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

CRISTIAN ARMANDO CASTILLA MARROQUIN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
FACULTAD DE INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO
IBAGUE-JULIO
2020

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

CRISTIAN ARMANDO CASTILLA MARROQUÍN

Diplomado de opción de grado para obtener el título de Ingeniero de Sistemas

Asesor:
Gustavo Adolfo Rodríguez
Ingeniero Informático

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
IBAGUE TOLIMA
2020

RESUMEN

En este proyecto de grado, se verá evidenciado el conocimiento y aprendizaje durante todo el curso de DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), mediante los escenarios 1 y 2 propuestos en la guía prueba de habilidades CCNA, por medio de este trabajo se pondrán a prueba las habilidades y el nivel de comprensión para dar solución a las diferentes configuraciones de cada dispositivo, como los protocolos de enrutamiento, comunicación mediante enlaces trocales, acceso a SSH, DHCP, NAT, mediante la simulación de escenarios en la herramienta Packet Tracer esto con el fin de prepararnos para tener más conocimientos, respecto al proceso técnico del área de sistemas.

ABSTRACT

In this degree project, you will see evidence of knowledge and learning throughout the CISCO DEPTH DIPLOMA course (DESIGN AND IMPLEMENTATION OF INTEGRATED LAN / WAN SOLUTIONS), through scenarios 1 and 2 proposed in the CCNA skills test guide, Through this work, the skills and level of understanding will be tested to solve the different configurations of each device, such as routing protocols, communication through trunks, access to SSH, DHCP, NAT, through the simulation of movements in the Packet Tracer tool this in order to prepare us to have more knowledge regarding the technical process of the systems area.

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Ibagué, 10 de junio de 2020

DEDICATORIA

Primeramente, este trabajo final se lo dedico a DIOS quien destino como propósito para mi vida, ser un Ingeniero de sistemas, quien me dio el entendimiento, la sabiduría, la salud y la constancia para resolver cada una de las actividades propuestas en este curso, en segundo lugar, a mis padres que siempre estuvieron conmigo, en general a toda mi familia y a mi novia que son los que me motivan día a día y me dan la fuerza de seguir luchando por mis sueños, y nunca me dejaron solo.

AGRADECIMIENTOS

En esta actividad quiero agradecerle a Dios quien es el que nos da la oportunidad tanto a mi como a todos de cumplir nuestros propósitos, también quiero aprovechar para brindar mis agradecimientos a los tutores que estuvieron en el transcurso de mi camino, a mis compañeros y amigos que estuvieron brindándome y compartiendo sus conocimientos opinando, corrigiendo y brindando su apoyo de acuerdo a su experiencia y conocimiento, la cual fue de gran significancia e importancia para realizar este trabajo.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

TABLA DE FIGURAS

Pág.

TABLA DE ANEXOS

Pág.

INTRODUCCIÓN

Internet es una parte esencial del mundo de hoy, porque podemos comunicarnos con ellos, y podemos mantener una conversación a distancia con nuestra familia, utilizándolos para el trabajo y otros servicios que benefician nuestro trabajo diario. En esta parte de Cisco, encontramos 4 unidades en las que nos enseñaron herramientas sobre formas y métodos de uso, y cómo usarlo de manera que nos beneficie. Satisfaga las necesidades de la red más amplia. También puede escalar bien en implementaciones de redes grandes.

En este trabajo, veremos estos protocolos y su importancia y características para enviar paquetes en la red, así como su configuración y otras cualidades y beneficios, como los observados por los protocolos de enrutamiento dinámico, al igual reconocer, entre otras características, la diferencia entre el enrutamiento de vector de distancia y el enrutamiento de estado de enlace, y cómo los enrutadores usan estos protocolos para determinar la ruta más corta a cada red y cómo implementan los protocolos de enrutamiento. El proveedor de estado de enlace envía información sobre su estado de enlace a otros enrutadores en el dominio de enrutamiento (es decir, redes conectadas directamente), incluida información sobre el tipo de red y los enrutadores vecinos en esas redes.

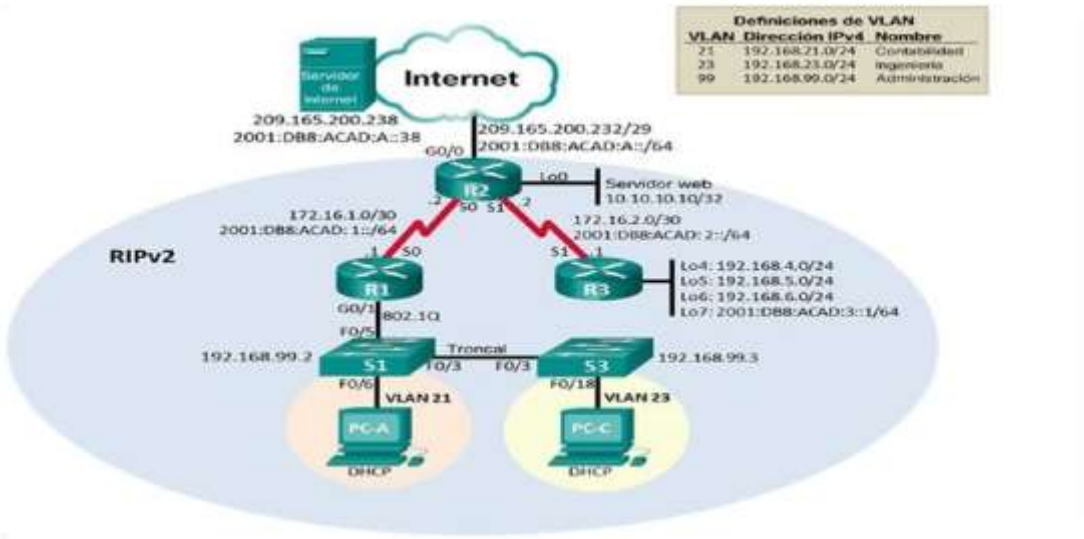
DESARROLLO DE LOS ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1 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.
Según la observación de la guía en este escenario se realizarán diferentes configuraciones que permitan la conectividad IPv4, como también IPv6, se implementara comandos para poner seguridad a los diferentes dispositivos, como también se llevara a cabo los diferentes comandos de DHCP, NAT, ACL

1.1 TOPOLOGIA

Figura 1 - Topología escenario 1



Fuente propia

1.2 PARTE 1: INICIALIZAR DISPOSITIVOS.

1.2.1 PASO 1: INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES

Se realizarán las configuraciones iniciales de cada uno de los dispositivos, para esto se tendrá que borrar la información que había, para comenzar a utilizar los comandos relacionados en la tabla 1.

Tabla 1 - comandos IOS

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	S1#Erase startup-config
Volver a cargar todos los routers	S1#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	S1#Erase startup-config S1#Delete flash:valn.dat
Volver a cargar ambos switches	S1#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	S!#Show vlan brief

1.3 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

1.3.1 PASO 1: CONFIGURAR LA COMPUTADORA DE INTERNET

Se configurarán de acuerdo a las direcciones IP que nos brinda la Topología de red, que se encuentra en la imagen 1, para cada uno de los routers, switches, servidores de internet y pc, como se muestra en la tabla número 2.

Tabla 2 – Configuración de la computadora 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	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

1.3.2 PASO 2: CONFIGURAR R1

Después de haber iniciado cada dispositivo y haber configurado los parámetros básicos, iniciaremos con la configuración de cada router, según lo estipulado en la Topología de red, en la cual deberemos modificar la configuración básica de un router donde esta incluye: poner nombre al router para poder localizarlo directamente por su nombre, también pondremos contraseñas para entrar por el exec privilegiado, con el fin de que solo las personas autorizadas puedan ingresar a esta información, también añadiremos el mensaje de banner motd para crear un aviso a las personas que no están autorizadas, luego estableceremos las direcciones IP de acuerdo a lo estipulado en la Topología.

Tabla 3 - Configuración R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	Router# Router(config)#hostname R1 R1(config)#exit
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1(config)#exit
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#exit
Mensaje MOTD	R1#config term R1(config)# banner motd # Se prohíbe el acceso no autorizado # R1(config)# exit

Interfaz S0/0/0	R1(config)#Interface s0/0/0 R1(config)#ip address 172.16.1.1 255.255.255.252 R1(config)#clock rate 128000 R1(config)#no shutdown R1(config)#exit R1(config)#interface s0/0/0 R1(config)#ipv6 enable R1(config)#ip address 2001:db8:acad:1::1/64 R1(config)#clock rate 12800 R1(config)#no shutdown
Rutas predeterminadas	R1(config)#interface serial 0/0/0 R1(config-if)#ip address 0.0.0.0 0.0.0.0 R1(config-if)#exit Configurar una ruta Ipv6 predeterminada de S0/0/0 R1(config)#interface Serial0/0/0 R1(config-if)#ipv6 address ::/0 R1(config-if)#exit

Nota: Todavía no configure G0/1.

1.3.3 PASO 3: CONFIGURAR R2

En este paso se realizará lo mismo que en el paso 2, configurando la información como lo indica la topología, como desactivar la búsqueda de DNS, cambiar nombre del router, ingresar la contraseña para entrar en modo privilegiado el mensaje motd, y todas las configuraciones que se aplicaron en el paso anterior.

Tabla 4 -Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class R2(config)#exit
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#end
Contraseña de acceso Telnet	R2(config)#line vty 0 4

	R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2#config term R2(config)#service password-encryption R2(config)#exit
Habilitar el servidor HTTP	No se puede configurar este comando
Mensaje MOTD	R2#config term R2(config)#banner motd # Se prohíbe el acceso no autorizado # R2(config)#exit
Interfaz S0/0/0	R2(config)#Interface s0/0/0 R2(config)#ip address 172.16.1.2 255.255.255.252 R2(config)#clock rate 128000 R2(config)#no shutdown R2(config)#exit R2(config)#interface s0/0/0 R2(config)#ipv6 enable R2(config)#ip address 2001:db8:acad:1::2/64 R2(config)#clock rate 12800 R2(config)#no shutdown
Interfaz S0/0/1	R2(config)#interface s0/0/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#no shutdown R2(config)#interface s0/0/1 R2(config-if)#ipv6 enable R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#interface g0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 Bad mask /29 for address 209.165.200.232 R2(config-if)#no shutdown R2(config-if)#exit R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit

Ruta predeterminada	R2(config)# interface G0/0 R2(config)# ip route 0.0.0.0 0.0.0.0 G0/0 R2(config)# exit R2(config)# interface G0/0 R2(config)# ipv6 route ::/0 G 0/0 R2(config)# exit

1.3.4 PASO 4: CONFIGURAR R3

En este paso al igual que en los dos pasoso anteriores se realizaran las configuraciones básicas con la información que nos brinda la Topología del escenario 1 se volverán a realizar cada una de las configuraciones que se les hizo a los routers R1 y R2 con la información que nos brinda la topología.

Tabla 5 - configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd %Se prohibe el acceso no autorizado!%
Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown R3(config-if)#exit

	R3(config)#interface s0/0/1 R3(config-if)# ipv6 enable R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown R3(config-if)#exit
Interfaz loopback 4	R3(config)#interface looback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface looback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface looback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface looback 7 R3(config-if)#ipv6 addres 2001:DB8:ACAD:3::1/64 R3(config-if)#exit

1.3.5 PASO 5: CONFIGURAR S1

En este paso configuraremos cada Switch con su respectivo nombre, como se indicó anteriormente, esto con el fin de identificar cada dispositivo, igualmente se podrán las contraseñas de seguridad, los textos de banner motd para poner en aviso a las personas que quiera entrar sin la autorización.

Tabla 6 - configuración S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S1 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 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd # Se prohíbe el acceso no autorizado # S1(config)#exit

1.3.6 PASO 6: CONFIGURAR EL S3

En este paso también se harán las configuraciones básicas correspondientes, como cambiar el nombre, poner contraseñas para ingresar en modo cifrado, todo esto con el fin de tener mayor seguridad y dinamismo al realizar las configuraciones siguientes que solicita la guía de actividades.

Tabla 7- Configuración S3

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

Mensaje MOTD	S3(config)#banner motd %Se prohibe el acceso no autorizado!%

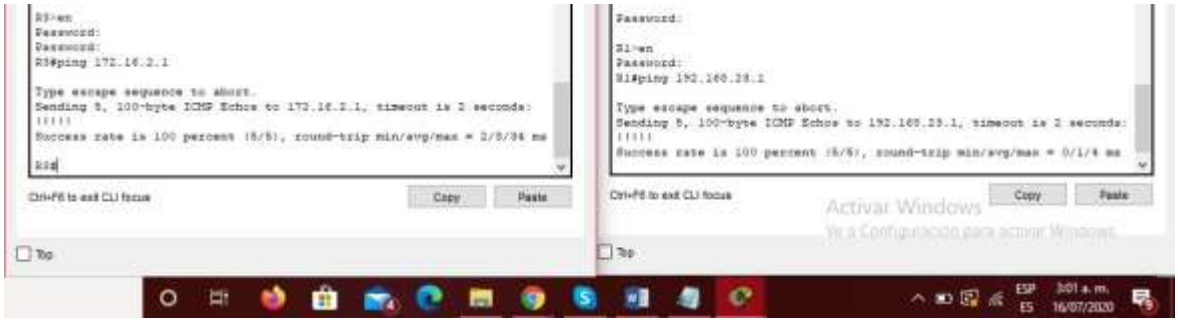
1.3.7 PASO 7: VERIFICAR LA CONECTIVIDAD DE LA RED.

El uso del comando ping es de suma importancia en la herramienta de Packet Tracer, ya que esta nos brinda la seguridad de verificar si las configuraciones que se hacen a los diferentes dispositivos queden, como se observa en la tabla 8 – verificar la conectividad, se puede observar que el direccionamiento IP quedo bien y se evidencian en las figuras 2 y 3.

Tabla 8 - Verificar la conectividad de la red

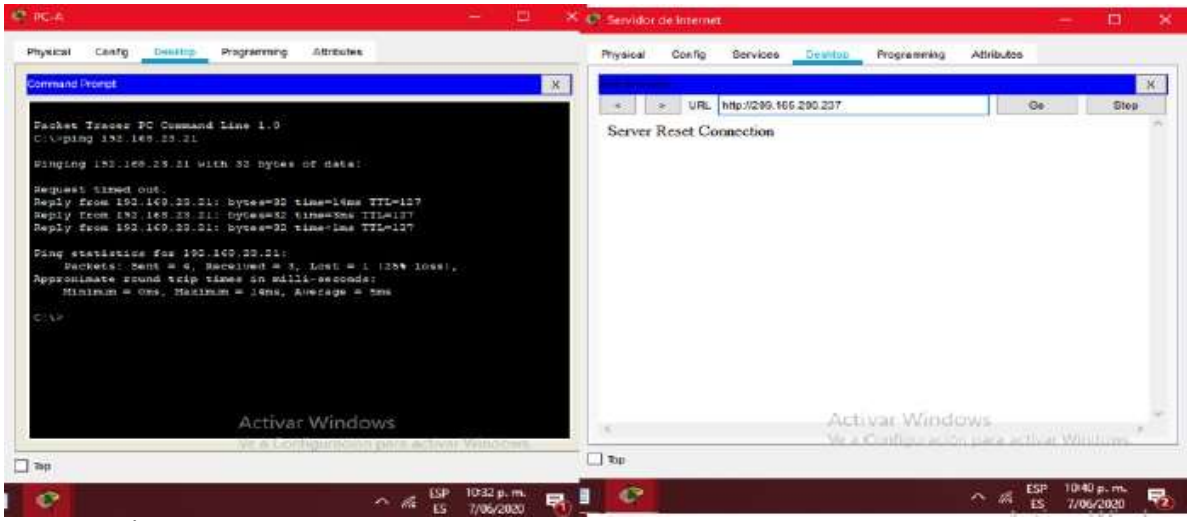
Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1
PC de Internet	Gateway predeterminado	209.165.200.233	Packet Tracer SERVER Command Line 1.0 C:\>ping 209.165.200.233

Figura 2 - resultados ping



Fuente propia

Figura 3 - verificación en la PC-A y el servidor de internet



Fuente propia.

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

1.4 PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

1.4.1 PASO 1: CONFIGURAR S1

En este paso se configurará la seguridad de cada switch, de las VLAN, para esto se debe la base de datos de la Vlan, Las VLAN son un mecanismo para permitir que los administradores de red creen dominios de broadcast lógicos que pueden abarcar un solo switch o varios switches múltiples, sin importar la proximidad física. Esta función es útil para reducir los tamaños de los dominios de broadcast o para permitir que los grupos o los usuarios se agrupen lógicamente sin necesidad de estar situados físicamente en el mismo lugar, también se configurara el direccionamiento de IP.

Tabla 9 - Configuración S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S1(config)#VLAN 21 S1(config-vlan)#name contabilidad S1(config-vlan)#VLAN 23 S1(config-vlan)#name ingieneria S1(config-vlan)#VLAN 99 S1(config-vlan)#name administracion

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
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	Utilizar la red VLAN 1 como VLAN nativa 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 S1(config-if-range)#
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

1.4.2 PASO 2: CONFIGURAR EL S3

En este paso se hará lo mismo que en el paso anterior se crearan bases de datos en la VLAN, en este caso VLAN 21 se llamara contabilidad, VLAN 2 Ingeniería y VLAN 99 administración, y la demás información que brinda la topología.

Tabla 10 - Configuración S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S3(config)# 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 S3(config-if)#
Asignar la dirección IP de administración	S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
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 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 21
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

1.4.3 PASO 3: CONFIGURAR R1

En R1 se configurarán las diferentes subinterfaces dándoles direcciones IP, en cada VLAN

Tabla 11 - Configuración R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	(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 Asignar la VLAN 23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23

	Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración R1(config-subif)#int g0/1.99 Asignar la VLAN 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

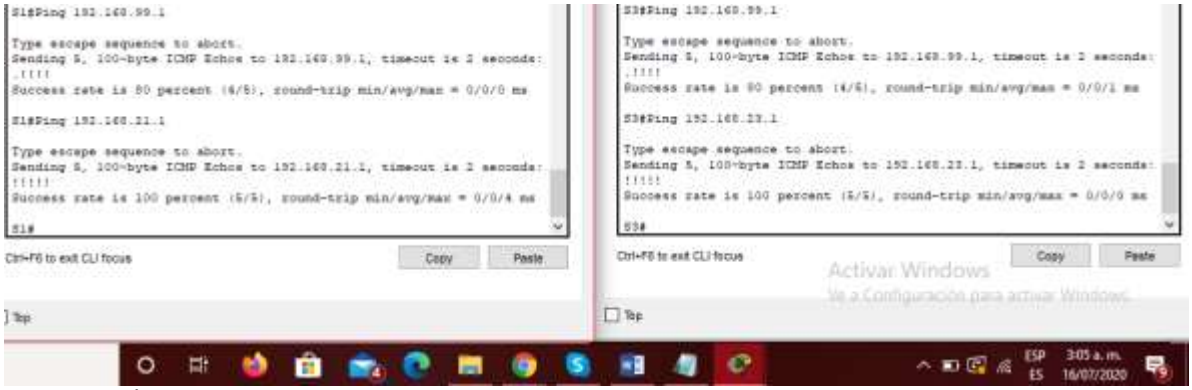
1.4.4 PASO 4: VERIFICAR LA CONECTIVIDAD DE LA RED

Como se puede observar se vuelve a utilizar el comando ping en los 2 switchs, para confirmar que el direccionamiento a las diferentes VLAN estén correctas

Tabla 12 - Verificación de red

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 4 – comando ping verificación de switchs.



Fuente propia.

1.5 PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

1.5.1 PASO 1: CONFIGURAR RIPV2 EN EL R1.

A continuación, se configurará el protocolo de routing dinamico RIPv2, después de hacer esta configuración se observarán las redes conectadas directamente y luego se establecerán las interfaces LAN como pasivas.

Tabla 13 - Configuración de RIPv2 en R1

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route connected 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 R1(config-router)#exit

1.5.2 PASO 2: CONFIGURAR RIPV2 EN EL R2.

En El Protocolo de Información de Encaminamiento o Routing Information Protocol RIP se utiliza por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados en este caso esto se hara en el R2.

Tabla 14 - Configuraciónn RIPv2 en 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	R2(config-router)#do show ip route connected 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

1.5.3 PASO 3: CONFIGURAR RIPV2 EN EL R3.

Se vuelve a emplear la configuración de RIPv2, para anunciar las IPv4 directamente conectadas.

Tabla 15 - configuraciòn RIPv3 en 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 172.16.4.0 R3(config-router)#network 172.16.5.0 R3(config-router)#network 172.16.6.0

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 R3(config-router)#no auto summary
Desactive la sumarización automática.	R3(config-router)#no auto summary

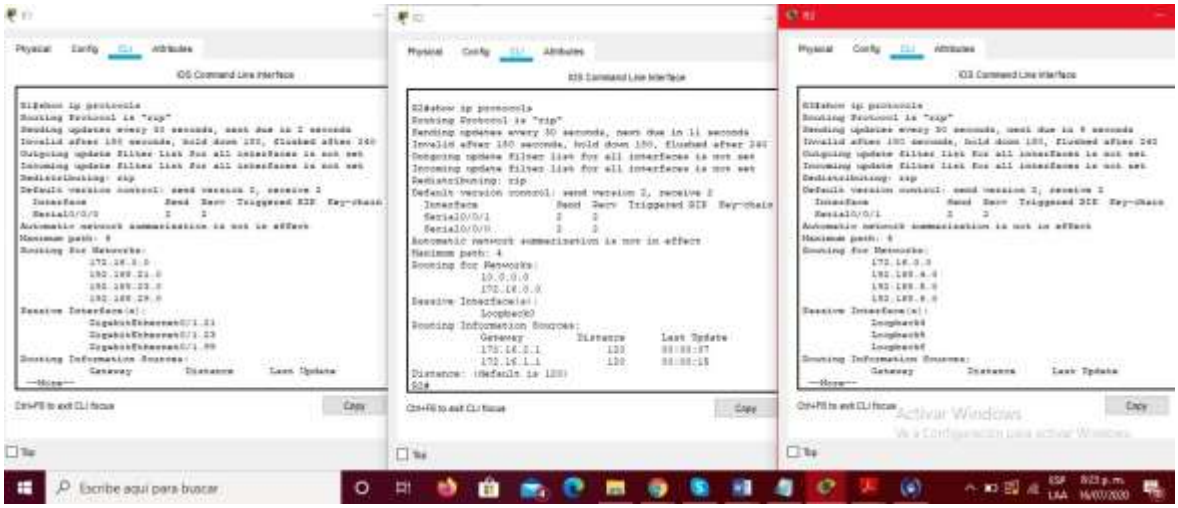
1.5.4 PASO 4: VERIFICAR LA INFORMACIÓN DE RIP

Mediante los protocolos de verificación se determinaran si la información configurada anteriormente es correcta.

Tabla 16 - Verificación de RIP

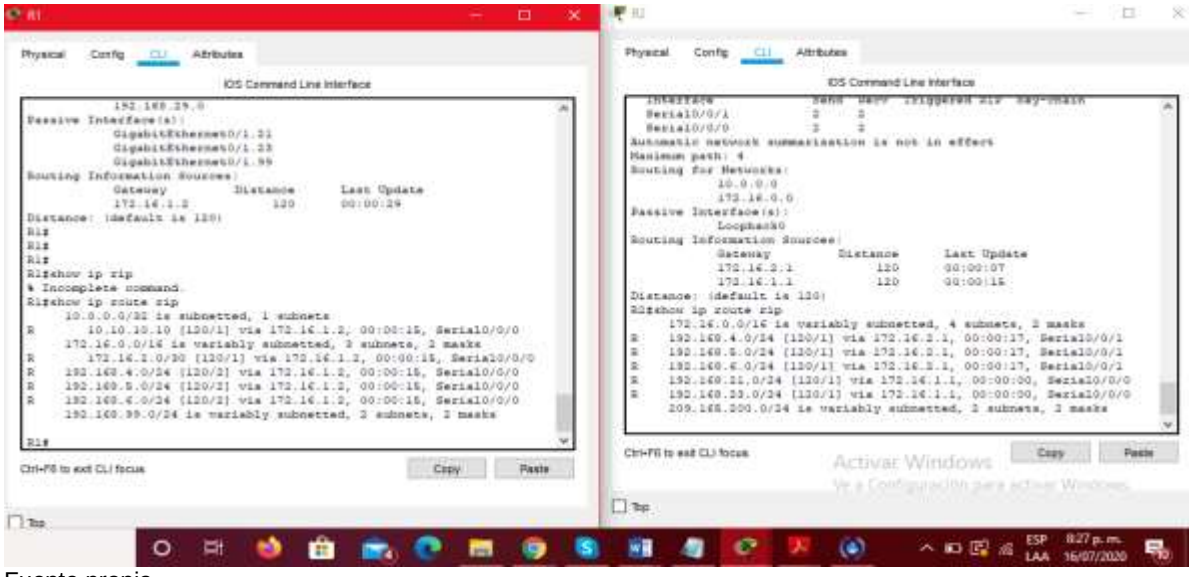
Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas RIP?	show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show run

Figura 5 - show ip proptocols en R1, R2, R3.



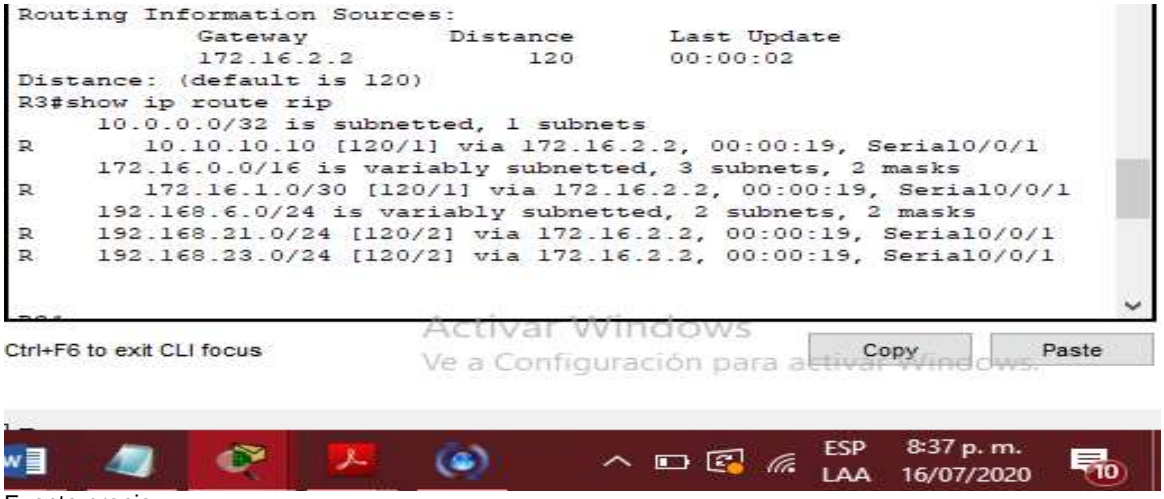
Fuente propia.

Figura 6 - show ip route rip



Fuente propia.

Figura 7 - show ip route rip



Fuente propia.

1.6 PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

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

DHCP es un servicio que permite configurar los parámetros de TCP/IP, como la dirección IP y la máscara de subred en los clientes (PC, computadora portátil, impresora, etc.) automáticamente. También se puede configurar en un router o switch que es lo que vamos hacer a continuación.

Tabla 17 - Configuarción en R1 como servidor

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#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 R1(dhcp-config)#exit
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 R1(dhcp-config)#exit

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

En este paso se configurará una base de datos local con una cuenta de usuario, donde se habilitará el servicio de servidor HTTP, luego se creará una NAT estática al servidor WEB, se asignará la interfaz interna y externa para la NAT, se definirá el pool y la NAT dinámica.

Tabla 18 - configuración de la NAT en R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No se puede configurar este comando en Packet Tracer

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	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 192.168.99.0 0.0.0.255 R2(config)#exit
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** 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 R2(config-if)#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.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.233 – 209.165.200.236** 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

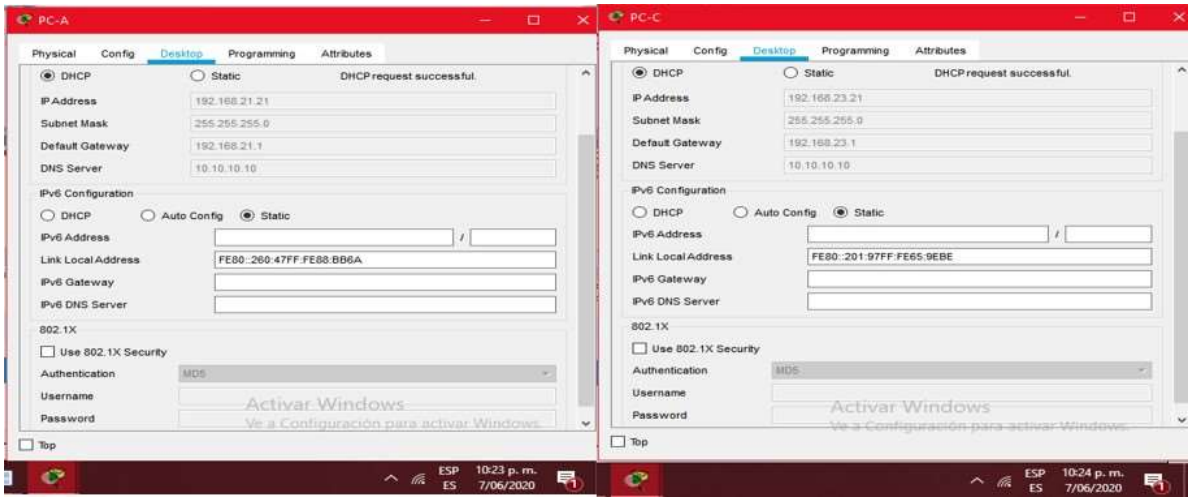
1.6.3 PASO 3: VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA

Se verificara por medio de los protocolos si DHCP y la NAT estática, quedaron configuradas correctamente configuradas.

Tabla 19 - Protocolo DHCP y la NAT estática

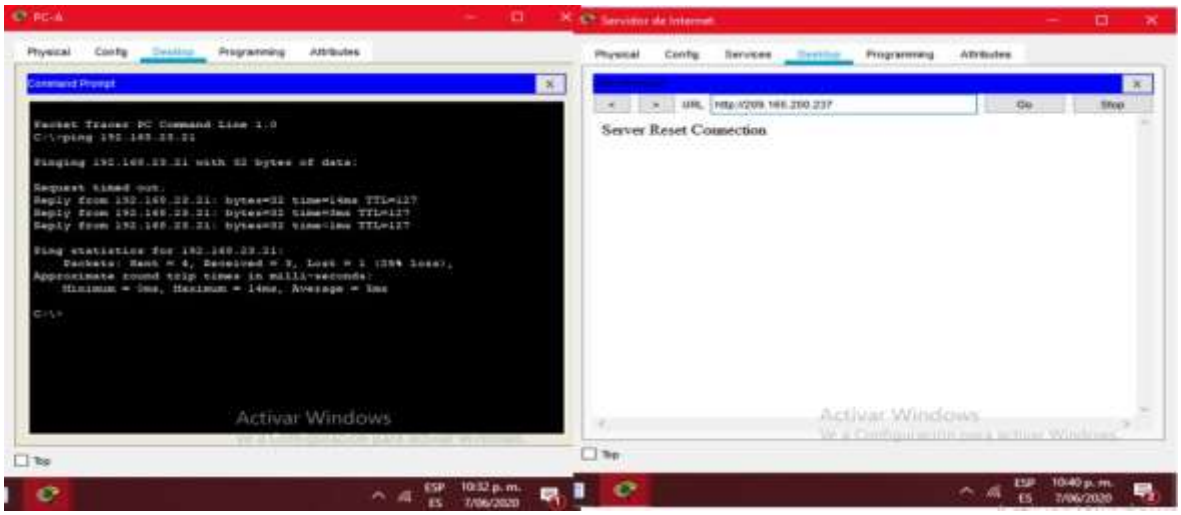
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	PC-A, Desktop, DHCP. IP Address 192.168.21.21 Subnet Mask 255.255.255.0 Default Gateway 192.168.21.1 DNS Server 10.10.10.10 Link local Address FE80::260:47FF:FF88:BB6A
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	PC-A, Desktop, DHCP. IP Address 192.168.23.21 Subnet Mask 255.255.255.0 Default Gateway 192.168.23.1 DNS Server 10.10.10.10 Link local Address FE80::201:97FF:FF65:9EBE
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Ping 192.168.23.21
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**	Servidor internet, Desktop, Web Browser, WRL: http://209.165.200.237

Figura 8 - Verificación PC-A, PC-C



Fuente propia.

Figura 9 - ping en PC-A y verificación del servido de internet



Fuente propia

.

1.7 PARTE 6: CONFIGURAR NTP

Se configurará en R1 y R2 la fecha y hora, se configurará en R2 un NTP, R1 se configurará como un cliente NTP, se configurará en R1 actualizaciones de calendario con hora NTP.

Tabla 20 - Configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 10:48:00 07 june 2020
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#NTP master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	Conf term Ntp server 172.16.1.1. Ntp update-calendar End

Figura 10 - Show ntp associations

Fuente propia.

1.8 PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

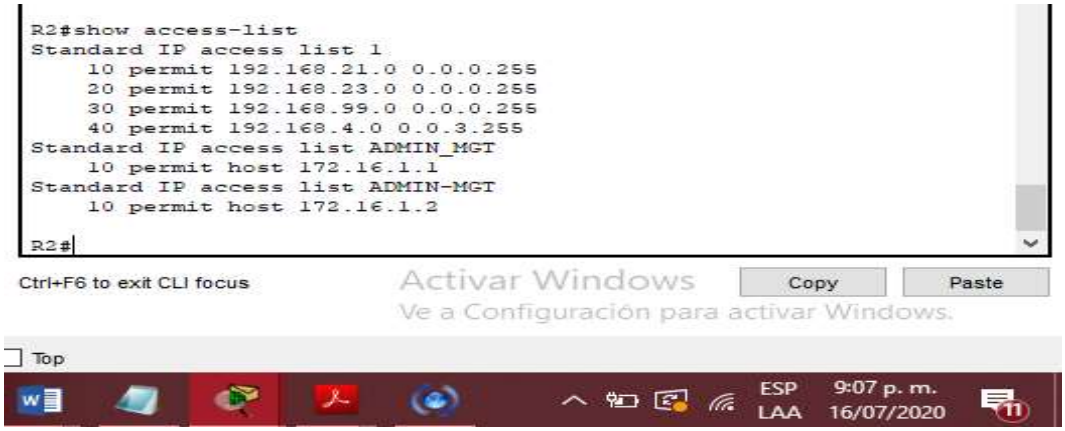
1.8.1 Paso 1: Restringir el acceso a las líneas VTY en el R2

Restringir el acceso a VTY es una configuración que permite definir las diferentes direcciones IP, a las que se les permite acceder por Telnet al proceso de EXEC del router.

Tabla 21 - Restringir el acceso a líneas VTY en R2

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

Figura 11 - Show access-list



Fuente propia.

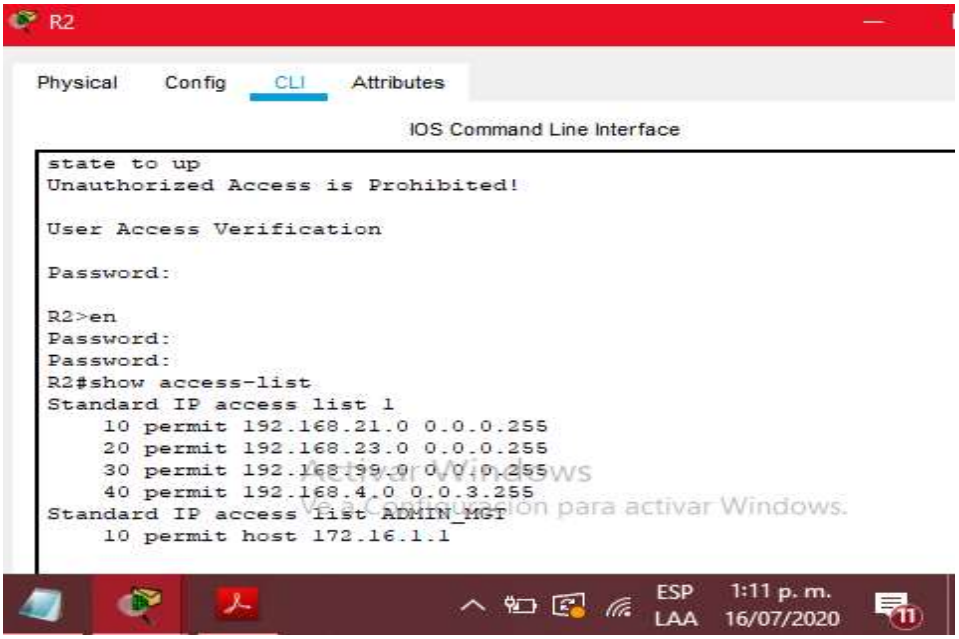
1.8.2 PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

en la tabla 22 – comandos de CLI, se dará respuesta a las preguntas sobre que comandos se deben utilizar correctamente para acceder a la información solicitada.

Tabla 22 - comandos de CLI

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
Restablecer los contadores de una lista de acceso	R2(config)#no access-list 10
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show access-list 1
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

Figura 12 - show access list

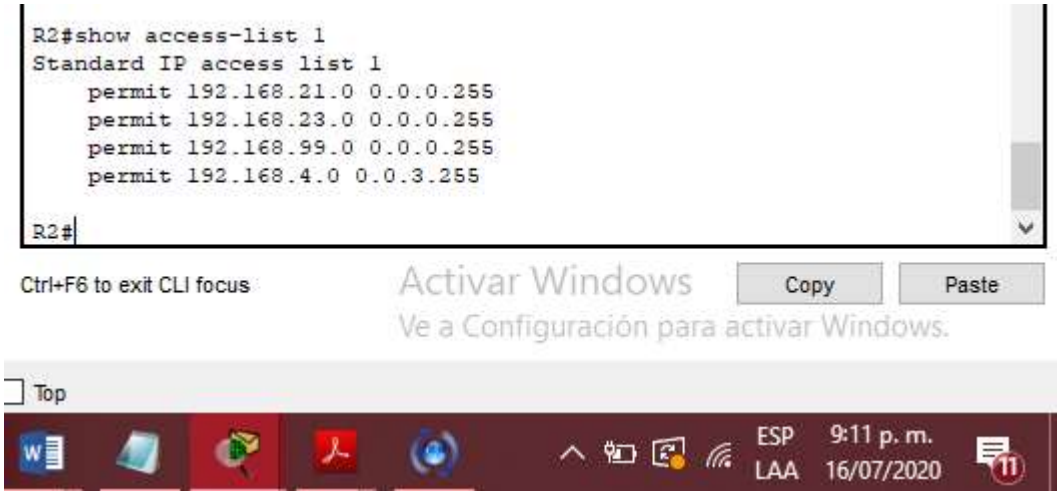


Fuente propia

Figura 13 - Show ip nat translations

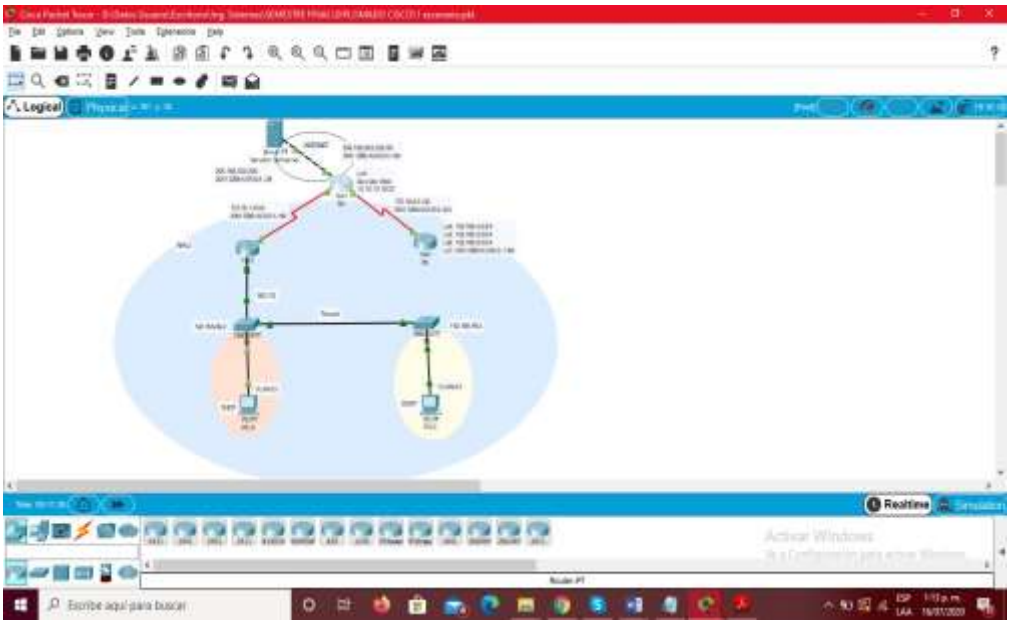
Fuente propia.

Figura 14 - Show access-list 1



Fuente propia.

Figura 15 - escenario final



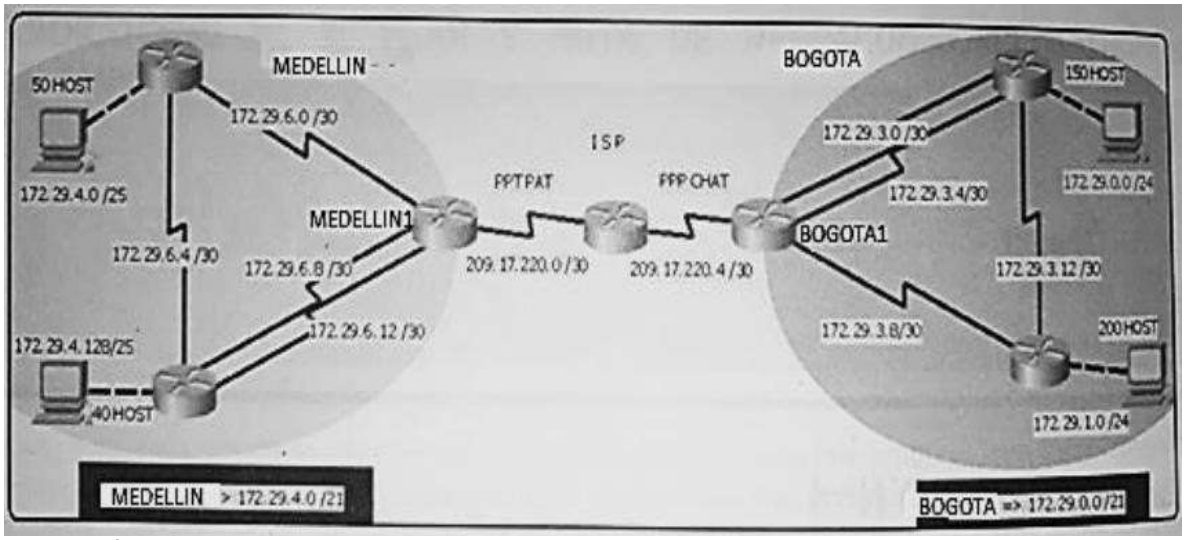
Fuente propia.

2 ESCENARIO 2.

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

2.1 TOPOLOGÍA DE RED

Figura 16 - Topología escenario 2



Fuente guía prueba de habilidades CCNA 2020

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

2.2 DESARROLLO

2.2.1 REALIZAR LAS RUTINAS DE DIAGNÓSTICO Y DEJAR LOS EQUIPOS LISTOS PARA SU CONFIGURACIÓN (ASIGNAR NOMBRES DE EQUIPOS, ASIGNAR CLAVES DE SEGURIDAD, ETC).

A continuación, se expondrá la configuración básica de un router, se iniciara dando identificación a los routers que pertenecen a una red esto con el fin de identificar cada router por su nombre, ya que esto nos ayuda a llevar un mejor orden y las posibilidades de confundiros con los dispositivos serian menos esto se hace con el comando hostname, seguido a esto se configurara una contraseña para entrar modo exec privilegiado para evitar que personas que no están autorizadas, configuren nuestros dispositivos, esto lo hacemos por el comando de configuración terminal (conf term) seguido enable secret “contraseña”, el comando login es el que verificara si quedo la contraseña o no.
Luego de esto configuraremos el mensaje ya que esta es una buena idea de seguridad se recomienda no dar la bienvenida en el mensaje, para hacer esta configuración se utiliza el comando banner motd y seguido a esto el mensaje, ejemplo: banner motd #Prohibido el acceso no autorizado por Cristian Castilla#.

Tabla 23 - Configuración Basica

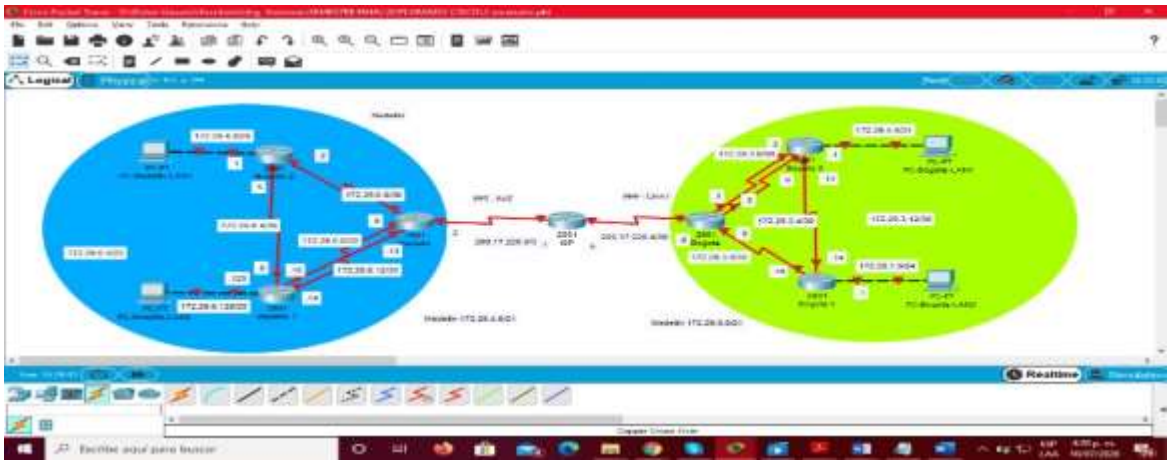
Dispositivo	Configuración Basica
Medellin	Router(config)#hostname Medellin Medellin(config)#enable secret class Medellin(config)#line console 0 Medellin(config-line)#password cisco Medellin(config-line)#login Medellin(config-line)#exit Medellin(config)#line vty 0 15 Medellin(config-line)#password cisco Medellin(config-line)#login Medellin(config-line)#service password-encryption Medellin(config)#banner motd #Prohibido el acceso no autorizado por Cristian Castilla Marroquin!# Medellin(config)#end
Medellin1	Medellin1(config)#hostname Medellin1 Medellin1(config)#enable secret class Medellin1(config)#line console 0 Medellin1(config-line)#password cisco Medellin1(config-line)#login Medellin1(config-line)#exit Medellin1(config)#line vty 0 15

	Medellin1(config-line)#password cisco Medellin1(config-line)#login Medellin1(config-line)#service password-encryption Medellin1(config)#banner motd #Prohibido el acceso no autorizado por Cristian Castilla Marroquin!# Medellin1(config)#end
Medellin2	Router(config)#hostname Medellin2 Medellin2(config)#enable secret class Medellin2(config)#line console 0 Medellin2(config-line)#password cisco Medellin2(config-line)#login Medellin2(config-line)#exit Medellin2(config)#line vty 0 15 Medellin2(config-line)#password cisco Medellin2(config-line)#login Medellin2(config-line)#service password-encryption Medellin2(config)#banner motd #Prohibido el acceso no autorizado por Cristian Castilla Marroquin!# Medellin2(config)#end
Bogota	Router(config)#hostname Bogota Bogota(config)#enable secret class Bogota(config)#line console 0 Bogota(config-line)#password cisco Bogota(config-line)#login Bogota(config-line)#exit Bogota(config)#line vty 0 15 Bogota(config-line)#password cisco Bogota(config-line)#login Bogota(config-line)#service password-encryption Bogota(config)#banner motd #Prohibido el acceso no autorizado por Cristian Castilla Marroquin!# Bogota(config)#end Bogota#
Bogota1	Router(config)#hostname Bogota1 Bogota1(config)#enable secret class Bogota1(config)#line console 0 Bogota1(config-line)#password cisco Bogota1(config-line)#login Bogota1(config-line)#exit Bogota1(config)#line vty 0 15 Bogota1(config-line)#password cisco Bogota1(config-line)#login Bogota1(config-line)#service password-encryption

	Bogota1(config)#banner motd #Prohibido el acceso no autorizado por Cristian Castilla Marroquin!# Bogota1(config)#end
Bogota2	Router#conf term Enter configuration commands, one per line. End with CNTL/Z. Bogota2(config)#enable secret class Bogota2(config)#line console 0 Bogota2(config-line)#password cisco Bogota2(config-line)#login Bogota2(config-line)#exit Router(config)#line vty 0 15 Router(config-line)#password cisco Router(config-line)#login Router(config-line)#service password-encryption Router(config)#banner motd #Prohibido el acceso no autorizado por Cristian Castilla Marroquin!# Router(config)#end
ISP	Router(config)#hostname ISP ISP(config)#enable secret class ISP(config)#line console 0 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#exit ISP(config)#line vty 0 15 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#service password-encryption ISP(config)#banner motd #Prohibido el acceso no autorizado por Cristian Castilla Marroquin!# ISP(config)#exit

2.2.2 REALIZAR LA CONEXIÓN FÍSICA DE LOS EQUIPOS CON BASE A LA TOPOLOGÍA DE LA RED

Figura 17 - Topología de la red sin conexión



Fuente propia

En la tabla 24, se puede observar cómo se construyeron los diferentes direccionamientos de IP para los diferentes dispositivos, de este modo se tendrá una manera más clara de saber que configuraciones.

Tabla 24 - Configuración de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara subred	Gateway determinado
ISP	S0/0/0	209.17.220.2	255.255.255.252	209.17.220.0
	S0/0/1	209.17.220.5	255.255.255.252	209.17.220.4
Medellín	S0/0/0	200.17.220.1	255.255.255.252	209.17.220.0
	S0/1/0	172.29.6.1	255.255.255.252	172.29.6.0
	S0/1/1	172.29.6.9	255.255.255.252	172.29.6.8
	S0/0/1	172.29.6.13	255.255.255.252	172.29.6.12
Medellín1	S0/0/0	172.29.6.2	255.255.255.252	172.29.6.0
	S0/1/0	172.29.6.5	255.255.255.252	172.29.6.4
	G0	172.29.4.1	255.255.255.252	172.29.4.0
Medellín2	S0/1/0	172.29.6.6	255.255.255.252	172.29.6.4
	S0/0/0	172.29.6.10	255.255.255.252	172.29.6.8
	S0/0/1	172.29.6.13	255.255.255.252	172.29.6.12
	G0	172.29.4.129	255.255.255.128	172.29.4.128
Bogotá	S0/0/0	209.17.220.6	255.255.255.252	209.17.220.4
	S0/1/0	172.29.3.1	255.255.255.252	172.29.3.0

	S0/0/1	172.29.3.5	255.255.255.252	172.29.3.4
	S0/1/1	172.29.3.9	255.255.255.252	172.29.3.8
Bogota 1	S0/0/0	172.29.3.2	255.255.255.252	172.29.3.0
	S0/0/1	172.29.3.6	255.255.255.252	172.29.3.4
	S0/1/0	172.29.3.15	255.255.255.252	172.29.3.12
	Go	172.29.0.1	255.255.255.0	172.29.4.0
Bogota 2	S0/0/0	172.29.3.10	255.255.255.252	172.29.3.8
	S0/1/0	172.29.3.14	255.255.255.252	172.29.3.12
	G0	172.29.1.1	255.255.255.252	172.29.1.0
PC-1	F0/0	172.29.4.0	255.255.255.252	172.29.4.1
PC-2	F0/0	172.29.4.133	255.255.255.128	172.29.4.129
PC-3	F0/0	172.29.0.5	255.255.255.0	172.29.0.1
PC-4	F0/0	172.29.1.4	255.255.255.128	172.29.1.1

En esta tabla se realizarán los diferentes enrutamientos para los diferentes dispositivos, se utilizarán comandos utilizados anteriormente.

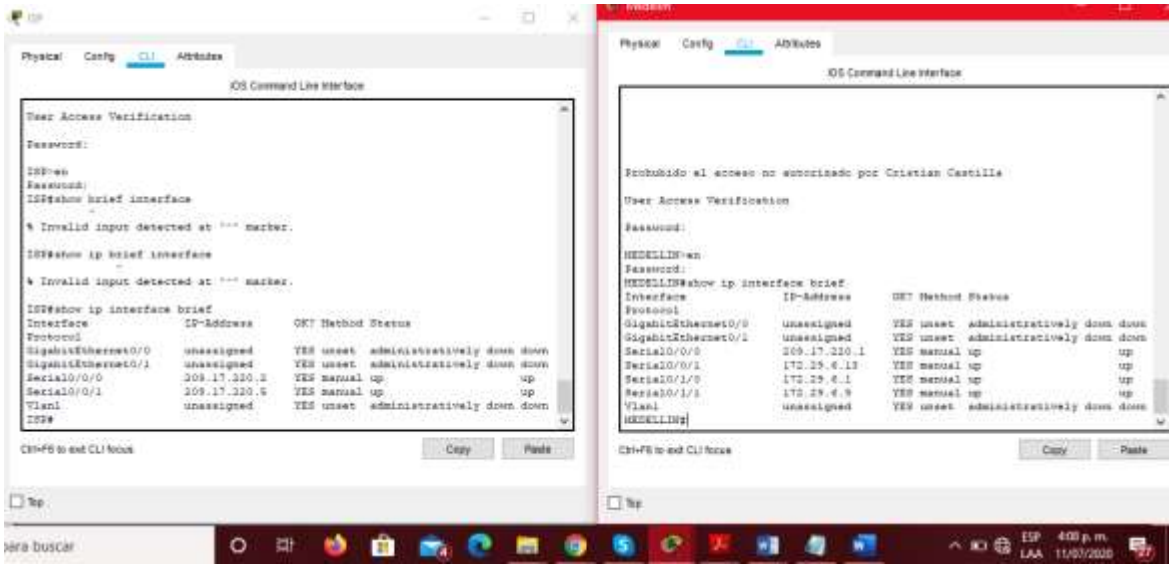
Tabla 25 - Configuración del enrutamiento.

Dispositivo	Configuración de enrutamiento
ISP	SP(config)#int s0/0/0 ISP(config-if)#ip address209.17.220.2 255.255.255.252 ISP(config-if)#clock rate 4000000 ISP(config-if)#no shut ISP(config-if)#int s0/0/1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 4000000 ISP(config-if)#no shut
Medellin	Medellin(config)#int s0/0/0 Medellin(config-if)#ip address 209.17.220.1 255.255.255.252 Medellin(config-if)# Medellin(config-if)#clock rate 4000000 Medellin(config-if)#no shut Medellin(config-if)#int s0/1/0 Medellin(config-if)#ip addres 172.29.6.1 255.255.255.252 Medellin(config-if)#clock rate 4000000 Medellin(config-if)#no shut Medellin(config-if)#int s0/1/1 Medellin(config-if)#ip addres 172.29.6.9 255.255.255.252 Medellin(config-if)#clock rate 4000000 Medellin(config-if)#no shut

	Medellin(config-if)#int s0/0/1 Medellin(config-if)#ip addres 172.29.6.13 255.255.255.252 Medellin(config-if)#clock rate 4000000 Medellin(config-if)#no shut
Medellín 1	Medellin1(config)#int s0/0/0 Medellin1(config-if)#ip address 172.29.6.2 255.255.255.252 Medellin1(config-if)#clock rate 4000000 Medellin1(config-if)#no shut Medellin1(config-if)#int s0/1/0 Medellin1(config-if)#ip address 172.29.6.5 255.255.255.252 Medellin1(config-if)#clock rate 4000000 Medellin1(config-if)#no shut Medellin1(config-if)#int g0/0 Medellin1(config-if)#ip address 172.29.4.1 255.255.255.252 Medellin1(config-if)#no shut
Medellín 2	Medellin2(config)#int s0/1/0 Medellin2(config-if)#ip address 172.29.6.6 255.255.255.252 Medellin2(config-if)#no shut Medellin2(config-if)#int s0/0/0 Medellin2(config-if)#ip address 172.29.6.10 255.255.255.252 Medellin2(config-if)#no shut Medellin2(config-if)#int s0/0/1 Medellin2(config-if)#ip address 172.29.6.13 255.255.255.252 Medellin2(config-if)#no shut Medellin2(config-if)# Medellin2(config-if)#int g0/0 Medellin2(config-if)#ip address 172.29.4.129 255.255.255.128 Medellin2(config-if)#no shut
Bogota	Bogota(config)#int s0/0/0 Bogota(config-if)#ip address 209.17.220.6 255.255.255.252 Bogota(config-if)#clock rate 128000 Bogota(config-if)#no shut Bogota(config-if)#int s0/1/0 Bogota(config-if)#ip address 172.29.3.1 % Incomplete command. Bogota(config-if)#ip address 172.29.3.1 255.255.255.252 Bogota(config-if)#clock rate 128000

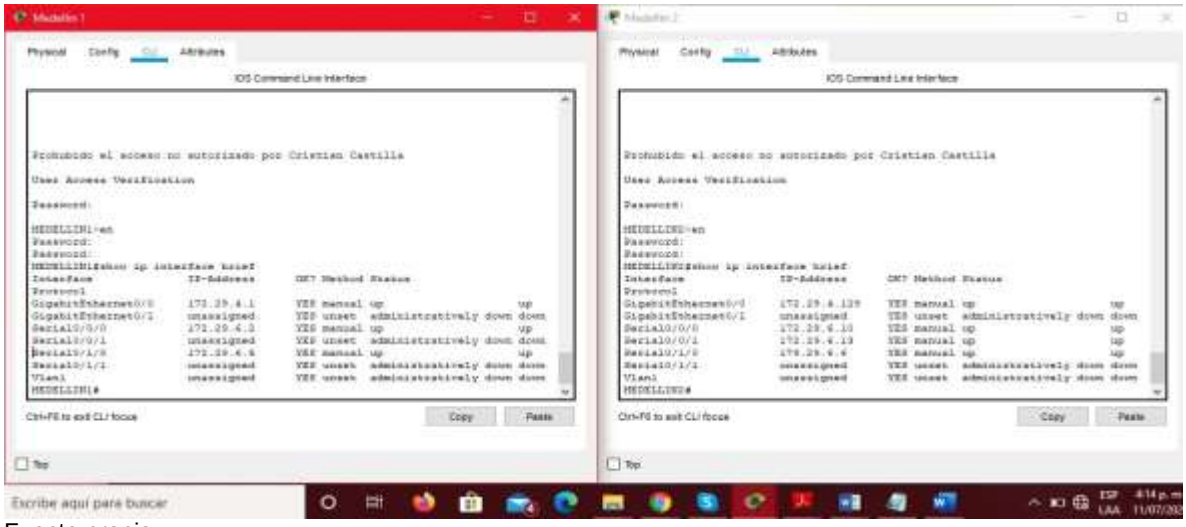
	Bogota(config-if)#no shut Bogota(config-if)#int s0/0/1 Bogota(config-if)#ip address 172.29.3.5 255.255.255.252 Bogota(config-if)#clock rate 128000 Bogota(config-if)#no shut Bogota(config-if)#int s0/1/1 Bogota(config-if)#ip address 172.29.3.9 255.255.255.252 Bogota(config-if)#clock rate 128000 Bogota(config-if)#no shut
Bogota 1	Bogota1(config)#int s0/0/0 Bogota1(config-if)#ip address 172.29.3.2 255.255.255.252 Bogota1(config-if)#clock rate 4000000 Bogota1(config-if)#no shut Bogota1(config-if)#int s0/1/0 Bogota1(config-if)#ip address 172.29.3.15 255.255.255.252 Bogota1(config-if)#no shut Bogota1(config-if)#int g0/0 Bogota1(config-if)#ip address 172.29.0.1 255.255.255.0 Bogota1(config-if)#clock rate 4000000 Bogota1(config-if)#no shut
Bogota 2	bogota2(config)#int s0/0/0 bogota2(config-if)#ip address 172.29.3.10 255.255.255.252 bogota2(config-if)#clock 4000000 bogota2(config-if)#no shut bogota2(config-if)#int s0/1/0 bogota2(config-if)#ip address 172.29.3.14 255.255.255.252 bogota2(config-if)#clock 128000 bogota2(config-if)#no shut bogota2(config-if)#int g0/0 bogota2(config-if)#ip address 172.29.1.1 255.255.255.252 bogota2(config-if)#no shut

Figura 18 - show ip interface brief



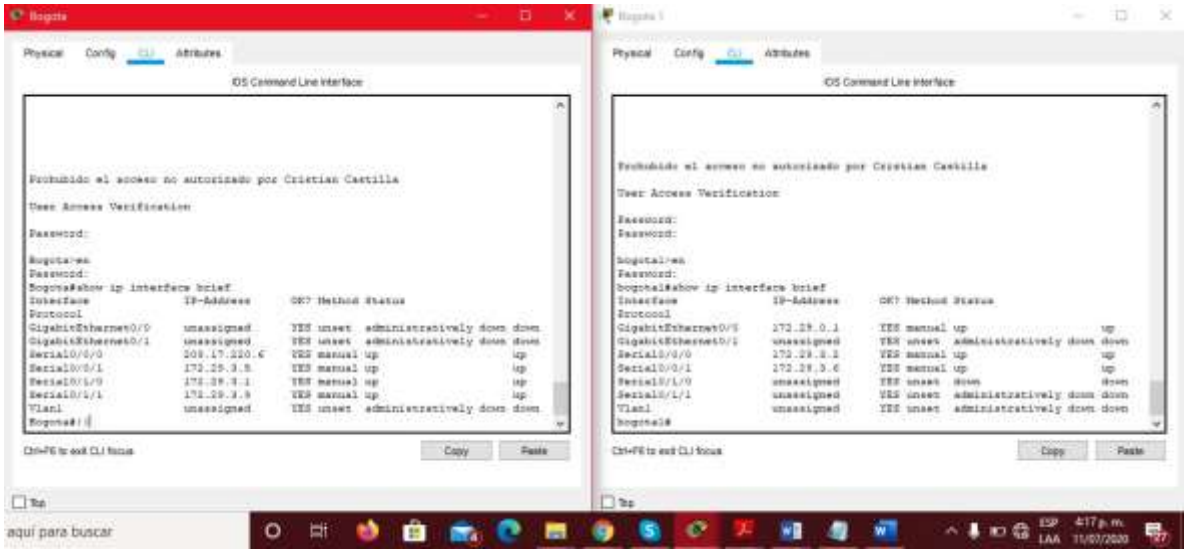
Fuente propia.

Figura 19 - Verificación interfaces MEDELLIN1 MEDELLIN2



Fuente propia

Figura 20 - Verificación interfaces BOGOTA, BOGOTA1



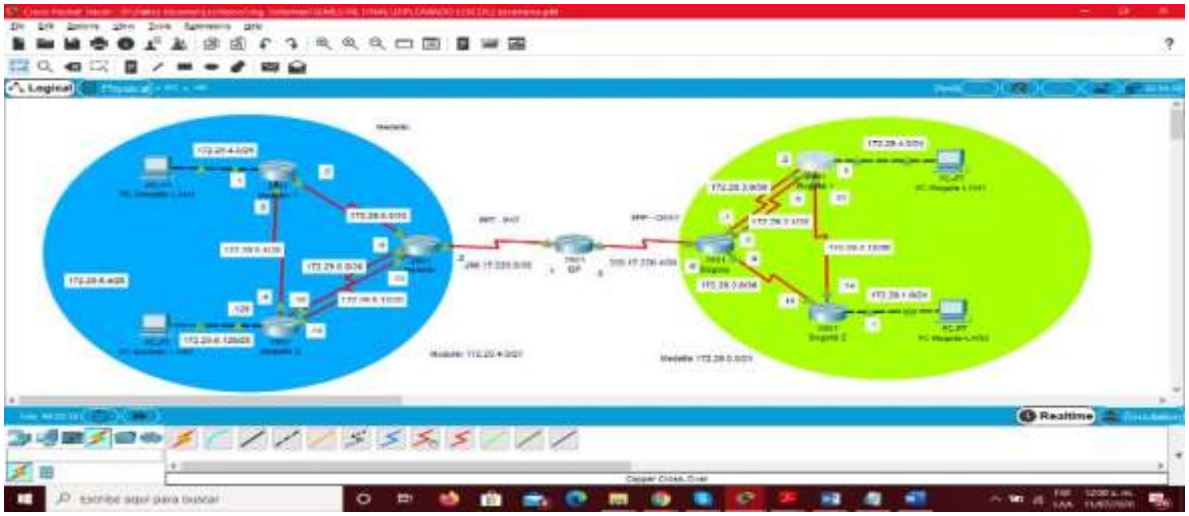
Fuente propia

Figura 21 - ping ISP

Fuente propia.

En esta imagen se observa la estructura de la topología aun sin conexiones.

Figura 22 - Topología de los routers conectados



Fuente propia.

2.3 PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

El direccionamiento Open Shortest Path First (OSPF), se utiliza como el camino mas corto que se usa para distribuir la información de ruteo dentro de un solo sistema autónomo. Se utiliza en cada uno de los routers comands como route id para identificar cada route, desfault-information originate, entre otros.

Tabla 26 - configuración OSPF

Dispositivo	Configuración OSPF en los routers
Medellin	MEDELLIN#configure terminal MEDELLIN(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.0 MEDELLIN(config)#router ospf 1 MEDELLIN(config-router)#router-id 1.1.1.1 MEDELLIN(config-router)#network 172.29.6.0 0.0.0.3 area 0 MEDELLIN(config-router)#network 172.29.6.8 0.0.0.3 area 0

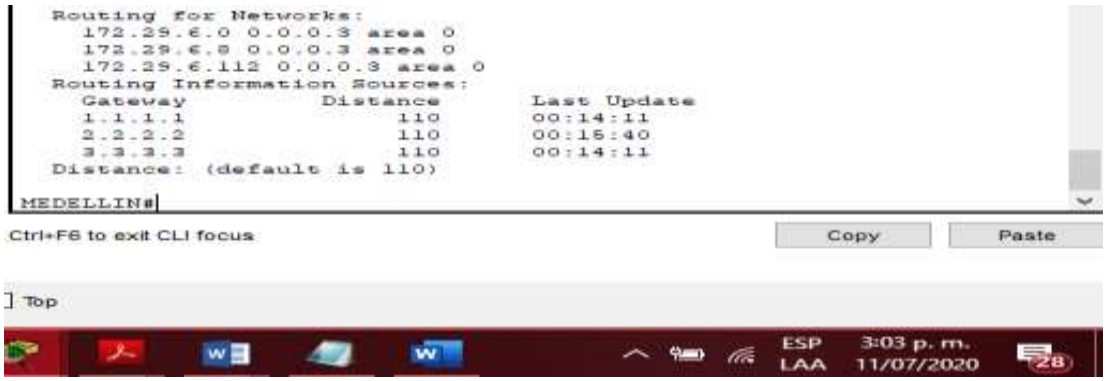
	MEDELLIN(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN(config-router)#default-information originate MEDELLIN(config-router)#end
Medellin 1	MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#router-id 2.2.2.2 MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 0 MEDELLIN1(config-router)#network 172.29.6.4 0.0.0.3 area 0 MEDELLIN1(config-router)#default-information originate MEDELLIN1(config-router)#passive-interface g0/0 MEDELLIN1(config-router)#end MEDELLIN1#
Medellin 2	MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#router-id 3.3.3.3 MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0 MEDELLIN2(config-router)#network 172.29.6.8 0.0.0.3 area 0 MEDELLIN2(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN2(config-router)#default-information originate MEDELLIN2(config-router)#passive-interface g0/0 MEDELLIN2(config-router)#end
Bogota	Bogota(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.4 Bogota(config)#router ospf 1 Bogota(config-router)#router-id 4.4.4.4 Bogota(config-router)#network 172.29.3.0 0.0.0.3 area 0 Bogota(config-router)#network 172.29.3.4 0.0.0.3 area 0 Bogota(config-router)#network 172.29.3.8 0.0.0.3 area 0 Bogota(config-router)#default-information originate Bogota(config-router)#end Bogota#
Bogota 1	bogota1(config)#router ospf 1 bogota1(config-router)#router-id 5.5.5.5 bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0 bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0 bogota1(config-router)#default-information originate bogota1(config-router)#passive-interface g0/0

	bogota1(config-router)#end bogota1#
Bogota 2	Bogota2(config)#router ospf 1 Bogota2(config-router)#router-id 6.6.6.6 Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0 Bogota2(config-router)#passive-interface g0/0 Bogota2(config-router)#end

2.3.1 PARTE 2: TABLA DE ENRUTAMIENTO.

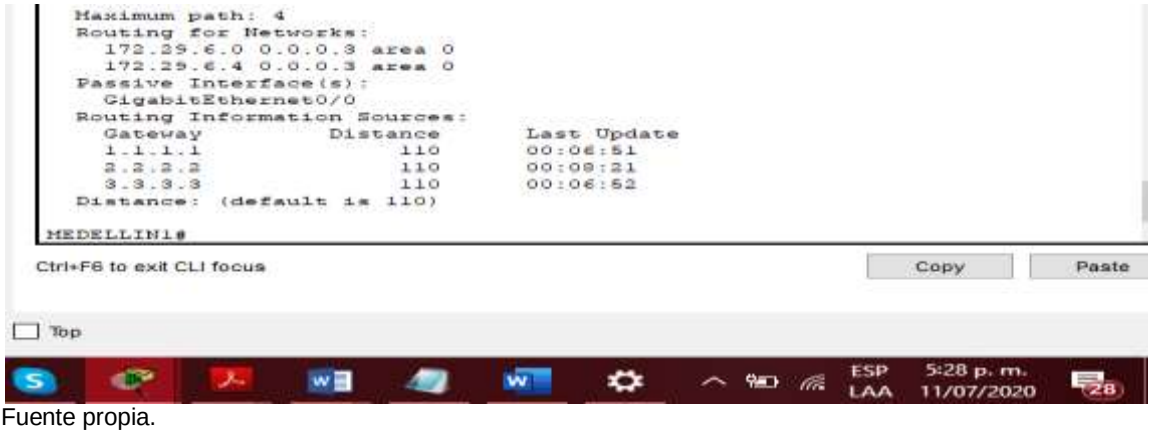
2.3.2 VERIFICACIÓN TABLAS DE ENRUTAMIENTO

Figura 23 - Verificación tabla de enrutamiento MEDELLIN



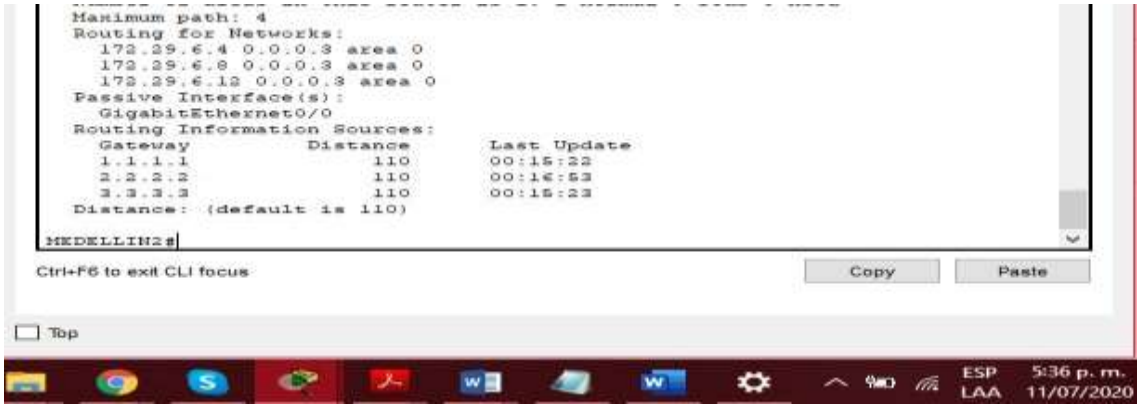
Fuente propia.

Figura 24 - verificación tabla de enrutamiento Medellin1



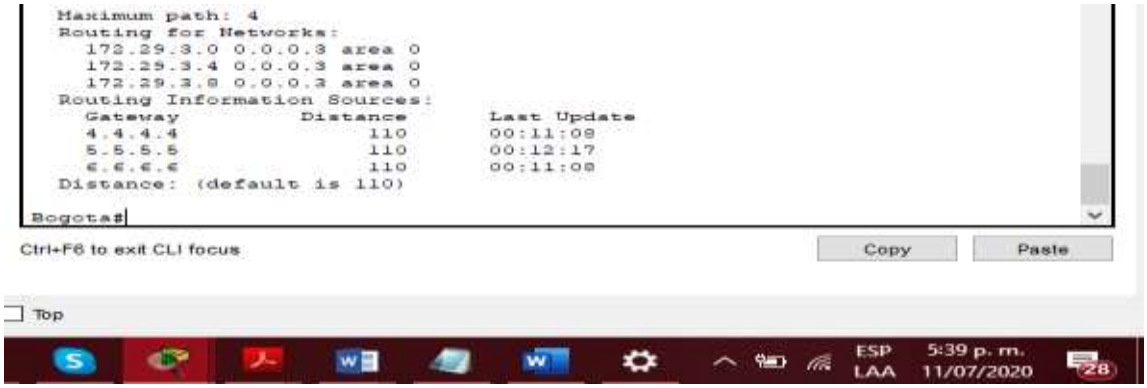
Fuente propia.

Figura 25 - verificación tabla de enrutamiento Medellin2



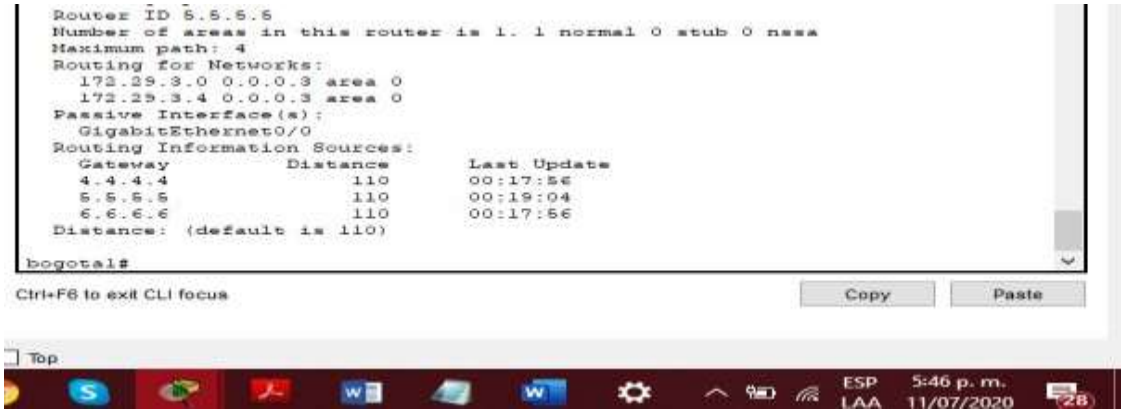
Fuente propia.

Figura 26 - Verificación tabla de enrutamiento Bogotá



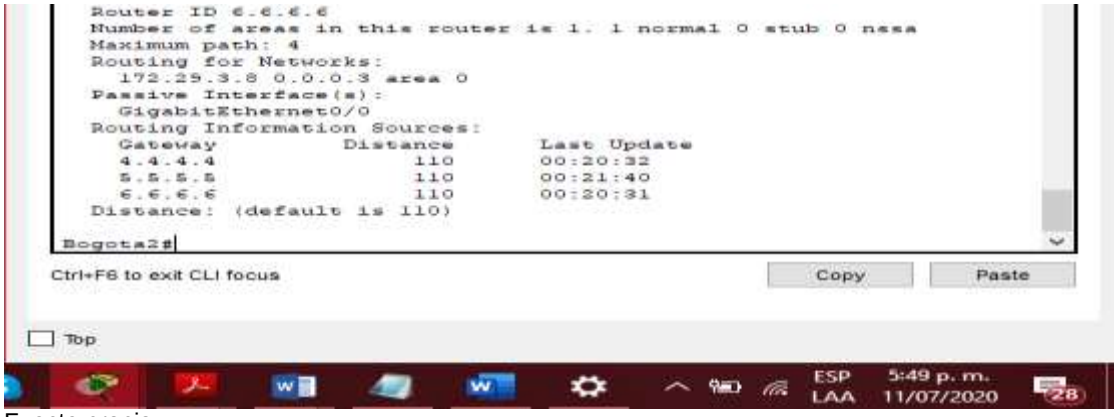
Fuente propia.

Figura 27 - Verificación tabla de enrutamiento Bogota1



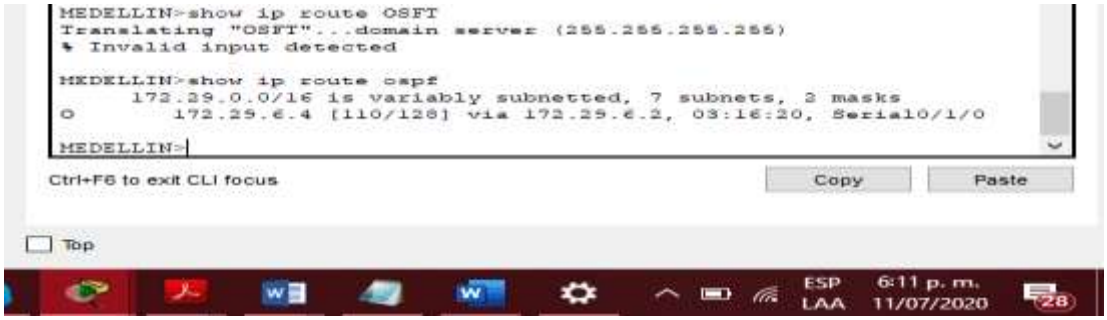
Fuente propia.

Figura 28 - Verificación tabla de enrutamiento Bogota2



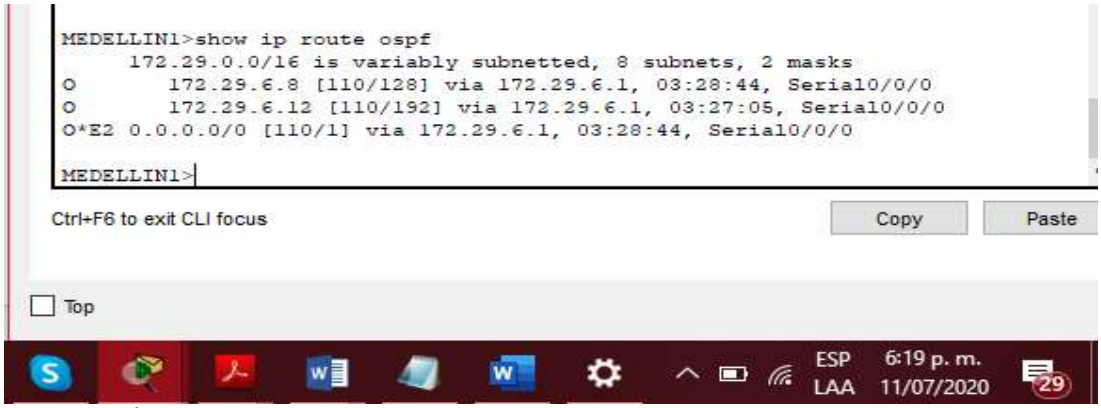
Fuente propia

Figura 29 - Verificación de los routers MEDELLIN



Fuente propia.

Figura 30 - Verificación de los routers MEDELLIN1

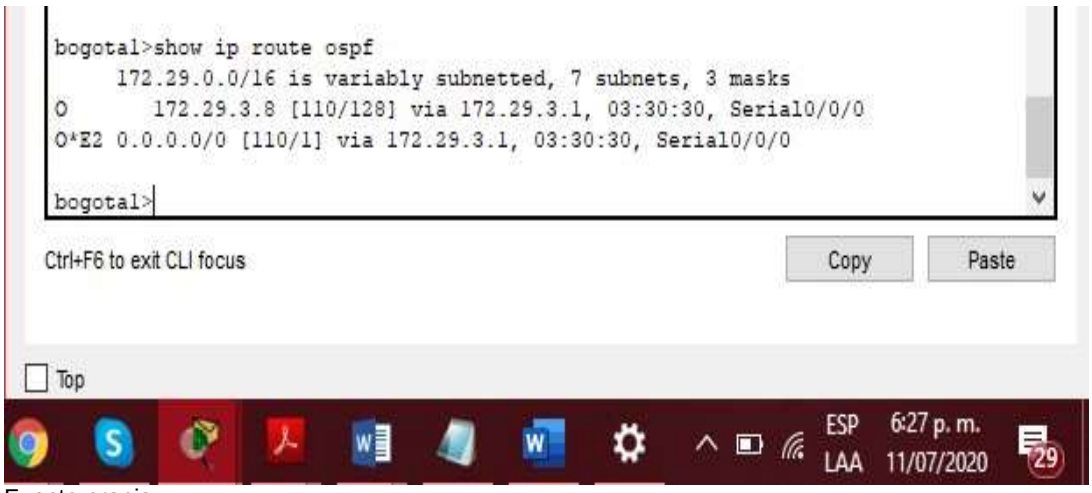


Fuente propia.

Figura 31 - Validación de los router MEDELLIN2

Fuente propia.

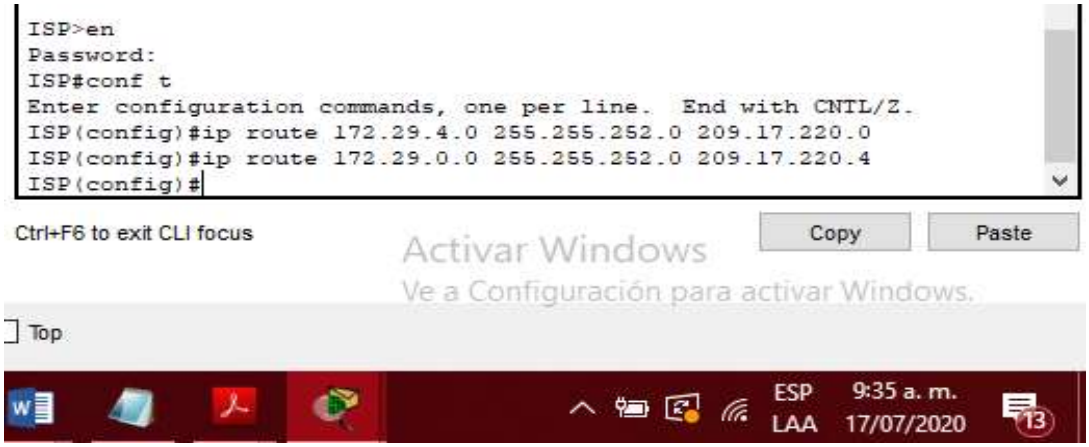
Figura 32 - Verificación de los router BOGOTA1



Fuente propia.

2.3.3 EL ROUTER ISP DEBERÁ TENER UNA RUTA ESTÁTICA DIRIGIDA HACIA CADA RED INTERNA DE BOGOTÁ Y MEDELLÍN PARA EL CASO SE SUMARIZAN LAS SUBREDES DE CADA UNO A /22.

Figura 33 - Verificación ISP conectadas.



Fuente propia.

2.4 PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF

Se utilizará el comando passive-interface G0/0, para no enviar la información a las pc, esto se hace únicamente ellos routers que tengan conexión con los PC.

Tabla 27 - Protocolo OSPF

Dispositivo	Configuración
Medellin1	MEDELLIN1#configure terminal. MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#router-id 2.2.2.2 MEDELLIN1(config-router)#passive-interface g0/0 MEDELLIN1(config-router)# MEDELLIN1#
Medellin2	MEDELLIN2#configure terminal. MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#router-id 3.3.3.3 MEDELLIN2(config-router)#passive-interface g0/0 MEDELLIN2(config-router)# MEDELLIN2#
Bogota1	bogota1#configure terminal. bogota1(config)#router ospf 1 bogota1(config-router)#router-id 5.5.5.5 bogota1(config-router)#passive-interface g0/0 bogota1(config-router)#

	bogota1#
Bogota2	Bogota2#configure terminal. Bogota2(config)#router ospf 1 Bogota2(config-router)#router-id 6.6.6.6 Bogota2(config-router)#passive-interface g0/0 Bogota2 (config-router)# Bogota2#

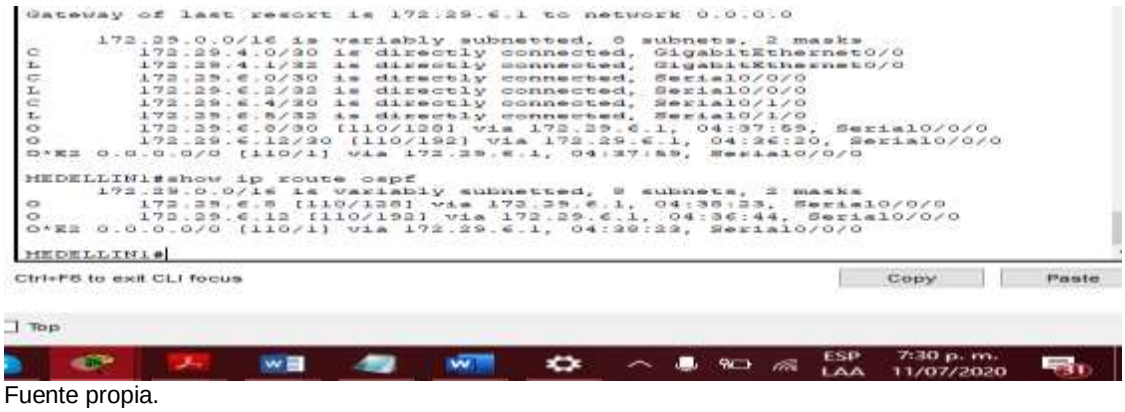
2.5 PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

Figura 34 - verificación del protocolo OSPF

Fuente propia.

Medellín1

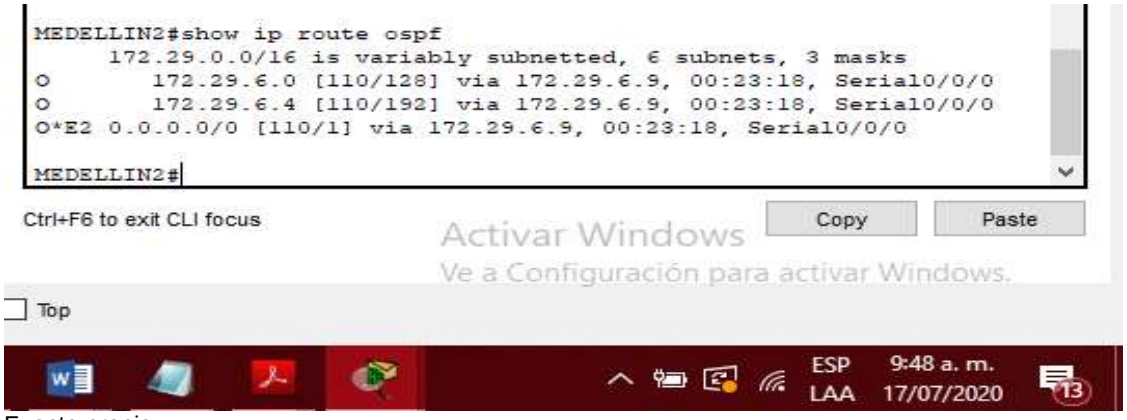
Figura 35 - Verificación protocolo OSPF - Medellín 1



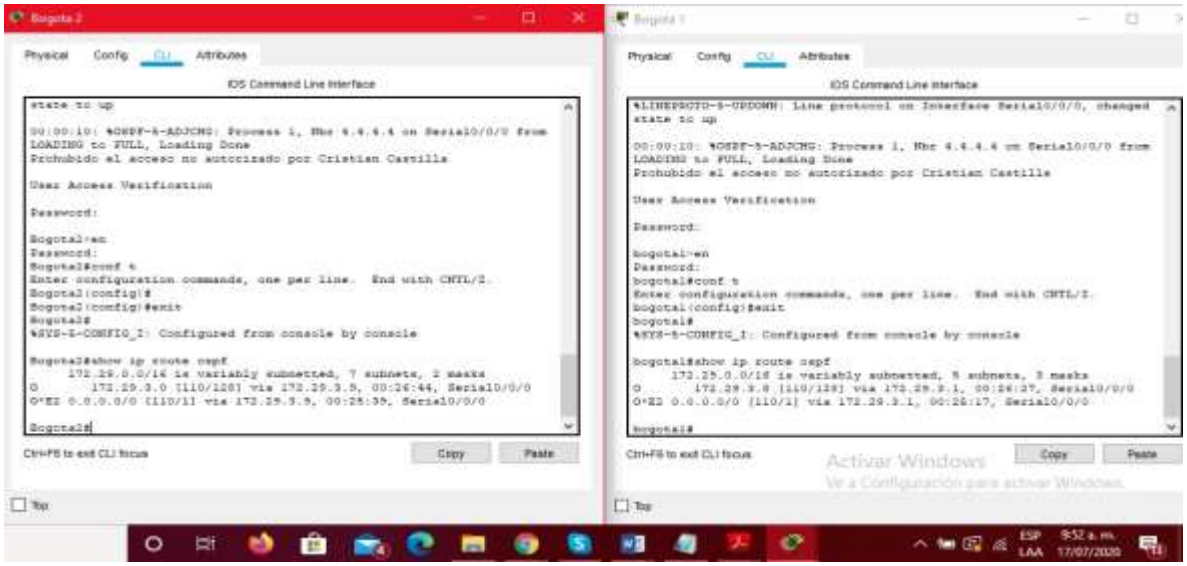
Fuente propia.

Medellín 2

Figura 36 – verificación protocolo OSPF - Medellin2



Fuente propia.



2.6 PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

PPP define un protocolo LCP extensible que permite la negociación de un protocolo de autenticación para autenticar a los peers antes de permitir que los protocolos de capa de red transmitan por el enlace. En los cuales se encuentran estos dos protocolos para la autenticación, PAP y CHAP.

Tabla 28 - encapsulamiento y autentificación PPP

Dispositivo	Configuración de encapsulamiento y autentificación PPP
ISP	SP#conf term ISP(config)#username Bogota password cisco ISP(config)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap ISP(config-if)# ISP# ISP#conf t ISP(config)#username Medellin ISP(config)#username Medellin 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#
Medellin1	MEDELLIN(config)#username ISP password cisco MEDELLIN(config)#int s0/0/0 MEDELLIN(config-if)#encapsulation ppp MEDELLIN(config-if)#ppp authentication chap MEDELLIN(config-if)#encapsulation ppp MEDELLIN(config-if)#ppp authentication pap MEDELLIN(config-if)#ppp pap sent-username Medellin password cisco
Bogotá2	Bogota#conf t Bogota(config)#username ISP password cisco Bogota(config)#int s0/0/0 Bogota(config-if)#encapsulation ppp Bogota(config-if)#ppp authentication chap Bogota(config-if)#

Figura 37 - verificación PPP – Medellín

Fuente propia.

2.7 PARTE 6: CONFIGURACIÓN DE PAT.

En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Tabla 29 - Configuración PAT

Dispositivo	Configuracion
Medellin	MEDELLIN>enable MEDELLIN#conf t MEDELLIN(config)#ip nat inside source list 1 interface s0/0/0 ovserload MEDELLIN(config)#

	MEDELLIN(config)#ip nat inside source list 1 interface s0/0/0 overload MEDELLIN(config)#access-list 1 permit 172.29.4.0 0.0.3.255 MEDELLIN(config)# MEDELLIN(config)# INT S0/0/0 MEDELLIN(config-if)#ip nat outside MEDELLIN(config-if)# INT S0/0/1 MEDELLIN(config-if)#ip nat intside MEDELLIN(config-if)#ip nat inside MEDELLIN(config-if)# INT S0/1/1 MEDELLIN(config-if)#ip nat inside MEDELLIN(config-if)#INT S0/1/0 MEDELLIN(config-if)#ip nat inside MEDELLIN(config-if)#
Bogota	BOGOTA>ENABLE BOGOTA#conf t BOGOTA(config)#ip nat inside source list 1 interface s0/0/0 overload BOGOTA(config)#access-list 1 permit 172.29.0.0 0.0.3.255 BOGOTA(config)#int s0/0/0 BOGOTA(config-if)#ip nat outside BOGOTA(config-if)#int s0/1/0 BOGOTA(config-if)#ip nat inside BOGOTA(config-if)#int s0/1/1 BOGOTA(config-if)#ip nat inside BOGOTA(config-if)#

2.8 PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP

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

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

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

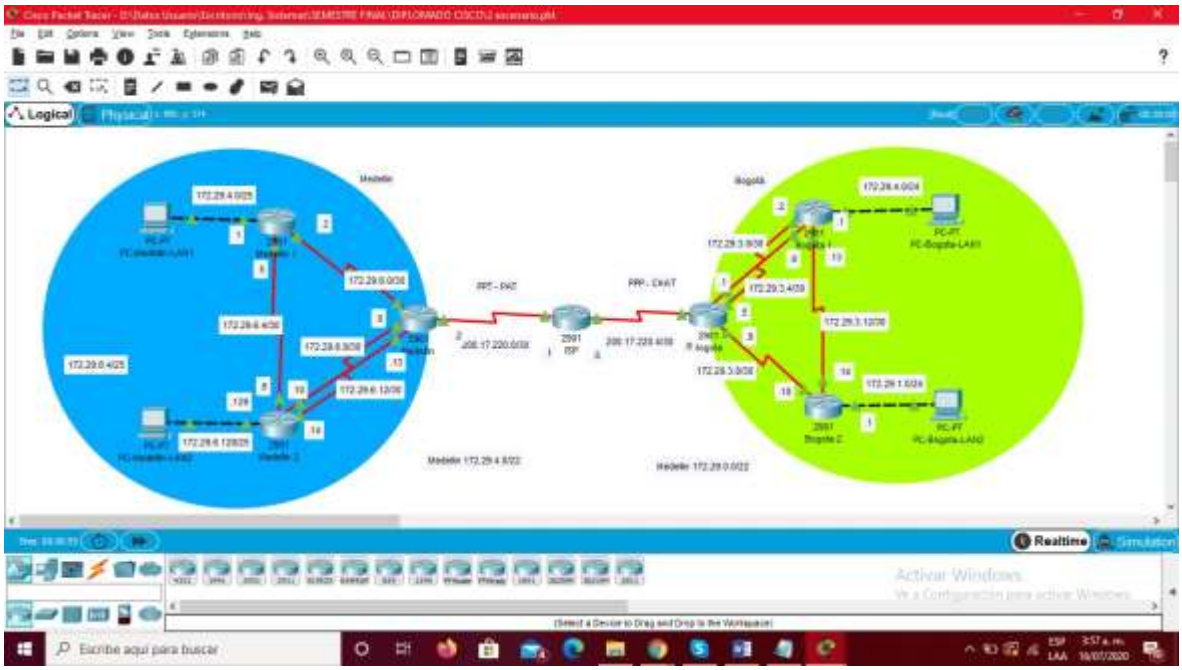
d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Tabla 30 – Configuración del DHCP

Dispositivos	Configuración
Medellin 2	MEDELLIN1#conf term

	MEDELLIN1(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.130 MEDELLIN1(config)#ip dhcp pool Medellin1-LAN1 MEDELLIN1(dhcp-config)#network 172.29.4.129 255.255.255.0 MEDELLIN1(dhcp-config)#default-router 172.29.4.129 MEDELLIN1(dhcp-config)#exit MEDELLIN1(config)#
Medellin 1	MEDELLIN1(config)#int g0/0 MEDELLIN1(config-if)#ip helper-address 172.29.6.5 MEDELLIN1(config-if)#exit
Bogotá2	Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4 Bogota2(config)#ip dhcp pool bogota_2 Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0 Bogota2(dhcp-config)#default-router 172.29.1.1 Bogota2(dhcp-config)#exit Bogota2(config)#ip dhcp pool Bogota_1 Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota2(dhcp-config)#default-route 172.29.0.1 Bogota2(dhcp-config)#end

Figura 38 - Topología final escenario 2



Fuente propia.

CONCLUSIONES

Este informe es muy importante para fortalecer todo el proceso de aprendizaje del curso DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), ya que al desarrollar esta práctica vimos reflejados diferentes comandos que sirven para configurar ip, direcciones de interfaces, cambiar nombre a diferentes dispositivos.

En el momento de realizar rutas para routers, switches y PCs es importante conformar una tabla de direcciones, donde contenga el nombre del dispositivo, Interfaz, Dirección IP, Mascara subred, Gateway determinado, para que de esta manera nos sea más fácil realizar las configuraciones de los dispositivos, con la menor posibilidad de cometer errores.

La herramienta de CISCO PACKET TRACER nos permite recrear diferentes tipos de escenarios, para que en algún momento de nuestra vida al ejercer la carrera como Ingenieros de Sistemas podamos llevar a cabo, cada conocimiento adquirdo.

BIBLIOGRAFIA

CISCO, Configuración del Switch. Disponible Principios de Enrutamiento y Conmutación. [en línea]. 2019. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO, Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. [en línea]. 2019 Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

CISCO, División de redesIP en subredes. Fundamentos de Networking. [en línea]. 2019 Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO, Direccionamiento IP. Fundamentos de Networking, [en línea]. 2019 Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO, NAT para IPv4. Principios de Enrutamiento y Conmutación. [en línea]. 2019 Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO, VLAN. Principios de Enrutamiento y Conmutación. [en línea]. 2019 Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

ANEXOS

Anexos 1 - Link escenarios 1 y 2

https://drive.google.com/drive/folders/1v1RcYSlJTjdDL5rXwAHMc5A6caZIGYDK?usp=sharing