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

DELIA ISABEL MAYORGA MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA “ECBTI”

INGENIERÍA DE SISTEMAS

VALLEDUPAR

2020

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

DELIA ISABEL MAYORGA MUÑOZ

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA PARA OBTENER TITULO DE PROFESIONAL INGENIERIA DE SISTEMA

NILSON ALBEIRO FERREIRA MANZANARES. TUTOR.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA “ECBTI”

INGENIERÍA DE SISTEMAS

VALLEDUPAR

2020

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

En esta oportunidad como estudiantes de la Universidad Nacional Abierta y a Distancias tenemos la oportunidad de desarrollar esta actividad como opción de grado, Para nosotros como futuros profesionales en ingeniería de sistemas, es esencial conocer el funcionamiento de las redes y saber cada uno de los beneficios que nos brindan, las mejoras a la productividad y seguridad al implementarlas.

A continuación desarrollaremos unos estudios de casos que giren entorno en la configuración de redes, se utilizaran los programa para simulación de redes conocidos como CISCO Packet Tracer y GNS3, en donde se distribuirá en dos escenarios, siendo el escenario 1 la configuración de una red pequeña que admita conexiones IPv4 e IPv6 incluyendo configuraciones complementarias y como segundo escenario manejaremos la configuración para interconexión de redes y dispositivos que se encuentran en diferentes puntos geográficos acorde a los lineamientos establecidos para esta interconexión, en donde al finalizar se mostrará de manera satisfactoria las configuraciones asignadas para cada escenario a desarrollar.

PALABRAS CLAVE: IPv4, IPv6, Red, CISCO, Packet Tracer, GNS3, Configuración, Comando, Protocolos.

ABSTRACT

In this opportunity as students of the National Open and Distance University we have the opportunity to develop this activity as a degree option. For us as future professionals in systems engineering, it is essential to know how networks work and to know each of the benefits that they provide us with improvements in productivity and security when implementing them.

Next we will develop some case studies that revolve around the network configuration, the network simulation programs known as CISCO Packet Tracer and GNS3 will be used, where it will be distributed in two scenarios, with scenario 1 being the configuration of a small network that supports IPv4 and IPv6 connections including complementary configurations and as a second scenario we will manage the configuration for interconnection of networks and devices that are in different geographical points according to the guidelines established for this interconnection, where at the end the assigned configurations will be displayed satisfactorily for each scenario to develop.

INTRODUCCIÓN

Vivimos en una era en donde la tecnología abarca la mayoría de nuestro entorno y el día a día de cada uno de nosotros, desde la búsqueda de información en una plataforma en internet hasta lo más profundo de todo aquello que hace que todo esto sea posible de realizar, como, por ejemplo, eso que nos permite conectarnos de una manera física o inalámbrica a todos estos dispositivos informáticos que nos facilitan estos servicios, lo que conocemos hoy en día como una “Red”.

Para nosotros como futuros profesionales en ingeniería de sistemas, es esencial conocer el funcionamiento de las redes y saber cada uno de los beneficios que nos brindan, las mejoras a la productividad y seguridad al implementarlas.

A continuación desarrollaremos unos estudios de casos que giren entorno en la configuración de redes, con ayudas de programas para simulación de redes, en donde se distribuirá en dos escenarios, siendo el escenario 1 la configuración de una red pequeña que admita conexiones IPv4 e IPv6 incluyendo configuraciones complementarias y como segundo escenario manejaremos la configuración para interconexión de redes y dispositivos que se encuentran en diferentes puntos geográficos acorde a los lineamientos establecidos para esta interconexión.

OBJETIVOS

Objetivo general.

Desarrollar de manera exitosa los casos de estudios comprendidos en la prueba de habilidades CCNA1: CCNA R&S: Introduction to Networks y CCNA2: CCNA R&S: Routing and Switching.

Objetivos especifico.

- Configurar la seguridad de switches y routing entre VLAN.
- Identificar protocolos de configuración de hosts dinámicos (DHCP), NAT, ACL, NTP.
- Identificar direccionamientos IP y protocolos de enrutamiento.

1. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1.1 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.

Topología

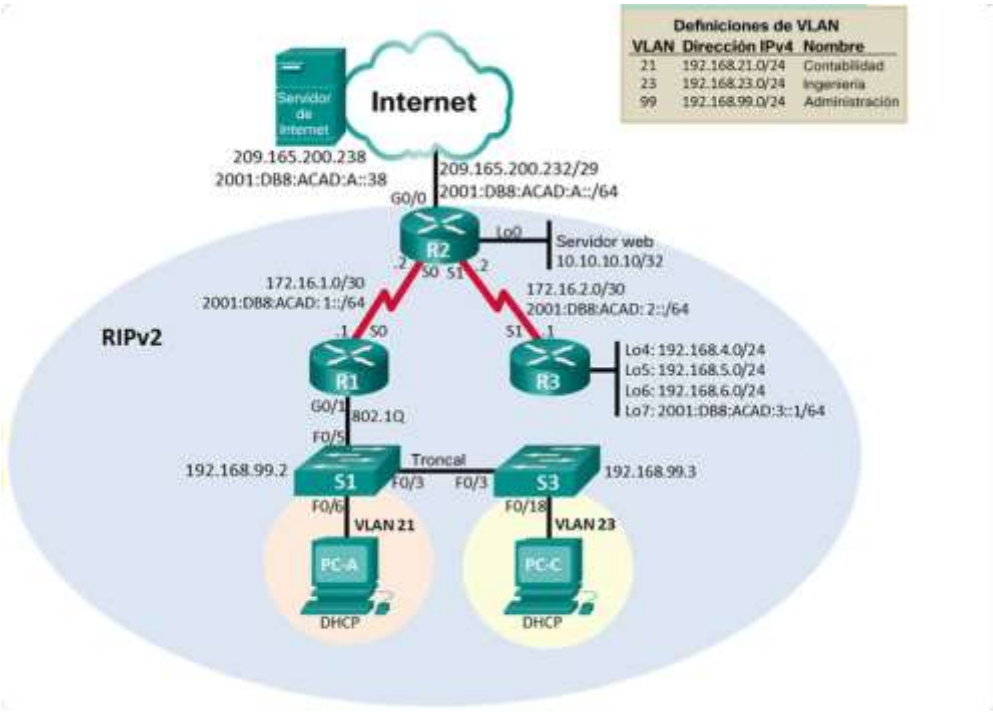

Figura 1. Topología escenario 1.

Parte 1: Inicializar dispositivos.

Damos inicio al Paso 1 en donde procederemos realizar las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tabla 1. Paso 1. Inicializar y volver a cargar los routers y los switches.

Parte 2: Configurar los parámetros básicos de los dispositivos.

Paso 1: Configurar la computadora de Internet.

Debemos realizar la respectiva configuración del servidor de Internet en donde usaremos la siguiente información:

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238/29
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:db8:acad:a::1

Tabla 2. Paso 1. Configurar la computadora de Internet.

Paso 2: Configurar R1.

Para realizar esta configuración procedemos a asignar un nombre al dispositivo para su identificación, incluyendo los siguientes datos de configuración:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz.
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 #ip route 0.0.0.0 0.0.0.0 s2/1 Configurar una ruta IPv6 predeterminada de S0/0/0 ipv6 route ::/0 s2/1

Tabla 3. Paso 2. Configurar R1, especificación.

Configuración	Especificación	Comando de verificación
Desactivar la búsqueda DNS	no ip domain-lookup	R1# show run (Buscar: no ip domain-lookup)
Nombre del router	hostname R1	(Buscar : R1> or R1# command prompt)
Contraseña de exec privilegiado cifrada	enable secret class	R1> enable (Escribir en modo usuario)
Contraseña de acceso a la consola	line con 0 password cisco login	R1# exit (Escribir en privilegiado)
Contraseña de acceso Telnet	line vty 0 4 password cisco login	R1# show run
Cifrar las contraseñas de texto no cifrado	service password-encryption	R1# show run
Mensaje MOTD	banner motd @ Se prohíbe el acceso no autorizado @	(verificar banner en el login)
Interfaz S0/0/0	interface s0/0/0 description Connection to R2 ip address 172.16.12.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:12::1/64 clock rate 128000 no shutdown	R1# show interface S0/0/0 R1# show controllers S0/0/0
Rutas predeterminadas	ip route 0.0.0.0 0.0.0.0 s0/0/0 ipv6 route ::/0 s0/0/0	R1# show ip route R1# show ipv6 route.

Tabla 4. Paso 2. Configurar R1, comando de verificación.

Paso 3. Configurar R2.

Para realizar esta configuración procedemos a asignar un nombre al dispositivo para su identificación, incluyendo los siguientes datos de configuración:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción. Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Tabla 5. Paso 3. Configurar R2.

Configuracion	Especificacion	Comando de verificacion
Deshabilitar busqueda DNS		R2# show run
Nombre	host R2	(Observar el prompt)
Conntraseñas encriptadas	enable secret class	R2> enable
Contraseña de consola	line con 0 password cisco login	R2# exit
Contraseña de telnet	line vty 0 4 password cisco login	R2# show run
Encriptar las contraseñas	service password-encryption	R2# show run
Habilitar server http	ip http server	R2# show run | include http
MOTD banner	banner motd @ Se prohíbe el acceso no autorizado @	(Verificar banner en el login)
Interfaz S0/0/0	interface s0/0/0 description Connection to R1 ip add 172.16.12.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:12::2/64 no shutdown	R2# show interface S0/0/0
Interfaz S0/0/1	interface s0/0/1 description Connection to R3 ip add 172.16.23.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:23::2/64 clock rate 128000 no shutdown	R2# show interface S0/0/1 R2# show controllers S0/0/1
Interfaz G0/0	interface g0/0 description Connection to ISP ip address 209.165.200.225 255.255.255.248 ipv6 address 2001:DB8:ACAD:2::1/64 no shutdown	R2# show ip interface G0/0

Tabla 6. Paso 3. Configurar R2. Comando de verificación.

Paso 4: Configurar R3.

Para realizar esta configuración procedemos a asignar un nombre al dispositivo para su identificación, incluyendo los siguientes datos de configuración:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Tabla 7. Paso 4. Configurar R3. Especificación.

Configuración	Especificación	Comando de verificación
Deshabilitar búsqueda DNS	no ip domain-lookup	R3# show run
Nombre del router	hostname R3	Mirar el prompt
Contraseña privilegiado	enable secret class	R3> enable
Contraseña de consola	line con 0 password cisco login	R3# exit
Contraseña de telnet	line vty 0 4 password cisco login	R3# show run
Encriptar contraseñas	service password-encryption	R3# show run
MOTD banner	banner motd @ Se prohíbe el acceso no autorizado.@	(Verificar banner en el login)
Interfaz S0/0/1	interface s0/0/1 description Connection to R2 ip address 172.16.23.1 255.255.255.252 ipv6 address 2001:db8:acad:23::1/64 no shutdown	R3# show interface S0/0/1
Interfaz Loopback 4	interface lo4 ip address 192.168.4.1 255.255.255.0	R3# show ip interface lo4
Interfaz Loopback 5	interface lo5 ip address 192.168.5.1 255.255.255.0	R3# show ip interface lo5
Interfaz Loopback 6	interface lo6 ip address 192.168.6.1 255.255.255.0	R3# show ip interface lo6
Interfaz Loopback 7	interface lo7 ipv6 address 2001:db8:acad:3::1/64	R3# show ip interface lo7
Rutas por defecto	ip route 0.0.0.0 0.0.0.0 s0/0/1 ipv6 route ::/0 s0/0/1	R3# show ip route R3# show ipv6 route

Tabla 8. Paso 4. Configurar R3. Comando de verificación.

Paso 5. Configurar S1.

Para realizar esta configuración procedemos a asignar un nombre al dispositivo para su identificación, incluyendo los siguientes datos de configuración:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 9. Paso 5. Configurar S1. Especificación.

Configuración	Especificación	Comando de verificación
Inhabilitar búsqueda DNS	no ip domain-lookup	S1# show run
Nombre del switch	hostname S1	Mirar el prompt
Contraseña de privilegiado	enable secret class	R3> enable
Contraseña de consola	line con 0 password cisco login	S1# exit
Contraseña de telnet	line vty 0 4 password cisco login	S1# show run
Encriptar las contraseñas	service password-encryption	S1# show run
MOTD banner	banner motd @ Se prohíbe el acceso no autorizado. @	(Verificar banner en el login)

Tabla 10. Paso 5. Configurar S1. Comando de verificación.

Paso 6. Configurar el S3.

Para esta configuración se asigna nombre al dispositivo para su identificación, incluyendo los siguientes datos de configuración:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 11. Paso 6. Configurar S3. Especificación.

Configuración	Especificación	Comando de verificación
Inhabilitar búsqueda DNS	no ip domain-lookup	S3# show run (Look for: no ip domain-lookup)
Nombre del switch	Hostname S3	(Look for : S3> or S3# command prompt)
Contraseña privilegiado	enable secret class	S3> enable (Type in privileged exec password)
Contraseña de consola	line con 0 password cisco login	S3# exit (Type in access password.)
Contraseña de telnet	line vty 0 4 password cisco login	S3# show run
Encriptar las contraseñas	Service password-encryption	S3# show run
MOTD banner	banner motd @ Se prohíbe el acceso no autorizado. @	(Verificar baner en el login.)

Tabla 12. Paso 6. Configurar S3. Comando de verificación.

Paso 7. Verificar la conectividad de la red.

Para la verificación se utilizará el comando ping para probar la conectividad entre los dispositivos de red.

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

Tabla 13. Paso 7. Verificar conectividad de la red.

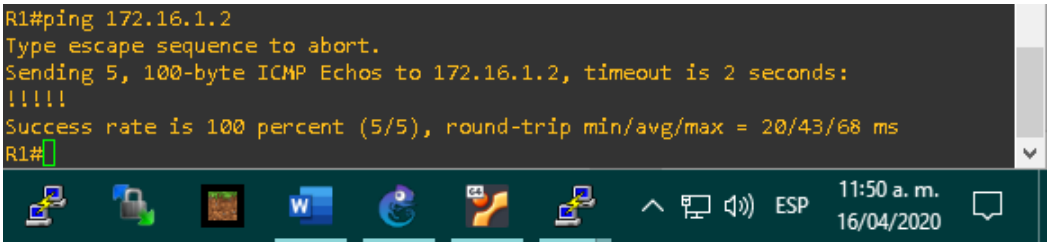

Figura 2. Paso 7, verificar la conectividad de la red R1 a R2.

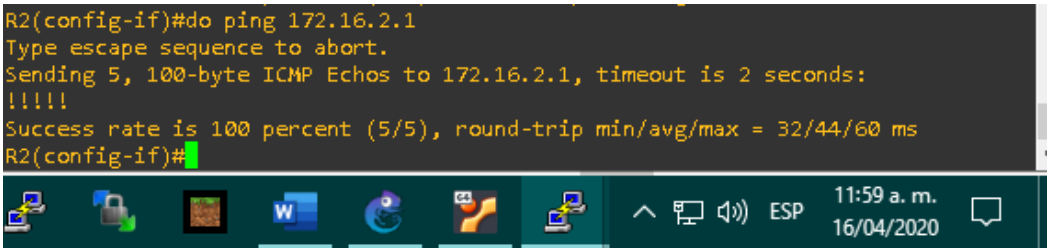

Figura 3. Paso 7, verificar la conectividad de la red R2 a R3.

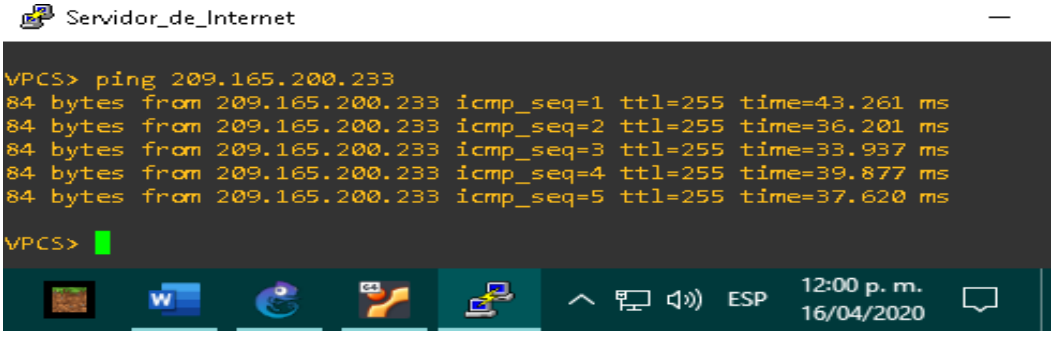

Figura 4. Paso 7, verificar la conectividad de la red PC a Gateway.

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

Paso 1. Configurar S1.
Para esta configuración procedemos a crear las VLANs y asignar un nombre, incluyendo los siguientes datos de configuración:

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
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
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Tabla 14. Paso 1. Configurar S1. Especificación.

Configuración	Especificación	Comando de verificación
Crear la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion	S1# show vlan
Asignar la dirección IP de administración	interface vlan 99 ip address 192.168.99.2 255.255.255.0	S1# show interface vlan 99
Asignar el gateway predeterminado	ip default-gateway 192.168.99.1	S1# show run | section default
Forzar el enlace troncal en la interfaz F0/3	interface F0/3 switchport mode trunk switchport trunk native vlan 1	S1# show interface trunk
Forzar el enlace troncal en la interfaz F0/5	interface F0/5 switchport mode trunk switchport trunk native vlan 1	S1# show interface trunk
Configurar el resto de los puertos como puertos de acceso	interface range F0/1-2, F0/4, F0/6-24, G0/1-2 switchport mode access	S1# show run | begin interface
Asignar F0/6 a la VLAN 21	interface F0/6 switchport access vlan 21	S1# show run interface f0/6
Apagar todos los puertos sin usar	interface range F0/1-2, F0/4, F0/7-24, G0/1-2 shutdown	S1# show ip interface brief

Tabla 15. Paso 1. Configurar S1. Comando de verificación.

Paso 2: Configurar el S3

Para esta configuración procedemos a crear las VLANs y asignar un nombre, incluyendo los siguientes datos de configuración:

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.
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.
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa.
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range.
Asignar F0/18 a la VLAN 23	
Apagar todos los puertos sin usar	

Tabla16. Paso 2. Configurar S3. Especificación.

Configuración	Especificación	Comando de verificación
Crear la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion	S3# show vlan
Asignar la dirección IP de administración	interface vlan 99 ip address 192.168.99.3 255.255.255.0	S3# show interface vlan 99
Asignar el gateway predeterminado	ip default-gateway 192.168.99.1	S3# show run | section default
Forzar el enlace troncal en la interfaz F0/3	interface F0/3 switchport mode trunk switchport trunk native vlan 1	S3# show interface trunk S3# show run interface f0/3
Forzar el enlace troncal en la interfaz F0/5 Configurar el resto de los puertos como puertos de acceso.	interface range F0/1-2, F0/4, F0/6-24, G0/1-2 switchport mode access	S3# show run | begin interface
Asignar F0/6 a la VLAN 21	interface F0/18 switchport access vlan 33	S3# show run interface f0/18
Apagar todos los puertos sin usar Apagar los puertos restantes	interface range F0/1-2, F0/4, F0/6-17, F0/19-24, G0/1-2 shutdown	S3# show ip interface brief

Tabla17. Paso 2. Configurar S3. Comando de verificación.

Paso 3: Configurar R1.

Para esta configuración se inicia con las subinterfaces y la asignación de IP y la respectiva descripción:

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
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
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
Activar la interfaz G0/1	

Tabla18. Paso 3. Configurar R1. Especificación.

Configuración	Especificación	Comando de verificación
Configurar la subinterfaz 802.1Q .21 en G0/1	interface g0/1.21 description LAN de contabilidad encapsulation dot1q 21 ip address 192.168.21.1 255.255.255.0	R1# show ip interface brief (Look to see if the .31 subinterface has the correct IP address and has an up/up status.)
Configurar la subinterfaz 802.1Q .23 en G0/1	interface g0/1.23 description LAN de Ingenieria encapsulation dot1q 23 ip address 192.168.23.1 255.255.255.0	R1# show ip interface brief (Look to see if the .33 subinterface has the correct IP address and has an up/up status.)
Configurar la subinterfaz 802.1Q .99 en G0/1	interface g0/1.99 description Lan de Administracion encapsulation dot1q 99 ip address 192.168.99.1 255.255.255.0	R1# show ip interface brief (Look to see if the .99 subinterface has the correct IP address and has an up/up status.)
Activar Interface G0/1	interface g0/1 no shutdown	(Se puede observador con el comando anterior)

Tabla 19. Paso 3. Configurar R1. Comando de verificación.

Paso 4: Verificar la conectividad de la red

Se utiliza el comando ping para probar la conectividad entre los switches y el R1.

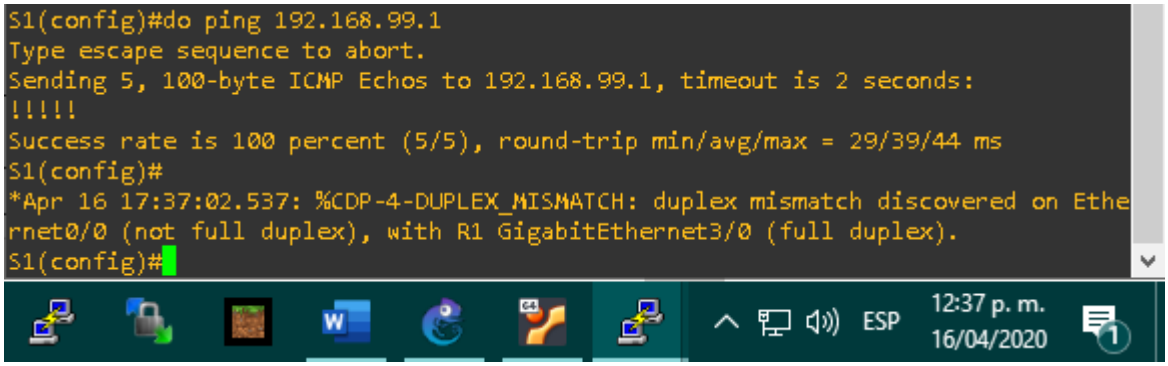

Figura 5. Paso 4. Verificar la conectividad de la red S1 a VLAN 99

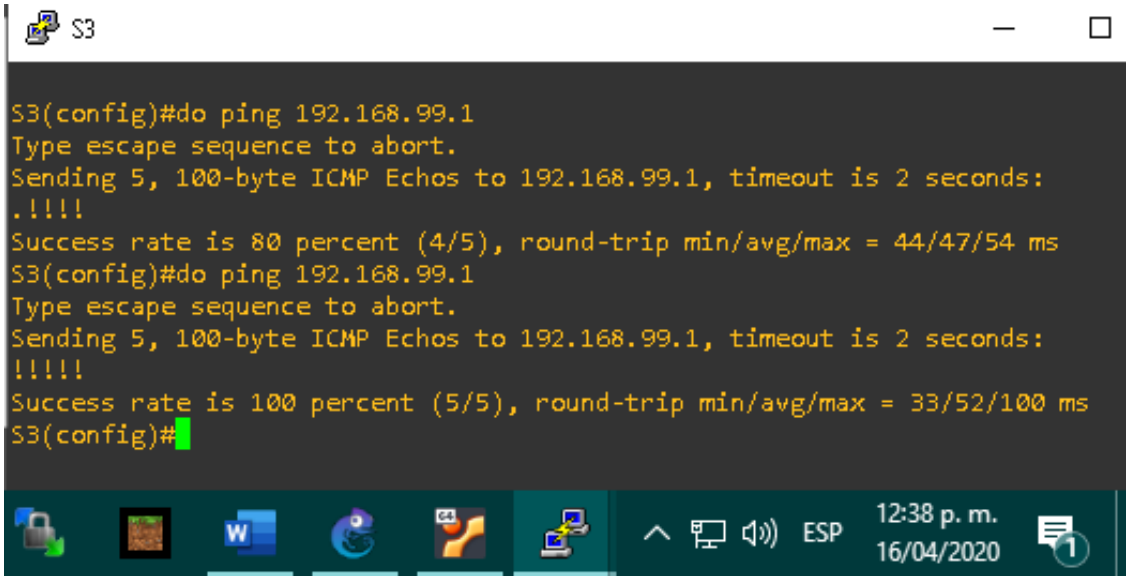

Figura 6. Paso 4. Verificar la conectividad de la red S3 a VLAN 99.

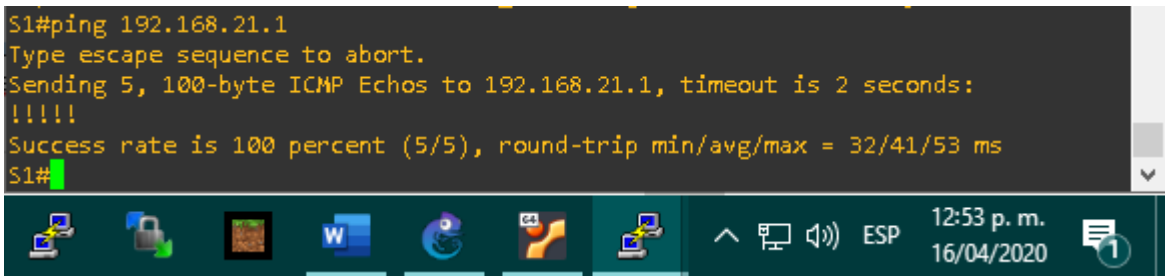

Figura 7. Paso 4. Verificar la conectividad de la red S1 a VLAN 21.

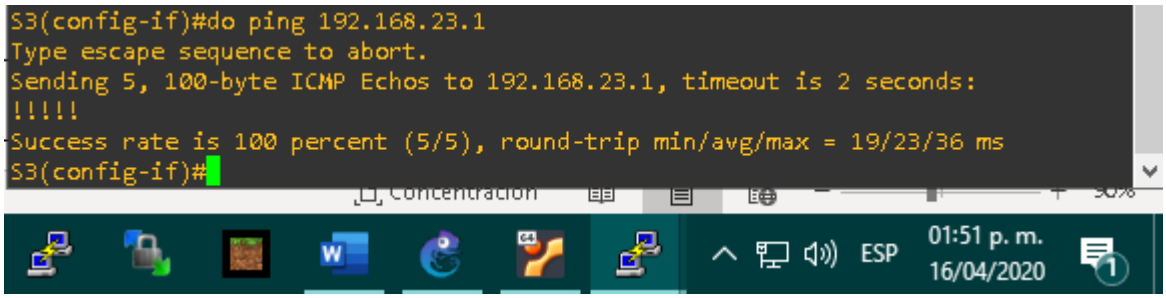

Figura 8. Paso 4. Verificar de la conectividad de la red S3 a VLAN 23.

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

Tabla 20. Paso 4. Resultados de ping.

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Procedemos a la configuración de RIPv2 con las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Tabla 21. Paso 1. Configurar RIPv2 en el R1.

Configuración	Especificación	Comando de verificación
Configurar RIP versión 2	router rip version 2	R1# show run | section router rip
Anunciar las redes conectadas directamente	network 172.16.1.0 network 192.168.21.0 network 192.168.23.0 network 192.168.99.0	R1# show run | section router rip
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99	R1# show ip protocols
Desactive la sumarización automática	no auto-summary	R1# show run | section router rip

Tabla 22. Paso 1. Comando de verificación.

Paso 2: Configurar RIPv2 en el R2.

Procedemos a la configuración de RIPv2 con las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Tabla 23. Paso 2. Configurar RIPv2 en el R2.

Configuración	Especificación	Comando de verificación
Configure RIP	router rip version 2	R2# show ip protocols
Anunciar las redes conectadas directamente	network 172.16.0.0 network 10.10.10.10	R2# show run | section router rip
Establecer todas las interfaces LAN como pasivas	passive-interface lo0	R2# show ip protocols
Desactive la sumarización automática	no auto-summary	R2# show run | section router rip

Tabla 24. Paso 2. Comando de verificación

Paso 3: Configurar RIPv2 en el R3.

Procedemos a la configuración de RIPv2 con las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Tabla 25. Paso 3. Configurar RIPv2 en el R3.

Configuración	Especificación	Comando de verificación
Configure RIP Version 2	router rip version2	R3# show run | section router rip
Anunciar redes IPv4 conectadas directamente	network 172.16.0.0 network 192.168.4.0 network 192.168.5.0 network 192.168.6.0	R3# show run | section router rip
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface lo4 passive-interface lo5 passive-interface lo6	R3# show ip protocols
Desactive la sumarización automática	no auto-summary	R3# show run | section router rip

Tabla 26. Paso 3. Comando de verificación.

Paso 4: Verificar la información de RIP.

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

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

Tabla 27. Paso 4. Pregunta – Respuesta.

Parte 5: Implementar DHCP y NAT para IPv4.

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

Para la configuración de R1 como servidor debemos exceptuar el rango de las direcciones y crear las siguientes configuraciones:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
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
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

Tabla 28. Paso1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.

Configuración	Especificación	Comando de verificación
Reservar primeras 20 direcciones IP en VLAN21 para configuración estática	ip dhcp excluded-address 192.168.21.1 192.168.21.20	R1# show run | section dhcp
Reservar primeras 20 direcciones IP en VLAN 23 para configuración estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20	R1# show run | section dhcp
Crear un pool de DHCP para la VLAN 21	ip dhcp pool ACCT network 192.168.31.0 255.255.255.0 dns-server 10.10.10.10 domain-name ccna-sa.com default-router 192.168.31.1	R1# show run | section dhcp R1# show ip dhcp bindings
Crear un pool de DHCP para la VLAN 23	ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 dns-server 10.10.10.10 domain-name ccna-sa.com default-router 192.168.23.1	R1# show run | section dhcp R1# show ip dhcp bindings

Tabla 29. Paso 1. Comando de verificación.

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

Para dicha configuración se deben realizar las siguientes tareas que son esenciales al momento de la configuración:

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
Habilitar el servicio del servidor HTTP	Ip http server Ip http secure-server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación.	Ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	Ip nat inside source static 10.10.10.10 209.165.200.237
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
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236
Definir la traducción de NAT dinámica	

Tabla 30. Paso 2. Configurar la NAT estática y dinámica en el R2.

Configuración	Especificación	Comando de verificación
Crear una base de datos local con una cuenta de usuario	username webuser privilege 15 secret cisco12345	R2# show run | section username
Habilitar el servicio del servidor HTTP	ip http server	R2# show run | section ip http
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local	R2# show run | section ip http
Crear una NAT estática al servidor web.	ip nat inside source static 10.10.10.10 209.165.200.237	R2# show ip nat translations
Asignar la interfaz interna y externa para la NAT estática	Interface lo0 ip nat inside interface g0/0 ip nat outside	R2# show run | begin interface
Configurar la NAT dinámica dentro de una ACL privada	access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255	R2# show access-lists
Defina el pool de direcciones IP públicas utilizables.	ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 55.255.255.248	R2# show run | section ip nat
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET	R2# show run | section ip nat

Tabla 31. Paso 2. Comando de verificación.

Paso 3: Verificar el protocolo DHCP y la NAT estática.

Procederemos a verificar que los PC asignados hayan aceptada la información suministrada por la IP del servidor DHCP.

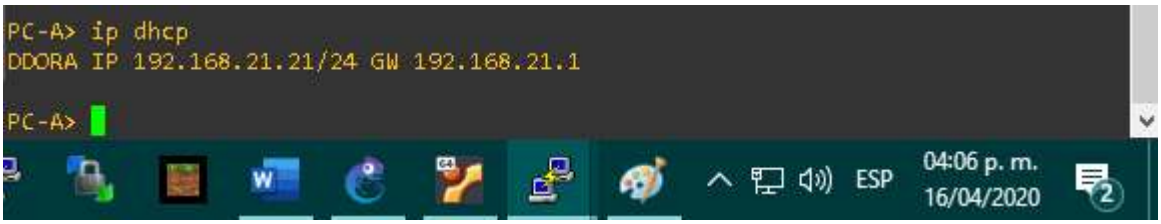

Figura 9. Paso 3. Verificar protocolo DHCP y la NAT estática PC-A.

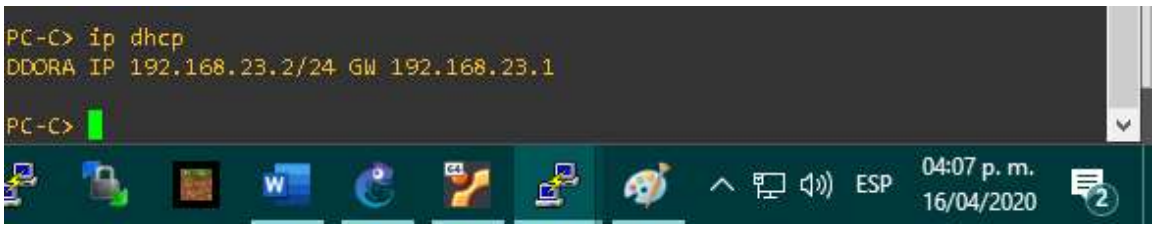

Figura 10. Paso 3. Verificar protocolo DHCP y la NAT estática PC-C.

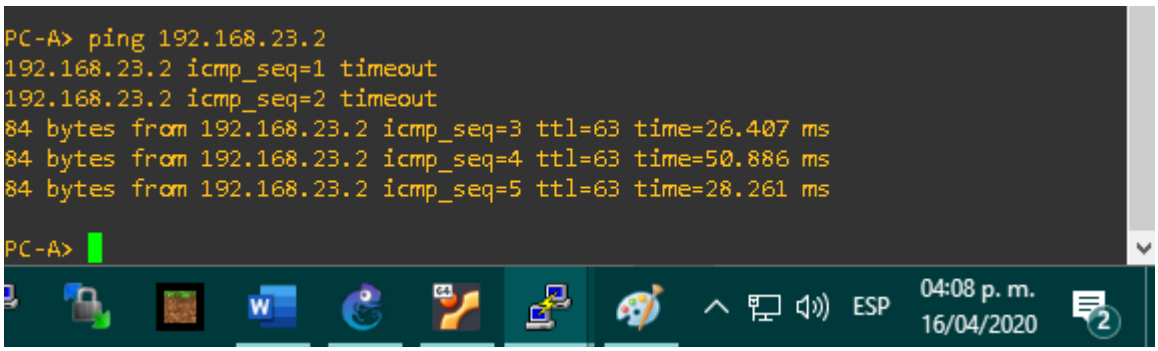

Figura 11. Paso 3. Verificar protocolo DHCP y la NAT estática.

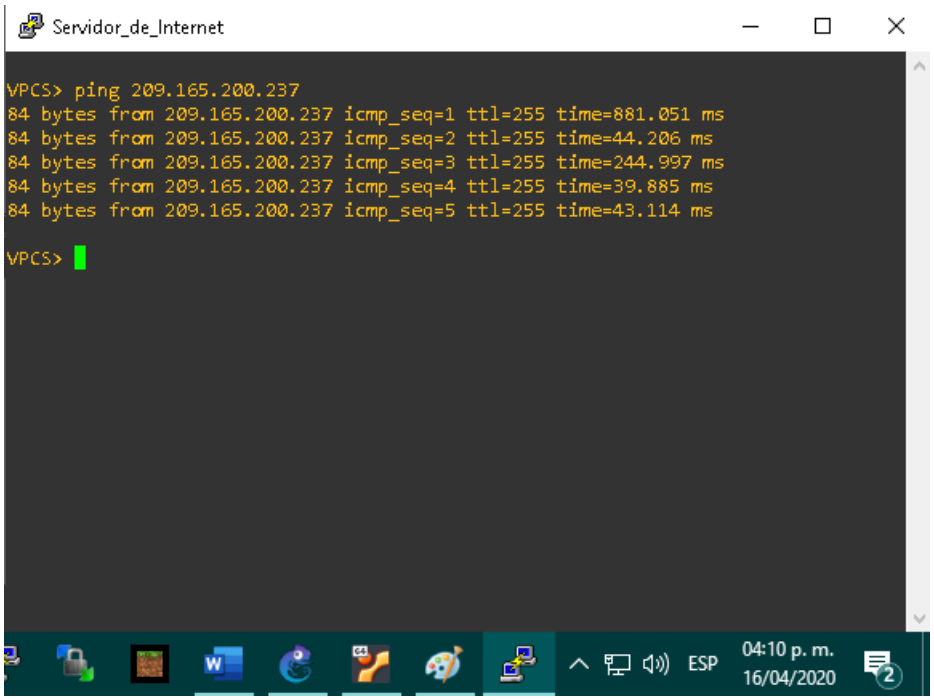

Figura 12. Paso 3. Verificar protocolo DHCP y la NAT estática Navegador Web.

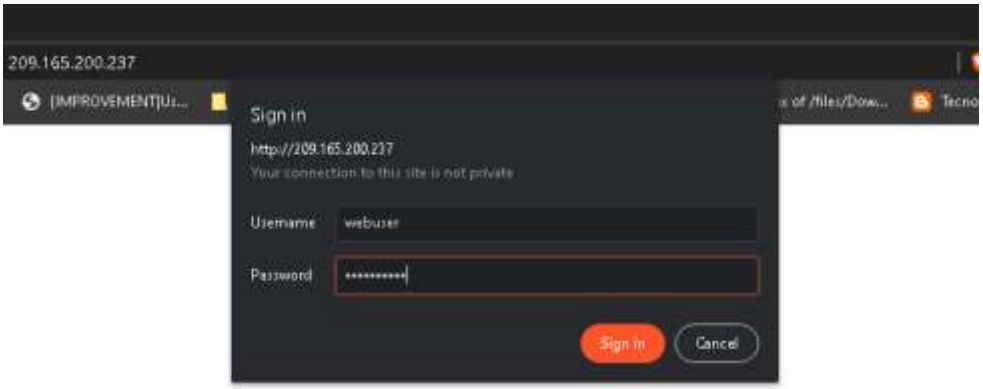

Figura 13. Paso 3. Verificar protocolo DHCP y la NAT estática.

```
Haciendo ping a 209.165.200.237 con 32 bytes de datos:
Respuesta desde 209.165.200.237: bytes=32 tiempo=202ms TTL=255
Respuesta desde 209.165.200.237: bytes=32 tiempo=40ms TTL=255
Respuesta desde 209.165.200.237: bytes=32 tiempo=72ms TTL=255
Respuesta desde 209.165.200.237: bytes=32 tiempo=39ms TTL=255

Estadísticas de ping para 209.165.200.237:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 39ms, Máximo = 202ms, Media = 88ms
```

Figura 14. Paso 3. Verificar protocolo DHCP y la NAT estática.

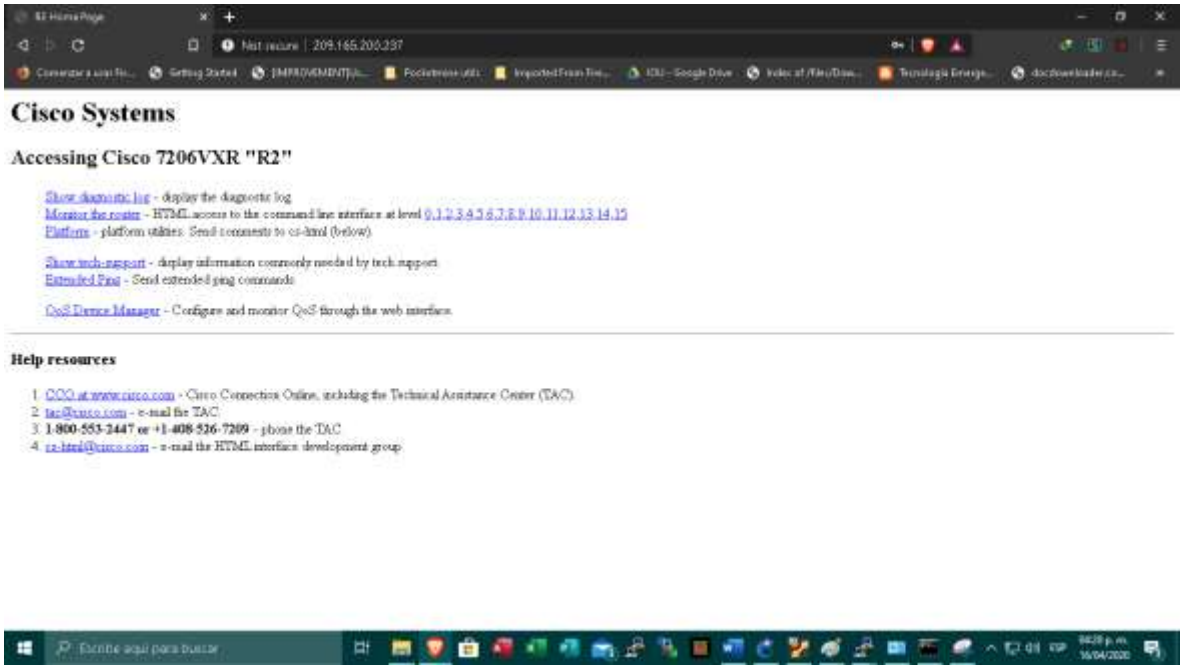

Figura 15. Paso 3. Verificar protocolo DHCP y la NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
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	Exitoso

Tabla 32. Paso 3. Prueba - Resultados.

Parte 6: Configurar NTP.

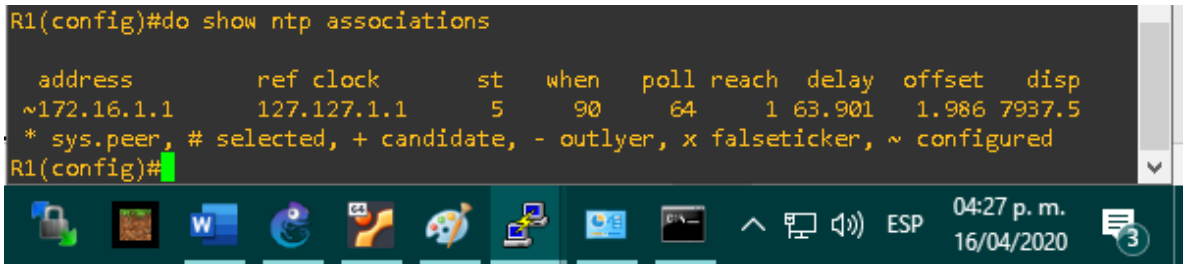

Figura 16. Configurar NTP.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Tabla 33. Parte 6. Configurar NTP.

Configuración	Especificación	Comando de verificación
Ajuste la fecha y hora en R2.	R2# clock set 9:00:00 5 march 2016	R2# show clock
Configure R2 como un maestro NTP	R2(config)# ntp master 5	R2# Show run | section ntp
Configurar R1 como un cliente NTP.	R1(config)# ntp server 172.16.12.2	R1# show run | section ntp
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1 (config)# ntp update-calendar	R1# show run | section ntp
Verifique la configuración de NTP en R1.	R1# show ntp associations	R1# show ntp associations

Tabla 34. Parte 6. Configurar NTP. Comando de verificación.

Parte 7: Configurar y verificar las listas de control de acceso (ACL).
Paso 1: Restringir el acceso a las líneas VTY en el R2.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Tabla 35. Paso 1. Restringir el acceso a las líneas VTY en el R2.

Configuración o tarea	Especificación	Comando IOS
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	ip access-list standard ADMIN-MGT permit host 172.16.1.1	R2# show access-lists
Aplicar la ACL con nombre a las líneas VTY	line vty 0 4 access-class ADMIN-MGT in	R2# show run | sec line vty
Permitir acceso por Telnet a las líneas de VTY	transport input telnet	R2# show run | section vty
Verificar que la ACL funcione como se espera	Exitoso	R1# telnet 172.16.1.1

Tabla 36. Paso 1. Comando IOS.

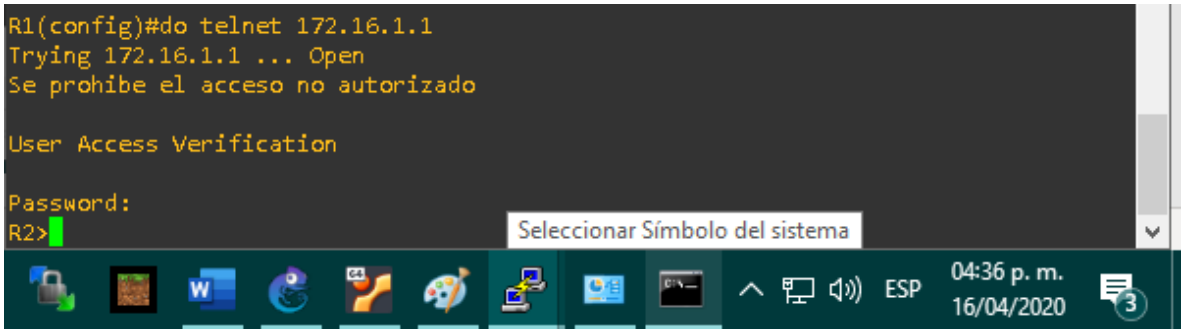

Figura 17. Paso 1. Restringir acceso.

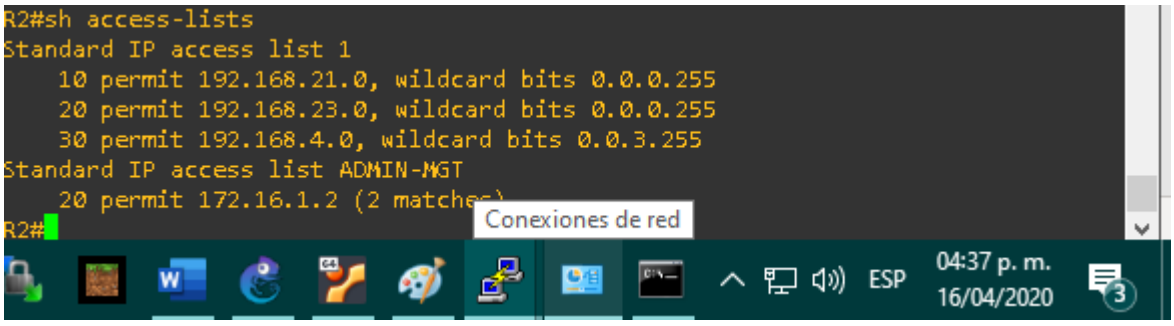

Figura 18. Paso 1. Lista de acceso.

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

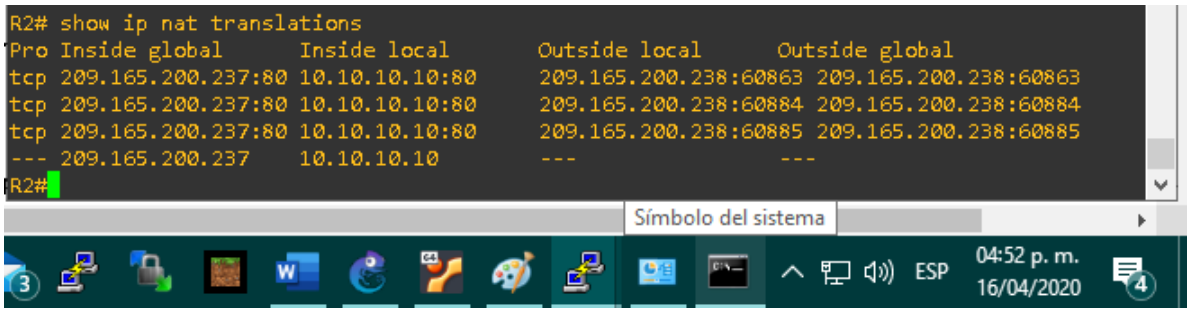

Figura 19. Paso 2. Introducir comando de CLI.

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?	show ip nat translations Nota: Para las traducciones de 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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	#clear ip nat translation *

Tabla 37. Paso 2. Descripción y comando.

1.2 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 la red.

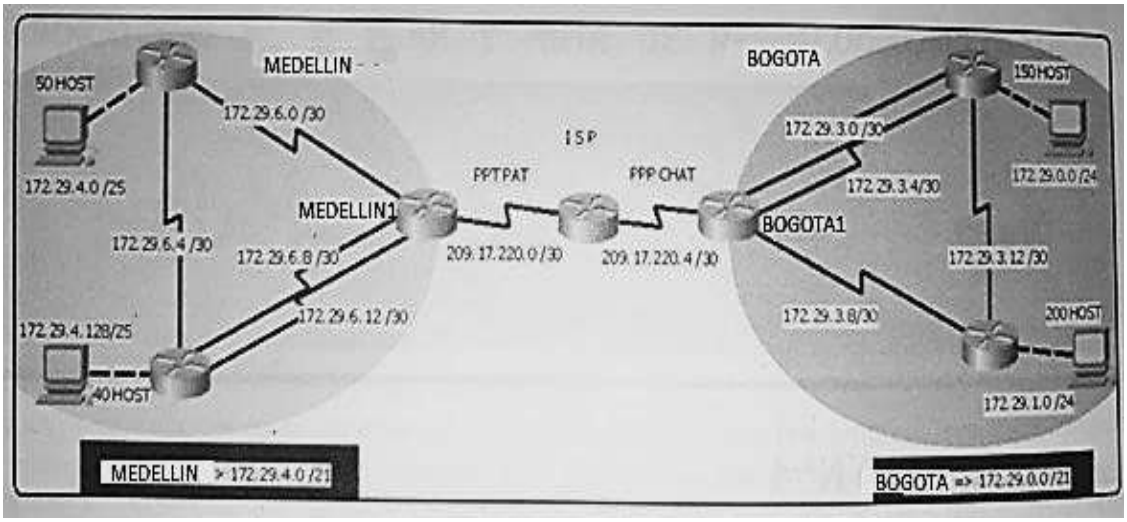

Figura 20. Esc2, Topología.

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.

Antes de iniciar con el desarrollo de dicho escenario debemos realizar lo siguiente:

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

Configuración	Especificación	Comando de verificación
Desactivar la búsqueda DNS	no ip domain-lookup	Equipo# show run (Buscar: no ip domain-lookup)
Nombre del equipo	hostname {NOMBRE_DEL_EQUIPO}	Mirar el prompt
Contraseña de exec privilegiado cifrada	enable secret class	Equipo> enable (Escribir en modo usuario)
Contraseña de acceso a la consola	line con 0 password cisco login	Equipo # exit (Escribir en privilegiado)
Contraseña de acceso Telnet	line vty 0 4 password cisco Login	Equipo # show run
Cifrar las contraseñas de texto no cifrado	service password-encryption	Equipo # show run
Mensaje MOTD	banner motd @ Se prohíbe el acceso no autorizado @	(verificar banner en el login)

Tabla 38. Esc2. Comando de verificación.

Realizar la conexión física de los equipos con base en la topología de red
Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Parte 1: Configuración del enrutamiento
Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Para que el enrutamiento de las redes fuera exitoso se tuvimos que ingresar al CLI en donde se ingresaron los comandos asignados para:

1. Enable: Permite acceder al modo privilegiado del router.
2. Network: Aquí agregamos la red que vamos a enrutar.
3. Configure terminal: Permite ingresar a modo de configuración global.
4. Router OSPF 1: Este permite el uso del protocolo de información de enrutamiento.

MEDELLIN1
router ospf 1
network 172.29.6.0 0.0.0.3 area 0
network 172.29.6.8 0.0.0.3 area 0
network 172.29.6.12 0.0.0.3 area 0
network 209.17.220.0 0.0.0.3 area 0

MEDELLIN2
router ospf 1
network 172.29.4.0 0.0.0.127 area 0
network 172.29.6.0 0.0.0.3 area 0
network 172.29.6.4 0.0.0.3 area 0

MEDELLIN3
router ospf 1
network 172.29.4.128 0.0.0.127 area 0
network 172.29.6.4 0.0.0.3 area 0
network 172.29.6.8 0.0.0.3 area 0
network 172.29.6.12 0.0.0.3 area 0

ISP
router ospf 1
network 209.17.220.0 0.0.0.3 area 0
network 209.17.220.4 0.0.0.3 area 0

BOGOTA1
router ospf 1
network 172.29.3.0 0.0.0.3 area 0
network 172.29.3.4 0.0.0.3 area 0
network 172.29.3.8 0.0.0.3 area 0
network 209.17.220.4 0.0.0.3 area 0

BOGOTA2
router ospf 1
network 172.29.1.0 0.0.0.255 area 0
network 172.29.3.8 0.0.0.3 area 0
network 172.29.3.12 0.0.0.3 area 0

BOGOTA3
router ospf 1
network 172.29.0.0 0.0.0.255 area 0
network 172.29.3.0 0.0.0.3 area 0
network 172.29.3.4 0.0.0.3 area 0
network 172.29.3.12 0.0.0.3 area 0

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.

Podemos observar que encontramos dos grupos de ceros que son los asignados a la dirección de red que luego conectaremos y los otros se le asignaran la mascara de red, por otra parte tenemos el serial, el cual corresponde a la interfaz que permite la comunicación.

BOGOTA1
1 - ip route 0.0.0.0 0.0.0.0 Serial0/1/0
2 - router ospf 1
redistribute static subnets

MEDELLIN1
1 - ip route 0.0.0.0 0.0.0.0 Serial0/1/0
2 - router ospf 1
redistribute static subnets

Donde uno corresponde a la asignación de la ruta según la ciudad y dos corresponde a la redistribución de la ruta con respecto al protocolo de enrutamiento.

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.

ip route 172.29.4.0 255.255.252.0 Serial0/3/0
ip route 172.29.4.128 255.255.255.128 Serial0/3/0
ip route 172.29.1.0 255.255.255.0 Serial0/3/1
ip route 172.29.0.0 255.255.252.0 Serial0/3/1

Parte 2: Tabla de Enrutamiento.

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

MEDELLIN2

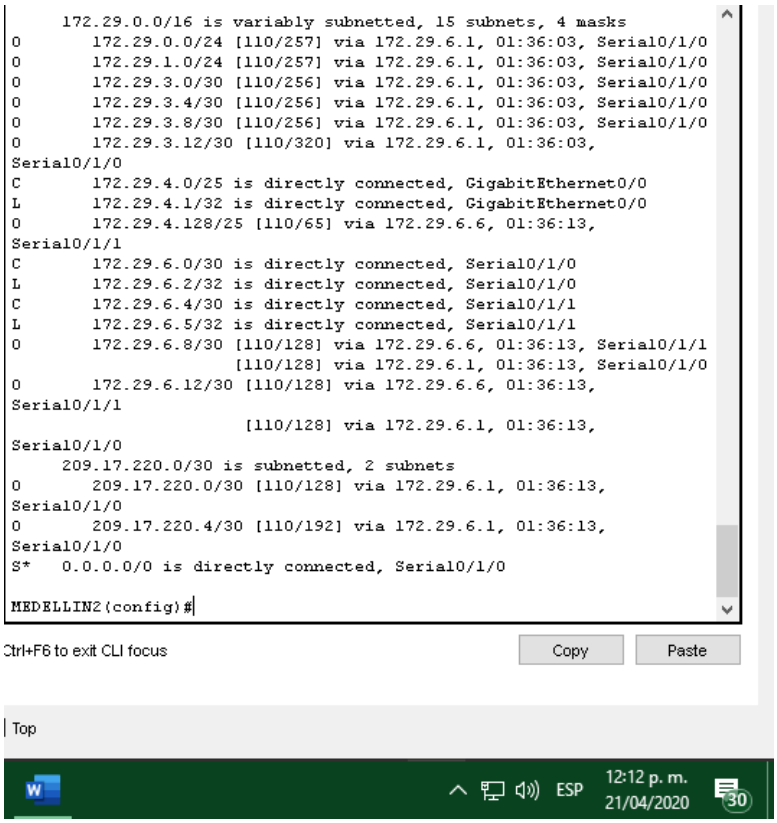

Figura 21. Esc2. Enrutamiento Medellin 2.

MEDELLIN 3

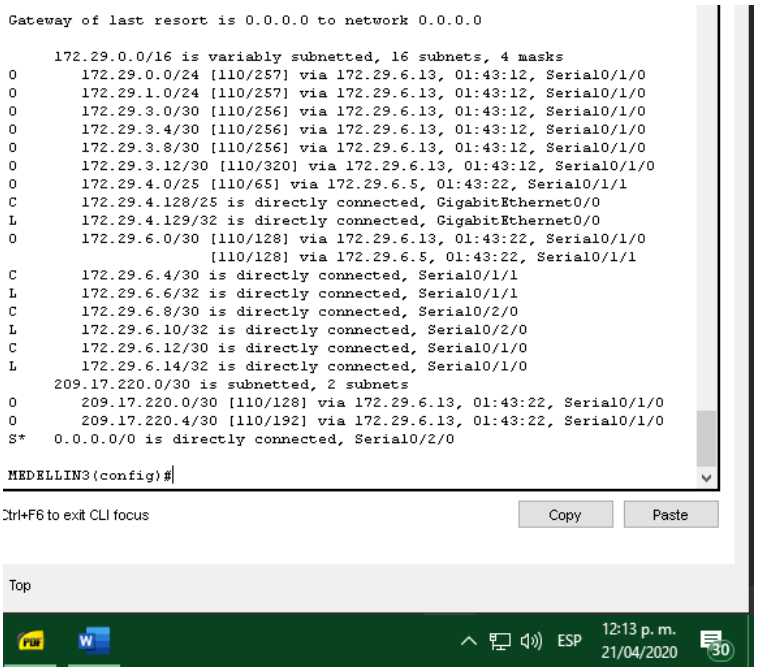

Figura 22. Esc2. Enrutamiento Medellin 3.

MEDELLIN 1

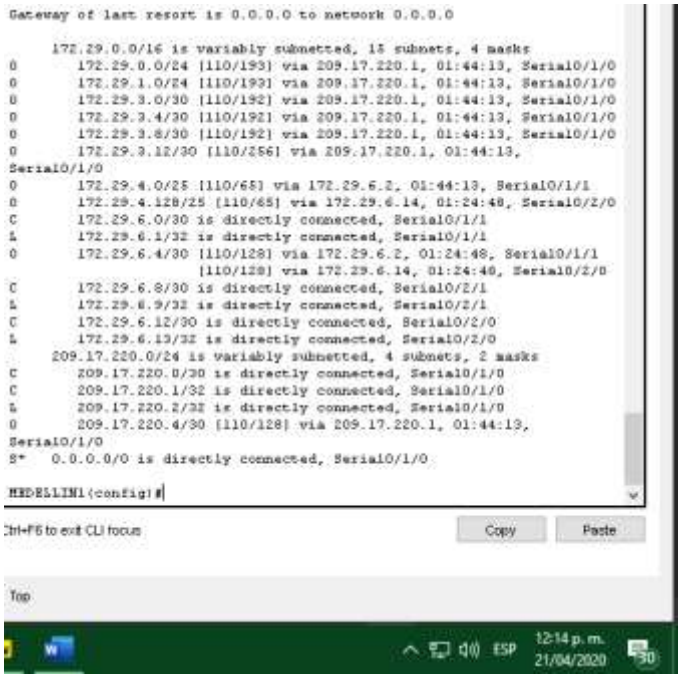

Figura 23. Esc2. Enrutamiento Medellin 1.

ISP

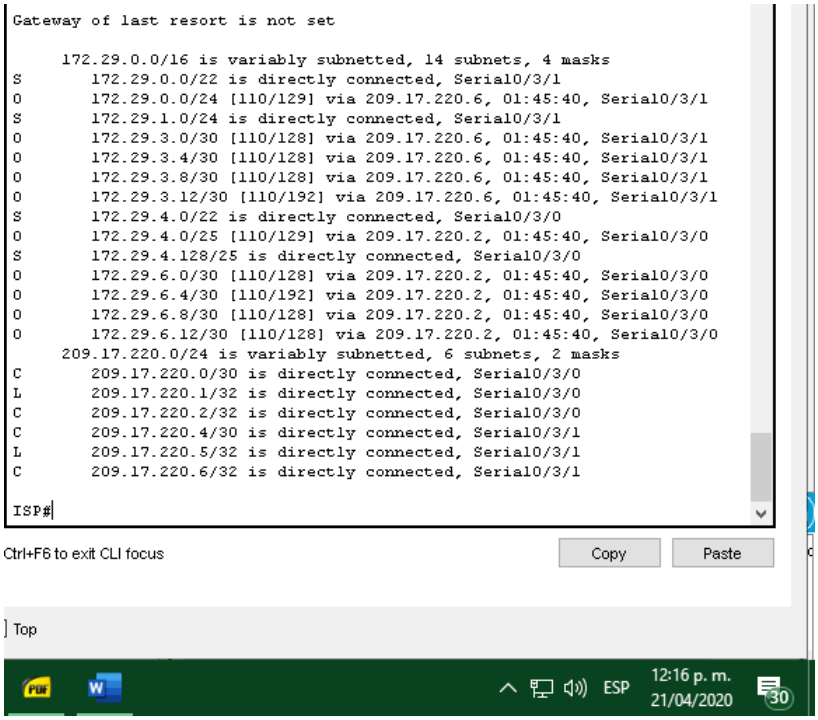

Figura 24. Esc2. ISP.

BOGOTÁ1

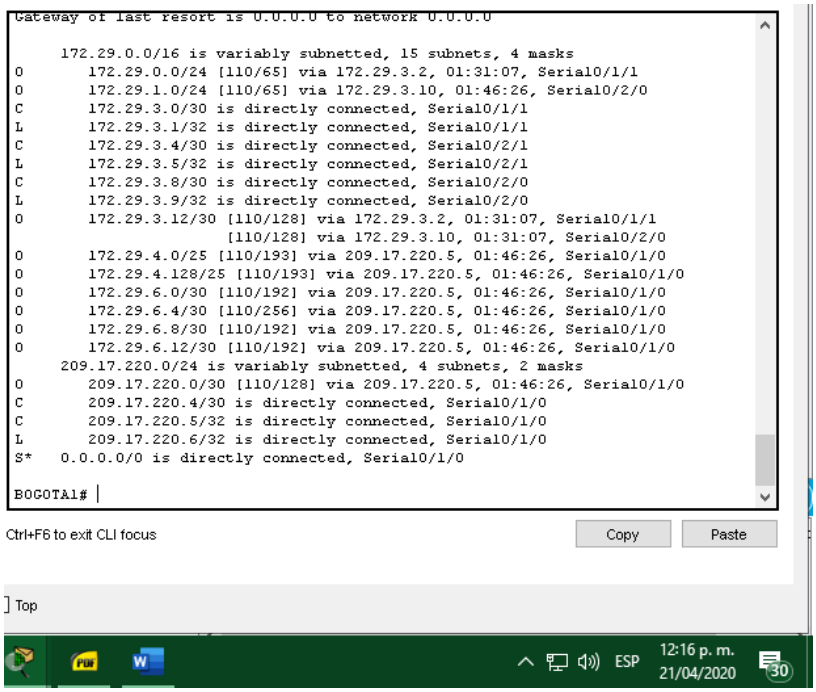

Figura 25. Esc2. Enrutamiento Bogotá 1.

BOGOTÁ3

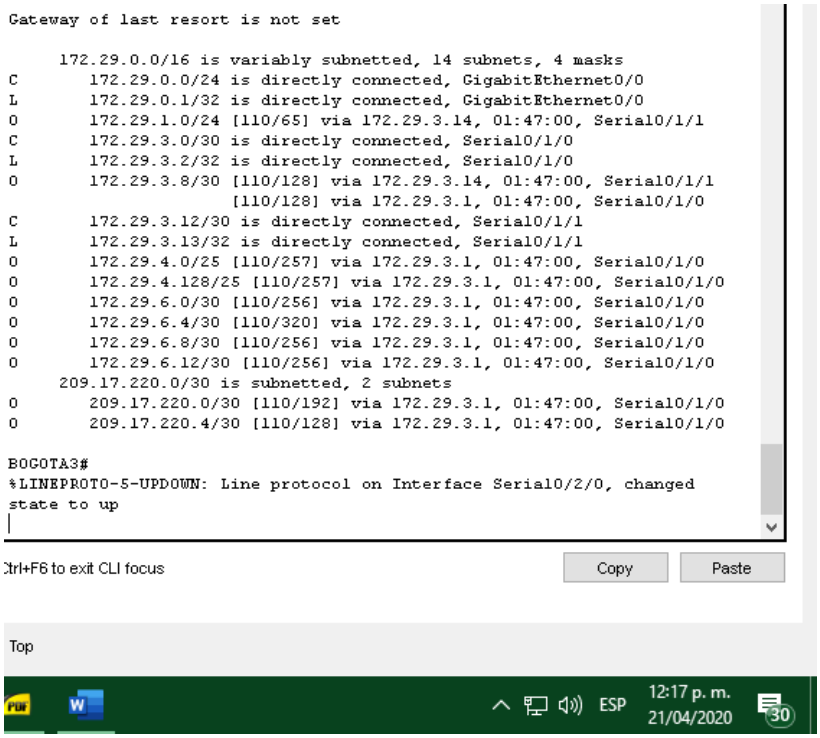

Figura 26. Esc2. Enrutamiento Bogotá 3.

BOGOTÁ2

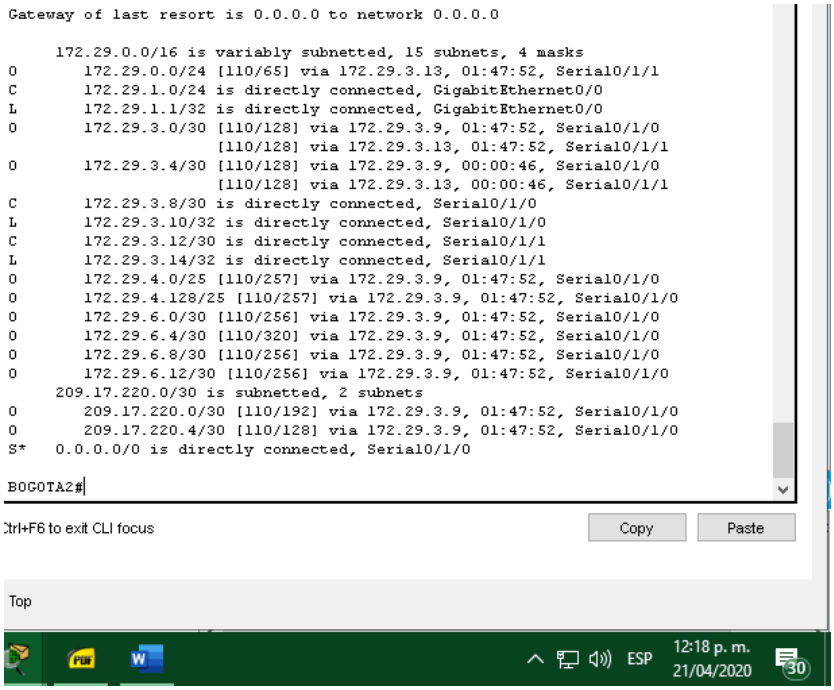

Figura 27. Esc2. Enrutamiento Bogotá 2.

Verificar el balanceo de carga que presentan los routers:

“En las siguientes imágenes se puede apreciar más detalladamente los balanceos de carga de las redes configuradas, en donde destacan los cambios de ruta que toma el envió del paquete, demostrando que puede varear la decisión de la ruta por donde se transmitirá el paquete”.

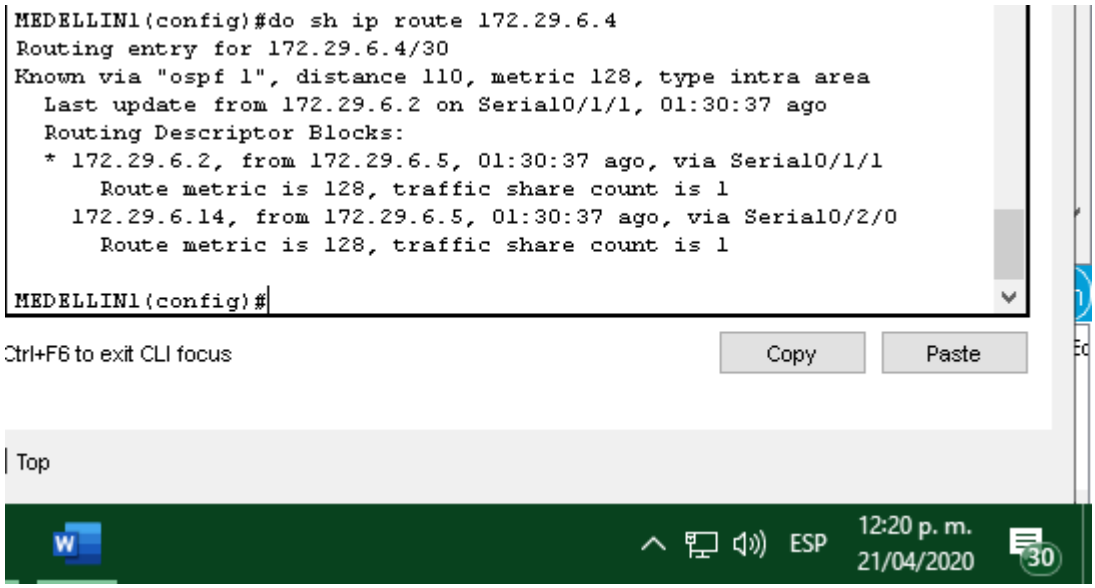

Figura 28. Esc2. Balanceo Medellín1.

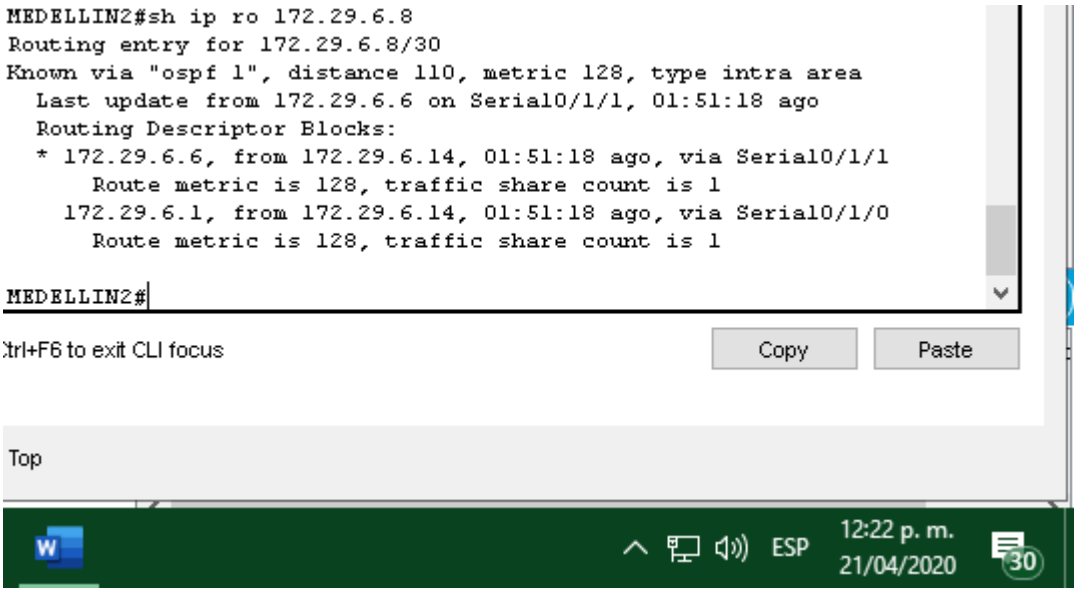

Figura 29. Esc2. Balanceo Medellín2.

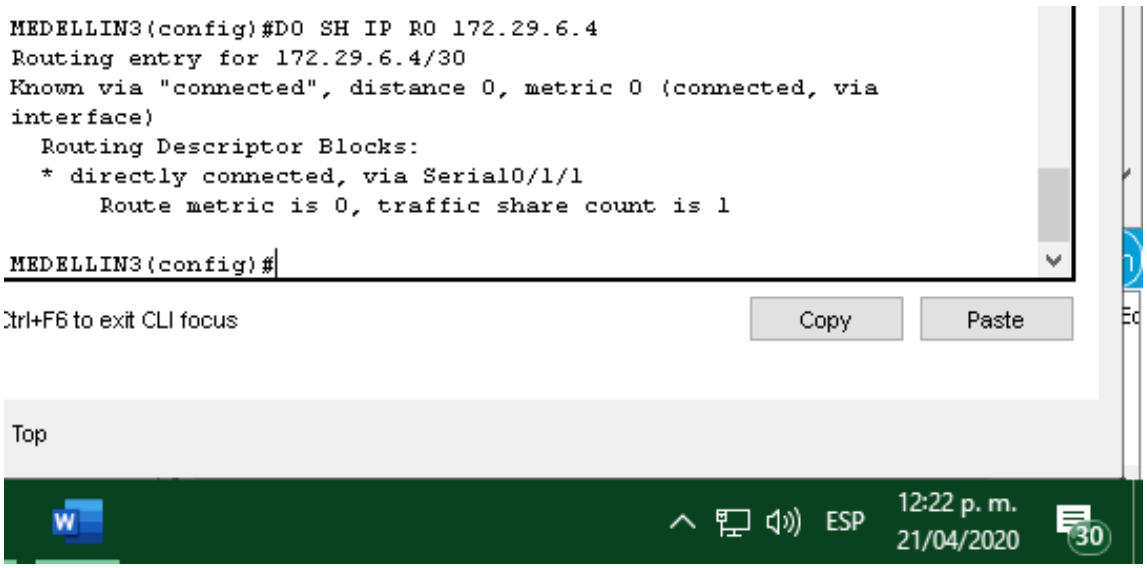

Figura 30. Esc2. Balanceo Medellín3.

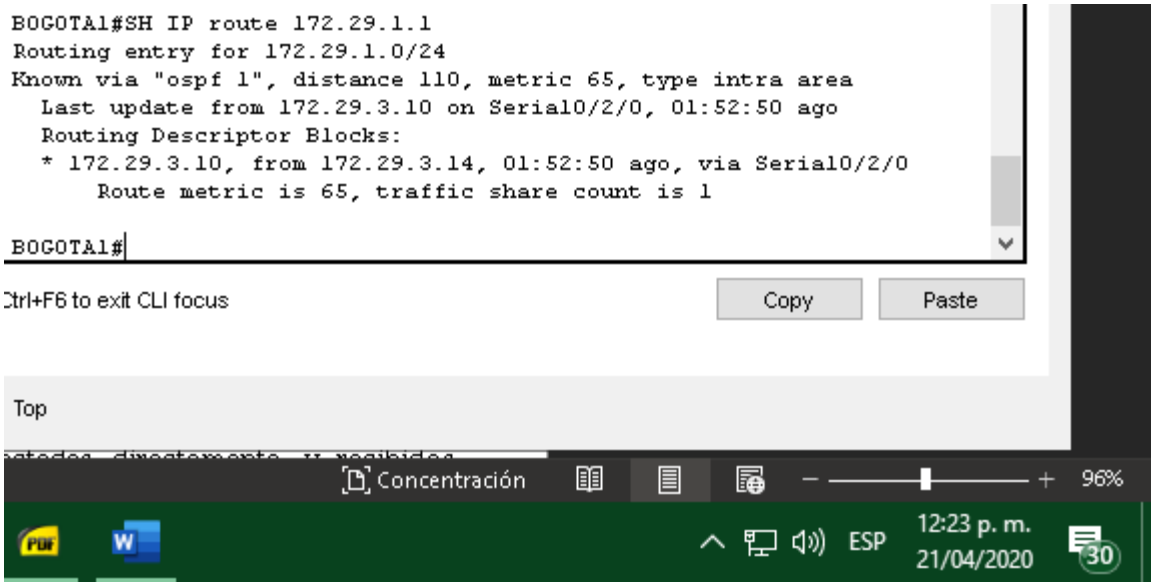

Figura 31. Esc2. Balanceo Bogotá1.

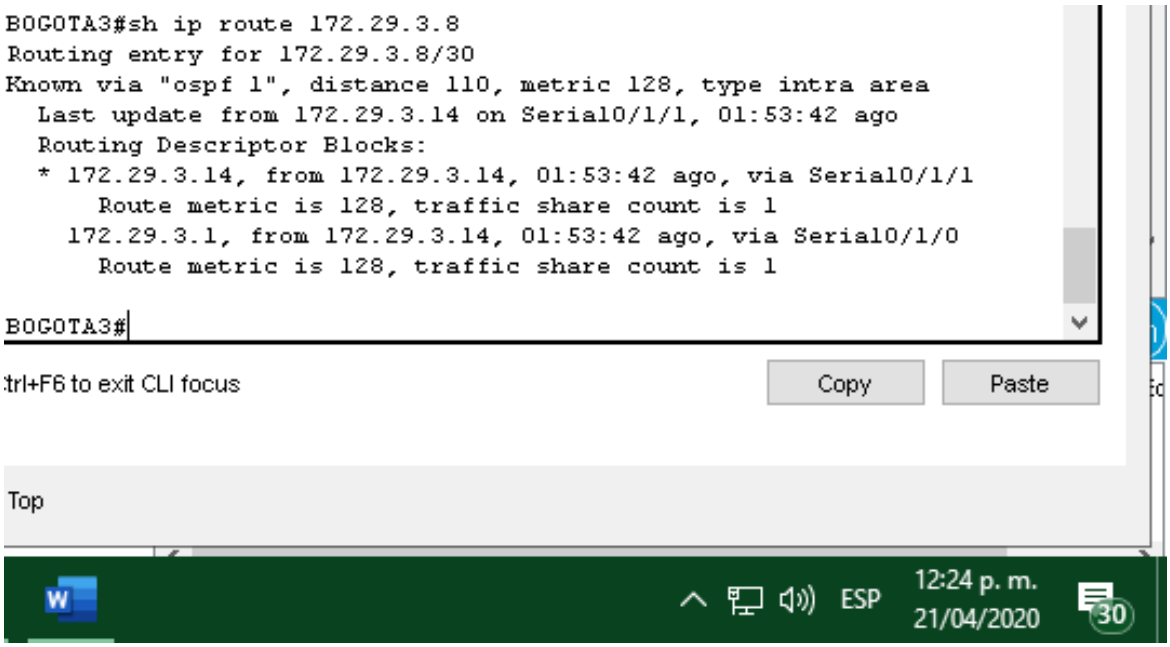

Figura 32. Esc2. Balanceo Bogotá3.

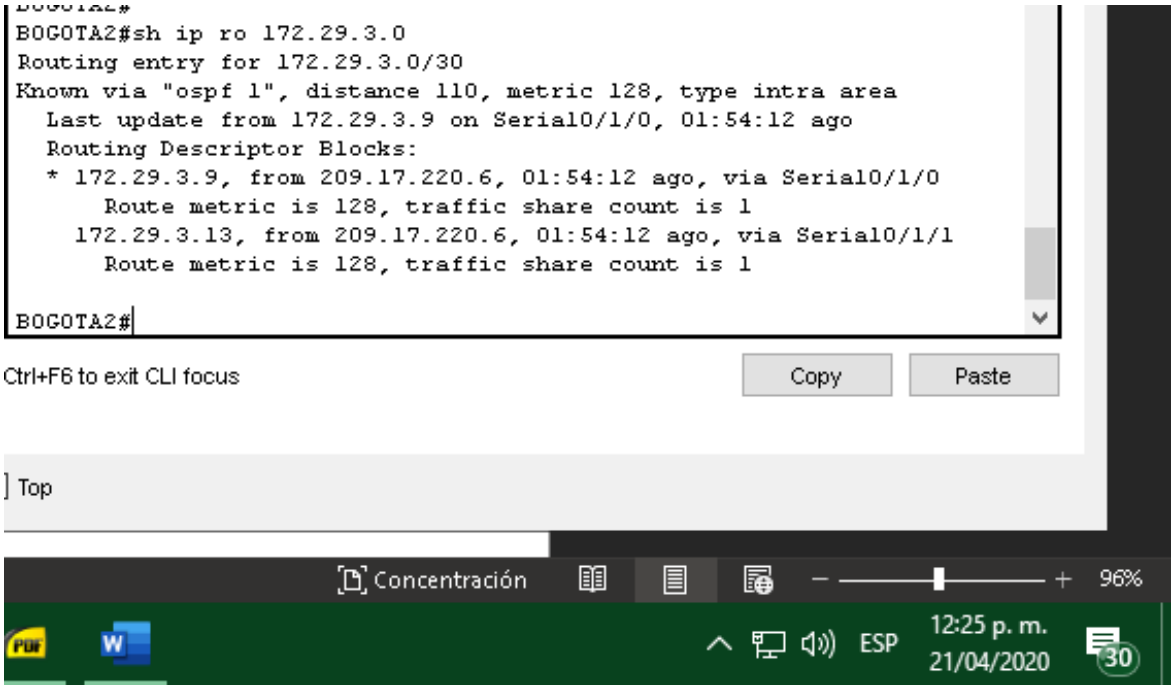

Figura 33. Esc2. Balanceo Bogotá2.

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

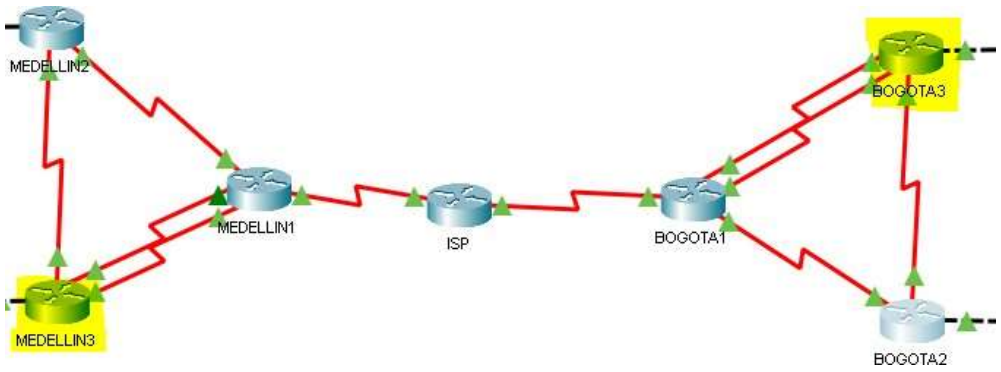

Figura 34. Esc2. Esquema Bogotá1 – Medellín1.

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

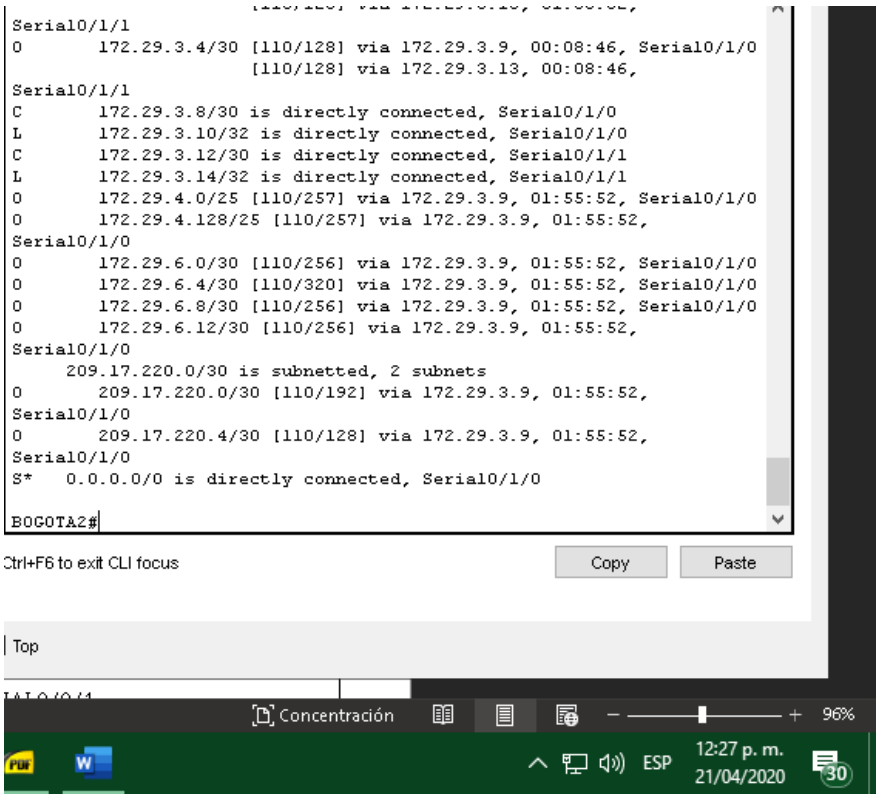

Figura 35. Esc2. Redes conectadas directamente Bogotá2.

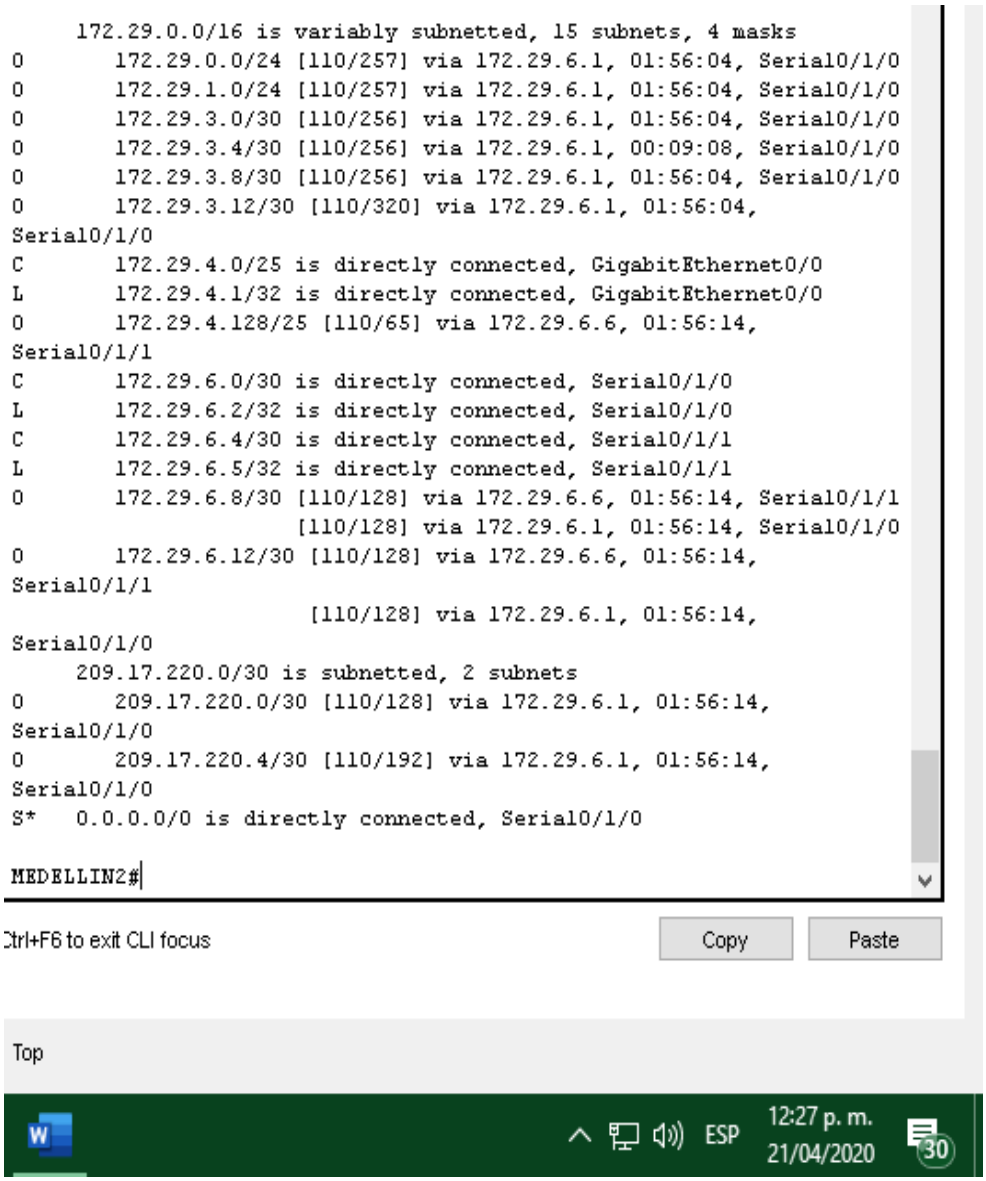

Figura 36. Esc2. Redes conectadas directamente Medellín2.

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

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

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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 39. Esc2. Interfaces de router.

BOGOTA1
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface s0/2/1

BOGOTA2
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface g0/0

BOGOTA3
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface g0/0

MEDELLIN1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface ss0/2/1

MEDELLIN2
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface g0/0

MEDELLIN3
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface g0/0

Parte 4: Verificación del protocolo OSPF.

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 lograr la verificación de este protocolo y a su vez la versión en un router, debemos ingresar de manera esencial por el modo privilegiado ya que de esta maneras lograremos realizar la verificación de manera exitosa, y esto se realizará ejecuntando el comando: <<show ip protocols>>

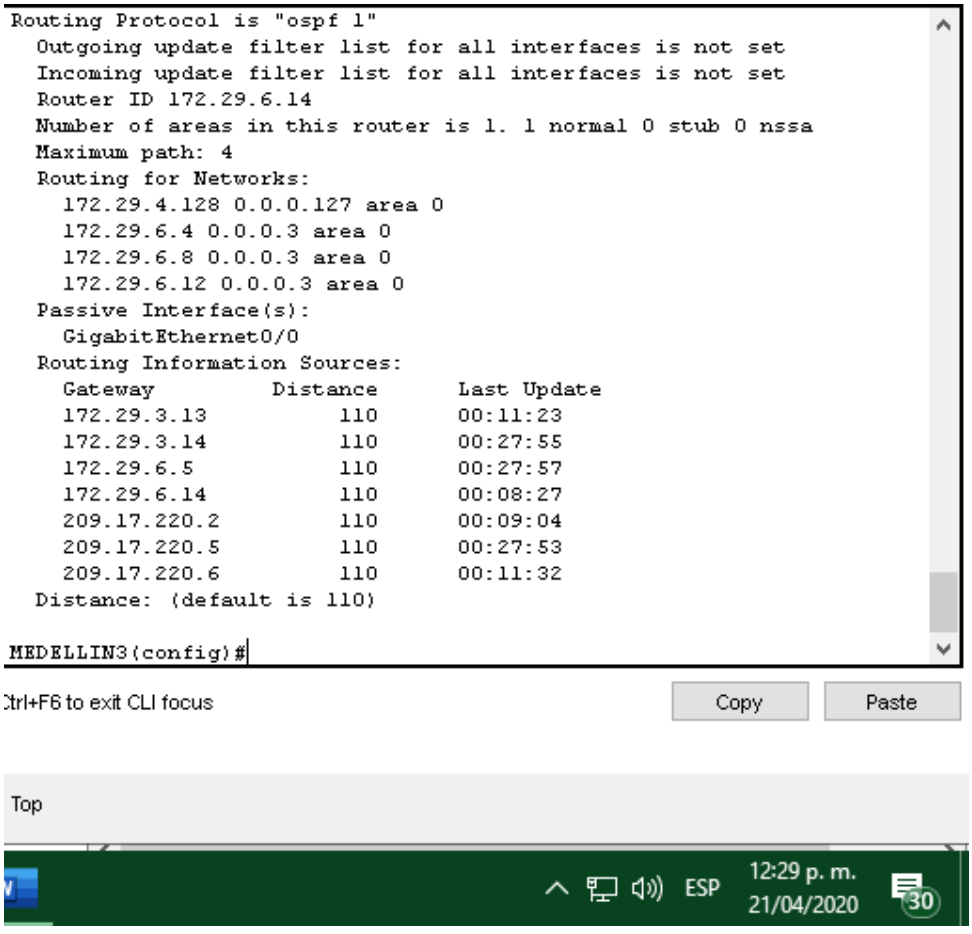

Figura 37. Verificar OSPF Medellín3.

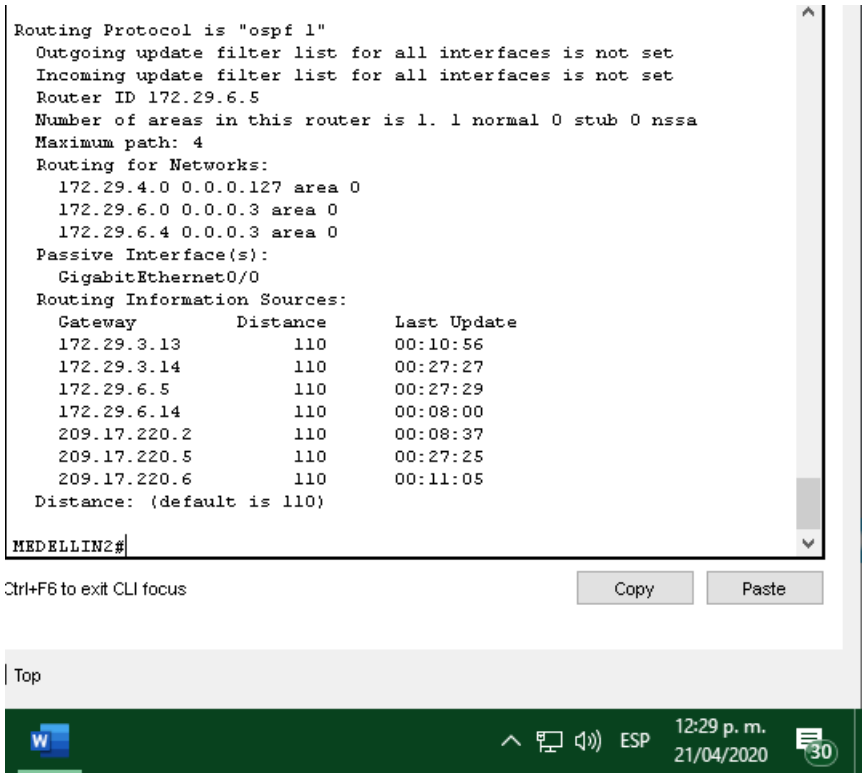

Figura 38. Verificar OSPF Medellín2.

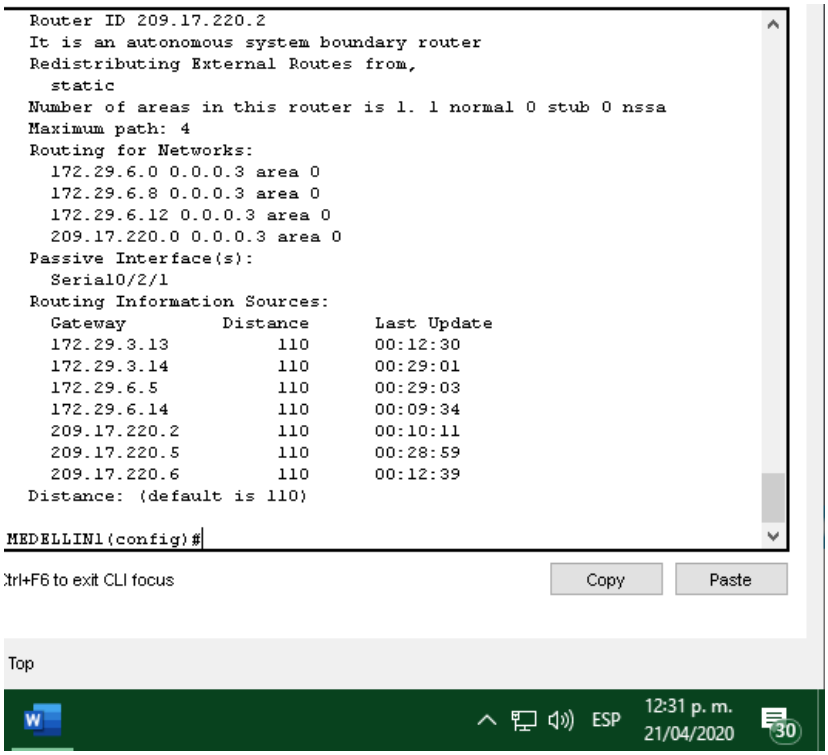

Figura 39. Verificar OSPF Medellín1.

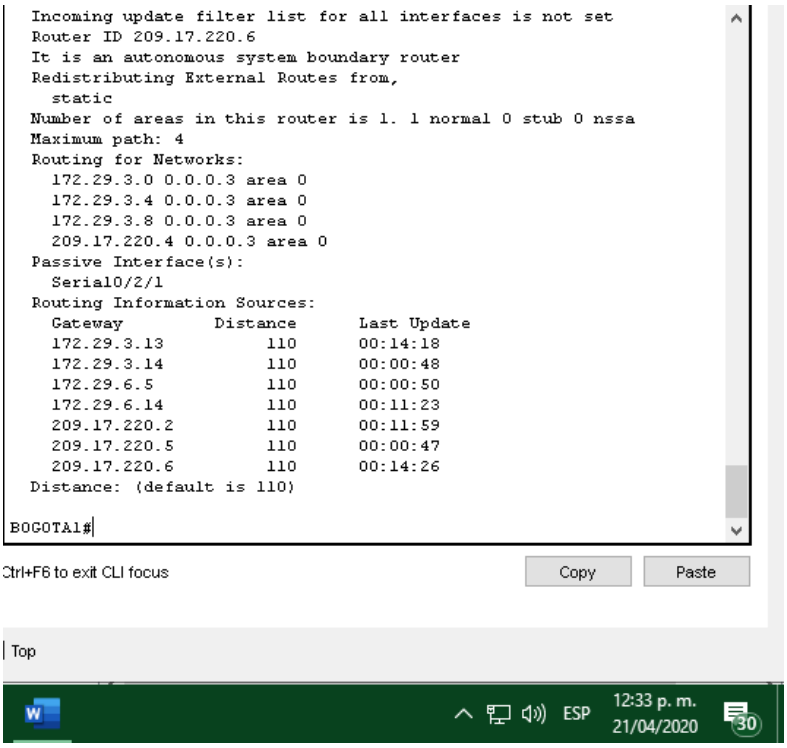

Figura 40. Verificar OSPF Bogotá1.

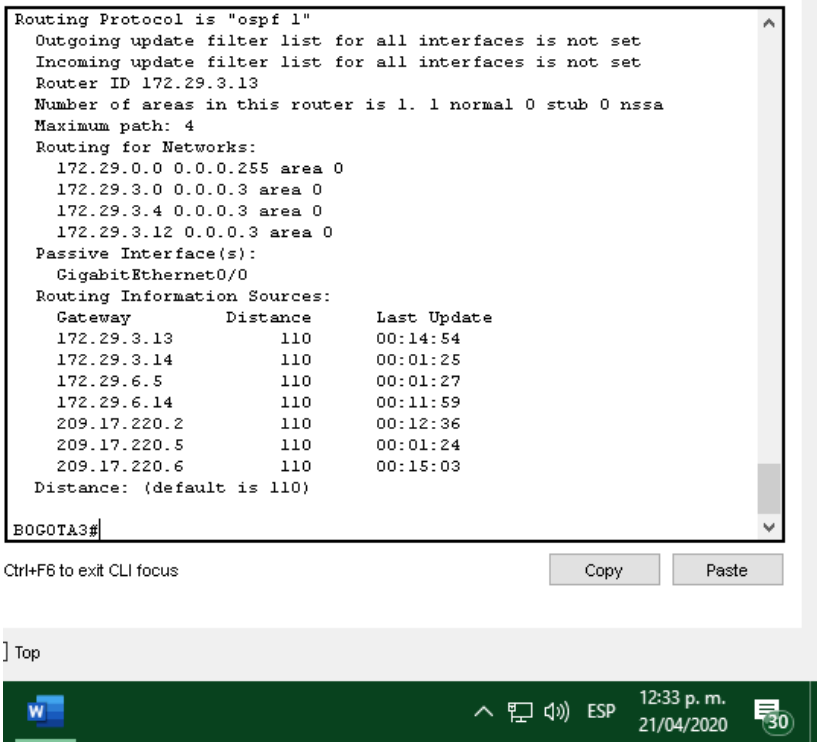

Figura 41. Verificar OSPF Bogotá3.

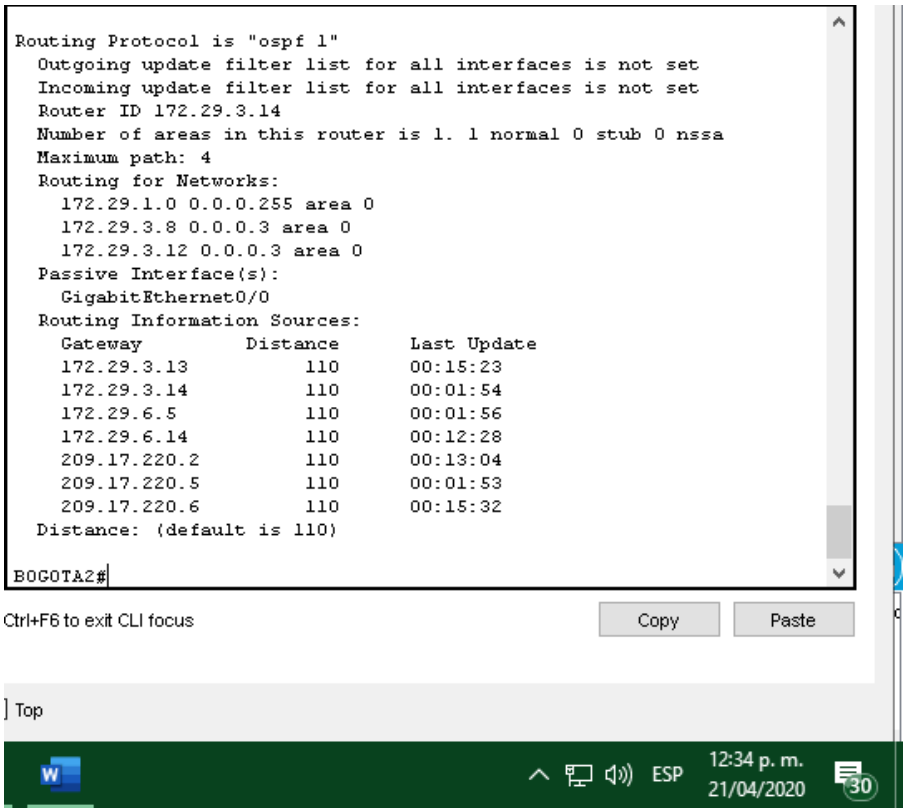

Figura 42. Verificar OSPF Bogotá2.

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

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

MEDELLIN 1
username ISP secret 5 ISP
interface Serial0/1/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username MEDELLIN1 password 0 MEDELLIN

(Para el caso de Medellín1, se creó un usuario con su respectiva contraseña desde el ISP y se configuró la interfaz con: “encapsulation ppp” con la ayuda del usuario local).

ISP
username BOGOTA1 secret 5 BOGOTA1
username MEDELLIN1 secret 5 MEDELLIN1
interface Serial0/3/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username ISP password 0 ISP
no keepalive

interface Serial0/3/1
encapsulation ppp
ppp authentication chap
no keepalive

(Para Bogotá1 se asignó un usuario local, a Medellín1 se creó usuario local, se configura de igual forma la interfaz con: “ppp authentication pap”, y se le aplica la misma configuración a la interfaz que dirige hacia Bogotá).

BOGOTA1
username ISP secret 5 ISP
interface Serial0/1/0
encapsulation ppp
ppp authentication chap

(Como ya se había mencionado, se le asigna un usuario local a Bogotá1, y esta vez se configura interfaz con: “ppp authentication chap”).

Parte 6: Configuración de PAT.

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

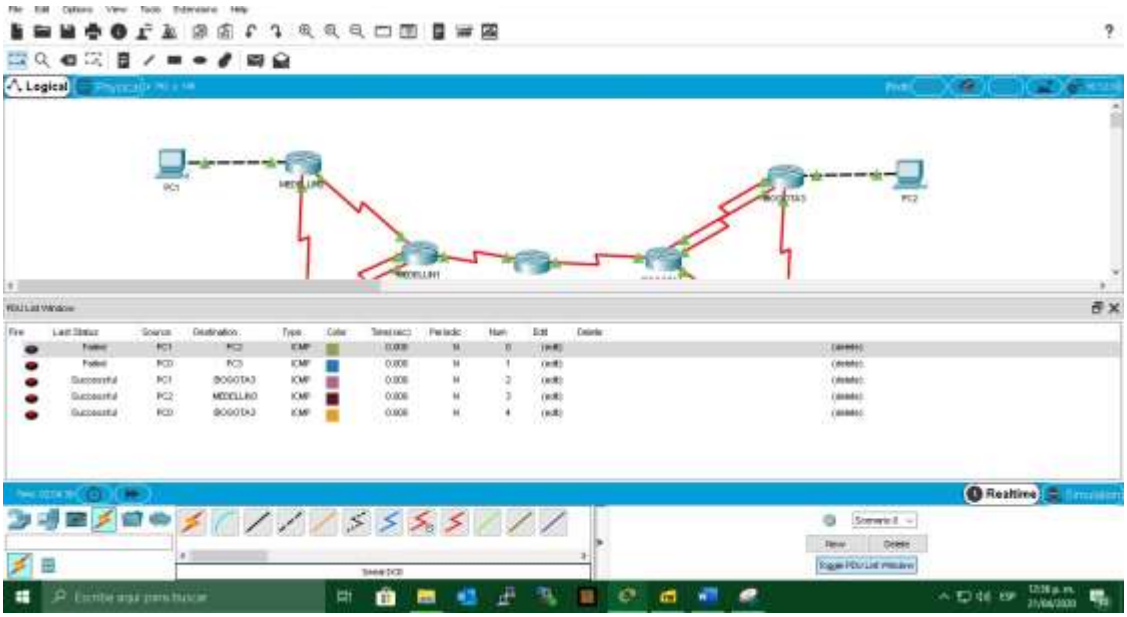

Figura 43. Topología, configuración de PAT.

Procedemos a configurar el NAT en el router Medellín1. Comprobamos que la traducción de direcciones indique las interfaces de entrada y de salida. Cuando se realiza 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.

"Hubo inconvenientes al realizar la respectiva configuración de PAT, debido a que no estaban configuradas las interfaces internas correspondientes al documento, sin embargo se dió una solución apropiada para resolver el problema asignando las interfaces dentro de las configuraciones del equipo"

MEDELLIN1
ip access-list standard HOST
permit 172.29.4.0 0.0.0.255
ip nat inside source list HOST interface Serial0/1/0 overload
interface Serial0/1/0
ip nat outside

interface Serial0/1/1
ip nat inside

interface Serial0/2/0
ip nat inside
interface Serial0/2/1
ip nat inside

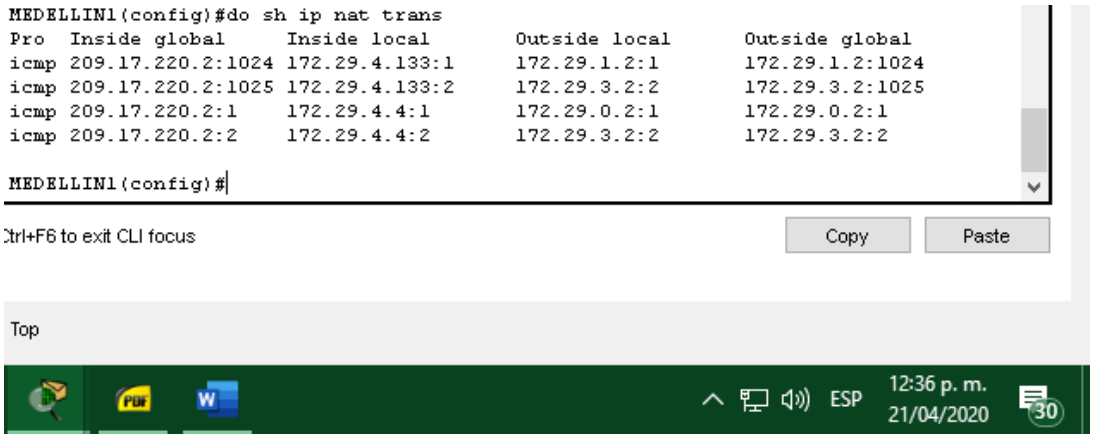

Figura 44. NAT Medellín1.

Procedemos a configurar el NAT en el router Bogotá1. Comprobamos que la traducción de direcciones indique las interfaces de entrada y de salida. Cuando se realiza 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.

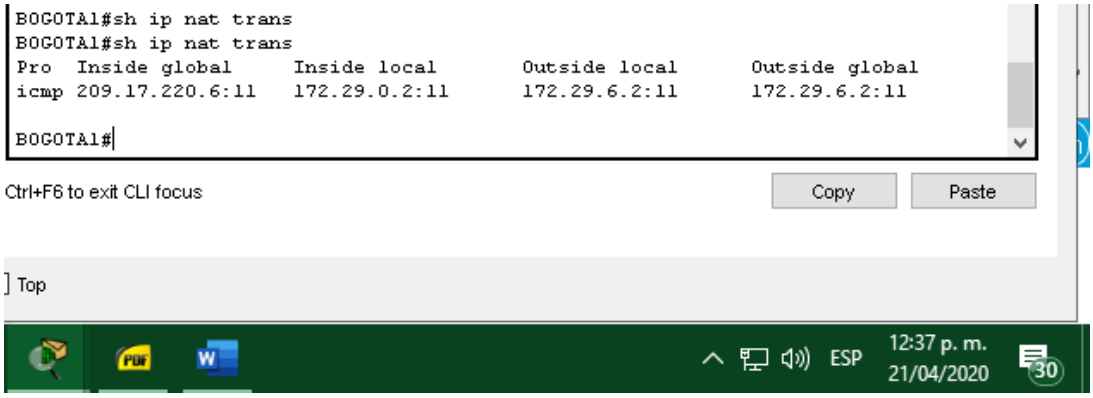

Figura 45. NAT Bogotá1.

ip access-list standard HOST
permit 172.29.0.0 0.0.0.255

```
ip nat inside source list HOST interface Serial0/1/0 overload
interface Serial0/1/0
ip nat outside

interface Serial0/1/1
ip nat inside
interface Serial0/2/0
ip nat inside

interface Serial0/2/1
ip nat inside
```

Parte 7: Configuración del servicio DHCP.

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

Para poder realizar esta configuración debemos realizar los siguientes pasos:

- ❖ Excluir direcciones que nos indiquen.
- ❖ Crear primer pool de direcciones para Medellín2.
- ❖ Crear tercer pool de direcciones para Medellín2.
- ❖ Crear pool para direcciones Bogotá2.
- ❖ Crear pool para direcciones Bogotá3.

```
MEDELLIN2
ip dhcp excluded-address 172.29.4.1 172.29.4.3
ip dhcp excluded-address 172.29.4.129 172.29.4.132

ip dhcp pool MEDELLIN2
network 172.29.4.0 255.255.255.128
default-router 172.29.4.1
dns-server 8.8.4.4
ip dhcp pool MEDELLIN3
network 172.29.4.128 255.255.255.128
default-router 172.29.4.129
dns-server 8.8.4.4
ip dhcp pool BOGOTA2
network 172.29.0.0 255.255.255.0
default-router 172.29.0.1
dns-server 8.8.8.8
ip dhcp pool BOGOTA3
network 172.29.1.0 255.255.255.0
```

default-router 172.29.1.1
dns-server 8.8.8.8

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

MEDELLIN3
interface GigabitEthernet0/0
ip helper-address 172.29.6.5

(Para esto debemos permitir el paso de broadcast)

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

BOGOTA2
interface GigabitEthernet0/0
ip helper-address 172.29.6.2

BOGOTA3
interface GigabitEthernet0/0
ip helper-address 172.29.6.2

(Igual al caso anterior, debemos permitir el paso de broadcast)

- Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Medellin2.

BOGOTA1

Interface s0/2/0
ip helper-address 172.29.6.2

Interface s0/1/1
ip helper-address 172.29.6.2

(De igual manera debemos permitir el paso de broadcast)

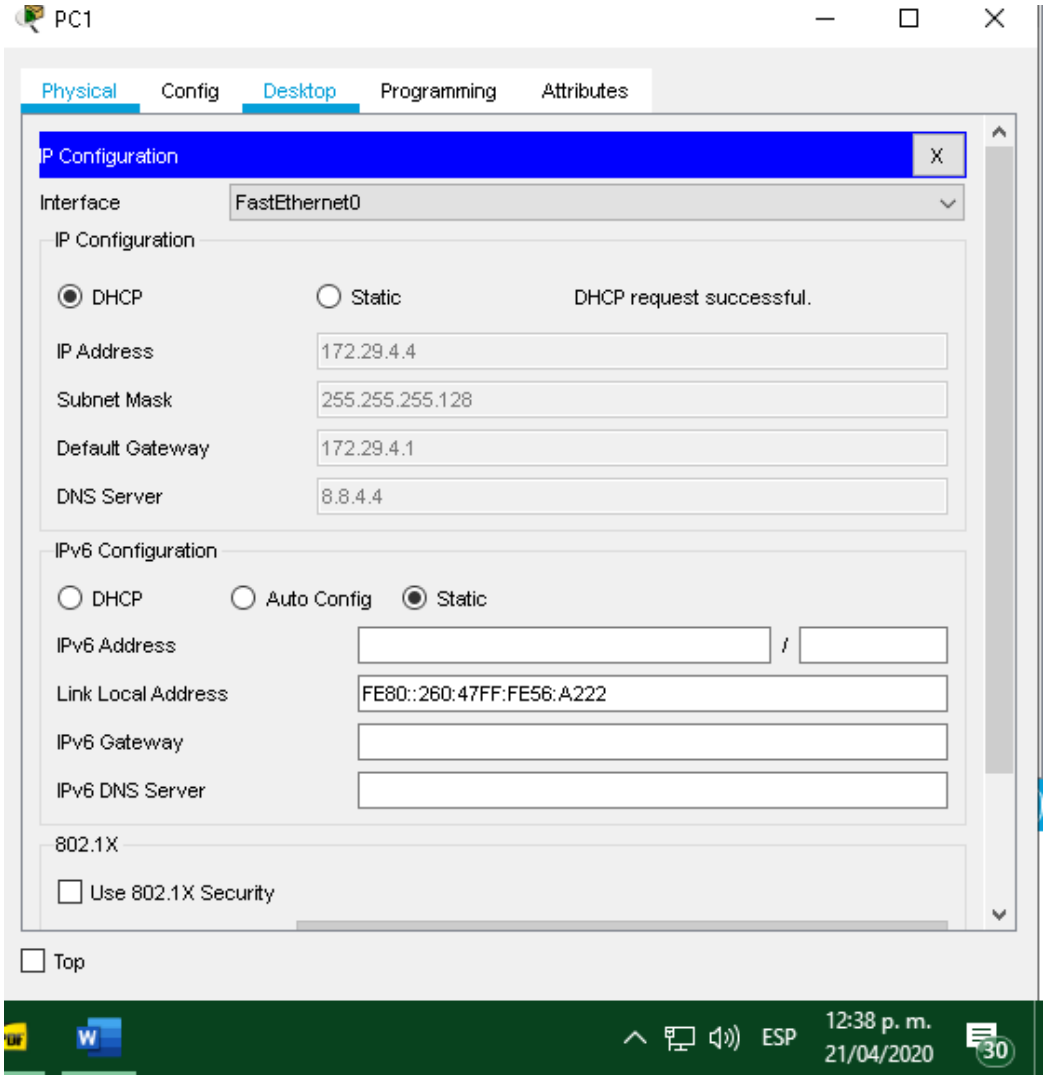

Figura 46. Router – IP 172.29.4.4

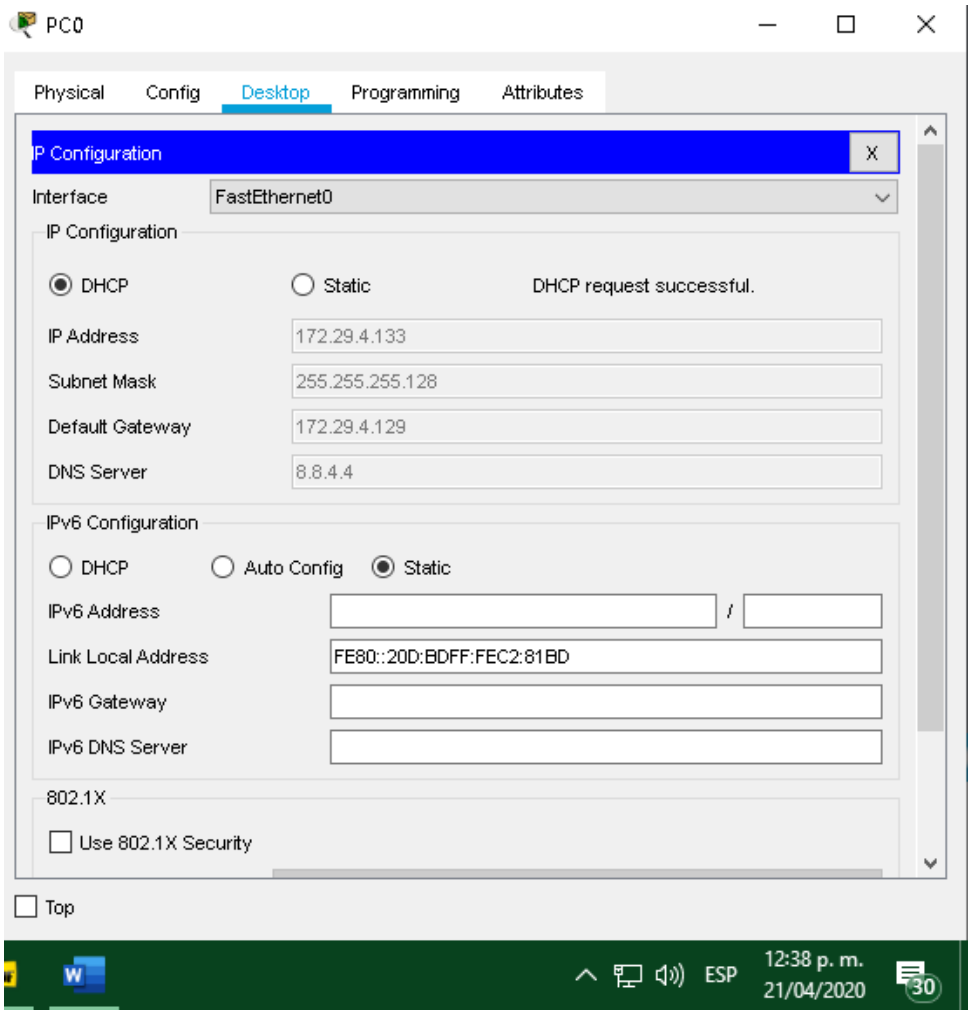

Figura 47. Router – IP 172.29.4.133

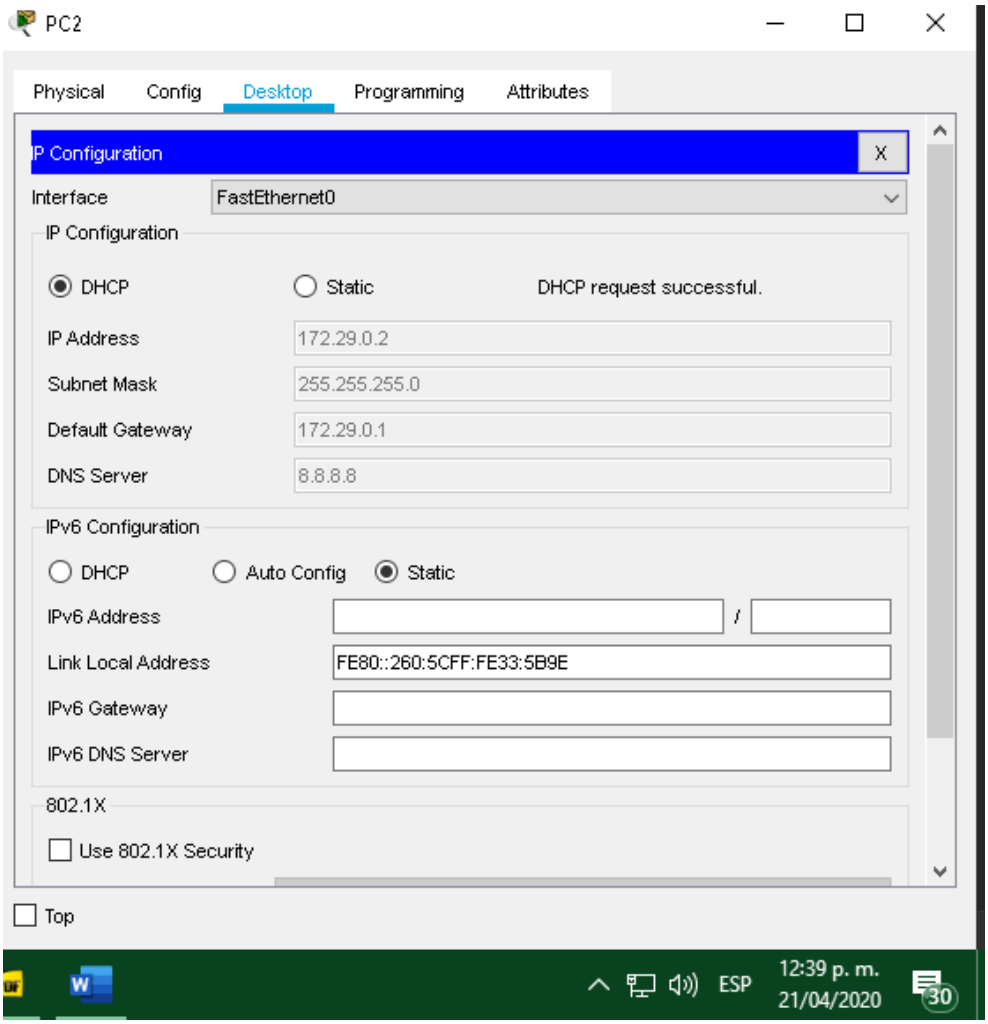

Figura 48. Router – IP 172.29.0.2

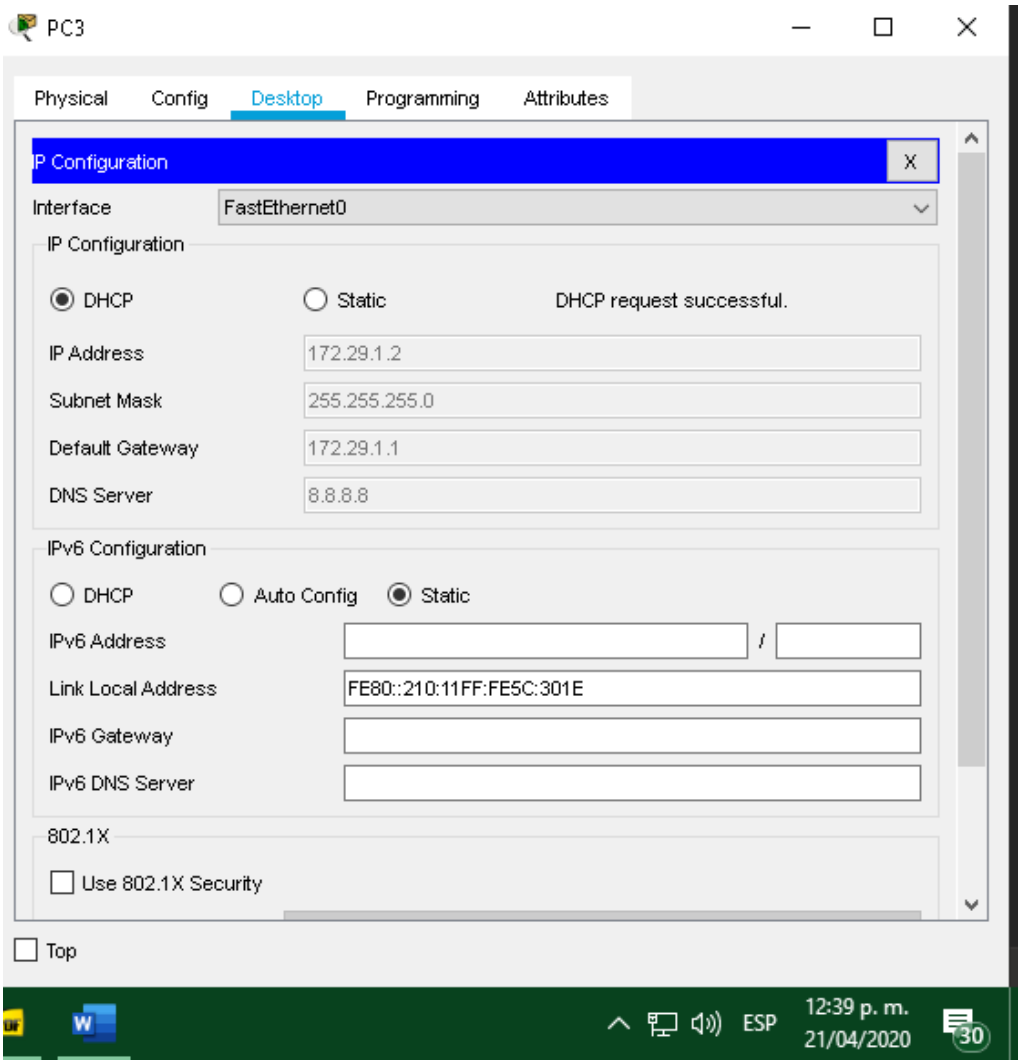

Figura 49. Router – IP 172.29.1.2

2. CONCLUSIONES

Como estudiantes logramos sentirnos satisfechos al saber que gracias a cada uno de los conocimientos adquiridos durante la realización del curso de diplomado de profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN) se pudo realizar de manera exitosa los dos casos de estudios establecidos para este desarrollo.
Se logró implementar de manera correcta las herramientas de simulación gráfica de red GNS3 y Packet Tracer, en la solución de los dos escenarios estipulados y permitiendo de igual forma cumplir con los objetivos establecidos.

Durante el desarrollo de pruebas de habilidades se logró configurar de manera exitosa cada uno de los comandos establecidos en los dos escenarios, permitiendo capacitarnos como futuros profesionales con un desempeño aceptable en el área de redes, como por ejemplo el desarrollo de enrutamientos, configuración de routers, direccionamientos IP, configuración de servicio DHCP, verificación de conectividad de red, entre otras incluidas en el documento.

3. REFERENCIAS BIBLIOGRÁFICAS

"IPv4 y IPv6 de la configuración en un punto de acceso de red inalámbrica". {En línea}. {13 de diciembre 2018}. Disponible en: (https://www.cisco.com/c/es_mx/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5176-configure-ipv4-and-ipv6-on-a-wireless-access-point.html)

CISCO "Asignación de direcciones IP. Fundamentos de Networking". {En línea} {2014} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO "Capa de Transporte. Fundamentos de Networking" {En línea} {2014}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO "Capa de Aplicación. Fundamentos de Networking". {En línea} {2014} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO "Soluciones de Red. Fundamentos de Networking". {En línea} {2014} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO "SubNetting. Fundamentos de Networking". {En línea} {2014}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

García, Jesús "Como configurar: HDCP, DNS, HTTP Y Conexión inalámbrica". {En línea}. {17 septiembre de 2015}. Disponible en: (https://outlook.office.com/mail/inbox/id/AAQkADgzNDdjZWQ5LWJlOGItNDdkNy1iYTJlLTJiNGMwYzdjZWNhYQAQAGOZUAkpNA1Dnhq4ZTIeNuE%3D)

Vesga, J. "PING y TRACER Como estrategia en procesos de Networking [OVA]" {En línea} {2014}. Disponible en: (https://1drv.ms/u/s!AmlJYei-NT1IhgTCtKY-7F5KIRC3)