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

CRISTIAM JAVIER OSORIO VANEGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA

INGENIERIA DE SISTEMAS

BOGOTA – CUNDINAMARCA

2020

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

CRISTIAM JAVIER OSORIO VANEGAS

Proyecto de grado presentado para optar el titulo

INGENIERO DE SISTEMAS

DOCENTE

ING. GUSTAVO ADOLFO RODRÍGUEZ

MSC EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA

INGENIERIA DE SISTEMA

BOGOTA – CUNDINAMARCA

2020

RESUMEN

Las redes y las comunicaciones son unos de los elementos esenciales en el desarrollo de la sociedad en la actualidad, por ello en la presente investigación se tratarán los principios básicos del routing y el switching siendo aplicados bajo un espacio de simulación el programa Packet Tracer con el fin de comprender las problemáticas que puedan presentarse y con ello brindar soluciones efectivas basados en el conocimiento y experiencia profesional. Esta actividad evaluativa en el diplomado de profundización de CCNA, ofrece los elementos para diseño y configuración de una red. Asimismo, permite la comprensión de los dispositivos y su comportamiento en relación a la configuración a través de comandos. De igual manera, se trabajan los servicios de los diferentes dispositivos con el fin de conocer las opciones de conectividad que puede haber tanto a nivel residencial como corporativo.

Palabras Claves: Packet Tracer, enrutamiento, dhcp, ospf, simulación, red.

ABSTRACT

Networks and communications are one of the essential elements in the development of society at present, so in this research the basic principles of routing and switching will be discussed, applying the Packet Tracer program with a simulation space with the In order to understand the problems that may arise and thereby provide effective solutions based on professional knowledge and experience. This evaluative activity in the CCNA deepening diploma offers the elements for designing and configuring a network. It also allows the understanding of the devices and their behavior in relation to the configuration through commands. In the same way, the services of the different devices are worked in order to know the connectivity options that may exist both at the residential and corporate level.

Key Words: Packet Tracer, routing, dhcp, ospf, simulation, network.

NOTA DE ACEPTACIÓN

Firma de Presidente del Jurado

Firma delJurado

Firma delJurado

Bogotá, 25 de julio de 2020

DEDICATORIA

Este proyecto de grado lo dedico a Dios, por la gran ayuda y motivación para sacar este proyecto adelante. También a mi familia que han estado en todo el proceso de formación apoyándome en todo momento motivándome en le proceso de formación demostrándome que si se puede si uno se lo propone con dedicación diciplina y actitud

AGRADECIMIENTOS

Agradezco a Dios Por concederme este estudió y la gran motivación para salir adelante

Agradezco a mis padres por motivarme a estudiar esta carrera

A mis hermanos por darme le ejemplo de salir adelante con esfuerzo

Gracias al tutor y mis compañeros por acompañarme en todo el proceso del curso

INTRODUCCIÓN

El mundo actual se desenvuelve ante un escenario donde las redes y las comunicaciones se apoderan de todas las actividades diarias, se puede decir que el hombre vive en un mundo cibernético en el cual la conexión e interacción constante forman parte del desarrollo social. Es por ello, que en la cotidianeidad surgen problemas y necesidades sociales derivadas de la comunicación entre redes ya sea desde un plano residencial común o a gran escala corporativa.

En consecuencia, el presente trabajo plantea un escenario donde se busca comprender las diferentes problemáticas surgidas en la actualidad y plantear soluciones derivadas del conocimiento académico y profesional. Asimismo, empleando, los recursos, programas, herramientas y códigos que faciliten un mayor desenvolvimiento profesional para el cumplimiento de los objetivos propuestos.

De igual manera, será un espacio de conocimiento donde a través de la experiencia simulada se busca generar matrices de aprendizajes que sirvan a los ingenieros y personas en general a comprender las redes como elementos importantes de nuestras vidas en relación a las comunicaciones y su trascendencia. Así como también, a plantear soluciones de acuerdo a su capacidad de acción.

TABLA DE CONTENIDO

Índice de tablas

Índice de Figuras

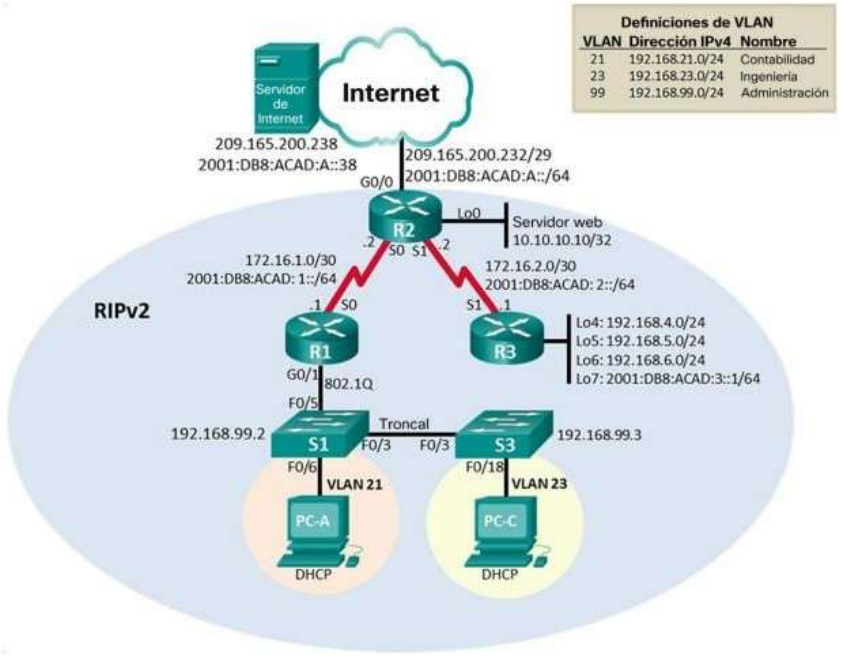
OBJETIVOS

1. Conocer y manejar el programa Packet Tracer como herramienta de simulación de casos reales para la aplicación de los conocimientos en el campo profesional.
2. Identificar el escenario de trabajo, herramientas, dispositivos y demás medios con los cuales se puedan crear redes de comunicaciones tanto a nivel residencial como corporativo.
3. Identificar y solucionar problemas derivados de subredes y direccionamiento IP, mediante el uso de herramientas y estrategias basadas en comandos y características del IOS.
4. Configurar los procesos básicos, enrutamientos y protocolos que permitan una efectiva comunicación entre las redes del caso de estudio.

Escenario 1

Topología de RED

FIGURA 1 – TOPOLOGÍA DE RED – ESCENARIO 1



Fuente: Diseño propio/Packet tracer

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.

Parte 1 Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

En esta primera etapa del escenario 1, se procede a leliminar configuraciones predeterminadas en los router, con el fin de que pueda haber conexión con mayor efectividad, y para que no existan barreras en relación a los demás procesos a realizar en las demás fases.

Por consiguiente, se inicia eliminando los starup de los routers, a través del comando #erase startup-config, posteriormente se reinician todos los routers, a través del comando #reload, con el fin de guardar la configuración y ejercer un mejor proceso a futuro. De igual manera, se procede a realizar dicho paso con los Switches, además de verificar que la red de datos VLAN no esté en la memoria flash de cada uno, todo ello con el fin de ejercer una creación de subredes Vlans con éxitos y sin inconvenientes.

TABLA 1 – PRIMER PASO ESCENARIO 1

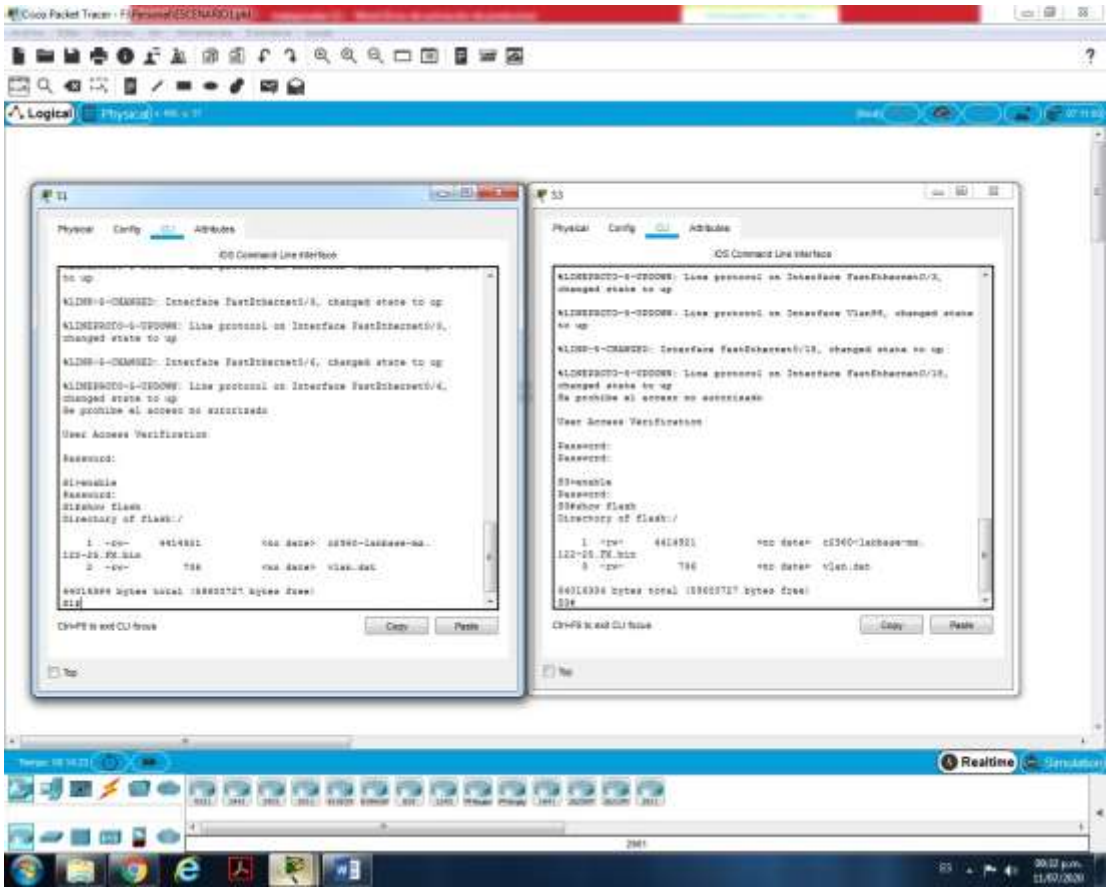
Tarea	Comando IOS
Eliminar el archivo starup-config de todos los router	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config

Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Fuente: Diseño Propio/ Packet Tracer

Verificación de Show Flash

FIGURA 2 – VERIFICACIÓN DEL COMANDO SHOW FLASH



Fuente: Diseño Propio/ Packet Tracer

Parte 2: Configurar Los Parámetros Básicos De Los Dispositivos

Paso 1: Configurar la computadora de Internet

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

Para este proceso, se considera el servidor como un dispositivo el cual proveerá de internet a la red, así como a las subredes, sin embargo, para lograr los resultados con mayor efectividad, se debe proceder a realizar lo siguiente:

1. Determinar la dirección IP del servidor aunado al máscara sub red del mismo
2. Determinar el Gateway del servidor como fuente principal
3. Determinar las direcciones IPV6 como enlaces de subredes

Para conseguir lo siguiente:

TABLA 2 – CONFIGURACIÓN DE IP DEL SERVIDOR

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.0
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Dirección IPv6/subred	2001:DB8:ACAD:A::1

Fuente: Diseño propio/ Packet Tracer

Paso 2: Configurar R1

En todo escenario planteado tanto en un espacio de simulación como en la vida real, es imprescindible la configuración básica para cada dispositivo, en este caso particular, la configuración se basará en primer lugar en la eliminación de la configuración de búsqueda DNS en cada uno de los routers, y por consiguiente, establecer nombre y protocolo de acceso a cada uno de ellos a través de los diferentes comandos del programa.

Es de resaltar, que para la configuración se comienza con el nombre de cada uno de los dispositivos, para proseguir con las claves de acceso, considerando la de habilitación o enable, la de la consola de línea o line console 0, así como la de la Telnet Cabe destacar, que dichas contraseñas deben ser encriptados como medio de seguridad en cada uno de los dispositivos. Por otra parte, también se configura el banner de acceso, con el fin de indicar al usuario, que el acceso es restringido y solo para personal autorizado.

Para obtener el siguiente proceso para cada uno de los router asignados al presente escenario de la práctica.

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 3 – CONFIGURACIÓN BÁSICA ROUTER 1

Elemento o Tarea de Configuración	Especificación
Desactivar la búsqueda DNS	Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#host R1 R1(config)#
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1(config)#line console 0

Contraseña de acceso a la consola	R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado# R1(config)#exit
Interfaz S0/0/0	R1(config)#interface s0/0/0 R1(config-if)#description conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
Rutas predeterminadas Ipv6	R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#exit

Fuente: Diseño propio/ Packet Tracer

Paso 3: Configurar R2 La configuración del R2 incluye las siguientes tareas:

TABLA 4 – CONFIGURACIÓN BÁSICA DEL ROUTER R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup Router(config)#exit
Nombre del router	Router(config)#host R2

Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado# R2(config)#exit
Interfaz S0/0/0	R2(config)#interface s0/0/0 R2(config-if)#description conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)# R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface s0/0/1 R2(config-if)#description conexion a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 This command applies only to DCE interfaces R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#interface g0/0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64

	R2(config-if)#no shutdown R2(config-if)# exit
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#description Servidor web simulado R2(config-if)#ip address 10.10.10.10 255.255.255.25
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#exit

Fuente: Diseño Propio/ Packer Tracer

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

TABLA 5 – CONFIGURACIÓN ROUTER 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup Router(config)#exit
Nombre del router	Router(config)#host R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
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 s0/0/1

	R3(config-if)#description conexion a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ip address 192.168.7.1 255.255.255.0 R3(config-if)#
Ruta predeterminada	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Fuente: Diseño Propio/ Packet Tracer

Paso 5: Configurar S1

Al igual que los router, es necesario configurar de manera básica cada Switch con el fin de establecer sus nombres y protocolos de seguridad. Para la configuración se comienza con el nombre de cada uno de los dispositivos, para proseguir con las claves de acceso, considerando la de habilitación o enable, la de la consola de línea o line console 0, así como la de la Telnet Cabe destacar, que dichas contraseñas deben ser encriptados como medio de seguridad en cada uno de los dispositivos. Por otra parte, también se configura el banner de acceso, con el fin de indicar al usuario, que el acceso es restringido y solo para personal autorizado.

La configuración del S1 incluye las siguientes tareas:

TABLA 6 – CONFIGURACIÓN BÁSICA DE SWITCHER 1

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

Fuente: Diseño propio/ Packet Tracer

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

TABLA 7 – CONFIGURACIÓN DEL SWITCHER 3

Elemento o Tarea de Configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup Switch(config)#exit
Nombre del switch	Switch(config)#host S3

Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S2(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado#

Fuente: Diseño Propio/ Packet Tracer

Paso 7: Verificar la conectividad de la red.

Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

TABLA 8 – VERIFICACIÓN DE PING EN ROUTERS

Desde	A	Dirección IP	Resultados del PING
R1	R2 s0/0/0	R1: 172.16.1.1 R2:172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!!

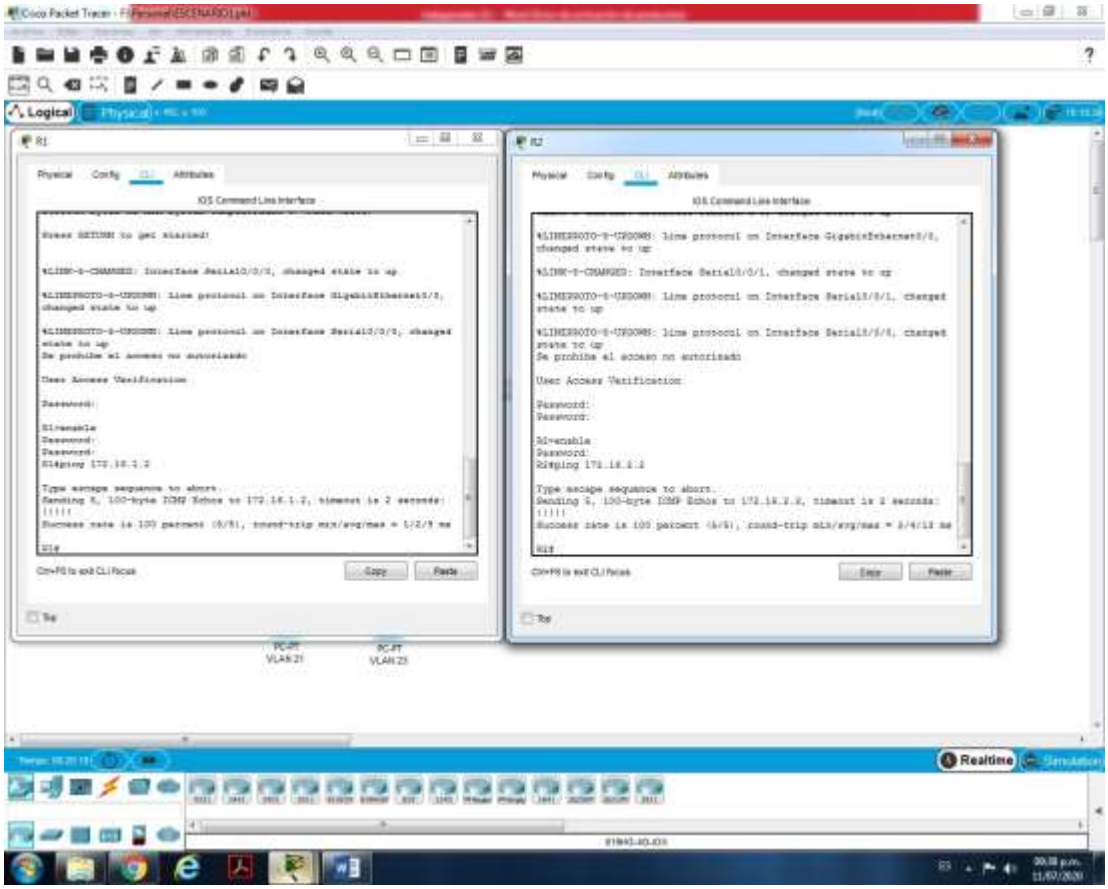
			Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/70 ms
R2	R3 s0/0/1	R2: 172.16.2.1 R3: 172.16.2.2	R2#ping 172.16.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/11 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Satisfactorio

Fuente: Diseño Propio/ Packet Tracer

Partiendo de lo anterior expuesto, a través del comando PING, se puede verificar la conexión entre cada uno de los routers, asimismo, nos determinará cuantos paquetes fueron enviados, así como el tiempo de espera para cada uno. Es de resaltar que para este caso particular, se obtuvo éxito en cada, considerando la siguiente figura.

Verificación de PING

FIGURA 3 – VERIFICACIÓN DE PING ENTRE R1, R2 Y R3 1



Fuente: Diseño propio/ Packet Tracer

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

Paso 1: Configurar S1

En la creación de subredes, en este caso específico las redes VLAN, es necesario configurarlas de manera directa en los Switch, con el fin de enlazar conexión, establecer nombres, asignar los puertos de acceso para cada una de ellas, así como el modo de acceso. Asimismo, configurar la dirección IP de cada una de las computadoras que tendrán conexión en las VLANS.

De igual manera, en la topología de la red planteada, se debe realizar un acceso TRUNK entre los dos Switch, esto con el fin de que el S3 y el S1, puedan leer las conexiones e información de cada uno sin inconvenientes, además de poder establecer y leer las redes VLANS. Para ello se establecerán tres redes VLANS, considerando la 21 como la de Contabilidad, la 23 como Ingeniería y la 99 como Administración, partiendo de:

La configuración del S1 incluye las siguientes tareas:

TABLA 9 – REGISTRO DE VLANS EN S1

Elemento o Tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)# 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 F0/3 S1(config-if)#switch mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface F0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
Apagar todos los puertos sin usar	S1(config-if-range)#shutdown

Fuente: Diseño propio/ Packet Tracer

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

TABLA 10 – REGISTRO DE VLAN S3

Elemento o Tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit
Asignar la dirección IP de administración.	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown

Asignar el gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Configurar el resto de los puertos como puertos de acceso	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown
Asignar F0/18 a la VLAN 21	S3(config-if)#switchport access vlan 23 S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown
Apagar todos los puertos sin usar	S3(config-if-range)#shutdown

Fuente: Diseño Propio/ Packet Tracer

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 11 – REGISTRO DE VLAN EN R1

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 VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#interface g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#interface g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#interface g0/1 R1(config-if)#no shutdown

Fuente: Diseño Propio/ Packet Tracer

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

TABLA 12 – VERIFICACIÓN DE PING 2

Desde	A	Dirección IP	Resultados de PING
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5)
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5)

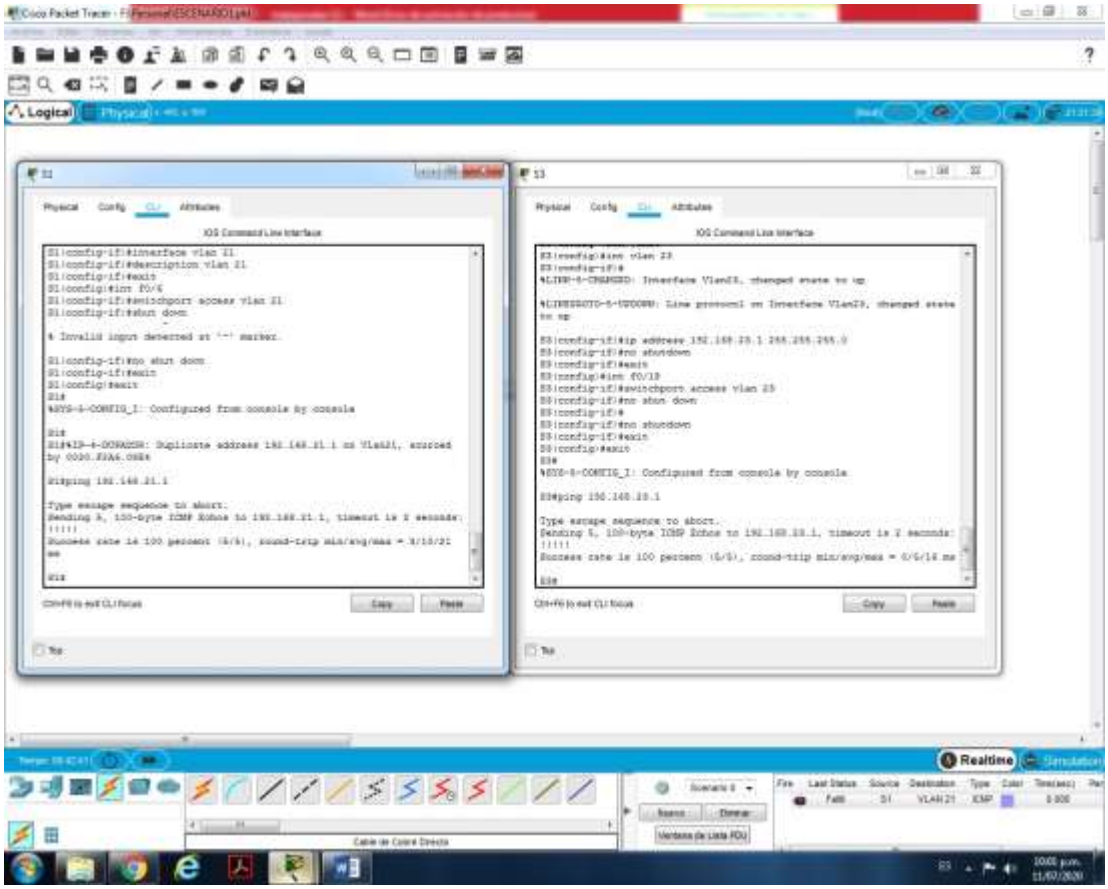
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5)
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5)

Fuente: Diseño propio/ Packet Tracer

Partiendo de lo anterior expuesto, a través del comando PING, se puede verificar la conexión entre cada uno de los routers y las redes VLANS, asimismo, nos determinará cuantos paquetes fueron enviados, así como el tiempo de espera para cada uno. Es de resaltar que para este caso particular, se obtuvo éxito en cada, considerando la siguiente figura.

Verificación de PING

FIGURA 4 – VERIFICACIÓN DE PING 2



Fuente: Diseño Propio/ Packet Tracer

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 13- RIP EN ROUTER R 1

Elemento o Tarea de Configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip
Anunciar las redes conectadas directamente	R1(config-router)#version 2 R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.1.8/30 is directly connected, Serial0/0/0 R1(config-router)#network 172.16.1.0 R1(config-router)#network 172.16.1.8
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface f0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Fuente: Diseño propio/ Packet Tracer

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

TABLA 14 –RIP EN EL ROUTER R2

Elemento o Tarea de Configuración	Especificación

Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 209.165.200.232
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática	R2(config-router)#no auto-summary

Fuente: Diseño propio/ Packet Tracer

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

TABLA 15 – RIP RIPV3 EN EL ROUTER R2

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)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0, Loopback7 R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0

	R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Fuente: Diseño propio/ Packet Tracer

Paso 4: Verificar la información de RIP

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

En fase del escenario 1, se busca observar como a través de determinados comandos, el programa indica el funcionamiento del enrutamiento RIP, en relación a las IP que se llegan a enrutar en los dispositivos y el estado actual de las conexiones partiendo del mismo. De igual manera, cabe descartar que el show ip protocols permite identificar cuales protocolos han sido configurados dentro del dispositivo para así determinar diversas acciones y decisiones en relación al funcionamiento de las redes.

TABLA 16 – VERIFICACIÓN DE COMANDOS RIP

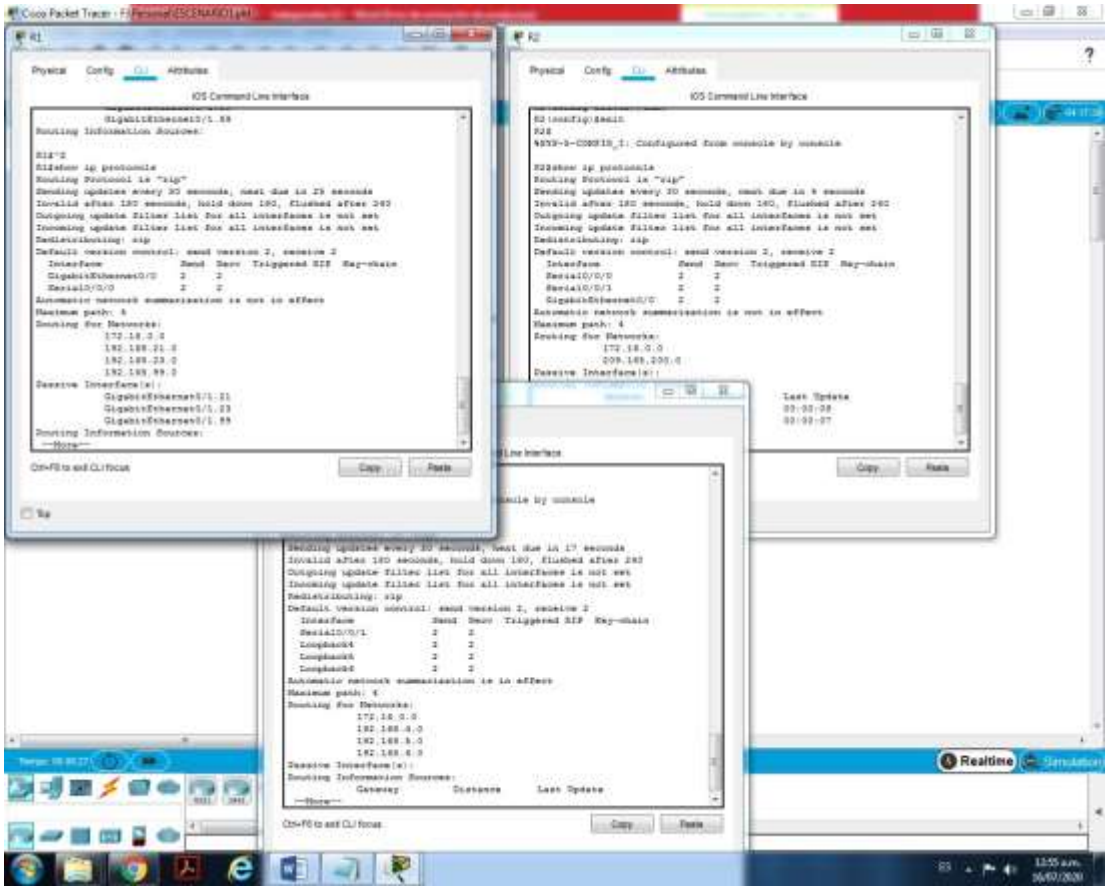
Elemento o Tarea de Configuración	Especificación
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	El show ip protocols, muestra la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas.
¿Qué comando muestra solo las rutas RIP?	show ip route rip muestra solo rutas de RIP

¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show run muestra la sección de RIP de la configuración

Fuente: Diseño propio/ Packet Tracer

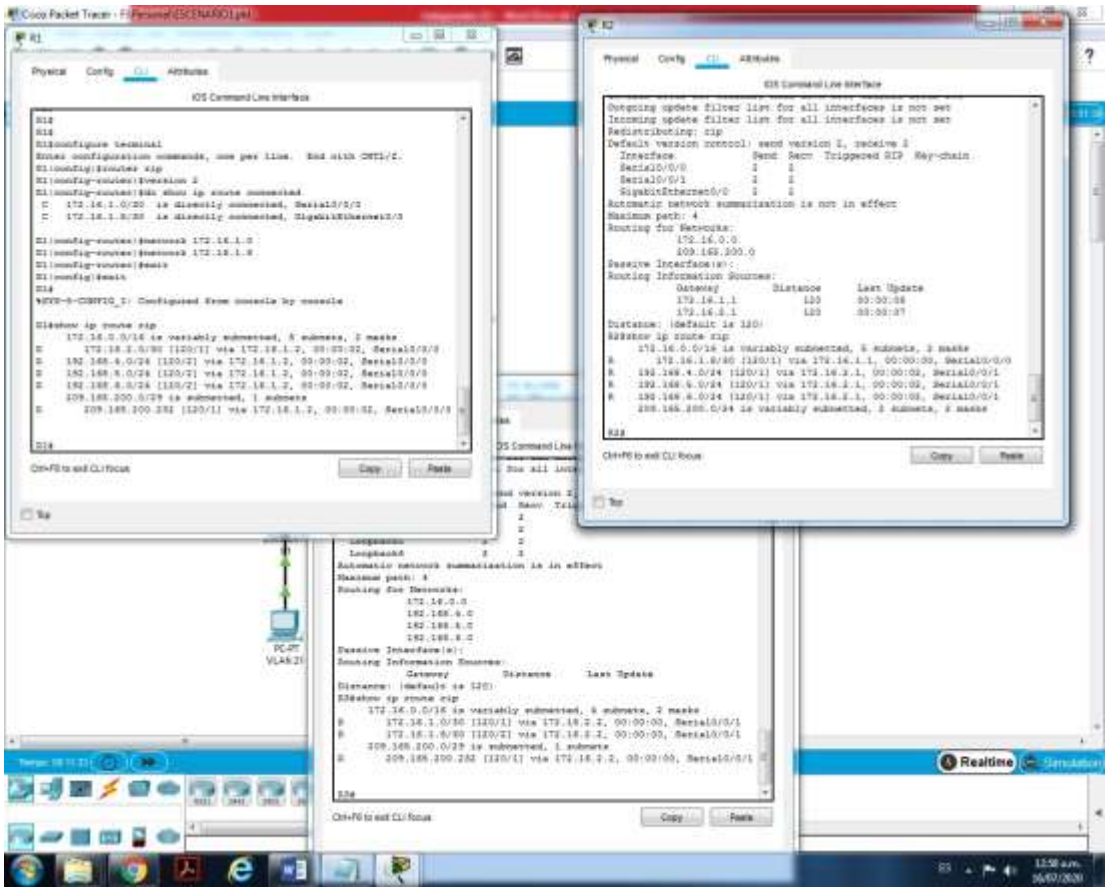
Verificación de comandos

FIGURA 5 - VERIFICACIÓN DE SHOW IP PROTOCOLS



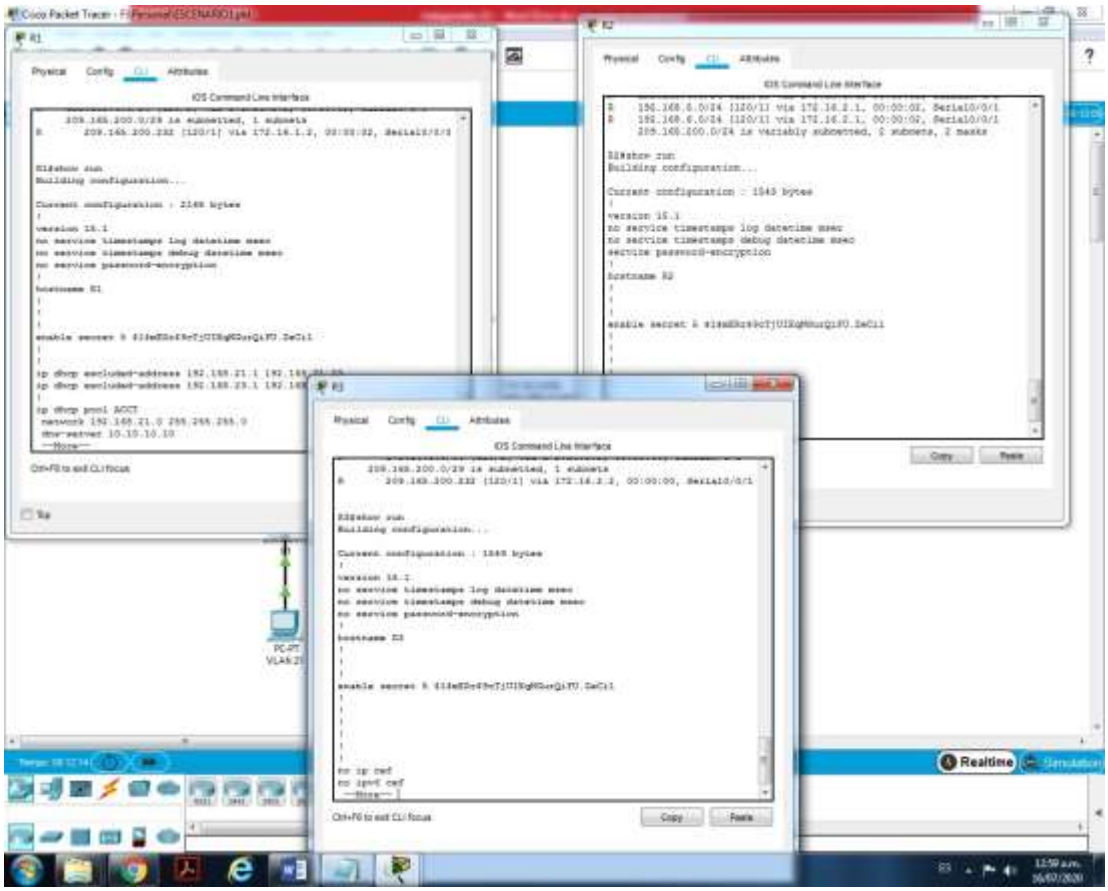
Fuente: Diseño Propio/ Packet Tracer

FIGURA 6 – VERIFICACIÓN DE COMANDO SHOW IP ROUTE RIP



Fuente: Diseño Propio/ Packet Tracer

FIGURA 7 – VERIFICACIÓN COMANDO SHOW RUN 2



Fuente: Diseño Propio/ Packet Tracer

Parte 5: Implementar DHCP y NAT para IPv4

En cualquier red ya sea residencial o corporativa, suele presentarse el servicio de DHCP, o en su definición, o aquel que se encarga de asignar direcciones IP, ya sea aun solo computador o a un grupo de estos. Sin embargo, hay que considerar, que para llevar a cabo este proceso se debe configurar el servidor o en este caso en es específico, el Router que dirige hacia las redes VLANS.

Para este servicio también se debe considerar:

1. Gateway
2. Direcciones Excluidas
3. La ayuda en dispositivos si se requiere

Por otra parte, la configuración NAT, permite traducir las direcciones de un conjunto a través de una sola en particular, con el fin de proteger todos los computadores y dispositivos de la red en el envío de información o en su efecto la salida o petición hacia el internet. Teniendo entonces el proceso de la siguiente manera:

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

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 17 – DHCP Y NAT PARA IPV4

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

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

Fuente: Diseño propio/ Packet Tracer

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

La configuración del R2 incluye las siguientes tareas:

TABLA 18 – NAT EN ROUTER R2

Elemento o Tarea de Configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237

Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Diseño propio/ Packet Tracer

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

TABLA 19 – VERIFICACIÓN DE DHCP Y NAT 3

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Satisfactorio

Verificar que la PC-A pueda hacer ping a la PC-C	Satisfactorio
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	--------

Fuente: Diseño propio/ Packet Tracer

Parte 6: Configurar NTP

En esta fase a través del comando NTP, se busca que la red disponga de un horario determinado a través de este servicio, el cual se requiere asignar el maestro y el cliente, para así establecer relaciones de conexión e indicación de tiempo y fecha en cada uno de los dispositivos. Teniendo:

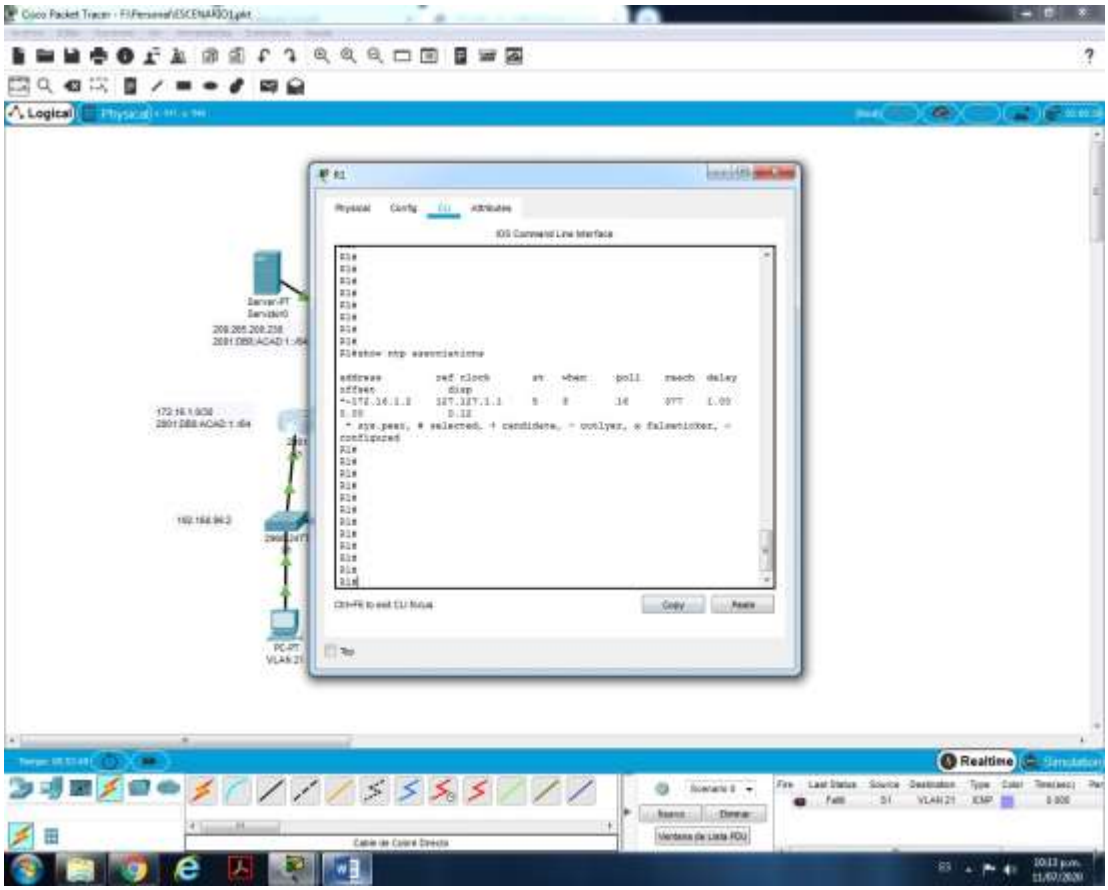
TABLA 20 – CONFIGURACIÓN DE NTP EN R1Y R2

Elemento o tarea de Configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 5 may 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

Fuente: Diseño propio/ Packet Tracer

Verificación de NTP

FIGURA 8 – VERIFICACIÓN DE NTP



Fuente: Diseño Propio/ Packet Tracer

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

En esta ultima fase del escenario 1, se busca la restricción del acceso a VTY, la cual permite definir las direcciones IP a las que se les brinda acceso remotamente al proceso de EXEC del router. Por lo tanto se puede controlar qué direcciones IP pueden acceder remotamente al router mediante la configuración de ACL en R2 y una instrucción access-class en las líneas VTY del mismo dispositivo.

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

TABLA 21 – RESTRICCIÓN DE ACCESOS EN R2

Elemento o tarea de Configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMINMGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Fuente: Diseño propio/ Packet Tracer

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

TABLA 22- CLI EN EL ROUTER R2

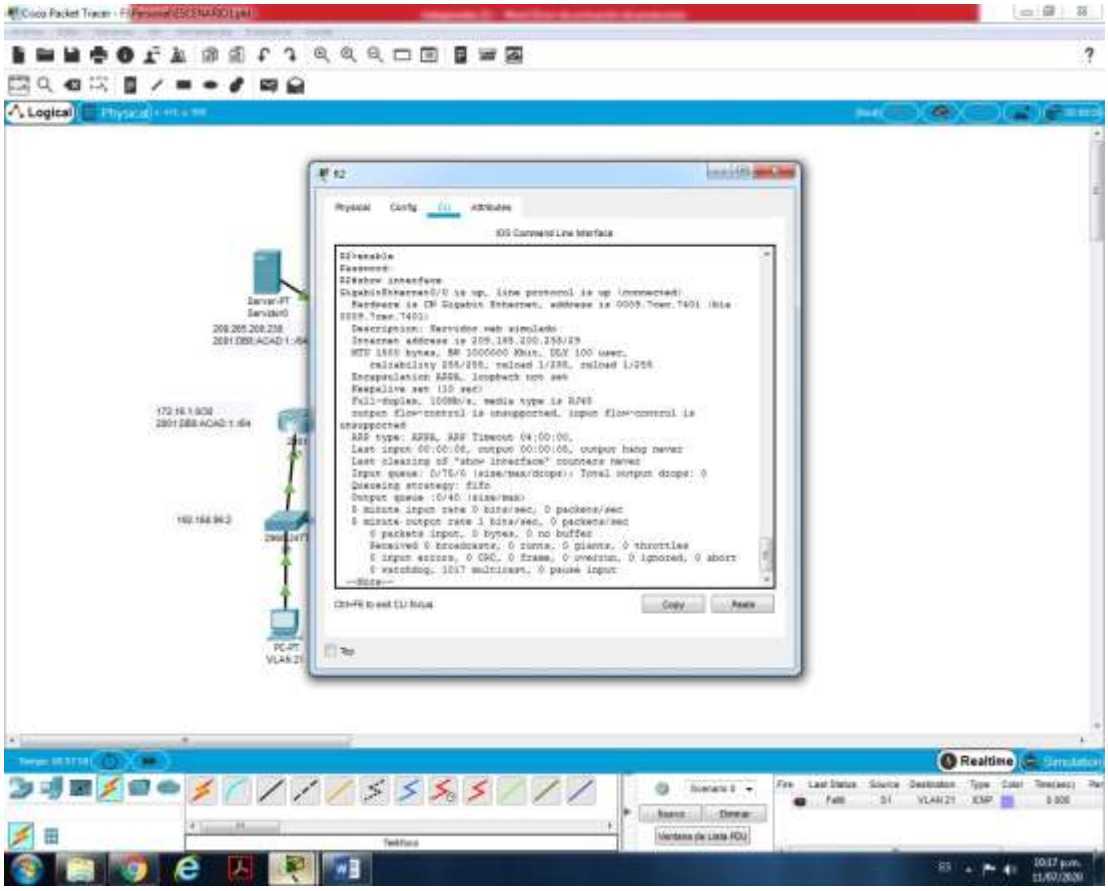
Descripción del Comando	Entrada del estudiante
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-list Standard IP access list 1 Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translation Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- R2#show ip nat translation Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.233:1025192.168.23.21:1025 209.165.200.238:80 209.165.200.238:80 tcp 209.165.200.233:1026192.168.23.21:1026 209.165.200.238:80 209.165.200.238:80 tcp 209.165.200.234:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations

Fuente: Diseño propio/ Packet Tracer

Verificación de NAT

FIGURA 9 – VERIFICACIÓN DE NAT

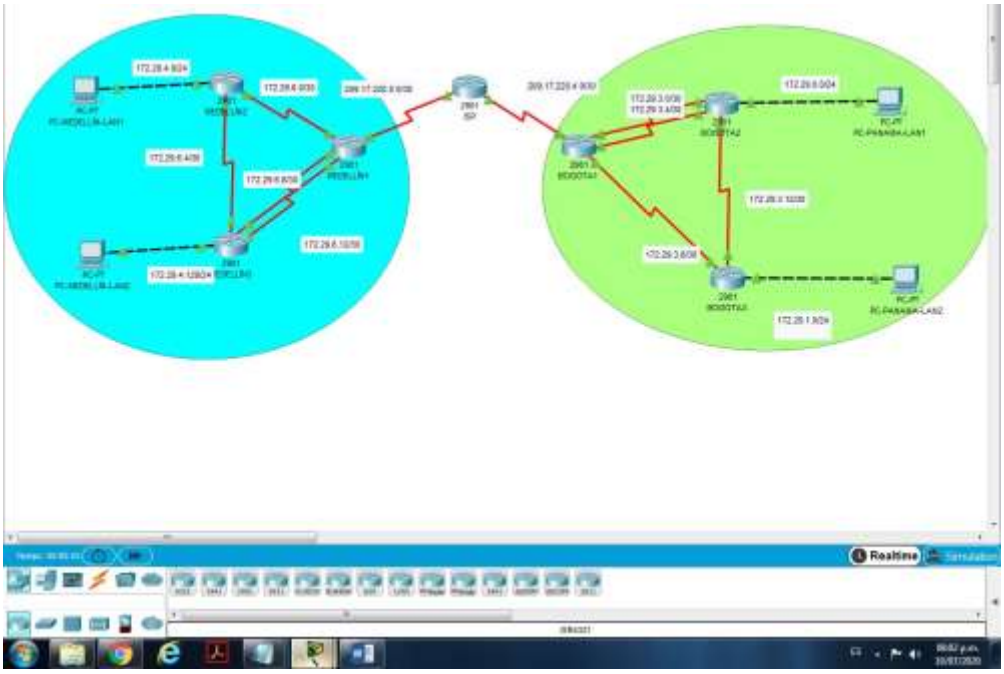


Fuente: Diseño propio/ Packet Tracer

Escenario 2

Topología de la red

FIGURA 10 – TOPOLOGÍA DE LA RED EMPLEADA



Fuente: Diseño Propio

Para el presente caso de estudio, se considera una red donde las comunicaciones se realicen en dos ciudades distanciadas, Partiendo de un servidor principal de servicio de internet y comunicaciones, el cual distribuye la información y datos a través de los distintos dispositivos.

Asimismo, este escenario facilita el uso de todos los conocimientos, en cuanto al manejo del programa Packet Tracer, en relación a su espacio de simulación, así como en la aplicación y configuración de direcciones IP, protocolos y servicios que promueven efectividad en los resultados que se desean. Aunado a ello, plantea un caso común para su comprensión y realización una vez terminado los estudios académicos.

Configuración básica de dispositivos

Para iniciar el caso de estudio, es necesario nombrar las redes de acuerdo al proveedor, las ciudades que se trabajarán y con ello las computadores que estarán conectadas a las mismas. De igual manera, se emplea un protocolo de seguridad para poder ingresar a cada configuración de los dispositivos, con el fin de que cada ciudad tenga a disposición el uso los mismos, solo por personal autorizado.

Partiendo de lo anterior, se procedió a configurar los dispositivos de acuerdo a la información de la siguiente tabla:

TABLA 23 – CONFIGURACIÓN BÁSICA DE DISPOSITIVOS

Dispositivo	Configuración
ISP	name(config)#host ISP ISP(config)#banner motd $Acceso Restringido solo para Personal Autorizado$ ISP(config)#enable secret cisco ISP(config)#line consol 0 ISP(config-line)#password clases ISP(config-line)#login ISP(config-line)#exit ISP(config)#line vty 0 15 ISP(config-line)#password clases ISP(config-line)#login ISP(config-line)#exit
Medellín1	Router(config)#host Medelln1 Medelln1(config)#banner motd $Acceso Restringido solo para Personal Autorizado$ Medelln1(config)#enable secret cisco Medelln1(config)#line consol 0 Medelln1(config-line)#password clases Medelln1(config-line)#login Medelln1(config-line)#exit

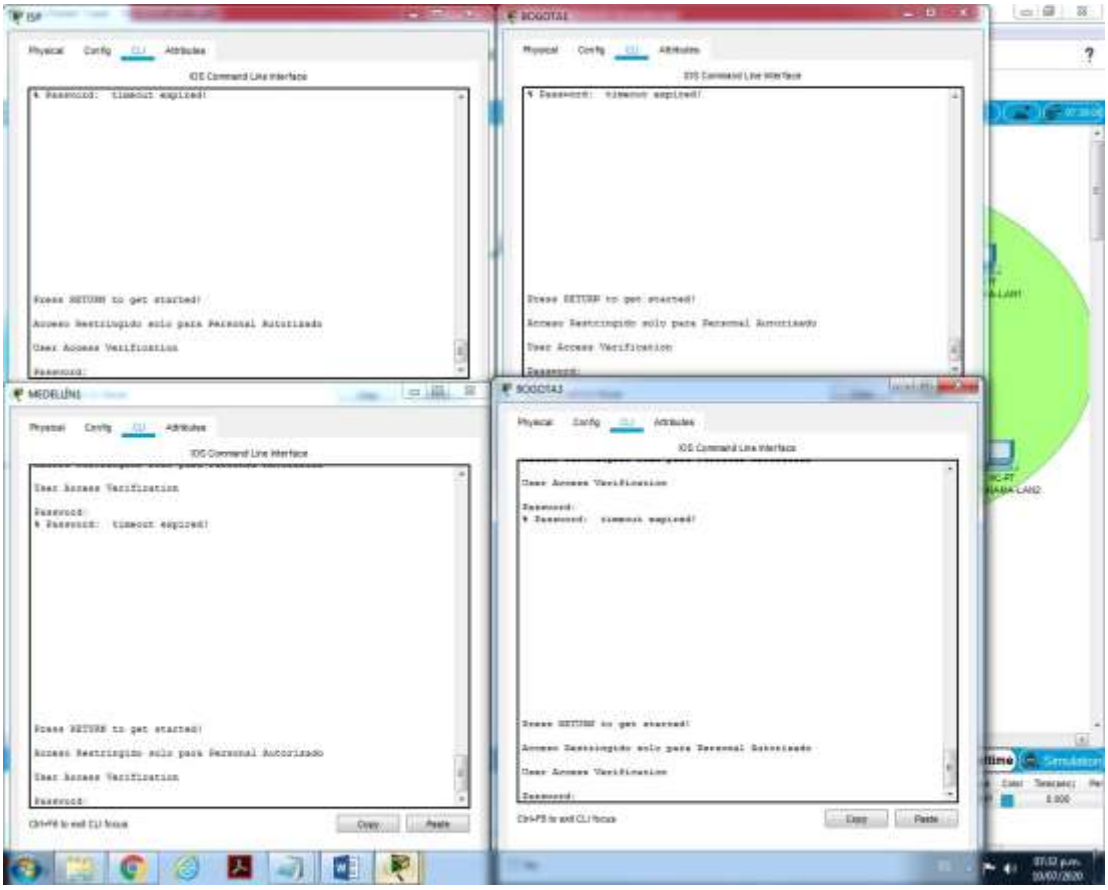
	Medelln1(config)#line vty 0 15 Medelln1(config-line)#password clases Medelln1(config-line)#login Medelln1(config-line)#exit
Medellín2	Router(config)#host Medelln2 Medelln2(config)#banner motd $Acceso Restringido solo para Personal Autorizado$ Medelln2(config)#enable secret cisco Medelln2(config)#line consol 0 Medelln2(config-line)#password clases Medelln2(config-line)#login Medelln2(config-line)#exit Medelln2(config)#line vty 0 15 Medelln2(config-line)#password clases Medelln2(config-line)#login Medelln2(config-line)#exit
Medellín3	Router(config)#host Medelln3 Medelln3(config)#banner motd $Acceso Restringido solo para Personal Autorizado$ Medelln3(config)#enable secret cisco Medelln3(config)#line consol 0 Medelln3(config-line)#password clases Medelln3(config-line)#login Medelln3(config-line)#exit Medelln3(config)#line vty 0 15 Medelln3(config-line)#password clases Medelln3(config-line)#login Medelln3(config-line)#exit
BOGOTA1	Router(config)#host BOGOTA1 BOGOTA1(config)#banner motd $Acceso Restringido solo para Personal Autorizado$ BOGOTA1(config)#enable secret cisco BOGOTA1(config)#line consol 0 BOGOTA1(config-line)#password clases BOGOTA1(config-line)#login BOGOTA1(config-line)#exit BOGOTA1(config)#line vty 0 15

	BOGOTA1(config-line)#password clases BOGOTA1(config-line)#login BOGOTA1(config-line)#exit!
BOGOTA2	Router(config)#host BOGOTA2 BOGOTA2(config)#banner motd $Acceso Restringido solo para Personal Autorizado$ BOGOTA2(config)#enable secret cisco BOGOTA2(config)#line consol 0 BOGOTA2(config-line)#password clases BOGOTA2(config-line)#login BOGOTA2(config-line)#exit BOGOTA2(config)#line vty 0 15 BOGOTA2(config-line)#password clases BOGOTA2(config-line)#login BOGOTA2(config-line)#exit
BOGOTA3	Router(config)#host BOGOTA3 BOGOTA3(config)#banner motd $Acceso Restringido solo para Personal Autorizado$ BOGOTA3(config)#enable secret cisco BOGOTA3(config)#line consol 0 BOGOTA3(config-line)#password clases BOGOTA3(config-line)#login BOGOTA3(config-line)#exit BOGOTA3(config)#line vty 0 15 BOGOTA3(config-line)#password clases BOGOTA3(config-line)#login BOGOTA3(config-line)#exit

Fuente: Diseño Propio

Verificación de Protocolo de seguridad

FIGURA 11 – VERIFICACIÓN DE SEGURIDAD



Fuente: Diseño Propio / Packet Tracer

Configuración de Direccionamiento IP

Ante un escenario compuesto de varios dispositivos, es necesario configurar el direccionamiento IP de cada uno, con el fin de establecer las conexiones con un alto nivel de efectividad. Para ello, es imprescindible establecer una ruta a través de una IP que permita generar una matriz de conexión y con ello facilidad de trabajo en la red principal y las sub redes.

Asimismo, para la configuración de los dispositivos, es requerido trabajar desde el sistema interno de cada uno y con ello apelar a la codificación necesaria para cumplir con el objetivo, considerando la siguiente información:

TABLA 24 – DIRECCIONAMIENTO IP

Dispositivo	Configuración de direccionamiento IP
Medellín1	Medellín1(config)#interface s0/0/0 Medellín1(config-if)#description conexion a ISP Medellín1(config-if)#ip address 209.17.220.2 255.255.255.252 Medellín1(config-if)#no shutdown
	Medellín1(config)#interface s0/0/1 Medellín1(config-if)#description conexion a medellin2 Medellín1(config-if)#ip address 172.29.6.1 255.255.255.252 Medellín1(config-if)#no shutdown
	Medellín1(config-if)#interface s0/1/0 Medellín1(config-if)#description conexion medellin3 Medellín1(config-if)#ip address 172.29.6.5 255.255.255.252 Medellín1(config-if)#no shut down Medellin1(config)#interface s0/1/1 Medellin1(config-if)#description conexion a medellin3 Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252 Medellin1(config-if)#no shutdown

Medellín2	Medellín2(config)#interface s0/0/0 Medellín2(config-if)#description conexion a medellin1 Medellín2(config-if)#ip address 172.29.6.1 255.255.255.252 Medellín2(config-if)#no shutdown Medellín2(config-if)#exit
	Medellin2(config)#interface s0/1/1 Medellin2(config-if)#description conexion a medellin3 Medellin2(config-if)#ip address 172.29.6.6 255.255.255.252 Medellin2(config-if)#no shutdown
	Medellín2(config)#interface g0/0 Medellín2(config-if)#ip address 172.29.4.1 255.255.255.0 Medellín2(config-if)#no shut down Medellín2(config-if)#exit
Medellín3	Medellin3(config)#interface s0/0/0 Medellin3(config-if)#description conexion a medellin1 Medellin3(config-if)#ip address 172.29.6.3 255.255.255.252 Medellin3(config-if)#no shutdown Medellin3(config)#interface s0/0/1 Medellin3(config-if)#description conexion a medellin1 Medellin3(config-if)#ip address 172.29.8.2 255.255.255.252 Medellin3(config-if)#no shutdown
	Medellin3(config)#interface s0/1/0 Medellin3(config-if)#description conexion a Medellin 2 Medellin3(config-if)#ip address 172.29.5.10 255.255.255.252 Medellin3(config-if)#no shutdown
	Medellín3(config)#interface g0/0 Medellín3(config-if)#ip address 172.29.4.128 255.255.255.0 Medellín3(config-if)#no shutdown Medellín3(config-if)#exit
BOGOTA1	BOGOTA1 (config)#interface s0/0/0 BOGOTA1(config-if)#description conexion a ISP BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#no shutdown BOGOTA1(config-if)#exit

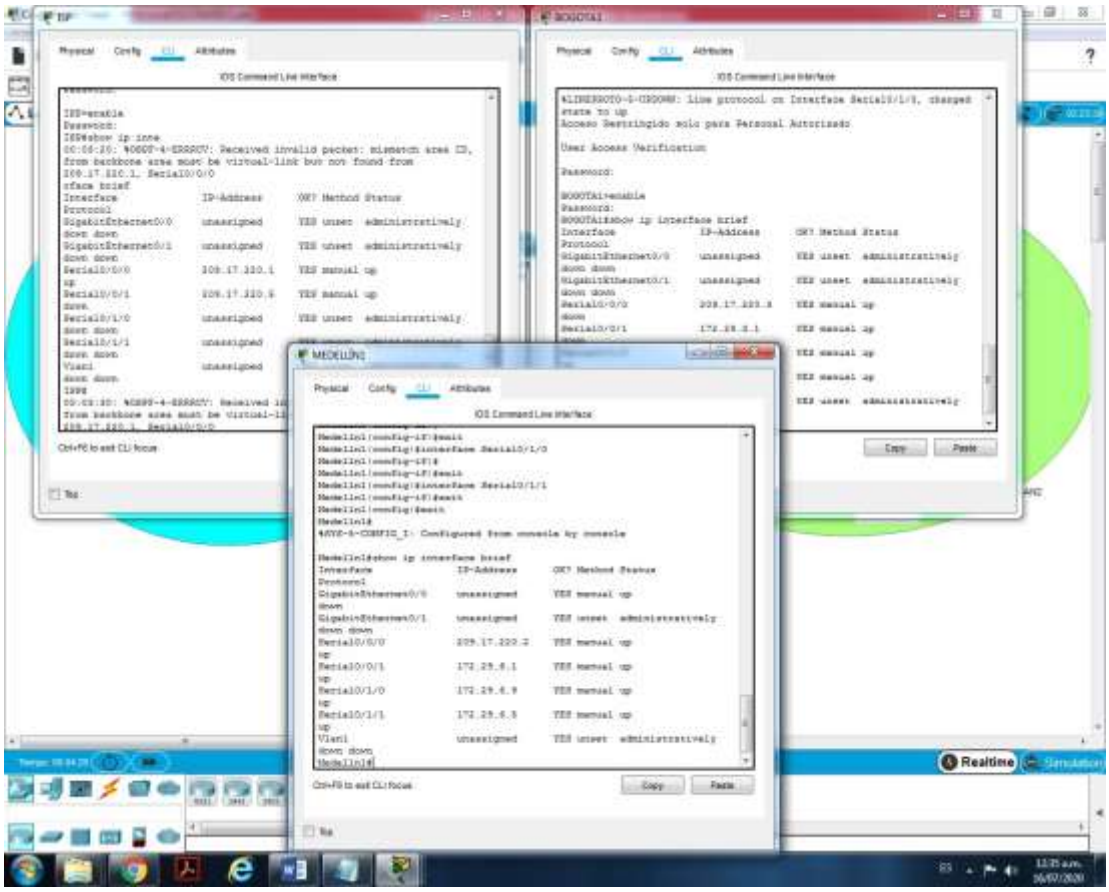
	BOGOTA1(config)#interface s0/0/1 BOGOTA1(config-if)#description conexion a BOGOTA2 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)#no shutdown BOGOTA1(config-if)#exit
	BOGOTA1(config)#interface s0/1/1 BOGOTA1(config-if)#description conexion a BOGOTA3 BOGOTA1(config-if)#ip addres 172.29.3.6 255.255.255.252 BOGOTA1(config-if)#no shutdown BOGOTA1(config-if)#exit
BOGOTA2	BOGOTA2(config)#interface s0/0/0 BOGOTA2(config-if)#description conexion a BOGOTA1 BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA2(config-if)#no shutdown BOGOTA2(config-if)#exit
	BOGOTA2(config)#interface s0/0/1 BOGOTA2(config-if)#description conexion a BOGOTA3 BOGOTA2(config-if)#ip address 172.29.3.9 255.255.255.0 BOGOTA2(config-if)#no shutdown BOGOTA2(config-if)#exit
	BOGOTA2(config)#interface g0/0 BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0 BOGOTA2(config-if)#no shutdown BOGOTA2(config-if)#exit
BOGOTA3	BOGOTA3(config)#interface s0/0/0 BOGOTA3(config-if)#description conexion a BOGOTA1 BOGOTA3(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA3(config-if)#no shutdown BOGOTA3(config-if)#exit
	BOGOTA3(config)#interface s0/1/1 BOGOTA3(config-if)#description conexion a BOGOTA2 BOGOTA3(config-if)#ip address 172.29.9.1

	255.255.255.0 BOGOTA3(config-if)#no shutdown BOGOTA3(config-if)#exit
	BOGOTA3(config)#interface g0/0 BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0 BOGOTA3(config-if)#no shutdown BOGOTA3(config-if)#exit
ISP	ISP(config)#interface s0/0/0 ISP(config-if)#description conexion a MEDELLIN1 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown
	ISP(config)#interface s0/0/1 ISP(config-if)#description conexion a BOGOTA1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown

Fuente: Diseño Propio/ Packet Tracer

Verificación de Configuración IP en Dispositivos

FIGURA 12 – VERIFICACIÓN DE IP



Fuente: Diseño Propio/ Packet Tracer

Enrutamiento a través del protocolo OSPF

Para distribuir la información de ruteo dentro de un solo sistema interno en el presente caso, es necesario utilizar el protocolo Open Shortest Path First (OSPF), el cual permite compartir información dentro de una red interna, considerando toda su estructura, desde los dispositivos genéricos dentro de una red normal hasta los computadores trabajados a través de redes Vlans.

Para ello, se procede desde el sistema interno para la codificación requerida y así conseguir los resultados propuestos, tal como se presentan a continuación:

TABLA 25 - ENRUTAMIENTO POR PROTOCOLO OSPF

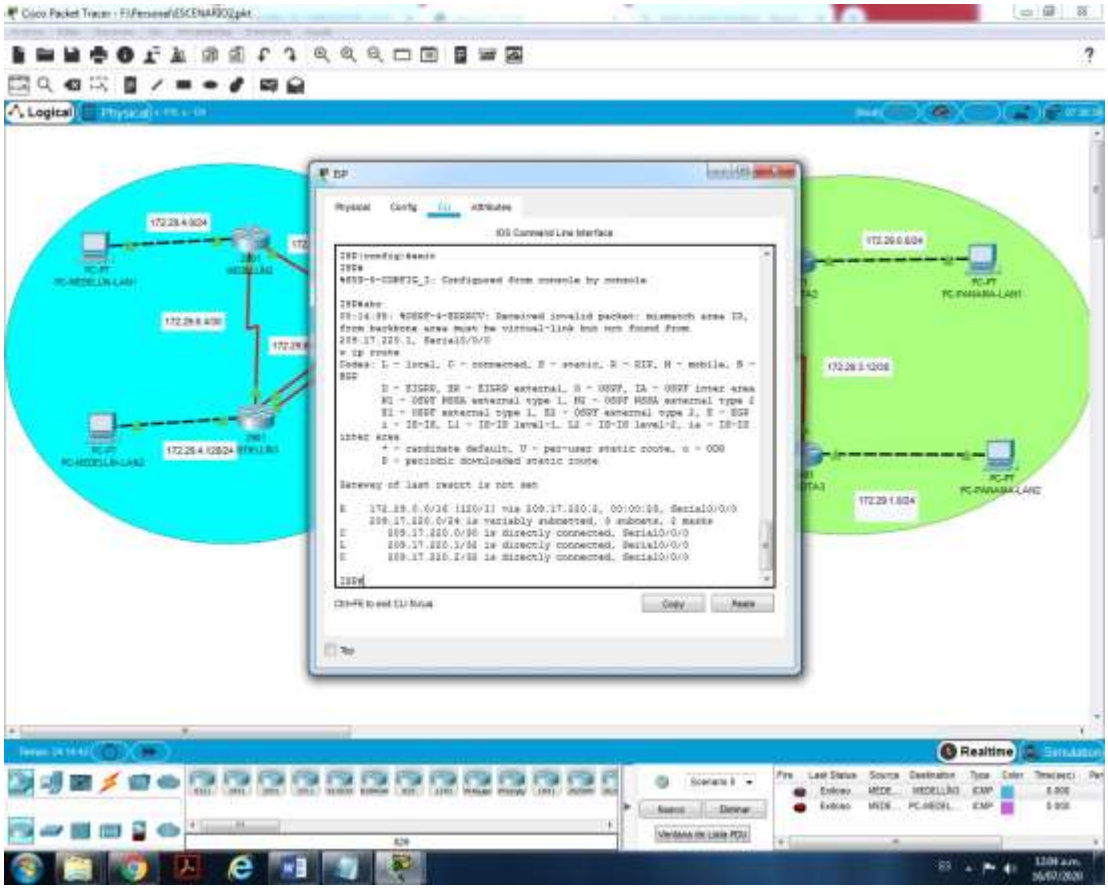
Dispositivo	Configuración OSPF
Medellín1	Medelln1(config)#router ospf 1 Medelln1(config-router)#router-id 1.1.1.1 Medelln1(config-router)#network 209.17.220.0 255.255.255.252 area 1 Medelln1(config-router)#network 172.29.6.0 255.255.255.252 area 1 Medelln1(config-router)#network 172.29.6.4 255.255.255.252 area 1 Medelln1(config-router)#network 172.29.6.8 255.255.255.252 area 1 Medelln1(config-router)#default-information originate Medelln1(config-router)#exit
Medellín2	Medelln2(config-router)#router-id 2.2.2.2 Medelln2(config-router)#network 172.29.4.0 255.255.255.252 area 1 Medelln2(config-router)#network 172.29.6.0 255.255.255.252 area 1 Medelln2(config-router)#network 172.29.6.4 255.255.255.252 area 1 Medelln2(config-router)#default-information originate Medelln2(config-router)#passive-interface g0/0
Medellín3	Medelln3(config)#router ospf 1 Medelln3(config-router)#router-id 3.3.3.3

	Medelln3(config-router)#network 172.29.4.0 255.255.255.0 area 1 Medelln3(config-router)#network 172.29.5.0 255.255.255.0 area 1 Medelln3(config-router)#network 172.29.6.0 255.255.255.0 area 1 Medelln3(config-router)#network 172.29.8.0 255.255.255.0 area 1 Medelln3(config-router)#default-information originate Medelln3(config-router)#passive-interface g0/0
BOGOTA1	BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#router-id 11.11.11.11 BOGOTA1(config-router)#network 209.17.220.0 255.255.255.252 area 1 BOGOTA1(config-router)#network 172.29.3.4 255.255.255.252 area 1 BOGOTA1(config-router)#network 172.29.3.8 255.255.255.252 area 1 BOGOTA1(config-router)#default-information originate BOGOTA1(config-router)#exit
BOGOTA2	BOGOTA2(config)#router ospf 2 BOGOTA2(config-router)#router-id 12.12.12.12 BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0 BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA2(config-router)#default-information originate BOGOTA2(config-router)#passive-interface g0/0 BOGOTA2(config-router)#exit
BOGOTA3	BOGOTA3(config)#router ospf 2 BOGOTA3(config-router)#router-id 13.13.13.13 BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 0 BOGOTA3(config-router)#network 172.29.3.0 0.0.0.255 area 0 BOGOTA3(config-router)#network 172.29.9.0 0.0.0.255 area 0 BOGOTA3(config-router)#default-information originate BOGOTA3(config-router)#passive-interface g0/0 BOGOTA3(config-router)#exit

Fuente: Diseño Propio/ Packet Tracer

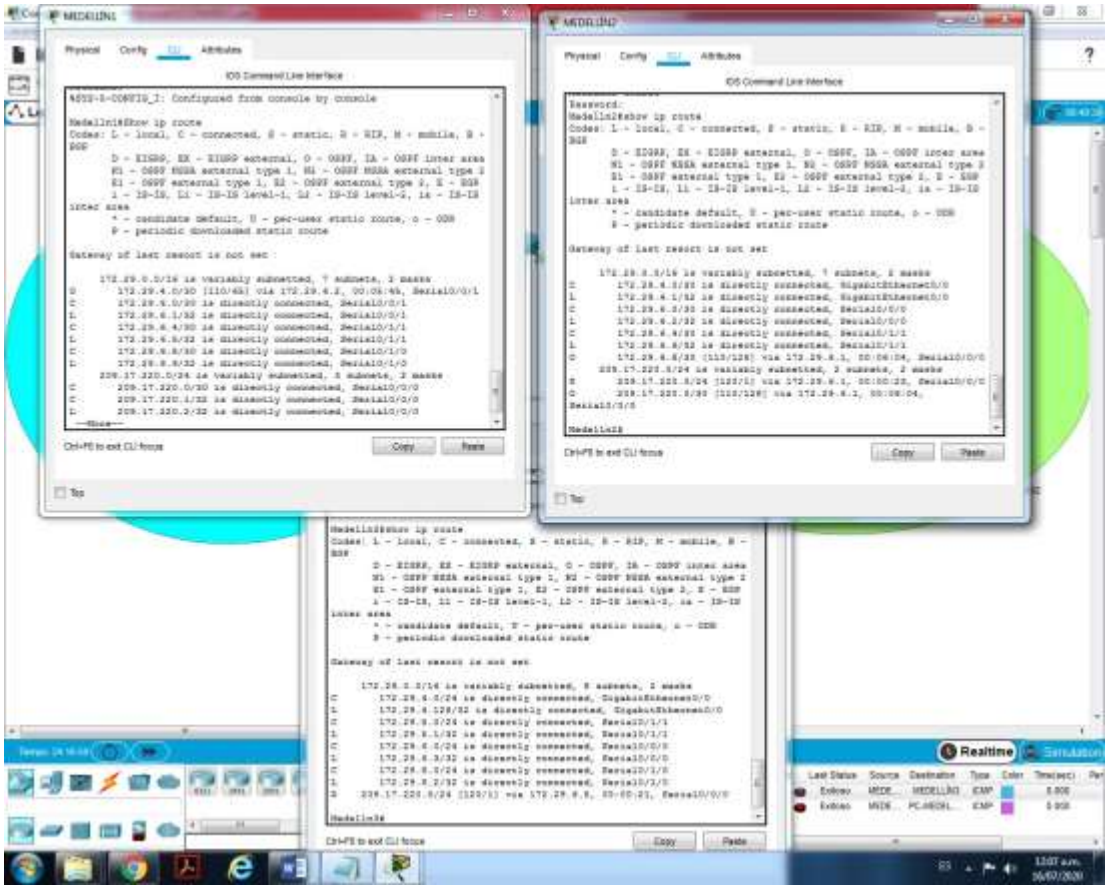
Verificación de OSPF

FIGURA 13 - SHOW IP ROUTE ISP



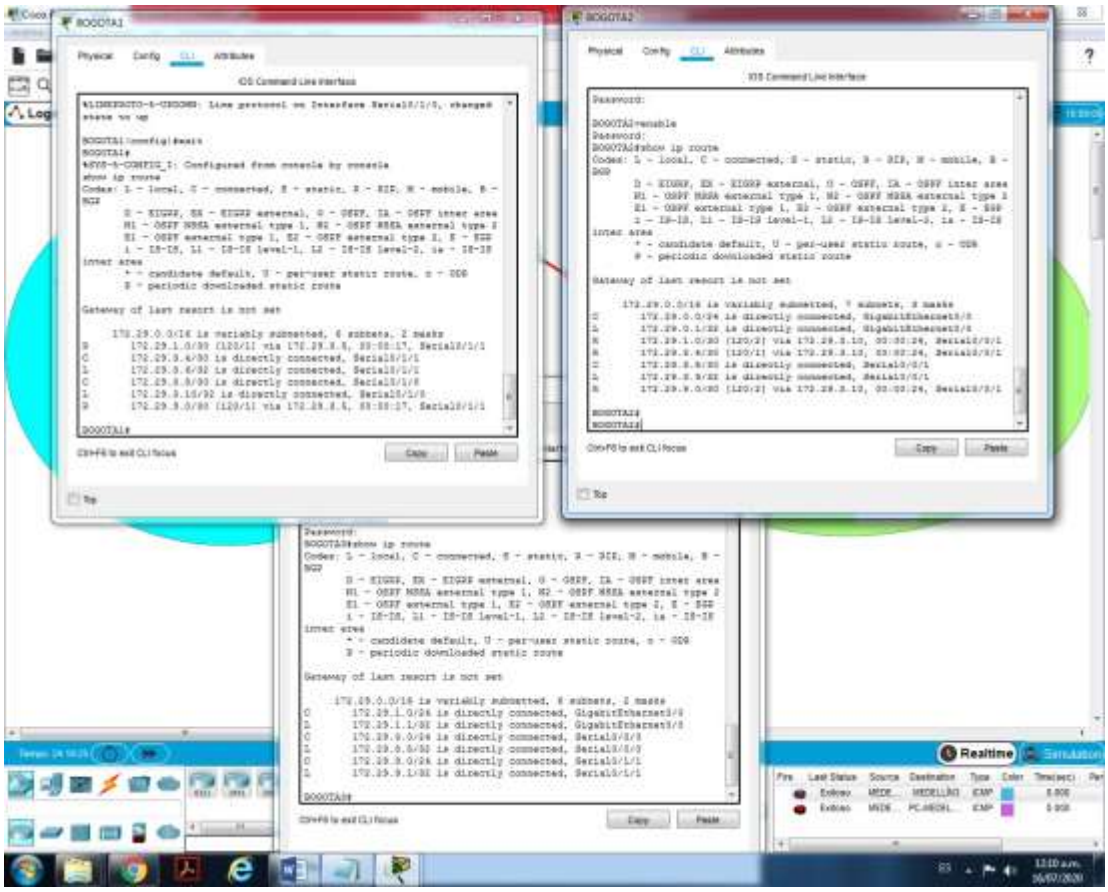
Fuente: Diseño Propio/ Packet Tracer

FIGURA 14 - SHOW IP ROUTE RED MEDELLIN



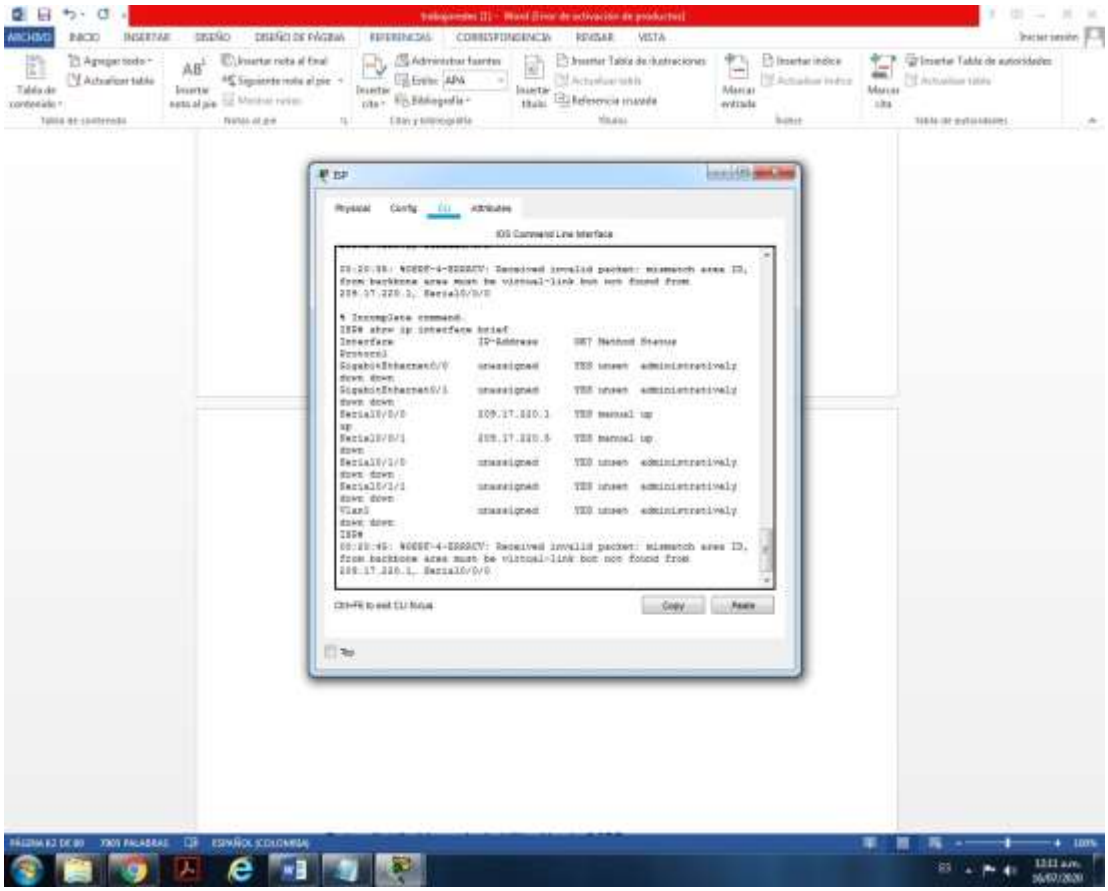
Fuente: Diseño Propio/ Packet Tracer

FIGURA 15 - SHOW IP ROUTE RED BOGOTA



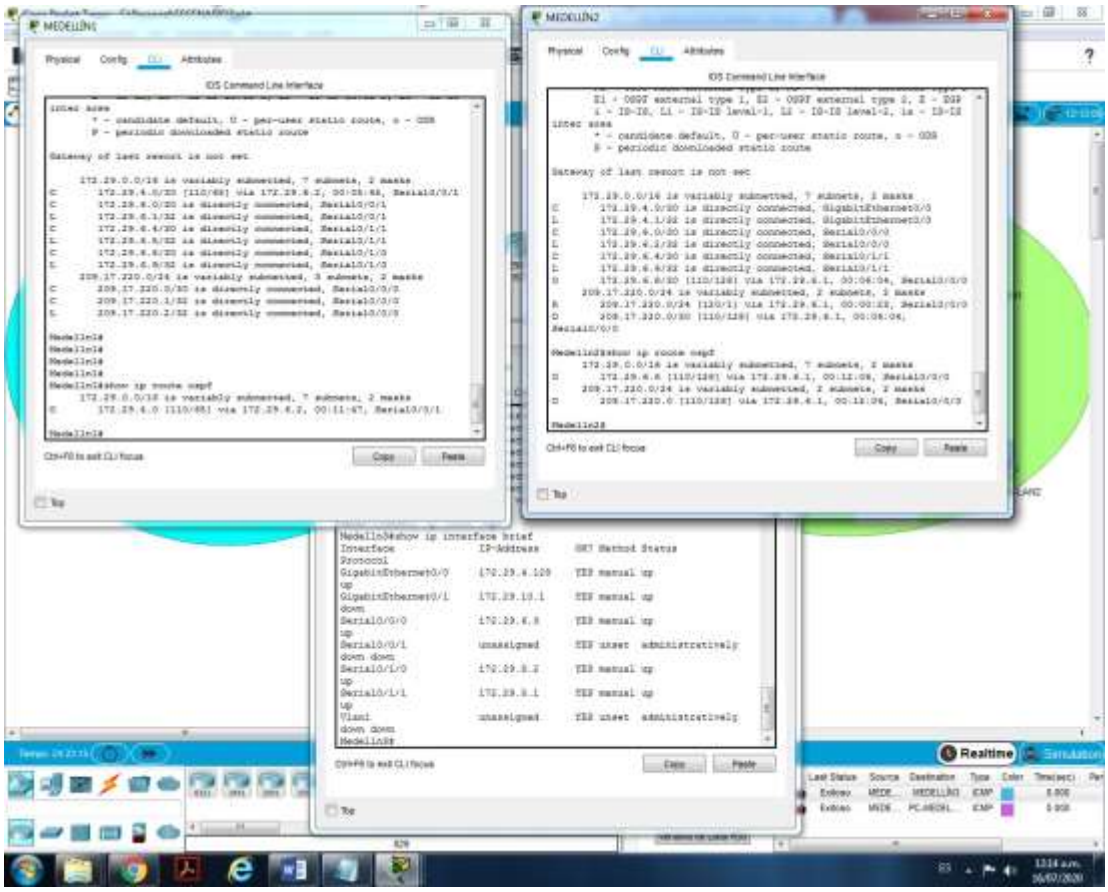
Fuente: Diseño Propio/ Packet Tracer

FIGURA 16 - SHOW IP INTERFACE BRIEF



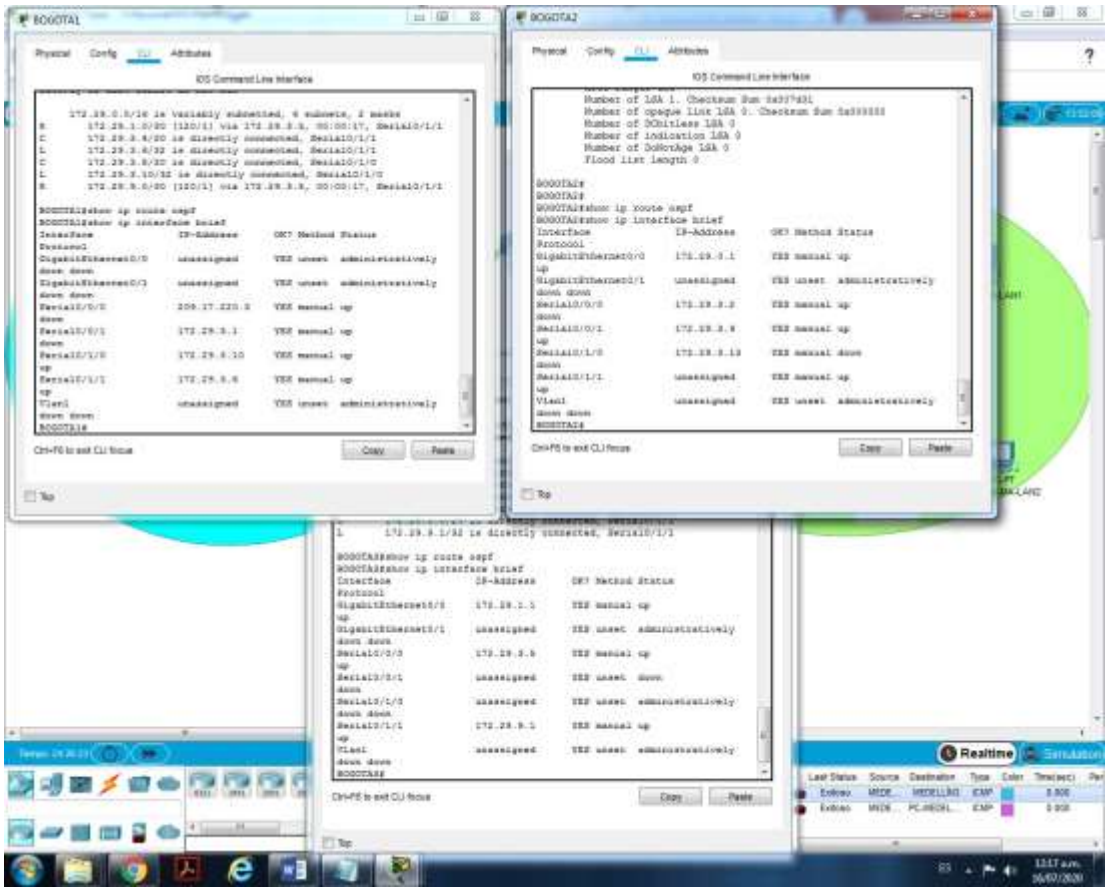
Fuente: Diseño Propio/ Packet Tracer

FIGURA 17 - SHOW IP ROUTE OSPF MEDELLIN



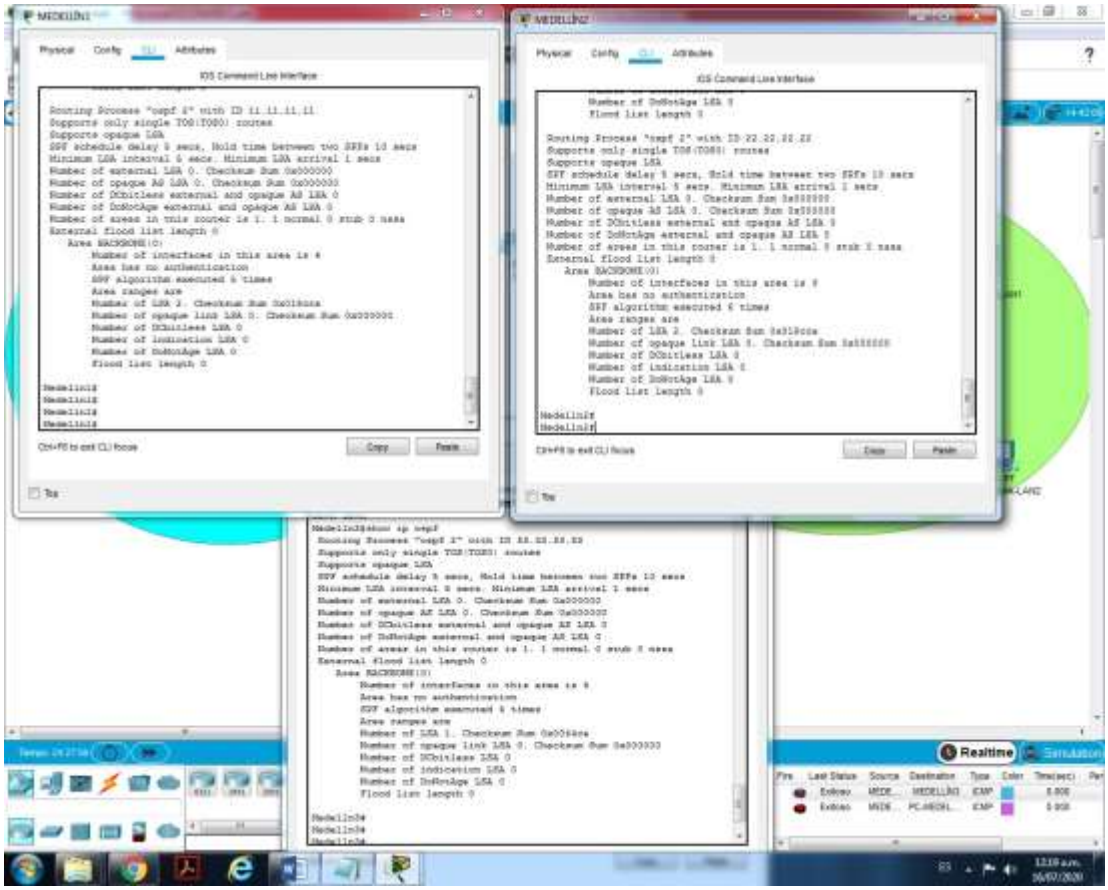
Fuente: Diseño Propio/ Packet Tracer

FIGURA 18 - SHOW IP INTERFACE BRIEF BOGOTA



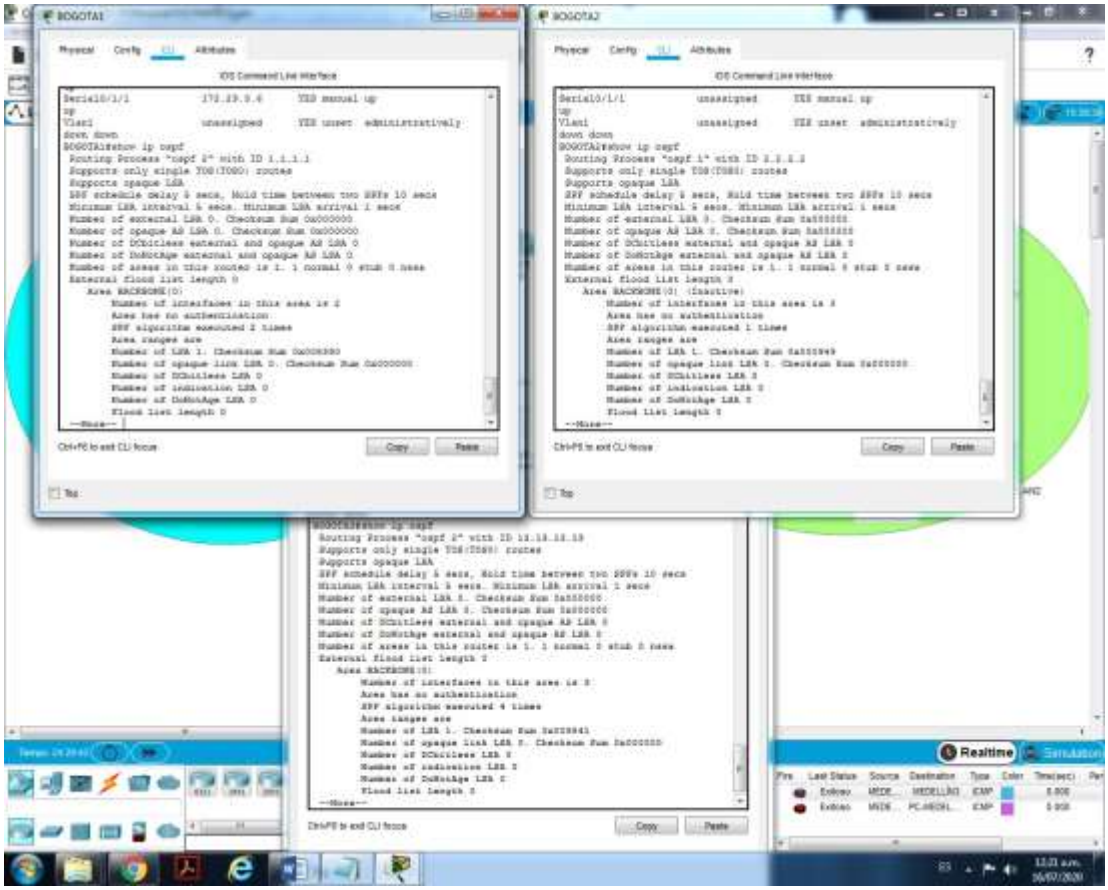
Fuente: Diseño Propio/ Packet Tracer

FIGURA 19 - SHOW IP OSPF MEDELLIN



Fuente: Diseño Propio/ Packet Tracer

FIGURA 20 - SHOW IP OSPF BOGOTA



Fuente: Diseño Propio/ Packet Tracer

Rutas distribuidas y deshabilitación de OSPF

Dentro de la aplicación del protocolo OSPF, es indispensable considerar los dispositivos principales que trabajaran dentro de la red interna, así como los que pasarán a un estado pasivo dentro de las funciones de comunicación. En el presente caso, serán las redes VLans, las cuales estarán determinadas por los computadores usados en las diferentes ciudades. Teniendo la siguiente codificación dentro del protocolo OSPF:

TABLA 26 – RUTAS DISTRIBUIDAS DE OSPF

Dispositivos	Configuración de ruta distribuida en OSPF
ISP	ISP(config)#ip route 172.29.0.0 255.255.252.0 200.100.50.2 ISP(config)#ip route 172.29.0.0 255.255.252.0 200.100.50.4

Fuente: Diseño Propio/ Packet Tracer

Deshabilitación de propagación de OSPF

TABLA 27 – DESHABILITACIÓN DE OSPF

Dispositivo	Deshabilitación de OSPF
Medellín 2	Medellín 2(config-router)#passive-interface g0/0 Medellín 2(config-router)#exit
Medellín 3	Medellín 3(config-router)#passive-interface g0/0 Medellín 3(config-router)#exit
BOGOTA2	BOGOTA2(config-router)#passive-interface g0/0 BOGOTA2 (config-router)#exit
BOGOTA3	BOGOTA3(config-router)#passive-interface g0/0 BOGOTA3 (config-router)#exit

Fuente: Diseño Propio/ Packet Tracer

Configuración del servicio DHCP

Partiendo de la topología de red del presente caso, se busca aplicar el servicio dchp, para así configurar los parámetros de TCP/IP, como la dirección IP y la máscara de subred automáticamente, los computadores de la red VLans de cada ciudad.

Para ello, se debe considerar, la creación del pool, así como también el Gateway y con ello el número de usuarios que dispondrá la subred para la creación de las IP. Asimismo, de acuerdo a la tipología del presente caso, es necesario trabajar el servicio desde el router 2 de cada ciudad, y aunado a ello utilizar el router tres como un dispositivo de ayuda que permita enlazar comunicaciones y finalizar el servicio en los computadores que tenga enlazado el mismo.

En el presente caso, se trabajó de acuerdo a la siguiente codificación:

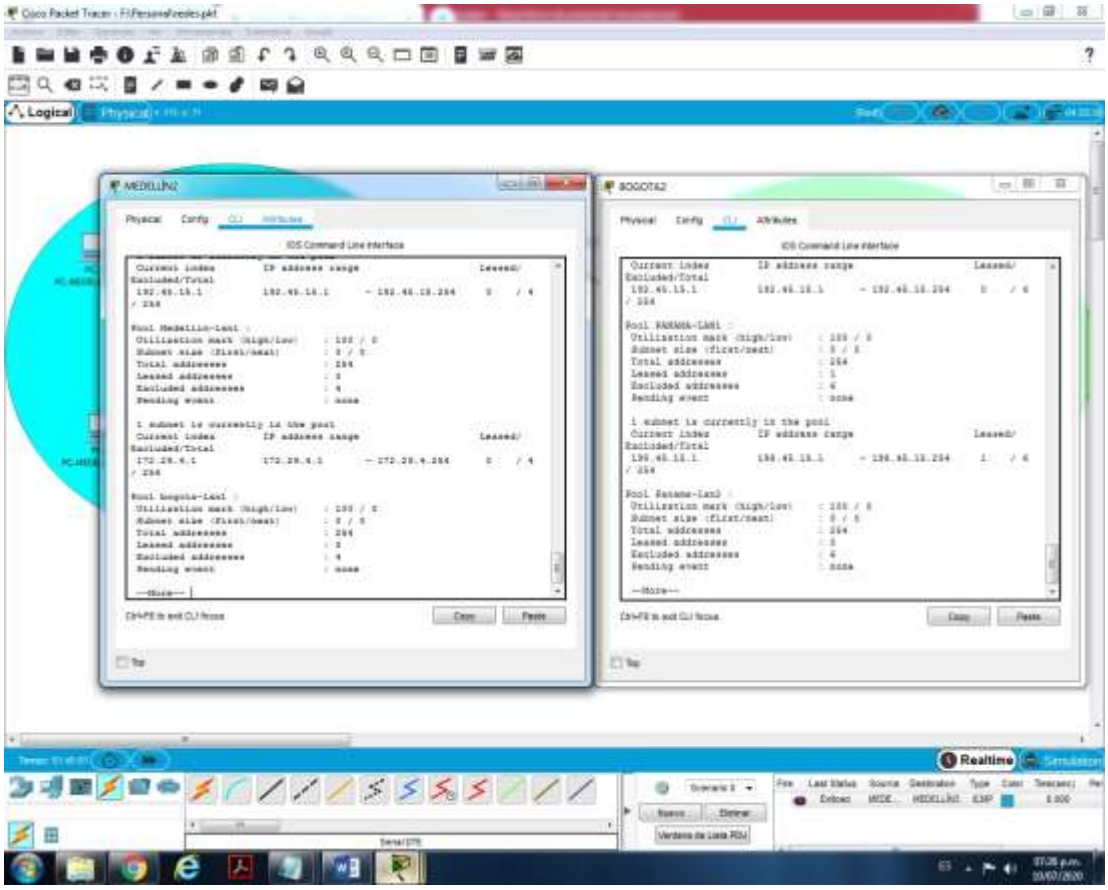
TABLA 28 – SERVICIO DE DCHP

Dispositivo	Configuración dhcp
Medellín2	Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10 Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133 Medellin2(config)# Medellin2(config)#ip dhcp pool Medellin2 Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.1 Medellin2(dhcp-config)#dns-server 8.8.8.8 Medellin2(dhcp-config)#exit Medellin2(config)#ip dhcp pool Medellin3 Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.129 Medellin2(dhcp-config)#dns-server 8.8.8.8 Medellin2(dhcp-config)#exit
Medellín3	Medellin3(config)#int s0/1/0 Medellin3(config-if)#ip helper-address 172.26.6.5

	Medellin3(config-if)#exit
BOGOTA2	BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10 BOGOTA2(config)#ip dhcp pool bogota-lan1 BOGOTA2(dhcp-config)#network 172.29.0.1 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.0.1 BOGOTA2(dhcp-config)#domain-name lan1.bogota.com BOGOTA2(dhcp-config)#exit BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10 BOGOTA2(config)#ip dhcp pool medellin-lan2 BOGOTA2(dhcp-config)#network 172.29.1.1 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.1.1 BOGOTA2(dhcp-config)#domain-name lan1.bogota.com BOGOTA2(dhcp-config)#exit
BOGOTA3	BOGOTA3(config)#interface g0/0 BOGOTA3(config-if)#ip helper-address 172.29.3.5 BOGOTA3(config-if)#exit

Fuente: Diseño Propio/ Packet Tracer

FIGURA 21 – VERIFICACIÓN DE DCHP



Fuente: Diseño Propio/ Packet Tracer

Configuración de traducciones NAT PAT

Planteando el escenario donde todas las redes públicas no entran al internet, debido a la capacidad de este último y la optimización que se debe tener en cuenta en los trabajos de redes y comunicaciones. Por lo tanto, es requerido plantear el uso de NAT y PAT como traductores de las redes internas, como un medio de seguridad y protección de las direcciones de uso privado. Por ello, se dispone de traducir toda la información que provenga de las redes interna bajo la dirección de red del router principal de cada ciudad.

En consecuencia, para el presente caso se trabajó de acuerdo a la siguiente estructura:

TABLA 29 - CONFIG. PAP Y CHAP 1

Dispositivo	Configuración PAP
ISP	ISP(config)#int s 0/0/0 ISP(config-if)#encapsulation PPP ISP(config-if)#PPP authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config)#int s 0/0/1 ISP(config-if)#encapsulation PPP ISP(config-if)#PPP authentication chap ISP(config-if)#ppp pap sent-username ISP password cisco
Medellin1	Medellin1(config)#int s 0/0/0 Medellin1(config-if)#encapsulation PPP Medellin1(config-if)#PPP authentication pap Medellin1(config-if)#ppp pap sent-username Medellin1 password cisco
BOGOTA1	Bogota1(config)#int s 0/0/0 Bogota1(config-if)#encapsulation PPP Bogota1(config-if)#PPP authentication chap Bogota1(config-if)#ppp pap sent-username Bogota1 password cisco

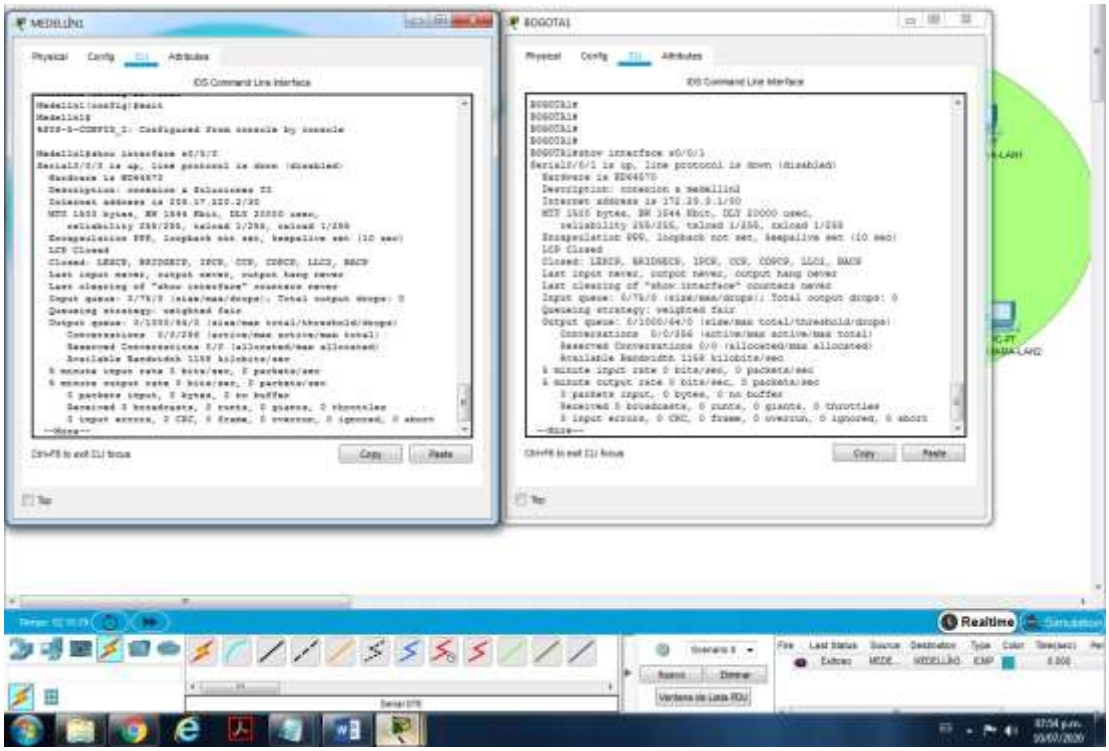
Fuente: Diseño Proprio/ Packet Tracer

TABLA 30 - CONFIGURACIÓN NAT 1

Dispositivo	Configuración NAT
Medellín1	Medellin1(config)#ip access-list standard host Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.0.255 Medellin1(config-std-nacl)#ip nat inside source list host interface s0/0/0 overload Medellin1(config)#int s0/0/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#int s0/0/1 Medellin1(config-if)#ip nat outside Medellin1(config-if)#int s0/1/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#int s0/1/1 Medellin1(config-if)#ip nat outside
BOGOTA1	Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.0.255 Bogota1(config-std-nacl)#ip nat inside source list host interface s0/0/0 overload Bogota1(config)#int s0/0/0 Bogota1(config-if)#ip nat outside Bogota1(config-if)#int s0/0/1 Bogota1(config-if)#ip nat outside Bogota1(config-if)#int s0/1/0 Bogota1(config-if)#ip nat outside Bogota1(config-if)#int s0/1/1 Bogota1(config-if)#ip nat outside

Fuente: Diseño Propio/ Packet Tracer

FIGURA 22 – VERIFICACIÓN DE PAP Y CHAP



Fuente: Diseño Propio/Packet Tracer

CONCLUSIONES

Las redes son un enlace de comunicaciones que se prestan para facilitar el intercambio de comunicaciones ya sea un espacio residencial o corporativo. Desde el plano del ejercicio, se presenta una tipología de red para diferentes ciudades donde se requiere establecer una red segura y efectiva. Partiendo de una tipología general, donde se configura los dispositivos con sus respectivos nombres y protocolos de seguridad para establecer políticas de seguridad y confianza en el manejo de dato e información de las empresas.

En el escenario 1, se presenta una red básica la cual le provee internet un servidor, en las mismas se configuran los dispositivos con la información básica y protocolos de seguridad, asimismo, se configura las redes VLANS y los enrutamientos en los dispositivos para poder tener un conexión efectiva entre cada uno de ellos.

Es de resaltar, que en el escenario se emplea el servicio DHCP para la asignación de las direcciones IP, así como el NAT, como traductor de direcciones, y el NTP como configuración del tiempo y fecha. Dentro de un plano general las conexiones en la red ejercen una función efectiva, dando resultados satisfactorios, los cuales pueden ser verificados con el comando PING; así como los diversos procesos de enrutamiento a través de los SHOW.

Posteriormente, en el escenario 2, se configura las direcciones IP para enlazar las conexiones y con ello se realiza el enrutamiento a través del comando OSPF para así lograr una conexión de manera interna dentro de cada ciudad. Es de resaltar, que en este último paso se procedió a hacer las rutas distribuidas y las deshabilitaciones con el fin de llevar un proceso óptimo.

Por último, se estableció el servicio DHCP para las respectivas VLans de cada ciudad y con ello las configuraciones NAT y PAPA como traducciones de

direccionamiento que permitan brindar seguridad en las redes privadas. Desde un plano de comunicaciones y resultados, el ejercicio cumplió con los objetivos propuestos, aunado a ello, proporciona los conocimientos y experiencia necesaria para poder implementar todo lo aprendido dentro del plano profesional y brindar así soluciones efectivas a las necesidades de la sociedad.

BIBLIOGRÁFIA

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación.

Recuperado:https://staticcourseassets.s3.amazonaws.com/RSE50ES/module4/index.html

CISCO. (2014). **Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación.**

Recuperado:https://staticcourseassets.s3.amazonaws.com/RSE50ES/module5/index.html

CISCO. (2014). **Enrutamiento Estático. Principios de Enrutamiento y Conmutación.**
Recuperado:https://staticcourseassets.s3.amazonaws.com/RSE50ES/module 6/index.html#6.0.1.1

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking.

Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2014). **VLANs.** Principios de Enrutamiento y Conmutación.

Recuperado:https://staticcourseassets.s3.amazonaws.com/RSE50ES/module3/index.html

ANEXOS

- Escenarios https://drive.google.com/drive/folders/1AJeN2NCJ5scamhKKiSvFxsx-6fozrIuO?usp=sharing