SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

KATERINE FERNÁNDEZ CARVAJAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
NEIVA-HUILA
JULIO 2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

KATERINE FERNÁNDEZ CARVAJAL

DOCUMENTO FINAL PARA GRADO

TUTOR

GUSTAVO ADOLFO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
NEIVA-HUILA
JULIO 2020

RESUMEN

El objetivo del siguiente trabajo tiene como fin demostrar las habilidades obtenidas en el transcurso del Diplomado en Profundización Cisco CCNA, mediante la solución de dos escenarios propuestos de la vida real, que nos llevan a comprender, solucionar y verificar diferentes ejercicios de configuración de switches y router mediante configuraciones de topologías de red y con el apoyo de la herramienta de simulación Packet Tracer.

ABSTRACT

The objetive of this paperis to demonstrate the skills obtained in the course of the Cisco CCNA Diplomado in Deepening, by solving two proposed real-life scenarios, which lead us to understand, solve and verify different switch configuration exercises and router using network topology tools and supported by Packet Tracer simulation tool

TABLA DE CONTENIDO

Pag.

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

En el presente trabajo se evidenciará el desarrollo de dos escenarios propuestos del trabajo final prueba de habilidades donde se detallan aspectos básicos de cómo funcionan las redes en entornos generales LAN y WAN a nivel de routing y switching, se comprenden las bases de la IPv4 e IPv6, configuraciones de equipos Cisco y demás elementos generales que hacen parte de CCNA1.

En el desarrollo de las habilidades y profundización en el diplomado de cisco segundo escenario, ponen a prueba la implementación de diferentes comandos de protocolos destacando el routing dinámico OSPF, la configuración de DHCP como servidor, la NAT, ACL. Cada uno de estos comandos son desarrollados a través de la implementación de las habilidades obtenidas en el transcurso del diplomado con la eficacia del desarrollo de cada una las actividades propuestas en el entorno de aprendizaje mediante la herramienta de simulación Packet Tracer.

Como consecuencia del desarrollo y los altos conocimiento de las habilidades aprendidas para poder desarrollar el documento final descrito como dos escenarios donde se implementan los protocolos establecidos mencionados anteriormente y complementados con las habilidades básicas de configuración de los dispositivos utilizados.

OBJETIVOS

Objetivo General:

Adquirir conocimientos en los conceptos de routing y switching mediante el desarrollo de los ejercicios propuestos en el escenario 1, los cuales serán simulados en la herramienta Cisco Packet Tracer

Objetivos específicos:

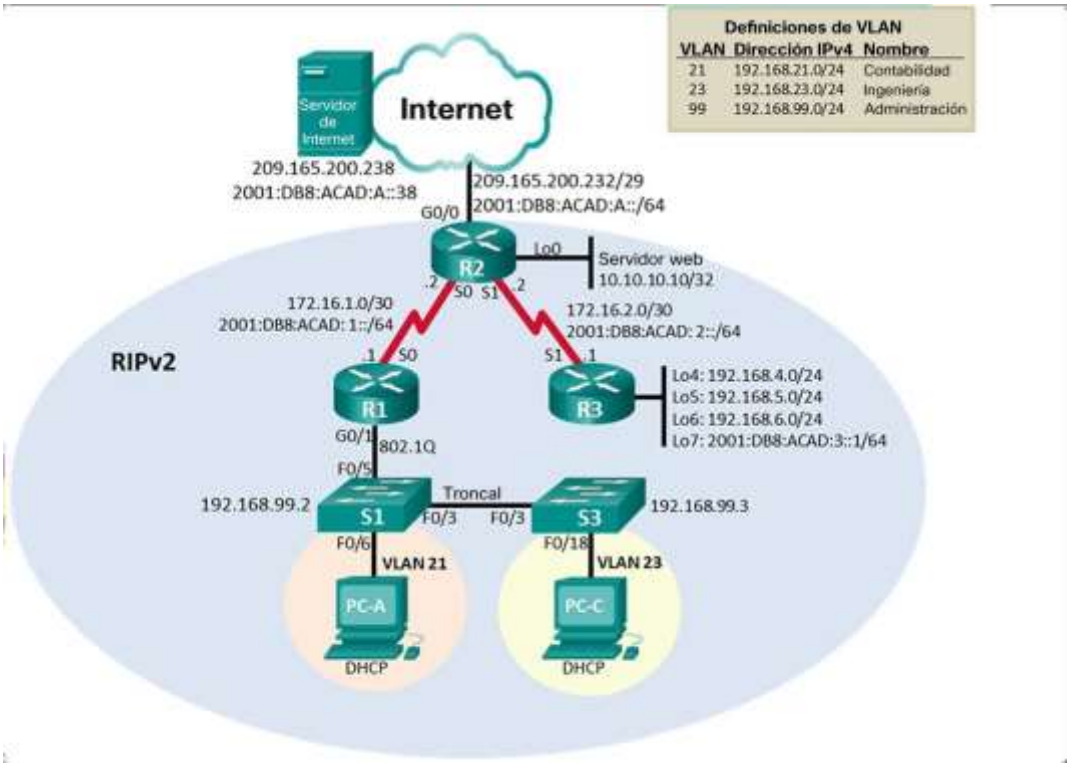
- Configurar equipos con sus correspondientes direccionamientos solicitados en la guía.
- Validar conectividad y restricciones en los equipos.
- Evidenciar los resultados obtenidos una vez se han aplicado las configuraciones en la herramienta de simulación Cisco Packet Tracer facilitadora de las configuraciones, análisis y obtención de resultados de acuerdo con el funcionamiento de la red configurada.

DESARROLLO ESCENARIO 1

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

Topología

Figura 1 Topología de red



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.

Se procede a configurar los dispositivos iniciando por una eliminación y reiniciación de los mismos, verificando que la base de datos VLAN no esté en la memoria flash de ambos switches. Con este proceso se verificará que los router no tengan datos cargados.

Tabla 1 Inicializar dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router› en 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# show vlan

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Se procede a configurar el dispositivo *servidor_internet* para simular el acceso a la nube con los parámetros establecidos, se establecen las direcciones IPv4, Ipv6/subred y sus respectivas Gateway predeterminado.

Tabla 2 Configuración de Parámetros

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes: Se procede a realizar la configuración base del R1, se configura nombre, contraseñas, mensaje motd y configuración de interfaz serial para conexión con R2.Se configuran rutas predeterminadas para que queden asociadas a la interfaz s0/0/0, con esta configuración todos los router tienen parámetros de iniciación.

Tabla 3 Configuración de parámetros R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router›en Router#configure t Router(config)#no ip domain-lookup
Nombre del router	Router›en Router#configure t Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#Description Conexion R1 y R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	S0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 S0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:
Se procede a realizar la configuración base del R2, se cambia nombre, contraseñas, mensaje motd y configuración de interfaz g0/0 para simular conexión a internet. Se configuran rutas predeterminadas para que queden asociadas a la interfaz g0/0, con esta configuración todos los router tienen parámetros de iniciación.

Tabla 4 Configuración de parámetros R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router›en Router#configure t Router(config)#no ip domain-lookup
Nombre del router	Router›en Router#configure t Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	Packet tracer no soporta este comando
Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado. #

Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description Conexion entre R2 y R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description Conexion R2 y R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description Conexion R2 a Internet R2(config-if)#ip address 209.165.200.232 255.255.255.248 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#int loopback 0 R2(config-if)#description interface Loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit R2(config)#int g0/1 R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shutdown R2(config-if)#
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Se realiza las siguientes configuraciones del R3: Nombre, contraseñas, mensaje motd, configuración de interfaz serial para conexión con R2. Se configuran rutas predeterminadas para que queden asociadas a la interfaz s0/0/1, se configuran interfaces loopback.

Tabla 5 Configuración de parámetros R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #se prohibe elacceso no autorizado#
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)# description conexion R2 y R3 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit R3(config)#

Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit R3(config)#
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit R3(config)#
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Se procede a configurar parámetros en el Switch 1, desactivando DNS, cambio de nombre, contraseñas de acceso a la consola y acceso telnet, configuración de cifrado las contraseñas de texto no cifrado y mensaje motd, por lo tanto, tiene parámetros para cuando ingrese a la consola.

Tabla 6 Configuración de parámetros S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohibe el acceso no autorizado. #

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:
Se procede a realizar las siguientes configuraciones a Switch 3: Desactivación del DNS, Cambio de nombre, contraseñas y mensaje motd, también el cifrado de contraseñas de texto, por lo tanto, tendrá parámetros de inicio cuando ingrese a la consola.

Tabla 7 Configuración de parámetros S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado.#

Paso 7: Verificar la conectividad de la red

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

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

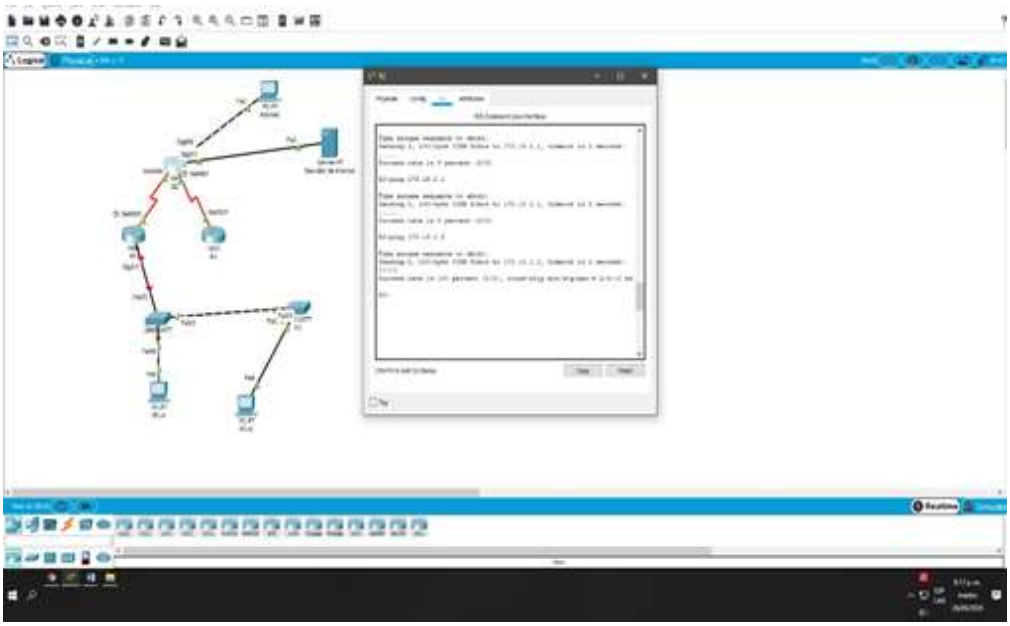
Se procede a realizar pruebas de ping a R1 hasta R2, y de R2 a R3 para verificar el enrutamiento de las cuales dan conexiones exitosas.

Tabla 8 Verificar conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/16 ms
R2	R3, S0/0/1	172.16.2.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/15 ms
PC de Internet	Gateway predeterminado		

Figura 2 Pruebas de Ping R1

Figura 3 Pruebas de Ping R2



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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas

Se procede a realizar las siguientes configuraciones a Swicth 1: Creación de base de datos de VLAN 21-23- 99, con el fin de identificar áreas se realiza asignación de nombres, asignación de direccionamiento, configuración del Gateway predeterminado. Se configura la interfaz f0/5 como puerto troncal.

Tabla 9 Configuración seguridad S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shut
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range f0/1, f0/2, f0/4, f0/7- 24, g0/1-2 S1(config-if-range)#switchport mode Access
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2 S1(config-if-range)#shut S1(config-if-range)#interface f0/4 S1(config-if)#shut S1(config-if)#interface range f0/7-24 S1(config-if-range)#shut S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#shut

Paso 2: Configurar seguridad el S3

La configuración del S3 incluye las siguientes tareas:

Se procede a realizar la configuración de Switch3 se le crea la base de datos de las VLAN 21-23-99, con el finde identificar áreas se le asignan sus correspondientes nombres, se configura el direccionamiento de la vlan 99 y el puerto f0/3 como troncal, los demás puertos se dejan en modo de acceso. Los puertos que no están en uso se apagan

Tabla 10 Configuración seguridad S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la direcciónIP de administración	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 23 (se modifica teniendo en cuenta que en grafico aparece vlan 23)	S3(config)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar seguridad R1

Las tareas de configuración para R1 incluyen las siguientes:

Para realizar su respectivo enrutamiento se procede a realizar la configuración de R1 se le crea la base de datos de las VLAN 21-23-99, se le asignan sus correspondientes sus correspondientes direcciones ip a las interfaces.

Tabla 11 Configuración seguridad R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#int g0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int g0/1.99 R1(config-subif)#description LAN de Administracion 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)#int g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

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

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

Para verificar la conectividad de los router se procede a realizar pruebas de ping entre los dispositivos en la cual todas salen exitosas.

Tabla 12 Verificar conectividad de la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3	R1, dirección VLAN 23	192.168.23.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Figura 4 Pruebas de Ping S1 A R1 dirección vlan99

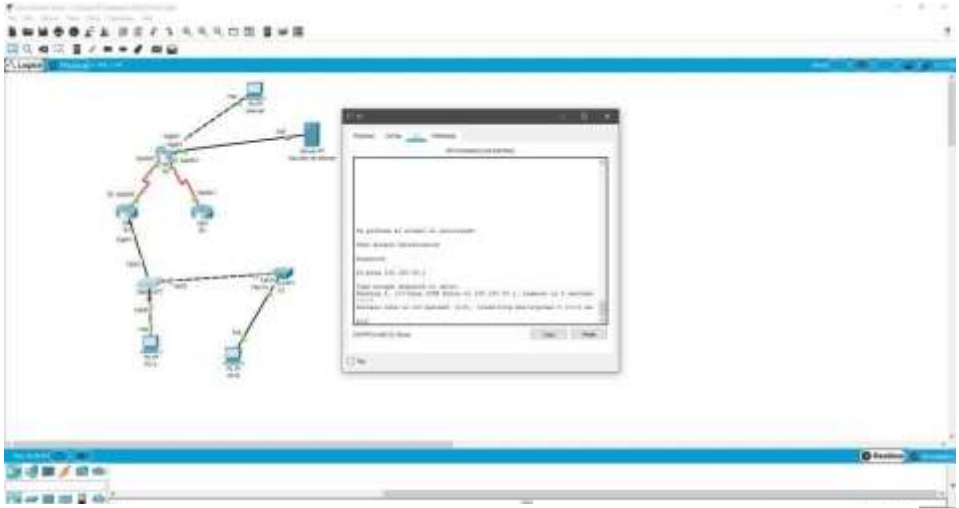


Figura 5 Pruebas de Ping S3 A R1 dirección vlan99

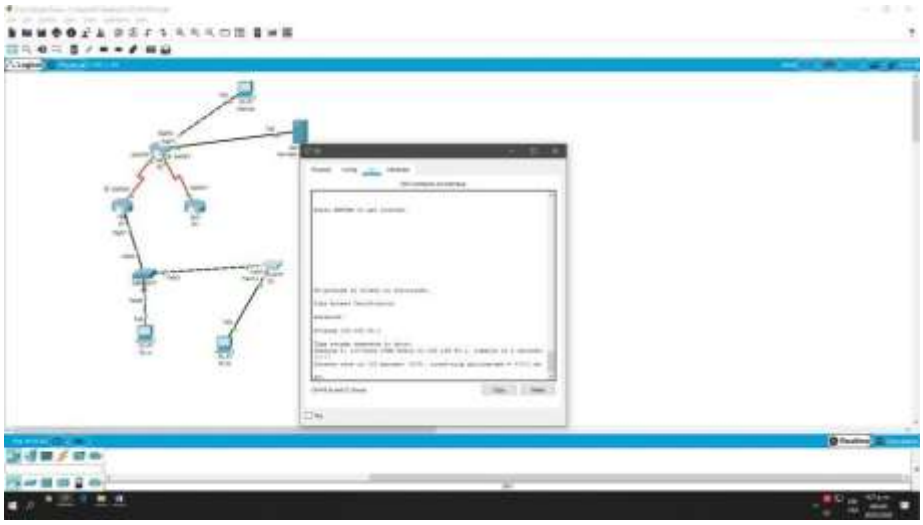


Figura 6 Pruebas de Ping S1 A R1 dirección vlan21

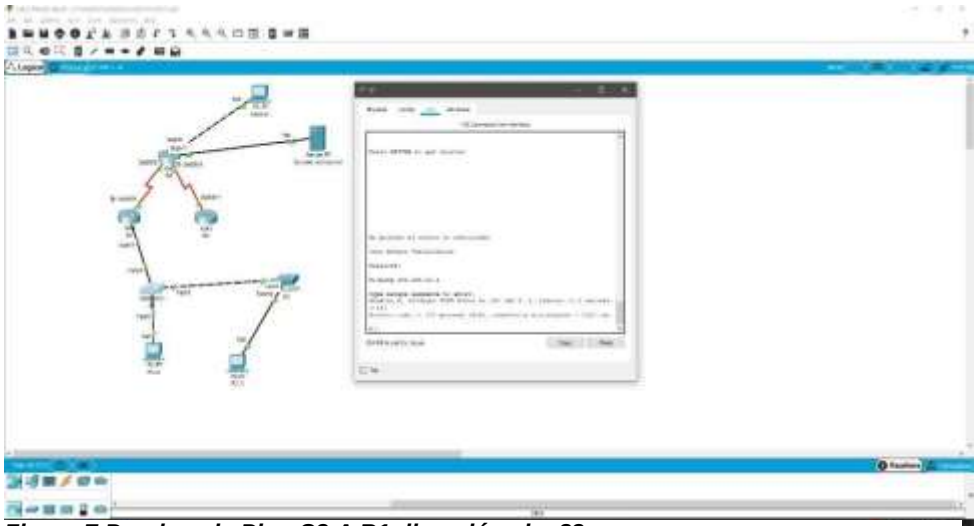
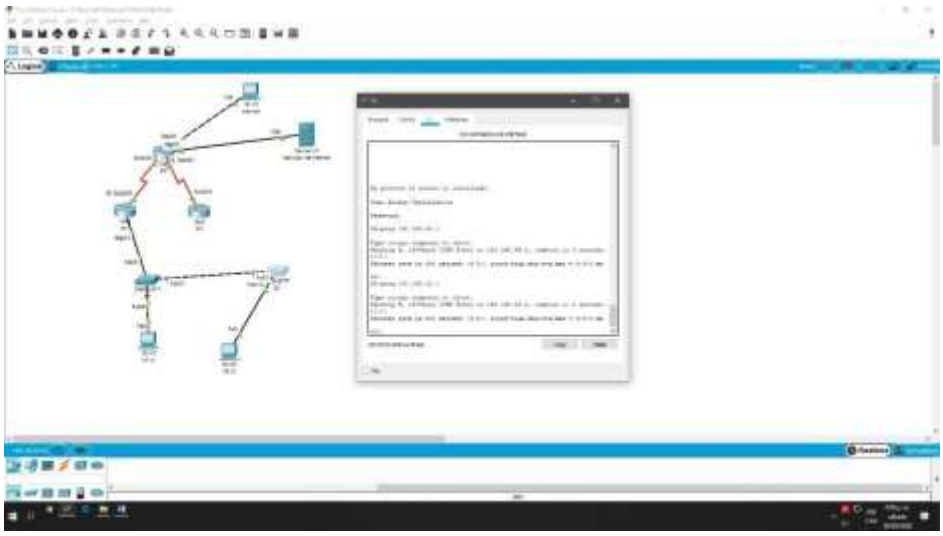


Figura 7 Pruebas de Ping S3 A R1 dirección vlan23



Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Se procede a realizar la configuración de RIPv2 en R1, se anuncian las redes que se han conectado directamente, se establecen las interfaces LAN como pasivas y se desactiva la sumarización automática, todo esto con el fin de permitir que el router intercambie datos de redes, para que el router realice el proceso de buscar la ruta más corta de llegada a su destino.

Tabla 13 Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#ver 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network192.168.21.0 0.0.0.3 area 0 R1(config-router)#network192.168.23.0 0.0.0.3 area 0 R1(config-router)#network192.168.21.0 0.0.0.255 area 0 R1(config-router)#network192.168.23.0 0.0.0.255 area 0 R1(config-router)#network192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface default R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Se realiza configuración RIPV2 a R2, se anuncian las redes que se han conectado directamente, se dejan pasivas las interfaces LAN y por último desactivamos la sumarización automática, todo esto con el fin de permitir que el router intercambie datos de redes, para que el router realice el proceso de buscar la ruta más corta de llegada a su destino.

Tabla 14 Configurar RIPv2 en R2

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#ver 2
Anunciar las redes conectadas directamente	R2(config-router)#network172.16.1.0 0.0.0.3 area 0 R2(config-router)#network172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#no passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Se procede a configurar RIPv3 versión 2 en R3, se anuncian las redes que se han conectado directamente, se dejan pasivas las interfaces LAN y por último desactivamos la sumarización automática, todo esto con el fin de permitir que el router intercambie datos de redes, para que el router realice el proceso de buscar la ruta más corta de llegada a su destino.

Tabla 15 Configurar RIPv3 en R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#ver 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#exit R3(config)#int s0/0/1 R3(config-if)#ipv6 rip unad enable R3(config-if)#int lo7 R3(config-if)#ipv6 rip unad enable R3(config-if)#exit
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#network192.168.4.0 0.0.3.255 area 0 R3(config-router)#network192.168.5.0 0.0.3.255 area 0 R3(config-router)#network192.168.6.0 0.0.3.255 area 0 R3(config-router)#passive-interface loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Paso 4: Verificar la información de RIP

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

Se procede a verificar los enrutamientos mediante los procesos RIP que estén configurados en el R1 para saber si están funcionando de la forma correcta.

Tabla 16 Verificación del RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R1#show ip route R
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1#debug ip rip R1#no debug ip rip

Figura 8 show ip protocols R1

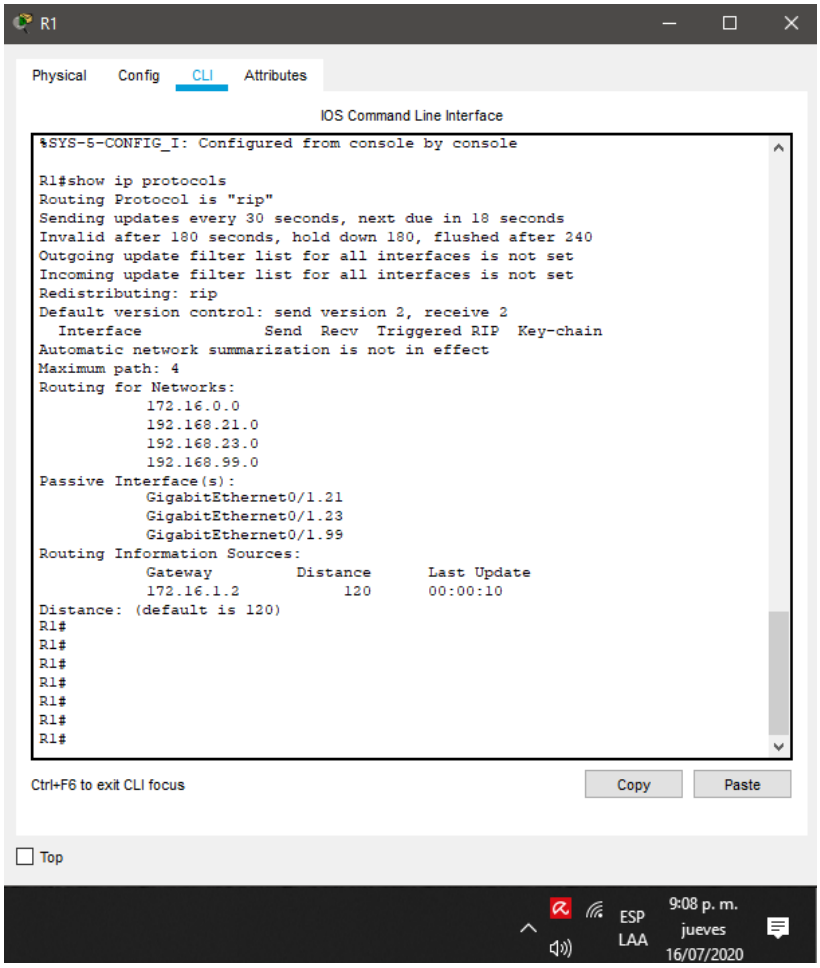


Figura 9 show ip route R-R1

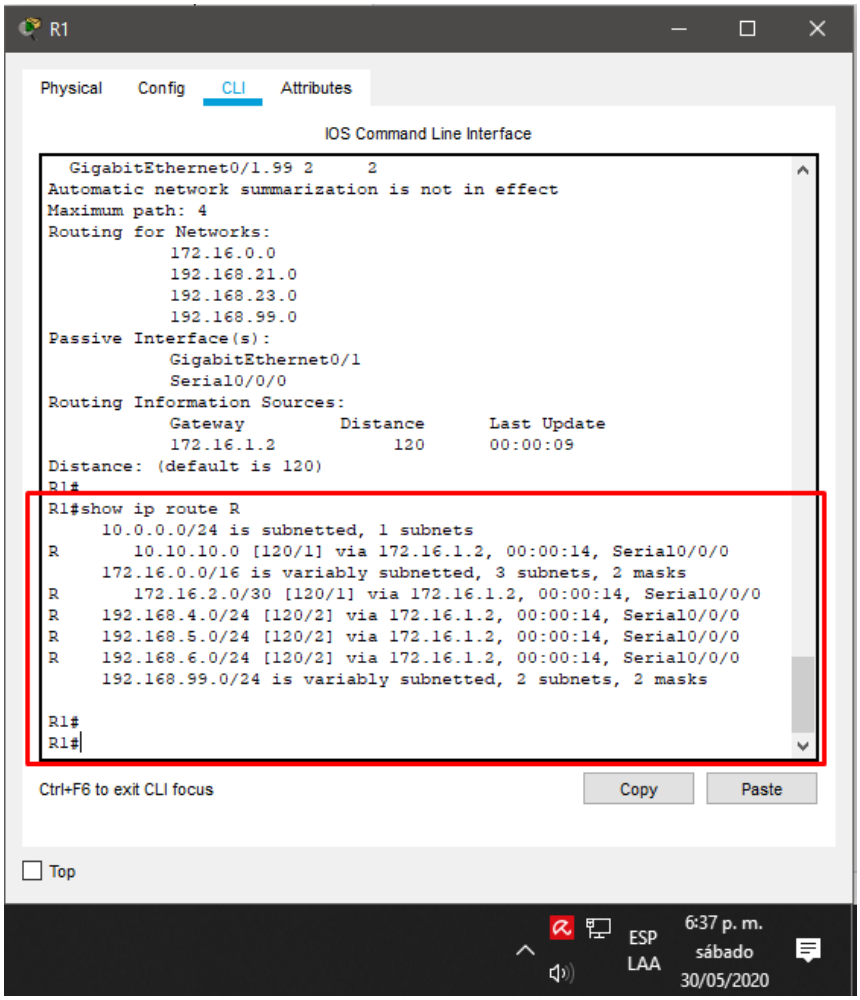
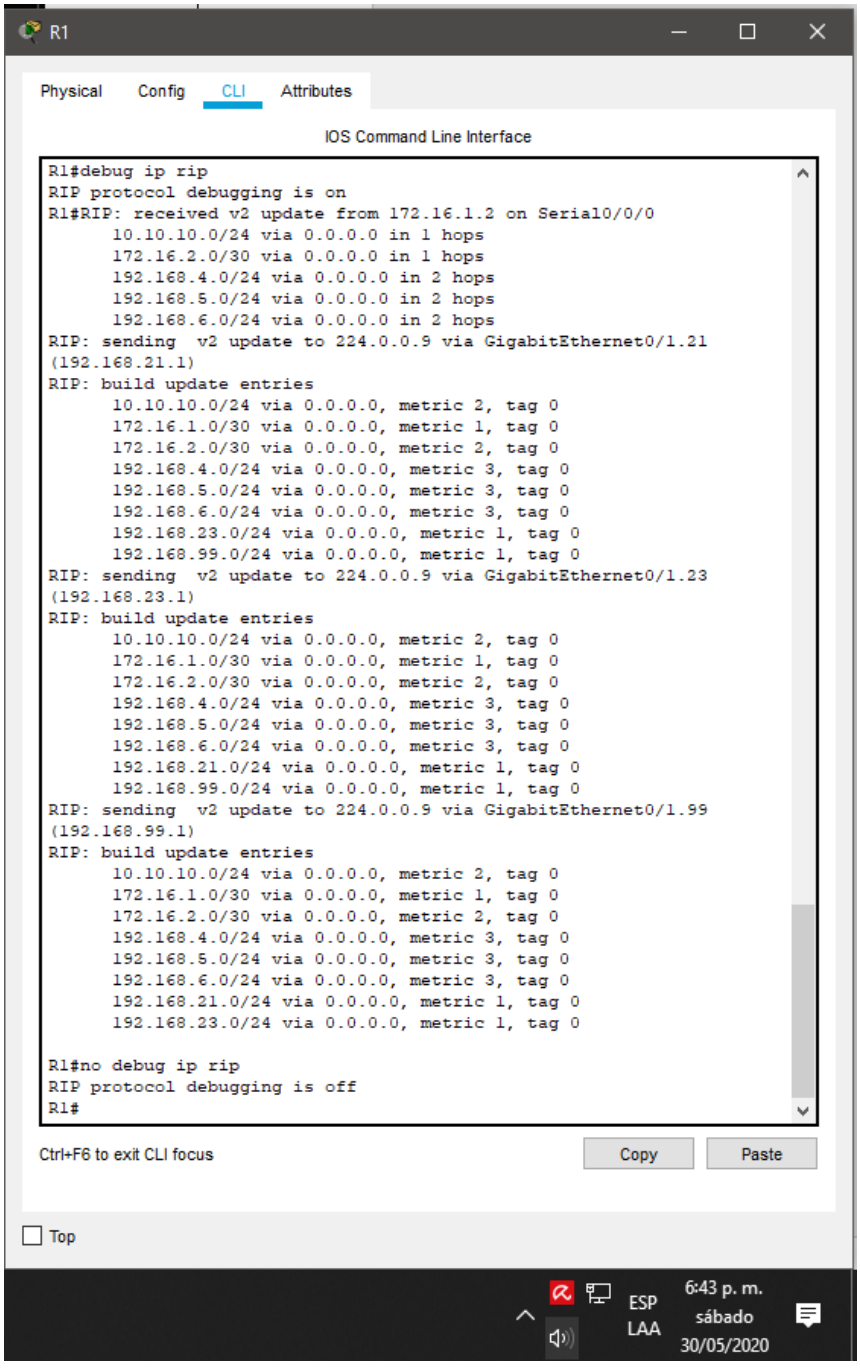


Figura 10 RIP en modo de debug



Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:
Se procede a configurar en R1 el servicio DHCP para que dé direccionamiento a las redes 21-23, también se configura para cada red, DHCP de las primeras 20 IPs.

Tabla 17 DHCP y NAT IPv4 en R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1

Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

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

La configuración del R2 incluye las siguientes tareas:

Se procede a realizar configuraciones de NAT estática para que desde internet el servidor sea visible con la IP 209.165.200.229, comenzando por crear la base de datos local, habilitar el servicio http que en este caso packet tracer no soporta, hasta definir la creación de una NAT dinámica.

Tabla 18 DHCP y NAT IPv4 en R2

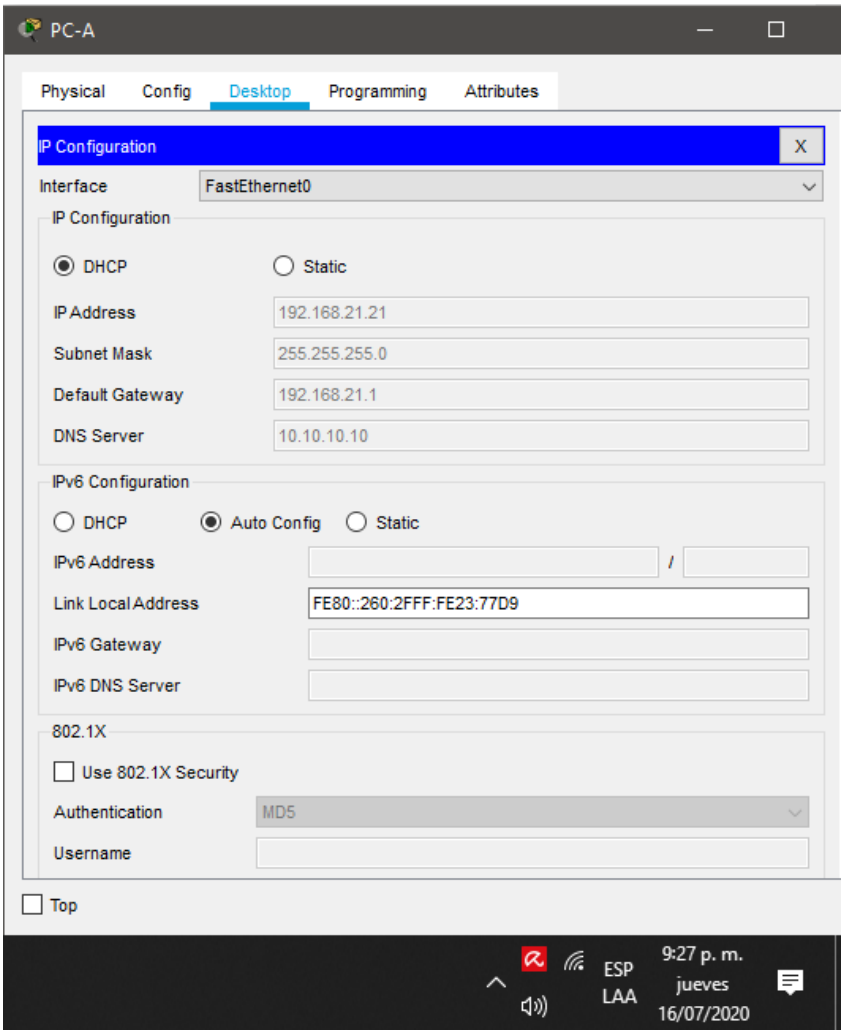
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco 12345
Habilitar el servicio del servidor HTTP	Packet tracer no soporta este comando
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config-if)#interface g0/0 R2(config-if)#ip nat inside R2(config-if)#interface g0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R3(config)#access-list 1 permit 192.168.4.1 0.0.3.255
Defina el pool de direcciones IP públicas utilizables	R2(config)#ip nat pool INTERNET 209.165.200.229 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT di	R2(config)#ip nat inside source list 1 pool INTERNET

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

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente. Se procede a realizar configuraciones en los dispositivos de DHCP y NAT estática para que trabajen bien se realizanlas siguientes actividades configurar PC-A y PC-C, hasta probar la conectividad de los mismos.

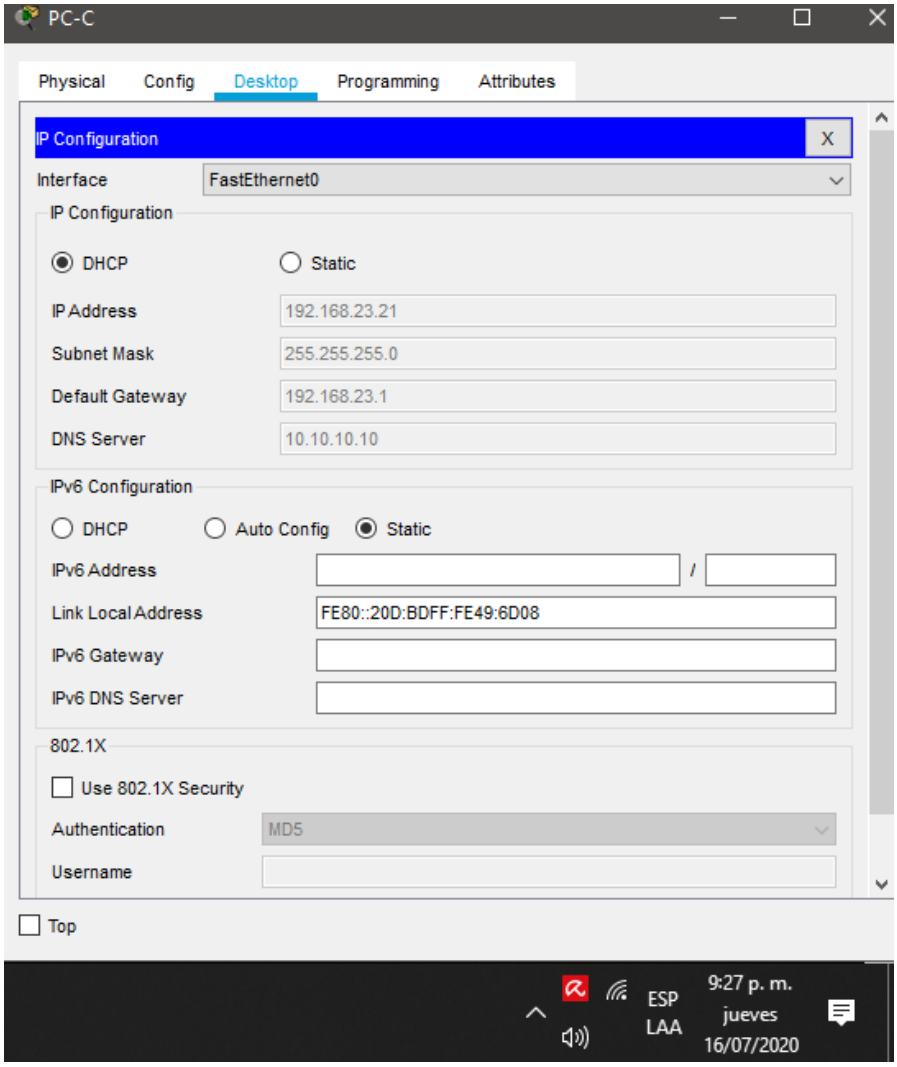
- **Prueba.** Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Figura 11 Configuración PC-A



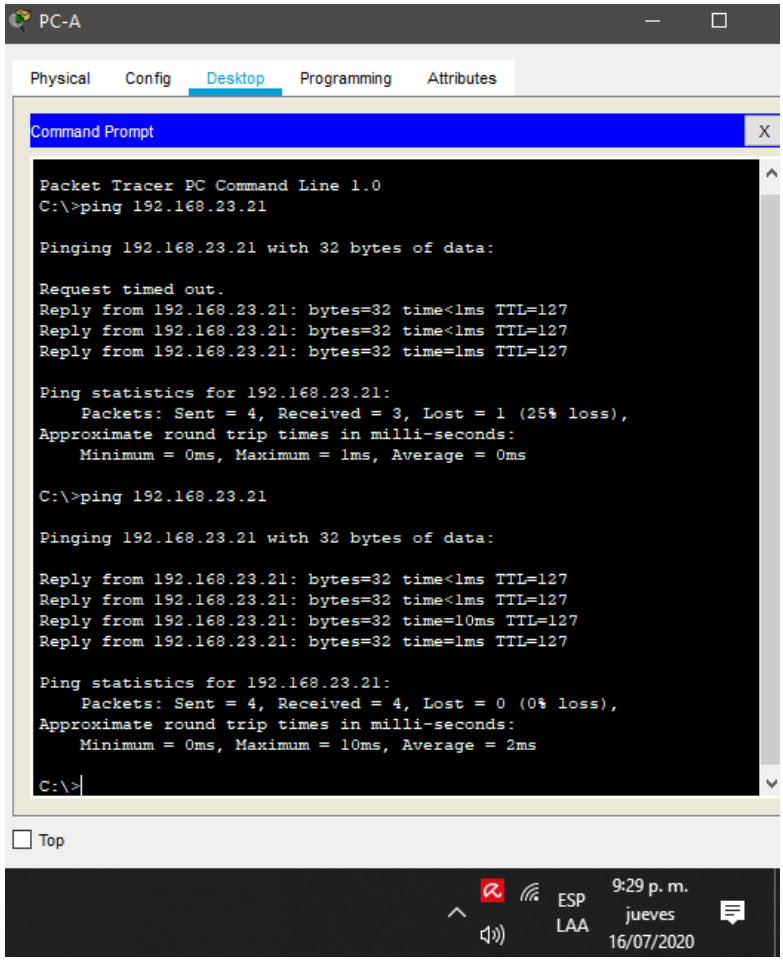
- **Prueba**. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

Figura 12 Configuración PC-C



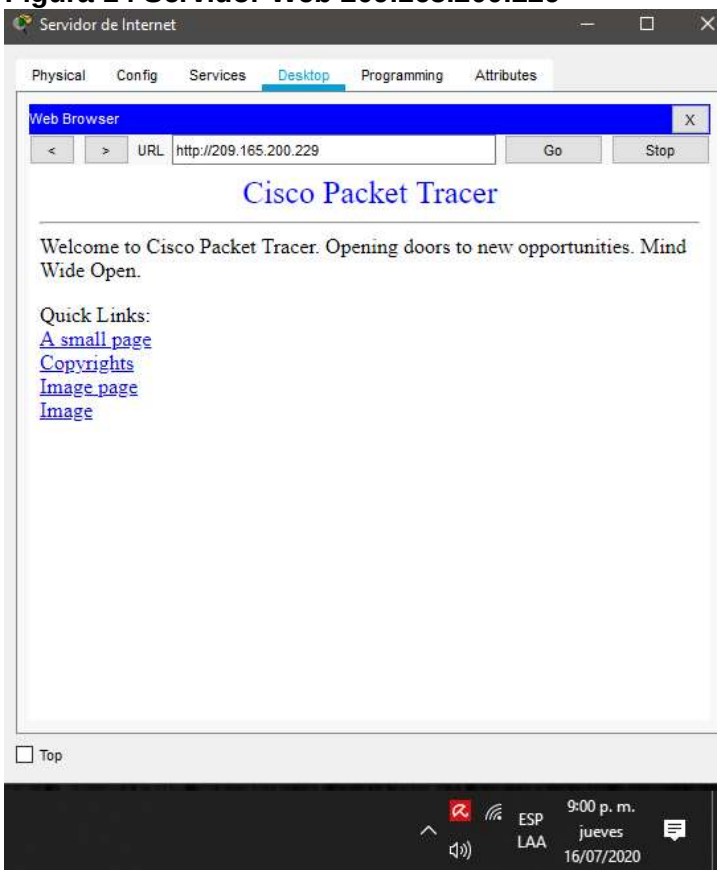
Prueba. *Verificar que la PC-A pueda hacer ping a la PC- C Nota: Quizá sea necesario deshabilitar el firewall de la PC.*

Figura 13 Conectividad entre PC-A y PC-C



- **Prueba**. Utilizar un navegador web en la computadora de Internet para acceder al servidor web (c) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Figura 14 Servidor Web 209.165.200.229



Parte 6: Configurar NTP

Se procede a realizar configuraciones NTP en R2 y R1, empezando con la configuración de relojes entre dispositivos,maestro NTP en R2 para que sea uncliente en R2 y en R1 configuración como un cliente NTP, actualizaciones de calendario periódicas y verificación de la configuración NTP.

Tabla 19 Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 mar 2016 R2#show clock 9:0:12.939 UTC Sat Mar 5 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1# show ntp associations

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

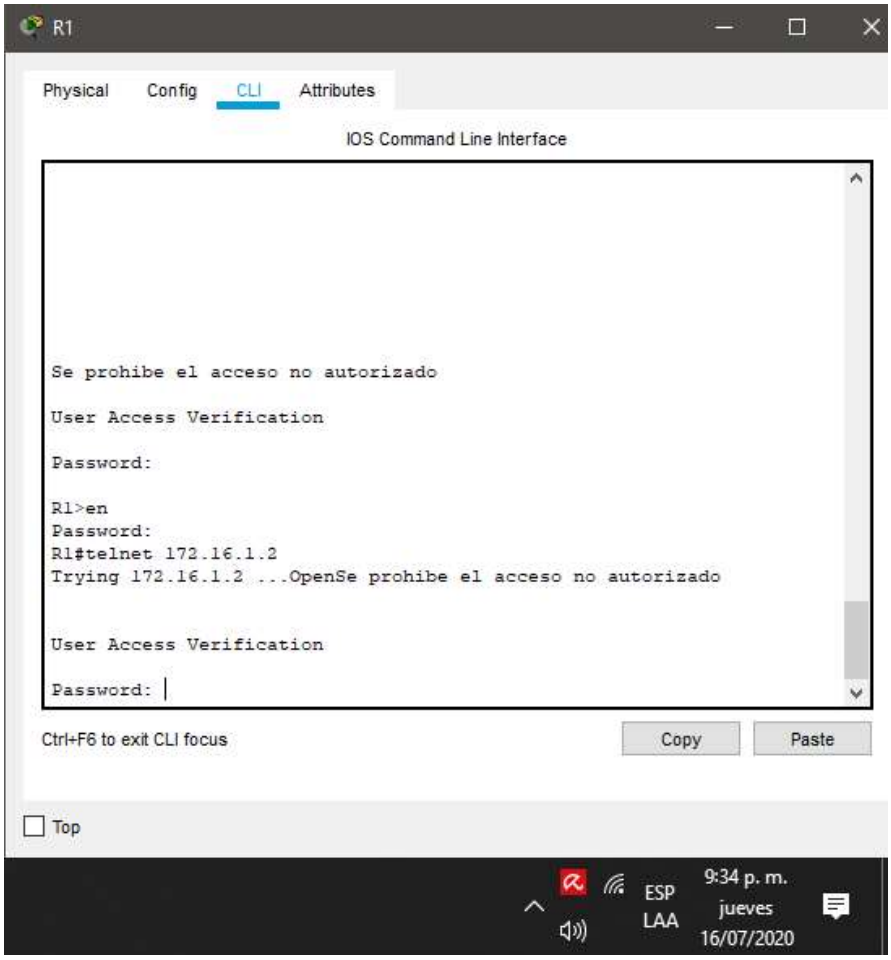
Paso 1: Restringir el acceso a las líneas VTY en el R2

Se procede a realizar las configuraciones de ACL en R2, empezando por configurar una lista de acceso para permitir que solo R1 establezca conexión telnet con R2, aplicar a las líneas vty, permitir accesos por telnet hasta la verificación de las mismas. Todo lo anterior permitirá que el host acceda remotamente a exec privilegiado en R1.

Tabla 20 Configuración ACL

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	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
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	R2# telnet 172.16.1.2

Figura 15 Verificación ACL



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

Se procede a realizar la visualización de las coincidencias recibidas por una lista de acceso con los comandos show access-lists, luego restablecemos los contadores de una lista de acceso y luego terminamos con la utilización de los comandos que sirven para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica, para mostrar traducciones NAT, y el comando que se utiliza para eliminar las traducciones de NAT dinámicas.

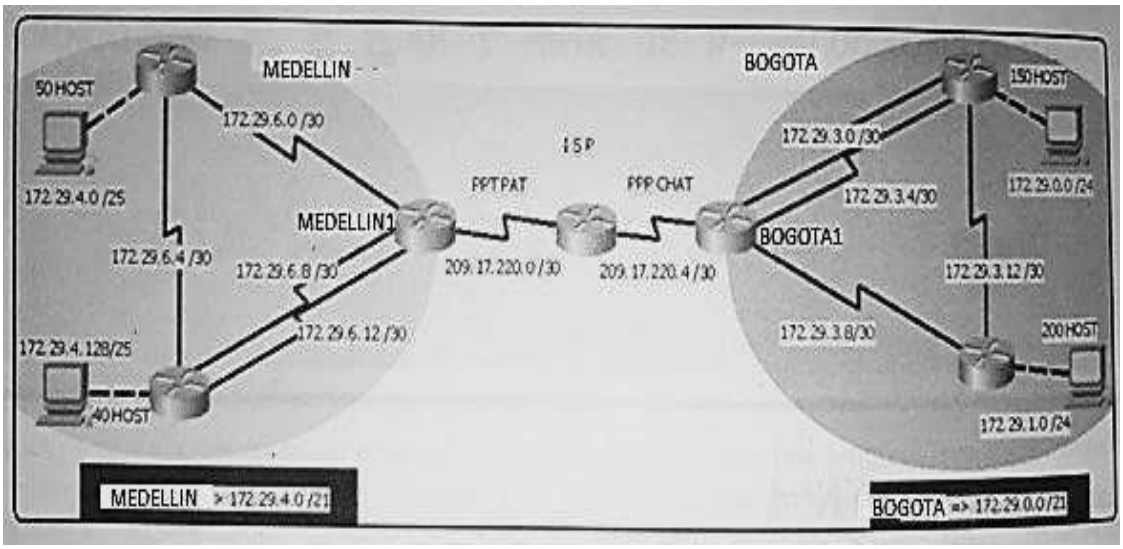
Tabla 21 Visualización de Access list

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2(config)#int s0/0/0 R2(config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

DESARROLLO 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.

***Figura 16 Topología escenario** 2*



Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán 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)

Diagnostico ISP

Se procede a realizar la configuración básica del router ISP, el cual conectará los router principales de Medellín y Bogotá, comenzando por el cambio de nombre, contraseñas de acceso y mensajes de bienvenida.

Tabla 22 Diagnostico ISP

Descripción del comando	Entrada del estudiante (comando)
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).	Router(config)#hostname ISP ISP(config)#no ip domain-lookup ISP(config)#enable secret class ISP(config)#line console 0 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#exit ISP(config)#line vty 0 15 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#exit ISP(config)#service password-encrytion ISP(config)#banner motd #Prohibido el acceso no autorizado#

Router BOGOTA

Debido a que los router no tienen configuración alguna, se procede a realizar la configuración básica de los routers del lado de Bogotá, se configura nombre de equipo, contraseñas, y motd.

Tabla 23 Configuración inicial Routers Bogota

Dispositivo	Configuración
BOGOTA1	Router(config)#hostname BOGOTA1 BOGOTA1(config)#no ip domain-lookup BOGOTA1(config)#enable secret class BOGOTA1(config)#line console 0 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#exit BOGOTA1(config)#line vty 0 15 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#exit BOGOTA1(config)#service password-encrytion BOGOTA1(config)#banner motd #Prohibido el acceso no autorizado#
BOGOTA2	Router(config)#hostname BOGOTA2 BOGOTA2(config)#no ip domain-lookup BOGOTA2(config)#enable secret class BOGOTA2(config)#line console 0 BOGOTA2(config-line)#password cisco BOGOTA2(config-line)#login BOGOTA2(config-line)#exit BOGOTA2(config)#line vty 0 15 BOGOTA2(config-line)#password cisco BOGOTA2(config-line)#login BOGOTA2(config-line)#exit BOGOTA2(config)#service password-encrytion BOGOTA2(config)#banner motd #Prohibido el acceso no autorizado#

BOGOTA3	Router(config)#hostname BOGOTA3 BOGOTA3(config)#no ip domain-lookup BOGOTA3(config)#enable secret class BOGOTA3(config)#line console 0 BOGOTA3(config-line)#password cisco BOGOTA3(config-line)#login BOGOTA3(config-line)#exit BOGOTA3(config)#line vty 0 15 BOGOTA3(config-line)#password cisco BOGOTA3(config-line)#login BOGOTA3(config-line)#exit BOGOTA3(config)#service password-encrytion BOGOTA3(config)#banner motd #Prohibido el acceso no autorizado# #

Routers Medellín

Debido a que los router no tienen configuración alguna, Se realiza configuración básica de los routers del lado de Medellín, se configura nombre de equipo, contraseñas, y motd.

Tabla 24 Configuración inicial Routers Medellin

Dispositivo	Configuración
MEDELLIN1	Router(config)#hostname MEDELLIN1 MEDELLIN1(config)#no ip domain-lookup MEDELLIN1(config)#enable secret class MEDELLIN1(config)#line console 0 MEDELLIN1(config-line)#password cisco MEDELLIN1(config-line)#login MEDELLIN1(config-line)#exit MEDELLIN1(config)#line vty 0 15 MEDELLIN1(config-line)#password cisco MEDELLIN1(config-line)#login MEDELLIN1(config-line)#exit MEDELLIN1(config)#service password-encrytion MEDELLIN1(config)#banner motd #Prohibido el acceso no autorizado#

MEDELLIN2	Router(config)#hostname MEDELLIN2 MEDELLIN2(config)#no ip domain-lookup MEDELLIN2(config)#enable secret class MEDELLIN2(config)#line console 0 MEDELLIN2(config- line)#password cisco MEDELLIN2(config- line)#login MEDELLIN2(config- line)#exit MEDELLIN2(config)#line vty 0 15 MEDELLIN2(config- line)#password cisco MEDELLIN2(config- line)#login MEDELLIN2(config-line)#exit MEDELLIN2(config)#serv ice pass MEDELLIN2(config)#serv ice password-encryption MEDELLIN2(config)#banner motd #prohibido el acceso no autorizado#
MEDELLIN3	Router(config)#hostname MEDELLIN3 MEDELLIN3(config)#no ip domain-lookup MEDELLIN3(config)#enable secret class MEDELLIN3(config)#line console 0 MEDELLIN3(config- line)#password cisco MEDELLIN3(config- line)#login MEDELLIN3(config- line)#exit MEDELLIN3(config)#line vty 0 15 MEDELLIN3(config- line)#password cisco MEDELLIN3(config- line)#login MEDELLIN3(config-line)#exit MEDELLIN3(config)#service pass MEDELLIN3(config)#service password-encryption MEDELLIN3(config)#banner motd #prohibido el acceso no autorizado.#

• Realizar la conexión física de los equipos con base en la topología de red

Se procede a realizar las conexiones de ip con su descripción y clock rate a cada interfaz de los router. Todo lo anterior se realiza para que calcule la ruta más corta entre dos nodos, por lo tanto, enrutara los puertos s0/1/1 y s0/1/0.

Tabla 25 Conexión Física Dispositivos

Dispositivo	Configuraciones
Router ISP	ISP(config)#int s0/0/0 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#description conexion ISP a MEDELLIN1 ISP(config-if)#clock rate 128000 ISP(config-if)#no shut ISP(config-if)#int s0/0/1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#description conexion ISP a BOGOTA1 ISP(config-if)#clock rate 128000 ISP(config-if)#no shut

BOGOTA1	BOGOTA1(config)#int s0/0/0 BOGOTA1(config-if)#description BOGOTA1 a ISP BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#no shut BOGOTA1(config-if)#int s0/1/1 BOGOTA1(config-if)#description conexion BOGOTA1 a BOGOTA3 BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shut BOGOTA1(config-if)#int s0/0/1 BOGOTA1(config-if)#description conexion Bogota1.0 a Bogota2.0 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shut BOGOTA1(config-if)#int s0/1/0 BOGOTA1(config-if)#description conexion Bogota1.1 a Bogota2.1 BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shut
BOGOTA2	BOGOTA2(config)#int s0/0/0 BOGOTA2(config-if)#description conexion Bogota2.0 a Bogota1.0 BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA2(config-if)#no shut BOGOTA2(config-if)#int s0/1/1 BOGOTA2(config-if)#description conexion Bogota2.1 a Bogota 1.1 BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA2(config-if)#no shut BOGOTA2(config-if)#int s0/0/1 BOGOTA2(config-if)#description conexion Bogota2 a Bogota3 BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252 BOGOTA2(config-if)#clock rate 128000 BOGOTA2(config-if)#no shut BOGOTA2(config-if)#int g0/0 BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0 BOGOTA2(config-if)#no shut

BOGOTA3	BOGOTA3(config)#int s0/0/0 BOGOTA3(config-if)#description conexion Bogota3 A Bogota1 BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252 BOGOTA3(config-if)#no shut BOGOTA3(config-if)#int s0/0/1 BOGOTA3(config-if)#description conexion Bogota3 a Bogota2 BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA3(config-if)#no shut BOGOTA3(config-if)#intg0/0 BOGOTA3(config-if)#ip address 172.29.1.1255.255.255.0 BOGOTA3(config-if)#no shut
MEDELLIN1	MEDELLIN1(config)#int s0/0/0 MEDELLIN1(config-if)#description MEDLLIN1 a ISP MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252 MEDELLIN1(config-if)#no shut MEDELLIN1(config-if)#int s0/1/0 MEDELLIN1(config-if)#description MEDELLIN1 a MEDELLIN2 MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shut MEDELLIN1(config-if)#int s0/1/1 MEDELLIN1(config-if)#description MEDELLIN1.1 a MEDELLIN3.1 MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shut MEDELLIN1(config-if)#int s0/0/1 MEDELLIN1(config-if)#description MEDELLIN1.2 a MEDELLIN3.2 MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shut

MEDELLIN 2	MEDELLIN2(config)#int s0/0/0 MEDELLIN2(config-if)#description MEDELLIN2 a MEDELLIN1 MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252 MEDELLIN2(config-if)#no shut MEDELLIN2(config-if)#int s0/0/1 MEDELLIN2(config-if)#description MEDELLIN2 a MEDELLIN3 MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252 MEDELLIN2(config-if)#clock rate 128000 MEDELLIN2(config-if)#no shut MEDELLIN2(config-if)#int g0/0 MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128 MEDELLIN2(config-if)#no shut
MEDELLIN3	MEDELLIN3(config)#int s0/0/0 MEDELLIN3(config-if)#description MEDELLIN3.1 a MEDELLIN1.1 MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252 MEDELLIN3(config-if)#no shut MEDELLIN3(config-if)#int s0/0/1 MEDELLIN3(config-if)#description MEDELLIN3 A MEDELIN2 MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252 MEDELLIN3(config-if)#no shut MEDELLIN3(config-if)#int s0/1/1 MEDELLIN3(config-if)#description MEDELLIN3.2 a MEDELLIN1.2 MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252 MEDELLIN3(config-if)#no shut MEDELLIN3(config-if)#int g0/0 MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128 MEDELLIN3(config-if)#no shut

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

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.

Se procede a realizar las configuraciones de enrutamiento mediante protocolo OSPF V2, utilizando sus respectivas direcciones.

Tabla 26 Enrutamiento

Dispositivos	Configuraciones
BOGOTA1	BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#router-id 4.4.4.4 BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area0 BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area0 BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area0 BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0 BOGOTA1(config-router)#end
BOGOTA2	BOGOTA2(config)#router ospf 1 BOGOTA2(config-router)#router 5.5.5.5 BOGOTA2(config-router)#network 172.29.3.0 0.0.0.3 area0 BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area0 BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0 BOGOTA2(config-router)#end
BOGOTA3	BOGOTA3(config)#router ospf 1 BOGOTA3(config-router)#router-id 6.6.6.6 BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 0 BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 0 BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA3(config-router)#end
MEDELLIN1	MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#router-id 1.1.1.1 MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area0 MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area0 MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0 MEDELLIN1(config-router)#end
MEDELLIN2	MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#router-id 2.2.2.2 MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.255 area 0 MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0 MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0 MEDELLIN2(config-router)#end
MEDELLIN3	MEDELLIN3(config)#router ospf 1 MEDELLIN3(config-router)#router-id 3.3.3.3 MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.255 area 0 MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area0 MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area0 MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN3(config-router)#end

b. Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Se procede a realizar la debida configuración de publicaciones de OSPF mediante la ip route de s0/0/0.

Tabla 27 Publicaciones de OSPF

Dispositivos	Configuraciones OSPF
MEDELLIN1	MEDELLIN1#conf t MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#default-information originate MEDELLIN1(config-router)#end
BOGOTA1	BOGOTA1#conf t BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#default-information originate BOGOTA1(config-router)#end

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.

Figura 17 Sumarización

		128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		
MEDELLİ																				
172	29	0	0	0	0	0	1	1	0		0	0	0	0	0	1	1	0		172.29.6.0/30
172	29	0	0	0	0	0	1	1	0		0	0	0	0	1	0	0	0		172.29.6.8/30
172	29	0	0	0	0	0	1	1	0		0	0	0	0	1	1	0	0		172.29.6.12/30
172	29	0	0	0	0	0	1	0	0		0	0	0	0	0	0	0	0		172.29.4.0/25
172	29	0	0	0	0	0	1	0	0		1	0	0	0	0	0	0	0		
172	29	0	0	0	0	0	1	0	0			172.29.4.128/25								
BOGOT A																				
172																				
172	29	0	0	0	0	0	0	1	1		0	0	0	0	1	0	0	0		172.29.3.8/30
172	29	0	0	0	0	0	0	1	1		0	0	0	0	0	0	0	0		172.29.3.0/30
172	29	0	0	0	0	0	0	1	1		0	0	0	0	0	1	0	0		172.29.3.4/30
172	29	0	0	0	0	0	0	1	1		0	0	0	0	1	1	0	0		
172	29	0	0	0	0	0	0	0	1		1	0	0	0	0	0	0	0		172.29.1.0/24
172	29	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0		172.29.0.0/24

Se procede a realizar la debida configuración del router ISP, incluyendo una ruta estática dirigida hacia cada red interna de Bogotá y Medellín.

Tabla 28 Configuración ruta estática ISP

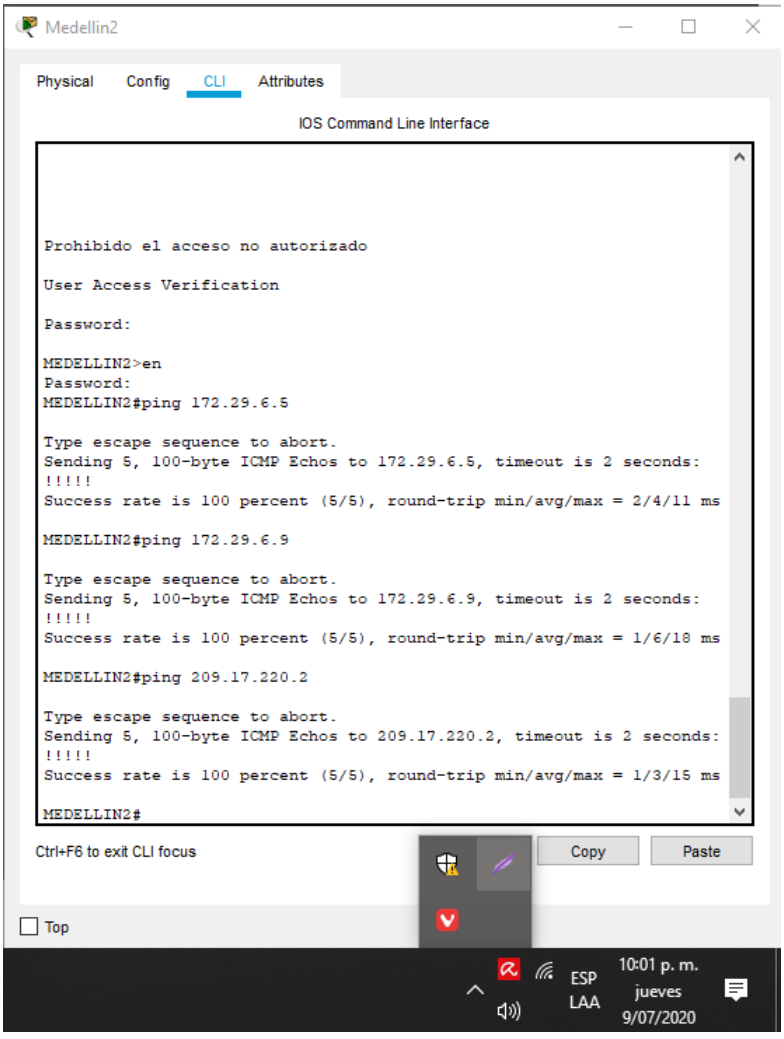
Dispositivos	Configuraciones
ISP	ISP#conf t ISP(config)#ip route 172.29.4.0 255.255.255.0209.17.220.2 ISP(config)#ip route 172.29.0.0 255.255.255.0209.17.220.6

Parte 2: Tabla de Enrutamiento.

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

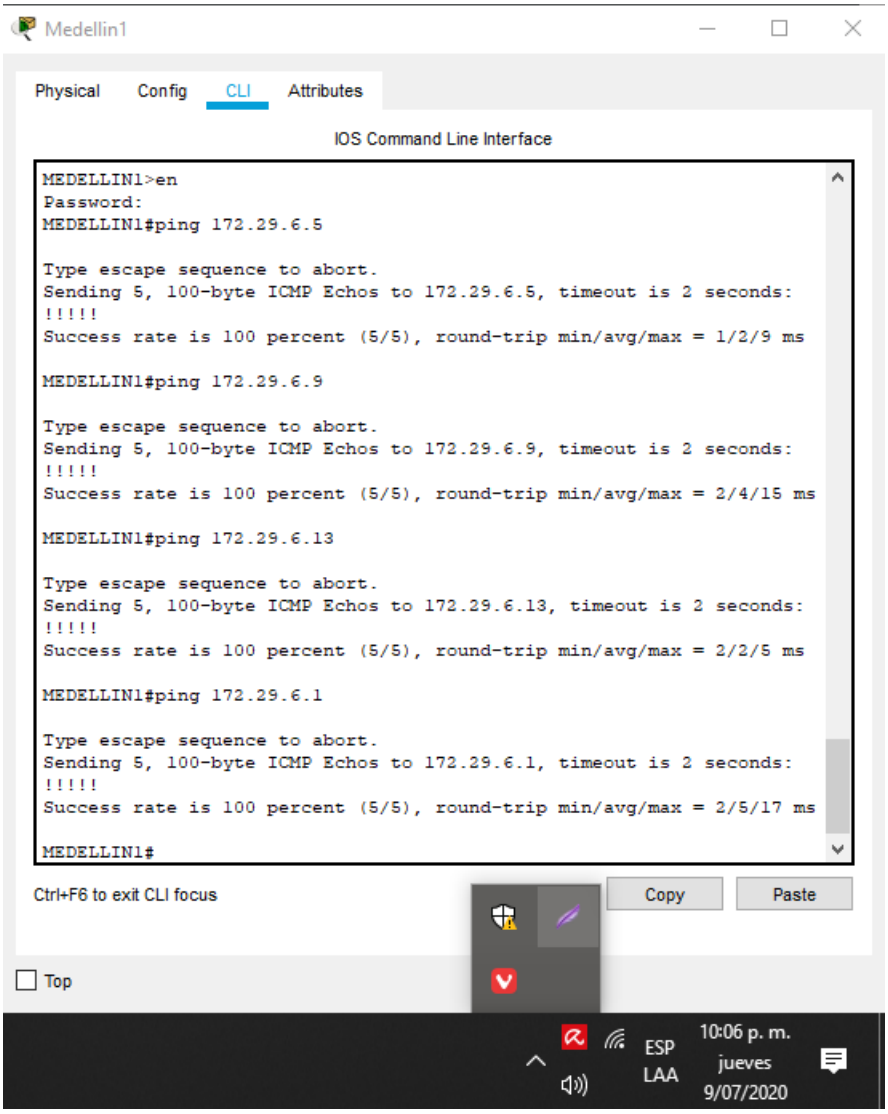
Se hace verificación mediante ping desde Medellin2 a la ip de Medellin1, Medellin3, IPS, dando exitosa la conexión.

Figura 18 Verificación Dispositivos Medellin2



Se realiza la verificación con ping con la ip de la subred Medellin1 hacia la ip de Medellin2, Medellin3 con satisfacción.

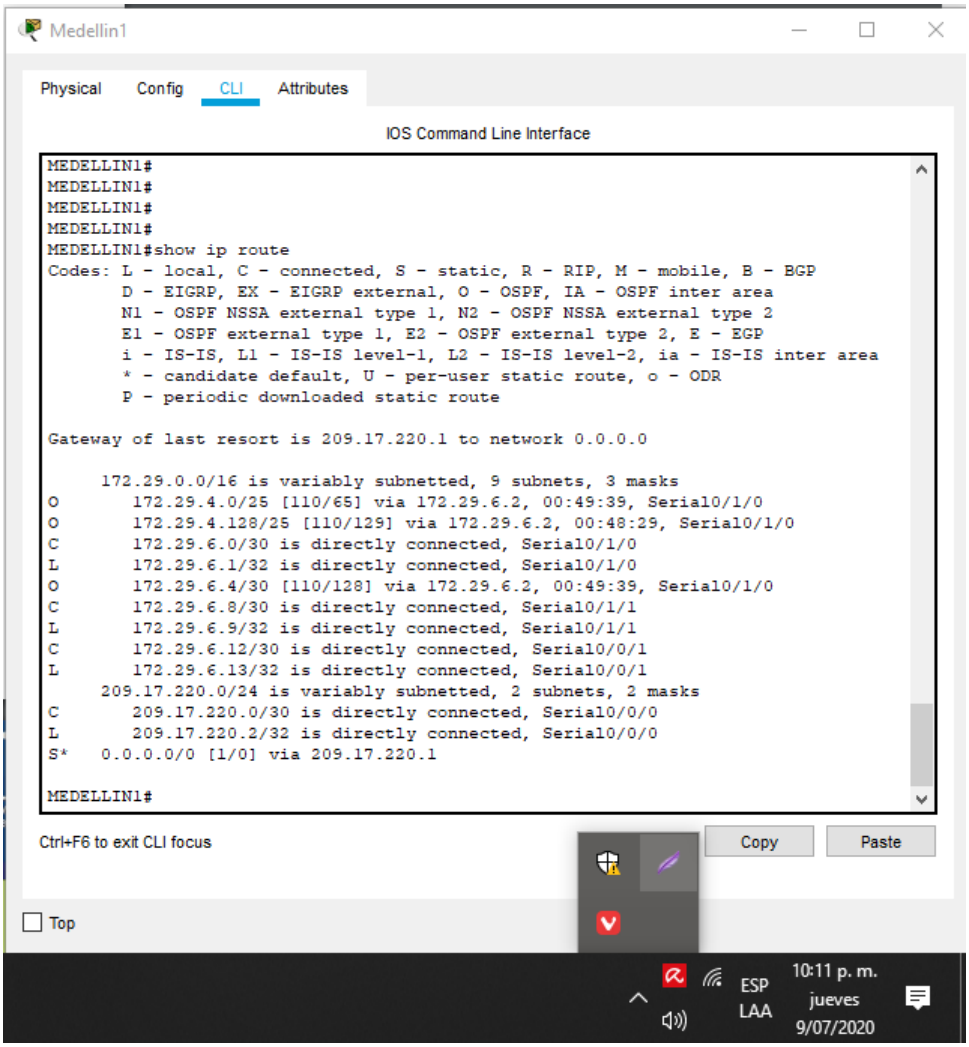
Figura 19 Verificación Dispositivos Medellin1



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

En el router MEDELIN1 hay Balanceo de cargue debido a que el router recibe varias trayectorias con el mismo costo y la misma distancia administrativa del destino.

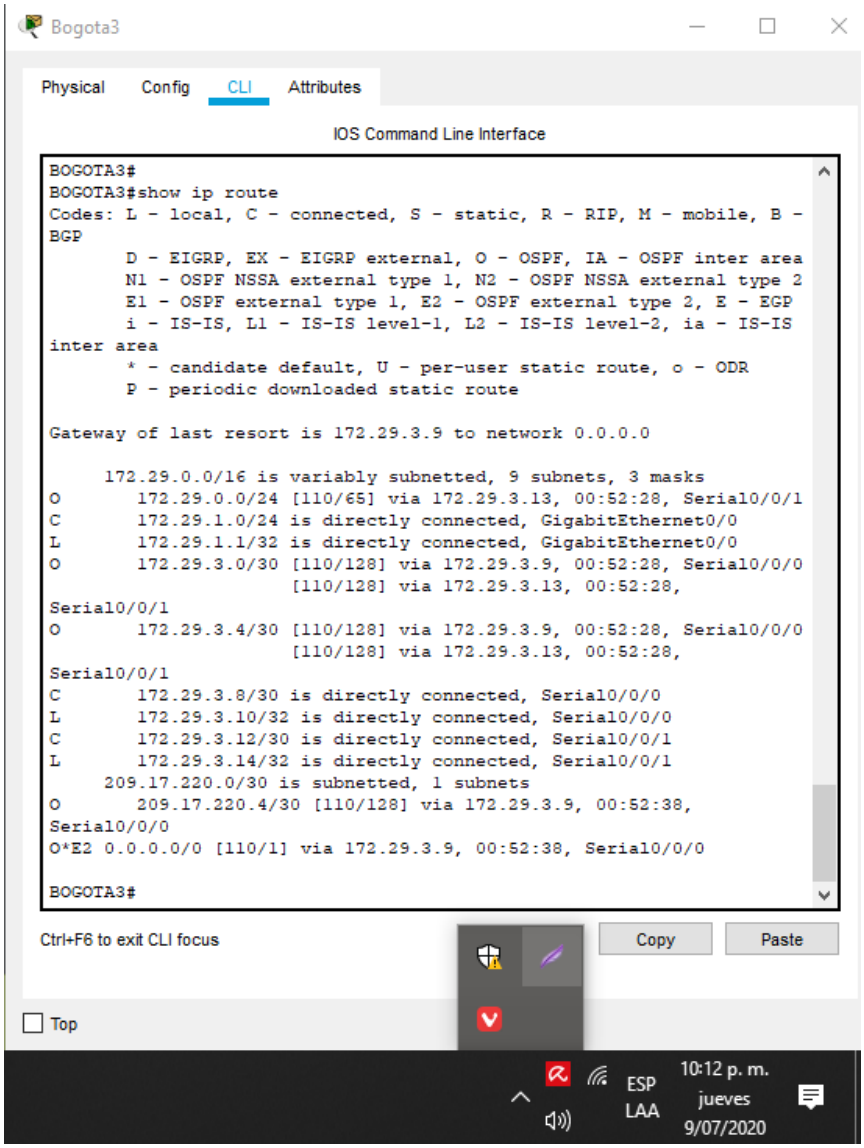
Figura 20 Verificación Balanceo Medellin1



Balanceo Bogota3

hay un balanceo de cargue en el router Bogota3 debido a que recibe varias trayectorias con el mismo costo y la misma distancia administrativa del destino.

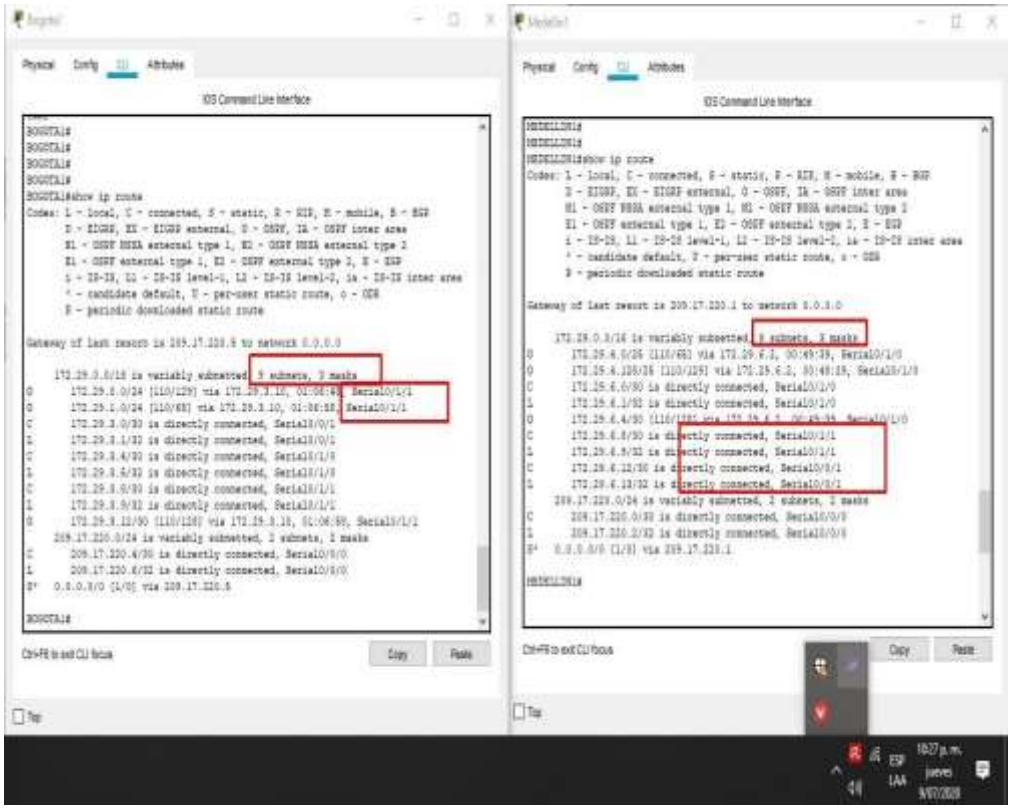
Figura 21 Verificación Balanceo Bogota3



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.

Los router Bogota1 y Medellin1 tienen similitud en sus rutas de redes.

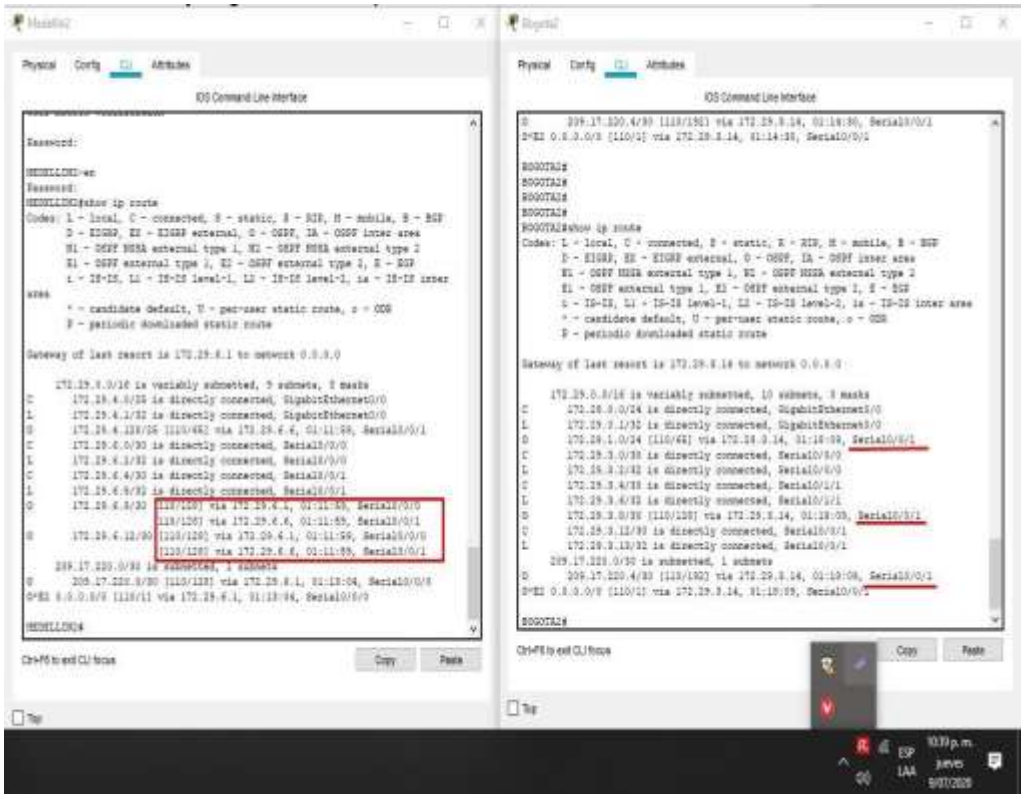
Figura 22 Similitud Routers



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

Se presentan redes conectadas y recibidas mediante OSPF.

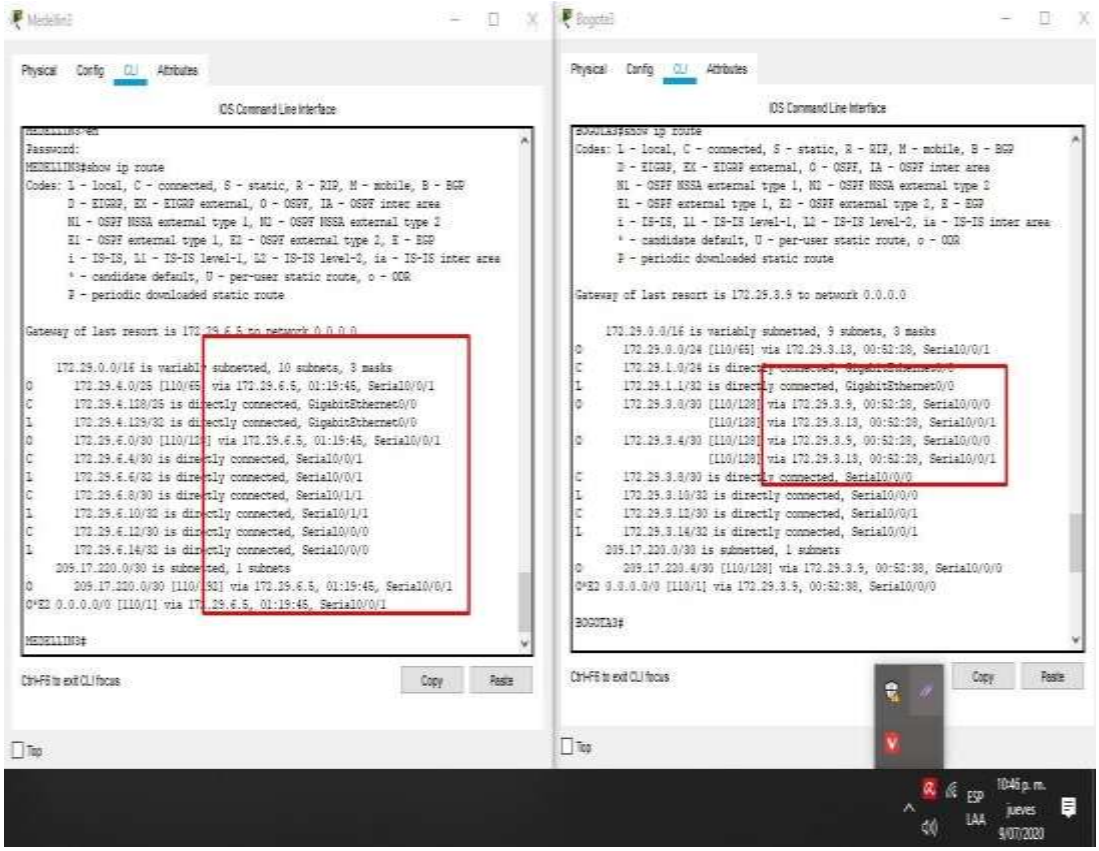
Figura 23 Show ip route Medellin2 y Bogota2



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

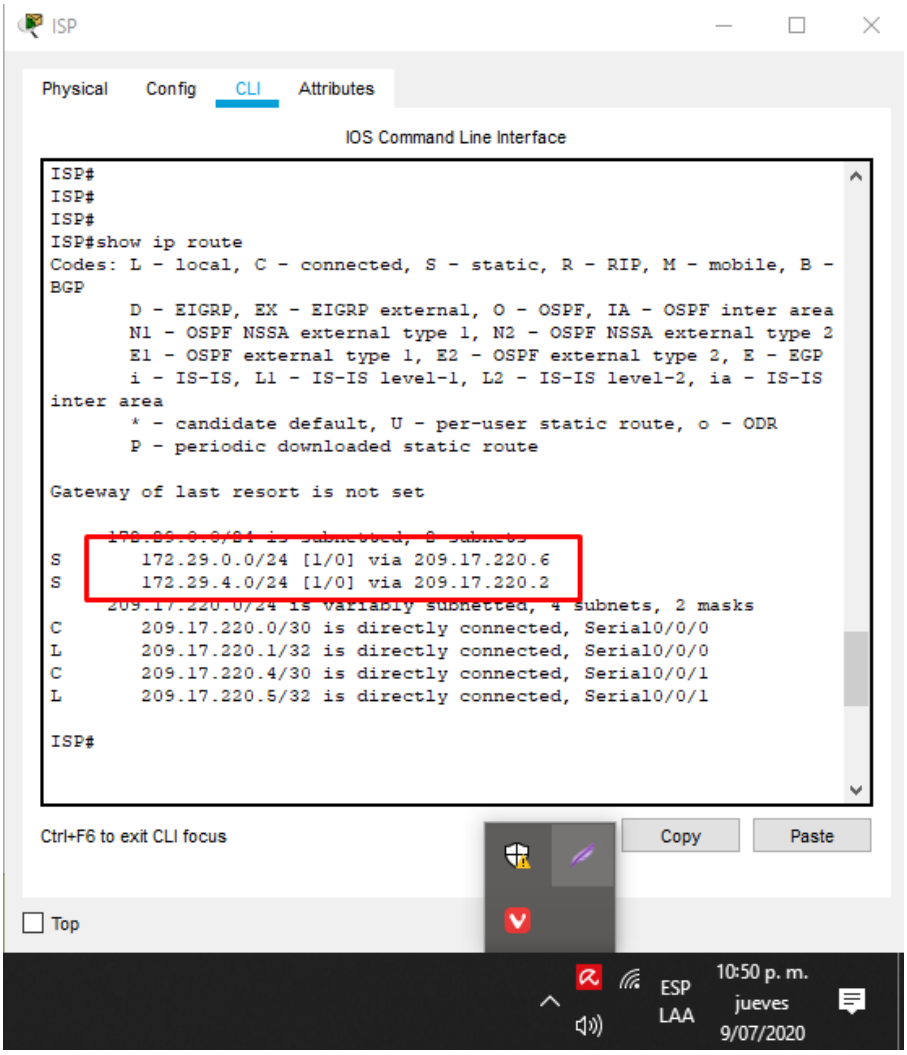
Las 3 rutas de la red el cual una de ellas es la redundante el cual es la clave para mantener la red confiable.

Figura 24 Show rutas redundantes



f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas. Se observa la ip de destino y la ip donde tiene que ser enviado.

Figura 25 Show ISP



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.

Se procede a deshabilitar la propagación del protocolo OSPF, en los router Bogota2, Bogota3, Medellin2, Medellin3, en los otros router no es necesario según las indicaciones dadas en la guía.

Tabla 29 Propagación de OSPF

ROUTER	CONFIGURACIONES
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	BOGOTA2#conf t BOGOTA2(config)#router ospf 1 BOGOTA2(config-router)#passive-interface g0/0 BOGOTA2(config-router)#end BOGOTA2#wr
Bogota3	BOGOTA3#conf t BOGOTA3(config)#router ospf 1 BOGOTA3(config-router)#passive-interface g0/0 BOGOTA3(config-router)#end BOGOTA3#wr
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	MEDELLIN2#conf t MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#passive-interface g0/0 MEDELLIN2(config-router)#end MEDELLIN2#wr
Medellín3	MEDELLIN3#conf t MEDELLIN3(config)#router ospf 1 MEDELLIN3(config-router)#passive-interface g0/0 MEDELLIN3(config-router)#end MEDELLIN3#wr
ISP	No lo requiere

Parte 4: Verificación del protocolo OSPF.

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

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

Desarrollo a y b.

Figura 26 Verificación OSPF Medellin1

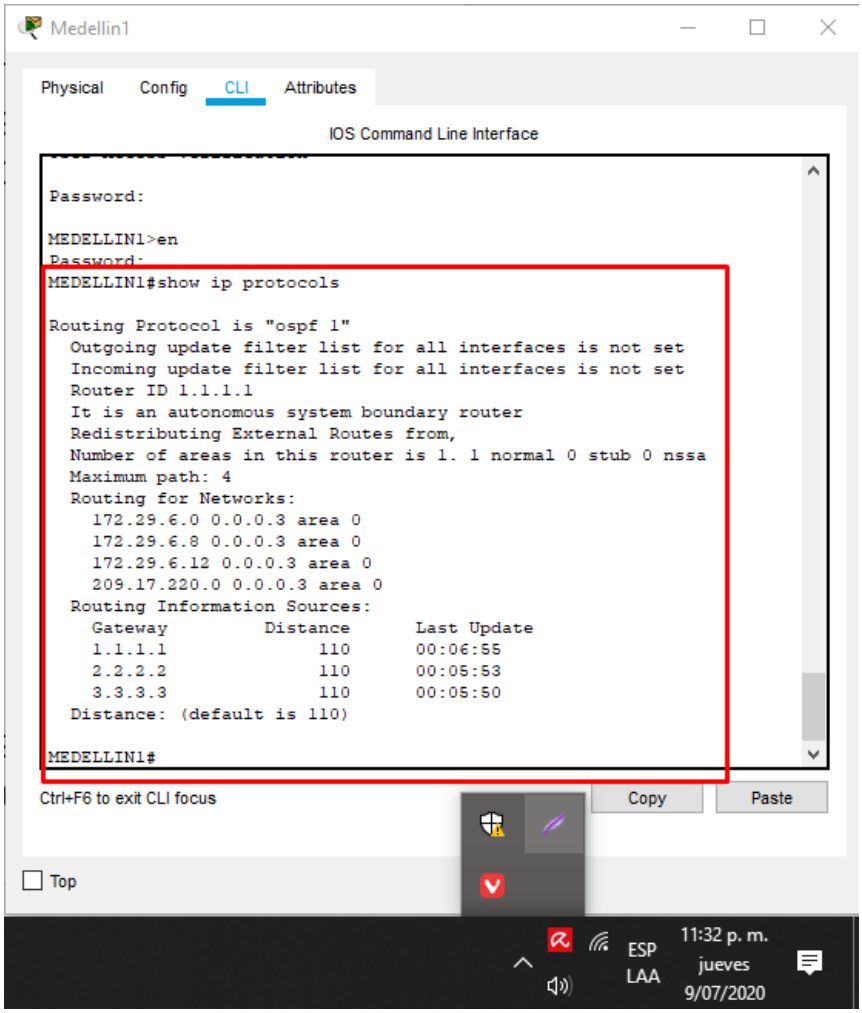


Figura 27 Verificación OSPF Medellin2

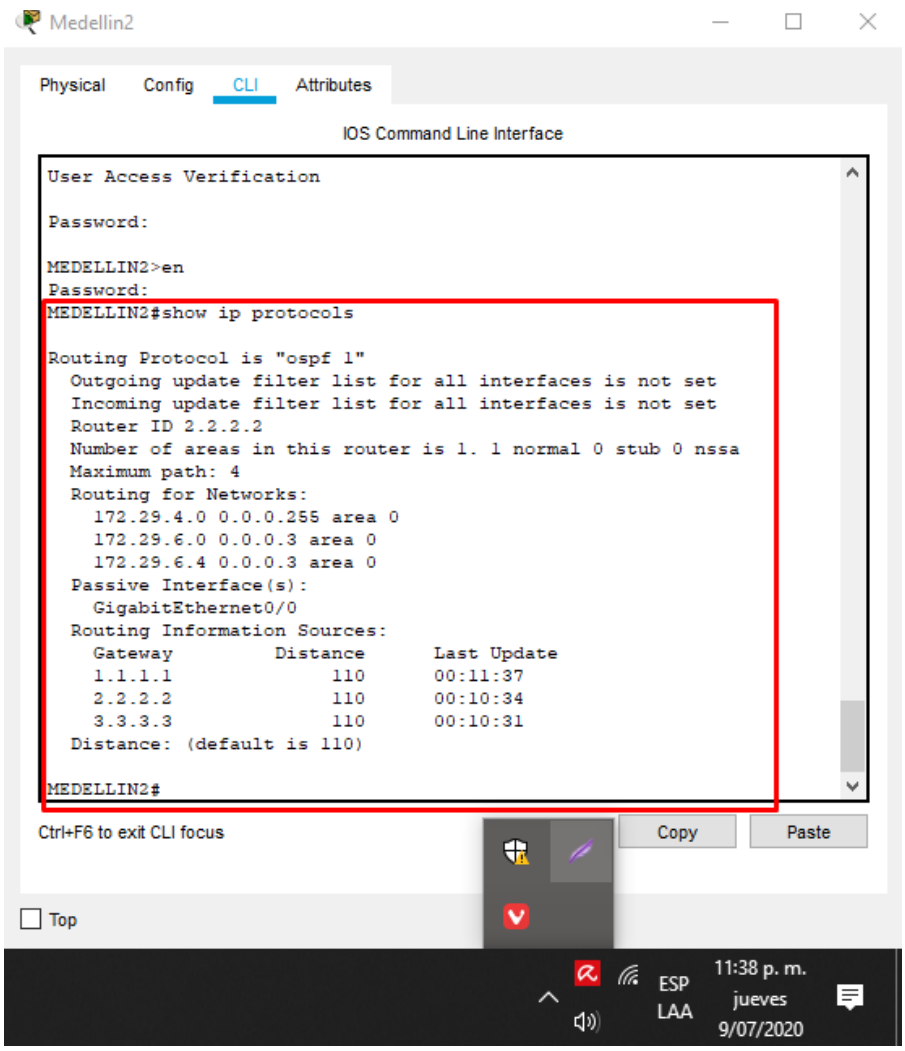


Figura 28 Verificación OSPF Medellin3

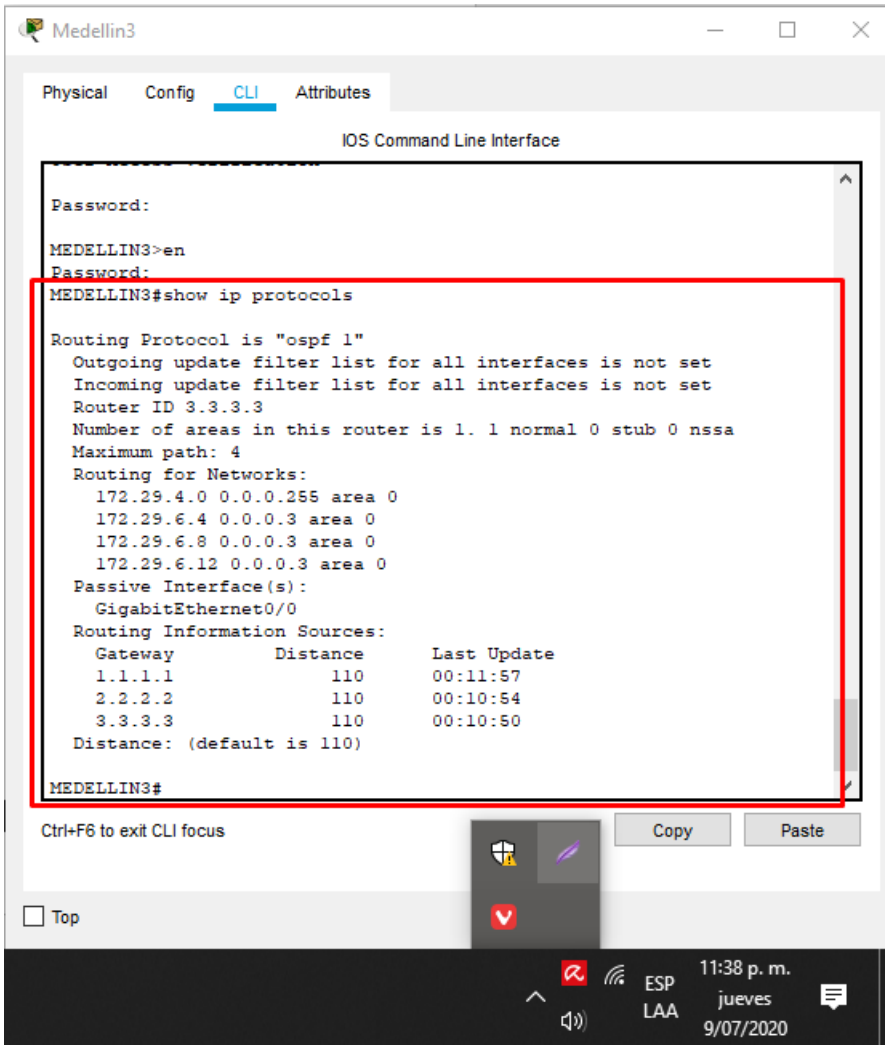


Figura 29 Verificación OSPF Bogota1

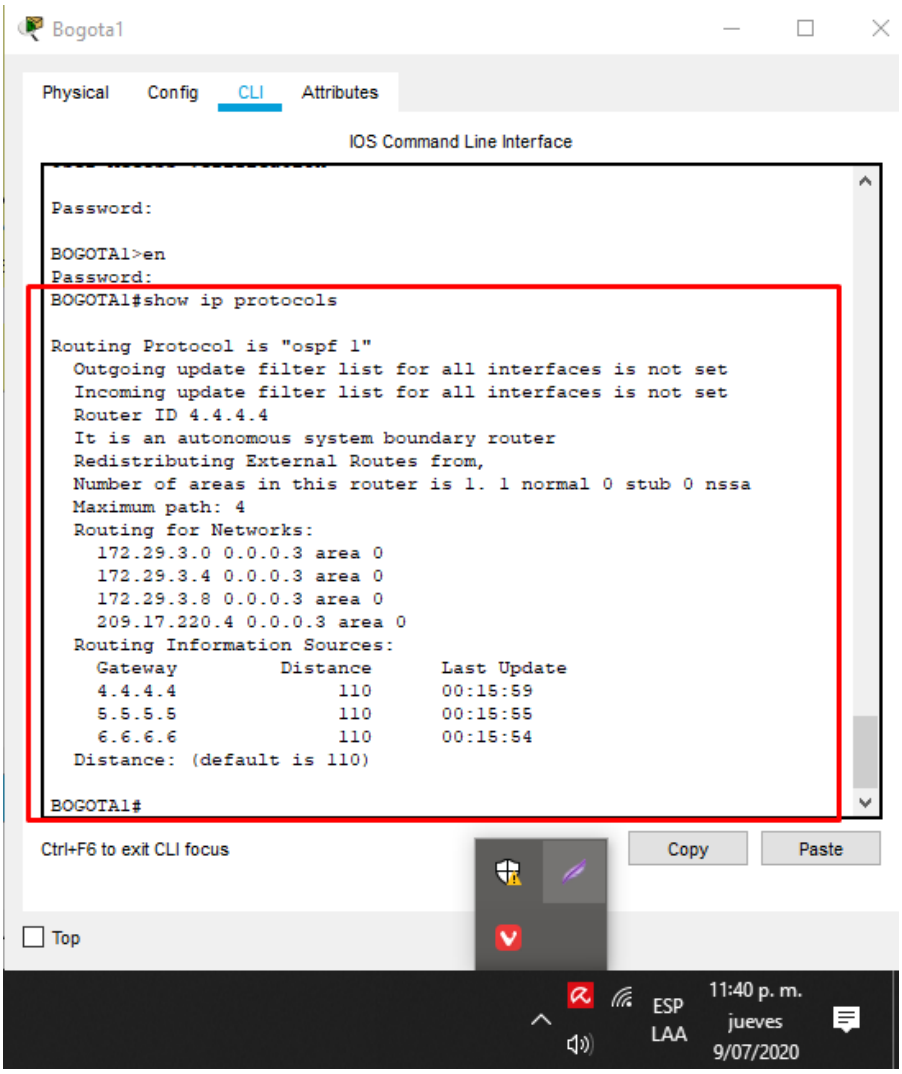


Figura 30 Verificación OSPF Bogota2

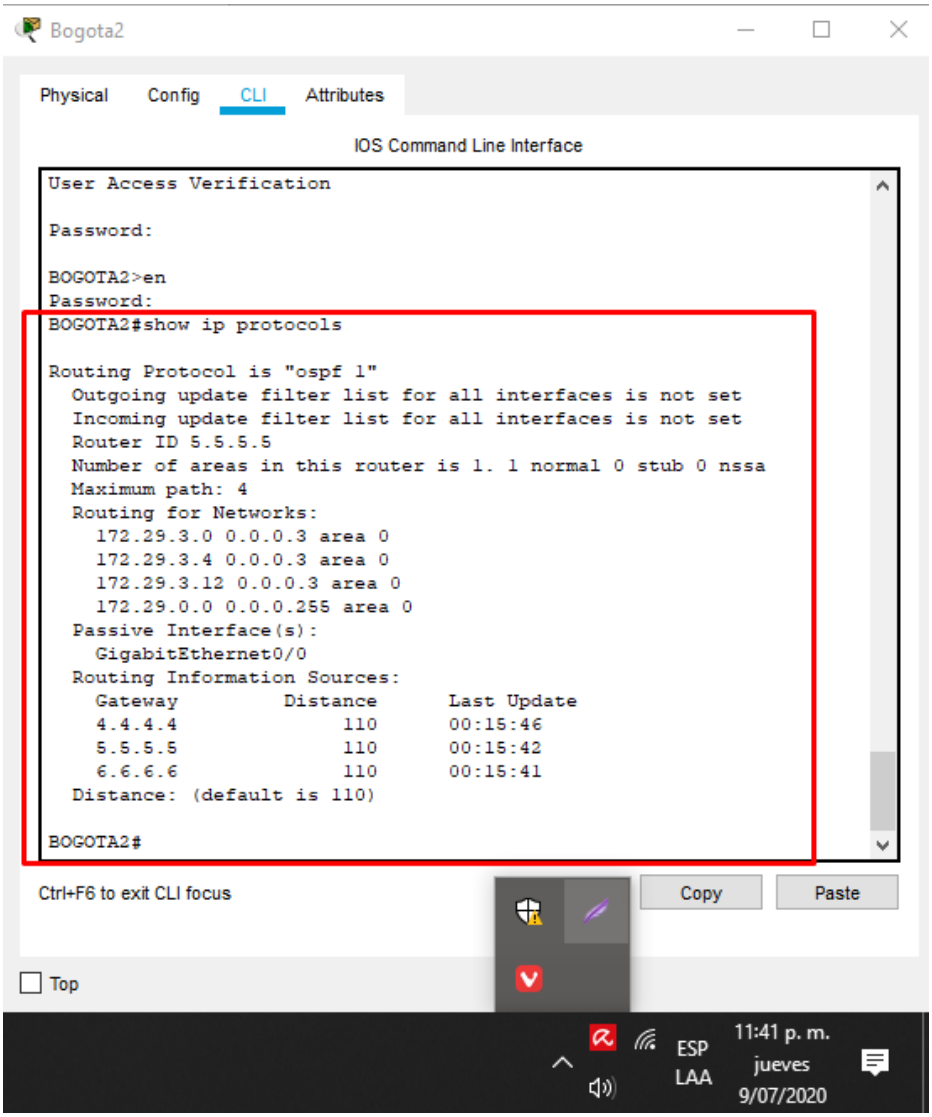
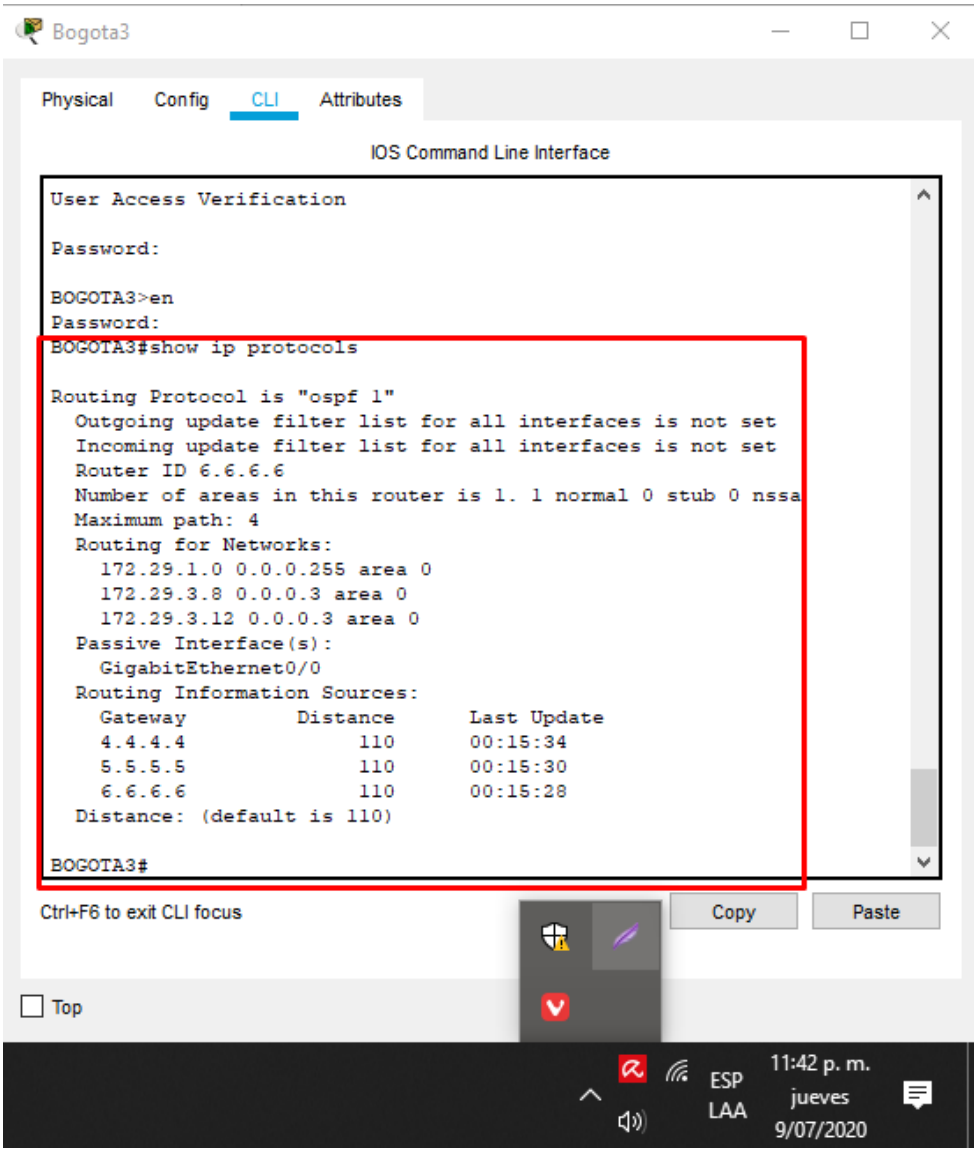


Figura 31 Verificación OSPF Bogota3



Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Se procede a realizar configuraciones ISP con autenticación PAT en los roter ISP Ymedellin1.

Tabla 30 Autenticación PAT

DISPOSITIVO	CONFIGURACIONES
ISP	ISP#conf t ISP(config)#username MEDELLIN1 password cisco ISP(config)#int s0/0/0 ISP(config-if)#encapsulation PPP ISP(config-if)#PPP authentication PAP ISP(config-if)#PPP PAP sent-username ISP password cisco ISP(config-if)#end
MEDELLIN1	MEDELLIN1#conf t MEDELLIN1(config)#username ISP password cisco MEDELLIN1(config)#int s0/0/0 MEDELLIN1(config-if)#encapsulation PPP MEDELLIN1(config-if)#PPP authentication PAP MEDELLIN1(config-if)#PPP PAP sent-username MEDELLIN1 password cisco MEDELLIN1(config-if)#exit

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

Se procede a realizar configuraciones en ISP y BOGOTA1 en las interfaces con autenticación chap.

Tabla 31 Autenticación Chap

DISPOSITIVO	CONFIGURACIONES
ISP	ISP#conf t ISP(config)#username BOGOTA1 password cisco ISP(config)#int s0/0/1 ISP(config-if)#encapsulation PPP ISP(config-if)#PPP authentication chap
BOGOTA1	BOGOTA1#conf t BOGOTA1(config)#username ISP password cisco BOGOTA1(config)#int s0/0/0 BOGOTA1(config-if)#encapsulation PPP BOGOTA1(config-if)#PPP authentication chap

Parte 6: Configuración de PAT.

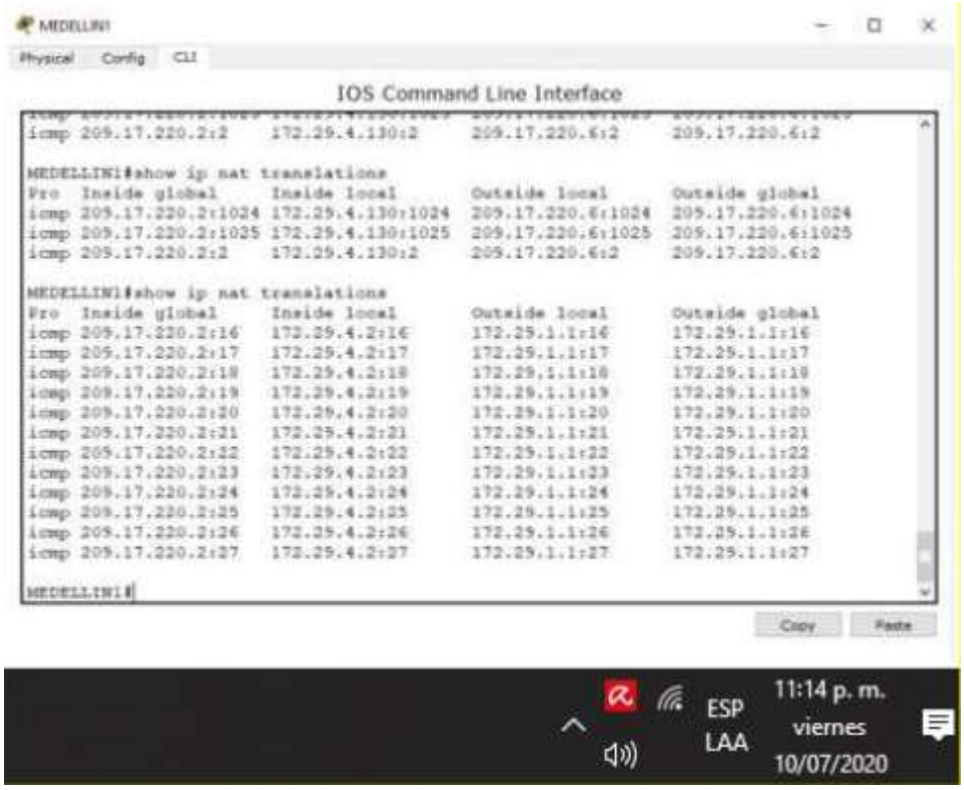
a En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

Tabla 32 Configuración PAT

DISPOSITIVO	CONFIGURACIONES
MEDELLIN1	MEDELLIN1(config)#ip access-list standard LAN-MEDELLIN MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.3.255 MEDELLIN1(config-std-nacl)#exit MEDELLIN1(config)#ip nat inside source list LAN-MEDELLIN interface s0/0/0 overload MEDELLIN1(config)#int s0/0/0 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#exit MEDELLIN1(config)#int s0/0/1 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#exit MEDELLIN1(config)#int s0/1/0 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#exit MEDELLIN1(config)#int s0/1/1 MEDELLIN1(config-if)#ip nat inside
BOGOTA1	BOGOTA1(config)#ip access-list standard LAN-BOGOTA BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.3.255 BOGOTA1(config-std-nacl)#exit BOGOTA1(config)#ip nat inside source list LAN-BOGOTA interface s0/0/0 overload BOGOTA1(config)#int s0/0/0 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#exit BOGOTA1(config)#int s0/0/1 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#exit BOGOTA1(config)#int s0/1/0 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)#end

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.

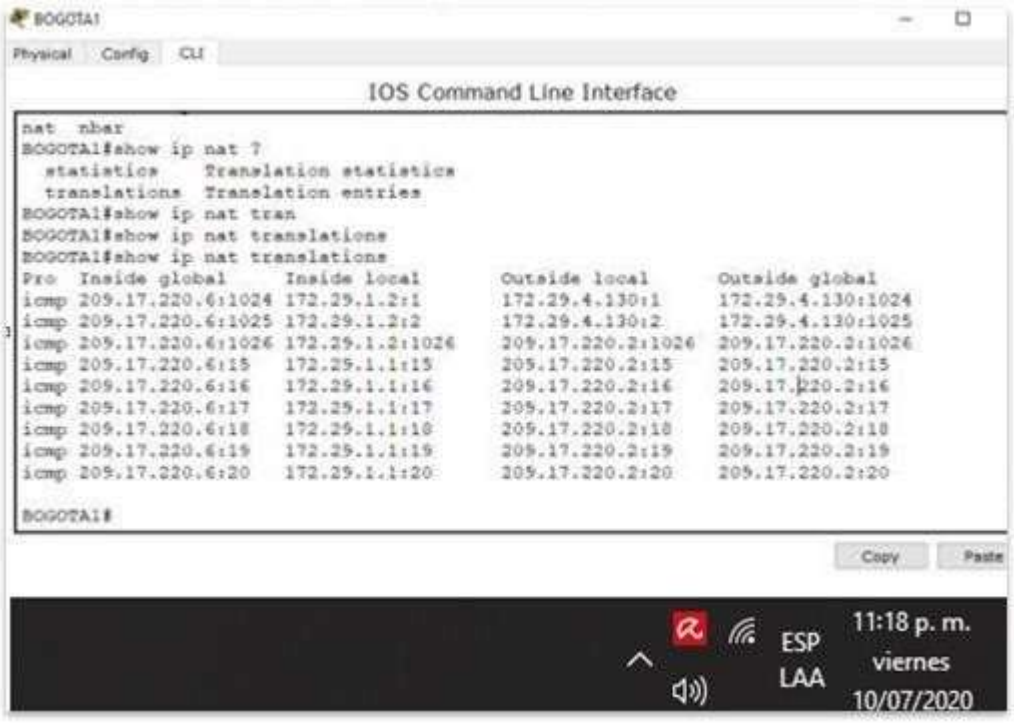
Figura 32 Traducción de direcciones en Router Medellin1



c. Proceda a configurar el NAT en el router Bogotá1.

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

Figura 33 Traducción de direcciones en Router Bogota1



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.

Se realizan configuraciones DHCP en MEDELLIN2 para que sea servidor en ambas redes lan.

Tabla 33 Configuración del servicio DHCP MEDELLIN2

DISPOSITIVO	CONFIGURACIONES
MEDELLIN2	MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.9 MEDELLIN2(config)#ip dhcp pool MEDELLIN-LAN1 MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.1 MEDELLIN2(dhcp-config)#domain-name lan1.medellin.com MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.136 MEDELLIN2(config)#ip dhcp pool MEDELLIN-LAN2 MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.129 MEDELLIN2(dhcp-config)#domain-name lan2.medellin.com MEDELLIN2(dhcp-config)#exit

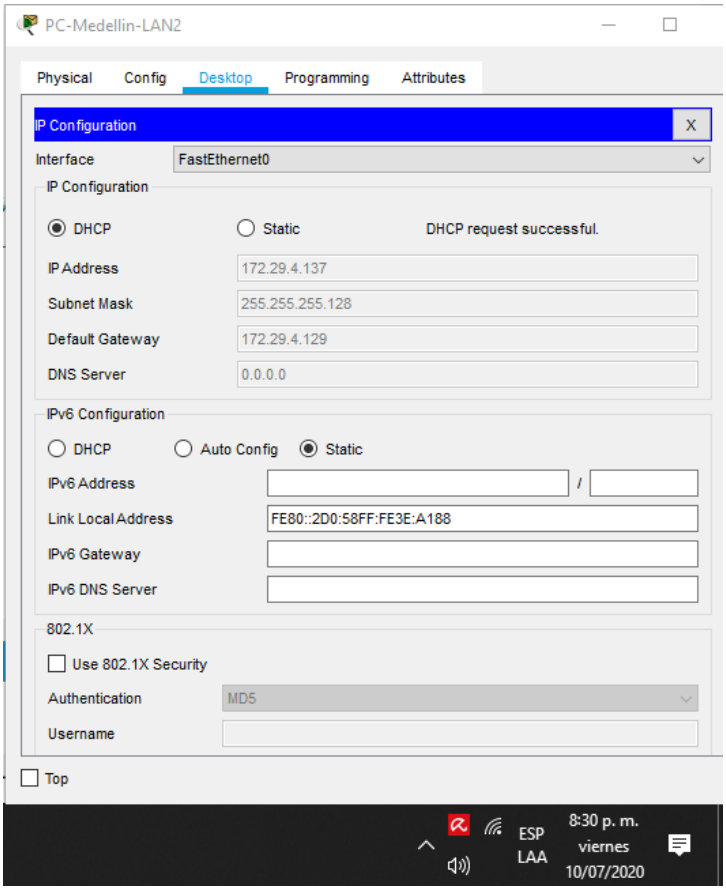
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

Se procede a realizar configuraciones en medellin3 para que habilite el paso de los mensajes.

Tabla 34 Habilitar Paso Medellin3

DISPOSITIVO	CONFIGURACIONES
MEDELLIN3	MEDELLIN3(config)#int g0/0 MEDELLIN3(config-if)#ip helper-address 172.29.6.5 MEDELLIN3(config-if)#exit MEDELLIN3(config)#

Figura 34 Configuración DHCP MEDELLIN



a. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes Lan.

Se realizan configuraciones DHCP en BOGOTA2 para que sea servidor en ambas redes lan.

Tabla 35 DHCP BOGOTA2

DISPOSITIVO	CONFIGURACIONES
BOGOTA2	BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4 BOGOTA2(config)#ip dhcp pool BOGOTA-LAN2 BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.1.1 BOGOTA2(dhcp-config)#exit BOGOTA2(config)#ip dhcp pool BOGOTA-LAN1 BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.0.1

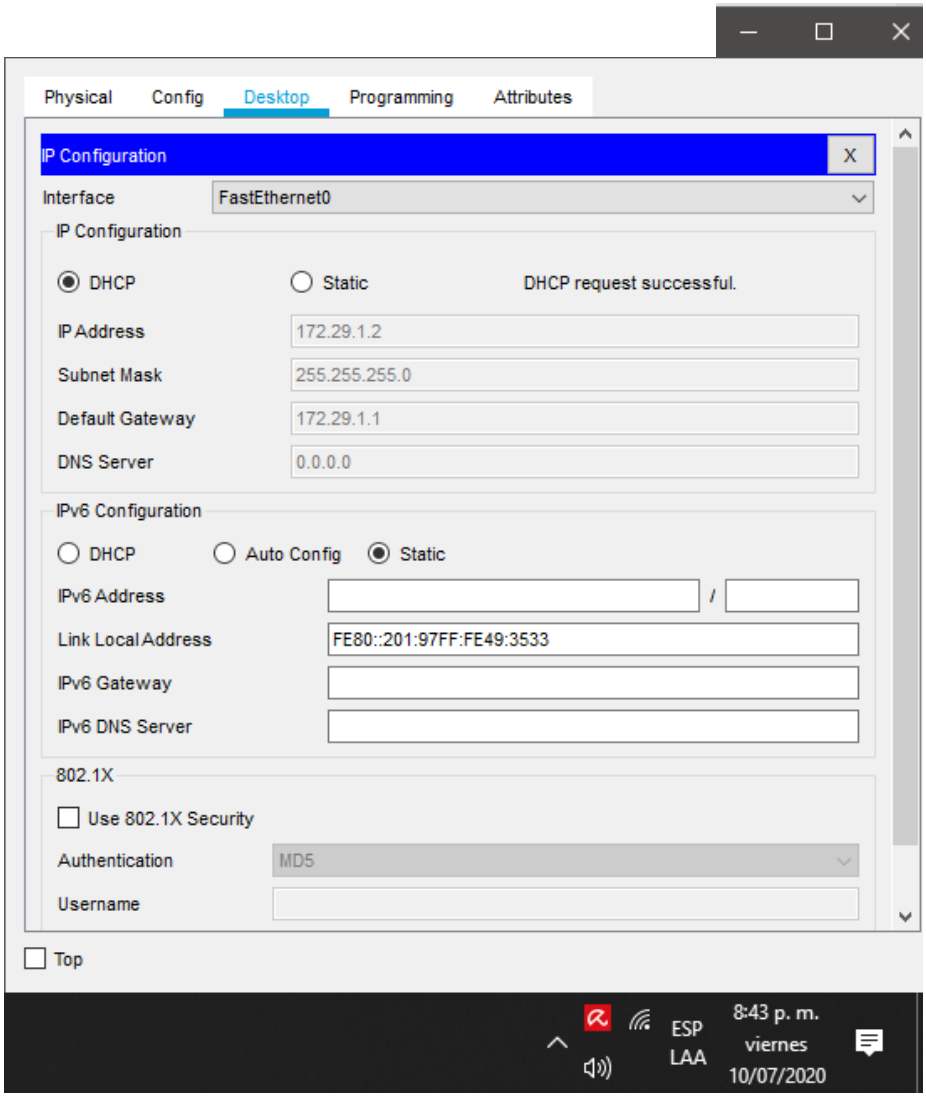
b. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Se procede a realizar configuraciones en BOGOTA3 para que habilite el paso de los mensajes broadcast.

Tabla 36 HABILITACIÓN BOGOTA3

DISPOSITIVO	CONFIGURACIONES
BOGOTA3	BOGOTA3(config)#int g0/0 BOGOTA3(config-if)#ip helper-address 172.29.3.13 BOGOTA3(config-if)#exit

Figura 35 DHCP BOGOTA



CONCLUSIÓN

Con el desarrollo del primer escenario, se logró adquirir conocimientos en varios conceptos de redes mediante el uso de la herramienta cisco packet tracert donde se realizaron los ejercicios de la guía y donde se hizo más fácil simular configuraciones básicas a equipos router y switches, vlans, restricciones y parámetros que aumentan la seguridad en la red, entre otras.

Para el desarrollo del segundo escenario se realizaron diferentes ejercicios que lograron identificar funciones en los equipos tales como verificación de una conexión entre los dispositivos dispuestos en la configuración inicial de la topología, configuraciones OSPF, DHCP, NAT además de las configuraciones iniciales de los dispositivos como los comandos hostname, contraseñas de acceso y mensajes motd.

BIBLIOGRAFÍA

UNAD NETACAD CISCO. (Julio de 2020). Acceso a la red. Obtenido de https://static-course-ssets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

UNAD NETACAD CISCO. (Julio de 2020). Asignación de direcciones ip. Obtenido de https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

UNAD NETACAD CISCO. (Junio de 2020). Direcciones de red IPv6. Obtenido de https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7.2.1

UNAD NETACAD CISCO.(Junio de 2020). Ethernet. Obtenido de https://staticcourse-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

UNAD NETACAD CISCO. (Julio de 2020). Exploración de la red fundamentos de Networking . Obtenido de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

UNAD NETACAD CISCO. (Junio de 2020). Protocolos de capa de red. Obtenido de https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6.1.1

UNAD NETACAD CISCO. (Julio de 2020). Protocolos y comunicaciones de red. Obtenido de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

UNAD NETACAD CISCO. (Junio de 2020). Verificación de conectividad. Obtenido de https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

UNAD NETACAD CISCO. (s.f.). Configuración de un sistema operativo de red. Obtenido de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

ANEXO 1. PRIMER ESCENARIO - SEGUNDO ESCENARIO

https://drive.google.com/drive/folders/1t-3mHJuFRbmf3CRlT9zS9TKcavBTqOzi?usp=sharing