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

OMAR ERNESTO TRASLAVIÑA DELGADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERIA DE SISTEMAS

BUCARAMANGA

2020

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

OMAR ERNESTO TRASLAVIÑA DELGADO

Trabajo como opción de grado para optar al título de

Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERIA DE SISTEMAS

BUCARAMANGA

2020

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

Lista de Figuras

Pág.

RESUMEN

El presente trabajo de grado se realiza con el propósito de afianzar de manera práctica los conocimientos adquiridos a lo largo del Diplomado De Profundización CISCO (Diseño e Implementación de Soluciones Integradas LAN/WAN), simulando escenarios de configuración presentes en entornos corporativos y atacados con el uso de tecnología CISCO.

El desarrollo del trabajo comprende 2 escenarios en los cuales se aplican los conocimientos adquiridos de configuración e implementación de seguridad de acceso a dispositivos, protocolos de enrutamiento dinámico (RIP, OSPF), acceso mediante Telnet o SSH, comunicación mediante enlaces troncales, asignación automática de direccionamiento IP (DHCP) y la implementación de traducción de direcciones de red NAT.

Palabras Claves: Computadora, Configuración, Dispositivos, Internet, Intranet, Red de Telecomunicaciones, Topología.

ABSTRACT

The present degree work is carried out with the purpose of practically consolidating the knowledge acquired throughout the CISCO Deepening Diploma (Design and Implementation of Integrated Solutions LAN / WAN), simulating configuration scenarios present in corporate environments and attacked with the use of CISCO technology.

The development of the work includes 2 scenarios in which the acquired knowledge of configuration and implementation of device access security, dynamic routing protocols (RIP, OSPF), access through Telnet or SSH, communication through trunks, automatic assignment of IP addressing (DHCP) and the implementation of NAT network address translation.

Key Words: Computer, Configuration, Devices, Internet, Intranet, Telecommunications Network, Topology.

INTRODUCCIÓN

El desarrollo de entornos simulados es una de las prácticas más efectivas para el afincamiento de conocimiento y es una base primaria, sólida y fuerte de experiencia que nos permite salir a un mundo real con capacidad de resolver un sin número de problemas presentados en la implementación o funcionamiento de redes de telemáticas.

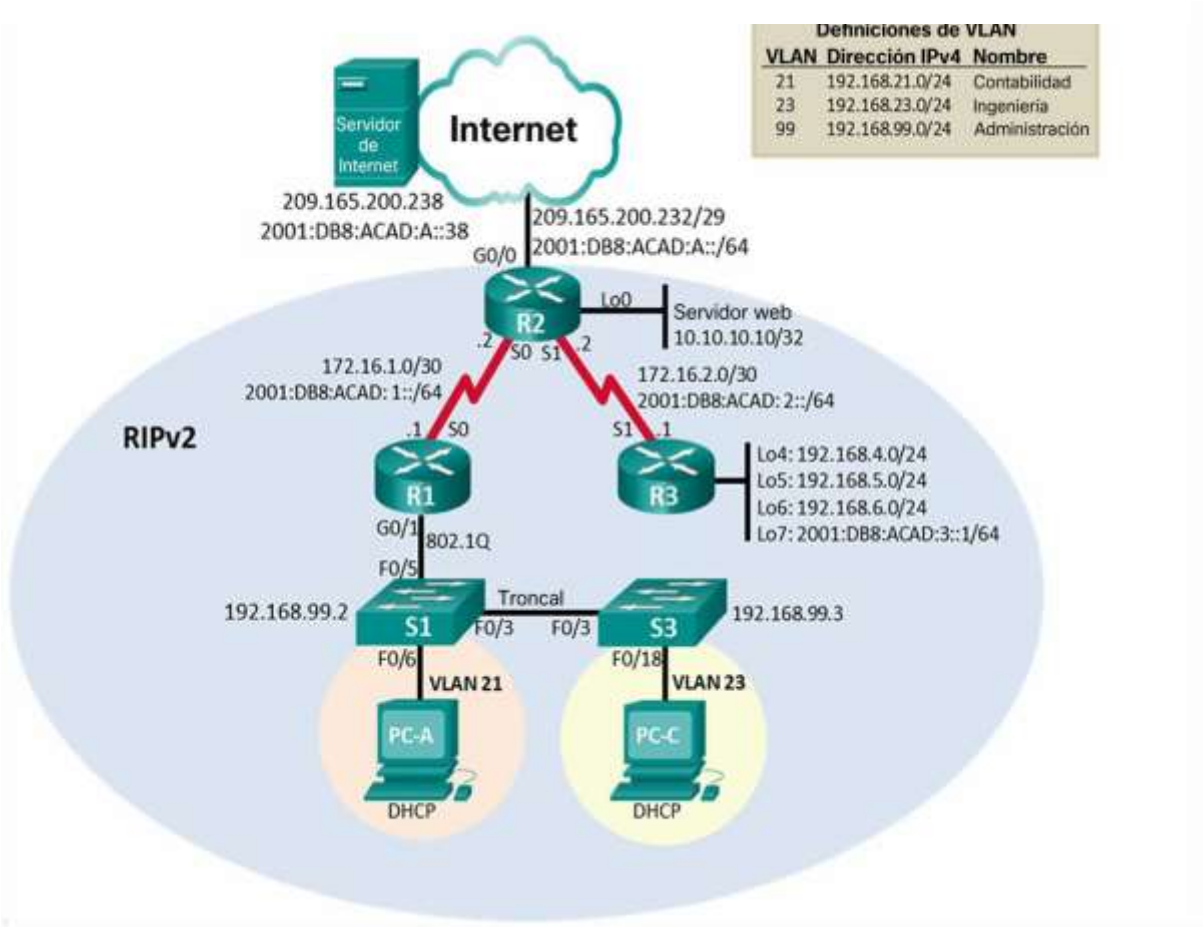
En el presente trabajo se realiza la configuración inicial de dispositivos como computadoras, Routers, y Switches, aprendemos de los niveles más básicos de seguridad que permitirán blindar nuestra red de posibles ataques o acceso no deseados; se introducen configuraciones de protocolos de enrutamiento dinámicos y estáticos y se analiza el comportamiento de cada uno de ellos dentro y fuera de una red de nivel local.

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



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.

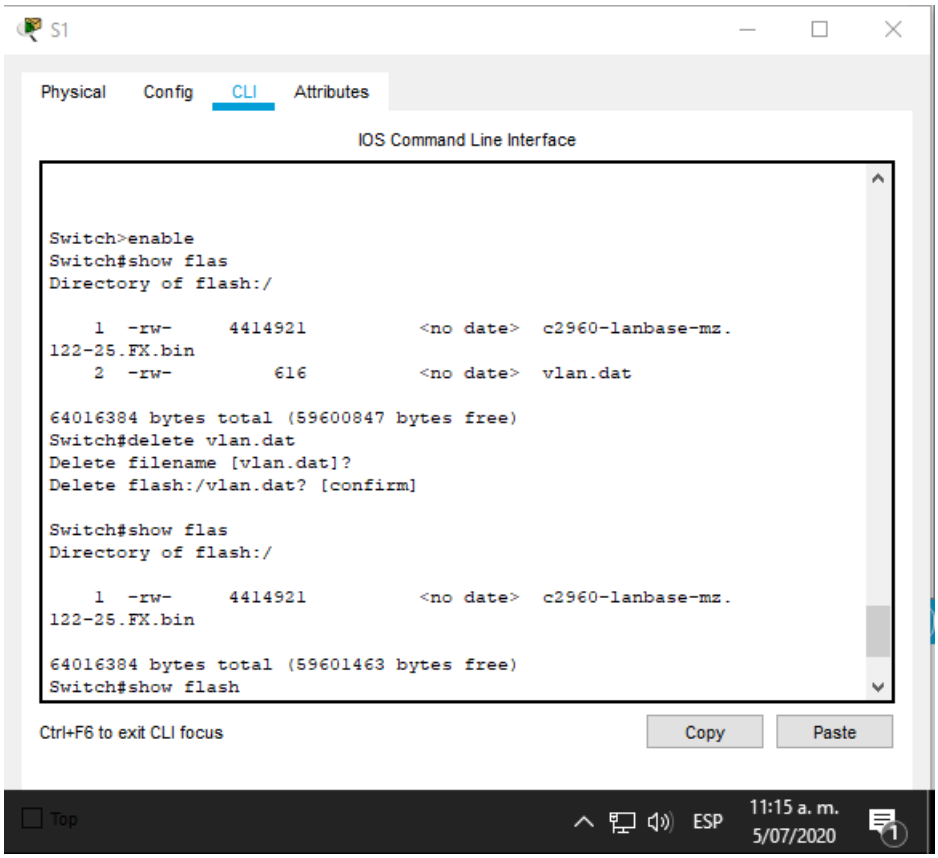
Para eliminar las configuraciones de inicio de los Switchs y Routers debemos eliminar el archivo de configuración inicial común para los dispositivos (startup-config) y eliminar las tablas VLAN (para Routers) y las Base MAC (para los Switch), después de realizados los pasos anteriores recargamos el dispositivo para completar la ejecución

Para realizar las tareas descritas en la tabla1 debemos acceder a los dispositivos en modo privilegiado y ejecutar los comandos de IOS descritos y aceptando los mensajes de confirmación generados por la ejecución de los comandos.

Tabla 1. Comandos de IOS

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router# erase startup-config Switch Router# delete nvram Router# delete flash:vlan.dat Router# copy running-config startup-config
Volver a cargar todos los routers	Router# reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch> enable Switch# erase startup-config Switch# delete 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 flash

Figura 2 - Verificación de eliminación VLAN Switch



Fuente: Elaboración propia Packet Tracer

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 configurara la PC-A configuramos direccionamiento IPv4 basado en la información de la tabla 2 de direccionamiento .

Tabla 2. Direccionamiento Servidor de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225

Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

Paso 2: Configurar R1

Las tareas de configuración inicial para R1 incluyen las siguientes:

Para la configuración inicial de R1 vamos a implementar algunas medidas de seguridad y optimizar el rendimiento; para implementar dichas medidas ingresamos al modo configuración global desde allí vamos a configurar un mensaje de acceso restringido para usuarios, asignar contraseñas de seguridad al acceso modo privilegiado, de consola y VTY, activar el inicio de sesión por contraseñas y por último desactivamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado nos interrumpan la entrada de comandos o visualización de información, configuramos el comando “logging synchronous” para el acceso de consola.

Para la asignación de contraseñas usamos el comando “password” que me permite asignar contraseñas en texto plano, es decir, sin utilizar algoritmos de encriptación; para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación “password-encryption”, que me encriptar todas las contraseñas almacenadas en texto plano.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado es “class” y para consola y VTY “cisco”; usamos el comando “secret” (encripta) para cifrar la contraseña de exec privilegiado y el comando password (no encripta) para los demás.

Para configurar el direccionamiento IPV4 e IPv6 de los dispositivos basado en la información de la topología debemos estar dentro del modo de configuración global para poder seleccionar la interfaz e implementar la configuración; cada

interfaz debe tener una descripción, direcciones IP y para conexiones DTE la frecuencia del reloj se establece en 2000000, una vez configurada la interfaz debe quedar activa.

Se deben configurar rutas predeterminadas IPV4 e IPV6 que me permita enviar el tráfico de red desconocido al router perimetral en este caso R2; usaremos las rutas 0.0.0.0 con mascara 0.0.0.0 e IPv4 del siguiente salto para IPv4 y la red :: prefijo /0 e IPv6 del siguiente salto para IPv6.

Al finalizar el procedimiento de configuración y en modo privilegiado vamos a copiar la configuración actual como de configuración de inicio usando el comando "copy running-config startup-config.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 3 para cada elemento o tarea de configuración.

Tabla 3 – Configuración inicial R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router> enable Router# conf t Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R1
Contraseña de exec privilegiado cifrada	R1(config)# enable secret class
Contraseña de acceso a la consola	R1(config)# line console 0 R1(config-if)# password cisco R1(config-if)# login R1(config-if)# exit
Contraseña de acceso Telnet	R1(config)# line VTY 0 4 R1(config-if)# password cisco R1(config-if)# login R1(config-if)# exit
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption

Mensaje MOTD	R1(config)# banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/0	R1(config)# interface S 0/0/0 R1(config-if)# ip address 172.16.1.1 255.255.255.252 R1(config-if)# description R1 LAN R2 R1(config-if)# no sh R1(config-if)# exit R1(config)# ipv6 unicast-routing R1(config)# interface S 0/0/0 R1(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)# clock rate 2000000 R1(config-if)# no sh R1(config-if)# exit
Rutas predeterminadas	R1# show ip route R1# conf t R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)# ipv6 route ::0/64 2001:DB8:ACAD:1::2 R1(config)# end R1# copy running-config startup-config

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Para la configuración inicial de R2 al igual que en R1 vamos a implementar algunas medidas de seguridad y optimizar el rendimiento; para implementar dichas medidas ingresamos al modo configuración global desde allí vamos a configurar un mensaje de acceso restringido para usuarios, asignar contraseñas de seguridad al acceso modo privilegiado, de consola y VTY, activar el inicio de sesión por contraseñas y por último desactivamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado nos interrumpan la entrada de comandos o visualización de información, configuramos el comando “logging synchronous” para el acceso de consola.

Para la asignación de contraseñas usamos el comando “password” que me permite asignar contraseñas en texto plano, es decir, sin utilizar algoritmos de encriptación; para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación “password-encryption”, que me encriptar todas las contraseñas almacenadas en texto plano.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado es “class” y para consola y VTY “cisco”; usamos el comando “secret” (encripta) para cifrar la contraseña de exec privilegiado y el comando password (no encripta) para los demás.

Para configurar el direccionamiento IPV4 e IPv6 de los dispositivos basado en la información de la topología debemos estar dentro del modo de configuración global para poder seleccionar la interfaz e implementar la configuración; cada interfaz debe tener una descripción, direcciones IP y para conexiones DTE la frecuencia del reloj se establece en 2000000, una vez configurada la interfaz debe quedar activa.

A diferencia de R1 en R2 encontramos una interfaz virtual (loopback) que me va a permitir por medio de configuración IPv4 simular un servidor Web.

Se deben configurar rutas predeterminadas IPV4 e IPV6 en R2 que me permitan acceso al “Servidor de Internet”; usaremos las rutas 0.0.0.0 con mascara 0.0.0.0 e IPv4 del siguiente salto para IPv4 y la red :: prefijo /0 e IPv6 del siguiente salto para IPv6.

Al finalizar el procedimiento de configuración y en modo privilegiado vamos a copiar la configuración actual como de configuración de inicio usando el comando “copy running-config startup-config.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 4 para cada elemento o tarea de configuración.

Tabla 4 - Configuración inicial R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router> enable Router# conf t Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R2
Contraseña de exec privilegiado cifrada	R2(config)# enable secret class
Contraseña de acceso a la consola	R2(config)# line console 0 R2(config-if)# password cisco R2(config-if)# login R2(config-if)# exit
Contraseña de acceso Telnet	R2(config)# line VTY 0 4 R2(config-if)# password cisco R2(config-if)# login R2(config-if)# exit
Cifrar las contraseñas de texto no cifrado	R2(config)# service password-encryption
Habilitar el servidor HTTP	R2(config)# ip http server
Mensaje MOTD	R2(config)# banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/0	R2(config)# ip interface S 0/0/0 R2(config-if)# ip address 172.16.1.2 255.255.255.252 R2(config-if)# description R2 LAN R1 R2(config-if)# no sh R2(config-if)# exit R2(config)# ipv6 unicast-routing R2(config)# interface S 0/0/0 R2(config-if)# ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)# no sh

	R2(config-if)# exit
Interfaz S0/0/1	R2(config)# ip interface S 0/0/1 R2(config-if)# ip address 172.16.2.2 255.255.255.252 R2(config-if)# ip description R2 LAN R3 R2(config-if)# no sh R2(config-if)# exit R2(config)# ipv6 unicast-routing R2(config)# interface S 0/0/1 R2(config-if)# ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)# clock rate 2000000 R2(config-if)# no sh R2(config-if)# exit.
Interfaz G0/0 (simulación de Internet)	R2(config)# ip interface G 0/0 R2(config-if)# ip address 209.165.200.233 255.255.255.248 R2(config-if)# ip description R2 LAN Servidor Web R2(config-if)# no sh R2(config-if)# exit R2(config)# ipv6 unicast-routing R2(config)# interface G 0/0 R2(config-if)# ipv6 address 2001:DB8:ACAD:A::38/64 R2(config-if)# no sh R2(config-if)# exit
Interfaz loopback 0 (servidor web simulado)	R2(config)# interface loopback 0 R2(config-if)# ip address 10.10.10.10 255.255.255.255 R2(config-if)# description Servidor Web Simulado R2(config-if)# exit
Ruta predeterminada	R2# show ip route R2# conf t R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.238 R2(config)# ipv6 route ::/0 2001:DB8:ACAD:A::38 R2(config)# end R2# copy running-config startup-config

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Para la configuración inicial de R3 al igual que en R2 y R1 vamos a implementar algunas medidas de seguridad y optimizar el rendimiento; para implementar dichas medidas ingresamos al modo configuración global desde allí vamos a configurar un mensaje de acceso restringido para usuarios, asignar contraseñas de seguridad al acceso modo privilegiado, de consola y VTY, activar el inicio de sesión por contraseñas y por último desactivamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado nos interrumpan la entrada de comandos o visualización de información, configuramos el comando “logging synchronous” para el acceso de consola.

Para la asignación de contraseñas usamos el comando “password” que me permite asignar contraseñas en texto plano, es decir, sin utilizar algoritmos de encriptación; para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación “password-encryption”, que me encriptar todas las contraseñas almacenadas en texto plano.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado es “class” y para consola y VTY “cisco”; usamos el comando “secret” (encripta) para cifrar la contraseña de exec privilegiado y el comando password (no encripta) para los demás.

Configurar el direccionamiento IPV4 e IPv6 de los dispositivos basado en la información de la topología; la configuración de cada interfaz debe tener una descripción, direcciones IP y para conexiones DTE la frecuencia del reloj se establece en 2000000, una vez configurada la interfaz debe quedar activa.

Al igual que en R2 en R3 debemos configurar interfaces virtuales (loopback) con direccionamiento IPv4 e IPv6 según la información de la topología y utilizando la primera interfaz disponible dentro de cada red

Se deben configurar rutas predeterminadas IPV4 e IPV6 que me permita enviar el tráfico de red desconocido al router perimetral en este caso R2; usaremos las rutas 0.0.0.0 con mascara 0.0.0.0 e IPv4 del siguiente salto para IPv4 y la red :: prefijo /0 e IPv6 del siguiente salto para IPv6.

Al finalizar el procedimiento de configuración y en modo privilegiado vamos a copiar la configuración actual como de configuración de inicio usando el comando "copy running-config startup-config.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 5 para cada elemento o tarea de configuración.

Tabla 5 - Configuración inicial R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router> enable Router# conf t Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R3
Contraseña de exec privilegiado cifrada	R3(conf)# enable secret class
Contraseña de acceso a la consola	R3(config)# line console 0 R3(config-if)# password cisco R3(config-if)# login R3(config-if)# exit
Contraseña de acceso Telnet	R3(config)# line VTY 0 4 R3(config-if)# password cisco R3(config-if)# login R3(config-if)# exit l

Cifrar las contraseñas de texto no cifrado	R3(config)# service password-encryption
Mensaje MOTD	R3(config)# banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/1	R3(config)# ip interface S 0/0/1 R3(config-if)# ip address 172.16.2.1 255.255.255.252 R3(config-if)# description R3 LAN R2 R3(config-if)# no sh R3(config-if)# exit R3(config)# ipv6 unicast-routing R3(config)# interface S 0/0/1 R3(config-if)# ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)# no sh R3(config-if)# exit
Interfaz loopback 4	R3(config)# interface loopback 4 R3(config-if)# ip address 192.168.4.1 255.255.255.0 R3(config-if)# exit
Interfaz loopback 5	R3(config)# interface loopback 5 R3(config-if)# ip address 192.168.5.1 255.255.255.0 R3(config-if)# exit
Interfaz loopback 6	R3(config)# interface loopback 6 R3(config-if)# ip address 192.168.6.1 255.255.255.0 R3(config-if)# exit l
Interfaz loopback 7	R3(config)# interface loopback 7 R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)# exit
Rutas predeterminadas	R3# show ip route R3# conf t R3(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)# ipv6 route ::/0 2001:DB8:ACAD:2::2 R3(config)# end R3# copy running-config startup-config

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Para la configuración inicial de S1 vamos a implementar algunas medidas de seguridad y optimizar el rendimiento; para implementar dichas medidas ingresamos al modo configuración global desde allí vamos a configurar un mensaje de acceso restringido para usuarios, asignar contraseñas de seguridad al acceso modo privilegiado, de consola y VTY 0 15, activar el inicio de sesión por contraseñas y por último desactivamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado nos interrumpan la entrada de comandos o visualización de información, configuramos el comando “logging synchronous” para el acceso de consola.

Para la asignación de contraseñas usamos el comando “password” que me permite asignar contraseñas en texto plano, es decir, sin utilizar algoritmos de encriptación; para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación “password-encryption”, que me encriptar todas las contraseñas almacenadas en texto plano.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado es “class” y para consola y VTY “cisco”; usamos el comando “secret” (encripta) para cifrar la contraseña de exec privilegiado y el comando password (no encripta) para los demás.

Al finalizar el procedimiento de configuración establecemos la configuración actual como de configuración de inicio.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 6 para cada elemento o tarea de configuración

Tabla 6 - Configuración Inicial S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch> enable Switch# conf t 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-if)# password cisco S1(config-if)# login S1(config-if)# exit
Contraseña de acceso Telnet	S1(config)# line VTY 0 15 S1(config-if)# password cisco S1(config-if)# login S1(config-if)# exit
Cifrar las contraseñas de texto no cifrado	S1(config)# service password-encryption
Mensaje MOTD	S1(config)# banner motd “Se prohíbe el acceso no autorizado” S1(config)# exit S1# copy running-config startup-config

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Para la configuración inicial de S3 al igual que en S1 vamos a implementar algunas medidas de seguridad y optimizar el rendimiento; para implementar dichas medidas ingresamos al modo configuración global desde allí vamos a configurar un mensaje de acceso restringido para usuarios, asignar contraseñas de seguridad al acceso modo privilegiado, de consola y VTY 0 15, activar el inicio de sesión por contraseñas y por último desactivamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado nos interrumpan la entrada de comandos o visualización de información, configuramos el comando “logging synchronous” para el acceso de consola.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado es “class” y para consola y VTY “cisco”; usamos el comando “secret” (encripta) para cifrar la contraseña de exec privilegiado y el comando password (no encripta) para los demás.

Para la asignación de contraseñas usamos el comando “password” que me permite asignar contraseñas en texto plano, es decir, sin utilizar algoritmos de encriptación; para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación “password-encryption”, que me encriptar todas las contraseñas almacenadas en texto plano.

Al finalizar el procedimiento de configuración establecemos la configuración actual como de configuración de inicio.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 7 para cada elemento o tarea de configuración

Tabla 7 - Configuración Inicial S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch> enable Switch# conf t 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-if)# password cisco S3(config-if)# login

	S3(config-if)# exit
Contraseña de acceso Telnet	S3(config)# line VTY 0 4 S3(config-if)# password cisco S3(config-if)# login S3(config-if)# exit
Cifrar las contraseñas de texto no cifrado	S3(config)# service password-encryption
Mensaje MOTD	S3(config)# banner motd “Se prohíbe 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:

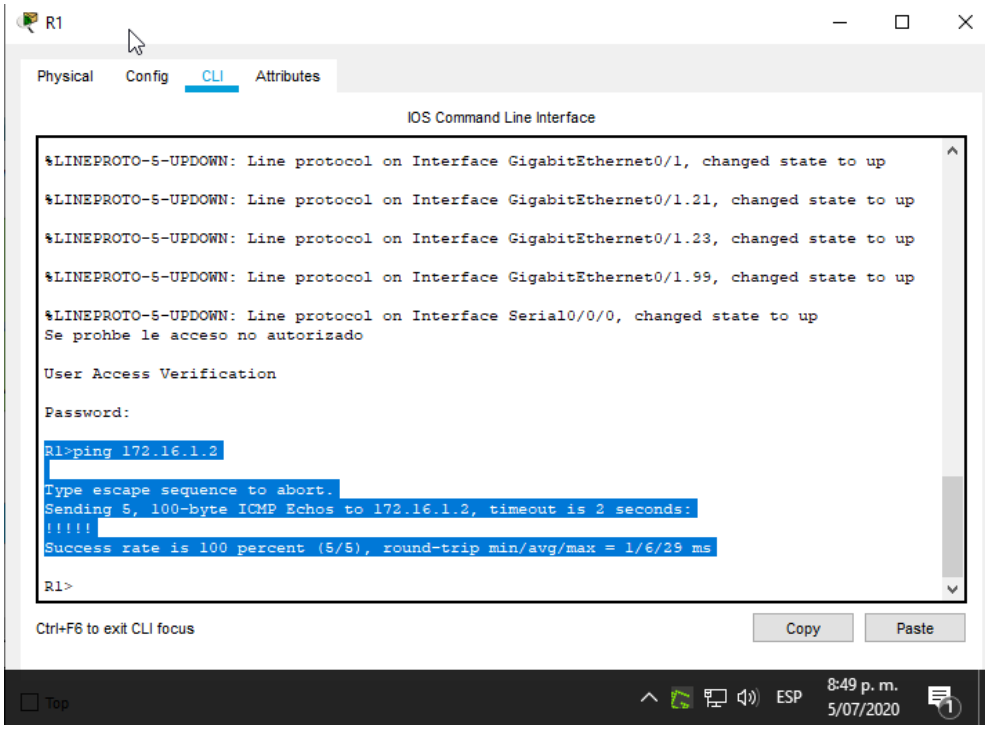
En la tabla 8 podemos notar en la columna de resultados que hasta el momento la configuración de los dispositivos avanza de manera satisfactoria y sin ningún problema.

En las imágenes 2, 3 y 4 podemos ver el resultado del comando ping en cada dispositivo.

Tabla 8 - Conectividad de la red

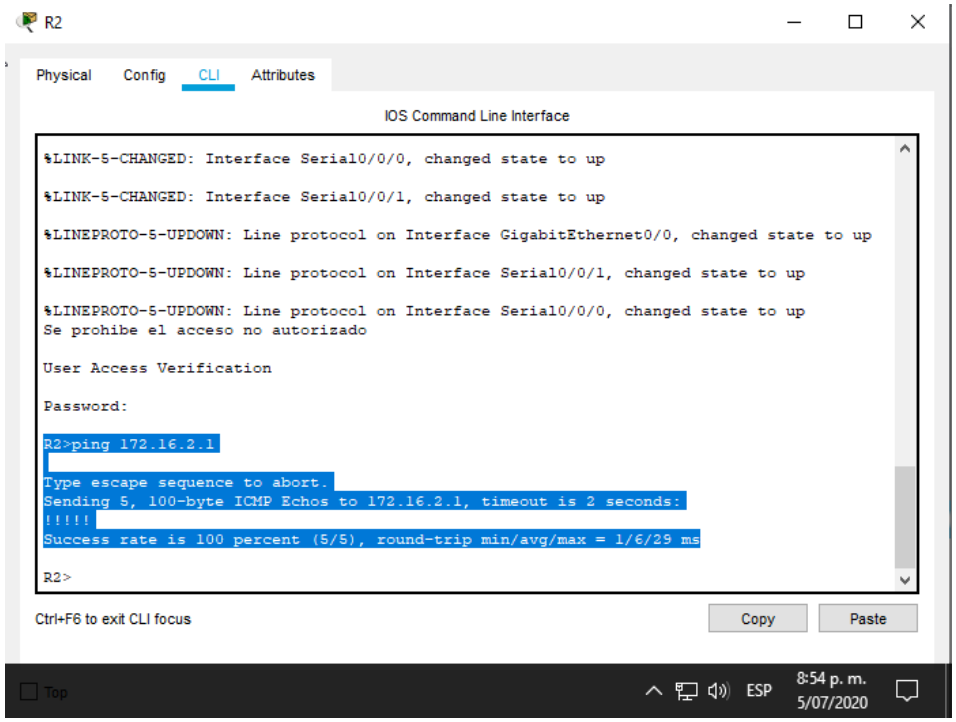
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Figura 3
R2	R3, S0/0/1	172.16.2.1	Figura 4
PC de Internet	Gateway predeterminado	209.165.200.232	Figura 5

Figura 3 - Ping R1 a R2



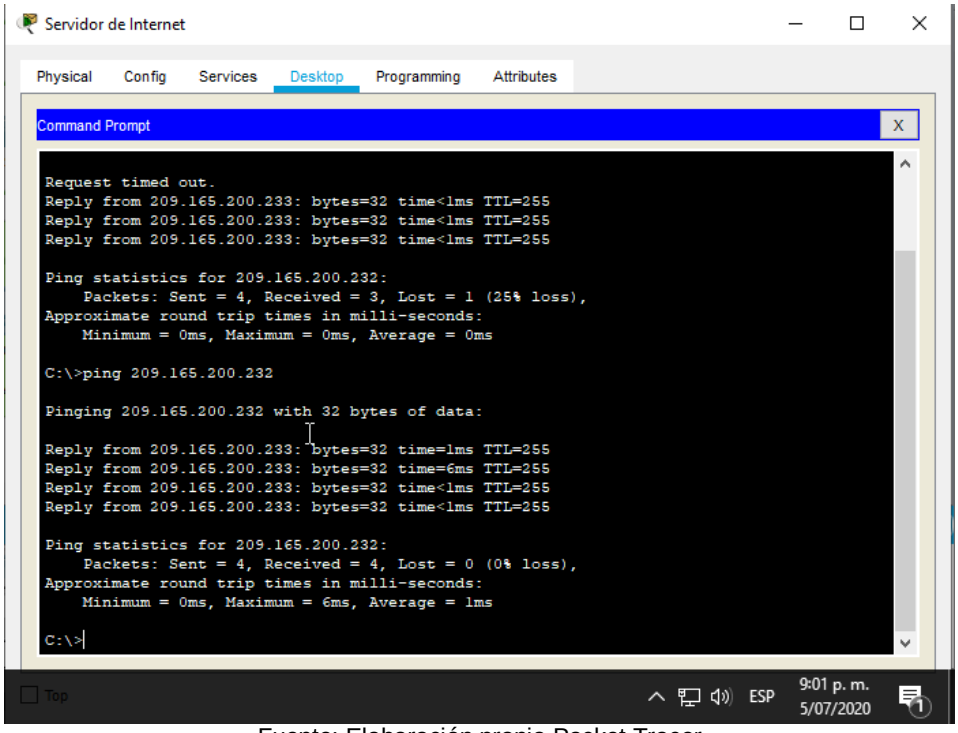
Fuente: Elaboración propia Packet Tracer

Figura 4 - Ping R2 a R3



Fuente: Elaboración propia Packet Tracer

Figura 5 -Ping PC Internet a Gateway Predeterminado



Fuente: Elaboración propia Packet Tracer

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:

Para configurar las VLAN lo primero que debemos hacer es crearlas; nos ubicamos en el modo de configuración global y con los comandos descritos en la columna “Especificaciones” de la Tabla 9 vamos a crear y asignarles propiedades como nombre y direccionamiento IP de administración.

Después de crear las VLAN vamos a seleccionar la VLAN 99 como VLAN administrativa y asignamos la IPv4 192.168.99.3 al S1 como se muestra en la topología.

Para permitir la comunicación entre las redes del Switch y el exterior vamos a configurar la dirección de gateway con la IPv4 192.168.99.1 que es la dirección IPv4 del siguiente salto en este caso R1.

Una vez creadas y configuradas las VLAN descritas en la topología (Contabilidad, Ingeniería, Administración), en modo configuración global vamos a seleccionar las interfaces del Switch que usaremos para conexión o administración de estas redes virtuales y en ellas vamos a configurar propiedades como descripción, direccionamiento IP y tipo de enlace (trunk); los otros interfaces del Switch basta con configurar el tipo de enlace (access) .

La VLAN 1 será asignada como VLAN nativa de los enlaces troncales del Switch en las interfaces F 0/5 y F 0/3.

Para impedir posibles violaciones de seguridad o ingresos no autorizados debemos apagar las interfaces no administrativas; podemos usar el comando "interface range" para seleccionar un rango de interfaces y no tener que configurar una por una.

Para que la PC-A pertenezca a la VLAN 21 como lo muestra la topología, debemos asignar la interfaz de conexión F 0/6 a dicha VLAN.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 9 para cada elemento o tarea de configuración.

Tabla 9 - Configuración de seguridad, VLAN y routing del Switch 1

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

	S1(config-vlan)# end
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)# exit
Asignar el gateway predeterminado	S1(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)# interface F 0/3 S1(config-if)# description Enlace troncal S1 – S3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# end
Forzar el enlace troncal en la interfaz F0/5	S1(config)# interface F 0/5 S1(config-if)# description LAN S1 – R1 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# end
Configurar el resto de los puertos como puertos de acceso	S1(config)# interface range F 0/6 – 24 S1(config-if-range)# switchport mode access S1(config-if-range)# exit
Asignar F0/6 a la VLAN 21	S1(config)# interface F 0/6 S1(config-if)# description S1 - VLAN 21 S1(config-if)# switchport mode access S1(config-if)# switchport access VLAN 21 S1(config-if)# exit
Apagar todos los puertos sin usar	S1(config)# interface range F 0/7 - 24 S1(config-if-range)# shutdown S1(config-if-range)# end

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Para configurar las VLAN lo primero que debemos hacer es crearlas; nos ubicamos en el modo de configuración global y con los comandos descritos en la columna “Especificaciones” de la Tabla 9 vamos a crear y asignarles propiedades como nombre y direccionamiento IP de administración.

Después de crear las VLAN vamos a seleccionar la VLAN 99 como VLAN administrativa y asignamos la IPv4 192.168.99.3 al S1 como se muestra en la topología.

Para permitir la comunicación entre las redes del Switch y el exterior vamos a configurar la dirección de gateway con la IPv4 192.168.99.1 que es la dirección IPv4 del enrutador más cercano (R1).

Una vez creadas y configuradas las VLAN descritas en la topología (Contabilidad, Ingeniería, Administración), en modo configuración global vamos a seleccionar las interfaces del Switch que usaremos para conexión o administración de estas redes virtuales y en ellas vamos a configurar propiedades como descripción, direccionamiento IP y tipo de enlace (trunk); los otros interfaces del Switch basta con configurar el tipo de enlace (access) .

La VLAN 1 será asignada como VLAN nativa del enlace troncal del Switch en la interface F 0/3.

Para impedir posibles violaciones de seguridad o ingresos no autorizados debemos apagar las interfaces no administrativas; podemos usar el comando “interface range” para seleccionar un rango de interfaces y no tener que configurar una por una.

Para que la PC-C pertenezca a la VLAN 23 como lo muestra la topología, debemos asignar la interfaz de conexión F 0/18 a dicha VLAN.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 10 para cada elemento o tarea de configuración

Tabla 10 - Configuración de VLAN, seguridad y routing de Switch 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3> enable S3# conf t 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 dirección IP de administración	S3(config)# interface vlan 99 S3(config-if)# ip address 192.168.99.3 255.255.255.0 S3(config-if)# exit
Asignar el gateway predeterminado.	S3(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)# interface F 0/3 S3(config-if)# description Enlace troncal S3 - S1 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native VLAN 1 S3(config-if)# exit
Configurar el resto de los puertos como puertos de acceso	S3(config)# interface range F 0/4 – 24 S3(config-if-range)# switchport mode Access S3(config-if-range)# exit
Asignar F0/18 a la VLAN 23	S3(config)# interface F 0/18 S3(config-if)# description S3 en VLAN 23 S3(config-if)# switchport mode access S3(config-if)# switchport access VLAN 23 S3(config-if)# no shutdown S3(config-if)# exit
Apagar todos los puertos sin usar	S3(config)# interface range F 0/19 - 24 S3(config-if-range)# shutdown S3(config-if-range)# end

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Para configurar enrutamiento VLAN dentro de R1 vamos a usar el tipo de enrutamiento router-on-a-stick; la configuración es bastante sencilla, solo debemos crear una subinterfaz por cada VLAN que vayamos a utilizar dentro de una interfaz.

Para la VLAN de Contabilidad, Ingeniería y Administración vamos a crear las subinterfaces .21, .23 y .99 respectivamente dentro de la interfaz de conexión o enlace trocal G 0/1.

Antes de asignar una IP a la subinterfaz, debemos configurarla para que funcione dentro de una VLAN específica, para lograrlo vamos a usar el comando "encaptulation dot1Q" ID_VLAN. para cada una de las interfaces.

Para cada Subinterfaz vamos a configurar una descripción, asignarla a la VLAN correspondiente (Según Topología) y un direccionamiento IP, que para este caso será la primera IP disponible de la VLAN a la cual pertenezca la subinterfaz

La descripción de las Subinterfaces debe cumplir con la sintaxis "LAN de VLAN ID".

Por último, todas las subinterfaces deben quedar activas.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 11 para cada elemento o tarea de configuración

Tabla 11 - Configuración de Routing R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1> enable R1# conf t R1(config)# interface G 0/1.21 R1(config-subif)# encapsulation dot1Q 21 R1(config-subif)# ip address 192.168.21.1 255.255.255.0 R1(config-subif)# description LAN de Contabilidad R1(config-subif)# no sh R1(config-if)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)# interface G 0/1.23 R1(config-subif)# encapsulation dot1Q 23 R1(config-subif)# ip address 192.168.23.1 255.255.255.0 R1(config-subif)# description LAN de Ingenieria R1(config-subif)# no sh R1(config-if)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)# interface G 0/1.99 R1(config-subif)# encapsulation dot1Q 99 R1(config-subif)# ip address 192.168.99.1 255.255.255.0 R1(config-subif)# description LAN Administracion R1(config-subif)# no sh R1(config-if)#exit
Activar la interfaz G0/1	R1(config)# interface G 0/1 R1(config-if)# no sh R1(config-if)#end

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:

Tabla 12 - Verificación Routing R1

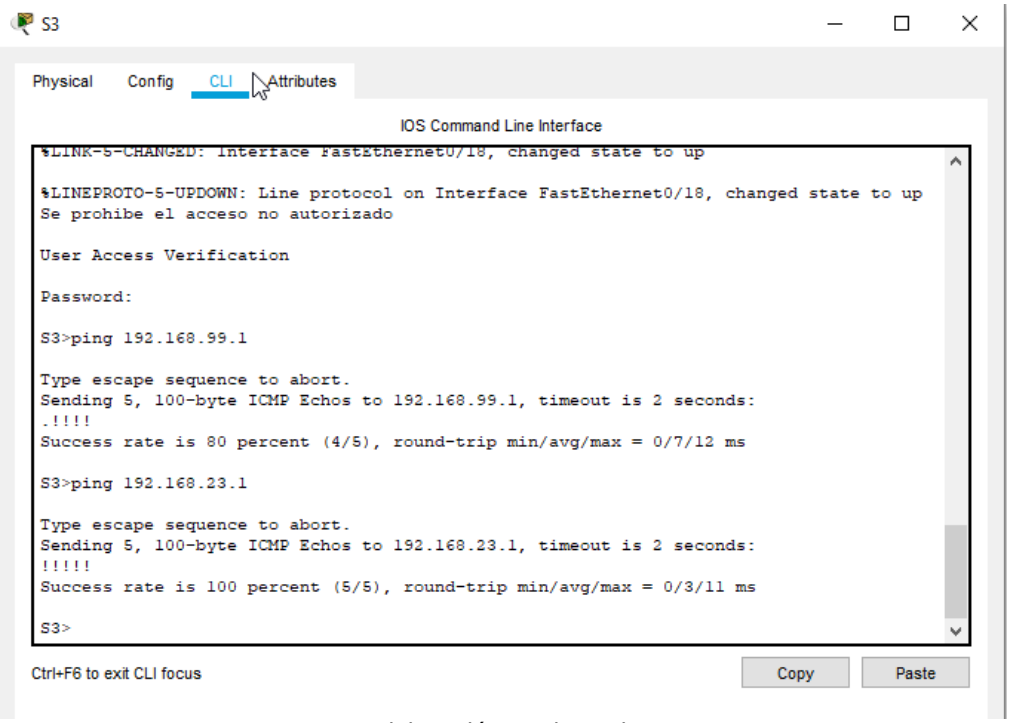
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Figura 7
S3	R1, dirección VLAN 99	192.168.99.1	Figura 8
S1	R1, dirección VLAN 21	192.168.21.1	Figura 7
S3	R1, dirección VLAN 23	192.168.23.1	Figura 8

Como podemos ver en las imágenes 6 y 7, los PING a las subinterfaces de R1 se completaron con éxito, prueba de que hasta el omento todo va bien dentro de nuestra configuración.

Figura 6 - Ping S1 a VLAN 99 y VLAN 21

Fuente: Elaboración propia Packet Tracer

Figura 7 - Ping S3 - VLAN 99 y VLAN 23



Fuente: Elaboración propia Packet Tracer

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para RIPv2 en R1 incluyen las siguientes:

El primer paso es ingresar al modo de configuración global; por medio del comando “router rip” habilitamos RIP y cambiamos la versión del protocolo mediante el comando “versión 2”

Después de activar y cambiar la versión del RIP vamos a anunciar las redes con la ayuda del comando “network” seguido de la IP de la red a presentar que para este caso son las conectadas directamente al router.

Para evitar el desperdicio de ancho de banda, desperdicio de recursos y riesgos de seguridad que se presenta con la actualización periódica del protocolo RIP

vamos a configurar las interfaces LAN como pasivas (No envía actualización RIP) con la ayuda del comando “passive-interfaces”.

Por último, para evitar que el RIP resuma automáticamente las redes a dirección con clase en routers fronterizos vamos a utilizar el comando “no auto-summary”.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 13 para cada elemento o tarea de configuración

Tabla 13 - Configuración RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1> enable R1# config t R1(config)# router rip R1(config-router)# versión 2
Anunciar las redes conectadas directamente	R1(config-router)# network 172.16.1.0 R1(config-router)# network 192.168.21.0 R1(config-router)# network 192.168.23.0 R1(config-router)# network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)# passive-interface G 0/1
Desactive la sumarización automática	R1(config-router)# no auto-summary R1(config-router)# end

Paso 2: Configurar RIPv2 en el R2

La configuración del RIP en R2 al igual que en R1 incluye las siguientes tareas:

El primer paso es ingresar al modo de configuración global; por medio del comando “router rip” habilitamos RIP y cambiamos la versión del protocolo mediante el comando “versión 2”.

Después de activar y cambiar la versión del RIP vamos a anunciar las redes con la ayuda del comando “network” seguido de la IP de la red a presentar que para este caso son las conectadas directamente al.

Para evitar el desperdicio de ancho de banda, desperdicio de recursos y riesgos de seguridad que se presenta con la actualización periódica del protocolo RIP vamos a configurar la interface LAN (loopback) como pasiva (No envía actualización RIP) con la ayuda del comando “passive-interfaces”.

Para evitar que el RIP resuma automáticamente las redes a dirección con clase en routers fronterizos vamos a utilizar el comando “no auto-summary”.

Por último, para efectos de pruebas vamos a omitir el anuncio de la red conectada a la interfaz G 0/0.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 14 para cada elemento o tarea de configuración.

Tabla 14 - Configuración de RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2> enable R2# config t R2(config)# router rip R2(config-router)# versión 2
Anunciar las redes conectadas directamente	R2(config-router)# network 10.10.10.10 R2(config-router)# network 172.16.1.0 R2(config-router)# network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)# passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)# no auto-summary R2(config-router)# end R2# copy running-config startup-config

Paso 3: Configurar RIP2 en el R2

La configuración del RIP en R3 al igual que en R2 y R3 incluye las siguientes tareas:

El primer paso es ingresar al modo de configuración global; por medio del comando “router rip” habilitamos RIP y cambiamos la versión del protocolo mediante el comando “versión 2”

Después de activar y cambiar la versión del RIP vamos a anunciar las redes con la ayuda del comando “network” seguido de la IP de la red a presentar que para este caso son las conectadas directamente al router.

Para evitar el desperdicio de ancho de banda, desperdicio de recursos y riesgos de seguridad que se presenta con la actualización periódica del protocolo RIP vamos a configurar las interfaces LAN (loopback) como pasivas (No envía actualización RIP) con la ayuda del comando “passive-interfaces”.

Por último, para evitar que el RIP resuma automáticamente las redes a dirección con clase en routers fronterizos vamos a utilizar el comando “no auto-summary”.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 15 para cada elemento o tarea de configuración.

Tabla 15 - Configuración de RIPv3 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3> enable R3# config t R3(config)# router rip R3(config-router)# versión 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)# network 172.16.2.0 R3(config-router)# network 192.168.4.0 R3(config-router)# network 192.168.5.0 R3(config-router)# network 192.168.6.0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)# passive-interface loopback 4 R3(config-router)# passive-interface loopback 5 R3(config-router)# passive-interface loopback 6
Desactive la sumarización automática.	R2(config-router)# no auto-summary R2(config-router)# exit

Paso 4: Verificar la información de RIP

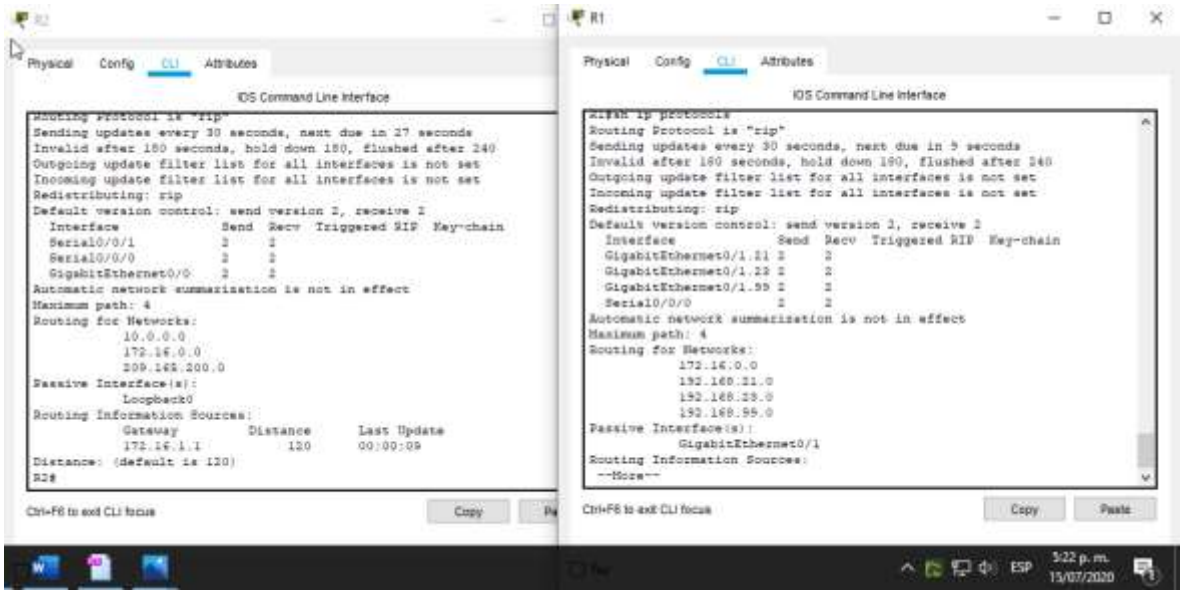
Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 16 - Verificación de información RIP v2

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 (Figura 8)
¿Qué comando muestra solo las rutas RIP?	show ip rip database (Figura 9)
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show running-config | section rip (Figura 10)

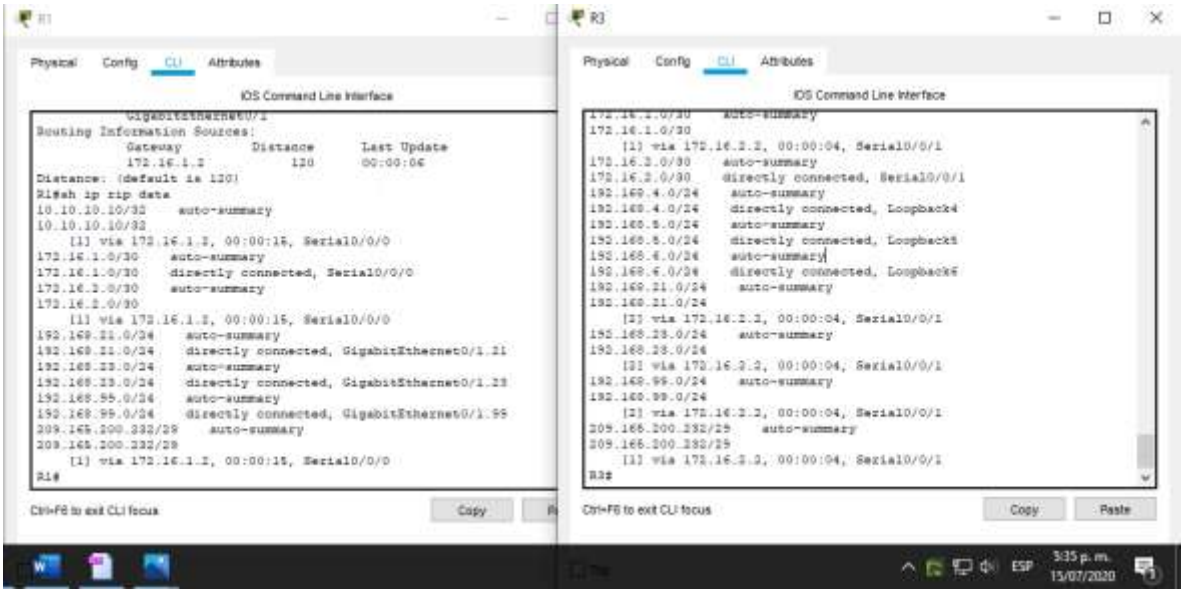
En las Figuras 8, 9 y 10 podemos verificar la información solicitada en cada una de las preguntas de la Tabla 16.

Figura 8 - Verificación ip Protocols



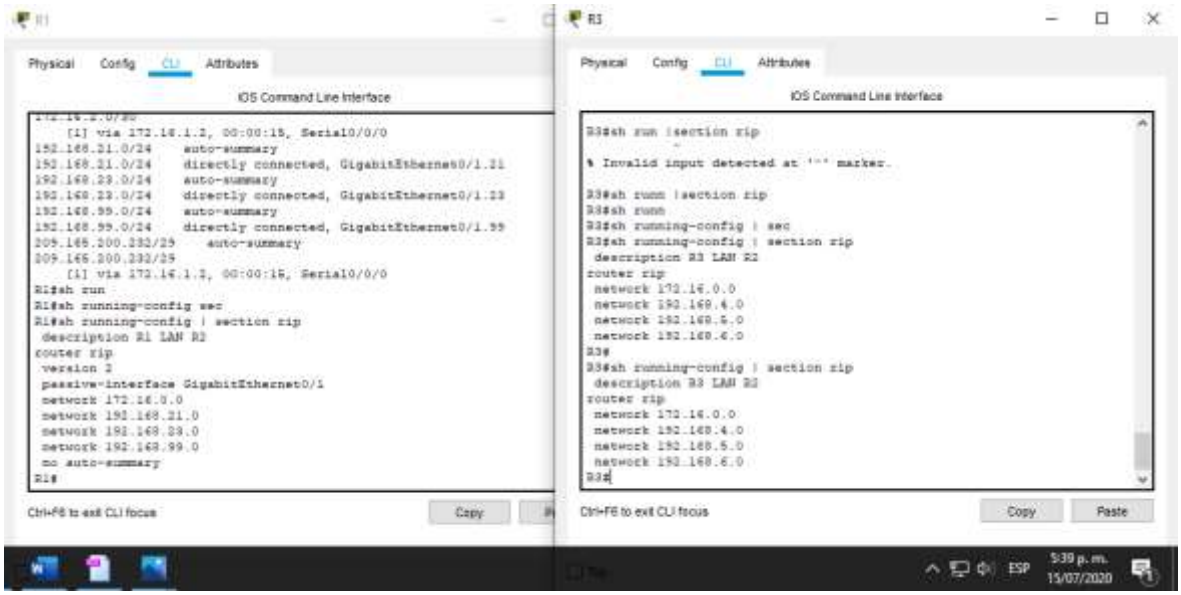
Fuente: Elaboración propia Packet Tracer

Figura 9 - Verificación Base de datos RIP



Fuente: Elaboración propia Packet Tracer

Figura 10 - Verificación RIP en ejecución



Fuente: Elaboración propia Packet Tracer

Parte 5: Implementar DHCP y NAT para IPv4

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

Un router cuando funciona como servidor DHCPv4 asigna todas las direcciones IPv4 disponibles de un conjunto de direcciones DHCP.

Desde el modo de configuración global vamos a configurar R1 como servidor DHCP; para excluir las primeras 20 direcciones para las redes VLAN 21 y VLAN 23 vamos a utilizar el comando “exclude-address”.

Paso seguido, configurar un pool de direcciones para cada VLAN con los siguientes datos:

- VLAN 21:
  - Nombre: ACCT
  - Servidor DNS: 10.10.10.10
  - Nombre de dominio: ccna-sa.com
  - Gateway: 192.168.21.1
- VLAN 23:

- Nombre: ENGNR
- Servidor DNS: 10.10.10.10
- Nombre de dominio: ccna-sa.com
- Gateway: 192.168.23.1

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 17 para cada elemento o tarea de configuración

Tabla 17 - Configuración DHCP R1 para VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1> enable R1# config t R1(config)# ip dhcp exclude-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)# ip dhcp exclude-address 192.168.23.1 192.168.23.21
Crear un pool de DHCP para la VLAN 21.	R1(config)# ip dhcp pool ACCT R1(dhcp-config)# dns-server 10.10.10.10 R1(dhcp-config)# domain-name ccna-sa.com R1(dhcp-config)# default-router 192.168.21.1 R1(dhcp-config)# network 192.168.21.0 255.255.255.0 R1(dhcp-config)# exit
Crear un pool de DHCP para la VLAN 23	R1(config)# ip dhcp pool ENGNR R1(dhcp-config)# dns-server 10.10.10.10 R1(dhcp-config)# domain-name ccna-sa.com R1(dhcp-config)# default-router 192.168.23.1 R1(dhcp-config)# network 192.168.23.0 255.255.255.0 R1(dhcp-config)# exit

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

La configuración del R2 incluye las siguientes tareas:

Para la configuración de NAT primero vamos a crear una cuenta de usuario dentro de una base de datos local con los siguientes datos:

- Nombre de Usuario: webuser
- Clave: cisco12345
- Nivel de Privilegio 15.

Vamos a realizar una asignación entre las direcciones local interna y las direcciones globales internas que permitirá a un equipo de la red local mediante traducción NAT llegar al servidor de internet.

Para configurar NAT vamos a usar la información proporcionada en la topología y una vez asignadas vamos a configurar las interfaces participantes en la traducción con respecto al NAT.

Para la configuración de NAT dinámica vamos a crear una lista de acceso que me permita la traducción de las redes de Contabilidad y de Ingeniería en R1 y un resumen de traducción de las redes LAN (loopback) en R3.

Para finalizar la configuración vamos a utilizar un pool de direcciones publicas dentro de R1 de nombre INTERNET y un conjunto de direcciones que incluyen las IP desde la 209.165.200.225 hasta la 209.165.200.228.

Para aplicar la configuración descrita anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 18 para cada elemento o tarea de configuración

Tabla 18 - Configuración de NAT estática y dinámica R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2> enable R2# config t R2(config)# username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)# ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)# ip http authentication local
Crear una NAT estática al servidor web.	R2(config)# ip nat source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)# int G 0/0 R2(config-if)# ip nat outside R2(config)#exit R2(config)# int S 0/0/0 R2(config-if)# ip nat inside R2(config)#exit R2(config)# int S 0/0/1 R2(config-if)# ip nat inside R2(config)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2(config)# access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)# access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)# access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)# ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET

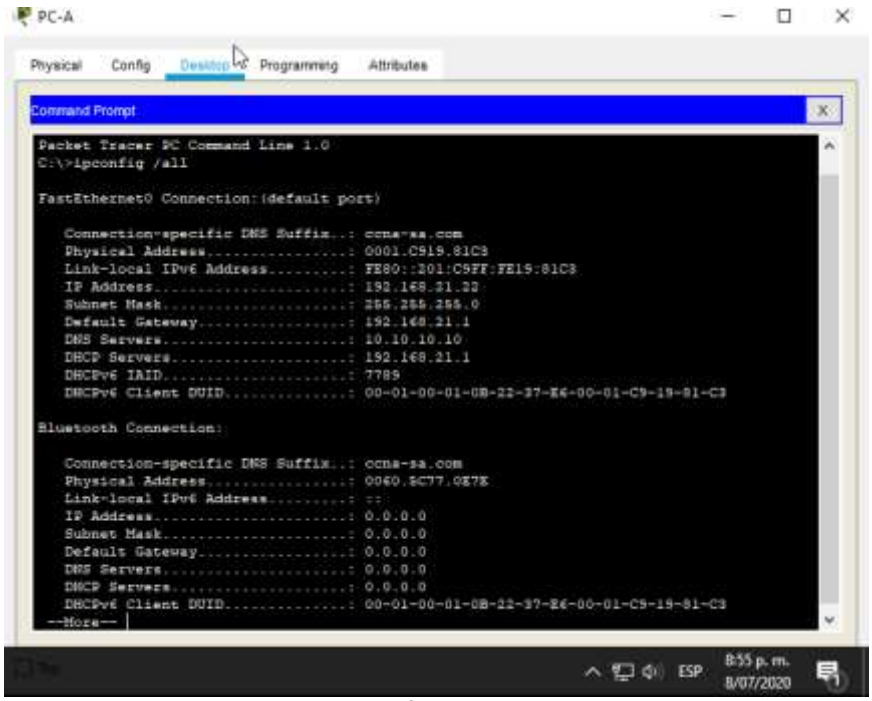
Paso 3: Verificar el protocolo DHCP y la NAT estática

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.

Tabla 19 - Verificación DHCP y NAT Estática

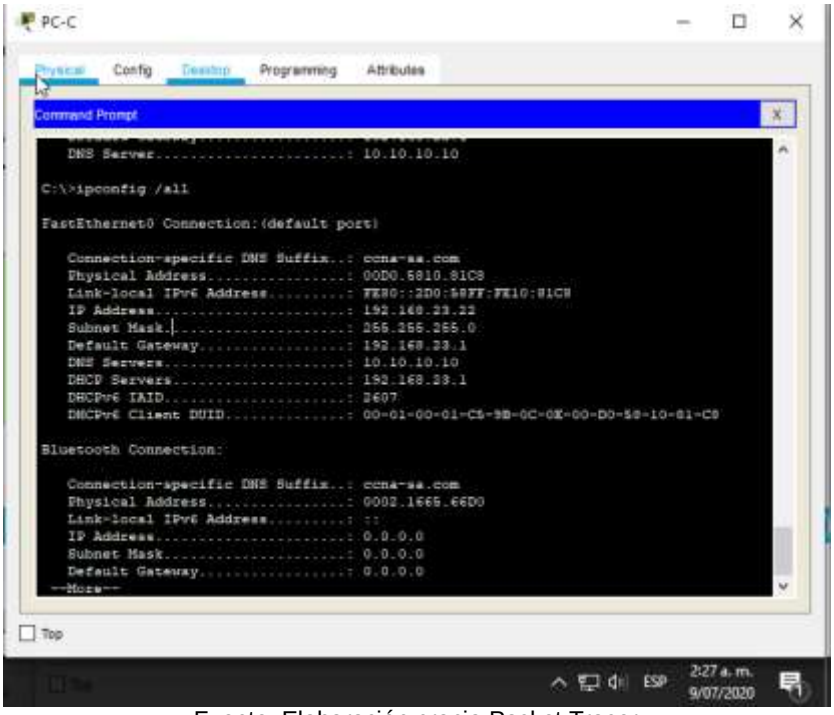
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 11
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 12
Verificar que la PC-A pueda hacer ping a la PC-C	Figura 13
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Figura 14

Figura 11 - Verificación DHCP PC-A



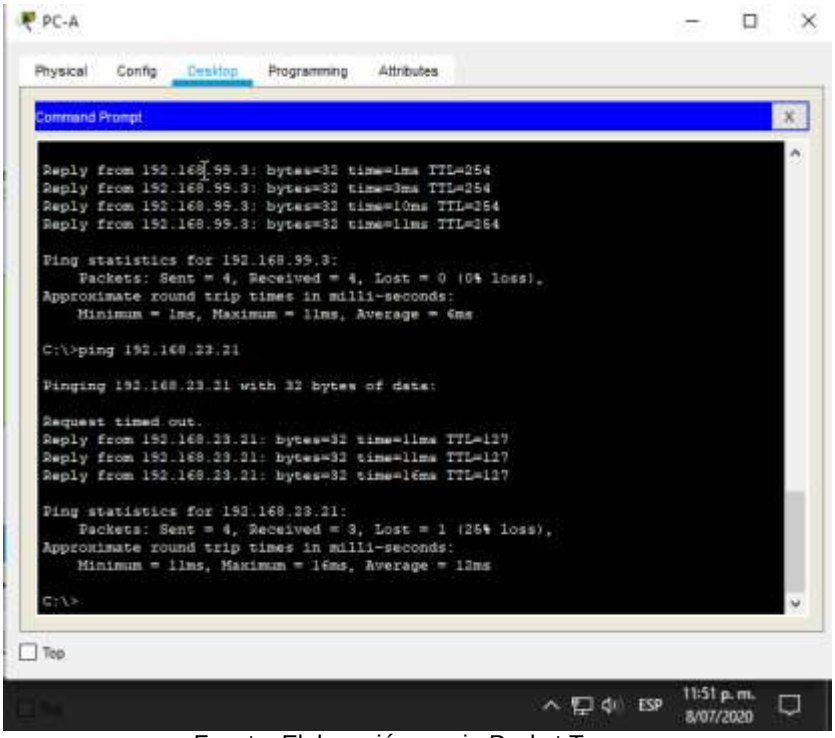
Fuente: Elaboración propia Packet Tracer

Figura 12 - Verificación DHCP PC-C



Fuente: Elaboración propia Packet Tracer

Figura 13 - Verificación de conexión DHCP entre PC-A y PC-B

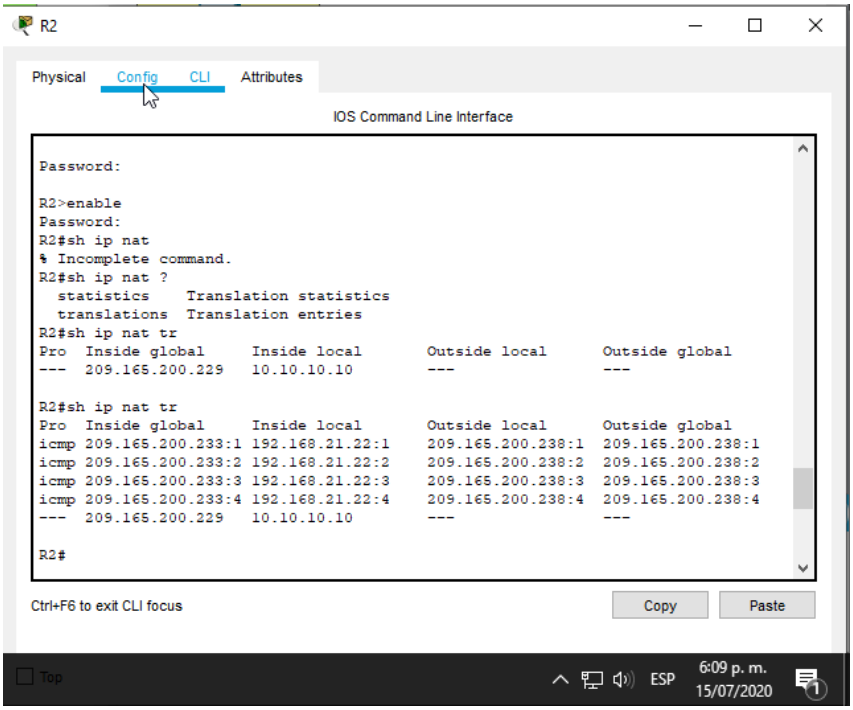


Fuente: Elaboración propia Packet Tracer

Figura 14 - Verificación de NAT

Fuente: Elaboración propia Packet Tracer

Figura 15 - Verificación traducción NAT R2



fuente: Elaboración propia Packet Tracer

Parte 6: Configurar NTP

En la siguiente configuración vamos a ver el funcionamiento del protocolo de tiempo NTC; lo primero que haremos es configurar la hora de R2 con ayuda del comando “clock set” en modo privilegiado vamos a asignar la fecha hora 9 de julio de 2020, 7:00 a.m., y verificamos la configuración usando el comando “show clock detail”.

Para poder sincronizar la hora de los dispositivos de la red a la misma de R2, vamos a establecer a R2 como servidor NTP estrato 5 y vamos a utilizar el comando de “ntp server” para asignar en los dispositivos a R2 como servidor NTP.

Para poder verificar la configuración usaremos los comandos “show ntp associations” que me permite ver la asociación del dispositivo al servidor NTP y el comando “show clock detail” que me permite visualizar en detalle la fecha hora.

Por último, vamos a utilizar el comando “show clock detail” para verificar la configuración de los dispositivos.

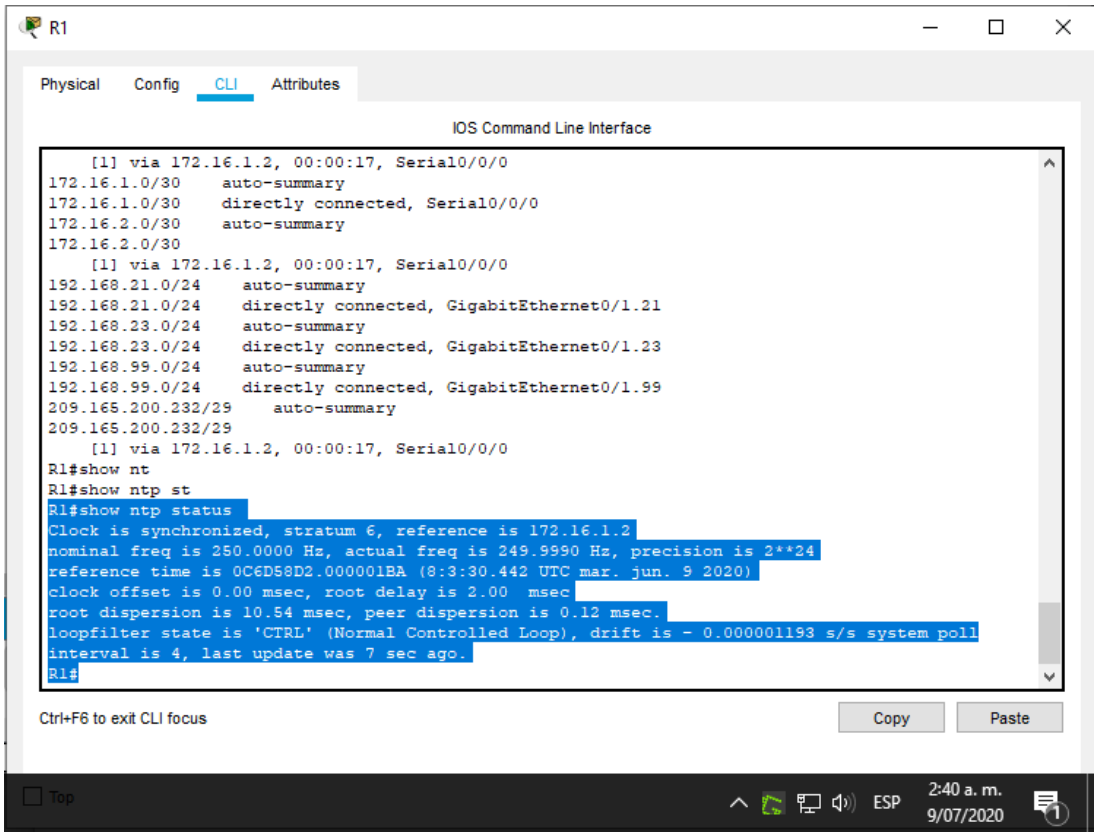
Para completar la configuración descrita vamos a ejecutar los comandos descritos en la especificación de la tabla 20 para cada elemento o tarea de configuración.

Tabla 20 - Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2> enable R2# config t R2(config)# clock set 10:00:00 jun 9 2020
Configure R2 como un maestro NTP.	R2(config)# ntp master 5 R2(config)# end
Configurar R1 como un cliente NTP.	R1> enable R1# config t R1(config)# ntp server 192.16.1.2

Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)# ntp update-calendar R1(config)# end
Verifique la configuración de NTP en R1.	R1(config)# show ntp status

Figura 16 - Verificación de NTP en R1



Fuente: Elaboración propia Packet Tracer

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

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

Para restringir el acceso a las conexiones Telnet o SSH, vamos a crear listas de acceso permitiendo o denegando el ingreso de los equipos dentro de la red.

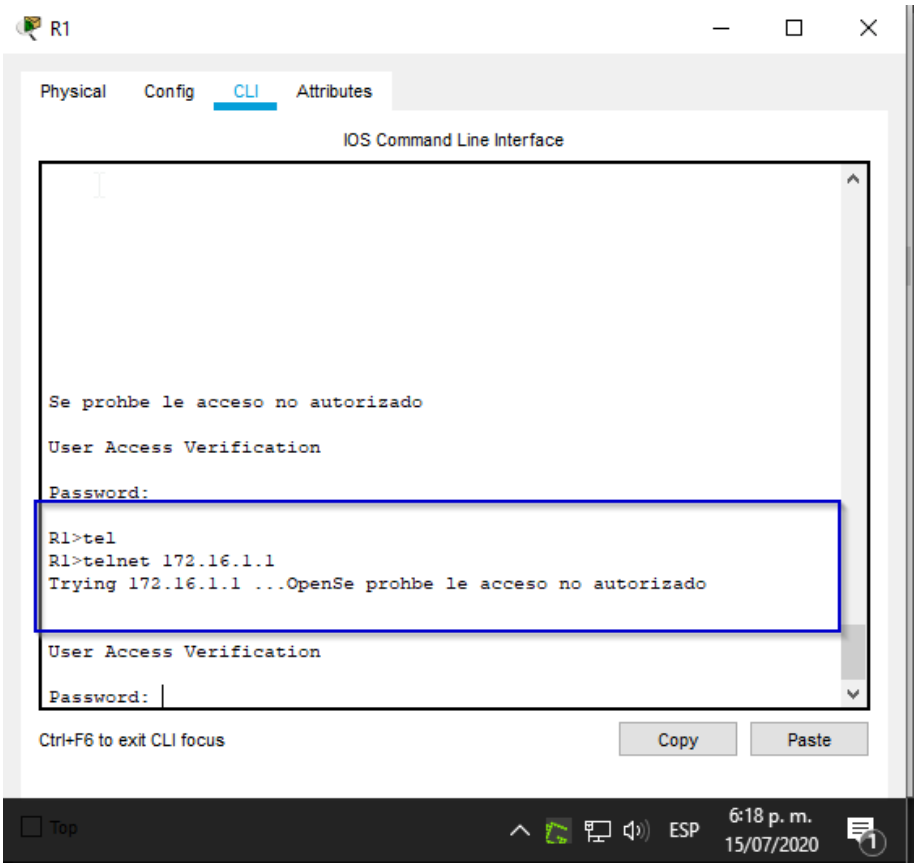
La ACL debe tener como nombre: ADMIN-MGT.

Para completar la configuración ejecutamos los comandos de especificación de la Tabla 21 para cada Elemento o tarea.

Tabla 21 - Configuración y Verificación de 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> enable R2# conf t R2(config)# ip access-list standard ADMIN-MGT R2(config-std-nacl)# permit host 172.16.1.1 R2(config-std-nacl)# exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)# line VTY 0 15 R2(config-line)# access-class ADMIN-MGT in R2(config-line)# exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)# line VTY 0 4 R2(config-line)# access-class ADMIN-MGT in R2(config-line)# end
Verificar que la ACL funcione como se espera	Figura 11

Figura 17 - Verificación ACL ADMIN-MGT



Fuente: Elaboración propia Packet Tracer

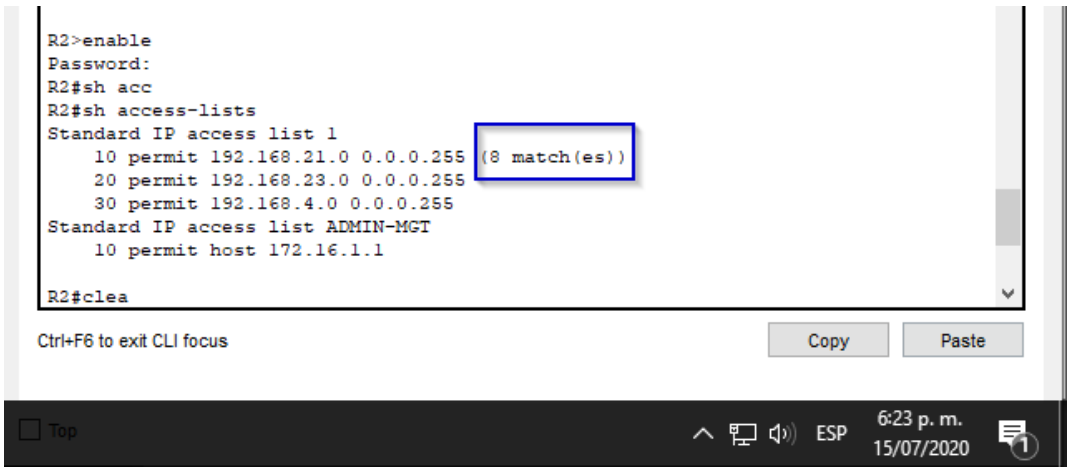
Paso 2: Comando de CLI

Desde el modo privilegiado vamos a verificar la información de las listas y el comportamiento de otros protocolos como NAT dentro de la red; para eso vamos a ejecutando los comandos descritos en las especificaciones de la Tabla 22.

Tabla 22 - Comandos CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2> enable R2# show access-list (Figura 18)
Restablecer los contadores de una lista de acceso	R2# conf t R2(config)# clear access-list counters Ver Figura 19
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2# show interface S 0/0/1 Ver Figura 20
¿Con qué comando se muestran las traducciones NAT?	R2# show ip nat translations Ver Figura 21
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2# clear ip nat translation Ver Figura 22

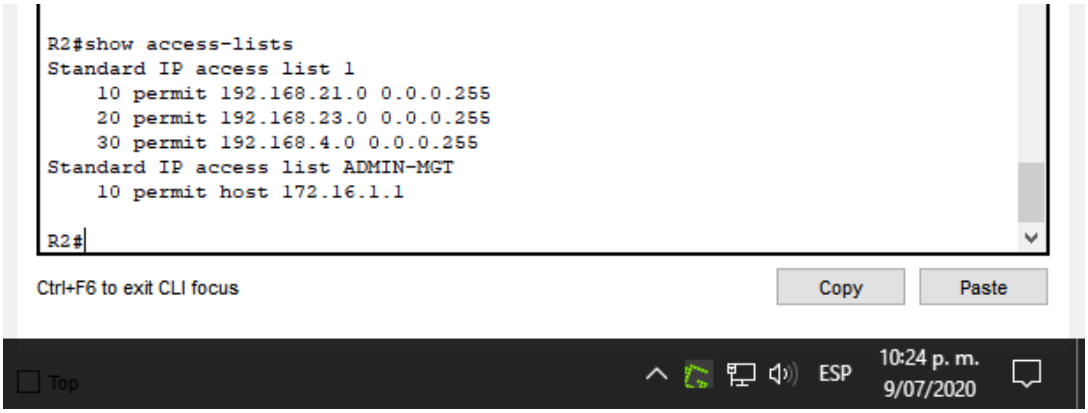
Figura 18 - Verificación access-list R2



Fuente: Elaboración propia Packet Tracer

observamos en la Figura 19 que los contadores de la lista de acceso se reinician

Figura 19 - Verificación access-list

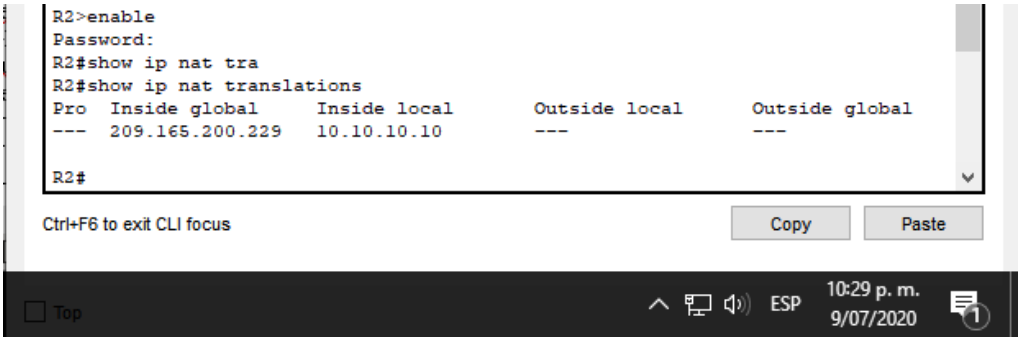


Fuente: Elaboración propia Packet Tracer

Figura 20 - Verificación ACL en Interface

Fuente: Elaboración propia Packet Tracer

Figura 21 - Verificación NAT Translation



Fuente: Elaboración propia Packet Tracer

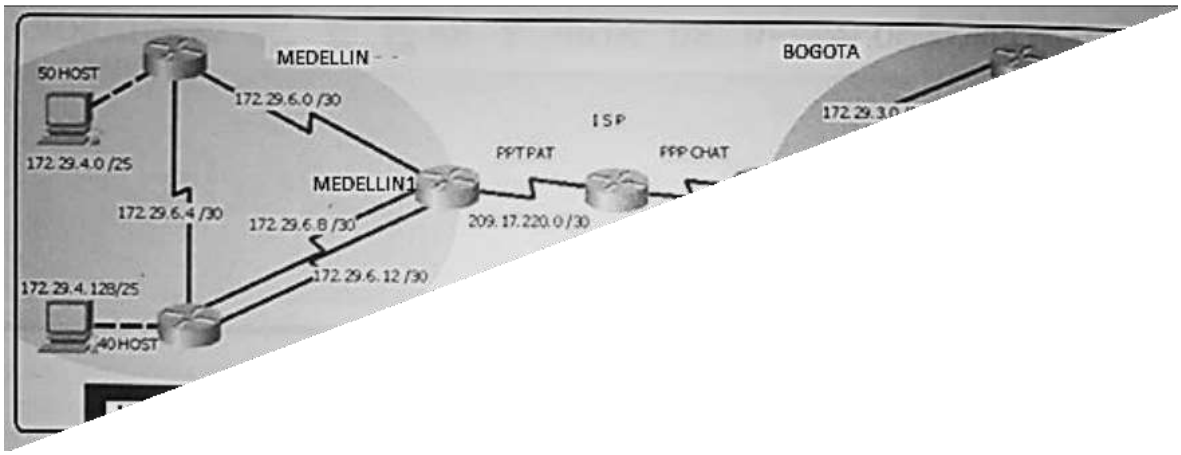
ESCENARIO 2

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

Figura 22 - 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. Configuración inicial

Trabajo Inicial

Paso 1: Configurar los parámetros básicos de los dispositivos.

Para la configuración inicial de R1 vamos a implementar algunas medidas de seguridad y optimizar el rendimiento; para implementar dichas medidas ingresamos al modo configuración global desde allí vamos a configurar un mensaje de acceso restringido para usuarios, asignar contraseñas de seguridad al acceso modo privilegiado, de consola y VTY, activar el inicio de sesión por contraseñas y por último desactivamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado nos interrumpan la entrada de comandos o visualización de información, configuramos el comando “logging synchronous” para el acceso de consola.

Para la asignación de contraseñas usamos el comando “password” que me permite asignar contraseñas en texto plano, es decir, sin utilizar algoritmos de encriptación; para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación “password-encryption”, que me encriptar todas las contraseñas almacenadas en texto plano.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado es “class” y para consola y VTY “cisco”; usamos el comando “secret” para cifrar la contraseña de exec privilegiado y el comando password (no encriptado) para los demás.

Al finalizar el procedimiento de configuración y en modo privilegiado vamos a copiar la configuración actual como de configuración de inicio usando el comando “write”.

La configuración descrita anteriormente, la vamos a aplicar en cada uno de los dispositivos de la Tabla 23.

Tabla 23 - Configuración inicial dispositivos

Dispositivo	Configuración Básica
Medellin1	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Medellin1 Medellin1(config)# enable secret class Medellin1(config)# line console 0 Medellin1(config-if)# password cisco Medellin1(config-if)# login Medellin1(config-if)# logging synchronous Medellin1(config-if)# exit Medellin1(config)# line VTY 0 4 Medellin1(config-if)# password cisco Medellin1(config-if)# login Medellin1(config-if)# exit Medellin1(config)# service password-encryption Medellin1(config)# banner motd "Se prohíbe el acceso no autorizado" Medellin1(config-if)# exit Medellin1# write
Medellin2	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Medellin2 Medellin2(config)# enable secret class Medellin2(config)# line console 0 Medellin2(config-if)# password cisco Medellin2(config-if)# login Medellin2(config-if)# logging synchronous Medellin2(config-if)# exit Medellin2(config)# line VTY 0 4 Medellin2(config-if)# password cisco Medellin2(config-if)# login Medellin2(config-if)# exit Medellin2(config)# service password-encryption

	Medellin2(config)# banner motd "Se prohíbe el acceso no autorizado" Medellin2(config-if)# exit Medellin2# write
Medellin3	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Medellin3 Medellin3(config)# enable secret class Medellin3(config)# line console 0 Medellin3(config-if)# password cisco Medellin3(config-if)# login Medellin3(config-if)# logging synchronous Medellin3(config-if)# exit Medellin3(config)# line VTY 0 4 Medellin3(config-if)# password cisco Medellin3(config-if)# login Medellin3(config-if)# exit Medellin3(config)# service password-encryption Medellin3(config)# banner motd "Se prohíbe el acceso no autorizado" Medellin3(config-if)# exit Medellin3# write
Bogota1	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Bogota1 Bogota1(config)# enable secret class Bogota1(config)# line console 0 Bogota1(config-if)# password cisco Bogota1(config-if)# login Bogota1(config-if)# logging synchronous Bogota1(config-if)# exit Bogota1(config)# line VTY 0 4 Bogota1(config-if)# password cisco Bogota1(config-if)# login Bogota1(config-if)# exit Bogota1(config)# service password-encryption

	Bogota1(config)# banner motd "Se prohíbe el acceso no autorizado" Bogota1(config-if)# exit Bogota1# write
Bogota2	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Bogota2 Bogota2(config)# enable secret class Bogota2(config)# line console 0 Bogota2(config-if)# password cisco Bogota2(config-if)# login Bogota2(config-if)# logging synchronous Bogota2(config-if)# exit Bogota2(config)# line VTY 0 4 Bogota2(config-if)# password cisco Bogota2(config-if)# login Bogota2(config-if)# exit Bogota2(config)# service password-encryption Bogota2(config)# banner motd "Se prohíbe el acceso no autorizado" Bogota2(config-if)# exit Bogota2# write
Bogota3	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Bogota3 Bogota3(config)# enable secret class Bogota3(config)# line console 0 Bogota3(config-if)# password cisco Bogota3(config-if)# login Bogota3(config-if)# logging synchronous Bogota3(config-if)# exit Bogota3(config)# line VTY 0 4 Bogota3(config-if)# password cisco Bogota3(config-if)# login Bogota3(config-if)# exit Bogota3(config)# service password-encryption

	Bogota3(config)# banner motd "Se prohíbe el acceso no autorizado" Bogota3(config-if)# exit Bogota3# write
ISP	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname ISP ISP(config)# enable secret class ISP(config)# line console 0 ISP(config-if)# password cisco ISP(config-if)# login ISP(config-if)# logging synchronous ISP(config-if)# exit ISP(config)# line VTY 0 4 ISP(config-if)# password cisco ISP(config-if)# login ISP(config-if)# exit ISP(config)# service password-encryption ISP(config)# banner motd "Se prohíbe el acceso no autorizado" ISP(config-if)# exit ISP# write

Paso 2: Conexión física de topología de red

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

Tabla 24 - Tabla de enrutamiento Escenario 2

Dispositivo	Interfaz	Conexión a	Dirección IP	Máscara	Gateway
Medellin1	S0/0/0	ISP	209.17.220.2	255.255.255.252	N.A
	S0/0/1	Medellin2	172.29.6.1	255.255.255.252	N.A
	S0/1/0	Medellin3	172.29.6.13	255.255.255.252	N/A
	S0/1/1	Medellin3	172.16.6.9	255.255.255.252	N.A
Medellin2	S0/0/0	Medellin1	172.29.6.2	255.255.255.252	N.A

	S0/0/1	Medellin3	172.29.6.5	255.255.255.252	N.A
	G0/0	Medellin-LAN1	172.29.4.1	255.255.255.128	N.A
Medellin3	S0/0/0	Medellin1	172.16.0.14	255.255.255.252	N.A
	S0/0/1	Medellin1	172.29.6.10	255.255.255.252	N.A
	S0/1/0	Medellin2	172.29.6.6	255.255.255.252	N.A
	G0/0	Medellin-LAN2	172.29.4.129	255.255.255.128	N.A
Bogota1	S0/0/0	ISP	209.17.220.6	255.255.255.252	N.A
	S0/1/0	Bogota2	172.29.3.1	255.255.255.252	N.A
	S0/1/1	Bogota2	172.29.3.5	255.255.255.252	N.A
	S0/0/1	Bogota3	172.29.3.9	255.255.255.252	N.A
Bogota2	S0/0/0	Bogota1	172.29.3.2	255.255.255.252	N.A
	S0/0/1	Bogota1	172.29.3.6	255.255.255.252	N.A
	S0/1/0	Bogota3	172.29.3.13	255.255.255.252	N.A
	G0/0	Bogota-LAN1	172.29.0.1	255.255.255.0	N.A
Bogota3	S0/0/0	Bogota1	172.29.3.10	255.255.255.252	N.A
	S0/0/1	Bogota2	172.29.3.14	255.255.255.252	N.A
	G0/0	Bogota-LAN2	172.29.1.1	255.255.255.0	N.A
ISP	S0/0/0	Medellin1	209.17.220.1	255.255.255.252	N.A
	S0/0/1	Bogota1	209.17.220.5	255.255.255.252	N.A
PC-Medellin-LAN1	Fa0	Medellin2	DHCP	255.255.255.128	172.29.4.1

PC-Medellin-LAN2	Fa0	Medellin3	DHCP	255.255.255.128	172.29.4.129
PC-Bogota-LAN1	Fa0	Bogota2	DHCP	255.255.255.0	172.29.0.1
PC-Bogota-LAN2	Fa0	Bogota3	DHCP	255.255.255.0	172.29.1.1

Paso 3: Configuración de direccionamiento IP

Basado en la información de la Tabla 24 vamos a configurar las interfaces de cada dispositivo y finalizamos con el comando “write” utilizado para sobrescribir la configuración inicial

Tabla 25 - Configuración direccionamiento IP

Dispositivo	Configuración Direccionamiento IP
Medellin1	Medellin1> enable Medellin1#conf terminal Medellin1(config)#int S 0/0/0 Medellin1(config-if)# description Conexion a ISP Medellin1(config-if)# ip address 209.17.220.2 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# exit Medellin1(config)#int S 0/1/0 Medellin1(config-if)# description Conexion a Medellin3 Medellin1(config-if)# ip address 172.29.6.13 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# exit Medellin1(config)#int S 0/1/1 Medellin1(config-if)# description Conexion a Medellin3

	Medellin1(config-if)# ip address 172.29.6.9 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# exit Medellin1(config)#int S 0/0/1 Medellin1(config-if)# description Conexion a Medellin2 Medellin1(config-if)# ip address 172.29.6.1 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# end Medellin1#write
Medellin2	Medellin2> enable Medellin2#conf terminal Medellin2(config)#int S 0/0/0 Medellin2(config-if)# description Conexion a Medellin1 Medellin2(config-if)# ip address 172.29.6.2 255.255.255.252 Medellin2(config-if)# no shutdown Medellin2(config-if)# exit Medellin2(config)#int S 0/0/1 Medellin2(config-if)# description Conexion a Medellin3 Medellin2(config-if)# ip address 172.29.6.5 255.255.255.252 Medellin2(config-if)# clock rate 2000000 Medellin2(config-if)# no shutdown Medellin2(config-if)# exit Medellin2(config)#int G 0/0 Medellin2(config-if)# description Conexion LAN a PC-Medellin-LAN1 Medellin2(config-if)# ip address 172.29.4.1 255.255.255.128 Medellin2(config-if)# no shutdown Medellin2(config-if)# end Medellin2#write Medellin2#write
Medellin3	Medellin3> enable Medellin3#conf terminal Medellin3(config)#int S 0/0/0 Medellin3(config-if)# description Conexion a Medellin1 Medellin3(config-if)# ip address 172.29.6.14 255.255.255.252

	Medellin3(config-if)# no shutdown Medellin3(config-if)# exit Medellin3(config)#int S 0/0/1 Medellin3(config-if)# description Conexion a Medellin1 Medellin3(config-if)# ip address 172.29.6.10 255.255.255.252 Medellin3(config-if)# no shutdown Medellin3(config-if)# exit Medellin3(config)#int S 0/1/0 Medellin3(config-if)# description Conexion a Medellin2 Medellin3(config-if)# ip address 172.29.6.6 255.255.255.252 Medellin3(config-if)# no shutdown Medellin3(config-if)# exit Medellin3(config)#int G 0/0 Medellin3(config-if)# description Conexion LAN a PC-Medellin_LAN2 Medellin3(config-if)# ip address 172.29.4.129 255.255.255.128 Medellin3(config-if)# no shutdown Medellin3(config-if)# end Medellin3#write
Bogota1	Bogota1> enable Bogota1#conf terminal Bogota1(config)#int S 0/0/0 Bogota1(config-if)# description Conexion a ISP Bogota1(config-if)# ip address 209.17.220.6 255.255.255.252 Bogota1(config-if)# no shutdown Bogota1(config-if)# exit Bogota1(config)#int S 0/1/0 Bogota1(config-if)# description Conexion a Bogota2 Bogota1(config-if)# ip address 172.29.3.1 255.255.255.252 Bogota1(config-if)# clock rate 2000000 Bogota1(config-if)# no shutdown Bogota1(config-if)# exit Bogota1(config)#int S 0/1/1 Bogota1(config-if)# description Conexion a Bogota2 Bogota1(config-if)# ip address 172.29.3.5 255.255.255.252 Bogota1(config-if)# clock rate 2000000 Bogota1(config-if)# no shutdown

	Bogota1(config-if)# exit Bogota1(config)#int S 0/0/1 Bogota1(config-if)# description Conexion a Bogota3 Bogota1(config-if)# ip address 172.29.3.9 255.255.255.252 Bogota1(config-if)# clock rate 2000000 Bogota1(config-if)# no shutdown Bogota1(config-if)# end Bogota1#write Bogota1#write
Bogota2	Bogota2> enable Bogota2#conf terminal Bogota2(config)#int S 0/0/0 Bogota2(config-if)# description Conexion a Bogota1 Bogota2(config-if)# ip address 172.29.3.2 255.255.255.252 Bogota2(config-if)# no shutdown Bogota2(config-if)# exit Bogota2(config)#int S 0/0/1 Bogota2(config-if)# description Conexion a Bogota1 Bogota2(config-if)# ip address 172.29.3.6 255.255.255.252 Bogota2(config-if)# no shutdown Bogota2(config-if)# exit Bogota2(config)#int S 0/1/0 Bogota2(config-if)# description Conexion a Bogota3 Bogota2(config-if)# ip address 172.29.3.13 255.255.255.252 Bogota2(config-if)# clock rate 2000000 Bogota2(config-if)# no shutdown Bogota2(config-if)# exit Bogota2(config)#int G 0/0 Bogota2(config-if)# description Conexion LAN A PC-Bogota-LAN1 Bogota2(config-if)# ip address 172.29.0.1 255.255.255.0 Bogota2(config-if)# no shutdown Bogota2(config-if)# end Bogota2#write
Bogota3	Bogota3> enable Bogota3#conf terminal Bogota3(config)#int S 0/0/0

	Bogota3(config-if)# description Conexion a Bogota1 Bogota3(config-if)# ip address 172.29.3.10 255.255.255.252 Bogota3(config-if)# no shutdown Bogota3(config-if)# exit Bogota3(config)#int S 0/0/1 Bogota3(config-if)# description Conexion a Bogota2 Bogota3(config-if)# ip address 172.29.3.14 255.255.255.252 Bogota3(config-if)# no shutdown Bogota3(config-if)# exit Bogota3(config)#int G 0/0 Bogota3(config-if)# description Conexion LAN a PC_Bogota-LAN2 Bogota3(config-if)# ip address 172.29.1.1 255.255.255.0 Bogota3(config-if)# no shutdown Bogota3(config-if)# end Bogota3# write
ISP	ISP# conf terminal ISP(config)# int S 0/0/0 ISP(config-if)# description Conexion a Medellin1 ISP(config-if)# ip address 209.17.220.1 255.255.255.252 ISP(config-if)# no shutdown ISP(config-if)# exit ISP(config)# int S 0/0/1 ISP(config-if)# description Conexion a Bogota1 ISP(config-if)# ip address 209.17.220.5 255.255.255.252 ISP(config-if)# clock rate 2000000 ISP(config-if)# no shutdown ISP(config-if)# end ISP# write

Parte 1: Configuración del enrutamiento

Paso 1: Configuración de OSPF

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

Tabla 26 - Configuración de OSFP

Dispositivo	Configuración OSPF en los Routers
Medellin1	Medellin1> enable Medellin1#conf terminal 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 area 0 Medellin1(config-router)# network 172.29.6.8 0.0.0.3 area 0 Medellin1(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medellin1(config-router)# default-information originate Medellin1(config-router)# end Medellin1# write
Medellin2	Medellin2> enable Medellin2#conf terminal Medellin2(config)#router ospf 1 Medellin2(config-router)# router-id 2.2.2.2 Medellin2(config-router)# network 172.29.6.0 0.0.0.3 area 0 Medellin2(config-router)# network 172.29.6.4 0.0.0.3 area 0 Medellin2(config-router)# network 172.29.4.0 0.0.0.127 area 0 Medellin2(config-router)# end Medellin2#write
Medellin3	Medellin3> enable Medellin3#conf terminal Medellin3(config)#router ospf 1 Medellin3(config-router)# router-id 3.3.3.3 Medellin3(config-router)# network 172.29.6.4 0.0.0.3 area 0 Medellin3(config-router)# network 172.29.6.8 0.0.0.3 area 0 Medellin3(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medellin3(config-router)# network 172.29.4.128 0.0.0.127 area 0 Medellin3(config-router)# end

	Medellin3# write
Bogota1	Bogota1> enable Bogota1# conf terminal 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 area 1 Bogota1(config-router)# network 172.29.3.4 0.0.0.3 area 1 Bogota1(config-router)# network 172.29.3.8 0.0.0.3 area 1 Bogota1(config-router)# default-information originate Bogota1(config-router)# end Bogota1# write
Bogota2	Bogota2> enable Bogota2#conf terminal Bogota2(config)# router ospf 1 Bogota2(config-router)# router-id 5.5.5.5 Bogota2(config-router)# network 172.29.3.0 0.0.0.3 area 1 Bogota2(config-router)# network 172.29.3.4 0.0.0.3 area 1 Bogota2(config-router)# network 172.29.3.8 0.0.0.3 area 1 Bogota2(config-router)# network 172.29.0.0 0.0.0.255 area 1 Bogota2(config-router)# end Bogota2#write
Bogota3	Bogota3> enable Bogota3# conf terminal Bogota3(config)# router ospf 1 Bogota3(config-router)# router-id 6.6.6.6 Bogota3(config-router)# network 172.29.3.4 0.0.0.3 area 1 Bogota3(config-router)# network 172.29.3.8 0.0.0.3 area 1 Bogota3(config-router)# network 172.29.1.0 0.0.0.255 area 1 Bogota3(config-router)# end Bogota3# write

Paso 2: Configuración ruta distribuida en OSPF

Los Routers Medellin1 y Bogota1 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.

Tabla 27 - Configuración de ruta distribuible OSPF

Dispositivo	Configuración Ruta Distribuida en OSPF
Medellin1	Medellin1# conf terminal 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)# end Medellin1# write
Bogota1	Bogota1# conf terminal 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)# end Bogota1# write

Paso 3: Configurar ruta Sumarizada ISP

El Router ISP debe tener una ruta estática dirigida hacia cada red interna de Medellin1 y Bogota1 para el caso se sumarizan las subredes de cada uno.

Tabla 28 - Ruta Sumarizada ISP

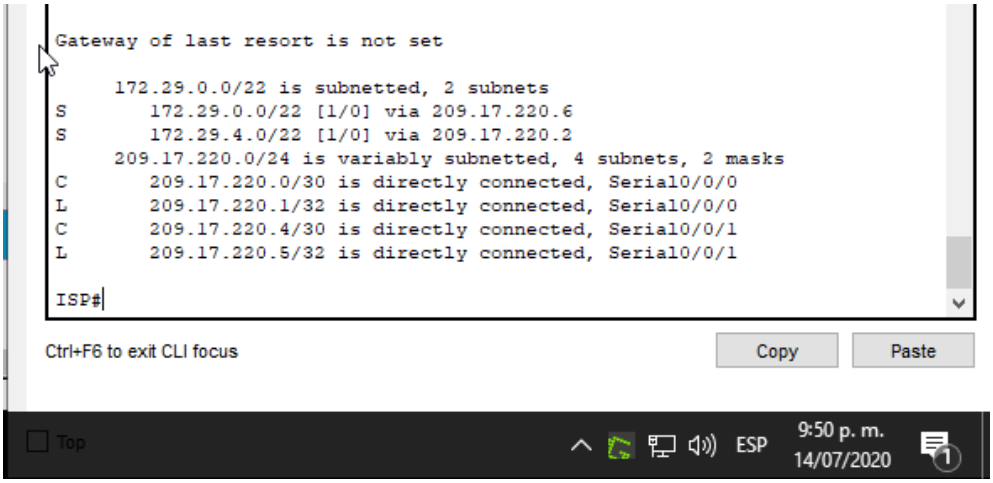
Dispositivo	Configuración Rutas Estáticas Sumarizada a Sedes
ISP	ISP# conf terminal ISP(config)# ip route 172.29.4.0 255.255.252.0 209.17.220.2 ISP(config)# ip route 172.29.0.0 255.255.252.0 209.17.220.6 ISP(config)# end ISP# write

Parte 2: Tabla de Enrutamiento.

Paso 1: Verificar tablas de enrutamiento

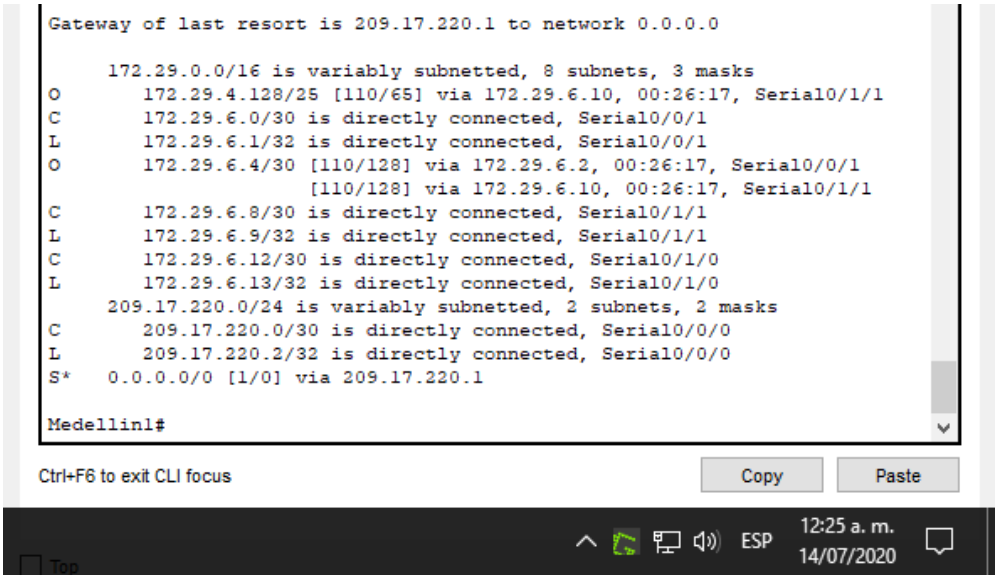
Para verificar la tabla de enrutamiento de cada uno de los Routers vamos a usar el comando “show ip route” en cada uno para comprobar las redes y sus rutas.

Figura 23 - Tabla de enrutamiento ISP



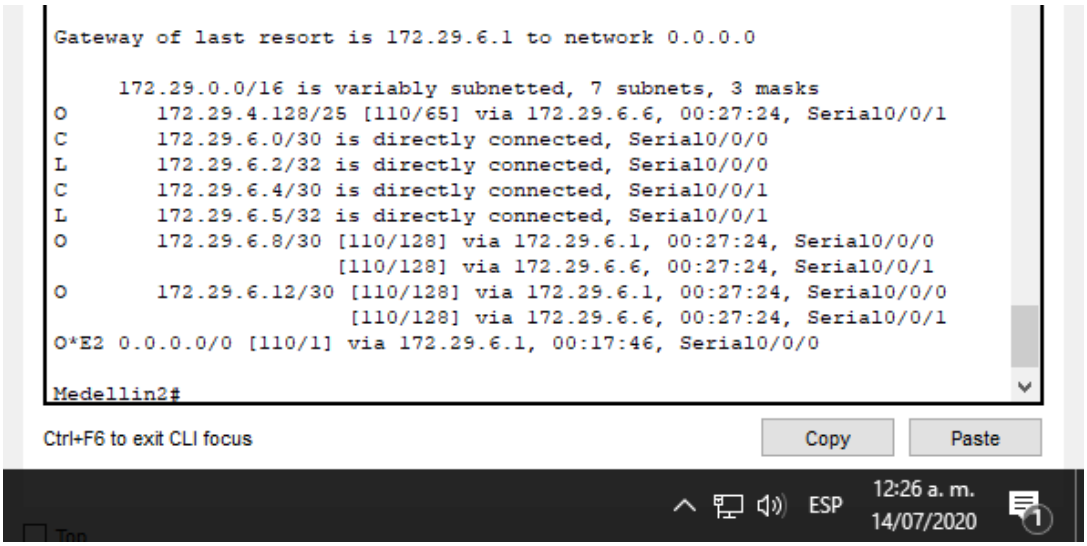
Fuente: Elaboración propia Packet Tracer

Figura 24 - Tabla de enrutamiento Medellin1



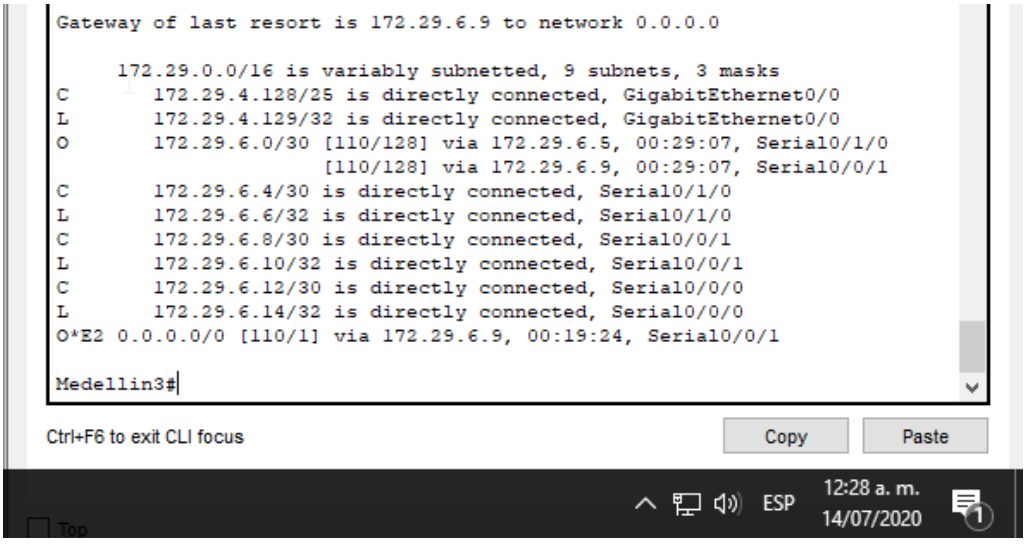
Fuente: Elaboración propia Packet Tracer

Figura 25 - Tabla de enrutamiento Medellin2



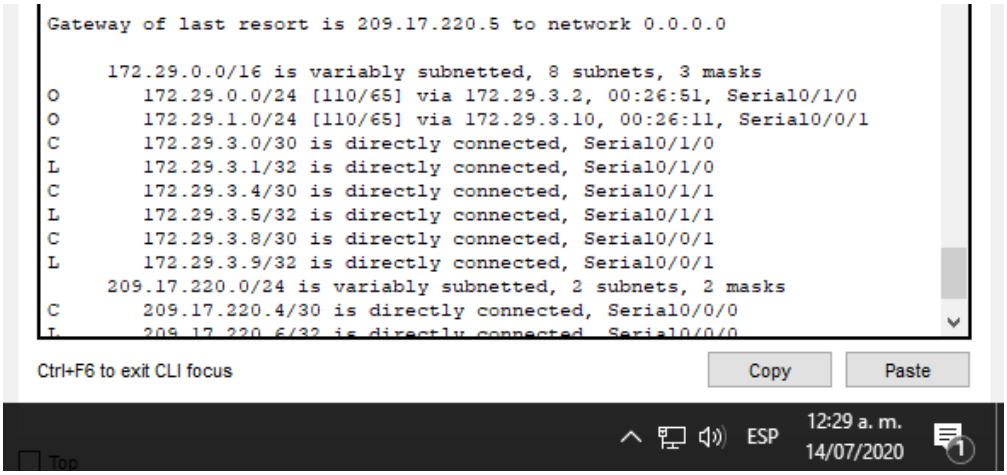
Fuente: Elaboración propia Packet Tracer

Figura 26 - Tabla de enrutamiento Medellin3



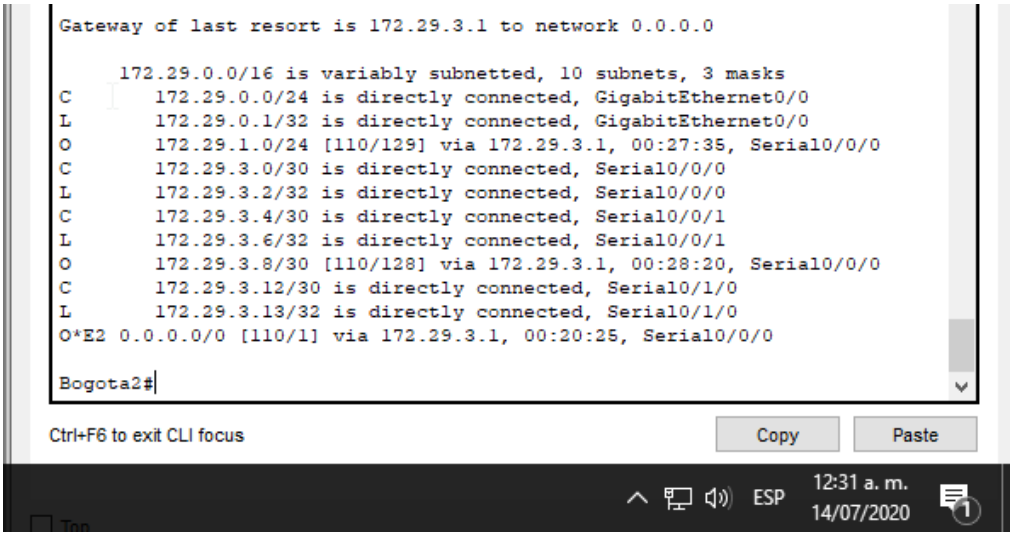
Fuente: Elaboración propia Packet Tracer

Figura 27 - Tabla de enrutamiento Bogota1



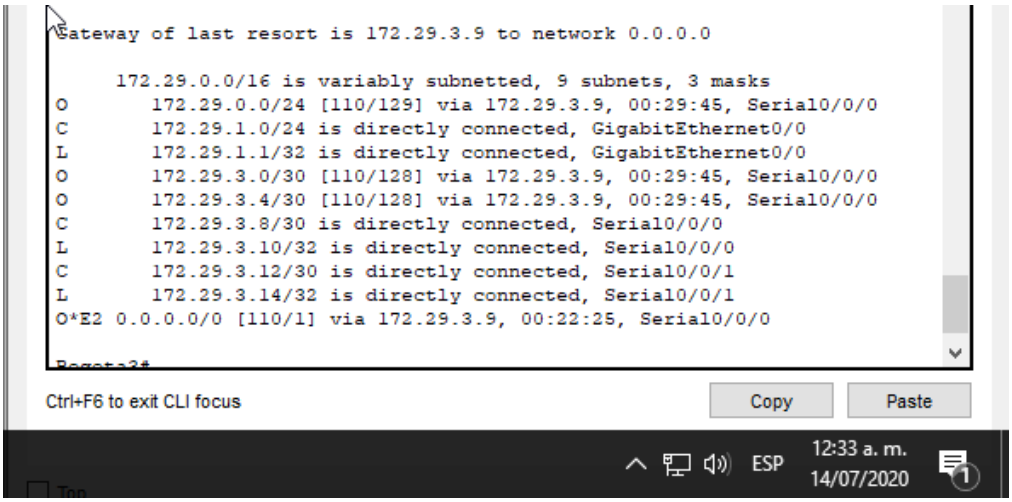
Fuente: Elaboración propia Packet Tracer

Figura 28 - Tabla de enrutamiento Bogota2



Fuente: Elaboración propia Packet Tracer

Figura 29 - Tabla de enrutamiento Bogota3

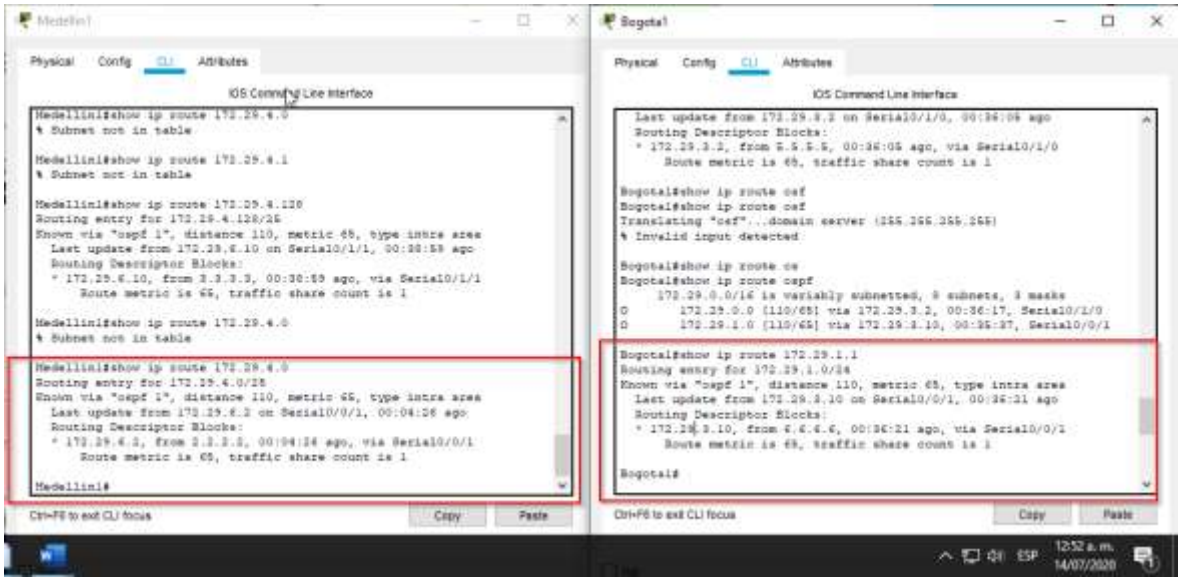


Fuente: Elaboración propia Packet Tracer

Paso 2: Verificar balanceo de carga

Verificamos el balanceo de carga de los Routers Medellin1 y Bogota1; usando las redes LAN1 de cada area como destino.

Figura 30 – Verificación de balanceo de carga Medellin1 - Bogota1

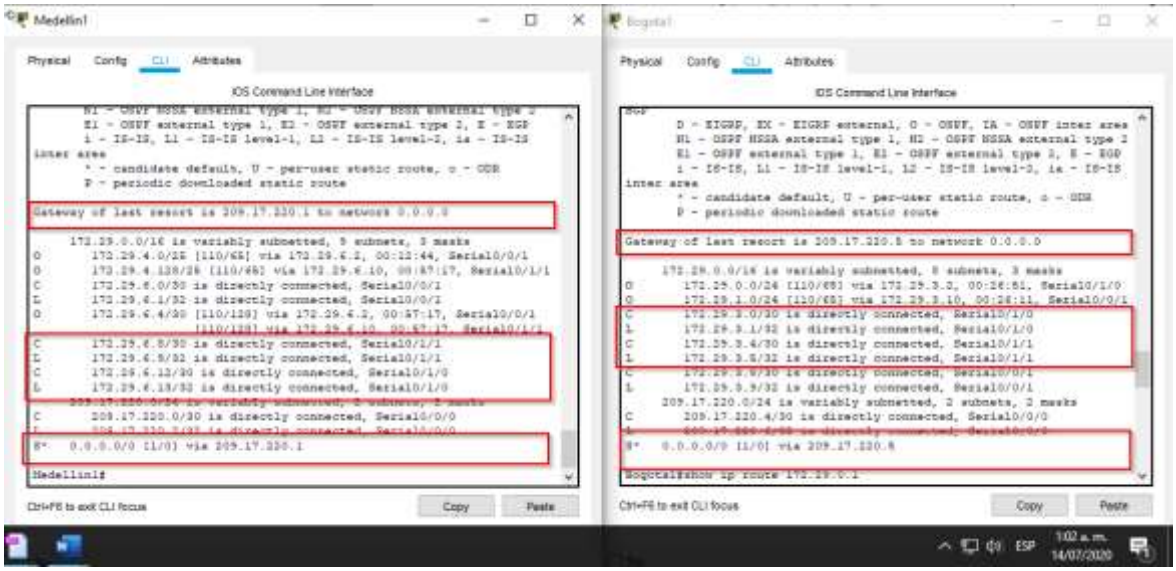


Fuente: Elaboración propia Packet Tracer

Paso 3: Ruta por defecto OSPF

Observamos en los Routers Medellin1 y Bogota1 una similitud por su ubicación, por tener un enlace doble de conexión hacia otro router y por la ruta por defecto manejada

Figura 31 – Verificación ruta por defecto Medellin1 y Bogota1

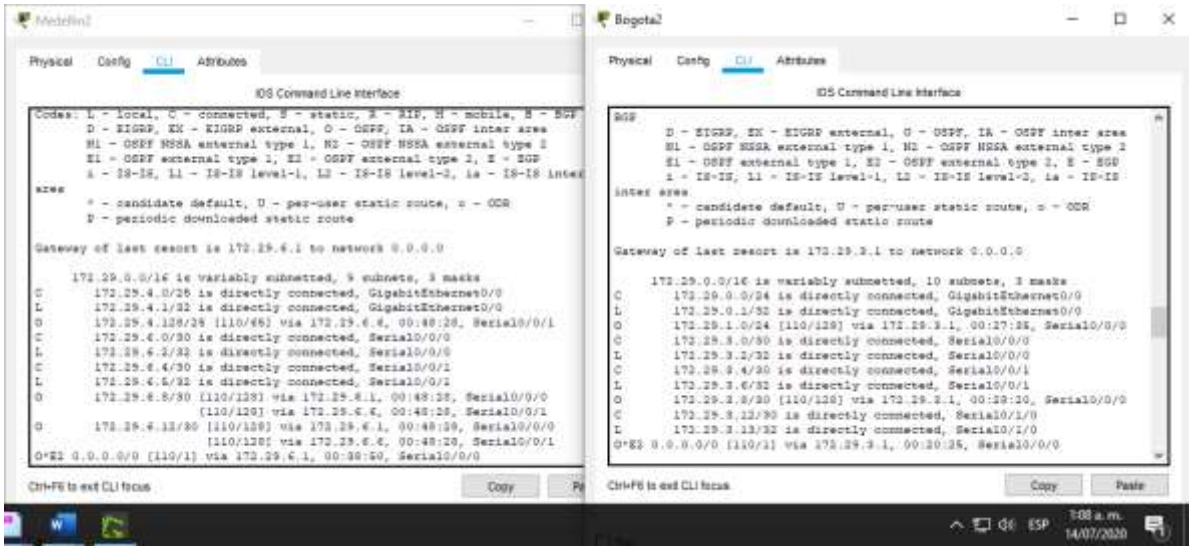


Fuente: Elaboración propia Packet Tracer

Paso 4: Verificación rutas directas OSPF

En la Figura 32. observamos los Routers Bogota2 y Medellin2 que al igual que los Routers Medellin1 y Bogota1, estos reciben las actualizaciones de OSPF y muestra las presentadas directamente.

Figura 32 - Verificación rutas directas y OSPF Medellin2 y Bogota2



Fuente: Elaboración propia Packet Tracer

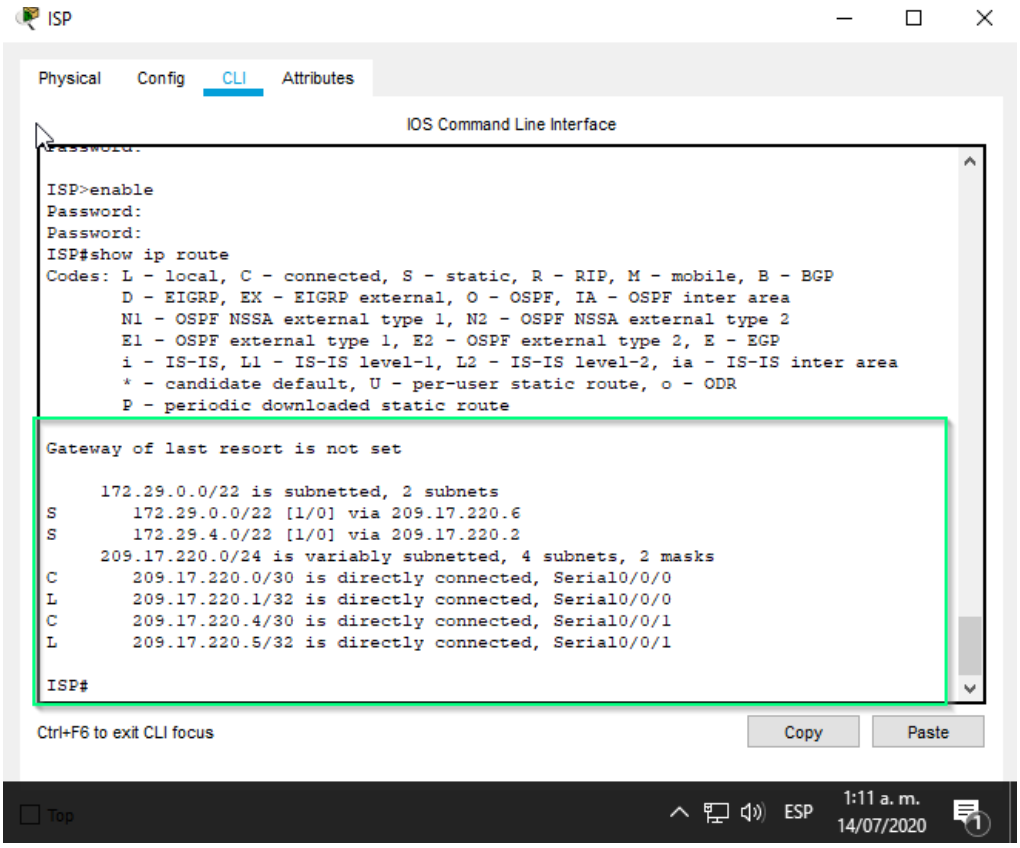
Paso 5: Rutas Redundantes

Las tablas de los Routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto. Figuras 25, 26, 28 y 29

Paso 6: Verificar tabla de enrutamiento ISP

Observamos que el Router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas ya que en él, no se debe, ni se ha configurado OSPF.

Figura 33 - Verificación enrutamiento ISP



Fuente: Elaboración propia Packet Tracer

Parte 3: Deshabilitar la propagación del protocolo OSPF.

Paso 1: Deshabilitar Propagación OSPF

Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, esta debe deshabilitarse en los Router que tengan conexiones hacia las LAN ejecutando el comando “passive-interface” para cada una de ellas.

Tabla 29 - Deshabilitación propagación OSPF

Dispositivo	Deshabilitación de propagación del protocolo OSPF
Medellin1	Medellin3> enable Medellin3# conf terminal Medellin3(config)# router ospf 1 Medellin3(config-router)# passive-interface S 0/0/0 Medellin3(config-router)# end Medellin3# write
Medellin2	Medellin2> enable Medellin2# conf terminal Medellin2(config)# router ospf 1 Medellin2(config-router)# passive-interface G 0/0 Medellin2(config-router)# end Medellin2# write
Medellin3	Medellin3> enable Medellin3# conf terminal Medellin3(config)# router ospf 1 Medellin3(config-router)# passive-interface G 0/0 Medellin3(config-router)# end Medellin3# write
Bogota1	Bogota1> enable Bogota1# conf terminal Bogota1(config)# router ospf 1 Bogota1(config-router)# passive-interface S 0/0/0 Bogota1(config-router)# end Bogota1# write
Bogota2	Bogota2> enable Bogota2# conf terminal Bogota2(config)# router ospf 1 Bogota2(config-router)# passive-interface G 0/0 Bogota2(config-router)# end Bogota2# write
Bogota3	Bogota3>enable

	Bogota3#conf terminal Bogota3(config)# router ospf 1 Bogota3(config-router)# passive-interface G 0/0 Bogota3(config-router)#end Bogota3# write

Parte 4: Verificación del protocolo OSPF.

Paso 1: Verificar y documentar opciones de enrutamiento

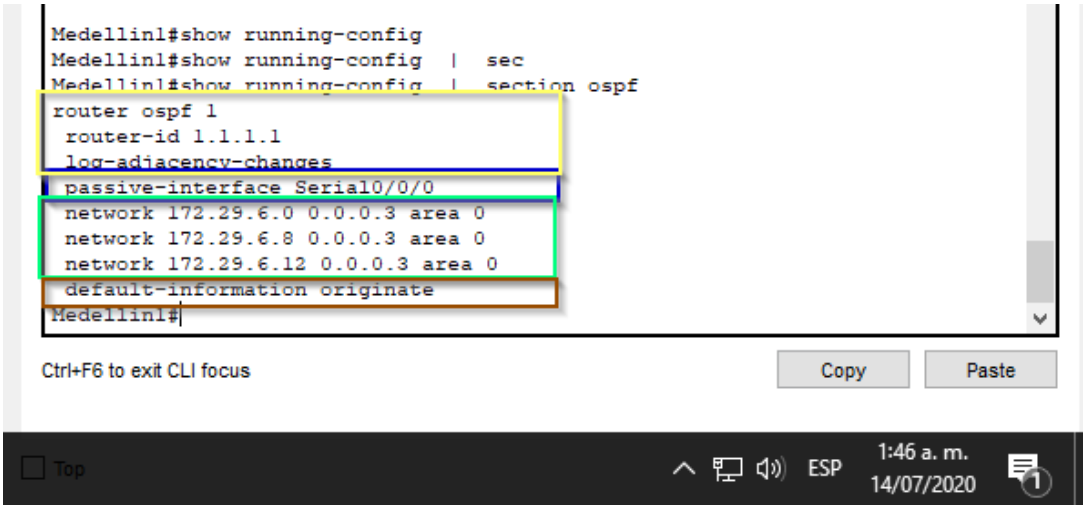
Para verificar las opciones de enrutamiento configuradas en los Routers, como el **passive interface**, la versión de OSPF y las interfaces que participan de la publicación entre otros datos vamos a ejecutar el comando “show running-config” y filtramos la sección de OSPF tal y como se muestra en la Figura 34 y 35.

Ejecutamos el comando en los routers Medellin1 (Figura 34) y encontramos información como:

En color amarillo tenemos la versión e identificación del router dentro de OSPF, en color azul encontramos las interfaces declaradas como pasivas, (es decir que no envían actualización de OSPF por esas interfaces) en color verde encontramos las redes presentadas dentro del router el cual encontramos configurada la interface S 0/0/0 (Conexión a ISP) como pasiva ya que no y en color Café (default-information originate) que lo que me dice es que el Router está distribuyendo la información de la ruta por defecto o enlace de último recurso.

Esta información es común y la vamos a encontrar en cada uno de los dispositivos en los cuales tengamos o necesitemos configurar un enrutamiento por medio del protocolo OSPF.

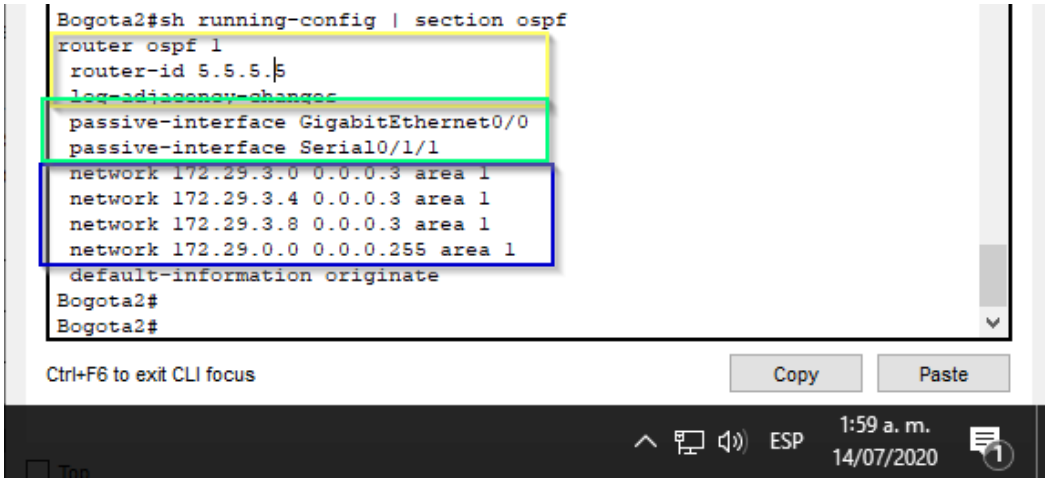
Figura 34 - Verificación información OSPF Medellin1



Fuente: Elaboración propia Packet Tracer

Observamos en en la Figura 35. la información del portocolo OSPF configurada para el Router Bogota2 y podemos ver la misma estructura.

Figura 35 - Verificación información OSPF Bogota2



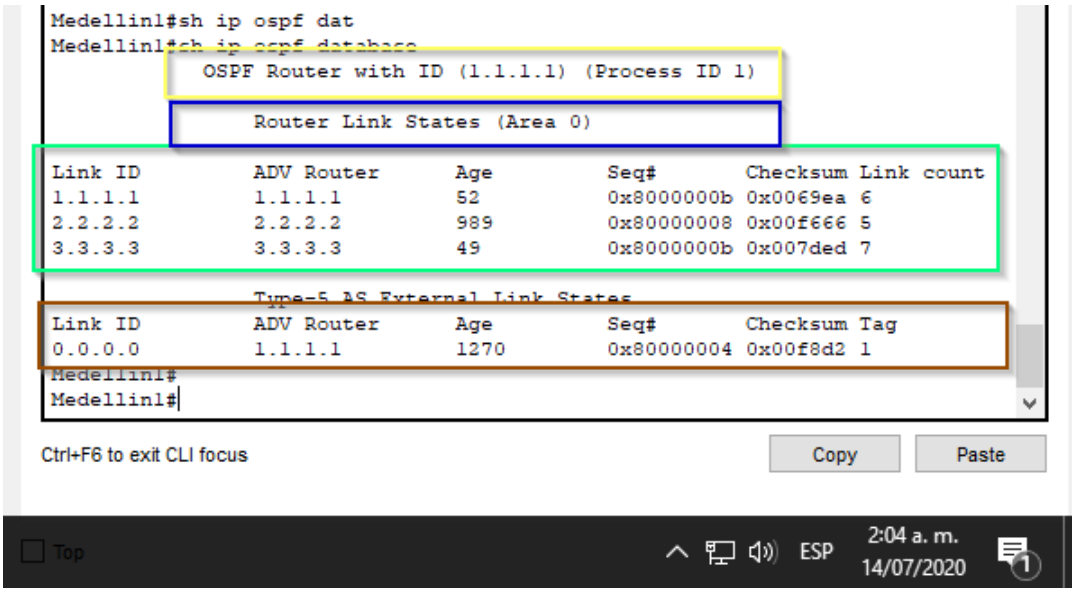
Fuente: Elaboración propia Packet Tracer

Paso 2: Verificar y documentar base de datos OSPF

En la base de datos OSPF del router Medellin1, Figura36. observamos la información almacenada de la configuración de enrutamiento.

En color amarillo tenemos la información de identificación del dispositivo y a que proceso de enrutamiento pertenece, en este caso el Router Medellin1 identificado con el ID 1.1.1.1 y que hace parte del OSPF identificado con el ID de proceso 1, en color azul encontramos el área a la cual pertenece el dispositivo, en color verde tenemos os ID de los vecinos o router conectados directamente y el tiempo de conexión y por último en color café la identificación del router perimetral.

Figura 36 - Verificación base de Datos OSFP Medellin1



Fuente: Elaboración propia Packet Tracer

Parte 5: Configurar encapsulamiento y autenticación PPP.

Paso 1: Autenticación PAT Medellin1.

Para la configuración de autenticación del enlace Medellin1 con ISP se debe crear un usuario a nivel local con clave de autenticación “cisco”, se configura el tipo de encapsulamiento de la interfaz (PPP) y definimos el tipo de autenticación como PAT. (Ver Tabla 30)

Ver Tabla 30

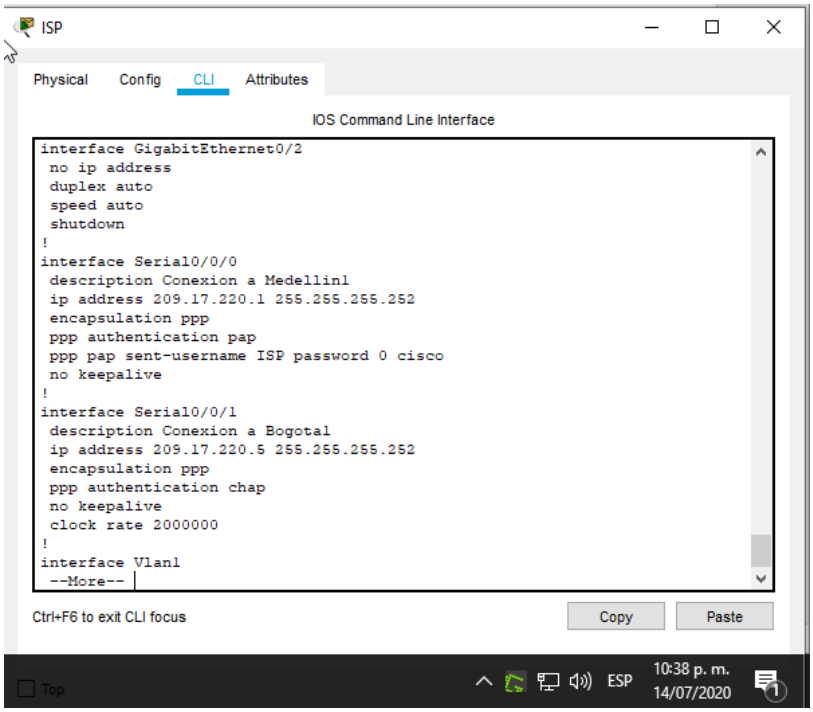
Paso 2: Autenticación CHAT Bogota1

Para la configuración de autenticación del enlace Bogota1 con ISP vamos a configurar PAP que a diferencia de PPP me permite autenticación Bidireccional. (Ver Tabla 30).

Tabla 30 - Configuración PAT Bogota1 - CHAT Medellin2

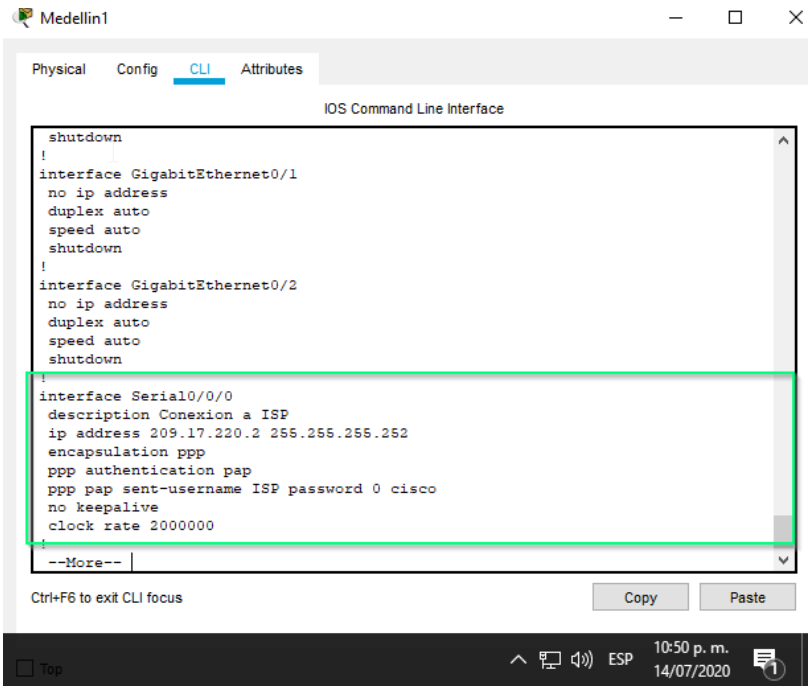
Dispositivo	Encapsulación y Autenticación PPP
Medellin1	Medellin1> enable Medellin1# conf terminal. Medellin1(config)# username ISP password cisco Medellin1(config)# interface s0/0/0 Medellin1(config-if)# encapsulation ppp Medellin1(config-if)# ppp authentication pap Medellin1(config-if)# ppp pap sent-username ISP password cisco Medellin1(config-if)# end
Bogota1	Bogota1> enable Bogota1# conf terminal Bogota1(config)# username Bogota1 password cisco Bogota1(config)# interface s0/0/0 Bogota1(config-if)# encapsulation ppp Bogota1(config-if)# ppp authentication chap Bogota1(config-if)# end
ISP	ISP# conf terminal ISP(config)# username Medellin1 password cisco ISP(config)# interface 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)# exit ISP(config)# username Bogota1 password cisco ISP(config)# interface s0/0/1 ISP(config-if)# encapsulation ppp ISP(config-if)# ppp authentication chap ISP(config-if)# end

Figura 37 - Verificación de Encapsulamiento y autenticación ISP



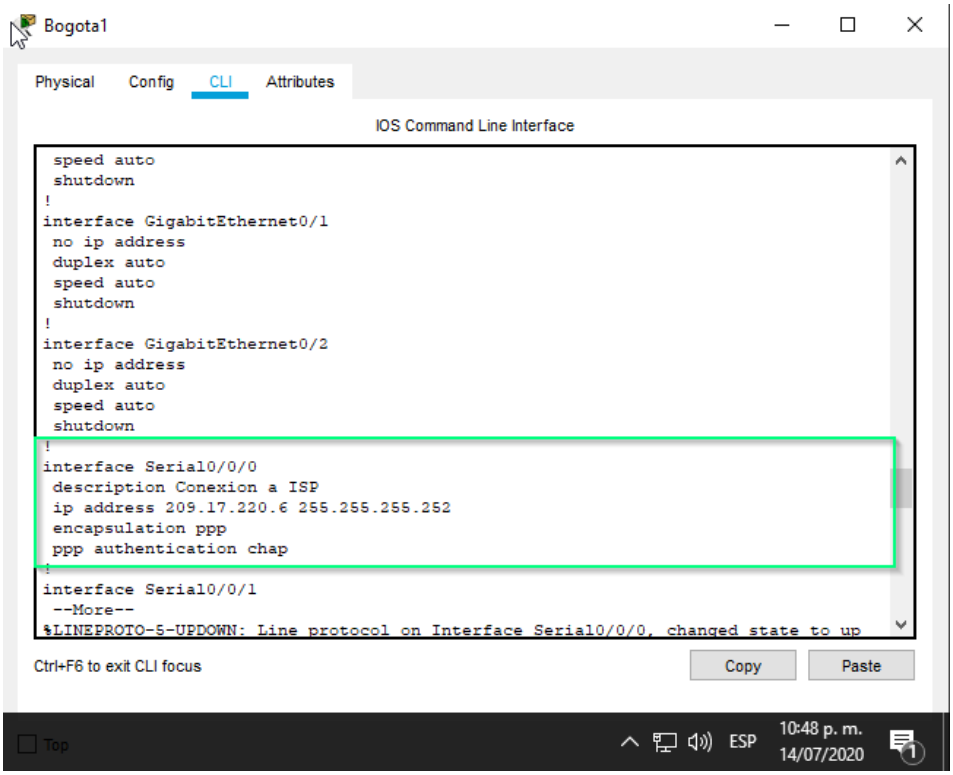
Fuente: Elaboración propia Packet Tracer

Figura 38 - Verificación autenticación Medellin1



Fuente: Elaboración propia Packet Tracer

Figura 39 - Verificación autenticación Bogota1



Fuente: Elaboración propia Packet Tracer

Parte 6: Configuración de PAT.

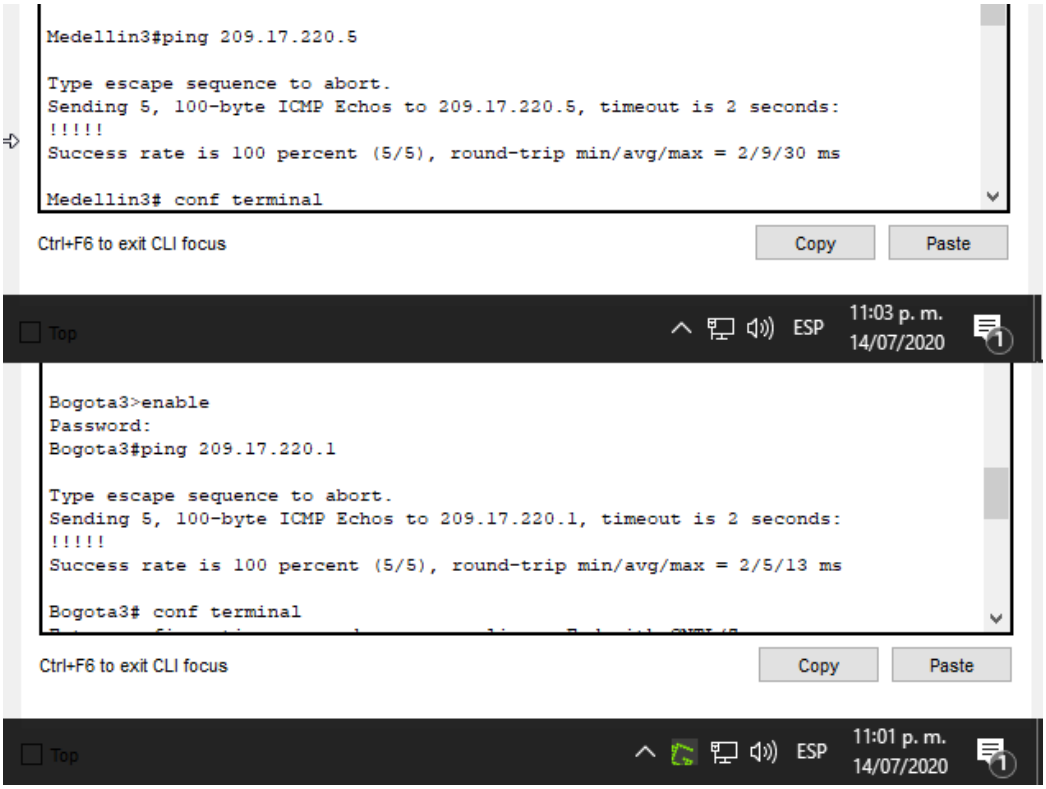
Paso 1: Verificación de conexión

En la topología, si se activa NAT en cada equipo de salida (Medellin1 y Bogota1), los Routers internos de una ciudad no podrán llegar hasta los Routers internos en el otro extremo, sólo existirá comunicación hasta los Routers Medellin1, ISP y Bogota1.

Nota: Al tener 2 áreas OSPF (0, 1) configuradas, cada una llega hasta el ISP.

En la Figura 40 podemos observar el comportamiento del ping desde Medellin3 a ISP y de Bogota3 a ISP

Figura 40 - Verificación de conexión sin NAT



Fuente: Elaboración propia Packet Tracer

Paso 2: Configuración NAT Bogota1

Después de verificar lo indicado en el paso anterior procedemos a configurar el NAT en el Router Bogota1.

para verificar que la traducción de direcciones indique las interfaces de entrada y de salida, hacemos ping y la dirección debe ser traducida automáticamente a la dirección de la interfaz serial externa del Router Bogota1, cómo diferente puerto.

Para la lista de acceso NAT configuramos la ruta 172.29.0.0 0.0.3.255

Paso 3: Configuración NAT Medellin1

Proceda a configurar el NAT en el Router Medellin1. 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 externa del Router Medellin1, cómo diferente puerto.

Para la creación de las nat en los routers frontera primero creamos una lista de control de acceso que me permita definir la red interna a la que voy a permitir acceder; paso a seguir es realizar la asignación de NAT y definir los tipos de acceso de cada una de las interfaces conectadas a los dispositivos.

Para la lista de acceso NAT configuramos la ruta Sumarizada 172.29.4.0 0.0.3.255.

Para completar la configuración descrita y solicitada en los pasos 2 y 3 vamos a utilizar los comandos descritos en la configuración de la Tabla 32.

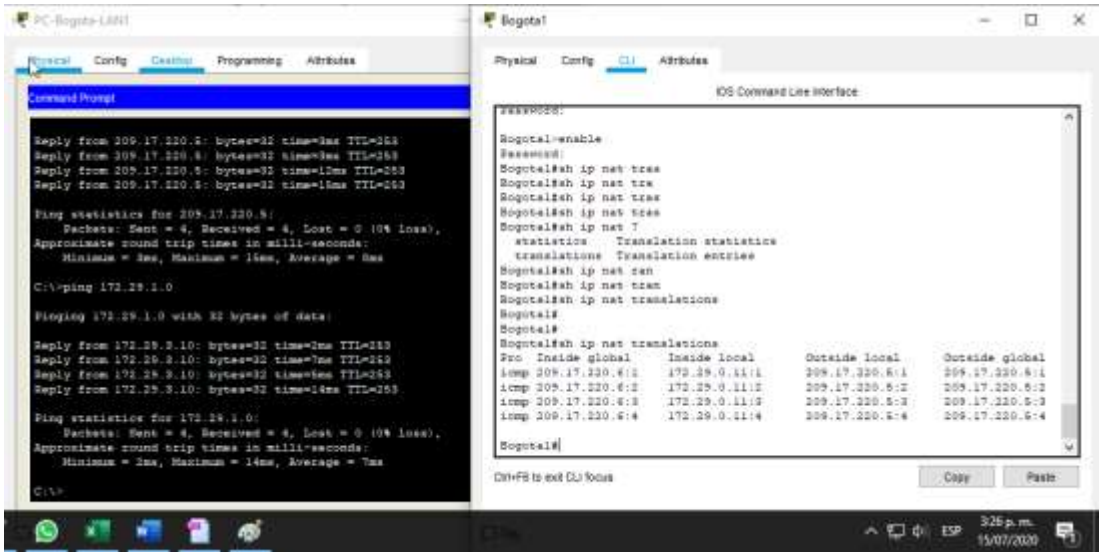
Tabla 31 - Configuración PAT

Dispositivo	Configuración PAT
Medellin1	Medellin1# conf terminal Medellin1(config)# ip access-list standar 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 S 0/0/0 overload Medellin1(config)# int S 0/0/0 Medellin1(config-if)# ip nat outside Medellin1(config-if)# exit Medellin1(config)# int S 0/1/0 Medellin1(config-if)# ip nat inside Medellin1(config-if)# exit Medellin1(config)# int S 0/1/1 Medellin1(config-if)# ip nat inside Medellin1(config-if)# exit Medellin1(config)# int S 0/0/1

	Medellin1(config-if)# ip nat inside Medellin1(config-if)# end Medellin1# write
Bogota1	Bogota1>enable Bogota1#conf terminal Bogota1(config)# ip access-list standar 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 S 0/0/0 overload Bogota1(config)# int S 0/0/0 Bogota1(config-if)# ip nat outside Bogota1(config-if)# exit Bogota1(config)# int S 0/1/0 Bogota1(config-if)# ip nat inside Bogota1(config-if)# exit Bogota1(config)# int S 0/1/1 Bogota1(config-if)# ip nat inside Bogota1(config-if)# exit Bogota1(config)# int S 0/0/1 Bogota1(config-if)# ip nat inside Bogota1(config-if)# end Bogota1# write

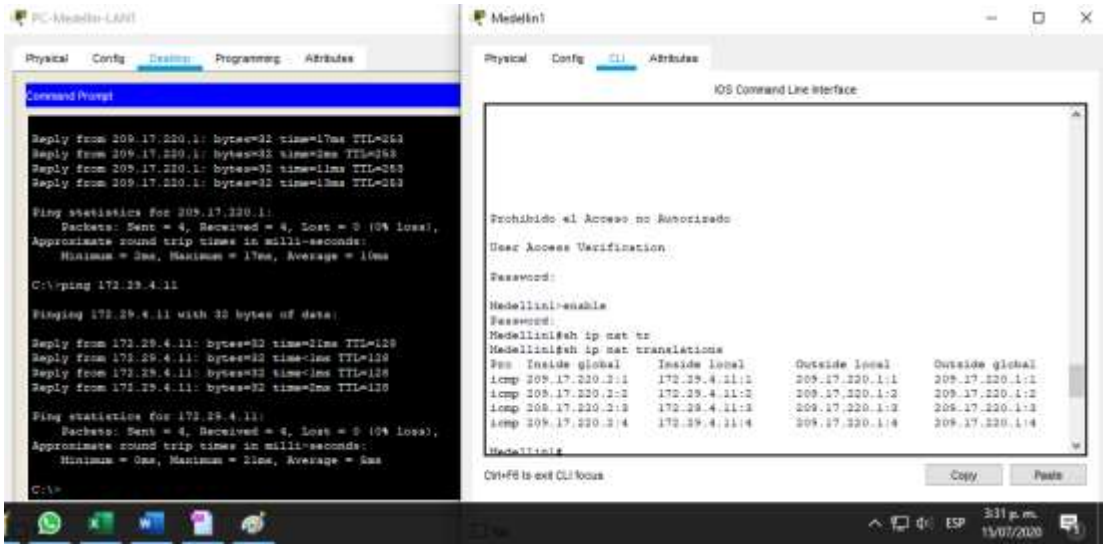
Después de configurar Medellin1 y Bogota1 podemos observar en las Figuras 41 y 42 la traducción de direcciones al enviar solicitudes de conexión desde las PC internas a ISP.

Figura 41 - Verificación NAT Bogota1



Fuente: Elaboración propia Packet Tracer

Figura 42 - Verificación NAT Medellin1



Fuente: Elaboración propia Packet Tracer

Parte 7: Configuración del servicio DHCP.

En la Tabla 31 vamos a insertar los comandos que me permiten la configuración de las configuraciones solicitadas en los pasos del 1 al 4.

Paso 1: Configurar Bogota2 como servidor DHCP

Vamos a configurar la red Bogota2 y Bogota3 donde el Router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

Paso 2: Habilitar Broadcast Bogota3

El Router Bogota3 deberá habilitar el paso de los mensajes broadcast hacia la IP del Router Bogota2; para eso usaremos el comando “helper-addres”.

Paso 3: Configurar Medellin2 como servidor DHCP

Vamos a configurar la red Medellin2 y Medellin3 donde el Router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

Paso 4: Habilitar Broadcast Medellin3

El Router Medellin3 deberá habilitar el paso de los mensajes Broadcast hacia la IP del Router Medellin2; para eso usaremos el comando “helper-addres”.

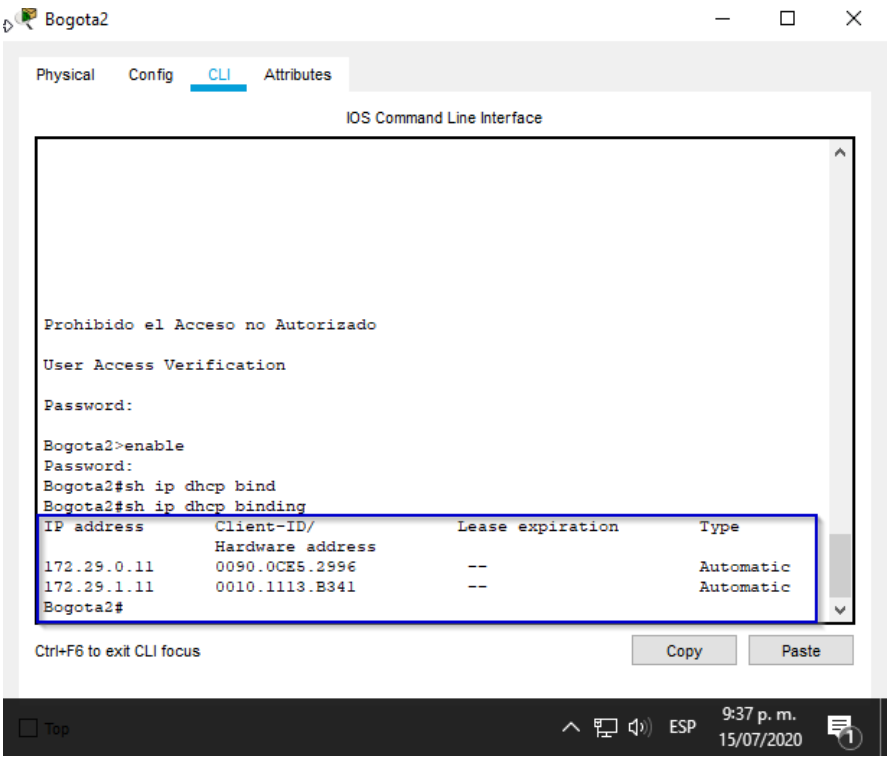
Tabla 32 - Configuración DHCP

Dispositivo	Configuración DHCP
Bogota2	Bogota2# conf terminal Bogota2(config)# ip dhcp excluded-address 172.29.0.1 172.29.0.10 Bogota2(config)# ip dhcp excluded-address 172.29.1.1 172.29.1.10 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 Bogota2(dhcp-config)# dns-server 4.4.4.4 Bogota2(dhcp-config)# domain-name lan1.Bogota.com Bogota2(dhcp-config)# exit 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)# dns-server 4.4.4.4 Bogota2(dhcp-config)# domain-name lan2.Bogota.com Bogota2(dhcp-config)# end Bogota2# write
Bogota3	Bogota3> enable Bogota3# conf terminal Bogota3(config)# int G 0/0 Bogota3(config-if)# ip helper-address 172.29.0.1 Bogota3(config-if)# end Bogota3# write
Medellin2	Medellin2> enable Medellin2# conf terminal Medellin2(config)# ip dhcp excluded-address 172.29.4.1 172.29.1.10 Medellin2(config)# ip dhcp excluded-address 172.29.4.129 172.29.4.138 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)# dns-server 4.4.4.4 Medellin2(dhcp-config)# domain-name lan1.Medellin.com Medellin2(dhcp-config)# exit Medellin2(config)# 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)# dns-server 4.4.4.4 Medellin2(dhcp-config)# domain-name lan2.Medellin.com Medellin2(dhcp-config)# end Medellin2# write
Medellin3	Medellin3> enable Medellin3# conf t Medellin3(config)# int G 0/0 Medellin3(config-if)# ip helper-address 172.29.4.1 Medellin3(config-if)# exit Medellin3(config)# write

Después de realizada la configuración vamos a verificar el estado del protocolo de direccionamiento DHCP con ayuda del comando “show ip dhcp binding”
En la Figura 43 podemos ver que hay 2 direcciones asignadas automáticamente para las PC de las LAN 1 y 2 de la red Bogota.

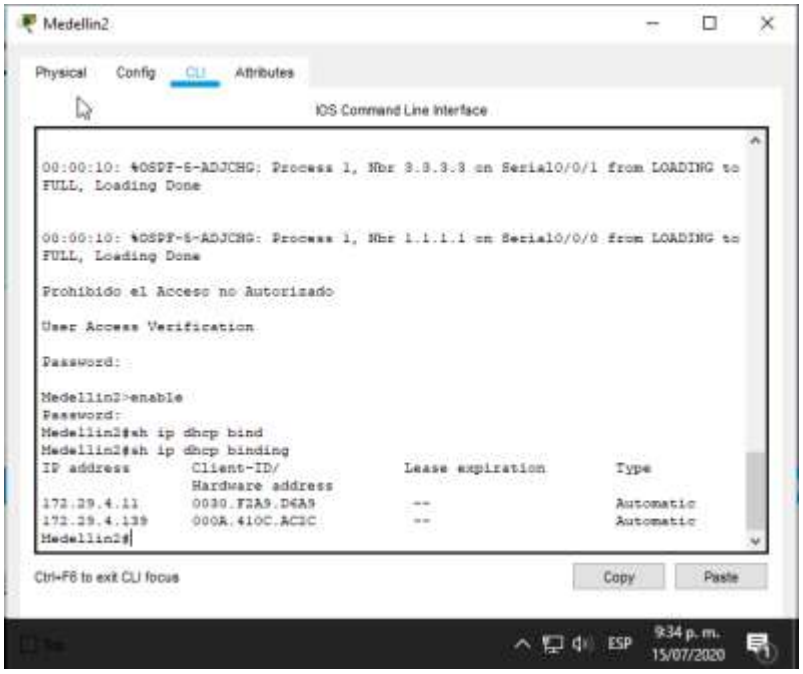
Figura 43 - Verificación estado DHCP Bogota2



Fuente: Elaboración propia Packet Tracer

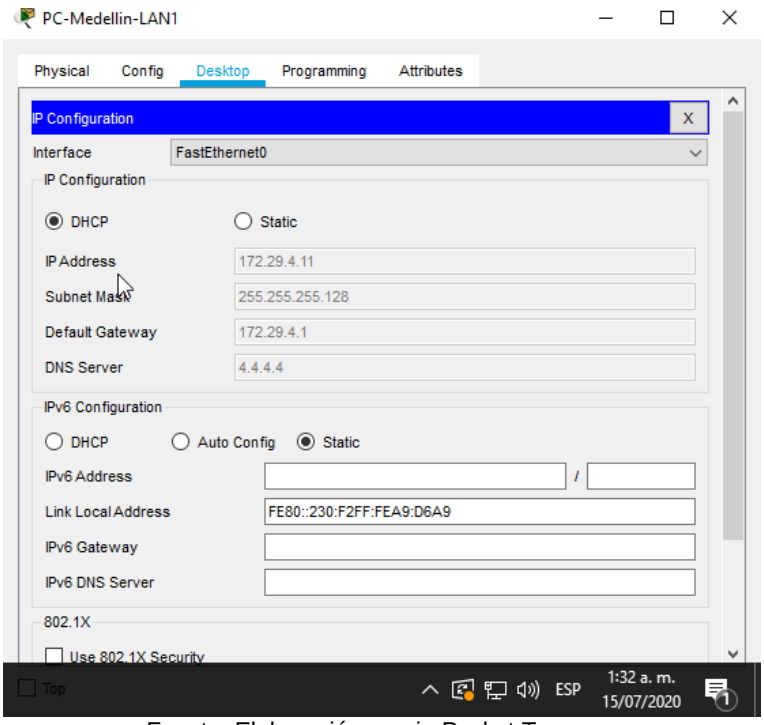
En la Figura 44 observamos al igual que en el router Bogota2, hay 2 host conectados con direccionamiento automático, que, en este caso si observamos la topología vemos que son las PC de las LAN 1 y 2 de Medellin.

Figura 44 - Verificación estado DHCP Medellin2



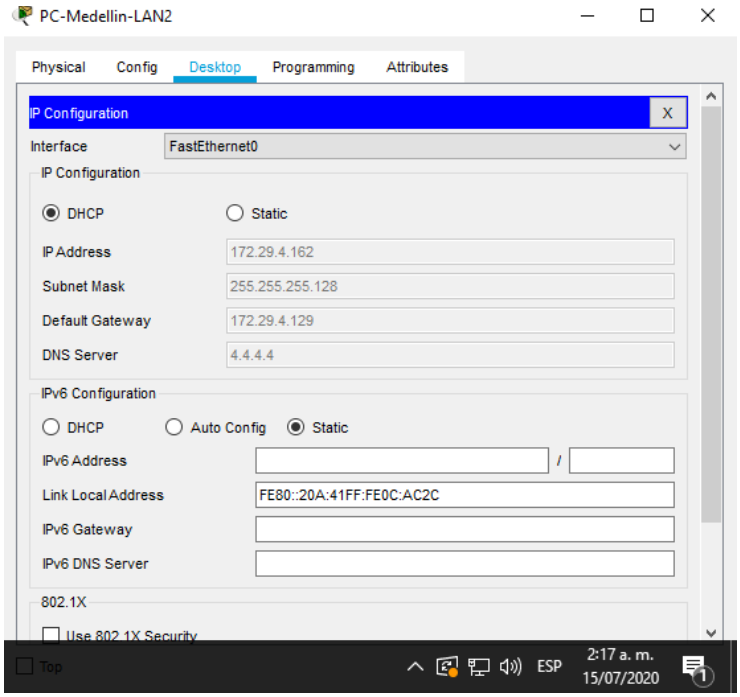
Fuente: Elaboración propia Packet Tracer

Figura 45- Verificación DHCP PC-Medellin-LAN1



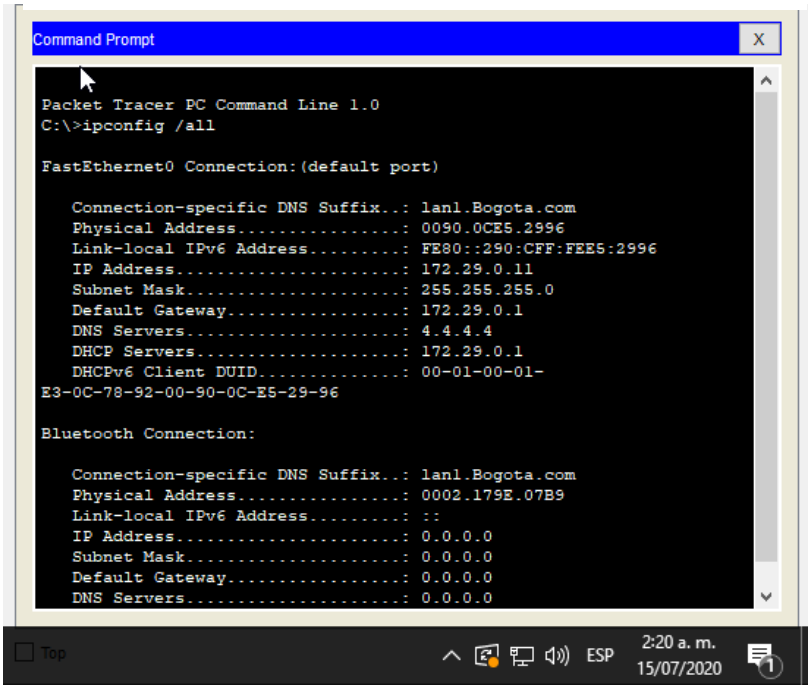
Fuente: Elaboración propia Packet Tracer

Figura 46 - Verificación DHCP PC-Medellin-LAN2



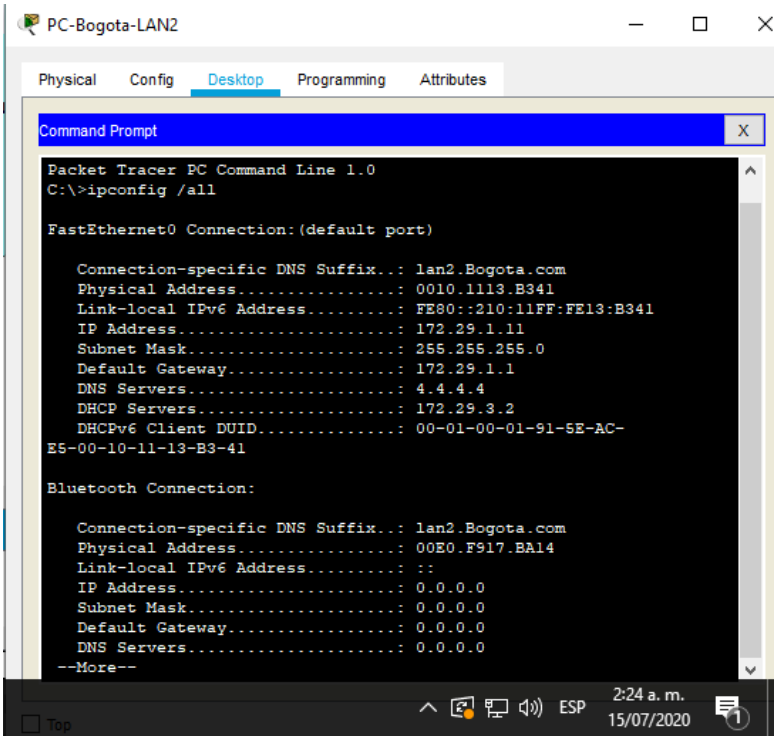
Fuente: Elaboración propia Packet Tracer

Figura 47 - Verificación DHCP PC-Bogota-LAN1



Fuente: Elaboración propia Packet Tracer

Figura 48 - Verificación DHCP PC-Bogota-LAN2



Fuente: Elaboración propia Packet Tracer

CONCLUSIONES

La asignación manual de direccionamiento IP en redes pequeñas resulta ser una tarea sencilla en redes pequeñas, pero a medida la red crece nace la necesidad de automatizar el proceso, de esta necesidad nace DHCP (Dynamic Host Configuration Protocol) protocolo de configuración dinámica de host que permite combinar la configuración manual (servidores, impresoras, routers) con la asignación dinámica (host) de configuración de direccionamiento IP para una red.

En cada escenario podemos notar la importancia de los protocolos de enrutamiento, podemos notar la diferencia entre el manejo de enrutamiento estático y dinámico, ya que a pesar de que en el presente trabajo configuramos redes pequeñas no dejaron de presentarse errores al momento de introducir o presentar redes; errores que generan mal funcionamiento o desperdicio de recursos de la red.

El conocimiento de la información que se almacena en el archivo de configuración en ejecución es de vital importancia al momento de presentar fallos de comunicación entre nodos y no tener una idea clara de por dónde empezar la búsqueda, ya que contiene toda la información de configuración del dispositivo y por medio del comando “show” me permite obtener un mapa inicial bastante claro de la función de cada dispositivo dentro de la red.

El desarrollo de escenarios como los planteados en el presente trabajo nos permiten visualizar de manera más clara el proceso de configuración de Routers o Switches

y el funcionamiento de las redes en nuestro entorno, preparándonos técnicamente para realizar trabajos de configuración y mantenimiento de redes en un entorno real.

BIBLIOGRAFIA

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

Configuración RIP. Recuperado de : https://ccnadesdecero.es/configuracion-del-protocolo-rip

Temática: Direccionamiento IP CISCO. (2019). Direccionamiento IP Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

Temática: División de redes IP en subredes CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

ANEXO 1 – Descarga Escenarios Packet Tracer

Link de descarga escenarios:

https://drive.google.com/drive/folders/1kPBoFSmE42fo8ALBDzNy3SXczd8OVB0r?usp=sharing