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

FREDDY JOVANNY JURADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE INGENIERIA
DIPLOMADO DE PROFUNDIZACION CISCO
SUBACHOQUE - CUNDINAMARCA
2020

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

FREDDY JOVANNY JURADO

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE INGENIERO DE SISTEMAS

TUTOR: HECTOR JULIAN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE INGENIERIA
DIPLOMADO DE PROFUNDIZACION CISCO
SUBACHOQUE - CUNDINAMARCA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Subachoque 20 de Mayo del 2020

Dedicatoria.

Dedico este trabajo a todo aquel que ha comprendido que si se aprende algo nuevo cada día, ese día no es perdido ni desaprovechado.

AGRADECIMIENTOS

Agradezco a todos los que brindaron sus conocimientos ya sea directa o indirectamente, invirtiendo su tiempo para que yo lograra comprender los temas más relevantes de este Diplomado.

TABLA DE CONTENIDO.

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

NETWORKING: aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos.

GATEWAY: aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos. Una red o red de datos es una red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos.

MASCARA SUBNETTING: La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

BIT: Dígito Binario. Unidad mínima de almacenamiento de la información cuyo valor puede ser 0 ó 1 (falso o verdadero respectivamente). Hay 8 bits en un byte

IPV4: es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

IPV6: es un sistema direccional del 128-bit usado para identificar un dispositivo en una red. Un direccionamiento del IPv6 se representa en ocho campos de los números hexadecimales, cada campo que contiene 16 bits. Un direccionamiento del IPv6 se divide en dos porciones, cada parte integrada por 64 bits. La primera parte que es la dirección de red, y la segunda parte la dirección de host.

PUERTO/REFLEJO DEL basado en protocolos divide la red física en los grupos VLAN lógicos para cada protocolo requerido. En el paquete de entrada, se marca la trama y la

calidad de miembro de VLAN se puede determinar sobre la base del Tipo de protocolo. Los grupos basados en protocolos a la asignación del VLA N ayudan a asociar a un grupo de protocolos a un puerto único.

QoS: El Calidad de Servicio (QoS) permite que usted dé prioridad al tráfico para diversas aplicaciones, los usuarios o los flujos de datos. Puede también ser utilizado para garantizar el funcionamiento a un nivel especificado, así, afectando a la calidad de servicio del cliente. QoS es afectado generalmente por los factores siguientes: jitter, tiempo de espera, y pérdida del paquete.

VLAN: El Reflejo es un método usado para monitorear el tráfico de la red. Con el puerto o el Reflejo del VLA N, las copias de entrante y los paquetes de salida en los puertos (puertos de origen) de un dispositivo de red se remiten a otro puerto (puerto de destino) donde se estudian los paquetes. Esto es utilizada como herramienta de diagnóstico por el administrador de la red.

VLA N basado en protocolos: Los grupos basados en protocolos pueden ser definidos y estar limitados a un puerto; por lo tanto, cada paquete que origina de los grupos de protocolos se asigna al VLAN configurado en la página. El VLA N

RESUMEN

Este trabajo busca identificar a través del desarrollo de escenarios, las habilidades y competencias adquiridas con el fin de profundizar en los diversos aspectos de Networking. Es decir, cada escenario debe estar completamente documentado con sus respectivos procesos, correspondientes al registro de la configuración de cada uno de los dispositivos, de cada una de las etapas, y de cada uno de los procesos de verificación.

Cada uno de los escenarios permite reforzar los conocimientos que se han ido adquiriendo en el desarrollo de diplomado de profundización CISCO; la configuración de los routers, switches, servidores y demás componentes de la red son conocimientos importantes que se deben adquirir con el fin de tener claro las posibles fallas que se pueden generar en las redes, para lograr mitigar de una manera más eficiente aquellos “errores” que se presentan a diario en la red.

Para lograr esto, debe tener presente lo importante que es el comprender la topología de la red, debido a que permite ver con mayor claridad todos los elementos y componentes que intervienen en la red, junto con la configuración que debe tener.

PALABRAS CLAVE: “Redes, Networking, Gateway, VLAN, Mascara Subnetting”.

1. INTRODUCCIÓN

La tecnología en las últimas décadas ha crecido de una manera exponencial, con el fin de mejorar la percepción de bienestar de la humanidad, pero es de resaltar los pasos agigantados que ha tenido “el mundo de las telecomunicaciones”.

Hace años era difícil imaginar que las redes serian indispensables para el desarrollo normal de nuestra vida, ya sea llamando desde nuestro celular o en video conferencia desde nuestro computador personal, o recibiendo clases a través de medios sincrónicos o asincrónicos. Pero, aunque todos disfrutamos de estos beneficios; muy pocos nos detenemos a pensar ¿cómo funciona?, ¿Cuál es la configuración que maneja?, ¿Por qué es necesario cada uno de los componentes que posee una red?, ¿Qué es una red? Entre otras cosas…

A través de este trabajo se pretende dar a conocer los conceptos adquiridos durante el diplomado CISCO CCNA, los cuales se resaltan la configuración de los parámetros básicos de los dispositivos, verificación de la conectividad, configuración de la seguridad.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Identificar las habilidades y competencias que se han adquirido en el desarrollo del diplomado de profundización CISCO

2.2. OBJETIVOS ESPECÍFICOS

- Configurar eficientemente la red de los escenarios 1 y 2 de acuerdo a las necesidades establecidas por cada uno de ellos.

- Comprender la importancia de la topología de la red como medio para implementar la configuración y/o mitigar las fallas.

3. PLANTEAMIENTO DEL PROBLEMA

3.1. DEFINICIÓN DEL PROBLEMA

El diseño e implementación de las redes convergentes a nivel empresarial y el uso de los diferentes protocolos enrutados dependen en gran medida de las necesidades de cada empresa y de su tipo de negocio; es responsabilidad de los ingenieros de redes ofrecer soluciones flexibles, escalables y seguras que contribuyan a mantener la conectividad y las comunicaciones siempre disponible para apoyar las metas de negocio y general valor a las organizaciones.

Cabe resaltar que las redes convergentes y su tecnología avanzan de manera rápida, es importante para los ingenieros equilibrar este avance con un enfoque de seguridad, que permita mitigar los riesgos que pueden surgir en cada momento.

3.2 JUSTIFICACIÓN

Las redes convergentes a nivel empresarial se han convertido en un medio valioso para las necesidades de cada empresa y de su tipo de negocio. Por tal razón este documento busca brindar de manera clara y precisa los métodos de configuración necesarios para la implementación eficaz de la red en cada uno de los escenarios.

Estos escenarios poseen las características y problemáticas que todo ingeniero de redes tendrá que enfrentar en su vida laboral, además de que permite una mayor claridad al diseñar y configurar soluciones soportadas de acuerdo a la topología de red requerida bajo el uso de los diferentes protocolos enrutados.

4. DESARROLLO DE LOS ESCENARIOS

4.1. ESCENARIO 1

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

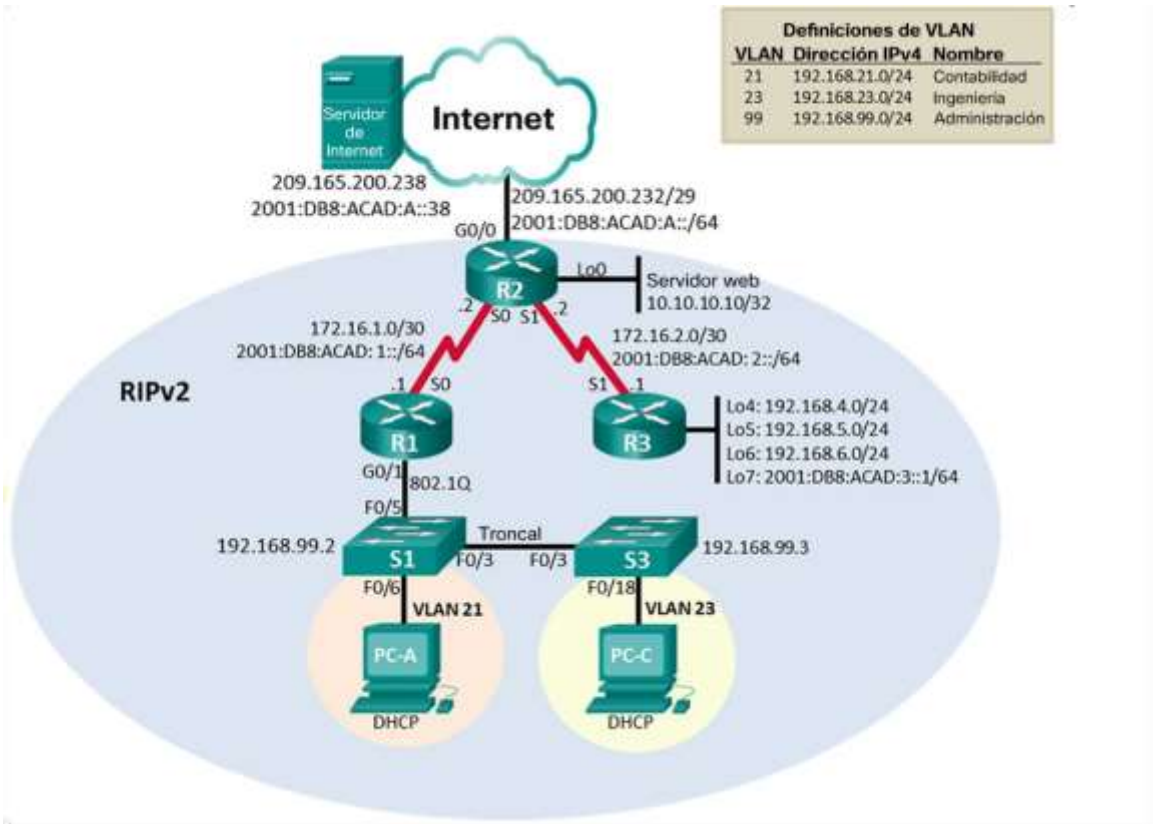


Figure 1. Topología escenario 1

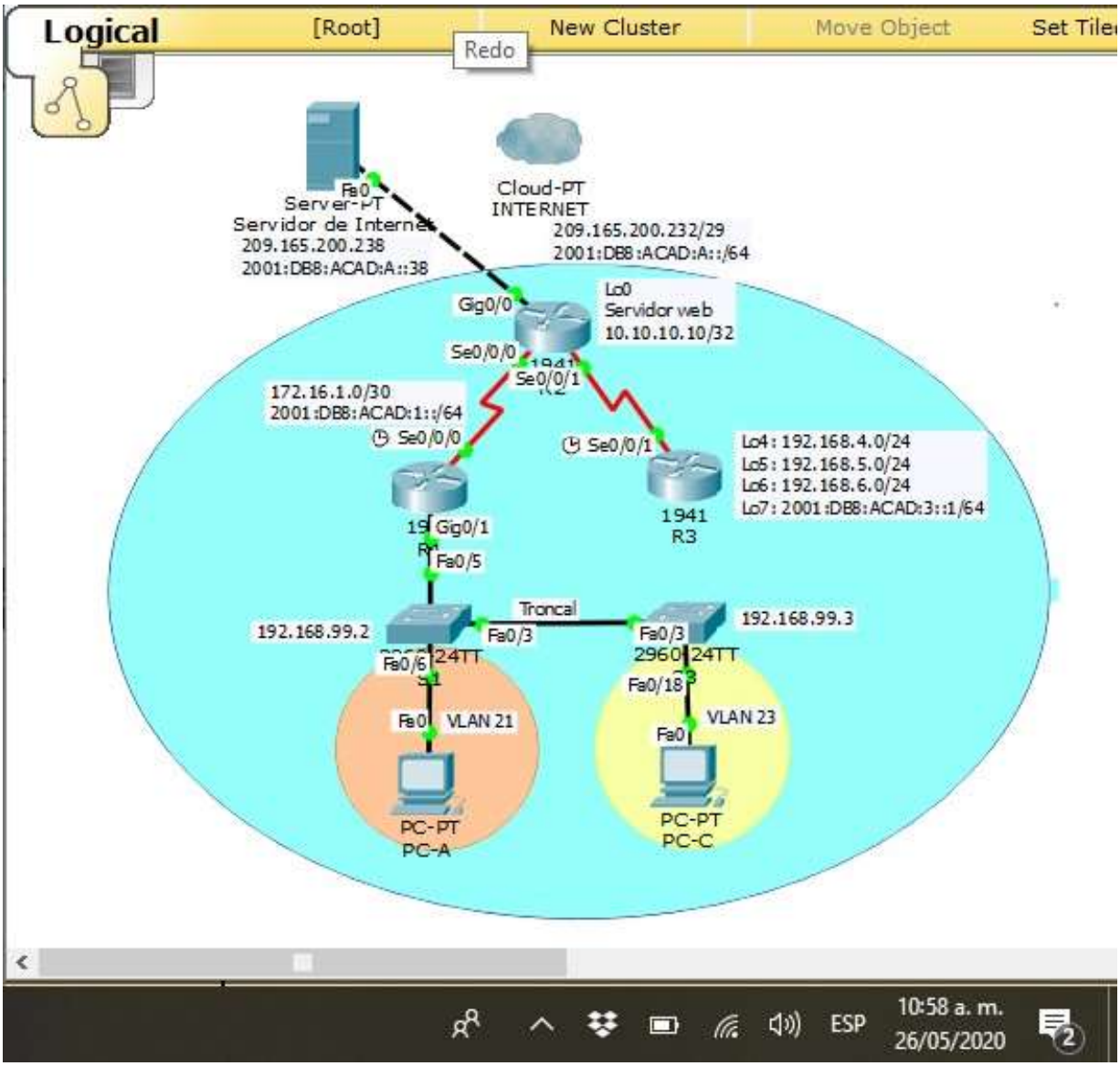


Figure 2. Topología escenario 1 en Packet tracer

.

Parte 1: Inicializar dispositivos

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

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

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

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers	Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	erase startup-config delete vlan.dat
Volver a cargar ambos switches	Reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	show flash

Tabla 1. Configuración de inicio

Parte 2: Configurar los parámetros básicos de los dispositivos

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):

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

Tabla 2 Configurar la computadora de Internet

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

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	Hostname R1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line console 0 Password **cisco** Login
Contraseña de acceso Telnet	Line vty o 15 Password **cisco**
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd “Se prohíbe el acceso no autorizado”

Interfaz S0/0/0	**Establezca la descripción** Interface serial 0/0/0 Description connection to R2 **Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones** Ip address 172.16.1.1 255.255.255.252 **Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones** Ipv6 address 2001:db8:acad:1::1/64 **Establecer la frecuencia de reloj en 128000** Clock rate 128000 **Activar la interfaz** No shutdown
Rutas predeterminadas	**Configurar una ruta IPv4 predeterminada de S0/0/0** Ip route 0.0.0.0 0.0.0.0 serial 0/0/0 **Configurar una ruta IPv6 predeterminada de S0/0/0** Ipv6 route ::0/0 serial 0/0/0

Tabla 3. Configurar Router 1

Nota: Todavía no configure G0/1.

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	hostname R2
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server

Mensaje MOTD	R2(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0	**Establezca la descripción** R2(config)#interface serial 0/0/0 R2(config-if)#description Connection to R1 **Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.** R2(config-if)#ip address 172.16.1.2 255.255.255.252 **Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.** R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 **Activar la interfaz** R2(config-if)#no shutdown

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

Interfaz G0/0 (simulación de Internet)	**Establecer la descripción.** R2(config-if)#interface g 0/0 R2(config-if)#description Connection to Internet **Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.** R2(config-if)#ip address 209.165.200.233 255.255.255.248 **Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.** R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 **Activar la interfaz** R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado)	**Establecer la descripción.** R2(config-if)#interface loopback 0 R2(config-if)#description servidor web simulado **Establezca la dirección IPv4.** R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	**Configure una ruta IPv4 predeterminada de G0/0.** R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 **Configure una ruta IPv6 predeterminada de G0/0.** R2(config)#ipv6 route ::/0 g0/0

Tabla 4. Configurar Router 2

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

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
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Se prohíbe el acceso no autorizado"

Interfaz S0/0/1	**Establecer la descripción** R3(config)#interface serial 0/0/1 R3(config-if)#description Connection to R2 **Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.** R3(config-if)#ip address 255.255.255.252 **Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.** R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 **Activar la interfaz** R3(config-if)#no shutdown
Interfaz loopback 4	**Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.** R3(config-if)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5	**Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.** R3(config-if)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	**Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.** R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	**Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.** R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5. Configurar Router 3

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "se prohibe el acceso no autorizado"

Tabla 6. Configurar Switch 1

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd "se prohibe el acceso no autorizado"

Tabla 7. Configurar Switch 3

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:

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

Tabla 8. Verificando conectividad de la red

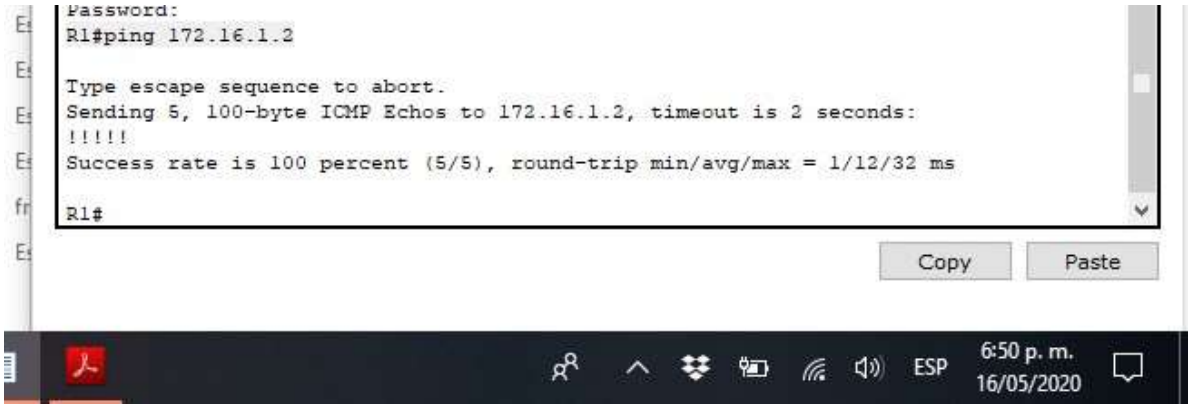


Figure 3. Verificando conectividad R1 a R2 S0/0/0

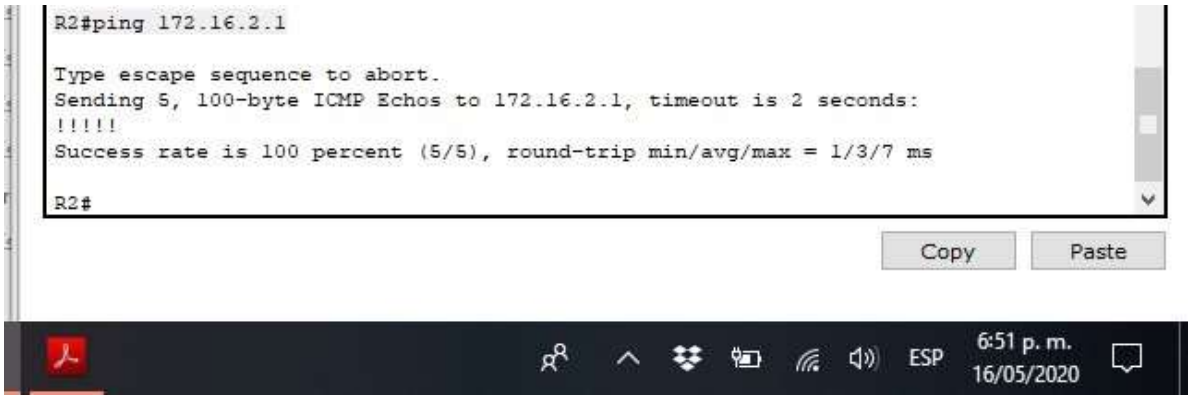


Figure 4. Verificando conectividad R1 a R2 S0/0/1

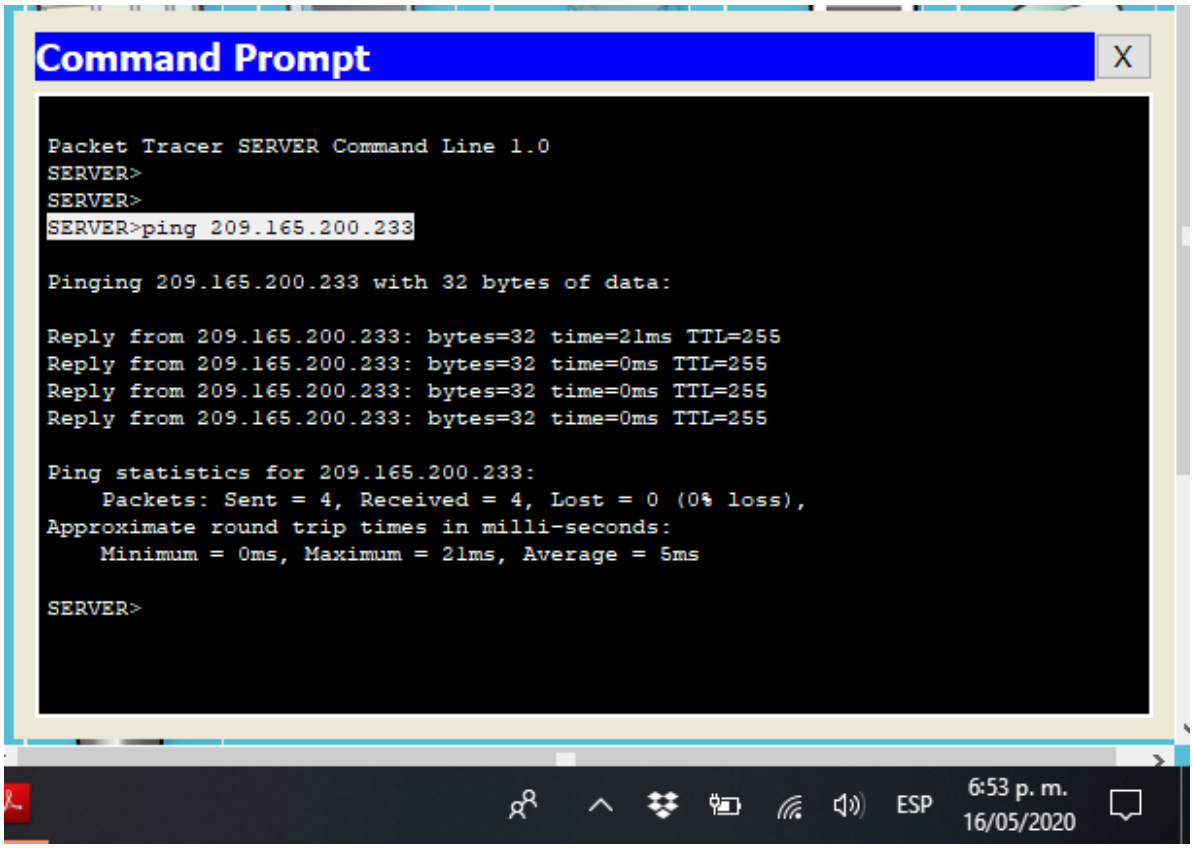


Figure 5. Verificando conectividad PC Internet a Gateway Predeterminado

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

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

Paso 9: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	**Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican** 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

Asignar la dirección IP de administración.	**Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología** S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	**Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.** S1(config)#ip default-gateway 192.168.99.1 S1(config)#interface f0/3 S1(config-if)#switchport mode trunk
Forzar el enlace troncal en la interfaz F0/3	**Utilizar la red VLAN 1 como VLAN nativa** S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	**Utilizar la red VLAN 1 como VLAN nativa** S1(config-if)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	**Utilizar el comando interface range** S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 9. Configurando la seguridad del Switch 1 y las VLAN

Paso 10: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	**Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.** S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	**Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología** S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit

Asignar el gateway predeterminado.	**Asignar la primera dirección IP en la subred como gateway predeterminado.** S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	**Utilizar la red VLAN 1 como VLAN nativa** S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	**Utilizar el comando interface range** S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 10. Configurando la seguridad del Switch 3 y las VLAN

Paso 11: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	**Descripción: LAN de Contabilidad** **Asignar la VLAN 21** **Asignar la primera dirección disponible a esta interfaz** R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	**Descripción: LAN de Ingeniería** **Asignar la VLAN 23** **Asignar la primera dirección disponible a esta interfaz** R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	**Descripción: LAN de Administración** **Asignar la VLAN 99** **Asignar la primera dirección disponible a esta interfaz** R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown

Tabla 11. Configurando la seguridad del Router 1 y las VLAN

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:

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Si

S3	R1, dirección VLAN 99	192.168.99.1	Si
S1	R1, dirección VLAN 21	192.168.21.1	Si
S3	R1, dirección VLAN 23	192.168.23.1	Si

Tabla 12. Verificando la conectividad de la red (dirección vlan)

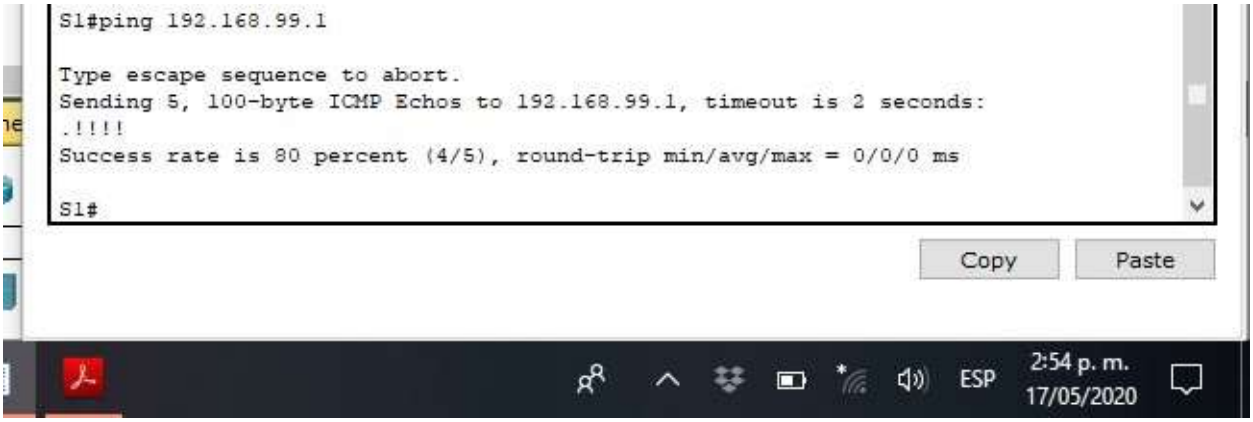


Figure 6. Verificando la conectividad de S1 a R1, dirección VLAN 99

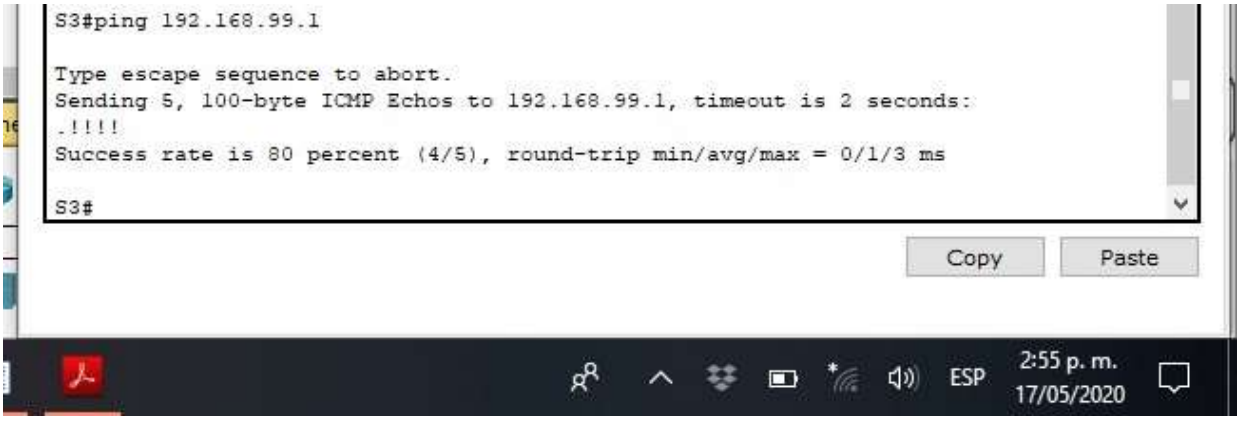


Figure 7. Verificando la conectividad de S3 a R1, dirección VLAN 99

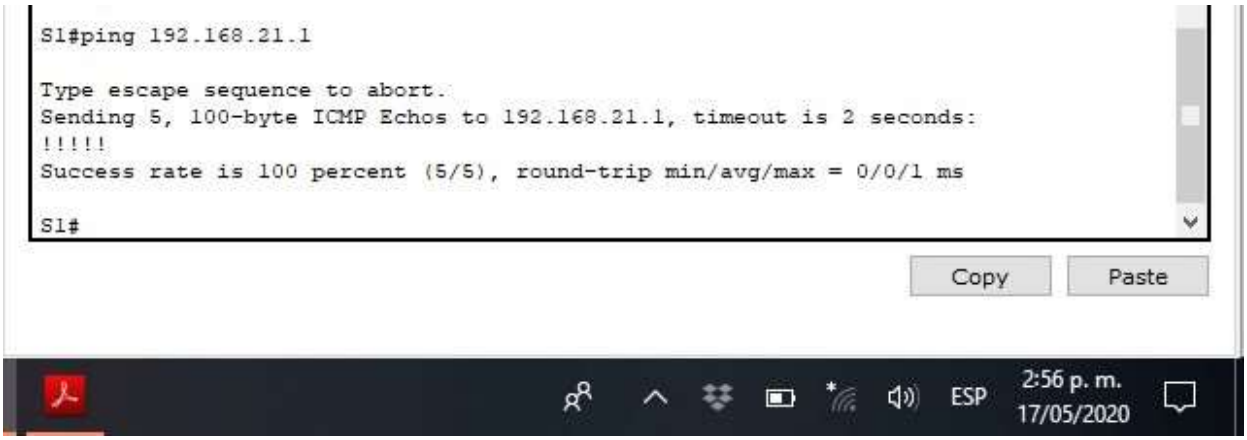


Figure 8. Verificando la conectividad de S1 a R1, dirección VLAN 21

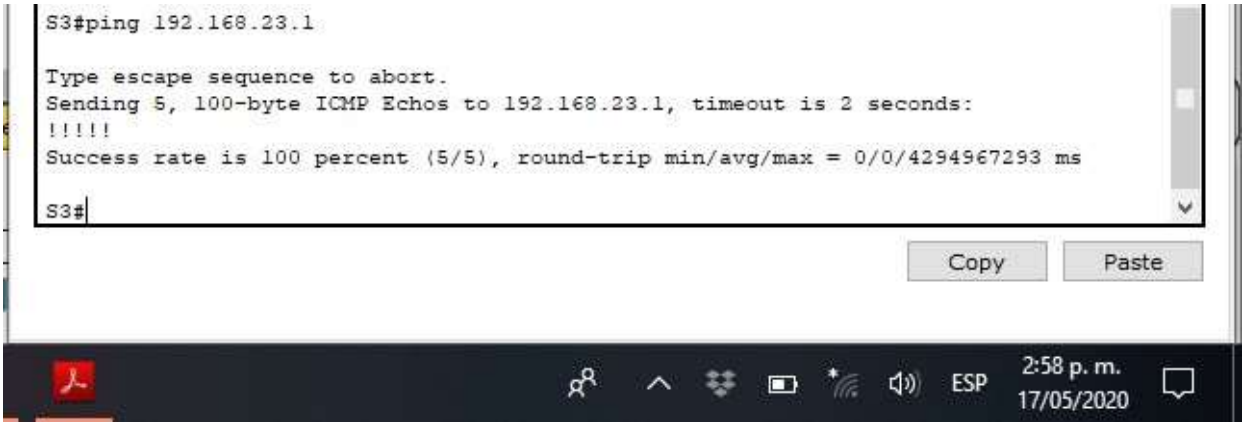


Figure 9. Verificando la conectividad de S1 a R1, dirección VLAN 23

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 13: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	**Asigne todas las redes conectadas directamente.** R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 13. Configurar RIPv2 en el Router 1

Paso 14: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	**Nota: Omitir la red G0/0.** R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 14. Configurar RIPv2 en el Router 2

Paso 15: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2

Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 192.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface 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

Tabla 15. Configurar RIPv2 en el Router 3

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:

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 running-config

Tabla 16. Verificando información de RIP

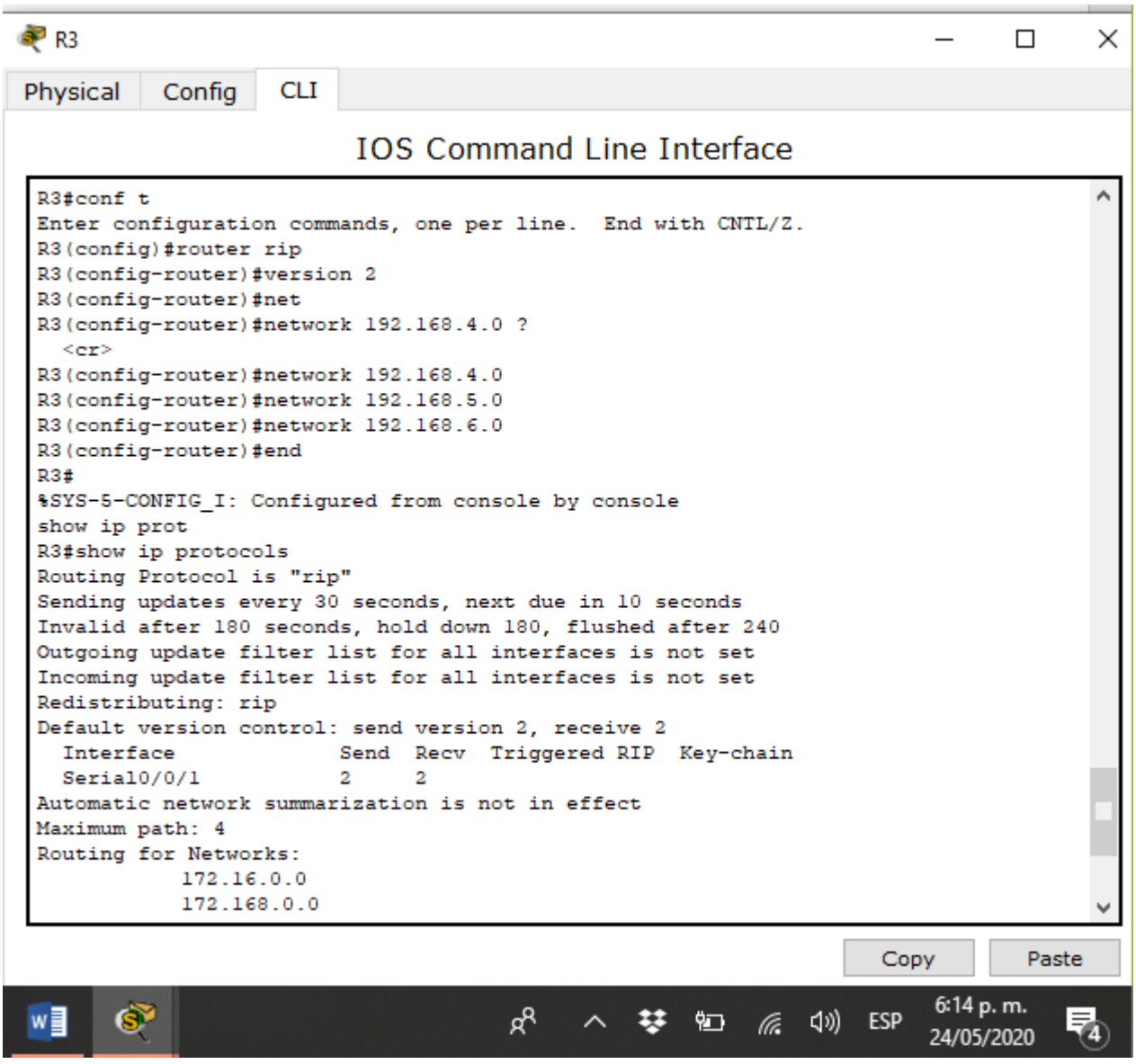


Figure 10. Verificando información de RIP

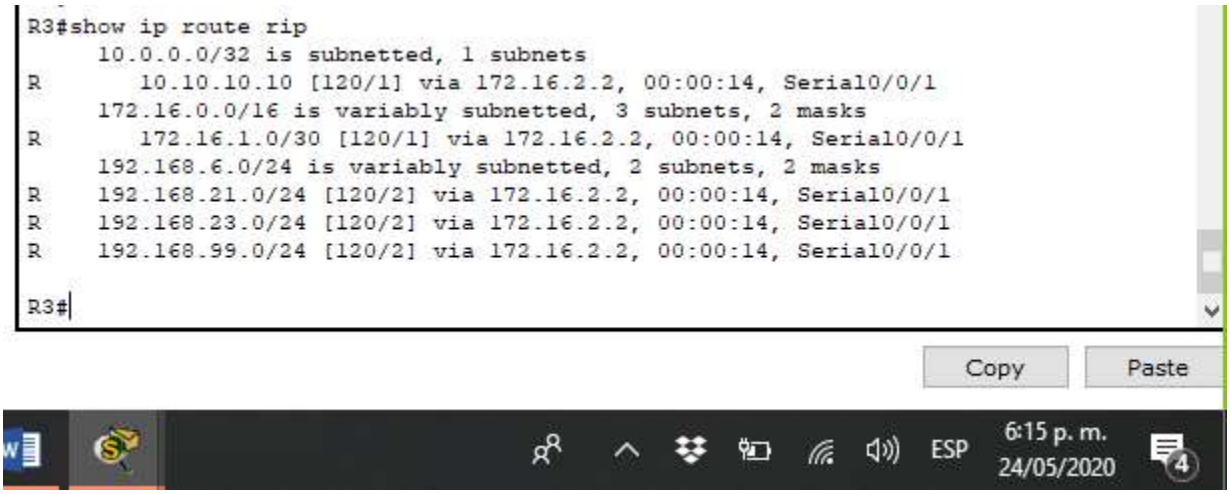


Figure 11. Verificando información de RIP

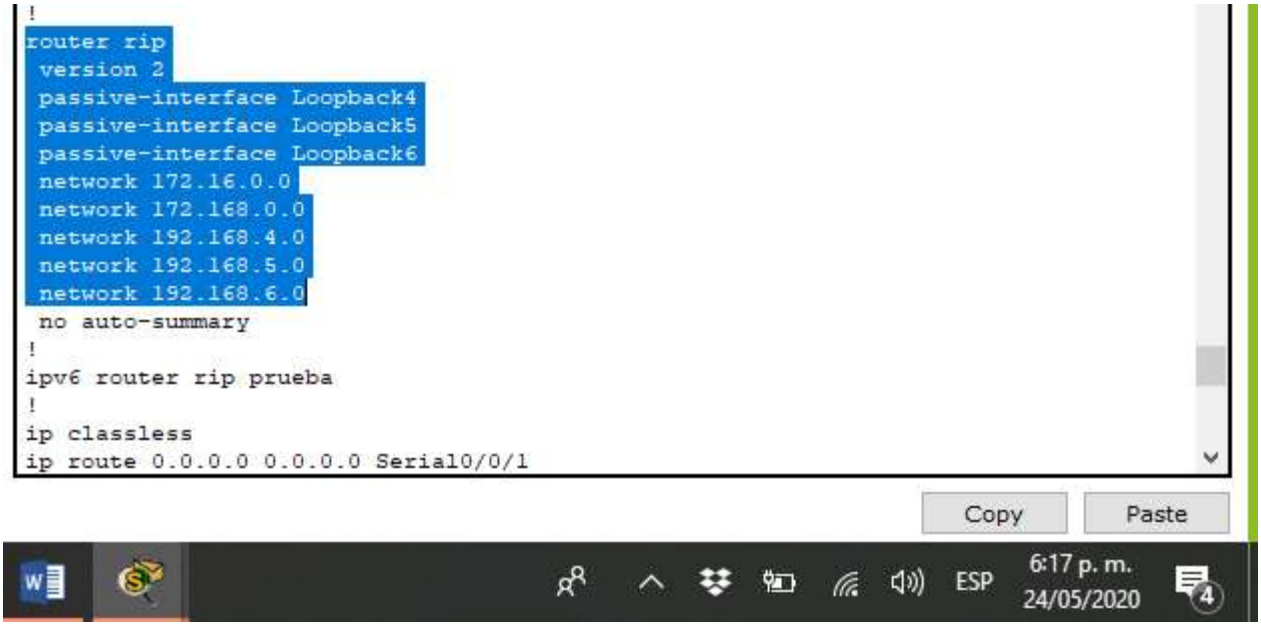


Figure 12. Verificando información de RIP

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	**Nombre: ACCT** **Servidor DNS: 10.10.10.10** **Nombre de dominio: ccna-sa.com** **Establecer el gateway predeterminado** R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

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

Tabla 17. Configurar el Router 1 como servidor de DHCP para las VLAN 21 y 23

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	**Nombre de usuario: webuser** **Contraseña: cisco12345** **Nivel de privilegio: 15** R2(config)#username webuser privilege 15 secret cisco12345

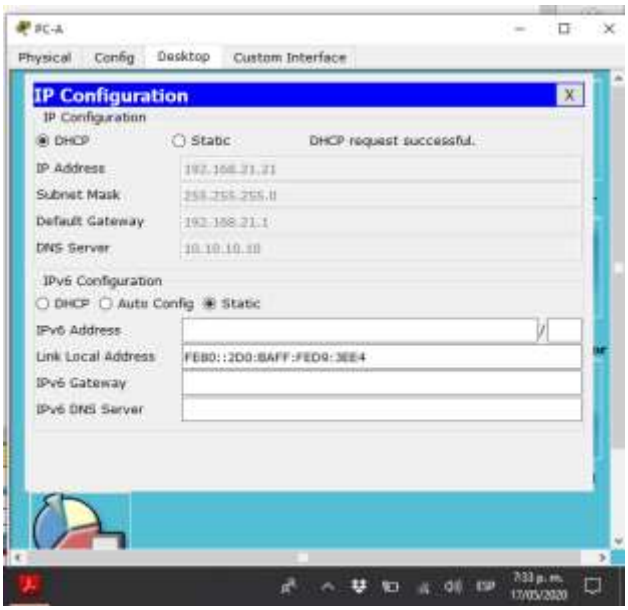
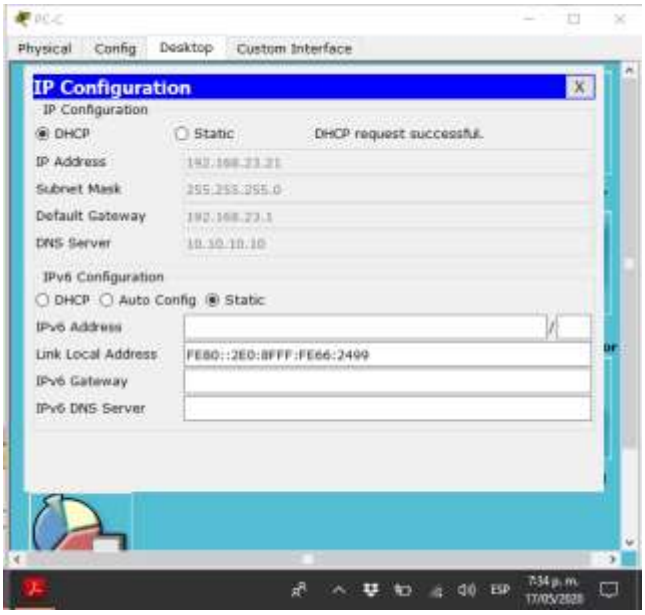
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** ***(no se usa el** 209.165.200**.229** por el rango es de **232** a **238**)* 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	**Lista de acceso: 1** **Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1** **Permitir la traducción de un resumen de las redes LAN (loopback) en el R3** R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** **(**no se usan esas direcciones debido a que el rango ese de **233 a 236** por que la **237** la usa el servidor de internet y la **232 e**l servidor web**)** 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

Tabla 18. Configurar el Router 2 NAT estática y dinámica

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.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figure 13. PC-A con información IP del servidor de DHCP*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Figure 14. PC-C con información IP del servidor de DHCP*

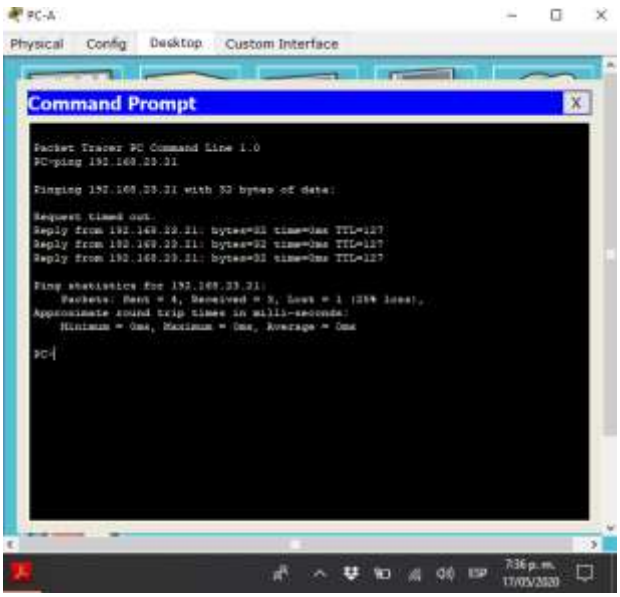
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Figure 15. PC-A hace PING a PC-A*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet trace no soporta el comando ip http server en R2 para poder activar el servidor web

Tabla 19. Verificando el protocolo DCHP y NAT estática

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 19:57:00 17 may 2020
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1(config)#show ntp associations

Tabla 20. Configurando NTP

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

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-cLass ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Tabla 21. Restringir el acceso a las VTY en el Router 2

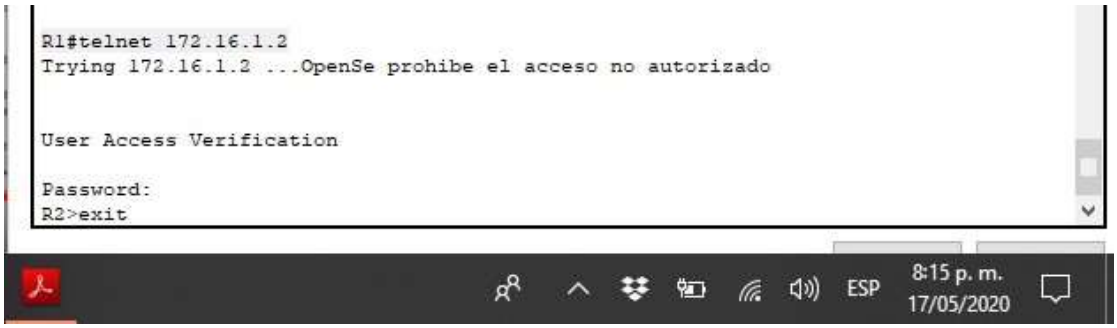


Figure 16. Se verifica que la ACL funcione

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

Descripción del commando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list  *Figure 17. Se verifica las coincidencias recibidas por la lista de acceso*
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. R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Tabla 22. Comando CLI

4.2. 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.

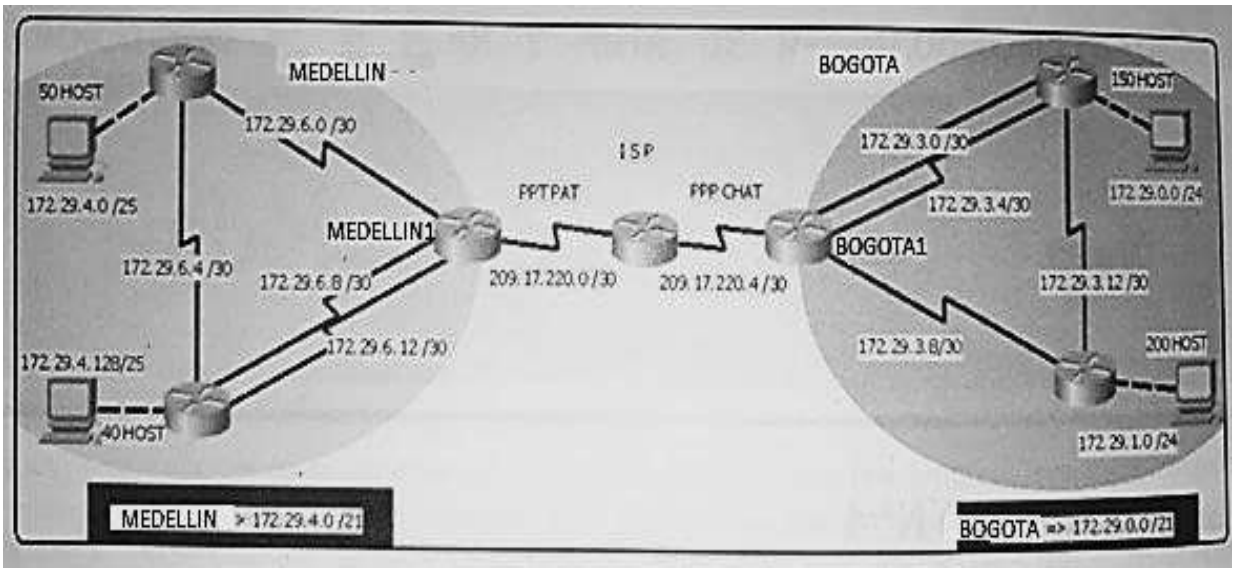


Figure 18. Topología escenario 2

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.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

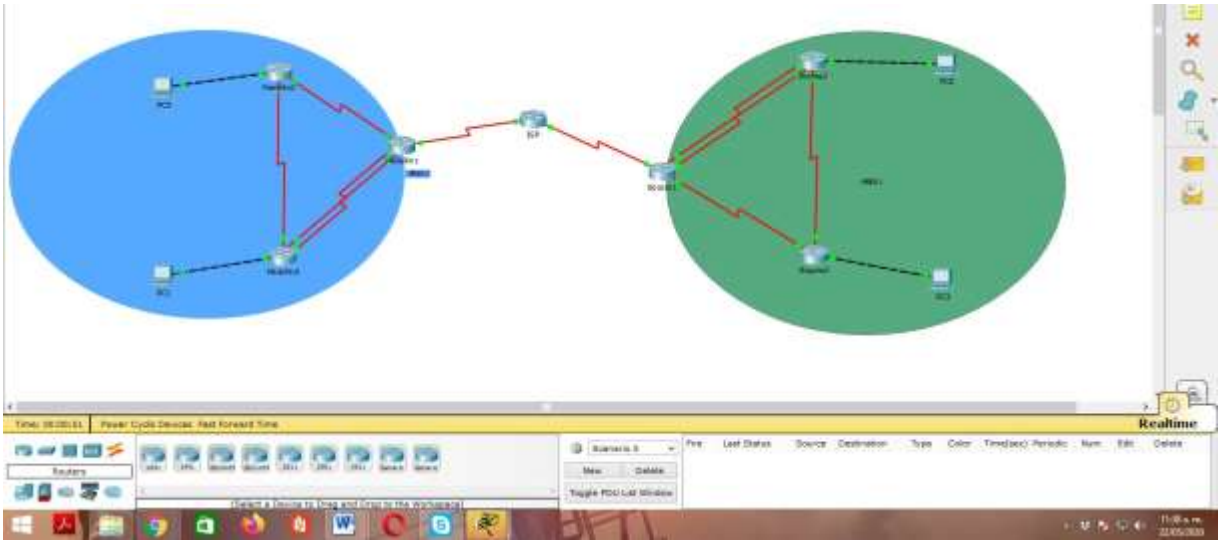


Figure 19. Topología escenario 2 en Packet Tracer

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.

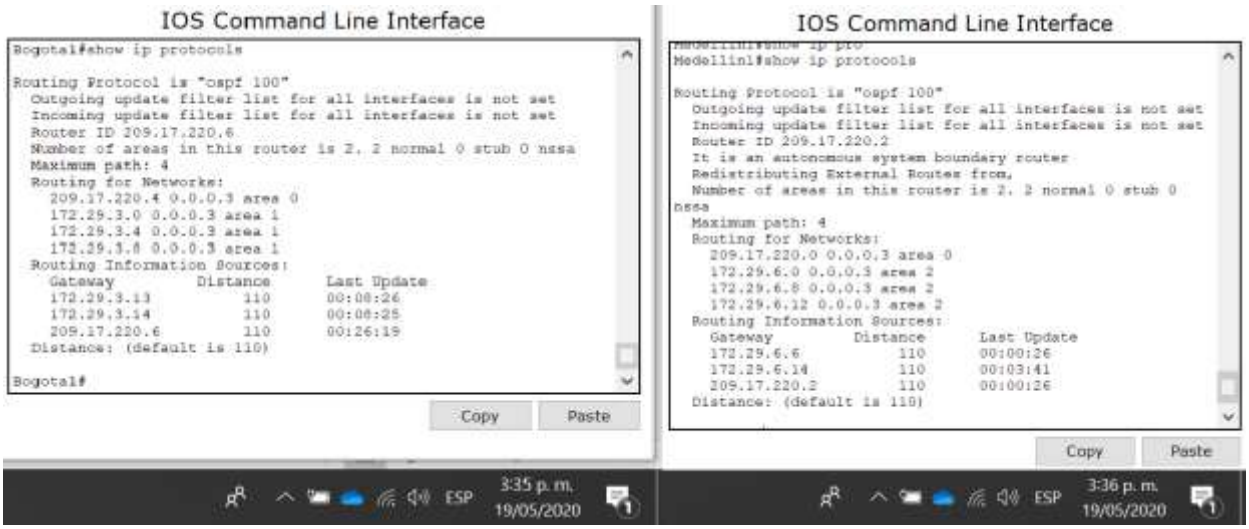


Figure 20. Router Bogota y Medellin

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

Figure 21. Routers de Medellín

Figure 22. Routers de Bogotá

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.

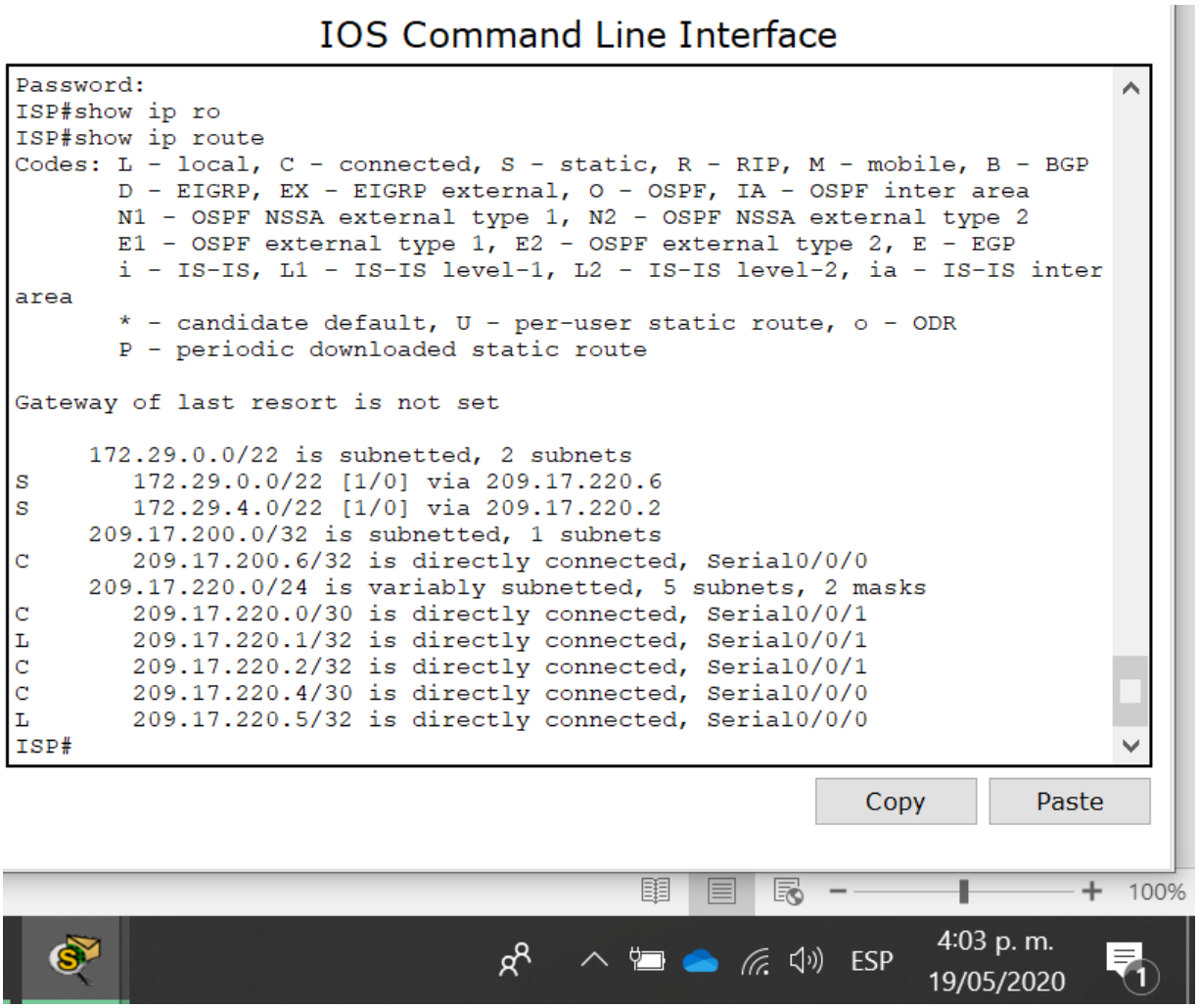


Figure 23. Router ISP con ruta estática a Bogotá y Medellín

Parte 2: Tabla de Enrutamiento.

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

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

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.

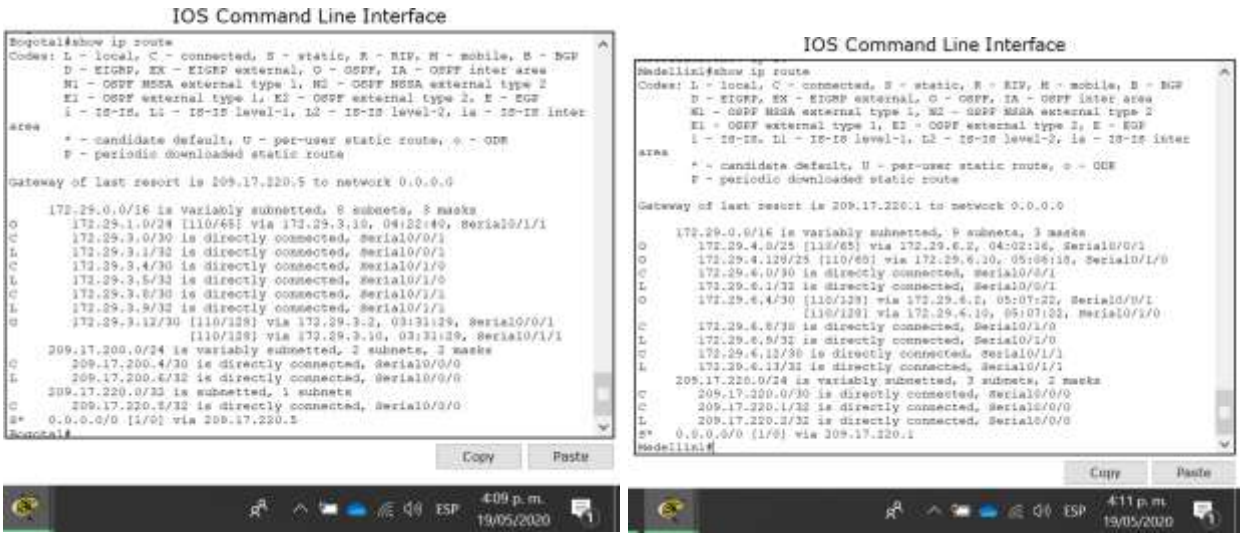


Figure 24. Se visualiza la respuesta de los puntos a, b, c

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

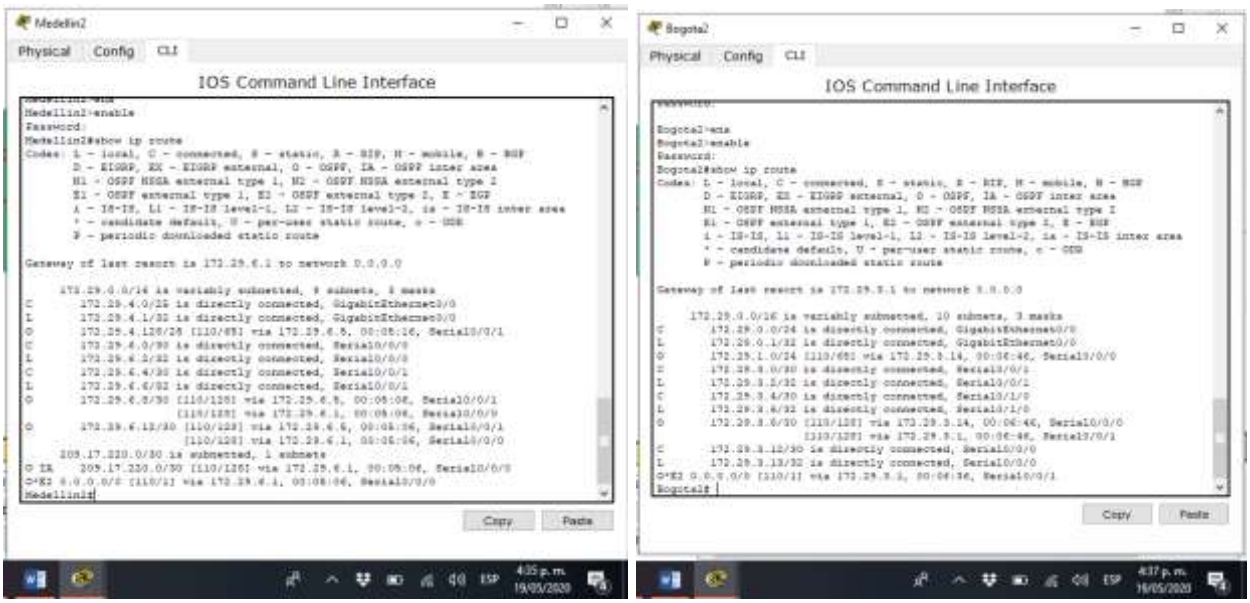


Figure 25. Routers Medellin2 y Bogota2

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

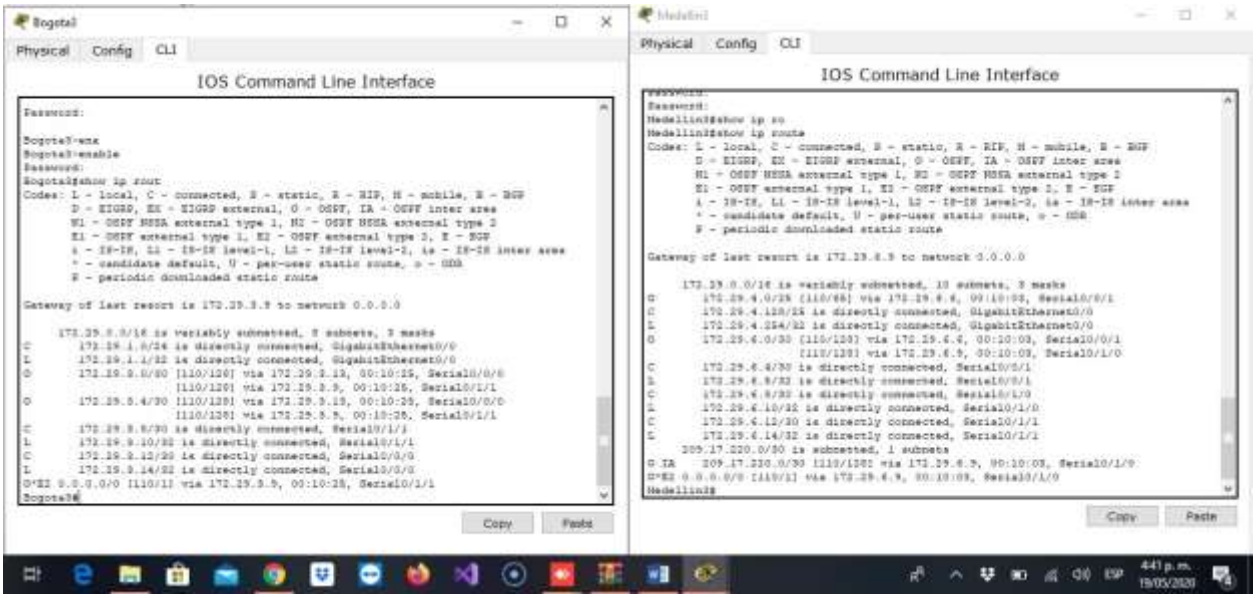


Figure 26. Rutas redundantes

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

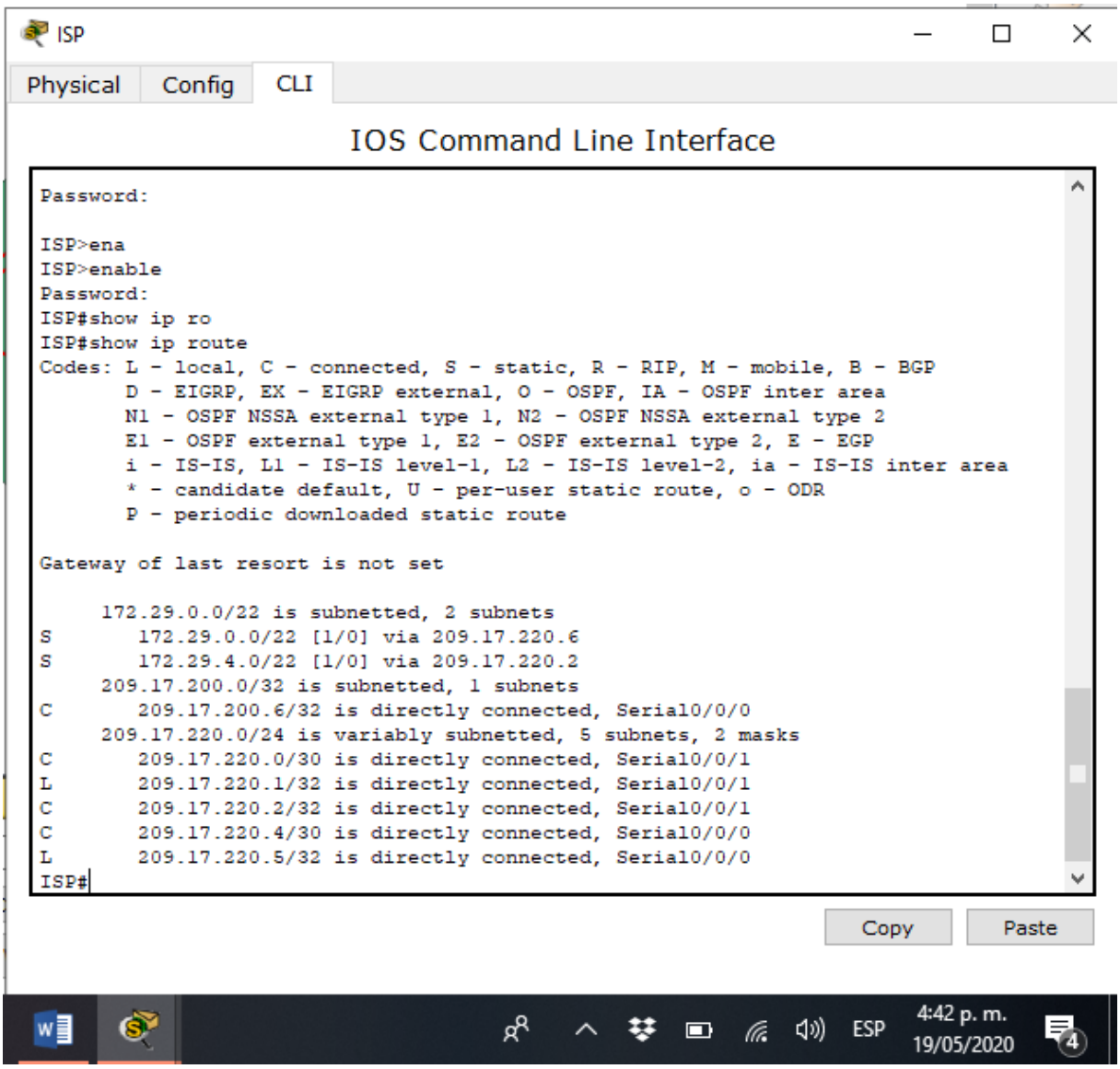


Figure 27. Router ISP

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.

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

Tabla 23. Interfaces de los Routers que se desactivan

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.

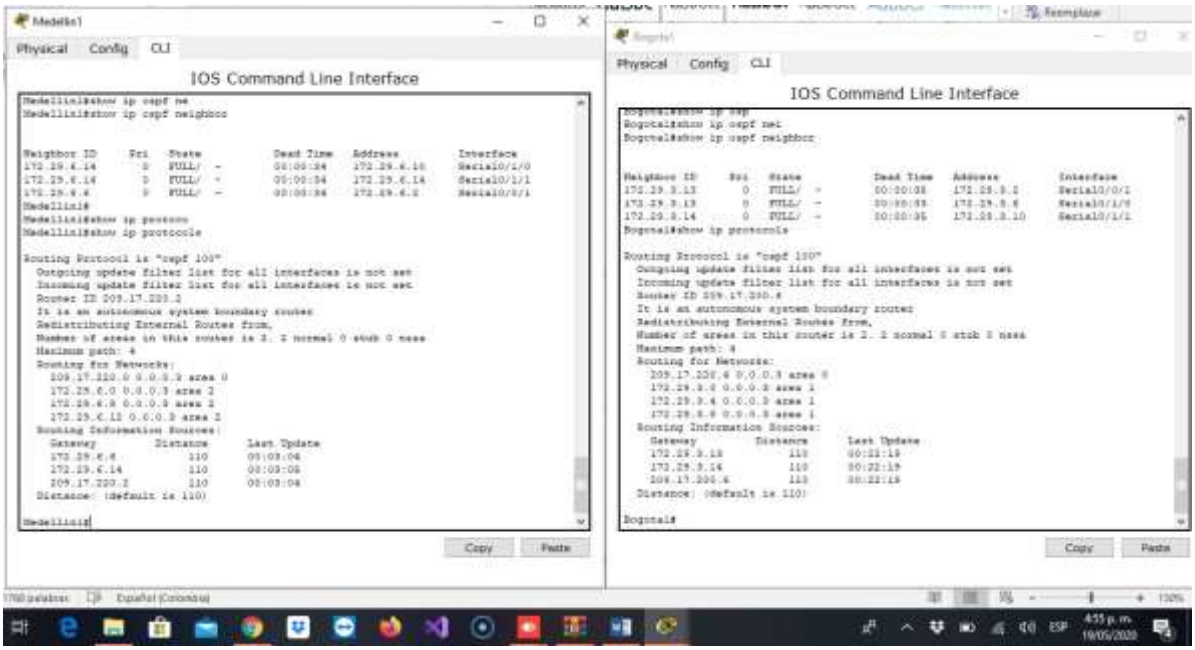


Figure 28. Opciones de enrutamiento configuradas en los Routers

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.

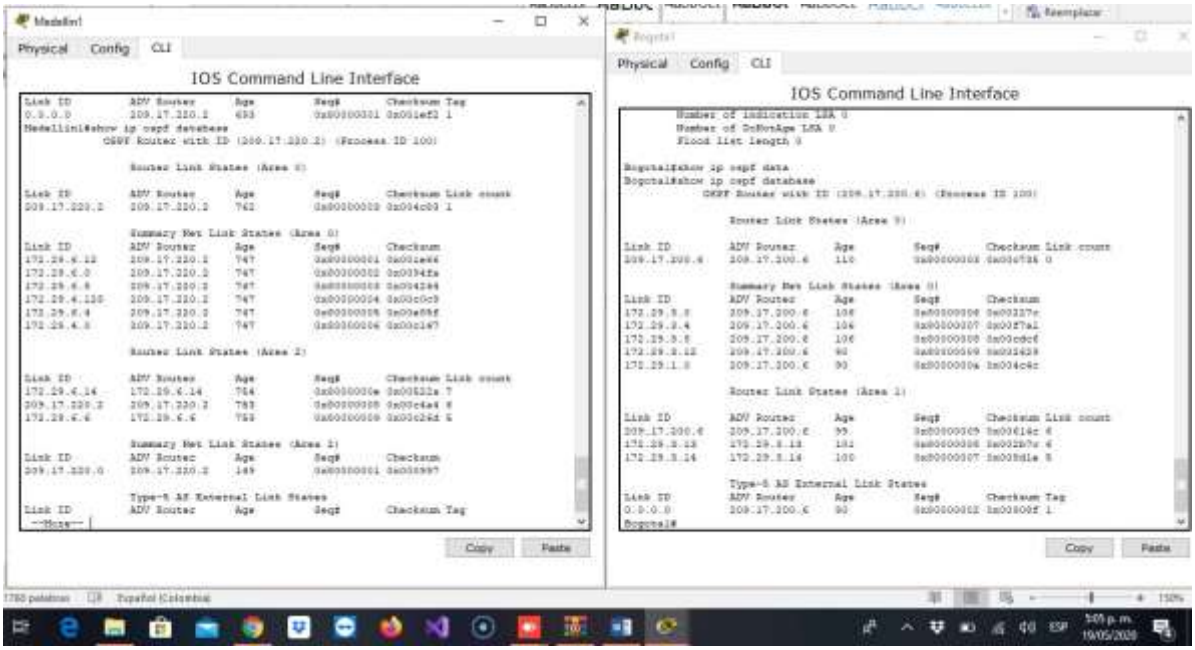


Figure 29. Base de datos OSPF de cada Router

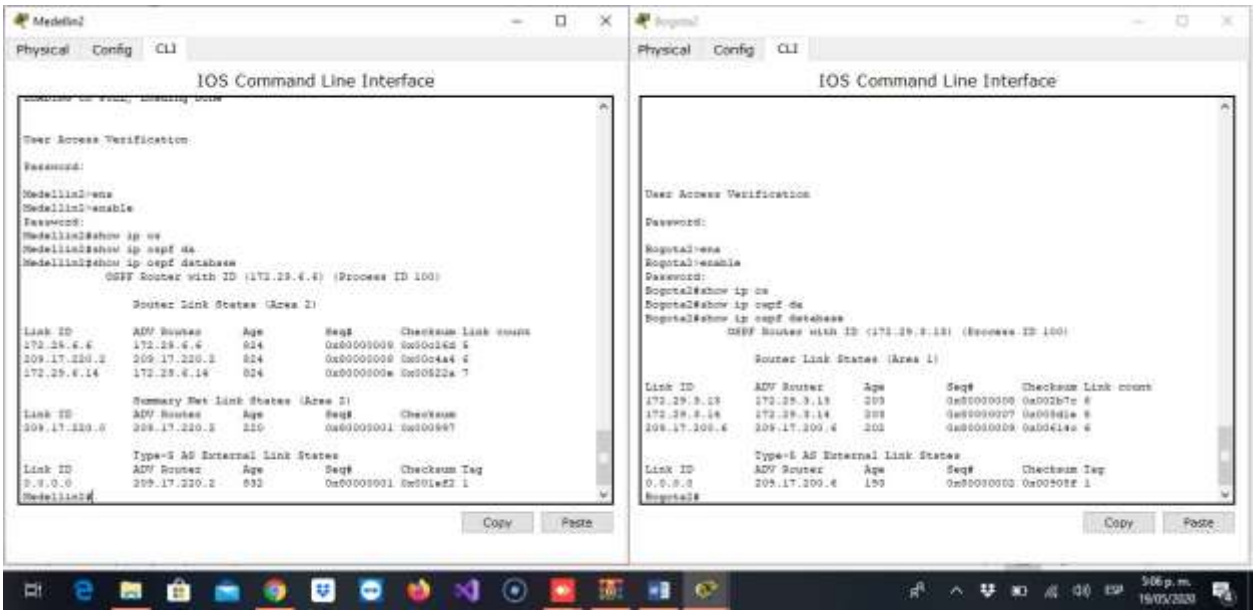


Figure 30. Base de datos OSPF de cada Router

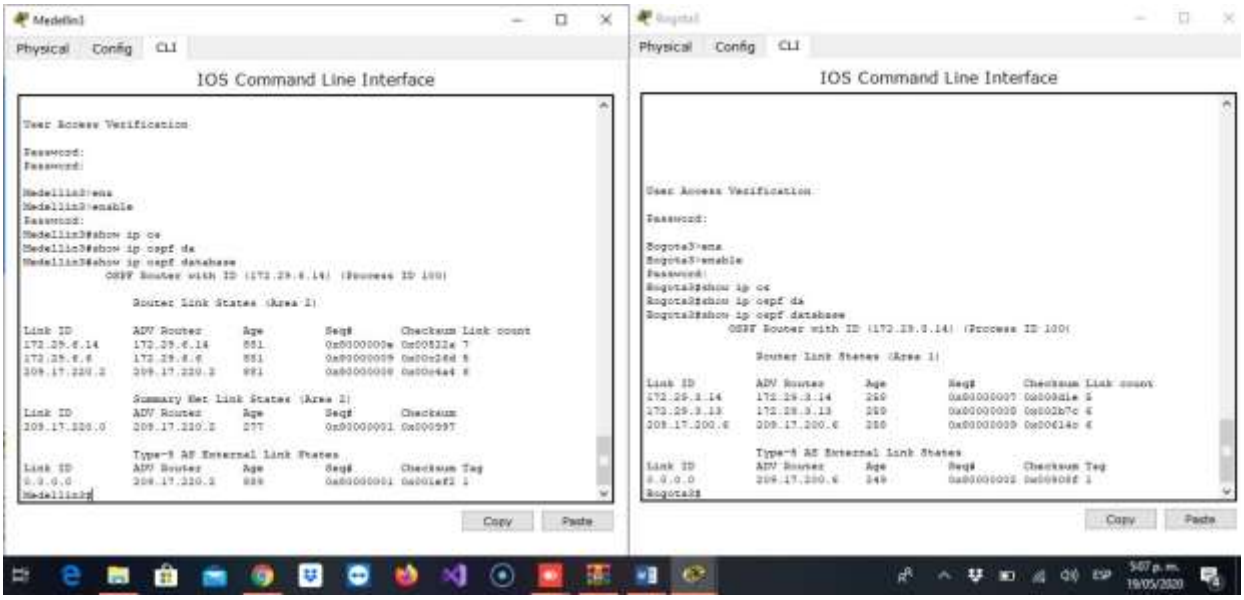


Figure 31. Base de datos OSPF de cada Router

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

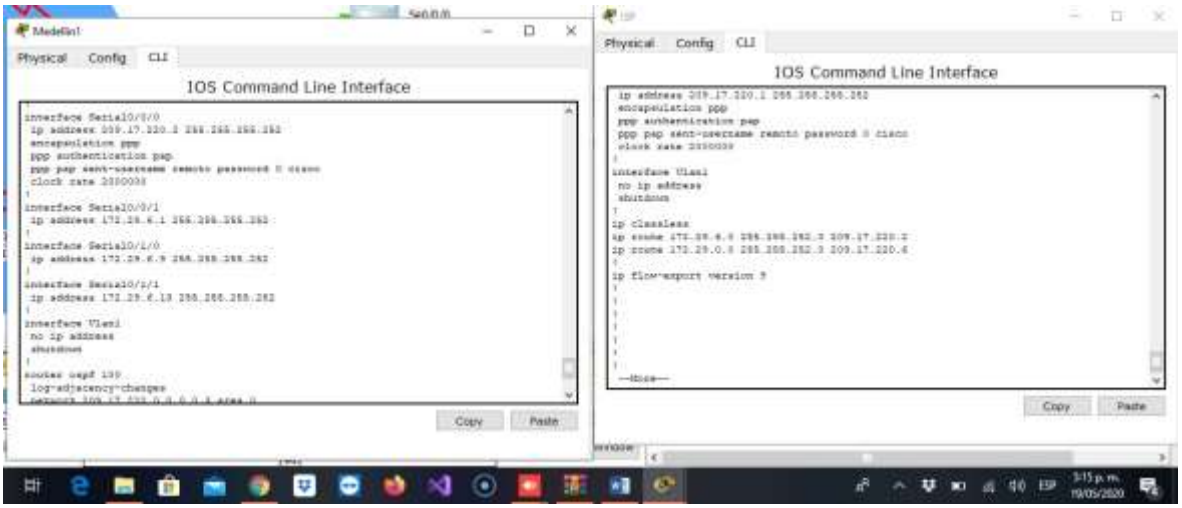


Figure 32. Autenticación PAP

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

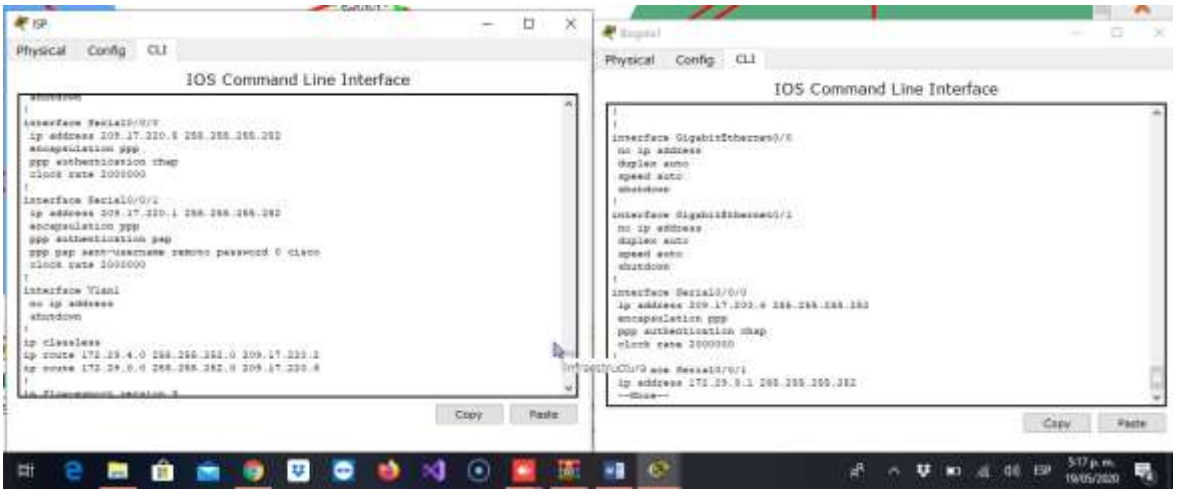


Figure 33. Autenticación CHAP

Parte 6: Configuración de PAT.

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

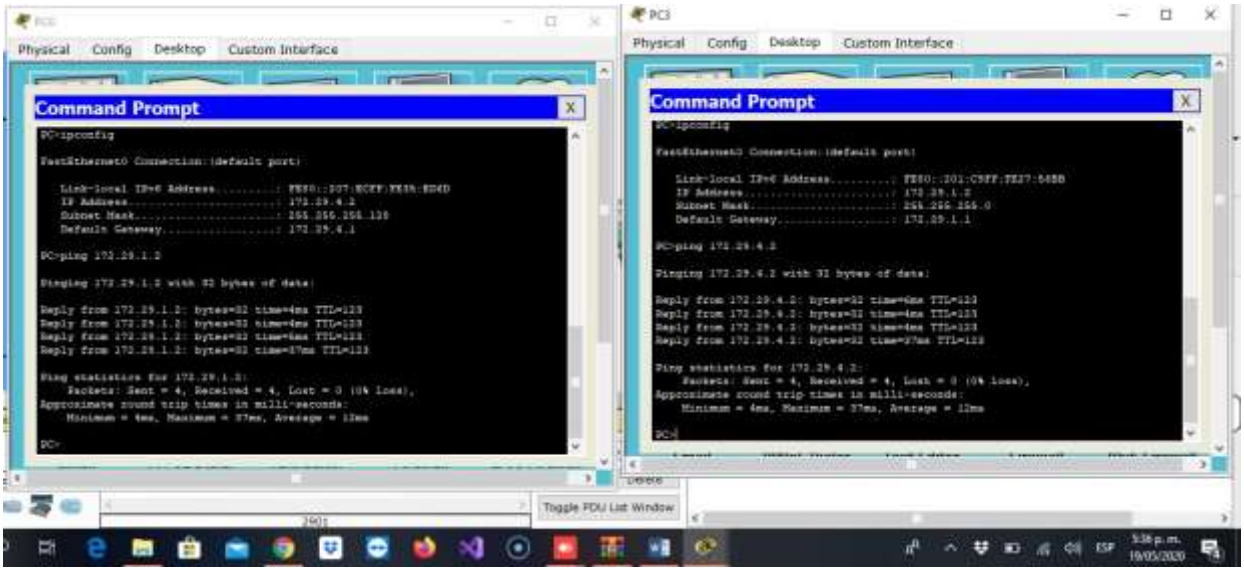


Figure 34. Ping desde PC-0 a PC-3 sin configuración NAT

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.

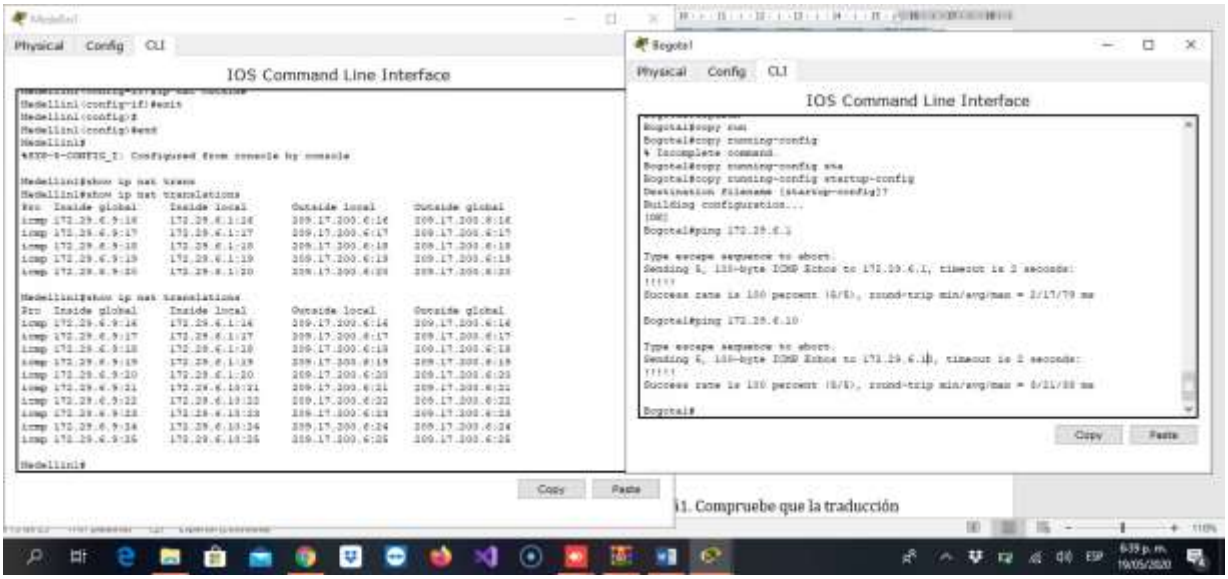


Figure 35. Configuración NAT en el Router Medellín 1

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.

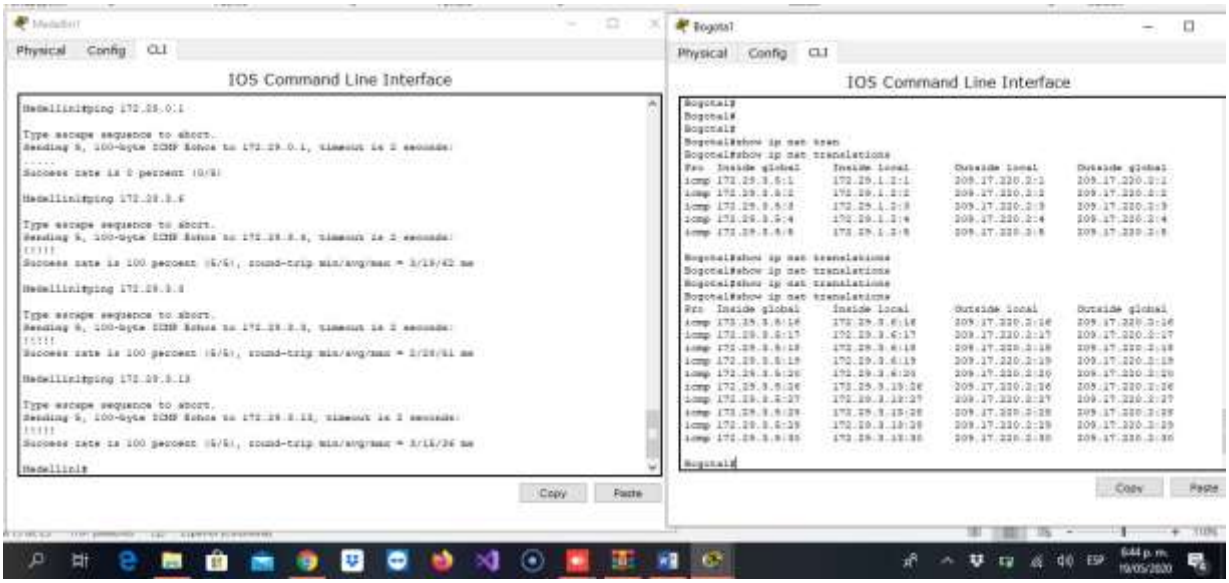


Figure 36. Configuración NAT en el Router Bogotá 1

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.

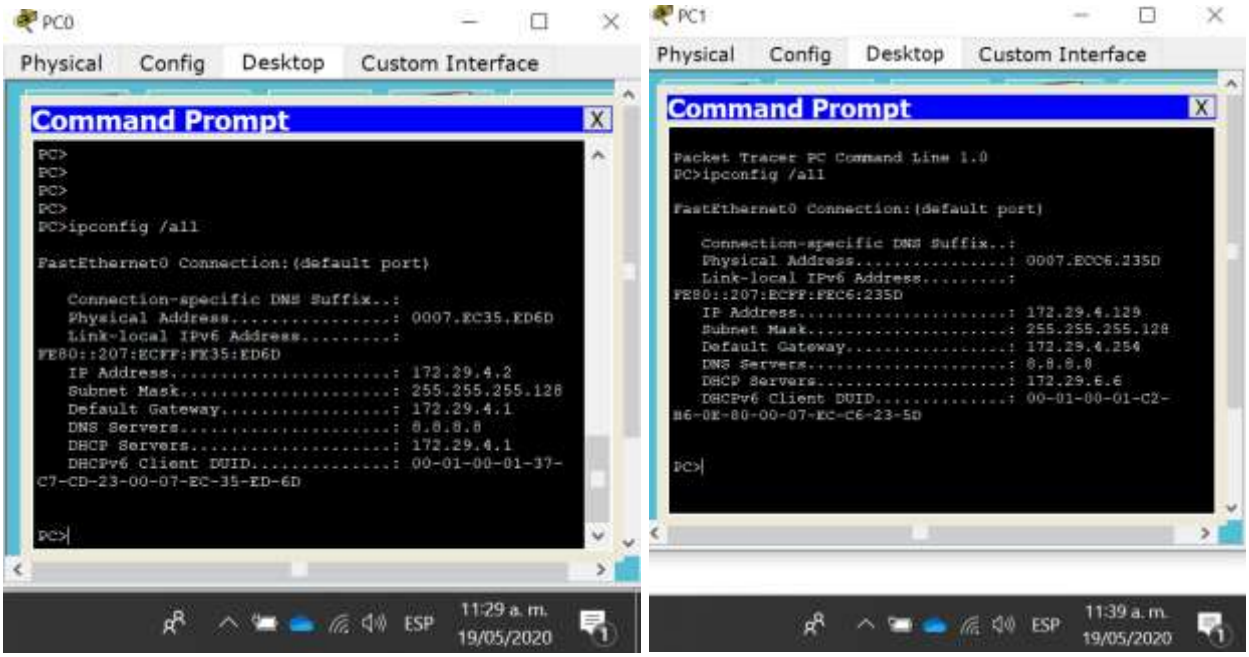


Figure 37. Servicio DHCP

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

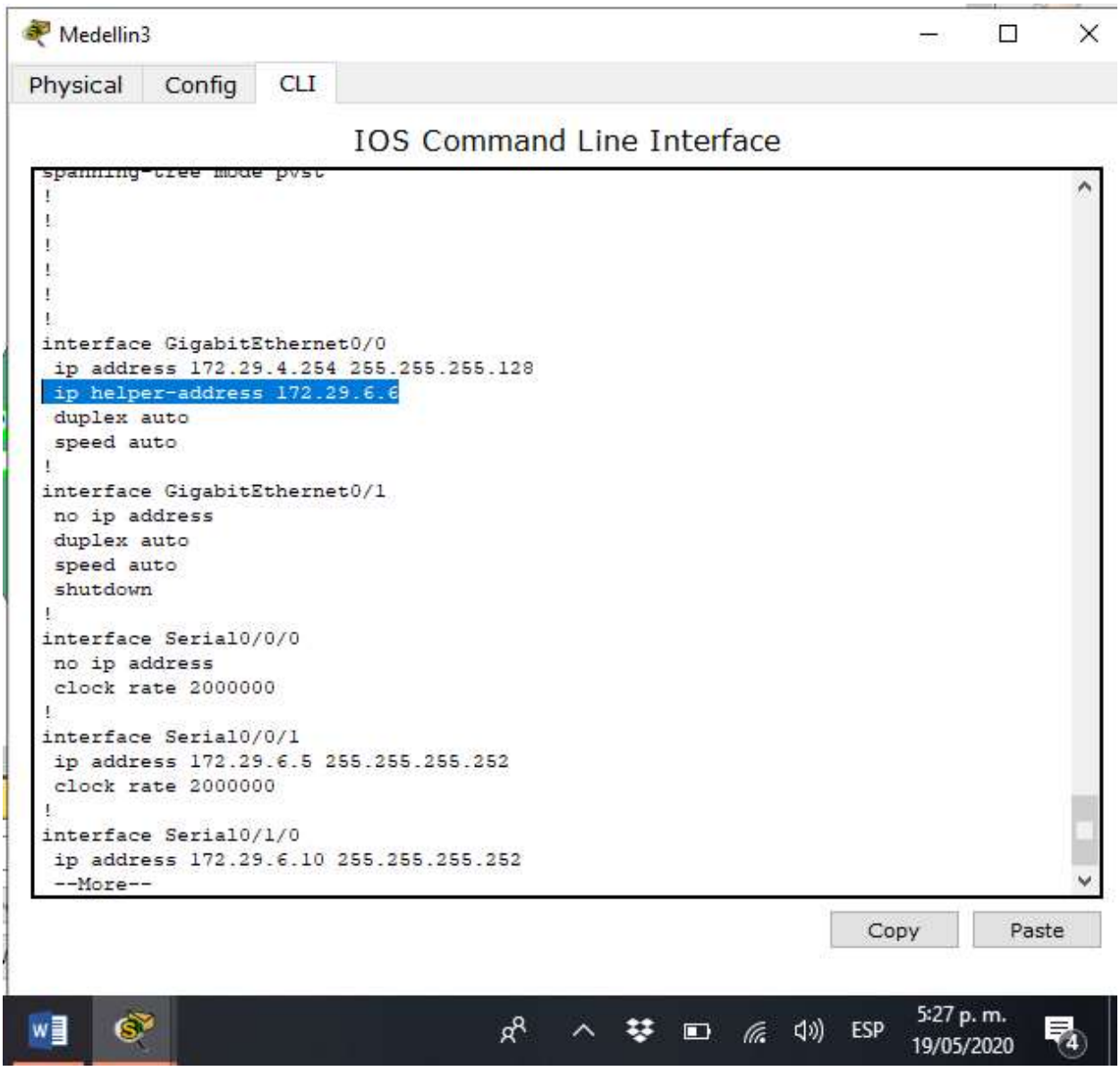


Figure 38. Verificando Router Medellín 3

c. Configurar la red Bogotá2 y Bogotá3 donde el Router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

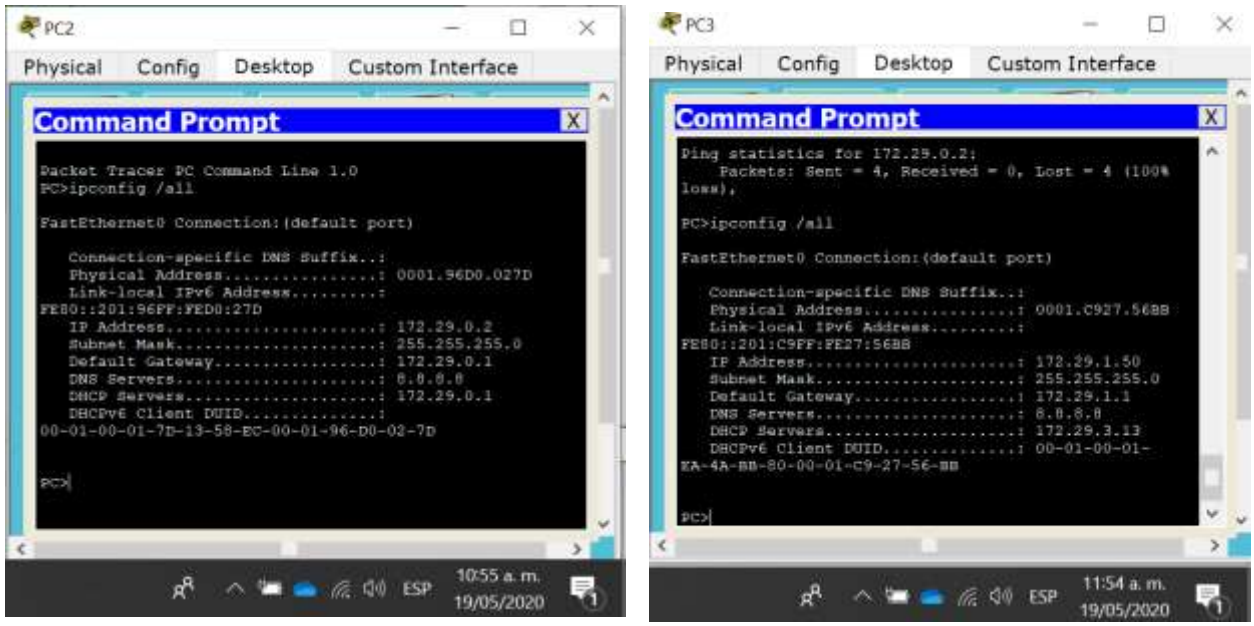


Figure 39. Servidor DHCP

d. Configure el Router Bogotá 3 para que habilite el paso de los mensajes Broadcast hacia la IP del Router Bogotá2.

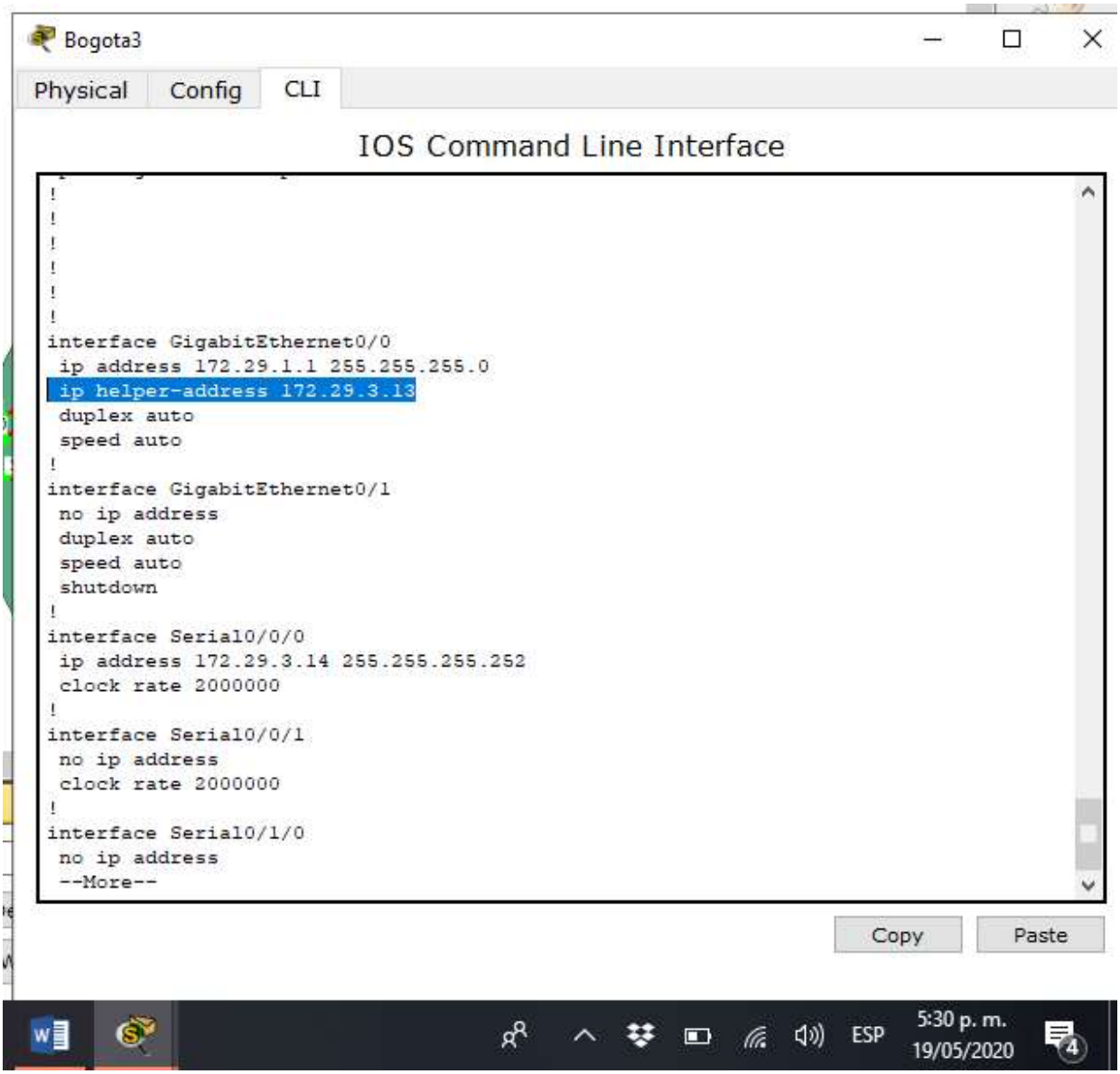


Figure 40. Verificando Router Bogotá 3

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

Comandos usados en el escenario 2

Router ISP

```
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#inter
ISP(config)#interface s
ISP(config)#interface serial 0/0/0
ISP(config-if)#ip addr
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#no shu
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#inter
ISP(config)#interface s
ISP(config)#interface serial 0/0/1
ISP(config-if)#ip add
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#no shu
ISP(config-if)#no shutdown
ISP(config-if)#exit

ISP(config)#route
ISP(config)#router os
ISP(config)#router ospf 100
ISP(config-router)#net
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
```

ISP(config)#interface serial 0/0/1
ISP(config-if)#en
ISP(config-if)#encapsulation ppp
ISP(config-if)#pp
ISP(config-if)#ppp au
ISP(config-if)#ppp authentication pap
ISP(config-if)#no shut
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#user
ISP(config)#username remoto password cisco

ISP(config-if)#ppp pap sent-username remoto password cisco
ISP(config)#username Bogota1 password class
ISP(config)#interface serial 0/0/0
ISP(config-if)#enc
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#exit

Bogota 1
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#inter
Bogota1(config)#interface s
Bogota1(config)#interface serial 0/0/0

```
Bogota1(config-if)#ip add
Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252
Bogota1(config-if)#no shu
Bogota1(config-if)#no shutdown
Bogota1(config)#interface serial 0/0/1
Bogota1(config-if)#ip add
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#no shu
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/1/0
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/1/1
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
```

```
Bogota1(config)#username ISP password class
Bogota1(config)#interface serial 0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#ip add
Bogota1(config-if)#ip address 209.17.200.6 255.255.255.252
Bogota1(config-if)#no shu
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
```

```
Bogota1(config)#router ospf 100
Bogota1(config-router)#netw
Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 0
Bogota1(config-router)#
01:13:00: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.5 on Serial0/0/0 from
LOADING to FULL, Loading Done
Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area Bogota1(config-
router)#network 209.17.220.4 0.0.0.3 area Bogota1(config-router)#
Bogota1(config-router)#
Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area Bogota1(config-
router)#network 172.29.3.0 0.0.0.3 area 1
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota1(config-router)#exit

Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
Bogota1(config)#router ospf 100
Bogota1(config-router)#default-information originate

Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
Bogota1(config)#ip nat inside source list 1 interface s0/1/0 overload
Bogota1(config)#inter s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/0/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
```

```
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#exit
Bogota1(config)#end
```

Bogota 2

```
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#inter
Bogota2(config)#interface ser
Bogota2(config)#interface serial 0/0/0
Bogota2(config-if)#ip add
Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota2(config-if)#no sh
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface serial 0/0/1
Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface serial 0/1/0
Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface gigabitEthernet 0/0
Bogota2(config-if)#ip add
Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota2(config-if)#no shutdown
```

```
Bogota2(config-if)#exit

Bogota2(config)#router ospf 100
Bogota2(config-router)#
Bogota2(config-router)#net
Bogota2(config-router)#network 172.29.3.0 0.0.0.3 area 1
Bogota2(config-router)#network 172.29.3.0 0.0.0.3 area 1
01:21:21: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/0/1 from
Bogota2(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota2(config-router)#
01:21:36: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/1/0 from
LOADING to FULL, Loading Done
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 1
Bogota2(config-router)#network 172.29.0.1 0.0.0.255 area 1


Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#ip dh
Bogota2(config)#ip dhcp poo
Bogota2(config)#ip dhcp pool LAN_1
Bogota2(dhcp-config)#ipadd
Bogota2(dhcp-config)#ip add
Bogota2(dhcp-config)#ip ad
Bogota2(dhcp-config)#netw
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#de
Bogota2(dhcp-config)#default-router 172.29.0.1
Bogota2(dhcp-config)#dns
Bogota2(dhcp-config)#dns-server 8.8.8.8
```

Bogota2(dhcp-config)#exit

Bogota 3

Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Bogota3(config)#
Bogota3(config)#
Bogota3(config)#inter
Bogota3(config)#interface s
Bogota3(config)#interface serial 0/0/0
Bogota3(config-if)#ip add
Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota3(config-if)#no sh
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#interface serial 0/1/1
Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#intr
Bogota3(config)#inte
Bogota3(config)#interface gi
Bogota3(config)#interface gigabitEthernet 0/0
Bogota3(config-if)#ip add
Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota3(config-if)#no shu

Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit

Bogota3(config)#router ospf 100
Bogota3(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.3.8 0.0.0.3 area 1
00:53:59: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/1/1 from LOADING to FULL, Loading Done
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 1
00:54:17: %OSPF-5-ADJCHG: Process 100, Nbr 172.29.3.13 on Serial0/0/0 from LOADING to FULL, Loading Done
Bogota3(config-router)#network 172.29.1.1 0.0.0.255 area 1

Medellin 1
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#onter
Medellin1(config)#inter
Medellin1(config)#interface s
Medellin1(config)#interface serial 0/0/0
Medellin1(config-if)#ip add
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#nos
Medellin1(config-if)#no shu
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit

```
Medellin1(config)#interface serial 0/0/1
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/1/0
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/1/1
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit

Medellin1(config)#router ospf 100
Medellin1(config-router)#net
Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 0
Medellin1(config-router)#net
01:41:38: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.5 on Serial0/0/0 from
LOADING to FULL, Loading Done
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 2
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 2
Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 2
Medellin1(config-router)#exit

Medellin1 (config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Medellin1 (config)#router ospf 100
Medellin1(config-router)#default-information originate

Medellin1(config)#interface serial 0/0/0
Medellin1(config-if)#en
```

Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
ppp aut
Medellin1(config-if)#ppp authentication pa
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#no sh
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#use
Medellin1(config)#username remoto password cisco
Medellin1(config)#interface serial 0/0/0
Medellin1(config-if)#ppp pap sent-username remoto password cisco

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

Medellin1(config)#end

Medellin 2

Medellin2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Medellin2(config)#ip add

Medellin2(config)#inter

Medellin2(config)#interface ser

Medellin2(config)#interface serial 0/0/0

Medellin2(config-if)#ip add

Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252

Medellin2(config-if)#no shutdown

Medellin2(config-if)#exit

Medellin2(config)#interface serial 0/0/1

Medellin2(config-if)#ip address 172.29.6.6 255.255.255.252

Medellin2(config-if)#no shutdown

Medellin2(config-if)#exit

Medellin2(config)#interface giga

Medellin2(config)#interface gigabitEthernet 0/0

Medellin2(config-if)#ip address 172.29.4.1 255.255.255.0

Medellin2(config-if)#no shutdown

Medellin2(config-if)#exit

Medellin2(config)#

Medellin2(config)#router ospf 100

Medellin2(config-router)#net

Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 2

Medellin2(config-router)#

01:43:50: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.2 on Serial0/0/0 from LOADING to FULL, Loading Done

Medellin2(config-router)#
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 2
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 2
Medellin2(config-router)#exit

Medellin 3

Medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#interface serial 0/0/1
Medellin3(config-if)#ip add
Medellin3(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin3(config-if)#no shut
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface serial 0/1/0
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface serial 0/1/1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface gi
Medellin3(config)#interface gigabitEthernet 0/0
Medellin3(config-if)#ip address 172.29.4.254 255.255.255.128
Medellin3(config-if)#no shu
Medellin3(config-if)#no shutdown

Medellin3(config)#router ospf 100
Medellin3(config-router)#net
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 2
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 2
01:45:53: %OSPF-5-ADJCHG: Process 100, Nbr 172.29.6.6 on Serial0/0/1 from LOADING to FULL, Loading Done
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 2
Medellin3(config-router)#
01:46:29: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.2 on Serial0/1/0 from LOADING to FULL, Loading Done
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 2
Medellin3(config-router)#
01:47:04: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.2 on Serial0/1/1 from LOADING to FULL, Loading Done
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 2
Medellin3(config-router)#exit

CONCLUSIONES

Las habilidades y competencias que debe adquirir un ingeniero de redes son de vital importancia para el manejo adecuado de las redes convergentes. Los dos escenarios planteados por este documento permiten comprender la operación de cada uno de los comandos de configuración con el fin de dar la solución más eficaz a las necesidades planteadas.

La topología de la red es una ayuda significativa al momento de implementar una red y de igual manera para hallar de una manera más ágil y precisa las fallas que se lleguen a presentar. Es decir, al momento de iniciar y comprender las necesidades planteadas por cada ejercicio, es preciso mirar detalladamente la topología de cada escenario con el fin de configurarla.

BIBLIOGRAFÍA

Configure NAT to Enable Communication Between Overlapping Networks. (s. f.). Cisco. Recuperado 20 de mayo de 2020, de https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Be.html

Ejemplo de Configuración de VLANs en Puntos de Acceso Aironet. (s. f.). Cisco. Recuperado 20 de mayo de 2020, de https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-lan-wlan/69773-vlan-ap-config.html

Gómez, J. A. (2010). Servicios en red. Editex. Recuperate of https://books.google.es/books?hl=es&lr=&id=vhit3ZmGQPsC&oi=fnd&pg=PA2&dq=configurar+una+red&ots=Tps7Ueya24&sig=kCdAW7bnB15PZV-cgwWDw8rLpJA#v=onepage&q=configurar%20una%20red&f=false

Guía de diseño de OSPF. (s. f.). Cisco. Recuperado 20 de mayo de 2020, de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Jesin, A. (2014). Packet Tracer Network Simulator. Packt Publishing Ltd. Recuperate of https://books.google.es/books?hl=es&lr=&id=eVOcAgAAQBAJ&oi=fnd&pg=PT9&dq=cisco+packet+tracer+&ots=bPMOorh5T9&sig=m8dcHYhL0RT9bPZ69-lxd4wu_Lc#v=onepage&q=cisco%20packet%20tracer&f=false