PRUEBA DE HABILIDADES CCNA 2020

KATHERINE TORRES GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNA
PALMIRA, VALLE DEL CAUCA
2020

PRUEBA DE HABILIDADES CCNA 2020

KATHERINE TORRES GONZÁLEZ

Proyecto de Grado presentado para optar por el título de:
INGENIERÍA DE SISTEMAS

Docente:
INGENIERO GUSTAVO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNA
PALMIRA, VALLE DEL CAUCA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado I

Firma del Jurado II

Palmira, Julio 21 de 2020

DEDICATORIA

Le dedico este logro a mi familia, como prueba de fortaleza y perseverancia en la consecución de metas pese a las adversidades, siempre de la mano de Dios

AGRADECIMIENTOS

Mis más sinceros agradecimientos en primer lugar a Dios por haberme permitido lograr esta meta, a mi madre por estar siempre
a mi lado apoyándome incondicionalmente y al docente Gustavo Rodríguez por su paciencia y guía en el desarrollo de este Diplomado

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

NAT (Network Address Translation): La traducción de direcciones de red o también llamado enmascaramiento de IP o NAT, es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

PAT (Port Address Translation): Es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet. Con PAT, una IP externa puede responder hasta a ~64000 direcciones internas

CHAP (Challenge Handshake Authentication Protocol): Es un protocolo de autenticación por desafío y fue definido en la RFC 1994. Es un método de autenticación remota o inalámbrica.

PPP (**Protocolo punto a punto, Point-to-Point Protocol**): Es un protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entre medias de ambos.

ACL (Access control list): Una lista de control de acceso o ACL es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.1
Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo con alguna condición.

IPv4 (Internet Protocol version 4, IPv4): El Protocolo de Internet versión 4, un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET. Definida en el RFC 791, el IPv4 usa direcciones de 32 bits, limitadas a 4 294 967 296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LAN).

ENRUTAMIENTO:
Es el proceso que el router utiliza para decidir donde enviar un paquete.

Podemos imaginar el router como un centro de tratamiento de cartas del correo, ahí lo que hacen es recibir todas las cartas, separar de acuerdo con su destino y enviarlas por el mejor camino. Existen 2 tipos de rutas, estáticas y dinámicas.

SUMARIZACIÓN: La sumarización de rutas es una técnica empleada en enrutamiento IP avanzado que permite sintetizar múltiples rutas IP contiguas en una única ruta.

INTRODUCCIÓN

Actualmente la tecnología forma parte de nuestra sociedad y en cierto modo dependemos de ella para realizar gran cantidad de labores diarias; el incremento en el uso de dispositivos electrónicos conectados a internet ha permitido expandir los límites y esta interacción ha significado la evolución de nuestra sociedad al punto de realizar gran cantidad de transacciones en segundos, acceder a toda clase de información y tener conexión en tiempo real con usuarios ubicados a larga distancia, logrando así contribuir al desarrollo de los países mediante la comercialización de productos y/o servicios a gran escala.

Sin embargo, esto supone un gran riesgo para la seguridad de la información de cada uno de los usuarios que accede a la web, por lo cual ha sido necesario implementar prácticas de seguridad que nos permitan mantener la confidencialidad de datos para cada equipo conectado a una red.

En este trabajo, realizaremos la distribución de una red acorde con las necesidades de 2 escenarios planteados y utilizaremos protocolos de configuración que permitirán garantizar la seguridad de la información de cada dispositivo contenido en ella.

JUSTIFICACIÓN

Mediante este proyecto de grado, se pretende dar ejemplo de la configuración ideal de una red que responda a los requerimientos de 2 escenarios planteados.

A medida que se plantea el diseño de red mediante el uso de un simulador (packet tracer) que permite visualizar la topología, también se realiza la configuración de cada uno de los dispositivos haciendo uso de protocolos de seguridad que permitan mantener la confidencialidad de los datos que circulan entre cada uno de los usuarios que hacen parte de la red.

OBJETIVOS

OBJETIVO GENERAL:

Realizar el diseño de una red que responda a los requerimientos de los escenarios planteados, cumpliendo con los estándares de calidad y seguridad establecidos por CISCO.

OBJETIVOS ESPECÍFICOS:

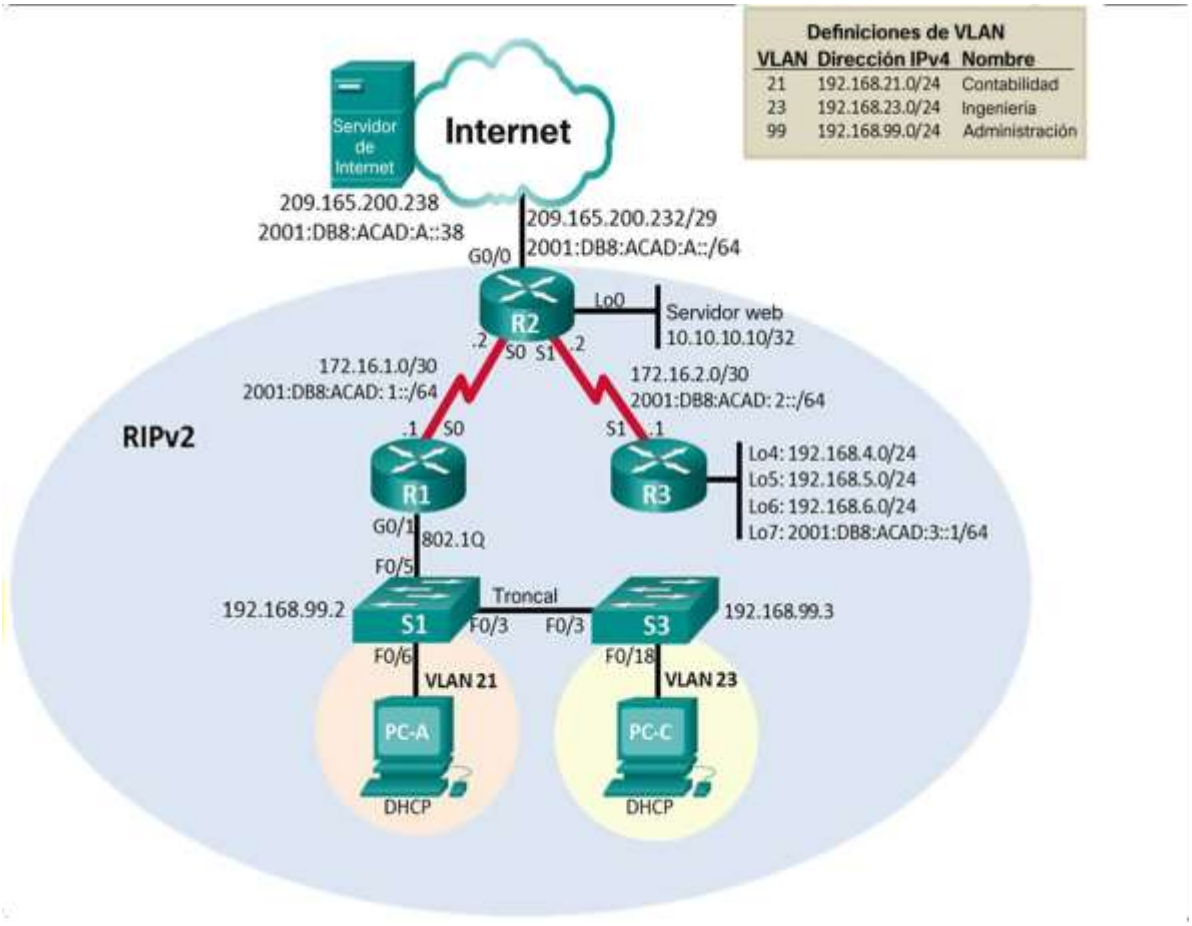
- Realizar el diseño de la topología de red acorde a los requerimientos planteados por los 2 escenarios.
- Desarrollar configuraciones para cada uno de los dispositivos de la red que permitan optimizar el flujo de información.
- Utilizar protocolos de seguridad en la configuración de cada dispositivo contenido en la red.

PLANTEAMIENTO DEL PROBLEMA

ESCENARIO 1

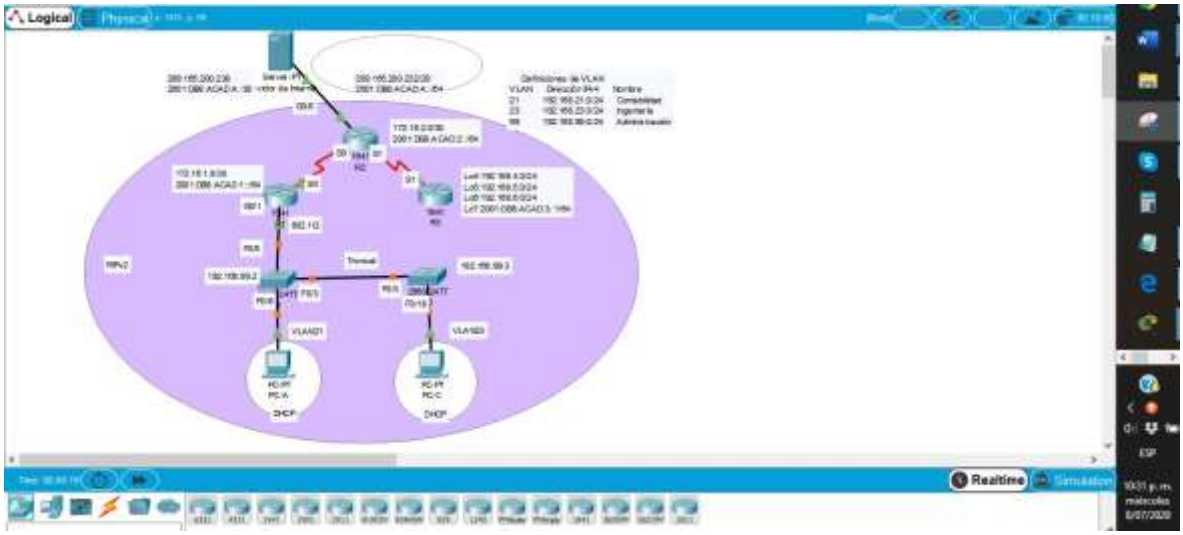
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de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

Figura 1. Topología de Red Escenario 1



Fuente: PRUEBA DE HABILIDADES CCNA 2020 16-02

Figura 2. Topología de Red



Fuente Propia

INICIALIZACIÓN DE TODOS LOS DISPOSITIVOS

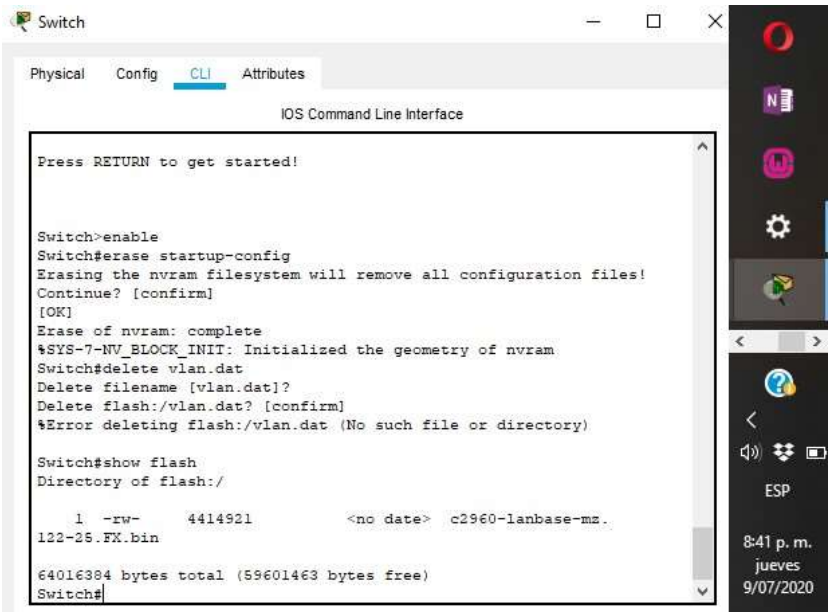
De acuerdo con los requerimientos planteados en el enunciado del Escenario 1, realizaremos la configuración inicial de cada uno de los dispositivos necesario. Como primer paso, borraremos cualquier tipo de configuración previa existente mediante el uso de los comandos relacionados en la tabla.

Tabla 1. Comandos de borrado de configuración inicial

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

Figura 3. Show flash Switch



Fuente: Propia

Configuración de los parámetros básicos de los dispositivos

Una vez inicializados cada uno de los dispositivos, procedemos a configurarlos de acuerdo direccionamiento IP planteado por la topología de red, comenzando por el Servidor de Internet, los Routers, Switches y PCs.

Tabla 2. Configuración Inicial Servidor

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***

Configuración R1

Configuramos el Router 1 de acuerdo con la topología propuesta, utilizando los comandos requeridos para cada una de las tareas indicadas:

Tabla 3. Configuración Inicial R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Acceso No Autorizado#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R2(config-if)#ipv6 route ::/0 g0/0

Configuración R2

Configuramos el Router 2 de acuerdo con la topología propuesta, utilizando los comandos requeridos para cada una de las tareas indicadas (desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http y generar un mensaje de alerta cuando la contraseña es incorrecta):

Tabla 4. Configuración Inicial R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server (*Este commando no funciona en Packet Tracer*)
Mensaje MOTD	R2(config)#banner motd #Acceso No Autorizado#
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown

Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#int l0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulated web server R2(config-if)#exit
Ruta predeterminada	R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config-if)#ipv6 route ::/0 g0/0

Configuración R3

Configuramos el Router 3 de acuerdo con la topología propuesta, utilizando los comandos requeridos para cada una de las tareas indicadas (desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http y generar un mensaje de alerta cuando la contraseña es incorrecta):

Tabla 5. Configuración Inicial R3

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

Contraseña de acceso Telnet	R32(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Acceso No Autorizado#
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int lo 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int lo 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int lo 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int lo 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas Predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Configuración S1

Configuramos el Switch 1 de acuerdo con la topología propuesta, utilizando los comandos requeridos para cada una de las tareas indicadas (desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http y generar un mensaje de alerta cuando la contraseña es incorrecta):

Tabla 6. Configuración Inicial S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal

	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line) #service password-encryption
Mensaje MOTD	S1(config)#banner motd #Acceso No Autorizado#

Configuración S3

Configuramos el Switch 3 de acuerdo con la topología propuesta, utilizando los comandos requeridos para cada una de las tareas indicadas (desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http y generar un mensaje de alerta cuando la contraseña es incorrecta):

Tabla 7. Configuración IP S3

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

Mensaje MOTD	S3(config)#banner motd #Acceso No Autorizado#

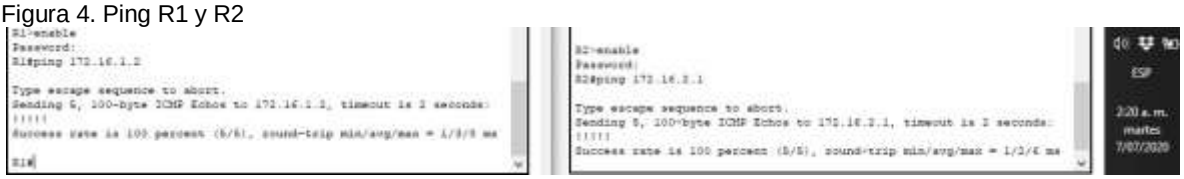
Verificamos la conectividad de la red

Mediante el uso del comando ping probamos la conectividad entre los dispositivos de red. A continuación, en la Tabla 8 podemos ver los comandos utilizados y los resultados obtenidos en cada uno de ellos:

Tabla 8. Prueba de conectividad R1, R2 y Servidor

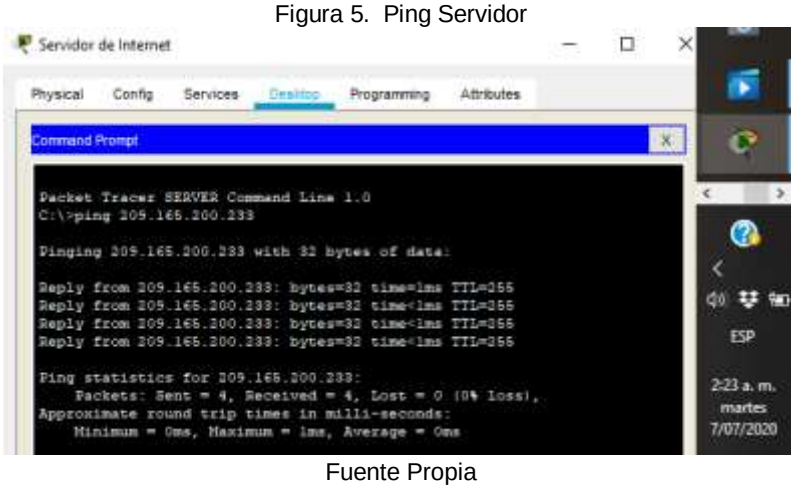
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233

Figura 4. Ping R1 y R2



Fuente Propia

Figura 5. Ping Servidor



Fuente Propia

CONFIGURACIÓN DE LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

Configuración S1

Realizamos la configuración del Switch 1 según la topología propuesta, asignando las vlan 21, 23 y 99 a los departamentos Contabilidad, Ingeniería y Administración respectivamente, utilizando los comandos requeridos para cada una de las tareas indicadas:

Tabla 9. Configuración de seguridad, VLAN y routing entre VLAN de S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#configure terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Configuración S3

Realizamos la configuración del Switch 1 según la topología propuesta, asignando las vlan 21, 23 y 99 a los departamentos Contabilidad, Ingenieria y Administración respectivamente, utilizando los comandos requeridos para cada una de las tareas indicadas:

Tabla 10. Configuración de seguridad, VLAN y routing entre VLAN de S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3#configure terminal S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Configuración R1.

Realizamos la configuración del Router 1 según la topología propuesta, asignando la subinterfaz de cada una de las vlan (21, 23 y 99) utilizando los comandos requeridos para cada una de las tareas indicadas:

Tabla 11. Configuración VLAN de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#configure terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Verificación de conectividad de la red

Mediante el comando ping realizamos la prueba de conectividad de los switches S1 y S3 con R1. En la figura 6 podemos visualizar el resultado de la ejecución de los comandos indicados en la Tabla 12:

Tabla 12. Prueba de Conectividad S1 y S3 con R1

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

Figura 6. Prueba de Conectividad S1 y S3 con R1

Fuente Propia

CONFIGURACIÓN DEL PROTOCOLO DE ROUTING DINÁMICO RIPV2

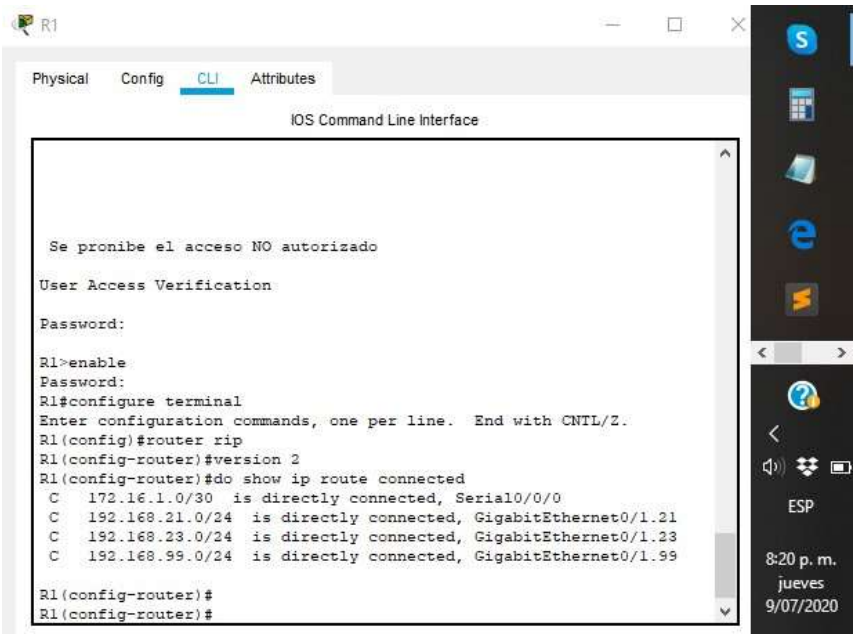
Configuración RIPv2 en el R1

Realizamos la configuración del Router 1 según la topología propuesta, especificando la ruta de cada una de las conexiones directas y estableciendo las interfaces LAN como pasivas:

Tabla 13. Configuración RIP de R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1#configure terminal R1(config)#router rip R1(config-router)#version 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 g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Figura 7. Do show ip Route Connected R1



Fuente: Propia

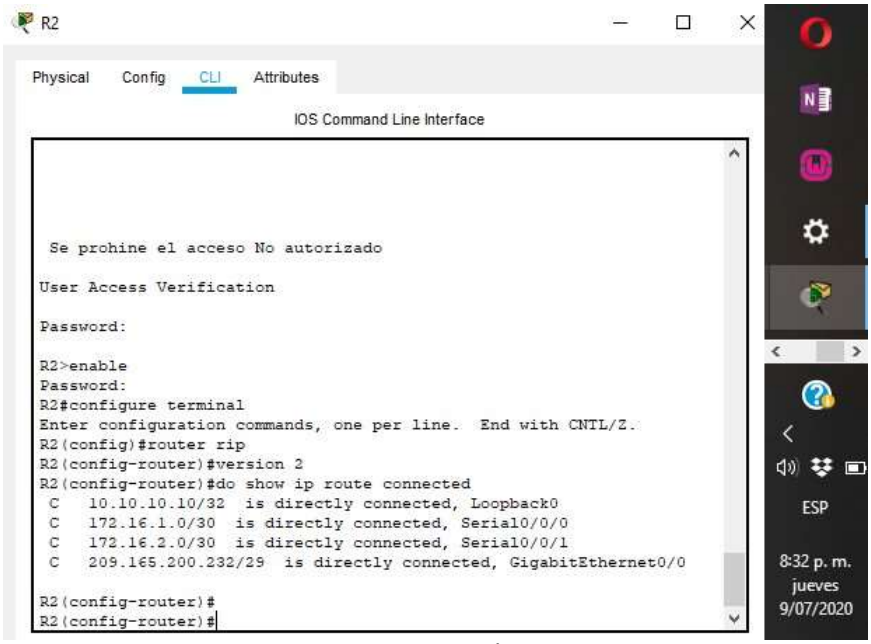
Configuración RIPv2 en el R2

Realizamos la configuración del Router 2 según la topología propuesta, especificando la ruta de cada una de las conexiones directas y estableciendo las interfaces LAN como pasivas:

Tabla 14. Configuración RIP de R2

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

Figura 8. Do show ip Route Connected R2



Fuente: Propia

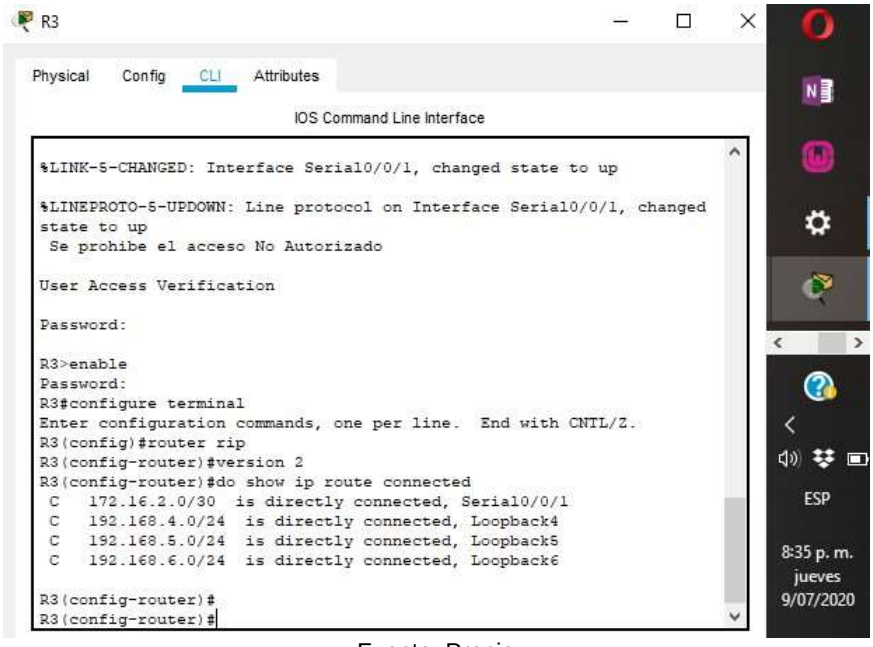
Configuración RIPv2 en el R3

Continuamos con la configuración del Router 3 según la topología propuesta, especificando la ruta de cada una de las conexiones directas y estableciendo las interfaces LAN como pasivas:

Tabla 15. Configuración RIP de R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#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.	R3(config-router)#no auto-summary

Figura 9. Do show ip Route Connected R3



Fuente: Propia

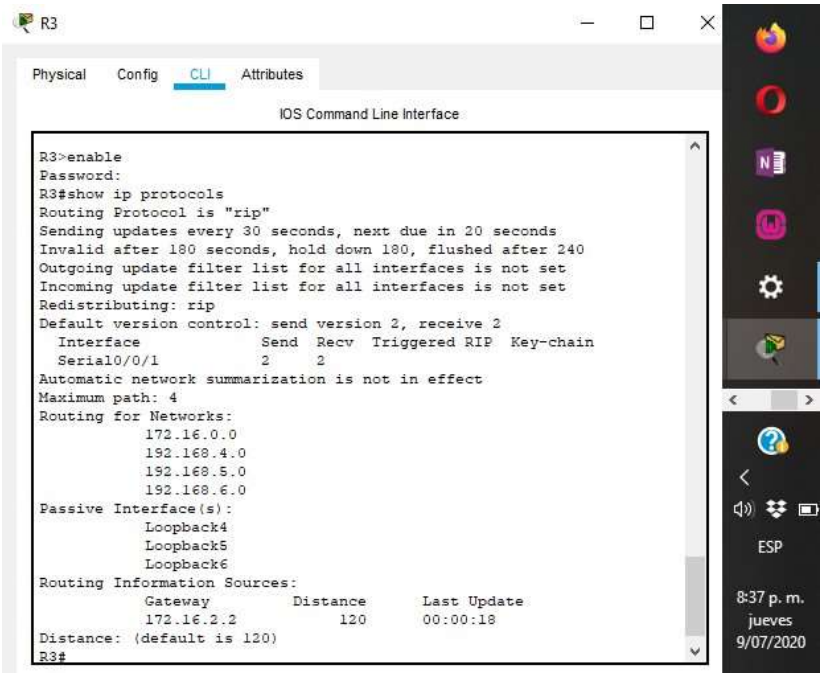
Verificación de la información de RIP

Con el fin de verificar el funcionamiento de RIP, ingresamos los siguientes comandos:

Tabla 16. Verificación funcionamiento RIP en R3

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?	R3#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R3#show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R3#show run | section router rip

Figura 10. Show ip protocols R3



Fuente: Propia

Figura 11. Show ip route rip R3

Fuente: Propia

Figura 12. show run | section router rip R3

Fuente: Propia

IMPLEMENTACIÓN DHCP Y NAT PARA IPV4

Realizamos la configuración del R1 como servidor de DHCP para las VLAN 21 y 23, reservando las primeras 20 direcciones IP para las respectivas vlan (21 y 23) y configurando el servicio DHCP posteriormente, todo mediante el uso de los comandos de la Tabla 17:

Tabla 18. Configuración de R1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R3(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

Configuración de la NAT estática y dinámica en el R2

Realizamos la configuración de R2 para establecer las NAT estática y dinámica, creando una base de datos local para garantizar el acceso de un usuario, habilitando el servicio HTTP y estableciendo una lista de acceso privada con las direcciones autorizadas para acceder:

Tabla 19. Configuración de NAT estática y dinámica en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2#configure terminal R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (*Este commando no funciona en Packet Tracer*)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local (*Este commando no funciona en Packet Tracer*)
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

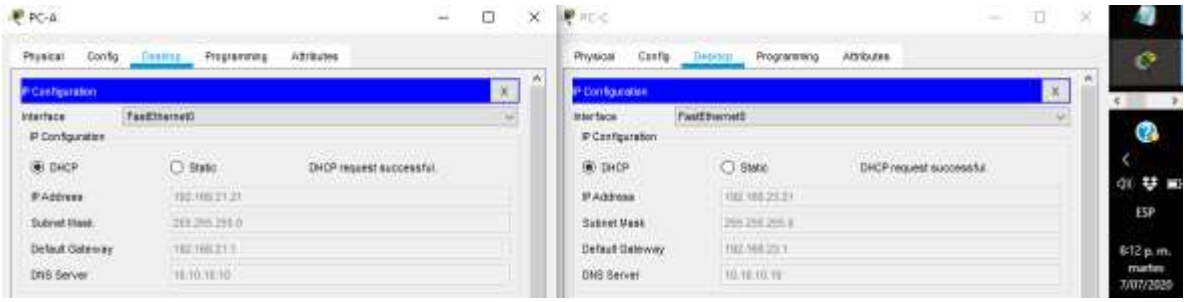
Verificación del protocolo DHCP y la NAT estática

Mediante el comando ping realizamos la comprobación de conectividad entre los dispositivos luego de las configuraciones previas.

Tabla 20. Verificación DHCP y NAT estática

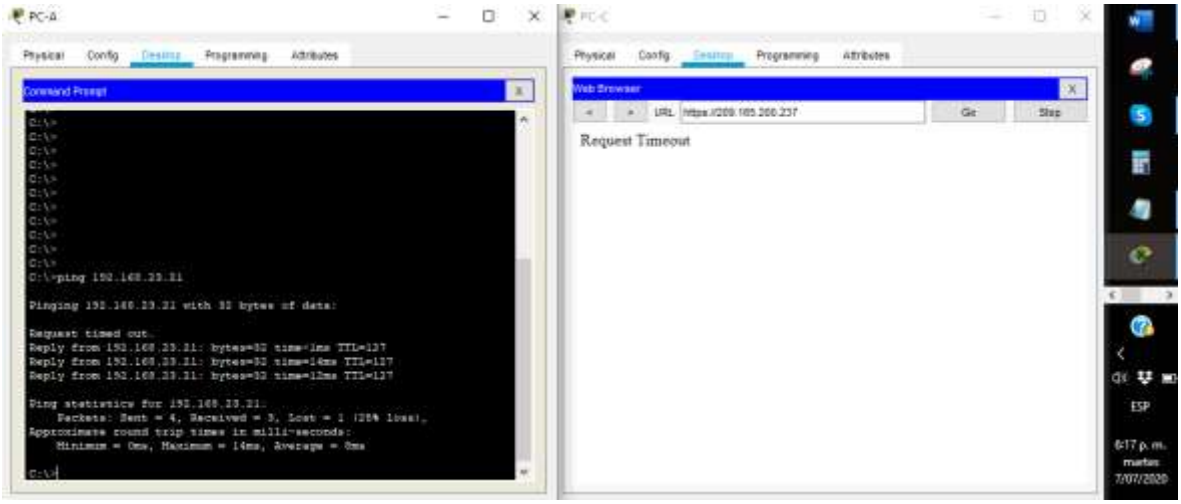
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	(No se pudo acceder dado que el *comando "ip http server" no funciona en Packet Tracer*)

Figura 13. Verificación DHCP en PC-A y PC-C



Fuente Propia

Figura 14. Ping PC-A a PC-C y Acceso al Servidor Web por Browser



Fuente Propia

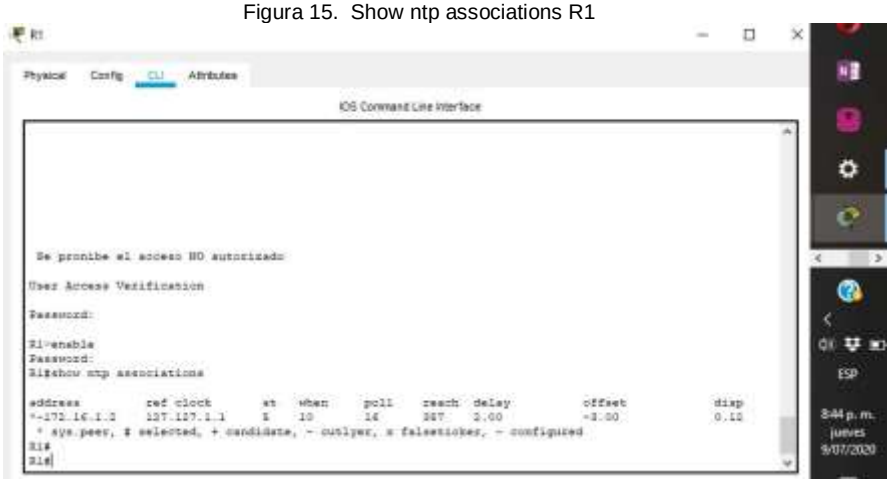
CONFIGURACIÓN NTP

Realizamos la configuración de NTP para configurar la hora de las computadoras de la red, estableciendo R2 como maestro (servidor) y R1 como cliente, sincronizando dicha información en la red. Finalmente, realizamos la verificación en la configuración de R1.

Tabla 21. Configuración NTP en R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	R2#configure terminal R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1#configure terminal R1(config)#ntp server 172.16.1.2
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#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 .INIT. 16 14 64 0 0.00 0.00 0.01 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1#

Figura 15. Show ntp associations R1



Fuente: Propia

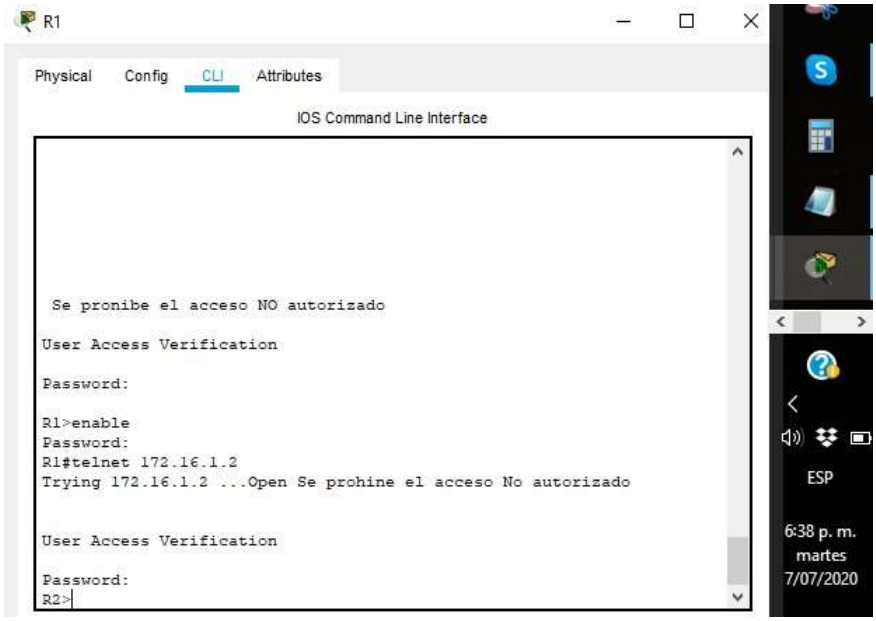
CONFIGURACIÓN Y VERIFICACIÓN DE LAS LISTAS DE CONTROL DE ACCESO (ACL)

Configuramos las listas de acceso, definiéndolas de acuerdo con los departamentos, restringiendo todo acceso a las líneas VTY. Posteriormente realizamos la verificación de las configuraciones mediante los comandos indicados en la Tabla 22:

Tabla 22. Configuración 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#configure terminal 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
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	Exitoso

Figura 16. Verificación de ACL en R1

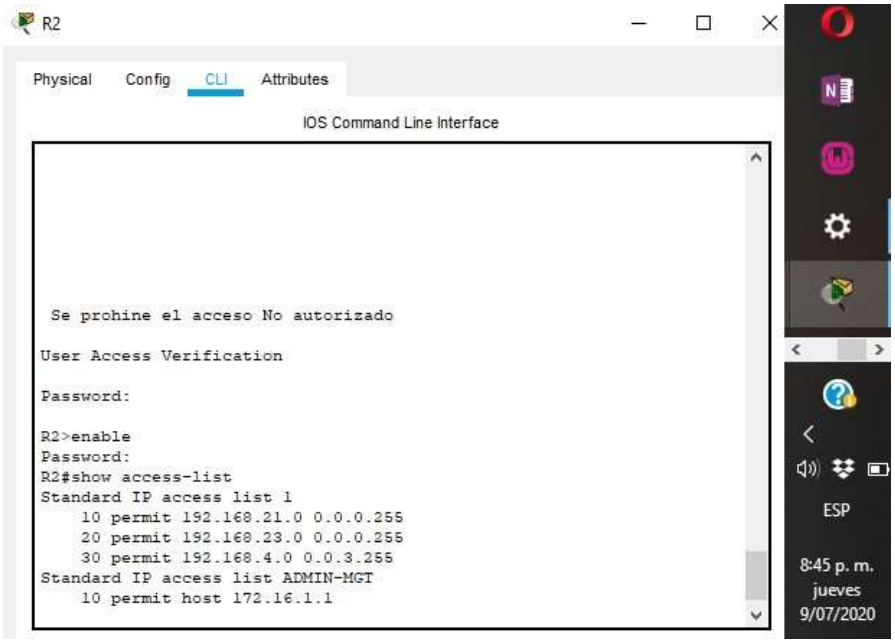


Fuente Propia

Tabla 23. Verificación de las ACL

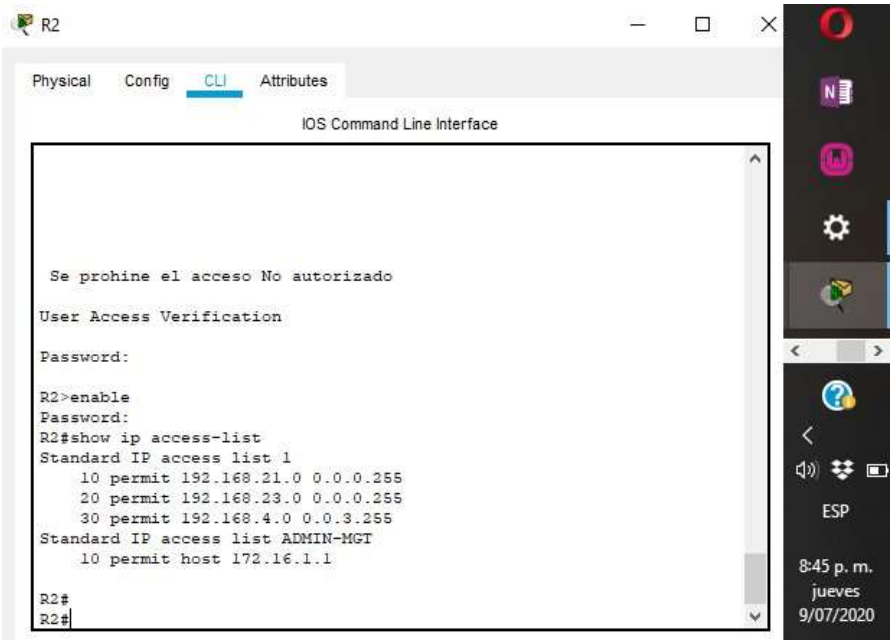
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 (6 match(es)) 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (4 match(es)) R2#show ip access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 (6 match(es)) 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (4 match(es))
Restablecer los contadores de una lista de acceso	R2#clear access-list counters R2#clear ip ? bgp Clear BGP connections dhcp Delete items from the DHCP database nat Clear NAT ospf OSPF clear commands route Delete route table entries
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations

Figura 17. Show access list R2



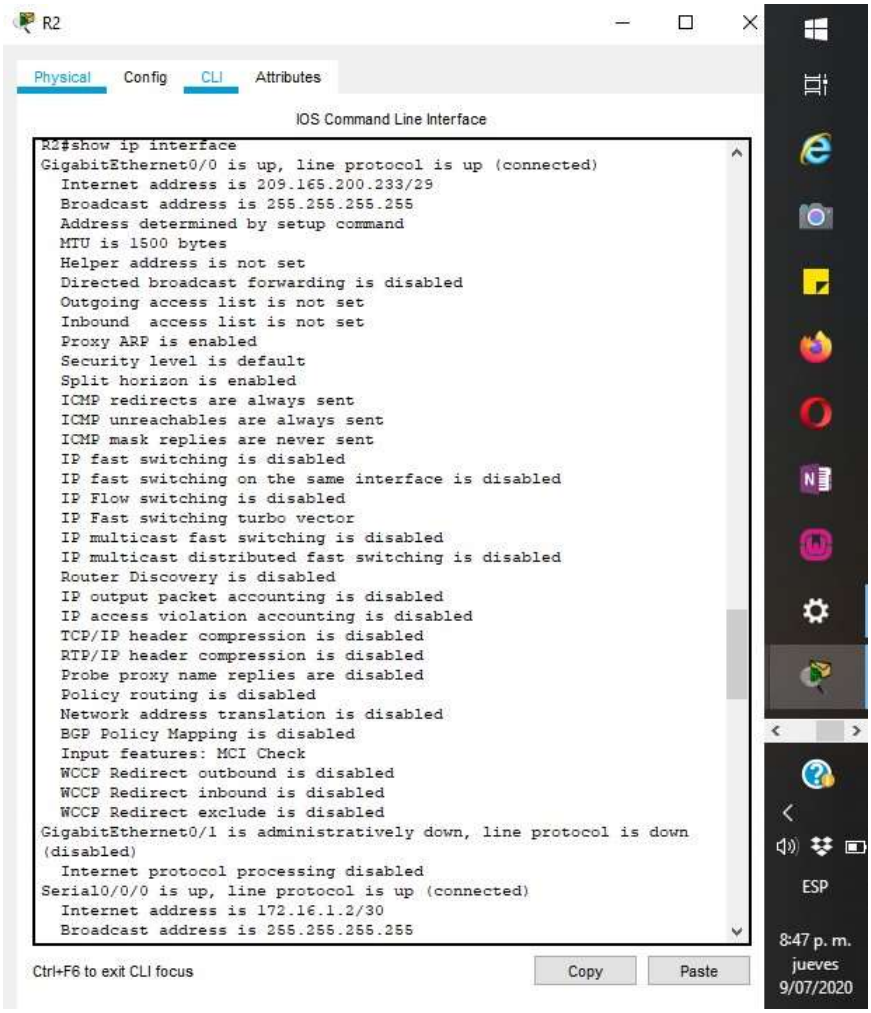
Fuente: Propia

Figura 18. Show ip access list



Fuente: Propia

Figura 19. Show ip interface

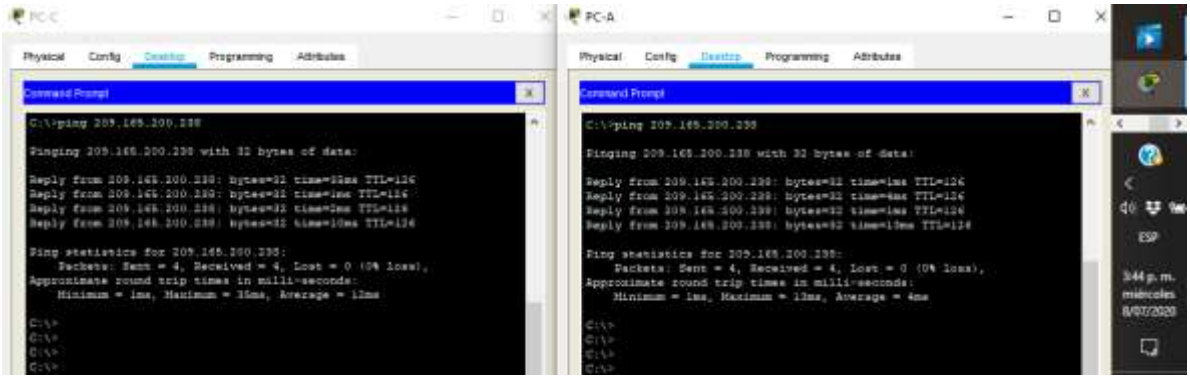


Fuente: Propia

Figura 20. Show ip nat translations

Fuente: Propia

Figura 21. Prueba de conectividad PC-C y PC-A con el Servidor

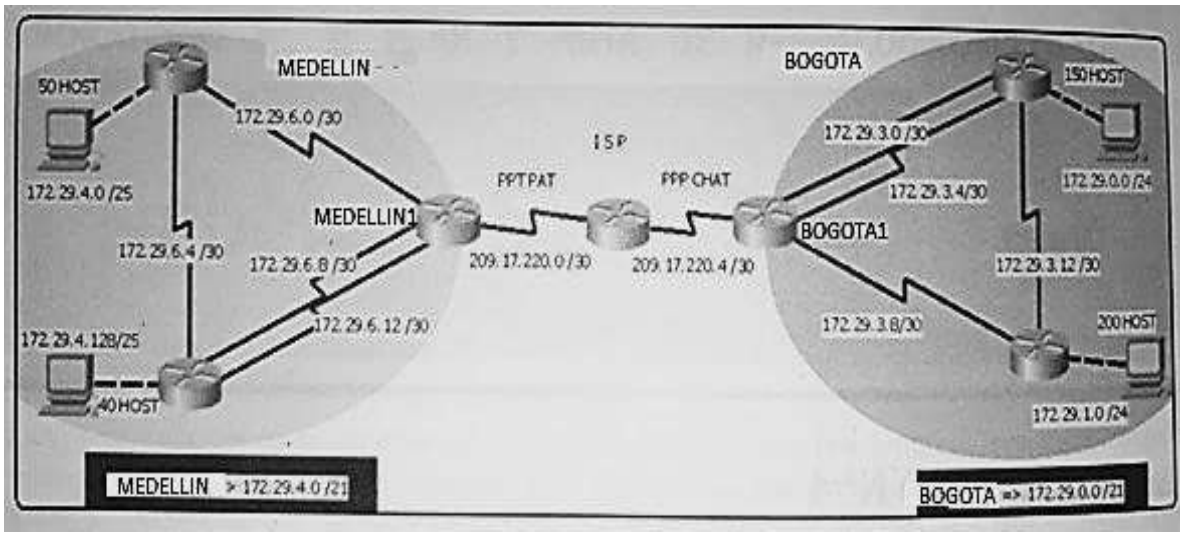


Fuente Propia

ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Figura 22: Topología de Red Escenario 2



Fuente: PRUEBA DE HABILIDADES CCNA 2020 16-02

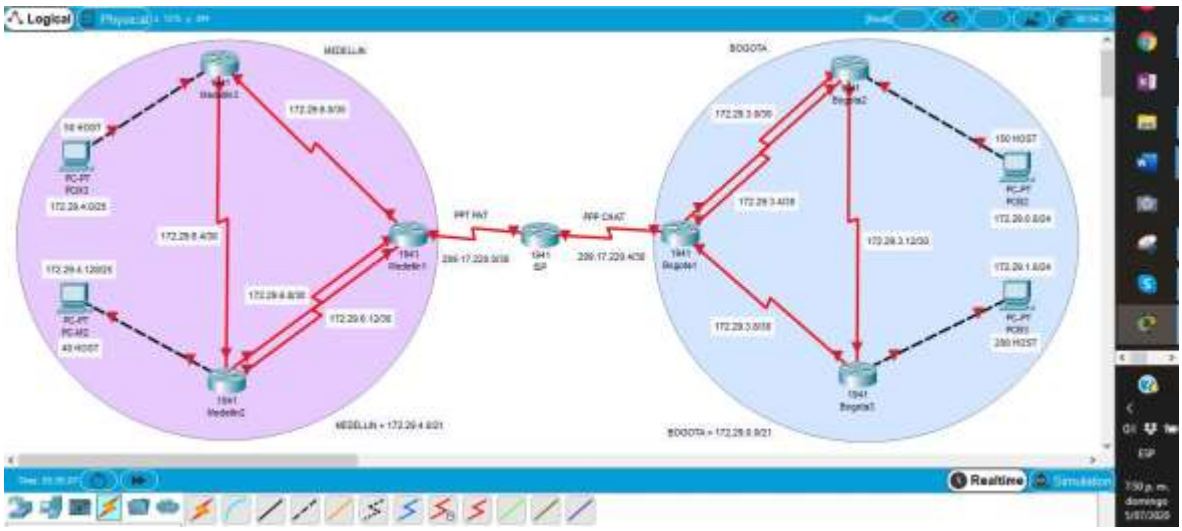
Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

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.

TRABAJO INICIAL

En el curso del diplomado, se presentó un trabajo inicial en el cual se realizaron las rutinas de diagnóstico para que cada uno de los dispositivos puedan ser configurados posteriormente con sus respectivos nombres y contraseñas de seguridad. Adicionalmente, se crearon las conexiones físicas de los dispositivos con base en la topología de red.

Figura 23. Topología de Red



Fuente: PRUEBA DE HABILIDADES CCNA 2020 16-02

A continuación, realizaremos las rutinas de diagnóstico de cada uno de los routers (ISP, Medellin1, Medellin2, Medellin3, Bogota1, Bogota2 y Bogota3). En los comandos de configuración básica, incluimos el nombre del dispositivo, establecimiento de credenciales de acceso y validación de usuario, además de la encriptación de la contraseña.

Tabla 24. Configuración Básica de Routers

Dispositivo	Configuración Básica
ISP	Router>enable Router#configure terminal Router(config)#hostname ISP ISP(config)#enable secret ISP ISP(config)#line console 0 ISP(config-line)#password ISP1 ISP(config-line)#login ISP(config-line)#line vty 0 15 ISP(config-line)#password ISP1 ISP(config-line)#login ISP(config-line)#service password-encryption ISP(config)#banner motd #Acceso No Autorizado#
Medellin1	Router>enable Router#configure terminal Router(config)#hostname Medellin1 Medellin1 (config)#enable secret Med1 Medellin1 (config)#line console 0 Medellin1 (config-line)#password Mede1 Medellin1 (config-line)#login Medellin1 (config-line)#line vty 0 15

	Medellin1 (config-line)#password Mede1 Medellin1 (config-line)#login Medellin1 (config-line)#service password-encryption Medellin1 (config)#banner motd #Acceso No Autorizado#
Medellin2	Router>enable Router#configure terminal Router(config)#hostname Medellin2 Medellin2 (config)#enable secret Med2 Medellin2 (config)#line console 0 Medellin2 (config-line)#password Mede2 Medellin2 (config-line)#login Medellin2 (config-line)#line vty 0 15 Medellin2config-line)#password Mede2 Medellin2 (config-line)#login Medellin2 (config-line)#service password-encryption Medellin2 (config)#banner motd #Acceso No Autorizado#
Medellin3	Router>enable Router#configure terminal Router(config)#hostname Medellin3 Medellin3 (config)#enable secret Med3 Medellin3 (config)#line console 0 Medellin3 (config-line)#password Mede3 Medellin3 (config-line)#login Medellin3 (config-line)#line vty 0 15 Medellin3 (config-line)#password Mede3 Medellin3 (config-line)#login Medellin3 (config-line)#service password-encryption Medellin3 (config)#banner motd #Acceso No Autorizado#
Bogota1	Router>enable Router#configure terminal Router(config)#hostname Bogota1 Bogota1 (config)#enable secret Bog1 Bogota1 (config)#line console 0 Bogota1 (config-line)#password Bogo1 Bogota1 (config-line)#login Bogota1 (config-line)#line vty 0 15 Bogota1 (config-line)#password Bogo1 Bogota1 (config-line)#login Bogota1 (config-line)#service password-encryption Bogota1 (config)#banner motd #Acceso No Autorizado#
Bogota2	Router>enable Router#configure terminal Router(config)#hostname Bogota2 Bogota2 (config)#enable secret Bog2 Bogota2 (config)#line console 0 Bogota2 (config-line)#password Bogo2 Bogota2 (config-line)#login Bogota2 (config-line)#line vty 0 15 Bogota2 (config-line)#password Bogo2 Bogota2 (config-line)#login Bogota2 (config-line)#service password-encryption Bogota2 (config)#banner motd #Acceso No Autorizado#

Bogota3	Router>enable Router#configure terminal Router(config)#hostname Bogota3 Bogota3 (config)#enable secret Bog3 Bogota3 (config)#line console 0 Bogota3 (config-line)#password Bogo3 Bogota3 (config-line)#login Bogota3 (config-line)#line vty 0 15 Bogota3 (config-line)#password Bogo3 Bogota3 (config-line)#login Bogota3 (config-line)#service password-encryption Bogota3 (config)#banner motd #Acceso No Autorizado#

Luego de tener en cuenta los requerimientos de la red planteada en el escenario 2, se elaboró la siguiente Tabla de Direccionamiento para cada uno de los dispositivos:

Tabla 25. Tabla de Direccionamiento IP

Dispositivo	Interfaz	Conexión a	Dirección IP	Máscara de Subred	Gateway Predeterminado
Medellin1	S0/0/0	ISP	209.17.220.2	255.255.255.252	N.A
	S0/0/1	Medellin2	172.29.6.13	255.255.255.252	N.A
	S0/1/0	Medellin2	172.29.6.9	255.255.255.252	N.A
	S0/1/1	Medellin3	172.29.6.1	255.255.255.252	N.A
Medellin2	S0/0/0	Medellin1	172.29.6.10	255.255.255.252	N.A
	S0/0/1	Medellin1	172.29.6.14	255.255.255.252	N.A
	S0/1/0	Medellin3	172.29.6.6	255.255.255.252	N.A
	G0/0	PCM2	**172.29.4.129**	255.255.255.192	
Medellin3	S0/0/0	Medellin1	172.29.6.2	255.255.255.252	N.A
	S0/0/1	Medellin2	172.29.6.5	255.255.255.252	N.A
	G0/0	PCM3	**172.29.4.1**	255.255.255.192	
Bogota1	S0/0/0	Bogota2	172.29.3.1	255.255.255.252	N.A
	S0/0/1	Bogota2	172.29.3.5	255.255.255.252	N.A
	S0/1/0	Bogota3	172.29.3.9	255.255.255.252	N.A
	S0/1/1	ISP	209.17.220.6	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	PCB2	**172.29.0.1**	255.255.255.0	
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	PCB3	**172.29.1.1**	255.255.255.0	
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
PCM2	Fa0	172.29.4.130	DHCP	255.255.255.192	172.29.4.129
PCM3	Fa0	172.29.4.2	DHCP	255.255.255.192	172.29.4.1
PCB2	Fa0	172.29.0.2	DHCP	255.255.255.0	172.29.0.1
PCB3	Fa0	172.29.1.2	DHCP	255.255.255.0	172.29.1.1

Una vez establecido el direccionamiento IP que tendrá la red, procedemos a asignar las ip correspondientes a cada una de las interfaces, especificando la máscara de red y especificando la velocidad de envío de datos a 128000 bits por segundo:

Tabla 26. Configuración de Direccionamiento IP

Dispositivo	Configuración Direccionamiento IP
ISP	ISP>enable ISP#configure terminal ISP(config)#int s0/0/0 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#no shutdown ISP(config-if)#int s0/0/1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown
Medellin1	Medellin1>enable Medellin1#configure terminal Medellin1(config)#int s0/0/0 Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)#int s0/0/1 Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config-if)#int s0/1/0 Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config-if)#int s0/1/1 Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown
Medellin2	Medellin2>enable Medellin2#configure terminal Medellin2(config)#int s0/0/0 Medellin2(config-if)#ip address 172.29.6.10 255.255.255.252 Medellin2(config-if)#no shutdown Medellin2(config-if)#int s0/0/1 Medellin2(config-if)#ip address 172.29.6.14 255.255.255.252 Medellin2(config-if)#clock rate 128000 Medellin2(config-if)#no shutdown Medellin2(config-if)#int s0/1/0 Medellin2(config-if)#ip address 172.29.6.6 255.255.255.252 Medellin2(config-if)#clock rate 128000 Medellin2(config-if)#no shutdown Medellin2(config-if)#int g0/0 Medellin2(config-if)#ip address 172.29.4.129 255.255.255.192 Medellin2(config-if)#no shutdown

Medellin3	Medellin3>enable Medellin3#configure terminal Medellin3(config)#int s0/0/0 Medellin3(config-if)#ip address 172.29.6.2 255.255.255.252 Medellin3(config-if)#no shutdown Medellin3(config-if)#int s0/0/1 Medellin3(config-if)#ip address 172.29.6.5 255.255.255.252 Medellin3(config-if)#clock rate 128000 Medellin3(config-if)#no shutdown Medellin3(config-if)#int g0/0 Medellin3(config-if)#ip address 172.29.4.1 255.255.255.192 Medellin3(config-if)#no shutdown
Bogota1	Bogota1>enable Bogota1#configure terminal Bogota1(config)#int s0/0/0 Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252 Bogota1(config-if)#no shutdown Bogota1(config-if)#int s0/0/1 Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown Bogota1(config-if)#int s0/1/0 Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown Bogota1(config-if)#int s0/1/1 Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown
Bogota2	Bogota2>enable Bogota2#configure terminal Bogota2(config)#int s0/0/0 Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252 Bogota2(config-if)#no shutdown Bogota2(config-if)#int s0/0/1 Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252 Bogota2(config-if)#clock rate 128000 Bogota2(config-if)#no shutdown Bogota2(config-if)#int s0/1/0 Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252 Bogota2(config-if)#clock rate 128000 Bogota2(config-if)#no shutdown Bogota2(config-if)#int g0/0 Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0 Bogota2(config-if)#no shutdown
Bogota3	Bogota3>enable Bogota3#configure terminal Bogota3(config)#int s0/0/0 Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config-if)#int s0/0/1 Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252

	Bogota3(config-if)#clock rate 128000 Bogota3(config-if)#no shutdown Bogota3(config-if)#int g0/0 Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0 Bogota3(config-if)#no shutdown

CONFIGURACIÓN DEL ENRUTAMIENTO

Configuramos el enrutamiento en la red usando el protocolo OSPF versión 2, declarando la red principal de cada uno de los routers (esto se puede hacer identificando las conexiones directas de cada uno de los routers) y desactivando la sumarización automática. En este caso no incluimos el router ISP porque tiene rutas estáticas sumarizadas (la configuración se hará posteriormente).:

Tabla 27. Configuración de enrutamiento OSPF versión 2

Dispositivo	Configuración OSPF en los Routers
Medellin1	Medellin1#configure terminal Medellin1(config)#router ospf 1 Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 1 Medellin1(config-router)#exit Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 Medellin1(config)#no auto-summary
Medellin 2	Medellin2#configure terminal Medellin2(config)#router ospf 1 Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 1 Medellin2(config-router)#network 172.29.6.8 0.0.0.3 area 1 Medellin2(config-router)#network 172.29.6.12 0.0.0.3 area 1 Medellin2(config-router)#network 172.29.4.128 0.0.0.63 area 1 Medellin2(config-router)#default-information originate Medellin2(config-router)#no auto-summary
Medellin 3	Medellin3#configure terminal Medellin3(config)#router ospf 1 Medellin3(config-router)#network 172.29.6.0 0.0.0.3 area 1 Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 1 Medellin3(config-router)#network 172.29.4.0 0.0.0.63 area 1 Medellin3(config-router)#default-information originate Medellin3(config-router)#no auto-summary
Bogota1	Bogota1#configure terminal Bogota1(config)#router ospf 1 Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 1 Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 1 Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 1 Bogota1(config-router)#exit Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 Bogota1(config)#no auto-summary
Bogota 2	Bogota2(config)#router ospf 1 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 172.29.3.12 0.0.0.3 area 1 Bogota2(config-router)#network 172.29.0.0 0.0.0.63 area 1 Bogota2(config-router)#default-information originate Bogota2(config-router)#no auto-summary

Bogota 3	Bogota3#configure terminal Bogota3(config)#router ospf 1 Bogota3(config-router)#network 172.29.3.8 0.0.0.3 area 1 Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 1 Bogota3(config-router)#network 172.29.1.0 0.0.0.63 area 1 Bogota3(config-router)#default-information originate Bogota3(config-router)#no auto-summary

Los routers Bogota1 y Medellín deben incorporar un enrutamiento por defecto que vaya al router ISP, además de redistribuirla dentro de las publicaciones de OSPF.

Tabla 28. Configuración de Ruta Redistribuida en OSPF

Dispositivo	Configuración Ruta Distribuida en OSPF
Medellin1	Medellin1#configure terminal Medellin1(config)#router ospf 1 Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 1 Medellin1(config-router)#default-information originate Medellin1(config-router)#exit
Bogota1	Bogota1#configure terminal Bogota1(config)#router ospf 1 Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 1 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)#exit

Dado que ISP se comunica directamente con Medellin1 y Bogota 1, tendrá que configurar una ruta estática que esté dirigida a la red interna de ellos, por lo cual se realizara la sumarización de las subredes de dichos routers a /22.

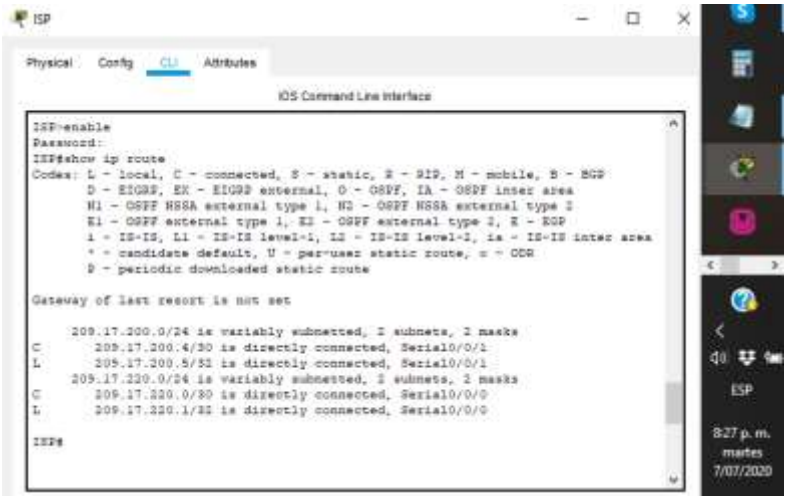
Tabla 29. Configuración de Rutas Estáticas Sumarizadas a Sedes

Dispositivo	Configuración Rutas Estáticas Sumarizadas a Sedes
ISP	ISP#configure 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

TABLA DE ENRUTAMIENTO.

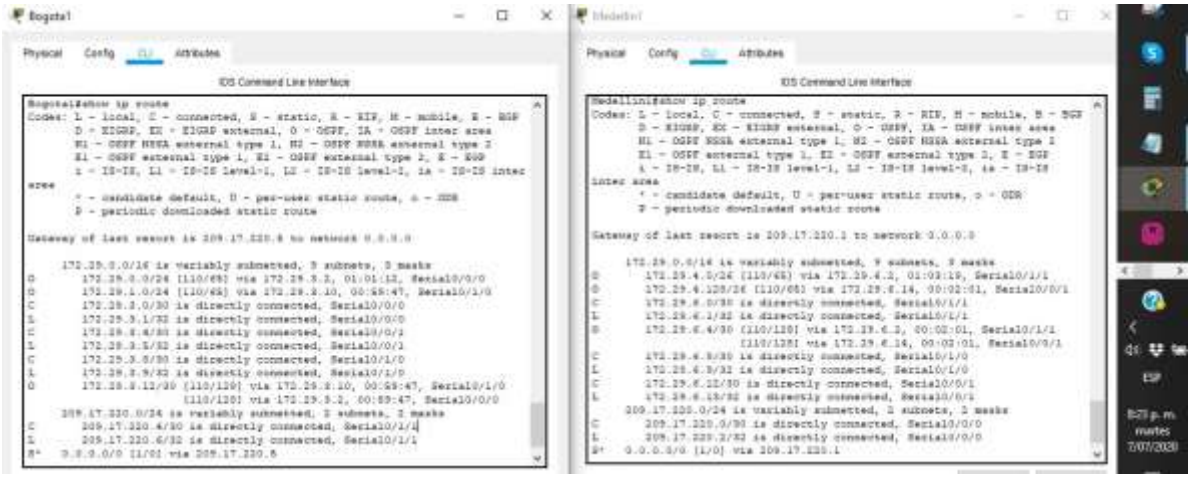
Verificamos la tabla de enrutamiento establecida previamente en cada uno de los routers utilizando el comando “show ip route” , este comando nos permite ver las redes y sus rutas, además del balanceo de carga que presentan los routers.

Figura 24. Verificación de enrutamiento ISP



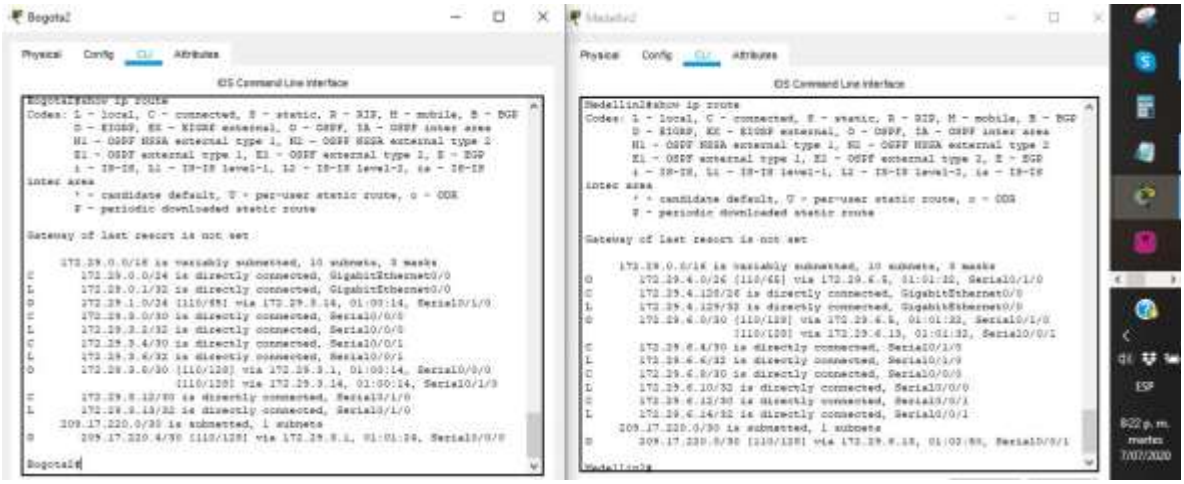
Fuente Propia

Figura 25. Verificación de enrutamiento Bogota1 y Medellin1



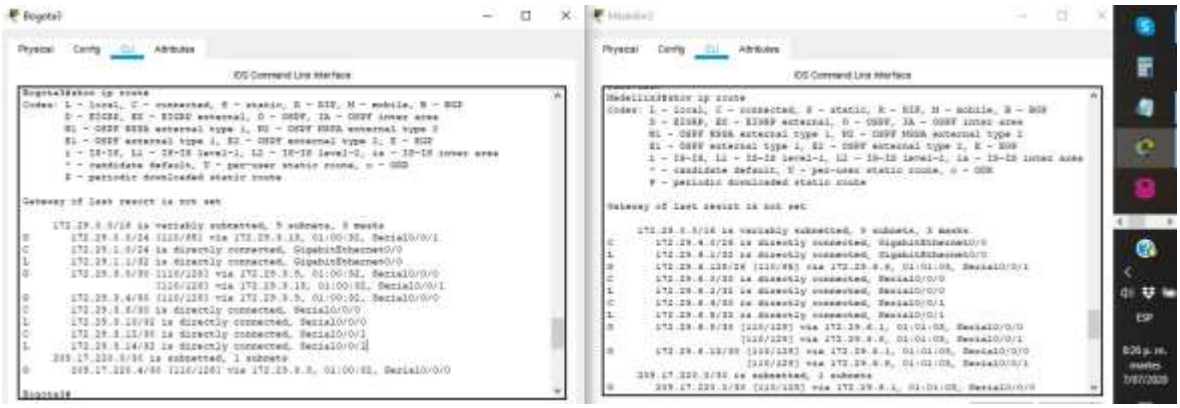
Fuente Propia

Figura 26. Verificación de enrutamiento Bogota2 y Medellin2



Fuente Propia

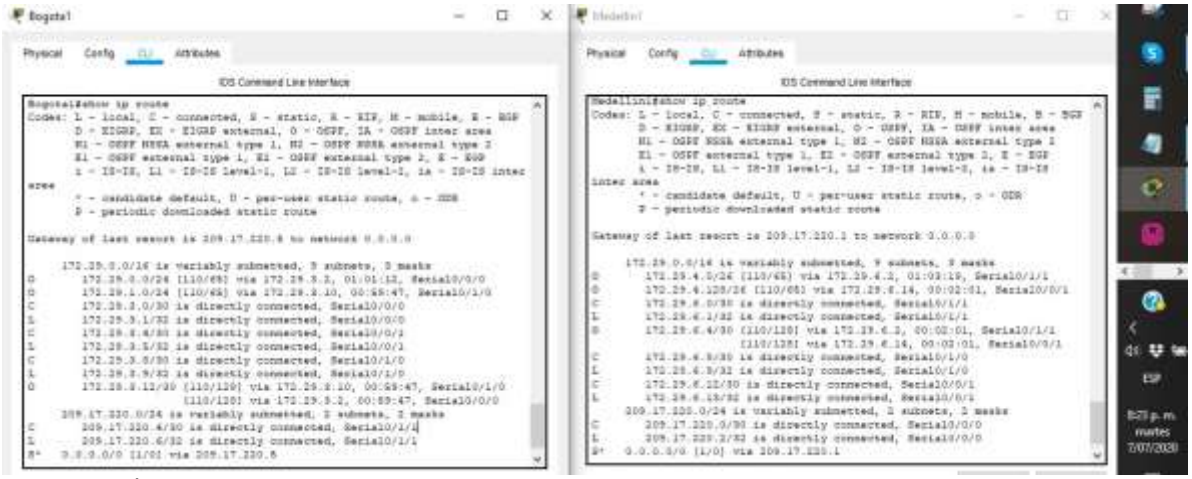
Figura 27. Verificación de enrutamiento Bogota3 y Medellin3



Fuente Propia

Como podemos ver en la Figura 28, existe cierta similitud entre los Routers Bogota1 y Medellín1, esto sucede por su ubicación y el hecho de tener 2 enlaces de conexión hacia ISP, además de la ruta por defecto que manejan.

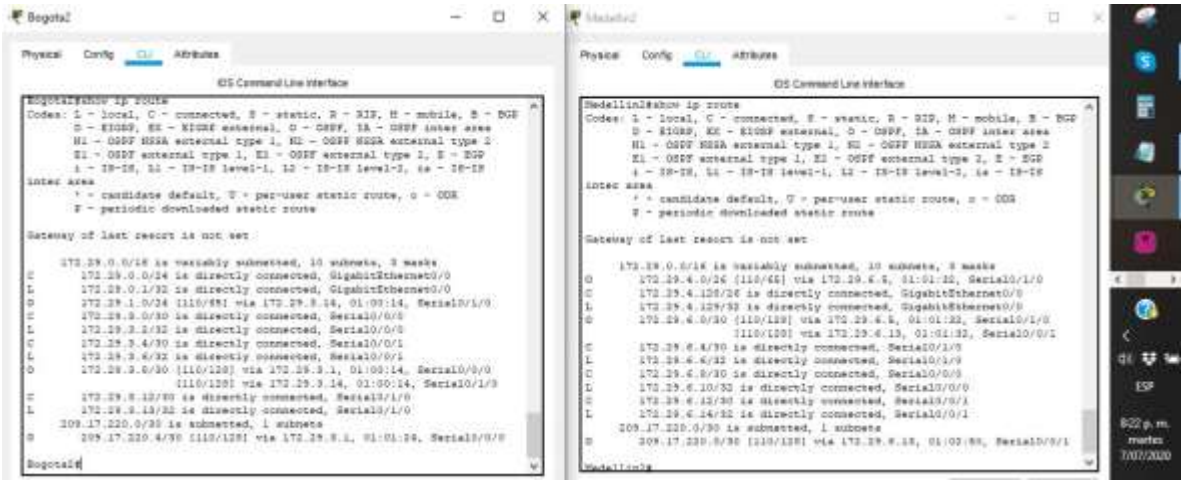
Figura 28. Comparación de conexión Bogota1 y Medellin1



Fuente Propia

De la misma forma, entre los routers Medellin2 y Bogota2 encontramos redes configuradas por OSPF y podemos visualizar las redundancias de la ruta establecida por defecto.

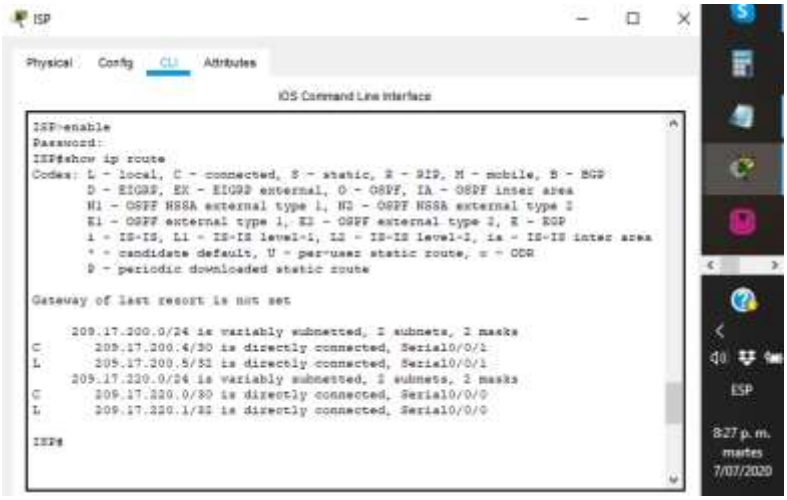
Figura 29. Comparación de conexión Bogota2 y Medellin2



Fuente Propia

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

Figura 30. Rutas estáticas ISP



Fuente Propia

DESHABILITACIÓN DE LA PROPAGACIÓN DEL PROTOCOLO OSPF.

Según la topología de red, existen algunas interfaces que no requieren OSPF, por lo cual procederemos a desactivarlas.
En la Tabla 29 encontramos el detalle de las interfaces a desactivar en cada router y en la Tabla 30 están los comandos utilizados para desarrollar esta tarea:

Tabla 30. Tabla de Interfaces para desactivar OSPF

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

Tabla 31. Deshabilitación de OSPF para cada Router

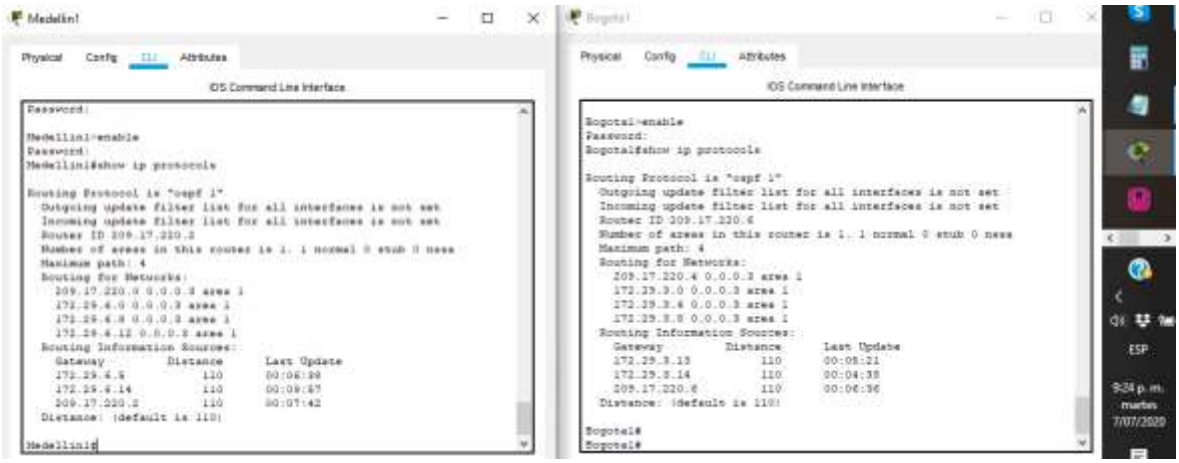
Dispositivo	Deshabilitación propagación del protocolo OSPF
Bogota2	Bogota2#configure terminal Bogota2(config)#router ospf 1 Bogota2(config-router)#passive-interface g0/0 Bogota2(config-router)#end Bogota2#wr
Bogota3	Bogota3#configure terminal Bogota3(config)#router ospf 1 Bogota3(config-router)#passive-interface g0/0 Bogota3(config-router)#end Bogota3#wr
Medellin2	Medellin2#configure terminal Medellin2(config)#router ospf 1 Medellin2(config-router)#passive-interface g0/0 Medellin2(config-router)#end Medellin2#wr

Medellin3	Medellin3#configure terminal Medellin3(config)#router ospf 1 Medellin3(config-router)#passive-interface g0/0 Medellin3(config-router)#end Medellin3#wr

VERIFICACIÓN DEL PROTOCOLO OSPF.

Una vez realizada la configuración del protocolo OSPF, procedemos a verificar las configuraciones de interfaz pasiva y su respectiva versión. Para esta tarea, utilizaremos el comando “show ip protocols”:

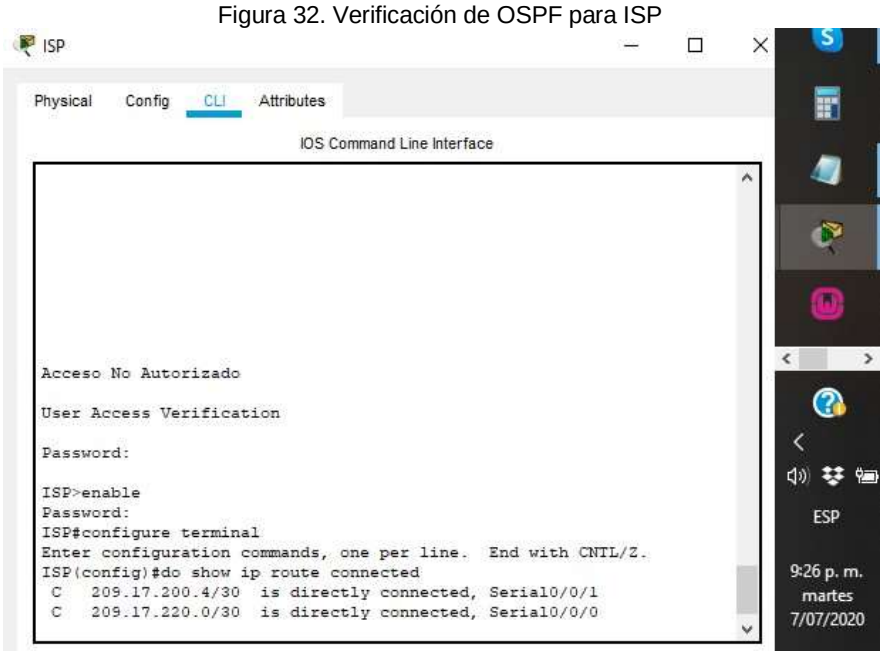
Figura 31. Verificación de OSPF para Medellin1 y Bogota1



Fuente Propia

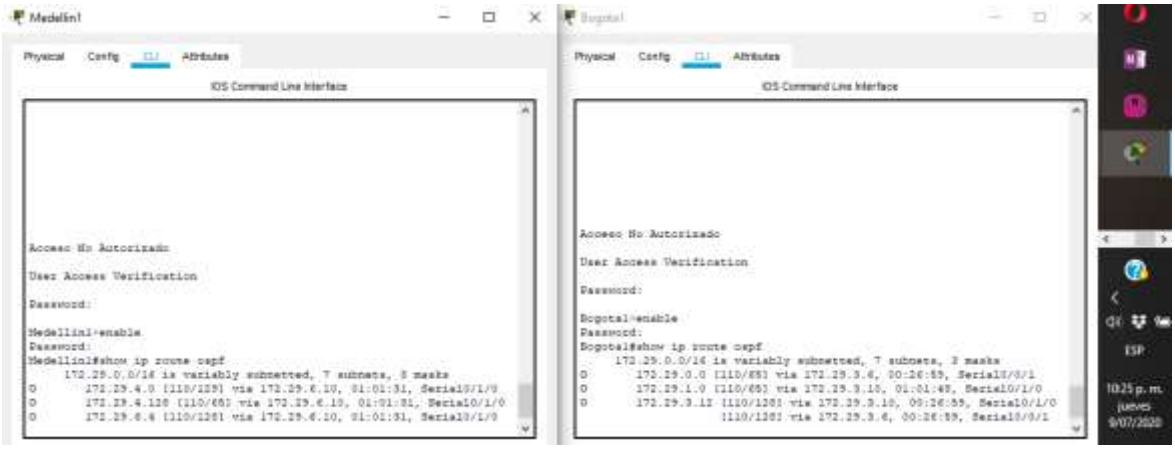
Continuamos con la verificación de la base de datos de OSPF para ISP, Medellin1, Medellin2, Medellin3, Bogota1, Bogota2 y Bogota3. Para esta tarea utilizaremos el comando “do show ip route OSPF”:

Figura 32. Verificación de OSPF para ISP



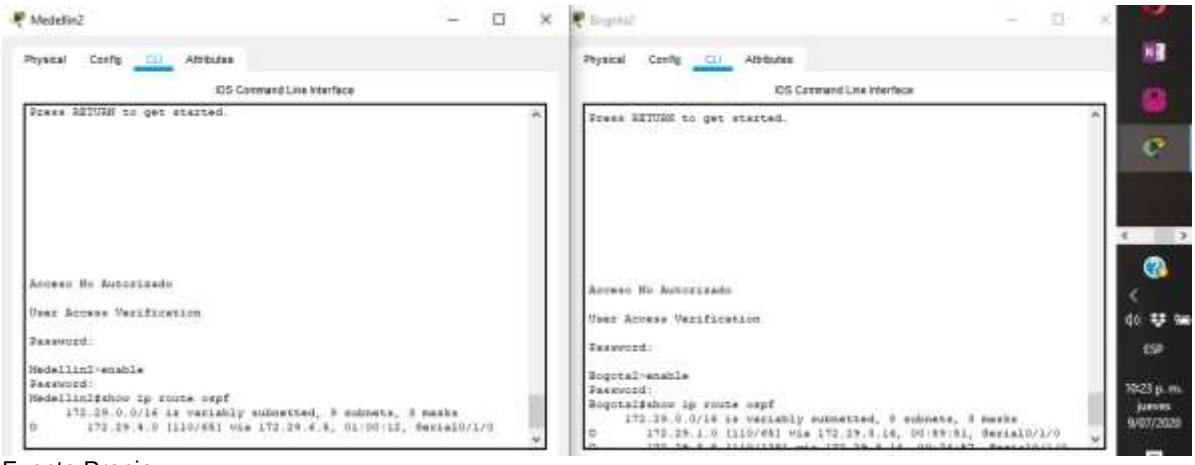
Fuente Propia

Figura 33. Verificación de OSPF para Medellin1 y Bogota1



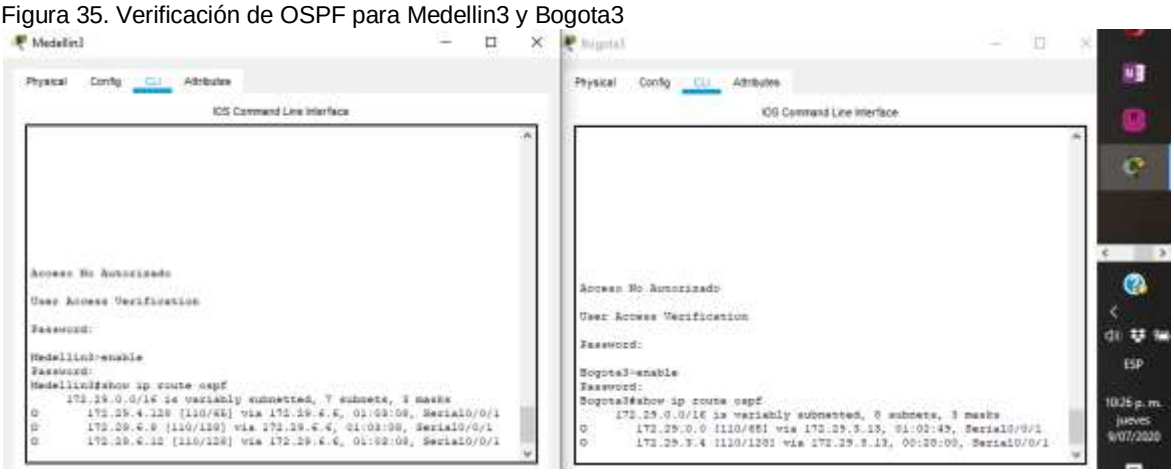
Fuente Propia

Figura 34. Verificación de OSPF para Medellin2 y Bogota2



Fuente Propia

Figura 35. Verificación de OSPF para Medellin3 y Bogota3



Fuente Propia

CONFIGURACIÓN DEL ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

Basados en la topología, debemos configurar el enlace Medellin1 con ISP mediante autenticación PAT.
El enlace Bogota1 con ISP se debe configurar con autenticación CHAP.

Tabla 32. Configuración CHAP Bogota1

Dispositivo	Encapsulación y Autenticación PPP
Medellin1	Medellin1#configure terminal Medellin1(config)#username ISP password cisco Medellin1(config)#int s0/0/0 Medellin1(config-if)#encapsulation ppp Medellin1(config-if)#ppp authentication chap Medellin1(config-if)#encapsulation ppp Medellin1(config-if)#ppp authentication pap Medellin1(config-if)#ppp pap sent-username Medellin1 password cisco
Bogota1	Bogota1#configure terminal Bogota1(config)#username ISP password cisco Bogota1(config)#int s0/0/0 Bogota1(config-if)#encapsulation ppp Bogota1(config-if)#ppp authentication chap
ISP	ISP#configure terminal ISP(config)#username Medellin1 password cisco ISP(config)#int s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config-if)#end
	ISP#configure terminal ISP(config)#username Bogota1 password cisco ISP(config)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap

CONFIGURACIÓN DE PAT.

Con el fin de garantizar la seguridad para cada uno de los dispositivos conectados a la red LAN de Bogotá y Medellín, activaremos la NAT (traducción de direcciones de red). en la salida de los router Medellin1 y Bogota1.
Una vez activamos la NAT, sólo habrá comunicación en la WAN, es decir, entre los routers Medellin1, ISP y Bogota1.
Se debe tener en cuenta la interfaz de salida de cada uno de los routers a configurar para tener conectividad (se realizará verificación con el comando ping entre los 3 routers).

Tabla 33. Configuración NAT de Medellin1 y Bogota1

Router	Configuración
Medellin1	Medellin1#configure terminal Medellin1(config)#ip nat inside source list 1 interface s0/0/0 overload Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255 Medellin1(config)#int s0/1/0 Medellin1(config-if)#ip nat inside Medellin1(config-if)#int s0/0/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#int s0/0/1 Medellin1(config-if)#ip nat inside Medellin1(config-if)#int s0/1/1 Medellin1(config-if)#ip nat inside
Bogota1	Bogota1#configure terminal Bogota1(config)#ip nat inside source list 1 interface s0/1/1 overload Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255 Bogota1(config)#int s0/0/0 Bogota1(config-if)#ip nat inside Bogota1(config-if)#int s0/1/0 Bogota1(config-if)#ip nat inside Bogota1(config-if)#int s0/0/1 Bogota1(config-if)#ip nat inside Bogota1(config-if)#int s0/1/1 Bogota1(config-if)#ip nat outside

CONFIGURACIÓN DEL SERVICIO DHCP.

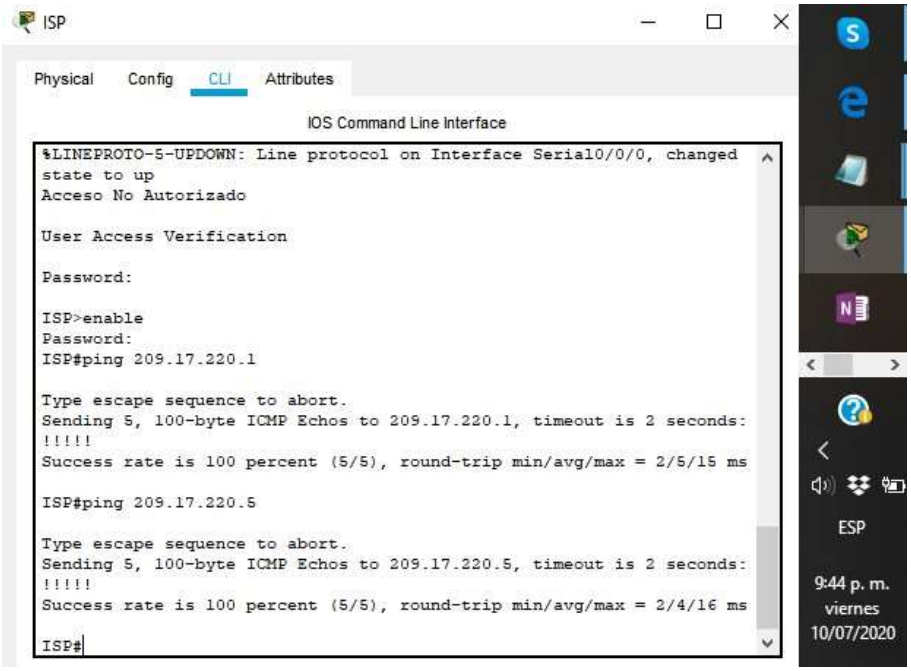
Ahora realizaremos la configuración del protocolo de configuración dinámica de Host o DHCP, para lo cual utilizaremos diversos comandos incluidos en la Tabla 36.
En primer lugar, configuraremos la Red de los routers Medellin2 (para que sea el servidor de las 2 redes LAN y Medellin3 para que habilite el paso de los mensajes de broadcast hacia la ip del servidor.
De igual forma, el router Bogota1 habilitará el paso de los mensajes broadcast hacia el servidor y configuraremos los routers Bogota2 y Bogota3 para que tengan como servidor el router Medellin2.

Tabla 34. Configuración DHCP según requerimientos

Dispositivo	Configuración DHCP
Medellin2	Medellin2#configure terminal Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5 Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.3.133 Medellin2(config)#ip dhcp pool Medellin2 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 8.8.8.8 Medellin2(dhcp-config)#exit Medellin2(config)#ip dhcp pool Medellin3 Medellin2(dhcp-config)#network 172.29.4.1 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.129 Medellin2(dhcp-config)#dns-server 8.8.8.8 Medellin2(dhcp-config)#exit172.29.6.2
Medellin3	Medellin3#configure terminal Medellin3(config)#int g0/0 Medellin3(config-if)#ip helper-address 172.29.6.2
Bogota2	Bogota2#configure terminal Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5 Bogota2(config)#ip dhcp pool Bogota2 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 8.8.8.8 Bogota2(dhcp-config)#ip dhcp pool Bogota3 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 8.8.8.8
	Bogota2#configure terminal Bogota2(config)#int g0/0 Bogota2(config-if)#ip helper-address 172.29.3.13

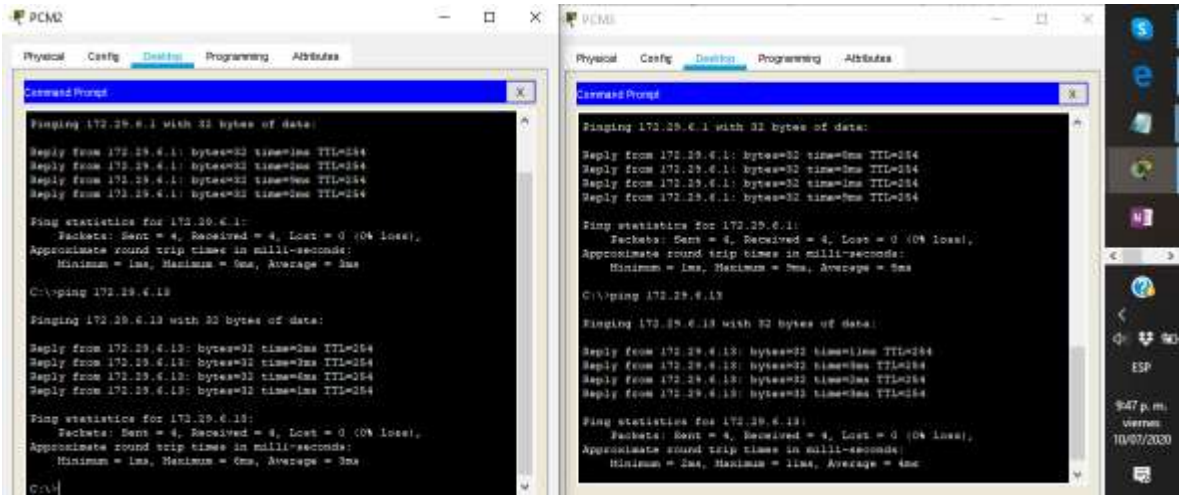
A continuación, realizamos la verificación de conectividad de todos los dispositivos de la red:

Figura 35. Ping ISP



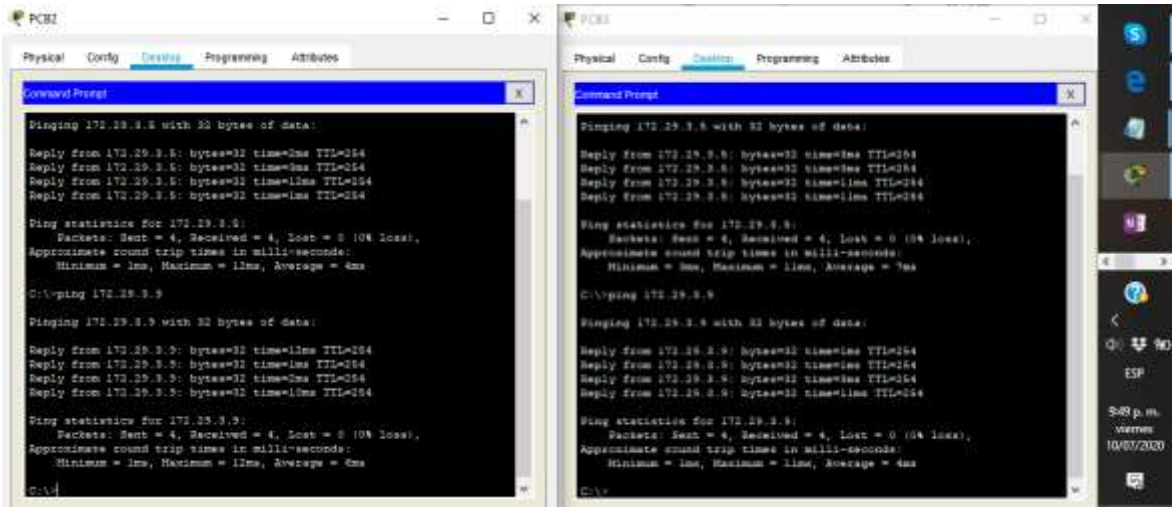
Fuente Propia

Figura 36. Ping PCM2 y PCM3



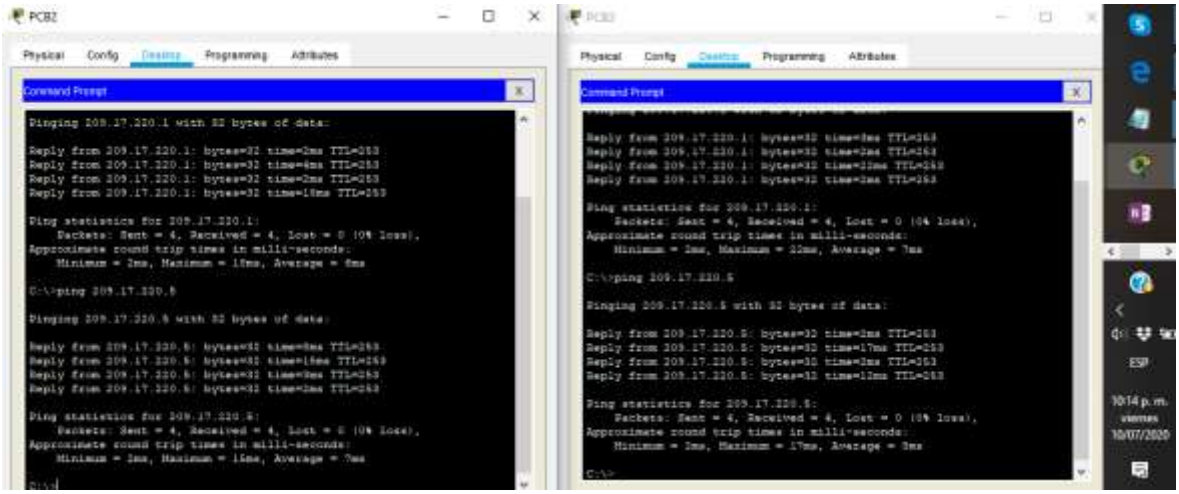
Fuente Propia

Figura 37. Ping PCB2 y PCB3



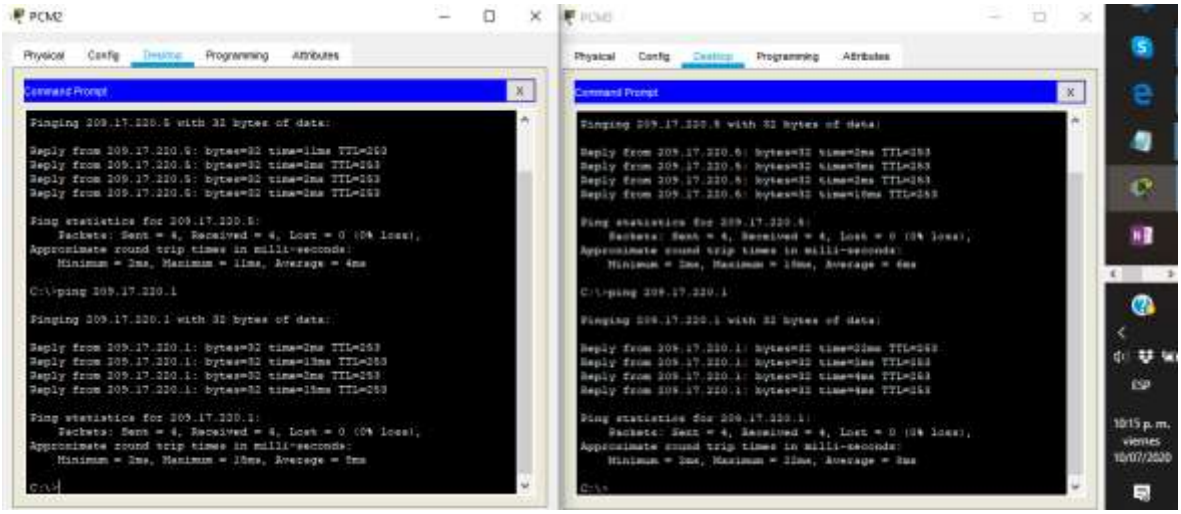
Fuente Propia

Figura 38. Ping PCB2 y PCB3 a Medellin 1 IP pública



Fuente Propia

Figura39. Ping PCM2 y PCM3 a Bogota1 IP pública



Fuente Propia

CONCLUSIONES

- Cuando se crea una red (bien sea física o mediante un simulador como Packet Tracer, utilizado en este proyecto), se debe verificar la cantidad de puertos seriales que poseen los routers y en caso de requerir adicionales, insertarlas previamente para agilizar la configuración de las conexiones con otros dispositivos.

- A la hora de elegir rutas predeterminadas a seguir por los routers, es fundamental tener en cuenta las direcciones IP asignadas a cada dispositivo, máscaras de subred y los puertos mediante los cuales se realizará la conexión, para evitar demoras y fallas en la comunicación de los dispositivos.

- El direccionamiento mediante PAT y PPP nos permite optimizar el direccionamiento IP de los dispositivos que componen la red (mediante el uso de IPs públicas y privadas), garantizando la seguridad en los datos compartidos por sus usuarios.

- Una forma de garantizar la seguridad en el acceso a los dispositivos de la red es mediante el uso de contraseñas de acceso, para ello es necesario utilizar protocolos de autenticación PAP y CHAP.

BIBLIOGRAFÍA

Barbosa, R. (2016, 2 agosto). Rutas Estáticas (Enrutamiento estatico), la magia que hace posible el ruteo. SeaCCNA. Recuperado de: https://seaccna.com/rutas-estaticas-enrutamiento-estatico/

Colaboradores de Wikipedia. (s. f.-a). Point-to-Point Pr - Wikipedia, la enciclopedia libre. Tomado de Wikipedia. https://es.wikipedia.org/wiki/Point-to-Point_Pr

Colaboradores de Wikipedia. (s. f.-b). Port address translation. Recuperado de Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Port_address_translation

Colaboradores de Wikipedia. (2019a, julio 30). CHAP. Recuperado de Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/CHAP#:%7E:text=CHAP%20es%20un%20protocolo%20de,usuario%20frente%20a%20un%20ISP.

Colaboradores de Wikipedia. (2019b, agosto 27). Lista de control de acceso. Recuperado de Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Lista_de_control_de_acceso

Colaboradores de Wikipedia. (2020, 21 junio). IPv4. Recuperado de Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/IPv4

NAT (Network Address Translation. (2020, 9 junio). Tomado de Wikipedia. https://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red

Sumarización de rutas. (s. f.). Recuperado de Wikipedia. http://librosnetworking.blogspot.com/2009/08/sumarizacion-de-rutas.html

“NAT para IPv4”. CISCO (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

“Listas de Control de Acceso”. CISCO (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

ANEXOS

Enlace One Drive con archivos ejecutables de los 2 escenarios en Packet Tracer.