SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL ESTUDIO DE TECNOLOGÍA CISCO

CRISTIAN DAVID LEDEZMA MOSQUERA

UNIVERSIDAD NACIONAL Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

QUIBDÓ

2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL ESTUDIO DE TECNOLOGÍA CISCO

CRISTIAN DAVID LEDEZMA MOSQUERA

INFORME FINAL PARA OBTENER EL TITULO DE INGENIERO EN SISTEMAS

DIEGO EDINSON RAMIREZ CLAROS “TUTOR”

UNIVERSIDAD NACIONAL Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
QUIBDÓ
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Quibdó - Chocó (23, 05, 2020)

Dedicatoria

Este artículo se le dedico a Dios primeramente porque sin él no hubiera podido terminar este proceso, a mi Familia por su apoyo incondicional y a todo el equipo de la UNAD que fueron el medió para hacer este sueño posible.

AGRADECIMIENTOS

Agradezco de primera mano el apoyo de Dios y mi familia durante todo este procesó de formación, porque el logro obtenido es el esfuerzo de muchos que han estado allí junto conmigo para lograr el cumplimiento de los procesos necesarios para llegar a este punto, agradezco a esta gran institución formativa como lo es la UNAD por ser la familia que me pidió cumplir mis sueños de ser Ingeniero en Sistemas

TABLA DE CONTENIDO

Pág.
1. Introducción 11
2. Objetivos 12
2.1 Objetivo general 12
2.2 Objetivos específicos 12
3 Planteamiento del problema 13
3.1 Definición del problema 13
3.2 Justificación 13
5.1 Materiales 14
5.2 Metodología 14
6 Desarrollo del proyecto 15
SCENARIO 1 15
Parte 1: Inicializar dispositivos 16
Parte 2: Configurar los parámetros básicos de los dispositivos 17
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 24
Parte 4: Configurar el protocolo de routing dinámico RIPv2 29
Parte 5: Implementar DHCP y NAT para IPv4 32
Parte 6: Configurar NTP 34
Parte 7: Configurar y verificar las listas de control de acceso (ACL) 34
ESCENARIO 2 36
parte 1: Configuración del enrutamiento 36
Parte 2: Tabla de Enrutamiento 41
Parte 3: Deshabilitar la propagación del protocolo OSPF 43
Parte 4: Verificación del protocolo OSPF 45
Parte 5: Configurar encapsulamiento y autenticación PPP 49
Parte 6: Configuración de PAT 50
Parte 7: Configuración del servicio DHCP 51
6.1 Análisis del desarrollo del proyecto 54
6.2 Cronograma 55
Conclusiones 56
Recomendaciones 57
Bibliografía 58

LISTA DE TABLAS

Pág.

Escenario 1

Tabla 1 Inicializar y volver a cargar los Reuters y los switches. 16
Tabla 2 Configurar la computadora de Internet. 17
Tabla 3 Configurar R1 17
Tabla 4 Configurar R2 19
Tabla 5 Configurar R3 21
Tabla 6 Configurar S1 21
Tabla 7 Configurar S1 22
Tabla 8 Verificar la conectividad de la red 22
Tabla 9 Configurar S1 25
Tabla 10 Configurar S3 26
Tabla 11 Configurar R1 27
Tabla 12 Verificar la conectividad de la red 27
Tabla 13 Configurar RIPv2 en el R1 29
Tabla 14 Configurar RIPv2 en el R2 30
Tabla 15 Configurar RIPv3 en el R2 31
Tabla 16 Verificar la información de RIP 31
Tabla 17 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 32
Tabla 18 Configurar la NAT estática y dinámica en el R2 33
Tabla 19 Verificar el protocolo DHCP y la NAT estática 34
Tabla 20 Configurar NTP 34
Tabla 21 Restringir el acceso a las líneas VTY en el R2 34
Tabla 22 Introducir el comando de CLI adecuado 35
Tabla 23 Deshabilitar la propagación del protocolo OSPF 44
Tabla 24 Cronograma 57

LISTA DE FIGURAS

Pág.

Escenario 1
Fig. 1 Topología 1 15
Fig. 2 Topología 2 16
Fig. 3 Verificar conectividad de la red R1..... 23
Fig. 4 Verificar conectividad de la red R2..... 23
Fig. 5 Verificar conectividad de la red Server0..... 24
Fig. 6 Verificar conectividad de la red S1..... 28
Fig. 7 Verificar conectividad de la red S3..... 28
Fig. 8 Verificar conectividad de la red S1..... 29
Escenario 2
Fig. 9 Topología de red 36
Fig. 10 Topología de red 37
Fig. 11 tabla de enrutamiento bogota3..... 42
Fig. 12 verificar balanceo de carga bogota1 42
Fig. 13 rutas estáticas Reuter ISP 43
Fig. 14 Verificación del protocolo OSPF Medellín 1..... 46
Fig. 15 Verificación del protocolo OSPF Medellín 2..... 46
Fig. 16 Verificación del protocolo OSPF Medellín 3.....47
Fig. 17 Verificación del protocolo OSPF Bogotá 1 47
Fig. 18 Verificación del protocolo OSPF Bogotá 2 48
Fig. 19 Verificación del protocolo OSPF Bogotá 3 48

GLOSARIO

ACL: es un concepto de seguridad informática usado para fomentar la separación de privilegios, esto permiten controlar el flujo del tráfico en equipos de redes, tales como Routers y Switches entre otros.

Encapsulamiento: son los datos que atraviesan la red y van siendo gestionados por diferentes elementos desde el origen al destino.

Enrutamiento: es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

LAN: red de área local en ingles Local Área Network es una red que funciona espacios pequeños, como por ejemplo una red de hogar, oficinas entre otras funciones.

NAT: Es el proceso de hacer que redes de ordenadores utilicen un rango de direcciones especiales y se conecten a Internet usando una única dirección IP y sirve para cualquier tipo de red.

Protocolos: son una lista de Control de Acceso, las ACLs permiten asignar permisos a usuarios o a grupos. Una ACL puede permitir o denegar el acceso de usuarios concretos a objetos protegidos.

WAN: es una red de área amplia que se encarga de unir redes de Internet de tipo LAN.

RESUMEN

La Universidad Nacional Abierta y a Distancia en convenio con CISCO Networking Academia, han puesto a disposición el diplomado: “CISCO diseño e implementación de redes LAN-WAN”, este convenio se realizó para que los próximo a graduarse de la escuela de Básica pudiéramos tener la oportunidad de afianzar conocimientos en el área de redes, permitiendo así que nosotros como egresados de la UNAD tengamos la aprobación de esta gran institución en nuestras experiencias profesionales como la elaboración de prototipos de redes que permitan dar repuestas a las necesidades que día a día surge en las empresas. La metodología utilizada en este campo de formación basadas en problemas en fundamental para el desarrollo de las competencias esenciales que necesitamos para afrontar problemas de comunicación que se presente interconexión de datos en cualquier lugar, por ello el material dispuesto está a la vanguardia con las problemáticas actuales de las redes de comunicación y su debida implementación en ambientes controlados permite desarrollar redes de datos que comuniquen al mundo que conocemos y al que estamos por descubrir, abriéndonos a una cantidad de información global que se trasmite a través del interconexión y que todos podemos acceder por ello la importancia de este diplomados en redes de comunicación.

Palabras claves: redes, tecnología comunicación, interconexión, dispositivos, información desarrollo, implementación, globalización, datos, empresas, desarrollo

1. INTRODUCCIÓN

El diplomado nos conllevó a conocer los conceptos y tecnologías básicos que comprenden redes grandes y pequeñas, estos conceptos nos permitieron complementar y configurar redes pequeñas con las diferentes aplicaciones u herramientas necesarias que necesitan para su eficaz funcionamiento.
la prueba de habilidades practica de cisco permite poner en práctica los conceptos y o habilidades adquiridas en la implementación de redes, para esto tuvo lugar en propiciar dos escenarios en el cual nosotros como estudiantes pudiéramos desarrollar lo aprendido durante el proceso de formación del diplomado de CISCO, que nos permitió aprender sobre temas como:
las redes y dispositivos que la conforman, configuración de los mismos para establecer una comunicación estable entre los mismo, incursionar en configuraciones VLAN, la configuración de DHCPv4 y DHCPv6, monitorear los diferentes estados de los routing como lo son el estático y el predeterminado

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Permitir evaluar las habilidades obtenidas en el diplomado con objeto de solucionar los diferentes escenarios expuestos en las practicas haciendo similitud de la vida real, pero en un escenario controlado como lo ofrece la herramienta Packet Tracer.

2.2 OBJETIVOS ESPECÍFICOS

Seleccionar y configurar los dispositivos necesarios para establecer la red solicitada para cada escenario.

busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado.

desarrollar las soluciones a los problemas relacionados con diversos aspectos de Networking.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

El problema a solucionar es la implementación de una red en cada uno de los diferentes escenarios expuesto con las diferentes especificaciones requeridas en estos.

3.2 JUSTIFICACIÓN

El problema anteriormente es la forma de practicar los conocimientos adquiridos en el Diplomado de Cisco, y la herramienta para su solución fue el uso de Cisco Packe Tracer por medio de la cual se establece el diseño de la red y las respectivas configuraciones a los dispositivos de acuerdo a lo requerido.

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

El material utilizado fue la Herramienta Software llamada Cisco Packet Tracer

5.2 METODOLOGÍA

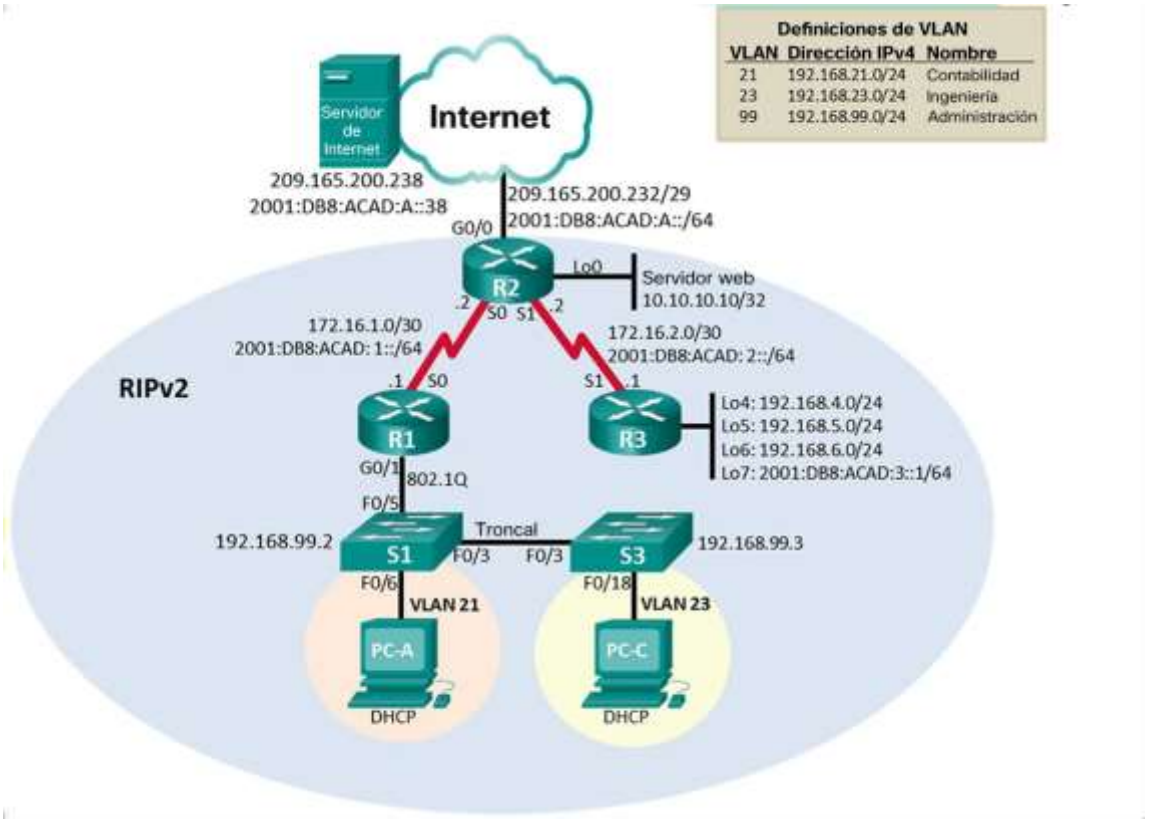
Técnicas o parámetros usados en el desarrollo del trabaja fue la implementación practica de los dispositivos.

6 DESARROLLO DEL PROYECTO

Escenario 1

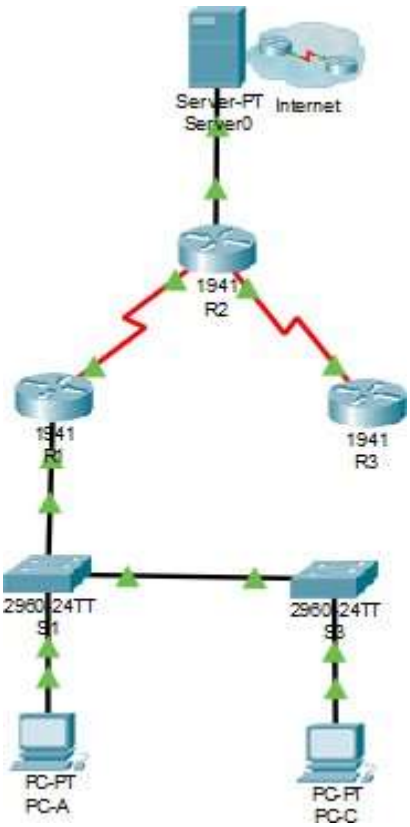
Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de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

Figura 1:Topología escenario 1



Parte 1: Inicializar dispositivos

Figura 2:Topología Escenario 1



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.

Tabla 1: Iniciar y volver a cargar los Router y los Switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar	Erase startup-config Delete vlan.dat

la base de datos de VLAN anterior	
Volver a cargar ambos switches	reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Show flash

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):

Tabla 2: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	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3:Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup con este comando lo desactivamos la búsqueda DNS
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description conection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 This command applies only to DCE interfaces R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4:Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup con este comando lo desactivamos la búsqueda DNS
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Habilitar el servidor HTTP	Ip http serve
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description conection to R1 R1(config-if)#ip address 172.16.1.2 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::2/64 R1(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description conection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description conection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int lo0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulated Web Server R2(config-if)#
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5:Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup con este comando lo desactivamos la búsqueda DNS
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Password: R3#conf t R3(config)#int s0/0/1 R3(config-if)#description conection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown R3(config-if)#
Interfaz loopback 4	R3(config-if)#int lo4 R3(config-if)#ip addres 192.168.4.1 255.255.255.0 R3(config-if)#
Interfaz loopback 5	R3(config-if)#int lo5 R3(config-if)#ip addres 192.168.5.1 255.255.255.0 R3(config-if)#

Interfaz loopback 6	R3(config-if)#int lo6 R3(config-if)#ip addres 192.168.6.1 255.255.255.0 R3(config-if)#
Interfaz loopback 7	R3(config-if)#int lo7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6:Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup con este comando lo desactivamos la búsqueda DNS
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7

Tabla 7:Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup con este comando lo desactivamos la búsqueda DNS
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Paso 7: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8:Verificar ña conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	Recibidos
R2	R3, S0/0/1	172.16.2.2	Recibidos
PC de Internet	Gateway predeterminado	209.165.200.233	Recibidos

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

Figura 3:Verificar conectividad de la red R1

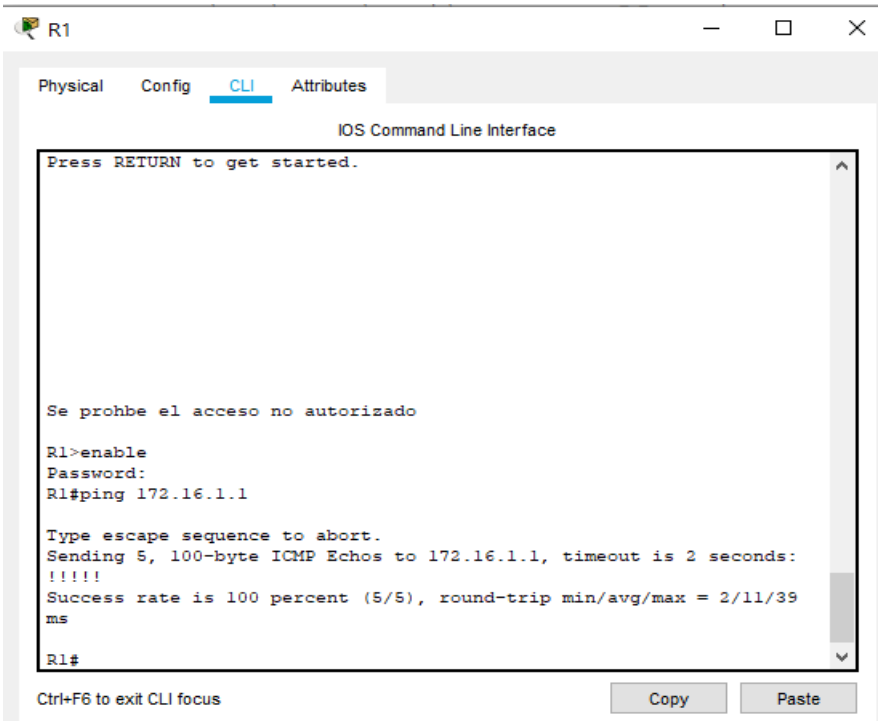


Figura 4:Verificar conectividad de la red R2

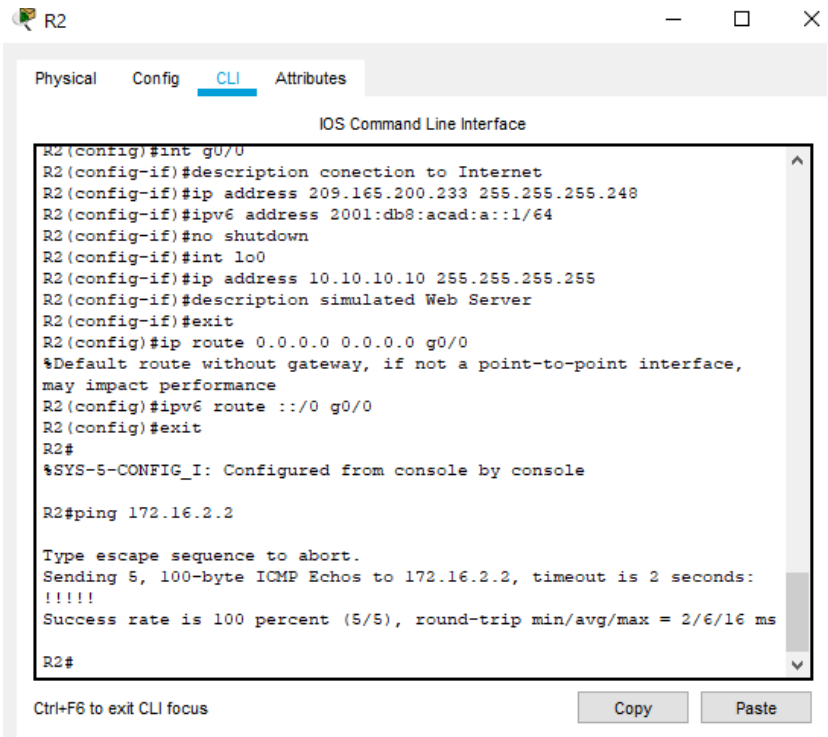
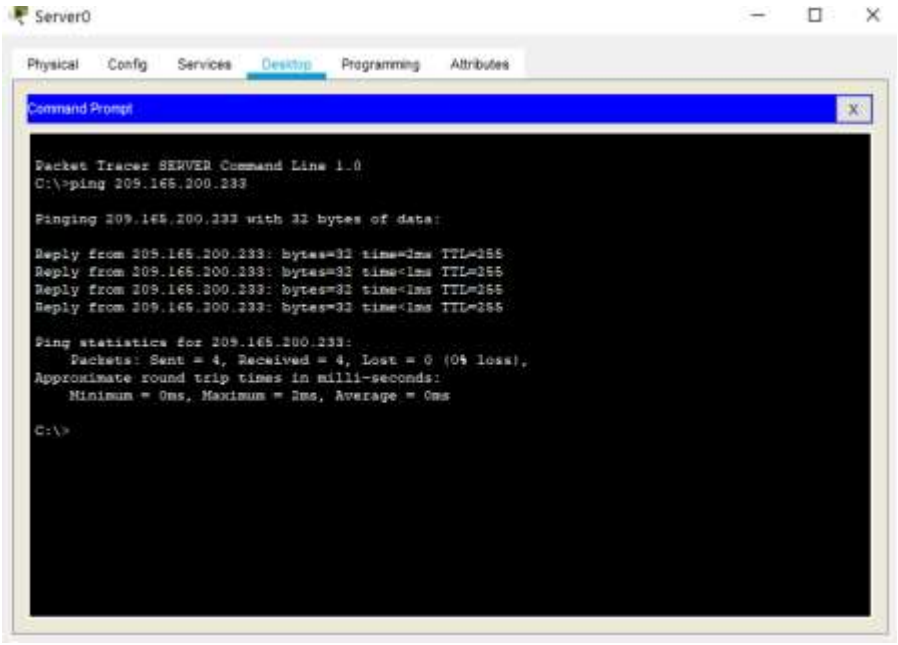


Figura 5:Verificar conectividad de la red Server0



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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9:Configurar 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 Administration S1(config-vlan)#

Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21 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)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10:Configurar 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
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)#switch mode trunk S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
Asignar F0/18 a la VLAN 21	S3(config-if-range)#switchport mode access S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11:Configurar R1

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

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:Verificar la conectividad de la red

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

Figura 6:Verificar conectividad de la red S1

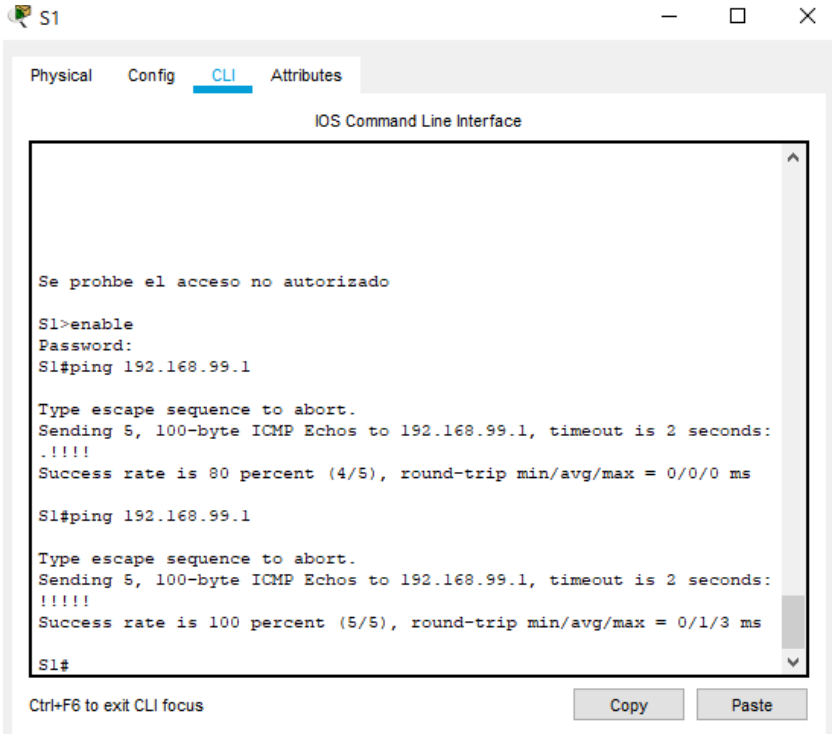


Figura 7:Verificar conectividad de la red S3

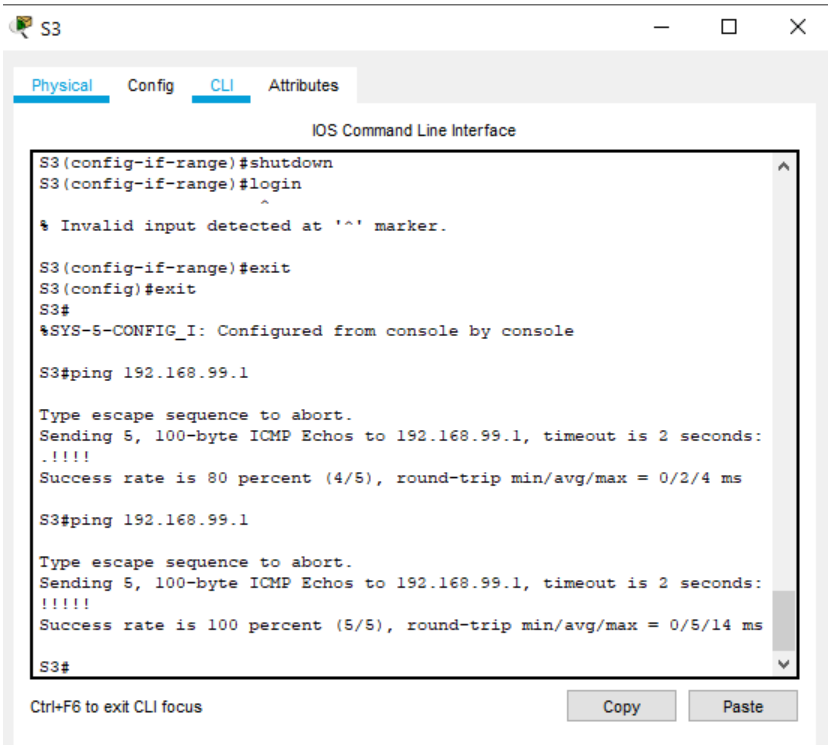
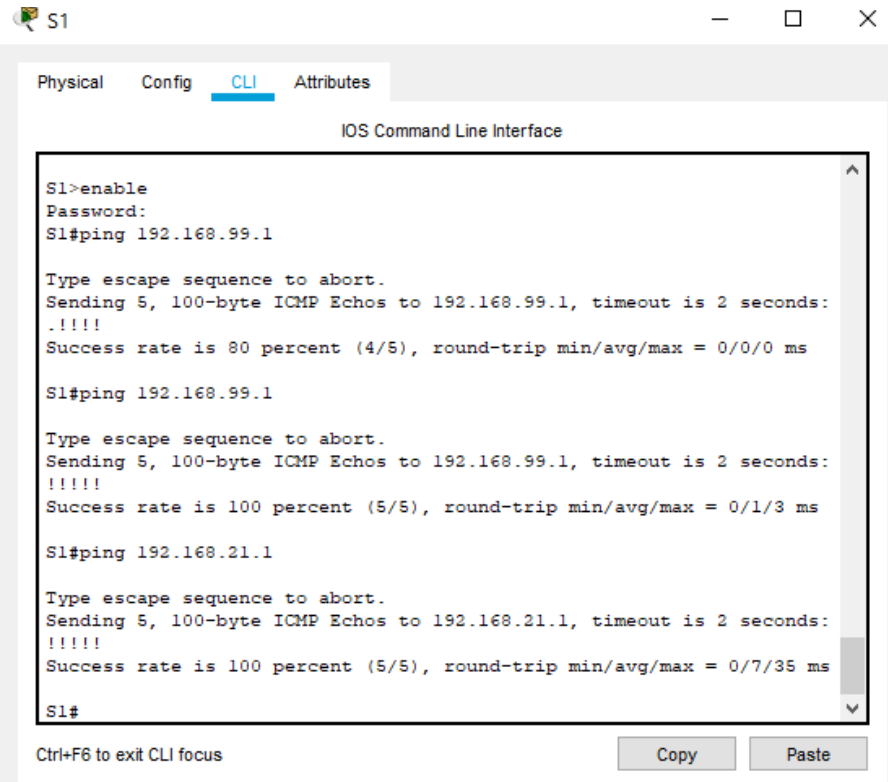


Figura 8:Verificar conectividad de la red S1



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:Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	En opciones de configuración ingrese los comandos rueter rip, versión 2
Anunciar las redes conectadas directamente	do show ip route conne
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14:Configurar RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2 R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 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
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. network 10.10.10.10 network 172.16.1.0 network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	passive-interface loopback 0
Desactive la sumarización automática.	no auto-summary

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15:Configurar RIPv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2 R3(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6
Anunciar redes IPv4 conectadas directamente	do show ip route conne
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface loopback 4 passive-interface loopback 5 passive-interface loopback 6
Desactive la sumarización automática.	no auto-summary

Paso 4: Verificar la información de RIP

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

Tabla 16:Verificar la información de RIP

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

Parte 5: Implementar DHCP y NAT para IPv4

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

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.31.1 192.168.31.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.33.1 192.168.33.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18:Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	el comando es ip http server

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No funcionó pero el comando es ip http authentication
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	Int lo 0, ip nat inside, int g0/0, ip nat aoutside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	ip nat inside sourse list l pool Internet

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 19:Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Dhcp faul
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Dhcp faul
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	correcto

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**	Request Timeout

Parte 6: Configurar NTP

Tabla 20:Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar
Verifique la configuración de NTP en R1.	do show ntp associations

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

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

Tabla 21:Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	correcto

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

Tabla 22:Introducir el comando de CLI adecuado

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

Escenario 2

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

Figura 9:Topología de red

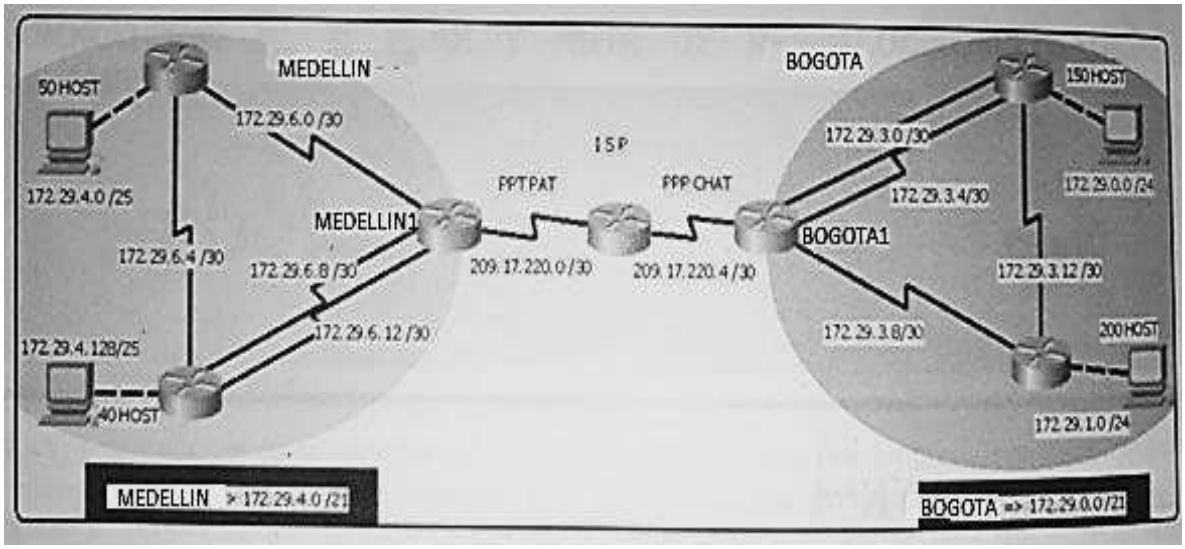


Fig. 9

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

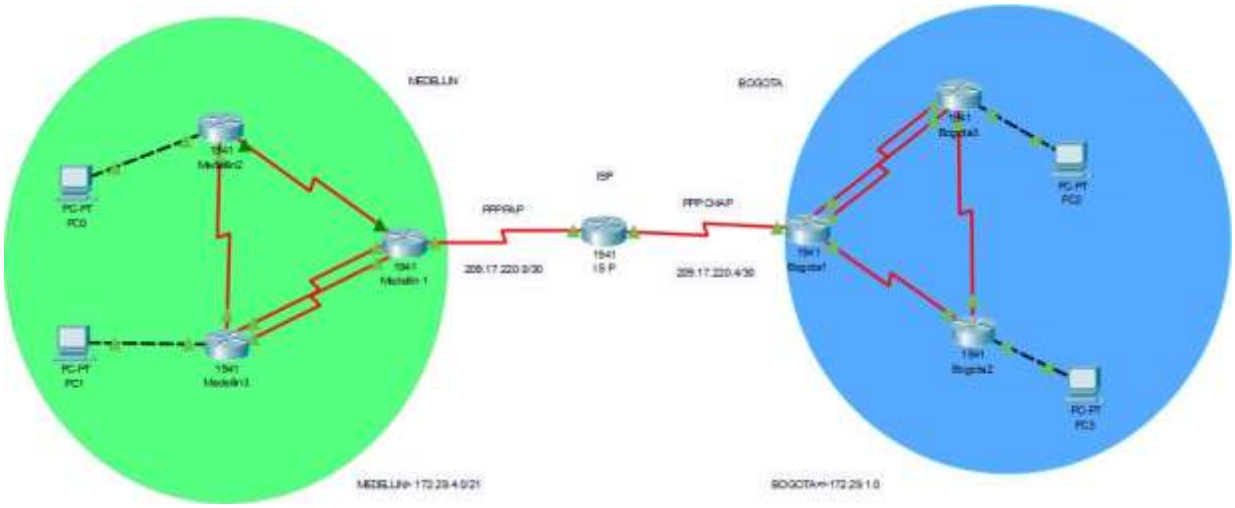
Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

Figura 10:Topología de red implementada



Parte 1: Configuración del enrutamiento

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

Bogota 1

Router(config)#router ospf 1

Router(config-router)#version 2

Router(config-router)#passive-interface Serial0/0/0

Router(config-router)#network 172.29.1.0

Router(config-router)#network 209.17.220.0

Router(config-router)#no auto-summary

Medellin 1

Router(config)#router ospf 1

Router(config-router)#version 2

Router(config-router)#passive-interface Serial0/0/0

Router(config-router)#network 172.29.1.0

Router(config-router)#network 209.17.220.0

Router(config-router)#no auto-summary

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

Medellin 1

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#route ospf 1
Router(config-router)#version 2
Router(config-router)#network 172.29.6.0
Router(config-router)#network 172.29.6.8
Router(config-router)#network 172.29.6.12
Router(config-router)#network 209.17.220.0
Router(config-router)#no auto-summary
Router(config-router)#
Router(config-router)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2
Router(config)#router ospf 1
Router(config-router)#default-information originate
```

Medellin 2

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#route ospf 1
Router(config-router)#version 2
Router(config-router)#network 172.29.6.4
Router(config-router)#network 172.29.6.0
Router(config-router)#network 172.29.4.0
```

Router(config-router)#no auto-summary

Router(config-router)#passive-interface f0/0

Medellin 3

Router>enable

Password:

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router ospf 1

Router(config-router)#version 2

Router(config-router)#network 172.29.6.4

Router(config-router)#network 172.29.6.8

Router(config-router)#network 172.29.6.12

Router(config-router)#network 172.29.4.128

Router(config-router)#no auto-summary

Router(config-router)#passive-interface f0/0

ISP

Router>enable

Password:

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router ospf 1

Router(config-router)#version 2

Router(config-router)#network 209.17.220.4

Router(config-router)#network 209.17.220.0

Router(config-router)#no auto-summary

Router(config-router)#exit

Router(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1

Router(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.5

Bogota 1

Router>enable

Password:

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router ospf 1

Router(config-router)#network 209.17.220.4

Router(config-router)#network 172.29.3.8

Router(config-router)#network 172.29.3.4

Router(config-router)#network 172.29.3.0

Router(config-router)#no auto-summary

Router(config-router)#exit

Router(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.6

Router(config)#router ospf 1

Router(config-router)#default-information originate

Bogota 2

Router>enable

Password:

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router ospf 1

Router(config-router)#version 2

Router(config-router)#network 172.29.3.8

Router(config-router)#network 172.29.3.12

Router(config-router)#network 172.29.1.0

Router(config-router)#no auto-summary

Router(config-router)#passive-interface f0/0

Bogota 3

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#version 2
Router(config-router)#network 172.29.3.0
Router(config-router)#network 172.29.3.4
Router(config-router)#network 172.29.3.12
Router(config-router)#network 172.29.1.0
Router(config-router)#no auto-summary
Router(config-router)#passive-interface f0/0
```

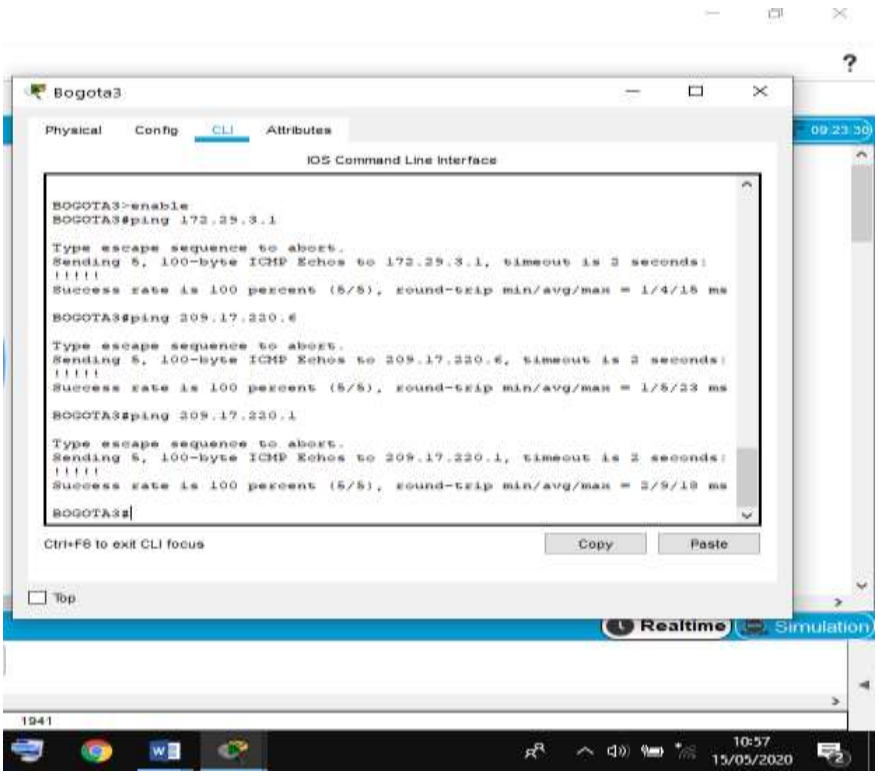
c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
Router(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.5
Router(config)#
```

Parte 2: Tabla de Enrutamiento.

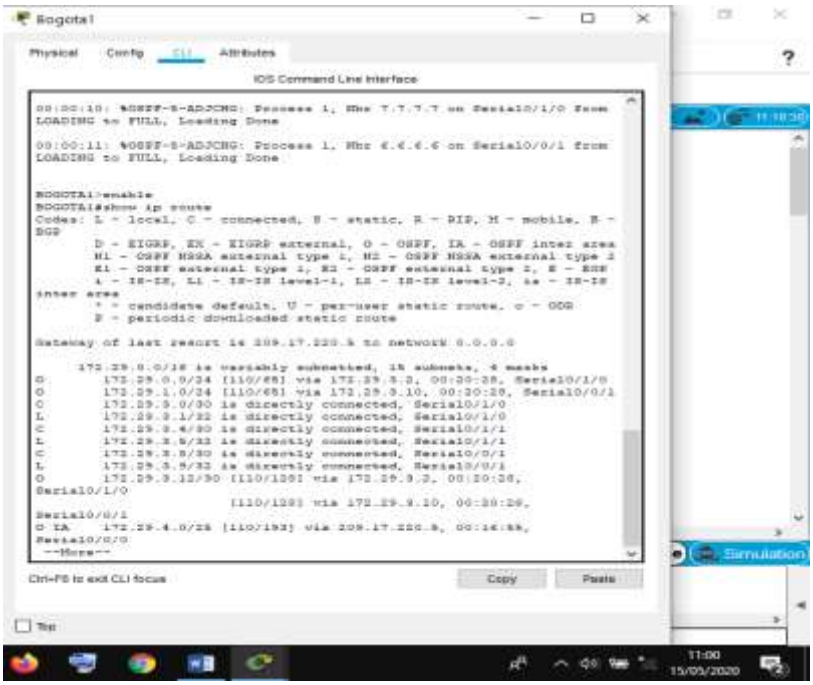
a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Figura 11:tabla de enrutamiento bogota3



b. Verificar el balanceo de carga que presentan los routers.

Figura 12:verificar balanceo de carga bogota1



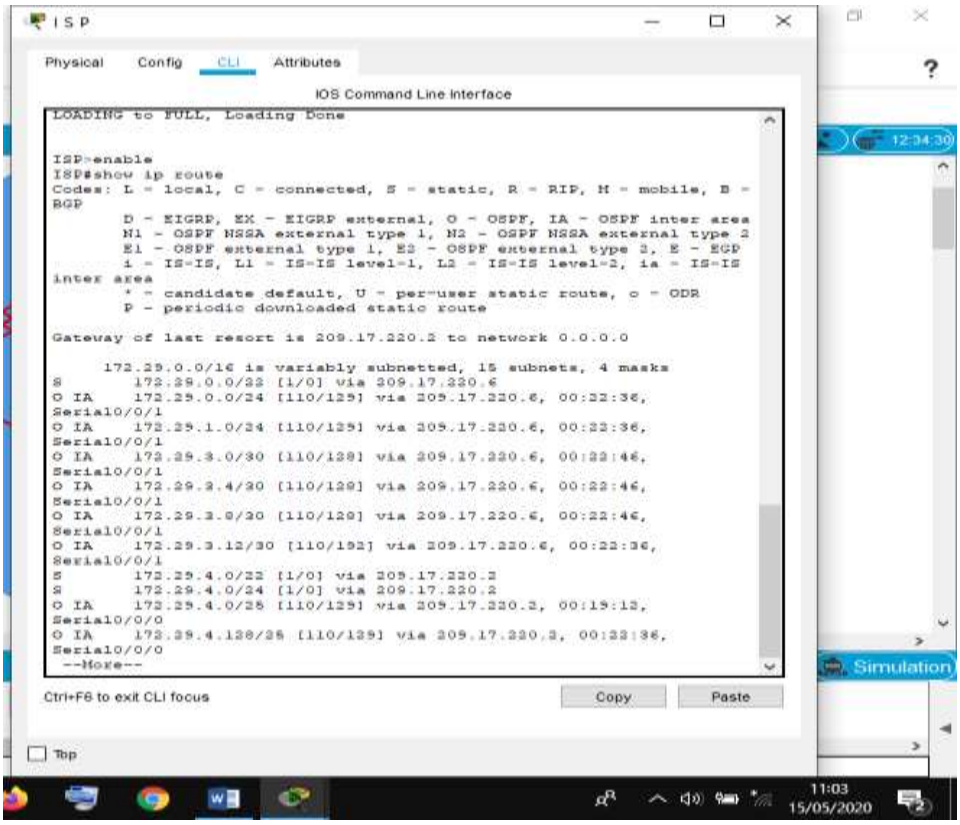
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

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

Figura 13:rutas estáticas Reuter ISP



Parte 3: Deshabilitar la propagación del protocolo OSPF.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 23:Deshabilitar la propagación del protocolo OSPF

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

Bogota 1

Bogota1>enable

Bogota1#conf t

Bogota1(config)#router ospf 1

Bogota1(config)#versión 2

Bogota1 (config-router)#Passive-interface s0/0

Bogota 2

Bogota2>enable

Bogota2#conf t

Bogota2(config)#router ospf 1

Bogota2(config)#versión 2

Bogota2 (config-router)#Passive-interface s0/0

Bogota 3

Bogota3>enable

Bogota3#conf t

Bogota3(config)#router ospf 1

Bogota3(config)#versión 2

Bogota3 (config-router)#Passive-interface fa0/0

Bogota3(config-router)#Passive-interface s0/2

Medellin1

Medellin1>enable

Medellin1#conf t

Medellin1(config)#router ospf 1

Medellin1(config)#versión 2

Medellin1(config-router)#passive-interface fa0/0

Medellin1(config-router)#passive-interface s0/2

Medellin 2

Medellin2>en

Medellin2#conf t

Medellin2(config)#router ospf 1

Medellin2(config)#versión 2

Medellin2(config-router)#passive-interface s0/1

Medellin 3

Medellin3>en

Medellin3#conf t

Medellin3(config)#router ospf 1

Medellin3(config)#versión 2

Medellin3(config-router)#passive-interface fa0/0

Parte 4: Verificación del protocolo OSPF.

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.

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.

Se ejecuta el comando show ip route en los diferentes router de la red

Figura 14: Verificación del protocolo OSPF Medellín 1

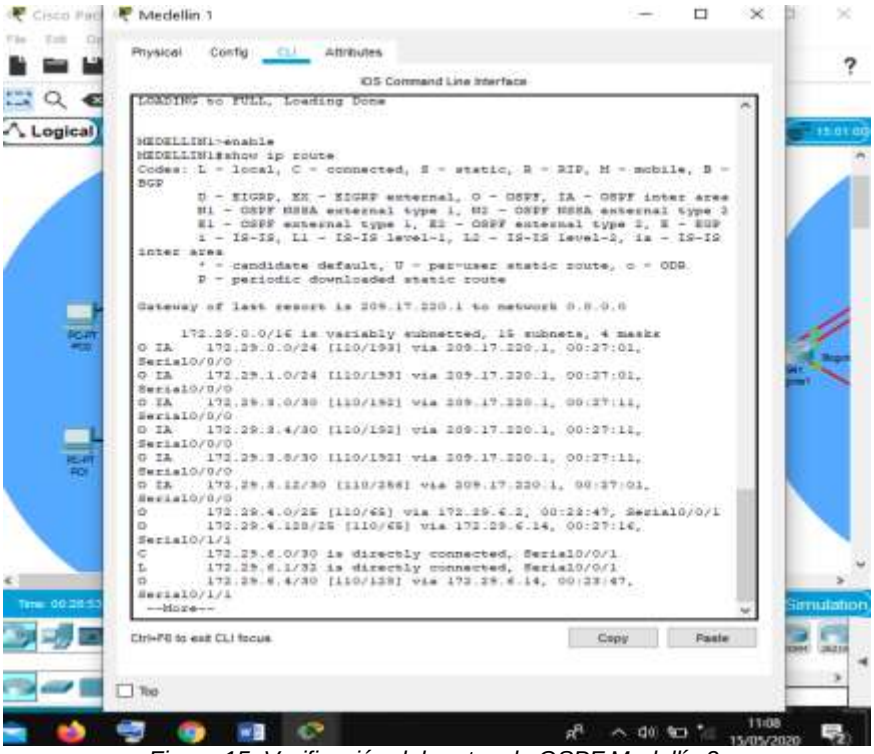


Figura 15: Verificación del protocolo OSPF Medellín 2

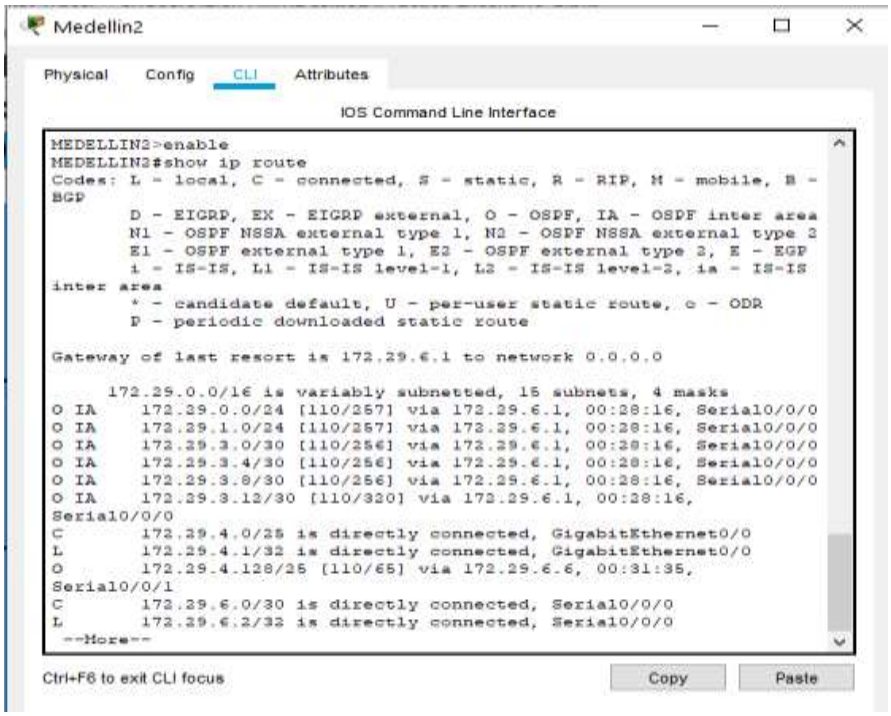
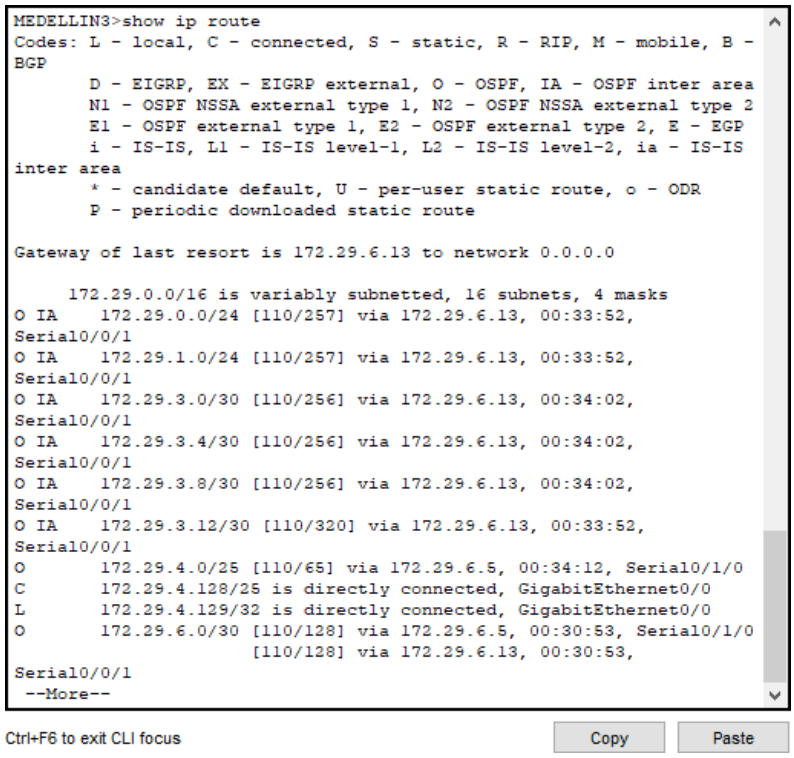


Figura 16: Verificación del protocolo OSPF Medellín 3



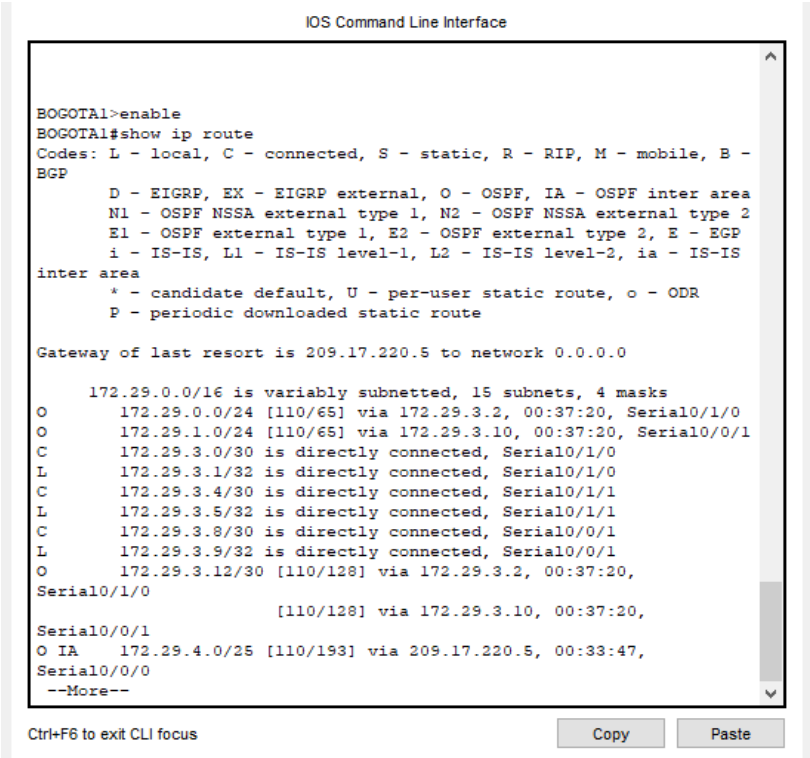
```
MEDELLIN3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.6.13 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 16 subnets, 4 masks
O IA    172.29.0.0/24 [110/257] via 172.29.6.13, 00:33:52,
Serial0/0/1
O IA    172.29.1.0/24 [110/257] via 172.29.6.13, 00:33:52,
Serial0/0/1
O IA    172.29.3.0/30 [110/256] via 172.29.6.13, 00:34:02,
Serial0/0/1
O IA    172.29.3.4/30 [110/256] via 172.29.6.13, 00:34:02,
Serial0/0/1
O IA    172.29.3.8/30 [110/256] via 172.29.6.13, 00:34:02,
Serial0/0/1
O IA    172.29.3.12/30 [110/320] via 172.29.6.13, 00:33:52,
Serial0/0/1
O       172.29.4.0/25 [110/65] via 172.29.6.5, 00:34:12, Serial0/1/0
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
O       172.29.6.0/30 [110/128] via 172.29.6.5, 00:30:53, Serial0/1/0
                      [110/128] via 172.29.6.13, 00:30:53,
Serial0/0/1
 --More--
```

Ctrl+F6 to exit CLI focus Copy Paste

Figura 17:Verificación del protocolo OSPF Bogotá 1



IOS Command Line Interface

```
BOGOTA1>enable
BOGOTA1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.5 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O       172.29.0.0/24 [110/65] via 172.29.3.2, 00:37:20, Serial0/1/0
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:37:20, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/1/0
L       172.29.3.1/32 is directly connected, Serial0/1/0
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/0/1
L       172.29.3.9/32 is directly connected, Serial0/0/1
O       172.29.3.12/30 [110/128] via 172.29.3.2, 00:37:20,
Serial0/1/0
                       [110/128] via 172.29.3.10, 00:37:20,
Serial0/0/1
O IA    172.29.4.0/25 [110/193] via 209.17.220.5, 00:33:47,
Serial0/0/0
 --More--
```

Ctrl+F6 to exit CLI focus Copy Paste

Figura 18:Verificación del protocolo OSPF Bogotá 2

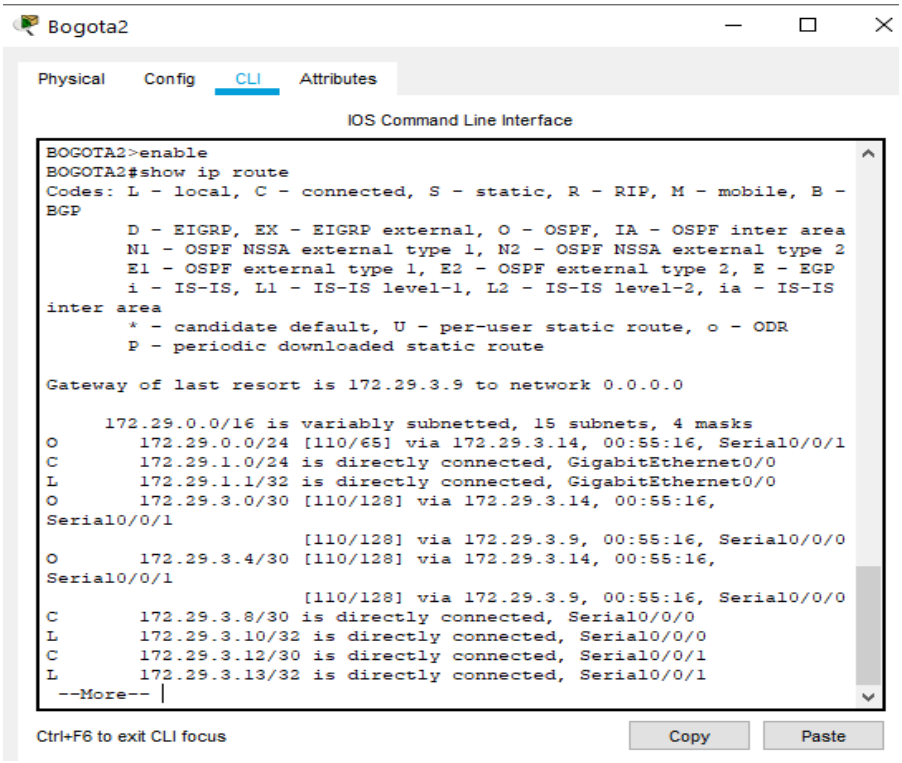
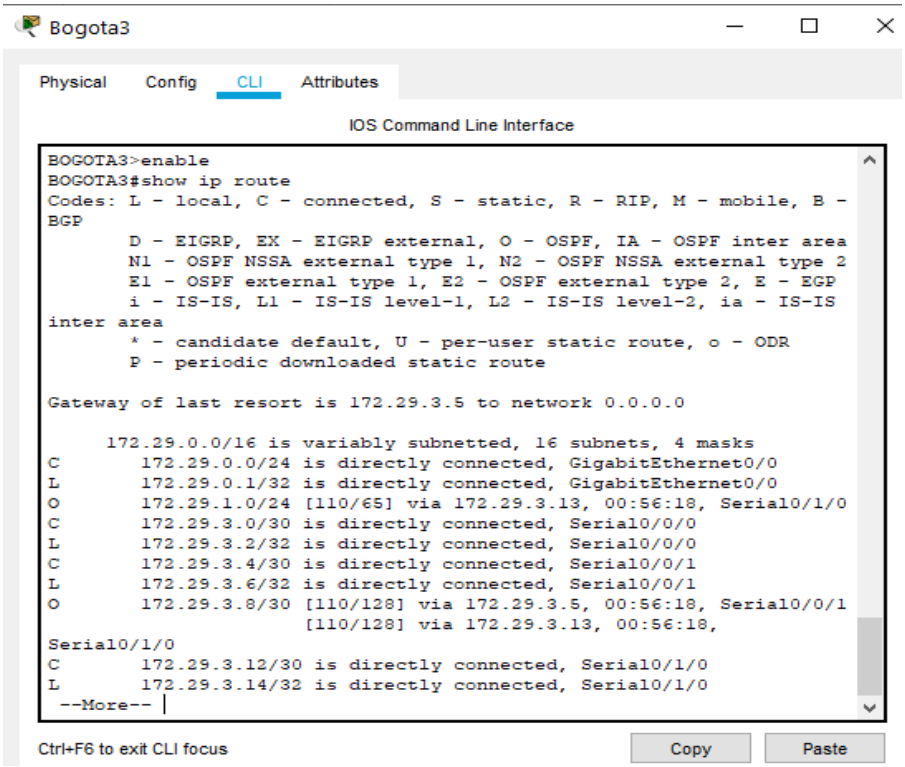


Figura 19:Verificación del protocolo OSPF Bogotá 3



Parte 5: Configurar encapsulamiento y autenticación PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

ISP

```
ISP>enable
Password:
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation PPP
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
```

Medellin1

```
Medellin1>enable
Password:
Medellin1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#username ISP password cisco
Medellin1(config)#int s0/1/0
Medellin1(config-if)#encapsulation PPP
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username Medellin_1 password cisco
Medellin1(config-if)#
```

b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

ISP

```
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#username Bogota_1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

ISP(config-if)#ppp authentication chap

ISP(config-if)#exit

ISP(config)#

BOGOTA_1

Bogota_1>enable
Password:
Bogota_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#username ISP password cisco
Bogota1(config)#int s0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#

Parte 6: Configuración de PAT.

a. 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.
b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.
c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Medellin1

Medellin1>enable

Password:

Medellin1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Medellin1(config)#ip nat inside source list 1 interface s0/1/0 overload

Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255

Medellin1(config)#int s0/1/0

Medellin1(config-if)#ip nat outside

Medellin1(config-if)#int s0/0/0

Medellin1(config-if)#ip nat inside

Medellin1(config-if)#int s0/0/1

Medellin1(config-if)#ip nat inside

Medellin1(config-if)#int s0/1/1

Medellin1(config-if)#ip nat inside

Medellin1(config-if)#

Bogota

Bogota_1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Bogota1(config)#ip nat inside source list 1 interface s0/0/0 overload

Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255

Bogota1(config)#int s0/0/0

Bogota1(config-if)#ip nat outside

Bogota1(config)#int s0/1/0

Bogota1(config-if)#ip nat inside

Bogota1(config-if)#int s0/0/1

Bogota1(config-if)#ip nat inside

Bogota1(config-if)#int s0/1/1

Bogota1(config-if)#ip nat inside

Bogota1(config-if)#

Parte 7: Configuración del servicio DHCP.

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

Medellin2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
Medellin2(config)#ip dhcp pool Medellin2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-route 172.29.4.1
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
Medellin2(config)#end
Medellin2#
Medellin2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#ip dhcp pool Medellin_3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-route 172.29.4.129
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
Medellin2(config)#
```

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

```
Medellin3>en
Medellin3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#int f0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
```

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

```
Bogota2>enable
Password:
Bogota2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 Bogota_2
```

```
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-route 172.29.1.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#p dhcp pool Bogota_3
% Ambiguous command: "p dhcp pool Bogota_3"
Bogota2(config)#ip dhcp pool Bogota_3
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-route 172.29.0.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#exit
```

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

```
Bogota3>en
Bogota3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#int f0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
```

6.1 ANÁLISIS DEL DESARROLLO DEL PROYECTO

Durante el desarrollo del proyecto puedo definir que lo más fundamental fue que me brindo teorías e implementación de herramientas para configurar una red básica con los diferentes componentes bien configurados, por lo tanto, considero que amplio el grado de conocimiento en las redes y su configuración haciéndome un ingeniero con mayor capacidad de reacción en este ámbito

6.2 CRONOGRAMA

Tabla 24:Cronograma

ÍTEM	DESCRIPCIÓN	TIEMPO
Escenario 1	La implementación y desarrollo del escenario con todas las configuraciones a los dispositivos.	6 días
Escenario 2	La implementación y desarrollo del escenario con todas las configuraciones a los dispositivos.	4 días
Estructura del trabajo	Ajustes del documento de acuerdo a las normas requerida “Icontec”	1 días

CONCLUSIONES

En estos escenarios pude implementar el tema de direccionamiento IP con los protocolos TCP/IP que son la base del direccionamiento, esto con el objetivo de interconectar las dos sucursales de la empresa que están ubicadas en diferentes ciudades como Medellín y Bogotá, así que realicé la configuración de los diferentes dispositivos como Reuter y pc con las respectivas direcciones IP y la máscara subred para que las comunicaciones de los equipos funcionen con normalidad.

En cuanto implementar seguridad a la red a través de deshabilitar los puertos de los SWITCHES que no se usaran a través de la interfaz de administración, puede evidenciar que el tráfico de la red se hace más ligero además de estar más segura la interconexión de la red.

Al establecer el dominio de VLAN para que la interconexión de la red no se dé sino con ROUTING que se haya especificado, esto se hizo a través de RIPv2 que es uno de los protocolos más sencillo de configurar y muy práctico para estilo de red y con el apoyo de la configuración del servidor con DHCP se le proporciono un direccionamiento IP a cada dispositivo para su interconexión.

Para la interconexión de la red del escenario utilice los protocolos IPV4 E IPV6 que son los protocolos vigentes de enrutamiento, aunque el IPV6 surgió en reemplazo de la V4 dado que proporciona una infraestructura más que completa para soportar la interconexión global con niveles altos de seguridad.

Muy relevante fue la implementar las soluciones a los escenarios dispuestos a desarrollar dado que pude evidenciar un aprovechamiento de los recursos o elementos adoptados durante su implementación, cada dispositivo y su respectiva configuración de los mismos adecuadamente por medio de la utilización de los siguientes protocolos: TCP/IP, IPV4 E IPV6 OSPF, DHCP, RIPv2 PPP, NAT.

RECOMENDACIONES

Como recomendación les dejo que revisen el material didáctico del curso para que estén familiarizados con todos los conceptos, comandos y configuraciones que se realizaron y pueda haber una mayor comprensión de las temáticas abordadas en este documento.

BIBLIOGRAFÍA

Byspel, B. (2017, 14 junio). Configurar servidor DHCP en Packet Tracer. Recuperado 5 junio, 2019, de https://byspel.com/configurar-servidor-dhcp-en-cisco- packet-tracer/

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

Exploración de la red Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

Victor E. Martinez G, V. E. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado 5 junio, 2019, de http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route-router-cisco/