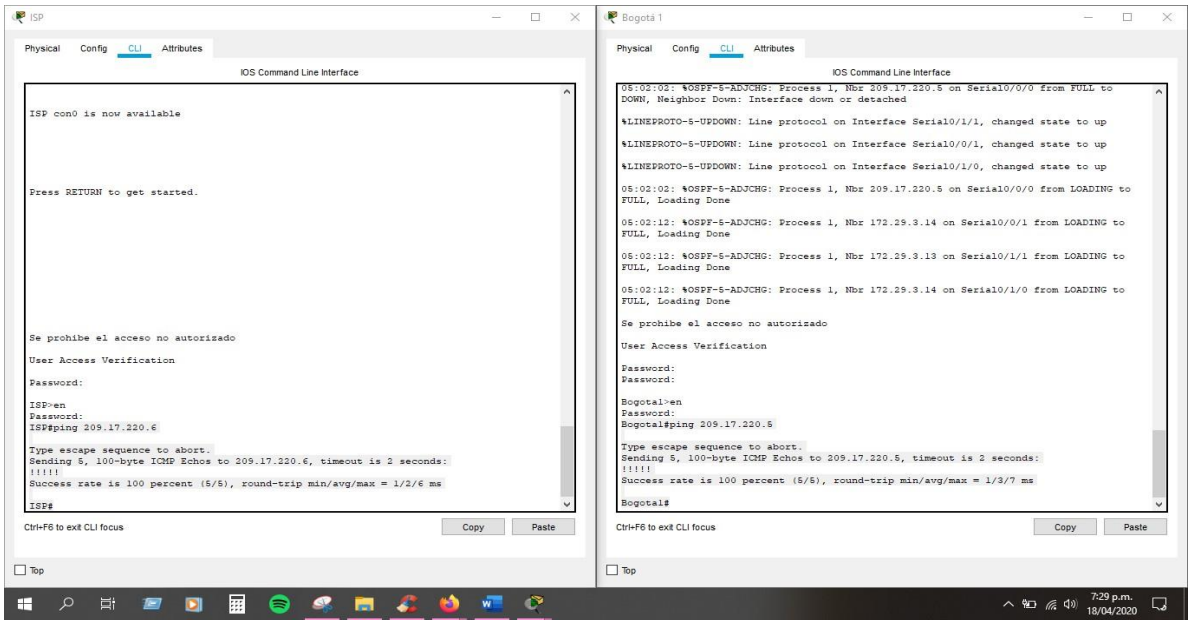
Para verificar la conectividad de CHAP, se realiza un ping entre los dos Routers, además de proporciona la captura de los resultados al implementar la prueba.

Comandos utilizados para realizar el ping entre ISP y Bogotá 1:

ISP#ping 209.17.220.6

Bogota1#ping 209.17.220.5

Figura 57. Verificación CHAP mediante ping de Bogotá 1 e ISP.



Parte 6: Configuración de PAT.

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

Activamos NAT para cada Router, para que sea PAT se adiciona el overload en las interfaces.

Ahora se activa NAT en Bogotá 1, teniendo en cuenta su interfaz de salida.

Bogotá 1

Bogota1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#ip nat inside source list 1 interface s0/0/0 overload

Se hace el mismo procedimiento para Medellín 1, teniendo en cuanta su interfaz de salida.

Medellín 1

```
Medellin1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#ip nat inside source list 1 interface s0/1/0 overload
```

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.

Teniendo en cuenta la parte 1 sección c; donde las redes cambiaron su netmask a /22, ahora antes de activar NAT; debemos encontrar la Wildcard para la red Medellín

Medellín -> 172.29.4.0/22 Class B

Tabla 38. Hallar Wildcard para la red Medellín.

Medellín		
Address:	172.29.4.0	10101100.00011101.000001 00.00000000
Netmask:	255.255.252.0 = 22	11111111.11111111.111111 00.00000000
Wildcard:	0.0.3.255	00000000.00000000.000000 11.11111111

Ahora, ya teniendo las Wildcard para cada red, se activan las NAT en Medellin1, así como se especifican sus interfaces de entrada y salida.

Medellín 1

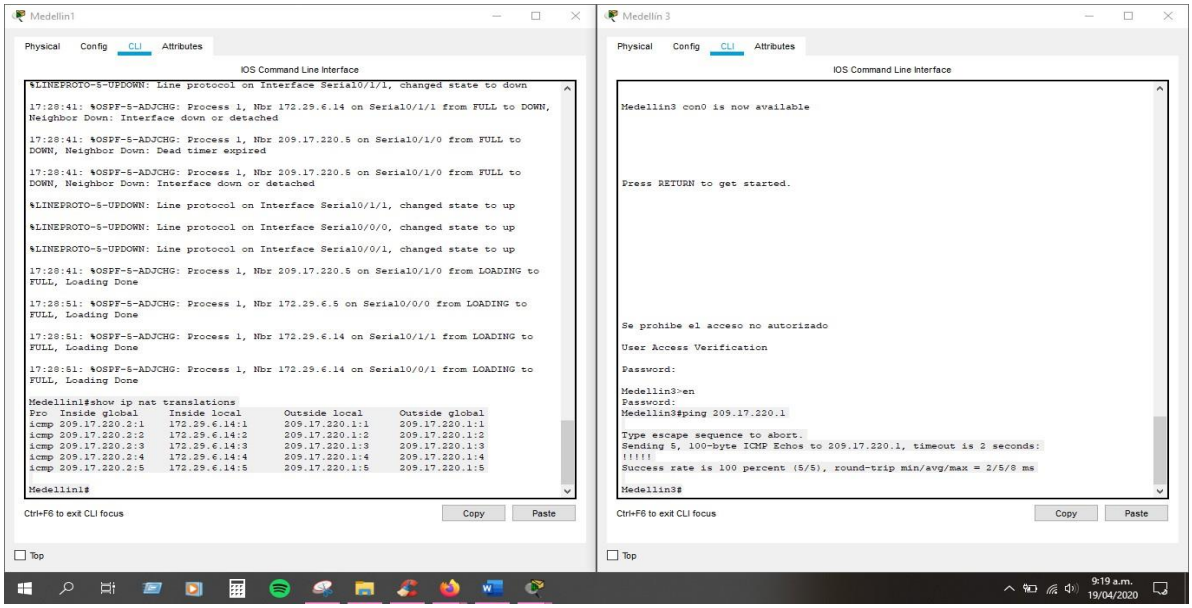
```
Medellin1(config)#ip nat inside source list 1 interface s0/1/0 overload
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin1(config)#int s0/1/0
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#int S0/0/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int S0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int S0/1/1
Medellin1(config-if)#ip nat inside
```

Se hace ping desde Medellin3 hacia fuera de la red, para verificar que la serial0/1/0 de Medellin1 realicen las traducciones configuradas para NAT.

Medellin3#ping 209.17.220.1

Medellin1#show ip nat translations

Figura 58. Verificación mediante ping para NAT en Medellín 1.



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.

Teniendo en cuenta la parte 1 sección c donde las redes cambiaron su netmask a /22, ahora antes de activar NAT; debemos encontrar la Wildcard para la red Bogotá.

Bogotá -> 172.29.0.0/22 Class B

Tabla 39. Hallar Wildcard para la red Bogotá.

Bogotá		
Address:	172.29.0.0	10101100.00011101.000000 00.00000000
Netmask:	255.255.252.0 = 22	11111111.11111111.111111 00.00000000
Wildcard:	0.0.3.255	00000000.00000000.000000 11.11111111

Ahora, ya teniendo las Wildcard para cada red, se activan las NAT en Bogota1, así como se especifican sus interfaces de entrada y salida.

Bogotá 1

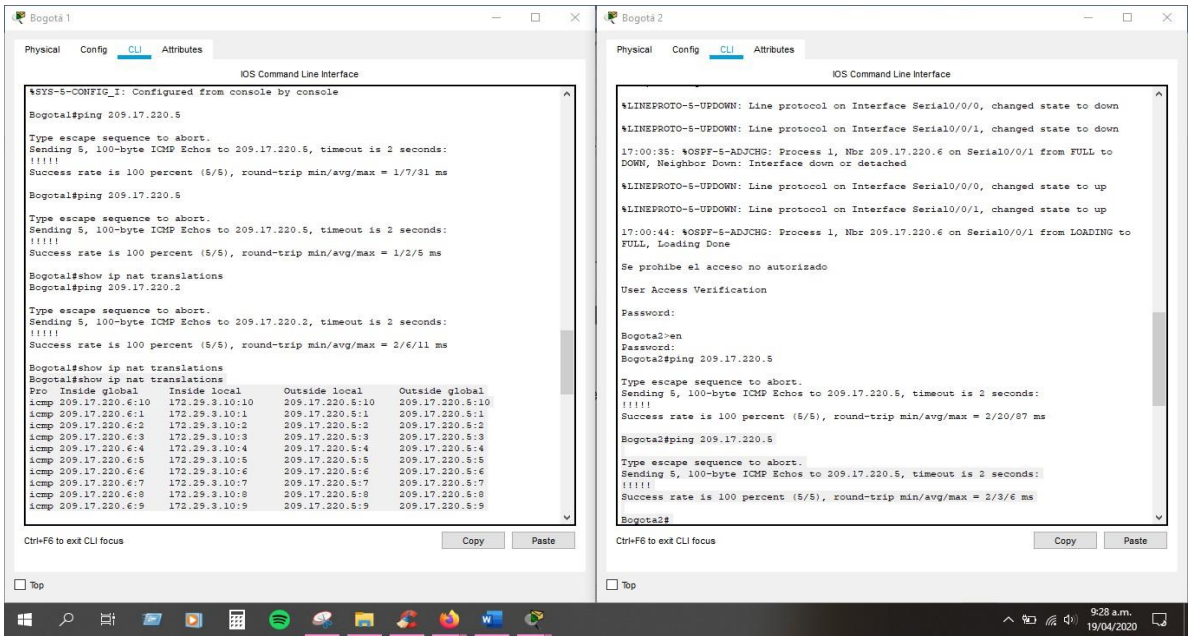
```
Bogota1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#ip nat inside source list 1 interface s0/0/0 overload
Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#int S0/0/1
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
```

Se realiza ping desde Bogota2 hacia fuera de la red, para verificar que la serial0/0/0 de Bogota1 realicen las traducciones configuradas para NAT.

```
Bogota2#ping 209.17.220.5
```

```
Bogota1#show ip nat translations
```

Figura 59. Verificación mediante ping para NAT en Bogotá 1.



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.

Medellín 2 Servidor DHCP

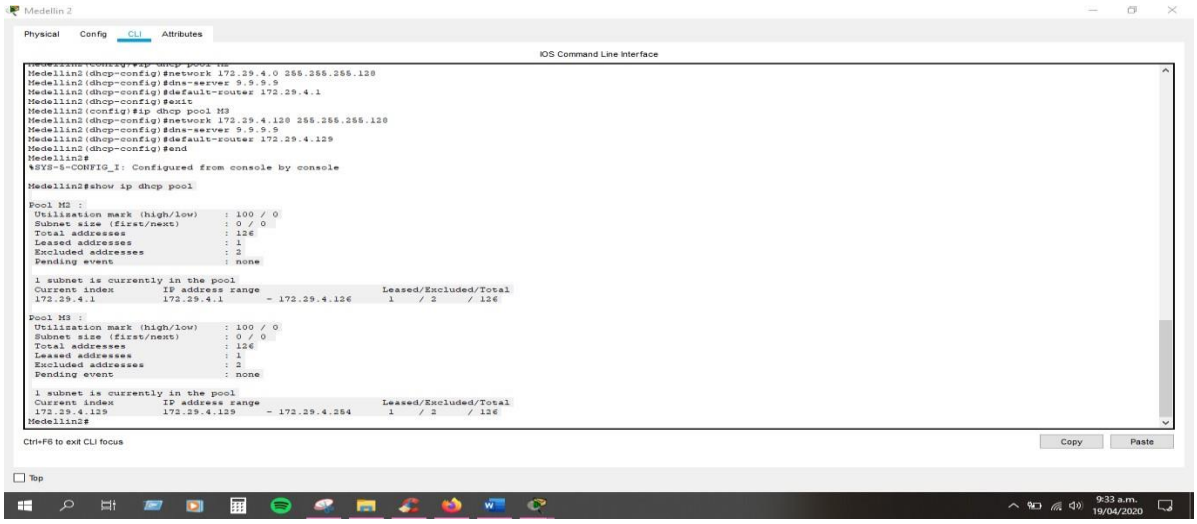
Se realiza la configuración de DHCP utilizando como DNS IBM Quad 9.

```
Medellin2>en
Password:
Medellin2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
Medellin2(config)#ip dhcp pool M2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#dns-server 9.9.9.9
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool M3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#dns-server 9.9.9.9
Medellin2(dhcp-config)#default-router 172.29.4.129
```

Para verificar se emite el siguiente comando:

```
Medellin2#show ip dhcp pool
```

Figura 60. Verificación servidor DHCP en Medellín 2.



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

Ya que la red LAN está configurada en diferentes rangos de IP mediante ip-helper solicitamos al servidor Medellín2 emitiendo su IP y luego emitiendo la interfaz de salida del cliente G0/0 para solicitar la configuración de DHCP.

Medellín 3 es donde está el cliente

Medellin3>en
Password:
Medellin3#
Medellin3#config 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)#exit

Luego de realizar la configuración DHCP, se verifica que las direcciones de los hosts estén proporcionadas a sus tarjetas de red emitidas desde el servidor:

Figura 61. Verificación IP por DHCP 50HOST de Medellín 2.

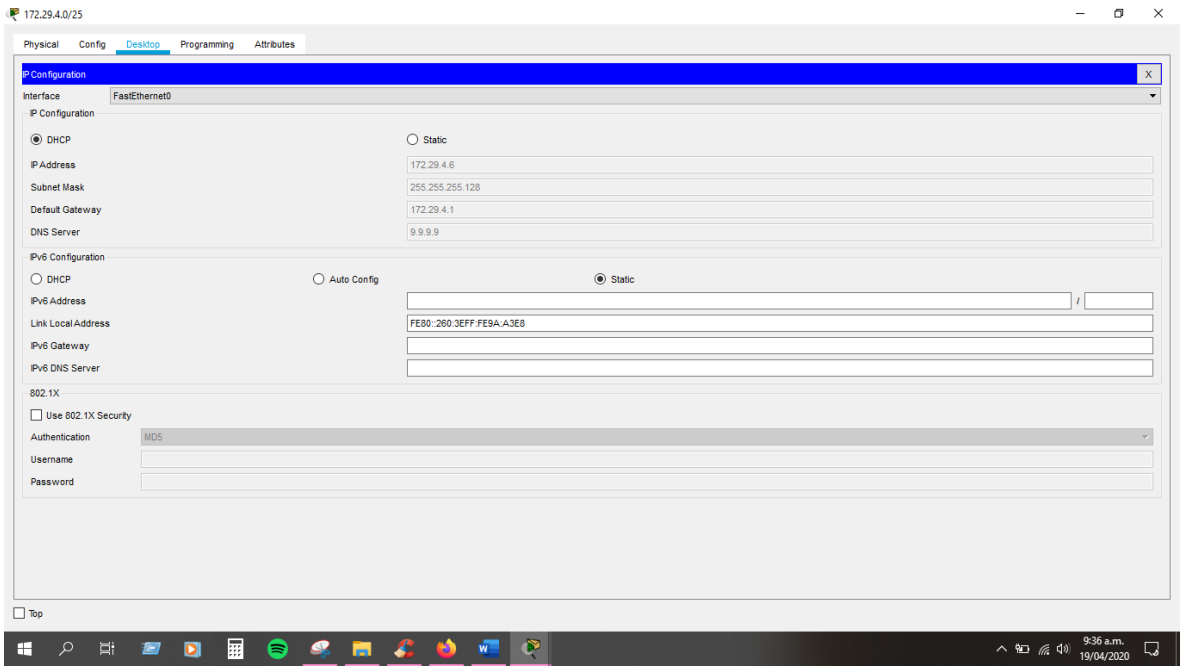
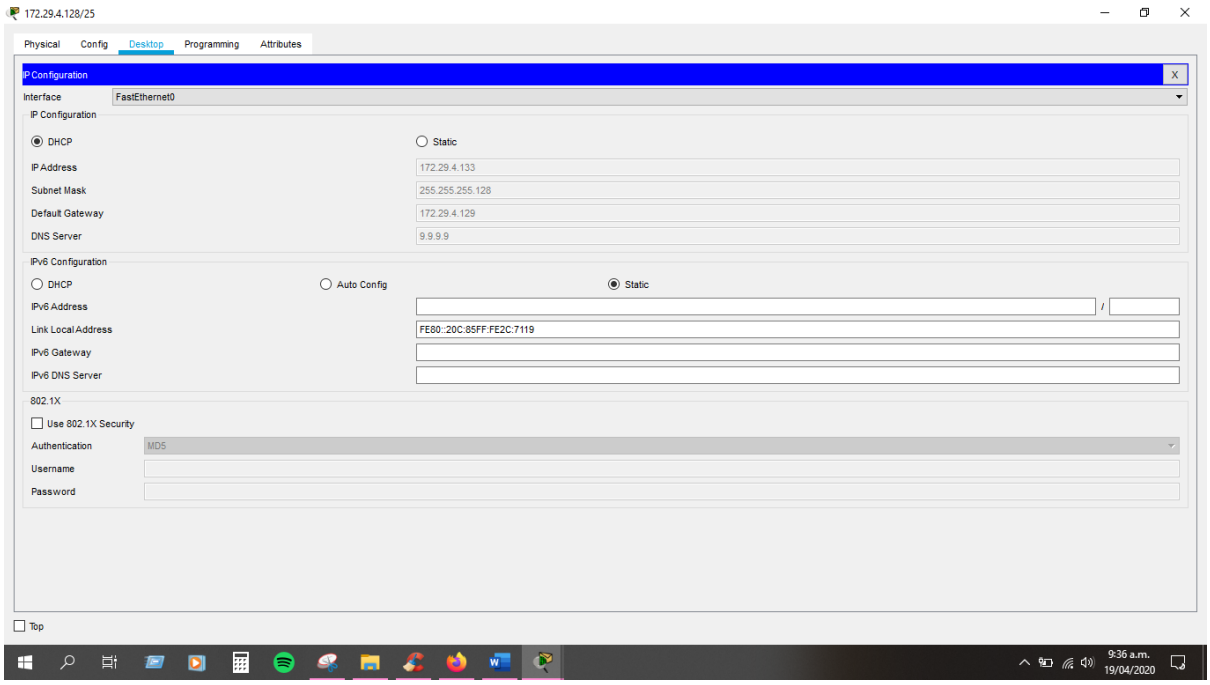


Figura 62. Verificación IP por DHCP 40HOST de Medellín 3.



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

Bogotá 2 Servidor DHCP

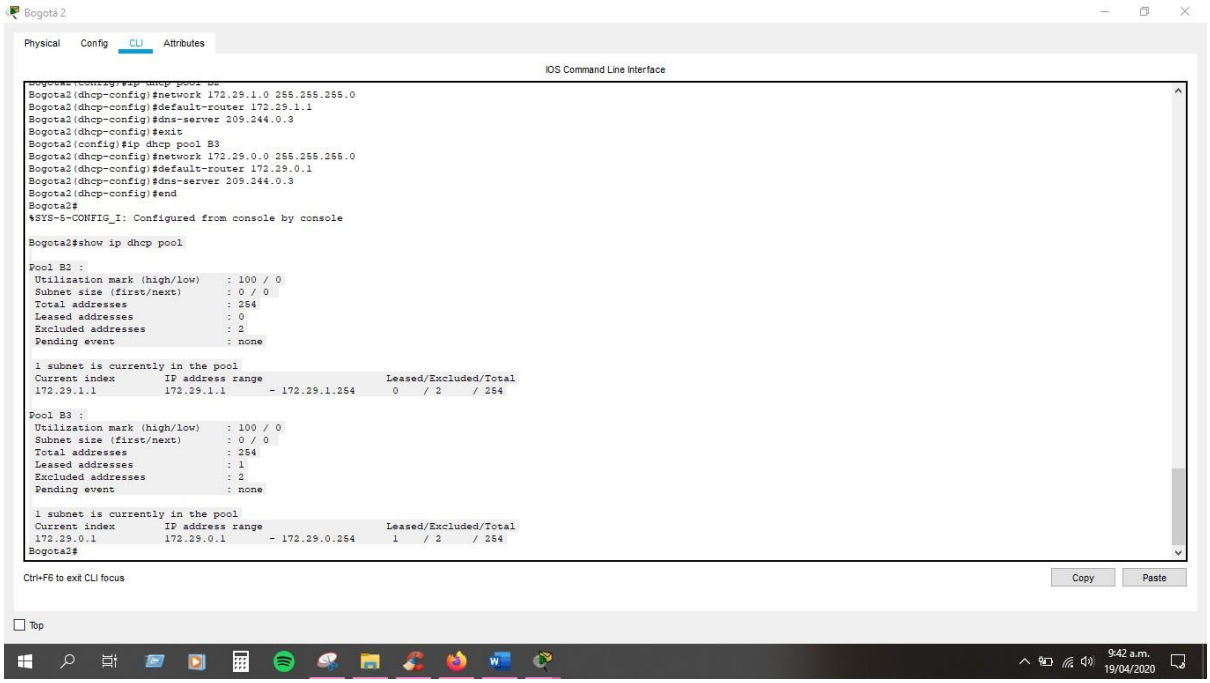
Se realiza la configuración de DHCP utilizando como DNS Level13.

```
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 B2
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 209.244.0.3
Bogota2(dhcp-config)#exit
Bogota2(config)#ip dhcp pool B3
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.0.1
Bogota2(dhcp-config)#dns-server 209.244.0.3
Bogota2(dhcp-config)#end
```

Para verificar se emite el siguiente comando:

Bogota2#show ip dhcp pool

Figura 63. Verificación servidor DHCP en Bogotá 2.



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

Ya que la red LAN está configurada en diferentes rangos de IP mediante ip-helper solicitamos al servidor Bogotá2 emitiendo su IP y luego emitiendo la interfaz de salida del cliente G0/0 para solicitar la configuración de DHCP.

Bogotá 3 es donde está el cliente

Bogota3>en
Password:
Bogota3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#int g0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
Bogota3(config-if)#exit
Bogota3(config)#

Luego de realizar la configuración DHCP, se verifica que las direcciones de los hosts estén proporcionadas a sus tarjetas de red emitidas desde el servidor:

Figura 64. Verificación IP por DHCP 200HOST de Bogotá 2.

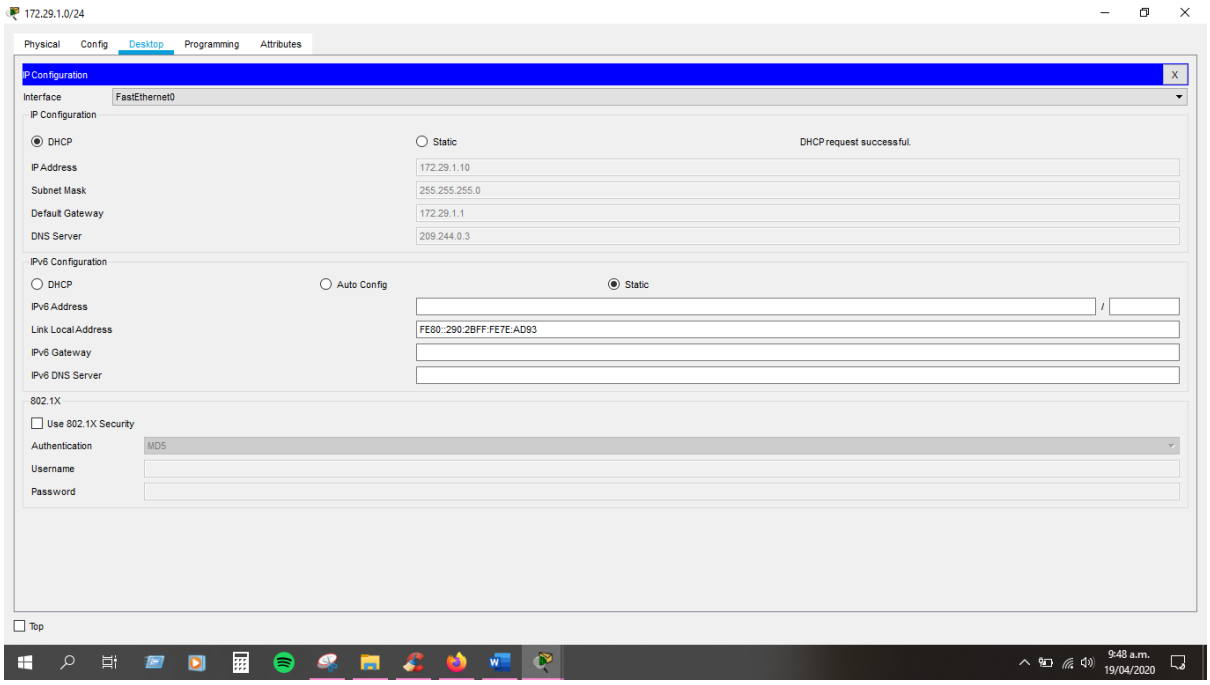
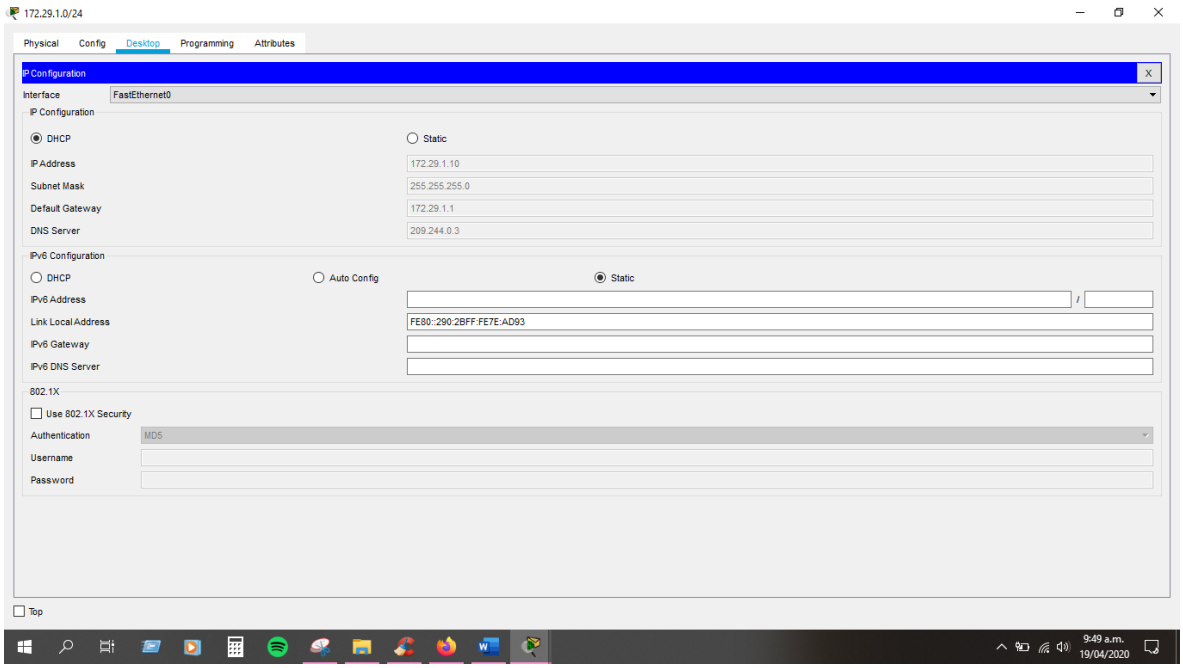


Figura 65. Verificación IP por DHCP 150HOST de Bogotá 3.



Para entrar más en detalle sobre los pings emitidos hacia ISP, se verifica realizando pruebas en cada uno de los hosts para las redes de Bogotá y Medellín.

Figura 66. Conectividad hacia ISP desde los Hosts de Bogotá.

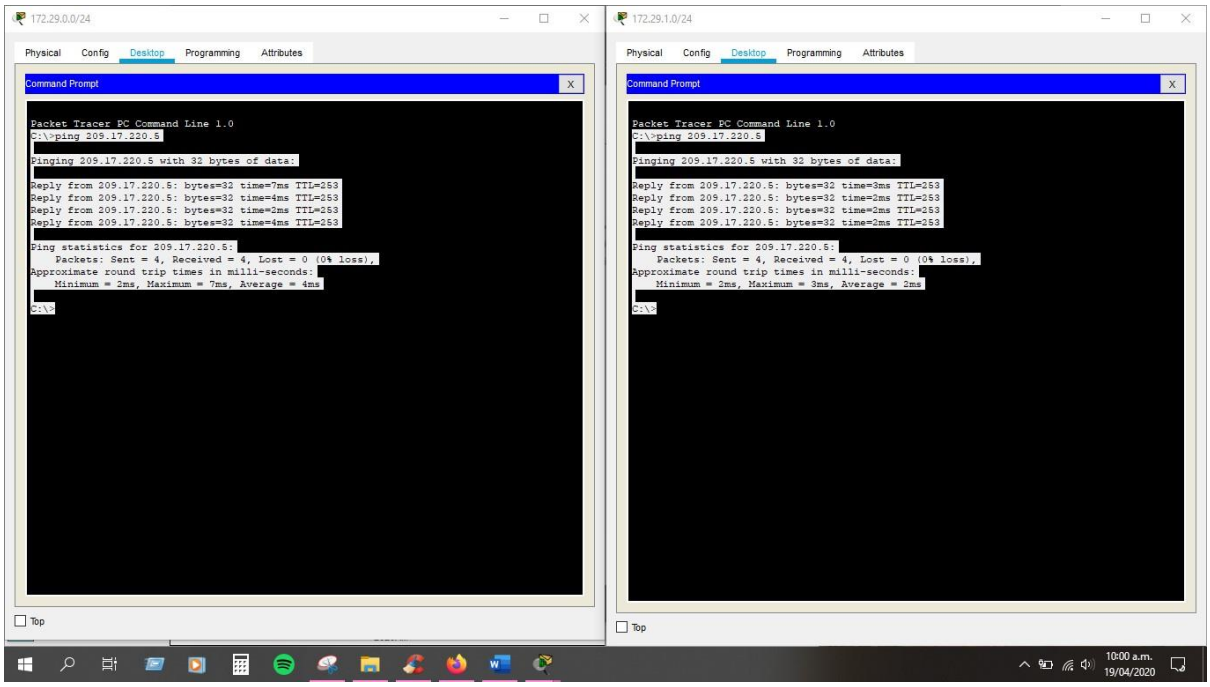
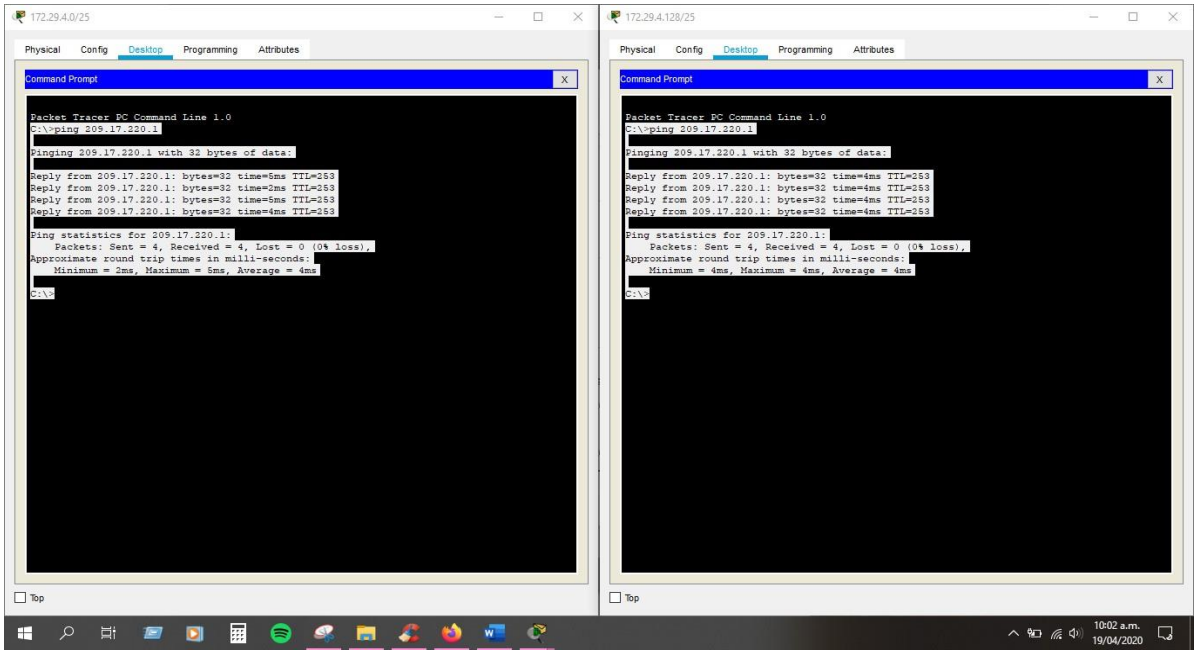


Figura 67. Conectividad hacia ISP desde los Hosts de Medellín.



CONCLUSIONES

En el presente informe se realizó dos tipos de escenarios, abordando los temas de seguridad de redes en VLANs, ACL, DHCP, NAT, NTP, RIPv2 en direccionamiento IPv4 e IPv6.

Además, se realizó la configuración de requerimiento en OSPF, DHCP por medio de Router implementando NAT, PAT, PPP, PAP y CHAP; para las redes de Medellín y Bogotá, para ser conectadas hacia ISP.

Asumiendo el rol de administrador para los escenarios, se muestran las destrezas y habilidades adquiridas durante el curso de CISCO CCNA implementadas en cada escenario; por lo que se requiere un orden preciso, paciencia y responsabilidad.

Es importante implementar el orden, como el mapa sobre lo que se va a trabajar, que rutas y que interfaces conectan con las redes especificamente para dar sus direcciones IP correspondientes a cada equipo como Routers, Switches, Servidores y PC’s; llegando a los resultados de conectividad entre redes para asi cumplir con los objetivos del presente informe y del curso.

BIBLIOGRAFÍA

Cisco. CCNA 1 and 2. Cisco Certified Network Associate, versión 3.1. [En línea]. [8 de abril del 2020]. Disponible en: https://studylib.es/doc/7481657/ccna-1-y-2---cisco-ccna-2

Cisco. CCNA 3 and 4. Cisco Certified Network Associate, versión 3.1. [En línea]. [8 de abril del 2020]. Disponible en: https://issuu.com/sanodemente/docs/ccna_3_y_4

Cisco. Routing and switshing essentials, Companion guide. [En línea]. [10 de abril del 2020]. Disponible en: https://vulms.vu.edu.pk/Courses/CS407/Downloads/Routing%20and%20Switching%20Essentials%20-%20Complete%20Book.pdf

Cisco. Routing Protocols, Companion guide. [En línea]. [15 de abril del 2020]. Disponible en: https://vdocuments.mx/routing-protocols-companion-guide.html

Cisco. Conceptos sobre tecnología de redes. [En línea]. [18 de abril del 2020]. Disponible en: https://www.cisco.com/c/es_co/solutions/smb/networks/infographic-basic-concepts.html

Cisco. Protocolos y comunicaciones de red. Fundamentos de Networking. [En línea]. [18 de abril del 2020]. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

Cisco. SubNetting. Fundamentos de Networking. [En línea]. [18 de abril del 2020]. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

Cisco. Guía de diseño de OSPF. [En línea]. [20 de abril del 2020]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html