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

JEYSON FERNANDO MERCADO MANGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

SANTA MARTA

2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Presentado por:

Jeyson Fernando Mercado Manga

Solución de dos escenarios presentes en entornos corporativos bajo el uso de tecnología cisco

Presentado a:

Gustavo Adolfo Rodríguez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

SANTA MARTA

2020

TABLA DE CONTENIDO

GLOSARIO 5
INTRODUCCION 11
OBJETIVOS 12
OBJETIVO GENERAL 12
OBJETIVOS ESPECIFICOS 12
ESCENARIO 1 13
Topología 13
Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos 14
Parte 2: Configurar los parámetros básicos de los dispositivos 16
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 31
Parte 4: Configurar el protocolo de routing dinámico RIPv2 40
Parte 5: Implementar DHCP y NAT para IPv4 49
Parte 6: Configurar NTP 53
Parte 7: Configurar y verificar las listas de control de acceso (ACL) 54
ESCENARIO 2 57
Topología 57
Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos 58
Parte 2: Configurar los parámetros básicos de los dispositivos 58
Parte 3: Configuración del enrutamiento 63
Parte 4: Tabla de enrutamiento 70
Parte 5: Deshabilitar la propagación del protocolo OSPF 76
Parte 5: Verificar el protocolo OSPF. 77
Parte 7: Configurar encapsulamiento y autenticación PPP 79
Parte 8: Configuración de PAT. 81
Parte 9: Configuración del servicio DHCP 82
CONCLUSIONES 87
BIBLIOGRAFIA 88
REFERENCIAS 89

LISTA DE ILUSTRACIONES

Ilustración 1 Topología de la red del escenario 1 13
Ilustración 2 Topología de la red en Cisco Packet Tracer 14
Ilustración 3 Verificación de las configuraciones basicas ping desde R1 a R2 30
Ilustración 4 Verificación de las configuraciones basicas ping desde R2 a R3 30
Ilustración 5 Verificación de las configuraciones basicas ping al PC de internet 31
Ilustración 6 Verificación de la vlan 99 desde S1 a R1 38
Ilustración 7 Verificación de la vlan 99 desde S3 a R1 39
Ilustración 8 Verificación de la vlan 21 desde S1 a R1 39
Ilustración 9 Verificación de la vlan 23 desde S3 a R1 40
Ilustración 10 Verificación de la información por medio del comando show ip protocols en R1 45
Ilustración 11 Verificación de la información por medio del comando show ip route rip en R1 45
Ilustración 12 Verificación de la información por medio del comando show run en R1 46
Ilustración 13 Verificación de la información por medio del comando show ip protocols en R2 46
Ilustración 14 Verificación de la información por medio del comando show ip router rip en R2 47
Ilustración 15 Verificación de la información por medio del comando show run en R2 47
Ilustración 16 Verificación de la información por medio del comando show ip protocols en R3 48
Ilustración 17 Verificación de la información por medio del comando show ip router rip en R3 48
Ilustración 18 Verificación de la información por medio del comando show run en R3 49
Ilustración 19 Verificación de DHCP en PC-C 53
Ilustración 20 Verificación del show interface en R2 56
Ilustración 21 Topología de la red del escenario 2 57
Ilustración 22 Topología de la red en Cisco Packet Tracer 58
Ilustración 23 Verificación del enrutamiento en M1 70
Ilustración 24 Verificación del enrutamiento en M2 71
Ilustración 25 Verificación del enrutamiento en M3 71
Ilustración 26 Verificación del enrutamiento en B1 72
Ilustración 27 Verificación del enrutamiento en B2 72
Ilustración 28 Verificación del enrutamiento en B3 73
Ilustración 29 Verificación de balanceo de cargas en M2 73
Ilustración 30 Verificación de las redes conectadas y recibidas por OSPF en M2 74
Ilustración 31 Verificación de las redes conectadas y recibidas por OSPF en B2 75
Ilustración 32 Verificación de las rutas redundantes en M3 75
Ilustración 33 Verificación de las rutas redundantes en B3 76
Ilustración 34 Verificación de OSPF en M1 78
Ilustración 35 Verificación de OSPF en M2 78
Ilustración 36 Verificación de OSPF en M3 78
Ilustración 37 Verificación de OSPF en B1 79
Ilustración 38 Verificación de OSPF en B2 79
Ilustración 39 Verificación de OSPF en B3 79
Ilustración 40 Verificación de configuración DHCP en PC0 84
Ilustración 41 Verificación de configuración DHCP en PC1 84
Ilustración 42 Verificación de configuración DHCP en PC3 85
Ilustración 43 Verificación de configuración DHCP en PC2 85

LISTA DE TABLAS

Tabla 1 Indicaciones para la verificación inicial de los dispositivos 16
Tabla 2 Indicaciones para configurar la computadora red internet 16
Tabla 3 Indicaciones para configurar a R1 19
Tabla 4 Indicaciones para configurar a R2 22
Tabla 5 Indicaciones para configurar a R3 25
Tabla 6 Indicaciones para configurar a S1 27
Tabla 7 Indicaciones para configurar a S3 29
Tabla 8 Verificación de conectividad en los routers y en el PC de internet 29
Tabla 9 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de S1 33
Tabla 10 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de S3 35
Tabla 11 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de R1 37
Tabla 12 Verificación de conectividad entre S1, S3 y R1 38
Tabla 13 Indicaciones para configurar RIPv2 en R1 41
Tabla 14 Indicaciones para configurar RIPv2 en R2 42
Tabla 15 Indicaciones para configurar RIPv2 en R3 44
Tabla 16 Comandos para realizar las verificaciones de las configuraciones que se realizaron 44
Tabla 17 Indicaciones para configurar R1 como servidor de DHCP 50
Tabla 18 Indicaciones para realizar la configuración NAT en R2 52
Tabla 19 Verificación del protocolo DHCP y NAT en los dispositivos 52
Tabla 20 Indicaciones para configurar NTP en R1 Y R2 54
Tabla 21 Indicaciones para configurar y verificar las ACL 55
Tabla 22 Comandos para realizar las verificaciones de las configuraciones realizadas en los dispositivos 55
Tabla 23 Des habilitación de los puertos seriales 77

GLOSARIO

ACL: Una lista de control de acceso o ACL (del inglés, access control list) 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. 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 a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI. [1]

DHCP: Reduce en gran medida los errores que se producen cuando las direcciones IP se asignan de forma manual, y puede estirar las direcciones IP al limitar el tiempo que un dispositivo puede mantener una dirección IP individual. DHCP está disponible tanto para IPv4 (DHCPv4) como para IPv6 (DHCPv6). En esta sección, se explora la funcionalidad, y características de DHCPv4. [2]

ENRUTAMIENTO: El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por "mejor ruta" y en consecuencia cuál es la "métrica" que se debe utilizar para medirla. [3]

ETHERNET: Es un estándar de redes de área local para computadores, por sus siglas en español Acceso Múltiple con Escucha de Portadora y Detección de Colisiones. [4]

NAT ESTATICA: Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. [5]

NAT DINAMICA: El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública. Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no

esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando. [6]

NTP: Network Time Protocol, es un protocolo diseñado para sincronizar los relojes de las estaciones de trabajo a través de la red. La versión 3 de este protocolo es un Internet Draft Standard, formalizado en la RFC 1305. El protocolo NTP versión 4 es una importante revisión del estandard mencionado, y se encuentra en desarrollo, pero aún no ha sido formalizado en una RFC. Una versión simple de NTP (SNTP) versión 4 se describe en la RFC 2030. [7]

OSPF: Open Shortest Path First (OSPF), camino más corto primero, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstra enlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo [8]

PPP: Protocolo punto a punto (PPP) (en inglés 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. Está estandarizado en el documento RFC 1661. Puede proporcionar autenticación, cifrado de la transmisión1 y compresión.[9]

PAT: La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos, ya que es el utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. Además del ahorro económico, también se ahorran direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública. [10]

PROTOCOLOS DE RED: Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. [11]

RED: Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos nodos y software conectados entre sí por

medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios. [12]

RIP: (Routing information protocolo, protocolo de información de encaminamiento) RIP es un protocolo de encaminamiento interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a internet como infovia, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos. [13]

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red. es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática. [14]

SWITCH: "Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local area network), es un sistema de comunicación inalámbrico para minimizar las conexiones cableadas. [15]

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local. [16]

RESUMEN

La configuración de redes informáticas en el ámbito de un ingeniero de sistemas o administrador de redes es necesario e indispensable para su desempeño laboral, en la actualidad existen varias herramientas las cuales nos hacen más accesible este conocimiento y así mismo permiten que sea más práctico y menos teórico el aprendizaje.

El desarrollo del primer escenario configura una pequeña red con conectividad IPv4 e IPv6 y se enfocó en la configuración del protocolo de routing dinamico RIPv2, el protocolo de configuración de hosts dinámico 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, mientras que en el segundo escenario se administra una red más grande, donde se configura el protocolo OSPF y habilita el encapsulamiento PPP y su autenticación, además de las listas de control de acceso y traducción de direcciones IP sobre NAT-PAT respectivamente.

La interconexión entre sí de cada uno de los dispositivos que forman parte de la topología, se realiza por cable ethernet y puertos seriales, con el fin de alcanzar el conocimiento de configuración de equipos informáticos mediante las herramientas presentadas en el programa cisco Packet Tracer y así aplicarlos en el campo laboral logrando el fácil manejo de cualquier configuración de red en entornos corporativos, mediante los protocolos y normas de configuración de cisco.

Palabras Claves: CISCO, Protocolos, Enrutamientos, Habilidades, Redes, Comunicaciones.

ABSTRACT

The configuration of computer networks in the scope of a systems engineer or network administrator is necessary and indispensable for their work performance, at present there are several tools which make us more accessible this knowledge and also allow it to be more practical and less theoretical learning.

The development of the first scenario configures a small network with IPv4 and IPv6 connectivity and focused on the configuration of the dynamic routing protocol RIPv2, the dynamic host configuration protocol DHCP, the translation of dynamic and static network addresses (NAT), access control lists (ACLs) and the server/client network time protocol (NTP), while the second scenario manages a larger network, where the OSPF protocol is configured and enables PPP encapsulation and authentication, as well as access control lists and IP address translation over NAT-PAT respectively.

The interconnection between each of the devices that are part of the topology, is done by ethernet cable and serial ports, in order to achieve the knowledge of computer equipment configuration through the tools presented in the cisco Packet Tracer program and thus apply them in the workplace and achieve the easy handling of any network configuration in corporate environments, through the protocols and configuration standards of cisco.

Keywords: CISCO, Protocols, Routing, Skills, Networking, Communications

INTRODUCCION

En este trabajo se desarrollarán dos escenarios, inicialmente se realizarán las configuraciones basicas de los dispositivos de la red y se interconectarán según cada topología.

Consecutivamente se deberá configurar una red pequeña que admita conectividad IPv4 e IPv6, se configurará routing entre las VLAN que se crearan, se implementará el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP) y el protocolo de tiempo de red (NTP) servidor/cliente, se configurara la traducción de direcciones de red dinámicas y estáticas (NAT) y listas de control de acceso (ACL).

Posteriormente se creará la conectividad en el segundo escenario por medio del protocolo OSPF, en el cual conectaremos dos redes diferentes, la primera será llamada Medellín y la segunda Bogotá, se habilitará el encapsulamiento PPP, las listas de control de acceso y traducción de direcciones IP sobre NAT-PAT respectivamente.

Durante la verificación se utilizarán los comandos comunes de CLI, por lo tanto, nuestro conocimiento en redes se verá nutrido con los avances en cada configuración que realizaremos.

OBJETIVOS

OBJETIVO GENERAL

- Configurar los dispositivos informáticos mediante las herramientas presentadas en el programa packet tracer, para así aplicarlos en el campo laboral y lograr el fácil manejo de cualquier configuración de red LAN Y WAN en entornos corporativos, mediante los protocolos y normas de configuración de CISCO.

OBJETIVOS ESPECIFICOS

- Realizar las configuraciones de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP, para dar soluciones de red y conectividad a redes LAN y WAN.
- Configurar esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANs en los dos escenarios propuestos, con el fin de comprender el modo de operación de las VLAN.
- Diseñar un esquema de direccionamiento IP para proporcionar conectividad; seguridad y acceso a LAN y WAN mediante el uso del protocolo DHCP; listas de control de acceso y traducción de direcciones IP sobre NAT-PAT respectivamente.
- Utilizar herramientas de simulación de acceso remoto con el fin de crear escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

ESCENARIO 1

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

Topología

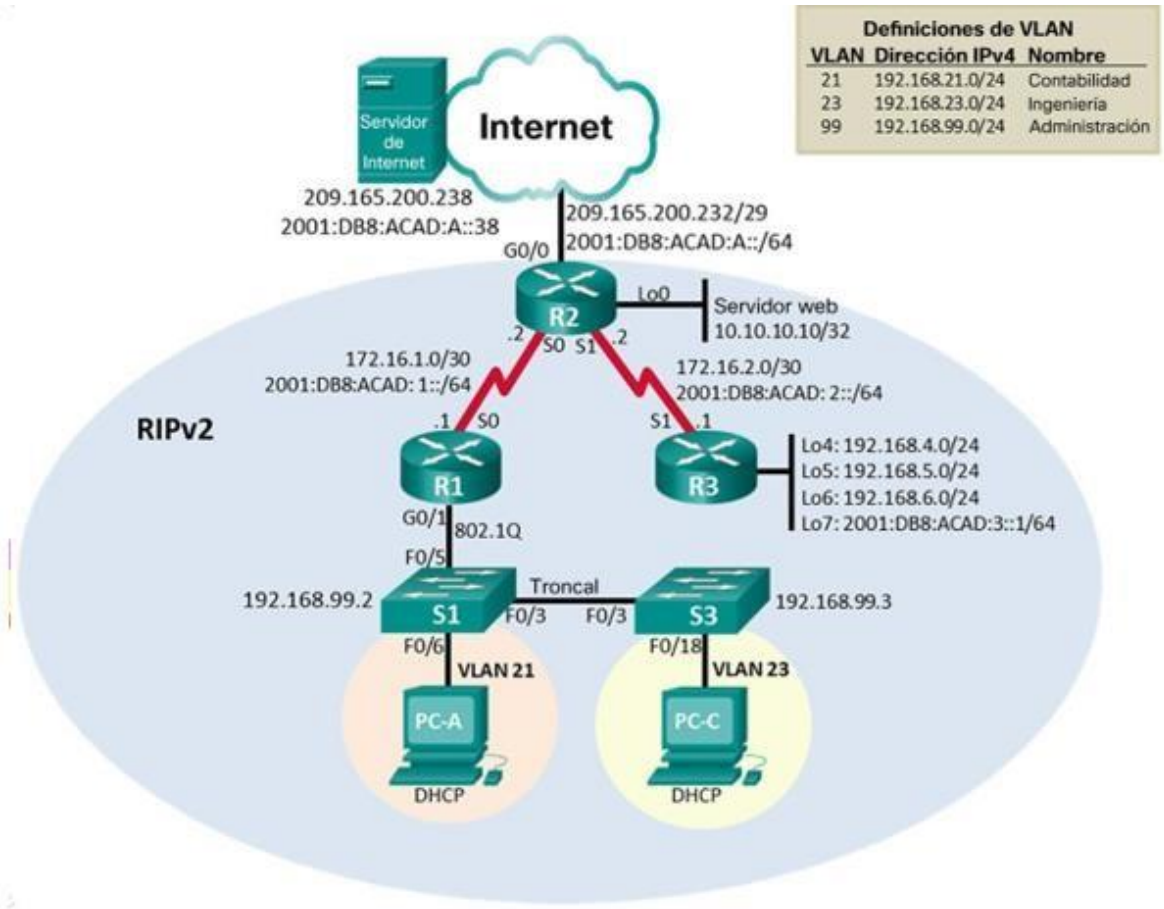

Ilustración 1 Topología de la red del escenario 1

Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos

En esta primera parte, se establece la topología de la red y se borra cualquier configuración anterior que tengan los dispositivos.

Paso 1: Realizar el cableado de red tal como se muestra en la topología

Efectuar la topología de la red, tal como se muestra en la figura 1, requiere inicialmente agregar a la pantalla principal del programa Packet Tracer tres router 2901 y dos switch 2960 y 3 PC's, y además observar que los dispositivos se encuentran unidos por cable ethernet y seriales.

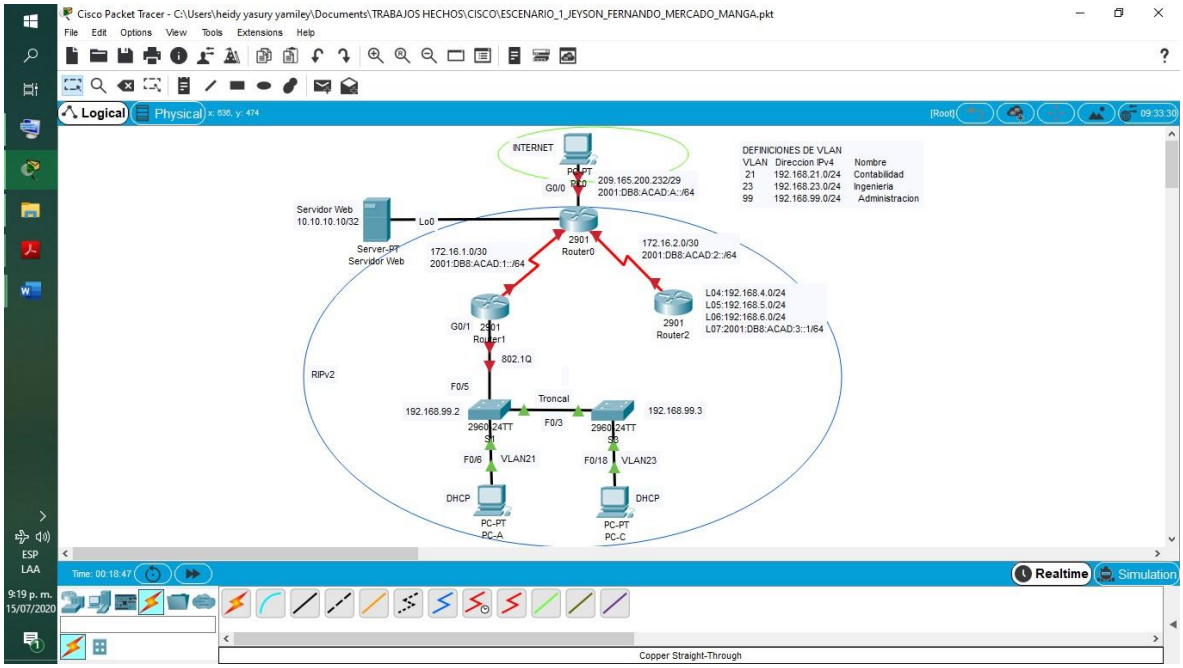

Ilustración 2 Topología de la red en Cisco Packet Tracer

Paso 2: Inicializar y vuelva a cargar los router y los switch

Para efectuar este paso, primero vamos a la pestaña CLI, allí damos enter y volvemos a presionar enter para iniciar, nos aparecerá la línea de comando router> y switch> según corresponda, esto quiere decir que los dispositivos están en usuario modo normal, y en este usuario no se puede realizar ninguna configuración. Entonces luego colocamos el comando enable para cambiar de usuario y damos

enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado router# y switch#, como se muestra a continuación.

Router> enable

Router#

Switch> enable

Switch#

Por medio del comando erase startup-config eliminamos los archivos y con el comando reload volverá a cargar los dispositivos.

Router> enable

Router# erase startup-config

Router# reload

Switch> enable

Switch# erase startup-config

Switch# reload

TAREA	COMANDO DE IOS
Eliminar el archivo startup-config de todos los routers	**Router#Erase startup-config** **Switch#Erase startup-config**
Volver a cargar todos los routers	**Router#Reload** **Switch#Reload**
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	**Router#Erase startup-config** **Router#Delete vlan.dat**

	Switch#Erase startup-config **Switch#Delete vlan.dat**
Volver a cargar ambos switches	**Router# Reload** **Switch#Reload**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	**Router#Show flash** **Switch#Reload**

Tabla 1 Indicaciones para la verificación inicial de los dispositivos

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar 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	**209.165.200.225**
Dirección IPv6/subred	**2001:DB8:ACAD:A::38/64**
Gateway predeterminado IPv6	**2001:DB8:ACAD:2::1**

Tabla 2 Indicaciones para configurar la computadora red internet

Paso 2: Configurar R1

Para realizar la configuración del primer dispositivo se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando router> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios. Como se realizó anteriormente.
2. Desactivar la búsqueda de nombres de dominio, para esto meramente colocamos el comando no ip domain lookup.

3. Cambiar el nombre de usuario, en este caso su nombre por defecto es router, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es R1.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del router banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el router permita el acceso por vía Telnet.
8. Configurar la interfaz s0/3/0 en R1, según la topología y establecer la frecuencia de reloj en 128000 para todas las interfaces DCE del router, además se configurarán rutas predeterminadas para ipv4 y ipv6 a través del comando ip route.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R1.

Router>enable

Router#configure terminal

Router(config)#hostname R1

R1(config)#no ip domain-lookup

R1(config)#service password-encryption

R1(config)#enable secret class

R1(config)#banner motd $Se prohibe el acceso no autorizado$

R1(config)#enable secret cisco

R1(config)#line console 0

R1(config)#password cisco

R1(config)#login

R1(config)#line vty 0 4

R1(config)#password cisco

R1(config)#login

R1(config)#interface s0/3/0

R1(config-if)#ip address 172.16.1.1 255.255.255.252

R1(config-if)#clock rate 128000

R1(config-if)#no shutdown

R1(config)#interface s0/3/0

R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64

R1(config-if)#no shutdown

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/3/0

R1(config)#ipv6 route ::/0 s0/3/0

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Desactivar la búsqueda DNS	**R1(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)#password cisco**
Contraseña de acceso Telnet	**R1(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**R1(config)#service password-encryption**
Mensaje MOTD	**R1(config)#banner motd $Se prohibe el acceso no autorizado$**
Interfaz S0/0/0	**R1(config)#interface s0/3/0** **R1(config-if)#ip address 172.16.1.1 255.255.255.252** **R1(config-if)#clock rate 128000** **R1(config-if)#no shutdown** **R1(config)#interface s0/3/0** **R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64**

	R1(config-if)#no shutdown
Rutas predeterminadas	**R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/3/0** **R1(config)#ipv6 route ::/0 serial s0/3/0**

Tabla 3 Indicaciones para configurar a R1

Paso 3: Configurar R2

Para realizar la configuración del router R2 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando router> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto meramente colocamos el comando no ip domain lookup.
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es router, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es R2.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del router banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el router permita el acceso por vía Telnet.
9. Configurar la interfaz s0/3/0 y s0/3/1 en R2, según la topología y establecer la frecuencia de reloj en 128000 para todas las interfaces DCE del router.
10. Configurar la interfaz G0/0 que conecta con el PC, para la simulación de internet. además, se configurar rutas predeterminadas para ipv4 y ipv6 a través del comando ip route, las direcciones IP se muestran en la topología.
11. Configurar la Interfaz loopback o servidor web simulado.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

Router>enable

Router#configure terminal

Router(config)#hostname R2

R2(config)#no ip domain-lookup

R2(config)#service password-encryption

R2(config)#enable secret class

R2(config)#banner motd $Se prohibe el acceso no autorizado$

R2(config)#enable secret cisco

R2(config)#line console 0

R2(config)#password cisco

R2(config)#login

R2(config)#line vty 0 4

R2(config)#password cisco

R2(config)#login

R2(config)#interface s0/3/0

R2(config-if)#ip address 172.16.1.2 255.255.255.252

R2(config-if)#clock rate 128000

R2(config-if)#no shutdown

R2(config)#interface s0/3/0

R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64

R2(config-if)#no shutdown

R2(config)#interface s0/3/1

R2(config-if)#ip address 172.16.2.2 255.255.255.252

R2(config-if)#clock rate 128000

R2(config-if)#no shutdown

R2(config)#interface s0/3/1

R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64

R2(config-if)#no shutdown

R2(config)#interface g0/0

R2(config-if)#ip address 209.165.200.232 255.255.255.240

R2(config-if)#no shutdown

R2(config)#interface g0/0

R2(config-if)#ipv6 address 2001:DB8:ACAD:A::/64

R2(config-if)#no shutdown

R2(config)#interface loopback 0

R2(config-if)#ip address 10.10.10.10 255.255.255.255

R2(config-if)#no shutdown

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0

R2(config)#ipv6 route ::/0 g0/0

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**
Contraseña de acceso a la consola	**R2(config)#password cisco**
Contraseña de acceso Telnet	**R2(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**R2(config)#service password-encryption**
Habilitar el servidor HTTP	
Mensaje MOTD	**R2(config)#banner motd $Se prohibe el acceso no autorizado$**
Interfaz S0/0/0	**R2(config)#interface s0/3/0** **R2(config-if)#ip address 172.16.1.2 255.255.255.252** **R2(config-if)#clock rate 128000** **R2(config-if)#no shutdown** **R2(config)#interface s0/3/0** **R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64** **R2(config-if)#no shutdown**

Interfaz S0/0/1	**R2(config)#interface s0/3/1** **R2(config-if)#ip address 172.16.2.2 255.255.255.252** **R2(config-if)#clock rate 12800** **R2(config-if)#no shutdown** **R2(config)#interface s0/3/1** **R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64** **R2(config-if)#no shutdown**
Interfaz G0/0 (simulación de Internet)	**R2(config)#interface s0/3/1** **R2(config-if)#ip address 172.16.2.2 255.255.255.252** **R2(config-if)#clock rate 12800** **R2(config-if)#no shutdown** **R2(config)#interface s0/3/1** **R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64** **R2(config-if)#no shutdown**
Interfaz loopback 0 (servidor web simulado)	**R2(config)#interface loopback 0** **R2(config-if)#ip address 10.10.10.10 255.255.255.255** **R2(config-if)#no shutdown**
Ruta predeterminada	**R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0** **R2(config)#ipv6 route ::/0 g0/0**

Tabla 4 Indicaciones para configurar a R2

Paso 4: Configurar R3

Para realizar la configuración del router R3 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando router> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto meramente colocamos el comando no ip domain lookup.

3. Cambiar el nombre de usuario, en este caso su nombre por defecto es router, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es R3.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del router banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el router permita el acceso por vía Telnet.
8. Configurar la interfaz s0/3/1 en R3 para ipv4 y ipv6, según la topología y establecer la frecuencia de reloj en 128000 para todas las interfaces DCE del router.
9. Configurar la interfaz G0/0 que conecta con el PC, para la simulación de internet.
10. Configurar la Interfaz loopback o servidor web simulado 4,5,6 y 7, las direcciones IP se encuentran en la topologia.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

Router>enable

Router#configure terminal

Router(config)#hostname R3

R3(config)#no ip domain-lookup

R3(config)#service password-encryption

R3(config)#enable secret class

R3(config)#banner motd $Se prohibe el acceso no autorizado$

R3(config)#enable secret cisco

R3(config)#line console 0

R3(config)#password cisco

R3(config)#login

R3(config)#line vty 0 4

R3(config)#password cisco

R3(config)#login

R3(config)#interface s0/3/1

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)#interface s0/3/1

R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64

R3(config-if)#no shutdown

R3(config)#interface loopback 4

R3(config-if)#ip address 192.168.4.0 255.255.255.0

R3(config-if)#no shutdown

R3(config)#interface loopback 5

R3(config-if)#ip address 192.168.5.0 255.255.255.0

R3(config-if)#no shutdown

R3(config)#interface loopback 6

R3(config-if)#ip address 192.168.6.0 255.255.255.0

R3(config-if)#no shutdown

R3(config)#interface loopback 7

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

R3(config-if)#no shutdown

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	**R3(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)#password cisco**

Contraseña de acceso Telnet	**R3(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**R3(config)#service password-encryption**
Mensaje MOTD	**R3(config)#banner motd $Se prohibe el acceso no autorizado$**
Interfaz S0/0/1	**R3(config)#interface s0/3/1** **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)#interface s0/3/1** **R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64** **R3(config-if)#no shutdown**
Interfaz loopback 4	**R3(config)#interface loopback 4** **R3(config-if)#ip address 192.168.4.0 255.255.255.0** **R3(config-if)#no shutdown**
Interfaz loopback 5	**R3(config)#interface loopback 5** **R3(config-if)#ip address 192.168.5.0 255.255.255.0** **R3(config-if)#no shutdown**
Interfaz loopback 6	**R3(config)#interface loopback 6** **R3(config-if)#ip address 192.168.6.0 255.255.255.0** **R3(config-if)#no shutdown**
Interfaz loopback 7	**R3(config)#interface loopback 7** **R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64** **R3(config-if)#no shutdown**

Tabla 5 Indicaciones para configurar a R3

Paso 5: Configurar S1

Para realizar la configuración del switch S1 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando switch> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto solamente colocamos el comando no ip domain lookup.
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es switch, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es S1.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del switch banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el switch permita el acceso por vía Telnet.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

Switch>enable

Switch#configure terminal

Switch(config)#hostname S1

S1(config)#no ip domain-lookup

S1(config)#service password-encryption

S1(config)#enable secret class

S1(config)#banner motd $Se prohibe el acceso no autorizado$

S1(config)#enable secret cisco

S1(config)#line console 0

S1(config)#password cisco

S1(config)#login

S1(config)#line vty 0 15

S1(config)#password cisco

S1(config)#login

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	**S1(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)#password cisco**
Contraseña de acceso Telnet	**S1(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**S1(config)#service password-encryption**
Mensaje MOTD	**S1(config)#banner motd $Se prohibe el acceso no autorizado$**

Tabla 6 Indicaciones para configurar a S1

Paso 6: Configurar el S3

Para realizar la configuración del switch S3 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando switch> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto solamente colocamos el comando no ip domain lookup.
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es switch, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es S3.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del switch banner motd y seguido el mensaje.

6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el switch permita el acceso por vía Telnet.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

Switch>enable

Switch#configure terminal

Switch(config)#hostname S3

S3(config)#no ip domain-lookup

S3(config)#service password-encryption

S3(config)#enable secret class

S3(config)#banner motd $Se prohibe el acceso no autorizado$

S3(config)#enable secret cisco

S3(config)#line console 0

S3(config)#password cisco

S3(config)#login

S3(config)#line vty 0 15

S3(config)#password cisco

S3(config)#login

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Desactivar la búsqueda DNS	**S3(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)#password cisco**
Contraseña de acceso Telnet	**S3(config)#password cisco**

Cifrar las contraseñas de texto no cifrado	**S3(config)#service password-encryption**
Mensaje MOTD	**S3(config)#banner motd $Se prohibe el acceso no autorizado$**

Tabla 7 Indicaciones para configurar a S3

Paso 7: Verificar la conectividad de la red

En este paso vamos a utilizar el comando ping en cada uno de los dispositivos para probar la conectividad entre los dispositivos de red.

Si algún ping entre los routers falla, los errores se corregiran usando los comandos show ip route, show ipv6 route y show ip interface brief para detectar los posibles problemas. ya que estos commandos nos permiten ver las configuraciones que se realizaron.

DESDE	A	DIRECCIÓN IP	RESULTADOS DE PING
R1	R2, S0/0/0	172.16.1.2	**R1#ping 172.16.1.2** **Success rate is 100 percent(5/5), round-trip min/avg/max = 1/9/38 ms**
R2	R3, S0/0/1	172.16.2.1	**R1#ping 172.16.1.2** **Success rate is 100 percent(5/5) round-trip min/avg/max = 1/2/8 ms**
PC de Internet	Gateway predeterminado	209.165.200.232	**>ping 209.165.200.232** **Reply from 209.165.200.232: bytes=32 time<1ms TTL=255**

Tabla 8 Verificación de conectividad en los routers y en el PC de internet

En las ilustraciones que observaremos a continuación se muestran los comandos tal como se escribirían en la ventana CLI del router y los resultados de conexión obtenidos en los router y el PC de internet.

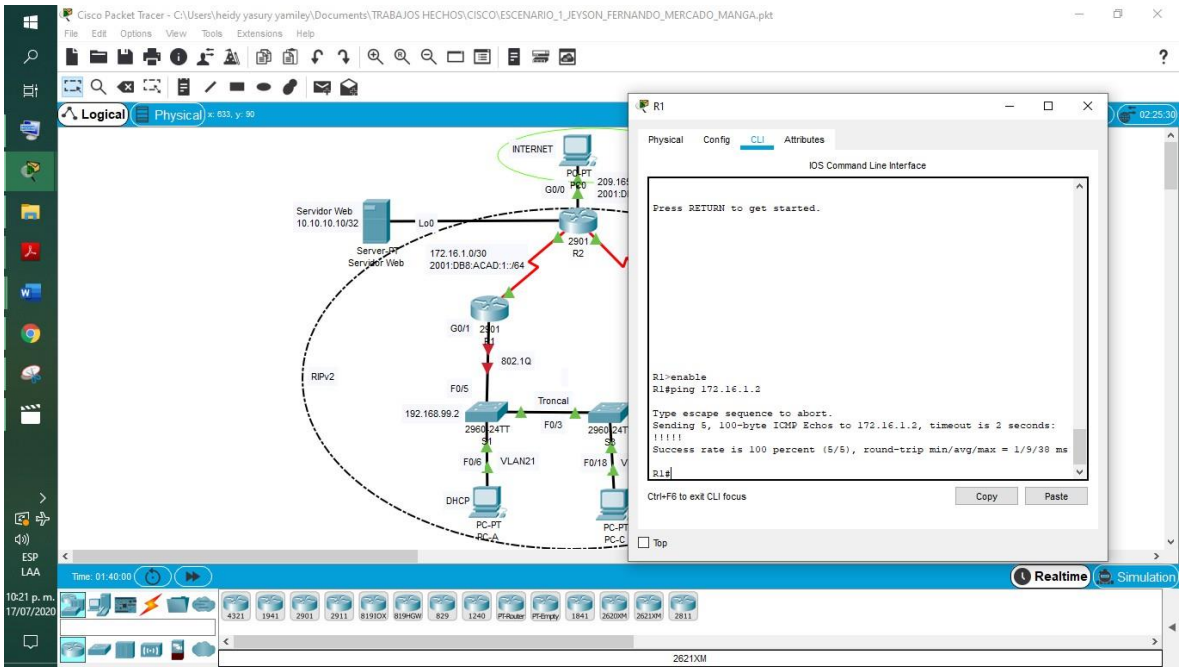

Ilustración 3 Verificación de las configuraciones basicas ping desde R1 a R2

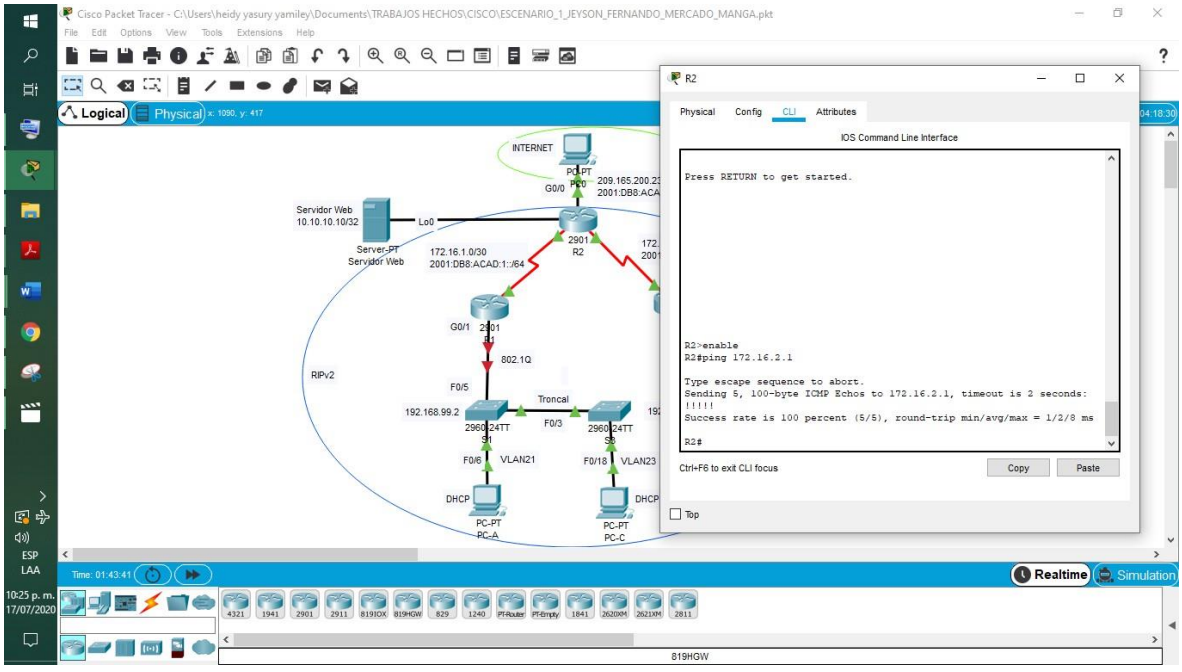

Ilustración 4 Verificación de las configuraciones basicas ping desde R2 a R3

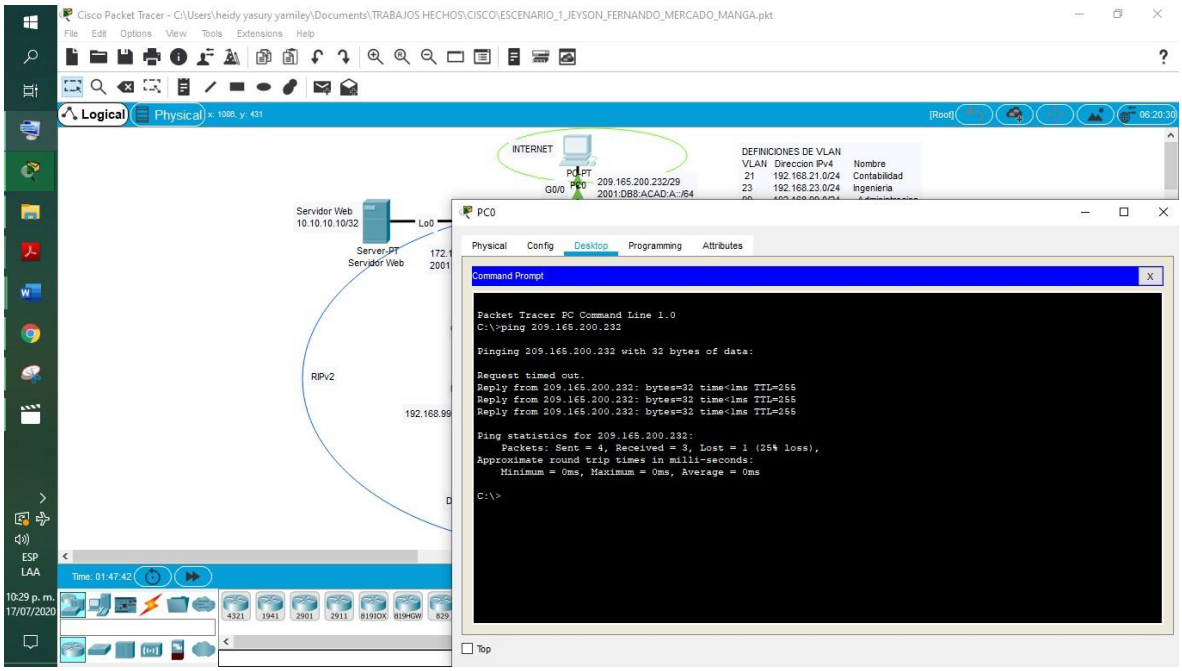

Ilustración 5 Verificación de las configuraciones basicas ping al PC de internet

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

Paso 1: Configurar S1

Primeramente, vamos a crear las tres VLAN con su respectivo nombre, luego vamos a configurar la dirección IP de las interfaces, direcciones que podemos observar en la topología y el gateway predeterminado para cada switch. Seguidamente configuramos la interface fa0/3 y fa0/5, como troncal para que se comunique con el router y utilizamos la red nativa 1, para que la información se transmita por esta vía. También se configuran los otros puertos como puertos de acceso con el comando switchport mode access.
A la interface fa0/6 se le asigna la VLAN 21, después apagamos los puertos sin usar por medio del comando no shutdown.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch S1.

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 administración

S1(config-vlan)#exit

S1(config-if)#interface vlan 99

S1(config-if)#ip address 192.168.99.2 255.255.255.0

S1(config)#ip default-gateway 192.168.99.1

S1(config-if)#no shutdown

S1(config-if)#exit

S1(config)#interface fa0/3

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#interface fa0/5

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#no shutdown

S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2

S1(config-if-range)#switchport mode access

S1(config-if)#interface fa0/6

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 21

S1(config-if)#no shutdown

S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2

S1(config-if-range)#shutdown

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 ingenieria** **S1(config-vlan)#vlan 99** **S1(config-vlan)#name administración** **S1(config-vlan)#exit**
Asignar la dirección IP de administración.	**S1(config-if)#interface 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)#interface fa0/3** **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)#interface fa0/5** **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 1** **S1(config-if)#no shutdown**
Configurar el resto de los puertos como puertos de acceso	**S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S1(config-if-rangen)#switchport mode access**
Asignar F0/6 a la VLAN 21	**S1(config-if)#interface fa0/6** **S1(config-if)#switchport mode access** **S1(config-if)#switchport access vlan 21** **S1(config-if)#no shutdown**
Apagar todos los puertos sin usar	**S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S1(config-if-range)#shutdown**

Tabla 9 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de S1.

Paso 2: Configurar el S3

Se crean las tres VLAN con su respectivo nombre en el switch S3, se asignan las direcciónes IP de las VLAN y el gateway predeterminado. Seguidamente configuramos la interface fa0/3, como troncal para que se comunique con el router y utilizamos la red nativa 1, para que la información se transmita por esta vía. También se configuran los otros puertos como puertos de acceso con el comando switchport mode access.

A la interface fa0/18 se le asigna la VLAN 21 y después apagamos los puertos sin usar por medio del commando shutdown.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

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 administración

S3(config-vlan)#exit

S3(config)#interface vlan 99

S3(config-if)#ip address 192.168.99.3 255.255.255.0

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.99.1

S3(config)#interface fa0/3

S3(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 1

S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2

S3(config-if)#switchport mode access

S3(config-if)#interface fa0/18

S3(config-if)#switchport mode access

S3(config-if)#switchport access vlan 23

S3(config-if-range)#no shutdown

S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2

S3(config-if-range)#shutdown

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear la base de datos de VLAN	**S3(config)#vlan 21** **S3(config-vlan)#name contabilidad** **S3(config-vlan)#vlan 23** **S3(config-vlan)#name ingenieria** **S3(config-vlan)#vlan 99** **S3(config-vlan)#name administración** **S3(config-vlan)#exit**
Asignar la dirección IP de administración	**S3(config)#interface vlan 99** **S3(config-if)#ip address 192.168.99.3 255.255.255.0** **S3(config-if)#exit**
Asignar el gateway predeterminado.	**S3(config)#ip default-gateway 192.168.99.1**
Forzar el enlace troncal en la interfaz F0/3	**S3(config)#interface fa0/3** **S3(config-if)#switchport mode trunk** **S3(config-if)#switchport trunk native vlan 1**
Configurar el resto de los puertos como puertos de acceso	**S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S3(config-if)#switchport mode access**
Asignar F0/18 a la VLAN 21	**S3(config-if)#interface fa0/18** **S3(config-if)#switchport mode access** **S3(config-if)#switchport access vlan 23** **S3(config-if-range)#no shutdown**
Apagar todos los puertos sin usar	**S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2** **S3(config-if-range)#shutdown**

Tabla 10 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de S3.

Paso 3: Configurar R1

En este paso se configurarán la subinterfaz 802.1Q en la interfaz g0/1, creamos los puertos virtuales para cada VLAN asignándole una dirección IP dependiendo de estas mismas y por último se enciende la interfaz por medio del comando no shutdown.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del switch.

R1(config)#interface g0/1.21

R1(config-subif)#description accounting LAN

R1(config-subif)#Encapsulation dot1q 21

R1(config-subif)#Ip address 192.168.21.1 255.255.255.0

R1(config-subif)# interface g0/1.23

R1(config-subif)#description accounting LAN

R1(config-subif)#Encapsulation dot1q 23

R1(config-subif)#Ip address 192.168.23.1 255.255.255.0

R1(config-subif)# interface g0/1.99

R1(config-subif)#description accounting LAN

R1(config-subif)#Encapsulation dot1q 99

R1(config-subif)#Ip address 192.168.99.1 255.255.255.0

R1(config-subif)# interface g0/1

R1(config-subif)#no shutdown

ELEMENTO O TAREA DE CONFIGURACIÓN	**ESPECIFICACIÓN**
Configurar la subinterfaz 802.1Q .21 en G0/1	**R1(config)#interface g0/1.21** **R1(config-subif)#description accounting LAN** **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)# interface g0/1.23** **R1(config-subif)#description accounting LAN** **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)# interface g0/1.99** **R1(config-subif)#description accounting LAN** **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)# interface g0/1** **R1(config-subif)#no shutdown**

Tabla 11 Indicaciones para configurar la seguridad del switch y el routing entre las vlan de R1

Paso 4: Verificar la conectividad de la red

Se utiliza el comando ping en cada uno de los dispositivos para probar la conectividad entre los dispositivos de red.

Si algún ping entre los routers falla, se corregira usando los comandos show ip route, show ipv6 route, show ip interface brief y show vlan brief para detector los posibles problemas, estos comandos nos permiten verificar las configuraciones que se realizaron y las vlan que se crearon con sus respectivas direcciones IP.

DESDE	A	DIRECCIÓN IP	RESULTADOS DE PING
S1	R1, dirección VLAN 99	192.168.99.1	**S1#ping 192.168.99.1** Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	**S3#ping 192.168.99.1** Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	192.168.21.1	**S1#ping 192.168.21.1**

			Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	**S3#ping 192.168.23.1** Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Tabla 12 Verificación de conectividad entre S1, S3 y R1

En las ilustraciones que observaremos a continuación se muestran los comandos tal como se escribirían en la ventana CLI del switch para realizar la verificación y los resultados de conexión obtenidos en los switch.

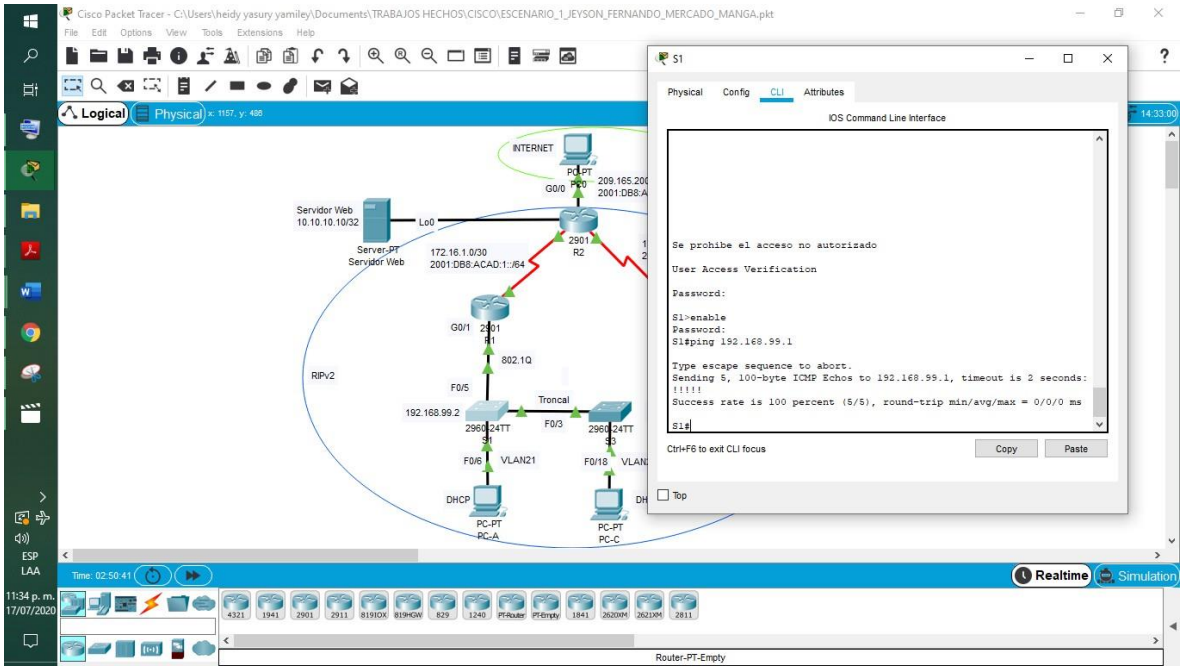

Ilustración 6 Verificación de la vlan 99 desde S1 a R1

Al realizar la verificación de conectividad en la red, primeramente, se obtuvieron algunos errores debidos a que a la hora de escribir los comandos en la ventana CLI, podemos cometer errores pequeños que afectan los buenos resultados que se esperan obtener a partir de las configuraciones realizadas y que omitimos por su pequeñez, pero que pueden provocar que la red no funcione correctamente, por ello es importante realizar verificaciones constantes.

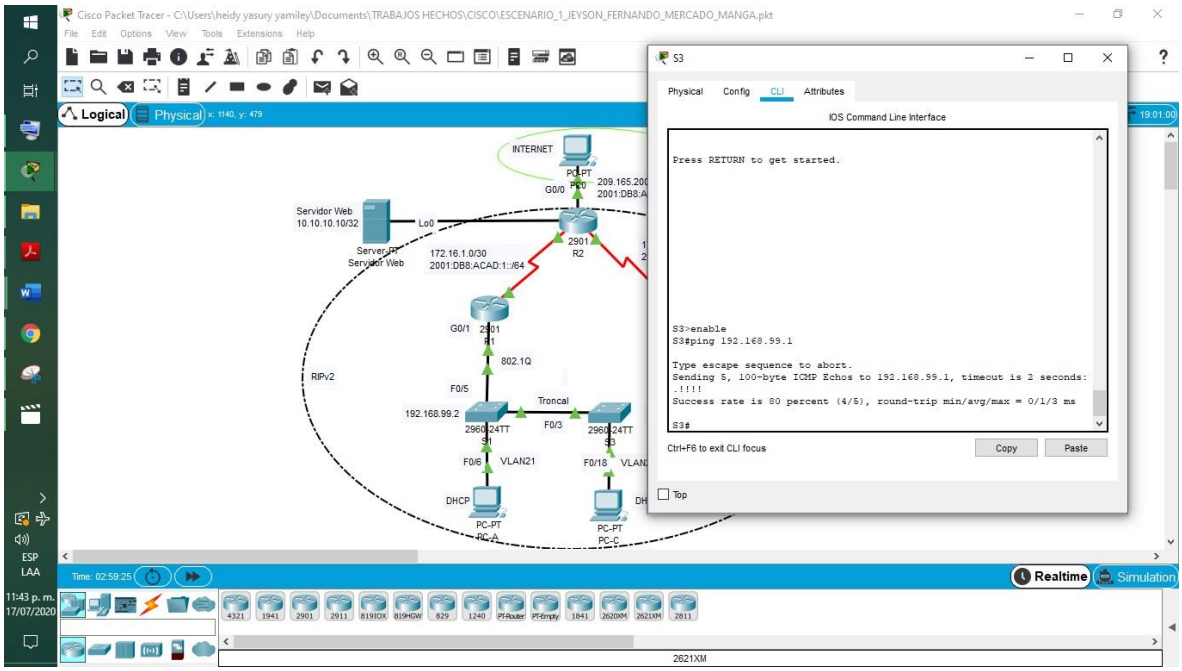

Ilustración 7 Verificación de la vlan 99 desde S3 a R1

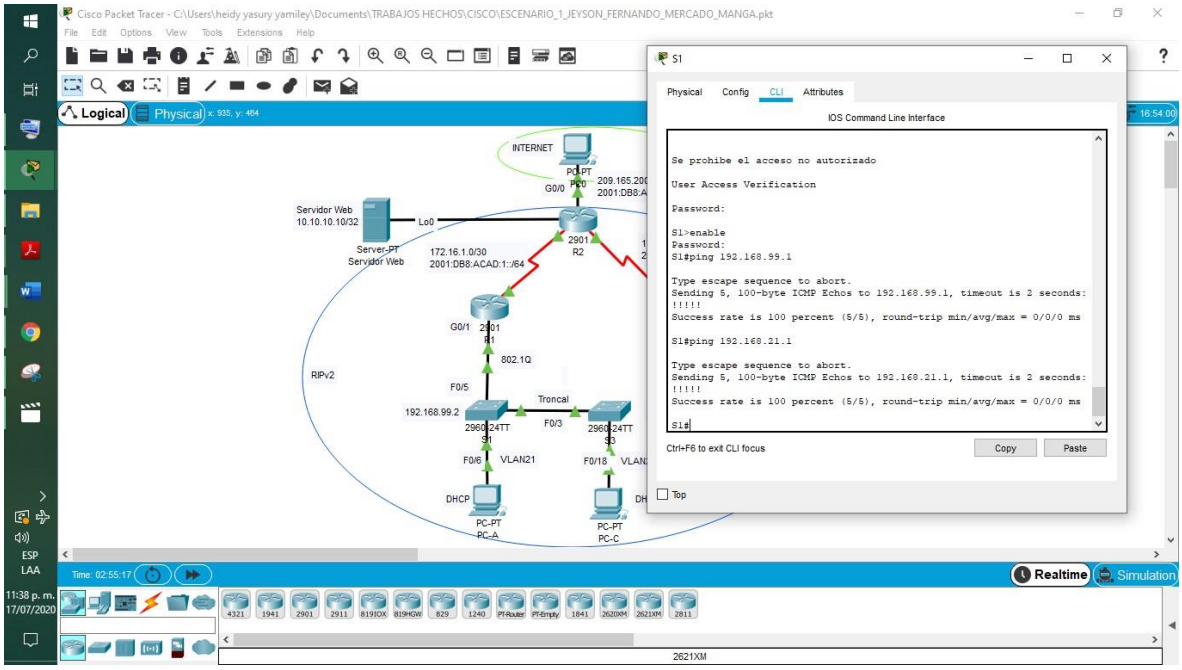

Ilustración 8 Verificación de la vlan 21 desde S1 a R1

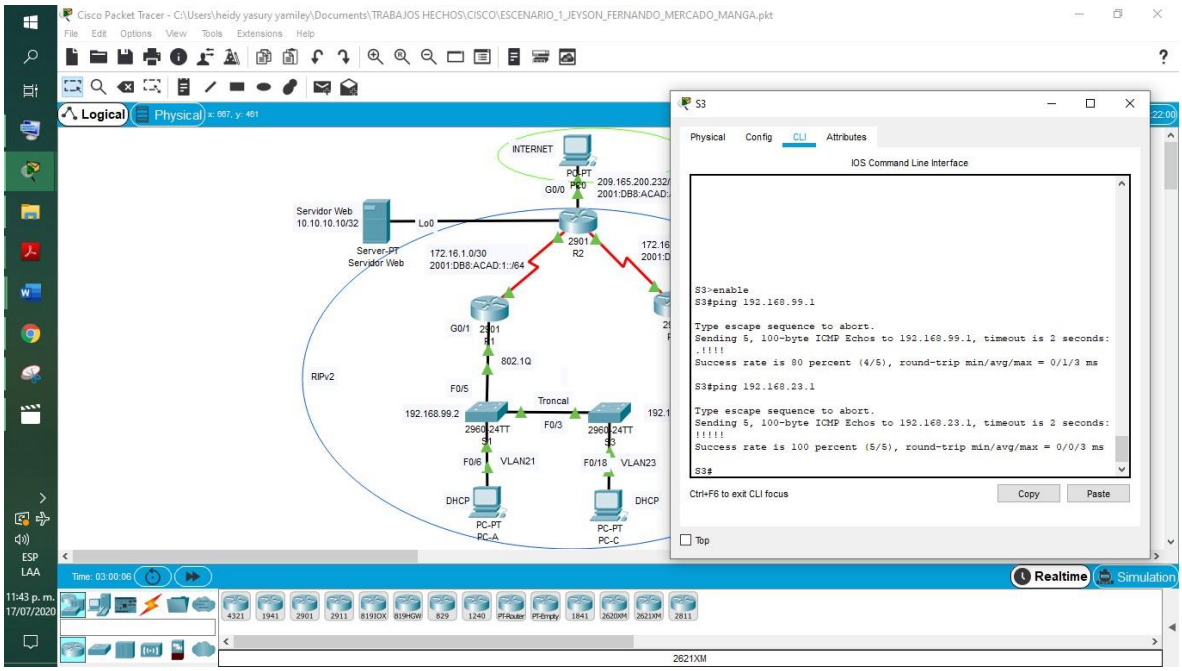

Ilustración 9 Verificación de la vlan 23 desde S3 a R1

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Los protocolos de enrutamiento facilitan el proceso de direccionamiento entre los router, enviando la información por la ruta más cerca, rápida y adecuada.

En este paso se configura el protocolo RIPv2 en el router R1, v2 quiere decir que se utiliza la versión 2, por medio del comando router rip entramos en el modo protocolo RIP, seguidamente colocamos la versión, después se anunciaran las redes que están conectadas directamente usando el comando network.

Se establecerán las interfaces LAN que son g0/1.21, g0/1.23 y g0/1.99 como pasivas, por medio del comando passive-interface y por último se desactiva la sumarizacion automática con el comando auto-summary

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

R1(config)#router rip

R1(config-router)#version 2

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

R1(config-router)#passive-interface g0/1.21

R1(config-router)#passive-interface g0/1.23

R1(config-router)#passive-interface g0/1.99

R1(config-router)#no auto-summary

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)#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**

Tabla 13 Indicaciones para configurar RIPv2 en R1

Paso 2: Configurar RIPv2 en el R2

En este paso se configura el protocolo RIPv2 en el router R2, v2 quiere decir que se utiliza la versión 2, por medio del comando router rip entramos en el modo protocolo RIP, seguidamente colocamos la versión, después se anunciaran las redes que están conectadas directamente usando el comando network.

Se establecerán las interfaces LAN loopback 4,5 y 6 como pasivas, por medio del comando passive-interface y por último se desactiva la sumarizacion automática con el comando auto-summary

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 172.16.1.0

R2(config-router)#network 172.16.2.0

R2(config-router)#network 10.10.10.10

R2(config-router)#network 192.168.4.0

R2(config-router)#network 192.168.5.0

R2(config-router)#network 192.168.6.0

R2(config-router)#passive-interface lo4

R2(config-router)#passive-interface lo5

R2(config-router)#passive-interface lo6

R2(config-router)#no auto-summary

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)#network 172.16.1.0** **R2(config-router)#network 172.16.2.0** **R2(config-router)#network 10.10.10.10** **R2(config-router)#network 192.168.4.0** **R2(config-router)#network 192.168.5.0** **R2(config-router)#network 192.168.6.0**
Establecer la interfaz LAN (loopback) como pasiva	**R2(config-router)#passive-interface lo4** **R2(config-router)#passive-interface lo5** **R2(config-router)#passive-interface lo6**
Desactive la sumarización automática.	**R2(config-router)#no auto-summary**

Tabla 14 Indicaciones para configurar RIPv2 en R2

Paso 3: Configurar RIPv2 en el R3

En este paso se configura el protocolo RIPv2 en el router R3, v2 quiere decir que se utiliza la versión 2, por medio del comando router rip entramos en el modo protocolo RIP, seguidamente colocamos la versión, después se anunciaran las redes que están conectadas directamente usando el comando network.

Se establecerán las interfaces LAN loopback 4,5 y 6 como pasivas, por medio del comando passive-interface y por último se desactiva la sumarizacion automática con el comando auto-summary

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

R3(config)#router rip

R3(config-router)#version 2

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

R3(config-router)#passive-interface lo4

R3(config-router)#passive-interface lo5

R3(config-router)#passive-interface lo6

R3(config-router)#no auto-summary

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 lo4** **R3(config-router)#passive-interface lo5** **R3(config-router)#passive-interface lo6**
Desactive la sumarización automática.	**R3(config-router)#no auto-summary**

Tabla 15 Indicaciones para configurar RIPv2 en R3

Paso 4: Verificar la información de RIP

Para realizar la verificación de las configuraciones que se realizaron en los router con el protocolo RIPv2 podemos utilizar el commando show ip protocols, este comando no solo nos muestra que protocolo estamos usando, sino también las rutas que anunciamos como cercanas al router y las rutas que se configuraron como pasivas.

El comando show ip route rip nos muestra solamente las rutas rip que configuramos

El comando show running-config nos permite ver todas las configuraciones que se han realizado en el dispositivo.

PREGUNTA	RESPUESTA
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	**R1#Show ip protocols** **R2#Show ip protocols** **R3#Show ip protocols**
¿Qué comando muestra solo las rutas RIP?	**R1#Show ip route rip** **R2#Show ip route rip** **R3#Show ip route rip**
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	**R1#Show run** **R2#Show run** **R3#Show run**

Tabla 16 Comandos para realizar las verificaciones de las configuraciones que se realizaron

En las ilustraciones que observaremos a continuación se muestran los comandos tal como se escribirían en la ventana CLI del router y la información de las configuraciones que se realizaron.

R1#Show ip protocols

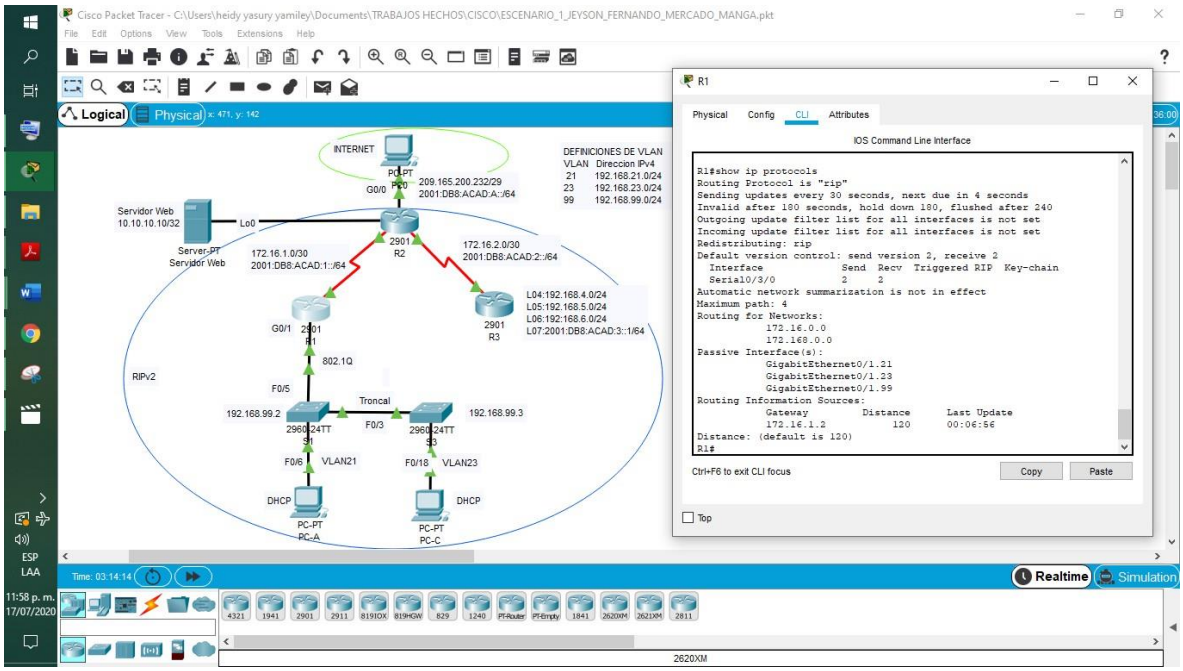

Ilustración 10 Verificación de la información por medio del comando show ip protocols en R1

R1#Show ip route rip

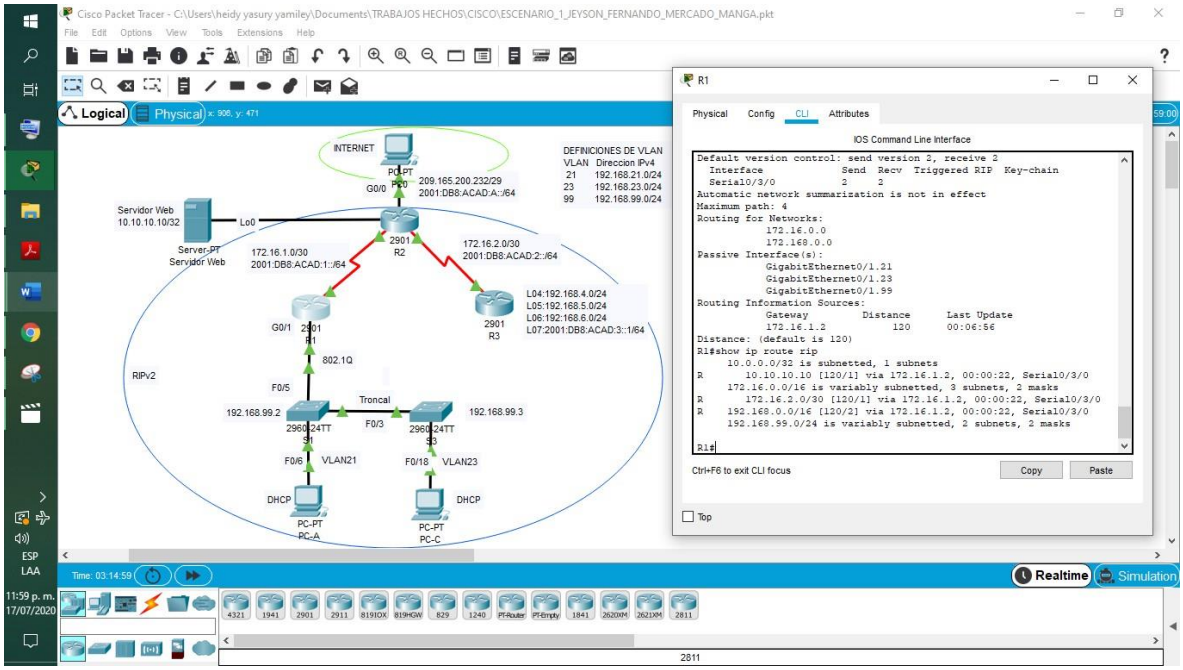

Ilustración 11 Verificación de la información por medio del comando show ip route rip en R1

R1#Show run

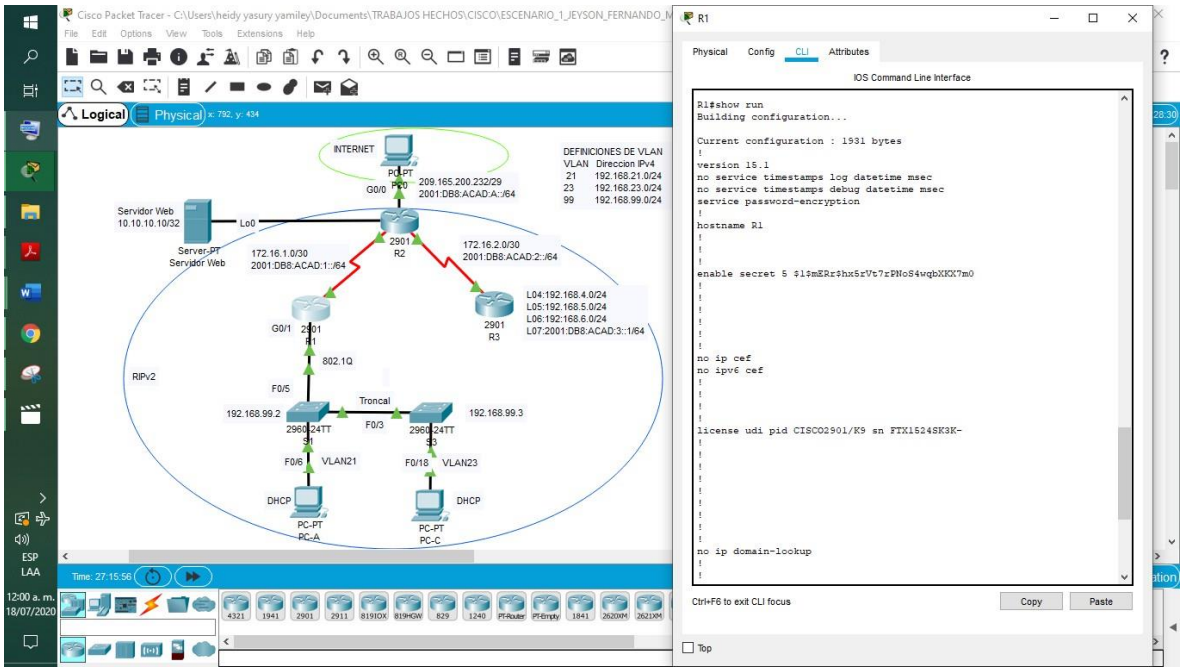

Ilustración 12 Verificación de la información por medio del comando show run en R1

R2#Show ip protocols

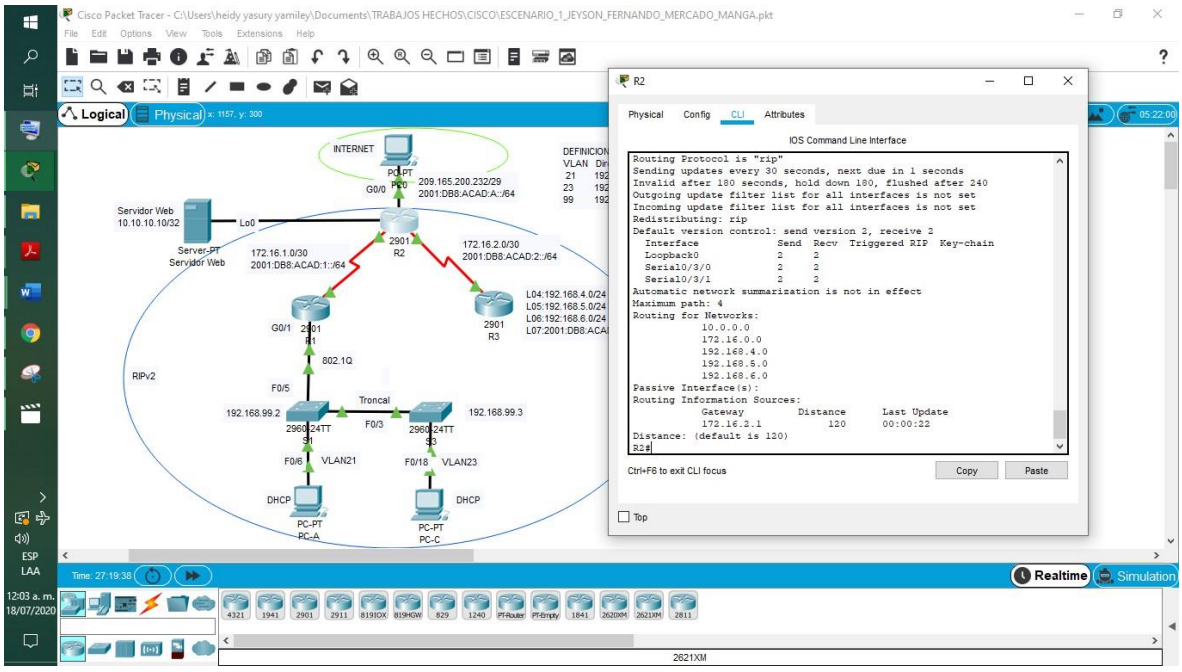

Ilustración 13 Verificación de la información por medio del comando show ip protocols en R2

R2#Show ip route rip

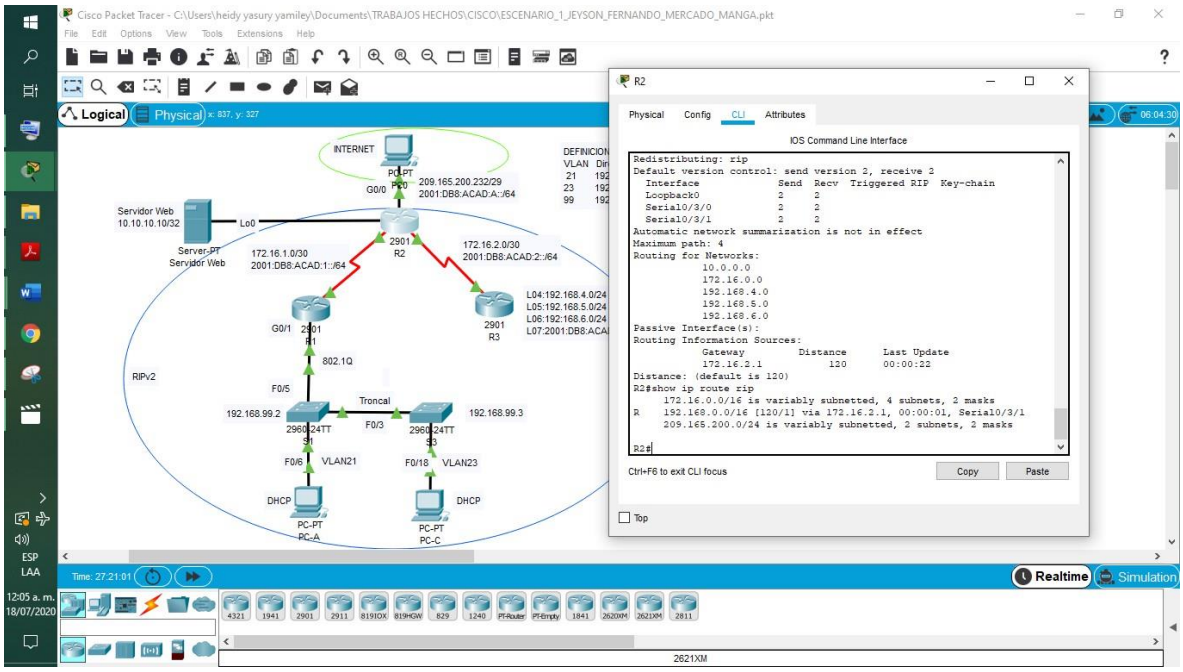

Ilustración 14 Verificación de la información por medio del comando show ip router rip en R2

R2#Show run

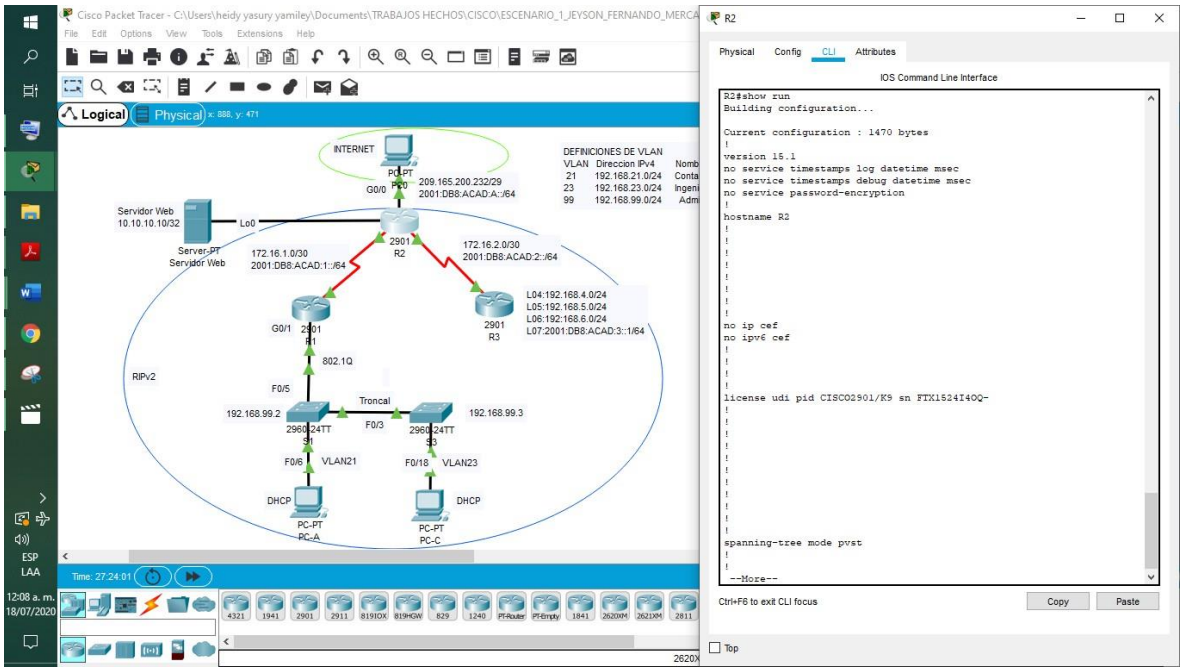

Ilustración 15 Verificación de la información por medio del comando show run en R2

R3#Show ip protocols

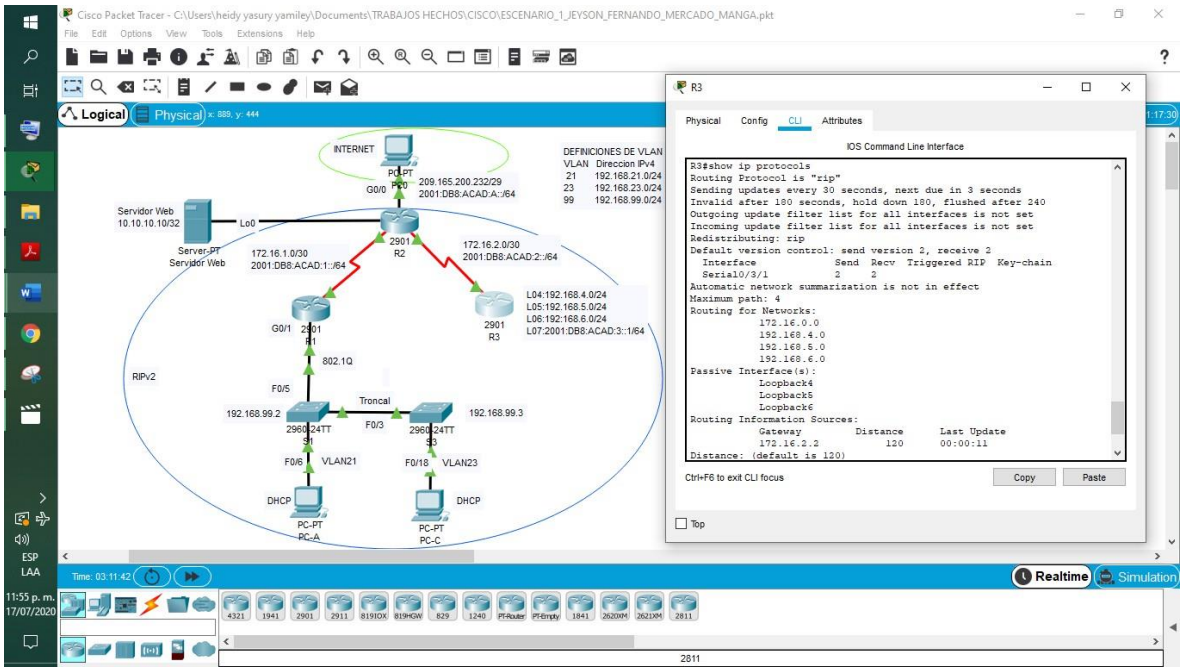

Ilustración 16 Verificación de la información por medio del comando show ip protocols en R3

R3#Show ip route rip

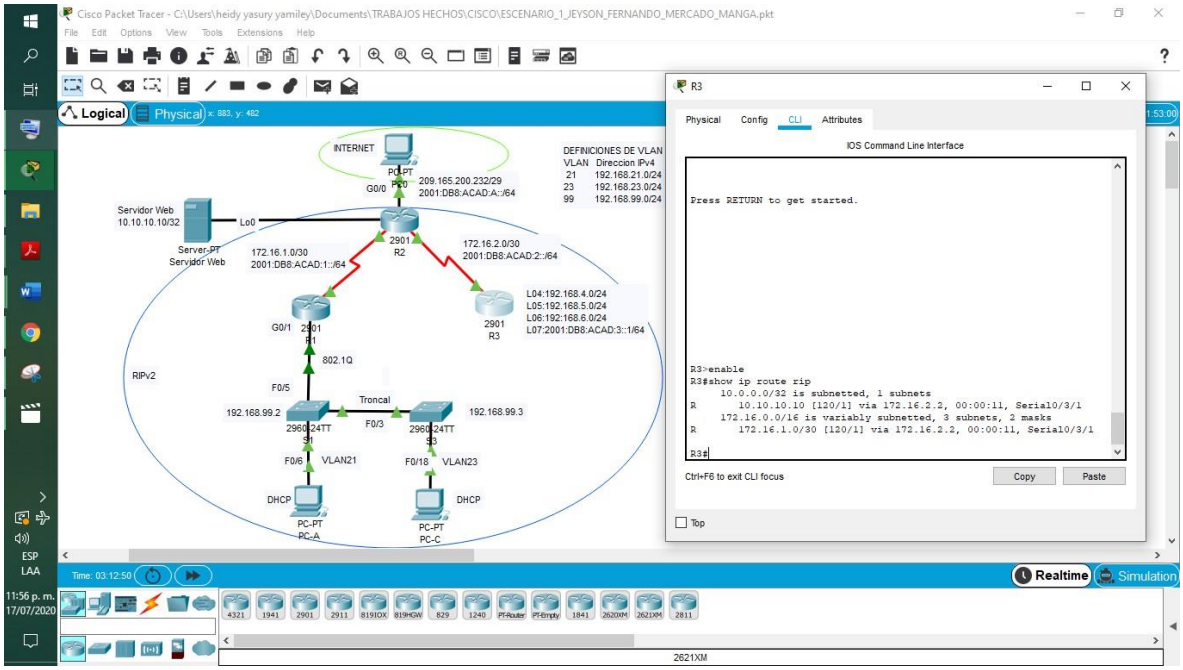

Ilustración 17 Verificación de la información por medio del comando show ip router rip en R3

R3#Show run

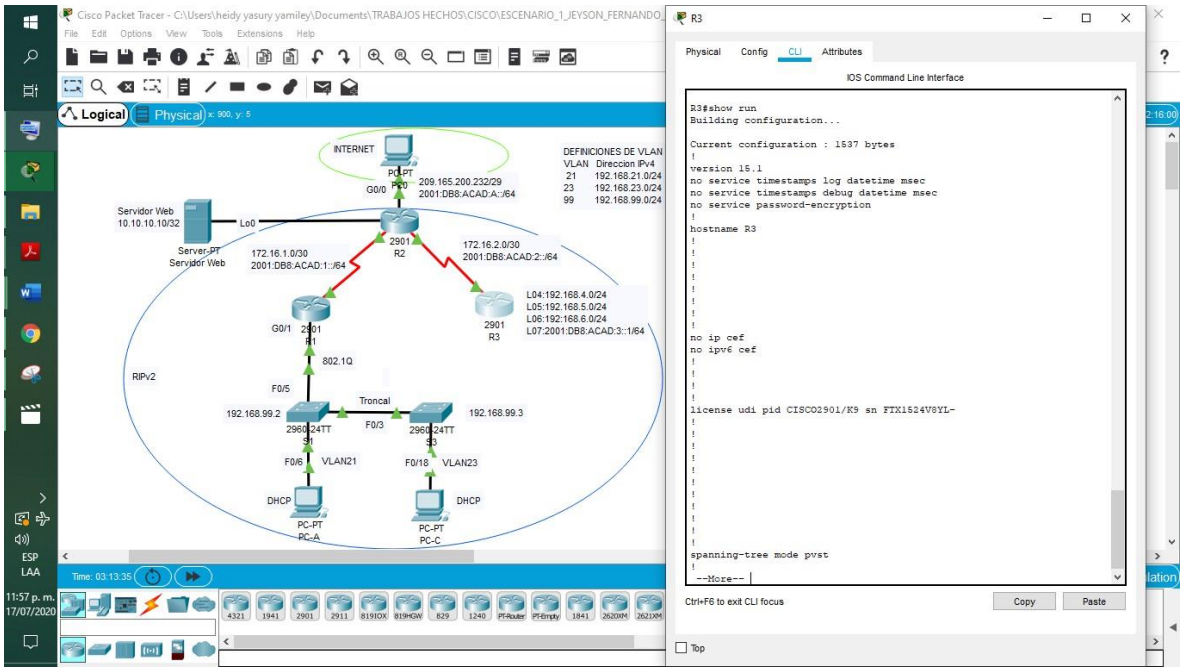

Ilustración 18 Verificación de la información por medio del comando show run en R3

Parte 5: Implementar DHCP y NAT para IPv4

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

Ahora configuramos el dhcp en R1, por medio del comando ip dhcp pool para la VLAN 21 y la 23, le asignamos un nombre ACCT y ENGNR, un servidor DNS con la IP 10.10.10.10, un nombre de dominio ccna-sa.com y la puerta de enlace según corresponda a la VLAN y además se guardan las primeras 20 direcciones IP para la VLAN 21 y la VLAN 23

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

R1(config)#ip dhcp pool ACCT

R1(config)#dns-server 10.10.10.10

R1(config)#domain-name ccna-sa.com

R1(config)#default-router 192.168.21.1

R1(config)#ip dhcp pool ENGNR

R1(config)#dns-server 10.10.10.10

R1(config)#domain-name ccna-sa.com

R1(config)#default-router 192.168.23.1

R1(config)#network 192.168.23.0 255.255.255.0

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 dchp pool ACCT R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.21.1**
Crear un pool de DHCP para la VLAN 23	**R1(config)#ip dhcp pool ENGNR R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.23.1**

Tabla 17 Indicaciones para configurar R1 como servidor de DHCP

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

Primero se crea una base de datos local por medio del comando user, en donde webuser es el nombre de usuario, privilege 15 es decir con privilegio 15 y con una contraseña secreta cisco 12345.

Luego creamos una NAT estatica con el commando ip nat inside source static con la direccion IP 10.10.10.10 y la puerta de enlace 209.165.200.229, despues asignamos la interfaz g0/1 como externa y la interfaz f0/6 como interna para la NAT estatica que se creo anteriormente.

Precisamos las direcciones IP publicas utilizadas con el comando ip nat pool.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R2.

R2(config)#user webuser privilege 15 secret cisco12345

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

R2(config)#interface gi0/1

R2(config)#ip nat outside

R2(config)#interface fa0/6

R2(config)#ip nat inside

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

R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear una base de datos local con una cuenta de usuario	**R2(config)#user webuser privilege 15 secret cisco12345**
Habilitar el servicio del servidor HTTP	**Packet Tracer no procesa la configuraion HTTP**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	**R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	**R2(config)#interface gi0/1** **R2(config)#ip nat outside** **R2(config)#interface fa0/6** **R2(config)#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 209.165.200.225 209.165.200.228 netmask 255.255.255.248**
Definir la traducción de NAT dinámica	**R2(config)#ip nat inside source list 1 pool INTERNET**

Tabla 18 Indicaciones para realizar la configuración NAT en R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

Para realizar este paso vamos a ingresar en la pestaña IP configuration del PC-A y del PC-C, allí observaremos si la información de IP del servidor de DHCP está funcionando, También ingresaremos a la pestaña command prompt para hacer ping desde el PC-A al PC-C y así poder comprobar que hay comunicación entre los equipos.

En las ilustraciones que observamos a continuación se muestra si en cada PC está funcionando el protocolo DHCP y si hay comunicación entre el PC-A y el PC-C.

PRUEBA	RESULTADOS
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	**DHCP request successful**
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	**DHCP request successful**
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	**Successful**
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	**Successful**

Tabla 19 Verificación del protocolo DHCP y NAT en los dispositivos

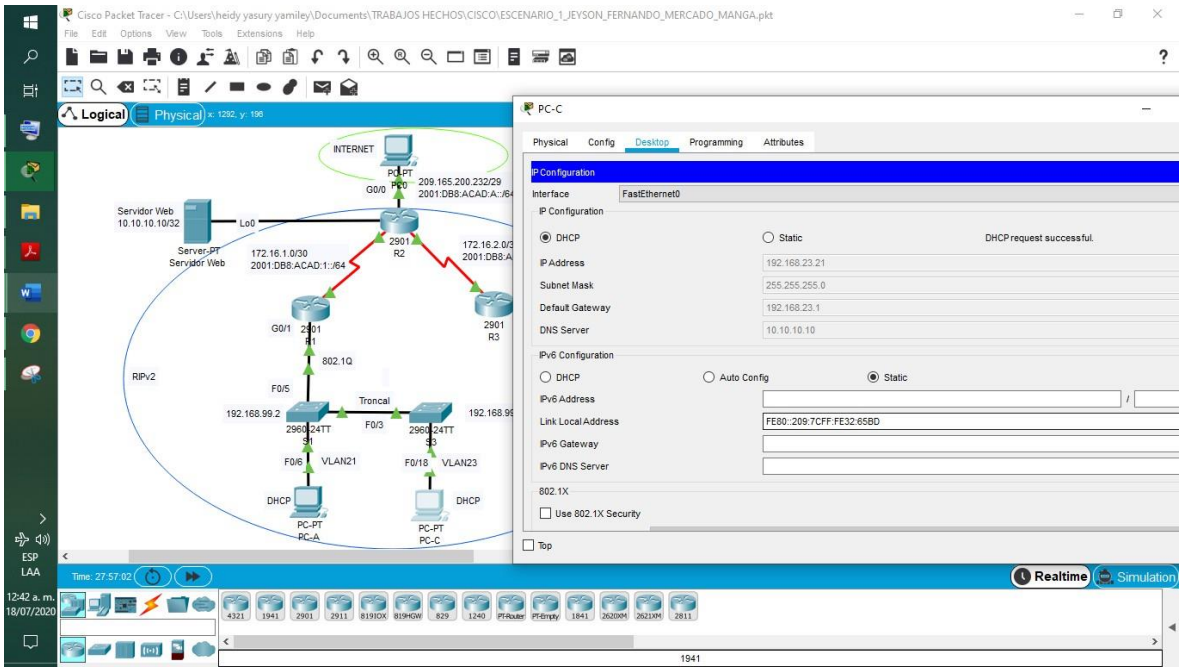

Ilustración 19 Verificación de DHCP en PC-C

Parte 6: Configurar NTP

NTP es un protocolo diseñado para sincronizar los relojes de las estaciones de trabajo a través de la red, por medio de los siguientes comandos realizaremos esta configuración en los dispositivos.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R1 y R2

R2#clock set 09:00:00 05 march 2016

R2(config)#ntp master 5

R1(config)#ntp client 5

R1(config)#ntp update-calendar

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(config)#ntp master 5**
Configurar R1 como un cliente NTP.	**R1(config)#ntp server 172.16.1.2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	**R1(config)#ntp update-calendar**
Verifique la configuración de NTP en R1.	**R1#show ntp associations** **R1#show clock**

Tabla 20 Indicaciones para configurar NTP en R1 Y R2

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

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

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R2, para restringir el acceso a las líneas de control de acceso.

R2(config)#ip access-list standart ADMIN-MGT

R2(config-std-nacl)#permit host 172.16 1.1

R2(config-std-nacl)#exit

R2(config-line)#line vty 0 4

R2(config-line)#access-class ADMIN-MGT in

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	**R2(config)#ip access-list standart ADMIN-MGT**

Aplicar la ACL con nombre a las líneas VTY	**R2(config-line)#line vty 0 4**
Permitir acceso por Telnet a las líneas de VTY	**R2(config-line)#access-class ADMIN-MGT in**
Verificar que la ACL funcione como se espera	

Tabla 21 Indicaciones para configurar y verificar las ACL

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

En la tabla que se muestra en este paso, observaremos algunos comandos necesarios según la necesidad que tengamos en el momento de estar realizando las configuraciones y después de terminarlas.

DESCRIPCIÓN DEL COMANDO	ENTRADA DEL ESTUDIANTE (COMANDO)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	**#show ip access list**
Restablecer los contadores de una lista de acceso	**#clear ip**
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	**#show ip interface**
¿Con qué comando se muestran las traducciones NAT?	**#show ip nat translations**
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	**#clear ip nat translations**

Tabla 22 Comandos para realizar las verificaciones de las configuraciones realizadas en los dispositivos

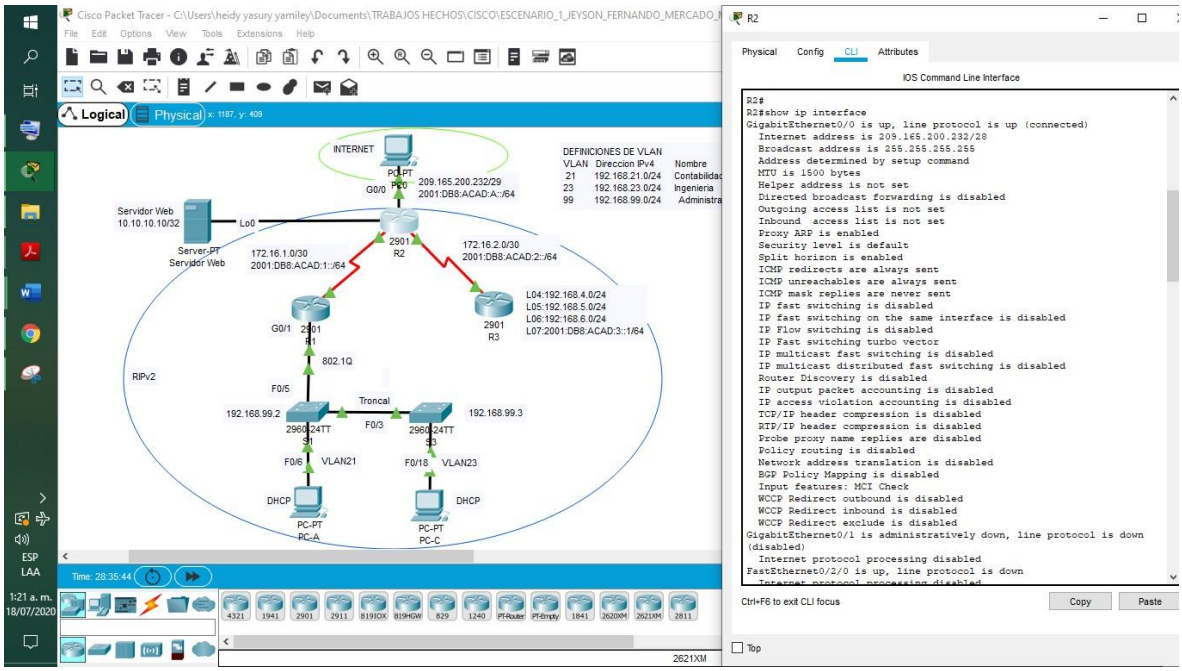

Ilustración 20 Verificación del show interface en R2

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.

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.

Topología

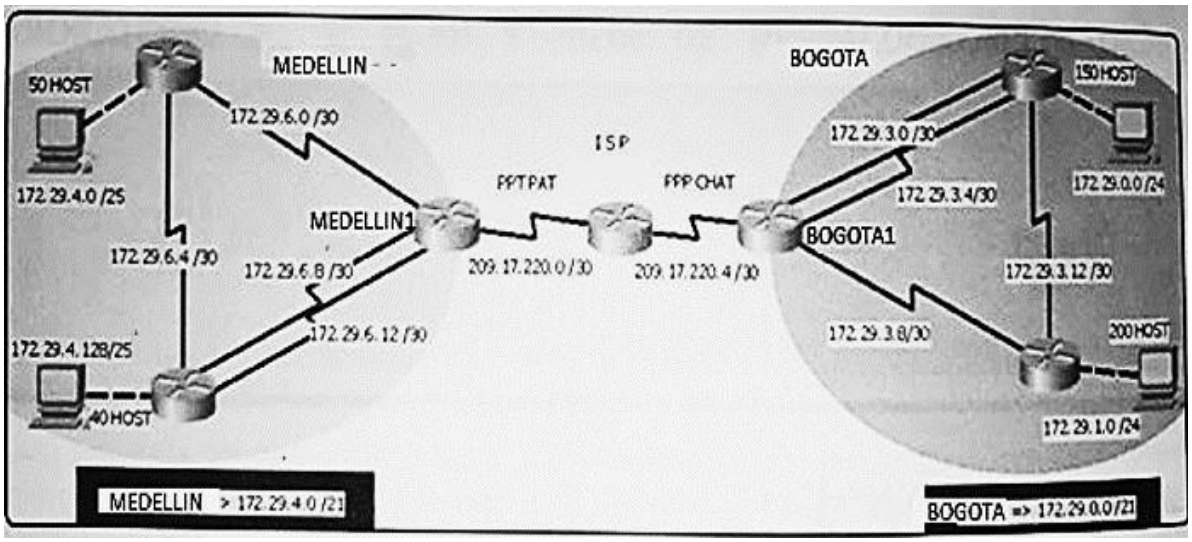

Ilustración 21 Topología de la red del escenario 2

Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos

En esta primera parte, se establece la topología de la red y se borra cualquier configuración anterior que tengan los dispositivos.

Paso 1: Realizar el cableado de red tal como se muestra en la topología

Efectuar la topología de la red, tal como se muestra en la ilustración, requiere inicialmente agregar a la pantalla principal del programa Packet Tracer siete router 2901 y 4 PC's, y además observar que los dispositivos se encuentran unidos por cable ethernet y puertos seriales.

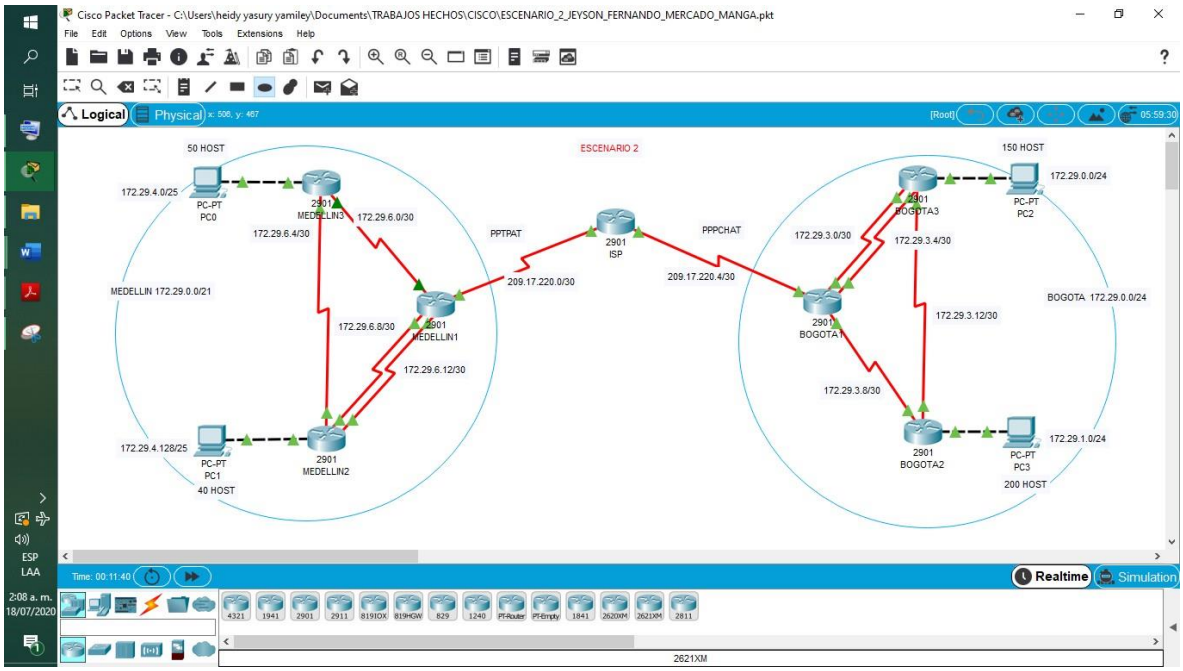

Ilustración 22 Topología de la red en Cisco Packet Tracer

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar los Routers

Para realizar la configuración de los dispositivos se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando router> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios. Como se realizó anteriormente.

2. Desactivar la búsqueda de nombres de dominio, para esto meramente colocamos el comando no ip domain lookup.
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es router, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que le corresponda.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del router banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el router permita el acceso por vía Telnet.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router según les corresponde.

- ISP

Router>enable

Router#configure terminal

Router(config)#hostname ISP

ISP(config)#no ip domain-lookup

ISP(config)#service password-encryption

ISP(config)#enable secret class

ISP(config)#banner motd $Se prohibe el acceso no autorizado$

ISP(config)#enable secret cisco

ISP(config)#line console 0

ISP(config)#password cisco

ISP(config)#login

ISP(config)#line vty 0 4

ISP(config)#password cisco

ISP(config)#login

- MEDELLIN 1 (M1)

Router>enable

Router#configure terminal

Router(config)#hostname M1

M1(config)#no ip domain-lookup

M1(config)#service password-encryption

M1(config)#enable secret class

M1(config)#banner motd $Se prohibe el acceso no autorizado$

M1(config)#enable secret cisco

M1(config)#line console 0

M1(config)#password cisco

M1(config)#login

M1(config)#line vty 0 4

M1(config)#password cisco

M1(config)#login

- MEDELLIN 1 (M2)

Router>enable

Router#configure terminal

Router(config)#hostname M2

M2(config)#no ip domain-lookup

M2(config)#service password-encryption

M2(config)#enable secret class

M2(config)#banner motd $Se prohibe el acceso no autorizado$

M2(config)#enable secret cisco

M2(config)#line console 0

M2(config)#password cisco

M2(config)#login

M2(config)#line vty 0 4

M2(config)#password cisco

M2(config)#login

- MEDELLIN 1 (M3)

Router>enable

Router#configure terminal

Router(config)#hostname M3

M3(config)#no ip domain-lookup

M3(config)#service password-encryption

M3(config)#enable secret class

M3(config)#banner motd $Se prohibe el acceso no autorizado$

M3(config)#enable secret cisco

M3(config)#line console 0

M3(config)#password cisco

M3(config)#login

M3(config)#line vty 0 4

M3(config)#password cisco

M3(config)#login

- BOGOTA 1 (B1)

Router>enable

Router#configure terminal

Router(config)#hostname B1

B1(config)#no ip domain-lookup

B1(config)#service password-encryption

B1(config)#enable secret class

B1(config)#banner motd $Se prohibe el acceso no autorizado$

B1(config)#enable secret cisco

B1(config)#line console 0

B1(config)#password cisco

B1(config)#login

B1(config)#line vty 0 4

B1(config)#password cisco

B1(config)#login

- BOGOTA 2 (B2)

Router>enable

Router#configure terminal

Router(config)#hostname B2

B2(config)#no ip domain-lookup

B2(config)#service password-encryption

B2(config)#enable secret class

B2(config)#banner motd $Se prohibe el acceso no autorizado$

B2(config)#enable secret cisco

B2(config)#line console 0

B2(config)#password cisco

B2(config)#login

B2(config)#line vty 0 4

B2(config)#password cisco

B2(config)#login

- BOGOTA 3 (B3)

Router>enable

Router#configure terminal

Router(config)#hostname B3

B3(config)#no ip domain-lookup

B3(config)#service password-encryption

B3(config)#enable secret class

B3(config)#banner motd $Se prohibe el acceso no autorizado$

B3(config)#enable secret cisco

B3(config)#line console 0

B3(config)#password cisco

B3(config)#login

B3(config)#line vty 0 4

B3(config)#password cisco

B3(config)#login

Parte 3: Configuración del enrutamiento

Paso 1: Configurar los puertos seriales de cada router

En esta parte se configurara el direccionamiento de cada router como se observa en la topologia.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router según les corresponde.

- ISP

ISP(config)#interface s0/3/0

ISP(config-if)#ip address 209.17.220.5 255.255.255.252

ISP(config-if)#no shutdown

ISP(config-if#exit

ISP(config)#interface s0/3/1

ISP(config-if)#ip address 209.17.220.1 255.255.255.252

ISP(config-if)#no shutdown

ISP(config-router)#exit

- MEDELLIN 1 (M1)

M1(config)#interface s0/3/1 (Ruta por defecto al ISP)

M1(config-if)#ip address 209.17.200.2 255.255.255.252

M1(config-if)#no shutdown

M1(config-if#exit

M1(config)#interface s0/3/0

M1(config-if)#ip address 172.29.6.1 255.255.255.252

M1(config-if)#no shutdown

M1(config-if#exit

M1(config)#interface s0/1/0

M1(config-if)#ip address 172.29.6.13 255.255.255.252

M1(config-if)#no shutdown

M1(config-router)#exit

M1(config)#interface s0/1/1

M1(config-if)#ip address 172.29.6.9 255.255.255.252

M1(config-if)#no shutdown

M1(config-router)#exit

- MEDELLIN 2 (M2)

M2(config)#interface s0/1/0

M2(config-if)#ip address 172.29.6.14 255.255.255.252

M2(config-if)#no shutdown

M2(config-if#exit

M2(config)#interface s0/1/1

M2(config-if)#ip address 172.29.6.10 255.255.255.252

M2(config-if)#no shutdown

M2(config-if#exit

M2(config)#interface s0/3/1

M2(config-if)#ip address 172.29.6.6 255.255.255.252

M2(config-if)#no shutdown

M2(config)#interface gi0/0

M2(config-if)#ip address 172.29.4.130 255.255.255.128

M2 (config-if)#no shutdown

M2 (config-router)#exit

- MEDELLIN 3 (M3)

M3(config)#interface s0/3/0

M3(config-if)#ip address 172.29.6.2 255.255.255.252

M3(config-if)#no shutdown

M3(config-if#exit

M3 (config)#interface s0/3/1

M3 (config-if)#ip address 172.29.6.5 255.255.255.252

M3 (config-if)#no shutdown

M3 (config-if#exit

M3 (config)#interface gi0/0

M3 (config-if)#ip address 172.29.4.2 255.255.255.252

M3 (config-if)#no shutdown

M3 (config-router)#exit

- BOGOTA 1 (B1)

B1 (config)#interface s0/3/0 (Ruta por defecto al ISP)

B1 (config-if)#ip address 209.17.220.6 255.255.255.252

B1 (config-if)#no shutdown

B1 (config-if#exit

B1(config)#interface s0/3/1

B1(config-if)#ip address 172.29.3.9 255.255.255.252

B1(config-if)#no shutdown

B1(config-if#exit

B1(config)#interface s0/1/0

B1(config-if)#ip address 172.29.3.1 255.255.255.252

B1 (config-if)#no shutdown

B1(config-router)#exit

B1(config)#interface s0/1/1

B1(config-if)#ip address 172.29.3.5 255.255.255.252

B1(config-if)#no shutdown

B1(config-router)#exit

- BOGOTA 2 (B2)

B2(config)#interface s0/3/1

B2(config-if)#ip address 172.29.3.10 255.255.255.252

B2(config-if)#no shutdown

B2(config-if#exit

B2(config)#interface s0/3/0

B2(config-if)#ip address 172.29.3.14 255.255.255.252

B2(config-if)#no shutdown

B2(config-router)#exit

B2(config)#interface gi0/0

B2(config-if)#ip address 172.29.1.2 255.255.255.0

B2(config-if)#no shutdown

B2(config-router)#exit

- BOGOTA 3 (B3)

B3(config)#interface s0/1/0

B3(config-if)#ip address 172.29.3.2 255.255.255.252

B3(config-if)#no shutdown

B3(config-if#exit

B3(config)#interface s0/1/1

B3(config-if)#ip address 172.29.3.6 255.255.255.252

B3(config-if)#no shutdown

B3(config-router)#exit

B3(config)#interface s0/3/0

B3(config-if)#ip address 172.29.3.13 255.255.255.252

B3(config-if)#no shutdown

B3(config-router)#exit

B3(config)#interface gi0/0

B3(config-if)#ip address 172.29.0.2 255.255.255.0

B3(config-if)#no shutdown

B3(config-router)#exit

Paso 2: Configurar el Protocolo OSPF en los routers

El Protocolo OSPF es un protocolo de routing de estado de enlace para las redes IP, entonces para configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declaramos la red principal y desactivamos la sumarización automática por medio del commando no auto-summary.

Los routers Bogota1 y Medellín incluiran en su configuración de enrutamiento una ruta por defecto hacia el router ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router según les corresponde.

- ISP

ISP(config)#router ospf 1

ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0

ISP(config-router)#network 209.17.220.0 0.0.0.3 area0

ISP(config-router)#no auto-summary

- MEDELLIN 1 (M1)

M1(config)#router ospf 1

M1(config-router)#network 172.29.6.0 0.0.0.3 area 0

M1(config-router)#network 172.29.6.8 0.0.0.3 area 0

M1(config-router)#network 172.29.6.12 0.0.0.3 area 0

M1 (config-router)#no auto-summary

- MEDELLIN 2 (M2)

M2(config)#router ospf 1

M2(config-router)#network 172.29.4.128 0.0.0.255 area 0

M2(config-router)#network 172.29.6.4 0.0.0.3 area 0

M2(config-router)#network 172.29.6.8 0.0.0.255 area 0

M2(config-router)#network 172.29.6.12 0.0.0.255 area 0

M2(config-router)#no auto-summary

- MEDELLIN 3 (M3)

M3(config)#router ospf 1

M3(config-router)#network 172.29.4.0 0.0.0.255 area 0

M3(config-router)#network 172.29.6.0 0.0.0.3 area 0

M3(config-router)#network 172.29.6.4 0.0.0.255 area 0

M3(config-router)#no auto-summary

- BOGOTA 1 (B1)

B1(config)#router ospf 1

B1(config-router)#network 172.29.3.0 0.0.0.3 area 1

B1(config-router)#network 172.29.3.4 0.0.0.3 area 1

B1(config-router)#network 172.29.3.8 0.0.0.3 area 1

B1(config-router)#no auto-summary

- BOGOTA 2 (B2)

B2(config)#router ospf 1

B2(config-router)#network 172.29.3.8 0.0.0.3 area 1

B2(config-router)#network 172.29.3.12 0.0.0.3 area 1

B2(config-router)#network 172.29.1.0 0.0.0.255 area 1

B2(config-router)#no auto-summary

- BOGOTA 3 (B3)

BOGOTA3(config)#router ospf 1

BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 1

BOGOTA3(config-router)#no auto-summary

Paso 3: Configurar en el router ISP una ruta estatica dirigida hacia M1 y B1

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, esto se realizara por medio del comando ip route.
A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de ISP, M1 y B1.

- ISP

ISP>enable

ISP#configure terminal

ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/3/0

ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/3/1

ISP(config)#ip route 172.29.4.128 255.255.255.128 s0/3/0

ISP(config)#ip route 172.29.1.0 255.255.255.0 s0/3/1

ISP(config)#exit

- MEDELLIN 1 (M1)

MEDELLIN1>enable

MEDELLIN1#configure terminal

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

MEDELLIN1(config)#exit

- BOGOTA 1 (B1)

BOGOTA1>enable

BOGOTA1#configure terminal

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

BOGOTA1(config)#exit

Parte 4: Tabla de enrutamiento

Paso 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Para realizar la verificación del enrutamiento en cada uno de los routers utilizaremos el comando show ip route, este nos permitirá ver como quedo el enrutamiento.

En las ilustraciones que observaremos a continuación se muestra el comando tal como se escribirían en la ventana CLI de cada router para realizar la verificación y la información de las configuraciones que se realizaron.

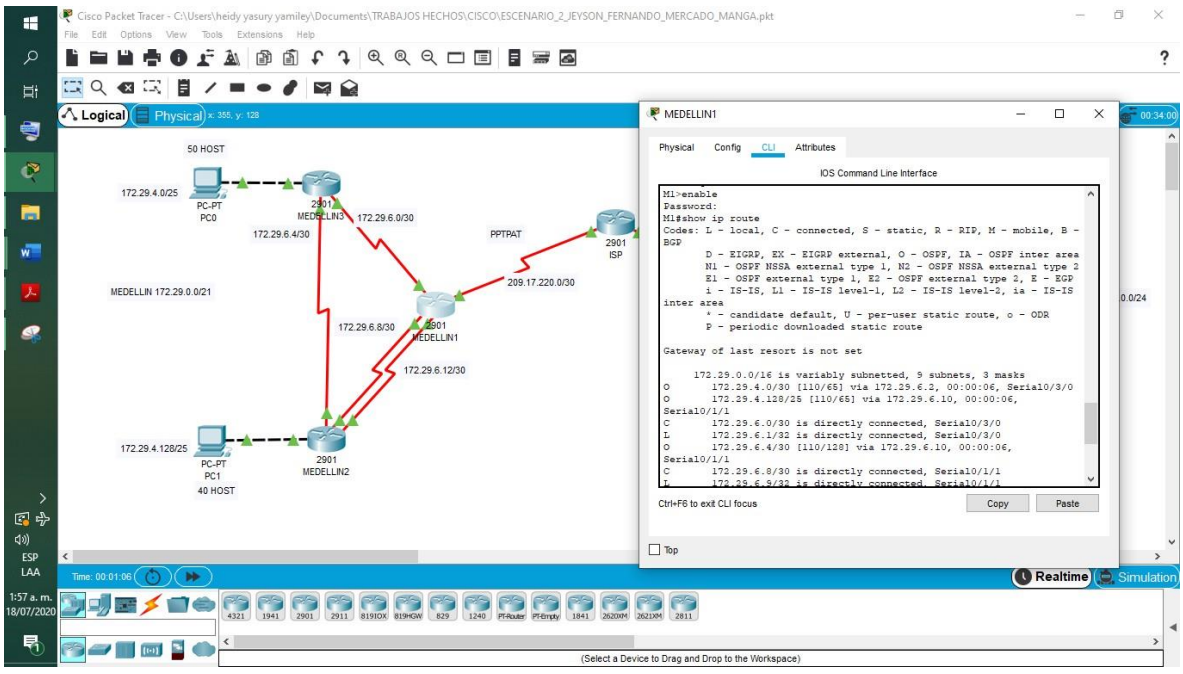

Ilustración 23 Verificación del enrutamiento en M1

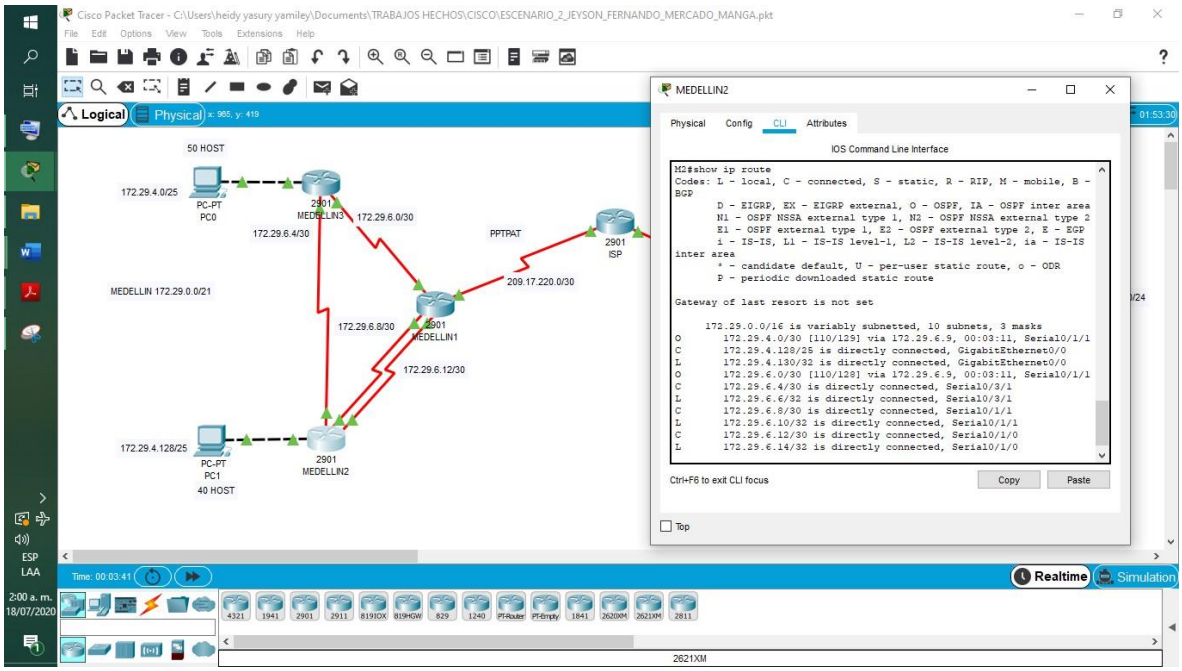

Ilustración 24 Verificación del enrutamiento en M2

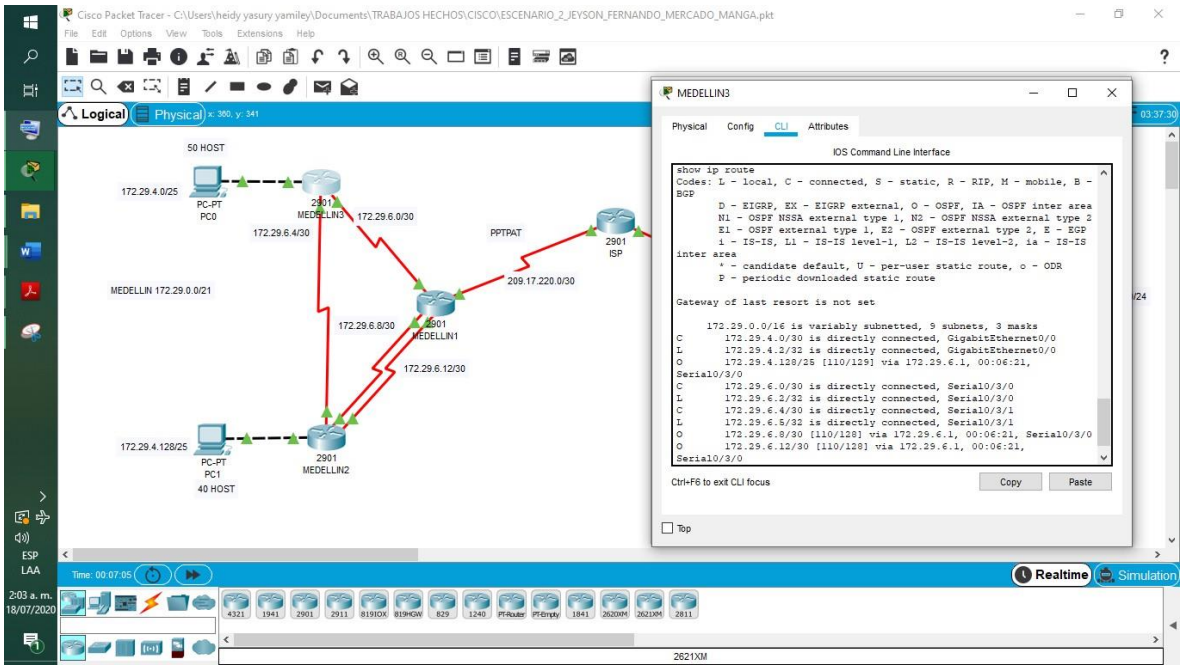

Ilustración 25 Verificación del enrutamiento en M3

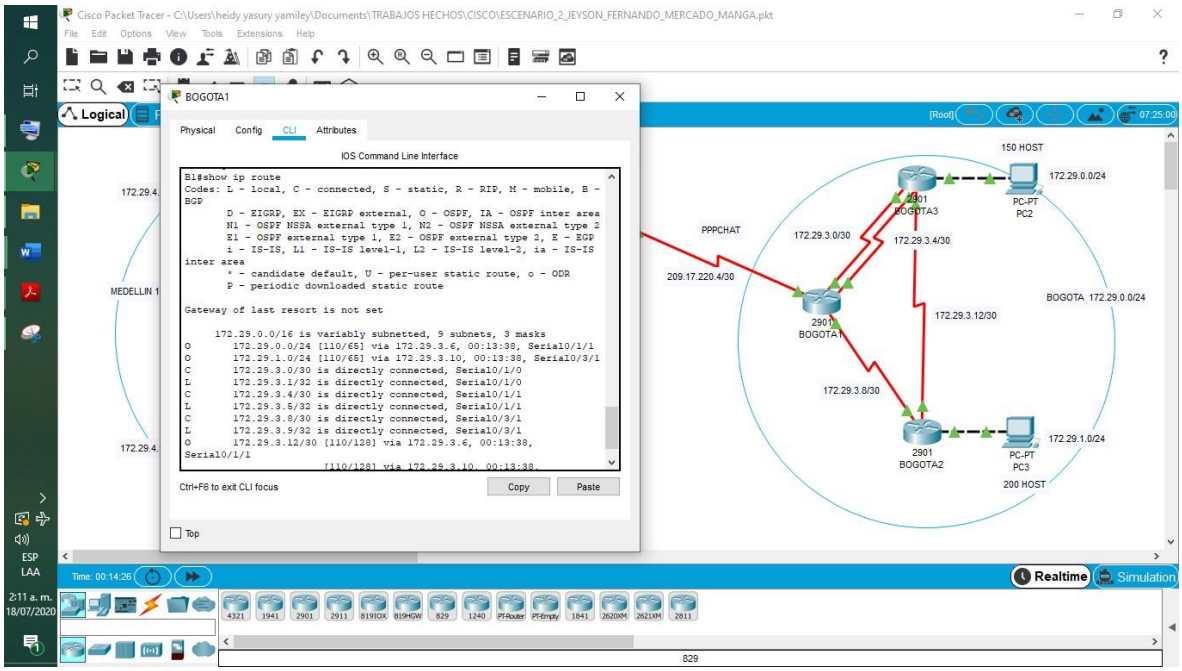

Ilustración 26 Verificación del enrutamiento en B1

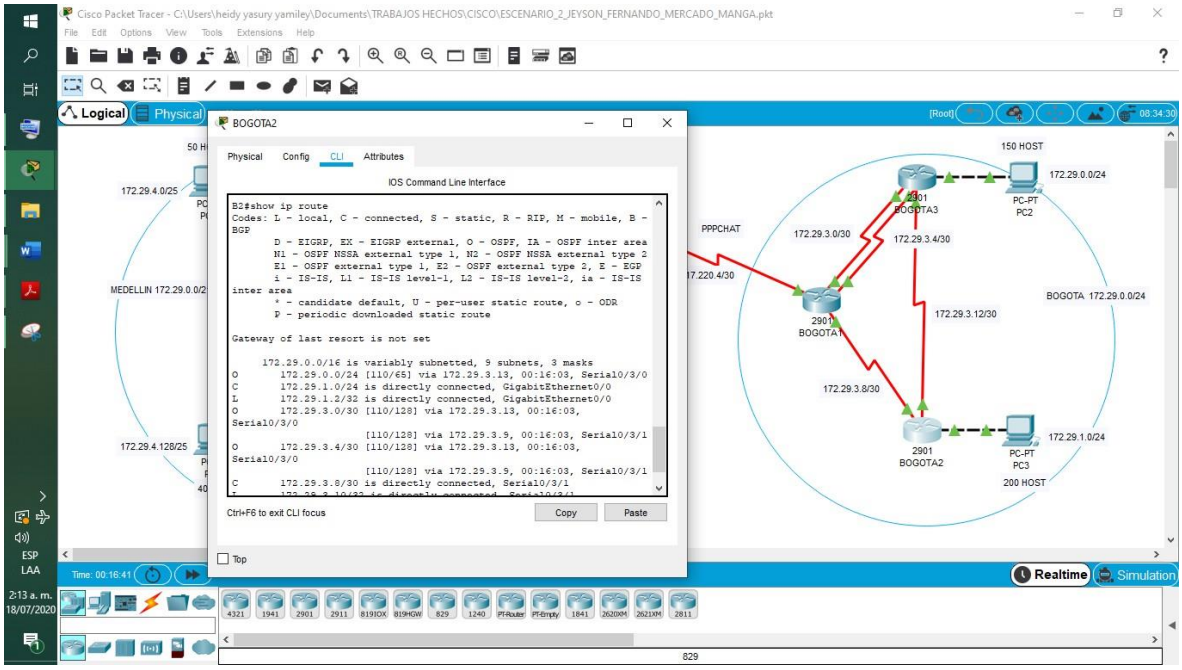

Ilustración 27 Verificación del enrutamiento en B2

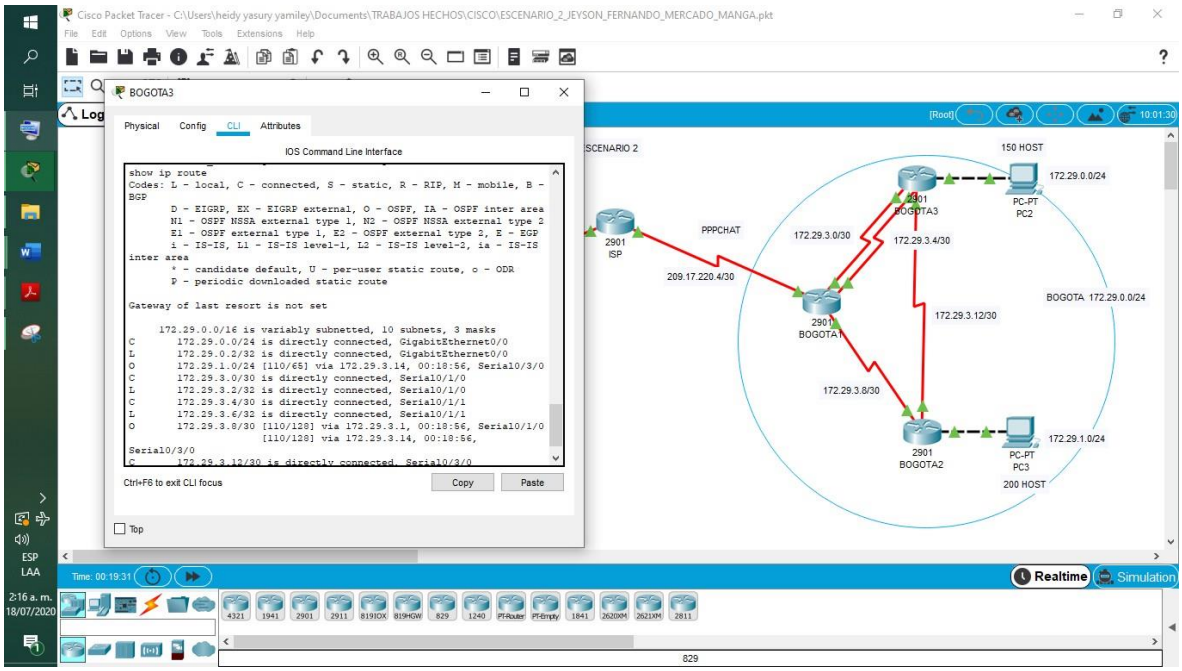

Ilustración 28 Verificación del enrutamiento en B3

Paso 2: Verificar el balanceo de carga que presentan los routers.

El balanceo de cargas se puede verificar observando en las conexiones dobles en donde se balancea el envio de informacion y en las rutas de los router con mas de una conexión. Como por ejemplo el router medellin2 (M2) en la ruta 172.29.6.0/30 encontramos mas de una rutas de envio de informacion por medio del comando show ip route realizaremos la verificacion.

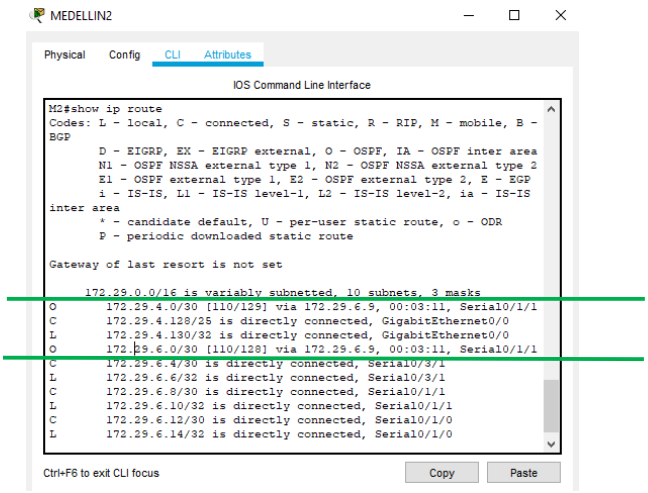

Ilustración 29 Verificación de balanceo de cargas en M2

Paso 3: Verificar que en los routers Bogotá1 y Medellín1 hay cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Si, podemos observar que Bogotá1 (B1) y Medellín1 (M1) son redes iguales, en numero de conexiones, ya que estas se conectan a igual numero de routers y al mismo tiempo se conectan con el router ISP.

Paso 4: Verificar que en los routers Medellín2 y Bogotá2 también se presentan redes conectadas directamente y recibidas mediante OSPF.

Por medio del comando show ip route podemos verificar que efectivamente en los router Medellin 2 (M2) y Bogota 2 (B2) también se presentan redes conectadas directamente.

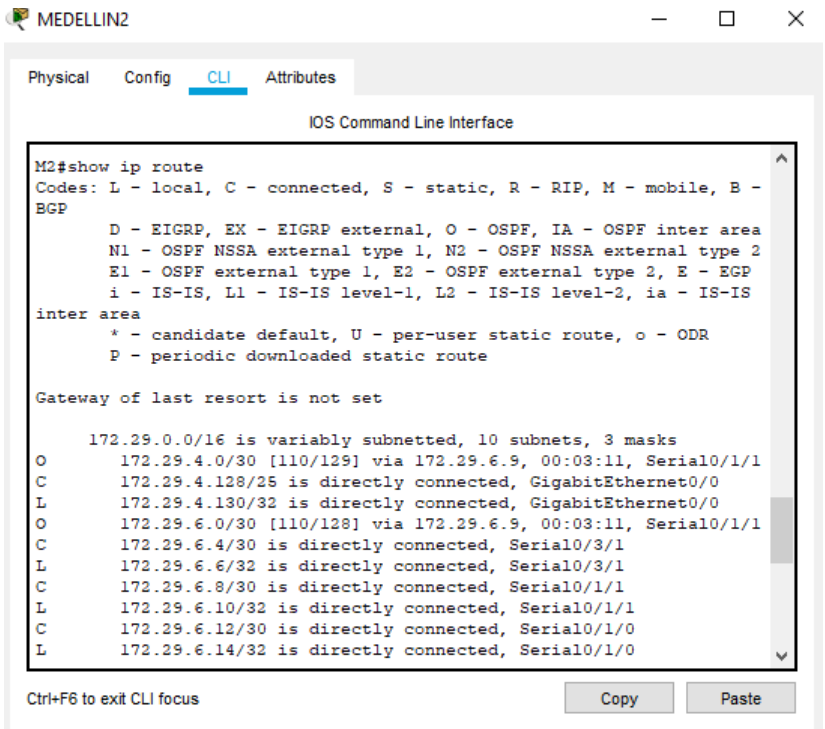

Ilustración 30 Verificación de las redes conectadas y recibidas por OSPF en M2

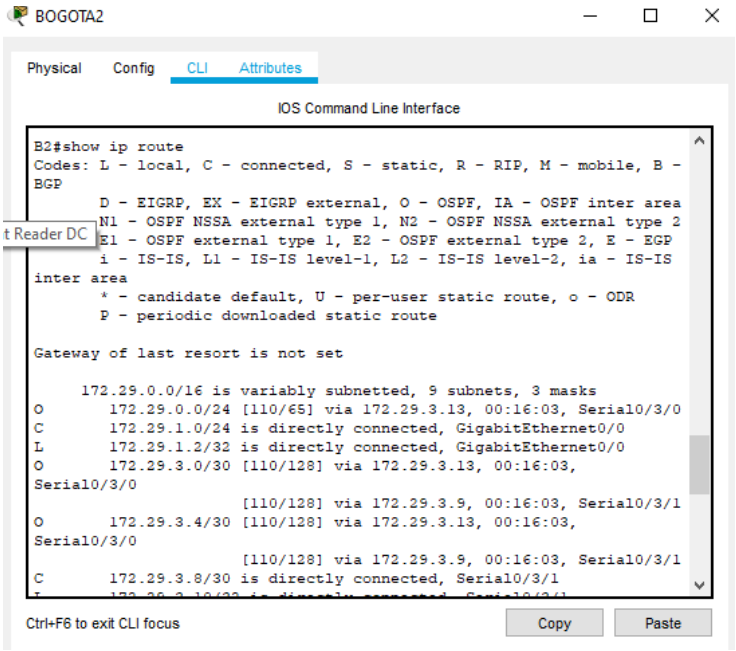

Ilustración 31 Verificación de las redes conectadas y recibidas por OSPF en B2

Paso 5: Verificar que las tablas de los router restantes permiten visualizar rutas redundantes para el caso de la ruta por defecto.

En el router Medellin 3 (M3) y Bogota (B3) se puede verificar las rutas redundantes por medio del codigo show ip route.

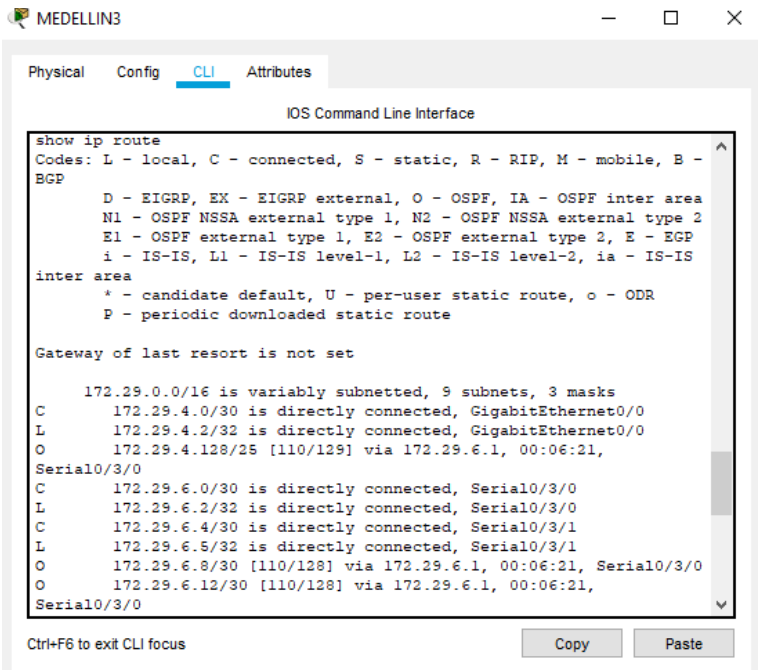

Ilustración 32 Verificación de las rutas redundantes en M3

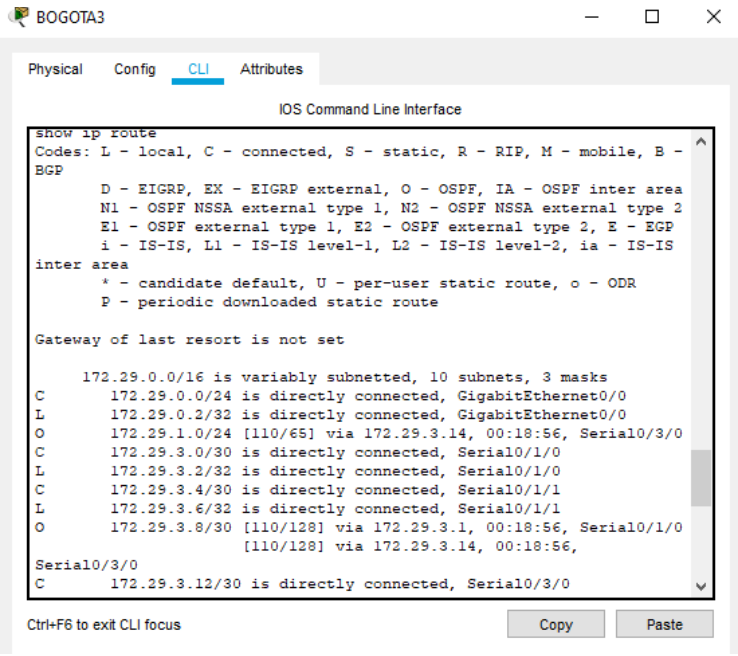

Ilustración 33 Verificación de las rutas redundantes en B3

Paso 6: Verificar que el router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Efectivamente el router ISP se configuro desde el inicio por medio de las interfaces pasivas para que solo indicara las rutas directamente conectadas en la zona de medellin y en la zona de bogota.

Parte 5: Deshabilitar la propagación del protocolo OSPF.

Paso 1: Deshabilitar la propagación del protocolo OSPF

Para no propagar las publicaciones por interfaces que no lo requieran en la siguiente tabla se indican las interfaces de cada Router que no necesitan desactivación.

Este procedimiento se desactivo previamente en la tercera parte, cuando se realizaron las configuraciones y asignaciones de los puertos seriales.

ROUTER	INTERFAZ
Bogota1	SERIAL0/3/0; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/3/0; SERIAL0/3/1

Bogota3	SERIAL0/1/0; SERIAL0/1/1; SERIAL0/3/0
Medellín1	SERIAL0/3/0; SERIAL0/1/1; SERIAL0/1/1
Medellín2	SERIAL0/3/0; SERIAL0/3/1
Medellín3	SERIAL0/1/0; SERIAL0/1/1; SERIAL0/3/0
ISP	No lo requiere

Tabla 23 Des habilitación de los puertos seriales.

Parte 6: Verificar el protocolo OSPF.

Paso 1: Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

El comando passive-interface evita que se envíen actualizaciones de routing a través de la interfaz del router especifico. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico.

Se utilizo el comando passiveinterface, para configurar una única interfaz como pasiva. También se configuro OSPF para que todas las interfaces del Router sean pasivas de manera predeterminada y, luego, habilito los anuncios de routing OSPF en las interfaces seleccionadas.

Paso 2: Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Esta verificacion se realizara en casi todos los routers excepto en el router ISP, por medio del commando do show ip route connected. Podemos apreciar las rutas que están conectadas con su dirección IP y el puerto de conexión.

- MEDELLIN 1 (M1)

M1#configure terminal

M1(config)# Router ospf 1

M1(config)# Do show ip route connected

```
M1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
M1(config)#do show ip route connected
 C    172.29.6.0/30  is directly connected, Serial0/3/0
 C    172.29.6.8/30  is directly connected, Serial0/1/1
 C    172.29.6.12/30  is directly connected, Serial0/1/0
 C    209.17.200.0/30  is directly connected, Serial0/3/1
```

Ilustración 34 Verificación de OSPF en M1

- MEDELLIN 2 (M2)

M2#configure terminal

M2(config)# Router ospf 1

M2(config)# Do show ip route connected

```
M2(config-router)#do show ip route connected
 C    172.29.4.128/25  is directly connected, GigabitEthernet0/0
 C    172.29.6.4/30  is directly connected, Serial0/3/1
 C    172.29.6.8/30  is directly connected, Serial0/1/1
 C    172.29.6.12/30  is directly connected, Serial0/1/0
```

Ilustración 35 Verificación de OSPF en M2

- MEDELLIN 3 (M3)

M3#configure terminal

M3(config)# Router ospf 1

M3(config)# Do show ip route connected

```
M3(config)#router ospf 1
M3(config-router)#do show ip route connected
 C    172.29.4.0/30  is directly connected, GigabitEthernet0/0
 C    172.29.6.0/30  is directly connected, Serial0/3/0
 C    172.29.6.4/30  is directly connected, Serial0/3/1
```

Ilustración 36 Verificación de OSPF en M3

- BOGOTA 1 (B1)

B1#configure terminal

B1(config)# Router ospf 1

B1(config)# Do show ip route connected

```
B1(config-router)#do show ip route connected
 C    172.29.3.0/30  is directly connected, Serial0/1/0
 C    172.29.3.4/30  is directly connected, Serial0/1/1
 C    172.29.3.8/30  is directly connected, Serial0/3/1
 C    209.17.220.4/30  is directly connected, Serial0/3/0
```

Ilustración 37 Verificación de OSPF en B1

- BOGOTA 2 (B2)

B2#configure terminal

B2(config)# Router ospf 1

B2(config)# Do show ip route connected

```
B2(config-router)#do show ip route connected
 C    172.29.1.0/24  is directly connected, GigabitEthernet0/0
 C    172.29.3.8/30  is directly connected, Serial0/3/1
 C    172.29.3.12/30  is directly connected, Serial0/3/0
```

Ilustración 38 Verificación de OSPF en B2

- BOGOTA 3 (B3)

B3#configure terminal

B3(config)# Router ospf 1

B3(config)# Do show ip route connected

```
B3(config-router)#do show ip route connected
 C    172.29.0.0/24  is directly connected, GigabitEthernet0/0
 C    172.29.3.0/30  is directly connected, Serial0/1/0
 C    172.29.3.4/30  is directly connected, Serial0/1/1
 C    172.29.3.12/30  is directly connected, Serial0/3/0
```

Ilustración 39 Verificación de OSPF en B3

Parte 7: Configurar encapsulamiento y autenticación PPP.

Paso 1: Según la topología se requiere que el enlace Medellín1 (M1) con ISP sea configurado con autenticación PAT.

Para realizar este paso, se realizarán configuraciones tanto en el router ISP como en (M1). A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router ISP Y M1.

- ISP

ISP(config)#Configure terminal

ISP(config)#Int s0/3/0

ISP(config)#Encapsulation pp

ISP(config)#Ppp pap sent-username ISP password cisco

IPS(config)#exit

- MEDELLIN1 (M1)

M1(config)#Configure terminal

M1(config)#Int s0/3/1

M1(config)#Encapsulation ppp

M1(config)#Ppp authentication pap

M1(config)#Ppp pap sent-username ISP password cisco

M1(config)#exit

Paso 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Para realizar este paso, se realizarán configuraciones tanto en el router ISP como en (B1). A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router ISP Y B1.

- BOGOTA 1 (B1)

B1 (config)#configure terminal

B1 (config)#username ISP password cisco

B1 (config)#Interface s0/3/0

B1 (config)#encapsulation ppp

B1 (config)#ppp authentication chap

B1 (config)#exit

- ISP

ISP(config)#Configure terminal

ISP(config)#Interface s0/3/0

ISP(config)#encapsulation ppp

ISP(config)#ppp authentication chap

ISP(config)#exit

Parte 8: Configuración de PAT.

Paso 1: 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.

Este paso se realizará en el router M1 y B1, por medio del comando ip nat inside o ip nat outside ingresamos a la configuración PAT. A continuación, se muestran los comandos tal como se escribirían en la ventana CLI de los router M1 y B1.

- MEDELLIN1 (M1)

M1(config)# Ip nat inside source list 1 interface s0/3/1 overload

M1(config)# Access-list 1 permit 172.29.4.0 0.0.3.255

M1(config)# Int s0/3/0

M1(config)# Ip nat outside

M1(config)# Int s0/3/1

M1(config)# Ip nat outside

M1(config)# Int s0/1/0

M1(config)# Ip nat outside

M1(config)# Int s0/1/1

M1(config)# Ip nat outside

- **BOGOTA1 (B1)**

B1(config)# Ip nat inside source list 1 interface s0/3/0 overload

B1(config)# Access-list 1 permit 172.29.0.0 0.0.3.255

B1(config)#Interface s0/3/0

B1(config)# Ip nat outside

B1(config)# Int s0/3/1

B1(config)# Ip nat outside

B1(config)# Int s0/1/0

B1(config)# Ip nat outside

B1(config)# Int s0/1/1

B1(config)# Ip nat outside

Paso 2: Verificar lo indicado en el paso anterior, luego 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 0/3/0 del router Medellín1, cómo diferente puerto

Comprobamos por medio del comando ping desde el PC2 a ISP cuya dirección IP por esa red es: 209.17.220.5 Ahora comprobamos también por el lado de MEDELLIN 1 con ping a ISP

Paso 3: 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 0/3/0 del router Bogotá1, cómo diferente puerto.

Parte 9: Configuración del servicio DHCP.

Paso 1: Configurar la red Medellín2 y Medellín3 donde el Router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.

A continuación, se muestran los comandos para realizar la configuración DHCP en M2 y M3, teniendo en cuenta que M2 sera configurado como servidor tal como se muestra en los siguientes comandos que se escribirían en la ventana CLI de los router según les corresponde.

- MEDELLIN 2 (M2)

M2(config)# Ip dhcp excluded-address 172.29.4.1 172.29.4.5

M2 (config)# Ip dhcp excluded-address 172.29.4.129 172.29.4.133

M2 (config)# Ip dhcp pool M2

M2 (config)# Network 172.29.4.0 255.255.255.128

M2 (config)# Default-router 172.29.4.1

M2 (config)# Dns-server 5.5.5.5

M2 (config)# exit

M2 (config)# Ip dhcp pool M3

M2 (config)# Network 172.29.4.128 255.255.255.128

M2 (config)# Default-router 172.29.4.129

M2 (config)# Dns-server 5.5.5.5

M2 (config)# Dns-server 5.5.5.5

Paso 2: El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

M3(config)# int g0/0
M3(config)# ip helper-address 172.29.6.5
M3 (config)# exit

Paso 3: Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

Comprobamos configuración DHCP en PC0

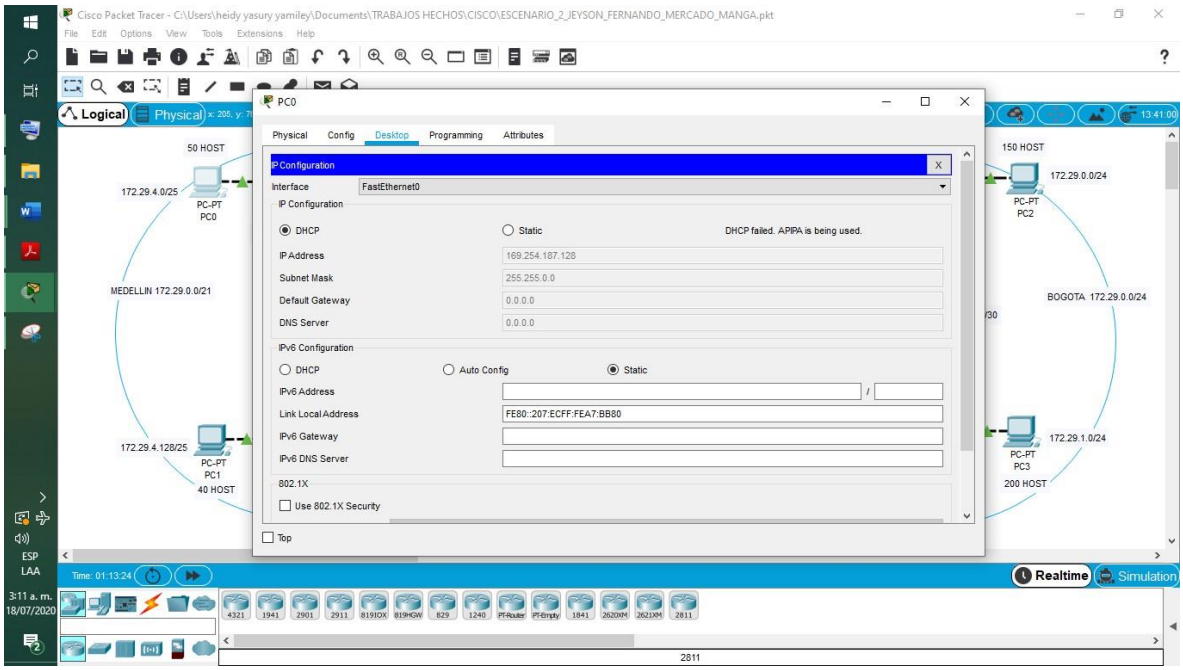

Ilustración 40 Verificación de configuración DHCP en PC0

Comprobamos configuración DHCP en PC1

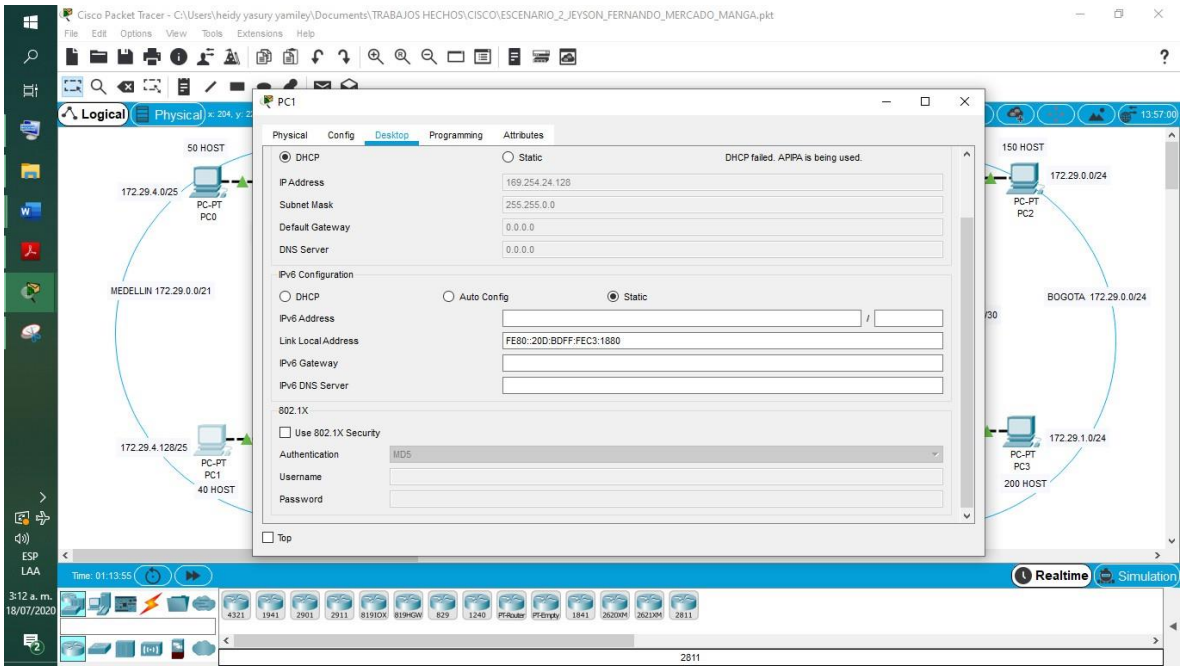

Ilustración 41 Verificación de configuración DHCP en PC1

Comprobamos configuración DHCP en PC3

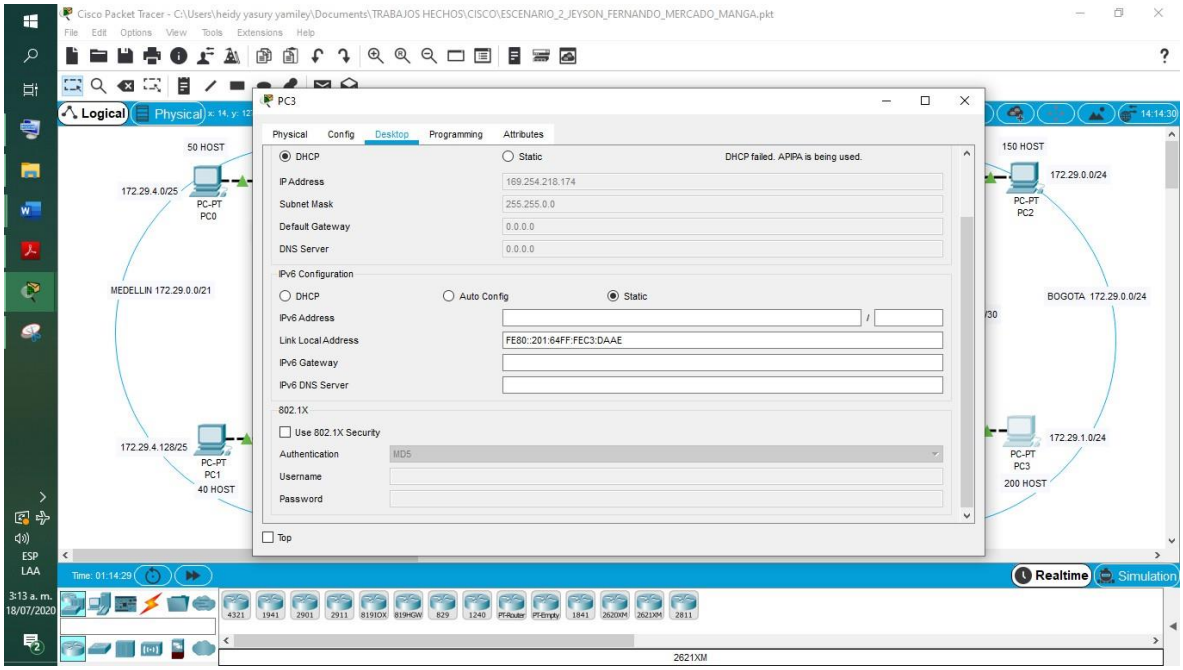

Ilustración 42 Verificación de configuración DHCP en PC3

Comprobamos configuración DHCP en PC2

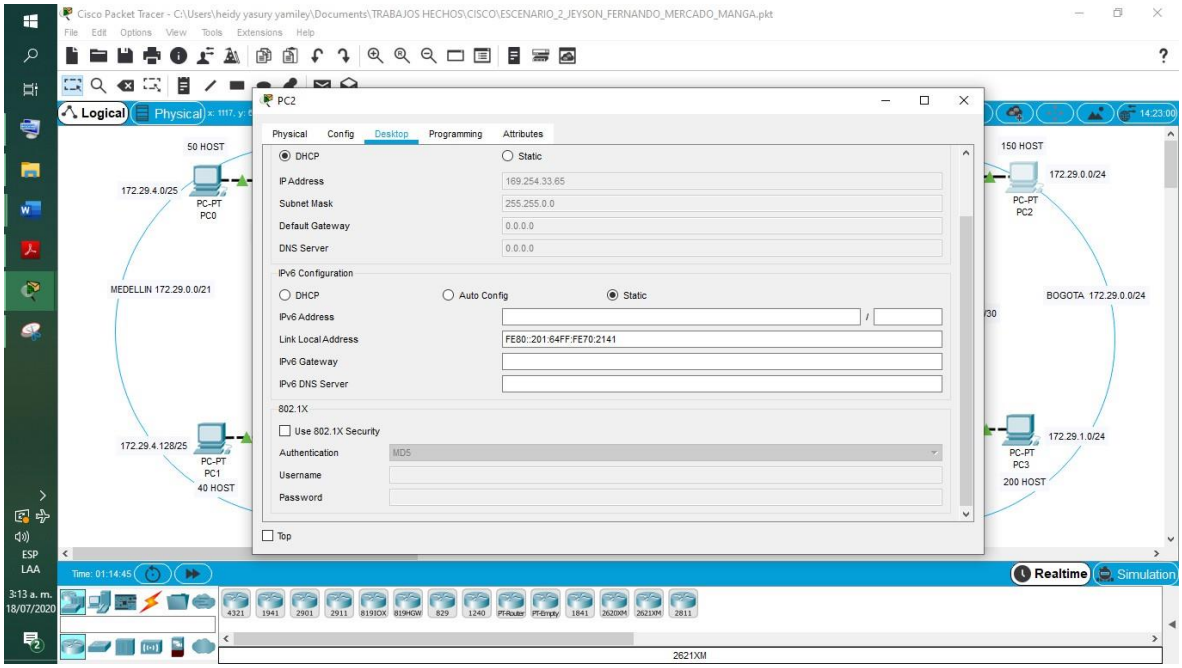

Ilustración 43 Verificación de configuración DHCP en PC2

Paso 4: Configure el Router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del Router Bogotá2.

- **BOGOTA 2 (B2)**

BOGOTA2(config)# Ip dhcp excluded-address 172.29.1..1 172.29.1.5

BOGOTA2(config)# Ip dhcp excluded-address 172.29.0.1 172.29.0.5

BOGOTA2(config)# Ip dhcp pool BOGOTA2

BOGOTA2(config)# Network 172.29.1.0 255.255.255.0

BOGOTA2(config)# Default-router 172.29.0.1

BOGOTA2(config)# Dns-server 5.5.5.5

BOGOTA2(config)#exit

BOGOTA2(config)#Ip dhcp pool BOGOTA3

BOGOTA2(config)#Network 172.29.4.128 255.255.255.128

BOGOTA2(config)#Default-router 172.29.0.1

BOGOTA2(config)#Dns-server 5.5.5.5

BOGOTA2(config)#exit

- **BOGOTA 3 (B3)**

BOGOTA3(config)# int g0/0

BOGOTA3(config)# ip helper-address 172.29.3.13

BOGOTA3(config)#exit

CONCLUSIONES

Después de las configuraciones realizadas en cada una de las redes a los dispositivos, se practicaron los comandos básicos de configuración y de verificación que como su nombre lo indica son primordiales para que los dispositivos funcionen correctamente, además los conocimientos acerca de los protocolos son una gran ayuda para el futuro de un administrador de redes, en esta actividad se establecieron las bases para desempeñarnos profesionalmente en las redes y comunicaciones.

A partir de configurar el protocolo RIP (Routing Information Protocol) en el primer escenario se percibió la importancia y facilidad de su implementación. El protocolo establece el intercambio de información entre los routers de una red de una manera mucho más sencilla, este no puede ser aplicado a grandes redes solo a redes pequeñas.

A diferencia del protocolo RIP el protocolo OSPF se aplica a grandes redes, pero más difícil su configuración.

El protocolo DHCP proporciona una administración fácil de las direcciones IP en los dispositivos, como pudimos observar en las configuraciones fue fácil realizar este procedimiento mientras que manualmente nos hubiéramos podido confundir y cometer errores.

La traducción de direcciones de red dinámicas y estáticas NAT envían la información mediante la dirección IP proporcionada por el PC y tiene la ventaja de ofrecer flexibilidad de las conexiones para seguridad cuando no se puede acceder desde el lugar de trabajo como tal, mientras que con PAT la información se enruta por una red privada, se asignan varias direcciones IP privadas a una única dirección IP publica o unas pocas disminuyendo la flexibilidad de conexiones.

Por otro lado, las verificaciones se realizaron por medio de los comandos show ip route, show ipv6 route, show ip route rip y show vlan brief. Comandos que facilitan la revisión de las configuraciones que se están realizando y por lo tanto corregir más rápido los errores.

Al realizar la verificación de conectividad en la red, primeramente, se obtuvieron algunos errores debidos a que a la hora de escribir los comandos en la ventana CLI, podemos cometer errores pequeños que afectan los buenos resultados que se esperan obtener a partir de las configuraciones realizadas y que omitimos por su pequeñez, pero que pueden provocar que la red no funcione correctamente, por ello es importante realizar verificaciones constantes.

BIBLIOGRAFIA

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course- assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course- assets.s3.amazonaws.com/RSE6/es/index.html#10

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static- course-assets.s3.amazonaws.com/RSE6/es/index.html#8

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

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course- assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static- course-assets.s3.amazonaws.com/ITN6/es/index.html#1

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

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

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static- course-assets.s3.amazonaws.com/RSE6/es/index.html#6

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

REFERENCIAS

[1] CCNA. *DHCP*. Recuperado de https://www.CCNA.coma

[2] ECURED. NTP. Recuperado de https://www.ecured.cu/NTP

[3] Enrutamiento dinámico OSPF con Packet Tracer. OSPF. Recuperado de https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer

[4] HERRAMIENTAS WEB. RIP, Recuperado de https://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html

[5]RED PROYDESA. EIGRP. Recuperado de https://www.proydesa.org/portal/index.php/noticias/1764-que-es-y-como-funciona-el-protocolo-eigrp-2

[6] REDES TELEMATICAS. SWITCH. Recuperado de http://redestelematicas.com/el-switchcomofuncionaysusprincipalescaracteristicas/#:~:text=Un%20switch%20o%20conmutador%20es,(o%20t%C3%A9cnicamente%20IEEE%20802.3).&text=Los%20switches%20realizan%20esta%20funci%C3%B3n%20para%20medios%20cableados.

[7] WIKIPEDIA (s.f) PPP (Point-to-Point Protocol). Recuperado de https://es.wikipedia.org/wiki/PointtoPoint_Protocol#:~:text=Protocolo%20punto%20a%20punto%20(PPP)%20(en%20ingl%C3%A9s%20Point%2D,dos%20nodos%20de%20una%20red.

[8] WIKIPEDIA (s.f). ENRUTAMIENTO. Recuperado de https://es.wikipedia.org/wiki/Encaminamiento

[9] WIKIPEDIA (s.f). PROTOCOLOS DE RED. Recuperado de https://es.wikipedia.org/wiki/Anexo:Protocolos_de_red#:~:text=Un%20protocolo%20de%20red%20designa,de%20una%20red%20de%20computadoras.

[10] WIKIPEDIA (s.f). RED. Recuperado de https://es.wikipedia.org/wiki/Red_de_computadoras

[11] WIKIPEDIA (s.f). ROUTER. Recuperado de https://es.wikipedia.org/wiki/Router#:~:text=Un%20r%C3%BAter%2C%E2%80%8B%20enrutador%2C%E2%80%8B,dentro%20de%20una%20red%20inform%C3%A1tica.

[12] WIKIPEDIA. (s.f.). ETHERNET. Recuperado de https://es.wikipedia.org/wiki/Ethernet

[13] WIKIPEDIA. (s.f.). *VLAN*. Recuperado de http://redestelematicas.com/

[2] WIKIPEDIA. (s.f.) ACL. Recuperado de https://es.wikipedia.org/wiki/Lista_de_control_de_acceso#:~:text=Las%20ACL%20permiten%20controlar%20el,de%20acuerdo%20a%20alguna%20condici%C3%B3n.&text=Tanto

[14] XAKATA. PAT. Recuperado de https://www.xatakamovil.com/conectividad/nat-network- address-translation-que-es-y-como-funciona

[15] XATAKA. NAT DINAMICA. Recuperado de https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-

como- funciona

[16] XATAKA. NAT ESTATICA. Recuperado de https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como- funciona

Escenarios 1 y 2
Link:
https://drive.google.com/drive/folders/120hYBKrOkstFQ8t7scojihkgWrAJubyx?usp=sharing